España | digital 2026

Cybersecurity in TETRA networks study

Financiado por la Unión Europea
NextGenerationEU

MINISTERIO DE TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO DE TRANSFORMACIÓN DIGITAL
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

March 2023

INCIBE-CERT_CYBERSECURITY_IN_TETRA_NETWORKS_STUDY_2023_v1.1.docx

Index

INDEX OF FIGURES

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO DE TRANSFORMACIÓN DIGITAL
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

1. About this study

This study aims to **explain TETRA networks** in all their aspects. This technology is very unknown in different sectors, but very useful depending on the needs and requirements of the companies or users.

The writing has a technical redaction since it is focused on explaining all the aspects related to TETRA networks both for users who do not know the protocol and for users who want to improve the security features of their TETRA networks or see the possibilities that it offers, but at the same time it maintains a basic language for the understanding of the study by any person interested in this technology.

The order of the contents is distributed in such a way that initially there is a theoretical knowledge of the technology in general, to later focus on the use of TETRA in different companies, as well as on the possible threats that can affect this technology and the security functionalities that can be implemented.

In addition, different measures for network securitization and vulnerability mitigation are proposed.

Finally, reference is made to current technologies with similarities to TETRA networks, a preview of possible future technologies is presented, and a conclusion is made evaluating TETRA as a communication technology in all its aspects.

2. Document organization

This study on TETRA networks presents a structure focused on the progressive learning of this radio technology. Initially there is the 3.- introduction, in which it is possible to find a brief introduction to TETRA technology, its uses, functionalities and main features to introduce concepts that later will be explained in a more extensive way.

After the introduction, the 4.- TETRA technology itself is explained, with a complete overview including types of users, frequency bands, architecture, main elements and technology used to operate the network.

In order to introduce TETRA in the different sectors in which it is used, an explanation of the 5.- private and public sector together with TETRA networks. This section will explain the use of TETRA networks in both the private and public sectors, as well as a map by communities indicating the use of this communication network. It also identifies a specific case of a private company using a TETRA network for communications.

Subsequently, and already introducing the study in the dangers and 6.- security threats in digital radio networks, an explanation of these problems is made, distinguishing between two types: Vulnerabilities in the modes of operation and architecture, in addition to vulnerabilities in the types of encryptions.

Combined with the previous section, the study covers the different 7.- security functionalities in TETRA devices, with a complete explanation of the functionalities, functions, security keys and encryption provided by TETRA to secure communications, as well as a detailed explanation of each of the functions and functionalities presented. In addition, and in relation to the section on TETRA in the public and private sector, the different 8.- security requirements in enterprise applications will be presented, being these, some basic concepts for the hardening of these networks in industrial environments added to the TETRA security functionalities of the previous section.

Since most of the information on security is theoretical, we have introduced a section with 9.- real security functionalities in TETRA devices. This section of the study explains and defines some real functionalities of TETRA devices. It also lists possible 10.- mitigations of vulnerabilities in TETRA networks: Technical and operational mitigations for vulnerabilities in TETRA networks. In turn, the concepts for specific cases such as lack of integrity, confidentiality and availability will also be explained,

To conclude the study, we have sought to compare current technologies like TETRA, and what is expected of this technology or possible variants in the future, so we have included a section on the 11.- migration scenario and its security features.

To conclude the study, some conclusions have been written about the overall assessment of TETRA technology in all its aspects.

3. Introduction

The **TETRA** (*Terrestrial Trunked Radio*) network is a standard developed in Europe in the 1990s by ETSI[1] (European Telecommunications Standards Institute), whose emergence came about as a result of the management of mobile communications for extreme cases, in which standard communication via telephone might not work properly. Therefore, it can be considered as **an alternative network for communications with emergency and security services to be always operational**.

TETRA unifies different **digital radio** interface alternatives for communication and serves as a standard for the construction of private mobile networks or PMR (*Private Mobile Radio*).

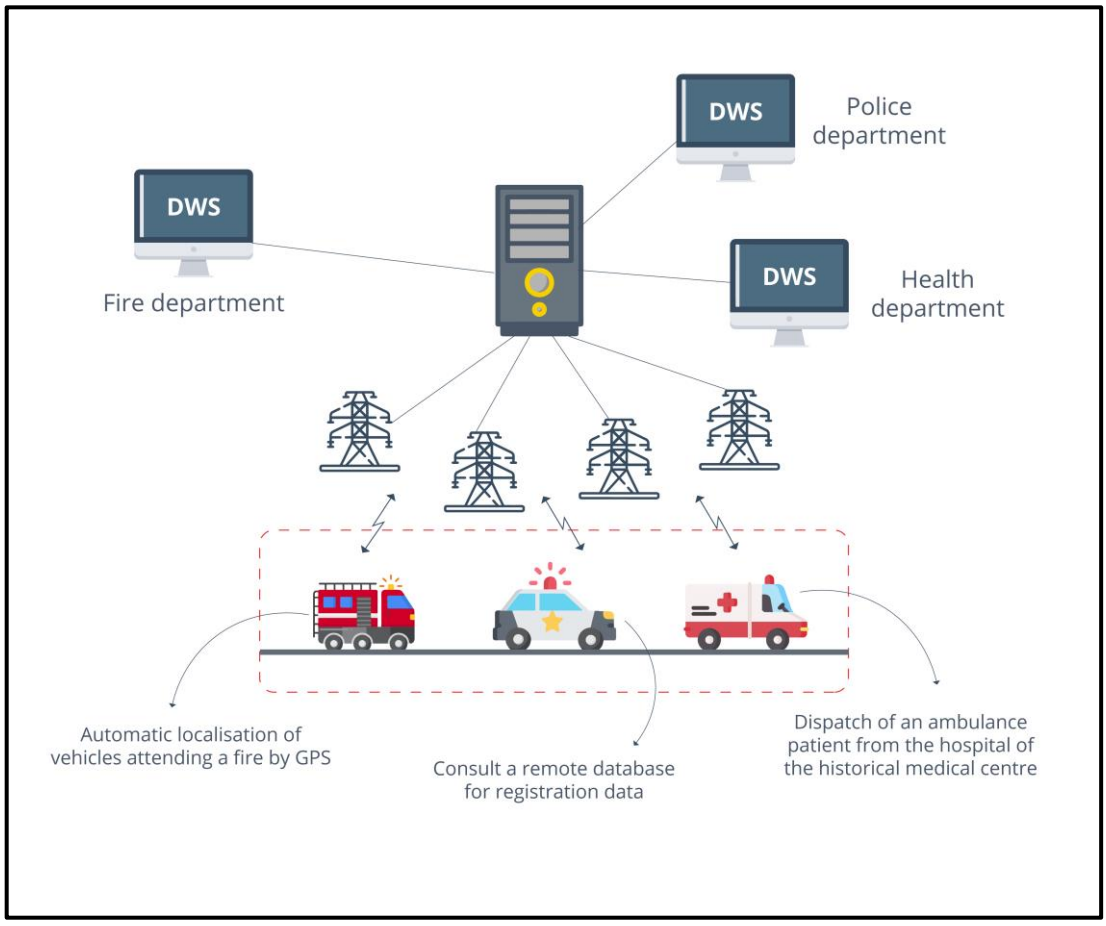


Illustration 1: Network structure of the TETRA system[2]

Today, these qualities allow different professional groups whose work is critical (police, firefighters, mobility agents, ambulances and even the national security communications network) to have an **advanced communications system with a high degree of reliability and security**.

[1] https://www.etsi.org

[2] https://tetralogik.com/tetra.html

These professional groups use the aforementioned **PMR networks**, which must always operate**, without any failure, in order to maintain an optimal level of communication, high voice quality, compatibility and availability in critical situations**.

Currently TETRA operates in **more than one hundred countries around the world.** Its high expansion lies in the characteristics presented above, which make it possible for any company with vital communications for its operation or any emergency infrastructure, regardless of whether it is public or private, to implement the standard in its communications. In addition, most countries in the world have reserved a frequency band for critical communications, i.e., communications vital for the welfare of people (such as police or emergency communications), or communications vital for the proper functioning of different companies with critical activities (offshore refineries, communication posts in ports and airports, companies in the nuclear sector, etc.). This band is in the 370-400 MHz range, a band in which a TETRA network can be implemented, thus simplifying the architecture creation process. Furthermore, the use of **such a low frequency allows achieving a greater coverage for each installed antenna**.

Although the frequencies may vary within a more or less established range, below, the different bands and the range of frequencies in MHz within which we could find different TETRA communications are detailed. It is worth noting the difference in frequencies between emergency services and public services, with a greater amplitude and diversity in the public service bands.

It is also widely used in communication networks within **sensitive industrial infrastructures**, such as refineries, due to the sensitivity of their work and location, as well as their need for high communication security to ensure authentication, confidentiality, integrity, availability and non-repudiation. In addition, TETRA provides **minimal set-up** time (<0.3 s), ***push-to-talk*** in group calls and **direct radio transmission (DMO)** between terminals.

Although TETRA provides different measures for **hardening the communications network**, such as the authentication protocol, it is true that there are flaws within the standard, such as those that can allow an attacker to override the authentication protocol, impersonate a base station and reduce the availability of access to the network by users. However, **there are methods or implementations capable of counteracting such flaws.**

Throughout this study, all the advantages offered by TETRA networks in terms of **security, ease of implementation and quality in emergency situations** will be detailed. Also, an analysis of TETRA networks in the private sector and the security of the implemented architecture will be made. On the other hand, the different threats that can affect the network will be explained, as well as the minimum requirements to be implemented to ensure that the communication is reliable and has no security failures.

4. TETRA technology

TETRA can be defined as a digital mobile radio standard, under the interoperability of the **TETRA Alliance**. Within this standard, there are also other variables such as TETRAPOL, which is used only to provide communications services to police forces in certain countries.

TETRA can have a wide range of users, ranging from law enforcement agencies, Homeland Security entities, the private sector and even individual end users.

As already introduced above, the main mission of TETRA is to cover different specific communication needs, for different types of users, in different environments and with very particular security measures, which could be grouped into:

- **PMR users (*Private Mobile Radio*):** Public safety entities, among which we find police, military, first responders....
- **PAMR users (*Public Access Mobile Radio*):** this group includes firefighters, ambulances, coast guard and other services with similar characteristics.

These two types of users depend on their communication being as optimal and secure as possible, since the correct performance of their work depends on it. Among the characteristics that these users seek for communication are good latency, security features against external agents and voice quality.

In turn, TETRA specifies two types of services when making a communication:

- **Basic services:** this may include individual calls, group calls or confirmed group calls (with authentication and authorization) and also different broadcast call services. As the name suggests, these are basic voice and, to a lesser extent, data services.
- **Supplementary services:** these services involve preemptive priority calling, priority calling, call holding, ambient listening, late entry services, area selection and DGNA (*Dynamic Group Number Assignment*).

These two services can be considered mission critical services and are services accessed by mobile users in different locations around the globe. This is one of the most important features of TETRA, the possibility for different users with different needs to be able to communicate, mainly because TETRA is the first truly open private digital mobile radio standard.

Being more specific, in terms of services and communications of TETRA users, below is a table that includes the different MHz frequencies of the bands used, both for basic and supplementary services within public services and emergency services.

Emergency Services			Public Service	
Number	Frequency pair (MHz)		Frequency Pair (MHz)	
	Band 1	Band 2	Band 1	Band 2
1	380-383	393-393	410-420	420-430
2	383-385	393-395	870-876	915-921
3			450-460	460-470
4			385-390	395-399.9

Table 1Frequencies by service

TETRA pursues the objective of being able to guarantee a multi-vendor and open market, and to this end, it specifies the following interfaces that it considers essential to achieve this objective:

- The **air interface** must ensure the interoperability of different terminal equipment for different manufacturers.
- **The terminal equipment interface** (TEI) should facilitate and facilitate the development of mobile data applications in a fully independent manner.
- The **inter-system interface** (ISI) must allow the interconnection of different TETRA networks, either from the same manufacturer or from different manufacturers.
- TETRA ensures with the inclusion of **Direct Mode Operation** (DMO) that communications between terminals are optimal even when out of network coverage.

