(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 383 146**

(51) Int. CI.:
G07C 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07118296 .8**
(96) Fecha de presentación: **11.10.2007**
(97) Número de publicación de la solicitud: **1912180**
(97) Fecha de publicación de la solicitud: **16.04.2008**

(54) Título: **Método y sistema para controlar un sistema de seguridad utilizando comunicación de campo cercano**

(30) Prioridad:
12.10.2006 US 546865

(45) Fecha de publicación de la mención BOPI:
18.06.2012

(45) Fecha de la publicación del folleto de la patente:
18.06.2012

(73) Titular/es:
Honeywell International Inc.
101 Columbia Road
Morristown, NJ 07960, US

(72) Inventor/es:
Addy, Kenneth L.

(74) Agente/Representante:
Lehmann Novo, Isabel

DESCRIPCIÓN

Método y sistema para controlar un sistema de seguridad utilizando comunicación de campo cercano

Antecedentes de la invención

Campo de la invención

La invención está relacionada en líneas generales con un sistema de seguridad y con sistemas de comunicación. En particular, esta invención está relacionada con el control de un sistema de seguridad utilizando un objeto remoto mediante la transmisión de señales de radiofrecuencia a un dispositivo objetivo, incluyendo el dispositivo objetivo un receptor y un transmisor capaces de recibir y transmitir señales de radiofrecuencia.

Antecedentes

Los sistemas de seguridad son bien conocidos y habituales tanto en entornos residenciales como comerciales en la medida que las personas buscan protegerse a sí mismas y a sus propiedades. Un sistema de seguridad incluye cualquier sistema de protección de la vida, la seguridad y la propiedad. Un equipo de seguridad que incluye un teclado como interfaz de usuario, un panel de control y una pluralidad de sensores se instala en un edificio residencial o comercial. Tanto un instalador como un propietario del equipo de seguridad pueden utilizar el teclado de la interfaz de usuario para controlar, configurar y gestionar el equipo de seguridad. Estas funciones de control incluyen armar el equipo de seguridad al abandonar las instalaciones y desarmar el equipo de seguridad al entrar en las instalaciones.

Un cambio en el estado del equipo de seguridad, por ejemplo armarlo o desarmarlo, se efectúa introduciendo una identificación personal y/o contraseña a través del teclado de la interfaz de usuario pulsando teclas en dicho teclado. A cada persona o personas que tienen autorización o credenciales para cambiar el estado se les asigna una contraseña. La contraseña se puede almacenar en la memoria del teclado de la interfaz de usuario o ser comunicada a un controlador del sistema a través de un bus (línea común de transmisión) por cable o mediante comunicaciones inalámbricas. Si la contraseña introducida coincide con la contraseña almacenada, el teclado transmite el cambio de estado deseado al panel de control utilizando un bus de datos, o la contraseña puede ser transmitida utilizando comunicaciones inalámbricas.

Alternativamente, un usuario puede disponer de un transmisor remoto, proporcionado frecuentemente en un dispositivo con teclas para control remoto o un mando a distancia de bolsillo que el usuario puede llevar en un llavero para cambiar el estado del equipo de seguridad, como, por ejemplo, armar y desarmar el sistema de seguridad. El transmisor puede ser un dispositivo que transmite frecuencias de radio, en cuyo caso el usuario puede encontrarse alejado del dispositivo de la interfaz de usuario, es decir, no en las inmediaciones del lugar en el que se encuentra el teclado de la interfaz. En otra alternativa, el transmisor puede ser un transmisor de infrarrojos. De cualquier modo, tanto al utilizar un teclado inalámbrico como un transmisor, el usuario puede estar obligado a introducir una identificación o una contraseña antes de poder cambiar el estado del equipo de seguridad.

La utilización de una contraseña tiene varios inconvenientes. La contraseña se puede olvidar o perder, creándose un riesgo para la seguridad. Si la contraseña se pierde debe cambiarse inmediatamente el código. Adicionalmente, un equipo de seguridad normalmente sólo proporciona un tiempo reducido para introducir la contraseña para desarmarlo, por lo que el usuario se ve apremiado al introducir la contraseña, lo que origina errores cuando se introduce la contraseña lo que, a su vez, da lugar a falsas alarmas. Por otro lado, la introducción de la contraseña puede resultar difícil para el usuario si está transportando cualquier cosa. Adicionalmente, los transmisores remotos operan en frecuencias VHF y UHF y el alcance operativo es tal que la información transmitida puede ser captada por agentes maliciosos que utilizan dispositivos "interceptadores de códigos".

En consecuencia, existe una necesidad de disponer de un método y un sistema capaces de cambiar el estado del equipo de seguridad de una forma rápida y segura.

El documento WO-A-03/062027 divulga un sistema para acceder a equipos de perforación de rocas en los que cada usuario tiene una categoría de usuario o un ID inalámbrico. El equipo de perforación de rocas está configurado para permitir el acceso a algunas o todas sus funciones en función del ID detectado.

Breve resumen de la invención

La presente invención describe una solución que permite a un usuario cambiar el estado o una función del sistema de seguridad situando un dispositivo portador dotado de un dispositivo de comunicación de campo cercano en las inmediaciones de un dispositivo objetivo dotado de un dispositivo de comunicación de campo cercano. La presente invención aprovecha las características bidireccionales de la comunicación de campo cercano.

Se divulga un sistema de control de un sistema de seguridad que comprende un dispositivo portador que dispone de un dispositivo de comunicación de campo cercano compatible con el estándar ISO/IEC 18092, y un dispositivo objetivo asociado que dispone de un segundo dispositivo de comunicación de campo cercano. Cuando se sitúa el dispositivo portador a menos de una distancia preestablecida del dispositivo objetivo, el dispositivo de comunicación de campo cercano del dispositivo portador modula un campo de radiofrecuencia que incluye información de identificación para el dispositivo de comunicación de campo cercano y credenciales de acceso para el dispositivo objetivo. El dispositivo objetivo determina, utilizando información almacenada en memoria, si el dispositivo portador está autorizado para cambiar el estado del sistema de seguridad, y hace que el estado del sistema de seguridad cambie si el dispositivo portador está autorizado para iniciar el cambio concreto.

El tipo de cambio está determinado por la duración de un período de tiempo en el que el dispositivo portador se encuentra dentro de un alcance preestablecido. El dispositivo portador puede armar o desarmar el sistema de seguridad. Alternativamente, el hecho de situar el dispositivo portador dentro del alcance puede conmutar el estado del sistema de seguridad, es decir, si éste se encuentra armado cambiar su estado a desarmado y viceversa.

El dispositivo portador puede ser cualquier objeto capaz de tener un dispositivo de comunicación de campo cercano integrado en el mismo, tal como un teléfono móvil, una PDA o un mando a distancia de bolsillo. El dispositivo objetivo puede ser un dispositivo de interfaz de usuario o una central de armado y desarmado.

El dispositivo objetivo se encuentra situado cerca de la entrada de una propiedad residencial o comercial. El sistema puede tener múltiples dispositivos objetivo. Si se utilizan múltiples dispositivos objetivo se escoge uno de ellos como dispositivo objetivo principal para asignar las credenciales de acceso y configurar el sistema de control, como, por ejemplo, determinar los umbrales de tiempo, el alcance y las funciones de control, y enviar esta información al dispositivo portador. Los restantes dispositivos objetivo determinarán sobre la base de la información emitida por el dispositivo portador si un cambio solicitado está autorizado.

También se divulga un método para controlar un sistema de seguridad utilizando una señal de comunicación de radiofrecuencia transmitida desde un dispositivo portador. El método incluye detectar una presencia de la señal de comunicación de radiofrecuencia. La señal de comunicación de radiofrecuencia incluye, al menos, una credencial de acceso. El método incluye, además, identificar la credencial de acceso, asociar la credencial de acceso identificada a un usuario autorizado específico entre los que figuran en una lista de usuarios autorizados, detectar un tipo de modificación para una función del sistema de seguridad de acuerdo con un criterio de detección predeterminado, y determinar si el usuario autorizado especificado está autorizado a realizar el tipo de modificación detectada y realizar la modificación.

El método de control comprende, además, convertir dicha credencial de acceso en una contraseña de usuario y transmitir la contraseña de usuario a un panel de control. La credencial de acceso expira tras un período de tiempo preestablecido.

El criterio de detección predeterminado es un umbral de tiempo. El umbral de tiempo es un período de tiempo en el que el dispositivo portador se sitúa dentro del alcance preestablecido de un dispositivo objetivo. El dispositivo portador puede armar o desarmar el sistema de seguridad.

Asimismo se divulga un método para configurar un sistema de seguridad para recibir señales de control remotas desde un dispositivo portador. El método incluye programar una lista de usuarios autorizados, asociar una credencial de acceso a cada uno de los usuarios autorizados, asignar una autoridad de control para cada función para cada uno de los usuarios autorizados, y determinar un criterio de detección para cada función.

El método incluye, además, asignar un plazo de expiración para cada una de las credenciales de acceso.

El método incluye, además, transmitir a un dispositivo portador para su almacenamiento la lista de usuarios autorizados, las credenciales de acceso, la autoridad de control para cada función para cada uno de los usuarios autorizados y el criterio de detección para cada función, cuando el dispositivo portador se sitúa dentro de un alcance preestablecido del dispositivo objetivo. Este alcance preestablecido se puede regular con antelación y, preferiblemente, es de aproximadamente 10 cm.

