(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 799 425**

(51) Int. CI.:

***H04W 48/18*** (2009.01)
***G08B 25/00*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **20.03.2015 PCT/GB2015/050822**

(87) Fecha y número de publicación internacional: **08.10.2015 WO15150731**

(96) Fecha de presentación y número de la solicitud europea: **20.03.2015 E 15713002 (2)**

(97) Fecha y número de publicación de la concesión europea: **18.03.2020 EP 3127373**

(54) Título: **Itinerancia inalámbrica de dispositivo de alarma**

(30) Prioridad:

**01.04.2014 GB 201405866**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**17.12.2020**

(73) Titular/es:

**CSL (DUALCOM) LIMITED (100.0%)**
**Salamander Quay West Park Lane**
**Harefield, Middlesex UB9 6NZ, GB**

(72) Inventor/es:

**CHANDORKAR, SANTOSH**

(74) Agente/Representante:

**ISERN JARA, Jorge**

## DESCRIPCIÓN

Itinerancia inalámbrica de dispositivo de alarma

Campo técnico

La presente divulgación se refiere a un método y un aparato para proporcionar comunicación a través de una red de radio, y a un dispositivo de alarma dispuesto para comunicarse a través de una red de radio. La presente divulgación se refiere adicionalmente a un método y aparato que proporcionan comunicación a través de la Internet, y un dispositivo de alarma dispuesto para comunicarse a través de la Internet. La presente divulgación se refiere adicionalmente a un servidor de interrogación dispuesto para comunicarse con un dispositivo de alarma a través de una red de radio. La presente divulgación se refiere adicionalmente a un servidor de interrogación dispuesto para comunicarse con un dispositivo de alarma a través de la Internet.

Antecedentes

El documento GB2465833 describe un método y aparato para proporcionar comunicación a través de una red telefónica pública conmutada (PSTN), entre un dispositivo de alarma y un dispositivo remoto tal como una pasarela de alarma, servidor de interrogación o centro de recepción de alarmas. El dispositivo de alarma es del tipo que comunica usando el protocolo de formato rápido multifrecuencia de tono dual (DTMF FF). Un dispositivo de interfaz proporciona tal comunicación comunicándose con el dispositivo de alarma usando un protocolo de DTMF FF, y comunicándose con el dispositivo remoto usando un protocolo de DTMF FF modificado, para superar los problemas cuando se comunica a través de una red telefónica de PSTN.

El documento WO2011/078634 describe un sistema de alarma que puede enviar un evento de alarma a cuatro, así llamados, teléfonos de alarma, que a su vez pueden reenviar el evento a otros cuatro teléfonos de alarma, generando una red de seguridad familiar o de vecindad (SMSecurity Network) con otros teléfonos de alarma. El teléfono de alarma envía eventos de alarma simultáneamente usando TCP/IP (Protocolo de Control de Transmisión/Protocolo de Internet) y ADSL (Línea Digital de Abonado Asimétrica), y usando inalámbricamente redes de telefonía móviles de GSM/SMS/GPRS (Sistema Global para Móviles / Servicio de Mensajes Cortos / Servicio General de Paquetes de Radio) para supervisar estaciones y a los teléfonos móviles de usuarios a través de mensajes SMS. El uso de dichos canales de transmisión garantiza que se notifica a la estación el evento de alarma generado en el sitio protegido. El teléfono de alarma puede autosupervisarse, en el que usuarios reciben eventos de alarma directamente a través de mensajes de texto SMS en sus teléfonos móviles. Un usuario puede interactuar con el teléfono de alarma a través de mensaje de texto SMS, incluyendo armar, desarmar, activar la sirena, comprobar estado, supervisar llamadas, etc. El sistema incluye una función de verificación de alarma por audio, en la que el usuario envía un comando por SMS al teléfono de alarma para que este abra el micrófono, permitiendo al usuario escuchar lo que está sucediendo en el lugar donde se activó la alarma.

Los dispositivos de alarma se usan en instalaciones domésticas, comerciales y otras instalaciones para señalizar una alerta indicativa de que se está cumpliendo una condición de alarma, tal como, por ejemplo, un dispositivo de seguridad provocando una alarma relacionada con un intruso entrando en las instalaciones, o dispositivos médicos, tales como alarmas dispersas o comunicadores personales, en un hospital de residencia de atención residencial provocando una alarma relacionada como un paciente abandonando una sala o una persona presionando un botón de ayuda. Después de señalizar una alerta, los dispositivos de alarma envían un mensaje de alarma a una ubicación remota de modo que puede tomarse una acción apropiada. Algunos dispositivos de alarma existentes se conectan a y forman parte de una red de alarma por la que el dispositivo de alarma puede comunicarse con una ubicación remota, tal como un centro de recepción de alarmas (ARC). Algunos dispositivos de alarma existentes usan la Red Telefónica Pública Conmutada (PSTN) para enviar los mensajes de alarma al ARC remoto que se conecta a la unidad de alarma a través de la PSTN. El ARC, a continuación, toma una acción apropiada, tal como informar a una persona responsable predeterminada, o a la policía, que se ha recibido un mensaje de alarma. La causa de la alerta puede investigarse a continuación.

Algunos dispositivos de alarma no proporcionan información de estado, que es información indicativa del estado de operación (o no operación) del dispositivo de alarma. Un operador de la red de alarma no puede determinar, a continuación, si estos dispositivos de alarma están operando correctamente.

Además, en algunas situaciones, se requiere situar dispositivos de alarma donde no es posible acceder a la PSTN. En algunas situaciones, se requiere que los dispositivos de alarma se puedan mover, por ejemplo un dispositivo de alarma situado dentro de un ascensor, o un dispositivo de alarma adaptado en una pieza grande de maquinaria movible tal como una excavadora o volquete, o un dispositivo de alarma que se coloca en diferentes ubicaciones dentro de un edificio.

Por lo tanto, se necesitan técnicas alternativas de comunicación de mensajes de alarma desde estos dispositivos de alarma a la ubicación remota. Una opción es usar una red telefónica celular. Sin embargo, tales redes no son lo suficientemente fiables para aplicaciones de seguridad tales como en las que es imperativo que exista una conexión fiable entre el dispositivo y la ubicación remota para la transmisión de mensajes de alarma y otra información de

estado.

Realizaciones de la presente divulgación buscan abordar estos problemas.

Sumario

Una invención se define en las reivindicaciones adjuntas.

También se divulga en este documento un método de operación de un dispositivo de alarma dispuesto para transmitir una señal de alarma indicativa de que se ha cumplido una condición de alarma, comprendiendo el método las etapas del dispositivo: acceder a un registro de una lista de redes celulares disponibles para el dispositivo para comunicación con las mismas, comprendiendo el registro información que identifica cada una de las redes y una medida de la fiabilidad de comunicación a través de cada red; seleccionar una red con la que establecer un enlace de comunicación basándose en la medida de la fiabilidad de comunicación a través de la red; e intentar establecer un enlace de comunicaciones con la red seleccionada.

El método puede comprender una etapa del dispositivo que efectúa un sondeo de redes celulares disponibles para la comunicación de dispositivo con las mismas para rellenar la lista con la información contenida en las mismas.

El sondeo puede efectuarse en el encendido del dispositivo, en respuesta a una señal recibida en el dispositivo desde una ubicación remota, en una planificación predeterminada o en respuesta a una entrada manual en el dispositivo desde un usuario.

La determinación puede basarse en una medida actualizada de la fiabilidad de comunicación a través de la red a la que el dispositivo ha establecido un enlace de comunicaciones, la medida actualizada obtenida durante la comunicación a través de ese enlace establecido.

La determinación puede basarse en la determinación de que un número predeterminado de medidas actualizadas están por debajo del nivel predeterminado.

La comunicación a través del enlace establecido por el que se obtiene la medida actualizada puede comprender el dispositivo enviando una señal de interrogación periódica desde el dispositivo a una ubicación remota y el dispositivo recibiendo desde la ubicación remota una señal de toma de contacto indicativa de que se ha recibido la señal de interrogación en la ubicación remota.

El método puede comprender, tras no recibir una toma de contacto esperada, finalizar el enlace establecido y seleccionar otra red a la que conectarse, siendo esa otra red la red para la que la medida de la fiabilidad de comunicación es la siguiente más alta.

El método puede comprender, después de que el dispositivo ha establecido un enlace de comunicaciones a través de una red que no es una red preferida predeterminada, finalizar periódicamente ese enlace e intentar establecer un enlace a través de la red preferida si la medida de fiabilidad de comunicación a través de esa red preferida es mayor que un nivel predeterminado.

Después de finalizar en enlace, el dispositivo puede intentar conectarse a la red preferida predeterminada si la medida de fiabilidad de comunicación a través de esa red preferida es mayor que un nivel predeterminado.

El dispositivo puede hacer no más de un número predeterminado de intentos repetidos para conectarse a la red seleccionada si fallan los intentos anteriores para conectarse a la red seleccionada. En un ejemplo se proporciona un método que comprende la etapa posterior de seleccionar otra red a la que conectarse basándose en la medida de la fiabilidad de comunicación a través de la red, e intentar establecer un enlace de comunicaciones con esta otra red seleccionada.

Después de finalizar un enlace de comunicaciones a través de una red, el dispositivo puede actuar en una señal que tiene que bloquearse en una red particular intentando establecer un enlace de comunicaciones con esa red y puede no intentar establecer un enlace de comunicaciones con otra red al menos hasta que se recibe una señal contraria.

El dispositivo puede comprender una SIM de itinerancia.

También se divulga en este documento un dispositivo de alarma según se define por cualquiera de los métodos anteriores.

En un ejemplo se proporciona un dispositivo de alarma dispuesto para acoplarse a un dispositivo de generación de señales de alarma para recibir una señal de alarma desde el mismo y para comunicar la señal de alarma a través de una red celular con la que el dispositivo de alarma ha establecido un enlace de comunicaciones.

También se divulga en este documento un medio legible por ordenador que comprende porciones de código ejecutables por medios de procesamiento de un dispositivo de alarma para provocar que ese dispositivo efectúe un método de acuerdo con cualquiera de los métodos anteriores.

Breve descripción de los dibujos

Realizaciones específicas de la divulgación se describen ahora a continuación a modo de ejemplo únicamente y con referencia a los dibujos adjuntos. Las realizaciones específicas se describen con referencia a un dispositivo de alarma que, en esta realización, es una alarma antirrobo instalada en instalaciones domésticas.

Sin embargo, el experto apreciará que las realizaciones descritas son adecuadas para su uso como otros tipos de dispositivo de alarma, incluyendo dispositivos de alarma médicos tales como alarmas dispersas, comunicadores personales y, de hecho, a cualquier dispositivo de comunicación que se usará para provocar una alarma, por ejemplo. Una alarma dispersa es un dispositivo de alarma que únicamente requiere potencia y una línea telefónica, eliminando la necesidad de un sistema de red por cable o fijo. Es común en muchas situaciones de esquemas de alojamiento protegido o agrupado. Se muestran las realizaciones específicas, en las que:

La Figura 1a muestra un diagrama esquemático de un sistema de señalización de alarma en el que operan dispositivos y métodos de la presente divulgación.

La Figura 1b muestra un diagrama esquemático de realizaciones específicas de dispositivos y métodos de la presente divulgación, dentro del sistema de señalización de alarma como se muestra en la Figura 1.

La Figura 2a muestra un diagrama esquemático de un gestor de conexiones dentro del sistema mostrado en la Figura 1a y la Figura 1b.

La Figura 2b muestra un diagrama esquemático de una realización específica de un gestor de conexiones dentro del sistema mostrado en la Figura 1b.

La Figura 3a muestra un diagrama esquemático de un gestor de impulsos dentro del sistema mostrado en la Figura 1a y la Figura 1b.

La Figura 3b muestra un diagrama esquemático de una realización específica de un gestor de impulsos dentro del sistema mostrado en la Figura 1b.

La Figura 4 muestra un diagrama esquemático de un dispositivo de alarma dentro del sistema mostrado en la Figura 1a y la Figura 1b.

La Figura 5 muestra las etapas de método asociadas con conexión de red dentro del sistema mostrado en la Figura 1b.

La Figura 6 muestra las etapas de método asociadas con conectividad y funcionalidad de comprobación de salud dentro del sistema mostrado en la Figura 1b.

La Figura 7 muestra las etapas de método asociadas con la determinación de idoneidad de red dentro del sistema mostrado en la Figura 1b.

La Figura 8 muestra las etapas de método asociadas con sondeo de red dentro del sistema mostrado en la Figura 1b.

La Figura 9 muestra las etapas de método asociadas con el establecimiento de una conexión de datos dentro del sistema mostrado en la Figura 1b.

La Figura 10 muestra las etapas de método asociadas con la realización de una toma de contacto de estado más transmisión/distribución de alarma y las etapas de método asociadas con el restablecimiento de conexión de datos, dentro del sistema mostrado en la Figura 1b.

La Figura 11 muestra una tabla de valores de RSSI ilustrativos como una función de conectividad de red.

Descripción específica de ciertas realizaciones ilustrativas

La Figura 1a muestra un diagrama esquemático de un sistema de señalización de alarma en el que operan dispositivos y métodos de la presente divulgación. En una realización de la presente divulgación un dispositivo de alarma (10) se dispone para operación en el sistema de señalización de alarma (1), y que hace uso de la Internet (40). En una realización adicional de la presente divulgación un dispositivo de alarma (10) se dispone para operación en el sistema de señalización de alarma (1), y que hace uso una red de radio (30). En una realización adicional de la presente

divulgación un dispositivo de alarma (10) se dispone para operación en el sistema de señalización de alarma (1), y que hace uso de una Red Telefónica Pública Conmutada (PSTN) (20).

Dentro del sistema de señalización de alarma mostrado en la Figura 1a existen a continuación un número de diferentes rutas que se usan para conectarse a un servidor de interrogación (60, 62), en el que el servidor de interrogación (60, 62) es un servidor al que se envían alarmas, llamadas de interrogación y metadatos desde el dispositivo de alarma (10).

Las rutas que se utilizan para conectarse a un servidor, desde un dispositivo embebido, son como se indican a continuación:

Trayectorias de GPRS/3G/4G

1. Dispositivo de alarma (10) -> enlace de radio (44) - GPRS/3G/4G -> Internet (40) -> Servidor de interrogación (60, 62)
2. Dispositivo de alarma (10) -> "APN privado" -> Servidor de interrogación (60, 62)
Un Nombre de Punto de Acceso es el nombre de una pasarela entre un dispositivo móvil de GPRS, 3G o 4G y otro dispositivo o red informática, que puede ser la Internet. Un dispositivo móvil que hace conexión de datos se configura con un APN que se presenta a un operador de red y se usa para determinar qué tipo de conexión de red debería crearse. Las rutas en los puntos 1 y 2 son similares, excepto que para la ruta 2 los datos transmitidos desde el dispositivo de alarma (10), tal como los enviados desde una tarjeta SIM, alcanzan servidores de interrogación (60, 62) sin alcanzar la Internet (40). El APN privado en el punto 2 se representa, por lo tanto, en la Figura 1a por el enlace de radio (35) y la red de radio (30). Sin embargo, en algunas realizaciones el enlace de radio (44) constituye el enlace de radio (35) y la red de radio (30).

Trayectoria de Red de Área Local (LAN)
3. Dispositivo de alarma (10) -> LAN (42) -> Internet (40) -> Servidor de interrogación (60, 62).

Trayectoria de PSTN
4. Dispositivo de alarma (10) -> red de PSTN (20) -> Pasarela de alarma (70) -> Servidor (60, 62).

Por simplicidad, el sistema de señalización de alarma (1) mostrado en la Figura 1a se describirán ahora con referencia a la realización de la presente divulgación que hace uso de la Internet (40), que se muestra en la Figura 1b. Sin embargo, se entenderá que la realización mostrada en la Figura 1b comprende métodos y dispositivos que tienen aplicabilidad en los métodos y dispositivos de las otras realizaciones de la presente divulgación como se muestra en la Figura 1a que hacen uso de una red de radio (30) sin usar la Internet (40), o al menos parte de una PSTN (20). Haciendo referencia a la Figura 1a, el experto apreciará que en realizaciones específicas la conexión a la Internet (40) puede ser a través de una conexión inalámbrica y, por lo tanto, en tales realizaciones específicas el sistema de señalización de alarma (1) también hace uso de una red de radio (30) para proporcionar acceso a la Internet (40).

Haciendo referencia a la realización mostrada en la Figura 1b, el sistema de señalización de alarma (1) comprende además un centro de recepción de alarmas (ARC) (50) y un centro de operaciones (80). En la Figura 1a únicamente se muestran un único dispositivo de alarma (10) y un único ARC (50), sin embargo se entenderá que un sistema de señalización de alarma (1) de este tipo podría incluir cualquier número de dispositivos de alarma (10) y podría incluir más de un ARC (50).

