(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 286 115**

(51) Int. Cl.:
G08B 21/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **01924153 .8**
(86) Fecha de presentación : **13.03.2001**
(87) Número de publicación de la solicitud: **1303843**
(87) Fecha de publicación de la solicitud: **23.04.2003**

(54) Título: **Sistema integrado de seguridad y comunicaciones, con un enlace de comunicaciones seguro.**

(30) Prioridad: **13.03.2000 US 188798 P**

(45) Fecha de publicación de la mención BOPI:
01.12.2007

(45) Fecha de la publicación del folleto de la patente:
01.12.2007

(73) Titular/es: **Honeywell International, Inc.**
101 Columbia Road
Morristown, New Jersey 07962, US

(72) Inventor/es: **Simon, Theodore;**
Winick, Steven;
Simon, Scott, H. y
Beach, Christopher, E.

(74) Agente: **Ungría López, Javier**

DESCRIPCIÓN

Sistema integrado de seguridad y comunicaciones, con un enlace de comunicaciones seguro.

Antecedentes de la invención

Esta invención se refiere a un sistema integrado de seguridad y comunicaciones. En particular, esta invención se refiere a un sistema de seguridad integrado con una conexión de Internet, en el que se puede acceder a varias características de comunicaciones y características del sistema de seguridad desde un teclado del sistema de seguridad.

Los sistemas de seguridad para propiedades residenciales son bien conocidos. En otros tiempos tales sistemas eran de tipo eléctrico o electromecánico, pero en tiempos más recientes son de tipo electrónico, estando basados en microprocesadores para controlar y realizar sus funciones. Además, aunque era común en otros tiempos que un sistema de seguridad residencial tuviese controles externos (por ejemplo, conmutadores accionados por tecla) para activar y desactivar el sistema a la salida y entrada, lo que proporcionaba un punto de ataque para intrusos potenciales, ahora es más común que un sistema basado en microprocesador proporcione retardos de entrada y salida, permitiendo que todas las interfaces de control estén dentro del perímetro protegido de los locales. Como resultado, el primer lugar al que va un ocupante que vuelva y entre en la vivienda es la interface de control más próxima del sistema de seguridad, para desarmar el sistema antes de que expire el retardo de entrada. Igualmente, el último lugar del que sale un ocupante que sale de los locales es la interface de control, para armar el sistema.

Alternativamente, o adicionalmente, el usuario puede tener un transmisor, dispuesto frecuentemente en forma de un mando a distancia a llevar en el llavero del usuario, para armar y desarmar el sistema. El transmisor puede ser un transmisor de radiofrecuencia, en cuyo caso el usuario no tendría que estar necesariamente muy cerca de cualquier posición particular en los locales, o puede ser un transmisor de infrarrojos, en cuyo caso el usuario tendría que estar muy cerca o al menos sustancialmente en la línea de visión de un receptor, que podría incluirse convenientemente como parte de la interface de control.

También es común que las viviendas estén equipadas con algún tipo de contestador telefónico, que registra un mensaje entrante del llamante, el nombre, y/o el número de teléfono, para la reproducción o revisión por el residente al volver a casa. El contestador o dispositivo de identificación de llamante también es uno de los primeros lugares a los que va un residente al volver a casa.

Muy recientemente, también es común que las personas tengan cuentas de correo electrónico para recibir mensajes por Internet u otras redes públicas de datos. Así, un tercer lugar al que vuelve un residente es un ordenador, para recoger el correo electrónico.

Los sistemas de seguridad del tipo explicado comunican casi universalmente con una “estación central” que supervisa o vigila el estado de cada sistema de seguridad. No solamente hay alarmas en comunicación con la estación central, que entonces actúa en ellas o avisa a los vigilantes para que actúen en ellas, sino que incluso la ausencia de comunicación puede ser considerada como un signo de posibles problemas en los locales protegidos. Además, se puede detectar una condición de mantenimiento (tal como una batería de reserva baja) y se puede enviar al servicio técnico o se puede avisar al propietario de los locales para que corrija la situación.

WO 99/46923 (D1) describe un sistema telefónico inalámbrico convencional que realiza funciones de seguridad. La disposición incluye un sensor, un dispositivo de salida de alarma, un controlador de sistema y una interface de usuario en forma de un teléfono inalámbrico estándar. WO 99/65192 (D2) utiliza Internet (o una red similar) para acceso remoto a sensores y electrodomésticos situados dentro de la casa. US 5 440 625 (D3) describe un sistema de comunicación por teléfono que tiene un servicio específico de un usuario particular en base a información presente en un dispositivo de memoria portátil.

Las comunicaciones entre el sistema de seguridad local y la estación central remota se han llevado a cabo tradicionalmente por línea terrestre o teléfono celular o por radio. Frecuentemente se utiliza más de un medio, para redundancia. Crecientemente, muchos de los locales protegidos, incluyendo tanto viviendas como negocios, tienen conexiones a alta velocidad con Internet. La utilización de tales conexiones para comunicar con la estación central sería más rápida que los otros métodos descritos anteriormente. Sin embargo, hay varios problemas asociados con la utilización de Internet para comunicaciones con la estación central.

En primer lugar, la naturaleza inherente de Internet origina el riesgo de intercepción o escucha de mensajes enviados en Internet. Esto significa que se precisa un método de encriptado seguro.

En segundo lugar, la mayor parte de las conexiones a Internet no tienen direcciones de Protocolo de Internet (“IP”) fijas, lo que significa que la estación central puede no estar segura, observando simplemente la dirección de origen, de que un mensaje viene de una posición particular. Por lo tanto, dado que la estación central debe aceptar mensajes de cualquier dirección IP, y usar otros datos en el mensaje para identificar el emisor, la estación central necesita alguna otra forma de autenticar que el emisor es quien parece ser.

En tercer lugar, en la mayoría de los casos donde los locales son servidos por una conexión de Internet, esa conexión está protegida por un "cortafuegos" para evitar el acceso no autorizado a ordenadores situados en los locales, por ejemplo, por "piratas". Esto hace difícil, si no imposible, que una estación central interrogue al sistema de seguridad en los locales mediante Internet, porque el cortafuegos evita el acceso a Internet desde el exterior.

En cuarto lugar, Internet todavía no ha alcanzado un estado suficientemente maduro en cuya disponibilidad se pueda confiar en todo momento. El servicio a una posición particular puede "caerse" en tiempos impredecibles.

No obstante, si se hallase una forma de usar Internet para la comunicación segura entre un sistema de seguridad de locales y una estación central, y el sistema funcionase, es decir, la conexión "no se cayese", es claro que Internet sería el canal de comunicaciones más rápido, en comparación con una línea terrestre o teléfono celular, o radio.

Tal sistema tendría múltiples canales disponibles para enviar mensajes a la estación central. Habría que utilizar los varios canales de la manera más eficiente, evitando la redundancia innecesaria, pero evitando también el retardo innecesario en la comunicación con la estación central.

Sería deseable poder minimizar el número de dispositivos electrónicos a los que una persona debe atender al volver o salir de los locales.

También sería deseable poder mejorar la seguridad de comunicaciones entre los locales y una red de datos externa.

Resumen de la invención

Un objeto de esta invención es minimizar el número de dispositivos electrónicos a los que una persona debe atender al volver o salir de casa.

También es un objeto de esta invención mejorar la seguridad de comunicaciones entre la casa y una red de datos externa.

Según esta invención, se facilita un sistema integrado de seguridad y comunicaciones según la reivindicación 1.

En una realización de la invención, la unidad de comunicaciones es una puerta de enlace de Internet. En una realización especialmente preferida, la puerta de enlace de Internet puede comunicar con Internet con seguridad desde detrás de un cortafuegos usando encriptado de clave pública compartida, creando una red privada virtual.

Breve descripción de los dibujos

Los anteriores y otros objetos y ventajas de la invención serán evidentes después de la consideración de la descripción detallada siguiente, tomada en unión con los dibujos acompañantes, en los que caracteres de referencia análogos se refieren a partes análogas en todos ellos, y en los que:

La figura 1 es un diagrama esquemático simplificado de una realización preferida de un sistema de seguridad según la presente invención.

La figura 2 es un diagrama esquemático simplificado de una segunda realización preferida de un sistema de seguridad según la presente invención.

La figura 3 es una vista en alzado de una primera realización de un teclado para uso en un sistema según la invención.

La figura 4 es una vista en alzado de una segunda realización de un teclado para uso en un sistema según la invención.

La figura 5 es un diagrama esquemático simplificado de la circuitería del teclado de la figura 4.

La figura 6 es una vista en alzado de una tercera realización de un teclado para uso en un sistema según la invención.

La figura 7 es un diagrama esquemático simplificado de una realización preferida de una unidad de interface telefónica según la invención.

Y la figura 8 es un diagrama esquemático simplificado de una realización preferida de un sistema de comunicaciones según la invención.

Descripción detallada de la invención

La presente invención reconoce que el primer lugar al que debe ir un usuario al entrar en una vivienda u otros locales protegidos por un sistema de seguridad es el teclado del sistema de seguridad, para desarmar el sistema (o ponerlo en un estado "armado en casa") antes de que termine el retardo de período de entrada. La invención también

reconoce que el último lugar al que va un usuario antes de salir de los locales es el teclado del sistema de seguridad, para armar el sistema antes de salir. Según la invención, funciones de comunicación, tales como Internet u otras funciones de redes públicas de datos, tal como correo electrónico, están a disposición del usuario en el teclado del sistema de seguridad. Dependiendo del número de funciones realizadas, y el nivel de funcionalidad proporcionado para cada función, puede ser posible usar un teclado convencional, o puede ser necesario un teclado mejorado, como se describe con más detalle a continuación.

Para que las funciones de comunicaciones estén disponibles en el teclado, el sistema de seguridad tiene que estar integrado al menos en cierto grado con el sistema de comunicaciones o sistemas implicado. Aunque los sistemas de seguridad están conectados de ordinario a una línea de teléfono, por ejemplo, para supervisión por la estación central, o a un dispositivo de comunicaciones por radiofrecuencia o celular, la presente invención prevé una mayor integración de la proporcionada normalmente.

El teclado de seguridad tiene preferiblemente al menos once teclas, para los dígitos 0-9 más una tecla de función tal como "#", y preferiblemente una duodécima tecla tal como "*", para imitar a un teclado de teléfono DTMF estándar. Además, el teclado tiene preferiblemente un altavoz para reproducir los mensajes grabados por el sistema. Los teclados más convencionales ya tienen un altavoz, por ejemplo, para emitir un aviso de "prealarma" durante el período de retardo de entrada (como recordatorio de que el sistema debe ser desarmado). También sería deseable que el teclado tuviese un indicador visual que podría ser usado para indicar la presencia de mensajes. Sin embargo, esto no es esencial, puesto que el sistema podría estar configurado para anunciar de forma audible, al desarme del sistema, si hay mensajes, y si los hay, cuántos.

El sistema de seguridad según la presente invención está conectado a una red de datos externa, de la que un ejemplo es Internet, para enviar o recibir correo electrónico y/o datos de Internet tal como páginas de la web mundial. Preferiblemente, si el sistema está conectado a una red de datos externa tal como Internet, la conexión es del tipo que siempre está conectado y activo. La red de datos externa puede ser usada como un canal de reserva para comunicación con la estación central que supervisa el sistema de seguridad, con una conexión telefónica de marcación tradicional o celular o canal de comunicación por radiofrecuencia como el canal primario, pero la red de datos externa también podría ser usada como el canal primario de supervisión de la estación central, usando los métodos de comunicaciones tradicionales como reserva. De cualquier forma, preferiblemente los varios canales se usan redundantemente para tener seguridad de que el mensaje llegue a la estación central. Más preferiblemente, una vez que tiene éxito la transmisión en un canal, se terminan los intentos incompletos de usar otros canales, como se describe con más detalle más adelante.

Según otro aspecto de la presente invención, una conexión de Internet entre los locales y la estación central puede ser usada para comunicaciones fiables seguras. Los problemas de seguridad y autenticación se resuelven usando encriptado de clave pública compartida. Cada sistema de los locales está provisto de una clave privada única. Por ejemplo, en una realización preferida, la clave privada se incorpora en el controlador de sistema al tiempo de la fabricación. La misma clave privada es compartida con la estación central. La estación central guarda así muchas claves privadas, una para cada una de las unidades que supervisa. Si la estación central comunica con una unidad particular, si es capaz de desencriptar la comunicación con dicha unidad usando la clave privada que la asocia con dicha unidad, que nadie en el mundo se supone que conoce, entonces la estación central conoce dos cosas. Primero: la estación central sabe que la unidad es la unidad que la estación central piensa que es, porque si fuese una unidad diferente, la clave privada no funcionaría para desencriptar la comunicación. Segundo: en virtud del encriptado de la misma clave privada, la estación central sabe que la comunicación es segura.

El problema restante del cortafuegos de los locales se resuelve haciendo que la unidad del local inicie periódicamente el contacto con la estación central. La mayoría de los cortafuegos no evitan las sesiones que se inician dentro del cortafuegos. Una vez abierta una sesión, la estación central puede enviar mensajes u otros datos a la unidad del local. Si la estación central no recibe respuesta de la unidad del local a los intervalos previstos, supone un problema y envía alguien a los locales. De otro modo, los intervalos de contacto se establecen de manera que sean suficientemente cortos para que no sea probable que la estación central acumule demasiados mensajes no enviados de los locales. El intervalo de contacto también puede depender del tipo de locales. Por ejemplo, un banco o joyería pueden tener contacto más frecuente con la estación central que una vivienda.