The following illustration provides a better understanding of the possible communications between various TETRA networks, within the same TETRA network, between devices without coverage and between terminal interfaces and the network.

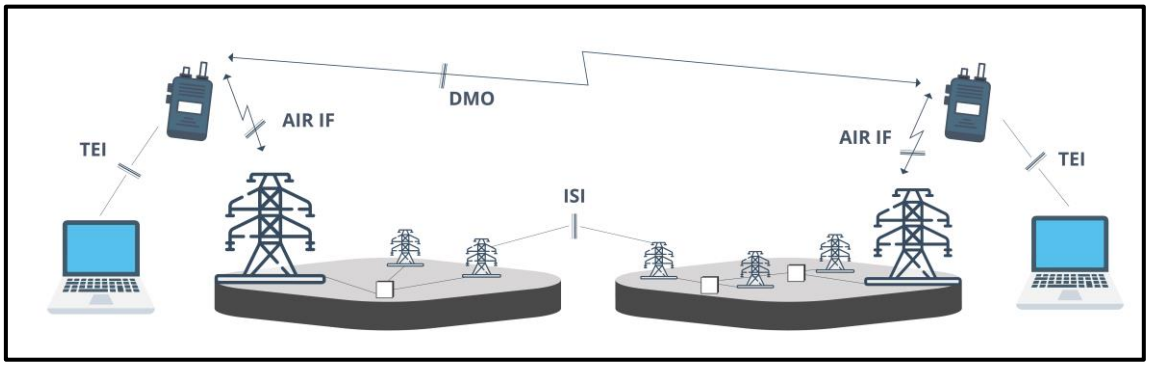


Illustration 2: TETRA architecture[3]

Once the possibilities in terms of users, devices, interfaces and different modes that can be implemented in a TETRA architecture have been discussed, it will be explained what technical features it offers with respect to other existing digital radio communication systems.

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

4.1. TETRA network infrastructure

The TETRA specification does not contemplate any type of network topologies since these can be flexible, i.e., depending on the situation or environment in which they are to be installed, they can be adapted and vary between a star, ring or mesh topology.

Within the standard, the network infrastructure is often referred to as the Switching and Management Infrastructure (SwMI), which will be explained in detail in section 4.2.2.1.1. *4.2 Technical characteristics*. The only thing that is defined in the TETRA standard are the entities and interfaces over which the devices within the infrastructure can and must be connected. Thanks to this, TETRA ensures interoperability and network management.

4.1.1. Entities

There are different entities within a TETRA system such as the following:

- A **Mobile TETRA System**, which include base stations (BS), switches, administration centers and operations.
- **Mobile Stations** (MS), which include the Mobile Termination Unit (MTU) and Terminal Equipment (TE).
- **Line Stations** (LS), which include, like the MS, the Mobile Termination Unit (MTU) and the Terminal Equipment (TE).
- The **central** network **administration unit.**
- Mobile stations operating in a DMO network.
- And as we will see later, the TETRA standard also contemplates **connections to other networks** such as the Public Switched Telephone Network (PSTN), Private Telephone Networks (PTN), Integrated Services Digital Network (ISDN) and Packet Data Networks (PDN).

4.1.2. Interfaces

Defined by TETRA for communication between some entities and for communication with other TETRA networks.

- **I1**: Air interface, through which the SwMI communicates with the mobile termination unit (MTU) of an MS.
- **I2**: Line Station Interface, through which the SwMI communicates with the line termination unit (LTU).
- **I3**: Inter-System Interface, through which two different TETRA networks communicate.
- **I4:** Interface between the MS station and the TE.
- **I4'**: Interface between the LS and the TE.
- **I5**: Network management interface.
- **I6**: Direct Mode Operation Interface (DMO). Through this interface, the Terminal Equipment working in a DMO network communicate.
- **Human Machine Interface**. Communication between the user and the machine.

In addition to these interfaces, the TETRA network, as mentioned above, can be connected to other networks through the *gateways* defined in each of the external networks.

4.2. Technical characteristics

TETRA is a communications platform that allows voice and data transmission, which together with the connectivity features it offers, represents a very advanced level in terms of PMR technology.

4.2.1. Fully digital system

As a first technical feature, TETRA is a **fully** digital system, capable of providing voice systems with a low error rate and high quality. In addition to this service, TETRA allows the transmission of data, either circuit-switched or packet-switched, allowing the operator to configure its transmission speed to adapt to the characteristics of the network and reduce possible errors as much as possible.

4.2.2. Time Division Multiple Access

TETRA employs **Time Division Multiple Access** (TDMA) with a capacity for four user channels. These channels are interleaved on a single carrier, with a carrier spacing of 25 kHz. This has a very important implication: Carrier spacing and TDMA provide excellent frequency spectrum efficiency. In addition, **only one radio unit is required for every four user channels.**

Although each channel can be occupied by one radio, in cases where a **very high data transfer rate** is required (maximum limit of approximately 28.8 kbits/s with basic technology), **it is necessary to be able to reserve all four channels,** thus achieving a high bit/s transfer rate.

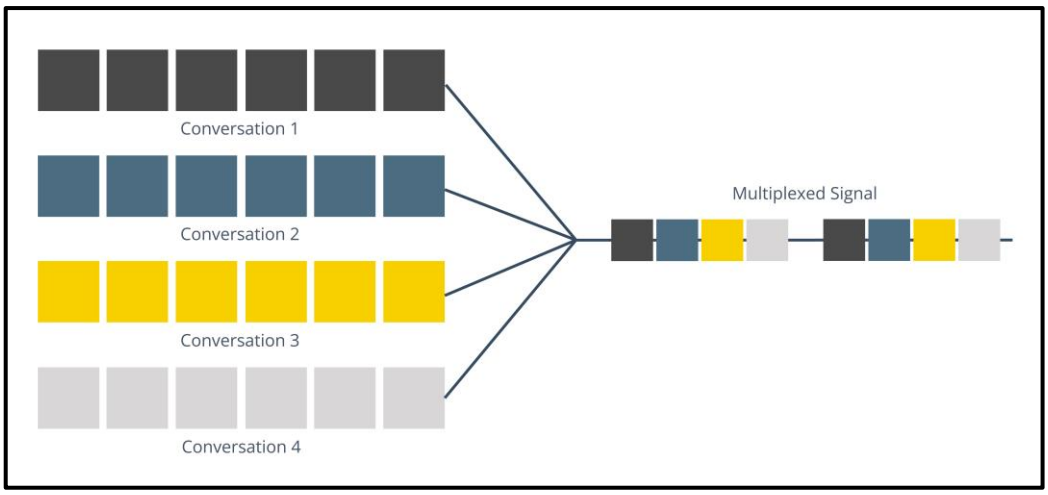


Illustration 3: Four user channels multiplexed into one 25 kHz channel

The use of four multiplexed channels, combined with the design of TETRA as a trunked system, has allowed, as can be seen in the following illustration, different organizations or entities to share and operate independently in the same environment in a secure way (if configured correctly), maintaining privacy and with optimal communication quality.

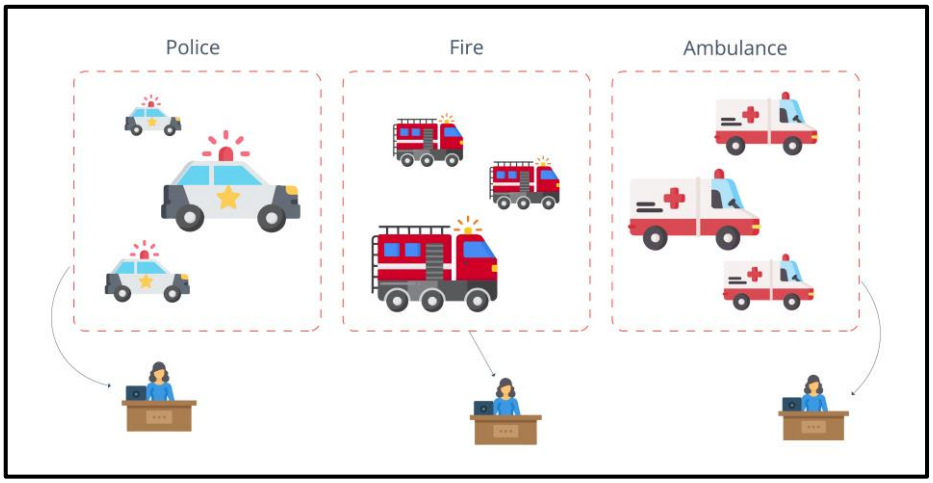


Illustration 4: Virtual interconnection within the same TETRA network[4]

4.2.3. High functionality

Another of the technological functionalities provided by TETRA is to maintain the high functionality of the network with an efficient use of resources, **thanks to the virtual interconnection carried out internally in the network**.

4.2.4. Set-up times and frame structure

This is one of the most important qualities of TETRA and the one that provides a differential advantage over other digital radio systems for emergency communications. The application of TDMA systems allows TETRA to have a **very low settling time** of about 300 ms, which, as mentioned above, is crucial for public safety and emergency services. TETRA allows both **duplex operations** for individual calls and **half-duplex operations** for group calls.

As for the frames of the TETRA structure, it **has four time slots per TDMA frame**. Subsequently, it is organized into eighteen TDMA frames per multiframe. In operations that transmit voice and data in circuit mode, the traffic of an eighteen-frame multiframe is compressed to seventeen TDMA frames, allowing the eighteenth frame to be used for control signaling without interruption of data flow. **This is called the control frame and provides the basis for the associated slow control channel or SACCH**.

In summary, the SACCH is able **to provide background control channel signaling** that is always present, even when all channels are assigned to traffic.

4.2.5. Connectivity and telecommunications servicies tetra

TETRA facilitates connectivity with other networks thanks to the features implemented in its standard. A TETRA network is capable of connecting to public and private telephone networks, to other data networks and to management and control systems.

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

The great advantage provided by TETRA, as can be seen in the following illustration, is that the use of a TETRA device can allow access to any system connected to the network without the need for converters or other linking devices.

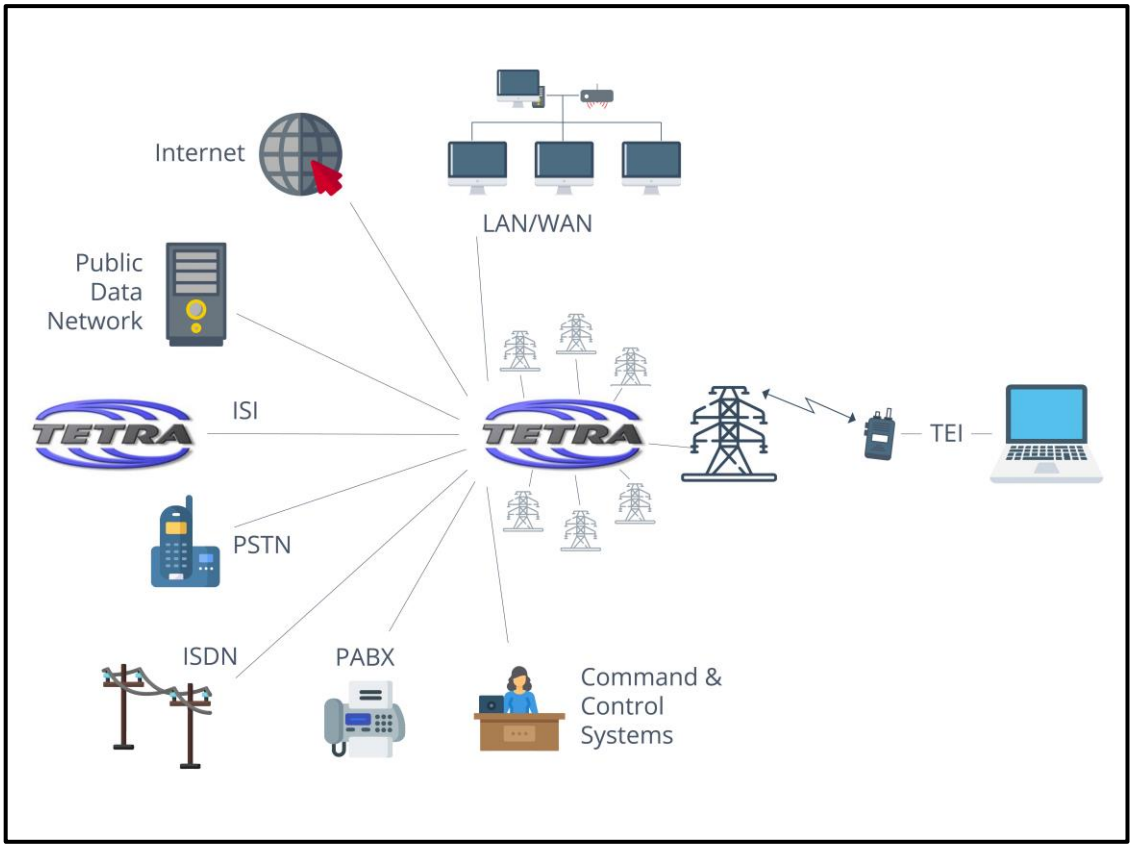


Illustration 5: Connectivity in TETRA networks[5]

Connectivity combined with bandwidth makes TETRA a superior platform for data application development.

