(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 669 353**

(51) Int. CI.:

G08B 25/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **18.04.2016 E 16165890 (1)**

(97) Fecha y número de publicación de la concesión europea: **28.03.2018 EP 3089132**

(54) Título: **Sistema y método para compartir o conectar un sistema de seguridad y de control del hogar**

(30) Prioridad:

29.04.2015 US 201514699199

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.05.2018

(73) Titular/es:

HONEYWELL INTERNATIONAL INC. (100.0%)
115 Tabor Road M/S 4D3 P.O.Box 377
Morris Plains, NJ 07950, US

(72) Inventor/es:

KHOT, BHARAT BALASO;
OH, ERIC;
CHHOKAR, AJAY PARTAP SINGH;
DURAISWAMY, KARTHIKEYAN POLLACHI;
GUDUGUNTLA, KIRAN KUMAR y
ALLURI, RAJENDRA KUMAR VENKATA

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Sistema y método para compartir o conectar un sistema de seguridad y de control del hogar

Campo de la invención

La presente solicitud se refiere a sistemas de seguridad y más en concreto al control de sistemas de seguridad.

Antecedentes

Se conocen sistemas para proteger personas y bienes dentro de áreas protegidas. Tales sistemas se basan típicamente en el uso de uno o más sensores que detectan amenazas dentro del área protegida.

Las amenazas a personas y bienes pueden originarse a partir de cualquiera de una serie de fuentes diferentes. Por ejemplo, un incendio puede matar o lesionar a ocupantes que quedaron atrapados por un incendio en una casa. Del mismo modo, el monóxido de carbono de un incendio puede matar a personas mientras duermen.

Alternativamente, un intruso no autorizado, tal como un ladrón, puede representar una amenaza a bienes que estén dentro del área. También se sabe que los intrusos hieren o matan a personas que viven en el área.

En el caso de los intrusos, pueden colocarse sensores en diferentes áreas en función de los usos respectivos de esas áreas. Por ejemplo, si hay personas presentes durante algunas partes de un día normal y no en otras ocasiones, los sensores pueden colocarse a lo largo de una periferia del espacio para proporcionar protección mientras el espacio está ocupado, mientras que se pueden colocar sensores adicionales en el interior del espacio y usarse cuando el espacio no esté ocupado.

En la mayoría de los casos, los detectores de amenazas están conectados a un panel de control local. En caso de que se detecte una amenaza a través de uno de los sensores, el panel de control puede hacer sonar una alarma sonora local. El panel de control también puede enviar una señal a una estación de vigilancia central.

Si bien los sistemas de seguridad funcionan bien, a veces son difíciles de usar. En consecuencia, existe una necesidad de mejores métodos para controlar tales sistemas.

La publicación de solicitud de patente US 2014/0266681A1 describe formas de vincular dinámicamente dos sistemas de seguridad y mostrar información de un sistema al usuario del otro.

La publicación de solicitud de patente US 2005/0353706A1 describe una interfaz entre dos sistemas de seguridad, donde la comunicación puede ser a través de un enlace RF, un enlace telefónico o una red informática.

Sumario de la invención

La presente invención se define en las reivindicaciones adjuntas.

Breve descripción de los dibujos

La figura 1 ilustra un diagrama de bloques de una red de sistemas de seguridad de acuerdo con este documento; y

La figura 2 representa un mapa tridimensional del área protegida de la figura 1.

Descripción detallada

Aunque las realizaciones descritas pueden adoptar muchas formas diferentes, en los dibujos se muestran realizaciones específicas de las mismas y en el presente documento se describirán en detalle entendiendo que la presente descripción se debe considerar como una ejemplificación de los principios de las mismas, así como el mejor modo de poner en práctica las mismas, y no pretende limitar la solicitud o las reivindicaciones a la realización específica ilustrada.

La figura 1 es un diagrama de bloques de una red 10 de sistemas de seguridad mostrada en general de acuerdo con una realización ilustrada. La red puede incluir cualquier número de sistemas de seguridad locales 12, 14, todos conectados a una estación de vigilancia central 16 a través de Internet 18.