Aunque el sistema es útil para permitir comunicaciones a través de cortafuegos, puede ser usado donde una o ambas partes comunicantes carecen de un cortafuegos. Las ventajas de dicho sistema incluyen obviar la necesidad de preparación por parte del usuario, así como la necesidad de un centro de datos externo para conocer la dirección IP de un dispositivo con que tiene que comunicar.

Aunque en el sistema recién descrito, la instalación en contacto seguro con los locales se ha descrito como una "estación central", no tiene que ser la misma "estación central" que supervisa y responde a condiciones de alarma. En cambio, es posible distinguir entre una estación central de supervisión, que realiza las funciones tradicionales de supervisión de alarmas, y una estación central de comunicaciones, que simplemente garantiza la seguridad del enlace de comunicaciones. Aunque en algunos casos ambas funciones pueden ser realizadas de hecho por una sola entidad, cae dentro de la presente invención que las funciones sean realizadas por facilidades separadas que incluso pueden ser propiedad de entidades separadas. Así, mientras que las compañías de alarma tradicionales continuarán operando estaciones centrales de supervisión, pueden contratar con proveedores de comunicaciones seguras para operar estaciones

centrales de comunicaciones para proporcionar conexiones de Internet seguras a sus abonados y después reenviarles las comunicaciones.

De hecho, el reenvío puede tener lugar por una conexión de Internet entre la estación central de supervisión y la estación central de comunicaciones que sea segura de la misma forma que la conexión entre los locales del abonado y la estación central de supervisión. Específicamente, la estación central de supervisión, segura detrás de su cortafuegos, iniciará todas las sesiones con la estación central de comunicaciones usando un encriptado de clave pública compartida.

Si, en tal realización, la estación central de supervisión desea contactar con una unidad del local del abonado, la estación central de supervisión inicia una sesión con la estación central de comunicaciones y transmite el mensaje a la estación central de comunicaciones. La estación central de comunicaciones pone en cola el mensaje para la unidad apropiada del local, y cuando dicha unidad del local entra posteriormente, la estación central de comunicaciones pide a la unidad del local que mantenga el canal abierto para recibir el mensaje de la estación central de supervisión. La estación central de comunicaciones envía entonces el mensaje a la unidad del local, y recibe una respuesta, si es apropiado. Si se recibe una respuesta, se pone en cola hasta la vez siguiente que entre la estación central de supervisión, tiempo en el que se transmite a la estación central de supervisión.

Igualmente, si la unidad del local tiene un mensaje para la estación central de supervisión, inicia una sesión con la estación central de comunicaciones y transmite el mensaje a la estación central de comunicaciones. La estación central de comunicaciones pone en cola el mensaje hasta que la estación central de supervisión entra posteriormente, cuando la estación central de comunicaciones pide a la estación central de supervisión que mantenga el canal abierto para recibir el mensaje de la unidad del local. La estación central de comunicaciones envía entonces el mensaje a la estación central de supervisión, y recibe una respuesta, si es apropiado. Si se recibe una respuesta, se pone en cola hasta la vez siguiente que entre la unidad del local, tiempo en el que se transmite a la unidad del local.

Establecido dicho sistema de comunicaciones seguras, no hay ninguna razón de seguridad por la que no depender de Internet como el canal primario de referencia de alarmas, en la medida en que es claramente el más rápido cuando está disponible. Si no está disponible, se puede usar uno o más de los otros canales de comunicaciones. Tradicionalmente, si falla un canal de comunicaciones primario, el sistema "cae" a un canal secundario. Según otro aspecto de la presente invención, el sistema no espera un fallo del canal primario antes de iniciar el contacto en un canal secundario.

Una forma de operar tal esquema de "señalización dinámica" según la invención sería hacer que ambos canales (o todos si se usan más de dos canales, por ejemplo, Internet, teléfono de línea terrestre, teléfono celular, comunicaciones celulares de canal de control tal como el conocido como MicroBurst® y que se puede obtener de Aeris Communications, Inc., de San Jose California, y/o radio) inicien comunicaciones al mismo tiempo, emitiendo instrucciones el primer método en tener éxito, después de tener éxito, para que los otros métodos pongan fin a sus intentos de comunicación. Este esquema tiene la ventaja de que la referencia de una condición de alarma (o cualquier otra condición) no tiene que esperar hasta que el canal primario falle antes de que se intente un canal secundario.

Por otra parte, el canal primario opera frecuentemente. Por lo tanto, el esquema de señalización dinámica recién descrito podría ser considerado ineficiente porque siempre inicia el (los) canal(es) de reserva incluso cuando no se necesita reserva. Por lo tanto, en un refinamiento del esquema de señalización dinámica, el canal primario recibe una "ventaja" antes de que se activen el canal o canales secundarios. Por ejemplo, si el canal primario es Internet, una sesión de informe exitosa tendría lugar normalmente en unos pocos segundos. Por lo tanto, los otros canales conectan automáticamente después de, por ejemplo, cinco segundos, a no ser que se reciba una señal de terminación del canal primario. Si el canal primario tiene éxito dentro de cinco segundos, no hay necesidad de activar los otros canales. Si el canal primario no tiene éxito en cinco segundos, todavía puede tener éxito, pero los otros canales se activarán, poniendo fin a los otros canales el primer canal que tenga éxito después de ese tiempo.

Se puede usar varias combinaciones de canales. Por ejemplo, el sistema podría depender de comunicaciones celulares de canal de control o Internet como el canal primario, con marcación de línea terrestre como el canal de reserva. O Internet podría ser el canal primario, siendo las comunicaciones celulares de canal de control el canal de reserva. Se podría usar cualquier otra combinación de los varios medios de comunicaciones.

Una vez que la red de datos externa está presente, son posibles otros usos además de la referencia del sistema de seguridad. Así, se podría utilizar un teclado del sistema del local adecuadamente equipado como un terminal para acceder a la red de datos externa. Según la invención, cuando un usuario desarma el sistema de seguridad en un teclado de sistema, por ejemplo, al volver a casa, los mensajes de correo electrónico entrantes son visualizados en el teclado. Para esta finalidad, el teclado de sistema tiene preferiblemente una pantalla de visualización alfanumérica, o una matriz activa, LCD u otra pantalla de panel plano, para visualizar los mensajes de correo electrónico, aunque se podría usar tecnología de síntesis de voz para presentar los mensajes de forma audible usando un altavoz en el teclado. También preferiblemente, el teclado tiene un indicador visual para indicar la presencia de mensajes a visualizar. Se podría prever una indicación audible, tal como una configuración particular de tonos o un aviso grabado o en voz sintetizada, de la presencia de mensajes al tiempo de desarme el sistema, en lugar de, o además de, una indicación visual.

Si el sistema facilita el correo electrónico, según la invención hay una dirección de correo electrónico particular asociada con el sistema, y se visualizaría dicho correo. En una realización más especialmente preferida, una dirección de correo electrónico separada para cada usuario autorizado del sistema está asociada con el sistema, y los mensajes

de correo electrónico apropiados del usuario son visualizados en base al código de paso, tarjeta de paso, transmisor codificado u otra ficha usada para desarmar el sistema. Así, el anuncio y/o la visualización de mensajes de correo electrónico mediante el teclado es personalizado para el usuario que está cerca de, o accediendo a, el teclado. Tal personalización mejora de forma significativa la usabilidad y "facilidad de uso" del sistema.

En otra realización de la invención, en lugar de, o además de, los mensajes de correo electrónico, el sistema visualiza páginas de la web mundial o datos similares de la red de datos externa. Los datos visualizados son preseleccionados por el usuario o usuarios. Así, se podría acceder a los mismos datos independientemente de quien acceda al sistema, o los datos podrían ser personalizados para usuarios individuales. Por ejemplo, en un sistema residencial, si un adulto desarma el sistema, se podría visualizar un informe bursátil, mientras que para un adolescente se podría visualizar un anuncio de un minorista favorito. Igualmente, al armar el sistema, lo que de ordinario significa que el usuario va a salir del local, se podría visualizar un informe de tráfico o del tiempo, u otros datos preseleccionados por el usuario. Si un usuario tiene más de un código de paso, o un transmisor con más de una tecla para armar o desarmar el sistema, una selección de datos diferente podría estar asociada con cada código de paso o tecla.

El sistema está configurado preferiblemente para permitir la recuperación de mensajes de correo electrónico de uno o varios teclados de sistema en todo el local, por separado de una operación de desarme. Esto se podría implementar en una realización previendo una tecla especial de recogida de correo electrónico, que entonces pediría al usuario un código de paso para identificar cuál de los usuarios autorizados potenciales está pidiendo la recogida de correo electrónico, o en una segunda realización se podría usar una secuencia de órdenes especiales en un teclado estándar para la misma función. En otra realización, los varios teclados de sistema presentes en el sistema podrían estar configurados en una red de área local, permitiendo a los usuarios en diferentes teclados que recojan independiente y simultáneamente el correo electrónico. En tal realización, las funciones del sistema de seguridad operan como en la realización no en red.

En otra realización, el teclado de sistema está provisto de un teclado completo y se puede utilizar como un terminal para entrar en Internet u otra red de datos externa para cualquier finalidad, incluyendo crear y enviar correo electrónico, buscar información en la web mundial, etc. En una variación de esta realización, el teclado está provisto de un micrófono para operaciones sonoras completas, y opcionalmente con altavoces estéreo en lugar de un solo altavoz monaural. En otra variación, el teclado también está provisto de una pantalla, tal como una pantalla de cristal líquido o plasma de gas o una pequeña pantalla de tubo de rayos catódicos, para presentar gráficos así como texto, y opcionalmente con una videocámara para operaciones vídeo plenas.

La unidad del local podría realizar todas estas funciones por sí misma, usando su conexión directa con la red de datos externa (por ejemplo, Internet). Sin embargo, por razones de seguridad, puede ser deseable evitar el contacto general entre la unidad del local y otros usuarios de Internet. Por lo tanto, en un sistema donde la unidad del local comunica con una estación central de comunicaciones como se ha descrito anteriormente (tanto si la estación central de comunicaciones también es la estación central de supervisión como si no), la estación central de comunicaciones podría mantener, por abono de usuario, registros de las direcciones de correo electrónico del usuario y las preferencias de contenidos (es decir, qué noticias, informe meteorológico, publicidad, etc., el usuario desea recibir, y cuándo), recuperar los datos de Internet (por ejemplo, usando "agentes" apropiados) y enviarlos a la unidad del local en base a códigos de paso recibidos. Si se dispone de uso interactivo directo de Internet en el sistema (lo que puede depender, primariamente, de qué bueno sea el teclado de la interface de usuario), la estación central de comunicaciones actuaría como un proxy para que el sistema de local acceda a Internet, manteniendo el enlace seguro con el local.

Según otra característica de la invención, un código de paso del usuario desbloquea otras contraseñas que el usuario puede tener con otras instituciones, tal como bancos u otras instituciones financieras. En una realización, las contraseñas se guardan en el controlador del local. En base a la entrada de un código de paso del usuario para acceder al sistema, si el usuario inicia entonces una sesión con una de las instituciones, la contraseña apropiada es transmitida, cuando sea necesario, a la institución sin ninguna otra acción por el usuario. Preferiblemente, el usuario también podría acceder al sistema usando un transmisor u otra ficha codificada y el sistema enviaría el código de paso correspondiente al autenticar la transacción financiera.

En otra realización, el código de paso del sistema de seguridad del usuario está registrado en las instituciones como un identificador fijo del usuario. Cuando el usuario accede al sistema del local con su código de paso o ficha codificada y entonces usa la red de datos externa para entrar en la institución financiera, el código de paso es enviado a la institución y es reconocido como una autorización segura. Aunque esta función tendría que ser por acuerdo y negociación anterior con la institución financiera, es potencialmente más segura, o al menos de menor riesgo, que enviar un personal número de identificación personal ("NIP") por la red de datos externa, incluso en forma encriptada.

En una realización especialmente preferida, las contraseñas son almacenadas en la estación central de comunicaciones. Si el usuario desea realizar, por ejemplo, una transacción bancaria, el usuario accede a un agente bancario en software en la estación central de comunicaciones y especifica la transacción, pero no tiene que introducir su contraseña para dicho banco. En cambio, el agente de software recupera la contraseña almacenada en la estación central de comunicaciones y procesa la transacción con el banco. Esta disposición requiere que los usuarios confíen sus contraseñas a la estación central de comunicaciones, pero los usuarios ya confían en la estación central de comunicaciones con su seguridad y propiedad valiosa, de modo que es probable que se sientan cómodos al confiar sus contraseñas a la estación central de comunicaciones.

Además de realizar las funciones de red de datos externa en teclados del sistema, en otra realización el sistema también tiene un puerto o puertos a los que uno o varios dispositivos terminales externos pueden estar conectados para usar la conexión de red de datos externa. Por ejemplo, uno o más ordenadores personales podrían estar conectados al sistema para dicha finalidad.

En otra realización, al sistema se podría acceder, con contraseñas apropiadas y otras medidas de seguridad, desde un ordenador o terminal externo en la red de datos externa, de modo que los parámetros del sistema de seguridad podrían programarse a distancia usando la red de datos externa más bien que una conexión de marcación como se ha descrito anteriormente. Además, a algunos datos del sistema de seguridad, tal como el estado de varios sensores, se podría acceder por la red de datos externa o enviar periódicamente a una dirección predeterminada en la red de datos externa. Por ejemplo, si uno de los sensores es una videocámara, la salida vídeo podría ser enviada periódicamente a un receptor predeterminado. Igualmente, el sistema podría estar conectado a dispositivos domóticos, tales como los compatibles con el sistema X-10® desarrollado por X-10 Limited, de Hamilton, Bermuda, que permite controlar a distancias las luces, la temperatura y otras funciones.

