1

OVERVIEW

This chapter provides an overview of public safety networks and critical communications systems. It is intended to be an executive summary. To provide a complete *picture*, some of the material (figures, text, etc) in other chapters are repeated here.

1.1 BACKGROUND

This book is a comprehensive treatment of technologies and systems used and to be used in public safety networks and mission-critical communications systems. The book also covers economic, financial, and policy issues as well as the design, deployment, and operation of such networks. Before we go further, let's explain what we mean by these networks:

> A **public safety network** is a communications system used by the agencies involved in public safety affairs. The communications system used by a police department is an example of a public safety network. Typical functions include first and emergency

Fundamentals of Public Safety Networks and Critical Communications Systems: Technologies, Deployment, and Management, First Edition. Mehmet Ulema.

responses to wide-scale natural disasters such as earthquakes, forest fires, flooding, and man-made disasters such as nuclear explosions, radiation, terrorism, as well as localized emergencies such as automobile accidents, fires, medical emergencies, and any other threats to public order. (Note that in Europe, the term PPDR, short for Public Protection and Disaster Relief, is used to refer to public safety and first responders networks).

A **mission-critical communications system** is a network used by organizations to provide communications infrastructure to carry out mission-critical functions. The communications system used by workers at a large construction site is an example of a mission-critical communications network. Mission-critical communications networks have been used in various sectors, such as construction, transportation, utilities, factories, and mining operations. (Note that in some literature, the term "mission-critical communication" is used to refer to the communications systems used by law enforcement and emergency services as well [1]).

Although public safety networks and mission-critical networks differ in scale, design, deployment, and operations, the technologies used by both types of networks are highly similar. Therefore, in this book, we adopt the words "critical communications" to refer to both public safety and mission/business critical communications systems and networks. Occasionally, we may use these names interchangeably.

Critical communications systems include a telecommunications network with wireless and wired components, a set of services and applications, a variety of end-user devices, as well as some operations support systems, also known as network management systems. Critical communication systems also make use of radio frequency bands to exchange voice, data, and multimedia applications needed to carry out their "critical" functions as well as to transmit and receive information among users in the field and technicians at command centers.

Figure 1.1 gives an idea of market segmentation of the critical communications field for a specific narrowband technology, namely Terrestrial Trunked Radio (TETRA).

What sets a critical communications network apart from a commercial communications network? Perhaps the most dominant characteristics of critical communications networks are that they provide the basis for *situational awareness* and *command and control* capabilities, which roughly translate into the following capabilities [3]:

- prioritize delivery of mission-critical data (e.g. bring the dispatch data into the field: ability to send more and detailed information to the officers in real time),
- survive multiple failures (robust, even in extreme conditions; site hardening; enhanced physical protection and battery back-up; redundancy [intra-network, inter-network; fallback to other networks when needed]),
- maintain data integrity and confidentiality (end to end full encryption; link security—both user and control planes; network operations and management security including related data),

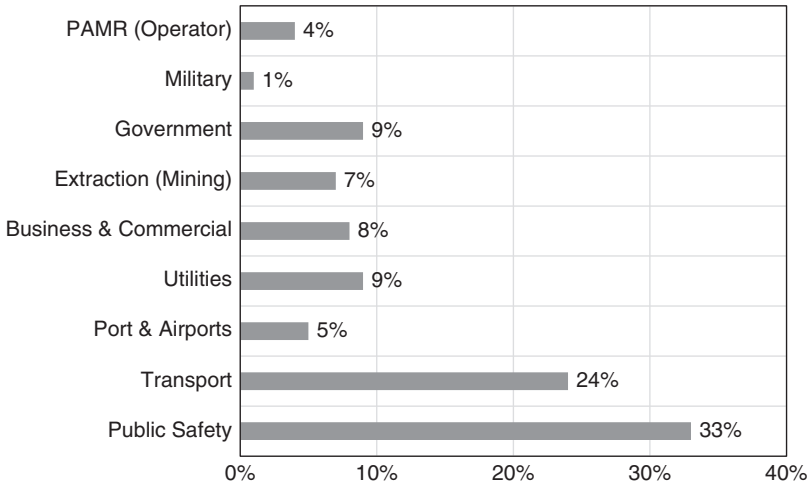


Figure 1.1. Sectors with TETRA-based critical communications [2].

- offer the essential coverage and capacity required (geographical coverage, not population coverage; symmetric usage [uplink-downlink] pattern, as opposed to downlink heavy commercial pattern),
- interoperate with other networks and extend coverage and capacity when needed (to enable communication among users outside network coverage, and to secure wide area communication even when users are outside normal network reach), and
- provide right to use and identity management support for officers, applications, and devices (to provision users with "right to use" of resources; dynamic priority and resource management for users and applications).

Many of the existing critical communications technologies have been in use for about 20 years now. They are mature, reliable, and relatıvely cost-effective in supporting critical voice applications. However, they are not designed to provide higher bandwidth supporting multimedia applications, which are requested by public safety agencies. Many countries have initiated projects to develop dedicated, nationwide public safety broadband networks to address these and other issues. For example, an authority called First Responders Network (FirstNet) was created in the USA in 2012 to establish such a national public safety broadband network.

Various industrial sectors having critical communication networks are also going through similar evolutionary phases. Superior capabilities and economy of scale offered by broadband technologies provide a rather attractive solution for upgrading the existing systems.

The standards organizations responsible for developing narrowband technologies has stated publicly that their future strategy is to be involved in developing Long Term Evolution (LTE)-based solutions for critical communications systems. However, it is expected that this transition will take a long time. While several countries have been planning for an LTE-based system, procurement activities for establishing nationwide systems based on older technologies such as TETRA and Project 25 are still taking place. The same trend is true in many other sectors as well.

Therefore, the primary objective of this book is to provide comprehensive coverage of the existing public safety technologies as well as the other technologies considered for future plans. We hope that the book becomes a valuable source for designing, deploying, and managing critical communications networks based on the narrowband and broadband technologies used in (or planned for) public safety networks and mission-critical communications systems.

Note that "national security" and "public safety" are two related, but separate topics. National security is mostly concerned with external/internal threats, whereas public safety concerns include natural disasters, accidents, and deliberately harmful acts.

1.2 TECHNOLOGIES USED IN CRITICAL COMMUNICATIONS

Old analog critical communications radio technologies have been replaced in most of the world by narrowband, all-digital, and voice and data technologies. Currently, narrowband digital radio systems are the primary technology used by public safety agencies and by many sectors. These systems are referred to as Land Mobile Radio (LMR) or Private Mobile Radio (PMR) systems, which are based on mainly Project 25, TETRA (and its variations), and Digital Mobile Radio (DMR) standards. TETRA has been the choice of public safety agencies and commercial and public organizations mainly in Europe and Project 25 technologies have been used mainly in North America. DMR-based systems, a newer narrowband, all-digital, standard technology, have also been chosen in some regions.

Partly due to the availability of commercial broadband applications, and partially due to increasing demand by public safety agencies, the possibilities of broadband data services for public safety networks are being discussed increasingly in many developed countries, including the USA and European countries. LTE technology is at the center of this new trend [4, 5].

1.2.1 Narrowband Land and Private Mobile Radio Systems

Project 25 is the code name for a technology based on the standards developed by the Telecommunications Industry Association (TIA) with the participation of the member organizations of the Association of Public Safety Communications Officials (APCO) and US federal agencies. More than 80 countries around the world have adopted

Project 25. Also, about 40 companies provide Project 25-compliant equipment and applications [6, 7].

TETRA is the code name for a technology based on the standards developed by the European Telecommunications Standards Institute (ETSI). TETRA is a trunked radio system, which became widely used in Europe first, then in many countries around the world. TETRA and Critical Communications Association (TCCA) estimates that more than 250 TETRA networks in more than 120 countries are deployed as of June 2016. TETRA uses TDMA technology with four user channels on one radio carrier. Packet data (low speed), as well as circuit data modes, are available. TETRA Enhanced Data Service (TEDS), included in TETRA 2, enables more data bandwidth to TETRA data service users. Although the standard is designed to provide up to 691 Kbps, in practice, users typically get a net throughput of around 100 Kbps. The low data rate is partially due to limitations in spectrum availability [8–10].

There is also another narrowband LMR technology, called TETRAPOL, which should not be confused with TETRA. TETRAPOL, not as popular as TETRA, is also a digital, cellular trunked radio system for voice and data communications with critical communications applications in mind. TETRAPOL was initially developed by a French company called Matra Communications. Today, TETRAPOL Forum leads the support and further development of TETRAPOL technology. TETRAPOL's air interface is based on FDMA and GMSK modulation; 12.5 kHz carrier spacing, along with 10 kHz carrier spacing, is available [11].