Continuando con la realización mostrada en la Figura 1b, el dispositivo de alarma (10) se dispone para enviar mensajes de alarma indicativos de una alerta de alarma en las instalaciones de un usuario (no mostradas) significando que ha sucedido algo para desencadenar la alarma, en la que el dispositivo de alarma (10) se instala o coloca, en un ARC (50), a través de una conexión de comunicación proporcionada por la Internet (40). El dispositivo de alarma (10) también puede disponerse para enviar mensajes de alarma a un ARC (50) a través del APN privado. El dispositivo de alarma (10) se dispone para enviar y recibir datos de servicio general de paquetes de radio (GPRS) a través de un operador de red 2G/3G/4G, tal como Vodafone UK, para transmisión y recepción a través de la Internet (40). Tal comunicación inalámbrica a y desde el dispositivo de alarma (10) se denomina en lo sucesivo "enlace de radio (44)" y, por lo tanto, como se ha analizado anteriormente el término enlace de radio (44) incluye la presencia de una red de radio (30), mantenida por uno o más operadores de red, para proporcionar conectividad a la Internet (40). Sin embargo el experto apreciaría que puede utilizarse otra comunicación inalámbrica. Por ejemplo, en otras realizaciones, el dispositivo de alarma (10) se dispone para enviar y recibir datos de sistema global para móviles (GSM). En otras realizaciones, el dispositivo de alarma (10) se dispone para enviar y recibir datos a través de una red de área local (42), tal como una red de área extensa, o bien a través de comunicación inalámbrica o bien alámbrica.

Continuando con la realización mostrada en la Figura 1b, el dispositivo de alarma (10) opera como un dispositivo de alarma autónomo (10) significando que es un dispositivo de alarma autosuficiente; sin embargo el dispositivo de alarma (10) tiene una interfaz de entrada/salida (413) para conexión a periféricos externos (450), que incluye un dispositivo de alarma adicional (450) (interfaz (413) y periféricos (450) no se muestran en la Figura 1b, pero se muestran en la Figura 4 analizada a continuación). El dispositivo de alarma adicional (450), al que tiene que conectase el dispositivo

de alarma (10), por ejemplo podría ser un sistema de alarma existente situado dentro de un edificio, pero que no tiene la funcionalidad de comunicación requerida. Por ejemplo, el dispositivo de alarma adicional (450) podría situarse de tal forma que no puede acceder a una PSTN, o el dispositivo de alarma adicional (450) podría montarse en una plataforma movible. Por lo tanto, retroadaptar el dispositivo de alarma (10) al dispositivo de alarma adicional habilita que mensajes de alarma se envíen desde el dispositivo de alarma adicional (450) a un ARC (50) a través de una conexión de comunicación proporcionada por la Internet (40). La conexión entre el dispositivo de alarma (10) y el dispositivo de alarma adicional (450) es mediante un cable corto, de un metro aproximado de longitud, pero en cualquier caso lo suficientemente largo para conectar los dos dispositivos que se sitúan normalmente cerca entre sí en una única sala. La interfaz de entrada/salida (413) en el dispositivo de alarma (10) es compatible con protocolos de comunicación comúnmente usados como se usan por equipo, tal como por ejemplo RS232 y RS485. Por consiguiente, en una situación de este tipo tanto el dispositivo de alarma (10) como el dispositivo de alarma adicional (450) son capaces de conectarse a y comunicarse a través de la Internet (40).

Continuando con el dispositivo de alarma autónomo (10) mostrado en la Figura 1b, el dispositivo de alarma (10) tiene un conjunto de sensores (419) que incluye un detector de movimiento, un acelerómetro, un sensor de temperatura, un detector de humo, un detector de monóxido de carbono y un sensor de GPS (el conjunto de sensores (419) no se muestra en la Figura 1b, pero se muestra en la Figura 4 analizada a continuación). El conjunto de sensores (419) se usa para determinar si se ha cumplido una condición de alarma, por ejemplo si se ha detectado movimiento y/o, por ejemplo, que se han recopilado datos indicativos de que hay un incendio en la vecindad. El experto apreciará que cambios en otros fenómenos físicos pueden conducir a que se cumpla una condición de alarma, y que el conjunto de sensores (419) puede contener cualquier sensor apropiado que puede usarse para determinar cuándo se ha cumplido una condición de alarma. Cuando la condición de alarma se ha cumplido, el dispositivo de alarma (10) se dispone para enviar un mensaje de alarma a través de la Internet al ARC (50), en la que se hace uso de VPN IPSEC/enlace de arrendado y trayectorias de X.25. VPN IPSEC es una red privada encriptada, usada para transmitir datos encriptados a través de la Internet. Enlace arrendado es una línea telefónica especializada que tiene mayor disponibilidad y garantía de conectividad. X.25 es un conjunto de protocolos usados para redes de área extensa, es el procesador de IP, y algunas infraestructuras de seguridad aún usan esta trayectoria de comunicación.

Existe una necesidad de informar periódicamente al ARC (50) de que el dispositivo de alarma (10) y su conexión a la Internet están operando correctamente. Una confirmación periódica de este tipo de que el dispositivo de alarma (10) está operando correctamente y está conectado correctamente a la Internet (40) es deseable ya que es posible que un dispositivo de alarma (10) podría fallar en cualquier momento por un número de razones, tales como, por ejemplo, eliminándose la potencia deliberadamente por un supuesto intruso, un fallo en la conexión a la Internet (40), o simplemente debido a un mal funcionamiento. Sin embargo, también existe una necesidad de separar un fallo en el dispositivo de alarma (10), tal como mal funcionamiento del dispositivo de alarma (10), de un fallo en la conexión a la Internet (40). Si el fallo es en la comunicación con la Internet (40), no en el dispositivo de alarma (10), existe una necesidad de minimizar la posibilidad de que se provoque una alarma falsa indicando que el dispositivo de alarma (10) ha fallado. Puede ser caro o inconveniente ocuparse de una falsa alarma de este tipo de ya que puede implicar, por ejemplo, llamar a la policía. Los métodos y dispositivos de la presente divulgación proporcionan una solución a este problema. En otras realizaciones, como se apreciaría por el experto, en un escenario tanto de seguridad como de telesalud, los métodos y dispositivos de la presente divulgación mitigan falsas alarmas cuando se producen pérdida de conectividad de corta duración.

El dispositivo de alarma (10) actúa para generar información con respecto a alarmas, estado de dispositivo y/o mensajes de prueba relacionados con el dispositivo de alarma (10). En una realización alternativa, en la que el dispositivo de alarma (10) se retroadapta en un dispositivo de alarma adicional (450), el dispositivo de alarma (10) también se dispone para recibir información con respecto a alarmas, información de estado con respecto a un dispositivo de alarma adicional (450) y/o mensajes de prueba desde y relacionados con el dispositivo de alarma adicional (450). El dispositivo de alarma (10) proporciona adicionalmente funcionalidad de interrogación que habilita la generación y transmisión de 'latidos' periódicos y datos accionados por evento, como se analiza ahora. Datos interrogados pueden usarse para determinar detección de pérdida de datos del dispositivo de alarma (10), y para determinar la integridad de la conexión a la Internet (40), por ejemplo cuando el dispositivo de alarma (10) pierde conectividad con la Internet (40), en el que la pérdida de conectividad se determina contando las llamadas de interrogación perdidas. Después de un cierto número de llamadas de interrogación perdidas el servidor de interrogación (60) generará una alarma al ARC (50) indicando un "fallo de interrogación". La forma en que el servidor está detectando las llamadas de interrogación perdidas es estimando la cantidad de interrogaciones esperadas desde el dispositivo de alarma (10) en un cierto lapso de tiempo. El número de interrogaciones generadas por el dispositivo de alarma (10) en un cierto lapso de tiempo, en otras palabras la frecuencia de interrogaciones, para dispositivos de seguridad depende del grado de la unidad. A medida que el grado aumenta, desde el Nivel 0 al Nivel 4 relacionado con un aumento en requisitos de seguridad, existe un aumento asociado en la frecuencia de interrogación. En algunas realizaciones el aumento en frecuencia de interrogación es proporcional al grado de la unidad (Nivel 0 a Nivel 4). En otras realizaciones, el experto apreciará que otros dispositivos, tales como dispositivos médicos, tienen tiempos diferentes, o frecuencias de interrogación, dependiendo de los requisitos específicos para el dispositivo. El servidor de interrogación (60) también genera una alarma al ARC (50) si se detecta un corte de potencia en un área geográfica dentro de la que se ubica el dispositivo de alarma (10), que se determina o bien a través de la entrada de un operador o desde una determinación de que unidades vecinas geográficamente están fallando como se ha analizado

anteriormente con respecto a determinación de un "fallo de interrogación" para el dispositivo de alarma (10).

Continuando con la realización mostrada en la Figura 1b, la información apropiada viaja desde el dispositivo de alarma (10) a la Internet (40) a través de un enlace de radio (44). La información viaja a través de la Internet (40). La información que emerge en lado lejano de la Internet (40) se envía a través de una línea telefónica (25) a un dispositivo directamente conectado a la línea telefónica (25) o a un dispositivo que está adicionalmente aguas abajo y puede conectarse a través de otras tecnologías de transmisión. El dispositivo al que se envía información depende del destino final, según se determina por el dispositivo de alarma (10). El destino final puede ser uno de un servidor de interrogación primario (60) o servidor de interrogación secundario (62), un centro de recepción de alarmas (50) o un centro de operaciones (80). Esto significa que información que emerge en el lado lejano de la Internet (40) se envía a través de línea telefónica (25) al servidor de interrogación primario (60) como el destino final, o pasa a través del servidor de interrogación primario (60) y se envía a través de un enlace de radio X.25 (65) al ARC (50) como el destino final, o pasa a través del servidor de interrogación primario (60) y se envía a través de un enlace de radio X.25 al centro de operaciones (80) como el destino final.

En el caso de que el ARC (50) sea el destino para la información, y siendo la información un mensaje de alarma, el ARC (50) observa el mensaje de alarma e informa a una persona responsable apropiada que es capaz de investigar a continuación las instalaciones en las que se instala el dispositivo de alarma (10) y dispositivo de alarma. En el caso de que el servidor de interrogación primario (60) sea el destino para la información, y siendo la información un mensaje de alarma, el servidor de interrogación primario (60) reenvía la información a través del enlace X.25 (65) al ARC (50). En el caso de que el centro de operaciones (80) sea el destino para la información, y sea la información un mensaje de alarma, el centro de operaciones (80) reenvía la información a través de un enlace X.25 (65) al servidor de interrogación primario (60) que a continuación reenvía la información a través del enlace X.25 (65) al ARC (50). En otras realizaciones el centro de operaciones (80) está en contacto de comunicación directa con el ARC (50), y en otras realizaciones el centro de operaciones (80) actúa como un ARC y directamente informa a la persona responsable apropiada. Continuando con la realización mostrada en la Figura 1b, incluso cuando el ARC (50) no se indica como el destino final para la información encaminada, porque la información se reenvía al ARC (50), el ARC puede aún informar a la persona responsable apropiada para que puedan tomar una acción.

Cada servidor de interrogación (60, 62) se dispone para supervisar mensajes de interrogación e inferir un mal funcionamiento del dispositivo de alarma (10) y/o su conexión de enlace de radio (44) a la Internet (40) si mensajes de interrogación no se reciben regularmente y, en este caso, para generar al menos un "mensaje de fallo de interrogación". En algunas realizaciones, cada servidor de interrogación (60, 62) puede reenviar o enviar otros tipos de mensajes además de o en lugar de mensajes de fallo de interrogación, por ejemplo alarmas.

Cada servidor de interrogación se conecta a y dispone para generar y reenviar mensajes de fallo de interrogación a la Internet (40) para distribuir a un teléfono móvil (90) del usuario a través del enlace de radio (95).
Cada servidor de interrogación se dispone adicionalmente para generar y reenviar mensajes de fallo de interrogación al ARC (50), y/o al centro de operaciones (80) a través del enlace de radio X.25 (65).

Los mensajes de alarma que están destinados para el teléfono móvil de un usuario se distribuyen a través de Protocolo de Internet al servidor de interrogación (60) y el servidor de interrogación (60) usa la infraestructura de SMS para distribuir el mensaje al teléfono (90) del usuario. Esto permite la supervisión del estado de SMS (fallo, entregado, pendiente). En otras realizaciones, los mensajes de alarma se envían directamente desde el dispositivo de alarma (10) al teléfono móvil (90) del usuario usando la infraestructura de SMS de GSM existente, sin embargo la supervisión del estado de SMS no es tan buena como la proporcionada cuando el mensaje de alarma se distribuye a través del servidor de interrogación (60).

La Figura 2a muestra un diagrama esquemático de un gestor de conexiones (2) dentro del sistema de señalización de alarma (1) mostrado en la Figura 1a y la Figura 1b; como se describe a continuación el gestor de conexiones es un algoritmo almacenado en memoria dentro del dispositivo de alarma (10) y, por lo tanto, el gestor de conexiones (2) no está físicamente como se muestra en las Figuras 2a y 2b, con el gestor de conexiones (2) en las Figuras 2a y 2b que sirve como una representación de la funcionalidad del gestor de conexiones (2) con respecto a partes del sistema de señalización de alarma. El gestor de conexiones (2) habilita la transmisión y recepción fiables de datos entre el dispositivo de alarma (10) y la Internet (40). El gestor de conexiones (2) opera para garantizar la integridad y características de rendimiento óptimas de la conexión de enlace de radio (44) entre el dispositivo de alarma (10) y la Internet (40) a través de una red de radio (30). En otra realización el gestor de conexiones (2) opera para garantizar la integridad y características de rendimiento óptimas de la conexión de LAN (42) entre el dispositivo de alarma (10) y la Internet (40). Esto puede entenderse a través de los ejemplos analizados a continuación.

Por simplicidad, el gestor de conexiones (2) mostrado en la Figura 2a se describirán ahora con referencia a la realización de la presente divulgación que hace uso de la Internet (40), que se muestra en la Figura 2b. Sin embargo, se entenderá que la realización mostrada en la Figura 2b comprende métodos y dispositivos que tienen aplicabilidad en los métodos y dispositivos de las otras realizaciones de la presente divulgación como se muestra en las Figuras 1a y 2a.

Haciendo referencia a la Figura 2b, la operación del gestor de conexiones (2) se describirá ahora con respecto a la realización de la presente divulgación en la que el dispositivo de alarma (10) se conecta a la Internet (40) a través del enlace de radio (44). El gestor de conexiones (2) habilita que se transmitan datos de forma fiable a y desde el dispositivo de alarma (10) y la Internet (40) a través del enlace de radio (44), y como tal el experto entenderá el gestor de conexiones (2) habilita la transmisión y recepción fiables de datos a través de una red celular (30) mantenida por uno o más operadores de red. El gestor de conexiones (2) proporciona la siguiente funcionalidad: habilita que dispositivos de alarma (10) se desplieguen en cualquier país, y se conecta a 'itinerancia' a través de proveedores de red según se requiera; resuelve problemas de conectividad multicapa (orientación, registro de datos, emisiones de señales, tasa de errores de bits (BER), recuperación desde un mantenimiento de estación e interferencia); evita "comportamiento agresivo" cuando existe una pérdida de conectividad; proporciona criterios objetivos relacionados con la decisión de realizar itinerancia a otras redes (30); y el propio gestor de conexiones (2) proporciona sintonización óptima de su funcionalidad.

El gestor de conexiones (2) habilita que el dispositivo de alarma (10), que se conecta a la Internet (40) a través del enlace de radio (44) a través de un operador de red, tal como Vodafone UK, a través de la red de radio (30), realice itinerancia de forma eficiente para distribuir y recibir datos independientemente del país y operadores de red. El gestor de conexiones (2) habilita que el dispositivo de alarma (10) se beneficie de una tarjeta de Módulo de Identidad de Abonado (SIM) de itinerancia, tal como la GDSP de Vodafone. Una SIM de itinerancia puede definirse como, por ejemplo, una tarjeta SIM de teléfono móvil que puede operar en más de una red.

Existe un problema en la forma en que la itinerancia funciona automáticamente, que se resuelve por métodos y dispositivos de la presente divulgación. Este problema, y sus repercusiones, se analizan ahora. Un usuario habitualmente tendrá un acuerdo con un operador de red doméstico particular. El operador de red doméstico mantendrá por sí mismo a continuación habitualmente una lista de operadores de red, que tienen un acuerdo de itinerancia con el operador de red doméstico. La lista de operadores de red se prioriza a continuación para proporcionar una lista preferida de operadores de red, con la lista preferida de operadores de red ordenada en sí misma sobre la base de preferencia, de tal forma que si la conexión con la red doméstica falla, se intenta un registro, y proporciona conexión, con una red, en el orden de la lista priorizada de operadores de red preferidos. Esto significa que un operador de red, que, por ejemplo, proporciona la señal más intensa de los operadores de red disponibles en un área en un momento particular, es improbable que se elija a menos que esté en la parte superior o hacia la parte superior de la lista priorizada de operadores de red preferidos. Únicamente cuando todos los operadores preferidos no están disponibles en un área dada, por ejemplo cuando no hay cobertura, se intenta un registro, y conexión proporcionada, con el operador de red proporcionando la señal más intensa de entre los otros operadores de red distintos de operadores de red preferidos dentro de la lista de operadores de red. Itinerancia automática, como se ha analizado anteriormente, proporcionada a través de, por ejemplo, un algoritmo de selección de operador automático (AT+COPS=0, donde 'AT+COPS' es un comando establecido que fuerza un intento para seleccionar y registrar el operador de red de GSM y cuando se establece a '0' indica que tal selección tiene que realizarse automáticamente), se encuentra habitualmente en la mayoría de teléfonos móviles y módulos de radio, proporciona una solución viable para la mayoría de aplicaciones no críticas, por ejemplo voz y navegación web.

