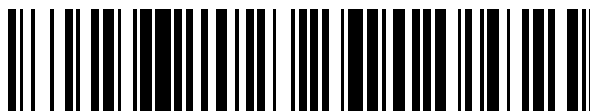


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 661 301**

51 Int. Cl.:

G08B 25/00 (2006.01)

G08B 13/196 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **21.01.2016** **E 16152328 (7)**

97 Fecha y número de publicación de la concesión europea: **17.01.2018** **EP 3048594**

54 Título: **Detección de desarme anónima con cámara incorporada**

30 Prioridad:

26.01.2015 US 201514605439

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

28.03.2018

73 Titular/es:

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

72 Inventor/es:

DING, XIANLONG;
REN, GUOPENG y
MA, XINYU

74 Agente/Representante:

LEHMANN NOVO, María Isabel

ES 2 661 301 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Detección de desarme anónima con cámara incorporada

5 CAMPO DE LA INVENCION

La presente invención se refiere a sistemas de seguridad y más en particular, a interfaz de sistemas de seguridad.

ANTECEDENTES DE LA INVENCION

10 Existen sistemas conocidos para la protección de personas y bienes dentro de zonas aseguradas. Dichos sistemas suelen estar basados en el uso de uno o más sensores que detectan amenazas dentro de la zona asegurada.

15 Las amenazas a personas y bienes se pueden originar a partir de cualquier cantidad de fuentes diferentes. A modo de ejemplo, un incendio puede matar o causar lesiones a los ocupantes que quedaron atrapados por un incendio en una vivienda. De modo similar, el monóxido de carbono procedente de un incendio puede matar a personas mientras duermen.

20 Como alternativa, un intruso no autorizado, tal como un ladrón, puede presentar una amenaza a los bienes dentro de la zona. Es conocido, además, que los intrusos hieren o matan a personas que viven dentro de la zona.

25 En el caso de intrusos, los sensores se pueden colocar en zonas diferentes sobre la base de los usos respectivos de dichas zonas. A modo de ejemplo, si existen personas presentes durante algunas partes de un día normal y no en otros momentos, entonces, los sensores se pueden colocar a lo largo de una periferia de ese espacio con el fin de proporcionar protección dentro del espacio ocupado, mientras que sensores adicionales se pueden colocar en el interior del espacio y utilizarse cuando el espacio no esté ocupado.

30 En la mayoría de los casos, los detectores de amenazas están conectados a un panel de control local. En el caso de que se detecte una amenaza a través de uno de los sensores, el panel de control puede emitir una alarma audible local. El panel de control puede enviar, además, una señal a una estación central de supervisión.

35 Aunque los sistemas de seguridad funcionan bien, se pueden desactivar por alguien que conoce los códigos de desactivación adecuados en una entrada en una zona asegurada. En consecuencia, existe la necesidad de mejores formas de protección contra el uso indebido de los sistemas de seguridad.

La Publicación de Patente de Estados Unidos nº US 7856558 describe un sistema para verificación biométrica y detección por coacción, utilizando una identificación biométrica e identificación de usuario único.

40 La Publicación de Solicitud de Patente de Estados Unidos nº US 2005/0253706 describe un método para interconectar dos sistemas de seguridad separados, utilizando un enlace de radiofrecuencias RF, un enlace telefónico o una red informática.

SUMARIO DE LA INVENCION

45 La presente invención se define por las reivindicaciones adjuntas.

BREVE DESCRIPCION DE LOS DIBUJOS

50 La Figura 1 ilustra un diagrama de bloques de un sistema de conformidad con este documento;

La Figura 2 ilustra una pantalla que se puede mostrar por el sistema de la Figura 1;

La Figura 3 ilustra una pantalla de advertencia que se puede mostrar por el sistema de la Figura 1.

55 DESCRIPCION DETALLADA DE LA INVENCION

60 Aunque formas de realización descritas pueden tener diferentes formas operativas, diferentes formas de realización específicas se ilustran en los dibujos y se describen, en detalle, aquí, en el entendimiento de que la presente idea inventiva ha de considerarse como un ejemplo de los principios, así como del mejor modo de su puesta en práctica, y no está prevista para limitar la puesta en práctica o las reivindicaciones a la forma de realización específica ilustrada.

