ChatGPT

Comunicación de las Balizas V16 Conectadas: Análisis Técnico

Introducción y contexto

Las **balizas de emergencia V16 conectadas** son dispositivos luminosos de preseñalización de peligro que, a partir del 1 de enero de 2026, sustituirán en España a los tradicionales triángulos reflectantes [1] [2]. A diferencia de las balizas V16 iniciales (no conectadas), estos nuevos dispositivos incorporan conectividad IoT integrada para **comunicar su activación, desactivación y posición geográfica en tiempo real** a la plataforma telemática de la Dirección General de Tráfico (DGT 3.0) [3] [4]. El objetivo es mejorar la seguridad vial: además de la señal luminosa visible (hasta 1 km de distancia) que alerta físicamente a otros conductores, la baliza conectada proporciona **"visibilidad virtual"** de la incidencia al enviar su ubicación a los centros de gestión de tráfico y a los sistemas ITS, permitiendo avisar con antelación a usuarios mediante navegadores, paneles de mensajes, etc. [5] [6]. Cada baliza homologada incluye una tarjeta SIM/eSIM IoT con servicio de datos **prepagado por al menos 12 años** (sin cuotas para el usuario) [7] [8], de forma que su conectividad funciona de manera autónoma y transparente cuando se activa en una emergencia. A continuación, se presenta un análisis técnico detallado de cómo se comunican estas balizas V16 conectadas, cubriendo las tecnologías de conectividad empleadas, los protocolos y datos transmitidos, las redes y plataformas involucradas, las implicaciones de seguridad y privacidad, posibilidades de interceptación, y algunas consideraciones sobre dispositivos y marcas específicas.

Tecnologías de conectividad empleadas (NB-IoT, LTE-M y otras)

Las balizas V16 conectadas utilizan **tecnología de comunicaciones móviles en banda licenciada, dentro de los estándares 4G/5G de baja potencia (LPWA) definidos por 3GPP** [9] [10]. En la práctica, esto se traduce en el uso de redes celulares IoT como **NB-IoT (Narrowband-IoT)** y **LTE-M (LTE Cat-M1)** para el enlace de datos. La propia normativa de la DGT exige estas tecnologías por su robustez y longevidad, evitando soluciones obsoletas (p. ej. 2G/3G) o no estandarizadas [9] [10]. Tanto NB-IoT como LTE-M operan sobre el núcleo de las redes LTE/5G existentes, pero están optimizadas para dispositivos IoT: ofrecen **bajo consumo, amplio alcance de cobertura y uso eficiente del espectro** (NB-IoT emplea un ancho de banda de sólo ~200 kHz, con modulación robusta y repetición de mensajes para cobertura en interiores, mientras LTE-M usa ~1.4 MHz con mayor velocidad y soporte de movilidad) [11]. En entornos rurales o con poca señal, NB-IoT suele tener ventaja por su "**cobertura en profundidad**", llegando prácticamente al 100% del territorio español gracias a su penetración mejorada [12]. De hecho, varios fabricantes han migrado de LTE-M a NB-IoT para mejorar la fiabilidad: por ejemplo, la baliza "SOS Road" de Orange en 2023 usaba LTE-M, pero su versión de 2025 incorporó **módulo NB-IoT** para aprovechar la mayor cobertura de la red NB-IoT nacional de Orange [13]. En cambio, otras balizas como la *Help Flash IoT* (desarrollada por Netun Solutions y comercializada con Vodafone) adoptaron NB-IoT desde el inicio, dado que Vodafone desplegó tempranamente esta tecnología en España [14] [15]. Por su parte Movistar (Telefónica) también proporciona conectividad NB-IoT a dispositivos como la baliza "Fase Light" mediante su plataforma Kite [16]. Conviene señalar que NB-IoT y LTE-M son tecnologías complementarias y ambas cumplen los requisitos; la selección depende del acuerdo entre el fabricante y el operador móvil. En cualquier caso, **todas las balizas V16 homologadas integran una SIM IoT solderada o embebida** (no extraíble) asociada a un *plan de datos*

IoT multi-anual con algún operador (Telefónica, Vodafone, Orange, etc.) [7] [17]. Esto permite que la baliza, al encenderse, **se conecte automáticamente a la red móvil IoT disponible** (haciendo *attach* al cell ID correspondiente) sin necesidad de que el usuario contrate ni configure nada. Los operadores garantizan la continuidad del servicio al menos durante 12 años, evitando obsolescencia temprana de la tecnología y manteniendo compatibilidad con sus redes futuras [9] [8] (por ejemplo, extendiendo NB-IoT dentro del marco 5G). En resumen, la comunicación radio de estas balizas se basa en **redes celulares IoT fiables (NB-IoT/LTE-M)** que ofrecen alcance y estabilidad superiores a alternativas no licenciadas (como LoRaWAN o Sigfox) y que están integradas en la infraestructura móvil con **mecanismos de autenticación y cifrado de nivel operador**.

Protocolos de comunicación y arquitectura de transmisión (capas TCP/IP, MQTT, etc.)

Una vez conectada a la red celular IoT, la baliza establece un canal de datos de baja velocidad hacia la plataforma del fabricante (o proveedor) del dispositivo. La **arquitectura de comunicación definida por la DGT** contempla dos tramos o protocolos: **Protocolo A** (entre la baliza V16 y los sistemas back-end del fabricante) y **Protocolo B** (entre el servidor del fabricante y el Punto de Acceso Nacional de tráfico de la DGT) [18] [19]. En el tramo *dispositivo -> fabricante* (Protocolo A), se ha estandarizado el uso de **IP sobre la red celular con transporte UDP** para enviar los mensajes de la baliza [20]. Es decir, la baliza encapsula sus datos en paquetes UDP (User Datagram Protocol) en vez de usar protocolos más pesados como TCP. UDP resulta adecuado por su baja sobrecarga y menor latencia en enlaces restringidos. Dado que UDP no garantiza por sí mismo la entrega, el estándar impone que **el operador móvil devuelva un paquete de acuse de recibo (ACK)** por cada mensaje recibido [21], proporcionando confirmación de llegada sin necesidad de reintentos complejos en la baliza. Esta comunicación suele realizarse a través de un **APN privado y seguro** provisto por el operador [17] [22]. En la práctica, cuando la baliza se activa, se conecta a un APN IoT específico (por ejemplo, el APN corporativo de Vodafone, Movistar, etc. para balizas V16) que **aisla el tráfico del acceso a Internet público**, encaminándolo directamente a la plataforma del fabricante o a la nube DGT según el caso. Esto mejora la seguridad y fiabilidad, al eliminar exposición a redes abiertas.