Sin embargo, para aplicaciones críticas, como se requiere dentro de un sistema de señalización de alarma (1) u otras aplicaciones de seguridad, en las que la integridad de señal es crítica, se requiere una solución para asegurar la integridad de señal y de conectividad. Limitaciones a superar, o al menos mitigar, en relación con itinerancia automática existente incluyen:

- El operador preferido puede no proporcionar la mejor intensidad de señal para un área dada y un operador no preferido puede ser la mejor alternativa. Una medida de intensidad de señal con una red de radio (30) es la Calidad de Señal de Célula (CSQ). La CSQ representa una indicación de la intensidad de señal de recibida (0-31) desde la estación base con la señal más intensa en una red particular (30). Una CSQ baja introduce problemas de comunicación de datos y de conexión tanto en datos de GSM como datos de GPRS.
- El operador preferido puede no proporcionar una señal con la mejor señal a ruido (S/N) para un área dada, y un operador no preferido puede ser la mejor alternativa. Una señal podría tener una CSQ relativamente alta pero tener una S/N relativamente baja, introduciendo de nuevo problemas de conexión de comunicación de datos tanto en datos de GSM y datos de GPRS.
- El operador preferido puede no proporcionar una señal con una tasa de errores de bits aceptable. En transmisión digital, el número de errores de bits es el número de bits recibidos de un flujo de datos a través de un canal de comunicación que se han alterado debido a ruido, interferencia, distorsión o errores de sincronización de bits. La tasa de errores de bits (BER) es el número de errores de bits dividido por el número total de bits transferidos durante un intervalo de tiempo. BER es por lo tanto una medición de rendimiento, y puede usarse para determinar la aceptabilidad de una red particular como debería apreciarse por el experto.

    ◦ El experto apreciará que S/N y BER pueden no ser muy dependientes del proveedor de red. Por ejemplo, una S/N baja o mala o BER inaceptable o mala también puede provocarse por un gran motor, generador o fuente de alimentación ruidosa que podría ubicarse en edificios particulares en la ubicación. Por lo tanto, el experto apreciará que es posible que S/N o BER mala puede provocarse por la topología. Por ejemplo, entre la estación base y el dispositivo existen edificios que no están presentes cuando se conectan a la estación base de otra

red que está colocada en una ubicación diferente.

- Mantenimiento o interferencia de estación base a menudo resulta en comportamiento inesperado del algoritmo de selección automática. Una interferencia de teléfono móvil es un instrumento usado para evitar un dispositivo móvil se comunique con estaciones base. Hace esto comunicando en la misma frecuencia que el dispositivo, creando colisiones que corrompen todas las comunicaciones.
- Un atributo de una red de radio particular (30) es el 'número de células' dentro de esa red (30), en la que, por ejemplo, cada célula podría habilitar 15 conexiones de enlace regular a la red (30), por ejemplo, habilitando cada célula 15 teléfonos celulares o móviles para conectarse a la red. Una red (30) con un número bajo de células puede conducir, por lo tanto, a problemas de conectividad durante periodos ocupados. El operador preferido puede ser un operador con una red (30) que ofrece un número tan bajo de células, que puede ser problemático cuando es crítico mantener la integridad de conexión como se requiere para sistemas de alarma.
- Algoritmos de selección automáticos no tienen en cuenta las SIM de itinerancia pura, donde "SIM de itinerancia pura" significa una SIM que siempre realizará itinerancia en el país en el que se despliega el dispositivo.
- Con itinerancia automática, el control es mínimo para el dispositivo anfitrión, resultando en rendimiento de itinerancia malo, que está menos adaptado a la aplicación.

Estos problemas y limitaciones se resuelven por los métodos y dispositivos de la presente divulgación, en los que el gestor de conexiones (2) habilita: itinerancia a través de redes de radio (30); conexión a operadores de red distintos al operador u operadores de red en una lista de operadores de red preferidos; conexión a operadores de red basándose en intensidad de señal, éxito de comunicación, señal a ruido, número de células; preferencia de usuarios. Haciendo referencia de vuelta a la Figura 2b, y con referencia a la Figura 4 que muestra el dispositivo de alarma (10) en más detalle, el dispositivo de alarma (10) tiene un módulo de radio (403) y SIM de itinerancia asociada (405), y el dispositivo de alarma (10) tiene una radio antena (407) conectada al módulo de radio (403), para transmitir y recibir datos de GPRS. El dispositivo de alarma (10) tiene un microcontrolador (401) que tiene la memoria (402) que incluye memoria flash y memoria no volátil. El microcontrolador (401) se conecta al módulo de radio (403) y procesa datos para transmisión por el módulo de radio (403) a través de la antena (407), y procesa datos recibidos por el módulo de radio (403) a través de la antena (407). El microcontrolador (401) controla el módulo de radio (403) en relación con tal transmisión y recepción de datos, y el microcontrolador (401) a través de la SIM de itinerancia (405) dentro del módulo de radio (403) controla el enlace de radio (44). Esto significa que el microcontrolador (401) controla y determina qué red (30) el dispositivo de alarma (10) se conecta, para la transmisión y recepción de datos a través de la Internet (40). El gestor de conexiones (2) es un algoritmo mantenido en la memoria (402), que cuando se ejecutan en el microcontrolador (401) habilita la transmisión y recepción fiables de datos entre el dispositivo de alarma (10) y la Internet (40).

El módulo de radio (403) tiene funcionalidad de sondeo proporcionada por Telit Comunicaciones S.p.A aunque el experto entenderá que puede usarse una funcionalidad de sondeo distinta de la proporcionada por Telet. La funcionalidad de sondeo es una herramienta de diagnóstico para proporcionar información en las redes de radio disponibles (30) en la ubicación. El microcontrolador (401) ordena al módulo de radio (403) que efectúe un sondeo. El módulo de radio (403) a través de la antena (407) explora el área y guarda datos del sondeo en una tabla de redes (404), con la tabla de redes (404) y datos asociados se guardan en la memoria (402). Los siguientes datos del sondeo se guarda en la tabla (404): ID de célula; recuento de célula; Código de Área de Ubicación (LAC); CSQ; e ID de estación base. (En este punto el ID de célula es un número generalmente único usado para identificar cada estación transceptora base (BTS) o sector de una BTS dentro de un Código de Área de Ubicación (LAC) si no está dentro de una red de GSM. El Código de Área de Ubicación (LAC) es un número de 16 bits usado como una referencia única para la ubicación de un abonado móvil dentro de una red de GSM. Se usa un código de red de servicio móvil (MNC) en combinación con un código de país de servicio móvil (MCC) (también conocido como una "tupla MCC / MNC") para identificar inequívocamente un operador/portador de telefonía móvil usando, por ejemplo, las redes móviles públicas terrestres de GSM/LTE, CDMA, iDEN, TETRA y UMTS y algunas redes móviles por satélite). Además, datos de T3212 (relacionados con la frecuencia con qué se requiere que el dispositivo de alarma (10) realice un procedimiento de actualización de ubicación periódico) están disponibles a partir del sondeo y en algunas realizaciones se guarda en la tabla (404). Para cada red disponible (30) en la ubicación, el código de país de servicio móvil (MCC), los códigos de red de servicio móvil (MNC) y el número de células se recopila también por el módulo de radio (403) a través de la antena (407) y guardan en la tabla de redes (404). Para cada red disponible (30) en la ubicación, el microcontrolador (401) ordena al módulo de radio (403) y la SIM de itinerancia (405) que se conecte a cada red (30) a su vez y ordena al módulo de radio (403), a través de la antena (407), que transmita un paquete de señales al servidor de interrogación primario (60) y en respuesta el servidor de interrogación primario (60) transmite un paquete de señales al dispositivo de alarma (10). El paquete de señales desde el servidor de interrogación primario (60) se recibe por el módulo de radio (403) a través de la antena (407), y el módulo de radio (403) transmite los datos recibidos al microcontrolador (401). El microcontrolador (401) analiza los datos recibidos, y determina una relación de S/N para la red. Los datos de S/N a través de las redes (30) se guardan también en la tabla de redes (404).

El proceso de adquisición de datos para rellenar la tabla de redes (404) se denomina una 'exploración de red'.

Los parámetros de sintonización para el algoritmo también se guardan en la tabla de redes (404), tal como 'red solicitada', mantenida por el operador de red particular, por ejemplo, Vodafone UK, a usarse si está disponible una

conexión a esa red. La red solicitada (34) es una red de radio (30) a la que el usuario del dispositivo de alarma (10) preferiría que se conectase el dispositivo de alarma (10) si fuera posible, por ejemplo el usuario puede haber considerado que una red particular (30) proporciona una conexión de red estable y robusta.

La información de la exploración de red, almacenada en la tabla de redes (404), proporciona al gestor de conexiones (2) información con respecto a la topología de red de radio dentro de la que se sitúa el dispositivo de alarma (10). El gestor de conexiones (2), ejecutándose en el microcontrolador (401) como se ha descrito anteriormente, es capaz de tomar, a continuación, decisiones de itinerancia objetivas, asistidas y optimizadas, en términos de cuándo debería hacerse un cambio en red (30) y a qué red (30) debería hacerse, a continuación, una conexión.

La tabla de redes (404) contiene los detalles necesarios de los operadores de red identificados durante la exploración de red, y la tabla de redes (404) lista los detalles de hasta 14 operadores de red. En otras realizaciones, los detalles de más o menos operadores de red pueden almacenarse en la tabla de redes (404). Los MCC y MNC inequívocamente identifican una red (30) y se usan para conmutar redes (30), a través del gestor de conexiones (2) que ordena al microcontrolador (401), el módulo de radio (403) y la SIM de itinerancia (405) para que se registren en y a continuación conecten con la red requerida (30), proporcionando de este modo el enlace de radio (44) a la Internet (40).

Cuando se han adquirido y guardado todos los datos en la tabla de redes (404), la tabla de redes (404) se rellena con una lista de redes disponibles (30), en orden de intensidad de señal (CSQ) decreciente para cada red (30). En otras realizaciones la lista rellenada de redes disponibles se ordena en términos de señal a ruido decreciente, y en otras realizaciones la lista rellenada de redes disponibles se ordena en términos de número de células, o BER. Si se ha indicado una red solicitada (30), esta se sitúa en la parte superior de la lista.

Usando la información en la tabla de redes (404), el gestor de conexiones (2) habilita que el dispositivo de alarma (10) haga saltos de red de acuerdo con la mejor intensidad de señal (CSQ), como se describe a continuación. En otras realizaciones los saltos de red pueden hacerse de acuerdo con disponibilidad tal como, por ejemplo, número de células, o de acuerdo con señal a ruido como se ha analizado anteriormente. El experto apreciará sin embargo que la tabla de redes (404) puede ordenarse con respecto a cualquiera de los datos obtenidos a través de las redes (30), habilitando que hagan saltos de red sobre la base de esos datos.

El sondeo, y los otros procesos usados para rellenar una tabla de redes (404), se desencadena por el gestor de conexiones (2) ordenando al microcontrolador (401), en combinación con el módulo de radio (403), como se ha analizado anteriormente, cuando el dispositivo de alarma (10) se pone en marcha por primera vez, por ejemplo cuando el dispositivo de alarma se enciende. Continuando con la realización mostrada en la Figura 2b, se determina un valor de CSQ mínimo dependiendo de una indicación de intensidad de señal recibida (RSSI) como una función de conectividad de red. En la Figura 11 se muestran los valores de RSSI ilustrativos como una función de conectividad de red. Usando los valores de RSSI como se muestra en la Figura 11 se determina un valor de CSQ mínimo y cuando la intensidad de señal cae por debajo del valor de CSQ mínimo el gestor de conexiones (2) determina que el dispositivo de alarma (10) debería cambiar la red (30) a la que se conecta usando información dentro de la tabla de redes (404).

Cuando se ha indicado una red solicitada (34), aunque el dispositivo de alarma (10) se conecta a una red (30) diferente porque la red solicitada (34) no estaba disponible anteriormente, el gestor de conexiones (2) intentará registrar periódicamente y conectar el dispositivo de alarma (2) a la red solicitada (34) incluso cuando la intensidad de señal actual para la red actual (31) está por encima del valor de CSQ mínimo.

Haciendo referencia a la Figura 3a, un gestor de impulsos (3) está provisto del sistema de señalización de alarma (1) mostrado en la Figura 1a y la Figura 1b. El gestor de impulsos (3) es un algoritmo que se mantiene en memoria en el microcontrolador (401) y el servidor. Cuando se usan juntos pueden detectar problemas con el canal de comunicación. El gestor de impulsos (401) también se usa para pasar información accionada por tiempo o evento entre el servidor y dispositivo. Como se ha analizado anteriormente, el gestor de impulsos (3) proporciona un protocolo de instrucción flexible que permite que el dispositivo de alarma (10) envíe latidos periódicos. Estos latidos de instrucción cuando se reciben por el servidor de interrogación primario (60) conducen al servidor de interrogación primario (60) que envía un impulso de retorno al dispositivo de alarma (10) como una 'toma de contacto'. La toma de contacto habilita que el dispositivo de alarma (10) determine que se conecta a la Internet (40) y en comunicación con la estación de interrogación (60). La toma de contacto, desde el impulso de retorno, también habilita la determinación de un valor de intensidad de señal asociado con el enlace de radio (44) que se usa para proporcionar la conexión a la Internet (40). Adicionalmente, se entenderá que si la estación de interrogación (60) no recibe tal interrogación periódica desde el dispositivo de alarma (10) puede hacerse una determinación para contactar con la persona responsable que puede tomar una acción si es necesario.

Por simplicidad, el gestor de impulsos (3) mostrado en la Figura 3a se describirá ahora con referencia a la realización de la presente divulgación que hace uso de la Internet (40), que se muestra en la Figura 3b. Sin embargo, se entenderá que la realización mostrada en la Figura 3b comprende métodos y dispositivos que tienen aplicabilidad en los métodos y dispositivos de las otras realizaciones de la presente divulgación como se muestra en la Figura 3a.

Haciendo referencia a la Figura 3b, el gestor de impulsos (3) es un algoritmo mantenido en la memoria (402), que

cuando se ejecuta en el microcontrolador (401) habilita la transmisión y recepción de datos de interrogación, y/o datos de evento, tales como un mensaje de alarma, entre el dispositivo de alarma (10) y el servidor de interrogación primario (60) a través de la Internet (40). El servidor de interrogación primario (60) escucha mensajes entrantes, realiza una toma de contacto de acuse de recibo en el que una señal de impulso de retorno se envía de vuelta al dispositivo de alarma (10), y procesa el mensaje por consiguiente. El experto entenderá claramente, por lo tanto, lo que significa 'interrogación', y por qué se usa el gestor de impulsos.
Los tipos de mensajes que se envían desde el dispositivo de alarma (10) al servidor de interrogación primario (60) son uno de los siguientes:

- Mensaje de alarma (formatos de la industria de seguridad: SIA, ID de contacto, Formato Rápido).
- Tipo C de interrogación periódica (por ejemplo, cada 10 minutos).
- Tipo D de interrogación accionada por evento (por ejemplo, batería baja, reinicio de dispositivo, restablecimiento de trayectoria).

Por lo tanto, existen dos tipos de interrogación, el tipo C, que se produce periódicamente, y el tipo D que se desencadena por el evento.

El periodo entre interrogaciones de tipo C es variable, dependiendo del nivel de grado y el estado de salud actual del dispositivo de alarma (10) en el campo. Por lo tanto, el dispositivo de alarma (10) puede tener múltiples tasas de interrogación, dependiendo de la situación. El dispositivo de alarma (10) interroga cada 10 minutos y donde hay un enlace de radio (44) a la Internet (40) y conexión hacia delante por línea telefónica (25) al servidor de interrogación primario (60), y se recibe un impulso de retorno de toma de contacto desde el servidor de interrogación primario (60) a través de la misma ruta por el dispositivo de alarma (10), el dispositivo de alarma determina que tiene una conexión al servidor de interrogación (60). Sin embargo, si el dispositivo de alarma (10) no recibe un impulso de toma de contacto de retorno desde el servidor de interrogación primario (60), el dispositivo de alarma (10) determina que la trayectoria ha fallado. El dispositivo de alarma (10) envía a continuación interrogaciones de latido a una tasa aumentada de una interrogación cada dos minutos a través de una trayectoria secundaria, y estas interrogaciones van o bien al servidor de interrogación primario (60) o bien al secundario (62). El servidor de interrogación primario (60) y el centro de operaciones (80) son capaces de enviar mensajes al dispositivo de alarma (10) para aumentar la tasa de interrogación si es necesario. En otras realizaciones, el dispositivo de alarma (10) interroga a una tasa distinta de 10 minutos, por ejemplo a una tasa por debajo o por encima de 10 minutos, y en otras realizaciones cuando el dispositivo de alarma no recibe una toma de contacto de retorno interroga a una tasa aumentada distinta cada dos minutos, por ejemplo, a una tasa por debajo o por encima de dos minutos.