DMR is the code name for a technology based on another ETSI standard for PMR and used in Europe and several regions of the world as a low-cost entry-level radio system for commercial and public safety use. DMR offers a quick and cost effective replacement for analog systems with all the benefits of a digital solution. DMR provides voice, data, and some supplementary services [12–15].

Table 1.1 provides a comparison of significant features of Project 25, TETRA, and DMR technologies.

Among these three narrowband digital technologies, Project 25 and TETRA have been around for more than 20 years. Therefore, there is a mature, tested, interoperable

TABLE 1.1. A Comparison of Project 25, TETRA, and DMR Features

Functionality	P25 Phase 1	P25 Phase 2	TETRA	DMR
Standards Organization	TIA	TIA	ETSI	ETSI
Channel Access Method	FDMA	TDMA	TDMA	TDMA
Channel Bandwidth	12.5 kHz	6.25 kHz	25 kHz	12.5 kHz
Raw Data Rate	9.6 Kbps	9.6 Kbps	36 Kbps	9.6 Kbps
Number of Time Slots	N/A	2	4	2
Direct Mode	Yes	Yes	Yes (DMO)	Yes (Tier 1)
Repeater (Talk-Through) Mode	Yes	Yes	No	Yes (Tier 2
Trunking Mode	Yes	Yes	Yes (TMO)	Yes (Tier 3)
Analog Fallback	Yes	Yes	No	Yes

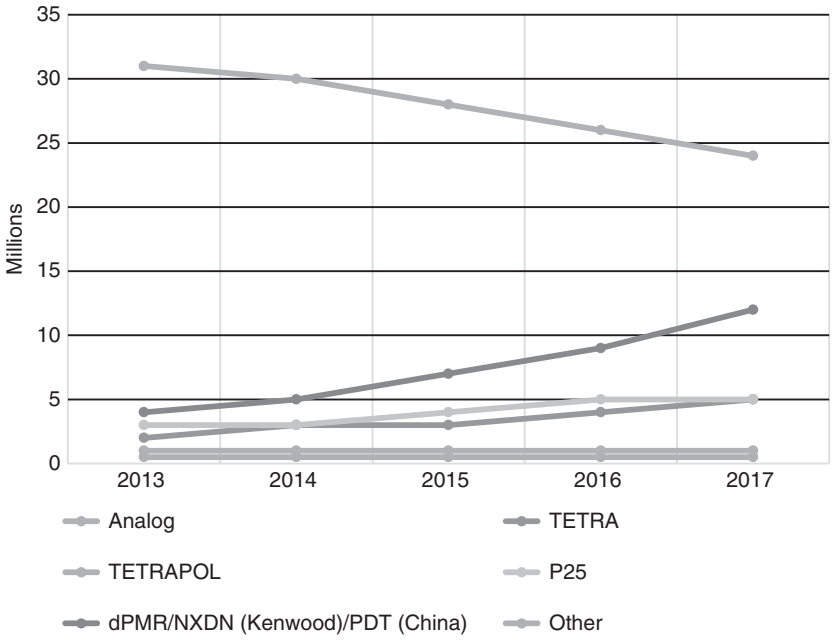


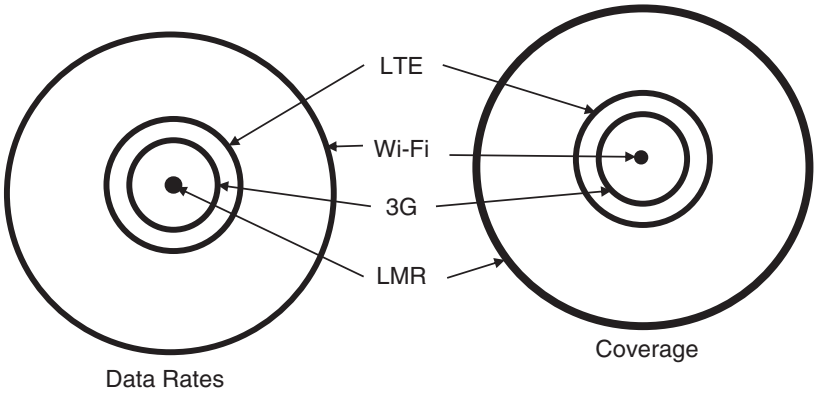
Figure 1.2. Global LMR subscriptions by technology: 2013–2017 (in millions) [16].

set of products available from many vendors. As shown in Figure 1.2, TETRA is the most widely used. Therefore, it is expected that equipment cost will be relatively lower than that of Project 25. DMR solutions may cost even less due to their less complicated architecture.

Project 25, TETRA, and DMR technologies are limited to providing data rates around 9.6–36 Kbps, which is rather slow to handle today's data-intensive applications, which require several megabits per second (Mbps) data rates. Therefore, public safety agencies have been looking into mobile broadband technologies to provide higher data rates [2, 17]. Lower indoor and rural handheld coverage and limited interoperability are some other design and economical limitations of these narrowband systems. ETSI and TIA agreed to work on a joint project called MESA to produce some specifications for a broadband standard for the critical communications ecosystem [18]. However, this was abandoned later on with the emergence of the concept of using LTE technology for critical communications systems.

1.2.2 Broadband Technologies for Critical Communications

Many public safety agencies around the world have been already using commercial broadband services (such as 4G and Wi-Fi) for data in conjunction with their



3G: Third Generation
Wi-Fi: Wireless Fidelity
LMR: Land Mobile Radio
LTE: Long Term Evolution

Figure 1.3. Coverage versus data rates [21].

voice-critical LMR systems. Furthermore, smartphones, tablets, and laptops have already been included as end-user devices by many agencies.

Although there are some different commercial mobile systems (such as Wi-Fi, WiMAX [19], and LTE) that are qualified as broadband technologies, there is a worldwide consensus that LTE is the technology choice for next generation critical communications systems [20–22] (see Figure 1.3 for a comparison of two important aspects of networking for some technologies). The US government recognized this and decided in 2009 on LTE as their platform for a national public safety network. Many other countries including China, England, Germany, Australia, and Qatar have also been focusing only on LTE-based public safety networks [16, 23–33]. Therefore, this book focuses on LTE-based broadband critical communications systems.

LTE is the only accepted technology worldwide as the fourth generation (4G) of mobile broadband communications systems. It is an evolution of second generation (2G), Global System Mobile (GSM), and third generation (3G) Wideband Code Division Multiple Access (W-CDMA) technologies. LTE-Advanced (LTE-A), the next version of LTE, is the "true 4G" because unlike ordinary LTE, it meets the 4G system requirements (such as higher speed) set by the International Telecommunication Union (ITU) [4]. LTE-A provides better coverage, greater stability, and faster performance. LTE-Advanced supports up to 100 MHz bandwidth and 1–3 Gbps (downlink) peak data rate (note that these are theoretical numbers). Carrier aggregation, one of LTE-A's capabilities, allows operators to combine their separate narrow channels into one broader channel [34] (LTE delivers data using a contiguous block of frequencies up to 20 MHz wide). This feature results in significant performance gain

TABLE 1.2. A Comparison of LTE and LTE-A Features

		LTE	LTE-A
Transmission Bandwidth (MHz)		≤20	≤100
Peak Data Rate (DL/UL) (Mbps)		300 (low mobility) 75 (high mobility)	1000 (low mobility) 500 (high mobility)
Latency (ms)	User Plane	<6	<6
	Control Plane	50	50

LTE, Long Term Evolution (per Release 8); LTE-A, LTE-Advanced (per Release 10); DL, Down Link; UL, Up Link; MHz, MegaHertz; ms, millisecond.

since the bandwidth available to a mobile device is now much larger [5, 34, 35]. See Table 1.2 for a list of three significant features of LTE and LTE-A.

LTE is growing rapidly all around the world. Reference [36] reported that LTE reached 270 million subscriptions and that number is projected to increase to around 1.3 billion by 2018. As of June 2014, LTE was commercially available on 146 networks in 107 countries. Additionally, as of June 2014, LTE-Advanced was commercially deployed on nine networks in seven countries worldwide [36]. As of June 2016, the same reference [36] reports that there were 1.29 billion LTE subscribers worldwide. It also reports that as of June 2016, there were 118 LTE-Advanced networks in 54 countries. They all point to the fact that LTE has been grown rapidly and is being adopted worldwide.

Building a new LTE-based network requires many billions of dollars. The site acquisition and site deployment associated with the radio access network require heavy spending. It is very crucial to prepare an efficient site deployment strategy by considering how to maximize coverage with less number of sites. The use of existing infrastructure is highly crucial. Also, any revenue generation opportunity, such as partnerships with utility companies, and commercial carriers should be seriously considered.

