TLP:CLEAR

España | digital 2026

Estudio de ciberseguridad en redes TETRA

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

TLP:CLEAR

Marzo 2023

INCIBE-CERT_ESTUDIO_CIBERSEGURIDAD_EN_REDES_TETRA_2023_v1.1

Índice

ÍNDICE DE FIGURAS

1. Sobre este estudio

La presente guía pretende **explicar las redes TETRA** en todos sus aspectos. Esta tecnología es muy desconocida en diferentes sectores, pero muy útil dependiendo de las necesidades y requerimientos de las empresas o usuarios.

La redacción tiene un carácter técnico ya que está enfocada a explicar todos los aspectos relacionados con las redes TETRA, tanto para usuarios que desconocieran el protocolo como para usuarios que quieran mejorar las características de seguridad de sus redes TETRA o ver las posibilidades que esta otorga, pero a su vez mantiene un lenguaje básico para la comprensión del estudio por parte de cualquier persona interesada en esta tecnología.

El orden de los contenidos se encuentra distribuido de tal forma que inicialmente se tenga un conocimiento teórico sobre la tecnología en general, para posteriormente ir enfocando los contenidos tanto a la utilización de TETRA en diferentes empresas, como a las posibles amenazas que pueden afectar a esta tecnología y las funcionalidades de seguridad que puede implementar.

Además, se proponen diferentes medidas para la securización de la red y la mitigación de las vulnerabilidades.

Por último, se hace referencia a las tecnologías actuales con similitudes a las redes TETRA, se expone un avance de posibles tecnologías futuras y se realiza una conclusión valorando TETRA como tecnología de comunicación en todos sus aspectos.

2. Organización del documento

El presente estudio sobre las redes TETRA presenta una estructura enfocada al aprendizaje progresivo sobre esta tecnología de radio. Inicialmente está la 3.- introducción**,** en la cual se hace una breve introducción a la tecnología TETRA, sus usos, funcionalidades y principales características para ir introduciendo conceptos que más adelante se explicarán de forma más extensa.

Tras la introducción, se explica la 4.- tecnología TETRA en sí, con un repaso completo incluyendo los tipos de usuarios, bandas de frecuencias, arquitectura, elementos principales y tecnología empleada para el funcionamiento de la red.

Para introducir a TETRA en los diferentes sectores en los que se usa, se realiza una explicación sobre el 5.- sector privado y público junto con las redes TETRA. En este apartado se explicará el empleo de redes TETRA tanto en el sector privado como en el sector público, así como un mapa por comunidades indicando el uso de esta red de comunicación. Además, identifica un caso concreto de una empresa privada que utiliza una red TETRA para comunicaciones.

Posteriormente, y ya introduciendo el estudio en los peligros y 6.- amenazas de seguridad en redes de radio digital, se realiza una explicación sobre dichas problemáticas, distinguiendo entre dos tipos: vulnerabilidades en los modos de operación y en la arquitectura, además de vulnerabilidades en los tipos de cifrado.

Combinando con el apartado anterior, el estudio abarca las diferentes 7.- funcionalidades de seguridad en dispositivos TETRA, con una explicación completa sobre las funcionalidades, funciones, claves de seguridad y cifrados proporcionados por TETRA para securizar las comunicaciones, así como una explicación detallada de cada una de las funciones y funcionalidades presentadas. Además, y en relación con el apartado de TETRA en el sector público y privado, se expondrán los diferentes 8.- requerimientos de seguridad en aplicaciones empresariales, siendo estos unos conceptos básicos para la securización de estas redes en los entornos industriales sumados a las funcionalidades de seguridad de TETRA del apartado anterior.

Ya que la mayor parte de la información en cuanto a la seguridad se refiere es teórica, se ha introducido un apartado con 9.- funcionalidades reales de seguridad en dispositivos TETRA. Este apartado del estudio explica y define algunas funcionalidades reales de los dispositivos TETRA. Así mismo, también se hace un listado de posibles 10.- mitigaciones de vulnerabilidades en redes TETRA: mitigaciones técnicas y operativas ante vulnerabilidades en las redes TETRA. A su vez, también se explicarán los conceptos para casos concretos como la ausencia de integridad, de confidencialidad y de disponibilidad,

Para ir finalizando el estudio, se ha buscado comparar entre las tecnologías actuales similares a TETRA, y qué se espera de esta tecnología o de posibles variantes en el futuro, por lo que se ha incluido el apartado del 11.- panorama de migración y sus funciones de seguridad.

Para finalizar el estudio, se han escrito unas conclusiones sobre la valoración global de la tecnología TETRA en todos sus aspectos.

3. Introducción

La red **TETRA** (*Terrestrial Trunked Radio*) es un estándar desarrollado en Europa en la década de 1990 por el ETSI[1] (Instituto Europeo de Normas de Telecomunicaciones), cuyo surgimiento vino de la mano de la gestión de comunicaciones móviles para casos extremos, en los que la comunicación estándar vía telefónica podría no funcionar correctamente. Por lo tanto, puede considerarse como **una red alternativa para que las comunicaciones con servicios de emergencia y seguridad estén siempre operativas**.

TETRA unifica diferentes alternativas de interfaces de **radio digital** para la comunicación y sirve como estándar para la construcción de redes móviles privadas o PMR (*Private Mobile Radio*).

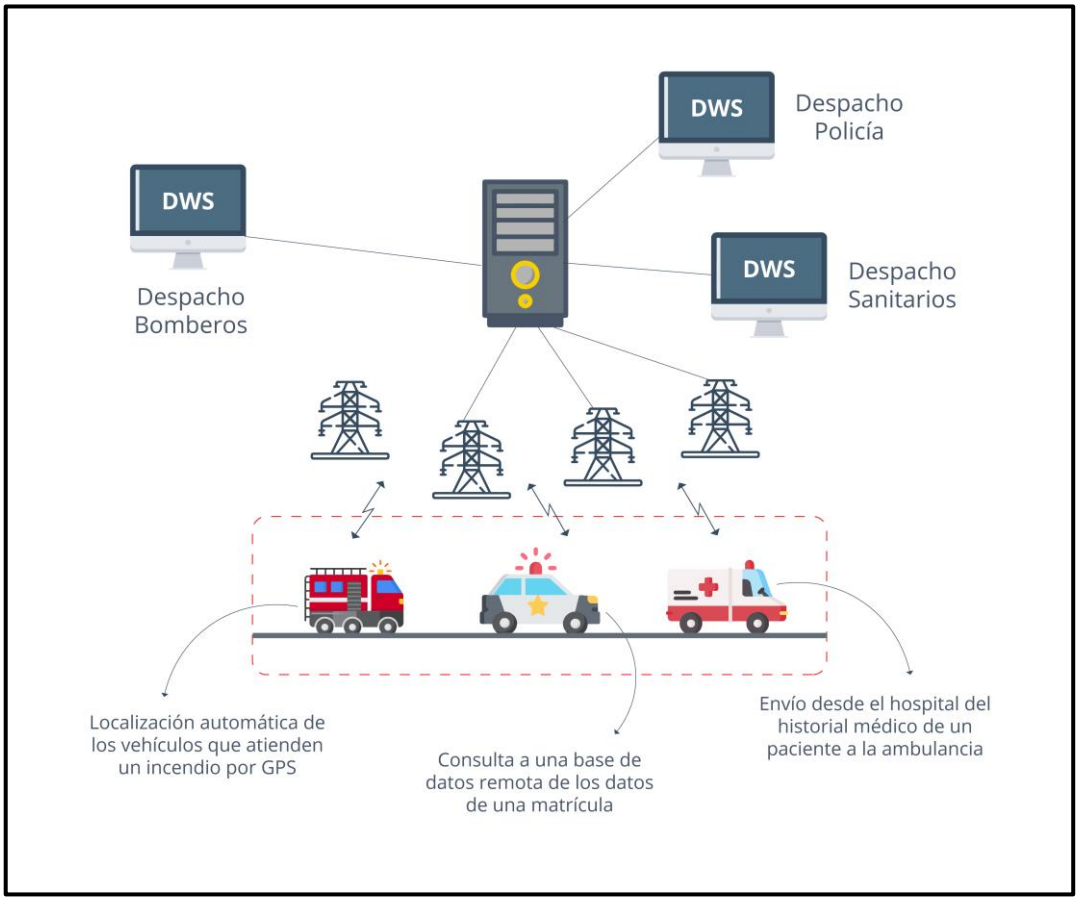


Ilustración 1: Estructura de red del sistema TETRA[2]

Hoy en día, estas cualidades permiten que diferentes grupos profesionales cuyo trabajo es crítico (policías, bomberos, agentes de movilidad, ambulancias e incluso la red de comunicaciones de seguridad nacional) puedan disponer de un **sistema de comunicaciones avanzado, con un alto grado de fiabilidad y seguridad**.

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

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

Estos grupos profesionales utilizan las **redes PMR**, anteriormente mencionadas, que han de funcionar **en todo momento, sin ningún fallo, para poder mantener un nivel de comunicación óptimo, una calidad de voz elevada, con compatibilidad y disponibilidad en situaciones críticas**.

En la actualidad, TETRA opera en **más de cien países a lo largo de todo el mundo.** Su elevada expansión radica en las características presentadas anteriormente, las cuales hacen que cualquier empresa con comunicaciones vitales para su funcionamiento o cualquier infraestructura de emergencias, independientemente de ser pública o privada, pueda implementar el estándar en sus comunicaciones. Además, la mayoría de los países del mundo tienen reservada una banda de frecuencias para comunicaciones críticas, es decir, comunicaciones vitales para el bienestar de las personas (como en las comunicaciones de la policía o emergencias), o comunicaciones vitales para el buen funcionamiento de diferentes empresas con actividades críticas (refinerías en altamar, puestos de comunicación en puertos y aeropuertos, empresas del sector nuclear etc.). Dicha banda está en el entorno de los 370-400 MHz, banda en la que se puede implementar una red TETRA simplificando así el proceso de creación de la arquitectura, además, la utilización de una **frecuencia tan baja permite alcanzar una mayor cobertura por cada antena instalada**.

Aunque las frecuencias puedan variar dentro de un rango más o menos establecido, más adelante se detallan las diferentes bandas y el rango de frecuencias en MHz dentro de las que podríamos encontrar diferentes comunicaciones TETRA. Cabe destacar la diferencia de frecuencias entre los servicios de emergencia y los servicios públicos, teniendo una mayor amplitud y diversidad en las bandas del servicio público.

Su uso también está muy extendido en redes de comunicación dentro de las **infraestructuras industriales sensibles**, como en las refinerías, debido a la sensibilidad de su trabajo y de su localización, así como su necesidad de contar con una elevada seguridad en las comunicaciones que garantice la autenticación, la confidencialidad, la integridad, la disponibilidad y el no repudio. Además, TETRA proporciona un tiempo de **establecimiento mínimo** (<0,3 s), ***push-to-talk*** (pulsar para hablar) en llamadas de grupo y **transmisión de radio directa (DMO)** entre terminales.

Aunque TETRA proporcione diferentes medidas para la **securización de la red de comunicaciones**, como el protocolo de autenticación, es cierto que existen fallos dentro del estándar como, por ejemplo, aquellos que pueden permitir a un atacante anular el protocolo de autenticación, suplantar la identidad de una estación base y reducir la disponibilidad de acceso a la red por parte de los usuarios. Sin embargo, **existen métodos o implementaciones capaces de contrarrestar dichos fallos.**

A lo largo de este estudio, se van a detallar todas las ventajas ofrecidas por las redes TETRA, en cuanto a su **seguridad, fácil implementación y calidad en situaciones de emergencia**. También, se realizará un análisis de las redes TETRA en el sector privado y de la securización de la arquitectura implementada. Por otra parte, se explicarán las diferentes amenazas que pueden afectar a la red, así como requerimientos mínimos a implementar para asegurar que la comunicación sea fiable y no tenga fallos de seguridad.

4. Tecnología TETRA

TETRA se puede definir como un estándar de radio móvil digital, bajo la interoperabilidad de **TETRA Alliance**. Dentro de este estándar, también existen otras variables como TETRAPOL, la cual es utilizada únicamente para dar servicio a las comunicaciones de cuerpos policiales en ciertos países.

TETRA puede tener una gran cantidad de usuarios, ya sean desde los mencionados cuerpos policiales, entidades de Seguridad Nacional, el sector privado e incluso usuarios finales individuales.

Como ya se ha introducido anteriormente, la principal misión de TETRA es cubrir diferentes necesidades concretas de comunicación, para diferentes tipos de usuarios, en diferentes entornos y con medidas de seguridad muy particulares y que podrían agruparse en:

- **Usuarios PMR (*Private Mobile Radio*):** Entidades de seguridad pública, entre los que encontramos a policías, militares, equipos de respuesta rápida…
- **Usuarios PAMR (*Public Access Mobile Radio*):** dentro de este grupo encontramos a los bomberos, ambulancias, guardacostas y demás servicios con características similares.

Estos dos tipos de usuarios dependen de que su comunicación sea lo más óptima y segura posible, ya que de ella depende la correcta realización de su trabajo. Entre las características que buscan estos usuarios para la comunicación encontramos: una buena latencia, elementos de seguridad ante agentes externos y calidad de voz.

A su vez, TETRA especifica dos tipos de servicios a la hora de realizar una comunicación:

- **Servicios básicos:** en este aspecto, se pueden incluir las llamadas individuales, las llamadas de grupo o las llamadas de grupo confirmado (con autenticación y autorización) y también diferentes servicios de llamada de difusión. Como su propio nombre indica, son servicios básicos de voz y en menor medida de datos.
- **Servicios suplementarios:** estos servicios envuelven las llamadas con prioridad preventiva, la llamada prioritaria, retención de llamadas, la posibilidad de realizar escuchas ambiente, servicios de entrada tardía, selección de área y la DGNA (asignación dinámica de número de usuarios o *Dynamic Group Number Assiggnment*).

Estos dos servicios se pueden considerar servicios de misión crítica y son servicios a los que acceden usuarios móviles en diferentes localizaciones dentro del planeta. Esta es una de las funcionalidades más importantes de TETRA, la posibilidad de que diferentes usuarios con diferentes necesidades sean capaces de comunicarse. Esto se debe principalmente a que TETRA es la primera norma digital de radio móvil privada verdaderamente abierta.