65 La Figura 1 ilustra un sistema de seguridad 10 que se muestra, en general, de conformidad con una forma de realización ilustrada. Dentro del sistema de seguridad se pueden incluir varios sensores 12, 14, utilizados para detectar amenazas dentro de una zona geográfica asegurada 16. Las amenazas pueden originarse a partir de cualquiera de entre una cantidad de fuentes diferentes. A modo de ejemplo, un intruso puede representar una

amenaza para personas y/o bienes, dentro de una vivienda o negocio. De modo similar, un incendio o fuga de gas pueden amenazar la seguridad de dichas personas y/o bienes.

5 En consecuencia, los sensores se pueden representar en cualquiera de una serie de formas diferentes. A modo de ejemplo, al menos algunos de los sensores pueden ser interruptores de límite colocados en las puertas y ventanas que proporcionan entrada y salida de la zona asegurada. Algunos otros de los sensores pueden ser sensores infrarrojos pasivos (PIR) colocados dentro de la zona asegurada con el fin de detectar intrusos que han podido eludir los sensores a lo largo de la zona periférica asegurada. Otros sensores pueden ser detectores de humo o incendio.

10 En la zona asegurada se incluye, además, un panel de control 17. El panel de control puede estar ubicado dentro de la zona asegurada, tal como se muestra en la Figura 1 o ubicado de forma distante.

15 El panel de control puede supervisar los sensores para activación. A la activación de uno de los sensores, el panel de control puede crear un mensaje de alarma y enviarlo a una estación central de supervisión 18. La estación central de supervisión puede dar respuesta mediante la reunión de la ayuda adecuada (p.ej., policía, departamento de bomberos, etc.).

20 El sistema de seguridad se puede controlar por un usuario humano, a través de la utilización de una interfaz de usuario 20 situada en la proximidad de una entrada en la zona asegurada. La interfaz de usuario puede incluir una pantalla de visualizaciones 22, que muestra un estado del sistema de seguridad (p.ej., armado, desarmado, etc.), y un teclado 24 para la introducción de instrucciones.

25 En el panel de control se incluye la interfaz de usuario y cada uno de los sensores puede ser uno o más aparatos procesadores (procesadores) 28, 30, funcionando cada uno bajo el control de uno o más programas informáticos 32, 34, cargados desde un soporte legible por ordenador no transitorio (memoria) 36. Tal como aquí se utiliza, la referencia a una etapa realizada por un programa informático se refiere, además, al procesador que pone en práctica dicha etapa.

30 A este respecto, un procesador de estado, dentro del panel de control, puede supervisar el teclado de la interfaz de usuario para proporcionar instrucciones procedentes del usuario humano. El usuario puede introducir un número de identificación personal (PIN) y dar instrucciones para armar o desarmar el sistema de seguridad. A la recepción de un número PIN y una instrucción a través del teclado, el procesador de estado puede comprobar el PIN con los números PINs de usuarios autorizados incluidos dentro de un fichero de referencia 38. Si el número PIN introducido coincide con el número PIN de uno de los usuarios autorizados, entonces, el procesador de estado puede poner en práctica la instrucción introducida junto con el PIN.

35 Si la instrucción es una orden de armar, entonces, el procesador de estado activa un procesador de alarma que supervisa los sensores. A la activación de cualquiera de los sensores, el procesador de alarma genera y envía el mensaje de alarma a la estación central de supervisión.

40 De modo similar, si la instrucción es una orden de armado total, entonces, el procesador de alarma solamente podrá supervisar sensores a lo largo de una zona periférica asegurada. Tal como se indicó con anterioridad, a la activación de uno de los sensores a lo largo de la zona periférica, el procesador de alarma genera y envía un mensaje de alarma a la estación central de supervisión.

45 En una forma de realización ilustrada, la interfaz de usuario incluye, además, una cámara de televisión 26. Un campo de visión (FOV) 40 de la cámara se extiende hacia fuera de la interfaz de usuario con el fin de capturar la cabeza y/o el rostro del usuario humano 42 que introduce los números PINs y las órdenes a través de la interfaz de usuario.

50 Imágenes procedentes de la cámara se supervisan por un procesador de reconocimiento facial. El procesador de reconocimiento facial puede funcionar para detectar la presencia de un rostro humano en el campo de visión d la cámara, al mismo tiempo que se introduce un PIN y una instrucción a través del teclado.