Cada uno de los sistemas de seguridad individuales puede incluir una serie de sensores 20, 22 que detectan amenazas dentro de un área geográfica segura respectiva 24. Los sensores pueden elegirse para detectar cualquiera de una serie de amenazas. Por ejemplo, algunos de los sensores pueden ser interruptores de límite colocados en las puertas y/o ventanas situadas en una periferia de las áreas protegidas y que detectan intrusos que entran en el área protegida. Otros de los sensores pueden ser detectores de infrarrojos pasivos (PIR) situados dentro de los espacios para la detección de intrusos que han podido burlar los sensores situados a lo largo de la periferia. Otros de los sensores pueden ser detectores ambientales (por ejemplo, de humo, fuego, monóxido de carbono, etc.).

Los sensores de cada uno de los sistemas de seguridad se pueden vigilar a través de un panel de control respectivo 26 situado dentro del área (como se muestra en la figura 1) o situado a distancia. Tras la activación de uno de los sensores, el panel de control puede enviar un mensaje de alarma a la estación de vigilancia central. La estación de vigilancia central puede responder pidiendo ayuda (por ejemplo, a la policía, al departamento de bomberos, etc.).

Situados dentro de la estación de vigilancia central, el panel de control y los sensores de cada uno de los sistemas de seguridad locales pueden ser uno o más aparatos procesadores (procesadores) 28, 30 cada uno funcionando bajo el control de uno o más programas informáticos 32, 34 cargados desde un medio legible por ordenador (memoria) 36. Tal como se usa en el presente documento, la referencia a un paso realizado por un programa informático también se refiere al procesador que ejecuta ese paso.

Dentro del área protegida de cada uno de los sistemas de seguridad locales está situada una interfaz de usuario 38, 40 utilizada por un usuario humano autorizado para controlar el sistema de seguridad local. La interfaz de usuario puede incluir una pantalla 42 que muestra el estado del sistema de alarma y un dispositivo de entrada de usuario (por ejemplo, un teclado) 44 a través del cual el usuario introduce instrucciones para controlar el sistema de seguridad. Alternativamente, la pantalla y el teclado se pueden combinar en una pantalla táctil. Tal como se usa en el presente documento, una interfaz de usuario puede referirse a la pantalla y el teclado, a una pantalla táctil o a una ventana presentada en la pantalla.

En la pantalla, también se muestra uno o más iconos 46, 48 utilizados para introducir instrucciones a través de la interfaz de usuario. Por ejemplo, uno de los íconos puede ser una instrucción de armado total. Otro ícono puede ser una instrucción de armado parcial. Un tercero puede ser una instrucción de desarmado.

Por ejemplo, para armar el sistema, el usuario puede activar el icono de armado total. Para desarmar el sistema, el usuario puede introducir un número de identificación personal (PIN) seguido de la activación del comando de desarmado o simplemente puede introducir su PIN.

Una vez armado, un procesador de alarma dentro del panel de control local del sistema de seguridad puede vigilar cada uno de los sensores. Tras la activación de uno de los sensores, el procesador de alarma puede enviar el mensaje de alarma a la estación de vigilancia central. El mensaje de alarma puede incluir un identificador del sistema de seguridad (por ejemplo, un número de cuenta, un identificador del sensor y una hora).

En una realización ilustrada, un usuario humano de un primer sistema de seguridad local puede permitir que un usuario humano de un segundo sistema de seguridad controle el primer sistema de seguridad a través de la interfaz de usuario del segundo sistema de seguridad. Esto puede ser importante cuando un miembro de la familia (por ejemplo, un padre) se va de vacaciones y desea que un hijo (que vive separado del padre) pueda controlar el sistema de seguridad del padre a través del sistema de seguridad del hijo.

En la realización ilustrada, el control remoto de los sistemas de seguridad se lleva a cabo a través de un procesador de control remoto de la estación de vigilancia central basándose en la información contenida en una serie de archivos de usuario 50, 52. En este caso, un archivo (por ejemplo, el archivo 50) del padre puede incluir un identificador 54 del hijo y un archivo (por ejemplo, el archivo 52) del hijo puede incluir un identificador del padre. En este caso, los identificadores pueden incluir un identificador respectivo de los sistemas de seguridad de padres e hijos, así como los PINES del padre autorizado y del hijo autorizado.