El acceso al sistema del local desde la red de datos externa también se realiza preferiblemente a través de la estación central de comunicaciones. Por ejemplo, la estación central de comunicaciones podría mantener un sitio de la web mundial a través del que los abonados podrían contactar con sus sistemas domésticos desde otro lugar. Así, un abonado en su puesto de trabajo podría entrar en el sitio de la web y dar la orden de encender un cierto aparato en la casa. Los sistemas en la estación central de comunicaciones, después de comprobar que el usuario está autorizado, pondrían en cola las instrucciones hasta la vez siguiente que el sistema doméstico entre en contacto, tiempo en el que se enviarían las instrucciones, y se encendería el aparato.

La invención se describirá ahora con referencia a las figuras 1-7.

Una realización preferida de un sistema de seguridad de local 10 según la presente invención se representa en la figura 1. Un controlador de sistema 11, similar a un modelo 6139T que se puede obtener de Alarm Device Manufacturing Company ("Ademco", división de Pittway Corporation), de Syosset, Nueva York, se ha modificado para comunicar por un bus 12, preferiblemente un bus de cuatro hilos, con al menos una interface de comunicaciones 13. La interface de comunicaciones 13 es una interface de red de datos externa/Internet, también como se ha descrito anteriormente, que puede ser un router o interface ADSL (bucle digital simétrico de abonado), que proporciona acceso continuo a Internet por una línea externa de comunicaciones 14 que puede ser una conexión continua adecuada a Internet. La interface de comunicaciones 13 también podría ser un módem, preferiblemente un módem de 56 kbps, que proporcione una conexión de marcación por la línea externa de comunicaciones 14, que podría ser una línea de teléfono analógica estándar. El controlador 11 tiene preferiblemente una batería de reserva 113 que sirve al menos al controlador 11 y a la interface de comunicaciones 13.

El sistema 10 también incluye sensores convencionales que pueden incluir sensores de seguridad o disparo o ambos, y uno o más teclados de sistema convencionales o mejorados 16 como se ha explicado anteriormente y como se describe con más detalle a continuación. Los teclados 16 pueden estar conectados directamente al controlador 11 de manera convencional, como se representa, en cuyo caso las funciones de comunicaciones son enrutadas entre los teclados 11 y la interface de comunicaciones 13 a través del controlador 11. Alternativamente, los teclados 16 pueden estar conectados al bus 12 para enrutar las señales del sistema de seguridad a y del controlador 11 y las funciones de comunicaciones a y de la interface de comunicaciones 13. En otra alternativa, los teclados 16 pueden estar conectados directamente al controlador 11 (para funciones de seguridad) y al bus 12 (para funciones de comunicaciones). El controlador 11 está conectado preferiblemente a un dispositivo de sonido 110 (por ejemplo, una campana o sirena) para hacer sonar condiciones de alarma, y está conectado preferiblemente a una unidad marcadora 111 para comunicar con una estación central de supervisión, por ejemplo, por una línea de teléfono estándar.

Uno o más dispositivos de comunicaciones 17 podrían estar conectados a la interface de comunicaciones 13 por una conexión directa o a través del bus 12 como se representa (pero de ordinario no a través de ambas conexiones). Los dispositivos de comunicaciones 17 podrían ser ordenadores personales o terminales de ordenador.

Los ordenadores personales o terminales de ordenador 17 están conectados preferiblemente a la interface de comunicaciones 13 mediante el bus 12, aunque también se puede usar una conexión directa (por ejemplo, una conexión de red de área local Ethernet).

La figura 2 representa otra realización preferida de un sistema 20 según la invención. El sistema 20 es similar al sistema 10, a excepción de que se representan una unidad de interface telefónica separada 21 y una unidad de interface de datos separada 22. Deberá ser claro, sin embargo, que el sistema según la invención podría incluir solamente la interface 22 o ambas interfaces 21 y 22.

Como se representa, en el sistema 20, los sensores 15, los teclados 16, el dispositivo de sonido 110 y el marcador 111 están conectados al controlador 11 como en sistema 10 de la figura 1. La unidad de interface telefónica 21, que está conectada preferiblemente a una línea de teléfono analógica estándar 23, está conectada preferiblemente al controlador 11 por el bus 12. Un primer grupo de teléfonos 24 está conectado preferiblemente a la unidad de interface telefónica 21. Las funciones de contestador telefónico/buzón de voz/PBX están disponibles preferiblemente en los teclados 16 mediante el bus 12 o a través del controlador 11 al que los teclados 16 pueden estar conectados directamente.

Las funciones de contestador telefónico/buzón de voz/PBX también pueden estar disponibles en los teléfonos 24 conectados a la línea de teléfono 23 a través de unidad de interface telefónica 21. Otro grupo de uno o más teléfonos 25 pueden ser conectados directamente a la línea de teléfono 23. En una realización de la invención, las funciones de contestador telefónico/buzón de voz/PBX descritas anteriormente no estarían disponibles en los teléfonos 25. Sin embargo, en una realización alternativa de la invención, la unidad de interface telefónica 21 podría supervisar en la línea de teléfono 23 tonos DTMF que significan ciertas señales de orden, y realizar las funciones correspondientes incluso a los teléfonos 25. Sin embargo, la unidad de interface telefónica 25 sería incapaz de desconectar un teléfono 25 de la línea de teléfono 23, y por lo tanto no podría realizar ninguna función que requiera dicha desconexión, tal como la función de dirección pública en los altavoces de teclado. Podría estar disponible un limitado número de funciones, donde la marcación de las órdenes no haría que se realizase una llamada de teléfono.

La unidad de interface de datos 22, que está conectada preferiblemente a la línea de datos 26, está conectada preferiblemente al controlador 11 por bus 12. Opcionalmente, uno o más ordenadores personales o terminales de ordenador 27 están conectados preferiblemente a la unidad de interface de datos 22, por ejemplo, por una red de área local (representada como un enlace directo a la unidad de interface de datos 22) con el fin de compartir la línea de datos 26. Las funciones de datos descritas anteriormente están disponibles preferiblemente en los teclados 16 o mediante el bus 12, o a través de controlador 11 al que los teclados 16 pueden estar conectados directamente. Las funciones de datos descritas anteriormente también pueden estar disponibles a los ordenadores personales o terminales de ordenador 27 conectados a la unidad de interface de datos 22. Alternativamente, los ordenadores personales o los terminales de ordenador 27 podrían compartir simplemente la línea de datos 26 por una conexión alternativa representada en línea discontinua, sin conectarse a la unidad de interface de datos 22.

Uno o varios ordenadores personales o terminales de ordenador 27 también pueden estar conectados a la unidad de interface telefónica 21 mediante uno o más módems 240 de la manera descrita anteriormente, para programar características de la unidad de interface telefónica 21, o para descargar y almacenar mensajes de buzón de voz entrantes de la unidad de interface telefónica 21.

La unidad de interface de datos 22 también tiene preferiblemente acceso a datos de uno o varios sensores 15, tal como una cámara de seguridad, para transmisión de los datos de sensor por Internet u otra red de datos externa para que los vea una persona autorizada, y a dispositivos domóticos 215 para accionamiento remoto como se ha descrito anteriormente.

El controlador 11 del sistema 20 también incluye preferiblemente un receptor de radiofrecuencia u otro (por ejemplo, infrarrojos) 112 que recibe señales codificadas de uno o más transmisores 28. Un transmisor simple podría tener una tecla 29 para enviar un código que identifique a un usuario autorizado particular, por ejemplo, para armar o desarmar el sistema. Un transmisor más complicado 28 podría tener dos (o más) teclas 29 para permitir que un solo usuario envíe una de dos (o más) señales diferentes para realizar diferentes funciones (como se ha descrito anteriormente).

La figura 3 representa una realización de un teclado convencional del sistema de seguridad 30 que podría ser usado con la invención. El teclado 30 incluye preferiblemente un teclado numérico del tipo de teléfono estándar, incluyendo los dígitos 0-9 y, preferiblemente, los símbolos "*" y "#". Estos podrían ser usados para emitir órdenes estándar del sistema de seguridad, tales como introducir códigos de paso, u órdenes de interface telefónica. También se facilitan preferiblemente teclas de función 32 para la entrada de órdenes del sistema. Se ha previsto indicadores visuales 33, que son preferiblemente diodos fotoemisores, pero que también puede ser bombillas de luz u otros indicadores, para realizar indicaciones estándar del sistema de seguridad, por ejemplo, un aviso de que se ha evitado una zona, una indicación de que el sistema ha estado en alarma, un fallo de corriente CA, etc, así como indicaciones de interface de teléfono tales como una indicación de espera de mensaje. La pantalla alfanumérica 34, que puede ser una pantalla estándar de dos líneas y dieciséis caracteres por línea, también proporciona indicaciones del sistema de seguridad, e indicaciones de interface de teléfono tal como, por ejemplo, datos de identificación del llamante.

El teclado 30 también tiene preferiblemente un altavoz 35, como es convencional para proporcionar, por ejemplo, una indicación audible de prealarma, que también se puede usar para proporcionar indicaciones audibles de la interface de teléfono tal como una indicación audible de espera de mensaje, y más en particular puede ser usado para la reproducción de mensajes. El altavoz 35 también podría ser usado para permitir al usuario hacer llamadas de teléfono (usando las teclas 31) a números de teléfono de anuncio solamente o de respuesta de voz donde no se necesita una comunicación bidireccional. En una realización alternativa, el teclado 30 incluye un micrófono, que permite la grabación de saludos de buzón de voz salientes. Si el sistema está configurado, como acaba de explicarse, para poder hacer llamadas desde el teclado 30, el micrófono 36 se podría usar para hacer tales llamadas.

La figura 4 muestra una realización de una realización preferida de un teclado mejorado 40 diseñado para operar con la unidad de interface de datos 22 para realizar funciones de datos. Así, el teclado 40 tiene preferiblemente, en lugar del teclado numérico 13, un teclado alfanumérico completo 41, junto con teclas de función 32 e indicadores visuales 33. El teclado 40 también tiene preferiblemente una pantalla gráfica completa 44 en lugar de una pantalla alfanumérica 34. La pantalla 44 podría ser una pantalla de cristal líquido ("LCD"), pantalla de plasma de gas o tubo de rayos catódicos ("CRT"), que podría ser una pantalla en color o monocromática. La pantalla 44 podría tener además una capacidad táctil, en cuyo caso el teclado alfanumérico 41 podría ser un teclado "blando" que se puede reclamar en la pantalla 44 cuando se desee. Preferiblemente, el teclado 40 también tiene dos altavoces 45, para funciones audio

estéreo, si es necesario, aunque en una realización alternativa preferida solamente se puede prever un altavoz 45. El teclado 40 también tiene preferiblemente un micrófono 46, y tiene opcionalmente una videocámara 47 para funciones vídeo dúplex total, si es necesario.

Un diagrama esquemático de bloques de la circuitería 50 de un teclado similar al teclado 40, pero que incorpora algunas de las funciones de la unidad de interface de datos 22, se representa en la figura 5. Si se disponen múltiples teclados, los teclados "esclavos" adicionales pueden omitir la circuitería de la interface de datos, o pueden incluirla aunque pueda ser redundante. La circuitería 50 se forma preferiblemente alrededor de una unidad central de proceso ("CPU") 51 tal como un microprocesador 80386 o equivalente, que se puede obtener de Intel Corporation, de Santa Clara, California. A la CPU 51 está conectada preferiblemente una memoria de acceso aleatorio ("RAM") 52 así como una memoria no volátil 53 (por ejemplo, NVRAM). Si el sistema usa encriptado de clave pública compartida como se ha explicado anteriormente, la clave privada se almacena preferiblemente en la memoria no volátil 53. También se facilita preferiblemente una interface audio 54, que conecta con la red de datos externa 26 para funciones de entrada/salida audio, además de conectar con señales audio procedentes de la unidad de interface telefónica 21, si está presente en el sistema.

El bus de expansión 55 conecta preferiblemente la CPU 51 al teclado 41 y los indicadores 33. El bus de expansión 55 también conecta preferiblemente con una interface de red 56 que permite conectar varios teclados 50 al sistema 20 para operación de las funciones de seguridad del controlador 11, para acceso independiente a la red de datos externa 26, y para conexión a otros teclados 50 en una red de área local en el local servido por el sistema 20. Un controlador gráfico 57, que tiene preferiblemente su propia RAM gráfica asociada 570, también está conectado preferiblemente al bus 55 para permitir que la CPU 51 active la pantalla LCD gráfica 44. Una interface de pantalla táctil 58 conectada a la CPU 51 (no representada) está integrada preferiblemente con la pantalla 44.

Se prevé preferiblemente un reloj en tiempo real 59 para la CPU 51, y toda la circuitería 50 es activada preferiblemente por un suministro de potencia de 12 voltios CC 500 como indican las líneas de trazos 501.

Finalmente, la interface 502 conecta con el controlador 11, preferiblemente mediante el bus 12, mientras que la conexión a la red de datos externa 26 se realiza preferiblemente por una interface serie 503 que es, o se conecta a, un router, interface ADSL, módem u otro dispositivo de conexión de datos.

Una realización preferida 400 de un teclado numérico simplificado para uso con la invención se representa en la figura 6. El teclado 400 incluye preferiblemente un subconjunto de las características de teclado 40. Así, incluye preferiblemente una pantalla gráfica completa 44 con capacidad de pantalla táctil, evitando un teclado alfanumérico completo 41, pero permitiendo un teclado "blando" que puede ser reclamado en la pantalla 44 cuando se desee. Preferiblemente, el teclado 400 también tiene un altavoz 45 y un micrófono 46.

