



## **E1.1 Informe de requisitos de seguridad y diseño de equipos de sensorización**

### Contenido

1	Resumen .....	2
2	Normativas/Legislación/Estándares .....	2
3	Requisitos de seguridad .....	4
3.1	Seguridad de los dispositivos sensores .....	4
3.2	Seguridad de las comunicaciones.....	4
3.3	Seguridad en la plataforma .....	5
4	Sistemas de comunicaciones .....	6
4.1	Comunicaciones IoT de largo alcance.....	9
4.1.1	Sigfox .....	9
4.1.2	LoRa .....	12
4.1.3	NB-IoT/LTE-M sobre 5G.....	16
4.2	Comunicaciones intervehiculares.....	17
4.2.1	802.11p.....	17
4.3	Análisis comparativo de las tecnologías de comunicaciones .....	18
4.4	Conclusiones.....	19
5	Dispositivos .....	20
5.1	Dispositivos sensores en almacenes.....	25
5.2	Dispositivos sensores en vehículos.....	26
6	Conclusiones .....	27
7	Referencias sobre Normativas/Legislación/Estándares.....	28



## 1 Resumen

Este documento analiza las normativas existentes en el ámbito de aplicabilidad del proyecto GUARDIAN, más concretamente en el transporte dentro del contexto agrícola (alimentos perecederos) y en el reparto de medicamentos para uso humano.

También recoge el conjunto de requisitos de seguridad que han sido identificados dentro del proyecto, tanto a nivel de los dispositivos sensores que se incorporarán en los vehículos de transporte, como a la hora de realizar el tratamiento de la información una vez enviada a la plataforma de almacenamiento, gestión y análisis de datos.

Finalmente se describirán las características de los dispositivos de nueva generación que serán instalados en los almacenes y en los vehículos, así como las tecnologías de comunicaciones que se pueden y/o se van a emplear.

## 2 Normativas/Legislación/Estándares

El proyecto se desarrolla en torno al Sector Logístico Refrigerado de alimentos y medicamentos, donde existe un alto grado de regulación tanto a nivel nacional como internacional.

En el caso concreto del transporte de alimentos perecederos, la normativa se centra en la definición de las características que deben cumplir los vehículos utilizados para el transporte de mercancías, donde el principal factor que se tiene en cuenta para garantizar el correcto mantenimiento de los productos durante todo el trayecto es la temperatura.

El punto de partida de la regulación de dichas características es el Acuerdo ATP (en referencia al *Acuerdo sobre transportes internacionales de mercancías perecederas y sobre vehículos especiales utilizados en esos transportes*) establecido en 1970 por Naciones Unidas, habiéndose consolidado la última versión del mismo en España en el BOE del 15 de Noviembre de 2013 [1].

En dicho acuerdo se definen principalmente los tipos de unidad en función de las necesidades frigoríficas/caloríficas, niveles de aislamiento, tolerancia a cambios de temperatura, autonomía ante una pérdida de alimentación, pruebas para comprobar que cada unidad cumple los criterios exigibles para el tipo de unidad que tiene asignado, etc. En concreto se definen los conceptos de unidades isotermas, refrigerantes, frigoríficas y caloríficas.

El registro de la temperatura se debe realizar de forma periódica, haciendo uso de un termógrafo homologado conforme a las normas UNE-EN 12830 [2], UNE-EN 13485 [3] y UNE-EN 13486 [4]. Tal y como se comenta en el artículo 5 punto 6 del Real Decreto 237/2000 del 18 de Febrero [5], aquellos vehículos que estén equipados con un termógrafo tendrán que ser verificados periódicamente en base a la orden ITC/3701/2006 [6].

En el ámbito de la distribución de medicamentos, la regulación gira en torno a las directrices impuestas por la normativa europea GDP (del inglés *Good Distribution Practice*, o *Buenas Prácticas de Distribución*) del 5 de Noviembre de 2013 (2013/C 343/01) [7], que extienden la Directiva 2001/83/CE [8].



THD GUARDIAN - TSI-100110-2019-20

Al no estar orientadas al objetivo final del proyecto, aun teniendo una relación directa, se dejarán fuera de este análisis otras normas/leyes/estándares que cubren los siguientes puntos:

- ▶ Directiva 2011/62/UE del Parlamento Europeo [9], que recoge las medidas de refuerzo que se exigen para intentar prevenir de entrada de medicamentos falsificados en la cadena de suministro legal. En esa área concreta modifica también lo definido en la Directiva 2001/83/CE.
- ▶ Directiva 2012/26/UE del Parlamento Europeo [10], relacionada con la *Farmacovigilancia*.
- ▶ IFS Food [11], que cubre, entre otras cosas, la fase de empaquetado de alimentos previa a la fase de transporte.

A nivel legal, en España sigue estando vigente lo publicado en el Real Decreto 782/2013 del 11 de Octubre [12], donde se indica explícitamente que las GDP que se usan como marco de referencia se irán actualizando periódicamente a nivel europeo, siendo la versión del 5 de Noviembre de 2013 mencionada anteriormente la más reciente.

Como tal, las GDP se basan en realizar una gestión de la calidad a nivel integral que abarque a todos los agentes implicados, desde la sede del fabricante hasta (no inclusive) los puntos de venta de medicamentos (principalmente farmacias), pasando por mayoristas, almacenes, brokers, etc. El objetivo es garantizar que se preserve la calidad de los medicamentos durante toda la cadena de suministro.

Asimismo se deberá extender a las empresas subcontratadas cuando alguna intervenga en cualquier fase del proceso, ya sea durante el almacenamiento, transporte, etc. de los medicamentos.

En términos generales se debe garantizar la correcta trazabilidad, de tal forma que se tomen registros de las distintas actividades en el momento en el que éstas se lleven a cabo, permitiendo detectar, registrar y notificar desviaciones en caso de producirse.

Las GDP además cubren otros dos puntos clave del proceso en cuanto a su relación con este proyecto, que son el almacenamiento y el transporte de los medicamentos.

En relación con los puntos de almacenamiento (denominados *locales*), y al margen de cuestiones más generales, se indica la necesidad de seguir procedimientos adecuados para controlar factores del entorno tales como temperatura, humedad, nivel de luz y limpieza, y concretamente se debe disponer como mínimo de un sistema de control y registro de temperatura.

Para el transporte, el distribuidor (mayoristas, etc.) será el responsable de garantizar y demostrar que los medicamentos se han mantenido dentro de los límites aceptables y las desviaciones de la temperatura, en caso de producirse, deberán notificarse tanto al distribuidor como al cliente. Además los dispositivos que se utilicen para controlar la temperatura deberán ser calibrados al menos una vez cada año.

Otro de los aspectos ligados a la eficiencia energética es la huella de carbono, que permite medir la cantidad de CO<sub>2</sub> emitida dentro de todo el proceso, incluyendo tanto el almacenamiento como la distribución de los productos.

En ese contexto es aplicable la siguiente normativa:

- ▶ Fomento del uso de biocarburantes conforme a lo especificado en el Real Decreto 1085/2015 del 4 de Diciembre [13].
- ▶ Especificaciones técnicas de las gasolineras, gasóleos, fuelóleos y gases licuados del petróleo en base a lo definido en el Real Decreto 61/2006 del 31 de Enero [14].



THD GUARDIAN - TSI-100110-2019-20

- ▶ Cambios en ciertos aspectos de las especificaciones técnicas del Real Decreto 61/2006 en lo referente al gasóleo de clase B conforme a lo indicado en el Real Decreto 1088/2010 del 31 de Enero [15]. En concreto se habla de combustibles para uso marítimo, pero en el fondo se trata del mismo combustible que se suele utilizar en los motores que alimentan los dispositivos de climatización de los remolques.
- ▶ Nuevos cambios en ciertos aspectos de las especificaciones técnicas del Real Decreto 61/2006 en lo referente al gasóleo de clase B conforme a lo indicado en el Real Decreto 1361/2011 del 7 de Octubre [16].
- ▶ Métodos de cálculo de la intensidad de emisiones de gases de efecto invernadero de los combustibles y la energía en el transporte conforme al Real Decreto 235/2018 del 27 de Abril [17] que a su vez modifica el Real Decreto 1597/2011 del 4 de Noviembre [18].

A nivel de estándares existe a nivel internacional el IFS Logistics [19], que regula todo el proceso logístico ya sea en almacenamiento o en transporte, y que pretende garantizar la correcta trazabilidad de los productos así como la auditoría externa de todos los procesos involucrados para garantizar el correcto mantenimiento de los mismos durante toda la cadena de suministro.

### **3 Requisitos de seguridad**

La seguridad dentro del proyecto debe ser aplicada a todos los niveles, empezando por los dispositivos de toma de datos (tanto en almacenes como en vehículos), siguiendo por la fase de envío de dichos datos a la plataforma y en última instancia también dentro de la propia plataforma.

#### **3.1 Seguridad de los dispositivos sensores**

El primer nivel de seguridad está en los propios dispositivos sensores, tanto en la propia toma de datos como a la hora de garantizar la validez de los mismos.

