



19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

11 Número de publicación: **2 364 371**

51 Int. Cl.:

G08B 13/12 (2006.01)

G08B 13/14 (2006.01)

G08B 13/16 (2006.01)

G08B 21/22 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Número de solicitud europea: **07716777 .3**

96 Fecha de presentación : **19.01.2007**

97 Número de publicación de la solicitud: **2123060**

97 Fecha de publicación de la solicitud: **25.11.2009**

54

Título: **Determinación electromagnética de la transgresión de la seguridad de un recinto.**

45

Fecha de publicación de la mención BOPI:
01.09.2011

45

Fecha de la publicación del folleto de la patente:
01.09.2011

73

Titular/es:
GEORGIA TECH RESEARCH CORPORATION
505 Tenth Street, N.W
Atlanta, Georgia 30332-0415, US

72

Inventor/es: **Michaels, Thomas y**
Michaels, Jennifer

74

Agente: **Carvajal y Urquijo, Isabel**

ES 2 364 371 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

Determinación electromagnética de la transgresión de la seguridad de un recinto

Antecedentes

5 Existen muchos tipos de amenazas causadas por el terrorismo. En algunas situaciones, los contenedores que llevan productos a un país pueden ser manipulados o contener material no autorizado o peligroso. Por ejemplo, un contenedor que transporta productos comerciales de un país a otro puede ser manipulado durante el transporte para que contenga material peligroso. La vulnerabilidad a adulteraciones es una desventaja en los dispositivos de seguridad de los contenedores convencionales. Las tecnologías de seguridad de los contenedores actuales sólo proporcionan protección limitada ante varias amenazas del transporte. En particular, los dispositivos de seguridad de contenedores convencionales no contemplan las amenazas que presentan los autores motivados, incluyendo, por ejemplo, los grupos terroristas. Por ejemplo, las estrategias convencionales no están dirigidas a un amplio espectro de riesgos con un enfoque en aquellos riesgos que amenazan la seguridad nacional. Además, las estrategias convencionales no proporcionan una serie de funciones resistentes a la adulteración incorporadas en un diseño. En otras palabras, las estrategias convencionales no están dirigidas a la vulnerabilidad ante métodos de adulteración incluso simplistas.

Un sistema y método para proporcionar seguridad a contenedores se revela en la patente US 2005/073406. El sistema incluye un sistema de detección para monitorear los contenidos del contenedor; un elemento de recepción de señal para recibir datos del sensor; un elemento de control para analizar los datos de sensor recibidos; un primer elemento transceptor para recibir señales que contienen datos del sensor desde el interior del contenedor y para transmitir dichas señales al exterior del contenedor; y un elemento de transceptor satelital para recibir señales desde el primer elemento de transceptor y para reenviar las señales recibidas mediante enlace ascendente del satélite a una ubicación remota.

El sistema de detección consiste en un conjunto de sensores elegido para ofrecer la vista más precisa y completa del entorno del contenedor, entre los cuales se incluye un sensor de la integridad del contenedor basado en una técnica de detección tal como una técnica ultrasónica pasiva, la medición de energía de RF reflejada o la medición de conductividad del contenedor.

La patente US 2006/164239 revela un contenedor de transporte y un método para monitorear dicho contenedor de transporte para detectar las condiciones del contenedor desde una ubicación remota, o detectar la condición de otros contenedores de transporte en las cercanías del contenedor de transporte. El contenedor de transporte puede incluir un micro-servidor incorporado que se comunica con una pluralidad de sensores dentro del contenedor. El micro-servidor puede servir como un nodo de Internet que permite comunicar las condiciones detectadas dentro del contenedor a dispositivos informáticos remotos por medio de Internet. El contenedor de transporte también puede incluir equipos anti-adulteración tales como una rejilla conductora, de modo tal que cualquier manipulación del contenedor afectará necesariamente a un parámetro eléctrico de la rejilla, y el cambio en el parámetro eléctrico se detectará después y hará que se active una alarma o se tome otra medida correctiva.