Las interrogaciones de tipo C se dividen en dos tipos de formatos. Cuando se interroga a una tasa alta se usa un formato corto de tipo C, que contiene únicamente la mitad de información para identificar el dispositivo de alarma (10), pero no otros datos. Interrogando a una tasa baja se usa un formato de Notación de Objeto de JavaScript (JSON), que habilita que se transmita más información relacionada con el estado del dispositivo de alarma (10). En otras realizaciones, se usan los formatos tales como TEXTO.

Para interrogaciones de tipo D, se usa el formato de datos de JSON para transmitir los datos relacionados con evento, y además de proporcionar información, tal como indicación de batería baja, se usan interrogaciones de tipo D para actualizar el perfil del dispositivo de alarma (10) en el servidor de interrogación primario (60), relacionado con intensidades de señal a través de redes (39), e integridades de sensor dentro del dispositivo de alarma (10). Las interrogaciones de tipo D que usan el protocolo de JSON usan información de distribución de notación de valor de clave (por ejemplo, BAT:3.7, MCC:234, CSQ:17).

La interrogación de tipo C desde el dispositivo de alarma (10) al servidor de interrogación primario (60), y las interrogaciones de toma de contacto de retorno desde el servidor de interrogación primario (60) al dispositivo de alarma (10), además de habilitar la determinación relacionada con la integridad de la trayectoria, habilitan la determinación de los valores de CSQ y relaciones de S/N como se ha analizado anteriormente.

Volviendo al gestor de conexiones (2) mostrado en la Figura 2b, el impulso de toma de contacto de retorno desde el servidor de interrogación primario (60), recibido como consecuencia del dispositivo de alarma (10) habiendo enviado una interrogación de latido periódica de tipo C que se recibió por el servidor de interrogación primario (60), por lo tanto, determina los valores de CSQ y también se usa para determinar las relaciones S/N y BER. En otras realizaciones, puede determinarse CSQ sin necesidad de una transmisión de alarma anterior.

El impulso de toma de contacto de retorno recibido por el dispositivo de alarma (10) desde el servidor de interrogación primario (60) se denomina un 'muestreo de CSQ'. Dentro del gestor de conexiones (2) se asigna el número 3 a un "valor de recuento de CSQ", y este se almacena en la memoria (402). El valor de recuento de CSQ se usa para determinar si el dispositivo de alarma (10) debería desconectarse de la red (30) a la que se conecta y registrarse y conectarse a una red diferente (30) para proporcionar un nuevo enlace de radio (44) a la Internet (40). Cuando 3 muestreos de CSQ consecutivos están por debajo del nivel de CSQ mínimo, que es cuando el número de muestras de CSQ por debajo del nivel de CSQ mínimo es igual al valor de recuento de CSQ, el gestor de conexiones (2) toma una decisión de 'salto fuera' y determina que debería iniciarse un proceso de 'salto a' a una nueva red (30). El gestor

de conexiones (2) habilita que un usuario indique que desean bloquearse a la red solicitada (34). Si se selecciona una opción de 'bloquear en red solicitada', y en ese momento el dispositivo de alarma (10) se conecta a la red solicitada (34), a continuación se ignora el valor de CSQ de muestreos de CSQ.

Además del gestor de conexiones (2) haciendo una decisión de salto fuera basándose en 3 muestras de CSQ consecutivas estando por debajo del nivel de CSQ mínimo, el gestor de conexiones (2) también toma la decisión de salto fuera en las siguientes situaciones:

- Durante operación normal, el dispositivo de alarma (10) se registra en una red (30) de un operador de red a través de la SIM de itinerancia (405) y, si existe una pérdida de registro, el gestor de conexiones (2) intenta registrarse de nuevo con un operador de red. Dentro del gestor de conexiones (2) se almacena un valor de 'Recuento de Fallos de Registro' igual a 3 en la memoria (402). Cuando el número de consultas de registro con un operador de red es mayor que el valor de Recuento de Fallos de Registro, es decir es igual a 4, el gestor de conexiones (2) toma una decisión de salto fuera. Puede usarse un valor de 'Recuento de Fallos de Registro' mayor de 3, pero esto conduce a la modificación de la forma en que el gestor de conexiones (2) intenta registrarse de nuevo para no conducir al dispositivo de alarma (10) de ser excluido de conexión a ese operador de red y, de hecho, a otros operadores de red, como se analiza a continuación en relación con la mitigación de comportamiento agresivo.
- Si en respuesta a una interrogación de latido de tipo C desde el dispositivo de alarma (10) que no conduce a un impulso de señal de toma de contacto de retorno desde el servidor de interrogación primario (60), como se ha analizado anteriormente la tasa de interrogación se aumenta. Si es que no existe ninguna respuesta de impulso de señal de toma de contacto a 3 interrogaciones consecutivas de latido desde el dispositivo de alarma (10) al servidor de interrogación primario (60), el gestor de conexiones (2) toma una decisión de salto fuera.
- Existen, por lo tanto, dos tipos de interrogaciones: interrogación "normal"; e interrogación "prioritaria". La interrogación normal es cuando el dispositivo de alarma (10) está operando sin haber un fallo detectado dentro del sistema de señalización de alarma, e interrogación prioritaria es cuando el dispositivo de alarma (10) ha determinado que existe un fallo, por ejemplo, que ha fallado una trayectoria a un servidor de interrogación.
- Si se han indicado las opciones de "red solicitada (34)" y el "retorno a la red solicitada después de 48 h", y el dispositivo de alarma (10) no ha cambiado redes (30) durante 48 horas, y la red actual (31) no es la red solicitada (34), el gestor de conexiones (2) toma una decisión de salto fuera. Se ha de observar que si se especifica una red solicitada (34), el dispositivo de alarma (10) intenta volver a esta red solicitada (34) en cada otro intento (cambio de red - salto a).

Después de que el gestor de conexiones (2) haya tomado una decisión de salto fuera, el gestor de conexiones (2) toma una decisión de 'salto a', en la que se toma una decisión objetivo basándose en los datos contenidos dentro de la tabla de redes (404) con respecto a qué red (30) saltar. El gestor de conexiones (2) aplica los siguientes procedimientos, en orden de prioridad:

1. Si se habilita bloquear en red solicitada, el dispositivo de alarma (10) debería conmutar a la red solicitada (34) y deshabilitar itinerancia, evitando por lo tanto cualquier intento de cambio de red adicional;
2. Si se habilita la red solicitada (34), cada intento alternativo debería hacerse a la red solicitada (34) (incluso mientras se avanza a través de la tabla de redes, como se describe en el punto 3 a continuación);
3. Si ninguno de los anteriores es verdadero a continuación el dispositivo de alarma (10) intentará usar la tabla de redes (404). La tabla (404) se lee de arriba a abajo, con entradas relacionadas con la mayor a menor intensidad de señal de redes disponibles (30); en otras realizaciones como se ha analizado anteriormente las entradas se rellenan sobre la base de otros criterios tales como BER, por ejemplo. Se usarán únicamente redes (30) con valores de CSQ por encima del valor de CSQ mínimo. Se harán intentos para cada entrada de red válida en la tabla sucesivamente (excepto la red actual (31)). Cuando la última entrada de red se ha intentado, el siguiente intento será de nuevo la primera entrada de red. Sin embargo, si se ha intentado la última entrada de red y el dispositivo de alarma (10) no puede establecer un enlace de radio (44) con la red (30) o un operador de red, el gestor de conexiones (2) lleva a cabo otra exploración de red para rellenar la tabla de redes (404) con datos actualizados de red y operador de red.

Como se ha analizado en el punto 3 anterior, se realiza una exploración de red durante el proceso de salto a cuando se han intentado todas las entradas válidas de la tabla de red (404). Además se realiza una exploración de red al encender del dispositivo de alarma (10). Una exploración de red también puede realizarse manualmente por un usuario tecleando un código apropiado en un teclado numérico en la interfaz de usuario (421) en el dispositivo de alarma (10); además de los datos analizados anteriormente que se introducen en la tabla de redes (404) ahora se almacena un ID de operador dentro de la tabla de redes (404). Adicionalmente, la exploración de red puede iniciarse a través de un comando remoto transmitido desde el centro de operaciones (80) al dispositivo de alarma (10). Una exploración de red sobrescribe los contenidos de la tabla de redes (404) con los nuevos datos adquiridos durante la exploración de red. Se evita que se produzca una exploración de red dentro de dos minutos de la inicialización de un módulo de radio (403). En otras realizaciones, se evitan que se produzcan exploraciones de red dentro de escalas de tiempo más cortas o mayores de dos minutos.

El gestor de conexiones (2), tomando la decisión de salto fuera después de cuatro intentos de registro fallidos a la red actual (31) y progresando a través de la tabla de redes (404) sobre la base de prioridad, no proporciona únicamente

un enlace de radio optimizado (44) a la Internet (40), sino que evita lo que se denomina 'comportamiento agresivo'. El comportamiento agresivo puede entenderse como se indica a continuación:
En el evento de un fallo para conectarse a cualquier red móvil de radio visible (30), es importante que una aplicación de máquina a máquina (M2M) no intente repetitivamente obtener adhesión de la red (30) y acceso a servicios. Si un dispositivo intentase repetitivamente acceder a redes móviles (30) cuando está excluido, la mayoría de operadores bloquearán el dispositivo a nivel de radio y lo harán permanentemente inútil.

El gestor de conexiones (2), mitiga tal comportamiento agresivo por el dispositivo de alarma (10) no intentando repetitivamente acceder a redes móviles (30) de tal manera, y además asegura que el dispositivo de alarma (10) no intente acceder a una red de radio (30) en un momento sincronizado con el desencadenador de reloj público, para evitar intentar conectarse en un momento en el que un número significativo de dispositivos de alarma dentro del área de cobertura de que red (30) están también intentando establecer una conexión que podría conducir al operador de red a determinar que tal acceso es un comportamiento agresivo.

Como se ha analizado anteriormente, durante operación normal, el gestor de conexiones (2) intenta registrarse de nuevo con una red (30) si se pierde una conexión. Se proporciona información adicional sobre cómo hace esto el gestor de conexiones (2) para evitar tal comportamiento agresivo, como se indica a continuación. Cuando el dispositivo de alarma (10) se da cuenta que una interrogación o una llamada de alarma no pasa hasta su servidor de interrogación primario (60) y servidor de interrogación secundario (62), esto indica que el enlace de radio (44) ha fallado y que no existe ninguna conexión con la red actual (31). Primero, el gestor de conexiones (2) intenta conectarse de nuevo con la red actual (31). Para entender lo que hace el gestor de conexiones (2) debemos introducir el contexto de protocolo de datos por paquetes (PDP) como se aplica en relación con el enlace de radio (44) y la conexión a la corriente (31) y/o una red (30). El contexto de PDP es una estructura de datos que contiene información de sesión relacionada con una sesión activa con una red (30) operada por un operador de red. Continuando con la realización mostrada en la Figura 2b, si la conexión con la red actual (31) ha fallado esto significa que el contexto de PDP con la red actual (31) no está activado o está en un estado en reposo o espera.

El gestor de conexiones (2) primero intenta conectarse de nuevo al servidor. Si eso falla a continuación el gestor de conexiones (2) intenta activar el contexto de PDP. Si la reactivación del contexto de PDP falla, el gestor de conexiones (2) intentará reactivar el contexto de PDP cuatro veces más con un retardo de tiempo, antes de cancelar el registro de la red actual (31) realizando una "decisión de salto a" (1050). El número de intentos de activación de contexto de PDP se establece por defecto a cuatro donde el retardo de tiempo entre cada uno se establece a un tiempo mínimo de un minuto para mitigar lo que se consideraría como comportamiento agresivo por el operador de red. El número de intentos de activación de contexto de PDP puede aumentarse, sin embargo el tiempo entre intentos se aumenta de nuevo para mitigar el comportamiento agresivo. Numerosos intentos de activación de contexto de PDP en una sucesión rápida y/o numerosos intentos de registro en una sucesión rápida podrían considerarse por el operador de red que constituye comportamiento agresivo y el gestor de conexiones (2) aumenta el tiempo entre intentos a medida que aumenta el número de intentos para evitar que tales intentos se consideren como agresivos. Las siguientes tablas proporcionan información sobre el tiempo usado entre activación de PDP e intentos de registro.

| Intento de activación de contexto de PDP | Intervalo de tiempo |
|---|---|
| 1-4 | Mayor de o igual a 1 minuto |
| 5 | Mayor de o igual a 15 minutos |
| 6 | Mayor de o igual a 30 minutos |
| 7-N | Mayor de o igual a una hora |

| Intento de registro | Intervalo de tiempo |
|---|---|
| 1-4 | Mayor de o igual a 1 minuto |
| 5 | Mayor de o igual a 15 minutos |
| 6 | Mayor de o igual a 30 minutos |
| 7-N | Mayor de o igual a una hora |

Si la reactivación y registro de contexto de PDP falla, como se ha analizado anteriormente, el gestor de conexiones (2) hará una decisión de salto fuera, seguida por el uso de la tabla de redes (404) para tomar una decisión de salto a. Si es que no puede proporcionarse una conexión a ninguna de las redes (30) dentro de la tabla de redes (404), incluyendo después de que se haya efectuado una nueva exploración de red para rellenar la tabla de redes (404) con datos de topología de operador de red de red actualizada, el gestor de conexiones (2) reiniciará el módulo de radio (403). Después del inicio del módulo de radio (403), se efectúa una nueva exploración de red después de un periodo de tiempo igual a o mayor de dos minutos desde la inicialización del módulo de radio (403). El gestor de conexiones (2), intenta registrar y a continuación activar el contexto de PDP con redes (30) usando los datos dentro de la recientemente rellenada tabla de red (404) como se ha analizado anteriormente. Si no puede establecerse un enlace de radio (44) a la Internet (40), el gestor de conexiones (2) reiniciará de nuevo el módulo de radio (403) usando periodos de tiempo como se muestra en la tabla a continuación, de nuevo para mitigar el comportamiento agresivo.

| Reinicio de módulo de radio (403) | Intervalo de tiempo |
|---|---|
| 1-4 | Mayor de o igual a 5 minutos |
| 5-6 | Mayor de o igual a 30 minutos |
| 7-N | Mayor de o igual a una hora |

Cuando la red (30) de un operador de red particular no es fiable, incluso aunque la intensidad de señal es aceptable o incluso alta, o si el dispositivo de alarma (30) oscila entre diferentes redes, o si existen redes particulares a las que el usuario no desea conectarse, los detalles de estos operadores de red pueden introducirse en una lista negra de redes, que se almacena a continuación en la memoria (402). El gestor de conexiones (2) no intentará conectarse a redes (30) si están en la lista negra.

Ahora se describirá en más detalle una realización del dispositivo de alarma (10) con referencia al diagrama esquemático mostrado en la Figura 4, en el que como se ha descrito anteriormente en otras realizaciones el dispositivo puede ser un dispositivo médico, y en otras realizaciones el dispositivo es cualquier dispositivo de comunicación con un módulo de radio y SIM de itinerancia. Continuando con la realización mostrada en la Figura 4, el dispositivo de alarma (10) tiene un microcontrolador (401) con memoria (402), módulo de radio (403) con SIM de itinerancia asociada (405) con funcionalidad de sondeo, antena (407) y conjunto de sensores (419) como se ha analizado anteriormente.

El dispositivo de alarma (10) se conecta a una fuente de alimentación externa (no mostrada) en el puerto de fuente de alimentación (no mostrado), y el puerto de fuente de alimentación se conecta al circuito de gestión de potencia (415), con un circuito de gestión de potencia (415) tiene un supervisor de tensión y corriente (417). El circuito de gestión de potencia (415) se dispone para recibir potencia desde el puerto de fuente de alimentación y para proporcionar una salida de fuente de alimentación regulada que se conecta al resto desde la circuitería del dispositivo de alarma (10) para ser capaz de suministrar potencia. El supervisor de tensión y corriente (417) se dispone para supervisar la tensión de fuente de alimentación y proporcionar una salida que se conecta al microcontrolador (201), capaz de informar al microcontrolador (201) si la tensión de entrada de fuente de alimentación está fuera de un intervalo de tensión predeterminado. El dispositivo de alarma (10) se dispone para operar desde un suministro eléctrico de CA de 240 V y 50 Hz AC somo se encuentra en el Reino Unido. En otras realizaciones, el dispositivo de alarma (10) se dispone para operar desde un suministro eléctrico de CA de 230 V y 50 Hz, y en otras realizaciones el dispositivo de alarma (10) se dispone para operar desde un suministro eléctrico de CA de 230 V y 60 Hz, y en otras realizaciones el dispositivo de alarma (10) se dispone para operar desde un suministro eléctrico de CA de 120 V y 60 Hz. El experto apreciará que el dispositivo de alarma (10) puede disponerse para operar desde cualquier suministro de energía eléctrica apropiado del mundo. En otras realizaciones, el dispositivo de alarma (10) se dispone para operar desde la tensión de CC en el intervalo de ejemplo 9 a 30 voltios, en las que, por ejemplo, en algunas de estas realizaciones el dispositivo de alarma (10) cuando se retroadapta a un dispositivo de alarma adicional (450) se dispone para tomar su potencia desde el dispositivo de alarma adicional (450). En otras realizaciones, en las que, por ejemplo, el dispositivo de alarma se retroadapta a un dispositivo de alarma adicional, el dispositivo de alarma se dispone para operar desde una fuente de alimentación de CC de 5 V.