Breve descripción de los dibujos

Estas y otras características, beneficios y ventajas de la presente invención se harán evidentes mediante referencia al texto y figuras siguientes, a través de las cuales los mismos números de referencia remiten a las mismas estructuras, en donde:

La Figura 1 es un diagrama que muestra una configuración de un sistema de control de acuerdo con la invención;

la Figura 2 es un diagrama de flujo del método de programación del dispositivo objetivo de acuerdo con la invención;

la Figura 3 ilustra un ejemplo de un teclado de interfaz de usuario utilizado para programar el sistema de control de acuerdo con la invención;

las Figuras 4A y 4B ilustran un ejemplo de bases de datos creadas en memoria de acuerdo con la invención;

la Figura 5 es un diagrama de flujo del método de control de acuerdo con un modo de realización de la invención;

la Figura 6 es un diagrama de flujo del método de control de acuerdo con otro modo de realización de la invención;

la Figura 7 es un ejemplo del sistema de control de la invención;

la Figura 8 es un segundo ejemplo del sistema de control de la invención; y

la Figura 9 ilustra una configuración del sistema de control cuando se actualiza una credencial de acceso en un dispositivo portador de acuerdo con la invención.

Descripción detallada de la invención

La Figura 1 ilustra un sistema de control para controlar un estado de un sistema de seguridad de acuerdo con un modo de realización de la invención. Como se ilustra, el sistema de control 1 incluye un dispositivo portador 10 y un dispositivo objetivo 20. El dispositivo portador 10 incluye un dispositivo de comunicación de campo cercano 15. El dispositivo portador 10 puede ser cualquier objeto o dispositivo capaz de tener un dispositivo de comunicación de campo cercano adosado, integrado, instalado o utilizado conjuntamente con un sistema de seguridad local instalado y que sea portátil. Por ejemplo, pero sin limitarse a, una tarjeta de acceso, un teléfono móvil, una PDA, un ordenador portátil, un reloj de pulsera, un lápiz, una pluma y un mando a distancia de bolsillo. El dispositivo objetivo 20 también incluye un dispositivo de comunicación de campo cercano 25. El dispositivo objetivo 20 puede ser un teclado de interfaz de usuario o dispositivo que esté asociado a un panel de control del sistema de seguridad o a una central independiente para armarlo y desarmarlo. Normalmente, el dispositivo objetivo 20 se encontrará situado cerca de una entrada o una puerta para que el usuario pueda armar o desarmar el sistema de seguridad al entrar o salir de la propiedad residencial o comercial.

Los dispositivos de comunicación de campo cercano 15 y 25 se comunican mediante inducción electromagnética utilizando una onda portadora de una única frecuencia. La frecuencia de la onda portadora se encontrará en una banda de frecuencia no regulada de 13,56 MHz.

Los dispositivos de comunicación de campo cercano 15 y 25 se pueden comunicar utilizando un modo activo o pasivo. En el modo pasivo, un dispositivo iniciador proporciona un campo portador y el segundo dispositivo responde modulando el campo existente. El segundo dispositivo se alimenta eléctricamente mediante la radiación del campo portador. En el modo activo, ambos dispositivos se comunican generando sus propios campos portadores e incluyen el suministro eléctrico. En el modo de realización preferido de la invención, el dispositivo de comunicación de campo cercano 15 del dispositivo portador 10 es un dispositivo pasivo. Adicionalmente, los dispositivos de comunicación de campo cercano 15 y 25 pueden transmitir datos a una entre diversas velocidades de transmisión de datos predeterminadas. Las velocidades de transmisión de datos pueden ser 106 kbit/s, 212 kbit/s ó 424 kbit/s. Como la cantidad de datos que hay que comunicar es pequeña, de conformidad con la invención la velocidad de transmisión de datos puede ser de 106 kbit/s, es decir, la velocidad más baja.

Cada dispositivo de comunicación de campo cercano 15 incluye un identificador exclusivo que permite al dispositivo ser identificado de forma única. El identificador exclusivo se almacena en memoria. Cuando un iniciador interroga al dispositivo, el dispositivo de comunicación de campo cercano 15 modula su identificador exclusivo sobre la señal portadora. Esto permite la identificación del dispositivo de comunicación de campo cercano 15 por parte del iniciador cuando un dispositivo portador 10 se sitúa dentro de un alcance preestablecido del dispositivo objetivo 20. El alcance preestablecido se puede regular o modificar reduciendo la potencia de emisión de la señal portadora inicial desde el dispositivo objetivo 20. Adicionalmente, es posible regular el alcance preestablecido mediante la elección del tamaño y del tipo de la antena de transmisión del dispositivo objetivo. En el modo de realización preferido se ajusta la potencia de transmisión y se elige el tipo de antena para determinar que el alcance preestablecido sea muy corto, esto es, de aproximadamente 10 cm.

De acuerdo con la invención, el dispositivo portador 10 pude ser identificado de forma unívoca gracias a su dispositivo de comunicación de campo cercano 15. Mediante esta identificación, se pueden asociar credenciales de acceso específicas, autorizaciones y funcionalidad a un dispositivo portador 10 específico en función del identificador exclusivo de su dispositivo de comunicación de campo cercano 15.

La Figura 2 ilustra un método de configuración para asociar el dispositivo portador 10 con credenciales de acceso, autorizaciones y funcionalidad. La configuración puede ser realizada por un instalador del sistema de seguridad, un propietario del sistema de seguridad o un responsable de seguridad de una empresa comercial (designados de aquí

en adelante como "el usuario").

El usuario puede configurar o programar el sistema de seguridad para que reconozca la actualización del portador utilizando un dispositivo de interfaz de usuario. La Figura 3 ilustra un ejemplo de dispositivo 300 de interfaz de usuario de acuerdo con la invención. El dispositivo 300 de interfaz de usuario puede ser suministrado, por ejemplo, como un periférico del panel de control principal o como un componente del panel de control principal. El dispositivo 300 de interfaz de usuario incluye como componentes un dispositivo de entrada para el usuario, tal como un teclado 310 y/o un micrófono 320 para reconocimiento del habla en un sistema activado mediante la voz, y un dispositivo de salida para el usuario, tal como una pantalla de visualización 330 y/o un altavoz 340. La pantalla de visualización 330 puede ser, por ejemplo, una pantalla de visualización de tipo LCD con capacidad para múltiples líneas y múltiples caracteres. Si el dispositivo 300 de interfaz de usuario es el dispositivo objetivo 20, el dispositivo 300 de interfaz de usuario puede incluir también el dispositivo de comunicación de campo cercano 25.

El usuario deberá pasar a un modo de programación. En el modo de programación, el usuario deberá registrar o introducir en el paso 200 el identificador exclusivo para el dispositivo portador 10 (dispositivo de comunicación de campo cercano). Existen dos opciones para introducir el identificador exclusivo. En un modo de realización, el usuario puede situar el dispositivo portador 10 próximo al dispositivo objetivo 20. El dispositivo de comunicación de campo cercano 25 del dispositivo objetivo 20 recibirá la señal portadora modulada con el identificador exclusivo. El dispositivo de comunicación de campo cercano 25 filtrará la señal portadora y demodulará la señal. Como resultado, el dispositivo de comunicación de campo cercano 25 enviará el identificador exclusivo. En un modo de realización, cuando el dispositivo objetivo es el dispositivo 300 de interfaz de usuario, el dispositivo 300 de interfaz de usuario almacenará directamente el identificador exclusivo desde el dispositivo de comunicación de campo cercano 25. En un modo de realización, cuando el dispositivo objetivo 20 es una central de armado y desarmado, para procesar el acceso se puede enviar el identificador exclusivo al dispositivo 300 de interfaz de usuario, bien a través de comunicación por cable o inalámbrica. El identificador exclusivo se almacena en memoria. El identificador exclusivo puede ser, por ejemplo, el Identificador Internacional de Equipos Móviles (IMEI) utilizado por los teléfonos que cumplen con la norma GSM, o el Identificador de Equipos Móviles (MEID) propio de un teléfono CDMA, que está integrado en un teléfono móvil.

En otro modo de realización, el usuario introducirá manualmente cada dígito del identificador exclusivo. El dispositivo 300 de interfaz de usuario le pedirá al usuario que introduzca cada dígito. A medida que el usuario introduce cada dígito, el dispositivo 300 de interfaz de usuario mostrará dicho dígito en la pantalla de visualización 330 con el fin de que el usuario pueda verificar la información introducida. Una vez introducidos todos los dígitos, el dispositivo 300 de interfaz de usuario le pedirá al usuario que verifique el identificador exclusivo. Después de que el identificador exclusivo haya sido verificado, el identificador exclusivo será almacenado en la memoria. En un modo de realización alternativo, los identificadores exclusivos pueden almacenarse en el panel de control del sistema de seguridad.

A continuación, en el paso 210 el usuario asociará el identificador exclusivo a una persona autorizada y a una contraseña, por ejemplo, a Juana Pérez o al teléfono móvil de Juana Pérez. Esta asociación se utilizará para todas las detecciones subsiguientes del identificador exclusivo con el fin de determinar si el identificador exclusivo corresponde a una persona con autorización para cambiar el estado del sistema de seguridad. El usuario programará un nombre de una persona autorizada. El nombre será almacenado en memoria y se asociará en la memoria con el identificador exclusivo.