Sobre esta capa UDP/IPv4 pueden usarse protocolos de aplicación ligeros. La normativa indica que se debe emplear un **"protocolo de comunicaciones estándar"** e intercambiable, sugiriendo un formato común de datos en texto [23] [21]. En efecto, la DGT ha definido un **modelo de trama de datos propietaria en formato texto plano** para los mensajes de incidente (detallado más adelante) [24] [25]. No se menciona MQTT, CoAP u otros protocolos IoT de alto nivel en las especificaciones oficiales; en cambio, la implementación típica parece ser el envío de la trama de datos mediante **payload UDP (por ejemplo vía socket sobre IP)** al servidor correspondiente, sin encapsulación adicional. Esto minimiza la complejidad en la baliza, que suele contar con microcontroladores modestos. Cabe destacar que *algunos fabricantes* pueden ofrecer herramientas de comprobación usando HTTP/HTTPS en la etapa de usuario (por ejemplo, portales web donde, mediante un QR o IMEI, es posible verificar la conexión de la baliza en un mapa) [26]. Sin embargo, internamente la baliza sigue comunicándose vía UDP IoT con el backend, y es este backend el que podría exponer una API web para el usuario final. En el tramo *fabricante -> DGT* (Protocolo B), la comunicación sí emplea interfaces seguras típicas de servicios web: la DGT 3.0 requiere que el fabricante se conecte a su plataforma **mediante autenticación por certificado digital** y posiblemente use HTTPS/REST o similares para transferir cada evento [27] [28]. El mensaje hacia la DGT incluye un *token* de sesión y campos JSON (como id de empresa, tipo de evento, timestamp, coords, etc.) [28] [29], lo que sugiere el uso de un servicio web o API estandarizada en el Punto de Acceso Nacional. En resumen, la pila de protocolos consta de: conectividad celular (NB-IoT/LTE-M) + IP (normalmente IPv4 privada) + **UDP en la capa de transporte** [23] + un **formato de datos ligero específico** definido por DGT; y posteriormente, a nivel servidor, integración mediante **APIs**

seguras entre el sistema del fabricante y la nube DGT 3.0. Esta aproximación evita depender de protocolos IoT genéricos como MQTT en el dispositivo, priorizando en cambio una solución directa, optimizada para mensajes breves y poco frecuentes. La sincronización temporal de todos los actores se asegura mediante **NTP** (los servidores utilizan hora UTC precisa de fuentes Stratum-1 oficiales) para estampar correctamente los eventos [30]. En suma, la baliza envía datagramas UDP a través de una red celular IoT privada, recibiendo ACK del operador, y esos datos viajan por rutas seguras hasta la DGT, todo ello sin intervención del conductor ni necesidad de *smartphone*.

Datos transmitidos y frecuencia de envío

¿Qué información envía exactamente la baliza conectada y con qué periodicidad? La normativa técnica establece con claridad varios puntos: (1) la baliza debe enviar un **mensaje de activación** a los 100 segundos de haberse encendido físicamente [31] [32], (2) debe continuar transmitiendo su posición de forma periódica **cada 100 segundos** mientras permanezca activa [33] [34], y (3) al apagarse, debe enviar un **mensaje de desactivación** para cerrar el incidente [35]. Este retardo inicial de ~100 s actúa como **periodo de gracia** para evitar falsas alarmas: si el usuario enciende la baliza accidentalmente o la apaga rápidamente, no se llegará a notificar nada a la DGT [32]. De hecho, la baliza **no transmite ubicación alguna si se apaga antes de 100 segundos** – no hay "aviso" hasta que se cumple ese tiempo mínimo con la luz encendida [36]. Ahora bien, una vez superado, la primera trama de "inicio de incidencia" se envía y a partir de ahí cada 100 s sale una trama de "incidencia en curso" repetitiva. Esta frecuencia (≈1 mensaje cada 1 minuto y 40 segundos) equilibra la necesidad de mantener actualizada la información con el ahorro energético y de ancho de banda (muy superior al mínimo de 30 minutos de autonomía luminosa exigido) [37] [34].

En cuanto al **contenido de los datos**, la DGT ha definido un modelo estandarizado de campos que la baliza envía en cada trama (Protocolo A). Todos los atributos se codifican en **formato de texto ASCII legible** [25]. Entre los campos principales se incluyen:

- **Identificadores y estado**: un campo de tipo de trama (0=inicio, 1=incidencia periódica, 2=fin) [38], un número de secuencia incremental (que se reinicia en cada nuevo incidente) [39], un identificador del fabricante y del dispositivo (únicos para cada baliza) [40], y versiones de hardware/firmware [40]. Con esto se individualiza el dispositivo y se puede verificar que opera con el software aprobado.
- **Datos de red móvil**: la baliza reporta el **IMEI** de su módulo de comunicaciones [41], el **identificador de celda** a la que está conectada junto con el nivel de cobertura NB-IoT (parámetro ECL) [42], y medidas de señal **RSSI/RSRP/RSRQ** (intensidad y calidad de la recepción) [43]. También envía el código de red **PLMN** (MCC+MNC del operador) [44]. Estos datos técnicos permiten al fabricante/operador monitorizar la calidad de la conexión y localizar la zona (por cell ID) en caso necesario, complementando la geolocalización por GPS.
- **Telemetría del dispositivo**: el **nivel de batería** (en décimas de voltio) [45], y el **tiempo de activación** en minutos [45]. Esto informa si la baliza tiene pila suficiente y cuánto lleva encendida, datos útiles para mantenimiento y para detectar usos anómalos (por ejemplo, activaciones demasiado largas o frecuentes).
- **Posicionamiento GNSS**: las **coordenadas geográficas** de la baliza (latitud y longitud en grados decimales, referidos a datum ETRS89) [25] [46], la **altitud** en metros [47], y parámetros de precisión como el **número de satélites utilizados**, el error horizontal estimado (EPE/HDOP) [47] y el *HDOP* multiplicado por cien [48]. La DGT exige una **precisión mejor de 5 metros** [49], por lo que las balizas incorporan receptores GNSS (GPS/Glonass/Galileo) capaces de obtener localizaciones muy exactas.
- **Temporalidad**: un **timestamp** con fecha-hora UTC (formato ISO8601 o YYYYMMDDHHMMSS) del momento de la medición [25] [50]. Esto sincroniza el evento en la plataforma.

