European Commission

Is Commercial Cellular Suitable for Mission Critical Broadband?

Study on use of commercial mobile networks and equipment for "mission-critical" high-speed broadband communications in specific sectors

FINAL REPORT

A study prepared for the European Commission
DG Communications Networks, Content & Technology by:

SCF ASSOCIATES LTD

Digital Agenda for Europe

This study was carried out for the European Commission by

SCF ASSOCIATES LTD

Authors: Simon Forge, Robert Horvitz and Colin Blackman

Cover images: Right and middle images: SCF Associates Ltd; left image: Wikia

Internal identification

Contract number: 30-CE-0603428/00-19

SMART number: 2013/0016

DISCLAIMER

By the European Commission, Directorate-General of Communications Networks, Content & Technology.

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

ISBN: 978-92-79-38679-4

DOI: 10.2759/54788

Contents

Figures

Tables

Abstract

This study examines the requirements, relative costings and possible implementations of broadband mission critical radio networks for three sectors – public protection and disaster relief (PPDR), utilities and intelligent transport services (ITS) for road and rail. Such services have traditionally been voice oriented, with dedicated networks having exclusive spectrum. New digital applications, such as smart grids for utilities, live video links for medical imaging and policing, call for broadband data. At this time, Europe's mobile network operators (MNOs) are rolling out mobile broadband based on the next generation of mobile technology for broadband (LTE). However, there is some reluctance within the mission critical sectors to employ commercial mobile services exclusively. Their major reservation is whether commercial operators are willing and able to provide long-term reliable and resilient services with the needed coverage and quality. Consequently the European Commission requested an independent study assessing the viability of future commercial mobile broadband networks for these applications. The study considered five options for implementation, analysing cost-benefits to compare them. The key conclusion is that commercial LTE networks could support mission critical needs but only if certain conditions are met. These conditions would fundamentally change the operating environment for the commercial mobile networks.

Résumé

La présente étude examine les exigences, les coûts relatifs et les mises en œuvre possibles de réseaux critiques de radiocommunications à bande large dans le cadre de trois secteurs (la protection civile et les secours en cas de catastrophe (PCSC), les services publics et les systèmes de transport intelligents (STI) routiers et ferroviaires). Traditionnellement, ces services ont été orientés vers la voix et ont disposé de réseaux dédiés avec des fréquences exclusives. Les nouvelles applications numériques, comme les réseaux intelligents pour les services publics ou les liaisons vidéo pour l'imagerie médicale et la police, nécessitent des données à large bande. À l'heure actuelle, les opérateurs de réseau mobile (ORM) européens déploient une large bande mobile basée sur la prochaine génération de technologies mobiles pour large bande (LTE). Néanmoins, les secteurs critiques font preuve d'une certaine réticence lorsqu'il s'agit d'avoir recours, à titre exclusif, aux services mobiles commerciaux. Leur principale réserve porte sur la question de savoir si les opérateurs commerciaux sont disposés et en mesure de fournir des services résistants, fiables et à long terme, qui offrent le niveau de couverture et de qualité nécessaire. C'est dans ce contexte que la Commission européenne a sollicité la réalisation d'une étude indépendante, en vue d'évaluer la viabilité des futurs réseaux mobiles commerciaux à large bande pour ces applications. L'étude a considéré cinq options de mise en œuvre et a analysé les coûts et bénéfices afférents à chacune d'entre elles, afin de les comparer. La principale conclusion de l'étude est que les réseaux LTE commerciaux pourraient répondre aux besoins des secteurs critiques, mais uniquement si certaines conditions sont remplies. Ces conditions modifieraient fondamentalement l'environnement opérationnel des réseaux mobiles commerciaux.

Fazit

Diese Studie untersucht die Voraussetzungen, relativen Kosten und möglichen Einsatzbereiche von missionskritischen Hochgeschwindigkeits-Breitband-Mobilfunknetzen in drei Sektoren - Sicherheits- und Rettungsdienste (PPDR), Versorgungswirtschaft sowie Intelligente Verkehrssysteme (ITS) für den Straßen- und Schienenverkehr. Diese Dienste verfügen traditionell über eigene Sprechfunknetzwerke auf reservierten Frequenzen. Neue digitale Anwendungen, wie z. B. intelligente Netze von Versorgungsunternehmen, Live-Videoverbindungen für die bildgebende Diagnostik oder die polizeiliche Überwachung usw. sind jedoch von einer Breitband-Datenübertragung abhängig. Derzeit bauen die europäischen Mobilfunknetzbetreiber ihre Breitbandnetze nach dem neuesten Mobilfunkstandard (LTE) weiter aus. Viele missionskritische Sektoren sind jedoch noch nicht bereit, sich ausschließlich auf kommerzielle Funknetze zu verlassen. Sie zweifeln insbesondere daran, ob die kommerziellen Anbieter willens und in der Lage sind, langfristig zuverlässige und ausfallsichere Dienste mit der nötigen Reichweite und Qualität bereitzustellen. Aus diesem Grund hat die Europäische Kommission eine unabhängige Studie in Auftrag gegeben, in der untersucht werden soll, ob für diese Sektoren künftig kommerzielle Breitband-Mobilfunknetze genutzt werden können. In der Studie wurden fünf Optionen anhand der Kriterien Umsetzung, Kosten und Nutzen miteinander verglichen. Sie kommt zu dem Ergebnis, dass kommerzielle LTE-Netze unter bestimmten Voraussetzungen für missionskritische Dienste geeignet sind. Diese Voraussetzungen würden jedoch die Geschäftsbedingungen für kommerzielle Mobilfunknetze grundlegend verändern.

Executive Summary

The aim of this study is to evaluate the options for mission critical communications utilising mobile broadband in three sectors – public protection and disaster relief (PPDR, principally police, fire and emergency medical services), utilities (electricity, gas and water) and the intelligent transport systems (ITS) now entering service, with a focus on road and rail. The two main options considered are the public land mobile networks (PLMNs) run by commercial operators and the dedicated networks created specifically for use in these sectors.

European society depends on mission critical services

Public safety, the assurance of working utilities and reliably operating transport systems are essential for modern European society. Such services cannot function without radio networks and increasingly they require wide-area wireless broadband support. This study examines the past, present and future of mobile communication for mission critical services in the three sectors. Traditionally, each sector has had its own dedicated networks, often with exclusive spectrum allocations.

To cite just one example, PPDR in the EU Member States (MS) has benefitted from significant capital investment (capex) of at least €19 billion. (The total may be higher as public accounts differ in transparency and completeness.) Most of the investment has been in TETRA and TETRAPOL technologies, with limited potential to support new data services, even though the voice channels might well be useful for another decade or more and so will form the basis for certain PPDR networks until a replacement technology is available. Moreover, the suppliers of mission critical technologies are specialised and few in number, with limited potential markets in Europe and globally. So economies of scale from the mass production of equipment cannot be attained and the small number of suppliers restricts competition. Furthermore, while international cooperation between PPDR and other vital services is growing in importance, interworking different manufacturers' implementations of TETRA and TETRAPOL has proven difficult. PPDR users are effectively locked in to specific implementations of the standards that interfere with cooperation across borders, jurisdictions and sectors.

European rail networks are currently deploying a 900 MHz service based on their own private communications networks, using a variant of GSM which could ultimately cost over €25 billion (our estimate). GSM is still the most widely supported cellular technology and it is well suited to the railways' needs. But it is similar to TETRA and TETRAPOL in having a limited number of sources of mission critical equipment designed specifically for railway use, and a very uncertain future, as the cellular industry wants to phase out GSM in favour of 3G and 4G. Thus, just how future support for the railways' new wireless networks would be provided is quite unclear.

Meanwhile, mission critical applications are now developing rapidly. Smart grids for utilities, video for road traffic management and medical imaging for ambulance teams require broadband data channels accessible across wide geographic areas. Broadband is becoming increasingly important for saving lives, keeping the lights on, preventing accidents and maintaining public order.

In this context, Europe's mission critical services are undergoing a major change as dependence on digital technology rises. Furthermore, the concept of "mission critical" communications is spreading from PPDR into other sectors as the European economy's interconnectedness and dependence on information-rich capabilities grows. As a result, the definition of "mission critical" is being extended from the key functions which protect safety of life to include maintenance of the macro-economy's smooth functioning (practical definitions for the future are explored in Section 2.4.).

More efficient mobile broadband networks are appearing, but there is a complication

In this context it appears fortunate that Europe's mobile network operators (MNOs) are currently rolling out high-speed mobile broadband. However, the mission critical sectors have reasonable apprehensions about relying exclusively on commercial mobile services, with two major reservations:

- Can commercial operators be trusted to provide reliable services under fixed-price contracts over long periods of time?

- Will they provide the needed level of network availability, resilience, service quality, security and coverage, particularly in emergencies?

Each of the three sectors considered here is closely allied with governments and the public sector as a whole. The emergency services expect government grants of priority resources, such as free spectrum and rights of way. But all EU Member States face budgetary constraints resulting from the financial crisis of 2008 and rising long-term debts. The squeeze on public services is expected to continue for a decade or more, leading to a contradiction: public services must reign in their spending even though citizens always expect them to do more.

Are commercial mobile networks a viable mission critical solution?

In an age of persistent austerity the question is increasingly asked: can commercial mobile networks adequately support mission critical communications, for broadband and voice? The economic advantages of using the same broadband technology base, infrastructure and spectrum bands for mission critical users as well as the mass market seem clear. But the question is whether the cost savings come with sufficient resilience and performance.

In response to the pressure on public budgets and the introduction of a new more efficient generation of mobile broadband technology, the European Commission requested an in-depth independent study of the costs and benefits of using commercial networks for mission critical purposes. SCF Associates Ltd. was asked to explore the communication requirements and options in three sectors – PPDR, utilities, and ITS – through a close examination of five scenarios.

It should be emphasised that the objective of this study is to examine the introduction of mobile *broadband* to mission critical services via commercial MNO networks. Moreover this study should examine the needs of *all three* sectors (utilities, ITS – road and rail – and PPDR).

These five scenarios explore the options on a cost basis among dedicated networks, commercial networks from the MNOs and new LTE commercial equipment hardened for use on a dedicated network. Our conclusions are that in general, the capex per user for commercial LTE networks, hardened and with geographic coverage extended to 99% of national territories, would be less than the capex per user for dedicated LTE networks. This is also the most attractive option in terms of value for money when capex and opex are combined, although the cost advantages vary according to which frequency bands are used. At 450 MHz, the cost per user of a dedicated network is cheaper in capex by over 40% compared to the commercial mobile broadband network at 800MHz. But when 10 years of opex is taken into account, the sharing of infrastructure costs favours the commercial networks, whether operating at 450, 700 or 800 MHz. A commercial LTE network operating at 800 MHz can give a capex cost per user that is lower by some 40% than a dedicated LTE network at 700 MHz. (If MNOs decide to operate commercial mission critical networks in the 700 MHz band, the capex costs could be up to 20% less than a similar network at 800 MHz.)

But cost is not the only consideration. Our overall conclusion is that it could be possible for commercial mobile broadband networks to be used for mission critical purposes but only ***if five conditions are met***.

The five conditions – which must be met in full – are these:

1. First the behaviour of commercial MNOs must be constrained to provide the services needed by mission critical users while preventing the use of "lock in" techniques to take unfair advantage of this expansion of the MNOs' market power and social responsibility. Such changes include not just stronger commitments to network resilience, but the acceptance of limits on price increases and contract condition revisions, ownership continuity assurances, and a focus on quality of service for priority mission critical traffic. Equally important for long-term relationships will be the mission critical services' *perception* of MNO behaviour and performance. For that, measures will be needed that go beyond service level agreements (SLAs) at a commercial contract level: new regulations regarding commercial MNOs services must be enforced by each Member State's national regulatory agency (NRA).
2. Commercial networks have to be "hardened" from RAN to core and modified to provide over 99% availability – with a target of "five nines". Geographic coverage must also be extended as needed for mission critical purposes and indoor signal penetration improved at agreed locations.
3. All this network hardening and extended coverage, along with the addition of essential mission critical functions and resilience, must be accomplished at reasonable cost. No more should be spent on the selective expansion and hardening of commercial networks for mission critical use than it would cost to build a dedicated national LTE network for that purpose.
4. Hardened LTE networks must be able provide the different types of service required by each of the three sectors. Each sector uses broadband in quite different ways. That is, not just for streaming video, image services and database access, as in PPDR, but for very low-latency telemetry and real-time control for utilities and transport. In the five network options examined in Chapter 4, accommodating the needs of the different sectors becomes easier as one moves from existing dedicated networks to LTE and then to more complex hybrid configurations.
5. However, there is a further high barrier: will commercial mobile networks be able to overcome ingrained Member State preferences for state controlled networks for applications that implicate public safety? This is not simply a legal, regulatory or economic question. Some Member States have specific histories of state control as part of their culture, traditions and politics, not to mention investments in current technologies with long payback cycles. Thus some Member States may want to continue using dedicated networks in the short and medium term even if they cost more – examples are Germany, Italy and France for PPDR. However, it cannot be said that they will always ignore cheaper alternatives. The MNOs may need to be more persuasive in putting forward their advantages. In the meantime, it must be left to Member States to choose.

These obstacles to commercial use cannot be removed immediately. But for the medium and long term, sharing commercial MNO infrastructures for both public and mission critical purposes makes economic sense. The crucial barrier is the current MNO mass-market business model, which needs to be suitably amended to provide appropriate levels of service to priority clients with special needs. But *perceptions* of the MNOs will take some time to change. Hence, as mission critical networks are the responsibility of national administrations, it is likely that dedicated state-owned networks will continue to be the preferred model in the near term. But at least for budgetary reasons, each Member State may consider moving from dedicated closed networks to shared commercial networks as the five conditions above are satisfied.

What measures are needed to meet these conditions?

Costing the scenarios in Chapter 4 for commercial, dedicated, shared and hybrid networks, it appears that budgetary requirements can be satisfied in several different ways. Moreover, our investigation of LTE in Chapter 3 shows that its capabilities can be brought up to mission critical levels if the standards organisations deliver what they promise, on time.

To perform this study, the requirements shaping the wireless communications needs of the three sectors were explored in depth (see Chapter 2 and the Appendixes, which are an integral part of this report). The PPDR community's requirements are well articulated by organisations such as the Law Enforcement Working Party (LEWP) and the TETRA and Critical Communications Association (TCCA). However, police perspectives tend to dominate those articulations. Fire fighters, emergency medical personnel and disaster relief organisations have somewhat different needs and these must be taken into account as well. So we give more attention to their requirements than is often the case (see Appendix A).

For the utilities, industry associations including the EUTC (European Utilities Telecommunication Council) and Eurelectric as well as specific utilities (Iberdrola, Alliander and others) gave us detailed input. The European Railway Agency (ERA) provided essential information and further study revealed the emerging requirements of roadway transportation. Across the three sectors we found diverse requirements:

- PPDR users expect to use mobile broadband much more extensively in the future, although each subsector has a different agenda: video and high-resolution images are of growing importance to law enforcement, while real-time sensors (including infrared cameras and through-the-wall motion detectors) are increasingly sought by fire fighters. Emergency medical services need high-resolution images for remote assistance in making accurate onsite injury assessments and diagnoses, while search and rescue teams find video-equipped drones enable a few people to survey large areas efficiently.

- Utilities are less interested in broadband than in reliable wide-area collection of brief machine-to-machine (M2M) data bursts from millions of meters and substations. Variable inputs from solar cells and wind turbines are changing the architecture of power generation today and posing new challenges for voltage regulation and network stability. Smart grids will add two-way communication requirements and new services beyond resource distribution. Many utilities insist on direct control of communications networks since they are legally obliged to provide reliable services. They cannot shift responsibility to their suppliers so they are loath to depend on third parties, such as MNOs, for support of real-time operational control.

- Narrowband data communication over circuit switched voice links are the new norm for train control in Europe. But in the sphere of non-operational/non-mission-critical wireless, passenger access to the Internet via Wi-Fi may be essential to achieving the growth in train passenger numbers sought by the European Commission to meet reduction targets for greenhouse gas emissions. Road vehicle bandwidth demands are more diverse and harder to predict. They range from vehicle-to-vehicle communications at 5.9 GHz to eCall accident reporting via cellular, to roadside cameras automatically reading vehicle license plate numbers to enforce speed limits and collect tolls.

Identifying the different requirements, then seeing if network sharing across sectors is still feasible and pricing the different ways to satisfy the requirements – these were the main challenges of this study.

Looking at the supply side, the current and foreseeable capabilities of commercial mobile networks are examined in Chapter 3. The key arena for evolving these capabilities is the ETSI/3GPP partnership for LTE standards development. The study looked at the process of adding mission critical capabilities to LTE, specifically in Releases 12, 13 and 14, to understand the probable timetable for delivering equipment with functions like Direct Mode Operation, Push-To-Talk and priority calling. We also looked at LTE equipment deployment patterns among the MNOs in the Member States, since the availability of new equipment does not in itself force the replacement of older equipment. The implication of the current roadmap for LTE is that hardly any mission critical functionality will be available in the field before 2016, some might be available in some places by 2018 and much more by 2020. Thus, before 2020, the LTE technology available for mission critical networks may be not be fully standardised.

The other major requirement for the introduction of new mission critical broadband networks is the availability of UHF frequencies. For cost effective equipment, a crucial parameter is the size of the market at each frequency, in terms of volume production. According to chipset manufacturers (on which the equipment suppliers depend), the 450 MHz band will be a fairly large market, led by rollouts in Brazil, Bangladesh and Finland. The 700 MHz market will also be economically viable globally and could well exceed the 450 MHz market in volume.

The capability of handsets to be multi-mode in several different frequency bands will depend on the antenna design and size as software-defined RF front ends are flexible, while MIMO provides superior throughput and signal strength. The aggregation of different frequency bands into “virtual channels” to supply greater bandwidth and thus faster data transfers is also possible with LTE.

Five scenarios were examined and commercial mobile LTE is the lowest cost *broadband* solution

Having understood the technical and spectrum possibilities, the study built five scenarios based on different types of deployments:

1. Dedicated networks and dedicated specialised equipment
2. Commercial MNO networks and commercial equipment
3. Dedicated networks with commercial networking equipment
4. Hybrid networks
5. A common multi-purpose network, perhaps regional in scale

Costs were the basis for comparing these options. The basic tenet of this comparison was the use of mobile broadband to add capabilities and thus increase the value of the network to its users and to society in general.

The first scenario looks at continuing with current dedicated networks and dedicated equipment – essentially the costs and benefits of continuing with TETRA/TETRAPOL. It shows that although the costs are high, they can be less than other options – but not when the value of the capabilities and benefits are factored in.

This is highlighted in scenario 3, a further configuration of a dedicated network, but with commercial LTE equipment, hardened. As we do not yet know the outcome of European discussions about possible re-allocations of frequencies, our modelling was calibrated to 800 MHz as a commercial band for LTE, with cost comparisons for lower and higher frequencies. As lower UHF bands might become available eventually, sensitivity analysis compared costs for the major cost driver, the number of base stations needed at various frequencies.

Scenario 2 is perhaps the key option, as it focuses on the use of commercial networks. A crucial cost is that of hardening for resilience, for both the radio access network (RAN) and the core network. (We assumed that government would pay for hardening but of course this is open to debate.) However, the main issue arising from this scenario is not the technology challenge of building a resilient network, but the regulatory, legal and contractual context. From the case study in Chapter 5 on the UK government's orchestration of a new PPDR network to replace the existing Airwave TETRA network, using commercial MNOs, a pragmatic contractual structure was defined, for use with scenarios 2 and 4. This was applied as a set of four contracts between a central government and commercial suppliers to fulfil four basic roles:

1. *Programme manager* – responsible for managing network services long term and the fulfilment of the other three contracts (termed the "Delivery Partner" by the UK government).

2. *Systems and network integrator* – may handle sales of handsets, apps and other equipment to the end user services (a role which can be separated from systems integration).

3. *Multiple MNOs offering mobile services at wholesale rates over hardened networks*. Interestingly, MNOs seem to see the mission critical market as a new revenue stream with a bright future, especially if government pays to harden the networks to meet PPDR standards. It is assumed that the government could buy capacity at wholesale rates for its PPDR services at much lower prices than individual subscribers. Also the bidding framework requires tenders from multiple MNOs, introducing competition into the price offers.

4. *Extension services for extra coverage* – since most commercial MNOs typically achieve 90% coverage while the PPDR community seeks 99% coverage including tunnels, underground garages and other enclosed public spaces.

Such contracts include clauses on everything from government step-in upon failure, SLAs on minimum availability, contract transfer limits, limits on *force majeure* claims, and so on. But more is needed to reassure the mission critical services, as we explore below.

Naturally this framework could be applied in the way favoured by the UK government, through direct contracts between the tenderers and the ministry of the interior (Home Office). Another approach may be more effective in the long term, with an MVNO as programme manager or above the programme manager. The Belgian network ASTRID is a case in point, with their Blue Light Mobile MVNO illustrating how such an approach could work (see Chapter 5).

In analysing the costs, the study found commercial LTE operation was the cheapest in simple financial terms (see Chapter 4). But other factors must be taken into account to assess the real value of any option, including network reliability as well as the degree of support for all three sectors, especially for M2M data.

In that vein, although the hybrid network in scenario 4 is much more expensive than the other options because of its complex architecture (given the implementation put forward here), it would unite utility and ITS networks better than either a purely commercial or dedicated network. It also offers greater flexibility for integrating existing networks and enabling a gradual migration.

More is needed than a good contract to attract and reassure users

However, in addition to contractual structures specific regulatory measures may be needed to reassure the three sectors (particularly those with regulatory obligations on continuity of service, such as the utilities) and ensure that MNO performance levels are maintained over decades. These measures are necessary to gain the trust of the user communities that MNO commercial behaviour will never disrupt mission critical services. Measures in specific areas are needed to build the confidence of these users in the MNOs:

1. Being prepared to upgrade to high standards of reliability and correct service failures as quickly as possible, without any degradation in that commitment over several decades

2. Acceptance of long-term (15 to 30 year) contract commitments to mission critical customers, with stable conditions and agreed rates

3. Providing priority access to mission critical services, especially when emergencies create a risk of network overload

4 Providing geographic coverage to meet the needs of mission critical users

5. Willingness to cooperate with other MNOs and MVNOs – for instance, in handing over a mission critical call to another operator with a better local signal

6. Keeping to the spirit and letter of long-term contracts for mission critical services without arbitrary changes in technical features, tariffs or service conditions

7. Readiness to submit cost-based pricing analyses of tariffs with full open book accounting for NRAs and government clients

8. Willingness to offer new charging regimes and metering procedures

9. Removal of excessive charges for international roaming across the EU and avoidance of "surprise charges" for previously agreed services.

Such measures are needed in light of the fact that today's MNOs have become the incumbents, much like their fixed line predecessors. They have evolved from being small upstarts and challengers of the status quo to being the dominant forces in the telecommunications market, with at least five times as many subscribers as fixed line carriers ever achieved. Mission critical mobile broadband will further extend their dominance.

In response, as emphasised in Chapter 6, it is essential to consider new measures that give national regulatory authorities (NRAs) specific new powers to cope with this situation on behalf of mission critical services:

1. MNOs should be mandated to support mission critical services. There seem to be two possible ways to do this:

- To operate as an MNO or an MVNO, licensees must agree to provide mission critical services. That may entail extended geographic coverage, hardening to meet minimum standards of availability and resilience, and designating an overall programme manager for mission critical services. It is effectively an additional set of licence conditions to operate a public mobile service.

- An alternative is that any purchase or exercise of a mobile spectrum licence brings with it the obligation to support mission critical services for as long as the licence is valid. Note that the grant of spectrum conditioned on mission critical provisions offers NRAs the power to re-assign the spectrum to a new operator, if the original one fails to perform. This mechanism gives effective control to the NRA through the potential for spectrum re-assignment, such that the spectrum is not ‘lost’.

The first alternative would begin with new licences; the second would begin with the transfer of an existing license. This is not a *universal* service obligation but a *specific* service obligation that extends MNO/MVNO responsibilities for the long term. On the positive side, it is a rare obligation that brings with it a new revenue stream, accompanied by government investment in resilience that will benefit all users of the network.

2. NRAs should have the power to introduce regulations that support and enforce the provisions of long-term MNO contracts with mission critical users.

3. NRAs should be authorised to grant priority access to commercial mobile network services for mission critical communications when justified by circumstances, including the handover of calls between MNOs when required. This may require amendment of existing guidelines, statutes or regulations.

4. NRAs should support governments in setting tariffs for mission critical services by research into true costs of MNO operation and through comparative cost studies with other NRAs and sources from outside the Member State. That may require forensic accounting and suitable preparations of the cost base declarations by MNOs.

Thus a key conclusion of this study is that commercial mobile networks could be suitable for mission critical communications within the right legal, regulatory and contractual framework. This conclusion allows each Member State to decide whether to employ MNOs for mission critical communications. No recommendation is made here to impose a common policy mandate (for example, through an EU Directive). However, Commission guidelines for Member States on NRA roles, actions, powers and responsibilities *vis-à-vis* MNO contracts with mission critical users might be desirable.

Should additional spectrum bands be reserved for mission critical services?

Since many Member State governments have statutory obligations for the provision of national mission critical communications (especially for PPDR), as well as political and cultural traditions effectively ensuring that government-owned-and-operated networks are the only viable option, dedicated spectrum will be required for them. Therefore, on the key question of whether there should be exclusive dedicated spectrum across the EU for mission critical services, a pragmatic direction is favoured. This is based on the subsidiarity principle: each Member State should choose its own direction. For those choosing to build dedicated mission critical networks, dedicated spectrum will be necessary – which is an additional financial burden, if the opportunity costs are recognised. These are not just the loss of auction revenues, i.e. the market value of the spectrum, but the loss of broadband’s economic stimulus effect on the general economy although it may be argued that the socio-economic benefit that same spectrum could give for mission critical functions might tend to compensate.

Economic circumstances may force a rethink of the affordability of a dedicated network over the next few years in some Member States. The costs might prove too much of a burden just when the LTE standards releases with mission critical functionality are transformed into new equipment and prices are reduced as the ramp-up of production volumes kick in. Should a Member State then decide to migrate from a dedicated closed to a shared commercial network, previously dedicated spectrum might be refarmed to commercial networks, either with mission critical users as the only clients, or as priority users with others sharing the network.

But which frequency band should be chosen? Overall, the debate turns on the frequency range as that sets the physical characteristics that determine cost and performance. That is at the heart of the clash between Europe’s television and cellular industries, highlighted in the recent report by the Lamy High Level Group, which failed to reach consensus on the future of the UHF spectrum below 790 MHz in the short term.

Our conclusion is that because of various stakeholder interests, especially those of existing military and PMR users, the main band used today for TETRA (380-400 MHz) is unlikely to be available across the EU, particularly not for conversion to LTE. The next band up, 450 MHz, is a more promising choice for dedicated use with nearly half of the Member States being prepared to consider it. Moving further up the spectrum, the surprise proposal at WRC-12 for ITU Region 1 to allow mobile use of 694-790 MHz is provoking much discussion across the EU, as the Lamy report shows. Although the report suggested a timetable for releasing the 700 MHz band to mobile, this would not be until some time between 2018 and 2022. That would coincide with more mature generations of LTE, in Releases 12-14, with most of the mission critical features needed by PPDR.

Whether a harmonised exclusive allocation is necessary and desirable, with commercial offerings alongside, is a key question. Our conclusion is that the diversity of views among the Member States makes a dedicated mission critical allocation at 700 MHz logical only in the short term, as a subsequent migration to commercially based services is likely to occur progressively over the next decade because of increasing economic pressure on government budgets.

Résumé analytique

La présente étude a pour objectif d'évaluer les options d'utilisation de la large bande mobile dans le cadre des communications critiques dans trois secteurs particuliers (la protection civile et les secours en cas de catastrophe (PCSC), principalement la police, les pompiers et les services médicaux d'urgence), les services publics (l'électricité, le gaz et l'eau) et les systèmes de transport intelligents (STI) mis en service à l'heure actuelle, avec un accent particulier sur les transports routier et ferroviaire). Les deux principales options envisagées sont d'une part les réseaux mobiles terrestres publics (PLMN, en anglais), gérés par des opérateurs commerciaux, et d'autre part les réseaux dédiés créés spécifiquement à l'attention de ces secteurs.

La société européenne dépend des services critiques

La sécurité publique, la garantie de disposer de services publics qui fonctionnent et la fiabilité des systèmes de transport sont essentielles pour la société européenne moderne. Ces services ne pourraient pas fonctionner sans les réseaux radio et doivent recourir, de plus en plus fréquemment, à la large bande sans fil à longue portée. La présente étude examine le passé, le présent et l'avenir des communications mobiles dans le cadre des services critiques, dans trois secteurs particuliers. Traditionnellement, chacun des secteurs étudiés disposait de ses propres réseaux dédiés, souvent avec l'attribution de fréquences exclusives.

Pour ne citer qu'un exemple, dans les États membres de l'UE, les services PCSC ont bénéficié d'investissements en capital (CAPEX) importants, à hauteur d'au moins 19 milliards d'euros (le montant total pourrait être plus élevé, dans la mesure où la transparence et l'exhaustivité des comptes publics varient). La plupart des investissements ont été alloués aux technologies TETRA et TETRAPOL, dont le potentiel limité pour assurer de nouveaux services de données est limité, bien que les canaux vocaux puissent encore être utiles au cours de la prochaine décennie ou au-delà et serviront ainsi de base à certains réseaux PCSC, tant qu'une technologie de substitution ne sera pas disponible. En outre, les fournisseurs de technologies critiques sont spécialisés et peu nombreux, et leurs marchés présentent un potentiel limité, tant en Europe qu'au niveau mondial. Dans ces conditions, il n'est pas possible de faire des économies d'échelle sur la production de masse d'équipements, et le faible nombre de fournisseurs restreint la concurrence. Par ailleurs, alors que la coopération internationale entre les services PCSC et d'autres services essentiels se renforce, l'interopérabilité entre les mises en œuvre des technologies TETRA et TETRAPOL des différents fabricants s'est avérée difficile. Dans les faits, les utilisateurs de PCSC sont prisonniers de mises en œuvre particulières de règles qui entravent la coopération entre les frontières, les juridictions et les secteurs.

Les réseaux ferroviaires européens déploient, à l'heure actuelle, un service à 900 MHz fondé sur leurs propres réseaux de communications privés, et ont recours pour cela à une variante du GSM, laquelle pourrait finir par coûter plus de 25 milliards d'euros (selon nos estimations). Le GSM demeure la technologie cellulaire la plus prise en charge, et elle se prête bien aux besoins du secteur ferroviaire. Néanmoins, à l'instar des technologies TETRA et TETRAPOL, elle dispose d'un nombre limité de sources d'équipements critiques, spécialement conçus pour un usage ferroviaire, et son avenir est très incertain, dans la mesure où l'industrie cellulaire souhaite remplacer progressivement la technologie GSM par la 3G et la 4G. Dans ces conditions, il y a lieu de s'interroger sur l'avenir de la prise en charge des nouveaux réseaux sans fil ferroviaires.

En attendant, les applications critiques se développent à toute vitesse. Les réseaux intelligents pour les services publics, la vidéo pour la gestion du trafic routier et l'imagerie médicale pour les équipes ambulancières nécessitent des canaux à large bande accessibles sur de vastes régions géographiques. La large bande devient de plus en plus importante pour sauver des vies, garder l'éclairage public en bon état de marche et maintenir l'ordre public.

Dans ce contexte, la dépendance par rapport aux technologies numériques prend de l'ampleur et les services critiques européens connaissent une évolution majeure. Par ailleurs, le concept de communications « critiques » se propage des services PCSC à d'autres secteurs, au fur et à mesure que l'interconnexion de l'économie européenne et sa dépendance à l'égard de capacités riches en information augmente. Par conséquent, la définition du terme « critique » n' englobe plus uniquement les fonctions clés de protection de de la vie humaine, mais comprend désormais le maintien du bon fonctionnement de la macro-économie (les définitions pratiques pour l'avenir sont examinées dans la section 2.4. ci-dessous).

Des réseaux mobiles à large bande font leur apparition, la situation se complique

Dans ce contexte, il est heureux que les opérateurs de réseaux mobiles (ORM) européens déploient, à l'heure actuelle, une large bande à haute vitesse. Néanmoins, les secteurs critiques ont des motifs raisonnables de s'inquiéter du fait de compter exclusivement sur les services mobiles commerciaux, et formulent, à ce propos, deux principales réserves, à savoir :

- Peut-on compter sur les opérateurs commerciaux pour fournir des services fiables dans le cadre de contrats prévoyant des prix forfaitaires sur la longue durée ?

- Seront-ils en mesure d'assurer le niveau de disponibilité du réseau, de résistance, de qualité du service, de sécurité et de couverture nécessaire, notamment en cas d'urgence ?

Chacun des trois secteurs examinés dans le cadre de la présente étude est étroitement lié aux gouvernements et au secteur public dans son ensemble. Les services d'urgence attendent des subventions publiques pour les ressources prioritaires, comme des fréquences gratuites et des droits de passage. Néanmoins, l'ensemble des États membres de l'UE se voit confronté à des restrictions budgétaires, en raison de la crise financière de 2008 et de l'augmentation des dettes à long terme. Les coupes budgétaires sur les services publics devraient perdurer pendant au moins les dix années à venir, ce qui donne lieu à la contradiction suivante : les services publics doivent freiner leurs dépenses alors que les citoyens attendent toujours davantage d'eux.

Les réseaux mobiles commerciaux sont-ils une solution viable pour les secteurs critiques ?

Dans un contexte d'austérité, la question suivante se pose de plus en plus : les réseaux mobiles commerciaux peuvent-ils prendre en charge de manière satisfaisante les communications des secteurs critiques, aussi bien en ce qui concerne la large bande que la voix ? Les avantages économiques liés à l'utilisation d'une base technologique à large bande, d'infrastructures et de bandes de fréquences identiques pour les utilisateurs critiques et le marché de masse semblent clairs. Reste à savoir si les économies réalisées s'accompagneraient d'une résistance et d'une performance suffisante.

En réponse à la pression dont les budgets publics font l'objet, et face à l'introduction d'une nouvelle génération, plus efficace, de technologies mobiles large bande, la Commission européenne a sollicité la réalisation d'une étude approfondie indépendante concernant le coût et les bénéfices de l'utilisation de réseaux commerciaux dans les secteurs critiques. C’est dans ce contexte que SCF Associates Ltd. a été chargée d’explorer les besoins de communication et les options concernant trois secteurs, à savoir les services PCSC, les services publics et les STI, dans le cadre de l’examen approfondi de cinq scénarios.

Il convient de souligner que la présente étude a pour objet d’examiner l’introduction de la *large bande* mobile dans le cadre des services critiques, par le biais des réseaux commerciaux ORM. En outre, l’étude doit s’intéresser aux besoins de *l’ensemble des trois secteurs* (services publics, STI (routiers et ferroviaires) et PCSC) considérés.

Ces cinq scénarios explorent les options, sur la base des coûts, parmi les réseaux dédiés, les réseaux commerciaux des ORM et les nouveaux équipements LTE aptes pour une utilisation dans le cadre d’un réseau dédié. Notre conclusion est la suivante : en général, les dépenses d’investissement de capital (CAPEX) par utilisateur pour les réseaux commerciaux LTE renforcés et fournissant une couverture géographique allant jusqu’à 99 % des territoires nationaux seraient inférieures à celles des réseaux LTE dédiés. Il s’agit là, également, de l’option la plus attractive en termes de rapport qualité-prix, en cas d’association des CAPEX et des OPEX (dépenses d’exploitation), bien que les avantages financiers varient en fonction des bandes de fréquence utilisées. À 450 MHz, le coût par utilisateur d’un réseau dédié inférieur de plus de 40 %, en termes de CAPEX, par rapport à un réseau mobile commercial à large bande fonctionnant à 800 MHz. Néanmoins, si l’on prend en considération 10 années d’OPEX, le partage des frais d’infrastructures favorise les réseaux commerciaux, que ceux-ci fonctionnent à 450, 700 ou 800 MHz. Un réseau commercial LTE fonctionnant à 800 MHz peut générer un coût en termes de CAPEX par utilisateur inférieur d’environ 40 % à celui découlant d’un réseau LTE dédié fonctionnant à 700 MHz (si les ORM décident d’exploiter des réseaux commerciaux dans des secteurs critiques avec une bande à 700 MHz, les coûts en termes de CAPEX pourraient être jusqu’à 20 % inférieurs à ceux afférents à un réseau semblable fonctionnant à 800 MHz.)

Mais le coût n’est pas le seul facteur à prendre en compte. Notre conclusion générale est que l’utilisation des réseaux mobiles commerciaux à large bande pourrait être possible à des fins de services critiques, mais uniquement ***si cinq conditions sont remplies***.

Les cinq conditions (qui doivent être toutes entièrement remplies) sont les suivantes :

1. Premièrement, l’intervention des ORM commerciaux doit se limiter à fournir les services dont les utilisateurs des services critiques ont besoin, tout en évitant de recourir à des techniques de blocage pour profiter de manière déloyale de cette expansion du pouvoir de marché et de la responsabilité sociale des ORM. Ces changements consistent non seulement à prendre des engagements plus forts en termes de résistance des réseaux, mais aussi à accepter des limitations aux hausses des prix et aux révisions des conditions contractuelles, ainsi qu’à assurer la continuité de l’autonomie et à mettre l’accent sur la qualité du service concernant le trafic afférent aux services critiques. La *perception* du comportement et des performances des ORM par les services critiques sera aussi importante pour des relations à long terme. Pour cela, des mesures seront nécessaires, au-delà des contrats de niveau de service (SLA, ou service level agreements, en anglais) au niveau du contrat commercial : de nouvelles règlementations concernant les services commerciaux ORM doivent être appliquées par les agences nationales de réglementation (ANR) de chaque État membre de l’UE ;

2. Les réseaux commerciaux doivent être « renforcés », du réseau d’accès radio au réseau central, et adaptés afin de fournir une disponibilité supérieure à 99 % (avec un objectif de « cinq neuf »). La couverture géographique doit, elle aussi, être étendue en fonction des besoins des

services critiques considérés, et la pénétration des signaux reçus dans les bâtiments améliorée dans certains emplacements ;

3. Le renforcement du réseau et l'extension de la couverture surveillée, ainsi que l'ajout de fonctions essentielles relatives aux services critiques et d'une résilience accrue, doivent se faire à un prix raisonnable. Il faut éviter de dépenser davantage sur l'expansion sélective et le renforcement des réseaux commerciaux en vue d'une utilisation dans le cadre de services critiques que les sommes qui auraient été consacrées à la mise en place d'un réseau national LTE dédié, à des fins identiques ;
4. Les réseaux LTE renforcés doivent être en mesure de fournir les différents types de services dont les trois secteurs considérés ont besoin. Chaque secteur utilise la large bande de différente façon. C'est le cas non seulement des flux vidéodes les services d'image et de l'accès à des bases de données (telles que celles PCSC), mais également de la télémétrie à très faible latence et du contrôle en temps réel pour les services publics et les transports. Dans les cinq options de réseaux étudiées dans le chapitre 4 de la présente étude, il devient plus facile de répondre aux besoins des différents secteurs lorsque l'on passe des réseaux dédiés existants aux réseaux LTE, puis à des configurations hybrides plus complexes ;
5. Il existe toutefois un autre obstacle de taille, qui consiste à déterminer si les réseaux mobiles commerciaux seront en mesure de dépasser la préférence de longue date des États membres pour des réseaux contrôlés par l'État pour les applications qui concernent la sécurité publique. Il ne s'agit pas là simplement d'une question juridique, réglementaire ou économique. Certains États membres de l'Union européenne ont un passé de contrôle étatique profondément ancré dans leurs cultures, traditions et politiques, sans parler des investissements sur des technologies actuelles aux durées d'amortissement longues. Dans ces conditions, certains États membres pourraient souhaiter continuer d'utiliser des réseaux dédiés à court et moyen termes, même si ceux-ci s'avèrent plus onéreux (cela pourrait être le cas, par exemple, de l'Allemagne, de l'Italie et de la France, en ce qui concerne les services PCSC). Toutefois, rien ne dit que ces pays ignoreront toujours les alternatives plus économiques. Les ORM devront peut-être se montrer plus persuasifs à l'heure de mettre en avant leurs avantages. En attendant, ce sera aux États membres de faire leur choix.

Les obstacles à un usage commercial évoqués ci-dessus ne peuvent pas être supprimés dans l'immédiat. Néanmoins, sur le moyen et le long termes, le partage des infrastructures commerciales des ORM à des fins publiques et critiques serait justifié sur le plan économique. Le principal obstacle est constitué par le modèle commercial de marché de masse actuel des ORM, lequel devrait être dûment modifié pour fournir des services de qualité appropriés aux clients prioritaires présentant des besoins particuliers. Toutefois, il faudra un certain temps pour que les *perceptions* des ORM changent. Ainsi, dans la mesure où les réseaux des services critiques relèvent de la responsabilité des administrations nationales, il semble probable que les réseaux étatiques dédiés continuent de constituer le modèle de choix à court terme. Néanmoins, ne serait-ce que pour des raisons budgétaires, chaque État membre de l'UE devrait envisager de passer des réseaux fermés dédiés aux réseaux commerciaux partagés, une fois que les cinq conditions listées ci-dessus auront été remplies.

Quelles mesures sont nécessaires pour remplir ces conditions ?

Dans le cadre des scénarios de budgétisation évoqués au chapitre 4 de cette étude, en ce qui concerne les réseaux commerciaux, dédiés, partagés et hybrides, il semble que les exigences budgétaires peuvent être satisfaites de plusieurs manières. Par ailleurs, notre enquête sur la technologie LTE, évoquée au chapitre 3 de la présente étude, met en évidence que les capacités peuvent être renforcées jusqu'à un niveau adapté aux services critiques si les organismes de normalisation fournissent ce qu'ils promettent, en temps et en heure.

Aux fins de la réalisation de la présente étude, nous avons examiné en profondeur les exigences qui façonnent les besoins en communications sans fil des trois secteurs considérés (voir chapitre 2 et les annexes, lesquelles font partie intégrante de ce rapport). Les exigences de la communauté PCSC sont bien énoncées par des organismes tels que le groupe de travail Law Enforcement Working Party (LEWP) et l'association TETRA and Critical Communications Association (TCCA). Néanmoins, les perspectives policières tendent à dominer ces exigences. Les pompiers, le personnel médical d'urgence et les organismes de secours en cas de catastrophe ont des besoins quelque peu différents, qu'il conviendrait de prendre en considération également. Aussi, dans le cadre des présentes, nous accorderons davantage d'attention à leurs exigences que cela est souvent le cas (voir annexe A).

S'agissant des services publics, les associations du secteur, dont l'EUTC (European Utilities Telecommunications Council) et Eurelectric, ainsi que celles afférentes à des services publics particuliers (Iberdrola, Alliander et autres) nous ont fourni des renseignements détaillés. L'Agence ferroviaire européenne (European Railway Agency (ERA) a mis à notre disposition des informations essentielles, et une étude complémentaire a mis en évidence les nouvelles exigences des transports routiers. Dans les trois secteurs considérés, nous avons identifié diverses exigences, à savoir :

- Les utilisateurs PCSC souhaitent utiliser la large bande mobile de façon bien plus intensive à l'avenir, bien que chaque sous-secteur ait des projets différents : la vidéo et des images à haute résolution revêtent une importance croissante dans le domaine de l'application de la loi, alors que les capteurs en temps réel (dont les caméras infra-rouges et les détecteurs de mouvement traversant les murs) sont de plus en plus prisés par les pompiers. Les services d'urgences médicales ont besoin d'images à haute résolution, dans le cadre de la télémédecine, afin d'être en mesure d'effectuer des appréciations et des diagnostics corrects sur site, alors que les équipes de recherche et de sauvetage estiment que les drones équipés de caméras vidéo permettent à des effectifs réduits d'examiner des zones étendues de manière efficace ;

- Les services publics sont moins intéressés par la large bande que par la collecte, sur des grandes surfaces, de paquets de données fiables de machine à machine (M2M), à partir de millions de mètres et postes de réseaux. À l'heure actuelle, les intrants variables en provenance des cellules solaires et des turbines éoliennes sont en passe de modifier l'architecture de la production d'énergie, et posent de nouveaux défis en termes de régulation du voltage et de stabilité des réseaux. Les réseaux intelligents ajouteront des exigences pour ce qui est de la communication bidirectionnelle, ainsi que de nouveaux services allant au-delà de la distribution des ressources. De nombreux services publics insistent sur le contrôle direct des réseaux de communications, dans la mesure où ils sont légalement tenus de fournir des services fiables. Ils ne peuvent pas transférer la responsabilité à leurs fournisseurs, raison pour laquelle ils sont réticents à l'idée de dépendre de tiers, tels que les ORM, pour la fourniture d'un contrôle opérationnel en temps réel ;

- La communication de données en bande étroite par liaison commutée par circuits (voix) constitue la nouvelle norme de contrôle ferroviaire en Europe. Cependant, dans la sphère du sans-fil non-opérationnel/non afférent à des services critiques, l'accès des passagers à Internet par le wifi pourrait s'avérer essentiel pour atteindre l'objectif d'augmentation du nombre d'usagers des lignes ferroviaires souhaité par la Commission européenne, en vue de réaliser les objectifs de réduction des émissions de gaz à effet de serre. Les demandes en matière de bande passante en provenance des véhicules routiers sont plus diverses et plus difficiles à prévoir. Elles vont des communications de véhicule à véhicule à 5,9 GHz au signalement d’accidents par le système « eCall » par téléphonie cellulaire, en passant par le placement de caméras le long des routes en vue de la lecture des numéros de plaque d’immatriculation des véhicules, pour faire respecter les limitations de vitesse et collecter les droits de péage.

Les principaux défis auxquels la présente étude a dû faire face ont été les suivants : identifier les différentes exigences selon les secteurs, pour déterminer ensuite si le partage des réseaux demeurait toujours faisable, et budgétiser les différentes façons de répondre auxdites exigences.

Du point de vue de l’offre, les capacités actuelles et prévisibles des réseaux mobiles commerciaux sont examinées dans le chapitre 3. Ces capacités peuvent être renforcées essentiellement dans le cadre du partenariat ETSI/3GPP pour le développement de normes LTE. Cette étude s’est intéressée au processus d’ajout de capacités en termes de services critiques à la technologie LTE, notamment en ce qui concerne ses versions 12, 13 et 14, afin de connaître le calendrier probable pour la mise à disposition d’équipements présentant des fonctionnalités telles que Direct Mode Operation (Mode direct), Push-To-Talk (Appuyer pour parler) et l’appel prioritaire. Nous nous sommes également penchés sur les modèles de déploiement des équipements LTE parmi les ORM des différents États membres de l’UE, dans la mesure où la disponibilité de nouveaux équipements n’oblige pas forcément à remplacer les anciens. Selon la feuille de route actuelle pour la technologie LTE, quasiment aucune des fonctionnalités pour les services critiques ne sera disponible avant 2016, certaines d’entre elles pourraient ne l’être, à certains endroits, qu’en 2018, et bien plus en 2020. Ainsi, avant 2020, la technologie LTE disponible pour les réseaux critiques pourrait ne pas être entièrement normalisée.

L’autre exigence majeure pour l’introduction de nouveaux réseaux à large bande pour les services critiques concerne la disponibilité de fréquences UHF. Pour des équipements rentables, un paramètre essentiel est la taille du marché pour chaque fréquence, en termes de volume de production. Selon les fabricants de puces (dont les fournisseurs d’équipements dépendent) la bande à 450 MHz constituera un marché assez grand, porté par des déploiements au Brésil, au Bangladesh et en Finlande. Le marché des 700 MHz sera, lui aussi, économiquement viable au niveau mondial, et pourrait dépasser celui des 450 MHz en volume.

Les capacités multimodes des téléphones pour plusieurs bandes de fréquence différentes dépendront de la conception de l’antenne et de la taille, dans la mesure où les appareils frontaux RF réalisés par logiciel sont flexibles, alors que les techniques MIMO fournissent un débit et une intensité des signaux supérieurs L’agrégation de différentes bandes de fréquence dans des « canaux virtuels », afin de fournir une largeur de bande plus importante et d’accélérer ainsi les transferts de données, s’avère également possible avec la technologie LTE.

L’examen de cinq scénarios a déterminé que la technologie mobile commerciale LTE constitue la solution *à large bande* la moins onéreuse

Compte tenu des possibilités techniques et en termes de fréquences, notre étude a défini cinq scénarios fondés sur différents types de déploiements, à savoir :

1. Les réseaux dédiés et les équipements spécialisés dédiés ;
2. Les réseaux commerciaux des ORM et les équipements commerciaux ;
3. Les réseaux dédiés avec des matériels de réseau commerciaux ;
4. Les réseaux hybrides ;
5. Un réseau commun polyvalent, peut-être de dimension régionale.

Le coût a été la base de comparaison de ces différentes options. Le principe de base de cette comparaison était l'utilisation de la large bande mobile en vue d'ajouter des capacités et d'augmenter ainsi la valeur du réseau pour ses utilisateurs et la société en général.

Le premier scénario porte sur la continuité dans les réseaux et les équipements dédiés actuels (essentiellement, les coûts et les avantages de poursuivre avec TETRA/TETRAPOL). Il souligne que même si les coûts sont élevés, ils pourraient être inférieurs à ceux découlant d'autres options (mais il n'en est pas ainsi lorsque la valeur des capacités et des avantages est prise en considération).

Cela est souligné dans le cadre du scénario 3, une nouvelle configuration d'un réseau dédié, mais avec des équipements LTE commerciaux renforcés. Dans la mesure où nous ne connaissons pas encore les résultats des débats européens concernant les réallocations éventuelles des fréquences, notre modélisation a été calibrée à 800 MHz, en tant que bande commerciale pour la technologie LTE, avec des comparaisons des coûts pour les fréquences plus basses et plus hautes. Les bandes plus basses UHF pouvant, au final, être disponibles, une analyse de sensibilité a comparé les coûts pour la principale source des coûts, à savoir le nombre de terminaux de base nécessaires à plusieurs fréquences.

Le scénario 2 constitue, peut-être, l'option clé, dans la mesure où il se concentre sur l'utilisation de réseaux commerciaux. Un coût essentiel est celui lié au renforcement à des fins de résistance, tant pour le réseau d'accès radio que pour le réseau central (nous sommes partis du principe que les gouvernements prendraient à leur charge les frais de renforcement, mais, évidemment, le débat sur la question reste ouvert). Néanmoins, le principal problème de ce scénario n'est pas le défi technologique constitué par la mise en place d'un réseau résistant, mais le contexte règlementaire, juridique et contractuel. À partir de l'étude de cas du chapitre 5 concernant l'orchestration, par le gouvernement britannique, d'un nouveau réseau PCSC devant remplacer le réseau Airwave TETRA déjà en place, à l'aide des ORM commerciaux, une structure contractuelle pragmatique a été définie afin de l'utiliser dans le cadre des scénarios 2 et 4. Cette structure a été appliquée à un ensemble de quatre contrats liant le gouvernement central et des fournisseurs commerciaux, afin de remplir quatre rôles fondamentaux, à savoir :

1. *Directeur de programme* – chargé de la gestion des services de réseau sur le long terme, ainsi que de l'exécution des trois autres contrats (désigné en tant que « Partenaire chargé de l'exécution » (Delivery Partner) par le gouvernement britannique) ;

2. *Intégrateur de systèmes et de réseau* – peut gérer les ventes de téléphones mobiles, d'applications et d'autres équipements aux utilisateurs finaux (un rôle susceptible d'être distinct de celui afférent à l'intégration de systèmes) ;

3. *ORM multiples proposant des services mobiles à des tarifs de gros sur des réseaux renforcés*. Fait intéressant, les ORM semblent considérer le marché des services critiques comme une nouvelle source de revenus, avec un avenir prometteur, notamment si le gouvernement prend à sa charge le renforcement des réseaux afin de se conformer aux normes PCSC. L'hypothèse de départ est que le gouvernement pourrait acheter à des tarifs de gros les services PCSC, à des prix bien plus bas que les souscripteurs individuels. De même, le cadre des marchés exige des offres en provenance d'ORM multiples, introduisant la concurrence dans les offres de prix ;

4. *Services d'extension pour une couverture additionnelle* – dans la mesure où la plupart des ORM offrent, en général, une couverture de 90 %, alors que la communauté PCSC souhaite

une couverture de 99 %, incluant les tunnels, les parkings souterrains et d'autres espaces publics fermés.

Ces contrats prévoient des clauses concernant l'ensemble des questions envisageables, de l'intervention du gouvernement en cas de défaillance aux SLA relatifs à un taux de disponibilité minimum, en passant par les limites concernant les cessions de contrat, les réclamations en cas de force majeure, etc. Il en faut néanmoins plus pour rassurer les services critiques, ainsi que cela sera évoqué ci-dessous.

Naturellement, ce cadre pourrait s'appliquer, selon les modalités retenues par le gouvernement britannique, au moyen de contrats directs liant les soumissionnaires et le Ministère de l'intérieur (Home Office). Une autre approche pourrait s'avérer plus efficace sur le long terme, avec un opérateur de réseau mobile virtuel (MVNO) désigné responsable du programme, ou placé au-dessus de ce dernier. Le réseau belge ASTRID en est un exemple, avec son MVNO Blue Light Mobile, qui illustre la manière dont une telle approche pourrait fonctionner (voir chapitre 5).

Dans le cadre de l'analyse des coûts, l'étude a conclu que l'exploitation commerciale LTE était la moins onéreuse en termes purement financiers (voir chapitre 4). Cependant, d'autres facteurs doivent être pris en considération pour évaluer la valeur réelle de toute option, et notamment la fiabilité du réseau et le degré de prise en charge pour chacun des trois secteurs considérés, en particulier en ce qui concerne les données M2M.

Dans le même esprit et bien que le réseau hybride du scénario 4 soit bien plus cher que les autres options en raison de son architecture complexe (au vu de la mise en œuvre dont il est ici question), il n'en demeure pas moins qu'il unifierait les réseaux des services publics et des STI mieux qu'un réseau purement commercial ou qu'un réseau dédié. De même, il offrirait davantage de flexibilité pour intégrer les réseaux existants et permettre une migration graduelle.

Il faut plus qu'un bon contrat pour attirer et rassurer les utilisateurs

Néanmoins, outre les structures contractuelles, des mesures règlementaires particulières pourraient s'avérer nécessaires pour rassurer les trois secteurs considérés (et notamment ceux tenus par des obligations réglementaires de continuité du service, comme les services publics) et garantir que les niveaux de performance des ORM se maintiennent au fil des décennies. Ces mesures sont requises pour convaincre les communautés d'utilisateurs que le comportement des ORM commerciaux ne perturbera jamais le fonctionnement des services critiques. De même, des mesures particulières sont nécessaires pour que ces utilisateurs aient confiance dans les ORM, à savoir :

1. Etre prêt à effectuer des mises à jour afin de se conformer à des normes élevées de fiabilité, ainsi qu'à corriger les défaillances du service dans les meilleurs délais, sans aucun affaiblissement de cet engagement au fil des décennies ;

2. Mettre en place des engagements contractuels sur le long terme (de 15 à 30 ans) avec les clients des services critiques, qui prévoient des conditions stables et des tarifs fixes consensuels ;

3. Fournir un accès prioritaire aux services critiques, notamment si les urgences entraînent un risque de surcharge du réseau ;

4. Mettre à disposition une couverture géographique répondant aux besoins des utilisateurs de services critiques ;

5. Etre prêt à coopérer avec d'autres ORM et MVNO (en transférant, par exemple, un appel à un service critique à un autre opérateur proposant un meilleur signal au niveau local) ;

6. Respecter à la lettre les contrats à long terme pour les services critiques, en évitant tout changement arbitraire des caractéristiques techniques, des tarifs ou des conditions de service ;

7. Etre prêt à présenter des analyses des prix fondées sur les coûts concernant les tarifs, avec une comptabilité transparente ouverte aux agences nationales de réglementation (ANR) et aux clients gouvernementaux ;

8. Etre prêt à proposer de nouveaux régimes de facturation et de nouvelles procédures de comptage ;

9. Supprimer les charges excessives pour l'itinérance internationale au sein de l'UE, et éviter les « changements surprises » des services convenus auparavant.

Ces mesures sont nécessaires du fait qu'à l'heure actuelle, les ORM sont devenus les opérateurs en place, comme leurs prédécesseurs de la téléphonie fixe. Ils sont passés du statut de jeunes entreprises et de challengers du *status quo* à celui de forces dominantes sur le marché des télécommunications, avec au moins cinq fois plus d'abonnés que ceux détenus par le passé par les opérateurs de téléphonie fixe. La large bande mobile pour les services critiques ne manquera pas de renforcer encore leur domination.

Ainsi, comme cela est souligné au chapitre 6 de la présente étude, il est essentiel d'envisager de nouvelles mesures accordant aux ANR de nouveaux pouvoirs spécifiques, qui leur permettent de faire face à une telle situation, au nom et pour le compte des services critiques, à savoir :

1. les ORM doivent être chargés de soutenir les services critiques. Il semble y avoir deux manières possibles d'y parvenir :

   - pour opérer en tant qu'ORM ou que MVNO, les sociétés autorisées doivent s'engager à fournir des services critiques. Il pourrait s'agir notamment d'une couverture géographique élargie et d'un renforcement pour se conformer aux normes minimales en termes de disponibilité et de résistance, ainsi que de la désignation d'un directeur de programme d'ensemble concernant les services critiques. Il s'agirait, en effet, de toute une série de nouvelles conditions d'autorisation pour exploiter un service mobile public ;

   - autre alternative, le fait que toute acquisition ou exploitation d'une licence concernant des fréquences mobiles comprenne l'obligation de prendre en charge des services critiques pendant toute la durée de l'autorisation. À noter que l'octroi de fréquences conditionné à la fourniture de services critiques accorderait aux ANR le pouvoir de réassigner les fréquences à un nouvel opérateur, si celui d'origine s'avérait défaillant. Ce mécanisme octroie un contrôle effectif aux ANR en la matière, de sorte que les fréquences ne sont pas « perdues ».

   La première alternative commencerait par de nouvelles licences, et la seconde par le transfert des licences existantes. Il ne s'agirait pas là d'une obligation de service *universel*, mais d'une obligation de service *particulière* élargissant les responsabilités des ORM/MVNO sur le long terme. Sur le plan positif, il s'agit d'une obligation rare, qui comporte de nouvelles sources de revenus, accompagnée d'investissements publics dans la résistance, qui bénéficierait à l'ensemble des utilisateurs du réseau ;

2. Les ANR doivent être autorisées à introduire des règlementations qui soutiennent et mettent en œuvre les dispositions des contrats à long terme conclus entre les ORM et les utilisateurs de services critiques ;

3. Les ANR doivent être autorisées à accorder un accès prioritaire aux services des réseaux mobiles commerciaux aux communications critiques, lorsque les circonstances le justifient, et notamment à décider de transmettre des appels entre les différents ORM si cela s'avère nécessaire. Cela pourrait nécessiter la révision des orientations, des lois et des règlementations actuellement en vigueur ;

4. Les ANR doivent aider les gouvernements à fixer des tarifs concernant les services critiques, en analysant les coûts réels d'exploitation des ORM et en effectuant des études comparatives des coûts avec d'autres ANR et sources extérieures à chaque État membre de l'UE. Cela pourrait nécessiter une forme de « juricomptabilité » et une préparation adaptée des déclarations des assiettes des coûts de la part des ORM.

Ainsi, l'une des principales conclusions de cette étude est que les réseaux mobiles commerciaux pourraient être adaptés aux communications critiques, sous réserve de la mise en place d'un cadre juridique, règlementaire et contractuel approprié. Cette conclusion permet à chaque État membre de l'UE de décider de recourir ou non aux ORM dans le cadre des communications critiques. Nulle recommandation n'est formulée dans la présente étude pour imposer un mandat politique uniforme (dans le cadre, par exemple, d'une directive européenne). Néanmoins, des lignes directrices de la Commission, à l'attention des États membres, sur les rôles, les actions, les pouvoirs et les responsabilités des ANR *vis-à-vis* des contrats conclus entre les ORM et les utilisateurs de services critiques pourraient s'avérer souhaitables.

Faut-il réserver des bandes de fréquence additionnelles aux services critiques ?

Compte tenu des obligations légales de nombreux États membres de l'UE relatives à la fourniture, sur le plan national, de communications critiques (notamment en ce qui concerne les services PCSC), ainsi que des traditions politiques et culturelles garantissant avec efficacité que les réseaux détenus et exploités par les gouvernements sont la seule option viable, des fréquences dédiées s'avéreront nécessaires. Dans ces conditions, pour déterminer s'il faut instaurer des fréquences exclusives dédiées, à l'échelle de l'UE, aux services critiques, une approche pragmatique doit être privilégiée. Elle repose sur le principe de subsidiarité : chaque État membre doit choisir sa propre direction. Pour ceux ayant décidé de mettre en place des réseaux dédiés aux services critiques, des fréquences dédiées s'avéreront nécessaires (ce qui constitue une charge financière additionnelle, si les coûts d'opportunité sont reconnus). Il ne s'agit pas là uniquement de la perte de recettes d'enchère, c'est-à-dire la valeur commerciale des fréquences, mais également de la perte de l'effet de levier économique de la large bande sur l'économie en général, bien que certains puissent considérer que le bénéfice socio-économique de ces fréquences aux fonctions des services critiques pourrait compenser cette perte.

La situation économique pourrait forcer à revoir le caractère abordable d'un réseau dédié au cours des prochaines années dans certains États membres. Les coûts pourraient constituer un véritable fardeau, lorsque les versions standard LTE dotées de fonctionnalités pour les services critiques donneront lieu à de nouveaux équipements et les prix diminueront en raison de la hausse des volumes de production. Si un État membre décide alors de migrer d'un réseau fermé dédié vers un réseau commercial partagé, les fréquences auparavant dédiées devront être réaffectées aux réseaux commerciaux, soit avec les utilisateurs des services critiques en tant que seuls clients, soit avec ces derniers en tant qu'utilisateurs prioritaires par rapport au reste des utilisateurs du réseau partagé.

Mais, quelle bande de fréquence faut-il choisir ? Globalement, le débat tourne autour de la gamme de fréquences, car cela définit les caractéristiques physiques qui déterminent les coûts et les performances. C'est bien cette question qui se trouve au cœur de l'opposition entre la télévision européenne et le secteur cellulaire, comme l'a souligné le récent rapport rédigé par le Groupe de haut niveau Lamy, lequel n'est pas parvenu à trouver un consensus sur l'avenir des fréquences UHF au-inférieures à 790 MHz à court terme.

Pour conclure, compte tenu des intérêts des différentes parties prenantes, et notamment de ceux des utilisateurs militaires et de la RMP, il est peu probable que la principale bande utilisée à l'heure actuelle pour TETRA (380-400 MHz) soit disponible à l'échelle de l'UE, et encore moins à des fins de conversion vers la technologie LTE. La bande immédiatement supérieure, de 450 MHz, constitue un choix plus prometteur pour une utilisation dédiée, quasiment la moitié des États membres de l'Union étant prêts à l'utiliser. Si l'on monte encore dans les fréquences, la proposition surprise à WRC-12 pour la région 1 UIT, qui consiste à permettre une utilisation mobile des fréquences 694 à 790 MHz, risque de susciter de vifs débats dans l'ensemble de l'Union européenne, comme le souligne le rapport Lamy. Bien que ce rapport ait suggéré un calendrier pour la mise à disposition de la bande à 700 MHz dans le secteur mobile, cela pourrait ne voir le jour qu'à l'horizon 2018-2022, ce qui coïnciderait avec des générations plus mûres de la technologie LTE, dans ses versions 12 à 14, présentant la plupart des fonctionnalités propres aux services critiques nécessitées par les services PCSC.

La question essentielle est de savoir si une allocation harmonisée exclusive, qui s'accompagne d'offres commerciales, est nécessaire et souhaitable. Selon notre conclusion, compte tenu de la diversité des points de vue parmi les États membres de l'UE, une allocation dédiée aux services critiques à 700 MHz n'est logique qu'à court terme, dans la mesure où une migration postérieure vers des services commerciaux risque d'avoir lieu progressivement au cours des prochaines décennies, en raison de la pression économique accrue sur les budgets publics.

Zusammenfassung

Diese Studie untersucht, ob Breitband-Funknetze für die missionskritische Kommunikation in drei Sektoren genutzt werden können - Sicherheit und Rettungsdienste (PPDR, insbesondere Polizei, Feuerwehr und Rettungsdienste), Versorgungswirtschaft (Elektrizität, Gas und Wasser) und die neuen Intelligenten Verkehrssysteme (ITS), die vor allem im Straßen- und Schienenverkehr verstärkt zum Einsatz kommen. Dabei werden im Wesentlichen zwei Optionen miteinander verglichen: öffentliche Mobilfunknetze (public land mobile networks - PLMN) kommerzieller Anbieter und zweckgebundene Netze, die speziell für diese Sektoren entwickelt wurden.

Die europäischen Gesellschaften sind abhängig von missionskritischen Diensten

Die öffentliche Sicherheit sowie zuverlässige Versorgungs- und Verkehrssysteme sind für die modernen europäischen Gesellschaften überlebenswichtig. Diese Dienstleistungen funktionieren nicht ohne Funknetze und sind zunehmend auch von Breitband-Funkdiensten mit hoher Reichweite abhängig. Diese Studie analysiert Vergangenheit, Gegenwart und Zukunft der missionskritischen Funkkommunikation in diesen drei Sektoren. Traditionell verfügte jeder dieser Sektoren über eigene Funknetze, meist mit eigens reservierten Frequenzen.

Um nur ein Beispiel zu nennen: In den Mitgliedstaaten der EU wurden Mittel in Höhe von mindestens 19 Mrd. € in die Sicherheits- und Rettungsdienste investiert. (Die Gesamtinvestitionen liegen womöglich noch höher, da die Staatsausgaben nicht immer völlig transparent und vollständig zugänglich sind.) Der größte Teil dieser Investitionen wurde in die Technologien TETRA und TETRAPOL investiert, die die neuen Datendienste nur eingeschränkt unterstützen, auch wenn die Sprechkanäle wohl noch für ein Jahrzehnt genutzt werden können und bis zur Einführung einer anderen Technologie die Basis für einige Funknetze der Sicherheits- und Rettungsdienste bilden werden. Die wenigen Hersteller, die missionskritische Technologien anbieten, sind sehr spezialisiert und haben in Europa und weltweit nur einen sehr begrenzten Markt. Dies bedeutet, dass Einspareffekte durch Massenproduktion kaum zustande kommen und auch der Wettbewerb zwischen den wenigen Anbietern nur eingeschränkt stattfindet. Außerdem hat sich gezeigt, dass sich die Geräte verschiedener Hersteller auf Basis der Standards TETRA und TETRAPOL nur schwer miteinander verknüpfen lassen, obwohl die internationale Zusammenarbeit zwischen PPDR und anderen zentralen Diensten immer wichtiger wird. Die uneinheitliche Umsetzung der Standards durch verschiedene Hersteller verhindert, dass die Nutzer der entsprechenden Geräte und Systeme grenz-, rechtssystem- und sektorübergreifend zusammenarbeiten können.

Die europäischen Eisenbahnsysteme nutzen derzeit einen 900 MHz-Dienst auf der Basis ihrer eigenen privaten Funknetze und einer Variante des GSM-Standards, der insgesamt über 25 Mrd. € kosten dürfte (unsere Schätzung). GSM ist immer noch die am häufigsten genutzte Mobilfunktechnologie und für die Bedürfnisse des Schienenverkehrs gut geeignet. Allerdings gibt es, wie bei TETRA und TETRAPOL, nur wenige Hersteller, die missionskritische Geräte speziell für den Schienenverkehr herstellen. Auch die Zukunftsaussichten des Standards sind eher düster, weil die Mobilfunkindustrie von GSM schrittweise auf 3G und 4G umsteigen will. Deshalb ist die Frage noch offen, mit welchen Geräten die neuen Funknetze im Schienenverkehr künftig genutzt werden können.

Gleichzeitig werden in schnellem Tempo neue missionskritische Anwendungen entwickelt. Intelligente Netze für Versorgungsdienste, Videosysteme für die Verkehrssteuerung und bildgebende

Diagnostik für den Rettungsdienst benötigen eine Breitband-Datenübertragung, die über große geografische Flächen verfügbar ist. Breitband wird immer wichtiger, um Leben zu retten, uns mit Strom zu versorgen, Unfälle zu verhindern und die öffentliche Ordnung aufrecht zu erhalten.

Aufgrund der wachsenden Abhängigkeit von digitalen Technologien sind die missionskritischen Dienste in Europa derzeit einem starken Wandel unterworfen. Und mit der verstärkten Interdependenz und Abhängigkeit der europäischen Wirtschaften von einer leistungsfähigen Datenübertragung wird das Konzept der „missionskritischen" Kommunikation auch für andere Sektoren zunehmend relevant. Deshalb umfasst der Begriff „missionskritisch" inzwischen nicht nur die wichtigsten Funktionen im Sicherheits- und Rettungssektor, sondern generell die reibungslose Abwicklung makroökonomischer Prozesse (Abschnitt 2.4 enthält Überlegungen zu einer praktischen Definition des Begriffs).

Effizientere Breitband-Funknetze kommen, aber es gibt ein Problem

In diesen Zusammenhang erscheint es wie eine glückliche Fügung, dass die europäischen Mobilfunknetzbetreiber derzeit ihre Hochgeschwindigkeits-Breitbandnetze massiv ausbauen. Die missionskritischen Sektoren haben jedoch zwei wichtige Einwände gegen die ausschließliche Nutzung kommerzieller Funknetze:

- Kann man sich darauf verlassen, dass kommerzielle Anbieter im Rahmen von langfristigen Verträgen zuverlässige Dienstleistungen zu Festpreisen anbieten?

- Bieten diese Netze die Zuverlässigkeit, Stabilität, Qualität, Sicherheit und Reichweite, die insbesondere in Notsituationen erforderlich sind?

Alle hier behandelten Sektoren sind eng mit ihren Regierungen und der öffentlichen Hand verbunden. Die Rettungsdienste erwarten, dass ihnen die Regierung wichtige Ressourcen, wie kostenlose Frequenzbänder und Vorfahrt im Straßenverkehr, einräumt. Allerdings sind alle Mitgliedstaaten der EU aufgrund der Finanzkrise von 2008 und ihren wachsenden langfristigen Schulden Sparzwängen ausgesetzt. Der Druck auf die öffentlichen Dienste wird vermutlich noch mindestens ein Jahrzehnt anhalten und erzeugt einen Widerspruch: die öffentliche Hand muss ihre Ausgaben kürzen, obwohl die Bürger immer mehr Dienstleistungen erwarten.

Sind kommerzielle Funknetze eine tragfähige Lösung für missionskritische Dienste?

In Zeiten anhaltender Sparzwänge stellt sich zunehmend die Frage: können kommerzielle Mobilfunknetze missionskritische Kommunikation über Breitband und Sprechkanäle angemessen unterstützen? Wenn missionskritische Dienste dieselbe Breitband-Technologie, Infrastruktur und Frequenzbänder nutzen, wie der Massenmarkt, scheinen die wirtschaftlichen Vorteile auf der Hand zu liegen. Die Frage ist, ob trotz der Kostenersparnis auch die gewünschte Ausfallsicherheit und Leistung gewährleistet bleibt.

Als Reaktion auf den Haushaltsdruck und die Einführung einer neuen, leistungsfähigeren Generation mobiler Breitbandnetze hat die Europäische Kommission eine unabhängige detaillierte Untersuchung der Kosten und Nutzen des Einsatzes kommerzieller Funknetze für missionskritische Dienste in Auftrag gegeben. SCF Associates Ltd. wurde gebeten, durch eine eingehende Analyse von fünf Szenarien den Kommunikationsbedarf und die Optionen in drei Sektoren - PPDR, Versorgung und ITS - zu bewerten.

Dabei ist zu beachten, dass in dieser Studie die Verwendung von mobilem *Breitband* für missionskritische Dienste über die Netze kommerzieller Mobilfunknetzbetreiber untersucht wird. Außerdem beinhaltet die Aufgabenstellung eine Analyse *aller drei* Sektoren (Versorgungswirtschaft, ITS auf Straße und Schiene sowie Sicherheits- und Rettungsdienste (PPDR).

Anhand dieser fünf Szenarien werden die Kosten für reservierte Funknetze, kommerzielle Netze von Mobilfunknetzbetreibern und neue kommerzielle LTE-Geräte, die für den Einsatz in reservierten Netzen umgerüstet werden, verglichen. Die Studie kommt zu dem Ergebnis, dass im Allgemeinen die Investitionskosten pro Nutzer bei kommerziellen LTE-Netzen, die aufgerüstet werden und 99 % des Hoheitsgebiets abdecken, geringer ausfallen, als bei speziell entwickelten LTE-Netzen. Die zweite Option ist auch dann am günstigsten, wenn man Investitions- und Betriebskosten gemeinsam betrachtet, obwohl die Kostenvorteile von den verwendeten Frequenzbändern abhängen. Bei 450 MHz liegen die Investitionskosten pro Nutzer eines reservierten Netzes um mehr als 40 % unter denen eines kommerziellen Breitband-Mobilfunknetzes mit 800 MHz. Berücksichtigt man jedoch die Betriebskosten für 10 Jahre, ergeben sich durch die einheitliche Infrastruktur Kostenvorteile für kommerzielle Netze, unabhängig davon, ob diese mit 450, 700 oder 800 MHz betrieben werden. Für ein kommerzielles LTE-Netz, das mit 800 MHz betrieben wird, liegen die Investitionskosten pro Nutzer um rund 40 % unter denen für ein reserviertes LTE-Netz mit 700 MHz. (Wenn Mobilfunknetzbetreiber kommerzielle missionskritische Netze auf einem Frequenzband von 700 MHz betreiben, liegen die Investitionskosten um rund 20 % unter denen eines entsprechendes Netzes auf 800 MHz.)

Allerdings stellen die Kosten nicht das einzige Kriterium dar. Die Studie kommt zu dem Schluss, dass kommerzielle Breitband-Mobilfunknetze für missionskritische Zwecke geeignet sind, sofern ***fünf Voraussetzungen erfüllt sind***.

D. h. die folgenden fünf Bedingungen müssen - vollständig - erfüllt sein:

1. Zunächst müssen kommerzielle Mobilfunknetzbetreiber dazu gezwungen werden, die von missionskritischen Nutzern benötigten Dienstleistungen zu erbringen, ohne durch „Lock-in"-Technologien diese Erweiterung ihrer Marktmacht und sozialen Verantwortung zu missbrauchen. Dazu müssen sich die Mobilfunknetzbetreiber nicht nur verpflichten, ihre Funknetze stabiler zu machen, sie müssen auch Begrenzungen bei der freien Gestaltung von Preisen und Vertragsbedingungen akzeptieren und die Kontinuität von Eigentumsverhältnissen sowie die hohe Qualität der Dienste für die missionskritische Datenübertragung garantieren. Für gute langfristige Geschäftsbeziehungen ist aber ebenso entscheidend, wie die missionskritischen Dienste Geschäftsgebaren und Leistung der Mobilfunknetzbetreiber *wahrnehmen*. Dafür ist mehr erforderlich als eine zivilrechtliche Dienstgütevereinbarung (SLA): die nationalen Regulierungsbehörden aller Mitgliedstaaten müssen kommerzielle Dienste von Mobilfunknetzbetreibern neu regulieren.
2. Kommerzielle Netze müssen vom Funkzugangsnetz bis zum Kernnetz so „verstärkt" und überarbeitet werden, dass sie eine Verfügbarkeit von 99 % erreichen, wobei möglichst eine „Hochverfügbarkeit" angestrebt werden sollte. Außerdem muss die geografische Reichweite und, an besonders vereinbarten Orten, auch die Signalreichweite in Innenräumen an die Bedürfnisse missionskritischer Dienste angepasst werden.
3. Die Verbesserung von Leistung, Reichweite, Zuverlässigkeit und anderen missionskritische Funktionen der Netze muss zu angemessenen Kosten umgesetzt werden. Die selektive Ausdehnung und Verbesserung kommerzieller Netze für missionskritische Zwecke darf nicht mehr kosten als der Aufbau eines eigenen nationalen LTE-Netzes speziell für diesen Zweck.

4. Die verstärkten LTE-Netze müssen in der Lage sein, für jeden der drei Sektoren maßgeschneiderte Dienstleistungen zu erbringen. Jeder Sektor nutzt ganz spezielle Breitband-Anwendungen. Dabei geht es nicht nur um die Übertragung von Videos, bildgebender Diagnostik und den Zugriff auf Datenbanken, wie bei den Sicherheits- und Rettungsdiensten, sondern auch um Telemetrie mit sehr niedrigen Latenzzeiten und die Steuerung von Versorgungs- und Verkehrsnetzen in Echtzeit. Bei den fünf in Kapitel 4 untersuchten Funknetzoptionen können die Bedürfnisse der einzelnen Sektoren umso leichter berücksichtigt werden, je weiter man sich von den bestehenden reservierten Netzen über herkömmliche LTE-Netze zu komplexeren Hybridsystemen bewegt.

5. Es gibt jedoch noch ein weiteres Hindernis: Können kommerzielle Mobilfunknetze die tief verwurzelte Gewohnheit der Mitgliedstaaten überwinden, für Funktionen der öffentlichen Sicherheit staatlich kontrollierte Funknetze zu verwenden? Dies ist nicht nur eine rechtliche, administrative oder finanzielle Frage. In einigen Mitgliedstaaten ist die staatliche Kontrolle Teil des kulturellen und politischen Erbes, ganz zu schweigen von den Investitionen in bestehende Technologien, die sich nur sehr langfristig amortisieren. Aus diesem Grund könnten einige Mitgliedstaaten, wie z. B. Deutschland, Italien und Frankreich, für ihre Sicherheits- und Rettungsdienste kurz und mittelfristig weiterhin auf spezialisierte Funknetze setzen, obwohl diese teurer sind. Dennoch dürften auch diese Staaten billigere Alternativen nicht dauerhaft ignorieren. Vielleicht müssen die Mobilfunknetzbetreiber ihre Vorzüge nur überzeugender anpreisen. In der Zwischenzeit liegt die Entscheidung bei den Mitgliedstaaten.

Diese Hindernisse für die Nutzung kommerzieller Netze lassen sich nicht sofort überwinden. Mittel- und langfristig ist die gemeinsame Nutzung der Infrastruktur von Mobilfunknetzbetreibern durch öffentliche und missionskritische Dienste wirtschaftlich sinnvoll. Das größte Hindernis sind die an den Massenmarkt ausgerichteten Geschäftsmodelle der Mobilfunknetzbetreiber, die an die besonderen Leistungs- und Qualitätsanforderungen von Kunden mit speziellen Bedürfnissen angepasst werden müssen. Die *Wahrnehmung* der Mobilfunknetzbetreiber wird sich allerdings nur langsam ändern. Da missionskritische Funknetze unter die Zuständigkeit nationaler Behörden fallen, dürften kurzfristig weiterhin vorwiegend staatliche Funknetze in diesen Sektoren zum Einsatz kommen. Sobald die oben genannten fünf Bedingungen erfüllt sind, dürften aber immer mehr Mitgliedstaaten zumindest aus Gründen der Wirtschaftlichkeit von geschlossenen Netzen auf offene kommerzielle Netze umsteigen.

Durch welche Maßnahmen können diese Bedingungen erfüllt werden?

In Kapitel 4 wurden die Kosten der einzelnen Szenarien für kommerzielle, reservierte, geteilte und hybride Funknetze analysiert. Dabei hat sich gezeigt, dass die finanziellen Vorgaben auf unterschiedliche Weise eingehalten werden können. Außerdem hat unsere Untersuchung der LTE-Technologie in Kapitel 3 ergeben, dass diese die für missionskritische Funktionen benötigte Qualität bietet, sofern die Normungsorganisationen ihre Versprechungen fristgerecht einlösen.

Für diese Studie wurden die Anforderungen an die drahtlose Datenübertragung in den drei Sektoren im Detail analysiert (siehe Kapitel 2 und die Anhänge, die ein wesentlicher Bestandteil dieses Berichts sind). Die Anforderungen der Sicherheits- und Rettungsdienste werden durch Organisationen wie die Arbeitsgruppe „Strafverfolgung“ des europäischen Rates, und die TETRA and Critical Communications Association (TCCA) klar formuliert. Diese Anforderungen werden jedoch häufig von der Perspektive der Strafverfolgungsbehörden dominiert. Feuerwehr, Rettungsdienste und

Katastrophenschutz haben ihre jeweils eigenen Bedürfnisse, die ebenfalls zu berücksichtigen sind. Daher werden ihre Anforderungen in dieser Studie besonders analysiert (siehe Anhang A).

Was die Versorgungsnetze angeht, erhielten wir von Wirtschaftsverbänden, wie der EUTC (European Utilities Telecom Council) und Eurelectric sowie von einzelnen Versorgern (Iberdrola, Alliander und andere) detaillierte Daten. Auch die Europäische Eisenbahnagentur (ERA) stellte wichtige Daten zur Verfügung, die durch weitere Untersuchungen zu einem klaren Bild der künftigen Anforderungen im Bereich des Schienenverkehrs ergänzt werden konnten. Die Anforderungen der drei Sektoren sind recht unterschiedlich:

- Alle Sicherheits- und Rettungsdienste werden künftig zunehmend mobile Breitband-Anwendung nutzen, wobei jedoch jeder Bereich eine eigene Agenda verfolgt: in der Strafverfolgung steht die Übertragung von Videos und hochaufgelösten Bildern im Vordergrund, bei der Feuerwehr dagegen eher Echtzeitsensoren (z. B. Infrarot-Kameras und tomografische Bewegungsmelder). Rettungsdienste brauchen hochauflösende Bildgebung für die genaue Diagnose und Bewertung von Verletzungen vor Ort und Such- und Rettungsteams könnten mit Hilfe von Drohnen mit Videofunktion große Bereiche schnell absuchen.

- Versorger sind an Breitbandnetzen wenig interessiert, sie benötigen eher einen zuverlässigen großflächigen automatisierten Datenaustausch (M2M) im Burst-Modus zwischen Millionen von Streckenmetern und Nebenstationen. Schwankende Einspeisungen von Solarmodulen und Windkraftwerken verändern die Struktur der Stromerzeugung und stellen Spannungsregelung und Netzwerkstabilität vor völlig neue Herausforderungen. Intelligente Netze ermöglichen neben der reinen Stromverteilung auch eine Zwei-Wege-Kommunikation und neuartige Regelfunktionen. Viele Versorger bestehen auf einem eigenen Kommunikationsnetz, weil sie gesetzlich verpflichtet sind, zuverlässige Versorgungsdienste zu erbringen. Weil sie diese Verpflichtung nicht auf ihre Auftragnehmer übertragen können, sind sie bei der Echtzeit-Steuerung ihrer Netze äußerst ungern von Dritten, z. B. einem Mobilfunknetzbetreiber, abhängig.

- Der neue Standard der Zugsteuerung in Europa ist die schmalbandige Datenübertragung über leitungsvermittelte Sprechverbindungen. Im Bereich der nicht operativen bzw. nicht missionskritischen drahtlosen Datenübertragung kann beispielsweise ein Internetzugang über Wi-Fi für alle Fahrgäste zur Steigerung der Passagierzahlen beitragen, die die Europäische Kommission anstrebt, um ihre Ziele bei der Senkung der Treibhausgasemissionen erreichen zu können. Welche Anwendungen künftig im Straßenverkehr genutzt werden, ist eine besonders komplexe und schwer zu beantwortende Frage. Sie reichen von der Datenübertragung zwischen einzelnen Fahrzeugen mit 5,9 GHz bis zur Unfallmeldung über eCall und die automatische Kennzeichenerfassung zur Überwachung von Geschwindigkeitsbegrenzungen und der Erhebung von Mautgebühren.

Für diese Studie wurden zunächst die unterschiedlichen Anforderungen der Sektoren identifiziert. Dann wurde geprüft, ob die Anwendungen über ein gemeinsames Funknetz betrieben werden können, und schließlich wurden die Kosten für die verschiedenen Lösungsoptionen berechnet.

Kapitel 3 behandelt die Angebotsseite und untersucht die aktuelle und zu erwartende Leistung und Qualität kommerzieller Mobilfunknetze. Das wichtigste Forum, von dem diese Leistung abhängt, ist die Partnerschaft von ETSI/3GPP zur Weiterentwicklung des LTE-Standards. Für diese Studie wurde der Prozess beobachtet, durch den missionskritische Funktionen in den LTE-Standard integriert werden, insbesondere in den Versionen 12, 13 und 14, und ein wahrscheinlicher Zeitplan für die Entwicklung von Systemen aufgestellt, die das Wechselsprechen, Sendeumschaltungen, Prioritätsverbindungen und ähnliche Funktionen ermöglichen. Außerdem haben wir untersucht, in welchem Umfang die Mobilfunknetzbetreiber in den Mitgliedstaaten bereits eine LTE-Infrastruktur einsetzen. Nur weil neue Systeme verfügbar sind, bedeutet dies nicht automatisch, dass ältere Anlagen ersetzt werden. Nach dem derzeitigen Fahrplan für LTE wird vor 2016 kaum eine missionskritische Funktion in der Praxis verfügbar sein, einige Funktionen dann eventuell ab 2018 und der Großteil ab 2020. Bis 2020 dürfte dementsprechend die für missionskritische Anwendungen geeignete LTE-Technologie nicht völlig standardisiert sein.

Die zweite wichtige Voraussetzung für die Einführung neuer missionskritischer Breitband-Funknetze sind verfügbare UHF-Frequenzen. Um Geräte kostengünstig herstellen zu können, muss der Markt für die jeweilige Frequenz groß genug sein, um eine Massenfertigung zu erlauben. Nach Angaben von Chipherstellern (von denen die Gerätehersteller abhängig sind), stellt das Frequenzband 450 MHz einen ziemlich großen Markt dar, weil in Brasilien, Bangladesch und Finnland bereits entsprechende Netze aufgebaut werden. Auch der 700 MHz-Markt wird weltweit wirtschaftlich rentabel und könnte den 450 MHz-Markt mengenmäßig sogar noch übertreffen.

Ob Handgeräte in mehreren unterschiedlichen Frequenzbändern einsetzbar sind, hängt von Form und Größe der Antenne ab, da die durch die Software definierten RF-Frontends flexibel sind, wobei Hardware mit mehreren Sende- und Empfangsantennen (MIMO) einen höheren Datendurchsatz und eine höhere Signalstärke bietet. Mit LTE ist aber auch die Bündelung mehrerer Frequenzbänder zu „virtuellen Kanälen“ möglich, was ebenfalls eine größere Bandbreite und damit eine schnellere Datenübertragung erlaubt.

Von den fünf analysierten Szenarien stellen kommerzielle LTE-Netze die kostengünstigste Breitband-Lösung dar

Anhand der Fakten zu technischen Möglichkeiten und Frequenzbändern wurden für die Studie fünf Szenarien mit unterschiedlichen Verwendungsoptionen entworfen:

1. Eigene Funknetze und speziell entwickelte Ausrüstung
2. Kommerzielle Funknetze von Mobilfunknetzbetreibern und kommerzielle Ausrüstung
3. Eigene Funknetze mit kommerziellen Geräten
4. Hybride Funknetze
5. Ein einheitliches multifunktionales Funknetz, möglicherweise für jeweils eine Region

Dann wurden die Kosten für diese Optionen berechnet und verglichen. Grundprinzip für den Vergleich war die Verwendung mobiler Breitbandnetze für zusätzliche Funktionen, die den Nutzern des Netzes und der Gesellschaft als Ganzes einen Mehrwert bieten.

Im ersten Szenario werden die bestehenden eigenen Funknetze und Spezialgeräte weiterhin genutzt, d. h. es wurden Kosten und Nutzen einer Weiterführung von TETRA bzw. TETRAPOL untersucht. Dabei hat sich gezeigt, dass die Kosten zwar hoch sind, jedoch niedriger als bei anderen Optionen, sofern nicht der Wert der zusätzlichen Funktionen und Vorteile mit eingepreist wird.

Dies zeigt sich besonders in Szenario 3, bei dem ein eigenes Funknetz mit kommerziellen, speziell aufgerüsteten Geräten betrieben wird. Da noch nicht über eine mögliche Neuverteilung von Frequenzen in Europa entschieden ist, basiert unsere Modellrechnung auf einem kommerziellen LTE-Funknetz auf 800 MHz, wobei die Kosten für niedrigere bzw. höhere Frequenzbänder ebenfalls berechnet und verglichen wurden. Da zu einem späteren Zeitpunkt möglicherweise niedrigere UHF-Frequenzbänder verfügbar sein werden, wurden anhand einer Sensitivitätsanalyse die Kosten für den wichtigsten Kostenfaktor, nämlich die Anzahl der für die verschiedenen Frequenzen benötigten Basisstationen, berechnet.

Szenario 2 ist vermutlich die beste Option, weil sie sich auf die Nutzung kommerzieller Funknetze konzentriert. Hier ist der entscheidende Kostenfaktor die Aufrüstung des Funkzugangsnetzes und des Kernnetzes, um die erforderliche Stabilität zu erreichen. (Wir gehen davon aus, dass die Regierungen die entsprechenden Kosten übernehmen würden, dies ist aber natürlich nur eine Annahme). Das größte Problem bei diesem Szenario sind jedoch nicht die technologischen Herausforderungen beim Aufbau eines stabilen Funknetzes, sondern der administrative, rechtliche und vertragliche Rahmen. Auf der Grundlage der in Kapitel 5 analysierten Fallstudie des neuen, von kommerziellen Mobilfunknetzbetreibern bereitgestellten PPDR-Funknetzes , mit dem die britische Regierung das derzeitige Airwave TETRA-Netz ersetzten wird, wurde eine pragmatische Vertragsstruktur definiert, die auch in den Szenarien 2 und 4 eingesetzt werden kann. Diese Vertragsstruktur besteht aus vier Verträgen zwischen einer Zentralregierung und kommerziellen Anbietern, durch welche vier wichtige Rollen zugewiesen werden:

5. *Programmmanager* – verantwortlich für das langfristige Management der Funknetzdienste und die Erfüllung der anderen drei Verträge (in der Terminologie der britischen Regierung der „Leistungspartner“).

6. *System- und Netzintegrator* – ist für den Vertrieb von Handgeräten, Software und anderen Geräten an die Endnutzer verantwortlich (diese Rolle kann unabhängig von der Systemintegration ausgeübt werden).

7. *Mehrere Mobilfunknetzbetreiber, die mobile Dienste mit Mengenrabatten über aufgerüstete Funknetze anbieten*. Interessanterweise sehen die Mobilfunknetzbetreiber in den missionskritischen Diensten neue Einkommensquellen mit strahlenden Zukunftsaussichten, insbesondere wenn die Regierung die Kosten für die Aufrüstung der Funknetze gemäß den Anforderungen des PPDR-Sektors übernimmt. In der Studie wird vorausgesetzt, dass die Regierung für ihren Sicherheits- und Rettungssektor Dienste zu einem wesentlich günstigeren Preis kaufen kann als einzelne Privatkunden. Außerdem wird durch das Ausschreibungsverfahren mit Angeboten mehrerer Mobilfunknetzbetreiber ein wettbewerbliches Element in die Preisbildung eingeführt.

8. *Zusatzleistungen für mehr Reichweite* – da die meisten kommerziellen Mobilfunknetzbetreiber nur 90% des Hoheitsgebiets abdecken, der PPDR-Sektor jedoch eine Abdeckung von 99 % benötigt, die auch in Tunneln, unterirdischen Garagen und anderen von Mauern umgebenen öffentlichen Räumen funktioniert.

Diese Verträge müssen zahlreiche Sonderklauseln enthalten, wie z. B. ein Eingriffsrecht der Regierung bei Netzausfällen, eine Dienstgütevereinbarung mit fester Mindestverfügbarkeit, eine Einschränkung der Vertragsübernahmen und eine Einschränkung der Möglichkeit sich auf *Höhere Gewalt* zu berufen usw. Für die Sicherheit missionskritischer Dienstleistung sind jedoch noch weitere Aspekte notwendig.

Ein entsprechender Rahmen kann natürlich, wie im britischen Fallbeispiel, durch direkte Verträge zwischen Anbietern und dem Innenministerium (Home Office) definiert werden. Langfristig kostengünstiger ist aber möglicherweise die Beauftragung eines Mobilfunkdiscounters als Programmmanager oder sogar als Leiter des Programmmanagers. Das belgische Funknetz ASTRID mit dem Mobilfunkdiscounter Blue Light Mobile ist ein Beispiel für einen entsprechenden Ansatz (siehe Kapitel 5).

Wie die Kostenanalyse ergeben hat, sind Optionen mit kommerziellen LTE-Netzen rein finanziell die günstigste Lösung (siehe Kapitel 4). Um den tatsächlichen Wert der einzelnen Optionen zu ermitteln, müssen jedoch auch andere Faktoren berücksichtigt werden, beispielsweise die Zuverlässigkeit des Funknetzes und seine Eignung für alle drei Sektoren, insbesondere bei der automatisierten Datenübertragung (M2M).

In diesem Sinne ist das hybride Funknetz aus Szenario 4 wesentlich besser für Versorgungs- und ITS-Netze geeignet, als entweder ein rein kommerzielles oder ein speziell entwickeltes Funknetz, kostet dafür aber auch mehr als diese. Weitere Vorteile wären seine höhere Flexibilität bei der Integration bestehender Funknetze und die Möglichkeit einer schrittweisen Umstellung.

Um Nutzer zu gewinnen braucht es mehr als einen guten Vertrag

Alle drei Sektoren (und insbesondere die Nutzer, die wie die Versorgungsunternehmen gesetzlich zu einer gewissen Betriebskontinuität verpflichtet sind) müssen sich darauf verlassen können, dass die Mobilfunknetzbetreiber auch in den kommenden Jahrzehnten die vereinbarte Leistungsqualität aufrecht erhalten. Um dies zu gewährleisten sind neben entsprechenden Vertragsstrukturen möglicherweise auch gesetzgeberische Maßnahmen erforderlich. Nur so können die betroffenen Sektoren davon überzeugt werden, dass das Geschäftsgebaren der Mobilfunknetzbetreiber ihre missionskritischen Dienste nicht gefährdet. Um das Vertrauen der Nutzer in die Mobilfunknetzbetreiber zu erhöhen, sind die folgenden Maßnahmen erforderlich:

1. Verpflichtung, schnellstmöglich ein hohe Stabilität und Zuverlässigkeit aufzubauen und Störungen unverzüglich zu beheben, die über mehrere Jahrzehnte auf dem gleichen hohen Leistungsniveau bestehen bleibt.

2. Langfristige (15 bis 30 Jahre) vertragliche Verpflichtungen gegenüber missionskritischen Kunden zu festen Bedingungen und Tarifen.

3. Vorrangige Bearbeitung missionskritischer Dienstleistungen, insbesondere in Notsituationen, in denen eine Überlastung des Funknetzes möglich ist.

4. Garantie einer geografischen Reichweite und Durchdringung, die den Bedürfnissen missionskritischer Nutzer entspricht.

5. Bereitschaft zur Zusammenarbeit mit anderen Mobilfunknetzbetreibern und Mobilfunkdiscountern - beispielsweise bei der Weiterleitung missionskritischer Anrufe an Anbieter mit einer höheren Signalstärke vor Ort.

6. Inhaltliche und wörtliche Einhaltung langfristiger Verträge für missionskritische Dienstleistungen ohne willkürliche Änderung von technischen Funktionen, Tarifen oder Geschäftsbedingungen.

7. Bereitschaft, die kostenbasierte Preisgestaltung von Tarifen anhand einer transparenten Buchführung gegenüber nationalen Regulierungsbehörden und öffentlichen Kunden offen zu legen.

8. Bereitschaft zur Einführung neuer Gebührensysteme und Messverfahren.

9. Aufgabe überteuerter Gebühren für Roaming-Dienste innerhalb der EU und Vermeidung von „Überraschungsgebühren“ für bereits vereinbarte Dienstleistungen.

Diese Maßnahmen sind erforderlich, weil die Mobilfunknetzbetreiber heute fast dieselbe Monopolstellung einnehmen, wie ihre Vorgänger aus den Zeiten des Festnetzes. Von kleinen Unternehmen, die den Status Quo herausfordern, haben sie sich zur dominanten Macht im

Telekommunikationsmarkt entwickelt. Inzwischen haben diese Unternehmen mindestens fünfmal mehr Abonnements verkauft als je ein Festnetzbetreiber. Die Einführung missionskritischer Breitband-Mobilfunknetze wird ihre Marktmacht zusätzlich stärken.

Als Reaktion auf diese Entwicklung ist es notwendig, die in Kapitel 6 beschriebenen Maßnahmen zu ergreifen, um den nationalen Regulierungsbehörden neue Mittel an die Hand zu geben, mit denen sie die Interessen der missionskritischen Sektoren vertreten können.

1. Mobilfunknetzbetreiber sollten gesetzlich verpflichtet werden, missionskritische Sektoren zu unterstützen. Dafür gibt es zwei mögliche Verfahren:

    - Für die Zulassung als Mobilfunknetzbetreiber oder Mobilfunkdiscounter müssen sich Unternehmen zur Erbringung missionskritischer Dienstleistungen verpflichten. Dazu kann die Ausweitung der geografischen Reichweite, die Erfüllung von Mindeststandards bei Leistung und Stabilität durch einen entsprechenden Ausbau der Infrastruktur und die Ernennung eines Programmmanagers für missionskritische Dienstleistungen gehören. Praktisch läuft dies auf eine Reihe neuer Zulassungsbedingungen für den Betrieb eines öffentlichen Funknetzes hinaus.