En el paso 220, el usuario puede asignar al menos una función que la persona autorizada pueda controlar. Cada persona autorizada puede disponer de diferentes niveles de control o autoridad. Por ejemplo, un responsable de seguridad de un edificio comercial puede tener el nivel de seguridad más alto, es decir, el control total de todas las funciones. Un empleado puede estar autorizado únicamente para armar o desarmar el sistema de seguridad. En el modo de realización preferido, el usuario puede programar cada una de las funciones o características que cualquier persona autorizada puede controlar. En otro modo de realización, el usuario puede programar una función o característica que una persona autorizada no puede controlar. Normalmente, las funciones de control serán desarmar, armar, armar en remoto y máximo retardo en remoto.

En el paso 230 el usuario programará el criterio de detección para cada función de control especificada. En el modo de realización preferido, el criterio de detección es un período de tiempo en el que el dispositivo portador 10 es situado dentro de un alcance preestablecido del dispositivo objetivo 20. En este modo de realización, el usuario programará valores específicos de los umbrales de tiempo para cada función. Por ejemplo, el dispositivo objetivo 20 hará que el sistema de seguridad se arme si el dispositivo portador 10 permanece dentro del alcance preestablecido del dispositivo objetivo 20 entre "0" y "X" segundos. El dispositivo objetivo 20 hará que el sistema de seguridad se arme en remoto si el dispositivo portador 10 permanece dentro del alcance preestablecido del dispositivo objetivo 20 entre "X" e "Y" segundos. El dispositivo objetivo 20 hará que el sistema de seguridad se desarme si el dispositivo portador 10 permanece dentro del alcance preestablecido del dispositivo objetivo 20 entre "Y" y "Z" segundos.

En otro modo de realización, el criterio de detección puede ser un número de veces que el dispositivo portador 10 es introducido dentro del alcance preestablecido de un dispositivo objetivo 20 durante un período de tiempo predefinido. En este modo de realización, el usuario programará un período de tiempo predefinido y unos valores numéricos de umbral para cada función. Por ejemplo, un dispositivo objetivo 20 hará que el sistema de seguridad se arme si el dispositivo portador 10 se mantiene dentro del alcance preestablecido del dispositivo objetivo "A" veces en "N" segundos. El dispositivo objetivo 20 hará que el sistema de seguridad se arme en remoto si el dispositivo portador 10 se mantiene dentro del alcance preestablecido del dispositivo objetivo 20 "B" veces en "n" segundos. El dispositivo objetivo 20 hará que el sistema de seguridad se desarme si el dispositivo portador 10 se mantiene dentro del alcance preestablecido del dispositivo objetivo 20 "C" veces en "N" segundos. Los valores numéricos de umbral y el período de tiempo predefinido se almacenarán en memoria y serán asociados con cada función.

Opcionalmente, en el paso 240, el usuario puede asignar credenciales de acceso que expiran en función de un parámetro predeterminado. Esta posibilidad proporciona diversas ventajas. En primer lugar, si el dispositivo portador se coloca incorrectamente o se pierde, la capacidad de controlar el sistema de seguridad expira y no es indefinida. En segundo lugar, un empresario puede controlar el acceso al sistema de seguridad simplemente mediante la utilización de una credencial de acceso con plazo de expiración. Esto resulta particularmente útil si existe un alto índice de rotación del personal. Asimismo, se puede utilizar esta función para registrar y controlar cuándo sale/entra un empleado de un centro (registrando el número de veces que se arma y desarma el sistema). Adicionalmente, esta función le da al propietario de un sistema de seguridad la oportunidad de permitir un acceso limitado a un sistema de seguridad a invitados, personal de limpieza, técnicos de reparación y a otras personas. En un modo de realización, se puede almacenar en el dispositivo de comunicación de campo cercano 15 una base de datos con las credenciales de acceso existentes. El dispositivo objetivo 20 puede activar periódicamente una de dichas credenciales de acceso de forma aleatoria. Cada credencial de acceso expirará tras un período de tiempo preestablecido.

El parámetro predeterminado puede ser un período de tiempo. Por ejemplo, la credencial de acceso puede expirar diariamente, semanalmente, mensualmente, etc. En el caso de los técnicos de reparación, la credencial de acceso puede ser por horas. Alternativamente, el parámetro predeterminado puede ser el número de veces que se utilice. Por ejemplo, un responsable de seguridad puede programar como parámetro predeterminado el valor 5 para los cinco días laborables de la semana.

También, opcionalmente, el usuario puede programar en el paso 250 los parámetros para determinar si la credencial de acceso se renovará automáticamente o se requerirá una renovación manual de las credenciales de acceso. Por ejemplo, las credenciales de acceso se pueden renovar automáticamente cada lunes.

A pesar de que se ha descrito que la programación del sistema de control 1 tiene lugar en el teclado 300 de la interfaz de usuario, la programación se puede realizar en cualquier dispositivo objetivo 20, como, por ejemplo, una central de armado y desarmado.

Las Figuras 4A y 4B ilustran ejemplos de bases de datos que se crean en memoria de acuerdo con un modo de realización de la invención.

Las dos bases de datos de las Figuras 4A y 4B se utilizarán para controlar al menos una función de los sistemas de seguridad. La base de datos 400 ilustrada en la Figura 4A se utilizará principalmente para determinar la autoridad, el tipo de autoridad y las credenciales de acceso para una persona o un dispositivo portador 10 concretos. La base de datos 420 ilustrada en la Figura 4B se utilizará para determinar la función o el aspecto de control solicitados. Como se muestra en la Figura 4A, la base de datos 400 incluye el identificador exclusivo del dispositivo de comunicación de campo cercano 15, el nombre asociado, la función autorizada y si la credencial de acceso expira (el motivo y en qué momento). La base de datos de la Figura 4B incluye una lista de funciones y el valor de umbral correspondiente.

En otro modo de realización, al menos una parte de las bases de datos 400 y 420 se puede almacenar en el dispositivo de comunicación de campo cercano 15. Cuando el dispositivo de comunicación de campo cercano 15 se encuentre dentro del alcance preestablecido transmitirá al dispositivo objetivo 20 las bases de datos 400 y 420 con la identificación y las credenciales de acceso. Esto tiene la ventaja de que, si el sistema de control incluye múltiples dispositivos objetivo 20, la administración de los derechos de seguridad se puede realizar mediante una comunicación bidireccional, en ambos sentidos, entre el dispositivo de comunicación de campo cercano 15 y un dispositivo objetivo principal.

La Figura 5 ilustra un método de control de acuerdo con un modo de realización de la invención. En este modo de realización, el criterio de detección para una función específica es un período de tiempo durante el cual el dispositivo portador 10 se mantiene dentro del alcance preestablecido del dispositivo objetivo 20.

Inicialmente, el dispositivo objetivo 20 emite en el paso 500 de forma continua una señal portadora utilizando el dispositivo de comunicación de campo cercano 25. En el paso 505, el dispositivo objetivo 20 determina si se

encuentra presente un dispositivo portador 10. Si no hay un dispositivo portador presente, el dispositivo objetivo 20 simplemente emite la señal portadora, es decir, regresa al paso 500. Si hay un dispositivo portador 10 presente dentro del alcance preestablecido, el dispositivo objetivo 20 pone en marcha en el paso 510 un cronómetro que se utiliza para determinar el tiempo durante el cual se mantiene el dispositivo portador 10 dentro del alcance preestablecido. Utilizando el dispositivo de comunicación de campo cercano 25 el dispositivo objetivo 20 determina en el paso 515 el identificador exclusivo para el dispositivo portador 10. El dispositivo de comunicación de campo cercano 25 filtra y modula la señal y genera el identificador exclusivo para el dispositivo portador 10. En el paso 520 se compara este identificador exclusivo contra una lista de identificadores exclusivos almacenada previamente. Si no coincide con ninguno de ellos, en el paso 525 se deniega el acceso de control. En un modo de realización, se puede enviar una notificación de dicha denegación a una central de control remota. Ello informará a la central de control remota de que un usuario no autorizado ha intentado acceder al sistema de seguridad.

Si en el paso 520 se produce una coincidencia, el dispositivo objetivo 20 determinará si el dispositivo portador 10 ha salido fuera del alcance preestablecido. Si ya no se detecta la comunicación desde el dispositivo portador 10, el dispositivo portador 10 se encuentra fuera de la distancia preestablecida. En un modo de realización, el dispositivo objetivo 20 puede indicar que el dispositivo portador 10 se encuentra fuera del alcance para notificárselo a un usuario. Esta indicación puede ser una indicación visual, como, por ejemplo, un destello luminoso, o una indicación audible, como, por ejemplo, un pitido o un sonido.

Si el dispositivo portador 10 se encuentra aún dentro del alcance preestablecido, el dispositivo objetivo 20 esperará hasta que el dispositivo portador 10 se mueva fuera del alcance para determinar la función de control solicitada. Si se determina que el dispositivo portador 10 se ha movido fuera del alcance preestablecido, en el paso 535 el dispositivo objetivo 20 detendrá el cronómetro. El valor indicado por el cronómetro indica el tiempo que el dispositivo portador 10 ha permanecido dentro del alcance preestablecido.

En el paso 540 el dispositivo objetivo 20 determinará la función de control solicitada. El dispositivo objetivo 20 comparará el valor indicado por el cronómetro con un valor umbral del período de tiempo almacenado previamente en memoria, para determinar la función de control solicitada mediante una búsqueda en la base de datos 420. La base de datos 420 contiene todas las funciones posibles en forma de sus valores de umbral correspondientes.

