(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 698 060**

(51) Int. CI.:

***H04W 12/12*** (2009.01)
***G06K 7/00*** (2006.01)
***G06K 7/10*** (2006.01)
***G06K 19/073*** (2006.01)
***H04W 4/00*** (2008.01)
***G09F 27/00*** (2006.01)
***H04W 4/80*** (2008.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **14.03.2013 PCT/US2013/031131**

(87) Fecha y número de publicación internacional: **22.05.2014 WO14077882**

(96) Fecha de presentación y número de la solicitud europea: **14.03.2013 E 13712097 (8)**

(97) Fecha y número de publicación de la concesión europea: **05.09.2018 EP 2795950**

(54) Título: **Sistema de seguridad NFC y método para deshabilitar etiquetas no autorizadas**

(30) Prioridad:

**19.11.2012 US 201261727907 P**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**30.01.2019**

(73) Titular/es:

**AVERY DENNISON CORPORATION (100.0%)**
**207 Goode Avenue, Suite 500**
**Glendale, CA 91203, US**

(72) Inventor/es:

**FORSTER, IAN J.**

(74) Agente/Representante:

**ELZABURU, S.L.P**

## DESCRIPCIÓN

Sistema de seguridad NFC y método para deshabilitar etiquetas no autorizadas

**Referencia cruzada a solicitud relacionada**

La presente solicitud reivindica la prioridad de la solicitud de patente provisional de los EE.UU. No. 61/727.907 presentada el 19 de noviembre de 2012.

**Antecedentes de la invención**

El documento WO 2011/094384 A1 describe un sistema publicitario y un método para usarlo. El sistema de publicidad incluye una fuente de luz que puede ser activada por dispositivos de comunicación de campo cercano para extraer información del sistema.

El documento XP031408012 describe la importancia del paradigma de seguridad de detección de intrusos de los sistemas de RFID. Se presenta una descripción general del estado de la técnica en seguridad de RFID y se investigan las limitaciones de las soluciones de seguridad tradicionales en base a conceptos fundamentales y protocolos criptográficos. Se propone un modelo de detección de intrusos mediante RFID que integra información de la capa de lector de RFID y capa de middleware para detectar el comportamiento anómalo en la red, mejorando así su resistencia a los ataques de seguridad.

Los dispositivos de identificación por radiofrecuencia (RFID), incluidos los dispositivos de RFID habilitados para comunicación de campo cercano (NFC), se utilizan para una variedad de propósitos. A menudo, tales dispositivos se forman como etiquetas o marbetes y se pueden utilizar para asociar un objeto con un código de identificación u otros datos, como los datos del sitio web. Dichos dispositivos de RFID pueden ser pasivos y, al recibir una señal, tal como una señal de excitación de un lector de RFID o habilitado para NFC, pueden ser activados. Los dispositivos pueden responder entonces con una comunicación deseada o proporcionar información asociada con un producto, artículo o servicio asociado con el dispositivo de RFID.

Específicamente, NFC es un protocolo de intercambio de datos diseñado para permitir que los dispositivos, incluidos los teléfonos móviles adecuadamente equipados y similares, interactúen con infraestructuras, como terminales de punto de venta y despacho de entradas en sistemas de transporte, o dispositivos de RFID en forma de "carteles inteligentes" o "puntos de contacto", por ejemplo. En tales situaciones, llevar un dispositivo habilitado para NFC a la proximidad de dicha infraestructura o dispositivos de RFID puede provocar la transmisión de datos al dispositivo habilitado para NFC, lo que da como resultado, por ejemplo, la apertura de una página web, la aceptación de un flujo de medios a través de Bluetooth o cualquiera de una serie de otras funciones.

A menudo, la forma de asociar un producto, artículo o servicio con un dispositivo de RFID es acoplar o adherir físicamente el dispositivo de RFID al producto o artículo, o asociarlo con publicidad relacionada con el producto, artículo o servicio, como el "póster inteligente" o "punto de contacto" descrito anteriormente. Por ejemplo, los marbetes de RFID se pueden acoplar adhesivamente a los objetos o pueden tener superficies que se adhieren directamente a los objetos. Las etiquetas de RFID se pueden asegurar al objeto de otras maneras, como mediante el uso de un sujetador de plástico, cuerda u otro mecanismo de sujeción. Dichos dispositivos de RFID pueden proporcionar datos a los dispositivos habilitados para NFC ubicados o colocados cerca de los dispositivos de RFID.

Además, los dispositivos de RFID a menudo están asociados con el producto o artículo, o elemento publicitario, de tal manera que ocultan o aseguran el dispositivo de RFID. Dichos métodos pueden proporcionar seguridad contra la eliminación o el uso indebido de un dispositivo de RFID. Sin embargo, en tales circunstancias, y particularmente con dispositivos habilitados para NFC diseñados para transmitir información a los consumidores con dispositivos y teléfonos móviles habilitados para NFC, hay un área designada (punto de contacto) en un anuncio o producto que indica que se puede obtener información si el dispositivo habilitado para NFC se coloca muy cerca de un área asociada con el dispositivo de RFID. Sin embargo, como se sabe entonces que la información puede obtenerse de tales áreas, los dispositivos de RFID vándalos o piratas a menudo se colocan muy cerca del área de NFC indicada. Los dispositivos vándalos o piratas a menudo contienen información falaz, engañosa, no deseada o maliciosa. Estos dispositivos se pueden acoplar o adherir a productos y artículos, o anuncios asociados con esos artículos, lo que lleva a que la información inapropiada o maliciosa se comunique sin saberlo al dispositivo habilitado para NFC de un usuario.

En funcionamiento normal, los teléfonos móviles que tienen habilitadas las funciones de NFC operan en modo de lectura/escritura de NFC. En este modo, el teléfono móvil transmite una consulta a la etiqueta de NFC que consiste en impulsos de campo magnético modulados a una frecuencia de portadora de 13,56 MHz. El lector de NFC en el teléfono móvil no tiene indicación previa de que una etiqueta de NFC esté próxima al teléfono hasta que una etiqueta de NFC responda a una consulta. Por lo tanto, un lector de NFC externo, tal como un teléfono móvil, transmitirá sistemáticamente consultas de interrogación de NFC hasta que se detecte una etiqueta de NFC.

**Compendio**

Los sistemas, aparatos y métodos de circuitos de detectores de NFC pueden proporcionar la detección de la colocación próxima de un lector de NFC externo a una ubicación específica en una superficie de visualización. La superficie de visualización puede estar destinada a visualizar indicios y permitir la interacción con un dispositivo de comunicación NFC integrado en la pantalla.