Asociado a los requisitos de trazabilidad impuestos por las GDP, se debe garantizar que los dispositivos sensores no sean manipulados. Por consiguiente se deben añadir medidas anti-tamper que permitan detectar intentos de acceso no autorizados.

Otro de los requisitos de trazabilidad es garantizar que los valores de los sensores sean válidos, lo que supondrá añadir mecanismos de detección de desviaciones de los valores mediante la instalación de sensores complementarios con los que detectarlas y, dentro del sistema de calidad, se deberá definir un protocolo de revisión y calibración periódica de los mismos.

Para garantizar que la trazabilidad sea consistente a nivel temporal, los dispositivos deberán poder detectar cambios de hora anormales derivados de posibles fallos en los relojes internos o como resultado de no tener accesible un servidor de hora.

#### **3.2 Seguridad de las comunicaciones**

La seguridad de las comunicaciones debe involucrar a ambos extremos, es decir, tanto a los dispositivos instalados en almacenes y en vehículos como a la propia plataforma que recibe los datos.

A nivel de dispositivos hay que diferenciar entre los instalados en almacenes, donde hay menos restricciones de autonomía a nivel eléctrico y donde se pueden instalar dispositivos más potentes teniendo en cuenta que hay alimentación continua, y los instalados en vehículos, en los que se intentará reducir el consumo en la medida de lo posible siempre que la propia infraestructura de comunicaciones lo permita de forma que sea ésta la que gestione la parte de seguridad.



THD GUARDIAN - TSI-100110-2019-20

Por lo tanto en el primer caso se hará uso de certificados digitales con los que establecer conexiones seguras SSL/TLS, mientras que en el segundo la parte de cifrado se intentará delegar en la seguridad de la capa de comunicaciones. De no ser posible, habrá que añadir soporte también para certificados digitales en los dispositivos instalados.

### **3.3 Seguridad en la plataforma**

Una vez recibidos los datos, y siguiendo con los principios impuestos por el sistema de calidad para garantizar que se cumplen las GDP y que se puede realizar una trazabilidad adecuada de los mismos, hay diversos aspectos que deben ser cubiertos.

Se pretende aplicar la tecnología blockchain (*cadena de bloques*). Por su propia naturaleza, dado que hace uso de redes distribuidas, está orientada a poder garantizar la integridad y disponibilidad de los datos, así como controlar que los accesos a ellos solo sean posibles para personas que estén autorizadas.

Como tal una cadena de bloques es un libro de registros en el que se anotan entradas validadas por un conjunto de nodos de la red distribuida (cada entrada es un conjunto de datos que se trata a modo de transacción), y que se divide en bloques de forma que cada entrada está firmada y a su vez cada bloque hace uso de datos contenidos en el resumen digital que se calcula del bloque anterior para mantener la cadena enlazada. De esa forma cualquier modificación en un bloque le afectará a los sucesivos y podrá ser detectada rápidamente.

En un despliegue real, la idea es que todos los agentes involucrados (mayoristas, almacenes, la propia plataforma, clientes, auditores externos, opcionalmente otros proveedores externos de servicios blockchain, etc.) formen parte de la red distribuida sobre la que se crea la cadena, de forma que no solo todos ellos tengan acceso a los datos (accesibilidad) y estos estén replicados (redundancia), sino que se establezca una relación de confianza a la hora de poder validar los registros que se han ido recogiendo y que serán utilizados dentro de los procesos definidos por el sistema de calidad.

Dentro de esos procesos, entre otros, se incluirá al menos el de detección de desviaciones de la temperatura para la notificación a los destinatarios designados, en caso de que se produzcan (dentro del proyecto no se contemplan otro tipo de actuaciones al margen de la detección, registro y notificación de las desviaciones).

Se deberán definir los mecanismos de gestión de identidades y control de acceso a los datos tanto para aquellos nodos que pueden insertar datos en la cadena como a los que solo tienen acceso de lectura.

Opcionalmente se puede plantear la posibilidad de hacer uso de múltiples cadenas para separar por un lado los datos obtenidos de los sensores (cadena principal), por otro todos los registros ligados al resto de procesos asociados al sistema de calidad, una tercera cadena que recoja la información obtenida mediante análisis de datos, etc.

En el caso concreto de este proyecto se hará uso en un proveedor de servicios blockchain para la creación y el acceso a la cadena.

Ligados a la gestión de pedidos, y como mecanismo de comprobación automática del mantenimiento de la cadena de frío durante todo el proceso (en general mantenimiento de la temperatura dentro del rango de temperaturas aceptable), se estudiará el uso de los denominados *smart contracts* (*contratos inteligentes*). Cada contrato se iniciará en el momento en el que se reciba



THD GUARDIAN - TSI-100110-2019-20

un pedido, de forma que tendrá una primera fase de comprobación inicial que asegure que los productos (medicamentos, alimentos, etc.) han sido almacenados y transportados hasta el punto de inicio de tramitación del pedido de forma correcta (un almacén, por ejemplo), y posteriormente se encargará de ir haciendo un seguimiento de los mismos en base a los datos provenientes del sistema de trazabilidad, de tal forma que se podrá saber si en algún punto se ha producido una desviación, lo que sería un sinónimo de incumplimiento del contrato. Si no se ha detectado ningún problema, el contrato se dará por finalizado y será aceptado en el momento de la recepción del mismo, y será anotado también como una entrada más dentro de la cadena, de forma que el sistema de calidad pueda hacer un seguimiento del cumplimiento de los contratos, ratio de contratos fallidos, puntos de fallo, etc.

A continuación se muestra una lista con requisitos más específicos que deberán cumplirse a nivel de plataforma.

ID	Descripción
RP-1	El acceso a la plataforma deberá estar debidamente securizado haciendo uso de los mecanismos que sean aplicables en función del tipo de interfaz que se ofrezca (acceso web sobre conexiones seguras, etc.).
RP-2	Se dispondrá de un sistema de autenticación/autorización para gestionar el acceso a la plataforma (gestión de usuarios con login/password, etc.).
RP-3	Se podrá gestionar la información relacionada con la seguridad asociada al acceso a la cadena, incluyendo el control de acceso a la misma, el alta o baja de nodos que forman parte de la red distribuida sobre la que se crea la cadena, etc.
RP-4	Se tendrá un sistema de gestión de dispositivos que forman parte del sistema, tanto a nivel de almacén como a nivel de vehículos.
RP-5	La información de seguridad (certificados, identidades, etc.) de los dispositivos del sistema deberá realizarse de forma segura, solo pudiendo realizarse modificaciones por parte del personal autorizado.

## 4 Sistemas de comunicaciones

### 4.1 Tecnologías de medio alcance para almacenes

#### 4.1.1 Wifi

El Wi-Fi es una red de área local (LAN) que proporciona acceso a Internet dentro de un rango limitado. Es la tecnología más usada para proporcionar redes inalámbricas en edificios públicos y privados, así como a nivel industrial en fábricas, almacenes, etc.

El Wi-Fi es una red en estrella donde hay un centro y todos los nodos o dispositivos se conectan a él. Esta topología en estrella hace que sea fácil agregar o quitar dispositivos sin afectar al resto de la red. El ancho de banda es alto, hasta 2 MHz, por lo que es perfecto para transmitir megas de datos y conectar dispositivos inteligentes como teléfonos o tabletas. Pero la desventaja es que sólo funciona si la señal es fuerte y estás cerca del punto de acceso. Su alcance medio es de 30 a 100 metros.

Otro problema es que no es una red de bajo consumo. Los dispositivos basados en Wi-Fi normalmente duran solo días con batería por lo que o están conectados a la red eléctrica o tienen que ser cargándolos diariamente.



#### 4.1.2 Zigbee

La tecnología ZigBee está diseñada para transportar pequeñas cantidades de datos a media distancia y consumir muy poca energía. A diferencia del Wi-Fi, es un estándar de red en malla, lo que significa que cada nodo de la red está conectado entre sí. No tienes que depender únicamente del enrutador y el punto final.

Esta tecnología también tiene un ancho de banda de canal bajo de 1 MHz por lo que no tiene interferencias con redes Wifi-existentes en la misma área. Está restringida a las redes de área personal inalámbricas (WPAN) y alcanza un promedio de 10 a 30 metros para las aplicaciones habituales. La velocidad de transferencia de datos de ZigBee también es menor que la de Wi-Fi. Su velocidad máxima es de solo 250 kbps, mucho más baja que la velocidad del Wi-Fi.

La mejor cualidad de ZigBee es su bajo consumo de energía. Además, su protocolo fue diseñado como “montar y olvidar”, lo que significa que una vez que lo configuras, puede durar meses.

#### 4.1.3 Z-Wave

**Z-Wave** es un protocolo de comunicaciones inalámbricas usado principalmente para la sensorización, control y automatización en edificios de todo tipo. Tiene una estructura de **red en malla** que utiliza ondas de radio de baja energía para comunicarse de un aparato a otro, permitiendo la monitorización y control inalámbrico para sistemas de seguridad, ahorro energético entre otros.