However, there are a few issues related to using LTE for critical communications systems [37]. A major one is the support (or lack thereof) of mission critical voice and Direct Mode Operations (DMO), which allow first responders to communicate directly with others when the infrastructure is not available. Some commercial LTE networks are used mainly for data and multimedia applications. For voice applications, the existing, older technologies (e.g. 3G networks) are used. While Voice over LTE (VoLTE) has been standardized and several commercial deployments have taken place, it is still not widespread [5, 38, 39]. It may take some time for VoLTE and DMO to become widely implemented and deployed. An example of a mission-critical voice application is "group calling," which allows a large number of first responders to be included in the same conversation.

The "3rd Generation Partnership Project" (3GPP), the standards developing organization that has been developing LTE technology related specifications,

has been actively involved in incorporating critical communications related features into upcoming LTE specifications, including device-to-device communications [40–45].

The future beyond LTE-A is highly promising as well. There has been a plethora of talks and activities to define the requirements of the fifth generation (5G) of mobile cellular technologies, which is envisioned to increase capacity and performance in order of magnitude compared to that of the current systems [46]. The current estimate is that 5G-based commercial networks will show up around 2020. Additionally, other technologies such as the Internet of Things (IoT), augmented reality, etc., may become a part of 5G and be commercially available. When and if these broadband-based technologies become available and commercially (read economically) viable, it is expected that critical communications systems will make use of these new technologies as well.

1.2.3 Interoperability

One of the weakest links in the current critical communications, especially in the public safety area, is interoperability [47, 48]. In many countries, there are no centralized common public safety networks that all agencies can use. It is most likely that different agencies use different communications technologies (interoperability problems may still be present due to differences in implementation, operation, and even jurisdiction; see Figure 1.4 for a comical depiction of the interoperability concern). Natural and manmade disasters have showed us that all agencies cooperating during such disasters must be able to communicate to be able to help the public. Therefore,

Figure 1.4. An example of interoperability solutions [49].

interoperability among all the networks (regardless of the technologies) used by all agencies is a paramount interest.

Currently, a makeshift arrangement is used for interoperability between two or more incompatible radio systems (e.g. "analog patching" between networks). Proprietary solutions also include interoperability via gateways, which use the same protocol for translating voice and data. This facilitates radios and protocols with different technologies to communicate.

The word interoperability is a loaded one. Its most comprehensive definition includes "governance, standard operating procedures, technology, training/exercises, and usage of interoperable communications" [22]. From the communications aspect, the word is used to mean that, for a given standard technology, the components built by different manufacturers work together. For example, an agency building a Project 25-based network acquires equipment from vendor X and vendor Y. The agency would want some guarantee that this equipment provided by two different vendors works when they are connected. This is typically verified by a set of *conformance* tests. All the technologies mentioned in this book have a set of well-defined procedures and standards to obtain *certificates* to prove the interworking of the equipment built by different vendors.

The same word, "interoperability," is also used to mean that different networks owned by different agencies work together. For example, an agent on network A should be able to communicate with another agent on network B. Network A and network B could be based on the same technology or each may be based on a different technology.

There are a bunch of interfaces and capabilities required for each technology to make it work with other technologies (this should include the networks based on analog technologies, which may be around for a while) (Table 1.3).

Also, applications, administration, operations, and security systems of each network should be configured to interoperate. Furthermore, public safety agencies may use a commercial landline and mobile network as well as Wi-Fi networks, especially during emergencies. Therefore, interoperability scenarios should also include these types of networks [21].

The Project 25-based system is already backward compatible with the existing DMR and other analog systems [22]. Furthermore, interoperability with commercial

TABLE 1.3. An Illustration of Possible Interoperability Scenarios

	Analog	P25	TETRA	DMR	LTE
Analog	x	x	x	x	
P25	x	x	x	x	x
TETRA	x	x	x	x	x
DMR	x	x	x	x	x
LTE		x	x	x	x

systems is also essential, especially during emergencies. Since the emergency call number system is one of the primary triggers for public safety activities, it is crucial that public safety networks be interoperable with emergency call centers as well.

There are several vendors offering solutions to provide complete interoperability with the LTE-based and Project 25-based system [50]. Since the Project 25 inter-systems interface is based on IP/TCP standards including Session Initiation Protocol (SIP) and Real-time Transport Protocol (RTP), which are also included in the LTE standards, the interoperability between these two should be relatively straightforward [51].

GERYON (Next Generation Technology Independent Interoperability of Emergency Services) was an EU R&D project. Its objective was to integrate the communication networks used by emergency—ambulances, fire brigades, civil protection teams—and safety (PMRs) management bodies with new generation telephone networks (4G, LTE). The project work plan defined a series of design and implementation work packages aimed at developing a non-commercial demonstrator prototype. At the end of the project, all its objectives were successfully fulfilled, resulting in a fully working IMS compatible ecosystem capable of providing PMR grade communications while paving the way for future professional LTE networks [52].

1.3 APPLICATIONS, SYSTEMS, AND END-USER DEVICES

The technologies discussed in the previous section are just one of the parts that make up the critical communications ecosystem. A complete ecosystem encompasses smart applications, supported by a set of comprehensive systems, purpose-built, intuitive devices, and comprehensive services as well. In other words, providing top levels of safety and efficiency to enable better decisions is about more than just better equipment and technology; it is about delivering new ways to connect users to information and each other. The critical communications ecosystem should deliver anywhere, anytime access to multimedia information with the priority, resiliency, and security that public safety agencies demand.

1.3.1 Applications and Systems

A modern critical communications ecosystem must be equipped with a variety of applications, from necessary push-to-talk to IP telephony to comprehensive multimedia voice and data applications. With narrowband technologies such as TETRA and Project 25, due to their low data rates, commercially available mobile devices such as smartphones and tablets are not available to critical communications systems users. However, to supplement the applications provided by narrowband technologies, commercial smartphones, and tablets connected to either a Wi-Fi or a commercial carrier, are frequently used by critical communication users. It is expected that with the introduction of LTE-based critical communications systems, smartphones and tablets,

as well as a variety of other multimedia devices, be a part of applications and devices available to first responders and law enforcement agencies. Body cameras, license plate readers, fingerprint scanners, virtual maps, and digital building plans are just some of the applications that are expected to be a part of the critical communications ecosystem.

APCO International is the world's largest organization of public safety communications professionals. APCO International maintains a website that provides an inventory of applications, referred to as APCO International's online Application Community (AppComm) [53]. The site has a collection of applications related to public safety and emergency response. Some of these applications (e.g. neighborhood crime map) can be used by the general public as well. These applications are typically mobile apps that are intended for use on a smartphone or tablet.

Systems and applications deployed and used in critical communications systems should allow the users of such systems to submit and retrieve information by end-user devices, terminals, as efficiently as possible.

While most applications are deployed over the Internet and mobile networks, there are just a few data applications over TETRA and Project 25 due to the low data rate provided by these narrowband technologies. However, there have been some offerings by various vendors to ease the concern somewhat. Some of these applications can even be easily modified by the user thanks to the APIs provided by the vendors. It is expected that these applications extend information availability to a variety of end-user devices. Via the vendor provided APIs, users can develop their solutions in addition to traditional applications such as a database, forms, image handling, webmail, and others.

There are some applications currently available for various sectors such as law enforcement agencies, first responders, transport, and utilities. Table 1.4 shows some examples.

TABLE 1.4. A Few Sector-Specific Examples [54]

Police	• Vehicle, driver, license information inquiry • Transmission of missing person(s) images • Crime report and stop & search forms • Vehicle incident report lookup
Airport	• Missing passenger information look-up and submission • Incident report form look-up and submission • Fuel figure submission • Webmail access
Field Service	• Safety inspection report look-up and submission • Missing part information & photo download via Intranet • Fault report look-up

There are several shared centers and supporting associated systems to serve all the users in a coordinated way. Two of the most important ones are briefly discussed below:

- *Incident Management System*—provides a mechanism for all the users and agencies to work together "to prevent, protect against, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location or complexity" [55]. Although each agency will have its control, command, and management centers, a unified incident control center provides smooth coordination and sharing of resources and capacities [55, 56].

  For example, in the USA, there is a new Department of Homeland Security (DHS) project called Unified Incident Command and Decision Support (UICDS), which will be used to share information for emergency operations. UICDS will be used to manage and share incident information across state and local lines, as well as with other federal agencies. Employing uniform standards, UICDS is intended to solve information interoperability problems, which have been a significant issue especially among public safety agencies [56].
- *Operations and Control Systems*—responsible for maintaining, administering, operating, and managing the whole network in a reliable, secure way. There may be agency-wide or region-wide centers and systems with similar responsibilities. All these systems should be connected, and activities need to be coordinated.

1.3.2 End-User Terminals and Consoles

Terminal devices used by public safety agencies strictly depend on the critical communications technology deployed by each agency. For example, the user devices for TETRA technology will be different from the user devices for Project 25 technology. Similarly, LTE-based critical communications devices will be drastically different from their narrowband counterparts, handling and displaying multimedia, just like the smartphones and tablets used commercially.