Después de que se haya determinado la función de control solicitada, el dispositivo objetivo 20 determinará en el paso 545 si el usuario autorizado asociado al identificador exclusivo está autorizado para controlar la función de control solicitada. El dispositivo objetivo 20 buscará en la base de datos 400 creada el registro correspondiente al identificador exclusivo y extraerá la función de control asociada. Si ninguna de las funciones de control asociadas coincide con la función de control solicitada, en el paso 525 se denegará el acceso de control. Si coincide una de las funciones de control asociadas que aparecen en la base de datos 400, el dispositivo objetivo 20 permitirá en el paso 550 que el sistema de seguridad sea controlado de la forma solicitada.

Normalmente, el dispositivo objetivo 20 enviará a un panel de control una señal de control correspondiente a través de un bus de datos. El panel de control, en función de la señal de control, ejecutará la función solicitada.

La señal de control es una contraseña exclusiva que se corresponde con el identificador exclusivo. La contraseña puede estar asociada al identificador exclusivo en la base de datos 400. En otras palabras, el dispositivo objetivo 20 convertirá el identificador exclusivo asociado al dispositivo portador 10 en una contraseña que pueda ser reconocida por el panel de control. La Figura 6 ilustra un método de control de acuerdo con otro modo de realización de la invención. En este modo de realización, el criterio de detección para una función específica es el número de veces que el dispositivo portador 10 se mantiene dentro del alcance preestablecido del dispositivo objetivo 20 durante un período de tiempo predefinido.

Inicialmente, en el paso 600, el dispositivo objetivo 20 emite de forma continua una señal portadora utilizando el dispositivo de comunicación de campo cercano 25. En el paso 605, el dispositivo objetivo 20 determina si se encuentra presente un dispositivo portador 10. Si no hay un dispositivo portador presente, el dispositivo objetivo 20 simplemente emite la señal portadora, es decir, regresa al paso 600. Si hay un dispositivo portador 10 presente dentro del alcance preestablecido, utilizando el dispositivo de comunicación de campo cercano 25 el dispositivo objetivo 20 determina en el paso 610 el identificador exclusivo para el dispositivo portador 10. En el paso 615 el dispositivo objetivo 20 determinará mediante la identificación si es la primera vez que el dispositivo portador 10 ha entrado dentro del alcance preestablecido, es decir, si se trata de un nuevo ciclo. Si el dispositivo objetivo 20 determina que la identificación representa el comienzo de un nuevo ciclo, es decir, es la primera vez durante el período de tiempo, el dispositivo objetivo 20 inicializará un contador en el paso 620 asignándole el valor 1 y, en el paso 625, ajustará el cronómetro al período de tiempo predefinido. A continuación, el dispositivo objetivo 20 esperará a que expire el período de tiempo predefinido y, simplemente, emitirá la señal portadora, es decir, regresará al paso 600. Si el dispositivo objetivo 20 determina que la identificación no representa el comienzo de un nuevo ciclo, es decir, es la n-ésima vez durante el período de tiempo predefinido, donde n es mayor que uno, en el

paso 630 el dispositivo objetivo 20 determinará si el período de tiempo predefinido ha expirado. Si el período de tiempo predefinido no ha expirado, el dispositivo objetivo 20 incrementará en el paso 635 en 1 un contador. A continuación, el dispositivo objetivo 20 esperará a que expire el período de tiempo predefinido y, simplemente, emitirá la señal portadora, es decir, regresa al paso 600.

Si el período de tiempo predefinido expira, a continuación el dispositivo objetivo 20 determina en el paso 640 si el identificador exclusivo coincide con algún identificador exclusivo almacenado previamente en la memoria asociado con usuarios autorizados. Si no coincide, en el paso 645 se deniega el acceso de control. En un modo de realización, se puede enviar una notificación de dicha denegación a una central de control remoto. Ello informará a la central de control remoto de que ha intentado acceder al sistema de seguridad alguien que no está autorizado para poder acceder al mismo.

En otro modo de realización, la determinación del paso 640 se realizará antes que la determinación del paso 615.

A continuación, el dispositivo objetivo 20 determinará en el paso 650 la función de control solicitada. El dispositivo objetivo 20 comparará el valor del contador con un valor numérico de umbral almacenado previamente en memoria para determinar la función de control solicitada mediante una búsqueda en la base datos 420.

Después de que se haya determinado la función de control solicitada, el dispositivo objetivo 20 determinará en el paso 655 si el usuario autorizado asociado al identificador exclusivo está autorizado a controla la función de control solicitada. El dispositivo objetivo 20 buscará en la base de datos 400 creada el registro correspondiente al identificador exclusivo y extraerá la(s) función(es) de control asociada(s). Si ninguna de las funciones de control asociadas coincide con la función de control solicitada, en el paso 645 se denegará el acceso de control. Si coincide una de las funciones de control asociadas que aparecen en la base de datos 400, el dispositivo objetivo 20 permitirá en el paso 660 que el sistema de seguridad sea controlado de la forma solicitada.

La Figura 7 ilustra un ejemplo del sistema de control de seguridad de acuerdo con la invención. Como se muestra, el sistema incluye un teclado 600 del sistema de seguridad como dispositivo objetivo 20 y un teléfono móvil 610 con una tarjeta inteligente como dispositivo portador 10. La tarjeta SIM del teléfono móvil se puede utilizar para almacenar diversas informaciones de identificación. Tanto el teléfono móvil 610 como el teclado 600 del sistema de seguridad incluyen dispositivos de comunicación de campo cercano 15 y 25. El sistema también incluye un panel de control 620. El teclado 600 del sistema de seguridad se comunica con el panel de control mediante una conexión por cable o inalámbrica. El teclado 600 del sistema de seguridad se sitúa cerca de la vía o de la puerta de entrada con el fin de que el sistema de seguridad se pueda armar cuando un usuario abandone las instalaciones, y desarmar rápidamente cuando un usuario entre en las mismas.

Cuando el teléfono móvil 610 entra dentro del alcance preestablecido del teclado 600 del sistema de seguridad, se puede utilizar el teléfono móvil 610 para controlar el sistema de seguridad, como, por ejemplo, para armar y desarmar el sistema. Por ejemplo, para desarmar el sistema, se puede situar el teléfono móvil 610 dentro del alcance preestablecido del teclado 600 del sistema de seguridad durante 2 segundos. Para armar el sistema, se puede situar el teléfono móvil 610 dentro del alcance preestablecido del teclado 600 del sistema de seguridad durante 1 segundo.

La Figura 8 ilustra otro ejemplo del sistema de control de seguridad de acuerdo con la invención. Tal como se muestra, el sistema incluye un teclado 600 del sistema de seguridad, una central 700 de armado y desarmado como dispositivo objetivo 20 y un teléfono móvil 610 con una tarjeta inteligente (que incluye el IMEI) como dispositivo portador 10. Tanto el teléfono móvil 610 como la central 700 de armado y desarmado incluyen dispositivos de comunicación de campo cercano 15 y 25. El sistema también incluye un panel de control 620. El teclado 600 del sistema de seguridad y la central 700 de armado y desarmado se comunican con el panel de control mediante una conexión por cable o inalámbrica. La central 700 de armado y desarmado se sitúa cerca de la vía o de la puerta de entrada con el fin de que el sistema de seguridad se pueda armar cuando un usuario abandone las instalaciones, y desarmar rápidamente cuando un usuario entre en las mismas. En este ejemplo, el teclado 600 del sistema de seguridad puede estar situado alejado de la vía o puerta de entrada. Este ejemplo impide o hace difícil el sabotaje en el teclado, puesto que el teclado pude estar oculto.

En este ejemplo, la central 700 de armado y desarmado puede incluir una memoria y un microprocesador para procesar directamente la información recibida desde el teléfono móvil 610. En este ejemplo, en lugar de programar directamente la central 700 de armado y desarmado, es decir, programar el dispositivo objetivo 20 como se describe en la Figura 2, la programación se puede realizar en al teclado 600 del sistema de seguridad. La información programada, como, por ejemplo, identificadores exclusivos, funciones y parámetros de expiración, se puede transmitir a la central 700 de armado y desarmado para su almacenamiento y posterior utilización en el proceso de las señales y la determinación del acceso. Alternativamente, la central 700 de armado y desarmado puede encargarse únicamente de demodular la señal recibida desde el teléfono móvil 610 y transmitir la información al teclado 600 del sistema de seguridad para cualquier determinación de acceso. En el caso de un teléfono móvil 610,

el dispositivo objetivo 20 transforma el ID NFC (por ejemplo, el IMEI), es decir, el identificador exclusivo, en una contraseña o paquete de datos, que se transmite a través del bus del sistema o mediante RF, que es reconocido por el controlador del sistema de seguridad.

Como se ha descrito más arriba, las credenciales de acceso pueden expirar después de un período de tiempo o número de utilizaciones predeterminados. Tras la expiración, la credencial de acceso se puede reactivar o actualizar de forma automática o manual. La credencial de acceso actualizada se puede grabar en la memoria del dispositivo portador 10. La actualización puede consistir simplemente en un bit extra asignado aleatoriamente. La Figura 9 ilustra un ejemplo de transferencia de actualización de acuerdo con un modo de realización de la invención. Según este ejemplo, el teléfono móvil 610 obtendrá la información para la actualización desde el teclado 600 del sistema de seguridad cuando el teléfono móvil 610 se encuentre en las inmediaciones del teclado. El teclado 600 del sistema de seguridad modula la información de actualización sobre la señal portadora. El teléfono móvil 610 recibirá la señal portadora modulada, filtrará y demodulará la señal portadora, y grabará la información de actualización en memoria. Cada vez que se utilice posteriormente el teléfono móvil para controlar el sistema, es decir, que se sitúe el teléfono móvil dentro del alcance preestablecido del teclado, dará lugar a que se transmita al teclado 600 del sistema de seguridad (dispositivo objetivo 20) la modulación de la nueva identificación actualizada. El proceso de actualización se inicia cuando el teléfono móvil 610 entra dentro del alcance preestablecido de un dispositivo objetivo 20 y se determina que la credencial de acceso ha expirado en función de un criterio predefinido, es decir, un período de tiempo o un número de utilizaciones.