    - Alternativ kann der Kauf oder die Nutzung von Mobilfunklizenzen mit der Verpflichtung verbunden werden, während der gesamten Gültigkeit der Lizenz missionskritische Dienste zu unterstützen. Wenn Lizenzen für bestimmte Frequenzen an missionskritische Dienste gebunden sind, eröffnet dies den nationalen Regulierungsbehörden die Möglichkeit, Frequenzen an einen neuen Anbieter zu übertragen, wenn der ursprüngliche Anbieter die geforderten Leistungen nicht erbringt. Dieser Mechanismus erlaubt den Regulierungsbehörden eine wirksame Kontrolle, weil Frequenzbänder neu zugewiesen werden können und damit nicht „verloren“ gehen.

    Bei der ersten Alternative steht die Vergabe neuer Lizenzen im Vordergrund, bei der zweiten die Übertragung bereits bestehender Lizenzen. Dabei handelt es sich nicht um eine *universelle* Leistungspflicht, sondern um eine *spezielle* Leistungspflicht, die Mobilfunknetzbetreibern bzw. Mobilfunkdiscountern langfristig neue Verpflichtungen auferlegt. Andererseits sind diese Verpflichtungen mit neuen Einkommensquellen verbunden, und die staatlichen Investitionen für mehr Netzstabilität kommen allen Nutzern des Funknetzes zugute.

2. Regulierungsbehörden müssen Vorschriften erlassen können, die in der Lage sind, langfristige Verträge zwischen Mobilfunknetzbetreibern und missionskritischen Nutzern zu fördern und deren Bestimmungen durchsetzen.

3. Regulierungsbehörden sollten kommerziellen Mobilfunkdiensten für missionskritische Datenübertragung vorrangigen Zugang gewähren können, wenn die Umstände dies gebieten, beispielsweise für die Weiterleitung von Anrufen zwischen einzelnen Mobilfunknetzbetreibern. Dazu müssen möglicherweise bestehende Richtlinien, Gesetze oder Vorschriften überarbeitet werden.

4. Regulierungsbehörden sollte ihre Regierungen durch Untersuchung der realen Kosten der Mobilfunknetzbetreiber und durch vergleichende Kostenanalysen mit anderen Regulierungsbehörden und anderen Quellen außerhalb des jeweiligen Mitgliedstaates dabei unterstützen, die Tarife für missionskritische Dienste festzulegen. Dazu sind ggf. eine forensische Rechnungsprüfung und eine zweckmäßige Offenlegung der Kostenrechnung durch die Mobilfunknetzbetreiber erforderlich.

Diese Studie kommt daher zu der Schlussfolgerung, dass kommerzielle Mobilfunknetze sich für die missionskritische Datenübertragung eignen, wenn entsprechende rechtliche, administrative und vertragliche Rahmenbedingungen vorliegen. Auf der Grundlage dieses Ergebnisses kann jeder Mitgliedstaat selbst entscheiden, ob er Mobilfunknetzbetreiber mit der missionskritischen Datenübertragung betrauen möchte. Diese Studie spricht keine Empfehlung für eine gemeinschaftliche politische Strategie aus (z. B. in Form einer EU-Richtlinie). Allerdings wäre es möglicherweise hilfreich, wenn die Kommission Leitlinien für Rolle, Aufgabe, Machtmittel und Zuständigkeit nationaler Regulierungsbehörden *in Bezug auf* mögliche Verträge zwischen Mobilfunknetzbetreibern und missionskritischen Nutzern entwickeln würde.

Sollten für missionskritische Dienstleistungen weitere Frequenzbänder reserviert werden?

Die Regierungen vieler Mitgliedstaaten sind gesetzlich zur Bereitstellung missionskritischer Datenübertragungssysteme (insbesondere für die Sicherheits- und Rettungsdienste) verpflichtet. Ihre politische und kulturelle Tradition macht Funknetze, die im staatlichen Besitz sind und vom Staat betrieben werden, zur einzig gangbaren Option. Aus diesem Grund sind für diese Funknetze reservierte Frequenzen erforderlich. Deshalb sollte die entscheidende Frage, ob europaweit bestimmte Frequenzbänder für missionskritische Sektoren reserviert werden müssen, pragmatisch beantwortet werden. Dies ergibt sich auch aus dem Subsidiaritätsprinzip, nach dem jeder Mitgliedstaat über seine eigenen Lösungswege entscheidet. Mitgliedstaaten, die spezielle missionskritische Funknetze aufbauen möchten, benötigen dazu reservierte Frequenzbänder, was bei Anrechnung der Opportunitätskosten eine zusätzliche finanzielle Belastung darstellt. Dabei geht es nicht nur um entgangene Auktionsgewinne, d. h. den Marktwert des Frequenzbands, sondern auch um den mangelnden Anschub für die wirtschaftliche Gesamtentwicklung. Allerdings könnte man auch argumentieren, dass diese Kosten durch die sozioökonomischen Vorteile der Nutzung des Frequenzbandes für missionskritische Dienste wieder ausgeglichen werden.

Die wirtschaftliche Lage dürfte in einigen Mitgliedstaaten dazu führen, dass die Rentabilität spezieller zweckgebundener Funknetze neu bewertet werden muss. Insbesondere dann, wenn die neuen LTE-Standards mit missionskritischer Funktionalität in neuen Geräten eingesetzt werden, deren Preise aufgrund der Massenproduktion sinken. Wenn Mitgliedstaaten dann von einem geschlossenen Funknetz auf ein offenes kommerzielles Funknetz umrüsten, können die bisher reservierten Frequenzbänder auf kommerzielle Funknetze verteilt werden. Diese können missionskritischen Nutzern dann entweder exklusiv oder zumindest vorrangig zur Verfügung gestellt werden.

Aber welche Frequenzbänder sollten reserviert werden? Die physikalischen Eigenschaften, die über die Kosten und Leistung des Funknetzes entscheiden, hängen vom Frequenzbereich ab. Um dieses Thema dreht sich auch der noch offene Streit zwischen den europäischen Rundfunk- bzw. Mobilfunkbetreibern, der auch im Bericht der hochrangigen Gruppe um Pascal Lamy über die künftige Nutzung der UHF-Frequenzen unterhalb von 790 MHZ behandelt wird.

Diese Studie kommt zu dem Ergebnis, dass aufgrund der zahlreichen beteiligten Akteure und insbesondere der vielen militärischen und privaten Nutzer, das derzeit für TETRA reservierte Frequenzband (380-400 MHz) vermutlich nicht europaweit freigegeben werden wird, vor allem nicht für die Umwandlung in ein LTE-Funknetz. Das nächsthöhere Frequenzband um 450 MHz ist schon eher ein vielversprechender Kandidat für ein speziell entwickeltes Funknetz, da bereits fast die Hälfte der Mitgliedstaaten eine entsprechende Verwendung zumindest erwägt. Wie der Lamy-Bericht zeigt, wird auch der überraschende Vorschlag der World Radiocommunication Conference 2012, in der ITU-Region 1 das Frequenzband 694-790 MHz für Mobilfunknetze freizugeben, europaweit heftig diskutiert. Allerdings soll das Frequenzband um 700 MHz gemäß dem Lamy-Bericht frühestens zwischen 2018 und 2022 für den Mobilfunk freigegeben werden. Dies würde dann mit ausgereiften Versionen des LTE-Standards zusammenfallen, bei denen in den Versionen 12-14 die meisten missionskritischen Funktionen, welche die Sicherheits- und Rettungsdienste benötigen, bereits enthalten sind.

Die entscheidende Frage ist, ob harmonisierte exklusive Zuweisungen überhaupt notwendig und wünschenswert sind, wenn derartige kommerzielle Angebote zur Verfügung stehen. Die vorliegende Studie hat gezeigt, dass zu diesem Thema unter den Mitgliedstaaten keine Einigkeit herrscht. Außerdem dürfte der zunehmende finanzielle Druck auf die staatlichen Haushalte dazu führen, dass im kommenden Jahrzehnt immer mehr Staaten schrittweise auf kommerzielle Dienstleistungen umsteigen. Aus diesen Gründen ist die Reservierung des Frequenzbands um 700 MHz für geschlossene missionskritische Funknetze höchstens kurzfristig sinnvoll.

Abbreviations

2G	Second Generation cellular (GSM)
3G	Third Generation cellular (UMTS, HSPA, EDGE, LTE)
3GPP	3rd Generation Partnership Project
AGA	Air-Ground-Air
APCO	Association of Public-safety Communications Officials
APT	Asia-Pacific Telecommunity
ARCEP	Autorité de Régulation des Communications Électroniques et des Postes
ATEX	ATmosphères EXplosibles (explosive atmospheres)
BBDR	Broad Band for Disaster Relief
BEM	Block Edge Mask
BTS	Base Transceiver Station
CCTV	Closed Circuit Television
CEPT	European Conference of Postal and Telecommunications Administrations
CDMA	Code Division Multiple Access
CDMA2000	Code Division Multiple Access 2000 (3G)
CITEL	Comisión Interamericana de Telecomunicaciones (Inter-American Telecommunication Commission)
C-ITS	Cooperative Intelligent Transport Systems
COCOM	COmmunications COMmittee, DG CONNECT
COTS	Commercial Off-The-Shelf (equipment)
DARPA	Defense Advanced Research Projects Agency
DMO	Direct Mode Operation
DMR	Digital Mobile Radio
DNO	Distribution Network Operator
DR	Disaster Relief
ECO	European Communications Office
ECC	Electronic Communications Committee
EDF	Électricité de France SA
EDGE	Enhanced Data for GSM Evolution
EFFUA	European Fire Fighters Unions Alliance
EPC	Evolved Packet Core (3GPP)
EPCIP	European Programme for Critical Infrastructure Protection
ERA	European Rail Agency
ERNCIP	European Reference Network for Critical Infrastructure Protection
ESENet	Emergency Services Europe Network
EIRENE	European Integrated Railway Radio Enhanced Network
ETC	Electronic Toll Collection
EMS	Emergency Medical Services
ENISA	European Network and Information Security Agency
ERTMS	European Rail Traffic Management System
ESMCP	Emergency Services Mobile Communications Programme (UK)
ESMIG	European Smart Metering Industry Group

ETCS	European Train Control System
ETSI	European Telecommunications Standards Institute
EUTC	European Utilities Telecommunication Council
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
EVC	European Vital Computer (onboard train control computer)
FDD	Frequency Division Duplex
FEU	Federation of European Union Fire Officers Associations
FLASH	Fast Low-latency Access with Seamless Handoff
FM	Frequency Modulation
GCSE	Group Communication System Enablers
GDF	Gaz de France
GHG	Greenhouse Gases
GO-CO	Government Owned – Commercially Operated
GO-GO	Government Owned – Government Operated
GPRS	General Packet Radio Service
GPS	Global Positioning Satellite
GSM	Global System for Mobile (2G)
GSM-R	Global System for Mobile - Railways
HAZMAT	Hazardous Material
HDTV	High Definition Television
HSDPA	High-Speed Downlink Packet Access (3G)
HSPA	High Speed Packet Access (3G)
HVAC	Heating, Ventilation and Air Conditioning
IC	Incident Commander
ICE	Intervention in Chemical Emergencies project
ICT	Information and Communications Technology
IEEE	Institute of Electrical & Electronics Engineers
IMS	IP multimedia subsystem
ISM	Industrial, Scientific and Medical (radio bands)
ITS	Intelligent Transport Systems
ITU	International Telecommunication Union
JPEG	Joint Photographic Experts Group
LAA	Licensed Assisted Access
LEWP	Law Enforcement Working Party
LPG	Liquified Petroleum Gas
LRIC	Long Run Incremental Cost
LRTC	Least Restrictive Technical Conditions
LSA	Licensed Shared Access
LSE	London School of Economics
LTE	Long Term Evolution (of UMTS)
LTE-A	LTE-Advanced
LTE-U	LTE-Unlicensed
M2M	Machine-to-Machine
MCPTT	Mission Critical Push-To-Talk
MFCN	Mobile/Fixed Communications Network
MORANE	Mobile Radio for Railway Networks in Europe
MPEG	Moving Picture Experts Group
MNO	Mobile Network Operator

MPT 1327	Ministry of Posts & Telegraph signalling standard 1327 (for trunked analogue radio networks with digital control channels)
MVNO	Mobile Virtual Network Operator
NATO	North Atlantic Treaty Organisation
NFV	Network Function Virtualisation
OAS	Organisation of American States
OFDM	Orthogonal Frequency-Division Multiplexing
OHCA	Out of Hospital Cardiac Arrest
PC	Personal Computer
PABX	Private Automatic Branch Exchange
PAMR	Public Access Mobile Radio
PLC	Power Line Communication
PLMN	Public Land Mobile Network
PMR	Professional Mobile Radio
PMSE	Programme Making and Special Events
PP	Public Protection
PPDR	Public Protection and Disaster Relief
PPP	Public-Private Partnership
PSTN	Public Switched Telephone Network
PTT	Push-To-Talk
QoS	Quality of Service
RAN	Radio Access Network
RF	Radio Frequency
RFID	Radio Frequency Identification
RSPG	Radio Spectrum Policy Group
SAB	Services Ancillary to Broadcasting
SAR	Search And Rescue
SCADA	Supervisory Control And Data Acquisition (system)
SCBA	Self-Contained Breathing Apparatus
SDN	Software Defined Network
SDR	Software Defined Radio
SIM	Subscriber Identity Module
SINE	SIkkerheds NEt (Denmark's "Safety Net")
SLA	Service Level Agreement
SRD	Short-Range Device
SRDoc	System Reference Document (ETSI request for a change in radio frequency allocation)
SWD	Staff Working Document
SWOT	Strengths, Weaknesses, Opportunities and Threats
TCCA	TETRA and Critical Communications Association
TDD	Time Division Duplex
TEDS	TETRA Enhanced Data Service
TEN-T	Trans European Network - Transport
UAV	Unmanned Aerial Vehicle
UMTS	Universal Mobile Telecommunications System (3G)
UNB	Ultra-Narrow-Band
UPS	Uninterruptible Power Supply
UTRA-FDD	UMTS Terrestrial Radio Access - Frequency Division Duplexing

UWB	Ultra-Wide Band
VAT	Value Added Tax
VICS	Vehicle Information Communication System
VoLTE	Voice over LTE
WAP	Wireless Application Protocol
WAS/RLAN	Wireless Access Systems including Radio Local Area Networks
WBB	Wireless Broad Band
W-CDMA	Wideband Code Division Multiple Access
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WRC-12, WRC-15	ITU World Radiocommunication Conferences in 2012 & 2015
WSD	White Space Device

1 Context, Objectives, Method and Description of Work Carried Out

1.1 Context

Managing a complex economy today is unthinkable without radio. Radio communications enable societies to respond effectively to emergencies, disasters and challenges to public order. For utilities, blanket coverage of populated areas by radio enables the rapid reporting of faults and supply/demand imbalances, preventing outages which could paralyse entire regions while managing peak load demand. The transportation sector benefits from wireless links in ways we are still just starting to explore.

General purpose communication platforms – such as broadband internet and advanced cellular networks – tend to be much more economically and spectrally efficient than dedicated networks. However, they might not have all the features of a network designed for a specific purpose. Thus, the efficiency gains and cost savings of shared infrastructure come at a price: some functionality might be sacrificed, along with a margin of safety from having independent networks (simultaneous failure of separate networks being less likely than the failure of one comprehensive network).

On the other hand, adding functionalities needed only by a subset of users raises the cost of a general purpose network. How significant the added cost, how much can be saved by sharing infrastructure, and how much efficiency and resilience are worth, are all subjects for debate. In fact, they are questions this study will explore after mapping the requirements and actual network deployments of the three sectors that are our focus, and after considering the current and emerging capabilities of commercial public cellular networks.

Yet there is little doubt that the current users of specialised networks are under pressure to find cost savings and additional bandwidth, and regulators are under pressure to increase efficiency of spectrum use. These factors are the key drivers for this study.

A common source of inefficiency in spectrum use was noted in the European Commission report *Perspectives on the Value of Shared Spectrum Access* (2012):

> the tradition of authorising communication infrastructures to be owned and operated by a single licensee or dedicated to a single purpose, application or profession. The result is that many channels and communication systems, used only intermittently, are permanently reserved for a small number of users. Idle resources are not available to any other service or user…

Is shared infrastructure a solution to the current lack of frequencies for mission critical broadband? This report will explore that issue and consider many related questions along the way.

1.2 Objectives

Our overall objective was to assess the possible cost savings if PPDR, ITS and utilities used non-specialist networks and equipment in place of dedicated networks and equipment. At the very least, that required estimating the cost of providing mission critical high-speed broadband to these sectors, with and without the use of commercial public networks. That in turn depends on a clear statement of the communication requirements of these sectors with sector-relevant definitions of "mission critical". But because public cellular has evolved to meet its own business criteria and license obligations, it is not yet always a perfect substitute for networks dedicated for PPDR, ITS and utilities applications. The tasks assigned for this study show the Commission realises that direct substitution may be not be feasible. Consequently, the study requires establishing a baseline of what is practical through:

- An analysis of how “mission critical” communications for the utility and intelligent transport (ITS) sectors differ from PPDR and from each other;
- Analysis of the extent to which state-of-the-art commercial mobile networks and equipment or the networks and equipment expected in the foreseeable future can meet the mission-critical and non-mission-critical requirements of these sectors;
- A description of the current situation with regard to the use of mobile communication networks in each of the 3 sectors (augmented with 6 case studies);
- Comparative overviews of the costs and benefits associated with meeting the wireless communication needs of the three sectors by different networking approaches for five scenarios:
    1. Dedicated specialised networks using specialised equipment only;
    2. Commercial networks using commercial equipment only;
    3. Dedicated specialised networks using commercial equipment;
    4. Hybrid solutions involving dedicated specialised and commercial networks;
    5. Assessing the extent to which the three sectors could share network infrastructure.

The final objective was to draw conclusions on current and future use of commercial mobile networks for mission critical communications in the three sectors.

1.3 Methodology and description of work carried out

Our approach was to examine the tasks set out in the terms of reference and prepare a widespread information gathering exercise before we could begin formulating this report. That required frequent contacts with professionals in the three sectors, through interviews (over 25 with sectoral representatives and other stakeholders such as suppliers, regulators and standards setting bodies) as well as the organisation of fact-finding events and site visits. We held a stakeholders’ workshop, attended a demonstration of proof of concept for a future LTE-based emergency services network and the Critical Communications industry conference in Amsterdam. We presented preliminary findings of our research at an ETSI 3GPP meeting that was considering extension of the LTE standards into mission critical functionality. These were supplemented by research into the equipment used in the three sectors as well as current commercial cellular service offerings, pricing and technology platforms. Much time was spent on cost analysis of existing systems across the EU, relying whenever possible on government audit reports. Finally all was pulled together and analysed, using a variety of approaches to extrapolate the costs of systems that do not exist today. Much effort was needed to fill gaps left by the limited information and accuracy of network cost data.

Thus in Chapter 2, requirements across the sectors are examined while Chapter 3 analyses the capabilities of commercial mobile networks to meet mission critical needs. In Chapter 4, the cost analysis of the various scenarios is considered, with a value analysis of the options and of social benefits. Case studies across the EU and the world are gathered in Chapter 5 while conclusions are drawn in Chapter 6.

2 Requirements that Shape Wireless Communication Needs for Mission Critical Operations

2.1 Introduction

For each of the three sectors (PPDR, utilities and ITS) we identify their requirements and describe the operational, functional and safety related needs which will have an impact on the type of wireless communications needed. We then provide a comprehensive overview of the main characteristics of current network operations and user equipment in each of the three sectors in Europe. Finally the chapter attempts to clarify the applicability and relevance of the terms "mission-critical" and "non-mission-critical" communications, taking into account the specific features and meanings of these terms in each sector.

Because the communication requirements of police agencies have been presented on many occasions, our detailed description of the basis for those requirements is in Appendix A**.** And since differences are often overlooked in the communication needs of police, fire brigades, search and rescue, emergency medical services and disaster response teams, our descriptions of the operational requirements of these other specialisations are in the same Appendix for easy comparison. The same logic dictated that the operational needs of the utility and transport sectors should be in the Appendixes, too: B and C. Finally, since the focus of this report is mobile broadband, requirements specific to voice communication are also described in the Appendixes. As a result, the first part of Chapter 2 contains only summaries of the communication requirements to give readers a shorter path to the analysis and conclusions that follow.

2.2 Summary of operational, functional and safety requirements

2.2.1 Public Protection and Disaster Relief

The following broad overview of PPDR requirements for radio communication is based on FP7 Project HELP's analysis of operational scenarios (Baldini, 2012):[1]

- Voice communication as a priority
- Broadband services for imaging
- Back-to-back and network communication for first responders
- Dedicated channels for each emergency service and tactical-level links between supervisors of different services at the scene
- Mobile control units need to transmit data back to strategic-level command centres
- Communication links between arriving support units and other public safety services
- Communications between tactical-level command units, their out-of-area control centres and those at or around the incident
- Interrupted communication flows between operational units and control centres must be re-established with the least delay

[1] More extensive collections of communication scenarios have been compiled by PPDR user organisations. See for example the Critical Communications Broadband Group's "Application and Service Matrix" (2012), http://www.tandcca.com/Library/Documents/Broadband/CCBG%20RG%20application+service%20matrix%20(version13-9-2012).xls

In the winter of 2008/09, the CEPT surveyed Member States, user organisations and industry groups about radio applications used by PPDR now and needed in the future. Table 2.1 lists the applications cited in the respondents' answers, in descending order of "usage intensity". Five of the six most used applications are non-voice – mainly narrowband data but also video. The only voice application in the top group is handset-to-handset (Direct Mode) operation or DMO. However, in analysing the survey's results, CEPT's Frequency Management Project Team 38 point out that although data applications outnumber voice applications in the "most used" group, more voice traffic is transmitted than data.

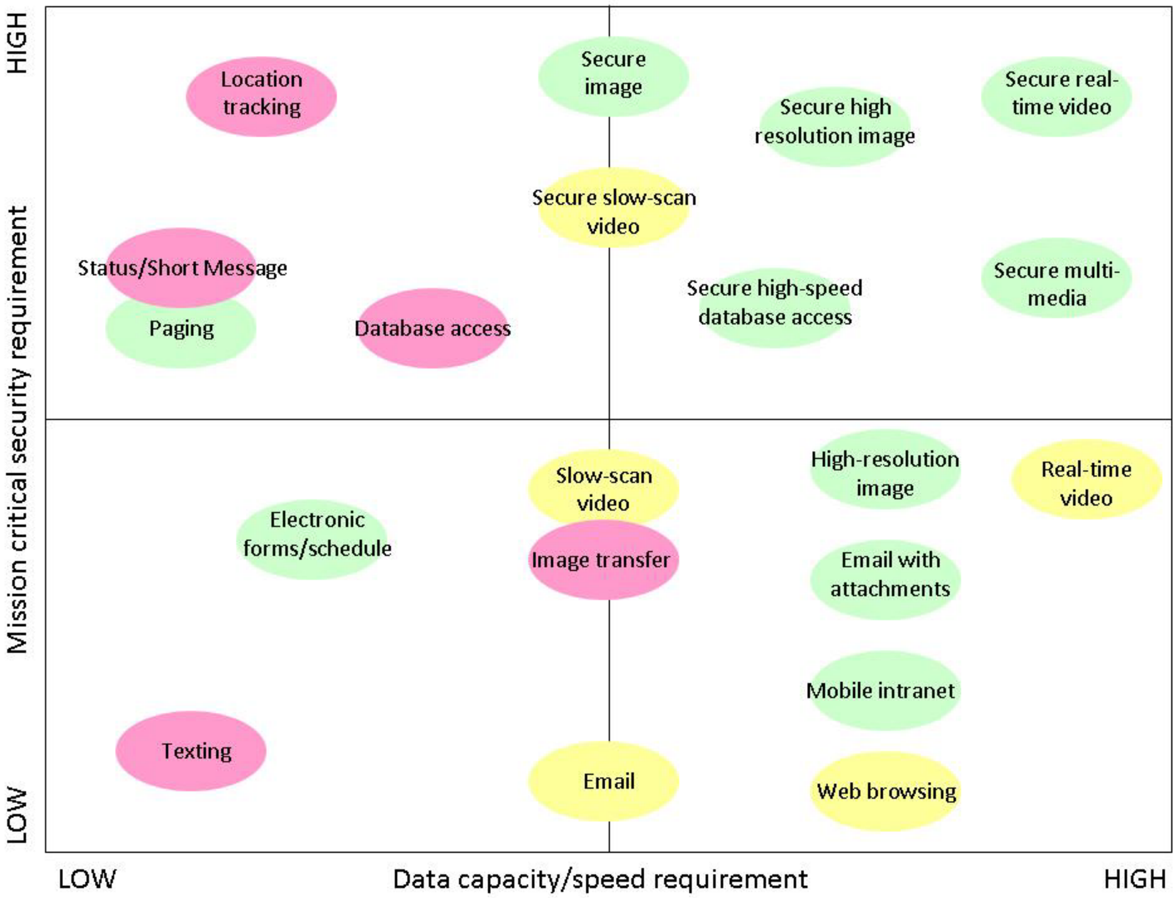
Table 2.1. Radio applications used by PPDR organisations in 2008/09

Intensity of use	Radio Applications
MOST USED (reported by 10-20 respondents)	Geo-location identification
	Database query/access
	Short data/message
	Status code messages[2]
	Direct mode communication
	Image/video/map/plan/photo transfer
MODERATE (reported by 5-9 respondents)	Group call
	Individual call
	Air-ground-air communications
	Command & control systems (dispatch)
	Data from ambulance to hospital
	Emergency call
LESS USED (reported by 1-4 respondents)	WAP query services
	Mobile Office (e-mail, internet)
	Calls to/from PSTN and PABX
	Tracking
	Priority call/access
	Trunked operations
	Fire applications
	Video call
	Paging
	Transportable links
	GPRS
	Fingerprint identification
	Police surveillance
	Vehicle licence plate identification
	Broadcast (all-call)
	IP data services for measuring sensors
	Satellite positioning
	Traffic enforcement system
	Fleet management
	Siren control
	RFID
	Disaster warning system
	Speed meter
	Video surveillance

Source: FM PT38 (2009)

[2] These are pre-coded text messages which replace required but routine voice updates (e.g., "On patrol" or "Arrived at scene").

Figure 2.1. PPDR data applications' bandwidth requirements versus mission criticality



Adapted from Byrnes, 2013

The relative bandwidth requirements and "criticality" of PPDR data application types were visualised in the chart above for a 2013 EU Presidency meeting. However, the colours are modified to correspond to the colours in Table 2.1, with pale green used for data types which have no equivalent in the table. Pale purple ovals show that the most frequently used radio applications in 2008/09 were relatively low bandwidth while high bandwidth applications were less often used (pale yellow). As there is no quantification, the size and placement of the coloured areas are only roughly indicative. A police perspective is emphasized but nevertheless it is a concise summary of the relationships among data application categories. Secure real-time video is the most demanding application.

Summary

From interviews and documentation, the functional requirements to support mission critical communications for PPDR services may be summarised as:

- **Constant availability** – PPDR effectiveness is undermined by network downtime, especially in emergencies. Networks should be available at least 99.99% of the time (i.e. less than 50 minutes per year of unplanned outages).
- **Ubiquitous coverage** – not just outdoors, but inside buildings (including large ferroconcrete structures such as shopping malls) and in tunnels (including subways).
- **Regionally harmonised spectrum** – to permit seamless operation of voice and broadband PPDR equipment across borders in Europe, including ad-hoc deployments of extra capacity coverage when and where needed, e.g. with vehicle-mounted communication hubs..

- **Differentiated priority classes** – so high priority communications are never blocked.
- **Support for dynamic talkgroups,** with the ability to change memberships at any time.
- **Automatic identification with authentication.**
- **Automatic location discovery and tracking** of personnel and response vehicles.
- **The ability to maintain connectivity** between any incident site and the relevant control room.
- **Fast call setup** (<200ms) and immediate access on demand: the **Push-to-talk** (PTT) function and **all-calls** (internal broadcasts).
- **Relay capabilities** for vehicles and personnel, with both handheld units and vehicles able to provide connectivity between handhelds and the command centre.
- **Support for Air-Ground-Air (AGA) communication** when and where needed.
- **Adequate quality of service** for both voice and data unaffected by location, with sufficient capacity for peak loads in times and places of crisis (not just a certain minimum signal strength).
- **The ability to roam onto commercial networks** when necessary.
- **Interworking between various PPDR services,** and increasingly, across borders.

Firefighting communication requirements

Fire sites tend to be harsh environments and portable devices that are not heat- and water-resistant may fail. It is also essential that handheld devices for firefighters can be used with gloves on**.** Sometimes there is a need for "intrinsically safe" radio equipment – equipment which cannot inadvertently produce a spark or heat that could ignite potentially explosive gases (ATEX Directive, 1994). Such devices cost more and are not needed at every fire so having just a few may be enough. They are particularly needed for industrial accidents and building evacuations owing to gas leaks.

Firefighters wearing self-contained breathing apparatus (SCBA) are constrained in their use of radios because the SCBA face piece reduces the intelligibility of speech:

> Speaking while wearing the SCBA means that the current work has to be paused, the radio has to be grasped, the speak button has to be located and pressed and respiration has to be adapted to talk clearly enough that the receiver can understand… In today's frontline firefighting practices, voice communication is the most important, and on many occasions the only tool for coordination… However, voice communication over radio is far from perfect and suffers from numerous problems. Communication frequently breaks down due to interferences, operating error while working with the SCBA (e.g., pressing the speak button on the radio by mistake) or insufficient maintenance (e.g., dead radio battery)…
>
> A conflict becomes apparent… the incident commander requires as much verbal information as possible to complete his task, but the firefighters who provide that information are hindered by the act of provision. This can even come to the point where queries by the incident commander are not answered because the current task is too demanding. The lack of response may be interpreted as an emergency by a commander waiting outside, which can in turn trigger a very complex process that involves [calling in] new resources and efforts. This in turn causes the superfluous deployment of personnel and vehicles, escalating the situation unnecessarily, incurring significant costs and risk… firefighters themselves recognize that the current tools limit their monitoring and therewith also their commanding…" (Scholz *et al.*, 2013)

Occupational safety is a top priority for fire fighters. The need to enter unfamiliar spaces that may contain imminent threats and multiple distractions, under conditions of poor visibility, is prompting the development of sensors to increase situational awareness for front-line personnel and those in charge of them. Sensors for location, air temperature, oxygen levels, heart rate, as well as infrared cameras to identify "hot spots" and ultra-wideband (UWB) devices for through-the-wall imaging and motion detection, are likely to proliferate in coming years. The radio bandwidth required by such sensors varies from a few kHz to many GHz in the case of UWB (UWB requires so much bandwidth that it must be deployed as a low-power "underlay" crossing through other allocations). All these sensors should be instantly readable so low-latency, real-time links are needed to support them. There is also a need for instant access to information about hazardous materials, downloadable building plans and maps, and 3D localisation technologies that work reliably indoors and out. The location of all fire fighters must be known at all times.

Summary

- **Voice is primary for fire communication.** Talk groups with DMO, push-to-talk, emergency alerts, and so on are essential for safety and success in tactical operations.
- **Speech intelligibility is a key issue,** made difficult by breathing apparatuses and noisy environments. (LTE's promise of higher audio fidelity is attractive though as yet unproven.)
- **Part-time volunteers are important to the fire services in large areas of Europe.** They require reliable wide-area call-ups using narrowband channels like paging and SMS. "Bring your own device" policies are not ideal but budget constraints make them expedient.
- **Securing fire communication channels through encryption is rarely necessary,** and indeed, allowing the public to monitor fire communications increases appreciation and understanding of their services to the community.
- **Route navigation assistance and location tracking are essential** for speedy dispatch. At the fire site, the location of all fire fighters must be known at all times.
- **In the near future, greater bandwidth for low-latency data transmissions will be needed** to support the image reports and remote control of scouting devices, infrared viewers, video and other sensors including UWB. Ready access to archives of building plans and information about hazardous materials represent new wide-area broadband requirements.
- **Lower frequency radio bands, even into the VHF region, provide better signal penetration** into buildings, so they are preferred for fire communications.
- **Handsets must be usable with gloves** and should be certified IEC IP67 resistant to dust and water. Intrinsically safe radio equipment is needed when there is a risk of accidentally igniting explosive gases in the atmosphere. Off-the-shelf consumer electronics are not intrinsically safe.

Emergency Medical Services' communication requirements

For Emergency Medical Services (EMS), radio links to patient delivery destinations and off-site sources of medical expertise are more important than links within the incident site, so reliable wide area access is more important than DMO. Communications security is needed mainly to protect information about patients' health condition and medical records since EMS workers rarely face the kind of threats that police encounter.

High-resolution medical imagery is increasingly important for accurate diagnosis and rapid treatment. This is a broadband data application that is not well supported today by TETRA. Broadband greatly expands options for "guided" handling of cases in the field. It also enhances communication between the patient pickup site and hospital, to prepare the medical staff in the period when lasting damage to health might be avoided. Our analysis suggests that EMS is the sector where expanded use of broadband would have the most positive socioeconomic impact (Lerner, 2012). Section 4.7 below attempts to quantify examples of the benefits of mobile broadband for emergency medicine.

But as shown in Appendix A, EMS teams do more scheduled (non-emergency) patient transports than emergency rescues, and life threatening situations are rare even in rescues. Using urgency and imminent threat to life as criteria, one might conclude that a minority of their communications are mission critical. However, any routine transport can enter a life-threatening phase without warning. So as with police and fire services, EMS teams require on-demand access to mission critical channels wherever and whenever they are judged necessary.

Other services

Even more than police, fire and EMS, search and rescue (SAR), crisis management and disaster response services are characterised by low demand for spectrum when help is not needed, punctuated by urgent demand and high spikes in traffic when it is. So this group of services frames the challenge, with special clarity, of having access to enough spectrum and appropriate infrastructure even though it is only occasionally needed.

Search and Rescue communication requirements

Disasters can occur anywhere and often affect large numbers of people. Search and rescue missions, on the other hand, might be organised to find just one person and they usually occur in less populated areas or difficult settings (caves, mountains, oceans, and so on). Commercial cellular or PMR repeater coverage may be poor or unavailable in such places, so ad hoc wireless networks are often needed. Airborne relays can help. Otherwise it is desirable for portable radios to have DMO capability and long signal ranges. That implies access to low frequency bands (all international SAR and distress calling channels are below 243 MHz, except for body-worn location beacons). Satellite solutions are attractive, too, and considerable bandwidth has been allocated recently to mobile satellite services, particularly for broadband, raising hopes that service costs will come down. Except for GPS and map-sharing, rescue missions rely on voice communication on open shared channels. But military rescues often occur in hostile environments so highly secure (even undetectable) channels are needed in that context.

Helicopters are prominent in SAR work because of their ability to fly at slow speed and low altitude, to lift the injured or drop supplies, or take off and land without a runway. But drones (UAVs) are likely to be used increasingly, too. Air-ground-air (AGA) communication is thus essential for SAR. If MNOs want to support emergency response activities, the decisive test is whether they can support AGA.[3] Note that there have been proposals in the USA to forbid transmissions on cellular frequencies by UAVs because of the risk of interference to terrestrial networks.[4]

Emergency Management and Disaster Response communication requirements

A simple timeline helps clarify the roles played by electronic communication networks in disasters. Once the roles are understood it becomes possible to identify functional requirements:

- **Before disaster strikes,** detection and early warning systems are needed.
- **During disasters,** public alert, mitigation, rescue, safety confirmation and evacuation assistance systems are needed.

---

[3] ETSI's designer guide for AGA (2011) notes that for "a cellular network providing a land-mobile radio service… significant design changes have to be implemented to service the requirements for effective AGA use… It is strongly recommended that antennas used for terrestrial radio cells are not shared with AGA sites [and] spectrum for AGA use is reserved solely for AGA…" See Appendix A for further discussion.

[4] Marcus, M. (2014) "Drones and Spectrum", *Spectrum Talk,* 14 August, http://www.marcus-spectrum.com/Blog/files/drones814.html

- **After disasters,** medical communication support for treatment of the injured and traumatised is needed, as are interim systems to help restore damaged infrastructure and re-establish contacts among family members, friends and neighbours. Ways to temporarily exploit and re-purpose communication capabilities that have survived are also useful.

Design principles for disaster communications using voice messaging and digital signs, portable communication hubs, smartphone apps to direct people to evacuation routes and refugee centres, and so on, are summarised in ITU-T's "Requirements for Disaster Relief System" (Technical Report FG-DR&NRR, 2014).[5]

Loss of electrical power is one of the most disruptive byproducts of a disaster, often cascading into the breakdown of other services needed for normal life. Cellular networks in particular can be impaired by power cuts even when not damaged by the disaster itself. So restoring the flow of electricity must be a top priority in disaster recovery plans and effective provisions for temporary backup power in cellular networks should be in place before disaster strikes. This is discussed in Chapter 3.1.2.

Fear that network blocking by congestion will lead to system failure during a crisis is often cited as the most compelling reason for emergency responders not to rely on commercial cellular for their communication needs. The 2013 annual report on major communication network outages by the European Network and Information Security Agency (ENISA) found that: "Overload was the cause affecting by far most user connections, more than 9 million connections on average per incident" (Dekker, Karsberg and Lakka, 2013, p. 15). So apparently this fear is well founded and must be addressed if mobile network operators are to win PPDR clients.

2.2.2 Utility communication requirements

The Electricity Transmission Grid and the European Gas Transmission Network are designated as "critical infrastructures of a European dimension" because a failure in one part of the network can propagate to other areas, potentially involving several countries. Even though numerous firms own different parts of these infrastructures and national borders often delineate the extent of ownership, in practice electricity and gas are "networks without national boundaries" (SWD[2013] 318 final).

Utility industry sources say their main functional communication requirements are:

- **Teleprotection** – safeguarding infrastructure and isolating sections of the network during fault conditions whilst maintaining service in unaffected parts of the network.
- **Data monitoring** via SCADA (Supervisory, Control And Data Acquisition) systems that continuously monitor networks so their current status is known.
- **Automation** – systems to autonomously restore service after an interruption or an unplanned situation.
- **Security** – systems to ensure the safety and security of plant.
- **Voice services** – to communicate with staff maintaining the network and responding to emergencies, whenever required, wherever they are.
- **Metering** – collecting data from smart meters and communicating with them for various reasons, such as demand management and to implement tariff changes.

---

[5] http://www.itu.int/en/ITU-T/focusgroups/drnrr/Documents/fg-drnrr-tech-rep-2014-5-DR_requirement.pdf

- **Connectivity** – telecommunication networks to interconnect the above services in a reliable and resilient manner under all conditions.

Other operational requirements include:

- **Coverage of all populated areas with points of presence throughout the service territory** and specific links to remote areas where essential infrastructures and supply sources are located (reservoirs, gas and oil storage tank farms, hydroelectric plants, and so on).
- **Costs must be low** as large numbers of terminals frequently transmit short bursts of data.
- **Continuity of service is vital,** and price stability over a 15-year period is desirable as that is a smart meter's lifespan. The quest for price stability favours the utility owning and operating the network, or sharing ownership with other utilities. Commercial cellular networks are seen as always wanting price increases (apparently they are unwilling to sign fixed price contracts for longer than five years).
- Owing to the cost of TETRA and the commercial cellular networks' lower level of resilience, **utilities want network separation,** to avoid having their operational communications disrupted or blocked by other users in a crisis. The high impact of major utility supply failures on the economy makes this a decisive issue even if overloading is rare.

What is not a utility requirement is high definition video or high bandwidth data communications, unless the utility itself offers the public broadband service. Most operational communications require very low data rates – between 10 and 64 kbps – but wide geographic coverage and "exacting availability, latency, jitter and synchronous requirements" (Grilli, 2013). Video is only needed for security monitoring of remote sites and even then most utilities consider 256 kbps sufficient for slowscan CCTV. (A data rate of 512 kbps appears just once on the requirements list in Appendix B, to enable field staff to access centrally stored real-time data to support their work at remote sites.)

In Section 2.3.2 below we discuss the rapid spread of portable data devices (laptops, tablets and smartphones) among utility employees. These require broadband connectivity, provided either by commercial cellular networks or through Wi-Fi hotspots. Such devices are increasingly used to interact with geographical information systems (GIS) and mapping applications, for asset management, damage reports, customer service, and so on. Broadband supports work outside the office – a convenience for routine operations and essential during emergencies.

Electricity communication requirements

Electricity distribution leads the utility sector in use of radio. Constant coverage of the customer base is needed but at comparatively low data rates – typically 9.6 kbps, although 64 kbps could be specified for equipment availability reasons and to allow for future developments.

Parts of a European Utilities Telecommunications Council (EUTC) "needs analysis" spreadsheet are reproduced in Appendix B. It shows that radio for teleprotection is distribution management's highest priority category. Very fast response times are needed to shield the network from the spread of failure conditions. Network surveillance, alerting and control responses demand <5 ms latency – that is to say, a detect/respond cycle of no more than 10 ms, to protect the expensive generators upstream. Supplying such speedy links would be a severe test of any commercial cellular network.

Europe is embarking on a massive deployment of smart meters for both load management and to deal with the decentralisation of generation capacity. GPRS has been used as one of the main connectivity options for smart meters, but most recent plans favour powerline communication (PLC). If GPRS is used in future it will be mainly to connect data concentrators at substations with processing centres.

Gas communication requirements

Natural gas is explosive and can cause death by suffocation. That means leaks must be detected and fixed quickly. Failing that, people must be evacuated from the area. Radio for dispatching and coordinating repair crews is thus essential and has been for decades, so gas utilities all have PMR networks, many of them analogue. Increasingly, however, utility field workers also carry portable data devices with professional applications installed. Analogue PMR networks cannot support these, so typically contracts are signed with one or more cellular network operators or satellite services for data connectivity, usually with roaming arrangements. Cost-benefit analysis to support smart meter deployment decisions has shown that large scale deployments of smart gas meters in private residences is generally not cost effective although for large customers it can be.

Water communication requirements

The water supply and sewage treatment industries lack electricity's need for immediacy. Moreover, buried infrastructure limits the use of radio. But because of the remoteness of many water assets from end-users, the industry's primary concern is maintaining reliable, long-distance communication links at low cost and radio is usually the least-cost option. Water utility communication typically involves sporadic small data bursts (as little as 10 bytes at 100 bps) coming from thousands of sensors in a large service area. Because of the large number of sensors, the cost of communication per sensor must be very low. That is in fact the main requirement. Cost concerns also inhibit the spread of "smart" water meters. Many EU Member States are starting to think about very large-scale water projects to deal with flooding, drought, climate change and the risk of rising sea levels. If these are implemented, much more use of radio will be needed for wide area sensor and remote activation networks.

Summary

- **Electricity generation and distribution are the utility sector's primary users of radio**.
- **Utilities use radio mainly for the routine but business critical demands of managing their distribution networks and supply chains. Repairs and monitoring are typical tasks.** But when they are in disruption recovery mode, radio use must be considered "mission critical" because of the potential scale of the economic impact.
- **Utilities require low data volumes at quite low transfer rates** although broadband is an emerging requirement for fieldworkers.
- **Tablets, laptops and smartphones are increasingly used by field staff** in many phases of utility work, including fleet management, damage assessment, customer relations, fault mapping and diagnosis. Such devices cannot be supported by the legacy analogue networks that are still in wide use, so utilities sign service and roaming contracts with the MNOs, preferably with long durations for price stability.
- Even though utilities are turning to MNOs to support field workers, **they still prefer to own dedicated communication networks** for distribution management operations because service disruptions generate legal liabilities.
- The use of GPRS to support smart meter deployments is in some sense a test of collaboration with the cellular industry. Utilities with public telecom or internet access subsidiaries have a different perception of bandwidth investments than utilities that are "pure plays".

- **Utilities do not need most of the PPDR-specific features sought from LTE** even though their repair crews work in teams. Thus, they are not likely to find dedicated private LTE networks implementing such features attractive.
- **Everyday teleprotection for electric utilities requires continuity of service with what commercial cellular operators would consider extreme even unattainable reliability** (99.999% availability) and consistently low latency (<5ms). For high voltage teleprotection, only dedicated fixed line networks can achieve this level of performance.
- **LPG gas depots, high-voltage electricity lines and nuclear power plants (along with their fuel/waste cycle) are critical infrastructures**, so keeping them secure is a critical mission.
- **Gas and water utilities have similar but limited uses for radio.** Water companies require very low cost sensors and metering up to the national level, mainly for pressure monitoring and leak detection. Gas networks require equipment that is intrinsically safe in explosive atmospheres, with high availability even for buried nodes.
- **National differences in market structure and business operation will make it hard for Europe's utility industries to find a single satisfactory answer to their wireless voice and data needs**. Given the slow evolution of utility infrastructures, convergence will not come quickly, if at all. For that reason, it is not likely that most utilities would agree to network sharing arrangements with PPDR, even while recognising the need for interoperability. However, network sharing between elements of the transportation and utility sectors might work, as might network sharing just among utilities.

2.2.3 Railway and Intelligent Transport Services communication requirements

The transport sector includes land, water and air. However the scope of this study is limited to land and thus to road and rail transport.

Road transport communication requirements

The Commission's Urban ITS Experts Group compiled a list of today's most widely deployed Intelligent Transport Systems (2013):

- **Traffic signals:** sensors, microprocessors and network interaction are transforming the humble but ubiquitous traffic light into a key component of any urban traffic management strategy, regulating the movement of vehicles, perhaps with the option of prioritising certain vehicle classes (eg police cars, fire engines, ambulances, buses).
- **GPS navigation** is so popular that many people already consider it essential.
- **Vehicle tracking by satellite** is used by freight transport operators for fleet management.
- **Real Time Passenger Information** helps mass transportation operators manage their schedules and provides passengers with information about when their bus or train will arrive (increasingly such information is sent automatically to portable devices).
- **Vehicle location data** can be obtained in various ways, including roadside sensors, probe vehicles and by tracking the signals of mobile phones carried by drivers and passengers.
- **Closed-circuit Television (CCTV)** is widely used to monitor roadway situations in real time with video cameras linked to traffic control centres.

- **Automatic Vehicle License Number Reading** to monitor journey times, enforce speed limits, collect congestion zone fees, spot unregistered vehicles or uninsured drivers, and so on.
- **Vehicle detection systems** are primarily used for managing parking spaces.
- **Pollution sensors** support air quality control and can also be used to detect traffic congestion indirectly.
- **Variable message signs** deliver timely notices to drivers, advising them about problems and diversions ahead, speed limit changes, and so on.
- **Access control schemes** can support road use charging on highways, or selectively exclude delivery vehicles at certain times of day.

Most of these are narrowband, short-range or passive so they need very little bandwidth. Among broadband applications, the transmission of real-time video to monitoring and evaluation centres is common. Two applications generate most of the data:

- Roadside cameras for monitoring of traffic flow for early detection of accidents and delays, to enforce speed limits, lane access restrictions, and so on.
- Security cameras in public transport hubs, subways and buses to detect and monitor suspicious activity.

The eCall project (described in Appendix C.1)[6] directly involves the cellular industry in first responder activity. Its success could lead to other areas of cooperation – or identify the limits of commercial cellular as a platform and partner.

In the future, driverless vehicles may require robust, secure and ubiquitous networks but it is not yet clear if that means a publicly owned or dedicated infrastructure.

Railway communication requirements

The European Integrated Railway Radio Enhanced Network System Requirements Specification[7] describes the rail industry's unique communication needs:

1. The network must recognise different priority and pre-emption rights.
2. All mobile equipment (except for data modems) must be able to broadcast messages from train controllers and from other trains.
3. The network must be able to assign "functional numbers" to mobile equipment so that a call to a specific train is routed automatically to the locomotive or the train's driver. (When a driver moves to a different train, the number used to reach them also changes even if they use the same radio.) Similarly, even though the controller changes with train location, the driver must reach the right person whenever the "controller" button is pressed. Finally, the network should be able to set up a group call to all train drivers in a certain area.
4. A "railway emergency call" is a group call with fast setup and warning tone to let drivers, controllers and others know of a danger that requires all trains in a certain area to reduce speed and be prepared to stop.

---

[6] http://ec.europa.eu/digital-agenda/en/ecall-time-saved-lives-saved
[7] http://www.era.europa.eu/Document-Register/Documents/Set-1-and-2-Index033-EIRENE%20SRS%20v1530.pdf

5. On trains with more than one locomotive, it should be possible to set up a permanent radio link between the locomotives.
6. Handovers from one trackside base station to another should occur within 300 ms.
7. Many functions are activated by dialling pre-set numbers. In this way, an authorised caller can connect to the train's public address or intercom system, trigger pre-recorded messages for passengers, call the conductors, the catering staff, the security chief, and so on.
8. A special "shunting mode" is used when train wagons decouple from a train and either move to a side track or to another train. In this mode the "shunting leader" can reassign functional numbers, change talk group memberships, declare a "shunting emergency", and so on.

Those are some of the current EIRENE requirements. However, the UIC Future Railway Mobile Communication System project is looking at future requirements. These must also be taken into account when considering the suitability of commercial networks for mission critical railway services.

Summary

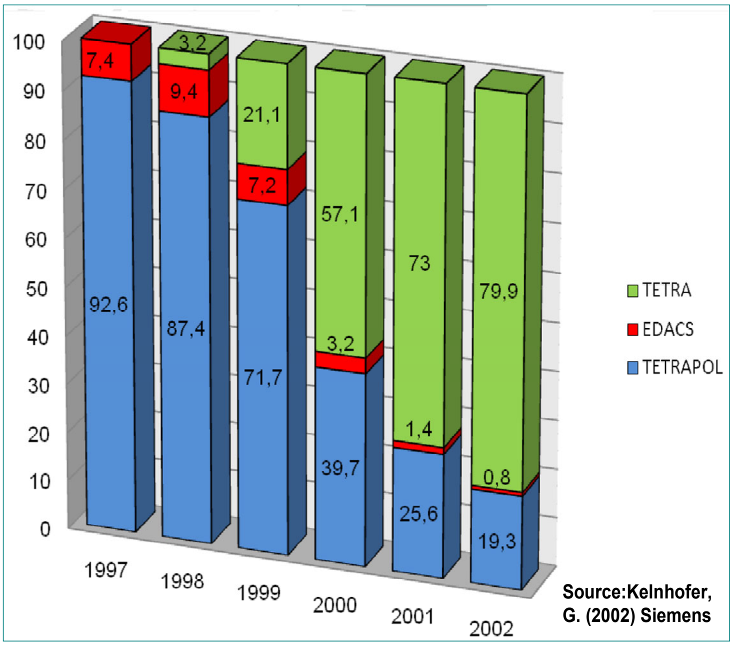
- **The diversity of ITS applications** is greater than the diversity of PPDR and utility applications, and yet most ITS applications are still "on the horizon" with uncertain spectrum requirements. Cooperative movements of large numbers of self-driving vehicles, for example, could require substantial radio bandwidth, as well as high availability and security.
- **Many current ITS applications are based on narrowband data**; GPRS is often an appropriate medium.
- For ITS applications that are local (e.g. vehicle to roadside, vehicle to approaching vehicle) cellular network infrastructure is unnecessary.
- **The only current ITS application requiring broadband is the delivery of multiple video streams** to traffic monitoring centres and for security in public transport.
- **The eCall project is an important test of "first responder cellular services"**. If successful it could evolve into a broader framework.
- **Railways need broadband mainly to supply passengers with information and internet access. It is not needed for the "mission critical" activity of train control**. In fact, it can be argued that train control and internet access must be kept separate to prevent remote "hijackings" and cyber attacks on rail safety systems.
- **Railways need secure talkgroup services** like those of first responders. DMO has not been used but it could be handy to have.
- **The reliability of data links to "radio block centres" is a primary consideration** because in ETCS Level 2 (explained below) loss of this connection stops train movement.
- **Many railway-specific communication requirements could probably be implemented as "apps" on top of any sufficiently reliable radio bearer.**
- **Railways would be content to keep using GSM-R for another 30 years** but manufacturer support could end sooner, possibly even before major deployments are finished.
- **GSM was presented to railways as a "future-proof" technology,** its huge popular base guaranteeing irreplaceability. It was also claimed that mass production of GSM components would mean lower prices for GSM-R equipment. Neither claim proved true, raising questions about the similar promotion of LTE for first responders.

2.3 Characteristics of wireless equipment and networks in the three sectors

2.3.1 Public Protection and Disaster Relief

In the 1980s, to promote inter-operability, ETSI started developing an open digital mobile radio standards suite for public safety and emergency services. Progress was slow so Matra of France split off to follow a faster track in order to respond to a ministerial request for a new digital radio network for the national gendarmerie. Matra won that tender with their new TETRAPOL system and RUBIS, launched in 1988, became the world's first nationwide digital PMR network. Matra reinforced their first-mover advantage by releasing descriptions of TETRAPOL's interfaces as open standards so other firms could make compatible equipment. In the 1990s TETRAPOL dominated Europe's digital PMR/PAMR market (see Figure 2.2).[8]

Figure 2.2. Digital PMR market shares in Europe for TETRA, EDACS and TETRAPOL, 1997-2002



Source: Kelnhofer, 2002.

But ETSI's standards development work continued. The Schengen Convention, meanwhile, promoted interoperability from a different angle: it directed signatories to consider "coordinating their programmes for the procurement of communications equipment, with a view to installing standardised and compatible communications systems" to facilitate cross-border cooperation among law enforcement and customs officials.[9] The Schengen Executive Committee asked ETSI if they had a standard which would meet their needs and, by 1995, ETSI could finally say yes: TETRA. Matra tried to get ETSI to endorse TETRAPOL, too, but it is ETSI policy not to endorse rival standards in the same market. Nevertheless, the Schengen Committee recognised TETRAPOL as an option, if only because it was already more widely deployed than TETRA.

After the Schengen Convention came into force the problem of TETRA/TETRAPOL interworking had to be confronted. The names of the standards may be similar but they are incompatible, as explained in Appendix A. Most countries realised that problems could be avoided if they adopted the same standard as their neighbours. ETSI's endorsement of TETRA – and not TETRAPOL – had a major impact. Countries that had not yet planned national public safety networks favoured TETRA and TETRAPOL's European market share shrank rapidly as Figure 2.2 shows.

---

[8] Chart from Kelnhofer, G. (2002) "Market Analysis for Professional Mobile Radio (PMR) and Public Access Mobile Radio (PAMR)", Siemens AG Österreich, reproduced in Hana, I. (2009) *Digitální radiokomunikační systémy: Tetrapol a Tetra,* Technická univerzita Ostrava (master's thesis), http://www.hanovi.cz/_media/ivos/diplomovap.pdf

[9] Quoted from Article 44 of the Schengen Convention.

Even though the build-out of big projects in Europe is subsiding now, the global TETRA market still grows with more than 250 governmental systems now operating and more than four million portable/mobile terminals likely to be in use by 2017. The infrastructure market is expected to expand 7-8% in 2014, fuelled mainly by Asia's public transport sector. TETRA sales are also growing in North America, now that the FCC allows the technology to be used there (not for public safety, however, to prevent interoperability problems with the favoured P25 standard). Utilities and public transport are TETRA's main markets in the USA. Global market segmentation is shown below.

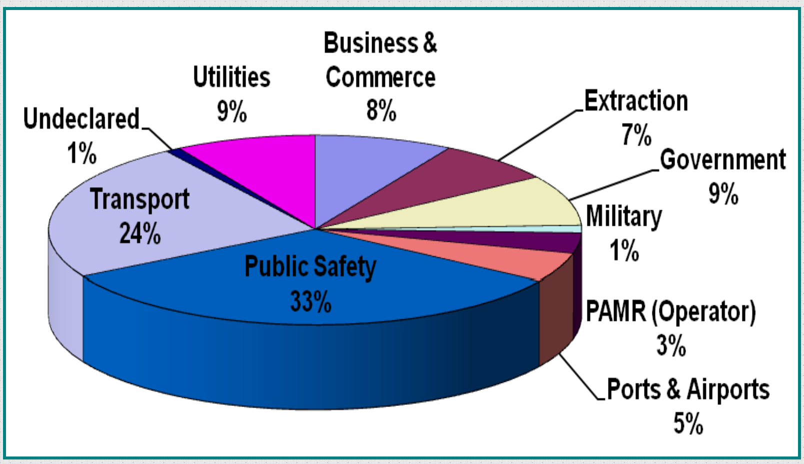
Estimates from publicly available sources indicate that EU Member States plus Norway have spent over €14.6 billion deploying TETRA and TETRAPOL networks for PPDR, plus almost €4 billion on mobile and portable terminals, and they spend an additional €1.35 billion each year operating these networks (possibly a low estimate). About 23,450 base stations now serve over 1.5 million users in Europe, for an average of 64 users per base station. However, since there are almost five million police, fire, EMS and rescue workers, there must be a great deal of equipment sharing (3 shifts in 24 hours) or continuing use of other mobile networks.

Large public safety networks based on TETRAPOL are still found in France, Spain, Slovakia and Switzerland, along with smaller networks in the Czech Republic and Romania. Latvia uses ASTRO25. Greece's TETRA network for PPDR, built for the Athens Olympics, had limited geographic coverage so as an austerity measure the government decided the police should go back to using their pre-TETRA radio system on 1 August 2014.[10] The UK is likewise planning early migration from TETRA to LTE. TETRA buildouts in Cyprus and Malta have not yet advanced. Italy's deployment halted in 2012 because of budget cuts, with only a quarter of the country covered, but build-out resumed this year. The other EU Member States all use TETRA for PPDR, though deployments are still unfinished in Germany, Italy, Luxembourg, Norway, Poland and Slovenia. In some cases, completion of the network was delayed by a decision to upgrade to TETRA Release 2 while Release 1 was still being deployed. See our individual country profiles in Appendix A for more details.

Even though the Schengen Convention focused on police cooperation across borders, the problems caused by first responders using different radio systems within a country were well known. So most Member States wanted their new security networks to be a common solution for all first responders. Thus, most governmental TETRA networks are used by police, border guards and customs officials, but also by rescue services, EMS teams, firefighters and military units with responsibilities for maintaining public order. In some countries it is possible for private organisations that work closely with public safety to subscribe as well.

However, TETRA and TETRAPOL developed before digital cameras became

Figure 2.3. Sectoral distribution of TETRA contracts in 2011



Source: Pasquali, 2011.

[10] Σουλιωτης, Γ. (2014) "Αγορά μη επανδρωμένων αεροσκαφών από ΕΛ.ΑΣ", 22 June, http://www.kathimerini.gr/772876/article/epikairothta/ellada/agora-mh-epandrwmenwn-aeroskafwn-apo-elas

so small and easy to use and before the smartphone showed how handy and versatile data terminals could be. As a result, support for data communication was limited. Intended mainly for the delivery of pre-coded status updates and short SMS-style text messages, the maximum data transfer speeds were comparable to dial-up modems from the 1980s. Realising that this was a potentially fatal weakness, the ETSI Board in 2005 mandated the development of TETRA Release 2, adding higher bandwidth data slots which could be integrated with existing TETRA installations in the same frequency bands. Called the TETRA Enhanced Data Service (TEDS), new modulation options were introduced for wider radio channels to support data traffic rates of up to 500 kbps. Equipment supporting TEDS entered the market in 2008-09. Release 2 proved so compatible with Release 1 equipment that vendors were able to offer their customers "TEDS ready" models requiring only a software upgrade. That makes it hard to determine how many currently deployed base stations are actually TEDS capable. Table 2.2 shows TEDS data throughputs in channels of different widths:

Table 2.2. Predicted data throughput (kbps) for various TEDS channel bandwidths

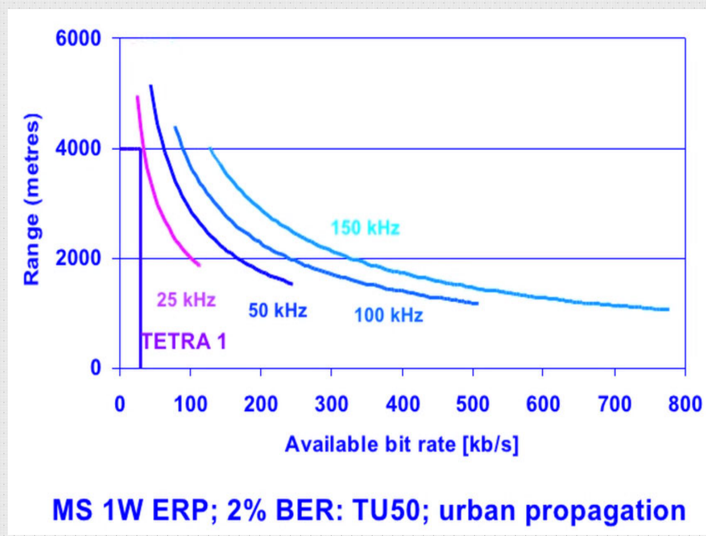
Throughput (kbps)	Channel bandwidth			
	25 kHz	50 kHz	100 kHz	150 kHz
Uplink	15 – 58	24 - 141	49 - 293	77 - 459
Downlink	15 -60	26 - 154	55 - 329	86 - 518

Source: ETSI, 2010b.

Norway's Nødnett was the first to start upgrading their network with TEDS. "Tests so far show file transfer rates of 80kb/s + on the uplink and 90kb/s + on the downlink over 64 QAM modulation operating in a 50kHz channel".[11] Recently they demonstrated the streaming of live video from a mobile terminal to a control centre and vice versa, as well as handoffs of live video from one base station to another.[12] However, as ETSI noted, "Whilst TEDS has been demonstrated streaming video it has been only low resolution and on an unloaded cell" (TR 102 022-1, 2012). Without major upgrades throughout the network, it will be a challenge for TETRA to support the data bandwidths that first responders now say are needed for their work.

One reason why broadband support is costly is the trade-off between signal range and throughput. This is an important issue affecting LTE no less than TETRA: higher data throughput means reduced signal range when spectrally efficient modulations are used. This is shown for TETRA in Figure 2.4. In practice this means more base stations are required to achieve "blanket" coverage for high throughput networks. According to Dewaele, boosting data transfer rates from 28.8 to 473.6 kbps across an entire TETRA

Figure 2.4. Data throughput v signal range (TEDS)



Source: Dewaele, 2001.

[11] Atkinson, J. (2014) "Norway's enhanced TETRA network", *Wireless Magazine*, 20 May, http://www.wireless-mag.com/Features/29484/norway%E2%80%99s-enhanced--tetra-network.aspx
[12] "Motorola Solutions successfully trials live video on Norway's public safety network", Motorola press release (10 March 2014), http://newsroom.motorolasolutions.com/Content/Detail.aspx?ReleaseID=18783 &NewsAreaID=2

network would require a hundred-fold increase in the number of base stations.

Another reason for the high cost impact is the large amount of redundancy in PPDR networks: extra switches maintained in "stand-by" mode, extra transceivers at base stations in key locations; multiple backhaul paths to bypass link failures; batteries and generators to provide electricity when mains power is lost. Another form of redundancy is that TETRA base stations have overlapping coverage to ensure continuity of service if a base station fails. All this redundancy is intended to make the networks resilient, to promote availability and sustain PPDR services when other communication systems fail. For LTE to provide PPDR users with a similar level of network resilience, similar measures will be needed.

In addition to Service Level Agreements, many EU Member States have adopted policies and regulations to ensure that PPDR networks remain operational even when mains power is lost. Some examples are shown in Table 2.3.

Table 2.3. Minimum PPDR back up power requirements in selected Member States + Norway

Country	Minimum back-up power requirement	Minimum back-up power for prioritised base stations
Norway (~2100 base stations)	8 hours @ 85% of base stations	48 hours @ 15% of base stations
Sweden (~1800 base stations)	24 hours @ 52% of base stations	7 days @ 48% of the BS
Denmark (~500 base stations; however, power outages due to weather are rare because the distribution network is mostly underground)	4 hours at 72% of base stations	48 hours @ 28% of base stations equipped with hydrogen fuel cells. These cover almost all the country.
Finland (~1350 base stations)	6 hours @ all base stations	200 base stations are connected to generators
Germany (~4400 base stations)	2 hours	Prioritised parts of the network have more back-up
UK (~3500 base stations)	6 hours @ 60% of base stations	5-7 days @ 40% of base stations

Source: Lyngstøl, 2013; Carpentier, 2013

While all PPDR networks claim to have excellent availability records – and most certainly do – they are not perfect. Particularly during buildout, when not all parts of the network are in place, systems have not been thoroughly debugged and users have not yet become accustomed to the quirks and limitations of the network, problems can and do occur. (Note that TETRA buildouts can take 5-10 years.) The reliability of public cellular networks is discussed in Section 3.1.2. However, comparing the reliability of public cellular and dedicated PPDR networks will remain problematic until both are subject to the same public disclosure and outage reporting rules.

With so much already invested in TETRA networks, and with so much acceptance from such demanding users, one might wonder why plans for TETRA Release 3 were not formulated to add broadband and multimedia capabilities to an already well-established solution. There were in fact efforts to produce TETRA 3. It is beyond the scope of this study to explore why they have not yet succeeded, but suffice it to say that TETRA has other shortcomings, less obvious than the lack of broadband, which proved decisive when combined. However, they have less impact on the new markets TETRA is finding today – transport, utilities and private security – so TETRA continues to win new customers albeit at a slower pace. Steppler (2011) identified the main problems:

> The TETRA industry was not able to agree upon a reference architecture for the TETRA Switching and Management Infrastructure (SwMI). No reference points and no interfaces between network elements have been standardized which prohibited multi-vendor markets within nationwide infrastructures…
>
> No control room interface has been standardized. This is why all TETRA infrastructure manufacturers provide proprietary APIs for control rooms and the TETRA + Critical Communications Association does not test and certify the interoperability of control rooms, although control rooms are essential in daily PMR operations…

The incompleteness of key components of the standard led to the development of proprietary solutions which in turn produced supplier lock-in and thus higher prices for equipment as buyers had no choice but to adopt non-interoperable solutions and, once chosen, stick with them. Nineteen equipment vendors have joined a TETRA interoperability improvement process.

Similar problems have plagued TETRA's Inter-System Interface (ISI), which was supposed to enable something like roaming from one TETRA system to another. Because of the extra layers of security and authentication, and different procedures demanded by different countries and professions, the process in TETRA is more complicated than cellular roaming.[13] And while cellular roaming is lucrative, TETRA roaming is not. Since firms contributing resources to the development of TETRA standards did not foresee significant revenue coming from ISI, resources simply were not committed to reaching a definitive solution for that part of the system. A similar problem could affect the development of new LTE standards for first responders, where there are highly sought capabilities that may not produce revenue either for network operators or equipment vendors.

As support for mission critical LTE has grown among public safety organisations, the suppliers of TETRA and TETRAPOL equipment began experimenting with hybrid products designed to accommodate this option. In 2011 Alcatel demonstrated a TETRA client application running on a ruggedised LTE terminal. This enabled communication with other TETRA users through an LTE network, using LTE frequencies, with access to normal TETRA services. An agreement between Alcatel and Cassidian/EADS followed, for the development of an LTE broadband terminal operating on TETRA frequencies.[14] Then EADS and the French interior ministry demonstrated a dual-mode 400 MHz base station supporting both TETRAPOL and LTE.[15] Clearly there are many ways to get from point A to point B. The economics of these hybrid paths are considered in Chapter 4.

One currently available broadband option gets surprisingly little attention: WiMAX. In 2010 and 2011 the Romanian government built a 1300 base station mobile WiMAX network to add nationwide broadband to their Special Telecommunication Service's TETRA network for just over €20 million. The network's coverage is shown in Figure 2.5.[16] It is said to support 2286 "subscribers" although it is not clear what that means, since the TETRA network has 1243 "subscribers" using 55,000 terminals.

[13] Nødnett in Norway and Rakel in Sweden have been developing an ISI solution that they believe "could lead to a break-through for the implementation of ISI between other networks". They plan to start using it in 2015-2016 (Dinkom, private correspondence, 2014).

[14] Alcatel-Lucent (2011) "LTE mobile broadband enhances public safety with shared video and data", http://www3.alcatel-lucent.com/features/lte_mobile_broadband/

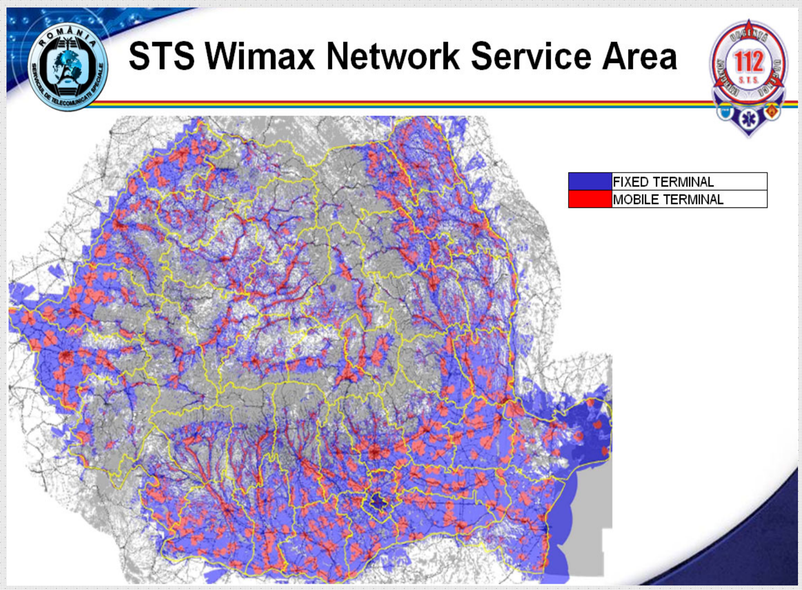
[15] EADS (2013) "Cassidian and the French Ministry of Interior demonstrate public safety mobile broadband", 2 April, http://www.cassidian.com/en_US/web/guest/public-safety-mobile-broadband

[16] "Airspan 4G solution deployed by STS Romania for nationwide mobile WiMAX network", Airspan press release (22 March 2011), https://www.airspan.com/2011/03/22/airspan-4g-solution-deployed-by-sts-romania-for-nationwide-mobile-wimax-network/

In any case, the IEEE 802.16e-2005 WiMAX network – Europe's largest – can relay live video, voice, text and other forms of broadband data concurrently through each base station sector.

Unfortunately, the belief that WiMAX will ultimately suffer the same fate as Sony's Betamax has resulted in a dearth of new portable terminal designs, so that even the recent drastic price cuts for base stations may not be enough to save the technology in Europe. WiMAX is clearly the most cost-effective solution for mission critical broadband even though it lacks the burgeoning ecosystem of promoters and suppliers that now surrounds LTE.

Figure 2.5. Coverage map of Romanian security services' WiMAX network



Source: Vasilca, 2012

2.3.2 Utilities

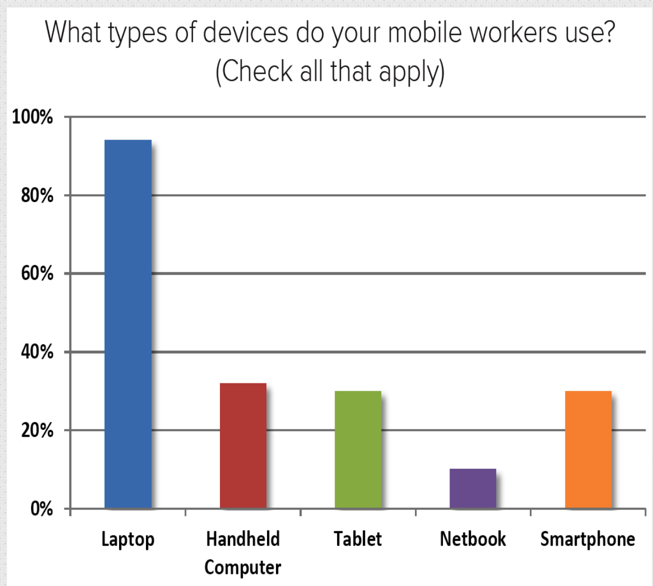
Utilities throughout the EU have a variety of radio networks in both the VHF and UHF bands, with national differences due mainly to spectrum allocation decisions made decades ago. (Older allocations often specified the technologies to be used in a particular band.) While specific channels are allocated for utility telemetry and remote meter reading, PMR spectrum is usually used for voice communication at 68-87.5 MHz, 146-174 MHz, 406.1-430 MHz or 440-470 MHz (Ferrús and Sallent, 2014). Utilities have long amortisation/depreciation cycles so many of their radio networks are over 20 or 30 years old. For network operations, utilities generally need radio channels of less than 20 kHz bandwidth, whether for data or voice. Trunked FM networks based on the MPT 1327 standard are still widely used to dispatch vehicles to customer premises to install, service or replace meters and to fix leaks and repair other faults in the distribution network. The equipment is inexpensive and easy to maintain yet digital control signals enable advanced features similar to TETRA and TETRAPOL (PTT, DMO, talkgroups, all-calls, and so on). Scanner owners report extensive use of such systems today in Germany, Netherlands, Poland and the UK, usually in the 420 MHz band – a band now being studied for possible future use by LTE.

TETRA is making modest inroads into Europe's utility sector. Hrvatska Elektro Privreda in Croatia led the way in 2001, followed by Dansk Olie og Naturgas A/S in Denmark. The Norwegian gas pipeline company Gassco is building a TETRA network for maintenance workers at its terminus in Northern Germany and TETRA also serves a large wind farm in the North Sea. Poland has decided that TETRA will replace the MPT 1327 network built by the national association of electricity distributors, because the manufacturer no longer supports it. But the €240 million price estimate for TETRA – without broadband – means the transition won't be rushed.[17]

Utilities are signing up for commercial cellular data contracts now that tablet PCs and laptops have shown they increase productivity. The USA is ahead of Europe in this regard so it may be instructive to consider a recent survey of mobile data use by utilities in North America. The survey covered all uses of mobile data, mission critical or otherwise, and all types of utilities, though most respondents were from the electricity subsector (NetMotion Wireless, 2013).

The survey found the use of portable data devices to be quite widespread and expanding to more utility worker categories. Seventy percent of the utilities reported that they equip their service technicians with portable data devices; 62% give them to meter technicians, 52% to line crews, 37% to digging or new construction crews, 12% to street light servicing crews and 10% to tree crews. Twenty-two percent of the utilities said that additional worker categories will get the devices soon – in particular, general managers and customer support staff. Figure 2.6 shows the types of devices used.

Figure 2.6. Portable data devices used by utility workers in North America



Source: NetMotion Wireless, 2013

All the utilities have service agreements with at least one commercial cellular operator, and because they operate across large areas, many have service and roaming agreements with several. Forty-five percent say their workers also access the corporate network using virtual private networks (VPN) via Wi-Fi, either through utility owned access points or public hotspots. In addition 15% have contracts with satellite companies because connectivity is sometimes needed where there is no Wi-Fi or cellular.

The most used mobile applications are (in descending order) GIS/mapping, mobile workforce management, asset management, customer relations management and fleet management. "About 30% of utilities employ in-house software developers that work closely with their field crews to understand their ongoing business requirements and write customized applications accordingly" (NetMotion Wireless, 2013). These applications support routine business activities but if the context shifts to, for example, recovery from storm damage, equipment failure or lost power, they become mission critical.

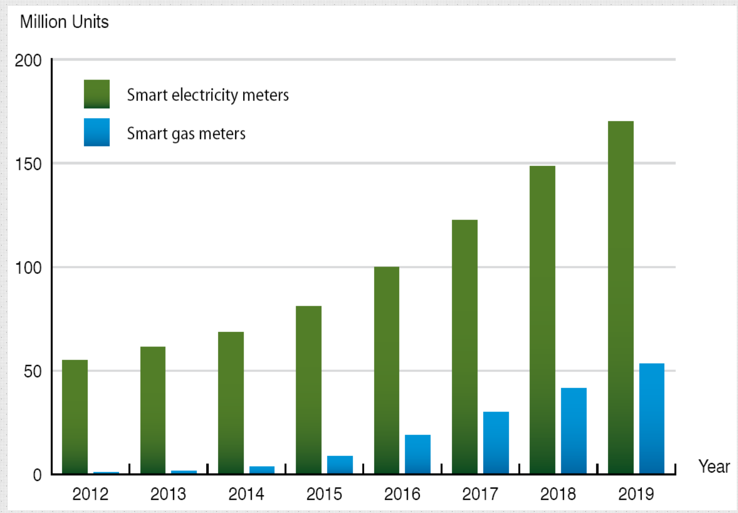
Electricity

A recent benchmarking report by Berg Insight (2013) for the European Commission provides insights into the current state of smart meter deployment in Europe. The target is conversion of 80% of metering points by 2020 for electricity; for gas the target is simply roll-out in a "reasonable" time

[17] "Energetyka wkrótce z systemem TETRA", *RadioTech.pl,* 13 August 2012, http://radiotech.pl/aktualnosci/z-kraju/161-energetyka-wkrotce-z-systemem-tetra.html

frame. Deployment obligations only arise from positive results produced by the cost-benefit analysis Member States were to complete in 2012.

Figure 2.7. Installed base of smart meters (electricity and gas) in the EU28+2, 2012-2019



Source: Berg Insight, 2013.

In Belgium, the Czech Republic, Germany, Latvia, Lithuania, Portugal and Slovakia the cost-benefit analysis produced negative or inconclusive results for electricity metering. However, Germany, Latvia and Slovakia found smart metering economically justified for smaller subsets of users so they plan limited roll-outs; the Czech Republic will reassess the situation in 2017. Belgium, Hungary, Lithuania and Portugal have put their deployment plans on hold and Bulgaria, Cyprus and Slovenia have either not finished their analysis or not announced their decisions.

Finland, Italy, Malta and Sweden have finished their deployments. All other Member States are planning or have started theirs. According to the European Commission, investment commitments of about €45 billion have been made to install almost 200 million electricity meters and 45 million gas meters by 2020 (COM[2014] 356 final). Nearly all the plans rely on power line communication (PLC), but 15 will also use GPRS. In addition, five countries report that they will use "radio" or "RF" links without specifying the technology or band. A country-by-country summary of the communication technologies is found in Appendix B.

GPRS gives commercial cellular network operators a toehold in smart metering, which could expand if smart grids develop from the metering networks. On the other hand, the demise of GSM could take GPRS with it unless LTE continues support through software emulation (as is likely).

Gas

Pipeline telemetry and the monitoring of pumps and distribution points in the gas distribution network use radio as a low cost solution. PMR systems are used for network maintenance and repair while some utilities turn to point-to-point microwave in fixed service allocations or licence free bands for their access point concentrators. Video surveillance of remote sites could drive bandwidth requirements higher in the future. This is especially important for Liquified Natural Gas terminal, storage depot and pumping plant security.

Cost benefit analysis showed that costs outweigh benefits in 12 Member States so large-scale deployments of smart gas meters are not expected in Belgium, Czech Republic, Denmark, Finland, Germany, Greece, Latvia, Portugal, Romania, Slovakia, Spain or Sweden. However, large roll-outs are expected in Austria, France, Ireland, Italy, Luxembourg, Netherlands and the UK. Neither Cyprus nor Malta has a gas network (COM[2014] 356 final).

Water

As with gas networks, video surveillance of remote sites may drive some higher bandwidth radio requirements in the future. This is important for maintaining the integrity of water supplies since drinking water is often stored as open lakes in unpopulated regions.

Radio is the least costly solution for monitoring tens of thousands of pumps, pressure meters and flow gauges. Sensors producing tens or hundreds of bits of data per second and reporting a few hundred bytes via ultra-narrowband (UNB) signals several times a day can use the licence exempt bands at 169, 422 or 870 MHz or long distance links below 50 MHz.

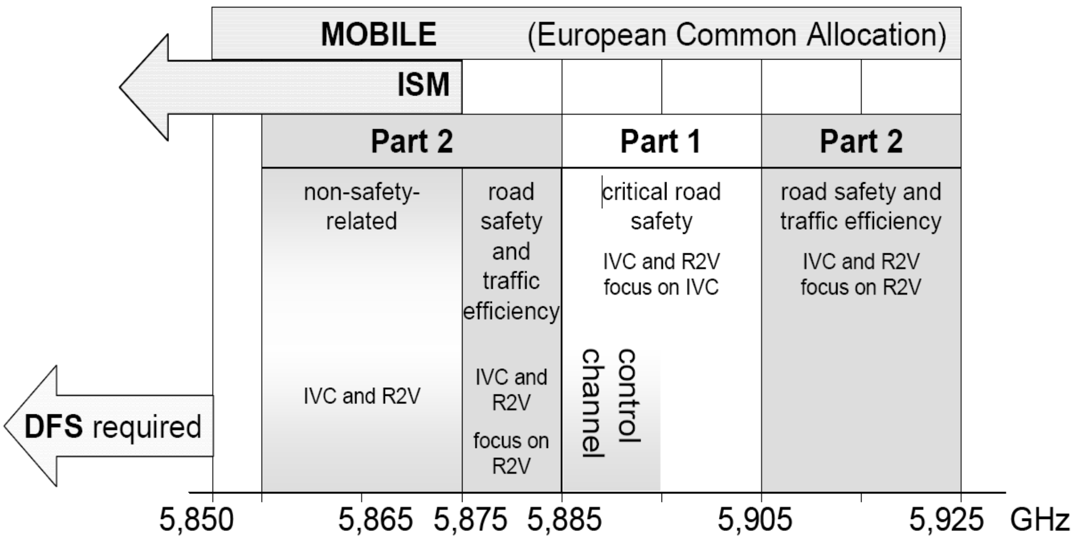
Remote meter reading is less common for water than for either electricity or gas, but it may be done for large customers using either UNB networks or legacy systems in the VHF range.

2.3.3 Intelligent Transport Services

Many of the ideas now referred to as Intelligent Transport Services (ITS) originated with the "Dedicated Road Infrastructure for Vehicle Safety in Europe" (DRIVE) programme in the 1980s. Some applications suggested by DRIVE required the use of radio frequencies so the ECC was asked to identify suitable frequency bands for them that could be made available throughout Europe. The bands identified were:

- 5.795-5.805 GHz for initial road-to-vehicle systems;
- 5.805-5.815 GHz, to be used on a national basis to meet the requirements of multi-lane road junctions;
- 63-64 GHz for vehicle-to-vehicle and road-to-vehicle systems; and
- 76-77 GHz for vehicular and infrastructure radar systems.

Figure 2.8. ITS band plan at 5.9 GHz



Source: CEPT Report 20, 2008.

The potential uses of 76-77 GHz were subsequently broadened to include vehicle speed measurement, vehicle counting, inter-vehicle range measurement, vehicle classification, traffic jam detection, lane occupation rate, wrong way driving detection, and so on.

Commission Decision 2008/671/EC harmonised use of the 5875-5905 MHz frequency band for safety-related ITS applications. These applications include cooperative systems based on vehicle-to-vehicle, vehicle-to-infrastructure and infra-structure-to-vehicle communication to increase the situational awareness of drivers (and their vehicles) about the traffic environment and to provide early warnings about the behaviour of other road users which could lead to hazardous conditions. To be effective, such communications must be fast and reliable, that is, not subject to interference. This allocation was considered a first step which, if successful, could be expanded by the addition of 5905-5925 MHz. At the time of the decision it was foreseen that these frequencies would be exploited rather quickly for vehicle-to-vehicle communication, but that it might take longer to work out appropriate authorisation and coordination schemes for infrastructure-to-vehicle and vehicle-to-infrastructure communications. However, V2V communication has been slow to develop in Europe and the CEPT is considering now whether to recommend WAS/RLANs use of these frequencies. Movement toward re-allocation seems to have given ITS developers an implicit "use it or lose it" message. The draft amended ECC Decision (08)01 recently adopted for public consultation by WG FM notes that:

> Cooperative ITS systems based on the ETSI ITS standards [for use in the 5875-5925 MHz band] will be deployed from 2015 onwards in vehicles with initial infrastructure installation appearing in the course of 2014. Major car manufacturers recently signed a memorandum of understanding to signal their intentions to provide cooperative ITS systems from 2015 on.[18]

See the case study of Japan's ITS Spot services in Section 5.6 for a hint of what might be coming.

Railways

GSM-R

The radio system devised for Europe's railways is based on GSM technology. Features have been added at the application level and exclusive frequencies have been allocated for GSM-R. But the technology is otherwise the same or similar to public 2G cellular. Indeed, since Member States can decide not to deploy GSM-R on existing railway lines that are lightly used or without international traffic, such routes increasingly rely on roaming arrangements with commercial cellular network operators for voice communication between control centres and trains.

The main difference between GSM and GSM-R networks is that the latter have a linear coverage pattern aligned with the tracks, instead of being arrayed to cover a wide area. Another difference is the role of data communication. The General Packet Radio Service (GPRS) was an afterthought in GSM, but in the future it will be crucial to the European Rail Traffic Management System (ERTMS).[19]

GSM-R has a harmonised allocation in Europe: mobile stations transmit at 876-880 MHz while base stations transmit at 921-925 MHz. Where additional GSM-R channels are needed, national regulators can authorise 873-876 MHz and 918-921 MHz, though these frequencies are shared with RFID and other short range devices. In some countries, military users have priority in the use of the supplemental

---

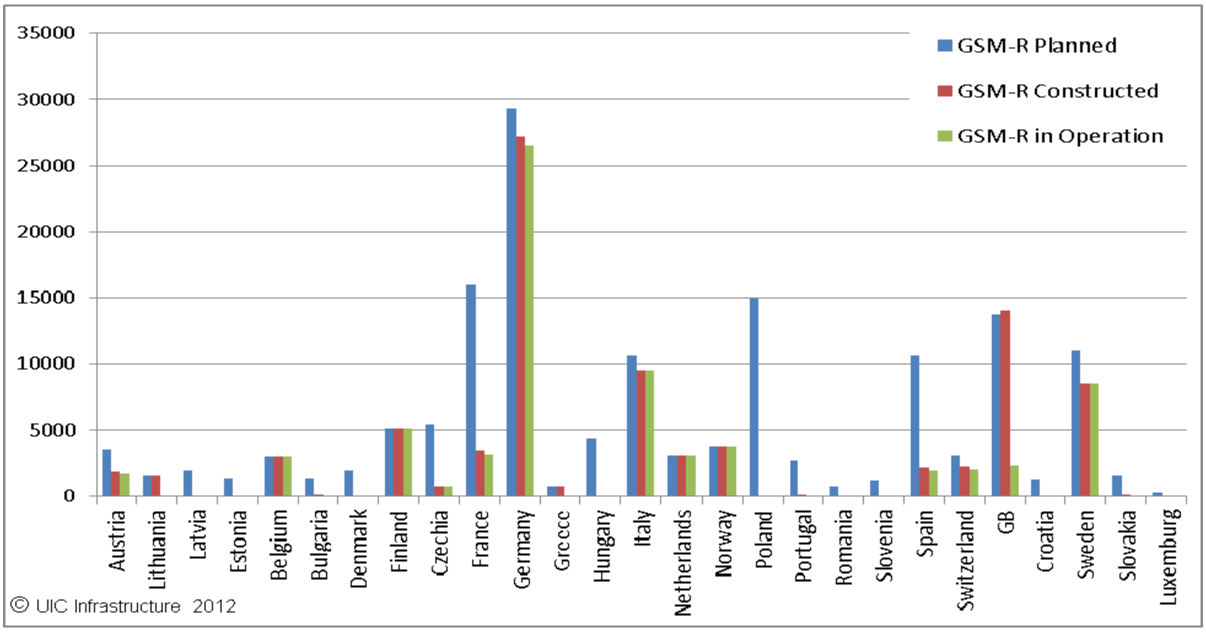
[18] WG FM (2014) "Draft amended ECC/DEC/(08)01: The harmonized use of the 5875-5925 MHz frequency band for Intelligent Transport Systems (ITS)", public consultation document, http://www.cept.org/files/1051/Tools%20and%20Services/Public%20Consultations/2014/Draft%20amended%20ECCRec(08)01.docx

[19] The decision to use narrowband data for train control was made before GPRS was added to the GSM specification. Consequently, ETCS today relies on data modems which utilise GSM-R voice circuits. Work is underway to migrate ETCS to GPRS and TCP/IP.

channels. For fall back, GSM-R equipment must also be capable of operating on standard commercial GSM frequencies (880-915 MHz and 925-960 MHz). GSM frequencies are now available to LTE, too, so there is a relatively short migration path from GSM-R to LTE if the railways want to take it – and if LTE gains the features needed by railways. On the other hand, because the GSM and GSM-R bands are adjacent, hundreds of incidents of public cellular interference into GSM-R have been reported.[20]

The following chart shows planned, constructed and actually operating GSM-R deployments in Europe. (Note that the numbers along the left edge of the chart represent km of track covered.)

Figure 2.9. GSM-R deployments: planned, constructed and operating



Source: SWD(2014) 48 final.

There are 220,172 km of railway lines in Europe. Eventually, 154,284 km will be covered by GSM-R. However, by mid-2013, GSM-R had been installed on 85,332 km and was operational on 70,211 km (Ilie, 2013, and SWD[2014]48 final). ETCS operates on just 4% of Europe's railway lines (see Table 2.5). Therefore the use of pre-GSM-R radio networks and older signalling systems for train control is still common and transition will be a long, slow process. Information about the mix of radio systems currently used by railways in the EU-28 can be found in Appendix C.

Table 2.5: Track km with ETCS in service

Country	Track km with ETCS in service	Country	Track km with ETCS in service
Austria	496	Latvia	0
Belgium	446	Lithuania	0
Bulgaria	387	Luxembourg	275
Croatia	0	Malta	0
Cyprus	0	Netherlands	365
Czech Republic	22	Norway	285
Denmark	0	Poland	310
Estonia	0	Portugal	0
Finland	50	Romania	311

[20] UIC (2011) "Interferences into GSM-R due to public mobile radio networks", presented at the 35th RSCom meeting, 23 March, https://circabc.europa.eu/sd/a/ff53dd07-3121-4b48-8724-d0aa478ec3f5/GSMR_Interferences_12 (for%20publication).pdf

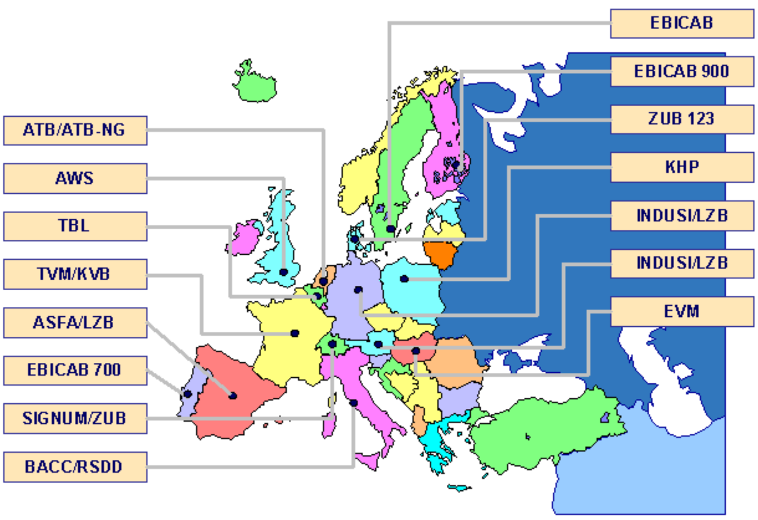
France	405
Germany	823
Hungary	280
Ireland	0
Italy	947
Slovakia	635
Slovenia	615
Spain	2112
Sweden	480
United Kingdom	218
TOTAL	**9 462**

Note that the process of migrating to ERTMS continues long after GSM-R is switched on. In Italy, for example, GSM-R roll-out ends this year but migrating to ETCS might take until 2026 (Rete Ferrovie Italiana, 2009). In Germany, Deutsche Bahn began deploying a backbone for GSM-R in 1999, but ETCS is not expected to become fully operational there until 2030.

ETCS

In 2009 the European Commission adopted an ERTMS deployment plan which set legally binding deadlines for implementing ETCS and GSM-R on key rail corridors (EC, 2009). Since not all tracks are or ever will be covered by GSM-R, ERTMS recognises four stages in the evolution of ETCS:

Figure 2.10. Europe's main pre-ETCS train control systems



Source: Faure, 2005

- At ETCS Level 0, trains are simply rolling stock without location or speed guidance.
- At ETCS Level 1, information is transmitted to trains by balises in the track, inductive loops or radio links. Line side signals are still required.
- At ETCS Level 2, data transmissions via GSM-R set the train's operating variables, principally the maximum speed and "movement authority". The difference between ETCS Level 1 and Level 2 is crucial because ETCS Level 2 eliminates the need for line side signalling.
- ETCS Level 3, which is not implemented yet, will eliminate the need for track based train positioning systems. It will implement a "moving block" concept (a "moving block" is a section of track which cannot be used by two trains at the same time). In Level 3 "integrity checking" will be done on the train, not by an external controller.

At ETCS Level 2, a radio data modem connects the train to its controller and if the connection is lost, the train loses "movement authority" and automatically stops. But trains, especially when travelling at high speed, have enormous momentum so they cannot stop immediately. (A high-speed train travels roughly 100 m in one second and it takes at least seven minutes for the train to come to a complete stop.) As a practical matter then, there is always a time-lag between the loss of radio contact with the controller, the loss of movement authority and the train stopping. This enables the train to keep moving if the loss of connectivity is relatively brief, which can happen if an interfering signal blocks the radio channel. As already noted, MNO networks interfere with GSM-R in certain places. This problem will worsen as GSM-R is implemented more widely and LTE begins replacing GSM at 900 MHz. Fortunately, only a few hundred meters of track are affected by any one cell site, so the train may pass out of the interference zone before it can stop. However, if it stops in the interference zone, the situation could become serious as it might be impossible for the signalling system to restore movement authority or for instructions to be sent verbally by radio to the driver.

TEN-T legislation approved by the European Parliament in November 2013 obliges Member States to put ERTMS into operation on their "core" rail networks by the end of 2030 and to deploy the communication infrastructure on their "extended" rail networks by the end of 2050 (European Parliament, 2013). The problem with this schedule is that manufacturer support for GSM-R could fade long before the last ERTMS projects are completed, jeopardising returns on some large investments and shortening the cost recovery period for all similar projects. The cellular industry wants to start retiring GSM in the next decade.

"As an industry we are happy with GSM-R and we want it to be around for another 30 years, but we are being forced to look at changing GSM-R because of the new public operator technologies context," explains Dan Mandoc, chairman of the railways' European Radio Implementation Group (Mandoc, 2013). According to SWD(2014) 48 final, "GSM-R will be supported by suppliers until at least 2028. Europe therefore needs to be prepared for an alternative solution by 2022… The new communication system(s) must be defined in 2018 and must be available for deployment by 2022 at the very latest and they must ensure co-existence with and manage migration from GSM-R."

Even if the GSM-R Industry Group continues supporting GSM-R after public GSM is retired, Mandoc fears that railways "could face a financial imperative towards network convergence as the costs of GSM-R support are expected to increase after the end of production [of GSM equipment for the public] is announced." (Mandoc, 2013) Work groups have already been formed to develop post GSM-R migration plans.

Costs

One aspect of the railway industry's experience with GSM-R deserves close scrutiny. The use of mass-market communication technologies like GSM had been expected to reduce equipment costs. The same argument is now being made for the use of LTE instead of specialised technologies. But the railways' experience casts doubt on that assumption: "when compared with TETRA… GSM-R also involves more capital expense and greater operating costs"[21] – despite the huge market for GSM products and the much smaller market for TETRA.

In fact the air interface is only a small part of a communication systems' total cost. According to Ericsson, 80% of the cost of a network results from base station sites and antenna masts:[22] the more base stations there are, the more the network costs. But there are also backhaul links, network management systems, system vetting, integration and maintenance, electric power and cooling for the transmitters, vehicles to retrofit and the cost of redundancy to increase reliability and resilience. All of these are needed for "mission critical" mobility regardless of the radio standard.

GSM-R's spread is gradually harmonising communications for Europe's railways and it will undoubtedly be used for the next decade at least. However, many legacy systems are still operating

---

[21] Malim, G. (2013) "LTE set to transform GSM-R but alternatives exist," *Wireless Magazine,* 6 November - http://www.wireless-mag.com/Features/27184/LTE_set_to_transform_GSM-R__but_alternatives_exist.aspx

[22] Ericsson (2013) "Parliamentary Inquiry Submission", quoted in paragraph 4.59 of "Chapter 4: Adequate spectrum for public safety agencies", *Completed Inquiry Report,* Joint Committee on Law Enforcement, House of Representatives, Parliament of Australia, http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/Completed_inquiries/2010-13/spectrummobilebroadband/report/c04

(see Appendix C.3 for country-by-country details). Safety must be preserved during the years of transition from older train control systems to ETCS. This requires what the industry calls Specific Transmission Modules (STMs), different for each country. STMs allow ECTS fitted trains to run on lines equipped with older signalling equipment. The cost of STM models varies as does the quantity of rolling stock needing them at any moment. So these are omitted from our calculations even though our modelling (reported in Chapter 4) shows that a long transition requiring interoperation between incoming and outgoing technologies has significant costs.

Based on trade press reports of projects in ten EU Member States, we calculate the average cost per km for GSM-R infrastructure as €58,792, and there is no evidence of a downward price trend. If 154, 284 km of European track will eventually be covered by GSM-R, the total cost of trackside equipment should be about €8.8 billion.

Based on projects reported in sixteen Member States, the average cost per km for ETCS Levels 1 and 2 infrastructure is €98,611 and €274,121 respectively, apart from any track improvements made at the same time. It is harder to estimate the length of track on which ETCS Level 2 will be deployed because Member States have some discretion outside the main corridors. But SWD(2014) 48 final indicates that ETCS is now in service on 9,462 km of track out of 38,845 km already contracted. If we suppose the need for ETCS Level 1 will fade away and Level 2 will eventually cover 50,000 km of track, deployment would cost about €13.7 billion at today's prices (ETCS prices are also not trending down).