Regardless of the technology used, end-user devices may be categorized as mobile radios, portable radios, and consoles.

Mobile radios are installed in a motor vehicle such as cars and motorcycles (Figure 1.5). Since mobile radios are attached to the vehicle, they are bulkier, larger, and heavier than portable radios. Mobile radios have some advantages over portables: much better range, higher power output, and powered by the vehicle battery (no worry about battery life).

Portable radios are always carried (handheld) by the users. Therefore, they are relatively small and lightweight. As seen in Figure 1.6, a portable radio has a microphone and speaker. Like any other wireless portable device, it has a dipole

Figure 1.5. An example of a mobile radio [57].

antenna, powered by a rechargeable battery. The advantages mentioned for mobile radios become disadvantages for portable radios: smaller range, battery life, and low power output.

Dispatch consoles are systems, but since they are used to monitor/control end-user devices, we discuss them in the end-user devices section (Section 11.4). They are used to monitor and control multiple groups at a single physical position. The example shown in Figure 1.7 includes a microphone as well as the capability to select and unselect speakers. It provides EMERGENCY control.

New products come with enhanced functionality like built-in GPS, Wi-Fi, and Bluetooth interfaces, encryption support, and personal alarm buttons. A range of accessories, such as chargers and headsets, is also available. Tablets, smartphones, vehicular modems, and USB data cards are expected to be widely available once LTE-based critical communications systems are in place.

Figure 1.6. Examples of Project 25 portable radios.

Figure 1.7. An example of a dispatch console [57].

1.4 STANDARDS, POLICIES, AND SPECTRUM

1.4.1 Frequency Spectrum for Critical Communications

Most voice land mobile radio systems in the USA use narrowband frequencies (12.5 kHz) in the VHF and UHF bands. However, the FCC has recently allocated 758–768 MHz and 788–798 MHz for base stations and mobile units use, respectively, 10 MHz wide for each direction for public safety applications. Also, for voice communications only, the 769–775 MHz and 799–805 MHz bands in 12.5 kHz narrowband increments are allocated for public safety use (Figure 1.8). The USA has also allocated a large band of the spectrum (50 MHz) in 4.940–4.990 GHz, although it is not clear how this would be used [58–60].

In Europe, the frequency bands 410–430 MHz, 870–876 MHz/915–921 MHz, 450–470 MHz, and 385–390 MHz/395–399.9 MHz are allocated for TETRA for civil use. For emergency services, the frequency bands 380–383 MHz and 390–393 MHz are allocated. If needed, these bands can be expanded from 383–395 MHz and

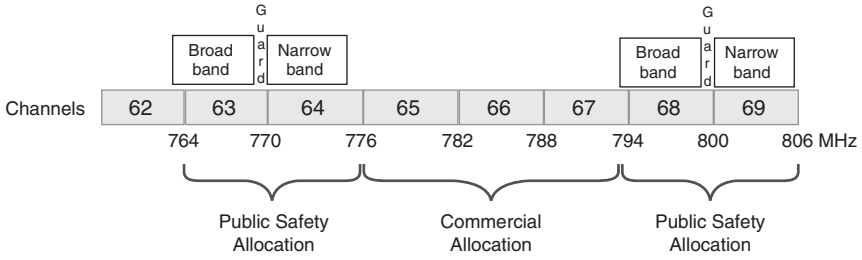


Figure 1.8. 700 MHz band plan for public safety services [61].

393–395 MHz to cover all of the spectrum [8, 62]. There is an ongoing effort in Europe to determine the most appropriate (and harmonized with other countries) frequency spectrum for broadband applications to be used by the public safety sector [8].

In several countries in Asia, like in Europe, the "380–400" MHz band is reserved for public safety organizations and the military as well. The 410–430 MHz band was allocated for civilian (private/commercial) use in other parts of the world, too. In Mainland China, the 350–370 MHz band is reserved for national security networks while the first 800 MHz band listed above is used in Hong Kong for private networks (Section 12.2.3). Russia has allocated 450–470 MHz for this purpose. In Australia and parts of the Middle East, spectrum has also been allocated for public safety broadband services

The book provides a more detailed discussion of how many countries around the world address spectrum issues.

1.4.2 Standards Development in Critical Communications

Traditionally, standardization of critical communications interfaces and protocols has been handled mainly in two Standards Development Organizations (SDOs), namely TIA for Project 25 and ETSI for TETRA and DMR-related projects. The standardization work on LTE-based standards has been carried out mainly by an entity called 3GPP, a collaboration among groups of telecommunications standards associations. It goes without saying that these SDOs do not operate in a vacuum. Many other organizations and even other SDOs provide input to this process. See Table 1.5 for a list of SDOs and other organizations involved in the standardization of critical communications systems.

In the following paragraphs, we briefly discuss several SDOs that play significant roles in the development of critical communications related specifications.

APCO and TIA collaborate, with some other organizations, to develop specifications for Project 25, also known as APCO Project 25, (which is the project name and number given by APCO) to produce public safety digital LMR standards. It is a joint project among the US APCO, the National Association of State Telecommunications Directors (NASTD), selected federal agencies and the National Communications System (NCS) in the USA, and the TIA. Project 25, designated as TIA-102, has been accepted as a national standard in the USA [6]. While APCO is the sole developer and formulator of the standard, TIA provides technical assistance and documentation for the standard. Project 25 is directed by a steering committee, which includes experts from various public safety agencies. Project 25 continues to evolve. The ongoing work in APCO, TIA, and other stakeholders has been centered on issues related to the interoperability between Project 25 and LTE-based public safety networks [63].

ETSI began the standards development for TETRA in the 1980s in Europe. The initial intent was to develop a standard for the wireless mobile network for commercial use. While ETSI was spending many years developing this comprehensive

TABLE 1.5. A List of SDOs and Other Organizations Involved in the Standardization of Critical Communications

SDOs, Organizations	Standards
APCO	P25
TIA	P25
ETSI	TETRA, TETRA/TEDS, DMR
3GPP	LTE, LTE-A
ATIS	All-IP and M2M infrastructure, Public Safety Related Applications Task Force (PSRA-TF), a Public-Safety Answering Point (PSAP)
ITU	Interoperability in Public Safety Mobile Networks, Spectrum for public safety communications
NPSTC (USA)	FirtsNet Requirements
TCCA	TETRA, TETRA to LTE Evolution
OMA	Push-to-talk over Cellular (PoC)

LTE, Long Term Evolution (per Release 8); NPSTC, National Public Safety Telecommunications Council; TCCA, TETRA and Critical Communications Association; TETRA, Terrestrial Trunked Radio; OMA, Open Mobile Alliance; APCO, Association of Public-Safety Communications Officials; TIA, Telecommunication Industry Association; ETSI, European Telecommunications Standards Institute; 3GPP, 3rd Generation Partnership Project; ATIS, Alliance for Telecommunications Industry Solutions; ITU, International Telecommunication Union.

system, GSM networks became popular and ubiquitous. This caused significant hardship for the companies invested in TETRA development and they identified the public safety market as a way to sell their products. TETRA in ETSI is expected to continue to provide enhancements only. In other words, ETSI has no plans to develop new technology in this area. The TETRA community has been active in moving toward LTE-based public safety networks as well. Some projects are underway to achieve seamless interoperability between TETRA and LTE-based public safety networks [64].

3GPP has been working on the standardization of LTE as part of the Release 8 feature set (a *release* in 3GPP refers to a group of added technology components). Following Release 8 and Release 9, significant improvements were incorporated into Release 10. With this new release, LTE got a new name as well: LTE-Advanced.

The first commercial LTE system was deployed in late 2009. 3GPP working groups added new features and technology components into later releases to improve LTE. Release 12 enhances LTE to meet public safety application requirements. Two critical public safety-related study items, Direct Mode Operation, and Group Call functions are included in Release 12 [43]. Public safety agencies and other stakeholders (such as TCCA, APCO, and FirstNet) are working together to drive the development of additional features that are typically associated with public safety systems [44, 65] (Figure 1.9).

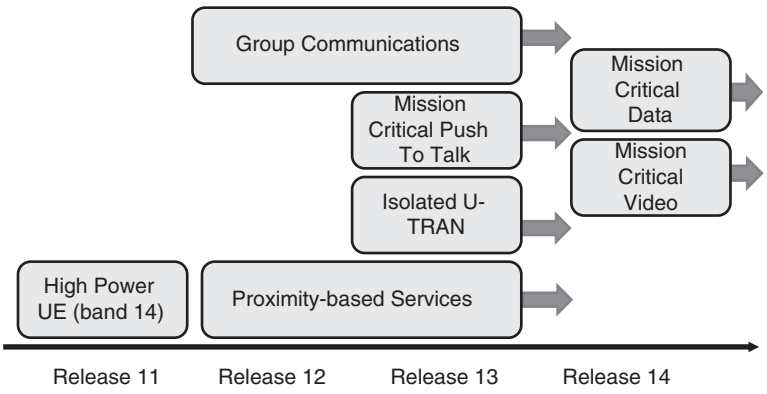


Figure 1.9. 3GPP critical communications related projects [66].