En otra realización, el archivo del padre puede incluir una serie de identificadores de personas que el padre está dispuesto a permitir que controlen el sistema de seguridad del padre. Esto puede incluir a otros hijos, parientes o vecinos cercanos. En cada caso, el identificador de la otra persona incluiría identificadores de sistemas de seguridad correspondientes y personas autorizadas para usar esos sistemas de seguridad.

Para transferir el control del sistema de seguridad de padre, el padre puede activar un icono de transferencia de control de sistema en la interfaz de usuario del padre. Luego se le puede pedir al padre que introduzca su PIN para asegurarse de que el usuario tenga la autorización adecuada para realizar este cambio.

En este sentido, un procesador de transferencia de control dentro del panel de control del sistema de seguridad del padre puede recibir las instrucciones y comparar el PIN introducido con un PIN de referencia local previamente guardado en la memoria. Si el PIN indica un usuario autorizado, se le pedirá al padre que seleccione o de otra manera designe a una persona para que se haga cargo del sistema de seguridad del padre. Una vez seleccionada la parte designada, el procesador de transferencia de control local puede transferir la solicitud al procesador de control remoto. El procesador de transferencia local también puede enviar un mensaje de chat a la persona indicando que el control del sistema de seguridad del padre se le ha dado a la persona a través del sistema de seguridad de hogar de la persona.

Una vez recibida la solicitud, el procesador de control remoto puede realizar un conjunto similar de pasos de validación antes de implementar la transferencia de control. Al validarse la solicitud, el procesador de control remoto puede implementar una conexión de control entre los dos sistemas de seguridad (por ejemplo, el sistema de seguridad del padre y el sistema de seguridad del hijo). En este sentido, la conexión de control puede basarse en un

procesador correspondiente dentro de los sistemas de seguridad de padre e hijo que emulan las funciones de control y el comportamiento de la interfaz de usuario de padre en la interfaz de usuario de hijo.

En una realización ilustrada, la interfaz de usuario del padre puede presentarse como una zona adicional en la interfaz de usuario del hijo. En otra realización, se puede acceder a la interfaz de usuario del padre (interfaz de usuario remota) a través de la interfaz de usuario del hijo seleccionando un icono de control de acceso asociado con el identificador del padre.

En cualquier caso, la interfaz de usuario presentada a distancia del sistema de seguridad del padre se puede presentar dentro de una ventana independiente de padre 58 en la interfaz de usuario del sistema de seguridad del hijo en tiempo real. En este sentido, un procesador de vigilancia asociado con la interfaz de usuario de hijo puede vigilar funciones de control o iconos de la ventana de padre para la activación para el usuario hijo. Tras la activación de cualquier función de control, una indicación de la función activada se transfiere de vuelta a un procesador de vigilancia correspondiente del sistema de seguridad de padre para su ejecución. Del mismo modo, las actualizaciones de estado en tiempo real del sistema de padre se presentan dentro de la ventana de padre en la interfaz de usuario del hijo.

En otra realización, el padre (o un primer usuario de un primer sistema de seguridad) puede decidir otorgar el control de su sistema de seguridad a un hijo (o segundo usuario), pero solo de forma limitada. Por ejemplo, el primer usuario puede querer únicamente habilitar las funciones de armar/desarmar y notificar violaciones de seguridad al segundo usuario. En este ejemplo, el primer usuario puede no querer permitir que el segundo usuario omita cualquier alarma o deshabilite cualquier cámara que grabe continuamente imágenes desde el espacio protegido del primer usuario.

En este caso, la primera persona accedería al icono de transferencia de control en la interfaz de usuario de su sistema de seguridad y se le presentaría una lista de funciones que el primer usuario desea transferir y a las que el segundo usuario podría acceder a través de la segunda interfaz de usuario. El primer usuario puede seleccionar la función de armar y desarmar y una función de notificación. El primer usuario puede seleccionar entonces el segundo usuario y activar un botón de transferencia de control. En respuesta a esto, el procesador de control remoto puede establecer el vínculo entre los sistemas de seguridad primero y segundo y enviar un mensaje de chat al segundo usuario que incluye una lista de funciones otorgadas al segundo usuario. Los mensajes instantáneos también se utilizan para notificar a la segunda persona las situaciones de seguridad que se producen dentro del área protegida de la primera persona.

