POLITECNICO DI TORINO

Master’s Degree in ICT for smart societies

Politecnico di Torino

Master’s Degree Thesis

Public safety networks. Analysis of the TETRA standard: history and evolution

Supervisor:

Prof. Daniele Trinchero

Candidate:

Alireza Esmaeilifar

July 2025

Abstract:

The objective of this thesis is to provide a comprehensive analysis of the TETRA (Terrestrial Trunked Radio) standard in the context of public safety. The study aims to trace the historical development and technical evolution of TETRA over the years, highlighting its key design principles, technical advances, and operational improvements. By evaluating the performance, interoperability, security, and integration with cellular networks, this study seeks to guide the design and optimization of public safety communication according to TETRA.

In this thesis, first, the network requirements for public safety are discussed, then the TETRA standard is introduced. Besides, the TETRA system is analyzed to understand how it can satisfy the requirement for public safety. Finally, active companies in the TETRA market are introduced and their solutions are compared according to the radio devices and base stations. Also, their solutions for TETRA over LTE and cellular networks are discussed.

Nowadays, public protection and disaster relief (PPDR) are widely used in all regions (cities and rural areas) because they bring essential characteristics like security and stability in the society and they secure the environment to maintain law and order; besides, they are to protect the life and values of citizens. Due to these reasons, they are also called public safety. It is used by firefighting systems, emergency medical services, law enforcement, and emergency and surveillance situations on land. To make communication between the team members and among the teams, there should be a communication system with special characteristics that works without interruption in harsh conditions. TETRA is one of the technologies that can satisfy public safety requirements. Due to its specific features, it is used widely not only in the EU but also in other territories like Asia and South America.

TETRA is a well-known TDMA two-way radio technology for digital voice and data. It was created by the European Telecommunications Standards Institute (ETSI). In the early 1990s, ETSI started developing to address the limitation of existing analog trunked services. The purpose was to create a unified system to support voice-over a digital technology for critical communications. The TETRA standard was completed in mid of the 90s and released to the market in 1997. It supports different frequency bands and can make interoperability among them; also, it has no dependency on the vendors. It is used to meet critical communication requirements for public safety organizations such as police, firefighters, medical services and etc. it is known for robust architecture and secure communication through features like end-to-end encryption, group calling, and data services based on narrowband Private Mobile Radio (PMR) communications. An important point about TETRA is that it is similar to other public safety communication systems like Project 25.

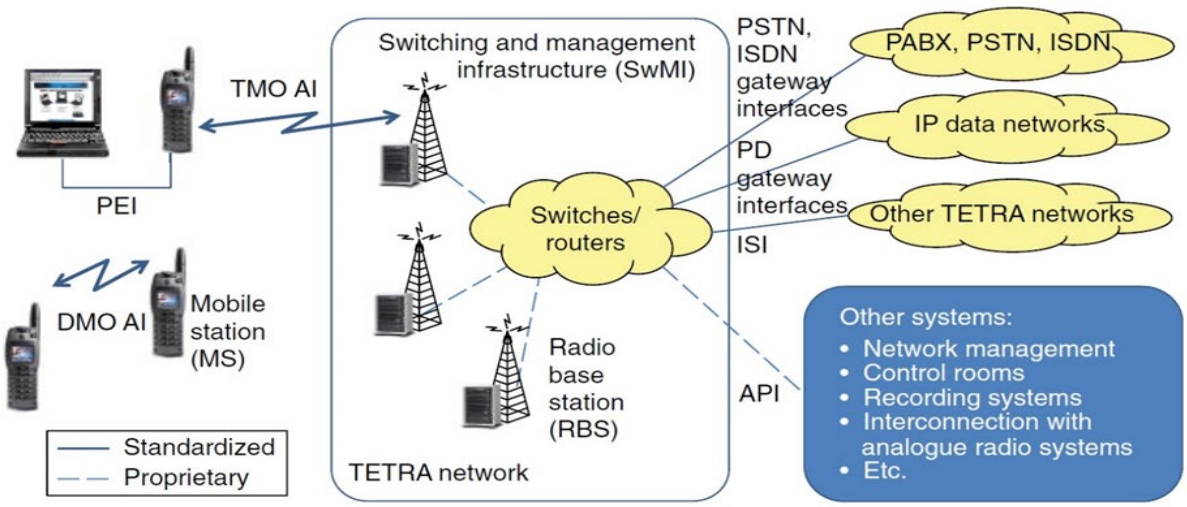

Figure 1: Network architecture of TETRA

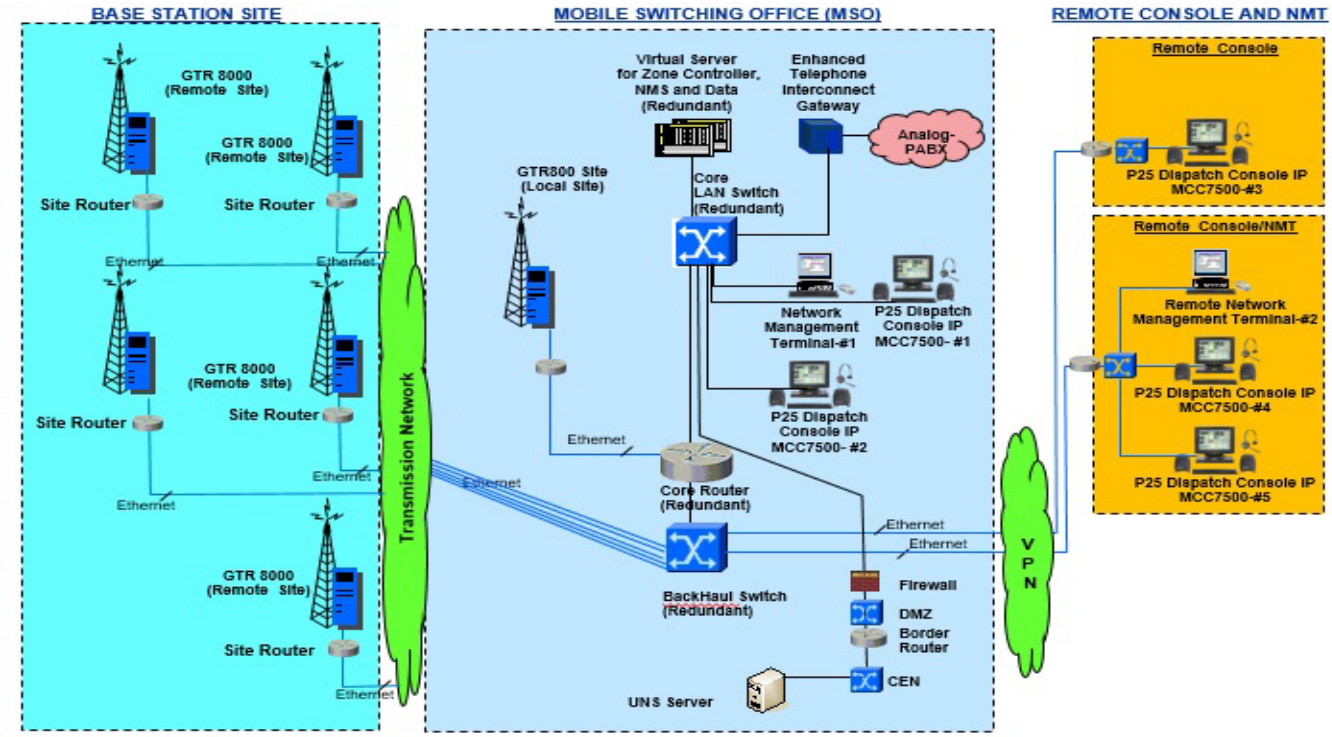

Figure 2: Network Architecture of Project 25 in USA

Like other technologies, TETRA has a physical layer that defines how bits are transmitted over the air including aspects like frequency, modulation, bit rate, frame structure, and channel access. Also, the TETRA physical layer is built for efficiency, robustness, and reliability in critical voice and low-rate data

communications. Due to robust modulation and error correction, resilient communication even in difficult radio conditions can be obtained.

One of the most important features of TETRA is the security and encryption mechanism which is one of the unique advantages of this technology. In TETRA, there are different security protocols according to sensitivity and use case of the solution, that can be used. The encryption key is varied from 32 to 192 bits, which makes the security algorithm so robust. Furthermore, each key is used for a specific use which makes this technology more flexible and robust in security terms. TETRA encryption algorithm (TEA) has 7 categories for different purposes in order to encrypt communications (for voice and video). Moreover, the Terminal Authentication Algorithm (TAA) is part of the mutual authentication process in TETRA's Air Interface Encryption (AIE), which ensures that a TETRA terminal (radio) is legitimate and authorized to use the network; also, the network is verified by the terminal. This feature prevents unauthorized devices from accessing the TETRA network and blocks unauthorized base stations.

This technology offers professional and regular call services for public safety use; besides, it can send messages and status updates. During a disaster, the landlines and mobile communications are getting full and search and rescue teams need to use the communication services without limitation in resource usage; also; there should be a system to allocate more resources to more important sections to make voice and video call and, in some cases, block the unnecessary units. Moreover, a system is essential to make a queuing system according to required resources which is known as priority handling. This feature is to manage the network resources, especially during high-traffic scenarios. It ensures that critical communications receive enough resources, precedence, and maintain reliability which is extremely important for public safety. In addition, it can provide group communication services, priority calls, seamless handover, GPS tracking and integration of voice and data which are very important for users during a mission-critical operation. In this technology, radio channels are centralized; in this way, each channel is assigned to a user automatically.

Another feature that is essential for a public safety communication system is high availability. It is one of the most important aspects of mission-critical services. In this case, the services must be available almost all the time. The availability for TETRA is close to 99.99 %. In order to achieve a high level of availability, TETRA networks use backup components. These backups are always kept up-to-date and ready to use if the main components fail.

Another point to be mentioned is the interoperability. One of the key strengths of TETRA is its high level of compatibility among products from different manufacturers. This is achieved due to The Critical Communications Association (TCCA)'s comprehensive Interoperability Certification process (IOP) that enables a multi-vendor market for TETRA in the case of equipment and systems. This open market benefits users with a wide range of compatible equipment, competitive prices, and rapid development of new products.

TETRA provides voice and dispatch services in direct mode operation (DMO) allowing direct peer-to-peer communication without reliance on infrastructure or trunked mode operation (TMO), which utilizes a centralized network for coordinated communications. They are one of the unique aspects of this technology with different use cases. TMO is used to transfer radio signals and two-way communication. The communication in this component is done through a network infrastructure which is a base station and switching and management infrastructure (SwMI). It is also used for point-to-point and point-to-multipoint communications that bring more secure voice and data transmission. This part is used in large

areas, particularly for public safety operations, transportation services, and utilities management. The network structure of this component secures reliable connectivity, centralized control, and efficient use of available frequencies. On the other hand, DMO allows the network components to connect with each other without base stations. It is an important component especially for public safety services because this feature allows first responders in an operation to connect to emergency personnel without any infrastructure if it may not be available or damaged. In this method, a radio device or a vehicle where radio devices mounted on it acts as a gateway to connect first responders who are out of range of primary infrastructure. Also, these team members can communicate with each other without any specific mechanism.

Also, the TETRA system uses virtual private network technology on a physical network that multiple organizations can share. In this way, due to the advantages of VPN technology, more security is the outcome of this method. Furthermore, each user group such as police, fire departments, emergency medical services, military, and public transport can use the TETRA network during disasters with the same infrastructure without compromising security or privacy. This feature brings scalability which is an important aspect of a technology.

Like other technologies that have been improved during the time in order to satisfy users' needs, TETRA release 2 or TETRA Enhanced Data Service (TEDS) is the enhanced version of this technology which was developed by ETSI too. It offers higher data rates and improved spectrum efficiency. It can support different Radio Frequency (RF) channel bandwidths such as 25, 50, 100, and 150 KHZ leading to higher speed rates which enables users to rate up to 500 kbit/s while version 1 is 28.8 kbit/s. Due to changes in market requirements, an enhanced version was released in 2005. It should be mentioned; that this version is completely compatible with the first version and can support the devices.

Another important aspect of TETRA is connecting to the cellular network which brings more advantages. Since mobile broadband devices have advanced in recent years, public safety agencies can utilize them more than before. As the quality of cellular networks improves, mission-critical users also need to use smartphones for their essential voice and data applications. In this way, Land Mobile Radio and Private Mobile Radio (LMR/PMR) industries can make it possible to use old narrowband networks and new broadband networks together. In this method, the TETRA network can communicate with high data throughput of broadband networks for voice mission-critical services. Also, transferring video streaming and high-quality images enhances situation awareness which is essential for today's mission-critical services. As a consequence, instead of transferring 7.2 kbps per timeslot or 28.8 kbps in total by using 4 timeslots in TETRA version 1 or up to 500 kbps for version 2, the TETRA over LTE can transfer 50 Mbps and above which is important for today's needs. This approach can be done in different ways. First of all, it allows existing LTE smartphone users to access TETRA services. This approach extends the TETRA network. This connection has the ability to control LTE bearer quality of service (QoS). An integrated or dedicated server/gateway manages the interconnection/translation for both traffic and signaling. In order to have a secure connection from smartphone users to the TETRA network, LTE users utilize VPN tunneling. It should be mentioned that this VPN tunnel (protocol) should be supported by the LTE network. Also, in some cases, if Wi-Fi or other networks are available, TETRA can switch to them. Different companies implement this feature differently; for instance, Airbus uses VPN on smartphones to connect to the Airbus cloud for mission-critical operation whenever other networks like W-Fi or LTE are available, while Motorola has implemented hardware on the radio devices that can switch to other networks in case of necessity like integrated solutions. The second one is gateways. It makes users use some services like GPS tracking, video

streaming, data transfer, and enhanced capabilities. In addition, it can work as a backup communication if the TETRA network fails; as a result, continuous service is ensured. In the gateway method, the push-to-talk (PTT) does not reuse TETRA protocol but it is based on other approaches like walkie-talkie but over cellular networks; so, the gateway should be adapted to TETRA requirements. The third approach is the integrated solutions. There is one server for the application layer, handling call processing. LTE users utilize an app on their smartphones; while TETRA users use their own devices. This approach is based on TCP/IP protocol.

Motorola, Hytera, and Airbus are the leading companies in TETRA technology. They bring some specific features thanks to their R & D departments; also, they can play an important role in introducing new solutions. In the TETRA market, Motorola is the leading solution for TETRA and TETRA over LTE. It is a company that provides important communication tools and services for businesses and governments. It was founded in 2011 after the separation of the original Motorola company. It provides more than 8 base stations and over 15 radio devices for various scenarios and applications from small networks to enterprise TETRA networks. Another important company is Hytera Communications, founded in 1993 in Shenzhen China, is one of the most famous providers of TETRA and other mission-critical solutions. Their TETRA systems offer secure, reliable, and efficient communication designed to meet the needs of industries like public safety, transportation, etc. Their system is according to ETSI standards which means it guarantees, it can work with other brands. Also, it ensures easy integration and reliable communication across different platforms. Hytera has purchased the TETRA manufacturing previously owned by Rohde & Schwarz. The third important company is Airbus. Airbus TETRA solution is one of the most famous manufacturers and a leading one in the world. It offers secure and reliable communication with instant push-to-talk features, helping teams stay connected. The system also works well with broadband networks, providing both voice communication and fast data services to improve operations. There are some other companies with less market share such as Funktel, Cassadian, Sepura, and Damm. Their radio devices and base stations have been discussed and compared with the other companies in the thesis.

Contents:

List of figures:

List of tables:

Acronyms:

PPDR	public protection and disaster relief
TETRA	Terrestrial Trunked Radio
LTE	long term evolution
PP	public protection
EMS	element management system
ECC	Emergency control center
PSAP	public safety answering point
PS	public safety
GSM	Global System for Mobile Communications
GPRS	General Packet Radio Service
EDGE	Enhanced Data rates for GSM Evolution
HSPA	High Speed Packet Access
ITU	International Telecommunication Union
DMO	direct mode operation
TMO	trunked mode operation
PSTN	public switched telephone network
DM-MS	direct mode management system
TEDS	TETRA Enhanced Data Service
UMTS	Universal Mobile Telecommunications System
VOIP	Voice over IP
3GPP	3rd Generation Partnership Project
Wi-Fi	wireless fidelity

LOS	line of sight
VSAT	very small aperture terminal
MSC	mobile switching center
AGA	air–ground–air
eMLPP	Enhanced Multi-Level Precedence and Pre-emption
AES	Advanced Encryption Standard
TEA	TETRA Encryption Algorithm
TAA	Terminal Authentication Algorithm
CKM	Cryptographic Key Management
GKM	group key manager
KSS	key stream sequence
SCK	Static Cipher Key
DCK	derived cipher key
DMR	Digital mobile radio
FIFO	first input first output
MPLS	Multiprotocol label switching
DHS	Department of Homeland Security
DQPSK	Quadrature Phase Shift Keying
FDMA	Frequency Division Multiple Access
TDMA	Time division multiple access
ACELP	Algebraic code-excited linear prediction
SACCH	Associated Control Channel
SNR	signal to noise ratio
NATO	north Atlantic Treaty Organization

QOS	quality of service
ISDN	integrated service digital network
SWMI	switch and management interface
AIE	air interface encryption
E2EE	end-to-end encryption
IV	initialization vector
SDS	short data service
GPS	global positioning satellite
IOP	interoperability certification process
TCCA	the critical communication association
MNC	mobile network code
MMC	mobile country code
GSSI	group short subscriber identity
GOS	grade of service
PTT	push to talk
MCPTT	mission critical push to talk
IWF	interworking function
SSL	secure socket layer
TLS	transport layer protocol
GRE	Generic Routing Encapsulation
VPN	virtual private network
IPsec	internet protocol security
RFID	Radio-Frequency Identification
TAA	TETRA authentication algorithm

ECC	Emergency control center

Chapter 1: network requirements for Public Safety

1.1. Introduction

Nowadays, public protection and disaster relief (PPDR) are widely used in all regions (cities and rural areas) because it brings essential characteristics like security and stability in the society and it secures environment to maintain law and order; besides, it is to protect the life and values of citizens. Due to this reason, it is also called public safety. If we want to describe the usage of public safety, we should mention firefighting systems, Emergency medical services, law enforcement, emergency and surveillance situation on land and air. They protect people lives, their property, environment and everything about the society. To make an organization and cooperation among them to have a better service, we need a network to connect them; as a result, it is known as public safety network. In this way, radio communications are so important. except these organizations, public authorities at different levels are the other users of this service. Military force is another organization that utilizes the PPDR.[1]

The telecommunications industry has been around for many years and it has made possible global communication. Radiocommunications are a part of telecommunications which is so important for PPDR. [2]

The communications in public safety are divided into 2 parts. First one is public protection (PP) and second one is disaster relief (DR). PP is the radiocommunication by the responsible agencies to deal with execution of the law and order, life protection and other emergency situations and DR is radiocommunication to the society to inform people about disasters, health issues, catastrophes regardless of human-made or natural.[1]

The emergency communications in PPDR are divided in 4 categories.

1. Communication between authorities/organization: it is the communication within and among organizations
2. Communication between authorities/organization to citizens: the communication of authorities with people or group of people.
3. Communication of citizens with authorities: it is the emergency call services
4. Communication among citizens

Services provided by PPDR are law enforcement (the function to prevent, investigate, apprehend or detain any individual), EMS (emergency medical service), firefighting, protection of the environment, search and rescue, border security, emergency management. In each part of the world, they may have different tasks and organizations. They are governmental organizations but, in some cases, some private organizations may also work with them.[1]

1.2. Frame work and communication requirements

1.2.1. public safety service fundamentals

PPDR services are widely used every day. For example, a disorder in a city happens; in this way, people need to call the emergency services. The system should be scalable, accessible in a case of an incident.

Now, we can sort the PPDR operation scenarios as below.

- First, the operational scenarios for PPDR are day-to-day operation which is a normal operation in a day.
- second, large emergency or public events that the PP which public protection and DR stands for disaster recovery are used and even the help of other jurisdictions may be requested to handle the problem.
- And the third of is disaster which means use of PPDR in case of a disaster. In this case, international aid may be requested.

These operations are in different domains which can be mentioned as urban environments with high density of people, rural environments with lower density of people but with more obstacles like hills, mountains, blue and green border like lake for blue and land for green and finally Port and airport like the urban environment with lower density of people with limited facilities. [1]

There are 3 dimensions to describe the operational scenarios.

- Geographic extension mentions the size of the area involved in the crisis,
- environmental complexity that describes the complexity of the emergency
- and the crisis severity that describes the level of risks to citizens. [1]

The system that is implemented for the disasters must be flawless in a way that can handle the enough network capacity to make many communications in a moment as well as enough capacity for the data to transfer. The duty to serve in public safety includes creating a safe, secure, and efficient communication system that prioritizes communication among responders. Modernizing networks, broadband applications, and social media brings both opportunities and challenges for public safety stakeholders. To address this, policies have been developed to involve the entire community in national preparedness efforts. In the U.S, the Department of Homeland Security (DHS) has worked with local governments to update the National Emergency Communications Plan, which integrates voice, video, and data sharing for all situations. The plan's success depends on the collaboration of the emergency communications community. [2]

About the network capacity these parameters have to be considered.

- Taking of calls and making dispatches
- Facilitation of the emergency resource management and the law enforcement unit
- Ensuring officer safety
- Creation of a system for handling reports
- Facilitation of special situation implementation of law enforcement agencies

The system must help manage the services and bring the facilities such as:

- Dispatches and call taking
- The resource controlling the local and national fire service apparatus
- The facilitation of fire alarm dispatching
- Conducting and coordinating the state fire incident command systems
- Facilitation of quick communication concerning hazardous materials

Also, the system must have the capacity for emergency medical services (EMS) communication elements such as:

- Fast and secure call taking and dispatch of the (EMS) personnel
- Efficient management of the allocation of EMS resources
- Enhanced management of EMS units
- Integration of specialized training in taking caller questions
- Facilitation of quick medical instructions on the telephone. [2]

when planning and implementation of communication in public safety is discussed, five components are mentioned.

1. facilitate communication among responders, law enforcements and people
2. ensure safe, fast and efficient communication within an agency
3. secure and efficient communication among agencies
4. interoperable communication among agencies
5. reliable communication among public safety agencies and support services

An efficient system must support a protocol to provide extra personnel and equipment during emergency situations. [2]

1.2.2. framework

Now, we dive into the frameworks. In framework, we have different categories as below.

- First is intervention team who are the core team to deal with crisis,
- next one is intervention team leader who are the leaders and need to have good understanding the situation
- we have dispatchers who supports intervention team and the last one are the backup team.

The communications can be intra communication which means in a jurisdiction and inter communications mentioning among different jurisdictions. The events are divided in 3 categories.

- First of all, day to day a routine operation with neighboring agencies to provide support or back up.
- Task force which means cooperation between different agencies.
- and mutual aid meaning to describe major events with large number of agencies.

It should be mentioned that 90 percent of scenarios are day-to-day activities so the system should support day-to-day and the other scenarios with the same performance. It means, when a disaster happens system should manage the communications like day-to-day missions. [1]

When a disaster happens, the groups to handle the situation from different organizations is created such as police, firefighters, medical services and etc. This communication framework can be like this.