El circuito de gestión de potencia (415) regula la tensión de fuente de alimentación entrante y suministra potencia a los componentes, el supervisor de tensión y corriente (417) supervisa la tensión de CA de fuente de alimentación externa y notifica al microcontrolador si la tensión de fuente de alimentación se sale de un intervalo definido. Tales eventos "fuera de intervalo" se registran también en el registro almacenado en la memoria de microcontrolador (403) y puede iniciar selectivamente (basándose en preferencias de usuario almacenadas) el envío de un mensaje por el dispositivo de alarma (10) al ARC (50) o al centro de operaciones (80). En otras realizaciones, en las que el dispositivo de alarma (10) se conecta a, y obtiene su potencia de, un dispositivo de alarma adicional (450), el supervisor de tensión y corriente (417) supervisa la fuente de alimentación de CC externa.

El dispositivo de alarma (10), tiene una interfaz de usuario (421) conectada al microcontrolador (401). La interfaz de usuario (421) habilita que un usuario del dispositivo de alarma (10) proporcione información para recibir información desde el dispositivo de alarma (10). La interfaz de usuario (421) tiene un teclado numérico con botones (no mostrados) mediante los que un usuario puede proporcionar información al dispositivo de alarma (10). La interfaz de usuario (421) tiene el visualizador LED (no mostrado) mediante el cual puede proporcionarse información al usuario. La interfaz de usuario (421) tiene una luz LED (no mostrada) para proporcionar estado de integridad de potencia al usuario, con un color rojo indicando que el dispositivo de alarma (10) está en una configuración alimentada, y una luz LED adicional (no mostrada) para proporcionar un estado de integridad del dispositivo de alarma (10) al usuario, con una luz verde que indica que el dispositivo de alarma (10) está operacional. Usando la interfaz de usuario (421) un usuario puede conectarse manualmente a una red (30) de su elección, a través del visualizador LED visualizando las redes disponibles (30), y seleccionando el usuario, a continuación, de la lista de redes disponibles. El gestor de conexiones (2) se conecta a continuación a esa red (30) como se ha analizado anteriormente. El experto entenderá claramente que la interfaz de usuario (421) depende de la aplicación para la que está usándose el dispositivo de alarma (10).

El dispositivo de alarma (10) tiene componentes de interacción de comunicación para interactuar con el microcontrolador (401), el gestor de conexiones (2) y el gestor de impulsos (3) externamente al dispositivo de alarma

(10). Los componentes de interacción son: una interfaz de PSTN (411) usada en conjunto con entrada salida externa (413) para el establecimiento y comunicación con y a través de una PSTN (20); una interfaz de red de área local (LAN) (409) usada en conjunto con el módulo de radio (403), o entrada salida externa (413), para el establecimiento y comunicación con y a través de la Internet (40); y el módulo de radio (407) usado directamente para el establecimiento y comunicación con y a través de la Internet (40), como se ha analizado anteriormente. En otras realizaciones, el módulo de radio (413) se usa para establecer un enlace de radio (44) directamente con el servidor de interrogación primario (60) y un servidor de interrogación secundario (62).

El dispositivo de alarma (10) se construye usando técnicas de fabricación de dispositivos electrónicos conocidas tales como, por ejemplo, el uso de placa de circuito impresos y carcasas de plástico moldeadas y/o contenedores de metal plegados. El lector experto estará familiarizado con tales métodos de construcción y no es necesario extenderse adicionalmente en este punto. El circuito de gestión de potencia (415) y el supervisor de tensión y corriente (417) se implementan usando o bien circuitería analógica o bien circuitería digital comúnmente conocidas. Por ejemplo, el supervisor de tensión y corriente (417) hace uso de uno o más comparadores, pero en otras realizaciones puede implementarse usando uno o más convertidores de analógico a digital, cuya salida debería alimentarse al microcontrolador (401) y la detección realizada por software ejecutándose en el mismo.

Los sistemas mostrados en la Figura 1a y la Figura 1b se construyen usando elementos comúnmente en uso, tales como líneas telefónicas (25), centrales telefónicas (no mostradas), una PSTN (20), una red de radio (30) (por ejemplo, una red de radio de GPRS, aunque otras realizaciones pueden usar una red de radio de GSM) y ARC existentes (50). El servidor de interrogación primario (60), servidor de interrogación secundario (62) y pasarela de alarma (50) se construyen usando equipo de servidor estándar en conjunto con interfaces estándar a líneas telefónicas, líneas X.25 de tipo kilostream y líneas arrendadas.

Como se ha analizado anteriormente, el dispositivo de alarma (10) puede proporcionarse con información de fechas. La actualización remota opera como se indica a continuación. Cuando el dispositivo de alarma (10) recibe una instrucción de actualización desde un dispositivo remoto (por ejemplo, desde un servidor de interrogación (60, 62), o desde el ARC (50)) que indica que debería efectuarse un procedimiento de actualización remoto, el dispositivo de alarma (10) cierra el enlace de comunicación con el dispositivo remoto y a continuación se conecta con el centro de operaciones (80). El centro de operaciones (80) es capaz, a continuación, de actualizar los contenidos de la memoria (402) del dispositivo de alarma (10) enviando mensajes al dispositivo de alarma (10), y de esta forma el gestor de conexiones (2) y gestor de impulsos (3) también con capaces de actualizarse, así como nuevas direcciones IP de dispositivos remotos a las que puede conectarse el dispositivo de alarma (10).

Un conmutador de llamada de administración se ubica en la interfaz de usuario (421) y presionando este un usuario puede provocar que el dispositivo de alarma (10) llame al centro de operaciones (80), si es necesario, por ejemplo si el usuario sospecha que el dispositivo de alarma (10) no está funcionando correctamente, presionando el conmutador de llamada de administración el centro de operaciones (80) en comunicación con el dispositivo de alarma (10) puede realizar una comprobación de diagnóstico del dispositivo de alarma (10).

Ahora se describirán métodos y dispositivos de las realizaciones de la presente divulgación con referencia a las Figuras 5 a 10, que muestran diferentes aspectos de operación de las realizaciones de la presente divulgación. El experto apreciará que tales métodos incluyen el uso de software o programa o programas informáticos que se ejecutan dentro de un microcontrolador apropiado, usado para controlar dispositivos para proporcionar los aspectos descritos de operación.

La Figura 5 muestra las etapas de método asociadas con conexión de red dentro del sistema mostrado en la Figura 1b. Las etapas de proceso en la Figura 5 constituyen un 'bucle maestro' efectuado por el gestor de conexiones (2). En resumen, los procesos dentro de la Figura 5 son:

1. Inicialización de módulo de radio.
2. Registro inicial (manual o automático).
3. Llamada de conectividad y funciones de comprobación de salud.
4. Otras tareas domésticas relacionadas con dispositivo (por ejemplo, actualización, captura de alarma).

Haciendo referencia a la Figura 5, en la etapa (510) se enciende el dispositivo de alarma (10), y en la etapa (520) el gestor de conexiones (2) determina si la última red (30) a la que se conectó el dispositivo de alarma (10) está disponible. Si la última red (30) está disponible, esta información se proporciona en la interfaz de usuario (421), y si el usuario elige conectarse a esta red (30) una presión un botón asociado en el teclado numérico de la interfaz de usuario (421) y el gestor de conexiones (2) se conecta 'manualmente' a esta red (30) que se produce en la etapa (530). El proceso a continuación avanza a la etapa (550). Si en la etapa (520) la última red no está disponible, o si el usuario no desea conectarse a la última red que estaba disponible, el proceso avanza a la etapa (540). En la etapa (540) el gestor de conexiones (2) usa la tabla de redes (404) para conectarse a una red (30) como se ha analizado anteriormente. El proceso y mueven etapa (550). En la etapa (550) y etapa (560) el dispositivo de alarma (10) lleva a cabo una comprobación de integridad, y si es necesario transmite un mensaje de tipo D al centro de operaciones (80).

La Figura 6 muestra las etapas de método asociadas con conectividad y funcionalidad de comprobación de salud dentro del sistema mostrado en la Figura 1b. En resumen, los procesos dentro de la Figura 6 son:

1. Tratamiento de alarma/interrogación.
2. Comprobación de sondeo de encendido por primera vez.
3. Recuento de registros fallidos - Cuántas veces falla el registro antes de itinerancia.
4. Recuento y valor de CSQ fallida - Si el valor de CSQ está por debajo del mínimo especificado durante N veces, la unidad realizará itinerancia.
5. Red solicitada - Si se especifica la "red solicitada" y se selecciona "retornar después de 48 h", el dispositivo de alarma (10) realizará itinerancia, después de estar en una red no preferida durante >48 h.

Haciendo referencia a la Figura 6, el proceso comienza en la etapa (605), que es la misma que la etapa (550) como se muestra en la Figura 5 en la que se hacen comprobaciones de estado de integridad y, a continuación, el proceso avanza a la etapa (610). En la etapa (610) el gestor de conexiones (2) determina si debe trasmitirse un impulso de señal de interrogación de tipo C y/o una señal de alarma de tipo D. Si es que no, el proceso avanza a la etapa (620). Si es que sí, el proceso avanza a la etapa (615) en la que el microcontrolador (401) ordena al módulo de radio (403) que envíe los datos necesarios, y el proceso avanza a la etapa (620). En la etapa (620) el gestor de conexiones (2) determina si el dispositivo de alarma (10) o módulo de radio (403) se acaban de encender, y si es que no, el proceso avanza a la etapa (630). Si es que sí, el gestor de conexiones (2) efectúa una exploración de red, y rellena la tabla de redes (404), y el proceso avanza a la etapa (630). En la etapa (630) el gestor de conexiones (2) determina si el número de consultas de registro es igual al Recuento de Fallos de Registro, y si es que no el proceso avanza a la etapa (640). Si es que sí, el proceso avanza a la etapa (635) en la que el gestor de conexiones (2) toma una decisión de salto a y pasa el proceso de conexión a la red (30), y el proceso avanza a la etapa (640). En la etapa (640) el gestor de conexiones (2) determina si la muestra de CSQ es menor que el valor de CSQ mínimo. Si es que no, el proceso avanza a la etapa (655). Si es que sí, el proceso avanza a la etapa (645) en la que se determina si el número de muestras de CSQ consecutivas, por debajo del nivel de CSQ mínimo, es igual al valor de recuento de CSQ. Si es que no, el proceso avanza a la etapa (655). Si es que sí, el proceso avanza a la etapa (650) en la que se hace una decisión de salto a para realizar itinerancia a una nueva red (30) usando la tabla de redes (404), a continuación de lo cual el proceso avanza a la etapa (655). En la etapa (655) se determina si se ha indicado una red solicitada (34) y se ha seleccionado la opción de retorno después de 48 horas, y si de modo que el dispositivo de alarma (10) se ha registrado en una red (30) distinta de la red solicitada (34) para una duración de tiempo mayor de 48 horas. Si es que no, el proceso avanza a la etapa (665). Si es que sí, el proceso avanza a la etapa (660) en la que se toma una decisión de salto a, a continuación de la cual el proceso avanza a la etapa (665) en cuyo punto el proceso vuelve en el bucle principal. Desde ahí, la etapa (550/605) se llama de nuevo a continuación de alguna tarea doméstica - etapa (560).

La Figura 7 muestra las etapas de método asociadas con la determinación de idoneidad de red dentro del sistema mostrado en la Figura 1b. En resumen, los procesos dentro de la Figura 7, constituyen la decisión de 'salto a', y son: El proceso de "decisión de salto a" evalúa la idoneidad de la red (30) a la que el dispositivo de alarma (10) está a punto de realizar itinerancia. Se tienen en cuenta los siguientes factores:

1. Opción de "Bloqueo a red solicitada" habilitada.
2. "Red solicitada especificada/seleccionada" (Registro a esta red se intenta cada otro intento).
3. Red actual evaluada está en lista negra
4. Decisión basándose en CSQ, Células, BER - la clasificación de la tabla puede variar.

    a. Decisión de CSQ pura. La tabla se clasifica por la CSQ más alta
    b. $CSQ \times K_{csq} + Célula \times K_{célula} + BER \times K_{ber}$ $K_{csq}$, $K_{célula}$, y $K_{ber}$ son coeficientes, también llamados ponderaciones, asociados con los parámetros *CSQ, Célula,* y *BER* respectivamente.
    c. Ajuste de umbral dinámico (cuando se alcanza el final de la tabla se reduce el umbral).
    d. Tiempo de inactividad

Haciendo referencia a la Figura 7, el proceso comienza en la etapa (705) que se refiere a las etapas de proceso de decisión de 'salto a'. Por lo tanto, las etapas (705) y las siguientes etapas como se muestra en la Figura 7, constituyen lo que se produce en las etapas 635, 650, 660 como se muestra en la Figura 6, y la etapa 1050 a analizarse a continuación con respecto a la Figura 10. En la etapa (710) se determina si se ha indicado 'bloquear en red solicitada (34)'. Si es que sí, el proceso avanza a la etapa (715) con la exploración de red funcionalidad estando deshabilitada, a continuación de la cual en la etapa (720) el gestor de conexiones (2) deshabilita la capacidad del dispositivo de alarma (10) para realizar itinerancia a través de redes (30). El proceso a continuación avanza a la etapa (750) analizada a continuación. Si en la etapa (710) se determinó que la opción de bloquear no se ha indicado, el proceso avanza a la etapa (725). En la etapa (725) se determina si se ha indicado una red solicitada (34), y si es así si este intento de registro constituye el intento 'alternativo' cuando se intenta efectuar el registro en la red solicitada (34). Si es que sí, el proceso avanza a la etapa (750) como se analiza a continuación. Si es que no el proceso avanza a la etapa (730) en la que se determina si existen algunas más entradas de la red (30) dentro de la tabla de redes (404) a analizar. Si es que no, esto significa que la última red (30) evaluada era la red válida más inferior (30) con la tabla de redes (404), y el proceso avanza a la etapa (735) en la que se efectúa una nueva exploración de red, después de la cual el proceso vuelve a la etapa (730). Si en la etapa anterior (730) no se ha alcanzado la red válida más inferior (30) dentro de la

tabla de redes (404) el proceso avanza a la etapa (740). En la etapa (740) se evalúa la siguiente red válida (30) para determinar si está en la lista negra y si es así el proceso vuelve a la etapa (725). Si la siguiente red válida (30) no está en la lista negra, el proceso avanza a la etapa (745). En la etapa (745), la tabla de redes (404) se ha clasificado sobre la base de CSQ y como tal, si la red evaluada en la actualidad tiene en valor de CSQ aceptable por encima del valor de CSQ mínimo, se intentará el registro en esta red - esto se introduce en el punto 4a anterior. Si el registro es satisfactorio, el proceso se detiene, pero si el registro no es satisfactorio el proceso avanza a la etapa (725). En otras realizaciones, la clasificación de la tabla de redes (404) es sobre la base de S/N o BER o número de células, por ejemplo.

En otra realización, introducida en el punto 4a anterior, la tabla de redes (404) se clasifica sobre la base CSQ, y número de células (Célula), y BER, en la que para cada red (30) del operador de red se asigna una figura de mérito a esa red usando los coeficientes $K_{csq}$, $K_{célula}$, y $K_{ber}$ asociados con CSQ, número de células (Célula) y BER respectivamente como se muestra anteriormente en el punto 4b. Los coeficientes $K_{csq}$, $K_{célula}$, y $K_{ber}$ se definen por usuario e introducen en el dispositivo de alarma (10) mediante el teclado numérico de la interfaz de usuario (421) o se proporcionan remotamente desde el centro de operaciones (80). En otra realización, introducida en el punto 4c anterior, si se alcanza el final de la tabla de redes (404) y no se ha encontrado ninguna red que tenga un valor de CSQ por encima del valor de CSQ mínimo, se aplica un ajuste de umbral dinámico, para que después de la siguiente exploración de red usada para rellenar la tabla de redes (404), habrá una mayor probabilidad de que se haya establecido un enlace de radio (44) satisfactorio. En una realización adicional, introducida en el punto 4d, las redes (30) dentro de la tabla de redes (404) se almacenan sobre la base del porcentaje de tiempo que esas redes no estuvieron disponibles, es decir, se clasifican sobre la base de tiempo de inactividad. En la etapa (750) el gestor de conexiones (2) se registra en la red solicitada (34), después de la cual el proceso avanza a la etapa (755) en la que el proceso finaliza.