Resumen de la invención

De acuerdo con realizaciones de la presente invención, se revelan sistemas y métodos para determinar intrusiones en recintos y otro tipo de información del recinto. Por ejemplo, puede determinarse una transgresión de una estructura. Un sensor, provisto en la estructura, puede operarse mediante una señal de frecuencia constante. El sensor puede comprender un primer elemento conductor y un segundo elemento conductor. El primer elemento conductor puede ser sustancialmente paralelo al segundo elemento conductor. Un patrón de onda estacionaria puede inducirse en el sensor mediante la señal de frecuencia constante que se refleja por fuera de un punto de terminación del sensor. Puede medirse al menos una característica del sensor provocada por el patrón de onda estacionaria de tensión. Puede determinarse si está ocurriendo una transgresión de una estructura cuando al menos una característica medida difiere de un valor determinado previamente en una cantidad predeterminada. El primer elemento conductor y el segundo elemento conductor pueden estar alojados entre dos capas que comprenden la estructura. La estructura puede comprender un suelo del contenedor. La transgresión de la seguridad detectada puede comprender una abertura de más de nueve pulgadas cuadradas.

Debe entenderse que tanto la descripción general precedente, como la descripción detallada que sigue a continuación, se proporcionan sólo a modo explicativo y de ejemplo, y no debe considerarse que restringen en modo alguno el alcance de la invención, tal como se describe y reivindica. Además, pueden proporcionarse características y/o variaciones adicionales a las expuestas en la presente invención. Por ejemplo, realizaciones de la invención pueden estar dirigidas a diferentes combinaciones y subcombinaciones de funciones descritas en la descripción detallada.

Breve descripción de los dibujos

Los dibujos adjuntos, que se incorporan a y constituyen parte de esta revelación, ilustran diferentes realizaciones de la presente invención. En los dibujos:

- La figura 1 es un diagrama de bloques de un entorno operativo;
- 5 La figura 2 es un diagrama que ilustra un contenedor;
- La figura 3 es un diagrama de bloques de un procesador;
- La figura 4 es un diagrama de flujo de un método para determinar intrusiones del recinto y otra información del recinto;
- La figura 5 es un diagrama que ilustra un subsistema ultrasónico de detección de transgresión de la seguridad;
- 10 La figura 6 es un diagrama que ilustra un sensor ultrasónico;
- La figura 7 es un diagrama que ilustra un sensor de línea de transmisión electromagnética (EMTL);
- La figura 8 es un diagrama que ilustra un sensor de línea de transmisión electromagnética (EMTL);
- La figura 9 es un diagrama que ilustra un subsistema EMTL;
- La figura 10 es un diagrama que ilustra un subsistema de detección de movimiento de un contenedor;
- 15 La figura 11 es un diagrama de flujo de un método para la detección de movimiento de un contenedor;
- La figura 12 es un diagrama que ilustra la absorción de radiación infrarroja;
- La figura 13 es un diagrama que ilustra un subsistema de detección de humanos;
- La figura 14 es un gráfico que ilustra una transmisión de trayecto de 10cm calculada para una banda de absorción de CO₂ de 4,3μm;
- 20 La figura 15 es un diagrama de flujo de un método para la detección de humanos en un recinto;
- La figura 16 es un diagrama que ilustra un subsistema para el estado de una puerta;
- La figura 17 es un diagrama que ilustra un revestimiento de película del control de luz;
- La figura 18 es un diagrama de flujo de un método para operar un sensor del estado de la puerta;
- La figura 19 es un diagrama que ilustra una fusión de sensores; y
- 25 La figura 20 es un diagrama que ilustra una fusión de sensores.

Descripción detallada

- La siguiente descripción detallada hace referencia a los dibujos adjuntos. Siempre que sea posible, se utilizan los mismos números de referencia en los dibujos y en la siguiente descripción para hacer referencia a los mismos elementos o a elementos similares. Mientras que pueden describirse realizaciones de la invención, son posibles modificaciones, adaptaciones, y otras implementaciones. Por ejemplo, pueden realizarse sustituciones, adiciones o modificaciones de los elementos ilustrados en las figuras, y de los métodos que se describen en este documento mediante la sustitución, reordenamiento o adición de pasos a los métodos revelados. Por lo tanto, la siguiente descripción detallada no limita la invención. En cambio, el alcance de la invención se define mediante las reivindicaciones adjuntas.
- 30
- 35 Intrusiones a un recinto y otra información sobre el recinto pueden determinarse de manera consistente con las realizaciones de la presente invención. Por ejemplo, un dispositivo de detección multimodal puede proporcionarse para asegurar los contenedores (por ejemplo, contenedores de transporte) contra diferentes amenazas. Estas amenazas pueden comprender, pero no se limitan a, transgresiones de la seguridad de una estructura, la apertura

de una puerta cerrada, y la presencia humana. Además, las realizaciones de la invención pueden incorporar un diseño integrado que incluye múltiples modalidades de detección, algoritmos de fusión de sensores y empaquetado relacionado. Las realizaciones de la invención pueden realizarse mediante uno o más de los subsistemas que se describen en detalle a continuación.

