Enrique Belda Esplugues
General Deputy Director of Information Systems and Communications for Security
Ministry of Interior. PhD in Civil Engineering, Canals and Ports from the Polytechnic University of Valencia (UPV).

Eduardo Bernabeu Piñana
Senior consultant. Systems Engineering for the Defense of Spain (ISDEFE)
Telecommunications Engineer
by the Polytechnic University of Catalonia (UPC).

ANALYSIS OF THE MULTI-CRITERIA ASSESSMENT METHOD FOR THE DEPLOYMENT AND IMPLEMENTATION OF THE FUTURE STATE DIGITAL EMERGENCY RADIOCOMMUNICATIONS SYSTEM (SIRDEE)

ANALYSIS OF THE MULTI-CRITERIA ASSESSMENT METHOD FOR THE DEPLOYMENT AND IMPLEMENTATION OF THE FUTURE STATE DIGITAL EMERGENCY RADIOCOMMUNICATIONS SYSTEM (SIRDEE)

Abstract: Public safety communications, which to date have been based on narrowband technologies with voice as the main service to be provided, are undergoing a transformation towards broadband technologies thanks to the standardization of services oriented to this sector, such as group communications, which will make it possible to adopt new services that were only available in commercial networks such as multimedia communications or data exchange. At present, public safety networks have various deployment modes based on commercial, hybrid or dedicated networks. Apparently, if an analysis of the different options is not carried out, the conclusion could be that any of them is valid for implementing a public safety communications network. This article proposes a multi-criteria evaluation method as well as an analysis of the above options to conclude which is the most suitable modality to deploy a network of this type.

Resumen: Las comunicaciones de seguridad pública, que hasta la fecha estaban basadas en tecnologías de banda estrecha siendo la voz el servicio principal a prestar, están experimentando una transformación hacia tecnologías de banda ancha gracias a la estandarización de servicios orientados a este sector como las comunicaciones de grupo y que permitirán adoptar nuevos servicios que sólo estaban disponibles en las redes comerciales como comunicaciones multimedia o intercambio de datos. En la actualidad, las redes de seguridad pública disponen de diversas modalidades de despliegue basadas en redes comerciales, híbridas o dedicadas. Aparentemente, si no se realiza un análisis de las diferentes opciones la conclusión podría ser que cualquiera de ellas es válida para implantar una red de comunicaciones de seguridad pública. Este artículo plantea un método de evaluación multicriterio a la vez que un análisis de las opciones anteriores para concluir cuál es la modalidad más adecuada para desplegar una red de este tipo.

Keywords: 3GPP Standards, communication systems, contracts, decision making, public safety communications.

Palabras clave: Estándares 3GPP, comunicaciones de seguridad pública, contratación, sistemas de comunicaciones, toma de decisiones.

1.- INTRODUCTION

The analysis aims to assess the appropriate (multi-criteria) method for the deployment and implementation of the future State Digital Emergency Radiocommunications System (SIRDEE).

Based on a completely real background, which is published as an introduction in all the Technical Specifications of the System currently in force in our country, and continuing with the state of the art of technology today, a starting hypothesis is established, a working methodology is defined and a solution to the proposed hypothesis is reached.

Finally, the section Conclusions reflects on the suitability of the established method, presenting alternative solutions assessed with the same criteria, determining that the current solution continues to be the most advantageous alternative and also envisaging that in the near future, with the appearance of new commercial solutions, this same method will lead to different results.

2.- BACKGROUND.

In 2000, the Secretary of State for Security formalised an agreement for the implementation and deployment of an Integral State Digital Emergency Radiocommunications System (SIRDEE), which would serve as a support for the provision of an integral and secure voice and data communications service to the State Security Forces and Corps throughout the national territory.

The SIRDEE network is based on TETRAPOL digital technology, owned by AIRBUS Defence & Space, has a national scope and is structured in such a way that it enables all users of the system to access the communications provided by the service with maximum security measures.

The full deployment of the SIRDEE was completed in 2005, and since then, the various agreements, which gave continuity to the system, have come to alleviate the shortcomings detected in the area of police communications (different working bands, isolated coverage of a discontinuous nature, a notorious lack of capacity, analogue technology, unencrypted communications, impossibility of transmitting data, etc.) and have made possible, to a large extent, the necessary coordination between the forces that make up the State Security Forces and Corps, as well as collaboration with other units, whether they are part of the Ministry of the Interior itself (Directorate of the Interior, Directorate of the National Security Forces and Corps) or in some other Public Administration Area (Nuclear Safety Council, Ministry of Defence –in particular the Military Emergency Unit–, Security Units of the Household of H.M. the King and the Presidency of the Government).

The SIRDEE is currently configured as an essential service, as it must provide the different user security and emergency services and units with secure and reliable communications, both in ordinary situations and in crisis or emergency situations. To this end, it has a fleet of 71,810 fully functional radio handsets within the frequency spectrum of the UNE 29 band segments, specifically in the 380-385 MHz and 390-395 MHz segments.

All these factors, together with the highest levels of security and availability that any police action requires anywhere in the country, both in ordinary situations and in emergencies, crises or special situations, have made SIRDEE a suitable tool with a high level of acceptance among users.

Theoretical and experimental studies are currently being carried out to determine its evolution towards a broadband technology that will provide network users with features similar to those available to any user of a commercial mobile communications network, while at the same time it is necessary to look for an alternative technology to the current ones, since the main manufacturers of narrowband networks are setting the year 2035 as the date of no continuity of these networks.

As will be seen, most countries have opted for LTE technology to carry out this evolution, but there are several challenges facing Public Protection and Disaster Relief (PPDR) networks:

– Spectrum availability

Despite the Commission's Implementing Decision (EU) 2016/687 of 28 April 2016 on the harmonisation of the 694-790 MHz frequency band [1], which establishes two frequency blocks for PPDR networks, it gave freedom to Member States for use in this application, and few countries have opted for this reservation. Among others, Spain.

In Spain, spectrum is available in the 450 MHz band (B31) and in the 700 MHz band (B68 and B28) according to the National Frequency Allocation Table (CNAF) [2].

– The availability of commercial solutions geared to this sector

There are currently few commercial mission-critical solutions that are fully compliant with 3GPP specifications. The equipment ecosystem is still small and handset chipset manufacturers do not yet see this sector as attractive due to lack of demand.

– The need to maintain current performance

The SIRDEE network has 95.8% geographical coverage and 99.88% availability. No commercial networks are currently capable of guaranteeing these figures.

The situation is so uncertain that it is difficult to make a decision on the most appropriate type of deployment, meaning that having a mechanism to support decision-making is very useful.

3.- STATE OF THE ART.

During the 1990s, a technological revolution was triggered by the arrival of the 2nd generation of mobile telephony (GSM), which led to a change in the way professional communications networks, known as PMR (Private Mobile Radio) or professional mobile communications networks, evolved towards digital trunking networks.

As a result, by the end of the same decade, three standards for such networks were available: P25, TETRA and TETRAPOL.

- P25:

This standard defined by the TIA (Telecommunications Industry Association) was mainly used in the USA and Canada, also known as APCO-25, due to the support received during the standardisation process from APCO (Association of Public-Safety Communications Officials-International). Its data transmission capacity is 3.6Kbps.

- TETRA

The TETRA (Terrestrial Trunked Radio) system[1], the digital trunking network standard for Europe, was defined by the European Telecommunications Standards Institute (ETSI), and is the most widely adopted trunking network, not only in Europe but also worldwide. Some examples of networks that have adopted this standard are the communications network of Metro de Madrid and the RESCAT emergency network of the Generalitat de Catalunya. Its data transmission capacity is limited to 7.2Kbps, although with the TEDS version it is capable of up to 80Kbps[2].

- TETRAPOL:

Although it is a trunking communications standard, it is a proprietary solution originating from Matra Communications, which for business reasons became part of the EADS industrial consortium, which later became AIRBUS. TETRAPOL is the solution chosen by the Ministry of the Interior for the deployment of the SIRDEE network since its inception in 2000. It has a data transmission capacity of 2.4Kbps.

All digital trunking standards have a data channel which, although it has a low transmission speed, allowed the development and incorporation of some practical applications such as fleet tracking and database queries.

However, while information and communication technologies have evolved on the commercial side, with the development of standards with improved data transmission performance, such as 3rd generation mobile services (EDGE, CDMA2000, UMTS and HSPA), fleet-oriented networks such as trunking have lagged behind and their users are now demanding access to broadband technologies that enable similar capabilities to those available in commercial networks. In fact, there have been proprietary solutions for small emergency services based on 3G technologies over commercial networks, as in the case of the Alcobendas Local Police [3].

The main technologies that can offer valid performance for mobile broadband communications in PPDR networks today include: WIMAX, LTE (4G) and 5G, which are briefly described in the following sections.

[1] The first technical specifications date back to 1994 (ESTI ETR 086-1, -2 and -3).
[2] https://www.motorolasolutions.com/en_xu/products/tetra/teds.html

3.1.- WIMAX

Acronym for Worldwide Interoperability for Microwaves Access, it is defined in the IEEE 802.16 standard, initially as a mechanism for bringing broadband to fixed installations where wired access is not possible.