La invención se ha descrito en la presente solicitud haciendo referencia a algunos ejemplos de modos de realización. Para aquellos experimentados en la técnica pueden resultar evidentes ciertas alteraciones y modificaciones, sin apartarse del alcance de la invención. Los ejemplos de modos de realización pretenden ser meramente ilustrativos, no limitantes del alcance la invención, que se define en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método para controlar un sistema de seguridad (1) utilizando una señal de comunicación de radiofrecuencia transmitida desde un dispositivo portador (10), que comprende los pasos de:

detectar una presencia de dicha señal de comunicación de radiofrecuencia (paso 505), incluyendo dicha señal de comunicación de radiofrecuencia una credencial de acceso;

determinar dicha credencial de acceso (paso 515);

asociar dicha credencial de acceso determinada con un usuario autorizado específico de una lista de usuarios autorizados (paso 520);

detectar un tipo de modificación para una función de dicho sistema de seguridad en función de un criterio de detección predeterminado (paso 540);

determinar si dicho usuario autorizado especificado está autorizado para realizar dicho tipo de modificación detectada (paso 545); y

realizar dicho tipo de modificación (paso 550), caracterizado por que dicho criterio de detección predeterminado es un umbral de tiempo, siendo dicho umbral de tiempo un período de tiempo donde dicho dispositivo portador es introducido dentro de un alcance preestablecido de un dispositivo objetivo (pasos 510, 530, 535, 540).

2. El método para controlar un sistema de seguridad de acuerdo con la reivindicación 1, en donde dicha credencial de acceso expira después de un período de tiempo preestablecido.

3. El método para controlar un sistema de seguridad de acuerdo con la reivindicación 1, en donde dicho tipo de modificación consiste en armar o desarmar dicho sistema de seguridad.

4. El método para controlar un sistema de seguridad de acuerdo con la reivindicación 1, en donde el paso de realizar dicho tipo de modificación comprende los pasos de:

convertir dicha credencial de acceso en una contraseña de usuario;

transmitir dicha contraseña de usuario a un panel de control.

5. El método para controlar un sistema de seguridad de acuerdo con la reivindicación 1, en donde antes de ejecutar los pasos de la reivindicación 1, el sistema de seguridad se configura para recibir señales de control remotas desde un dispositivo portador mediante:

la programación de una lista de usuarios autorizados (paso 200);

la asociación de una credencial de acceso con cada uno de los usuarios autorizados (paso 210);

la asignación de una autoridad de control para una función para cada uno de dichos usuarios autorizados (paso 220); y

la determinación de un criterio de detección para cada función (paso 230).

6. El método de acuerdo con la reivindicación 5, que comprende, además, el paso de:

asignar un plazo de expiración para cada una de dichas credenciales de acceso (paso 240).

7. El método de acuerdo con la reivindicación 5, que comprende, además, el paso de:

determinar dicho alcance preestablecido.

8. El método de acuerdo con la reivindicación 7, en donde dicho alcance preestablecido es de aproximadamente 10 cm.

9. El método de acuerdo con la reivindicación 6, en donde el método comprende, además, el paso de:

transmitir una credencial de acceso actualizada a dicho dispositivo portador.

10. El método de acuerdo con la reivindicación 5, en donde el paso de programar dicha credencial de acceso comprende el paso de introducir dicho dispositivo portador dentro de un alcance preestablecido de un dispositivo objetivo.

11. El método de acuerdo con la reivindicación 5, que comprende, además, el paso de:

enviar a un dispositivo portador, para ser almacenados, la lista de usuarios autorizados, la credencial de acceso, la autoridad de control para una función para cada uno de dichos usuarios autorizados y el criterio de detección para cada función.

12. El método de acuerdo con la reivindicación 11, en donde el dispositivo portador (10) incluye un dispositivo de comunicación de campo cercano (15) compatible con ISO/IEC 18092.

13. El método de acuerdo con la reivindicación 12, en donde, cuando el dispositivo portador (10) se introduce dentro de un alcance preestablecido de un dispositivo objetivo (20), el dispositivo portador (10) envía a dicho dispositivo objetivo (20), utilizando el dispositivo de comunicación de campo cercano (15), la lista de usuarios autorizados, la credencial de acceso, la autoridad de control para una función para cada uno de dichos usuarios autorizados y el criterio de detección para cada función y el identificador exclusivo.

14. Un sistema de control de un sistema de seguridad (1), que comprende:

un dispositivo portador (10) que dispone de un dispositivo de comunicación de campo cercano (15) compatible con ISO/IEC 18092 asociado a dicho dispositivo portador (10); y

un dispositivo objetivo (20) que dispone de un segundo dispositivo de comunicación de campo cercano (25) asociado a dicho dispositivo objetivo (20);

cuando dicho dispositivo portador (10) se introduce dentro de una distancia preestablecida de dicho dispositivo objetivo (20), dicho dispositivo de comunicación de campo cercano (15) de dicho dispositivo portador (10) transmite un campo de radiofrecuencia que incluye información de identificación acerca de dicho dispositivo de comunicación de campo cercano (15) y credenciales de acceso para controlar dicho sistema de seguridad (1), dicho segundo dispositivo de comunicación de campo cercano (25) de dicho dispositivo objetivo (20) recibe dicho campo de radiofrecuencia y hace que cambie un estado del sistema de seguridad (1) si dicho dispositivo portador (10) está autorizado para iniciar dicho cambio, caracterizado por que un tipo de dicho cambio está determinado por una medición de un período de tiempo en el que dicho dispositivo portador (10) se ha introducido dentro de dicho alcance preestablecido.

15. El sistema de control del sistema de seguridad de la reivindicación 14, en donde dicho dispositivo portador (10) es un teléfono móvil.

16. El sistema de control del sistema de seguridad de la reivindicación 14, en donde dicho dispositivo portador (10) es un mando a distancia de bolsillo.

17. El sistema de control del sistema de seguridad de la reivindicación 14, en donde dicho dispositivo objetivo (20) es un teclado de una interfaz de usuario.

18. El sistema de control del sistema de seguridad de la reivindicación 17, en donde dicho teclado de interfaz de usuario está ubicado próximo a una entrada.

19. El sistema de control del sistema de seguridad de la reivindicación 18, en donde dicho dispositivo objetivo (20) es una central de armado y desarmado ubicada próxima a una entrada.

20. El sistema de control del sistema de seguridad de la reivindicación 14, en donde el sistema comprende, además, una pluralidad de dispositivos objetivo (20), uno de dicha pluralidad de dispositivos objetivo (20) es designado como dispositivo objetivo principal para la asignación de credenciales de acceso y la transmisión a dicho dispositivo portador (10) de las credenciales de acceso y al menos algún otro parámetro, los restantes de dicha pluralidad de dispositivos objetivo hacen que cambie un estado del sistema de seguridad si dicho dispositivo portador (10) está autorizado para iniciar dicho cambio determinado en función de las credenciales de acceso asignadas.

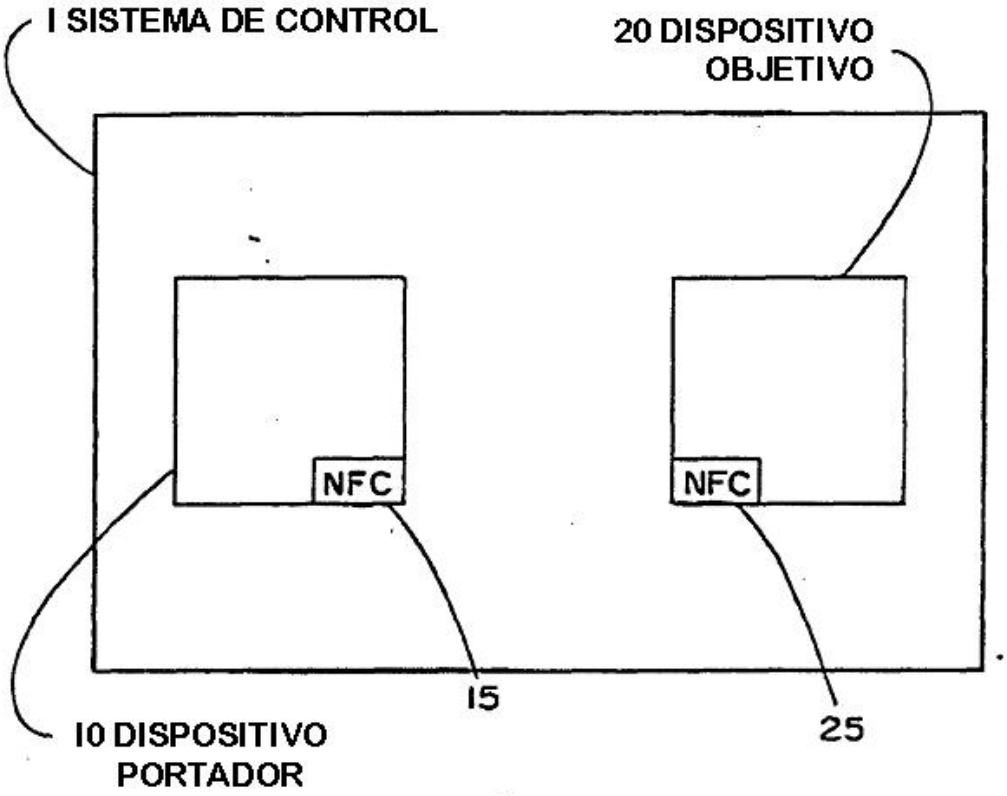
I SISTEMA DE CONTROL
20 DISPOSITIVO OBJETIVO
NFC
NFC
15
25
10 DISPOSITIVO PORTADOR