As for telecommunication services, they can provide full spectrum communication capacity between users and terminals. In the **TETRA standard, it is established that communication teleservices cover all voice communication services**, in addition, it is also indicated that a bearer service must provide communication capacity between terminal network interfaces.

For example, suppose a TETRA network is installed in an offshore refinery. For this type of industry, it is of utmost importance to use devices that have the APEX directive approved, since any device that fails to comply with these measures may pose a risk to the infrastructure. In this aspect, TETRA devices (with APEX directive in order), which are oriented to communications within the infrastructure itself (being the case of a private company) but thanks to the interconnection with other networks, can allow operators to make calls via telephone in exceptional cases where necessary, thus reducing the risk that could involve using a base mobile device.

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

5. Combination of private and public sector together with TETRA networks

The great usefulness of TETRA networks in communication issues makes them one of the main means of communication for environments where some privacy in communication is needed. There are many TETRA networks around the world, but at this point we will focus on the main networks that can be found throughout Spain, dividing them by autonomous communities. The purpose of these TETRA networks can be for both public and private companies.

The data in these sections do not reflect the current situation of the sectors, due to confidentiality, system protection and the fact that most companies that use TETRA networks are companies in critical sectors, so data prior to 2019 will be used and do not fully reflect the TETRA situation in Spain, although it is similar.

5.1. Private Sector

There are **about 50 TETRA networks**, which can be found in companies such as:

- Airports:
  - Ibiza Airport
  - Malaga Airport - Costa del Sol
  - Alicante - Elche airport
  - El Prat airport in Barcelona, where more than 1,600 terminals were installed.
- Ports:
  - The port of Valencia
  - The port of Gandía
- Trains:
  - The Madrid train
  - The Valles train and the Llobregat-Anoia line
  - The train of the Basque Country (Euskotren)

An example of these aforementioned networks, being one of the largest we can find in Spain is that of the Valencia Port[6], which in 2018 spent a total of 54,450€ on TETRA elements, which are divided into the following equipment:

- 37 units Motorola MTP3250 handheld tetra 280-430 MHz --> includes 1 standard TETRA/GPS antenna, 1 high capacity 2150mAh battery, belt clip, side shield, accessory connector.
- 37 units Motorola dual tabletop charger base
- 37 units Motorola MTP3250 enable GPS Feature --> License activation.
- 2 units Motorola MTM5400 TETRA base radio with handheld microphone
- 2 units High performance UHF TETRA collinear 3dBd antenna

[6]https://contrataciondelestado.es/wps/wcm/connect/2b8767f8-c39f-46e6-84bb-31f134367a51/DOC2021010412493048-05540-Contrato.pdf?MOD=AJPERES

- 2 Motorola MTM5400 radio + antenna installation and commissioning
- 39 radio terminal configurations.
- 1 radio terminal discharge in TETRA DIPC system and positioning system.
- 1,095,050 divided in 2 installments, the first installment for a maximum of 9 months for the installation of the systems and the following 36 months for the maintenance of the different elements.

As we have seen, TETRA networks are common in the private sector, especially in companies that require fast and effective communication for any unforeseen event that may occur with the main network.

5.2. Public sector

In the public sector, the TETRA networks found are used for other types of services, mostly for the following three types of services:

- Security servicies.
- Rescue services.
- Medical services.

The following illustration shows a visual map showing the base stations in each autonomous community:

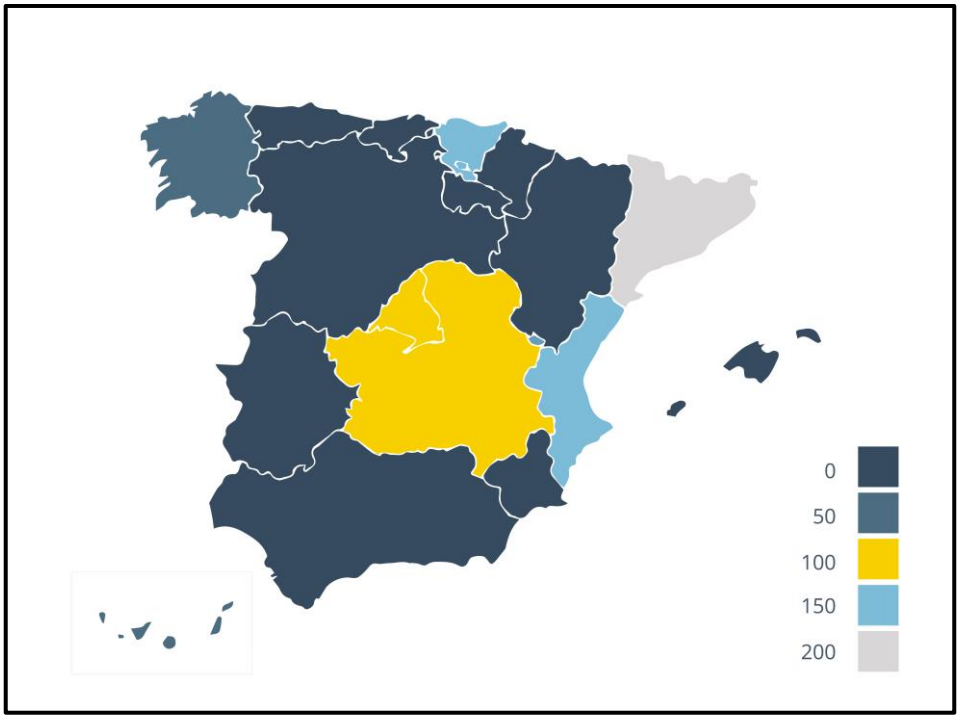


Illustration 6: TETRA network base stations in Spain

In addition, in order to have a better understanding of the magnitude of TETRA networks in Spain, below is an assessment of the number of users by terminals in different autonomous communities, as well as whether they use TETRA, EDMR or analog technology.

Comunidad Autónoma	Tecnología	Nº Usuarios
GALICIA	TETRA	7500 terminales
CATALUÑA	TETRA	No se especifican
CASTILLA LA MANCHA	TETRA	1500 terminales
CASTILLA Y LEÓN	ANALÓGICO	-
ARAGÓN	TETRA	209 terminales
EXTREMADURA	EDMR	Aproximadamente 1000 terminales
CANTABRIA	ANALÓGICO	-
ASTURIAS	ANALÓGICO	-
CANARIAS	TETRA	5000 terminales
BALEARES	TETRA	1500 terminales
VALENCIA	TETRA	Aproximadamente 8200 usuarios
NAVARRA	TETRA	Hasta 3000 terminales
MADRID CANAL ISABEL II	TETRA	Inicial 10000 usuarios, ampliable hasta 15000
MURCIA	TETRA	1700 terminales
PAÍS VASCO	TETRA	2500 emisoras
LA RIOJA	DMR	500 terminales
ANDALUCIA	DMR	7000 terminales

Illustration 7: Terminals by Spain communities[7]

[7] https://www.juntadeandalucia.es/contratacion/document/download?refCode=2022-0000045331&refDoc=2022-0000045331-2

6. Security threats in digital radio networks

As in any network, the possibility of a security breach is always present. Specifically in TETRA networks, the same protocol structure is used as in an IP network, therefore, the vulnerabilities presented in any IP network are also present in TETRA architectures.

6.1. Vulnerabilities in operating modes and architecture

In order to explain some of the vulnerabilities, let's take a quick look at what operations can be performed and how TETRA network architectures are designed.

The TETRA system consists of ***Base Stations*** (**BS**), which are infrastructure elements dedicated to management and switching with air interface. Communications are made through the air interface to mobile stations, to other networks through gateways, with an intersystem interface with other TETRA networks and with terminals or mobile stations (**MS, *Mobile Station*).**

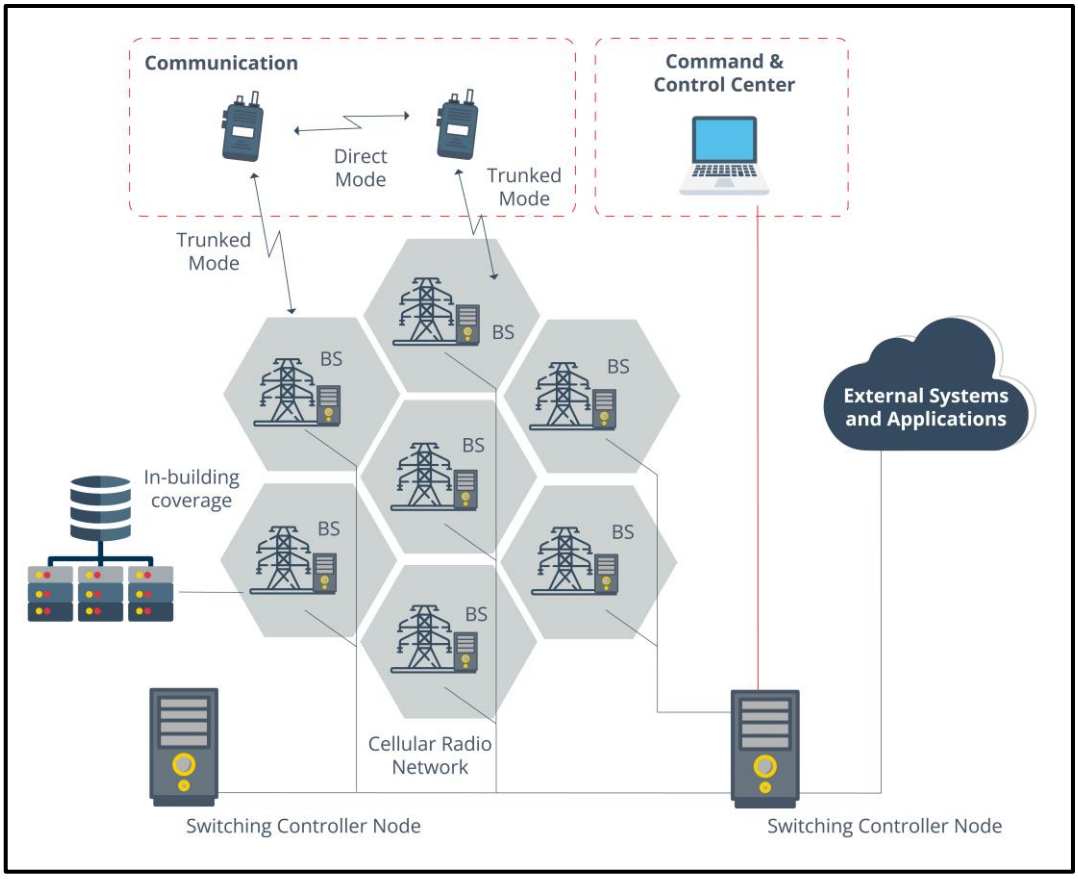


Illustration 8: Architecture and modes of operation[8]

[8] https://personales.unican.es/perezvr/pdf/TETRA-UC_13_7_2010.pdf

BSs forward information from an MS to the requested receiver. These base stations interact with another base station controller (**BSC, *Base Station Controller***), which in turn will communicate with a mobile switching center (**MSC, *Mobile Switch Center*)**. The MSs will be able to communicate with each other, even when they are out of range of a base station.