However, there is a version for mobility, 802.16e with high data rate and long range, using licensed and unlicensed spectrum. Subsequently, 802.16m emerged as a serious candidate for 4G deployment and a competitor with LTE. In fact, both standards are quite similar, as they were defined on the basis of the requirements set out for International Mobile Telecommunications (IMT) - Advanced.

Unfortunately, this technology has been falling into oblivion as LTE has become the technology of choice globally to implement the 4th generation mobile communications solution, resulting in a limited range of equipment, high cost and low probability of survival compared to LTE, making it highly risky to consider WIMAX as an alternative technology to evolve the SIRDEE network.

3.2.- LTE (4G)

In 1998, the 3GPP (3rd Generation Partnership Project) was created to draw up the technical specifications for the 3rd generation mobile system as an evolution of GSM, leading to Release 99 (published in December 1999) with the definition of the UMTS system[4].

The 3GPP project provides a comprehensive description of mobile communications systems through three technical specification development groups (TSGs): Radio Access Network (RAN), Network Core and Terminals (CT) and Services Aspects (SA).

Within each technical specification group there are working groups dedicated to discussing and approving specifications that are published, once frozen, in a particular Release. Specifically, the TSG SA is home to the WG6 working group on critical communications applications.

The first version of what is considered LTE (Long Term Evolution) corresponds to Release 8, published in 2008. However, the 4th generation of mobile communications (4G) is implemented from Release 10 onwards, with LTE-Advanced, which can reach peak speeds of 1 Gbps on the downlink and 500 Mbps on the uplink [5].

Another important development in the 3GPP specification is the incorporation of the first specifications related to the Public Safety (PS) sector. Release 12 was published in 2015, including group communications, the improvement of the MBMS service (eMBMS - evolved Multimedia Broadcast Multicast Service) and proximity services (ProSe) for direct mode communications and LTE as an alternative for public safety communications began to be considered. Information on the functional architecture for the support of mission critical services, including MCPTT and MBMS, can be found in the 3GPP Technical Specification TS 23.280 [6].

Below is a summary of the main Mission Critical (MC) facilities that 3GPP has included in the following releases [7]:

- Release 13:
  - MCPTT (Mission Critical Push-To Talk),
  - Group Communications Management
  - eMBMS (evolved MBMS)
  - ProSe, with high power terminals (1.25W)

- Release 14:
  - MCPTT for video and data
  - Improvements to the eMBMS
  - End-to-end security
  - IOPS (Isolated Operating Public Safety) - Degraded operating mode for the cell.
  - Improved protocol and architecture of the MCPTT solution

- Release 15:
  - Quality of Service in public networks
  - IWF (Interworking Functionality) - Interoperability between MC-LTE and non-LTE networks.
  - IoT integration

- Release 16
  - MC-LTE interoperability - roaming between mission critical networks[3].

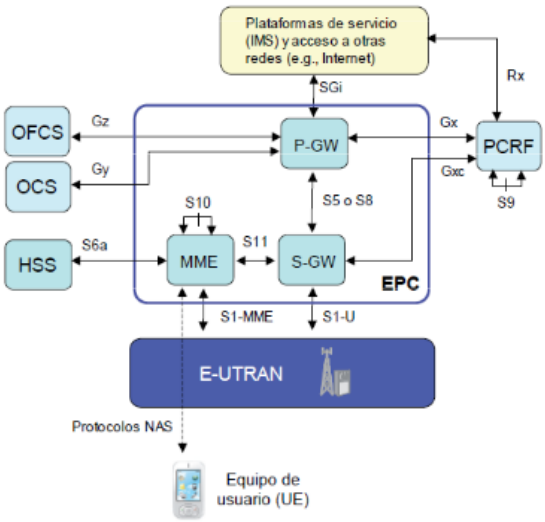

Figure 1 Basic LTE network architecture (Source: [8])

[3] All information on the 3GPP project specifications can be found on the website https://www.3gpp.org/.
Chapter 5 of the book "LTE: Nuevas tendencias en comunicaciones móviles" ["LTE: New Trends in Mobile Communications] by the Vodafone Spain Foundation [8] describes the architecture of an LTE network. (See Figure 1).

As can be seen, the architecture of an LTE network is defined by 4 blocks or layers:

- User or *terminal* equipment: which allows users to access the services provided by the LTE network.
- *Radio* Access Network or (E-UTRAN): is the network of base stations (called eNodeB) that provide connectivity between terminals and the EPC backbone.
- *Core* or network core (EPC): is the backbone network that performs the necessary functions to provide IP connectivity between the terminals (through E-UTRAN) and the external platforms or networks that offer the services.
- *Services* offered by platforms such as the IP Multimedia Subsystem (IMS) or through connection to other external networks.

It is not the purpose of this document to describe how an LTE network works, but a conceptual understanding of these four layers is important to understand the different deployment models that will be presented later.

3.3.- 5G

The 5th generation of mobile communications (5G) is based on the evolution of LTE and is defined by 3GPP Release 15 [9]. Its main objective is to increase the bit rate (up to 10 Gbps) and reduce latency (down to 1 ms), which will drive the so-called Internet of Things (IoT) and machine-to-machine (M2M) communications.

The main target sectors for this new technology are automotive (autonomous cars) and medicine, although other sectors will benefit, such as households and sports.

As seen in the previous section, Release 15 and 16, which are part of the 5G definition, evolve the Mission Critical facilities.

At present, some countries already include the use of 5G in their future plans for the deployment of public safety networks, although due to the particularities of this technology, it should be geared towards the development of specific applications or the interconnection of devices.

It is a very nascent technology that is not yet sufficiently deployed and proven to be considered as a valid alternative for a critical communications network, let alone for a national deployment as is the case with SIRDEE.

3.4.- Public safety nets in other countries

In order to see how other cases of critical communications networks evolving to broadband are being used, below is a compilation of the solutions chosen by some representative countries:

- *USA - FirstNet [10]:*

FirstNet was created in 2012 with the aim of creating a large broadband communications network for public safety and emergency forces. It uses LTE technology and has a 2x10 MHz spectrum allocation in the 700 MHz band (B14) with a public-private partnership agreement with the operator AT&T. This agreement consists of the following:

- FirstNet cedes spectrum (20 MHz) to AT&T and initially finances with $6.5 billion, and AT&T must deploy and operate a nationwide broadband network for security and emergencies for more than 25 years.
- AT&T will invest some $40 billion over the life of the agreement to deploy, operate and maintain the network, while ensuring that public safety needs are included.
- AT&T may use the spectrum provided by FirstNet for commercial purposes when it is not being used by law enforcement and emergency services. The operator shall prioritise service to such bodies over commercial use.
- Service prioritisation will consist of both prioritisation of communications and denial of service to commercial users to avoid saturation of stations during emergencies.

According to https://www.firstnet.com/coverage.html when the network reaches its deployment target it will cover an area of 2.27 M miles^2 (3.65 M km^2), equivalent to 76.2% of the continental US.

- *UK - ESN [12]:*

ESN (Emergency Services Network) is the UK emergency network that will replace the narrowband Airwave network and is based on a commercial 4G network with prioritisation over commercial users.

Although initially planned to go into operation in 2017 to replace Airwave in its entirety in December 2019, in 2018 the Home Office renegotiated the contracts due to technological unavailability and the cost overruns required (an additional £3.1 billion on top of those already budgeted, bringing the total to £9.3 billion).

Availability was postponed to December 2022, and new forecasts indicate that it will not be available until the end of 2024.

- *France - PCSTORM Project [13]:*

The objective of the PCSTORM project is to have a national network based on LTE technology (RRF - Radio Network of the Future) together with tactical cells as additional capacity where required.

In a first phase, tests were conducted on a public LTE network for emergency services (INPT Network) and on a private 700MHz network (2x5MHz B28) for the Gendarmerie (RUBIS Network), with commercial network backup.

Phase II envisages the use of dedicated spectrum (700MHz) awarded to one operator to provide an end-to-end service, with public network back-up where it is not reached. In that case they must coexist.

It is envisaged as a hybrid network, with a commercial operator providing the radio access layer, and a dedicated network core to be operated by the French Ministry of the Interior. The operator must facilitate prioritisation over commercial users, as well as the possibility of roaming for interconnection with other operators' networks, but this requires a change in the Telecommunications Law.

It should be fully available before 2024, the year of the Paris Olympics.

Currently, the use of the 450MHz band is also being considered due to the high cost of deployment in 700MHz.

- *Germany - BDBOS:*

The initial approach was to maintain the TETRA network for voice, while data would employ a hybrid solution, using commercial operator infrastructure in the 700 MHz band and a dedicated network on 450 MHz.

At present, service over public network is not considered as a replacement option for the TETRA network due to the lack of service guarantee. A final solution based on a quality assured private LTE network is envisaged.

On the spectrum side, there was a fierce battle between BDBOS and critical infrastructure operators in the energy and water industry over the allocation of the 450 MHz band. The contract was finally awarded to the latter[4], so it is likely that a hybrid solution will be chosen.

- *Czech Republic - PEGAS [14]:*

In the Czech Republic, Nordic Telecom has 2x4.25 MHz in the 410-430 MHz band available for PPDR use throughout the Czech Republic.

Together with Nokia, it plans to deploy a dedicated LTE network for security and emergency services and industrial IoT on an exclusive basis. As it is based on Nokia products, it is a solution that works in Unicast, as Nokia does not yet have a solution that implements eMBMS.