5 A modo de ejemplo no limitativo, la figura 1 ilustra un sistema de seguridad 100 en el cual pueden implementarse las características y principios de la presente invención. Como se ilustra en el diagrama de bloques de la figura 1, el sistema 100 puede incluir un contenedor 105, una red 110 y un procesador 115. El contenedor 105 puede incluir sensores 120. Un controlador 125 también puede estar incluido en el contenedor 105 para coordinar la comunicación entre los sensores 120 y el procesador 115.

10 El procesador 115 puede estar monitoreado u operado por un usuario, por ejemplo, que desea implementar seguridad en el contenedor. Además, el usuario también puede ser una organización, empresa o cualquier otra entidad que desee tal cosa. El contenedor 105 puede comprender, pero no se limita a, un contenedor de transporte configurado para su utilización para el transporte de productos desde una ubicación a otra. Por ejemplo, el contenedor 105 puede estar lleno de productos, asegurado, y colocado sobre un barco, aeronave o camión para ser transportado. Aunque que el contenedor 105 puede consistir en un contenedor de transporte, puede consistir, por ejemplo, en cualquier recinto cuya ubicación, movimiento, seguridad, transgresiones de la seguridad de una estructura, estado de posición de la puerta o presencia humana pueda monitorearse. Como se describirá en detalle a continuación, los datos recogidos por los sensores 120 pueden enviarse al procesador 115 a través de una red 110. Mientras que el sistema 100 sólo ilustra un contenedor 105, el procesador 115 puede monitorear una pluralidad de contenedores. La figura 2 muestra el contenedor 105 en más detalle.

15 El sistema 100 puede proporcionar seguridad para el contenedor con múltiples modalidades de detección, monitoreo de condiciones, y capacidad de alerta avanzadas. El sistema 100 puede incorporar una serie de sensores 120 y también tecnologías de fusión de sensores que pueden concentrarse en una variedad de amenazas para el contenedor. Entre las amenazas específicas que pueden detectarse se incluyen, por ejemplo, transgresiones de la seguridad de la estructura del contenedor 105, presencia de ocupantes no autorizados (por ejemplo, humanos) en el contenedor 105, apertura de la puerta del contenedor 105 y condiciones ambientales asociadas al contenedor 105. Además, el movimiento del contenedor 105 y la temperatura y humedad dentro del contenedor 105 pueden controlarse. La información recopilada 120 puede procesarse mediante el procesador 115. El procesador 115 o controlador 125 puede determinar si se ha producido una transgresión de la seguridad con el contenedor 105 y emitir una alerta.

20 Pueden utilizarse diferentes interfaces de comunicaciones para proporcionar acceso remoto en el sistema 100. Una interfaz de comunicaciones local (por ejemplo, ubicada en el controlador 125) puede proporcionar comunicación inalámbrica entre el procesador 115 y los sensores 120 en un radio de 150 metros del contenedor 105 utilizando, por ejemplo, el protocolo IEEE 802.15.4. Este protocolo puede ser lo suficientemente robusto para permitir, por ejemplo, distancias de transmisión de 50 metros incluso cuando un transmisor asociado con cualquiera de los sensores 120 está rodeado por otros contenedores que pueden obstruir los radiotransmisores utilizando otros protocolos. La interfaz de comunicación local puede permitir a los usuarios con dispositivos informáticos portátiles (por ejemplo, asistentes digitales personales (PDA, por sus siglas en inglés)) consultar el contenedor 105 o recibir alertas de seguridad del contenedor 105. Las comunicaciones de larga distancia pueden lograrse entre el procesador 115 y los sensores 120 mediante una interfaz RS-485 (por ejemplo, ubicada en el controlador 125) hasta un sistema de la marina de seguimiento y etiquetado de productos (del inglés MATTS, Marine Asset Tagging and Tracking). También puede proporcionarse una interfaz física (por ejemplo, un cable) entre el procesador 115 y el controlador 125 asociado con los sensores 120 para permitir cargar actualizaciones del firmware directamente al controlador 125.