Siendo más específicos, en cuanto a los servicios y las comunicaciones de los usuarios TETRA, a continuación se muestra una tabla que engloba las diferentes frecuencias en MHz de las bandas utilizadas, tanto para servicios básicos, como suplementarios dentro de los servicios públicos y los servicios de emergencia.

Servicios de Emergencia			Servicio Público	
Número	Pareja de frecuencias (MHz)		Pareja de Frecuencias (MHz)	
	Banda 1	Banda 2	Banda 1	Banda 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

Tabla 1: Frecuencias por servicio

TETRA persigue el objetivo de poder garantizar un mercado multi vendedor y abierto y para ello especifica las siguientes interfaces que considera esenciales para conseguir dicho objetivo:

- La **interfaz aérea** debe garantizar la interoperabilidad de los diferentes equipos terminales para distintos fabricantes.
- En **la interfaz de equipos terminales** (TEI) debe facilitar y facilita el desarrollo de aplicaciones de datos móviles de forma totalmente independiente.
- La **interfaz entre sistemas** (ISI) debe permitir la interconexión de diferentes redes TETRA ya sean de un mismo fabricante o de distintos fabricantes.
- TETRA garantiza con la inclusión del funcionamiento en **Modo Directo** (DMO) que las comunicaciones entre terminales sean óptimas incluso estando fuera de la cobertura de la red.

La siguiente ilustración permite tener un mejor conocimiento acerca de las posibles comunicaciones entre varias redes TETRA, dentro de una misma red TETRA, entre dispositivos sin cobertura y entre las interfaces de los terminales y la red.

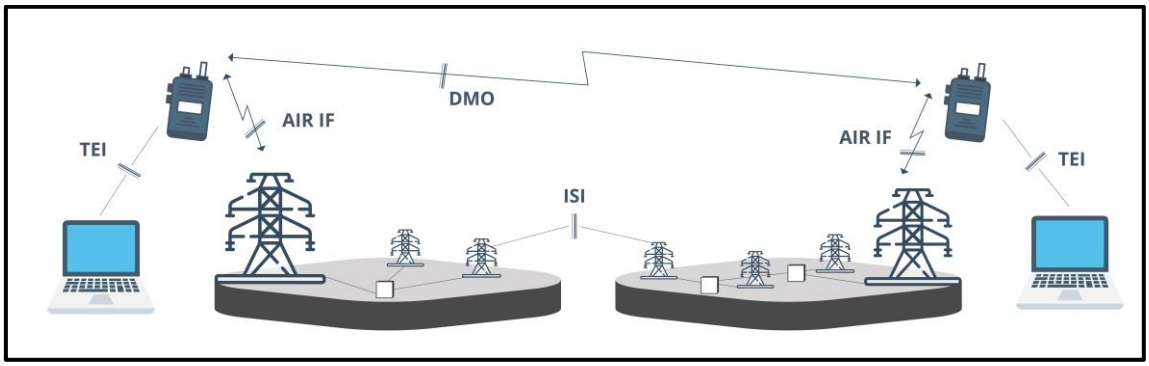


Ilustración 2: Arquitectura TETRA[3]

Una vez que se han comentado, a grandes rasgos, las posibilidades en cuanto a los usuarios, dispositivos, interfaces y diferentes modos que se pueden implementar en una arquitectura TETRA, se va a explicar qué características técnicas otorga respecto a otros sistemas de comunicación radio digitales existentes.

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

4.1. Infraestructura de una red TETRA

La especificación TETRA no contempla ningún tipo de topologías de red ya que estas pueden ser flexibles, es decir, dependiendo de la situación o entorno en el que se quieran instalar, pueden adaptarse y variar entre una topología en estrella, anillo o malla.

Dentro del estándar, la infraestructura de la red suele tomar el nombre de Infraestructura de Administración y Conmutación (SwMI), la cual se explicará más adelante en detalle en el apartado *4.2 Características técnicas*. Lo único que sí se define en el estándar TETRA son las entidades e interfaces sobre las que se pueden y han de conectarse los dispositivos dentro de la infraestructura. Gracias a esto, TETRA consigue asegurar la interoperabilidad y la administración de la red.

4.1.1. Entidades

Existen diferentes entidades dentro de un sistema TETRA como son las siguientes:

- Un **Sistema TETRA Móvil**, el cual comprende las estaciones base (BS), conmutadores, centros de administración y las operaciones.
- Las **Estaciones Móviles** (MS), las cuales comprenden a la Unidad de Terminación Móvil (MTU) y el Equipo Terminal (TE).
- Las **Estaciones de Línea** (LS), las cuales comprenden, al igual que las MS, a la Unidad de Terminación Móvil (MTU) y al Equipo Terminal (TE).
- La **unidad de administración central** de red.
- Estaciones móviles operando en una red DMO.
- Y como veremos más adelante, el estándar TETRA también contempla las **conexiones con otras redes,** como puede ser la Red Telefónica Pública Conmutada (PSTN), con las Redes Telefónicas Privadas (PTN), con la Red Digital de Servicios Integrados (ISDN) y con las Redes de Datos Empaquetados (PDN).

4.1.2. Interfaces

Definidas por TETRA para la comunicación entre algunas entidades y para la comunicación con otras redes TETRA.

- **I1**: Interfaz aire, por la cual se comunica el SwMI con la unidad de terminación móvil (MTU) de una MS.
- **I2**: Interfaz de la Estación de Línea, a través de la cual, se comunica la SwMI con la unidad de terminación de línea (LTU).
- **I3**: Interfaz Inter-Sistema, por la que se comunican dos redes TETRA distintas.
- **I4:** Interfaz entre la estación MS y el TE.
- **I4'**: Interfaz entre la LS y el TE.
- **I5**: Interfaz de administración de red.
- **I6**: Interfaz de Operación en Modo Directo (DMO). A través de esta interfaz, se comunican los Equipos Terminales que trabajan en una red DMO.
- **Interfaz Hombre Máquina**. Comunicación entre el usuario y la máquina.

Además de las presentes interfaces, la red TETRA, como bien se ha dicho anteriormente, se puede conectar a otras redes. Dicha comunicación se realiza a través de los *gateways* definidos en cada una de las redes externas.

4.2. Características técnicas

TETRA es una plataforma de comunicaciones que permite la transmisión de voz y datos, que junto a las características de conectividad que ofrece, supone un nivel muy avanzado en cuanto tecnología PMR se refiere.

4.2.1. Sistema totalmente digital

Como primera característica técnica, hay que destacar que TETRA es un sistema **totalmente** digital, capaz de proporcionar sistemas de voz, con una baja tasa de error y una alta calidad. A mayores de este servicio, TETRA permite la transmisión de datos, ya sean conmutados por circuitos o por paquetes, permitiendo al operario configurar su velocidad de transmisión para adaptarse a las características de la red y reducir al máximo los posibles errores.

4.2.2. Acceso Múltiple por División de Tiempo

TETRA emplea el **Acceso Múltiple por División de Tiempo** (TDMA) con capacidad para cuatro canales de usuario. Dichos canales están intercalados en una única portadora, con una separación de portadoras de 25 kHz. Esto tiene una implicación muy importante y es que, gracias a la separación de portadoras y el TDMA, se consigue una excelente eficiencia del espectro de frecuencias. Además, **se consigue que solo sea necesaria una unidad de radio para cada cuatro canales de usuario.**

Aunque cada canal pueda ser ocupado por una radio, en los casos en los que se requiere una **altísima transferencia de datos y a una gran velocidad** (tope máximo aproximadamente 28,8 kbits/s con una tecnología básica), **es necesario poder reservar los cuatro canales,** consiguiendo así una gran velocidad de transferencia de bits/s.

Ilustración 3: Cuatro canales de usuario multiplexados en uno de 25 kHz

La utilización de cuatro canales multiplexados, combinado con el diseño de TETRA como un sistema troncalizado, ha permitido, como se puede apreciar en la siguiente ilustración, que diferentes organizaciones o entidades puedan compartir y operar de forma independiente en el mismo entorno de forma segura (si se configura de forma correcta), manteniendo la privacidad y con una calidad de comunicación óptima.

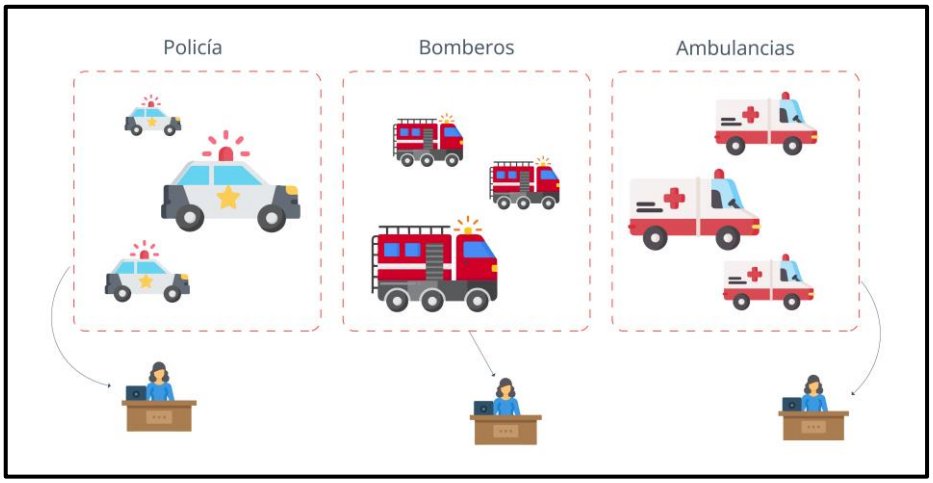


Ilustración 4: Interconexión virtual dentro de una misma red TETRA[4]

4.2.3. Elevada funcionalidad

Otra de las funcionalidades tecnológicas proporcionadas por TETRA es la de mantener la alta funcionalidad de la red con un uso eficiente de recursos, **gracias a la interconexión virtual realizada internamente en la red**.

4.2.4. Tiempos de establecimiento y estructura de tramas

Se trata de una de las cualidades más importantes de TETRA y la que aporta una ventaja diferencial respecto a otros sistemas de radio digital para las comunicaciones de emergencia. La aplicación de sistemas de TDMA permite a TETRA poseer un **tiempo de establecimiento muy bajo**, de unos 300 ms aproximadamente, que como se ha mencionado antes, es crucial para los servicios de seguridad pública y de emergencia. TETRA permite tanto las **operaciones dúplex** para llamadas individuales como **operaciones semidúplex** para llamadas de grupo.

En cuanto a las tramas de la estructura en TETRA, esta **posee cuatro ranuras de tiempo por trama TDMA**. Posteriormente, se organiza en dieciocho tramas TDMA por multi trama. En las operaciones que se transmiten voz y datos en modo circuito, el tráfico de una multi trama de dieciocho tramas se comprime y pasa a ser de diecisiete tramas TDMA, permitiendo así que la decimoctava trama se pueda utilizar para la señalización de control sin interrupción de flujo de datos. **Se denomina trama de control y proporciona la base para el canal de control asociado lento o SACCH**.

En resumen, el SACCH es capaz **de proporcionar la señalización del canal de control** de fondo que siempre está presente, incluso cuando todos los canales están asignados a tráfico.

4.2.5. Conectividad y servicios de telecomunicaciones tetra

TETRA facilita la conectividad con otras redes gracias a las características implementadas en su estándar. Una red TETRA es capaz de conectarse con redes telefónicas públicas y privadas, a otras redes de datos y a sistemas de gestión y control.

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

La gran ventaja proporcionada por TETRA, y como se puede observar en la siguiente ilustración, es que la utilización de un dispositivo TETRA puede permitir acceder a cualquier sistema conectado a la red sin necesidad de tener convertidores u otros dispositivos de enlace.

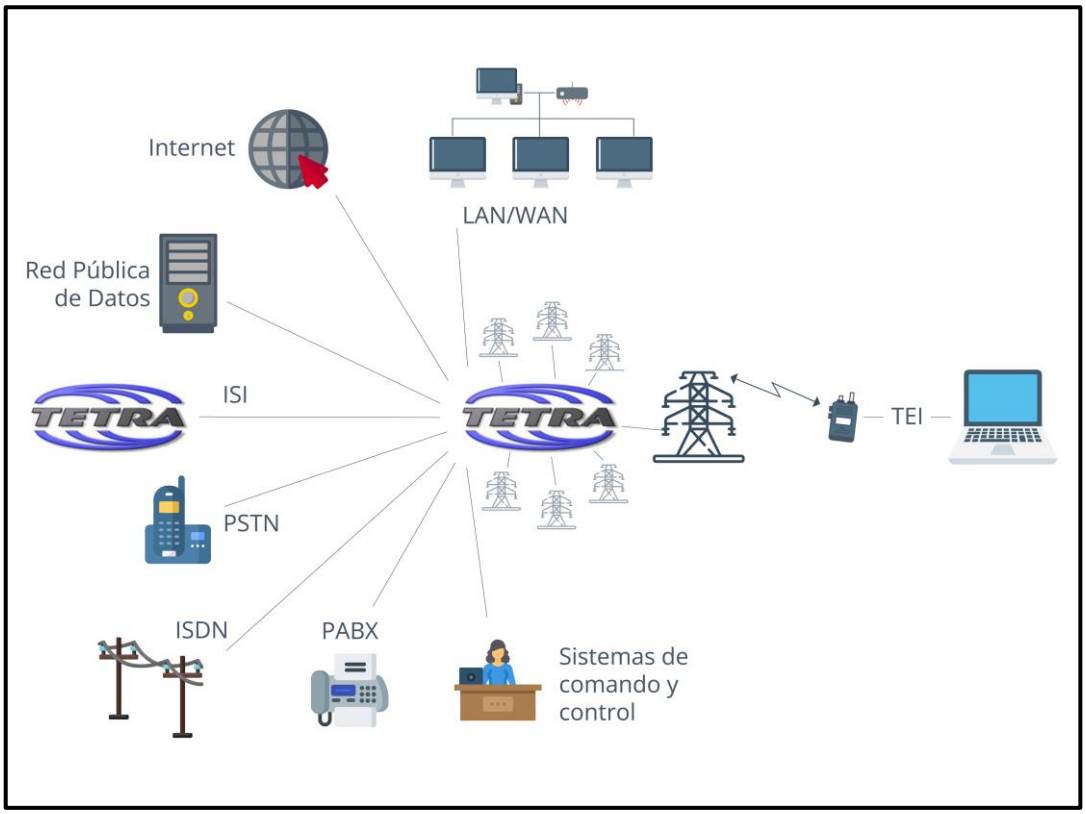


Ilustración 5: Conectividad en las redes TETRA[5]

La conectividad, combinada con el ancho de banda, hace de TETRA una plataforma superior para el desarrollo de aplicaciones de datos.