For internet connections or for exceptional situations where the dedicated network is not available, the commercial network will be used.

The major drawback of this solution is that Nordic Telecom has not yet found terminals that work in this band.

- *Finland - VIRVE [15]:*

The VIRVE network, based on TETRA technology, was scheduled to end its life cycle at the end of 2020 to be replaced by VIRVE 2.0, based on LTE technology.

This network is operated by Erillisverkot, a company wholly owned by the Finnish government. Its evolution towards LTE will consist of a hybrid solution, where the network core is dedicated, provided by Ericsson, and the radio access network is shared with the commercial network of a selected operator. This is similar to the model used in the UK for its ESN network.

[4] https://www.behoerden-spiegel.de/2021/03/09/zuschlag-fuer-frequenzen-erteilt/

To ensure service availability to law enforcement and emergency services, a legislative change was made so that the law allows certain usage privileges to government users by prioritising network service in congestion situations, as well as the possibility of national roaming when the contracted operator's network is not available.

Migration from TETRA to LTE will take place between 2022 and 2025, during which time both technologies will coexist.

- *Korea - SafeNet [16]:*

LTE network over dedicated spectrum at 700MHz (band 28) with 10+10 MHz available. They have already achieved an MCPTT application using eMBMS under 3GPP standard[5].

The radio access network is shared with three dedicated network cores (public safety, rail service and maritime service). It also shares radio access network with the commercial network.

Indeed, from a technological point of view there is no alternative to LTE, as we have seen the consensus is widespread for all countries that are deploying broadband services for mission critical communications.

The alternatives or differences between solutions put forward by the main national public safety networks in the world focus on the deployment strategy, i.e. whether public, private or hybrid solutions are used.

The following section will describe the different deployment alternatives currently being considered.

4.- TECHNOLOGICAL ALTERNATIVES.

Since 2015, when the need for a technological change of direction in the SIRDEE network arose due to the demands of network users, the only technology that has been considered as a possible path to broadband is LTE (4G).

As seen in the previous section, most countries that are evolving their public safety networks towards broadband have decided to use LTE technology, as in reality, there is no other valid option. Globally, no network proposes solutions that are not based on 4G or 5G, the latter for the time being only on paper.

It has also been found that various strategies have been employed in the different countries considered, ranging from solutions based on public commercial networks to private or dedicated networks, as well as hybrid solutions.

Our analysis will focus precisely on the type of solution or strategy adopted.

[5]https://www.computerweekly.com/news/252499799/First-3GPP-compliant-public-safety-network-with-MCPTT-launches-in-South-Korea

a) Commercial networks

This is the use of commercially available networks deployed by mobile operators for security and emergency purposes, sharing network resources with other users.

The Core, Radio and Services layer is provided by the operator, and the Terminals layer, depending on the agreement with the operator, may be provided by the user or included in the service agreement.

The main advantage of a commercial network is that it is normally fully deployed and operational over most of the required territory and has ample bandwidth available.

In addition, as these are general purpose networks where there are a large number of users, the equipment ecosystem is large and economies of scale have an important impact on the prices of this equipment.

However, as commercial networks, they are designed to optimise the economic revenues of the operator owning the network or the service in the case of virtual operators. This means that geographic coverage is focused on population demand, traffic absorption capacity is sized to optimise the relationship between equipment amortisation and quality of service to the user, and sites are usually not adequately protected against contingencies.

Furthermore, they are not intended for public safety and emergency communications which typically employ group communications where one user transmits and many receive. As commercial networks do not implement the MBMS service, communications are Unicast, i.e. they use one carrier per user receiving the communication, which unnecessarily increases spectral usage.

On the other hand, in disaster situations, commercial users drastically increase the demand for communications, making access to the service impossible for other users, either due to lack of service capacity or due to radio spectrum saturation in base station reception.

All these drawbacks have an impact on the availability of the service, which is one of the essential parameters to be properly tuned in a public safety communications network.

Finally, the implementation of the MCPTT application is done through an OTT (Over-The-Top) application that is usually proprietary to a manufacturer and will not comply with the 3GPP specification, so interoperability between organisations is questionable to say the least [17].

b) Dedicated Networks

As the name suggests, these are networks for dedicated use, in this case exclusively for emergency services and public safety, and resources are not shared with other types of users.

These networks are tailored to the user's needs, with the user defining technical requirements such as coverage, security and availability among others, as well as

functional requirements such as group communications, emergency calls, etc. In this case, the four essential layers that define the network (Core, Radio, Terminals and Services) are controlled by the owner of the network or service.

As these networks use spectrum reserved specifically for public safety and emergency users, their working band does not coincide with those used by commercial operators, which implies a smaller variety of equipment that also does not benefit from economies of scale; however, with the harmonisation of the 700 MHz band there will most likely be no equipment problem in this band.

In terms of capacity, given the spectral scarcity that is normally available [2], it is almost essential to employ techniques to optimise their use, such as MBMS [18], and it would be desirable to be able to apply carrier aggregation [19] to improve bandwidth.

On the other hand, dedicated networks such as SIRDEE have demonstrated their robustness and availability in critical and delicate moments, such as natural disasters, terrorist attacks or events of high concentration of people in which commercial networks have not been able to provide the service because of high demand for communications or due to system unavailability.

c) Hybrid Solutions

Hybrid solutions are the strategy being employed by most countries that have not opted for a dedicated network, and consist of sharing part of the network infrastructure with a commercial operator.

- FirstNet case (USA): PS and commercial users share AT&T's commercial RAN with both commercial and FirstNet spectrum, but PS users have priority over others.
- ESN case (UK): ESN is established as a virtual operator (S-MVNO) sharing the RAN and part of the Core. This means that there is a dedicated Core part and the service layer is controlled by ESN.
- VIRVE case (Scandinavian countries): It is a MOCN (MultiOperator Core Network) type configuration. This means that the spectrum and RAN belongs to a commercial operator and the network core is dedicated to PS.

Another case could be the use of a dedicated network that is complemented by a commercial network with which it shares its RAN to access areas where the dedicated network does not have coverage.

5.- OBJECTIVE OF THE WORK

The purpose of this work is to carry out an analysis from a technical, economic and political point of view of the different existing alternatives for the necessary evolution of the State's emergency communications network towards a broadband technology that improves the current communication capacities for Public Safety services.

For this analysis, a multi-criteria assessment methodology will be presented, trying to obtain as objective an evalutation as possible of some of the parameters that influence the specification of a public safety communications service and which will be

applied to the various alternatives that have been identified in the previous sections and with data obtained for similar environments.

The aim of this work is to check how technical, economic and political decisions influence the selection of a specific implementation strategy and, on that basis, to determine which one might be the most appropriate for the specific case of Spain (SIRDEE network).

6.- METHOD

6.1.- Hypothesis of proposed solution.

Any of the alternatives identified in Section 4 would be suitable for providing a mobile broadband communications service, although it would be too early to conclude that any of them would be suitable for providing an adequate service to public safety and emergency services.

In order to carry out such an assessment, it is necessary to analyse some parameters, which have already been discussed, and which allow the service provided by a communications network to be characterised in some way. There are many other parameters, each of which could be analysed in detail, but this study will focus on those that are considered to be the most immediate and contribute the most weight to the decision.

These parameters are as follows:

- *Geographical coverage:* the geographical area covered by the service offered by the communications network at the time of contracting or its evolution over time, considering aspects such as surface area or population affected.
- *Traffic offered or traffic carried:* refers to the capacity of the network to carry the traffic demanded by users, whether commercial or public safety, and which may be limited by available resources or by contract.
- *Service availability:* this is one of the key parameters of any system, and will provide information on how long the service is operational, an aspect to be taken into account especially in crisis situations.
- *Security:* refers to the measures taken to ensure that information passing through the network is not compromised, either by unauthorised access to end-to-end elements, inappropriate encryption, poor key management, etc.
- *Cost:* is the price of the service and will require adapting the information to be able to compare the cost of each of the identified deployment alternatives.
- *Political decisions:* this is one of the issues that cannot be overlooked when it comes to critical services for a country, such as a national communications network for public security. These decisions can be related to both domestic and foreign policies.

The hypothesis is based on the assumption that a multi-criteria assessment methodology, evaluating as objectively as possible the above parameters used as criteria, can serve as an indicator of which strategy is the most recommended in each situation to address a technological evolution in the State's security and emergency communications network. This methodology is developed in the next section.

6.2.- Parameter assessment methodology.

As mentioned in section above, the methodology to be followed is the multi-criteria assessment, which can be represented by the following algebraic expression:

$$Score = \sum_{i=1}^{N} \alpha_i P_i \qquad (1)$$

Where α_i are the weights assigned to each criterion in percentage, assigned so that they must meet that they must meet $\sum_{i=1}^{N} \alpha_i = 100\%$.

And P_i are the scores obtained for each criterion or parameter involved in the assessment normalised to 10.

Therefore, the next step should be to determine the weight to be attached to each criterion and the mechanism for determining the score for each of these criteria, seeking as far as possible ways that are objective.

a) Determination of the scoring method

- *Geographical coverage (P_1):*

The coverage of a communications network can be defined as the area of land that is served by the network. This is a basic parameter in the definition of a network and has two objectives: to maximise the area of influence and the number of users it serves.