Tetra has three modes of operation or data transmission:

1. **V+D (Voice plus Data):** Grants the possibility of switching the type of switching between voice and data or using both at the same time.
2. **DMO (Direct Mode Operation):** Communication between two mobile stations even if they are out of range of the base station.
3. **PDO (Packet Data Optimized):** Only allows data transmission.

As mentioned above, the architecture or protocol stack of the TETRA Air Interface is like that of the IP protocol, therefore, it is susceptible to attacks. Within this protocol stack in TETRA, there are three layers:

- **Physical layer:** It allows to have control of the most important radio characteristics, among which we can find modulation and demodulation, as well as synchronization. This layer uses TDMA with four time slots as described in previous sections. In addition, it uses a DQPSK pulse *shaping* modulation scheme with a 25 kHz radio channel and 36 Kbps channel rate. In certain TETRA implementations, the use of FDMA is allowed.
- **Link layer:** The data is organized in two L2 frames. It is further divided into two sublayers with different functionalities. The first part LLC (Logical Control Link) is responsible for data transmission and retransmission. On the other hand, the MAC (Media Access Control) whose function is to control channel access, channel coding and decoding, *interleaving, routing* and multiplexing.
- **Network layer:** It is divided between a user plane in charge of managing voice and user data and a control plane used to manage signaling and control data. It also has the function of controlling network procedures.

These layers may present different vulnerabilities of a general nature, like those of any other communications network, as well as the vulnerabilities inherent to the IP protocol.

In certain cases where the configuration is wrong or the correct security levels have not been established, an external agent could perform a low complexity attack on the logical channels that represent the interface between protocols and the radio subsystem, since they are one of the sensitive points in the communication. Information between the upper and lower MAC level is passed through logical channels where specific information from one or both directions can be passed.

As TETRA uses TDMA to access the channel, several users can share the same radio frequency, but in different time slots, so an attacker could take advantage of a misconfiguration to access those time slots and obtain that information.

6.2. Vulnerabilities in TETRA encryption types

Eavesdropping is one of the major problems in radio communications, which, together with *sniffing* and traffic analysis, makes the implementation of security measures almost a mandatory requirement.

To prevent eavesdropping by external agents, TETRA allows the introduction of AIE (*Air Interface Encryption*) and E2EE (*End to End Encryption*) as mentioned in the following section. *7 Security functionalities in TETRA devices*.

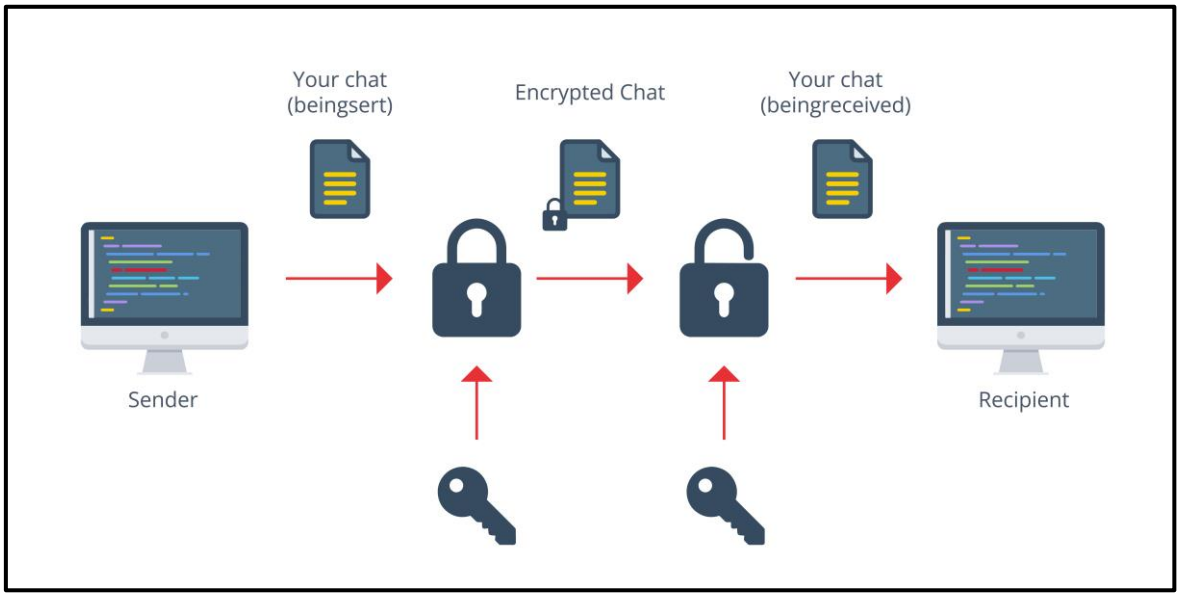


Illustration 9: E2EE Encryption[9]

AIE protects against eavesdropping by protecting signaling, identities, voice and data. One of the disadvantages of using this method alone to reduce costs is the possibility of *sniffing* data within the network, which is solved by end-to-end encryption.

Like AIE, E2EE also has vulnerabilities when it comes to end-to-end encryption, since it is only implemented on the traffic channel, but not on the control channel, hence the need to implement it together with AIE.

[9] https://www.gizlogic.com/zoom-e2ee-encriptacion-extremo-a-extremo/

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO DE TRANSFORMACIÓN DIGITAL
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

7. Security functionalities in TETRA devices

TETRA seeks to guarantee greater security, providing different protection measures, always trying to ensure:

- **Authentication** of users for access to the network by radio terminals, through the possibility of establishing an **authorization** system**,** which will be granted by the administrator, allowing access to the corresponding communication.
- **Confidentiality** of communications, thanks to the incorporation of air-to-air encryption (between terminal and base station) and mechanisms that prevent message decryption at intermediate communication points.
- Information **integrity**, thanks to the incorporation of a wide range of security controls (back-end security, mechanism to prevent unauthorized use of dispatcher software, access detection controls, monitoring technology, etc.).
- Finally, measures can also be implemented to ensure **availability** and **non-repudiation.**

The following are the different **security functionalities present in TETRA networks to protect the information transmitted by their users** (be it voice traffic, user data or other information related to user identities and operations).

- **Security mechanisms:** Autonomous functions capable of ensuring a specific security objective. Among these functions we can find the confidentiality of the information, or the authentication of the terminals used in the communication.
- **Security management functions:** This range of functions is used to manage, operate and control the security mechanisms implemented individually. Their main function is to make the security mechanisms of different networks interoperable. Key management between devices is one of the functionalities present in TETRA networks, allowing the implementation of the protection measures mentioned above, specifically the authentication measure.
- **Standard cryptographic algorithms:** Different specific mathematical functions used for the creation of cryptographic keys that allow an adequate level of security, without hindering interoperability between systems.
- **Lawful interception mechanisms:** Functions used to ensure lawful access to information.

On the other hand, TETRA implements the following additional security measures:

- **Air Interface Encryption (AIE):** Able to protect voice traffic, signaling and identity on the radio communication (air) leg. It should be noted that in addition to protecting transmitted voice, SDS messages and packet data that may be transmitted, air interface encryption can also protect all voice and data headers, signaling, identity registration and user anonymity, and finally, attack response.
- **Disabling or "death" of a terminal: This** makes it possible for different lost terminals not to be a threat to the global security of the network.

- **End-to-End Encryption (E2EE):** Protects all data and signaling along the entire communication path, from one Endpoint to another Endpoint, including passage through the system.

These measures or implementations are proposed by TETRA, the use of the network does not imply the need to implement these measures, but they are recommendations, and their use depends exclusively on the end user.

In the following, different security implementations available in TETRA networks will be detailed.

7.1. Mutual authentication with the air interface

One of the main keys of the TETRA standard is that it supports mutual authentication of an MS and the network. This network is often referred to as the Switching and Management Infrastructure (SwMI).

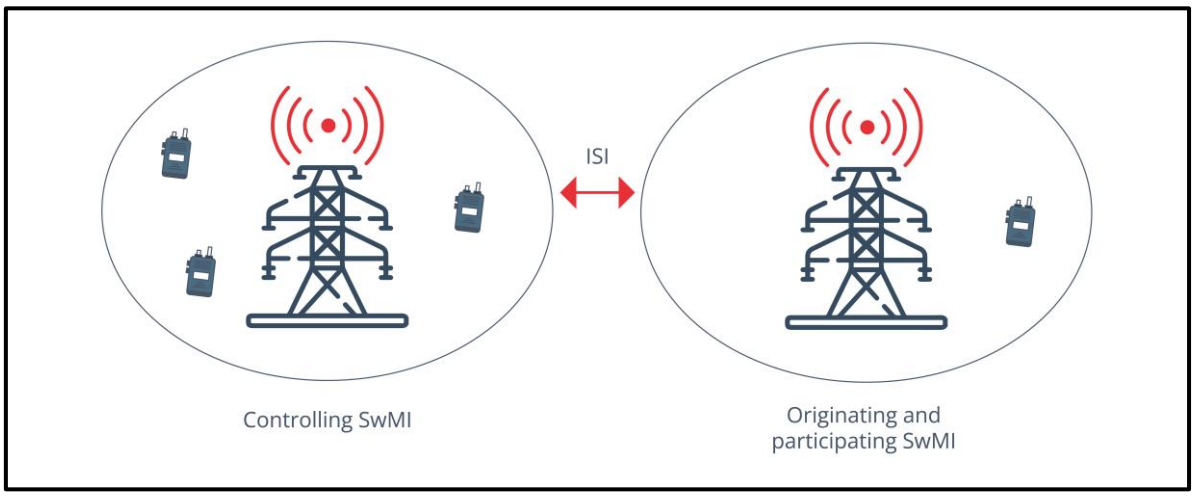


Illustration 10: SwMI architecture[10]

Access control provides a firm basis for security in general. In addition, it offers the following possibilities when implemented in a communications architecture:

- Correct access from a public place to the communications network by the MOH and to the services that the network may provide.
- Implementation in the system of the derived encryption key (DCK) and single session key encryption to guarantee confidentiality in the transfer of information and ensure optimal authentication.
- The derived encryption keys are shared between the different stations.
- Creation of different secure distribution channels for the transmission of information.
- Exhaustive control of the activation and deactivation of an MS.
- Control that the MS are legitimate and must be able to connect to the network.

The mutual authentication mechanism (network and mobile station) is available for both voice and data and, in addition to the features shown above, it should also be noted that the use of the authentication key K (independent for each MS/SIM) implies that the K will

[10] https://www.researchgate.net/figure/Scenario-2-Originating-and-controlling-SwMI-are-not-collocated_fig10_275270770

be stored both in the MSs and in the network. This storage is done in authentication centers or AUCs.

It also has the ***Direct Mode Operation*** **(DMO)** function, which does not have an explicit authentication, since the different mobile stations do not share the keys with each other, unlike the mutual authentication. To make up for this security gap, Static ***Cipher Keys*** **(SCK)** are implemented, which can provide implicit mutual authentication using a single set of standardized algorithms.

7.2. Encryption of communications in the TETRA network

As mentioned above, the air interface has its advantages and disadvantages, one of the most important cons being the possibility of an external agent eavesdropping on communications between *Endpoints.*

Currently, communications between wireless mobile devices require a minimum level of security for communications over the air interface. With this, different security measures are sought to ensure the connection between the MS and the network. In the case of these mobile devices, security is usually implemented and only the security of the air interface is sufficient.