En cuanto a los servicios de telecomunicaciones, son capaces de proporcionar una capacidad de comunicación para todo el espectro entre usuarios y terminales. En el **estándar TETRA, se establece que los teleservicios de comunicación abarquen todos los servicios de comunicaciones de voz**, además, también se indica que un servicio portador debe proporcionar capacidad de comunicación entre interfaces de red de terminales.

Por ejemplo, supongamos que se instala una red TETRA en una refinería en alta mar. Para este tipo de industria, es de suma importancia la utilización de dispositivos que tenga la directiva APEX aprobada ya que cualquier dispositivo que incumpla dichas medidas puede suponer un riesgo para la infraestructura. En este aspecto, entran los dispositivos TETRA (con directiva APEX en orden), los cuales están orientados a comunicaciones dentro de la propia infraestructura (siendo el caso de una empresa privada) pero que gracias a la interconexión con otras redes, pueden permitir a los operarios realizar llamadas vía telefónica en casos excepcionales en los que sean necesarios reduciendo así el riesgo que podría suponer usar un dispositivo móvil base.

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

5. Combinación del sector privado y público junto con las redes TETRA

La gran utilidad de las redes TETRA en temas de comunicación hace que sean uno de los principales medios de comunicación para entornos en los cuales se necesita cierta privacidad en la comunicación. Existe una cantidad extensa de redes TETRA por el mundo, pero en este punto nos centraremos en las principales redes que podemos encontrar por toda España, dividiéndolas por comunidades autónomas. La finalidad de estas redes TETRA puede ser tanto para empresas públicas como para empresas privadas.

Los datos de estos apartados no reflejan la actual situación de los sectores, debido a la confidencialidad, protección de los sistemas y que la gran mayoría de empresas que usan redes TETRA son empresas de sectores críticos, por lo que se usarán datos previos al año 2019 y que no reflejan totalmente la situación de TETRA en España aunque sea similar.

5.1. Sector Privado

Existen **alrededor de 50 redes TETRA** que podemos encontrar en empresas como:

- Aeropuertos:
  - El aeropuerto de Ibiza
  - El aeropuerto de Málaga - Costa del Sol
  - El aeropuerto de Alicante - Elche
  - El aeropuerto del Prat en Barcelona, donde se instalaron una cantidad superior a 1.600 terminales.
- Puertos:
  - El puerto de Valencia
  - El puerto de Gandía
- Trenes:
  - El tren de Madrid
  - El tren del Vallés y la línea de Llobregat-Anoia
  - El tren del País Vasco (Euskotren)

Un ejemplo de estas redes anteriormente mencionadas, siendo una de las más grandes que podemos encontrar en España, es la del Puerto de Valencia[6], que en 2018 se gastó un total de 54.450€ en elementos TETRA, divididos en los siguientes equipos:

- 37 unidades Motorola MTP3250 portátil tetra 280-430 MHz --> incluye 1 antena estándar TETRA/GPS, 1 batería alta capacidad 2150mAh, clip de cinturón, protector lateral conector de accesorios
- 37 unidades Motorola base cargadora de sobremesa dual
- 37 unidades Motorola MTP3250 enable GPS Feature --> Licencia activación
- 2 unidades Motorola MTM5400 radio base TETRA con micrófono de mano

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

- 2 unidades Antena UHF TETRA colineal 3dBd de altas prestaciones
- 2 instalaciones y puesta en marcha de radio Motorola MTM5400 + antena
- 39 configuraciones terminal de radio
- 1 alta de terminal de radio en sistema TETRA DIPC y sistema de posicionamiento.
- Mientras que en el 2020 hizo un plan con la compañía Amper Sistemas, S.A. de 45 meses por un total de 1.095.050€ divididos en 2 plazos, el primer plazo 9 meses como máximo para la instalación de los sistemas y los siguientes 36 meses para el mantenimiento de los diferentes elementos.

Como se ha podido observar, las redes TETRA son comunes en el sector privado, sobre todo en empresas que requieren de una comunicación rápida y efectiva ante cualquier imprevisto que pueda haber con la red principal.

5.2. Sector público

En el sector público, las redes TETRA encontradas son utilizadas para otro tipo de servicios, en su mayoría para los tres siguientes tipos de servicios:

- Servicios de seguridad.
- Servicios de rescate.
- Servicios médicos.

En la siguiente ilustración se puede observar un mapa visual donde nos muestra las estaciones base en cada comunidad autónoma:

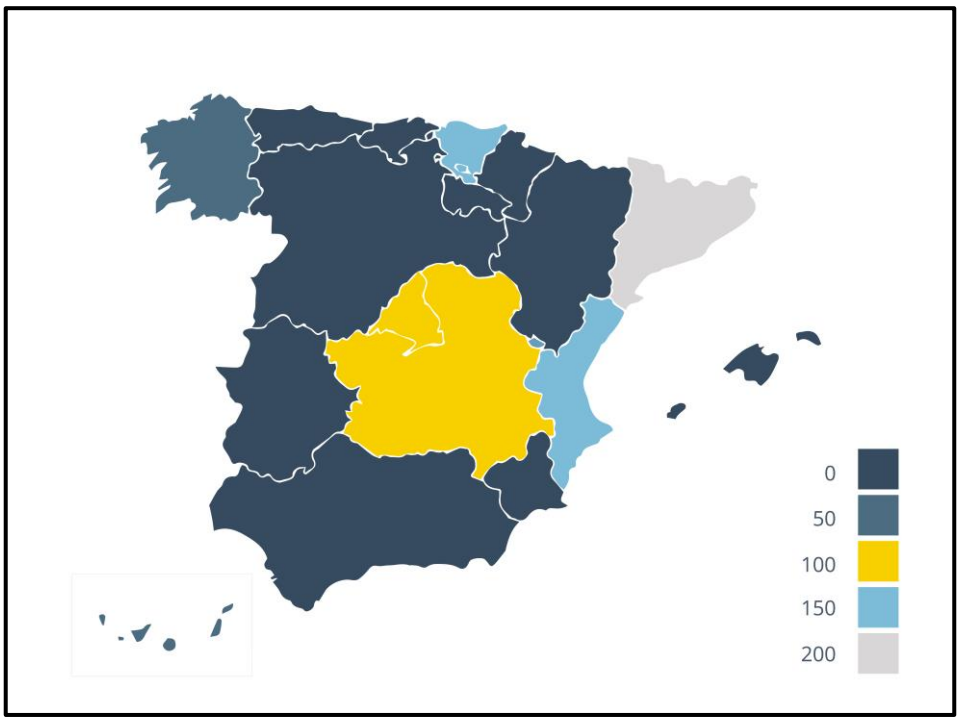


Ilustración 6: Estaciones base de redes TETRA en España

Además, para tener una mejor comprensión de la magnitud de redes TETRA en España, a continuación se muestra una valoración del número de usuarios por terminales en diferentes comunidades autónomas, así como si usan la tecnología TETRA, EDMR o analógico.

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

Ilustración 7: Terminales por comunidad [7]

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

6. Amenazas de seguridad en redes de radio digital

Como en cualquier red, la posibilidad de que haya un fallo en la seguridad siempre está presente. Concretamente en las redes TETRA, se utiliza la misma estructura de protocolo que en una red IP, por lo tanto, las vulnerabilidades presentadas en cualquier red IP también están presentes en las arquitecturas TETRA.

6.1. Vulnerabilidades en los modos de operación y en la arquitectura

Para poder explicar algunas de las vulnerabilidades vamos a hacer un rápido repaso a que operaciones se pueden realizar y como están diseñadas las arquitecturas de las redes TETRA.

El sistema TETRA consta de estaciones base (**BS, *Base Station***), las cuales son elementos de la infraestructura dedicados a la gestión y conmutación con interfaz aérea. Las comunicaciones se realizan mediante la interfaz aire a estaciones móviles, a otras redes mediante pasarelas, con una interfaz intersistemas con otras redes TETRA y con los terminales o estaciones móviles (**MS, *Mobile Station*).**

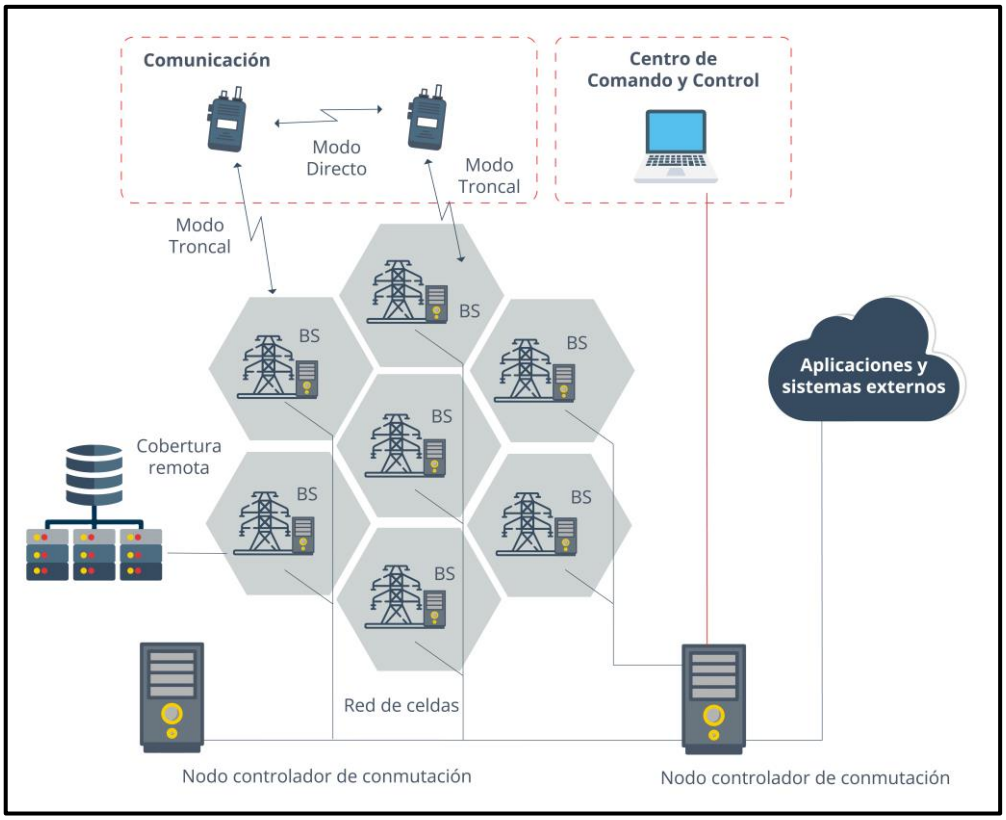


Ilustración 8: Arquitectura y modos de operación[8]

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

Las BS reenvían la información desde una MS al receptor solicitado. Estas estaciones base interactúan con un controlador de otra estación base (**BSC, *Base Station Controller***), que a su vez realizará una comunicación con un centro de conmutación móvil (**MSC, *Mobile Switch Center***). Las MS podrán comunicarse entre sí, incluso estando fuera del rango de una estación base.

TETRA posee tres modos de operación o transmisión de datos:

1. **V+D (Voz más Datos):** Otorga la posibilidad de conmutar el tipo de conmutación entre voz y datos o utilizar ambos a la vez.
2. **DMO (Modo Directo de Operación):** Comunicación entre dos estaciones móviles incluso si estas están fuera del rango de la estación base.
3. **PDO (Paquete de Datos Optimizado):** Solo permite la transmisión de datos.

Tal y como se mencionó anteriormente, la arquitectura o pila de protocolos de la Interfaz Aérea de TETRA es similar a la del protocolo IP, por lo tanto, es susceptible de recibir ataques. Dentro de esta pila de protocolos en TETRA, encontramos tres capas:

- **Capa física:** Permite tener un control de las características de radio más importantes, entre las que podemos encontrar la modulación y la demodulación, además de la sincronización. Esta capa utiliza TDMA con cuatro ranuras de tiempo como las expresadas en apartados anteriores. Además, utiliza un esquema de modulación de impulsos *shaping* DQPSK con un canal de radio de 25 kHz y velocidad de canal de 36 Kbps. En ciertas implementaciones de TETRA, se permite la utilización de FDMA.
- **Capa de enlace:** Los datos se organizan en dos tramas L2. Además, está dividida en dos subniveles con diferentes funcionalidades. Una primera parte LLC (Link de Control Lógico) ocupado de la transmisión y retransmisión de datos. Por otra parte, la MAC (Control de Acceso al Medio) cuya función es la de controlar el acceso a los canales, la codificación y decodificación del canal, el *interleaving, routing* y la multiplexación.
- **Capa red:** Se divide entre un plano de usuario encargado de gestionar la voz y los datos de los usuarios y un plano de control empleado para gestionar la señalización y los datos de control. También tiene la función de control de procedimientos de la red.

Estas capas pueden presentar diferentes vulnerabilidades de carácter general, similares a las de cualquier otra red de comunicaciones, así como las vulnerabilidades propias del protocolo IP.

En ciertos casos en los que la configuración es errónea o no se han establecido unos niveles de seguridad correctos, un agente externo podría realizar un ataque de baja complejidad sobre los canales lógicos que representan el interfaz entre protocolos y el subsistema de radio, ya que son uno de los puntos sensibles en la comunicación. La información entre el nivel MAC superior e inferior se pasa a través de canales lógicos donde pueden pasar información específica de una o ambas direcciones.

Como TETRA utiliza TDMA para poder acceder al canal, varios usuarios pueden compartir la misma frecuencia de radio, pero en diferentes ranuras de tiempo, por lo que un atacante podría aprovechar una mala configuración, para acceder a dichas ranuras de tiempo y obtener dicha información.

6.2. Vulnerabilidades en los tipos de cifrado de TETRA

Las escuchas clandestinas son uno de los grandes problemas existentes en las comunicaciones de radio, que junto al *sniffing* y el análisis del tráfico, hacen que la implementación de medidas de seguridad sea casi un requisito obligatorio.

Para prevenir las escuchas por parte de agentes externos, TETRA permite introducir el AIE (*Air Interface Encryption*) y el E2EE (*End to End Encryption*) como se mencionará en el apartado *7 Funcionalidades de seguridad en dispositivos TETRA*.