Based on published reports of contract awards, it seems to cost about €26,714 to equip a locomotive with GSM-R. On average, ETCS Level 1+2 locomotive equipment costs €223,698 and ETCS Level 2 locomotive equipment costs €142,654. Supposing again that the need for ETCS Level 1 goes away and about 15,000 locomotives will be equipped with ETCS Level 2, they could cost about €2.1 billion to equip. So the total cost of ETCS Level 2 deployment, onboard and trackside, should be about €15.8 billion. GSM-R for 20,000 locomotives would cost about €0.5 billion, making the total cost of GSM-R deployment, onboard and trackside, €9.3 billion.

Thus, the deployment cost of ERTMS (GSM-R plus ETCS) is likely to be in excess of €25 billion. That does not include the cost of handheld radios, equipment for ETCS Level 1 or Level 3, migration to post-GSM-R networks or expansion of the high-speed rail network.

Summary

The choice of GSM as the platform for railway-specific communication systems was promoted 15 years ago as "future proof", in the belief that the technology's public popularity would make it irreplaceable, and the hardware cheaper. There is a warning here for LTE-based systems: if sectoral users commit to a particular technology based on the expectation of cost savings from large production volumes and mass market standards, given that their equipment replacement cycles are longer than mass market manufacturers are accustomed to, there is always a risk that the manufacturers will start shifting to newer technologies – like 5G – before the sectoral users have settled in to the current generation of products, denying them sufficient time to extract their investment's full value and forcing them to start replacing "stranded assets" that are still serviceable. LTE is not the final stage of cellular development. It is a 3G technology with 4G (LTE-Advanced) already entering the market and 5G "coming fast and furious".[23] The risk of lock-in to

[23] "'5G is coming fast and furious,' [Tareq Bustami] told *FierceWirelessTech*, with many operators planning to commercialize services in 2020. Working backward, that means initial deployments and field trials will start happening in 2018, so standards must be set in 2016…" Quoted in Parker, T. (2014) "Freescale exec: '5G is coming fast and furious'", *FierceWirelessTech,* 29 July, http://www.fiercewireless.com/tech/story/freescale-exec-5g-coming-fast-and-furious/2014-07-29 The European Commission and the Government of South Korea recently agreed to cooperate in the development of 5G,

LTE, from tailoring it to fit today's requirements so well, is just as great as it was with GSM-R, TETRA and TETRAPOL, because new and unforeseen requirements – like broadband – always emerge. Unless ERTMS and first responder communication support can be made technology neutral – detached from particular radio standards and defined as services or in software – "mission critical" Europe may always be burdened by costly commitments to aging equipment which works well but no longer fits their needs or budget.

The rail industry at least seems to have understood this and a new approach to the selection of post GSM-R radio networks is emerging. The relevant principles are these (the complete text is in Appendix C.3):

> The basic goal is that the on-board ETCS, EVC, is installed once (with an IP interface) and not affected by any subsequent change in the communication technology. Therefore, the specifications of the ETCS application should be separated from the transmission layer (bearer specifications)… The system should be flexible enough to allow the use of multiple technologies. One could consider several (IP-based) bearers: GSM-R (GPRS/EDGE); WIFI, LTE, satellite, etc., but also simple digital (and cheap) technology. This could also foster the expansion of ETCS to other regions of the world…

2.4 Applicability and relevance of the terms "mission-critical" and "non-mission-critical"

The Terms of Reference for this study specified a focus on possible roles for commercial mobile networks and technology in the provision of "mission critical high-speed broadband". No definition of "high-speed" was provided as there is a general reluctance to pick a number representing the minimum data transfer speed or bandwidth that can be considered "high speed" – or even "broadband". As Fornefeld and his colleagues noted: "There is no definitive answer as the bandwidth required to run Internet applications is continuously increasing and infrastructure standards are also continuously improving to face the growing demand". (Fornefeld *et al.,* 2008, p. 9)

Broadband is defined in ITU-R Recommendation M.2015 (2012a) as "data rates in the order of 1–100 Mbit/s with channel bandwidths dependent on the use of spectrally efficient technologies".[24] The Digital Agenda for Europe calls for all Europeans to have access to data connection speeds of at least 30 Mbps by 2020, with at least 50% of households having access to speeds above 100 Mbit/s. Therefore 30 Mbps became a benchmark for "high speed" in this study, as this bandwidth easily accommodates the simultaneous transmission of HD video, voice and browsing data. It also implies WiMAX or LTE, as these are the only widely available mobile broadband network technologies supporting such speeds. On the other hand, many essential applications in all three sectors actually require much lower data transfer rates, so 30 Mbps is a target not a minimum requirement.

The term "mission critical" requires more consideration. It has become common in discussions of public safety communications, with definitions offered by multiple sources. There is some convergence among these but none is entirely satisfactory. Samples are found in Appendix D where, in addition to "mission-critical communications", there are references to mission critical situations, solutions, services, operations, infrastructures, users, professions, information, and so on. One also

---

with funding available for projects starting in 2016. See "Landmark agreement between the European Commission and South Korea on 5G mobile technology", press release IP/14/680 (16 June 2014), http://europa.eu/rapid/press-release_IP-14-680_en.htm

[24] Other definitions are used in other ITU texts. This one is cited because REC M.2015 is devoted to "Frequency Arrangements for Public Protection and Disaster Relief Radiocommunication Systems in UHF Bands in Accordance with Resolution 646 (Rev.WRC-12)".

finds overlapping concepts like "life critical", "safety critical", "business critical", "mission essential" and "mission assured".

The word "critical" by itself has several meanings, some clearly unrelated to missions of any kind (e.g. critical reviews of a new play). The relevant meaning seems to be something that is *essential, vital or decisive.* "Critical" is also used in physics (as in "critical mass" or "critical state") to describe a potentially unstable situation where small additional inputs have unusually large outputs, like a phase change or a nuclear chain reaction. That seems relevant, too.

The core idea of "mission critical", then, seems to be that mission failure would jeopardise one or more human lives or put at risk some other asset whose impairment or loss would significantly harm society or the economy. A corollary is that even small degradations of communication supporting the mission could have large and possibly dire consequences.

"Risk to life" provides a rather clear test of criticality, even though perceptions of risk are subjective. But the scope of the phrase "mission critical" is made elastic, vague and arguable by including other assets whose loss would cause significant harm (which assets? how significant?). Yet that is the situation today since many of the quotes cited in the Appendix D clearly want the definition of "mission critical" to encompass more than just direct threats to life. Fires damage property more often than they injure or kill people, but firefighting is widely acknowledged to be a critical mission. Electrical blackouts may kill not anyone, but they could, and they can also cause large scale economic disruption.

In the utility and transport sectors, incidents happen with significant but diffuse impacts on society or the economy – disruptions and delays that cause economic harm if many people are affected or the duration is long. ENISA calculates the significance of MNO network outages with a mathematical function that combines the number of users affected with the duration of the outage. The same can be done for power cuts or traffic jams to produce a simplified scale of socioeconomic damage. Some level of impact could then be identified as the threshold of significance, which might vary from subsector to subsector according to an agreed impact per user per hour. Preventing harm above those levels could then be defined as a "critical mission" in addition to preventing injury or loss of life.

But when someone's job is protecting lives or keeping electricity flowing, does it make sense to distinguish between "mission critical" and "non-mission critical" for particular communications? The TCCA suggests that job responsibility is enough to identify "mission critical users":

> Mission Critical users are those that are responsible for the health, safety, security and welfare of our citizens. Police, Fire, Ambulance, rescue services and specifically the Military would be classed as Mission Critical. Those that ensure the availability of Electricity, Oil and Gas, Water and Core Transport services, without which modern life would quickly degenerate, are also classed as Mission Critical…" (TCCA, 2013a).

In fact it only makes sense to differentiate between "mission critical" and "non-mission critical" communications if those categories determine the choice of channel, network or level of encryption to use. If the same channels and networks carry both communication types with the same level of security it is not necessary to distinguish between them.

It is noteworthy that the ITU avoids the phrase "mission critical" except when quoting member contributions. Their new draft report on PPDR distinguishes instead between:

- day-to-day operations (planned);
- large emergency and/or public events (planned and/or unplanned); and
- disasters (unplanned). (ITU, 2013b)

But the need for a binary distinction arises from the fact that commercial cellular networks can satisfy some but not all of the communication needs of PPDR, utilities and transport – for broadband internet access, for example, but not for secure group conversation. This may be temporary: either LTE will acquire the reliability and functionality needed by PPDR or hybrid equipment will combine voice-via-TETRA with broadband-via-LTE. In the first case, all communications would go via LTE though it is not yet clear if the needed reliability will be provided by new dedicated networks or by hardening public networks. Since ENISA reports that major outages of commercial mobile networks are mainly because of overloading and failures of a few specific core elements, significantly reducing downtime might not be difficult or costly. (A public consultation on the costs of hardening mobile networks would be useful.) Since everyone now depends on constant mobile connectivity, and since the Framework Directive[25] makes Member States responsible for ensuring "the continuity of supply of services provided" by public communication networks, the case for hardening cellular networks for everyone, not just first responders, seems compelling.

However, there is an immediate need to decide how to fulfil the requirements of first responders while commercial cellular networks are still only partly suitable. First responders want affordable access to broadband services as soon as possible and in as wide an area as possible. But it would be a mistake to equate broadband with "non-mission critical" and voice with "mission critical" just because the networks available today impose that distinction. Most PPDR professionals accept that not all voice communication is "mission critical" and a lot of broadband could be. We regard these terms as oversimplifications of what is actually a continuum or hierarchy. We use them anyway because an aim of this study is to clarify their applicability and relevance.

2.4.1 Not an either/or

Part of our task has been to determine if there is – or could be – agreement on how to distinguish "mission critical" from "non-mission critical" in voice and data, and to discover if the distinction is – or could be – made similarly in each of the sectors examined. However, as noted above, by expanding the scope of "mission critical" beyond situations where life is at risk, the definition becomes elastic and arguable. There are valid reasons for including property risks and significant harm to society and the economy. So enlarging the scope does not add unnecessary ambiguity, it reveals deeper truths: *mission criticality comes not from the subject matter or the content of the communication but from the context, and the scales of risk and harm have many more than two levels.*

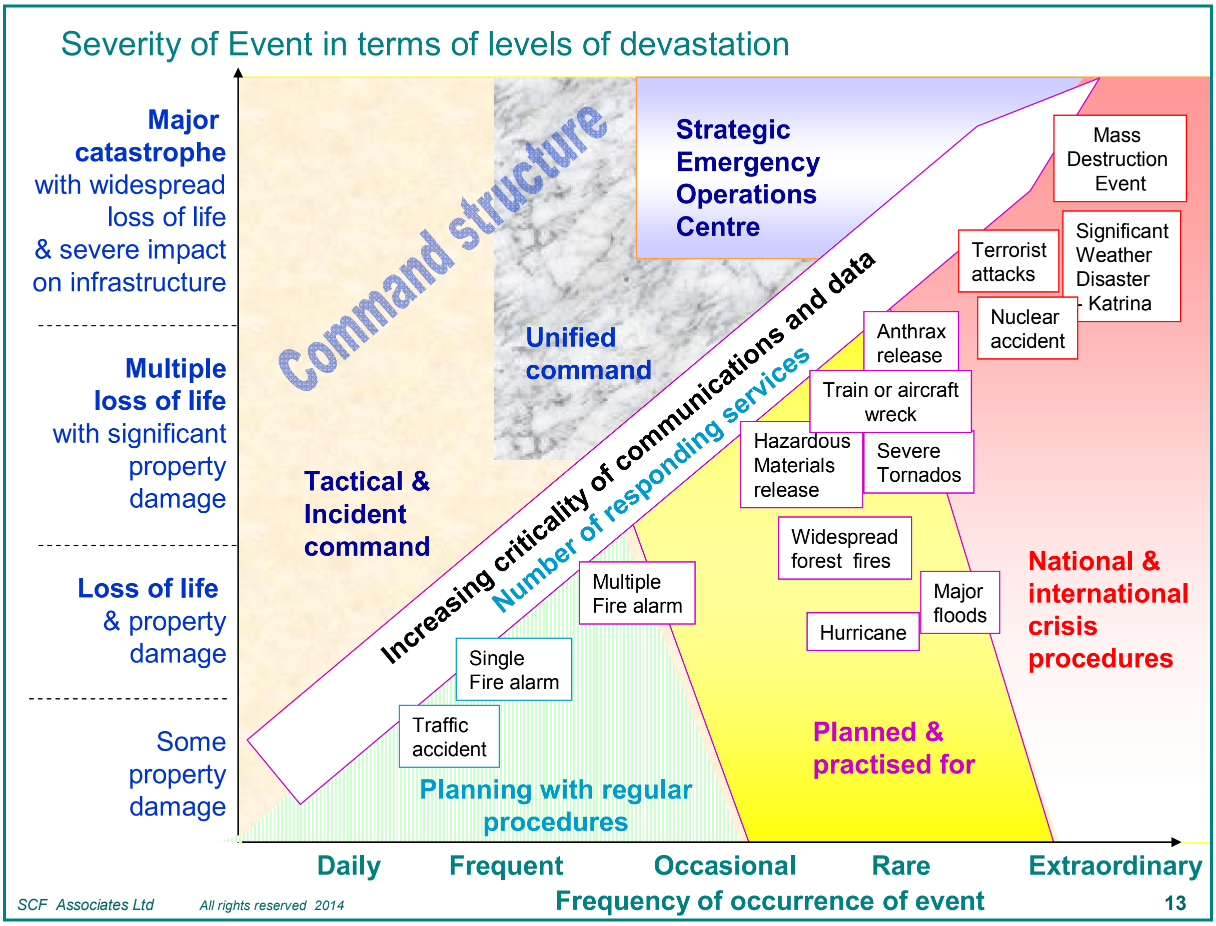
The European Smart Metering Industry Group (ESMIG) provides a clear example: "power quality data is not mission critical when a grid is in steady state, but can be vital in stabilizing a grid in highly stressed or damaged condition" (Strabbing, 2012). An automobile recognised as belonging to a fugitive is a "mission critical" clue; the same automobile, unrecognised, is not. Because any act or fact has meanings in multiple contexts, which can change, criticality must be a continuum. Figure 2.11 uses a hierarchy of event severities and responses to illustrate the "criticality continuum" from a PPDR perspective.

The diagonal arrow in the diagram represents a continuum aligned with increasing levels of devastation and numbers of responding agencies along with a decrease in the frequency of occurrence. The continuum is marked by step-changes, like those shown on the left side of the diagram: small property damage, loss of life/property, multiple loss of life/significant property damage, etc. Most of these step-changes are *within* the "mission critical" category, which is why they are omitted in

[25] Article 13a of 2009/140/EC says in paragraph 2: "Member States shall ensure that undertakings providing public communications networks take all appropriate steps to guarantee the integrity of their networks, and thus ensure the continuity of supply of services provided over those networks."

constructing the "mission critical"/"non-mission critical" dichotomy. (This may also be why interoperability between agencies and jurisdictions is often overlooked as a requirement for "mission critical" communications.)

Figure 2.11. The continuum of criticality with PPDR command/response hierarchies



Source: Adapted from Bhatia, 2012

2.4.2 Differences by sector

Since we believe the "mission critical/non-mission critical" distinction is an oversimplification of what is actually a continuum or hierarchy, discussing the different ways the distinction applies in the three sectors seems secondary to understanding why immediate access to reliable and secure wireless communication channels is needed in some situations but not in others. Therefore this section focuses on differences in sectoral needs rather than on definitions.

Public Protection and Disaster Relief

Compiling definitions of "mission critical" in PPDR has made it obvious that most are designed to fit police requirements primarily. The police are especially concerned that their tactical communications might be intercepted during the run-up to a raid or their locations might be tracked by criminals who could use the information to avoid capture or organise an ambush. Thus, in many of the definitions the need for security to prevent eavesdropping is paramount:

> The expression "mission critical" is used for situations where human life, rescue operations and law enforcement are at stake and public safety organizations cannot afford the risk of having transmission failures in their voice and data communications or for police in particular to be 'eave-

> dropped'… Where communication needs are non critical: human life and properties are not at stake, administrative tasks for which the time and security elements are not critical. (ECC Report 102, 2007a)

Fire brigades rarely express a need for communication security as they do not fear the consequences of eavesdropping. Communication security has a different role in EMS than in police work or firefighting: the need for security arises from privacy rights vested in personal medical data. There is minimal risk from interceptions of vital sign monitoring data as special training and equipment is needed to make it meaningful. That could change as more consumer-oriented equipment is introduced for non-emergency situations like outpatient monitoring and homecare. Many of these applications will be smartphone based, interfacing cellular networks and personal area networks such as Bluetooth. But the emerging security concern is not data interception so much as unauthorised access to the device for capricious and possibly malicious remote control.[26]

There is a long-standing tradition in search and rescue of using unencrypted channels, although that has changed in the military where rescues often occur in hostile environments. In disaster relief operations, a mix of secure and monitorable channels would seem to be optimum, as there is a need to give the public accurate and current information about the situation even when normal broadcasting channels are blocked. Triage decision making, on the other hand, is a process which always needs privacy.

Utilities

In contrast to PPDR, utilities consider voice communication "mission critical" only in a few special cases, according to the EUTC response to one of our questionnaires. The special cases are:

- ensuring the safety of people (employees, customers and the general public), particularly in emergency situations, and
- restoring normal operations and supply following an interruption of service.

Utilities' "mission critical" communications are mainly machine-to-machine (M2M) – for the management and control of supply and distribution networks. Such systems must obviously be secure, protected against unauthorised access from the public internet.

There are also security concerns with smart meters. Consumer resistance to their deployment is often based on the fear that private in-home activities might be revealed or monitored through patterns of electricity consumption or appliance use. Even the monitoring of inactivity is a risk: being able to identify unoccupied dwellings would be a boon to burglars. But the need for security does not make smart meters "mission critical". However, there will be a scale change when and if these systems develop into smart grids. Those are already seen as potentially "critical" infrastructures.

Operator Security Plans have not yet been drawn up for the European Electricity Transmission Grid and Gas Transmission Network. When these plans are developed they should include authorisation for gas and electricity alert and repair teams to use first responder networks to help restore service if their own networks are down. (President Obama has proposed adding electricity service restoration crews to the list of those entitled to use FirstNet.[27])

---

[26] Kinkead, G. (2014) "A Contraceptive Implant with Remote Control", *MIT Technology Review,* 4 July, http://www.technologyreview.com/news/528121/a-contraceptive-implant-with-remote-control/

[27] Berst, J. (2013) "Obama wants to elevate linemen to first responder status", *Smart Grid News,* 10 May, http://www.smartgridnews.com/artman/publish/Business_Strategy/Obama-wants-to-elevate-linemen-to-first-responder-status-5753.html

Transport

In Section 2.4, with the utility and transport sectors in mind, we proposed a simple scale for assessing "significant harm" to society or the economy, oriented toward events like traffic snarls and power outages, in order to recognise their prevention as "mission critical" when they are of sufficient scale. It is an odd but significant feature of the transport sector that maintaining normal traffic flow is a critical mission.

In the road safety subsector, two applications stand out as uniquely capable of saving lives: collision avoidance radars, built into many new car models, and the new eCall system, which will enable vehicles to summon emergency services automatically, via commercial cellular networks using the phone number "112". In the rail sector, data communications for train control must be considered "mission critical". It will become even more important if we enter an era of driverless trains. The same would apply to driverless road vehicles. The radio networks supporting such services must be robust, reliable, secure, constantly available and low latency, which fits the functional description of a "mission critical" network.

2.4.3 Broadband needs by sector

The need for broadband is largely driven by three factors: the need to transmit video or high resolution images, to use geographic information systems (GIS) or to access the internet.

In the utility sector, specific high security sites need video surveillance coverage (e.g. nuclear power plants, LNG terminals, gas storage sites) and field workers are increasingly using the internet to communicate with headquarters, update databases, manage customer relations, and so on. Commercial cellular is often used for these functions, but the vast majority of utility data transmissions are very low bandwidth, intermittent bursts of small packets from large numbers of measuring devices. GPRS is often used with smart meters but many electricity distribution companies now plan to utilise PLC, shifting radio links to their concentrator sites to send data to and from network management centres. Concentrating data from many sources adds to the duty cycle more than it increases required bandwidth.

In the transport sector, the need for broadband today is mainly for road traffic management, where CCTV is widely deployed to detect accidents and monitor congestion, for automatic number plate reading in connection with speed limit enforcement, toll collection and sometimes for detecting unregistered vehicles or tracking the movements of specific individuals. CCTV is also used for security in transportation hubs (airports, train stations) and in car parks where it has proven effective in reducing crime. It is possible that driverless vehicles will require broadband support although the dimensions of this need are not yet clear. First generation vehicles have mainly been autonomous, using onboard processing of onboard sensors. This may be because of the lack of roadside radio communication infrastructure. But if the technology is taken up on a large scale, more layers of intervehicle coordination and safety-enhancing situational awareness will be needed. The other area where there is already an identified need for broadband is for access to the internet by railway passengers during journeys. This cannot be considered "mission critical" but it may be essential for achieving the EU goal of reducing greenhouse gas emissions.

The greatest need for broadband comes from PPDR, for all three services – police, fire and medical. Car-mounted and body-worn video cameras are becoming standard equipment for the police. In coming years, there is likely to be a migration from slow-scan and standard definition video to high definition, which will greatly increase bandwidth requirements. Not much of this video needs to be transmitted in real time, but when the level of urgency escalates, it is important to have that option available. Augmented reality, which overlays data on real time video, is an emerging tool with great potential, and the use of video to record witness statements is also growing. Fire departments are increasingly interested in the use of through-the-wall UWB motion detectors, infrared cameras to see through smoke, and sensors to monitor body temperature, heart rate, oxygen levels, and so on. Efforts are underway to reduce the need for humans to enter burning buildings and that involves greater use of camera equipped robot "scouts". All these tools require short range, low latency, real time wireless channels.

2.4.4 Conclusion

The distinction between "mission critical" and "non-mission critical" is an oversimplification of what is actually a hierarchy or continuum of criticality extending from minor incidents to international catastrophes. Nevertheless the distinction is relevant because public safety radio networks are tailored to the needs of "mission critical" use and they are voice oriented, while broadband is quickly emerging as a necessity that can only be obtained today through "non-mission critical" networks. Commercial cellular is the obvious choice for wide area mobile broadband even though it is not yet ready to support either "mission critical" broadband or voice. This situation is probably temporary – although temporary means 3-6 years – and the length of the transition imposes questions such as: to what extent is broadband "mission critical", and which voice communications are not "mission critical"? However, because the "mission critical/non-mission critical" distinction depends on context, which is fluid and can change unpredictably, it is better to look at the communication requirements of specific activities in specific situations.

But to the extent that a stable definition of "mission critical" is needed to help determine the dimensions, performance and coverage requirements of secure networks, or to decide who should have access to priority channels, the following definition could be useful:

> *A mission is "critical" when its failure would jeopardise one or more human lives or put at risk some other asset whose impairment or loss would significantly harm society or the economy. In such cases even small degradations of communication supporting the mission could have possibly dire consequences.*

Unfortunately, the phrase "mission critical" is made elastic and arguable by going beyond risk to life to include damage to other assets with significant socioeconomic impact. Yet that is the situation today: political leaders and professionals in the three sectors seem to agree that a broader definition of "mission critical" is appropriate even when there is limited agreement on the definition's exact boundaries.

In the utility and transport sectors, incidents happen with significant but diffuse impact on society or the economy – disruptions and delays that cause economic harm if many people are affected or the duration is long. ENISA calculates the significance of communication network outages with a mathematical function that combines the number of users affected with the duration of the outage. The same could be done for power cuts or traffic jams to produce a simplified scale of socioeconomic harm. Some level of impact could then be identified as the threshold of significance, which might vary from subsector to subsector according to an agreed impact per user per hour. Preventing socioeconomic damage above agreed levels could then be defined as a "critical mission" (in addition to preventing injury or loss of life), while damage below agreed levels might at most be "business critical" – affecting specific individuals or firms but not enough to harm society or the wider economy.

Part of our task has been to determine if there is – or could be – agreement among the sectors on a definition of "mission critical" for voice and data. However, we found that the three sectors assess criticality very differently, leading to different network requirements. Whether they could or would share a network anyway probably depends on the details of the offered service, costs, rights, incentives and regulatory assurances.

3 Capabilities of Commercial Mobile Networks for Mission Critical Communication

This chapter focuses on the core question of this study: can commercial cellular networks satisfy the "mission critical" communication needs of PPDR, utilities and ITS?

The Terms of Reference for this study indicate that in answering this question our attention should focus on (i) "state of the art commercial mobile networks and equipment" and (ii) "networks and equipment which are expected to be available in foreseeable future".

We understand "state of the art commercial mobile networks and equipment" to mean cellular networks utilising the latest available LTE technology. LTE, "Long Term Evolution", is a standards suite that ETSI and the 3G Partnership Project (3GPP) are developing through successive releases over many years. The first full version of LTE was Release 8, "frozen" in December 2008.[28] Capabilities sought by the PPDR community will be added in Releases 12 and 13, now being drafted.

Given that PPDR requirements differ from the normal service offerings of commercial cellular, it is safe to say that today's "state of the art" networks and equipment satisfy PPDR requirements only partially. The same might be said for utilities and transport, although for different reasons. These conclusions are amplified below.

It is thus more interesting to consider networks and equipment likely to be available in the "foreseeable future". Fortunately, much of the 3GPP's work is done openly. Documentation posted on their website – proposals, drafts, meeting reports and schedules of future work – is freely accessible and their work patterns and procedures are firmly established.

It takes 3GPP 18-24 months to progress from the first sketches of what a release might contain to the date when it is "frozen". In general, then, the content and timing of future LTE releases is foreseeable though the further into the future one peers, the greater is the uncertainty: seeing beyond the next two releases is almost impossible.

Nevertheless we understand "networks and equipment which are expected to be available in foreseeable future" to mean future draft releases of LTE for which preliminary descriptions of the planned features are available.

Phased releases of new cellular standards come more or less regularly but equipment based on earlier releases remains in service for years. So not all cellular mobile networks have "state of the art" equipment. The fact that different generations (2G, 3G, 4G) and mutually incompatible air interfaces coexist is hidden by the fact that modern handsets contain multiple radios so they can interoperate with several kinds of network without the user being aware of the complexities. But these complexities do matter so we must consider deployment patterns in addition to the development of standards.

It is also important to distinguish between LTE as a technology and the service offerings of commercial cellular networks. LTE is being developed for commercial cellular networks – that fact

---

[28] 3GPP (2008) "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description", TS 36.300, version 8.7.0, http://www.3gpp.org/ftp/specs/archive/36_series/36.300/36300-870.zip

strongly shapes the standards development process – but it may also be possible to create LTE networks for "mission critical" users based on some other business model and a different offering of features. This has been suggested because, as noted earlier, there is rather more enthusiasm in the three sectors for LTE's potential as a technology than for the business practices of commercial cellular.

In order to understand the "foreseeable future" of mobile networks and equipment, it is necessary to understand the process of standards development; how MNOs deploy new equipment in existing networks; and how new networks utilising cellular technology could emerge. This chapter considers these topics after reviewing today's "state of the art" networks from the public safety user's perspective. This is followed by an overview of how the 3G Partnership Project works. The next section looks at how LTE standards are evolving. Since demand for "mission critical broadband" is already evident, we consider the timing of the introduction of new networks and services. Finally we look at harmonised bands for broadband and potential bands for "mission critical" broadband.

3.1 State-of-the-art commercial mobile networks and equipment

The introduction to this chapter says that today's "state of the art" commercial cellular networks and equipment satisfy the "mission critical" requirements of PPDR *only partially* and the same can be said for utilities and transport, though for different reasons. *Only partially* needs clarification, as do the different reasons. So before taking up other topics it may be helpful to summarise the shortcomings of today's networks.

3.1.1 Voice standards

Networks based on the current 3G cellular standards – not just current versions of LTE but UTRA-FDD, CDMA2000, W-CDMA, EDGE, HSDPA, and so on.[29] – do not support talk groups, direct mode operation, push-to-talk, emergency alarms and other voice features considered essential by first responders. LTE support for simple one-to-one voice calls is particularly limited – because, of the many 3G "flavours", it is the least backwardly compatible with analogue telephony. LTE was originally intended to provide cellular subscribers with higher broadband speeds. Today's handsets only use LTE for data sessions. When a voice call is initiated or received, the handset automatically falls back to an older 2G or 3G network using one of its pre-LTE radios.

LTE's lack of support for simple voice calls was recognised early as a weakness and corrections were proposed; the GSM Association's endorsement of a particular approach settled the matter.[30] Now, as GSMA's technology director put it, "Everyone is heading to VoLTE [Voice over LTE] – just taking different paths to get there".[31] At this stage, then, compatibility among networks and handsets implementing VoLTE is not assured and it could take a year or two of product development, marketplace competition and standards refinement to move from a minimum set of agreed definitions to an integrated array of optimised features. Unfortunately, time to sort out VoLTE's problems is a luxury 3GPP does not have.

---

[29] It is not necessary to know what these abbreviations stand for. It is only necessary to know that LTE is not the only 3G implementation.

[30] GSMA's endorsement is embodied in "The IP Multimedia Subsystem (IMS) Profile for Voice and SMS", Non-binding Permanent Reference Document IR.92, http://www.gsma.com/newsroom/wp-content/uploads/ 2014/06/IR92v8-0.pdf

[31] Hutton, D. (2012) "Overview of RCS and VoLTE", GSM Association, presented at ETSI's RCS-VoLTE Plugtest, 10 October, http://www.etsi.org/plugtests/RCS-VOLTE/pres/121010%20Overview%20of%20RCS%20and%20VoLTE%20v2.pdf

Fast call setups have been touted as a benefit of LTE, and the technology is in fact optimised for low latency. But in the background is a technical issue that exemplifies the kind of fine-tuning and debugging which standards developers must complete to make a complex technology like LTE viable, and which illustrates why the process is slow.

The VoLTE implementation embraced by the cellular industry is based on 3GPP's IP Multimedia Subsystem (IMS), a framework for delivering multimedia services using the Internet Protocol. In addition to voice calling, IMS supports broadband video so it is an important part of the LTE toolkit. IMS streamlines the running of media applications but is itself complex and burdensome to deploy and maintain on networks and local processors. So GSMA proposed using a simplified "stack", which is still being developed and tested. The good news for first responders is that IMS includes a session-based "presence server" which can support talk groups, DMO, push-to-talk, emergency alerts, "access approval", and so on. On the downside IMS has so many layers that signalling is slow, adding a delay factor that accumulates as call volumes increase, especially when received signal strength is low as is normal near the edge of an LTE base station's coverage area. Since LTE coverage is based mainly on small cells, more of the service area will be near edges than is the case today with macrocells.

Therefore, using the current IMS "stack" – which could be improved in later releases – LTE call setup times lengthen as traffic gets heavier. For people trying to deal with an emergency this is an unwelcome pattern. Far from solving the problem of service collapse because of overloading and congestion, thanks to higher spectrum efficiency, LTE may be more susceptible to congestion than earlier cellular interfaces unless this is resolved.[32]

3.1.2 Resilience

A more serious problem is the limited resilience of today's commercial cellular networks. Resilience is defined by the European Network and Information Security Agency (ENISA) as:

> the ability of a system to provide and maintain an acceptable level of service in face of faults (unintentional, intentional, or naturally caused) affecting normal operation. In this context, the main objective of a resilient communications infrastructure is that faults are 'invisible' to users in the sense that it may result to degradation in terms of Quality of Service (QoS) but within an accepted predefined range of values that are described in the Service Level Agreement (SLA) between the service provider and the user. (ENISA, 2009, p. 3)

ENISA collects, analyses and reports annually on severe outages of electronic communication networks in the Member States. Their most recent report, reviewing 79 incidents from 2012, notes that most "incidents (around 48%) affected mobile telephony or mobile Internet. This would suggest that mobile services are more at risk of large-scale outages. We drew a similar conclusion last year" (ENISA, 2013). The average number of end-users affected by each large outage in 2012 was 1.8 million in mobile telephony and 1.7 million in mobile internet. Network overload "was the cause affecting by far most user connections, more than nine million connections on average per incident. In second and third place came software bugs with four million affected connections and power cuts with three million connections".

"Natural phenomena" (storms, floods, and so on) caused the longest outages – an average of 36 hours per incident – as well as the most lost user-time (the number of affected subscribers times the outage

[32] 3GPP is aware of the problem and is addressing it. LTE Release 11 (frozen in June 2013) includes preliminary steps toward a new IMS "overload control" architecture which reacts to "near-congestion" conditions by temporarily throttling new incoming calls to avoid overloads. Another approach is embodied in the simplified but standards conformant IMS stack developed by Prof. Khalid Al-Begain and his team at CEMAS at the University of South Wales. General Dynamics UK is deploying their stack in mission-critical LTE networks (www.cemas.mobi).

duration). But recovery time from “human error” was also substantial: 26 hours on average. In 37% of the incidents, the public’s ability to call the 112 emergency number was affected. Sixty percent of the outages blamed on “third party failures” were because of loss of electric power, resulting in an average of 2.8 million subscribers losing service for an average of 13 hours.

Finally – and perhaps most useful for improving resilience – ENISA identified the assets responsible for “system failures” and the percentage of incidents attributed to each cause. The top five points of system failure were: switches (18%); user and location registers (14%); base stations and controllers (9%), mobile switching (9%); and the core network (5%).

A followup ENISA study focuses specifically on the problem of improving the resilience of commercial cellular networks to electricity supply disruptions. Karsberg, Moulinos and Dekker (2013) found that:

- “power cuts are typically not considered a major threat by the interviewed providers” (apparently because brief power cuts are common – and localised – so business continuity planning is geared to dealing with outages in small areas lasting just seconds or minutes);
- “Many Member States consider power cut resilience to be a market rather than a regulatory issue…” And yet: “NRAs make the assessment that ordinary customers place little value on the extent to which providers are resilient to power cuts.” Consequently: “A majority of NRAs believe that current protection levels are not adequate and they would like to see power cut resilience to become a market differentiating factor for network and providers.”
- However, since power cut resilience is not a “market differentiating factor”, many would shift responsibility to energy regulators to reduce the frequency and duration of power outages: “In some countries, the energy sector has taken significant steps in defining socio-economically acceptable quality of service levels, whereas in some countries the [mobile cellular] providers face the fact that there are no special contractual agreements with the power companies containing SLA-based requirements.”

The Electronic Communications Framework Directive (2009/140/EC) says in Article 13a paragraph 2:

> Member States shall ensure that undertakings providing public communications networks take all appropriate steps to guarantee the integrity of their networks, and thus ensure the continuity of supply of services provided over those networks.

More could be done to make that obligation a reality. But first, discussion is needed regarding what steps are “appropriate”. Threats to the continuity of cellular service vary from one member state to another, so whatever is needed to sustain a consistent level of service will not be the same everywhere. Responsibility for the cost of improving resilience also needs to be debated. In a few Member States, public funds have been used to supply generators and other equipment to mobile network operators. In others there has been public-private cost sharing. In still others, carriers have been required to bear the costs themselves. But regulators in the Member States seem to agree with ENISA that too little is being done to make commercial mobile networks resilient.

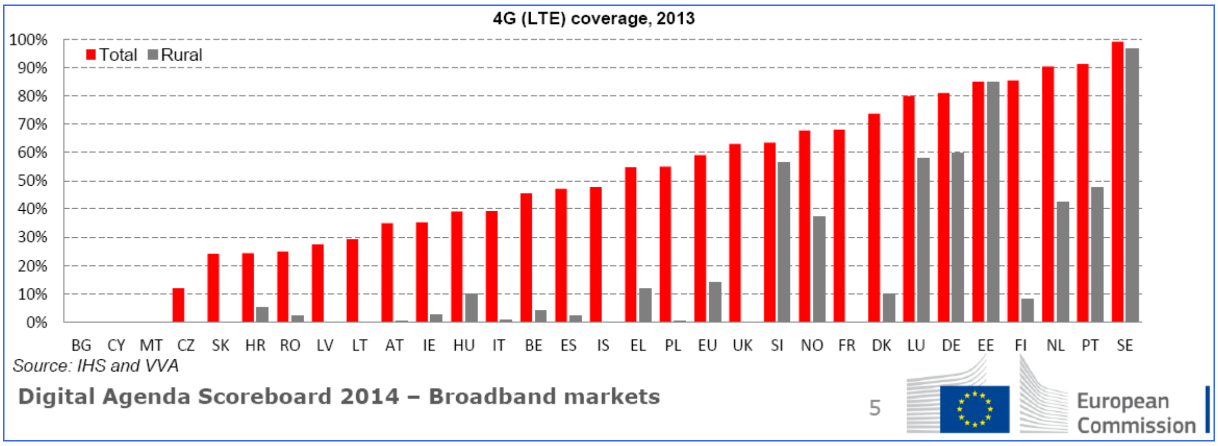
In the case of LTE, the cost of backup power and redundant facilities could be increased by the large number of small cells expected to be deployed. On other hand, small cell hardware is much less costly than macrocells, which could make redundancy more affordable. Small cells also consume much less power, perhaps enabling more use of backup batteries and renewable power sources (e.g. fuel cells, solar) to keep the batteries full. It is not known if cellular network operators in Europe will fight against higher minimum standards for network resilience as fiercely as their counterparts in the USA.

But the way these issues have been handled in the USA underscores the importance of reaching some sort of mutual understanding before a solution is imposed.[33]

3.1.3 Coverage

According to the Digital Agenda Scoreboard, LTE coverage in the EU is growing rapidly, from about 27% at the end of 2012, to nearly 60% at the end of 2013:

Figure 3.1. LTE coverage in the EU, end of 2013



A simple forward projection might suggest LTE coverage will exceed 90% by the end of 2014. But coverage growth does not proceed at a constant rate nor is it spread evenly. About a third of the Member States are off to a slow start while the small grey bars on the chart show rural coverage lagging urban coverage by a wide margin: at the end of 2013 only about 13% of rural households in the EU had an LTE signal. Even that estimate may be too high. Unless the researchers who compiled the data for the Digital Agenda Scoreboard actually visited millions of homes with signal measuring devices, they may have relied on carriers' coverage claims that are often enhanced for marketing purposes. For example, 3G operator claims in 2011 that their networks covered 97% of the UK population were challenged by the BBC, which conducted its own survey using 44,600 volunteers to check 42 million locations with their handsets for a total of 1.7 million hours. The volunteers found a 3G signal 75% of the time.[34] This led Ofcom to tighten up both its coverage requirements and enforcement so that at the end of 2013 the carriers finally achieved 90% coverage.[35]

In Figure 3.1, Sweden appears to have reached the highest level of LTE coverage in Europe. An IHS press release about their findings likewise asserts: "In Sweden, 99.2 percent of households are in areas

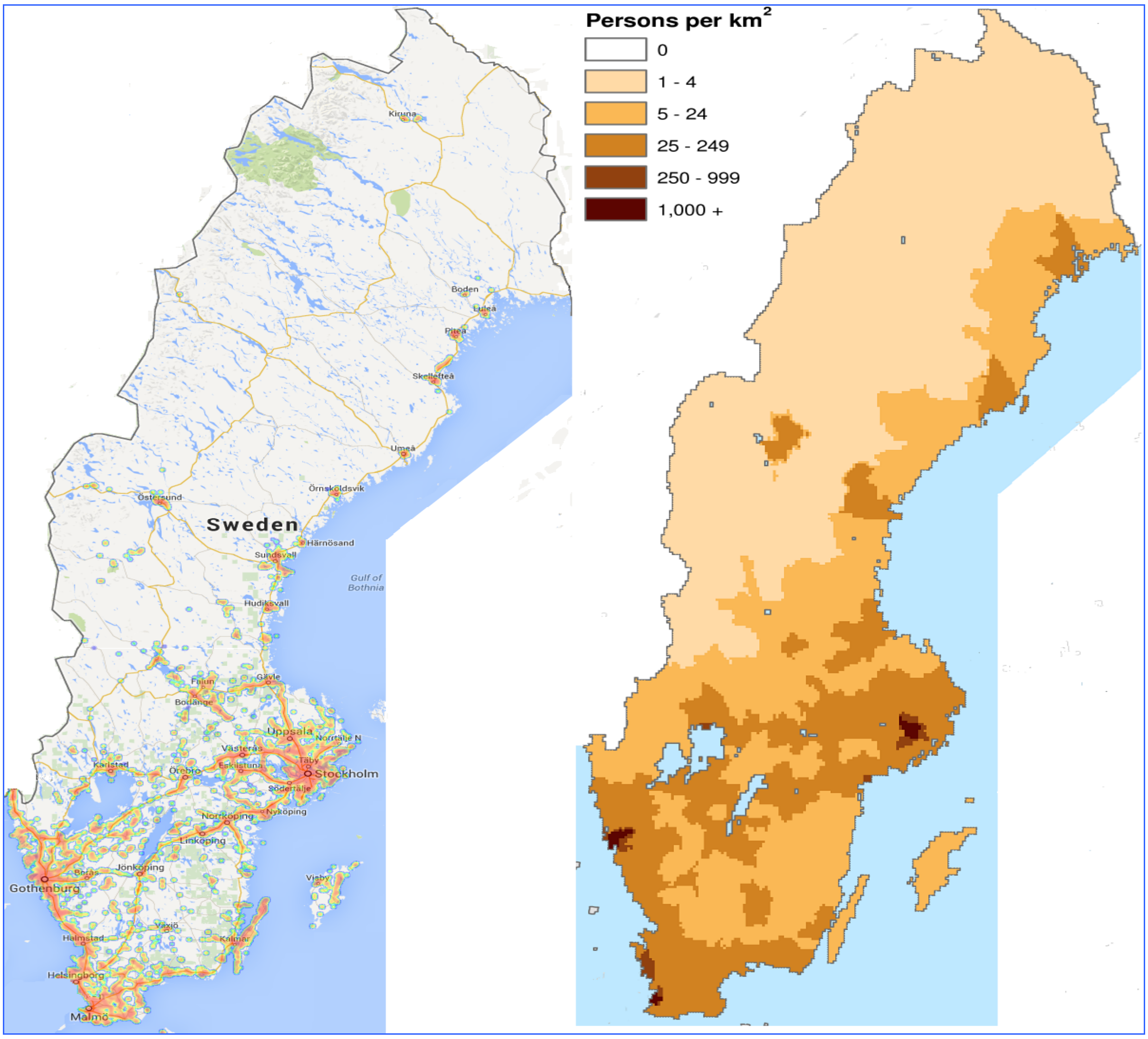
[33] In 2007 (after Hurricane Katrina) the FCC ordered all fixed and mobile carriers "to have an emergency back-up power source for all assets that are normally powered from local AC commercial power". The cellular trade association, CTIA, went to court to block the order and won, mainly because the FCC failed to conduct a public consultation about the cost of compliance. More recently, after superstorm Sandy, when there was renewed public pressure for backup power at cell sites, the FCC issued a meek order leaving it to the MNOs to decide what measures are appropriate. Savouring their victory, a CTIA spokesman said, "No government regulation can provide any greater incentive than carriers already have to provide the most reliable service possible". Quotes from Goldstein, P. (2013) "FCC proposal would require carriers to report cell tower outages in wake of disasters", *Fierce Wireless*, 27 September, http://www.fiercewireless.com/story/fcc-proposal-would-require-carriers-report-cell-tower-outages-wake-disaster/2013-09-27, and FCC (2007) "In the Matter of Recommendations of the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks: Order" EB Docket No. 06-119 and WC Docket No. 06-63, http://fjallfoss.fcc.gov/edocs_public/attachmatch/FCC-07-107A1.pdf

[34] Wakefield, J. (2011) "3G mobile data network crowd-sourcing survey", *BBC News,* 24 August, http://www.bbc.co.uk/news/business-14574816

[35] UK Office of Communication (2013) "Ensuring 3G coverage compliance", 7 November, http://media.ofcom.org.uk/news/2013/3g-coverage-compliance/

covered by advanced 4G mobile broadband”[36] (by which they mean LTE). Rural coverage appears just slightly less. Is this plausible? In Figure 3.2, a population distribution map of Sweden is placed to the right of a map showing the actual strength of LTE signals measured by people who installed OpenSignalMaps’ smartphone application. This app measures cellular and Wi-Fi signal strengths everywhere the handset goes and reports the data anonymously to a hub in London. The signal strengths shown on the map are cumulative – that is, gathered over many months – and the map is updated constantly so it is current to August 2014. It is not known how many signal mappers are in Sweden but since seven million copies of the app are in use, mainly in Europe, there are probably thousands. In any case, the signal strength map suggests LTE coverage in Sweden must be less than 99.2% of households. The coverage of rural areas is also more limited than one might suspect from the DAS data.[37]

Figure 3.2. Measured LTE coverage (left) versus population distribution (right) in Sweden



Map sources: http://opensignal.com, 19 August 2014 (left); Center for International Earth Science Information Network (2005) “Sweden, Population Density, 2000”, *Gridded Population of the World,*

---

[36] IHS (2014) “Data confirms EU hit ‘Broadband for All’ target…”, press release, 28 May, http://press.ihs.com/press-release/technology/data-confirms-eu-hit-broadband-all-target-ihs-technology-says

[37] The Swedish Post and Telecom Authority (PTS) says that according to their data, LTE covered 42% of the national territory at the end of 2013, but 98% of Sweden’s population lives in that area. The TETRA network used by PPDR also has limited coverage in the mountainous western part of the country (PTS, private correspondence, October 2014).

version 3, http://sedac.ciesin.columbia.edu/downloads/maps/gpw-v3/gpw-v3-population-density/swedens-thumbnail.jpg (right)

OpenSignalMap visualisations of LTE coverage for all the EU Member States have been checked and the pattern is consistent: actually detected coverage is less than claimed – with one notable exception: Germany had strict requirements for rural coverage in their LTE roll-out and the map corroborates both their success in attaining that coverage and the accuracy of the Digital Agenda Scoreboard's German data. In all other cases the discrepancy between claimed coverage and signal strength appears significant – though not in cities. LTE signals at this stage are an urban phenomenon while claims of extensive rural coverage in countries like Estonia and Slovenia have not been substantiated.

First responders, especially fire brigades and EMS, seek ubiquitous signal coverage because they must deal with incidents anywhere. Water and gas companies need links to their supply sources. In neither case does commercial LTE today provide the needed coverage. Unless carriers are either required or given incentives to extend their coverage beyond population centres and busy transport routes, it won't happen: they are businesses, after all. If public safety agencies are to rely on commercial cellular networks for mobile services then vigorous reality checks on the carriers' coverage claims are needed to gain confidence that the promised coverage is there.

3.1.4 Different models

In Chapter 2 the importance of air-ground-air communications for search and rescue, public protection and disaster relief was noted. ETSI's design guide for AGA communication points out that "significant design changes have to be implemented [for cellular networks] to service the requirements for effective AGA use… It is strongly recommended that antennas used for terrestrial radio cells are not shared with AGA sites [and] spectrum for AGA use is reserved solely for AGA" (ETSI, 2011). Given that many critical missions depend on it, support for AGA is a litmus test of whether public safety organisations can rely solely on commercial cellular networks for mobile services. AGA support obviously has costs. How those costs are borne needs to be discussed because that could determine the networks' willingness to support such a service. Alternatively, AGA might be set up and operated as a separate "overlay" network.

The list of PPDR requirements from Section 2.2.1 also calls for differentiated priority classes, so high priority public safety communications are never blocked by nonessential communications. 3GPP is addressing this need in upcoming releases of LTE standards. But a problem arises because LTE is basically an internet service. In April 2014, the European Parliament adopted the Connected Continent resolution, which embraces net neutrality: "The principle of 'net neutrality' in the open internet means that traffic should be treated equally, without discrimination, restriction or interference, independent of the sender, receiver, type, content, device, service or application…" (European Parliament, 2014) BEREC's response to the Commission's 2010 consultation on network neutrality also concluded that traffic management on mobile networks should be non-discriminatory: "a mobile network access may need the ability to limit the overall capacity consumption per user in certain circumstances… [When] this does not involve selective treatment of content it does not, in principle, raise network neutrality concerns."

Network neutrality is clearly at odds with the "selective treatment of content" to ensure that certain messages get priority treatment and favouring certain subscriber groups. But BEREC acknowledges that when non-neutrality results from a legal obligation, rather than from the service provider's own initiative, it can be acceptable. For instance: "National regulations could impose priority use of telecommunications infrastructure for security forces, medical personnel, etc". But in that case, the 2009 Framework Decision limits the scope of the imposition:

> Any of these measures regarding end-users' access to, or use of, services and applications through electronic communications networks liable to restrict those fundamental rights or freedoms may only be imposed if they are appropriate, proportionate and necessary within a democratic society, and their implementation shall be subject to adequate procedural safeguards… (Article 1.3a)

What makes non-neutrality a politically sensitive issue, according to Marsden (2013), is that it exercises "the technology of censorship" even when the aim is different – and commercial carrier censorship of subscriber communications is acceptable in Europe "only in limited circumstances". Unfortunately, network neutrality is generally at risk from LTE because each release adds new tools for application-based charging.[38]

It should not be hard for any state to create a legal obligation for commercial carriers to give priority rights to emergency services. But to protect the principle of network neutrality some states might rather have prioritised communications in a closed *non-public* network since prioritisation is not objectionable there. This may be a consideration in deciding whether to use public or dedicated networks for services requiring priority rights.

Prioritisation is just one issue separating the "carrier model" from the "public safety model". There are others and such differences can introduce tensions. They will be challenging to reconcile:

Table 3.1. Different models: Public Safety versus Commercial Carriers

Issues	Carrier Model	Public Safety Model
Goals	Maximise revenue & profit	Protect life & property
Capacity	Defined by "busy hour" on a typical day	Defined by "worst-case scenario"
Coverage	Population-density	Territorial, focused on what may need protection
Availability	Outages undesirable (revenue loss)	Outages unacceptable (lives threatened)
Communications	One-to-one	Dynamic groups, one-to-many, field crews/control centre
Broadband data traffic	Internet access (mainly downloads)	Traffic mainly within agency (more uploads than downloads)
Subscriber information	Owned by carrier	Owned by agency
Prioritisation	Minimal differentiation – by subscription level or application	Significant differentiation - by role & incident level (dynamic)
Authentication	Carrier controlled, device authentication only	Agency controlled, user authentication
Preferred charging method	Per minute for voice, per GB for data	Quarterly or annual subscription with unmetered use

Source: Compiled from Vratonjić (2013), Alcatel-Lucent (2014), Motorola (2014) and interviews

[38] 3GPP (2014) "…Policy and charging control architecture (Release 13)", Technical Specification TS 23.203 V13.0.1, http://www.3gpp.org/ftp/specs/archive/23_series/23.203/23203-d01.zip

3.2 Commercial networks and equipment expected in the foreseeable future

LTE is a work in progress. To understand how it may evolve it is necessary to understand how the 3G Partnership Project (3GPP) works. They create the standards for LTE networks and equipment, and standards determine the key aspects of implementations.

3.2.1 Standards

In the late 1990s Nortel Networks and AT&T Wireless decided to cooperate in developing cellular mobile internet technologies starting from the data support capabilities of GSM. British Telecom, France Telecom, Telecom Italia, Telenor, Nokia and other companies joined the effort, establishing a "3G IP standards forum" in 2000. The name changed to 3GPP as the partners took on the broader task of developing standards for next-generation global wireless networks. The 3GPP support staff – known as the Mobile Competence Centre – is based at ETSI headquarters in Sophia-Antipolis, France.

Six "Organisational Partners" guide the work of 3GPP: Japan's Association of Radio Industries and Businesses; the US Alliance for Telecommunications Industry Solutions; the China Communications Standards Association; ETSI; Korea's Telecommunications Technology Association; and Japan's Telecommunication Technology Committee. The Organisational Partners are themselves membership organisations, so the companies and institutions belonging to them are individual members of 3GPP (405 at last count).

Thus most 3GPP members are companies based in Europe, Asia or the USA that make mobile communications equipment or which own or operate networks. A smaller number are standards organisations, trade associations, intergovernmental or governmental entities. In addition, "Market Participation Partners" (MPPs) are invited to advise 3GPP. The TETRA and Critical Communications Association (TCCA) became a 3GPP MPP in October 2013.

Standards development is *contribution driven.* Unless 3GPP members commit resources to developing a particular specification, it will not find its way into a release. Since most 3GPP members either sell equipment or services, if a feature does not increase revenue, directly or indirectly, resources will not be committed to developing it. Conversely, a feature that deprives a network of revenue is even less likely to be supported. Thus, 3GPP members look at communication network features and specifications very differently than PPDR professionals.

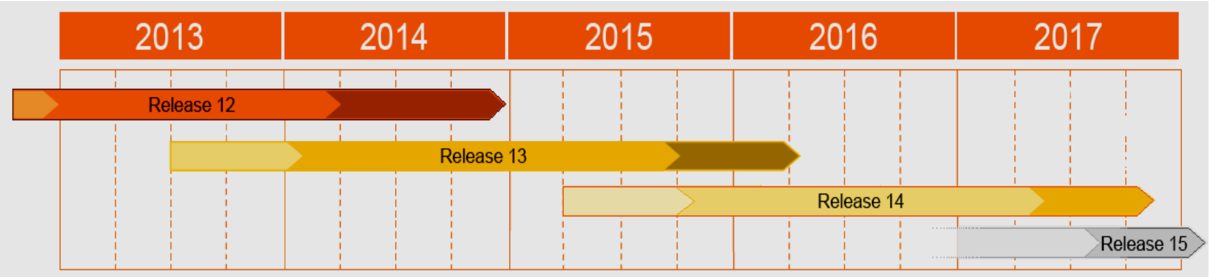
Standards development in 3GPP progresses through three stages, with freeze dates for each stage:

Stage 1: defining service requirements from the users' perspective
Stage 2: defining an abstract architecture to support those requirements
Stage 3: defining an implementation of the architecture

A "release" is an internally consistent set of specifications – dozens or even hundreds of them, defining and describing every aspect of the communication system. As the name suggests, a release is intended for release to the world after the Organisational Partners approve it.[39] Figure 3.3 shows provisional timelines for 3GPP's current and near future standards development projects:

[39] Procedures for creating and maintaining specifications are described in http://www.3gpp.org/ftp/specs/archive/21_series /21.900/21900-b01.zip

Figure 3.3. 3GPP provisional schedule for LTE releases to 2017



Source: Bertenyi, 2014.

In 2009 the US National Public Safety Telecommunications Council (NPSTC) decided LTE should be the radio platform for a new nationwide public safety network with broadband capabilities. They engaged with 3GPP to evolve the LTE standards toward the needs of public safety, recognising that some new features and capabilities might also be useful to business users and consumers. Because of the size of the US market and the fact that they catalysed global interest in public safety LTE, the USA has significant influence on 3GPP's work in this field. LTE Release 11 included an air interface profile for high-power user terminals conforming to new FCC rules for the "Public Safety Block" at 700 MHz.[40] Since other countries may also want to be able to use off-the-shelf equipment for public safety broadband at 700 MHz, the FCC rules are a convenient precedent and 3GPP's early response to the needs of the US market means the first wave of mobile terminals could be available as early as next year. However, delays in FirstNet's buildout (which is expected to take about 10 years [NPSTC, 2013]) could slow the pace of product introduction and the first wave of devices will in any case lack the mission critical features still in development.

Interest has grown recently in the possibility of using 450-470 MHz for public safety LTE. This is discussed in more depth in Section 3.4. What put it on the agenda was the fact that many countries had already designated this range for PPDR when the 2007 World Radiocommunication Conference identified it for future use by cellular networks, too. In June 2012, Brazil awarded a new cellular license for this range, and since no specifications existed yet for LTE at 450 MHz, 3GPP agreed to develop them for Release 12.

Another relevant near-future 3GPP project is the "Study on Isolated Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Operation for Public Safety".[41] The idea is to standardise adaptations which make the most of communication functions remaining after an LTE network is severely impaired by disaster. The situations explored so far in this stage 1 study are when:

- a base station is no longer available to local users
- a base station's backhaul link is cut or impaired
- a temporary base station is deployed with limited or no backhaul
- connectivity is restored to part of the network which had been isolated.

This work is for Release 13 so it is not yet clear what it will enable.

---

[40] 3GPP (2013) "…Public safety broadband high power User Equipment (UE) for band 14", Release 11, Technical Report TR 36.837 V11.0.0, ftp://ftp.3gpp.org/Specs/2012-12/Rel-11/36_series/36837-b00.zip

[41] 3GPP (2014) "Study on Isolated Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Operation for Public Safety (Release 13)", Technical Report TR 22.897 V13.0.0, http://www.3gpp.org/ftp/specs/archive/22_series/22.897/22897-d00.zip

For Releases 12 and 13, 3GPP agreed to focus on standards for DMO (which they call Proximity Services or ProSe) and Group Communication System Enablers (GCSE) for talk groups, all-calls, and so on. With a December 2014 freeze date set for Release 12, the current draft specifications are virtually complete. Release 13's freeze date is March 2016 so it is much less developed. Release 14, tentatively planned for freezing in the fourth quarter of 2017, could see the first 5G features introduced but no description has been issued; the content and timing of that release are both likely to be influenced by WRC-15.

Recalling the three-stage process described above, ProSe stages 1 and 2 have been completed: requirements and abstract architectures are defined in Release 12. 3GPP foresees that public LTE subscribers might want proximity services, too, though with less strict security/authentication features than public safety users (Henze, 2013). A Bluetooth-like feature – "proximity discovery" – lets someone know that a friend is nearby so they can initiate a communication, share files or play games together. It might also enable a PC to back up the contents of a handset via LTE. The current concept is that communications between public safety users can be direct, terminal-to-terminal, even if a base station is in range, but public users can communicate terminal-to-terminal only if no base station is in range. This is because carriers see "off-network" communication as a potential revenue loss. Unless new usage tracking mechanisms are devised, ProSe could deprive cellular operators of chargeable activities regardless of whether users are public safety or the general public. Consequently, Technical Specification 32.277 will define new ways for carriers to collect charging data for proximity services.[42] The approach is to rely on "delayed reporting": terminals will record usage for delivery to network management later. A first draft of the specification was published in May 2014 but work continues. Since the freeze date for Release 12 is so near, completion of this work must be pushed back into Release 13.

3GPP's focus so far has been on ways to charge the public for proximity services. If first responders have a service contract that does not impose charges for ProSe, they will not be billed. (The specification is designed to ensure that charging data can be collected even if it is not used.) But a separate "Study on Charging support for ProSe one-to-many Direct Communication for Public Safety use" is underway, aimed specifically at making it possible to charge public safety users for off-network groupcalls. A preliminary draft was published in August 2014.[43] However, the work will obviously not be finished in time for Release 12. Depending on the findings of the study, a mechanism for off-network groupcall charging could be added to TS 32.277.

The second stage of GCSE (defining an architecture) is nearly finished and a security architecture has been defined. But work on stage 3, including congestion management, has barely begun. With the Release 12 freeze imminent, this work will also have to be finished in Release 13. However, according to draft ECC Report 218:

> GCSE will provide the basic platform support for group communications such as multicasting and group management, but not the actual application. This means that group voice calls will require a group call application in the terminals and a respective application server in the network on top of the GCSE support. Similarly, any other group communications will require an application (the same or a different one). (ECC, 2014b, p. 21)

While this provides flexibility and allows for customisation (not all user groups need the same features), it could also lead to interoperability problems and vendor lock-in.

---

[42] 3GPP (2014) "…Proximity-based Services (ProSe) charging", Release 12, Technical Specification TS 32.277 V0.1.0 http://www.3gpp.org/ftp/specs/archive/32_series/32.277/32277-010.zip

[43] 3GPP (2014) "…Charging management; Study on Support of ProSe Direct Communication for Public Safety", Technical Specification TS 32.277 V0.1.0, http://www.3gpp.org/ftp/specs/archive/32_series/32.844/32844-010.zip

“Mission Critical Push-to-Talk” (MCPTT) combines ProSe and GCSE and is native to Release 13. Although the concept seems simple – and familiar from earlier PPDR radio systems – a high degree of planning and contextual intelligence is required to optimise performance:

> The MCPTT service is intended to support communication between several users (a group call), where each user has the ability to gain access to the right to talk in an arbitrated manner. However, the MCPTT service also supports private calls between pairs of users… To the extent feasible, it is expected that the end user's experience will be similar regardless if the MCPTT service is used under coverage of an EPC network or based on ProSe without network coverage…
>
> MCPTT service provides a means for a user with higher priority (e.g., emergency condition) to override (interrupt) the current talker. MCPTT service also supports a mechanism to limit the time a user is able to talk (hold the floor) thus permitting users of the same or lower priority a chance to gain the floor… An MCPTT service user may join an already established MCPTT group call (late call entry). In addition the MCPTT service provides Talker ID and user location determination features…[44]

MCPTT is the archetypal mission critical voice service. It is hard to imagine any police or fire department migrating to a network that lacks this capability, though it does not matter so much to the other sectors examined in this study. The rapporteur for this 3GPP work item says stages 2 and 3 are half finished, but Release 13 won’t freeze until the end of the first quarter in 2016. Allowing 18-24 months for product development means LTE equipment with enough mission-critical voice support to be a plausible alternative to TETRA could enter the market in the late-2017 to mid-2018 timeframe. The UK wants to start migrating from TETRA to LTE in 2016, taking 4 years to complete the task. They are probably most sensitive to the timing of equipment availability. From their perspective 2018 is late but still manageable.

One issue that might concern some public safety users is whether the encryption available on public LTE networks is strong enough for mission critical situations. 3GPP has already had to accommodate a variety of national requirements and restrictions with regard to encryption so flexibility in that area has been built in to LTE. Accommodating additional encryption packages for specific user groups should not require fundamental changes.

As for the other sectors within the scope of this study, it is too soon to say if LTE will meet their needs because enhanced support for M2M links is still in development with more work planned for Release 13. Utilities, on the other hand, are cost sensitive. So even if LTE’s specifications are adequate, the tariffs and service agreements offered by network operators will be decisive factors.

To sum up, 3GPP has welcomed requests from NPSTC and TCCA for features that would enable first responders to use LTE for mission critical communications. New work items have already been completed for Release 11; more are underway for Releases 12 and 13. Profiles are being developed for LTE networks and equipment to operate at 450 MHz, 700 MHz and 800 MHz, along with support for DMO, group communications, push-to-talk and communicating on impaired/damaged networks. These specifications should be delivered between the end of 2014 and the first quarter of 2016 so products based on the new standards could be ready for introduction in the 2016-2018 time frame. But even then, ECO notes, “It will take still a few years before PPDR functions have been fully specified, implemented, tested and integrated into the LTE solutions from most vendors” (Gulyaev, 2014).

---

[44] 3GPP (2014) “Mission Critical Push to Talk MCPTT”, TS 22.179 V0.6.0, Release 13, http://www.3gpp.org/ftp/specs/archive/22_series/22.179/22179-060.zip

.

But by 2020 LTE could be a practical alternative to TETRA, TETRAPOL, ASTRO/P25, etc., able to meet the mission critical needs of PPDR. For the utility and transport sectors it is too soon to tell what future LTE releases will provide but there will always be communications needs for which cellular is not the right solution because of the network architecture or tariff structure.

Yet as we saw with GCSE a key question remains: "how much functionality should be 'baked in' to the LTE infrastructure and how much should be delivered by non-standardised application servers. The use of application servers will allow different organizations or regions to customise the system operation to their own needs whereas 'baked in' solutions may be more efficient and simpler" (Sharp, 2013). The split between standardised and customised solutions also affects how much sectoral spending on mobile communication support goes to cellular networks and how much goes to "over the top" service providers.

Because the public safety market is small, relative to the size of the MNOs' public customer base, and because LTE's feature set is shaped mainly by the need to generate revenue, 3GPP's willingness to cater to the needs of public safety must be based on an assessment that this group can and will pay premium prices for special features, or that some special features for public safety may support new products and services for the general public as well. The time and effort put into ensuring that charging data can be captured for DMO shows how much revenue matters. Adding demanding features that only a few customers need raises costs for everyone so it is important to find the right balance between desirable options and essential requirements.

3.2.2 Deployment

Cellular network operators had hoped the improvements in user experience offered by LTE would let them charge premium prices. That is not proving the case, at least in Europe, and it seems to be slowing the pace of LTE buildout.

According to Kim (2014), LTE is offered in France with no premium over other 3G services and Europe now has the lowest average pricing for LTE of any region ($34.89 per month).[45] Since LTE networks are costly and there is "little direct revenue upside" (Kim, 2014), deployment plans are being stretched out. Analysys Mason confirms that "momentum seems to be slowing" globally, with new LTE network launches peaking in 2012 and declining ever since (see Figure 3.4). Regulators in Austria, Bulgaria, Croatia, France, Hungary, Luxembourg, Poland, Romania, Slovenia and Sweden report no new market demand for the 2.6

Figure 3.4. New LTE network launch rate declining since 2012

Source: Analysys Mason, 2014.

[45] Kim, G. (2014) "Europe has lowest LTE retail prices: good for consumers, not service providers", *Information age,* 7 January, http://www.information-age.com/technology/mobile-and-networking/123457567/europe-enjoys-the-cheapest-4g-lte-tariffs-in-the-world

GHz band while Bulgaria, Malta and Portugal report no new demand for 1.8 GHz (SWD[2014] 249 final, p. 15).

So even if the right capabilities are in the standards, cellular customers' willingness to pay seems to be limiting the rate at which commercial LTE spreads. That must raise questions about when – or even if – the coverage will be expansive enough to meet the needs of first responders. That could be changed by networks at 400-800 MHz.

3.3 Bands currently harmonised for wireless broadband

The bands currently harmonised for wireless broadband in Europe are of two types: licensed and license exempt.[46] Broadband is delivered in license exempt bands mainly by systems conforming to the IEEE 802.11 standards. The harmonised frequency ranges are:

2400–2483.5 MHz 5150–5350 MHz 5470–5725 MHz 57–66 GHz

CEPT has been mandated to study the feasibility of adding 5350–5470 MHz and 5725–5925 MHz to the WAS/RLAN allocation (Radio Spectrum Committee, 2013b). That would create a continuous span from 5150 to 5925 MHz, permitting very wide channels and great flexibility in how the frequencies are used. But it could also cause interference to incumbent systems (radars mainly) and discourage the development of ITS safety systems at 5875–5905 MHz. Since CEPT's report on this topic is not due until spring 2015, it is not known what they will recommend.

The proposed bands for Broad Band Disaster Relief (BBDR) applications are also relevant to this study. These are recommended for agencies and organisations dealing with large-scale disruptions of social functions (ECC/REC/[08]04). Using WAS/RLAN technology on a no-protection/no-interference basis, BBDR equipment can be deployed where and when needed, with or without links to other PPDR systems. Two frequency ranges have been proposed for BBDR operations: 5150–5250 MHz and 4940–4990 MHz. The first is part of the public WAS/RLAN allocation, so BBDR does not have exclusive access; however, interoperation with public networks is a potentially useful condition. WRC-12 harmonised the second frequency range for ITU Regions 2 and 3, but in Europe this is an exclusive military band. Possibilities for civilian use in NATO countries are limited.

In November 2013, Decision ECC/DEC/(13)03 harmonised the use of 1452–1492 MHz for Mobile/Fixed Communications Networks Supplemental Downlinks (MFCN SDL). MFCN SDL is defined as:

> "a mobile broadband system, which by means of base station transmitters in the network, uses unpaired spectrum in the downlink to provide a supplemental downlink capacity to carry comprehensive text, audio, images, data, sound and video content in general, in a unicasting, multicasting or broadcasting mode to mobile devices" (CEPT Report 54, 2014)

In other words, it is a supplemental overlay facilitating faster delivery of audiovisual and other large-volume unidirectional data streams to mobile devices, perhaps using carrier aggregation with two-way cellular bands. RSPG has recommended the adoption of "complementary measures to further promote the use of this band for SDL, while preserving the possibility for Member States to use part of this band for other uses such as broadcasting" (RSPG13-521 rev.1, 2013). This band was previously allocated for digital audio broadcasting via satellite and terrestrial stations. Given the intended uses, PPDR, utilities and ITS may find this band inappropriate to their needs.

[46] Because the underlying subject of this study is mobile broadband, spectrum allocations for fixed broadband are not considered in this section.

3.3.1 Commercial cellular bands

Since LTE is allowed now in any band designated for commercial mobile, the following licensed frequency ranges can be considered harmonised for mobile broadband:

880–915 MHz	1805–1880 MHz	2110–2170 MHz
925–960 MHz	1900–1980 MHz	2500–2690 MHz
1710–1785 MHz	2010–2025 MHz	3400–3600 MHz

In addition, the following licensed bands were designated for mobile cellular at WRC-07:

450–470 MHz 790–862 MHz 2300–2400 MHz

However, those new bands are not fully cleared so the presence of incumbents limits cellular usage:

> Delays in assignment of the 800 MHz band are the main obstacle to 4G development. The 1800 MHz band remains the most used band to deploy LTE (in more than 20 Member States), while the 2,6 GHz band is used in 19 Member States... In a few Member States operators also provide LTE in the 900 MHz band, although this band is still mostly used for GSM… (SWD[2014] 249 final, p. 15)

If PPDR, utilities or the transport sector wish to subscribe to commercial networks for their communications needs, then no additional authorisation is needed for them to start. Lower frequency bands suit most sectoral needs better than higher because of superior propagation, building penetration, smaller "radio shadows", and so on. Commercial mobile, on the other hand, prefers higher frequency bands because these interact more efficiently with the small hidden antennas of smartphones and tablets and the shorter signal range allows more base stations to fit within a smaller area to provide more capacity.

So in the context of public mobile use by the three sectors, the lowest available bands (790–862 MHz and 450–470 MHz) are of greatest interest even though they are not commercially significant yet – along with the 700 MHz band as a near future possibility.

3.3.2 400 MHz

The 450–470 MHz range is particularly attractive for public safety broadband because it has already been designated for both PPDR and cellular mobile networks. In addition, ECC Decision (08)05 indicated that bandwidth for PPDR data communication could also be made available at 410–430 MHz. (That range has not been designated for cellular but presumably it could be.)

The 400 MHz frequencies are close enough to the current public safety band at 380–400 MHz that radio propagation is similar. That means the existing signal coverage might be approximated at either 410–430 MHz or 450–470 MHz by repurposing TETRA antenna masts and base stations for LTE, reducing both the cost of build-out and the waste of prior investments. (Commercial TETRA networks in Europe often use 410–430 MHz or 450–470 MHz so they would find it easy to migrate to LTE 450, too.)

In Section 3.2.1 it was noted that Brazil awarded the first LTE license for 450 MHz, even though no equipment had yet entered the market. That prompted 3GPP to develop a new technology profile for this band. Brazil's communications ministry then licensed a second carrier for nationwide LTE 450 service and investments totalling $450 million are planned to cover 1,611 cities, 14 states and 91.5%

of the rural population by the end of 2015.[47] According to the ministry's director, LTE 450 is the "only economical way" to deliver mobile broadband across vast, sometimes sparsely populated areas, as base stations have up to 30-50 km range. He foresees this band as also having "strong use applications for public safety, M2M and many other fields".[48]

Brazil may have been first with licenses, but Huawei and UkkoVerkot (a mobile data service provider with a nationwide CDMA network in Finland) are actually the first to deploy a commercial LTE 450 MHz network. They plan to cover all of Finland by the end of 2014 simply by updating UkkoVerkot's 241 base stations, which already cover 99% of the population. Apparently all they have to do is replace the CDMA 450 channel card: the existing radio units and antennas will be re-used. The system will be broadband only (no voice calls) and will target "demanding customer segments like businesses, field and home workers, authorities and transportation industry". Average download speeds are expected to be 3-10 Mbps. Upload speeds will average 1-3 Mbps with a maximum of 6 Mbps.[49] Meanwhile, the Dutch utility Alliander bought 450 MHz spectrum rights from KPN and then hired the firm to build and manage a dedicated CDMA network for smart grid applications.[50]

A 450 MHz Alliance has been established to promote the band, now that LTE 450 has brought fresh attention to it.[51] But it is still not clear if cellular networks for public subscribers will develop in this band or if the future lies in dedicated networks. In Brazil, the first offer of 450 MHz licenses for public cellular attracted no bids because extensive coverage obligations were attached. It was not until the government offered tax exemptions that commercial operators became interested.[52]

Twenty MHz is the minimum spectrum requirement for PPDR broadband according to ECC Report 199 (2013). The 410–430 MHz and 450–470 MHz bands are each that wide. However, the availability of spectrum within these bands is constrained by the need for a duplex gap and block edge masks or buffers to mitigate interference. For that reason only 2 x 5 MHz is actually allowed for data transmission at 430–450 MHz in Brazil (Rocha *et al*., 2013). If both 410–430 MHz and 450–470 MHz could be used, that would be sufficient, but about half the NRAs responding to a recent FM 49 questionnaire "do not see any possibility of making frequencies in the 400 MHz range available for BB PPDR LTE networks…"[53] The other half see only limited possibilities in the more distant future, because these bands are intensively used by government agencies and land mobile PMR networks, which would have to be moved, bought out or protected. Of the two bands, 410–430 MHz would be harder to repurpose, regulators say. In 2015 the CEPT Work Group on Spectrum Engineering (WG

---

[47] Ministério das Comunicações (2014) "Ministério autoriza R$ 450 milhões em projetos", 6 August, http://www.mc.gov.br/telecomunicacoes-noticias/31841-ministerio-autoriza-r-450-milhoes-em-projetos

[48] The director mentioned that Motorola and EADS helped develop the 450 MHz profile for LTE Release 12, suggesting early commercial interest in the possibility of public safety use of this band. Gontijo, J. (2014) "LTE 450MHz in Brazil", presented at the LTE450 Global Seminar, Amsterdam, 25 June, http://450alliance.org/wp-content/uploads/2014/08/LTE450-Global-Seminar-Meeting-notes.pdf.

[49] UkkoVerkot (2014) "Truly nationwide LTE network in Finland", presentation at LTE World, http://450alliance.org/wp-content/uploads/2014/07/UkkoVerkot_Amsterdam_LTE_World.pdf; Haaramo, E. (2014) "Where in the world has the best 4G coverage, even for the remotest spots?", ZDnet.com, 6 June, http://www.zdnet.com/where-in-the-world-has-the-best-4g-coverage-even-for-the-remotest-spots-7000030286/; "World's first commercial LTE 450MHz Network in Finland", *4G Portal,* 8 July 2014, http://4g-portal.com/worlds-first-commercial-lte-450mhz-network-in-finland

[50] De Groot, P. (2014) "KPN and utilities", presentation for the EUTC, http://www.eutc.org/sites/default/files/public/UTC_Public_files/kpn.pdf

[51] http://450alliance.org

[52] TeleGeography (2014) "LTE-450 projects approved, worth USD197m", *CommsUpdate,* 8 August, http://www.telegeography.com/products/commsupdate/articles/2014/08/08/lte-450-projects-approved-worth-usd197m/

[53] "ECO summary of replies to the FM49 questionnaire to CEPT administrations on the European availability of the 400 MHz range for broadband PPDR LTE networks", Meeting Document FM49(14)003rev1, Annex 2, http://cept.org/DocumentRevisions/fm-49---radio-spectrum-for-public-protection-and-disaster-relief-(ppdr)/4812/FM49(14)003rev1_ECO%20summary%20of%20replies%20to%20FM49%20questionnaire%20on%20400%20MHz

SE) will launch a new study on the feasibility of deploying PPDR LTE networks in the 400 MHz band.

In Section 3.3.3 we discuss multi-band aggregation. Even if 400 MHz does not have enough available bandwidth to be a complete solution, whatever bandwidth is available there could be aggregated with spectrum at 700 MHz or used as a broadband supplement to TETRA at 380–400 MHz, at least in some countries. The latter option would require dual-mode/dual-band "hybrid" terminals, but such devices have already been demonstrated.

3.3.3 2300 MHz

Use of this band varies across Europe. In some countries it is primarily military, used for training, flight tests and aeronautical telemetry. In other countries it is used for CCTV and Services Ancillary to Broadcasting (SAB): wireless video cameras and microphones. But harmonised conditions for cellular use of the 2300-2400 MHz band were agreed at the ECC meeting in June 2014:

> This Decision applies the Least Restrictive Technical Conditions (LRTC) for efficient frequency use, centred on the block edge mask (BEM) concept, which are as technology neutral as possible. The LRTC are intended to allow coexistence between MFCN applications in the 2300 - 2400 MHz band and to ensure coexistence with systems above 2400 MHz, e.g. with RLANs.
>
> This band is rather different from others where similar initiatives have been applied, because of a range of important incumbent services in limited but specific parts of Europe. The ECC understands the importance of coexistence with other users of this band and this Decision identifies Licensed Shared Access (LSA) as the recognised approach for Administrations wishing to introduce MFCN while maintaining current and long-term incumbent use. ECC intends to develop further guidelines to aid Administrations in developing an appropriate sharing framework for coexistence between MFCN and incumbent services and applications at the national level.[54]

A public consultation on these proposals has just ended but the results have not yet been published.

3.3.4 Multi-band aggregation

The fact that the 2.3 GHz band is adjacent to the 2.4 GHz Wi-Fi band makes it easy to deploy LTE systems with "carrier aggregation" so that license exempt bandwidth can be combined with licensed bandwidth to deliver larger volumes of data. 3GPP calls this technique "Licensed Assisted Access". It is not actually necessary for the aggregated bandwidths to be near each other in frequency and licensed bandwidths can be aggregated, too (eg 900 MHz + 1800 MHz, 450 MHz + 2600 MHz, etc).

Two points are worth noting here: one is that the use of license exempt bandwidth by commercial LTE networks is likely to become common, both as a supplement and an alternative to licensed spectrum,[55] and two, the LTE subscriber will in general not be able to tell when part or all of their communications bandwidth in a particular session is unlicensed. The recent announcement of a successful aggregation of 5 GHz WAS/RLAN spectrum with LTE operating in lower bands shows that the distinction between licensed and license exempt bandwidth is eroding quickly in cellular practice, while aggregation erodes the distinctive profile of any band, licensed or exempt (Docomo, 2014).

[54] ECC (2014) "37th ECC Meeting, Aarhus, Denmark, 24-27 June 2014", press release, http://www.cept.org/ecc/37th-ecc-meeting,-aarhus,-denmark,-24-27-june-2014

[55] 3GPP organised a workshop on "LTE in Unlicensed Spectrum" last June. This is a link to a summary and all the presentations: http://www.3gpp.org/news-events/3gpp-news/1603-lte_in_unlicensed

Aggregation will have a profound impact on spectrum management in the future, increasing dynamic formations of bandwidth into virtual channels and undermining band-specific service allocations.

3.4 Potential future bands for mission critical broadband

Future bands for mission critical broadband can only be found among the bands already used for broadband – discussed in the previous section – or bands that could be used for that purpose. The "RSPG Opinion on Strategic Challenges Facing Europe in Addressing the Growing Spectrum Demand for Wireless Broadband" (RSPG13-521) analysed all frequencies between 400 MHz and 6 GHz, and:

> identified the steps which need to be taken (the roadmap) to make particular frequency bands available for wireless broadband... A consequence of this is that 1701.5 MHz of spectrum can be identified as being already available for wireless broadband with a further 140 MHz identified with the potential to become available in the near term (by 2015) and 886 MHz having been identified as spectrum with potential to support broadband applications in the medium term (i.e. beyond 2015).

The bands with "the potential to become available in the near term (by 2015)" are 1452‐ 1492 MHz and 2300–2400 MHz. Both are discussed in Section 3.3. The bands said to have "potential to support broadband applications in the medium term" are:

694–790 MHz	1375–1400 MHz	1427–1452 MHz	1880–1900 MHz
3800–4200 MHz	5350–5470 MHz	5725–5875 MHz	5875–5925 MHz

The frequency ranges with a white background are discussed elsewhere in this report; here we comment on those highlighted in green:

1375–1400 MHz: This band is currently used by defence systems and long-hop, low-data-rate fixed point-to-point links with narrow channels (25 or 50 kHz). In some countries it is used by broadcasters for programme making (wireless cameras). But: "This band is essential for NATO, specifically for long range and high resolution radars and terrestrial radio relay. NATO nations operate radars using this band as part of the NATO Integrated Air and Missile Defence System…"[56]

1427–1452 MHz: Use is similar to 1375–1400 MHz but NATO does not considered it essential for radar. However, 1400–1427 MHz is allocated to the Earth Exploration-Satellite, Radio Astronomy and Space Research services on a coprimary basis. Any wireless broadband deployments in the adjacent bands (1375–1400 MHz and 1427–1452 MHz) must strictly limit their out-of-band emissions to a level ensuring protection of passive services. That could be a problem for LTE, yet CEPT may propose 1427–1452 MHz as a new candidate band for cellular mobile at WRC-15 anyway. If it is identified for cellular, it could be considered for PPDR broadband as well, though for hot-spot capacity boosts rather than wide area coverage.

1880–1900 MHz: This is the original DECT cordless phone band. While sales are declining, millions of handsets are still in use throughout Europe. But with only 20 MHz of total bandwidth, this band is too small to support the PPDR broadband requirement.

---

[56] CEPT CPG PTD (2014) "Possible candidate band in L band: scenario to be considered", Meeting Document CPG-PTD(14)169, http://www.cept.org/Documents/cpg-pt-d/17637/CPG-PTD(14)169_France_Possible-candidate-band-in-L-band-scenario-to-be-considered.

3800–4200 MHz: Compatibility studies for this band were presented in ECC Report 100 (2007). This is part of the Fixed Satellite Service C-band, still used to some extent in Europe, more so in Africa. Even with protection zones around satellite earth stations, making it available for mobile broadband would augment the already identified spectrum at 3400–3600 and 3600–3800 MHz creating a very large contiguous band where 100 MHz channel widths would be possible. This could emerge as an important band for LTE, particularly in cities.

In 2011 CEPT's Electronic Communications Committee established a new project team on radio spectrum for PPDR: FM49. Their main task is to identify harmonised frequency bands for future European public safety broadband systems. The candidate bands they have identified so far are 410–430 MHz, 450–470 MHz, 694–790 MHz, 1900–1920 MHz and 2010–2025 MHz. The first two were discussed in Section 3.3.1; the third frequency range is discussed in the following section, and the last two are discussed in Section 3.4.3.

3.4.1 700 MHz

Like most of the world, FM49 was surprised by the tabling of a proposal at WRC-12 to allocate the 694–790 MHz band to mobile services in ITU Region 1 (the EU is in Region 1). In the end, the Conference decided to identify this band for mobile and broadcasting services on a co-primary basis after the next WRC at the end of 2015. That may seem like a reasonable compromise but the reality, as Pascal Lamy noted in the High Level Group report on future uses of UHF, is that for "conventional mobile networks to have access to this band, terrestrial broadcasting networks would have to clear it because both types of networks cannot coexist in the same frequency band with today's technology" (Lamy, 2014).

Perhaps surprisingly, the WRC-12 proposal came from the Arab and African nations, not from mobile operators: "European operators were not in [a] rush for the 700 MHz allocation, as they are still in the process of launching their services in the 800 MHz" band (El-Moghazi *et al.,* 2014, p. 6). Operator caution and the FirstNet project in the USA created an opening for PPDR. In February 2013, the EC mandated CEPT to develop the least restrictive harmonised "technical conditions for the introduction of wireless broadband in the 700 MHz band… while also taking into account other priority areas of EU spectrum policy such as public protection and disaster relief (PPDR)…" (Radio Spectrum Committee, 2013a) This is now the "most supported range for BB PPDR (WAN) as discussed in FM 49" (ECC, 2014b).

The RSC mandate recognised that any "common regulatory action at EU-level should be guided by an EU-level political agreement on the long-term use of the 700 MHz band… [Therefore the] exploitation of the results of this mandate does not necessarily entail the development of a technical implementation measure under the Radio Spectrum Decision". In other words, the Commission wanted FM49's advice on what arrangements make sense from a technical perspective, not a decision on what to do about DTV or PPDR or whether public or dedicated networks should provide 700 MHz LTE. Answers to the more challenging questions must be based on a vision of the UHF band's long-term future – which is still being developed – and the requirements and preferences of individual Member States – which are also still forming. So "flexible harmonisation" is the immediate goal, to enable each country to decide how much or how little spectrum to provide for PPDR, DTV, mobile broadband and other applications like PMSE and M2M in the 694–790 MHz frequency range.

The recent High Level Group report on the future of UHF proposed "a compromise which foresees coordinated repurposing of the 700 MHz band to mobile services while linking it to reassurances for the sustainable development of terrestrial broadcasting in spectrum below the 700 MHz band" (Lamy, 2014). But divisions within the Group mean that there is no consensus proposal on the pace of transition to mobile use (despite Lamy's suggested "deadline" of 2020 plus or minus two years), nor on a common European position for WRC-15 regarding future use of UHF.

Nevertheless, CEPT Report 53 (currently still only a draft) provides a "preferred channelling arrangement" for the 700 MHz band. The proposal is compatible with the lower duplex part of the Asia-Pacific Telecommunity's plan because "inter-regional harmonisation" promotes economies of scale thereby reducing equipment costs and making roaming easier.

Figure 3.5. 700 MHz options considering PMSE, PPDR and other services on a national basis

694-703	703-708	708-713	713-718	718-723	723-728	728-733	733-738	738-743	743-748	748-753	753-758	758-763	763-768	768-773	773-778	778-783	783-788	788-791
							Duplex Gap											
Guard band (1)	Uplink						Gap (1)	SDL (1)				Downlink						Guard band (1)
9 MHz	30 MHz (6 blocks of 5 MHz)						5 MHz	20 MHz (up to 4 blocks of 5 MHz)				30 MHz (6 blocks of 5 MHz)						3 MHz

(1) The usage of the guard bands and of the duplex gap of the paired band plan (733-758 MHz) is considered for national options described hereafter to respond to market demand on PMSE, PPDR, M2M.

Source: CEPT Report 53, 2014.

"Flexible harmonisation" in this context means sub-band boundaries in national allocations are allowed to differ within a shared "tuning range", using 5 MHz channels as building blocks and LTE as a shared enabling technology. A common technology and tuning range mean the same equipment can be used throughout Europe even if the frequencies authorised for particular purposes vary from country to country. Since the bandwidth available for MFCN would be 2x30 MHz (and up to 20 MHz for Supplemental Down Links, identified as "SDL" in Figure 3.5), that could accommodate both PPDR and public cellular subscribers, as well as PMSE and M2M.

The ECC is now studying a proposal to authorise PPDR use of the 733–758 MHz duplex gap and perhaps the 694–703 MHz and 788–791 MHz guard bands while public cellular systems use the up- and downlink blocks. According to the *ECC Newsletter*,

> The likely density of deployment of PPDR and its different dynamics compared with general public mobile services could make such an arrangement achievable with relatively little opportunity cost to other services, or constraints to PPDR. However, there would, at least in principle, be a risk of pre-emption of use of the band, including below 694 MHz... Of course that would still be subject to the relevant coordination with neighbouring countries, which is a significant practical constraint, but a different issue. (Thomas, 2014, p. 4-7)

ECC Report 218, due in 2015 and now being finalised, considers the needs of specialised applications and service delivery options for PPDR broadband – commercial, dedicated and hybrid networks in various configurations. Since service delivery options are explored here in Chapter 4, it may be sufficient to note that our study offers a complementary perspective, emphasizing economic aspects.

3.4.2 800 MHz

Report ITU-R M.2033 on "Radiocommunication objectives and requirements for public protection and disaster relief" (2003) identified 794–806 MHz and 806–869 MHz for PPDR operations while also recognising CITEL's regional designation of 821–824 MHz and 866–869 MHz for PPDR in the Americas. Resolution 646 (WRC-03) similarly encouraged countries in ITU Region 3 (Asia) to consider 806–824 MHz and 851–869 MHz for “achieving regionally harmonized frequency bands/ranges for advanced public protection and disaster relief solutions”.

So there is ample precedent for the harmonised use of 800 MHz by PPDR elsewhere in the world. According to the chairman of FM49, the Law Enforcement Working Party of the European Presidency (LEWP), the UK and Swedish governments and 4 companies in the mobile industry support PPDR broadband in the 790–862 MHz band as an option for PPDR organisations in Europe which have signed contracts with the MNOs. Because they plan an early migration from TETRA to LTE, the UK in particular sees 800 MHz as a necessary interim solution. FM49 considered proposing the addition of 800 MHz to the list of bands designated for PPDR in Region 1 when Resolution 646 is updated at WRC-15, but opinion among the FM49 members was divided. In the end the matter was left for WG FM to decide.[57]

3.4.3 2000 MHz

Future PPDR use of 1900–1920 MHz and 2010–2025 MHz was recently proposed by FM49. Draft CEPT Report 52 (2014) suggests these bands might be used for high-capacity, temporary and localised event-related deployments, either where the existing public safety network cannot handle all the traffic or where there is no public safety network coverage. The suggested use case is real-time transmission of video and still photos, including downlinks from helicopters and drones. Only limited deployments are possible in these bands because they are already used by licensed cellular networks in some areas. (Instead of PPDR as a cellular “client”, in these bands they would be rivals.) Other applications may be permitted in these bands, too, including wireless microphones and cameras for news professionals covering the events where PPDR is present. Coexistence between PPDR and Services Ancillary to Broadcasting (SAB) could be problematic. An EC consultation on possible uses for these bands showed limited support for PPDR; more interest was expressed in building a region-wide Direct-Air-to-Ground Communications Network to support inflight internet and multimedia delivery. Such a network would require a regionally harmonised allocation whereas Member States could individually decide to authorise ad hoc video surveillance.

3.4.4 Other future possibilities

Although it will be for the Member States to decide, opening the 700 MHz band could make a very significant contribution to meeting the needs of PPDR and the general public for mobile broadband and other forms of wireless connectivity. Other frequency ranges now allocated for PMR, fixed or mobile satellites, commercial cellular and license exempt applications could also be usable to varying degrees. So it may be time to start shifting attention from where to find more bandwidth to how best to use it – which networks are most cost effective and reliable, how soon will they be available, what is a acceptable price and how to pay?

Meanwhile, work will continue on re-adjusting the supply of spectrum to satisfy current and future demand. The RSPG has already starting looking toward renewal of the Commission’s Radio Spectrum Policy Programme (RSPG14-553 final). Their most relevant proposal is to consider “best practices on the duration and timeline for potential new bands that could be made available for WBB in the short and medium term including relicensing of frequency bands already harmonized”.

WRC-15 will revise PPDR focused Resolution 646 (WRC-03, rev. WRC-12), probably adding new frequency bands to reflect growing interest in broadband and the clarification of options since WRC-

[57] CEPT (2014) “FM49 progress report to WGFM#79 meeting”, Meeting Document FM49(14)012, 26 February, http://www.cept.org/Documents/fm-49/16192/FM49(14)012_FM49-progress-report-to-WGFM79-meeting

12. New bands will also be identified for IMT, the ITU's name for the family of cellular mobile technologies. Any new bands identified for both PPDR and IMT will realign European thinking about options for mission critical broadband.

Practical solutions to the problem of self-interference (which makes duplexing necessary for two-way communication) are leading to the introduction new products which claim to be able to transmit and receive on the same frequency (Choi *et al.*, 2010; Ahmed and Eltawil, 2014). The 700 MHz band plan offered by CEPT in Report 53 shows how wasteful duplexing is and if the new devices work as claimed, the amount of spectrum available to all FDD systems will effectively double. This has yet to be factored into the thinking of regulators – and standards developers – because a large demonstration system has not yet been built.[58] But if and when it is, self-interference cancellation is likely to have enormous impact on spectrum management, as great or greater than bandwidth aggregation.

The EC-funded METIS 2020 research project aims to increase 5G's spectrum efficiency a thousand fold[59]. They are exploring specific application areas which take into account some of the sectors of concern here: teleprotection in smart grid networks, massive arrays of sensors and actuators (as used by utilities and ITS) and traffic efficiency and safety. METIS is already preparing for WRC-18/19 in its standardisation efforts.

Thanks to breakthroughs like self-interference cancellation and projects like METIS, in a few years work on 5G cellular will start to define new approaches to mobile networking and establish new equipment requirements. As current thinking about the needs of PPDR, utilities and ITS revolve around LTE, there will be a need to reassess the relationship between LTE and 5G in light of the requirements of "mission critical" communications in the three sectors. The concept of heterogeneous networks ("hetnets"), explored in Chapter 4, could be a bridge, preventing lock-in to any particular technology, standards version or frequency band, while honouring the promise explicit in the name "Long Term Evolution".

---

[58] Dyer, K. (2014) "Commercialised Full Duplex radio by next year claims Kumu Networks founder", *The Mobile Network,* http://the-mobile-network.com/article/Mjg3/Commercialised-Full-Duplex-radio-by-next-year-claims-Kumu-Networks-founder.html#sthash.BOwU8Pxj.dpuf

[59] https://www.metis2020.com/

4 Estimating Costs and Benefits of Wireless Communication Needs

4.1 Comparison of five possible options

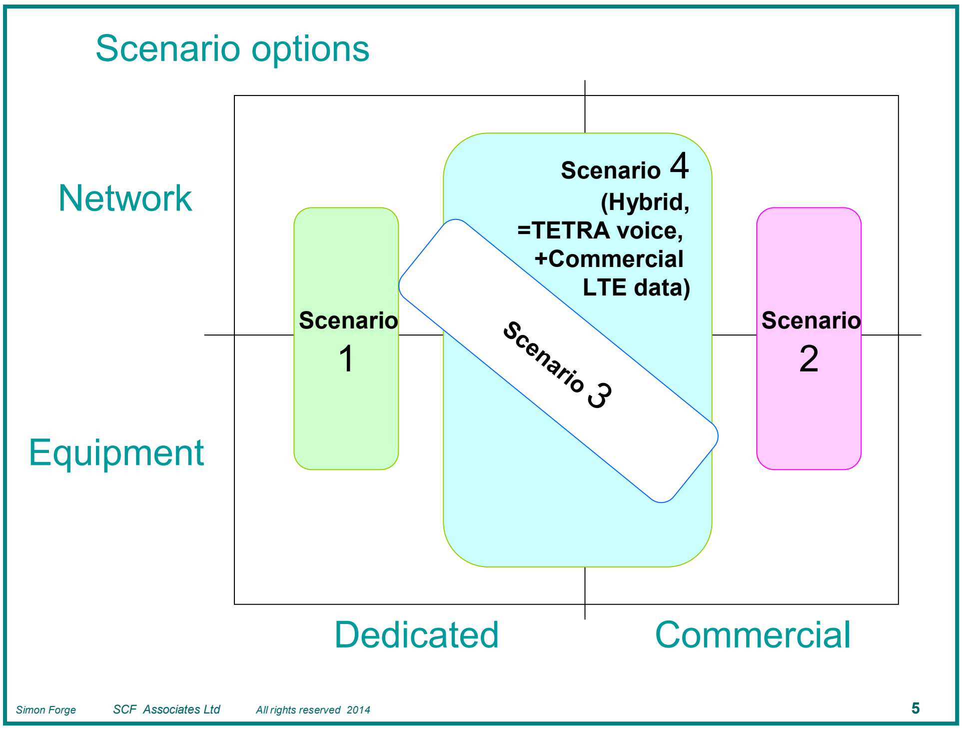
4.1.1 Objective of the comparative analysis of the network options

In this part of the study, scenarios are used to explore the potential costs and benefits of meeting the wireless communication needs of PPDR, utilities and ITS, through different combinations of commercial and dedicated networks and equipment. Five alternative networking options were compared:

- Dedicated specialised networks using specialised equipment only
- Commercial networks using commercial equipment only
- Dedicated specialised networks using commercial equipment
- Hybrid solutions involving dedicated specialised and commercial networks
- An assessment of the feasibility of a common multi-purpose network for use by all three sectors simultaneously.

The options for the first four scenarios are shown below while the fifth, considering feasibility of a common multi-purpose network for use by all three sectors simultaneously, may use various combinations. It covers all of the options shown in the figure below, in one way or another:

Figure 4.1. Comparing the options in dedicated and commercial based networks



4.1.2 Approach

The overall approach adopted was to assess not just the financial cost of the infrastructure but its operational value in terms of what it actually offers the user sectors functionally, i.e. value for money. Any additional cost factors that may degrade or enhance the cost-benefit balance are also examined, for instance a small number of specialised suppliers on the negative side, or the possible reuse of high capital cost assets on the plus side. Results are examined from the point of view of the overall cost per user, in view of the functional value.

In Section 4.7, the social cost and value of such services are examined in an effort to give balance to what, up to that point, has been a purely financial discussion.

Generally, total cost of ownership of a mobile cellular radio network over the long term includes both the initial costs to build, largely capex, plus the operational costs, opex, over one or two decades as well as the depreciation of assets. That may be taken over three to ten-year amortisation, depending on the item. Major cost elements to be taken into account in any total cost of ownership analysis include (see also Table 4.1):

- Approximately (up to) 70% of any mobile cellular network is the RAN (radio access network). Much of that cost is not equipment but is the site real estate (either rented or purchased). In addition to that is the cost of wayleaves for passing backhaul ducts and cabling into the core switching network. In a major city they can be expensive. Each base station basically comprises the multiple transceivers for each sector, with the antennae and structural steel mast supports, cabling for backhaul and power, as well as the auxiliaries – the power supplies (which should be UPS) plus HVAC and security systems in their protective shelters. Some cabled fixed-line backhaul communication transmission to the core network may replace microwave.
- To connect and manage the RAN is a fixed line, core network for long distance transmission and switching. It is comprised of a hierarchy of packet routing elements and gateways to the PSTN, internet, international transit lines and directly to other mobile networks. In addition it handles activation, service control, failover, authentication and mediation for charging. These elements all require their own network equipment sites.
- Most mobile networks will have a set of business support systems (BSS) for managing the network, especially billing and accounting plus user support systems, such as customer centres of some kind with databases. All may be housed in data centres, and/or in separate customer support call centres.
- Network management using operational support systems (OSS) controlled from several Network Operation Centres (NOCs), which have a management network (TMN) for remote monitoring, set up and field maintenance.