En una realización de ejemplo, un circuito puede controlar un sistema de seguridad de NFC que escanea etiquetas no autorizadas fijadas a la superficie de una pantalla. El sistema de seguridad de NFC puede ser activado por un teléfono móvil habilitado para NFC colocado cerca de la región indicada para recibir un mensaje codificado con NFC desde la pantalla. Se puede realizar una exploración de seguridad de NFC antes de que el teléfono móvil lea el mensaje de la etiqueta de NFC prevista en la pantalla.

Otras realizaciones de ejemplo pueden incluir habilitar modos de visualización interactivos, por ejemplo, para realizar selecciones indicadas en la pantalla o detectar gestos de movimiento a través de la cara de la pantalla. Dicha interacción puede ser útil para configurar los contenidos de la etiqueta de NFC en función de una interacción específica del usuario.

**Breve descripción de los dibujos**

Las ventajas de las realizaciones de la presente invención serán evidentes a partir de la siguiente descripción detallada de las realizaciones de ejemplo. La siguiente descripción detallada debe considerarse junto con las figuras adjuntas, en las que:

La figura 1 es una vista esquemática de una realización de ejemplo de un circuito de detector para NFC.

La figura 2 es una vista esquemática de una realización de ejemplo de un detector de NFC, para controlar la iluminación de Diodos Emisores de Luz (LED) integrados en una zona de lectura de NFC.

La figura 3 es una vista esquemática de una realización a modo de ejemplo de una NFC para activar un sistema de seguridad de NFC cuando un lector de NFC externo se coloca cerca de una zona de lectura de NFC que contiene una etiqueta de NFC.

La figura 4 es una vista esquemática de una realización de ejemplo de un detector de NFC para activar el sistema de seguridad de NFC cuando se coloca un lector de NFC externo cerca de una bobina inductiva.

La figura 5 es una vista esquemática de una realización a modo de ejemplo de un detector de NFC que incorpora un circuito contador que registra el número de ocasiones en que se coloca un lector de NFC externo cerca de una bobina inductiva receptora de un detector de NFC.

La figura 6 es un diagrama de flujo a modo de ejemplo que muestra un orden de operaciones para un sistema de seguridad de NFC.

**Descripción detallada**

La invención se define en las reivindicaciones independientes de la invención y se divulga en la siguiente descripción y en los dibujos relacionados dirigidos a realizaciones específicas de la invención. Se pueden idear realizaciones alternativas sin apartarse del alcance de la invención. Adicionalmente, los elementos bien conocidos de las realizaciones de la invención a modo de ejemplo no se describirán en detalle o se omitirán a fin de no ocultar los detalles relevantes de la invención. Además, para facilitar la comprensión de la descripción, sigue la explicación de varios términos utilizados en este documento.

Como se usa en el presente documento, la expresión "a modo de ejemplo " significa "que sirve como ejemplo, caso o ilustración". Las realizaciones descritas en este documento no son limitantes, sino que sólo son ejemplares. Debe entenderse que las realizaciones descritas no deben interpretarse necesariamente como preferidas o ventajosas sobre otras realizaciones. Además, las expresiones "realizaciones de la invención", "realizaciones" o "invención" no requieren que todas las realizaciones de la invención incluyan la característica, la ventaja o el modo de operación explicados.

En general, refiriéndose a las Figs. 1-6, realizaciones de ejemplo descritas en este documento pueden describir sistemas de seguridad de NFC, a veces denominados sistemas de Perro Vigilante (Watch Dog) de NFC. En algunas realizaciones a modo de ejemplo, las consultas transmitidas por el lector de NFC externo en modo lector / escritor pueden usarse para detectar cuándo está colocado un teléfono móvil cerca de una ubicación específica en una superficie de visualización usando circuitos de detector de NFC.

Un sistema de seguridad de NFC a modo de ejemplo puede incluir un lector de NFC, un controlador de seguridad y una bobina inductiva con circuitos de adaptación de impedancia. Las funciones de un sistema de seguridad de NFC pueden ser detectar etiquetas no autorizadas, desactivar dichas etiquetas y alertar al personal de mantenimiento sobre un problema.

La detección de etiquetas no autorizadas se puede lograr mediante un componente del lector de NFC que transmite comandos de interrogación de NFC a una bobina inductiva. La bobina inductiva puede distribuir energía magnética sobre la superficie de la pantalla que está siendo interrogada para detectar etiquetas no autorizadas. Un controlador de seguridad de un sistema de seguridad de NFC de ejemplo puede no realizar interrogaciones de manera constante, de modo que puede no interferir con un canal de comunicación de un lector de NFC externo y un dispositivo de NFC tal como una etiqueta de NFC. El controlador de seguridad puede activar la lectura a intervalos regulares o condicionalmente en el estado de una línea de señal, tal como desde otro controlador o sensor. El detector de NFC se puede configurar para enviar una señal al sistema de seguridad de NFC cuando está colocado un teléfono cerca de una ubicación específica en la superficie de una pantalla.

Realizaciones a modo de ejemplo pueden requerir un diseño de circuito menos complejo que otras soluciones que utilizan un circuito lector de NFC. En algunas realizaciones a modo de ejemplo, los elementos principales del circuito de detector de NFC pueden incluir una bobina receptora inductiva, un desmodulador de RF y un detector de umbral. El circuito del detector de NFC puede no descodificar la señal de datos de un lector de NFC externo para detectar su ubicación próxima en una superficie de visualización. Además, el detector de NFC puede estar diseñado solo para recibir señales de RF y puede no transmitir señales de RF, a diferencia de un lector de NFC. Como tal, se pueden integrar múltiples detectores de NFC en un sistema de visualización sin interferir con un canal de comunicación de un lector de NFC externo o un dispositivo de comunicación NFC previsto, como una etiqueta de NFC.

En una realización a modo de ejemplo, una pantalla puede incluir dos o más detectores de NFC colocados separados sobre la superficie de visualización, de modo que los usuarios pueden indicar las elecciones usando la colocación del teléfono móvil basándose en indicaciones de visualización. Por ejemplo, si un usuario de la pantalla coloca un lector externo tal como un teléfono móvil directamente sobre uno de los detectores de NFC, entonces la pantalla puede indicar la selección del usuario, como la información de salida. En el mismo ejemplo, un teléfono móvil colocado sobre otro detector de NFC puede indicar que se desea información de llegada. Una vez que el usuario ha realizado una selección, la memoria de etiquetas de NFC puede formatearse con el mensaje de NDEF apropiado, que en este ejemplo puede incluir un enlace a la información de llegada o salida.