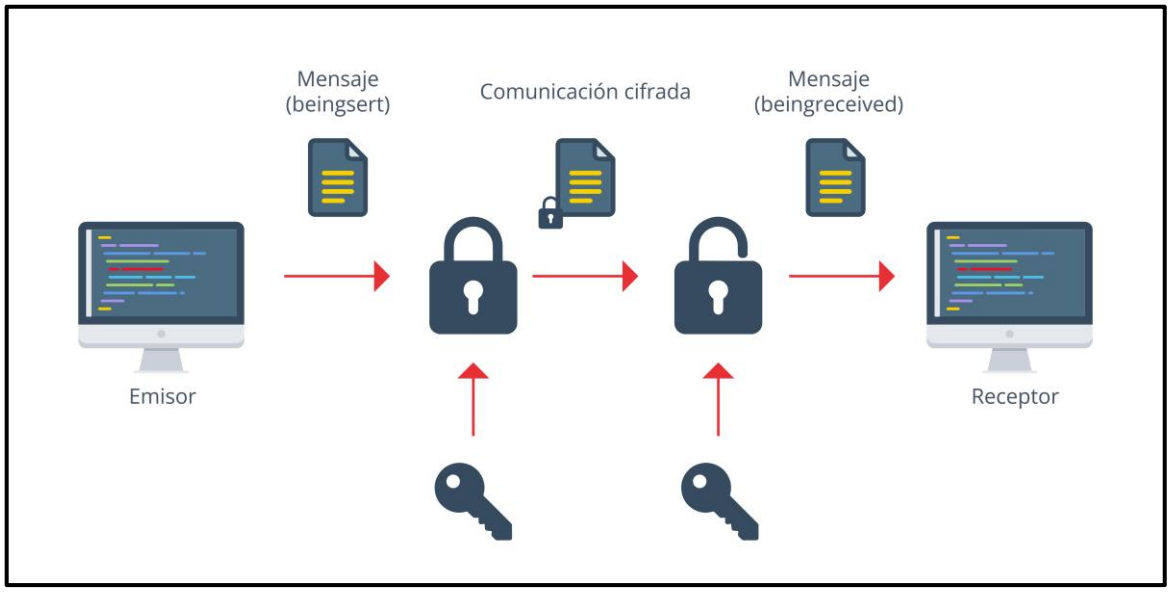


Ilustración 9: Cifrado E2EE[9]

AIE permite protegerse ante escuchas clandestinas protegiendo la señalización, las identidades, la voz y los datos. Una de las desventajas de utilizar solo este método para reducir costes es la posibilidad de realizar un análisis de los datos con *sniffers* dentro de la red, lo cual se soluciona mediante el cifrado de extremo a extremo.

Al igual que el AIE, el E2EE también tiene vulnerabilidades a la hora de cifrar de extremo a extremo, ya que solo se implementa en el canal de tráfico, pero no sobre el canal de control, de ahí la necesidad de implementarlo junto con el AIE.

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

7. Funcionalidades de seguridad en dispositivos TETRA

TETRA busca garantizar en mayor medida la seguridad, proporcionando diferentes medidas de protección, intentando asegurar siempre:

- La **autenticación** de los usuarios para el acceso a la red por parte de los terminales de radio, mediante la posibilidad de establecer un sistema de **autorización,** la cual, será otorgada por el administrador, permitiendo el acceso a la comunicación correspondiente.
- La **confidencialidad** de las comunicaciones, gracias a la incorporación del cifrado aire-aire (entre terminal y estación base) y de mecanismos que impiden descifrar el mensaje en puntos intermedios de la comunicación.
- La **integridad** de la información, gracias a la incorporación de un gran abanico de controles de seguridad (seguridad en *Back-end*, mecanismo para impedir el uso no autorizado de *software de dispatcher*, controles de detección de acceso, tecnología de monitorización, etc.).
- Por último, también se pueden implementar medidas para garantizar la **disponibilidad** y el **no repudio.**

A continuación, se muestran las diferentes **funcionalidades de seguridad presentes en las redes TETRA para proteger la información transmitida por sus usuarios** (ya sea tráfico de voz, datos de usuarios u otra información relacionada con las identidades y operaciones de los usuarios).

- **Mecanismos de seguridad:** Funciones autónomas capaces de asegurar un objetivo de seguridad específico. Entre estas funciones podemos encontrar la confidencialidad de la información o la autenticación de los terminales utilizados en la comunicación.
- **Funciones de gestión de la seguridad:** Este rango de funciones se utilizan para administrar, operar y controlar los mecanismos de seguridad implementados de forma individual. Su principal función es la de realizar la interoperabilidad de los mecanismos de seguridad de diferentes redes. La gestión de claves entre dispositivos es una de las funcionalidades presentes en las redes TETRA, permitiendo implementar las medidas de protección anteriormente mencionadas, concretamente la medida de autenticación.
- **Algoritmos criptográficos estándar:** Diferentes funciones matemáticas específicas, utilizadas para la creación de claves criptográficas que permitan tener un nivel de seguridad adecuado, sin entorpecer la interoperabilidad entre sistemas.
- **Mecanismos de intercepción lícita:** Funciones empleadas para asegurar el acceso legal a la información.

Por otro lado, TETRA implementa las siguientes medidas de seguridad adicionales:

- **Cifrado de la interfaz aire (AIE):** Capaz de proteger el tráfico de voz, la señalización y la identidad en el tramo de radio comunicación (aire). Cabe destacar

que además de proteger la voz transmitida, los mensajes SDS y los datos por paquetes que se puedan transmitir, el cifrado de interfaz aire también puede proteger todas las cabeceras de voz y datos, la señalización, el registro de identidades y el anonimato de los usuarios y por último, la respuesta a ataques.

- **Deshabilitación o "muerte" de un terminal:** Posibilita que diferentes terminales perdidos no puedan ser una amenaza para la seguridad global de la red.
- **Cifrado extremo a extremo (E2EE):** Protege todos los datos y señalización en todo el tramo de comunicación, desde un *EndPoint* hasta otro *EndPoint*, incluyendo el paso por el sistema.

Estas medidas o implementaciones son propuestas por TETRA, el uso de la red no implica la necesidad de instaurar dichas medidas, sino que son recomendaciones y su uso depende exclusivamente del usuario final.

A continuación, se van a detallar diferentes implementaciones de seguridad de las que disponen las redes TETRA.

7.1. Autenticación mutua con la interfaz aérea

Una de las principales claves del estándar TETRA es que admite la autenticación mutua de una MS y la red. Esta red se suele denominar como "*Switching and Management Infrastructure*" o Infraestructura de administración y conmutación (SwMI).

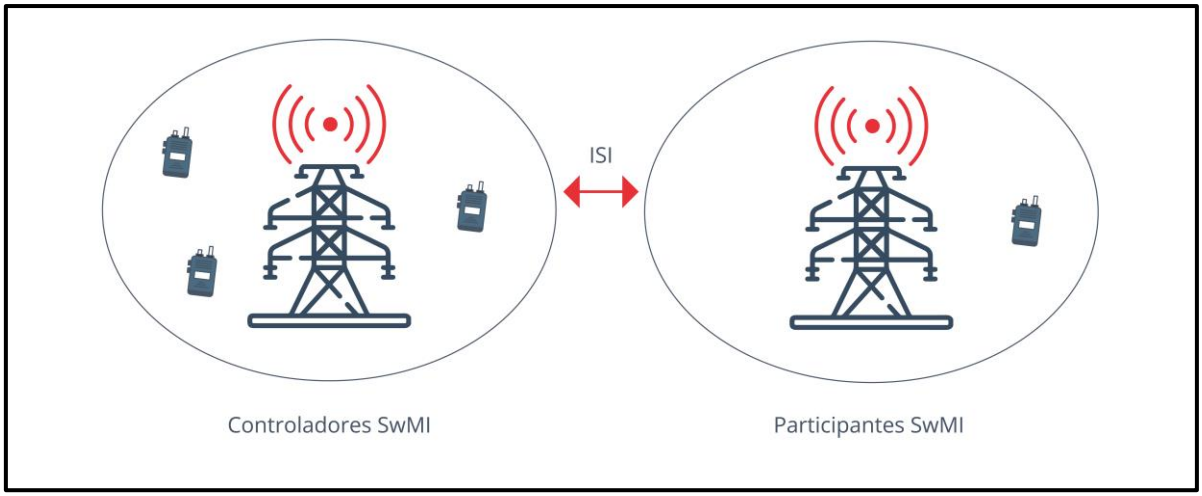


Ilustración 10: Arquitectura SwMI[10]

El control de acceso permite tener una base firme para la seguridad en general. Además, otorga las siguientes posibilidades a la hora de ser implementado en una arquitectura de comunicaciones:

- Correcto acceso desde un lugar público a la red de comunicaciones por parte de la MS y a los servicios que la red pueda otorgar.
- Implementación en el sistema de la clave de cifrado derivada (DCK) y del cifrado de clave de sesión única para garantizar la confidencialidad en la transferencia de información y asegurar la autenticación de forma óptima.
- Las claves de cifrado derivadas son compartidas entre las diferentes estaciones.

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

- Creación de diferentes canales de distribución seguros para la transmisión de información.
- Control exhaustivo de la activación y desactivación de un MS.
- Control de que los MS son legítimos y deben poder conectarse a la red.

El mecanismo de autenticación mutua (red y la estación móvil) está disponible tanto para voz como para datos y, además de las características mostradas anteriormente, también cabe destacar que la utilización de la clave de autenticación K (independiente para cada MS/SIM) implica que la K se almacenará, tanto en los MS, como en la red. Este almacenamiento se realiza en centros de autenticación o AUC.

También cuenta con la función de **modo directo (DMO, *Direct Mode Operation*)**, que no dispone de una autenticación explícita, ya que las diferentes estaciones móviles no comparten las claves entre sí a diferencia del de autenticación mutua. Para suplir esta diferencia de seguridad, se implementan las **claves de cifrado estático (SCK, *Static Cipher Key*)**, las cuales son capaces de proporcionar una autenticación mutua implícita utilizando un único conjunto de algoritmos estandarizados.

7.2. Cifrado de comunicaciones en la red TETRA

Como se ha mencionado anteriormente, la interfaz aérea tiene sus ventajas y desventajas, siendo uno de los contras más importantes la posibilidad de que un agente externo realice escuchas sobre las comunicaciones entre *EndPoints*.

En la actualidad, las comunicaciones entre dispositivos móviles inalámbricos requieren de un nivel de seguridad mínimo para las comunicaciones mediante la interfaz aérea. Con esto, se busca que diferentes medidas de seguridad aseguren la conexión entre las MS y la red. En el caso de estos dispositivos móviles, la seguridad suele venir implementada y únicamente con la seguridad de la interfaz aérea es suficiente.

En el caso de las redes TETRA, en las que se requiere un elevado nivel de seguridad, es muy común la implementación de medidas de seguridad adicionales para aumentar el nivel base de seguridad de las comunicaciones entre MS, y, entre MS y la red. Ya no es solamente necesaria la seguridad de la interfaz aérea, sino también dentro de la red. La implementación de la seguridad extremo a extremo proporciona unos valores mínimos que aseguren la integridad del sistema mediante el cifrado de las comunicaciones.

A continuación, se explican los diferentes tipos de cifrado y sus usos en una red TETRA:

- **Cifrado de la interfaz aérea:** Esta opción permite al usuario la posibilidad de cifrar la voz y los datos, mediante diferentes algoritmos de cifrado que permiten personalizar el nivel de seguridad según las necesidades del usuario. La posibilidad de cifrar a través de la interfaz aérea entre la MS y el SwMI está disponible tanto para comunicaciones grupales, como para comunicaciones de carácter individual.
  El cifrado de la interfaz aérea es de suma importancia ya que permite tener un nivel de seguridad elevado, tanto para el habla, como para los datos transmitidos entre MS. Por otro lado, el cifrado de señalización otorga protección contra el análisis del tráfico, reduciendo así, al mínimo, las posibilidades de que un agente externo a la comunicación pueda descifrar quién se está comunicando con quién y desde que zonas lo están haciendo.
- **Cifrado de extremo a extremo:** TETRA se caracteriza por tener diferentes variables en su servicio extremo a extremo, permitiendo al usuario final la capacidad

de personalizar el cifrado, para adaptarlo en mayor medida a sus requisitos. Esto permite que diferentes grupos de usuario, dependiendo de su nivel de seguridad (no es lo mismo la seguridad en el ámbito militar que en el ámbito de la sanidad), tengan la posibilidad de personalizar al máximo el cifrado extremo a extremo de acuerdo con sus propios requisitos.

- **Marco de cifrado extremo a extremo de la Asociación TETRA:** Aunque TETRA permita una elevada personalización en las comunicaciones extremo a extremo en función del nivel de seguridad que se requiera, la Asociación TETRA ha implementado soluciones estandarizadas que hacen que los usuarios finales (incluso los que tienen altos requisitos de seguridad sobre un parámetro del cifrado extremo a extremo) no necesiten especificar el resto de las características del sistema extremo a extremo.
  El Grupo de Prevención de Fraudes y Seguridad de la Asociación TETRA (*Security and Fraud Prevention Group* – SFPG) creó la Recomendación 02 para especificar al máximo nivel todas las características necesarias para que el servicio extremo a extremo sea correcto, además de especificar al detalle los algoritmos criptográficos y cómo han de implementarse.
  La primera implementación utilizó el Algoritmo Internacional de Cifrado de Datos (IDEA). Posteriormente, en una segunda implementación, se añadió el Estándar de cifrado avanzado (AES), aunque no haya un algoritmo estándar definido por la SFPG, suelen usarse los siguientes:
    - **AES-128:** Adoptado como el algoritmo de cifrado predeterminado de TETRA.
    - **AES-256:** Empieza a implementarse por algunos fabricantes de terminales ya que proporciona un mayor nivel de seguridad cuando se busca un elevado nivel de confidencialidad.

  Estos algoritmos en múltiples ocasiones se ven relevados por la implementación de algoritmos de dominio público con características similares pero confeccionados de forma más personalizada y que son totalmente válidos para el cifrado extremo a extremo de una comunicación en la red TETRA.
  El uso de algoritmos de dominio público está basado en la disponibilidad de MS y en las soluciones de gestión de claves de varios fabricantes. En general, el marco ha sido diseñado para adaptarse a una variedad de políticas de seguridad, y la flexibilidad se logra a través de una serie de opciones de operativa simple. La obtención de copias de las recomendaciones está disponible en la Secretaría del SFPG[11].
- **Anonimato de usuarios:** El estándar TETRA permite que no solo las comunicaciones entre usuarios sean cifradas, sino que también incorpora diferentes mecanismos para asegurar el anonimato de los usuarios que están transmitiendo datos o voz a través de la red. Existe la posibilidad de implementar un cifrado dinámico para cifrar las identidades individuales y grupales de los usuarios. Además, la característica “dinámico” proporciona la capacidad para cifrar de diferentes formas en diferentes ocasiones a un mismo usuario, asegurando así la integridad del usuario.