25 La detección de transgresión de la seguridad en el contenedor 105 puede lograrse, por ejemplo, a través de sensores ultrasónicos y sensores electromagnéticos incluidos en los sensores 120. Estos sensores pueden detectar cambios en la estructura del contenedor. Los sensores ultrasónicos pueden instalarse como un conjunto disperso montado en las paredes del contenedor 105. Los sensores ultrasónicos pueden operar de manera pasiva o activa. Por ejemplo, los sensores ultrasónicos pueden operar de manera pasiva mediante la escucha de ondas elásticas en las paredes del contenedor 105 que pueden indicar un intento de penetrar en el contenedor. Para la operación pasiva, pueden utilizarse uno o más sensores en cada pared como receptores ultrasónicos para detectar señales correspondientes a "eventos ultrasónicos" (por ejemplo, ondas elásticas en las paredes del contenedor 105). La naturaleza de estas señales en el dominio de tiempo, dominio de frecuencia o el dominio de tiempo-frecuencia puede utilizarse para separar señales de ruido generadas por transgresiones de la seguridad de eventos de ruido no provocados por transgresiones de la seguridad. En el dominio de tiempo-frecuencia, por ejemplo, puede utilizarse una transformada de wavelet, una transformada Chirplet u otras transformadas similares.

30 Además, los sensores ultrasónicos pueden operar de manera activa mediante la transmisión de una señal (por ejemplo, una onda elástica de impulso) en la pared y la posterior comparación de la respuesta debido a la señal transmitida con una respuesta de señales transmitidas previamente. Además, la señal puede transmitirse en el suelo, techo o en cualquier otra parte del contenedor 105 en la cual la señal pueda transmitirse, y no se limita a las

paredes. Cambios en la respuesta ultrasónica a las paredes del contenedor 105, por ejemplo, pueden indicar una nueva transgresión de la seguridad y puede generar una alarma mediante el procesador 115 o controlador 125. En otras palabras, la operación activa puede involucrar la transmisión y recepción de señales que comprenden ondas ultrasónicas en las paredes del contenedor 105 utilizando diferentes pares de sensores (es decir, transductores) que pueden adherirse a la pared. Las ondas elásticas ultrasónicas son ejemplos y las señales propagadas en las paredes pueden consistir en otros tipos de señales. Un transductor puede operarse como un transmisor y otro como receptor.

Las ondas ultrasónicas generadas por el transmisor pueden grabarse mediante el receptor. Este proceso puede repetirse para múltiples combinaciones de transductor de transmisión/recepción. Para cada evento de transmisión/recepción, las ondas ultrasónicas se propagan por todas las paredes del contenedor 105 e interactúan con límites, variaciones estructurales naturales y transgresiones de la seguridad. Las señales de ondas ultrasónicas recibidas pueden contener información sobre el material/estructura entre y cerca del par de transductor de transmisión/recepción en particular utilizado para la medición ultrasónica activa. En el modo activo, las formas de onda ultrasónicas recibidas pueden analizarse y compararse con formas de onda de referencia (por ejemplo, formas de onda grabadas antes de que se produjera la transgresión de la seguridad). Las características computadas tanto de las señales ultrasónicas activas como pasivas pueden computarse y analizarse, por ejemplo, mediante el procesador 115 o controlador 125 como una función de tiempo para detectar y caracterizar transgresiones de la seguridad potenciales.

Todos los sensores 120 pueden integrarse en un solo sistema de monitoreo. Como se describe en más detalle a continuación, los algoritmos de fusión de datos pueden utilizarse para detectar, ubicar y calcular la gravedad de una transgresión de la seguridad o transgresión de la seguridad potencial. La combinación de procesos de monitoreo ultrasónico pasivo y activo puede proporcionar un método de detección robusto para la detección de transgresiones de la seguridad. Aunque se hace referencia a contenedores de transporte con anterioridad, las realizaciones de la invención pueden aplicarse a cualquier tipo de recinto.