Su tecnología de red de malla inalámbrica permite que cualquier nodo hable con los nodos adyacentes directa o indirectamente, controlando cualquier nodo adicional. Los nodos que están dentro del rango se comunican directamente entre sí. Si no están dentro del rango, pueden enlazarse con otro nodo que esté dentro del rango de ambos para acceder e intercambiar información.

La interoperabilidad de Z-Wave en la capa de aplicación asegura que los dispositivos puedan compartir información y permite que todo el hardware y el software de Z-Wave trabajen juntos.

Aunque Z-Wave es propietario, el estándar se está abriendo cada vez más y, de hecho, la seguridad para el transporte de señales de Z-Wave sobre redes IP, y el middleware de Z-Wave son de código abierto desde 2016.

Por último, cabe destacar que Z-Wave utiliza diferentes bandas en Estados Unidos y en Europa; y los dispositivos no son compatibles entre sí. Utiliza la banda ISM de 915 MHz (en los EE.UU.) y la banda RFID de 868 MHz (en Europa). Hay que tenerlo en cuenta a la hora de fabricar los equipos de OdinS inicialmente orientados al mercado europeo.

#### 4.1.4 Análisis comparativo para sensorización y control de almacenes refrigerados

El problema es que todos los sensores y equipos Wi-Fi **suelen depender de una plataforma en la nube** para indicar las funciones de control. Eso significa que, si te quedas sin internet, no habrá disponible de algunas funciones de eficiencia energética y control sobre los almacenes refrigerados.

Por contra, podemos monitorizar y controlar los sensores y actuadores **Z-Wave y ZigBee de terceras empresas o fabricados por OdinS usando uno o varios Gateway controladores diseñados por**



THD GUARDIAN - TSI-100110-2019-20

**OdinS**, que permiten administrar todos los dispositivos sin depender de la nube por lo que podremos controlar los almacenes e instalaciones de la logística refrigerada aun cuando Internet esté caído. Y por eso, se diseñarán y desarrollará equipos configurables con capacidad de control local así también el funcionamiento será más rápido y efectivo. Por ejemplo, apagado de equipos consumidores de energía (aire-acondicionado, luces, etc) en la logística refrigerada cuando no sean necesarios según las configuraciones establecidas en los gateways. Por último, la tabla siguiente muestra brevemente las diferencias entre Zwave y Zigbee.

A continuación, se muestran las ventajas y desventajas de cada una de las tecnologías de comunicaciones Zwave y Zigbee:

	<b>Z-Wave</b>	<b>Zigbee</b>
<b>Banda de frecuencia</b>	800-900 MHz	2,4 Ghz
<b>rango</b>	Máximo 100 metros	Alrededor de los 10-20 metros
<b>Velocidad de datos</b>	Hasta 100 kbps	250 kbps
<b>Tipo de red</b>	Red de malla	Red de malla
<b>Número máximo de dispositivos de cada red de malla</b>	232	65.000
<b>Salto máximo entre dispositivos</b>	4	10
<b>seguridad</b>	Mecanismo de seguridad propietario Security 2 (S2)	Cifrado simétrico AES de 128 bits
<b>compañía detrás</b>	Silicon Labs	Estándar abierto (IEEE 802.15.4) – Zigbee Alliance
<b>Productos certificados (año 2020)</b>	Más de 2400	Más de 2.500

### Z-Wave

- Comunicación inalámbrica más fiable.
- La señal recorre una distancia más larga.
- Gran compatibilidad entre gadgets compatibles con el estándar.
- Baja velocidad de transferencia de datos entre dispositivos.
- Menos dispositivos compatibles en la misma red
- La señal viaja en un máximo de 4 saltos entre dispositivos.

### Zigbee

- Admite una tasa de datos más alta entre dispositivos.
- Muy adecuado para áreas grandes con muchos dispositivos (máximo 65.000 dispositivos).
- Estándar de código abierto.
- Menos fiable en el camino inalámbrico en comparación con Zwave.
- Funciona a 2,4 Ghz, que es un entorno de frecuencia similar a Wifi (más interferencias y menor alcance).

## 4.2 Comunicaciones IoT de largo alcance para vehículos

### 4.2.1 Sigfox

Es una red de largo alcance y bajo consumo para IoT (Internet of Things), diseñada para funcionar con baterías y con cobertura 95% en el territorio urbano y rural a nivel nacional. Además el despliegue de la red en otros países se está extendiendo con rapidez tanto en Europa, EEUU, Sudamérica y Asia.

La solución de Sigfox se basa en una infraestructura de antenas y estaciones base totalmente independientes de las redes existentes, creando una red única a nivel global gracias a la colaboración de Sigfox con los operadores de telefonía de cada país.

El principal objetivo de Sigfox es permitir que cualquier objeto pueda estar conectado a internet de forma asequible, en cualquier lugar y sin que necesite estar recargando su batería constantemente.

Una de las principales ventajas o características de Sigfox es que, al contrario que otras tecnologías, Sigfox no utiliza tecnologías radio propietarias. A nivel tecnológico utiliza UNB (Ultra Narrow Band), es decir, utiliza canales de ultra banda estrecha de 100Hz, con modulación BPSK (Binary Phase Shift Keying) y velocidades de transmisión a 1000bps. La banda sobre la que se asienta la red es 868Mhz (Europa), con alcances teóricos de hasta 10Km. El impacto de usar UNB es que para transmitir y recibir información se utiliza significativamente menos energía que otras tecnologías como GSM o la radio de banda ancha.

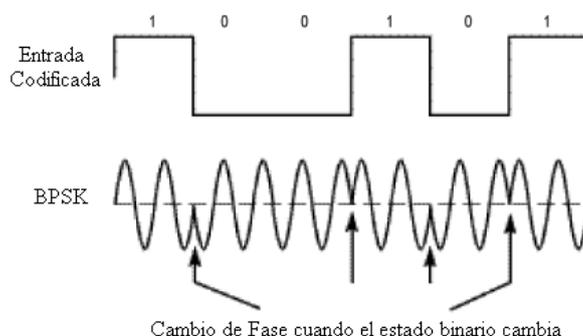


Figura 1: BPSK

Esta red está pensada, como la mayoría de IoT, para dispositivos de baja velocidad y baja transferencia de datos, por lo que en Sigfox los paquetes están limitados entre 0 y 12 bytes de carga útil, permitiendo el envío máximo de 140 mensajes por día. Como ventaja dada esta limitación de datos es que cada estación base puede manejar hasta un millón de dispositivos conectados, pero es fácilmente escalable aumentando la densidad de estaciones base.

Si se compara Sigfox con las tradicionales redes móviles, se puede decir que el consumo es hasta 600 veces menor. En números, una red tradicional de móviles puede llegar a consumir hasta 440MW/h para proveer conexión a 1000 millones de dispositivos 10 veces al día, en cambio Sigfox para la misma cantidad de dispositivos consumiría solamente 120KW/h.



## THD GUARDIAN - TSI-100110-2019-20

Las principales características son:

- ▶ Eficiencia energética, alargando la duración de las baterías hasta en 15 años (depende del dispositivo).
- ▶ Uso de frecuencias libres y resistentes a interferencias.
- ▶ Conectividad física UNB (Ultra Narrow Band) bidireccional.
- ▶ Gestión sencilla y basada en la nube.
- ▶ Cobertura a nivel internacional.
- ▶ Identificación del usuario empotrada en el dispositivo.
- ▶ Conforme con ETSI y FCC.
- ▶ Conexión sencilla (Plug & Play).

Atendiendo a las características de esta tecnología, se puede ver que está pensada para comunicar cualquier sensor que requiera un bajo consumo de energía y baja transferencia de datos. Además por su largo alcance y cobertura la hace ideal para su uso en medios rurales o donde otras tecnologías no llegan (ej. GPRS) y los sensores han de funcionar mediante baterías.

La arquitectura de Sigfox está basada en una red tipo estrella que además está inspirada más en la tecnología del telégrafo que en las redes de banda ancha. La idea viene del sistema de comunicaciones que se utilizaba en los submarinos de II Guerra Mundial, donde se enviaban mensajes muy cortos utilizando transmisiones de baja potencia y larga distancia.

THD GUARDIAN - TSI-100110-2019-20

Sigfox está basado en una infraestructura tipo sistema de telefonía móvil, donde existen una serie de células (antenas o estaciones base) en un rango promedio de 30-50Km en zonas rurales y 3-10Km en zonas urbanas donde hay mayores obstáculos y el ruido es mayor. Estas células son las que hacen de pasarelas entre los dispositivos finales y la nube Sigfox (backend), para que la aplicación de usuario pueda comunicarse con ellos.

En Sigfox existen modos de comunicación para los dispositivos finales, los unidireccionales y los bidireccionales. En los primeros están pensados para dispositivos que no requieren de mensajes provenientes del lado del usuario o servidor, son meros productores de información, dentro de estos tipos de dispositivos se pueden englobar sensores o detectores. En los bidireccionales se englobarían aquellos dispositivos que requieren de configuración o actuaciones remotas, como pueden ser programadores, controladores, etc.