With regard to the first objective, an analysis of the territorial evolution of the SIRDEE network during its implementation has been carried out. Details of the percentage of territory covered and the number of stations deployed per service year can be found at Table 1 . These data can be seen graphically at Figure 2 .

Año	Nº Provincias	% territorio	Nº Estaciones	Δestaciones
2000	4	4,5	138	138
2001	12	23,4	461	323
2002	9	36,3	691	230
2003	12	60,4	968	276
2004	10	74,5	1.183	215
2005	5	87,2	1.398	215
2020	--	95,8	1.536	138

Table 1 Evolution of the SIRDEE network deployment (Source: SIRDEE): Prepared internally)

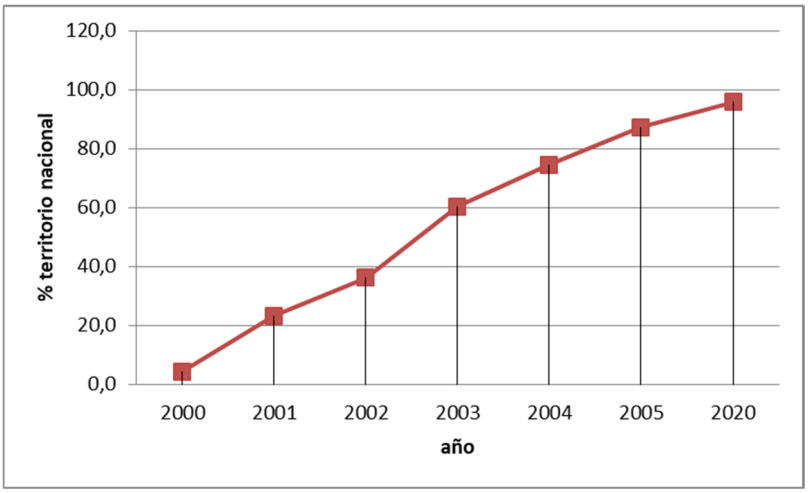

Figure 2 Evolution of the percentage of geographical coverage of the SIRDEE network as a function of the years of deployment (Source: SIRDEE): Prepared internally)

There are currently 1,536 stations deployed for a coverage of 95.8% of the territory.

As can be seen, in the first 5 years of deployment, the initial coverage objective is achieved (close to 90% of the territory), and from that moment onwards the deployment of new cells is aimed at optimising the network to reinforce certain locations or provide coverage to small spaces.

The first station was placed on 5 October 2000 and by the end of 2005 the deployment was completed in all provinces with a total of 1,398 stations for a 90% territorial coverage. Averaging over the first 6 years, deployment was at an approximate rate of 260 stations per year, although as can be seen in Table 1 in the second year more than 300 stations were deployed.

With this information, one can try to predict the time needed to realise an LTE deployment. However, it should be borne in mind that the SIRDEE network deployment analysed was carried out with TETRAPOL technology and not LTE, and that the frequency band used is 380-400 MHz and for the dedicated LTE network the 450 MHz or 700 MHz band or both are foreseen, which could considerably multiply the number of stations.

Following the first experiences with LTE technology, although the data are not yet conclusive, the best predictions estimate 1.5 times the number of stations needed to complete a deployment equivalent to the narrowband network and the least promising ones up to 4 times, so that between 2,295 and 6,129 LTE stations would be required in each case.

Assuming that the human resources made available for LTE deployment are the same as for narrowband deployment, the speed of station deployment will follow the average of 260 stations/year, and it would therefore take between 8 and 23 years to have the network fully deployed.

The other analysis that can be made is by considering the other coverage objective: maximising the number of users to which the network provides the service, or also giving priority coverage to areas where the population is concentrated.

According to an article on the distribution of the Spanish population published in the newspaper La Razón [20], only 12.7% of the national territory is occupied.

Another article, this time in El País [21], indicates that 90% of the Spanish population is concentrated in 30% of the territory. Information that will be useful in conducting this analysis.

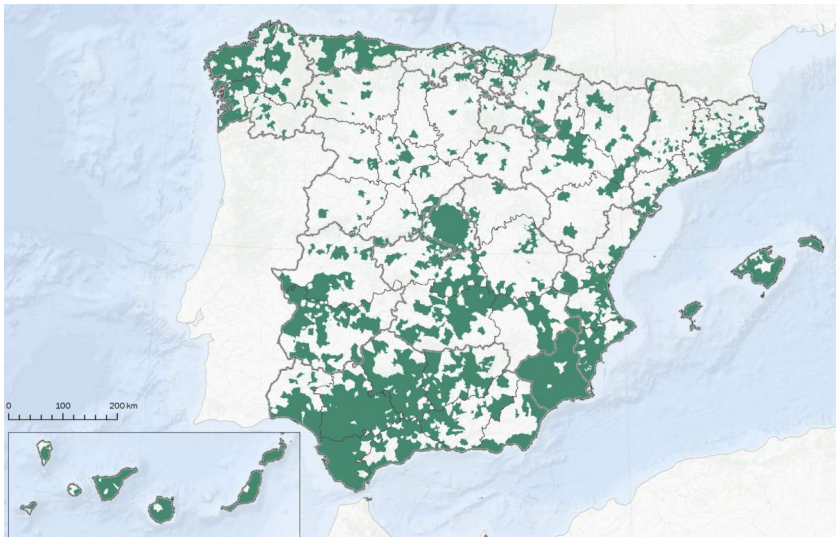

Figure 3 Municipalities that account for 90% of the Spanish population (Source: El País [21])

A regression line can be obtained from the data in Table 1 to provide information on the number of stations or time needed to cover a certain percentage of territory. Specifically, the two necessary expressions have been obtained:

$$t(años) = 0.059P_{cob} - 0.0263 \quad (2)$$

$$N_{estaciones} = 14.814P_{cob} + 99.897 \quad (3)$$

These two expressions can be used to estimate the number of stations and the time needed to cover a certain percentage of territory. The result obtained for four cases (30%, 50%, 90% and 95%) of territorial deployment for TETRAPOL technology and its LTE equivalent is included in Table 2 .

	Nº de años para desplegar					
	TETRAPOL		**LTE 450MHz (x1.5)**		**LTE 700MHz (x4)**	
% Territorio	Nº Est.	Años	Nº Est.	Años	Nº Est.	Años
30%	544	1,7	816	3,1	2.177	8,4
50%	841	2,9	1.261	4,8	3.362	12,9
90%	1.433	5,3	2.150	8,3	5.733	22,0
95%	1.507	5,6	2.261	8,7	6.029	23,2

Table 2 Number of stations and years required (Source: Prepared internally)

Based on this information, it can be estimated that it would take approximately 1.7 years to provide coverage of the territory where 90% of the population is concentrated with TETRAPOL technology and about 3 years using 450 MHz LTE stations.

However, public security is a common service for the entire population and should not be focused on the points where the population is most concentrated. The SIRDEE network currently covers more than 95% of the Spanish territory. To complete LTE coverage equivalent to the current SIRDEE network would, according to these estimates, take between 2,300 and 6,000 stations, over a timeframe of between 8 and 23 years.

However, these times can be reduced considerably. An operator can deploy more than 4,000 stations per year[6], which could reduce deployment time from 1 to 3 years assuming sufficient budget in each year.

In terms of how to assess this criterion, an expression is proposed that measures how close the available coverage (provided by the network) is to the desired target, i.e:

$$P_1 = 10x\frac{\%Cobertura\ disponible(t)}{\%Cobertura\ objetivo} \qquad (4)$$

The %Coverage Available being the coverage offered for a commercial or hybrid network or the coverage available on a time-dependent basis for a dedicated network to be deployed.

- *Traffic offered or traffic carried (P_2):*

In order to determine the traffic capacity of an LTE network, several aspects need to be taken into account, such as:

– available spectral bandwidth,
– spectral efficiency
– type of service demanded by the user (voice, video, data, etc.)
– compression algorithms,
– error control
– distance from user terminal to station
– etc.

Although when it comes to broadband networks, the tendency is to think of data applications, as this is precisely the shortcoming of the narrowband networks discussed in Section 0, the reality is that they should primarily be able to support voice traffic needs, as this is the basic service of a public safety communications network.

ETSI Technical Report TR 136.912 [22] publishes spectral efficiency data that provides valuable information for understanding the actual capabilities of an LTE cell.

[6] Telefónica Móviles data: in 2020 they deployed 4,615 4G stations from Ericsson alone.

From Page 39 of this report we extract Table 3 with information on the capacity of supported VoIP users as a function of cell type for LTE Rel-8 for average spectral efficiency values, where antenna configuration (A) is a MIMO of 4 co-polarised antennas spaced 4λ apart and configuration (B) is a MIMO of co-polarised antennas correlated 0.5λ apart. This information has been obtained from simulations carried out by the main LTE manufacturers, as described on Page 49 of [22].