Todos estos datos de la trama *Protocolo A* viajan del dispositivo al backend del fabricante. Sin embargo, la **información que finalmente llega a la DGT 3.0** (Protocolo B) es más reducida y enfocada en la incidencia en sí, **anonimizando el origen**. Al transferir un evento al Punto de Acceso Nacional, el fabricante genera un `actionid` **único por incidente que** no revela el ID del dispositivo [28]**. Los campos enviados a DGT incluyen esencialmente: un identificador de cliente (CN del certificado del fabricante)** [28]**, el** `actionid` **del evento, un** token cifrado de autenticación **proporcionado por DGT 3.0** [51]**, la** hora de detección **del evento, las** coordenadas (lon, lat) **del vehículo averiado, el** tipo de evento **(ej. "vehículo detenido") y si es activación, estado o fin** [29]**, además de la** calidad de info (precisión GPS) [52]**.** No se transmite ningún dato personal del conductor **ni matrícula del vehículo** [53]**; la señal es completamente anónima, solo indica que *"hay un vehículo con incidente en tal ubicación a tal hora"*. De hecho, la DGT 3.0 no guarda información personal ni rastrea vehículos individuales, sino que registra eventos anónimos para gestionar la seguridad vial** [54] [55]**. Los datos se usan operativamente y luego se descartan. Además, la baliza** no emite ningún dato mientras está apagada **– no existe comunicación en reposo ni monitorización continua del vehículo** [56]**. Solo *"despierta"* en caso de emergencia cuando el usuario la activa manualmente, enviando la mínima información necesaria (coordenadas, hora, tipo de señal)** [57]**. En conclusión, la baliza conectada transmite** mensajes cortos (unos pocos cientos de bytes)** cada 100 s con su ubicación y estado, empezando ~1,67 min tras la activación. Esto permite alertar a las autoridades y a otros conductores con suficiente antelación, sin abrumar la red ni comprometer la privacidad del usuario.

Redes y plataformas utilizadas en la comunicación (operadoras, DGT 3.0, etc.)

En el ecosistema de las V16 conectadas intervienen principalmente **las redes celulares de los operadores móviles** y la **plataforma DGT 3.0** del organismo de tráfico. Cada baliza homologada viene asociada (generalmente por acuerdos comerciales) a una de las grandes operadoras españolas: **Telefónica (Movistar)**, **Vodafone** u **Orange**, que proveen la conectividad NB-IoT/LTE-M a través de sus infraestructuras IoT nacionales [58] [59]. Por ejemplo, Movistar comercializa la baliza "Fase Light" con una SIM IoT que utiliza la cobertura NB-IoT de Movistar (casi 100% del territorio) mediante su plataforma Kite [16]; Vodafone colabora con Netun Solutions en la baliza Help Flash IoT, que integra una SIM global de Vodafone y opera sobre su red NB-IoT profunda en España [14] [4]; Orange ofrece la baliza SOS Road Connected, vinculada a su red IoT propia (que, en versiones recientes, también se apoya en NB-IoT) [13]. No obstante, desde el punto de vista del usuario **no importa de qué compañía sea cliente su móvil ni requiere contratar nada**: la baliza funcionará de manera autónoma con la SIM interna incluida [58] [7]. La SIM se autentica en la red del operador designado con credenciales preconfiguradas y registra el dispositivo en una **APN corporativa privada** reservada para estos servicios [17]. Esta APN permite que los datos viajen por la red del operador directamente **hasta el servidor del fabricante o un agregador**, normalmente a través de un **tunel VPN o enlace dedicado** hacia Internet o redes privadas. En algunos casos, los fabricantes pueden emplear plataformas IoT intermedias; por ejemplo, Telefónica dispone de Kite Platform para gestionar SIMs IoT y enrutar datos de dispositivos conectados [60]. No existe interacción con el smartphone del conductor ni con redes locales: todo va por la red celular de larga distancia.

Una vez que la **señal de incidencia** sale de la baliza y alcanza el **backend del fabricante**, es reenviada inmediatamente al **Punto de Acceso Nacional (NAP) de Información de Tráfico**, que en España corresponde a la plataforma **DGT 3.0** [18] [19]. La DGT 3.0 es una nube/servidor central que recibe información de múltiples fuentes ITS (vehículos conectados, servicios de auxilio, etc.) y la pone a disposición de usuarios y proveedores de servicios en tiempo real, conforme a directivas europeas de datos de tráfico [61] [62]. En el caso de las balizas V16, cuando el backend del fabricante comunica un evento con su token y coordenadas, la plataforma DGT 3.0 integra esa alerta en sus sistemas de gestión

de tráfico. **¿Qué ocurre entonces con esa información?** Por un lado, la DGT la envía a los **Centros de Gestión de Tráfico regionales** y al sistema **LINCE** (Localizador de Incidencias en Carretera) [63]. LINCE permite visualizar las incidencias en mapas y a su vez alimenta los **paneles de mensaje variable (PMV)** en las carreteras [63]. Así, en cuestión de un par de minutos, puede aparecer en un panel luminoso un aviso del tipo "Vehículo averiado a 3 km" para advertir a los conductores incluso *no conectados*. Por otro lado, la DGT 3.0 redistribuye la alerta de forma telemática a los **servicios conectados de los usuarios**: aplicaciones móviles de navegación, GPS de coches compatibles, etc. (lo que la normativa denomina *"triángulo virtual V-27"*) [64]. Es decir, si un conductor usa un navegador como Google Maps, Waze u otros integrados con DGT, podría recibir un aviso de incidencia antes de llegar al punto, permitiéndole extremar precauciones o cambiar de carril [65] [66]. Todo este flujo ocurre de manera **automática y anónima**: la baliza emite su posición *100 s después* de encenderse [67], la plataforma DGT la procesa y la comunica "a todos los conductores conectados" en la zona [68], mejorando la seguridad colectiva. Ningún dato de la persona averiada es público; solo la ubicación del obstáculo y el hecho de que hay una emergencia activa.