In the case of TETRA networks, where a high level of security is required, it is very common to implement additional security measures to increase the base level of security of communications between MSs, and between MSs and the network. Security is no longer only required at the air interface, but also within the network. The implementation of end-to-end security provides minimum values to ensure the integrity of the system by encrypting communications.

The different types of encryptions and their uses in a TETRA network are explained below:

- **Air interface encryption:** This option allows the user the possibility to encrypt voice and data, using different encryption algorithms that allow customizing the security level according to the user's needs. The ability to encrypt over the air interface between the MS and the SwMI is available for both group and individual communications.
  Encryption of the air interface is extremely important as it provides a high level of security for both speech and data transmitted between MSs. On the other hand, signaling encryption provides protection against traffic analysis, thus minimizing the chances of an agent outside the communication being able to decipher who is communicating with whom and from which areas they are communicating.
- **End-to-end encryption:** TETRA is characterized by having different variables in its end-to-end service, allowing the end user the ability to customize the encryption, to further adapt it to their requirements. This allows different user groups, depending on their security level (security in the military field is not the same as security in the healthcare field) to have the possibility to customize the end-to-end encryption to the maximum according to their own requirements.
- **TETRA Association end-to-end encryption framework:** Although TETRA allows for a high level of customization in end-to-end communications depending on the level of security required, the TETRA Association has implemented standardized solutions that mean that end users (even those with high security requirements on one end-to-end encryption parameter) do not need to specify the rest of the end-to-end system features.

The *Security and Fraud Prevention Group* (SFPG) of the TETRA Association created Recommendation 02 to specify at the highest level all the features necessary for the end-to-end service to be correct, in addition to specifying in detail the cryptographic algorithms and how they are to be implemented.
The first implementation used the International Data Encryption Algorithm (IDEA). Later, in a second implementation, the Advanced Encryption Standard (AES) was added, although there is no standard algorithm defined by the SFPG, the following are commonly used:

- **AES-128:** Adopted as the default TETRA encryption algorithm.
- **AES-256:** It is starting to be implemented by some terminal manufacturers as it provides a higher level of security when a high level of confidentiality is required.

These algorithms are often superseded by the implementation of public domain algorithms with similar characteristics but more customized and fully valid for the end-to-end encryption of a communication in the TETRA network.
The use of public domain algorithms is based on the availability of MS and multi-vendor key management solutions. Overall, the framework has been designed to accommodate a variety of security policies, and flexibility is achieved through several simple operational options. Copies of the recommendations are available from the SFPG Secretariat[11].

- **User anonymity:** The TETRA standard allows not only communications between users to be encrypted, but also, incorporates different mechanisms to ensure the anonymity of users who are transmitting data or voice over the network. Dynamic encryption can be implemented to encrypt individual and group user identities. In addition, the "dynamic" feature provides the ability to encrypt in different ways at different times to the same user, thus ensuring user integrity.

7.3. Security Management Functions - Encryption Keys

Although TETRA networks involve the use of security features built into the system, this does not guarantee that the system is totally hardened, although it does limit where vulnerabilities may exist.

Security management in TETRA networks, in general, is concerned with ensuring that security functions are properly managed, but also that the different mechanisms are properly integrated and that interoperability between TETRA systems in a secure manner is effective.

One of the vulnerabilities of TETRA networks is the management of security keys, which contain the secret information that will be used to access the system or to decrypt encrypted information. The management of these keys is as important, if not more so, than any other security mechanism implemented in the network. According to the TETRA Association SFPG[12], functionality and flexibility are key words when it comes to key management, as well as in the end-to-end encryption framework, where it has developed different recommendations to support security management, especially key management.

[11] https://tcca.info/members_pages/sfpg-recommendations/

[12] https://tcca.info/members_pages/security-fraud-prevention-group-sfpg/

In the following, different types of keys and their functionalities in the use of TETRA networks will be detailed:

- **Authentication key:** The authentication key K, is the key used for mutual authentication between an MS and the SwMI. The TETRA standard defines in its standard three possibilities for generating this key: a function for a fixed user of an authentication key, the possibility for a user to enter an authentication code and a combination of both. In addition, in most systems, an MS is required to store the K-key or UAK key, due to the difficulty of certain systems in storing keys with long codes.
- **Keys for air interface encryption:** In this regard, there are different types of encryption keys. The keys can be sent via the air interface to the MSs with *Over the Air Re-Keying* (OTAR), directly in the authentication process or pre-loaded in the MSs.

  These keys can have different ranges of life, both long and short term, being possible to introduce mechanisms to protect keys with a very long lifetime.

  Within the air interface encryption keys are the following specific keys mentioned above:

  - **Derived Cipher Key (DCK):** Enables encryption between the network and the MS individually. The derivation is performed during the authentication process. The aforementioned feature also implies that, during a voice call, in communications from the MS to the network (downstream) or from the network to a mobile station (upstream), an implicit authentication can be provided.
  - **Common Cipher Key (CCK):** Generated and distributed by the SwMI. It is encrypted by the DCK to each of the mobile stations. When the common encryption key is distributed to a mobile station via the air interface, the aforementioned OTAR process is used. In addition, the CCK is encrypted with the DCK of the MS itself. This type of key is very common for distributed MS groups or for location areas (LA).
  - **Group Cipher Key (GCK):** This key has its binding associated to a very specific user group. As with CCK, for GCK, the key is generated by SwMI and distributed to the MSs in a group. In the same LA, the GCK is combined with the CCK to achieve a special and specific algorithm called "Group Specific Key" or MGCK which is used to encrypt the messages of the previously created group. In a more specific case, where the GCK is distributed to an MS over the air interface using OTRA, the communication would be encrypted with a session key derived from the authentication key for that MS.
  - **Static Cipher Key (SCK):** This key is the default key of the TETRA network if encryption is used. It does not require prior authentication.

    The significance of the static rating is that its value is not modified by any other security mechanism. TETRA allows the use of up to 32 SCK keys in the same MS, which makes a large number of communications possible. SCK is compatible with group systems and with systems using DCK and CCK as alternatives.

    In case a direct mode or DMO communication is being used, SCK keys could be grouped with several user groups.

The use of these keys is at the discretion of the end user. Misuse of any key could allow an external agent to attack the TETRA network.

7.4. Security classes in a TETRA network

TETRA provides the following security classes to classify the encryption security of the air interface:

Class	Encryption	OTAR	Authentication
1	No	No	Optional
2	Static key	Optional	Optional
3	Dynamic key	Required	Required
3G	Dynamic key	Required	Required

Table 2Security classes in TETRA networks

- **Class 1:** This class is the most insecure of all and does not provide the possibility of any type of encryption or *Over the Air Re-Keying*. It only allows the option of including an authentication mechanism.
- **Class 2:** SCK keys (up to a maximum of 32) are loaded on all terminals in the network. They are usually stored either for a long period of time or for life. This class always operates in the before mentioned Direct Mode or DMO service. This class is also used when implementing a base station working in isolation.
- **Class 3:** Involves dynamic keys (DCK), which are automatically generated from the terminal's internal key with each authentication and are used individually in communications between terminal and base station. The "downstream" communication is encrypted with the CCK key, which has been previously loaded over the air (OTAR).
- **Class 3G:** This class is like Class 3. Its only difference is that it can be applied for groups, so the DCK key is still used for upstream communications, the CCK key for signaling and the GCK key for each group. As in Class 3, the keys are loaded with OTAR.

To get an idea of the security of Class 3 air interface encryption, the keys are approximately 80 bits long, which allows the network to generate up to 1.2x10^24 keys. This means that, with current mechanisms, it takes approximately four million years to decrypt a key.

7.5. Disabling of TETRA terminals

Disabling a terminal in case of loss or theft is a crucial security measure, as a lost terminal can pose a security threat to the integrity of the TETRA system.

TETRA allows thanks to this option:

- Termination of the terminal's activity as a radio.
- Permanent deletion of keys, including the secret key that enables device authentication.
- The "Temporary Disable" option deletes the traffic keys but allows a short-range ambient listening.
- A rapid response to device loss or theft.

This process of disabling TETRA terminals is subject to the export control that will be explained later, but for which every manufacturer must request permission to export a device that has this option within the system.

7.6. Standard cryptographic air interface encryption algorithms

TETRA is a standard capable of providing different cryptographic algorithms for different purposes, although it also allows the non-use of some of these algorithms to create an unsecured network. There are different recommendations for the creation of TETRA networks to have a minimum-security level depending on the functionality of the network.

In addition to the ciphers available for the air interface, TETRA also supports alternative algorithms created by independent and external users. These algorithms will only be valid if they meet minimum requirements imposed by TETRA and provided that the end-user agrees to use such algorithms to the detriment of losing support from different vendors.

TETRA considers several requirements to specify the standard algorithms, among these requirements can be highlighted:

- **The need for diversity:** with many TETRA applications and networks, there is a possibility that not all users of the standard may want to publicly share encryption algorithms, so that in certain cases, such as different European Public Safety Organizations, a proprietary standard air interface encryption algorithm, different from any standard algorithm, is required. This ensures that the encryption is totally independent of any other association, providing a substantial increase in the security of the network if encrypted.
- **Export control regulations:** Most devices that include encryption algorithms are subject to country-specific export controls. According to the Wassenaar Arrangement, in Category 5[13], Part 2, the entire cryptography control policy for major industrial countries can be reviewed.

  In TETRA, there are four standard encryption algorithms for single architecture systems. These algorithms have been developed by ETSI's Security Algorithms Expert Group (SAGE).

- **TEA1**: Generally this algorithm is intended to be exportable outside Europe, which has generated a great affinity for different Public Security entities in several countries, as well as for many private sector companies, which require an important level of security.
- **TEA2**: Its use is only allowed in Public Safety organizations in Europe and therefore, they have a very high export control.
- **TEA3**: Used for Public Security and Military Organizations in different places where TEA2 is not allowed (outside Europe). It also has a very restrictive export control, although its use is allowed outside Europe, in certain very specific cases.
- **TEA4**: It is designed for use in areas outside Public Security. Its use is minimal, being the least used of the above mentioned algorithms.

[13] https://www.boe.es/buscar/doc.php?id=DOUE-L-2001-80554

These algorithms are export restricted and are controlled by the regulations defined in the aforementioned1998 Wassenaar Arrangement[14]. These algorithms are all proprietary to ETSI except for TEA2.

It should be noted that these algorithms are highly resistant to attempts to break them, but advances in technology can bring with them new ways of overcoming this resistance and breaching encrypted data. In any case, attention should be paid to the configuration of the systems and the encryption used, trying to customize the security configuration as much as possible with the architecture to be used.

[14] https://www.europarl.europa.eu/doceo/document/E-4-1998-4065_EN.html?redirect

8. Security requirements for enterprise applications

With the above mentioned, regarding the security functionalities and capabilities provided by TETRA, it should be noted that most of the existing TETRA networks are from the IT world, since for OT environments the security functionalities are minimal.

Throughout this section, reference will be made mainly to the OT world and the implementations and security requirements for this sector.

It must be remembered that each OT installation is a world, so it is important to investigate our network and observe what may or may not be convenient to disable. It is suggested to activate at least class 2 security in the industrial network, previously explained in the section "Security classes in a TETRA network", with authentication of the active elements together with the possibility of disabling the terminals and the possibility of encryption in the air interface.

The network must be segmented according to different industrial standard concepts, such as **PERA** (*Purdue Enterprise Reference Architecture*), grouping and isolating the assets, as well as controlling the communication flow between them.

The information sent by the devices at the different layers corresponding to levels 2 and 3, i.e., link and network, will be encrypted.