Note that many of these functions may be outsourced to third parties, especially the ownership and management of base station sites. Other costs include overheads with finance, administration, legal, inter-operator and NRA negotiations and some operators include marketing costs, inter-operator mobile termination charges (MTC) and the spectrum licence fee. In the costs analysed here, the cost of network rollout concentrates on the first two major items (principally capex) to create the network, although the opex over one or two decades may well exceed that, especially for maintenance teams on a three-shift basis, 24x7x365.

4.1.3 The opportunity cost of spectrum is a further cost element to consider

Across all of the scenarios an extra cost enters, either to be added in some options or avoided in others. Dedicated networks require dedicated spectrum, which has a value or opportunity cost that should be considered, even if donated by governments as a free grant. The question of shared spectrum bands against exclusive use of spectrum for the three sectors would introduce the concept of additional costs for the value of that exclusivity. If a reserved band of spectrum is put forward for these users (or just for one such as PPDR) then an opportunity cost could be used to assess its value and to justify such an award.

It would be based on the average price paid at auction for mobile spectrum in the commercial market, which varies widely by Member State. Additional annual charges for the spectrum licence, as required in many Member States, would be added to this, to give a ten-year cost. An alternative option is that exclusive spectrum should be paid for by its users, as already is the case for some users in some Member States, for instance for rail for GSM-R in some countries.

In general, charging for spectrum in this manner would be a national level decision, as in this area the European Commission can only recommend, not mandate. However, given that the other costs of these networks, such as real estate and hardened equipment, generally are much more expensive, spectrum may form a relatively small element of total costs.

Table 4.1. The major cost elements in a high resilience mobile network

CAPEX Elements

- Sites for outside plant - base stations (eNode B), the IP packet switching gateways and routers, NOCs, etc, with back-up sites as needed – leased or purchased
- Network elements: outside plant, gateways and internal cabling, with back-up dual units – purchase
- Civil works and cable laying for backhaul and core network
- Civil works for site build, mast erection etc.
- Power supply infrastructure and HVAC - adapt what already exists or build
- Handsets and vehicle terminals (specialised or generic); installation of vehicle units
- Wayleaves for backhaul and core network ducts, with alternative routing
- Data centre with infrastructure, equipment and software licence purchases
- Business support systems (BSS) – purchase or develop
- Spectrum licences (if applicable - if payable with annual fees, then under OPEX, as well)
- Operational support systems (OSS) network management with NOCs and telecommunications management network - purchase and deploy
- Back office and front office centres and equipment (legal, accounting) - purchase & implement

OPEX Elements

- Cost of capital
- Operational, maintenance, maintenance teams 24x7, design and development staff / HR cost
- Power: supply infrastructure, & HVAC with UPS 5 days; operation with mains supply charges
- Maintain, operate, manage network, outside plant, gateways & internal cabling, all 24x7
- Data centre infrastructure and operations, equipment, software maintenance, energy costs and annual software licences
- Operate administration, back office (payroll, legal, accounts), front office ('sales', etc) with all staff costs.
- Operational costs of hardening including extra security, power and equipment maintenance and site protection.

Naturally for each dedicated network the above profile may be different, although many of the same line items may appear as operational or capital costs, eg staffing, transceiver sites and backhaul, whether leased lines or owned. We discuss the options for such data sources in further detail below. In setting the costs of a network, Hallahan & Peha (2010) have examined costs of the various alternatives for the nationwide public safety wireless network in the USA. They showed that costs of emergency networks change by adjusting eight key parameters and so mission critical networks are quite similar to commercial mobile networks in operation. Major impacts come from variations as shown in the table below.

Table 4.2. The basic costing parameters for mission critical networks

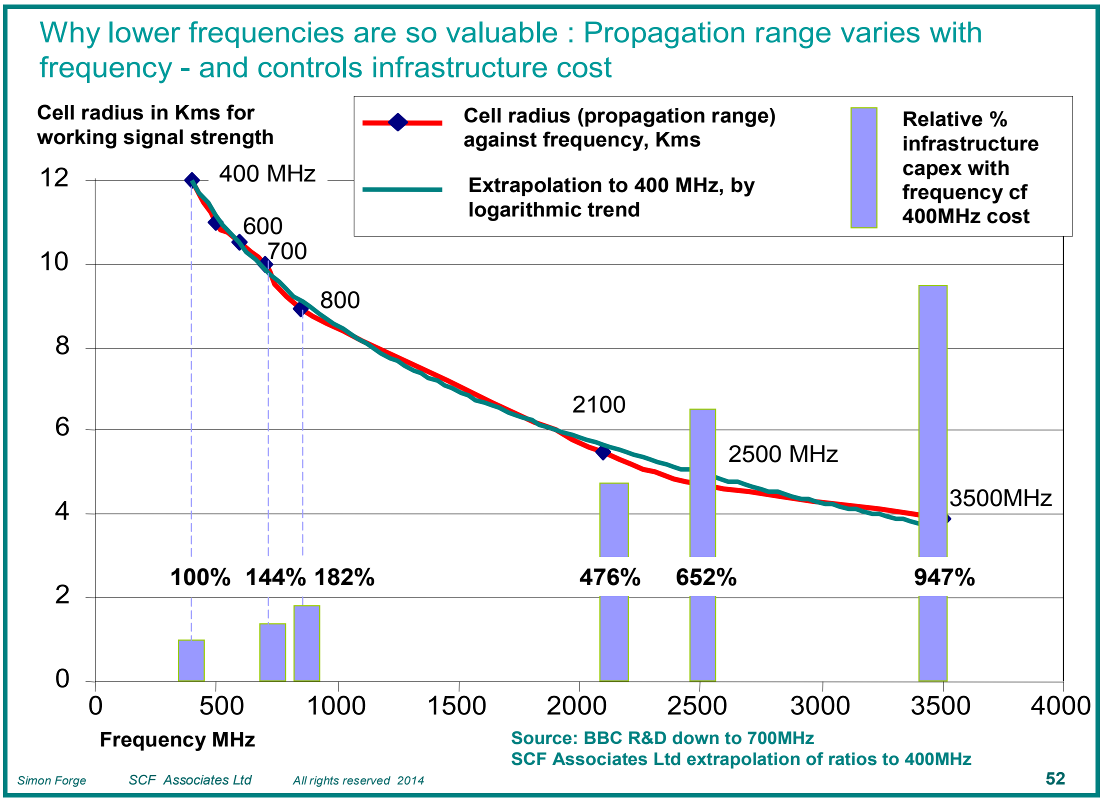
Parameter	***Impacts***
1. Frequency band	Sets range and thus cell density[60] with the overall network costs
2. Coverage area	Varies by country and sets capex and opex levels
3. Signal reliability	Requires higher quality network, perhaps higher cell density and improved transceiver design, possibly channel aggregation
4. Building penetration margin	May demand higher cell density, higher power and/or improved receiver sensitivity and thus increases costs
5. Aggregate capacity required	Affects specification of base station transceiver in bit rate, channels, signal strength and number of cell sectors to meet peak traffic demands in an emergency for an expected number of users
6. Highest user data rate	Affects specification of transceiver and cell size and thus costs
7. Population/area	Affects cell size required and overall costs and for mission critical functions, the emergency capacity required
8. Build-out requirements short term and longer term	Limits on fraction of the geographic area to be covered and/or the fraction of the population covered for a progressive build – higher densities of populations will require more cells and so increase implementation costs.

These are the major factors that impact investment and operating costs. Perhaps the most important is the first, in that wave propagation characteristics depend on the frequency. Lower frequencies are more suitable for large cells and for providing indoor coverage. Higher frequencies are more suitable for small cells, in order to provide more capacity.

The relative investment costs for capex for an area to have coverage are shown in Figure 4.2, compared with a TETRA network at 400 MHz.

[60] Reducing the operating frequency from 2.6 GHz to 800 MHz reduces network capex by up to 12 times - SCF Associates Ltd (2007) "Economic Impacts of Alternatives Uses of the Digital Dividend", http://camfordassociates.com/wp.../11/DD-Final-PUBLIC-Report-v10.1.pdf

Figure 4.2. Relationship between capex and frequency for mobile networks



The estimated infrastructure capex at the common LTE frequencies around 1800 MHz is approximately 450% more than the capex at 400 MHz. At 700 MHz the capex is 44% more, while at 800 MHz it is 82% greater, although various technology and propagation interference effects, as well as antennae sizes and engineering, may be used to mitigate the differences. Note that the opex to run the network will increase nearly in the same proportion as base station density, for maintenance and 24x7 repair teams while the core network demands will also increase in the same ratio, though there may well be some economies of scale. The LTE core network (or System Architecture Evolution, in 3GPP in terminology) will be engineered to handle the volume of traffic from base stations at peak demand for a given coverage area and disposition of base stations. Thus its infrastructure must reflect the topology and number of the base stations with their expected traffic volume – including the cost of ducts, cabling, backhaul, wayleaves, packet routing etc, which mirror this. Consequently, the core network connection and topology is taken to be approximately in proportion to base station numbers. As well as a cost model exercise, the value of benefits or negative effects must be estimated, as illustrated in the table following (for a utilities non-mission critical example).

Table 4.3. Impacts of a dedicated mesh network compared with public commercial mobile

Networking service or feature	Costs	Benefits	Downside impacts or comparative losses
Provision of low speed data monitoring for electricity smart grid via commercial mobile GPRS (100 kbps and under)	For a major EU economy, with a national smart grid infrastructure, €3 billion over 20 years	Major savings in build of peak power plants due to smart grid management. Lower energy costs and consumption by 3% over 20 years. Lower GHG emissions.	Higher running communications costs by €1.5 billion over 20 years, *cf* a dedicated ad hoc SRD mesh network at 870 MHz.

Such concepts are the basis for analytical discussion on the costs/benefits of the five networking options. Our analysis makes the following assumptions:

- We omit the financial estimates of the cost impacts of network failure: eg in terms of lives lost due to non-response to an emergency, traffic congestion worsening, road accidents increasing, more electricity wasted, etc. However, we can identify potential benefits or losses qualitatively. Also we can rank the probability and relative size of the impact, positive or negative, against the network choice as part of their comparison, in a Risk Register. Thus, although we cannot credibly quantify the benefits financially of a lower crime rate, fewer peak power plants needed, less time wasted in traffic, etc, we can identify and rank them. Also we may be able to give some indicative estimates that are relevant as the probable results of more effective PPDR, ITS and utilities services.
- Benefits in the case of dedicated networks are to be defined narrowly as just the benefits of having a network designed to the users' specifications, with a limited number of identified communicators with responsible professional usage.
- The benefits of subscribing to a public network, on the other hand, would include avoiding the necessity of a large upfront investment and freedom from the burdens of network management, including repairs and procurements, plus the spectrum availability.
- It is necessary to include the benefits of high-speed broadband for PPDR, ITS, and the utilities, since it is the quest for those benefits – and the fear that existing networks might not be able to deliver them – which is causing a fundamental re-appraisal of the value of existing networks. But only certain ITS, PPDR and utilities applications need high-speed broadband. Those that do will include new applications enabled by broadband (eg sharper video for trial evidence, or better resolution for medical assessments at the accident scene by telemedicine staff), the value of which need to be weighed against additional costs in adopting new arrangements for wireless communication.[61]
- The fifth option is more complex in that it involves a common platform for all users.

4.1.4 Cost–benefit methodologies

Any approach to estimating the costs of these scenarios across the 28 Member States must use approximations because cost structures for works, real estate, and so on, vary from country to country. Producing highly accurate forecasts for each Member State is not a realistic goal. Ultimately more helpful is to take a pragmatic approach that identifies the main factors as cost centres and then builds on these. The aim is to produce a simplified model of network costs, which can be augmented for specific cases if required.

The basis of the method is that the costs of operating various combinations of networks can be broken down into a limited number of opex and capex cost elements. These are of the same category for all types of network, whatever the options chosen among dedicated and specialised or commercial options, although their actual value varies with the option. These basic cost elements are modulated by their situation as dedicated and specialised, or else, based on commercial MNO public networks and the technology used (LTE, TETRA, etc).

[61] Some guidance in quantifying such benefits is available from various sources globally, e.g. Ure, J. (2013) *Public Protection and Disaster Relief (PPDR) Services and Broadband in Asia and the Pacific: A Study of Value and Opportunity Cost in the Assignment of Radio Spectrum,* http://trpc.biz/wp-content/uploads/PPDR-_Report_16-May-2013_FINAL-2.pdf and Ford, G. S. & Spiwak, L. J. (2011) "Public Safety or Commercial Use? A Cost/Benefit Framework for the D Block", Phoenix Centre Policy Bulletin No.26, http://heartland.org/sites/all/modules/custom/heartland_migration/files/pdfs/29464.pdf

The main cost factors are based on four assumptions:

1. There are common basic cost components that can be aggregated to create more realistic estimates even when details are incomplete or unavailable. The basic capex cost items for radio network infrastructures are as outlined in Table 4.1. They include all the capex and opex items ranging from 24x7 maintenance teams to the electricity supply (a commercial 3G base station currently consumes around 4.5MWh of power annually; this may be less for LTE, so 12 000 3G base stations in one Member State consume 50GWh per annum[62]).

Again, these items can be aggregated as an approximate common standard base station opex cost, per year. The opex annual cost can be aggregated over 10 years to give a standard cost measure. The net cost per base station, opex and capex, can then be used as the network cost sizing parameter.

***2. The second assumption is that the density of base stations varies according to three standard settings by user population density*:**

Standard setting	Nominal Range from Base Station, Km
Urban	1
Suburban	2
Rural	10

Thus, the urban case has base stations with a range from the antenna of 1 km (which is an effective radius of operation for building penetration, including ferroconcrete structures). This range may be modulated by technology, so a factor to adjust range and therefore density may be included, eg for LTE at 2.6 GHz, suitable in-building reception may require a 0.5km radius.

The area covered may be calculated using these distance as radii. The question then arises of cell overlaps, so a normal mobile hexagonal cell structure is achieved rather than just touching coverage circles. This becomes essential when data rates fall quickly at cell edges (eg for higher frequency LTE, a 10 Mbps data rate at the cell centre may fall off to 200 kbps at the cell edge as signal processing cannot compensate for the decrease in received strength of emission). Such effects indicate a higher cell density is required and so a suitable adjustment factor must be included in density estimations. However, in a mission critical configuration, far greater overlap may be sought, so that if one cell fails, other cells may provide coverage with automatic failover, either by having suitable overlap as standard, or by increasing signal power to cover the failed station's outage zone. Thus ranges may be modifiable if required by local conditions.

3. ***The third assumption is that the overall national network cost can be approximated as the sum of the costs attributed per base station***, using area as the key parameter, with proportions of rural, urban and suburban adjusting the density of base stations.

It also assumed that typical numbers of handsets and in-vehicle terminals per base station can be used to factor in the cost of end-user terminals, attributing these costs to the base stations. Mobile hubs or base stations, either in vehicles, or in a backpack, for event driven extra coverage, can be added as a percentage of all base stations. But as they are rarely more than 1% to 5% of the fixed base stations, their number may be within the error range.

[62] Grant, P., and Fletcher, S., (2011) "Cut it out: how do we cut energy consumption of mobile base stations", IET, *Engineering and Technology,* Vol.6, Issue 2 .

Note that both infrastructure and terminal costs in the EU vary according to purchaser status by as much as 20% due to Value Added Tax (VAT) obligations. These may apply to network equipment and terminals procurement. While public services may be exempt from such taxes in certain Member States, thus lowering the net cost, commercial operators will not be.

4. ***The fourth assumption is that the real value of a mission critical broadband network is to be found in its social benefits*** – that is to say it should be measured, on the one hand, in terms of reduced risk of losses to society, and on the other on how this compares with the costs of building and operating such a network. Often it is only possible to make qualitative assessments of the former, with some insight into the quantitative assessment of the latter using both top-down and bottom-up analysis.

These four assumptions form the basis of cost-benefits assessment. While they do introduce approximation and thus 'best effort' calculations, they simplify the process of making estimates while enabling comparisons between options.

4.1.5 Extra conditions must be taken into account

Some conditions must be included which modify the results:

- For commercial networks, the site costs may be lower as mission critical networks will share sites with existing MNO services, although equipment may be separate
- Commercial base station sites will need to be 'hardened', which adds implementation costs and also subsequent equipment replacement cost. Such a process would include extra power supplies and adding UPS for 72 hour autonomy or more, with additional HVAC, alternative routing for backhaul, automatic failover to other base stations, possible raising of equipment to avoid flooding, etc.
- There is likely to include a deflation effect when equipment passes from early installation to commercial volume production. This may be up to 60% (perhaps more).
- The scaling of the network for more users in the EU should be considered as both the capability for broadband becomes available and with it more applications, and greater value to users and also as the cost per user comes down. Density of existing users, eg in the PPDR sector varies greatly across the EU in published figures and so scaling for larger user populations in the future is seen as prudent.

The opportunity cost of spectrum is a further cost element to consider across all of the options, either to be added or, in certain options, a cost that has been avoided.

Dedicated networks require dedicated spectrum, which has a value or opportunity cost that should be considered, even if donated by the Member State government as a free grant. The question of shared spectrum bands against exclusive use of spectrum for the three sectors would also introduce the concept of additional costs for the value of that exclusivity. If a reserved band of spectrum is put forward for these users (or just for one such as PPDR) then an opportunity cost could be used to assess its value and to justify such an award. It would be based on the average price paid at auction for mobile spectrum in the commercial market, which varies widely by Member State. Additional annual charges for the spectrum licence, as required in many MS, would be added to this, to give a ten year cost. However, an offset may be considered, in that there may be stimulation to the economy, or a social value in saved lives, that would counterbalance the pure market value at auction. An alternative option is that exclusive spectrum should be paid for by its users, as already is the case for some users in some Member States – for instance for rail for GSM-R in some countries.

In general, charging for spectrum in this manner would be a national level decision. However spectrum value for a dedicated network may form a relatively small element of total cost, compared with base station site acquisitions and hardened equipment. But even so, dedicated spectrum in general will be a much more expensive element for dedicated networks than for the commercial counterparts, where re-use of the existing spectrum is an inherent part of the commercial offering.

Note that the assumption that spectrum costs are low compared with site acquisition costs may not hold true for railways, because the base station and outside plant sites may already exist on land owned by the railway while the communications links to the sites may be provided over railway owned networks. For a network supporting all three sectors, this possibly could offer savings for all, if the rail sites can be re-used for all three mission critical sectors in a shared network.

4.1.6 The results of the comparison of the scenarios in summary

The approach above has been applied to the five options which are explored in detail in the following subsections. Note that the summary of results in the table below contains best estimates on a purely financial basis built on the information available. These estimations look to a future of a denser usage of mission critical services than today as broadband exploitation takes off. Current users from the PPDR sector total under 2 million for the whole of Europe in the official figures available (for the EU-28 plus Norway and Switzerland). The future costs anticipate a scaling to a higher density of users applied across the EU as broadband mobile use increases, driven by new applications which increase its value and so the numbers of mission critical users, with expansion into the three sectors with more capacity being given to M2M communications. The density applied is based on the user numbers in one advanced TETRA user, the UK, applied across the EU landmass. Costs of handsets and other terminals are not included.

Initial commercial mobile estimate were made for an 800MHz PLMN network for scenario option 2, because figures were available and these are shown in the table below. Research with commercial organisations who have in the past signed contracts, or are now bidding for contracts for mission critical networking has yielded only a few inputs due to their commercial sensitivity, although certain confirmatory contributions have been provided.

The net results, in terms of the cost per user, indicates that at 450 MHz, the dedicated LTE network (Option 3) is cheaper in capex alone by over 40%, but when taking opex into account over ten years, the spreading of infrastructure costs for personnel and support favours the commercial networks, even when they are at 800 MHz as shown here. Note that it is possible that suitable antenna design can somewhat mitigate these frequency effects on infrastructure cost.

However, if the dedicated LTE network of scenario option 3 is operating at 700 MHz, the commercial mobile option 2 at 800 MHz, can give a capex cost per user that is lower by some 40%. Moreover if MNOs decide to operate commercial mission critical networks in the 700 MHz band, the capex costs would be appropriately reduced from 800MHz, with the base station sites required reducing by up to 20% and costs approximately in proportion:

Table 4.4. Estimates of cost comparisons for the network options compared

Networking Option Scenarios	Capex estimated investment per user, for PPDR sector only, €	Capability in terms of media carried and multi-sector support	Opex €Bns /year
1: Dedicated specialised networks using specialised equipment only as for today (TETRA/ TERAPOL)	€7,150 (from existing public official figures – but may be underestimated due to different accounting practices, eg whether VAT included and all local/central costs)	Voice and narrowband data only, really for PPDR	€1.35
2 Commercial mobile networks using hardened commercial LTE equipment (800MHz)	€ 4,982	Can carry broadband traffic of all kinds for the 3 sectors - video, image and M2M data	€ 0.6
3 Dedicated specialised network using hardened commercial equipment At 700MHz: At 450MHz:	 € 6,990 € 3,510	Dedicated: Probably not applicable for other sectors or restricted in their support. Can carry M2M data in large volumes, if engineered to.	Estimated at 10% of capex € 4.0 € 1.8
4: Hybrid solutions (10 year spend)	€21,400 if no M2M data also carried. €12,800 if 40% of capacity for M2M	Can carry broadband traffic of all kinds for all 3 sectors video, image and M2M data equally	€ 5.4
5:Feasibility assessment for a common multi-purpose network for all 3 sectors	Feasible but more advanced in concept for resilience and capability.	Broadband traffic of all kinds for all the 3 sectors - video, image and M2M data equally	Between 5% and 10% of capex pa

Sources: cost estimates, based on research on publicly available accounts and NRA documents on future network costing (Ofcom etc|)

Opex figures are taken from a simple fixed relationship with the capex total of that of the existing dedicated networks (some 10%) and so may be an under estimate, except for option 2, commercial networks, where it is assumed that a far lower relation exists, estimated as at most being under 50% of the dedicated network of Option 1, due to spread of opex costs for 24x7 staff and consumables, etc, over all commercial operations. The most useful source here has been from the work of NRAs, with extensive cost models built over the long term (eg 12 years) for mobile networks[63] and also studies giving cost analyses for commercial networks at multiple frequencies, especially from Ofcom.

4.2 Networking option 1: Dedicated specialised networks using specialised equipment

4.2.1 Description

This option exploits specialised equipment for a radio network dedicated to mission critical PPDR and other emergency services, with its own sites, spectrum and a closed user community. Currently, the three sectors examined here rely on their own dedicated specialised networks and equipment for most of their radio communication needs, sharing only sparsely. TETRA is widely used for PPDR services although some Member States use TETRAPOL (notably France and Spain). The scenario here

[63] For example the LRIC cost modelling tool for MCT rates from Ofcom: www.ofcom.org.uk/static/LRIC_files/index.html

assumes the use of existing TETRA and even TETRAPOL equipment for a decade or more, as various stakeholders (both users and suppliers) have put forward to us in our research, also seeking EU-wide continuation of the allocated TETRA frequencies in the 380-430 MHz range. As noted in previous chapters, a short-term upgrade of TETRA networks exists, to TEDS (TETRA Enhanced Data Service). Its data rates require wider channels (25 kHz to 150 kHz) to support a data throughput of 25 kbps, and possibly up to 500kbps, depending on local conditions.

Dedicated networks are used by railway operators and by most utilities to various extents. They are rarely TETRA based networks and instead use either industry-wide allocated frequencies (as for GSM-R in the 900 MHz range for the EU rail networks) or a very diverse set of frequencies and network types across the EU for utilities. Utilities may be using digital PMR and even analogue networks in the VHF range but also wholly owned mobile cellular networks (eg Alliander with a 450 MHz CDMA network in the Netherlands).

PPDR networks are usually centred on control room operations for command, for groups of users that may need PTT functions and local working without base station interactions. Of all the five options here, the uses of dedicated networks and equipment is the only one that the PPDR sector has explored with any cost-benefits analyses (although these may not be complete).

This first option currently implies continuation of the specialised equipment of the TETRA and TETRAPOL types. LTE-based dedicated emergency and military networks are being rolled out in certain countries outside the EU, such as Jordan, with pre-standard commercial LTE equipment (with some upgrades, such as ruggedised handsets). This LTE successor option is explored in Option 3, which specifically examines commercial equipment used with dedicated networks.

Access to TETRA networks is also used in the two sectors other than PPDR, but to a limited extent in some EU MS, and also by governments and some military forces that may share TETRA network access.

Option 1 also tends to be based on a government owned, government operated model, but the network may also be operated and managed through a special government owned MVNO while another public or private entity owns the assets (eg as in ASTRID in Belgium). Other options for commercial operation of dedicated networks and equipment are in place in the EU, whether the assets are government owned (GO-CO), as in Austria and Germany, or privately owned (CO-CO), as in Denmark and the UK. It may also be that the public sector provides some or all of the base station sites, even if the stations are equipped and run by a commercial operator.

As previously noted, the comparison of costs uses largely capex and only opex where there are demonstrable clear differences (opex being so difficult to estimate with reliable accuracy, although a network's capex may give an indication of its opex).

4.2.2 Value assessment

If TETRA only is used, even with a 50 kbps data extension, TEDS, the offering is effectively voice, with slow-speed data and is really for PPDR. Such functions favour the requirements of the police services, possibly more than the other two ES. TETRA offers limited data networking and certainly not a broadband capability. Thus its use of images and video is quite restricted. Transport of data files and data updates is fairly limited also.

Hence, in consideration of use by all three sectors, its value is low. In consideration of the future value to the PPDR services, it is only viable as a voice-based support for operations and cannot support future demands for secure image and video transfer. Some sources (eg the UK police) note that

TETRA coverage operates well for personnel outdoors and that indoor coverage is variable, sometimes poor, unless indoor repeaters can be used.

TOTAL OPERATIONAL VALUE is **Low** because of the factors given above.

4.2.3 Extra cost factors

Additional cost factors for the Option are due to the lock-in effects of a specialised technology and low number of suppliers:

- The specialised network technology which is TETRA or TETRAPOL has a low number of suppliers with possibly a limited future availability beyond five years, so that specially constructed equipment will need to be ordered, perhaps on a piece by piece arrangement in the future
- The relatively small user population which makes the handsets and terminals additionally expensive (a range of €600-1200 and up to €2000 for a vehicle)
- There is a possibility that the spectrum used (380-430 MHz, varying by MS) may be reclaimed by NATO after 2020, in some Member States.
- Considering a current dedicated network and specialised equipment for ITS, the railways' GSM-R has a similar limited future for the current technology, with an end perhaps around 2020 as suppliers (originally NORTEL) have disappeared.

Other factors include the opportunity cost of a dedicated spectrum band at commercial auction rates, even if this donated by a government direct grant.

4.2.4 Cost reducing factors

The frequency used by TETRA and TETRAPOL (in the region of 400 MHz) tends to make high signal strength available over longer ranges than the higher UHF frequencies and thus reduces the cost on network capex and opex, perhaps by a factor of 10 against a network at over 1 GHz as base station coverage is extended. Indoor working should be improved also.

4.2.5 Table of costs analysis

Europe has already invested heavily in its mission critical infrastructure in the EU, to date, using data collected over all EU-28 Member States:

Table 4.4. TETRA infrastructure cost in the EU to date: summary from public records

Cost Item	Spend, € billions
Total spent on TETRA+TETRAPOL infrastructure (EU-28 + Norway, no handsets)	14.6
Cost of terminals (mobile handsets, vehicle mounted and others)	4.0
Annual opex for TETRA+TETRAPOL network operations	1.353
Installed Base	**Number of items**
TETRA+TETRAPOL terminals	1.57 Million
TETRA+TETRAPOL base stations	24,450
Annual Opex cost per base station with all core and other opex, in Euros	€55337

This is based on several inputs:

Analysis of existing public records or expenditure on TETRA networks in the EU. Here we examine some of the public records available for infrastructure cost information and one of the most illuminating is the TETRA private operator in the UK, Airwave Solutions. It is a private company which owns and operates "the largest public safety radio communications network in the world", serving "police, fire and ambulance services as well as local authorities, utilities and transport providers" in the UK. Airwave publishes annual cost accounts which are more detailed than other reporting seen for other TETRA operations in the EU.

In particular, its annual report from 2012 lists its current value of assets of property, plant and equipment with amortisation as about €1.8 billion (£1,423,621,000) for at least 250,000 users (with all other government users, perhaps 345,000 in all). It has over 3,800 base stations in the UK's network. However Airwave was reinforced for underground operation in the London area, with extra capabilities following the London terrorist attack of 7th July 2005.

In June 2007, in a UK government debate, Baroness Harris of Richmond noted that the UK police force would pay charges of €1.875 billion (£1.5 billion) over 19 years for the TETRA service; but the total cost of the system to the UK government had risen to some €5 billion[64] (£4 billion).

Although we are not including terminals in the infrastructure costs, TETRA product catalogues give interesting insights into the spread of equipment pricing across the EU. Prices per handset vary by MS generally in the range of €600 - €1200, while vehicle mounted terminals may be of the order of €2000 plus installation costs ranging from €200-2000. Sometimes the terminal costs are borne by the end-user organisation so they are not always accounted for in published network costs. As an indication the total European market, overall size in a 2013 market analyst report noted $1.0273 billion was spent on TETRA/TEDS network infrastructure and equipment in 2011.

4.2.6 Overall costs per user

Note that the estimate for the overall cost per user is effectively that for PPDR – as there is less information on use for ITS and utilities because the usage for these applications is largely restricted to emergency teams in some utilities. The net estimate a blended average from our basic research into costing across the EU MS. Thus the estimation figure below gives a relative cost of the items that make up the TETRA RAN costs per base station (with TEDS 25 kbps data channel).

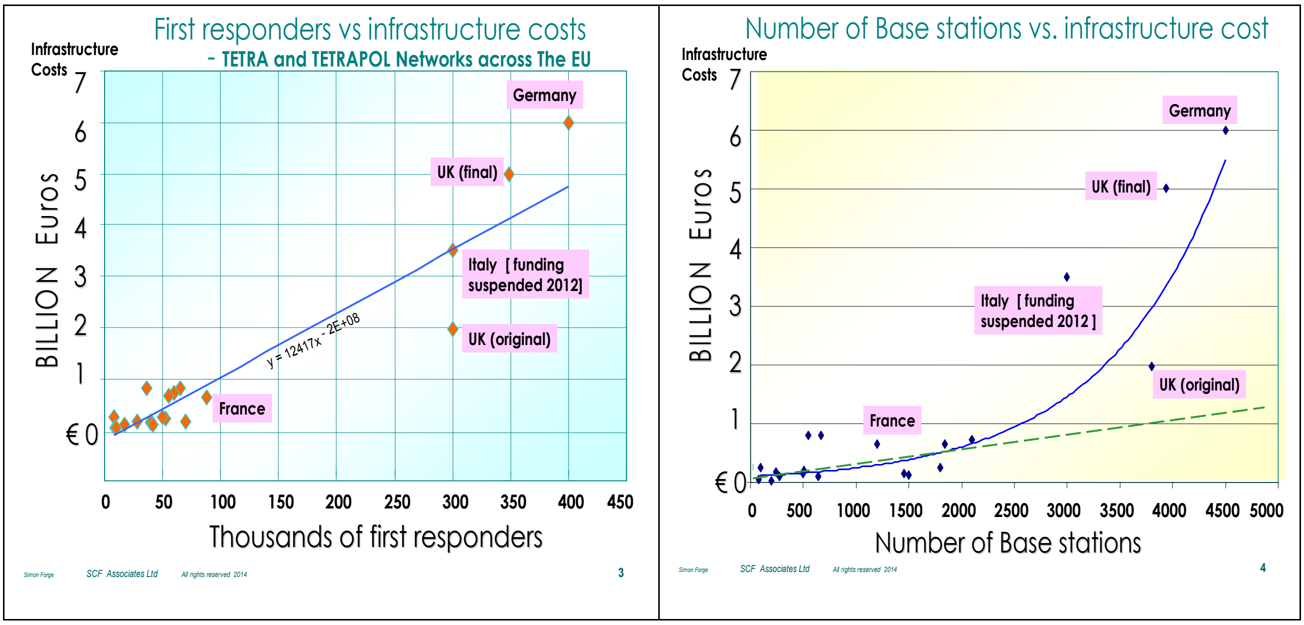
From the publicly available information, this research indicates an average cost of TETRA/ TETRAPOL infrastructure per user across the EU-28 of €7,150 (not including user subscriptions or any operating expenditure).

Also these estimates may have discrepancies between costing statements, due to the content of the original figures from the EU Member States – for instance whether VAT is due, and is included in the figures. In consequence, the overall aggregated figures may be in some doubt. Analysis of the publicly available figures for TETRA and TETRAPOL emergency service network expenditures indicates a considerable variation in apparent cost per unit across the EU, be that measured in terms of base stations or end-user terminals – and whether at the start or end of the investment cycle. The diagrams below show the published sums for total infrastructure spend, against the numbers of first responder users and of base stations, with a possible trend line.

---

[64] UK Parliamentary records, Hansard, 21 June 2007, column 390, http://www.publications.parliament.uk/pa/ldhansrd/text/70621-0011.htm

Figure 4.3. Relationship and variance in costs of mission critical network rollouts – measures of the spread of the cost of radio infrastructure against Member States in the EU



Examining the costs of infrastructure against number of base stations gives a non-linear variation, as shown in the figure where the larger systems diverge rapidly. Thus it is evident that estimates of infrastructure cost per end-user, (or end-user terminal, as some are vehicle-mounted) vary considerably, showing strongly marked scatter or variance.

This ranges from the largest estimated cost, at €22,409/user for Austria to some €15,000 for Germany, with €12,326 for the Netherlands and €2,100 for Spain. This scatter is mostly due to variations in what is included – or excluded - as net expenditure may be dispersed across different budgets and not aggregated. The Spanish example shows results for a national network. But additional costs may also be paid by the local emergency services for their network facilities, not included in these national infrastructure costs.

Turning to infrastructure cost per base station, the results appear equally random, as the Netherlands' figures attribute expenditure of €1.47 million per base station, Greece €2.69 million, while Germany spends €1.33 million and Sweden just €0.143 million. Spain apparently spends even less at €0.101 million; it does have the lower cost TETRAPOL network. However this does not explain the discrepancy with other TETRAPOL using nations, such as France, at some €533,000 per base station - some 400% more.

In conclusion, the costs of TETRA/TETRAPOL are probably much higher than estimates from the published accounts show, indicated by the scatter of results being so high. Thus the aggregate figure of near €14 billion capex spending so far in the EU may be an underestimate as not all costs attributable have been included.

For instance, using a median base station price of €1.33million, as in the latest German network, would give a total spend of some €35.6 billion for the 26,700 base stations given in the published account figures, for what is largely a voice only network. The infrastructure cost per user terminal would then be € 19,280, rather than €7,150.

In summary, this is the PPDR community's preferred networking option. But financially it is vulnerable in an age of continued austerity for the EU public services.

4.3 Networking option 2: Commercial networks using commercial equipment only

4.3.1 Description

The commercial MNO option is based on re-use of the network infrastructure built for commercial services for mission critical applications, by enhanced resilience through “hardening” the LTE networks and extending its patterns of use for faster uplinks. It is assumed that the commercial operation can provide the minimum set of features required.

It is also expected that public service use of commercial MNO contracts can choose coverage selectively for hardening sites across multiple operators as needed in each location. Hence costs would be reduced to a minimum, as not all of an MNO’s sites are hardened. It would also satisfy state aid rules, by providing equal advantage to all the MNOs. This assumes roaming across MNOs will be in force and effective. Consequently, many Member States have reduced infrastructure competition, in that the MNOs share physical infrastructure to reduce operating costs, eg four service providers may in fact operate over two physical networks. In this case it would be necessary to selectively harden each of the two networks by geography, although they would be exploited by the four MNOs. Moreover, the use of inter-MNO agreements through Licensed Shared Access (LSA) between MNOs can also be harnessed for critical communications, just as it is already used for normal commercial operations in some Member States. All of this tends to support the goal of hardened networks across all operators.

Contracting of multiple MNOs would also to reduce the risks of lock-in, and a single network being the point of failure. Most importantly, it should also involve the ability to roam across national MNOs to obtain the best signal strength for any situation.

Thus an administrative mechanism of a central contracting authority for the three sectors would be most useful. It may indicate the need for an MVNO type of structure to manage the contracted MNOs and systems integrators on behalf of the three sectors. Such a network may be commissioned and contracted by government on behalf of the various sectors but could be owned and operated by commercial interests (‘CO-CO’) under specific conditions including SLAs with penalties. The SLAs would be employed by the end-users to manage the relationship with MNOs. This option would probably also require a highly specialised system integrator to bring all systems, networks and handset apps together.

The applications for mission critical services could be developed by the MNOs, which should have the capability to develop the new services, or to sub-contract their development. It may be that the national body responsible for critical infrastructures, with the MNOs, manages the build via systems integrators, who integrate network equipment and software from the OEM network and handset suppliers and also provide maintenance. Such an operation will require specific contractual structures, for multi-partner collaboration, probably through SLAs, to ensure a resilient critical infrastructure on top of commercial LTE platforms. An alternative approach is to commission the services from a single MNO, either nationally or by sub-region within one country. That may leave end-users to the problems of monopoly pricing and SMP behaviour, if coverage were to be limited to a single network operator. It would require specific counter-measures in the SLA formulation.

One key consideration is the charging infrastructure within LTE for use with the various emergency services as well as with the sectors of utilities and ITS. The latter may require very low cost fixed price charges over many years. Conventional SIM card structures may be inappropriate, especially for sensor networks with very low costs. Here a SIM-less operation on bundles of transactions be they data, voice or short messaging may be useful.

As explored in previous chapters, the costing of a commercially based network is controlled by the main operational parameters (some being defined in the LTE air interface E-UTRA, the *evolved UMTS terrestrial radio access*):-

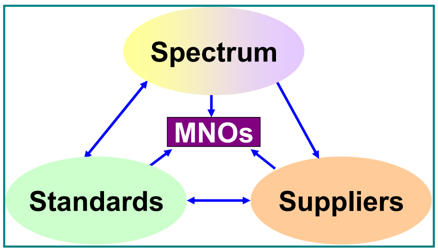
1. Geographic coverage of operations of existing MNOs - which may need to be extended for the mission critical role from as low as 85% to over 95%, perhaps 99% of landmass. Enhanced coverage should involve all MNOs, assuming handover between them.
2. The throughput level required of the network, in terms of data speeds and numbers of simultaneous user sessions. This may be defined as the minimum sufficient for broadband service for every mission critical service user, with a (high) upper limit on the number of simultaneous user sessions. A minimum broadband rate for up- and down-links must also be defined for universal coverage. It may be at least 2 Mbps, with higher 10-50 Mbps preferred long term, although the LTE standard expects 300/75 Mbs peak downlink/uplink. The LTE standard allows for 200 simultaneous active data users in each cell for each 5MHz of spectrum, uplink or downlink. Mission critical applications tend to need equal uplink and downlink speeds, rather than the emphasis on download, as for civilian users and may use uplink more.
3. The frequencies employed, for up link and downlink, which dictate:-
   - The range of (macro)cells and thus the cost of the hardened upgraded network. The LTE standard may be optimum for up to 5 km radius cells although smaller cells may be used for urban settings (the absolute maximum may be far higher, but with degraded performance. In urban settings the higher LTE frequencies of up to 2.6 GHz might be used, for 1km radius cells.
   - The extent of building penetration with the level indoor signal strength
   - The availability of equipment and handsets in the chosen frequency bands. The mobile industry depends on the suppliers offering volume-priced equipment, including that hardened versions for network infrastructure as well as handsets. This cost advantage will be restricted to the standard commercial frequencies.

   In general, lower frequencies give better performance, so the lowest common commercial frequency, around the 800 MHz band, is likely to be preferred. However, the WRC-15 conference may yield 700 MHz spectrum for commercial uses in Region 1. The possibility of mission critical dedicated spectrum in closely adjacent bands at 700 MHz is explored under scenario option 3.
4. The total RAN bandwidth available for broadband transmissions. If it is insufficient, the percentage of 'not-spots' grows quickly. Tests of LTE with 5 MHz up- and down-links were too narrow for the protocol to give 2 Mbps universally; 10MHz bands were needed.
5. The transmitting power adopted (for base stations and for handsets).
6. Network topology, including the use of smaller/lower cost cells and indoor customer premises equipment.
7. Adding LTE to an existing commercial network demands higher backhaul data speeds and capacity. Adding priority users will require further additional backhaul and core network capacity, with interfaces to their control room systems.

Some of these conditions may be specified, for instance in a coverage obligation on the MNO for the landmass geographic coverage, data speed and also building penetration. A further requirement will be for commercial networks to provide coverage in tunnels and other underground areas, perhaps by connection via a leaky feeder or other dedicated distribution system.

Security of the dedicated TETRA networks, especially in their data modulation protocols has been carefully designed for high protection, and so is considered a major advantage. However commercial network technology in advancing to LTE also has progressed significantly in its inherent built-in security feature, both in terms security of communications and in security of the network system against cyber attacks, which the 3GPP task force for mission critical see as an important agenda item.

In general, costs will also be subject to the availability of the broadband network technology in a standard form for mass production. So the standards setting process for LTE is a crucial element. In general, offerings of mission critical services by the commercial MNOs can be summarised as being determined through three MNO dependency relationships shown below:



When migration from TETRA begins, the ETSI 3GPP standards process will not have delivered all the mission critical functions required so the first commercial networks will rely more on applications in handsets to implement them over a less functional core and RAN. The 3GPP standards for LTE will progressively add these functions through Releases 12 to 15, through to 2020.

4.3.2 Value assessment

This network offers broadband capability for video, voice and data files. Its potential value is therefore high. Any potential drawbacks are not so much technical but intrinsically commercial, since this option requires the long-term efforts and co-operation of the MNOs and the supplier community. Without appropriate conditions of MNO operation (probably eventually regulatory) the level of risks would diminish the value of this option, as the probabilities of MNO non-performance in this critical area are fair to medium. It would be best suited to PPDR operations but with suitable engineering and tariff structures it could handle the short data bursts of M2M traffic for utilities and rail also. The overall value assessment must be tempered by this:

TOTAL OPERATIONAL VALUE = **Medium** without reduction measures for the commercial risks of relying on MNOs. If these risks can be significantly reduced, the value would become **high**.

4.3.3 Extra cost factors

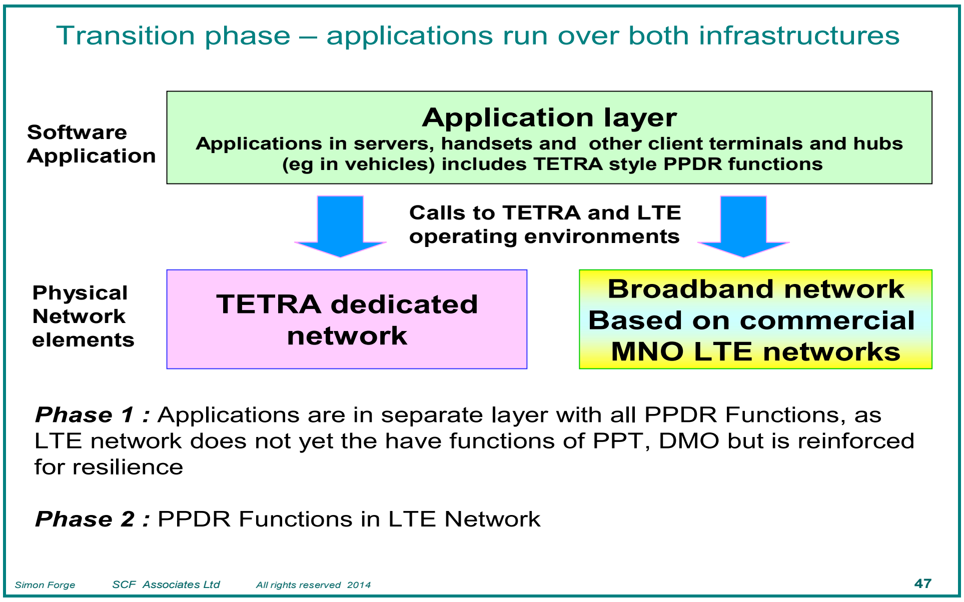
The additional cost factors are the firstly the need to extend the network to national coverage (of the order of 99%) for mission critical applications, from commercial coverage (perhaps as low as 85% but more usually 95%).

Secondly there is the need to extend total network availability, from perhaps as low as 95% end to end for commercial operations, to at least 99.99% by suitable hardening. Commercial LTE network equipment and handsets have limited hardening, at whatever frequency. Extension of the equipment's service availability is required, from as low as 98% for standard commercial products to 99.99% by suitable hardening measures, such as redundant units and extra UPS, as well as better housing, HVAC and security.

Migration from the existing dedicated networks to commercial cellular will cause both operational problems and extra costs. Thus any such transition will require system integrators and support entities. During the transition, end-user terminals, especially handsets, are likely to be dual-mode (TETRA/LTE, for example) and should be capable of seamless interworking between old and new systems. Base stations might also be dual-mode if transceivers for both technologies can be co-located (if they must operate in different frequency bands, this may not be the case). Interconnecting the networks could occur physically at various points – in the control room with gateways, in base stations or in the end-user terminals. The cost of each option could decide how the interconnection is made.

It will probably take several years for LTE standards to incorporate the essential PPDR requirements. In the meantime, PPDR functionalities could be supplied in an applications layer by software on top of the network. Eventually (perhaps around 2018-2020), fully proven LTE PPDR releases may emerge with these applications embedded in the network, as shown in the figure:

Figure 4.4. Transition phase application level integration of legacy and future PPDR networks



This approach, with functional integration at the application level, offers the possibility of smoother interworking during the migration period. It requires a layered architecture so applications can run on both network systems with a consistent user experience.

4.3.4 Cost-reducing factors

The network can replace any existing TETRA/TETRAPOL network (perhaps progressively) and so can benefit from the existing dedicated sites and their physical backhaul connections (ducts and wayleaves) as well as possibly the core switching sites and facilities, to give extra coverage for the hardened commercial network. However whether the existing sites would be charged for, and how much, may reduce the advantages of this factor. Certainly there is an opportunity cost that would be foregone if they are transferred at no charge.

This network option does not require extra dedicated spectrum as it is based on existing licensed spectrum. Note that it would be best suited to bands at sub-1 GHz frequencies and as low as possible – probably at 800 MHz if the 700 MHz is not (yet) available. The commercial frequencies for LTE above 1 GHz might be used in urban setting for lower radius, small cell working.

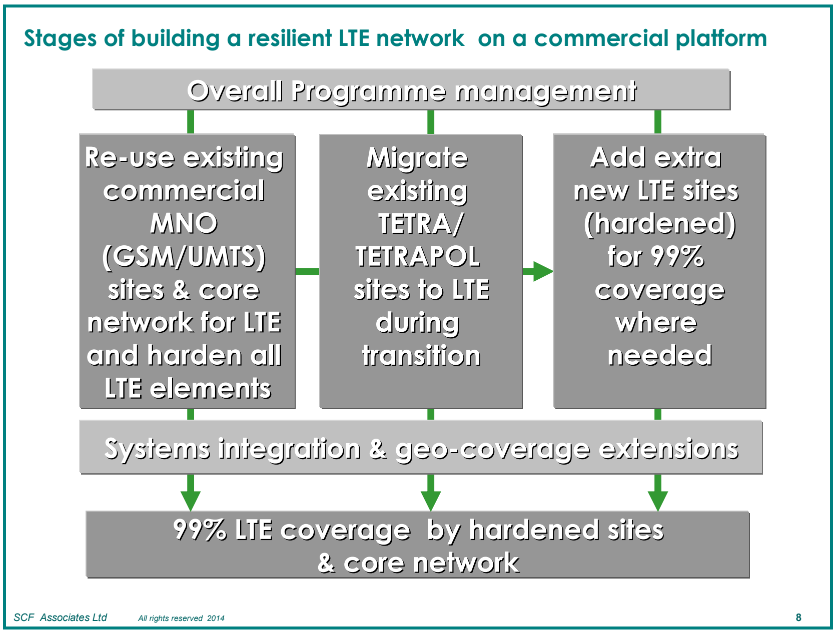
Table of costs analysis

The costs for this option of a purely commercial based service must incorporate the costs of hardening the network and extending LTE coverage to be comparable to TETRA/TETRAPOL. We employed several sources here:

- Discussions with MNOs who are about to embark on offering a resilient commercial service with PPDR functions (such as PTT and DMO) for PPDR services have highlighted the costs involved. These network offerings should be comparable to or exceed TETRA/TETRAPOL dedicated network coverage and performance. Such services may be open to the other sectors, of utilities, rail, road, etc. Their analysis should allow for variations in propagation, population density, terrain features etc while assuring indoor coverage as well as outdoor.
- First analysis of costs from NRAs, notably from Ofcom studies with a series of reports over the last few years on commercial MNO costs for LTE at 700, 800 and 900 MHz.
- A new tendered network in one European country with set pricing of its four lots has been announced by the UK government's Home Office for its ESMCP project on 7 July 2014, for the emergency services network (ESN) build and operation.

The transition process from commercial level mobile quality to a mission critical network is summarised below:

Figure 4.5. Stages in building high resilience on a commercial mobile platform



The costs per user terminal are derived from two estimation approaches as follows:

1) The first approach is to take an average cost to upgrade a commercial LTE mobile network to its hardened form by percent of geographic coverage. This was given for a specific example now in preparation in one Member State, as an indication:

- Estimates of hardening are of the order of €25 million to €38 million for 1% land coverage, ie for 100% coverage that implies = €2.5 billion to €3.75 billion for the land area.
- These guidelines give an indication of the cost of a hardened LTE broadband infrastructure per sq km, which we can apply across EU for each MS. For a cell radius of 3 km, or 28.3 km^2 this 1% of the land area contains 86 cells or €290,170/cell to €435,296/cell, ie net costs for

RAN and core network hardening for the upgrade of each LTE cell. For a larger cell radius of 5 km, this area is 78.55 km^2, or 31 cells in 1% of coverage, ie €806,104/cell to €1,209,156/cell. The reality would be a mix of large, medium and small cells.

- Overall cost per user for this infrastructure, for 350,000 users, would be of the order of €7,140 to €10,700.
- Although quite approximate, it also offers an estimate for the whole of the EU land mass, taken as 4.423 million km2 of a scaling up factor of 18.157, so that:

The range of cost for equipping the EU landmass with hardened LTE commercial cellular networks for mobile broadband would be of the order of €45 to €68 billion.

However, this estimate was founded on an approximate indication. It was not backed up by detailed figures for actual costs. Thus it is used here as a sanity check, ie a 'ballpark' figure, only to see if the estimates by a more accurate and detailed means could be verified by it. This more detailed approach was pursued below.

2) The second approach employs initial analyses of costs from various NRAs over the last three years, notably by the UK NRA, Ofcom, with a series of reports on commercial MNO costs for LTE at 700, 800 and 900 MHz. These attempt to examine the problems of including rural coverage with dense urban coverage, while taking into account the reality of specific population and terrain distributions. The aim has been to overcome inherent limitations of previous modelling exercises, focused for densely populated areas

The UK regulator Ofcom has examined an example of a mission critical network using commercial mobile LTE technology to provide broadband service and based on commercial 800 MHz spectrum range.[65] The target capability is a minimum sustained downlink speed of not less than 2 Mbps with uplink speeds of similar rates across the whole cell area.

These studies have aimed at a network based on upgrading existing sites, using LTE technology largely at 800 MHz spectrum to deliver mobile broadband coverage beyond the 3G footprint to equal the current coverage of 2G technology. Indoor reception and transmission are important and so coverage with a 90% probability of indoor reception for an area corresponding to at least 95% of the population have been the targets. This would result in coverage by future mobile broadband approaching today's 2G coverage after 2020 at the earliest.

It would reuse the existing emergency services' sites, which are already strategically placed but are sparse in coverage compared to the commercial networks but may have the advantages of hardened features. Only using the commercial MNO sites without any legacy sites could vary the costs. Depending on legacy network sites and features it might be more expensive, or in some MS perhaps cheaper.

The studies propose various cell sizes but mainly consider a macrocell network directly to an indoor mobile user. Their modelling suggests that for the UK, a network of around 9,000 sites using a 2x5 MHz 800 MHz carrier could provide a 2 Mbps service, with 90% confidence of indoors coverage, to an area within which 95% of the UK population lives.[66] However, evidence given to the UK

---

[65] Ofcom, 2013, *LTE brings a new capability to mobility: how might it enable a range of cross- sector services*, A report for Ofcom, the UK communications regulator, PA, November 2013

[66] Consultation on assessment of future mobile competition and proposals for the award of 800 MHz and 2.6 GHz spectrum and related issues", Ofcom, 22nd March 2011, from: http://stakeholders.ofcom.org.uk/binaries/consultations/combined-award/summary/combined-award.pdf
and also: Ofcom study 2012, *Cost of extending 800 MHz mobile broadband coverage obligation for the UK*, Real Wireless.

Parliament, by the MNO EE (Everything Everywhere), on 19 May 2011, suggested that the bandwidth as well as the frequency of the spectrum used played a significant role in meeting this coverage obligation. EE demonstrated in rural trials that 2 x 5 MHz of sub 1 GHz spectrum would not be capable of providing sufficient performance or capacity to handle broadband traffic levels in rural 'not-spot' areas. It was found that the minimum of sub-1 GHz spectrum necessary for the commercial viability of wireless access is 2x10 MHz for rural broadband.

Several variations on this model are possible:

- An alternative approach to pure macrocells could be to supplement them with small cell technology using LTE relays and Wi-Fi; this is explored in Option 4 on hybrid networks.
- Going to a higher data speed, of 7 Mbps (symmetric communications suitable for mission critical) has also been examined. It was found to require far more base stations, perhaps an extra 33% in addition to the 9000 sites at 800 MHz (for 2 MBps to cover the UK), ie some 3000 extra sites, according to one study which extended coverage to 99% of the population[67] .
- Various assumptions have been made in the various prior studies[68] which should be taken as perhaps, at best within a margin of error band of 30% (positive and negative):
- Some 33% of current MNO cell sites would have the resilience level of TETRA sites (ie have backup and failover transmission installed). This may be an overestimate of the actual conditions for MNO networks across the EU and a zero figure may be judicious.
- Where additional network rollout is needed to bridge the coverage gap, then an estimate of the proportionate mix of cell types and cost per site may be taken as approximately:
    - Large - 35%, €112,500 (£90,000)
    - Medium - 35% €93750 (£75,000)
    - Small - 30% €43750 (£35,000)

A summary table is shown below for a coverage-based estimation of the total costs of sharing commercial MNO networks to give the required coverage, based on the itemised costs given by the studies referenced, and then extrapolated for the EU landmass. The estimated total number of sites needed for geographic coverage in this scenario's analysis includes those for extension to 99% of the UK land area, with extra sites, plus hardening of existing MNO sites.

---

67 "*Infrastructure analysis and solutions for 800MHz network deployment*", ICT Knowledge Transfer Network, May 2011- suggested approximately 3,000 extra sites would be necessary and would also to extend coverage from 95% to 99% of the UK population; the 3,000 sites figure is an estimate based on the graph of Figure 2:
https://connect.innovateuk.org/c/document_library/get_file?folderId=865485&name=DLFE-32798.pdf

68 Ofcom, 2013, *ibid*

Table 4.5. Summary of costs for scenario option 2

Summary table	€
1 Costs of acquisition and preparation of existing sites - which comprises: cost to co-locate/ convert for existing GSM/UMTS sites; cost to take over existing TETRA sites and re-equip	998 million
2 New site acquisition & construction (average)	74 million
3 Hardening equipment on EXISTING sites plus conversion costs to 800 MHz LTE- Itemised cost base	528 million
4 Hardening equipment on NEW sites for 800 MHz LTE (may be additional costs in core and backhaul diversity)	20 million
Total cost for the UK	1744 million
UK landmass area, km^2	**243,610** km^2
EU landmass area km^2	**4423000** km^2
Total cost for EU, pro rata scaling up factor of 18.16	32 **billion**
Cost per user in EU, at density of users as for UK	4982

Sources: Ofcom reports and scaling by area-based estimates by SCF Associates Ltd

This estimates the costs for a total EU-wide network capex as being €32 billion for investment to build the mission critical network by hardening existing commercial sites and the core network and also re-using existing emergency sites for an 800 MHz LTE system; without handsets.

The cost per user depends on the population of users expected. For the UK emergency services population of 350,000 users this would yield an infrastructure cost per user of €4982 for an EU-wide population of 6.3 million users. The exact EU current user population is not available but our own research indicates around 1.8 million users at least, for TETRA with TETRAPOL, although whether all are counted (eg in Spain and France) is unclear.

3) The set up of a new system in one European country by tender bid with set pricing of its four lots has been announced by the UK government's Home Office for its ESMCP project on 7 July 2014, for the emergency services network (ESN) build and operation. As a further approach to costing this may act as an approximate indication for checking previous estimates:

Table 4.6. Bid price envelope for a commercial mission critical network, largely for PPDR

ESMCP Lot	Minimum bid £ millions	Maximum bid, £ millions
Lot 1 - ESN Delivery Partner (DP) managing the transition from old to new systems:	60	95
Lot 2 - ESN User Services (US) - developing and operating the telecoms infrastructure and public safety applications, installing equipment and making sure everything is integrated and works:	120	245
Lot 3 - ESN Mobile Services (MS) - providing an enhanced mobile communications network service with enhanced availability for the emergency services and highly available full coverage:	200	530
Lot 4 - ESN Extension Services (ES) - providing a highly available telecoms infrastructure covering parts of the UK outside regular mobile network coverage :	175	350
Total for UK, € millions	€690 (£555)	**€1525 (£1220)**
For the EU, pro rata scaling up factor of 18.16 on coverage area, € billion		**€28 billion**

These figures are used solely as an indicative check. They show that effectively for one EU country, the UK, the cost to build a new system, with some (not all) costs of transition is expected to be of the order of €1.5 billion, if the maximum figure for tender bids is taken, as shown above.

In the estimates used here, the comparative figures used are based on capex for infrastructure, required to roll out the network. However, looking longer term, it may be noted that subsequent renewal of the LTE commercial hardened equipment in comparison to other technologies may be a relatively smaller cost in five to seven years. LTE equipment costs may be expected to reduce with volume production over that timeframe, possibly in a competitive market by approximately 30-60%, if it follows the preceding pattern of pricing of 3G UMTS network elements. So while for other technologies (eg TETRA) equipment renewal may be a larger expenditure but only at 10 year intervals perhaps, a commercial LTE hardened network renewed every five to seven years may still present a lower net cost. Moreover the replacement LTE equipment is likely to exhibit better resilience, lower power consumption and higher security. Moreover the use of software protocol stacks with NFV for LTE core SDN would reduce that cost still further and the associated installation costs of outside plant moving into the data centre.

Turning to an EU-wide approximation, based on the geographic land area scaling factor of 18.156 yields a maximum estimate of a total EU cost of €28 billion. This approach is open to dispute. Each EU Member State has a different urban density and proportion of urban coverage as against suburban and rural, while the landscape disposition is also highly variable (eg compare Finland and the Benelux MS) to that at best it may have a difference between the budgeted estimate and actual cost of plus or minus 30% in variance.

The UK Home Office has announced the shortlists of bidders for each lot for the ESN, which will replace the Airwave narrowband TETRA network currently used by the UK's police, fire and ambulance services. The shortlists for the two network infrastructure elements (Lots 2 and 3) consisted of the incumbent TETRA network provider Airwave Solutions, as well as EE, Vodafone and Telefonica/O2. In Lot 2, Astrium, Airwave, CGI IT, Motorola, and HP competed for the systems integration, network management and emergency systems operations responsibility. Previously an 'Apps Store' for the emergency services was included in Lot 2 but this may now been separated for allocation in a separate call for tender.

4.3.5 Overall costs per user

As shown in Table 4.5 above, infrastructure cost per user is estimated as:

In terms of infrastructure cost per user, and applying the same user density as for the UK (of 350,000 users) this would indicate a sum of €4,982. There are questions over this figure in that the cost for hardening the core networks given in the source estimates appears to be quite low, perhaps too low in the final accounting.

4.4 Networking option 3: Dedicated specialised networks using commercial equipment

4.4.1 Description of the option

Option 3 is related closely to Option 1, being a separate dedicated network with specialised PPDR type equipment. But it differs from Option 1 in moving to commercial mobile radio equipment as much as possible for building the dedicated network (not shared with the general public) with a broadband capability.

Although Wi-Fi and WiMAX offer cheaper equipment and efficient use of licence exempt spectrum, they have shortcomings which seem to leave LTE as the main default choice for the future for such a dedicated networks as the current TETRA/TETRAPOL technologies are not capable of broadband delivery. Thus the mission critical networking direction for the longer-term future will most probably be some form of hardened and dedicated LTE technology (the TCCA has mapped a migration timeline). The existing technology that may require a more rapid upgrade to LTE is TETRAPOL, seen as not having a long-term future by some of its current users; TETRA may have a longer transition period. However there is a risk that if standards from 3GPP are late, mission critical enhanced LTE will not be viable in the timeframe required also with the risk that non-standard hardened and PPDR extended LTE will gain a hold. This risk demands a rapid response from the 3GPP community.

Normally the way forward for migration could be seen as a macro cell replacement. However for urban communities the concepts of small cells are also being considered and these are explored further in the hybrid option, the fourth scenario option.

Option 3 may also satisfy the governance preference of the PPDR community, in that the network is owned and operated by government or a public enterprise, as with Option 1. A private subcontractor working under strict contractual constraints and with full liability might also be acceptable (ie GO-CO) with dedicated, government owned assets. Conceivably, a dedicated network could also “borrow” cellular frequencies, when needed, through Licensed Shared Access (LSA) agreements or emergency pre-emption.

In more general terms of physical implementation, there are two basic approaches to building a dedicated network with commercial technology for use by “mission critical” users which have differing cost structures:

1. Build from new completely – implying that all the infrastructure, base station sites, control centres, etc. must be acquired and equipment deployed – the most expensive.
2. Re-use the physical assets of an existing emergency services network – which requires a migration from used equipment and infrastructure to new network systems but will be the more usual situation in the EU MS and should cost less as existing real estate assets (the most expensive item in the urban environments of the most developed economies) are re-used.

In either case, this scenario is aimed at profiting from the availability of commercial off-the-shelf technology (COTS). Yet as noted above, such COTS technology still must be “hardened”, at least for PPDR users. So the deployment of hardened dedicated LTE networks could stimulate the production of ruggedised equipment based on standard protocols for network infrastructures and for end-user terminals. That would eliminate the need to modify products one element at a time, but the mission critical demands of enhanced transmission power, receiver sensitivity and ruggedness still mean that the overall costs are likely to be higher than ordinary LTE equipment, even if compatibility with normal cellular protocols is retained and customisation is performed on an industrial scale. Market surveys[69] suggest the installed base of public safety LTE eNodeB base stations will reach a compound annual growth rate of nearly 60% between 2014 and 2020. By 2020, the installed base of emergency services LTE eNodeB base stations could be nearly 155,000 units serving an estimated four million public-safety subscribers worldwide.

Sectors such as utilities and perhaps road and rail emergency teams could use existing PPDR infrastructures in some countries to a limited extent for their own purposes (eg in the UK). However,

---

[69] IEEE Comms Society, www.community.comsoc.org/blogs/isabellamurray/public-safety-lte-mobile-broadband-market-2014-2020, also, Reportsnreports, *Global Public safety LTE and Mobile Broadband market 2014 to 2020*

utilities may also have their own “mission critical” applications based on dedicated networks of a quite different type, as explored in Chapter 2 (Requirements) often with legacy technologies, including VHF frequencies and even analogue working in some MS. As remarked, ITS networking is a less well-defined sector, and a common application set is not yet established. Moreover ITS is an evolving field and some foreseeable developments require very large initial investments.

One further point is that MNOs in the EU are currently planning for commercial LTE networking technology based on frequency division duplex (FDD). It is designed to support symmetrical data flows for FDD pairs of uplink and downlink channels of equal size. However, LTE’s time division duplex (TDD) variant has asymmetric up/downlinks, more appropriate to the data traffic generated by utilities and ITS sectors. Thus a dedicated LTE network for those two sectors probably should use TDD rather than FDD. However, versions of LTE which support both FDD and TDD are also coming to market, which would be a preferable choice for dedicated network based on commercial LTE equipment, for all sectors.

4.4.2 Value assessment

Option 3 offers broadband and all data services as well as voice. This is a specialised network for mission critical services only and would be standalone. Use of a common standard (LTE) technology should make interfacing to other networks, countries and services easier than today’s dedicated networking technologies. As mentioned, dedicated networks require dedicated spectrum, which has an opportunity cost (or value) that could be considered, even if donated as a free grant.

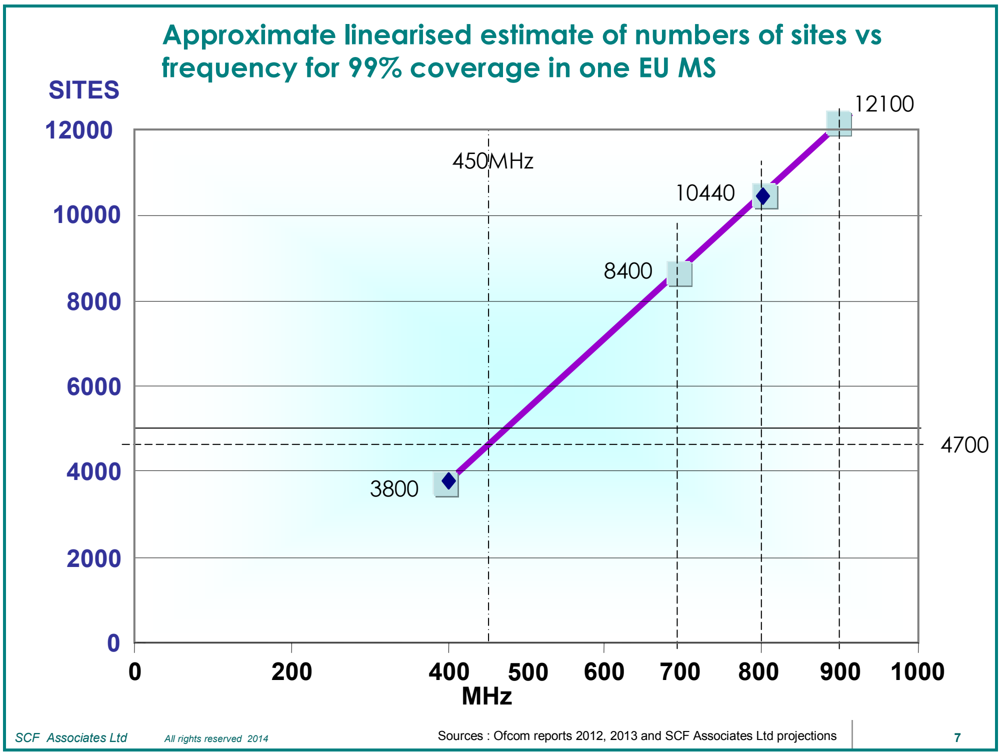
TOTAL OPERATIONAL VALUE = **Medium to high** but it is really more oriented to PPDR than the other sectors, except for their emergency maintenance teams.

4.4.3 Extra cost factors

Re-use of an existing TETRA or TETRAPOL network is likely to require additional sites for the same coverage. Commercial LTE bands have a shorter range than the 380-430 MHz of the current emergency services networks in the EU.

A mission critical network operating above the current 400 MHz (unlikely for the future) at 450, 700, 800, or even 900 MHz, pays the cost penalty, associated with the higher frequency in the density of base stations required. These rapidly rising costs with frequency are shown in the linearised approximation of the figure below:

Figure 4.6. Relation between base station site numbers and operational frequency, linearised



LTE equipment at 400 MHz would be likely to be a special custom production at high cost.

However, Qualcomm, one of the largest LTE chipset suppliers, have produced a 450 MHz chipset version for LTE handsets for the Brazilian market - but this is not a standard commercial MNO frequency elsewhere, although a few countries such as Bangladesh have show interest. So the market is limited. Nor is it a dedicated frequency in the EU for mission critical networks, although it is used in some countries for dedicated utility networks, as in the Netherlands. There, 450 MHz CDMA is reused by a utility (Alliander). For networking with LTE below the 450 MHz frequency band, Qualcomm tests have highlighted how LTE protocol signals suffer from degradation, in that the number of bits/Hertz must be increased for the same bit-rate of broadband coverage but the distorting impacts of interference on signals are more serious than at higher frequencies (Qualcomm, 2014).

Commercial LTE network equipment and handsets have limited hardening, be it at 900, 800 or 700 MHz. There is thus a need to extend the equipment's service availability from as low as 98% for standard commercial products to 99.99% by suitable hardening measures, such as redundant units and extra UPS, as well as better housing, HVAC and security.

A move to LTE will also demand higher backhaul data speeds than existing dedicated networks and much increased capacity (from 10 kbps voice to 2 Mbps video data). Replacement of the core network infrastructure would be made, probably modifying many switching sites and their connections, for a new IP-based switching configuration.

Specialised handsets may still be needed. The question is whether commercial units with some added applications could be used. More ruggedised versions would cost much more, perhaps about €1000, at the level of existing TETRA units.

4.4.4 Cost-reducing factors

Re-use of existing TETRA/TETRAPOL sites will offer at least a third of sites and possibly far more, depending on the geographic situation and their disposition in each MS and the frequency of LTE used. Again, whether there would be a charge for these sites is an important question and estimates here are for no charges being made by governments transferring these assets.

If WRC-15 proposes new 700 MHz bands for dedicated critical communications services, and if individual Member States follow this, then a large enough market for volume production might appear for dedicated LTE equipment between 694 and 790 MHz. With closely sited emergency and commercial bands, the hope is that their adjacent nature would make commercial handsets and transceivers available at lower cost for use in the dedicated emergency bands. With the possibility of a global emergency services market in the 700 MHz band, volume equipment savings for the network elements and for potential use of standard handsets for broadband, with suitable apps. Overall capex for network deployment could be significantly reduced. Note that the availability of 700 MHz, if it does occur would not be made in the EU before 2018 and perhaps later – after 2020. The availability of other dedicated frequencies in lower bands (400 or 450 MHz) is unlikely for the reasons explained above, and also commercial equipment at commercial prices is less likely due to the much small market, unless the technology designs lend themselves to multi-band operations at much lower frequencies while maintaining the lower commercial price. Even the continued availability of the TETRA bands in 380-430 MHz may be in question after 2020 in some Member States.

Use of hardened commercial LTE networks and their subsequent increased reliability could drive further roll-out beyond mission critical. The net effect could be to reduce the cost of hardened LTE equipment, so that such equipment could even become mainstream. That would drive high volume production and lower prices. Lower prices would make the difference between hardened or unhardened networks and equipment much less. Note that the same effect has been seen in computing equipment where failover clusters in web farms for cloud computing are now mainstream but originally the ideas of massive redundancy and high resilience failover management, with backup UPS etc, were considered too expensive for general use. Moving to commercial LTE networks which are SDN with NFV would accelerate this trend as much more of future networking technology will reside in the data centre.

4.4.5 Table of costs analysis

In these estimates certain costs are excluded from the basic cost of creating the infrastructure:

- Handsets (additional cost of €300–1200 per officer and up to €2000 per vehicle, before installation charges)
- OPEX, as not considered for infrastructure build costs
- Charges for spectrum; it is assumed that spectrum for a dedicated network could be under government grant, although an opportunity cost is considered below.
- Charges for any re-use of existing sites

Being a dedicated network, all sites are purchased freehold or are on long-term lease (minimum 50 years). Costs in the tables below are shown for a dedicated network at 800 MHz for comparison with the commercial platform (Option 2) but the costs for 700 MHz and other possible frequencies are also summarised in a further table below in an approximate sensitivity analysis of cost and frequency. The major costs are the Network sites as well as the equipment costs for the RAN and core networks, with the IT support items in network operations centres and data centres. Assessment of overall costs can be made via two approaches – either build from new, acquiring all sites, or, with savings from re-use of existing sites. A comparison of these costs is shown below with savings that can be made by re-use:

Table 4.7. Costs to build from new at 800MHz

Model 1 - Build from new completely	**Net costs, Millions £**	**Millions EUROS**
1 Costs of sites	**£732**	**€ 915**
2 Costs of equipment/technology installed	**£1,755**	**€ 2,194**
3 Costs of hardening	**£253**	**€ 317**
Total in billions of Euros for one MS (UK example)	**£2.74**	**€ 3.43**
Total cost for EU-28 in billions of Euros		**€ 62.2**

Source: Estimates using inputs as for Option 2

For model 2 the costs are estimated with savings from existing PPDR site re-uses:

Table 4.8. Savings from reuse of existing PPDR sites (TETRA)

Model 2 – savings by re-uses of existing emergency services sites (for TETRA) at no site cost for transfer	**Millions Euros**
Savings on re-use of TETRA sites:	**€324**
Savings on equipping TETRA sites for LTE	**€276**
Extra spend for TETRA sites:	**- € 72**
NET saving by using existing TETRA sites (UK example) Millions Euros	**€528**
Total savings for EU-wide network, billions Euros	**€9.55Bn**

Savings from re-use of existing emergency service sites would reduce the costs to build the network by approximately 12%, to €55 billion, if the savings applied for the sample country (the UK) can be applied across the EU-28 for the 800 MHz LTE case. However this also makes a key assumption, that these sites are handed over at no cost. In reality, there may be a real cost, as the current site operator may wish to gain some return on the sites, with their facilities, as they are seen as valuable assets. Even if no return is required, as they are considered state property, accounting procedures may demand that they are valued at an opportunity cost for alternative uses or sales commercially.

The table below shows the costs estimates for each frequency and numbers of sites for the example MS, extended to all the EU, using the graph of site densities and frequency. It assumes the same volume productions costs of LTE equipment for all frequencies, which may not be the case.

Table 4.9. Variation in costs with operational frequencies

Sensitivity analysis - estimates on the approximate costs by operational spectrum band used Variation in costs, for EU-28 wide coverage with re-use of existing sites/assets for dedicated networks over 800MHz norm				
Operational frequency MHz	**Number of sites**	**Ratio to 800 MHz case**	**% difference**	**Estimated total cost, € billions**
400	3800	0.364	-63.6	**€ 13.0**
450	4700	0.450	-55.0	**€ 18.4**
700	8400	0.805	-19.5	**€ 40.5**
800	10439	1.000	0.0	**€ 52.6**
900	12100	1.159	15.9	**€ 62.5**

However, building dedicated networks from existing assets may not be viable in all MS. The assumption is thus made of a blended view, of 40% being new-build networks entirely and 60% having re-use of existing sites, with costs as follows:

Operational frequency MHz	**Estimated EU-wide total cost, € billions**	**Cost /user, €**
400	**€ 16.9**	€ 2,665
450	**€ 22.2**	€ 3,511
700	**€ 44.3**	€ 6,991
800	**€ 56.4**	€ 8,909
900	**€ 66.3**	€ 10,471

When including the savings made by re-use of sites in all MS, the effect would make a higher proportional saving at lower frequencies - over 30% at 400 MHz. Therefore network costs at the lowest probable frequency of 450 MHz, if available for dedicated networking, would be the most attractive. For this case, the savings from re-use of legacy sites could cut the total costs for the EU to around €20 billion. This assumes that the critical communications version of the LTE protocol (release 14 or after) will give the same or better range, building penetration and QoS for broadband at 450 MHz as at the commercial frequencies. However, it also assumes that the LTE Core and RAN network equipment at 450 MHz would have the same pricing as that at 800 MHz. There are questions over whether the more limited size of the 450 MHz market would increase equipment prices, as considered above. Moreover, building dedicated networks from existing assets may not be viable in all MS. Thus we make the assumption of a blended view of 40% being new-build networks entirely and 60% having re-use of existing sites, as shown in the second part of the table above.

How do these estimates compare with other proposed dedicated LTE mission critical networks? The Los Angeles area network, Los Angeles Regional Interoperable Communications System (LA-RICS) is designed for more than 51,000 users (34,000 first responders and 17,000 secondary responders, eg from public works called in during an emergency). Designed for advanced video and data capabilities it will also use IP voice over LTE (VoLTE) on its 700 MHz network. Due for completion in August 2015, under the FirstNet initiative for funding a major part of its $175Million cost for the 231-base station network based on a Band Class 14 eNodeB. This RAN will employ the 20 MHz of 700 MHz spectrum licensed to FirstNet under the terms of a spectrum-lease agreement. The network must meet the interoperability and reliability standards of the FirstNet system, exploiting an evolved packet core network. Its funding includes initial testing with 1,000 LTE vehicle modems units at 700 MHz. Average approximate cost per eNodeB base station is €560,000 (U$760,000). This compares with an estimated €330,000 Euros per base station for an EU-wide network based on new sites, but possibly with a lower average site cost per base station in the EU than Los Angeles and lower average core-network costs for cabling etc.

4.4.6 Overall costs per user

In terms of estimates of infrastructure cost per user terminal, and applying the same user terminal density as for the UK of 350,000 user terminals, for LTE at 700 MHz, this would indicate a sum of some € 6,990/user, but at 450MHz, some € 3,510 in capex.

The decisions on spectrum choices and LTE technology capabilities (ie with regard to standards development and frequency allocations) must be taken soon. For dedicated frequencies, eg at 700 MHz, or possibly 450 MHz, there is a window of opportunity in the run up to WRC-15 for European consensus that must be pursued, if this scenario is to continue beyond 2020 for broadband working. However the migration path is still unclear and so may require pre-standard hardened LTE in diverse frequency bands until a clear decision is taken at an EU or perhaps global level. Difficulties and delays in the standards process might force a change of the standards process to a new or extended (outsourced) body – which is possibly problematic.

4.5 Networking option 4: Hybrid solutions

4.5.1 Description

Because of austerity-constrained funding in parts of Europe and the limited amount of dedicated public safety spectrum, various models of mission critical communication are gaining attention. Many stakeholders see TETRA's lack of support for broadband as a serious problem which they wish to address with various "bolt on" schemes. Consequently, as a pragmatic solution, this option turns to the creation of a "hetnet" which integrates both existing mission critical voice networks, in the short term, with future broadband radio networks, both dedicated with their exclusive spectrum, and commercial mobile with licences from auctions.

Moreover such a hybrid hetnet solution could incorporate different cell sizes, which may then exploit different frequencies, rather than just a mono-frequency solution for the broadband successor to TETRA. Thus this option should offer stronger probabilities of meeting the diverse demands across the three sectors. To cater more closely to their needs it would integrate different types of networks, each suited to specific sector requirements. In summarised form, their demands could be reduced to:

- PPDR – TETRA style functionality and resilience with a broadband capability covering over 99% of the territory
- Utilities – very low cost, highly resilient monitoring and control for millions of sensors and controllers with relatively slow speed data rates but rapid time constants (5-10 ms). More often, FIXED radio networking is used, which requires few or no handovers or mobile features; mobile networks are used being conveniently available, proven radio technology.
- ITS – resilient voice and data, for managing transport systems such as rail signalling or response to road traffic accidents, with mobile applications.

As the subject is complex, due to the many potential choices which will also change and evolve with time, we first review the scope of network technology choices and then their application to the topography in which they will be used. We may then assign technologies to particular user environments. That then yields an approach to overall costing.

Moreover, a hybrid solution has the advantage of providing an opportunity to separate out some mission critical applications and support them in a way which allows other applications to then be less critical. For example, an optimised independent low bandwidth highly resilient service for ETCS would allow the criticality of voice communication to be reduced. Thus although a hybrid solution may seem more expensive, in absolute financial terms, when weighed against its advantages, it may in fact give better value for money than other options, in covering all requirements better.

The FP7 HELP project looked in depth at hybrid solutions and concluded that for a smooth transition, "multi-network solutions are definitely required, involving dedicated and commercial networks, as well as legacy PMR networks". A hybrid approach also offers a method of handling a transitional phase between technologies and media (from voice only to video) smoothly and flexibly. So for mission critical infrastructure networks, the term 'hybrid' would imply the most evident current and future technology choices:

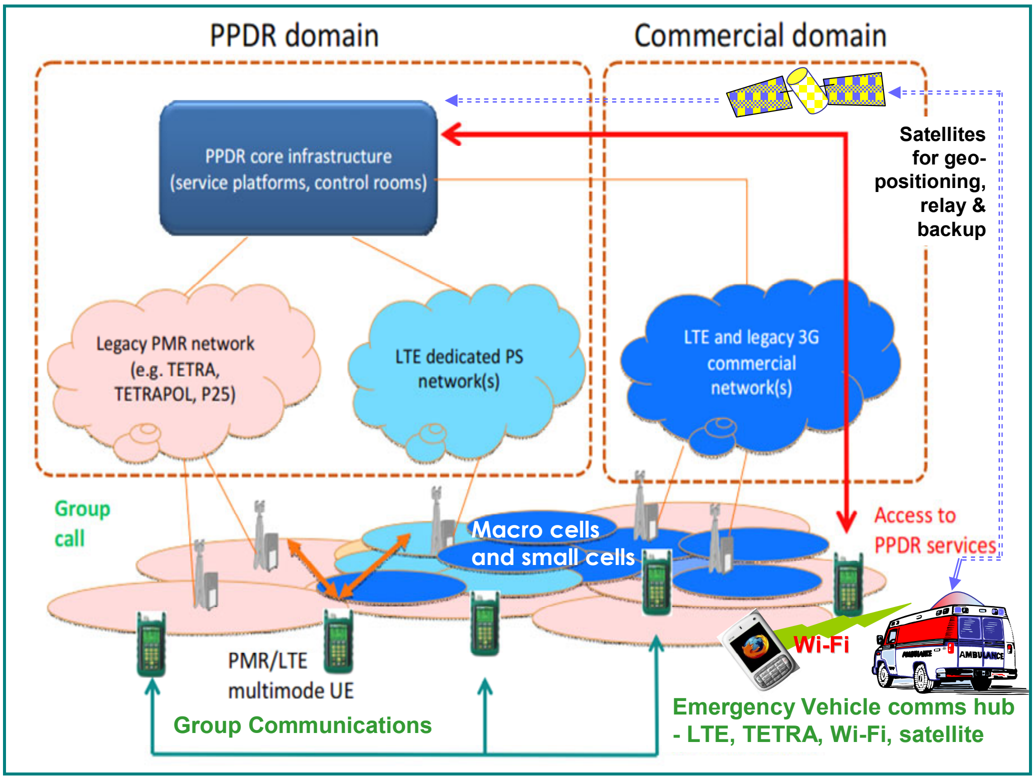
- "Legacy" TETRA voice, in a transition phase
- Commercial LTE broadband data, at sub-1GHz frequencies
- Novel options for dense urban working at higher frequencies, using commercial LTE for small cells, or unlicensed LTE; Wi-Fi in urban hotspots offers a cost-effective, simple solution which may enhance indoor service. One more even ambitious plan is to augment new and existing PPDR networks by a satellite network for small cell structures in dense urban environments, for example with a 2GHz satellite coverage .
- Re-use of legacy 3G and 2G commercial networks, with GPRS, EDGE and HSPA.

Such configurations are already being planned in some EU Member States, such as the UK. They are complex, combining not just dedicated TETRA and commercial LTE, but also the satellites and Wi-Fi networks mentioned, with any other mode of communication available, even amateur radio bands. They are aimed largely at PPDR but could also be for utilities if they could combine low speed data networks in mesh or capillary topologies. They may also combine sharing of commercial network assets with use of dedicated assets and these may be mixed by network types – eg shared RANs (usually commercial MNO) perhaps with a dedicated core network for reasons of security, connectivity to control rooms, etc, and/or cost. Moreover, in a commercially based RAN operation, roaming freely across all national MNOs would be a key goal.

The above analysis may be broadened by various alternative technology options that have been suggested to extend from a single monolithic platform based on one technology such as LTE. Many emergency services already envisage integrating other communications networks such as Wi-Fi and satellite, with communications hubs that may integrate 2G and 3G mobile in case of lack of coverage (eg by TETRA or LTE). Such schemes often propose use of the spectrum above 1 GHz. In the Solaris 2GHz satellite case cited, the focus is dense urban areas for high PPDR data throughput with good indoor coverage may be offered at a cost per bit that is substantially lower than the use of a 700 MHz network in the same area. A major advantage of the heterogeneous approach is the capability it offers for different types of users, not only the PPDR community. Support can be offered for the operations of utilities and transport by rail or road, despite their very specific demands - for example GSM-R functions that progress to ETCS Level 2 and 3 for 'signalling in the cab' for rail, or for smart grids and smart cities. Hybrid networking has the scope to support the different sectors.

Starting with the PPDR domain first, the diagram below summarises the integration in a hybrid network of the two major options for such networks – integrating both legacy and future technologies for PPDR:

Figure 4.7. Federating the commercial and dedicated network domains



Source: Baldini, G. *et al* (2012), with additions from observed live demonstrations of emergency PPDR communication.

Such hybrid configurations are not just speculative. There are already moves in this direction combining TETRA and LTE. For example, Rohill, specialising in professional mobile communications equipment, has announced its LTEtraNode system, a LTE/TETRA network. A pilot demonstration is planned with the network operator SETAR on Aruba, in the Caribbean, with public LTE integrated with TETRA networks to offer mission critical voice and broadband for the local emergency services on private and public networks. With Huawei and Alcatel-Lucent, Rohill is planning networks for the generic 3GPP defined frequency bands, plus other lower and higher frequency bands for specific coverage and capacity requirements. The aim is to provide the mission critical end user with access to the same data capacity and capabilities that already have been introduced for public networks, with enhanced availability, reliability and encryption. Here, Rohill and others are aiming further than the PPDR market at the other sectors – notably transport and utilities, including the oil and gas industry. Multi-mode terminals are part of this initiative, to be built to open standards, suitable for different applications.

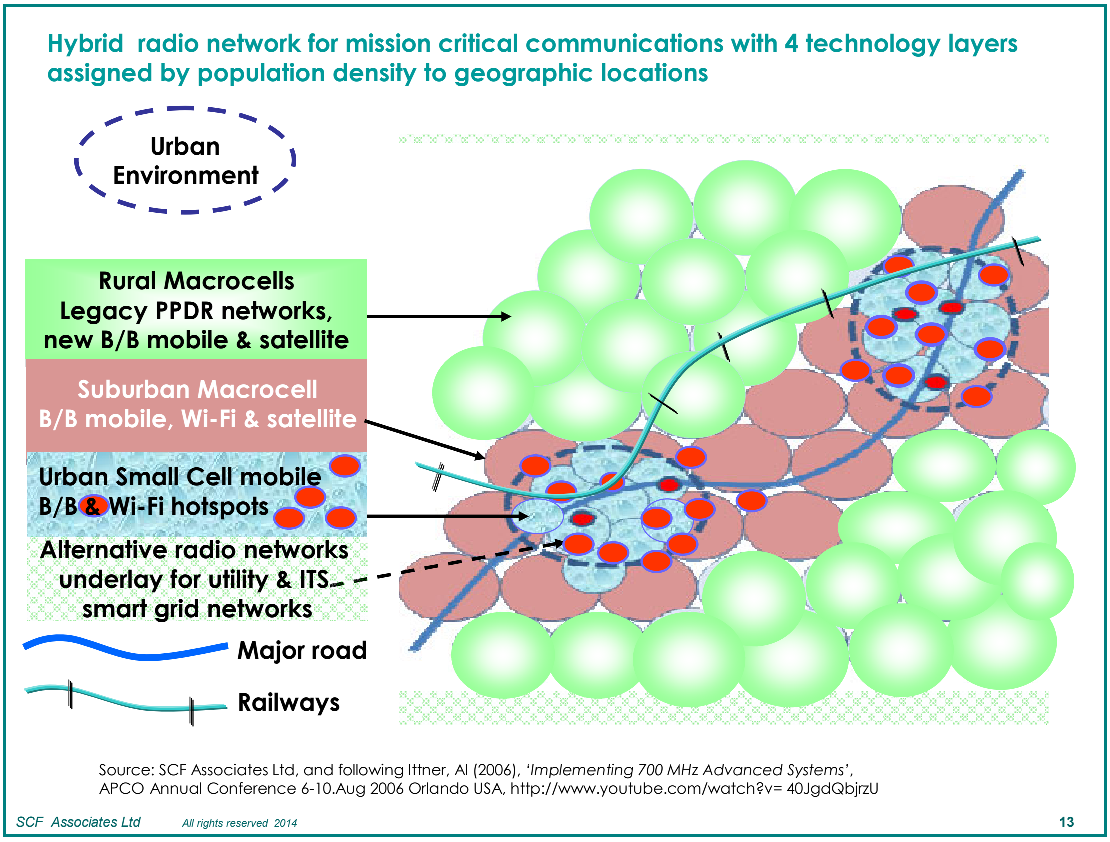
Management is more complex and requires clear divisions of responsibilities - and SLAs: However, this approach – if it is to be more than an ad hoc, temporary solution – requires a carefully managed commercial contractual structure. Ownership and operation would necessarily be more complex than in a homogenous unitary network, as a hybrid network can mix user-owned with shared assets and public assets, using subscription services and subcontracted support functions. As with Option 2, there is likely to be a need for a prime contractor as a single point of responsibility for management and security. A systems integrator who may be separate, is required to resolve hardware/software and terminal/base-station problems. These two entities must manage the changing technology situation within each subnet and develop strategies for migrating to new configurations as subnets are retired, during the migration phases. Multiple interfaces with commercial organisations are needed, implying a complex structure of service level agreements (SLAs).

There are financial advantages in short-term capex and also enhanced operational continuity: A key advantage of a hybrid configurations is that it enables existing TETRA networks (in which there is already heavy investment) to continue while broadband is added. "Bolt on" broadband could have mission critical and non-mission critical components, perhaps based on the use of dedicated, opportunistic and shared public wireless networks. In disaster recovery or emergency situations, first responders may have no choice but to use whatever communication paths are available, so multiple paths are likely to offer connection under all conditions. This is only a short-term financial saving solution, as gradually the legacy TETRA networks will be replaced. But there are other approaches as well: for instance, location-variable technology choices which match data rates to population density, which requires multi-mode handsets.

Options for the technical choices for a hybrid network: Combining LTE broadband with TETRA voice or TETRA voice with WiMAX or Wi-Fi have been common suggestions. Rather than deploying their own private LTE infrastructure, some in the PPDR community are considering deploying a limited dedicated LTE infrastructure footprint. It would exploit shared networks with commercial partners, in a multi-mode hybrid network, using the resources from commercial LTE networks, as in Option 2. The RAN is the prime target as this is so expensive. However, the future hybrid options here may go further and exploit satellite and legacy mobile systems (2G and 3G). One possible configuration is shown in the figure below, which tries to capture the reality of some ES operations today which match network type and population density. Such networks are becoming increasingly diverse, embracing satellite, Wi-Fi and multi-mode hubs as relays and command centres for a fire-ground or an incident-ground.

However the real advantage is the capability to integrate communications for the other two sectors of ITS and utilities, as replacements for GSM-R can be offered, roads and cities can be covered for transport modes plus integration of real-time low latency networks for smart grids:

Figure 4.8. Matching network technology to population density



The hybrid mission critical radio network has technology choices based on population density: The concept is for a hybrid variable data rate Mission Critical network with four layers:

- The base layer to start with is a narrowband network for voice for rural areas, perhaps a TEDS extension to TETRA with low bit-rate data capacity. Progressively it would be reinforced by mobile broadband, probably macro-cell LTE eventually (but initially with 3G UMTS HSPA, and also satellite back-up for data). Eventually TETRA elements would be phased out, by each MS, beyond 2018-2022.
- The second layer is a suburban broadband LTE network (bit-rate between 1 to 2Mbps and over). It shares the same base station sites with the legacy narrowband TETRA network, co-locating and adding further adding sites as necessary for its macro-cell frequency band, to cover areas of a higher population density – especially around the major traffic arteries. It may operate at any working LTE range from 450 to 900 MHz as permitted and available. It may mix priority use of commercial MNO LTE networks and dedicated LTE networks.
- The third layer is an urban broadband network, with small cells. As these broadband base stations have smaller coverage areas they may employ the higher frequencies - but will then require more base station sites. A small-cell configuration for LTE may use a higher frequency than 1 GHz, ie between 1 and 3 GHz depending on the balance between spectrum availability and cost limits, due to cell density. It may also use LTE-U, for the RAN and in directional mode for the first stage of backhaul to a core network access point. Integration with Wi-Fi acts as a supplementary layer for broadband offloading and general backup. Portable base stations may be added as required, eg at large public events or at incident sites such as fire grounds, to form ad hoc networks, established whenever there is a need for additional capacity. All these alternatives would link into macro-cell LTE or satellite, 2G or 3G, for connectivity on a best-served basis. Satellite coverage at 2 or 3 GHz is even possible.
- The fourth layer consists of integration with specialised networks for utilities and ITS sectors, such as smart grids in the licence exempt ranges (eg 870-876 MHz) and ultra narrow band cellular and WSD. The technologies for the non-PPDR sectors could also include Wi-Fi or other vehicle mounted short-range technology above 1GHz, possibly in the 5.9GHz ranges for inter-vehicle communications. Each of these alternatives could be linked into LTE or satellite, 2G or 3G, for longer-range connectivity on a best-served basis.

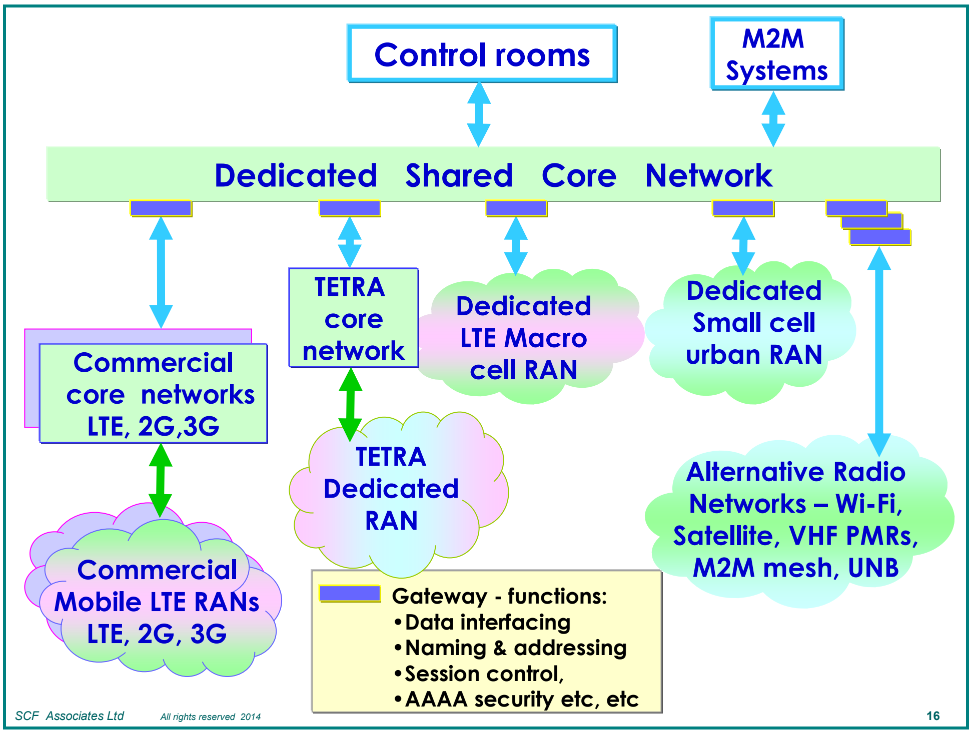
Such initiatives assume diversity of network technologies rather than a single technology, to offer redundancy and resilience through multiple paths. The availability of vehicle mounted hubs to extend the coverage of LTE systems and possibly TETRA, and to create local "hot spots" could also be harnessed. Mobile communication hubs are appearing in two forms: either as built-in equipment permanently installed in vehicles or as bolt-on TETRA/LTE/2G/3G/Wi-Fi/satellite pods on top of a vehicle, containing the antennae, transceivers and amplifiers, as well as back-pack units.

Also, satellites may be employed as an alternative backhaul connection, usually for data, such as medical images, but possibly for voice, when the latency can be tolerated. Effectively, satellite links are used to extend coverage into areas lacking terrestrial signal coverage. Hydra, for example, is a deployable LTE network co-funded by the UK government using Ka band satellites in a joint PPP with Quortus, Avanti and British APCO. It offers a private dedicated LTE overlay anywhere in the country. The satcom terminals have a 2km range for interfacing to LTE, or 2G/3G mobile, and a secure groundstation having dedicated fibre links. The use of Wi-Fi for use with commercial handsets/tablets is a common feature of such hubs. Two main diversity algorithms are used for the choice of voice or data path:

- The best quality of communication, usually the highest signal strength, or
- The cheapest communication link for the current environment.