FIG. 1

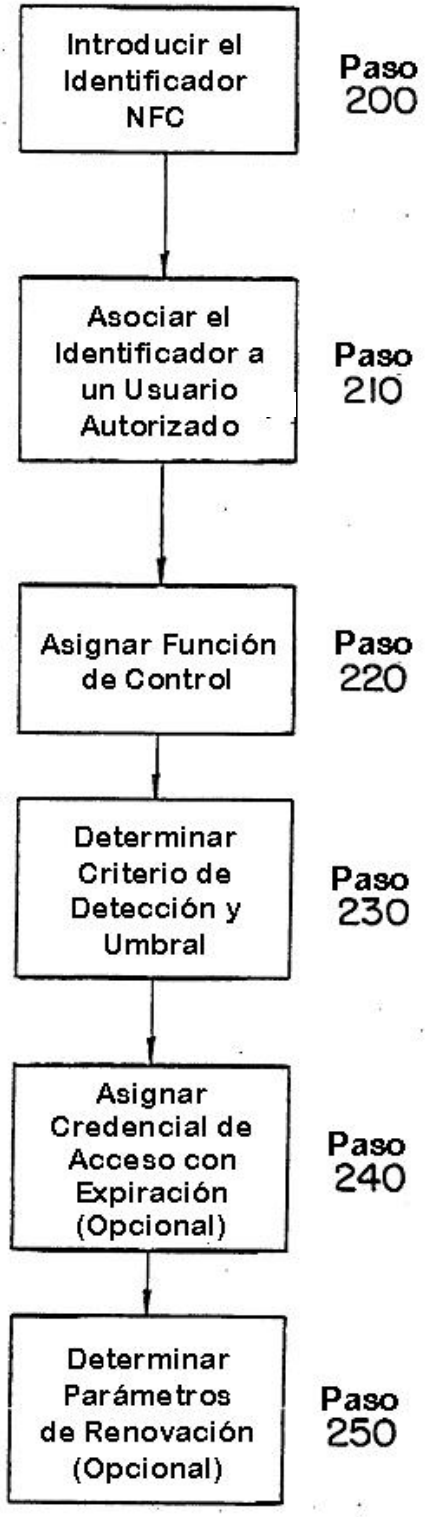
Introducir el Identificador NFC
Paso 200
Asociar el Identificador a un Usuario Autorizado
Paso 210
Asignar Función de Control
Paso 220
Determinar Criterio de Detección y Umbral
Paso 230
Asignar Credencial de Acceso con Expiración (Opcional)
Paso 240
Determinar Parámetros de Renovación (Opcional)
Paso 250

FIG.2

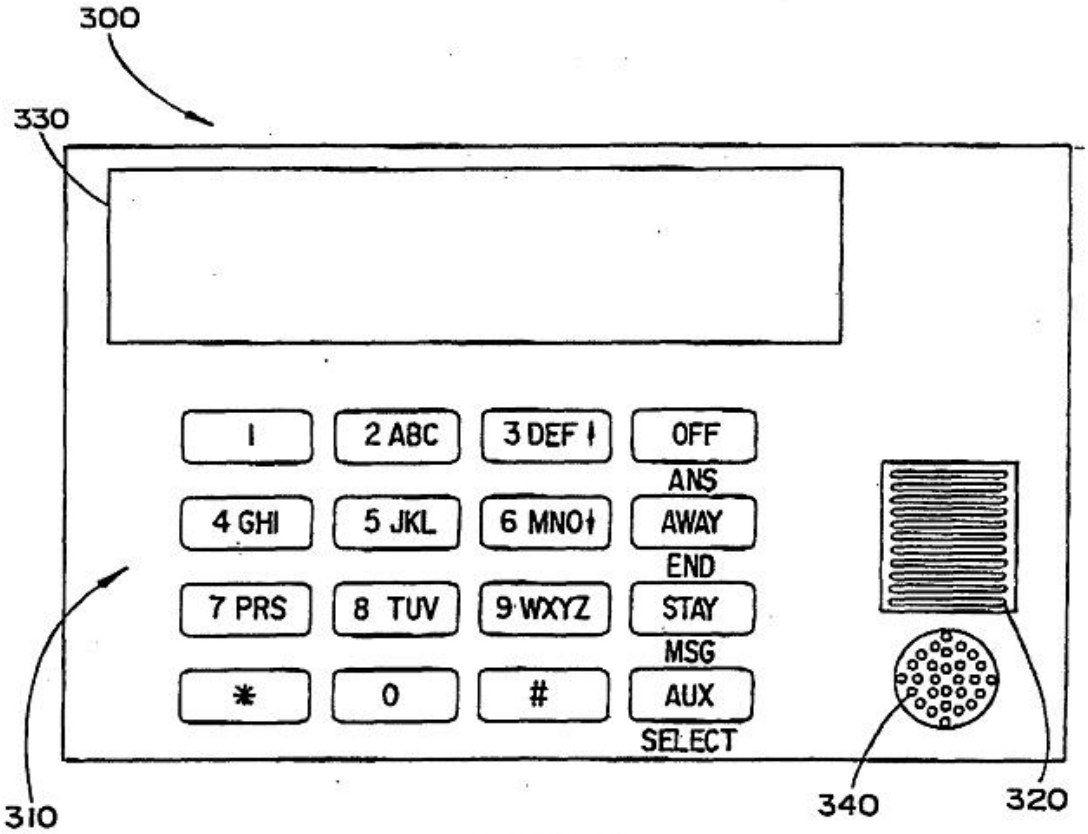
300
330
1
2 ABC
3 DEF
OFF
ANS
4 GHI
5 JKL
6 MNO
AWAY
END
7 PRS
8 TUV
9 WXYZ
STAY
MSG
*
0
#
AUX
SELECT
310
340
320

FIG.3

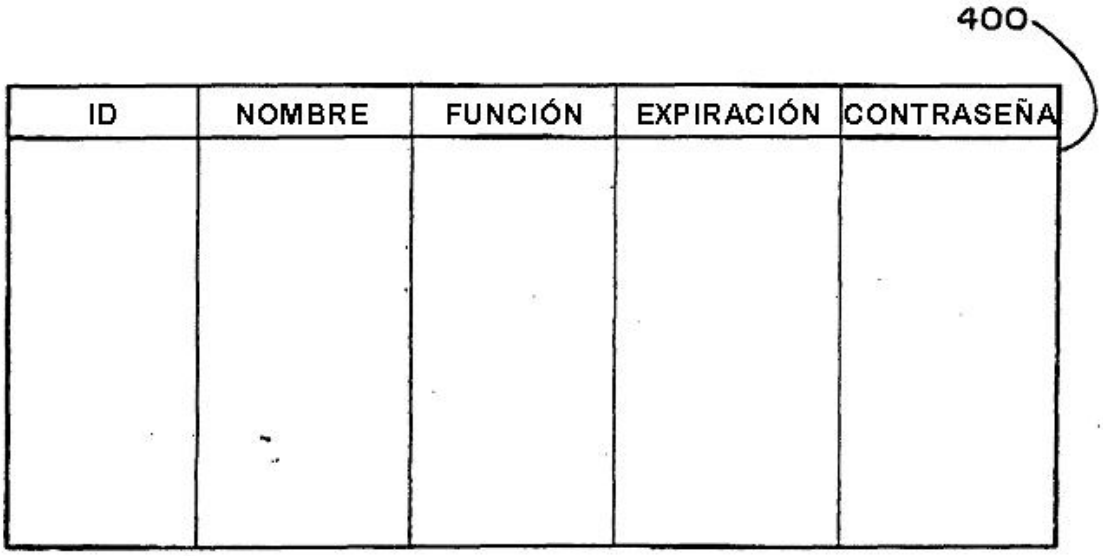
400
ID
NOMBRE
FUNCIÓN
EXPIRACIÓN
CONTRASEÑA