The segmentation of the different users that we can find within our TETRA network should be done looking for the separation between groups, but also the possibility of connection between them if necessary. We will create groups for the different workstations, i.e. a group for cleaning, another for technicians, etc., and, within them, we will create another group to differentiate between workers, authorized personnel, calls of high importance, etc.

In addition, access control to the medium will be performed. For this purpose, some of the techniques known for telecommunications presented below will be used:

- **ALOHA:** Designed by the University of Hawaii as a radio-link access method in 1970, currently in disuse. Its main feature has been *Free for All*, i.e., if a station has a frame to send, it sends it directly. The medium is shared by all stations. Other features are:
  - nodes use a shared channel.
  - if transmissions overlap, they collide.
  - the destination node confirms the correct frames.
  - if a node does not receive the ACK confirmation, the connection is determined as a *timeout* and the frame is assumed to have collided.
  - if no ACK is received, the frame will be resent a limited number of times.

  As ALOHA has only a single channel to share, there are possibilities of collision between frames from different stations. In the following example, 4 stations are shown sending 8 frames in total, of which only 2 frames survive:

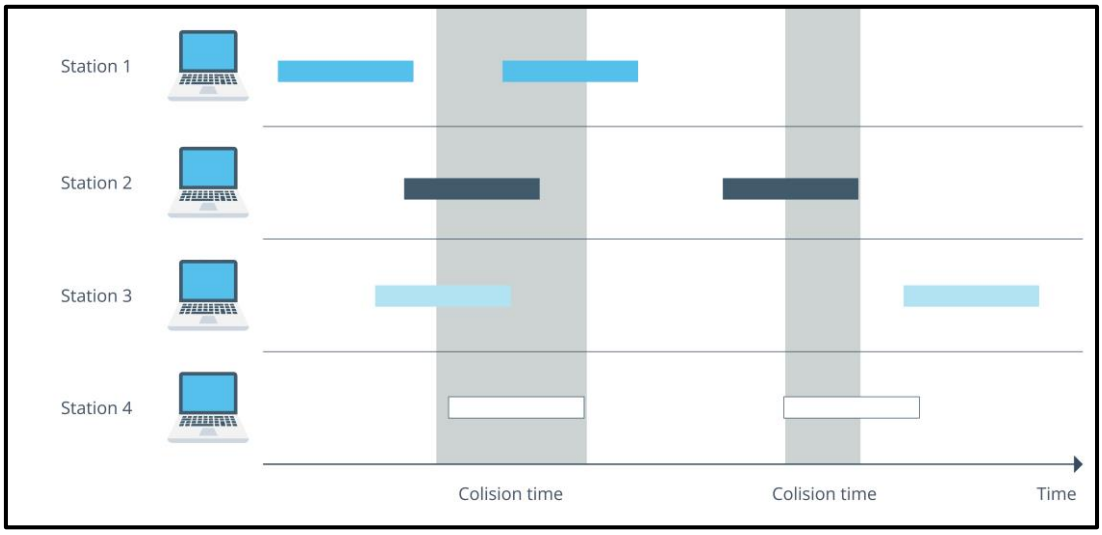


Illustration 11: Sending frames with the ALOHA protocol[15]

In it, the following results can be observed:

- there are four stations trying to transmit.
- each station has sent two frames.
- Specifically, six plots conflict and only the first plot of the first season and the second plot of the third season survive.
- conflicting frames should be forwarded.
- even if a single bit of the frame coincides with the collision duration time, the frame will collide and must be resent.

To eliminate the frame forwarding process and improve communication, the Slotted ALOHA was designed and implemented, which avoided collisions between frames by defining the sending times.

- **CSMA:** CSMA or *Carrier Sense Multiple Access* is a medium access protocol that reduces the probability of connection, thus increasing communication performance. This is because the stations listen before transmission, to know the channel status and whether they can transmit, thus reducing the probability of collision, but not eliminating it completely, due to the propagation of the signal in the shared medium over space and time.
  Within CSMA there are three persistence modes as shown in the following image:

[15] https://redes.umh.es/RC/RC-Slides-U4.pdf

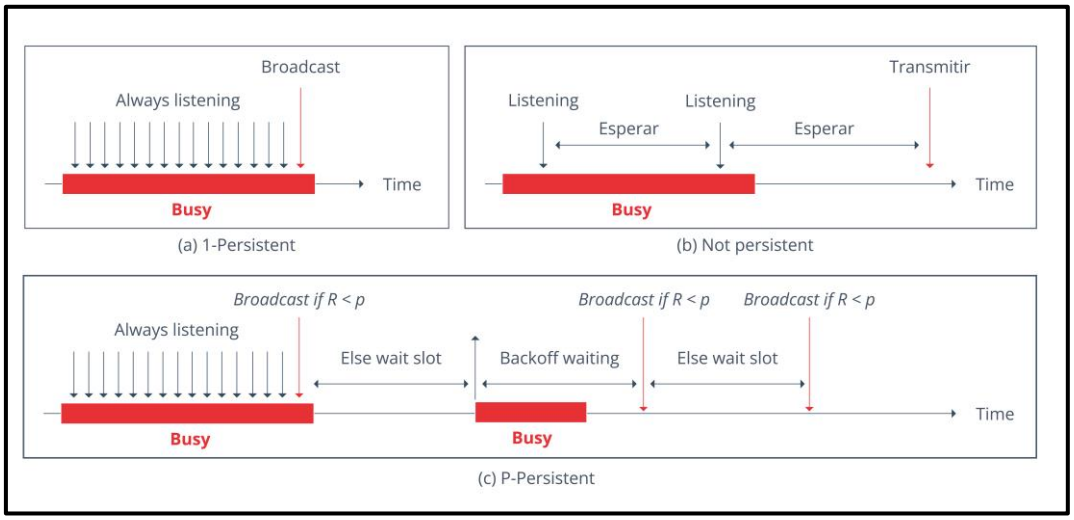


Illustration 12: Types of persistence in CSMA[16]

In addition to the features defined above, CSMA enhances its performance by means of protocol variables, such as the following:

- **CSMA/CD**: *Carrier Sense Multiple Access with Collision Detection,* is a variant of the protocol that defines the process to be followed in case of collision and listens after sending frames to see if the transmission has been successful. In addition, to improve transmissions, CSMA/CD has a frame size restriction.
- **CSMA/CA**: *Carrier Sense Multiple Access with Collision Avoidance,* is another variant of the protocol focused on wireless networks.

- **FDMA:** FDMA or Frequency Division Multiple Access is a multiplication technique used in multiple communications protocols. This protocol controls access to the medium, which is done by dividing the available spectrum into channels, which correspond to different frequency ranges, assigning these channels to different users and communications to be carried out, without interference between them. Among its most relevant features, we find:
  - easy implementation in radio systems,
  - rigid resource management and unsuitable for variable traffic flows,
  - need for an antenna duplexer for duplex transmission,
  - individual channel assignment per user,
  - demand-dependent allocation.

- **TDMA:** From its acronym *Time Division Multiple Access***,** this protocol represents Time Division Multiple Access and is the most widely used protocol in TETRA. This protocol has already been explained in detail in section *Time Division Multiple Access*. It consists of time division multiple access, which allows multiple conversations sharing the same radio channel, this being one of the main features of TETRA. If you want to know more about Digital Mobile Radio or about the

[16] https://redes.umh.es/RC/RC-Slides-U4.pdf

operation of TDMA you can get that information in the article "Digital Mobile Radio in Industry 4.0"[17].

[17] https://www.incibe-cert.es/en/blog/digital-movile-radio-industry-40

9. Real security functionalities

Throughout this section some real functionalities of TETRA devices will be explained and defined, since the security functionalities defined above are theoretical possibilities granted by the standard, which not many devices have within their reach, or their implementation may imply a high purchase price.

This section will refer to the real security possibilities provided by the TETRA protocol for a specific radio (neither brand nor model is specified, due to security regulations). The actual characteristics of the device are detailed below:

- **TEI:** *Terminal Equipment Identity,* is a radio identification number, established by the company in charge of manufacturing the device and can never be modified. This feature provides secure device identification.
- **PIN/PUK *User Authentication*:** PIN (*Personal Identification Number)* and PUK (*PIN Unblocking Key*) are very common features in mobile devices, for authentication each time the device is turned on. In case of failure to enter the four digits of the PIN a certain number of times, the device will lock and request the PUK for user authentication.
  Both the code and the number of attempts are defined in the *codeplug* or configuration file.
- **Secure DMO:** This method allows the radio to communicate in direct mode with key encryption. When the SCKs are granted by the OTRA, the radio will indicate if it contains the correct keys, if not, it issues a message indicating 'OTRA incomplete'. This allows to know in a correct way if the direct communication is correct and secure.
- **Radio *Disable/Enable*:** This feature, which only some radios in TETRA networks have, allows a general controller to enable or disable the operation of the radio. In case the functionality is disabled, the radio will not be able to participate in any voice calls and will ignore all other services.
  There is a special case where, if the device is in deactivated mode, but receives a TETRA subscription with the correct SSI and MNI, the radio will revert to active status.
- **Radio *Permanent Disable*:** This feature allows you to completely disable a radio to, for example, protect the network from an attack from another radio or from the infected radio itself. It should be noted that if the *Permanent disabled* mode is enabled, the radio will become inoperable. This feature can also be used by an attacker to disable the different terminals one by one and cancel communications, which is why special attention should be paid to its configuration, and its functionality should only be activated by means of security keys.
- **SIM Security**: SIM Security consists of the following groups of security functions:
  - E2EE voice and related key management;
  - network access and authentication parameters;
  - key management for AIE;
  - OPTA, modification, encryption and transfer;
  - AES for E2EE SIM interface and SIM-terminal authentication.

  The SIM is an integrated circuit card that contains a file system and an application. The application performs the following actions:

- generation of key stream segments (KSS).
- synchronization for E2EE;
- TETRA authentication algorithm based on the SIM K-key;
- key management for E2EE keys.
- SIM interface encryption and authentication using AES.

- **High Assurance Boot:** The radio has a feature that ensures that the code and data displayed on the radio are authentic and have not been altered.
  - The *hardware* forces the HAB module to run at boot time.
  - the module checks if all *software* comes from a trusted source.
  - the radio checks the signature of the code segments and data present in the radio using a public/private key mechanism. If the HAB authentication of the *flashed software* fails, it does not allow the radio *software* to run.

10. Vulnerability mitigation

The TETRA infrastructures used in the industrial and transportation sectors were designed and deployed about twenty years ago and about fifteen years ago, respectively. At that time, the level of awareness of cyber threats was lower than it is today, in addition to the fact that there was no public availability of tools for security analysis and/or attacks on these networks, so the perceived risk was low. All this meant that, in order to simplify the implementation and the complexities associated with security management, not all the security features offered by the TETRA standard were taken advantage of.

Currently, these networks are in operation in critical applications in different businesses and sectors. Normal operations are perfectly functional, but it is not easy to apply the security measures presented in the previous chapter "Securing TETRA networks", which is why this operation could be affected, or even have a significant cost.

The implementation of a secure communications network, either by maintaining TETRA or by implementing one of its alternatives, is usually a long-term project that depends on a detailed impact and cost study (See *Combination of private and public sector together with TETRA networks* to quantify costs")

In this situation, there is the possibility of temporarily implementing some mitigating strategies, in which it is possible to maintain part of the infrastructure currently in use, while adding security functions with a low impact. These have been divided into: 'technical mitigations', those that affect the configuration of the technology itself; and 'operational mitigations', those actions that can be taken to minimize the impact in the event that the implemented TETRA system can be breached.

10.1. Technical mitigation

In most industrial networks, the integrity and availability of communications are considered critical, while **confidentiality** of communications **is not an essential** but **desirable functionality.**

In these cases, mutual authentication between TE and SwMI, using the authentication mechanism, should at least be used. This solution has the advantage that authentication is usually supported by all computers and networks, unlike TEA (*Tiny Encryption Algorithm*) 1/2/3/4 encryption, which usually requires specific licenses or has usage limitations. **Authentication will therefore be available without the need to replace equipment or upgrade licenses**. Significantly limiting the capacity for illicit interference in communications.