En otra realización ilustrada, la interfaz de usuario accesible a distancia puede incluir un mapa tridimensional (3D) del área protegida controlada a distancia, como se muestra en la figura 2. En este caso, el mapa 3D puede mostrarse en una interfaz de usuario del primer sistema de seguridad y, alternativamente, puede presentarse a través de una ventana 102 mostrada en la interfaz de usuario 100 del segundo sistema de seguridad. En este caso, el mapa 3D puede mostrar las ubicaciones de uno o más sensores 104. La ventana también puede incluir uno o más controles de funciones 106 tales como armar y/o desarmar.

En otra realización más, el usuario del primer sistema puede otorgar el control de un sistema de automatización del hogar situado dentro de la primera área al segundo usuario a través de la segunda interfaz de usuario. En este caso, el sistema de automatización del hogar puede mostrarse como un ícono independiente en la primera interfaz de usuario y que, alternativamente, puede presentarse y controlarse a través de la segunda interfaz de usuario.

En general, las interfaces de usuario de los sistemas de seguridad convencionales solo pueden controlar y acceder a sus sistemas. No pueden acceder a los sistemas de seguridad y automatización del hogar de terceras personas de la familia o de otras personas de confianza en otros lugares. Estas deficiencias del estado de la técnica se pueden resumir como sigue: 1) los propietarios de viviendas actualmente no tienen ningún mecanismo de intercambio para que otras personas de confianza vigilen y gestionen sistemas de seguridad y control del hogar desde cualquier parte del mundo cuando el usuario no está y no puede acceder a su sistema del hogar; 2) los propietarios de viviendas no cuentan actualmente con un mecanismo de acceso seguro que permita el acceso total o parcial a información de estado recuperada de sistemas de seguridad y control del hogar desde cualquier parte del mundo; 3) los propietarios de viviendas no tienen un mecanismo para proporcionar acceso restringido a zonas/habitaciones/áreas específicas a otras personas (por ejemplo, amigos, parientes, vecinos, visitantes, personal de servicio, etc.) durante períodos de tiempo provisionales y con código de acceso de seguridad restringido; 4) los propietarios de viviendas no tienen un mecanismo de intercambio para un sistema de seguridad y/o automatización del hogar que permita el acceso a otros usuarios para establecer y configurar zonas y dispositivos, crear o actualizar mapas de planta; y 5) los propietarios de viviendas no tienen un mecanismo de intercambio que permita el acceso total o parcial a sistemas de automatización del hogar (por ejemplo, electrodomésticos, iluminación, HVAC, puerta, puerta de garaje, llave de paso, sensores de inundación, etc.) y controles de vigilancia sanitaria cuando el usuario principal está fuera de casa y quiere que un vecino u otra persona de confianza se encargue de la casa en caso de catástrofes naturales, inundaciones, etc.

Los sistemas de las figuras 1 y 2 funcionan basándose en el concepto de redes sociales/intercambio. El sistema de vigilancia central proporciona los servicios de intercambio como parte de los servicios de notificación de alarmas

para el sistema. Esto proporciona acceso e intercambio seguros a nivel mundial que conectan múltiples sistemas entre sí para el control y la gestión de acceso a la seguridad y la automatización del hogar.

El sistema de vigilancia central también proporciona acceso total o parcial a sistemas de seguridad para la vigilancia y el control de alarmas, incendios y otras situaciones graves cuando el usuario está fuera de casa, de viaje, etc., para usuarios de confianza. Otros usuarios pueden acceder fácilmente al sistema compartido, al menos parcialmente, a través de su aplicación, sistema o software de alarma convencional para controlar la casa de un padre, etc.

El sistema de vigilancia central proporciona acceso total o parcial a sistemas de automatización del hogar (por ejemplo, electrodomésticos, iluminación, HVAC, puerta, puerta de garaje, llaves de paso, sensores de inundación, etc.) y control de vigilancia sanitaria cuando el usuario principal está fuera de casa para que los usen usuarios de confianza Otros usuarios pueden acceder fácilmente al sistema compartido a través de sus respectivas aplicaciones o sistemas para vigilar la casa de un padre, etc. El sistema proporciona acceso temporal a vecinos que pueden ayudar a cuidar personas, personal de servicio, electrodomésticos en caso de urgencias médicas, situaciones de atención médica, situaciones de cuidado de niños, entrega de envíos, desastres naturales, inundaciones, etc. Los sistemas existentes disponibles en el mercado no ofrecen ninguna funcionalidad comparable. El sistema de la figura 1 es muy útil durante inundaciones u otros desastres naturales.

El sistema de la figura 1 proporciona acceso total o parcial a través de los mapas 3D de la figura 2 a amigos, parientes, vecinos, visitantes y familiares de todo el mundo. En este sentido, el acceso se basa en el concepto de compartir redes sociales. La estación de vigilancia central proporciona servicios de intercambio, aplicación de chat y notificación como parte de un sistema de vigilancia existente. La estación de vigilancia central también proporciona información de sistemas contiguos y externos que se muestra en el mapa 3D a través de una aplicación de chat utilizada para compartir y notificar. Basado en el sistema de la figura 1, un usuario puede programar el acceso restringido a una zona/área durante un período de tiempo provisional a amigos, parientes, vecinos, visitantes, personal de servicio a través de códigos de acceso individuales usando, al menos en parte, aplicaciones existentes. Las aplicaciones existentes pueden mantener a los propietarios actualizados sobre situaciones del hogar. Después de establecerse un intercambio de acceso vigilado bidireccional, es posible acceder a los sistemas de seguridad de otras personas para su vigilancia, notificación y gestión. Una vez que el usuario accede al mapa de planta de otro usuario, como en la figura 2, puede realizar operaciones de onda Z o modificar el mapa de planta dependiendo del nivel de acceso otorgado. El sistema de la figura 1 mantiene un registro de situaciones y notifica al propietario tales situaciones.

En general, el sistema de la figura 1 funciona proporcionando una pluralidad de sistemas de seguridad, cada uno detectando amenazas dentro de un área geográfica protegida respectiva diferente y cada uno notificando amenazas detectadas a una estación de vigilancia central, enviando un usuario humano de un primer sistema de seguridad de la pluralidad de sistemas de seguridad una notificación a un usuario humano autorizado de un segundo sistema de seguridad de la pluralidad de sistemas de seguridad a través de la estación de vigilancia central, autorizando la notificación el control del primer sistema de seguridad por el usuario del segundo sistema de seguridad en respuesta a la notificación, estableciendo la estación de vigilancia central una conexión de control entre los sistemas de seguridad primero y segundo y el usuario del segundo sistema de seguridad que controla el primer sistema de seguridad a través de una interfaz de usuario del segundo sistema de seguridad.

Alternativamente, el sistema incluye una pluralidad de sistemas de seguridad, cada uno detectando amenazas dentro de un área geográfica protegida respectiva diferente y cada uno notificando amenazas detectadas a una estación de vigilancia central, una interfaz de usuario de un primer sistema de seguridad de la pluralidad de sistemas de seguridad que recibe una instrucción de un usuario humano del primer sistema de seguridad y que hace que el primer sistema de seguridad envíe una notificación a un usuario humano autorizado de un segundo sistema de seguridad de la pluralidad de sistemas de seguridad a través de la estación de vigilancia central, autorizando la notificación el control del primer sistema de seguridad por parte del usuario del segundo sistema de seguridad, un procesador de la estación de vigilancia central que establece una conexión de control entre los sistemas de seguridad primero y segundo y una interfaz de control del segundo sistema de seguridad que permite al usuario del segundo sistema de seguridad controlar el primer sistema de seguridad a través de una interfaz de usuario del segundo sistema de seguridad.

Alternativamente, el sistema incluye una estación de vigilancia central, una pluralidad de sistemas de seguridad, teniendo cada uno al menos un sensor que detecta amenazas dentro de un área geográfica protegida respectiva y notifica las amenazas detectadas a la estación de vigilancia central, un procesador de un primer sistema de seguridad de la pluralidad de sistemas de seguridad que envía una instrucción desde un usuario humano del primer sistema de seguridad a un procesador correspondiente de la estación de vigilancia central, haciendo la instrucción que el procesador correspondiente establezca una conexión de control para el control del primer sistema de seguridad por un segundo sistema de seguridad de la pluralidad de sistemas de seguridad y una interfaz del segundo sistema de seguridad que permite a un usuario humano del segundo sistema de seguridad controlar el primer sistema de seguridad a través de una interfaz de usuario del segundo sistema de seguridad.

De lo anterior, se observará que pueden realizarse numerosas variaciones y modificaciones sin apartarse del ámbito de aplicación de este documento. Debe entenderse que no se pretende o se insinúa ninguna limitación con respecto al aparato específico ilustrado en el presente documento. Por supuesto, se pretende cubrir mediante las reivindicaciones adjuntas, todas las modificaciones que estén dentro del ámbito de aplicación de las reivindicaciones. Además, los flujos lógicos representados en las figuras no requieren el orden particular mostrado, o el orden secuencial, para lograr resultados deseables. Se pueden proporcionar otros pasos, o se pueden eliminar pasos, a partir de los flujos descritos, y se pueden añadir otros componentes o eliminarlos de las realizaciones descritas.

REIVINDICACIONES

1. Método que comprende:

proporcionar unos sistemas de seguridad primero y segundo, en el que el primer sistema de seguridad (12) detecta amenazas dentro de una primera área geográfica protegida, el segundo sistema de seguridad (14) detecta amenazas dentro de una segunda área geográfica protegida (24) y ambos sistemas de seguridad primero y segundo notifican las amenazas detectadas a una estación de vigilancia central (16);

el primer sistema de seguridad envía una notificación al segundo sistema de seguridad a través de la estación de vigilancia central después de recibir y validar una identificación personal (PIN) recibida de un primer usuario y selecciona a una persona para hacerse cargo del primer sistema de seguridad, en el que la notificación proporciona el control del primer sistema de seguridad mediante el segundo sistema de seguridad, recibiendo el segundo sistema de seguridad la notificación;

en respuesta al segundo sistema de seguridad que recibe la notificación, el segundo sistema de seguridad recibe y autoriza el PIN de un segundo usuario;

en respuesta al segundo sistema de seguridad que valida el PIN recibido del segundo usuario, la estación de vigilancia central establece una conexión de control entre los sistemas de seguridad primero y segundo; y

el segundo sistema de seguridad controla el primer sistema de seguridad a través de una interfaz de usuario (38) del segundo sistema de seguridad.

2. Método según la reivindicación 1, en el que la notificación comprende un mensaje de chat.

3. Método según la reivindicación 1, que comprende además que la interfaz de usuario (38) del segundo sistema de seguridad (14) muestre el control del primer sistema de seguridad (12) como una zona añadida del segundo sistema de seguridad.

4. Método según la reivindicación 1, que comprende además que la interfaz de usuario (38) del segundo sistema de seguridad (14) muestre información de estado del primer sistema de seguridad (12).

5. Método según la reivindicación 1, que comprende además que la interfaz de usuario (38) del segundo sistema de seguridad (14) muestre una interfaz de usuario (40) del primer sistema de seguridad (12).

6. Método según la reivindicación 1, que comprende además que el primer sistema de seguridad (12) otorgue el control de solo una parte del primer sistema de seguridad al segundo usuario.

7. Método según la reivindicación 1, que comprende además que el primer sistema de seguridad (12) otorgue el control del primer sistema de seguridad al segundo usuario durante un período de tiempo limitado.

8. Método según la reivindicación 1, en el que el control del primer sistema de seguridad (12) comprende el control de un sistema de automatización del hogar dentro de la primera área geográfica protegida.

9. Método según la reivindicación 1, en el que la primera área geográfica protegida se muestra como un mapa tridimensional en la interfaz de usuario (38) del segundo sistema de seguridad (14).

10. Aparato que comprende:

unos sistemas de seguridad primero y segundo, en el que el primer sistema de seguridad (12) detecta amenazas dentro de una primera área geográfica protegida, el segundo sistema de seguridad (14) detecta amenazas dentro de una segunda área geográfica protegida (24) y ambos sistemas de seguridad primero y segundo notifican amenazas detectadas a una estación de vigilancia central (16);

una interfaz de usuario (40) del primero sistema de seguridad que recibe una instrucción de un primer usuario del primer sistema de seguridad que hace que el primer sistema de seguridad envíe una notificación al segundo sistema de seguridad a través de la estación de vigilancia central después de recibir y validar una identificación personal (PIN) del primer usuario, y selecciona una persona para hacerse cargo del primer sistema de seguridad, en el que la notificación proporciona el control del primer sistema de seguridad mediante el segundo sistema de seguridad;

una interfaz de usuario (38) del segundo sistema de seguridad que recibe la notificación y recibe y autoriza un PIN de un segundo usuario en respuesta al segundo sistema de seguridad que recibe la notificación;

un procesador (28) de la estación de vigilancia central que establece una conexión de control entre los sistemas de seguridad primero y segundo en respuesta al segundo sistema de seguridad que valida el PIN del segundo usuario; y

una interfaz de control del segundo sistema de seguridad que permite al segundo usuario del segundo sistema de seguridad controlar el primer sistema de seguridad a través de la interfaz de usuario del segundo sistema de seguridad.

11. Aparato según la reivindicación 10, en el que la notificación comprende un mensaje de chat.

12. Aparato según la reivindicación 10, que comprende además una pantalla de la interfaz de usuario (38) del segundo sistema de seguridad (14) que muestra el control del primer sistema de seguridad (12) como una zona añadida del segundo sistema de seguridad.

13. Aparato según la reivindicación 10, que comprende además un procesador del segundo sistema de seguridad (14) que muestra información de estado del primer sistema de seguridad (12) en la interfaz de usuario (38) del segundo sistema de seguridad.

14. Aparato según la reivindicación 10, que comprende además un procesador del segundo sistema de seguridad (14) que emula la interfaz de usuario del primer sistema de seguridad (12) en la interfaz de usuario (38) del segundo sistema de seguridad.

15. Aparato según la reivindicación 10, en el que la instrucción comprende una limitación de uso del primer usuario del primer sistema de seguridad (12) que otorga el control de una parte del primer sistema de seguridad al segundo usuario.

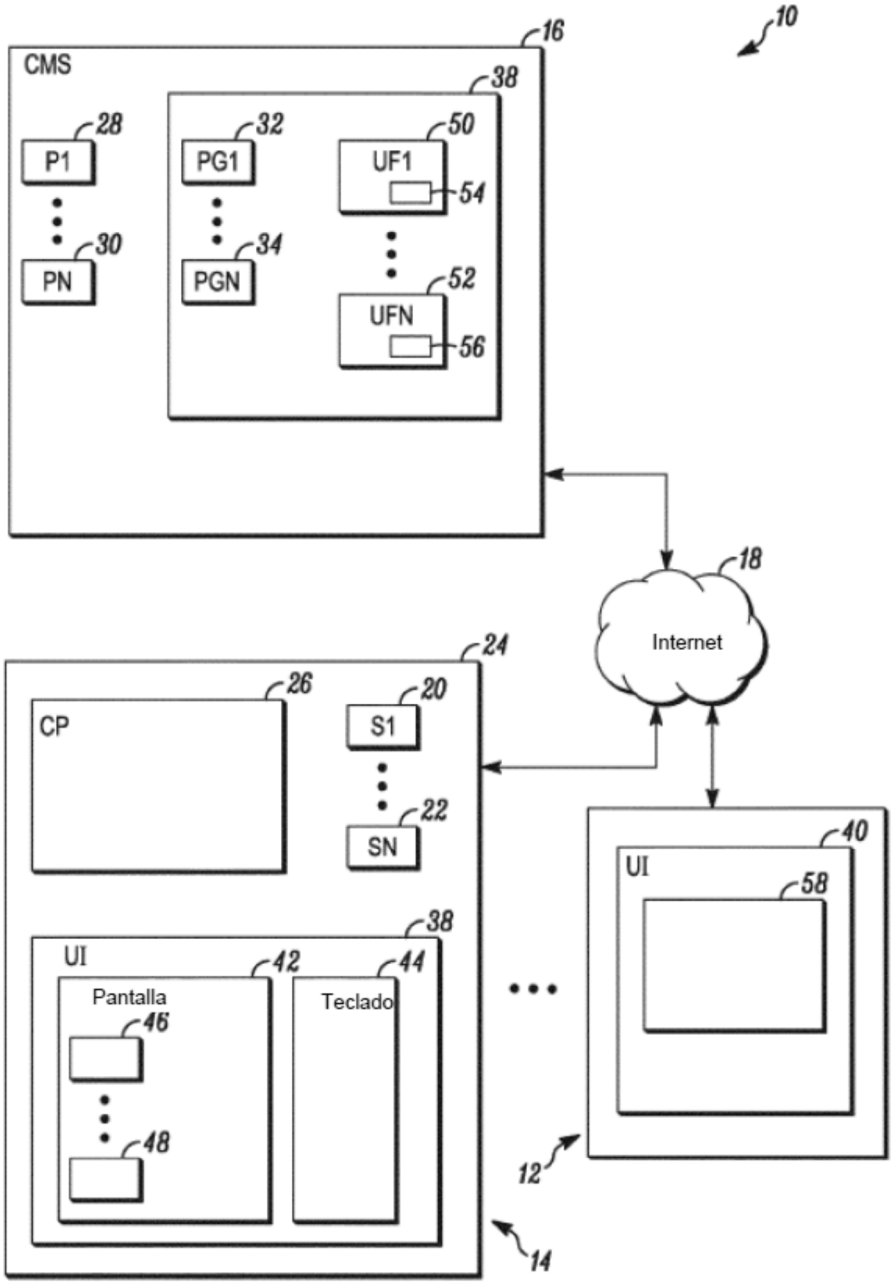
10
16
CMS
38
28
P1
30
PN
32
PG1
34
PGN
50
UF1
54
52
UFN
56
18
Internet
24
26
CP
20
S1
22
SN
40
UI
58
38
UI
42
Pantalla
46
48
44
Teclado
12
14