Using a shared core network as the key integration layer is the principle of the implementation architecture. This is shown below in conjunction with the main components of the hybrid network:

Figure 4.9. Federating multiple networks into a hybrid multi-network – one suggested configuration



The layout above is just one possible architecture among many. Choice of a single design is necessary for costing proposes. Whatever are its key elements, they must provide the specific functions of:

- Federation - the shared core network acts to federate the various RANs. For building a heterogeneous network with legacy RANs and also for other networks for the non-PPDR networks, gateways for interfacing which include security feature are needed. As such it may be best served by an Internet Protocol (IP) using LTE IP technology for the future. Note that the Internet Protocol (IP) was originally designed for military fixed networks, so it may be adapted for mission critical communications, even though it has been often perceived as having no service guarantees but as just a cheap network without the reliability for mission critical communication.
- Gateways may not be necessary for protocol conversion for the native LTE RAN and Core networks but the gateway functions of security access, naming and addressing for a single namespace, possibly for extra encryption and for TETRA, etc, would be probably required.
- But resilience and prioritisation can be added: LTE on top of the shared core network provides procedures for prioritised handling emergency calls and for multimedia priority services, plus an end-to-end Quality of Service (QoS) framework with broadcast of alert messages. The core

shared network equipment for a mission critical network must meet high standards in terms of resilience, reliability and security, with its resources dedicated to mission critical services[70] .

- To carry multiple services for the different sectors, a form of a service-oriented approach that focuses on service scalability and quality, as well as per service end to end security will be needed (perhaps with an IP/MPLS structure). With a service aware infrastructure, priority services can be set up dynamically for mission critical applications, with guaranteed bandwidth for peak requirements, and for support of real-time applications.
- To handle all network protocols, multi-mode terminal equipment might well be required.
- Core networks from the different technologies may be progressively absorbed into the shared dedicated core network with time. A transition phase across the multi-network configuration will be needed as legacy networks migrate. This may use the application layer software as the integrating mechanism between network technologies, as shown in scenario option 2 above.

Note that with this approach there are several caveats and qualifications:

- Spreading applications and services across multiple networks using a software layer on top of the physical networks may only be the best approach for the initial stage of heterogeneous network integration, as used in the previous scenario to bridge multiple technologies.
- If operating in conjunction with the commercial networks, there may be a need for new SIM card solution – which may be multiple access for the various MNOs via one card, or indeed SIM-less, especially for the utilities, or just a software construct, set up by over the air (OTA) provisioning on demand (for the latter case, stronger security measures and encryption would be demanded, eg for ‘man in the middle’ attacks).
- For the small cell networks, the macro-cell LTE frequency could still be used. However, with spectrum available at higher frequencies suitable for smaller cells and also the emergence of unlicensed LTE (LTE-U), small cell technology could take advantage of those spectrum bands, at potentially lower cost. That would entail multimode handsets / in-vehicle terminal-hubs.
- The shared core network and possibly its gateways could be implemented for reasons of cost, protection and flexibility as virtualised functions (NFV), for a software defined network (SDN). This would offer far more flexibility for a transition between technologies as the LTE technology evolves with mission critical functions and also if the network migrates to commercial platforms from exclusive dedicated RANs.
- Cloud-based implementations may well prove too hazardous for mission critical operations, so dedicated or secure MNO data centres would be mandatory, while questions of judicial jurisdiction of data may be raised, for which tenderers in the recent bids have had to comply with, by providing proof of national custody of all data and evidence of national processing chains.

4.5.2 Value assessment

This hybrid solution targets investment where it is needed to increase socio-economic benefits for all the three sectors. A hybrid network approach for a mission critical environment offers high value as it can provide:

---

[70] FM49 White Paper, (2013), Federal Ministry of the Interior, Project Group on Public Safety Digital Radio; Federal Coordinating Office, Alt-Moabit 101D,10559 Berlin, Germany, On the Future Architecture of Mission Critical Mobile Broadband PPDR Networks, Version 1.1, 19 NOV2013

- Network functions on a basis of needs – not just for PPDR but with suitable additions can be made apt for utilities and for rail to replace GSM-R, as well as for other ITA applications, such as e-Call.
- It can be engineered to extend voice communications to video in an incremental manner
- A hybrid configuration offers continuation of use of TETRA sunk investments with parallel transition in a progressive manner
- The new functions of LTE for mission critical and enhancements (such as LTE multicast for broadcast) can be exploited as they are released progressively while harnessing other back-up technologies (TETRA, Wi-Fi, satellite)

4.5.3 Additional cost factors

There are various possible extra cost factors in this configuration:

- Inter-network gateways – for each network type to attach to the shared Core network – ie not just for TETRA and LTE at control room level, as in a simpler PPDR network in transition
- Multi-mode handsets which may be seen as necessity for workforces operating across multiple types of networks. Commercial smart phone handsets normally have Wi-Fi, 2G, 3G as well as LTE and also have Blue Tooth. However TETRA or TETRAPOL is outside the scope of the standard commercially based handsets in their ruggedised form
- The cost of progressive transition from a TETRA base to LTE
- Separated costs of spectrum are not taken into account – because for commercial networks they are included in charges and for many of the alternative networks they are licence exempt while TETRA usually employs a government granted licence.

4.5.4 Reducing cost factors

These include the introduction of small cells and re-use of several resources:

- Re-use of existing TETRA RAN sites as replacement for in a dedicated LTE network or as additional coverage need for an MNO-based RAN
- Re-use of existing core network assets – be it the physical ducts and switching sites, or possible even the fibre optic network cabling and distribution frames for control rooms, etc.
- Balancing macro-cells and small cells may provide cost advantages. For rural networks, wide deployment, where coverage outweighs the need for concentrated capacity macro-cells are the lower cost approach. For a high-density mobile network the primary challenge lies in adding more traffic in a crowded spectrum situation. Above a certain demand capacity density level, small cells and also possibly Wi-Fi solutions may be more cost effective than macro sites (above a threshold of 0.02 Gbps/km^2/MHz).[71]

4.5.5 Table of costs analysis

Defining and considering cost drivers of the network architecture is essential to the costing exercises. The basic system consist of eight main cost elements which include the legacy networks as well as the

---

[71] Madden, J., *Yes, LTE small cells are cheaper than macro*, 25 March 2014, FierceWirelessTech

replacement LTE dedicated and commercial networks with urban small cells as a future infrastructure component. Costing analysis for the hybrid infrastructure is based on the essential functional elements:

- Commercial RANs - with hardened 800 MHz LTE RAN and Core as interface (as in scenario 2)
- Gateways for all RANs to join Shared Core Network
- Shared core network (as the interface for all radio networks)
- Dedicated TETRA (legacy in transition- Scenario 1) RAN with own Core Network for interface
- Dedicated LTE-800 RAN - may be absorbed into commercial after 2026 varying by MS (scenario 3) - 450 or 700 MHz could be far lower investment cost
- Alternative radio networks for diversity - Wi-Fi, satellite, VHF PMR, mesh, UNB
- Legacy GPRS for utility and Smart grid, Smart city - 2G & 3G
- Small cell coverage - start off dedicated or commercial, as appropriate.

The vital element is the set of gateways for all RANs to join the Shared Core Network - for the interfacing gateway structure it is assumed that:

- Each MS has its own gateways for all technologies in use locally.
- Multiple gateways for each technology are deployed per MS, to avoid a single point of failure and also to give the capacity required, with minimal latency for delay-critical communications.
- Average of 10 gateways for each technology per MS, plus equal number of failover backup - larger landmasses may have more while smaller MS may have less. They may sited where topographically is the lowest cost in view of the layout of communications links (eg major cities) or wherever they are most protected.
- For alternative radio technologies (eg mesh networks for smart grids and machine-to-machine, M2M, applications) specialist gateways will be needed and costing assumes coverage of a complete MS landmass with low cost units.
- Gateways operate as much as possible in the lower OSI layers (physical and network) for simplicity, reliability and lower cost.

Conditions of operation and costing of the overall hybrid network system - various assumptions are made and summarised in the tables below:

- Each of the major networks would be built out from start of 2017 to 2026 with final stage only being reached at the end of 2031, five years later and each covers a specific setting (rural, etc).
- Legacy networks (TETRA and 2G/3G GPRS) would decline during that time, gradually, allowing for phased migration with testing of the new, by geographic area. Thus several networks in the same area would be operating in parallel, possibly through interfaces to the control rooms, which may also act as interfacing centres at operational level.
- Tetra networks decline with linear reduction of coverage until 2026, being supplemented by LTE broadband each year on a regional geographic basis (would need an overlap of 2 years to switch off each TETRA covered region).
- Base stations includes vehicle mounted communications hubs.
- All of shared cored network and interfacing gateways are built by end 2026 with EU coverage.

- Shared core could expand with time to absorb the core networks of other technologies .
- Cost for the LTE dedicated network is estimated for the 800 MHz frequency band as a maximum cost. Use of 450 or 700 MHz or a combination should significantly reduce the investment cost (perhaps by around 50%).
- Cost can be estimated as the capex cost to build new capacity, plus the opex cost to maintain legacy capacity that is being amortised, plus the cost of opex to maintain new capacity.
- All values given are approximations and best estimates, which can give no more than one specific outline estimate of the costs; Opex per annum is taken very simply at 15% of Capex invested value in that year.

Table 4.10. Nine basic cost parameters for the eight cost elements

Investment Cost per network technology (CAPEX)	Geo-graphic Location	Cost per cell, €	Cell coverage in km2	EU Coverage in km2	No. of cells	Start % of potential EU coverage	Net cost at start Mn € (end 2017)	Full roll-out cost, EU Mn Euros (end 2031)
1 Commercial RANs - with hardened LTE	Rural & Suburban Macrocells	167023	23	4201850	179436	10	2997	29970
2 Gateways for all RANs	All areas			4201850		20	31	157
3 Shared core network (	All areas	22039		4201850		20	835	4177
4 Dedicated TETRA (legacy in transition-	Rural & Suburban Macrocells	494462	79	4201850	53493	70	18515	26450
5 Dedicated LTE-800 MHz RAN - may be absorbed into commercial after 2026	Rural and suburban Macrocells	328164	28	4201850	148591	0	0	48762
6 Alternative radio networks for diversity- Wi-Fi, mesh, UNB, ..	All areas	200	1	4423000	5630808	0	0	1126
7 Legacy GPRS - 2G & 3G	All areas	100000	28	4423000	156411	20	3128	15641
8 Small cell coverage	Urban areas	6000	1	221150	281540	0	0	1689
TOTAL COST for the EU landmass for the hybrid network, millions Euros							**25507**	**127973**

Table 4.11. CAPEX: networks' value in operation

Investment Cost per network technology (CAPEX)	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	Final % of potential EU coverage	Net capex thru 2026 MN€	2027	2028	2029	2030	2031	Final % of potential EU coverage	Net Capex 2017 - 2031 MN€
1 Commercial RANs with LTE at 800MHz)	4346	5694	7043	8392	9740	11089	12438	13786	15135	16483	55	16483	17682	18881	20080	21279	22477	75	22477
2 Gateways for all RANs to join Shared Core	44	56	69	82	94	107	119	132	144	157	100	157	0	0	0	0	0	100	157
3 Shared core network (interface for all RANs)	1170	1504	1838	2172	2506	2840	3175	3509	3843	4177	100	3007	0	0	0	0	0	100	3007
4 Dedicated TETRA (legacy in transition- Scenario 1) RAN with own Core	16664	14812	12961	11109	9258	7406	5555	3703	1852	0	0	0	0	0	0	0	0	0	0
5 Dedicated LTE-800 MHz RAN - may be absorbed into commercial after 2027 by MS	2194	4389	6583	8777	10971	13166	15360	17554	19749	21943	45	21943	19505	17067	14629	12191	9752	20	0
6 Alternative radio networks for diversity - Wi-Fi, VHF, mesh, UNB	68	135	203	270	338	405	473	541	608	676	60	676	766	856	946	1036	1126	100	1126
7 Legacy GPRS - 2G & 3G	2894	2659	2424	2190	1955	1721	1486	1251	1017	782	5	0	0	0	0	0	0	0	0
8 Small cell coverage dedicated or commercial as appropriate	8	17	25	34	42	51	59	68	76	84	5	84	95	105	115	125	135	8	135
TOTAL COST for the EU landmass for the hybrid network, millions Euros																			**69254**

Note: assuming all can start in 2017, for build completed by end 2031.

Table 4.12. OPEX for hybrid network operations and support taken at a standard rate to 2031

Operational Cost per network (OPEX)	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	**Final % of potential EU coverage**	OPEX net spend thru 2026	2027	2028	2029	2030	2031	Final % of potential EU coverage	net Opex 2017 thru 2031
1 Commercial RANs with LTE at 800MHz)	652	854	1,056	1,259	1,461	1,663	1,866	2,068	2,270	2,473	**55**	15,622	2,652	2,832	3,012	3,192	3,372	75	854
2 Gateways for all RANs to join Shared Core	7	8	10	12	14	16	18	20	22	24	**100**	151	0	0	0	0	0	100	8
3 Shared core network (interface for all RANs)	175	226	276	326	376	426	476	526	576	627	**100**	4,010	0	0	0	0	0	100	226
4 Dedicated TETRA (legacy in transition- Scenario 1) RAN with own Core	2,500	2,222	1,944	1,666	1,389	1,111	833	555	278	0	**0**	12,498	0	0	0	0	0	0	2,222
5 Dedicated LTE-800 MHz RAN - may be absorbed into commercial after 2027 by MS	329	658	987	1,317	1,646	1,975	2,304	2,633	2,962	3,291	**45**	18,103	2,926	2,560	2,194	1,829	1,463	20	658
6 Alternative radio networks for diversity - Wi-Fi, VHF, mesh, UNB	10	20	30	41	51	61	71	81	91	101	**60**	557	115	128	142	155	169	100	20
7 Legacy GPRS - 2G & 3G	434	399	364	328	293	258	223	188	153	117	**5**	2,757	0	0	0	0	0	0	399
8 Small cell coverage dedicated or commercial as appropriate	1	3	4	5	6	8	9	10	11	13	**5**	70	14	16	17	19	20	8	3
TOTAL COST for the EU landmass for the hybrid network, millions Euros	**4,108**	**4,390**	**4,672**	**4,954**	**5,236**	**5,518**	**5,800**	**6,082**	**6,363**	**6,645**		**53,767**	**5,707**	**5,536**	**5,365**	**5,195**	**5,024**		**4,390**

NB: Opex has been approximated over the 15 year life as being static, at 15%. In fact it would be cyclical with the amortisation durations and renewals but the support and maintenance tending to increase at end of life of the various technologies.

In summary the total costs as first estimates for this scenario option can be summarised as follows:-

Table 4.13. Summary of costs for scenario 4

Aggregated costs item	Net expenditure over 10 years, € billions	Net expenditure over 15 years, € billions
Capex over rollout to 2031	**€ 42,351**	**€ 69,254**
Opex over l rollout to 2031	**€ 53,767**	**€ 80,594**
Total expenditure 2017-2031, € billion	**€ 96,118**	**€ 149,848**

Thus the approximated first estimates of the networking system are far more expensive than preceding scenario options but it offers the possibility of ITS and utility support at potentially low cost for the long term.

4.5.6 Overall costs per user

With its extended functionality and a (human) user population of 7 million mission critical operatives of various types across the EU-28 by 2026 is assumed. If the total cost is taken by only those operatives, the cost per user is:

- €13,731 for the first 10 years, then
- €21,406 when the full 15 year opex is factored in and all the features are rolled out.

However evaluation against a pure TETRA or LTE dedicated or commercial network with only human responders to PPDR emergencies is not a balanced comparison because it does not take into account the ability to handle M2M communications for mission critical functions for the utilities and ITS over its broadband capacity.

For each node (base station or mesh network access point, or similar for utilities, train movements or roadside communications) that could be at least 200,000 messages/second if multiplexed for a 20 Mbps bandwidth, handling real-time M2M applications such as control signalling, monitoring and alarm messages from smart grids, city infrastructure and vehicles of 250 bytes at 100 kbps with latency of under 5ms. Including this capability may be a fairer analysis of the value.

Hence, if some 40% of network capacity is devoted to this M2M traffic then the 15 year total cost per human user for the remaining 60% of broadband mobile may be taken as being approximately €12,800, or due to the 15 year roll-out, of the order of €860 per annum per human user.

If the network hybrid has the capacity to handle real-time controls for 5 million electrical supply substations and communications via mesh networks for smart grids with some 300 million attached metering points (approximately an average of 10 million points per MS for utilities and ITS), then approximations to the cost per data point for sensors and actuators may be made.

The approximate cost per monitored or controlled data sensor or actuator would be of the order of €200 over 15 years, or €13 / point per year, using 40% of the total capacity devoted to M2M.

Note that this assumes that data traffic from a substation can be taken as having a volume comparable to a monitored point, perhaps differing in data content and structure. It also presumes that the overall data volume is static, because more efficient coding is used that compensates for any further growth in the monitored/controlled points – and more reliable communications mean less waste (ie better resilience could mean that certain overheads in data transmission, eg Hamming codes, and resends, etc, can be cut).

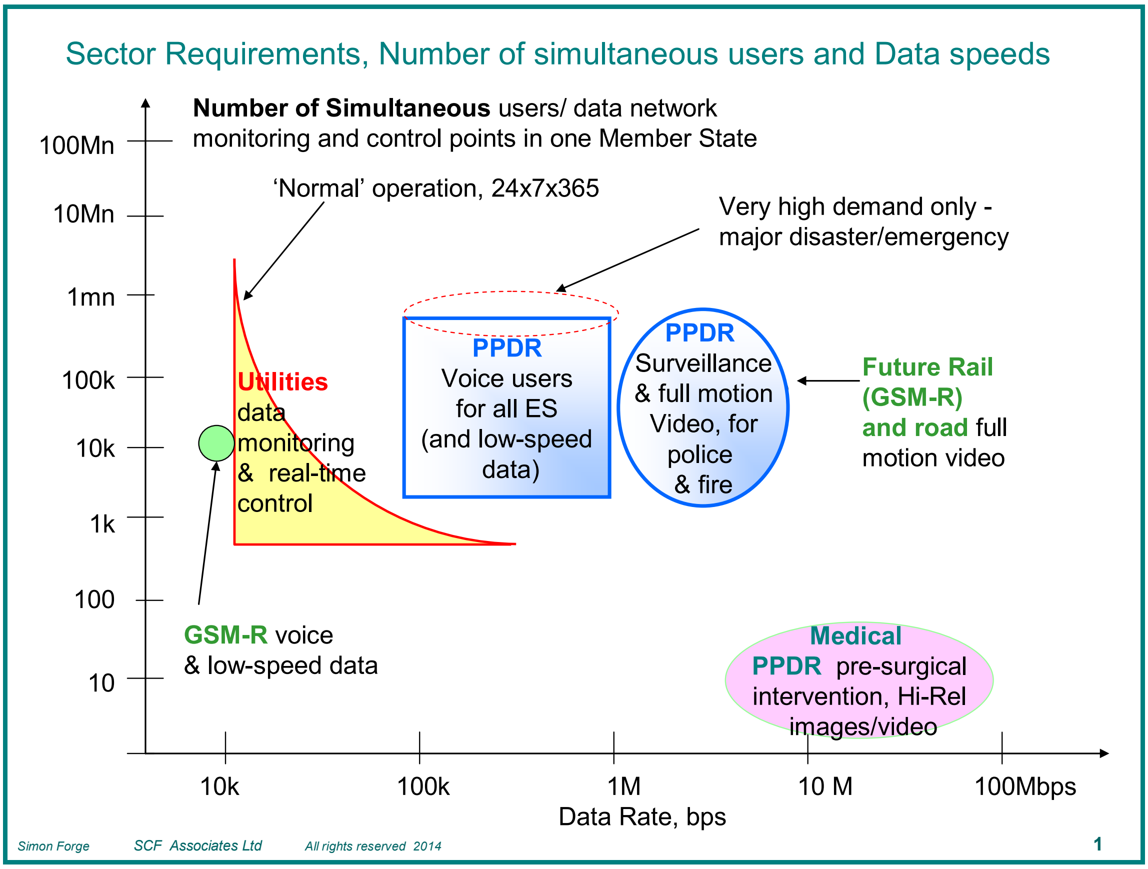
4.6 Networking option 5: A common multi-purpose network for use by all three sectors

4.6.1 Description of the option

Here the objective is to examine whether sharing of a common platform by all three sectors is feasible. However the concept must go further than the hybrid hetnet of the previous scenario, option 4. That explored a highly robust network federated from existing PPDR and hardened commercial platforms, with interfaces for smart grids in a heterogeneous mix, using a shared core network as its connecting backbone. The latter design is a really a pragmatic architecture for migrating between various network technologies while expanding the functional capability from one sector to three sectors, with high resilience.

Building a critical infrastructure for Europe *from new* is somewhat different to the previous scenarios. It implies founding a common basis for the sharing of a single platform by all three sectors, not an amalgamation of different networks. But is this sharing of a common platform by all three sectors really feasible? Here, it is necessary to return to the requirements of each sector, summarised in the figure below for bandwidth and capacity:

Figure 4.10. Differences across the three sectors in requirements: data rates and user numbers



What the figure shows is a diverse set of data speeds and user numbers, without much overlap across sector. That makes the search for a common platform difficult. However, despite these differences, the concept of a common mission critical communications infrastructure could become feasible as there are various areas of commonality and cases where the needs are complementary across the three sectors. One common prime need is for coverage and capacity in Europe's rural areas. More specifically the needs are common for railways and PPDR for rural coverage but both have, for much of the time, low capacity requirements. Utilities also need rural coverage for managing the transport of energy and water as well as for control of generation, rather than for distribution. The needs for each sector are encapsulated in the table below, which summarises the functional requirements from the perspective of broadband needs also:

Table 4.14. Comparing the three sectors' requirements for a common platform

Sector	Is the need for mobile radio mission critical?	Main demand now for radio networks	Future main demand for radio networks	Drivers for radio comms (now & future)	Need for mission critical broadband
PPDR	Absolutely: communication failure or delay may lead to death or injury	High resilience voice with team working tools & link to control centre	High resilience voice, video & broadband data	Protection & safety of lives & property	Limited but growing, esp. for emergency medical
Utilities	Important for low cost communication for increasing number of data points. Failure could lead to interruption of supply	Low data rates for control & measurement data; Need rapid detection of outages & load/voltage/ phase/ problems, with rapid response at low cost	Same as today but with more complex real-time management in high volume for distributed supply in-feed & demand	Network protection & efficient operation with new smart grids and Expected spread of smart metering	Absent, except for emergency teams & liaison with other services; high capacity may be useful for high volume data traffic at slow speed
ITS (Rail)	Limited: network failure causes delays; might pose threat to life	High resilience voice for safe train movement	Unclear but far more complex real-time management for faster operations and dependencies	Safe movement of trains and road vehicles. Higher autonomy and sophistication of vehicle control systems.	Low but may grow for safety of rail lines with higher speed & growth in road traffic density and vehicle technology.

The aim of a common platform would be to build anew. That implies use of commercial networks where available and appropriate would be limited to only where they fill a gap that cannot be filled by a bespoke network. It would require more network types than just LTE, whether in dedicated infrastructures or in networks shared with the public.

Table 4.15. Technical features and advances required for a common platform by each sector

Sector	Key features of a common platform for each sector in data and voice terms
PPDR	Voice/ video /broadband data applications for safety of life Voice /data/video for protection of public order, safety and security Voice /data/video- protection of property
Utilities Electricity, Gas, Water (-using Electricity as metaphor for all 3)	Distribution and load dispatch control for operational management, ms by ms, ie delay-critical, at slow data rates (usually between 10 kbps and 100 kbps) Alarms for outage detection and reporting Restoring service after failure, involving repair teams Threat to life from accidents/events, requiring repairs Keep regulatory obligations on sole responsibility and liability for failure
Rail **Road**	Train control for operational management minute by minute, voice and data Restoring service after failure, data reporting and repair teams Threat to life from train accident/events Threat to life – from road accidents/events - voice and data Traffic management - data

Thus in considering such a design, several practical factors must be included:

- From the table above, it becomes evident that a critical factor is the type of data being transported over the various networks. Different data types should be segregated as much as possible to maximise system performance and security. For example, there should be no way by which the transfer of mission critical data could be impacted by transfer of administrative data, such as email. A data prioritisation scheme is obligatory.
- Also much of the data for PPDR systems may be designed for person-to-person communication and should be separated from M2M based control systems communications. That may call for more network types than just LTE, whether in dedicated infrastructures such as LE mesh networks or dedicated LTE.
- Of particular importance for design of a common platform is the geographic coverage which the three sectors require. As noted, water and gas utilities have remote key assets to control and monitor, while PPDR must respond to incidents anywhere, including remote areas, where costs may rise but population density decreases.
- In the actual conditions within the EU, a further complication is the national sovereignty over matters concerning PPDR, telecommunications, utilities and transport. One way forward, in consideration of these political divisions, is to offer an optional infrastructure which each MS can move towards, depending on their capabilities and stance on the requirements for independence of PPDR, utilities and ITS.

4.6.2 Options for technical choices for a common platform

A possible basis for the foundation of a common platform could include commercial mobile networks, where appropriate for all three sectors. But that would not be the primary design motive. Instead, the prime architectural objective would be a highly robust infrastructure, for all three sectors. It would be designed for non-stop operation in crises despite failures of one or more of its segments, maintaining EU-wide service even under physical or cyber attack. Thus it would try to use the latest in resilient and proven networking technology plus an architecture that copes with very different sector requirements from the outset.

The design basis would be redundancy of connections (to at least four alternative routing paths for packets with triple processing and switching nodes, designed for service continuity during partial network failure or destruction[72]). The viability of such a network therefore depends on coalescing slow speed, large data volume data networks, as in the previous hybrid scenario, as well as broadband mobile radio for 'instant' critical communications for PPDR for video and voice.

This network, if so engineered, might form part of the critical infrastructure for Europe. As such it relates to existing European programmes, such as The European Programme for Critical Infrastructure Protection (EPCIP) and its network initiative ERNCIP (European Reference Network for Critical Infrastructure Protection) including the security and resilience of communications networks for smart grids and other networked resources.

The asymmetric data flows in most ITS and utility applications makes LTE's TDD variant preferable in a shared network. But PPDR may need the symmetric bandwidth provided by FDD. The combined FDD/TDD variant of LTE could be a compromise. That might imply a dedicated network or else a

---

[72] Baran, Paul, (1964) On distributed Communications, VIII, The multiplexing station, Memorandum RM-3764-PR, USAF Project Rand, August 1964; also, Baran, Paul (1964), On distributed communications networks, IEEE Trans. Comms.,01 Mar 1964;

multi-protocol LTE network (possibly with an MPLS type routing) adapted for a commercial platform, which would probably be based originally on FDD.

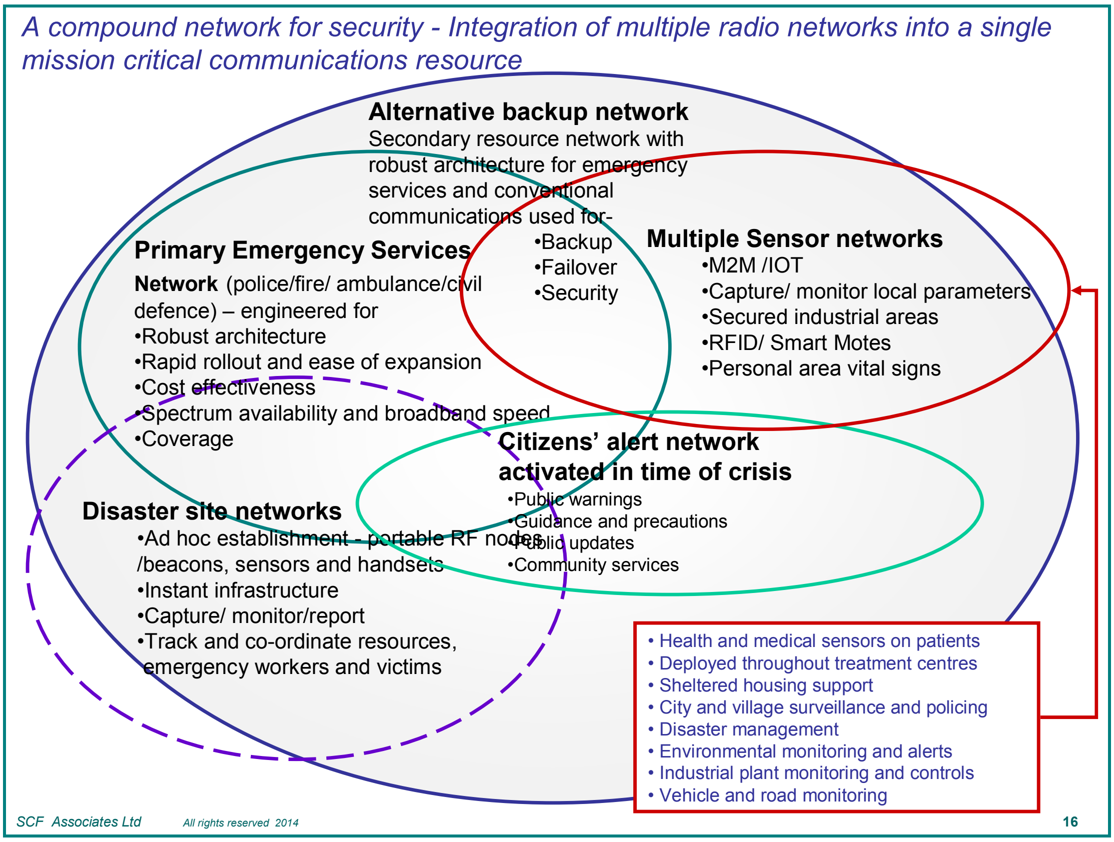
A crucial issue is whether this common platform should use its own dedicated spectrum - it is an open question, with several options. As noted earlier, the specific radio frequency range strongly influences the cost of the radio access network. As a critical infrastructure element, certainly it should deserve band – most probably in the 450 MHz or 700 MHz region, if commercial networks and their frequencies cannot suffice.

The lack of EU-wide agreements on the precise allocation, as discussed earlier in Chapter 3, may preclude a further spectrum allotment separate from public cellular. But if a common platform is to be built, that strengthens the arguments for a *dedicated band* or bands, perhaps in *both* the 700 and 450 MHz swathes.

In addition, licence exempt SRD networks will be an important component for the M2M applications. Thus, while commercial cellular might not be the whole solution, LTE may not be the right technology for all sectors in all situations. However it is in the nature of a compound network that a variety of different frequency ranges are needed to match their specific physical attributes with the needs of each subnet and application.

Accordingly for a common platform, an array or hierarchy of different network technologies and spectrum bands might be expected with interconnected functions and overlapping coverage for resilience. One overview of this approach is in the figure below:

Figure 4.11. Compound network architecture for critical communications for multiple sectors

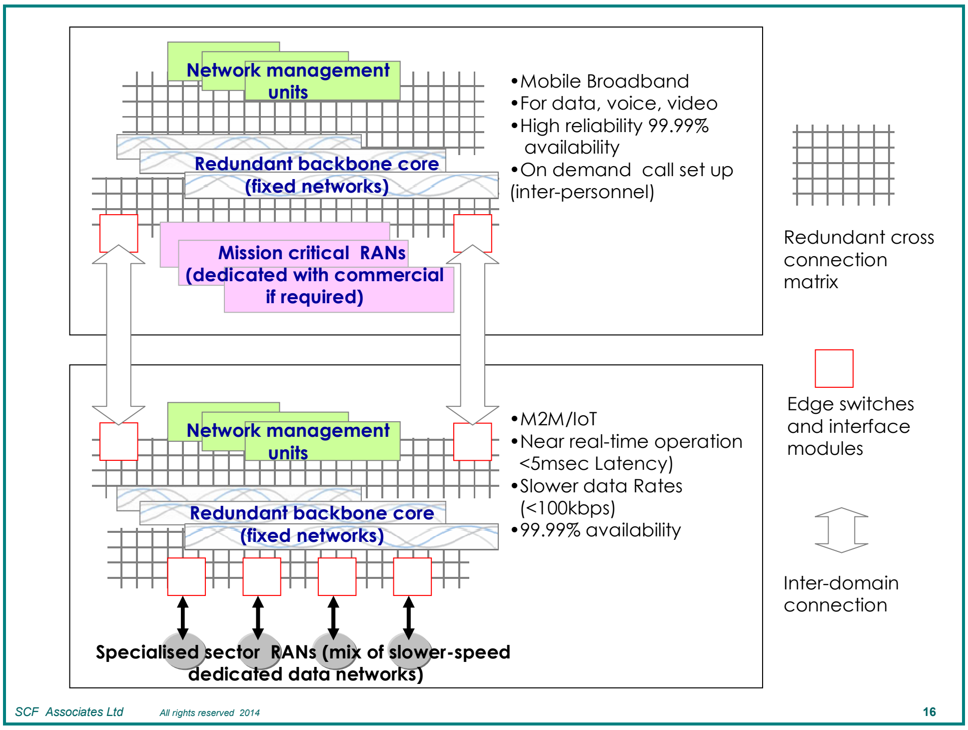


Subnets may inter-operate for applications requiring input from different data flows. The network as a whole might be self-organising, as in current mobile networks. Such structures were considered in the US in the aftermath of Hurricane Sandy, though not for a common critical services platform but principally for PPDR. Such a compound network would bring together a variety of supporting network technologies into a single platform, including:

- For low cost data monitoring, integration with mesh networks using lightweight protocols (SIM-free); especially useful for utilities and transport
- Hardened LTE: ideally a set of private dedicated national networks, but for reasons of economy, in some areas it may have to be based on infrastructure shared with or borrowed from commercial mobile networks
- Extra communications services with wide coverage on an opportunistic basis – satellite for data (voice unlikely), 2G and 3G commercial where working and available plus vehicle mounted wireless communication hubs with satellite links for ad hoc deployments
- For disaster areas and incident - portable base stations and vehicle mounted small cell sites combining Wi-Fi with cellular connectivity giving opportunistic network access capabilities to enable devices without a mobile broadband connection to access the internet through "found" local WLANs. This would be useful in regions with underdeveloped or missing infrastructure, in the wake of disasters or crises. It could also support utility and ITS applications

At the top of the diagram above is a key network not mentioned so far: a physically distinct and logically autonomous back-up network for emergency services. This back-up network could take over high priority functions of command and control, supporting sudden or gradual failover of the principal emergency network. Previous studies of common service platforms have focussed on the importance of a back-up layer with a common backbone with its own resilience measures to avoid being a single point of failure. Military experience with resilient networks in hazardous environments points to a more segmented structure to give higher resilience[73]; one configuration is shown in the figure below:

Figure 4.12. Integrating multiple service networks, with failover back-up



[73] One example is Walicki S., Brenner, R., (2013) NSWCCD-SSES Code 965, Mission Critical Interior Communications Networks Branch, Mission Critical Network Design & Implementation, US Navy, May 2013

In the figure, core network backbones unite multiple radio networks, separated into domains by function, for low speed data for M2M data functions and for mobile broadband. Such a compound network with its servers could be a platform for emergency service applications across the three sectors. An example of interworking is as follows:

Example of operation: One such application might be a context aware manager which collects and synthesizes information from multiple networks. For instance, an ambulance driving across a busy city is given real-time routing data from the city's traffic sensor networks. The medical team receives data on the casualties, including perhaps vital signs from victims equipped with body sensors. Meanwhile an environmental sensor network supplies information on explosive gases in the factory fire they are heading towards, and identifies the need for a fire-ground mesh network with an interface to the control room. That also alerts the utilities to the need to isolate the building electrically to reduce the risk of further explosions in adjacent buildings as gases escape. Such a network would be assembled "on the fly" for these specific locations and events.

4.6.3 Cost–benefit analysis

The compound network described above, with its resilient broadband bus, is a major investment. It could easily be the most expensive of all the network options considered in this Task. So it would only make economic sense if there are significant benefits or financial advantages for all three sectors and for society in general. The social benefits may be difficult to cost but it could be argued that such a network offers the most significant returns on investment over the long term of all the options discussed in this study, because:

- An EU-wide network would enable the PPDR services to be integrated into other sectors in a common platform, for full inter-operability in emergencies and in routine operations
- It would be the first public service network with a planned capability to cope with an international disaster across multiple EU Member States. The aim would be to deal successfully with the severe damage of a natural disaster, such as wide area flooding across several countries or a man-made calamity at the level of a Fukushima meltdown, requiring a large-scale evacuation.
- Climate change, with more frequent and larger storms as well as the prospect of rising sea levels threatening major population centres like Copenhagen, Stockholm, Helsinki, Amsterdam and London, demands preparation and response on a larger scale than Europe has considered in decades.
- The structure of this network would provide a uniquely resilient environment with multiple options and no single point of failure.
- This level of cost and capability only makes sense as a Europe-wide undertaking. It is too demanding to be a national system.

Cost sharing among the three sectors and across national frontiers is a pragmatic way to finance it, with the additional value of the capability to respond to large-scale catastrophes. Therefore the cost/benefits analysis turns not just on the issue of how much such a common network would offer the two sectors other than PPDR but also what it could offer in *extra European security and resilience* beyond a more 'conventional' PPDR network.

Research and interviews have shown that utilities, despite their innate conservatism and cost-consciousness, are keen to explore the benefits of infrastructure sharing as mobile communication architectures evolve, while rail also see the need to advance its networks. The utility industry recognises that in the future it may not be possible for each utility to own and operate its own communication networks. For the utilities however, the network control issues are not just technical or purely economic. They also involve regulatory concerns related to their operational and liability obligations, as well as social responsibilities for resource distribution and farsighted investment. Utility regulators across the EU hold the utilities responsible for service and supply interruptions, not the utilities' suppliers. That is why utilities feel obliged to control essential operating assets such as communication networks. However, under the right conditions, the use of a common platform could be advantageous if it is fit to purpose, secure and more reliable than a privately owned system.

The railways are in some ways like the utilities, seeking absolute reliability and availability for their train control signalling systems. A Europe-wide signalling system with high redundancy is very appealing at this time with the need to replace GSM-R. Cost sharing for the many Member States that wish to expand their rail networks, especially by adding new high speed lines, becomes an attractive concept.

4.6.4 Feasibility of a common platform for all three sectors

Six main factors control the feasibility of constructing such a platform. Essentially, all are barriers:

- Political: it is unclear if the Member States' governments could agree to cede control of national networks and concur on the setup conditions and agree on long term ownership, governance, management (and financing) of such a project. It might take years of European and national negotiations and probably multiple votes in national legislatures to build a Europe-wide network.
- The details of how to finance the initial investment and how to share the operating costs are not clear, particularly when the payback period may be thirty years or more.
- Governance structure: who sets up, administers, builds, operates and maintains – and with what contractual structure, financial controls and auditing. To interface with the three sectors, either a single MVNO or a service provider for each sector may be required, which could be a separate specialised MVNO.
- Security concerns: interfacing so many organisations creates security risks and conflicts between different standards and approaches to security. Some functions and data may require isolation as well as new agreements on access rights and responsibilities.
- Migration from the existing national networks: maximum re-use of existing investments is essential for making this network affordable. Migration planning is essential for success.
- Delay in creating an effective network: - a roadmap for the integration of existing national networks should reasonably allow at least five years of preparation before the foundations are laid and integration could begin.

4.6.5 Value assessment - a SWOT analysis of option 5

The scenario is quite different from the others discussed above. Its feasibility is questionable because it is so ambitious, somewhat amorphous and technically complex. A SWOT analysis gives only a qualitative value assessment, but outlines the key threats and opportunities:

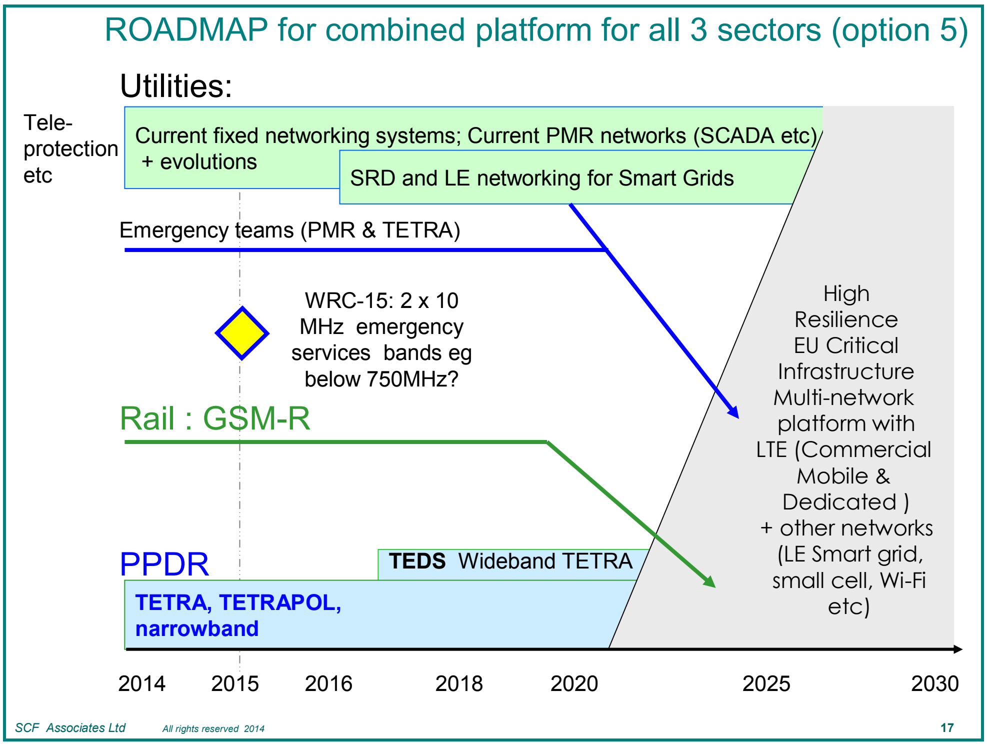
Strengths	**Opportunities**
▪ Co-funded by all 3 sectors ▪ Provides international inter-working between national PPDR, utilities and rail operators ▪ Pooled knowledge and resources can give a uniform level of service and security for the whole EU ▪ Provides a resilient environment with multiple technical options, diverse routing, and back-up/failover (no single point of failure) ▪ Can offer a higher function successor to existing fragmented systems with a migration path for existing systems and investments	▪ Gives capability to cope with international disasters across multiple Member States at a scale similar to the Fukushima catastrophe ▪ Provides an EU planned network for the emergency services to be integrated with other sectors in a common platform ▪ Offers complete interworking for everyday operations in the 3 sectors as well as for emergency situations
Weaknesses	**Threats**
▪ High cost ▪ Major political barriers - requires many bodies to interact and then to agree on common goals ▪ High initial costs for integrating diverse national networks ▪ Requires spectrum agreements across the EU on multiple common bands ▪ Incorporating changing technology will be a constant challenge	▪ If ill-designed, could act as a single point of failure in a major disaster ▪ Requires progressive ceding of powers by the three sectors and by national governments, reducing their capacity to manage and operate dedicated networks, powers they may not relinquish ▪ Even if they give their approval, MS governments might continue supporting rival national schemes that weaken the new offering ▪ May fail due to complexity, especially as it requires careful attention to SLAs and to network gateway interfaces

The threat items include the failures in negotiations and planning. Just preparing for a common critical communications network is a formidable task. The most difficult areas may concern national sovereignty, jurisdiction and responsibility. In practice that would require, at least:

- A large, multinational legal, operational and diplomatic planning team, working with all stakeholders from the MS governments and user sectors for several years, including military, security and civil defence organisations, as well as the three sectors.
- In parallel, a second team, to work with technology, operational and standards stakeholders, to approach design, by first quickly preparing a detailed functional specification for the three sectors and secondly a risk analysis of potential points of failure, weaknesses and mitigations.
- As the legal and financial framework would be at EU level, it would require all stakeholder organisations to actively promote it at the national and sector level, if it is to succeed.

One possible timeline for a migration path to 2030, also taking into account TCCA plans (which are largely aimed at the PPDR community) is illustrated in the figure below:

Figure 4.13. Overview of timeline for migrating to a Europe-wide combined services platform



4.7 The socioeconomic cost of disasters and emergencies

The preceding analysis is entirely financially oriented, being in terms of outlays and cost savings. A balance must be struck between costs of providing such a network and its socio-economic impacts. Analysis of such networks is not a pure cost-comparison consideration, although the cost of saving lives in medical emergencies, from injury and death prevented may be figured into that balance, as well as the savings on damage to property and costs of maintaining a secure environment. Limiting injury and preventing avoidable deaths provides a significant socioeconomic benefit, also measurable in financial terms. Broadband mobile offers a key opportunity for assistance at multiple points in the emergency call to reduce fatalities and the disabilities from injuries. Taking injuries due to accidents and violence, these are a major public health problem in the EU:

- Injuries are the fourth most common cause of death, after cardiovascular diseases, cancer, and respiratory diseases. Every two minutes one EU-citizen dies of an injury.
- More than 233,000 people are killed in the EU-27 each year (annual average 2008-2010) and disabling many more due such injury in accidents and violence.[74] Deaths from road transport account for nearly 16% of all injury fatalities. According to WHO mortality figures, the annual toll of road transport in the EU is about 38,000 fatalities. For each EU fatal injury case, 25 people are admitted to hospital, 145 are treated as hospital outpatients and more seek treatment elsewhere, e.g. by family doctors. Consequently each year a 5.7 million people are admitted to hospital and 33.9 million people are treated as hospital outpatients for an accident or violence related injury.

Broadband mobile would offer better routing and dispatch of the PPDR services to accidents with mapping data and locality images. For injury it could offer telemedical support for paramedic personnel at the incident ground, real time information on patient condition, hospital availability for

[74] European Association for Injury Prevention and Safety Promotion (EuroSafe) (2011) "Injuries in the European Union 2008-2010, Summary of injury statistics for the years 2008-2010, issue 4

critical care patients, hospital operating theatre preparation using injury imaging and patient monitoring, telemedical intervention en route to hospital with accurate navigation capability,

With a figure of €2.1 million per life.[75] and a 5% saving due to mission critical services being better able to intervene in emergency, through medical services and police intervention, this equates to €24 billion saved per year across the EU. A 10-year aggregated figure would pay for any of the scenario options presented here, including scenario 5. Also a one per cent reduction in service quality equates to a socioeconomic cost of €4.6 billion encompassing 168,000 incidents that could be at risk.[76]

For medical emergencies one example is 'out of hospital cardiac arrests' (OHCA). For this type of emergency, during each 100 ambulance calls, research indicates 'avoidable fatalities' occur on route. So around 1,858 OHCA deaths could be avoided in the EU if ambulances were able reach 75% of critical ('Category A') patients within 8 minutes.[77] This equates to a socioeconomic value of €3.8 billion per year, based on the value of life figure of €2.1 million.

Therefore, which of the five optional scenarios is optimal for the EU? Overall results from comparing the five scenarios are summarised in the conclusions with key recommendations, in Chapter 6.

[75] Grous, Alexander (2013) *Socioeconomic Value of Mission Critical Mobile Applications for Public Safety in the EU:2x10MHz in 700MHz in 10 European Countries*, Centre for Economic Performance, LSE, UK, Dec 2013
[76] Grous, A., (2013) *ibid*
[77] Grous, A., (2013) *ibid*

5 Current Use of Commercial Mobile Networks for Mission Critical Communications

Here we look beyond Europe, as well as within, for case studies across the three sectors that reveal interesting aspects of the mission critical/cellular nexus, and that could act as pointers to the future, with directions to avoid as well as to follow. These cases highlight practical arrangements between public/private entities in charge of those sectors and commercial mobile operators, the required parameters of wireless communications services, the design and overall viability of such networks as well as cost information.

5.1 Case study: UK Emergency Services Mobile Communications Programme (ESMCP)

5.1.1 Background

The UK government via the Home Office plans to replace its Public-Private Partnership (PPP) contract with Airwave Ltd. for the national TETRA network serving 275 000 emergency services personnel. Airwave is a narrowband network under a contract that would have to be relet, if not replaced. Current Airwave user contracts have 15-year lives, running out in 2015/2016 (e.g. for the UK police). Currently the Airwave contract charges approximately UK£400Mn/year and covers the UK with a fairly reliable voice network. Airwave's network uses 2 x 5 MHz bands at 400 MHz granted by the Ministry of Defence, a grant that will continue to 2020 at least.

The Emergency Services Mobile Communications Programme (ESMCP) is the Home Office initiative designed to replace Airwave, which still has an operating contract ending in 2020. Introducing a new phase in PPDR support, the Home Office's Emergency Services Network (ESN) for broadband support of PPDR services is based on commercial LTE.

In deciding to pursue a commercial replacement option, the key question facing the UK government was: can the UK afford a dedicated private dedicated network with TETRA (or a successor) technology? In an age of UK austerity, with over 30% cuts scheduled by central government for public sector budgets progressively over the next five years, Airwave is considered too expensive and too limited in functionality. In particular its technology does not enable broadband. Airwave was viewed as a single purpose network: emergency services voice only. Hence at the outset, four options faced the UK government:

1. Do nothing: ie continue contracts with Airwave, perhaps with the latest TETRA technology;
2. Use existing commercial MNOs' LTE national networks enhanced with UK landmass coverage, hardening, diverse routing, UPS (Uninterruptible Power Supply) and non-blocking upgrades for resilience;
3. Go hybrid: ie use the existing or upgraded TETRA plus a private LTE network for broadband;
4. Build a bespoke dedicated private LTE network (which would need its own spectrum, probably in the UHF band).

From a detailed cost/benefit analysis, the Home Office chose the commercial network (option 2) based on its business case, which came out better than a private network option. It responds to the view that a new, more cost effective solution is required today for PPDR services. The ESMCP development project is currently in start-up phase with calls for tender to be adjudicated by September 2014 following two rounds of submissions. Migration from the Airwave network should begin in 2016. Thus, at time of writing, this project tender is at a critical point and certain detailed information is still confidential.

The advent of a commercial technology with high data speeds, LTE, is being used as an opportunity to break with Airwave and to move to a commercial basis for network provision. It will be based on contracts with Service Level Agreements (SLAs) using the two major MNO owned networks in the UK, EE and Telefonica/Vodafone, for broadband mobile infrastructure. Contracts are now in the bid phase with evaluated results to be declared in September 2014.

The decision to replace the current TETRA based emergency network was taken on strong financial grounds, as the PPP contract only allowed for increases in annual changes under an agreed formula, with no possibility of downward revisions. In an epoch of ongoing austerity, such contracts require governments to rethink the requirements of emergency services' communications.

The ESMCP project is staffed within the Home Office by some 45 full-time professionals. They include specialists in legal contracting, large scale procurement and contract negotiation, as well as the technical side. They are led by an experienced procurement and contracting specialist from the Ministry of Defence.

5.1.2 Major features and technical architecture

The ESN will be set up for both mission critical and non-mission critical mobile (broadband) communications for the ES and related services on purely commercial LTE national networks. For PPDR, the ESN must offer Airwave equivalent functionality, with the same or greater resilience but at far lower cost. It must be compatible with commercial terminal equipment if a particular ES so requires. The special responder features of TETRA (group call, PTT, DMO, etc.) must be supported but with broadband as well as voice, for officers on foot and for vehicles. Naturally this demands the capability for tiered emergency priority in disasters. Primarily, the future ESN must support Airwave's 247,000 current users, plus some 40,000 vehicles, 200 control rooms for 49 police forces and 50 fire services, plus regional health trusts for ambulance. The aim is to complete a concurrent transition across the UK in two years.

The basic objective is to provide a connection platform for the ES, enabling them to invest in their own applications at the terminal equipment level. Hence they may use commercial handsets, so the primary user communities will purchase and install those apps that characterise their particular service.

However, a future ESN should also be available for several groups of secondary users with lower priority, who may need to share the higher security features of the ESN platform, being public services but not first responders. These authorised sharers of ESN would include specific units in the Ministry of Defence, tax and customs services, central government departments, the Border Force, the Ministry of Justice, 378 local authorities, as well as certain emergency departments in utilities (gas, electricity, water) plus the railways, the Bank of England, the Royal Mail and many transport authorities for ports and airports with their own emergency and fire services. Users are to be divided geographically into 12 regional groups, each of 11,000 to 50,000 users.

To provide such a network, the project is based on 4 contracts, or lots, with Lot-3 being contracts with the MNO while Lot-2 relates to ESN network build through systems integration and Lot-1 to overall programme management. This structure is aimed at ensuring compliance with SLAs and a managed roll-out. Migration from Airwave is expected to take to 2020 at least and Airwave will continue to offer service during that time.

The Home Office has performed a detailed economic study based on an outline business case (OBC) for building a commercial model of operations with government funding of ES users. Hardening of commercial networks will be paid for by the UK government under Lot-3. The user population is expected to be 350,000 to 400,000, at minimum. On the question of transgressing State Aid rules for the MNO network upgrades, the Home Office have verified that their proposed actions and support provoke no contravention.

The whole project is thus reliant on the MNOs seeing the PPDR market as attractive – which they appear to do so. It is considered as another premium rate business market with highly specialised requirements and additional systems, but with the extra specialist items paid for eventually by the client.

The ESN's technical architecture is to be based on the current LTE standard release but with an extra PPDR capability, which will be carefully specified. The Home Office team have worked on the interim standards necessary and have a preferred set, which also covers the transition from TETRA. Thus the initial programme does not expect to use separate (or new hardened) network elements but instead upgrade the existing LTE eNodeB base station equipment already installed, with greater autonomy from mains power.

Note that the lower power demands of modern LTE transceivers and backhaul interfaces mean that back-up batteries may be employed at cell sites (with several days' autonomy) instead of LPG/diesel generators. Power demands drop dramatically for an LTE eNodeB (perhaps from 10-20kW to 1.5 – 2kW) using self-organising energy management, especially with local renewable sources.

During migration and switchover, the 2 networks (Airwave and ESN) will be active simultaneously and so will require real-time data interfaces. These are to be implemented at the control room level using an IP interface module between the 2 network systems. Interestingly, the network is expected not to need extra maintained reserve capacity, as saturation is not considered likely: the LTE priorities system can curtail the data rates of downloads and streaming by commercial customers to give ES priority for data and voice. There is also an ES requirement for pre-emptive capability, for priority access, with prioritised call queuing, a feature which is limited in the current Airwave system. The network designers also expect to exploit cell overlaps as a form of resilience, i.e. for failover to an alternative base station. Design of the end-to-end security architecture is still evolving.

On the question of whether ES operations might in reality need some form of overlay dedicated network with their own frequency bands, separate from the commercial network, this is considered unnecessary, as it is assumed that the commercial solution will be completely effective. Employing each MNO's assigned spectrum avoids the need for extra bands. The commercial option is also expected to cover any future new specialist applications which could demand spectrum for reasons of priority, capacity or extended coverage range at lower cost.

For the Technical Specifications, the design policy is to use open international standards, currently 3GPP Release 12 for LTE. Proof of concept tests, implemented by Qualcomm and Huawei, have been completed in Mexico. Also tested were the Proximity Services for DMO, with the aim of achieving the same technical specifications and performance in the field as for Airwave. A major requirement (and challenge) is to provide a constant data rate over all of a cell, for all cells, and for all ES users equally - but with the capability for tiered emergency priorities in the event of disasters or vital interventions.

The LTE pilot testing confirmed that the planned network can support simultaneous call set-ups for 100 ES officers in the same cell while carrying heavier than normal commercial traffic.

Many key technical specifications at the application level are to be defined by apps hosted on ESN handsets. Some backward compatibility is implied here, as that handset may be a 3G phone - not necessarily the latest LTE-A smartphone. The ES also need certain features such as in-tunnel connectivity which Airwave has in some areas. Transport For London may require that across London for its underground metro services, presumably via leaky feeders. A capability for ground-to-air communications for low flying aircraft (probably up to 1000 meters altitude) is also envisaged. Such additions come under a special contract (under Lot 4).

Current specifications for the expected Android type handsets might use the Open Mobile Alliance (OMA) specification for the Kodiak PTT function over cellular based on an enhanced IP Multimedia Subsystem (IMS), although quite how OMA and 3GPP LTE specifications will work together is still unclear. Also there is a hope that for in-building and edge of coverage operation, MIMO antennae will be in service for higher effective receiver sensitivity as well as for handling potentially higher user density to maintain data rates. For broadband data terminals, specialist ruggedised kit is already available from major PPDR suppliers (eg Selex, Motorola, etc). But the Home Office is now asking whether specialised devices will always be needed – or can apps on ordinary commercial devices provide the functionality demanded?

5.1.3 Levels of infrastructure sharing

The ESMCP aims to maximise sharing of commercial infrastructure with the emergency services. The intent is to be entirely dependent on the main commercial MNOs (EE, Telefonica, Vodafone and possibly BT – Airwave has also been accepted in the first qualification round) sharing their infrastructure. One hurdle for the project is that UK coverage of Airwave is 98% of the landmass but MNO commercial coverage is around 85%, so the Home Office would have to add some 14% of coverage. That addition will be part of the Lot-4 contract. During the transition period up to 2020, Airwave's TETRA network will remain in place with an extension of its 2016 contract, so the load would be shared between TETRA and LTE networks during the first 4 years (the migration phase) of the new contract. Moreover the MNOs do not have the resilience built into their base stations that Airwave has. Recent flooding in Ireland highlighted the potential weaknesses of the commercial cellular networks, where 20% of the networks' base stations were out of service but the TETRA network continued due its design of overlapping cells, so an alternative cell was usually available if a base station became flooded.

Also, commercial mobile networks in the UK typically have 5 hours of autonomous power whereas the PPDR sector prefers up to 7 days (168 hours) of UPS as well as diverse routing and no core element failures (e.g. the packet switches or home location register [HLR]). So the key question for the Home Office is how much funding will be needed to bring commercial cellular networks up to the required PPDR resilience level of perhaps 99.999% availability, and handsets to the levels of ordinary TETRA terminals, if 100% dependence on the Commercial networks is to be achieved.

5.1.4 Structure of the contract and SLA provisions

Financial structuring has been carefully prepared and is reflected in the contracts proposed. For the first of two rounds of bidding, the Home Office has set both maximum and minimum financial limits, presumably to avoid tenderers underbidding with non-realistic levels of resources for the project. These financial limits are drawn from the complex cost model of the ESMCP network and its operational structure. In 2020 or 2021 these contracts will be rebid. The programme has a contractual structure of four primary lots:

Table 5.1. Structure of the ESMCP contract awards

Lot and title	Role of contractor	First round limits on contract values
Lot 1 - Delivery Partner (DP)	Managing the transition programme from old to new systems. Overarching organisation for programme management and transition services for implementation and rollout. This lot includes transitioning 200 control rooms as required by conversion from Airwave. Tenderer for this lot alone must be separated from other lot bidders.	**£60m- £95m**
Lot 2 - ESN User Services (US) provider	Providing an enhanced mobile communications network service with enhanced availability for the emergency services and highly available full coverage. Requires all systems and networks integration. May include supply of equipment and apps for ES use – i.e. handsets and special network equipment, ruggedised with support such as a device catalogue via an apps store and its management (this may become a separate contract).	**£120m- £245m**
Lot 3 - ESN Mobile Services (MS) provider	Providing the resilient connections into commercial mobile network(s) with data as a premium service for coverage and resilience. To be based on an enhanced commercial mobile service with maximised availability for the ES and full landmass coverage.	**£200m- £530m**
Lot 4 - ESN Extension Services (ES)	Providing a highly available telecoms infrastructure, covering parts of the UK outside regular mobile network coverage. Edge coverage beyond commercial footprint - Extensions of existing LTE networks to cover UK geography not covered by normal commercial networks (ie extend from 85% to over 95%) also specific cases eg tunnels, air-ground-air, etc.	**£175m- £350m**
Total costs		**€ 694m- €1525m (£555m - £1220m)**

Source: UK Home Office

The Programme Bid Selection Schedule is as follows:

- Full business case with chosen configuration and bidders pre-selected (January - March 2014);
- Business case approval by central government at first gate by end March 2014: Summary Outline Business Case (SOBC) estimates of costs and time are then delivered for the UK government's Major Projects Review panel, MPRG;
- Tenders from the Lot bidders are returned (end of May 2014);
- Evaluation tenders in 4 Lots (by September 2014);
- Contract award (April 2015);
- Mobile service with MNOs commences (late 2016):

- Mobile Services under 'LOT 3' has its first contract covering 2016-2021 then re-procurement for 2021- 2025.
- Mobilisation and installation, with rollout and commissioning, is expected to take some 18 months for the largest part but at least 4 years is expected for complete migration from Airwave.

From "Day 1" a national LTE service may be required but not all there. So progressive migration from Airwave can be expected, an incremental rollout geographically, as the Airwave contract will continue to 2020 alongside the LTE-based ESN rollout.

Building up from a level of few users who are paying for services initially, the MNOs will have to be compensated by some incentive premium in advance during the first start-up phase when usage is low, to help justify the MNO's prior investments in 2014-2016, adding resilience and handling PPDR services into control rooms. Therefore some of the lots are front-loaded, i.e. as the majority of expenditure is expected to occur with build, in the first years, with far less later for maintenance. In contrast, some Lots will be annual rolling contracts. Note that the operator could be an MVNO (perhaps specialised) rather than an MNO, and Airwave may also bid. There are timetable risks as certain principal events may intervene, e.g. the UK elections in 2015.

In addition, the UK ESCMP will purchase wholesale mobile capacity (in the form of data sessions at agreed speeds and voice connectivity minutes) from whoever will be the first MNO contractor for the first contract (the Lot 3 providers in the ESMCP project tendering). This extra contract is to be let over 2016-2021 on behalf of the ES and would cover "business critical" services. Such procurement of wholesale capacity could bring a major expansion of the commercial MNOs' traffic – and with it, their revenues – as the ESMCP procures both mission critical and non-mission critical mobile (broadband) communications for the ES and related services. Note that this provides a strong lever and incentive for the MNOs to:

a) Participate in the mission critical offering
b) Keep to the SLAs, as infringement could exclude them from the tied government business critical contracts that accompany the mission critical role

Furthermore, the number of users of this "business critical" mobile service could be much greater than for the mission critical broadband contract itself. For instance, there are some five million staff in the PPDR sector in the EU but only 1.5 million TETRA terminals and even allowing for three-shift working in some services, this indicates a strong business market. The wholesale pricing for the MNO services will be regulated (i.e. capped) by the contract terms and supervised by the Home Office. However, the question for MNOs in a saturated market becomes: can we afford *not* to participate in order to draw on these new revenue streams?

Overall, the mechanism appears to be a sort of 2-sided market, as the Home Office buys in bulk at wholesale prices and the various PPDR users then use their communications funds to purchase capacity from the Home Office. Moreover, the capacity that the PPDR and other public sector users can buy for their non-mission critical mobile needs will replace the current mobile contracts for voice and data – a further financial incentive for the MNOs to co-operate strongly.

5.1.5 Levels of risk of the whole venture, expected resilience and final liability

The key risk is that the programme is based on the MNOs' dedication to maintaining quality of service for the emergency services, which may fail sooner or later. To analyse the various risks, a strong emphasis has been placed on three key areas:

a) Analysis of the commercial risks of using the LTE MNOs;

b) Comparative analysis of costs of the various options via business cases, for a dedicated network, a shared network and wholly commercially-based network;

c) Review of the technical aspects by using the MNOs to provide "proof of concept" pilot demonstrations (due to the current early status of LTE standards development, pilots have been based on 'pre-standard' LTE equipment).

For the analysis tasks, the Home Office built a 15-year model of LTE commercial operation for the PPDR services and found it significantly cheaper than the alternatives over that period for voice and data. To assess the failure likelihood of the whole procurement, modelling has also been used, with a quantitative risk assessment (QRA) having an optimism bias and reference class forecasting (as used for other high risk government funded projects, such as NASA's plutonium fuelled spacecraft – which it ruled out). This model took around a year to build.

Results of these Home Office studies so far indicate that satisfactory resilience compared to Airwave can be added for the future commercial LTE networks. Resilience will be dependent on MNO implementations – and MNOs will be asked to provide incremental resilience, built up from commercial levels. Resilience will thus increase over time – and so there is a time factor in the resilience expected.

The real question about resilience is the comparison of the situation today of the MNO commercial networks and Airwave. About a third of Airwave's 3800 UK sites have UPS – but not all. And this fraction was only expanded to the current level of coverage after the July 7th attacks in London in 2005. The commercial networks have autonomy of only a few minutes today, and far more base stations – around 18,000 in their 85% UK coverage, so 5 or 6 commercial MNO sites cover one Airwave site. (The operating frequency differences – 400 MHz for Airwave and 800, 900 MHz, or even 2.6 GHz, for commercial networks – explain the differences in cell densities).

The aim is to harden those LTE sites where continuity of service will be needed most – i.e. a selective approach – for hours of autonomy or perhaps days. The UK road network is to be used as the basis for coverage. The aim is to have 5 to 7 days autonomy for the key ESMCP sites, just as Airwave has for some 30% of its sites today.

Resilience would be further enhanced if there were several MNOs and they all agreed to roaming between them dependent on signal strength. However the MNOs apparently claim such domestic roaming is not possible. It is unclear why that should be, as there is no technical reason why such handovers cannot occur. Domestic roaming based on signal strength could easily be added to the extended functionality of LTE for PPDR, so this present inability must be based on commercial argument. An obvious solution would be special SIM cards for emergency responders enabling access with the highest priority to any MNO network on detection of a threshold level of signal strength.

Liability will be based on conventional government procedures: liability for failure of the commercial networks used for PPDR purposes under contract is in the end the responsibility of government (by signing MNO contracts) and exercised through the contract conditions. Although details of the SLAs are still confidential, it is possible that these conditions include "step-in" clauses for failure, so the government can step in and take direct control of MNO operations, with periods during which appropriate penalties must be paid by the MNOs

The question of whether the Home Office is liable in case of loss of life due to negligence, either by its own actions or by that of the contracted MNOs, is to some extent covered by the position of governments generally, in acting as the final point of liability. Hence this is not considered an abnormal liability risk, as traditionally the government takes liability directly, effectively acting as its own insurer. Certainly the Home Office expects that the commercial MNO contracts will contain suitable safeguards in their SLAs to ensure that failure due to negligence is unlikely. But it is unclear how certain this can be made – and a suitable response to this issue may be one of the tendering conditions. In practice, the UK government will take a case by case approach to liability and possible failings by the MNOs that lead to avoidable death or injury.

5.1.6 Future directions

ESMCP contracts will be relet in 2021. By then, the 3GPP forum should have delivered fully functional, mission-critical LTE Advanced standards for use in the new contracts, with time for pilot testing.

5.1.7 Key lessons for this study

- It may be possible to provide a commercial basis for PPDR, but only if a *legal framework* which constrains the MNOs to fulfill their SLAs is imposed with strict compliance. The SLA is the key to the viability of this option. Moreover, the MNOs have to be in agreement with this, meaning they must see a profitable outcome under the requirements.

- The structure of this contract-letting framework, in four lots ranging from programme management to sale of mobile broadband megabytes, with systems integration, distribution of handsets and apps stores, is an example for other Member States.

- With mission critical and business critical contracts tied, the impact on the retail mobile market will be far greater, giving MNOs strong incentives to co-operate.

5.2 Case Study: FirstNet

FirstNet is the informal name of the Nationwide Public Safety Broadband Network, which is expected to provide the USA with the kind of shared infrastructure and interoperability among public safety agencies which Europe has been developing since the Schengen Agreement.

The need for a comprehensive public safety network in the US was brought out by the terrorist attacks of 11 September 2001 and the communication problems that plagued the first responders dealing with that emergency. FirstNet will use some of the 700 MHz frequencies freed by television's switch from analogue to digital. However, it will not immediately replace the patchwork of local-area radio networks used across the US. Instead FirstNet will provide secure broadband alongside the existing networks. Mission critical voice will come later, when the users decide that LTE's implementation is mature and reliable enough.

FirstNet is still in the preliminary planning stage, without an agreed business model, technical design or deployment schedule, although its administrative structure, partnership principles and basic technical requirements have been outlined. It is governed by the First Responder Network Authority, an "independent entity" within the US Commerce Department's National Telecommunications and Information Administration (NTIA). The radio access network will be based on LTE standards but with a hardened infrastructure. Many other countries are likely to take advantage of the availability of 700 MHz equipment developed for the US market, though it is not clear if FirstNet as a model will be replicated elsewhere – or if it will work as intended in the US.

5.2.1 Background

In 2006 the US Federal Communications Commission (FCC) proposed that some "digital dividend" spectrum might be used by public safety agencies and commercial mobile networks on a shared basis. The following year they decided to implement a 700 MHz Public/Private Partnership if a certain minimum bid was reached in the license auction for 758–763 MHz and 788–793 MHz. However, that minimum bid was not reached, apparently because of conditions attached to the license, which included the winning bidder funding a nationwide broadband network for public safety use and allowing public safety users to preempt commercial use of the auctioned frequencies during emergencies.[78]

After much debate about other options, FirstNet was authorised in 2012, with $7 billion from future spectrum auctions earmarked for research and development, a governance structure to oversee the network and the build-out itself. The network will be for federal, state and local public safety agencies, utility and public transportation companies and others responsible for critical infrastructures. Since that user base is about 5.4 million individuals, about 1.8 million of them might become FirstNet subscribers, if Europe's experience with TETRA is any guide (see Section 2.3.1).

An Interoperability Board was formed to develop minimum technical requirements for FirstNet. The board recommended the use of commercial LTE standards, including Voice over LTE when that stabilises, as well as IPv4/v6 and specific encryption algorithms. It also identified a few areas where it might be necessary to supplement or override the LTE standards, e.g. changing an application's priority in life-threatening circumstances, the handling of overlapping jurisdictional priorities, etc.[79]

FirstNet signed spectrum lease agreements with four public safety communications projects to serve as testbeds for various aspects of the new network. (Negotiations are still underway with a fifth.) The New Jersey project, for example, is a procurement pilot for transportable base stations. The project in Los Angeles will establish principles for prioritising bandwidth use among agencies with different functions. The testbeds were chosen from among projects that won federal grants to develop public safety LTE networks.

NTIA's First Responder Network Authority is overseen by a 15 member board which holds the renewable 10-year license to 20 MHz of public safety broadband spectrum (758–768 MHz and 788–798 MHz). The board consists of the Secretary of Homeland Security, the US Attorney General, the Director of the Office of Management and Budget, and 12 individuals appointed by the Secretary of Commerce. A 40-member Public Safety Advisory Committee provides advice and subject matter expertise. Representatives of professional organisations and official entities serve on the PSAC along with front-line (non-management) first responders. A National Council of Statewide Interoperability Coordinators mediates FirstNet's "state outreach" efforts, and each state has an Interoperability

[78] Nilsson, K. R. (2008) "Report: D Block Investigation", Office of Inspector General, US Federal Communications Commission, 25 April, http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-281791A1.pdf
[79] Technical Advisory Board for First Responder Interoperability (2012) "Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network: Final Report", 22 May, http://apps.fcc.gov/ecfs/document/view?id=7021919873

Governance Body to coordinate state involvement in FirstNet. FirstNet headquarters in Reston, Virginia, has a relatively small staff with familiar titles like general manager, chief counsel, etc., but the "technical headquarters" is in Boulder, Colorado, 3000 km away.

Two years into the project, the overall dimensions and cost of FirstNet are still uncertain. The $7 billion commitment from Congress was "seed money": the network's total cost is "estimated by experts to be in the tens of billions of dollars over the long term, with similarly large sums needed for maintenance and operation."[80]

Since the spectrum auctions supplying FirstNet with startup funds have not happened yet, FirstNet has borrowed about $2 billion from the US Treasury. Meanwhile NTIA has given out $116 million in State and Local Implementation Planning Grants to fund regional workshops and individual consultation visits by FirstNet representatives to each state and territory. After each visit, Statewide Communication Interoperability Plans will be developed, integrating national level information with local conditions, existing systems and resources. The state-level plans will influence FirstNet's design and help determine the nature and extent of each state's involvement. Governors have 90 days to review the plan for their state, consult with their public safety advisors, and decide whether to participate. States can choose not to join FirstNet but they will still have to interoperate with it – that is, they must start using LTE for public safety and support interstate roaming on whatever network they build. States that opt out have 180 days to submit an alternative plan to the FCC and NTIA. They can apply for federal subsidies but will be expected to pay at least 20% of their network costs.

The possibility of states getting broadband coverage from other suppliers was seen as a way to impose economic discipline on FirstNet and prevent the negative aspects of a nationwide monopoly. However, uncertainty about the total number of users and the local resources available makes it difficult for FirstNet to develop network deployment and business plans. Instead they must consider a range of options – for example, from 14,000 to 35,000 base stations nationwide. Uncertainty about what they will be able to offer and at what price has undermined partner signups and encouraged a proliferation of alternative proposals. Opinions are divided about how bad the situation is, but the telecommunication expert who monitors FirstNet's progress for the US Congress said last March that "we are on the verge of a serious crisis of confidence re FirstNet".[81] A few weeks later the general manager resigned[82] and a permanent successor is still being sought 6 months later.[83]

The latest information available suggests that FirstNet will not have a clear sense of what it will cost to join their network, or what the coverage offers and build-out schedule will be, until the middle of 2015.[84] That means state participation decisions will be made early in 2016.

[80] Moore, L. K. (2014) "The First Responder Network (FirstNet) and Next-Generation Communications for Public Safety: Issues for Congress", US Congressional Research Service, http://fas.org/sgp/crs/homesec/R42543.pdf

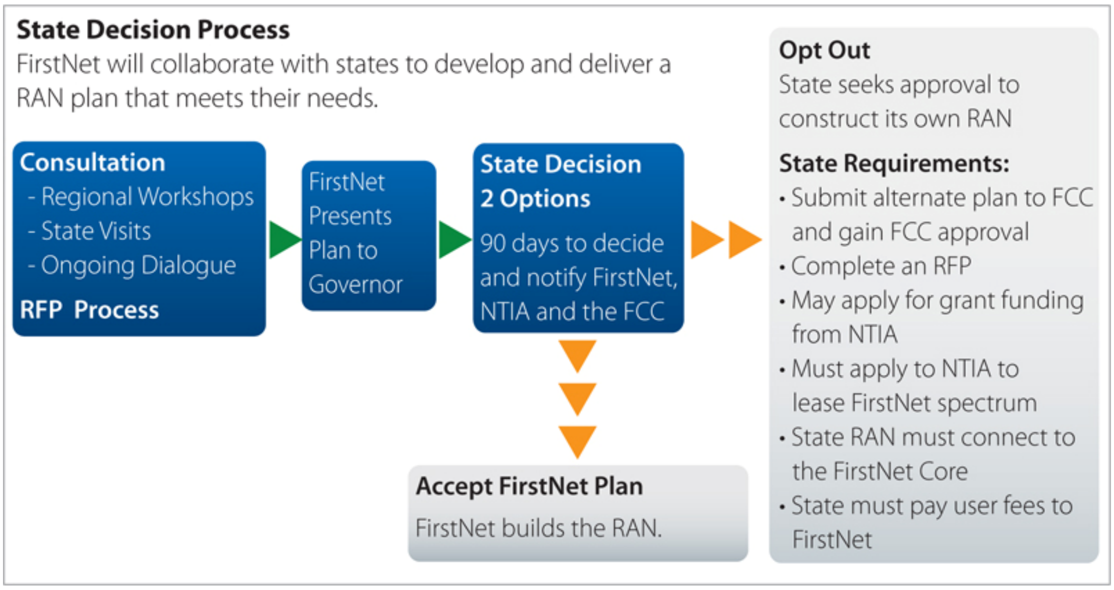
[81] Email from Linda K. Moore to RCC Consultants, March 2014, http://rcc.typepad.com/blog/2014/03/broadband-conversations-17-a-federal-government-analyst-says-we-are-on-the-verge-of-a-serious-crisis.html

[82] Baschuk, B. (2014) "D'Agostino FirstNet Board Resignation Signals Turbulence Amid Ethics Investigation", Bloomberg News Agency, 16 April, http://www.bna.com/dagostino-firstnet-board-n17179889629/

[83] "Q&A with FirstNet's Acting General Manager", *Mission Critical Communications,* 7 October, 2014 http://www.rrmediagroup.com/onlyonline.cfm?OnlyOnlineID=483

[84] Nolin, J. (2014) "Clearer timeline for FirstNet not expected until at least '15", *Urgent Communications,* 24 July, http://urgentcomm.com/public-safety-broadbandfirstnet/clearer-timeline-firstnet-not-expected-until-least-15

Figure 5.1. How each US state decides whether to join FirstNet



Source: Wood, 2014

5.2.2 Major features

Apart from user fees, income is supposed to come to FirstNet from the private sector under rules drafted by Congress for the creation of public-private partnerships. Incentives for private partners include gaining rights to operate, use and service parts of the network. The leasing of radio frequencies to third parties when public safety does not need them is seen as another important source of income. Many partnerships are expected to be based on contributions of access to existing facilities. According to FirstNet's first general manager, Bill D'Agostino, "we'll look to co-locate on existing facilities first. We'll look at assets public safety agencies already have. We'll also look at assets that state governments and the federal government have… Only as a last resort will we look to build a new tower…"[85]

Even though FirstNet intends to exploit existing networks as much as possible, public safety and commercial, "it won't be a carrier wireless network," D'Agostino contends. "The core, for example, has to be highly secure to provide much of our cybersecurity… The hardening of the core and the core's security layers will be fundamentally different from a carrier network".

Another key difference is in FirstNet's handling of video: "Video is going to place a huge demand on the network bandwidth. That's where local control comes in, and that's another distinction between the wireless carrier networks and FirstNet's network. Local public safety agencies will have control of FirstNet users. [They will] decide who gets video, when they get it, and what type of delay may be necessary. That's how we intend to manage bandwidth demand".

Other departures from carrier network norms include taller antenna masts in rural areas to increase signal range, more use of repeaters and tower-top amplification, and much more use of transportable base stations. There will also be "a lot of redundancy built into the network with multiple layers of backhaul, satellite backup also seems likely, and battery backup for the ability to keep the network's

[85] Biby, R. (2014) "FirstNet's First Steps", *Above Ground Level Magazine,* February issue, page 17-26, http://online.qmags.com/AGL0214

terrestrial sites on the air... and potentially the ability to fall back onto carrier networks for roaming", D'Agostino adds.

If FirstNet will use existing networks and roaming, how much of the network will actually be supplied by commercial carriers? "I'm not sure carriers will ever give public safety communications preemption rights and the ability to preempt their customer base during emergencies. That's why it's fundamentally important that we build the FirstNet network", D'Agostino concludes, instead of simply buying service from carriers.

5.2.3 Key lessons for this study

An analysis of FirstNet by the US National Institute of Standards and Technology concluded that 38,000 base stations are needed to cover 95% of the US population with LTE broadband at 750 MHz.[86] The use of higher power handsets, as permitted for first responders, reduces the number of base stations needed to 34,000. Previous revenue projections suggested that a network with more than 35,000 base stations will not be financially self-sustaining. So the business model assumed by Congress might work, though compromises would increase the chances of success while reducing network capabilities. NIST says giving up the requirement for indoor signal coverage will reduce the number of base stations needed by about 14%. Reducing the population coverage goal from 95% to 85% lowers the site count by just over 28%. That latter calculation may be why FirstNet's general manager thought transportable base stations such a good solution. US population density is much lower than Europe's, but transportable LTE base stations might be a solution for Europe's less populous regions, too.

5.3 Case Study: ASTRID's Blue Light Mobile

Belgium's nationwide network for first responders is called ASTRID (All-round Semi-cellular Trunked Radio with Integrated Dispatching). *Mobilecomms-Technology.com* says it was "the world's first nationwide TETRA network with IP capability" for public safety and security agencies.[87] The Nokia-built ASTRID network in Belgium is also the world's only system in which radio, paging, telephone via computer aided dispatch (CAD) are fully integrated in a single environment.

ASTRID is a government owned corporation founded in 1998. Five hundred base stations and 11 CAD control rooms were deployed between 2000 and 2003 to support 40,000 subscribers. (Today there are 56,000 subscribers). They also operate a nationwide POCSAG network with 220 antennas on the TETRA towers for calling out more than 12,000 volunteer firefighters with pocket pagers.

When TETRA TEDS entered the market in 2008-9, ASTRID's managers considered upgrading. But they found it would cost 40-45% as much as the original network and the speed gains for data were small. So they started thinking about other ways to develop broadband. From the start they were interested in working with Belgium's cellular network operators because the cost of building a new dedicated PPDR network would have been prohibitive. More importantly, the commercial networks have better geographic coverage and better indoor reach, according to Jo Dewaele, who has been with ASTRID since the start. The other reality was very little actual use of broadband by Belgium's PPDR

---

[86] Golmie, N. et al. (2014) "Modeling and Performance Analysis of a Public Safety Broadband Network", NIST, presented at the Public Safety Stakeholders' Conference, 3-5 June, http://www.pscr.gov/projects/broadband/700mhz_demo_net/meetings/stakeholder_mtg_062014/slides/day_1/Nada_Golmie_Richard_Rouil_PSBB_Stakeholder_June2014_modeling.pdf
[87] "ASTRID TETRA Network, Belgium", http://www.mobilecomms-technology.com/projects/astrid/

community despite their interest in having the capacity. (Apparently that is still the case.) So ASTRID had to find a solution involving minimal investment in equipment.

They came to the idea of a collective "wholesale roaming" subscription on existing commercial cellular networks. Special 3G SIM cards give ASTRID subscribers the status of international roamers on Belgium's three commercial cellular networks (Proximus, Mobistar and Base) and eleven networks in four neighbouring countries (Netherlands, Germany, Luxembourg and France), but with higher priority than public subscribers. As international roamers, if the signal from one network is lost, the portable device is automatically switched to another with a roaming agreement with "Blue Light Mobile," ASTRID's virtual broadband network. Having access to multiple networks provides better coverage than any single network offers.

Officially launched on 29 April 2014, Blue Light Mobile's role is to mediate between public safety organisations and the commercial carriers, standardising and simplifying the acquisition of service and providing a "one stop shop" for subscribing, user authentication, customer care and problem resolution. The ASTRID Service Centre provides round-the-clock support 7 days/week as well as "additional guarantees with regard to the network's data security".[88] (The Blue Light SIM card is configured to provide end-to-end encryption for data sessions into the "private cloud" maintained by ASTRID for individual security services and shared applications.) Creating a special brand also holds users who might have tried to make individual arrangements with specific carriers.

"We are the first in the world to use this formula," says Christian Mouraux, project leader for Blue Light Mobile. "Already quite a few experts from abroad have been contacting us with an interest in creating a similar service".[89] In spring 2014, Sweden's RAKEL network tested EADS' Tactilon software to manage secure broadband access for mobile subscribers via commercial cellular networks.[90] Germany has had roaming deals for its first responders while the BDBOS network is being built and Estonia plans to develop an MVNO to provide broadband and VoIP for its security services starting next year.[91]

Blue Light Mobile was tested by 10 Belgian police and fire services before it "went live". One of the test zones was on the Netherlands border, to see if cross-border interference or "inadvertant roaming" would be problems. They were not, and the field testers reported that Blue Light's data communication was faster than their fixed line computer in the station. Another test involved searching police databanks and sending images from automatic number plate recognition cameras during a football match with a risk of misbehaviour by fans. There were no problems, either with the fans or the data transmissions (MVNO Dynamics, 2014).

---

[88] "Belgium Operator, Astrid, adds 3G MVNO for public services", *MVNO Dynamics,* 30 April 2014, http://www.mvnodynamics.com/2014/04/30/belgium-operator-astrid-adds-3g-mvno-public-services/

[89] "ASTRID launches Blue Light Mobile, an innovative broadband data service", ASTRID press release, 29 April 2014, http://www.astrid.be/templates/content.aspx?id=168&LangType=1033

[90] "Sweden Selects Airbus (Cassidian) for Rakel Data Services Pilot", *Radio Resource Magazine,* 21 January 2014, http://mccmag.com/newsArticle.cfm?news_id=10372

[91] This project is listed in the RIKS Development Plan (2014-2018), http://www.riks.ee/docs/DEVELOPMENT_PLAN_2014_2018.pdf

In the spring of 2012 ASTRID published a tender which split the Blue Light project into three components. Prospective bidders could decide if they wanted to pursue one, two or all three:

1. Supplying and managing the SIM cards;
2. Responsibility for the roaming hub and integration with ASTRID's other services; or
3. Supplying equipment for ASTRID's management of the service (VPN, servers, etc.).

Three partners were chosen in May 2013, each for a different component: Halys supplies and manages the SIM cards, Belgacom is responsible for the roaming hub and Astrium supplies equipment for managing Blue Light.

Subscription prices and package deals are described on the website (http://www.bluelightmobile.be). TETRA IP subscribers get a free SIM card and up to 500 MB of free data per card per month. Activating additional SIM cards costs €10 each plus €20.75/month for groups with TETRA IP subscriptions, the amount of free data varying with the number of SIM cards in the group. For new subscribers, the SIM card costs €10 plus €20.75/month for 500 MB of data. Going over the data limit incurs additional fees as does making too many long distance voice calls. (ASTRID is not trying to profit from the service – they just want to break even.) Utilities are able to sign up for Blue Light Mobile, as they can for ASTRID's TETRA and paging services.

Apparently this solution is working well for the number of users who have signed up so far. But providing support to thousands of users could bring new challenges. It is also not clear yet if the user base and running costs will reach the levels assumed in the business plan, for the service to become self-supporting but revenue neutral.

Blue Light Mobile is considered a temporary solution to the problem of supplying PPDR users with mobile broadband. However, "temporary" could mean 5-10 years.

5.3.1 Key lessons for this study

- Thoughtful/careful project design can make the MVNO approach succeed, even if scaling up to full size is a challenge.
- Branding can add as much value to a specialised network as to a public network.
- The assumption that PPDR networks have better coverage than commercial cellular networks is not always true, especially if one has access to all the commercial networks

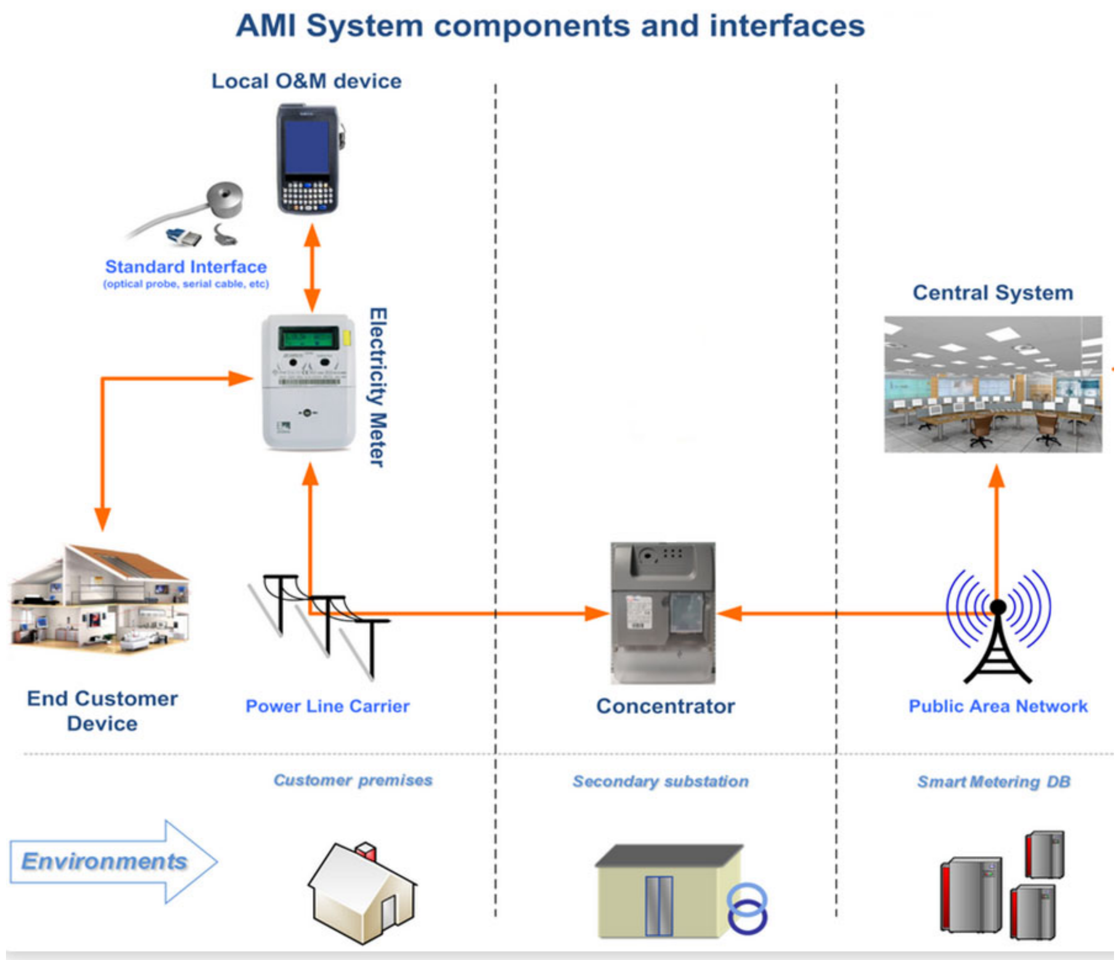
5.4 Case Study: ENEL

Unlike police forces and traffic management agencies, utilities are businesses so they can have relationships with MNOs that go beyond provider and customer. Consider ENEL (Ente Nazionale per l'Energia Elettrica), Italy's former state electricity agency.

ENEL is Europe's second largest utility with electricity, gas and solar energy operations in 40 countries on four continents. In Europe it has investments, partnerships and subsidiaries in France, Greece, Portugal, Romania, Russia, Slovakia and Spain.

It is only a slight exaggeration to say that ENEL invented the smart meter. They were the first to design and provide all-electronic electricity meters for their customers and Italy was the first country in the world to reach full deployment of these meters (almost 31 million by 2006). Motivated not just by a need for greater business efficiency but by a bold vision of their future after privatisation as a "meta-utility", ENEL saw the smart meter as a gateway between "upstream services", which they would co-ordinate, and buildings full of smart devices needing integration and remote management. To prepare for that future they co-founded one of Europe's first converged telecom companies. Wind Telecomunicazione offered the public fixed and mobile telephony and internet access using ENEL's optical fibre backbone. This subsidiary would also support the smart meter network with GPRS for data relay, GSM for the installation crews, and home internet access via PLC if that proved technically possible. But when its ambitious CEO was forced to leave, ENEL changed strategy and in 2005 they sold their telecommunication division to re-focus on being an energy company. ENEL is still a market leader, but now oriented toward renewable "green power".

Figure 5.2. ENEL's Automatic Metering Infrastructure



Source: Meters and More

5.4.1 Background

ENEL was created in 1962 by nationalising over 1200 local companies to form Italy's National Agency for Electrical Energy. In 1991 ENEL started developing the first system for remote meter reading using Powerline Communication (PLC). The first prototype was working by 1993. Their aims then were practical: to reduce operating costs and losses due to electricity theft while improving customer service. By 1998, Project SITRED had deployed 80,000 electromechanical meters to log power consumption and transmit the data back to headquarters in short bursts. But the cost per meter was unacceptably high.

Successive Italian governments had made the privatisation of ENEL a priority but were unable to complete the task due to the lack of consensus on a regulatory framework and a structure for the market. A law creating an independent regulator for the energy sector was adopted in November 1995. Then in 1996 an EU directive was agreed by energy Ministers setting minimum requirements for opening Europe's electricity markets to competition.

So in 1996 ENEL got a new Chief Executive Officer, Francesco Tatò, to prepare the state company for competition after loss of its protected status. One of Tatò's first decisions was to co-found, with Deutsche Telekom and France Telecom, a "converged carrier" to offer the public fixed and mobile telephone service and internet access: Wind Telecomunicazione. In 2000, using €11 billion it received from the sale of assets to create competition in the electricity market, ENEL bought Italy's second largest fixed telephone network, Infostrada, from Vodafone to merge it with Wind.[92] It then bought out its partners' shares in Wind to acquire full ownership of the combined enterprise.

Italy's utility regulator (Autorità per l'energia elettrica e il gas, AEEG) quickly launched an investigation into the impact ENEL's acquisitions might have on competition, arguing that the mergers

> strengthen its dominant position in the market for the supply of electricity. Enel, by jointly offering utilities and telecommunications services, and in particular using strategies such as joint billing and joint promotion of the bundled services, would be able to 'lock in' its current electricity customers, reducing substantially the impact of the liberalisation on the Italian electricity markets…[93]

But in June 2003 AEEG decided there would be no negative impact so they approved the deal, as did Italy's competition authority and DG Competition.[94]

In 1999 Italy transposed EU Directive 96/92/EC to open their electricity sector to competition and ENEL became a group of companies, with ENEL Distribuzione in charge of electricity distribution and thus metering. By this time they had embarked on a new project – Telegestore ("remote manager") – to create an Automated Metering Infrastructure for all ENEL customers. The main difference from SITRED was the scale of the project. Telegestore meters were also more advanced – electronic digital rather than electromechanical – and designed for two-way communication (though not in real-time). Prototypes and pre-production models were created in 2000 and 2001. Deployment plans were formulated and in 2002 began in earnest with the installation of 700 000 meters per month. Deployment was virtually complete by 2006 when the regulator stepped in to require all of Italy's electricity distributors to deploy smart meters with a minimum degree of functionality and to ensure they were all interoperable. In other words, ENEL's meters were not deployed to meet a regulatory obligation. The obligation came after the job was finished, to create a level playing field among electricity distributors and to ensure that customers could switch utilities without having to change meters.

> [M]any in the industry anticipated that the electricity meter could be transformed into a 'residential gateway', connecting, through power lines, the electricity provider upstream with any intelligent device downstream, including other meters, local plants, even home appliances. Some hoped that this

---

[92] ING Barings (2001) "Company Update: ENEL", 8 January, http://www.borsaitaliana.it/bitApp/view.bit?lang=it&target=StudiDownloadFree&filename,pdf/3009.pdf

[93] AEEG referred the case to Italy's telecom authority, AGCOM, which consulted DG Competition. This quote is the EC's summary of the AGCOM's case in their press release IP/01/79 (19 January 2001) - http://europa.eu/rapid/press-release_IP-01-79_en.htm

[94] Case COMP/M.2216 (Merger ENEL, Wind, Infostrada, 2001), http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=2_M_2216 L'Autorità Garante della Concorrenza e del Mercato (2003) "C5846 - Enel/Wind Telecomunicazioni", Provvedimento n. 12095, http://www.agcm.it/concorrenza/concentrazioni/download/41256297003874BD/F79B04A2FE0221ACDC1256D56004CB17F.html?a=p12095.pdf

> innovation would leverage the launch of a radical change in the provision of user services through powerline communication, and, in particular, that it would finally launch the long anticipated and much coveted home automation market… (Rossi *et al.,* 2008)

In Wind Telecomunicazione Tatò saw synergies and cost savings for ENEL, especially in the Telegestore project. Wind began offering GPRS to customers in 2001. While PLC was used to connect the Telegestore meters to the nearest low-voltage substation, the data concentrator at each substation was connected to ENEL's communication centre using GPRS whenever possible.[95] Wind also provided ENEL's field crews and meter installers with mobile voice communication. In 2002 Wind had over 7,600 GSM base stations covering 98.2% of Italy's population.[96] Their 2006 financial report indicates that ENEL paid them €90 million for GPRS and other mobile communication services in 2005.[97]

5.4.2 Business aspects

With Tatò's departure in 2002, ENEL's direction changed back towards being a more conventional utility.[98] By owning Wind, ENEL was able save the money it would have spent on GSM/GPRS while ensuring reliable access to those services. Unfortunately, their savings on services were dwarfed by the losses incurred by Wind from the public side of their business: €1.4 billion in 2002 alone. These losses were caused mainly by the need to buy a 3G license and to expand and upgrade their mobile and fixed networks to compete with larger rivals. So in 2005, ENEL traded its Wind ownership for just over €3 billion in cash plus a share of the company that owned Orascom Telecom, a transaction which enabled ENEL to offload €7 billion in Wind debt.[99] In 2011, Wind became part of the Vimpelcom group.

By 2006 ENEL had already redistributed its GPRS contracts more evenly, using all suppliers in the Italian market: TIM, Vodafone and Wind.[100] Today ENEL has a marketing partnership with Vodafone: the two companies offer discounts to customers who buy bundled services from them – apparently without the regulator objecting.[101]

The Telegestore network cost €2.1 billion to deploy and €67.3 million per year to operate, paid for by revenue from customer billings. The meters are the most expensive element, amounting to 66% of total cost (€63-80 per site, depending on the model). Data concentrators amount to 7% of the total cost (€5-9, depending on the number of meters per concentrator, including switches, modems, external antennas and protective boxes for outdoor installation). Installation added about 20% to the cost, and 7% went for the telecom infrastructure, software licenses, system integration and human resources. The average total data transmission time per meter per year is about 6 minutes (Zito, 2010). Once in place the investment enabled ENEL Distribuzione to reduce its operating costs from €80 per customer in 2001 to €52 per customer in 2013.

---

[95] CapGemini (2007) "Comparatif international des projets de compteurs évolués sur les marchés électriques de sept États; Annexes – Fiches Pays", pour le Commission de Régulation de l'Énergie, http://www.cre.fr/documents/deliberations/communication/evolution-du-comptage-electrique-basse-tension-de-faible-puissance/consulter-l-annexe-1-comparatif-international

[96] ENEL (2003) "Relazione Semestrale 30 Giugno 2003", http://www.grupposnai.it/sites/grupposnai.it/files/30.06.2003_relazione_semestrale_snai_s.p.a_2003_primo_semestre_-_file_pdf

[97] Wind (007) "Growth and De-leveraging – Delivered: 2006 Results", page 22, https://www.windgroup.it/fileadmin/reports/results_presentations/2007/en/Wind_FY2006_results.PDF

[98] Turani, G. (2002) "Kaiser Franz, manager di ferro che piaceva tanto a Berlusconi", *La Repubblica,* 14 May, http://www.repubblica.it/online/lf_dietro_il_listino/020514tato/tato/tato.html

[99] Southwood, R. (2005) "Egyptian Businessman Buys Italy's ENEL Telecom Unit", *Balancing Act Africa,* no. 259, http://www.balancingact-africa.com/news/en/issue-no-259/money/egyptian-businessman/en

[100] Gallo, L. (2006) "Enel, la svolta Telegestore", 27 March, *Corriere delle Comunicazioni,* http://www.corrierecomunicazioni.it/archivio-giornale/2006/19/Corcom_24.pdf

[101] https://www.enelenergia.it/mercato/libero/it-IT/sconti_e_premi/promozioni/vodafone

Today 34 million Telegestore meters communicate with more than 350,000 data concentrators using the PLC protocol developed for Project SITRED. In 2009 ENEL decided to open the SITRED protocol, which had been proprietary, hoping to make it the de facto global standard for smart meters. It is now called “Meters and More”.[102] While the concentrators can send information and instructions to individual meters, real-time control is not possible with today’s meters. (Real-time communication is a significant energy drain as the meters must remain receptive all the time.) However, a new generation of meters will be introduced soon. These will be designed with electric vehicle charging, solar power and smart grid support in mind, though their total range of capabilities is not yet known.