Antenna configuration	Environment	ITU requirement	Number of samples	Capacity [User/MHz/Cell]
Antenna configuration (A)	Indoor	50	3	140
	Urban Micro	40	3	80
	Urban Macro	40	3	68
	High Speed	30	3	91
Antenna configuration (C)	Indoor	50	3	131
	Urban Micro	40	3	75
	Urban Macro	40	3	69
	High Speed	30	3	94

Table 3 LTE FDD Rel.8 VoIP capacity (Source: ETSI TR136.912 [22])

From this data it is possible to know the number of simultaneous conversations that can take place in a cell, based on the available bandwidth. The results obtained for an antenna configuration (A) are shown in Table 4 .

Tipo de celda	Capacidad	Servicio Voz-Comunicaciones simultáneas				
	Usuario/MHz/Celdal	1,4MHz	3 MHz	5 MHz	10 MHz	20 MHz
Indoor	140	196	420	700	1400	2800
Urban Micro	80	112	240	400	800	1600
Urban Macro	68	95	204	340	680	1360
High Speed	91	127	273	455	910	1820

Table 4 Simultaneous voice communications in Unicast mode (Source: Prepared internally)

From this data it can be deduced that a voice channel for a Micro type cell consumes an equivalent of 12.5 KHz of bandwidth, exactly the same as a TETRAPOL voice channel of the SIRDEE network.

This data refers to voice communications in unicast mode, i.e. when group communications are made, each of the users in the group that are in the same cell will count as one communication. Example: for a group of 200 users in the same cell with a bandwidth of 5 MHz, a single communication would consume half of the available spectrum.

In a public safety network most communications are group communications. In urban areas most terminals have common groups programmed and therefore there will be a spectral consumption in proportion to the number of users belonging to the group, so that a group communication, which in a TETRAPOL cell would occupy 12.5 KHz of spectrum, using LTE would occupy Nx12.5 KHz, where N is the number of users in that group and cell.

Therefore, it is important to count the number of terminals enrolled in the same cell and group in order to dimension the bandwidth needs. Statistical data on the number of registered passengers in the same cell at peak hour for three urban typologies obtained

from the SIRDEE network is available in Table 5 and can be used as an approximation for this calculation.

Ciudad	Nº inscritos / celda
Madrid	400
Sevilla	100
>50.000 hab	120

Table 5 Number of registered terminals per cell according to type of city (Source: Prepared internally)

Taking into account that the spectrum allocations for dedicated PPDR networks is 5+5MHz on 450 MHz and 3+3 MHz on 700 MHz, and the data from Table 5 it can be concluded that the available spectrum may not be sufficient even for voice communications. It should be noted that LTE cells are expected to be smaller and contain a smaller number of registered users. However, this data is for voice communications and will worsen drastically when using other types of services that require higher bandwidth, such as video calls, or massive data traffic, such as sending files, querying databases or sending positions for AVL systems.

On the other hand, one can analyse the behaviour of commercial networks, which have a higher spectrum allocation, and surprisingly come to the conclusion that they cannot guarantee sufficient capacity either. With a bandwidth of 20 MHz, 1,600 users simultaneously generating or receiving a voice call at the same time would be enough to saturate the cell. Any event that concentrates people, such as a demonstration or a football match, could and does cause the service to be blocked.

For example, a football match at the Santiago Bernabéu stadium with a full capacity (81,044 spectators according to [23]), assuming an even distribution of attendees among the 4 major operators that provide service in Spain (Orange, Telefónica, Vodafone and Grupo Másmóvil) [24] would have more than 20,000 users/operator. Assuming that each operator has a station with 20 MHz of bandwidth, it would be enough for 10% of the viewers to want to use the network to saturate the cell, rendering it unusable for public safety services.

This is obviously not the case for a known event such as this one, where operators apply measures to guarantee a minimum service, such as antenna sectorisation, use of micro cells or optimisation of signal regeneration algorithms, and provided that the event runs normally. But this example provides enough information to infer that in unforeseen events, such as a demonstration, an accident or a natural disaster, a commercial network will not be able to provide service to either commercial or public safety users.

It appears from the above paragraphs that, under normal conditions, neither a dedicated network for exclusive use for public safety services with scarce spectrum, as is the case in Spain, nor a commercial network for shared use with other subscribers, would offer sufficient capacity to absorb the traffic generated by its users. However, mechanisms are in place to improve this performance in both dedicated and commercial networks.

In the case of dedicated networks, the eMBMS service defined from 3GPP Release 9 onwards can be implemented. By implementing this service, individual (one-

to-one) calls would continue to be established in Unicast mode consuming the spectral resources already exposed, but it introduces a great improvement in the case of group calls (one-to-many), either voice or video, whose spectral consumption is equivalent to an individual call of that type regardless of the number of users belonging to the group.

No information has been found on the implementation of the eMBMS service in commercial networks beyond pilot experiences, but there may be other mechanisms to improve traffic capacity for public safety services, such as the prioritisation of public safety services communications over commercial users or the rejection of commercial users by the network in foreseen situations, such as disasters or events with a high concentration of people, but this could only be done through appropriate regulation.

Once it is known in a simplified way how to measure the traffic capacity of an LTE network, a method to score the network performance in this aspect will be determined.

Based on the above, a simple and quick way that could be used to assess the traffic capacity of the network is the number of **simultaneous communications** it is able to handle. As seen in the previous paragraphs, it has a direct relationship with the available bandwidth and the number of users registered in the cell belonging to the same group.

Therefore, the assessment of this criterion should be based on the utilisation of available network capacity. For the sake of simplicity, only VoIP service (according to Table 4) will be considered in group communications, which are common in public security services, under the assumption that all users in the group are registered in the same cell.

The scoring in this case would be expressed as follows:

$$P_2 = 10x \frac{num_{com}}{num_{com\_max}} \qquad (5)$$

Where num_{com} is the number of simultaneous communications that can be made in a cell and num_{com_max} is the value of the alternative with the highest number of simultaneous communications.

For unicast communications, the maximum number of simultaneous communications possible in a cell shall be determined by the number of users in each group registered in that cell. Considering, for the sake of simplicity, homogeneous groups in terms of number of users, the number of simultaneous communications would be:

$$num_{comunicaciones} = Cap_{max}/N \qquad (6)$$

Where Cap_{max} is the maximum capacity according to the available bandwidth according to the data in Table 4, where N is the number of users in each group.

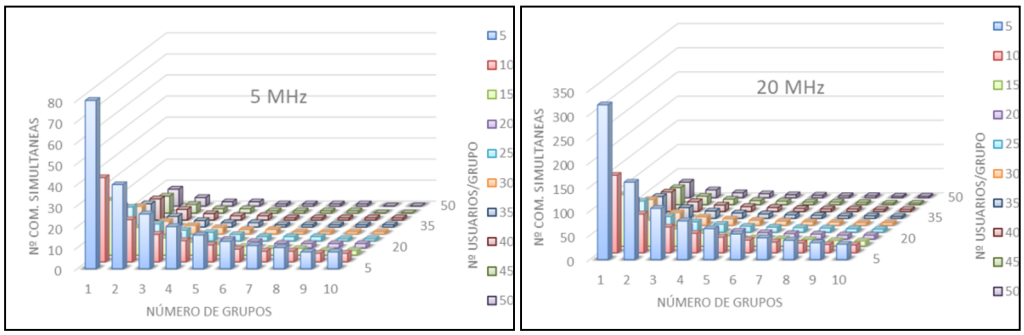

Figure 4 Evolution of the number of simultaneous communications according to the number and size of the groups in the same Unicast cell (Source: Prepared internally)

For communications using the eMBMS service, a group communication would have a consumption equivalent to an individual communication, regardless of the number of users in the group, so the number of simultaneous communications would be Cap_{max}.

- *Service availability (P_3):*

This is one of the quality parameters of a communications network and measures the time the service offered is operational in relation to the total time. This parameter is key and should always be kept in mind.

Certain practices can be used to improve service availability depending on the value to be achieved. To this end, it is possible to act on:

– Power: Having an emergency power supply system can keep the system in service when there are power outages for as long as the system is set up.
– Hardware: in addition to requiring a certain reliability of hardware equipment, some elements can be redundant, such as the baseband of a station, routing equipment, etc.
– Software: To avoid software failures, virtual machines can be implemented that run on the same machine working in Hot Stand-By mode so that if there is a problem, another machine is immediately put into service.
– Geo-redundancy: there are equipment rooms that due to their neuralgic importance in the network, such as a switching centre, a certain amount of hardware redundancy is not sufficient and requires a higher level of protection to prevent the consequences of possible natural disasters or sabotage. In this case, the option of having several equivalent centres in different locations is considered.

The availability of a system is defined as the percentage of available time relative to the total in a generic observation period [25].

$$D(\%) = \frac{T_{disponible}}{T_{observación}} x100 \qquad (7)$$

Then there are other variants of availability, which may be a function of territorial coverage, or the traffic capacity offered by the network. These two parameters may introduce unavailability of the service for the user, but will not be accounted for since these two parameters are somehow already quantified in the previous points.

To make the availability assessment, the availability of the network shall be taken with respect to the target availability, and this can be calculated by the following expression:

$$P_3 = 10x\frac{D(\%)}{D_{objetivo}(\%)} \qquad (8)$$

Target availability being the value currently required of a public safety net.

- *Security (P_4):*

As indicated in the previous section, security includes measures taken to ensure that information in transit through the network is not compromised.