FIG.4A

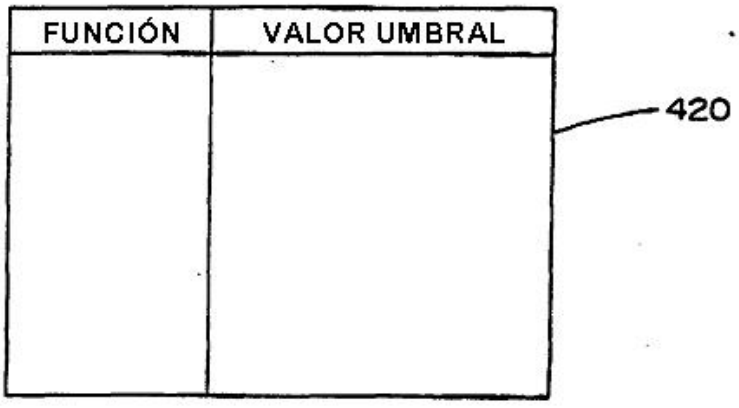
FUNCIÓN
VALOR UMBRAL
420

FIG.4B

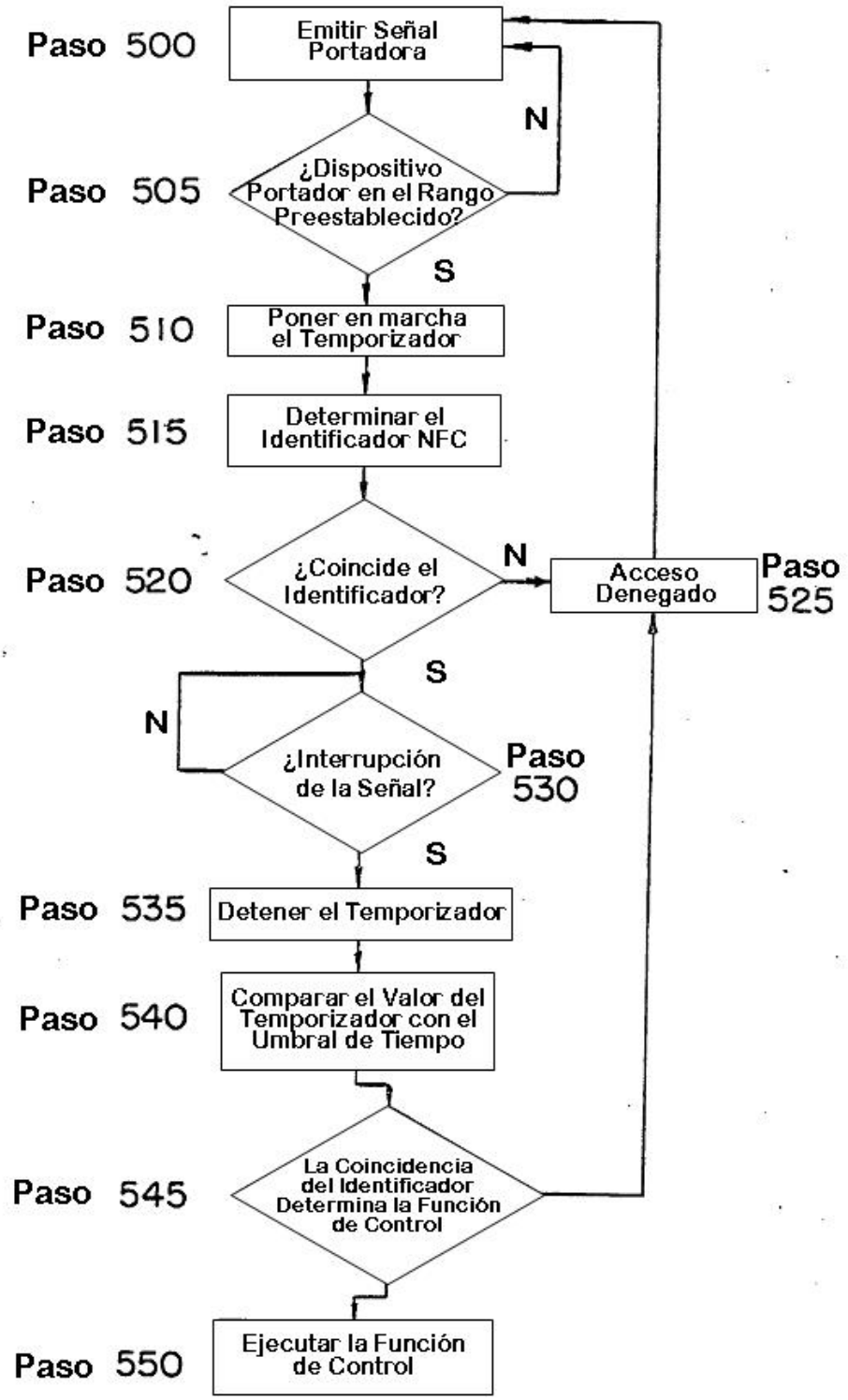
Paso 500
Emitir Señal Portadora
N
Paso 505
¿Dispositivo Portador en el Rango Preestablecido?
S
Paso 510
Poner en marcha el Temporizador
Paso 515
Determinar el Identificador NFC
Paso 520
¿Coincide el Identificador?
N
Acceso Denegado
Paso 525
S
N
¿Interrupción de la Señal?
Paso 530
S
Paso 535
Detener el Temporizador
Paso 540
Comparar el Valor del Temporizador con el Umbral de Tiempo
Paso 545
La Coincidencia del Identificador Determina la Función de Control
Paso 550
Ejecutar la Función de Control

FIG. 5

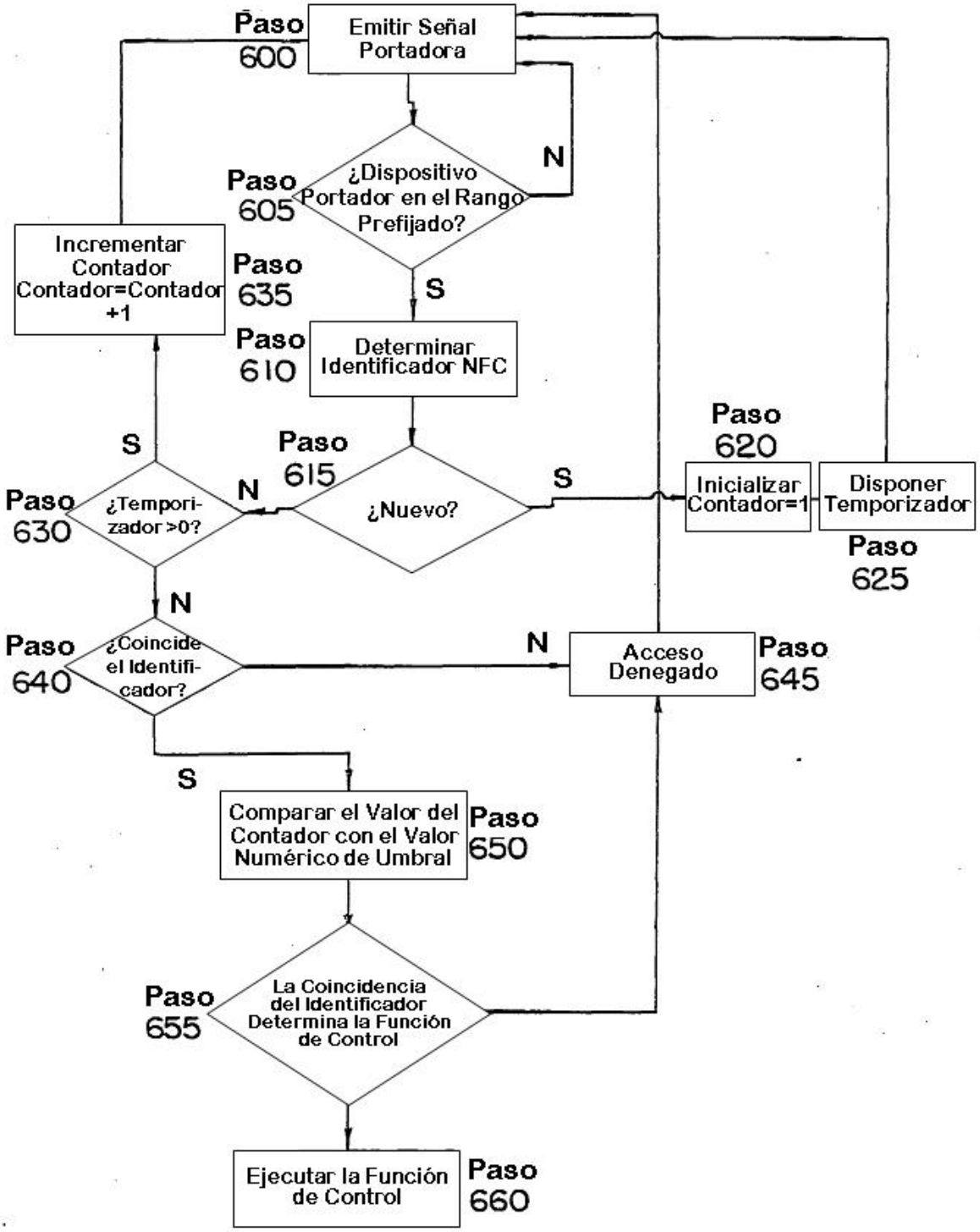
Paso 600
Emitir Señal Portadora
Paso 605
¿Dispositivo Portador en el Rango Prefijado?
N
S
Paso 635
Incrementar Contador Contador=Contador +1
Paso 610
Determinar Identificador NFC
Paso 615
¿Nuevo?
S
N
Paso 620
Inicializar Contador=1
Disponer Temporizador
Paso 625
Paso 630
¿Tempori-zador >0?
S
N
Paso 640
¿Coincide el Identifi-cador?
N
Acceso Denegado
Paso 645
S
Comparar el Valor del Contador con el Valor Numérico de Umbral
Paso 650
Paso 655
La Coincidencia del Identificador Determina la Función de Control
Ejecutar la Función de Control
Paso 660