Figura 2: Arquitectura Sigfox

Sigfox provee al usuario una solución global basado en un servicio en la nube, también llamado Sigfox *Backend*, donde toda la infraestructura está ya configurada, lo cual facilita su puesta en marcha, ya que no tiene que crear la infraestructura, solamente conectar los dispositivos a la red. Por tanto el usuario solo se tiene que encargar de desarrollar su aplicación en base a la API que proporciona Sigfox para el acceso a los dispositivos a través de la nube, mediante protocolos estándar como REST o MQTT.

Esto es una ventaja ya que la red está disponible y lista para usar cuando el usuario lo desee, pero por el contrario, es menos flexible en el caso de que se quiera montar una red propia, ya que no es posible (sigue el mismo concepto de las redes de telefonía móvil).

Para usar la red Sigfox e integrar un dispositivo en su red, requiere el uso de módems compatibles y certificados, por lo que al día de hoy muy pocos fabricantes disponen de soluciones Sigfox, pues el coste para integrar su tecnología en ellos es alto.



THD GUARDIAN - TSI-100110-2019-20

En el apartado de seguridad y privacidad, Sigfox emplea distintas técnicas de seguridad para preservar la privacidad en las comunicaciones, pero no impone ningún formato específico en los datos ni en el formato de los mismos. Para ello el protocolo de comunicación a nivel físico emplea mecanismos de salto de frecuencia para evitar la interceptación de los mensajes y la replicación de los mismos.

#### 4.2.2 LoRa

Esta tecnología se basa también de una red de largo alcance y bajo consumo diseñada para funcionar con baterías en una red regional, nacional o global. LoRa (Long Range Wide-area network) es una tecnología inalámbrica patentada por la empresa Semtech que proporciona ventajas significativas tanto en el bloqueo como en la selectividad respecto a las técnicas de modulación convencionales, resolviendo el compromiso de diseño tradicional entre el alcance, la inmunidad a las interferencias y el consumo de energía.

Sus principales características son:

- ▶ Muy bajo consumo, lo que permite que los dispositivos que la integren puedan llegar a funcionar durante años con la misma batería.
- ▶ Tiene un gran alcance, permitiendo llegar a lugares de difícil acceso aun no teniendo visión directa.
- ▶ Es una red bidireccional, y también permite comunicación multicast (difusión).
- ▶ Tasa de transferencia de datos variable desde 300bps a 50kbps.
- ▶ Comunicaciones seguras, mediante el cifrado de las mismas.
- ▶ Es ideal en el ámbito IoT, ya que permite el seguimiento de equipos a un coste mínimo, monitorizar una ciudad, sin necesidad de red wifi o móvil, lecturas de contadores remotas, etc.

Una de las características principales que es su bajo consumo se debe a la forma en que se envía la información. Para ello utiliza una técnica de modulación FM de espectro ensanchado patentada (Chirp Spread Spectrum) dentro de un ancho de banda para canal fijo. Esta tecnología permite implementar una velocidad de transferencia de datos variable, utilizando factores ortogonales de propagación que permite al diseñador optimizar potencia de transmisión manteniendo el ancho de banda.

En el lado del receptor los datos son recuperados volviendo a multiplicar con una réplica de la secuencia de dispersión generada localmente. Este proceso comprime el ancho de banda ensanchado, devolviendo la señal a su ancho de banda original.

En la codificación tradicional de los sistemas de espectro ensanchado, la portadora cambia de fase en el transmisor de acuerdo al código a enviar. Este proceso generalmente se realiza multiplicando los datos a enviar por un código de ensanchamiento, conocido como chirp. Chirp hace referencia al símbolo más pequeño que puede ser enviado. Esta secuencia de chirps se origina a una velocidad mucho más rápida que los datos y por tanto, el ancho de banda de la señal se distribuye más allá del ancho de banda de la señal original.

Chirp Spread Spectrum fue desarrollado para aplicaciones de radar en 1940. Se usaba en numerosas comunicaciones seguras militares. En los últimos 20 años, este tipo de modulación ha visto una mayor adopción en aplicaciones de bajas necesidades de transmisión en potencia y por su robustez ante multirayectos, atenuación, interferencias, etc.



THD GUARDIAN - TSI-100110-2019-20

Debido a estas características CSS fue adoptada por el IEEE para su uso en redes de baja velocidad de transferencias (LR-WPANs) en el estándar 802.15.4, para aplicaciones que requieren un mayor alcance que el alcanzable con otros tipos de modulación como OQPSK.

En LoRa, la modulación por espectro ensanchado es generada por una señal chirp que continuamente varía en frecuencia. Una ventaja de este método es que las diferencias de tiempo y frecuencia entre el emisor y el receptor, son equivalente lo que reduce la complejidad del diseño del receptor. Como consecuencia el ancho de banda de la señal chirp es equivalente al ancho de banda del espectro de la señal.

Las ventajas de usar esta modulación son:

- ▶ Ancho de banda escalable.
- ▶ Envoltorio constante/baja potencia.
- ▶ Alta robustez.
- ▶ Inmunidad a señales multitrayecto y atenuadas.
- ▶ Inmune al efecto Doppler.
- ▶ Largo alcance.
- ▶ Aumento de la capacidad de la red, gracias a utilizar distintos factores de propagación simultáneamente.
- ▶ Alcance y localización, debido a su habilidad para discriminar entre errores de tiempo y frecuencia.

La frecuencia de transmisión para Europa está fijada en la banda 868 Mhz, dejando libre el uso de los canales por el operador, aunque se fijan 3 canales que todas las pasarelas (gateways) deben escuchar constantemente (868.10, 868.30 y 868.50 Mhz). Cada dispositivo final debe de ser capaz de manejar hasta 16 canales.

Sobre la capa física de LoRa se define la arquitectura LoRaWAN. Su arquitectura se basa en una topología en estrella (o conjunto de estrellas), donde las pasarelas (gateways) transmiten la información de forma transparente entre los dispositivos finales (nodos LoRa) y el servidor central (backend). Por tanto, las pasarelas se conectan al servidor central mediante protocolo estándar IP, y los dispositivos finales hacen uso de la comunicación inalámbrica LoRa para, mediante un salto o varios, llegar hasta el servidor central.

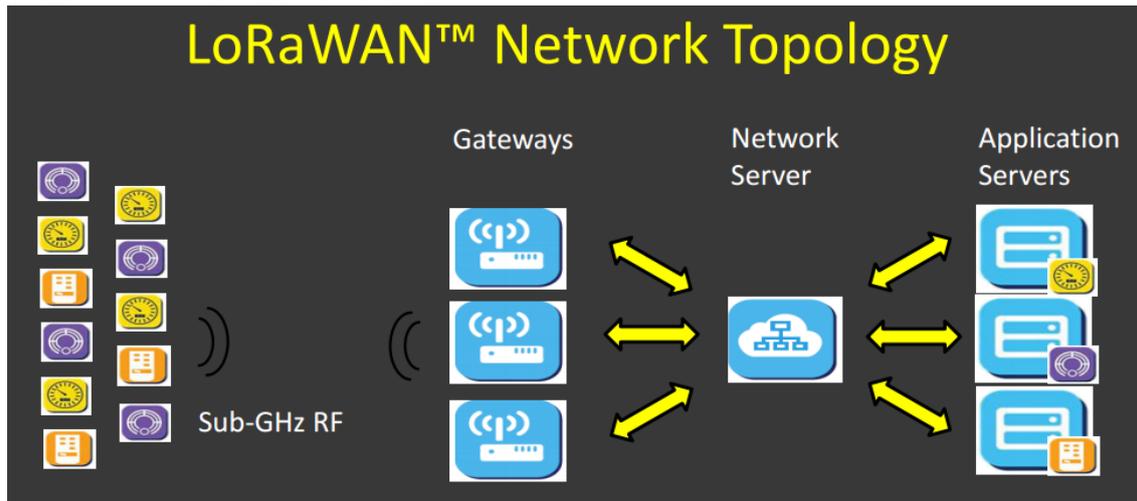


Figura 3: Arquitectura LoRaWAN

La comunicación entre dispositivos finales se realiza utilizando distintos canales con modulación de espectro ensanchado y distintas canales de frecuencia, lo que permite que los datos no se interfieran entre sí, generándose de esta forma una serie de canales “virtuales” que aumentan la capacidad de la pasarela. Para maximizar la duración de la batería de los dispositivos, el servidor de red gestiona la velocidad de datos y nivel de señal RF para cada dispositivo de forma individual mediante un esquema de velocidad de datos adaptativa (**Adaptative Data Rate**).