1.5 PLANNING, DESIGN, DEPLOYMENT, AND OPERATIONAL ASPECTS

Planning, designing, and deployment of a critical communication system depend on many factors, including the type of organization, the number of organizations to share the system, the coverage, interoperability, existing systems, data requirements, nationwide plan, finance, and frequency spectrum.

This section provides an overview of how planning, designing, and deployment of a critical communication system deal with these questions during various stages of making a new critical communications system a reality.

1.5.1 Planning

Although the level of effort, activities, and contents heavily depend on the factors mentioned above, there are some common activities in planning for a critical communications system. Common activities include conducting a set of feasibility studies, developing a business case, performing a risk analysis, drawing up a roadmap, developing a business plan and a project plan, and establishing a project team.

A **feasibility study** is an analysis of the viability of an idea, a project, through a disciplined and documented process of thinking [67]. It is perhaps the most critical phase in the development of a project [68]. The feasibility study is conducted before developing a formal business plan [69]. A feasibility study results in a feasibility report that provides documentation that the idea was thoroughly investigated. The feasibility report explains in detail whether the project under investigation should be carried out. A typical feasibility study includes operational feasibility, market feasibility, financial/economic feasibility, organizational/managerial feasibility,

environmental feasibility, and legal feasibility. Note that not all these types may apply to a given feasibility study [69].

Before a feasibility study begins, we need to know what is being studied. Is it for upgrading an existing system or establishing a brand new system? Therefore, a set of criteria addressing the necessity, attainability, completeness, consistency, and complexity must be established as the first step in a feasibility study. These criteria will define conditions for the selected approach to be acceptable to the users and other stakeholders.

A set of more specific criteria that are directly related to the technology, operations, cost, finance, and the users must be established as well. Some examples are user expectations, data rate requirements, performance (throughput, capacity, and latency), availability, reliability, resiliency, security, scalability, evolvability, interoperability, manageability, cost-effectiveness, and more.

1.5.2 Technology Considerations for a Critical Communications System

Based on the discussions in Section 1.2, we can safely say that, currently, there are four major candidate technologies to consider: TETRA, Project 25, DMR, and LTE. Again, depending on what exists and what criteria and requirements are established, there may be different scenarios constructed. A table similar to Table 1.6 may be

TABLE 1.6. A Template for a Qualitative Comparison of Technology Considerations

		Criteria				
		Criterion 1	Criterion 2	Criterion 3	Criterion 4	Criterion 5
1	Do Nothing					
2	DMR Only					
3	P25 Only					
4	TETRA Only					
5	DMR + TETRA					
6	P25 + TETRA					
7	LTE Only					
8	LTE Shared					
9	Commercial LTE					
10	P25 + LTE					
11	TETRA + LTE					
12	P25 + TETRA + LTE					
13	Other Consideration					

constructed where available technology considerations can be listed, and a qualitative scoring (low, medium, and high) can be assessed for each criterion established already.

The alternatives that include more than one technology may be preferred for various reasons. For example, there may be existing deployment based on a technology that may not satisfy the established criteria and requirements. In this case, while deploying a new system based on another technology, the existing system may continue to serve alongside the other technology for the foreseeable future. Another reason for the dual technology consideration could be that one technology may not satisfy all the requirements. Therefore, the two technologies jointly provide full coverage of all the requirements.

However, it is clear that the LTE technology-based approach should be the long-term goal. All immediate, intermediate, and long-term activities should be planned based on this primary objective in mind. A roadmap must be developed toward the realization of this objective.

1.5.3 Economic and Financial Considerations

The cost of planning, deploying, and operating a critical communication system is very high. This is especially much higher for nationwide critical communications networks; the estimated costs of broadband-based public safety networks around the world are running over many billions of dollars. Naturally, substantial costs are surrounded by substantial cost uncertainties. Therefore, accurate cost estimations and fine points of financing are critically important. Specific mathematical models can be beneficial in minimizing potential errors and should be used before the implementation stage [70–75].

Government projects are not usually profit driven and are undertaken for the good of society, and the costs are covered by the government budget [62]. Therefore, many government projects are financed by the taxpayers and are not subject to the classic cost-benefit analysis performed by commercial corporations. However, it is strongly suggested that governments implement general corporate financing rules as much as possible in evaluating their projects to ensure that optimality is achieved in initiating and managing projects.

Financing a critical communications network is challenging; government-operated public safety networks are especially a complicated issue mostly due to the size of financing and integrated ongoing operating cost of the project. No government can easily include a line item in billions of dollars without proper planning and preparation and without disturbing the ongoing operations of the government. A project of this magnitude would require the use of all possible forms of financing including government bonds, equipment leasing, vendor financing, private partnerships, and sharing the network with utility companies and the like [74, 76]. Specific taxes on harmful line items may also be considered; among them are cigarettes and alcohol.

This book provides a detailed discussion of the cost-benefit structure. An analysis by a European economic center indicates that the socioeconomic benefits computed for European Union countries would be approximately 34 billion Euros, annually. In contrast, the opportunity cost of the above scenario for the European Union is to sell the spectrum at an auction to obtain a one-off economic gain totaling 3.7 billion Euros [2, 77]. Naturally, the benefits are several times greater than the opportunity cost, suggesting there that there should be no doubt in implementing broadband public safety networks. The government must educate all involved parties about the socioeconomic benefits of broadband public safety networks.

A proper cost-of-capital estimation also helps the government in the planning and financing stages as it creates a reference value, a benchmark to compare alternatives. With an accurately computed cost of capital value, the government will negotiate better.

1.5.4 Paving the Way

However, before we design, develop, and operate a critical communications system, we need to have a high level, but clear understanding of what needs to be done. We are referring to policy and institutional framework, which should include the following:

- An overall *communications policy* for the entire organization or the whole country, whichever applies; the plan should address commercial, public, government, and military needs and interests. The critical communications system must be an integral part of this plan. The National Broadband Plan prepared by the FCC is an example of this case [78]. If this plan does not exist, it must be developed before launching a critical communications project.
- A separate *authority* with full and overall responsibility to build and maintain the critical communications system, to handle the coordination among all the stakeholders and users, and to make the necessary adjustments and improvements to the network as conditions change and technology evolves.
- In the case of a public safety network, a comprehensive evaluation of potential spectrum alternatives to support a new public safety communications system must be performed. Sufficient bands (at least 2×10 MHz) in 700 MHz and 800 MHz must be considered for public safety broadband spectrum as well. Unique attributes of each of these bands, including some technical and regulatory issues, need to be carefully considered in this evaluation.

Building a new critical communication system that is flexible and adaptable to changing needs is a significant challenge. The book recommends a gradual (as opposed to a top-down) approach, which requires that the system be built incrementally and iteratively; each increment is tested under the most possible realistic conditions by the

stakeholders involved before the next increment is handled. Next, the book recommends the establishment of a framework for a *national test bed* in which implementations of a new system or subsystem can be validated before they are put into service.

1.5.5 Design and Deployment

Before the deployment of the critical communications system, a high-level *network architecture*, followed by a detailed *network design* must be prepared. As part of this effort, an outreach program must also be developed and executed to gain the maximum level of acceptance from all stakeholders. The processes for supply acquisition must be determined and carried out.

Network Architecture is a framework for the specification of the components and the configuration of a communications system. It is a blueprint that is utilized in developing a detailed network design and in deploying the network. Usually, it is composed of two primary documents: a functional architecture consisting of the functions necessary and needed for the network and a physical architecture, where the functional entities are mapped into corresponding physical counterparts. The operational principles and procedures, as well as the data formats used in its operation, may be a part of these architecture specifications.

Luckily, general network architectures for the well-known critical communications technologies are well-specified and documented. Chapter 12 provides a more detailed discussion on these.

In the context of a public safety network deployment, LTE can follow some structural variations, mainly because there are many existing commercial LTE deployments in almost every country.

- **Private Public Safety LTE Network—**a private LTE RAN and core network infrastructure for the sole purpose of public safety services.
- **Hosted Core Public Safety LTE Network—**public safety entities share a common core network that services their own private LTE eNodeBs.
- **Shared Commercial Public Safety LTE Network—**public safety agencies use commercial LTE networks for public safety services.

Each of these options has advantages and disadvantages, technically, financially, as well as politically [79]. However, a typical implementation of an LTE network is composed of five distinct segments: e-UTRAN, transport, EPC, applications, and operations support systems. Each of these segments presents a different set of challenges in design and deployment.