Un diagrama esquemático de bloques de la circuitería 60 de una realización preferida de una unidad de interface telefónica 21 según la invención se representa en la figura 7. Una unidad central de proceso (CPU) 61 controla preferiblemente las varias funciones de interface de teléfono y buzón de voz/contestador telefónico descritas anteriormente, como es convencional. El procesador de señales digitales (DSP) 62, conectado a la CPU 61, maneja las funciones de procesado de voz requeridas para las funciones de buzón de voz/contestador telefónico. Como se ha explicado anteriormente, DSP 62 permite preferiblemente la operación en dúplex total, de modo que si una llamada entrante no es captada en uno de los teléfonos del local, y el sistema 60 contesta la llamada, el llamante (si es suficientemente consciente de las funciones del sistema) puede anunciarle preferiblemente por los altavoces del sistema incluso mientras el mensaje de salida se está reproduciendo (en caso de que los residentes estén casa y deseen responder a la llamada). DSP 62 también incluye preferiblemente un decodificador DTMF incorporado que interpreta pulsaciones de tono doble/multifrecuencia (es decir, "Touch-Tone") realizadas en los teléfonos del local o remotos para permitir la entrada de órdenes del sistema desde tales teléfonos.

La CPU 61 y el DSP 62 están conectados a la memoria de acceso aleatorio 63, todos previstos preferiblemente como un solo conjunto de chips 64 junto con dos CODECs 65, 66. Un conjunto de chips adecuados es la familia de conjuntos de chip PCD600X que se puede obtener de de Philips Electronics, N.V., de Eindhoven, Países Bajos. Estos conjuntos de chip incluir UN CPU central 8051, RAM a bordo de 756 bytes, un DSP de punto fijo de 16 bits (con código ROM enmascarado), dos CODECs analógicos y convertidores generales digital a analógico y analógico a digital de 8 bits. El modelo PCD6002 incluye 32 kilobytes de OTP ROM, mientras que el modelo PCD6001 es sin ROM, pero puede ser usado, por ejemplo, con 64 kilobytes de memoria EPROM externa 67. Además, se puede prever una memoria flash 68, donde se puede almacenar mensajes de voz y otros datos de voz y configuración.

El conjunto de chips 64 está conectado a un microcontrolador 69, tal como un microcontrolador P87CL883, que también se puede obtener de Philips Electronics, que, a su vez, está conectado a una interface de sistema de seguridad 600, que permite preferiblemente el control del controlador del sistema de seguridad 11 de teléfonos conectados como se ha explicado anteriormente, y que permite preferiblemente el acceso a funciones de buzón de voz en los teclados del sistema. El microcontrolador 69 dirige el tráfico entre el sistema de seguridad 11 y la CPU 61/DSP 62, para determinar, por ejemplo, si una señal u orden de un teclado o teléfono se facilita como una orden del sistema de seguridad o una orden PBX/buzón de voz/contestador, o, a la inversa, si una señal u orden de sistema de seguridad 11 o CPU 61/DSP 62 se facilita como una orden relacionada con teléfono o una orden del sistema de seguridad. Esto permite enrutar adecuadamente las órdenes, y también permite poner los dispositivos en línea o fuera de según sea apropiado (por

ejemplo, desconectar teléfonos de la línea de teléfono de la oficina central cuando un teléfono esté siendo usado para enviar un mensaje por los altavoces del teclado).

Un módem 601, como puede ser convencional, puede estar conectado a la interface de línea de teléfono 602. El módem 601 podría servir como un dispositivo de comunicaciones de seguridad de reserva, permitiendo que el controlador 11 comunique con una estación central de supervisión si no se dispone de canales normales.

La interface de línea de teléfono 602 también está conectada mediante CODEC 65 a la CPU 61 y el DSP 62 para que la CPU 61 y el DSP 62 puedan realizar las funciones PBX/buzón de voz/contestador descritas anteriormente. El CODEC 66 conecta el DSP 62 al bus audio del sistema de seguridad 603 (también conectado a la interface del sistema de seguridad 600), permitiendo que la circuitería 60 comunique con los altavoces del teclado del sistema de seguridad. Además, la interface de línea de teléfono 602 conecta la línea de teléfono de la oficina central y los teléfonos del local al sistema y uno a otro. Las conexiones se hacen preferiblemente a través de relés adecuados (no representados) de modo que, en caso de fallo de potencia, la línea de teléfono de la oficina central se conectaría directamente a los teléfonos del local, mantener el servicio telefónico en el local.

Toda la circuitería 60 es activada preferiblemente por un suministro de potencia CC nominal de 12 voltios desde el controlador del sistema de seguridad 11, como indican las líneas de trazos 604.

Un sistema de comunicaciones 700 como el descrito anteriormente, que incorpora la presente invención, se representa en la figura 8. El sistema de comunicaciones 700 incluye una estación central de comunicaciones 701, al menos una estación central de supervisión 702 (una compañía de supervisión central abonada al sistema central de comunicaciones podría tener más de una estación de supervisión, o se podría abonar a más de una compañía de supervisión), y una pluralidad de sistemas de local 703, todos conectados a Internet 704.

Cada sistema de local 703 incluye preferiblemente un sistema 10 como se representa en la figura 1, incluyendo preferiblemente una unidad de interface 50 como se representa en la figura 5 que almacena una clave privada. El sistema 10 dentro del sistema 703 tiene una unidad de acceso a Internet 705, con acceso controlado por un cortafuegos 706.

Cada estación central de supervisión 702 tiene igualmente un procesador 707 que almacena una clave privada, una unidad de acceso a Internet 705 y un cortafuegos 706. El procesador 707 incluye un almacenamiento de datos (no representado) que guarda una o más bases de datos que identifican los locales a supervisar y el nivel de servicio de cada local, una base de datos de acciones a tomar en caso de varias condiciones de alarma u otras condiciones insólitas, etc.

La estación central de comunicaciones 701, además de tener una unidad de acceso a Internet 705 y un cortafuegos 706, tiene servidores de aplicación remotos 708 (estos pueden estar situados en otro lugar en las dependencias de los proveedores de los servicios en los servidores 708). La estación central de comunicaciones 701 también incluye redirectores seguros 711 que tienen acceso al almacenamiento de clave privada 709 para almacenar las claves privadas de todos los sistemas con los que comunica. Los redirectores 711 realizan el encriptado y desencriptado usando las teclas para comunicar con dichos sistemas.

La estación central de comunicaciones 701 comunica con Internet 704 a través del cortafuegos 706 y la unidad de acceso a Internet 705, conectando Internet al bus inseguro 713. Las comunicaciones en el bus inseguro 713 destinadas a los servidores remotos 708 pasan a través de redirectores 711 al bus seguro 714, con seguridad en base a las claves privadas almacenadas en 709.

Otro servidor web 712 mantiene el sitio web descrito anteriormente que permite a los usuarios desde cualquier posición de acceso a Internet 710 enviar instrucciones a los sistemas del local 10. Dado que el punto de servidor web 712 es permitir a un usuario en cualquier punto de acceso a Internet 710 acceder a su sistema seguro 703, y es probable que el punto de acceso 710 no esté registrado para usar redirectores 711, el servidor web 712 está preferiblemente protegido, como se representa, por seguridad convencional tal como encriptado SSL (Secure Socket Layer), tarjetas inteligentes, etc.

Entre los servidores remotos 708 hay servidores de retransmisión para retransmitir comunicaciones entre los varios sistemas 702, 703, así como desde el servidor 712 a las unidades 50 de los sistemas del local 10 en las unidades 702, como se ha descrito anteriormente, después de que las unidades redirectoras segundas 711 abren canales seguros.

La estación central de comunicaciones 701 puede estar separada de la estación central de supervisión 702 como se representa, o las estaciones 701 y 702 podrían estar combinadas o situadas conjuntamente. Igualmente, independientemente de sus posiciones relativas, podrían ser operadas por partes idénticas o diferentes.

El sistema de comunicaciones descrito podría ser usado para ofrecer o implementar varias características de seguridad.

Una función de los sistemas centrales de supervisión de alarmas es “supervisar” los sistemas de locales de alta seguridad como el sistema de alarma de un banco. Tradicionalmente se utilizaba un sistema de pregunta y respuesta en

el que la estación central contactaba individualmente periódicamente con cada sistema supervisado para asegurarse de que recibía una respuesta, y para comprobar el estado del sistema. Si no lo hacía, o si su estado no era normal, se tomaban las medidas apropiadas. En los sistemas posteriores, el sistema supervisado llamaba simplemente periódicamente por sí mismo, sin necesidad de ser interrogado. De nuevo, se tomaba la acción apropiada si el sistema supervisado no entraba a tiempo, o su estado no era normal. Según la presente invención, dado que el sistema del local tiene que entrar periódicamente, puede ser programado para informar de su estado al mismo tiempo. Cuando el sistema no entra, o fallo el estado normal, se actúa apropiadamente.

Igualmente, se puede hacer que dos sistemas de local 10 operen como un solo sistema comunicando a través de la estación central de comunicaciones 701. Por ejemplo, si una compañía tiene múltiples posiciones, se puede introducir los códigos de paso de empleados individuales sólo en el sistema en su posición "inicial", pero los sistemas situados en otras posiciones reconocerían los códigos de paso porque los sistemas podrían comunicar a través de la estación central de comunicaciones 701. Aunque tales sistemas pueden ser implementados tendiendo cables entre edificios adyacentes, la presente invención permite implementar tales sistemas entre posiciones extensas sin tender hilos ni alquilar líneas dedicadas caras.

Otra función que se podría implementar usando la presente invención es la descarga de datos de configuración al sistema 10. Los datos de configuración para la interface de usuario 16 o 50, incluyendo sitios web preferidos de varios usuarios, etc, así como datos de configuración de seguridad de los controladores 11, podrían estar almacenados en un servidor remoto 708 y descargarse cuando su sistema particular entre para ver si algún otro sistema desea contactar con él. En el caso de descarga de la configuración del controlador de seguridad 11, esto elimina la necesidad de que operadores de la estación central de alarma mantengan bancos de marcadores separados para descargar como hacen ahora.

Según otra función de la presente invención, si uno de dispositivos domóticos 215 es una videocámara, el sistema permite a un usuario en cualquier terminal 710 en Internet acceder con seguridad a la alimentación vídeo. El usuario entra en el servidor web 712 y pide la alimentación vídeo. La próxima vez que entre el sistema 703 del que la videocámara deseada es parte, el redirector 711 estableció un enlace al servidor 712, que reenvía la alimentación vídeo al usuario. En una alternativa a esta realización, que consume mucha anchura de banda a causa de la naturaleza de vídeo, el sistema puede evitar la retransmisión del vídeo, y por ello conservar anchura de banda, permitiendo comunicaciones directas seguras entre el terminal 710 y el sistema 703. Esto se puede hacer, después de autenticar ambas partes, enviando a cada parte una clave de sesión (generada, por ejemplo, por generador de claves de sesión seguras 715) y la dirección IP de la otra parte, y permitiendo que las partes comuniquen directamente. Cada parte sabe que recibió de forma segura la clave de sesión y la dirección de la otra parte, y, por lo tanto, cuando establecen comunicaciones entre sí, confían en que la comunicación es autorizada. En hecho, tal disposición puede ser usada incluso para comunicaciones de anchura de banda baja, si se desea.

Aunque cada uno de los componentes del sistema de comunicaciones 700 representado incluye un cortafuegos 706, el cortafuegos 706 se podría omitir de uno o más componentes. Como se ha explicado anteriormente, el sistema tiene ventajas incluso sin cortafuegos.

En otra realización, el sistema 10 no tiene que incluir características de seguridad. En cambio, el sistema 10 podría incluir solamente características de comunicaciones, y el sistema de comunicaciones 700 podría ser un sistema para comunicaciones seguras para los usuarios de Internet que lo deseen. Los abonados al sistema de comunicaciones 700 podrían permanecer seguros detrás de su cortafuegos, iniciándose las sesiones solamente por sus propios sistemas 10 a través de redirectores seguros 711. Si un abonado comunicase con otro abonado, cada uno comunicaría solamente cuando su propio sistema respectivo iniciase la sesión con los redirectores 711. Una comunicación, del primer abonado en iniciar una sesión, destinada a otro abonado, sería mantenida por los redirectores 711 hasta que el segundo abonado, a quien va dirigida la comunicación, hasta que la unidad del segundo abonado iniciase su propia sesión. En cada posición de abonado, se podría unir uno o más ordenadores personales al sistema 10, si se desea.

Preferiblemente, en una realización incluyendo características de seguridad, cada sistema 10 incluye al menos un canal secundario de comunicaciones, ilustrado en la figura 7 como el marcador 712, que está conectado preferiblemente a la interface de teléfono 713 de la estación de supervisión 702 por una línea telefónica pública conmutada 714. Naturalmente, el canal secundario puede incluir en cambio, o también, uno o más canales alternativos tal como un teléfono celular, celular de control de canal, o un radio enlace (no representado). Como se ha explicado anteriormente, el sistema podría intentar ambos (o todos los) canales, emitiendo el primer canal en tener éxito una señal u orden a través del sistema 10 para poner fin al (a los) otro(s) canal(es). Sin embargo, como también se ha explicado anteriormente, preferiblemente el canal primario tiene ventaja (por ejemplo, cinco segundos por delante) con respecto al (a los) canal(es) secundario(s). Los canales secundarios se inician solamente si el canal primario no tiene éxito dentro del período de "ventaja". Posteriormente, todos los canales intentan comunicar con la estación de supervisión 702 y el primero en lograrlo, que todavía puede ser el canal primario (por ejemplo, si Internet es el canal primario, puede haberse producido un retardo por tráfico pesado), pondrá fin, después del éxito, a los otros canales enviando una señal u orden a través del sistema 10.