Otro punto clave en el tema de las comunicaciones IoT es la confidencialidad de los datos, para ello, LoRa lo ha resuelto con varias capas de cifrado, basado en AES-128:

- ▶ Clave de red única (EUI64), que garantiza la seguridad a nivel de red (NwkSKey).
- ▶ Clave única de aplicación (EUI64), que garantiza la seguridad a nivel de extremo a extremo en el nivel de aplicación (AppSKey).
- ▶ Clave específica de dispositivos (EUI128).

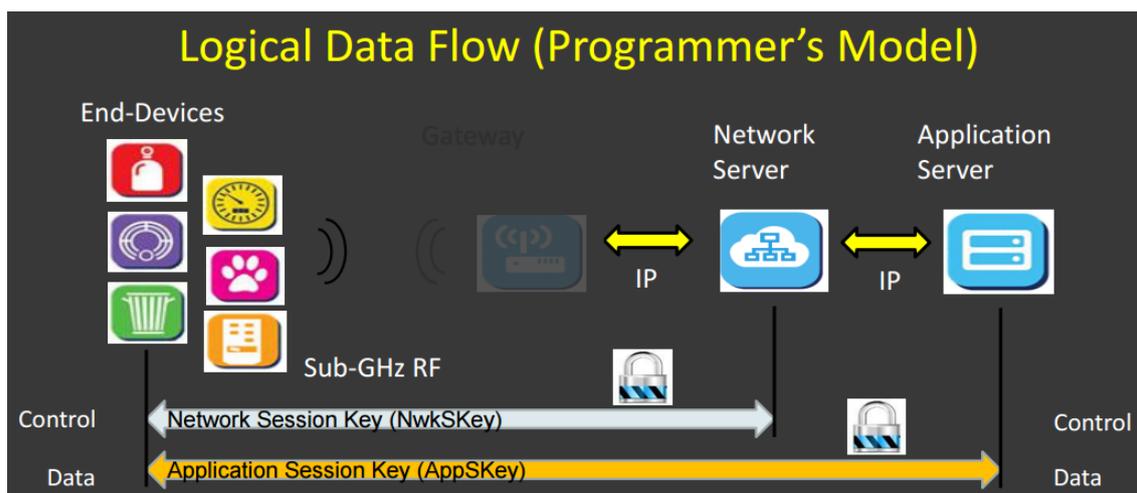


Figura 4: Modelo de programación

El estándar LoRaWAN también define distintas clases de dispositivos en base a los tipos de comunicación que realicen y el grado de optimización que se desee:

- ▶ **Clase A.** Son dispositivos que permiten comunicaciones bidireccionales. La comunicación en sentido dispositivo al servidor se realiza en base a las necesidades del dispositivo final, con una pequeña variación basada en una base de tiempo aleatoria (tipo protocolo ALOHA). Por el contrario las comunicaciones en sentido servidor al dispositivo, deberán esperar hasta que el dispositivo realice su siguiente comunicación programada. Este tipo de dispositivos se utiliza cuando hay pequeñas transferencias de datos en intervalos largos de tiempo y es el dispositivo el que inicia la comunicación.

### Device Class A



Figura 5: Comunicación dispositivos clase A

- ▶ **Clase B.** Son dispositivos con ventanas de recepción programadas, es decir, cada dispositivo final activan la recepción en ventanas temporales programadas, el cual recibe una baliza sincronizada desde la pasarela, que permite al servidor saber cuándo el dispositivo está a la escucha.

### Device Class B

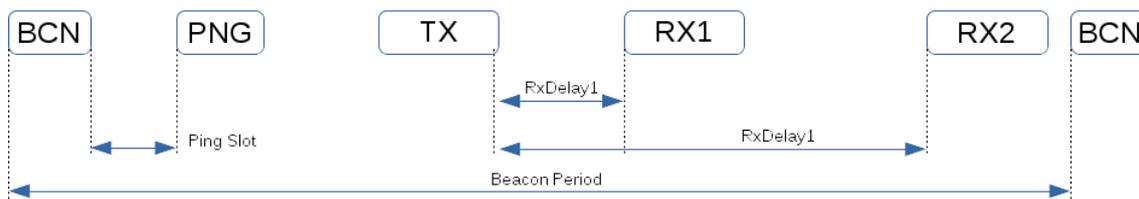


Figura 6: Comunicación dispositivos clase B

- ▶ **Clase C.** Son dispositivos que siempre están a la escucha y solamente transmiten cuando lo requieren, permitiendo de esta forma el recibir información desde el servidor en cualquier momento.

### Device Class C



Figura 7: Comunicación dispositivos clase C

#### 4.2.3 NB-IoT/LTE-M sobre 5G

Ante el avance imparable de las tecnologías IoT, el organismo 3GPP que reúne 7 organizaciones de estandarización mundiales para las tecnologías 3G/4G/LTE/5G (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC), inició la definición de estándares de comunicaciones específicos para IoT con los siguientes condicionantes:

- ▶ Uso del espectro licenciado, garantía de calidad y de ausencia de interferencias por concurrencia.
- ▶ Creación de perfiles de bajas tasas de datos.
- ▶ Creación de perfiles de bajo consumo eléctrico.
- ▶ Posibilidad de disponer de HW de bajo coste por debajo de la barrera de 5\$.
- ▶ Posibilidad de ofrecer costes de comunicación reducidos y adaptados a las aplicaciones propias de IoT.



Figura 8: Categorías de comunicaciones dentro del estándar LTE

Esto dio lugar a las evoluciones del LTE/4G adaptadas al IoT (Cat M1 o Cat M y Cat NB o NB-IOT). Ambas son versiones reducidas del 4G y están optimizadas para aplicaciones de bajo consumo de datos y energía y veremos su despliegue mundial a partir de 2017 dentro de la estrategia de IoT de las operadoras.

Narrow Band IoT (NB-IoT), antes conocido como LTE Cat-NB, es un estándar del 3GPP aprobado en Junio de 2016 e incluido dentro de la release 13 de LTE. Ofrece una cobertura adicional de 20 dB sobre el GPRS y, debido a su diseño, su consumo de energía es mínimo permitiendo duración de baterías de más de 10 años, tamaño de dispositivos mínimo y un coste por dispositivo inferior. Mantiene la compatibilidad con la infraestructura de red móvil existente y ofrece el mismo nivel de seguridad que el LTE. NB-IoT cuenta con todas las ventajas de una tecnología estándar, respaldada por los mayores fabricantes y operadores del mundo. Puede desplegarse en varias bandas de frecuencia, si bien la óptima es la frecuencia de 800 MHz en la que se maximiza la penetración. Utiliza un ancho de banda de tan sólo 200 kHz con una portadora autocontenida.

NB-IoT soporta hasta 100.000 dispositivos conectados a una misma celda sin los problemas de colisión de envío que se producen en otras tecnologías (Sigfox y LoRa) con espectro no licenciado. Y, a diferencia de Sigfox, es totalmente bidireccional, permitiendo usos en los escenarios que requieren actuaciones de forma remota.



THD GUARDIAN - TSI-100110-2019-20

Posteriormente se decidió englobar NB-IoT/LTE-M dentro de 5G, donde se sigue manteniendo como tecnología radio para dispositivos de bajo consumo.

#### **4.2.4 Comunicaciones intervehiculares**

Una vía de mejora futura queda abierta en el campo de las comunicaciones entre vehículos ante la posibilidad de añadir nuevos servicios en tiempo real de cara por ejemplo a la optimización de rutas si se diera la situación de que un vehículo cercano pudiera servir de apoyo en un momento dado durante la fase de distribución. Otro escenario podría ser el de un segundo vehículo que ofrece apoyo ante la previsión de una desviación inminente en el control de la temperatura por un problema técnico.

En esos y otros escenarios similares (los más habituales a día de hoy están ligados a envío de notificaciones en caso de detección de congestión, accidentes, etc.) son aplicables los protocolos de comunicación intervehiculares, siendo a día de hoy el más predominante el 802.11p. Se comentan a continuación algunas de las características generales del mismo.

##### **4.2.4.1 802.11p**

El protocolo 802.11p pertenece a la familia de protocolos 802.11 definidos por el IEEE para dispositivos inalámbricos, familia en la que están también por ejemplo las variantes asociadas a las redes Wifi.

En 802.11p las comunicaciones se denominan DSRC (del inglés *Dedicated Short Range Communications*) que utilizan canales de 10 MHz en la franja de 5.9 GHz. En Estados Unidos la pila de comunicaciones está recogida dentro del estándar WAVE (del inglés *Wireless Access in Vehicular Environments*) mientras que en Europa se usa el estándar ITS-G5.

La principal diferencia frente a otros protocolos inalámbricos es que en 802.11p se elimina la fase de asociación ya que en el escenario habitual el tiempo de visión entre dos vehículos suele ser pequeño. Por lo tanto estamos hablando de un protocolo diseñado para trabajar sobre redes adhoc. Además se elimina la seguridad de los niveles inferiores de la arquitectura, delegando así todo el control de la misma en la capa de aplicación.



