Universidad Zaragoza
1542

Trabajo Fin de Grado

NECESIDAD DE ENLACE DE DATOS DE UN GACA PARA LA IMPLANTACIÓN DE TODAS LAS CÉLULAS TALOS NECESARIAS. POSIBLES SOLUCIONES.

CAC. D. Héctor Mainar Rubio

Director académico: Col Artª (R) Antonio Martínez de Baños Carrillo

Director militar: Cap Artª Alberto Aznar Calavia

Centro Universitario de la Defensa-Academia General Militar

2022

“La artillería convierte en un espectáculo lo que hubiese sido una simple batalla.”

Rey Federico II el Grande

Agradecimientos

La realización de este Trabajo Fin de Grado se ha llevado a cabo durante las prácticas externas en el Grupo de Artillería de Campaña (GACA I/20) del Regimiento de Artillería de Campaña nº 20, encuadrado en la Brigada Aragón I.

En primer lugar, quisiera expresar mi especial gratitud a mi director académico el coronel D. Antonio Martínez de Baños Carrillo por su gran implicación y sus constantes consejos y orientaciones para la realizar este trabajo de la mejor manera posible.

Por otro lado, agradecer a mi director el capitán D. Alberto Aznar Calavia, jefe de la Batería de Plana Mayor del Grupo de Artillería de Campaña I/20, al capitán D. José Ramón Álvarez Moya, jefe de la 1ª Batería, al teniente D. Rodrigo Miguel Campo, FDO de Grupo, encuadrado en la Batería de Plana Mayor del Grupo de Artillería de Campaña I/20, a la teniente Dña. Rebeca Santos Palenzuela, jefe de la 1ª sección de la 1ª Batería y al alférez reservista voluntario D. Óscar Fernando Salas Moreno, su total implicación para afrontar este proyecto. A la vez, agradecerles también sus consejos en cuanto al trato con el personal, que es de gran importancia para el ejercicio del mando en las unidades.

Por último, agradecer a todo el personal del Grupo su trato y su entera disponibilidad para ayudar en lo posible, y en especial a la Batería de Plana Mayor y a la 1ª Batería en las cuales he realizado estas prácticas externas y como no a mi familia y amigos que han sido los que me ha estado apoyando en los momentos de flaqueza para poder cumplir mi sueño de ser oficial del Ejército de Tierra.

RESUMEN

La utilización de métodos de enlace de datos basados en IP LAN para la transmisión de datos entre las células TALOS pueden proporcionarnos ventajas significativas en cuanto a la rapidez del enlace y el alcance de dicha transmisión de enlace. Todo esto hace que se obtenga una visión del campo de batalla en tiempo real.

El motivo principal de este trabajo de fin de grado es buscar una solución factible y posibilista a las debilidades que en la actualidad existen en la artillería de campaña y que están relacionadas con la falta de enlace, cobertura y alcance todo ello sin menospreciar la seguridad de transmisión de los datos transmitidos. Por tal motivo, este trabajo está focalizado en la utilización de *hardware* y procedimientos que utilizan la tecnología IP LAN y que puede ser una solución al enlace de datos de las células TALOS de un GACA, acercándose al concepto de “Fuegos en red” presente en el proyecto de Fuerza 2035.

Se ha realizado un estudio de las distintas soluciones compatibles IP LAN, entre las que se encuentran red VPN (Hamachi), LoRa / LoRaWAN, antena Ubiquiti (Bridge) y el conjunto router Wifi, repetidor y antena de alta impedancia. Se detallan sus características fundamentales, haciendo hincapié en la seguridad que proporciona cada una de ellas, ya que es uno de los factores que más peso tiene a la hora de buscar nuevas soluciones al problema del enlace; conclusión obtenida después de las encuestas realizadas al personal del Grupo de Artillería de Campaña (GACA 20).

Para estudiar la viabilidad de cada una de las soluciones propuestas se ha utilizado el análisis DAFO en el cual se detallan todas las debilidades, amenazas, fortalezas y oportunidades de cada una de las soluciones. Además, debido a que el coste económico es un factor importante, se ha realizado un estudio de mercado para poder dar un presupuesto real de lo que costaría cada solución.

Palabras clave

Enlace, TALOS, C^2, IP LAN, Artillería.

ABSTRACT

The use of IP LAN-based data link methods for data transmission between TALOS cells can provide significant advantages in terms of link speed, and link transmission range. Thus, it is possible to obtain a view of the battlefield in real time.

The main reason for this final degree project is to find a feasible and possible solution to the weaknesses that currently exist in the field artillery framework and are related to the lack of link, coverage and scope, all without underestimating the security of data transmission. For this reason, this work is focused on the use of hardware and procedures that use IP LAN technology and that can be a solution to the data link of the TALOS cells of a GACA, approaching the concept of "network fires", present in the *Fuerza 2035* (Force 2035) project.

A study of the different compatible IP LAN solutions has been carried out, among which are the VPN network (Hamachi), LoRa / LoRaWAN, Ubiquiti antenna (Bridge) and the Wifi router, repeater and high impedance antenna set. Its fundamental characteristics are detailed, emphasizing the security provided by each of them, since security is one of the heaviest factors when looking for new solutions to the link problem after the surveys that have been carried out among the personnel of the Field Artillery Group (GACA 20).

To study the viability of each of the proposed solutions, the SWOT analysis has been used in which all the strengths, weaknesses, opportunities, and threats of each of the solutions are detailed. In addition, because economic cost is an important factor, a market survey has been taken into consideration in order to give a real budget of what each solution would cost.

In short, the implementation of procedures and new hardware for data link using IP LAN technology would mean opening up a wide range of possibilities to alleviate current problems due to the means available.

KEYWORDS

Link, TALOS, C^2, IP LAN, Artillery.

INDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ABREVIATURAS, SIGLAS Y ACRÓNIMOS

A/D: Apoyo Directo.

ACA: Artillería de Campaña.

ACAF: Adquisición y Control de Apoyo de Fuegos.

ACO: *Airspace Control Orders* (Orden de Control del Espacio Aéreo).

AES: *Advanced encryption Standard* (Encriptación Estándar Avanzada).

AES: *Advanced Encryption Standard* (Estándar de Cifrado Encriptado).

ARP: *Address Resolution Protocol* (Protocolo de resolución de Direcciones).

ASCA: *Artillery Systems Cooperation Activities* (Sistema de Cooperación de Actividades de Artillería).

ATO: *Air Tasking Order* (Orden de Misión Aérea).

ATP: Autopropulsado.

BCL: Búsqueda de Canal Libre.

Bía: Batería.

BOMET: Boletín Meteorológico.

C^2: *Command and Control* (Mando y Control).

CMAC: *Cypher-Based Message Authentication Code* (Código de autenticación de mensajes basado en cifrado).

CO: Centro de Operaciones.

COMSEC: *Communication Security* (Seguridad de las Comunicaciones).

DAFO: Debilidades, Amenazas, Fortalezas y Oportunidades.

DEN: Destacamento de Enlace.

DNS: *Domain Name System* (Nombre del Dominio del Sistema).

DRECO: Destacamento de Reconocimiento.

ECM: *Electronic Countermeasures* (Contramedidas Electrónicas).

EPM: *Electronic Protective Measures* (Medidas de Protección electromagnéticas).

ET: Ejército de Tierra.

FAS: Fuerzas Armadas.

FD: Frecuencia Fija Digital.

FDC: *Fire Director Center* (Centro Director de Fuegos).

FDO: *Fire Director Officer* (Oficial Director de Fuegos)

FFC: Frecuencia Fija de Canal.

FFG: Frecuencia Fija General.

FSE: *Fire Support Element* (Elemento de Apoyo de Fuegos).

GIS: *Geographic Information System* (Sistema de Información Geográfica).

HF: *High Frecuency* (Frecuencia Alta).

HPT: *High Pay-off Target* (Objetivo de Alto Rendimiento).

HVT: *High Value Target* (Objetivo de Alto Valor).

IP: *Internet Protocole* (Protocolo de Internet).

JLP: Jefe de Línea de Piezas.

LAN: *Local Area Network* (Red de Área Local).

LPWAN: *Low Power Area Network* (Red de Área de Baja Potencia).

NVIS: *Near Vertical Incidence Skywave* (Onda celeste de incidencia casi vertical).

OAV: Observador Avanzado.

OTAN: Organización del Tratado del Atlántico Norte.

PC: Puesto de Mando.

PCBON: Puesto de Mando de Batallón.

PDA: *Personal Digital Assistant* (Asistente Digital Personal).

PLM: Plana Mayor.

RACA: Regimiento de Artillería de Campaña.

SFR: Salto de Frecuencia.

TCP: *Transmission Control Protocol* (Protocolo de Control de Transmisión).

TFG: Trabajo de Fin de Grado.

TRANSEC: *Transmission Security* (Seguridad de las Transmisiones).

UDP: *User Datagram Protocol* (Protocolo de Datagrama de Usuario).

UHF: *Ultra High Frecuency* (Frecuencia Ultra Alta)

VHF: *Very High Frecuency* (Frecuencia muy Alta).

VPN: *Virtual Private Network* (Red Privada Virtual).

WAN: *Wide Area Network* (Red de Area Amplia).

WEP: *Wireless Equivalent Privacy* (Privacidad Equivalente Inalámbrica).

WPA: *Wireless Protected Access* (Protección de Acceso inalámbrica).

WPS: *Wi-Fi Protected Setup* (Configuración de Wi-Fi Segura)

1 INTRODUCCIÓN

Este Trabajo de Fin de Grado (TFG), ha sido realizado en el Regimiento de Artillería de Campaña Número 20 (RACA 20), perteneciente a la Brigada Aragón I y, esta a su vez, a la División Castillejos. Dicho trabajo trata sobre el estudio de la "Necesidad de Enlace de Datos de todas las células TALOS de un Grupo de Artillería de Campaña". Esta necesidad surge de la aparición de nuevos escenarios de conflicto y el cambio constante en los métodos y procedimientos que hay que adaptar a estos escenarios.

Desde los orígenes de la Artillería en el siglo XVI, la rapidez con la que se adquirían los objetivos ha sido vital para hacer fuego de manera eficaz y oportuna sobre ellos; conforme ha evolucionado la guerra, la rapidez exigida ha sido cada vez más demandante. Hoy en día los actos de guerra se deciden en cuestión de minutos e incluso segundos, por ello se necesitan medios acordes con esta premisa del tiempo.

Hasta hace unos pocos años todos los datos y órdenes se transmitían a través de fonía mediante radios, como la AN/PRC-25 o la radio PR4G. Desde 1991 hasta 2010, se utilizó el sistema "GAXI", un sistema de Mando y Control (C^2) de artillería que fue desarrollado en el GACA XI, de ahí su nombre. Este sistema supuso una revolución y conllevó a empezar a utilizar la transmisión por datos.

Hoy en día existe un sistema de C^2, desarrollado por la empresa GMV el sistema TALOS, un sistema que permite a las unidades de artillería de campaña planear y conducir una operación por medio del TALOS Táctico y calcular con precisión los datos de tiro que necesitan las piezas para hacer fuego y batir un objetivo, mediante el TALOS técnico. Aparte de estos dos subsistemas del TALOS existen varias versiones para PDA / Tablet, que permiten funciones más básicas pero suficientes para según qué puesto táctico. Este sistema se usa no solo en artillería, sino que también puede integrar morteros y fuegos de la armada.

La forma que se tiene de enlazar este sistema y sus subsistemas actualmente es mediante la radio PR4G, la cual permite tanto tráfico de datos como de fonía. Pero existen habitualmente dificultades a la hora de transmitir datos y fonía a la vez, a pesar de que la radio cuenta con modo habilitado para ello. Ante este problema y la falta de enlace por fallos del sistema TALOS se opta por utilizar la fonía para transmitir órdenes lo cual deriva en un retraso en la transmisión de estas; ya que sí es cierto que es rápida y segura, aunque infinitamente más lenta (ver anexo 'protocolo de fuego de una pieza') que un sistema de transmisión de datos en el cuál las órdenes llegan en el acto,

"El empleo de sistemas automáticos para remitir las órdenes y los datos hace que se eviten errores a la hora de ser transmitidos. No obstante, la transmisión de los datos a las piezas que no estén dotadas de sistemas automáticos se realiza por sistema de voz, lo que puede dar lugar a algún error o necesidad de repetición de las órdenes o a alguna de sus partes." (Mando de Adiestramiento y doctrina , 2021).

Por todo lo anterior expuesto, ante la necesidad de que todas las células de un GACA tengan enlace de datos y la falta de un consenso sobre estas nuevas tecnologías en la doctrina, se proponen una serie de posibles soluciones de datos a este problema y que pueden dar una idea firme sobre hacia dónde encaminar el enlace.

A falta de una doctrina común, las unidades han probado soluciones muy diversas, llegando a hacer avances en algunos aspectos del enlace, pero sin un éxito total. Por todo ello, durante este estudio se van a presentar, estudiar y valorar varias opciones, analizando los pros y contras de cada una de ellas, teniendo en cuenta la Taxonomía de Bloom[1] , para intentar buscar la solución a dichos problemas de enlace de datos mediante el estudio de varias soluciones que incluyen nuevo *hardware* y procedimientos.

1.1 Estructura del trabajo

Dicho trabajo se va a organizar en primer lugar con la exposición de los objetivos y alcance de este proyecto, además mediante el estudio del arte, se mostrará cómo se realiza el enlace en la actualidad en las unidades de artillería de campaña del ejército español. A continuación, se realizará el estudio de cada una de las soluciones propuestas, en la que se analizarán los pros y los contras de cada una de ellas y las oportunidades que ofrece cada una. Una vez estudiadas y analizadas todas las soluciones, se realizará un estudio económico de los costes que supondría adquirir un sistema para cada solución y finalmente, se concluirá con las lecciones aprendidas de este estudio.

[1] La Taxonomía de Bloom, desarrollada por el psicólogo estadounidense Benjamin Bloom, es una clasificación piramidal de los objetivos educativos basado en la complejidad del proceso cognitivo que conllevan.

2 OBJETIVOS Y METODOLOGÍA

2.1 Objetivos y alcance

El objetivo general de este trabajo es encontrar soluciones al enlace de datos de un GACA, utilizando medios disponibles en dotación y otros no disponibles pero que se podrían adquirir, mediante el uso de sistemas IP LAN.