In the *e-UTRAN segment*, the determination of the number of eNBs (LTE base stations) and their locations are critically important in the design of the network. The necessary information impacting coverage and capacity design must be identified, collected, processed, and calculated. The book provides extensive details about the type of information needed in this context [80].

In the *transport segment*, a backhaul network must be designed to carry traffic from eNBs to the elements in the core network. The high-level design should focus on the transport media, transport technology, and the topology. To meet LTE requirements, the fiber as a transport media, Layer 2 as a transport technology, and the ring topology is highly recommended [81].

In designing the EPC, the *core network*, a critical decision is to determine whether to deploy a centralized or distributed architecture. A distributed model is favorable because of the importance of network availability. The LTE core network design also includes core network dimensioning, which is used to determine the number of nodes and the capacity required.

Applications to be used by the users and agencies must be a part of the design and planning of the LTE network and its sites. Some applications require high bandwidth capacity while others involve real-time transmission. Typical applications that can be used in the public safety sector are video, dispatch, fingerprint, image transfer, voice over IP, push to talk, mobile database query, machine to machine, and monitoring.

Operation Support Systems (OSSs), which are used to keep the network up and running, and providing its services satisfactorily as "promised," must be a part of the overall design and planning of the public safety network. OSS functionalities include fault management, configuration management, accounting management, performance management, and security management (FCAPS).

After the architectural concepts discussed above are approved, a detailed **network design**, also called *low-level network design*, must be prepared. A detailed design document describes how the network infrastructure should be built and engineered to meet the specific goals and objectives delineated in various documents, including the network architecture. Usually, the detailed design includes every single bit of information that is necessary for building and deploying the network. For example, the identification of the switch ports that need to be connected to the router should be specified in a detailed network design.

Designing a critical communications system requires engineers knowledgeable in cellular network design since there are certain similarities such as planning for the cellular sites and deployment, a radio network, back-haul transmission, and the core network. However, there are several significant differences especially in coverage and capacity (radio network dimensioning is mostly coverage driven by a critical communications network). For example, a critical communications system uses group calls with only one channel per group, but several sites in one call. The average call duration is much shorter. Unlike a commercial network, the additional traffic that dispatch stations and command systems generate and receive needs to be incorporated in critical communications systems.

Once the planning and design phase is completed and approved, activities in deploying the network should begin. Like the design phase, the deployment phase also includes careful considerations for each segment of the overall network. Before the actual deployment begins, a *deployment plan* must be developed to include installation, integration, and test procedures for the nodes to be deployed. It is most likely that the deployed systems will include equipment from a number of different

vendors. Therefore, it is crucial to perform an end-to-end system integration testing to verify the requirements established during the design and procurement phase. When the system integration is completed, a verification testing must be performed to verify stability, media quality, robustness, maintainability, capacity, and coverage. All these are explained in greater detail in the book.

1.5.6 Operations, Administration, Maintenance, and Provisioning (a.k.a. Management)

Once the network is deployed, and integration and verification tests are performed, the network is ready to provide services to its users. For the system to work correctly, there needs to be a "network and service management infrastructure" in place. This includes a set of OSSs, applications, plans, policies, procedures, and people. This area is crucial for a critical communications system since in extreme situations—on-scene operations—the system must be extremely resilient and must be up to help the first responders. An *operations plan* to describe the resources, organizations, responsibilities, policies, and operations procedures to monitor and manage the network efficiently must be developed. The operations plan and procedures are executed by staff members of a Network Operations and Control Center (NOCC), which is set up to monitor, control, and manage all segments of the network. In either case, it is crucial to implement the same type of operation procedures. It is highly recommended that the NOCC organization and operations models be aligned with the standard enhanced Telecommunications Operations Map (eTOM) defined by the Telecommunications Management Forum (TMF) and the Information Technology Infrastructure Library (ITIL) to synchronize the activities among geographically dispersed regional centers when applicable [82, 83].

The term O*perations Support System (OSS)* is a generic term used to refer to the systems used in operating, administering, maintaining, and provisioning the networks. Depending on the size of the network, there could be many OSSs—regional, national, specialized (e.g. billing), general purpose, etc. Moreover, there may be more specific names used to signify the specific purpose that an OSS is used for. The Telecommunication Management Network (TMN) provides a framework to name OSSs more formally. Briefly, TMN defines management layers (business, service, network, and element) and names OSSs according to the layer in which they are used. For example, the OSS used at the service management layer is called the Service Management System (SMS). Accordingly, the OSS used at the network management layer is called Network Management Systems (NMS)[84] (the term NMS is also used generically especially in smaller, data specific networks [e.g. LANs] to refer to the management workstations used in managing [i.e. operating, administering, and maintaining] networks).

In critical communication networks too, OSSs are used to enable configuration, management, and maintenance of all network elements (e.g. switches, base stations, dispatcher consoles, and links). Both Project 25 and TETRA networks have

standardized interfaces to OSSs, which typically use the Simple Network Management Protocol (SNMP) to collect network management information and alarms (note that both Project 25 and TETRA specifications use the term NMS, rather than OSS). Depending on the size of the network, there could be a hierarchy of OSSs. For example, a low-level OSS (e.g. SNMP Console Manager) may report the information collected to higher-level systems for further processing and displaying. Note that an SNMP Console Manager can request information and the status of one or more alarms from any network element.

The OSS typically records all network events in a database or files. Date, time, and source, together with the event type, are recorded to enable system reporting including network traffic loading and usage and timeslot distribution. Daily files can be further processed by specialized systems or manually in spreadsheets to provide detailed statistical analysis for performance management reporting and system optimization.

1.6 SUMMARY AND CONCLUSIONS

This book deals with the technologies, systems, and applications used in public safety and mission-critical communications specific operations. The book covers economic, financial, and policy issues as well as the design, deployment, and operation of such systems.

Critical communications networks provide the basis for *situational awareness* and *command and control* capabilities, which roughly translate into the delivery of mission-critical data, survivability against multiple failures, maintenance of data integrity and confidentiality, essential full coverage and capacity, interoperability with other networks, and required support for officers, applications, and devices.

As of writing this book, most old analog technologies used for critical communications systems have been replaced by *all* digital narrowband technologies led by Project 25, TETRA, and DMR standards. There is also a higher consensus that LTE be the technology of the future for critical communications systems. TETRA has been the choice of public safety agencies mainly in Europe and Project 25 technologies mainly in North America, but both have worldwide deployments as well. DMR-based systems have also been chosen in some regions, although not as extensively as TETRA and Project 25.

Project 25 and TETRA technologies are mature, widely used, tested, reliable, and feature rich in voice applications. These narrowband technologies are somewhat limited in providing data services. Also, narrowband technologies are more expensive since the target market is limited, compared to the commercial mobile market. The demand for data-intensive applications by public safety agencies is increasing.

LTE technology is an ideal candidate for a nationwide critical communications system, especially for public safety applications. It is a proven and tested technology for commercial use and nationwide broadband networks. It is handling broadband

data applications an order of magnitude better than the narrowband systems. For the first time in history, LTE has emerged as a single worldwide standard and is used commercially everywhere around the world. The scale of economy is just outstanding. A growing number of countries, including the USA, have chosen LTE for their public safety networks already.

A complete critical communication system encompasses applications supported by a set of comprehensive systems, purpose-built, intuitive devices, and comprehensive services. While applications are commonly deployed over the Internet, application developers have traditionally been unable to produce packet data applications over TETRA and Project 25 due to the low data rate provided. However, there have been some offerings by various vendors to ease the concern somewhat. There are some applications currently available for various markets including, but not limited to, police, fire, ambulance, transport, airport, field service, and utilities.

To serve all the users in a coordinated way, critical communications systems usually have some centers and associated support systems. Two of the most important ones are incident management systems, which enable all the users and agencies to work together to handle incidents that are reported or detected, and operations and control systems, which are used to operate, administer, and maintain the network.

Terminal devices for the users of critical communications systems strictly depend on the underlying communications being used. For example, the user devices for TETRA technology will be different from the user devices for Project 25 technology. Similarly, LTE-based critical communications devices will be drastically different from its narrowband counterparts, handling and displaying multimedia, just like the smartphones and tablets used commercially. Regardless of the technology being used, end-user devices can be roughly categorized as mobile radios, portable radios, and consoles.

As expected, spectrum issues are being addressed in many countries around the world.

Each region has a slightly different approach. For example, in the USA, most voice land mobile radio systems use narrowband frequencies in the VHF and UHF bands. However, the FCC has recently allocated 758–768 MHz and 788–798 MHz for base stations and mobile units use, respectively.

Standardization of critical communications interfaces and protocols has been handled mainly by the TIA for Project 25 and by the ETSI for TETRA and DMR-related projects. The standardization work on LTE-based standards has been carried out mainly by 3GPP, a collaboration among groups of telecommunications standards associations.