5.4.3 Key lessons for this study

The smart meter as a gateway between upstream services and home networks, automated appliances and personal devices still seems a credible vision. It could even be enhanced by future developments. Indeed, it not so different from the cellular industry’s vision of 4G, where operator billing systems serve not just mobile telephony but broadband, mobile broadcasting, hotspots, mobile banking, apps and cloud services. But where MNOs rely on cellular radio, electric utilities rely on PLC, a technology with more limited development potential. In both cases, though, converged businesses raise challenging questions about the possible re-emergence of monopolies after a few brief decades of progress through competition.

5.5 Case study: Duke Energy

5.5.1 Background

With gross revenues of over $24 billion in 2013, Duke Energy is the largest electric power holding company in the USA. The parallels – and contrasts – with ENEL are striking: where ENEL is known for its commitment to renewable “green energy”, Duke is known for its nuclear and coal-fired plants – it is the second largest emitter of greenhouse gases in the US.[103] And where ENEL thought that owning a telecommunications network and a proprietary automation control platform would give it early advantages in serving “networked homes” – but then they changed direction – Duke is taking an opposite approach, playing the “long game”, content to be a mobile cellular customer while developing open source “smart nodes” that could eventually support smart city functions: “Duke Energy has no desire to be in the communications business,” explains David Masters, Duke’s former manager of technology development.[104] “We need to harness already existing expertise and capabilities that the cellular networks provide in designing, building, and maintaining the communications” while focusing on electricity generation, low cost distributed data processing platforms and open-source apps to regulate distribution.

Yet there are similarities, too. What ENEL describes as a “data concentrator” at neighbourhood substations, Duke calls a “communications node”. The difference between a concentrator and a node is the amount of intelligence, software and connectivity options embedded in the device, which reflects the greater capabilities per unit cost of today’s digital devices. “Think of the communications node as an iPhone for the modern grid,” Masters says. “It is a device with the future communications capability for multiple networks, with capability to route the data between multiple devices and with

[102] Bigliani, R. (2009) “Enel Makes its Smart Meters ‘Open Source’”, *IDC Community,* https://idc-community.com/energy/smart-grid/enel-makes-its-smart-meters-open-source http://www.metersandmore.com/
[103] Political Economy Research Institute (2013) “Greenhouse 100 names top climate polluters”, University of Massachusetts at Amherst press release, 5 June, http://www.peri.umass.edu/greenhouserelease/
[104] Masters, D. (2011) “Duke Energy: Developing the communications platform to enable a more intelligent electric grid”, https://www.duke-energy.com/pdfs/OP-David-Masters-SmartGrid-Comm-Platform-02-01-11.pdf

enough storage and processing power to enable an extensible ecosystem of data applications which are anticipated to be built over a number of years" (Masters, 2011).

Thus, even now, but more so in the future, the communications node's role is not so much to concentrate metering data for delivery to headquarters, it is to identify exceptions to normal data patterns and assess or report those exceptions. Increasingly, it will be able to initiate responses without an order from headquarters. Moving processing power to the network edge and utilising exception based reporting enables Duke to reduce the costs of data communication and storage by up to 90% while also reducing problem response times from minutes to seconds. For Duke, the substation node is the gateway to the future, not the electricity meter.

5.5.2 Major features and technical architecture

Given their environmental record, Duke Energy is not the kind of company one would expect to join the open-source/open-hardware movement – or to urge their suppliers and cohorts to join, too. But they are:

> "Here's a breakdown of what could be one of the most important concepts in distributed grid operations and data analytics out there… a $35 piece of off-the-shelf computing hardware… beloved by hackathon participants and middle-school programming instructors everywhere: the Raspberry Pi. Adding this credit-card-sized circuit board to its grid nodes allowed Duke to manage some of the more complex computing tasks it was seeking to accomplish out at the edges of the network…"[105]

Raspberry Pi and the philosophy behind it seem to have inspired Duke to initiate "a potentially revolutionary project: getting some of the world's biggest smart grid technology vendors to open up their systems… to connect smart meters, solar inverters, battery controllers, distribution grid control systems and network nodes, all with open-source adapters that render them capable of 'talking' to one another." (St. John, 2013)

This group is known informally as "The Coalition of the Willing" and they have started working their way through a long list of projects which involves taking standard power grid management tools and creating compact, open-source work-alikes that can run on Raspberry Pi's Linux operating system, and device interfaces enabling diverse equipment from different vendors to communicate. They are starting to present their work to standards organisations like CENELEC and OASIS in hopes of establishing their outputs as industry-wide solutions. (Some have also joined Meters and More, the group ENEL founded to promote their PLC protocol.) A nontechnical description of the open source smart grid project can be found in St. John (2014) and a short presentation of the philosophy behind it (in the form of a manifesto) in Smith (2014).

From Masters' comments about preferring to buy service from cellular networks rather than having power companies go into the communications business one might think this project could be a source of new utility spending on LTE. But a deeper look makes it seem quite the opposite. Since the main thrust of the project is decentralising grid management and building up local processing, data flow over long paths to the home office is being cut by up to 90%, and replaced by short point-to-point hops and mesh links using PLC and license exempt spectrum. Raiford Smith, Duke's director of smart grid emerging technology, gives the example of "a single substation with 30 voltage regulators, each connected to Duke's SCADA system via cellular modems, at a total cost of $36,000. 'What we did instead is put a Wi-Fi modem in each of those, and one communications node' to connect them, at a

---

[105] St. John, J. (2013) "Duke Energy: From Smart Grid Devices to Grid Computing Platform", *Green Tech Media,* 2 October, http://www.greentechmedia.com/articles/read/duke-energy-from-smart-grid-devices-to-grid-computing-platform

total cost of $2,500, he said… ‘with that, I’ve got an aggregation point for the data [which can put a] view of all 30 voltage regulators into a single set of data points for reduced network traffic and integration complexity… detecting outages ‘faster, more efficiently, and at lower cost’…” (St. John, 2013)

5.5.3 Future directions

Behind this project is the growing realisation that society’s need for continuous delivery of electric power is the result of our limited ability to store large amounts of electricity. Should that change – and the development of electric vehicles, battery-powered portables and renewable energy has intensified research into electricity storage to the point where some progress might eventually occur – then the need for constant real-time electricity delivery could diminish. In the same way that everyone’s ability to record video and play it back on demand reduces the dependence on broadcasting, if generating and storing electricity at the network edge advances, companies like Duke and ENEL could eventually find reduced reliance on their services. So Duke is committed to minimising the cost of management of its supply network as quickly as possible, using open source software and very low cost neighbourhood-level processors.

5.5.4 Key lessons for this study

Commercial mobile networks support work outside the office for utility employees with portable devices. In some cases GPRS connectivity between substations and utility headquarters is supplied for remote meter reading data. The first niche seems moderately secure but the second, despite the current deployment of smart meters on a massive scale in Europe, could eventually be undermined by the decentralisation of electricity generation and grid management.

Both ENEL and Duke use GPRS to connect the nodes or concentrators to the back office. Data from the meter normally gets to the node via PLC, though in Duke’s case there are other options as well: the license exempt 920 MHz ISM band is widely used in the US to transmit metering data over short range radio links. More generally, the technical management at Duke is clear that utilities need diverse wired and wireless media to fulfill different requirements and the relevant technology options evolve faster than traditional utility assets. Thus it may make more sense to use a service provided by a third party rather than buy, or build and own, several wireless networks for decades.

5.6 Case study: ITS Spot

Appendix C.1 reports that “timetables for the roll-out of next-generation ITS technologies, and especially Cooperative ITS (C-ITS) systems, now look hopelessly optimistic” (Jandrisits, 2013). But one place where roll-out is racing ahead is Japan. They have been developing roadway ITS and now cooperative ITS for almost 20 years, establishing the country as the clear world leader.

5.6.1 Background

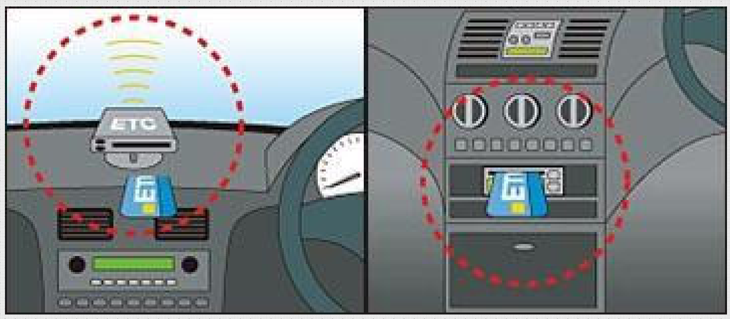
A Vehicle Information Communication System (VICS) started operating in 1996, providing real time traffic alerts and updates to Japanese drivers in the form of maps, short texts and simple graphics for display on the screen of their car’s onboard navigation system. From the start information was delivered through 3 different channels:

- subcarriers on NHK’s FM broadcast signals (range 10-50 km, bandwidth 16 kbps),
- 2.5 GHz beacons (mainly on expressways; range 70 m, bandwidth 64 kbps) and

- infrared beacons (on ordinary roads; range 3.5 m, bandwidth 1 Mbps).

VICS shows the locations of parking lots, road works and accidents, congestion reports, travel restrictions (road closures, temporary speed limits) and data for re-calculating the best routes and time to destination. Twenty million onboard VICS units were deployed in Japan by 2007.[106]

Figure 5.3. Japan's onboard ETC device, an add-on or integrated with the vehicle



Source: ITS Technology Enhancement Association, Japan

VICS was joined in 2001 by Electronic Toll Collection (ETC). Dashboard devices combining a 5.8 GHz radio transceiver and ETC payment card reader are now found in nearly 90% of the cars using Japan's toll roads. Payment cards are issued by companies with contracts with the toll road operators. They can be either ETC only, or a credit card with ETC account support. ETC enables vehicles to drive through toll plazas without stopping – though they must slow down – and payments are deducted automatically from the cardholder's account.

VICS began transmitting at 5.8 GHz, too, making it possible to integrate the service with ETC in one device. At that point the combined VICS/ETC onboard unit became a platform for launching additional services.

5.6.2 Major features and technical architecture

ITS Spot was developed in 2009, combining VICS and ETC and adding new safety enhancement features. This became the world's first nationwide vehicle/infrastructure ITS system when the Ministry of Land, Infrastructure, Transport and Tourism began deploying ITS Spot transceivers along roads with heavy traffic. About 1600 roadside transceivers were installed to support Dedicated Short Range Communication (DSRC) links conforming to the ISO 15628 standard, at locations meeting these criteria:

- Just before exit/entrance ramps of junctions and where major roads divide;
- Where drivers approach major bottlenecks; and
- Where it benefits drivers to receive timely traffic information.[107]

On intercity expressways the ITS Spot installations are 10-15 km apart. They are about 4 km apart on urban expressways (see map on the following page). By January 2014, 220,000 "Spot compatible" mobile ETC terminals had been shipped and sales are accelerating.

In addition to VICS and ETC, the "safe driving support" services offered by ITS Spot at present are mainly warnings displayed on the navigation screen, often with accompanying audio. These are customised according to vehicle speed ("you are going too fast"), the alignment of the vehicle relative

[106] http://www.vics.or.jp/english/

[107] ITS Joint Program Office (2013) *US-Japan Collaborative Research on Probe Data: Assessment Report – Final,* US Department of Transportation, http://ntl.bts.gov/lib/51000/51100/51168/US-JP_Probe_Data_ Final_Report_v8_2__FHWA-JPO-13-091_.pdf

to the roadway ("stay within marked lanes") or need for merging assistance ("caution, vehicle merging from left"). The system also recommends safe following distances with the car ahead, in light of the driving speed and road conditions. ITS Spot's information is updated 2-3 times every 5 minutes and is usually available in three languages: Japanese, English or Chinese.

Figure 5.4. ITS Spot-compatible car navigation system (left) and ITS Spot roadside transceiver (right)

Source: Japan's Ministry of Land, Infrastructure, Transport and Tourism.

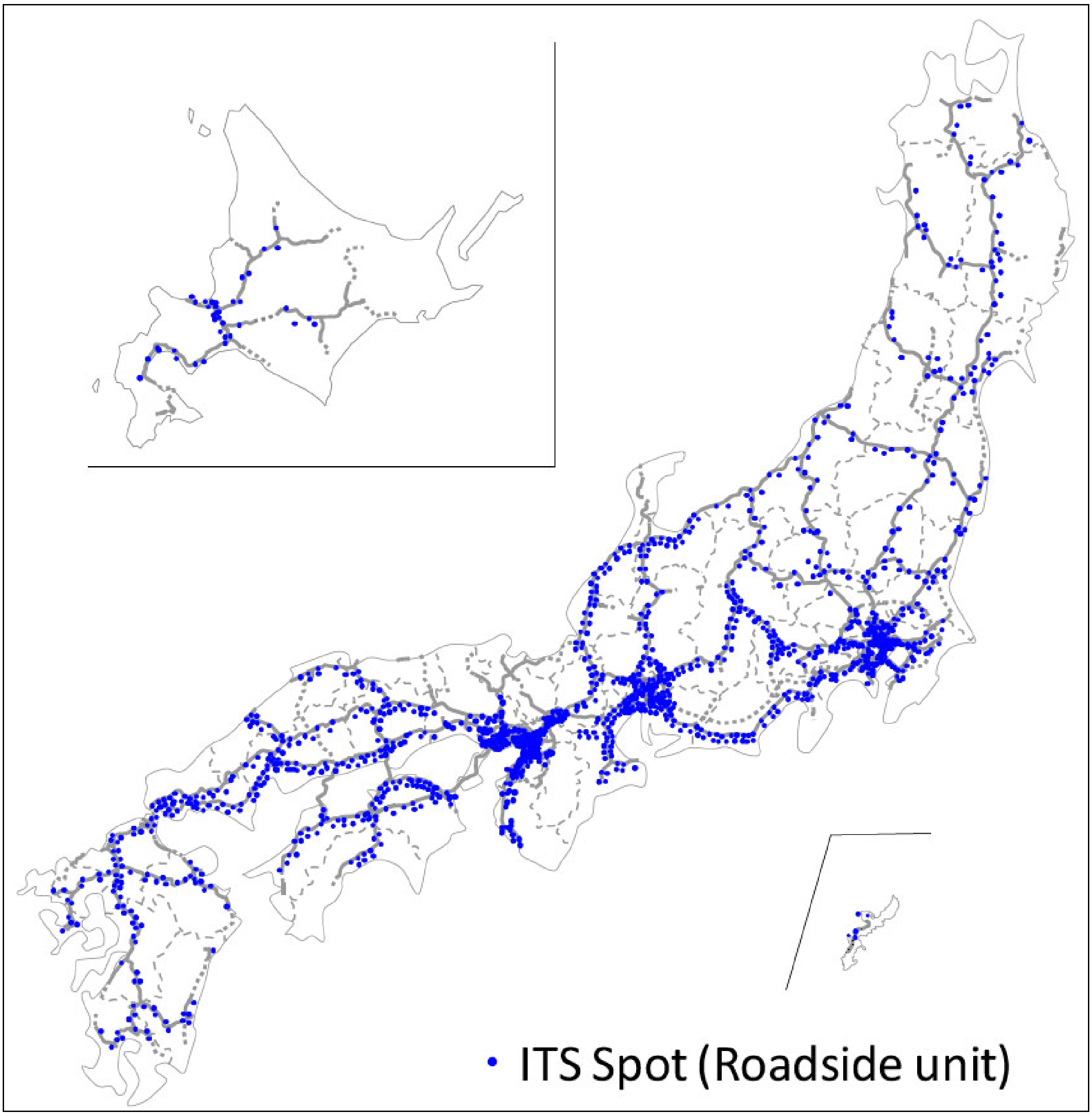
Private companies have been involved in developing ITS Spot, mainly as equipment producers, but the Ministry wants commercial firms to begin using the infrastructure to deliver services, too – e.g. to promote tourist attractions and restaurants, for guided tours, etc. A programme of experimentation with smartphones has begun, not just delivering information to them for display but also using them as information sources – e.g. tracking Bluetooth signals to measure speed of travel. It seems that interest is currently focused on the handset rather than on cellular networks as delivery systems.

The Digital Short Range Communications Security Platform is used to secure transmissions between onboard and roadside units. DSRC-SPF is said to be functionally equivalent to the Internet's Secure Socket Layer protocol.

Because the communication between the onboard ITS Spot equipment and the fixed infrastructure is two way, it is possible not only to deliver information to moving vehicles but to collect information from them – if drivers have consented to providing what is called "probe data". No special monitoring devices are installed to collect probe data. Just the standard elements of the vehicle navigation system are used: GPS receiver, gyro sensor and acceleration sensor. Three types of probe data are collected:

- **Basic information:** data about the car's navigation system (including manufacturer and model number), data about the vehicle (including part of the vehicle information entered by the user when they set up the navigation system, but not enough to identify the vehicle or driver exactly);
- **Travel records:** including time stamps, coordinates and category of road (expressway, urban expressway, arterial road, or other). The beginning- and end-points of journeys are not recorded to protect privacy;
- **Behaviour records:** time stamps, coordinates, direction, road category, longitudinal acceleration, lateral acceleration, and yaw angular velocity. To limit the accumulation of data, only sudden braking or sharp turns are recorded, as such events might occur just before an accident.

Figure 5.3. Map of roadside ITS Spot deployments



Source: Suzuki *et al.* (2014)

The vehicle's navigation system is able to store data from the last 80-100 km. This is uploaded when the vehicle passes an ITS Spot site and is then erased from navigation memory. Probe data is considered the property of the expressway companies and the Ministry of Land, Infrastructure, Transport and Tourism. Some of it is apparently shared with Japan's National Police Agency (ITS Joint Program Office, 2013, p. 29). But the Ministry did not start "mining" the collected data until 2013 when it decided what applications would be useful. The applications now being developed are:

- Aggregations of the average speed of travel on each road segment
- Aggregations of time required to travel various routes
- Locations where sudden braking and acceleration tend to occur

The Ministry realises that public acceptance is crucial for the development of more assertive forms of ITS, so they actively survey users to understand what is popular or unpopular, wanted or unwanted, in the existing services. Japanese culture is unique but some of the surveys' general findings may be relevant elsewhere. For example, it is clear that users welcome ITS Spot information, particularly about emergency situations (accidents, earthquakes, etc.) when they are on an unfamiliar road or when conditions are abnormal. But when they are familiar with the route and traffic is flowing normally, ITS Spot's eagerness to help is less appreciated. Perhaps surprisingly, the provision of still images of road conditions ahead has not been well received.

5.6.3 Future directions

The Ministry has said that ITS Spot-compatible ECS devices should be able to access the Internet at rest stops on expressways. Fifty stops already provide this service; more will be added.

Beyond that, the next stage of co-operative ITS development seems to be for ITS Spot to gain an "assistive" role in determining vehicle speed, in order to synchronise traffic flow: Co-operative/Adaptive Cruise Control. This would prevent the propagation of "deceleration waves" through congested zones leading to stop-and-go traffic jams, and to help maintain safe distances between vehicles by creating ad hoc "platoons". The advantage of platooning is that it enables traffic to be densified, increasing the road's carrying capacity without increasing risk of collision, while at the same time saving energy because vehicles in the platoon create a shared "slipstream" of reduced wind resistance (Suzuki, 2014).

By the 2020s the Ministry anticipates that progressive expansion of ITS Spot's capabilities and authority over vehicle movement will phase out the need for in-vehicle drivers.

5.6.4 Key lessons for this study

- The future of ITS is already unfolding in Japan, or at least part of it is. It will be interesting to see how the 760 MHz vehicle safety band develops alongside the now actively used 5.8 GHz band. It will clarify if both bands are needed, are they complementary, etc.
- The lack of involvement of the MNOs in Japan's leading edge ITS programme may be significant. However, the MNOs apparently do transmit probe data to the companies which sell navigation systems so they can update their maps and improve their routing algorithms. The public is probably unaware of this activity.
- While it is interesting that privacy protection measures are taken by the Ministry for their archive of probe data, it is not clear if the same protections are applied to data shared with the National Police Agency.

5.7 Legal considerations

Here we briefly examine some of the legal aspects of relying on commercial cellular networks to support mission critical services and other legal and regulatory issues related to their operational requirements. One of the tasks assigned for this study was to, in each sector,

> examine the level of legal certainty which is needed to establish a basis for agreements for the shared use of networks and make a distinction between various levels of sharing, such as sharing of active and passive network infrastructure with or without sharing of access to a common spectrum resource on the basis of individual authorizations (LSA).

Our research revealed few situations embodying those conditions in practice. Licensed Shared Access agreements (LSAs) are such a new regulatory instrument that they are not yet used for spectrum sharing among different networks in any of the three sectors. Approved in February 2014, ECC Report 205 notes that "The first practical use cases of LSA will be to provide access to additional spectrum for mobile broadband services (MFCN)… [possibly in] the band 2300-2400 MHz" where CEPT is developing harmonised conditions for the introduction of MFCN (see Section 3.3.3 above). But before LSA can be implemented, communication interfaces must be standardised between:

- Licensed incumbents and LSA repositories (where information is stored about spectrum availability and conditions of use)
- Different LSA repositories
- LSA repositories and LSA controllers (which manage spectrum access based on sharing rules and repository information)
- LSA respositories and national regulatory authorities
- LSA controllers and secondary LSA users

None of these interfaces has been standardised yet. "Sharing frameworks" must also be adopted by regulators at the national level and CEPT may need to develop Reports and Decisions for specific bands to ensure harmonisation. The whole process could take a few more years to complete.

So far as we can tell, agreements on the shared use of networks by PPDR organisations only depend on a "level of legal certainty" when the network is privately owned and operated (CO-CO). As Appendix A.13 indicates, such cases in the EU exist now only in Denmark, Ireland, Portugal, Spain and the UK. Some legal certainty is provided in those cases by Service Level Agreements with penalties. But these rest on the resilience and redundancy built into the network at the hardware level, usually as the result of custom designs to satisfy performance criteria in the build-out contracts and checked during acceptance of the completed system. SLAs are also supplemented in some cases by the requirements of ISO 9001 quality management certification. Particularly for organisations contemplating a move to CO-CO networks, the prospect of relying solely on an SLA may cause anxiety.

5.7.1 Legal acceptance of video evidence in courts in the European Union

Our research makes it clear that the desire to transmit and receive good quality video is one of the main drivers of demand for public safety broadband, be it mission critical or otherwise. Video can capture details difficult to describe in a written report and may also present those details more believably than a personal synopsis or recollection. Thus it can be credible evidence for what happened when or who said or did what to whom. But information on the legal status of such evidence, from the European Commission, DG Justice (Department B1, Criminal Justice), indicates that the EU Member States differ greatly in their acceptance of evidence recorded and transmitted electronically. Physical presence of witnesses and their testimony in court is often preferred. While there is some acceptance of recorded video or audio evidence among the Member States (e.g. hearings of witnesses and victims) there is still limited acceptance of other types of electronic evidence. Nor is there a clear trend toward greater acceptance of video as criminal evidence in trials. This gap between the police's embrace of video and the apparent caution of courts needs to be addressed. The solution may be better chains of custody to ensure the integrity and authenticity of broadband data when used as trial evidence or in investigations.

5.7.2 NRA rights to authorise the prioritisation of mission critical communications over a PLMN

In several EU MS, NRAs have no powers to give priority of emergency communications for the PPDR services over other users of a commercial PLMN, even for safety of life. Powers to request that MNOs accord such priority do vary by MS but in several cases, such as Denmark, NRAs do not have these powers over priority of traffic.

5.7.3 Regulatory powers over MNOs to provide mission critical services

At the current time, MNOs have no general obligation across the EU, apart from voluntary contractual guarantees (that they may enter into with SLAs) to provide the resilience and QoS required by the three sectors, of PPDR, utilities and ITS sector. Thus failure by an MNO to respect the contract is purely a contractual dispute, to be considered by arbitration perhaps or in the civil courts but not under telecommunications regulation.

Ensuring the priority of mission critical communications over a commercial mobile network would require an extension of the current powers of NRAs in most EU MS, most probably in conjunction with extra conditions in the licence to operate a PLMN and /or in the spectrum licence that an MNO holds. Those extra conditions would ensure that MNOs provide suitably resilient networks, appropriate responses to interruption of service and the accepted quality of service for mission critical communications.

6 Conclusions

6.1 Towards a definition of "mission critical"

In our survey of user and supplier stakeholders, we sought to clarify the definition of "mission critical" communications for each of the three sectors. There was a diversity of responses with some overlap but gaps and shortcomings as well. Desk research also revealed a range of inconsistent views. However, the one point on which many definitions seemed to agree is that a mission becomes critical when human life is at risk. If that was sufficient to define criticality, we could stop there. But we found that many people want to go beyond the simple criterion of life at risk to include risks of damage to valuable assets. For that reason we propose the following general definition of "mission critical":

> A mission is "critical" when its failure would jeopardise one or more human lives or put at risk some other asset whose impairment or loss would significantly harm society or the economy.

"Risk to life" provides a rather clear test even though perceptions of risk are subjective. But the scope of the phrase "mission critical" is made elastic and arguable by including other assets whose loss would cause significant harm (which assets? how significant?). Yet that is the situation today.

In the utility and transport sectors, incidents happen with significant but diffuse impacts on society or the economy – disruptions and delays that cause economic harm if many people are affected or the duration is long. ENISA calculates the significance of communication network outages with a mathematical function that combines the number of users affected with the duration of the outage. The same can be done for power cuts or traffic jams to produce a simplified scale of socioeconomic damage. Some level of impact could then be identified as the threshold of significance, which might vary from subsector to subsector according to an agreed impact per user per hour. Preventing harm above those levels could then be defined as a "critical mission" (in addition to preventing injury or loss of life), while harm below those levels could be considered "business critical" if the damage is largely confined to one enterprise.

But statements differentiating between "mission critical" and "non-mission critical" assume that a distinction *can* be cleanly drawn which will be recognised as intuitively correct. Part of our task has been to determine if there is – or could be – agreement across the three sectors on how and where to draw this distinction, for voice and for data. Our conclusion is that the three sectors interpret criticality differently so some inconsistency is inevitable.

For PPDR, the range is marked by step-changes, from small property damage, to significant property damage up to loss of life or multiple loss of life, etc. Most of these step-changes are within the "mission critical" category, not from non-critical to critical. Utilities in contrast see machine-to-machine (M2M) data communications for the control of supply systems as "mission critical" while voice is only mission critical when network malfunctions are being repaired, or the public is in danger. In the case of ITS, avoiding injuries, accidents and large negative economic impacts can all be considered "mission critical" while in the rail industry, maintaining safe operation is the most critical issue.

The "mission critical/non-mission critical" dichotomy is thus an oversimplification. There are degrees of criticality and many different but valid ways to distinguish critical from non-critical.

6.2 Feasibility of using commercial mobile networks for mission-critical communications

Today's commercial mobile radio networks provide minimally acceptable levels of resilience and security, perhaps because differences in resilience and security are rarely considered in choosing a carrier. ENISA's studies show that large-scale outages are frequent for MNOs, with briefer and localised outages almost too numerous to track. Dropped or blocked calls occur even when the network is working properly. Current technical commercial network designs do not take into consideration the needs of mission critical users nor do commercial networks yet accommodate the specific PPDR emergency features such as Push-To-Talk or the low latency requirements of smart grids. They may only become feasible contenders with major upgrades as explored previous chapters, with the addition of:

- Hardening for resilience to improve their availability from 95% to over 99% – with UPS, diverse routing, dual redundant RANs and core elements, failover, etc.
- New functionality specifically supporting teamwork in emergency situations. 3GPP LTE Releases 12-15 are expected to add them gradually by 2018-2020.
- Faster set-up, call prioritisation and always-open links.
- Tariff structures that do not charge users for emergency features on a pay-per-use basis. Fire fighters trapped in a burning building should not have to worry about how much their calls for help will burden the brigade's budget.

Based on past experience, the emergency services, utilities, and ITS players are reluctant to become wholly dependent on the MNOs. These three priority sectors have absolute commitments to the conservation of life and continuity of service. As they pointed out across many interviews and in the stakeholder workshop, MNOs do not share these commitments. Many utilities have regulatory obligations to deliver service under all conditions so they feel they must control their communications infrastructures – they cannot hand off liability to an MNO; railways may be in a similar position in many Member States.

Hence the issue is one of responsibility, and implicitly, who owns the spectrum licence. Who owns the network might be less of an issue. However, the three sectors on a standard commercial network without controls are vulnerable. The mission critical community would be less than 5% of the user base and thus could be in a weak negotiating position.[108]

Moreover, some Member State governments do not consider that their PPDR services should operate on any network that is not GO-GO or at least GO-CO. The concept of CO-CO is anathema to their state obligations and perhaps constitutional statutes.

Thus in what is put forward here, flexibility to opt out of using commercial mobile at Member State level and to build dedicated mission critical networks must be considered because the decision is a national prerogative and some states clearly prefer that option.

On the other hand, there are other forces at work that could give the MNOs incentives to comply with a new operational regime. Today's consumption of mobile services is nearing saturation in the EU. New consumers are hard to find – so commercial strategy focuses on retention of existing subscribers

[108] Public Safety Communications Europe expressed the scepticism of many when they noted that this report proposes "a new kind of MNO who puts social responsibility over shareholder value and acts like the service providers for dedicated TETRA networks… combined with additional services. It is questionable if this is possible." PSC Europe, private correspondence, 31 October 2014

while tempting other MNO's subscribers to switch provider. Until now, the MNOs have seen their future only in offering broadband mobile services for residential and business segments, while facing the severe financial burden of rolling out the next generation of technology, LTE. The latter burden has the effect of driving the MNOs towards offering additional services.

To renew their infrastructure, the MNOs need to finance LTE investment despite the present borrowing conditions. Following the 2008 economic crisis, these are quite different to the 1999/2000 3G investment rounds or those of previous decades when banks were eager to finance mobile expansion. However, the promise of long-term revenues from new and stable sources such as government could make the next borrowing rounds for new network investment much easier as bank covenants for new loans are negotiated. For MNOs, the prospect of additional utility and transport revenues is too tempting to ignore: there are few new long-term revenue streams around, let alone those backed by government investment in the MNO's own infrastructure, with major economic sectors as customers, such as the utility and transport industries. The key to security for the lenders, and shareholders, is the long-term nature of such revenue streams, which MNOs hope will attract pension and insurance funds as investors.

That explains some of the unexpectedly strong MNO interest in the opening rounds of bidding for the UK contracts for PPDR services. An MNO that wins would have a higher value attached to its capital assets and revenue prospects and thus to its share price. That would reduce the cost of borrowing for LTE roll-out, as a secure government backed contract would be at hand, with new revenues and major asset investments that can be reused to secure other revenue streams. Most surprisingly from MNO interviews, it might even imply that a change in the MNO short-term business model could be in sight. But to assure such a business model evolution, further change is needed, beyond network hardening, if the MNOs are to become the foundation of a mission critical infrastructure. A fundamental revision of MNO (and MVNO) behaviour models in key areas of MNO activities would be needed, specifically:

1. Being prepared to upgrade to high standards of reliability and response to failure, over the long term without any degradation in that commitment over several decades

2. Acceptance of long-term (15 to 30 year) contract commitments to customers and in particular to mission critical services

3. Providing priority access to mission critical services, especially when emergencies create a risk of network overload

4 Providing geographic coverage to meet the needs of mission critical users

5. Willingness to work with other MNOs and MVNOs – for instance, in handover of a call to the operator with the strongest signal, for mission critical communications

6. Keeping to the spirit and letter of long-term contracts for mission critical services without arbitrary changes in technical features, tariffs or contract conditions of service.

7. Readiness to submit cost-based pricing analyses of tariffs with full open book accounting for NRAs and government clients

8. Willingness to prepare new charging regimes that abandon the SIM-card model when necessary

9. Removal of any international roaming excesses across the EU and any "surprise charges" for agreed services.

Instead, a contrary pattern pertains currently. MNOs are driven by their boards and marketing departments to a specific business model that excludes long-term accords on any aspect of the business, apart from some spectrum licence agreements. Even these may be liable to opportunistic variations in ownership, sharing arrangements and reuse for new technologies. Generally the outlook of the mobile industry's business model in the EU is short-term, with product cycles for its service offerings ranging from two to eighteen months.

Thus to ensure MNO performance is maintained over decades, we consider that specific regulatory measures should be introduced, in addition to contractual structures. Such regulation is especially needed to reassure the three sectors, particularly those with regulatory obligations on continuity of service such as the utilities.

Use of apparently binding commercial SLAs on MNOs is unlikely to be enough. Introducing regulatory obligations is therefore necessary, in order to effect direct change in MNO behaviour, modifying the short-term outlook for the commercial conduct of affairs. That requires that the current position on both the legal obligations of MNOs and that of NRA powers over mission critical communications be amended.

But is this justified? The mobile industry has benefited from being treated as a new entrant to the telecoms sector, of being the lesser player between the 1980s and the 1990s *vis-à-vis* the fixed line incumbents, with extensive freedoms to grow being offered. Since the year 2000, that market position has changed dramatically as the numbers of MNO customers began to rival fixed line subscribers; by 2004 mobile subscribers exceeded fixed line globally. Thus the MNOs (many of which originated as subsidiaries of fixed line operators) are the new industry incumbents.

A position of significant market power implies a strong justification for change in the ground rules of regulation governing MNO commercial behaviour, especially to prevent lock-in by single MNO dependence, with preference for multiple MNO contracts. Mobile broadband will extend that power, especially with entertainment services such as OTT (over the top) TV. Overriding market power and the ability to offer a mission critical infrastructure introduces a need for appropriate service obligations. The essence of the new obligations required to redefine MNO commercial behaviour is outlined in the nine clauses highlighted above. As a result, it is essential to consider new measures that give national regulatory authorities (NRAs) specific new powers to cope with this situation on behalf of mission critical services:

1) MNOs should participate with enhanced responsibility in EU society and the economy with mandates to support mission critical services, to be implemented under two possible approaches:

   - Either to operate as an MNO, or an MVNO, in the EU will require observing obligations on provision of capacity and functions for mission critical networking services if so required by the Member State and its NRA (possibly in conjunction with other specialists, such as systems integrators). This is effectively a licence to operate as a mobile service provider. A harmonised form of such a network licence might be a useful instrument across the EU for mission critical operations.
   - Or an alternative is that any purchase of, or current exercise of, a mobile spectrum licence brings with it the obligation to support mission critical services for as long as the spectrum licence is valid. Note that the grant of spectrum conditioned on mission critical provisions offers NRAs the power to re-assign the spectrum to a new operator, if the original one fails to perform. This mechanism gives effective control to the NRA through the potential for spectrum re-assignment, such that the spectrum is not 'lost'.

   Some may view this as a universal service obligation. It is not. It is a *specific* service obligation, being restricted to emergency services and mission critical operations. MNOs *already observe security mandates* from most Member State governments for some kinds for policing activities.

2) NRAs should have the authority to introduce such regulation nationally under their own administrations and then to enforce it, assuring the provision of the mission critical support is

correctly delivered according to the long-term contracts and with the QoS required by the mission critical sectors.

3) NRAs should have the authority to set preferential priorities for mission critical communications carried by MNOs' commercial networks. That means they can take precedence over public consumer and business communications in specific circumstances. This would assure unblocked delivery, on the grounds of safety of life and continuity of essential services, over non-critical communications. NRAs would also ensure handover of a mission critical communications to the strongest signal among a group of MNOs, as determined by the local terminal.[109]

4) NRAs should support governments in setting tariffs for mission critical services by research into the true costs of MNO operation and comparative cost studies with other NRAs and sources from outside the Member State. This will require suitable accounting efforts by NRAs and appropriate preparations of the cost base declarations by MNOs.[110]

Mission critical services would be defined to include electricity, water and gas supplies, as well as eCall, and other appropriate road management and railway operations.

The key conclusion is that there is a potential role for the commercial MNO networks but only under specific regulatory structures to accompany the contractual commitment. Note that this leaves the choice of employing the MNOs as the foundation for mission critical communications up to each Member State. Who owns/operates the network is still a matter of national statuary obligations, politics and culture, which establishes the perceived risk and that varies by Member State. Thus there is no recommendation to impose a common EU policy mandate, though it may be useful to develop a consistent set of recommendations for Member States choosing to rely on commercial networks, in whole or in part.

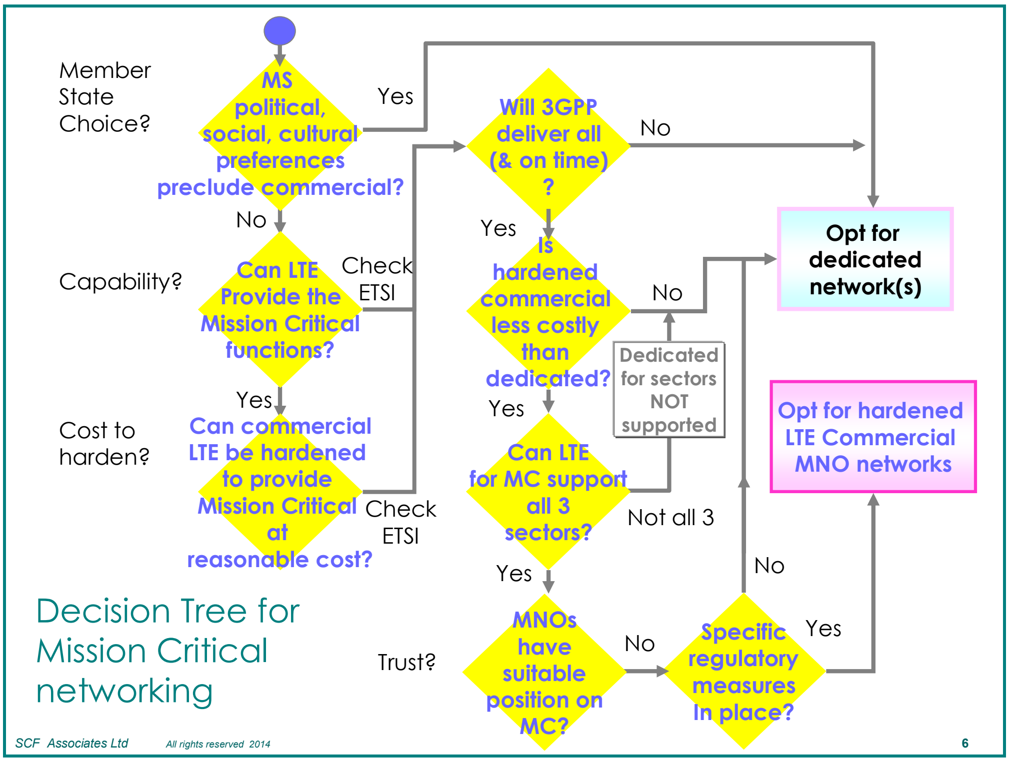
Barriers to commercial use cannot be removed immediately. But considering the medium and long term, sharing of the commercial MNO infrastructures for mission critical purposes makes economic sense. As noted, the crucial barrier is the current MNO mass-market business model, which needs to be suitably amended to provide guarantees of appropriate levels of mission critical service. Moreover *perceptions* of MNO capability and intentions will take some time to change. Hence, we expect dedicated networks to continue in operation for some time but progressively, for budget reasons, each Member State may well decide to move away from dedicated networks to shared commercial networks, as the various barriers outlined above are overcome.

Thus understanding the practical route to commercial mobile networks for governments and stakeholders can be seen as a series of decisions, as shown in the decision tree below, which summarises the way forward for this major new European initiative:

[109] UK Government (2014) "Open Consultation: Tackling Partial Not-Spots in Mobile Phone Coverage", Department for Culture, Media & Sport, 5 November, https://www.gov.uk/government/consultations/tackling-partial-not-spots-in-mobile-phone-coverage; see also Aittokallio, A. (2014) "UK government outlines plans for compulsory national roaming", *Telecoms.com,* 5 November, http://www.telecoms.com/301271/uk-government-outlines-plans-for-compulsory-national-roaming/

[110] This would complement and extend work performed during the past decade on harmonising regulatory accounting frameworks. See BEREC (2014) "Regulatory Accounting in Practice 2014", Report BoR (14) 114, 25 September, http://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/4595-berec-report-regulatory-accounting-in-pr_0.pdf

Figure 6.1 Decision tree for moving to commercial mobile mission critical broadband networks



6.3 Conclusions on the cost comparisons of the various options

Comparing the scenarios in a "for and against" analysis with relative value of costs and benefits is summarised in Table 6.1. A key task for the study was to identify the optimal scenario: for whom, in what circumstances, when and why:

- As summarised in Section 4.1, overall it is Scenario 2, using commercial mobile networks for broadband functionality, that is the most attractive in terms of value for money when capex and opex are combined, although advantages vary with the operating frequency. The net results, in terms of the cost per user, indicates that at 450 MHz, the dedicated network is cheaper in capex alone by over 40%, but when taking opex into account over ten years, the spreading of infrastructure costs for personnel and support favours the commercial networks, even at 800 MHz. However, if the dedicated LTE network of scenario option 3, with hardened commercial LTE equipment, is operating at 700 MHz, the commercial mobile, option 2 here at 800 MHz, can give a capex cost per user that is lower than the dedicated scenario of option 3 by some 40%. If MNOs decide to operate commercial mission critical networks in the 700 MHz band, the capex costs would be reduced from 800MHz, with up to 20% fewer base station sites required and costs lowered approximately in proportion.
- But the appeal of this option is effectively minimised if the objections and reservations of mission critical users are not addressed. As explained, that depends on stronger regulatory safeguards than are available today to assure trusted working between the three sectors and the MNOs, for the long term. It does offer the possibility of supporting utilities and ITS, if the data handling capabilities of an IP channel can be exploited at low cost for M2M applications or as a federator of specialised low cost networks.
- For the PPDR community alone, Scenario 1 (staying with TETRA for as long as possible) is really a shorter-term solution. Several major PPDR stakeholders realise that the value for money is limited by the lack of sufficient bandwidth for video and imaging applications. Thus Scenario 3, of dedicated networks based on LTE with hardened LTE equipment and handsets plus the UPS and

diverse routing, is the obvious next step for PPDR if dedicated networks cannot be abandoned for statutory, cultural and political reasons. However, even here, budgetary priorities may force reconsideration.

- However, if all three sectors are considered equally, then Option 4, a hybrid scenario combining existing PPDR networks with a phased move to a common LTE mix of dedicated and commercial mobile networks comes into play as being more flexible. Certainly the MNOs see this as a viable way forward. It does have technical challenges in federating multiple network types efficiently and at reasonable cost. But it offers the Member States flexibility in their support and financing decisions for dedicated and/or commercial networks, with decisions made at their own pace. Important time-dependent decisions on both the LTE standards and those on which spectrum bands may be available for dedicated networks can be accommodated perhaps more easily than other options. Enhanced flexibility makes the hybrid scenario a realistic and attractive choice.
- The final scenario, Option 5, a common network especially designed for all three sectors, leaves the past behind and starts with a fresh concept, embracing a resilient safety and emergency services network on a regional scale for Europe. A pragmatic view is that this option might be desirable but impossible to negotiate in any medium term future.
- Pure cost comparisons should also take in the social value of such services to obtain a balance. Some social values can be attributed a quantitative economic worth, in terms of loss of life, disruption, loss of output and so on.

A table of the five Options, comparing their strengths/advantages and disadvantages, follows below:

Table 6.1. Comparing the five network options

Scenario option	For	Against	Relative value
1 Dedicated network, dedicated spectrum, dedicated equipment: ▪ TETRA and GSM-R use continues for some years	▪ Exploits existing high value investment across the EU ▪ Reliable and suited to PPDR & railway use ▪ Rollout unfinished in some MS ▪ Allocated frequencies in the 400MHz band lowers buildout cost as fewer base stations needed than in higher bands ▪ Current investments good for another 10 years, largely for voice and nonbroadband data	▪ No broadband ▪ Suited to PPDR and railways more than to the other sectors ▪ Fairly high cost as limited suppliers and limited market volume ▪ TETRA difficult to interwork internationally – custom deployments by MS ▪ Older technologies, end of life in sight ▪ 400MHz frequencies may be reclaimed by NATO in some MS	**Low**
2 Commercial MNO networks with: ▪ Commercial LTE equipment hardened for resilience and 99.99% availability ▪ Extra coverage for 99% landmass, ▪ Prioritised mission critical traffic ▪ Improved single cell operation for group working ▪ TETRA/GSM-R features on LTE (DMO, ProSe, etc)	▪ Broadband capability ▪ Lower cost as using existing commercial infrastructure ▪ Operates in already allocated & licensed spectrum ▪ Uses new technology that is being adapted to mission critical needs (LTE) with a 20+ year life ▪ Exploits international standards and should easily provide interworking across the EU, between MS and different sectors ▪ Although most suited to PPDR, it could handle utilities and rail with hardened networks to meet the resilience requirements, if can carry M2M low data rate traffic at low cost efficiently.	▪ Must put trust in commercial concerns with a short term outlook – the MNOs – for which Mission Critical may form 5% of the market at most ▪ May need extra regulatory provisions and NRA powers to make operating viable and attractive to the 3 sectors ▪ Needs strong contractual SLAs and possibly an MVNO structure ▪ LTE Technology still not yet mature and proven for mission critical ▪ Standards still evolving – all will not be there before 2018/2020 so 'pre-standard' technology till then - and depends on 3GPP delivering ▪ Must use commercial spectrum so unless 700MHz used, hardening could be relatively expensive ▪ Tariffs for all sectors would have to be negotiated for low flat rate data carriage	**High***

3 Dedicated networks with commercial equipment (LTE)	▪ Broadband capability ▪ Lower cost equipment including handsets ▪ Dedicated operation as preferred by all 3 sectors ▪ Closer to current status of PPDR and GSM-R radio networks	▪ Needs own physical infrastructure, and depending on operational frequency band may be more expensive than TETRA in real estate ▪ Need to have a suitable exclusive frequency band - unclear which that will be across the MS– 450 or 700 MHz? ▪ Better suited to PPDR than other 2 sectors	**Medium**
4 Hybrid	▪ Could accommodate all 3 sectors more effectively than options 1, 2 and 3 if properly designed ▪ Can re-use existing TETRA/GSM-R sites while incorporating new LTE in a phased migration, allowing LTE to mature ▪ If can handle high volume messaging for utilities and ITS, then cost effective, otherwise expensive ▪ Offers EU-wide basic structure able to adapt to different needs of each MS	▪ Complex to build ▪ Complex to operate – will need MVNO structure, perhaps by sector ▪ May be very expensive if all benefits across the 3 sectors are all realised ▪ Gateways and interfaces between different networks add cost and may penalise performance unless well designed ▪ Frequencies of operation of each element RAN unclear currently ▪ Actual performance difficult to predict ▪ Shared RAN could be single point of failure unless redundancy and failover built in	**Medium**
5 Common single network for mission critical	▪ Designed for all three sectors from outset ▪ Could offer trans-EU disaster resilient platform for public safety, more survivable than other options ▪ Avoids problems of different technologies, although could use LTE as base	▪ Needs completely rethought approach to mission critical networks ▪ Actual costs unclear – possibly far more expensive than other options ▪ Optimal design is unclear – requires a thorough design exercise but will be complex and closer to military networks in redundancy requirements ▪ Role of commercial mobile networks may be limited ▪ Needs difficult negotiations with all stakeholders across the EU, by MS	**Low****

*Only if assurances on long-term service levels and contractual SLA obligations can be enforced, perhaps with new regulatory provisions - else Medium or Low.

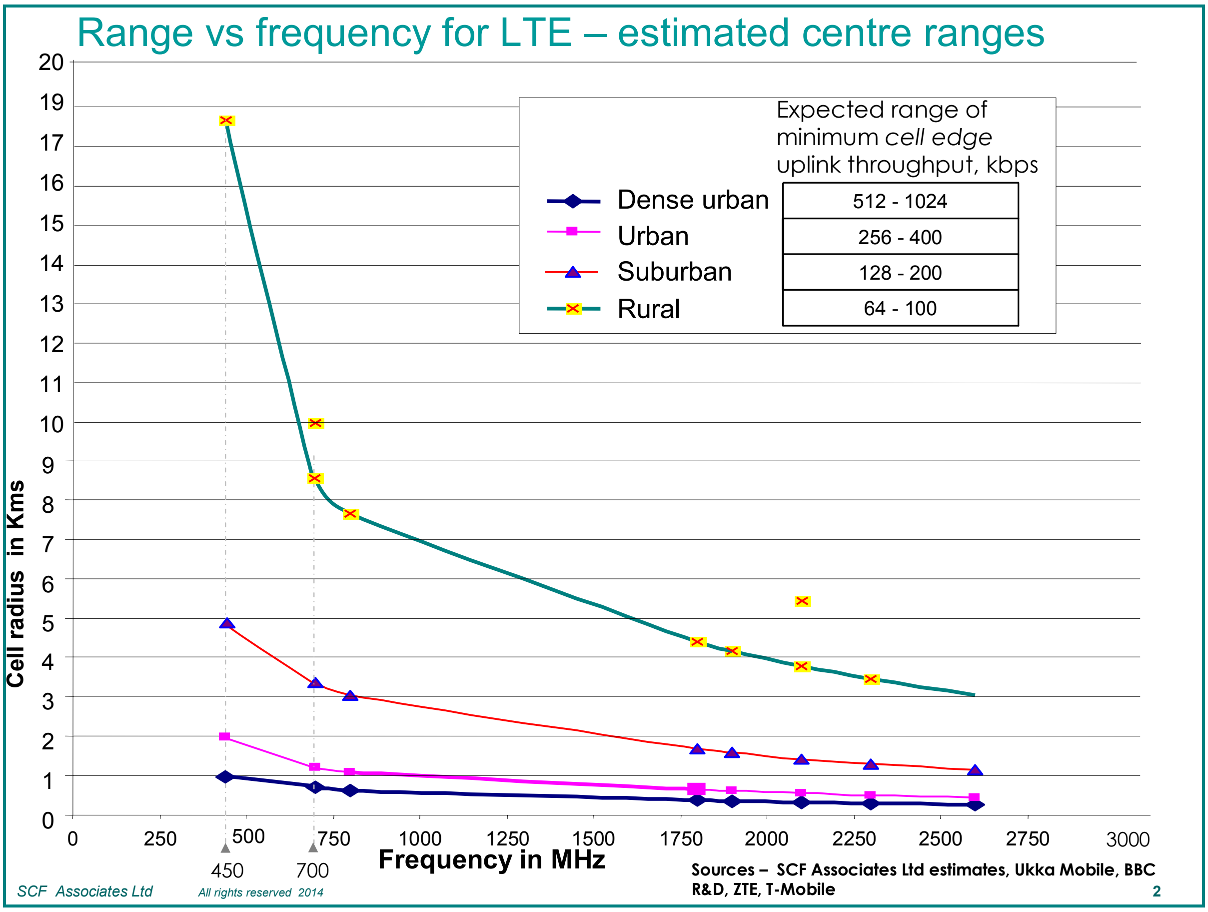
** Higher expense, long negotiations and design phases, despite offering a possible EU “safety shield”.

In summary, scenarios for options 2 and 4 may offer the most practical way forward but with certain significant barriers within each to be overcome.

6.4 Spectrum demands and possible ways forward

As emphasised previously, radio propagation characteristics depend on the frequency. Lower frequencies are more suitable for large cells (particularly useful in rural areas) and for assuring indoor coverage, as Figure 6.1 emphasises for LTE. Note that this figure gives curves for various propagation environments from dense urban to rural. More curves could have been added to show “interference limited” ranges, but these would not change the basic fact that signal range depends mainly on frequency and the environment. Such curves anyway are means with some scatter, taken from varied sources with differing power levels. Note also the fairly pessimistic cell edge uplink ranges, for LTE in 2012. Cell edge throughput may be improved with new technology such as MIMO. Essentially, these curves form the crux of the spectrum debate.

Figure 6.1. Graphs of range vs frequency - the crux of the spectrum debate



Overall the debate turns on the fact that the spectrum band chosen sets the propagation range for adequate signal strength, which in turn controls:

- Provision of enough capacity for all users, especially in disaster overload conditions
- Coverage requirements across the national geographic areas for varied terrain (dense forest, mountains, urban canyons, etc).

Also it is necessary to note that 2x10MHz has been identified as the minimum channel bandwidth for mission critical broadband, using today's technology (CEPT ECC Report 199). The following sections identify the spectrum ranges that are the most likely contenders for the implementation of mission critical broadband services in the EU Member States.

6.4.1 The '400 MHz band' (380-410 MHz, 410-430 MHz and 450-470 MHz) – individually or aggregated

In considering availability, the lower two bands may be subject to strong military claims and long duration licenses have been issued in all three bands. According to the Law Enforcement Working Party, "the 400 MHz spectrum suffers from the highest user density in Europe".[111] This is unfortunate, because the superior propagation characteristics of these bands reduce the number of sites needed to provide coverage and are especially advantageous for rural areas. Thus, because of limited availability

[111] LEWP (2014) "LEWP position on BB PPDR frequencies", http://cept.org/Documents/wg-fm/18091/INFO-004_Statement-on-BB-PPDR-frequencies-and-on-WRC15

across the EU, the band is difficult to consider as a stand-alone solution for the full 2x10 MHz needed, despite obvious advantages, especially the 450 MHz range where military claims are less likely.

In reply to a CEPT FM 49 questionnaire to NRAs in 2013 on the possibility of making all or part of the 410-430 MHz and/or 450-470 MHz bands available for broadband PPDR LTE networks, approximately half of the respondents (11 out of 24) saw no possibility, including Italy and the UK. Many of these administrations referred to heavy usage of the band by other services. Most of these are narrowband and digital PMR/PAMR for which refarming is difficult. The same proportion of the remaining respondents (11 of 24) saw some possibilities for limited uses in sub-bands. These were mostly at 450-470 MHz, but in the middle- to long-term future (e.g. France and Germany after 2020). This could only be under conditions like shared usage with commercial LTE networks (ECO, 2014).

The variable availability of these bands across the EU could create a more fragmented mission critical spectrum situation. On the other hand, the appearance of 450 MHz markets in other parts of the world, as well as in the EU (eg in Finland) might help foster economies of scale. And as mentioned, the band is already used with CDMA for certain utilities in the Netherlands.

To counter the limited availability of bandwidth in specific frequency ranges, LTE is able to aggregate different frequency ranges to create “virtual channels”. Such a mixed-band solution could take a 2x5 MHz block in the 410-430 MHz and/or 450-470 MHz range and 2x5 MHz from another frequency range. Thus the 400 MHz bands might be viable options as part of a 2x10 MHz channel mix that includes other frequency ranges.

For LTE at 450 MHz, the 450 Alliance, an industry consortium, leads the way with suppliers such as Qualcomm for chipsets and Huawei for equipment. Huawei is already installing a 450 MHz LTE network in Finland, with rollout taking less than six months because they are upgrading an existing CDMA network and a few hundred base stations are enough to cover the whole landmass. A theoretical exercise for a dedicated 450 MHz network for Germany showed that just 1,588 sites would provide nationwide coverage including in-building penetration in most built-up areas (450 Alliance, 2014).

That could offer flexibility to EU Member States if some other band is chosen in conjunction with it. The most likely contender could be the 700 MHz band, which might form a background for a future EU spectrum decision. There could also be aggregation with another band, even using a commercial MNO’s 2x5 MHz RAN, which would require some form of carefully tariffed roaming agreement.

Obviously 2x10 MHz would be the preferred goal, but that may not be realistic. Our conclusion is that if the 450 MHz band with at least 2x5 MHz can be agreed on, and reserved across the EU, that could be the most desirable outcome, especially if it can be matched by a complementary 2x5 MHz channel from another band, to assure broadband operation with current technology. It could be used as an exclusive mission critical band, or it may be exploited by commercial operators providing mission critical services under licence, if a Member State decides to pursue that path. But agreement across the EU on a harmonised allocation may be difficult to achieve.

6.4.2 The future of the 700 MHz band is being considered by regulators

In the absence of a consensus on the 450 MHz band, and with the decisions reached in WRC-12, parts of the 694–790 MHz band are being considered for mission critical applications. One possibility could be for those Member States that want to build dedicated networks to reserve 2x10 MHz, while the rest of the 700 MHz band might be allocated for commercial MFCN, PMSE, M2M, etc. Such a decision would provide adequate bandwidth in the EU, and may encourage more Member States to move to commercial LTE platforms, if adequate spectrum for lower cost networks were made available. Currently commercial LTE networks have different spectrum allocations around the globe. That is why adoption of the 700 MHz LTE band is so important for commonality, for mission critical applications as much as for commercial mobile. Note that the lower in the 700 MHz band the dedicated swathes are positioned, the better this would be for price and field performance. More generally, the band possesses attractive physical propagation characteristics. LTE technology exploits beam-forming and MIMO-type eNodeB-antenna systems very effectively at 700 MHz, even more so than at 450 MHz. But note that a network at 700 MHz will be approximately twice as expensive as one at 450 MHz because of the increased number of base station sites, equipment volumes and backhaul connections. Use of the 700 MHz band could optionally be either as a dedicated network, a commercial solution or in a combined, hybrid solution.

Choice of the 700 MHz band is strongly supported for mobile broadband by the PPDR community in Europe (as represented through the CEPT ECC FM49 working group). Consequently, various Member States are considering national decisions endorsing mobile broadband for PPDR specifically. That could become the core of an EU-wide harmonised band plan. However television broadcasters in the EU oppose the use of this band for either mission critical or commercial broadband.

The key question here is that, when use of the 700 MHz band for mobile in the EU begins, whether a harmonised exclusive allocation for mission critical services is necessary and desirable, in the potential presence of commercial offerings. Our conclusion is that the diversity of policy views among Member State governments makes re-allocation for dedicated networks likely in the short-term, with a subsequent migration to commercially based services also likely longer term as economic pressures mount. Note that this migration from a dedicated allocation to a commercial network could be helped, not hindered, by a prior exclusive reservation if it is also transferred.

6.4.3 Bands above 790MHz

IMT bands above IMT-790 may be useful as auxiliaries for broadband mission critical services. Any or all LTE-bands harmonised in CEPT above 790 MHz could be used for this. Thus handsets that can make use of multiple IMT bands above the two discussed already will be useful for broadband back-up, probably using the commercial services, be they LTE at 800 or 900 MHz or 3G UMTS at 1 to 3 GHz. Certainly many MNOs are considering small cell architectures for broadband delivery at much faster speeds, which might be useful for mission critical services on an opportunistic basis.

Commercial mobile radio networks use frequency bands much higher than those used for current PPDR networks (800-2600 MHz, versus 380-400 MHz). Higher frequencies are more suitable for small cell networks and thus urban settings, in order to provide more capacity but they may require more power, especially at cell edges. Thus PPDR use of commercial mobile radio networks requires an analysis of whether the bands used by a specific network meet their requirements. Broadband capabilities would be enhanced if PPDR services could combine dedicated and commercial networks above 1 GHz. Hardened terminal suppliers would need multiple RF chipsets to cover all the bands, but the result would be terminals which can be used in multiple countries, providing economies of scale. Whether voice in this situation would be VoLTE or provided by some other 3G flavour, or even GSM, is unclear.

6.4.4 Summary – the short and long term views

The reality across the EU is that some Member State governments, for statutory, cultural or political reasons, will today accept only government ownership of mission critical communication networks. In such cases, there is no question whether mission critical users should have dedicated spectrum for dedicated networks: *they must.* Therefore all cannot be left to commercial networks in the short to medium term. But to retain the advantages of high volume equipment production, some sort of EU-wide agreement on the leading spectrum candidate bands (450 or 700 MHz) is needed.

In the short term: 450 MHz offers the best network economics but 700 MHz may be more practical and attainable. A short-term compromise might be 2x5 MHz in each of the two contender bands, aggregated to produce a 2x10 MHz bandwidth.

Long term solutions: the WRC-15 conference is likely to have longer term impact, perhaps over the next two or three decades, with the WRC-18 conference probably having reinforcing effects. On the other hand, a trend in this area that may have unexpected benefits for mission critical broadband is the development of LTE for licence exempt spectrum, as both a supplement (in carrier aggregation) and an alternative to licensed spectrum. 3GPP is studying these ideas now and they may lead to new feature sets in future standards releases. Mission critical communication might be able to take advantage of this, too, on a dynamic opportunistic basis, with suitable signal processing for resilience, security and maximum flexibility.

6.5 Lessons from the case studies

Here we give just the key messages from each of the six case studies.

6.5.1 Use of commercial networking - the Emergency services mobile communications project (UK)

Among the case studies of commercial cellular use, perhaps the most interesting is not yet in service – the UK Emergency Services Mobile Communications Project (ESMCP). The primary motivation for pursuing this course is economic, even though the delivered network should have capabilities beyond what Airwave (the current PPDR network) offers. But as the new network will be based on "pre-standard" LTE releases, substantial effort has gone into the close control of risk, with detailed modelling of financial outlays and technological risks. Unrealistic low bids have been ruled out, i.e. those which indicate that a tenderer has underestimated the task.

6.5.2 FirstNet (USA) – building a dedicated PPDR network

This case study is a lesson in the need for agreement among stakeholders in countries, like the USA, where devolved rights are strong, *before* taking the decision to proceed. Two years into the project FirstNet is still at the preliminary planning stage, without an agreed business model, technical design or deployment schedule, in part because individual states can "opt out" if they don't like what FirstNet offers.

The second lesson is that failure of US regulation to assure priority carriage for mission critical communications over commercial networks has ruled out the option of relying on the MNOs to own and operate FirstNet. Before he resigned FirstNet's general manager observed that American MNOs would probably never grant public safety pre-emption rights even during emergencies. That is why the USA must fund a dedicated PPDR network instead of buying services from commercial carriers.

6.5.3 Blue Light Mobile (ASTRID, Belgium) – the MVNO approach

An important first message is that ASTRID found it possible to trust MNOs to provide a resilient, reliable service with higher priority for first responders than for public subscribers. Second, it is possible to find a solution involving minimal investment in equipment by using those MNOs. A mission critical network has been created virtually by using ASTRID's encryption and identity management on commercial networks. "Blue Light Mobile" is an MVNO that acts as single managerial interface between the Belgian MNOs and ASTRID subscribers. A third message is that having access to multiple networks provides better coverage than any single network. Blue Light terminals automatically switch to another network if local signal strength fades to unacceptable levels. Cross-MNO SIM cards provide the equivalent of international roaming, and roaming rights extend into neighbouring countries. A fourth message is that branding and "helpdesk" support are useful for public safety services, no less than for commercial services, and can retain users who might have tried to make their own arrangements with individual carriers.

6.5.4 ENEL (Italy) – utility as telecom provider

The first lesson from this case study is that there are synergies between nationwide electricity distribution companies and nationwide telecom networks, to the extent that regulators need to decide if joint ownership is anti-competitive. ENEL was Italy's state-owned electricity network. Its post-privatisation strategy involved creating a converged telecom company that could supply it – and its customers – with fixed and mobile telephony and Internet services. ENEL saw smart electricity meters as portals to homes for the delivery of services beyond electric power: these homes would eventually have devices needing remote management which ENEL was uniquely positioned to provide. Thanks to ENEL's ambitious vision, Italy was the first country in the world to fully deploy smart meters. But a leadership change ended ENEL's dream of becoming a key player in home automation and the delivery of information services for subscribers. It sold its debt-ridden telecom subsidiary and now focuses on green energy.

Nevertheless, the synergies that ENEL saw were real and led to substantial reductions in per-customer operating costs. The lower operating costs led to a payback of the initial investment (capex) in less than three years. That is a second message from this case study. A third message is that the average total data transmission time per meter per year is only about six minutes, so communications are a very small part (about 4%) of the metering system's operating cost.

6.5.5 Duke Energy (USA) – preparing for tomorrow's smart grid/smart city infrastructure

Duke Energy has put together an industry supplier coalition as a practical base for moving into smart grids with a very low cost, high performance, open standard platform. In this way they are challenging other suppliers that want to continue using proprietary protocols to protect their market niches and keep their customers, the utilities, locked in.

Duke's management decided that they do not want to be in the telecom business: communication technology evolves faster than traditional utility assets so for them it makes more sense to use a service provided by a third party rather than buy, or build and own, several wireless networks over many decades.

6.5.6 ITS Spot (Japan) – national ITS network for traffic information and management

Japan is the clear world leader in the development of cooperative ITS. ITS Spot is a cluster of services based on two-way 5.8 GHz dashboard radios with built-in card readers that interface with GPS navigation systems and automatically deduct road use fees as vehicles pass through checkpoints.

Perhaps the most important message from Japan's ITS experience is that public acceptance is crucial to the development of more ambitious forms of traffic management. So the authorities actively survey users to understand what is liked or disliked about existing services. A corollary is that once the basic service platform is in place, slow progress is a good thing, allowing time to build familiarity and public acceptance. Third, privacy protections must be in place from the start for both active and archived vehicle data, especially when police have access to the data.

A fourth message seems significant even though it is hard to interpret: cellular networks are not involved in Japan's leading edge ITS programme even though ITS Spot wants entrepreneurs to create new mobility based applications and innovative uses for the roadway communication network.

6.6 Could LTE fill the "TETRA gap"?

6.6.1 LTE can do it - if the conditions are right

Certainly LTE can fill the TETRA gap for PPDR if it is:

- ***Technically fully capable*** – which means that the standards development organisations, ETSI 3GPP and to some extent the OMA, must deliver mission critical functionality, sooner rather than later. 3GPP LTE Releases 12, 13 and 14 should cover DMO, PPT and resilience. Late delivery will complicate uptake. As our research highlighted, current LTE equipment has performance problems in handling voice and multimedia which need to be resolved.[112] New implementations of the IMS stack in a collapsed form may overcome its current inefficiencies for call setup in high volume. A key question for mission critical services is whether an "Open IMS" stack will become a standard construct. It will be essential for VoLTE QoS also.
- ***Allowed to –*** investments in TETRA (especially in unfinished deployments such as Germany's) are not sacrosanct, so new spectrum for dedicated mobile broadband networks is on the agenda at WRC-15 and across the EU. That is to say, we may have a "two track Europe" for a while as both late-start TETRA and early-start PPDR-dedicated LTE are deployed in neighbouring countries.

But TETRA still has major advantages for mission critical communications, in terms of:

- ***Reliability*** – though that is mainly due to the way networks are designed and constructed rather than the air interface.
- ***Range and building penetration*** – a frequency dependent property and an implementation issue also. If LTE were allocated the same or nearby frequencies (at 450 MHz, for example) it would enjoy the same propagation.
- ***Security*** – designed from an architectural level upwards to resist attack, it offers far superior levels of security over the current generations of commercial mobile technology for voice and narrowband data

But TETRA has some disadvantages, too:

[112] CEMAS, Mobile Computing and Networks Research Centre, University of South Wales, UK, interview

- A small number of equipment suppliers, high prices and proprietary lock-in problems.
- No broadband capability.
- Incomplete interworking standards between different TETRA networks (ISI), interfering with emergency service personnel working together across networks and borders, despite the original design objective in the 1995 specification. Even within a single network, products from different TETRA manufacturers cannot always interoperate.
- Lack of common standards for control room interfacing, leading to proprietary solutions. This brings with it a lack of common standards for network management functions (Steppler, 2011).

Nevertheless, LTE is only technically feasible for mission critical use if it has the promised new functionalities:

- All required PPDR functions added to 3GPP standards for suppliers to begin designing equipment.
- Performance is adequate – especially extensions with prioritisation, MCPTT, etc, as well as consistent support for VoLTE, the use of MIMO for better signal reception, broadband data with aggregated band pairing and supplementary links if required, etc
- Networks are sufficiently redundant and resilient.

6.6.2 LTE for mission critical M2M, utilities, road and rail?

Could LTE offer a solution for sectors other than PPDR? For the utilities this not just a question of PPDR features so much as very high reliability, low-bit rate bursty data messaging at ultra low cost for M2M type applications on a massive scale of many millions of metering points, control actuators and monitoring sensors. As mentioned earlier, there are cheaper networks with more appropriate specifications for these applications than LTE. The structures proposed here use LTE as a federator of M2M networks, not as the prime platform.

For rail, LTE-R has already been tested in pilot form in the current GSM-R bands in the EU. However, the statement quoted in Appendix C.4 points a different way forward: separating train control functions from the radio layer to a maximum degree, so railways could have a variety of options for implementing ETCS. That seems the only "future-proof" solution. On the other hand, LTE is likely to develop support for eCall (automatic road accident reporting) as well as any GSM or UMTS network.

> With PPDR functions added to the 3GPP standards, LTE could supplement and then eventually replace TETRA/TETRAPOL, and with global volume production, do so at lower cost while adding capabilities that TETRA/TETRAPOL will never match. Although relatively new, LTE is already cheaper than TETRA, and within 3-5 five years, LTE equipment prices should be significantly less, for both commercial and mission critical markets. But as was emphasized in Chapters 2 and 3, the radio interface technology has little impact on total network costs. Developing and operating base station sites, erecting antenna masts, the total number of base stations needed to cover an area, and the degree of redundancy needed are the real cost drivers and these apply to any mission critical network, regardless of the standard.

6.7 Could a common regional critical infrastructure be built?

The answer is yes, but the barriers to such a project are the large upfront investment; the multinational negotiations needed to reach agreement on the design, financing, management and ownership structure, etc.; and the novelty of the concept itself.

There are areas of commonality across the three sectors as well as complementary demands. But the greatest commonality is in the "back end" – the need for backhaul – rather than in the "front end" – the radio access node. That is the logic of focusing on a critical infrastructure rather than a common radio network. Also the incremental cost of adding users to an existing network is marginal if common requirements have already satisfied but the number of users and sectors expands. The cost per user falls as user numbers increase since network costs are relatively fixed.

A common Europe-wide platform could have economic benefits for all three sectors while providing a more secure safety net for a future digital society if it can be adequately engineered – organisationally, financially and technically. Its successes and failures would be a demonstrator for other regions and for global systems.

However, this concept differs substantially from the other four scenario options, which are all variations on existing networks with new technology incorporated in various combinations. Scenario 4, the hybrid network, is the most complex of these and it, too, aims to be a common platform for all three sectors but from the starting point of legacy networks which are gradually replaced. This is quite different from Scenario 5, which is a bespoke mission critical platform designed anew, and so it is much more challenging politically. It would require EU-wide agreement on:

- Economic justification and long term funding requirements (eg would funding be regional, national, or some combination?) That could complicate and delay agreements on the way forward.
- Which sectors should to be served and therefore which functions to support.
- System security and protections derived from risk assessments.
- Technical architecture for resilience that will serve all sectors and their evolving requirements, with broadband as well as narrowband data channels for the utilities, PPDR and ITS.

It would probably have to start as an EU-wide solution, but it could gradually integrate national PPDR functions. That is where the greatest difficulty would be encountered, and the most delicacy needed, in that for the majority of current PPDR networks across the EU, the network is operated under government control for the national public safety community. A common critical infrastructure would be different in that governments would contribute but not necessarily control everything.

Bibliography

----- (1999) "Commercial Wireless Performance Evaluation Comparison & Applicability Report," SAFECOM Program, US Dept. of Homeland Security, http://www.safecom program.gov/library/Lists/Library/Attachments/235/Commercial_Wireless_Performance_Evaluation.pdf

----- (2005) *The impact of video evidence on modern policing: Research and best practices from the IACP study on in-car cameras,* International Association of Chiefs of Police, http://www.cops.usdoj.gov/Publications/video_evidence.pdf

----- (2006) "EC-RRG Guidelines for the Providers of Critical National Telecommunications Infrastructure", Electronic Communications Resilience and Response Group, UK, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/86101/telecoms-ecrrg-resilience-guidelines.pdf

----- (2009) "APT Report on 'Possible Harmonized Use of Bands 406.1-430 MHz, 806-824/851-869 MHz, 4940-4990 MHz, 5850-5925 MHz for PPDR Application in some APT Countries', APT/AWF/REP-08, http://www.aptsec.org/sites/default/files/APT-AWF-REP-08APT_Report_on_PPDR.doc

----- (2010) "Communication Requirements of Smart Grid Technologies", US Department of Energy, http://www.smartgrid.gov/sites/default/files/Smart_Grid_Communications_Requirements_Report_ 10-05-2010.pdf

----- (2012) "APT Report on PPDR Applications Using IMT Based Technologies and Networks", APT/AWG/REP-27, http://www.aptsec.org/sites/default/files/Upload-files/AWG/APT-AWG-REP-27_APT_Report_PPDR_IMT_Based_Technologies.doc

----- (2012) "Dealing with Disasters: Technical Challenges for Mobile Operators", GSM Association, http://www.gsma.com/mobilefordevelopment/dealing-with-disasters-technical-challenges-for-mobile- operators

----- (2012) "European Integrated Railway Radio Enhanced Network System Requirements Specification Version 15.3.0", https://www.uic.org/IMG/pdf/p0028d004.3-15.3.0.pdf

----- (2013) Archive of contributions to the FCC Workshop on Network Resiliency, 6 February at Brooklyn Law School, NY, USA, https://www.edas.info/web/fcc-nr2013/

----- (2013) "APT Report on Usage of Intelligent Transportation Systems in APT Countries", APT/AWG/REP-18 (Rev.1), http://www.aptsec.org/sites/default/files/Upload-files/AWG/APT-AWG-REP-18-R1-APT_Report_on_Usage_of_ITS.docx

----- (2013) "APT Report on Technical Requirements for Mission Critical Broadband PPDR Communications", APT/AWG/REP-38 (September edition), http://www.aptsec.org/sites/default/files/Upload-files/AWG/APT-AWG-REP-38-APT_Report_on_PPDR.docx

450 Alliance (2014) "The Economics of 450 MHz Band for the Smart Grid and Smart Metering", http://www.450-connect.de/dokumente/WhitePaper_Economics_450MHz_SmardGrid.pdf

Adnet, F., Petrovic, T. and Lapostolle, F. (2011) "Comparison of prehospital emergency care systems in Europe and the United States", chapter 4 in *The ESC Textbook of Intensive and Acute Cardiac Care,* Oxford University Press, http://oxfordmedicine.com/view/10.1093/med/9780199584314.001.0001/med-9780199584314-chapter-004

Ahmed, E., & Eltawil, A. M. (2014) "All-Digital Self-interference Cancellation Technique for Full-duplex Systems", 20 June, http://arxiv.org/abs/1406.5555

Alcatel-Lucent (2014) "The US's Nationwide Public Safety LTE Network and the Global Adoption of LTE for Next-Gen Mission-Critical Communications", http://www.slideshare.net/junsukseo946/ss-38161804

Ambulancezorg Nederland (2010) "Ambulance Care in Europe", http://www.ambulancezorg.nl/download/downloads/202/report-ambulancecare-in-europe-jan-2010.pdf

Andersson, K. & Kafle, V. P. (2014) "Disaster-Resilient Mobile Network Architecture", *Proceedings of the 11th Annual IEEE Consumer Communications & Networking Conference: 5th IEEE CCNC International Workshop on Mobility Management in the Networks of the Future World (MobiWorld 2014),* http://pure.ltu.se/portal/files/88326433/p359_andersson.pdf

Baldini, G. (2010) Report of the workshop on "Interoperable Communications for Safety and Security" jointly organized by DG ENTR & DG JRC with the support of EUROPOL and FRONTEX, http://publications.jrc.ec.europa.eu/repository/bitstream/111111111/14970/1/lbna24540enc.pdf

Baldini, G., *et al.* (2012) "The Evolution of Public Safety Communications in Europe: the results from the FP7 HELP project", ETSI Reconfigurable Radio Systems Workshop, http://docbox.etsi.org/workshop/2012/201212_rrs/presentations/jrcec_baldini.pdf

Baran, P. (1964a) *On Distributed Communications: VIII. The Multiplexing Station,* Memorandum RM-3764-PR, USAF Project Rand, August, http://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3764.pdf

Baran, P. (1964b) "On Distributed Communications Networks", *IEEE Transactions on Communications,* Vol. CS-12, No. 1, 1 March, http://www.cs.ucla.edu/classes/cs217/Baran64.pdf

Beckebanze, H. (2001) "Warum Setzen die BOS nicht einfach auf öffentliche Mobilfunknetze?" [Why not simply put public safety communications on public mobile networks?], Deutsche Polizeitechnisches Institut, http://www.pfa.nrw.de/PTI_Internet/pti-intern.dhpol.local/Funk/Aufsatz_UMTS.pdf

Bennett, J. (2014) "Public-safety LTE deployments accelerate slowly", *RadioResource Media Group,* http://www.radioresourcemag.com/onlyonline.cfm?OnlyOnlineID=440

Berbineau, M. (2001) "Les systèmes de télécommunication existants ou émergants et leur utilisation dans le domaine des transports guidés", *Synthese No. 40,* Institut Francais des Sciences et Techniques des Reseaux, de l'Amenagement et des Transports, http://www.ifsttar.fr/fileadmin/user_upload/editions/inrets/Syntheses/Syntheses_INRETS_S40.pdf

BEREC (2010) "Response to the European Commission's consultation on the open internet and net neutrality in Europe", BoR (10) 42, 30 September, http://berec.europa.eu/eng/document_ register/subject_matter/berec/download/0/188-berecs-response-to-the-european-commissi_0.pdf

BEREC (2012) "Differentiation practices and related competition issues in the scope of Net Neutrality", BoR (12) 31, 29 May, http://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/35-berec-draft-report-for-public-consultati_0.pdf

Berg Insight (2014) "Smart Metering in Europe", http://www.berginsight.com/ReportPDF/ProductSheet/bi-sm10-ps.pdf

Bertenyi, B. (2014) "Developments in 3GPP – Release 12 and beyond", 3GPP, http://www.3gpp.org/ftp/Information/presentations/presentations_2014/2014_05_bertenyi_3GPP_Rel12_beyond.pdf

Bhatia, B. (2012) "Wireless Technology Standards for Emergency Telecommunications", presented at ITU International Workshop on Emergency Communications and Information Management, Bangkok, Thailand, http://www.itu.int/ITU-D/asp/CMS/Events/2012/emergencyworkshop/Bharat_Bhatia.pdf

Bretschneider, M. (2004) "Emergency and security communication in Germany ('BOS-NETZ 200x'): Is TETRA, TETRAPOL or a GSM/UMTS based solution favorable?", Universität Hannover, http://www.bretschneidernet.de/publications/bos-paper/html/

Budka, K. C., *et al.* (2011) "Public Safety Mission Critical Voice Services Over LTE", *Bell Labs Technical Journal,* Volume 16, issue 3, pages 133-149, http://onlinelibrary.wiley.com/doi/10.1002/ bltj.20526/abstract

Burns, J., and Jervis, V., eds. (2013) "PPDR's Current and Future Scenarios", Public Protection and Disaster Relief - Transformation Centre, Deliverable D2.1, version 2.00, http://www.ppdr-tc.eu/userfiles/deliverables/PPDR-TC-D2.1-v2.00_1567038775.pdf

BWCS (2012) "The European Market for Train-based Wireless Broadband Services", cited in Parsons, R. (2012) "Past & Future of Wi-Fi on Train Services", *EURAILmag,* http://eurailmag.com/past-future-of-wi-fi-on-trains-services/

Calle-Sánchez, J., *et al.* (2013) "Top Challenges of LTE to become the next generation railway communication system", in *Computers in Railways XIII* (WIT Press), pages 85-96, http://www.google.cz/books?id=f7eE3ZaTdMcC

Carbone, J. (2010) "Safety Critical Systems in Rail Transport", Express Logic Ltd., http://rtos.com/images/uploads/Safety-Critical_Systems_In_Rail_Transportation.pdf

Carlberg, K., *et al.* (2003) *Preferential Emergency Communications: From Telecommunications to the Internet,* Kluewer Academic Publishers, http://books.google.com/books?id=FFbk45g_hJsC

Carpentier, P. (2013) "The Danish nationwide emergency network SINE and perspectives for the future", presented at When Every Second Counts: Advanced Broadband Mobile Emergency Communications, Copenhagen, 14 November, http://amcham.dk/files/editor/2_-Slides_2013-11-14_DTU_konference_2.pdf

CDG (2013) "The 450 MHz Band for the Smart Grid and Smart Metering", CDG 450 Connectivity Special Interest Group, http://www.cdg.org/resources/files/white_papers/CDG450SIG_450MHz_Band_Smart_Grid_Smart_Metering_Concept-SEPT2013.pdf

CEPT (2012) "Catalogue of PPDR Applications Related Requirements", Meeting Document FM49(12)035 Annex 3, http://www.cept.org/Documents/fm-49/7164/FM49(12)035_Report-PT49-to-WGFM-75-Annex-3-Catalogue

CEPT (2014) "Draft Report A from CEPT to the European Commission in response to the Mandate 'to develop harmonised technical conditions for the 694 -790 MHz ("700 MHz") frequency band in the EU for the provision of wireless broadband and other uses in support of EU spectrum policy objectives'", Draft CEPT Report 53 for public consultation, http://www.cept.org/files/1051/Tools%20and%20Services/Public%20Consultations/2014/Draft%20CEPT%20Rep53.zip

Chang, S. (2012) "Broadband Mobile Communication for PPDR Applications – IEEE 802.16 GRIDMAN", ITU International Workshop on Emergency Communications and Information Management, Bangkok, Thailand, http://www.itu.int/ITU-D/asp/CMS/Events/2012/emergency workshop/SungCheol_Chang_ETRI.pdf

Chen, W.-P., *et al.* (2007) "Performance Measurement, Evaluation and Analysis of Push-to-Talk in 3G Networks", *Proceedings of the IEEE International Conference on Communications,* pages 1893-1898, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4288986

Choi, I. J., *et al.* (2010) "Achieving Single Channel, Full Duplex Wireless Communication", presented at MobiCom 2010, http://web.stanford.edu/~skatti/pubs/mobicom10-fd.pdf

COCOM (2013) "Implementation of the European emergency number 112 – Results of the sixth data-gathering round", Communications Committee Working Document 13-04 REV1, DG Communications Networks, Content and Technology, http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1674

Comfort, L. K., Boin, A., & Demchak, C. C., eds. (2010) *Designing Resilience: Preparing for Extreme Events,* University of Pittsburgh Press

Commission Staff Working Document (2013) "On a new approach to the European Programme for Critical Infrastructure Protection: Making European Critical Infrastructures more secure", SWD(2013) 318 final, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/docs/swd_2013_318_on_epcip_en.pdf

Commission Staff Working Document (2014) "Implementation of the EU regulatory framework for electronic communications – 2014", SWD(2014) 249 final, http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=6473

Council of the European Union (1996) "Council Directive 96/48/EC of 23 July 1996 on the interoperability of the trans-European high-speed rail system", http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31996L0048

Council of the European Union (2009) "The Council Recommendation on improving radio communication between operational units in border areas" 10141/09 ENFOPOL 143, TELECOM 116, COMIX 421 (4-5 June 2009), http://www.cept.org/files/9421/Council%20Recommendation%2010141-09.pdf

Critical Communications Broadband Group (2012) , "CCBG RG application + service matrix", TETRA + Critical Communications Association, http://www.tandcca.com/Library/Documents/Broadband/CCBG%20RG%20application+service%20matrix%20(version13-9-2012).xls

Critical Communications Broadband Group (2013) "Mission Critical Mobile Broadband: Practical standardisation & roadmap considerations", TETRA + Critical Communications Association, http://www.tandcca.com/Library/Documents/CCBGMissionCriticalMobileBroadband whitepaper2013.pdf

de Bruijne, M., van Eeten, M.J.G., Roe, E. and Schulman, P. (2006) "Assuring High Reliability of Service Provision in Critical Infrastructures", *International Journal of Critical Infrastructures,* Volume 2, Number 2/3, pages 231-246.

De Groeve, T., *ed.* (2013) "Overview of Disaster Risks that the EU faces", European Commission Joint Research Centre, http://publications.jrc.ec.europa.eu/repository/bitstream/111111111/29598/1/lb-na-25822-en-n.pdf

Dekker, M., Christoffer, K. and Lakka, M. (2013) "Annual Incident Reports 2012", ENISA, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2012

Denef, S., *et al.* (2011). "ICT Trends in European Policing", Comparative Police Studies in the EU (COMPOSITE), Deliverable 4.1, http://repub.eur.nl/pub/40565/metis_185158.pdf.