Desde la perspectiva de **infraestructura de red**, las balizas aprovechan las mismas **bandas móviles licenciadas (800-900 MHz, etc.)** que NB-IoT/LTE-M utilizan en cada operador, beneficiándose de la cobertura de larga distancia y la priorización que estas redes suelen tener (por ejemplo, NB-IoT puede usar repetición y potencias mayores para alcanzar sitios remotos). A diferencia de dispositivos que usan WiFi o Bluetooth, aquí la comunicación es **directa a la nube a través del operador móvil**, similar a cómo funcionan otros IoT críticos (telemedicina, alarmas, smart meters) [36]. Por diseño, la transmisión no depende de que haya cobertura 3G/4G convencional, ya que NB-IoT está desplegado incluso en áreas sin apenas señal de telefonía (permite comunicaciones en lugares donde un móvil corriente quizás no tendría cobertura de datos, gracias a su alta sensibilidad) [4] [69]. Esto resuelve uno de los escenarios preocupantes: que un conductor accidentado en una zona aislada "sin cobertura de móvil" pueda de todos modos enviar su ubicación vía la baliza IoT [70] [4]. En resumen, las **operadoras móviles** proporcionan la red de transporte (NB-IoT/LTE-M, APN privada), y la **DGT 3.0** actúa como el concentrador central que recibe las posiciones y las distribuye a **otros sistemas de tráfico y usuarios**. Todo el ecosistema está alineado con iniciativas de *ITS* (sistemas de transporte inteligente) de la UE para compartir datos de tráfico en tiempo real de forma estandarizada [61] [62].

(Nota: Aunque las balizas conectadas avisan a la DGT y mejoran la señalización, no deben confundirse con sistemas eCall ni notificación directa a emergencias. La propia DGT aclara que la V16 conectada no llama a ambulancias o grúas; el conductor sigue siendo responsable de solicitar auxilio a 112 o a su seguro, ya que la baliza no envía datos personales ni de contacto [71]. Su función es principalmente preventiva e informativa para el tráfico.)

Implicaciones técnicas de seguridad y privacidad (sniffing, spoofing, MITM, etc.)

Dado que las V16 conectadas operan sobre redes celulares IoT y transmiten información de ubicación, es crucial analizar **la seguridad de estas comunicaciones y posibles vectores de ataque**. En términos generales, la arquitectura se ha diseñado con consideraciones importantes de seguridad y privacidad, pero ningún sistema es invulnerable. Veamos punto por punto:

- **Cifrado y autenticación en la red celular:** Las comunicaciones NB-IoT/LTE-M heredan los **mecanismos de seguridad de LTE/5G**. Cada dispositivo lleva una SIM/eSIM con claves criptográficas que autentican su acceso a la red del operador. Una vez adjunto a la red, todo el tráfico de datos entre la baliza y la estación base está protegido mediante cifrado a nivel de capa de enlace (AES-128 o algoritmos 3GPP equivalentes) de la misma forma que en las conexiones

4G normales [72]. De hecho, *"3GPP define estándares de seguridad robustos para LTE-M y NB-IoT, asegurando que todos los datos se transmitan por canales cifrados"* [72]. Adicionalmente, las balizas están **aisladas en APNs privadas** sin salida directa a Internet [17], lo que las protege de accesos externos no autorizados. Esto significa que **interceptar o espiar** el tráfico de una baliza *por métodos convencionales* es extraordinariamente difícil. Un atacante no puede simplemente "escuchar" las comunicaciones como haría con un walkie o con WiFi, ya que están en frecuencias celulares licenciadas y cifradas punto a punto entre la SIM y el núcleo de la red móvil. Se requeriría equipamiento especializado (por ejemplo, un receptor SDR avanzado capaz de sintonizar la portadora NB-IoT y decodificar LTE físicamente) y aún así enfrentaría el cifrado del operador, que sin las claves de la SIM es prácticamente irrompible en tiempo real. Herramientas de radio frecuentes en entornos de *hacking*, como la **Flipper Zero**, no tienen la capacidad técnica para decodificar señales NB-IoT/LTE-M: el Flipper puede captar señales simples en sub-GHz (433 MHz, 868 MHz) con modulación básica, pero **no puede demodular ni desencriptar tramas LTE** (OFDM complejo con criptografía) ni actuar como estación base celular. Por tanto, un *hacker* con un Flipper Zero **no podría sniffar** las comunicaciones de la baliza conectada ni extraer su ubicación en directo – simplemente no está dentro del alcance de ese dispositivo.

- **Protección del hardware SIM y la interfaz de datos:** Las especificaciones requieren que la **tarjeta SIM no sea extraíble** [17] [73]. Muchas balizas usan SIMs soldadas (MFF2) o eSIM integradas, de modo que un usuario malicioso no puede retirar la SIM para usarla en otro equipo. Esto previene un ataque trivial que sería poner la SIM de la baliza en un teléfono o modem para intentar hacerse pasar por ella. Asimismo, la provisión es automática y no expone credenciales al usuario [74]. Cualquier intento de manipular el dispositivo (por ejemplo, desarmarlo para acceder a puertos debug o a la SIM) en teoría invalidaría la certificación y podría activar mecanismos anti-fraude. De hecho, los operadores deben proveer una **"herramienta de gestión de alarmas de fraude"** para detectar usos indebidos y **bloquear automáticamente las comunicaciones** si se sospecha manipulación o abuso [75] [76]. Un caso de abuso podría ser, por ejemplo, múltiples activaciones falsas repetidas de una baliza con el fin de generar alarmas fantasmas; ante eso, el sistema podría anular la SIM o ignorar sus mensajes tras cierto umbral.