Planning, designing, and deployment of a critical communications system depend on many factors including whether it is for a country or a commercial company, whether it will be a nationwide or a regional system, and whether there is already an existing system in place. Although the level of effort, activities, and contents heavily depends on the factors mentioned above, there are some common activities in planning for a critical communications system. A feasibility study

needs to be conducted in developing a formal business plan. A typical feasibility study should include operational feasibility, market feasibility, financial/economic feasibility, organizational/managerial feasibility, environmental feasibility, and legal feasibility.

An essential part of the planning effort is to select a technology for the planned critical communications systems. Currently, there are four major candidate technologies to consider: TETRA, Project 25, DMR, and LTE. Alternative scenarios that include more than one technology may be preferred for various reasons such as to fulfill the requirements outlined in the planning step. A consensus is that the LTE technology-based approach is the long-term goal.

The cost of planning, deploying, and operating a critical communications system is very high, running over several billion dollars. Naturally, substantial costs are surrounded by substantial cost uncertainties. Therefore, accurate cost estimations and fine points of financing are critically important. Specific mathematical models can be beneficial in minimizing potential errors and should be used before the implementation stage. A project of this magnitude would require the use of all possible forms of financing including bonds, equipment leasing, vendor financing, private partnerships, sharing the network with utility companies, and the like.

Before the deployment of the system, a *network architecture*, followed by a detailed *network design* must be prepared. The processes for supply acquisition must be determined and carried out. Once the planning and design phase is completed and approved, activities in deploying the network should begin. Before the actual deployment begins, a *deployment plan* must be developed to include installation, integration, and test procedures for the nodes to be deployed. It is crucial to perform an end-to-end system integration testing to verify the requirements established during the design and procurement phase.

For the system to work correctly, there needs to be a "network and service management infrastructure" in place. An *operations plan* to describe the resources, organizations, responsibilities, policies, and operations procedures to monitor and manage the network efficiently must be developed. This area is crucial for a critical communications system since in extreme situations, that is on the scene operations, the system must be extremely resilient and must be up to help the first responders.

REFERENCES

1. TETRA and Critical Communications Association, "Broadband spectrum for mission critical communication needed," Position Paper, Aug. 2013.
2. B. Mattsson, "TETRA News—TETRA evolution for future needs," *TETRA Applications*, Mar. 17, 2014. [Online]. Available: http://www.tetra-applications.com/27885/news/tetra-evolution-for-future-needs. [Accessed: Jul. 24, 2016].
3. National Public Safety Telecommunications Council, "Defining public safety grade systems and facilities final report," A NPSTC Public Safety Communications Report, May 2014.

4. A. Bleicher, "LTE-Advanced is the real 4G," *IEEE Spectr*., Dec. 31, 2013. [Online]. Available: https://spectrum.ieee.org/telecom/standards/lte-advanced-is-the-real-4g.
5. C. Cox, *An Introduction to LTE: LTE, LTE-Advanced, SAE, VoLTE and 4G Mobile Communications*, 2nd ed. John Wiley & Sons, 2014.
6. S. Burfoot, P. Chan, and D. Reitsma, "P25 radio systems training guide, revision 4.0.0," Codan Radio Communications, 2013.
7. J. Oblak, "Project 25 phase II," EFJohnson Technologies, Dec. 2011.
8. The Network Encyclopedia, "Terrestrial Trunked Radio (Tetra) in The Network Encyclopedia," 2013. [Online]. Available: http://www.thenetworkencyclopedia.com/entry/terrestrial-trunked-radio-tetra/. [Accessed: Jul. 19, 2016].
9. P. Stavroulakis, *TErrestrial Trunked RAdio—TETRA*. Springer Science & Business Media, 2007.
10. J. Dunlop, D. Girma, and J. Irvine, *Digital Mobile Communications and the TETRA System*. John Wiley & Sons, 2013.
11. Tetrapol, "Tetrapol forum." [Online]. Available: http://www.tetrapol.com/. [Accessed: Jul. 24, 2016].
12. "DMR versus TETRA systems comparison Version 1v2," *Radio Activity Solutions*, 2009.
13. B. Bouwers, "Comparison of TETRA and DMR," Rohill Technologies, 2010.
14. R. Marengon, "A TETRA and DMR comparison," *Radio Resource Magazine*, Apr. 1, 2010. [Online]. Available: https://www.rrmediagroup.com/Features/FeaturesDetails/FID/174.
15. "The DMR standard," *Digital Mobile Radio Association*, Dec. 29, 2010. [Online]. Available: http://dmrassociation.org/the-dmr-standard/. [Accessed: Jul. 24, 2016].
16. Signals and Systems Telecom, "The public safety LTE & mobile broadband market: 2012–2016," Market Report, Nov. 2012.
17. "TETRA and LTE working together v1.1." TETRA and Critical Communications Association, Jun. 2014.
18. Project MESA, Service Specification Group—Services and Applications, "Statement of requirements executive summary." [Online]. Available: http://www.projectmesa.org/MESA_SoR/mesa_sor_executive_summary.pdf. [Accessed: Sep. 13, 2018].
19. WiMAX Forum, "AeroMACS, WiGRID, and WiMAX advanced technologies." [Online]. Available: http://www.wimaxforum.org. [Accessed: Jul. 24, 2016].
20. Motorola Solutions, "The future is now: Public safety LTE communications," Motorola Solutions White Paper, Aug. 2012.
21. Tait Limited, "Introducing unified critical communications," White Paper, 2014. [Online]. Available: https://go.taitradio.com/introducing-unified-critical-communications-for-public-safety.html. [Accessed: Sep. 13, 2018].
22. B. Deverall, Added Value Applications, "Briefing for E-Gif Working Group on incorporating the APCO P25 standards into the e-government interoperability framework," Sep. 19, 2006.
23. "Comments of internet 2 to NTIA," Counsel for Internet 2, Docket No. 120928505-2505-01, Nov. 2012.
24. The Critical Communications Association (TCCA), "TCCA signs market representation partner agreement with 3GPP." [Online]. Available: https://tcca.info/tcca-signs-market-representation-partner-agreement-with-3gpp/. [Accessed: Sep. 13, 2018].

25. TETRA and Critical Communications Association, "Mission Critical Mobile Broadband: Practical standardization & roadmap considerations," White Paper, Feb. 2013.
26. D. Jackson, "UK seeks to replace TETRA with LTE as early as 2016," *Urgent Communications*, Jun. 6, 2013. Available: http://urgentcomm.com/tetra/uk-seeks-replace-tetra-lte-early-2016.
27. E. Dahlman, S. Parkvall, and J. Skold, *4G LTE/LTE-Advanced for Mobile Broadband*. Academic Press of Elsevier, 2011.
28. National Telecommunications Information Agency, "Desirable properties of a national public safety network," Report and Recommendations of the Visiting Committee on Advanced Technology, Jan. 2012.
29. I. Sharp, "Delivering public safety communications with LTE," 3rd Generation Partnership Project, Jul. 2013.
30. TCCA, "TCCA liaison to 3GPP SA on group communications and proximity services," 3GPP SP-120456, Jul. 2012.
31. 3rd Generation Partnership Project, "3GPP release 12 LTE," Mar. 2015. [Online]. Available: http://www.3gpp.org/specifications/releases/68-release-12. [Accessed: Sep. 13, 2018].
32. Alcatel-Lucent, "Alcatel-Lucent and first responders conduct trial of 4G LTE public safety broadband mobile network," Alcatel-Lucent Press release, Nov. 2013.
33. National Telecommunications and Information Administration, "FirstNet." [Online]. Available: http://www.ntia.doc.gov/category/firstnet. [Accessed: Sep. 13, 2018].
34. C. Gessner, *Long Term Evolution: A Concise Introduction to LTE and its Measurement Requirements*. Rohde & Schwarz Publication, 2011.
35. W. Lehr and N. Jesuale, "Spectrum pooling for next generation public safety radio systems," in *IEEE Proc. Dynamic Spectr. Access Netw. (DySPAN2008) Conf.*, Chicago, Oct. 2008, pp. 1–23.
36. 5G Americas, "List of 3G/4G deployments worldwide (HSPA, HSPA+, LTE." [Online]. Available: http://www.4gamericas.org/en/. [Accessed: Jul. 24, 2016].
37. A. M. Seybold, "Seybold's take: Public safety's 700 MHz LTE network an opportunity for vendors," *Fierce Wireless*, Mar. 14, 2012. Available: https://www.fiercewireless.com/wireless/seybold-s-take-public-safety-s-700-mhz-lte-network-opportunity-for-vendors.
38. M. Poikselkä, Harri Holma, Jukka Hongisto, Juha Kallio, and Antti Toskala, *Voice over LTE (VoLTE)*. John Wiley & Sons, 2012.
39. Etherstack, "PMR-LTE network solutions: Push-to-talk PMR over LTE," White Paper, 2013.
40. K. Doppler, M. Rinne, C. Wijting, C. Ribeiro, and K. Hugl, "Device-to-device communication as an underlay to LTE-Advanced networks," *IEEE Commun. Mag.*, vol. 47, no. 12, pp. 42–49, Dec. 2009.
41. P. Janis, C.-H. Yu, K. Doppler, C. Ribeiro, C. Wijting, K. Hugl, O. Tirkkonen, and V. Koivunen, "Device-to-device communication underlying cellular communications systems," *Int. J. Commun. Netw. Syst. Sci.*, vol. 2, no. 3, pp. 169–178, 2009.
42. Qualcomm, "Study on LTE Device to device proximity discovery," 3rd Generation Partnership Project, TSG RAN Meeting #57, 2012.
43. 3rd Generation Partnership Project, "Mobile broadband standard: LTE." [Online]. Available: http://www.3gpp.org/technologies/keywords-acronyms/98-lte. [Accessed: Jul. 24, 2016].