El canal primario, que recibe la ventaja, es preferiblemente el canal más rápido, porque si opera, funcionará normalmente de forma suficientemente rápida para no tener que activar los otros canales. En un sistema donde Internet esté disponible como un canal, sería el canal más rápido. El canal celular de canal de control sería el más rápido

siguiente y recibiría la ventaja en un sistema sin acceso a Internet. El canal por radio sería el más rápido siguiente y recibiría la ventaja en un sistema sin acceso a Internet o celular de canal de control. Los teléfonos celulares y de línea terrestre tienen velocidades comparables; si son los únicos canales disponibles, el teléfono de línea terrestre lo intenta normalmente primero y tiene la ventaja.

Un usuario del sistema según la invención puede acceder preferiblemente a funciones de datos y opcionalmente a funciones de teléfono en una posición central al entrar en el local. Se ve así que se facilita un sistema de seguridad que minimiza el número de dispositivos electrónicos a los que una persona debe atender al volver a casa, combinando las funciones de los varios dispositivos. El sistema también se puede usar en cualquier tiempo en que el usuario esté en casa. También se realizan comunicaciones seguras entre el sistema del local y otros sistemas. Los expertos en la técnica apreciarán que la presente invención se puede poner en práctica de forma distinta a las realizaciones descritas, que se presentan a efectos de ilustración y no de limitación, y la presente invención se limita solamente por las reivindicaciones siguientes.

REIVINDICACIONES

1. Un sistema integrado de seguridad y comunicaciones para supervisar locales de usuario, incluyendo el sistema:

al menos un sensor (15);

al menos un dispositivo de salida de alarma (110);

al menos una interface de control de usuario (13) situada en los locales de usuario; y

un controlador de sistema (11) conectado al sensor (15), el dispositivo de salida de alarma (110) y la interface de control de usuario (13);

donde al menos una de la al menos una interface de control de usuario está conectada a una red de datos externa y está dispuesta para enviar y/o recibir correo electrónico y/o datos de Internet, y el sistema tiene al menos un usuario autorizado, y tiene una unidad de autorización para identificar de forma única cada uno de al menos uno de los usuarios autorizados y, cuando uno del al menos un usuario autorizado introduce una orden de armado o desarmado del sistema de seguridad en la interface de control de usuario activando la unidad de autorización, usando un indicio único para uno del al menos un usuario autorizado, correo electrónico y/o datos de Internet personalizados para dicho usuario son visualizados en la al menos una interface de control de usuario.

2. El sistema integrado de seguridad y comunicaciones de la reivindicación 1, donde la al menos una de la al menos una interface de control de usuario (13) está conectada además a al menos un canal alternativo.

3. El sistema integrado de seguridad y comunicaciones de alguna de las reivindicaciones precedentes, donde:

la al menos una interface de control de usuario (13) es utilizada por un usuario para introducir órdenes que afectan a un estado del sistema; y

el sistema, cuando el estado indica que el sistema está activo, supervisa el al menos un sensor (15) y emite una alarma en el dispositivo de salida de alarma (110) cuando el al menos un sensor (15) indica que existe una condición de alarma.

4. El sistema integrado de seguridad y comunicaciones de la reivindicación 3, donde el acceso al correo electrónico es restringido en base al estado del sistema.

5. El sistema integrado de seguridad y comunicaciones de la reivindicación 4, donde el correo electrónico es accesible cuando el estado es consistente con la presencia de un usuario autorizado en los locales de usuario.

6. El sistema integrado de seguridad y comunicaciones de la reivindicación 5, donde:

la interface de control de usuario (13) presenta para acceso en la interface de control de usuario solamente correo electrónico dirigido al usuario autorizado particular.

7. El sistema integrado de seguridad y comunicaciones de la reivindicación 5 o la reivindicación 6, donde:

la interface de control de usuario (13) presenta acceso en la interface de control de usuario a un mensaje de correo electrónico enviado por el usuario autorizado particular.

8. El sistema integrado de seguridad y comunicaciones de alguna de las reivindicaciones precedentes, donde:

cuando uno del al menos un usuario autorizado introduce una orden de armado o desarmado del sistema de seguridad en la interface de control de usuario (13) activando la unidad de autorización usando un indicio único para uno del al menos un usuario autorizado, la interface de control de usuario (13) envía un mensaje de correo electrónico a un receptor predeterminado advirtiendo de la entrada de la orden por el usuario.

9. El sistema integrado de seguridad y comunicaciones de alguna de las reivindicaciones precedentes, donde:

la red de datos externa es Internet;

los datos de Internet incluyen páginas de la web mundial; y

cuando uno del al menos un usuario autorizado introduce una orden de armado o desarmado del sistema de seguridad en la interface de control de usuario (13) activando la unidad de autorización usando un indicio único para uno del al menos un usuario autorizado, el sistema recupera una página de la web mundial dirigida al uno del al menos un usuario autorizado y visualiza la página de la web mundial en la interface de control de usuario (13).

10. El sistema integrado de seguridad y comunicaciones de la reivindicación 9, donde:

la interface de control de usuario (13) incluye un receptor;

el indicio incluye un transmisor respectivo codificado de forma única con múltiples códigos para cada uno del al menos un usuario autorizado;

la activación de la unidad de autorización incluye activación de un código seleccionado de los múltiples códigos por uno del al menos un usuario autorizado en rango de comunicación del receptor; y

el sistema recupera una página diferente de la web mundial en base a cuál de los múltiples códigos ha sido seleccionado.

11. El sistema integrado de seguridad y comunicaciones de la reivindicación 9 o la reivindicación 10, donde:

la interface de control de usuario (13) incluye un teclado numérico (31;41);

el indicio incluye un respectivo código de paso único para cada uno del al menos un usuario autorizado; y

la activación de la unidad de autorización incluye la entrada del código de paso en el teclado.

12. El sistema integrado de seguridad y comunicaciones de cualquiera de las reivindicaciones 9 a 11, donde:

la interface de control de usuario (13) incluye un receptor;

el indicio incluye un transmisor respectivo codificado de forma única para cada uno del al menos un usuario autorizado; y

la activación de la unidad de autorización incluye activación del transmisor codificado en el rango de comunicación del receptor.

13. El sistema integrado de seguridad y comunicaciones de la reivindicación 12, donde el receptor y el transmisor codificado son inalámbricos.

14. El sistema integrado de seguridad y comunicaciones de cualquiera de las reivindicaciones 8 a 13, donde:

la interface de control de usuario (13) incluye un lector de fichas;

el indicio incluye una ficha codificada de forma única para cada uno del al menos un usuario autorizado; y la activación de la unidad de autorización incluye presentación de la ficha codificada al lector de fichas.

15. El sistema integrado de seguridad y comunicaciones de alguna de las reivindicaciones precedentes, donde:

uno del al menos un usuario autorizado activa la unidad de autorización usando un indicio único para uno del al menos un usuario autorizado; la red de datos externa es Internet; y la activación de la unidad de autorización registra uno del al menos un usuario autorizado por Internet en la interface de control de usuario (13).

16. El sistema integrado de seguridad y comunicaciones de alguna de las reivindicaciones precedentes, donde:

uno del al menos un usuario autorizado introduce una orden de armado o desarmado del sistema de seguridad en la interface de control de usuario (13) activando la unidad de autorización usando un indicio único para uno del al menos un usuario autorizado; uno del al menos un usuario autorizado usa la red de datos externa para acceder a una institución financiera para realizar una transacción financiera;

el indicio es registrado con la institución financiera como un identificador del uno del al menos un usuario autorizado; y

el indicio es enviado a la institución financiera como parte de la transacción financiera.

17. El sistema integrado de seguridad y comunicaciones de alguna de las reivindicaciones precedentes, donde:

el sistema transmite señales de datos de seguridad a una estación central de comunicaciones mediante la red de datos externa y un canal alternativo y espera su reconocimiento; y

cuando el reconocimiento llega de un primero de la red de datos externa y el canal alternativo, el sistema termina la transmisión de los datos de seguridad en un segundo de la red de datos externa y el canal alternativo.

18. El sistema integrado de seguridad y comunicaciones de la reivindicación 17, donde:

uno de la red de datos externa y el canal alternativo opera normalmente más rápido que otro de la red de datos externa y el canal alternativo; y

el sistema comienza la transmisión de las señales de datos de seguridad en uno de la red de datos externa y el canal alternativo antes de comenzar la transmisión de las señales de datos de seguridad en el otro de la red de datos externa y el canal alternativo.

19. El sistema integrado de seguridad y comunicaciones de la reivindicación 17 o la reivindicación 18, incluyendo además un cortafuegos entre la interface de control de usuario y la red de datos externa; donde:

el cortafuegos permite solamente la comunicación que se origina en el sistema y evita la comunicación que se origina en la red de datos externa; y

para recibir el reconocimiento de la estación central de comunicaciones, el sistema inicia la comunicación con la red de datos externa de modo que el cortafuegos permita la comunicación, incluyendo la comunicación iniciada una consulta a la red de datos externa para que el reconocimiento sea comunicado de la estación central de comunicaciones al sistema.

20. El sistema integrado de seguridad y comunicaciones de la reivindicación 19, donde la consulta a la red externa incluye una consulta a la estación central de comunicaciones.

21. El sistema integrado de seguridad y comunicaciones de cualquiera de las reivindicaciones 17 a 20, donde el canal alternativo es una línea de teléfono (23).

22. El sistema integrado de seguridad y comunicaciones de cualquiera de las reivindicaciones 17 a 21, donde:

el sistema transmite señales de datos de seguridad a una estación central de comunicaciones mediante una pluralidad de canales; y

cuando el reconocimiento llega de un primer canal de la pluralidad de canales, el sistema termina la transmisión de los datos de seguridad en cada uno de los otros canales múltiples.

23. El sistema integrado de seguridad y comunicaciones de la reivindicación 22, donde:

uno de la pluralidad de canales opera normalmente más rápido que otros de la pluralidad de canales; y

el sistema comienza la transmisión de las señales de datos de seguridad en uno de la pluralidad de canales antes de comenzar la transmisión de las señales de datos de seguridad en los otros de la pluralidad de canales.

24. El sistema integrado de seguridad y comunicaciones de alguna de las reivindicaciones precedentes, incluyendo más de una de las interfaces de control de usuario (13), funcionando cada una de las interfaces de control de usuario como un terminal independiente de la red de datos externa.

25. El sistema integrado de seguridad y comunicaciones de alguna de las reivindicaciones precedentes, incluyendo además un cortafuegos entre la interface de control de usuario y la red de datos externa, donde:

el cortafuegos permite solamente la comunicación que se origina en el sistema y evita la comunicación que se origina en la red de datos externa; y

para recibir datos, el sistema inicia la comunicación con la red de datos externa de modo que el cortafuegos permita la comunicación, incluyendo la comunicación iniciada una consulta a la red de datos externa para que los datos buscados sean comunicados de la red de datos externa al sistema.

26. El sistema integrado de seguridad y comunicaciones de alguna de las reivindicaciones precedentes, donde las funciones del sistema son accesibles a distancia mediante la red de datos externa.

27. El sistema integrado de seguridad y comunicaciones de alguna de las reivindicaciones precedentes, donde el sistema acepta órdenes de un usuario mediante la red de datos externa.

28. El sistema integrado de seguridad y comunicaciones de la reivindicación 27, incluyendo además un cortafuegos entre la interface de control de usuario y la red de datos externa, donde:

el cortafuegos permite solamente la comunicación que se origina en el sistema y evita la comunicación que se origina en la red de datos externa; y

para recibir las órdenes del usuario, el sistema inicia la comunicación con la red de datos externa de modo que el cortafuegos permita la comunicación, incluyendo la comunicación iniciada una consulta a la red de datos externa para que las órdenes dadas por el usuario sean comunicadas de la red de datos externa al sistema.

29. El sistema integrado de seguridad y comunicaciones de alguna de las reivindicaciones precedentes, donde el sistema envía señales de datos de seguridad a receptores predeterminados mediante la red de datos externa.

30. Un método integrado de seguridad y comunicaciones para supervisar locales de usuario, incluyendo el método:

proporcionar al menos un sensor (15);

proporcionar al menos un dispositivo de salida de alarma (110);

proporcionar al menos una interface de control de usuario (13) en los locales de usuario; y

proporcionar un controlador de sistema (11) conectado al sensor (15), el dispositivo de salida de alarma (110) y la interface de control de usuario (13);

donde al menos una de la al menos una interface de control de usuario está conectada a una red de datos externa y está dispuesta para enviar y/o recibir correo electrónico y/o datos de Internet, y el sistema tiene al menos un usuario autorizado, y tiene una unidad de autorización para identificar de forma única cada uno de al menos uno de los usuarios autorizados y cuando uno del al menos un usuario autorizado introduce una orden de armado o desarmado del sistema de seguridad en la interface de control de usuario activando la unidad de autorización, usando un indicio único para uno del al menos un usuario autorizado, correo electrónico y/o datos de Internet personalizados para dicho usuario se visualizan en la al menos una interface de control de usuario.

31. El método integrado de seguridad y comunicaciones de la reivindicación 30, donde la al menos una de la al menos una interface de control de usuario (13) está conectada además a al menos un canal alternativo.

32. El método integrado de seguridad y comunicaciones de la reivindicación 30 o la reivindicación 31, donde:

la al menos una interface de control de usuario (13) es utilizada por un usuario para introducir órdenes que afectan a un estado del sistema, y el método incluye además:

cuando el estado indica que el sistema está activo, supervisar el al menos un sensor (15) y enviar una alarma en el dispositivo de salida de alarma (110) cuando el al menos un sensor (15) indica que existe una condición de alarma.