As a complement to authentication, or in those cases where for any reason it is not possible to apply it, it is possible to use the functionality of **blacklists** and **whitelists** of user equipment identity (TEI), so that the network only allows the association of allowed equipment. While the TEI can be modified by a sufficiently advanced attacker, in general, TETRA equipment usually has a unique TEI that requires lab-level tools and maintenance, not always easily accessible. In addition, the TEI identifier is less accessible than ISSI identifiers. Therefore, black and white lists can be an effective measure against less sophisticated attackers.

Those applications that require data confidentiality can opt for end-to-end encryption, for example, those that handle specially protected personal information, be it medical data or activities that must remain confidential, or the communications of security and surveillance personnel. This makes it possible to maintain a ***legacy*** network (integrated) without the need for changes or *downtime* (periods of maintenance or disabling of the services provided by the network), while at the same time giving critical user groups of terminals the ability to operate with encrypted groups, maintaining compatibility and interoperability in groups in the clear with the rest of the users.

It is also important to remember that a network that supports over-the-air encryption does not usually require encryption to be in use for all terminals and groups, but simply indicates that it supports encryption. This makes it possible to carry out a migration plan progressively, first by identifying the users that may require confidentiality, and then by providing the cryptographic keys and group encryption for these users.

In the uses of TETRA for OT network data transmission, such as SCADA, there are also several specific mitigations.

SDS-based applications should incorporate an **application-level encryption layer** based on robust, industry-recognized algorithms (e.g., AES), and with a secure implementation that provides both confidentiality and authentication, as well as protection against replay. This layer would also function as an end-to-end system, protecting from the PLC equipment to the SCADA controller. In this way, the information always travels encrypted, both in the air interface and in the SwMI network.

Applications that make use of IP data encapsulated over SNDCP (*Sub Network Dependent Convergence Protocol*) should also implement encryption, either by encrypting the payload in communications, or by using low-overhead VPN protocols, such as IPsec in Transport Mode.

10.2. Operational mitigation

Operational mitigation includes those working procedures that address the shortcomings of TETRA communication networks based on the way users use the technology. This allows improvements to be implemented without affecting software or hardware configurations, such as terminals or SwMI.

Operational mitigations respond mainly to three types of vulnerabilities, those affecting the **confidentiality** of transmitted information, those affecting the possible **integrity** of communications and those resulting from the loss of **availability** of communications.

10.2.1. Mitigations to the lack of confidentiality in TETRA networks.

Although as a rule most communications in an industrial installation do not require special secrecy, there are some situations where it is important to preserve the confidentiality of the information transmitted. When the TETRA network does not have air interface encryption or E2EE, some compensatory measures can be taken.

- **Use of agreed language:** This is a traditional procedure in open (analog) radio networks that makes up for this deficiency. It is especially practical in security communications, such as facility surveillance. **In agreed language, the designation of people, common locations and everyday situations is encoded**

by means of pre-agreed and commonly used code words. In many cases even these procedures remain in use in TETRA networks for historical reasons or because it provides a formal and unambiguous language for professional communications. In this way, occasional eavesdropping limits the use that can be made of access to communications. In an example of agreed language, a guard who has just returned from his perimeter patrol to his static guard post could be coded using agreed language as "Oscar-3 goes to Blue situation at Mike's point".

- **Use of alternative secure communications to transmit specific details that require confidentiality:** Certain communications such as personal data of customers or users, specific details of normal business operations, etc., may require privacy, both from malicious external actors and from those workers who are not directly involved in the operations carried out. In these cases, a **mitigating measure is to carry out a direct communication by an alternative means that offers more privacy**. In traditional radio jargon this is often referred to as "making a low line" and involves making a telephone call (which in analog telephony is considered a low frequency line, as opposed to the very high frequency of VHF/UHF radio communications). Nowadays, private communications can use means other than telephone, such as mobile messaging applications, video calls or other means. This procedure also increases the agility of communications by freeing the group of users from long conversations such as passing a list of personal data, or that require a long exchange of communications such as discussing the solution of a problem in the company's activity.

10.2.2. Mitigations to the lack of integrity in TETRA networks.

In cases where an attacker manages to get hold of functional equipment, either through loss, theft or because he is able to impersonate a valid terminal, there is a risk that the integrity of communications will be affected. The attacker can introduce both voice and data communications, give false commands, affect confidence in real commands or simply cause disruption to communications.

In **critical environments, this eventuality must be taken into account in emergency plans, incorporating a procedure to validate confusing or doubtful orders**.

Thus, for example, when faced with a questionable order, the caller may be asked to communicate by an alternative method, to ask a trusted third party to confirm his order or communication, to verify his identity by knowing details that only a worker should know, or a combination of the above.

10.2.3. Mitigations for loss of TETRA communications availability.

In many industrial or critical infrastructure environments, the voice and data communications function via the TETRA network is one of the essential means for business continuity. Without the possibility of communication between operators, activities must be suspended or severely degraded. The TETRA network may be totally or partially unavailable or may be subject to an accidental outage or an outage caused by external attackers.

In critical environments, the PACE methodology is used to designate pre-established communication systems, depending on the availability of communications and the situation in which they are used.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO DE TRANSFORMACIÓN DIGITAL
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

PACE is an acronym for Primary, Alternate, Contingency and Emergency. PACE designates the order in which a user will move through the available communication systems until contact can be established. Ideally, each method will be completely separate and independent of the other communication systems. For each method, the person wishing to communicate should try several times to establish contact and if this is not possible move on to the next option.

A communication plan based on PACE exists for a specific mission or task within the organization; it should not necessarily be the same for all workers. The plan should consider the exchange of information, both within work groups and with hierarchical superiors. An organization may have multiple plans for different situations, activities and/or external entities. Although, for simplicity, it can be common if it is noted that the single PACE plan has sufficient flexibility.

A PACE plan is neither a frequency plan (which details the frequency allocation and radio spectrum characteristics of the network in use) nor a user group or fleet plan (since the entire network could be inoperative).

The PACE plan system is expressed as a **list of order of precedence of communications**: primary, alternate, contingency and emergency. The plan designates the order in which a group of users will move through the available communications systems until contact can be established. The plan does not designate other factors, such as the exact radio channel or talk group to be used if a radio is used, but rather the order in which the radio is planned to be used and the agreed method of communications between groups.

Emergency Management and Communications should coordinate the development of PACE plans for the various functions and departments within their organization to ensure that critical communication links can be maintained by the incident command. **Departmental PACE plans should be coordinated with Emergency Management and the Communications Department**. It is critical that individual departments nest their plan within the broader Emergency Plan to ensure that the organization has the resources to execute the plan and reduce unnecessary duplication of assets. Developing comprehensive PACE plans will not guarantee flawless communications in a disaster, but it can help clear up some of the problems encountered in all emergency situations.

The elements of the PACE plan typically have the following areas:

- **Primary:** The usual method of communication in a normal working situation, in this case it will normally be the TETRA network.
- **Alternative:** The communication method to use if the previous one is not available, but the normal activity of the work operation has not been affected.
- **Contingency:** The method of communication to be used if both planned systems are not available. Usually, if this situation occurs, it is also foreseeable that there will be a collateral impact on the normal operation of the facilities.
- **Emergency:** Implies a disaster of such magnitude that all previous means of communication have been lost and all work activities should probably be suspended and focus on self-protection or assistance to those affected.

Based on the above, an example of a PACE plan for an industrial facility of the chemical plant type, where the main means of communication is the TETRA network, could be as follows:

- **Primary:** *TETRA network*. Normal plant operation.
- **Alternative**: *VOIP landline telephone network*. Operators will have a sufficiently large network of VOIP landline telephones throughout the plant to allow them to communicate between workstations or with the control room.
- **Contingency**: *Mobile telephony*. All the plant's own communication systems are inoperative. The control room has an external telephone with a direct line to the telephone operator or a cell phone. All operators know the number of the control room and can call with their corporate terminal, their personal terminal or through traditional landline telephony both in the plant itself and in the vicinity.
- **Emergency**: *112*. The facility has been affected by a major disaster, affecting all corporate communications systems. For example, the control room itself has been rendered inoperative. There is a need for communications to maintain the safety of people and facilities. 112 is used because it will be available from any telephone terminal, even if there is no coverage from the operator of the line or if the terminal is blocked (in the case of cell phones) and because calls have preference in the telephone network. Workers will call 112 to communicate the current situation, the means they require or can offer to ensure safety. This plan will have been previously coordinated in the corresponding chemical risk emergency plans. The 112 can refer to the control entity of such emergency plan or make group calls type multiconference or call mediation, serving as a bridge for communications between several workers in the facility.

11. Migration landscape and its security functions

Throughout this section we will explain the current situation of TETRA networks and the migration to future technologies that aim to equal it, improving performance or reducing cost, and to technologies that aim to exceed the possibilities offered by a TETRA network.

11.1. Current technologies

Today, **TETRA is the network with the largest number of critical communications equipment in the world**, and although 4G/LTE technology is emerging more and more strongly, and the open standard MCOP has a greater affinity at present, TETRA networks remain the official bastion of emergency communications in many countries.

11.1.1. 4G LTE - Long Term Evolution

4G/LTE or 4G Long Term Evolution refers to the "Long Term Evolution" of 4G technology and can be considered as the new version of GSM/UMTS standards. This standard was developed by the 3GPP (*3rd Generation Partnership Project)* in a relentless quest to increase the speed of data networks thanks to a new digital signal processing.

LTE can reach transmission speeds of at **most 300 Mbps**, which are incompatible and do not meet the requirements of the 4G standard, so 3GPP developed the **LTE-Advanced** technology**, in which different aspects of the technology were improved to allow it to be compatible with 4G.**

One of the characteristics of this type of technology is that, as in 3G connections, the bandwidth capacity of LTE, LTE-Advanced and 4G technologies is shared by all users who are currently connected simultaneously to the same base station. On the other hand, the quality of the connection quality, in this case, will depend on the user's distance from the station and the existing interfaces.

11.1.2. MCOP Standard

MCOP or Mission Critical Open Platform is a collaborative project between the U.S. Department of Commerce and the National Institute of Standards and Technology (NIST).

The main objective of the MCOP proposal is the definition, development and validation of the MC Open Platform. Its architecture is designed in different layers:

- **MCOP Unified Open Application API**: Provides a flexible interface for clients. In addition, it allows access to the Apps developed for the environment.
- **MCOP Open Source SDK**: Implements the protocols developed by 3GPP in the application API.
- **MCOP Integration API:** Different plugins are designed between user and manufacturer to increase the capabilities of MCOP apps, as well as to support LTE operations.
- **MCOP OAM/OTA Open Access**: Interface capable of allowing the user and the manufacturer to configure and develop interfaces.

11.1.3. Lora and LoRaWan Technology

There are other types of technology today capable of performing similar functions to those presented by TETRA networks.

LoRa is a wireless technology (like Wifi, Bluetooth, LTE, SigFox or Zigbee) that uses a radio frequency modulation patented by Semtech.

The modulation technology is called **Chirp Spread Specturm or CSS** and is used in military and space communications.

Among its most important characteristics are the following:

- high tolerance to interference.
- high sensitivity for receiving data (-168 dB).
- based on "Chirp" modulation.
- low consumption.
- long range (between 10 and 20 km).
- low data transfer (up to 255 bytes).
- point-to-point connection.

Another relevant aspect of this technology is that they work in the **868 MHz frequency band** in Europe, which is like that used by TETRA technology. Currently, **LoRa** technology is focused on IoT connections over long distances where sensors that do not have mains power are needed. Some of its applications are: **Smart Cities**, applications in places with poor coverage and for the construction of private networks with sensors and actuators.

On the other hand, there is the **LoRaWan** network protocol, which uses LoRa technology to create low-power but wide-area networks. This protocol is composed of two components:

- **Gateways**: These are the architecture's antennas, responsible for receiving and sending information to the nodes.
- **Nodes:** These are each of the end devices that make up the network. They send and receive information to/from the Gateways.