44. *Wikipedia, the free encyclopedia*, "3GPP standards," Jun. 30, 2016. Available: https://en.wikipedia.org/wiki/3GPP.
45. J. Liu, Y. Kawamoto, H. Nishiyama, N. Kato, and N. Kadowaki, "Device-to-device communications achieve efficient load balancing in LTE-Advanced networks," *IEEE Wirel. Commun.*, vol. 21, no. 2, pp. 57–65, Apr. 2014.
46. 5G-PPP, "5G-PPP." [Online]. Available: https://5g-ppp.eu/. [Accessed: Jul. 24, 2016].
47. US Department of Homeland Security SAFECOM, "Public safety statement of requirements for communications & interoperability," vol. 1, Version 1.2, Oct. 2006.
48. P. R. Kempkerhttp, Department of Homeland Security, "Basic gateway overview." [Online]. Available: http://www.c-at.com/Customer_files/Fairfax%20rally/Module%201%20-%20Basic%20Gateway%20Overview.ppt. [Accessed: Sep. 13, 2018].
49. E. Olbrich, "Public safety communications research public safety LTE," presented at the LTE World Summit, Barcelona, May 2012.
50. D. Witkowski, "Effectively testing 700 MHz public safety LTE broadband and P25 narrowband networks," Anritsu Company, 2013.
51. D. Tuite, "Can public-safety radio's P25 survive LTE?." [Online]. Jul. 17, 2012. Available: https://www.electronicdesign.com/analog/can-public-safety-radio-s-p25-survive-lte.
52. EU CORDIS, "GERYON (Next generation technology independent interoperability of emergency services)," 284863.
53. APCO International, "APCO Application Community." [Online]. Available: http://appcomm.org/. [Accessed: Jul. 25, 2016].
54. Team Simoco, "TETRA-GTI applications." [Online]. Available: http://www.simocogroup.com/resources/product_datasheets/tetra/tetra-gti/TETRA-GTI_Applications.pdf. [Accessed: Jun. 25, 2016].
55. A. M. Seybold, "FirstNet brings changes to Unified Incident Command," *IMSA J.*, Feb. 2014.
56. J. W. Morentz, C. Doyle, L. Skelly, and N. Adam, "Unified Incident Command and Decision Support (UICDS) a Department of Homeland Security initiative in information sharing," in *Proc. IEEE Conf. Technol. Homeland Security (HST '09)*, Boston, May 2009, pp. 182–187.
57. Motorola Solutions web site. [Online]. Available: http://www.motorolasolutions.com/en_us/products/two-way-radios.html. [Accessed: Jul. 25, 2016].
58. Public Safety Spectrum Trust. [Online]. Available: http://www.psst.org/. [Accessed: Jul. 18, 2016].
59. Carlos M. Gutierrez, Meredith A. Baker, US Department of Commerce, National Telecommunications Information Agency, "Spectrum management for the 21st century: The President's spectrum policy initiative—Federal strategic spectrum plan," Mar. 2008. [Online]. Available: http://www.ntia.doc.gov/reports/2008/FederalStrategicSpectrumPlan2008.pdf. [Accessed: Sep. 13, 2018].
60. Federal Communications Commission, "FCC takes action to advance nation-wide broadband communications for America's first responders," Jan. 2011. [Online]. Available: http://hraunfoss.fcc.gov/edocs public/attachmatch/DOC-304244A1.pdf. [Accessed: Sep. 13, 2018].
61. "Federal Communications Commission, 700 MHz band plan for public safety services." [Online]. Available: https://www.fcc.gov/general/700-mhz-public-safety-spectrum-0. [Accessed: Sep. 13, 2018].

62. TETRA and Critical Communications Association, "Spectrum saves lives: High speed data for the police and emergency services," presented at the The Operators Workshop, 2011.
63. "Project 25: What's next for the Global Standard?," *Mission Critical Communications Magazine*, Oct. 2013.
64. "TETRA + Critical Communications Association." [Online]. Available: http://www.tandcca.com/. [Accessed: Jul. 24, 2016].
65. "3GPP." [Online]. Available: http://www.3gpp.org/. [Accessed: Jul. 24, 2016].
66. R. Favraud, A. Apostolaras, N. Nikaein, and T. Korakis, "Towards Moving Public Safety Networks," *IEEE Commun. Mag.*, vol. 54, no. 3, pp. 14–20, Apr. 2016.
67. H. Hoagland and L. Williamson, *Feasibility Studies*. [Online]. University of Kentucky, 2000. Available: http://www.parcodelfuenti.it/dossier/documenti/Dispensa.Univ.Kentucky.pdf.
68. H. Tompson, "Business feasibility studies: Dimensions of business viability," Best Entrepreneur, 2003.
69. W. Truitt, *A Comprehensive Framework and Process*. London: Quorum Books, 2003.
70. R. Hallahan and J. M. Peha, "Quantifying the costs of a nationwide broadband public safety wireless network," in *Proc. 36th Telecommun. Policy Res. Conf.*, Arlington, Sep. 2008.
71. R. Hallahan and J. M. Peha, "The business case of a nationwide wireless network that serves both public safety and commercial subscribers," in *Proc. 37th Telecommun. Policy Res. Conf.*, Arlington, Sep. 2009.
72. R. Hallahan and M. Peha, "Compensating commercial carriers for public safety use: Pricing options and the financial benefits and risks," in *Proc. 39th Telecommun. Policy Res. Conf.*, Arlington, Sep. 2011.
73. Federal Communications Commission, "The public safety nationwide interoperable broadband network: A new model for capacity, performance and cost," White Paper, Jun. 2010.
74. J. M. Peha, "A public-private approach to public safety communications," *Issues Sci. Technol.*, vol. 29, no. 4, 2013.
75. N. Bolari, "Indirect returns and use of NPV in financial viability modelling of critical communications networks," *IEEE Commun. Mag.*, vol. 54, no. 3, pp. 38–43, Mar. 2016.
76. Utilities Telecom Council, "Sharing 700 MHz public safety broadband spectrum with utilities: A proposal." [Online]. Oct. 2012. Available: https://utc.org/wp-content/uploads/2018/02/Sharing-700-MHz-Public-Safety-Broadband-Spectrum-With-Utilities-2.pdf.
77. A. Grous, "Socioeconomic value of mission critical mobile applications for public safety in the EU: 2 × 10 MHz in 700 MHz in 10 European countries," Centre for Economic Performance, London School of Economics and Political Science, Dec. 2013. Available: http://eprints.lse.ac.uk/69180/1/Grous_Socioeconomic_value_of_mission_critical_applications_UK_2013_author.pdf.
78. Federal Communications Commission, "Connecting America: The national broadband plan." [Online]. Mar. 2010. Available: https://transition.fcc.gov/national-broadband-plan/national-broadband-plan.pdf.
79. Federal Communications Commission, "Public safety tech topic #22—Application of emerging wireless broadband technology for public safety communications." [Online].

Available: https://www.fcc.gov/help/public-safety-tech-topic-22-application-emerging-wireless-broadband-technology-public-safety. [Accessed: Sep. 13, 2018].

80. S. Palat and P. Godin, "LTE network architecture: A comprehensive tutorial," Alcatel Lucent, Strategic White Paper, 2009.
81. Aviat Networks, "Five recommendations for building FirstNet-ready backhaul networks," White Paper, Aug. 2013.
82. TM Forum, "Business Process Framework (eTOM)." [Online]. Avaialble: https://www.tmforum.org/business-process-framework. [Accessed: Sep. 13, 2018].
83. "IT Infrastructure Library (ITIL)." [Online]. Available: https://www.itgovernanceusa.com/itil. [Accessed: Jul. 25, 2016].
84. S. Aidarous and T. Plevyak, eds., *Telecommunications Network Management into the 21st Century*. IEEE Press, 1994.