

DESCRIPCIÓN

Sistema de monitorización de seguridad

Campo técnico

La presente invención se refiere a un sistema de monitorización de seguridad para monitorizar locales, un dispositivo de autenticación portátil para
5 dicho sistema, y un procedimiento para operar dicho dispositivo de autenticación portátil.

Antecedentes

Los sistemas de monitorización de seguridad para monitorización de
10 locales, a menudo citados como sistemas de alarma, normalmente proporcionan unos medios para detectar la presencia y/o acciones de personas en las instalaciones, y reaccionan ante los eventos detectados. Comúnmente, tales sistemas incluyen sensores para detectar la apertura y el cierre de puertas y ventanas, detectores de movimiento para controlar espacios (tanto
15 dentro como fuera de edificios) en busca de signos de movimiento, micrófonos para detectar sonidos como cristales rotos y sensores de imagen para capturar imágenes fijas o en movimiento de zonas monitorizadas. Dichos sistemas pueden ser autónomos, con indicadores de alarma como sirenas y luces intermitentes que pueden activarse en caso de que se detecte una condición
20 de alarma. Dichas instalaciones incluyen normalmente una unidad de control (que también puede denominarse una unidad central), generalmente alimentada por la red, que está acoplada a los sensores, detectores, cámaras,

etc. ("nodos"), y que procesa notificaciones recibidas y determina una respuesta. La unidad central puede estar conectada a los distintos nodos mediante cables, pero cada vez más está conectada de forma inalámbrica, en lugar de por cables, ya que esto facilita la instalación y también puede proporcionar algunas garantías contra la desactivación efectiva de sensores/detectores al desconectarlos de la unidad central. De manera similar, para facilitar la instalación y mejorar la seguridad, los nodos de tales sistemas normalmente incluyen una fuente de alimentación autónoma, tal como una fuente de alimentación de batería, en lugar de ser alimentado por la red.

10 Como alternativa a los sistemas autónomos, un sistema de monitorización de seguridad puede incluir una instalación en un local, doméstico o comercial, que está vinculado a una Estación Central de Monitorización (CMS) donde, normalmente, los operadores humanos gestionan las respuestas requeridas por diferentes tipos de alarmas y notificaciones. En
15 tales sistemas monitorizados centralmente, la unidad central en la instalación del local normalmente procesa las notificaciones recibidas de los nodos en la instalación, y notifica a la Estación Central de Monitorización solo algunas de estas, dependiendo de la configuración del sistema y de la naturaleza de los eventos detectados. En tal configuración, la unidad central en la instalación
20 actúa efectivamente como una puerta de enlace entre los nodos y la estación central de monitorización. De nuevo, en tales instalaciones, la unidad central puede estar conectada por cables o de forma inalámbrica, a los diversos nodos

de la instalación, y estos nodos serán normalmente de batería en lugar de alimentación de red.

En ambos tipos de sistemas, la unidad central es normalmente responsable de armar y desarmar el sistema, pero no puede ubicarse cerca de una puerta de entrada. Cuando el dueño de la casa regresa a las instalaciones monitorizadas donde el sistema de monitorización está en estado armado, el sistema debe desarmarse con bastante rapidez, por ejemplo, dentro de los 30 segundos de abrir la puerta. Si la unidad central no se encuentra cerca de la puerta de entrada, puede ser difícil para el propietario llegar a la unidad central e ingresar a tiempo el código de desarmado, que generalmente puede tener de 4 a 6 caracteres o dígitos. Obviamente, esto plantea un desafío aun mayor para los ancianos o enfermos. Por esta razón, se sabe que se debe proporcionar una unidad cerca de la puerta de entrada por medio de la cual el propietario puede desarmar el sistema. Esta unidad, que puede denominarse un nodo de desarmado, se puede proporcionar dentro de las instalaciones protegidas cerca de cada entrada principal, pero en otras instalaciones solo la única entrada principal contara con un nodo de desarmado. El nodo de desarmado normalmente se fijará, por ejemplo, a una pared u otra superficie del local, cerca de la entrada relevante al edificio o espacio protegido. Algunas instalaciones pueden estar configuradas de manera que el sistema solo pueda armarse o desarmarse mediante un nodo de desarmado, la unidad central posiblemente ni siquiera incluye un teclado o funcionalidad NFC.

Aunque la provisión de un nodo de desarmado adyacente a la entrada a las instalaciones protegidas significa que el dueño de la casa no tenga que caminar hasta la unidad central para ingresar el código de desarmado, hay ocasiones en que es inconveniente tener que ingresar el código de desarmado

5 manualmente incluso a través de un nodo de desarmado. Por ejemplo, si el dueño de la casa lleva un bebé, paquetes, o está cargado de otra manera, o si el dueño de la casa está con muletas, aun puede ser extremadamente inconveniente tener que ingresar un código de desarmado manualmente. Y en tales circunstancias, puede ser extremadamente inconveniente para un usuario

10 tener que presentar un dispositivo de autenticación portátil o "llave electrónica" físicamente a un nodo de desarmado, por ejemplo, tocando el nodo de desarmado con la llave electrónica, dado que, al igual que ingresar manualmente un código de desarmado, esto requiere que el usuario tenga una mano "libre" para permitir que se presente la llave electrónica.

15 Sería deseable poder reducir o incluso eliminar este problema mientras se mantiene un alto nivel de seguridad.

Las realizaciones de la invención permiten el desarmado de manos libres de un sistema de monitorización de seguridad mientras se mantiene un alto nivel de seguridad. Es decir, las realizaciones de la invención proporcionan

20 un sistema en el que un usuario puede lograr un desarme seguro y apropiado con un dispositivo de autenticación portátil (por ejemplo, un mando u otra ficha física) sin la necesidad de que el usuario tome ninguna acción (que no sea

llevar el dispositivo de autenticación portátil en o sobre su persona).

Compendio de la invención

De acuerdo con un primer aspecto, la presente invención proporciona un dispositivo de autenticación portátil para su uso con un sistema de monitorización de seguridad para un edificio o un espacio seguro dentro de un edificio u otra propiedad fija, incluyendo el sistema:

una unidad de control para controlar, armar y desarmar el sistema de monitorización de seguridad;

un detector para detectar la irrupción de una entrada que da acceso al edificio o al espacio seguro;

un nodo de desarmado para desarmar el sistema, teniendo el nodo de desarmado una interfaz de usuario para recibir una entrada de usuario para desarmar el sistema, y un transmisor de radiofrecuencia para transmitir, como consecuencia de la entrada del usuario, una señal de desarmado a la unidad de control;

comprendiendo el dispositivo de autenticación portátil:

un transceptor de radiofrecuencia,

una memoria que almacena una identificación de dispositivo de autenticación portátil,

un sensor de movimiento

y un procesador conectado operativamente al transceptor, el sensor de movimiento y la memoria;

en el que el sensor de movimiento está configurado para detectar el movimiento del dispositivo de autenticación portátil y para proporcionar una salida basada en el movimiento detectado del dispositivo de autenticación portátil, y en el que el procesador está configurado para determinar si el
5 dispositivo de autenticación portátil es estacionario o está en movimiento, basado en la salida del sensor de movimiento;

en el que el dispositivo de autenticación portátil está configurado para recibir una instrucción de desarmado, a través del transceptor desde el nodo de desarmado para transmitir a la unidad de control una solicitud de desarmado
10 que contiene la identificación del dispositivo de autenticación portátil; y en el que el procesador está configurado para transmitir la solicitud de desarmado instruida solo si, cuando se recibe la instrucción, el dispositivo de autenticación portátil no se considera estacionario.

La conveniencia del usuario mejora con respecto a los sistemas
15 conocidos al proporcionar un dispositivo de autenticación portátil que permite el desarmado con manos libres, y al incluir un sensor de movimiento y hacer que el dispositivo de autenticación portátil solo proporcione el mensaje de desarme instruido si, cuando se recibe la instrucción, el dispositivo de autenticación portátil no se considera estacionario, la seguridad se mejora porque queda un
20 dispositivo de autenticación portátil cerca del nodo de desarmado, en lugar de ser llevado por alguien que abre la puerta, no transmitirá un mensaje de desarmado a la unidad de control. Esto significa que si un mal actor abre la

puerta para ingresar al espacio seguro, el sistema no se desarmara automáticamente como consecuencia de que un dispositivo de autenticación portátil se haya dejado cerca del nodo de desarmado correspondiente.

Preferentemente, el dispositivo de autenticación portátil está configurado para transmitir a la unidad de control la solicitud de desarmado que incluye un
5 identificador de transmisión de desarmado recibido en la instrucción de desarmado desde el nodo de desarmado. Al cambiar el identificador de transmisión de desarmado entre eventos de desarmado, es más difícil para los malos actores engañar al sistema. Los identificadores de transmisión de
10 desarmado pueden, por ejemplo, ser números aleatorios o pueden seleccionarse de un gran conjunto de números y variar entre cada evento de desarmado. De esta manera, se mejora la seguridad del sistema frente, por ejemplo, a la reproducción de una grabación de una transmisión auténtica.

Un dispositivo de autenticación portátil de acuerdo con el primer aspecto
15 puede considerarse estacionario si el sensor de movimiento no detecta movimiento en el momento en que se recibe la instrucción.

Como alternativa, un dispositivo de autenticación portátil de acuerdo con el primer aspecto puede considerarse estacionario si el sensor de movimiento no ha detectado movimiento del dispositivo de autenticación portátil durante un
20 período predeterminado que precede al momento en que se recibe la instrucción.

Un dispositivo de autenticación portátil de acuerdo con el primer aspecto

puede configurarse adicionalmente para recibir una instrucción que no sea una instrucción de desarmado a través del transceptor, incluyendo un indicador, desde la unidad de control para realizar una acción; y en el que en el caso de que la otra instrucción incluya el indicador, el procesador está configurado para
5 hacer que el dispositivo de autenticación portátil realice la acción indicada, independientemente de si, cuando se recibe la instrucción, se determina que el dispositivo de autenticación portátil es estacionario.

Los dispositivos de autenticación portátiles configurados de esta manera pueden activarse mediante una señal de RF, desde la unidad de control o
10 desde un nodo de desarmado, permitiendo verificar y/o actualizar el estado de todos los dispositivos de autenticación portátiles dentro del alcance. También sería posible realizar una auditoria de todos los dispositivos de autenticación portátiles en el rango de, digamos, la unidad de control. Si un dispositivo de autenticación portátil de este tipo incluyera uno o más indicadores visuales, un
15 transductor de audio, un transductor háptico, y se configuraran para generar una salida usando uno o más de estos cuando así lo indique una instrucción recibida que incluye el indicador, se podría hacer que un dispositivo de autenticación portátil perdido se anunciara.

Un dispositivo de autenticación portátil de acuerdo con el primer aspecto
20 puede tener su procesador configurado para que deje de generar un recuento del tiempo transcurrido desde que el dispositivo de autenticación portátil estuvo en movimiento por última vez después de que el recuento del tiempo desde

que el dispositivo de autenticación portátil estuvo en movimiento por última vez alcance un valor umbral predeterminado. Es decir, el procesador puede dejar de contar una vez que se alcanza un umbral predeterminado, o puede haber otro, umbral superior que determina cuando el procesador deja de contar. Esto
5 ayuda a reducir el consumo de energía del procesador, lo cual es beneficioso para la duración de la batería.

Cualquiera de estos dispositivos de autenticación portátiles podría configurarse para recibir la instrucción de desarmado en un primer canal de radio, incluyendo la instrucción de desarmado instrucciones para transmitir el
10 mensaje de desarme que contiene el identificador de transmisión de desarmado (si se usa) y la ID del dispositivo de autenticación portátil en un segundo canal de radio cuyos parámetros de transmisión son diferentes de los del primer canal de radio y se especifican en las instrucciones recibidas; y para controlar el transceptor para transmitir el mensaje que contiene el identificador
15 de transmisión (si se usa) y la ID del dispositivo de autenticación portátil en el segundo canal de radio usando los parámetros de transmisión especificados.

Al disponer el dispositivo de autenticación portátil para enviar el mensaje que contiene el identificador de transmisión de desarme (si se usa) y la ID del dispositivo de autenticación portátil en el segundo canal de radio en un canal
20 cuyos parámetros de transmisión especificados difieren de aquellos en los que se recibió el mensaje de instrucción de desarme, y que se especifican en las instrucciones de la unidad de control, es mas difícil para los malos actores

hacerse pasar por un dispositivo de autenticación portátil válido y, por lo tanto, se mejora la seguridad del sistema.

De acuerdo con un segundo aspecto, la presente invención proporciona un sistema de monitorización de seguridad para un edificio o un espacio seguro
5 dentro de un edificio u otra propiedad fija, incluyendo el sistema:

un detector para detectar la irrupción de una entrada que da acceso al edificio o al espacio seguro;

una unidad de control;

un nodo de desarmado para desarmar el sistema, teniendo el nodo una
10 interfaz de usuario para recibir una entrada de usuario para desarmar el sistema, y un transmisor de radiofrecuencia para transmitir, como consecuencia de la entrada del usuario, una señal de desarmado a la unidad de control;

y un dispositivo de autenticación portátil de acuerdo con el primer
15 aspecto para permitir el desarmado con manos libres del sistema de monitorización de seguridad;

teniendo la unidad de control un transceptor de radiofrecuencia y una memoria que almacena una identidad de dispositivo de autenticación portátil para el dispositivo de autenticación portátil;

20 estando la unidad de control configurada:

en respuesta a recibir una notificación de una irrupción de entrada del detector, para:

- (i) iniciar un temporizador de período de entrada;
- (ii) transmitir un mensaje de activación al nodo de desarmado para que el transmisor RF del nodo de desarmado transmita una señal/baliza de activación para activar el dispositivo de autenticación portátil; y
- 5 (iii) en respuesta a la recepción, antes de que expire el temporizador del período de entrada, una señal de desarmado de radiofrecuencia del dispositivo de autenticación portátil que incluye la identidad registrada del dispositivo de autenticación portátil, para desarmar el sistema de monitorización de seguridad; y
- 10 (iv) en caso de que el sistema de monitorización de seguridad no este desarmado antes de que expire el período de entrada, hacer que el sistema de monitorización de seguridad entre en un estado de alarma;
- (v) en el que, adicionalmente: la unidad de control está configurada para iniciar un temporizador de desarmado de manos libres en respuesta a la
- 15 recepción de una notificación de irrupción de entrada del detector, y en el caso de que no se reciba ninguna señal de RF que incluya la identidad del dispositivo de autenticación portátil registrado antes de que expire el temporizador de desarmado de manos libres, transmitir una señal al nodo para hacer que el nodo proporcione una notificación en el sentido de que el intento
- 20 de desarme con manos libres ha fallado; o
- (vi) el nodo de desarmado está configurado para iniciar su propio temporizador de desarmado de manos libres en respuesta a la recepción del

mensaje de activación de la unidad de control, y, en el caso de que el temporizador de desarme de manos libres del nodo desarme expire sin que la unidad de control haya informado al nodo de desarmado del sistema de monitorización de seguridad, para proporcionar una notificación en el sentido
5 de que el intento de desarme con manos libres ha fallado.