THD GUARDIAN - TSI-100110-2019-20

A nivel de capas se ofrece la posibilidad de ofrecer aplicaciones ITS (del inglés *Intelligent Transport Systems*) usando directamente una pila IPv6 completa, con TCP/UDP/etc. a nivel de transporte y con IPv6 a nivel de red, pero también ofrece una solución alternativa usando BTP (del inglés *Basic Transfer Protocol*) a nivel de transporte y GeoNetworking a nivel de red. BTP es un protocolo ligero de nivel de transporte, mientras que GeoNetworking es un protocolo orientado a comunicaciones en áreas geográficas en el que se añaden algunas mejoras a nivel de routing que permiten establecer comunicaciones en varios modos, incluyendo tanto punto a punto como punto a multipunto a nivel geográfico (GeoBroadcast para envío a todos los nodos de un área y GeoAnycast para envío a cualquier nodo de un área).

Los componentes principales que se definen dentro de esta tecnología son las estaciones ITS, existentes tanto a nivel de infraestructura (equipos instalados físicamente en puntos de la misma) como a nivel del propio vehículo (dentro de la unidad de abordaje), de forma que las primeras permiten ofrecer servicios añadidos como por ejemplo avisos de retenciones o accidentes en ubicaciones que pudieran afectar al vehículo en su trayecto, entre otros, aunque como tal las prioritarias son las segundas, y son las que permiten la comunicación directa entre vehículos como tal.

#### 4.2.5 Análisis comparativo de las tecnologías de comunicaciones

A continuación, se muestran las ventajas y desventajas de cada una de las tecnologías de comunicaciones:

##### ► Sigfox.

- Ventajas: Bajo consumo eléctrico. Facilidad de uso. Reducido coste de tarifa de datos.
- Desventajas: Cobertura de red muy débil a nivel mundial. Saturación del espectro no licenciado. Tecnología propietaria no estándar. No permite comunicación bidireccional. Reducido volumen de datos que se puede enviar cada día.
- Recomendado: Sensores de ultrabajo consumo para monitorizar información sin realizar actuaciones.

##### ► LoRa.

- Ventajas: Bajo consumo eléctrico. Varios perfiles de uso. Permite comunicación bidireccional (con limitaciones) y despliegue de punto de acceso.
- Desventajas: Mezcla de redes operadas y no operadas. Muy poca cobertura de red existente a nivel mundial. Requiere de servidor de datos propio.
- Recomendado: Despliegue de múltiples equipos de control en un área de largas distancias sin buena cobertura 5G y reduciendo el coste del mantenimiento de tarifas móviles con operadoras.

##### ► NB-IoT/LTE-M sobre 5G.

- Ventajas: Bajo consumo eléctrico. Permite comunicación bidireccional completa. Hace uso de la infraestructura existente. Menor ratio de colisiones al trabajar sobre banda licenciada. Alta seguridad en las comunicaciones (el mismo nivel que LTE). Mayor ancho de banda.
- Desventajas: El coste varía dependiendo de las distintas tarifas móviles.
- Recomendado: Equipos que necesiten tener la mayor cobertura posible y, opcionalmente, con soporte bidireccional completo.

##### ► 802.11p.

- Ventajas: Optimizado para comunicación de eventos circunscritos en un área geográfica que permiten adaptar las rutas de vehículos cercanos en caso de incidencias.
- Desventajas: No diseñado para envío masivo de datos desde vehículos hacia plataforma. Poco despliegue actual.
- Recomendado: Entornos donde se desea publicar eventos a otros vehículos en caso de emergencias, atascos, accidentes o similares.



Además, la siguiente tabla muestra los valores comparativos de NB-IoT con Sigfox y LoRa, de acuerdo a las especificaciones técnicas del estándar NB-IoT y a la información disponible de Sigfox y LoRa Alliance.

	LoRa	Sigfox	NB-IoT
<b>cobertura</b>	160dB	157 dB	164dB
<b>tecnología</b>	propietaria	propietaria	Abierto LTE
<b>espectro</b>	no licenciada	no licenciada	Licenciada (LTE /otra)
<b>restricciones de envío</b>	si	si	no
<b>restricciones potencia transmitida</b>	si (14dBm = 25mW)	si (14dBm = 25mW)	no (23 dBm = 200mW)
<b>velocidad de bajada</b>	<0.1 kbps	<10kbps	0,5-200kbps
<b>velocidad de subida</b>	<0.1 kbps	<10kbps	0,3-180 kbps
<b>vida batería (200b/día)</b>	10+	10+	15+
<b>seguridad</b>	baja	baja	muy alta

Figura 9: Comparativa de tecnologías Sigfox, LoRa y NB-IoT

### 4.3 Conclusiones

El escenario sobre el que se va a desarrollar el proyecto (en la parte IoT, véase, en los vehículos) se caracteriza, entre otras cosas, por lo siguiente:

- ▶ Va a haber un intercambio de importantes volúmenes de información.
- ▶ Es importante disponer de la máxima cobertura posible para detectar/notificar cuanto antes las posibles desviaciones en la temperatura que se pudieran producir.
- ▶ La seguridad es fundamental como parte del proceso de validación de la información dentro del sistema de calidad.

El diseño de nuevos equipos de sensorización y control para la logística refrigerada deben tener en cuenta las características de las tecnologías de comunicación IoT. Ninguna tecnología es ideal para todos los escenarios de vehículos y almacenes, sino que cada tecnología dispone de ventajas relevantes para ser aplicados en escenarios concretos. Además, estas tecnologías se pueden combinar para proporcionar la mejor solución de gestión integral de los almacenes y vehículos de transporte refrigerados.

Para almacenes e instalaciones interiores, a diferencia de Wifi, es mejor las tecnologías mesh multisalto como Zigbee y Zwave de bajo consumo y que simplifica la instalación de sensores con batería sin grandes costes de instalación y despliegue que pueden ser gestionados por uno o varios controladores localmente sin depender de la conexión a la nube para acciones eficientes y más rápidas. En el caso de vehículos, LORA permite grandes despliegues de equipos de sensorización y telecontrol con bajo coste de mantenimiento sin necesidad de tarifas de transmisión de datos en ciudades, sin embargo, todavía no existen suficientes redes desplegadas en España y Europa para dar cobertura a soluciones de este tipo. Por otro lado, las restricciones en cuanto a cantidad de información que tiene Sigfox la descartan como solución viable, y la mayor cobertura a nivel tanto nacional como internacional así como un nivel de seguridad muy superior (el mismo que LTE) hacen que la opción más interesante sea NB-IoT. Además, este aspecto es importante en favor de NB-IoT

THD GUARDIAN - TSI-100110-2019-20

ya que permite utilizar dispositivos en vehículos más sencillos y de menor consumo, una vez que es la propia red la que protege el propio canal de comunicaciones de forma segura. Por último, el protocolo 802.11p es el menos usado ya que, más que un ser una solución como tal, puede servir de apoyo en algunos escenarios donde la infraestructura (y el resto de los vehículos) lo permita. En cualquier caso, hoy en día no hay apenas despliegue a nivel mundial a nivel de infraestructuras, y a nivel de vehículos se está en la fase inicial de su implantación en el mercado automovilístico.

## 5 Diseño de equipos de sensorización y control basados en tecnologías IoT

En esta sección, se muestra el diseño hardware de los nuevos equipos de sensorización y control para soportar las tecnologías IoT comentadas anteriormente y sus respectivos módulos de comunicación inalámbrica. Además, se indica los protocolos y conexiones soportadas por los equipos diseñados por OdinS que permiten una amplia monitorización de los parámetros de consumo energético y condiciones del estado de las mercancías refrigeradas en almacenes y vehículos.

### 5.1 Nuevos módulos de comunicación basados en tecnologías IoT

Para el diseño hardware de los nuevos equipos, se han seleccionado los siguientes módulos comerciales que soportan las tecnologías IoT (GPRS/3G, LTE-M/NB-IoT, Sigfox y LoRa) para comprobar y evaluar sus características y comportamiento en escenarios de sensorización y control.

- **GPRS/3G.**

- **Módulo SIM800C de la empresa SIMCOM.** SIMCOM es una empresa dedicada al desarrollo de soluciones de comunicaciones inalámbricas especializadas en M2M, centrada en el desarrollo de módulos de comunicaciones GPRS, 3G, LTE, UMTS, HSPA, GPS, etc. El SIM800C es un módulo GPRS cuatribanda de pequeñas dimensiones y bajo coste, controlado de forma sencilla mediante comandos AT y con pila TCP/IP integrada.



Figura 10: Módulo GPRS SIM800C

- **Módulo M95 de la empresa QUECTEL.** QUECTEL es también una empresa dedicada principalmente al desarrollo de soluciones inalámbricas especializadas en M2M. Dispone de soluciones GPRS, 3G, LTE, UMTS, 4G, etc. El módulo M95 es un módulo GPRS cuatribanda, de reducidas dimensiones, con pila TCP/IP integrada, manejo mediante comandos AT estándar y que presume de un bajo consumo.



Figura 11: Módulo GPRS M95



- **LTE-M/NB-IoT.**

- **Módulo BG96 de la empresa QUECTEL.** El módulo BG96 es un módulo que soporta los estándares celulares de LTE-M y NB-IoT de ultra bajo consumo que se controla mediante comandos AT.