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

7.3. Funciones de gestión de seguridad – Claves de cifrado

Aunque las redes TETRA implican la utilización de funciones de seguridad integradas en el sistema, esto no garantiza que el sistema sea totalmente seguro, aunque si limita sobre qué elementos puede existir una vulnerabilidad.

La gestión de seguridad en las redes TETRA, en general, se ocupa de que las funciones de seguridad se gestionen correctamente, pero también se ocupa de que los diferentes mecanismos se integren de la forma adecuada y de que la interoperabilidad entre sistemas TETRA de forma segura sea efectiva.

Uno de los puntos vulnerables de las redes TETRA es la gestión de las llaves o claves de seguridad, las cuales contienen la información secreta que se utilizará para dar acceso al sistema o para descifrar la información cifrada. La gestión de estas claves es de suma importancia, tanto o más que cualquier otro mecanismo de seguridad implementado en la red. Según la TETRA Association SFPG[12] la funcionalidad y la flexibilidad son palabras claves a la hora de gestionar las claves, al igual que en el marco de cifrado extremo a extremo, donde ha elaborado diferentes recomendaciones para apoyar a la gestión de la seguridad, en especial a la gestión de claves.

A continuación, se van a detallar diferentes tipos de claves y sus funcionalidades en el uso de las redes TETRA:

- **Clave de autenticación:** La clave de autenticación K, es la clave empleada para la autenticación mutua entre una MS y el SwMI. El estándar TETRA define en su normativa tres posibilidades a la hora de generar esta clave: una función para un usuario fijo de una clave de autenticación, la posibilidad de que un usuario ingrese un código de autenticación y una combinación de ambos. Además, en la mayoría de los sistemas, se requiere que una MS almacene la clave K o la clave UAK, debido a la dificultad de ciertos sistemas en el almacenamiento de claves con códigos largos.
- **Claves para el cifrado de la interfaz aérea:** En este aspecto, existen diferentes tipos de claves de cifrado. Hay posibilidad de que las claves se envíen mediante la interfaz aérea a los MS con *Over The Air Re-Keying* (OTAR), directamente en el proceso de autenticación o encontrarse precargadas en los MS.
  Estas claves pueden tener diferentes rangos de vida, tanto a largo como a corto plazo, siendo posible introducir mecanismos para proteger las llaves con una vida útil muy larga.
  Dentro de las claves de cifrado de la interfaz aérea encontramos las siguientes claves específicas y que se han mencionado anteriormente:
  - **Clave de cifrado derivada (DCK):** Permite el cifrado entre la red y la MS de forma individual. La derivada se realiza durante el proceso de autenticación. La característica mencionada anteriormente, también implica que, durante una llamada de voz, en comunicaciones desde la MS a la red (descendente) o desde la red a una estación móvil (ascendente), se pueda proporcionar una autenticación implícita.
  - **Clave de cifrado común (CCK):** Generada y distribuida por el SwMI. Se cifra mediante el DCK a cada una de las estaciones móviles. Cuando la clave de cifrado común se distribuye a una estación móvil a través de la interfaz aérea, se utilizar el mencionado proceso de OTAR. Además, la CCK

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

se cifra con la DCK de la propia MS. Este tipo de clave es muy común para grupos de MS distribuidos o para áreas de ubicación (LA).

- **Clave de cifrado de grupo (GCK):** Esta clave tiene su vinculación asociada a un grupo de usuarios muy específico. Al igual que en la CCK, para la GCK, la clave se genera mediante el SwMI y se distribuye a las MS de un grupo. En un mismo LA, el GCK se combina con el CCK para conseguir un algoritmo especial y específico denominado "Clave de Grupo Específico" o MGCK que es utilizado para cifrar los mensajes del grupo creado anteriormente. En un caso más específico, en el que el GCK se distribuya a una MS a través de la interfaz aérea usando OTRA, la comunicación se cifraría con una clave de sesión derivada de la clave de autenticación para dicha MS.
- **Clave de cifrado estático (SCK):** Esta clave es la clave predeterminada de la red TETRA si se utiliza cifrado. No requiere de autenticación previa.

  El significado de la calificación estática radica en que su valor no se modifica por otro mecanismo de seguridad. TETRA permite el uso de hasta 32 claves SCK en una misma MS, lo que posibilita bastantes comunicaciones. SCK es compatible con sistemas en grupo y con sistemas que usen DCK y CCK como alternativas.
  En el caso de que se esté utilizando una comunicación en modo directo o DMO, las claves SCK se podrían agrupar con varios grupos de usuarios.

La utilización de estas claves queda a decisión del usuario final. Un uso indebido de alguna clave podría permitir a un agente externo atacar a la red TETRA.

7.4. Clases de seguridad en una red TETRA

TETRA contempla las siguientes clases de seguridad que permiten clasificar la seguridad de cifrado de la interfaz aire:

Clase	Cifrado	OTAR	Autenticación
1	No	No	Opcional
2	Clave estática	Opcional	Opcional
3	Clave dinámica	Obligatorio	Obligatorio
3G	Clave dinámica	Obligatorio	Obligatorio

Tabla 2: Clases de seguridad en redes TETRA

- **Clase 1:** Esta clase es la más insegura de todas y no otorga la posibilidad de ningún tipo de cifrado ni de la llamada *Over The Air Re-Keying*. Únicamente posibilita la opción de incluir un mecanismo de autenticación.
- **Clase 2:** Las claves SCK (hasta un máximo de 32) se cargan en todos los terminales de la red. Suelen estar almacenadas o por un largo período de tiempo o de por vida. Esta clase suele operar siempre en el ya mencionado servicio de Modo Directo o DMO. También se suele usar estar clase cuando se implementa una estación base trabajando de manera aislada.
- **Clase 3:** Implica a las claves dinámicas (DCK). Estas se generan automáticamente a partir de la clave interna del terminal, con cada autenticación y se usan de forma

individual en las comunicaciones entre terminal y estación base. La comunicación "descendente" se cifra con la clave CCK, la cual ha sido previamente cargada por aire (OTAR).

- **Clase 3G:** Esta clase es una similar a la Clase 3. Su única diferencia radica en que se puede aplicar para grupos, por lo que se sigue usando la clave DCK para comunicaciones ascendentes, la clave CCK para señalización y la clave GCK para cada grupo. Al igual que en la Clase 3, las claves son cargadas con OTAR.

Para hacerse una idea de la seguridad del cifrado de interfaz de aire en una Clase 3, las claves poseen una longitud de aproximadamente 80 bits, lo cual permite a la red generar hasta 1,2x10^24 claves. Esto supone, que, con los mecanismos actuales, se necesiten aproximadamente cuatro millones de años en descifrar una clave.

7.5. Deshabilitación de terminales TETRA

La deshabilitación de un terminal en caso de pérdida o robo es una medida de seguridad crucial, ya que un terminal extraviado puede suponer una amenaza de seguridad para la integridad del sistema TETRA.

TETRA permite gracias a esta opción:

- La finalización de la actividad del terminal como radio.
- El borrado permanente de las claves, incluida la clave secreta que permite la autenticación del dispositivo.
- La opción "Deshabilitación temporal" realiza un borrado de las claves de tráfico, pero permite realizar una escucha ambiente de corto alcance.
- Una respuesta rápida ante la pérdida o robo del dispositivo.

Este proceso de deshabilitación de terminales TETRA, se ve supeditado al control de exportación que se explicará más adelante, pero por el que todo fabricante deberá solicitar permiso para la exportación de un dispositivo que tenga esta opción dentro del sistema.

7.6. Algoritmos criptográficos estándares de cifrado de interfaz aire

TETRA es un estándar capaz de proporcionar diferentes algoritmos criptográficos para diferentes propósitos, aunque también permite la no utilización de alguno de estos algoritmos para crear una red sin seguridad. Existen diferentes recomendaciones para la creación de las redes TETRA para tener un nivel de seguridad mínimo dependiendo de la funcionalidad de la red.

A mayores de los cifrados disponibles para la interfaz aérea, TETRA también admite algoritmos alternativos creados por usuarios independientes y externos. Estos algoritmos solo serán válidos si cumplen con unos requisitos mínimos impuestos por TETRA y siempre que el usuario final acepte usar dichos algoritmos en detrimento de poder perder el apoyo de diferentes proveedores.

TETRA tiene en cuenta varios requisitos para especificar los algoritmos estándar, entre estos requisitos pueden destacarse:

- **La necesidad de diversidad:** ante una gran cantidad de aplicaciones y redes TETRA, existe la posibilidad de que no todos los usuarios del estándar quieran compartir de forma pública los algoritmos de cifrado, por lo que, en ciertos casos,

como podrían ser diferentes Organizaciones Europeas de Seguridad Pública, se requiere de un algoritmo de cifrado de interfaz aérea estándar propio, diferente a cualquier algoritmo estándar. Esto asegura que el cifrado sea totalmente independiente de cualquier otra asociación, suponiendo un aumento sustancial de la seguridad de la red en caso de estar cifrada.

- **Reglamento de control de exportaciones:** La mayoría de los dispositivos que incluyen algoritmos de cifrado están sujetos a los controles de exportación específicos de cada país. Según el Acuerdo de Wassenaar, en la Categoría 5[13], parte 2, se puede revisar toda la política de control de criptografía para los principales países industriales.

  En TETRA, existen cuatro algoritmos de cifrado estándar para los sistemas de una arquitectura. Estos algoritmos han sido desarrollados por el Grupo de Experto en Algoritmos de Seguridad (SAGE) de ETSI.

- **TEA1**: Generalmente este algoritmo está contemplado para ser exportable fuera de Europa, lo cual ha generado una gran afinidad por diferentes entidades de Seguridad Pública de varios países, así como de muchas empresas del sector privado, las cuales requieren de un nivel de seguridad importante.
- **TEA2**: Su uso solo está permitido en organizaciones de Seguridad Pública en Europa y por lo tanto, tienen un control de exportación muy elevado.
- **TEA3**: Utilizado para la Seguridad Pública y Organizaciones Militares en diferentes lugares donde TEA2 no está permitido (fuera de Europa). También tiene un control de exportación muy restrictivo, aunque si está permitido su uso fuera de Europa, en ciertos casos muy concretos.
- **TEA4**: Está diseñado para un uso en ámbitos fuera de la Seguridad Pública. Su uso es mínimo, siendo el algoritmo menos utilizado de los anteriormente mencionados.

Estos algoritmos son de exportación restringida y están controlados por la normativa definida en el mencionado Acuerdo de Wassenaar de 1998[14]. Estos algoritmos son propiedad de la ETSI a excepción del TEA2.

Cabe destacar que estos algoritmos poseen una gran resistencia ante intentos de ruptura, pero el avance de las tecnologías puede traer consigo nuevas formas de superar esta resistencia y vulnerar los datos cifrados. En todo caso, se debe prestar atención a la configuración de los sistemas y al cifrado empleado, intentando personalizar al máximo la configuración de seguridad con la arquitectura que se vaya a utilizar.

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

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

8. Requerimientos de seguridad en aplicaciones empresariales

Con lo mencionado anteriormente, en cuanto a las funcionalidades y capacidades de seguridad proporcionadas por TETRA, cabe destacar que la mayor parte de las redes TETRA existentes son del mundo IT, ya que para entornos OT las funcionalidades de seguridad son mínimas.

A lo largo de este apartado se hará referencia, principalmente, al mundo OT y a las implementaciones y requerimientos de seguridad para este sector.

Se ha de recordar que cada instalación OT es un mundo, por lo que es importante investigar nuestra red y observar qué puede o no ser conveniente desactivar. Se sugiere activar como mínimo la seguridad de clase 2 en la red industrial, anteriormente explicada en el apartado "Clases de seguridad en una red TETRA", con la autenticación de los elementos activos junto a la posibilidad de desactivar los terminales y la posibilidad de cifrado en la interfaz aérea.

Se deberá segmentar la red de acuerdo con diferentes conceptos normativos industriales, como por ejemplo el **PERA** (*Purdue Enterprise Reference Architecture*), consiguiendo agrupar y aislar los activos, además de controlar el flujo de comunicación entre ellos.

Se cifrará la información enviada por los dispositivos en las diferentes capas correspondientes a los niveles 2 y 3, es decir, de enlace y de red.

La segmentación de los diferentes usuarios que podamos encontrar dentro de nuestra red TETRA deberá hacerse buscando la separación entre grupos, pero también la posibilidad de conexión entre ellos si fuese necesario. Crearemos los grupos para los diferentes puestos de trabajo, es decir, un grupo de limpieza, otro de técnicos, etc., y, dentro de ellos, crearemos otro grupo para diferenciar entre trabajadores, personal autorizado, llamadas de importancia elevada, etc.

Además, se realizará un control de acceso al medio. Para ello, se usarán algunas de las técnicas conocidas para telecomunicaciones que se presentan a continuación:

- **ALOHA:** Diseñado por la Universidad de Hawái como método de acceso a radio-enlaces en 1970, actualmente en desuso. Su principal característica ha sido *Free for All*, es decir, si una estación tiene una trama para enviar, la envía directamente. El medio es compartido por todas las estaciones. Otras características son:
  - los nodos utilizan un canal compartido;
  - si se solapan transmisiones, estas colisionan;
  - el nodo destino confirma las tramas correctas;
  - sí un nodo no recibe la confirmación ACK, se determina la conexión como *timeout* y se supone que la trama ha colisionado;
  - si no se recibe ACK, la trama se reenviará un número limitado de veces.