En otra realización a modo de ejemplo, una pantalla puede incluir múltiples detectores de NFC incrustados sobre una superficie. El sistema de visualización puede detectar cuándo el usuario mueve el teléfono móvil a lo largo de una ruta reconocida por el sistema de visualización, lo que puede denominarse un gesto, tal como, por ejemplo, siguiendo una ruta circular a lo largo de indicaciones de visualización. Cuando el sistema de visualización reconoce un gesto, se puede preparar un mensaje de NFC personalizado para el usuario, que puede ser leído por el teléfono móvil habilitado para NFC.

Algunas realizaciones a modo de ejemplo pueden reducir el consumo de potencia en sistemas que utilizan el detector de NFC para controlar el estado activo de transceptores de NFC, tales como los lectores de NFC y los dispositivos de NFC en modo “de igual a igual”. Es posible que un lector de NFC utilizado en el sistema de seguridad de NFC desee transmitir suficiente potencia para interrogar etiquetas no autorizadas que podrían fijarse a la pantalla. La potencia para la función de interrogación puede ser de hasta 4 vatios, dependiendo del intervalo de operación deseado y del tamaño de la bobina de NFC transmisora. Utilizar un detector de NFC para controlar el estado activo de un lector de NFC puede reducir el consumo de energía, por ejemplo, limitando las funciones de interrogación a las condiciones necesarias, tal como cuando un lector de NFC externo se acerca a la pantalla.

Además, la utilización del detector de NFC para un menor consumo de energía puede permitir que un sistema de visualización funcione con energía de la batería en lugar de una conexión a la red eléctrica. En una realización a modo de ejemplo, el sistema de visualización puede usar una batería como potencia de apoyo para situaciones en las que se ha interrumpido la alimentación de la red.

En otra realización de ejemplo, el detector de NFC puede controlar los modos de funcionamiento de un lector de NFC de igual a igual, que puede funcionar para transmitir mensajes de NFC a través del Protocolo de Intercambio de NDEF Simple (SNEP) al lector NFC externo. En esta realización de ejemplo, el sistema de visualización puede funcionar con baterías, lo que puede requerir que el lector de igual a igual se active solo cuando está presente un lector de NFC externo.

Con referencia ahora al ejemplo de la Fig. 1, se puede mostrar una vista esquemática de una realización de ejemplo de un circuito de detector de NFC. Los elementos del detector pueden incluir una bobina receptora 102 inductiva de campo cercano con un elemento 104 de adaptación de impedancia, un desmodulador 106 y un detector de umbral 108.

La bobina receptora inductiva 102 puede incluir un inductor distribuido adaptado para ser receptivo a campos magnéticos alternos en las proximidades de la bobina. El condensador 104 puede formar un circuito de adaptación de impedancia entre la bobina receptora inductiva 102 y una línea de transmisión 110, tal como, por ejemplo, una línea de transmisión de 50 ohmios.

El circuito de adaptación de impedancia puede estar adaptado para permitir una transmisión de baja pérdida de energía de señal entre la bobina receptora inductiva 102 y la línea de transmisión 110, que puede estar conectada a

otros circuitos del detector de NFC.

El condensador 104 de la Fig. 1 es sólo una realización de ejemplo de un circuito de adaptación de impedancia; pueden existir otras configuraciones de circuito que pueden, por ejemplo, aumentar el ancho de banda a través de la banda de frecuencia, pero requieren el uso de una circuitería más compleja para implementar el circuito de adaptación de impedancia. Dichos circuitos de adaptación de impedancia pueden incluir cualquier circuito de adaptación de impedancia conocido en la técnica.

En esta realización de ejemplo, cuando un lector de NFC externo está próximo al detector de NFC, el circuito desmodulador 106 puede recibir una señal de RF por la línea de transmisión 110 para la recuperación de la señal de datos original sin una onda portadora de RF. El desmodulador 106 en la Fig. 1 puede ser un detector de envolvente de diodo, usado, por ejemplo, debido a un circuito relativamente simple y un bajo consumo de potencia. Sin embargo, si se desea una mejor discriminación de señal o filtrado de entrada, cualquier otro circuito desmodulador conocido en la técnica puede implementarse con el compromiso de diseño asociado en la complejidad del circuito y el consumo de potencia. La señal de salida del desmodulador 106 puede incluir impulsos de tensión continua 116 que pueden desplazarse a través de la línea de transmisión 112 al circuito detector de umbral 108.

El circuito del detector de umbral 108 puede conducir una señal de salida de dos estados, normalmente en el estado "deshabilitado", al estado "habilitado" cuando la tensión de salida del desmodulador excede el punto de voltaje "habilitado" o de umbral alto. La separación de los niveles de umbral alto y bajo del detector de umbral 108 puede formar una función de histéresis, de modo que el estado de salida "habilitado" no pueda restablecerse al estado "deshabilitado" hasta que el voltaje de entrada sea inferior al punto de voltaje de umbral "desactivado". Como tal, el estado de salida del detector de umbral puede no oscilar si el voltaje de entrada oscila alrededor de cualquier punto de umbral de voltaje. El detector de umbral 108 del ejemplo de la Fig. 1 puede ser un circuito disparador Schmitt de baja potencia. El circuito disparador Schmitt se puede utilizar, ya que es un circuito bien documentado comúnmente utilizado en muchas aplicaciones de circuitos; por lo tanto, el diseño e implementación de un disparador Schmitt no se describe en detalle aquí. Sin embargo, se pueden implementar otros detectores de umbral conocidos en la técnica, según se desee. La salida del detector de umbral 108 puede conducir la señal de salida de dos estados a través de la línea de transmisión 114 a circuitos de salida digital para el sistema huésped 118. La salida digital 118 al sistema huésped puede implementarse con circuitos necesarios para amortiguar o bloquear el estado de salida del detector de NFC para uso inmediato o posterior por los circuitos de entrada del sistema huésped.

La Fig. 2 es una vista esquemática de una realización de ejemplo de un detector de NFC que puede controlar la iluminación de los Diodos Emisores de Luz (LED) integrados en una zona de lectura de NFC. El circuito puede estar adaptado para indicar al usuario que el dispositivo de NFC externo se ha colocado en una región adecuada o deseada para leer la etiqueta de NFC deseada. El elemento inductivo del detector de NFC y los LED se pueden ubicar cerca de la zona de lectura de NFC. Otros elementos del circuito pueden no tener una ubicación crítica con respecto a la superficie de la pantalla y pueden colocarse donde mejor se adapte o desee. El detector de NFC 202 en el circuito de ejemplo puede conducir el voltaje de la línea de control 220 al valor de estado "habilitado" cuando un lector de NFC externo está próximo al detector de NFC, o al valor de estado "desactivado" cuando no hay un lector NFC externo está cerca del detector. El circuito impulsor de LED 204 puede ajustar la fuente de tensión y corriente en la línea 222 con relación al suelo 210 a la condición apropiada para iluminar los LED 206 y 208 dentro de la pantalla ubicada cerca de la zona de lectura de NFC.