33. El método integrado de seguridad y comunicaciones de la reivindicación 32, donde el acceso al correo electrónico es restringido en base al estado del sistema.

34. El método integrado de seguridad y comunicaciones de la reivindicación 33, donde el correo electrónico es accesible cuando el estado es consistente con la presencia de un usuario autorizado en los locales de usuario.

35. El método integrado de seguridad y comunicaciones de la reivindicación 34, donde el método incluye además:

presentar, para acceso en la interface de control de usuario (13), solamente correo electrónico dirigido al usuario autorizado particular.

36. El método integrado de seguridad y comunicaciones de la reivindicación 34 o la reivindicación 35, donde el método incluye además

presentar en la interface de control de usuario (13) acceso a mensajes de correo electrónico enviados por el usuario autorizado particular.

37. El método integrado de seguridad y comunicaciones de cualquiera de las reivindicaciones 30 a 36, donde:

cuando uno del al menos un usuario autorizado introduce una orden de armado o desarmado del sistema de seguridad en la interface de control de usuario (13) activando la unidad de autorización usando un indicio único para uno del al menos un usuario autorizado, envía un mensaje de correo electrónico a un receptor predeterminado advirtiendo de la entrada de la orden por el usuario.

38. El método integrado de seguridad y comunicaciones de cualquiera de las reivindicaciones 30 a 37, donde:

la red de datos externa es Internet;

los datos de Internet incluyen páginas de la web mundial; y

el método incluye además, cuando uno del al menos un usuario autorizado introduce una orden de armado o desarmado del sistema de seguridad en la interface de control de usuario (13) activando la unidad de autorización usando un indicio único para uno del al menos un usuario autorizado, recuperar una página de la web mundial dirigida al uno del al menos un usuario autorizado y presentar la página de la web mundial en la interface de control de usuario (13).

39. El método integrado de seguridad y comunicaciones de la reivindicación 38, donde:

la interface de control de usuario (13) incluye un receptor; y

el indicio incluye un respectivo transmisor codificado de forma única con múltiples códigos para cada uno del al menos un usuario autorizado, y el método incluye además:

activar la unidad de autorización activando un código seleccionado de los múltiples códigos del transmisor codificado en el rango de comunicación del receptor; y

recuperar una página diferente de la web mundial en base a cuál de los múltiples códigos ha sido seleccionado.

40. El método integrado de seguridad y comunicaciones de la reivindicación 38 o la reivindicación 39, incluyendo además:

proporcionar un teclado (31;41) en la interface de control de usuario (13); donde:

el indicio incluye un respectivo código de paso único para cada uno del al menos un usuario autorizado; y

la activación de la unidad de autorización incluye la entrada del código de paso en el teclado.

41. El método integrado de seguridad y comunicaciones de cualquiera de las reivindicaciones 38 a 40, donde:

la interface de control de usuario (13) incluye un receptor; y

el indicio incluye un respectivo transmisor codificado de forma única a cada uno del al menos un usuario autorizado, y el método incluye además:

activar la unidad de autorización activando el transmisor codificado en el rango de comunicación del receptor.

42. El método integrado de seguridad y comunicaciones de cualquiera de las reivindicaciones 38 a 41, donde:

la interface de control de usuario (13) incluye un lector de fichas; y

el indicio incluye una ficha codificada de forma única para cada uno del al menos un usuario autorizado, y el método incluye además:

activar la unidad de autorización presentando la ficha codificada al lector de fichas.

43. El método integrado de seguridad y comunicaciones de cualquiera de las reivindicaciones 30 a 42, donde:

uno del al menos un usuario autorizado activa la unidad de autorización usando un indicio único para uno del al menos un usuario autorizado; y

la red de datos externa es Internet, y el método incluye además:

a la activación de la unidad de autorización, registrar uno del al menos un usuario autorizado por Internet en la interface de control de usuario (13).

44. El método integrado de seguridad y comunicaciones de cualquiera de las reivindicaciones 30 a 43, donde:

uno del al menos un usuario autorizado introduce una orden de armado o desarmado del sistema de seguridad en la interface de control de usuario (13) activando la unidad de autorización usando un indicio único para uno del al menos un usuario autorizado;

el uno del al menos uno usuario usa la red de datos externa para acceder a una institución financiera para realizar una transacción financiera; y

el indicio es registrado con la institución financiera como un identificador del uno del al menos un usuario autorizado, y el método incluye además:

enviar el indicio a la institución financiera como parte de la transacción financiera.

45. El método integrado de seguridad y comunicaciones de cualquiera de las reivindicaciones 30 a 44, incluyendo además:

transmitir señales de datos de seguridad a una estación central de comunicaciones mediante la red de datos externa y un canal alternativo y esperar su reconocimiento; y

cuando el reconocimiento llega de un primero de la red de datos externa y el canal alternativo, terminar la transmisión de los datos de seguridad en un segundo de la red de datos externa y el canal alternativo.

46. El método integrado de seguridad y comunicaciones de la reivindicación 45, donde:

uno de la red de datos externa y el canal alternativo opera normalmente más rápido que otro de la red de datos externa y el canal alternativo; y

la transmisión de las señales de datos de seguridad a la estación central de comunicaciones mediante uno de la red de datos externa y el canal alternativo comienza antes de la transmisión de las señales de datos de seguridad a la estación central de comunicaciones mediante el otro de la red de datos externa y el canal alternativo.

47. El método integrado de seguridad y comunicaciones de la reivindicación 45 o la reivindicación 46, donde:

hay un cortafuegos entre la interface de control de usuario y la red de datos externa, permitiendo el cortafuegos solamente la comunicación que se origina en el sistema y evitando la comunicación que se origina en la red de datos externa, y el método incluye además:

recibir el reconocimiento de la estación central de comunicaciones, iniciar comunicación con la red de datos externa de modo que el cortafuegos permita la comunicación, incluyendo la comunicación iniciada una consulta a la red de datos externa para que el reconocimiento sea comunicado de la estación central de comunicaciones al sistema.

48. El método integrado de seguridad y comunicaciones de la reivindicación 47, donde la consulta a la red externa incluye una consulta a la estación central de comunicaciones.

49. El método integrado de seguridad y comunicaciones de cualquiera de las reivindicaciones 45 a 48, donde el canal alternativo es una línea de teléfono.

50. El método integrado de seguridad y comunicaciones de cualquiera de las reivindicaciones 45 a 49, incluyendo además:

transmitir señales de datos de seguridad a una estación central de comunicaciones mediante una pluralidad de canales; y

cuando el reconocimiento llega de un primer canal de la pluralidad de canales, terminar la transmisión de los datos de seguridad en cada uno de los otros múltiples canales.

51. El método integrado de seguridad y comunicaciones de la reivindicación 50, donde:

uno de la pluralidad de canales opera normalmente más rápido que otros de la pluralidad de canales; y

la transmisión de las señales de datos de seguridad a la estación central de comunicaciones mediante uno de la pluralidad de canales comienza antes de la transmisión de las señales de datos de seguridad a la estación central de comunicaciones mediante los otros de la pluralidad de canales.

52. El método integrado de seguridad y comunicaciones de cualquiera de las reivindicaciones 30 a 51, donde:

hay un cortafuegos entre la interface de control de usuario (13) y la red de datos externa, permitiendo el cortafuegos solamente la comunicación que se origina en el sistema y evitando la comunicación que se origina en la red de datos externa, y el método incluye además:

para recibir datos, iniciar comunicación con la red de datos externa de modo que el cortafuegos permita la comunicación, incluyendo la comunicación iniciada una consulta a la red de datos externa para que los datos buscados sean comunicados de la red de datos externa al sistema.

53. El método integrado de seguridad y comunicaciones de cualquiera de las reivindicaciones 30 a 52, incluyendo además aceptar órdenes de un usuario mediante la red de datos externa.

54. El método de seguridad de la reivindicación 53, donde:

hay un cortafuegos entre la interface de control de usuario (13) y la red de datos externa, permitiendo el cortafuegos solamente la comunicación que se origina en el sistema y evitando la comunicación que se origina en la red de datos externa, y el método incluye además:

para recibir las órdenes del usuario, iniciar comunicación con la red de datos externa de modo que el cortafuegos permita la comunicación, incluyendo la comunicación iniciada una consulta a la red de datos externa para que las órdenes dadas por el usuario sean comunicadas de la red de datos externa al sistema.

55. El método integrado de seguridad y comunicaciones de cualquiera de las reivindicaciones 30 a 54, incluyendo además enviar señales de datos de seguridad a receptores predeterminados mediante la red de datos externa.

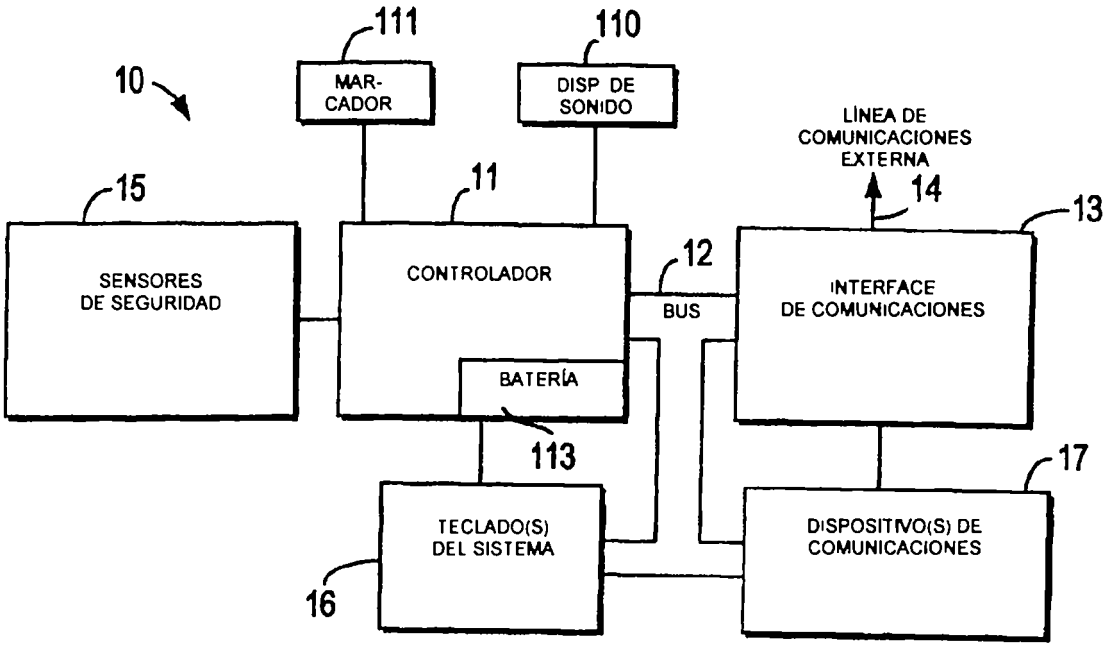
10
111
MAR-
CADOR
110
DISP DE
SONIDO
LÍNEA DE
COMUNICACIONES
EXTERNA
14
15
11
13
SENSORES
DE SEGURIDAD
CONTROLADOR
12
BUS
INTERFACE
DE COMUNICACIONES
BATERÍA
113
17
TECLADO(S)
DEL SISTEMA
DISPOSITIVO(S) DE
COMUNICACIONES
16

FIG. 1

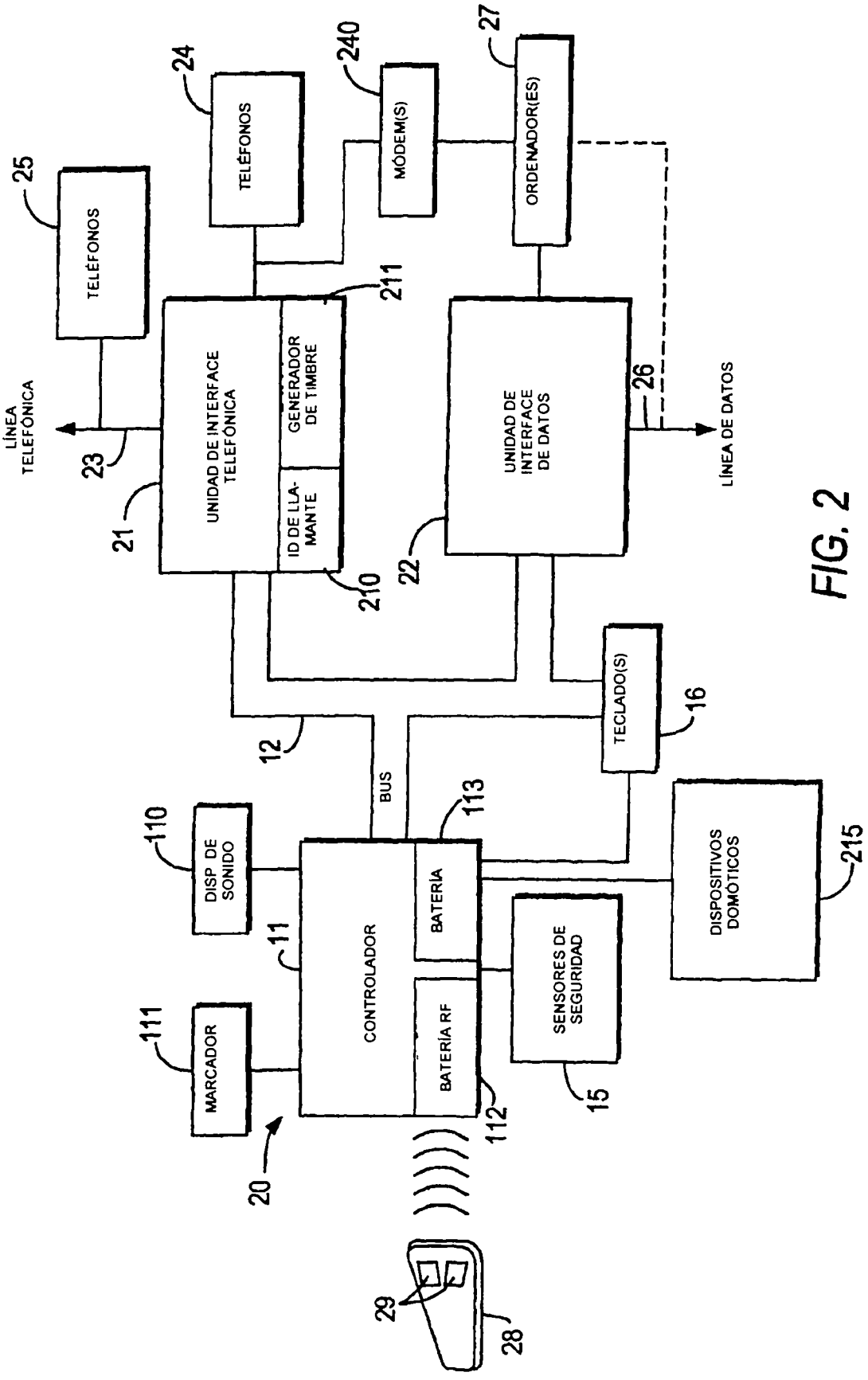
TELÉFONOS
25
TELÉFONOS
24
MÓDEM(S)
240
ORDENADOR(ES)
27
LÍNEA TELEFÓNICA
23
UNIDAD DE INTERFACE TELEFÓNICA
21
GENERADOR DE TIMBRE
ID DE LLA-MANTE
211
210
UNIDAD DE INTERFACE DE DATOS
22
26
LÍNEA DE DATOS
TECLADO(S)
16
12
BUS
113
DISP. DE SONIDO
110
CONTROLADOR
11
BATERÍA
BATERÍA RF
112
DISPOSITIVOS DOMÓTICOS
215
SENSORES DE SEGURIDAD
15
MARCADOR
111
20
29
28