FIG. 1

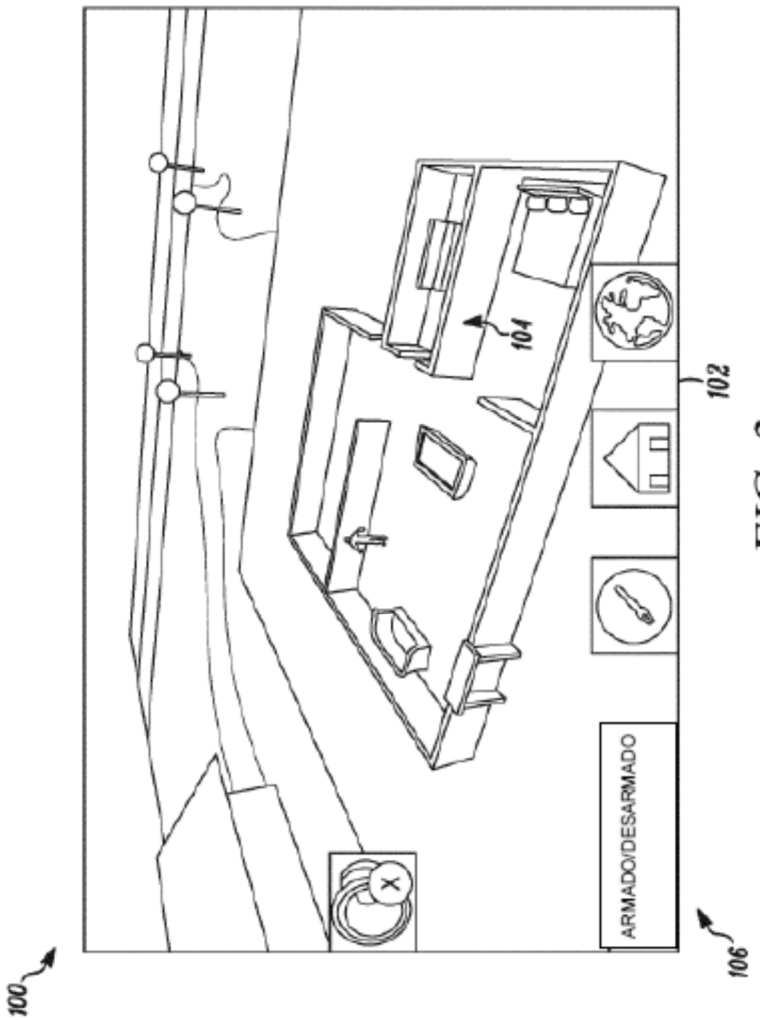

FIG. 2