- Firstly, Communications among PPDR unit/team on the field. They make communications with the mobile members of a team or with the other team members. Emergency control center (ECC) is the core part deployed for PPDR which is the house number of operational systems.
- Another central element is the public safety answering system (PSAS). In this section the physical calls are from citizens are received. For some specific situation temporary headquarters can be established. In a team, team members need to communicate with each other. This communication is to manage the team, considering the situation and reassembling the team, enabling the reports and etc. secondly, communication between ECCs which is emergency control center and team members is essential too. The main feature for this communication type is described as seamless radio coverage through the used area, enough traffic for the incident, sufficient voice quality not to disorder the communication and some special features to change the settings in real-time.
- Thirdly, Connection between ECCs can be through fiber optics, microwave, copper land lines to show the importance of the connection between the ECCs, this should be mentioned that if a wrong call is connected to an ECC it should be forwarded to another center, more than one ECC is involved in an operation.

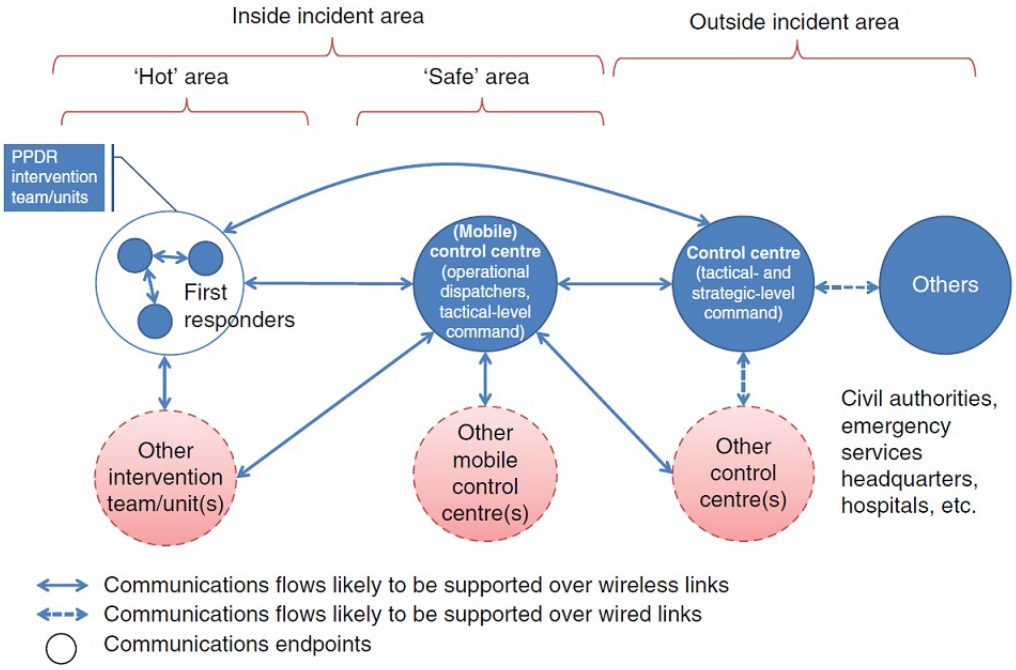

Figure 1.1: communication flows in an incident.[1]

Communications requirements among ECCs must:

1. Establish communications links to support speech and data services.
2. Conform to the relevant procedures established by the ECCs or their organizations.
3. Support conference calls

- Fourthly, another type is communication among PSAP and ECC. PSAP and ECC are two different functionalities that may or may not be integrated. The PSAP, after reception of an emergency call from an individual/citizen, communicate without delay with the competent ECC and transmit the location and nature of the emergency of the calling party along with any other relevant information that may be available associated with the call. So, a good connection among all ECCs is important to transmit voice and data received by an PSAP.
- Fifthly, communications among PSAPs. it should be mentioned that the PSAP works independently and it is not subjected to special need. Their tasks are subjected as below:
    1. The call is controlled by the receiving PSAP.
    2. The call is immediately transferred to the normal PSAP, which handles all the case. So, the location must be accessible to other PSAPs.
    3. Depending on local procedures, the receiving PSAP may transfer the call directly to the relevant
- Last but not the least, another type of communication is the communication the special task force, temporary headquarters and the ECCs. They need permanent bidirectional links. It should be available during a disaster.

It should be pointed out that it types of communication needs to be effective, fast, reliable as well as secure. It depends on the availability of the network to give the real-time service. To describe better, two types of operational situation is mentioned:

- Mission‐critical situations
- Non‐mission‐critical situations

1.3. Voice services and data services for PS

There are some key elements to describe the voice services in PS.

- Direct to talk around: it is a unit-to-unit communication when wireless network in not accessible. It means communication with infrastructure is not accessible.
- Push to talk: it is a standard communication happening today. By pushing a button on the communication device, voice is transmitted to the other units.
- Group call: it is a communication from one to many
- Full duplex: like the wireless and PSTN in today.
- Emergency alerting: in life-threating condition and require access to the system immediately.
- Audio quality: which is so important to have a high-quality voice communication

Another services to be mentioned is data services. this type of communication is used in addition to voice services. For instance, the video communications such as video for tasks like crime scene monitoring, highway surveillance, and assessing damage from wildfires using real-time video from drones or aircraft is another type of communication which is used in PPDR. Due to the growing of full motion video streaming, the application of these services is growing more and more.

Different applications require different rates for speed, reliability, and capacity. Some of them needs dedicated communication systems; however, these systems should allow other apps to share the data when it is needed. Using common standards can help exchange the required information smoothly. When multiple apps share a network, there should be enough capacity to handle all the data. [1]

The table below illustrates a list of potential data-centric applications for PPDR use.

Service	throughput	timeliness	robustness
Voice communication	Low	Real-time	high
Video streaming	High	Real-time	medium
Positioning info	low	high	high
messaging	low	Real-time	high
File transfer	Medium to High	Some delay	medium
Video (slow scan)	medium	low	low
Data base access (remote)	medium	Some delay	medium
Personnel monitoring	low	high	high

Table 1.1: a list of potential data-centric applications for PPDR use

1.4. Communication systems for PPDR

It relates to main communication technology used in PPDR. First, we look into the requirements for the communication.

- Service capabilities and performance: required services for a PPDR operation are such as

  PTT operations, broadcasting/group communications and talk around for voice communications.

  Some of them are in motion. Fast responsiveness and low latency requirements are typically required for these services. High quality equipment is needed in this way

- Strict control of the communications means: it is the cooperation and control of communication channels. It considers the group calls and the administration of the terminals. [1]

- Security‐related requirements: reliable communication between PPDRs and within a PPDR that requires security for this purpose. It may cover the security encryption and integrity mechanisms. [1]
- Coverage: the complete coverage is essential for a PPDR. This coverage is 24/7/365. In case of a mission, due to the load on the network, some other equipment can be added to better service such as repeaters and reconfiguration of the network. In addition, the indoor and outdoor coverage is required. [1][2]
- Capacity: When a disaster happens, there is more traffic; in this way, the required traffic should be anticipated. For example, by using transportable base stations and other required devices.
- High level of service availability: Service availability relates to the amount of time (usually per year) that a service is up and running. It needs layered redundancy [1][2]
- System reconfiguration: rapid reconfiguration of the system in PPDR is essential. This includes robust operation, administration and maintenance [1]
- Interconnection: communication to public network may be needed; so, the connection to mobile terminals and percentage terminals is done based on the particular PPDR operational requirements. [1]
- Interoperability: it is done in different levels. From basic level such as communication of firefighter of an organization to the higher levels. It is not technical aspect sometimes it relates to legal frameworks. It is not limited to frequencies and equipment communication via dispatch centers, interconnection of the PPDR networks through wire line interfaces or use of technologies like radio communications. [1][2]
- Spectrum usage and management: it needs to have access to other terrestrial mobile networks. There may be some systems to support PPDR; in this way, the number of interfaces to support PPDR from non-PPDR should be minimized as much as possible. [1]
- Regulatory compliance: it should be supported by different regulations. A huge range of frequencies needs to be supported. It should be mentioned that the agreement between different regulations and the PPDR system is needed to do this feature. Various types of systems like HF, satellite, amateur, etc. [1]
- Cost-related requirements: it is extremely important because the authorities invest on these facilities every 10-15 years, so cost-effective requirements are very important as well as they should be resistant. [1]
- Scalability: the services need to be available in different speeds, cell loads, etc. [2]
- Availability: the network should be available 100% of the day. [1][2]

1.5. Used technology for PPDR communication

A common classification of technologies used for PPDR communications is based on the average data rates required by the supported PPDR applications [3]

- Narrowband (NB): it delivers voice communication as well as the low data rate communications. The data rates are around a few hundred kilobits per second and radio frequency channels up to 25 KHZ [1]. TETRA and TETRAPOL uses this technology and Project 25 (P25), which provide wide-area network coverage. it is person to person or one to many communications with PPT [2]. Besides, analogue systems are conventional and trunked. They are called as professional/private mobile radio (PMR) or land mobile radio (LMR) technologies especially in north America. While, these systems are used in North America, they are used in other sectors like transportation, industry, private security, and the military.[1]
- Wideband (WB): it refers to the technologies that can carry data rates around several thousand kilo bit per second. The PPDR system to support WB are under development. The TETRA enhanced data service (TEDS) is an example. The radio frequencies are up to 150KHZ. It is emailing possible communication with attachment. Downloading and uploading images [1]. This technology provides data rates for application between 384 to 500 kbps. TETRA 2 utilizes this technology to transmit more data rates. But it is not widely used in the market because it cannot satisfy the required data rates for all apps [2].
- Broadband (BB): this mentions the technologies with higher data rates that carry more information and is utilized for data consuming apps. They are the candidate to support PPDR. Thay are Wi-Fi like radio interfaces that can be operated on open bands such as 4.4 GHZ for military and 4.9 GHZ for PPDR in some countries. The LTE is being developed under BB for PPRD. Internet and intra net access, video streaming, remote control for robotic devices, high resolution images [1]. The data rates can go up to 300 Mbps in LTE networks. a good example for this technology is TETRA over LTE (long term evolution) which improves the bandwidth and capability of the TETRA for PPDR. [2].

Chapter 2: characteristics of TETRA network

2.1. introduction

TETRA is a well-known TDMA two-way radio technology for digital voice and data. It was created by the European Telecommunications Standards Institute (ETSI) [1]. In early 1990s, ETSI started developing to address the limitation of existing analogue trunked services. The aim was to create a unified system to support voice over a digital technology for critical communications [18]. The TETRA standard was completed in mid of 90s and released to the market in 1997. It supports different frequency bands and can make interoperability among them; also, it has no dependency on the vendors [1]. It is used to meet critical communication requirements for public safety organizations such as police, firefighters, medical services and etc. it is known for robust architecture and secure communication through features like end-to-end encryption, group calling and data services based on narrowband PMR communications. [25] An important point about TETRA is it is similar to other public safety communication systems like project 25. [6].

This technology offers professional and regular call services for public safety use; besides, it can send messages and status updates. Another important point to be mentioned is that in this technology, digital encryption and high audio quality are offered. [1] in addition, it can provide group communication services, priority calls, seamless handover, GPS tracking and integration of voice and data which are very important for users during a mission-critical operation. In this technology, radio channels are centralized; in this way, each channel is assigned to a user automatically [2].

TETRA provide voice and dispatch services in direct mode operation (DMO) allowing direct peer-to-peer communication without reliance on infrastructure or trunked mode operation (TMO) which utilizes a centralized network for coordinated communications [2] .Also, it includes various technical aspects like air and network interfaces. Error correction is another aspect of this technology to be mentioned. [2]

TETRA system uses virtual private network technology on a physical network that multiple organizations can share it. In this way, each user group can use the TETRA network during disasters because public cellular networks are unstable or out of service due to overload. [2]

TETRA has two versions and like other technologies, it has enhanced over time. The first version included voice and data but was not sufficient due to the increase in demand from the users within the public safety agencies [2]. The second release of TETRA is enhanced version was developed to improve data communication and it offers wider channels to support higher data rates. This version was released in 2005 [1].

Another advantage of TETRA network is that due to requirement of sending video streaming and data with larger sizer, TETRA has the ability to integrate with mobile broadband communication like 4G/LTE and 5G. in this way, when responders are out of TETRA coverage, TETRA network is down or they need to send large data files that requires broadband communications, they can switch to mobile network. [2]

2.2. physical layer characteristics

TETRA has different technological features related to physical layer that are explained as below.

2.2.1. fundamental features

1. Modulation is π/4. TERTA uses differential Quadrature Phase Shift Keying (DQPSK) for the primary modulation technique. It is efficient for digital communication and useful to reduce errors [4]. DQPSK involves the polarization multiplexing of two different QPSK signals. As a result, spectral efficiency has improved by a factor of 2. It is an alternative to use 16-PSK, instead of QPSK to double the spectral efficiency [5]. It reduces unwanted emissions but can create signal fluctuations. As a consequence, it needs a less efficient linear power amplifier.[8]
2. Modulation rate is 36 Kbps. This rate has been achieved by the π/4 Differential Quadrature Phase Shift Keying (DQPSK) modulation scheme. The symbol baud rate is 18,000 symbols per second and each symbol is mapped to 2 bits. As a result, the modulation rate is 36000 [6].
3. To improve data transmission capabilities, adaptive modulation techniques have been utilized. In this way, the dynamical selection of the modulation depends on the current network conditions; therefore, we have optimization of data throughput and reliability (in TEDS). For instance, in a normal and favorable condition, higher-order modulation schemes can be utilized in order to increase data rates, while more robust schemes can be used in challenging environments to ensure reliable communication. [37]
4. TETRA frame has four timeslots per TDMA frame and is organized into 18 TDMA frames per multi frame. In circuit mode, traffic is compressed from 18-frame multi frame into 17 TDMA frame. In this way, the 18^{th} frame is left for control signaling. This control frame is to enable the Slow Associated Control Channel (SACCH). It provides a constant background control channel signal even when all channels are busy. It is a key feature of TETRA protocol.[36] In addition, it is possible to have four separated communication channels to share a same bandwidth. the system utilizes ta combination between FDMA and TDMA.[4]
5. Voice coder rate is ACELP (4.56 kbps net). In this technology, the net data rates are 4.56 kbps and a gross are about 7.2 kbps. It is designed for high-quality voice transmission [7]. This is a very efficient voice coding method. It uses a speech coding algorithm that distributes pulses to a linear prediction filter. [36] It is a type of linear predictive coding (LPC) based on the code-excited linear prediction (CELP) method. The main advantage of this function is its algebraic codebook that can be made very large (over 50 bits) without causing issues with storage (RAM/ROM) or complexity (CPU time). [15]

2.2.2. Channel characteristics

1. Channel spacing is 25 KHZ. Channel spacing refers to the separation between different radio channels to avoid interference and to ensure a clear communication. Each radio channel has a bandwidth of 25 KHZ. The separation between uplink and downlink is 10 MHZ. [4].

2. Channel Coding and Error Correction: in order to improve data integrity, TETRA utilizes robust channel coding techniques. It is based on two ways. First one is conventional encoding. It provides error correction capabilities to decrease the effects of transmission errors. And the second one is scrambling. In this method, data security and minimization of the likelihood of repetitive patterns that could lead to signal degradation should be ensured
3. A single slot has 255 usable symbols, with the rest of the time used for synchronization and other functions. One frame contains 4 slots, and a multi frame is 1.02 seconds which contains 18 frames. Hyper frames are also used, mainly for synchronization with encryption algorithms. [15]
4. Maximum data rates are 28.8 kbps. This data rates are achievable when the four slots of a 25-kHz carrier are combined and the data is sent with error control but with lower protection. [1]

2.2.3. Frequency characteristics

1. This technology operates in 380 to 470 MHz frequency range. Each cell has a pair of carriers for uplink and downlink that are separated by 10 MHz (VHF) or 45 MHz (UHF). By using TDMA, each carrier provides 4 physical channels with slots of 14.167 ms and a 25 kHz bandwidth. The TETRA TDMA Frame lasts 56.67 ms. The first time slot on the first carrier transmits the BCCH (broadcast control channel) for synchronization and control [7].
2. Each frequency range which is used in TETRA has some specific name and usages that are sorted as below.

Frequency range (MHZ)	Usage field	More information
380–385 / 390–395	Emergency Services	Used by emergency services like police, firefighters, and disaster relief services, mainly in Europe.
410-430	Civil & private networks	Used in many European and Asian countries for government and civilian networks.
450-470	Commercial & private networks	Utilized for business, transport, and private security services.
806–821 MHz & 851–866 MHz	land mobile radio services	critical communication systems for industries like transportation and utilities

Table 2.1: the frequency rages for TETRA

Now, we can observe the frequency range of TETRA for each country.

Country	Frequency range (MHZ)	Application
France	380–400	Emergency services
	410–430	Civil & private networks
Belgium	380–386.5	Emergency services/civilian
	390–396.5	Emergency services/civilian
	410–420	Civil & private networks
Netherlands	380–386.5	Emergency services
	390–396.5	Emergency services
	410–430	Civil & private networks
Germany	380–385	Emergency services
	390–395	Emergency services
	406–410	Direct Mode Operation (DMO)
Ireland	380–385	Emergency services
	390–395	Emergency services
	385–389.9	Civilian/private
	395–399.9	Civilian/private
Italy	380–390	Emergency services/armed forces
	462	Civilian/private
Norway	380–385	Emergency services
	390–395	Emergency services
	406.1–426	Civil & private networks
	870–876	land mobile radio services
Slovenia	380–385 (MS)	Emergency services
	390–395 (BS)	Emergency services
South Africa	420–423	Emergency services, public works
Sweden	380–395	Emergency services
	425–429	Civilian/airport/public transportation
UK	380.0125–384.9875	Emergency services
	390.0125–394.9875	Emergency services
	410.0125–412.9875	Civil & private networks
	420.0125–421.9875	Civilian/private
	450, 460 / 452, 462	Commercial & private networks
	454, 464 or 460	Commercial & private networks
	423, 413	Civilian/private
Hong Kong	382.65–399.9	Emergency services
	410–430	Emergency services
	806–818	Civil/Private
	851–863	Civil/Private
Portugal	380–395	Emergency services
	420–430	Commercial/Private
Saudi Arabia	350–370	Military & Security
	380–395	Emergency services

	385–399.99	Emergency services
	410–430	Civil & private networks
	450–470	Commercial & Regional
	870–921	land mobile radio services

Table 2.2: TETRA frequency ranges by each region [6]

2.2.4. Diversity reception

It is a technique also known as space diversity or spatial diversity in order to improve signal quality reception and reliability by reducing the adverse effects of fading and interference. It is obtained by utilizing different antennas to receive a same signal through different propagation paths; in this way, the likelihood of signal degradation reduces. Since in our signal, we have multipath propagation due to obstacles on the signal way, rapid fluctuation in signal amplitude is inevitable; as a result, diversity reception helps counter these fluctuations. It is helpful to have a stable and reliable communication. By combing signal from different antennas, the system can enhance the overall signal-to-noise ratio; as a consequence, we have clearer audio and data transmission. [41]

2.2.4.1. Implementation in TETRA base stations

in TETRA base stations, we have 3 different diversity reception techniques that are explained as below.

- The First technique is single diversity reception. It uses a single antenna to receive the signal. This method does not employ any diversity techniques, such as space or polarization diversity to improve signal quality and reliability. As a result, single diversity reception is more prone to have issues like signal fading and interference which can affect the overall performance of the communication system.[41]
- The second technique is dual diversity. Some base station like MTS2 Motorola series use dual diversity based on 2 antennas to receive signal. In this way, we have a better signal reception. There are two different techniques to implement this kind of diversity
    1. Audio Switching Diversity: this method uses two antennas to avoid problems that are caused by signal reelection. The antennas should be far enough from each other. Only of the antennas is used. In this way, switching will happen when the signal from one of antennas gets too weak
    2. Ratio diversity: two receivers are employed at a same time and their audio outputs based on the signal levels are mixed. A panning circuit starts working when the signal level is high and keeps working until both receivers have strong signals again. This method can anticipate early signal drop out and switches to the stronger one

(with higher signal-to-noise ratio, SNR) before noise occurs [42]. this kind of diversity (maximum ratio combining) is employed in airbus base stations which improves the uplink budget by 3 to 8 dB compared to single receiver antenna solutions. [45]

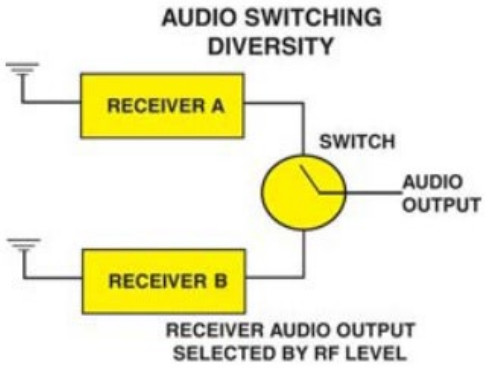

Figure 2.1: audio switching design [45]

- The third technique is triple diversity. Advanced base stations, such as the Hytera DIB-R5, support triple diversity reception. In this way, by using three antennas, the better signal reception is achievable. It is used to ensure secure and reliable voice communication and high-speed data transmission. [43]

2.3. advantages of TETRA network

The main benefit of TETRA in comparison with other technologies such as GSM are:

- The lower frequency used by TETRA provides a longer range, which means it can cover larger areas with fewer transmitters. It leads to reduce infrastructure costs.
- During a voice call, TETRA communications are not interrupted when moving to a different network site. This feature is often found in PMR networks and includes fallback modes like base stations handling local calls.
- when there is no network, mobile devices are switched to direct mode and they share the channels directly (walkie-talkie mode)
- In gateway mode, a single mobile connected to the network can relay signals for other nearby mobiles that are out of range. This does not need a dedicated transponder system, unlike analogue radio systems

- TETRA offers a point-to-point function that traditional analogue emergency radio systems did not provide. This feature lets users create a one-to-one radio link between devices without requiring a control room operator or dispatcher.
- Unlike cellular technologies that connects one person to another (one-to-one), TETRA can handle one-to-one, one-to-many, and many-to-many connections. These modes are particularly useful for public safety and professional users during a disaster.
- Portable and deployable network solutions are available for PPDR operations for a temporary mode.
- Network solutions are available in both reliable circuit-switched architectures (like telephony) and flat IP architectures with soft switches. [6]
- TETRA offers very fast call setup time (300 ms), which is important for public safety and emergency services. It supports both semi-duplex (for group communication) and duplex (for individual calls) operations. TETRA provides group calls and one-to-one call communications which is important for mission critical operations. Also, since it has priority call management, it can handle urgent network traffic effectively. [36]
- TETRA backhaul Network Redundancy Plan for Disaster Recovery in Mission Critical Communications is about creating a robust and resilient network infrastructure to ensure continuous communication during emergencies. Emergency radio systems are essential for ground forces in disaster recovery. TETRA is a global standard for mission critical mission and with 4G-LTE/5G can be used. Developing an emergency network is based on the two main challenges:
    - Careful planning and optimization: the base station should have good coverage
    - Creating resilient radio backhaul connections: which is a redundancy plans for fast recovery in TETRA technology. [1]

radio backhaul connects BSs to the network backbone through Mobile Switching Centers (MSCs), which is connected to other networks like the Public Switched Telephone Network (PSTN).