Tal sistema de monitorización de seguridad proporciona comodidad al usuario al tiempo que permite la provisión de un alto nivel de seguridad del sistema.

En el sistema de monitorización de seguridad de acuerdo con el
10 segundo aspecto de la invención, la unidad de control puede configurarse para:

incluir un identificador de transmisión de desarme en el mensaje de activación, y el mensaje de activación está dispuesto para hacer que el nodo de desarmado incluya el identificador de transmisión de desarme en la señal/baliza de activación transmitida desde el transmisor de RF del nodo de
15 desarmado;

solo desarmar el sistema de monitorización de seguridad en respuesta a la recepción antes de la expiración del temporizador del período de entrada de una señal de desarmado de radiofrecuencia que incluye la identidad del dispositivo de autenticación portátil registrada del dispositivo de autenticación
20 portátil si la señal de desarmado también incluye el identificador de transmisión de desarmado; y

en el caso de que la unidad de control este configurada para iniciar un

temporizador de desarmado de manos libres, para transmitir una señal que haga que el nodo de desarmado proporcione una notificación en el sentido de que el intento de desarme con manos libres ha fallado solo si no se recibe ninguna señal de RF que incluya la identidad del dispositivo de autenticación portátil registrado y el identificador de transmisión de desarme antes de que expire el temporizador de desarme con manos libres. Al cambiar el identificador de transmisión de desarmado entre eventos de desarmado, es más difícil para los malos actores engañar al sistema. Los identificadores de transmisión de desarmado pueden, por ejemplo, ser números aleatorios o pueden seleccionarse de un gran conjunto de números y variar entre cada evento de desarmado. De esta manera, se mejora la seguridad del sistema.

En los sistemas de monitorización de seguridad según el segundo aspecto, el dispositivo de autenticación portátil puede considerarse estacionario si el sensor de movimiento no detecta movimiento en el momento en que se recibe la instrucción.

Como alternativa, en los sistemas de monitorización de seguridad de acuerdo con el segundo aspecto, el dispositivo de autenticación portátil puede considerarse estacionario si el sensor de movimiento no ha detectado movimiento del dispositivo de autenticación portátil durante un período predeterminado que precede al momento en que se recibe la instrucción.

En los sistemas de monitorización de seguridad según el segundo aspecto, el dispositivo de autenticación portátil puede tener su procesador

configurado para que deje de generar un recuento del tiempo transcurrido desde que el dispositivo de autenticación portátil estuvo en movimiento por ultima vez después del recuento del tiempo desde la ultima vez que el dispositivo de autenticación portátil estuvo en movimiento alcanza un valor umbral predeterminado. Es decir, el procesador del dispositivo de autenticación portátil puede dejar de contar una vez que se alcanza el umbral predeterminado, o puede haber otro, umbral superior que determina cuando el procesador deja de contar. Esto ayuda a reducir el consumo de energía del procesador, lo cual es beneficioso para la duración de la batería.

10 Un sistema de monitorización de seguridad de acuerdo con el segundo aspecto de la invención puede incluir múltiples nodos de desarmado, cada uno asociado a diferentes entradas que dan acceso al edificio o al espacio seguro, cada nodo de desarmado tiene una ID de nodo de desarmado única, cada una de las diferentes entradas tiene un detector respectivo con una ID respectiva
15 diferente, y la unidad de control almacena las ID del nodo de desarmado, las ID del detector y una asociación entre cada detector y uno asociado de los nodos de desarmado; en el que la unidad de control se configura, en respuesta a recibir un mensaje de irrupción de entrada desde un detector, para usar un identificador de detector incluido en el mensaje recibido para identificar el nodo
20 de desarmado asociado e incluir el identificador de nodo de desarmado para el nodo de desarmado identificado en el mensaje de activación transmitido para apuntar selectivamente al nodo de desarmado identificado entre los múltiples

nodos de desarmado del sistema.

La selección selectiva del nodo de desarmado asociado a la entrada cuya irrupción se ha detectado mejora la seguridad al garantizar que el desarme no sea causado por la presencia de un dispositivo de autenticación portátil en proximidad de algún otro nodo de desarmado.

De acuerdo con un tercer aspecto, la presente invención proporciona un procedimiento de funcionamiento de un dispositivo de autenticación portátil para su uso con un sistema de monitorización de seguridad para un edificio o un espacio seguro dentro de un edificio u otra propiedad fija, incluyendo el sistema: una unidad de control para controlar, armar y desarmar el sistema de monitorización de seguridad; un detector para detectar la irrupción de una entrada que da acceso al edificio o al espacio seguro; un nodo de desarmado para desarmar el sistema, teniendo el nodo de desarmado una interfaz de usuario para recibir una entrada de usuario para desarmar el sistema, y un transmisor de radiofrecuencia para transmitir, como consecuencia de la entrada del usuario, una señal de desarmado a la unidad de control;

el dispositivo de autenticación portátil comprende: un transceptor de radiofrecuencia, una memoria que almacena una identificación de dispositivo de autenticación portátil,

un sensor de movimiento y un procesador conectado operativamente al transceptor, el sensor de movimiento y la memoria; comprendiendo el procedimiento: usar el sensor de movimiento para detectar el movimiento del

dispositivo de autenticación portátil;

proporcionar una salida basada en el movimiento detectado del dispositivo de autenticación portátil; determinar, usando el procesador, si el dispositivo de autenticación portátil es estacionario o está en movimiento,

5 basado en la salida del sensor de movimiento;

proporcionar una salida basada en el movimiento detectado del dispositivo de autenticación portátil;

determinar, usando el procesador, si el dispositivo de autenticación portátil es estacionario o está en movimiento, basado en la salida del sensor de

10 movimiento;

recibir una instrucción de desarmado, a través del transceptor, desde el nodo de desarmado para transmitir a la unidad de control una solicitud de desarmado que contiene la ID del dispositivo de autenticación portátil; y cuando se recibe la instrucción, determinar si el dispositivo de autenticación portátil se

15 considera estacionario;

y, solo si el dispositivo de autenticación portátil se considera no estacionario, transmitir la solicitud instruida.

En el procedimiento de acuerdo con el tercer aspecto, la instrucción de desarmado recibida por el transceptor incluye un identificador de transmisión de desarmado y una instrucción para incluir el identificador de transmisión de desarmado en la solicitud de desarmado. Al cambiar el identificador de transmisión de desarmado entre eventos de desarmado, es más difícil para los

20

malos actores engañar al sistema. Los identificadores de transmisión de desarmado pueden, por ejemplo, ser números aleatorios o pueden seleccionarse de un gran conjunto de números y variar entre cada evento de desarmado. De esta manera, se mejora la seguridad del sistema.

- 5 En el procedimiento de acuerdo con el tercer aspecto, el dispositivo de autenticación portátil puede considerarse estacionario si el sensor de movimiento no detecta movimiento en el momento en que se recibe la instrucción.

 Como alternativa, en el procedimiento de acuerdo con el tercer aspecto,
10 el dispositivo de autenticación portátil puede considerarse estacionario si el sensor de movimiento no ha detectado movimiento del dispositivo de autenticación portátil durante un período predeterminado que precede al momento en que se recibe la instrucción.

 Para las diversas realizaciones de la presente invención, en muchas
15 instalaciones domésticas, todas las entradas monitorizadas pueden ser entradas equipadas con puertas, y monitorizar una irrupción puede implicar detectar la apertura de una puerta o el paso de una persona a través de una puerta. Pero algunas o todas las entradas monitorizadas pueden no incluir puertas u otros cierres, de modo que la detección de una irrupción puede
20 implicar el uso de un sensor de movimiento o visual para detectar la presencia o el movimiento de una persona en una entrada, tal como a través de un camino, pasillo u otra abertura.

Se describirán realizaciones preferidas de la invención ahora, a modo de ejemplo solamente, con referencia a los dibujos adjuntos, en los que:

La Figura 1 es una vista general de un sistema de monitorización de seguridad de acuerdo con un primer aspecto de la invención;

5 La Figura 2 es un dibujo esquemático que muestra un edificio estilizado en el que está instalado un sistema de monitorización de seguridad de acuerdo con una realización de la invención;

La Figura 3 es un diagrama de temporización que ilustra un procedimiento de control de un sistema de monitorización de seguridad de
10 acuerdo con una realización de la invención;

La Figura 4 es un dibujo esquemático que muestra características de elementos del sistema de monitorización de seguridad de acuerdo con una realización de la invención;

La Figura 5 es un diagrama de flujo que ilustra un aspecto del
15 funcionamiento de un dispositivo de autenticación portátil de acuerdo con una realización de la invención;

La Figura 6 es un dibujo esquemático que ilustra una disposición de elementos de un sistema de monitorización de seguridad de acuerdo con una realización de la invención;

20 La Figura 7 es un dibujo esquemático que ilustra el funcionamiento de la función del receptor del dispositivo de autenticación portátil y una posible estructura de paquetes para una transmisión desde un nodo de desarmado; y

Las Figuras 8a y 8b son dibujos esquemáticos que ilustran un sistema de monitorización de seguridad de acuerdo con una realización de la invención en el que se proporciona un nodo de desarmado fuera de la zona o edificio protegido por el sistema.

5 **Descripción específica**

La Figura 1 es una vista general de un sistema de monitorización de seguridad de acuerdo con un primer aspecto de la invención. La figura muestra una vista en planta aproximada de una vivienda doméstica 110, que puede ser un edificio tal como una casa o un espacio seguro, tal como un departamento,
10 en un edificio y que está protegido por un sistema de vigilancia de seguridad 100. La vivienda tiene una puerta de entrada 120, en una puerta que es una entrada principal que da acceso al vestíbulo de entrada 125 del edificio o al espacio seguro. La puerta 120 está equipada con un sensor de puerta 130 para detectar la apertura de la puerta. El sensor de puerta 130 es normalmente,
15 pero no necesariamente, un interruptor de activación magnética que se instala en el lado de apertura de la puerta, opuesto al lado de la bisagra. Se apreciará que el sensor de la puerta es un ejemplo de un detector para detectar la irrupción de la entrada representada por la puerta. También se apreciará que la irrupción de una entrada también se puede detectar usando un sensor de
20 movimiento tal como un sensor PIR, una cámara de video u otro sensor de imagen, un sensor de presión montado en el suelo, o algún otro sensor de contacto o sin contacto, cualquiera de los cuales puede usarse para detectar la

irrupción de una entrada a un edificio, jardín, granja, etc., y que por lo tanto puede generar una señal de activación de alarma para indicar la irrupción de una entrada monitorizada.

El sensor de puerta 130 incluye un transmisor de RF, no mostrado, que
5 transmite una señal de irrupción de entrada a una unidad central 140 del sistema de monitorización 100 en caso de que se abra la puerta.

En esta instalación, el control o unidad central 140 está montado debajo de las escaleras 150 que conducen a un piso superior. La unidad de control incluye al menos un primer transceptor de RF para recibir transmisiones del
10 sensor de puerta y otros nodos del sistema. La unidad central se comunica con una estación de monitorización central 150 a través de una conexión por cable a través de un enlace de datos por cable 160 a una conexión de banda ancha 170 dentro de las instalaciones a Internet 180, o de forma inalámbrica, normalmente usando un segundo transceptor. La unidad de control también
15 puede comunicarse mediante una conexión Wi-Fi, por ejemplo, a un punto de acceso Wi-Fi que da acceso a Internet a través de una banda ancha u otro enlace de datos. Los primeros transceptores de RF para la comunicación con los nodos del sistema generalmente usaran una banda ISM (Científico y Médico Industrial), tal como la banda de 868 MHz en Europa. Los primeros
20 transceptores de RF también pueden ser compatibles con Bluetooth. El segundo transceptor, para la comunicación con la estación de monitorización central 150 también puede usar una banda ISM, como la banda de 868 MHz en

Europa, pero también puede usar una red móvil (PLMN) como GSM 3G, 4G o UMTS. Preferentemente, la unidad central 140 tiene varias formas de comunicarse con la estación de monitorización central 150, de modo que incluso si una ruta está atascada o no está disponible, la unidad central aun
5 puede informar y recibir comunicaciones de, la estación de monitorización central.

La residencia de la Figura 1 incluye varias habitaciones 190, 200, 210, además del vestíbulo de entrada 125. Las habitaciones 190 y 200 conducen al hall de entrada y tienen ventanas 240, pero no puertas exteriores.
10 Normalmente, todas las ventanas estarán provistas de uno o más sensores 245 para detectar la apertura de la ventana, rotura del vidrio, manipulación indebida o similar. La habitación 210 es una cocina y comedor combinados que tiene una puerta 220 de entrada externa, que también está equipada con un sensor de puerta 230. El comedor 210 de la cocina también tiene una fila de
15 puertas 250 corredizas y acristaladas plegables, que constituyen una entrada para la cual también se proporcionan sensores de puerta 260.

Como es convencional, el sistema también incluye detectores de movimiento, tales como detectores 290 PIR para controlar todas o algunas de las habitaciones o espacios dentro del edificio, algunos o todos pueden tener
20 dispositivos de captura de imágenes asociados, tal como cámaras de video. Estos u otros sensores de movimiento también se pueden usar para detectar la irrupción de una entrada, tal como la apertura de una puerta de entrada, en

lugar de usar un sensor de puerta como un dispositivo de contacto magnético. El sistema también puede incluir uno o más micrófonos para detectar y capturar, sonidos tales como cristales rotos y otros sensores para detectar la apertura de puertas internas, la ocurrencia de inundaciones, la incidencia de
5 fuego o humo, etc.

En el vestíbulo 125, cerca de la puerta de entrada 120, un nodo de desarmado 270 está montado en una pared. El nodo de desarmado 270 tiene una interfaz de usuario, que incluye una pantalla táctil o teclado para recibir una entrada del usuario para desarmar el sistema, y un transmisor de
10 radiofrecuencia, no mostrado, para transmitir, como consecuencia de la entrada del usuario, una instrucción de desarmado a la unidad de control 140. Un nodo de desarmado 280 similar también está montado en una pared de la cocina 210 cerca de la puerta trasera 220. Aunque las puertas 250 también dan acceso al espacio seguro, y están provistas de sensores de puerta para
15 detectar cuando se abren, no se proporciona ningún nodo de desarmado correspondiente para las mismas. Esto se debe a que las puertas corredizas 250 normalmente se mantienen atornilladas en el interior, para que no se espere que un ocupante o residente ingrese al edificio a través de estas puertas cuando el sistema de seguridad y monitorización este armado. En
20 consecuencia, cualquier entrada por esas puertas cuando el sistema está armado es probable que sea una entrada no autorizada. De manera similar, puede ser que la puerta de atrás siempre este cerrada por dentro cuando la

5 casa queda desocupada, para que no se espere una entrada legítima a través de la puerta trasera cuando el sistema de monitorización de seguridad está armado, en cuyo caso, el nodo de desarmado 280 para la puerta trasera puede no proporcionarse. Por el contrario, el propietario puede querer armar el sistema cuando trabaje en su jardín trasero, al que se accede a través de la puerta trasera 220, por lo que es útil proporcionar un nodo de desarmado en la cocina junto a la puerta trasera. De hecho, un propietario de jardín puede encontrar muy atractivo poder desarmar el sistema desde la cocina en lugar de tener que caminar hacia la unidad 140 central, ya que esto reduciría la probabilidad de que barro del jardín quedara en el pasillo, por ejemplo.

15 El sistema está dispuesto de modo que pueda desarmarse del estado armado usando el nodo de desarmado adyacente o cerca de la entrada a través de la cual se ingreso el espacio protegido. Una vez que un detector se activa por una irrupción detectada de una entrada, tal como la apertura de una puerta, transmite una señal de RF a la unidad central, incluyendo un identificador para el detector, por ejemplo, sensor de puerta, de modo que la unidad central pueda distinguir entre señales recibidas de detectores en diferentes entradas monitorizadas. En respuesta a la recepción de un mensaje de irrupción de entrada, tal como una indicación/mensaje de apertura de puerta de un sensor de puerta, la unidad central inicia un temporizador de período de entrada, que establece una ventana de tiempo dentro de la cual se debe desarmar el sistema, que si falla, la unidad central hará que el sistema de

monitorización de seguridad entre en estado de alarma. Entrar en un estado de alarma puede implicar el sonido de alarmas y luces intermitentes en las instalaciones. Si la instalación de la alarma está conectada a una estación central de monitorización, la unidad central generalmente indicara el estado de alarma a la estación central de monitorización, lo que puede conducir a la intervención humana, escaneado de video, monitorización de audio, etc.

Para desarmar el sistema, normalmente un código puede necesitar ser ingresado en el sistema, ya sea en la unidad de control o en un nodo de desarmado. Si hay mas de un nodo de desarmado, la unidad de control puede usar el conocimiento de la proximidad de nodos de desarmado particulares y detectores de irrupciones de entrada particulares (por ejemplo, sensores de puerta) para permitir desarmar solo desde el nodo de desarmado adyacente al detector de violaciones de entrada (por ejemplo, PIR o dispositivo de contacto magnético) que transmitió la señal de irrupción de entrada. Los nodos de desarmado pueden incluir un teclado físico o una pantalla táctil para permitir que un usuario ingrese un código de desarmado apropiado, y pueden incluir indicadores visuales y/o un panel de visualización para indicar el progreso y el estado actual del sistema. Este enfoque para desarmar un sistema armado requiere una intervención manual con el nodo de desarmado. Los nodos de desarmado también pueden incluir una antena de comunicación de campo cercano (NFC) y un transceptor para la comunicación con un dispositivo habilitado para NFC, tal como un dispositivo de autenticación portátil en forma

de mando, un teléfono móvil, un reloj, etc. para permitir que el sistema se arme y desarme colocando el dispositivo habilitado para NFC a unos pocos centímetros del nodo de desarmado. Pero otra vez, para poder desarmar el sistema con un dispositivo con NFC habilitado, un usuario debe tener una
5 mano libre para poner el dispositivo habilitado para NFC en contacto cercano con el nodo de desarmado.

Para permitir el desarme con manos libres, además, el sistema está provisto de uno o más dispositivos de autenticación portátiles, tal como etiquetas o mandos. El o cada dispositivo de autenticación portátil tiene una
10 identidad de dispositivo de autenticación portátil que está registrada con la unidad de control, y un transceptor para recibir señales de un nodo de desarmado y para transmitir señales a la unidad de control. Cada dispositivo de autenticación portátil puede ser opcionalmente un dispositivo habilitado para NFC, como se acaba de describir. Cada dispositivo de autenticación portátil
15 también incluye un sensor de movimiento configurado para detectar el movimiento del dispositivo de autenticación portátil y para proporcionar una salida al procesador en función del movimiento detectado del dispositivo de autenticación portátil. El procesador está configurado para determinar si el dispositivo de autenticación portátil está estacionario o en movimiento, basado
20 en la salida del sensor de movimiento. Convenientemente, el sensor de movimiento puede ser un acelerómetro. Preferentemente, el acelerómetro es un acelerómetro de múltiples ejes, por ejemplo, 3 ejes. El funcionamiento del

sistema usando uno o más de dichos dispositivos de autenticación portátiles se describirá ahora con referencia a las Figuras 2, 3 y 4.

La Figura 2 muestra un edificio estilizado en el que se instala un sistema de monitorización de seguridad de acuerdo con una realización de la invención.

5 La instalación incluye una unidad central 140, y una puerta 50 que da acceso al edificio tiene un sensor de puerta 130 para detectar la apertura de la puerta (mas generalmente, la irrupción de una entrada). Adyacente a la puerta y dentro del espacio seguro hay un nodo de desarmado 270. El nodo de desarmado está fijado preferentemente a la estructura del edificio de modo que
10 su ubicación con respecto a la entrada 50 sea fija y la asociación entre el detector de irrupción de entrada particular y el nodo de desarmado. El propietario/residente 66 de la propiedad tiene un mando 300 que se puede usar para permitir el desarmado del sistema de monitorización con manos libres. El mando tiene una identidad que se ha registrado con la unidad central, y puede
15 haber mas de un mando, cada uno con un identificador único que se registra con la unidad central y se almacena en su memoria.

La Figura 4 muestra los componentes principales de los diversos dispositivos que participan en el procedimiento de desarmado de manos libres. La unidad de control 140 incluye un procesador 400 con una memoria 410
20 asociada que almacena, entre otras cosas, identidades para los mandos que están registrados en el sistema, identidades para los detectores (por ejemplo, PIR y/o dispositivos de contacto magnético) y nodos de desarmado del sistema

junto con una asociación entre cada nodo de desarmado y el detector para la entrada mas cercana al nodo de desarmado relevante. Estas identidades y asociaciones se almacenan en una base de datos 415 dentro de la memoria 410. La unidad central incluye al menos un transceptor 420 de RF, con antena 422 asociada, para la comunicación con los distintos nodos y sensores del sistema de monitorización. Normalmente, habrá un segundo transceptor 430 como se muestra, también con una antena 432 asociada, para la comunicación con la estación central de monitorización 150, como respaldo o alternativa a una conexión de datos por cable a Internet a través de una interfaz de red 440.

10 Las antenas de los diversos transceptores serán normalmente todas internas a la unidad central. El procesador 400 está conectado a, y controla, la memoria 410, los transceptores 420, 430 y la interfaz de red 440. La unidad central generalmente extrae energía de la fuente de alimentación doméstica (generalmente denominada fuente de alimentación principal) que alimenta una

15 fuente de alimentación 450 dentro o asociada a la unidad central. La unidad central también incluye una fuente de alimentación autónoma de respaldo, tal como una fuente de alimentación de batería, que automáticamente se vuelve operativa en caso de que falle la fuente de alimentación externa. La fuente de alimentación autónoma interna se basa en pilas recargables 460 que se

20 mantienen continuamente cargadas por la fuente de alimentación 450. La unidad central también puede incluir una interfaz de usuario 425, que incluye una pantalla 426, una almohadilla táctil o teclado 427, un altavoz 428, y un

micrófono 429. La almohadilla táctil o teclado pueden proporcionarse haciendo que la pantalla sea sensible al tacto o como una unidad distinta de la pantalla.

La unidad central puede estar dispuesta para aceptar a través de la almohadilla táctil o teclado un código o códigos para armar y desarmar el sistema. La

5 unidad central también puede incluir una antena de comunicación de campo cercano (NFC) y un chip NFC correspondiente o circuitos equivalentes que se pueden usar, por ejemplo, para detectar la presencia de un "dispositivo de desarmado" proporcionado al usuario del sistema y que es capaz de comunicarse con la unidad central mediante comunicación de campo cercano.

10 Los mandos también pueden estar provistos de una antena NFC y un chip o circuito equivalente, para que puedan usarse como "llaves electrónicas de desarmado" con la unidad central y con los nodos de desarmado habilitados con NFC.

El nodo de desarmado 270 incluye un procesador 470 con una memoria
15 480 asociada que almacena una ID del nodo de desarmado. El nodo de desarmado también incluye una interfaz de usuario 485 que comprende un teclado o almohadilla numérica, 510, indicadores, por ejemplo, LED, 500, y opcionalmente una pantalla 490. Si se proporciona una pantalla, se puede usar para proporcionar la funcionalidad de teclado o almohadilla numérica mediante
20 el uso de una pantalla táctil como pantalla 490. Un transceptor 520, con una antena 522 asociada (que normalmente será interna, en lugar de externa como se ilustra), está controlado por el procesador 470 y se usa para comunicarse

con la unidad central 140 y el mando 300. El nodo de desarmado incluye una fuente de alimentación autónoma, por ejemplo, fuente de alimentación de batería, 525, y en general ésta será la única fuente de alimentación, ya que normalmente se prefiere no tener que conectar los nodos de desarmado a la

5 fuente de alimentación principal. Se puede proporcionar un altavoz 530 para que se puedan dar mensajes audibles e instrucciones a un usuario en el nodo de desarmado. Estos mensajes audibles y las instrucciones pueden ser automáticos, generados por la unidad central, todo por el propio nodo de desarmado, pero adicionalmente el altavoz 530 puede usarse para retransmitir

10 mensajes desde una estación central de monitorización 150. Por ejemplo, el altavoz se puede usar para proporcionar un mensaje de éxito o fallo de desarmado, y para proporcionar un aviso al usuario para que ingrese sus credenciales (por ejemplo, código de acceso) en caso de que falle el desarme de manos libres. Convenientemente, el nodo de desarmado también puede

15 incluir un micrófono 535 para permitir que un usuario en el nodo de desarmado mantenga una conversación con un operario humano en, por ejemplo, una estación de monitorización central 150, o incluso con los servicios de emergencia, por ejemplo, si la estación de monitorización central lo conecta. Preferentemente, el nodo de desarmado 270 está fijado al edificio u otra

20 propiedad fija protegida por el sistema de monitorización de seguridad, por ejemplo, fijado a una pared interna a una altura conveniente para el funcionamiento del usuario; por ejemplo, fijado a una altura entre 1 metro y 1,5

metros del suelo.

El sistema puede estar dispuesto de manera que un nodo de desarmado solo pueda usarse para desarmar el sistema de un estado armado, o puede estar dispuesto para permitir que el sistema este armado (por ejemplo, en un estado armado parcial o totalmente armado) y desarmado desde un nodo de desarmado. Al igual que la unidad central, el nodo de desarmado también puede incluir una antena de comunicación de campo cercano y un chip 472 para habilitar un dispositivo de seguridad de desarmado, tal como un mando habilitado con NFC, para ser usado para desarmar el sistema al llevar el dispositivo a unos pocos centímetros del nodo de desarmado.

El nodo de desarmado está configurado preferentemente para encriptar sus transmisiones de radio y para desencriptar las señales recibidas, para que sean posibles comunicaciones seguras con la unidad de control 140. El cifrado puede basarse en un secreto compartido entre la unidad de control 140 y el nodo de desarmado 270.

El detector para detectar la irrupción de la entrada se ilustra aquí como un sensor de puerta 130 para detectar la apertura de una puerta. Este sensor de puerta incluye un procesador 550, con una memoria 555 asociada que almacena un identificador para el sensor de puerta, un transceptor 560, con una antena interna 562 asociada, conectado y controlado por el procesador 550, todo alimentado por una fuente de alimentación autónoma 570, por ejemplo, una batería. Al igual que con el nodo de desarmado, normalmente la

fuente de alimentación autónoma 570 será la única fuente de alimentación para el sensor de puerta. El sensor de puerta incluye además un interruptor, por ejemplo un par de contactos, 575, que se controlan mediante la apertura y el cierre de la puerta a la que está asociado el sensor de puerta. Normalmente, los contactos 575 responden a la presencia de un campo magnético proporcionado por un imán 580. El imán generalmente está unido a la hoja de la puerta, mientras que los contactos suelen estar fijados al marco de la puerta. Los contactos 575 pueden cerrarse en presencia del campo magnético, abriéndose cuando los contactos y el imán se separan a medida que se abre la puerta, o pueden abrirse en presencia del campo magnético, cerrándose cuando se retira el campo cuando se abre la puerta. Alternativas, tales como sensores de efecto Hall o una disposición de detección óptica, se pueden usar en lugar de contactos controlados magnéticamente. Sin embargo, como el sensor de puerta funciona con baterías, la disposición del sensor es preferentemente una que consume poca o ninguna energía en el estado de reposo (puerta cerrada), lo que hace atractivo el uso de contactos controlados magnéticamente.

El dispositivo de autenticación portátil 300 incluye un procesador 600, con una memoria 605 asociada que almacena un identificador para el dispositivo de autenticación portátil, un transceptor 610 y una batería 615 que proporciona energía al procesador y al transceptor. El transceptor 610, que tiene una antena 612 asociada, puede ser un transceptor de activación por

radio. El uso de un transceptor de activación por radio generalmente permite una reducción en la cantidad de energía consumida por el dispositivo de autenticación portátil, extendiendo así la vida útil de la batería del dispositivo de autenticación portátil. Como alternativa, el transceptor puede ser un transceptor de sondeo convencional diseñado para un bajo consumo de energía. Este transceptor de sondeo, cuando está en un estado de reposo, periódicamente alimenta solo el extremo frontal de su circuito receptor para escuchar (sondear) las señales de baliza. Si se detecta una señal de baliza, posiblemente sujeta a algún nivel de potencia mínimo, el resto del circuito receptor se activa para recibir transmisiones. Este transceptor de sondeo puede escuchar no más de aproximadamente 10 ms, por ejemplo, durante 2 ms a menos que se detecte una señal de baliza. La frecuencia con la que el transceptor realiza el sondeo es un compromiso entre la duración de la batería y la capacidad de respuesta. Un período entre eventos de sondeo de 1 a 2 segundos generalmente brindará una capacidad de respuesta satisfactoria con una duración aceptable de la batería. Normalmente, el sistema se configurará para permitir que se establezca y cambie el período de sondeo, mediante un comando de configuración de RF desde la unidad central.

El transceptor, de cualquier tipo, está controlado por el procesador y permite la comunicación por radio con la unidad central 140 y el nodo de desarmado 270. El dispositivo de autenticación portátil incluye un sensor de movimiento 650, configurado para detectar el movimiento del dispositivo de

autenticación portátil y para proporcionar una salida al procesador 600, a la que está operativamente conectado, basado en el movimiento detectado del dispositivo de autenticación portátil. El procesador está configurado para determinar si el dispositivo de autenticación portátil está estacionario o en movimiento, basado en la salida del sensor de movimiento. El sensor de movimiento es normalmente un acelerómetro, por ejemplo, un acelerómetro de 2 o 3 ejes, aunque se pueden usar otros tipos de sensores de movimiento. Por lo general, el sensor de movimiento tendrá una administración de energía inteligente basada en el movimiento, de modo que se minimice el consumo de energía en caso de que no se detecte movimiento durante un cierto período de tiempo.

Cuando el detector de movimiento no detecta movimiento, el procesador puede configurarse para generar un recuento del tiempo transcurrido desde que el dispositivo de autenticación portátil estuvo en movimiento por última vez. El dispositivo de autenticación portátil puede configurarse para apagar el transceptor del dispositivo de autenticación portátil en el caso de que el dispositivo de autenticación portátil se considere estacionario. El transceptor solo puede volver a activarse en caso de que se detecte movimiento nuevamente.

El dispositivo de autenticación portátil puede considerarse estacionario si el sensor de movimiento no detecta movimiento en el momento en que se recibe la instrucción. Como alternativa, el dispositivo de autenticación portátil

puede considerarse estacionario si el sensor de movimiento no ha detectado movimiento del dispositivo de autenticación portátil durante un período predeterminado que precede al momento en que se recibe la instrucción.

El dispositivo de autenticación portátil también puede incluir uno o más botones 620 que un usuario puede usar para emitir comandos o respuestas. El dispositivo de autenticación portátil también puede incluir uno o más indicadores visuales 625, por ejemplo, uno o más LED, para indicar un estado, para confirmar una presión de botón, o similar. Por ejemplo, un solo indicador multicolor, tal como un LED, se puede usar para proporcionar múltiples indicaciones diferentes mientras se mantiene bajo el recuento de componentes y se pueden hacer compactas las dimensiones del mando. El dispositivo de autenticación portátil está configurado preferentemente para encriptar sus transmisiones de radio y para descryptar las señales recibidas, para que las comunicaciones seguras con la unidad central sean posibles. El cifrado puede, por ejemplo, basarse en un secreto compartido entre la unidad central y el dispositivo de autenticación portátil.

La Figura 3 es un diagrama de tiempo que muestra la secuencia de eventos y acciones de los diversos elementos del sistema de seguridad que caracterizan un procedimiento, de acuerdo con una realización de la invención, de controlar un sistema de monitorización de seguridad para lograr el desarmado del sistema con manos libres. El diagrama se refiere a las operaciones del detector de irrupción de entrada, por ejemplo, el sensor de

puerta 130, la unidad central 140, el nodo de desarmado 270 y el dispositivo de autenticación portátil 300.

El procedimiento comienza en 305 con el detector detectando un evento, por ejemplo, la apertura de la puerta cuyo estado detecta y responde a esto usando su transceptor RF para transmitir un mensaje de irrupción de entrada. Este mensaje de irrupción de entrada, que incluye la identificación del detector, se recibe en un transceptor de la unidad de control 140. En este ejemplo, se supone que el detector es un dispositivo de contacto magnético, pero el procedimiento es el mismo o esencialmente el mismo si la irrupción de entrada se detecta usando un sensor de movimiento como un dispositivo PIR o una cámara de video.

La unidad central comienza, en 310, un temporizador de período de entrada, que se establece durante el período dentro del cual el procedimiento de desarme debe completarse antes de que la unidad de control provoque que el sistema entre en una condición de alarma, por ejemplo, en el intervalo de 20 a 40 segundos. La unidad central identifica el detector que transmitió el mensaje de irrupción de entrada desde la ID del detector contenida en el mensaje recibido, y recupera de la base de datos 415 la ID del nodo de desarmado que está asociado al sensor de puerta identificado. Si no hay un nodo de desarmado asociado al sensor de puerta identificado, la unidad central espera la entrada de un código de desarme en la interfaz de usuario 425 o la llegada de un mensaje desde otro nodo de desarmado (por ejemplo, un

mensaje que indique que se ha ingresado el código de acceso de desarme en ese nodo de desarmado) si eso está permitido por la configuración del sistema. Sin embargo, si la base de datos revela que el sensor de puerta (detector de irrupción de entrada) está asociado a un nodo de desarmado, la unidad central

5 incluye el código de identificación para ese nodo de desarmado en un mensaje que transmite, en 315, al nodo de desarmado 270 para hacer que el nodo de desarmado active, en 320, un indicador, un LED 500 por ejemplo, o para emitir un sonido a través del altavoz 530, para indicar a la persona que ingresa al espacio seguro que el sistema está armado y que se deben tomar medidas

10 para desarmar el sistema dentro del período establecido para el temporizador del período de entrada. El mensaje también hace que el nodo de desarmado transmita, en 330, una señal de baliza o señal de sondeo para despertar el transceptor en cualquier dispositivo de autenticación portátil (o al menos en cualquier dispositivo de autenticación portátil que este en movimiento o que no

15 haya apagado su transceptor después de un período de no movimiento) dentro de la vecindad del objetivo desarme el nodo, y preferentemente incluye un identificador especial para ser incluido en la señal de baliza o señal de sondeo, y detalles de la cuenta regresiva del paquete que se usara. El identificador especial suele ser un número aleatorio o pseudoaleatorio cuyo valor cambia en

20 cada uso. El dispositivo de autenticación portátil escucha las señales de baliza en uno o más canales cuyos parámetros son conocidos por cada uno de los dispositivos de autenticación portátiles, por ejemplo, al haber sido

preprogramados, pero mas preferentemente se ha comunicado al o a cada dispositivo de autenticación portátil cuando ese dispositivo de autenticación portátil se registro por primera vez en la unidad central (aunque, por supuesto, la unidad central podría actualizar periódicamente estos parámetros a través de un intercambio de mensajes con los dispositivos de autenticación portátiles).

En este momento, la unidad de control 140 preferentemente también comienza, en 325, un temporizador valido de baliza desarmado de manos libres, que determina el tiempo dentro del cual la recepción por parte de la unidad central de un mensaje desde un dispositivo de autenticación portátil (por ejemplo, mando) que incluye el identificador especial (si se usa) será efectivo para desarmar el sistema. La configuración valida del temporizador de baliza de desarmado de manos libres también se incluye en el mensaje enviado al nodo de desarmado. Las características de la señal de baliza o de sondeo transmitidas por el nodo de desarmado se eligen preferentemente para que el rango efectivo de la señal de baliza sea pequeño, preferentemente del orden de unos pocos metros, por ejemplo, no mas de 5 metros para detección por un dispositivo de autenticación portátil, para que solo sea efectivo al despertar un dispositivo de autenticación portátil en las inmediaciones del nodo de desarmado. Estas características se describirán en más detalle a continuación.

El transceptor 610 de un dispositivo de autenticación portátil 300 que se encuentra a pocos metros del nodo de desarmado (y que no está actualmente en un estado de apagado después de un período de no movimiento) recibe la

señal de baliza y se activa. El transceptor 610 recibe y decodifica la señal de baliza, recuperando el identificador especial (si se usa). El controlador del dispositivo de autenticación portátil hace que el transceptor 610 del dispositivo de autenticación portátil transmita, en 340, un mensaje que incluye la
5 identificación del dispositivo de autenticación portátil y el identificador especial (si se usa) a la unidad central 140.

La unidad central verifica que el identificador especial (si se usa) es valido (lo que significa que es uno emitido dentro del período actual del temporizador valido de baliza de desarmado de manos libres) y también
10 verifica si la ID del dispositivo de autenticación portátil corresponde a una registrada con la unidad central. Si se pasan ambas comprobaciones (si se usa un identificador especial), la unidad central en 345, desarmara el sistema si el mensaje del dispositivo de autenticación portátil, que contiene la identificación del dispositivo de autenticación portátil y el identificador especial (si se usa), se
15 recibió antes de que expirara el temporizador valido de baliza de desarmado de manos libres. En esta etapa, la unidad de control también puede enviar un mensaje adicional al nodo de desarmado para hacer que el nodo de desarmado proporcione una notificación del hecho de que el sistema ha sido desarmado, por ejemplo, el nodo de desarmado puede activar una luz
20 indicadora 500 apropiada y/o proporcionar un sonido o anuncio de "desarme exitoso" a través del altavoz 530. La unidad central también puede enviar un mensaje adicional al dispositivo de autenticación portátil para que el mando

genere una señal que indique el desarmado exitoso del sistema, por ejemplo, iluminando un indicador en el dispositivo de autenticación portátil.

Como se describirá mas adelante, el mensaje de solicitud de desarmado enviado por el dispositivo de autenticación portátil a la unidad de control también puede incluir un informe sobre los niveles RSSI de los mensajes recibidos por el dispositivo de autenticación portátil desde el nodo de activación, y la unidad de control puede usar la información sobre los niveles RSSI medidos en dicho informe para determinar si se debe confiar o no en la solicitud de desarme recibida, es decir, si se debe ignorar la solicitud de desarme como no valida sobre la base de que es probable que provenga de un actor deshonesto (fuera del rango habitual del nodo de desarmado) en lugar de un usuario autorizado dentro del alcance del nodo de desarmado.

Si el temporizador valido de baliza de desarmado de manos libres caduca sin que la unidad de control haya recibido un mensaje de un dispositivo de autenticación portátil que incluye una ID de dispositivo de autenticación portátil registrada y el identificador especial (si se usa), la unidad central preferentemente transmite otro mensaje, en 360, al nodo de desarmado (incluido el identificador de nodo de desarmado relevante) para que el nodo de desarmado proporcione un aviso visual o audible, o ambos, indicando la necesidad de desarmar el sistema de alguna otra manera, por ejemplo, ingresando las credenciales apropiadas (como una contraseña o PIN) en el nodo de desarmado. El nodo de desarmado proporciona este aviso,

visualmente o audiblemente, o ambos, en 365. Cualquier credencial ingresada en el nodo de desarmado es enviada por el nodo de desarmado a la unidad central. Si la unidad central recibe la credencial adecuada antes de que expire el temporizador del período de entrada, el sistema está desarmado.

- 5 Se notará que las credenciales de desarmado no se verifican en el nodo de desarmado, con el nodo de desarmado enviando un mensaje de "éxito", si corresponde a la unidad central, sino que las credenciales ingresadas se transmiten desde el nodo de desarmado a la unidad central donde se verifican.

El nodo de desarmado se puede configurar para enviar, en 350, si no se
10 ha recibido un mensaje de éxito/fallo de desarme desde la unidad central, un mensaje de sondeo a la unidad central después de la expiración del período de temporizador válido de baliza de desarmado de manos libres para verificar si el nodo de desarmado debe proporcionar una indicación de éxito de desarmado. Si la unidad central recibe dicho mensaje de sondeo, transmite una respuesta
15 de sondeo para indicar el éxito/fallo y hacer que el nodo de desarmado proporcione una indicación de éxito de desarme, o para indicar un fallo, y la necesidad de proporcionar credenciales de desarmado de algún tipo, según proceda.

Si no se recibe un mensaje apropiado de un dispositivo de autenticación
20 portátil dentro del temporizador válido de baliza de desarmado de manos libres y no se reciben las credenciales de desarmado apropiadas antes de que expire el temporizador del período de entrada, la unidad de control identifica un

estado de alarma. Si el sistema está respaldado por una estación central de monitorización (CMS), la unidad central enviara un mensaje de cambio de estado al CMS, normalmente con el identificador del detector de irrupción de entrada que primero indicó un evento de irrupción de entrada, tal como la
5 apertura de una puerta. El CMS puede hacer que la unidad de control active cámaras de video relevantes u otros dispositivos de captura de imágenes, dispositivos de captura de audio, etc. y proporcionar datos de estos al CMS. El CMS también puede invocar la intervención humana según corresponda.

El sistema puede configurarse de tal manera que, si el nodo de
10 desarmado detecta una entrada en su interfaz de usuario 485, de si un sensor de comunicación de campo cercano (NFC) 472 en el nodo de desarmado detecta la presencia de una etiqueta NFC apropiada (llave electrónica de desarmado), la transmisión de la baliza de desarmado mediante el nodo de desarmado se detiene o se impide. En cuyo caso, el sistema es desarmado por
15 la unidad central si se proporcionan las credenciales de desarme apropiadas en el nodo de desarmado (o en la unidad central) a través de una interfaz de usuario o por medio de una etiqueta NFC registrada (es decir, una etiqueta que se haya registrado previamente en la unidad central), antes de la expiración del temporizador del período de entrada.

20 En una realización alternativa, la unidad central no inicia un temporizador de desarmado de manos libres, pero en su lugar, el nodo de desarmado inicia dicho temporizador al recibir el mensaje enviado en la etapa

315 por la unidad central. Si el nodo de desarmado no recibe un mensaje de éxito de desarmado de la unidad central antes de que expire el temporizador de desarmado de manos libres, el nodo de desarmado proporciona una advertencia audible y/o visual en el sentido de que el desarmado con manos
5 libres ha fallado y que el sistema debe desarmarse de alguna otra manera, por ejemplo, ingresando un PIN o código de acceso, o usando una etiqueta NFC registrada, para evitar que el sistema pase a un estado de alarma. El temporizador de desarmado de manos libres que ejecuta el nodo de desarmado tiene, por supuesto, una duración lo suficientemente corta como
10 para garantizar que caduque antes del temporizador del período de entrada que ejecuta la unidad central. Si el sistema de gestión de seguridad puede proporcionar temporizadores de entrada de diferentes duraciones, luego, la unidad central se configura para informar al o a cada nodo de desarmado de la duración del temporizador del período de entrada que se ha configurado, y se
15 tiene en cuenta el tiempo que le toma a la unidad central procesar un mensaje de puerta abierta y para un nodo de desarmado para responder al mensaje enviado en la etapa 315, para que la duración del temporizador de desarmado en manos libres se pueda ajustar adecuadamente para adaptarse a la duración del temporizador de período de entrada seleccionado.

20 Preferentemente, la comunicación de RF entre la unidad central y los nodos, los detectores y los sensores de los sistemas de monitorización de seguridad de acuerdo con las realizaciones de la invención usan bandas de

radio industriales, científicas y médicas (ISM), tal como en Europa la banda de 868 MHz. Dentro de la banda de 868 MHz hay varias subbandas dedicadas a "SRD no específicas" que son de interés. Para la señal de baliza/sondeo que usa el nodo de desarmado para activar un dispositivo de autenticación portátil
5 cercano, generalmente estamos interesados en diseñar comunicaciones de corto alcance, tal como se describirá en breve con referencia a la Figura 6.

La Figura 5 es un diagrama de flujo que ilustra un posible procedimiento para un dispositivo de autenticación portátil de acuerdo con una realización de la invención para determinar si responde a una transmisión recibida. En 1000,
10 el dispositivo de autenticación portátil recibe una transmisión de RF en su transceptor (el transceptor no se ha apagado después de una determinación de que el dispositivo de autenticación portátil es estacionario). Como una primera etapa, 1100, el dispositivo de autenticación portátil determina si la transmisión recibida es o no una instrucción de desarmado, es decir, que incluye un
15 identificador de transmisión de desarmado de algún tipo, por ejemplo, ser una baliza de alerta o mensaje de éxito o fallo de desarmado. Si la determinación es negativa, es decir, no es una instrucción de desarme, el procedimiento pasa a la etapa 1200.

Si la determinación es positiva, el procedimiento continúa con la etapa
20 1300 en la que se verifica el estado de movimiento del dispositivo de autenticación portátil. Si se determina que el dispositivo de autenticación portátil es estacionario, el procedimiento pasa a la etapa 1400. Si el dispositivo

de autenticación portátil está configurado para apagar su transceptor después de un período de no movimiento, cuando el mando se considera estacionario, el dispositivo de autenticación portátil posteriormente no recibirá ninguna transmisión de RF (hasta después de que se detecte que el dispositivo de autenticación portátil se ha movido nuevamente) y, por lo tanto, este procedimiento no tiene lugar. Pero si se determina que el dispositivo de autenticación portátil se está moviendo, en 1600, el procedimiento pasa a la etapa 1800.

En la etapa 1400, el procesador determina si el dispositivo de autenticación portátil debe considerarse estacionario, por ejemplo, comprobando un recuento (o alguna otra medida del tiempo transcurrido) desde que se determino por última vez que el dispositivo de autenticación portátil se estaba moviendo. Si el recuento es menor que un recuento de umbral predeterminado, se determina que el dispositivo de autenticación portátil, 1500, es un dispositivo de autenticación portátil "vivo" que se puede usar para proporcionar una instrucción de desarmado a la unidad central (es decir, el dispositivo de autenticación portátil no se considera estacionario), y el procedimiento continua con la etapa 1800. Si el dispositivo de autenticación portátil se considera estacionario, entonces el dispositivo de autenticación portátil no transmitirá ningún mensaje de desarmado y el procedimiento finalizara a las 17:00.

El período de inactividad que se acepta como indicativo de que un

dispositivo de autenticación portátil está "activo" puede establecerse de manera diferente en diferentes instalaciones, pero normalmente este período no será más de aproximadamente 60 segundos. Un corte a los 30 segundos suele ser suficiente para la mayoría de los usuarios, aunque para instalaciones de sistemas donde los ocupantes o usuarios del espacio seguro son ancianos o están enfermos, 30 segundos pueden no ser lo suficientemente largos. Preferentemente, el período de corte se mantiene relativamente corto, en no más de un minuto más o menos.

Si en la etapa 1300 se determina que el dispositivo de autenticación portátil se está moviendo 1600, el procedimiento pasa a la etapa 1800.

En la etapa 1800, el dispositivo de autenticación portátil genera un mensaje de transmisión que incluye la ID del dispositivo de autenticación portátil y el identificador de transmisión de desarmado (si se usa) y otros parámetros que el sistema requiera (por ejemplo, un informe de RSSI medido).

En la etapa 1200, cuando se determina que la transmisión no es una instrucción de desarmado, el dispositivo de autenticación portátil puede programarse simplemente para leer la transmisión y actuar sobre el contenido, o para verificar un determinado indicador o indicadores y responder de manera diferente en función del indicador(es) determinado(s) como presente(s). Por lo tanto, por ejemplo, el sistema de monitorización puede estar dispuesto de manera que el dispositivo de autenticación portátil este configurado para recibir una instrucción que no sea una instrucción de desarmado a través del

transceptor, incluyendo un indicador, desde la unidad de control para realizar una acción; y en el que en el caso de que la otra instrucción incluya el indicador, el procesador está configurado para hacer que el dispositivo de autenticación portátil realice la acción indicada, independientemente de si,

5 cuando se recibe la instrucción, se determina que el dispositivo de autenticación portátil es estacionario. Los dispositivos de autenticación portátiles configurados de esta manera pueden activarse mediante una señal de RF, desde la unidad de control o desde un nodo de desarmado, permitiendo verificar y/o actualizar el estado de todos los dispositivos de autenticación

10 portátiles dentro del alcance. También sería posible realizar una auditoria de todos los dispositivos de autenticación portátiles en el rango de, digamos, la unidad central. Si un dispositivo de autenticación portátil de este tipo incluyera uno o más indicadores visuales, un transductor de audio, un transductor háptico, y se configuraron para generar una salida usando uno o más de estos

15 cuando así lo indique una instrucción recibida que incluye el indicador, se podría hacer que un dispositivo de autenticación portátil perdido se anunciara. Por supuesto, este enfoque solo funcionaría con todos los dispositivos de autenticación portátiles si no estuvieran configurados para apagar sus transceptores después de un período de no movimiento, o si ninguno de ellos

20 hubiera apagado su transceptor cuando la señal de RF desde la unidad de control o nodo de desarmado fue transmitida.

Los dispositivos de autenticación portátiles de acuerdo con la invención

pueden configurarse para escuchar instrucciones relacionadas con el desarmado de manos libres solo en un canal o canales particulares, con frecuencia dada y modulación dada, pero para escuchar otro canal o canales en una frecuencia diferente y posiblemente con modulación diferente para otro tipo de instrucciones.

Las instrucciones de desarmado recibidas desde un nodo de desarmado generalmente no contienen una ID de dispositivo de autenticación portátil, porque, si hay mas de un dispositivo de autenticación portátil registrado en la unidad central, no se puede suponer que si la persona que abrió la puerta está llevando un dispositivo de autenticación portátil cuya detección ha sido detectada. Pero otro mensaje puede estar dirigido a un dispositivo de autenticación portátil particular o a un grupo de dispositivos de autenticación portátiles que es un subconjunto de todos los dispositivos de autenticación portátiles registrados. En consecuencia, un dispositivo de autenticación portátil de acuerdo con las realizaciones de la invención también puede estar dispuesto para verificar el contenido de los mensajes recibidos para la presencia de la identificación de ese dispositivo de autenticación portátil. De esta manera, la unidad de control puede apuntar a un dispositivo de autenticación portátil individual o a un grupo de dispositivos de autenticación portátiles. Por ejemplo, en el caso de que un dispositivo de autenticación portátil se extravíe, la unidad central marcada con la ID del dispositivo de autenticación portátil particular que se ha perdido puede transmitir un mensaje

de "anunciarme". Si otros dispositivos de autenticación portátiles reciben el mensaje, no le responden, porque está marcado como un mensaje de "anunciarme" y no contiene su ID. Mientras que el dispositivo de autenticación portátil que falta ve que el mensaje está marcado como un mensaje de "anunciarme", reconoce su propia identificación y anuncia su presencia usando uno o más de sus indicadores incorporados (por ejemplo, uno o más LED, o proporcionando un anuncio háptico, por "zumbido" o vibración).

En general, los sistemas de monitorización según las realizaciones de la invención no se configuraran para transmitir solo mensajes de desarmado a dispositivos de autenticación portátiles, sino que también se configuraran para enviar otros tipos de mensajes a dispositivos de autenticación portátiles. En los sistemas que solo envían mensajes de desarmado de dispositivos de autenticación portátiles, un dispositivo de autenticación portátil solo necesita reconocer un mensaje recibido como mensaje de desarmado y responder con el identificador de transmisión de desarmado (si se usa) y la ID del dispositivo de autenticación portátil (aunque, tal como se explicara posteriormente, es posible que se requieran dispositivos de autenticación portátiles para realizar mediciones RSSI e incluir estos, o un informe basado en estos, como parte de la respuesta). Pero en los sistemas donde hay tipos de mensajes adicionales, los tipos de mensajes generalmente se dividen en dos clases: mensajes dirigidos que se dirigen a un subconjunto de uno o más de todos los dispositivos de autenticación portátiles registrados, que incluyen una o mas ID

de dispositivo de autenticación portátil, y respecto de las cuales se busca una reacción solo de los dispositivos de autenticación portátil que tienen una ID incluida en el mensaje; y mensajes grupales o generales, con respecto a los cual se busca una reacción de cualquier dispositivo de autenticación portátil
5 que recibe el mensaje, y que, por lo tanto, no necesita incluir una ID de dispositivo de autenticación portátil (y que, por lo tanto, generalmente no incluirá ninguna ID de dispositivo de autenticación portátil). Por ejemplo, se puede configurar una unidad central para instruir al dispositivo de autenticación portátil involucrado en un evento de desarmado de manos libres para
10 proporcionar un indicador de éxito de desarmado en un evento de desarmado exitoso. Dicha instrucción incluirá preferentemente la ID del dispositivo de autenticación portátil que transmitió la solicitud de desarmado a la unidad central (la ID del dispositivo de autenticación portátil se ha incluido en esa solicitud de desarmado).

15 Los mensajes pueden enviarse a dispositivos de autenticación portátiles al menos desde la unidad de control (de los cuales, en algunos sistemas, puede haber mas de una) y nodos de desarmado. Cuando hay múltiples tipos de mensajes, pueden etiquetarse como mensaje de desarmado, agrupado y dirigido - etiquetas que se pueden considerar como indicadores de clase. Si se
20 requiere una granularidad mas fina, se puede proporcionar un nivel adicional de indicadores, de modo que un tipo de mensaje se indica mediante un indicador principal (mensaje de desarmado, agrupado, o dirigido), y (al menos

para agrupado y dirigido) un indicador secundario que indica el tipo de mensaje específico dentro de la clase. Como alternativa, se puede proporcionar un solo nivel de indicadores, con normalmente múltiples indicadores para cada una de las clases de grupo y objetivo.

5 La Figura 6 es un diagrama esquemático que ilustra por que generalmente queremos que el rango de las señales de baliza de los nodos de desarmado tenga un rango mas corto que las transmisiones desde la unidad central de un sistema de monitorización. Una primera persona que ingresa a un espacio seguro abre una puerta, por ejemplo, la puerta de entrada que da
10 acceso a una calle, que es monitorizado por el sensor de puerta 130 u otro detector. La persona lleva un dispositivo de autenticación portátil (por ejemplo, mando) 300 que está registrado en la unidad de control del sistema de monitorización. Adyacente a la puerta que se abre hay un nodo de desarmado 270. La unidad central 140 del sistema incluye una base de datos 415 que
15 almacena una asociación entre un identificador para el sensor de puerta 130 u otro detector, y un identificador para el nodo de desarmado 270. Al espacio seguro también se puede acceder por otra puerta del edificio, por ejemplo, una puerta trasera que da acceso a un jardín trasero del edificio, y esa puerta está equipada con otro sensor de puerta 730 u otro detector. También cerca de la
20 puerta de atrás, dentro del espacio seguro, hay otro nodo de desarmado 770. Un segundo dispositivo de autenticación portátil, 700, es transportado por otra persona que también ocupa el espacio seguro, quien está trabajando en el

jardín trasero.

Cuando la primera persona abre la puerta principal y la unidad central hace que el primer nodo de desarmado transmita una señal de baliza, es deseable que la señal de baliza sea recibida por el primer mando 300 que está
5 adyacente (digamos dentro de un metro o dos como máximo) del primer nodo de desarmado 270, para que se active el primer mando, pero que el segundo dispositivo de autenticación portátil 700, que es llevado por la segunda persona que trabaja en el jardín trasero, no reciba esa señal de baliza y, por lo tanto, no se active. Por supuesto, en el escenario que acabamos de describir, la persona
10 que abre la puerta principal y la persona que lleva el segundo dispositivo de autenticación portátil son ocupantes "legítimos" de las instalaciones seguras, para que no haya ningún problema inherentemente en enviar una señal de desarme desde el segundo dispositivo de autenticación portátil con respecto a una entrada realizada por la primera persona (como podría ocurrir si la primera
15 persona se hubiera olvidado de llevar su mando), como podría suceder si el rango efectivo de la señal de baliza del primer nodo de desarmado 270 fuera recibido y accionado por el segundo dispositivo de autenticación portátil 700. Pero por supuesto, sería una situación diferente si la persona que abriera la puerta de entrada fuera un villano que entraba ilegalmente a las instalaciones
20 por la puerta de entrada. En este caso, incluso si el villano no tenía un mando registrado, su entrada aun daría como resultado que el sistema se desarmara si el rango efectivo de la señal de baliza del primer nodo de desarmado hiciera

que el segundo dispositivo portátil de autenticación enviara una señal de desarmado a la unidad de control. Por esta razón, generalmente queremos que el rango efectivo de señales de baliza de los nodos de desarmado se restrinja a la vecindad inmediata del nodo de desarmado e incluya el espacio entre el
5 nodo de desarmado y la puerta a la que está asociado.

Estos escenarios también ilustran por que queremos que la unidad de control dirija los mensajes de baliza solo al nodo de desarmado que está asociado al detector de irrupción de entrada (por ejemplo, el sensor de puerta) que ha detectado e informado de una irrupción de entrada. Queremos que los
10 mensajes de baliza sean detectables por todos los nodos de desarmado, donde sea que se encuentren. Entonces, si los mensajes de baliza fueran genéricos, posiblemente harían que todos los nodos de desarmado transmitan señales de baliza, el segundo dispositivo de autenticación portátil de la persona que trabaja en el jardín trasero podría activarse mediante señales de baliza
15 desde el segundo nodo de desarmado, cuando un villano sin un dispositivo de autenticación portátil estaba efectuando la entrada ilícita a través de la puerta principal, incluso si las señales de baliza de los nodos de desarmado eran de muy corto alcance.

Dentro de la banda de 868/869 MHz en Europa, la subbanda entre 869,7
20 y 870 MHz es particularmente interesante para usar cuando se transmiten señales de baliza de corto alcance desde los nodos de desarmado porque proporciona un canal relativamente amplio, el canal de baliza, que permite el

uso de una alta velocidad de datos, por ejemplo, 250 kbit/s, lo cual es útil para reducir el rango efectivo de la señal de baliza. El techo de potencia radiada efectiva de 5 mW tampoco plantea una restricción significativa para esta aplicación. Por estas razones, esta subbanda entre 869,7 y 870 MHz es la

5 banda de frecuencia preferida para las transmisiones de corto alcance desde el nodo de desarmado, y que se usan para la comunicación con dispositivos de autenticación portátiles, por ejemplo, para la transmisión de mensajes de activación.

Aunque, por las razones que acabamos de dar, preferimos transmitir las

10 balizas desde el nodo de desarmado mas cercano a la entrada que dio lugar a la señal de activación de la alarma, alternativas son posibles.

Por ejemplo, un sensor que detecta la irrupción de una entrada transmite una señal de activación de alarma, incluyendo un identificador de sensor, que es detectada por la unidad de control. La unidad de control reconoce el

15 identificador del sensor y lo usa para recuperar el identificador del nodo de desarmado asociado al sensor correspondiente. La unidad de control luego transmite un mensaje, que puede ser un mensaje de activación, incluyendo el identificador de nodo de desarmado relevante que tiene el efecto de hacer que el nodo de desarmado relevante escuche las señales de los mandos

20 (dispositivos de identificación portátiles). La unidad de control luego transmite una señal de activación de control que puede recibir cualquier control adyacente a cualquiera de los nodos de desarmado. Cualquier mando que

recibe la señal de despertador desde la unidad de control responde transmitiendo una señal de respuesta, incluyendo su propio identificador, que solo es detectable por un nodo de desarmado dentro de no mas de aproximadamente 2 metros del mando (usando características de transmisión de potencia seleccionadas adecuadamente, velocidad de datos, etc. para garantizar un rango de transmisión efectivo corto). Un nodo de desarmado que recibe la señal de respuesta del mando luego transmite una señal, incluyendo el identificador del mando, a la unidad de control que luego determina si el identificador del mando es para un mando registrado. De esta forma, solo el nodo de desarmado cuyo identificador se incluyo en la transmisión desde la unidad de control detecta la respuesta del mando.

Como otra alternativa, el nodo de desarmado puede configurarse para generar una señal de activación de alarma que se transmite a la unidad de control en respuesta a la recepción de una señal de irrupción de entrada desde un sensor configurado para detectar la irrupción de una entrada al edificio o espacio seguro. Es decir, el sensor transmite una señal con respecto a una irrupción detectada, cuya señal es recibida por el nodo de desarmado asociado en lugar de por la unidad de control. La unidad de control luego transmite una señal de activación de control que puede recibir cualquier control adyacente a cualquiera de los nodos de desarmado. Cualquier mando que recibe la señal de despertador desde la unidad de control responde transmitiendo una señal de respuesta, incluyendo su propio identificador, que solo es detectable por un

nodo de desarmado dentro de no mas de aproximadamente 2 metros del mando. Un nodo de desarmado que recibe la señal de respuesta del mando luego transmite una señal, incluyendo el identificador del mando, a la unidad de control que luego determina si el identificador del mando es para un mando registrado. De esta forma, solo el nodo de desarmado cuyo identificador se incluyo en la transmisión desde la unidad de control detecta la respuesta del mando. Sin embargo, este enfoque es menos preferido que las alternativas ya mencionadas, porque si la señal del sensor que detecta la irrupción de una entrada solo es recibida por la unidad de control a través del nodo de desarmado, en lugar de directamente, la seguridad del sistema se reduce: el nodo de desarmado se convierte en un punto de debilidad, porque si está deshabilitado o sus señales bloqueadas de alguna manera por un mal actor, la unidad de control no recibirá ninguna señal de activación de alarma con respecto a la irrupción. Por esta razón, seria deseable incluir características antisabotaje en el nodo de desarmado, tales como sensores para detectar e informar sobre intentos de abrir el nodo de desarmado, y posiblemente también implementar una función de "latido" en la cual el nodo de desarmado periódicamente "se registra" con la unidad de control - el fallo de la unidad de control para recibir el latido, o la recepción de un mensaje de sabotaje desde el nodo de desarmado que hace que la unidad de control determine una condición de alarma que se informa a la estación central de monitorización (si está presente) y que proporciona señales de alarma (audio y ópticas) a través

de la instalación de alarma - así como enviar informes al teléfono del usuario - correo electrónico, según proceda. Dichas características de seguridad adicionales también pueden estar presentes en los nodos de desarmado de acuerdo con cualquiera de las otras realizaciones y variantes.

5 Lograr una vida útil efectiva de la batería de los nodos y sensores en los sistemas de alarma y monitorización es una preocupación constante, debido a que el fallo de la batería deshabilita el nodo o sensor relevante, lo que puede conducir a la pérdida de seguridad, y el reemplazo de la batería puede implicar una visita al sitio por parte del proveedor del sistema, lo cual es costoso e
10 inconveniente. Para un dispositivo de autenticación portátil, la pérdida de energía de la batería significa que el dispositivo de autenticación portátil deja de funcionar, lo cual es inconveniente para el usuario, y la causa del fallo puede no ser evidente para el usuario, por lo que el usuario puede requerir una visita al sitio para identificar y solucionar el problema. En consecuencia,
15 estamos interesados en reducir el consumo de energía en todos los componentes alimentados por batería del sistema, incluyendo el dispositivo de autenticación portátil. Por esta razón, el uso de un receptor de radio de activación en el dispositivo de autenticación portátil es atractivo, aunque también se puede obtener una vida útil aceptable de la batería usando un
20 receptor de radio mas convencional que periódicamente se despierta para escuchar (sondear) las señales de baliza.

Una forma de reducir el consumo de energía del dispositivo de

autenticación portátil durante el procedimiento de activación es que el dispositivo de autenticación portátil utilice la detección en 2 etapas, un ejemplo de la cual se da en la figura 7. Se puede usar una primera etapa de detección del transceptor del dispositivo de autenticación portátil para realizar una

5 primera etapa que implica simplemente verificar un nivel RSSI. Por ejemplo, el transceptor en el dispositivo de autenticación portátil puede realizar periódicamente una breve verificación RSSI sondeando el canal de baliza, usando solo el extremo frontal de RF del transceptor, por ejemplo, para un primer período de menos de unos pocos milisegundos, preferentemente, una

10 fracción de milisegundo, por ejemplo, alrededor de 0,5 milisegundos, y luego volver a su estado de reposo si el nivel de RSSI detectado está por debajo de un umbral preestablecido. Si el nivel de RSSI detectado está por encima del umbral, el dispositivo de autenticación portátil escucha durante un breve período una palabra de sincronización desde el nodo de desarmado, por

15 ejemplo, durante un segundo período de unos pocos milisegundos, por ejemplo, durante menos de 10 milisegundos, por ejemplo, 5 ms. Si no se detecta ninguna palabra de sincronización, el transceptor vuelve a su estado de reposo. Pero si se detecta una palabra de sincronización, el transceptor inicia el receptor de radio completo que permanece encendido, por ejemplo, durante

20 un tercer período de entre 8 y 16 ms, por ejemplo, 10 ms, para recibir el paquete de activación completo. Cada paquete durara normalmente del orden de 220 LIS, y el nodo de desarmado puede transmitir durante 2 a 4 segundos,

por ejemplo, durante 3 segundos, lo que significa que el dispositivo de autenticación portátil debería poder recibir de 20 a 30 paquetes. Claramente, la elección de la duración de los distintos períodos es una compensación entre el consumo de energía, la experiencia y la precisión del usuario, pero los tiempos
5 dados representan un compromiso razonable como punto de partida para ajustarse según sea necesario.

La detección de RSSI se puede lograr activando solo los componentes frontales del transceptor, evitando la necesidad de encender todo el transceptor. Si el nivel de RSSI detectado está por debajo de un umbral, el
10 dispositivo de autenticación portátil determina que es poco probable que haya datos validos disponibles y detiene su verificación RSSI hasta el próximo ciclo. El período del ciclo determina el período de tiempo durante el cual el nodo de desarmado necesita transmitir su baliza y también establece un límite inferior sobre la rapidez con la que es probable que ocurra un desarme con manos
15 libres en promedio. El intervalo de activación del dispositivo de autenticación portátil, que está controlado por un reloj en el dispositivo de autenticación portátil, normalmente se elegirá en función de la duración de la baliza del nodo de desarmado. Por ejemplo, si el nodo de desarmado transmite su baliza durante 2 segundos, entonces, un intervalo de activación del dispositivo de
20 autenticación portátil de un segundo proporcionaría una buena probabilidad de que un dispositivo de autenticación portátil dentro del alcance de un nodo de desarmado de transmisión pueda activarse y recuperar la información

necesaria de la señal de baliza. Un dispositivo de autenticación portátil con un intervalo de activación (período entre eventos de sondeo) de 2 segundos a menudo será lo suficientemente frecuente cuando el nodo de desarmado este configurado para transmitir su señal de baliza durante 3 segundos. El intervalo de activación del dispositivo de autenticación portátil se puede configurar convenientemente entre un cuarto y dos tercios de la duración de la baliza. Al hacer que el dispositivo de autenticación portátil verifique el RSSI durante un período muy breve, por ejemplo, unos pocos milisegundos, en cada evento de sondeo, generalmente se puede obtener una buena duración de la batería. Un tiempo de ciclo relativo más corto no es técnicamente problemático, pero es probable que use proporcionalmente más energía de la batería y, por lo tanto, acorte la vida útil de la batería de manera proporcional. El tiempo de ciclo podría ser más de la mitad de la duración de la baliza, siempre que el sistema permita que el dispositivo de autenticación portátil capture la baliza rápidamente después de activarse, para que el dispositivo de autenticación portátil pueda recuperar la identificación especial necesaria (si se usa).

El nodo de desarmado transmite una señal de baliza, en el canal de baliza, que preferentemente incluye la palabra de código especial (que se muestra como ID en la figura 7) recibida desde la unidad de control para este evento de desarmado de manos libres. Normalmente, la señal de baliza estará compuesta por una secuencia de paquetes, cada uno comenzando con un preámbulo, seguido de una palabra de sincronización, luego un identificador

que es la ID especial de la unidad central. Preferentemente, cada paquete incluye un valor de cuenta regresiva, disminuyendo el valor de la cuenta regresiva en uno en cada paquete posterior (a cero en el paquete final de la secuencia) e indicando el número de paquetes hasta el final de la secuencia de
5 paquetes.

La señal de baliza es reconocida como tal por el dispositivo de autenticación portátil, porque es el único mensaje de ese tipo con el formato relevante en ese canal, haciendo que el dispositivo de autenticación portátil transmita una respuesta que incluye la palabra de código especial
10 (identificación especial).

Al incluir información de secuencia en la baliza desde el nodo de desarmado, es posible que el dispositivo de autenticación portátil determine cuando finalizara la transmisión de baliza. Usando esta información, el dispositivo de autenticación portátil puede retrasar la transmisión de su
15 respuesta a la unidad central hasta que el nodo de desarmado haya terminado de transmitir, de modo que sea más fácil para la unidad central detectar la respuesta del dispositivo de autenticación portátil sin interferencia local. Esto significa que la potencia de transmisión del dispositivo de autenticación portátil puede mantenerse baja, prolongando la vida de la batería del dispositivo de
20 autenticación portátil, mientras sigue permitiendo que la unidad de control reciba la respuesta del dispositivo de autenticación portátil. Además, cuando el dispositivo de autenticación portátil captura paquetes de baliza, puede calcular

cuanto tiempo pasara antes de que termine la secuencia. Si los paquetes capturados están al principio de la secuencia, el dispositivo de autenticación portátil puede "posponer" o apagarse mientras espera que finalice la secuencia, y luego volver a activarse para transmitir su respuesta a la unidad central justo
5 después de que finalice la secuencia.

El dispositivo de autenticación portátil escuchara múltiples paquetes para poder usar estadísticas para obtener una cifra RSSI fiable, y puede informar sobre la cifra RSSI para cada uno de los paquetes detectados.

Como refinamiento, el controlador del dispositivo de autenticación
10 portátil puede usar información de movimiento del sensor de movimiento incorporado del dispositivo de autenticación portátil para controlar el sondeo mediante el transceptor del dispositivo de autenticación portátil. Es decir, el sondeo puede suspenderse en el caso de que el procesador considere que el dispositivo de autenticación portátil es estacionario, por ejemplo, si el sensor de
15 movimiento no detecta movimiento y el procesador determina que un recuento desde la ultima vez que se determino que el dispositivo de autenticación portátil se está moviendo es mas que un recuento umbral predeterminado, el dispositivo de autenticación portátil se considera estacionario y el sondeo puede suspenderse por completo o puede reducirse la frecuencia del sondeo
20 (la opción preferida, ya que eso significa que se puede hacer que los dispositivos de autenticación portátiles "perdidos" se anuncien en el próximo sondeo). Por ejemplo, la frecuencia de los sondeos puede reducirse a entre la

mitad y la vigésima parte, o menos, de la frecuencia habitual. Por el contrario, si el procesador determina que el dispositivo de autenticación portátil aun se está moviendo, o se ha estado moviendo recientemente (de modo que el dispositivo de autenticación portátil no se considera estacionario), se mantiene

5 la frecuencia de sondeo habitual. El procesador del dispositivo de autenticación portátil puede configurarse para que deje de generar el recuento de tiempo transcurrido desde que el dispositivo de autenticación portátil estuvo en movimiento por ultima vez después de que el recuento del tiempo transcurrido desde que el mando estuvo en movimiento por ultima vez alcanza el valor

10 umbral predeterminado, ya que esto puede reducir el consumo de energía del dispositivo de autenticación portátil, lo cual es bueno para mejorar la duración de la batería.

Para reducir el alcance efectivo de la baliza de radio, se transmite desde el nodo de desarmado a baja potencia (por ejemplo, -20 dBm o menos) con

15 una alta velocidad de datos (por ejemplo, 250 kbps o mas, digamos 400 kbps) y con un índice de modulación bajo, para dar un alcance efectivo de no mas de aproximadamente 5 metros. Al usar un índice de modulación subóptimo, logramos tres cosas: enviar rápidamente muchos paquetes, reducir la sensibilidad para disminuir el rango y ajustarse dentro del espectro dado.

20 Limitamos la potencia de salida del nodo de desarmado para limitar el rango. Para dificultar la recepción desde una distancia mayor, tenemos una velocidad de datos alta y un índice de modulación bajo. Sin embargo, la razón principal

no es el mal presupuesto del enlace, sino la velocidad. Cuanto mayor sea la velocidad de bits, mas paquetes se pueden usar para la estimación. La sensibilidad está en el rango de alrededor de -90 dBm con esta configuración e intentamos estar en línea de visión, lo que significa que la distancia desde el

5 transmisor se da como el desvanecimiento del canal con la distancia, usando la formula de Friis.

El cifrado, por ejemplo basado en claves compartidas, se usa preferentemente para todas las transmisiones desde y hacia la unidad de control en cada una de las realizaciones de la invención.

10 Como se ha mencionado previamente, otra opción para mejorar la seguridad, que se puede usar con cualquiera o todas las opciones anteriores para mejorar aun mas la seguridad del sistema, es para que el dispositivo de autenticación portátil incluya, en el mensaje de respuesta enviado a la unidad de control, detalles de los resultados de las determinaciones RSSI realizadas

15 por el dispositivo de autenticación portátil. En particular, el nodo de desarmado puede configurarse para enviar una serie de mensajes de activación cuando la unidad de control le solicite que envíe una instrucción de desarmado, preferentemente incluyendo un identificador de transmisión de desarmado único, al dispositivo de autenticación portátil. Y el dispositivo de autenticación

20 portátil puede configurarse para determinar el nivel RSSI de cada uno de los mensajes de la serie que se reciben desde el nodo de desarmado. El dispositivo de autenticación portátil puede configurarse para incluir en la

solicitud de desarmado enviada a la unidad central un informe basado en los niveles RSSI determinados. Por ejemplo, el dispositivo de autenticación portátil puede configurarse para enviar un resumen de los niveles RSSI medidos, tal como la cantidad de mensajes/paquetes medidos o medidos por encima de
5 cierto nivel, nivel máximo de RSSI, nivel medio de RSSI, etc.

El sistema puede usar la inclusión de los datos RSSI para reducir la susceptibilidad del sistema a "retransmitir ataques" del tipo usado para engañar a los sistemas de entrada pasiva (PES) de automóviles.

El dispositivo de autenticación portátil informaría de los valores RSSI
10 como, por ejemplo, valores máximos/mínimos, y un promedio, y la unidad central puede mantener valores preestablecidos de fábrica para un desarme "real", y/o estos pueden complementarse o reemplazarse con valores del mundo real obtenidos durante la puesta en marcha/prueba del sistema.

En lugar de que la unidad de control verifique la identidad del dispositivo
15 de autenticación portátil, también sería posible que los nodos de desarmado incluyan una lista de dispositivos de autenticación portátiles registrados y que los nodos de desarmado en lugar de que la unidad de control realice la verificación de la identidad del dispositivo de autenticación al recibir la respuesta de los dispositivos de autenticación de la señal de activación/baliza.
20 El nodo de desarmado, tras una autenticación exitosa, transmitiría un mensaje de desactivación de alarma a la unidad de control. Este enfoque requeriría, por supuesto, que la unidad de control actualice los nodos de desarmado con

adiciones y eliminaciones a la lista de dispositivos de autenticación registrados. Este es un enfoque menos preferido debido a la necesidad de aumentar la carga de mantener listas actualizadas tanto en la unidad de control como en los nodos de desarmado.

5 Asimismo, aunque como se ha descrito hasta ahora, la unidad central ha generado cualquier identificador de transmisión de desarme o ID de evento y luego se ha transmitido a un nodo de desarmado para incluirlo en un mensaje de activación del nodo de desarmado, otras alternativas son, por supuesto, posibles. Por ejemplo, el nodo de desarmado podría generar un identificador de
10 transmisión de desarmado o ID de evento y proporcionarlo a la unidad central para que la unidad central verifique cualquier transmisión del mando recibida en busca de la presencia del identificador de transmisión de desarmado o ID de evento correcto o verificarse a si mismo cualquier transmisión del mando recibida por la presencia del identificador de transmisión de desarme correcto o
15 ID de evento y transmitir el resultado de la verificación a la unidad central. En general, es preferible que la unidad central genere y verifique el identificador de transmisión de desarmado o la ID de evento, en lugar de delegar una o ambas funciones a un nodo de desarmado, porque esto reduce el riesgo de que un mal actor adopte la apariencia de un nodo de desarmado para engañar al
20 sistema.

Además de que puede usarse dentro del espacio monitorizado, un nodo de desarmado de acuerdo con las realizaciones de la invención podría

disponerse de manera útil fuera del espacio o edificio monitorizado como un medio para que un usuario desbloquee una puerta que da acceso al espacio de edificio monitorizado y que tiene una cerradura controlada electrónicamente, y desarmar el sistema de monitorización. La provisión de dicho nodo de desarmado ubicado externamente también podría permitir a un usuario bloquear la cerradura controlada electrónicamente de una puerta de acceso con o sin armar el sistema. Para este uso, un nodo de desarmado incluiría preferentemente una disposición de selector para permitir que un usuario inicie un evento. Por ejemplo, el nodo de desarmado podría incluir un selector para permitir que un usuario desbloquee la cerradura de una puerta controlada electrónicamente y desarmar el sistema de monitorización de un estado armado, un selector para bloquear la cerradura de la puerta y otro selector para armar el sistema o para bloquear la cerradura de la puerta y armar el sistema. Este bloqueo controlado electrónicamente normalmente incluiría un receptor de RF, por ejemplo, un transceptor de RF, para recibir mensajes de control para bloquear y desbloquear la cerradura, y normalmente también incluiría medios para descifrar mensajes cifrados recibidos por el receptor. Los selectores se pueden proporcionar en forma de teclado o como "botones" individuales, preferentemente usando tecnología de detección de capacitancia en lugar de interruptores mecánicos.

En uso, de acuerdo con una primera realización, y como se ilustra esquemáticamente en la Figura 8b, dicho nodo de desarmado ubicado

externamente reaccionaria al funcionamiento de uno de los selectores (evento #1) al iniciar un procedimiento de "activación en radio" (evento #3) efectivamente para buscar cualquier dispositivo de autenticación portátil de usuario dentro del alcance (dentro de 5 metros o menos, por ejemplo, dentro de 1 o 2 metros) del nodo de desarmado transmitiendo mensajes de activación generalmente como se describió anteriormente. El mensaje de activación incluye preferentemente una ID de evento única (por ejemplo, un número aleatorio) que cumple la misma función de mejora de seguridad que la ID de evento única que la unidad de control se ha descrito previamente como generadora para cada evento de apertura de la puerta. Además, el nodo de desarmado también transmitiría un informe (evento #2) a la unidad de control indicando el selector que se activo, es decir, informando a la unidad central de la solicitud del usuario. El informe del nodo de desarmado también incluye el identificador del nodo de desarmado y la ID de evento único (si se usa). Un dispositivo de autenticación portátil de usuario que recibe dicho mensaje de activación responde transmitiendo (evento #4) un mensaje a la unidad central, incluyendo la ID de evento único (si se usa) y su propia ID. Preferentemente, el dispositivo de autenticación portátil del usuario también está configurado para realizar mediciones RSSI en mensajes de activación recibidos desde el nodo de desarmado e incluir información sobre estas mediciones RSSI en el mensaje enviado a la unidad de control.

En una segunda realización alternativa, el nodo de desarmado ubicado

externamente reaccionaria al funcionamiento de uno de los selectores (evento #1) usando su transceptor RF para enviar un mensaje de solicitud de estado de cambio a la unidad de control (evento #2), incluyendo los detalles del cambio solicitado, junto con la ID del nodo de desarmado. El nodo central transmitiría

5 (evento #3) una respuesta que incluye la ID del nodo de desarmado, preferentemente junto con un identificador de evento único (por ejemplo, un número aleatorio) que es efectivo para hacer que el nodo de desarmado inicie un procedimiento de activación en radio. La respuesta de la unidad central podría incluir un comando para el nodo de desarmado, o el sistema podría

10 estar dispuesto de modo que el nodo de desarmado responda a la recepción de un mensaje de la unidad central que preferentemente incluya un identificador de evento único junto con la ID del nodo de desarmado iniciando el procedimiento de activación por radio. El nodo de desarmado que recibe tal respuesta, incluyendo su propia identificación, usaría su transceptor de RF

15 para transmitir (evento #4) señales de activación por radio, incluyendo el identificador de evento único (si se usa). Un dispositivo de autenticación portátil que recibe las señales de despertar en la radio despertaría y transmitiría una señal (evento #5) que incluye su propia ID y el identificador de evento único (si se usa). Si, como se prefiere, el dispositivo de autenticación portátil incluye un

20 acelerómetro, tal como se ha descrito anteriormente, entonces el procesador del dispositivo de autenticación portátil determinara si el dispositivo de autenticación portátil es estacionario o no, y solo transmitirá la respuesta en el

caso de que el dispositivo de autenticación portátil no se considere estacionario. Preferentemente, el dispositivo de autenticación portátil del usuario también está configurado para realizar mediciones RSSI en mensajes de activación recibidos desde el nodo de desarmado e incluir información sobre
5 estas mediciones RSSI en el mensaje enviado a la unidad central.

Tanto con la primera como con la segunda realización de este aspecto de la invención, la secuencia de operaciones continúa como sigue.

La unidad central, al recibir el mensaje del dispositivo de autenticación portátil del usuario, se comprueba si la ID del dispositivo de autenticación
10 portátil incluida en el mensaje está registrada en la unidad central y también si la ID del evento coincide con la de un evento "actual". Si el mensaje recibido del dispositivo de autenticación portátil del usuario incluye información RSSI, la unidad central también tendrá esto en cuenta al decidir si la solicitud de cambio de estado es válida. Si se determina que la unidad central es válida, entonces
15 la unidad central realiza la solicitud, por ejemplo, enviar un comando de desbloqueo a la cerradura de la puerta correspondiente (evento #6 en la figura 8a y evento #5 en la Figura 8b) y desarmar el sistema de monitorización de seguridad, o enviar un comando de bloqueo a la cerradura de la puerta correspondiente y armar el sistema. Además, la unidad central puede
20 configurarse para enviar una notificación de cambio de estado al nodo de desarmado (evento #6 en la figura 8a, y evento #5 en la figura 8b), incluyendo la ID del nodo de desarmado, para que el nodo de desarmado pueda indicar el

cambio de estado de forma visible o audible.

Asimismo, si el dispositivo de autenticación portátil del usuario incluye un dispositivo háptico, la unidad central puede transmitir una instrucción al dispositivo de autenticación portátil de mando para hacer que el dispositivo de autenticación portátil active el dispositivo háptico para indicar la finalización de la acción solicitada. Un dispositivo de autenticación portátil que tiene uno o más indicadores visuales, por ejemplo, uno o más LED, también puede activarse para proporcionar una indicación visual de la finalización de una acción solicitada.

10 Un dispositivo de autenticación portátil que tiene un elemento háptico también puede configurarse para proporcionar retroalimentación háptica al recibir un mensaje de activación de un nodo de desarmado (preferentemente un modo diferente de retroalimentación para completar con éxito una acción solicitada), para que un usuario sepa que el dispositivo de autenticación portátil
15 ha sido "encontrado" por el nodo de desarmado.

La unidad de control puede transmitir opcionalmente un mensaje de "fallo" de solicitud de acción, incluyendo la ID del nodo de desarmado, que el nodo de desarmado puede usar para proporcionar comentarios sobre el fracaso para completar una acción solicitada. La unidad central también puede
20 enviar un mensaje de fallo, incluyendo la ID del dispositivo de autenticación portátil, que el dispositivo de autenticación portátil puede usar para proporcionar comentarios sobre el fracaso para completar una acción

solicitada.

Si el sistema de monitorización de seguridad que tiene un nodo de desarmado fuera del edificio monitorizado o la zona monitorizada es uno que está conectado a una estación de monitorización central, puede ser útil para el propietario registrado del sistema de monitorización de seguridad estar informado de las solicitudes fallidas para cambiar el estado. En particular, cuando se realiza una solicitud de acción mediante el funcionamiento de un selector de eventos, y no se encuentra un dispositivo de autenticación portátil autorizado, o se reciben señales de una fuente no autorizada, la unidad de control puede informar de los detalles del evento a la estación central de monitorización. La estación central de monitorización puede actuar sobre tales informes, mediante, por ejemplo, enviando agentes humanos para inspeccionar las instalaciones, pero también puede enviar dichos informes al propietario registrado. Por ejemplo, el usuario registrado puede tener una "aplicación" de teléfono inteligente que puede organizarse para recibir notificaciones de la estación central de monitorización. La estación central de monitorización puede estar dispuesta para proporcionar notificaciones en tiempo real o casi en tiempo real de solicitudes de acciones fallidas. Dicho sistema puede mejorarse aun mas mediante la notificación a la aplicación de solicitudes de acción y sus resultados tanto para el éxito como para el fracaso, configurando la unidad central para informar todas las solicitudes de acción y sus resultados a la unidad central de monitorización.

Un sistema de monitorización de seguridad que usa un nodo de desarmado montado externamente también podría beneficiarse al incluir dispositivos de autenticación portátiles (por ejemplo, mandos) provistos de un acelerómetro, tal como se describe en el contexto de las realizaciones anteriores, para evitar problemas con un mando estacionario que permite el desarmado del sistema y el desbloqueo de la cerradura controlada electrónicamente.

Otros aspectos relacionados con las realizaciones del dispositivo de autenticación portátil incluyen lo siguiente:

1. Un dispositivo de autenticación portátil para usar con un sistema de monitorización de seguridad para un edificio o un espacio seguro dentro de un edificio u otra propiedad fija, incluyendo el sistema:

una unidad de control para controlar, armar y desarmar el sistema de monitorización de seguridad; un detector para detectar la irrupción de una entrada que da acceso al edificio o al espacio seguro; un nodo de desarmado para desarmar el sistema, teniendo el nodo de desarmado una interfaz de usuario para recibir una entrada del usuario para desarmar el sistema, y un transmisor de radiofrecuencia para transmitir, como consecuencia de la entrada del usuario, una señal de desarmado a la unidad de control; comprendiendo el dispositivo de autenticación portátil: un transceptor de radiofrecuencia, una memoria que almacena una ID del dispositivo de autenticación portátil, un sensor de movimiento y un procesador conectado operativamente al

transceptor, el sensor de movimiento y la memoria; en el que el sensor de movimiento está configurado para detectar el movimiento del dispositivo de autenticación portátil y para proporcionar una salida basada en el movimiento detectado del dispositivo de autenticación portátil, y en el que el procesador está configurado para determinar si el dispositivo de autenticación portátil está estacionario o en movimiento, en base a la salida del sensor de movimiento; en el que el dispositivo de autenticación portátil está configurado para recibir una instrucción de desarmado, a través del transceptor, desde el nodo de desarmado para transmitir a la unidad de control una solicitud de desarmado que contiene la ID del dispositivo de autenticación portátil; y en el que el procesador está configurado para transmitir la solicitud de desarmado ordenada sólo si, cuando se recibe la instrucción, el dispositivo de autenticación portátil no se considera estacionario.

2. El dispositivo de autenticación portátil según el párrafo 1, en el que el dispositivo de autenticación portátil se considera estacionario si el sensor de movimiento no detecta movimiento en el momento en que se recibe la instrucción.

3. El dispositivo de autenticación portátil según el párrafo 1, en el que el dispositivo de autenticación portátil se considera estacionario si el sensor de movimiento no ha detectado ningún movimiento del dispositivo de autenticación portátil durante un período predeterminado anterior al momento en que se recibe la instrucción.

4. El dispositivo de autenticación portátil según cualquiera de los párrafos anteriores, en el que el dispositivo de autenticación portátil está configurado para transmitir a la unidad de control la solicitud de desarmado que incluye un identificador de transmisión de desarmado recibido en la instrucción
5 de desarmado del nodo de desarmado.

5. El dispositivo de autenticación portátil según cualquiera de los párrafos anteriores, en el que el dispositivo de autenticación portátil está configurado para: activarse periódicamente de un estado de suspensión en el que su transceptor está inactivo a un estado parcialmente activo en el que sólo
10 parte del transceptor está activado para realizar una verificación RSSI para un primer período; volver al estado de suspensión al final del primer período a menos que la verificación de RSSI revele un nivel de RSSI por encima de un umbral predeterminado; permanecer en el estado parcialmente activo durante un segundo período, en el caso de que la verificación de RSSI revele un nivel
15 de RSSI por encima de un umbral predeterminado, para detectar la presencia de una palabra de sincronización; volver al estado de suspensión a menos que se detecte una palabra de sincronización antes del final del segundo período; y activar completamente el transceptor durante un tercer período, si se detecta una palabra de sincronización dentro del segundo período, para escuchar un
20 paquete de activación en radio.