Figura 12: Módulo BG96 para LTE-M y NB-IoT

- **Zwave:**

- **Aeotec Z-Stick Gen5 Plus.** Es un módulo fabricado por la empresa Aeotec. Este módulo incorpora un microcontrolador, chip radio y conexión USB para montarse en cualquier dispositivo con puerto USB para trabajar con redes Zwave. En el caso, los módulos implementan toda la tecnología y protocolo Zwave, lo cual simplifica la implementación en el equipo controlador de sensorización y control, sin necesidad de tener que implementar esta parte el usuario final.



Figura 13: Módulo Aeotec Z-Stick Gen5 Plus

- **Zigbee:**

- **CC2531 Módulo USB-Zigbee Dongle.** Texas es una empresa dedicada al desarrollo de chip de todo tipo y entre ellos dispone este chip radio preparado para trabar en distintas bandas y compatible Zigbee lo que permite realizar diseños a medida basados en redes. Por el contrario, tiene la desventaja de tener que integrar el software para el manejo de estas en el dispositivo desarrollado.



Figura 14: CC2531 Módulo USB-Zigbee Dongle

- **SIGFOX**

- **Módulo Telit LE51-868S.** Telit es una empresa dedicada al desarrollo de soluciones inalámbricas que abarca tanto soluciones radio, como GPRS, 3G, LTE, GPS, Sigfox, etc. El módulo LE51-868S presume de una alta sensibilidad de señal de hasta -126dBm, muy bajo consumo y listo para utilizar en la red Sigfox. Su potencia de transmisión es configurable, lo que permite reducir aun mas el consumo según necesidades y permite un alcance de hasta 2Km. Otra característica de este módulo es que permite ser utilizado fuera de la red Sigfox, permitiendo velocidades de transferencia mayores que esta (hasta 100Kbps).



Figura 15: Módulo Sigfox LE51-868S

- **Módulo TD next TD1207R.** TD next es un proveedor de tecnologías para IoT y especializada en soluciones Sigfox. Las características destacadas del módulo son su bajo precio, reducidas dimensiones y su bajo consumo. Posee la misma sensibilidad que módulo Telit y está certificado por Sigfox, por lo que está listo para su uso.



Figura 16: Módulo TD next TD1207R

- **LORA.**

- **Módulo Microchip RN2483-I/RM101.** Microchip es una empresa dedicada principalmente al desarrollo microcontroladores, pero que poco a poco se va expandiendo adquiriendo terceras empresas para abarcar más sectores, como las comunicaciones inalámbricas, tipo Zigbee, Wifi, Bluetooth, LoRa, etc. Sobre todo

relacionadas con el mundo IoT para aplicaciones M2M, Smart City, redes de sensores, etc. En el caso del módulo RN2483, se trata de un módulo de Clase A que implementa LoRaWAN. Como características destaca su manejo mediante sencillos comandos ASCII, reducido tamaño, E/S de propósito general y EUI-64 integrado.

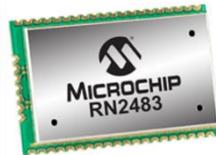


Figura 17: Módulo Microchip RN2483

- **Módulo IMST iM880B.** IMST es un centro de desarrollo de soluciones inalámbricas, circuitos de alta frecuencia y sistemas de comunicaciones. El módulo iM880B permite ser usado como base de radio LoRa simplemente o bajo el protocolo LoRaWAN con la especificación de la LoRa Alliance. Entre sus características destacan su alta sensibilidad (-138dBm) y su alcance de hasta 15Km.



Figura 18: Módulo IMST iM880B

- **Módulo RFM95W del fabricante HopeRF,** incorpora el módem de largo alcance LoRa que proporciona una comunicación de espectro expandido de gama ultra larga y una inmunidad de alta interferencia mientras minimiza el consumo de corriente. RFM95W puede lograr una sensibilidad de más de -148dBm usando un cristal de bajo costo. La alta sensibilidad combinada con el amplificador de potencia integrado de +20 dBm genera un módulo de largo alcance, líder en la industria que lo hace óptimo para cualquier aplicación que requiera robustez y larga distancia. El RFM95W proporciona excepcional ruido de fase, selectividad, linealidad del receptor y IIP3 para un consumo de corriente significativamente menor que los módulos de la competencia.



Figura 19: Módulo HopeRF RFM95W

## 5.2 *Diseño para soporte de diferentes módulos de tecnologías IoT*

En los equipos de sensorización y control, se ha mejorado el diseño hardware para soportar el uso de diferentes módulos de comunicación y así facilitar el uso de la tecnología IoT que sea más interesante según el lugar y condiciones del escenario concreto de despliegue y aplicación del sistema de monitorización y control de la logística refrigerada. El equipo dispone de un único slot plug-play compatible con cada placa de conexionado que integra el módulo requerido de la tecnología IoT elegida.

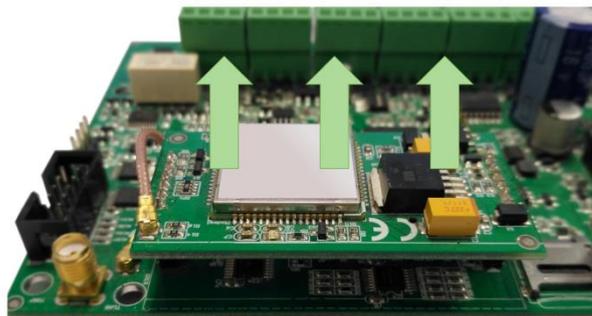


Figura 20: Diseño de placa conexionado para múltiples módulos IoT

## 5.3 *Diseño para Inserción de tarjeta SIM con tecnologías celulares*

En las tecnologías celulares es necesario el uso de tarjeta SIM que identifica y posibilita la conexión a las estaciones bases de las operadoras que ofrecen GPRS/3G y en el futuro LTE-M y NB-IoT. La inserción de la tarjeta SIM se debe realizar siempre con la alimentación desconectada. Para insertarla, se deben seguir los siguientes pasos:



Figura 21: Diseño para tarjeta SIM de tecnologías celulares

- 1) Se extrae la placa de conexionado del módulo celular como se indica en la figura.
- 2) Se abre el compartimento de la tarjeta SIM deslizándolo hasta desbloquearlo, se inserta la tarjeta SIM en dicho compartimento y se cierra.
- 3) Se vuelve a colocar la placa de conexionado del módulo celular en la posición inicial.

#### **5.4 Diseño de conexionado de antena para módulos IoT**

En el diseño, se ha incluido un conector SMA hembra para el conexionado de la antena que recibe y transmite la señal inalámbrica que generan los módulos de comunicación IoT. Para facilitar el uso de diferentes módulos IoT, hay un latiguillo uFL-uFL que interconecta el módulo IoT específico con el conector SMA de antena, sin necesidad de soldar o desoldar ningún componente hardware.



Figura 22: Conexionado de antena para módulos IoT

#### **5.5 Equipos de sensorización y control para almacenes refrigerados**

En los almacenes hay dos ámbitos en los que se debe hacer un seguimiento.

Por un lado, y asociados a los requisitos de trazabilidad impuestos por las GDP, están las cámaras dentro de los propios almacenes donde se guardan los productos y para las que se debe estar realizando un seguimiento de temperatura, humedad y nivel de luz. Tal y como se ha comentado anteriormente, los dos prioritarios, dado que son obligatorios en este caso, son temperatura y humedad.

Hay que tener en a su vez cuenta algunas recomendaciones propuestas por las GDP respecto a la toma de datos de temperatura y humedad, y es que se resalta la importancia que tiene el control en torno a puntos donde hay más variaciones de los valores, como por ejemplo en torno a puertas o cerca de posibles fuentes de calor, si las hubiera.

Por otro, de cara a buscar una mejora en la eficiencia energética, se deberán monitorizar los consumos de todos aquellos subsistemas que se tengan instalados. En principio los que más suelen influir son los de refrigeración y los de iluminación, para los que se deberá poder tomar mediciones por zonas de forma que se pueda identificar con el mayor detalle posible cuáles de ellas son las que más están influyendo a nivel global.

Se intentará buscar una solución lo más robusta posible en este escenario en el que hay menos restricciones de cara a instalar nuevo equipamiento asociado a la toma de datos. En la medida de lo posible se dispondrá de diferentes tecnologías de comunicación inalámbrica y cableada para soportar el mayor abanico posible de conectividad tanto a nivel de comunicación de los equipos de sensorización y control con la plataforma (Ethernet, Wifi) como a nivel de conexionado entre de los

THD GUARDIAN - TSI-100110-2019-20

sensores con los concentradores. En concreto conector USB para módulos Zwave y Zigbee, así como conexiones 4-20 mA / 0-10 V, buses RS-485 o similares, etc.

A continuación, se muestra a nivel de bloques un diagrama con los módulos que debe incluir el dispositivo concentrador de sensores a instalar en el almacén.