Estos materiales son civiles y por lo tanto no disponen, *a priori*, de una seguridad tan alta como nos dan los medios que se tienen en dotación como es la PR4G, pero que pueden ser de utilidad para tener una base desde la que empezar y poder dotarles con la seguridad adecuada.

Para poder llegar al objetivo general hay que cumplir una serie de objetivos específicos los cuales son:

- Describir el problema de enlace de datos.
- Analizar qué medios serían eficientes y aptos para el enlace de datos.
- Realizar un estudio de mercado de las posibles soluciones.
- Comparar los elementos que cumplan nuestras necesidades.
- Valorar cada una de las soluciones propuestas.
- Proponer una solución viable que solucione dichos problemas.

El alcance de este proyecto se limita a un GACA en A/D a una Brigada, sin entrar en el ámbito de morteros ni de fuegos de la armada, con lo cual cuando se hable de piezas nos referiremos al Obús 'ATP M-109 A5E' y al Obús 'Light Gun L118', ambos materiales del GACA 20. Descartamos, por tanto, el Obús '155/52 SIAC', por no ser orgánico de la unidad y porque, al ser un obús tecnológicamente más avanzado, no tiene tantos problemas de adaptación al sistema C^2.

Figura 1: Izquierda a derecha. Obús Light Gun L118 y Obús ATP M-109 A5E (Fuente: (Army Guide, 2012), (As.com, 2022))

También se va a realizar un estudio de cada célula TALOS y sus necesidades para comprobar si el sistema TALOS que utilizan es el óptimo o si sería necesario alguna modificación.

En este Trabajo de Fin de Grado, se va a estudiar y a probar la posibilidad de enlazar el sistema TALOS por comunicaciones IP, así como qué células podrían mejorar su eficacia implantando este sistema de comunicación.

De todos los modos IP que el sistema TALOS nos ofrece, este TFG se centrará en estudiar los modos 'IP LAN UDP Multicast', 'IP LAN UDP Broadcast' e 'IP LAN TCP' con

un nodo central; excluyendo el 'IP LAN Unicast', 'IP LAN Harris 7800S', 'IP LAN TLX5', 'IP MUX' e 'IP SAP'. Cabe decir que los modos anteriormente citados, no se analizarán como tal, sino que, partiendo de esos modos, se van a proponen soluciones al enlace con diversos materiales, los cuales serán expuestos y explicados en el cuerpo de este trabajo.

2.2 Metodología

Se utilizará una metodología constructivista basada en una visión holística y epistemológica del estudio del planteamiento[2]. La Taxonomía de Bloom es la base de la concreción de los objetivos de este TFG. El asesoramiento sintetizado de especialistas, el análisis de documentos bibliográficos, y los resultados de una encuesta dirigida tanto al personal de la unidad en la que se desarrolla en trabajo (RACA 20) como también a otras unidades similares (GACA VI y GACA I/11), son los elementos esenciales de la metodología. Todo lo expuesto reflejará el verdadero problema que tienen las unidades en la transmisión de datos en campaña y vislumbrarán los mejores medios de transmisión de datos.

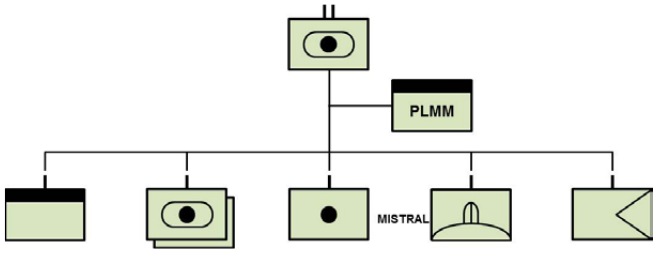


Figura 2: Orgánica de un GACA (Fuente: (Mando de Adiestramiento y doctrina , 2021))

Se utilizarán herramientas para mostrar secuencias de acciones, gráficos para mostrar los resultados, así como un análisis DAFO[3] de cada una de las soluciones que se estudien. Estos datos permitirán categorizar la información para, posteriormente, valorar el rendimiento del enlace. Se hará una aproximación de valoración económica de lo que supondría la puesta en práctica del sistema TALOS con los nuevos elementos de enlace.

En cuanto a las encuestas se ha optado por las de respuesta cerrada, para intentar focalizar lo máximo posible en los temas que afectan al desarrollo de este TFG. En las entrevistas se ha optado por un sistema mixto o semiestructurado en el cuál no estaban fijas las preguntas, con esto se consigue que sean de carácter más informal y el entrevistado se encuentre más cómodo y tenga libertad para contestar lo que de verdad piensa, sin tener que ceñirse a responder a una pregunta.

[2] Gerald M. Edelman ilustra esta idea diciendo que «Cada acto de percepción es en cierto grado un acto de creación y cada acto de memoria es a cierto modo un acto de imaginación». (Páez, 2019)

[3] El análisis DAFO es una técnica indispensable para analizar y dar constancia de la situación actual de un determinado proyecto, con esta técnica se pueden reunir los aspectos claves de un proyecto, debilidades, amenazas, fortalezas y oportunidades.

Tras analizar los resultados de la primera encuesta, podemos decir que el enlace por métodos IP LAN, es necesario implementarlo en los enlaces vía TALOS y, sería una buena línea de estudio y mejora. La segunda encuesta se focalizó en las características que deben tener esos sistemas IP LAN, y se llegó a la conclusión de que la seguridad, el ancho de banda y el coste eran lo que más valoraban los encuestados. Por ello, en cada sistema se procederá a explicar la seguridad que nos ofrece y el ancho de banda. En el ámbito económico, se realizará un estudio de costes de cada una de las soluciones planteadas (Ver Anexo I).

Para dar mayor veracidad a las encuestas se comprobó, durante los distintos ejercicios de instrucción y adiestramiento realizados en las prácticas en la unidad, que los problemas de enlace eran frecuentes, llegando a perder el enlace durante mucho tiempo y entre varias células debido al alcance de los medios disponibles y a la orografía del terreno, por lo tanto, quedó reflejado que era un problema real y que había que buscar otros medios de enlace que paliaran estos problemas de enlace.

3 ANTECEDENTES Y MARCO TEÓRICO

3.1 Antecedentes

Como se ha dicho anteriormente en la introducción, después del sistema de transmisión GAXI, se desarrolló el sistema TALOS que se ha ido actualizando conforme a la evolución de las necesidades de la artillería. El sistema TALOS cuenta con dos subsistemas. El subsistema TALOS Técnico, cuya función es llevar a cabo la dirección del tiro, y el TALOS Táctico que sirve para el planeamiento y la conducción de las operaciones. Actualmente el sistema TALOS cuenta con varias opciones de transmisión de datos (IP LAN UDP, IP LAN TCP, etc.), pero en la práctica sólo se utiliza la transmisión mediante la radio PR4G, ya que es el único recurso que dispone el ET con seguridad suficiente y que tiene de las capacidades necesarias para la transmisión de datos. Existen varios modos de transmisión de datos IP LAN, que se incluyen en él, pero no se disponen de medios para llevarlo a cabo; por tanto, siempre se opta por la PR4G. En caso de fallo, la transmisión de datos deja de existir y se realiza por medio de fonía. Actualmente, en algunas unidades, se están probando varios sistemas de transmisión diferentes de la radio PR4G, pero en la doctrina no se incluye ningún modelo a seguir, excepto con la PR4G (GMV, 2020).

Una de las últimas versiones de esta radio, la PR4G Supermux, cuenta con el modo de transmisión IP SAP (datos) e IP MUX (datos y fonía). Por medio de datos, lo que hace es crear paquetes de transmisión datos y enviarlos, pero no de manera simultánea, sino que los envía de forma sucesiva. En la realidad, este modo da muchos problemas ya que la malla se suele saturar cuando se aumenta la actividad y es debido al escaso ancho de banda de la PR4G.

3.2 Estado del arte

A continuación, se va a exponer cómo funciona el TALOS (tanto el técnico como el táctico, según doctrina), los enlaces que se forman y cómo se realiza el enlace actualmente en las unidades con el material de dotación.

3.2.1 Talos Técnico

Como se ha mencionado anteriormente el TALOS Técnico sirve tanto para el mando y control de los fuegos de ACA, morteros o fuegos de la armada. En este caso nos centraremos en los fuegos de ACA según el manual de referencia de ACA del ET, el cual contempla algunas diferencias con respecto a lo que dice el manual de la empresa GMV. Las células TALOS que deben funcionar con el TALOS Técnico son: FDC (tanto de Grupo como de Bía), Observadores Avanzados (OAVs) y Destacamento de Reconocimiento (DRECO). Todas estas células están implicadas en la ejecución y/o la corrección de los fuegos.

El sistema es capaz de ofrecer un preciso cálculo de los datos de tiro, introducir BOMET, asignar quién va a realizar una acción de fuego, y recalcular los datos con la corrección hecha por los OAVs (GMV, 2020).

Mediante el TALOS Técnico y fonía se crea la Malla de Tiro, en la que se encuentran los FDCs, las piezas y los OAVs.[4]

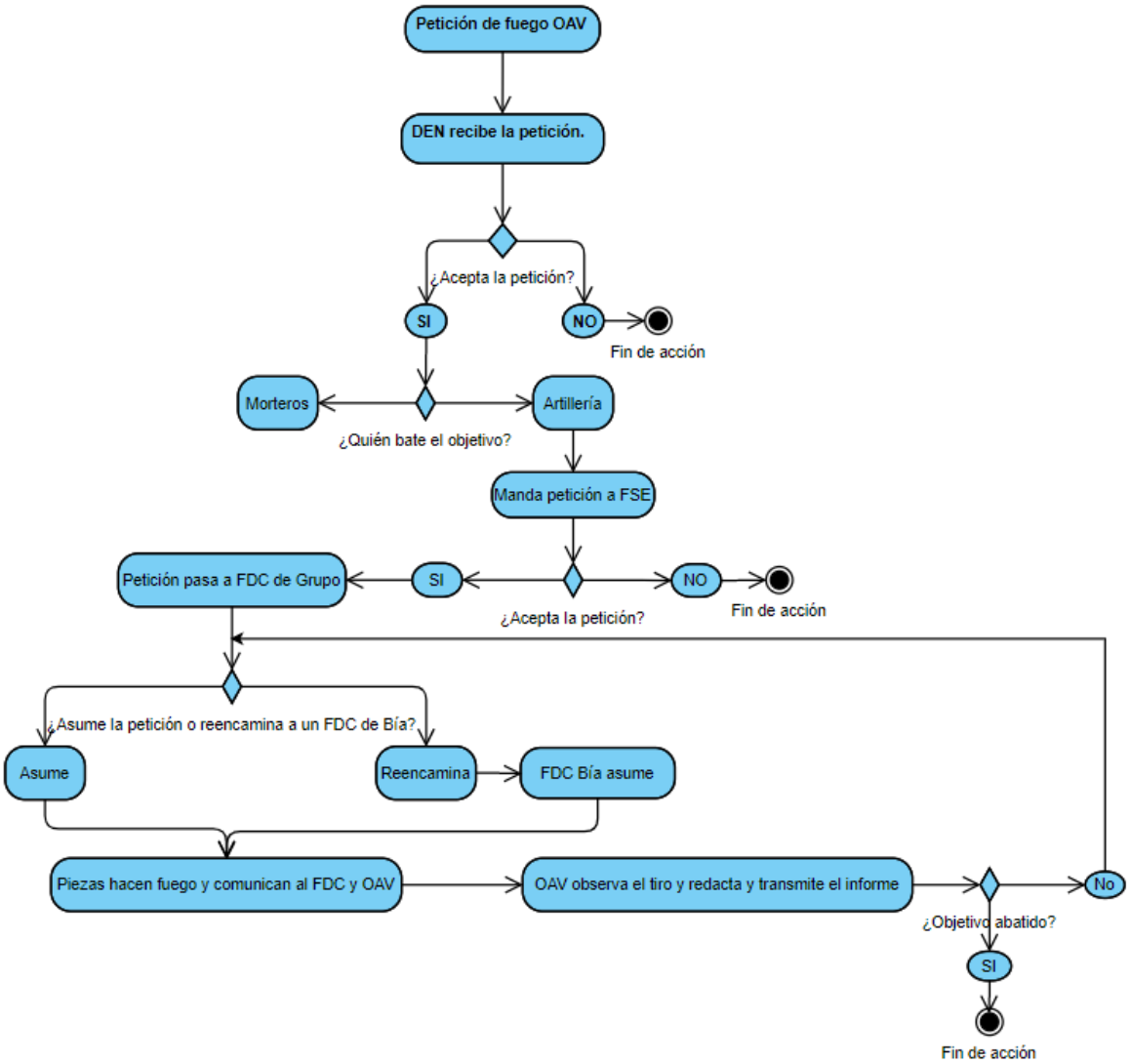


Figura 3: Esquema Acción de Fuego (Fuente: Elaboración propia (Mediante el programa visual Paradigm, 2021))

[4] Visual Paradigm es un programa que tiene diversas herramientas para llevar a cabo el desarrollo de un proyecto. Este programa se vio en la asignatura de la Ingeniería de Oficina de Proyectos.

3.2.2 Talos Táctico

El sistema táctico del TALOS permite preparar futuras acciones de fuego, coordinar todos los fuegos directamente y saber dónde están y cómo están todos sus elementos, como por ejemplo el número de proyectiles disponibles. El TALOS Táctico es una herramienta más orientada al planeamiento y a la conducción que al cálculo de datos de tiro del que se encarga el TALOS Técnico. El TALOS Táctico tiene la capacidad de crear las unidades que van a participar en las operaciones y mostrar su posición en tiempo real en el medio GIS que el sistema integra. También permite establecer medidas de coordinación de la maniobra, rutas, material, personal, estado de las unidades y la creación de objetivos pudiendo fijar objetivos como HVT y HPT. En cuanto al planeamiento permite cargar en el sistema las misiones de apoyo tipo, la matriz de efectos, el modelo de acción y los planes de cambio de posición, entre otras.

Aparte de este planeamiento puramente de artillería, permite coordinar y agregar medidas para el control del espacio aéreo (ACO y ATO), las cuales se difunden a todas las unidades de la maniobra para evitar que se derriben aeronaves propias o aliadas, así como permitir establecer zonas en las que se realizará fuego por parte del ejército del aire.