Devine, T., *et al.* (2013) *LTE brings a new capability to mobility: How might it enable a range of cross-sector services?,* PA Consulting Group for the UK Office of Communications, http://stakeholders.ofcom.org.uk/market-data-research/other/technology-research/2013/Future-LTE-Services/

Dewaele, J. (2001) "User Requirements: TETRA TEDS Colloquium", ETSI TCCE, http://portal.etsi.org/tcce/pptpres/tedsrev2.ppt

DG MOVE (2014) *EU Transport in Figures: Statistical Pocketbook,* http://ec.europa.eu/transport/facts-fundings/statistics/pocketbook-2014_en.htm

Docomo (2014) "DOCOMO and Huawei confirm LTE network over unlicensed spectrum - key advancement toward the global standardization of LAA technology", NTT/Docomo press release, 21 August, https://www.nttdocomo.co.jp/english/info/media_center/pr/2014/0821_00.html

Durantini, A., *et al.,* (2008) "Integration of Broadband Wireless Technologies and PMR Systems for Professional Communications", 4th International Conference on Networking and Services, http://dx.doi.org/10.1109/ICNS.2008.30

EC (2009) "Commission Decision of 22 July 2009 amending Decision 2006/679/EC as regards the implementation of the technical specification for interoperability relating to the control-command and signalling subsystem of the trans-European conventional rail system (the European Deployment Plan)" C(2009)5607, http://ec.europa.eu/transport/modes/rail/interoperability/ertms/doc/edp/edp_en.pdf

EC (2011) “White Paper: Roadmap to a Single European Transport Area – Towards a competitive and resource efficient transport system” COM/2011/0144 final - http://ec.europa.eu/transport/themes/strategies/ 2011_white_paper_en.htm

EC (2014a) “Report from the Commission: Benchmarking smart metering deployment in the EU-27 with a focus on electricity”, COM(2014) 356 final, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2014:356:FIN

EC (2014b) “Commission Staff Working Document on the state of play of the implementation of the ERTMS Deployment Plan”, SWD(2014) 48 final, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/swd/com_swd(2014)0048_/com_swd(2014)0048_en.pdf

ECC (2007a) “Public Protection and Disaster Relief Spectrum Requirements”, Report 102, http://www.erodocdb.dk/docs/doc98/official/pdf/ECCRep102.pdf

ECC (2007b) “Compatibility studies between Broad Band Disaster Relief (BBDR) and other systems”, Report 110, http://www.erodocdb.dk/docs/doc98/official/pdf/ECCRep110.pdf

ECC (2008) “Decision of 27 June 2008 on the harmonisation of frequency bands for the implementation of digital Public Protection and Disaster Relief (PPDR) radio applications in bands within the 380-470 MHz range”, ECC/DEC/(08)05, http://www.erodocdb.dk/docs/doc98/official/pdf/ECCDec0805.pdf

ECC (2013) “User requirements and spectrum needs for future European broadband PPDR systems (WideArea Networks)”, Report 199, http://www.erodocdb.dk/Docs/doc98/official/pdf/ECCREP199.PDF

ECC (2014a) “Licensed Shared Access”, Report 205 (February), http://www.erodocdb.dk/Docs/doc98/official/pdf/ECCREP205.PDF

ECC (2014b) “Harmonised conditions and spectrum bands for the implementation of future European broadband PPDR systems”, Draft ECC Report 218, Meeting Document FM(14)090r1 Annex 1, FM49(14)012, http://www.cept.org/Documents/fm-49/13111/FM49(13)048rev1_Draft-ECC-Report-B-new-version-with-incorporated-texts-from-Forum-and-input-contributions

ECO (2014) “ECO summary of replies to FM49 questionnaire on 400 MHz”, Meeting Document FM49(14)003rev2(2), http://www.cept.org/ecc/groups/ecc/wg-fm/fm-49/client/meeting-documents/file-history?fid=15326

El-Moghazi, M. A., Whalley, J. and Irvine, J. (2014) “European influence in ITU-R: the end of an era of dominance?”, *info,* Vol. 16, No. 4, pages 1-17, http://www.econstor.eu/bitstream/10419/88486/1/773359214.pdf

ENISA (2009) “Stock taking report on the technologies enhancing resilience of public communication networks in the EU member states”, http://www.enisa.europa.eu/publications/archive/stock-tech-res/at_download/fullReport

ETSI (1995) “Radio Equipment and Systems (RES); Trans-European Trunked RAdio (TETRA) system; Packet Data Optimized; Part 1: General network design”, ETS 300 393-1, http://www.etsi.org/deliver/etsi_i_ets/300300_300399/30039301/01_60/ets_30039301e01p.pdf

ETSI (2006a) "Technical characteristics for Broadband Disaster Relief applications (BB-DR) for emergency services in disaster situations; System Reference Document", Technical Report TR 102 485, V1.1.1, http://www.cept.org/files/9421/ETSI%20TR%20102-485%20on%20BB-DR.pdf

ETSI (2006b) "Emergency Communications (EMTEL); Overview of Emergency Communications Network Resilience and Preparedness", Technical Report TR 102 445 V1.1.1, http://www.etsi.org/deliver/etsi_tr/102400_102499/102445/01.01.01_60/tr_102445v010101p.pdf

ETSI (2008) "Project MESA; Service Specification Group - Services and Applications; Statement of Requirements (SoR)", Technical Specification TS 170 001 V3.3.1, http://www.etsi.org/deliver/etsi_ts/170000_170099/170001/03.03.01_60/ ts_170001v030301p.pdf

ETSI (2009) "…5 GHz BroadBand Disaster Relief applications (BBDR)…" Harmonised European Standard EN 302 625, V1.1.1, http://www.etsi.org/deliver/etsi_en/302600_302699/302625/01.01.01_60/en_302625v010101p.pdf

ETSI (2010a) "Additional spectrum requirements for future Public Safety and Security (PSS) wireless communication systems in the UHF frequency range", Technical Report TR 102 628 V1.1.1, http://www.etsi.org/deliver/etsi_tr/102600_102699/102628/01.01.01_60/tr_102628v010101p.pdf

ETSI (2010b) "Terrestrial Trunked Radio (TETRA); Release 2; Designer's Guide; TETRA High-Speed Data (HSD); TETRA Enhanced Data Service (TEDS)", Technical Report TR 102 580, http://www.etsi.org/deliver/etsi_tr/102500_102599/102580/01.01.01_60/tr_102580v010101p.pdf

ETSI (2011) "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Designers' guide; Part 6: Air-Ground-Air", Technical Report TR 102 300-6 V1.1.1, http://www.etsi.org/deliver/etsi_tr/102300_102399/10230006/01.01.01_60/tr_10230006v010101p.pdf

ETSI (2012a) "User Requirement Specification; Mission Critical Broadband Communication Requirements", Technical Report TR 102 022-1 V1.1.1, http://www.etsi.org/deliver/etsi_tr/102000_102099/10202201/01.01.01_60/tr_10202201v010101p.pdf

ETSI (2012b) "Emergency Communications (EMTEL); European Public Warning System (EU-ALERT) using the Cell Broadcast Service", TS 102 900 V1.2.1, http://www.etsi.org/deliver/etsi_ts/102900_102999/102900/01.02.01_60/ts_102900v010201p.pdf

European Parliament (1996) "Decision No 1692/96/EC of the European Parliament and of the Council of 23 July 1996 on Community guidelines for the development of the trans-European transport network", http://ec.europa.eu/transport/wcm/infrastructure/grants/2008_06_20/2007_tent_t_guidlines_en.pdf

European Parliament (2013) "Regulation (EU) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on Union guidelines for the development of the trans-European transport network and repealing Decision No 661/2010/EU", http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32013R1315:EN:NOT

European Parliament (2014) "Legislative resolution of 3 April 2014 on the proposal for a regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent…", text adopted 3 April, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0281+0+DOC+XML+V0//EN

EuroSafe (2013) "Injuries in the European Union 2008-2010: Summary of injury statistics for the years 2008-2010", Issue 4, European Association for Injury Prevention and Safety Promotion, http://ec.europa.eu/health/data_collection/docs/idb_ report_2013_en.pdf

Faure, C. (2005) "Working Document on the deployment of the European Rail Traffic Management System ERTMS", DG MOVE, http://www.docstoc.com/docs/49182659/Working-Document-on-the-deployment-of-the-European-Rail-Traffic-Management-System-ERTMS

Federal Communication Commission (2013) "Impact of the June 2012 Derecho on communications networks and services", http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-318331A1.pdf

Federal Coordinating Office, Project Group on Public Safety Digital Radio (2013) "On the Future Architecture of Mission Critical Mobile Broadband PPDR Networks", version 1.1, German Ministry of the Interior, http://www.cept.org/Documents/fm-49/14437/FM49(13)-071-Info_White-Paper-on-Mission-Critical-Mobile-Broadband-PPDR-Networks

Ferrús, R. and Sallent, O. (2014) "Extending the LTE /LTE-A Business Case to Professional Mobile Radio", Wireless World Research Forum, Meeting 32 (Marrakesh, Morocco, 20-22 May), http://www.wwrf32.ch/tl_files/Themes/wwrf32/Presentations/WWRF32-WGC-02-LTE-Professional-Mobile-radio.pdf

Fornefeld, M., Delaunay, G., and Elixmann, D. (2008) *The Impact of Broadband on Growth and Productivity, A study on behalf of the European Commission,* http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/broadband_impact_2008.pdf

Frazer, P., *et al.* (2003) *Current status, knowledge gaps, and research needs pertaining to firefighter radio communication systems,* TriData Corporation, http://www.cdc.gov/niosh/fire/pdfs/ffrcs.pdf

Grilli, A. (2013) "Why Utilities Need Access to Radio Spectrum", European Utility Telecom Council Radio Spectrum Strategy Group, http://eutc.org/system/files/UTC_private_file/EUTC%20Spectrum%20Position%20Paper-9April2013.pdf

Grous, A. (2013) "Socioeconomic Value of Mission Critical Mobile Applications for Public Safety in the EU: 2x10MHz in 700MHz in 10 European Countries", London School of Economics, http://www.tandcca.com/Library/Documents/Broadband/LSE PPDR EU.PDF

Gulyaev, A. (2014) "A European Harmonised Spectrum for Broadband PPDR", presented at Critical Communications Europe, 10-12 March, http://www.cept.org/files/1050/Deliverables/ECO%20presentations/A%20European%20Harmonised%20Spectrum%20for%20BB%20PPDR%20CCE%20conferene%2010-12%20March%202014%2C%20Amsterdam%20-%20AG.pptx

Hallahan, R., and Peha, J. M. (2008) "Quantifying the costs of a nationwide broadband public safety wireless network" *Proceedings of the 36th Telecommunications Policy Research Conference,* http://www.ece.cmu.edu/~peha/costs_of_public_safety_network.pdf

Hallahan, R., and Peha, J. M. (2009) "The business case of a nationwide wireless network that serves both public safety and commercial subscribers", *Proceedings of the 37th Telecommunications Policy Research Conference,* http://www.ece.cmu.edu/~peha/profitability_of_ public_safety_ network.pdf

Hallahan, R., and Peha, J. M. (2010) "Policies for Public Safety Use of Commercial Wireless Networks", *Proceedings of the 38th Telecommunications Policy Research Conference,* http://users.ece.cmu.edu/~peha/public_safety_priority_access.pdf

Hamadeh, D. (2014) "Bringing Public Safety Communications to the Next Generation", presented at the 2nd African Preparatory Meeting for WRC-15, January, http://www.atu-uat.org/ index.php/download-categories/category/12-annex-2?download=146:ppt-9-2ndapmforwrc-15-motorola

Handley, J. P., Smith, R. and Laval, S. S. (2014) "The Coalition of the Willing: Leveraging the Vendor Community and the Principles of Open Source in the Utility Space", DistribuTech 2014, http://s36.a2zinc.net/clients/pennwell/dtech2014/Public/SessionDetails.aspx?SessionID =7055

Henze, T. (2013) "LTE proximity services", presented at the Broadband World Forum, http://www.slideshare.net/zahidtg/lte-proximity-services

Hunt, R. C. (2002) "Emerging communication technologies in emergency medical services", *Prehospital Emergency Care,* Volume 6, Number 1 (January-March), pages 131-6, https://www.ncbi.nlm.nih.gov/pubmed/11789642

Ilie, E. (2013) "Advanced technologies increase interoperability on the European railway networks", *Railway Pro,* August, http://www.railwaypro.com/wp/?p=13338

ITU (2003) "Radiocommunication objectives and requirements for public protection and disaster relief", Rep. ITU-R M.2033, http://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2033-2003-PDF-E.pdf

ITU (2012a) "Frequency Arrangements for Public Protection and Disaster Relief Radiocommunication Systems in UHF Bands in Accordance with Resolution 646 (Rev.WRC-12)", Rec. ITU-R M.2015, http://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2015-0-201203-I!!PDF-E.pdf

ITU (2012b) "Working Document Towards a Preliminary Draft Revision of Report ITU-R M.2228: Advanced Intelligent Transport Systems (ITS) Radiocommunications", Meeting Document 5A/198-E (Annex 20), https://www.itu.int/md/dologin_md.asp?lang=en&id=R12-WP5A-C-0198!N20!MSW-E

ITU (2013a) "Working Document Towards a Preliminary Draft Revision of Report ITU-R M.2033 - Radiocommunication objectives and requirements for Public Protection and Disaster Relief (PPDR)", 3 June, https://www.itu.int/md/dologin_md.asp?lang=en&id=R12-WP5A-C-0306! N20!MSW-E

ITU (2013b) "Working Document Toward A Preliminary Draft New Report ITU-R M.[B-PPDR] "Broadband Public Protection and Disaster Relief Communications", 3 June, https://www.itu.int/md/dologin_md.asp?lang=en&id=R12-WP5A-C-0306!N21!MSW-E

ITU (2013c) "Working Document Toward a Preliminary Draft Revision of Recommendation ITU-R M.2015 - Frequency arrangements for public protection and disaster relief radiocommunication systems in UHF bands in accordance with Resolution 646 (Rev.WRC-12)", 3 June, https://www.itu.int/md/dologin_md.asp?lang=en&id=R12-WP5A-C-0543!N14!MSW-E

ITU (2013d) "The use of International Mobile Telecommunications (IMT) for broadband Public Protection and Disaster Relief (PPDR) applications", Preliminary Draft New Report [IMT.BROAD.PPDR], 15 October, https://www.itu.int/md/dologin_md.asp?lang=en&id=R12-SG05-C-0064!R1!MSW-E

ITU-T Focus Group on Disaster Relief Systems, Network Resilience and Recovery (2014) "Overview of Disaster Relief Systems, Network Resilience and Recovery", Technical Report FG-DR&NRR Version 1.0, http://www.itu.int/en/ITU-T/focusgroups/drnrr/Documents/ fg-drnrr-tech-rep-2014-1-Overview.pdf

Jackson, D. (2013) "UK seeks to replace TETRA with LTE as early as 2016", *Urgent Communications,* http://urgentcomm.com/tetra/uk-seeks-replace-tetra-lte-early-2016

Johur, J. J. (2013) *Evaluating the Benefits of Mission-Critical Mobile Broadband to the UK Police Service,* Henley Business School, MBA thesis

Karsberg, C., Moulinos, K. and Dekker, M. (2013) "Power Supply Dependencies in the Electronic Communications Sector", ENISA, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/power-supply-dependencies/at_download/fullReport

Kilbourne, B. & Bender, K. (2010) "Spectrum for Smart Grid: Policy Recommendations Enabling Current and Future Applications", Utilities Telecom Council/IEEE, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5622000

Lamy, P. (2014) "Report to the European Commission: Results of the Work of the High Level Group on the Future Use of the UHF Band (470-790 MHz)", 26 August, http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=6721

Lavalle, C., *et al.* (2005) "Towards an European integrated map of risk from weather driven events" (EUR 22116 EN), EC Joint Research Centre, http://publications.jrc.ec.europa.eu/repository/bitstream/111111111/7732/1/EUR_22116_2005_Lavalle_et_al.pdf

Law Enforcement Working Party Radio Communication Expert Group & ETSI (2012) "LEWP-RCEG/ETSI Matrix of Applications", CEPT/ECC Meeting Document FM49(12)035 Annex 4, http://www.cept.org/Documents/fm-49/7166/FM49(12)035_Report-PT49-to-WGFM-75-Annex-4-Matrix

Lerner, E. B., *et al.* (2012) "An economic toolkit for identifying the cost of Emergency Medical Services (EMS) systems: detailed methodology of the EMS Cost Analysis Project (EMSCAP)", *Academic Emergency Medicine,* volume 19, issue 2 (February), pages 210–216, http://onlinelibrary.wiley.com/doi/10.1111/j.1553-2712.2011.01277.x/pdf

Liam, M. and Mendiratta, V. B. (2011) "Mission critical communication networks for railways", *Bell Labs Technical Journal,* Volume 16, Issue 3 (December), pages 29 - 46, http://onlinelibrary.wiley.com/doi/10.1002/bltj.20520/pdf

Loeb, J. (2014) "Minister: Police tech use 'not up to scratch'", *Police Oracle,* 30 June, http://www.policeoracle.com/news/Police+IT+and+Technology/2014/Jun/30/Minister-Police-tech-use-not-up-to-scratch_84033.html

Longstaff, P. H. (2005) "Security, Resilience, and Communication in Unpredictable Environments Such as Terrorism, Natural Disasters and Complex Technology", Center for Information Policy Research, Harvard University, http://pirp.harvard.edu/pubs_pdf/longsta/longsta-p05-3.pdf

Lyngstøl, T. H. (2013) "Public Safety, from Narrowband to Broadband - Dilemmas and Challenges", presented at When Every Second Counts: New Advanced Broadband Mobile Emergency Communications, Copenhagen, 14 November, http://amcham.dk/files/editor/4_-20131114_When_every_second_counts_THL.pdf

Lyon, R. M., *et al.* (2013) "The inaugural European emergency medical dispatch conference – a synopsis of proceedings", *Scandinavian Journal of Trauma, Resuscitation and Emergency Medicine,* Volume 21 (September), pages 73-76, http://www.sjtrem.com/content/21/1/73

Mandoc, D. (2012) "Future Railway Mobile Telecommunication Systems – Project Proposal", *UIC eNews,* number 314, http://www.uic.org/com/article/3209

Mandoc, D. (2013) "Defining a transition path to IP-based railway communications", *TrackTalk*, Issue 6, http://www2.alcatel-lucent.com/blogs/tracktalk/issue-6/defining-a-transition-path-to-ip-based-railway-communications/

Marcus, J. S., *et al.* (2010) *PPDR Spectrum Harmonisation in Germany, Europe and Globally,* WIK-Consult, http://www.wik.org/uploads/media/PPDR_Harmonisation_en_public_final_01.pdf

Marcus, J. S. (2013) "The need for PPDR broadband spectrum in the bands below 1 GHz", WIK-Consult discussion paper, http://www.tandcca.com/Library/Documents/Broadband/WIK%20report%20on%20PPDR%20Spectrum.pdf

Marsden, C. (2013) "Net Neutrality Law: Past Policy, Present Proposals, Future Regulation?", presented at the Internet Governance Forum, 25 October, http://ssrn.com/abstract=2335359

Masters, D. (2014) "The Communications Node and the Open Source Revolution", Ambient blog, 12 March, http://www.ambientcorp.com/blog/bid/338940/The-Communications-Node-and-the-Open-Source-Revolution

Mazza, S. L. (2008) "An Evaluation of Self Contained Breathing Apparatus Voice Communication Systems", US National Fire Academy, http://www.usfa.fema.gov/pdf/efop/efo42145.pdf

McKinsey & Co. (2012) "Seizing the 4G opportunity", https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/High%20Tech/PDFs/Seizing_4G_2012-02.ashx

Merklinger, J. M. (2008) Chapter 15: "Public Emergency Services Alarm, Dispatch, and Communications Systems" in *Fire Protection Handbook,* [US] National Fire Protection Association

Monemian, M., *et al.* (2009) "Analytical model of failure in LTE networks", IEEE 9th Malaysia International Conference on Communications, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5431443

Motorola (2009) "Interconnecting TETRA systems", http://www.motorolasolutions.com/web/Business/_Documents/White%20Paper/_Static%20files/Interconnecting%20TETRA%20systems.pdf

Mulloly, M. (2014) "LTE network launches are becoming less frequent as focus shifts to emerging markets and LTE-A upgrades", Analysys Mason, 3 July, http://www.analysysmason.com/Research/Content/Comments/LTE-emerging-upgrades-Jul2014-RDTN0/

Murray, I. (2014) "The Public Safety LTE & Mobile Broadband Market: 2014–2020", IEEE Communications Society, 12 March, http://community.comsoc.org/blogs/isabellamurray/public-safety-lte-mobile-broadband-market-2014-2020

MSB and DNK (2014) "Cross-border Communication for DNK/Nødnett and MSB/Rakel Systems", Myndigheten för samhällsskydd och beredskap & Direktoratet for nødkommunikasjon, https://www.msb.se/Upload/Produkter_tjanster/Rakel/Nyheter_och_kalender/ISI/Radio_Terminal_Requirements_for_ISI_20140526.pdf

National Highway Traffic Safety Administration (2014) "US Department of Transportation issues advance notice of proposed rulemaking to begin implementation of vehicle-to-vehicle communications technology", 18 August, http://www.nhtsa.gov/About+NHTSA/Press+Releases/2014/NHTSA-issues-advanced-notice-of-proposed-rulemaking-on-V2V-communications

NetMotion Wireless (2013) "Mobile Technology Use in the Utility Industry: Benchmarking Study", http://www.slideshare.net/NetMotionWireless/net-motion-wireless20102011utilitymobiletechnologybenchmarkingstudyrpt

Noam, E., Pupilloa, L., and Kranz, J. J., eds. (2012) *Broadband Networks, Smart Grids and Climate Change*, Springer, http://books.google.cz/books?id=m5NqtXAoKPAC

New York City Mayor's Office (2014) "Mayor de Blasio, Commissioner Bratton, and District Attorney Vance Announce Major Initiative to Enhance NYPD Mobile Communications", press release, 23 October, http://www1.nyc.gov/office-of-the-mayor/news/490-14/mayor-de-blasio-commissioner-bratton-district-attorney-vance-major-initiative-to#/0

Oudot, J.-M. (2007) "Contracting issues in network industries", *Network Industries Quarterly,* Volume 9, Number 4, pages 3-4, http://newsletter.epfl.ch/mir/index.php?module=eplfiles&func= getFile&fid=65&inline=1

PA Consulting Group (2013) *LTE brings a new capability to mobility: how might it enable a range of cross-sector services?,* report for Ofcom UK, http://stakeholders.ofcom.org.uk/binaries/research/technology-research/2013/Ofcom_Future_LTE_Services_Study.pdf

Pasquali, F. (2011) "TETRA Success Stories", presented at the TETRA Congress USA, http://www.tandcca.com/Library/Documents/TETRA_Resources/Library/Presentations/FortWorth2011FrancescoPasquali.pdf

Paul, U., *et al.* (2011) "Understanding Traffic Dynamics in Cellular Data Networks", IEEE Infocom, http://www.wings.cs.sunysb.edu/~upaul/paper/Infocom11-final-version.pdf

Peltola, M. (2011) *Evolution of Public Safety and Security Mobile Networks,* licentiate thesis, Aalto University School of Electrical Engineering, Espoo, Finland, http://lib.tkk.fi/Lic/2011/urn100448.pdf

Projectgruppe Digitalfunk UAG Technik (1999) "Taktische-Betriebliche Anfordungen von Hubschraubern an ein digitales funknetz" [Tactical-operational requirements of helicopters on digital networks], http://www.pfa.nrw.de/PTI_Internet/pti-intern.dhpol.local/Funk/BOS_Lust-Boden-Anbindung/BOS_Luft-Boden-Anbindung.PDF

Projektgruppe Feuerwehr Dienstvorschriften des Ausschusses für Feuerwehrangelegenheiten, Katastrophenschutz und zivile Verteidigung (1999) *Feuerwehr-Dienstvorschrift 100: Führung und Leitung im Einsatz* [Fire Service Regulation 100: Leadership and management in practice], Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, http://www.idf.nrw.de/service/downloads/pdf/fwdv100.pdf

RSC (2013a) "Mandate to CEPT to develop harmonised technical conditions for the 694-790 MHz ('700 MHz') frequency band in the EU for the provision of wireless broadband and other uses in support of EU spectrum policy objectives", RSCOM12-37rev3, https://circabc.europa.eu/d/d/workspace/SpacesStore/6eda88bf-ed1a-4af4-bb26-9f985db5956d/20130312-125805_RSCOM12-37rev3_Mandate_CEPT_700_MHz%20FINAL%20doc.pdf

RSC (2013b) "Mandate to CEPT to study and identify harmonised compatibility and sharing conditions for Wireless Access Systems including Radio Local Area Networks in the bands 5350-5470 MHz and 5725-5925 MHz ('WAS/RLAN extension bands') for the provision of wireless broadband services", Working Document RSCOM13-32rev3 final, http://www.cept.org/Documents/se-24/14034/SE24-5GHzRLAN-Info02_EC-Mandate-on-5-GHz-RLANs

RSPG (2013a) "RSPG Opinion on Strategic Challenges Facing Europe in Addressing the Growing Spectrum Demand for Wireless Broadband", RSPG13-521 rev1, https://circabc.europa.eu/d/a/workspace/SpacesStore/c7597ba6-f00b-44e8-b54d-f6f5d069b097/RSPG13-521_RSPG%20Opinion_on_WBB.pdf

RSPG (2013b) "Report on Spectrum for Wireless Broadband and Broadcasting in the Frequency Range 400 MHz to 6 GHz", RSPG13-522, https://circabc.europa.eu/d/a/workspace/SpacesStore/6e0575cf-5244-4707-a811-c45b61b29377/RSPG13-522-Final_RSPG_Report_on_WBB.pdf

RSPG (2013c) "RSPG Report on Strategic Sectoral Spectrum Needs", RSPG13-540 (rev2), https://circabc.europa.eu/d/d/workspace/SpacesStore/f15d622c-183f-44d4-8412-19f2335a714d/RSPG13-540rev2_RSPG%20Report%20on%20Sectoral%20needs.pdf

Remley, K. A., *et al.* (2006) "Radio Communications for Emergency Responders in Large Public Buildings: Comparing Analog and Digital Modulation", *Proceedings of ISART*, pages 79-82, http://www.eeel.nist.gov/kate_papers/R9_ISART06_Remley_PFD1.pdf

Remley, C. A., *et al.* (2010) "NIST Measurements in the 750 MHz Band to Support Emergency Response Radio Communications", US National Institute of Standards & Technology, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=905183

Rocha, A. *et al.* (2013) "LTE 450 MHz technology for broadband services in rural and remote areas: Case study of Brazil", *ITU News,* No. 10, https://itunews.itu.int/en/4618-LTE-450MHz-technology-for-broadband-services-in-rural-and-remote-areas-BR-Case-study-of-Brazil.note.aspx

Rossi, F., *et al.* (2008) "Incorporating a New Technology into Agent-Artifact Space: The Case of Control System Automation in Europe", pages 289-310, in Lane, D., *et al.*, eds. (2009) Complexity Perspectives in Innovation and Social Change, Methodos Series (Volume 7), Springer, http://link.springer.com/chapter/10.1007%2F978-1-4020-9663-1_11

Rysavy, P. (2014) "Beyond LTE: Enabling the Mobile Broadband Explosion", Rysavy Research, http://www.4gamericas.org/documents/Beyond%20LTE_Enabling_Mobile%20Broadband%20Explosion_August_2014x.pdf

Scandella, F. (2012) *Firefighters: Feeling the Heat,* European Federation of Public Service Unions/European Trade Union Institute, http://www.etui.org/content/download/5386/53353/file/Guide_firefighters.pdf

Schengen Subgroup on Telecommunications (1997a) "Anforderungen an die Endgeräte und deren Bedienoberfläche in den zukünftigen digitalen Bündelfunksystemen der Schengener Staaten" [Requirements for terminals and their user interface in future digital trunk radio systems of the Schengen states], SCH/I-Telecom (96) 44, 5. rev, http://www.pfa.nrw.de/PTI_Internet/pti-intern.dhpol.local/Funk/Schengen-Endgeraete/Schengen-Endgeraete.PDF

Schengen Subgroup on Telecommunications (1997b) "Ergänzungen/Präzisierungen der Anforderungen an die Endgeräte und deren Bedienoberfläche in den zukünftigen digitalen Bündelfunksystemen der Schengener Staaten" [Additions/clarifications to the requirements for terminals and their user interface in future digital trunk radio systems of the Schengen states], http://www.pfa.nrw.de/PTI_Internet/pti-intern.dhpol.local/Funk/BOS_Ergaenzungen_zu_endegeraete1/BOS-Ergaenzungen_zu_Endgeraete1.PDF

Scholz, M. *et al.* (2013) "A Concept for Support of Firefighter Frontline Communication", *Future Internet,* Vol. 5, p. 113-127, http://www.mdpi.com/1999-5903/5/2/113/pdf

Schulman, P. R. & Roe, E. M. (2007) "Designing Infrastructures: Dilemmas of Design and the Reliability of Critical Infrastructures", *Journal of Contingencies and Crisis Management,* Volume 15, Number 1, pages 42-49.

Schipper, F. & van der Vleuten, E. (2008) "Trans-European network development and governance in historical perspective", *Network Industries Quarterly,* Volume 10, Number 3, pages 5-7, http://newsletter.epfl.ch/mir/index.php?module=epflfiles&func=getFile&fid=111&inline=1

Sharp, I. (2013) "Delivering Public Safety Communications with LTE", *3GPP News,* http://www.3gpp.org/news-events/3gpp-news/1455-Public-Safety

Smith, R. L. (2014) "Smart Grid Manifesto", *Transmission & Distribution World,* 17 March, http://tdworld.com/grid-opt-smart-grid/smart-grid-manifesto

Snow, A. P., *et al.* (2000) "Reliability and Survivability of Wireless and Mobile Networks", *IEEE Computer,* Volume 33, Issue 7, http://web.mit.edu/mgr/Public/to%20print/Snow%20-%202000%20-%20Reliability%20and%20Survivability%20of%20Wireless%20and%20Mobile%20Networks.pdf

Spring, G. (2013) "Global Public Safety - LTE: An Australian Perspective," PSCR Public Safety Broadband Stakeholder Conference, Westminster, Colorado, USA, http://www.pscr.gov/projects/broadband/700mhz_demo_net/meetings/stakeholder_mtg_062013/slides/day_3/Jun6-Spring-Global_PS_LTE.pdf

Steppler, M., et al. (2011) "Evolution of TETRA to a 4G All-IP Broadband Mission Critical Voice plus Data Professional Mobile Radio Technology", P3 Communications white paper, http://www.p3-group.com/downloads/4/1/7/5/P3_-_Evolution_of_TETRA_-_White_Paper_-_v1.0.pdf

Strabbing, W. (2012) "ESMIG answers on public consultation on the use of Spectrum for more efficient energy production and distribution", European Smart Metering Industry Group, https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/PC_energy_efficiency.zip

Telecom Regulatory Authority of India (2012) "Telecom network failures during Emergencies/Disasters – Priority routing of calls of persons engaged in 'response and recovery'", Consultation Paper No. 11/2012, http://www.trai.gov.in/WriteReaddata/ConsultationPaper/Document/consultationpaper10052012.pdf

TCCA (2013a) "The Strategic Case for Mission Critical Mobile Broadband: A review of the future needs of the users of critical communications", http://www.tandcca.com/Library/Documents/Broadband/MCMBB%20Strategic%20Case%20v1_0.pdf

TCCA (2013b) "Future Broadband Spectrum needs for PPDR: Communiqué from Roundtable discussion, 23rd May 2013", http://www.tandcca.com/Library/Documents/Broadband/PPDR%20Spectrum%20Communique%20-%20Roundtable%20 may2013.pdf

Thomas, M. (2014) "Ready when needed: technical conditions for mobile broadband at 700 MHz band", *ECC Newsletter*, October issue, pages 4-7, http://apps.ero.dk/eccnews/oct-2014/ready-when-needed.html

UK Office of Communication (2011) "Wholesale mobile voice call termination - Modelling Annexes (Non Confidential version), http://stakeholders.ofcom.org.uk/binaries/consultations/mtr/statement/MCT_statement_Annex_6-10.pdf

Urban ITS Expert Group (2013) "Guidelines for ITS Deployment in Urban Areas", European Commission ITS Action Plan, http://ec.europa.eu/transport/themes/its/road/action_plan/doc/2013-urban-its-expert_group-guidelines-on-traffic-management.pdf

Ure, J. (2013) *Public Protection and Disaster Relief (PPDR) Services and Broadband in Asia and the Pacific: A Study of Value and Opportunity Cost in the Assignment of Radio Spectrum,* University of Hong Kong, http://trpc.biz/wp-content/uploads/PPDR-_Report_16-May-2013_FINAL-2.pdf

US Fire Administration (2008) "Voice Radio Communications Guide for the Fire Service", Federal Emergency Management Agency, http://www.usfa.fema.gov/downloads/pdf/publications/Voice_ Radio_Communications_Guide_for_the_Fire_Service.pdf

[US] National Public Safety Telecommunications Council (2013) "Why Can't Public Safety Just Use Cell Phones and Smart Phones for Their Mission Critical Voice Communications?", Tech Brief, US Department of Homeland Security, http://www.npstc.org/download.jsp?

tableId=37&column=217&id=2712&file=Why_Cant_PS_Just_Use_Cell_Phones_NPSTC_130415.pdf

[US] National Public Safety Telecommunications Council (2011) "The Need for a Nationwide Broadband Concept for Public Safety", US Department of Homeland Security, http://www.npstc.org/download.jsp?tableId=37&column=217&id=1047&file=NPSTC%20Position%20BB%20Network%2020110310.pdf

[US] NPSTC Broadband Working Group (2011) "Mission Critical Voice Communications Requirements for Public Safety", http://www.npstc.org/download.jsp?tableId=37&column=217&id=2024&file=Functional%20Description%20MCV%20083011%20FINAL.pdf

[US] NPSTC Broadband Working Group (2013) "Functional Description of Mission Critical Voice", version 5, US Department of Homeland Security, http://www.npstc.org/.../Functional%20Description%20MCV%20v5.doc

Varone, J. C. (1996) "Fireground Radio Communications and Firefighter Safety", US National Fire Academy, http://www.usfa.fema.gov/downloads/pdf/tr_96cv.pdf

Vasilca, I.-S. (2012) "The STS National Network", EU Emergency Services Workshop, http://www.eena.org/ressource/static/files/_sts-national-network.pps

Vratonjić, M. (2013) "The Future of Public Safety Radio Communications", Motorola, http://www.eena.org/ressource/static/files/futureofpmr.pdf

Vujičić, B. (2006) "Modeling and Characterization of Traffic in a Public Safety Wireless Network", masters thesis, Simon Fraser University, http://www.ensc.sfu.ca/~ljilja/cnl/pdf/bozidar_thesis.pdf

Walicki, S., & Brenner, R., (2013) "Mission Critical Network Design & Implementation: The Past, the Present & Recommendations for the Future of Interior Communications Data Networks in the Fleet", NSWCCD-SSES Code 965, US Navy, May, https://www.navalengineers.org/ProceedingsDocs/IntelligentShips/ISSX/A3_Walicki_Paper.pdf

Waters, C., ed. (2014) "Signalling Supplement", *European Railway Review,* issue 1-2014, http://www.europeanrailwayreview.com/digital/signalling-supplement-2014/

Welte, T. (2011) "Applied Research on Security of TETRA Radio", Chaos Computer Club Camp, http://media.ccc.de/browse/conferences/camp2011/cccamp11-4496-applied_research_on_security_of_tetra_radio.html

WiMAX Forum (2013) "Requirements and Recommendations for WiMAX as Public Safety (PS) and Public Protection & Disaster Relief (PPDR)", WMF-T31-134-R022v01, http://resources.wimaxforum.org/sites/wimaxforum.org/files/technical_document/2014/02/WMF-T31-134-R022v01-SPWG.pdf

Appendix A. Public Protection & Disaster Relief (PPDR)

A.1 Voice communication

First responders generally work in teams. Team membership extends into communication as a "talk group" that shares radio channels to update all group members simultaneously, providing a common platform for discussion, questions, assignments, warnings, etc. The ability to define and redefine talk groups quickly is essential for effective teamwork. Thus it is a first requirement for first responders.

Talk group communications are monitored by an on-site incident manager and often, too, by a control centre which may be some distance away (the control centre may also record or log the conversation). "Push-to-talk" (PTT) is the ability to address a particular individual or group at the press of a single button. This is a time-saving tool first responders rely on in urgent situations. A related tool is "emergency alert" – essentially an alarm button with overriding priority which indicates that a member of the group is in peril and needs to communicate immediately.

Talk groups are usually geographically compact. So it is desirable for team members to be able to communicate with each other, handset to handset, even if there is no base station to relay the signals. This is called Direct Mode Operation (DMO) or Proximity Service (ProSe). Similarly, it is desirable for a handset to be able to relay communications from a nearby handset to a base station or to additional handsets, forming an ad hoc mesh.

Commercial cellular networks today are not set up for talk groups, all-calls, direct mode or handset meshes, though they can support push-to-talk somewhat if user handsets have that function. However, adding functionalities to LTE like those just mentioned, which are needed by public safety professionals, is a priority now for the 3rd Generation Partnership Project (3GPP) and ETSI. It will take a few years for the standards to be developed and a few more years for the new standards to be implemented in hardware. This process is discussed in detail in **Section 3.2.1**. But note that TETRA, TETRAPOL, DMR, P25, MPT-1327 and other professional mobile radio systems already have these functionalities. However, they lack support for broadband which is LTE's strength.

A.2 Data communication

Wireless bandwidth requirements for many specific PPDR communication activities, current and anticipated, are estimated in Table A.1.

But given the already extensive use of data applications and the limited bandwidth for data in TETRA and TETRAPOL networks, it may not be surprising that PPDR professionals today use commercial public networks to send and receive data (and occasionally for voice communication) even though such networks are often described as unsuitable for "mission critical" information. Eleven respondents to the CEPT questionnaire mentioned in Section 2.2.1 reported using such networks professionally. In our interviews we found Blackberries especially popular.[113] For those who believe public subscriber networks and equipment are too insecure for mission critical PPDR consider that:

---

[113] Jowett, T. (2010) "Police save £112m a year using BlackBerrys", *TechWeek Europe,* 7 October - http://www.techweekeurope.co.uk/news/rim-touts-significant-police-costs-savings-with-blackberry-platform-10449.

- RIM's encryption is approved for the sending of sensitive information by the UK's Communications-Electronics Security Group. Nokia smartphones with the S60 interface are similarly approved.[114]
- The German government awarded RIM a major contract in 2013 to provide secure mobile communications within the federal agencies.[115]
- Samsung "Knox" devices (including the Galaxy S4) are approved for use on US Defense Department networks.[116]

Table A.1. Representative sample of data rates needed to support non-voice PPDR applications

Non-voice Applications	2005 Voice % impact	kbytes	kbits	Transfer time (seconds)	kbit/s (Net)	Application group
Location Services	-2 %	0,1	0,8	1	0,8	Real time short data
Telemetry (real time transfer)	0 %	0,2	1,6	0,5	3,2	Real time short data
Operation and control	0 %	0,2	1,6	0,5	3,2	Real time short data
Biodynamic vital data sampling, inc. ECG	0 %	5	40	10	4	Real time short data
Telemetry (Real time - 5 kbytes)	0 %	5	40	10	4	Real time short data
WAP/on-line forms	0 %	3	24	5	4,8	Database Interaction
People & Vehicles status/location/messaging (1 kbyte)	-2 %	1	8	1	8	Real time short data
Data tasking e.g. command and control/work management	-5 %	5	40	5	8	Database Interaction
Fingerprint data abstracted from the fingerprint image	0 %	10	80	10	8	File transfer
Content Push (10 kbytes)	1 %	10	80	4	20	File Transfer
Interagency Communications inc. Intranet (10 kbytes)	0 %	10	80	4	20	File Transfer/Office Application
Database inquiries 10 kbytes to 100 kbytes	0 %	12.5	100	5	20	Database Interaction
Mobile computing - office applications	0 %	12.5	100	5	20	Office Application
Connect to hospitals and national health comm. network	0 %	100	800	20	40	File Transfer
Connect to hospitals and national health comm. network	1 %	50	400	10	40	Office Application
Internet incl. web browsing 10 kbytes to 50 kbytes (per page)	0 %	50	400	10	40	Office Application
Video streaming (surveillance)	0 %			delay a few seconds	50	Video Transfer
Graphics, maps, location 100 kbytes to 1 Mbyte	-1 %	125	1 000	20	50	Image Transfer
e-mails incl. Attachments 2 Mbytes	0 %	2 000	16 000	300	53	File Transfer
Video Conferencing 64 kbit/s	0 %				64	Video Transfer
Image transfer (image JPEG ± 50 kbytes)	0 %	100	800	10	80	Image Transfer
Fingerprint image	0 %	100	800	10	80	Image Transfer,
Video clips 1 Mbyte to 2 Mbytes	0 %	2 000	16 000	32	500	Video Transfer

Source: ETSI TR 102 491 V1.1.1 (2005), page 18

114 For a list of nonmilitary wireless equipment approved for secure communication in the UK, see the GCHQ's Commercial Products Assurance Results webpage, http://www.cesg.gov.uk/finda/Pages/CAPSResults.aspx.

115 Rosenbach, M., Poitras, L. and Stark, H. (2013) "iSpy: How the NSA accesses smartphone data", *Der Spiegel,* 9 September, http://www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html

116 Samsung (2013) "Samsung Knox approved by Department of Defense for use in US Government", 6 May press release, https://www.samsung.com/sg/news/localnews/2013/samsung-knox-approved-by-department-of-defense-for-use-in-us-government

A.3 Police services

So far PPDR has been discussed as if communications were the same in all the specialised services (police, fire, emergency medical, mountain rescue, etc.). There are commonalities, but there are also differences which affect the use of spectrum and the need for specific features including DMO and broadband. Such differences will now be explored.

According to Eurostat, in 2012 there were 1 726 142 police officers in the EU Member States. 27 521 991 incidents of crime were reported, including 2 173 470 violent crimes (physical assaults, robberies, rapes, homocides, etc.; see **Table A.2**.[120] On average then each officer files a crime report every few weeks but less than 8% involve a threat to human life. Aside from minor traffic violations, the vast majority of crimes committed in Europe concern physical property and are reported after the perpetrator left the scene so the police response is not so urgent. If "mission critical" is defined in terms of urgency or imminent risk to human life then only a small percentage of police communications is "mission critical". However, situations can shift unexpectedly from routine to life-threatening. Therefore, immediate access to channels for mission critical communication should always be available to police officers outside the station and it should be their decision when to use such channels.

Unlike other first responders, a policeman's time is often spent on patrol or on duty in public places – to be visible as a deterrent to crime, but also to watch for traffic violations, suspicious behaviours, unapprehended suspects, etc. Patrols imply mobility and mobility needs radio to maintain command-and-control links and "situational awareness" for timely and appropriate responses. Voice is the preferred mode for such communications.

Table A.2: Numbers of police officers & reported crimes per year per country

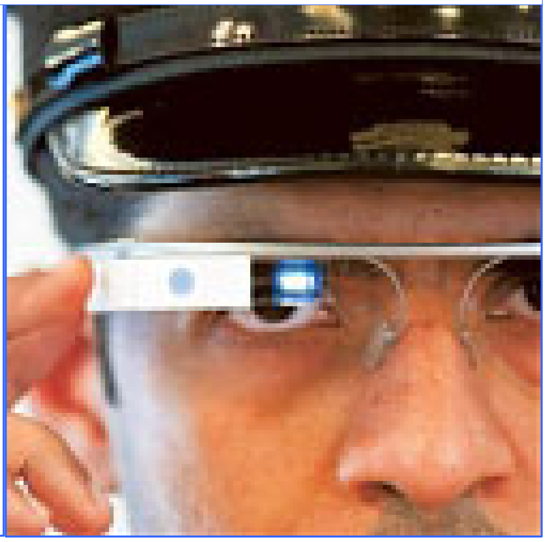
Country	Police officers	Incidents of reported crime/year
Austria	27 767	548 027
Belgium	46 784	1 073 773
Bulgaria	28 167	120 558
Croatia	21 339	72 171
Cyprus	5 263	7 973
Czech Rep.	38 291	304 528
Denmark	10 758	440 772
Estonia	4 424	40 816
Finland	8 037	425 421
France[117]	203 982	3 521 256
Germany	243 982	5 997 040
Greece	54 657	194 144
Hungary	36 503	472 236
Ireland[118]	13 424	103 178
Italy	276 750	2 818 834
Latvia	6 482	49 905
Lithuania	9 530	75 349
Luxembourg	1 736	37 639
Malta	1 902	15 623
Netherlands	39 735	1 139 720
Norway	7 941	273 541
Poland	96 322	1 119 803
Portugal	46 083	403 200
Romania	53 132	308 468
Slovakia	24 230	90 351
Slovenia	7 371	91 430
Spain	249 907	2 268 867
Sweden	19 890	1 402 588
UK	149 694	4 104 780

Source: Eurostat, 2014: "Table 1: Crimes reported by the police" and "Table 8: Number of police officers"[119]

[117] The number of reported crimes in France is from 2009 (the most recent data available).
[118] The number of reported crimes in Ireland is from 2006 (the most recent data available).
[119] http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Crime_trends_in_detail
[120] We take these statistics at face value even though experts who work with them warn that "police data actually describes more the recording practices of the officials than the amount of crime…" See "European Statistics", a special issue of the *European Journal on Criminal Policy and Research,* Vol 18, No 1 (March 2012), http://link.springer.com/journal/10610/18/1/

Figure A.1 (left) Policeman wearing a video camera (source: NBC News)

Figure A.2 (right) Policeman wearing Google Glass (source: TrendBird.biz)



A.4 Police video

Video, on the other hand, is the main driver of police demand for mobile broadband. Since wireless bandwidth is not yet available for video streaming on a large scale in Europe, only glimpses of its potential impact can be found in police uses of recorded video. But the experience of early adopters has been positive:

> The overwhelming majority of officers having used in-car camera systems do not wish to patrol without them… about one third of officers perceived a feeling of increased safety when the camera was in use… Many officers also reported having used the presence of the camera to de-escalate situations that they felt were becoming confrontational by informing citizens that they were being recorded… nearly half (48%) reported that citizens have become less aggressive after learning the event was being recorded…
>
> When community members were asked if they support the police's use of in-car cameras, 94% stated that they do support it and approve the use of the camera. However, 71% suggested that they should be informed when they are being videotaped… The public recognizes that the camera systems not only help prevent the abuse of authority, but they also serve as a valuable tool to ensure the integrity of an agency. (Nichols *et al*., 2004)

In-car video is more prevalent in the US than in Europe, perhaps because foot patrols are rarer there and random violence is a bigger problem. On the other hand, police "spy-cars" do not seem to have as much public support on this side of the Atlantic; their use has been banned in some contexts.[121]

It is not clear yet what the public response to body-worn video cameras will be but they may be recognised as helping to prevent abuses, as the quote above indicates. The first controlled experiment based on an actual deployment (in California) found that over the course of a year, police-worn video cameras led to a 50+ percent reduction in incidents where force was used and a 90 percent drop in citizen complaints (Farrar, 2013). If discreet cameras or something like Google Glass become standard equipment, the public may simply assume police are always relaying or recording what they see, giving both sides in an encounter reasons to behave carefully.

[121] Payne, T. (2014) "'Greedy' councils banned from using 'spy-cars' that issued £300m in parking fines", *The Independent,* 21 June, http://www.independent.co.uk/news/uk/greedy-councils-banned-from-using-spycars-that-issued-300-million-in-parking-fines-9553625.html

Non-mobile police video systems have become common in Europe although their contributions to deterrence and convictions are still uncertain, with large differences from one jurisdiction to another in both public acceptance and measurable impact (Webster, 2012). In any case it is unlikely that cellular network operators will ever gain a significant share of the backhaul market for fixed video surveillance so we consider that application only in the context of the transport sector.

Video captures details difficult to describe in words and it can present those details more credibly than a personal synopsis or later recollection. Thus it can supply compelling evidence for what happened when or who said or did what to whom. But EU Member States differ widely in their acceptance of evidence recorded and transmitted electronically. Audio or video testimony (remote hearings of witnesses and victims, for example) is accepted for some types of crime but the admissibility of other electronic evidence (video captured on location, communication intercepts, etc.) is limited. Differences in the way Member States set these limits can create problems in cross-border cases. One interviewee noted that there seems to be no trend toward greater acceptance of video as evidence in criminal trials.[122] This gap between the growing embrace of video by police and the apparent caution of courts deserves closer examination.

The ability to stream video wirelessly in real-time may be limited in Europe but in 2012, 46% of local police agencies in the US reported that they have this capability. How they use it suggests how it might be used in Europe:

> Twenty-six percent said they use it for investigative purposes; 23 percent use it during traffic stops; 21 percent use video to help ensure officer safety; 19 percent use it in responding to calls for service; 16 percent use it to provide officer accountability. (A given agency could cite multiple purposes for video transmissions.) In addition, 11 percent cited other uses of wireless video streaming, such as video cameras contained in [mobile robots] used in bombing, barricade, or hostage situations; monitoring of remotely located critical infrastructure, such as water supply facilities; video streaming to monitor crowds during major events; and video feeds from helicopters during pursuits.
>
> Twenty-three percent of responding agencies said they stream video from fixed surveillance cameras to police vehicles – for example, to give responding officers information about what to expect as they are traveling to a crime scene. Most agencies said they plan to increase this capability, and on average, they expect that in five years, 81 percent of their vehicles will have this capability (McGinty, 2012).

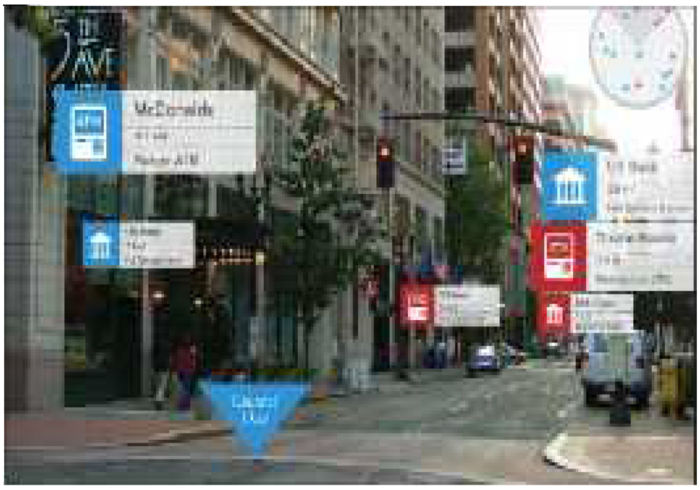


Figure A.3 Augmented Reality application from Germany

Screen-shot of dashboard monitor in T-Systems' prototype patrol car for the Brandenburg Police, showing live video overlaid with information labels identifying "points of interest" in the scene. (Source: Klauth, 2013)

Real-time video processing is already producing valuable – though sometimes controversial – new tools for police work. Europe is the largest regional market for automatic licence number readers

[122] Forge, S. (2014), telephone interview with Oliver Tell, DG Justice, 24 June 2014.

(Global Industry Analysts Inc., 2013). These facilitate searches for stolen vehicles and the ticketing of traffic code violaters. They can also be used to track the movements of specific cars. Automatic face recognition is another rapidly developing field. Installed at many airports and rumoured to be used to identify vandals in public protests, such applications require fast access to large databases of images, as would be enabled by additional spectrum for public safety broadband.

The interaction between live video and stored data also supports Augmented Reality (AR) applications, as demonstrated in the new patrol car T-Systems is developing for the Brandenburg police in Germany. A monitor built into the dashboard can display street views captured by cameras mounted on the vehicle, with "points of interest" labelled to describe places in the scene (Klauth, 2013). Numerous applications of AR for police work have been suggested because they accelerate and improve decision-making in "any situation requiring information that is not directly available or detectable by human senses" (Cowper and Buerger, 2003).

A.5 Other police data requirements

ECC Report 199 (2013)[123] provides an estimate of the cumulative data bandwidth needs for routine (non-emergency) police operations. The differences between "low" and "medium" estimates in the table below result from different assumptions about spectrum efficiency for real-time video transmissions at the edge of a cell and not to different assumptions about the amount of data transmitted:

Table A.2. Police data bandwidth requirement in routine (non-emergency) situations:

Frequency band	Traffic assumption	Low estimate	Medium estimate
420 MHz	1 incident near cell edge, 3 incidents near cell centre & background communications	8.0 MHz uplink 7.6 MHz downlink	12.5 MHz uplink 10.5 MHz downlink
750 MHz	1 incident near cell edge, 2 incidents near cell centre & background communications	7.1 MHz uplink 6.9 MHz downlink	10.7 MHz uplink 9.0 MHz downlink

Table A.3. Police data bandwidth requirement in extreme cases:

Frequency band	Traffic assumption	Less stringent case	Worst case
Independent of frequency band	Royal Wedding traffic scenario with background communications	10.3 MHz uplink	14.3 MHz uplink
Independent of frequency band	London riots traffic scenario with background communications	5.8 MHz uplink	7.8 MHz uplink

A significant amount of paperwork is generated by crime cases, consuming perhaps 20% of a policeman's time. To the extent that this paperwork must be completed at the station, officers are not available for other duties. So all police departments have an interest in reducing the time spent on

[123] "User requirements and spectrum needs for future European broadband PPDR systems (Wide Area Networks)", CEPT, http://www.erodocdb.dk/Docs/doc98/official/Word/ECCREP199.DOCX

paperwork or enabling it to be done outside the station. Many projects are underway now in the Member States to digitise criminal justice records, replacing paper with electronic forms which can be filed offsite and processed automatically. The UK's Policing and Criminal Justice Minister, for instance, wants a "largely paperless" police force by 2016, claiming that portable electronic devices will save up to 4.5 million hours of officers' time each year and cut patrol car mileage 20% by eliminating trips back to base to complete paperwork (Loeb, 2014). Filing documents electronically does not require broadband but broadband does make the process faster.

A.6 Examples of current police radio equipment

Figure A.4. Swedish police car with RAKEL (TETRA) transceiver above a still-used older radio system's transceiver and a digital video monitor

Source: *Wikipedia*

When cellular was first introduced the equipment was so large that it had to be mounted in vehicles. Today hardly any cellular terminals are made for installation in vehicles. However, public demand for "connected cars" might change that, which would benefit PPDR if they also migrate to cellular. PPDR relies on vehicle-mounted radios as much as on handhelds.

Pictured at right is a police flashlight with built-in wireless video camera. Along with body-worn and car-mounted cameras, it is a reminder of how much video already permeates policework.

A.7 Fire services

Table A.4: Number of Firefighters & fires per year per country (2006-2010)

Country	Firefighters	Stations	Fires
Austria	262 431	4 856	34 775
Belgium	17 749	252	27 095
Bulgaria	8 223	175	32 125
Croatia	60 563	1 923	7 025
Cyprus	966	31	6 344
Czech Rep.	85 842	7 925	20 004
Denmark	8 000	306	18 355
Estonia	2 531	160	9 866
Finland	15 920	1 046	15 555
France	237 609	7 277	336 433
Germany	1 080 655	37 717	190 190
Greece	16 624	775	34 783
Hungary	21 073	112	22 063
Ireland	3 547	222	34 505
Italy	33 000	103	223 570
Latvia	2 986	92	10 872
Lithuania	2 428	84	17 209
Netherlands	26 851	1 034	47 327
Norway	12 017	831	12 750
Poland	475 172	16 920	154 569
Portugal	49 100	473	37 758
Romania	140 324	291	15 833
Slovakia	40 070	115	11 605
Slovenia	96 563	1 311	5 128
Spain	23 323		115 267
Sweden	15 919	1 016	28 824
UK	60 500	2 053	358 249

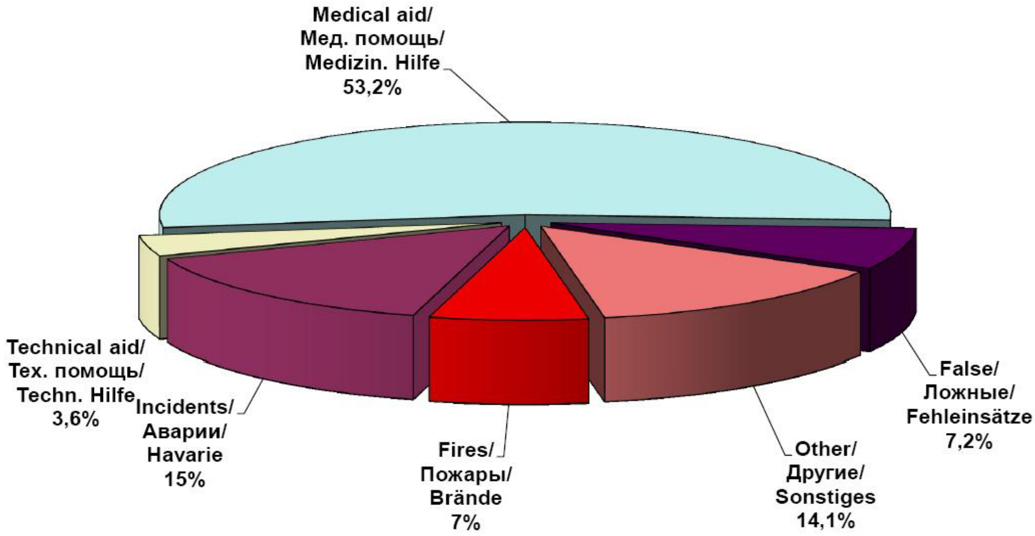
Source: Brushlinsky *et al.*, 2012

Note: The numbers of firefighters and fire stations are averaged over the period 2001 to 2010. The "Fires" column shows the average number of fire incidents per country per year from 2006 to 2010.

The EU Member States have about 2.8 million firefighters (Brushlinsky *et al.,* 2012). The work they do and the time devoted to each task vary from place to place and seasonally. But putting out fires generally takes less of a fireman's time than activities like providing emergency medical assistance, fire prevention, training drills, investigating the causes of fires, animal rescues, responding to road accidents, etc. According to the 2012 edition of *World Fire Statistics*, just 7% of the calls for help to fire services are about fires. Especially in rural areas, the largest fraction of calls to fire brigades is for medical assistance.

"Fire services are increasingly being merged with emergency, civil defence or disaster management services and are taking on a wider range of tasks and responsibilities" (Lethbridge, 2013). In most European countries the number of reported fires is slowly declining, as are property losses and casualty rates, thanks to the wide deployment of smoke detectors and the success of other prevention measures. However, the growing use of synthetic materials enables indoor fires to produce more toxic smoke and fumes than in the past. So when a building fire does start, rapid suppression is vital.

Figure A.5. What calls to fire services are about (globally)



***Source*: Brushlinsky *et al.*, 2012**

The dispatching of personnel and equipment to a fire must be as fast as possible. Navigating through heavy traffic or finding the best route to an unfamiliar location often requires control room guidance. Vehicle location awareness is thus crucial and at the fire-site, localisation services are needed to pinpoint all personnel and, if possible, show the building layout and safe exit/escape paths. The risks of getting lost in a smoke-filled interior are all too frequently encountered. Research is underway to reduce or eliminate the need for humans to enter burning buildings.

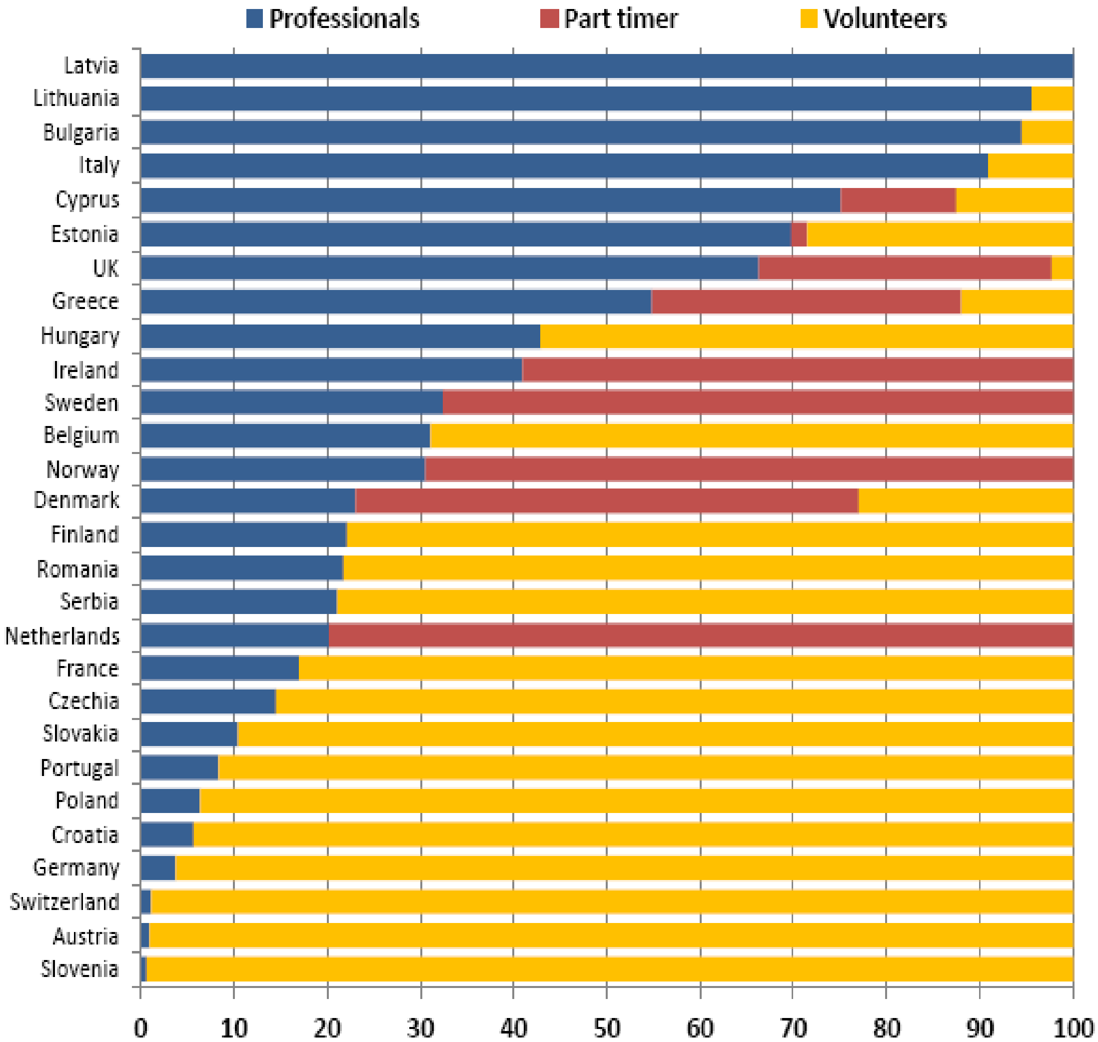
European states vary in the ratio of paid professionals to volunteers and seasonal to year-round firefighters. The data is summarised in Figure A.6. Austria, Slovenia and Germany rely to a great extent on volunteers, in contrast to Latvia, Lithuania, Bulgaria and Italy, which have few or no volunteers. In general, the states with large numbers of firefighters have so many because most are part-time volunteers. This requires the use of a wide-area, low-bandwidth radio system (paging or SMS) for call-up.

The budgets of volunteer and part-time fire brigades are often too small to cover the cost of TETRA subscriptions and equipment for everyone. Consequently, many of the brigades keep older radio systems in service longer than their urban counterparts or have “bring your own device” policies. Urban and rural areas differ, too, in the frequency of various fire types. Different tactics – and thus different communication processes – are needed to put out a forest fire than a fire in a high-rise building or an automobile.

A.8 Firefighter Voice Communications

When units are dispatched it is common practice to assign them two radio channels: one, the “command” channel, is for communication between the IC and the dispatch centre; the other, a “tactical” channel, is for communication within the fire-site. If spectrum is available, additional tactical channels can be assigned for complex operations or if voice traffic exceeds the capacity of a single channel. But it is challenging to follow transmissions from several channels simultaneously. Recordings of voice exchanges during fire fights which ended badly often show that some at the scene missed essential information because they were monitoring a different channel. A single tactical channel with strict communication discipline is the best way to ensure that critical messages are heard even if more frequencies are available.

Figure A.6. Percentage of professional, part-time and volunteer firefighters as percentages of the total fire workforce

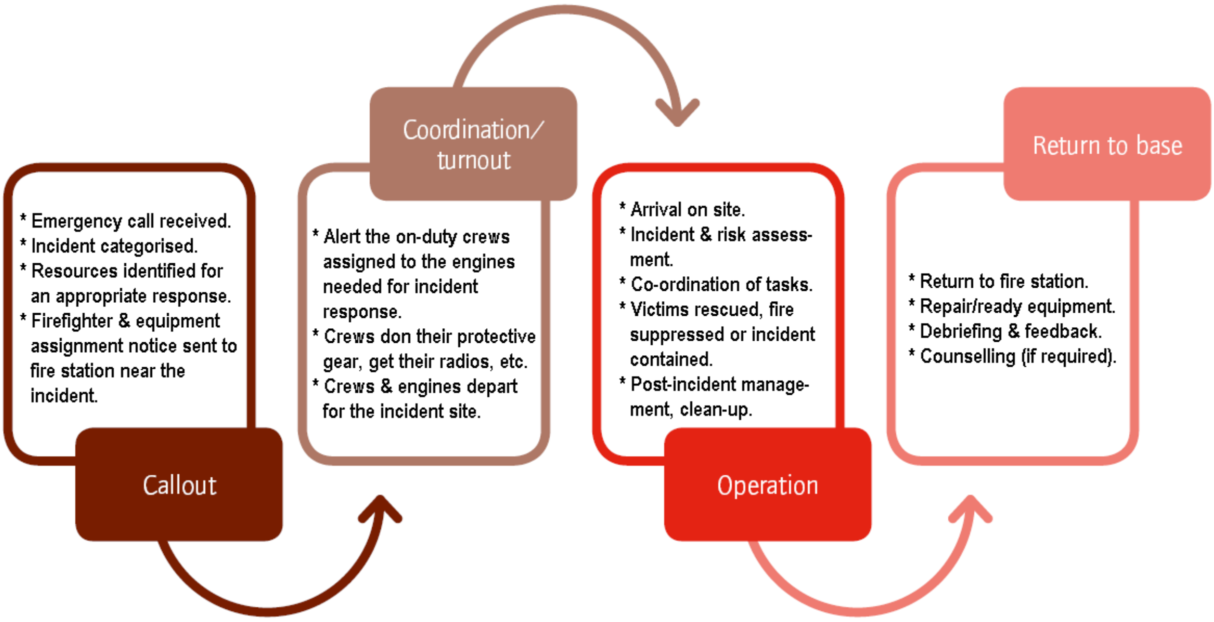


Source: Adapted from Scandella, 2012

If more than one fire unit arrives at an incident, an on scene command structure is set up and led by the Incident Commander (IC), who becomes the focal point of communications. The IC manages the dispatched resources, coordinates the fire attack, oversees the firefighters' safety and provides accountability. The dispatcher plays a supporting role, monitoring and logging fireground events, processing requests for more resources and possibly recording the fireground's radio traffic.

Despite all the diversity in tactical fire communications, there is an underlying pattern, a chain of events with four essential links:

Figure A.7. Four essential communication stages in fire incidents



***Source*: Adapted from Scandella, 2012**

A.9 Examples of current fire radio equipment

Figure A.8. Motorola handsets for firefighters

Introduced in 2010, Motorola's APX7000 series of handheld radios was designed specifically for firefighters. The thick rubberised shell is certified IEC IP67 resistant to dust and water. Flourescent colouring makes the radio easier to see in smoky environments. Extra-large knobs can be recognised by touch alone and gripped while wearing thick gloves – even though they also have extra-stiff rotation and position clicks so they cannot be turned accidentally. Large red alarm buttons are at the base of the antenna. Long whip antennas support lower radio frequencies and capture weaker signals. Microphones with extra noise supression are on both front and back so the handset can be used in either position.

Figure A.9 "Intrinsically safe" TETRA handsets

"Intrinsically safe" TETRA handsets, which meet ATEX standards for use in explosive atmospheres, are produced by Sepura, Funkwerk and Cassidian. They may look like other portables but their innards are tested and certified by specialist laboratories, having been designed to prevent sparking and avoid heat concentrations on the circuit boards. Pictured at left are the Funkwerk FT4 Ex, Cassidian THR9 Ex and Sepura STP8 X.

Figure A.10. Crisis mitigation robot

The Croatian company Dok-Ing has developed a fire-fighting and "crisis mitigation" robot for environments too hazardous for humans (industrial chemical plants, ammunition dumps, nuclear reactors, etc.). Remotely controlled by radio from up to 1500m away, the MVF-5 has six waterproof video cameras (one of them infrared), as well as sensors for heat, oxygen, explosive gases and location. Onboard reservoirs hold 2000 liters of water and 500 liters of foam, or water and foam can be pumped from external sources. A hydraulic claw/cutter mounted ahead of the bulldozer blade can cut through obstacles or lift up to 2 tonnes for path clearance.

A.10 Emergency Medical Services

EMS work closely with other first responders, particularly fire brigades, offering urgent on-site care to unwell or injured citizens and, if necessary, transport to treatment centres. Specially equipped road vehicles (ambulances or medivans) usually deliver EMS teams but on rare occasions helicopters may be used (e.g. to deliver organs for transplants, to reach victims not accessible by road, or to carry patients whose lives are in such immediate danger that ground transport is too slow).

EMS dispatchers must quickly evaluate the urgency of a reported condition, give the caller useful short-term advice (what to do before the medical team arrives) and send the right resources to the right location. Accurate dispatch is essential in major trauma cases – strokes, seizures, cardiac arrest, upper airway obstructions – as patient survival depends on the speed of the EMS response. Fortunately, such cases are relatively rare: "of the 1350 calls received every day by London Ambulance Service only two or three relate to trauma patients” (Adnet *et al.,* 2011). Country-level data about the numbers and percentages of urgent or life-threatening cases encountered by ambulance crews is in **Table A.5**.

Non-urgent calls thus represent a large part of the EMS workload – up to 40% by most counts – and these can interfere with responses to real emergencies. Some national systems now have physicians or nurses working in dispatch centres to help call takers distinguish cases which are urgent from those which are not. Several countries are introducing non-emergency telephone numbers to offload calls for less urgent medical assistance (Lyon, 2013).

In many countries the staffing and structure of EMS missions correspond to the dispatcher’s assessment of how life-threatening a reported situation is. Adnet *et al.* (2011) describe the emerging norm in Europe as a “two-level rescue system with a medicalised second level”.

Table A.5. Numbers of EMS personnel & incidents (2008)

Country	EMS workers (2008)	Dispatch Centers (2008)	Incidents (2008)
Austria	~2 500 ambulances with ~59 000 personnel (including 50 000 volunteers).	52	~170 000 life-threatening emergencies per year; ~450 000 non-life-threatening emergencies; 2.2 million transports of immobile patients and 800,000 transports of mobile patient per year.
Bulgaria	1 025 ambulances (including 350 spares) 6587 EMS personnel plus administrative support.	28	Call centres received 866 678 calls in 2007.
Estonia	90 ambulances, 1 336 EMS personnel.	1	~250,000 EMS dispatches per year, of which 70% were not urgent.
Finland	~800 ambulances, about 2 000 EMS personnel in private ambulance services; unknown how many work in municipal services (a few hundred?).	15	About 500 000 – 600 000 EMS dispatches per year plus 800 000 – 1 000 000 patient transports per year.
Lithuania	256 ambulances, 2 350 ambulance personnel.	56	729 698 people received “ambulance care services” in 2007
Netherlands	670 ambulances with about 4 400 ambulance personnel.	25	About 1 million dispatched responses per year, including 400 000 life-threatening or urgent situations and 200 000 urgent but not life-threatening situations. The rest were planned patient transports.
Poland	1 411 ambulances with about 23 000 ambulance personnel.	290	
UK	There were 1721 ambulances in 11 “ambulance trusts” in 2007 (no data for the other 8 “ambulance trusts” or for private ambulance services); 17 028 personnel work in the 11 ambulance trusts.	33	In England, 5.9 million dispatched responses to scene of an incident; of these about 450 000 were emergencies, 500 000 were non-urgent or patient transport requests.

Source: Ambulancezorg Nederland, 2010

The first level is undertaken by ambulances and/or fire vehicles delivering emergency medical technicians trained in basic first aid and authorised to practice cardiac life support and resuscitation. If the initial call for help suggests a life-threatening emergency, a second-level response can be dispatched simultaneously, including a physician and possibly a nurse, anesthesiologist or other appropriate specialist. The trend in EMS is toward more advanced on-site treatment rather than faster pickup and delivery to a hospital.

Radio communication between the dispatcher and the responder begins on route to the scene, for directional guidance, to share new information about the patient's condition or medical background, etc. Once on scene, the responders can use their radio link to the dispatcher to consult with an off site physician via phonepatch. Data from biomedical sensors deployed in the field (portable ultrasound, electrocardiograms, etc.) can be transmitted for expert evaluation. But because most EMS radio systems are still voice oriented, the paramedic may have to verbally summarise the output of a monitoring device. This is an unsatisfactory situation which can lead to the use of 3G cellular networks (if in range) to send pictures, charts and data. Accuracy of diagnosis can depend on the clarity of a transmitted image so there is real value in high resolution pictures (Strode, 2003).

It is unusual for EMS personnel to find their lives threatened when they answer a call for help; police and firefighters are more often at risk. So the justification for secure channels in EMS is to protect patient privacy rather than the responders or their missions. Another difference is that on site radio communication among EMS responders is often unnecessary as they tend to remain in close enough proximity for acoustic communication – unless the incident covers a large area.

Another very important difference is economic. Except for private guards, all police departments are publicly funded government agencies. EMS, on the other hand, has degrees of privatisation and volunteerism that vary from country to country and from place to place. Some ambulance services are private firms which charge patients a fee for transport. Others are businesses whose clients are insurance companies, public health funds or government bureaux. Some have monopoly concessions, others have won short-term procurement contracts. Some are run by giant transnationals like the Red Cross (in Germany, for example). Others are run by volunteer fire brigades. EMS views on commercial cellular networks as suppliers of mobile connectivity are likely to depend on self-perceptions of bargaining power, the cost of the offered services and whether costs can be passed on to sponsors, customers or public budgets. These are all highly variable.

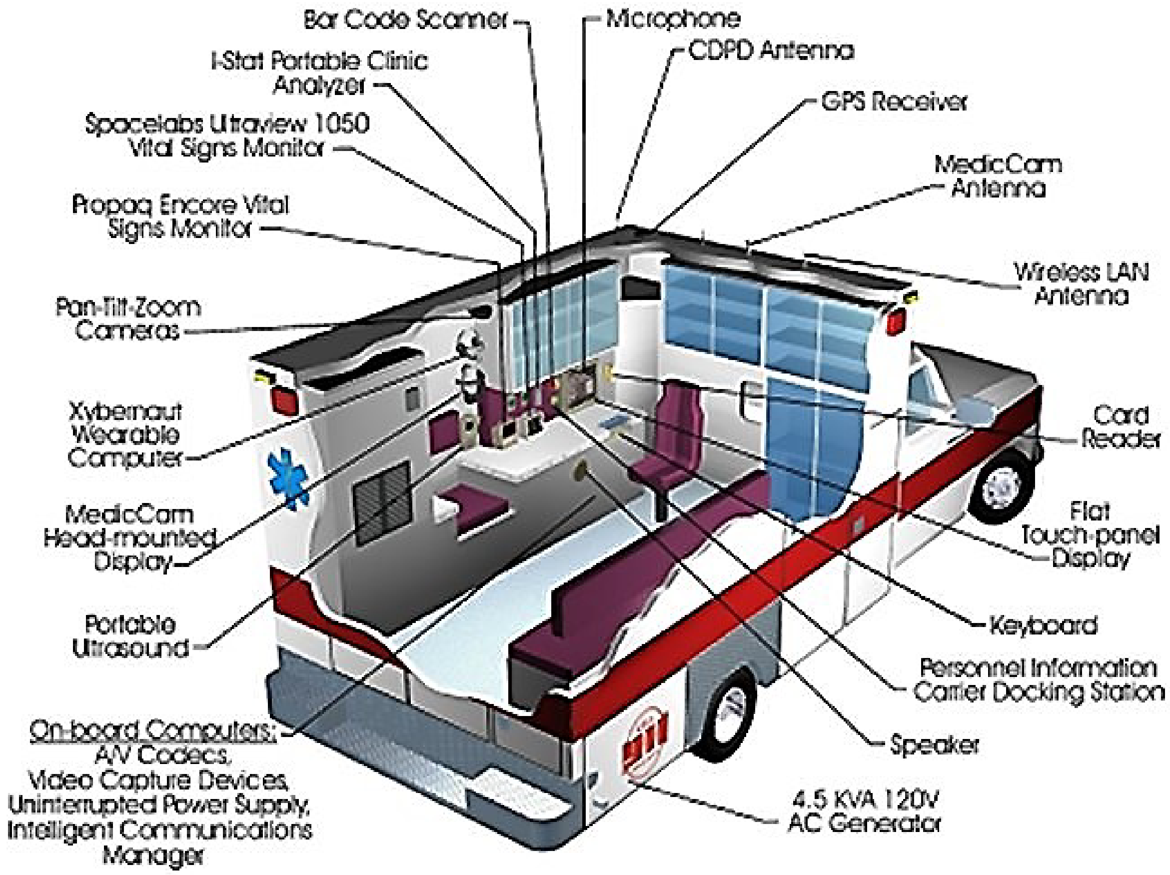
A.11 Examples of current EMS equipment

The Philips Intellivue MP2 was one of the first compact portable multi-parameter patient monitoring devices for ambulance use. Battery powered with a simplied touch-screen interface, it collects all basic physiological data for export through either a wired or wireless LAN connection. From there the data can go by cellular or satellite to a hospital, where a fixed-location counterpart system enables the staff to monitor the patient's condition before arrival.

Figure A.11. Philips Intellivue MP2 portable patient monitor

The way the MP2 interleaves data for simultaneous transmission was innovative in its day. But 5 years on, focus has shifted to data capture and integration on a much grander scale. The LifeBot DREAMS ambulance (below) was originally developed for the US Army. DREAMS (which stands for Disaster Relief and Emergency Medical Services) is the ambulance's operating system. All onboard devices are networked and everything that happens in the vehicle is documented with audio, video and data recording. If there is a sufficient communications link, prioritised physiological data from the patient can be transmitted along with live audio and video. The ambulance is equipped well enough to be a supplemental or substitute emergency room and it was used that way in Texas after Hurricane Rita.

Figure A.12. LifeBot DREAMS Ambulance



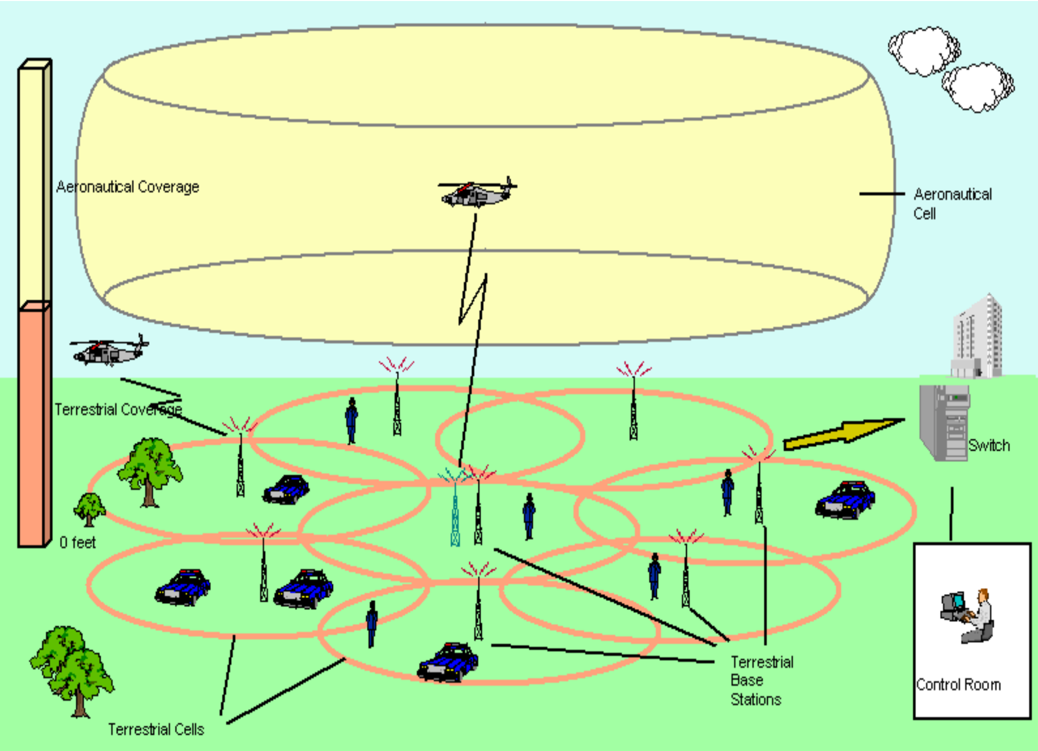
A.12 Other disaster response and rescue services

Since 1900 floods have been the most common type of disaster in Europe, according to the EM-DAT Database (http://emdat.be/): 341 of them, an average of 3 per year. Air transport accidents (253), severe storms (204), earthquakes (158) and rail accidents (141) are next ranked in frequency. More recently DG ECHO's Emergency Response Centre, in their first 6 months of operation, processed assistance requests triggered by fires in Hungary, Spain, Portugal, Romania and Italy; floods in Sweden; earthquakes in Italy and Bulgaria; and an industrial accident in Bulgaria.[124]

The ITU Focus Group on Disaster Relief Systems, Network Resilience and Recovery recommends broadcasting alerts to mobile handsets because people tend to have them nearby all the time. Cellular broadcast channels have been specified for the 3GPP Public Warning System (PWS). (ETSI, 2012b) The Netherlands tested the EU-ALERT implementation of PWS and showed that it "works well on 2G handsets but that smartphones on the 3G network were less well supported".[125] 3GPP is trying to resolve these problems.

Civil protection legislation adopted in 2013 called on the Commission to "establish and regularly update a cross-sectoral overview and map of natural and man-made disaster risks the Union may face…" The first overview was published in April 2014 to accompany a Communication on "managing risks to achieve resilience" (COM[2014] 216 final). Progress reports on the establishment of emergency management systems in each member state were given in the overview. They show that today's emergency management systems are mainly integrations of seconded resources to support crisis response co-ordination centres. In the future crisis management networks might evolve into permanent new public safety institutions needing their own "mission critical" resources.

Figure A.13. Public safety Air-Ground-Air interaction with cellular network



Source: ETSI, 2011.

ECC Decision DEC/(06)05 designated 384.8 - 385.0 MHz / 394.8 - 395.0 MHz for harmonised airborne use related to land mobile emergency services and 384.75 - 384.80 MHz/394.75 - 394.80 MHz if additional channels are needed. But since HD video is increasingly streamed from air to ground (for police aerial surveillance and damage assessments after disasters, less often during rescues), the required bandwidth challenges the capacity of any radio network: the UK Home Office says their helicopter video downlinks are 42 MHz wide.[126]

[124] "The first six months of activity of the GMES Emergency Management Service – Mapping", *GMES Observer,* issue 1 (November), http://www.copernicus.eu/newsletters/issue01/inthefield_emsmapping.html

[125] GSMA (2013) "Mobile Network Public Warning Systems and the Rise of Cell-Broadcast", http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2013/01/Mobile-Network-Public-Warning-Systems-and-the-Rise-of-Cell-Broadcast.pdf

[126] Quoted in ECC Meeting Document FM49(13)048rev2.

A.13 Public safety networks in the EU plus Norway

Note: Letters P and G are used to describe network owners and operators. P = Private, G = Government

---

Austria

Network owner: G
"Digitalfunk BOS Austria" is a public-private partnership based on a 25 year contract between the Bundesministerium für Inneres [BMI = federal ministry of the interior] and Tetron GmbH. BOS = Behörden und Organisationen mit Sicherheitsaufgaben [authorities and organizations with security tasks].

Network operator: P
Tetron GmbH is a joint venture created to build and operate the BOS network. It is owned 65% by Motorola and 35% by Alcatel Lucent.

Dimensions: The BOS network is based on TETRA technology. It has 2 net management centers, 2 switching centers (plus one for testing applications before deployment), 8 gateways and 670 base stations now serving over 36,000 radio terminals. When completed it should have 6 switches (plus 1 fallback), 1,250 above-ground base stations and 60 base stations in Vienna's subway.

Economics: Austria's provinces provide sites for base stations and bear some local operating costs. A 2013 audit of BMI's spending on BOS calculated the total cost of the infrastructure in service at the end of 2012 as €809 million, including provincial contributions. The annual radio service fee for the complete network will be €36.48 million, according to the auditors. But based on recent contract amendments, the auditors also predict a cost overrun of €180 million by 2029. Thus, the total 25-year cost of the BOS network is calculated as €1.15 billion.[127]

Belgium

Network owner: G
ASTRID is a 100% government owned non-profit corporation established by law in 1998. Network deployment began in 2001.

Network operator: G (ASTRID)

Dimensions: ASTRID has 11 switches and about 500 TETRA base stations supporting 40,000 subscribers. There are also 225 base stations for PocSAG paging, mainly for rescue services and volunteer fire brigades.

Economics: In 1998 the Interior Commission estimated the cost of building the ASTRID network at 5.8 billion Belgian francs plus 4.685 billion francs for terminals (a total of 10.485 billion francs, or 12.687 billion francs including VAT [€314.5 million]).[128] ASTRID subscription prices are based on the build-out cost of the network infrastructure (€143.8 million), divided by a 15-year depreciation period (€9.6 million/year), and divided again by the number of subscribers in the network's design capacity (40 000). That calculation has been adjusted for inflation since 1998 so an annual subscription in mid-2013 cost €331 plus VAT. Nongovernment subscribers pay

[127] *Bericht des Rechnungshofes: Vergabepraxis im BMI mit Schwerpunkt Digitalfunk*, Bund 2013/2 [*Report of the Court of Auditors, Procurement Practices in the Ministry of Interior with Focus on Digital Radio*], http://www.rechnungshof.gv.at/fileadmin/downloads/2013/berichte/teilberichte/bund/Bund_2013_02/Bund_2013_02_1.pdf

[128] "Projet de loi relatif aux radiocommunications des services de secours et de sécurité – Rapport fait au nom de la Commission de l'Interieur, des affaires generales et de la fonction publique par M. Pieter de Crem", Chambre des Représentants de Belgique, Session Ordinaire, 30 Avril 1998, pages 13-14, http://www.lachambre.be/FLWB/pdf/49/1435/49K1435006.pdf

more. ASTRID's actual operating cost is 3 times what subscribers pay, or €28.8 million/year.[129] The national government makes up the difference.

Bulgaria

Network owner: G
Starting in 2001 the Interior Ministry developed a TETRA network primarily for border control. At the same time the Ministry of Defense developed a separate TETRA network for the Army. In 2010 the Ministry of Defense proposed integrating the two networks but it is not clear if this happened.

Network operator: G
Dimensions: The Interior Ministry's network has 111 fixed base-stations and 3 mobile base-stations with a backbone of 120 microwave nodes, covering 81% of the territory. The number of users is unknown.

Economics: Very little information about costs is available. The first phase of the border control network was funded by the PHARE programme, then expanded with a €2.5 million Schengen grant from Norway.

Croatia

Network owner: G
Ministarstvo Unutarnjih Poslova (MUP, the Interior Ministry) owns MUPnet. Deployment began in 2004, it became operational in 2006, with full deployment expected in 2014. MUPnet has two subnets: one for emergency responders, one for "civilians" (e.g.; Zagreb public transport).

Network operator: G (MUPnet).

Dimensions: Based on TETRA technology, MUPnet now has 110 base stations and about 100 dispatch centres, designed to support 30,000 end-users.

Economics: In 2005 the government borrowed €28 million for MUPnet's build-out; €143.6 million more was borrowed for expanding MUPnet between 2005 and 2011.[130] Spending tapered off after 2011 to about €10.5 million/year, so we estimate the total cost of the infrastructure at about €200 million. Adding in portable and mobile terminals would raise the total system cost to about €300 million.

Cyprus

In 2007-8, the Department of Electronic Communication consulted the public on whether to authorise a TETRA network but "no entity demonstrated interest in establishing an island-wide network to cover all needs".[131] In 2009, the Cyprus Police invited firms to volunteer to undertake site surveys and estimate the cost of a TETRA network but received no offers.[132] Thus, public safety agencies are probably still using legacy analogue radio networks.

Czech Republic

[129] "Waar voor uw geld - De ASTRID-abonnementsprijs nader bekeken" [Value for money – A closer look at the ASTRID subscription price], http://www.astriddirect.be/nl/nieuws/waar-voor-uw-geld-de-astrid-abonnementsprijs-nader-bekeken

[130] Republika Hrvatska Državni Ured za Reviziju [Republic of Croatia State Audit Office (2011), "Izvješće o Obavljenoj Reviziji - Ministarstvo Unutarnjih Poslova" [On the Audit of the Interior Ministry], http://www.revizija.hr/izvjesca/2011-rr-2011/01-korisnici-drzavnog-proracuna/16-ministarstvo-unutarnjih-poslova.pdf

[131] Department of Electronic Communications (2009) "Ετήσια Έκθεση [Annual Report] 2008", Government of Cyprus, http://www.mcw.gov.cy/mcw/dec/dec.nsf/All/EEAA2F3FF5FDC3A1C22577210030EED7/%24file/%25CE%2595%25CF%2584%25CE%25AE%25CF%2583%25CE%25B9%25CE%25B1%2520%25CE%2588%25CE%25BA%25CE%25B8%25CE%25B5%25CF%2583%25CE%25B7%25202008.pdf

[132] Cyprus Police (2009) "Digital Radio Network System – TETRA Preliminary Survey", http://www.police.gov.cy/police/police.nsf/C99F799851D0B75CC22578A90027217D/%24file/Digital%20Radio%20Network%20System-TETRA.doc

Network owner: G
The Interior Ministry owns PEGAS, a mixed TETRA + TETRAPOL network for public safety/governmental use with nationwide coverage. There are 12 TETRA networks in the Czech Republic, including the municipal networks of Prague and Brno.

Network operator: G/P
The Czech Post Office is responsible for managing PEGAS but Pramacom s.r.o. is their subcontractor. URS Ltd. manages PEGAS data services.

Dimensions: PEGAS has more than 42 switching centers and 218 base stations covering 97% of the country with signals in the 380 - 400 MHz range and supporting 27,000 wireless terminals. In Prague, the TETRA Municipal Radio System has 19 base stations serving 1,500 police terminals, 2,500 transport company terminals and 100 for the city's Crisis Team.

Economics: The first (TETRAPOL) phase of PEGAS' buildout, from 1994 to 2003, cost approximately €135 - €200 million. In 2012 a €1 million contract was awarded for "renewal" of the oldest PEGAS base stations.

Denmark

Network owner: P
SINE (short for "Sikkerheds Net" or "Safety Net") is owned by a Motorola subsidiary, Dansk Beredskabs Kommunikation (DBK, Danish Emergency Communications). The Danish Government signed a 10-year lease for public safety organizations' use of SINE channels. DBK also has a commercial license to serve Copenhagen's transport authority (Movia) and the Danish State Railway (Danske Statsbaner, DSB).

Network operator: P
Motorola operates SINE for DBK.

Dimensions: About 500 SINE TETRA base stations cover 43,000 km^2 (99.5% of the country) and serve about 24,000 public safety personnel using 19,000 portable and mobile terminals. Fire brigades are the largest user group (15,000), followed by police (6 500).[133]

Economics: DBK's website says (in Danish) that the "government will pay 1.6 billion krone [€214 million] for establishment and access to the SINE network for ten years (2010-2020)."[134] According to an official evaluation of the proposal, Gartner Denmark estimated that a further 520 million krone (€71 million) will be needed for portable and mobile terminals, implying a total system cost of about €285 million. Looking at the "establishment and access" fee, Gardner estimated that 40% can be attributed to the build-out and 60% to ongoing use.[135]

Estonia

Network owner: G
ESTER is owned by SMIT (Siseministeerium = the Interior Ministry). It serves only state-budgeted entities but that could change in future.

Network operator: G
Operated by Riigi Infokommunikatsiooni Sihtasuts (RIKS, the State Infocommunication Foundation), a service agency of the Ministry of Enterprise.

---

133 Henningsen, P. (2011) "SINE Services: Common Operational Picture for Blue Light forces in Denmark", SINE, presented at the Nordic Workshop on Smart Cities, http://www.geoforum.dk/Admin/Public/Download.aspx?file=Files%2FFiler%2FPrsentationer%2FNordic+workshop+on+Smart+City+GIS%2FSession+11+-+Peter+Andreas+Henningsen.pdf

134 http://sikkerhedsnet.dk/om-sine/oekonomi/

135 Tværministerielt Radioudvalget (2006) "Rapport vedrørende et nyt landsdækkende radiokommunikationssystem for det samlede beredskab" [Report on a new nationwide radio communication system for all emergency services], Government of Denmark, pages 13-14, http://jm.schultzboghandel.dk/upload/microsites/jm/ebooks/andre_publ/rapport%20vedr%20et%20nyt%20alndsd%C3%A6kkende%20radiokomm_system.pdf

Dimensions: ESTER is a TETRA network covering all of Estonia with about 100 base stations and one switching center serving 10,000 public safety users. Buildout began in 2008 and was completed in less than 3 years. In addition, 5 base stations belonging to Finland's VIRVE network are located on Estonia's north coast to help cover the Gulf of Finland and to ensure intercommunication among the two countries' border guards.

Economics: No information about the cost of ESTER build-out is available but RIKS' current telecommunication usage fees are online.[136] RIKS' development plan for 2014-2018 calls for creating a mobile virtual network with commercial cellular networks in order to provide public safety users with broadband and VoIP, while developing a voice communications system integrated with ESTER to cover Estonia's islands and territorial waters.[137]

Finland

Network owner: G
Owned by the Government of Finland, VIRVE (VIRanomais VErkko = "authority radio network") was the world's first nationwide TETRA system. Buildout began in 1998 and full coverage was achieved in 2002. Migration to TEDS began in 2010.

Network operator: G
VIRVE is managed by Suomen Virveverkko Oy, a subsidiary of Suomen Erillisverkot Oy (Finland Security Networks Ltd.), which is owned by the government and overseen by the Prime Minister's office.

Dimensions: The VIRVE network has 1,500 base stations and 15 switching centers serving 40,000 terminals with about 60,000 individual users.

Economics: The original budget for VIRVE's buildout was €134 million. Annual subscription fees are negotiated by the Prime Minister's Office, the Ministry of Internal Affairs and Erillisverkot. Current fees and subscriptions are found at http://www.erillisverkot.fi/public/files/Virve%20hinnasto%202014.pdf They range from €366 to €797 per year (not including VAT), the high end being a fixed rate package with no additional telephone connection or per minute charges. Assuming an average of €600/year per subscriber, VIRVE's annual subscription revenue should be about €24 million/year.

France

Network owner: G

INPT = Infrastructure Nationale Partageable des Transmissions (National Shared Transmission Infrastructure) is for rescue and security forces. It links many formerly separate networks point-to-point and serves the national police and civil security forces, the gendarmerie, fire and rescue services, urgent medical aid services (EMS) and the marine battalion brigade of Marseille. The major interconnected radio networks are:

> ACROPOL = Automatisation des Communications Radiotéléphoniques Opérationnelles de POLice: owned by the Interior Ministry for use by the national police, ACROPOL is the country's largest TETRAPOL network. Deployment began in 1994 and was completed in 2006.
>
> The RUBIS network, launched in 1986, was the world's first large-scale digital PMR network. Completed in 2000 and owned by the Ministry of Defence for use by the Gendarmerie (military police), TETRAPOL was implemented in the VHF band (73.3 - 80 MHz).
>
> ANTARES = Adaptation Nationale des Transmissions Aux Risques Et aux Secours: expanding ACROPOL's infrastructure this TETRAPOL network provides inter-operability for firefighters, low-flying aircraft and rescue teams. Started in 2005, its coverage is still incomplete so analog VHF use persists in some areas.

---

[136] http://www.riks.ee/docs/RIKS_Hinnakiri_al_ 01.01.2014_kinnitatud_18.12.2013.pdf
[137] See http://www.riks.ee/docs/DEVELOPMENT_PLAN_2014_2018.pdf

In addition to 6 national TETRAPOL networks, France has 130 local and regional TETRA networks. The latter are mainly used by local governments and major transport enterprises.

Network operator: G, P
The Interior and Territorial Planning Ministry, along with subcontractors Thales and EADS/Airbus, manage the ACROPOL and ANTARES networks.[138] The army's Centre National de Supervision manages the RUBIS network.

Dimensions: ACROPOL covers about 85% of the country, with two network management centers and 1 100 base stations serving 40,000 end-user terminals. ANTARES is still in roll-out, expanding ACROPOL's infrastructure. When deployment is complete, the combined ANTARES-ACROPOL network will have more than 1 300 base stations serving more than 110,000 radio terminals. Firefighters will be moved from the 80 MHz band to the harmonised 380 - 400 MHz band. Rubis' 97 cells and extensive microwave "backhaul" network link 37,000 portable radios and 11,700 mobile and desktop terminals.

Economics: ACROPOL cost over €640 million to deploy. In addition, a 9-year contract with EADS worth €637.7 million was signed in 2004 for infrastructure and terminal maintenance and the management of usage rights.[139] Auditors criticised the lack of a way to measure ACROPOL's costs and the absence of a single line totalisation of operating expenses ["l'absence d'un instrument de mesure des coûts et d'une ligne unique d'exécution des dépenses d'ACROPOL"] but nevertheless estimated the annual operating costs as €39,135,581 for 2005, €52,784,431 for 2006, about €60 million in 2007, increasing to about €73 million in 2012.[140]

In 2008, when ANTARES was in early rollout, regional fire brigades were told that handheld TETRAPOL radios with geolocation would cost about €1,700 each, plus VAT; €3,200 plus VAT for a mobile terminal with geolocation. So a departmental fleet of 5 mobile and 5 portable terminals would be about €25,000. Gateways to the INPT infrastructure would cost an additional €25,000.[141]

Germany

Network owner: G
The Federal Government (through the Ministry of Interior) and the 16 German länder jointly own BDBOS (Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben, the German Federal Agency for Digital Radio of Security Authorities and Organisations).

Network operator: P
EADS is interim manager of the BDBOS project after the dismissal of DB Telematik.

Dimensions: Deployment started in 2009 and should be "substantially completed" by the end of 2014. When finished BDBOS will be the largest TETRA network in Europe, with about 4,500 base stations, 58 switching centers, 4 transit switching centers and 2 network management centers. BDBOS claimed to have 410,000 users in January 2014. When complete it will support about 500,000 users.

Economics: BDBOS' costs are financed jointly by the federal government and the länder. Local governments must buy end-user terminals and contribute to the infrastructure costs on their territory, but some local costs are subsidised.[142] See footnote for a link to the BDBOS Schedule of Fees.[143] The decision in 2002 to build BDBOS was based on a cost estimate of €2.75 billion. But in 2006 the parliament's budget committee estimated that

---

[138] Bechir, J. L., *et al.* (2007) "Mission d'audit de modernisation: Rapport sur l'exploitation et la maintenance du système ACROPOL", Contrôle général des armées, http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/074000358/0000.pdf
[139] Bechir *et al.* (2007), page 7.
[140] *ibid.*
[141] Gout, L. and Lamoulère, J. (2008) "Rapport d'Étude: SAMU et Radiocommunications" [Study report: EMS and radiocommunication], Observatoire Régional des Urgences de Midi-Pyrénées, https://www.orumip.fr/wp-content/uploads/2010/03/RappAntares.pdf
[142] "Sonderförderprogramm für Zuwendungen des Freistaates Bayern zur Beschaffung der Endgeräte des digitalen BOS-Funks in Bayern", Anlage zum IMS vom 15. November 2012 Az.: ID1-2244.2-605, http://www.stmi.bayern.de/imperia/md/content/stmi/sicherheit/feuerwehr/rechtl_grundlagen/121115_ims_anlage_215_i.pdf
[143] "BDBOS-Kostenverordnung", http://www.buzer.de/gesetz/10149/index.htm

BDBOS would cost €5.1 billion over 15 years.[144] The federal government's agreed contribution is €3.6 billion for the period 2007-2021.[145] But German media routinely claim the total cost to 2021 will exceed €10 billion when €6 billion in operating costs and non-federal contributions are included.[146] The FAQ on BDBOS' website says "BDBOS die Gesamtkosten nicht bekannt" [the total costs of BDBOS are not known].[147]

Greece

Network owner: G
The Ministry of Public Order and Citizen Protection owns C4I, the public safety network originally built for the 2004 Athens Olympics.

Network operator: ?
OTE Tetra Services had been managing C4I but the Government did not renew OTE's contract which ended 1 August 2014 (see "Economics" section below).

Dimensions: 93 base stations cover Athens, a few other major cities, the most used highways and some of the Greek islands.

Economics: More than €280 million was spent building C4I for the Olympics. Arbitration subsequently reduced the cost to about €250 million because some subsystems never passed the acceptance tests and were not needed after the Games ended. OTE's contract for managing the network expired in July 2014.[148] *Kathimerini* says that from 1 August 2014 the government will revive the pre-TETRA analogue police radio network (adding encryption), rather than continue paying OTE €4.5 million annually for C4I's maintenance.[149]

Hungary

Network owner: G
Ownership of the nationwide TETRA based EDR (Egységes Digitális Rádiótávközlő Rendszer = Unified Digital Radio System) began with Professional Mobile Private Limited Company (Pro-M zrt.), a joint venture of Magyar Telekom & T-Mobile Hungary, formed in 2005 to build and operate the network. The government-owned National Infocommunications Service Company (NISz zrt., which manages the government's ICT infrastructure) bought EDR in 2012.

Network operator: G
NISz zrt.

Dimensions: EDR has 4 switching centers, with 265 fixed and 5 mobile base stations serving 42,000 wireless terminals.

Economics: The government's 2005 contract with Pro-M stipulated flat-rate billing. The total annual service fee agreed then was 9,325 million HuF (about €37.3 million) plus VAT. The total cost of EDR was foreseen in 2006 as HUF 20 - 22 billion (about €79 million). But the completed system was sold to NISz zrt in 2012 for an estimated 19.9 billion HUF (€71.1 million). A €7.5 million contract was signed in 2013 for 23 new base stations and higher capacity switching equipment to support additional base stations.

---

[144] http://www.parlament-berlin.de/ados/16/Haupt/vorgang/h16-0060.A-v.pdf
[145] Bücken, R. (2014) "Hey BOS(S), ich brauch mehr Bandbreite", *PMR*, March issue, http://www.pmev.de/fileadmin/user_upload/Presse/NET/1403_s12_pmr.pdf
[146] Lutz, M. (2010) "Milliarden-Debakel beim Digitalfunk der Polizei", *Die Welt*, 25.02, http://www.welt.de/politik/deutschland/article6541887/Milliarden-Debakel-beim-Digitalfunk-der-Polizei.html
[147] http://www.bdbos.bund.de/SharedDocs/Downloads/DE/faq_buerger.html: "Da sich im Rahmen des Projektes Digitalfunk BOS Bund, Länder und Kommunen die Kosten teilen – beispielsweise beschaffen diese getrennt die Endgeräte und Leitstellen für ihre Behörden und Organisationen mit Sicherheitsaufgaben – sind der BDBOS die Gesamtkosten nicht bekannt."
[148] http://epikaira.gr/article/ligei-i-sumvasi-toy-TETRA-epistrofi-ton-epikoinonion-tis-elastis-pyrosvestikis-kai-toy-ekav-sto-2003
[149] Σουλιωτησ, Γ. (2014) "Αγορά μη επανδρωμένων αεροσκαφών από ΕΛ.ΑΣ", 22 June, http://www.kathimerini.gr/772876/article/epikairothta/ellada/agora-mh-epandrwmenwn-aeroskafwn-apo-elas

Ireland

Network owner: P
The National Digital Radio Service (NDRS) is for public safety agencies. It is owned by TETRA Ireland Communications Ltd., a joint venture of Eircom, Motorola and Sigma Wireless.

Network operator: P
TETRA Ireland Communications Ltd.

Dimensions: 2 main switching sites and about 640 base stations cover 96% of the territory and territorial waters out to 20 km from shore, with enhanced indoor signal penetration at 2500 locations. In the 1st quarter of 2013 An Garda Síochána (the national police force) had 15 267 subscriptions out of NDRS' total of ~17,000, making them the largest user group by far. (Other users include 1,300 prison officials and 100 customs officials.) Irish firefighters are expected to migrate to NDRS in 2014 - 2016.

Economics: The *Irish Examiner* said in 2009 that the NDRS infrastructure (then being built) would cost about €100 million. In 2013 a member of the Irish parliament asked the Minister of Justice if NDRS "represents value for money at €40 million per annum"; the Minister did not comment on or challenge the cited price. Expenditures reported by the Garda on their website show that their TETRA subscriptions cost €6,844,501 in the 4th quarter 2012 and €803,549 in the 3rd quarter of 2013. In addition to the subscriptions, Garda must pay for their terminal equipment.

Italy

Network owner: G
In 2003 Selex ES (a Finmeccanica subsidiary) and EADS won contracts to start building the "Interpolizie" TETRA network for the Ministry of Internal Affairs, to enable Italy's 5 police forces to intercommunicate.

Network operator: P
Selex ES manages at least their part of the network.

Dimensions: The plan was to deploy about 3,000 TETRA base stations for 90% territorial coverage, with 300 control centers and about 300,000 users.

Economics: The anticipated cost of the "Interpolizie" network in 2003 was €3.5 billion. €560 million was appropriated in 2006 to start the build-out but funding was suspended in 2012 due to the financial crisis, with only a quarter of the country covered. Selex ES then proposed connecting pre-TETRA analogue networks to working parts of the digital TETRA network as an interim measure. In June 2014 *Italia Oggi* reported that TETRA deployments would resume now that the Interior Ministry has about €500 million in new funding for projects proposed by the regions.[150]

Latvia

Network owner: G
The Interior Ministry owns the nationwide ASTRO25 network, which is based on APCO P25 analogue/digital technology.

Network operator: P
Motorola

Dimensions: One switching center supports both analogue and digital communications. In 2011 there were just under 8,200 subscriber terminals using the network. In 2014, the analogue and digital P25 networks will be

[150] Gerosa, F. (2014) "Finmeccanica, attese a breve novità su contratti Tetra", *Italia Oggi,* 4 June, http://www.italiaoggi.it/news/dettaglio_news.asp?id=201406041506583184

integrated, 9 new base stations will be added to the 55 already deployed, and 6 242 new portable and mobile radios will be distributed to bring support up to 10,000 first responders.

Economics: Funded by the European Regional Development Fund, €16.2 million will be spent this year upgrading the ASTRO25 network.

Lithuania

Network owner: G
The Interior Ministry owns "Skaitmeninės mobiliojo radijo ryšio sistemos" (SMRRS = digital mobile radio network system), the national TETRA network used by border guards, police and some emergency services.

Network operator: G
The network is managed by Informatikos ir ryšių departamentas, the Information Technology and Communications Department of the Interior Ministry.

Dimensions: 221 base stations (including 15 air-to-ground access points) serve about 8,700 end-user terminals. A similar number of security and rescue workers use pre-TETRA radios which operate in the 148 - 174 MHz band.[151]

Economics: €27.3 million was allocated in 2007 for build-out of the SMRSS network. A further €2.3 million was authorised in 2010 for 2500 additional radio terminals, and in 2011 €300,000 was authorised for a SMRRS control center and base stations for the use of railway police in the Kaliningrad-Russian corridor.[152]

Luxembourg

Network owner: G
The build-out of RENITA, a TETRA network for police, fire, customs, the army and emergency services, was not funded until January 2014. The Ministry of State will own RENITA.

Network operator: G+P
RENITA will be operated by a public-private partnership between EPT (Entreprise des Postes et Télécommunications) and ConnectCom s.a.r.l., a local supplier of DMR/TETRA equipment. Launch is planned for 2015.

Dimensions: 75 base stations will cover the whole country, serving up to 9,500 radio terminals used by 11,500 people.

Economics: The Governing Council allocated €36.6 million for RENITA's design and deployment; the first 5,000 terminals are expected to cost €13.5 million. The operating cost is expected to be about €4.7 million/year.

Malta

Network owner: G
Owned by the Department of Civil Protection

Network operator: ?
Safety services apparently use a 440 - 470 MHz Public Access Mobile Radio (PAMR) network.[153]

Dimensions:

---

[151] "Finansuotinų projektų pagal Išorės sienų fondo 2008", http://www.vrm.lt/fileadmin/Padaliniu_failai/ES_paramos_administravimo/ISf/isf_2011_projektai.pdf
[152] http://www.vrm.lt/fileadmin/Padaliniu_failai/ES_paramos_administravimo/ISf/111018_Nr1V-767.doc
[153] The PAMR network is mentioned in the Malta Communications Authority's 2006 "Policy Review and Strategic Framework of Radio Spectrum Management Consultation Paper", http://www.mca.org.mt/sites/default/files/attachments/consultations/2012/policy-review-radio-rpectrum-0.pdf

Economics: A parliamentary inquiry in May 2006 asked the Government why TETRA equipment worth €930,000 has been in storage since 2001, never deployed or used by the Department of Civil Protection. The Government's answer [in Maltese] was that there are "ongoing discussions with the company that provided this service while running another separate study on the use of this system. The radio system that the department is normally using is more sophisticated than TETRA."[154]

Netherlands

Network owner: G
The Ministry of Security and Justice is administratively responsible for "C2000", the government owned TETRA network; "P2000", the paging network mainly used by firefighters and ambulance services, and the "M2000" alarm system.

Network operator: G
Managed by VTSPN (Voorziening tot samenwerking Politie Nederland = Police Cooperation Facility Netherlands)

Dimensions: There are two network management centers, 27 control rooms, 15 switching centers and 544 registered sites (including 480 antenna masts) covering 97% of the territory and serving 65,000 radio terminals (85,000 end-users). A recent coverage improvement project added 67 new antenna masts.