For a public safety service, the communications network should be deployed in sites and switching and management rooms that have:

– Security measures to prevent unauthorised intrusions that could lead to sabotage.
– Sensorisation in the event of power cuts, smoke, temperature, etc.
– Power back-up system, either by battery bank or generator set.
– Redundancy in radio equipment elements.
– Redundancy in the rest of the elements that make up the network.

In addition, all elements that allow access to the system must have access control, authentication and auditing systems that allow it to be known who has accessed the system and what actions have been taken.

On the other hand, there must be a sufficiently robust encryption and key management system to protect the information circulating on the network. As well as using equipment with security guarantees issued by a reference centre such as the CCN (National Cryptographic Centre).

In contrast to a communications network designed for public security services, a commercial network lacks certain security features to ensure that information is protected.

Given the impact of these elements on the availability of the network, the presence of some of these elements will be reflected in the score for this criterion. Therefore, in order to simplify and to account in some way for whether the type of network offers these features, 3 scores are defined.

$$P_4 = \begin{cases} 10, si\ cuenta\ con\ estos\ medios \\ 5, si\ cuenta\ parcialmente\ o\ los\ comparte \\ 0, si\ no\ cuenta\ con\ estos\ medios \end{cases} \qquad (9)$$

- *Cost (P_5):*

This criterion is measured by the price of the service and will require adapting the information in order to be able to compare the cost of each of the identified deployment alternatives.

The current cost of the SIRDEE service will be used as a benchmark, although it will be difficult to find a point of comparison as the services are generally not comparable.

In the case of SIRDEE the service includes, in addition to the network access service, the following elements:

– Terminals of different types
– Control rooms
– Network monitoring
– Security Technology Centre
– Maintenance
– Training

The current cost of the narrowband service is €70.2m per year excluding VAT.

Considering that the network is serving 72,000 terminals, the cost per terminal per year would amount to approximately €976. This price will serve as a benchmark as to whether the change of technology could bring an economic advantage.

For the price assessment, the maximum and minimum prices will be taken for the selected alternatives.

$$P_5 = 10x\frac{Precio_{máximo} - Precio_{evaluado}}{Precio_{máximo} - Precio_{mínimo}} \quad (10)$$

- *Political decisions:*

This is one of the issues that cannot be overlooked when it comes to critical services for a country such as a national communications network for public security. These decisions can be related to both domestic and foreign policies.

This criterion cannot be used as an assessment element, but it does have an influence on the rest of the criteria that can influence the outcome of the assessment in favour of one deployment strategy or another.

Below we identify, by way of example, some of the policies that could have a major impact on the deployment strategy and how they may affect the value of some criteria.

Domestic policy decisions may include:

Decision to regulate the prioritisation of emergency communications on commercial networks: this decision would improve the availability and traffic capacity that a commercial network can offer to public safety services, both in areas of high concentration of people and in crisis situations.

– Decision to regulate national roaming: even if the service was contracted with a single commercial network operator, the existence of roaming would guarantee an extension of the available coverage by complementing the other existing networks in Spain.

– Decision to oblige operators to strengthen the protection of sites serving critical infrastructure areas.
– Decision to prioritise service availability in certain areas based on factors such as population or crime concentration.

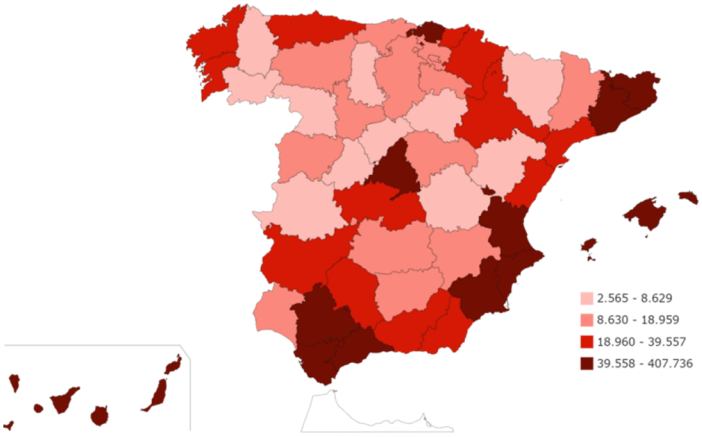

Figure 5 Criminal offences by province in 2019 (Source: INE)

Foreign policy decisions could include the rejection of technologies from China because of international agreements with other countries that veto China over trade issues or lack of trust on security issues.

Most commercial operators are using Huawei's technology[7] so a decision to do so, once the service is migrated to broadband, would cause chaos in the communications network.

b) Determination of weights

After a brief analysis of the parameters on which the initially proposed assessment criteria are based, it has been concluded that the criteria of coverage, traffic capacity, availability, security and cost will be assessed and scored, leaving the criterion of political decisions as an element that may condition the score of the previous criteria at any given time.

As for the distribution of weights, in an attempt to influence the opinion of the author of this analysis as little as possible, a survey was carried out among different actors in the public security communications sector. For this purpose, five opinion profiles related to the world of communications networks were asked for their opinion on the importance of each of the assessment criteria: a network operator, a technology manufacturer, a network manager, a technology consultant and a public administration manager.

To this end, participants were asked to give an importance score for each criterion, with 1 for "not very important" and 5 for "very important".

The results of the survey were as follows:

7 https://www.eldiario.es/tecnologia/conectividad-alas-auge-huawei-europa_1_1675218.html

	Cobertura	Tráfico	Disponibilidad	Seguridad	Coste
Op_red	4	4	5	5	3
Fabricante	5	5	5	4	3
Responsable	3	4	5	4	3
Consultor	3	4	5	4	3
Gestor	3	4	5	4	3
Punt. Media	3,52	4,18	5,00	4,18	3,00
Pesos	**18%**	**21%**	**25%**	**21%**	**15%**

Table 6 Obtaining the weights associated with each criterion (Source: Prepared internally)

Finally, a table summarising the method used to assess each criterion and its weighting is included.

Assessment criteria	**Description**	**Weighting**
Degree of coverage	$P_1 = 10x\frac{\%Cobertura\ disponible(t)}{\%Cobertura\ objetivo}$	18%
Traffic capacity	$P_2 = 10x\frac{num_{com}}{num_{com\_max}}$	21%
Availability	$P_3 = 10x\frac{D(\%)}{D_{objetivo}(\%)}$	25%
Security	$P_4 = \begin{cases} 10, si\ cuenta\ con\ estos\ medios \\ 5, si\ cuenta\ parcialmente\ o\ los\ comparte \\ 0, si\ no\ cuenta\ con\ estos\ medios \end{cases}$	21%
Cost of the service	$P_5 = 10x\frac{Precio_{máximo} - Precio_{evaluado}}{Precio_{máximo} - Precio_{mínimo}}$	15%

Table 7 Summary of the alternative assessment methodology (Source: Prepared internally)

6.3.- Proposed solution.

Once the methodology to be applied to assess the most convenient strategy has been explained, it will be applied to the different cases that may arise in the future.

- *Coverage (P_1):*

For a public safety communications network, the coverage objective should aim to reach as much of the territory as possible, since emergencies can happen anywhere. Therefore, the current coverage target of the SIRDEE network (95.8%) can be used as a benchmark for defining an initially desirable coverage target.

– Commercial Network:

The following figures show the 4G coverage maps for the 3 largest operators operating in Spain. As can be seen, coverage focuses on population concentrations. (See Figure 3)

Of the three coverage maps presented, the one with the largest geographic coverage is that of Movistar, which is estimated to cover 70% of the territory.

$$P_1 = 10x\frac{70}{95.8} = 7.3\ puntos$$

However, if the government were to regulate the possibility of national roaming between available operators' networks this score would increase, although at first glance from coverage maps it would not increase dramatically. In such a case it could be concluded that $P_1 > 7.3$ *points*.

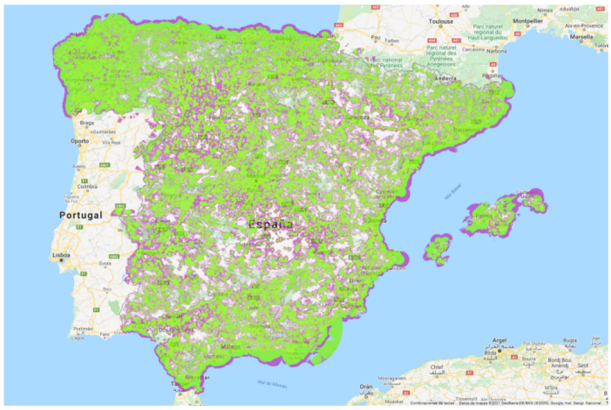

Figure 6 Movistar's 4G geographic coverage [27].

Figure 7 Orange's geographic coverage [28].

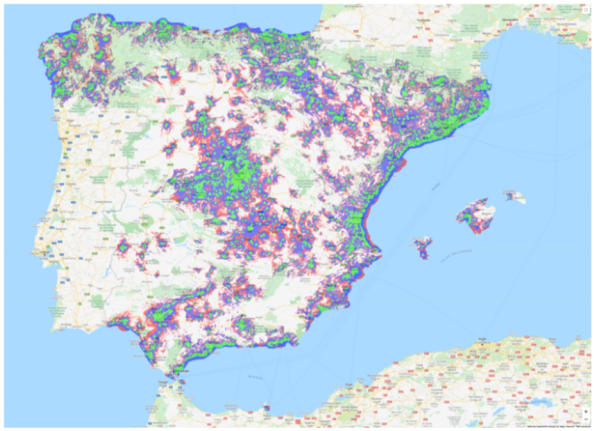

Figure 8 Vodafone's 4G geographic coverage [29].