FIG. 2

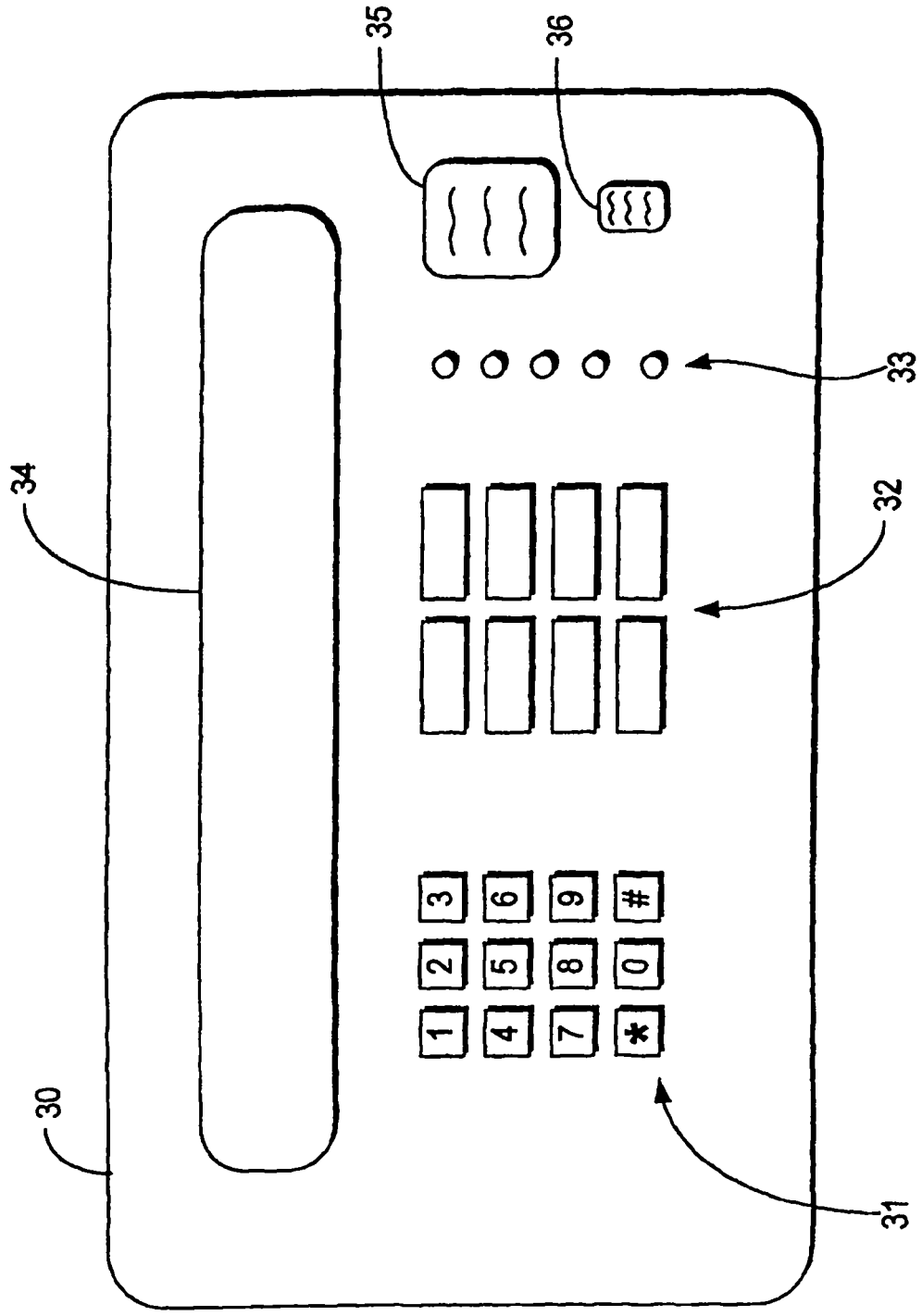

FIG. 3

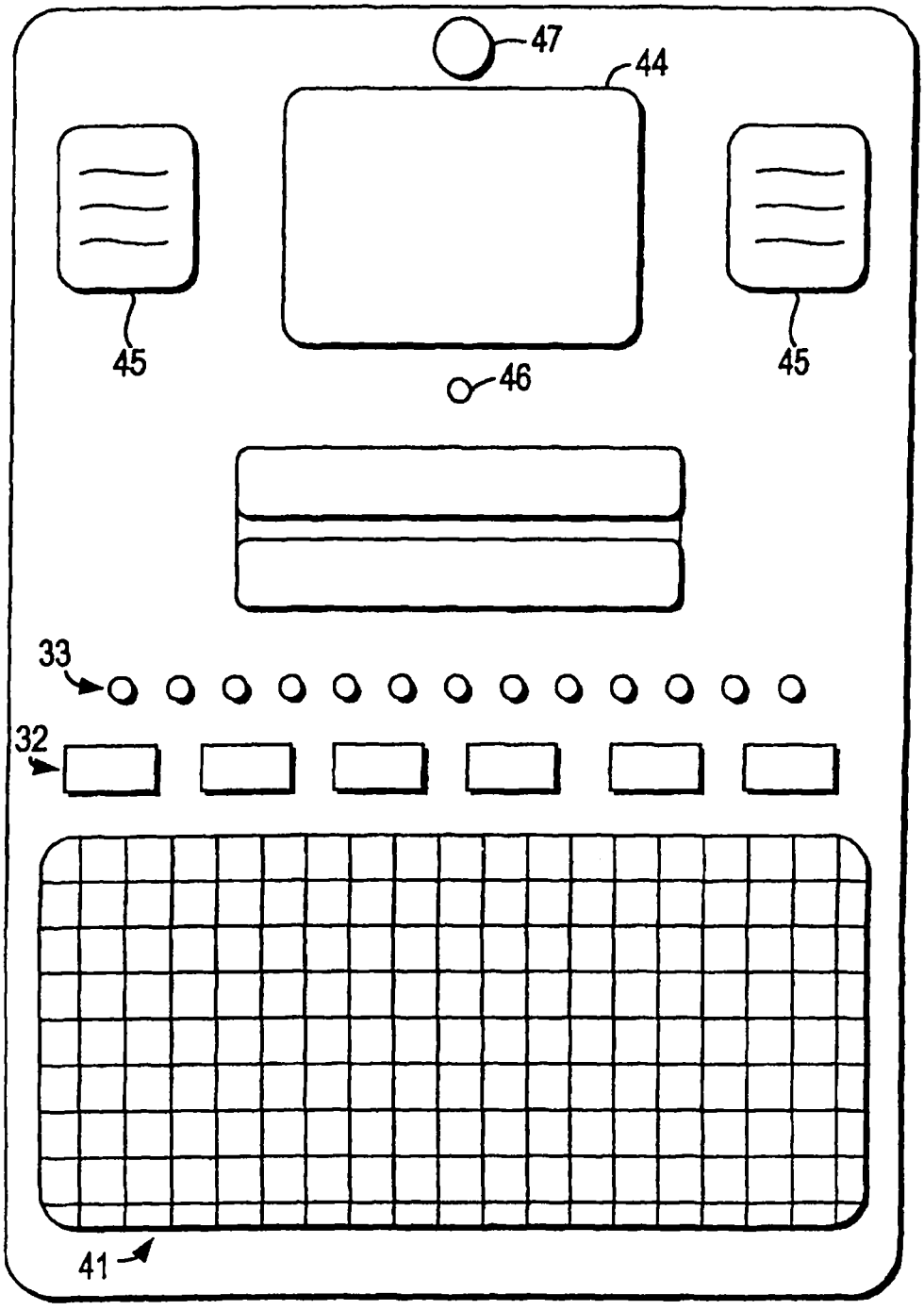

FIG. 4

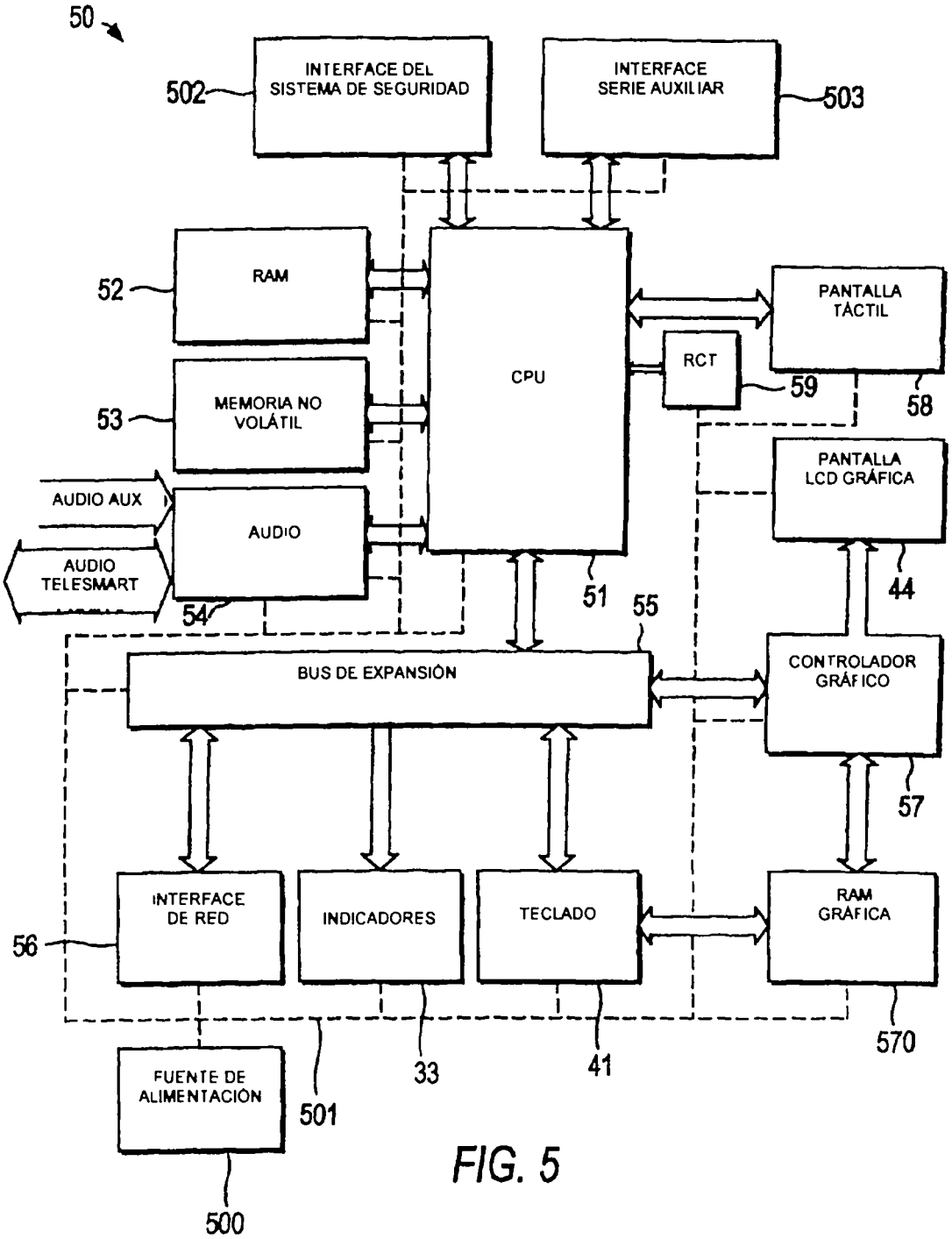
50
INTERFACE DEL SISTEMA DE SEGURIDAD
502
INTERFACE SERIE AUXILIAR
503
RAM
52
CPU
PANTALLA TÁCTIL
RCT
59
58
MEMORIA NO VOLÁTIL
53
PANTALLA LCD GRÁFICA
AUDIO AUX
AUDIO
AUDIO TELESMART
54
51
55
44
BUS DE EXPANSIÓN
CONTROLADOR GRÁFICO
57
INTERFACE DE RED
INDICADORES
TECLADO
RAM GRÁFICA
56
570
33
41
FUENTE DE ALIMENTACIÓN
501
500

FIG. 5

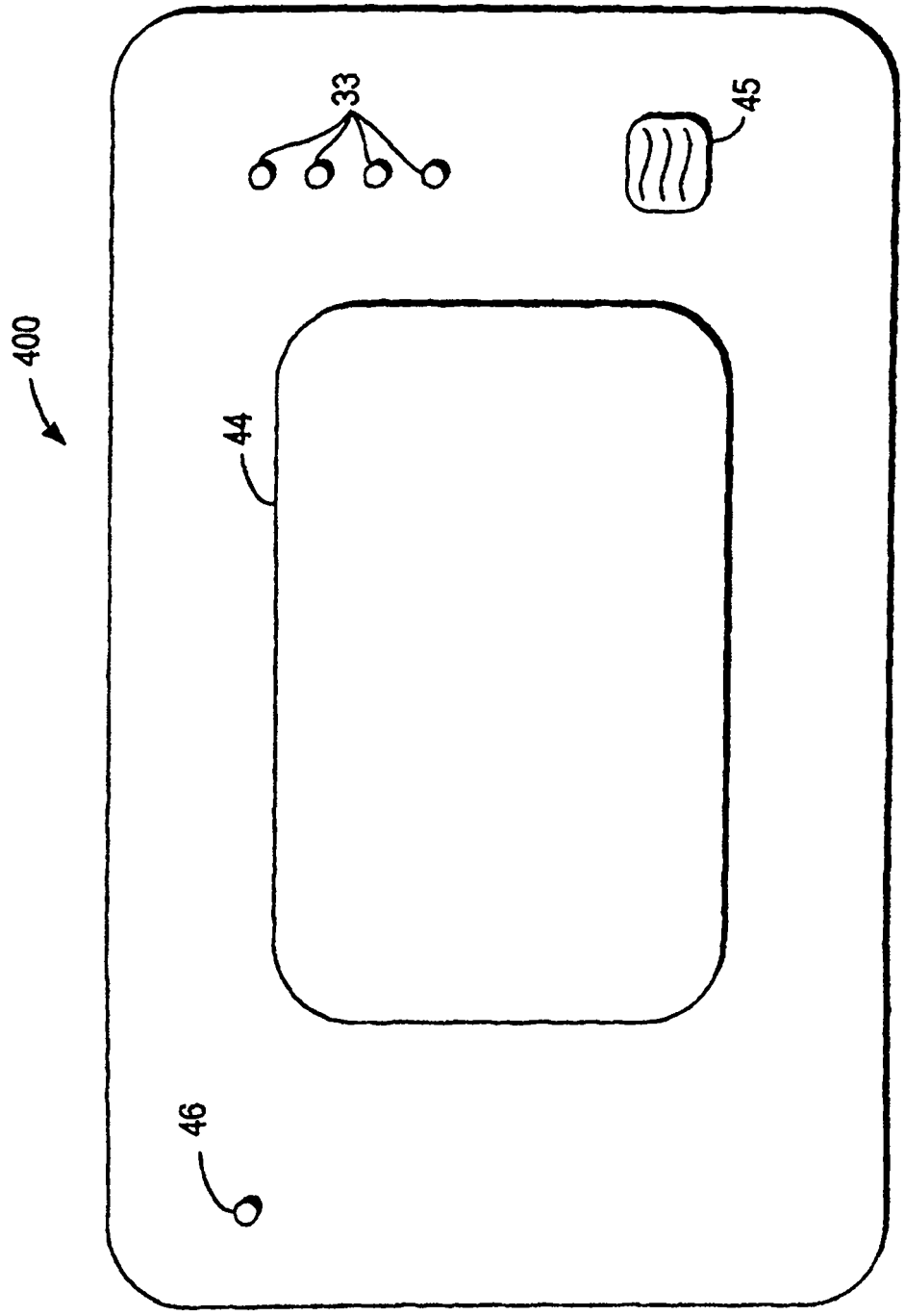

FIG. 6

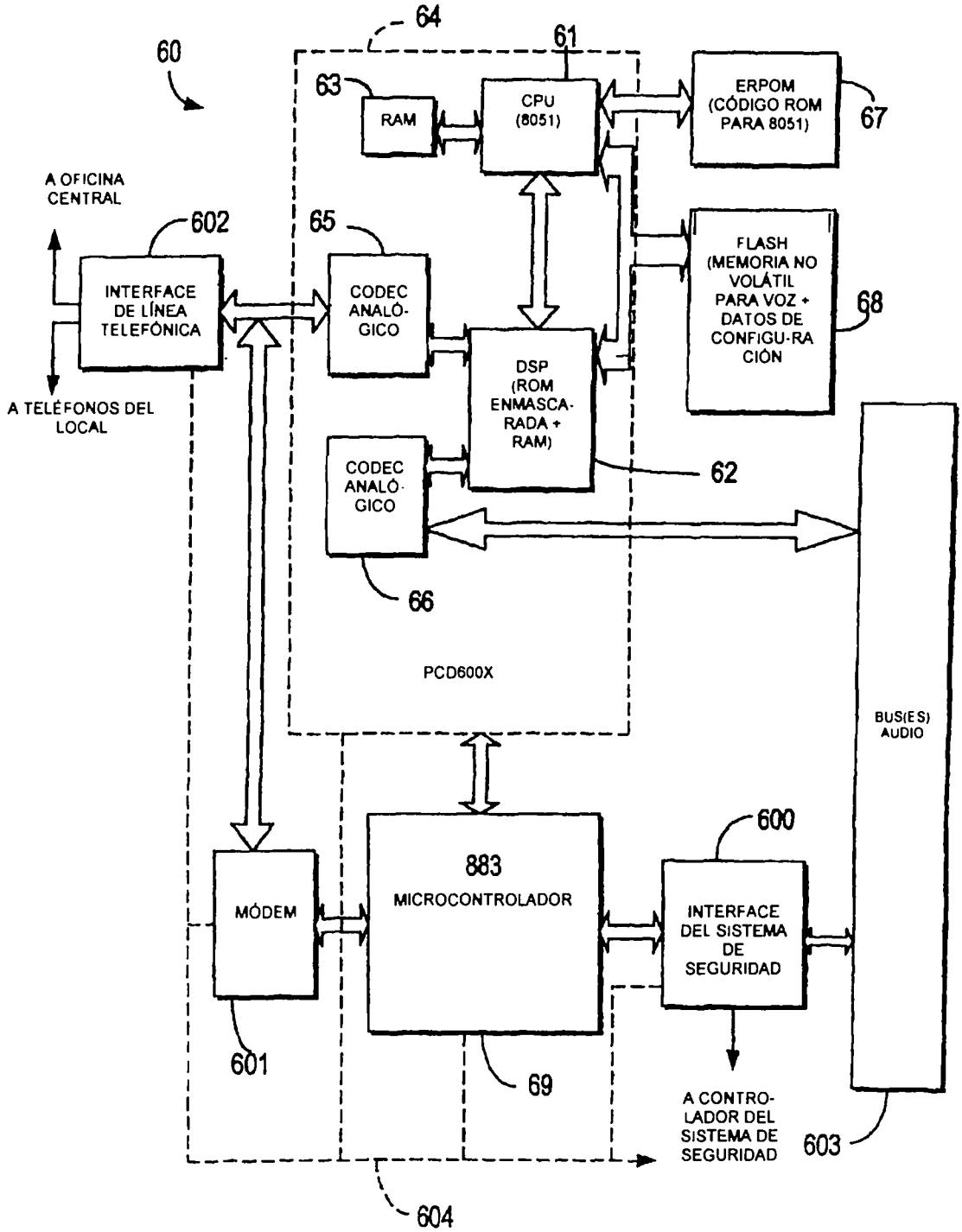
60
64
61
63
RAM
CPU (8051)
ERPOM (CÓDIGO ROM PARA 8051)
67
A OFICINA CENTRAL
602
65
INTERFACE DE LÍNEA TELEFÓNICA
CODEC ANALÓ-GICO
FLASH (MEMORIA NO VOLÁTIL PARA VOZ + DATOS DE CONFIGU-RA CIÓN
68
DSP (ROM ENMASCA-RADA + RAM)
A TELÉFONOS DEL LOCAL
CODEC ANALÓ-GICO
62
66
PCD600X
BUS(ES) AUDIO
600
883
MICROCONTROLADOR
MÓDEM
INTERFACE DEL SISTEMA DE SEGURIDAD
601
69
A CONTRO-LADOR DEL SISTEMA DE SEGURIDAD
603
604

FIG. 7

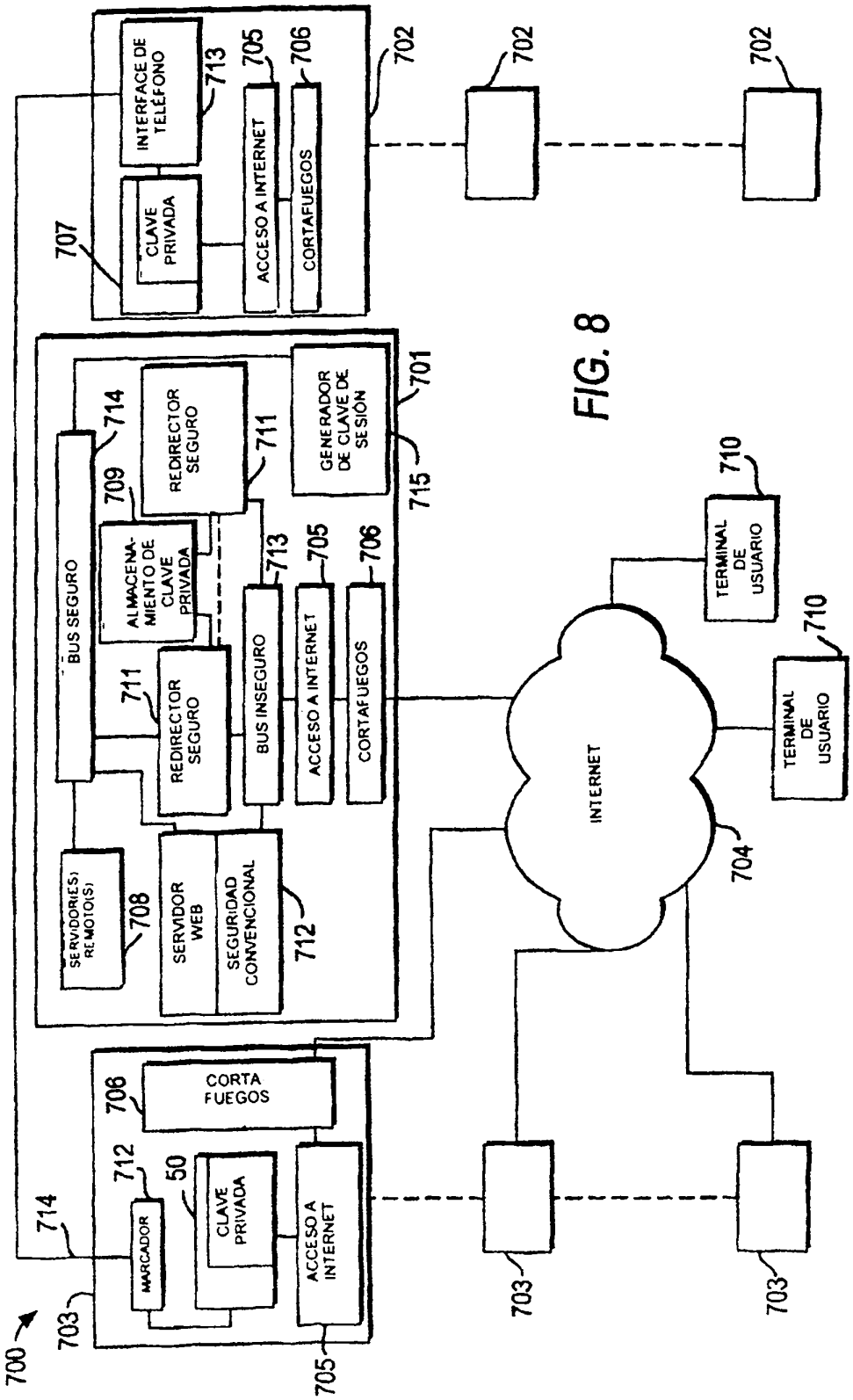
700
703
705
714
712
MARCADOR
50
CLAVE PRIVADA
ACCESO A INTERNET
706
CORTA FUEGOS
708
SERVIDOR(ES) REMOTO(S)
SERVIDOR WEB
SEGURIDAD CONVENCIONAL
712
BUS SEGURO
711
REDIRECTOR SEGURO
709
ALMACENAMIENTO DE CLAVE PRIVADA
713
BUS INSEGURO
705
ACCESO A INTERNET
706
CORTAFUEGOS
714
REDIRECTOR SEGURO
711
GENERADOR DE CLAVE DE SESIÓN
701
715
707
CLAVE PRIVADA
INTERFACE DE TELÉFONO
713
705
ACCESO A INTERNET
706
CORTAFUEGOS
702
702
702
703
703
INTERNET
704
TERMINAL DE USUARIO
710
TERMINAL DE USUARIO
710

FIG. 8