- **Privacidad de los datos transmitidos:** Como mencionamos, la baliza **no envía información personal identificable** – ni nombre, ni matrícula, ni número de teléfono [53]. Solo coordenadas e indicador de emergencia. La DGT recibe datos *anónimos* y los utiliza para fines de seguridad vial [54]. Además, la plataforma está sujeta a RGPD y diseñada para **evitar el rastreo individual** [77]. Por ejemplo, cada evento tiene un identificador único distinto del ID de dispositivo, lo que impide correlacionar que el mismo coche tuvo dos incidentes en diferentes días (a ojos de la plataforma serían solo dos eventos independientes anónimos). Los datos se eliminan tras su uso operativo [55]. También es importante destacar que **la baliza no "espía" ni geoposiciona al conductor en condiciones normales**: mientras está apagada permanece completamente inactiva (ni GPS ni radio funcionan). No hay transmisiones periódicas de latidos (*heartbeat*) ni envío de ubicación del vehículo salvo que se active por emergencia [56]. Esto mitiga riesgos de privacidad, ya que no se puede usar la red de balizas para vigilar movimientos de vehículos o construir historiales de localización. Desde el punto de vista del usuario, hasta que uno no pulsa el botón SOS de la baliza, el dispositivo es silencioso.

- **Ataques de *sniffing* y *Man-in-the-Middle*:** Como ya se señaló, pinchar la comunicación inalámbrica directamente es sumamente complicado por el cifrado. Sin embargo, un atacante muy avanzado podría intentar un ataque *MITM* montando una **estación base celular falsa** (*rogue eNodeB*). En LTE, esto no es sencillo ya que existe autenticación mutua SIM-red, pero se han demostrado técnicas en entornos controlados donde un dispositivo IoT se conecta a una

celda impostora que simula ser la red legítima (por ejemplo, publicitando un identificador de red igual al del operador). Si la baliza llegase a asociarse a esta estación falsa, el atacante podría potencialmente recibir sus paquetes UDP. No obstante, tendría que también proporcionar conectividad real o reinyectar las tramas a la red para que la DGT no detecte la desaparición del mensaje. Además, el intruso necesitaría las claves de cifrado o forzar a la baliza a desactivar cifrado (lo cual en LTE estándar no es posible sin que el dispositivo lo rechace). Resumiendo, un **MITM sobre NB-IoT** requeriría equipamiento y conocimientos propios de agencias o investigadores de seguridad muy especializados; **no es un vector al alcance de delincuentes comunes** ni de aficionados. Por otro lado, **sniffing pasivo** (escucha no intrusiva) de NB-IoT podría detectar la portadora y quizá demodular señal con SDR, pero sin las claves solo obtendría bytes cifrados incomprensibles. Incluso identificar qué dispositivo es cuál en aire sería complejo sin conocer IMSIs, etc. Por tanto, es razonable afirmar que **la interceptación clandestina de estas comunicaciones es altamente dificultosa**, más aún que en un móvil convencional, ya que ni siquiera se puede forzar a 2G (NB-IoT no tiene modo inseguro equivalente a GSM). Los estándares de seguridad celular han sido probados en sectores exigentes (financiero, telemedicina) y se confía en ellos también para las balizas [36].

- **Ataques de *spoofing* o suplantación:** Otra categoría es intentar enviar datos falsos a la plataforma DGT haciéndose pasar por una baliza legítima. Aquí, debido a la cadena de confianza, **no cualquiera puede reportar un incidente a DGT 3.0**: solo servidores autenticados con certificado de la DGT pueden hacerlo [27] [28]. Un atacante no puede inyectar directamente un evento en DGT sin haber comprometido primero el servidor del fabricante o su certificado. ¿Y suplantar la baliza hacia el servidor del fabricante? Para ello necesitaría credenciales válidas (la SIM) y conocer el formato exacto de trama. Si, hipotéticamente, lograra clonar la SIM de una baliza (lo cual implica extraerla y romper la seguridad SIM algo nada trivial), podría enviar mensajes a la plataforma del fabricante con el mismo ID de dispositivo. Sin embargo, el fabricante detectaría anomalías (ej. dos ubicaciones distintas simultáneas para un mismo ID, o uso fuera de rango) y además el canal es privado. **Replay attacks** (repetir capturas válidas) también serían difíciles: primero hay que conseguir la captura (cosa no trivial como vimos), y luego reinyectarla en el momento justo. Además, las tramas llevan números de secuencia y *timestamp* [40] [47], lo que podría invalidar reenvíos tardíos (un duplicado podría ser descartado por no seguir la secuencia esperada o un timestamp incoherente). Con todo, un atacante sofisticado que comprometiera la seguridad a nivel de operador o de backend podría generar *spoofing* de alertas. Por ejemplo, si alguien hackease el servidor de un fabricante con credenciales DGT, podría enviar una falsa ubicación. Pero esto ya excede el ámbito del dispositivo V16 y cae en la seguridad de TI del backend, donde se supone que existen certificados y autenticación robusta. En resumen, **la posibilidad de generar alertas falsificadas existe principalmente si se vulneran los sistemas centrales**, no tanto interceptando la radio.

- **Ataques de denegación de servicio (DoS/Jamming):** Un riesgo más tangible es intentar inutilizar la comunicación mediante **inhibición de frecuencias**. Un agresor con un transmisor de interferencias podría, en teoría, **bloquear la banda NB-IoT/LTE-M** localmente, impidiendo que la baliza se conecte. NB-IoT al usar bandas bajas es relativamente resistente, pero un inhibidor suficientemente potente cerca podría anular la señal. Esto sería análogo a bloquear la cobertura móvil en general, algo ilegal pero posible. De igual modo, **interferir el GPS** (spoofing o jamming) es otro vector: enviando señales GPS falsas, se podría engañar a la baliza sobre su ubicación. Un atacante podría intentar que la baliza reportase coordenadas erróneas (p.ej. mediante un *GPS spoofer* hacerle creer que está a 100 km de distancia). Esto requeriría equipamiento de radio GPS especializado, pero hay casos documentados de spoofing de GNSS. No obstante, la repercusión estaría limitada: generaría una incidencia en un lugar incorrecto, que al no encontrar realmente un vehículo averiado, sería descartada por las autoridades al verificarse como falsa alarma. DGT

y los operadores podrían cruzar información (por ejemplo, la cell ID recibida no concuerda con la supuesta latitud) para detectar incoherencias. En cualquier caso, estos ataques de **jamming/ spoofing son posibles pero localizados**, y además afectan por igual a otros sistemas (incluyendo móviles y navegadores de la zona).