La Fig. 3 es una vista esquemática de una realización de ejemplo de un detector de NFC que puede activar un sistema de seguridad de NFC cuando un lector de NFC externo, tal como un teléfono móvil, se coloca cerca de una zona de lectura de NFC que contiene una etiqueta de NFC. El circuito del detector de NFC 302 puede activar la línea 310 con un nivel de voltaje de salida que significa el estado "habilitado" del sistema de seguridad 304. Al detectar el voltaje de estado "habilitado" en la línea 310 de control de activación, el sistema de seguridad puede realizar un comando de inventario de NFC con un lector de NFC interno. El lector de NFC interno puede transmitir comandos de protocolo de aire de NFC a través del cable 312 a la red de adaptación 308 y luego a la bobina de transmisión 306. Si el sistema de seguridad descubre una etiqueta no autorizada, se pueden tomar las acciones apropiadas, como, por ejemplo, deshabilitar la etiqueta o enviar una petición de ayuda al personal de mantenimiento. Cuando se completa la función de seguridad de NFC, el sistema puede pasar al modo de suspensión para un mínimo consumo de energía. Posteriormente, el circuito del detector de NFC puede permanecer inactivo durante un tiempo específico, para permitir que el lector de NFC externo transfiera el contenido de la etiqueta de NFC autorizada sin interferencia del sistema de seguridad de NFC.

La Fig. 4 es una vista esquemática de una realización de ejemplo de un detector de NFC que puede activar el sistema de seguridad de NFC cuando un lector de NFC externo, tal como un teléfono móvil, se coloca cerca de una bobina inductiva común 408. La bobina inductiva puede incluir un elemento común tanto para el detector como para el sistema de seguridad. El uso de una bobina común puede ser tal que cada circuito establezca una conexión exclusiva al cable 412 que se conecta a la bobina común 408. Se puede usar un estado de "detección" y un estado de "seguridad" para seleccionar una conexión a una bobina de NFC común 408. El estado inicial y nominal del sistema puede ser el estado de "detección". Cuando el sistema de visualización está en el estado de "detección", el circuito detector de NFC puede tener control de prioridad de la bobina de NFC común 408, mientras que el sistema de seguridad puede desconectarse de la bobina común 408 y configurarse para un modo de reposo de baja energía.

El detector de NFC puede vigilar continuamente las señales de un lector de NFC externo, como un teléfono móvil. Al detectar una señal de un lector externo, el sistema puede pasar al estado de "seguridad". En el estado de "seguridad", el detector de NFC puede desconectarse de la bobina de NFC común 408 al poner en circuito abierto la conexión al cable 412. El detector de NFC puede entonces conducir el voltaje de la línea de activación 406 al estado "habilitado". El sistema de seguridad puede detectar el estado "habilitado" de la línea de activación 406 y puede pasar al estado de "seguridad". Tras la transición al estado de "seguridad", el sistema de seguridad puede conectar la bobina de NFC común 408 conmutando la conexión de circuito del sistema al cable 412 desde un circuito abierto a un cortocircuito. El sistema de seguridad puede emitir entonces comandos de inventario de NFC a la bobina común 408 para verificar si hay etiquetas no autorizadas adheridas a la pantalla. Si están fijadas etiquetas no autorizadas a la pantalla, el sistema de seguridad puede realizar acciones tales como intentar deshabilitar la etiqueta no autorizada o realizar una petición para que el personal de mantenimiento elimine la etiqueta no autorizada. Una vez completada la operación de seguridad, el sistema de seguridad puede abrir la conexión del circuito al cable 412, puede indicar al detector de NFC que el modo de seguridad está completo, y luego puede pasar al estado operativo de baja potencia. El estado del sistema puede ser devuelto a un modo de "detección". Al pasar del estado de "seguridad" al estado de "detección", el circuito del detector de NFC puede permanecer inactivo durante un tiempo específico para permitir que el lector de NFC externo transfiera el contenido de la etiqueta de NFC autorizada sin interferencia del sistema de seguridad de NFC.

La Fig. 5 es una vista esquemática de una realización de ejemplo de un detector de NFC 502 que puede incorporar un circuito contador 504 que puede registrar el número de casos en que un lector de NFC externo, tal como un teléfono móvil, se coloca cerca de una bobina inductiva receptora de un detector de NFC. El valor almacenado del circuito contador puede usarse, por ejemplo, para determinar medidas para la efectividad de la pantalla. La línea de señal 510 puede encaminarse a otras funciones 506 que detectan el estado de la señal de salida del detector de NFC. Las otras funciones 506 pueden incluir, por ejemplo, un sistema de seguridad de NFC o un sistema de visualización interactivo como se describió anteriormente.

La Fig. 6 es un diagrama de flujo de ejemplo que describe aspectos del sistema de seguridad de NFC. En esta realización de ejemplo, el tiempo 602 puede representar cualquier momento después de implementar y/o activar un sistema de seguridad de NFC. El sistema puede incluir sensores 604 que funcionan para detectar cualquier señal de NFC indeseada o maliciosa. Por lo tanto, si los sensores 604 están activos y no detectan ninguna señal maliciosa, el sistema puede pasar al modo de reposo 606. Si los sensores 604 están activos y detectan una señal maliciosa, se puede tomar una acción de respuesta deseada 610. La acción de respuesta puede incluir el bloqueo de la señal maliciosa o la destrucción del dispositivo malicioso. Si la acción 610 es exitosa, el sistema puede regresar al modo de reposo 606. Si la acción no tiene éxito, el sistema puede tratar de tomar la acción 610 deseada de nuevo, o se puede enviar una señal al personal apropiado. Como se puede apreciar por lo anterior, también se puede utilizar cualquier otro curso de acción que use otros componentes.

La descripción anterior y las figuras adjuntas ilustran los principios, realizaciones preferidas y modos de operación de la invención. Sin embargo, no debe interpretarse que la invención está limitada a las realizaciones particulares descritas anteriormente. Los expertos en la técnica apreciarán variaciones adicionales de las realizaciones explicadas anteriormente.