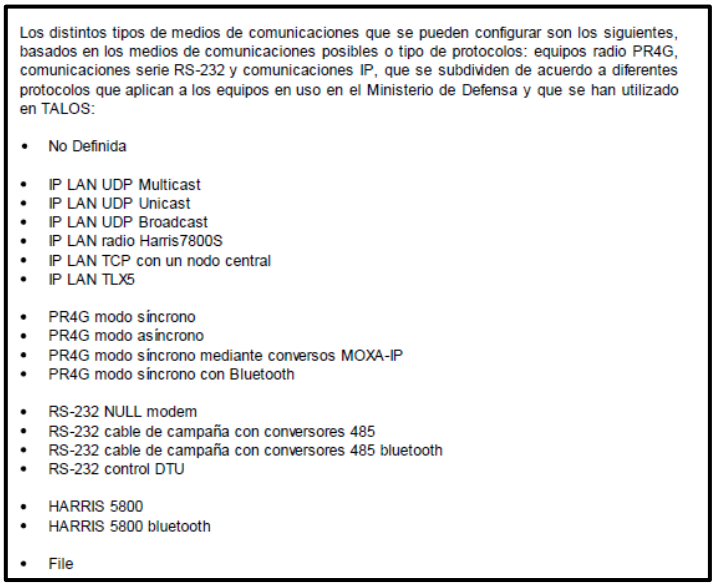
Este subsistema, el TALOS Táctico, es el utilizado en los FSE de distinto nivel. También se utiliza a nivel de unidades de artillería para todo lo relativo a mando y control, implantándose en los distintos CO y puestos de mando generados por los GACA,s. Actualmente se está introduciendo el TALOS táctico en los OAV´s. Este subsistema les da mucha más capacidad de transmisión ya que están desplegados a vanguardia junto con las unidades de maniobra. Por ello, tener un sistema de mando y control en el que puedan cambiar diversos aspectos de la maniobra en tiempo real es mucho más rápido y permite que se lleve un control más efectivo. Para poder entenderlo mejor se puede explicar fácilmente con un ejemplo, el OAV ve que en una ruta por la que se pretendía avanzar, está minada y, este hecho, no ha sido detectado en el transcurso de la maniobra; por lo tanto, el OAV puede transmitir mediante el TALOS táctico un informe que el jefe de la maniobra puede ver de forma instantánea. La gran ventaja es que la toma de decisiones se puede acortar en el tiempo (GMV, 2020).

3.2.3 Malla T2T

Se debe configurar la malla T2T para que el FDC de Grupo y el CO se puedan comunicar correctamente, puesto que el primero tiene el subsistema técnico y el segundo el subsistema táctico, Esta malla que no es más que un método de enlace, normalmente por cable, conecta ambos TALOS para poder ejercer el control total de los fuegos, teniendo ambos sistemas unidos y con posibilidad de comunicación entre ellos.

3.2.4 Enlace datos

A pesar de que el sistema TALOS cuenta con bastantes opciones de configuración a la hora de establecer los enlaces de datos, en realidad la que más se utiliza cuando se sale de instrucción, por no decir la única, son las comunicaciones mediante la radio PR4G, orgánica en todas las unidades del ET.



Los distintos tipos de medios de comunicaciones que se pueden configurar son los siguientes, basados en los medios de comunicaciones posibles o tipo de protocolos: equipos radio PR4G, comunicaciones serie RS-232 y comunicaciones IP, que se subdividen de acuerdo a diferentes protocolos que aplican a los equipos en uso en el Ministerio de Defensa y que se han utilizado en TALOS:

- No Definida

- IP LAN UDP Multicast
- IP LAN UDP Unicast
- IP LAN UDP Broadcast
- IP LAN radio Harris7800S
- IP LAN TCP con un nodo central
- IP LAN TLX5

- PR4G modo síncrono
- PR4G modo asíncrono
- PR4G modo síncrono mediante conversos MOXA-IP
- PR4G modo síncrono con Bluetooth

- RS-232 NULL modem
- RS-232 cable de campaña con conversores 485
- RS-232 cable de campaña con conversores 485 bluetooth
- RS-232 control DTU

- HARRIS 5800
- HARRIS 5800 bluetooth

- File

Figura 4: Tipos de medios de comunicaciones TALOS (Fuente: (GMV, 2020))

Como podemos ver en la Figura 4, aparte de los modos de PR4G, existen muchos otros en los que no hace falta una radio que es un material cripto y de gran valor para el ejército, sino que mediante comunicaciones IP de distinta naturaleza se puede hacer funcionar el sistema TALOS con un alto rendimiento.

También existe la posibilidad de enlazar mediante cable, pero prácticamente ni se contempla, además como se ha dicho anteriormente, la guerra actual es cuestión de segundos, por ello este método no es válido en una situación real.

3.2.5 Modo de enlace por radio PR4G

Actualmente, el material que se dispone para realizar el enlace de las diferentes células TALOS es mediante la radio PR4G, siendo necesarias por cada célula una radio para el enlace de datos y una radio para el enlace por fonía, con la excepción de las nuevas radios PR4G Supermux, mencionadas anteriormente.

Esta radio de fabricación francesa, marca Thales, está actualmente en dotación en dos versiones[5], la segunda y tercera versión (PR4G V2 Y PR4G V3), siendo esta última en la que centraremos el estudio ya que es la que ostenta las mejores características en cuanto a enlace y seguridad. Cabe destacar que todavía en algunas unidades se utilizan las PR4G V2 para suplir la gran demanda en cuanto a enlaces que son necesarios actualmente.

[5] En servicio en las Fuerzas Armadas españolas desde 1992 cuando se introdujo su primera versión (PR4G V1), la cual está en desuso actualmente.

Tabla 1: Principales Características de enlace de la radio PR4G V3 (Fuente: (THALES , 2019))

Temperatura funcionamiento	-40ºC a 70ºC
Potencia de salida	10 W, 5 W, 0,25 W Versión vehicular de 50 W
Banda de frecuencia	De 30 a 88 MHz. Espaciado de 25 KHz, 2.320 canales
Transmisión de datos	Enrutamiento de paquetes IP Hasta 38,4 Kbps (módem asíncrono) Hasta 19,2 Kbps (canal dedicado) Hasta 4,8 Kbps (voz y datos simultáneos)
Modos de trabajo	Analógico, digital y relé.

Como podemos observar en la tabla, es una radio que apenas tiene limitaciones de temperatura en un ambiente habitable. Cuenta con una potencia máxima en su versión vehicular de 50 W y una potencia máxima en su versión portátil de 10 W, con esto permite un alcance máximo de 25 km en su montaje vehicular y de unos escasos 8 km en su montaje portátil; cabe decir que existe una configuración con antenas VHF sobre mástil HC – 30, que alcanza 50 y 15 kms, respectivamente, pero el establecer una antena de éstas características, hace que se pierda el aspecto de la movilidad ya que requiere tiempo montar esta configuración. Esta radio tiene la función relé que consiste en recibir y repetir una señal recibida con la potencia que disponga esa radio relé que dependerá de su configuración (portátil o vehicular) y que permitiría hacer despliegues más extensos.

Se trata de una radio que trabaja en VHF y consta de 2320 canales. Respecto a la transmisión de datos, podemos ver que la velocidad de transmisión no es muy alta, sobre todo en el modo de voz y datos simultáneos. (Mando de Apoyo y Doctrina, 2018).

Figura 5: Radio PR4G V3 ((THALES , 2019))

Esta radio tiene dos modos de trabajo, en analógico y en digital.

3.2.5.1 Modo Analógico

La radio funciona en frecuencia fija sin cifrar. Este modo permite la interoperabilidad con otras radios VHF de diferentes familias. El canal de FFG (frecuencia fija general) y las FFC (frecuencias fijas de canal) trabajan en este modo. Que no dispone de las claves de seguridad COMSEC y solo funciona para enlace de fonía.

3.2.5.2 Modo Digital

Hay cuatro modos digitales principales. En estos modos se puede aplicar el cifrado de la comunicación mediante una clave COMSEC. En todos los modos digitales, cuando la radio no está transmitiendo se encuentra en estado de “escucha”, de manera que, además del tráfico propio de la malla, vigila los siguientes canales:

• Canal de tiempo (para recibir la sincronización).

• Frecuencia fija de canal.

• Frecuencia fija general.

Por defecto, todas las vigilancias están habilitadas. Solo puede habilitar o deshabilitar las vigilancias sobre las frecuencias fijas.

Los modos digitales son:

• SFR (Salto en frecuencia). En este modo de funcionamiento se ejecutan 300 saltos de frecuencia por segundo. La ley de salto en frecuencia se obtiene utilizando una clave TRANSEC que garantiza una secuencia de frecuencias pseudoaleatoria. Este modo necesita de una radio que sincronice estos saltos y que se denomina ‘directora’.

• BCL (Búsqueda de canal libre). En este modo las radios cambian de frecuencia cada vez que emiten, escogiendo aquella que encuentran como mejor disponible de entre las que se han introducido en el plan de frecuencias.

• MIX (Modo mixto). En cada emisión, la radio escoge el modo de trabajo: SFR o BCL.

• FD (Frecuencia fija digital). La radio emite en frecuencia fija, pero a diferencia de los modos analógicos, la voz está digitalizada y se permite el cifrado de la comunicación.

Los modos SFR, BCL y MIX son interoperables entre sí (PR4G V3 Supermux).

• SAP: permite exclusivamente la transmisión de datos.

• MUX: a diferencia del modo SAP, permite la transmisión de voz y datos simultáneamente (Mando de Apoyo y Doctrina, 2018).

4 ESTUDIO DE LAS DISTINTAS CONFIGURACIONES IP LAN

A continuación, se van a exponer las distintas soluciones al enlace de datos, utilizando tanto material que existe en dotación como material civil, de coste sumamente inferior y que pueden marcar el futuro de los enlaces de datos dentro de la ACA e incluso en el futuro enlace por datos de la FUERZA 2035.

En el concepto de FUERZA 2035, que son los objetivos que se quieren lograr en el ejército español mediante adquisición de material e implantando nuevos procedimientos, se define el concepto de “Fuegos en Red”, que conlleva que todos los sistemas estén interconectados entre sí para obtener un dominio total del campo de batalla (Ejército de Tierra, 2019).

En este apartado, el más amplio, se expondrá el cuerpo fundamental del trabajo y se argumentarán las ideas principales y secundarias del mismo. Como se ha visto en los resultados de las encuestas, la seguridad en las comunicaciones es de los aspectos más relevantes a la hora de elegir un sistema que sustituya al actual.

4.1 Red VPN

Una VPN es una “red privada virtual”, es una tecnología de red que permite conectarse a una red local (LAN) en base a una red no controlada como es el caso de internet. Esta tecnología funciona creando un túnel encriptado a través de la red. Para realizar esta conexión se necesita un servidor VPN y uno o varios dispositivos desde los cuales se conectan, por ejemplo, un ordenador o un smartphone. Con este sistema no usaremos nuestra dirección IP, si no que usaremos la del servidor VPN. Este sistema no es inviolable del todo, pero consigue evitar ataques cibernéticos como ARP Spoofing[6] o DNS Spoofing[7].

Esta tecnología ya está implantada en el mundo civil y muchas empresas lo utilizan (Calvo, 2019) (Barbosa, 2020).

[6] La suplantación de identidad ARP Spoofing es un tipo de ataque cibernético en el cuál un actor malicioso envía mensajes ARP (Protocolo de resolución de direcciones) falsos a través de una LAN. Esto conlleva que el atacante conocerá la dirección IP real y puede tener acceso a los mensajes que se manden y reciban, así como, enviar mensajes falsos o detener los datos enviados. (Veracode, 2020)

[7] La suplantación de identidad del servidor de nombres de dominio o DNS Spoofing es un ataque cibernético en el cuál el actor malicioso consigue falsificar la dirección IP, consiguiendo que se desvíe el tráfico de datos a un servidor falso (Ionos, 2020).

Figura 6: Estructura VPN (Fuente: (Dataustral, 2021))

Hamachi es un *software* de la empresa LogMeIn, la cual permite crear una red local (LAN) y conectar dispositivos que están conectados por WAN. Una red LAN se suele crear en varios dispositivos que están cercanos a un mismo router, pero con Hamachi, se pude emular estén donde estén los dispositivos, con el único requisito que tengan conexión 3G o superior (Ver Anexo II). Además, estas redes llamadas VPN, son canales privados de extremo a extremo lo que conlleva una mayor privacidad. Para más seguridad, el sistema de encriptación con el que cuenta Hamachi es AES- 256, el cuál es casi imposible de descifrar sin saber la clave con la que se empezó la encriptación (vpn, 2020).

4.1.1 Protocolo de seguridad AES

El protocolo AES es un método de cifrado que protege los mensajes enviados y recibidos para evitar que un agente ajeno pueda verlos, robarlos o incluso insertar información falsa. Este protocolo utiliza la Ley de Moore[8] y se basa en operaciones que se ejecutan en bloques de 16 *bytes* (matriz 4 x 4). El funcionamiento se basa en una serie de trasformaciones, sustituciones y permutaciones de los *bytes* y consigue un texto cifrado el cual sólo se puede resolver si se conoce la clave y haciendo los pasos en orden inverso, es decir, que se necesita la clave tanto para el cifrado como para el descifrado (Jiménez, 2021).

Los protocolos más seguros son el AES-128 y el AES-256:

- **AES-128:** Se trata de un algoritmo que tiene una codificación basada en 128 bits, es decir que las claves que se creen mediante este protocolo van a tener un número equivalente a 2^{127} combinaciones en rondas de 10.

- **AES – 256:** Consiste en una codificación de 256 *bits*. Utiliza 14 rondas y las claves con este cifrado son de 2^{255} posibilidades.

[8] La Ley de Moore, la enunció Gordon Moore, cofundador de Intel, cuando se dio cuenta de que el número de transistores por unidad métrica en los circuitos electrónicos se había duplicado año tras año. Lo que viene a decir que predijo que cada vez los transistores serían más pequeños siguiendo la regla de que cada dos años habría el doble (Navas, 2018).

4.1.2 Estructura de los enlaces de un GACA mediante Hamachi

La estructura de los enlaces mediante Hamachi es bastante simple ya que es compatible con todos los dispositivos que están conectados a una red 3G.

Antes de usar Hamachi se tiene que instalar el programa en todos los dispositivos y crear las mallas que se requieran.