  Como ALOHA solo dispone de un único canal para compartir, hay posibilidades de colisión entre tramas de estaciones diferentes. En el siguiente ejemplo se muestran 4 estaciones enviando 8 tramas en total, de las cuales únicamente 2 tramas sobreviven:

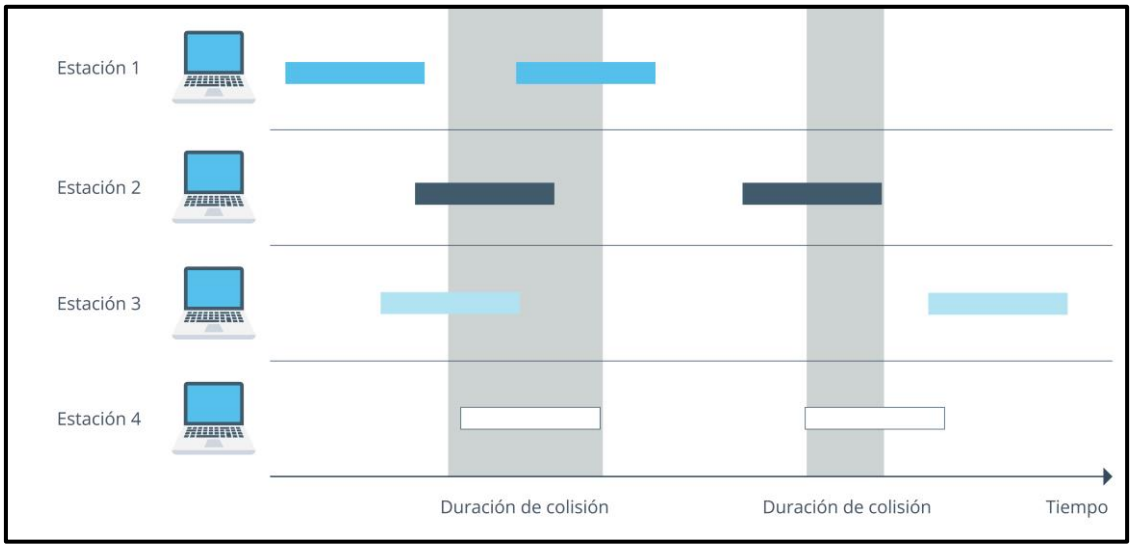


Ilustración 11: Envío de tramas con el protocolo ALOHA[15]

En él, se pueden observar los siguientes resultados:

- hay cuatro estaciones tratando de transmitir;
- cada estación ha enviado dos tramas;
- concretamente, seis tramas entran en conflicto y únicamente la primera trama de la primera estación y la segunda trama de la tercera estación sobreviven;
- las tramas en conflicto deberán ser reenviadas;
- aunque un solo bit de la trama coincida con el tiempo de duración de la colisión, la trama colisionará y deberá ser reenviada.

Para eliminar el proceso de reenvío de tramas y mejorar la comunicación, se diseñó e implementó el ALOHA Ranurado, el cual evitaba las colisiones entre tramas definiendo los tiempos de envío.

- **CSMA:** El CSMA o *Carrier Sense Multiple Access* es un protocolo de acceso al medio que reduce la probabilidad de conexión, aumentando así el rendimiento de la comunicación. Esto se debe a que las estaciones realizan escuchas antes de la transmisión, para conocer el estado del canal y saber si pueden o no transmitir, reduciendo así las probabilidades de colisión, pero no eliminándolas por completo, debido a la propagación de la señal en el medio compartido a lo largo del espacio y tiempo.
  Dentro de CSMA hay tres modos de persistencia, como se puede ver en la siguiente imagen:

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

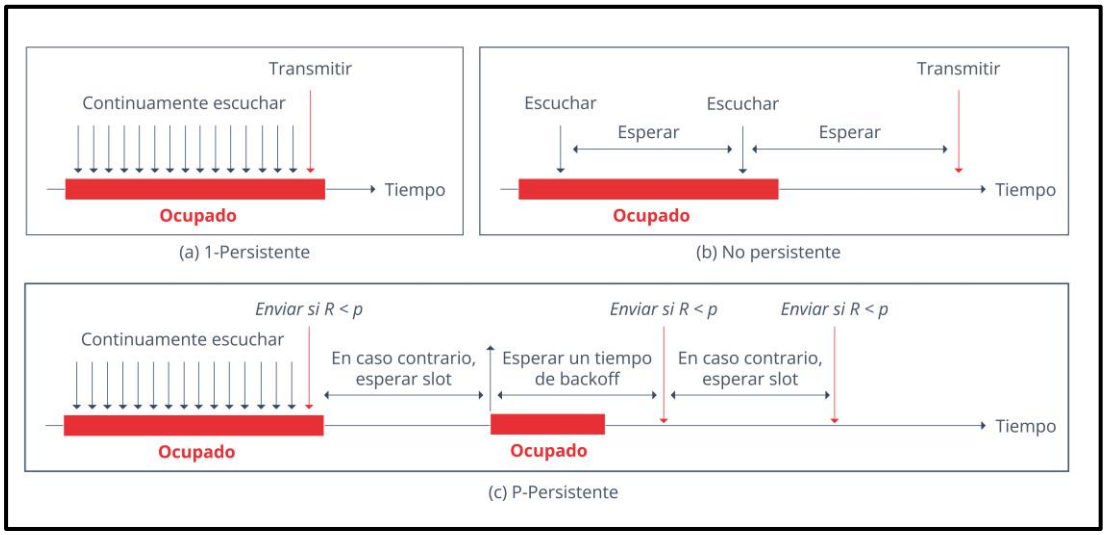


Ilustración 12: Tipos de persistencia en CSMA[16]

A parte de las características definidas anteriormente, CSMA mejora sus prestaciones mediante variables del protocolo, como las siguientes:

- **CSMA/CD**: *Carrier Sense Multiple Access with Collision Detection,* es una variante del protocolo que define el proceso a seguir en caso de colisión y realiza escuchas tras el envío de las tramas para ver si la transmisión ha sido exitosa. Además, para mejorar los envíos, CSMA/CD tiene una restricción del tamaño de la trama.
- **CSMA/CA**: *Carrier Sense Multiple Access with Collision Avoidance,* es otra variante del protocolo enfocado para redes inalámbricas.

- **FDMA:** El FDMA o Acceso Múltiple por División de Frecuencia, es una técnica de multiplicación usada en múltiples protocolos de comunicaciones. Este protocolo controla el acceso al medio, que se realiza dividiendo el espectro disponible en canales, los cuales corresponden a distintos rangos de frecuencia, asignando estos canales a diferentes usuarios y comunicaciones a realizar, sin interferencias entre ellos. Entre sus características más relevantes, encontramos:
  - fácil implementación en sistemas de radio,
  - gestión de recursos rígidos y poco apta para flujos de tránsito variable,
  - necesidad de un duplexor de antena para transmisión dúplex,
  - asignación individual de canales por usuario,
  - asignación dependiente de la demanda.

- **TDMA:** De sus siglas en inglés *Time Division Multiple Access*, este protocolo representa el acceso múltiple por división de tiempo y es el protocolo más utilizado en TETRA. Dicho protocolo ya ha sido explicado en detalle en el apartado *Acceso Múltiple por División de Tiempo*. Consiste en el acceso múltiple por división de tiempo, que permite múltiples conversaciones compartiendo el mismo canal de radio, siendo esta una de las características principales de TETRA. Si deseas

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

conocer más sobre el tema de radio móvil digital o acerca del funcionamiento del TDMA, puedes obtener esa información en el artículo "Radio Móvil Digital en la industria 4.0"[17].

[17] https://www.incibe-cert.es/blog/radio-movil-digital-industria-40

9. Funcionalidades reales de seguridad

A lo largo de este apartado se van a explicar y definir algunas funcionalidades reales de los dispositivos TETRA, ya que las funcionalidades de seguridad definidas anteriormente son posibilidades teóricas otorgadas por el estándar, que no muchos dispositivos tienen a su alcance o que su implementación puede implicar un elevado precio de compra.

Este apartado va a hacer referencia a las posibilidades reales de seguridad proporcionadas por el protocolo TETRA para una radio concreta (no se especifica ni marca, ni modelo, por normativa de seguridad). A continuación, se detallan las características reales del dispositivo:

- **TEI:** El *Terminal Equipment Identity* es un número identificativo de la radio, establecido por la empresa encargada de la fabricación del dispositivo y nunca se puede modificar. Esta característica proporciona la identificación de dispositivos de forma segura.
- **PIN/PUK *User Authentication*:** El PIN (*Personal Identification Number)* y el PUK (*PIN Unblocking Key*) son características muy comunes en los dispositivos móviles, para la autentificación cada vez que se enciende el dispositivo. En caso de fallar en la introducción de los cuatro dígitos del PIN un número determinado de veces, el dispositivo se bloqueará y solicitará el PUK para la autenticación del usuario.
  Tanto el código, como el número de intentos vienen definidos en el *codeplug* o archivo de configuración.
- **Secure DMO:** Este método permite a la radio comunicarse por modo directo con cifrado por clave. Cuando los SCK son otorgados por el OTRA, la radio indicará si contiene las claves correctas, en caso negativo, esta emite un mensaje indicando 'OTRA incompleto'.
  Esto permite saber de forma correcta si la comunicación directa es correcta y segura.
- **Radio *Disable/Enable*:** Esta característica que solo poseen algunas radios de las redes TETRA permite a un controlador general activar o desactivar el funcionamiento de la radio. En caso de que la funcionalidad esté desactivada, la radio no podrá participar en ninguna llamada de voz e ignorará el resto de los servicios.
  Existe un caso especial en el que, si el dispositivo está en modo desactivado, pero recibe una subscripción TETRA con el correcto SSI y MNI, la radio volverá a su estado activo.
- **Radio *Permanent Disable*:** Esta funcionalidad permite desactivar por completo una radio para, por ejemplo, proteger a la red de un ataque desde otra radio o de la propia radio infectada. Cabe destacar que si se activa el modo *Permanent Disable,* la radio se volverá inoperable. Esta característica también puede ser utilizada por un atacante para inhabilitar los diferentes terminales uno a uno y cancelar las comunicaciones, es por ello, que se debe prestar especial atención a su configuración, y que su funcionalidad solo se active mediante unas claves de seguridad.
- **SIM Security**: La seguridad de la SIM consta de los siguientes grupos de funciones de seguridad:
  - E2EE de voz y gestión de claves relacionada;

- parámetros de acceso a la red y autenticación;
- gestión de claves para AIE;
- OPTA, modificación, cifrado y transferencia;
- AES para E2EE de interfaz SIM y autenticación SIM-terminal.

La SIM es una tarjeta de circuito integrado que contiene un sistema de archivos y una aplicación. La aplicación realiza las siguientes acciones:

- generación de segmentos de flujo de claves (KSS);
- sincronización para E2EE;
- algoritmo de autenticación TETRA basado en la clave K de la SIM;
- gestión de claves para las claves E2EE;
- cifrado y autenticación de la interfaz SIM mediante AES.

- ***High Assurance Boot*:** La radio dispone de un elemento que garantiza que el código y los datos que aparecen en la radio son auténticos y no han sido alterados.
  - El *hardware* obliga al módulo HAB a ejecutarse en el momento del arranque;
  - el módulo comprueba si todo el *software* procede de una fuente de confianza;
  - la radio comprueba la firma de los segmentos de código y los datos presentes en la radio mediante un mecanismo de clave pública/privada. Si falla la autenticación HAB del *software flasheado*, no permite que se ejecute el *software* de la radio.

10. Mitigación de vulnerabilidades

Las infraestructuras TETRA usadas en el ámbito industrial, o de transporte, fueron diseñadas y desplegadas hace unos veinte años y unos quince años respectivamente. En aquel momento el nivel de concienciación sobre ciber amenazas era menor al de hoy en día, a esto se añadía que no existía la disponibilidad pública de herramientas para el análisis de seguridad y/o ataque a estas redes, por lo que el riesgo percibido era bajo. Todo ello supuso que, para simplificar la implantación y las complejidades asociadas a la gestión de seguridad, no se aprovecharan todas las funciones de seguridad que ofrece el estándar TETRA.

En la actualidad, estas redes están en funcionamiento en aplicaciones críticas de diferentes negocios y sectores. Las operativas normales se encuentran perfectamente funcionales, pero no es fácil aplicar las medidas de seguridad presentadas en el capítulo previo "Securización de redes TETRA", es por ello que se podría ver afectada esta operativa, o incluso tener un coste importante.

La implantación de una red de comunicaciones segura ya sea manteniendo TETRA o implantando alguna de sus alternativas suele ser un proyecto a largo plazo que depende de un estudio pormenorizado de impacto y costes (Véase *Combinación del sector privado y público junto con las redes TETRA* para cuantificar gastos")

Ante esta situación, existe la posibilidad de implementar transitoriamente algunas estrategias mitigatorias, en las que es posible mantener parte de la infraestructura actualmente en uso, al mismo tiempo que se irán añadiendo funciones de seguridad con un bajo impacto. Estas han sido divididas en: 'mitigaciones técnicas', aquellas que afectan a la configuración de la propia tecnología; y 'mitigaciones operativas', aquellas acciones que se pueden tomar para minimizar el impacto en la contingencia de que el sistema TETRA implantado pueda ser vulnerado.

10.1. Mitigación técnica

En la mayoría de las redes en el ámbito industrial, se consideran criticas la integridad y la disponibilidad de las comunicaciones, mientras que la **confidencialidad** de las comunicaciones **no es una funcionalidad esencial**, aunque sí **deseable**.

En estos casos, se debe al menos utilizar la autenticación mutua entre TE y SwMI, mediante el mecanismo de autenticación. Esta solución tiene la ventaja de que la autenticación suele estar soportada por todos los equipos y redes, al contrario que el cifrado TEA (*Tiny Encryption Algorithm*) 1/2/3/4, que suele requerir de licencias específicas o tener limitaciones de uso. La **autenticación, por tanto, estará disponible sin necesidad de sustituir equipos o de actualizar licencias**. Limitando de forma importante la capacidad de interferencia ilícita en las comunicaciones.

Como complemento a la autenticación, o en aquellos casos en que por cualquier razón no sea posible aplicarla, es posible utilizar la funcionalidad de **listas negras** y **listas blancas** de identidad de equipo de usuario (TEI), de forma que la red solo permita la asociación de equipos permitidos. Si bien el TEI puede ser modificado por un atacante lo suficientemente avanzado, en general, los equipos TETRA suelen tener un TEI único que requiere de

herramientas a nivel de laboratorio y mantenimiento, no siempre fácilmente accesibles. Además, el identificador TEI es menos accesible que los identificadores ISSI. Por tanto, las listas negras y blancas pueden ser una medida eficaz contra atacantes menos sofisticados.