FIG. 6

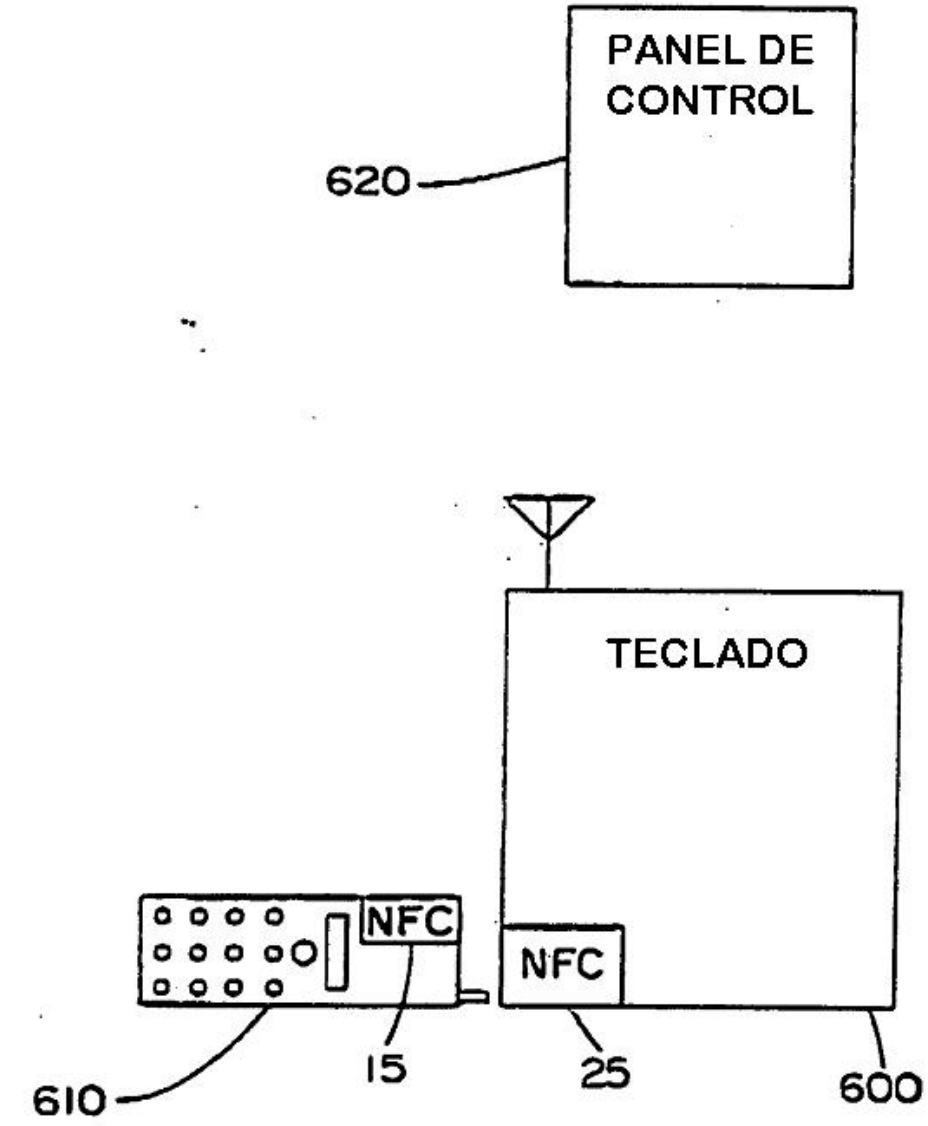

FIG. 7

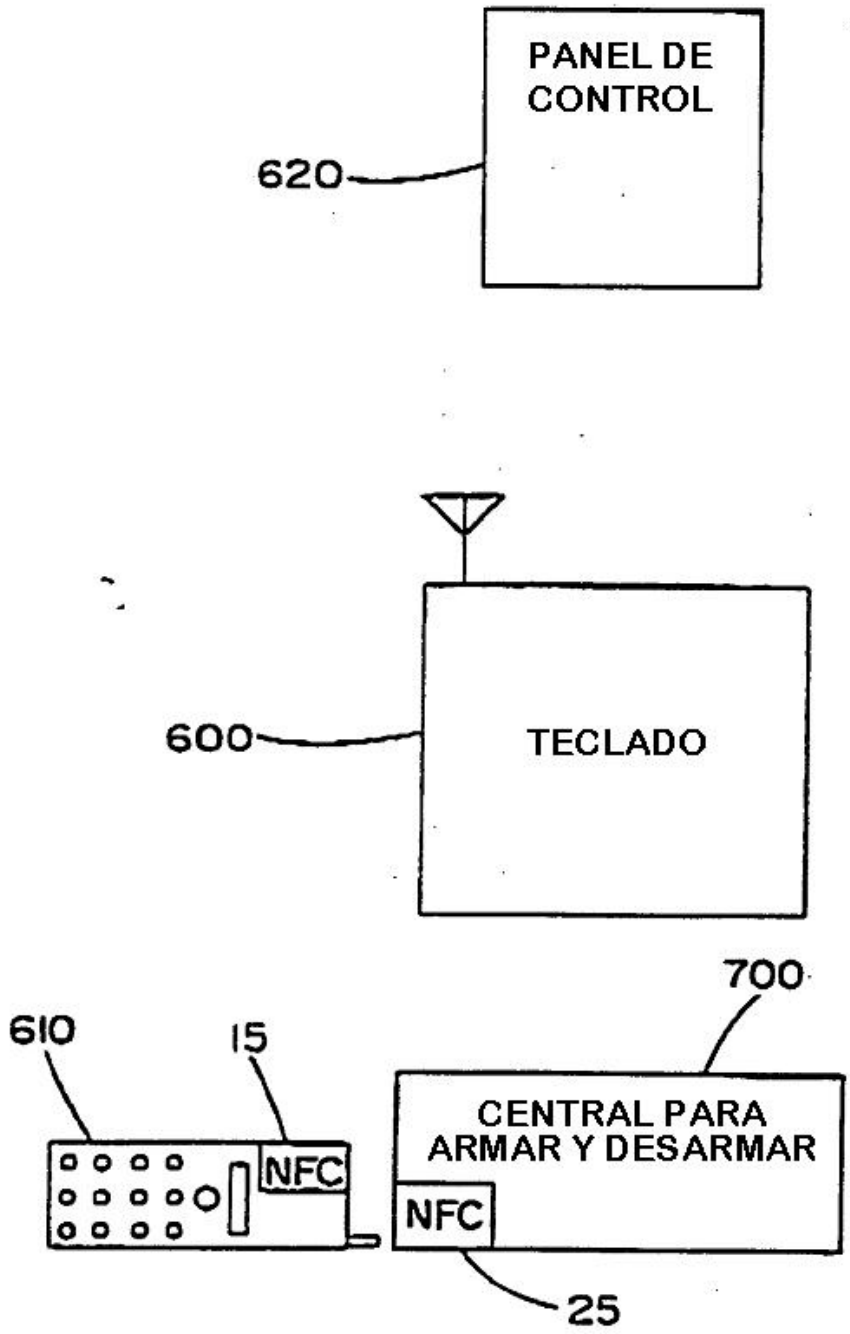
PANEL DE CONTROL
620
600
TECLADO
700
610
15
NFC
CENTRAL PARA ARMAR Y DESARMAR
NFC
25

FIG. 8

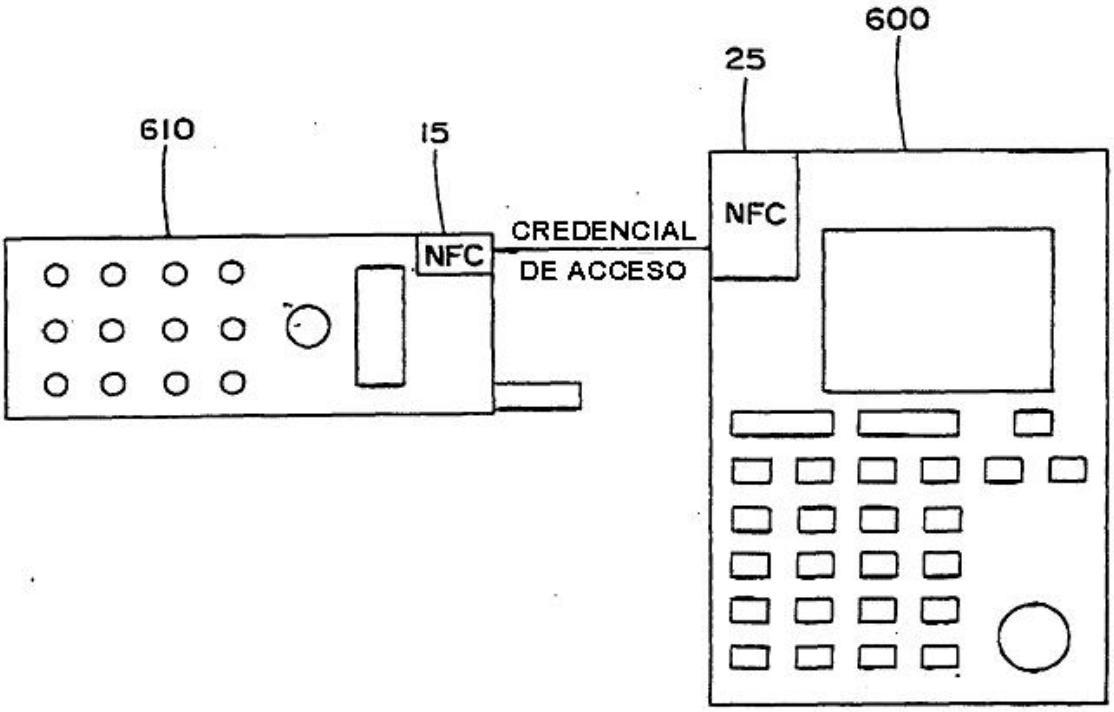

FIG.9