Para poder utilizar Hamachi el dispositivo debe tener instalado un sistema operativo compatible con éste, pudiendo ser Windows, Mac y Linus. Además, hay una versión Android y iPhone para equipos portátiles tipo móviles o PDA (vpn, 2020).

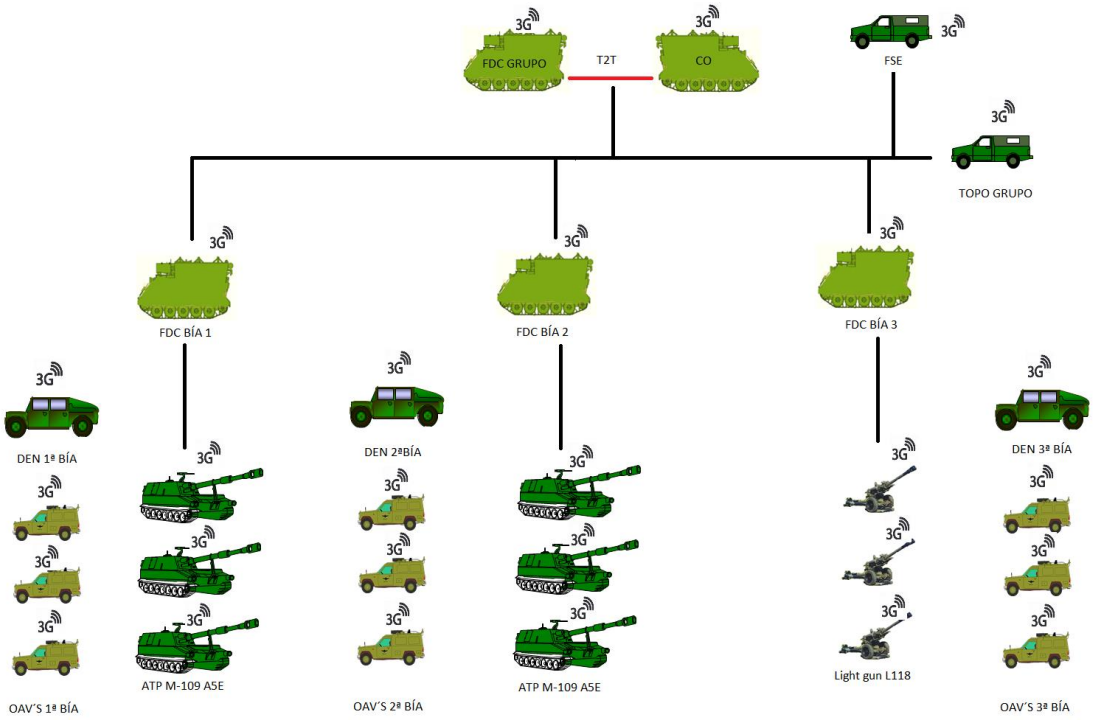


Figura 7: Configuración Enlace de un GACA mediante VPN (Fuente: Elaboración propia, 2021)

4.1.3 Análisis DAFO HAMACHI (Red VPN)

Tabla 2: Análisis DAFO Hamachi (Fuente: Elaboración propia, 2021)

ANÁLISIS DAFO HAMACHI	
Debilidades	**Amenazas**
• Tecnología Civil. • Sólo 5 células por malla en la versión gratuita. • Dependencia de cobertura 3G.	• Posibilidad de robo de datos. • Caída del servidor • Zonas de sombra 3G. • Escasa seguridad.
Fortalezas	**Oportunidades**
• Versión de pago, hasta infinitas células por malla. • Precio económico. • No depende de la visión directa entre células. • Distintas configuraciones de malla. • Interfaz muy intuitiva. • Seguridad AES- 256	• Capacidad de enlace a nivel global. • Posibilidad de tener cobertura global. • Crear una VPN a nivel interno de las FAS.

- **Debilidades:** Se trata de una tecnología civil; por lo tanto, dependeríamos de su servicio y estaríamos expuestos a fallos ajenos a nosotros. Destacar que se trata de un servicio gratuito de hasta 5 células, número insuficiente debido a que se necesitan un número muy superior de células. Por último, una de las mayores debilidades es la dependencia de disponer de una buena señal de cobertura, puesto que esta tecnología funciona como mínimo con cobertura 3G.

- **Amenazas:** Como todo sistema electrónico, puede ser vulnerable a ciberataques que busquen no solo perturbar la señal sino sacar información con distintos fines; además, los servidores pueden ser atacados para evitar su correcto funcionamiento o simplemente que se produzca algún fallo en los mismos y, por ello, se interrumpa la conexión por un tiempo desconocido. Las zonas de sombra de cobertura pueden limitar el despliegue, esto supone un gran problema si tenemos en cuenta que hay muchos lugares donde no existe cobertura y, aunque la hubiera, se podría perturbar fácilmente esa señal.

- **Fortalezas:** Esta solución es muy económica ya que la versión de pago dispone de dispositivos ilimitados y sólo se necesitaría disponer para los equipos TALOS de una conexión a internet, como la que pueden tener los teléfonos móviles. Además, cuenta con varias configuraciones de las mallas, las cuales son muy útiles, pudiendo modificarlas según las necesidades de la operación. Esta aplicación tiene la ventaja de que no necesita de la visión directa entre los equipos ya que sólo necesita tecnología 3G, pudiendo usarse 4G y 5G si se dispusiera de esa cobertura. También cuenta con una interfaz muy intuitiva lo que implica que la formación de los operadores es mínima para poder trabajar. Por último, utiliza un sistema de seguridad AES – 256, con el cual la posibilidad de que se pueda obtener información de esa señal es prácticamente nula.

- **Oportunidades:** Este sistema ofrece unas capacidades que nos da la oportunidad de tener enlace a nivel mundial, por lo tanto, al ser una tecnología de bajo coste y de fácil implantación. Se podría implantar un sistema de este tipo a nivel interno de las Fuerzas Armadas obteniéndose una ventaja, ya que no se dependería de una empresa civil y se trabajaría con más seguridad.

4.2 Sistema LoRa / LoRaWAN

En este apartado se va a estudiar el sistema LoRa / LoRaWAN, así como la seguridad que este ofrece y su posible implantación como método de enlace de datos.

4.2.1 ¿Qué es LoRa y LoRaWAN?

LoRa es una tecnología para comunicar pequeños dispositivos electrónicos empleados en la denominada Internet de las Cosas (IoT). LoRa es una tecnología inalámbrica (al igual que WiFi, Bluetooth, LTE, SigFox o Zigbee) que emplea un tipo de modulación en radiofrecuencia. Esta tecnología fue creada por la empresa Semtech[9].

LoRaWAN es un protocolo de red que usa la tecnología LoRa, para redes de baja potencia y área amplia, LPWAN (*Low Power Wide Area Network*) empleado para comunicar y administrar dispositivos LoRa.

El protocolo LoRaWAN se compone de *gateways* y nodos:

Los *gateways* son las antenas que se encargan de la emisión y recepción de datos a los nodos.

Los nodos son los dispositivos (sensores) que emiten y reciben la información a los *gateways* (LoRaWAN, 2020).

[9] Semtech es una empresa de EEUU, líder en semiconductores analógicos y de señal mixta de alto rendimiento, y algoritmos avanzados para infraestructura, equipos industriales y de consumo de alta gama (Semtech, 2020).

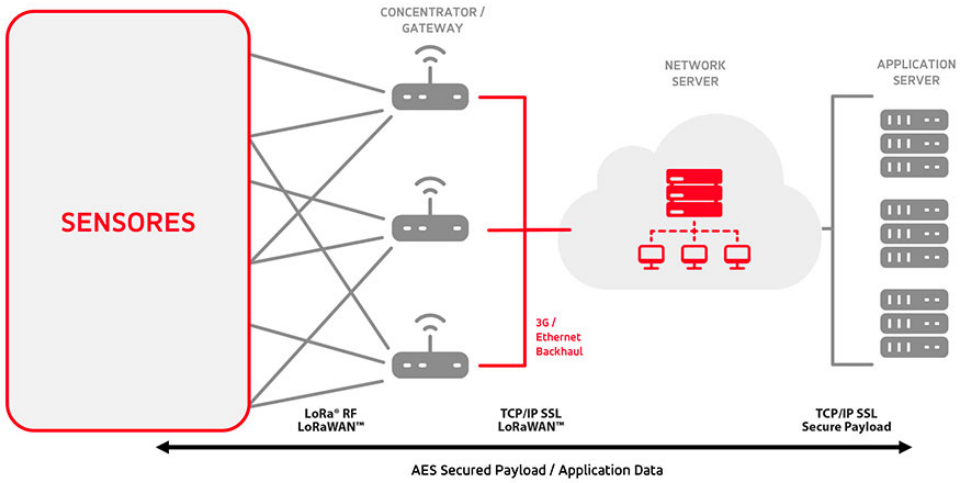


Figura 8: Esquema funcionamiento LoRa (Fuente: (Sáez, 2021))

4.2.2 Seguridad LoRaWAN

La seguridad de LoRaWAN se basa en el uso de algoritmos estándar y seguridad punto a punto. Entre sus propiedades destacan la autenticación mutua, protección de integridad y confidencialidad.

En cuanto a la autenticación mutua, garantiza que entre un dispositivo final LoRa (nodos o gateways) y la red LoRaWAN, los mensajes son autenticados desde su origen hasta su destino, estando encriptados y protegidos. Esto conlleva a que la información que se reciba proceda de un dispositivo legítimo y que los datos sean incomprensibles por los intrusos.

La seguridad de este sistema se basa en algoritmos criptográficos AES. En concreto, utiliza un el algoritmo AES 128 bits. Además, se combina con protocolos CMAC para la protección de la integridad y CTR para la encriptación. A cada dispositivo LoRaWAN se le asigna una clave AES de 128 bits y un identificador único global.

Tanto el receptor como el emisor realizan una solicitud de conexión entre ellos para verificar su identidad (Sáez, 2021) (Reimondo, 2019).

4.2.3 Análisis DAFO LoRa / LoRaWAN

Tabla 3: Análisis DAFO LoRa / LoRaWAN (Fuente: Elaboración propia, 2021)

ANÁLISIS DAFO LORA / LORAWAN	
Debilidades • Necesidad de "visión directa" entre células. • Escaso ancho de banda. • Necesitad de personal que pueda configurar el *software*.	**Amenazas** • Pérdida de "visión directa" entre las células. • En caso de condiciones adversas no está totalmente preparado para soportar climatología adversa.
Fortalezas • Bajo consumo. • Alta tolerancia a las interferencias. • Alta sensibilidad para recibir datos. • No necesita estar conectado a la corriente eléctrica. • Bajo coste. • Encriptación segura. • Fácil configuración y manejo. • Geolocalización.	**Oportunidades** • Posibilidad de conectar todas las células TALOS fácilmente. • Posibilidad de usar esta tecnología para la obtención de parámetros meteorológicos (sensores). • No hipotecar las radios actuales en sistemas de datos y utilizarlas únicamente para fonía.

- **Debilidades:** Esta tecnología necesita de visión directa o con pocos obstáculos entre sus células para que estas se puedan enlazar y poder transmitir la información de forma adecuada; además, cuenta con un ancho de banda limitado, lo que puede derivar en problemas a la hora de enviar archivos grandes. Esta tecnología presenta la ventaja de que se puede programar de infinitas formas según sus necesidades, pero esto conlleva la necesidad de personal especializado capaz de manejar la programación.

- **Amenazas:** Al moverse las células cuando se efectúa un cambio de asentamiento, puede ser que no se vean entre ellas y no se pueda disponer de este enlace; por otro lado, el *hardware* disponible actualmente no se encuentra totalmente preparado para soportar climatología adversa, y eso iría en contra de los estándares del ET.

- **Fortalezas:** Estos dispositivos apenas consumen energía, lo que es muy idóneo para operaciones de larga duración ya que permiten reducir la huella logística; pueden alimentarse mediante baterías y mediante corriente eléctrica. Es muy resistente ante las interferencias y tiene una alta sensibilidad para recibir señal, lo cual nos permite que, con un mínimo de fortaleza de señal, se pueda enlazar. Utiliza un triple cifrado que hace que esta tecnología sea extremadamente segura. Al tener muchas posibilidades de configurar las diferentes mallas, este sistema es de bajo coste y se puede configurar de infinitas maneras según las necesidades; así mismo decir que, una vez creado el programa, su configuración es muy sencilla, y por tanto, el operador no necesita demasiada formación para operarlo. Este sistema permite obtener una geolocalización sin GPS.

- **Oportunidades:** Alternativa de bajo coste y de gran rendimiento ante los fallos de conexión mediante PR4G. Esta tecnología permite programar el dispositivo y al poder añadirle diversos componentes, como son unos sensores, se podría utilizar también como estación meteorológica, que directamente podría enviar la información obtenida. Ante la fácil saturación del ancho de banda de las PR4G, se puede usar este sistema para el envío de cierta información y evitar saturar las mallas de transmisiones.

4.3 Antena Ubiquiti

4.3.1 ¿Qué es Ubiquiti y qué prestaciones nos ofrece?

En este apartado nos centraremos en las soluciones que ofrece la empresa Ubiquiti Networks, Inc[10], especializada en antenas. Este material utiliza la tecnología AirMax que rompe con la tradicional tecnología basada en el protocolo 802.11, que se utiliza en las redes de uso interior para la conexión vía Wifi, entre otras.

Hay diversidad de dispositivos Ubiquiti, pero a grandes rasgos se pueden clasificar en dos tipos: ‘Enterprise’ y ‘Broadband’. EL primero de ellos se utiliza para desplegar redes Wifi potentes y cableadas en un entorno cercano; se utiliza en domótica, circuitos de vigilancia por video y VozIP. El segundo está dedicado a las conexiones a grandes distancias. Es el que se va a desarrollar en este trabajo ya que tiene los requisitos necesarios en los que estamos trabajando. A continuación, se va a detallar cómo funciona esta tecnología (Spw, 2019).

[10] Ubiquiti Networks, Inc, es una empresa estadounidense, fundada en 2003, que diseña y fabrica soluciones inalámbricas tanto para redes de uso interior como redes de uso exterior de larga distancia (Spw, 2019).