55 El campo de visión de la cámara está ajustado de modo que un procesador de imagen, acoplado a la cámara, sea capaz de capturar una imagen del usuario que introduce el número PIN y la instrucción por intermedio del teclado. La imagen capturada se incorpora en una notificación de desarme que se envía a la estación central de supervisión. La notificación de desarme (y la imagen) se memorizan en un fichero como pruebas de quién introdujo la orden junto con la hora y el identificador del sistema de seguridad. Lo anterior proporciona prueba forense importante si más adelante se encontrara que el sistema de seguridad ha sido utilizado de forma inadecuada.

60 En una forma de realización ilustrada, el procesador de detección fácil se utiliza para una operación de control del sistema de seguridad a través de la interfaz de usuario. A modo de ejemplo, si el procesador de estado debe recibir un número PIN válido y una orden, la puesta en práctica de dicha orden podría retrasarse hasta que se detecte un rostro humano frente a la cámara.

65

Conviene señalar, a este respecto, que la interfaz de usuario de la Figura 1 se puede situar, normalmente, dentro de la zona asegurada. Para que un usuario pueda introducir una orden de desarme, al usuario se le solicitará primero que abra una puerta (p.ej., una puerta frontal) para tener acceso a la interfaz de usuario y luego, introducir la orden de desarme.

5 Una vez abierta la puerta, el usuario puede activar un sensor de intrusión conectado a la puerta. En respuesta, un procesador de retardo podría retrasar la activación de una alarma de intrusión durante un período de tiempo predeterminado (período de tiempo de espera) con el fin de permitir a los usuarios autorizados introducir un número PIN válido y la instrucción de desarme. Sin embargo, si el usuario debe introducir su número PIN y una instrucción de desarme mientras está evitando, de forma deliberada, la cámara, entonces, el tiempo de retardo predeterminado terminaría antes de la puesta en práctica de la orden de desarme y se enviaría un mensaje de alarma a la estación de superficie central y se puede activar una alarma local.

15 Dicho de otro modo, la ejecución de órdenes de desarme son objeto de la función lógica AND con la detección de un rostro humano en frente de la interfaz de usuario. Lo que antecede añade otro nivel de integridad al uso adecuado del sistema de seguridad.

20 No es necesario, para el procesador de reconocimiento facial, ser capaz de determinar la identidad del usuario. La única cosa que debe ser capaz de realizar el procesador de reconocimiento facial es detectar la presencia de un rostro humano (cualquier rostro humano) en el campo de visión de la cámara.

25 El control de órdenes de desarme, por el procesador de reconocimiento facial, puede suceder según cualquiera de una serie de métodos distintos. A modo de ejemplo, el procesador de reconocimiento facial puede escanear, continuamente, el campo de visión para detectar rostros humanos. Como alternativa, el procesador de reconocimiento facial puede iniciar el escaneo solamente a la activación de uno o más de los botones, en la interfaz del usuario, o puede incluso retrasar el escaneo hasta que se detecte un número PIN válido. En cualquier caso, el único requisito es la presencia concurrente de un número PIN válido, una orden de desarme y un rostro humano, en un campo de visión de la cámara.

30 En una forma de realización ilustrada, un procesador de supervisión puede controlar el retardo requerido para la detección facial y presentar una advertencia a un usuario, en la pantalla de la interfaz del usuario. A modo de ejemplo, la Figura 2 ilustra una imagen procedente de la cámara en el caso en donde un usuario ha colocado su mano sobre la cámara, con lo que se bloquea cualquier detección de un rostro humano. En respuesta, el procesador de supervisión puede mostrar la imagen que se ilustra en la Figura 3 en la pantalla de la interfaz de usuario. En este caso, en tanto que el usuario mantenga su mano sobre la cámara, la pantalla, ilustrada en la Figura 3, seguirá mostrándose hasta que termine el período de tiempo de espera y se active una alarma. Por otro lado, si el usuario debe retirar su mano antes del final del período de tiempo de espera, entonces, podría ponerse en práctica la orden de desarme y el sistema de seguridad podría entrar en un estado de desarme. En ese momento, una imagen facial procedente del campo de visión, se envía, además, a la estación central de supervisión.

40 El sistema de la Figura 1 ofrece ventajas importantes sobre los diseños actuales. A modo de ejemplo, un sistema puede tener una cámara integrada en el panel de control. Cada vez que se desarme el sistema, la cámara captura una imagen (fotografía) y la envía a la estación central de supervisión con el fin de registrar quién desarmó el sistema.