This protocol is also focused on IoT communications and among its most important features we can find the following:

- bidirectional connections with end-to-end encryption to ensure security;
- low energy consumption;
- long range (10 to 20 Km);
- almost infinite connection of sensors and equipment (1 million nodes per network).
- low transmission frequency, mobility and location services.
- interoperability of the various LoRaWan networks around the world.

Due to the relentless growth of IoT devices today, **LoRa and LoRaWan networks are experiencing considerable growth** and, although their applications are not in terms of radio for critical or emergency communications, their features allow them to be configured for these aspects.

11.2. Future technologies

There are forecasts that **TETRA will continue to grow for some more years,** until the emergence and establishment of new technologies with similar possibilities to those offered by TETRA.

Currently, TETRA must coexist with the LTE technology for public safety equipment, with a reliability and availability very similar to TETRA. This coexistence is already a requirement, because it seeks to have, in the same device, the advantages provided by 4G (such as high data transmission capacity) but maintaining the security that TETRA allows to implement in its networks.

Another aspect to be considered is the MCOP alternative, which improves different aspects of TETRA previously mentioned, making it a clear competitor.

11.2.1. Technology 5 G

As if that were not enough with 4G technology and its version with LTE, added to MCOP, the emergence of 5G may represent a radical advance in terms of future technologies with similarities or improvements with respect to TETRA.

5G will have the so-called ***Network Slicing***, allowing the different telephone operators to subdivide their main network into sub-networks, which will be semi-independent of each other. All this will make it easier to solve one of the major problems of the technologies described above, i.e., vulnerability to large crowds of users and data in the networks.

Network Slicing will allow the creation of different systems of what could be classified as "small parallel pipes", in which the obstruction of one does not pose a risk to communication between devices within the network. In addition, this segmentation would allow to dedicate some of the 'pipes' for a specific purpose, such as critical communications, allowing to separate this type of high-risk communications from other communications with a more basic character.

All these advantages and solutions provided in the future by 5G mean that TETRA will be forced to coexist not only with 4G but also with 5G, to improve many aspects and problems of using only TETRA.

12. Conclusions

TETRA technology is one of the best or the best option for communications in security, health and business organizations whose service is considered critical due to its purpose and importance.

Due to the quality of the service provided, the insertion of a single frequency plan, added to the possibility of organizing many communication channels, traffic management, introduction of high-level communications and their protection, make the TETRA standard one of the major references in critical communications. **After thirty-three years of existence, it can be stated that TETRA has been consolidated as the reference standard for radio frequency communications, both public and private.**

Analyzing in depth, TETRA provides users with some of the most important aspects of radio frequency, communication **efficiency**, **quality** and **security** derived from the functions of the standard. Its encryption of the air interface is one of the most remarkable aspects since it allows a very secure point-to-point communication, in addition to guaranteeing high quality and speed in the transmission of both voice and data or both together.

On the other hand, throughout the study, emphasis has been placed on the possible vulnerabilities associated with TETRA, as well as how to mitigate them or even, in some cases, eliminate them, because, like any other technology, it has known vulnerabilities and others yet to be known, but the important thing is that the **TETRA** standard has **a large number of possibilities when it comes to protecting against different types** of **attacks.**

As we have seen throughout this section, it is important to note that the *characteristics. In* Spain, TETRA is quite widespread and companies with critical functions have incorporated TETRA devices for their communications due to its characteristics.

In the face of all this, it is worth noting that TETRA has maintained stable growth since its creation in 1990, but the future is uncertain and with new technological advances, such as 5G or LoRaWan, the standard's status in critical communications may be eclipsed.

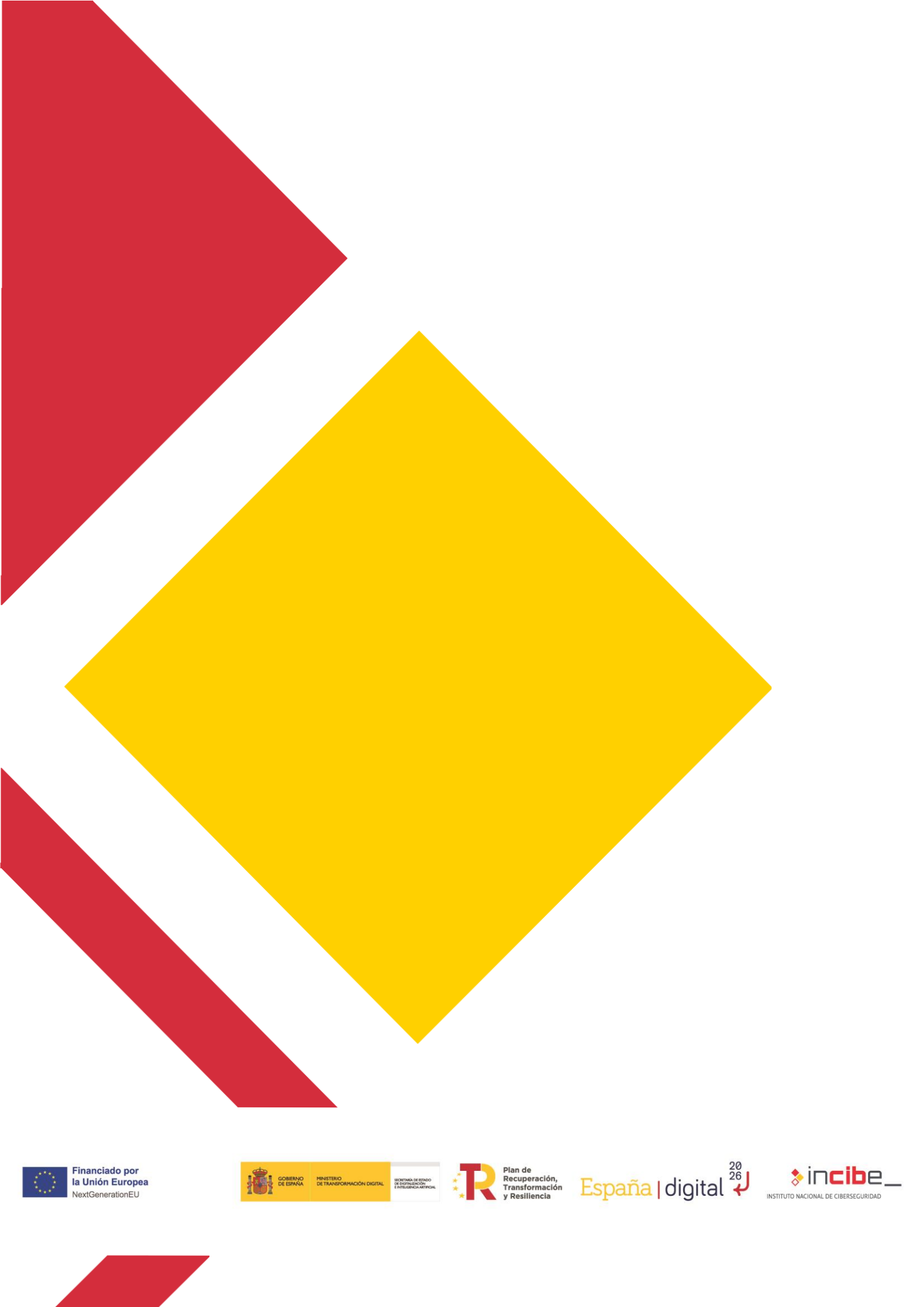
There is no doubt that TETRA has properties that make it a unique standard for critical communications in both the private and public sectors. And even if other technologies eventually replace it in the future, the standard will always be present in the history of communications.

13. Acronym glossaries

- **TETRA**: Terrestrial Trunked Radio
- **PMR**: Private Mobile Radio
- **MHz**: Megahertz
- **PAMR**: Public Access Mobile Radio
- **DGNA**: Dynamic User Number Assignment
- **TEI**: Terminal Equipment Interface
- **DMO**: Direct Mode
- **SwMI**: Switching & Management Infrastructure
- **MS**: Mobile Stations
- **TE**: Terminal Equipment
- **MTU**: Mobile Termination Unit
- **LS**: Line Stations
- **PTN**: Private Telephone Networks
- **ISDN**: Integrated Services Digital Network
- **PSTN**: Public Switched Telephone Network
- **PDN**: Packaged Data Networks
- **TDMA**: Time Division Multiple Access
- **KHz**: Kilohertz
- **SACCH**: Slow Associated Control Channel
- **PDO**: Optimized Data Package
- **LLC**: Logic Control Link
- **MAC**: Media Access Control
- **AIE**: Air Interface Encryption
- **E2EEE**: End to End Encryption
- **DCK**: Derived Cipher Key
- **SCK**: Static Cipher Key
- **SFPG**: Security and Fraud Prevention Group
- **IDEA**: International Data Encryption Algorithm
- **OTAR**: Over The Air Re-Keying
- **CCK**: Common Cipher Key
- **LA**: Location Areas
- **GCK**: Group Cipher Key
- **MGCK**: Group Specific Cipher Key
- **SAGE**: Expert Group on Security Algorithms
- **TEA**: TETRA Encryption Algorithms.
- **PERA**: Purdue Enterprise Reference Architecture
- **OT**: Operation Technologies
- **SCADA**: Supervision, Control and Data Acquisition
- **PLC**: Programmable Logic Controller
- **VPN**: Virtual Private Network
- **LTE**: Long Term Evolution
- **MCOP**: Mission Critical Open Platform

14. References

Reference	Title, author, date and web link
[Ref.- 1]	Analysis of the TETRA digital trunked radio standard and its possible application in Ecuador". July 8, 2011 URL: https://bibdigital.epn.edu.ec/handle/15000/3961
[Ref.- 2]	"MTH800 Product Information Manual" March 2014. URL: https://learning.motorolasolutions.com/node/491/download
[Ref.- 3]	"Introduction to TETRA technology". URL: https://www.qsl.net/kb9mwr/projects/dv/tetra/tetra.pdf
[Ref.- 4]	"Planning of a radio system based on TETRA technology for monitoring a sensor network" July 2017. URL: https://repositorio.upct.es/xmlui/handle/10317/6563?locale-attribute=en
[Ref.- 5]	"Customer Programming Software (CPS) Plus 7.7 User Guide" March 2021 URL: https://manuals.plus/m/528b073c9d49014fdbeac9880790da4f11f5892062e216e5442b89d877340a32
[Ref.- 6]	"MTM800 E Product Information Manual" April 2013 URL: https://learning.motorolasolutions.com/node/501/download
[Ref.- 7]	"Security Analysis of the Terrestrial Trunked Radio (TETRA) Authentication Protocol" 2013. URL: https://www.semanticscholar.org/paper/Security-Analysis-of-the-Terrestrial-Trunked-Radio-Duan-Mj%C3%B8lsnes/7d28c6ea7ea986d370c135d93effc36133816032
[Ref.- 8]	"TETRA TCCA Security" URL: https://tcca.info/tetra/tetra-your-service/security/
[Ref.- 9]	"Maintaining TETRA Security" March 2020 URL: https://tcca.info/documents/March_2020_Maintaining_TETRA_Security.pdf/
[Ref.- 10]	"Tetra Security" February 2006 URL: http://www.signalspaning.se/tetra/TETRA_Security.pdf
[Ref.- 11]	"ANNEX II- JUSTIFICATION OF THE TECHNOLOGY OF THE EMERGENCY NETWORK OF THE REGIONAL GOVERNMENT OF ANDALUSIA" 2016. URL: https://www.juntadeandalucia.es/contratacion/document/download?refCode=2022-0000000408&refDoc=2022-0000000408-2
[Ref.- 12]	"Introduction to TETRA digital trunked communication networks" July 2010 URL: https://personales.unican.es/perezvr/pdf/TETRA-UC_13_7_2010.pdf



Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO DE TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

España | digital 2026

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD