(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 440 248**

(51) Int. CI.:

G08B 13/00 (2006.01)
G08B 13/22 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **27.04.2007 E 07719653 (3)**

(97) Fecha y número de publicación de la concesión europea: **02.10.2013 EP 1946276**

(54) Título: **Control de entrada con sistema de seguridad**

(30) Prioridad:

04.05.2006 US 381675
25.09.2006 WO PCT/CA2006/001578
11.01.2007 US 884536 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.01.2014

(73) Titular/es:

HERSHKOVITZ, SHMUEL (100.0%)
53 FORTUNE BAY INLET
FREEPORT, BS

(72) Inventor/es:

HERSHKOVITZ, SHMUEL

(74) Agente/Representante:

PONTI SALES, Adelaida

DESCRIPCIÓN

Control de entrada con sistema de seguridad.

Campo de la invención

[0001] La presente invención trata sobre sistemas de seguridad contra intrusiones y, en particular sobre la activación y desactivación del control de dichos sistemas de seguridad.

Antecedentes de la invención

[0002] Un sistema de seguridad convencional consta de una cantidad de sensores o detectores para detectar una intrusión en instalaciones protegidas, como p. ej., una vivienda u oficina, mediante un sistema de control para interpretar las señales de los detectores o sensores con el fin de generar una alarma. El sistema de control para pequeños sistemas de seguridad consta típicamente de un solo panel de control y de un solo teclado. El panel de control está conectado por cable o de forma inalámbrica a todos los sensores y detectores, y ejerce control sobre la generación de alarmas sea mediante una sirena local o mediante una conexión de telecomunicación, como p. ej., una red telefónica o una red cableada. El panel de control también está conectado al teclado que sirve de interfaz del usuario dentro de las instalaciones protegidas para activar y desactivar el sistema de seguridad y para programar o configurar el sistema de seguridad.

[0003] La mayoría de los sistemas de seguridad permiten que el usuario ingrese un código mediante el teclado para activar el sistema de seguridad y el mismo código o uno diferente para desactivarlo. El teclado se encuentra en un lugar seguro dentro de las instalaciones protegidas y para aquellos detectores que detectan el ingreso o la salida, se utiliza un temporizador para demorar la acción de generar la alarma desde el momento en que el sensor o detector genera una señal de intrusión. Este temporizador se puede definir en una demora de 15 a 60 segundos para dar tiempo a que el usuario entre o salga.

[0004] En muchos sistemas, el teclado también se puede usar para programar o definir funciones, como p. ej., que sensores o detectores, identificados como zonas dentro de las instalaciones protegidas sean activados o desactivados. Para ello se suele utilizar el teclado y, en muchos sistemas, el usuario ingresa un código de seguridad especial por medio del teclado para ingresar un modo de programación o de definición.

[0005] Otra característica común que se puede programar o definir mediante el teclado es el modo de permanencia. El modo de permanencia es un modo activado en el cual las instalaciones continúan protegidas contra intrusiones mientras los ocupantes permanecen en las instalaciones. En este modo de operación, no se toma en cuenta la detección de sensores y detectores dentro de las instalaciones protegidas, por ejemplo, los detectores infrarrojos pasivos de movimiento, los detectores de intrusión de microondas de desplazamiento Doppler, los sensores de puertas de paso internas y los sensores de celdas de carga del piso. Sólo los sensores y detectores que monitorizan esencialmente entradas y salidas permanecen activados. El modo de permanencia se configura típicamente mediante el ingreso del modo de programación y la selección de zonas que estarán desactivadas durante el modo de permanencia. El modo de permanencia se activa y desactiva (para ingresar en el modo de ausencia) mediante la introducción de un código de seguridad y la selección del modo de permanencia o de ausencia. El modo de permanencia protege el perímetro de las instalaciones y es muy importante en zonas en que existe alguna amenaza de intrusión mientras los ocupantes se encuentran dentro de las instalaciones. Cuando el ocupante de las instalaciones protegidas que se encuentran en el modo de permanencia decide salir, el sistema se desactiva y se vuelve a activar en el modo de ausencia, en el cual los sensores y detectores de las instalaciones protegidas están activos.

[0006] Estos sistemas de seguridad convencionales son vulnerables a los intrusos que pueden vigilar las instalaciones desde afuera y entrar en ellas en el momento en que un ocupante entra o sale y los demás ocupantes permanecen dentro con el sistema de seguridad activado en el modo de permanencia. Como consecuencia del uso del temporizador para permitir el ingreso o la salida, una o más zonas del sistema de seguridad queda inactiva durante el período definido; en ese período no sólo el ocupante puede salir o entrar sin generar una alarma sino también un intruso. Una vez dentro de las instalaciones, el modo de permanencia permite que el intruso se desplace sin generar ninguna alarma. Dado que el ocupante puede llamar al número de telefónico para emergencias (911) o utilizar un botón de pánico del sistema de seguridad para generar una alarma, los intrusos pueden recurrir a la violencia para dominar a los ocupantes que permanecen dentro de las instalaciones. Si bien se puede generar una alarma más tarde después de que el intruso haya abandonado las instalaciones, se trata de un problema menor para el intruso y la alarma simplemente no cumple su función. Cuando un usuario ingresa en instalaciones protegidas por un sistema convencional, existe una demora de entrada para que ingrese el código; de lo contrario, se genera una alarma al término de ese período de demora. Cuando se ingresa el código, el sistema se desactiva por completo. Desde ese momento y hasta que el sistema se vuelva a activar en el modo de permanencia las instalaciones en su totalidad están desprotegidas. Se trata de un proceso de dos pasos, a saber, primero se debe ingresar un código para desactivar el sistema y luego, otro código para activarlo. Esta demora para ingresar los dos códigos puede ser suficiente para que un intruso aproveche el hecho de que el sistema está desactivado. El intruso que observa y

conoce los hábitos de los ocupantes puede esperar a que alguien salga o entre en las instalaciones para ingresar por cualquiera de las zonas.

[0007] En el documento de patente US 6.111.502 se describe un sistema de seguridad que opera en diversos modos (es decir, las horas de oficina, noche o fin de semana), el sistema dispone de un sistema de vigilancia perimetral, un sistema de vigilancia volumétrica y un control de acceso de puerta principal. Durante las horas de oficina, el sistema de seguridad está desactivado. Por la noche, el sistema de vigilancia perimetral está activado pero el sistema de vigilancia volumétrica sólo se activa si ningún trabajador permanece en el lugar. En el modo de fin de semana, el sistema de vigilancia del perímetro permanece activado pero el sistema de vigilancia volumétrica se desactiva si el control de acceso de puerta principal permite a una persona a entrar por la autenticación de insignia. Sin embargo, la puerta principal no está protegida por el sistema de vigilancia perimetrales y es vulnerable a los intrusos.

[0008] El documento US 5.461.372 constituye el estado más cercano de la técnica. Este documento divulga un sistema y método para modificar los niveles de seguridad dentro de un sistema de seguridad. De acuerdo con esta descripción, se aplican los cambios si así se requiere a los puntos de detección sujetos a predefinido estado de activado individuo en diferentes modos. Esta técnica anterior no divulga el establecimiento de un temporizador de cuenta atrás para proporcionar una demora entre la detección de una intrusión y la generación de una alarma, ni la emisión de una señal de paso en la autenticación, ni la eliminación de o ignorar el primero evento de intrusión en la memoria en respuesta a dicha generación de paso.

[0009] El aprovisionamiento de una demora para facilitar un procedimiento de ingreso es en sí mismo conocido en la técnica. Por ejemplo, el documento "Galaxy 16 and 15 plus User's guide" (Honeywell Security / Ademco Microtech) divulga una funcionalidad tal. En el sistema Galaxy mencionado, sin embargo, se produce una alarma incondicionalmente a desviación de una zona de entrada durante el procedimiento de ingreso. El sistema carece, por lo tanto, la flexibilidad de reconocer, ya sea desviaciones legítimas de la zona de entrada o intrusiones ilegítimas pasando por una zona de entrada. La presente invención, definida por las reivindicaciones adjuntas, soluciona las deficiencias antes mencionadas.

Resumen de la invención

[0010] De acuerdo con un primer aspecto de la presente invención, se ofrece un sistema de seguridad que permite al usuario entrar o salir de instalaciones protegidas sin comprometer la seguridad del resto del sistema, de acuerdo con la reivindicación 1.

[0011] De acuerdo con un segundo aspecto de la presente invención, se ofrece un sistema de seguridad que al estar activado en un modo de ausencia activa de inmediato, con una sola acción, el modo de permanencia (sin que antes se haya producido una desactivación temporaria) cuando el usuario ingresa en las instalaciones y digita un código.

[0012] De acuerdo con un tercer aspecto de la presente invención, se ofrece un sistema de seguridad que incluye un teclado para que el usuario ingrese el código de seguridad cuyo ingreso especifica la acción del código que incluye activar o desactivar el sistema y, por lo menos, una entrada o salida. A los efectos de la entrada, la autenticación de la persona que ingresa en las instalaciones es importante; mientras que para salir la autenticación se puede lograr en algunas formas de realización presionando una tecla del teclado sin necesidad de recurrir al uso de contraseñas.

[0013] De acuerdo con un cuarto aspecto de la presente invención, se suministra un sistema de seguridad en el que se usa un teclado satélite para ingresar el código cerca de un punto de entrada o de salida de las instalaciones protegidas que se utiliza para ingresar un código de entrada o de salida. Este teclado se puede usar para autenticar una salida presionando un botón porque el teclado se encuentra dentro de las instalaciones con seguridad desactivada y el paso de salida principal relacionado con el teclado no es ambiguo.

[0014] De acuerdo con un quinto aspecto de la presente invención, se ofrece un sistema de seguridad que puede ser usado por, al menos, algunos usuarios en todo momento en el modo de permanencia y tales usuarios sólo cuentan con códigos para permitir el ingreso y la salida, mientras que otros tienen códigos para activar y desactivar el sistema de seguridad en su totalidad además de aquellos códigos de entrada y de salida.

[0015] De acuerdo con un sexto aspecto de la presente invención, se ofrece un sistema de seguridad que tiene más de una configuración de modo de permanencia con la posibilidad de seleccionar una configuración deseada entre las configuraciones del modo de permanencia. Tales configuraciones se pueden organizar como una función con distintos niveles de seguridad y, opcionalmente, el nivel de seguridad puede aparecer indicado en la interfaz de usuario. Un ejemplo de tales configuraciones diferentes es el modo de permanencia nocturna en el cual las zonas para dormir no están activadas mientras que las de uso diurno están activadas y un modo de permanencia diurno en el que todas las zonas interiores no están activadas. En general, las configuraciones del modo de permanencia están determinadas por el uso que el ocupante hace de las instalaciones, es decir, los sectores que no se usan están activados y los que se usan, desactivados, mientras que el perímetro interior-exterior permanece activado.

Una puerta de vidrio corrediza en una plataforma cercada puede estar desactivada en el modo de permanencia en caso de que las áreas exteriores sean consideradas parte de las instalaciones protegidas. Otras puertas y ventanas pueden estar activadas.

[0016] En caso de que la interfaz de usuario (por ejemplo, el teclado) se encuentre en una zona interior en la que la alarma está activada, se puede usar un teclado satélite dentro del área sin seguridad activada para alternar entre las configuraciones del modo de permanencia antes de que los ocupantes ingresen en una zona interior con seguridad activada o se pueda realizar una autenticación de paso inmediatamente después de ingresar en una zona interior activada.

[0017] De acuerdo con un séptimo aspecto de la presente invención, se ofrece un sistema de seguridad cuyas zonas con detectores están clasificadas con "demora de entrada o de salida" o con "alarma inmediata", en el último caso, el usuario debe suministrar una autenticación de desactivación específica o bien, se dispara la alarma de inmediato sin que el usuario pueda detenerla. La autenticación de desactivación específica puede estar disponible opcionalmente, para una cantidad reducida de usuarios u ocupantes; mientras que la autenticación de entrada o de salida por zonas específicamente identificadas a este fin puede estar disponible para todos los usuarios u ocupantes autorizados. Para evitar falsas alarmas, sería conveniente combinar la seguridad física, como por ejemplo, cerrojos y candados, a fin de evitar que los ocupantes o usuarios (en especial aquellos que no están autorizados para utilizar la autenticación de desactivación específica) utilicen accidentalmente las puertas clasificadas como de "alarma inmediata".

[0018] Opcionalmente, el sistema de seguridad se puede programar con distintas clasificaciones de seguridad para las zonas con la posibilidad de seleccionar una de las configuraciones de clasificación deseada. La configuración de clasificación se puede combinar con la del modo de permanencia, de acuerdo con el sexto aspecto de la presente invención. De este modo se puede elegir cómo organizar las configuraciones según el nivel de seguridad.

[0019] De acuerdo con un octavo aspecto de la invención, se ofrece un sistema de seguridad que funciona con un transmisor inalámbrico para autorizar entradas y salidas. El transmisor se puede usar como sustituto de la introducción del código manual o como primer paso de la autenticación, a saber, para habilitar una demora para la función de entrada o de salida (sin generar una alarma inmediata) sin eximir al usuario de la introducción de códigos o de autenticaciones. En caso de que el sistema de seguridad esté configurado para permitir el ingreso o salida utilizando distintos recorridos por las instalaciones protegidas y el transmisor inalámbrico tenga un alcance suficiente para detectar el ingreso o la salida cuando éstas se realizan por recorridos distintos, la invención ofrece la posibilidad de determinar un recorrido para entrar o salir siguiendo las autorizaciones del transmisor inalámbrico mediante la detección de una zona para distinguir recorridos dentro del sistema de seguridad.

[0020] De acuerdo con un noveno aspecto de la invención, se ofrece un sistema de seguridad que cuenta con una zona de omisión que se reactiva automáticamente cuando se detecta que ya no se necesita omitirla. Por ejemplo, la omisión de una zona que representa un sensor de ventana se puede autenticar mediante el teclado y la omisión se levanta automáticamente cuando la ventana se vuelve a cerrar. De este modo, el uso de la omisión es más seguro y más práctico dado que no es necesario utilizar el teclado para anular la omisión. La anulación de la omisión se puede producir instantáneamente o con una breve demora de unos pocos segundos, proporcionando esta última opción una función de "anulación de rebote".

Breve descripción de las figuras

[0021] La presente invención se podrá comprender mejor mediante la siguiente descripción detallada que hace referencia a las figuras adjuntas, a saber:

La Figura 1 es un diagrama de flujo que ilustra la secuencia de pasos operacionales de un sistema de seguridad que se encuentra en un modo de permanencia de acuerdo con un ejemplo.

La Figura 2 es un diagrama esquemático de bloques de un sistema de seguridad de acuerdo con la invención que tiene un controlador de autorización de entradas que genera una señal de paso para cancelar un evento de intrusión.

La Figura 3 es un diagrama esquemático de bloques de un sistema de seguridad que tiene un controlador de autorización de entradas que genera una señal de paso específica de una zona para cancelar un evento de intrusión en un zona específica;

La Figura 4 es un diagrama esquemático de bloques de un sistema de seguridad que tiene un controlador de autorización de entradas que funciona junto con un controlador de autenticación de activación y desactivación para generar una señal de paso para cancelar un evento de intrusión.

La Figura 5a es una representación esquemática del contenido de una pila de eventos de intrusión que corresponde a la forma de realización de la Figura 2 para dos entradas dentro de las instalaciones protegidas con un único paso autenticado;

La Figura 5b es una representación esquemática del contenido de una pila de eventos de intrusión que corresponde a la forma de realización de la Figura 3 para una salida y una entrada de intruso autorizada dentro de las instalaciones protegidas con un único paso autenticado específico de una zona;

La Figura 5c es una representación esquemática del contenido de una pila de eventos de intrusión que corres ponde a la forma de realización de la Figura 3 para dos entradas en las instalaciones protegidas con un único paso autenticado específico de una zona; y

La Figura 6 es un diagrama de bloques de hardware de una posible instrumentación de la invención.

Descripción detallada de la invención

[0022] En la Figura 1, se resume esquemáticamente el funcionamiento de un sistema de seguridad en el cual los pasos 30 a 40 son similares a los de los sistemas convencionales, mientras que los pasos 50 y superiores son nuevos. Un sistema de seguridad se activa en un "modo de permanencia" único en el paso 30 y, en tanto y en cuanto, los sensores y detectores activos del modo de permanencia no detecten intrusión alguna (paso 32), no se toma ninguna medida.

[0023] La activación del sistema en el modo de permanencia implica la selección de uno de una cantidad de modos de permanencia con distintos niveles de seguridad. Estos diferentes "modos de permanencia" pueden corresponder a diferentes particiones de las instalaciones protegidas y a distintos niveles de seguridad. Una vez detectada una intrusión, se inicia una cuenta regresiva de demora de entrada o de salida en el paso 33. De inmediato, se indica la zona de la intrusión en la interfaz de usuario del sistema de seguridad en el paso 34.

[0024] Opcionalmente y de acuerdo con algunas formas de realización de la invención, se pueden clasificar las zonas como "de alarma con demora de entrada/salida" o "de alarma inmediata". Si la intrusión detectada en el paso 32 se produce en una zona clasificada como "de alarma inmediata", el sistema puede pasar sin dilación al paso 37 o bien, puede funcionar con cierta demora sin ofrecer la opción de autenticación de paso normal. Esto se puede hacer según el funcionamiento convencional de este tipo de sistemas que exige que el usuario introduzca un código de desactivación del sistema 13 (paso 35) que, de acuerdo con la presente invención, puede no ser conocido por todos los usuarios u ocupantes o bien, según el ejemplo de la Figura 1 con el paso 50, pero con una autenticación especial. Si la zona está clasificada como zona con "alarma de demora de entrada/salida", el proceso se realiza según lo indica la Figura 1.

[0025] En el modo de operación convencional, el usuario sólo tiene dos opciones: no hacer nada, y el sistema de seguridad generará una alarma una vez que haya transcurrido la demora (pasos 36 y 37) o desactivar el sistema antes de que transcurra el lapso de demora (pasos 35 y 38). Una vez que el sistema se desactiva en el paso 38, el usuario debe volver a activarlo en el paso 39 para volver a estar protegido. Sin embargo, el sistema de seguridad aplica la demora de salida normal en el paso 40 antes de dar comienzo al modo de permanencia activado normal en el paso 30.

[0026] En el ejemplo de la Figura 1, el usuario tiene una opción adicional de autenticar un paso (paso 50) para autorizar el ingreso o la salida de las instalaciones protegidas antes de que transcurra el período de demora. La autenticación de paso en el paso 50 puede requerir la introducción de un código especial en un teclado u otro medio de autenticación equivalente por parte de un ocupante de las instalaciones protegidas. Cuando se usa la autenticación de paso, el sistema de seguridad permanece activado y en funcionamiento para todas las demás zonas. Para la zona que se usó para el ingreso o la salida, el sistema detectará que la zona está "abierta", es decir que se detecta la intrusión, y que luego está "cerrada", es decir cuando cesa la detección de la intrusión. El sistema se asegurará de que la detección de la intrusión cese en el paso 51, por ejemplo, el sensor de la puerta detecta que la puerta se ha cerrado después de una entrada o salida. Se puede proporcionar una demora por el tiempo máximo que una puerta puede quedar abierta antes de que comience a sonar la alarma. Cuando la puerta se cierra, la zona de la puerta se puede volver a activar de inmediato (o bien, puede volver a activarse después de una breve demora de "anulación de rebote" de unos pocos segundos para asegurarse de que la puerta se ha cerrado bien y permanentemente) o, en particular, en el caso de una salida, puede permanecer sin activar por el lapso especificado para la demora de salida. A continuación, la pantalla de la zona en la interfaz del sistema de seguridad en la que tuvo lugar la intrusión se restablece en el paso 52, y se restablece la demora de entrada/salida en el paso 53. Posteriormente, el sistema de seguridad regresa al modo de permanencia activado normal en el paso 30.

[0027] Las Figuras 2 a 4 ilustran esquemáticamente un sistema de seguridad de acuerdo con una primera forma de realización. Tal ilustración esquemática tiene el propósito de ayudar a comprender la invención, sin seguir necesariamente una forma de instrumentación real que puede incluir circuitos lógicos dedicados, circuitos programados, un microcontrolador programado, una computadora programada o cualquier combinación de los

anteriores. En una forma de realización, el sistema de seguridad comprende los elementos ilustrados en la Figura 6, específicamente, un microcontrolador 60 programado con un código de programa apropiado que, al ejecutarse, realiza la acción ilustrada en la Figura 1, una fuente de alimentación 61 con respaldo de batería y un convertidor de CA a CC, un oscilador de fuente de señal con reloj 62 y una memoria no volátil 63. Una unidad con teclado y pantalla 64 del sistema de seguridad está conectada al microcontrolador 60 a través del bus serial 65.

[0028] En las Figuras 2, 3 y 4, los sensores y detectores de seguridad 10 de las instalaciones protegidas están conectados mediante una conexión segura (cableada, óptica o inalámbrica) a un gestor de alarmas 16 a través de un filtro de modo de permanencia o de ausencia 12. Las entradas de zona pueden ser señales analógicas generadas por detectores de intrusión conectados a pines ADC del microcontrolador 60 y un módulo de software que se ejecuta en el procesador 60 puede interpretar los estados analógicos y mantener un registro o almacenamiento en memoria de cada zona con los estados de detector correspondientes para que sean interpretados por el filtro 12. Las entradas de zona también pueden provenir del bus 65, o de un módulo de interfaz inalámbrico que comprende circuitos de hardware inalámbricos 66 y el correspondiente módulo de software de interfaz inalámbrico que se ejecuta en el procesador 60. El filtro 12 se configura utilizando una interfaz de programación 18 para indicarle al filtro 12 la lista de zonas activadas y desactivadas así como también las zonas de modo de permanencia. El filtro 12 es esencialmente un módulo de software en el procesador 60.

[0029] Las zonas pueden identificarse típicamente como de alarma inmediata o con temporizador o con cuenta regresiva antes de que se dispare la alarma, como zona activada o habilitada, desactivada u omitida, en un modo de seguimiento en el que la zona es omitida como una función de detección de otra zona que por su parte está activada. El modo de seguimiento se usa para zonas adyacentes a puertas, por ejemplo. De esta forma, el gestor 16 sólo toma en cuenta aquellos eventos de intrusión que provengan de zonas activadas habilitadas en el modo seleccionado, sea de ausencia o de permanencia. Cuando se produce un evento de intrusión, el gestor 16 hace que la pantalla de estado 20 muestre este evento. El gestor de alarmas 16 es esencialmente un módulo de software que se ejecuta en el procesador 60.

[0030] La interfaz de programación 18 utiliza el teclado y la pantalla 64 para autenticar primero un usuario maestro y 17 permitir que tal usuario maestro configure el sistema que incluye la definición de los códigos de usuario válidos. La interfaz de programación es esencialmente un módulo de software que se ejecuta en el procesador 60 y que opera junto con el teclado/pantalla 64. Cuando el gestor de alarmas 16 recibe una señal de intrusión proveniente de un sensor o detector 10 a través del filtro 12, ingresa el evento en la memoria 17 (incluida en el procesador 60) que puede disponerse como una memoria intermedia de pila o circular, y da comienzo a una cuenta regresiva del temporizador antes de generar la alarma mediante la unidad 25. La salida de la sirena de alarmas se hace utilizando el circuito de controlador 25a conectado a un pin de salida del procesador 60, mientras que la alarma silenciosa se realiza mediante el circuito de discado telefónico 25b y un módulo de software de módem que se ejecuta en el procesador 60.

[0031] En algunas formas de realización, el controlador de autorización de ingreso 24 incluye el uso de un transmisor inalámbrico para autenticar un paso. El transmisor puede ser un transceptor portátil, que funciona a baterías, y que puede llevarse en un llavero u otro elemento similar. El transmisor se puede usar en reemplazo del teclado para introducir del código manualmente o como primer paso de la autenticación; es decir para habilitar una demora para la función de entrada o de salida (sin generar una alarma inmediata) sin eximir al usuario de la introducción de códigos o de algún otro tipo de autenticación. El sistema de seguridad incluye un receptor inalámbrico que detecta el código transmitido por el transmisor del usuario. Cuando se usa un transmisor para habilitar la entrada, el perímetro puede permanecer activado y generar una alarma instantánea cuando se lo traspasa. El uso de un transmisor permite que el ingreso se realice sin alarma instantánea. El hecho de exigir una autenticación adicional utilizando un código de entrada o no puede ser una opción de programación del usuario, como una función del nivel de seguridad deseado. El transceptor de usuario también puede tener un indicador del estado del sistema, como por ejemplo una luz verde constante para el estado desactivado, una luz verde intermitente para una autenticación de paso en el modo de permanencia, una luz roja intermitente para el estado de alarma, una luz roja constante para el modo totalmente activado o el modo de ausencia y una luz amarilla constante para el modo de permanencia en estado activado. En algunas formas de realización, el transmisor inalámbrico puede cumplir una función doble: activar la autenticación de paso y accionar un dispositivo para abrir una puerta o el portón de garaje.

[0032] En caso de que el sistema de seguridad esté configurado para permitir el ingreso o salida utilizando distintos recorridos por las instalaciones protegidas y el transmisor inalámbrico tenga un alcance suficiente para detectar el ingreso o la salida cuando éstas se realizan por recorridos distintos, la invención ofrece la posibilidad de determinar un recorrido para entrar o salir siguiendo las autorizaciones del transmisor inalámbrico mediante la detección de una zona que distingue recorridos dentro del sistema de seguridad. Un recorrido es un conjunto de zonas que operan con una demora de entrada o de salida que detectaría el ingreso o la salida de una persona de las instalaciones. Al determinar qué recorrido se usa para el ingreso o salida, se pueden dejar otros recorridos activados en modo instantáneo.

[0033] En algunas formas de realización, la interfaz 18 se puede usar para programar más de un modo de configuración de permanencia. Tales configuraciones se pueden organizar como una función de los distintos niveles de seguridad. La pantalla 20 puede mostrar el nivel de seguridad seleccionado. Un ejemplo de tales configuraciones diferentes es un modo de permanencia nocturna en el cual las zonas para dormir no están activadas mientras que las de uso diurno están activadas y un modo de permanencia diurno en el que todas las zonas interiores no están activadas. En general, las configuraciones del modo de permanencia están determinadas por el uso que el ocupante hace de las instalaciones, es decir, los sectores que no se usan están activados y los que se usan, desactivados, mientras que el perímetro interior-exterior 20 permanece activado. Una puerta de vidrio corrediza en una plataforma cercada puede estar desactivada en el modo de permanencia en caso de que las áreas exteriores sean consideradas parte de las instalaciones protegidas. Otras puertas y ventanas pueden estar activadas.

[0034] En caso de que la interfaz de usuario (p. ej., el teclado) 64 se encuentre en una zona interior en la que la seguridad está activada, se puede usar un teclado satélite asociado con el controlador 22 y/o el controlador 24 dentro del área sin seguridad activada para alternar entre las configuraciones del modo de permanencia antes de que un ocupante ingrese en una zona interior con seguridad activada o se puede realizar una autenticación de paso inmediatamente después de ingresar en una zona interior con seguridad activada. El controlador de activación y desactivación 22, al igual que el controlador de autorización de ingreso 24, se proporcionan usando la unidad de teclado y pantalla 64 junto con los módulos de software correspondientes que se ejecutan en el procesador 60. Los códigos de seguridad establecidos usando la interfaz 18 se almacenan en la memoria no volátil 63.

[0035] En otras formas de realización, la interfaz de programación 18 se usa para clasificar zonas como con "demora de entrada y/o de salida" o con "alarma inmediata"; en el último caso, se exigirá al usuario que suministre una autenticación de desactivación específica o bien, se disparará la alarma de inmediato sin que el usuario pueda detenerla. En este caso, la interfaz 18 comunica esta configuración al gestor de alarmas 16, preferentemente a través del filtro de modo de permanencia 12. Cuando el filtro de modo de permanencia emite una señal al gestor de alarmas 16 para indicar que en una zona activada se ha detectado una intrusión, el gestor de alarmas 16 determina si se trata de una zona de alarma "con demora" o "inmediata". Si se trata de una zona de alarma "con demora", se puede usar la autenticación de paso como en la forma de realización de las Figuras 2 o 3. Si la zona está clasificada como de alarma "inmediata", el sistema se puede configurar para que genere una alarma inmediata, específicamente, el gestor 16 emite la señal de alarma 25 de inmediato, o bien, se puede instrumentar una demora evitando que se genere la alarma ya sea mediante la desactivación del sistema o mediante una autenticación de paso especial. La autenticación de desactivación específica está preferentemente disponible para una cantidad reducida de usuarios u ocupantes; mientras que la autenticación de entrada o de salida por zonas específicamente identificadas a este fin puede estar disponible para todos los usuarios u ocupantes autorizados.

[0036] Se podrá apreciar que, en algunas formas de realización, la interfaz de programación 18 se puede usar para definir en cada configuración de modo de permanencia qué zonas pueden ser utilizadas por cuáles usuarios para entrar y salir.

[0037] Distintas listas pueden gestionar las entradas y la salidas, ya que puede darse el caso que se admita que un usuario autentique una salida por una puerta y que la misma puerta no sea segura para entrar. Por ejemplo, puede ser aceptable autenticar a un usuario desde las instalaciones para salir por una puerta que da a un callejón trasero, mientras que ningún usuario podrá ingresar por esa puerta, debido a un riesgo mayor de que algún intruso violente dicha puerta.

[0038] De igual modo, algunos usuarios pueden estar autorizados a entrar o salir por ciertas zonas, mientras que otros no. La autenticación de paso puede identificar usuarios individuales de un nivel de usuarios (grupo de usuarios) para que se pueda gestionar la entrada/salida de usuario de forma más precisa. El registro de entradas y salidas de los usuarios se puede realizarse con total eficiencia si la autenticación es exclusiva para cada usuario. En el caso de que ciertos usuarios, tales como empleados o niños, no estén autorizados para activar o desactivar el sistema, pero no obstante, puedan simplemente usar una autorización de paso, se puede dotar de mayor seguridad al sistema.

[0039] Para evitar falsas alarmas, se combina la seguridad física, como por ejemplo, cerrojos y candados con el sistema de seguridad electrónico, a fin de evitar que los ocupantes o usuarios (en especial aquellos que no están autorizados para utilizar la autenticación de desactivación específica) utilicen accidentalmente las puertas clasificadas como de "alarma inmediata".

[0040] Opcionalmente, el sistema de seguridad se puede programar con distintas clasificaciones de seguridad para las zonas con la posibilidad de seleccionar una de las configuraciones de clasificación deseada. La configuración de clasificación se puede combinar con la configuración del modo de permanencia y comunicar a un gestor de alarmas 16 a través del filtro de modo de permanencia 12. Esto también ofrece la opción de organizar las configuraciones de acuerdo con el nivel de seguridad que se puede mostrar en la pantalla 20.

[0041] En la Figura 2, se incluye un controlador de activación y desactivación 22 para autenticar a un usuario y, a continuación, activar o desactivar el sistema de seguridad enviando la señal correspondiente al gestor de alarma 16.

También se proporciona un controlador de autorización 24 para autenticar a un usuario y permitir el paso. Los códigos de usuario válidos utilizados por los dos controladores 22 y 24 pueden ser iguales o diferentes, y pueden ser específicos del usuario o no. El gestor de alarmas 16 responde a la señal de paso eliminando u omitiendo de alguna otra manera un evento de intrusión en la memoria 17. Si sólo se registró un evento, un solo paso provocará que el gestor de alarmas continúe operando en el modo de permanencia y que la pantalla 20 no indique ningún evento de intrusión. Si se registraron dos o más eventos, un único paso hará que el gestor de alarmas simplemente elimine u omita el primer evento recibido y que la pantalla muestre los eventos restantes (específicamente, las zonas en que se detectó la intrusión). El usuario tendría que usar el controlador de autorización de ingreso 24 repetidamente para generar señales de paso adicionales con el fin de eliminar todos los eventos para impedir que se dispare una alarma. Sin embargo, en las configuraciones convencionales, dos eventos generados durante una salida o entrada serían una indicación de actividad de intrusión.

[0042] En la Figura 3, el funcionamiento es similar al de la Figura 2 con la excepción de que el controlador 24 genera una señal de paso que identifica la zona en la que se autoriza y el gestor 16 elimina u omite únicamente el evento que corresponde a la zona identificada. Esto permite identificar claramente en pantalla 20 las zona exactas en las que se ha detectado un evento no autorizado una vez que el usuario haya autenticado el paso en la zona específica.

[0043] La identificación de la zona en la señal de paso puede hacerse mediante un teclado que está relacionado con la zona de entrada/salida específica. Precisamente a tal fin, se puede ubicar un teclado satélite en las inmediaciones del ingreso o salida. El teclado ubicado con este propósito se puede definir para identificar el ingreso o salida local de forma predeterminada, aunque también se pueda usar, mediante la pulsación de una tecla adicional, para autenticar una entrada o salida por otra puerta.

[0044] Como alternativa a la forma de realización de la Figura 2, la funcionalidad del controlador de modo de permanencia 24, tal como se ilustra en la Figura 4, se puede proporcionar en conjunción con el controlador 22 con fines de autenticación del usuario, y al mismo tiempo, por ejemplo, permitir que el usuario presione una tecla en un teclado para emitir una autenticación de paso en lugar de un comando de señal de desactivación o activación. Como ejemplo de ello, el usuario podría ingresar en las instalaciones protegidas y crear un evento de intrusión. En el teclado de interfaz de usuario, el usuario introduce el código normal para desactivar el sistema. No obstante, el controlador 22 envía esta señal al controlador 24 para su procesamiento. El controlador 24 hace que un indicador del teclado de interfaz comience a parpadear o se encienda de alguna otra manera para indicar que el sistema se desactivará a la brevedad, por ejemplo, en tres segundos. Si el usuario presiona una tecla del teclado, posiblemente asociada con el indicador intermitente, el controlador 24 enviará una señal de autenticación de paso 16 al gestor de alarmas. Si la tecla no se presiona en el breve período indicado, el controlador 24 emite la señal de desactivación autenticada. Para el usuario, esta forma de realización permite la utilización de un código único y la pulsación de una sola tecla para cambiar la función autenticada de desactivación total a la de paso. El hecho de usar un único código puede resultar más sencillo para el usuario, sea porque sólo tiene que memorizar un código para ingresar en el teclado o porque sólo debe contar con un dispositivo RFID.

[0045] Para autorizar un paso para salir de las instalaciones protegidas, el funcionamiento es similar. El usuario introduce el código de desactivación normal en el controlador 22. Posteriormente, el controlador 24 hace que la pantalla 20 muestre una indicación de que se ha autenticado una desactivación y que tendrá efecto a la brevedad. El usuario puede presionar una tecla dentro de un breve período para hacer que el controlador 24 envíe una autenticación de paso al gestor de alarmas 16 en lugar de una señal de desactivación. Si el ingreso del usuario no se produce durante el breve período, el controlador 24 envía una señal de desactivación.

[0046] Como alternativa a la forma de realización de la Figura 3, la tecla que se debe presionar puede indicar la zona para la cual se debe emitir una autorización de paso, y de este modo, se emitirá una autorización de paso y especificará la zona al mismo tiempo. Obviamente, es igualmente posible que se exija que para entrar se solicite una autorización de paso adicional en lugar de una desactivación del sistema y que se deba introducir algún dato adicional para solicitar que la autorización de paso se aplique a la zona especificada.

[0047] Se podrá apreciar que se pueden usar transponedores RFID, tarjetas inteligentes, llaves tipo Dallas®, tarjetas de banda magnética, interruptores de cerradura con llave, escáneres biométricos o algún dispositivo similar en reemplazo o como complemento del teclado para autenticar a los usuarios u ocupantes. En las formas de realización anteriores, la autenticación del paso se lleva a cabo mediante un controlador 24 dentro de las instalaciones protegidas. Sin embargo, se podrá apreciar que cuando se autentica a un usuario fuera de las instalaciones protegidas como parte del control de acceso, dicha autenticación se puede usar en combinación con la autenticación interna a los fines de la autenticación de paso o bien, en reemplazo de la autenticación interna de la autenticación de paso en el interior de las instalaciones seguras. Dicha configuración del sistema de seguridad se puede definir como una función de ciertas puertas y/o como una función de ciertos usuarios. Dado el caso de que se definan distintas configuraciones para el modo de permanencia, la autenticación de control de acceso se puede usar para autenticar el paso en algunas de tales configuraciones y no así en otras.

[0048] Como se ilustra en la Figura 5a, si el ocupante ingresa en las instalaciones protegidas y unos segundos más tarde ingresa un ladrón por otra entrada, los eventos se podrán registrar como se muestran. En la forma de

realización de la Figura 2, la autorización de paso no identifica el evento y, por consiguiente, se supone que éste es el primer evento que debe ser autorizado. La pantalla continuará mostrando el evento pendiente de la "puerta trasera" una vez autenticado el paso y se generará una alarma a menos que se tome alguna otra medida.

[0049] Como se ilustra en la Figura 5b, si el ocupante abandona las instalaciones protegidas y unos segundos más tarde ingresa un ladrón por otra entrada, los eventos se podrán registrar como se muestra. En la forma de realización de la Figura 3, la autorización de paso identifica el evento y los ocupantes que permanecen en las instalaciones verán en la pantalla el evento pendiente de la zona de la "puerta trasera" y se generará una alarma a menos que se tome alguna otra medida.

[0050] Como se ilustra en la Figura 5c, si un ladrón vigila cuidadosamente a un ocupante que ingresa en las instalaciones protegidas, tal vez con la ayuda de un observador provisto de un radiotransmisor, y el ladrón ingresa por otra entrada unos segundos antes que el ocupante, los hechos se podrán registrar como se muestra. En la forma de realización de la Figura 3, la autorización de paso identifica el evento y los ocupantes verán en la pantalla el hecho pendiente de la zona de la "puerta del patio" y se generará una alarma a menos que se tome otra medida.

[0051] Si bien la invención se ha descrito haciendo referencia a las entradas y salidas también se puede aplicar a la autorización para abrir una ventana o una puerta con fines de ventilación. En esta forma de realización, se ofrece un sistema de seguridad que cuenta con una zona de omisión que se reactiva automáticamente cuando se detecta que ya no se necesita la zona de omisión. Por ejemplo, la omisión de una zona que representa un sensor de ventana se puede autenticar mediante el teclado y la omisión se levanta automáticamente cuando la ventana se vuelve a cerrar. De este modo, el uso de la omisión es más seguro y más práctico dado que no es necesario utilizar el teclado para anular la omisión. La anulación de la omisión se puede producir instantáneamente o con una breve demora de usos segundos, proporcionando esta última opción una función de "anulación de rebote".

REIVINDICACIONES

1. Sistema de seguridad que comprende sensores o detectores (10),
que comprende además
un gestor de alarma (16) al que dichos sensores o detectores (10) están conectados, en los que dicho hombre gestor de alarma (16) captura un evento en una memoria (17) tras la recepción de una señal de intrusión de un sensor o detector (10), e inicia un temporizador de cuenta atrás para proporcionar un retardo entre la detección de una señal de intrusión de un sensor o detector (10) y la generación de una alarma (25), un controlador de autorización de entrada (24) adaptado para autenticar un usuario y que emite una señal de pase después de la autentificación,
siendo el sistema operable en un modo de parada en el que al menos unos sensores perimetrales o detectores (10) de las instalaciones protegidas son configurables para estar activados y unos sensores o detectores interiores (10) dentro de dichas instalaciones protegidas están desactivados, y
siendo el sistema además operable para evitar la generación de una alarma (25) en respuesta a la autenticación de dicho usuario durante dicho retardo cuando dicho usuario activa dichos sensores o detectores (10) perimetrales de las instalaciones protegidas, haciendo que el gestor de alarma (16) elimine o ignore el primer evento de intrusión en la memoria (17) con respecto a dicha señal de paso, de tal manera que sin desactivar dichos sensores o detectores perimetrales de las instalaciones protegidas, dicho controlador de autorización de entrada (24) está adaptado para restaurar dicho estado activado durante dicho retardo en respuesta a dicha autenticación de dicho usuario.

2. Sistema de seguridad tal como se define en la reivindicación 1, en el que dicho controlador de autorización de entrada (24) también está adaptado para autenticar a un usuario a punto de salir de dicho perímetro y restaurar dicho modo de parada siguiendo la detección de la abertura de dicho perímetro por dicha salida causando que una zona se abra sin generar dicha alarma (25) y sin desactivar dichos sensores perimetrales o detectores (10) de instalaciones protegidas, haciendo que el gestor de alarma (16) elimine o ignore el primer evento de intrusión en la memoria (17) en respuesta a dicha señal de pase.

3. El sistema de seguridad tal como se define en la reivindicación 2, en el que dicho modo de parada se restaura inmediatamente después de un breve retraso de rebote después de la detección de cierre de dicha zona.

4. El sistema de seguridad tal como se define en una cualquiera de las reivindicaciones 1 a 3, en el que dicho controlador de autorización de entrada (24) autentica a dicho usuario mediante la detección de un código de entrada en un teclado (64) situado dentro de dichas instalaciones protegidas.

5. El sistema de seguridad tal como se define en la reivindicación 4, en el que dicho sistema de seguridad está adaptado para usar dicho teclado (64) para activar y desactivar dicho sistema de seguridad.

6. El sistema de seguridad tal como se define en la reivindicación 5, en el que dicho sistema de seguridad está adaptado además para utilizar dicho teclado (64) para la programación de dicho sistema de seguridad.

7. El sistema de seguridad tal como se define en una cualquiera de las reivindicaciones 4 a 6, en el que dicho código se acepta para autenticar a dicho usuario y a la señal a dicho controlador de autorización de entrada (24) para evitar la generación de dicha alarma (25).

8. El sistema de seguridad tal como se define en la reivindicación 7, en el que dicho código identifica un punto de entrada a través de dicho perímetro, dicho sistema de seguridad está adaptado para generar dicha alarma (25) si se detecta también un punto de entrada diferente, haciendo que el controlador de autorización de entrada (24) genere una señal de paso que identifica la zona a través del cual se debe autoriza un pase, y haciendo que el gestor de alarma (16) retire o ignore el evento de intrusión en la memoria (17) en respuesta a dicha señal de pase correspondiente a dicha zona.

9. El sistema de seguridad tal como se define en una cualquiera de las reivindicaciones 1 a 3, que comprende además un transmisor trans inalámbrico portátil y un receptor inalámbrico, estando el receptor inalámbrico adaptado para recibir un código de dicho transmisor, reciniendo dicho controlador de autorización de entrada (24) dicho código y utilizándolo para autenticar a dicho usuario.

10. El sistema de seguridad tal como se define en la reivindicación 9, en el que dicho controlador de autorización de entrada (24) autentica por otro lado al usuario tras la entrada en dichas instalaciones mediante la detección de un código captado en un teclado situado dentro de dichas instalaciones protegidas.

11. El sistema de seguridad tal como se define en la reivindicación 9 o la 10, en el que dicha activación de dichos sensores o detectores (10) perimetrales de instalaciones protegidas hace que una zona de dicho sistema de seguridad se abra, y dicho estado activado se restaura inmediatamente después de un breve retardo de entrada después de detección de cierre de dicha zona.

12. El sistema de seguridad tal como se define en la reivindicación 1, en el que dichos sensores o detectores perimetrales (10) de instalaciones protegidas activados incluyen sensores o detectores (10) asociados con al menos una zona dentro de dicho perímetro de las instalaciones protegidas, estando dicho modo asociado con una partición de dichas instalaciones protegidas.

13. El sistema de seguridad tal como se define en la reivindicación 12, en el que se define más de una configuración de modo de parada y dicho controlador de autorización de entrada (24) está adaptado para permitir que una de dichas configuraciones de modo parada pueda ser seleccionada por el usuario.

14. El sistema de seguridad tal como se define en la reivindicación 13, en el que dichas configuraciones de modo parada representan diferentes niveles de seguridad.

15. El sistema de seguridad tal como se define en la reivindicación 14, que comprende además una representación de dicho nivel de seguridad seleccionado.

16. El sistema de seguridad como se define en cualquiera de las reivindicaciones 1 a 11, en el que dicho sistema de seguridad está adaptado para funcionar selectivamente en dicho modo de parada o en un modo de desplazamiento, funcionando dicho sistema de seguridad en dicho modo de desplazamiento tanto con dichos sensores o detectores perimetrales (10) de instalaciones protegidas y los sensores o detectores (10) interiores activados, y dicho controlador de autorización de entrada (24) está adaptado además para autenticar dicho usuario durante dicho retraso y disponer el sistema de seguridad en dicho modo de parada sin generar dicha alarma y sin desactivar dichos sensores o detectores perimetrales (10) de instalaciones protegidas.

17. El sistema de seguridad como se define en una de las reivindicaciones 1 a 11, en el que dicho controlador de autorización de entrada (24) está adaptado para definir cuáles de dichos sensores o detectores perimetrales (10) de instalaciones protegidas deben incluirse en la entrada o salida con dicho controlador de autorización de entrada (24) restaurando dicho modo de parada sin generar dicha alarma (25) y sin desactivar dichos sensores o detectores (10) perimetrales de instalaciones protegidas.

18. El sistema de seguridad tal como se define en la reivindicación 17, en el que dicho sistema está adaptado para generar una alarma inmediata (25) cuando otros de dichos sensores o detectores perimetrales (10) de instalaciones protegidas están involucrados en la entrada o la salida.

19. El sistema de seguridad tal como se define en la reivindicación 17, en el que dicho sistema está adaptado para generar una alarma (25) cuando otros de dichos sensores o detectores perimetrales (10) de instalaciones protegidas están involucrados en la entrada o salida en ausencia de autenticación de dicho usuario diferente de dicha autenticación del controlador de modo parada (24).

20. El sistema de seguridad tal como se define en una cualquiera de las reivindicaciones 1 a 11, en el que dicho controlador de modo parada (24) está adaptado para tener una configuración según la cual dicho controlador de modo parada (24) autentica a dicho usuario como una función de dos cualesquiera de entre: una zona correspondiente a dichos sensores o detectores (10) perimetrales de instalaciones protegidas; una salida, una entrada o ambas, y un usuario individual o uno de entre una pluralidad de grupos de usuarios.

21. El sistema de seguridad tal como se define en la reivindicación 20, en el que se define más de una configuración y dicho controlador de autorización de entrada (24) está adaptado para permitir que una de dichas configuraciones pueda ser seleccionada por el usuario.

22. El sistema de seguridad tal como se define en la reivindicación 21, en el que dichas configuraciones representan diferentes niveles de seguridad.

23. El sistema de seguridad tal como se define en la reivindicación 20, en el que dicho controlador de modo parada (24) está adaptado para autenticar a dicho usuario como una función de: una zona correspondiente a dichos sensores o detectores (10) perimetrales de instalaciones protegidas; una salida, una entrada o ambas; y un usuario individual o uno de una pluralidad de grupos de usuarios.

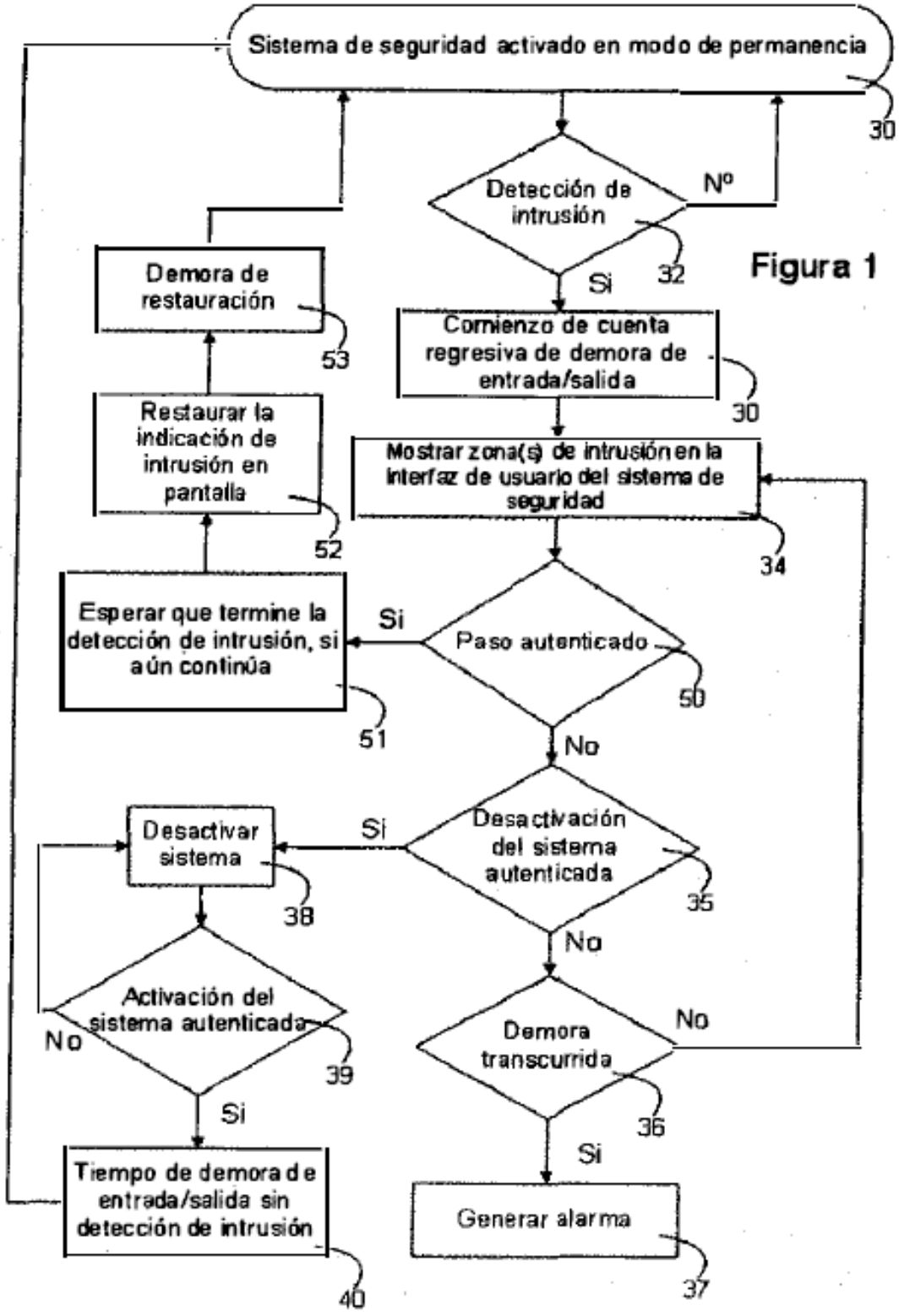
Sistema de seguridad activado en modo de permanencia
30
Detección de intrusión
Nº
Si
32
Demora de restauración
53
Comienzo de cuenta regresiva de demora de entrada/salida
30
Restaurar la indicación de intrusión en pantalla
52
Mostrar zona(s) de intrusión en la interfaz de usuario del sistema de seguridad
34
Esperar que termine la detección de intrusión, si aún continúa
51
Si
Paso autenticado
50
No
Desactivar sistema
38
Si
Desactivación del sistema autenticada
35
No
Activación del sistema autenticada
39
No
Si
Demora transcurrida
No
36
Si
Tiempo de demora de entrada/salida sin detección de intrusión
40
Generar alarma
37

Figura 1

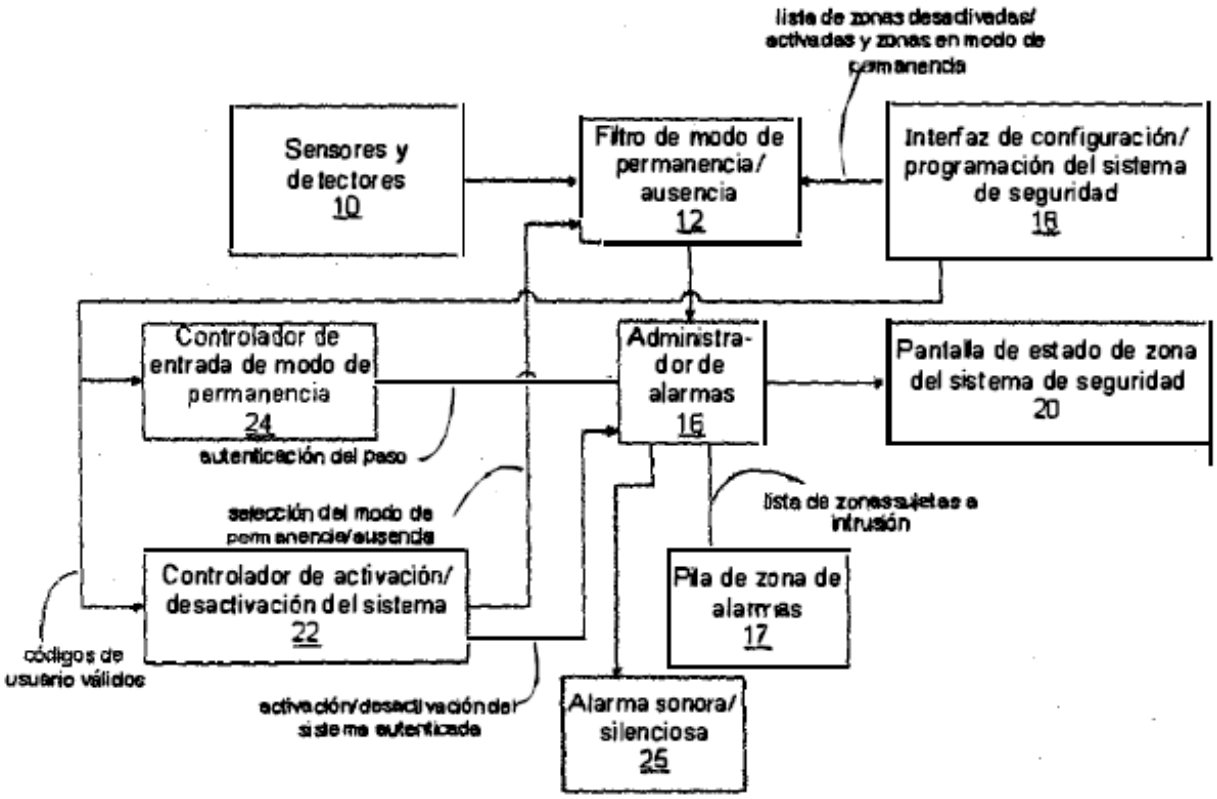
lista de zonas desactivadas/ activadas y zonas en modo de permanencia
Sensores y detectores 10
Filtro de modo de permanencia/ ausencia 12
Interfaz de configuración/ programación del sistema de seguridad 18
Controlador de entrada de modo de permanencia 24
autenticación del paso
Administrador de alarmas 16
Pantalla de estado de zona del sistema de seguridad 20
selección del modo de permanencia/ausencia
lista de zonas sujetas a intrusión
Controlador de activación/ desactivación del sistema 22
Pila de zona de alarmas 17
códigos de usuario válidos
activación/desactivación del sistema autenticada
Alarma sonora/ silenciosa 25

Figura 2

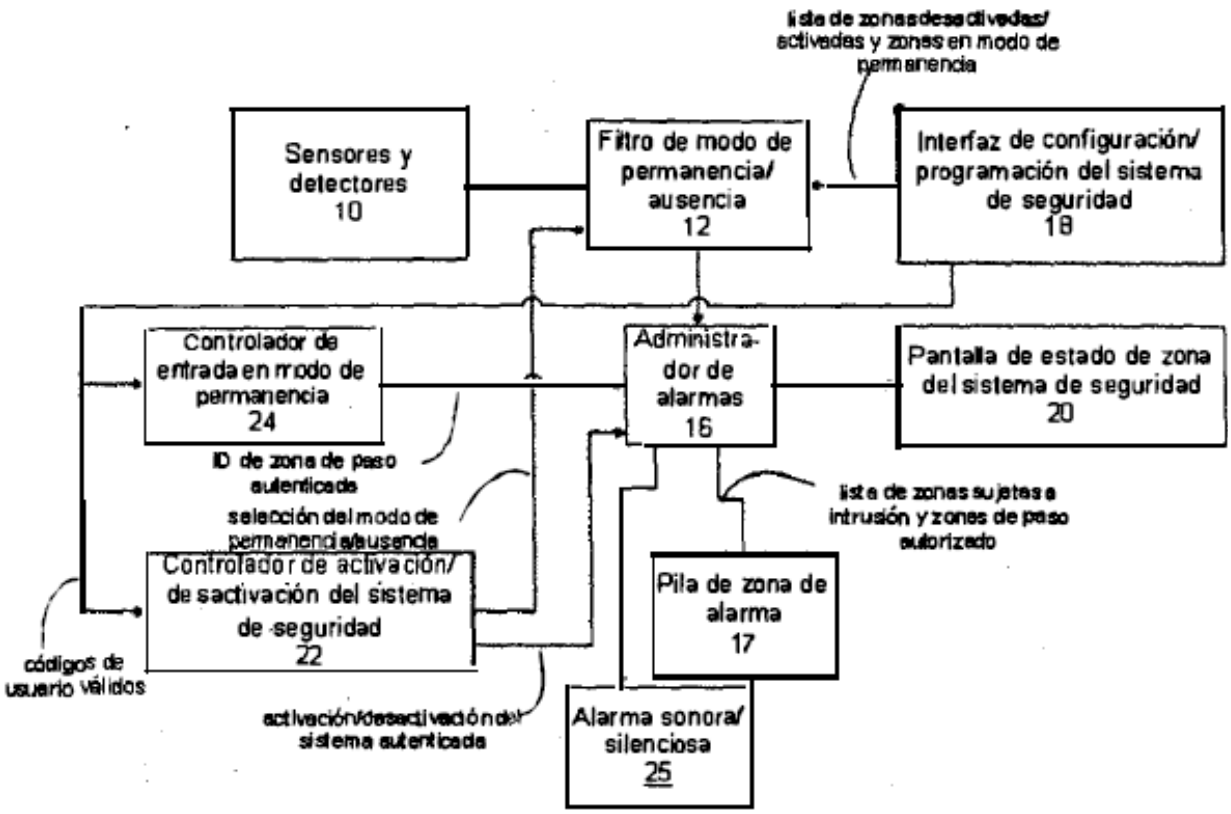
lista de zonas desactivadas/ activadas y zonas en modo de permanencia
Sensores y detectores 10
Filtro de modo de permanencia/ ausencia 12
Interfaz de configuración/ programación del sistema de seguridad 18
Controlador de entrada en modo de permanencia 24
Administrador de alarmas 16
Pantalla de estado de zona del sistema de seguridad 20
ID de zona de paso autenticada
selección del modo de permanencia/ausencia
lista de zonas sujetas a intrusión y zonas de paso autorizado
Controlador de activación/ desactivación del sistema de seguridad 22
Pila de zona de alarma 17
códigos de usuario válidos
activación/desactivación del sistema autenticada
Alarma sonora/ silenciosa 25

Figura 3

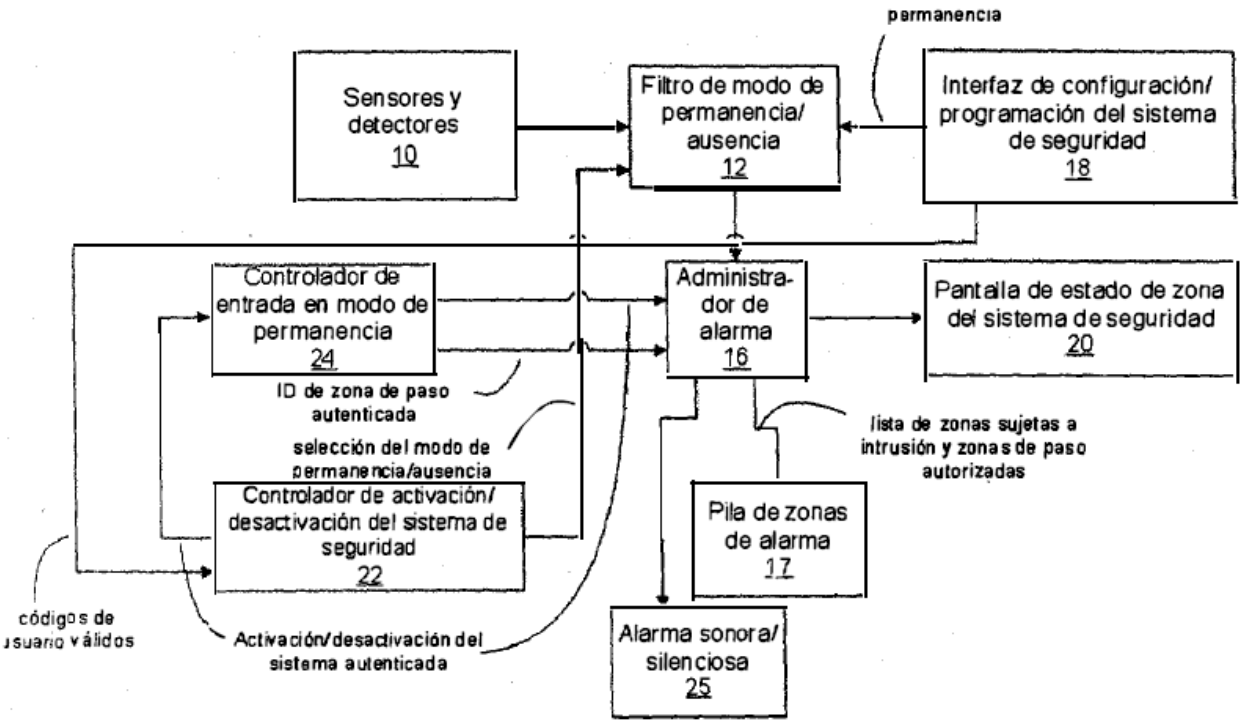
permanencia
Sensores y detectores 10
Filtro de modo de permanencia/ ausencia 12
Interfaz de configuración/ programación del sistema de seguridad 18
Controlador de entrada en modo de permanencia 24
Administra-dor de alarma 16
Pantalla de estado de zona del sistema de seguridad 20
ID de zona de paso autenticada
selección del modo de permanencia/ausencia
lista de zonas sujetas a intrusión y zonas de paso autorizadas
Controlador de activación/ desactivación del sistema de seguridad 22
Pila de zonas de alarma 17
códigos de usuario válidos
Activación/desactivación del sistema autenticada
Alarma sonora/ silenciosa 25

Figura 4

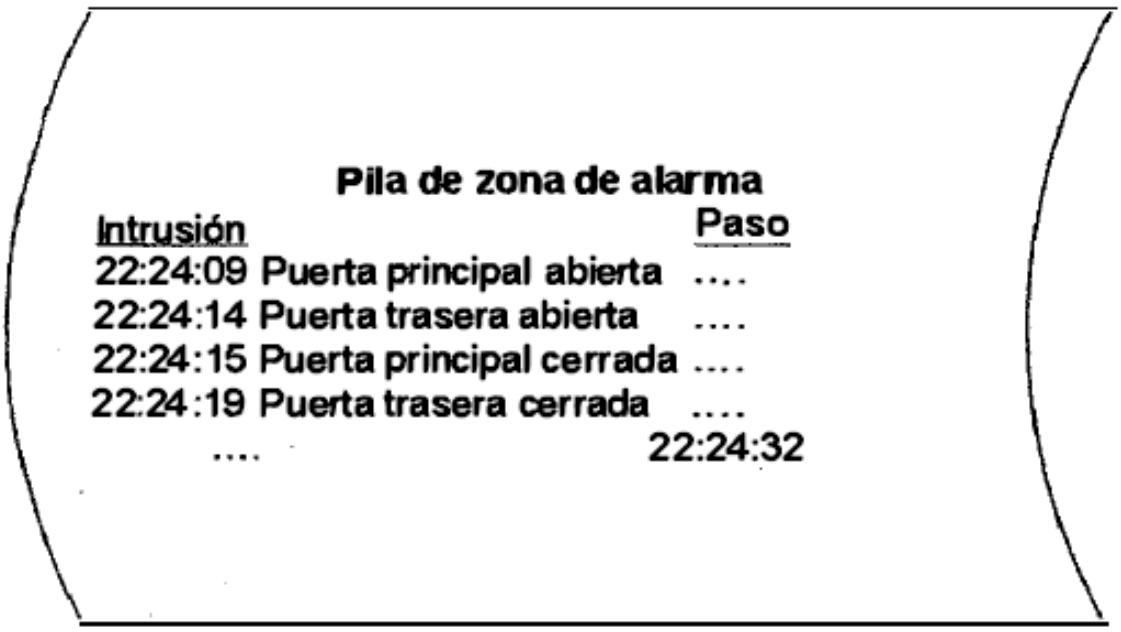

Figura 5A

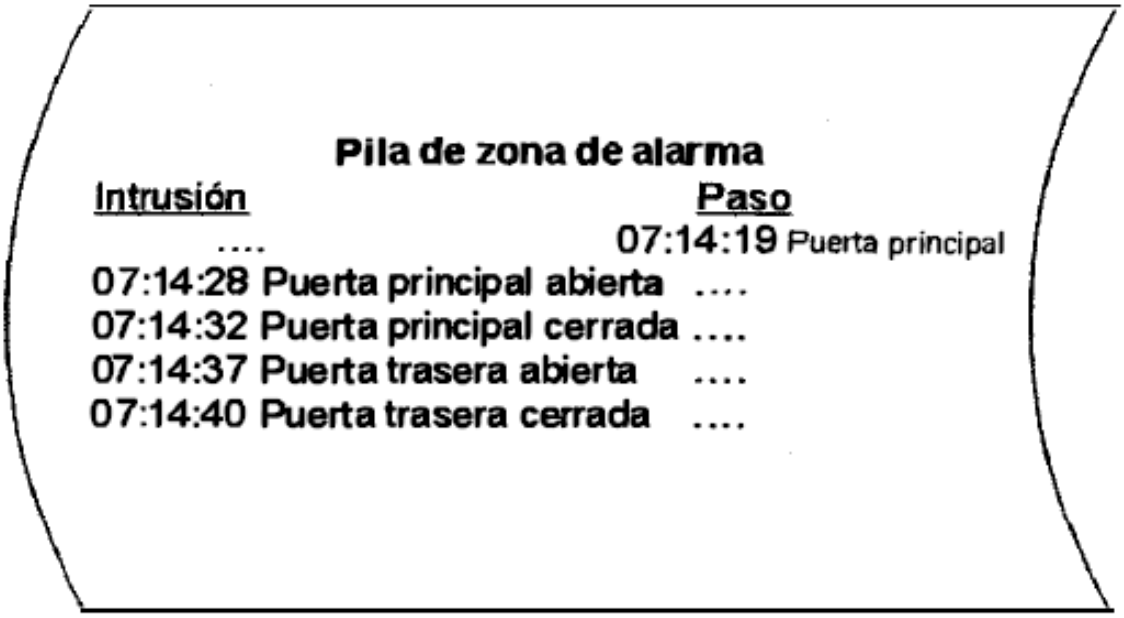

Figura 5B

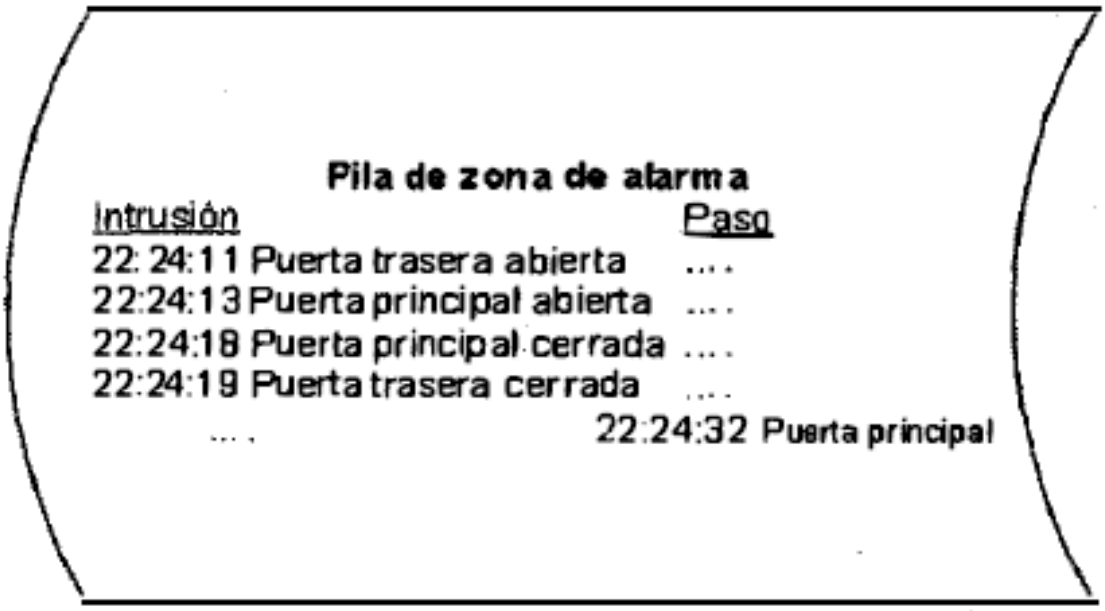
Pila de zona de alarma
Intrusión
Paso
22:24:11 Puerta trasera abierta ....
22:24:13 Puerta principal abierta ....
22:24:18 Puerta principal cerrada ....
22:24:19 Puerta trasera cerrada ....
....
22:24:32 Puerta principal

Figura 5C

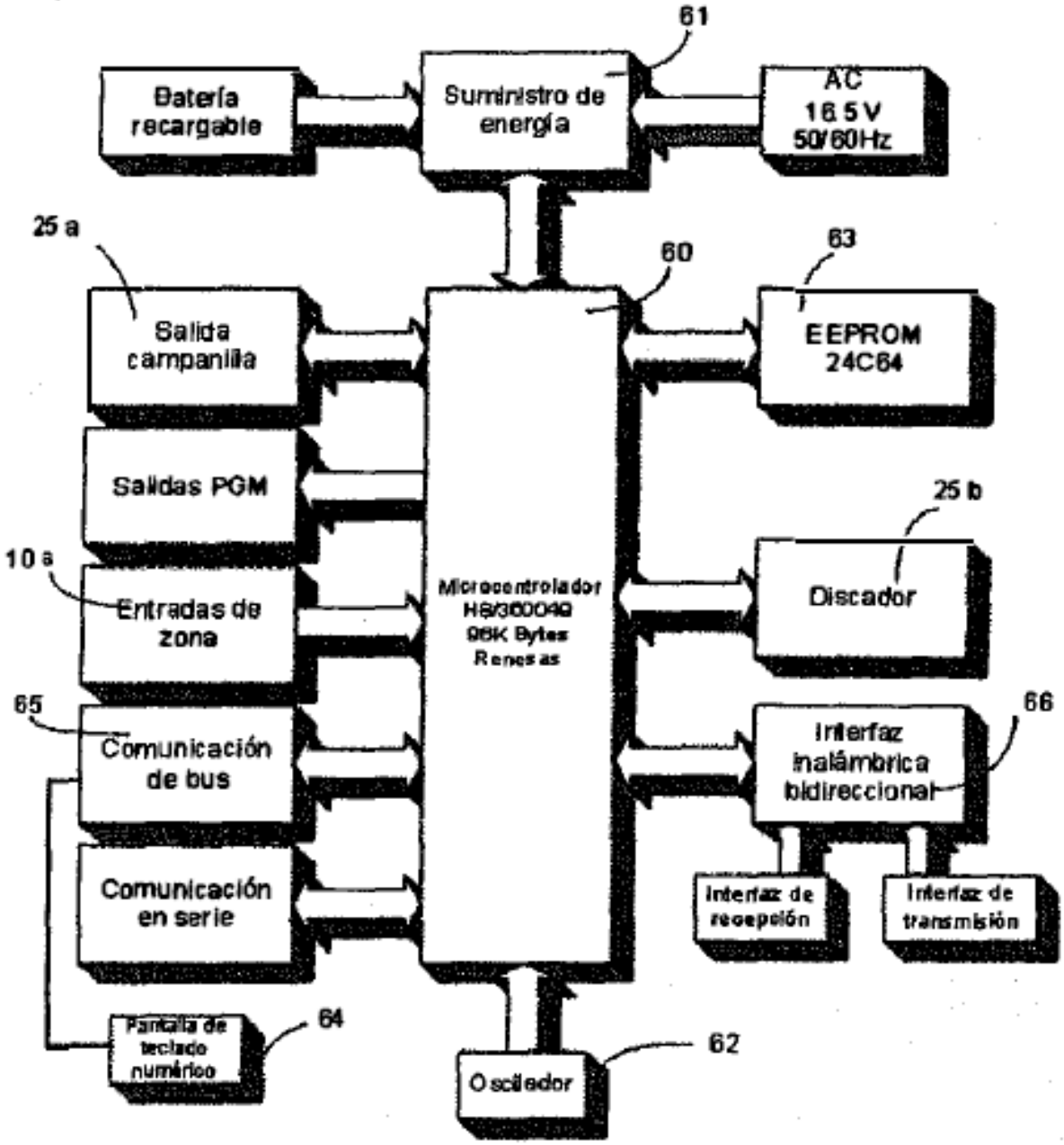
61
Batería recargable
Suministro de energía
AC 16.5 V 50/60Hz
25 a
60
63
Salida campanilla
EEPROM 24C64
Salidas PGM
25 b
10 a
Entradas de zona
Microcontrolador H8/36004Q 96K Bytes Renesas
Discador
65
66
Comunicación de bus
Interfaz inalámbrica bidireccional
Comunicación en serie
Interfaz de recepción
Interfaz de transmisión
Pantalla de teclado numérico
64
62
Oscilador

Figura 6