La Figura 8 muestra las etapas de método asociadas con sondeo de red dentro del sistema mostrado en la Figura 1b. En resumen, los procesos dentro de la Figura 8, constituyen un sondeo y exploración de canal de banda (exploración de red). Para recordar, un sondeo se desencadena por el microcontrolador (401) del dispositivo de alarma (10) cuando el dispositivo de alarma (10) se pone en marcha por primera vez y cuando la tabla de redes (404) se agota. El microcontrolador anfitrión (401) ordena al módulo de radio (403) que explore el área y guarde todos los datos útiles tales como ID de célula, recuento de célula, LAC (Código de Área de Ubicación), CSQ, ID de estación base, etc. Toda esta información se sitúa en la tabla de redes (404), guarda en la memoria no volátil (402), que se usa cuando se conmutan redes.

Haciendo referencia a la Figura 8, el proceso comienza en la etapa (810), que corresponde a la etapa (625) en la Figura 6 y etapa (735) en la Figura 7, y avanza a la etapa (820). En la etapa (820) se efectúa la exploración de red como se ha analizado anteriormente, y en la etapa (830) se rellena la tabla de red (404), después de la cual etapa (840) el proceso finaliza.

La Figura 9 muestra las etapas de método asociadas con el establecimiento de una conexión de datos dentro del sistema mostrado en la Figura 1b. En resumen, los procesos dentro de la Figura 9, constituyen procesos de PDP - conectividad de datos realizados por el gestor de conexiones (2). Para recordar, después de registrarse en una red (30), el dispositivo de alarma (10) necesita establecer una conexión de datos adjuntando y activando el contexto de PDP. Esto a continuación habilita que el dispositivo de alarma (10) consiga conectividad IP y se comunique con el mundo exterior. Ocasionalmente el operador de red situará el dispositivo de alarma (10) en un estado de espera o de reposo. Mientras está ahí, el dispositivo de alarma (10) podría no ser capaz de señalizar. Para traer de vuelta el dispositivo de alarma (10) al estado listo, el dispositivo de alarma (10) necesita actualizar su PDPD o bien separando completamente o bien intentando conectarse con el servidor de interrogación (60) a través del enlace de radio (44) y la Internet (40) a través de la red (30). Debe tenerse cuidad cuando se actualiza el PDP ya que la SIM podría señalarse como agresiva y bloquearse completamente. El gestor de conexiones (2) asegura que esto no sucede.

Haciendo referencia a la Figura 9, en la etapa (910) comienza el proceso de actualización de PDP, en el que la etapa (920) el gestor de conexiones (2) separa y desactiva el contexto de PDP como se ha analizado anteriormente. A continuación de la cual, en la etapa (930), el gestor de conexiones (2) adjunta y activa el contexto de PDP, después de la cual etapa (940) el proceso finaliza.

La Figura 10 muestra las etapas de método asociadas con la realización de una toma de contacto de estado y las etapas de método asociadas con el restablecimiento de conexión de datos, dentro del sistema mostrado en la Figura 1b. En resumen, los procesos dentro de la Figura 10 constituyen transmisión de interrogación y alarma. Para recordar, cuando hay presente una transmisión pendiente, la toma de contacto y la carga útil se envían al servidor de interrogación (60). Si la llamada falla más que el valor de Recuento de Fallos de Registro, el dispositivo de alarma (10) intenta traer de vuelta la conexión de datos, o bien intentando reconectarse con el servidor de interrogación (60) o bien actualizando el contexto de PDP. Mientras la recuperación está en progreso, el dispositivo de alarma (10) no debería exceder los intentos por minuto recomendados por el operador. Una vez que la transmisión es satisfactoria, el dispositivo de alarma (10) registra la tasa de errores de bits calculada a partir de la última transmisión. La BER también se guarda en la tabla de redes (404) junto con el resto de los datos que describen la topología de red circundante.

Haciendo referencia a la Figura 10, el proceso de envío de una interrogación y/o una alarma comienza en la etapa

(1010), y progresa a la etapa (1020) en la que se efectúa el proceso de toma de contacto a y desde el servidor de interrogación (60). En la etapa (1030) el gestor de conexiones (2) determina si la transmisión ha sido satisfactoria, que si lo ha sido el proceso avanza a la etapa (1090) en la que se registra la BER y el proceso finaliza en la etapa (1100). Si en la etapa (1030) se determinó que la transmisión no ha sido satisfactoria, el proceso avanza a la etapa (1040) que se determina si el número de interrogaciones es menor que o igual al valor de Recuento de Fallos de Registro, y si es que no el proceso avanza a la etapa (1050) en la que se toma una decisión de salto a, analizada en relación con la Figura 7, después de la cual el proceso se detiene en la etapa (1060). En la etapa (1040) si se determinó que el número de interrogaciones de latido, y un retorno de toma de contacto fallido asociado, era menor que el valor de Recuento de Fallos de Registro el proceso avanza a la etapa (1070) en la que el gestor de conexiones (2) determina si el módulo de radio (403) está operando dentro de tiempos recomendados como se requiere por el operador de red, y si es que no el proceso vuelve a la etapa (1020), mientras que si los tiempos están dentro de los límites, el proceso avanza a la etapa (1080) en la que se efectúa actualización de PDP como se ha analizado con respecto a la Figura 9 comenzando desde la etapa (910). Después de la etapa (1080) el proceso vuelve a la etapa (1020).

En una realización alternativas a la mostrada en la Figura 1b, un dispositivo de interfaz (15) se intercala entre el dispositivo de alarma (10) y una red de radio (30) [como se muestra en la Figura 1a], y/o un dispositivo de interfaz (15) se intercala al dispositivo de alarma (10) y una PSTN (20). En estas realizaciones adicionales alternativas, el dispositivo de interfaz (15) proporciona comunicación entre el dispositivo de alarma (10) y un dispositivo de recepción remoto a través de la red de radio (30) y/o PSTN (20) y explica retardos de transmisión de extremo a extremo impredecibles, que de otra manera para comunicación de acuerdo con el protocolo de Formato Rápido DTMF conduciría a errores de transmisión. La operación de un dispositivo de interfaz (15) dentro de un sistema de señalización de alarma (1) que comprende al menos parte de una PSTN se ha descrito en la patente GB2465833B, a los presentes solicitantes que se incorpora por referencia. El experto entenderá que el dispositivo de interfaz (15) que proporciona comunicación a través de una PSTN (20) de acuerdo con el protocolo de Formato Rápido DTMF, puede modificarse para proporcionar comunicación a través de una red de radio (30) de acuerdo con el Formato Rápido DTMF a través de provisión de un módulo de radio y antena y procesamiento de electrónica asociado para transmisión de radio de acuerdo con el Formato Rápido DTMF.

El dispositivo de interfaz (15) como se analiza en estas realizaciones alternativas y alternativas adicionales no se analizará más en este punto, y se dirige al experto a los contenidos en el documento GB2465833B a los presente solicitantes para implementar tal dispositivo de interfaz (15) dentro de estas realizaciones.

En una realización alternativa adicional, en la que el dispositivo de alarma (10) se retroadapta a un dispositivo de alarma adicional (450), se envían mensajes de alarma desde el dispositivo de alarma adicional (450) a un ARC a través de una conexión de comunicación proporcionada por la red de radio (30) o por la PSTN (20).

En el caso de que la información indica que se ha cumplido una condición de alarma y uno cualquiera de la pasarela de alarma (70), el servidor de interrogación primario (60) o centro de operaciones (80) es el destino final para la información, el uno de la pasarela de alarma (70), el servidor de interrogación primario (60) o centro de operaciones (80) reenvía la información al ARC (50). Como anteriormente, el ARC (50) puede informar, a continuación, a la persona responsable apropiada para que puedan tomar una acción.

El dispositivo de alarma (10) puede ser una unidad de alarma contra incendios, una unidad de alarma contra intrusos doméstica o comercial, una unidad de alarma personal o un dispositivo médico tal como el usado para alarmas dispersas y/o comunicadores personales. El experto apreciará que el dispositivo de alarma (10) puede usarse en otras soluciones de notificación de información de alarma, seguridad, salud u otra información crítica.

Características de las realizaciones descritas y mostradas en las figuras pueden combinarse en cualquier combinación, como se entendería por el lector experto como practicables.

El alcance de la presente divulgación no pretende limitarse a ninguna realización particular descrita, sino que en su lugar se define mediante las reivindicaciones adjuntas.

**REIVINDICACIONES**

1. Un método de operación de un dispositivo de alarma (10) dispuesto para transmitir una señal de alarma indicativa de que se ha cumplido una condición de alarma, comprendiendo el método las etapas del dispositivo (10):

acceder a un registro de una tabla de redes de redes celulares (404) disponibles para el dispositivo (10) para comunicación con las mismas, comprendiendo el registro información que identifica cada una de las redes y una medida de la fiabilidad de comunicación a través de cada red, en el que tras la determinación por el dispositivo (10) de que la medida de la fiabilidad de comunicación a una red a la que el dispositivo ha establecido un enlace de comunicaciones ha caído por debajo de un nivel predeterminado, finalizar ese enlace de comunicaciones, en el que la medida de la fiabilidad de comunicación a través de cada red comprende un valor de Calidad de Señal de Célula "CSQ";
seleccionar otra red con la que establecer un enlace de comunicación, siendo esa otra red la red para la que la medida de la fiabilidad de comunicación es la siguiente más alta en la tabla de redes (404); e intentar establecer un enlace de comunicaciones con la red seleccionada;
en el que la tabla de redes se clasifica sobre la base de Calidad de Señal de Célula "CSQ", número de células "Célula" y Tasa de Errores de Bits "BER" de acuerdo con:

$$(CSQ \times K_{csq}) + (Célula \times K_{célula}) + (BER \times K_{ber});$$

en la que $K_{csq}$, $K_{célula}$ y $K_{ber}$ son coeficientes asociados con los parámetros CSQ, Célula y BER, y se proporcionan remotamente desde un centro de operaciones (80).

2. Un método de acuerdo con la reivindicación 1 y que comprende la etapa del dispositivo (10) que efectúa un sondeo de redes celulares disponibles para el dispositivo para comunicación con las mismas para rellenar la tabla de redes con la información contenida en las mismas.

3. Un método de acuerdo con la reivindicación 2, en el que el sondeo se efectúa en el encendido del dispositivo (10), en respuesta a una señal recibida en el dispositivo desde una ubicación remota, en una planificación predeterminada o en respuesta a una entrada manual en el dispositivo (10) desde un usuario.

4. Un método de acuerdo con la reivindicación 1, en el que la determinación se basa en una medida actualizada de la fiabilidad de comunicación a través de la red a la que el dispositivo (10) ha establecido un enlace de comunicaciones, la medida actualizada obtenida durante la comunicación a través de ese enlace establecido.

5. Un método de acuerdo con la reivindicación 4, en el que la determinación se basa en la determinación de que un número predeterminado de medidas actualizadas están por debajo del nivel predeterminado.

6. Un método de acuerdo con la reivindicación 5, en el que la comunicación a través del enlace establecido por el que se obtiene la medida actualizada comprende que el dispositivo (10) envíe una señal de interrogación periódica desde el dispositivo a una ubicación remota y que el dispositivo (10) reciba desde la ubicación remota una señal de toma de contacto indicativa de que se ha recibido la señal de interrogación en la ubicación remota.

7. Un método de acuerdo con la reivindicación 6, en el que tras no recibir una toma de contacto esperada, finalizar el enlace establecido y seleccionar otra red a la que conectarse, siendo esa otra red la red para la que la medida de la fiabilidad de comunicación es la siguiente más alta.

8. Un método de acuerdo con cualquier reivindicación anterior, en el que después de que el dispositivo ha establecido un enlace de comunicaciones a través de una red que no es una red preferida predeterminada, finalizar periódicamente ese enlace e intentar establecer un enlace a través de la red preferida si la medida de fiabilidad de comunicación a través de esa red preferida es mayor que el nivel predeterminado.

9. Un método de acuerdo con la reivindicación 8, en el que después de finalizar en enlace, el dispositivo (10) intenta conectarse a la red preferida predeterminada si la medida de fiabilidad de comunicación a través de esa red preferida es mayor que el nivel predeterminado.

10. Un método de acuerdo con cualquier reivindicación anterior, en el que el método comprende que el dispositivo (10) no haga más de un número predeterminado de intentos repetidos para conectarse a la red seleccionada si fallan los intentos anteriores para conectarse a la red seleccionada.

11. Un método de acuerdo con cualquier reivindicación anterior y que comprende la etapa de, después de finalizar un enlace de comunicaciones a través de una red, el dispositivo (10) actuando en una señal que tiene que bloquearse en una red particular intentando establecer un enlace de comunicaciones con esa red y no intentando establecer un enlace de comunicaciones con otra red al menos hasta que se recibe una señal contraria.

12. Un dispositivo de alarma (10) que tiene medios adaptados para efectuar el método de una cualquiera de las

reivindicaciones anteriores.

13. Un dispositivo de alarma (10) de acuerdo con la reivindicación 12 y dispuesto para acoplarse a un dispositivo de generación de señales de alarma (60) para recibir una señal de alarma desde el mismo y para comunicar la señal de alarma a través de una red celular con la que el dispositivo de alarma (10) ha establecido un enlace de comunicaciones.

14. Medio legible por ordenador que comprende porciones de código ejecutables por medios de procesamiento de un dispositivo de alarma (10) para provocar que ese dispositivo efectúe un método de acuerdo con cualquiera de la reivindicación 1 a reivindicación 11.

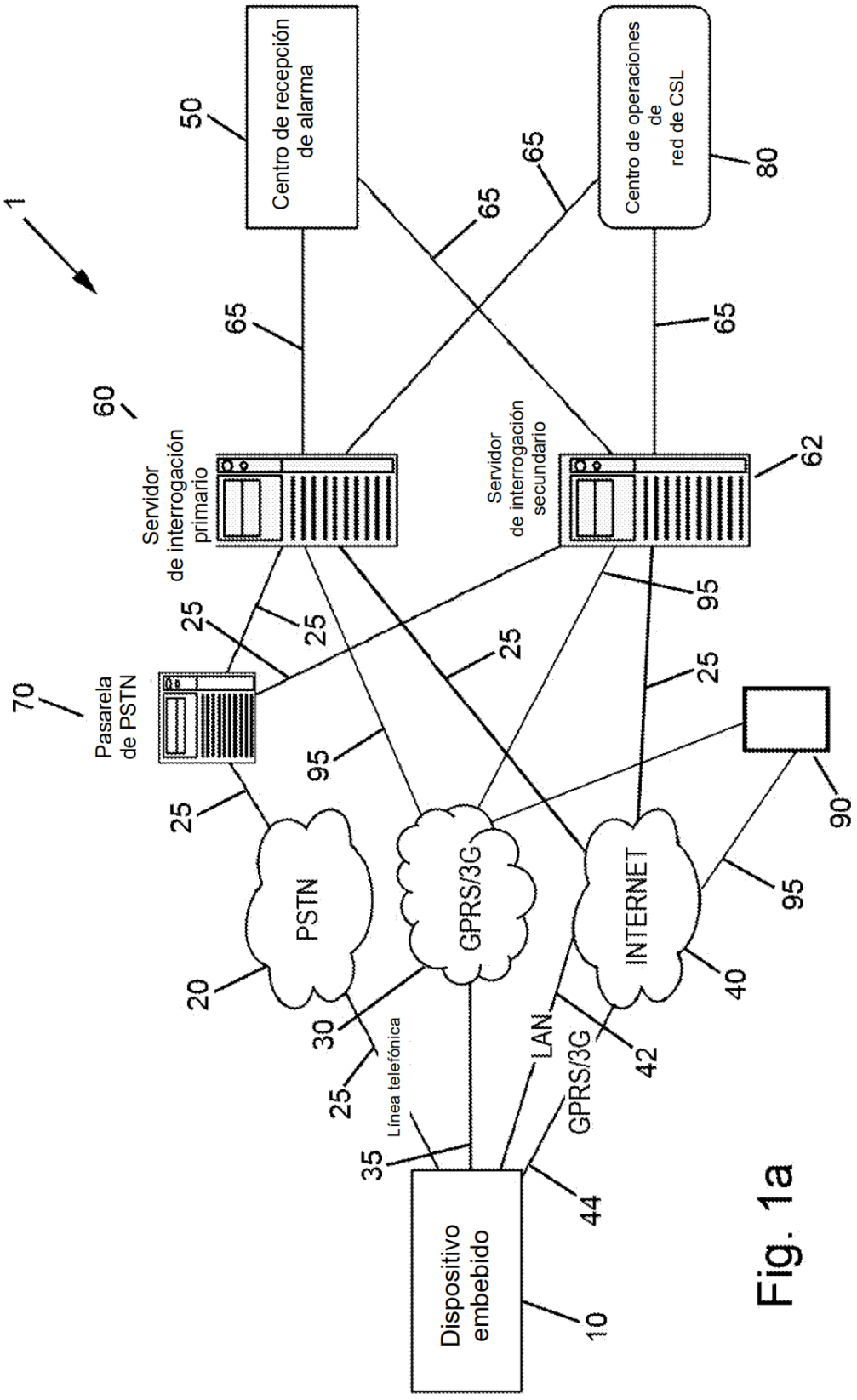
1
50
Centro de recepción de alarma
65
65
Centro de operaciones de red de CSL
80
65
65
60
Servidor de interrogación primario
Servidor de interrogación secundario
62
25
25
25
95
25
70
Pasarela de PSTN
95
25
90
PSTN
GPRS/3G
INTERNET
95
20
30
40
LAN
GPRS/3G
42
25
Línea telefónica
35
44
Dispositivo embebido
10