– Dedicated Network:

The dedicated network is not deployed, but according to the data collected in Section 0, it can be estimated that in order to achieve a deployment equivalent to 70% of the geographical area, between 1,700 and 4,500 stations would be necessary, and for 95% between 2,260 and 6,000, which is initially unfeasible except for a budgetary improvement in the contract that would allow deployment times to be shortened to between 2 and 4 years, or the duration of a contract plus an extension.

Under normal conditions and with a 3-year contract, only 30% coverage could be achieved.

Therefore, the score could be between

$$P_1 = 10x\frac{30}{95.8} = 3.1\ puntos \text{ and } P_1 = 10x\frac{95.8}{95.8} = 10\ puntos$$

Therefore, a policy decision aimed at improving the budget of the Contract could accelerate the availability of coverage or if this decision is aimed at prioritising deployment in certain areas it could influence the speed of deployment.

– Hybrid Network:

Coverage calculation for hybrid network is more complex as several factors are involved: the type of hybridisation and the coverage provided by the radio access network which may be shared or complemented by a commercial operator.

Although initially, it can be said that at least $P_1 > 7.3$ *points*.

- *Traffic capacity (P_2):*

Today, the essential service of a public safety communications network is voice, so it must be ensured that the available traffic capacity of the network covers at least this service.

The capacity in number of individual VoIP communications (Table 4) that an LTE cell can serve based on the available bandwidth was shown in 0, as well as its variation when group communications are introduced.

For the assessment of this criterion, an urban micro-cell will be taken in which there are registered users working in groups of 20 and 50 users per group.

– Commercial Network:

Assuming a commercial network with available bandwidth of 20 MHz, the maximum capacity will be 1600 VoIP communications. This type of network works only in Unicast mode, therefore, the number of simultaneous communications will be:

Num_{com}= 1600/20=**80**

Num_{com}= 1600/50=**32**

In reality, the capacity will be lower, as bandwidth is shared with commercial users of the network.

– Dedicated Network:

A dedicated network with 5 MHz bandwidth has 400 VoIP communications, but when using eMBMS each group communication will consume the equivalent of one Unicast communication. Therefore, **the number of simultaneous communications will be 400**, despite having less bandwidth than in the previous case.

– Hybrid Network:

In this type of network, although a MOCN type modality would allow working in MBMS mode, as the RAN is shared with an operator and they use this service, it will not be possible to implement it and take advantage of its benefits in terms of spectral use, so, although they have 20 MHz of bandwidth, it will pass through as in commercial networks and will have a capacity of **80 and 32 simultaneous communications**, depending on the size of the group.

Therefore, applying the expression defined for this criterion gives the following results:

	Commercial Network	Dedicated Network	Hybrid Network
P_2 (20 users/group)	2	10	2
P_2 (50 users/group)	0.8	10	0.8

- *Availability (P_3):*

Typically, the required availability of a public safety or emergency communications system is above 99%. Real examples are the mobile communications network of the Govern de les Illes Balears with a contractually required availability for the radio access network of 99.7% [30] or the emergency digital communications network of Galicia with an availability for individual base stations of 99.7% and for the radio access network of 99.975% [31].

Therefore, requiring an availability value of 99.8% for such a network would be within reason. In fact, the current average availability of the SIRDEE network is over 99.8%.

– Commercial Network:

For commercial networks it has not been possible to find actual service availability information, but an estimate can be made thanks to the availability data from the SIRDEE network.

All SIRDEE grid sites have power backup, which the commercial grid does not. Therefore, by observing the power outage data for a specific period and for a province, it is possible to deduce the inoperative time of a commercial grid, since it does not have energy back-up. In this case, as indicated in Table 8, the availability of a commercial network would be above 97.33%, without taking into account other factors that may leave the network without service.

Month	Province	Ebs	Hours/Batt	% NON-FALL EB	% SIRDEE Service	% Service WITHOUT Batt
January	Malaga	43	764	2.47%	99.80%	97.33%

Table 8 Estimated unavailability in case of not having batteries (Prepared internally)

$$P_3 = 10x\frac{97.33}{99.8} = 9.75\ puntos$$

– Dedicated Network:

The dedicated network shall comply with the availability requirements for public safety networks and shall therefore have an availability value of 99.8% or higher.

$$P_3 = 10x\frac{99.8}{99.8} = 10\ puntos$$

– Hybrid Network:

Based on the type of hybridisation chosen, sharing the radio access network with the commercial network would mean inheriting the availability seen for the commercial network, i.e. 97.33%.

Alternatively, the radio access network could normally be dedicated, meeting public safety requirements, but complemented by the commercial network in areas where there is insufficient coverage.

In that case, it follows that the availability in this type of network will be equal to or greater than 97.33% and less than 99. 8%. Therefore,

$$10\ puntos > P_3 \geq 9.75\ puntos$$

- *Security (P_4):*

– Commercial Network:

Such networks, owned by commercial operators, do not usually have security features at their sites and therefore do not have a prior security check on the personnel hired and working on the premises:

$$P_4 = 0\ puntos$$

– Dedicated Network:

These networks are prepared with security features at all levels, with good password management, access control and the hiring of security-guaranteed personnel, therefore:

$$P_4 = 10\ puntos$$

– Hybrid Network:

This type of network, having shared elements, will, depending on the type of hybridisation, share security elements that will protect some infrastructures. Therefore:

$$P_4 = 5\ puntos$$

- *Cost (P_5):*

– Commercial Network:

To find the cost of a critical communications service based on a commercial network, no data has been found, but an estimate can be made from the commercial tariffs of the main operators (Movistar, Orange and Vodafone) [32], [33], [34] with 4G flat-rate tariffs with unlimited data. In general, these tariffs are around €20 per line per month. This is equivalent to €240 per year, but does not include terminal, terminal maintenance, MCPTT application and of course the control room service.

– Dedicated Network:

For the estimation of the cost of a dedicated network, a cost estimate has been used based on operational information from the SIRDEE network, assuming a network in the 450 MHz band. Considering a 10-year amortisation period, the cost of the service would be around M€70m/year[8].

Assuming that the number of terminals is maintained (72,000), the cost of the service would be approximately €972/year per terminal, slightly lower than the current cost of the narrowband service.

– Hybrid Network:

Case of France [35]: early this year, the critical communications service was put out to tender for 48 months renewable for an additional 36 months for a total value of €900m. In principle, it appears from the information in the tender journal that the coverage concerns only the metropolitan areas of France.

[8] For reasons of data protection, no further details of this study can be included.

The expected number of users of the network is 400,000. Taking into account that the user to terminal ratio is 2 to 1, according to the news published in Critical Communications Today [36] there would be 200,000 terminals. On this basis, it is estimated that the service should cost approximately **€643/year** per terminal.

The publication of FirstNet's tariffs has also been found [37], although it is very varied and depends on the type of plan, the 5GB and 50 GB monthly tariff with terminal included can be taken as a reference. The result of the calculation is included in Table 9.

Type of tariff	Price/month ($)	Price/year ($)	Price/year (€)
5GB	$61	€732	€604
50GB	$247	$2,964	€2,445

Table 9 Cost of the FirstNet network for the 5GB and 50 GB per month plans (Source: FirstNet)

From the above price data we can estimate the final expression based on the maximum and minimum prices.

$$P_5 = 10x\frac{2445 - Precio_{evaluado}}{2445 - 240}$$

The following table shows the scores obtained for each case:

	Commercial Network	Dedicated Network	Hybrid Network	
P_5	10	6.7	France	8.2
			$FirstNet_{5GB}$	8.3
			$FirstNet_{50GB}$	0

a) Final score:

Once the individual scores for each criterion have been obtained, the weighting corresponding to each criterion is applied in order to obtain the final score for each alternative:

	Peso	Red Comercial	Red Dedicada	Red Híbrida
Cobertura	**18%**	7,3	3,1	7,3
Tráfico	**21%**	2	10	2
Disponibilidad	**25%**	9,75	10	9,75
Seguridad	**21%**	0	10	5
Coste	**15%**	10	6,7	8,2
TOTAL	**100%**	**5,67**	**8,28**	**6,45**

b) Influence of some political decisions on scoring:

In Section 0, we identified some hinterland policies that could be developed that could affect the performance of the alternatives under study in some way. We then proceed to assess how they actually influence the final assessment of each of them.

Some of the interior policies identified include:

- Decision to regulate the prioritisation of emergency communications in commercial networks: Considering that commercial and hybrid networks do not implement the MBMS service, the actual capacity of these networks will not increase. What will happen is that the total capacity or the capacity estimated in such prioritisation will be exclusively for public security services, but they will not be better than those calculated without this policy.
- Decision to regulate national roaming: It will lead to an improvement in coverage for services using the commercial and hybrid networks, although it can be seen from the coverage maps included in Section 0 that a similar level of coverage to the SIRDEE network will not be achieved. It is estimated that 80% of the entire territory could be reached. Its score would therefore change to 8.3.
- Decision to oblige operators to strengthen the protection of sites serving critical infrastructure areas: this decision: This decision would result in operators protecting part of their infrastructure, but would not reach the level required for a public safety network, so the score in that case would be 5.
- Decision to prioritise service availability in certain areas based on factors such as population or crime concentration. This decision would change deployment priorities but not the overall values for coverage, traffic or availability.