Por lo tanto, las realizaciones descritas anteriormente deben considerarse como ilustrativas en lugar de restrictivas. Por consiguiente, debe apreciarse que los expertos en la técnica pueden realizar variaciones en esas realizaciones sin apartarse del alcance de la invención como se define en las siguientes reivindicaciones.

**REIVINDICACIONES**

1. Una pantalla publicitaria que comprende un sistema de seguridad de NFC, que comprende, además:

un controlador de seguridad del sistema de seguridad de NFC; al menos un detector de NFC (202) colocado en una parte de una superficie de la pantalla;

al menos una etiqueta de NFC auténtica;

un lector interno de NFC del sistema de seguridad de NFC, interno a la pantalla publicitaria, colocado cerca del al menos un detector de NFC (202) para formar una zona de lectura de NFC;

una bobina inductiva del sistema de seguridad de NFC (408), distribuyendo la bobina inductiva (408) una energía magnética sobre una superficie de la pantalla; y en la que el detector de NFC está configurado para activar el sistema de seguridad de NFC, enviando una señal al sistema de seguridad de NFC, cuando un lector de NFC externo, exterior a la pantalla publicitaria, está colocado cerca de la pantalla publicitaria para leer al menos una etiqueta de NFC de la presentación publicitaria; y en la que el lector de NFC interno, tras la activación, está configurado para detectar una etiqueta de NFC no autorizada aplicada a la pantalla publicitaria y para crear una señal con la bobina inductiva (408) para desactivar la etiqueta de NFC no autorizada.

2. El sistema según la reivindicación 1, en el que el sistema de seguridad de NFC está adaptado adicionalmente para generar una alerta al detectar las etiquetas no autorizadas.

3. El sistema según la reivindicación 1, en el que la bobina inductiva (408) está configurada para conectarse y desconectarse al y del al menos un detector de NFC (202).

4. Un método para implementar un sistema de seguridad de NFC (304) que comprende:

proporcionar una pantalla de publicidad que presenta un sistema de seguridad de NFC (304) que tiene un controlador de seguridad, un lector interno de NFC, interior a la pantalla publicitaria, una bobina inductiva (408), y teniendo pantalla publicitaria al menos un detector de NFC; tras colocar un lector de NFC externo, exterior a la pantalla publicitaria, cerca de la pantalla publicitaria para leer al menos una etiqueta de NFC de la pantalla publicitaria, activar el sistema de seguridad de NFC mediante el detector de NFC, enviando, mediante el detector de NFC, una señal al sistema de seguridad de NFC; detectar una señal maliciosa de al menos una etiqueta de NFC no autorizada de la pantalla publicitaria por el lector interno de NFC al activarse; y

determinar una acción (610) por el sistema de seguridad de NFC para desactivar al menos una etiqueta de NFC no autorizada.

5. El método según la reivindicación 4, en el que la acción (610) genera una alarma para eliminar la etiqueta de NFC no autorizada.

6. El método según la reivindicación 5, cuyo método comprende además bloquear la señal maliciosa de la etiqueta de NFC no autorizada después de la etapa de detección.

7. El método según la reivindicación 5, cuyo método comprende además destruir un dispositivo malicioso después de la etapa de determinación.

8. El método según la reivindicación 5, cuyo método comprende la etapa adicional de fracasar en la detección de al menos una señal maliciosa, de manera que el sistema de seguridad de NFC entra en un modo de reposo (606).

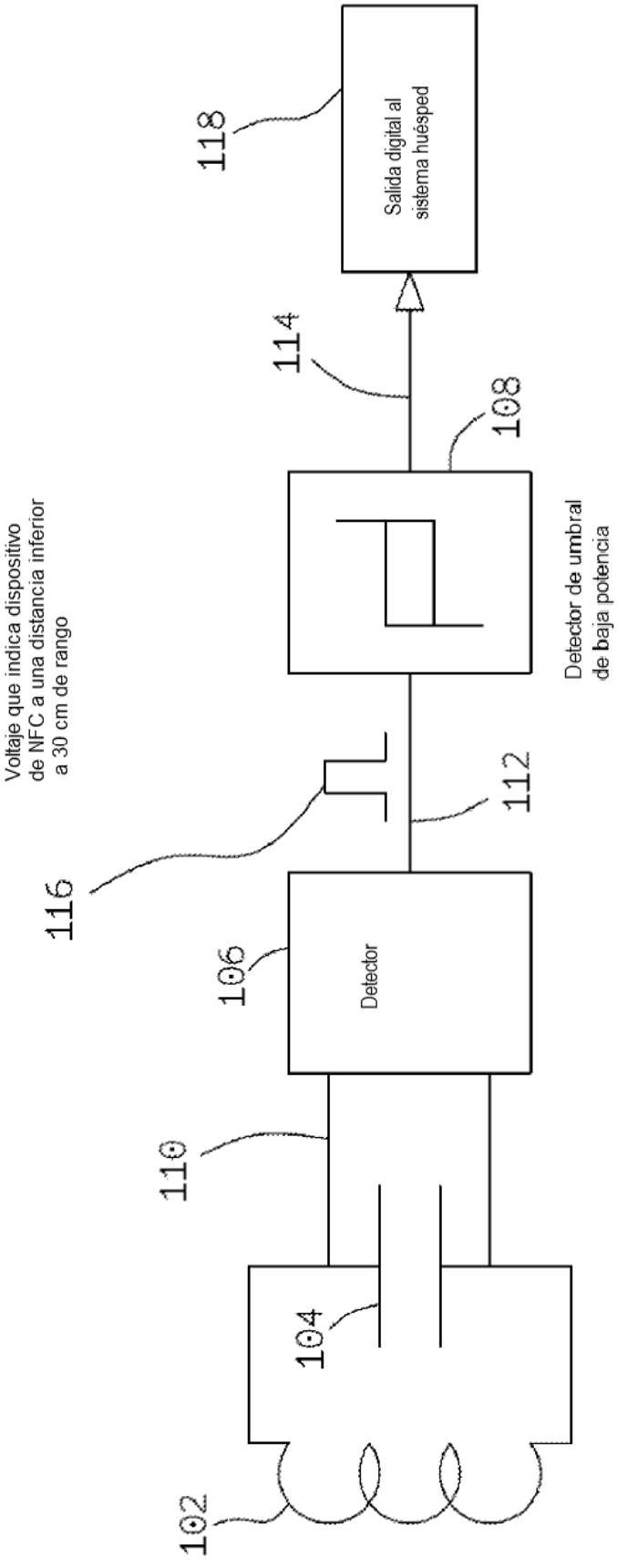
118
Salida digital al sistema huésped
114
108
Detector de umbral de baja potencia
Voltaje que indica dispositivo de NFC a una distancia inferior a 30 cm de rango
116
112
106
Detector
110
104
102