Fig. 1a

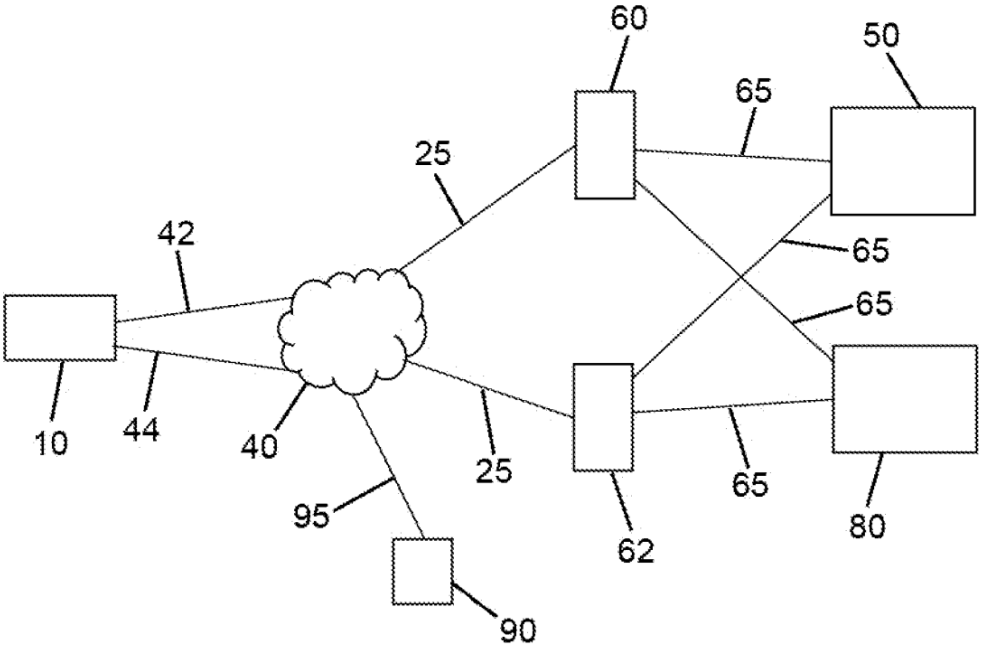


Fig. 1b

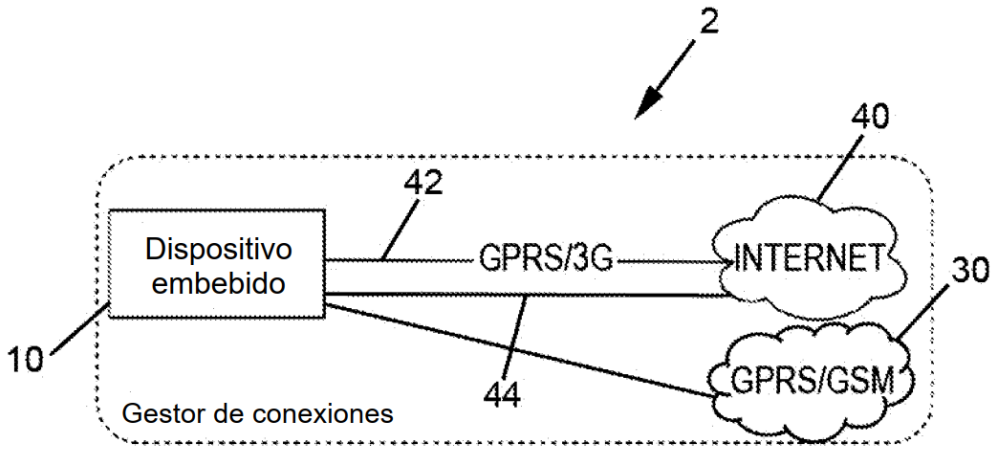
2
40
42
Dispositivo embebido
GPRS/3G
INTERNET
30
10
44
GPRS/GSM
Gestor de conexiones

Fig. 2a

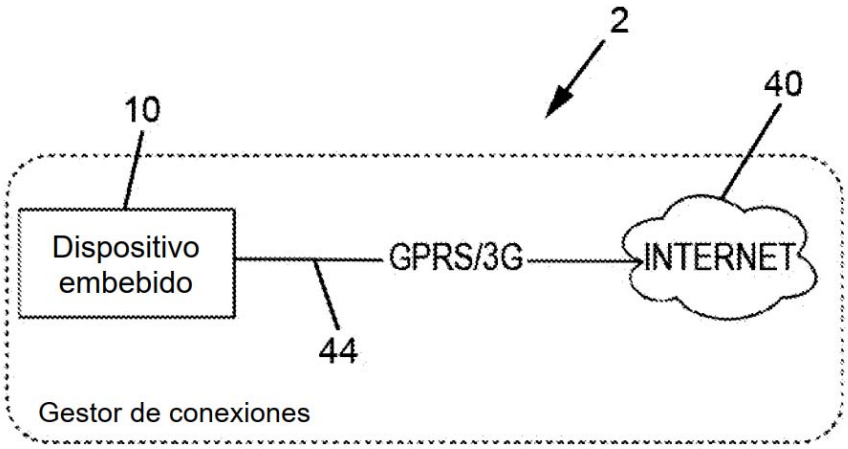
2
40
10
Dispositivo embebido
GPRS/3G
INTERNET
44
Gestor de conexiones

Fig. 2b

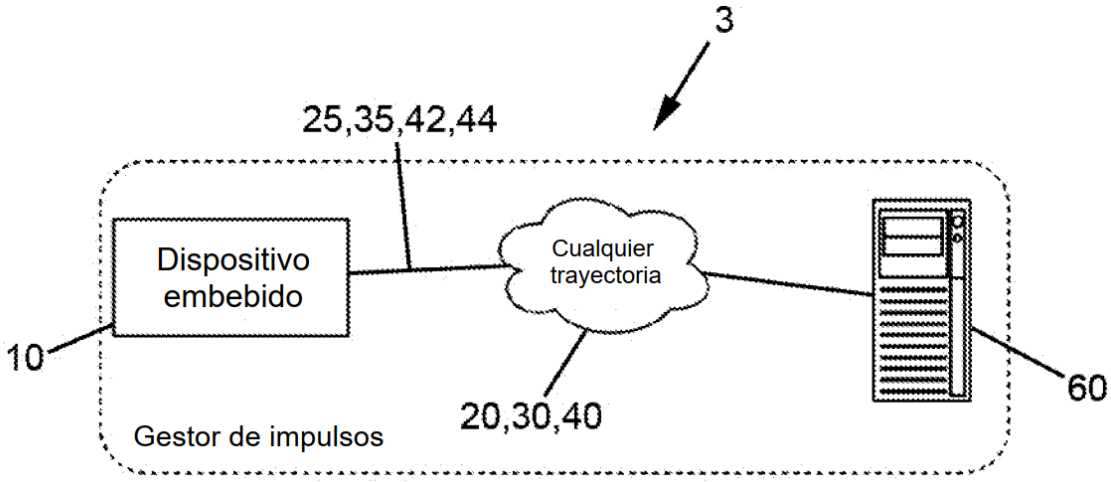
3
25,35,42,44
Dispositivo embebido
Cualquier trayectoria
10
20,30,40
60
Gestor de impulsos

Fig. 3a

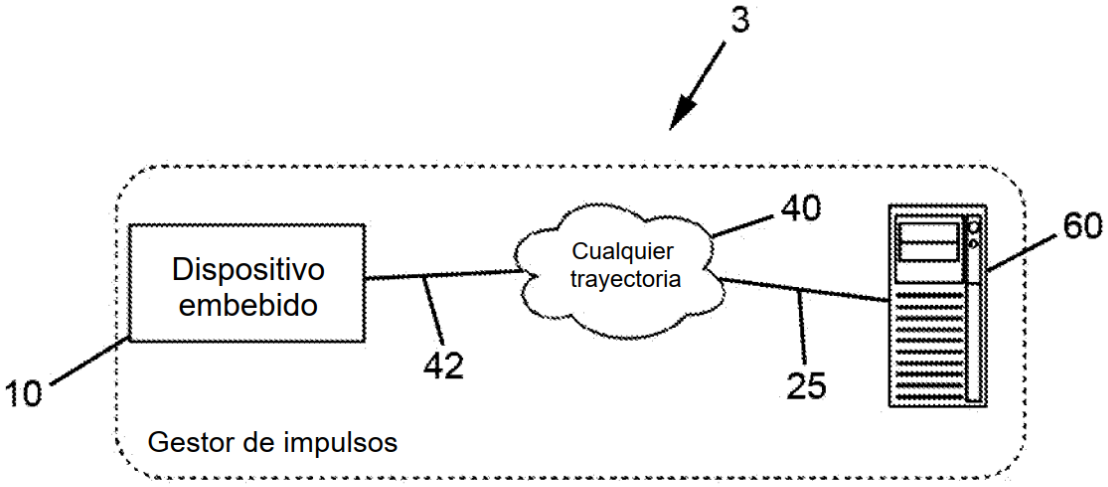
3
40
60
Dispositivo embebido
Cualquier trayectoria
42
25
10
Gestor de impulsos

Fig. 3b

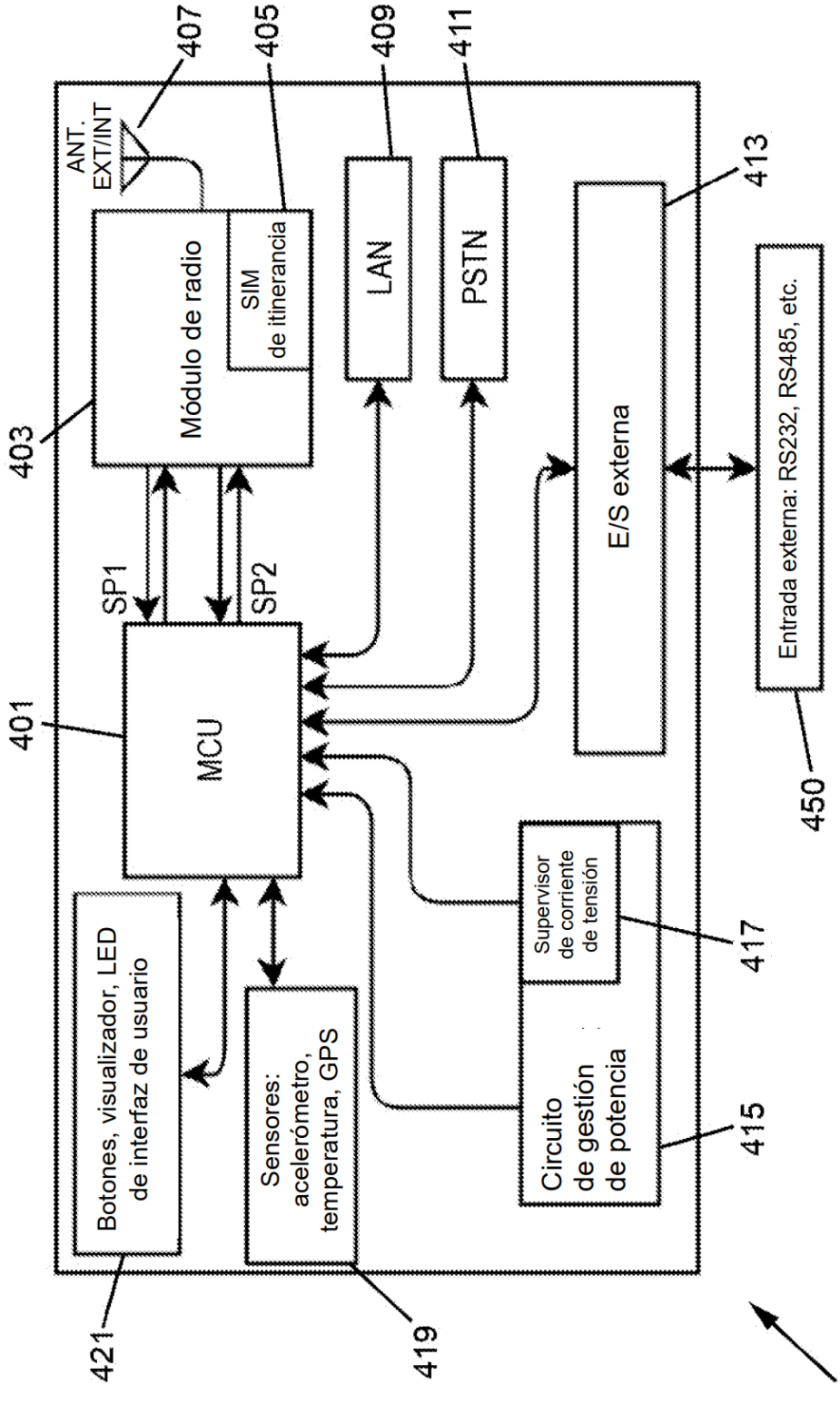
ANT. EXT/INT
407
405
409
411
413
403
Módulo de radio
SIM de itinerancia
LAN
PSTN
E/S externa
Entrada externa: RS232, RS485, etc.
450
SP1
SP2
401
MCU
Botones, visualizador, LED de interfaz de usuario
Sensores: acelerómetro, temperatura, GPS
Supervisor de corriente de tensión
Circuito de gestión de potencia
417
415
421
419
10

Fig. 4

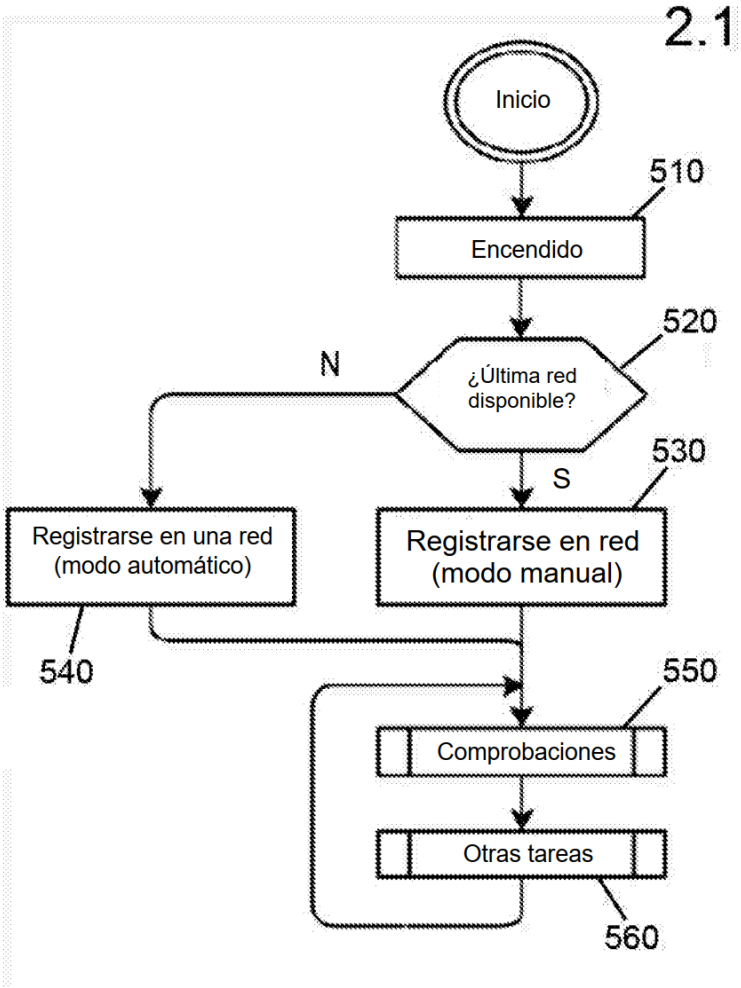
2.1
Inicio
510
Encendido
520
¿Última red disponible?
N
S
530
Registrarse en una red (modo automático)
Registrarse en red (modo manual)
540
550
Comprobaciones
Otras tareas
560