Aquellas aplicaciones que requieren confidencialidad de datos permiten optar por el cifrado extremo a extremo, por ejemplo, las que manejen información de carácter personal especialmente protegida, ya sean tanto datos médicos o actividades que deban permanecer confidenciales, como las comunicaciones del personal de seguridad y vigilancia. Esto permite mantener una red ***legacy*** (integra) sin necesidad de cambios ni *downtime* (períodos de mantenimiento o inhabilitación de las prestaciones proporcionadas por la red), al mismo tiempo que se otorga a los grupos de usuarios críticos de terminales la capacidad de operar con grupos cifrados, manteniendo la compatibilidad e interoperabilidad en grupos en claro con el resto de los usuarios.

También es importante recordar que una red que permite el cifrado a nivel aire no suele requerir que este se encuentre en uso para todos los terminales y grupos, simplemente indica que soporta la posibilidad de cifrado. Esto hace posible realizar un plan de migración de forma progresiva, primero con la identificación de los usuarios que pueden requerir de confidencialidad y, posteriormente, proporcionando las claves criptográficas y el cifrado de grupos para estos usuarios.

En los usos de TETRA para la transmisión de datos de redes OT, como SCADA, existen también una serie de mitigaciones específicas.

Las **aplicaciones basadas en SDS** deberían incorporar una **capa propia de cifrado a nivel aplicación** basado en algoritmos robustos reconocidos por la industria (por ejemplo, AES), y con una implementación segura que otorgue tanto confidencialidad, como autenticación, además de protección contra replay. Esta capa, además, funcionaría como un sistema extremo a extremo, protegiendo desde el equipo PLC hasta el controlador SCADA. De esta forma, la información viaja siempre cifrada, tanto en el interfaz aire, como en la red SwMI.

Las aplicaciones que hacen uso de datos IP encapsulados sobre SNDCP (*Sub Network Dependent Convergence Protocol*) deberían implementar igualmente el cifrado, bien sea mediante el cifrado del payload en las comunicaciones, o mediante el uso de protocolos de VPN de bajo overhead, como IPsec en Transport Mode.

10.2. Mitigación operativa

La mitigación operativa incluye aquellos procedimientos de trabajo que suplen las deficiencias de redes de comunicación TETRA basadas en la forma en la que los usuarios utilizan la tecnología. Esto permite implementar mejoras sin necesidad de afectar a las configuraciones *software* o *hardware*, tales como terminales o SwMI.

Las **mitigaciones operativas** responden principalmente a tres tipos de vulnerabilidades, las que afectan a la **confidencialidad** de la información transmitida, las que afectan a la posible **integridad** de las comunicaciones y las que se derivan de la perdida de **disponibilidad** de las comunicaciones.

10.2.1. Mitigaciones a la ausencia de confidencialidad en redes TETRA.

Aunque por norma general la mayoría de las comunicaciones de una instalación industrial no requieren de especial secreto, existen algunas situaciones en las que es importante preservar la confidencialidad de la información transmitida. Cuando la red TETRA no dispone de cifrado en interfaz aire o E2EE, es posible adoptar algunas medidas compensatorias.

- **Uso de lenguaje convenido:** Es un procedimiento tradicional en redes de radio abiertas (analógicas) que suplía esta deficiencia. Es especialmente práctico en comunicaciones de seguridad, como puede ser la vigilancia de las instalaciones. **En el lenguaje convenido, la designación de las personas, ubicaciones habituales y situaciones cotidianas se codifica mediante palabras clave convenidas de antemano y usadas de forma habitual**. En muchas ocasiones incluso estos procedimientos permanecen en uso en redes TETRA por cuestiones históricas o porque aporta un lenguaje formal e inequívoco a las comunicaciones profesionales. De esta manera, ante una escucha ocasional se limita el aprovechamiento que pueda hacerse del acceso a comunicaciones. En un ejemplo de lenguaje convenido, un vigilante que acaba de regresar de su ronda perimetral a su puesto de vigilancia estático podría codificarse mediante lenguaje convenido como “Oscar-3 pasa a situación Azul en punto Mike”.
- **Uso de comunicaciones alternativas seguras para transmitir detalles concretos que requieren confidencialidad:** Determinadas comunicaciones como datos personales de clientes o usuarios, detalles concretos de la operativa normal de negocio, etc., pueden requerir de privacidad, tanto frente a actores externos maliciosos, como a aquellos trabajadores que no estén directamente involucrados en la operativa realizada. En estos casos una **medida mitigatoria es la realización de una comunicación directa por un medio alternativo que ofrece más privacidad**. En el argot de radio tradicional suele conocerse como “realizar línea baja” e implica realizar una llamada telefónica (que en telefonía analógica se considera línea de baja frecuencia, frente a la frecuencia muy alta de las comunicaciones de radio VHF/UHF). Actualmente las comunicaciones privadas pueden usar medios distintos del telefónico, como aplicaciones de móvil de mensajería, videollamada u otros medios. Este procedimiento además aumenta la agilidad de las comunicaciones al dejar libre el grupo de usuarios de conversaciones largas como pasar una lista de datos personales, o que requieran un intercambio largo de comunicaciones como discutir la solución una problemática en la actividad de la empresa.

10.2.2. Mitigaciones a la ausencia de integridad en redes TETRA.

En los casos en los que un atacante consigue hacerse con un equipo funcional, ya sea por pérdida, robo o porque es capaz de suplantar a un terminal válido, existe el riesgo de que la integridad de las comunicaciones se vea afectada. El atacante puede introducir tanto comunicaciones de voz, como de datos, dando órdenes falsas, afectar a la confianza sobre ordenes verdaderas o simplemente causar molestias en las comunicaciones.

En **entornos críticos, esta eventualidad debe tenerse en cuenta en los planes de emergencia, incorporando un procedimiento para validar órdenes confusas o dudosas**.

Así, por ejemplo, ante una orden dudosa, puede solicitarse al interlocutor que se comunique por un método alternativo, que pida a un tercero confiable que confirme su orden o comunicación, que verifique su identidad mediante el conocimiento de detalles que solo un trabajador debería conocer, o bien una combinación de las anteriores.

10.2.3. Mitigaciones a la pérdida de disponibilidad de comunicaciones TETRA.

En muchos entornos industriales, o de infraestructuras críticas, la función de comunicaciones de voz y datos mediante la red TETRA forma parte de los medios esenciales para la continuidad del negocio. Sin posibilidad de comunicación entre los operarios, las actividades deben suspenderse o quedar fuertemente degradadas. La red TETRA puede dejar de estar disponible de forma total o parcial, o bien puede ser objeto de una caída de servicio accidental o derivada de atacantes externos.

En entornos críticos se utiliza la metodología PACE para designar los sistemas de comunicación preestablecidos, en función de la disponibilidad de comunicaciones y de la situación en la que se utilizan.

PACE es un acrónimo de Primario, Alternativo, Contingencia y Emergencia. PACE designa el orden en el que un usuario se moverá a través de los sistemas de comunicación disponibles, hasta que pueda establecerse el contacto. Idealmente, cada método será completamente separado e independiente de los otros sistemas de comunicación. Para cada método, la persona que desea comunicar debería intentar en varias ocasiones establecer contacto y si no es posible pasar a la siguiente opción.

Un plan de comunicación basado en PACE existe para una misión o tarea específica dentro de la organización no debe ser el mismo obligatoriamente para todos los trabajadores. El plan debe considerar el intercambio de información, tanto dentro de grupos de trabajo, como con los superiores jerárquicos. Una organización puede tener múltiples planes para diferentes situaciones, actividades y/o entidades externas. Aunque, por simplificar, puede ser común si se observa que el plan PACE único tiene la suficiente flexibilidad.

Un plan PACE no es un plan de frecuencias (que detalla la asignación de frecuencias y las características del espectro radioeléctrico de la red en uso) ni un plan de grupos o flotas de usuarios (ya que toda la red podría estar inoperativa).

El sistema del plan PACE se expresa como una **lista de orden de precedencia de las comunicaciones**: primario, alternativo, de contingencia y de emergencia. El plan designa el orden en el que un grupo de usuarios se moverá a través de los sistemas de comunicación disponibles hasta que se pueda establecer el contacto. El plan no designa otros factores, como el canal de radio exacto o el grupo de conversación que se utilizará si se usa una radio, sino el orden en el que se planea usar la radio y el método acordado de comunicaciones entre grupos.

Los responsables de la gestión de emergencias y de las comunicaciones deben coordinar el desarrollo de planes PACE para las diferentes funciones y departamentos de su organización, con el fin de garantizar que el mando del incidente pueda mantener los enlaces de comunicación críticos. **Los planes PACE departamentales deben coordinarse con la Gestión de Emergencias y el Departamento de Comunicaciones**. Es fundamental que los departamentos individuales aniden su plan dentro del Plan de

Emergencia más amplio, para asegurar que la organización tenga los recursos para ejecutar el plan y reducir la duplicación innecesaria de activos. El desarrollo de planes PACE exhaustivos no garantizará unas comunicaciones perfectas en una catástrofe, pero puede ayudar a despejar algunos problemas que se encuentran en todas las situaciones de emergencia.

Los elementos del plan PACE suelen tener los siguientes ámbitos:

- **Primario:** El método de comunicación habitual en situación normal de trabajo, en el caso que nos ocupa normalmente será la red TETRA.
- **Alternativo:** El método de comunicación a utilizar si el anterior no está disponible, pero la actividad normal de la operativa de trabajo no se ha visto afectada.
- **Contingencia:** El método de comunicación a emplear si ambos sistemas previstos no están disponibles. Habitualmente, si se da esta situación, también es previsible que existe una afectación colateral a la operación normal de las instalaciones.
- **Emergencia:** Implica un desastre de tal magnitud que todos los medios de comunicación anteriores se han perdido y probablemente debe suspenderse toda actividad laboral y centrarse en la autoprotección o asistencia a afectados.

En base a lo anterior, un ejemplo de plan PACE para una instalación industrial del tipo planta química, en la que el medio de comunicación principal es la red TETRA, podría ser el siguiente:

- **Primario:** *Red TETRA*. Operación normal en la planta.
- **Alternativo**: *Red de telefonía fija VOIP*. Los operarios dispondrán de una red lo suficientemente amplia de teléfonos fijos VOIP en toda la planta, que le permitan comunicar entre puestos de trabajo o con la sala de control.
- **Contingencia**: *Telefonía móvil*. Todos los sistemas de comunicación propios de la planta están inoperativos. La sala de control dispone de un teléfono externo con línea directa contra el operador de telefonía o de un teléfono móvil. Todos los operarios conocen el número de la sala de control y puede llamar con su terminal corporativo, su terminal personal o a través de telefonía fija tradicional tanto de la propia planta como de sus proximidades.
- **Emergencia**: *112*. La instalación se ha visto afectada por un desastre de grandes proporciones, con afectación a todos los sistemas de comunicaciones corporativos. Por ejemplo, la propia sala de control ha quedado inoperativa. Existe la necesidad de comunicaciones para mantener la seguridad de las personas y las instalaciones. Se utiliza el 112 pues estará disponible desde cualquier terminal telefónico, incluso si no existe cobertura del operador de la línea o si el terminal se encuentra bloqueado (en el caso de móviles) y porque las llamadas tienen preferencia en la red telefónica. Los trabajadores llamarán al 112 para comunicar la situación actual, medios que requieren o pueden ofrecer para garantizar la seguridad. Este plan se habrá coordinado previamente en los planes de emergencia de riesgo químico correspondiente. El 112 puede derivar a la entidad de control de dicho plan de emergencias o bien realizar llamadas de grupo tipo multiconferencia o mediación de llamadas, sirviendo de puente para las comunicaciones entre varios trabajadores de las instalaciones.

11. Panorama de migración y sus funciones de seguridad

A lo largo de este apartado se va a explicar la situación de las redes TETRA en la actualidad y la migración hacia futuras tecnologías que pretenden igualarla, mejorando prestaciones o reduciendo el coste, y a tecnologías que pretenden superar las posibilidades que nos otorga una red TETRA.

11.1. Tecnologías actuales

En la actualidad, **TETRA es la red con mayor número de equipos de comunicaciones críticas en el mundo**, y aunque, la tecnología 4G/LTE está cada vez surgiendo con mayor fuerza, y el estándar abierto MCOP tiene una mayor afinidad en la actualidad, las redes TETRA siguen siendo el baluarte oficial de las comunicaciones de emergencia en muchos países.

11.1.1. 4G LTE – *Long Term Evolution*

La **tecnología 4G/LTE o 4G *Long Term Evolution*** hace referencia a la "Evolución a Largo Plazo" de la tecnología 4G y se puede considerar como la nueva versión de los estándares GSM/UMTS. Este estándar, fue desarrollado por la 3GPP (*3rd Generation Partnership Project)* en una incesante búsqueda por aumentar la velocidad de las redes de datos gracias a un nuevo procesamiento digital de señal.

LTE puede alcanzar velocidades de transmisión de como **máximo 300 Mbps**, que son incompatibles y no cumplen con los requisitos del estándar 4G, por lo que 3GPP, desarrollo la tecnología **LTE-Advanced, en la que se mejoraron diferentes aspectos de la tecnología para permitirla compatibilizarse con el 4G**.

Una de las características de este tipo de tecnologías es que, al igual que en las conexiones 3G, la capacidad de ancho de banda de las tecnologías LTE, LTE-Advanced y 4G es compartida por todos los usuarios que en ese momento se encuentren conectados de forma simultánea a una misma estación base. Por otra parte, la calidad de la conexión, en este caso, dependerá de la distancia del usuario a la estación y de las interfaces existentes.

11.1.2. Estándar MCOP

MCOP o Plataforma Abierta de Misión Crítica es un proyecto colaborativo entre el Departamento de Comercio de EEUU y el Instituto Nacional de Estándares y Tecnología (NIST).

El principal objetivo de la proposición MCOP es la definición, desarrollo y validación de la *MC Open Platform*. Su arquitectura está diseñada en diferentes capas:

- ***MCOP Unified Open Application* API**: Otorga una interfaz flexible para los clientes. Además, permite el acceso a las Apps desarrolladas para el entorno.
- ***MCOP Open Source* SDK**: Implementa los protocolos desarrollados por 3GPP en la aplicación API.

- ***MCOP Integration* API:** Entre usuario y fabricante se diseñan diferentes *plugin* para aumentar las capacidades de las apps MCOP, así como para apoyar a operaciones LTE.
- ***MCOP OAM/OTA Open Access***: Interfaz capaz de permitir al usuario y al fabricante configurar y desarrollar interfaces.