45 En un diseño actual de este tipo, el sistema se puede desarmar mientras que la cámara integrada está bloqueada por la mano de un usuario, según se ilustra en la Figura 2. De este modo, cualquiera que tenga una contraseña válida puede desarmar el sistema sin que su imagen sea capturada por la cámara y memorizada para futura referencia.

50 El sistema de la Figura 1 resuelve estos problemas. A modo de ejemplo, cuando alguien intenta desarmar el sistema, el panel detecta si el rostro de alguien está en el campo de visión de la cámara, a través de un algoritmo de reconocimiento de imagen que se pone en práctica en un procesador correspondiente. El sistema puede desarmarse solamente cuando el rostro de alguien puede capturarse en imagen de la pantalla. Si se introduce el código de usuario correcto (PIN) y la cámara no puede detectar ningún rostro, el sistema mostrará una ventana emergente y una alarma de voz, hasta que se pueda detectar un rostro de un usuario dentro de un período de tiempo limitado.

60 Después de que se introduzca un desarme/contraseña por un usuario autorizado, el panel realiza un escaneo de un rostro antes de desactivar el sistema de seguridad. La operación de desarme se realiza solamente cuando se detecta un rostro dentro de un cierto tiempo predeterminado. De no ser así, el sistema mantiene el estado armado y las alarmas hasta la activación de un sensor.

65 En una forma de realización ilustrada, el algoritmo de reconocimiento facial no requiere un alto grado de fiabilidad de detección facial. Dicho de otro modo, el algoritmo de reconocimiento facial no necesita detectar quién está intentando desarmar el sistema. Lo único que es necesario es que el algoritmo de reconocimiento facial sea capaz

de detectar si al menos un rostro humano está en el campo de visión de la cámara cuando se activa la función de desarme.

5 En general, el sistema incluye un panel de control de un sistema de seguridad que protege una zona geográfica asegurada, una entrada de usuario, introducida en el panel, que recibe una instrucción de desarme, para desarmar el sistema de seguridad, una cámara, incluida en el panel, que captura una imagen de una persona que introduce la instrucción de desarme, y un procesador que desarma el sistema de seguridad en respuesta a la instrucción de desarme recibida, solamente cuando un rostro humano de la persona se detecta por la cámara.

10 Como alternativa, el sistema incluye un sistema de seguridad que protege una zona geográfica asegurada, un panel de control situado próximo de una entrada a la zona geográfica asegurada, una interfaz de usuario que se incluye en el panel que recibe una instrucción para desarmar el sistema de seguridad, una cámara, incluida en el panel, que captura una imagen de una persona que introduce la instrucción de desarme, y un procesador que desarma el sistema de seguridad a la recepción de la instrucción de desarme, a través de la interfaz de usuario, y a la detección de un rostro humano dentro de la imagen capturada.

15 Como alternativa, el sistema incluye un sistema de seguridad que protege una zona geográfica asegurada, un panel de control del sistema de seguridad, una interfaz de usuario del panel de control que recibe una instrucción para desarmar el sistema de seguridad, una cámara, incluida en el panel, que captura una imagen de una persona que se aproxima a la interfaz de usuario, un procesador de reconocimiento facial que detecta un rostro humano dentro de la imagen capturada, y un procesador que desarma el sistema de seguridad a la recepción de la instrucción de desarme y a la detección del rostro humano.