*Fig. 1*

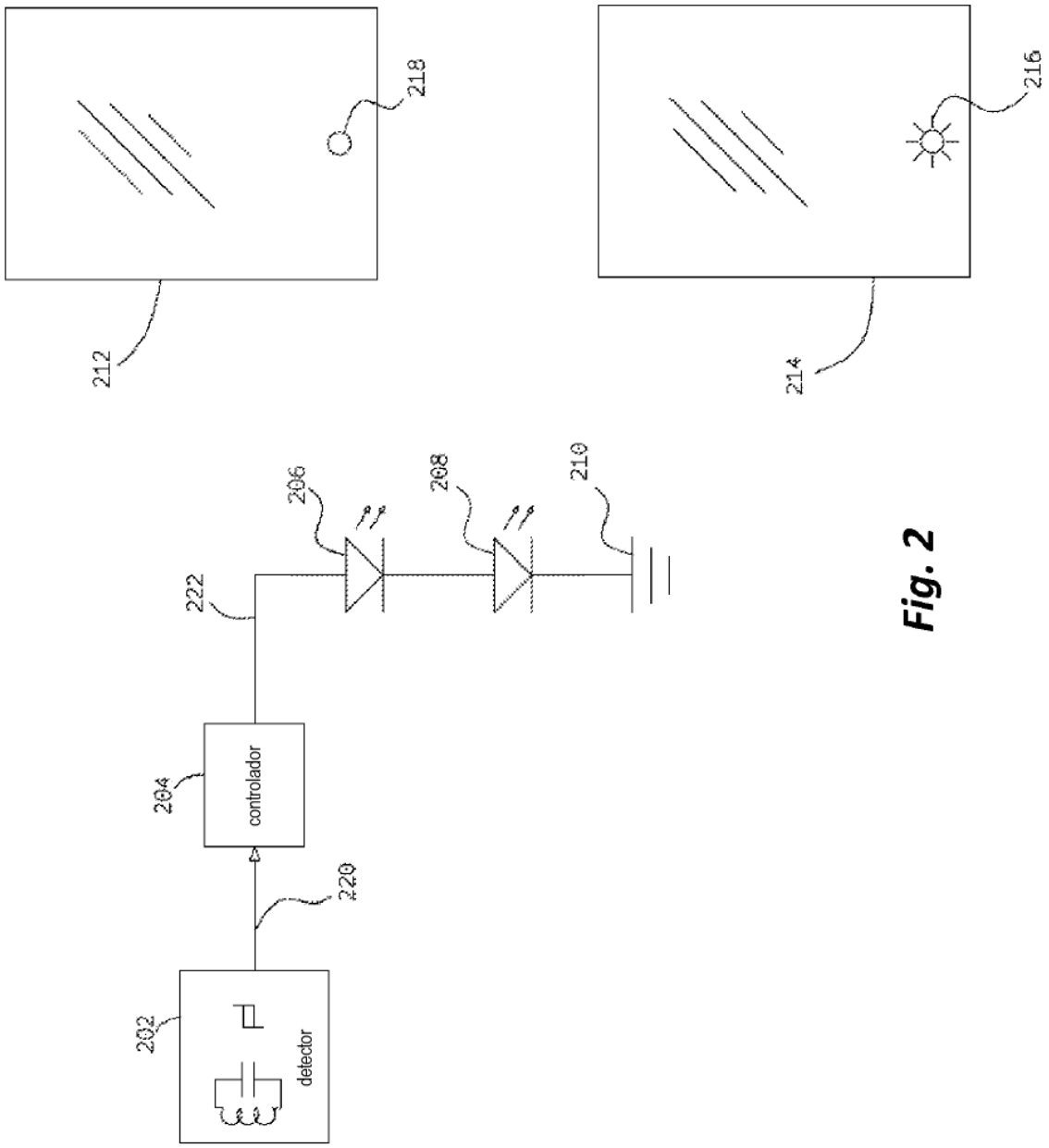
218
216
212
214
206
208
210
222
204
controlador
220
202
detector

Fig. 2

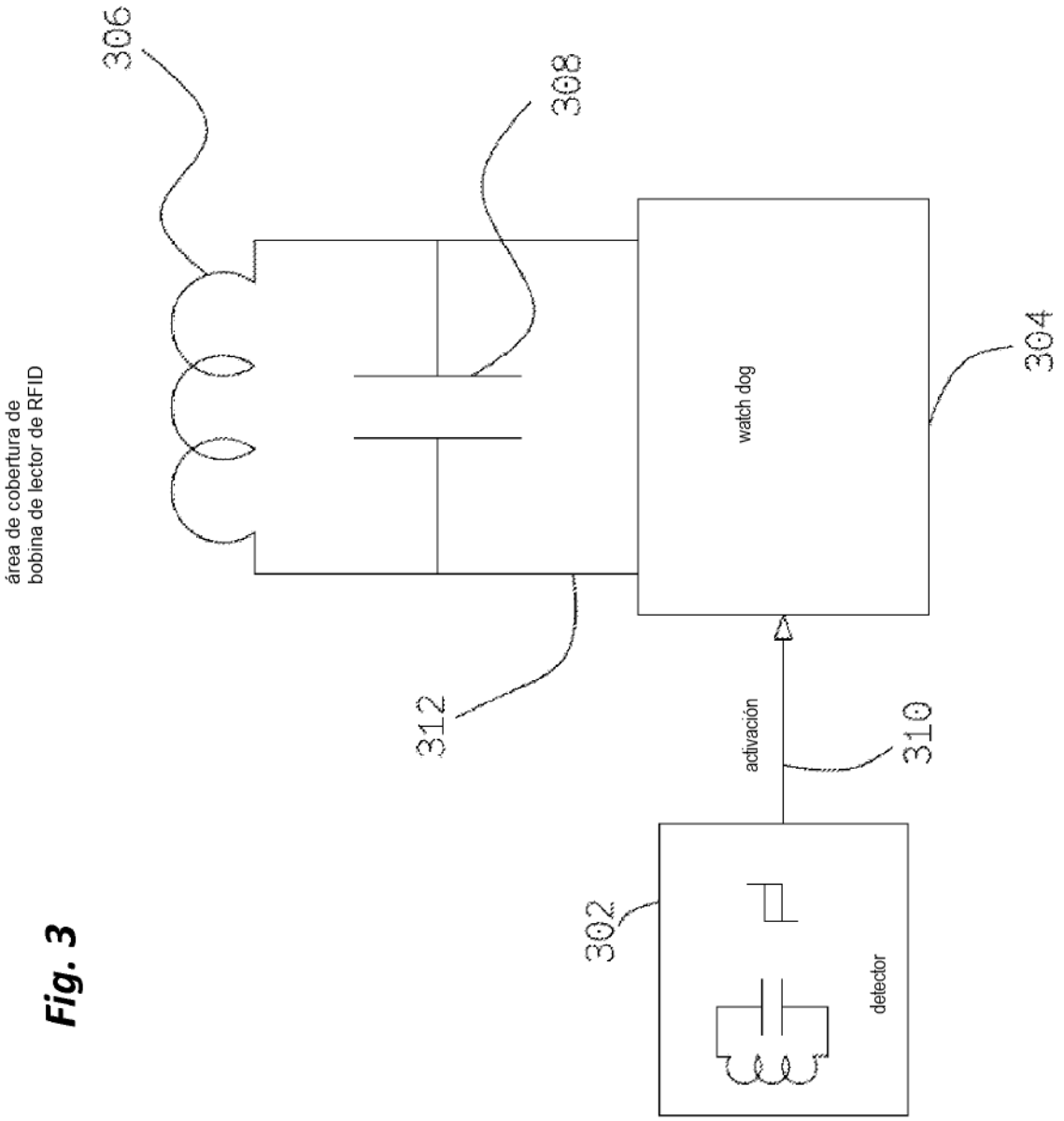
306
308
304
watch dog
312
activación
310
302
detector
área de cobertura de
bobina de lector de RFID