11.1.3. Tecnología Lora y LoRaWan

Existen otros tipos de tecnología en la actualidad capaces de realizar funciones similares a las presentadas por las redes TETRA.

LoRa es una tecnología inalámbrica (similar a Wifi, Bluetooth, LTE, SigFox o Zigbee) que emplea una modulación en radiofrecuencia patentada por Semtech.

La tecnología de modulación se denomina ***Chirp Spread Specturm* o CSS** y emplea en comunicaciones de ámbito militar y espacial.

Entre sus características más importantes, destacan las siguientes:

- alta tolerancia a las interferencias.
- alta sensibilidad para recibir datos (-168 dB).
- basado en modulación “Chirp”.
- bajo consumo.
- largo alcance (entre 10 y 20 km).
- baja transferencia de datos (hasta 255 bytes).
- conexión punto a punto.

Otro de los aspectos relevantes de esta tecnología es que trabaja en la banda de **frecuencias de los 868 MHz** en Europa, siendo similar a la utilizada por la tecnología TETRA. Actualmente, la tecnología **LoRa** está centrada en las conexiones IoT a grandes distancias en las que se necesiten sensores que no dispongan de corriente eléctrica de red. Algunas de sus aplicaciones son: las ***Smart Cities*** (ciudades inteligentes), aplicaciones en lugares con poca cobertura y para la construcción de redes privadas con sensores y actuadores.

Por otro lado, está el protocolo de red **LoRaWan**, el cual emplea la tecnología LoRa para crear redes de baja potencia, pero con mucha amplitud. Este protocolo tiene dos componentes:

- ***Gateways***: Son las antenas de la arquitectura, se encargan de recibir y enviar la información a los nodos.
- **Nodos:** Son cada uno de los dispositivos finales que componen la red. Envían y reciben información desde/hacia los *Gateways*.

Este protocolo está centrado también en las comunicaciones IoT y entre sus características más importantes podemos encontrar las siguientes:

- conexiones bidireccionales con cifrado de extremo a extremo para garantizar la seguridad;
- bajo consumo de energía;
- largo alcance (10 a 20 Km);
- conexión casi infinita de sensores y equipos (1 millón de nodos por red);
- baja frecuencia de transmisión, movilidad y servicios de localización;
- interoperabilidad de las diversas redes LoRaWan en todo el mundo.

Debido al incesante crecimiento de los dispositivos IoT en la actualidad, **las redes LoRa y LoRaWan están experimentando un crecimiento considerable** y, aunque sus aplicaciones no sean en términos de radio para las comunicaciones críticas o de emergencia, sus características permiten ser configuradas para estos aspectos.

11.2. Tecnologías futuras

Existen previsiones de que **TETRA seguirá creciendo durante algunos años más,** hasta el surgimiento y asentamiento de nuevas tecnologías que cuenten con posibilidades semejantes a las ofrecidas por TETRA.

En la actualidad, TETRA ha de convivir con la mencionada tecnología LTE para equipos de seguridad pública, con una fiabilidad y disponibilidad muy similar a TETRA. Esta convivencia ya es un requisito en sí misma, porque se busca contar, en un mismo dispositivo, con las ventajas proporcionadas por el 4G (como la alta capacidad de transmisión de datos) pero manteniendo la seguridad que TETRA permite implementar en sus redes.

Otro de los aspectos que hay que tener en cuenta es el de la alternativa MCOP que mejora diferentes aspectos de TETRA expuestos anteriormente, lo cual le convierte en un claro competidor.

11.2.1. Tecnología 5G

Por si no fuera poco con la tecnología 4G y su versión con LTE, sumado a MCOP, el surgimiento del 5G puede suponer un avance radical en cuanto a tecnologías futuras con similitudes o mejoras respecto a TETRA.

El 5G contará con el llamado ***Network Slicing***, permitiendo a los diferentes operadores de telefonía subdividir en subredes su red principal, siendo estas semiindependientes entre sí. Todo esto facilitará solucionar uno de los grandes problemas de las tecnologías expuestas anteriormente, es decir, la vulnerabilidad ante grandes aglomeraciones de usuarios y datos en las redes.

Network Slicing permitirá crear diferentes sistemas de lo que se podría clasificar como “pequeñas tuberías” paralelas, en la que la obstrucción de una no supone un riesgo para la comunicación entre dispositivos dentro de la red. Además, esta segmentación, permitiría dedicar alguna de las ‘tuberías’ para un determinado propósito, como puede ser el de las comunicaciones críticas, permitiendo separar este tipo de comunicaciones de alto riegos, de otras comunicaciones con un carácter más básico.

Todas estas ventajas y soluciones proporcionadas en un futuro por el 5G hacen que TETRA se vea obligada a convivir no solo con el 4G sino también con el 5G, para mejorar muchos aspectos y problemáticas de usar solamente TETRA.

12. Conclusiones

La tecnología **TETRA** es una de las mejores o la mejor opción para las comunicaciones en organismos de seguridad, salud y empresas cuyo servicio es considerado crítico por su finalidad e importancia.

Debido a la calidad del servicio proporcionado, a la inserción de un plan único de frecuencias, sumado a la posibilidad de organizar un gran número de canales de comunicación, gestión del tráfico, introducción de comunicaciones de alto nivel y su protección, hacen del estándar TETRA una de las grandes referencias en comunicaciones críticas. **Tras treinta y tres años de existencia, se puede afirmar que TETRA se ha consolidado como el estándar de referencia para comunicaciones por radiofrecuencia, tanto públicas, como privadas.**

Analizando en profundidad, TETRA otorga a los usuarios algunos de los aspectos más importantes de la radiofrecuencia, la **eficiencia** en la comunicación, la **calidad** y la **seguridad** derivada de las funciones del estándar. Su cifrado de la interfaz aérea es uno de los aspectos más destacables ya que permite tener una comunicación punto a punto muy segura, además, de garantizar una alta calidad y velocidad en la transmisión tanto de voz como de datos o ambos juntos.

Por otro lado, a lo largo del estudio se ha hecho hincapié en las posibles vulnerabilidades asociadas a TETRA, además de cómo mitigarlas o incluso, en algunos casos, llegar a eliminarlas, y es que, como cualquier otra tecnología, tiene vulnerabilidades conocidas y otras todavía por conocer, pero lo importante, es que el estándar **TETRA cuenta con una gran cantidad de posibilidades a la hora de protegerse contra diferentes tipos de ataque**.

Como bien se ha podido observar a lo largo del apartado *Combinación del sector privado y público junto con las redes TETRA*, en España, TETRA está bastante extendido y las empresas con funciones críticas han incorporado dispositivos TETRA para sus comunicaciones debido a sus características.

Ante todo esto, cabe destacar que TETRA mantiene un crecimiento estable desde su creación en 1990, pero el futuro es incierto y los nuevos avances tecnológicos, como el 5G o LoRaWan, el estatus que posee el estándar en comunicaciones críticas puede verse eclipsado.

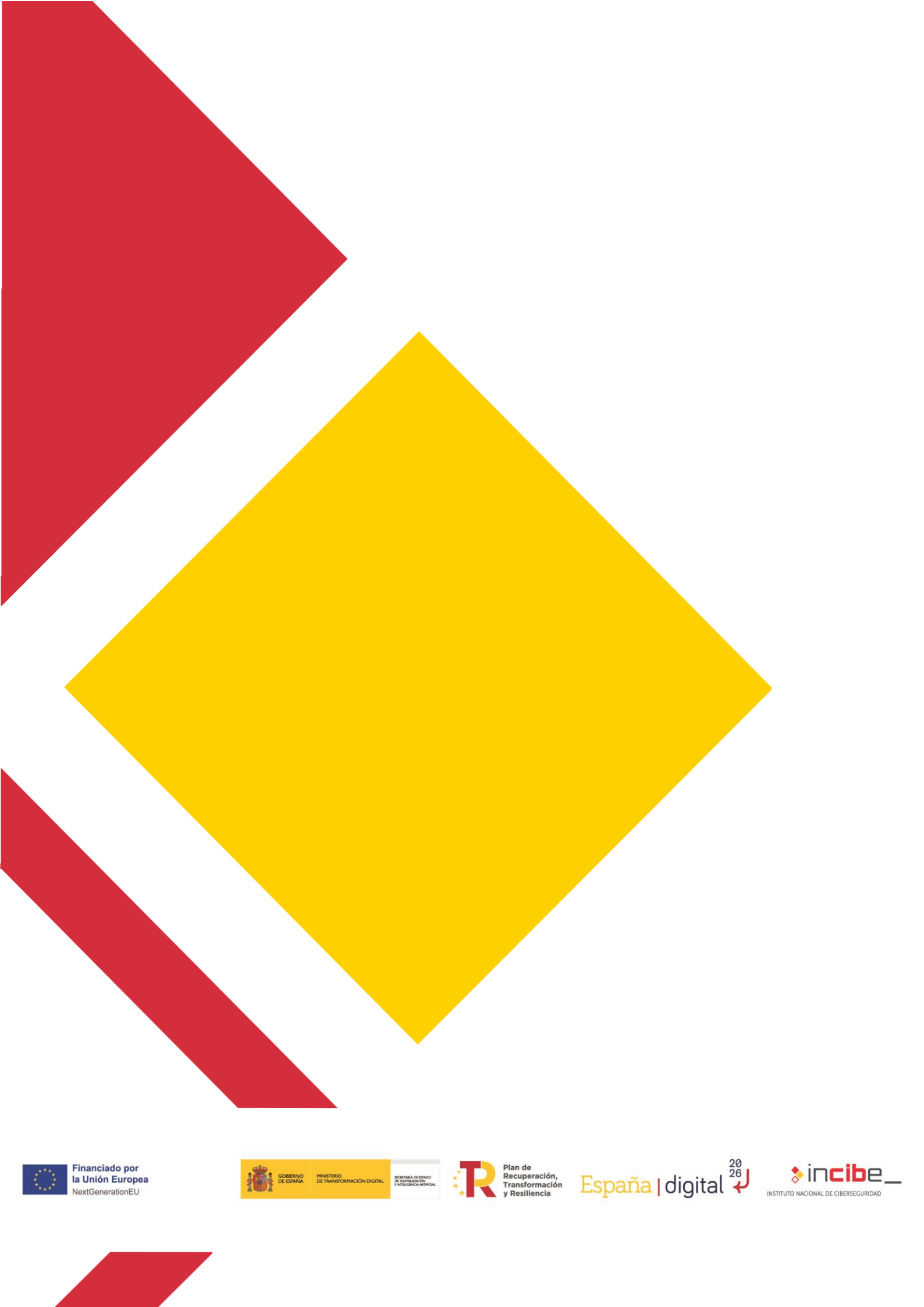
Sin duda alguna TETRA posee propiedades que lo convierten en un estándar único para comunicaciones críticas, tanto del sector privado, como del sector público. Y, aunque en el futuro otras tecnologías acaben reemplazándolo, el estándar seguirá siempre presente en la historia de las comunicaciones.

13. Glosarios de acrónimos

- **TETRA**: Terrestrial Trunked Radio
- **PMR**: Radio Móvil Privada
- **MHz**: Megahercio
- **PAMR**: Radio Móvil de Acceso Público
- **DGNA**: Asignación Dinámica de Número de Usuarios
- **TEI**: Interfaz de Equipos Terminales
- **DMO**: Modo Directo
- **SwMI**: Infraestructura de Administración y Conmutación
- **MS**: Estaciones Móviles
- **TE**: Equipo Terminal
- **MTU**: Unidad de Terminación Móvil
- **LS**: Estaciones de Línea
- **PTN**: Redes Telefónicas Privadas
- **ISDN**: Red Digital de Servicios Integrados
- **PSTN**: Red Telefónica Pública Conmutada
- **PDN**: Redes de Datos Empaquetados
- **TDMA**: Acceso Múltiple por División de Tiempo
- **KHz**: Kilohercio
- **SACCH**: Canal de Control Asociado Lento
- **PDO**: Paquete de Datos Optimizado
- **LLC**: Link de Control Lógico
- **MAC**: Control de Acceso al Medio
- **AIE**: Air Interface Encryption
- **E2EEE**: End to End Encryption
- **DCK**: Clave de Cifrado Derivada
- **SCK**: Clave de Cifrado Estático
- **SFPG**: Security and Fraud Prevention Group
- **IDEA**: Algoritmo Internacional de Cifrado de Datos
- **OTAR**: Over The Air Re-Keying
- **CCK**: Clave de Cifrado Común
- **LA**: Áreas de Ubicación
- **GCK**: Clave de Cifrado de Grupo
- **MGCK**: Clave de Cifrado de Grupo Específico
- **SAGE**: Grupo Experto en Algoritmos de Seguridad
- **TEA**: Algoritmos de Cifrado TETRA.
- **PERA**: Purdue Enterprise Reference Architecture
- **OT**: Operation Technologies
- **SCADA**: Supervision, Control and Data Acquisition
- **PLC**: Programmable Logic Controller
- **VPN**: Red Privada Virtual
- **LTE**: Long Term Evolution
- **MCOP**: Plataforma Abierta de Misión Crítica

14. Referencias

Referencia	Título, autor, fecha y enlace web
[Ref.- 1]	"Análisis del estándar de radio troncalizado digital TETRA y de su posible aplicación en el Ecuador. 8 de Julio de 2011 URL: https://bibdigital.epn.edu.ec/handle/15000/3961
[Ref.- 2]	"MTH800 Product Information Manual" marzo de 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]	"Planificación de un sistema de radiocomunicaciones basado en tecnología TETRA para monitorizar una red de sensores" Julio de 2017 URL: https://repositorio.upct.es/xmlui/handle/10317/6563?locale-attribute=en
[Ref.- 5]	"Customer Programming Software (CPS) Plus 7.7 User Guide" marzo 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" marzo 2020 URL: https://tcca.info/documents/March_2020_Maintaining_TETRA_Security.pdf/
[Ref.- 10]	"Tetra Security" febrero 2006 URL: http://www.signalspaning.se/tetra/TETRA_Security.pdf
[Ref.- 11]	"ANEXO II- JUSTIFICACIÓN DE LA TECNOLOGÍA DE LA RED DE EMERGENCIAS DE LA JUNTA DE ANDALUCÍA" 2016 URL: https://www.juntadeandalucia.es/contratacion/document/download?refCode=2022-0000000408&refDoc=2022-0000000408-2
[Ref.- 12]	"Introducción a las redes de comunicación trunking digital TETRA" Julio 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