Figura 9: Configuración Ubiquiti sobre TOA (Fuente: Elaboración propia, 2022)

Figura 10: Configuración sobre mástil (Fuente: Elaboración propia, 2022)

4.3.2 Tecnología AirMax

Como ya se ha dicho anteriormente, AirMax sustituye al protocolo 802.11 mejorando sus prestaciones y eliminando sus desventajas. AirMax es una tecnología que se encuentra dentro de 'Broadband'; prioriza a los usuarios activos en vez de los pasivos, lo que conlleva a una mejor latencia o menor retardo a la hora de la transmisión de datos. En cuanto al protocolo AirMax decir que se basa en la tecnología de radio MIMO[11] que ofrece una transmisión de datos reales de hasta 150 Mbps dependiendo de la configuración que puede ser bien 'Enlace punto a punto' o bien 'Enlace punto-multipunto'.

El 'enlace punto a punto' conecta 2 redes como si se tratase de una sola permitiéndose el intercambio de datos entre dichas redes. Se consigue una velocidad de transmisión de datos de hasta 150 Mbps. El 'enlace punto-multipunto' consiste en que un punto central transmite información hacia otros puntos y, desde estos hacia el nodo central evitando transmitir información de punto a punto directamente sin pasar por el nodo central. En esta configuración se consiguen velocidades de transmisión de datos de hasta 100 Mbps (Arci, 2019) (DeanTenas, 2020).

4.3.3 Seguridad Ubiquiti

En cuanto a la seguridad podemos diferenciar entre la seguridad de *software* y de *hardware*. En cuanto a *software* podemos implementar el mayor protocolo de seguridad que dispongamos, pero en lo que respecta a los productos Ubiquiti nos tenemos que centrar en la seguridad a nivel *hardware* pues es la que los hace diferentes con respecto al resto de soluciones planteadas. Se puede configurar con 'seguridad WEP' *(Wireless Equivalent Privacy)* que se trata de un proceso muy anticuado con muchos fallos. Por otro lado, está la 'seguridad WPA' *(Wireless Protected Access)* que fue la solución a los problemas de seguridad que mostraba la seguridad WEP. Por último, se encuentra la 'seguridad WPA2' que mejora sustancialmente a su predecesora WPA. Por ser la que más interesa al estudio se va a analizar la WPA2 (Spw, 2019).

WPA2 utiliza un algoritmo de cifrado simétrico por bloques AES (Ver apartado 4.1.1) al contrario que sus predecesoras, que utilizan un algoritmo de cifrado de flujo,

Esta versión introduce dos nuevos protocolos de seguridad:

- **4-way *Handshake* o negociación de 4 mensajes**: En primer lugar, se crea una PSK *(Pre Shared Key)*. Tanto el nodo principal como el de los usuarios pueden proveer al otro la clave para la autenticación PMK *(Pairwise Master Key)*, de modo que los mensajes enviados entre ellos sólo puedan ser descifrados sabiendo dicha clave; con esto se evitan ataques de usuarios maliciosos. Además, con este protocolo se crea otra clave llamada PTK *(Pairwise Transient Key)* la cual se genera mediante varios atributos como son la dirección MAC del nodo principal y la dirección MAC del usuario. Por último, se genera una cuarta clave GTK *(Group Temporal Key)*, que es una clave temporal que se utiliza para descodificar los mensajes enviados.

[11] MIMO es una tecnología en la que una antena receptora tiene la capacidad de recibir tanto la onda trasmitida directamente como las ondas rebotadas de esa misma onda, las cuales llegan con un desfase en el tiempo. Esto permite combinar los datos de las diferentes ondas para aumentar la eficacia y el poder de captación de la señal (Webedia Brand Services, 2016).

- **Group Key Handshake - GTK:** La GTK es temporal, por lo tanto, necesita actualizarse cada cierto tiempo, normalmente cada vez que un usuario deja la red, así se evita que ese usuario siga recibiendo datos**.** Cada vez que sucede esto, el nodo central envía una nueva clave a cada usuario y, este último, le envía un acuse de recibo de la nueva clave.

Se puede observar que es una tecnología que utiliza diversos protocolos de seguridad que la hacen muy fiable, pero, para obtener el mayor rendimiento, hay que configurarlo de tal manera que se introduzcan contraseñas seguras (más de 20 dígitos) y desconectar el WPS *(Wi-Fi Protected Setup)* para evitar usuarios maliciosos (Córdoba, 2017).

4.3.4 Análisis DAFO Ubiquiti

Tabla 4: Análisis DAFO Ubiquiti (Fuente: Elaboración propia, 2021)

ANÁLISIS DAFO UBIQUITI (BRIDGE)	
Debilidades • Necesidad de enfrentarse los aparatos. • Poca seguridad. • Necesidad de un aparato por cada célula. • Tecnología civil.	**Amenazas** • Pérdida de visión entre ellos. • Posibilidad de interferencias del enemigo.
Fortalezas • Largo alcance. • Alta transmisión de datos. • Fácil de configurar. • Resistente a condiciones meteorológicas adversas. • Bajo coste. • Fácil de instalar.	**Oportunidades** • Establecer una conexión rápida y eficaz. • No hipotecar las radios actuales en sistemas de datos y utilizarlas únicamente para fonía.

- **Debilidades:** Para cada célula se necesita un aparato con el cuál recibir y emitir información. Este sistema tiene la necesidad de que todos los aparatos utilizados tengan visión directa entre sí; esto implica que un aparato pueda perder el enlace si hay algún obstáculo entre ellas. Este sistema, *a priori,* no tiene apenas medidas de seguridad. Dichas medidas deberían ser aportadas por el tipo de transmisión de datos. Se trata de una tecnología civil.

- **Amenazas:** En el caso de que se perdiera la visión entre dos células, serían incapaces de enlazar entre ellas y, por consiguiente, se perdería el enlace, teniendo que volver a reorientarse y conseguir enlazar, lo que supondría una pérdida de tiempo. Como este dispositivo no cuenta con ninguna medida de seguridad en su fabricación, sería fácilmente perturbable por los sistemas de guerra electrónica del adversario.

- **Fortalezas:** Con esta tecnología se consigue un largo alcance, de hasta 30 Kms (permite una alta transmisión de datos por lo que solucionaríamos el problema de saturación de las mallas). Este tipo de tecnología está diseñada para ser usada en exteriores de forma continua, por lo tanto, está diseñada para resistir climatología adversa. Otra característica de este sistema es su bajo coste si lo comparamos con lo que cuesta el equipo del que actualmente disponemos; por lo tanto, a pesar de que se tuviera algún problema de rotura del material o fallo del propio aparato interno, obtener un recambio sería asequible y se podría tener en *stock*. El montaje de estas antenas es muy sencillo, basta con conectarla al dispositivo del que se quiera enviar los datos, elevarlo en altura (si hace falta), y encararlo hacia otro aparato para el intercambio de información. Además, se puede acceder desde el dispositivo al que está conectado para ver su estado y realizar cambios en algunos de sus parámetros.

- **Oportunidades:** Permite realizar una conexión prácticamente de manera instantánea, lo cual es de vital importancia para poder tomar decisiones lo más rápidas posibles y poder llevar el control en tiempo real de la batalla.

Debido a su ancho de banda y a la ganancia de estas antenas se pueden enviar datos, e incluso hasta video, de manera eficiente y rápida, lo cual, las hace mucho más eficaces que las radios actuales permitiendo de más información de las operaciones. Además, el uso de esta tecnología como método de transmisión de datos permite deshipotecar radios y utilizarlas como radios de fonía en otros cometidos.

4.4 Router Wifi + Repetidor + Antena de alta impedancia

4.4.1 Router Wifi

La tecnología Wifi utiliza ondas de radio para transmitir datos de un enrutador a los dispositivos conectados y así poder intercambiar información y tener todo interconectado. Esta solución ya se aplica en algunas unidades, pero sólo se ha conseguido enlace a escasas decenas de metros. Donde más se utiliza es en la instrucción de Grupo que se realiza en un aula con todos los equipos cercanos pero separados para simular un despliegue real y así, poder practicar sin tener los problemas de un despliegue real en los que influye la meteorología, la orografía, etc.

Para aplicar esta solución se necesita un router que conectado a una fuente de alimentación cree una red LAN, en la cual los demás equipos se puedan conectar a ella e intercambiar información entre sí. Para ello, dichos equipos deberán contar con una antena Wifi (Cisco, 2018).

4.4.2 Repetidor

Un repetidor Wifi sirve para aumentar la señal inicialmente emitida por un *router* y así poder llegar a tener más alcance usando la misma red Wifi. Su funcionamiento consiste en dos enrutadores, uno de ellos recibe la señal Wifi, lo transmite al otro y este vuelve a emitir la señal potenciada, de manera que ganamos alcance y calidad en la señal. Estos aparatos requieren de energía eléctrica para poder funcionar; hay que tener la precaución de situarlos donde todavía la señal Wifi sea estable y con buena calidad para sacarle su mayor rendimiento. Se pueden usar tantos repetidores como se quiera para llegar a tener el alcance deseado (Fernández, 2021).

4.4.3 Antena Alta Impedancia

La impedancia de una antena es la relación entre la tensión y la corriente en sus terminales de entrada.

$$Z_i = \frac{V_i}{I_i} = R_a + jX_a$$

Figura 11: Impedancia de una antena (Fuente: (UPV, 2016))

Con una mayor impedancia, que se consigue entre otras formas incrementando el voltaje o disminuyendo la corriente, estas antenas consiguen ser más susceptibles a las ondas, dicho de otro modo, al tener una alta impedancia consiguen recibir y transmitir datos con escasa señal. Aplicado a nuestro caso, donde haya escasa cobertura Wifi, con estas antenas se puede amplificar la señal haciendo que se pueda transmitir información a mayor distancia sin tener pérdida de señal considerable.

4.4.4 Conjunto Wifi + Repetidor + Antena de Alta Impedancia

Con lo expuesto anteriormente, los tres sistemas por separado no son lo suficientemente útiles para mejorar sustancialmente el enlace. La combinación de los tres sistemas hace que se trate de una solución asequible que mejora mucho el alcance del enlace, pudiendo usarse para la transmisión de datos debido al ancho de banda disponible. En cuanto al despliegue de los medios, cada célula debería contar con ambos sistemas (repetidor y antena de alta impedancia), con los cuales según las necesidades propias del despliegue utilizar uno de ellos, o ambos, para conseguir el enlace entre todas las células.

4.4.5 Seguridad Wifi

En cuanto a la seguridad, la tecnología Wifi, que engloba los tres sistemas, indicar que utiliza varios cifrados, desde WEP hasta WPA2-AES (Ver apartado 4.4.3). De todos ellos el que más seguridad nos brinda es el WPA2 – AES. En cuanto a la seguridad de los mensajes, podemos implementar el mayor protocolo de seguridad que dispongamos.

4.4.6 Análisis DAFO Wifi

Tabla 5: Análisis DAFO Wifi (Fuente: Elaboración propia, 2021)

ANÁLISIS DAFO WIFI + REPETIDOR + ANTENA ALTA IMPEDANCIA	
Debilidades • Necesidad de un amplificador por cada célula (solo válido para portátiles). • Vulnerable a climatología. • Tecnología civil. • Necesidad de compatibilidad con todos los tipos de *hardware* de los que se disponen.	**Amenazas** • Posible perturbación por el enemigo. • Según orografía, perdida de enlace.
Fortalezas • Alcance suficiente. • Fácil instalación. • Precio muy económico. • Salva pequeños accidentes geográficos. • Seguridad suficiente.	**Oportunidades** • Dar cobertura a todo un despliegue de ACA con muy pocos medios y de poco coste. • No hipotecar las radios actuales en sistemas de datos y utilizarlas únicamente para fonía. • Conexión rápida y eficaz.

- **Debilidades:** Cada célula debe disponer de una antena de alta impedancia para asegurar, sea cual sea su despliegue, una conexión estable. Además de que sólo se pueden conectar a los ordenadores portátiles y no a las PDA[12], todas las células TALOS disponen de un ordenador portátil, desde el cuál se maneja el programa pero los OAV,s disponen de PDA,s, debido a que a su reducido tamaño y peso, son fáciles de transportar, ya que éstas células van acompañando a las unidades de maniobra y por lo tanto puede darse la posibilidad de que se vaya a pie y tengan que llevar todo el equipo encima. Son sistemas que no disponen de protección necesaria para soportar climatología adversa, por lo que se tendría que adaptar algún tipo de carcasa que no afectara al rendimiento pero que asilara de los agentes meteorológicos. Se trata de una tecnología civil con los riesgos que conlleva de suministros y repuestos.

[12] Se comprobó de manera práctica que el sistema operativo del que actualmente disponen las PDA *(Windows Embedded),* no es compatible con las antenas de alta impedancia disponibles en el mercado.

- **Amenazas:** A pesar de que las conexiones Wifi están cifradas con el protocolo WPA2- AES, se pueden ver perturbadas por algún ataque electrónico que evite o dificulte la transmisión de datos. En el caso de un tener un despliegue amplio o una avería en un repetidor, se podría perder el enlace entre algunas células, teniendo que volver a instalar otro o bien funcionar por fonía. En cuanto al terreno, si el despliegue está en terreno muy abrupto y las distintas células separadas por grandes obstáculos geográficos, posiblemente habrá mala conexión, pudiéndose solucionar colocando un repetidor donde haya visibilidad entre los dos puntos que no tienen enlace.

- **Fortalezas:** Con estos tres sistemas se consigue un alcance suficiente hasta en los despliegues más amplios de un GACA ya que su instalación es muy sencilla y, por lo tanto, no requiere apenas instrucción del operador para instalarlo y manejarlo. Al tratarse de una tecnología que está muy extendida, la obtención de estos productos es muy económica puesto que hay mucha oferta. Además, no es imperativo que dispongan de visión directa entre dichas células ya que las ondas que emiten estos sistemas pueden salvar pequeñas masas del terreno sin tener apenas perdida de señal.

- **Oportunidades:** Se puede conseguir un despliegue amplio de un GACA de un modo muy económico, eficiente y con un despliegue escaso de medios. Además, se consigue deshipotecar las radios para poder utilizarlas en los casos que más se necesiten. En cuanto a la velocidad de transmisión de datos esta solución es muy eficaz puesto que se puede enviar un volumen de datos aceptable a una alta velocidad, lo que se refleja en el aumento de información a la hora de tomar una decisión casi en tiempo real.