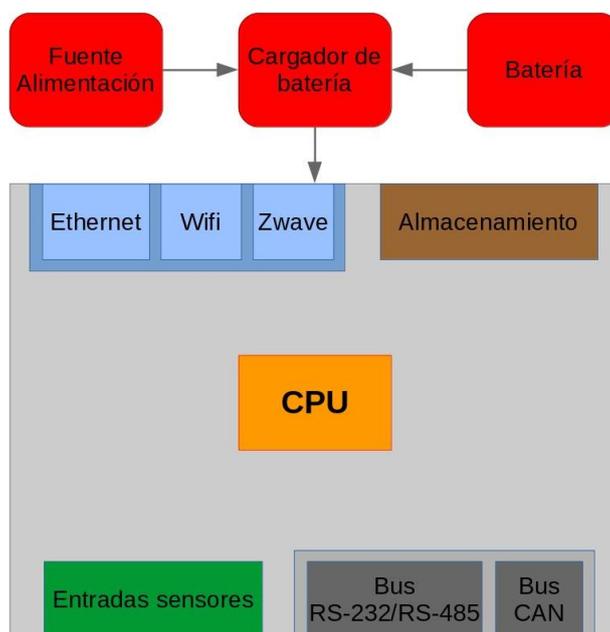


Figura 23: Equipo de sensorización y control de almacenes refrigerados

### 5.6 Equipos de sensorización y control para vehículos refrigerados

En los dispositivos instalados en los vehículos también influyen los dos factores comentados en la sección anterior.

El primero es la propia monitorización de la temperatura dentro del contexto de la trazabilidad de la distribución de los productos. Opcionalmente se valorará la posibilidad de hacer una monitorización de la humedad, aunque no es el caso habitual ya que en la mayoría de los casos se trata de vehículos refrigerados, sobre todo en el transporte de alimentos, donde incluso pueden ir congelados y la humedad no aporta apenas información.

A la hora de diseñar la solución habrá que analizar hasta qué punto es viable realizar una instalación cableada dentro del propio vehículo. Es por eso que se plantea aquí la posibilidad de utilizar uno o más dispositivos inalámbricos que recojan la información en varios puntos y la envíen a un único nodo concentrador que hará las veces de pasarela hacia la plataforma. Con respecto a la comunicación con la plataforma, se proporcionará un socket de conexión múltiple que permitirá elegir entre diferentes módulos inalámbricos IoT de largo alcance que sean explicado anteriormente, aunque según el análisis realizado nos decantamos por la tecnología NB-IoT por sus beneficios de consumo/seguridad y su mayor cobertura a nivel internacional en los próximos años.

El segundo es la mejora en la eficiencia energética. En los vehículos intervienen principalmente el consumo asociado a la propia conducción (velocidad, uso de marchas cortas/largas, etc.) así como las rutas empleadas para cada trayecto.

THD GUARDIAN - TSI-100110-2019-20

Para medir el consumo, se evaluará la viabilidad técnica de monitorizar ese valor en tiempo real ya que no siempre se tiene acceso a dicha información al tratarse de datos propietarios de los fabricantes de vehículos.

Para la parte relacionada con rutas, se recogerán los datos de las coordenadas GPS de los vehículos en paralelo con la monitorización de la temperatura. Se analizará qué solución es más interesante en función de la ubicación de los sensores, teniendo en cuenta que en muchos vehículos los remolques están compartimentados.

A continuación, se muestra a nivel de bloques el diseño con los módulos que debe incluir el equipo concentrador de sensores a instalar en el vehículo.

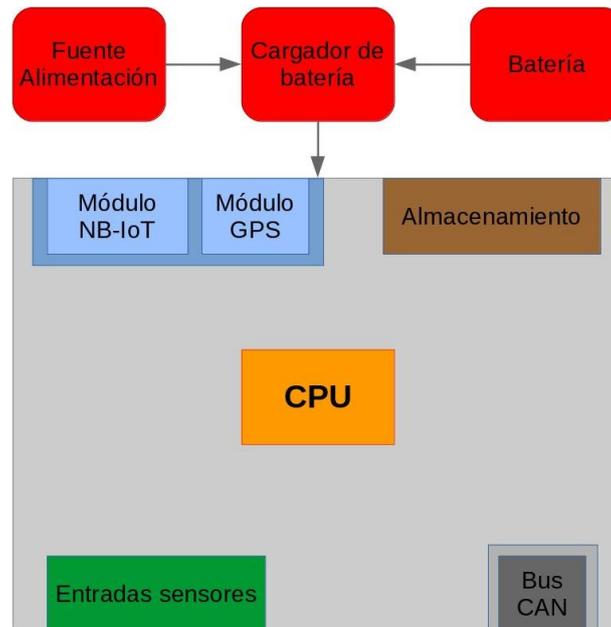


Figura 24: Equipo de sensorización y control para vehículos refrigerados

## 6 Conclusiones

El transporte de alimentos u otros productos a temperatura controlada está ampliamente extendido por lo que, a nivel nacional e internacional, existe una normativa que cubre todas las etapas del proceso de distribución que garantizan la detección de desviaciones, caso de producirse, siempre que se apliquen los protocolos existentes.

Dentro de las distintas etapas de la cadena de suministro, indistintamente de la norma o estándar concreto que se esté aplicando, siempre existe un denominador común en torno al que gira todo el proceso de validación, y es un sistema de gestión de calidad. En él se definen todos los procesos a ejecutar que, de forma rigurosa, establecen una metodología a seguir.

La seguridad es otro de los aspectos clave que se deben tratar dentro del sistema de trazabilidad, para lo que se han definido un conjunto de requisitos mínimos que, en la práctica, se traducirán en aplicar dos tecnologías concretas, que son *blockchain* y *smart contracts*.

En relación con la fase de envío de datos y también en relación la seguridad de dicho proceso, se han analizado varias de las tecnologías existentes en la actualidad tanto para almacenes interiores como vehículos en el exterior. Y, finalmente, toda la recogida y envío de datos requiere de una serie de



THD GUARDIAN - TSI-100110-2019-20

dispositivos que deberán ser utilizados tanto en almacenes como en vehículos, y que deberán ofrecer las opciones de conectividad requeridos tanto a nivel de comunicaciones como con los sensores. Dado que no existe una tecnología ideal para todos los casos, se han diseñados los equipos de sensorización y control para que puedan soportar diferentes tecnologías de comunicación para garantizar las mejores condiciones de disponibilidad de servicio de red, consumo reducido de energía, seguridad y cantidad de datos que se pueden transmitir.

## 7 Referencias sobre Normativas/Legislación/Estándares

- [1] BOE 15 de Noviembre de 2013 (ATP) <https://www.boe.es/boe/dias/2013/11/15/pdfs/BOE-A-2013-11936.pdf>
- [2] UNE-EN 12830:2019 <https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0061766>
- [3] UNE-EN ISO 13485:2018 <https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0060449>
- [4] UNE-EN 13486:2002 <https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0027124>
- [5] Real Decreto 237/2000 <https://www.boe.es/boe/dias/2000/03/16/pdfs/A10799-10815.pdf>
- [6] Orden ITC/3701/2006 <https://www.boe.es/boe/dias/2006/12/06/pdfs/A42884-42890.pdf>
- [7] GDP 5 de Noviembre 2013 <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2013:343:0001:0014:ES:PDF>
- [8] Directiva 2001/83/CE <https://www.boe.es/doue/2001/311/L00067-00128.pdf>
- [9] Directiva 2011/62/UE <https://www.boe.es/doue/2011/174/L00074-00087.pdf>
- [10] Directiva 2012/26/UE <https://www.boe.es/doue/2012/299/L00001-00004.pdf>
- [11] IFS Food <https://www.ifs-certification.com/index.php/es/standards/4132-ifs-food-standard-es>
- [12] Real Decreto 782/2013 <https://www.boe.es/boe/dias/2013/10/19/pdfs/BOE-A-2013-10950.pdf>
- [13] Real Decreto 1085/2015 <https://www.boe.es/boe/dias/2015/12/05/pdfs/BOE-A-2015-13208.pdf>
- [14] Real Decreto 61/2006 <https://www.boe.es/buscar/pdf/2006/BOE-A-2006-2779-consolidado.pdf>
- [15] Real Decreto 1088/2010 <https://www.boe.es/boe/dias/2010/09/04/pdfs/BOE-A-2010-13704.pdf>
- [16] Real Decreto 1361/2011 <https://www.boe.es/boe/dias/2011/10/20/pdfs/BOE-A-2011-16468.pdf>
- [17] Real Decreto 235/2018 <https://www.boe.es/boe/dias/2018/05/01/pdfs/BOE-A-2018-5890.pdf>
- [18] Real Decreto 1597/2011 <https://www.boe.es/boe/dias/2011/11/05/pdfs/BOE-A-2011-17465.pdf>
- [19] IFS Logistics <https://www.ifs-certification.com/index.php/es/standards/2761-ifs-logistics-es>