Economics: Launched in 2000, the C2000 rollout was finished in 2005 at a cost to the government of €603 million. (*Total Telecom* said the cost was €700 million.) In addition, public safety organisations paid about €165 million for end-user equipment (portables, mobiles and pagers), training and regional project management. The recent coverage improvement project is estimated to have cost about €33.2 million. The total system cost is thus over €800 million.

Norway

Network owner: G
Deployment of the government owned Norwegian Public Safety Network (Nødnett) began in 2007 and completion is expected by the end of 2015.

Network operator: G+P
The Directorate for Emergency Communications (Dinkom, subordinate to the Ministry of Justice and Security) was established to build and manage Nødnett. In 2012 Motorola Solutions replaced Nokia Siemens Networks as Nødnett's prime contractor, with responsibility for operating the network until 2025.

Dimensions: Nødnett will cover 79% of the territory, 200 tunnels and 100% of the population with about 2,100 base stations. There are over 80 control centers for about 40,000 end-user terminals. The completed network will support about 80,000 users.

Economics: Dinkom's director told *TETRA Today* in 2011 that "we are talking about a life-cycle cost of about 10 billion NOK [€1.3 billion]"[155] The 2004 cost estimate was 3.6 billion NOK (€411 million) but then it was decided to cover the whole population and upgrade to TEDS. The national government pays for infrastructure but subscribing organisations pay for operating costs and terminal equipment. The annual subscription fee for a control room terminal, for example, is NOK 40,000 (€4,800) while a stand-by terminal is NOK 1,500 (€180). Since the amount of message traffic has little impact on the cost of operation there are no usage fees and as more users sign up, the per terminal subscription costs go down.

---

[154] "Dibattiti Tal-Kamra Tad-Deputati (Rapport Uffiċjali u Rivedut)", L-Għaxar Parlament, Seduta Nru. 388 [Debates of the House of Representatives (Official Report and Revised), 10th Parliament, Sitting No. 388], Paragraph 19305, 23 May 2006, http://www.parlament.mt/file.aspx?f=999
[155] Lambley, R. (2011) "An essential investment", *TETRA Today,* 1 October, http://www.tetratoday.com/news/an-essential-investment

Poland

Network owner: G
The national government has applied for EU funding to consolidate many locally initiated TETRA nets into 2 national networks: OCSŁR (Ogólnopolskiego Cyfrowego Systemu Łączności Radiowej = National Digital Radio Communication System), for first responders, and OSAP (Ogólnopolskiej Sieci Administracji Publicznej = National Network of Public Administration).

Network operator: P, G (diverse)

Dimensions: It is not yet clear which existing networks will become part of the national public safety network.

Economics: The first plan for a nationwide PPDR network was developed in 2003, with a cost estimate of nearly 5 billion zloty (€1.1 billion).[156] In 2010 a tender was announced for firms interested in integrating and operating the existing security networks as Stage 1 of OCSŁR. The tender was annulled when the government decided to seek bids instead for expanding TETRA coverage to all of Poland along with SIS into neighbouring countries.

Portugal

Network owner: P
In 2006 the Interior Ministry awarded a 5-year "build-own-operate" contract to Siresp S.A., a consortium 42.31% owned by Grupo Galilei (an investment fund spun off from the National Bank of Portugal), 30.55% owned by Portugal Telecom, 14.9% owned by Motorola and 12% owned by Esegur. Siresp is an acronym for Integrated Network for Emergency and Security Portugal.

Network operator: P
Completed in 2010, the network is operated for Siresp by Telecomunicações Móveis Nacionais, S.A. (TMN, the mobile phone subsidiary of Telecom Portugal).

Dimensions: Currently there are 502 TETRA base stations, 53 dispatch centers, 6 switches, and 2 mobile stations with satellite links, serving a designed capacity of 53,500 users.

Economics: An official 2001 estimate of the network's build-out cost was €100-150 million. However, the contract awarded in 2006 to the only bidder was €340.7 million, subsequently renegotiated to €291.3 million. Siresp collects service fees from the agencies using the network (the Red Cross, the national fire service and volunteer fire departments, the directorate of prisons, the Army, Air Force and Navy, the national EMS institute, police, border guards, the nature conservancy and the intelligence service). Telecom Portugal's annual report for 2012 says its Siresp ownership share produced €15.1 million in revenue in 2011 and €14.275 million in 2012. Grupo Galilei's 2012 annual report says their ownership share was worth €87.505 million and generated €4.743 million in revenue. That suggests Siresp's net profit in 2012 was about €11.21 million and the network's asset value was €206.82 million. A further implication is that TMN collected a €10.85 million service fee for managing the network.

Romania

Network owner: G
The Government of Romania owns the national TETRA, TETRAPOL and WiMAX networks.

Network operator: G

[156] Instytut mikroMAKRO (2011), *TETRA for Poland: Organisational and Business Models,* http://www.mikromakro.pl/ wp-content/uploads/2012/02/TETRA-raport-mikromakro-14-07-2011en1.pdf

Serviciul de Telecomunicaţii Speciale (STS) manages the government intranet, the national TETRA, TETRAPOL, WiMAX and "112" emergency call networks. STS is organised by the Supreme Council of National Defence but controlled by committees of Parliament.

Dimensions: STS uses TETRA for voice and narrowband data, WIMAX for broadband. 544 TETRA base stations, 94 TETRAPOL base stations and 1,300 WiMAX base stations serve 55,000 end user terminals. The Integrated System for Border Security (TETRA) interfaces with one internal security TETRAPOL network in each county. The TETRAPOL network, known as Phoenix, pre-dated the others (it was deployed between 1998 and 2002).

Economics: Cassidian/EADS signed a €650 million contract in 2004 to begin upgrading the communications equipment of Romania's border guards. A follow-on contract in 2005 reduced the value of the project to €545 million but added a requirement for a TETRA network which would eventually cover all of Romania's border counties and serve other public safety agencies, too. The STS WiMAX network cost just over €20 million.

Slovakia

Network owner: G
SITNO is a national TETRAPOL network owned by the Ministry of Interior. Primarily used by civilian and military police forces, it became operational in 2008.

Network operator: GP
SITNO is operated by the Ministry of Interior's telecom department with technical support from RCTT s.r.o., EADS' Slovak partner.

Dimensions: About 100 base stations organised into 8 regional networks serve nearly 12,000 SITNO users. The networks were upgraded in 2011-12 to accommodate up to 20,000 users. The main user groups are the police, fire brigades and military security. The ministry installed an analogue/digital interface to make migration easier. EMS professionals tried SITNO at the end of 2012 but decided to stay on their analogue network until requested improvements are implemented. The mountain rescue service also has a separate 166 - 174 MHz analogue network used by some fire brigades.

Economics: The Interior Ministry's initial 1997 estimate of SITNO's cost was €64.5 million. By 2005 €122 million had actually been spent on it and a further €12.4 was needed for completion, totalling €134.4 million just for infrastructure.[157] A plan to incorporate SITNO into a military-run "Integrated Defense System" has been discussed for years; the plan's budget shows additional investments would be needed of A 2012 purchase order for TETRAPOL terminals from Cassidian gives some typical prices: €1,263 for a handheld, €1,642 for a vehicle mounted transceiver (including VAT).

Slovenia

Network owner: G
Deployment of a TETRA network (the Unified Digital Radio Network of Public Authorities) for the Interior Ministry, to replace the existing APCO 25 network, began in 2003. In July 2013 the Government solicited offers from private companies to complete and manage the network, perhaps becoming co-owners in a "public-private partnership."[158] A decision is expected soon.

Network operator: P
Currently managed by an outside contractor.

---

[157] MacLeod, M. (2005) "Radio project revived", *Slovak Spectator,* 17 January, http://spectator.sme.sk/articles/view/18376/
[158] Ministry of Interior (2013) "Public call to promoters to submit an application detailing their interest in operating a public-private partnership project", Government of Slovenia http://www.mnz.gov.si/fileadmin/mnz.gov.si/pageuploads/JAVNA_NAROCILA/LETO_2013/1200-13-jzp_poziv_promotorjem_razpis_TETRA_EN.doc.

Dimensions: The TETRA network now has 1 mobile and 79 fixed base stations, plus 36 dispatch centers, covering ~65% of Slovenia's territory and serving about 7000 users. The government hopes to have as many as 37,000 users when the network is fully developed (disaster relief and civil protection agencies are still using analog networks). The midterm deployment strategy review expects users to have 17,900 handheld and 10,080 vehicle-mounted terminals.

Economic comments: The government's 2007 midterm project review (just mentioned) adjusted the network cost forecasts to reflect their actual build-out experience. By 2007 they had spent €12.65 million to deploy over half of the network, and thought another €10 million would be needed to finish it. Leasing mountain locations for antenna masts would cost €900,000 annually, plus a one-time investment of €230,000 for microwave links and €810,000 annually for leased lines to connect base stations to switches. That implies a total investment of nearly €23 million plus €1,710,000 annually for leases. However, at least €780,000 could be saved annually by retiring older police and military radio systems.[159]

Spain

Network owner: P, G
Telefonica S.A. owns the TETRAPOL network infrastructure of SIRDEE (Sistema de Radiocomunicaciones Digitales de Emergencia del Estado), but the radio frequencies are assigned to the Ministry of the Interior which buys mobile communication services from SIRDEE for various national security and police forces under automatically renewed 4 year contracts. Because of SIRDEE's subscriptions costs (and other reasons), many regional governments, fire brigades and ambulance services decided to create their own networks based on TETRA; some are privately owned, some are governmental.

Network operator: P, G
Telefonica manages the SIRDEE network. Operation of the TETRA networks varies by region.

Dimensions: SIRDEE has 186 switches, over 1 500 base stations and 70 000 end-user terminals covering 95% of Spain'.

Economics: €147 million was invested in the build-out of SIRDEE.[160] The per-terminal subscription fee was initially about €3,000 per year but apparently by 2010 that had come down to about €1,000 per year.

Sweden

Network owner: G
The RAKEL network for public safety agencies is owned and managed by the Swedish Government's Agency for Civil Contingencies (Myndigheten för samhällsskydd och beredskap = MSB). The first base stations started operating in 2006 and the network was completed at the start of 2011.

Network operator: G (MSB)
Dimensions: This TETRA network has 18 switches, 2,000 base stations, and more than 50,000 users in 300 organisations.

Economics: The initial budget for RAKEL was 2 billion krone (€221 million). By 2005 it had risen to 2.3 billion krone for construction (€258 million) plus 390 million krone per year to operate (€43.9 million/year). Subscriptions are priced according to the user class: municipalities pay 6000 krone (€675) per subscriber per year while commercial subscribers pay 9500 krone (€1066) per year. Individual services are priced, too, varying by user class. However, there is no usage fee for voice calls or short data messages.

---

[159] Ministry of Higher Education, Science and Technology (2007) "Strategija graditve enotnega digitalnega radijskega omrežja državnih organov Republike Slovenije", Government of Slovenia, http://www.arhiv.mvzt.gov.si/fileadmin/mvzt.gov.si/pageuploads/DEK/Elektronske_komunikacije/Strategije/Strategija_TETRA_2007-enotno_dig_omrezje.pdf
[160] According to Algieri, E. (2010) "Public Safety Networks in Spain", http://www.tandcca.com/Library/Documents/TETRA_Resources/Library/Presentations/Turkey2010Algieri.pdf

United Kingdom

Network owner: P
In 2000 the Police Information Technology Organisation (PITO, now part of the Home Office) launched a "public finance initiative" to design, build and operate Airwave, a nationwide TETRA system for UK police. BT won the contract and rollout began in 2001. But ownership transfers and buyouts led to the 2007 purchase of Airwave Solutions Ltd. by subsidiaries of Australia's Macquarie Bank for £1.9 billion. The Home Office's contract with Airwave ends in 2016 and their spectrum license expires in 2020.

Network operator: P
Airwave Solutions Ltd. but the UK Home Office is seeking an alternative.

Dimensions: Airwave has 8 live switch sites (+8 recovery switches), 3,800 base stations covering 99% of the UK and 300,000 individual users belonging to 300 organisations.

Economics: The original cost estimate for the Airwave network consisted of a core service charge of £1.18 billion (€1.41 billion), payable in monthly installments for 19 years, plus about £290 million (€350 million) over 19 years for optional services.[161] That would be about €93.2 million per year. However, annual reports of the Home Office's predecessor agency show the UK Government paid £250,551,000 (€294 million) for Airwave services in 2010-11[162] and £242,345,000 (€283.5 million) in 2011-12, plus another £144,278,000 (€168.8 million) for "resilience" and for Airwave installations in the London Underground.[163] Airwave subscribers also pay £80 – £100 million (€93.6 – €117 million) per year on "non-Airwave communication services" (i.e., data, long distance and cellular).[164] In March 2014, a British court postponed Macquarie's obligation to repay £1.73 billion which they had borrowed to buy Airwave.[165]

A.14 TETRA vs TETRAPOL: a comparison

The similarity of the names might suggest these standards are closely related but that is only true in an historical sense. These tables, adapted from the Swiss Office of Communications' "TETRAPOL Factsheet" (2005), highlight the individual differences and advantages.[166]

Table A.6. Differences between TETRA and TETRAPOL

Parameter	TETRA	TETRAPOL
Multi-access structure	Time Division Multiple Access (TDMA)	Frequency Division Multiple Access (FDMA)
Net data transmission rate	Protected: <19.2 kbit/s Non-protected: <28.8 kbit/s	Protected: <4.8 kbit/s Non-protected: <7.2 kbit/s
Modulation	π/4 Differential Quaternary Phase-Shift Keying (DQPSK)	Gaussian Minimum Shift Keying (GMSK)
RF carrier separation	25 kHz	10 kHz or 12.5 kHz

[161] National Policing Improvement Agency (2010) *Annual Report and Accounts 2009/10,* UK Government Stationery Office, http://www.npia.police.uk/en/docs/NPIA_Annual_Report_and_Accounts_2009-10.pdf
[162] National Policing Improvement Agency (2011) *Annual Report and Accounts 2010/11,* UK Government Stationery Office, http://www.npia.police.uk/en/docs/Annual_Report_and_Accounts_2010_11.pdf
[163] National Policing Improvement Agency (2012) *Annual Report and Accounts 2011/12,* UK Government Stationery Office, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/247028/0241.pdf
[164] Zilis, M. (2013) "UK Preps for Broadband Mission-Critical Network", *RadioResourceMediaGroup,* 13 August, http://www.radioresourcemag.com/onlyonline.cfm?OnlyOnlineID=400
[165] Moses, A. and Miecamp, J. (2014) "Guardian Digital Gets UK Court Backing for Debt Restructuring", *Bloomberg BusinessWeek,* 28 March, http://www.businessweek.com/news/2014-03-28/guardian-digital-gets-u-dot-k-dot-court-backing-for-debt-restructuring
[166] http://www.bakom.admin.ch/themen/technologie/01220/index.html

Table A.7. Advantages and disadvantages of TETRA and TETRAPOL

Advantages of TETRAPOL vis-à-vis TETRA	Disadvantages of TETRAPOL vis-a-vis TETRA
In low traffic situations, TETRAPOL's modulation provides up to 50% greater signal range than TETRA's for the same peak transmission power. TETRAPOL requires only about half as many base stations as TETRA to cover a certain area. Common-frequency (simulcast) transmissions are easier to implement with TETRAPOL. Low out-of-band emissions. Equipment is available for a wider range of frequencies, VHF as well as UHF.	TETRA's data transmissions are up to 4 times faster than TETRAPOL's. TETRAPOL's spectrum efficiency is lower than TETRA's. Duplex operation is not simple to realise in TETRAPOL. Fewer manufacturers produce TETRAPOL equipment, meaning less price competition and less choice for purchasers. TETRA is supported by ETSI.

Appendix B. Utilities

The organisation of utilities and utility markets varies across Europe, influencing the configuration of networks and requirements for wireless communication. Some countries have centralised industries – France, for example, with EDF for electricity and GDF Suez for gas – while Germany has hundreds of municipal-level utilities which distribute electricity, gas and water (hot and/or cold) and in some cases telecommunication services as well. Some countries separate utility assets, with distribution handled by one entity while supplies are sourced by another; others separate wholesale and retail operations. In general, utility use of telecommunications is diverse and radio is just one option.

B.1 Electricity communication requirements

All utilities make extensive use of fixed line communications. In the case of electricity, powerline communication (PLC), which uses the wires delivering electric power to transmit data as well, can be implemented on both high and low voltage lines. Most "smart meter" deployments in Europe are expected to use PLC to some extent. However, radio is valuable because:

- The communication medium is independent of the assets managed – i.e. if a high-voltage line goes down, or a storm drain floods the co-located cable ducts, communication need not be interrupted as radio networks can be engineered to survive damage to the utility's distribution infrastructure.
- If a radio service is interrupted, it can usually be restored more quickly than a wired service.
- Radio is flexible and can be deployed more quickly than cabling.
- In most situations, radio networks cost less to deploy than wire-based networks, especially if rights-of-way are needed or there is a large number of link paths.

According to the EUTC, utility communication requirements include:

- High communications network availability: up to 99.999% in some cases.
- High reliability, such that any periods of non-availability do not occur when the network is stressed.
- Resilient architecture, with as much redundancy as possible.
- Mains power autonomy for up to 72 hours for critical elements, more in special cases.
- Low latency which could be as stringent as 6 ms maximum.
- Security against physical disruption and electronic intrusion as set by national cybersecurity requirements.
- Connectivity to all network assets, including those in remote or sparsely populated areas – even offshore windfarms.
- Low cost.[167]
- Appropriate bandwidth, varying from as little as 600 bps at the extremities to 2-10 Mbps at concentrators feeding into fixed-line fibre-based or microwave core networks.
- Support for distributed control with intelligence spread throughout the network, so responses do not depend on a single central hub.
- Long-lasting operation and support, as utility assets are generally expected to last 15-50 years (replacing telecommunication assets might force a plant or service to shut down so it is a nontrivial exercise).

[167] According to a EUTC representative, price makes GPRS preferable to TETRA: transmitting data from one meter via GPRS costs about €10/year while transmitting the same data with a TETRA modem through TETRA network costs about €1000/year. But according to Martin Miklas of RWE Polska, even GPRS is too expensive: "We already have today 6000 smart meters [sending data via GPRS], so I know how much we pay for one SIM card monthly! If we pay this money, then we can forget smart metering because the opex itself will kill the case." Quoted in Lambley, R. (2012) "On the starting grid", *Land Mobile UK,* 14 December, http://www.landmobile.co.uk/news/on-the-starting-grid

Table B.1 High priority requirements for electrical utilities: teleprotection

FOR RADIO CONNECTED DEVICES ONLY

Service	Description	Priority or criticality	Type of service	Coverage	Volume in 2010	Predicted volume in 2015	Predicted volume in 2020	Predicted volume in 2030	Data rate required	Data volume	Latency	Availability	Comments
PROTECTION													
Class A: Unit Protection (over 100kV)	Connection between protection devices at either end of a transmission line	high	pt-pt	main routes	0	5	10	15	64 kbits/s	continuous	5ms	99.99%	Duplicated circuits with max 400us differential delay
Class B: Distance protection (over 100kV)	Fast overcurrent protection on long transmission lines	high	area	specified sites	0	5	25	50		1 kbyte	5ms	99.99%	
Class C: Blocking signals (over 100kV)	Broadcast signal from a protection relay detecting a fault to delay the operation of adjacent protection relays	high	pt-pt	main routes	0	10	30	60		continuous	5ms	99.99%	Duplicated circuits with max 400us differential delay
Class D: protection for circuits of less than 100kV	Protection equipment for medium voltage equipment	high	pt-pt	main routes	0	20	100	200		continuous	10ms	99.99%	Duplicated circuits with max 1ms differential delay
Class E: remote access to protection relays	Remote configuration of protection relays from control centre	medium	pt-pt	specified sites	0	20	50	100		1 Mbyte	1s	90%	

Source: EUTC, 2013

Radio's role in electrical utility operations is expanding as sensors and telemetry come into wider use and growing numbers of field workers have portable data devices. Radio is also needed for more stringent network management, to keep the electricity supply stable amidst fluctuating demand and variable power sources like wind turbines and photovoltaic cells. Offshore wave, tidal and wind farms must be connected, though fixed lines can often be used, perhaps with radio backup. In any case, the trend is towards decentralised power generation. Over time, this will reshape network architectures and change the way electricity distribution is managed. An evolution from hierarchical to geodesic networks is virtually inevitable, but the impact on spectrum requirements is not yet clear.

The real driver of change in electric utilities is the move from centralised hydrocarbon-based power generation to widely dispersed intakes of renewable clean energy. This requires distributed management ("smart grid" technology) using radio links on the low voltage side for consumption monitoring and voltage regulation. These radio links can be some combination of short-range license exempt meshes, home area networks (HANs), utility owned point-to-point, GPRS or cellular (if affordable). For other utility operations, a dedicated VHF band allocation can support wide area, long distance services.

In the coming decade, the main challenge for utilities is to adapt to the transformation of electricity generation – from the burning of traditional carbon fuels in a few big power stations, to a large number of low emission sources of renewable energy distributed throughout the grid. With "smart grid" technologies, power can be saved by managing load profiles, persuading customers to adjust their behaviour to reduce peak power consumption through the use of variable pricing, and by rewarding them for contributing power to the grid. Large investments in power generation can be avoided if more resources are devoted to load control.

Table B.2. Smart metering deployments, with focus on electricity (2014)

Country	Metering points (millions)	Roll-out	Communication technologies	Total investment (millions, estimated)
Austria	5.7	2012-2019	From the smart meter to the data concentrator: 70% PLC and 30% GPRS. From the data concentrator to the Data Management System: 100% Fibre Optics.	€3195
Czech Republic	5.7	Negative business case so no plan yet; reconsider in 2017	PLC from smart meter to data concentrator; GPRS (or any other applicable wire-less technology) where impossible to use PLC. GPRS+fibre optics from the data concentrator to DMS.	€4367
Denmark	3.28	2014-2020	PLC, GPRS/GSM, WiFi & RF.	€310 per year
Estonia	0.709	2013-2017	PLC (90%), GPRS (10%).	€110
Finland	3.3	2009-2013	PLC (30%), GPRS (60%), RF (10%).	€692
France	35	2014-2020	PLC.	€4500
Germany	47.9	Still consulting stakeholders	GPRS/UMTS/LTE (80%), PLC/BPL (20%), DSL (5%), Fibre-optics (5%).	€6 493 (by 2022), €14 466 (by 2032)
Greece	7	2014-2020	PLC from smart meter to DMS.	
Ireland	2.2	2014-2019	PLC/RF.	€1 040
Italy	36.7	2001-2011	PLC from smart meter to data concentrator. GSM/GPRS from data concentrator to DMS.	€3 400
Latvia	1	2015-2017	PLC from smart meter to data concentrator. GSM from data concentrator to data centre.	€75.6
Luxembourg	0.26	2015-	PLC, GPRS.	€35

		2018		
Malta	0.26	2009-2014	PLC and GPRS.	€20
Netherlands	7.6	2012-2020	PLC and GPRS.	€3 340 (electricity+gas)
Poland	16.5	2012-2022	PLC.	€2200
Romania	9	2013-2022	PLC from smart meter to data concentrator. GSM/GPRS, WiFi/WiMAX and fibre optics from data concentrator to DMS.	€712
Slovakia	2.625	2013-2020	For direct communication between meter and DMS (with no middleware): GSM/GPRS/ETHN. For indirect communication (with middleware): PLC, RF, and/or WAN.	€69
Spain	27.77	2011-2018	PLC.	?
Sweden	5.2	2003-2009	From smart meter to data concentrator: mix of GPRS, PLC and/or Radio (46%); PLC only (37%); Radio only (17%); GPRS (1%). From data concentrator to Distribution Management System: GPRS (86%); IP (fiber, etc.) (33%); Other (17%); Radio (9%); PLC (8%).	€1500
United Kingdom	32.94 for electricity, 26.63 for gas	2012-2020	A range of technologies will be used including cellular and long range radio.	€9295

Source: Commission Staff Working Document: "Country fiches for electricity smart metering" SWD(2014) 188 final, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2014:188:FIN

Note: there is a regionally harmonised license exempt allocation for meter reading at 169.400 - 169.475 MHz. How widely used this channel is today is not known but none of the new plans for deploying smart meters relies on it.

B.2 Gas utility communication requirements

Wireless communication requirements for the gas industry are similar to the electricity industry's but more limited (fast response times to support teleprotection applies only to electricity, where microseconds matter). With gas, network conditions change slowly, though the need to diversify Europe's gas sources, brought into focus by the crisis in Ukraine, suggests changes in the transnational pipeline network could be forthcoming – but the process will take years.

The cost-benefit analyses performed by Member States for smart metering show significant differences between gas and electricity: the economic justification for deploying smart gas meters in residences is weaker, especially when joint installations and shared communication infrastructures are not assumed. PLC is always an option for electricity but it is practical for gas only with a short radio hop to safely separate watts and hydrocarbons.

As political pressure mounts to find new sources of natural gas, the industry faces new challenges in meeting demand. The existing regional pipeline network may have to be extended to diversify routing and incorporate new supply sources. "If you cannot move the gas around, you cannot have a single gas market," observes Gilles Darmois.[168] On the other hand, except for security and the dispatching of repair crews, the gas industry's use of radio is limited.

B.3 Water utility communication requirements

Europe's water industry must eventually come to grips with the problem of leakage. Huge investments are being considered for the renewal or creation of large sewage systems for storage, long distance carriage and treatment as Europe's urban centres expand. Thames Water in the UK, for instance, will invest €5 billion for just one system in the London area.[169] Adaptable long-distance conduit systems are also being discussed as climate change induces more floods and droughts. Water redistribution over large areas requires storage capacity in many places, as well as run-offs with actively managed valves, sluices and gates.[170] This does not even begin to address the longer-term prospect of rising sea levels.

The EC has an increasing number of Directives which affect water quality, waste water treatment, habitats and also a Water Framework Directive for EU-level harmonisation and modernisation. These drivers ensure that slow but substantial change is coming, towards more real-time control of water supplies and distribution at the regional level. Consequently, modern systems for sewage treatment and the storage and distribution of water are likely to rely increasingly on large numbers of low cost radio sensors to provide constant monitoring for smarter control and automation. According to Slater, "Water utilities are now finding that near real-time information from their distribution networks goes beyond meter reading. Intelligence can be delivered that helps them reduce costs, fix leakages, task field crews more effectively and helps transform their daily operations from a reactive to proactive nature. This is the business driver behind the smart water network concept".[171] Slater's point is that sensors other than usage meters are growing in importance.

---

[168] Matalucci, S. (2014) "The real problem of shale gas in Europe: financing", *Natural Gas Europe,* 28 July, http://www.naturalgaseurope.com/gilles-darmois-finance-shale-gas-europe

[169] Ashton, J. (2014) "Thames Water seeks international backers for London's £4bn super-sewer", *The Independent,* 23 March, http://www.independent.co.uk/news/business/news/thames-water-seeks-international-backers-for-londons-supersewer-9211182.html

[170] Gersonius, B., *et al.* (2013*),* "Climate change uncertainty: Building flexibility into water and flood risk infrastructure", *Climatic Change*, Springer, Volume 116(2), http://ideas.repec.org/a/spr/climat/ v116y2013i2p411-423.html; Ashley, R., and Cashman, A. (2006) "The impacts of change on the long term future demand for water sector infrastructure", *Infrastructure to 2030*, OECD, Paris, http://www.oecd.org/ futures/infrastructureto2030/37182873.pdf

[171] Slater, A. (2011) "Developing Smart Water Networks across Europe", *WaterWorld,* Vol. 27, No. 1, http://www.waterworld.com/articles/wwi/print/volume-27/issue-1/editorial-focus/developing-smart.html

Appendix C. Intelligent Transport Systems (ITS)

C.1 Road traffic management communication requirements

According to the *US Traffic Control System Handbook,* in ITS “only the transmission of a considerable number of CCTV signals requires the use of broadband communication”.[172] Everything else is narrowband though that may change in the future. Nevertheless we begin with ITS use of video.

Video cameras at fixed locations can send data via wire but it is usually cheaper to use radio and that also makes changing the camera location easier. Although easily intercepted, Wi-Fi is now the most widely used link technology for CCTV. Traditionally a 2.4 GHz activity, the 5 GHz band is now preferred because it offers wider channels, less interference, smaller antennas and more easily focused radio beams.

Since many agencies post live videofeeds on the internet , with camera location information, it is possible to sample the numbers of traffic cameras in various Member States. Here are representative counts of live traffic video camera feeds on the internet :

Austria = 529	Finland = 180	Luxembourg = 70	Poland = 567
Croatia = 153	Hungary = 41	Netherlands = 22	Slovenia = 156
Denmark = 208	Italy = 881	Norway = 288	

Poland’s trafficam website is unique in reporting both the number of monitoring centres and the number of video feeds each centre receives. From that, one sees that the monitoring centres receive an average of 6 video streams, though the actual number varies from 1 to 20. That may not be typical; a country like the UK with over 10 000 traffic cams[173] probably has many more feeds into each centre.

Calculating the bandwidth needed to transmit CCTV images is complicated by fact that video compression varies with the speed and efficiency of the compressor “chip” and how much the image changes from frame to frame. Roughly speaking, an IP camera with 640 x 480 pixels screen resolution using MPEG-4 compression at 7.5 frames/sec needs about 325 kbps of bandwidth. Six streams require about 2 Mbps. If Wi-Fi is used, protocol overhead and error correction must be factored in, so the total bandwidth for one stream probably exceeds 700 kbps. A Wi-Fi link from a video aggregation and relay point with 6 inputs thus requires about 4.2 Mbps. However, a video resolution of 640 x 480 pixels may be too low for automatic number plate recognition. Rapid uptake of HDTV for surveillance is expected in the coming decade, driven by improvements in software for automatic number and face recognition. Transmitting those images to monitoring centres will certainly require broadband.

Another radio-in-transport topic of great interest today is *eCall*. The European Commission adopted a set of proposals requiring all vehicles produced in the EU after October 2015 to incorporate a system which automatically reports accidents to the nearest “112” emergency call centre via cellular, indicating the vehicle type and location. When the vehicle’s airbags are activated, a voice session is launched. All commercial cellular networks are required to recognise eCalls by the end of 2014 and all Member States are to install eCall handling platforms in their emergency call centres by the fourth

[172] Dunn Engineering Associates and Siemens ITS (2005) “Chapter 9: Communications”, *Traffic Control System Handbook,* US Department of Transportation, http://www.ops.fhwa.dot.gov/publications/fhwahop06006/chapter_9.htm
[173] Their feeds are collected at http://www.bbc.co.uk/travelnews/

quarter of 2015. Because about 30,000 people die in road accidents each year in the EU, it has been estimated that eCall could save thousands of lives by reducing delays in medical intervention. According to HeERO (the Harmonised eCall European pilot project), "the EU's economic loss caused by road accidents amounts to more than €160 billion per year. If all cars were equipped with the eCall system, up to €20 billion could be saved annually".[174] eCall is an important example of cellular use by first responders. Successful co-operation in implementing the system could develop into a broader framework.

Table C.1. License exempt allocations for transport and traffic telematics

Frequency band	Notes
870.0 - 875.8 MHz	License exempt use of this band may be denied in some European countries that use all or part of the band for defence/governmental systems. In other countries that use 873-876 MHz for ER-GSM, duty cycle is limited to ≤0.01% with a maximum transmit on-time of 5ms/1s. Access to the ER-GSM sub-band by automotive SRD applications requires additional mitigation measures. 500 mW e.r.p. restricted to vehicle-to-vehicle applications. 100 mW e.r.p. restricted to in-vehicle applications. Adaptive Power Control is required in which the APC is able to reduce a link's transmit power from its maximum to ≤5 mW.
5795 - 5815 MHz	For Dedicated Short Range Communications (DSRC), intended for high data rate (up to 1 Mbit/s) communication systems for Road Transport and Traffic Telematics (RTTT) applications. An individual license may be required for high power stations
21.65 - 26.65 GHz	For automotive Short Range Radars (SRR). See detailed requirements in ECC/DEC/(04)10. New SRR equipment shall not be placed onto the market as of 1 July 2013.
24.050 - 24.500 GHz	For vehicle radars. See *ERC Recommendation 70-03* for rules governing this band.

Source: ERC Recommendation 70-03 (2014), Annex 5.

A substantial amount of research on road hazard mitigation has been funded by the EC under the umbrella of "co-operative ITS" (C-ITS). The practical requirements of many use cases are still hazy, but the general idea is for vehicles to signal each other automatically via radio, to share hazard warnings, indicate sudden braking or the intention to turn, avoid accidents and coordinate cooperative driving (caravans or "road trains"). The radios used for these applications might be license exempt in dedicated or shared bands or associated with public cellular networks. Unfortunately, "the original timetables for the roll-out of next-generation ITS technologies, and especially Cooperative ITS (C-ITS) systems, now look hopelessly optimistic".[175] In the US, the national traffic safety agency is just starting to draft rules to enable the implementation of vehicle-to-vehicle (V2V) communications, suggesting that the field is still quite immature globally (NHTSA, 2014).

Despite that assessment the most ambitious "next-generation ITS technology" made its debut in 2007 at DARPA's Urban Challenge, a race for driverless vehicles organised by the US Defense Advanced Research Projects Agency. Driving 80 km on paved and unpaved roads at a decommissioned Air Force base, the cars had to conform to California traffic rules, obey traffic signals at intersections, navigate around blocked routes and avoid other vehicles driven by humans and robots to finish in the

[174] http://www.heero-pilot.eu/view/en/ecall.html
[175] Jandrisits, M. (2013) "Cooperative cooperation", *ITS International,* July-August, http://www.itsinternational.com/categories/utc/features/amsterdam-group-turn-its-theory-into-practice/

shortest possible time. “It was a watershed moment,” said Raj Rajkumar, whose team won the $2 million prize. “It was the first time it was demonstrated that vehicles could drive themselves, without anybody in them, following all the rules that you and I follow when driving – the first time in history autonomous driving in realistic conditions was no longer science fiction.”[176] The cars in DARPA’s race were all controlled by computers responding to sensors. But if this technology is commercialised (as seems inevitable), radio links will probably be added to increase the vehicle’s information resources and perhaps assert control if unsafe driving is detected.

The social and economic impact of self-driving vehicles is increasingly recognised as potentially huge – and imminent. It is also clear that this development will impose stringent requirements on the robustness and availability of the networks which keep traffic flowing safely. Should these be considered “mission critical” even when no humans are in, for example, a fleet of trucks?[177] If commercial cellular networks are used for traffic control and service is interrupted, bringing traffic to a halt, is the carrier liable for the economic consequences?

ITS is evolving rapidly, with new concepts and applications emerging every year. Consensus is still weak on the bandwidth requirements, appropriate frequency ranges and authorisation regimes for new applications, let alone those which have not yet been defined. More than any other sector in this study, ITS’ spectrum requirements are mainly over the horizon. However, a framework for thinking about what lies ahead is found in the 2DECIDE project’s “Toolkit for Sustainable Decision Making in ITS Deployment”, presented (with minor refinements) in **Table C.2:**

Table C.2. Prospective ITS applications

Disaster Response Management & Coordination Coordination with emergency agencies Disaster data management Disaster response management **Transport-related Electronic Payment Services** Financial transactions Integration services **Emergency Services** Automatic accident reporting and emergency services calls Emergency vehicle management Hazardous material and incident notification Transport-related emergency notification & personal security **Freight Transport Management** Intelligent truck parking Management of hazardous goods **Intelligent Vehicle Services** Automated vehicle operations Safety readiness Driver impairment (drowsiness, alcohol)) Lane-keeping Distance keeping	Enhanced safety for vulnerable road users Safety provisions for pedestrians using intelligent junctions & links **Traffic Management & Operations Services** Demand management Incident management Policing/enforcement Transport infrastructure maintenance management Traffic management & control Adaptive traffic control at intersections Priority to selected travelers (e.g. cyclists, pedestrians) and/or vehicles (e.g. emergency) Delay minimisation Green wave Information infrastructures Traffic control centers Traffic information centers Road/weather monitoring Traffic monitoring Parking facilities management Planning & forecasting traffic conditions Traffic flow control Specific control measures for vulnerable road users Specific control measures for bridges Specific control measures for tunnels

[176] Calem, R. E. (2014) “Driverless cars on the rise”, *IT Is Innovation*, January-February, http://www.ce.org/i3/ Features/2014/ January-February/Driverless-Cars-on-the-Rise

[177] The Vienna Convention on Road Traffic (1968; amended 1993) has been signed by all EU members except for Ireland and Netherlands. *Inter alia,* it denies the legality of driverless vehicles. Article 8 states: “every moving vehicle or combination of vehicles shall have a driver…” and driver is defined in Article 1 as “any *person* [emphasis added] who drives a motor vehicle…” If the Commission wants to facilitate the development of self-driving vehicles, it may be time to revisit this treaty, which is online at http://www.unece.org/trans/conventn/crt1968e.pdf.

Platooning
Speed control
Collision avoidance
Intelligent vehicle safety
Vision enhancement
Co-operative systems
Traffic safety
Traffic efficiency
Supporting services
Value-added services

Public Transport Services
Demand-responsive & shared transport
Public transport management
Communication systems
Electronic payment

Road Transport Related Personal Safety
Public travel security
Safety enhancement for disabled road users

Traffic management for specific vehicles (wide loads, dangerous cargo, etc.)
Co-ordinated traffic management
Variable message signs for traffic guidance
Ramp metering
Dynamic lane management

Weather & Environmental Conditions Monitoring Services
Environmental conditions monitoring
Weather monitoring

Traveller Information Services
On-trip information
Pre-trip information
Route guidance & navigation (on-trip)
Trip planning support
Information about travel services
Route guidance & navigation (pre-trip)

C.2 Railway communication requirements

In the same way that radio networks for public safety emerged as local initiatives based on proprietary technologies, leading to acute interoperability problems, individual European railways deployed analogue communication systems which were mutually incompatible. As a result, long-distance trains had to be equipped with multiple radios for use on different track segments – an unsatisfactory situation that lingers still today.

"Council Directive 96/48/EC of 23 July 1996 on the interoperability of the trans-European high-speed rail system" began tackling this problem. The scope of the Directive was limited to high-speed lines but strategic aims were identified:

- reliability and safety of services, enhanced by migration to a new generation of technology for train signalling with a fail-safe design;
- interoperability; and
- economic efficiency through standards encouraging a competitive market in equipment, software and support services (Decision No 1692/96/EC). [178]

Five years later a new Directive expanded the interoperability requirements from high-speed lines to all trans-European rail traffic.[179] By 2011 the goal was not just interoperability but commonality, as the European Railway Agency adopted technical regulations specifying GSM-R.

Devised by and for railways, GSM-R's radio interface is based on GSM to take advantage of the design experience, parts availability and economies of scale of equipment produced for the public. However, GSM-R has many features not found in public implementations of GSM, including talkgroups, all-calls, emergency pre-emption, location-variable numbering, and interaction with trackside sensors and signals. It also has the EIRENE-MORANE specifications which enable connectivity to be maintained during hand-offs from one base station to another even at 500 km/h. For in addition to voice support, GSM-R is the radio component of the European Rail Traffic Management

[178] "Decision No 1692/96/EC of the European Parliament and of the Council of 23 July 1996 on Community guidelines for the development of the trans-European transport network", http://ec.europa.eu/transport/wcm/infrastructure/grants/2008_06_20/2007_tent_t_guidlines_en.pdf
[179] "Directive 2001/16/EC of the European Parliament and of the Council of 19 March 2001 on the interoperability of the trans-European conventional rail system", http://eur-lex.europa.eu/legal-content/EN/TXT/?uri= CELEX:32001L0016

System (ERTMS); its data links support the European Train Control System (ETCS). The radio modem connecting a train to the control centre has priority over all other onboard usage because if the control connection is broken, the train loses "movement authorisation" and must stop.

In contrast to PPDR, Direct Mode Operation is rarely used in railway communication. Specific channels were designated for DMO when the ECC recommended frequencies for GSM-R. But no EU member state actually implemented GSM-R DMO due to co-existence issues with TDMA based GSM networks. Consequently ECC Decisions (02)09[180] and (02)10[181] were amended in 2011 to remove references to DMO.[182]

The GSM-R Requirements Specification also makes no reference to broadband. The modem speeds used by the European Train Control System are 2.4, 4.8 and 9.6 kbps. Connection to the internet is considered not only unnecessary for railway operations but risky, giving potentially malicious strangers a chance to interfere with mission critical safety systems. As far as the railways are concerned, the internet is only for passengers and and passenger information services (schedules, ticket prices, etc.). As one interviewee put it, "You don't access the internet to drive a train".

But internet access for train passengers has been shown to boost ridership. The European Commission's 2011 Transport White Paper set a goal of reducing greenhouse gas (GHG) emissions by about 20% by the year 2030 and by 60% by the year 2050. Transportation produces about a quarter of all GHG emissions and because railways are 3-4 times more energy efficient than road or air transport, moving goods and people by rail must become a prominent feature of Europe's future transportation mix if the GHG emission reduction targets are to be reached. According to the White Paper:

> 30% of road freight over 300 km should shift to other modes such as rail… by 2030, and more than 50% by 2050… Triple the length of the existing high-speed rail network by 2030 and maintain a dense railway network in all Member States. By 2050 the majority of medium-distance passenger transport should go by rail... (COM/2011/0144 final)

But in 2012 rail carried less than 7% of passengers and 11% of freight in the EU-28 (DG MOVE, 2014). So to reach those ambitious future targets, the rail industry must increase its carrying capacity and attractiveness to customers. Granted that the mobile broadband supporting Wi-Fi access might have to be kept separate from train control, as is the case today. But broadband for passengers could help the rail industry reach the Transport White Paper's goals.

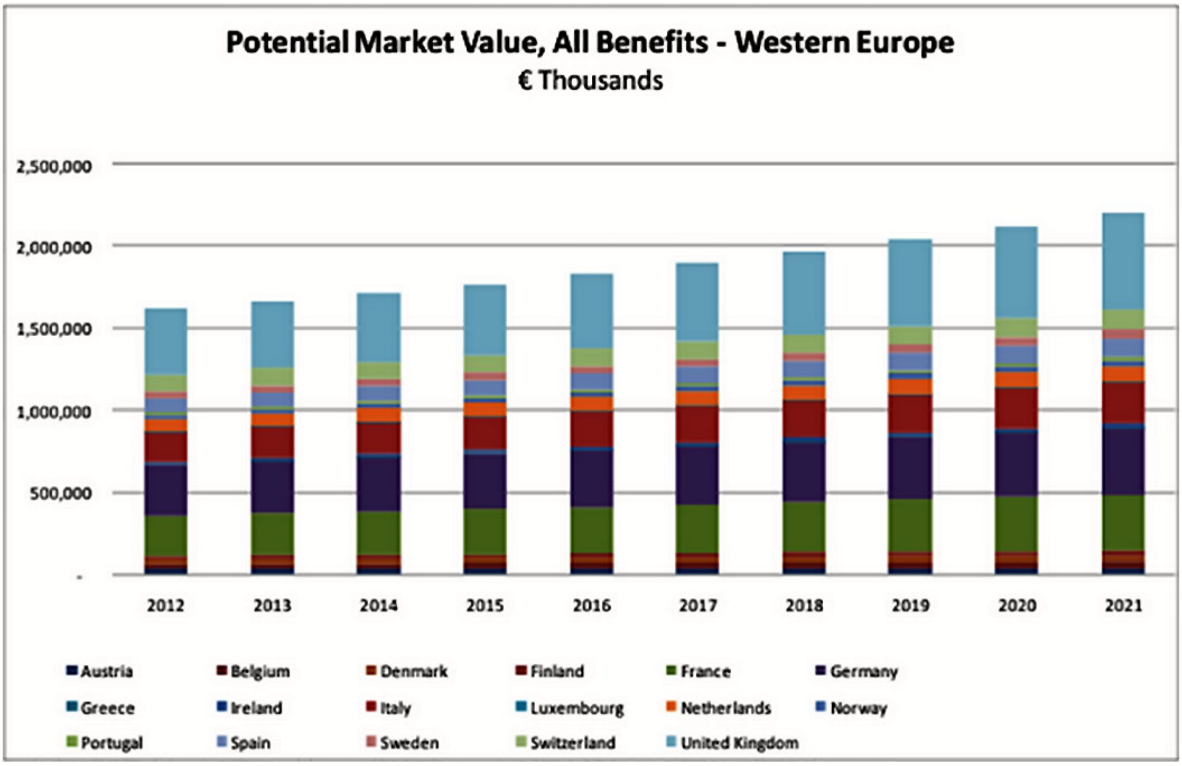
---

[180] "ECC Decision of 15 November 2002 on free circulation and use of GSM-R mobile terminals operating within the frequency bands 876-880 MHz and 921-925 MHz for railway purposes, in CEPT countries…, amended 11/03/2011", http://www.erodocdb.dk/docs/doc98/official/word/ECCDec0209.doc

[181] "ECC Decision of 15 November 2002 on exemption from individual licensing of GSM-R mobile terminals operating within the frequency bands 876-880 MHz and 921-925 MHz for railway purposes…, amended 11/03/2011", http://www.erodocdb.dk/docs/doc98/official/word/ECCDec0210.doc

[182] This history was recounted by Ireland's Commission for Communications Regulation while introducing a new GSM-R licensing regime. See ComReg (2011) "Response to Information Notice 10/84: Licensing Regime for GSM for Railway Operations", Document No. 11/90, http://www.comreg.ie/_fileupload/publications/ComReg1190.pdf

Figure C.1. Potential value of train-based broadband in Western Europe, 2012-2021



Source: BWCS, 2012.

Many railway requirements now seem implementable in software as apps. For that reason, there is not much concern in the industry about having to use commercial cellular instead of their own dedicated networks. The main consideration is that *whatever network is used, it must always be available or the trains will stop moving.* There might have to be some cost-sharing to put base stations in places where there are few other subscribers and to add redundancy to track coverage, but that would be cheaper than dedicated networks. Cab radios and ruggedised handsets with special-purpose buttons would still be needed by some crew members. However, others can use consumer-grade equipment so long as the tuning range includes GSM-R frequencies. The handover time from base station to base station is also not a decisive issue. Nor is it a rigid requirement: if a handoff takes 400ms instead of 300 ms but call continuity is preserved, the exact number of milliseconds is not important.

Like the utility industry, the rail industry is conservative and prefers to rely on proven technologies with long life cycles. However, unlike the airline industry, where voice is used for traffic control, train control is based on narrowband data. That makes driverless trains feasible. These already operate as "people movers" at airports and in the subway systems of Copenhagen, Paris, Budapest, Barcelona and elsewhere.[183] Driverless freight train experiments are conducted from time to time without publicity. These rely on trackside sensors, not video, so the bandwidth requirements are low.

Nevertheless there are situations where broadband would be useful for railway operations, even if not essential: e.g., for downloading equipment condition data from trains moving at normal speeds, to deliver video from a camera at the front of the train to the driver so he has a better view of the track ahead, cameras in freight cars for security, etc.

183 In addition, remote control via short-range radio enables driverless shunting operations.

Table C.3. License exempt railway allocations

Frequency band	Application	Notes
984 - 7484 kHz	Balise up-link (ground to train)	Transmitting only on receipt of a Balise / Eurobalise telepowering signal from a train. Note: centre frequency is 4234 kHz
7.3 - 23.0 MHz	Loop up-link (ground to train) systems including Euroloop	Spread spectrum signal, code length 472 chips, transmitting only in the presence of trains. Note: centre frequency is 13.547 MHz
27.090 - 27.100 MHz	Balise tele-powering and down-link (train to ground) systems including Eurobalise and activation of the loop/Euroloop	May be optionally used for activation of the loop/Euroloop. Note: centre frequency is 27.095 MHz
76 - 77 GHz	Obstruction/vehicle detection via radar sensor at railway level crossings.	For ground based vehicle and infrastructure systems only

Source: Adapted from ERC Recommendation 70-03, Annex 4

Communication between moving trains ("rolling stock") and trackside beacons, sensors, induction loops and other devices traditionally uses license exempt spectrum. Cellular networks are not a practical alternative, regardless of whether dedicated or commercial.

C.3 Currently Deployed Railway Radio Equipment & Networks

Austria: By the end of 2012, ETCS Level 2 had been deployed on 218 km of track. Build-out of GSM-R is planned to finish in the third quarter of 2015[184] (it will not be implemented on small feeder lines). However, the legacy analogue FM network still operates as a backup on most routes and is even being reinforced by new installations in tunnels. TETRA base stations for the use of fire brigades are also being added to some railway tunnels. Frequencies used by the legacy network are 79.800 - 81.025 MHz for shunting; 165.600 - 171.375 MHz for technical services; and 410.000 - 470.000 MHz for voice and data.[185]

Belgium: Route-by-route shutdown of the legacy radio system began in 2005. By the start of 2011, all trains and more than 3,000 km of tracks were equipped with GSM-R.[186] Migration of train control to ETCS will begin in 2015 on the high-speed lines.[187]

Bulgaria: All railroad lines in Bulgaria are covered by an analogue radio system for dispatching and maintenance which operates in the 450 MHz band. "In accordance with the requirements of the national regulations and norms the special dispatching systems are built as independent systems and are not connected with the other telecommunication network".[188] Radio channels for shunting

[184] OBB (2014) "GSM-R Service Entry Plan", http://www.oebb.at/infrastruktur/en/_p_Network_Access/Digitaler_Funk_GSM_-_R/02_DMS_Dateien/_GSM_R_ Service_Entry_Plan.jsp

[185] ERA (2010) "EMC for European Railways", http://www.era.europa.eu/Document-Register/Documents/67575_ERA_EMC_Study_Final_Report%20Issue%2005.pdf

[186] ERA (2010)

[187] InfraBel (2014) "Network Statement, Appendix C.7: Map Planning ETCS (22-12-2010)", http://www.infrabel.be/sites/default/files/documents/C7%20Map%20Planning%20ETCS%20(22-12-2010).pdf

[188] "Report for the Factual Condition of the Railway Infrastructure (Network Statement)", version 01, change 06, Bulgarian National Railway Infrastructure Company, July 2014, http://www.rail-infra.bg/assets/Documents/network%20statement_en/network%20statement%202014/network_statement_09072014.pdf

operations are in the 150 MHz band. A GSM-R switching centre with base stations on a route to the Greek-Turkish border is expected to enter service soon.

Croatia: Croatia is not currently involved in any TEN-T funded projects.[189] Railway development is a second priority, with more resources going into the road network. Deployment of GSM-R began with the goal of covering about 1,280 km of track and the project is about half done. The minister of transport is expected to approve a final procurement plan, including ETCS, in summer 2014.[190] At the end of 2011 the first line with ERTMS/ETCS train control began operating. Otherwise there is no automatic train control in Croatia, though there are local "autostop" devices.[191] Railway lines without GSM-R continue using analog UHF.

Czech Republic: 2,766 km of track will be covered with GSM-R by the year 2015, which means pre-GSM-R networks are still in use: Traťový rádiový systém (Track Radio System) operates in the 160 and 450 MHz bands; the non-interoperating ASCOM radio network also uses 450 MHz near stations, to link train drivers, dispatchers and maintenance/repair crews. Bandwidth of the 160 MHz FM channels was reduced from 25 to 12.5 kHz at the start of 2013 so the analogue network's life could be prolonged.[192]

Cyprus: Cyprus has had no railway operations since 1951. In 2010 the government said it would commission a feasibility study for a new intercity rail service but nothing seems to have come of that.

Denmark: A gradual transition began on 1 January 2013 when the new GSM-R network was activated. GSM-R data is expected to be available on all rail lines by 2021.[193] Meanwhile the Radiometrix MSR-3 analog radio network continues operating in the 868 - 870 MHz band. Both systems are available on every line. It is not known how long this arrangement will last. The 450 MHz band is used by both Line Radio and Local Station Radio networks though they are non-interoperable. Storno CP1000 radios are used for shunting operations (146 - 174 MHz and 403 - 433 MHz/438 - 470 MHz). S-line (suburban Copenhagen) radios support both voice and data communication in the 900 MHz band. They are not interoperable with GSM-R and the only source for these radios now is "reclamation from old S-trains". All S-line trains should be equipped with GSM-R by August 2015.[194]

Estonia: Because most of their rail traffic is still with Russia, Estonians are not rushing to deploy GSM-R or ETCS.[195]

Finland: GSM-R buildout on 3,556 km of track started in 2002 and was completed at the end of 2009. Trains rely on public GSM for an additional 852 km.

France: Deployment of GSM-R began in 2004 on the high-speed lines. Synerail, a public-private partnership, was formed in 2009 to build and operate a nationwide ERTMS network for Réseau Ferré de France (RFF) until 2025 when it is supposed to be turned over to RFF and operated/maintained by

---

[189] European Commission (2014) "Croatia", Innovation and Networks Executive Agency, http://inea.ec.europa.eu/en/ten-t/ten-t_projects/ten-t_projects_by_country/croatia.htm

[190] Aleksić, G. (2013) "Nova Regulativa u Području Sigurnosti i Interoperabilnosti Željezničkog Sustava", *Željeznice* 21, issue 2/2013, http://www.hzinfra.hr/fgs.axd?id=11640

[191] HŽ Infrastruktura (2014) *Network Statement 2015,* http://www.hzinfra.hr/lgs.axd?t=16&id=11921

[192] "Prohlášení o dráze 2014: Příloha F - Traťové rádiové systémy" [Railway Statement 2014, Appendix F – Track Radio Systems], Správa Železniční Dopravní Cesty [Czech Railway Infrastructure Administration], http://www.szdc.cz/soubory/prohlaseni-o-draze/2014/priloha-f-2014.pdf

[193] Banedanmark (2014) "GSM-R Programme Information", http://uk.bane.dk/visArtikel_eng.asp?artikelID=8350

[194] Thøgersen, T. E. (2013) "Register of Infrastructure covering the analogue radio system and the GSM-R system (part of the ERTMS subsystem)", version 2.0, BaneDanmark, http://www.bane.dk/hentmedie.asp?filID=15312; Thomsen, L. (2014) *Network Statement 2014*, BaneDanmark, http://uk.bane.dk/hentmedie.asp?filID=15926 "Siemens Rail Automation completes GSM-R installation on Danish S-bane fleet", *European Railway Review,* 23 December 2013, http://www.europeanrailwayreview.com/19747/rail-industry-news/siemens-rail-automation-completes-gsm-r-installation-on-danish-s-bane-fleet/

[195] "ERTMS implementation plan for Estonian conventional rail network" (2007), http://ec.europa.eu/transport/modes/rail/interoperability/ertms/doc/edp/national_deployment_plans/estonia_ndp.pdf

Societé Nationale des Chemins de fer Français (SNCF). The €1.2 billion GSM-R network, with 2,500 base stations and 17 base station controllers supporting 10,000 cab radios and 30,000 handhelds along 14,000 km of track, is supposed to be finished in 2015.[196] But deployment of ETCS is 5-8 years behind schedule. Consequently, high speed trains still use the older TVM (Transmission Voie-Machine, track-to-train transmission) for speed control, although border-crossing trains also have ETCS. RFF will soon start decommissioning the Radio Sol-Train (ground-train radio) which has linked train crews and traffic controllers since the late 1970s and which is still used in some neighbouring countries. Video and data capabilities were added to RST in the 1980s and 1990s, making it one of the most sophisticated of all legacy railway telecommunication systems.[197] RST reportedly uses frequencies near 70, 200, 468 and 1400 MHz.

Germany: Deutsche Bahn was the first railway operator to begin deploying infrastructure for GSM-R, in 1999.[198] In August 2014 the transition from analogue FM is finally supposed to end. Germany's railway network is Europe's largest, so it has the largest GSM-R network as well. Because it therefore has very busy rail hubs, DB has been licenced to use the E-GSM-R expansion bands at 873 - 876 MHz and 918 - 921 MHz.[199]

Greece: The Hellenic Railways Organisation (OSE) installed radios in all their stations and trains after a serious rail accident in the 1970s. Ten FM channels at 149.870 - 149.970 MHz and 150.290 - 150.350 MHz were assigned to OSE. Today just 3 channels (150.050 - 151.600 MHz) are used with a 4th held in reserve. OTE's commercial TETRA network is used on the line connecting Athens International Airport to Acharnes. A 103 base station GSM-R network started replacing these older radio systems in 2006; build-out is expected to finish in 2014. A "build-operate-transfer" contract was agreed, with the contractor responsible for engineering, design, procurement, testing, acceptance, user training, operation and maintenance of the system for 3 years before it is transferred to OSE.[200]

Hungary: Hungary apparently wants to have GSM-R deployed on 4,360 km of track by 2020, but it did not award the first contract until the end of 2013.[201] The first contract for ETCS Level 2 build-out quickly followed. However, both contracts are so recent that legacy train radio systems are still in use throughout the country: a "non-selective" analogue network operates at 160 MHz while a "selective"

---

196 The total cost estimate comes from European Investment Bank (2010) "Rail safety: the EIB lends EUR 280m in support of the French network", press release, http://www.eib.org/infocentre/press/releases/all/2010/2010-021-france-securite-ferroviaire-la-bei-sengage-en-faveur-du-reseau-francais-avec-280-millions-deur.htm. That describes the Synerail project as "amounting to EUR 1bn", to which we add the €180 million awarded to Nortel in 2003 for pre-Synerail network elements. See "SNCF, RFF select Nortel for GSM-R", *Telecom Paper* (2003), http://www.telecompaper.com/news/sncf-rff-select-nortel-for-gsmr—360731

197 Terrier, J.-E. (2003) "La radio sol trains à la SNCF (1976-2002)", *Flux,* No. 54, October-December, http://olegk.free.fr/flux/Flux54/pdffl54/09CourbeTerrier83-86.pdf

198 "Nortel upgrade keeps Deutsche Bahn's wireless railroad network running smoothly", *Market Wired,* 12 June 2008, http://www.marketwired.com/press-release/Nortel-Upgrade-Keeps-Deutsche-Bahns-Wireless-Railroad-Network-Running-Smoothly-867729.htm Müller, K. (2007), "Current GSM-R situation in Germany", *European Railway Review,* issue 2/2007, http://www.europeanrailwayreview.com/1088/err-magazine/past-issues/current-gsm-r-situation-in-germany/

199 Antwort der Bundesregierung (2012) "Technische Probleme beim europäischen Zugleitsystem ERTMS", Drucksache 17/8946 (22.03), Bundestag, http://dip21.bundestag.de/dip21/btd/17/091/1709111.pdf

200 Melissinos, C. D. (2011) "Explaining the GSM-R project in Greece", *European Railway Review,* issue 1-2011 (15 February), http://www.europeanrailwayreview.com/8198/err-magazine/past-issues/issue-1-2011/explaining-the-gsm-r-project-in-greece/; ERGOSE (2014) "Installation of GSM-R", http://www.ergose.gr/index.php?option=com_content&view=article&id=178&lang=en; "Greek railway signalling: radio communications", *Wikipedia,* https://en.wikipedia.org/wiki/Greek_railway_signalling; RFC7 Orient Corridor (2011) *Implementation Plan of Rail Freight Corridor 7, 'Orient Corridor'",* http://www.rfc7.eu/ckfinder/userfiles/files/RFC7_Implementation_Plan_v_November_2013.pdf

201 (2013) "GSM-R Facts & Figures", *RailwayPro,* August, http://www.railwaypro.com/wp/wp-content/uploads/2013/08/GSM-R.pdf

analogue network operates at 450 MHz. Four different automatic train control systems are used: EVM, EEVB, INDUS and ETCS.[202]

Ireland: As an island with a relatively small population and a rail network whose track gauge differs from other systems in Europe (even from the UK), Ireland could have used the "isolated network" exemption offered in the guidelines for developing the trans-European transport network, to avoid deploying ERTMS.[203] They delayed their decision for many years, but contracts were finally awarded in 2012 for GSM-R coverage of the Dublin Area Rapid Transit (DART) system as Phase 1 of a nationwide rollout.[204] Meanwhile, two legacy radio systems are used outside Dublin: "Mode A" operates on 4 channels in the 456 - 461 MHz range. This supports general calls to all trains or discrete calls to specific trains. Text messages can also be transmitted in either direction and calls can be patched through to the PABX. This system was updated a few years ago to extend its useful life.[205] "Mode C" has more limited capability and is used only on two rail lines. With Mode C there is "no provision for discrete communication to specific trains - all trains in the area can hear both sides of the conversation"[206] – and signal range is limited to about 5 miles.

Italy: GSM-R deployment began in 2004. By 2012 there were over 1,600 base stations covering 10 600 km of track.[207] Rollout was recently completed. ETCS has been implemented on a few international corridors but full rollout will be slow and costly with some projects already 3 - 5 years behind schedule.

Latvia: Latvian Railway recently awarded a contract for a trackside optical fiber network to "provide a technological platform for ERTMS (GSM-R) implementation".[208] In other words, GSM-R deployment has not yet begun. On all railway sections their old simplex AM communication system uses 2130 kHz for voice communication between dispatchers and trains. Additionally, narrowband FM in the 150 and 450 MHz frequency ranges is used near stations for shunting, equipment maintenance and emergency conditions.[209]

Lithuania: Deployment of GSM-R was completed in 2010 while ETCS deployment began this year.

Luxembourg: As in France, the Radio Sol-Train network is still used, though Luxembourg's is simpler than France's. A user's manual can be downloaded from the national regulatory authority. Primary frequency is 468.050 MHz. ETCS deployment should be finished by the end of 2014 and ERTMS/GSM-R should become operational in 2016.[210]

Malta: No train network.

---

[202] Vasúti Pályakapacitás-elosztó Kft. (2014) *Network statement on terms and conditions of the use of the open access railway network of MÁV ZRT and Gysev ZRT for the timetable year 2014/2015,* https://www2.vpe.hu/document/2886/NS%202014-2015%20M8A%20Text.zip

[203] "Regulation (EU) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on Union guidelines for the development of the trans-European transport network…", http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2013.348.01.0001.01.ENG Whereas (15) says: "The particular situation of isolated or partially isolated rail networks should be recognised by way of exemptions from certain infrastructure requirements".

[204] "Kapsch wins Irish Rail GSM-R tender for the implementation of a digital train radio system", press release, 2 February 2012, http://www.kapsch.net/kcc/press/pressitems/kcc_120202_pr

[205] Kessel, C. (2010) "Control from First Principles", *Rail Engineer,* December issue, http://content.yudu.com/Library/A1q4i9/RailEngineerDecember/resources/26.htm

[206] Irish Rail (2014) *Network Statement,* http://www.irishrail.ie/media/ie2014networkstatement_publishedversion21_1.pdf

[207] Senesi, F. (2012) "Italian Experience: ETCS L2", presented at the UIC ERTMS World Conference in Stockholm, http://www.uic.org/cdrom/2012/10_ERTMS-Conference2012/docs/C3-Enzo-MarzilliV1.pdf

[208] Latvian Railway (2014) "Latvijas dzelzceļš paraksta līgumu par maģistrālā datu pārraides tīkla mkodernizāciju", press release (9 June), http://ldz.lv/?object_id=5569

[209] Latvian Railway (2007) "European Rail Traffic Management System (ERTMS) National Implementation Plan – Latvia", http://ec.europa.eu/transport/modes/rail/interoperability/ertms/doc/edp/national_deployment_plans/latvia_ndp.pdf

[210] Département des transports (2014) *Luxembourg Railway Network Statement 2015*, http://www.mt.public.lu/ministere/services/direction_chemins_fer/ACF/Document_reference/pdf_DRR_2015_EN.pdf

Netherlands: Netherlands was the first country to migrate its rail services completely to GSM-R – in 2007 – after covering 3,000 km of rail lines. About 20% of the NS rolling stock is equipped for ETCS and a 10-year programme for deploying the new train control system has been agreed, gradually replacing the ATB automatic train protection equipment.[211]

Poland: With 23,000 km of tracks, Poland has the third largest railway system in Europe. GSM-R deployment began in 2011 and by 2020 they plan to have 15,000 km of track covered. Deployment of the first analogue FM radiotelephone system started in 1972. That system, which operates simplex in the 150 - 156 MHz band, is still used by Polish State Railways (PKP) along with many newer systems. The first dual mode (analogue/digital) radio system – the 450 MHz Zugfunk 2000, made by Kapsch – was deployed near Warsaw in the 1990s. PKP operates about 30,000 radios – stationary, mobile and portable – many of them made by Radmor, Poland's leading producer of radios for the defense industry. A special feature of the Radmor radios is a patented acoustic alarm signal that can be sent selectively to any or all trains or dispatchers within range. When a moving train receives the distinctive 3-tone signal, braking automatically begins.[212]

Portugal: The telecom regulator ANACOM authorised GSM-R use in 2008, but the first test installation – a single base station – was not made until 2012.[213] In April 2014, the rail infrastructure manager REFER invited firms to register for "future restricted or negotiated procedures" for the supply of GSM-R equipment, suggesting that build-out may soon begin.[214] Meanwhile, the older proprietary Radio Solo Comboio (track-to-train radio) is still used on most lines for voice and data communication. It is essentially a private cellular system using 4 channels in the 450 MHz band. Sampling converts the analogue signal to digital for backhaul when trackside optical fiber is available. But the limitations of the system are significant: the priority of each call is determined by the dispatcher and only one voice channel can be active at any moment within each section of track. Alarms are received by all stations but the 1200 bps data rate is archaic.[215]

Romania: With over 20,000 km of track, Romania has the 4th largest rail network in the EU. But after Ceauşescu it has been neglected, with an estimated €400 million worth of investments, repairs and maintenance work postponed as the budget deficit of CFR-SA, the infrastructure manager, grew year after year. An infusion of EU funds helped start ETCS Level 1 deployment in 2012 and the buildout of ERTMS continues along Pan-European Corridor IV. But legacy systems for communication (narrowband FM at 146.000 – 146.800 MHz) and for train control (INDUSI) still predominate.[216] Despite – or maybe because of – its financial constraints, Romania is an innovator in railway use of wireless broadband, just as it is in PPDR with its security services' WiMAX network: WLAN networks "cover every major railway depot in Romania and… enable communication between the depots and passenger coaches… the train management system of passenger coaches collects fault logs,

[211] "Government approves Dutch ETCS roll-out strategy", *Railway Gazette,* 14 April 2014, http://www.railwaygazette.com/news/infrastructure/single-view/view/government-approves-dutch-etcs-roll-out-strategy.html

[212] Przelaskowski, K. (2011) "Polish State Railways: Achieving a successful first GSM-R link", *European Railway Review,* issue 1-2011 (15 February), http://www.europeanrailwayreview.com/8195/err-magazine/past-issues/issue-1-2011/polish-state-railways-achieving-a-successful-first-gsm-r-link/

[213] Government of Portugal (2011) "Contrato 237706: Fornecimento, instalação e colocação em serviço do subsistema BSS do sistema GSM-R - Projecto Piloto", http://publicos.pt/contrato/237706; REFER (2012) "Primeira chamada GSM-R na rede ferroviária nacional", press release, 14 March, http://www.refer.pt/MenuPrincipal/ComunicacaoSocial/Noticias.aspx?View=Details&ItemId=387

[214] Diário da República Portuguesa (2014) "Anúncio de procedimento n.º 1792/2014", 2nd series, no. 65, https://dre.pt/pdfdiacp/2014/04/065/407735674.pdf

[215] Duarte Santos, A. J., *et al.* (2005) "Tracking Trains via Radio Frequency Systems", *IEEE Transactions on Intelligent Transportation Systems,* Vol. 6, No. 2, June, http://www.av.it.pt/nbcarvalho/docs/Revista26.pdf

[216] CFR-SA (2013) *Network Statement,* http://www.cfr.ro/files/ddr/eng/CFR%20NETWORK%20STATEMENT_pdf.pdf

and when detecting the depot WLAN network, the data package [is automatically] transferred from coach to depot…”[217]

Slovakia: Level 1 ETCS is only operational on a section of track near the capital Bratislava, but by the end of 2015 ERTMS should be deployed on most of the network. Until then and for some time thereafter, legacy analogue radio and train control systems will be used.[218]

Slovenia: In 2008 the Slovenian Ministry of Infrastructure was awarded €1.155 million from the EU's TEN-T programme to develop a national GSM-R implementation plan.[219] In 2013 the Ministry awarded a €117 million "turnkey" contract to Kapsch to deploy GSM-R on the country's 1,230 km rail network by the end of 2015, and then to service and maintain the network for 5 years.[220] Meanwhile, Slovenia continues using their analogue "radiodispečerskimi zvezami" (radio dispatcher communication) system which covers 80% of the tracks and uses 457.450 - 458.300 MHz paired with 467.450 - 468.300 MHz.[221]

Spain: The state-owned rail infrastructure manager ADIF has put 16,130 km of fiber optic cable along its tracks for its own communication needs and to provide backhaul for other telecom operators, particularly the MNOs. Thus they own about 25% of all the dark fiber in Spain, making them the market leader.[222] The track gauge used in Spain's rail network differed from the rest of Europe so tracks are slowly being modified to accommodate rolling stock of either gauge. Spain's ERTMS coverage is the most extensive in Europe, with ETCS Level 1 on about 1,300 km of track and Level 2 on about 700 km (mainly the high-speed lines). However, validation of the first Level 2 line did not come until mid-2014.[223] Therefore, multiple train control systems are still in use, and GSM-R coexists with the analogue Train-Ground radiotelephone system.

Sweden: The first commercial GSM-R deployment began here in 2000 and was completed in 2007. 10,700 km of track are now covered by about 1,200 base stations and 350 repeaters. But plans for implementing ETCS have been cautious since the existing train control system (ATP) is expected to remain viable into the 2020s. A special transition module was developed for onboard use which captures data from ATP trackside equipment and converts it into a format readable by ETCS. With this interim solution, full migration to ETCS is not expected before 2030.[224] Meanwhile, UIC's "low cost, low traffic" version of ETCS was pilot tested on 135 km of track which had been manually supervised.[225] More recently the first prototype ETCS Level 3 system was demonstrated.

United Kingdom: The GSM-R programme began in 2008 and buildout finishes in 2014. ETCS deployment begins in 2015 and the 197/205 MHz analogue National Radio Network will be replaced by GSM-R. Telecommunications regulator Ofcom is expected to rescind NRN's frequency allocation

---

[217] EKE-Electronics (2009) "EKE-Electronics to Deliver WLAN Depot Network for Coach Diagnostics to CFR Romanian Railways", press release via *Railway Technology,* 16 March, http://www.railway-technology.com/contractors/computer/eke-electronics/press12.html

[218] "Kapsch and AZD Praha to install GSM-R in trans-European train route in Slovakia", *Think Railways,* 29 April 2014, http://www.think-railways.com/kapsch-azd-praha-install-gsm-r-trans-european-train-route-slovakia/

[219] http://inea.ec.europa.eu/en/ten-t/ten-t_projects/ten-t_projects_by_country/slovenia/2007-si-60460-s.htm

[220] "Kapsch to supply GSM-R train communications to Slovenia", *Railway Technology,* 12 September 2013, http://www.railway-technology.com/news/newskapsch-supply-gsm-rtrain-communications-slovenia/

[221] Slovenske Železnice (2014) "Telecommunications", http://www.slo-zeleznice.si/en/company/infrastructure/rail_network/telecommunications; Zupan, U. (2014) "Network Statement of the Republic of Slovenia 2015", Slovenske Železnice, http://www.slo-zeleznice.si/en/company/traffic_management/network_statement/network_statement_for_the_republic_of_slovenia_for_2015

[222] ADIF (2014) "El negocio de las telecomunicaciones en Adif", http://www.adif.es/es_ES/infraestructuras/telecomunicaciones/telecomunicaciones.shtml

[223] "Spain's ADIF validates ERTMS on Albacete-Alicante line", *Railway Technology,* 5 June 2014, http://www.railway-technology.com/news/newsspains-adif-validates-ertms-on-albacete-alicante-line-4285955/

[224] UNIFE (2013) "Factsheet #14: ERTMS deployment in Sweden", http://www.ertms.net/wp-content/uploads/2013/12/FS18_ERTMS_Deployment_in_Sweden.pdf

[225] UIC (2011) "ERTMS regional pilot in Sweden, with a view to beginning commercial operation by the end of 2011", *UIC eNews* no. 242, 15 June, http://uic.org/com/article/ertms-regional-pilot-in-sweden?page=thickbox_enews

by 2015 and perhaps the 448/454 MHz Cab Secure Radio allocation as well.[226] The Channel Tunnel already has complete GSM-R coverage but currently all trains must be equipped with Cab Secure Radio, too.[227] Train control in the Channel Tunnel is based on TVM 430 plus KVB.

C.4 Post-GSM-R radio systems for railways

Principles for defining an appropriate post-GSM-R radio technology were given in the "Commission Staff Working Document on the State of play of the implementation of the ERTMS Deployment Plan":[228]

- The future ETCS data communication bearer should be IP-based.
- The basic goal is that the on-board ETCS, EVC, is installed once (with an IP interface) and not affected by any subsequent change in the communication technology.
- Therefore, the specifications of the ETCS application should be separated from the transmission layer (bearer specifications).
- Existing ETCS functions should be guaranteed.
- The future ETCS data communication bearer could also be used by other applications. It should not be designed in isolation.
- The system should be flexible enough to allow the use of multiple technologies. One could consider several (IP-based) bearers: GSM-R (GPRS/EDGE); WIFI, LTE, satellite, etc., but also simple digital (and cheap) technology. This could also foster the expansion of ETCS to other regions of the world.
- The R&D projects and cooperation with other sectors are critical and should not duplicate efforts.
- The following characteristics are important to be able to decide on the suitability of a candidate solution: QoS, capacity, availability (especially in dense areas), standardised solution (no '-R'), harmonious coexistence with public communication networks (resilience to interferences), affordability.
- Network ownership will have to be considered. There are various models possible, such as having a national dedicated network, a European dedicated network, or a public network. What is important is that the network will have to fulfil the ETCS requirements, regardless of who owns it.
- Spectrum assignment is a key point to be taken into account, considering that spectrum scarcity is a reality. The needs of railways have to be advocated in global fora, such as 3GPP for standardisation and the 2018 World Radio Conference, as required…
- The new communication system(s) must be defined in 2018 and must be available for deployment by 2022 at the very latest and they must ensure co-existence with and manage migration from GSM-R.

---

[226] Network Rail (2014) "The 2015 Network Statement", http://www.networkrail.co.uk/2015NetworkStatement.pdf
[227] "HS1 Network Statement", May 2014, http://highspeed1.co.uk/media/19591/hs1_network_statement__may_2014_.pdf
[228] http://ec.europa.eu/transport/modes/rail/interoperability/ertms/doc/edp/swd(2014)48-ertms-deployment-plan.pdf

Appendix D. Sample definitions of "mission critical"

Autorité de Régulation des Communications Électroniques et des Postes (ARCEP):

> "Une application dite « à mission critique » se dit d'une application qui doit tenir la charge et réclame un niveau très élevé en matière de fiabilité." [An application said to be mission critical is an application which must take priority and demands a high level of reliability]

European Conference of Postal and Telecommunications Administrations (CEPT):

> ECC Report 102 (2007), paragraphs 1.4.1 and 1.4.2: "The expression 'Mission Critical' is used for situations where human life, rescue operations and law enforcement are at stake and public safety organizations cannot afford the risk of having transmission failures in their voice and data communications or for police in particular to be 'eave-dropped'… Where communication needs are non critical: human life and properties are not at stake, administrative tasks for which the time and security elements are not critical."

German Project Group on Public Safety Digital Radio:

> "A mobile radio communication system must fulfil four key requirements in order to be usable for mission critical communication:
>
> 1. "The infrastructure must be resilient, redundant and highly available…
> 2. "Communication must be reliable…
> 3. "Communication must be secure…
> 4. "Point-to-multipoint communication must be supported…
>
> "If a mobile radio communication system does not fulfil the above four 'mission critical' requirements completely, then it can only be used for business critical communication. In general, commercial mobile radio networks are only capable of supporting business critical communication…"

Law Enforcement Working Party (LEWP):

> "Mission critical operations' for PPDR organisations address situations where human life and goods (rescue operations, law enforcement) and other values for society are at risk, especially when time is a vital factor.
>
> "This means we define 'mission critical information' as the vital information for PPDR to succeed with the operation.
>
> "'Mission critical communication solutions' therefore means that the PPDR organisations need secure reliable and available communication and as a consequence cannot afford the risk of having failures in their individual and group communications (*e.g.* voice and data or video transmissions)."

Radio Spectrum Policy Group

The RSPG's Report on Strategic Sector Spectrum Needs uses the phrase "mission-critical" in two contexts without attempting a dictionary-type definition: instead, the Report lists "applications and services that have been identified by PPDR users" as examples of mission-critical communication:

- "high resolution video communications from wireless clip-on cameras to a vehicle mounted laptop computer, used during traffic stops or responses to other incidents;

- "video surveillance of security entry points such as airports with automatic detection based on reference images, hazardous material or other relevant parameters;
- "remote monitoring of patients. The remote real time video view of the patient can demand up to 1 Mbit/s. This demand for capacity can easily be envisioned during the rescue operation following a major disaster. This may equate to a net capacity of over 100 Mbit/s;
- "high resolution real time video from, and remote monitoring of, firefighters in a burning building;
- "the ability to transmit building plans to the rescue forces."

TETRA and Critical Communications Association (TCCA)

"'Mission Critical' is defined as a function whose failure leads to catastrophic degradation of service that places public order or public safety and security at immediate risk. These systems are paramount to the operation of a nation's public safety and critical infrastructure services and are therefore required to have particular and adequate inbuilt functionality, availability, security and interoperability.

"In simple terms, Mission Critical users are those that are responsible for the health, safety, security and welfare of our citizens. Police, Fire, Ambulance, rescue services and specifically the Military would be classed as Mission Critical. Those that ensure the availability of Electricity, Oil and Gas, Water and Core Transport services, without which modern life would quickly degenerate, are also classed as Mission Critical…

"Mission Critical communication services are supplied by special communication solutions where reliability, availability, stability and security of the communication service are vital to ensure continuous availability of services that are critical to maintaining the wellbeing of society… Mission Critical communications include hardware, software, as well as communication facilities (including sufficient radio frequency (spectrum) capacity) to transmit and share information between users in the field and command centres, in a dependable and secure manner."

[US] National Public Safety Telecommunications Council Broadband Working Group

"The key elements for the definition of mission critical voice include the following:

- "Direct or Talk Around...
- "Push-to-Talk (PTT)…
- "Full Duplex Voice Systems…
- "Group Call...
- "Talker Identification…
- "Emergency Alerting…
- "Audio Quality…"

[US] Public Safety Advisory Committee

"A mission critical communication is that which must be immediate, ubiquitous, reliable and, in most cases, secure.

"EXPLANATION: An 'immediate' communication must be capable of being transmitted and received instantaneously, without waiting for a system to be set up, a clear channel or a dial tone. A 'ubiquitous' communication is that which can be transmitted and received throughout the area that the mission requires. A 'reliable' communication system must be designed, constructed and maintained such that short-term disruptions are minimal. Finally, security, while not currently available in many situations, is increasingly a requirement for law enforcement and other sensitive communications. In this case, ‘security’ is provided with ‘voice privacy’ encryption.”

EURELECTRIC

“In general within the framework of smart network management, all process control messaging services for the distribution system, for all generation systems (local or central) and all dedicated alarm control messages should be considered as ‘mission-critical‘ on a long term. Until such time as dedicated alarm control messages can be remotely generated (at downline or generation sites), monitoring messages from particular network locations may be “mission-critical” also… [It] is the expectation that, depending on the network design, the communication systems in the medium to lower voltage elements of network monitoring and control will also become more mission-critical in the (near) future. This does not automatically mean that the requirements of all systems are identical, and the level of criticality here is only below critical until such time as there are extremely high penetrations of DG [?] on LV [low-voltage] networks. These communications improve supervision and control and ensure power quality standards are maintained, but are ultimately not critical for safety and supply.

“…dedicated fixed lines like fibre optics networks [are] the preferred solution given the high level of requirements of mission-critical applications… Wireless connections are also becoming more important as mission-critical communication needs increase in the lower voltage sections of the distribution grid for control and monitoring through field devices at rural locations served by overhead network. In addition smart metering for customers in rural or less populated areas will primarily require a wireless solution. In both these cases, wired solutions are not economically viable and would not offer the service at the most critical time, when physical connection could be broken by network faults. Wireless solutions are also considered very suitable for connecting a large number of smart connections (in houses), as back-up system or as primary solution in cases where wired solutions are too expensive or not feasible for distribution automation. Wireless connections are likely to become more important as mission-critical communication needs increase in the lower voltage sections of the distribution grid.”

“Finally, Private Mobile Radio communication (PMR) should be considered as a mission critical communication tool for operational staff in case of blackout situations as mobile phone systems will be unavailable after some hours of breakdown.”

Appendix E. Final Presentation Workshop Summary

1. The workshop brought together nearly 100 representatives from a variety of stakeholders, which included the emergency services, utilities, transport, national regulatory agencies (NRAs), mobile network operators (MNOs), private mobile radio (PMR) operators and also equipment suppliers. It had two main objectives - first to present the findings of the study and secondly to gather feedback and views from the stakeholders.

2. Chairing the meeting, Andreas Geiss (DG CNECT, Head of Unit B4), who noted that the subject was of increasing interest, especially with the apparent savings available from commercial networks and with decisions apparent at WRC-15, the major session on the findings began.

3. The study team made a concise presentation explaining the findings, and outlining the key questions the study was expected to review.

4. Simon Forge began with the conclusions on four key questions:

    - Could LTE technically provide the mission critical functions and features necessary to replace current TETRA networks which are largely voice oriented?
    - Could hardened LTE do that at reasonable cost?
    - Is hardened commercial mobile LTE less costly than a dedicated LTE network?
    - What is the reality of the network supplier position? – Can MNOs be trusted to deliver on their undertakings in commercial agreements for a mission critical environment for operations?

The above questions analysed and answered the two basic issues that confronted the study - to what extent and at what cost (in financial and non-financial terms such as safety of life and social acceptance) can commercial cellular networks provide the functionality, coverage, bandwidth and reliability needed by “mission-critical” communications of PPDR, as well as ITS and Utilities? And to what extent can the economies of scale of global mass markets for commercial equipment be exploited to reduce the investment and operational costs for the provision of "mission-critical" high-speed broadband communications?

The main conclusion put forward by the study was: the commercial MNO networks will be a feasible option, technically and financially, ***BUT ONLY IF*** a specific regulatory structure is developed to assure their service level commitment. Without this structure, the risk may be too high and all three user sectors are highly reluctant to become completely dependent on the MNOs.

Simon Forge then outlined five possible options that were considered in the study, with their value assessments and relative costs comparisons, for:

- Dedicated specialised networks using specialised equipment only
- Commercial networks using commercial equipment only
- Dedicated specialised networks using commercial equipment

- Hybrid solutions involving dedicated specialised and commercial networks

- Common multi-purpose network for use by all three sectors simultaneously

5. Robert Horvitz went on to describe the study's understanding of the concept of "mission critical", the requirements of the three relevant sectors (PPDR, utilities, and ITS) and examples from the six case studies in outline. He also noted that the ENISA reports had given a calculation method for the level of the harm that mobile network outages cause and that equipment standards and plans for improving network resilience could be driven by this.

6. A discussion lasting over two hours was then opened up to the floor and the following comments were noted.

7. An attendee from a police organisation in the PPDR sector first put forward the view that the main conclusion should be reversed (on Slide 6) – ie that the commercial networks could NOT be used. Only if the MNOs were constrained by suitable regulation then perhaps a possibility of their utility in mission critical services could be foreseen.

8. A stakeholder from the utility industries then put forward the point that one condition should be turned around – reservation of spectrum for mission critical uses. Employing commercial networks meant that dedicated spectrum would not be needed and so existing allocations would be given up, perhaps to the MNOs. But if the MNOs failed to deliver, then that spectrum would be lost and none would be reserved for the mission critical sectors, which could be left stranded. Moreover the MNOs were claiming 1200 MHz for commercial use while the DTT broadcasters wanted 200MHz but the mission critical users claimed only a small faction of that at between 10MHz and 30MHz (eg for 2x15 MHz). In conclusion, reserved spectrum was essential, in case of letdown by MNOs.

9. The Chair noted that the enormous diversity on which bands were available across the EU Member States (MS) and that a common choice was not straightforward as each national situation on appropriate spectrum choice was different.

Moreover the EU does not expect to have binding EU measures or choices of spectrum for mission critical operations.

10. However the report does call for guidelines to support MS in making choices over the regulatory conditions to be applied for MNOs offering mission critical services. If followed, the EU must pick a way through the different MS requirements and budgets available in advancing these proposals on use of the MNOs. Moreover subsidies must be given by MS, if this way forward is chosen so the MS will need guidance. It would be beneficial if those stakeholders present could provide comments on what these guidelines should be.

11. The Chair also noted that the contention that 2x10 MHz was a small amount of spectrum was debateable – it depends where ist is in the spectrum – and so is it really so small?

12. An attendee from the ITS sector then noted that a further key point to emphasise was interoperation at EU level, not MS as the Chair had acknowledged. Running railway services across all MS faced major obstacles in terms of common radio communications. Interoperability between the railways in different MS was of paramount concern. A clear direction from the EU (in fact the EC) was needed to provide a complete and rapid solution. If the decisions are made at MS level then the railways would all lose interoperability.

13. Robert Horvitz emphasised that the ETSI 3GPP group wanted to extend LTE functionality for all the three sectors and the efforts on standardisation of this group needed to be strongly encouraged. It was only limited by the resource commitments of its members.

14. A stakeholder from the PPDR community noted that the emergency services already outsourced fixed line services to commercial operators satisfactorily, under the existing regulatory structure and this was an example of using commercial suppliers successfully.

15. An attendee from an NRA thanked the team for the report and suggested that the meeting take a more positive attitude on the role of MNOs. The various commentators should not underestimate the capacity of the report's readers to understand the conditions being called for. He also noted that signal levels and coverage of LTE in his own MS was higher than cited in the report.

16. A leading supplier of telecommunications equipment noted that WRC-15 conference had PPDR allocations as an agenda item, which would not return for many years. Thus a consolidated EU-wide view was necessary. The onus was on the NRAs to change the worlds of PPDR and perhaps of the MNOs by introducing suitable proposals for PPDR working.

17. An MNO noted that what they saw in the next WRC-15 round of spectrum awarding negotiations was extremely difficult to predict.

18. A representative of an organisation for small PMR operators in one MS noted that coverage must include those occluded premises such as tunnels and underground spaces where mission critical operations were also needed. These ranged from tunnels for public transport to nuclear plant sites and that consideration of radio networks in enclosed zones must be considered as well.

19. A delegate from a PPDR organisation noted that there would need to be a detailed analysis of what has to be done to a commercial mobile network to make it suitable for PPDR needs. Guidelines are not enough. Moreover, the MNOs will not be imposed on – they will refuse to co-operate. The need for broadband will come in over the next 3 to 5 years far more strongly than today. In these circumstances it could be that broadband is never available on a mission critical network basis. The only way to change behaviour of MNOs would be via conditions onl the frequencies they depend on.

20. Interoperability across the services also needs to be emphasised – perhaps more iin the study. Harmonised spectrum (across the EU) would be one way of assuring interoperability – that would imply dedicated mission critical spectrum.

21. The Chair noted that dedicated spectrum was not enough. Those calling for dedicated spectrum were not taking into account the cost elements, as examined in the study and that nobody would pay for the dedicated infrastructure to go with the spectrum. That investment is equally crucial.

22. A delegate from a leading supplier of PPDR telecommunications equipment noted that when all the spectrum was auctioned off to MNOs, the governments and mission critical services would have lost control. The fear is that it cannot be taken back. Moreover a dedicated network is not the same as dedicated spectrum – the spectrum is more final when lost.

23. A representative of a government MVNO offering PPDR TETRA services over a dedicated network plus outsourced services for data and broadband via MNOs noted that the dedicated spectrum acted as back-up. Use of commercial MNOs was a real opportunity. But the fallback was there just in case, as the MVNO had its own PPDR spectrum, for voice.

24. Fire services across the EU needed to use the MNOs as they were constantly out of coverage of their own dedicated networks and wanted to apply broadband video and data increasingly in their work. A representative from an association of 22 EU fire services noted they still needed voice communications and would like control of their own dedicated spectrum for that. However, the fire services were constantly out of coverage of their own PPDR networks and needed to use the commercial networks in such cases.

The question was – how should this be effected, ie what was the next step? – Would and could the European Commission give guidance here?

25. An attendee from a major PPDR service noted that broadband services were needed in the short term and that services from the MNOs were not enough. The PPDR services wanted dedicated spectrum, and suitable networks for broadband data as soon as possible. Also, all Mission Critical users needed to share such networks to reduce costs.

26. Another PPDR delegate noted that dedicated spectrum did not mean dedicated networks necessarily but that government would retain control of the spectrum allocation. If all the frequencies are auctioned off to MNOs then control is lost. The same is true for the utilities' and railways' needs. Unless certain essential measures are taken, control will be lost. The choice of spectrum was the next step and whether it would be 400MHz or 700MHz would make a difference to network planning but should be one of those. The hybrid solution seemed attractive but would be more expensive.

27. The attendee from an equipment supplier noted that the re-use of existing TETRA sites and some of its equipment for LTE technology could not extend to re-use of the antennae, which are quite different for LTE especially with MIMO functions.

28. A representative from an organisation monitoring the resilience and performance of the commercial networks noted that use of the commercial PLMNs must be included in risk assessments for national security.

29. The representative of a government PPDR MVNO noted that use of a mix of MNOs would be the optimal network for all Member States. But it would be a new type of MNO that combined mission critical services with commercial sales, like ASTRID in Belgium. The hybrid option offered a way forward despite being more expensive and complex as re-use of current TETRA networks were possible. The hybrid model was the way forward, even if the way forward was development through the MNOs, a hand over parallel phase would be needed. That implied dedicated spectrum was required, with its dedicated base stations. There have been some problems in that such spectrum reservations may not have always been used and so have remained idle. The solution might be to share spectrum across dedicated and commercial networks BUT to have the facility for pre-emption for mission critical communications, as having a higher priority.

30. An NRA asked what would be the effect of such new initiatives of mandating the MNOs to take mission critical responsibilities. Would that undermine existing contracts that are in place? Were 15 to 30 year contracts necessary – or could shorter contracts such as 5 years be used instead? What incentives would there be in a long term contract to maintain the service levels?

31. Simon Forge replied that in socio-economic terms, the time was right to reconsider all options. NRAS and governments would have to take a view on current contracts and on future assignments, especially with new spectrum developments such as the release of the 700MHz band. These new commercial contracts as well current contracts should be under review. On the question of length of contracts, all three sectors had strongly emphasised their need for stable long-term networking

and therefore long-term network partners, in a mode quite different to the commercial contracts of the past.

32. An attendee from an electricity utility then noted that their position was to take over ownership of a 450MHz CDMA operation and run it themselves, but use a local MNO to operate the network. This was necessary as the mobile market did not deliver what they needed in long-term service and resilience. The position put forward in the report of use on the MNOs contained too many ‘ifs’. Utilities in the EU are under pressure to roll out millions of smart meters in the near future and the cost driver is the total price of connection of each, which must be of the order of Euros per year. The utility was planning 3 million units and had just added another 2 million. Control of their own private mobile network was the only way to cope with that.

33. A representative of a national utility considering the use of MNOs as part of a network for smart grids noted that spectrum was a negotiating tool with the MNOs.

Spectrum control should be considered as a risk management tool with the MNOs. However utilities also require a tactical system, to be deployed when all else fails, ie their own back-up that they can control. Some of the proposals put forward in the report will take time to implement, so testing with the MNOs needs to start now on operational reliability, resilience capability and consistency of service levels offered in the long term. In general, whatever path were chosen, harmonised EU spectrum would be essential to lower costs

34. A representative from an NRA noted that any solution must consider all the 28 EU MS. Looking at one simple solution across all the EU MS just would not work. Many of the views put forward reflected specific national perspectives and all MS were different. MS varied in population, preparation to pay for mission critical services, size of networks, functional requirements, etc. Moreover, the simple preference of dedicated over commercial was not the choice as the two were not comparable in offerings or value for money.

35. The Chair then put forward a proposal for comment of making a call for tender, in order to determine a price tag for the willingness of MNOs to co-operate on specific conditions. Replies to such a tender would indicate the degree of market interest.

36. A delegate from a PPDR service noted that it would be interesting to see such a tender to price co-operation. But if it contained no dedicated networking with its spectrum then the service would fail, leaving MS without a solution.

37. A representative from the government administration managing a major PPDR rollout noted that it would be surprising if long-term contracts could solve anything. Their own experience had been that the providers may suddenly change business plan/ and or ownership and that there would then be a struggle with big business to force compliance. Moreover large contracts were difficult to dominate. Change requests for mission critical requirements, for instance, were highly problematic to pursue. The commercial providers would only follow the movements of the stock market and the demands of their shareholders.

38. Such tenders were already being seen in the UK, stated the representative of a mission critical industry association.

39. The UK regulator noted that the agency supported this tender process and the emergency network initiative, but worked at arms length with the Ministry involved.

40. The representative of a university research group examining LTE for mission critical networking noted that one network provider for all services across the three sectors could raise difficulties and so specialist network providers would be needed for certain services. Hence services should be categorised in a layered classification, to prioritise them. Then the provider of the service could be chosen. The services themselves should be categorised with high priority receiving most bandwidth.

41. The attendee from a smart grid network supplier for SRDs noted that the difference between 99% and 99.999% was enormous in costs and in technical capabilities, while the work items being studied by the 3GPP initiative for hardened LTE were limited.

42. An attendee from a mission critical equipment supplier noted that the wireless Internet access afforded by MNOs via 2G connection and handset offered an unguarded entry point for access to the whole MNO network operation, including any prioritised LTE systems.

43. Simon Forge replied that security was always a moving target and should, ideally, be built in at the architectural level, but that did not stop new developments in security being incorporated in LTE networks for mission critical purposes. He noted that in the banking industry, measures used 10 years ago for large-scale inter-bank transfers had been superceded several times over the last decade as new security threats had been identified. The same process of replacement was likely to be used in mission critical networking over several decades.

44. The representative of a European industry association for the utilities noted that pricing for a specific service was equally important. The cost per year for the utilities' smart grid monitoring sensors and actuators had to be under 10Euro/year, yet it was crucial to have priority over consumers' traffic, which is not an offering that the MNOs would be likely to make.

45. Moreover it is not as if the money is not there to build dedicated networks – in the UK for instance, there is a €14 Billion project to install smart meters, but there no public demand for such a scheme, yet the funds are available. So the funds for more expensive dedicated networks should be available.

46. Then on the question of the dedicated spectrum required, the mission critical services are only asking for some 20MHz or 30MHz - which is less than some 2% to 3% of the 1200 MHz that the mobile industry is demanding for LTE.

47. Moreover the versions of LTE in Releases 12, 13 and 14 can be used equally well in a private network as in a commercial one.

48. Use of commercial mobile may lead to competition inefficiencies, especially if one MNO is subsidised while others are not. This would also lead to inefficiencies in infrastructure support if all 3 or 4 MNOs in each MS had to receive government subsidies. The alternative could be to subsidise only one MNO - which be preferential state aid. More generally, the move to subsidised hardened networks would seem to go against the principle of infrastructure competition in mobile networks on an equal basis.

49. In the UK, the Ministry concerned seems to be happy with the competition inefficiencies its initiative based on commercial networks could engender. Is competition law being taking account of adequately? The commercial MNO-based emergency network project also contrasts with the situation in one part of the UK, Northern Ireland, where a mission critical network for the emergency services continues under public sector ownership and management. So 2 contractual models are in use.

50. A PPDR representative asked what would be the commercial situation if the government offers the frequencies it owns, but retains ownership of them, while they are being used by a commercial operator. It is well to note that most countries in the EU are looking at a hybrid model as they wish to continue with TETRA/ TETRAPOL for some time into the future. Moreover there are the restrictions at European level on financing one MNO against another that would have to be resolved if all of the national MNOs are not involved.

51. A further PPDR spokesperson put forward the increasing need for cross- border operations seamlessly. Thus they have been looking at using the commercial public mobile networks. The frequencies needed for this must be closely looked at if it is to work. Their organisation has starting working on the concept of a regional network, not just a national one. Thus the 700 MHz seems the most suitable choice – as any dedicated use could more easily overlap with commercial if need be – as recommended in the report.

52. The Chair noted at this stage that the retention of dedicated spectrum for reasons of control purely was a motive driven by the past and by current experiences of commercial mobile. The future may not be the same. There is a need to understand the individual plans in this arena of all the Member States across the EU. There is also the possibility of using LTE in dedicated networks, and LTE is conducive to this as explored in the report. Evidently there will be strong support for hybrid networks across the EU, in which commercial tenders will be involved and so their participation can be tested. Evidently it would be necessary to design tenders such that they impose the relevant conditions, as outlined in the study. More discussion will now be necessary at Member State level on the ways in which Europe will move forward here.

53. In a closing summary, the Chair stated that, the meeting appeared to be keen to obtain further views from the European Commission on just what the EU guidelines would be for managing a commercially based mission critical network successfully. These EU guidelines would not be legally binding but should be based on subsidiarity principles, with the aim of offering guidance to MS and NRAs in drawing up both their regulatory framework for operating such networks with MNOs and their contract conditions.

European Commission

Is Commercial Cellular Suitable for Mission Critical Broadband?

Study on use of commercial mobile networks and equipment for "mission-critical" high-speed broadband communications in specific sectors.

Luxembourg, Publications Office of the European Union

2014 – 266 pages

ISBN: 978-92-79-38679-4

DOI: 10.2759/54788

CATALOGUE NUMBER
KK-04-14-644-EN-N

DOI: 10.2759/54788 ISBN: 978-92-79-38679-4