4.5 Análisis Económico

A continuación, se va a llevar a cabo un análisis económico de las distintas soluciones. Decir que se va a incluir sólo el coste del sistema en sí, sin tener en cuenta costes como el cableado, tornillería, etc., para adaptarlos a los distintos vehículos, aunque de una solución a otra, estos gastos no supondrían una gran diferencia económica (Ver Anexo III).

Tabla 6: Análisis Económico (Fuente: Elaboración propia, 2022)

	HARDWARE	CONTRATACIÓN SERVICIO EXTERNO
VPN (HAMACHI)	27 € (Tarjeta con conexión a internet con datos ilimitados a alta velocidad)	45 €/ Año (Max. 32 células)
LoRa / LoRaWAN	47 € (Antena, bidireccional)	-
BRIDGE (UBIQUITI)	60 € (Antena bidireccional) 199 € (Antena omnidireccional)	-
WIFI + REPETIDOR + ANTENA DE ALTA IMPEDANCIA	Wifi: 74 € Repetidor:75€ Antena Alta Impedancia: 32 € Total: 181 €	-

Tabla 7: Coste total de un GACA[13] (Fuente: Elaboración propia, 2022)

	HARDWARE	CONTRATACIÓN SERVICIO EXTERNO
VPN (HAMACHI)[14]	9072 € / año	45 €/ Año (Max. 32 células)
LoRa / LoRaWAN	1316 € (Antena bidireccional)	-
BRIDGE (UBIQUITI)	1680 € (Antena bidireccional) 5572 € (Antena omnidireccional)	-
WIFI + REPETIDOR + ANTENA DE ALTA IMPEDANCIA	Wifi: 2072 € Repetidor: 2100 € Antena Alta Impedancia: 896 € Total: 5068 €	-

[13] Se han considerado 28 células TALOS que son las que tiene un GACA con todos sus medios desplegados.

[14] Se puede observar que el coste de esta solución es notablemente superior a las demás, para reducir este coste sería necesario implementar un servicio de internet y una VPN propios del ejército.

5 LINEAS DE TRABAJO FUTURAS

Las soluciones anteriormente estudiadas existen hoy en día y pueden ser útiles para el concepto de "Fuegos en red", de la Brigada 2035. Si ponemos la vista en un futuro más lejano, surgen nuevas soluciones posibles que aún están por desarrollar y perfeccionar pero que marcan el camino a seguir. A continuación, se van a exponer algunas de esas posibles soluciones.

Una solución al enlace que cumpliría el criterio de "Fuegos en red", sería el Link 22, el cual está en fase de desarrollo. Para entender cómo funciona debemos referirnos a sus antecesores, Link 11B y Link 16.

Link 11B desarrollado por EE.UU., con un uso principalmente naval y para el combate antiaéreo, surge para proporcionar interoperabilidad entre plataformas y que sirva de enlace de datos de vigilancia, gestión del campo de batalla y control de armamento. Actualmente se utiliza en todas las plataformas de combate antiaéreo (terrestres, aéreas y navales). En cuanto a sus características destacar que puede operar en HF y UHF, necesita de visión directa entre sus células, el enlace es bidireccional y permite poder integrarse con el sistema de mando y control de la defensa aérea.

Link 16 es un enlace de datos táctico, en tiempo real, cifrado, que opera en UHF, necesita de línea de visión directa entre sus células y cuenta con múltiples aptitudes para construir redes. Está diseñado para intercambio de datos tácticos en tiempo real, entre plataformas militares existentes en un determinado escenario, proporcionando información precisa para la asignación de trazas, el control de fuegos y la mejora en el conocimiento de la situación. Es imprescindible para los sistemas de AAA con capacidad antimisil.

Link 22 será un híbrido entre los dos casos expuestos anteriormente, mejorando la transmisión de datos mediante HF y UFH, y conseguirá un enlace vía satélite y a larga distancia, por lo cual, no se necesita de visión directa entre sus células. Este sistema está pensado para la defensa aérea pero debido al concepto de "Fuegos en Red" y a sus altísimas capacidades de enlace sería una buena solución para tener todos los fuegos interconectados y disponer de una visión del espacio de batalla en tiempo real, para mejorar la gestión de los recursos y la conducción de la batalla.

Otra solución al enlace que también cumpliría el requerimiento de "Fuegos en Red", sería el uso de microsatélites[15] que de manera autónoma reencaminaran el tráfico de datos por redes múltiples en caso de ambientes saturados. Estos satélites podrían de tener la capacidad de crear redes de comunicaciones en zonas concretas. Estos satélites contarán con fuertes EPM (Medidas de Protección Electromagnéticas) que los hará poco vulnerables a las ECM (Contramedidas Electrónicas) de los sistemas enemigos.

[15] Son satélites de pequeño tamaño que pueden ofrecer múltiples oportunidades a la hora de mejorar el concepto del enlace. Información obtenida del Trabajo Fin de Grado del CAC. Francisco Cantizano Reina de Artillería.

6 CONCLUSIONES

Hoy en día, la tecnología está en constante evolución y con ello cada vez son mejores los sistemas de armas que se desarrollan, siendo más rápidos y potentes, lo que conlleva a tener una visión en tiempo real del campo de batalla. Mediante medios que permitan transmitir gran cantidad de datos instantáneamente se garantizaría poder tener el control de todos los movimientos que surgen en operaciones y dar una respuesta casi instantánea a cualquier amenaza. Por este motivo, se ha realizado este estudio en el que se exponen medios de enlace y transmisión con gran capacidad de transmisión de datos, alcance y seguridad.

Para abordar el análisis de las distintas soluciones al enlace, en primer lugar, se ha pretendido mediante una serie de encuestas y entrevistas no formalizadas, obtener información sobre los sistemas utilizados en la actualidad y de sus debilidades, para así sacar un perfil de las soluciones a estudiar y desarrollar en este trabajo. Como se puede observar, lo que más preocupa al personal encuestado y entrevistado, que son usuarios y conocen bien los sistemas que se usan hoy en día, es la capacidad de trasmisión de datos, en concreto el ancho de banda y la velocidad de transmisión, la seguridad de esos sistemas ante posibles ataques electrónicos y el coste de dichas soluciones, puesto que es un factor que hay que tener en cuenta.

Como herramienta fundamental a la hora de estudiar cada solución se consideró la elaboración de análisis DAFO de cada una de las soluciones al enlace de datos. Como se ha mencionado antes, el factor económico es de especial relevancia, por ello se consideró realizar hacer un análisis económico de los distintos sistemas llevándose a cabo un minucioso estudio del mercado.

En cuanto a estimar un resultado de qué solución es óptima, no se puede establecer la hegemonía de una solución respecto a otras, puesto que cada una tiene sus características propias, pero todas ellas podrían desarrollarse de forma más específica para dar solución al concepto de la Brigada 2035, “Fuegos en Red”. La mejor solución sería una mezcla entre varias de ellas para así asegurarse el enlace en caso de que alguna se viera afectada por alguna circunstancia. Según mi opinión, una solución viable sería tener un enlace por VPN ya que te ofrece una cobertura global y en caso de que no se dispusiera de esa cobertura, obtener el enlace mediante un sistema LoRa / LoRaWAN ya que ofrece un gran alcance.

Para concluir, hay que decir que ejecutar un TFG requiere de una sólida formación que se nos ha proporcionado gracias al grado de Ingeniería de Organización Industrial, realizando análisis con herramientas que hemos ido consolidando demás de la precisión y eficacia a la hora de determinar qué información puede ser valiosa para tomar decisiones.

7 Referencias

Arci, 2019. *Arci.* [En línea]
Available at: https://www.arci.com.mx/transmision-inalambrica/airmax/
[Último acceso: 13 Abril 2022].

Army Guide, 2012. *Army Guide.* [En línea]
Available at: http://www.army-guide.com/eng/product1941.html
[Último acceso: 3 11 2021].

As.com, 2022. *As.* [En línea]
Available at: https://as.com/diarioas/2022/03/15/actualidad/1647337948_251517.html
[Último acceso: 22 Marzo 2022].

Barbosa, D. C., 2020. *Weliveseurity.* [En línea]
Available at: https://www.welivesecurity.com/la-es/2020/05/19/para-que-sirve-vpn/
[Último acceso: 13 Noviembre 2021].

Calvo, D., 2019. *nextpit.* [En línea]
Available at: https://www.nextpit.es/vpn-como-se-configura
[Último acceso: 12 Noviembre 2021].

Cisco, 2018. *¿Qué hace un router?.* [En línea]
Available at: http://www.upv.es/antenas/Tema_1/impedancia.htm
[Último acceso: 14 Abril 2022].

Córdoba, D. d., 2017. *WPA2: ¿Cómo funciona este algoritmo? Seguridad Wi-Fi.* [En línea]
Available at: https://juncotic.com/wpa2-como-funciona-algoritmo-wifi/
[Último acceso: 14 Abril 2022].

Dataustral, 2021. *Dataustral.* [En línea]
Available at: https://dataustral.com/2021/03/19/beneficios-de-una-vpn/
[Último acceso: 13 Noviembre 2021].

DeanTenas, 2020. *DeanTenas.* [En línea]
Available at: https://www.deantenas.com/antenas-wifi/para-que-sirven-las-antenas-de-ubiquiti/
[Último acceso: 13 Abril 2022].

Ejército de Tierra, 2019. Tendencias tecnológicas aplicables a los fuegos. *Fuerza 2035,* pp. 38 - 40.

Fernández, Y., 2021. *Repetidor WiFi, qué es y cómo funciona.* [En línea]
Available at: https://www.xataka.com/basics/repetidor-wifi-que-como-funciona
[Último acceso: 14 Abril 2022].

GMV, 2020. *Manual de Usuario TALOS Táctico.* Madrid: GMV.

GMV, 2020. *Manual de Usuario TALOS Táctico Administración.* Madrid: GMV.

GMV, 2020. *Manual de Usuario TALOS Técnico PC.* Madrid: GMV.

Ionos, 2020. *Ionos.* [En línea]
Available at: https://www.ionos.es/digitalguide/servidores/seguridad/dns-spoofing/
[Último acceso: 12 Noviembre 2021].

Jiménez, J., 2021. *Redeszone.* [En línea]
Available at: https://www.redeszone.net/tutoriales/seguridad/diferencias-cifrado-aes-128-aes-256/
[Último acceso: 3 Abril 2022].

LoRaWAN, 2020. *LoRaWAN.* [En línea]
Available at: https://lorawan.es/
[Último acceso: 13 Noviembre 2021].

Mando de Adiestramiento y doctrina , 2021. *PD4-323 TÁCTICA. EMPLEO DEL GACA.* Granada: Misterio de Defensa.

Mando de Apoyo y Doctrina, 2018. *MI-500 Radioteléfono PR-4G.* Granada: Ministerio de Defensa.

Navas, M. Á., 2018. *profesionalreview.* [En línea]
Available at: https://www.profesionalreview.com/2018/04/01/que-es-la-ley-de-moore-y-para-que-sirve/
[Último acceso: 3 Abril 2022].

Páez, G., 2019. *Territorio Escrito.* [En línea]
Available at: https://territorioescrito.com/2019/06/01/en-que-consiste-el-enfoque-constructivista-de-la-educacion/#:~:text=Gerald%20Edelman%2C%20Premio%20Nobel%20de,modo%20un%20acto%20de%20imaginaci%C3%B3n%C2%BB.
[Último acceso: 10 Abril 2022].

Reimondo, G., 2019. *Humanizationofthechnology.* [En línea]
Available at: https://humanizationoftechnology.com/seguridad-en-redes-lorawan/revista/iot/01/2019/
[Último acceso: 13 Abril 2022].

Sáez, J. H., 2021. *Interempresas.* [En línea]
Available at: https://www.interempresas.net/TIC/Articulos/347552-El-despegue-de-la-tecnologia-LORAWAN-para-una-conectividad-global-y-cibersegura.html
[Último acceso: 3 Abril 2022].

Semtech, 2020. *semtech.* [En línea]
Available at: https://www.semtech.com/
[Último acceso: 3 Abril 2022].

Spw, 2019. *Spw.* [En línea]
Available at: https://www.spw.es/ubiquiti1.html
[Último acceso: 13 Abril 2022].

THALES , 2019. *THALES.* [En línea]
Available at: https://www.thalesgroup.com/es/pr4g-fstnet#:~:text=La%20PR4G%20permite%20la%20transmisi%C3%B3n,con%20comunicaciones%20de%20voz%20simult%C3%A1neas
[Último acceso: 5 Marzo 2022].

UPV, 2016. *Impedancia.* [En línea]
Available at: http://www.upv.es/antenas/Tema_1/impedancia.htm
[Último acceso: 14 Abril 2022].

Veracode, 2020. *Veracode.* [En línea]
Available at: https://www.veracode.com/security/arp-spoofing#:~:text=ARP%20spoofing%20is%20a%20type,or%20server%20on%20the%20network.)
[Último acceso: 12 Noviembre 2021].

vpn, 2020. *vpn.* [En línea]
Available at: https://www.vpn.net/
[Último acceso: 13 Noviembre 2021].

Webedia Brand Services, 2016. *¿Cuál será el estándar Wi-Fi del futuro? MIMO viene con ganas.* [En línea]
Available at: https://www.xataka.com/tecnologiazen/cual-sera-el-estandar-wi-fi-del-futuro-mimo-viene-con-ganas
[Último acceso: 14 Abril 2022].

8 ANEXOS

8.1 Anexo I: Encuestas

8.1.1 Encuesta inicial

Responda a este formulario indicando la respuesta que usted crea. Siendo 1 poco grado de satisfacción y 5 el máximo grado de satisfacción.

¿Cree usted que el sistema TALOS es útil para Artillería de Campaña?

1 2 3 4 5

¿Cree usted que el sistema TALOS TÉCNICO es útil para Artillería de Campaña?

1 2 3 4 5

¿Cree usted que el sistema TALOS TÁCTICO es útil para Artillería de Campaña?

1 2 3 4 5

¿Cree usted que se utiliza el sistema TALOS explotando todo su potencial?