20
25

REIVINDICACIONES

1. Un aparato que comprende:
 - 5 un panel de control (17) de un sistema de seguridad (10) que protege una zona geográfica asegurada (16);
una entrada de usuario, transmitida por el panel de control, que recibe una instrucción de desarme que demanda el desarme del sistema de seguridad;
 - 10 una cámara (26) incluida en el panel de control, que captura una imagen de una persona (42) que introduce la instrucción de desarme; y
un procesador (28) que desarma el sistema de seguridad en respuesta a la instrucción de desarme recibida por la entrada de usuario, solamente cuando se detecta un rostro humano de la persona por la cámara,
15 caracterizado por cuanto que
el rostro humano de la persona se detecta por la cámara sin la determinación de una identidad de la persona.
- 20 2. El aparato según la reivindicación 1, en donde el procesador (28) envía la imagen, con la instrucción de desarme, a una estación central de supervisión (18).
3. El aparato según la reivindicación 1, en donde la instrucción de desarme incluye un número de identificación personal (PIN) de la persona (42).
- 25 4. El aparato según la reivindicación 1, en donde el procesador (28) mide un período de tiempo entre la entrada de la instrucción de desarme y la detección del rostro humano.
5. El aparato según la reivindicación 4, en donde el procesador (28) compara el período de tiempo con un valor umbral e inicia operativamente una alarma de intrusión al detectar que el período de tiempo ha superado el valor umbral.
- 30 6. El aparato según la reivindicación 5, en donde el procesador (28) envía la alarma de intrusión a una estación central de supervisión (18).
- 35 7. El aparato según la reivindicación 1, en donde el procesador (28) muestra una alarma en el panel de control (17) después de la detección de la instrucción de desarme y antes de la detección del rostro humano.
- 40 8. El aparato según la reivindicación 7, en donde la alarma comprende una ventana emergente que se muestra en una pantalla del panel de control (17).
9. El aparato según la reivindicación 8, en donde la ventana emergente muestra un mensaje de texto que indica que la instrucción de desarme ha fallado puesto que no se ha podido detectar el rostro humano por la cámara (26).