*Fig. 3*

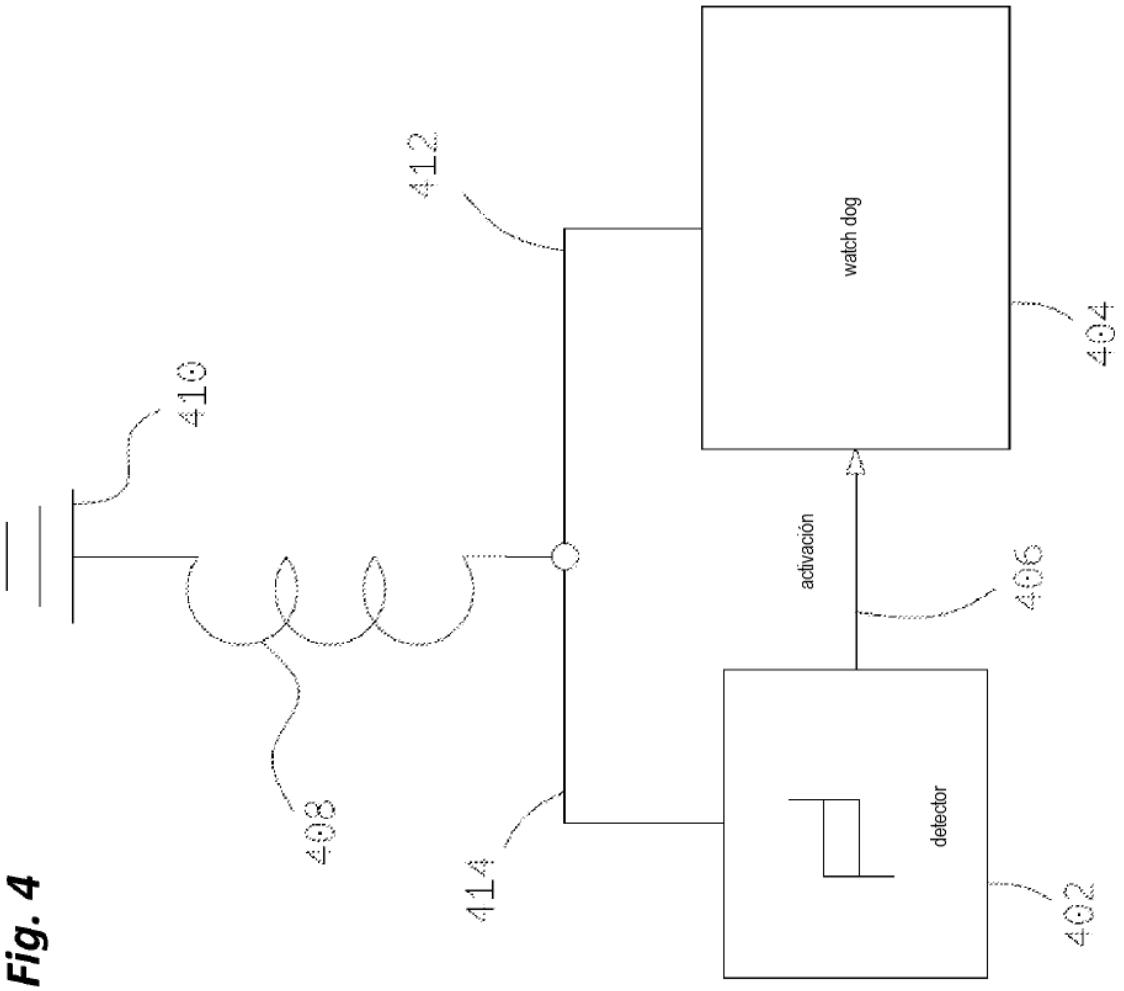


Fig. 4

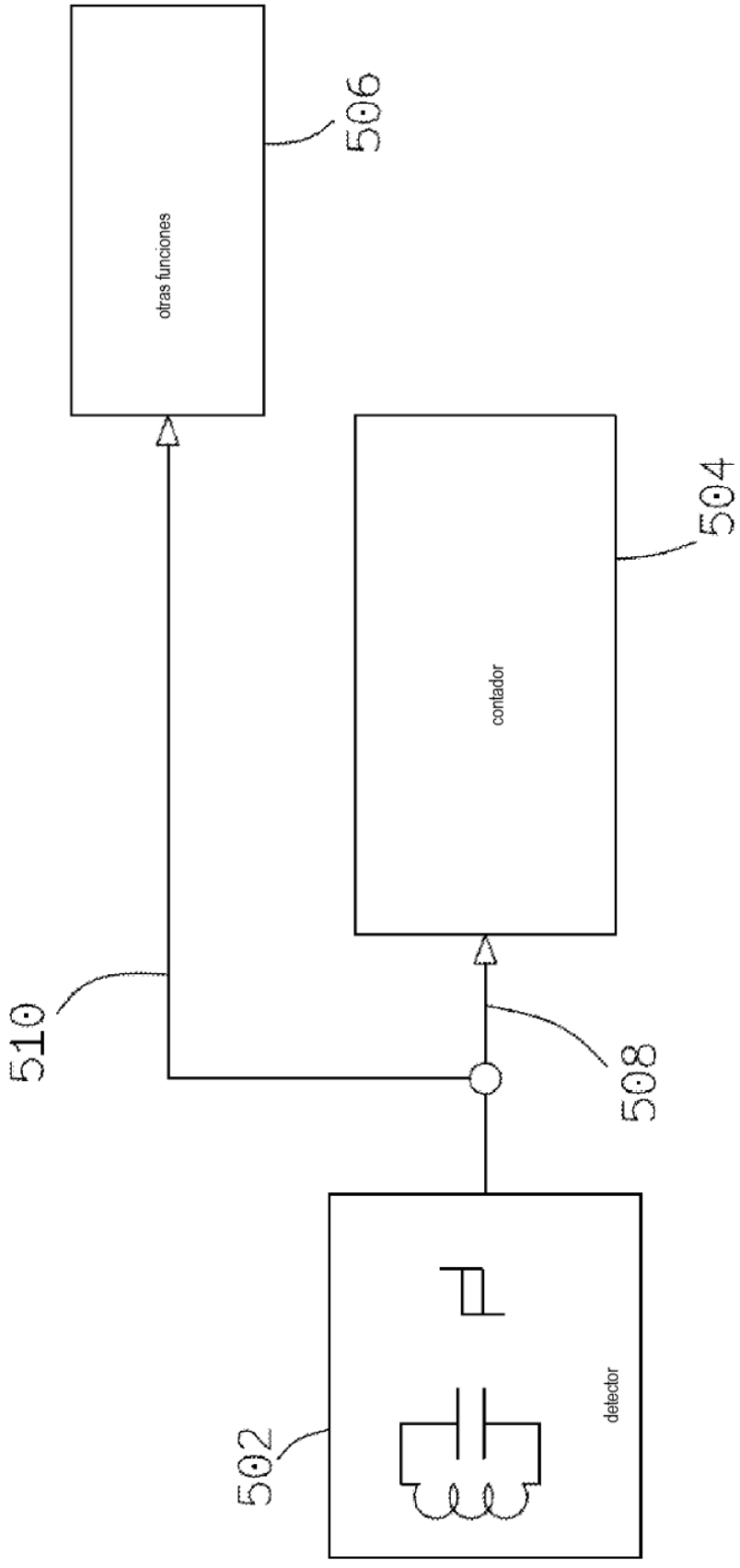


*Fig. 5*

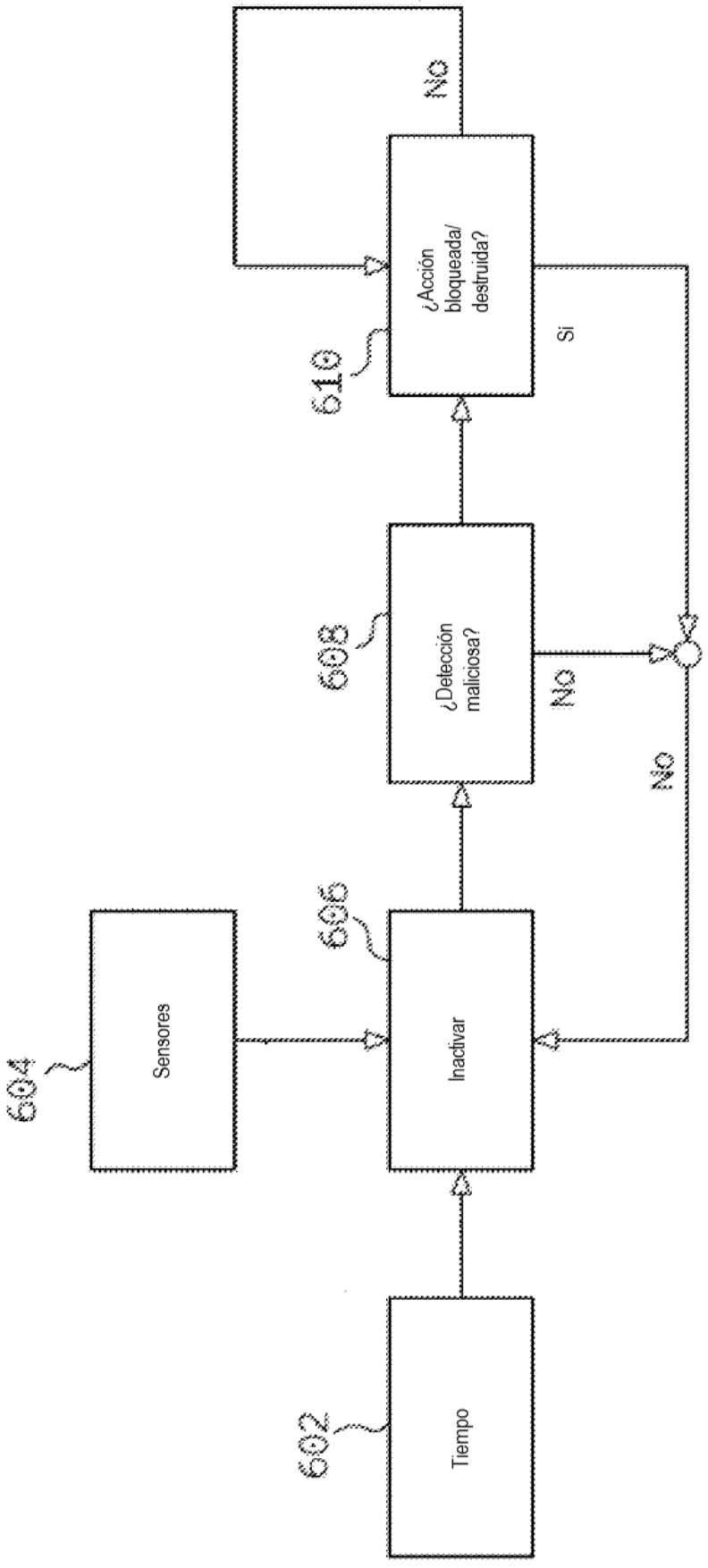
602
Tiempo
604
Sensores
606
Inactivar
608
¿Detección maliciosa?
610
¿Acción bloqueada/ destruida?
No
Si
No
No

Fig. 6