1 2 3 4 5

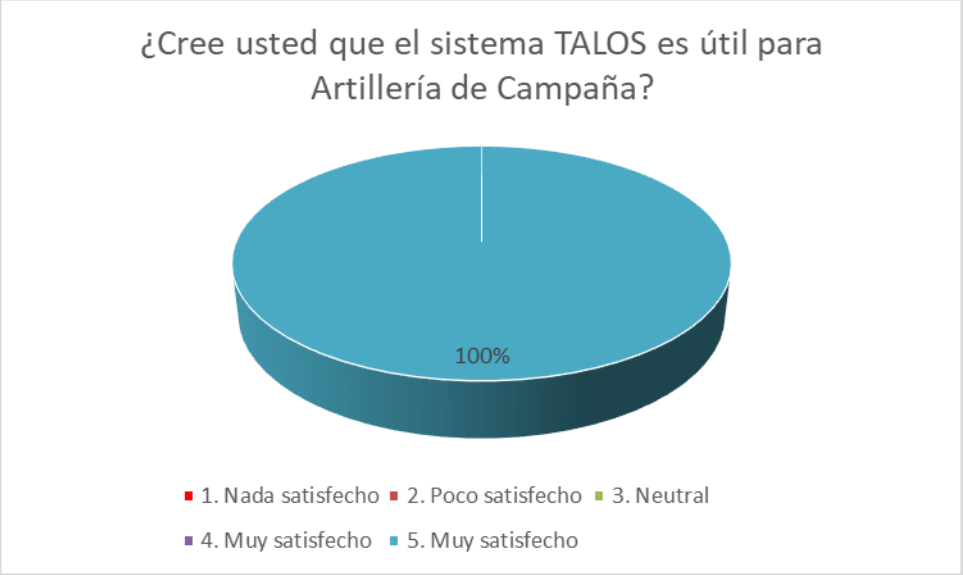
¿Cree usted que usar las configuraciones IP LAN con el TALOS supondría un avance en la transmisión de datos?

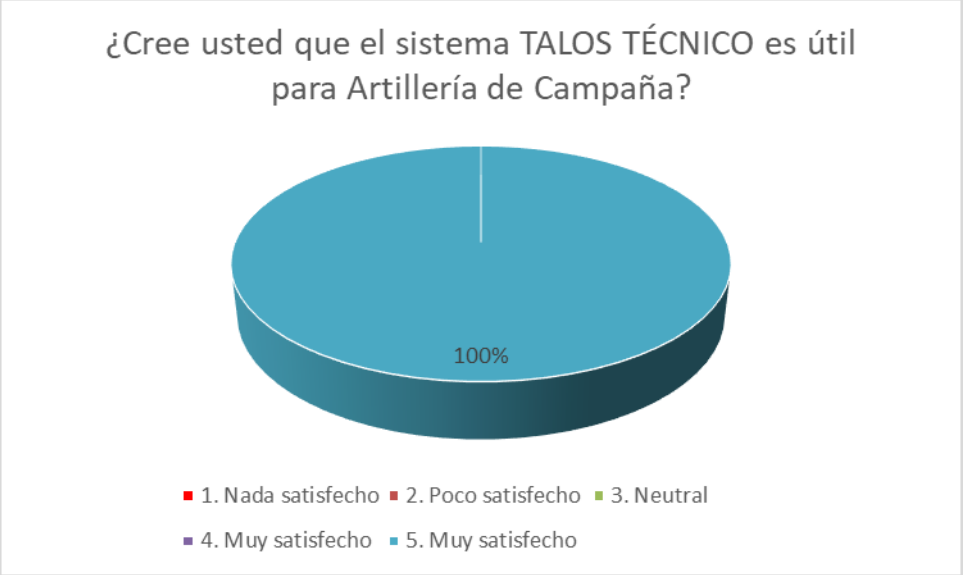
1 2 3 4 5

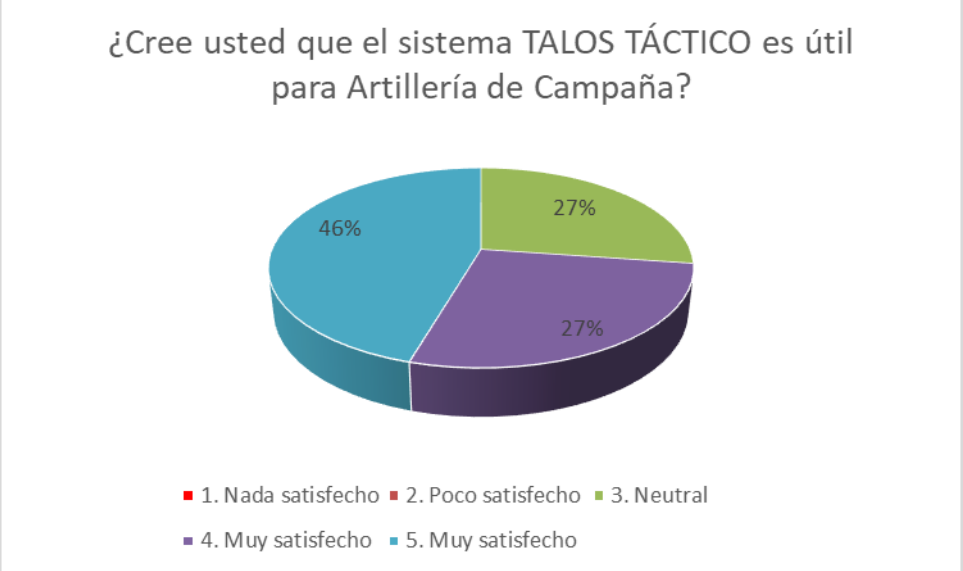
¿Cuál cree usted que es el problema principal por el cual el sistema TALOS suele fallar? (Puede marcar una o varias).

- Software
- Medios disponibles / Hardware actual
- Interoperabilidad de los subsistemas
- Desconocimiento de todas las capacidades del programa
- Falta de instrucción de los Operadores
- El subsistema TALOS del que dispongo según mi puesto táctico no es el adecuado

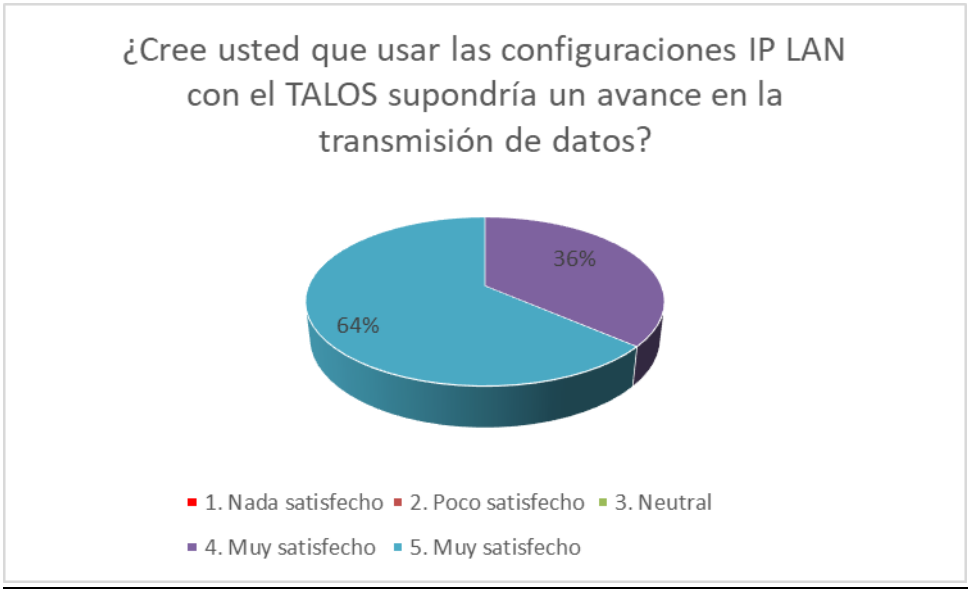
Resultados:

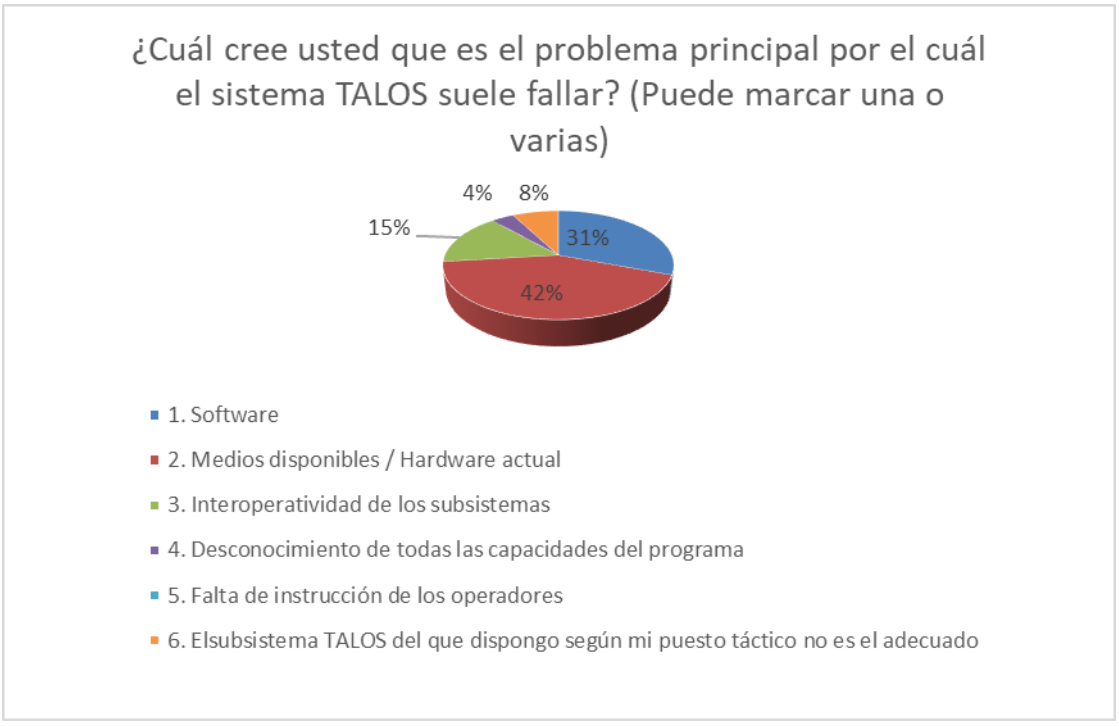

¿Cree usted que el sistema TALOS es útil para Artillería de Campaña?
100%
1. Nada satisfecho
2. Poco satisfecho
3. Neutral
4. Muy satisfecho
5. Muy satisfecho


¿Cree usted que el sistema TALOS TÉCNICO es útil para Artillería de Campaña?
100%
1. Nada satisfecho
2. Poco satisfecho
3. Neutral
4. Muy satisfecho
5. Muy satisfecho


¿Cree usted que el sistema TALOS TÁCTICO es útil para Artillería de Campaña?
46%
27%
27%
1. Nada satisfecho
2. Poco satisfecho
3. Neutral
4. Muy satisfecho
5. Muy satisfecho


¿Cree usted que se utiliza el sistema TALOS explotando todo su potencial?
9%
91%
1. Nada satisfecho
2. Poco satisfecho
3. Neutral
4. Muy satisfecho
5. Muy satisfecho


¿Cree usted que usar las configuraciones IP LAN con el TALOS supondría un avance en la transmisión de datos?
36%
64%
1. Nada satisfecho
2. Poco satisfecho
3. Neutral
4. Muy satisfecho
5. Muy satisfecho


¿Cuál cree usted que es el problema principal por el cuál el sistema TALOS suele fallar? (Puede marcar una o varias)
4%
8%
15%
31%
42%
1. Software
2. Medios disponibles / Hardware actual
3. Interoperatividad de los subsistemas
4. Desconocimiento de todas las capacidades del programa
5. Falta de instrucción de los operadores
6. Elsubsistema TALOS del que dispongo según mi puesto táctico no es el adecuado

8.1.2 Segunda encuesta

Responda a este formulario indicando la respuesta que usted crea. Siendo 1 muy poco importante y 5 muy importante.

¿Cómo de importante es para usted la seguridad?

1 2 3 4 5

¿Cómo de importante es para usted la velocidad de transmisión de datos?

1 2 3 4 5

¿Cómo de importante es para usted el ancho de banda?

1 2 3 4 5

¿Cómo de importante es para usted el alcance de dicho medio?

1 2 3 4 5

¿Cómo de importante es para usted el coste del sistema?

1 2 3 4 5

¿Cómo de importante es para usted la facilidad de su uso por parte de los operadores?

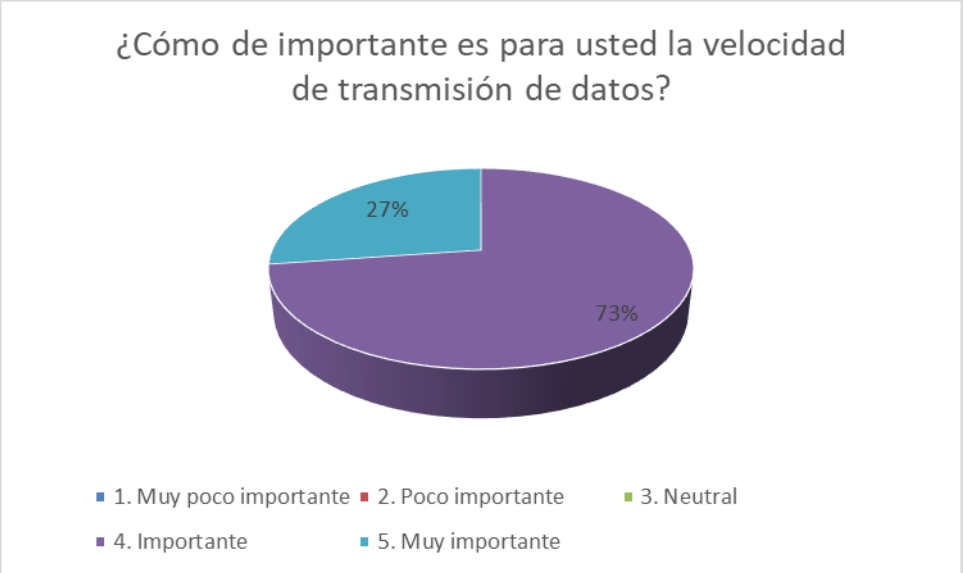
1 2 3 4 5

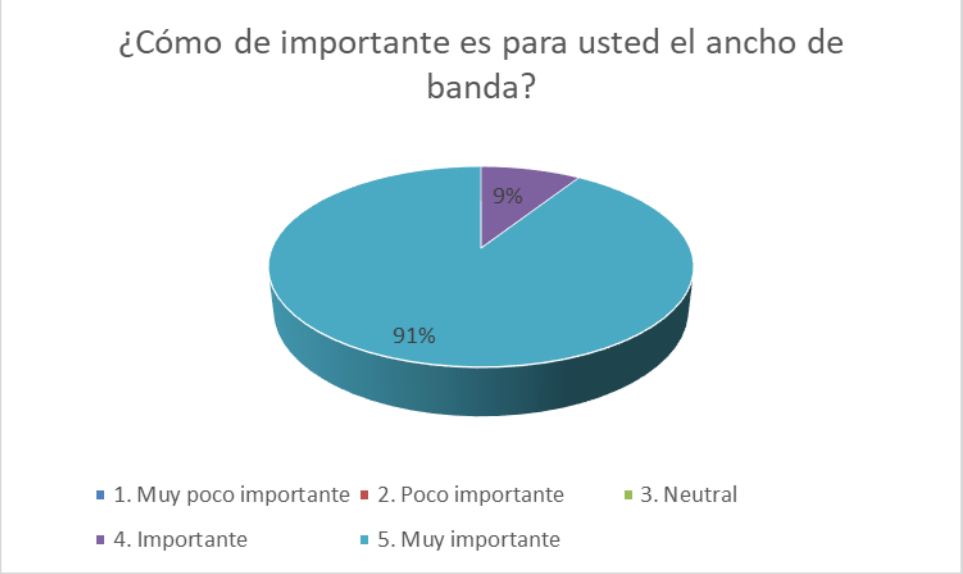
¿Cómo de importante es para usted la facilidad de instalación?