En cuanto a **herramientas de análisis para investigadores de seguridad**: usando *Software Defined Radios* (SDR) de rango adecuado (como USRP, HackRF, BladeRF, etc.), es concebible intentar decodificar NB-IoT. Existen implementaciones de código abierto (srsRAN, OpenAirInterface) que soportan NB-IoT a nivel experimental, lo que permitiría a un investigador configurar una "torre" de NB-IoT de laboratorio. Con hardware y conocimientos, se podría *sniffar* la interfaz radio y hasta establecer una *celda señuelo*. Pero reiteramos que, sin las claves SIM, solo se obtendría tráfico cifrado. Un investigador ético podría, por ejemplo, **probar la baliza en un entorno controlado** (con su propia SIM de prueba y eNB privado) para analizar las tramas en claro – algo útil para ver si algún dato sensible se envía sin cifrar a nivel de aplicación. Pero fuera del laboratorio, con las balizas reales en producción, la comunicación está protegida.

Resumen de vectores de ataque: La **superficie de ataque directa sobre la comunicación V16** es limitada gracias al uso de redes celulares seguras y a la simplicidad del dispositivo (no tiene interfaces locales tipo Bluetooth a explotar, salvo en modelos muy concretos que lo usen para apps). Los principales riesgos técnicos podrían venir de: (a) sabotaje de la señal (jamming), (b) intentos de fraude masivo (uso indebido de muchas balizas para saturar el sistema con alertas, aunque habría contramedidas de bloqueo [75]), o (c) brechas en la seguridad de los servidores centrales o APIs. Desde la perspectiva del usuario común, la transmisión de su baliza está **"protegida y blindada"** en gran medida – tal como se anuncia, utiliza redes seguras como NB-IoT/LTE-M similares a las de alarmas y telemedicina [36], y cumple RGPD evitando identificar al conductor. En conclusión, aunque ningún sistema conectado está exento de riesgos, las balizas V16 conectadas implementan un **modelo de seguridad en capas** (cifrado celular, red privada, SIM fija, datos mínimos) que dificulta enormemente las escuchas ilegales o la manipulación externa de las comunicaciones.

Análisis técnico de dispositivos y marcas específicas

Existen numerosas marcas y modelos de balizas V16 conectadas homologadas por la DGT [78], incluyendo tanto dispositivos "independientes" vendidos por fabricantes de accesorios, como versiones distribuidas por las propias operadoras móviles. Técnicamente, **todas deben cumplir la misma norma** (Real Decreto 159/2021 y especificaciones DGT 3.0) en cuanto a luminosidad, autonomía, conectividad y protocolo, por lo que su funcionamiento esencial es equivalente. No obstante, **algunas incorporan características adicionales o diferencias de implementación** dignas de mención para el público técnico:

- **Movistar – Baliza V16 *Fase Light***: Es la baliza oficial asociada a Telefónica. Utiliza **conectividad NB-IoT sobre la red Movistar** (plataforma Kite de Telefónica Tech) [16], con cobertura IoT casi total en España. Su SIM IoT viene operativa hasta enero de 2038 (excediendo el mínimo de 12 años) [79]. Emplea **4 pilas AAA** como alimentación, lo que le da una autonomía destacada de hasta ~2,5 horas de uso continuo [79] (muy por encima de los 30 min requeridos). Esta baliza integra una aplicación móvil llamada **"SOS Alert"** que se conecta vía smartphone, no para la función DGT (que es autónoma), sino para facilitar asistencia en carretera: el usuario puede, mediante la app, **enviar datos de su póliza de seguro y ubicación a la plataforma TIREA** (usada por aseguradoras) [80]. Esto permite agilizar la solicitud de grúa o ayuda mecánica, aprovechando la activación de la baliza como detonante. La baliza en sí se fabrica con materiales reciclados y cuenta con componentes optimizados (su reflector fue desarrollado en la Univ.

Complutense) [81], detalles que muestran colaboración I+D a nivel local. En cuanto a protocolos, Fase Light sigue la norma UDP/IoT estándar. Movistar comercializa este dispositivo a unos 50 € (libre, con descuentos para clientes) [82].

- **Orange – Baliza V16 *SOS Road Connected***: Orange lanzó su propia baliza conectada en 2023, bajo la marca "SOS Road". Inicialmente usaba la **red LTE-M** de Orange [83], pero la versión actualmente en venta (2025) fue actualizada para usar **módulo NB-IoT** en la red de Orange [13], mejorando cobertura en zonas rurales. Se alimenta con **3 pilas AA** alcalinas [84], con servicio de datos incluido hasta diciembre de 2038 [85]. Esta baliza **se distingue por su simplicidad**: **no posee app móvil dedicada** ni Bluetooth [86]. La configuración inicial es tan sencilla como escanear un **código QR** en el envase, el cual permite verificar en una web el estado de la baliza (conexión a red, GPS y batería) [86]. Este método de *diagnóstico vía QR* agiliza comprobar que la baliza está operativa sin requerir instalación de apps. Una vez en uso, simplemente con colocarla en el techo y encenderla, envía la ubicación a DGT cada 100 s [87]. Orange destaca que su baliza tiene una **antena GNSS potente y módulo NB-IoT avanzado** para garantizar la comunicación con DGT incluso en entornos complicados [88]. Su luz LED cubre 360º y alcanza 1 km, y utiliza un imán de neodimio para fijación [89] [90]. La ausencia de funcionalidad extra (como apps de seguro) se compensa con un **uso "plug & play"**: es encender y listo. También es ligeramente más económica en el mercado libre (se ha visto ~40 € online). En resumen, la Orange SOS Road prioriza máxima cobertura (NB-IoT), facilidad de uso y cumple con creces las especificaciones, incluyendo datos hasta 2038 sin coste [91] [92].