6. El dispositivo de autenticación portátil del párrafo 5 en el que la duración del período entre eventos de activación es de al menos un segundo.

7. El dispositivo de autenticación portátil según cualquiera de los párrafos anteriores, en el que el dispositivo de autenticación portátil está configurado además para determinar el nivel RSSI de cada uno de una pluralidad de mensajes recibidos desde el nodo de desarmado; e incluir en la solicitud de desarmado enviada a la unidad de control información sobre los niveles RSSI determinados.

8. El dispositivo de autenticación portátil según cualquiera de los párrafos anteriores, en el que el dispositivo de autenticación portátil está configurado además para recibir una instrucción distinta de una instrucción de desarmado a través del transceptor, incluyendo un indicador, desde la unidad de control para realizar una acción; y en el que, en el caso de que la otra instrucción incluya el indicador, el procesador está configurado para hacer que el dispositivo de autenticación portátil realice la acción ordenada independientemente de que, cuando se recibe la instrucción, se determine que el dispositivo de autenticación portátil está estacionario.

9. El dispositivo de autenticación portátil del párrafo 8, en el que el dispositivo de autenticación portátil incluye uno o más de: un indicador visual, un transductor de audio, un transductor háptico, y está configurado además para generar una salida usando uno o más de estos cuando así lo indique un recibió instrucciones, incluido el indicador.

10. El dispositivo de autenticación portátil de cualquiera de los párrafos 1 a 8, en el que el dispositivo de autenticación portátil incluye un

transductor háptico y además está configurado para generar una salida usando el transductor háptico en respuesta a recibir la instrucción de desarmado.

11. El dispositivo de autenticación portátil de cualquiera de los párrafos anteriores, en el que el transceptor de radiofrecuencia del dispositivo de autenticación portátil está configurado para recibir la instrucción de desarmado en una frecuencia en la banda de 869,7 a 870 MHz.

12. El dispositivo de autenticación portátil de cualquiera de los párrafos anteriores, en el que el dispositivo de autenticación portátil está configurado para: recibir la instrucción de desarmado en un primer canal de radio, incluyendo la instrucción de desarmado instrucciones para transmitir el mensaje de desarmado que contiene la ID del dispositivo de autenticación portátil en un segundo canal de radio cuyos parámetros de transmisión son diferentes a los del primer canal de radio y están especificados en las instrucciones recibidas; y controlar el transceptor para transmitir el mensaje que contiene la ID del dispositivo de autenticación portátil en el segundo canal de radio usando los parámetros de transmisión especificados.

13. El dispositivo de autenticación portátil del párrafo 12, en el que el dispositivo de autenticación portátil está configurado para controlar el transceptor para transmitir el mensaje que contiene un identificador de transmisión de desarmado recibido en la instrucción de desarmado.

14. El dispositivo de autenticación portátil de cualquiera de los párrafos anteriores, en el que el dispositivo de autenticación portátil está

configurado para apagar su transceptor una vez que se considera que el dispositivo de autenticación portátil está estacionario.

15 15. El dispositivo de autenticación portátil del párrafo 14, en el que el dispositivo de autenticación portátil está configurado para no encender su transceptor nuevamente hasta que el procesador determine nuevamente que el dispositivo de autenticación portátil está en movimiento.

16. El dispositivo de autenticación portátil de cualquiera de los párrafos anteriores, en el que el sensor de movimiento comprende un acelerómetro.

10 17. El dispositivo de autenticación portátil del párrafo 16, en el que el acelerómetro es un acelerómetro de 3 ejes.

15 18. Un sistema de monitorización de seguridad para un edificio o un espacio seguro dentro de un edificio u otra propiedad fija, incluyendo el sistema: un detector para detectar la irrupción de una entrada que da acceso al edificio o al espacio seguro; una unidad de control; un nodo de desarmado para desarmar el sistema, teniendo el nodo una interfaz de usuario para recibir una entrada del usuario para desarmar el sistema, y un transmisor de radiofrecuencia para transmitir, como consecuencia de la entrada del usuario, una señal de desarmado a la unidad de control; y un dispositivo de autenticación portátil tal como se define en cualquiera de los párrafos 1 a 3 para permitir el desarmado con manos libres del sistema de monitorización de seguridad; teniendo la unidad de control un transceptor de radiofrecuencia y

20

una memoria que almacena una identidad del dispositivo de autenticación portátil para el dispositivo de autenticación portátil; la unidad de control que se está configurando: en respuesta a recibir una notificación de una irrupción de entrada del detector, para:

5 (i) iniciar un temporizador del período de entrada;

 (ii) transmitir un mensaje de activación al nodo de desarmado para provocar que el transmisor de RF del nodo de desarmado transmita una señal/baliza de activación para activar el dispositivo de autenticación portátil; y

 (iii) en respuesta a recibir, antes de que expire el temporizador del
10 período de entrada, una señal de desarmado de radiofrecuencia desde el dispositivo de autenticación portátil que incluye la identidad registrada del dispositivo de autenticación portátil, para desarmar el sistema de monitorización de seguridad; y

 (iv) en el caso de que el sistema de monitorización de seguridad no se
15 desactive antes de que expire el período de entrada, hacer que el sistema de monitorización de seguridad entre en un estado de alarma;

 (v) en el que, además: la unidad de control está configurada para iniciar un temporizador de desarmado de manos libres en respuesta a recibir una notificación de una infracción de entrada desde el detector, y en el caso de que
20 no se reciba ninguna señal de RF que incluya la identidad del dispositivo de autenticación portátil registrado antes de que expire el temporizador de desarmado de manos libres, transmitir una señal al nodo para hacer que el

nodo de desarmado proporcione una notificación en el sentido de que el intento de desarmado de manos libres ha fallado; o

(vi) el nodo de desarmado está configurado para iniciar su propio temporizador de desarmado de manos libres en respuesta a recibir el mensaje de activación de la unidad de control y, en el caso de que el temporizador de desarmado de manos libres del nodo de desarmado expire sin el desarmado habiendo sido informado el nodo por la unidad de control del desarmado del sistema de monitorización de seguridad, proporcionar una notificación en el sentido de que el intento de desarmado con manos libres ha fallado.

10 19. El sistema de monitorización de seguridad como se define en el párrafo 18, en donde la unidad de control está configurada para: incluir un identificador de transmisión de desarmado en el mensaje de activación, y el mensaje de activación está dispuesto para hacer que el nodo de desarmado incluya el identificador de transmisión de desarmado en la señal/baliza de
15 activación transmitida desde el transmisor de RF del nodo de desarmado; solo desarmar el sistema de monitorización de seguridad en respuesta a recibir antes de la expiración del temporizador del período de entrada una señal de desarmado de radiofrecuencia que incluye la identidad registrada del dispositivo de autenticación portátil desde el dispositivo de autenticación portátil
20 si la señal de desarmado también incluye el identificador de transmisión de desarmado; y en el caso de que la unidad de control esté configurada para iniciar un temporizador de desarmado de manos libres, transmitir una señal

para hacer que el nodo de desarmado proporcione una notificación en el sentido de que el intento de desarmado de manos libres ha fallado solo si no se recibe ninguna señal de RF que incluye la identidad del dispositivo de autenticación portátil registrado y el identificador de transmisión de desarmado
5 antes de que expire el temporizador de desarmado de manos libres.

20. El sistema de monitorización de seguridad como se define en el párrafo 18 o 19, que incluye múltiples nodos de desarmado, cada uno asociado con una entrada diferente que da acceso al edificio o al espacio seguro, teniendo cada nodo de desarmado una ID de nodo de desarmado única,
10 teniendo cada una de las diferentes entradas una respectiva detector con una ID respectiva diferente, y la unidad de control almacena las ID de los nodos de desarmado, las ID de los detectores y una asociación entre cada detector y uno asociado de los nodos de desarmado; en el que la unidad de control está configurada, en respuesta a recibir una notificación de irrupción de entrada
15 desde un detector, para usar un identificador de detector incluido en la notificación recibida para identificar el nodo de desarmado asociado y para incluir el identificador del nodo de desarmado para el nodo de desarmado identificado en el mensaje de activación transmitido para apuntar selectivamente al nodo de desarmado identificado entre los múltiples nodos de
20 desarmado del sistema.

21. El sistema de monitorización de seguridad de cualquiera de los párrafos 18 a 20, en donde el o cada detector es un detector de movimiento,

por ejemplo un detector PIR.

22. El sistema de monitorización de seguridad de cualquiera de los párrafos 18 a 20, en donde el o cada detector es un sensor de puerta, por ejemplo un sensor de contacto magnético.

5 23. El sistema de monitorización de seguridad de cualquiera de los párrafos 18 a 22, en el que el dispositivo de autenticación portátil está configurado para: activarse periódicamente de un estado de suspensión en el que su transceptor está inactivo a un estado parcialmente activo en el que sólo parte del transceptor está activado para realizar una verificación RSSI para un
10 primer período; volver al estado de suspensión al final del primer período a menos que la verificación de RSSI revele un nivel de RSSI por encima de un umbral predeterminado; permanecer en el estado parcialmente activo durante un segundo período, en el caso de que la verificación de RSSI revele un nivel de RSSI por encima de un umbral predeterminado, para detectar la presencia
15 de una palabra de sincronización; volver al estado de suspensión a menos que se detecte una palabra de sincronización antes del final del segundo período; y activar completamente su transceptor durante un tercer período, si se detecta una palabra de sincronización dentro del segundo período, para escuchar un paquete de activación por radio.

20 24. El sistema de monitorización de seguridad de cualquiera de los párrafos 18 a 23, en donde el dispositivo de autenticación portátil está configurado para determinar el nivel RSSI de cada uno de uno o más mensajes

recibidos desde el nodo de desarmado; e incluir en la solicitud de desarmado enviada a la unidad de control información sobre los niveles RSSI determinados.

25. El sistema de monitorización de seguridad del párrafo 24, en
5 donde la unidad de control está configurada para desarmar el sistema de monitorización de seguridad en respuesta a recibir la señal de desarmado de radiofrecuencia desde el dispositivo de autenticación portátil solo en el caso de que la información RSSI satisfaga criterios predeterminados.

26. Un procedimiento para operar un dispositivo de autenticación
10 portátil para usar con un sistema de monitorización de seguridad para un edificio o un espacio seguro dentro de un edificio u otra propiedad fija, incluyendo el sistema: una unidad de control para controlar, armar y desarmar el sistema de monitorización de seguridad; un detector para detectar la irrupción de una entrada que da acceso al edificio o al espacio seguro; un nodo
15 de desarmado para desarmar el sistema, teniendo el nodo una interfaz de usuario para recibir una entrada del usuario para desarmar el sistema, y un transmisor de radiofrecuencia para transmitir, como consecuencia de la entrada del usuario, una señal de desarmado a la unidad de control; comprendiendo el dispositivo de autenticación portátil: un transceptor de radiofrecuencia, una
20 memoria que almacena una ID del dispositivo de autenticación portátil, un sensor de movimiento y un procesador conectado operativamente al transceptor, el sensor de movimiento y la memoria; comprendiendo el

procedimiento: usar el sensor de movimiento para detectar el movimiento del dispositivo de autenticación portátil; proporcionar una salida basada en el movimiento detectado del dispositivo de autenticación portátil; determinar, usando el procesador, si el dispositivo de autenticación portátil está
5 estacionario o en movimiento, en base a la salida del sensor de movimiento; recibir una instrucción de desarmado, a través del transceptor, desde el nodo de desarmado para transmitir a la unidad de control una solicitud de desarmado que contiene la ID del dispositivo de autenticación portátil; y cuando se recibe la instrucción, determinar si el dispositivo de autenticación portátil se
10 considera estacionario; y, sólo si se considera que el dispositivo de autenticación portátil no está estacionario, transmitir la solicitud instruida.

27. El procedimiento del párrafo 26, en el que la instrucción de desarmado recibida por el transceptor incluye un identificador de transmisión de desarmado y una instrucción para incluir el identificador de transmisión de
15 desarmado en la solicitud de desarmado.

28. El procedimiento del párrafo 26 o del párrafo 27, en el que el dispositivo de autenticación portátil se considera estacionario si el sensor de movimiento no detecta movimiento en el momento en que se recibe la instrucción.

20 29. El procedimiento del párrafo 26 o del párrafo 27, en el que el dispositivo de autenticación portátil se considera estacionario si el sensor de movimiento no ha detectado ningún movimiento del dispositivo de autenticación

portátil durante un período predeterminado anterior al momento en que se recibe la instrucción.

30. El procedimiento de cualquiera de los párrafos 26 a 29, que comprende además: determinar el nivel RSSI de uno o más mensajes recibidos desde el nodo de desarmar; e incluir en la solicitud de desarmado enviada a la unidad de control información sobre los niveles RSSI determinados.

31. El procedimiento de cualquiera de los párrafos 26 a 30, que comprende además, después de transmitir la solicitud de desarmado a la unidad de control: recibir una instrucción de la unidad de control para generar una señal que indique el desarmado exitoso del sistema; y generar la señal que indica el desarmado exitoso del sistema.

32. El procedimiento de cualquiera de los párrafos 26 a 31, incluido el apagado del transceptor del dispositivo de autenticación portátil en caso de que el dispositivo de autenticación portátil se considere estacionario.

33. El procedimiento del párrafo 32, que incluye: mantener el transceptor del dispositivo de autenticación portátil en estado apagado hasta que el procesador determine nuevamente que el dispositivo de autenticación portátil está en movimiento; y encender el transceptor del dispositivo de autenticación portátil una vez que el procesador determina que el dispositivo de autenticación portátil está en movimiento.

34. El procedimiento de cualquiera de los párrafos 26 a 29, en el que el dispositivo de autenticación portátil: se activa periódicamente de un estado

de suspensión en el que su transceptor está inactivo a un estado parcialmente activo en el que sólo parte del transceptor está activado para realizar una verificación RSSI para un primer periodo; vuelve al estado de suspensión al final del primer período a menos que la verificación de RSSI revele un nivel de RSSI por encima de un umbral predeterminado; permanece en el estado parcialmente activo durante un segundo período, en el caso de que la verificación de RSSI revele un nivel de RSSI por encima de un umbral predeterminado, y escucha la presencia de una palabra de sincronización; vuelve al estado de suspensión a menos que se detecte una palabra de sincronización antes del final del segundo período; y activa completamente su transceptor durante un tercer período, si se detecta una palabra de sincronización dentro del segundo período, y escucha un paquete de activación por radio.

15

20