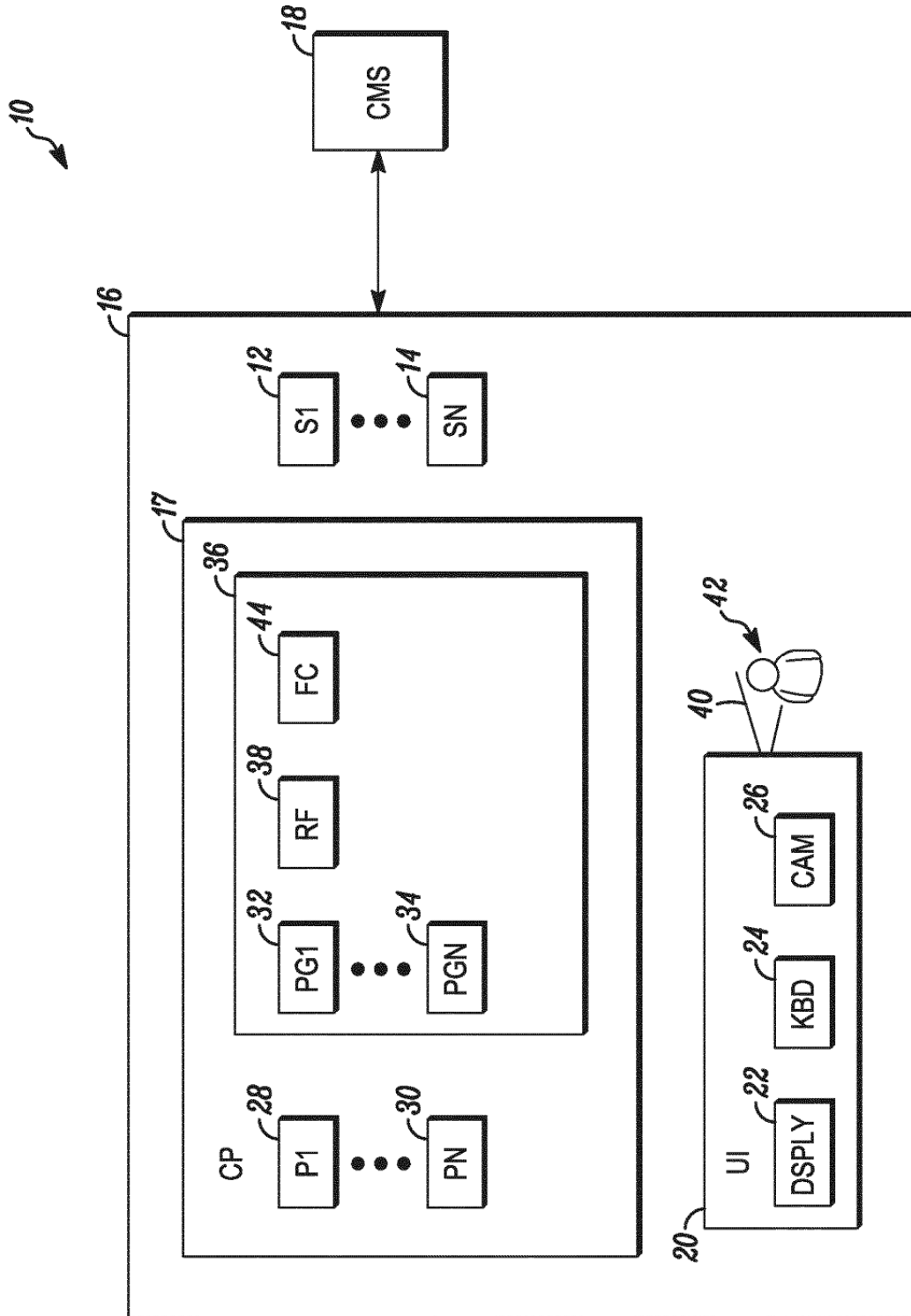


FIG. 1

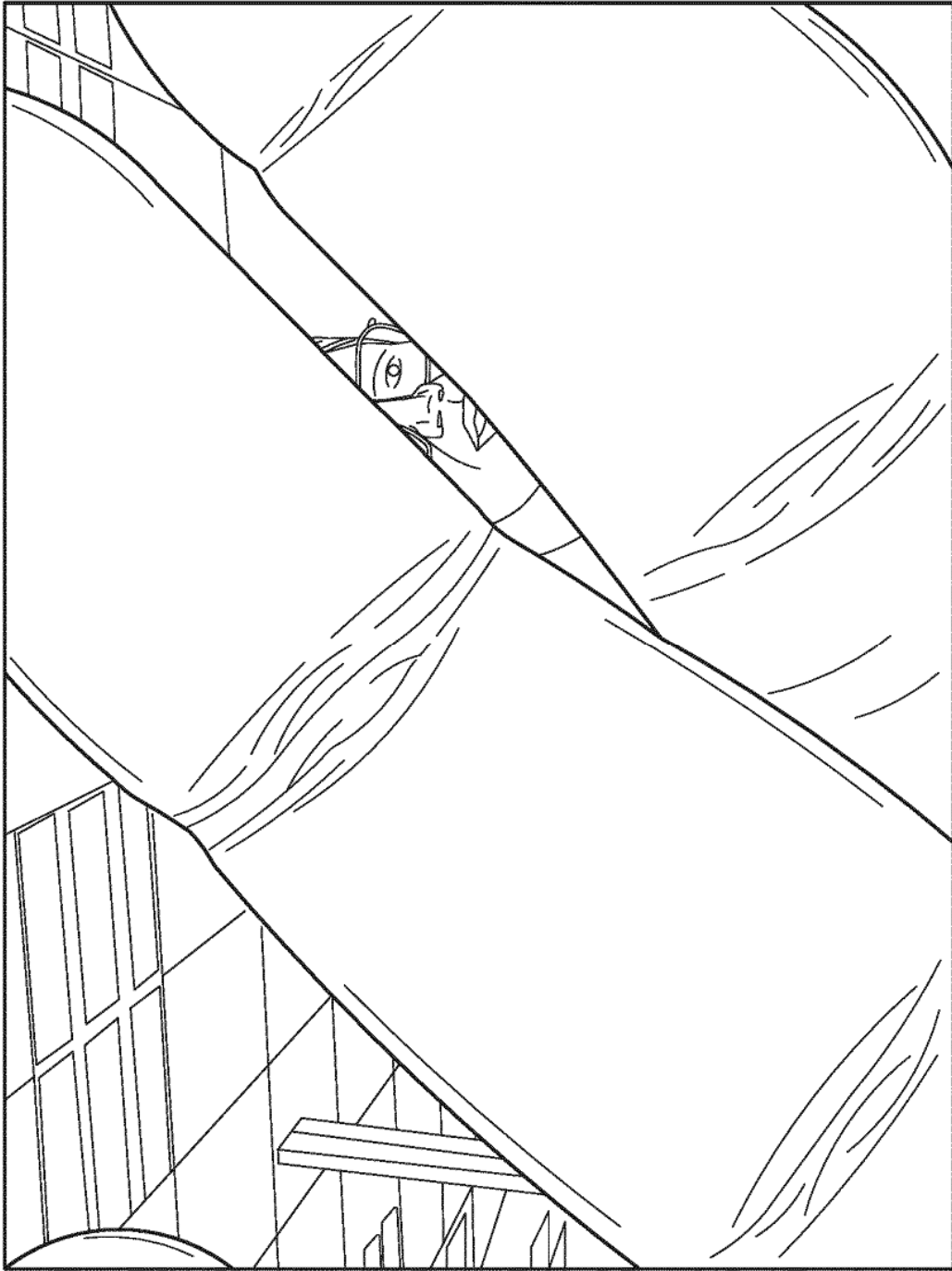