In order to deploy critical radio links, we need to consider factors like traffic intensity, propagation conditions, deployment cost, site locations and interference. Optical fiber is common for base station (BS) connectivity due to high bandwidth and low attenuation. However, in rural and forest areas, optical fiber is costly and not robust against fire. Satellite links offer resilience due to constant Line-Of-Sight (LOS), but are very expensive to maintain for all BSs nationwide. Microwave backhaul links offer a cost-effective middle ground. Although they have limited capacity and shorter ranges compared to optical fiber, they can provide high data rates up to 1 Gbps. Their deployment is simple. It does not require infrastructure along the radio link which makes them less vulnerable to events like wildfires. [17]

- One important aspect of TETRA network is TETRA Mobility Management. This feature is like GSM. It includes a database that stores user information, subscribed services, cipher keys, and user identities. When a user visits a different network, authentication happens via the home database, and essential user information is downloaded to the visitor database.[2]

2.4. TETRA version 2

TETRA release 2 is the enhanced version of this technology which is developed by ETSI too. It offers higher data rates and improved spectrum efficiency. It can support different RF channel bandwidths such as 25, 50, 100, 150 KHZ which leads to higher speed rates. Besides, the supported modulation schemes are π/4-DQPSK, π/8-D8PSK, 4-QAM, 16-QAM, and 64-QAM which enables users bit rates from 100 to 500 kbit/s. Due to changes in market requirements, the manufacturers decided to improve TETRA standards to satisfy these needs. As early 1999, the both manufacturers, technical committee and TETRA association, identified that this technology should be enhanced in different areas. In this way, enhanced version was released in 2005. [34]

We can monitor the standardized features of version 2 as below.

- Trunked Mode Operation (TMO) Range Extension: TETRA network has the ability to cover an area about 58 KM. However, the longer range was required for some organizations in order to have a better service in air-ground-air (AGA). For this requirement, by changing burst rate in uplink and downlink as well as guard time, the TMO range of TETRA can be extended to 83 KM.
- Adaptive Multiple Rate (AMR) Voice Codec: the rate of this codec is around 4.75 kbit/s and it was chosen for possible use in the future. However, it has been suspended due to the market requirement in the future.[34]
- TETRA Enhanced Data Service (TEDS): it is a high-speed TETRA service which it uses different RF channels bandwidths and data rate in order to have flexible use of PMR frequency bands. This release is fully compatible with the first release. It has been designed and optimized for PMR frequency bands and it is for all TETRA market application. Table 2.3 illustrates different RF channels and data rates supported in this technology. [34]

Modulation	Channel bandwidth			
*	25 KHZ	50 KHZ	100 KHZ	150 KHZ
π/4-DQPSK	15.6	*	*	*
π/8-D8PSK	24.3	*	*	*
4-QAM	11	27	58	90
16-QAM	22	54	116	179
64-QAM (r=1/2)	33	80	175	269
64-QAM (r=2/3)	44	107	233	359
64-QAM (r=1)	66	160	249	538

Table 2.3: Packet Data Throughput Downlink [kbit/s][34]

With use of adaptive modulation schemes, user bit rate is from 10 to 500 kbit/s. The TETRA protocol stack is reused as much as possible in order to an easy transition from TETRA release 1. TEDS can support up to 8 multimedia applications and allows for QOS negotiation for real time applications like voice, video, and telemetry by checking the delay, throughput, priority and reliability. It also supports sectored cells which can enable the use of existing TETRA release 1 base sites without requiring additional sites. [34]

In table 2.4, we can observe the issues of TETRA release1 and market needs to release version 2.

Market needs	issues	TETRA user requirements
Mission critical multimedia data for multiple users	TETRA Release 1 can handle some multimedia (e.g. slow scan video),	High Speed Packet Data (TEDS)
Roll-out of nationwide networks	not to install extra sites when upgrading to TETRA 2 Continue to use TETRA 1 radios	TETRA R2 backwards compatible with R1. Operate inside TETRA R1 frequency bands.
Air to ground & linear utilities	Small proportion of applications operate over much larger distances.	Enhance coverage
Deploy TETRA for special operations	Specialist users want full duplex telephony to own networks	NATO codec
Complement 3G in PMR/PAMR	Need to optimize for 3G - compatible services, provisioning, roaming etc.	High Speed Packet Data (TAPS or TEDS) AMR codec, SIM evolution Spectrum efficiency, Network capacity, system performance, QoS, terminal optimization

Table 2.4: why we need TETRA release 2 [34]

now, we can compare the features of release 1 and 2 by table 3.

feature	Release 1	Release 2
Maximum data rates	Up to 28.8 kbps (multi-slot packet data)	Up to 500 kbps (TEDS with 64-QAM)
Modulation scheme	π/4-DQPSK	π/4-DQPSK, π/8-D8PSK, 4-QAM, 16-QAM, 64-QAM
Channel bandwidth	Fixed 25 kHz	Flexible: 25 kHz, 50 kHz, 100 kHz, 150 kHz
Spectrum efficiency	Lower	Improved efficiency with wider bandwidth options
Voice capability	Digital Trunked Radio with high-quality voice	Improved voice handling and simultaneous voice & data transmission
security	Encryption and authentication	Enhanced encryption and security measures

Use case focus	Primarily voice communication with limited data	Enhanced data services for mission-critical applications
Backward compatibility	N/A	Compatible with TETRA v1 systems

Table 2.5: comparison between V1,2

TETRA V+D radio terminals with TEDS need more RF bandwidth in comparison with base station equipment. Although TEDS-only radio terminals won't have Direct Mode Operation (DMO), every TETRA PSS Network will always have both TETRA V+D and TEDS radio terminals that have been deployed nationwide. because of these factors, the maximum required bandwidth for a radio terminal to transmit and receive the signals are determined. [16]

2.5. Interfaces of TETRA

TETRA has various interfaces. First, we describe the interfaces.

- Interface 1 is the radio air interface.
- Interface 2 is the line station interface.
- Interface 3 is intersystem interface. It allows the interconnection of the TETRA networks by different manufacturers.
- Interface 4 mentions the terminal equipment interface for the mobile station. It refers to the terminal equipment interface for a line station.
- Interface 5 refers to the network management interface.
- interface 6 refers to the direct mode interface.[2]

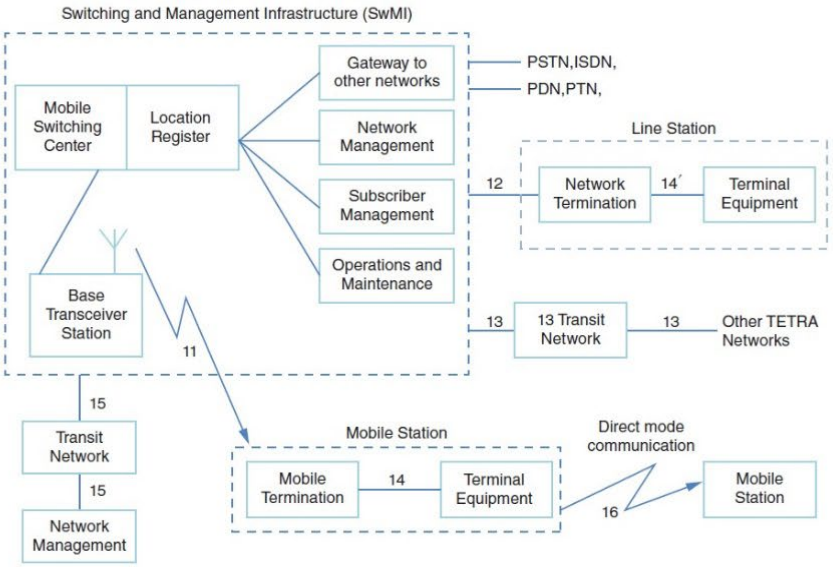

Figure 2.2: TETRA interfaces [2]

2.6. TETRA network components

Network components refer to functional structure of TETRA network. They are divided into different parameters as they are described below:

1. The Mobile Station: it is physical equipment for subscribers. Also, an identity module known as the subscriber identity module and the TETRA equipment identity, which is unique to each device. The TETRA equipment input system lets operators enter the equipment identity. It allows them to disable stolen equipment fast.
2. TETRA Line Station: line station works similar to a mobile station. The infrastructure connections can be managed and switched over an ISDN which provide the same functionality as mobile stations.
3. The Switching Management Infrastructure (SWMI): it consists base stations that manage core communications between line and mobile stations over ISDN. It handles call and channel; in addition, it has databases with subscriber information.
4. Network Management Unit: This interface gives the remote and local management functionalities

5. Gateways: it connects a TETRA network to a non-TETRA network like ISDN, PDN, and PSTN. Information should be converted or translated according to protocols for this connection. [2]

Now, we can discuss how the TETRA network operates. TETRA equipment has a unique identity during manufacturing which is similar to cellphones' IMEI. It helps distinguish communication parties in a TETRA network. It is similar to how GSM technology uses the international mobile equipment identity. The figure 2.3 illustrates this information.

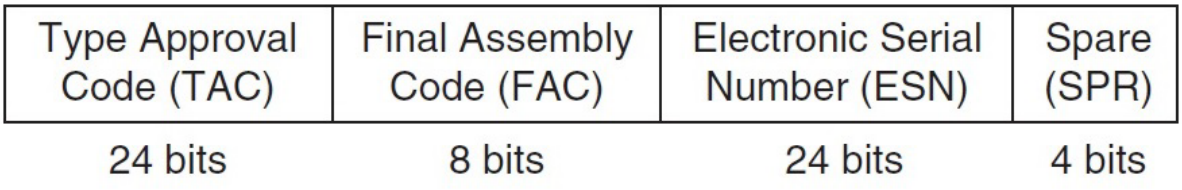

Figure 2.3: The TEI/TETRA equipment identity [2]

The mobile network identity in TETRA identifies different network forms. After it is identified, the base station broadcasts the mobile network identity, which can include operator information, the country code, or both. [2]

Also, TETRA subscriber identity makes connection subscribers to their billing information and subscribed services. The TETRA subscriber identity has the contents shown in Figure 2.4. TETRA also has a unique group-call service system with a group TETRA subscriber identity, in addition to individual subscriber identities. [2]

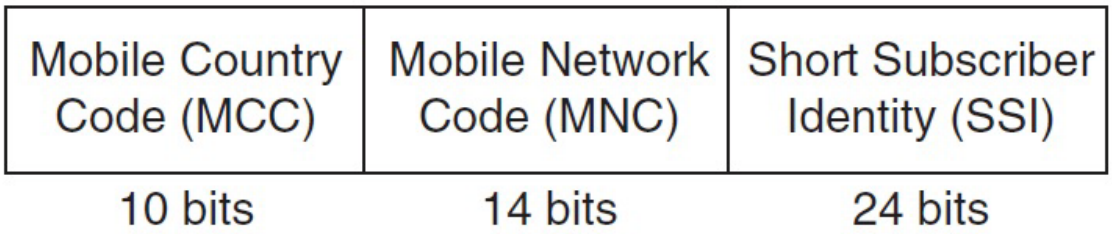

Figure 2.4: TETRA subscriber identity [2]

A schematic overview of TETRA network can be illustrated in figure 2.5.

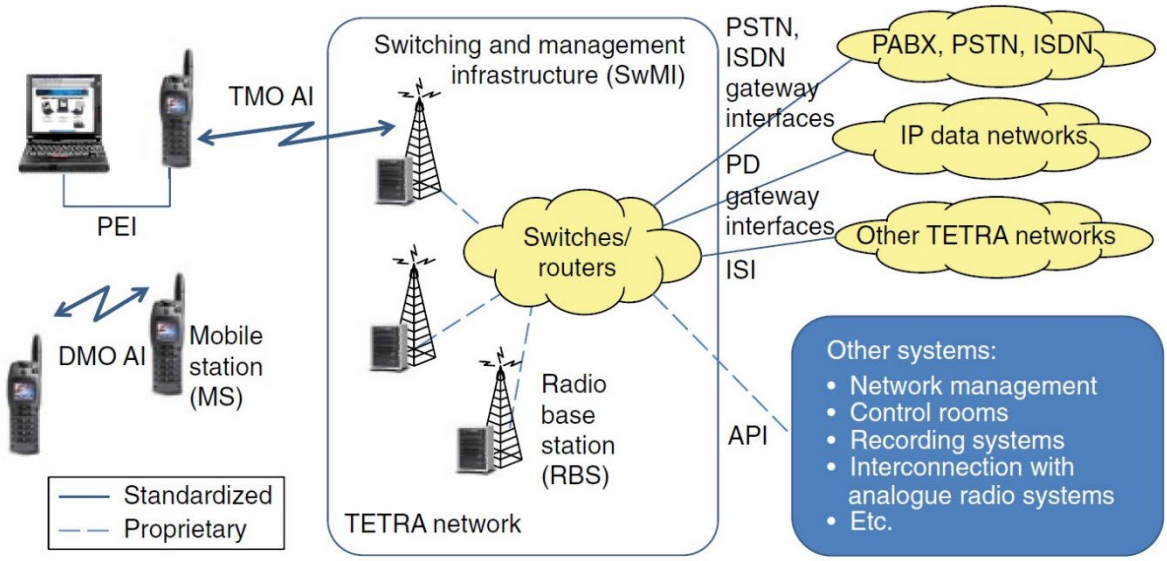

figure 2.5: Network architecture and standardized interfaces of a TETRA system.[1]

The core network is switching and management infra (SwMI), consist of radio base stations interconnected through a one or more hierarchy of switches and routers (RBS). The components are connected to core such as PSTN/ISDN, IP gateways. Some interfaces are standardized, but many within the SwMI are proprietary. On the radio side, we have TMO and DMO. A standardized Peripheral Equipment Interface (PEI) is also provided, allowing the TETRA terminal to be divided into two distinct components: the terminal equipment (TE) and the mobile termination (MT). The TE can be a PC or another computing device, while the MT functions as a modem. [1]

It is a suitable technology for mission-critical this standard has been developed over 120 countries. It has adopted by so many users such as emergency units as the largest user group.[1]

2.7. security of TETRA network

Security features of TETRA networks based on the Confidentiality, Integrity, reliability, Non-repudiation, Authentication.

- The first feature points out that only authorized personnel or people should have access to the information being passed along.
- The second one mentions Only authorized users are allowed to make changes to the information in the exchange.

- The third one is Authorized users should always have access to resources and services to complete their tasks.
- The fourth one refers to This requires that the sender cannot deny that he/she sent the message.
- And the last one the requirement that the sender's identity is verifiable by the recipient. [2]

Now, it is necessary to mention some of the main security features of TETRA standards.

- Authentication: The authentication service allows a TETRA terminal and network verify each other's real identity. By knowing a shared secret key. It is unique for each terminal and only available in the terminal and a secured server of the home TETRA network [1].
- Air interface encryption (AIE): it encrypts the voice and signaling between a TETRA terminal and its TETRA network. It supports a number of over the air TETRA encryption. The encryption can be static and dynamic.
- Enable and disable: This service provides a mechanism by which a terminal can be denied or allowed access to a TETRA system.
- Supports for E2EE: the parties can communicate by ciphering the whole communication data at terminal level. So, variety of algorithms can be used [1].

Protection against eavesdropping and manipulation of voice and data, as well as the exclusion of third-party use are essential requirements for critical communication systems, especially with the increase in cybercrime. TETRA security features are developed by experts and are designed to work together to meet public safety requirements. They guarantee the security when the devices are used even in case of different manufacturers because they are inseparable part of the standard. This standard has a strong mutual authentication between devices and the network. These factors make the TETRA network trustworthy. Moreover, the authentications are up to user level. [26]

If a device is lost or stolen, it is crucial to prevent it from accessing the network. TERRA offers security options to prevent using the device; in the other word, it disables the device either temporarily or permanently. TETRA also protects against eavesdropping by encrypting user and signaling information over the air interface between devices and infrastructure. It is for both individual and group communications, voice, data, and direct mode operations. Various encryption algorithms, both standard and proprietary, are supported. [26]

TETRA allows for customizable end-to-end encryption. This means that a user organization may easily customize an end-to-end encryption system to suit their needs. In TETRA technology this flexibility is essential and can be implemented for different user groups. [26]

TETRA allows user organizations to control and manage security mechanisms. It ensures they work together as a consistent system. Since key management is the most important factor in security, a large number of features are used in order to support it. These features are updated regularly to have a secure communication until 2035 and beyond.[26]

Since TETRA networks utilize all-IP design, it allows for an advance protection like firewalls. TETRA network can be used in standalone (disconnected from internet) or integrated with other devices for an organization which enables some mechanisms against cyberattacks and threats. The used devices are equipped by closed and secure operating systems which is the most important factor in security in this network. [26]

2.7.1. security protocols

TETRA encryption algorithm also known as TEA is utilized for air interface encryption to protect voice and data transmissions. Also, in TETRA, we have TETRA Authentication Algorithm (TAA) which mentions authentication and key management processes. TEA has 7 categories while TAA has 2. In TETRA, end-to-end encryption utilizes well-known algorithms like AES128 or AES256.

- TEA 1 was designed for commercial applications and for worldwide use. The key strength is 32bit which is weak for an encryption algorithm. As a result, the main drawback of this algorithm is that this method of encryption is easy to decrypt which is an easy purpose for attacking. It was designed in mid 1990s to be easily exportable.
- TEA2 was only restricted to public safety organizations in Europe. It is an alternative algorithm for TEA 1 which any significant report about vulnerability of this algorithm has been published. This algorithm uses 80-bit keys without any reduction in the key length, but deployment of these algorithms is more restricted than TEA1.
- TEA3 is the third algorithm for TETRA security. It is used for the public safety organizations outside of Europe. It is widely used for TETRA systems and stronger than TEA 2.
- The fourth algorithm is TEA 4. Like TEA 1, it is used for commercial purposes with certain export restrictions. Like first algorithm, it is a basic one for security. in the other word, it is used for commercial purposes that do not carry sensitive data. it is less secure than TEA2 and 3 but more robust than TEA1.
- TEA 5,6,7 are the last published algorithms of the TEA family. They were introduced in 2022. they are known as TEA set B algorithms. the process of key generation of these algorithms is close to each other. they were introduced to omit the weakness of previous algorithms. the algorithm of this encryption method is as follow.

  1. Initialization Vector Mixing: first the 80-bit IV (initialization vector) is processed based on a 10-stage linear recursion to generate a 192-bit mixed IV (IVX)
  2. key and IV combination: the cipher key (CK) and IVX are combined to create two items. first one is a 192-bit Mode Key (CKM) and the second one is 192-bit Mode IV (IVM).
  3. Block Formation: consecutive 256-bit blocks are generated according to the IV and a fixed ASCII identifier such as "TEA 7" or 6 or 5 is assigned as the algorithm name and and a 32-bit counter (incremented with each block)
  4. Encryption process: These blocks are encrypted using a 256-bit variant of Rijndael with a 192-bit key (CKM).
  5. Keystream generation: The encrypted blocks are concatenated together according to the keystream sequence (KSS), and if the final block is longer than 256 bits, the extra blocks are discarded.

  Their difference is in their usages. TEA 5 is used for European emergency networks which is successor to TEA2. It is designed for police, military, intelligence agencies, and emergency personnel within Europe. TEA6 is for friendly non-European emergency and military networks, replacing TEA3. It is meant for use by similar organizations outside Europe. finally, TEA7 Available for critical infrastructure and other civil applications, succeeding TEA1.[46]

one important point about TEA7 is that with an effective key size of 56 bits (reduction key), it serves as the counterpart to TEA- {1,4}. The key size reduction is achieved by defining an S-box in a way for a given Initialization Vector (IV), the collision entropy of the key limits the security against brute force attacks to 56 bits.[54]

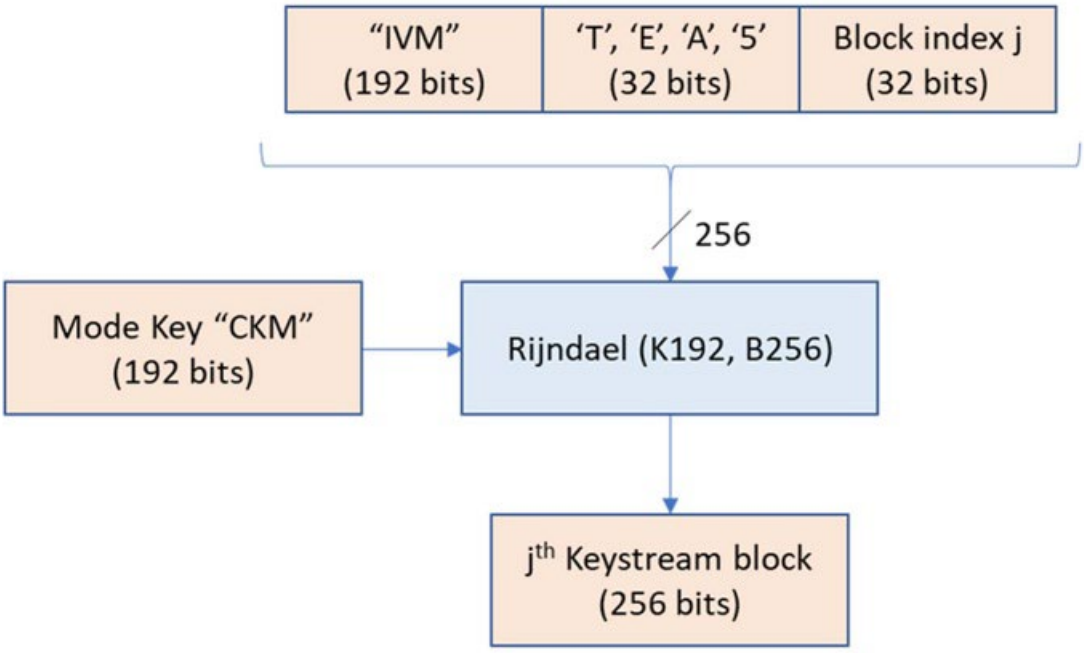

figure 2.6: TEA 5,6,7 key generation [46]

The other protocol in TETRA is TAA. This protocol is for authentication, key derivation, and Over the Air Re-keying (OTAR). It has 2 versions. TAA 1 is primarily used for commercial purposes and has restricted export and the second version is designed for European emergency services. the length of key in both algorithms is 128 bits; however, the first version is utilized in the environments that the sufficient security is exploited. The second version of this algorithm is used in critical infrastructure for emergency services, requiring higher security standards. TAA 2 is to vanish the vulnerabilities that has been found in TAA 1. It is as strong as TEA 5 and 6. [9]

2.7.2. Authentication in TETRA

The purpose of this part refers to fundamental security service that secures the connections of TETRA. In this procedure, both parties verify their identity. If one of the parties is a public interface, a signed certificate should be issued by an authority. When symmetric keys are used in the network, it is assumed

that high level of security is in the network. In TETRA, one knows the secret shared between two parties. for instance, the authentication center and the mobile station. [2]

The authentication key uses two kinds of algorithms. First one is symmetric and the second one is asymmetric key. [2]

The process of symmetric key is based on the below.

- The sender and the recipient share a similar or the same secret key
- If a symmetric key leak from one of the interfaces, it makes the whole system insecure
- Preventive actions are useful in order to update of the secret code/key
- Symmetric key algorithms have steam and block cipher schemes
- Block cipher schemes divide the plain text into fixed blocks and it encrypts the block systematically.
- A stream cipher, on the other hand, operates on the principle of one plain text and one digit at a time
- A secret key starts a pseudo-random keystream sequence, which combines with the plain text.

The process of asymmetric key is based on the below.

- In public key/ asymmetric key, the decryption and the encryption processes utilize different keys.
- In asymmetric key cryptography, a mathematical function is used instead of a substitution or permutation function
- This process is very difficult to do with a computer, especially when trying to extract one key from another key and the cryptographic algorithm
- Every user here possesses a pair of keys, which are in the form of public and private keys.
- When two parties want to communicate, the sender needs to know the receiver's public key to encrypt the message with it.
- When the recipient gets the message, they can use the private key for decrypting the message [2]

In table 2.6 we can observe the functionality of symmetric and asymmetric key.

Feature	symmetric	asymmetric
Number of Keys Used	1 key (same key for encryption and decryption)	2 keys (public key and private key)
Key type	Shared secret key	Public key (shared) and private key (kept secret)
Encryption Process	Sender encrypts data with secret key	Sender encrypts data with recipient's public key
Security	lower	higher

Table 2.6: the difference between symmetric and asymmetric algorithm

2.7.3. The Process of Authentication Key Generation

In TETRA, symmetric keys are used to make authentication. The mobile station retrieves a user authentication key when it registers to the network for the first time. The user authentication key is stored

in the SIM card of the terminal equipment and in the authentication center's database. The key denoted as K which is required for authentication. There are three ways to generate this key. [2]

- The first one is From the AC or the authentication code, which is the pin code that the user enters.
- the second one is Generated through the TB1 algorithm from the user authentication code stored in the GSM, which has the algorithm TB2.
- the third method for generating the authentication key (K) uses both the user account code (UAC) and the authentication center (AC). [2]

the lengths of the KS', K, and KS are all 128 bits. The authentication key (K) cannot be used directly in the authentication process. However, it can be used to generate session keys, which are denoted as KS' and KS. [2]

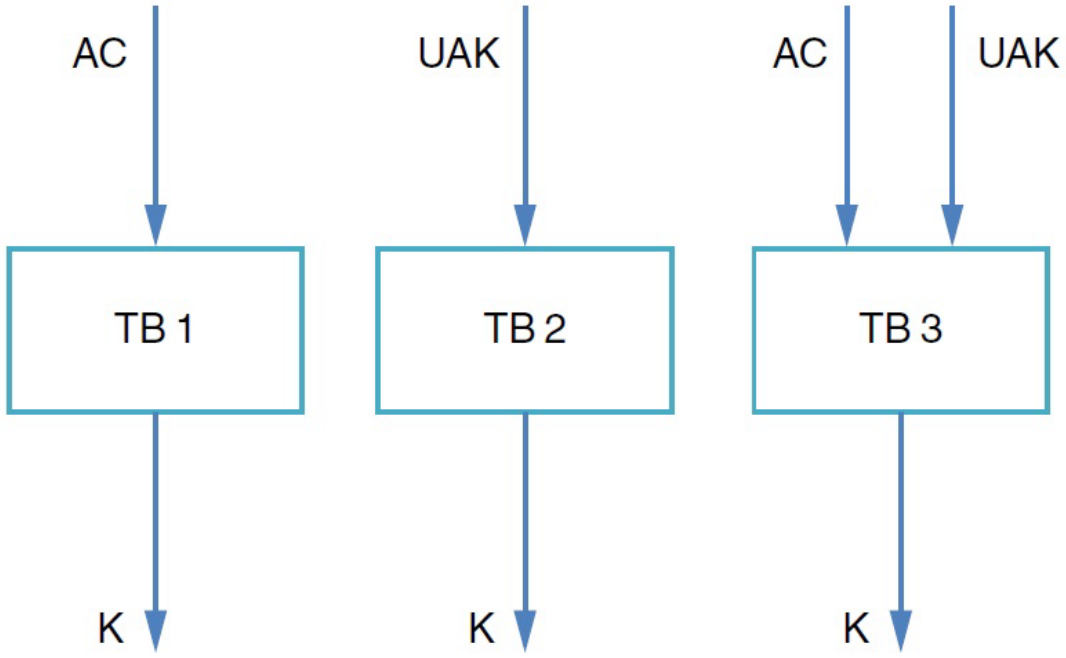

Figure 2.7: Authentication keys generation.[2]

2.7.4. Authentication Procedures

In TETRA, authentication works in three ways: the mobile station (MS) verifies the network (SwMI), the network verifies the mobile station, or they verify each other. The network's infrastructure, like

an authentication center and base station performs the verification. A random code (RS) and a key (K) are used to create a session key (KS) using an algorithm called TA11. This process is done by the home system's authentication center. [47]

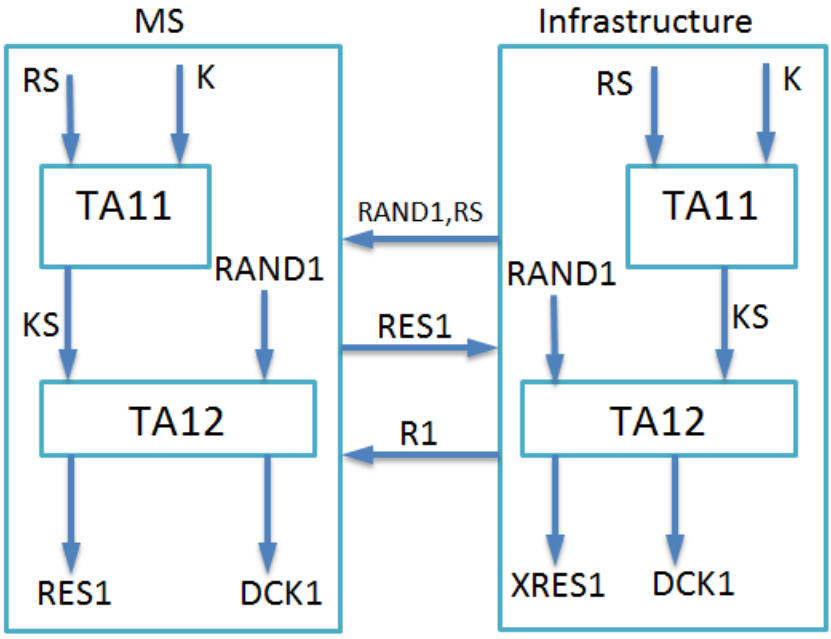

figure 2.8: Authentication of a user [47]

According to the figure 2.8, The infrastructure creates a random number (RAND1) and sends it to the mobile station (MS) as a challenge. The MS calculates a response (RES1) using the session key (KS) and an algorithm called TA12. During this process, a key called DCK1 (part of the derived cipher key) is also created. The infrastructure then checks if RES1 matches the expected response (XRES1). If they match, the authentication result (R1) is marked as TRUE; otherwise, it's marked as FALSE. [47]

The process of infrastructure verification by the mobile station (MS) is similar to how the MS infrastructure is verified. However, the algorithms TA11 and TA12 are replaced by TA21 and TA22, and a different session key (KS') is used. This process also generates another part of the derived cipher key, called DCK2. [47]

The TETRA system also supports mutual authentication. It begins as one-way authentication, and the challenged side decides whether to make it mutual. The second authentication will only happen if the first authentication succeeds. [47]

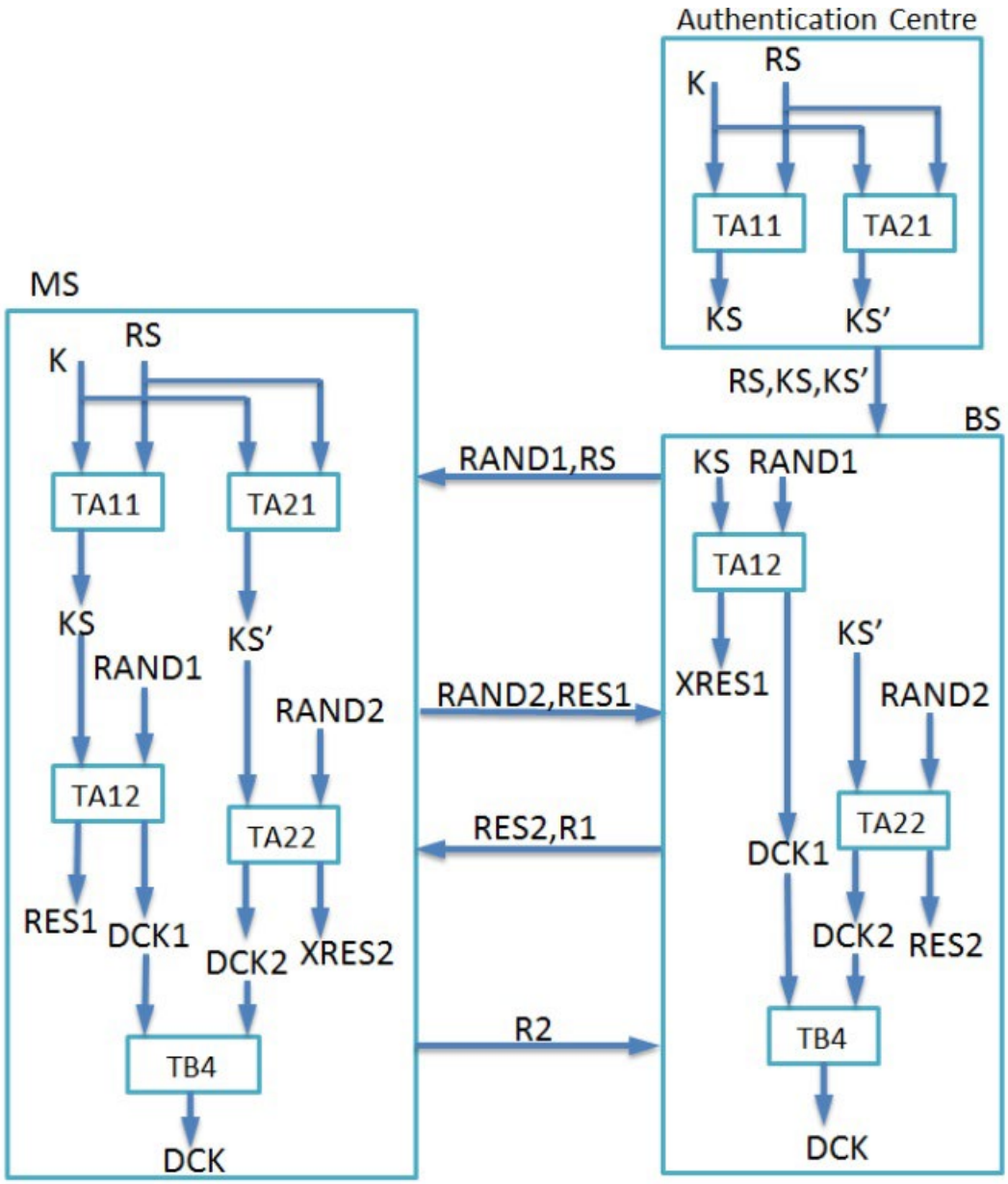

figure 2.9: mutual authentication initiated by the infrastructure [47]

the method of authentication is as following sentences.

- The authentication center checks if the user's key (K) matches their identity (ITSI). in this way, it uses the key (K) and a random value (RS); then, session keys (KS and KS') are created.
- These session keys and the random value (RS) are sent to the base station. therefore, the base station generates another random number (RAND1) and sends it along with RS to the user's device (MS). [47]

- The user's device (MS) creates session keys and calculates a response (RES1), which is sent back to the base station. For mutual authentication, the user can also send a random number (RAND2) to the base station. [47]
- The base station compares the user's response (RES1) with an expected response (XRES1). If they match, the base station calculates a response (RES2) and confirms success (R1 = TRUE).
- The user's device (MS) compares the base station's response (RES2) with its expected response (XRES2). If they match, it confirms success (R2 = TRUE). At this point, mutual authentication is complete. [47]
- During this process, keys (DCK1 and DCK2) are used in an algorithm (TB4) to create a final cipher key (DCK). [47]

2.7.5. Key Management

The keys in TETRA includes:

- Derived Cipher Key (DCK): s a cryptographic key used for securing communication between TETRA radios and network infrastructure. it is used for encrypting and decrypting voice and data communications. also, it ensures that each communication session has a unique encryption key. furthermore, it Prevents unauthorized interception and ensures confidentiality. [47]
- Common Cipher Key (CCK): For each Location Area (LA), the infrastructure creates and distributes a common cipher key to all mobile stations (MS). It is typically used for group communications, such as team-wide encrypted calls or broadcasts. Unlike the Derived Cipher Key (DCK), which is generated for session-based encryption, the CCK is pre-distributed and shared among authorized users. [47]
- Group Cipher Key (GCK): The group cipher key (GCK) is created and shared with mobile stations in a group by the infrastructure. However, GCK is not used directly for communication; it is adjusted using either the Common Cipher Key (CCK) or Sealed Common Key (SCK) to produce a Modified Group Cipher Key (MGCK). The MGCK is then used to encrypt group calls, ensuring their security. [47]
- Static Cipher Key (SCK): The static cipher key is known to both infrastructure and the MS, the value of SCK shall never change. A terminal could store up to 32 SCKs. The SCK could be used in systems that do not implement authentication. It could also be used for encryption in the Direct Mode operations. [47]

In table 2.7, we compare the characteristics of the keys in TETRA.

Feature	DCK	SCK	GCK	CCK
purpose	Encrypts individual calls or data sessions	Root key for deriving encryption keys	Encrypts group communications within a specific team	Encrypts common group calls/messages
usage	Generated dynamically for each session	in systems that do not implement authentication	Used within a predefined group	Shared among a broader network for group calls
Key type	Session-based key	Long-term root key	Group-specific key	Network-wide key
Update frequency	Generated for each session	Rarely updated (unless key management requires)	Periodically updated for security	Periodically updated for security
Encryption scope	Individual user communication	in the Direct Mode operations	Group-based encryption (specific teams	Group-based encryption (larger network)

table 2.7: comparison between security keys

Chapter 3: how the TETRA satisfies the network requirements for the public safety

3.1. introduction

As it was mentioned in the first chapter, public safety networks have some requirements that without them the PPDR operation is not possible. Since TETRA is a mission-critical technology which is widely used in public safety, it needs to satisfy these requirements.

In this chapter, first TETRA network is explained and then by explaining each component and it is discussed how they satisfy public safety requirements.

3.2. Network description

In figure 3.1 we can observe a whole overview of a TETRA network. In this figure, we have dispatchers which plays a crucial role in TETRA networks by managing and coordinating communications for public safety and other critical operations. Their responsibilities are as below:

- call handling: refers to management of voice and data calls. They ensure the info are routed to correct responders
- Incident Coordination: they facilitate communications during emergencies by providing real-time updates and instructions.
- Supplementary services: they refer to preemptive priority calls, call authorization, group patching, monitoring, listen to the calls of two users, call termination
- Support and Assistance: they guide the responders by short data services (SDS) [10]
- the network manager or management system is the second part to mention. It requires to be flexible with a distributed modular architecture to be adopted to customer needs. This section is useful in order to rapid service deployment, rapid service activation. Mange the distributed data. It also should be helpful to reduce the costs and monitor the services in timely manner. This can be done through the elimination of repetitive processes and equipment, improve the service response time, tune the performance of the system. If the intelligence is used in the system, these goals are achievable with high level of resource management [11].

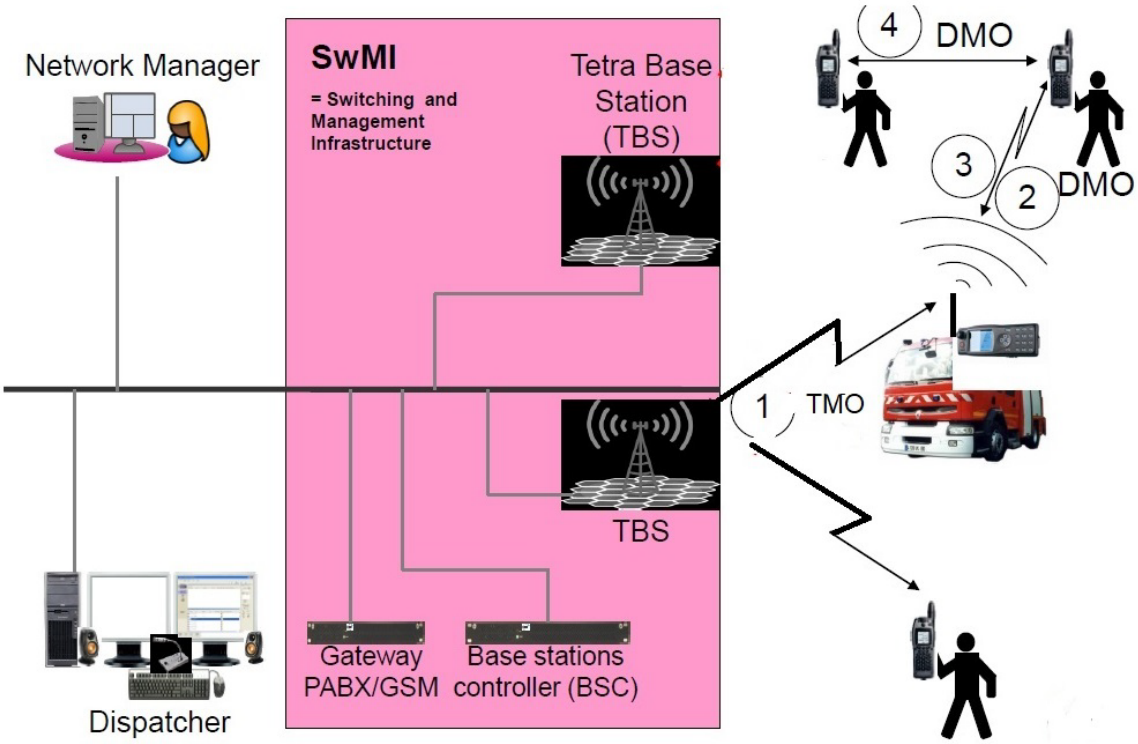

Figure 3.1: network overview [11]

TETRA usually works in group calling mode which means by pressing one button a connection is created from user to a group or dispatcher. TETRA terminals can act as mobile phones allowing direct calls to other TETRA users or the public phone network (PSTN). Emergency buttons on the terminals let users send emergency signals to the dispatcher, even if other activities are happening.[11]

3.2.1. TMO

Trunked Mode Operation (TMO) is one of the most important and fundamental components of the TETRA. It is used to transfer radio signals in a two-way communication. The communication in this component is done through a network infra which is a base station and switching and management infrastructure (SwMI). It is also used for point-to-point and point-to-multipoint communications that brings more secure voice and data transmission. It is the primary mode in TETRA where group calls, individual calls, and data services are handled. This infra is used in large areas particularly for public safety operations, transportation services, and utilities management. The network structure of this component secures reliable connectivity, centralized control, and efficient use of available frequencies. [6]

For achieve this goal, MSs communicate with each other through TETRA V+D air interface which is controlled by Switching and Management Infrastructure (SwMI) that typically are base stations and switches. [13]

Key features of TETRA TMO can be described as below:

- Network-Based Communication: TMO relies on the network base station to manage and route communications. [6] Base stations are to create a reliable communication across a specific area; also, transmission and reception of signals are done through this component. The second component in the network-based communication is the SwMI. It is the backbone of the TETRA network and handle some tasks such as call control, routing, and managing group or individual communications. It also has control nodes, switches, and databases to ensure smooth network operations. The third part is the core network. It handles the interconnection between base stations and external communication systems such as public telephone networks or other TETRA networks. Management of authentication, encryption, and billing functions are the other tasks of this part to mention. Priority calls, group allocations, and user permissions are defined in the network-based communication which is used for mission-critical operation. Mobility support is another responsibility of this part. It points out that when users move in the covered area, switching between the base stations is done in this part as well. Frequency reuse and interoperability with other networks or external systems like PSTN via gateways is the responsibility of this part too. The connections in this part are secured through mutual authentication. [1][4]
- Voice and Data Services: TMO supports a range of services such as voice calls, status messages, short data service (SDS) and packet-switched or circuit-switched data communication. The voice services are divided into individual calls (one-to-one like traditional phone calls), group calls (one-to-many, a user can talk with a group of people), broadcast calls (one-way communication to a group of users), emergency calls (priority calls in critical situations), supplementary services to enhance voice communication (call forwarding, call hold, call waiting, and caller identification). For data, status messaging (conveys specific messages), short data services (similar to SMS to exchange short data), packet data services (transmission of packet-switched data, GPS location updates, and other IP-based communications), circuit data services (a continuous, dedicated data channel for applications which needs consistent data streams), Location Services.[21][8]
- Emergency communications: it is used for emergency situation to provide reliable and fast communications. It is for police, fire fighters and emergency medical services due to their robustness and ability to handle high-priority calls. Also, it provides priority calls which means a call that has a priority over other calls, group calls mentioning a call from one user to a group of users which is crucial during coordinated emergency responses. [4]

3.2.2. DMO

DMO allows two network components connect with each other without any infra like base station (Two groups of UE are connected to each other). It is an important component especially for public safety

services because this feature allows first responders in an operation connects to emergency personnel without any infrastructure if it may not be available or damaged. We have two types of DMO.

- Ad-hoc DMO: Devices are connected to each other without any infra. In this case, protocols like Wi-Fi Direct, Bluetooth, or Zigbee are utilized.
- Infrastructure DMO: The network helps the devices connect directly, using DMO gateways or other specific components.[23]

Ad-hoc DMO is used when network infrastructure is not available or reliable. In this way, first responders can communicate with each other when there is no network coverage. Like campers or hikers use ad hoc DMO to stay in touch without using cellular network.[23]

Infrastructure DMO is used when network infrastructure is available but unreliable or congested. First responders can use it when they are in large-scale emergency situation like natural disasters, terrorist attacks or when the network is overloaded. [23]

Since reliable communication is vital for people's safety and well-being, DMO provides network even it is unreliable.[23] For example, it is operational outside the coverage of TMO or TMO is overloaded. In this way, TMO has higher latency but DMO has minimal latency. It should be mentioned that DMO is a unique system with specific feature for TETRA which makes it different from other public and private cellular networks [2]

Another benefit of DMO is that without network configuration, it provides a network. Devices can quickly and easily connect to each other without any infra which is particularly useful in emergencies where fast communication is crucial and can save lives.[23]

In DMO subscriber radio units communicate using radio frequencies which are outside the control of the TETRA TMO network. It is possible to use either TMO or RMO through base stations.[14]

3.2.2.1. DMO application

As it was mentioned before, the main application of Direct Mode Operation (DMO) in TETRA is to extend the range of the Trunked Mode Operation (TMO) network. This allows handheld communication devices to work in areas of the TETRA network that only have mobile radio coverage. To achieve this goal, a vehicle which TETRA radio terminal with a gateway on it is utilized to link the mobile devices or radio terminals that operates in DMO with the TMO network. [14]

The key roles of DMO can be described and summarized as below:

- Local Area Communication: it is for local communication outside of TMO range such as such during localized work activities or major incidents
- Network Coverage Extension: it can extend network coverage provided by TMO. In this way, hand portable terminals can communicate with each other in areas with poor coverage.

- Capacity Relief: it provides additional communication capacity when the TMO network is busy or overloaded
- Emergency Use: it is for emergency use when infra is not available. [14]

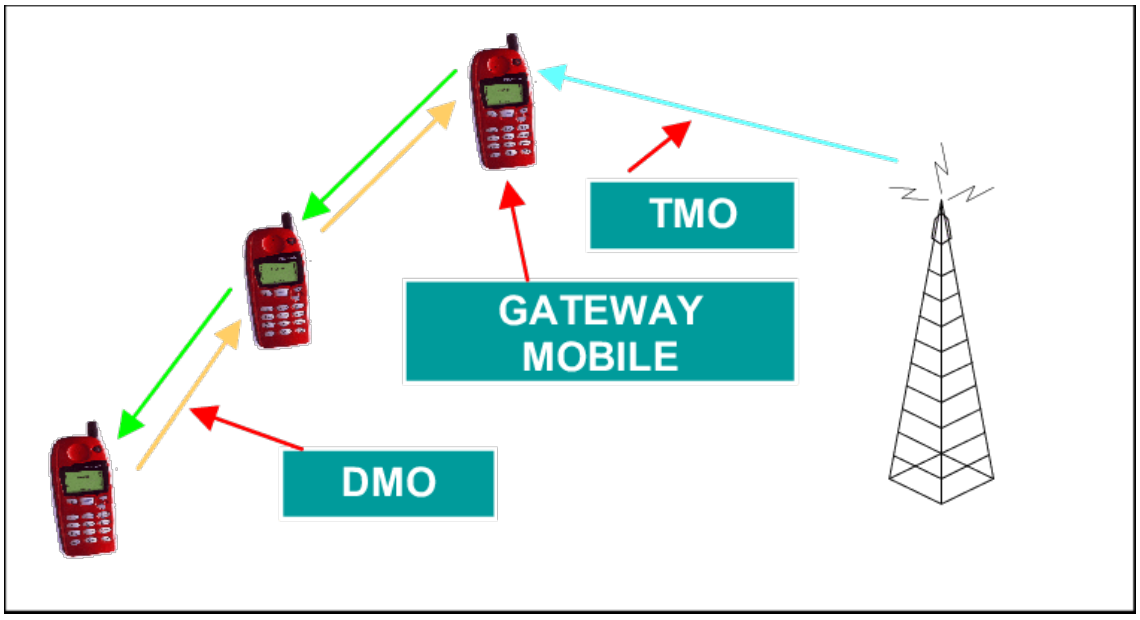

Figure 3.2: DMO concept [14]

DMO has four interface models.

- DMO terminal to DMO terminal: This model enables direct communication (point-to-point or point-to-multipoint) between DM-MSs using the direct mode air interface. DM-MS provide the sync reference which is called master device. when a DM-MS creates a call is master and any device is synched with the master is called slave. [24]
- DMO repeater: This model applies to operation using a Direct Mode – Repeater Enabled Operation (DM-REO) between the end MSs. The DM-REP (Direct Mode Repeater) receives information from a transmitting mobile device on an "uplink timeslot" and then it is retransmitted by a downlink timeslot. The DM-REP decodes and re-encodes the signals it receives to enhance overall link performance.[24]
- TETRA V+D to DMO Dual Watch: it can be one of these states:
    1. The device stays inactive in both modes, while regularly checking both the V+D mode control channel and a chosen DM radio frequency.
    2. When a device is communicating with another device (DM-MS) using the Ud air interface, it also periodically monitors the V+D mode control channel through the Um air interface. It should be pointed out that Ud is the interface for Direct Mode, while Um is the interface for Trunked Mode communications.

3. When a device communicates with the TETRA Switching and Management Infrastructure (SwMI) in V+D mode using the Um air interface, it also periodically monitors a selected DM radio frequency carrier. Dual Watch allows radio terminals to periodically listen for calls on both DMO and TMO depending on the selected mode. This feature is available on both hand portable and mobile radio terminals, requiring TMO network RF coverage for hand portable radios to function effectively [24]

- DMO gateways: This operation model involves using a DM-GATE in a TETRA V+D network. The DM-GATE handles the differences in protocol between the Ud and Um air interfaces and ensures the required interconnectivity is done between Direct Mode (DM) and the TETRA V+D network. (it translates the different protocols). DMO Gateways can link Direct Mode Operation (DMO) communication nets to the Trunked Mode Operation (TMO) network, not only to extend TMO network coverage but also to connect local DMO nets to the TMO network independently of RF coverage. [24]

Even though Direct Mode Operation (DMO) RF coverage is generally sufficient, it sometimes needs enhancement in areas with significant building clutter causing signal loss. In such cases, a Repeater facility in a vehicle-mounted TETRA mobile radio terminal or a transportable radio unit can provide the necessary coverage. This Repeater facility is available only on mobile radio terminals and can include a Gateway to link DMO and Trunked Mode Operation (TMO) communications when needed. [14]

The goal of this model is to help define the interfaces that exist between various device types and if relevant to any other involved terminal or network entities. The reference models are used to cover all possibilities and provide a framework in order to describe requirements according to technical point of view for various devices [4].

Now, for a conclusion, based on table 3.1 we can compare the characteristics of DMO and TMO according to the discussions were made before.

Feature	DMO	TMO
Communication type	Direct, device-to-device	Via network infrastructure (base stations)
range	Limited to radio-to-radio distance	Wide-area coverage via base stations
Dependence on infra	No infrastructure required	Requires TETRA network infrastructure
Call type	Simplex calls (one at a time)	Full-duplex and group calls supported
Coverage extension	Can use a DMO Gateway to connect to TMO	Extended via TETRA base stations
reliability	Reliable in case of network failure	High reliability within network coverage
Encryption and security	Limited security options	Strong encryption and authentication

Use case	Emergency operations, off-network communication, disaster scenarios	Routine public safety, transportation, utility, and industrial communication
capacity	Limited (depends on available radios)	High capacity, supporting multiple users and groups
Feature supported	Basic voice and messaging	Advanced features like dynamic group calls, location tracking, and data transfer

Table 3.1: the comparison between TMO and DMO capabilities

3.2.3. Teleservice and bearer service

A teleservice is used for enabling communication according to voice and data between users that uses TETRA protocols (end-to-end communication). It is based on the Terminal Equipment (TE) functions and the network's bearer service. It is used to handled private calls, group calls and short data service (SDS). This is done through TMO or DMO. [13]

One of the features for public safety is individual call (private calls). An individual call is a one-to-one communication between two parties. It can only be set up if both parties have selected the same radio frequency. Each individual has a unique number (ITSI) used to address them. The operation mode is simplex, meaning communication happens in one direction at a time. Individual calls can be set up with or without a presence check. A presence check allows the caller to see if the other party's terminal is switched to the radio frequency and responds to a message before the call is set up. The voice teleservices in TETRA support the transmission of speech according to a TETRA specific voice codec. [13]

Another service handled by teleservice is group calling. TETRA usually works in group calling mode which means by pressing one button a connection is created from user to a group or dispatcher. A group call is a communication where one person can talk to several others at the same time. This can only happen if everyone involved has chosen the same radio frequency. A group call is completely a sequence of a related call transaction according to two or more DM-MSs. The number of participants in a group call is not fixed. Users with active mobile devices can communicate directly with the help of TETRA terminals or the public phone network (PSTN). There is an emergency buttons on the terminals to let users send emergency signals to the dispatchers even if other activities are happening. [13]

Group calling is extremely important for mission-critical services and public safety users who can use it in a disaster to communicate with each other in order to make a better coordination and to have an efficient team work. This feature operates in two modes: TMO and DMO. [31]

In TMO, group calling is done through SwMI. When a user initiates a group call by pressing the PTT button, this request is sent to the central part (SwMI); then, necessary resources are dedicated to this request. In

this way, a user can create a talk group and connect to others. Since it is centralized, it can be managed by the network easily and the quality of the service stays decent. [31]

The second method is based on DMO. Since in this scenario, the network coverage is not available and direct communication is preferred. In this method, the radios can communicate with each other without SwMI. As a result, group calls can be created in an appropriate way by pressing the PTT button, users can immediately communicate regardless of their proximity. [31]

The key features of this communication are defined as below.

- PTT operation: by pressing this button communication is established
- Talk group scanning: TETRA radio can monitor talk groups simultaneously through scanning feature. This feature ensures users receive relevant information across different groups. Scanning can be performed in passive or active procedure. In active method, the radio informs the network about talk groups that it is monitoring; as a result, the network can manage the communications more effectively. In passive mode, the radios do not inform the SwMI about monitoring the talk groups. In this method, the scanning was programmed before. This type of scanning reduces signal traffic and is particularly useful when resources in the network need to be conserved. [31]
- Priority management: the system supports various call properties; in this way, critical communications are transmitted over regular traffic. For instance, emergency group calls have the highest priority. [31]
- Late entry: Radios can join an ongoing group call, even if they were not active at the start of the call, ensuring that users can participate in communications as soon as they become available. This feature is especially useful for users who turn on their devices or are covered during an active group call. [31]

In a group, all members share a single, pre-defined number called their group number (GTSI). This is the number used to address them. The air interface can support multiple groups on a DM RF carrier. However, in normal operation mode, only one group can communicate to use the carrier at a time. In frequency-efficient mode, two groups can communicate using the carrier at the same time. In an operation, there is one DM channel per RF carrier while in frequency efficient mode there are two. Furthermore, there is an open or common group number including all of the users to make call to users who have the same DM RF carrier. [13]

Only one group number (GTSI) is sent over the air interface, and no acknowledgement is needed. The main goal is to set up calls quickly. The operation mode is simplex which means communication happens in one direction at a time. [13]

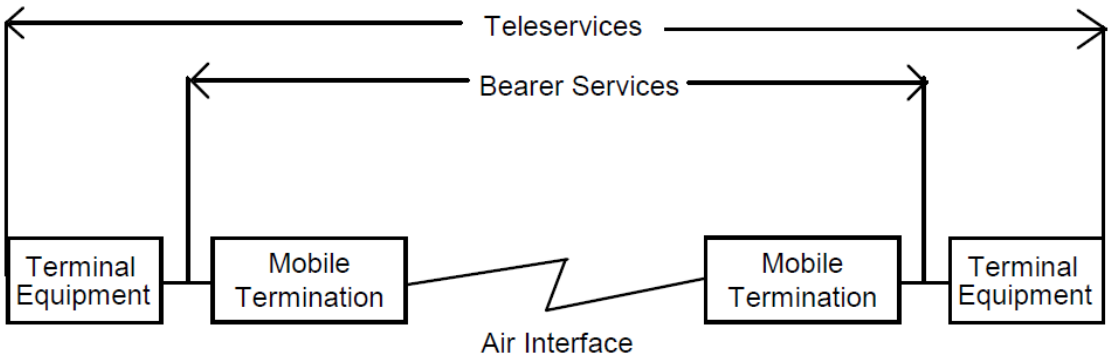

Figure 3.3: Concept of bearer services and teleservices [13]

Another point to be mentioned is bearer connection. A bearer connection allows point-to-point or point-to-multipoint data communication between mobile stations (MSs) on the same Direct Mode (DM) RF carrier. It is according to the lower layer (1-3) based on Open Systems Interconnection (OSI) protocol stack. [13]

This service ensures that the transmitted data are reliably and efficiently done between two parties of the network. It has various feature explained as below.

- rate adaptation: the data rates are adjusted based on the network and devices requirements
- speech and data swapping: the data and voice is transmitted during a call
- modern selection: the appropriate way for connection is chosen. especially when there is interworking with other networks like ISDN.

These services are necessary to maintain the reliability and the quality of a communication in TETRA which are hugely utilized in public safety, transportation and other critical serveries [44]

feature	teleservice	Bearer service
Purpose	End-to-end user communication (voice/data)	Provides transport layer for data services
Examples	Voice calls, telephony	SDS
User Interaction	Direct (human-to-human communication)	Indirect (device-to-device data exchange)

Table 3.2: Teleservices vs. Bearer Services in TETRA

3.3. High availability and interoperability

High availability is one of the most important aspects in mission-critical services. In this case, the services must be available almost all the time. The availability for TETRA is between 99.95% to 99.999%. To achieve this high level of availability, TETRA networks use backup components. These backups are always kept up-to-date and ready to use if the main components fail. [26]

Additionally, using battery backups and having multiple base stations in the same area helps to keep the network running smoothly. In this way, if one of the components fail, another component can handle the situation without interruption. [26]

Apart from backup components, TETRA always have a backup links to the base stations. This link redundancy is important to make sure TETRA radio users can stay in touch with the control room and with other users even if they are outside the base station's coverage area. [26]

finally, TETRA base stations support local fallback mode. When there is no link to the core infra, the TETRA users continue the communication within the base station. Specific TETRA features are developed to give base stations with network-wide coverage priority above isolated ones. TETRA networks are designed to meet these high availability needs, and network operators have full control to make the most of these solutions. [26]

In public safety and security, quick responses are essential because this service delays with peoples' lives. Instant reaction in a case of emergencies is crucial and even a small delay leads to death for civilians. The same goes for business and industrial communication, where immediate access to information helps prevent downtime and economic losses. TETRA has been designed for such situations. Call setup id instant and important calls are given a proactive status to ensure scheduling availability. [26]

Furthermore, the caller is given instant visual and audible feedback in case the called party is unreachable or busy. [26]

A TETRA system starts working as soon as it is powered on. If there is a failure, it has an automatic recovery system to switch to standby components or gradually reduce functions to maintain communication. In this way, it is one of the ways to keep the network available in any situation [26]

SDS messages are sent instantly and can be used in emergencies. This feature allows real-time tracking of mobile devices and quick creation of groups, enabling fast and accurate responses in the field. [26]

TETRA provide facilities for voice recording with the wide range of logging facilities for CDR, which makes fast and easy incident reconstruction and traceability. This allows for quick and easy reconstruction of incidents with immediate access to voice recordings which removes the need for extra clarifying calls in critical situations. [26]

Another point to be mentioned is interoperability. One of the key strengths of TETRA is its high level of compatibility among products from different manufacturers. This is achieved due to TCCA's comprehensive Interoperability Certification process (IOP) that enables a multi-vendor market for TETRA in case of equipment and systems. This open market benefits users with a wide range of compatible equipment, competitive prices, and rapid development of new products. It also provides a large market, faster adoption, and better opportunities for investment in new developments. TCCA's IOP Certification process

is based on live test sessions which are performed on commercial products based on interoperability and test cases. These are generated by TCCA's Technical Forum as an agreed interpretation of the ETSI TETRA standards and are representative of actual operational conditions and users' needs. [27]

All signaling exchanged between the tested devices are traced and checked against the profile specifications and test cases by an independent Certification Authority (currently ISCOM). After this process, IOP Certificates are issued. This thorough testing, which includes detailed protocol testing rather than just basic functional testing, is validated and certified by an independent body, showcasing the unmatched specificity and reliability of the TETRA standard. [27]

Another mode for interoperability in TETRA is ISI (Inter-System Interoperability). The concept of this function is illustrated in figure 3.4.[27]

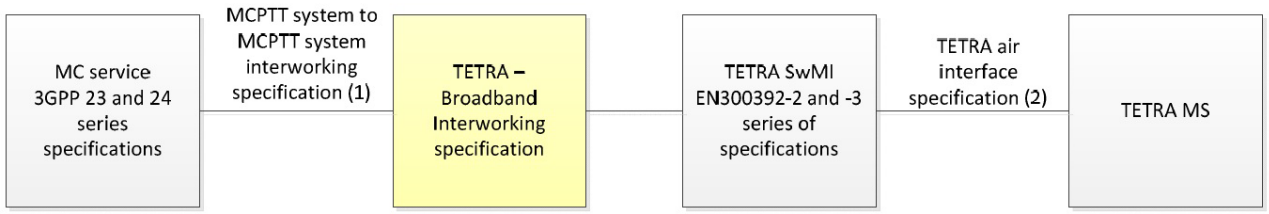

Figure 3.4: Concept of the interworking function [27]

The study will use the TETRA Inter-System Interface and the mission critical push-to-talk (MCPTT) interworking interface from 3rd Generation Partnership Project (3GPP) Release 15 as models. The TETRA SwMI interface may use the TETRA ISI or separate from standardization. This allows different systems to communicate if they are on the same network, which is useful for cross-border operations and large events, enabling different agencies to communicate easily.[28]

The TETRA standard uses the Individual TETRA Subscriber Identity (ITSI) to identify subscribers apart from vendors. ITSI includes a 24-bit Mobile Network Identifier (MNI), which consists of the Mobile Country Code (MCC) and Mobile Network Code (MNC), and an Individual Short Subscriber Identity (ISSI). TETRA can carry an external subscriber number field for addresses outside the TETRA system, with a limit of 24 digits (0-9, '*', '#' or '+'). A new external number field could be added, but carrying up to 255 characters could be problematic, especially for talking party identity, as it may delay calls. Group identities in TETRA use the Group TETRA Subscriber Identity (GTSI), which includes the MNI and Group Short Subscriber Identity (GSSI). [28]

3.4. Priority handling

This feature is to manage the network resources especially during the high traffic scenarios. It ensures that critical communications receive enough resource, precedence and maintain the reliability which is extremely important for a public safety. [32]

During a busy period, TETRA makes access to network for users according to their priority. 16 levels of priority are defined in this network. It allows different Grade of Service (GoS) and tariffs. For instance, front line officers acquire the highest priority level in a mission-critical operation while normal users get the lowest. [32]

TETRA uses a First in First Out (FIFO) queue in the trucking controller to handle calls by priority level during busy periods. Users only send a request for a call and when the resources are available the call is established. It reduces stress and frustration during busy times. [32]

Another part to be mentioned is priority levels. It points out the levels that determines the order in which calls are processed, particularly when the network experiences congestion. Higher levels are allocated higher resources to make a call. The Supplementary Service Priority Call (SS-PC) specifies the definition, activation, deactivation, and interrogation for the usage of low and high call priorities in the TETRA system. [33]

call queuing and preemption is another aspect to point out. TETRA systems implement a queuing mechanism managed by the trucking controller. Calls are handled and store based on the FIFO algorithm and order by the priority level. In this way, users just make a call and once a traffic is available call is connected but it is based on the algorithm and priority which was mentioned before. Thereby, it reduces user stress and frustration during busy periods. [33]

In an extreme case, If the network becomes fully occupied, the system may block lower priority calls to free up resources for higher priority communications. This mechanism is vital for an emergency situation because it is essential to make a call. This priority always ensures that a call with higher priority is always done even there is a stress over the network. For emergency calls, they always acquire resources from the network because they always have the highest priorities. [32]

This assignment and management always are done by the network administrators based on organizational policies and operational requirements. This configuration allows flexibility in adapting priority management mechanisms to the specific needs of different user groups in the TETRA network. [32]

3.5. Integration with mobile networks

Another capability of TETRA is hybrid solutions. In this method, TETRA network can communicate with high data throughput of broadband networks for voice mission-critical services. Also, transferring video streaming, high-data transfer, enhance situation awareness that are essential for today's mission-critical services. [35]

Since mobile broadband devices have advanced in recent years, the public safety agencies can utilize them more than before. As the quality of cellular networks improves, mission-critical users also need to use smartphones for their essential voice and data applications. In this way, LMR/PMR industries can make it possible to use old narrowband networks and new broadband networks together. [35]

The 3GPP has defined Mission Critical Push-To-Talk (MCPTT) services and protocols for smartphones. They are working on creating a standard for an interworking function (IWF) between MCPTT services and non-MCPTT (LMR/PMR) services. [35]

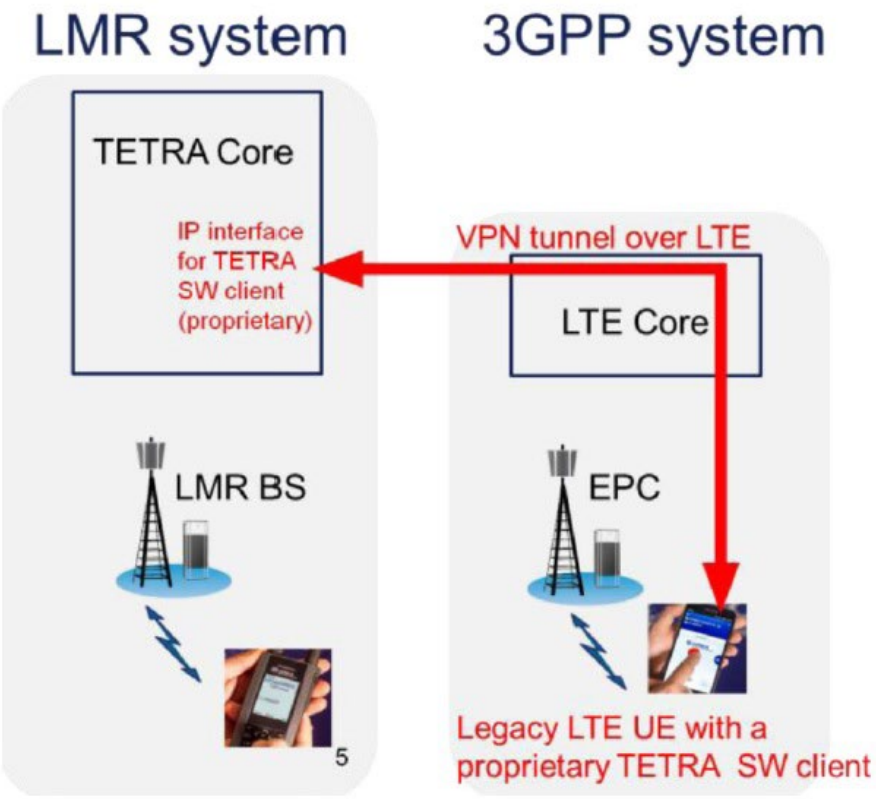

Figure 3.5: the concept of TETRA services over LTE [35]

While the standardization of interworking is still ongoing, and PMR/LMR users are transforming their services to new Push-To-Talk (PTT) services, the industry has developed interim solutions. These solutions use existing TETRA and 3GPP standards, LTE networks, and off-the-shelf smartphones to meet user needs. [35]

The idea behind this is to provide the TETRA service from TETRA core network to both legacy TETRA terminal and LTE smartphones via LTE or Wi-Fi networks. The service can work with any LTE or Wi-Fi network no matter what it is a commercial or dedicated one. An off-the-shelf LTE smartphone can be used with its own SIM card and the service uses an additional TETRA identity via the TETRA app on the smartphone. The quality of service and reliability depends on the broadband network used. [35]

TETRA file transfer is 7.2 kbit/s per time slot. But in case of integration with 5G/LTE, it can transfer high resolution video streaming, voice data and images like 50Mb/s. [6]

During the migration of services, using TETRA and LTE together allows connections between users on both networks. For some users, this may be a long-term solution until the LTE system's reliability, mission-critical functions, and security are guaranteed. [35]

Where LTE coverage is still being deployed or not viable due to economic or geographic reasons, existing TETRA coverage, along with Direct Mode Operation (DMO), gateways, and repeaters, can be used.

Some users on sensitive missions may prefer the extra security of TETRA and isolation from public access systems but still need to connect with others on LTE occasionally.

The MCDATA standard will include interworking of Short Data Service (SDS), allowing operational procedures and productivity gains from using SDS to continue. [35]

3.5.1. Interworking Requirements

To utilize TETRA over LTE network some services are necessary as below.

- Group calls, including emergency and broadcast calls
- Short Data Service (SDS)
- Individual calls (duplex and semi-duplex)
- Packet data service

Users also need some services such as:

- Late entry on either system
- The identity of the parties, which is transmitted between systems
- Restriction of calling and talking party identities carried between systems
- Group management on both systems
- Further supplementary services as required

Also, some additional services can be supported such as

- Prioritization schemes enabling the handling of priority requests between different systems.
- Pre-emption

Security services like authentication, air interface encryption, and end-to-end encryption (E2EE) must be maintained. For seamless service transport, solutions are needed for identity management, group control and communication protocols. While most regions have proposed solutions, the biggest challenge is end-to-end encryption and key management. Maintaining voice encryption and ciphering across interconnected systems is critical for secure communication between TETRA and MCPTT terminals and control rooms. [35]

3.5.2. Overview of standard architecture

The below figure illustrates a generic solution for interworking between LTE and non-LTE systems for MCPTT. LMR/PMR systems define the network equipment like base stations and terminals. In MCPTT systems, the MCPTT server supports MCPTT services centrally. To enable communication between these systems, an interworking function (IWF) is used for protocol translation, identity mapping, routing, and more. [35]

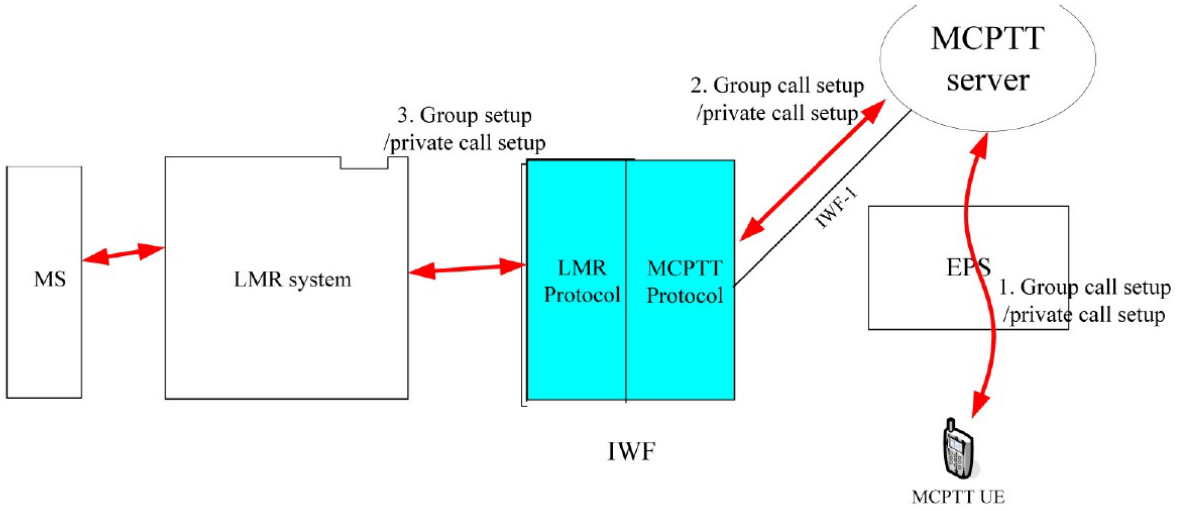

Figure 3.6: IWF architecture [35]

An interworking function (IWF) is added between the MCPTT system and the LMR/PMR system to enable communication between them.

The Interworking Function (IWF) has two parts:

1. An interface to the MCPTT system, using existing MCPTT reference points based on the 3GPP TS 23.379 specification.
2. An interface to the LMR/PMR system, using reference points defined by the LMR/PMR system.

3.5.3. Standardized Interworking of data services (MCData – TETRA)

LMR/PMR systems describe the equipment and parts that make up the network, like base stations and terminals. In MCPTT systems, the MCPTT server offers centralized support for services. an interworking

function (IWF) is used to translate protocols, map identities, route data and more for communication between these different systems. [35]

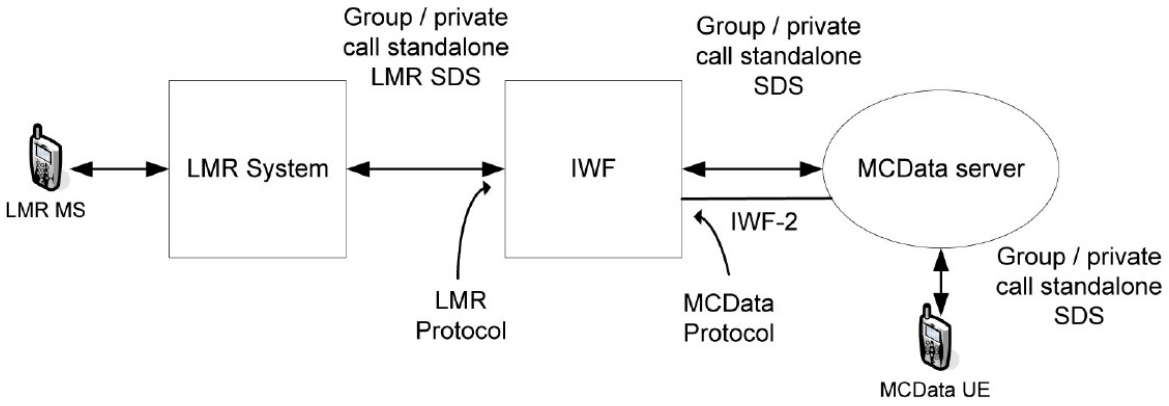

Figure 3.7: architecture of standalone SDS about MCdata and LMR systems [35]

IWF is based on two parts

- There is an interface to the MCPTT system that follows the current specification (3GPP TS 23.379). The IWF-1 can use some of the existing MCPTT connection points (like MCPTT-3 between two MCPTT servers).
- There is an interface to the LMR/PMR system that uses connection points defined by the LMR/PMR system

The IWF1 interface is mentioned, but not fully defined, in the 3GPP TS 23.379 specification. It serves as the connection point that allows MCPTT systems to work with older systems.

To exchange standalone SDS data between MCData and LMR/PMR systems, the MCData specification will identify the IWF functionalities that support interworking with the MCData system and the IWF-2. [35]

3.5.4. Early solution

The solution is based on the three components.

- A PTT (Push-To-Talk) application runs on an LTE smartphone.
- A PTT protocol operates between the smartphone application and a network server.
- A network server interfaces with the smartphone application, handles requests, sends commands, manages user audio and data, and connects to the TETRA system.

In some cases, the network server controls the PTT application, processes call requests, and sets up calls. In other cases, it defers to a TETRA control server for these tasks. [35]

3.5.4.1. PTT application

It is designed to be installed on supported smartphones like Android or iOS. The deployment method can vary, allowing the end user or supplier to install, modify, or update the application over the air. The PTT app works with a dedicated button or virtual button to make a connection online or records a voice plays it during a mission-critical operation. The PTT app can run entirely in software or use the smartphone's hardware and peripherals. If the end user plans to switch to a 3GPP standard-compliant approach, the upgrade or replacement method needs to be considered. [35]

3.5.4.2. PTT protocol

A dedicated Push-To-Talk (PTT) protocol is used between the PTT application and the network server. This protocol uses IP over LTE. This protocol can be based on an existing standard such as OMA PoC or the MCPTT specification, or it can be based on a unique approach chosen by the vendor. The protocol is based on the speech coding which is according to AMR or ACELP or a proprietary one. The security is in accordance with a open standard or TETRA standard. If migrating to a 3GPP standard-compliant approach, interoperability between proprietary and 3GPP speech coding must be considered. [35]

3.5.4.3. Network server

The role of network server is to provide service for PTT apps. It communicates with the PTT app over IP through LTE network. The network server can connect to LTE as a separate data app. It is based on the LTE system's QOS. It might have a better connection that regular users and could connect to policy control and charging function to set up data priorities. Network server can control the calls over LTE and can make communication with TETRA. As a result, the connection between two networks can be established. On the other hand, it can work as a gate and allows TETRA to control all calls especially calls over LTE. [35]

3.5.5. Solutions of TETRA Connectivity to LTE

The next parts of will describe various methods for connecting with LTE. These methods may focus on different parts of the solution, so there could be some overlap. Any solution available on the market might include features from more than one of these methods.

3.5.5.1. TETRA services over LTE

TETRA over LTE uses a secure VPN tunnel in order to connect an LTE smartphone app to the TETRA service network. To dispatchers and TETRA radio users, smartphone users are TETRA subscribers, who can use the same services and join the same groups. Security, availability, and priority can be provided via LTE access from a commercial cellular operator or a dedicated LTE service for public safety. [35]

This solution enables TETRA operators to add and expand services to a new user base of critical infrastructure (utilities and transport) and public services (healthcare) — all within their existing TETRA network. It lowers costs of investment by treating LTE smartphone users the same as TETRA radio users. LTE phones with TETRA apps can also be served by the TETRA systems. [35]

They do not interfere with the traditional TETRA radio users but instead, they have extended services to LTE phone users. Users of both types can share services and take part in calls together. Full access for smartphone users includes individual and group calls, PSTN calls via TETRA (tel. no.), and service prioritization of usage (as for TETRA radio users). [35]

there are some TETRA servers that support wi-fi and LTE communications like Motorola and Airbus servers and radio devices. In this way, when TETRA network is not accessible or out of service, the devices can switch to other networks automatically in order to have a continuous service. [35] (more details are mentioned in chapter 4)

Another type to be mentioned is TETRA over LTE. This service enables users to talk with each other in group call with their smartphones. Control room staff can manage this service. However, an app is necessary to join a meeting (explained in Airbus catalogues). [35]

Another point that should be mentioned is that whether this service is the same as public safety LTE or not. Public safety LTE refers to LTE standard features for public safety, defined by the 3GPP, and includes various solutions for public safety users which is from entire radio networks to single applications. One example is a professional public safety application running on an LTE network, which could be either a commercial broadband network or a dedicated one used only by a public safety organization. Another example is a complete LTE system with important public safety features. Some of these features are already defined in the standards, while others are still in development and will be included in future releases. [35]

3.5.5.2. Gateways

TETRA can be integrated with cellular network by using gateways and dispatch systems that enables communication between two networks. It is essential during a disaster or terrorist attack which makes the responders works with each other efficiently. [35]

This interoperability makes users use some services like GPS tracking, video streaming, data transfer and enhancing capabilities. In addition, it can be worked as a backup communication when TETRA network fails; in this way, the continuous service will be ensured.[29]

In the gateway method, the PTT does not reuse TETRA protocol but it is based on other approaches like OMA POC (like walkie talkie but over cellular networks), 3GPP MCPTT or fully proprietary. In this way, the gateway needs to be adopted to TETRA requirements. The TETRA interface may be proprietary or based on a standard such as the TETRA inter-system interface. [35]

A gateway is a device to connect the local network to any mobile network. Gateways can manage calls separately for TETRA and PTT users or use a single server for all calls. TETRA can support both group calls and individual calls but there are some limitations. The reliability of solution depends on the quality of LTE solution of the chosen gateway. [35]

The gateway solution needs to convert addresses between networks to identify users and groups. It might also need to adjust speech coding methods, but it can use TETRA's ACELP codec directly as an option.

In this method, a security approach is required to provide separate security between the network server and application client on the LTE side, different from the TETRA network. However, if the TETRA ACELP codec is used throughout, TETRA end-to-end encryption can also be implemented. [35]

3.5.6. Integrated solutions

Integration of TETRA and LTE is beyond the application layer according to OSI or TCP/IP architectures. Base stations from both technologies connect to a single core and database for optimal performance and maintenance. All switching intelligence is centralized; in this way, both technologies only appear at radio level. [35]

There is one server for the application layer, handling call processing. LTE users utilize an app on their smartphones; while, TETRA users use their own devices.

When TETRA network is combined with LTE network, same database is used for the subscribers. This means on server handle the calls and it eliminates the second server for this case. While the LTE's e NodeB has a standardized interface, that TETRA does not. [35]

Mission critical app can be directly connected to LTE network using MCPTT and MC DATA interfaces. This means basic services work without concern for the terminal technology (TETRA, LTE). As a result, a control and command center can make selective or group calls and messages without knowing the terminal type. [35]

Most TETRA users prefer to keep their numbering plan which may not be the same for the other connected networks. Most TETRA numbering plans aren't compatible with standard NMIs used by public

operators. This is issue can be solved with a central database. All terminals have a standard NMI and a local address according to TETRA system which is recorded in a single database with automatic address conversion. [35]

3.5.7. characteristics of each approach

TETRA over LTE, Gateways, and Integrated approaches include commitments from suppliers to evolve with the standards. These approaches allow to have vary degree of interworking and the flexibility to choose the LTE terminal suppliers which considers security needs. The functionality for interworking is different; in this way, it is important that the solution meet the requirements. [35]

3.5.7.1. TETRA over LTE

For advantages, it should be pointed out that it allows existing LTE smartphone users to access TETRA services. This approach extends TETRA network. This helps start interworking and develop procedures with public safety broadband data applications that are already in use. [35]

The real connection from LTE to TETRA is a link which is from the smartphones to TETRA network. This connection has the ability to control LTE bearer QoS. An integrated or dedicated server/gateway manages the interconnect/translation for both traffic and signaling. [35]

In order to have a secure connection from smartphone users to TETRA network, the LTE users utilize a VPN tunneling. It should be mentioned that this VPN tunnel (protocol) should be supported by LTE network. The most common type of VPN is IPSec. SSL/TLS, GRE over IPsec and MPLS VPN are also other types of frequently used VPNs. [35]

TETRA end-to-end encryption (e2ee) needs security key storage in the LTE terminal and key exchange over LTE. Commercial LTE smartphones require a separate smart card-based solution. In addition, ACELP of TETRA voice coding must be supported in MCPTT standard to make an interworking between TETRA and MCPTT.[35]

3.5.7.2. Gateways

The idea of having gateway in TETRA network is well-known because to connect the TETRA network to PSTN, we need to have gateways. As a result, this approach can be extended to LTE network. The LTE side of the network will be standard if different suppliers are used. The exclusive part involves mapping services between TETRA and LTE.

Vendor solutions must consider security to protect the TETRA network. A separate gateway cannot manage TETRA end-to-end encryption (e2ee) without support in both TETRA and LTE terminals. Additionally, using commercial LTE smartphones requires a separate smart card-based solution. [35]

3.5.7.3. Integrated solutions

TETRA over IP and Gateway solutions expand existing TETRA networks. The Integrated Solution is best for new installations which uses a single core and common database for all connected networks.

It supports the numbering plan with a central subscriber database which centralizes user information and simplifying the routing of PTT and other communications. [35]

In table 3.3, we can compare the characteristics of TETRA and TETRA over LTE(MC-LTE).

feature	TETRA	TETRA over LTE(MC-LTE)
technology	Narrowband PMR (Professional Mobile Radio)	Broadband LTE-based
bandwidth	25 kHz per channel	1.4 MHz – 20 MHz per channel
Data speed	Up to 28.8 kbps (single slot)	Up to 100 Mbps (downlink) and 50 Mbps (uplink)
latency	~250 ms	~30-50 ms
Voice quality	Narrowband, optimized for critical comms	HD voice, VoLTE, and push-to-talk (PTT) support
coverage	Long-range, optimized for wide-area networks	Dependent on LTE infrastructure (can be extended with private LTE)
reliability	Very high, designed for emergency use	High, but depends on LTE infrastructure and network congestion
Encryption and security	Strong end-to-end encryption (TEA algorithms)	LTE security features (e.g., IPSec, SIM-based authentication)
interoperability	Standardized for emergency services, public safety, and utilities	Supports integration with existing TETRA networks and IP-based services
Multimedia support	Limited (mainly voice and short data)	Supports video streaming, large data transfer, and multimedia messaging
scalability	Designed for public safety and utilities	More flexible for broader applications (public safety, transport, etc.)
Deployment cost	High (dedicated infrastructure required)	Variable
Use case	Emergency services, military, transportation, utilities	Mission-critical broadband applications, smart cities, public safety

Table 3.3: comparison between TETRA vs TETRA integrated with mobile network characteristics

Chapter 4: analysis of the commercial solutions

in this chapter, we discuss the commercial solutions in the market and compare them.

4.1. Motorola

Motorola is a company that provides important communication tools and services for businesses and governments. it was founded in 2011 after separation of the original Motorola company; however, the history of the telecommunication for this company returns to 1939. Motorola is the leading company for TETRA solution with the hugest market in the world. it has the most variety for TETRA in the market not only for the base stations but also for the radio devices.

Motorola Solutions has set up TETRA networks worldwide, like the Airwave network in the UK and the SIRESP network in Portugal, which are used by emergency services. The company focuses on making public safety communication based on advanced technology and continues to grow with new ideas and strategic partnerships.[48]

4.1.1 Motorola solution for base stations

- Motorola Solutions for base stations is under DIMETRA brand. one of the BSs is DIMETRA X Core. This system ensures long-lasting, reliable communication for critical tasks, featuring advanced security, scalability, and smart interfaces. It can expand from one site to over 5,000 and it is one of the flexible devices in the world. DIMETRA X Core is energy-efficient, which means in a long period, it reduces energy costs. It has scalable pricing, so organizations only pay for what they need. The software-defined core allows seamless upgrades and the addition of new capabilities. It also supports mobile broadband integration while protecting existing radio access networks.1000 Dimetra X has been sold worldwide showing its reliability. The system supports features like Inter System Interface, enabling seamless communication for international cooperation during emergencies. [48]
- DIMETRA Express is an all-in-one TETRA system that integrates base radios and a switch into a compact unit, ideal for small to medium-sized networks. It is designed for quick setup and ease of use, with features like browser-based installation and web-based app compatibility. The system can integrate into other networks using a single IP address and supports high upload capacity for many subscribers. This solution provides various communication services (voice, data, and telephony) and can grow to cover multiple sites as the organization expands.
- MTS series are the high-end base stations of Motorola which are categorized as MTS1, MTS2, MTS4 and MTS4l. [48]
    1. DIMETRA MTS1 TETRA Base Station: it is a compact, lightweight solution with an IP66 weather-resistant for indoor and outdoor use. it offers flexible installation options (wall, pole, tower, vehicle) and supports rapid deployments. furthermore, it was designed for minimal operational costs and seamless "TETRA everywhere" coverage. it is Ideal for rapid deployment applications. [48]
    2. DIMETRA MTS2 TETRA Base Station: it is a highly flexible, small base station designed to reduce site acquisition, installation, and maintenance costs. it fits into

a 19-inch cabinet for optimal space utilization and can be expanded to a 4-carrier system. [48]

3. DIMETRA MTS4 TETRA Base Station: it is useful for coverage and resilience during both natural and man-made events. also, it offers best-in-class radio performance and a fully redundant design, ensuring high reliability. it is Ideal for mission-critical communications, delivering high performance while minimizing costs. [48]
4. DIMETRA MTS4L TETRA/LTE Base Station: A hybrid solution that integrates LTE alongside TETRA by adding an eNodeB into the TETRA Base Station cabinet. [48] in addition, it provides flexible collaboration between TETRA and LTE systems for a seamless, future-ready communication network. [48]

figure 4.1: M2 base station [48]

4.1.2. Motorola radio devices

Motorola has the most variety in radio devices in TETRA. they are equipped with BT version 4.1,5.2, 5.3 in different models, wi-fi and LTE for some other models. besides, they are strong security features such as CCK, GCK, and other key features alongside with TEA A and B sets. supporting DMO repeater is another important feature of this radio devices. one of the high-end TETRA radio devices is MXP 660 which supports TEA 1-3 and 5-7 and LTE and BT v 5.3. [48]

Figure 4.2: MXP 660 TETRA radio device [48]

4.2. Airbus

Airbus TETRA solution is one of the most famous manufacturers and a leading one in the world. It offers secure and reliable communication with instant push-to-talk features, helping teams stay connected. The system also works well with broadband networks, providing both voice communication and fast data services to improve operations. Airbus' TETRA is trusted worldwide, used in over 80 countries by more than two million people every day which is mostly used in tough environments. [49]

4. 2.1. Airbus base stations

- reliable coverage is so important for professional networks. if the area is not covered, it is challenging for the users. However, the TB3 TETRA base from Airbus is designed to meet this requirement, improving service quality, providing more coverage, or both. it can bring optimal availability for the network. besides by providing enough coverage, it can reduce operating costs particularly through remote operation and maintenance, a field where Airbus TETRA System has been a leader. [49]
- The TB3hp mini-TETRA base station is one of the most powerful base stations of the TETRA network from Airbus. it is used for quick deployable networks with huge network coverage standalone use, and temporary radio coverage. when capacity is not required, this base station is ideal to exchange radio signals. it offers various antenna setup due to its high output power (15W), extreme sensitivity, and Rx diversity. despite its small size, it can provide services like large TB3 base stations. including data and air interface encryption, type 1 handover, and base station fallback. it can provide radio services for the areas without radio coverage. It can be connected via satellite to a DXT3 or Taira switch to offer the same services as other base stations. Multiple TB3hp stations can be linked to a DXT3 or Taira switch to create a powerful wide-area radio network. it can also provide radio signals for indoor environments like subway using two carriers for capacity or resilience. [49]
- Customers benefit from Airbus's critical communications ecosystem through ongoing cooperation with leading companies, which leads to new innovations. The latest example is the TB4 hybrid base station, the first to offer both TETRA and 4G/5G radio access. The TB4 uses the latest cellular network technology, like multicarrier remote radios, to enable a smooth transition to hybrid networks. The TB4 hybrid base station supports both TETRA and broadband LTE access. It offers the same powerful features as the TB3, such as Air-Interface Encryption, Type 1 Handover, and base station fallback, plus lower power consumption and the option to use remote radio units for operational cost savings. TB3 customers can use their existing antenna setups with the TB4, saving on network planning and implementation costs [49]
- The TB3p mini-TETRA base station is a powerful and compact unit, about the size of a laptop, that offers the same features as the larger TB3 base station. It provides hotspot coverage for areas the network doesn't reach, including indoor and outdoor gaps, and data hotspots with its TEDS capability. The TB3p consumes less than 50W, making it highly energy-efficient with a small carbon footprint. It is cost-effective as it doesn't require costly site rentals and transmission fees. this base station is used by Cassadian. [49]

4.2.2. Airbus radio devices

Airbus makes TETRA devices for reliable and secure communication, especially for public safety, transport, and utilities. Their TH1n TETRA radio is small, lightweight, and easy to use. It’s very flexible, acting as a radio, pager and even has Voice Feedback to use without looking at it. The TH9 TETRA radio is tough and powerful, with GPS for location tracking and wireless connectivity for accessories, making it great for

emergencies or covert use. they are two of TETRA radio devices offered by Airbus; however, in the upcoming parts, we compare the TETRA radio devices of Airbus with other brands. [49]

figure 4.3: airbus TH1n radio device [49]

4.3. Hytera

Hytera Communications, founded in 1993 in Shenzhen in China, is one of the most famous providers of TETRA and other mission-critical solutions. Their TETRA systems offer secure, reliable, and efficient communication designed to meet the needs of industries like public safety, transportation, and etc. their system is according to ETSI standard which means it guarantees, it can work with other brands. also, this ensures easy integration and reliable communication across different platforms. Hytera's TETRA systems offer flexible designs to meet different needs such as:

- Centralized architecture for high reliability with redundancy.
- Distributed architecture for full TETRA functions across networks.
- Lightweight architecture for small networks, focusing on efficiency and quick setup.[50]

4.3.1. Hytera base station

- iBS: The iBS base station was designed for indoors and outdoors environments. It's compact, lightweight, and easy to transport, making it quick to set up and cost-reducing one. It can be installed on walls or antenna masts which is flexible to be installed. [50]
- DIB R5: The DIB-R5 compact is a small, lightweight base station perfect for indoor setups with low-capacity needs. It can handle to four TETRA carriers and has one or two racks based on capacity. Its fully redundant design ensures reliability, and it supports triple diversity reception. Meeting

the TEDS standard, it provides secure voice communication and fast data transmission for critical missions.[50]

figure 2.4: iBS TETRA base station.[50]

4.3.2. Hytera radio devices

Hytera offers different radio devices for TETRA. These devices are designed to make a reliable and efficient communication. They satisfy the requirements of TETRA devices in different fields. Key features are described as below.

- Compliance with ETSI Standards: Hytera's TETRA devices are compatible to the European Telecommunications Standards Institute (ETSI). this design ensures interoperability and seamless integration with other compliant systems.[50]
- Advanced Functionality: These radios support features such as end-to-end encryption, GPS positioning, and other communication modes. To mention them individual, group, and emergency calls, enhancing operational efficiency and safety. .[50]
- Durable Design: they were built to work in harsh environments, Hytera's TETRA radios are often rated for dust and water resistance, ensuring reliable performance in challenging conditions.

Hytera's TETRA radio devices are utilized worldwide in various mission-critical applications, including public safety, transportation, and utilities. .[50]

4.4. Cassidian

Cassidian, once part of EADS, focused on defense and TETRA communication systems. In 2014, it became part of Airbus Defense and Space, with its TETRA solutions now under Airbus' Secure Land Communications. Cassidian contributed to secure communication projects globally, such as systems in Thailand and a tram network in Shenyang, China, boosting mission-critical operations worldwide. their office in Turin is Aladina Radio S.r.l. they offer Airbus TP3 mini for base station and TH9 for radio device.[52]

4.5. Funktel

Funktel is a German company fucuses on highly secured devices for public safety, hazardous environments and emergency services. with durable design, advanced safety features, and compliance with global standards, their TETRA solutions ensure secure and reliable communication in tough condition. in addition, since they were designed based on an open standard, they are compatible with other brands their base station is. DAMM and their radio devices are FT4, FT5 and FT5s. [51]

4.6. Sepura

Sepura Limited, founded in 2002 in Cambridge, UK, is a leading provider of TETRA communication solutions. Its products are used in over 90 countries across sectors like public safety, military, transportation, and utilities. Sepura is known for innovation and quality, making it a trusted name in critical communication worldwide. their radio devices are famous which are SC20, SC21, SC23, SCL3 and STP8X. [53]

4.7. comparison of base stations features

In this part, the different features of base station such as frequency, connectivity, security and other features are compared.

4.7.1. supported frequency

As was mentioned in the second chapter, in TETRA various frequency ranges are supported having specific names. in the following table, the supported frequency of each TETRA base station is specified. as it is seen airbus base stations have the biggest range for frequency support in TETRA.

Device/frequency bands	Emergency Services	Civil & private networks	Commercial networks	land mobile radio services
Motorola Express	*	*	*	*
Motorola Dimetra X	*	*	*	*
Motorola DIMETRA MTS1	*	*	*	

Motorola DIMETRA MTS2	*	*	*	*
Motorola DIMETRA MTS4	*	*	*	*
Motorola DIMETRA MTS4l	*	*	*	*
Airbus TB3	*	*	*	*
Airbus TB3hp	*	*	*	*
Airbus TB4 hybrid BS	*	*		
Cassidian(airbus) TB3mini	*	*	*	*
HYTERA DIB R5	*	*		
HYTERA iBS	*	*		
DAMM TETRA Flex	*	*	*	*

table 4.1: supported frequencies for BSs

4.7.2. transmitting power

this feature is one of the most important aspects of a TETRA base station. higher transmitting power is better; however, it consumes more energy. TEDS has lower transmitting power compared to TETRA Version 1 mainly due to higher data rates and modulation schemes.

transmitting power	V1 (W)	V2 (W)
Motorola Express	5 to 40(configurable)	
Motorola Dimetra X	1 to 40(configurable)	
Motorola DIMETRA MTS1	•40 (without Tx combining) •25 (with Tx hybrid combining)	
Motorola DIMETRA MTS2	•40 (without Tx combining) •25 (with Tx hybrid combining)	
Motorola DIMETRA MTS4	•25 •40	•10 •20
Motorola DIMETRA MTS4l	•25 •40	•10 •20
Airbus TB3	25 To 40	

Airbus TB3hp	max. 15 per carrier	
Airbus TB4 hybrid BS	40	
Cassidian(airbus) TB3mini	20	
HEYTRA DIB R5	25	10
HYTERA iBS	40	
DAMM TETRA Flex	20	

table 4.2: transmitting power of BSs

4.7.3. Transmitting protocols

these parts related to the supported protocols by base station to connect to the network.

Device/protocols	Ethernet	MPLS	Satellite transmission	IP	E1	TEDS	LTE/5G	GPS
Motorola Express	*			*				
Motorola Dimetra X	*			*		*	*	
Motorola DIMETRA MTS1	*	*	*	*	*	*		
Motorola DIMETRA MTS2	*	*	*	*	*	*		*
Motorola DIMETRA MTS4	*	*	*	*	*	*		
Motorola DIMETRA MTS4l	*	*	*	*	*	*	*	
Airbus TB3	*		*	*	*	*		*
Airbus TB3hp	*		*	*	*	*		*
Airbus TB4	*		*	*	*	*	*	*
Cassidian(airbus) TB3mini	*				*	*		
HYTERA DIB R5	*		*	*	*	*		*
HYTERA iBS								*
DAMM TETRA Flex	*			*	*	*		

table 4.3: supported protocols by BSs

4.7.4. Power consumption

one of the most important aspects of a TETRA base station is power consumption. the lower is the better. however, it depends on other parameters such as supported frequencies, transmitting power and etc.

Device	Power consumption (W)
Motorola Express	60
Motorola Dimetra X	•single rack: 1200 •redundancy racks: 800
Motorola DIMETRA MTS1	•100 Watt (at 10 Watt Tx) •75 Watt (at 1 Watt Tx)
Motorola DIMETRA MTS2	•350-470 MHz: 640, •806-870 MHz: 700
Motorola DIMETRA MTS4	•350-470 MHz: 1300, •806-870 MHz: 1445
Motorola DIMETRA MTS4l	•UHF:1300 •800 MHZ:1445
Airbus TB3	65
Airbus TB3hp	•100 (1–carrier) •200 (2–carrier)
Airbus TB4	•100 (1–carrier) •200 (2–carrier)
Cassidian(airbus) TB3mini	50
HYTERA DIB R5	•1500 with 4 carriers •850 with 2 carriers
HYTERA iBS	400
DAMM TETRA Flex	75

table 4.4: power consumption of BSs

4.7.5. operating temperature

this table indicates the temperature range that TETRA BSs can be operated. it illustrates that nearly in all conditions they are operational.

Device	Operating temp (°C)
Motorola Express	-30 to +60
Motorola Dimetra X	-40 to +75
Motorola DIMETRA MTS1	-30 to +55
Motorola DIMETRA MTS2	•-30 to 55 (without fans) • -30 to 60 (with fans)
Motorola DIMETRA MTS4	•UHF: -30 to 60 •800 MHZ: -30 to 55
Motorola DIMETRA MTS4I	•UHF: -30 to 60 •800 MHZ: -30 to 55
Airbus TB3	-10 to 55
Airbus TB3hp	-10 to 55
Airbus TB4	-40 to 55
Cassidian(airbus) TB3mini	-10 to +55
HYTERA DIB R5	-30 to +55
HYTERA iBS	-40 to 60
DAMM TETRA Flex	-25 to +55

table 4.5: operational temperature

4.7.6. security

it is one of the most important features of each TETRA base stations and the higher security, the higher network confident and data delivery.

device/feature	authentication	AIE	End-to-end encryption	Local Site Truncking	Jamming detection	Base station fallback	Remote and local alarm
Motorola Express	*	*	*	*			
Motorola Dimetra X	*	*	*				
Motorola DIMETRA MTS1	*	*	*	*	*		
Motorola DIMETRA MTS2	*	*	*	*	*		
Motorola DIMETRA MTS4	*	*	*	*	*		
Motorola DIMETRA MTS4l	*	*	*	*	*		
Airbus TB3	*	*	*		*	*	*
Airbus TB3hp	*	*	*		*	*	*
Airbus TB4	*	*	*		*	*	*
Cassidian(airbus) TB3mini	*	*	*		*	*	*
HYTERA DIB R5	*	*	*	*	*		
HYTERA iBS	*	*					
DAMM TETRA Flex	*	*	*	*			

table 4.6: security features of BSs

4.7.7. diversity reception

as it was mentioned it the second chapter, this feature shows the signal reception quality which is indicate the power to reduce the noise.

device/diversity	single	dual	triple	duplexed	Non duplexed
Motorola Express		*	*		
Motorola Dimetra X		*	*		
Motorola DIMETRA MTS1	*	*			
Motorola DIMETRA MTS2	*	*	*		
Motorola DIMETRA MTS4	*	*	*	*	*

Motorola DIMETRA MTS4l	*	*	*	*	*
Airbus TB3			*		
Airbus TB3hp			*		
Airbus TB4			*		
Cassidian(airbus) TB3mini	*				
HYTERA DIB R5			*		
HYTERA iBS			*		
DAMM TETRA Flex		*			

table 4.7: diversity reception in BSs

4.7.8. other features

this part indicates some specific feature of BSs. some of them were mentioned in some datasheets; on the contrary, some of them were not.

device/feature	Operating bandwidth (MHz)	Carrier spacing (kHz)	Carrier spacing (TEDS) (kHz)	Receiver sensitivity (dBm)	Remote configuration	Work in humid condition
Motorola Express	• 350-470 MHz: 5 • 806-870 MHz: 19	25	25 / 50	•UHF: -120, -113.5 •800 MHz: -119.5, -113	*	
Motorola Dimetra X	• 350-470 MHz: 5 • 806-870 MHz: 19	25	25 / 50	• 350-470 MHz: -120 static, -113.5 faded •806-870 MHz: -119.5 static, -113 faded	*	
Motorola DIMETRA MTS1	5	25	25 / 50	•-117.5 static • -111 faded	*	
Motorola DIMETRA MTS2	•UHF: 5 •800 MHZ: 19	25	25 / 50	•UHF: -120 static, -113.5 faded •800 MHz: -119.5 static, -113 faded	*	
Motorola DIMETRA MTS4	•UHF: 5 •800 MHZ: 19	25	25 / 50	•UHF: -120 static, -113.5 faded	*	

				•800 MHz: -119.5 static, -113.5 faded		
Motorola DIMETRA MTS4l	•UHF: 5 •800 MHZ: 19	25	25 / 50	•UHF: -120 static, -113.5 faded •800 MHz: -119.5 static, -113.5 faded	*	
Airbus TB3		25		•dynamic: -112 •static: -119	*	
Airbus TB3hp		25		Dynamic: -112		
Airbus TB4		25		Dynamic: -112	*	
Cassidian(airbus) TB3mini		25		Dynamic: -112		
HYTERA DIB R5		25	Up to 150	-119	*	*
HYTERA iBS		25		•static: -120 •dynamic: -112		*
DAMM TETRA Flex				• diversity, static: -121 • without diversity, static: -118 • with diversity, dynamic: -118 • without diversity, dynamic: -112	*	*

table 4.8: other features

4.8. comparison of radio devices

In this part, the different features of radio devices such as frequency, connectivity, security and other features are compared.

4.8.1. battery capacity and uptime

one of the most important aspects of each radio device is its battery capacity and its uptime showing its operationality time. some of devices are offered with two battery capacity because the customer can choose different features in radio devices.

Device/battery info	Battery capacity (mAh)	Up time (h)
Motorola st 7000	2300	20
Motorola MTP 3000	1950 & 3400	
Motorola Mtm 5400	3800	24
Motorola Mtp 850	1850	23
Motorola Mtp 6650	1950 & 3400	24
Motorola Mxm 600	1900 & 3400	
Motorola Mxp 660	1900 & 3400	24
Motorola Mtp 8000	2000	
Motorola MXM 7000	3000	
Motorola St7500	2300	22
Airbus THR8800i	2000	25
Airbus TH1n	1950	20
Airbus TMR8800i	3800	
HYTERA MT680	3800	
HYTERA PT310	3800	
HYTERA PT350	3800	
HYTERA PT560h	2000 & 2500	27
HYTERA PT580h	1800 & 2500	22
HYTERA PT790	1800	14
HYTERA PT890	2150	26
HYTERA PTC760	2900 & 4000	14 & 20
HYTERA PTC680	2400 & 4000	
HYTERA PT590h	2000	22
Cassadian TH9	1900	19 & 25
Funktel FT5S	1900 & 3800	22 & 31
Funktel FT5	1900 & 3850	22 & 31
Sepura cs20	1160 & 1880	22
Sepura cs21	1160 & 1880	22
Sepura cs23	1160 & 1880	22
Sepura scl3	1160 & 1880	22
Sepura stp8x	1400	25

table 4.9: battery capacity and up time of radio devices

4.8.2. frequency bands

like base stations, each radio device can support some of frequency bands.

Device/frequency bands	Emergency Services	Civil & private networks	Commercial & private networks	land mobile radio services
Motorola MXM 7000	*	*	*	
Motorola MTP 8000	*	*	*	*
Motorola Mtm 5400	*	*		
Motorola Mtp 850	*	*		
Motorola Mtp 6650	*	*		
Motorola Mxm 600	*	*		
Motorola Mxp 660	*	*		
Motorola Mtp 3000	*	*		
Motorola St7000	*	*		
Motorola St7500	*	*		
Airbus THR8800i	*	*		
Airbus TH1n	*	*	*	*
Airbus TMR8800i	*	*	*	*
HYTERA MT680	*	*	*	*
HYTERA PT310	*	*	*	*
HYTERA PT350	*	*	*	*
HYTERA PT560h	*	*	*	*
HYTERA PT580h	*	*	*	*
HYTERA PT790	*	*	*	*
HYTERA PT890	*	*	*	*
HYTERA PTC760	*	*	*	*
HYTERA PTC680	*	*	*	*
HYTERA PT590h	*	*	*	*
Cassadian TH9	*	*		
Funktel FT5S	*	*	*	
Funktel FT5	*	*	*	
Sepura cs20	*	*	*	*
Sepura cs21	*	*	*	*
Sepura cs23	*	*	*	*
Sepura scl3	*	*	*	*
Sepura stp8x	*	*	*	*

table 4.10: supported frequency bands of radio devices

4.8.3. operating temperature and storage temperature

since TETRA radio devices are used in harsh environments, the operating temperature is so important and, in each condition, they should resist.

Device	Operating temp (°C)	Storage temp (°C)
Motorola MXM 7000	-30 to 60	-40 to 85
Motorola MTP 8000	-30 to 60	-40 to 85
Motorola Mtm 5400	-30 to 60	-40 to 85
Motorola Mtp 850	-30 to 60	-40 to 85
Motorola Mtp 6650	-30 to 60	-40 to 85
Motorola Mxm 600	-30 to 70	-40 to 85
Motorola Mxp 660	-30 to 70	-40 to 85
Motorola Mtp 3000	-30 to +60	-40 to 85
Motorola St7000	-20 to +55	-30 to 85
Motorola St7500	-30 to 60	-40 to 85
Airbus THR8800i	-30 to 60	-40 to 85
Airbus TH1n	-30 to 60	-40 to 85
Airbus TMR8800i	-30 to 60	-40 to 85
HYTERA MT680	- 25 to + 65	-40 to 85
HYTERA PT310	-20 to 60	-40 to 85
HYTERA PT350	-20 to 60	-40 to 85
HYTERA PT560h	-30 ~ + 60	-40 to 85
HYTERA PT580h	-30 ~ + 60	-40 to 85
HYTERA PT790	-30 to 70	-40 to 85
HYTERA PT890	-30 ~ + 60	-40 to 85
HYTERA PTC760	–25 to 60	-40 to 85
HYTERA PTC680	-20 to 60	-40 to 85
HYTERA PT590h	-20 to 60	-30 to 85
Cassadian TH9	-20 to 55	-30 to 75
Funktel FT5S	-20 to 55	-30 to 75
Funktel FT5	-20 to 55	-30 to 75
Sepura cs20	-20 to +60	-40 to +85
Sepura cs21	-20 to +60	-40 to +85
Sepura cs23	-20 to +60	-40 to +85
Sepura scl3	-20 to +60	-40 to +85
Sepura stp8x	-20 to +60	-40 to +85

table 4.11: operating and storage temperature of radio devices

4.8.4. protection level

each device has protection level that shows its resistance to humidity, heat and dust. some devices have different levels of protection because manufacturers built different models for the devices.

Device/protocol	Protection level
Motorola MXM 7000	IP54
Motorola MTP 8000	IP64,65,66,67
Motorola Mtm 5400	IP67
Motorola Mtp 850	IP54
Motorola Mtp 6650	IP68
Motorola Mxm 600	Ip67
Motorola Mxp 660	Ip65,66,68
Motorola Mtp 3000	Ip65,66,67
Motorola St7000	Ip54,67
Motorola St7500	Ip65,67
Airbus THR8800i	Ip55
Airbus TH1n	Ip65
Airbus TMR8800i	Ip65
HYTERA MT680	Ip54,67
HYTERA PT310	Ip65-68
HYTERA PT350	Ip65-68
HYTERA PT560h	Ip68
HYTERA PT580h	Ip67
HYTERA PT790	Ip65-68
HYTERA PT890	Ip67
HYTERA PTC760	Ip6x
HYTERA PTC680	Ip67
HYTERA PT590h	Ip67
4	Ip65
Funktel FT5S	Ip65
Funktel FT5	Ip65
Sepura cs20	IP65, IP66, IP67 & IP68
Sepura cs21	IP65 and IP67
Sepura cs23	IP65, IP66, IP67 & IP68 IPx5
Sepura scl3	IP65, IP66, IP67 & IP68
Sepura stp8x	IP67

table 4.12: protection level of radio devices

4.8.5. connectivity

this part illustrates the supported protocols and hardware devices to connect over the network or other devices

Device/protocol	BT	USB	Wifi	RFID	LTE	NFC	TEDS
Motorola MXM 7000	*5.1	*			*		
Motorola MTP 8000	*4						
Motorola Mtm 5400	*						*
Motorola Mtp 850	*	*					
Motorola Mtp 6650	*4.1		*	*			
Motorola Mxm 600	*5.3		*				
Motorola Mxp 660	*5.3		*	*	*	*	*
Motorola Mtp 3000	*4.1			*			
Motorola St7000	*4.1						
Motorola St7500	*4.1						
Airbus THR8800i		*	*				
Airbus TH1n		*	*				
Airbus TMR8800i		*	*				
HYTERA MT680	*						
HYTERA PT310	*						
HYTERA PT350	*						
HYTERA PT560h	*						
HYTERA PT580h	*		*			*	*
HYTERA PT790	*		*		*	*	*
HYTERA PT890	*5.2		*			*	*
HYTERA PTC760	*		*		*	*	*
HYTERA PTC680	*		*		*	*	*
HYTERA PT590h	*5.2						
Cassadian TH9	*4						
Funktel FT5S	*4						
Funktel FT5	*4						
Sepura cs20	*	*	*				
Sepura cs21	*	*	*				
Sepura cs23	*	*	*				
Sepura scl3	*	*	*				
Sepura stp8x	*						

table 4.13: connectivity of radio devices

4.8.6. security services

one of the most important aspects of TETRA radio devices is security showing the AIE supported protocols and security keys, mutual and end-to-end encryption.

Device/protocol	TEA1	TEA2	TEA3	TEA4	TEA5	TEA6	TEA7	EE2E	Mutual auth	CCK/DCK	SCK	GCK
Motorola MXM 7000		*						*		*	*	*
Motorola MTP 8000	*	*	*					*				
Motorola Mtm 5400	*	*	*					*				
Motorola Mtp 850	*	*	*					*				
Motorola Mtp 6650	*	*	*					*		*	*	*
Motorola Mxm 600	*	*	*		*	*	*	*				
Motorola Mxp 660	*	*	*		*	*	*	*				
Motorola Mtp 3000	*	*	*					*				
Motorola St7000	*	*	*					*				
Motorola St7500	*	*	*					*				
Airbus THR8800i	*	*	*					*				
Airbus TH1n	*	*	*					*				
Airbus TMR8800i	*	*	*					*				
HYTERA MT680	*	*	*	*				*		*	*	
HYTERA PT310	*	*	*					*				
HYTERA PT350	*	*	*					*				
HYTERA PT560h	*	*	*	*				*	*			
HYTERA PT580h	*	*	*	*				*	*	*	*	*
HYTERA PT790	*	*	*	*				*	*	*	*	*
HYTERA PT890	*	*	*					*				
HYTERA PTC760	*	*	*	*				*	*	*	*	
HYTERA PTC680	*	*	*	*				*	*	*	*	
HYTERA PT590h	*	*	*	*				*	*	*	*	
Cassadian TH9	*	*	*					*				
Funktel	*	*	*					*				

FT5S												
Funktel FT5	*	*	*					*				
Sepura cs20	*	*	*	*				*				
Sepura cs21	*	*	*									
Sepura cs23	*	*	*					*				
Sepura scl3	*	*	*	*				*				
Sepura stp8x	*	*	*	*				*				

table 4.14: supported security features for radio devices

4.8.7. location services

this part relates to positioning features and supported satellite for radio devices. also, in some datasheets, the accuracy level of the calculated positioning of these devices were mentioned.

Device/protocol	LIP	A-GPS	GPS	GLONASS	Gallileo	BEIDoU	QZSS	Accuracy (m)
Motorola MXM 7000	*	*	*	*		*		5
Motorola MTP 8000	*		*	*		*		5
Motorola Mtm 5400	*		*					5-10
Motorola Mtp 850	*		*					5-10
Motorola Mtp 6650	*		*	*	*	*	*	1.2
Motorola Mxm 600	*		*	*	*	*	*	1.2
Motorola Mxp 660	*		*	*	*	*	*	1
Motorola Mtp 3000	*		*	*		*		
Motorola St7000	*		*	*				
Motorola St7500	*		*	*				
Airbus THR8800i		*	*	*	*	*		3
Airbus TH1n	*		*	*				
Airbus TMR8800i	*		*	*				
HYTERA MT680	*		*	*				
HYTERA PT310	*		*					2.5
HYTERA PT350	*		*					2.5
HYTERA PT560h	*		*					2.5
HYTERA PT580h	*		*	*		*		
HYTERA PT790	*		*	*		*		10
HYTERA PT890	*		*	*	*	*		1
HYTERA PTC760	*		*	*		*		
HYTERA PTC680	*		*	*		*		
HYTERA PT590h			*	*				

Cassadian TH9		*	*	*	*	*		
Funktel FT5S	*		*	*	*	*		5
Funktel FT5	*		*	*	*	*		5
Sepura cs20			*	*	*	*		
Sepura cs21			*	*	*	*		
Sepura cs23			*	*	*	*		
Sepura scl3	*		*	*	*	*		
Sepura stp8x	*		*	*	*	*		

table 4.15: positioning services for radio devices

4.8.8. other features

this section illustrates other features supported by TETRA radio devices such as DGNA (dynamic group number assignment), SDS (short data service), PD (packet data), PEI (peripheral equipment interface).

Device/protocol	PTT	SDS	PD	PEI	TMO G.call	DMO G.call	WAP	DGNA
Motorola MXM 7000	*	*			*	*		
Motorola MTP 8000	*	*		*	*	*		
Motorola Mtm 5400	*	*	*	*	*	*		
Motorola Mtp 850	*	*	*		*	*		
Motorola Mtp 6650	*	*	*		*	*		
Motorola Mxm 600	*	*	*	*	*	*		*
Motorola Mxp 660	*	*	*	*	*	*	*	*
Motorola Mtp 3000	*	*	*	*	*	*		
Motorola St7000	*	*			*	*		
Motorola St7500	*	*			*	*		
Airbus THR8800i	*	*			*	*	*	*
Airbus TH1n	*	*			*	*	*	*
Airbus TMR8800i	*	*			*	*	*	*
HYTERA MT680	*	*			*	*	*	*
HYTERA PT310	*	*			*	*	*	*
HYTERA PT350	*	*			*	*	*	*
HYTERA PT560h	*	*			*	*	*	*
HYTERA PT580h	*	*	*		*	*	*	*
HYTERA PT790	*	*	*		*	*		*
HYTERA PT890	*	*			*	*		*
HYTERA PTC760	*	*			*	*	*	*
HYTERA PTC680	*	*			*	*		*

HYTERA PT590h	*	*			*	*	*	*
Cassadian TH9	*				*			*
Funktel FT5S	*				*	*	*	*
Funktel FT5	*	*			*	*	*	*
Sepura cs20	*	*	*		*	*	*	*
Sepura cs21	*	*	*		*	*	*	
Sepura cs23	*	*	*	*	*	*	*	*
Sepura scl3	*	*	*	*	*	*	*	*
Sepura stp8x	*				*			

4.16: supported other features for radio devices

4.9. Integration of TETRA with other networks based on commercial solutions

since TETRA is a wide area network (WAN), it can be connected to other networks to make a unified solution. according to this Motorola, Hytera and Airbus created a unified communication solution to connect to TETRA network even from a private network. for instance, TETRA is out of reach or the network is not reliable, and the most reliable network is Wi-Fi or LTE; in this way, the TETRA radio device can be connected to this.

4.9.1. Hytera Smart One

Hytera SmartOne is an integrated dispatch and interaction platform that connects multiple communication systems including TETRA, DMR, LTE and broadband (Wi-Fi, 4G, 5G, etc.). It combines the multiple professional functions such as dispatching, voice recording, automatic vehicle location (AVL) and camera monitoring based on the use of one intelligent interface. Regardless of used radio technology, it is possible to connect various mobile radio networks at the same time which ensures the network is in control. It is ideal to deliver unified communication and to find out the potentiality of the radio network. individual and group calls, positioning services and text messages are the other features to be mentioned. [50]

versatile smart one functions are described as below:

- Integration of TETRA, DMR conventional, XPT DMR trucking and MPT: The feature can connect to various mobile radio systems at the same time. It combines all call, GPS, and message activities into one interface, making it great for managing large and mixed radio networks. [50]
- cross-technology communications: SmartOne links users of various mobile radio systems. It acts as a gateway, allowing groups and individuals from different systems to join the same voice calls and send text messages to each other. [50]

- wired or wireless communication: SmartOne can work as a radio dispatcher for all radio technologies, not just through an IP connection. For example, you can use its dispatcher features in mobile emergency vehicles [50]
- scalability: SmartOne is flexible and works for different system sizes. It can be a simple stand-alone setup on one computer or a larger client-server system with central servers and remote workstations. [50]
- TETRA-LTE Interconnection: LTE/5G can connect to TETRA with PTT application
- Wi-Fi & Private LTE Support: it enables users on Wi-Fi networks to communicate with TETRA users via SmartOne. [50]

the uses cases of this protocol are such as:

- emergency services. it allows smart phones users and radio users to communicate with each other.
- workers with different devices can communicate with each other and finally, transport systems
- transport systems. it provides interoperability between TETRA radios and broadband users in critical situations. [50]

4.9.1.1. Different solution by smart one

- first solution to make a unified communication is wireless interconnection This solution is based on a gateway in order to connect different mobile radio networks to make an inter-system communication.
- Sometimes, they need to talk to each other, and the command center needs to manage both. The Hytera SmartOne solution helps by installing two mobile radios and a gateway in an emergency vehicle, making communication between the two systems possible. [50]

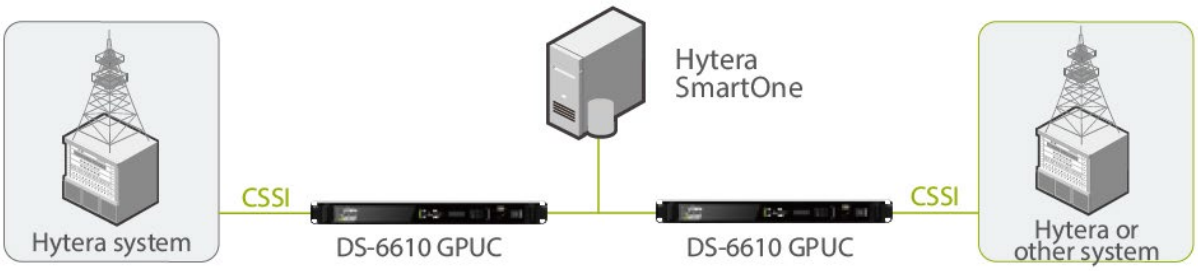

figure 4.5: smart one wireless solution [50]

- The second solution is based on the wired approach. This solution uses a PMR manufacture system or Inter Subsystem Interface (ISSI) interface to connect to Hytera SmartOne. In urban areas, a DMR trunking system is used, while the suburbs use DMR Tier 2. The Hytera SmartOne solution connects these two systems smoothly, allowing terminals to move between them and communicate through a shared dispatcher. [50]

figure 4.6: wired solution [50]

- The third one is according to mobile interconnection approach. Hytera SmartOne DS-6610 VPUC supports car-mounted installations which makes possible the inter-connection and dispatching. in this case, The DS-6610 VPUC is a quick-to-deploy on-site command center. It connects different devices, supports inter-department collaboration, and allows real-time communication between the on-site command center and headquarters, thanks to its multiple interfaces and strong processing capabilities. [50]
- And the last solution is based on interconnection approach. if different networks are connected together into Hytera smartone, the dispatcher on this platform can easily achieve unified platform for all network users. During major emergencies, multiple departments using systems like DMR Trunking, TETRA, or the PSTN Network may be involved. Hytera SmartOne enables communication and coordination among these departments to ensure efficient dispatching. [50]

figure 4.7: smart one [50]

4.9.2. Motorola Wave

Motorola WAVE (formerly WAVE PTX) is a Push-to-Talk over Broadband (PoC) solution that connects TETRA, DMR, LTE, and Wi-Fi users through a cloud or a premised platform. The default cloud for this platform is Microsoft Azure. when a TETRA cannot connect to the network, but a Wi-Fi or LTE is accessible, by connecting to that network, it is possible to use TETRA. Even with a mobile phone, it is possible to

connect to the network. This is particularly useful for organizations that need to collaborate across agencies or regions. [48]

key features are:

- Broadband PTT (Push-to-Talk). Enables instant communication between smartphones, tablets, PCs, and TETRA radios. also, to facilitate group communication, the system makes use of broadband networks that are independent of carriers. Even in situations where traditional radio coverage is not available, users can stay connected thanks to this feature
- Group & Individual Calls. Allows team communication across different devices and networks.
- Wi-Fi & LTE Compatibility. Works on public/private LTE and Wi-Fi networks.
- connect radio-to-radio: it connects multiple radio devices no matter what they are.
- extend radio to broadband: radio devices can connect to broadband networks
- MCPTT (Mission Critical PTT) Compliance. Ensures reliable, secure communications for first responders.
- Secure Messaging & File Sharing. Supports text, images, and videos between TETRA and broadband users.
- GPS Location & Geofencing. Tracks user locations in real time for better operational awareness
- Wave gateway: The main hub is the Wave PTX radio gateway. In addition to supporting features like real-time presence, over-the-air device management, and smooth network roaming, it links several communication systems.
- Client applications: Wave PTX provides desktop, web, and mobile apps that let users access PTT services. For example, the MXm5000 is one of the devices that can connect to the wave using a web application. Multimedia messaging, geofencing, location tracking, and even video streaming for improved situational awareness is all supported by these apps.[48]

4.9.2.1. solution for TETRA

Motorola Solutions DIMETRA™ system provides secure, efficient, and customizable communication for various markets. WAVE enhances this by extending DIMETRA networks to broadband users, improving team collaboration. It supports up to 39 simultaneous calls and 300 talk groups, while ensuring secure communication with encrypted talk groups. Emergency calls can connect WAVE and DIMETRA users, enabling quick and collective responses. [48].

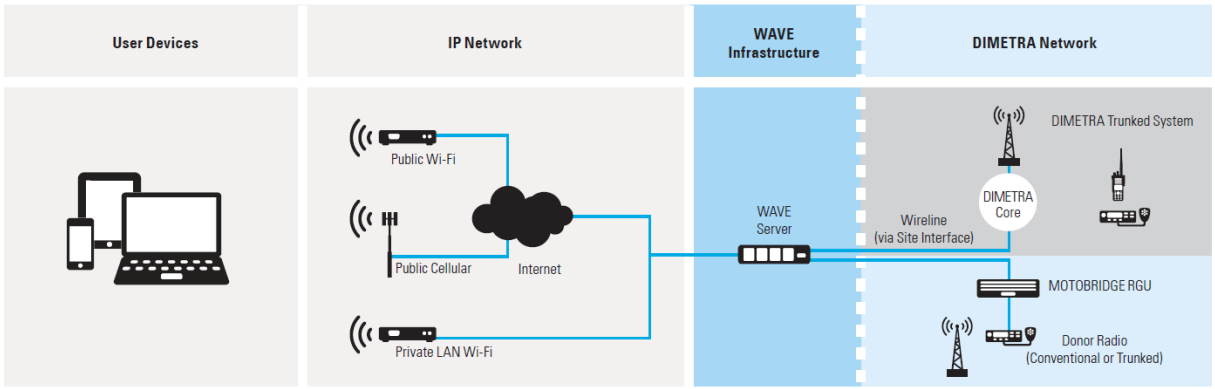

figure 4.8: Dimetra solution for TETRA and other emergency services [48]

the radio device should support this technology. For instance, Motorola MXP 660 is one of the most advanced Motorola radio devices that support wave. in this way, when TETRA is not accessible, it switches to other networks like Wi-Fi or LTE. This ensures continuous connectivity by leveraging hybrid communication systems. [48]

4.9.3. Airbus Tactilon Agnet

to facilitate secure group communications between multiple devices, Agnet TETRA integrates smartphones with TETRA technology. It complements Airbus TETRA and broadband systems and avoids drastic changes by combining existing solutions for radio operators, control room personnel and smartphone users. Smartphone multimedia services are also provided. Agnet TETRA is reliable in the long term as it is designed to meet current needs alongside future communication developments. The solution is designed for iOS, Android and Windows to use the TETRA network [49]

4.9.3.1. how it works

when shifting from narrowband to broadband, it's crucial to maintain reliable 4G/5G network coverage. Agnet over Satcom (satellite communication) provides global connectivity by integrating deployable networks and satellite communications for uninterrupted service. actually, with a VPN connection users can connect to the Airbus network to use TETRA and emergency services. this technology works on LTE/5G, wi-fi. it works on smartphones, tablets, desktop PCs, and rugged devices. [49]

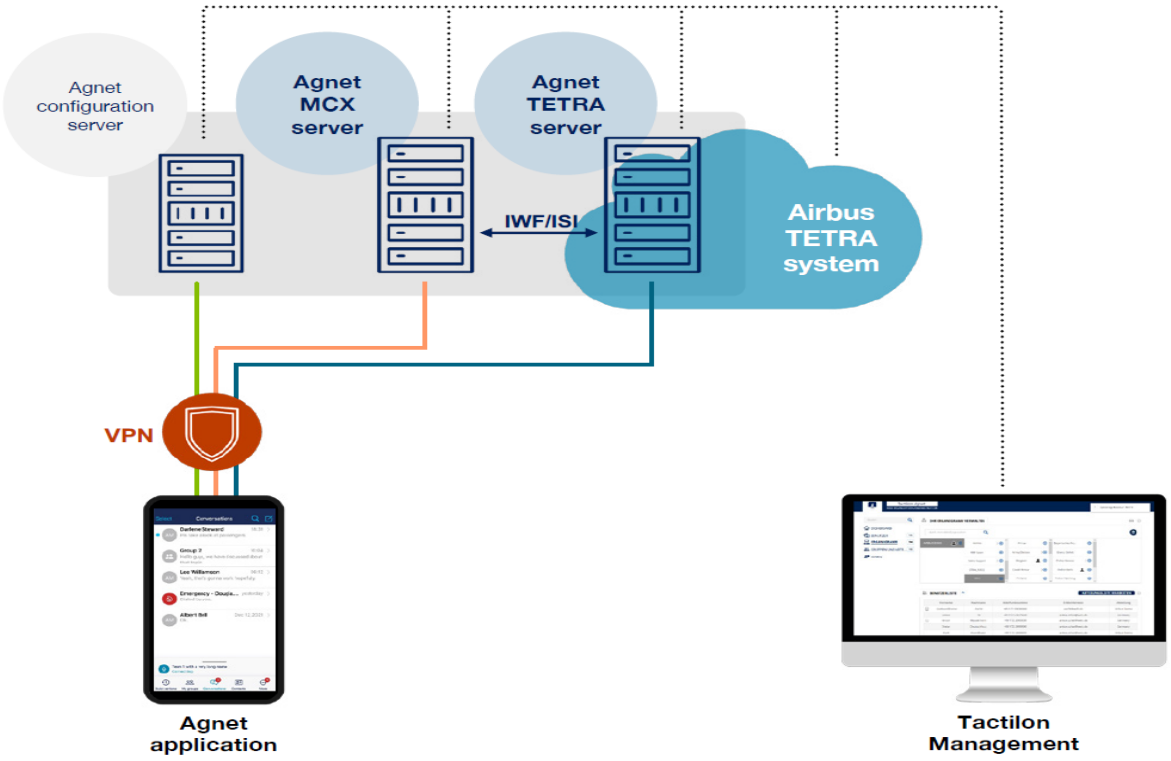

figure 4.9: Agnet solution [49]

Agnet TETRA helps public safety operators to migrate to open ecosystem MCX solutions compliant with 3GPP standards in a staged and managed manner. This reduces risks and helps operators solve problems one at a time. It helps users transition to smartphones without losing too much comfort. This approach also enables users to manage funds, meet device expectations, and maintain operational performance of critical functions for the network. [49]

The combination of the Agnet TETRA mobile application and Tactilon Management solution enables seamless transition support. Users of the Agnet TETRA mobile application are able to use dual communications with TETRA and MCX groups or users simultaneously. During the transition, Tactilon Management takes care of subscriber provisioning. Also, Agnet Configuration Server (CS) collaborates with Tactilon Management by sending configuration updates using 3GPP and CMS (content management systems) interfaces to the Agnet TETRA mobile application. In the realm of critical communications, Agnet TETRA is truly remarkable and unique.[49]

now, we can compare the Motorola wave Hytera smart one and Airbus Agnet with each other.

Feature	Hytera smartone	Motorola Wave	Airbus Agnet
Platform type	Integrated Dispatch & Interworking	Cloud-based	Cloud-based
TETRA-LTE bridging	*	*	*
Unified dispatch	*	*	*

DMR-TETRA integration	*	*	*
PTT over cell	*	*	*
Group and individual call	*	*	*
Wi-Fi support	*	*	*
Network messaging	*	*	*
MCPTT		*	*
Location tracking	*	*	*
Cloud deployment		*	*
End-to-end encryption	*	*	*
Connects	TETRA radio devices	TETRA radio devices	PCs, tablets, smartphones
Recommended for	Private Networks & Utilities	Enterprise Public Safety	Public Safety & Critical operation

table 4.17: comparison between commercial solution for integration of TETRA with other networks

Chapter 5: Conclusion

in this thesis, we analyzed the TETRA and public safety network with its requirements. The analysis reveals the important role of TETRA for public safety networks.

TETRA offers some advantages such as encryption, reliability, prioritization, group communication, sending files over the network to cope with the mission-critical operation needs. However, due to satisfy users' requirements improving the TETRA was inevitable; as a result, the TETRA v2 was published.

in order to transfer high quality images and video streaming, TETRA v2 was not enough; so, the new feature in TETRA to integrate with LTE and high-speed cellular networks was introduced. the integration of this technology with this mobile network is so important and reveals a key feature of this technology with makes it different from other public safety communication technologies.

Furthermore, In the market, we have different brands and technologies that their characteristics have been compared. Using standards-based approaches allows users to benefit from open competitive markets and it allows the users utilize different suppliers. For those who needs immediate solutions, there are various options from companies that offers different levels of inter-working. in this thesis, even we introduced some commercial solution to connect the TETRA over wi-fi or LTE/5G when TETRA is not accessible.

Commercial LTE systems provide good service, and they make a best effort. However, they need to be hardened, updated to the latest 3GPP Release, and potentially, they have an area coverage expanded for even better performance.

Future research and technological advancements should focus on a frame to ameliorate this technology such as enhancing security in hybrid public safety networks according to legal, regulatory, and policy considerations and TETRA over satellite is another topic to work on.

Bibliography:

[1] Mobile Broadband Communications for Public Safety: The Road Ahead Through LTE Technology, Ramon Ferrús and Oriol Sallent

[2] Public Safety Networks from LTE To 5G, Abdulrahman Yarali

[3] Report ITU-R M.2033, 'Radiocommunication objectives and requirements for public protection and disaster relief', 2003

[4] https://www.rfwireless-world.com/Tutorials/TETRA-radio-system.html

[5] https://en.wikipedia.org/wiki/Phase-shift_keying

[6] https://en.wikipedia.org/wiki/TETRA

[7] TETRA TECHNOLOGY: A MODERN PRIVATE CELLULAR SYSTEM Kashif Mehboob, Iqbal Muhammad Umair, Mirza Shoaib Ahmed

[8] TETRA factsheet Terrestrial Trunked Radio Federal Department of the Environment, Transport, Energy and Communications DETEC

[9] https://tcca.info/tetra/tetra-documentation/research_disclosures

[10] https://wwsinternational.com.au/Tetra_2011/sources/Dispatchers /PERSEUS_Dispatcher_Applications_EN_LR.pdf

[11] Terrestrial Trunked Radio (TETRA); Part 4: Network management, Reference: DTR/TETRA-01011-4 provided by ETSI

[12] https://www.pi4tta.nl/wp-content/uploads/simple-file-list/STTA-TMO-Getting-Started-v0_82_EN.pdf

[13] ETSI EN 300 396-1

[14] https://tcca.info/tetra/direct-mode-operation-dmo/

[15] https://en.wikipedia.org/wiki/Algebraic_code-excited_linear_prediction

[16] ETSI TR 102 513 V1.1.1

[17] Development of TETRA Radio Backhaul Network Redundancy Plan for Disaster Recovery in Mission

Critical Communications, Samuel Heleno *, Carlos A. Femandes

[18] https://www.etsi.org/technologies/tetra

[19] https://www.rohde-schwarz.com/us/technologies/cellular/tetra/tetra/tetra-tetra-2_55941.htm

[20] ETSI TR 102 021-5 V1.2.1

[21] https://tcca.info/tetra/tetra-your-service/voice-data/

[22] Introduction to TETRA Technology, et industries

[23] https://www.telecomtrainer.com/dmo-direct-mode-operation/

[24] Study on TETRA DMO and Mobile Ad-Hoc Networking, He Xiaoben

[25] https://pbeaxell.com/about/glossary/what-is-tetra

[26] https://tcca.info/tetra/home/always/

[27] https://tcca.info/tetra/tetra-your-service/interoperability/

[28] ETSI TR 103 565 V1.1.1

[29]https://wraycastle.com/blogs/glossary/tetra-radio-interoperability-with-cellular-networks?srsltid=AfmBOooyOoZ-FYHgjLv0Af6LFr9TLNT8OJYDb1owxcYyxbJ_KPIqg4N7

[30] ETSI - TETRA Technology Overview

[31] Motorola TETRA feature

[32] https://tcca.info/tetra/for-tetra-specialist/voice-services-facilities

[33] ETSI EN 300 392-12-10

[34] https://tcca.info/tetra/for-tetra-specialist/tetra-release-2

[35] August 2018 TETRA Connectivity to LTE by TCCA

[36] https://www.qsl.net/kb9mwr/projects/dv/tetra/tetra.pdf

[37] TETRA Enhancement Based on Adaptive Modulation, Ali R. Abood, DOI: 10.1007/978-981-33-6981-8_11

[38] https://www.ntia.gov/files/ntia/publications/compendium/0335.40-0399.90_01DEC15.pdf

[39] https://tcca.info/broadband/regulatory-radio-regulation-and-spectrum-updated-30-12-2009-2

[40] ETSI TS 100 392-15

[41] Improving recovered signal quality in TETRA Systems by Sepura

[42] https://lectrosonics.com/comparing-diversity-reception-techniques/

[43] https://www.hytera.com/eu/products/tetra-system/dib-r5-advanced

[44] https://en.wikipedia.org/wiki/Bearer_service

[45] https://criticalcommunications.airbus.com/en/tb3-tetra-base-station

[46] ETSI TS 104 053-2

[47] Security Analysis of TETRA, Shuwen Duan

[48] https://www.motorolasolutions.com/en_xu/products/tetra.html

[49] https://criticalcommunications.airbus.com/en/tetra/devices-and-accessories

[50] https://www.hytera.com/en/product-new/digital-radio/tetra-systems.html

[51] https://funktel.com/en/downloads

[52] https://aladinaradio.it/it-it/soluzioni/progettazione-reti/TETRA/index.php

[53] https://sepura.com/it/tetra/

[54] Observations on TETRA Encryption Algorithm TEA-3 Jens Alich1, Amund Askeland2, Subhadeep Banik3