Therefore, considering the political factor, the final score would be as follows:

	Peso	Red Comercial	Red Dedicada	Red Híbrida
Cobertura	**18%**	8,3	3,1	8,3
Tráfico	**21%**	2	10	2
Disponibilidad	**25%**	9,75	10	9,75
Seguridad	**21%**	0	10	5
Coste	**15%**	10	6,7	8,2
TOTAL	**100%**	**5,85**	**8,28**	**6,63**

7.- CONCLUSIONS.

A multi-criteria methodology for the selection of the strategy for the deployment and implementation of a broadband communications network for public safety has been proposed, which has provided an assessment for each of the identified alternatives.

The conclusions should aim, on the one hand, at the validity of the method and, on the other hand, at justifying the possible strategy that should be chosen for the evolution of the public safety net.

The result obtained in the assessment of alternatives reflects the current situation and having a dedicated network is the most convenient deployment strategy at present when it comes to providing a communications service to public security forces.

However, technological developments and the emergence of new commercial solutions in the coming years may modify the current performance of commercial and hybrid networks, influencing a possible change in the result obtained by applying this methodology under the new circumstances.

On the other hand, this methodology could also be "fine-tuned" by applying greater precision to certain assessment criteria. A clear example would be to increase territorial precision in the availability of coverage.

As a final thought, these systems suffer from the so-called "fire extinguisher phenomenon", which is the necessary expenditure on an object that goes unnoticed in most of its useful life, and one could conclude that it is completely dispensable because it is not used; however, when an emergency situation arrives, if it is not there the impact of not having it can be terrible, and the same happens with public safety and emergency communications networks, they are the only ones that work in disaster situations and must continue to do so.

8.- REFERENCES

[1] Commission Implementing Decision (UE) 2016/687, of 28 April 2016, on the harmonization of the 694-790 MHz frequency band for terrestrial systems capable of providing wireless broadband electronic communications services and for flexible national use in the Union.

[2] Ministry of Economic Affairs and Digital Transformation. *National Frequency Allocation Table*. Order ETD/1449/2021, 16 December 2021. Available at: https://www.boe.es/buscar/act.php?id=BOE-A-2021-21346&p=20211224&tn=3

[3] "*La Policía Local de Alcobendas implanta un innovador sistema de comunicaciones móviles*", La Vanguardia, 30 August 2011. Available at: https://www.lavanguardia.com/local/madrid/20110830/54208745054/la-policia-local-de-alcobendas-implanta-un-innovador-sistema-de-comunicaciones-moviles.html

[4] *Release 1999*, 3GPP Release 99, December 1999. Available at: https://www.3gpp.org/specifications-technologies/releases/release-1999

[5] T. Nakamura, "*Proposal for Candidate Radio Interface Technologies for IMT-Advanced Based on LTE Release 10 and Beyond (LTE -Advanced)*," in ITU-R WP5D 3rd Workshop on IMT-Advanced, 5 October 2009.

[6] *Common functional architecture to support mission critical services, Stage 2 (Release 17)*, 3GPP TS 23.280 V17.6.0, April 2021.

[7] 3GPP website. Available at: https://www.3gpp.org/.

[8] R. Agustí Comes, F. Bernardo; F. Casadevall, R. Ferrús, J. Pérez and O. Sallent,. "LTE: Nuevas tendencias en comunicaciones móviles". Vodafone Spain Foundation. 2010, p. 55-109.

[9] *Release 15 Description*, 3GPP TR 21.915 V15.0.0, September. 2019. Available at: https://www.3gpp.org/ftp/Specs/archive/21_series/21.915/

[10] First Responder Network Authority, "*FirstNet Partners with AT&T to Build Wireless Broadband Network for America's First Responders*", Available at: https://2014-2018.firstnet.gov/news/firstnet-partners-att-build-wireless-broadband-network-americas-first-responders

[11] FirstNet. *Nationwide Coverage*, Available at: https://www.firstnet.com/coverage.html

[12] M. Warwick, *New UK Emergency Services Network delayed yet again. It will be outdated before it is operational*, TelecomTV, 15 September 2020, Available at: https://www.telecomtv.com/content/4g-lte/new-uk-emergency-services-network-delayed-yet-again-it-will-be-outdated-before-it-is-operational-39673/

[13] R. Mellies, *France Broadband PPDR Network: RRF Status update,* presented at Public Safety Radiocommunications Group, November 2022.
[14] *Rugged LTE 410-430 MHz terminal for PPDR*. Nordic Telecom Systems a.s., 16 March 2020, p 4-8.
[15] J Nally, *"Finland strides ahead with Virve 2.0,"* Critical Comms, Nov/Dec 2020, Available at: https://issuu.com/westwick-farrowmedia/docs/critical_comms_nov_dec_2020/s/11206246
[16] J. O'Halloran, "*First 3GPP-compliant public safety network with MCPTT launches in South Korea*," Computer Weekly, 26 April 2021. Available at: https://www.computerweekly.com/news/252499799/First-3GPP-compliant-public-safety-network-with-MCPTT-launches-in-South-Korea
[17] T. Gray, "*Why MCPTT Interoperability is Vital for Public Safety*," MissionCritical Communications, 4 February 2019. Available at: https://www.rrmediagroup.com/Features/FeaturesDetails/FID/896
[18] *Multimedia Broadcast/Multicast Service (MBMS), Architecture and functional description (Release 17),* 3GPP TS 23.246 V17.0.0, March 2022.
[19] J. Wannstrom, "*Carrier Aggregation explained*", 3GPP. Available at: https://www.3gpp.org/technologies/101-carrier-aggregation-explained
[20] J. Alonso, "*La distribución de la población española, una anomalía en Europa"*, La Razón, 10 Jan 2021, Spain, (in Spanish) [Online]. Available: https://www.larazon.es/economia/20210110/6jbova3gyvbcxggjmzc3vhswai.html
[21] J. Marcos, "*El 30% del territorio español concentra el 90% de la población"*, El País, 8 Oct 2018, Spain, (in Spanish) [Online]. Available: https://elpais.com/politica/2018/10/05/actualidad/1538767620_420819.html
[22] *LTE; Feasibility study for Further Advancements for E-UTRA (LTE-Advanced) (3GPP TR 36.912 version 11.0.0 Release 11)*. ETSI Technical Report TR 136.912, October 2012, p 34-40.
[23] *Santiago Bernabeu Stadium*, Real Madrid CF. Available at: https://www.realmadrid.com/estadio-santiago-bernabeu
[24] *Récord histórico de portabilidad: más de 1 millón de cambios de operador en septiembre*, CNMC, 18 December 2020. Available at: https://www.cnmc.es/prensa/mensual-telecos-portabilidad-record
[25] *Availability performance parameters and objectives for end-to-end international constant bit-rate digital paths,* ITU-T G.827, Sep, 2003, pp 4-7.
[26] T. Herrero, "*El 5G aviva la batalla tecnológica entre China y EEUU*", El Diario. 26 February 2019. Available at: https://www.eldiario.es/tecnologia/conectividad-alas-auge-huawei-europa_1_1675218.html
[27] *Cobertura geográfica 4G de Movistar*. Movistar. Available at: https://www.movistar.es/particulares/coberturas/movil
[28] *Cobertura geográfica 4G de Orange*. Orange. Available at: https://www.orange.es/4g#
[29] *Cobertura geográfica 4G de*. Vodafone. Vodafone. Available at: https://www.vodafone.es/c/conocenos/es/vodafone-espana/mapa-cobertura-movil/
[30] *Pliego de Prescripciones Técnicas de la Red Digital de Comunicaciones Móviles en las Islas Baleares*, Govern de Illes Balears, October 2010.
[31] *Xunta de Galicia. Technical Specifications for the Galician Corporate Network of Mobile Digital Emergency and Security Communications*. Ministry of Industry, Energy and Tourism. December 2012.
[32] Movistar service tariffs. Available at: https://www.movistar.es/particulares/movil/tarifas-moviles/

[33] Orange service tariffs. Available at: https://www.orange.es/tarifas/movil
[34] Vodafone service tariffs. Available at: https://www.vodafone.es/c/particulares/es/productos-y-servicios/movil/contrato/tarifas-contrato/
[35] Radio Network of the Future (RRF), French Ministry of Interior, Tenders Electronic Daily, 4 December 2020, Available at: https://ted.europa.eu/udl?uri=TED:NOTICE:586641-2020:TEXT:FR:HTML&tabId=5&tabLang=en
[36] *France's push for public safety broadband*. Critical Communications Today. 19 August 2019. Available at: https://www.criticalcomms.com/features/france-ppdr-broadband-rrf-pcstorm
[37] Mobile-Pooled & Mobile-Unlimited Plans for the FirstNet Evolved Packet Core, FirstNet (AT&T), USA, 2022. Available at: https://www.firstnet.com/content/dam/firstnet/white-papers/GOV-firstnet-primary.pdf