FIG. 2

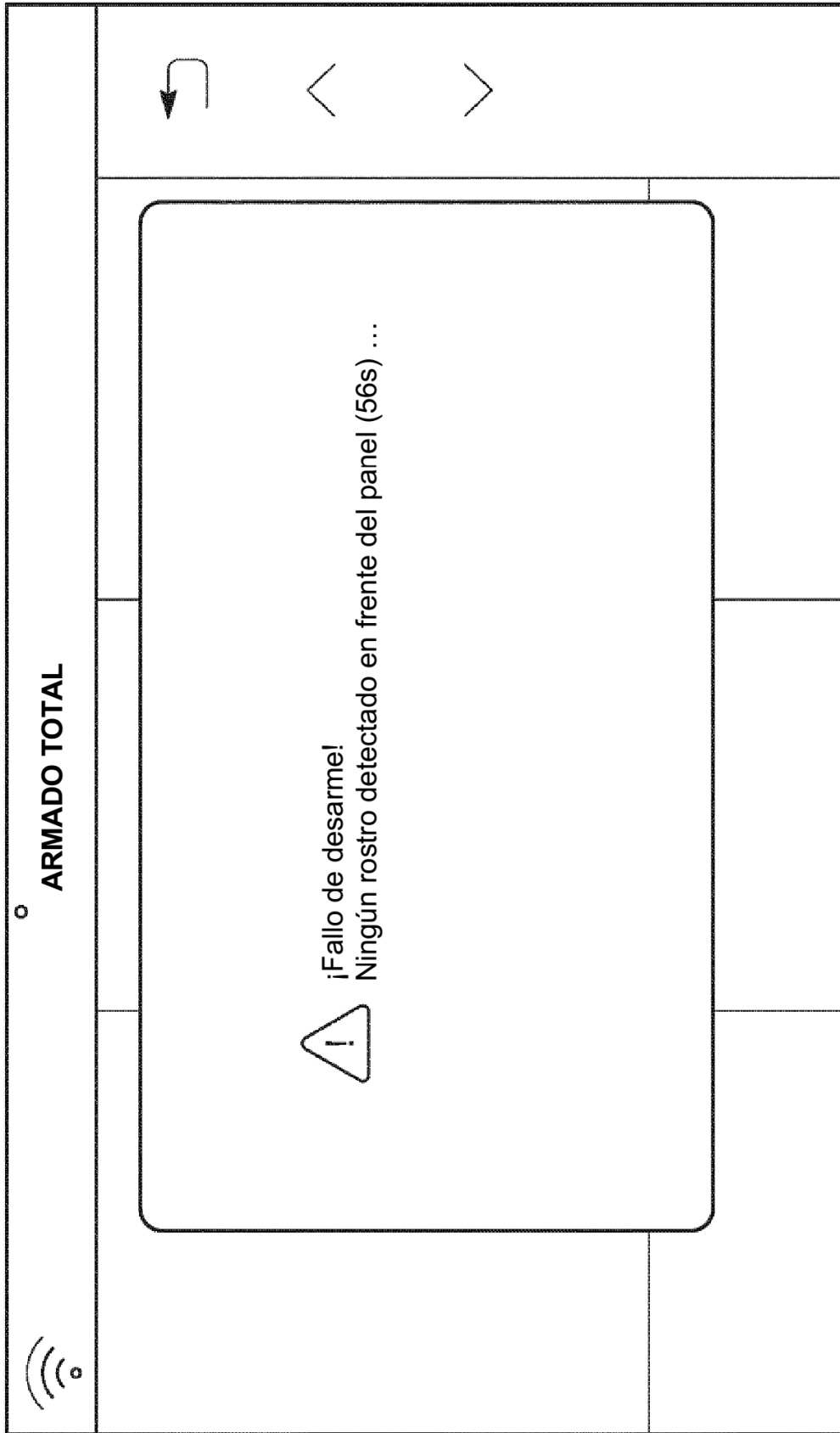


FIG. 3