1 2 3 4 5

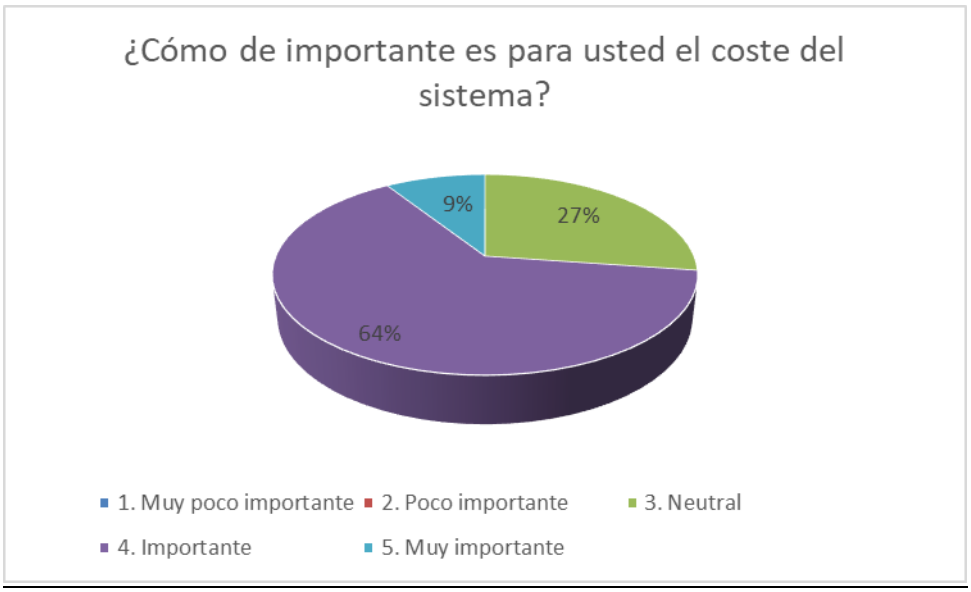
Resultados:


¿Cómo de importante es para usted la seguridad?
100%
1. Muy poco importante
2. Poco importante
3. Neutral
4. Importante
5. Muy importante

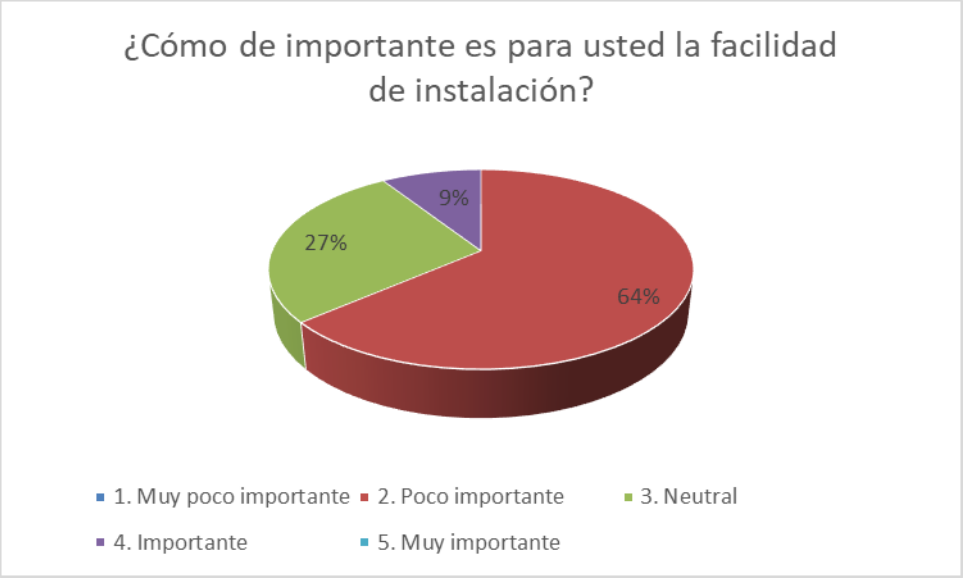

¿Cómo de importante es para usted la velocidad de transmisión de datos?
27%
73%
1. Muy poco importante
2. Poco importante
3. Neutral
4. Importante
5. Muy importante


¿Cómo de importante es para usted el ancho de banda?
9%
91%
1. Muy poco importante
2. Poco importante
3. Neutral
4. Importante
5. Muy importante


¿Cómo de importante es para usted el alcance de dicho medio?
27%
27%
46%
1. Muy poco importante
2. Poco importante
3. Neutral
4. Importante
5. Muy importante


¿Cómo de importante es para usted el coste del sistema?
9%
27%
64%
1. Muy poco importante
2. Poco importante
3. Neutral
4. Importante
5. Muy importante


¿Cómo de importante es para usted la facilidad de su uso por parte de los operadores?
9%
18%
73%
1. Muy poco importante
2. Poco importante
3. Neutral
4. Importante
5. Muy importante

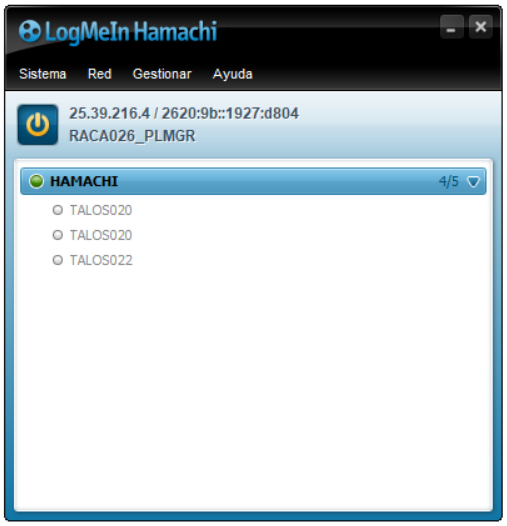

¿Cómo de importante es para usted la facilidad de instalación?
9%
27%
64%
1. Muy poco importante
2. Poco importante
3. Neutral
4. Importante
5. Muy importante

8.2 Anexo II: Configuración Hamachi

INSTRUCCIONES

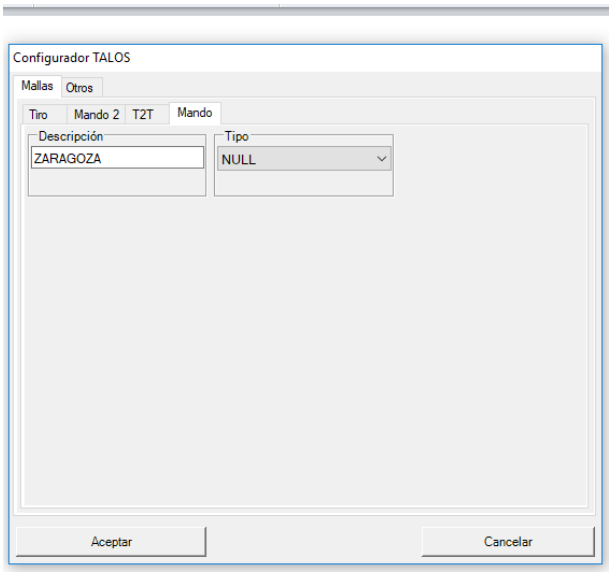
1º Conectar el equipo a internet.

2º Una vez establecida la conexión con HAMACHI, verá los equipos que están conectados en la red.



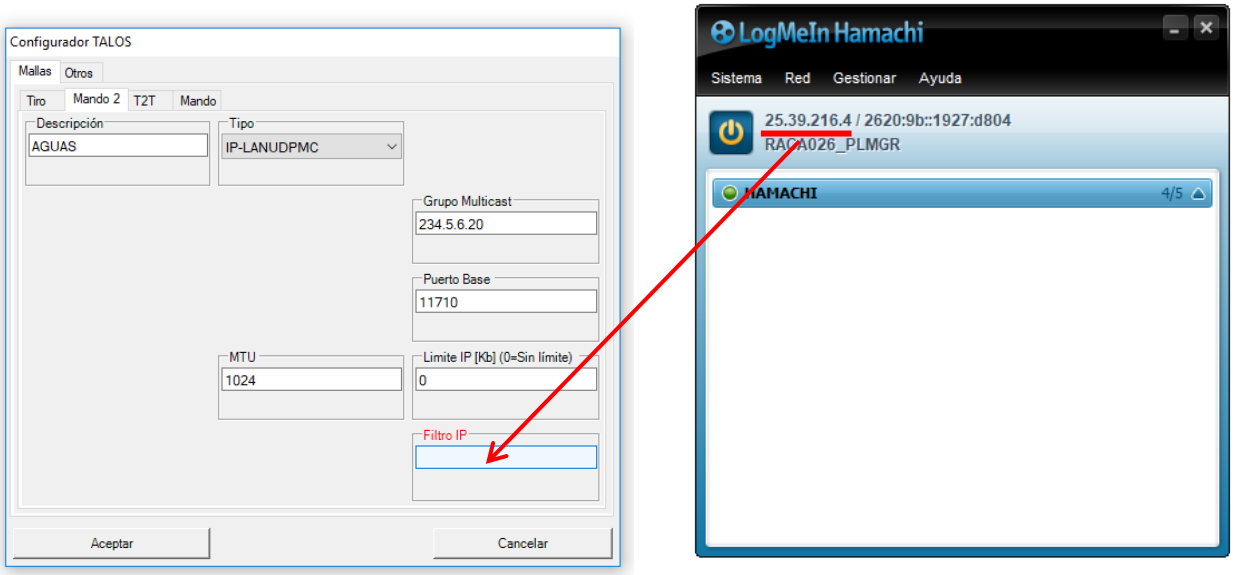
3º Configuración de las comunicaciones de TALOS:

MALLA DE MANDO 1



CONFIGURAR COMO RED LOCAL

MALLA DE MANDO 2



Filtro IP: " la IP que le asigne HAMACHI a ese equipo"

AÑADIR UN EQUIPO NUEVO A LA RED HAMACHI

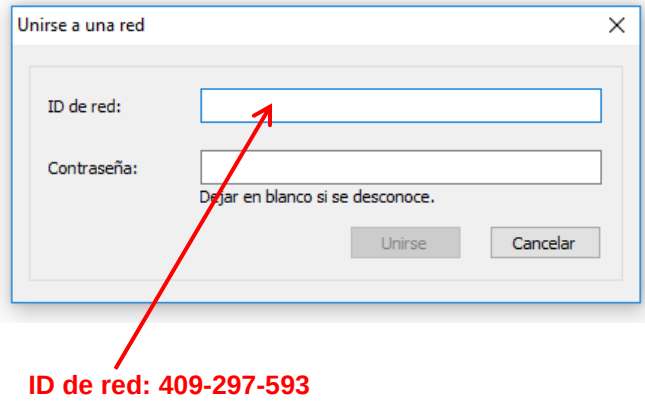
En caso de que fuese necesario añadir un nuevo pc a la RED HAMACHI ya creada deberán seguirse los siguientes pasos:

1º Copiar el siguiente enlace en el navegador:

ENLACE DESCARGA HAMACHI

https://secure.logmein.com/hamachi/ih1.asp?lang=es&c=bh3bijbc9yakguvdkujglwnlfdytk7q8mboaj83v

2º Descargar e instalar la aplicación de HAMACHI.



ID de red: 409-297-593

8.3 Anexo III: Medios Hardware

LORA:https://www.amazon.es/Ebyte-E90-DTU-433L30E-Ethernet-Wireless-Transceptor/dp/B09BFCHVMF?th=1(Consultado el 15/04/2022)

UBIQUITI:

Unidireccional:https://www.wifisafe.com/bridge-litebeam-5ac-gen2-de-23dbi.html (Consultado el 15/04/2022)

Omnidireccional:https://shopdelta.eu/antena-omnidireccional-amo-5g13-ubiquiti-5-45-ghz-5-85-ghz-13-dbi_l6_p8763.html (Consultado el 15/04/2022)

WIFI:https://www.pccomponentes.com/tp-link-eap225-punto-de-acceso-gigabit-mu-mimo-inalambrico-ac1350?gclid=Cj0KCQjwjN-SBhCkARIsACsrBz5TieF3_jv2TOar35qsJw2QvFQQSET05JbJRRrCoA1xl0Fk_3IrwmwaAswnEALw_wcB (Consultado el 15/04/2022)

RECEPTOR:https://www.amazon.es/dp/B088R4MP65?tag=wifilink-21&linkCode=osi&th=1&psc=1&keywords=Repetidor%20Wifi%20Exterior%20Largo%20Alcance (Consultado el 15/04/2022)

ANTENA ALTA IMPEDANCIA: https://es.rs-online.com/web/p/antenas-rfid/2059979 (Consultado el 15/04/2022)