Fig. 5

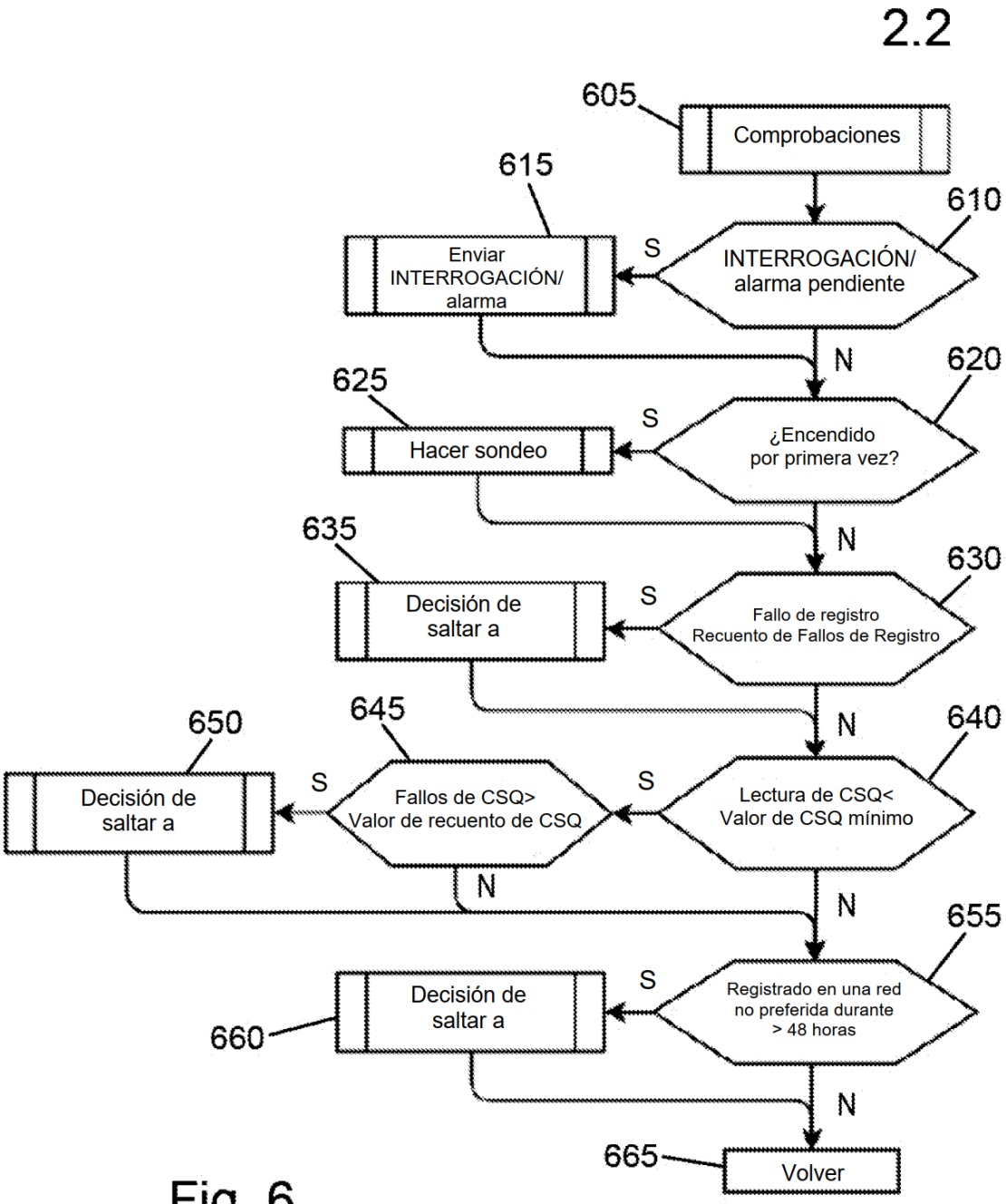
2.2
605
Comprobaciones
615
610
Enviar INTERROGACIÓN/ alarma
S
INTERROGACIÓN/ alarma pendiente
N
620
625
S
Hacer sondeo
¿Encendido por primera vez?
N
635
630
Decisión de saltar a
S
Fallo de registro Recuento de Fallos de Registro
N
650
645
640
Decisión de saltar a
S
Fallos de CSQ> Valor de recuento de CSQ
S
Lectura de CSQ< Valor de CSQ mínimo
N
N
655
Decisión de saltar a
660
S
Registrado en una red no preferida durante > 48 horas
N
665
Volver

Fig. 6

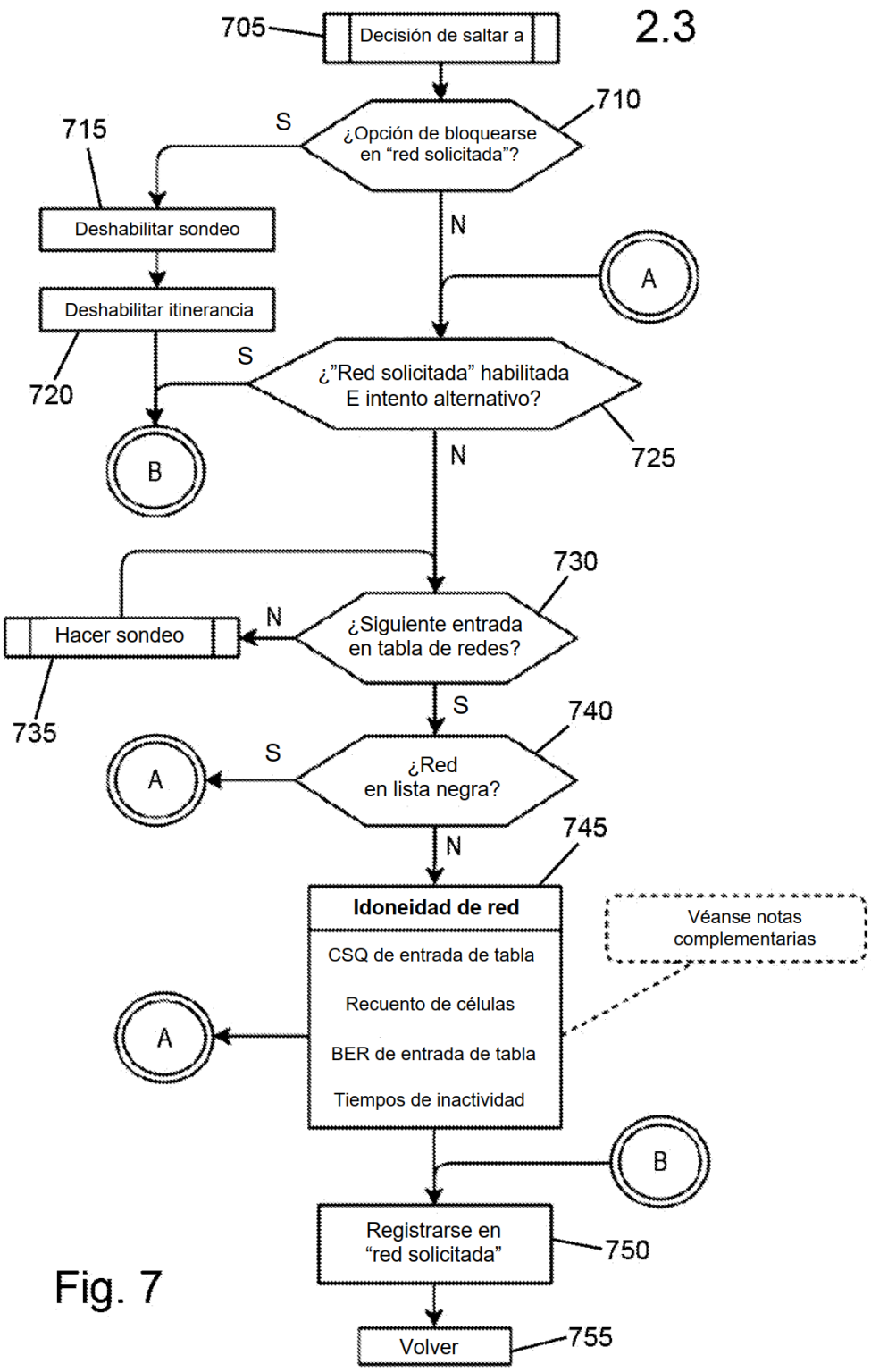
2.3
705
Decisión de saltar a
710
¿Opción de bloquearse en "red solicitada"?
S
715
Deshabilitar sondeo
Deshabilitar itinerancia
720
N
A
S
¿"Red solicitada" habilitada E intento alternativo?
725
B
N
730
¿Siguiente entrada en tabla de redes?
N
Hacer sondeo
735
S
740
¿Red en lista negra?
S
A
N
745
Idoneidad de red
CSQ de entrada de tabla
Recuento de células
BER de entrada de tabla
Tiempos de inactividad
Véanse notas complementarias
A
B
Registrarse en "red solicitada"
750
Volver
755

Fig. 7

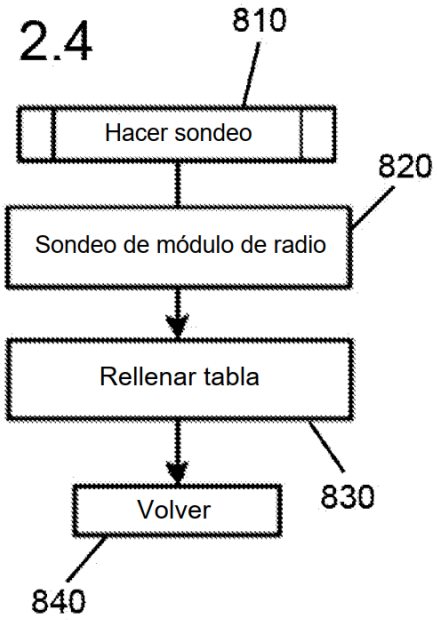
2.4
810
Hacer sondeo
820
Sondeo de módulo de radio
Rellenar tabla
830
Volver
840

Fig. 8

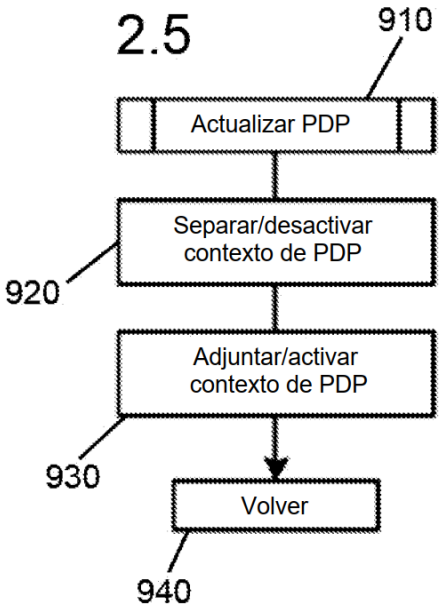
2.5
910
Actualizar PDP
Separar/desactivar contexto de PDP
920
Adjuntar/activar contexto de PDP
930
Volver
940

Fig. 9

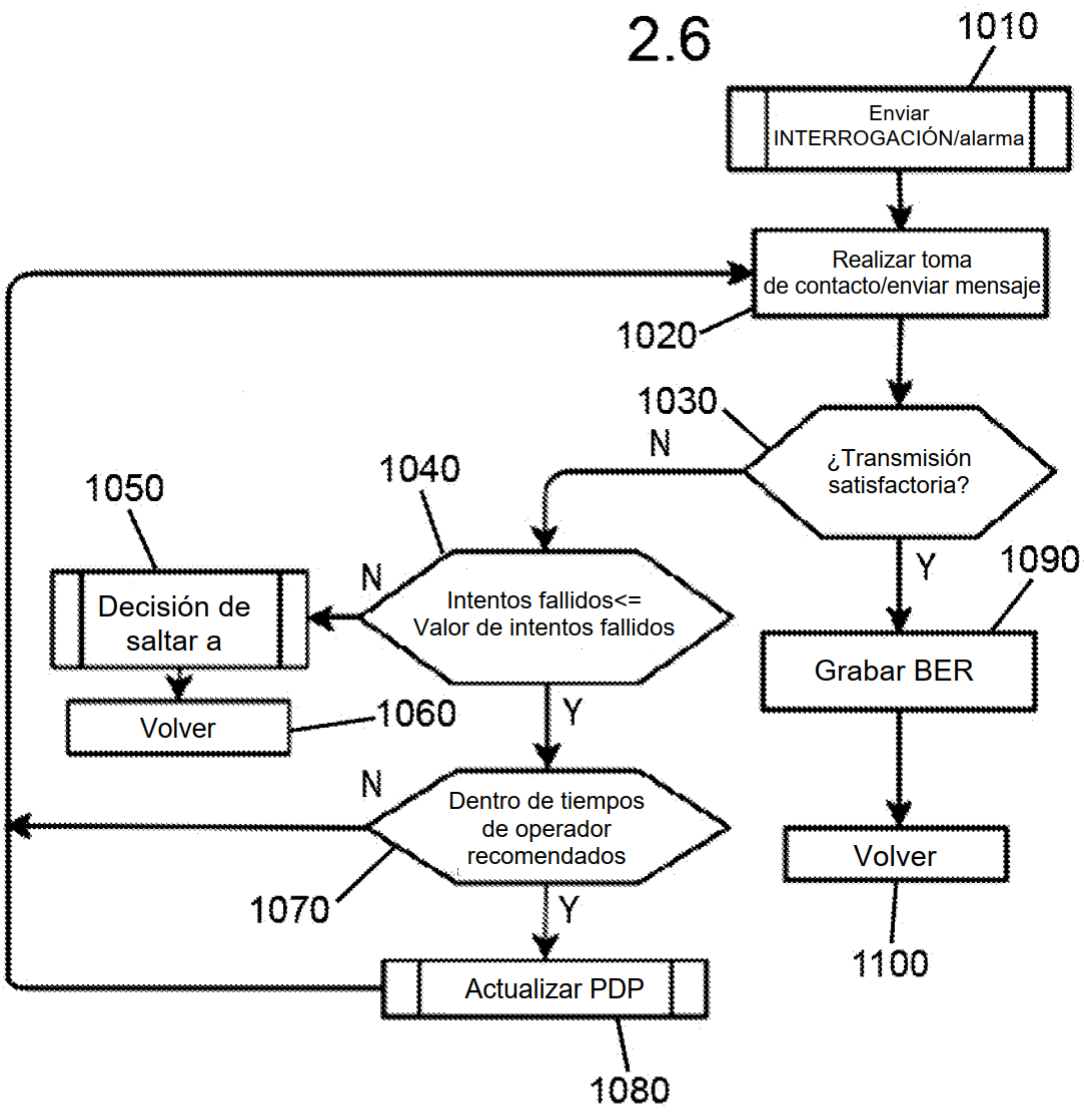
2.6
1010
Enviar INTERROGACIÓN/alarma
Realizar toma de contacto/enviar mensaje
1020
1030
N
¿Transmisión satisfactoria?
Y
1090
Grabar BER
Volver
1100
1040
N
Intentos fallidos<= Valor de intentos fallidos
1050
Decisión de saltar a
Volver
1060
Y
N
Dentro de tiempos de operador recomendados
1070
Y
Actualizar PDP
1080

Fig. 10

| RSSI | % de RSSI | Señal en dBM | 2G | 3G | Propiedad de red |
|---|---|---|---|---|---|
| 0 | 0 | -113 | Inutilizable | Inutilizable | Ninguna |
| 1 | 3 | -111 | Inutilizable | Inutilizable | |
| 2 | 6 | -109 | Inutilizable | Inutilizable | |
| 3 | 10 | -107 | Inutilizable | Inutilizable | |
| 4 | 13 | -105 | Solo SMS | Inutilizable | |
| 5 | 16 | -103 | Solo SMS | Inutilizable | |
| 6 | 19 | -101 | Solo SMS | Inutilizable | |
| 7 | 23 | -99 | Mala | Mala | Heterogénea |
| 8 | 26 | 97 | Mala | Mala | |
| 9 | 29 | -95 | Mala | Mala | |
| 10 | 32 | -93 | Mala | Mala | |
| 11 | 35 | -91 | Mala | Mala | |
| 12 | 39 | -89 | Buena | Buena | |
| 13 | 42 | -87 | Buena | Buena | |
| 14 | 45 | -85 | Buena+ | Buena | |
| 15 | 48 | -83 | Buena+ | Buena+ | |
| 16 | 52 | -81 | Buena+ | Buena+ | |
| 17 | 55 | -79 | Buena+ | Mejor | Homogénea |
| 18 | 58 | -77 | Mejor | Mejor | |
| 19 | 61 | -75 | Mejor | Mejor | |
| 20 | 65 | -73 | Mejor | Mejor | |
| 21 | 68 | -71 | Mejor | Mejor | |
| 22 | 71 | -69 | Mejor | Mejor | |
| 23 | 74 | -67 | Mejor | Mejor | |
| 24 | 77 | -65 | Mejor | Mejor | |
| 25 | 81 | -63 | Mejor | Mejor | |
| 26 | 84 | -61 | Mejor | Mejor | |
| 27 | 87 | -59 | Mejor | Mejor | |
| 28 | 90 | -57 | Mejor | Mejor | |
| 29 | 94 | -55 | Mejor | Mejor | |
| 30 | 97 | -53 | Mejor | Mejor | |
| 31 | 100 | -51< | Mejor | Mejor | |

Fig. 11