- **Vodafone – Baliza V16 *Help Flash IoT***: Fue **la primera baliza conectada homologada** por la DGT, desarrollada por la startup gallega Netun Solutions en conjunto con Vodafone [15]. Opera con **NB-IoT sobre la red de Vodafone** (SIM global preinstalada) [93] [94], asegurando una cobertura muy amplia con pocas zonas sombra (salvo enclaves montañosos extremos) [94]. Usa **4× pilas AAA** y al igual que Movistar, alcanza ~2,5 h de destellos con baterías nuevas [95]. La Help Flash IoT aporta como diferencial la inclusión de **conectividad Bluetooth** y una app móvil llamada **"Incidence"** [96]. Esta app permite a la baliza interactuar con el smartphone del usuario para, por ejemplo, **notificar automáticamente el incidente a aseguradoras como Reale, Mapfre o Axa** [96], agilizando trámites de asistencia. Es un enfoque similar al de Movistar SOS Alert pero con su propia plataforma. El Bluetooth integrado también podría servir para comprobar el estado del dispositivo o actualizar firmware, si fuera necesario, sin quitar la tapa. En cualquier caso, la funcionalidad principal de conexión con DGT 3.0 se realiza independientemente vía NB-IoT, con el Bluetooth como complemento opcional. Esta baliza se comercializa no solo vía Vodafone (en tiendas como El Corte Inglés, Amazon, etc.), siendo muy popular; Vodafone reportó que ya en 2025 se habían vendido **más de 250.000 unidades** de Help Flash IoT en España [97] [15]. Su precio ronda 50 € de lista, aunque con variaciones según promociones. Tecnológicamente, fue un caso de uso exhibido por Vodafone sobre cómo NB-IoT puede mejorar la seguridad vial (se presentó incluso en el Mobile World Congress) [14] [98].

- **Otras marcas destacables:** Además de las anteriores vinculadas a telecos, el mercado ofrece dispositivos de otros fabricantes: por ejemplo, **FlashLED SOS V16**, **Netun *Connected V**Zero***, **Eruvial PF Led One V16**, **Hella V16**, **Osram V16**, **Cegasa/Don Feliz V16** entre muchas. Todas ellas comparten la conectividad IoT (muchas usando módulos Quectel, SimCom u otros con NB-IoT) y garantizan 12 años de servicio. Algunas optan por **baterías recargables** de litio en lugar de pilas desechables – por ejemplo, ciertas balizas incluyen una batería interna recargable por el enchufe mechero del coche, ofreciendo la comodidad de no tener que sustituir pilas. En cualquier caso deben asegurar 30+ min de luz a -10ºC, por lo que la mayoría sigue usando químicas primarias (alcalinas) debido a su fiabilidad y baja autodescarga. En cuanto a **homologación**, todos los modelos pasan por laboratorios designados (IDIADA, LCOE, etc.) que

certifican tanto la parte lumínica (candela, ángulo, IP54, etc.) como la parte de conectividad (se comprueba que cumplen con el protocolo y que tienen el *certificado Telco* de contrato IoT) [99] [9]. Esto nivela bastante las especificaciones técnicas base. Por ello, las diferencias entre marcas residen más en *usabilidad y extras*: unas tienen apps de auxilio, otras no; algunas incluyen funciones añadidas vía app (p.ej. enviar coordenada a contactos de emergencia, como hace la app SOS Alert complementaria) [100]; otras son más básicas. **Ninguna baliza, sin embargo, realiza llamadas de emergencia** ni funciones de comunicación de voz – su propósito se limita a señalizar la presencia y ubicación del vehículo averiado, complementando pero no sustituyendo otros sistemas de emergencia. La **seguridad cibernética** de los distintos modelos en principio es homogénea al estar todas obligadas a usar los mismos canales cifrados y protocolos estándar. Sí podría haber variaciones en cómo cada fabricante implementa su backend y almacena los datos (p.ej. algunos podrían monitorizar el estado de sus dispositivos para mantenimiento proactivo, otros no). Desde una postura neutral, se puede afirmar que **todas las balizas V16 conectadas homologadas comparten un núcleo tecnológico común (NB-IoT/LTE-M, UDP, GPS, 12 años de conectividad)** y cumplen los requisitos legales, diferenciándose principalmente en **comodidades adicionales** (tipo de batería, presencia de app complementaria, materiales, precio).

A modo de resumen comparativo, la siguiente tabla contrasta las características técnicas de tres modelos representativos ligados a operadoras:

Modelo / Marca	Conectividad IoT (Operador)	Alimentación & Autonomía	Funciones Adicionales
Movistar V16 Fase Light	NB-IoT en red Movistar (Telefónica) [16]	4× AAA (< 2.5 h uso) [79]	App móvil “SOS Alert” (vía Bluetooth) para envío de datos a aseguradoras TIREA [80]
Orange SOS Road	NB-IoT en red Orange (antes LTE-M) [13]	3× AA (~2 h estimadas)	Sin app dedicada; configuración por QR web [86]. Envío DGT automático cada 100 s [87].
Vodafone Help Flash IoT	NB-IoT en red Vodafone [94]	4× AAA (~2.5 h uso) [95]	Bluetooth + App “Incidence” para notificar a aseguradoras (Reale, Mapfre, etc.) [96]. Primera baliza homologada.

Nota: A pesar de pequeñas diferencias, todas cumplen con intensidad 40-700 candelas, visibilidad 360º, frecuencia destellos 0.8-2 Hz, IP54, estabilidad 180 Pa, y operación -10ºC a 50ºC [101] [102]. Además, todas garantizan conectividad IoT gratuita hasta al menos 2037-2038 (≥12 años) [8] [91]. Esto asegura que el usuario que adquiera cualquiera de ellas estará cubierto durante la vida útil prevista, sin pagos adicionales.

Conclusión

Las balizas V16 conectadas representan un caso de uso innovador de las tecnologías IoT aplicadas a la seguridad vial. Técnicamente, combinan **hardware sencillo pero robusto** (LED de alta intensidad, GNSS, módulo celular LPWA) con una **infraestructura de comunicaciones sofisticada** (redes NB-IoT/LTE-M, protocolos IoT, plataformas en la nube) para lograr un resultado crítico: alertar rápidamente y de forma anónima la localización de un vehículo inmovilizado, mejorando la prevención de accidentes secundarios. Hemos visto que utilizan estándares abiertos y seguros – respaldados por operadores

móviles – cumpliendo con los requisitos de interoperabilidad europeos. Los protocolos de datos se han diseñado minimizando tráfico pero asegurando la información esencial (100 segundos, coordenadas precisas) [31] [53], y la arquitectura garantiza que la **información llegue donde tiene que llegar**: a la DGT y, por extensión, al resto de conductores y servicios de auxilio. En materia de **ciberseguridad**, las balizas se benefician de la seguridad intrínseca de las redes celulares (cifrado fuerte, SIM autenticada) [72], además de políticas adicionales (SIM sellada, APN privada, anonimización de datos) [17] [55] que las hacen resistentes a ataques convencionales. Si bien siempre habrá algún vector teórico para un adversario muy avanzado (p.ej. jamming o intrusión en backend), el nivel de protección es acorde a su uso público masivo. Para la comunidad técnica (pentesters, ingenieros), las V16 conectadas ejemplifican un **entorno IoT cerrado y crítico**, donde la superficie de ataque se ha reducido intencionalmente y donde cualquier prueba de seguridad debe realizarse con sumo cuidado y posiblemente en entornos controlados (dada la implicación legal de generar falsas alarmas de tráfico).

En última instancia, más allá de debates comparativos con los triángulos físicos, desde un punto de vista neutral y técnico, las balizas V16 conectadas constituyen un **sistema de señalización IoT distribuido** con estándares modernos, capaz de integrarse en la **movilidad conectada** que se está desplegando. Su éxito dependerá no solo de la tecnología, sino también de la adopción correcta por parte de los usuarios (instalación adecuada, mantenimiento de baterías, etc.) y de la robustez operativa de las plataformas DGT 3.0 para manejar potencialmente millones de dispositivos en el futuro. Por ahora, la base técnica parece sólida y orientada a la fiabilidad: hemos pasado de un simple triángulo reflectante estático a una *baliza inteligente* que combina luz, telecomunicaciones y datos en tiempo real para salvar vidas en la carretera.

Fuentes: Las afirmaciones y detalles técnicos se basan en la normativa oficial de la DGT (Real Decreto 159/2021 y Resolución 30/11/2021) [3] [103], en documentación de la plataforma DGT 3.0 [65] [63], en publicaciones de operadores móviles y fabricantes (Vodafone, Orange, Movistar) [94] [83], así como en análisis independientes. Todas las características mencionadas (conectividad NB-IoT/LTE-M, intervalos de 100 s, datos enviados, medidas de seguridad) están respaldadas por dichas fuentes para asegurar la fidelidad y objetividad del artículo.

---

[1] [2] [5] [6] [71] [78] DGT - Dispositivos de preseñalización V16
https://www.dgt.es/muevete-con-seguridad/tecnologia-e-innovacion-en-carretera/Dispositivos-de-presenalizacion-V16/

[3] [10] [18] [19] [20] [21] [22] [23] [24] [25] [27] [28] [29] [30] [31] [33] [35] [38] [39] [40] [41] [42] [43] [44] [45] [46] [47] [48] [49] [50] [51] [52] [61] [62] [73] [76] [103] BOE-A-2021-20433 Resolución de 30 de noviembre de 2021, de la Dirección General de Tráfico, por la que se define el protocolo y el formato para el envío de datos desde la señal V-16 al Punto de Acceso Nacional, en el ámbito de la Directiva 2010/40/UE del Parlamento Europeo y del Consejo, de 7 de julio de 2010, por la que se establece el marco para la implantación de los sistemas de transporte inteligente en el sector del transporte por carretera.
https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-20433

[4] [15] [69] [70] [93] [97] 250,000 IoT beacons light the way to better Spanish road safety | Vodafone IoT
https://iot.vodafone.com/news-and-insights/250-000-iot-beacons-light-the-way-to-better-spanish-road-safety

[7] [11] [12] [13] [16] [58] [59] [60] [64] [79] [80] [81] [82] [84] [85] [86] [92] [94] [95] [96] Estas son las balizas V16 conectadas de Movistar, Orange y Vodafone: guía de compra y comparativa
https://www.xatakamovil.com/guias-de-compra/estas-balizas-v16-conectadas-movistar-orange-vodafone-guia-compra-comparativa

[8] [9] [17] [74] [75] [99] cdn.shopify.com
https://cdn.shopify.com/s/files/1/0918/8786/2086/files/Escrito-Directriz_MOV-2022-03_Proceso-para-la-certificacion-de-senales-V16-conectadas-a-DGT-3_0_Anexo-I.pdf?v=1747216488

14 98 IoT portable traffic emergency light
https://www.vodafone.com/mobile-world-congress-2021/iot-portable-traffic-emergency-light

26 V16 Emergency Beacon with DGT 3.0 Geolocation User Manual
https://manuals.plus/ae/1005008545218777

32 36 53 54 55 56 57 77 Baliza V16 conectada sin cuotas Compra segura
https://herodriver.es/blogs/noticias/es-segura-la-transmision-de-datos-en-las-balizas-conectadas

34 37 63 65 66 67 68 100 101 102 Normativa
https://geobaliza.com/pages/normativa?srsltid=AfmBOooqcKJyucYUzotAm7qFIVjiNG8V6NMstFdrJiARhHzBmOO50Odc

72 What Is IoT Security? Common Challenges and How to Protect Your Devices
https://www.zipitwireless.com/blog/iot-security-what-it-is-its-challenges-and-why-it-matters

83 87 88 89 90 91 Baliza V16 conectada: la tecnología que salva vidas en carretera
https://blog.orange.es/producto/baliza-v16-conectada-dgt-tecnologia-salva-vidas-carretera/