Para detectar transgresiones de la seguridad en partes del contenedor 105 fabricado en un material para el cual los sensores ultrasónicos mencionados con anterioridad podrían no ser capaces de detectar una transgresión de la seguridad, pueden utilizarse sensores electromagnéticos conforme a la invención. Por ejemplo, el suelo del contenedor 105 puede ser de madera o cualquier otro material no X adecuado para los sensores ultrasónicos mencionados con anterioridad. Por lo tanto, los sensores ultrasónicos mencionados con anterioridad pueden no poder detectar una transgresión de la seguridad en el suelo del contenedor 105. Los sensores electromagnéticos, por ejemplo, pueden comprender cada uno líneas de transmisión pareadas que pueden colocarse en el suelo del contenedor 105. Una señal de radiofrecuencia (RF) con una frecuencia conocida puede aplicarse a líneas de transmisión pareadas para poder generar un patrón de onda estacionaria. Como se describe en más detalle a continuación, el patrón de onda estacionaria puede monitorearse mediante un controlador 125 o procesador 115 para detectar transgresiones de la seguridad del suelo del contenedor 105. Además, la frecuencia utilizada por los sensores electromagnéticos puede generarse de manera pseudo-aleatoria de modo que el sensor sea difícil de manipular.

Una transgresión de la seguridad puede definirse, por ejemplo, como un intento de intrusión que produce un orificio de nueve pulgadas cuadradas de superficie o mayor en un lateral de un contenedor. Además, las transgresiones de la seguridad pueden detectarse con una probabilidad de detección mayor del 75% y dentro de un rango de dos minutos desde que ocurre. Cualquier tasa de falsa alarma correspondiente puede ser menor a 0,003 falsas alarmas por viaje del contenedor. Cualquiera de los sensores 120 puede ser adecuado para la instalación en contenedores nuevos y usados en menos de dos horas para permitir una utilización generalizada. Debido a las amenazas de características únicas impuestas al suelo, un sensor utilizado para el suelo puede no ser sensible a los clavos insertados a través del suelo para asegurar el cargamento, daños en el suelo asociados al uso normal, y condiciones de carga. El entorno marítimo puede requerir que el sensor no sea sensible ni a la humedad en el contenedor ni al contenido de humedad del suelo.

De manera consistente con las realizaciones de la invención, los sensores electromagnéticos (es decir, sensores de línea de transmisión electromagnética (EMTL, por sus siglas en inglés)) pueden comprender una rejilla de cintas conductoras paralelas que están instaladas en el suelo entre dos secciones de contrachapado para formar una línea de transmisión electromagnética. El espaciado de los conductores y la construcción de la rejilla puede ser tal que colocar clavos en el suelo u otros daños asociados con el uso normal pueden no alterar de manera significativa (ni mediante la interrupción ni mediante el corte) los conductores en la rejilla. Sin embargo, hacer un orificio con una superficie (por ejemplo, mayor de nueve pulgadas cuadradas) puede romper la rejilla y cambiar de este modo las características de la línea de transmisión.

Estos cambios en las características de la línea de transmisión pueden detectarse mediante la medición del patrón de onda estacionaria de tensión en la línea de transmisión. Un patrón de onda estacionaria puede inducirse en una línea de transmisión cuando la línea de transmisión es conducida a una frecuencia constante. Pueden ocurrir reflexiones en el final de la línea. Este patrón puede caracterizarse por la ubicación de los puntos de tensión máxima

y mínima, la separación entre esos puntos, y la relación entre los valores de tensión máxima y mínima, que se conoce como la relación de onda estacionaria de tensión (VSWR, por sus siglas en inglés). Estas características de línea de transmisión pueden medirse mediante la detección de la tensión en la línea en diferentes ubicaciones a lo largo de la rejilla en varias frecuencias de entrada diferentes. Estas frecuencias pueden aplicarse como ráfagas de RF cortas en el rango de frecuencia, por ejemplo, de 1MHz a 50MHz. El ciclo de trabajo para la generación de señal puede calcularse para ser menor a 0,001% para alcanzar un objetivo de detección de transgresión de la seguridad de 2 minutos. El proceso de EMTL antes mencionado puede ser efectivo para detectar transgresiones de la seguridad mientras no estén afectadas ni por clavos a través de, por ejemplo, el suelo ni por efectos de carga. Además, la operación de los sensores puede mantenerse después de que las líneas de la rejilla entren en corto circuito o sean interrumpidas. Aunque se desarrolló para contenedores de transporte, este concepto puede aplicarse como un proceso de detección de penetración de otros recintos.

En combinación con los medios de detección de la invención, los sensores 120 también pueden incluir sensores de la presencia de dióxido de carbono (CO₂). Por ejemplo, puede detectarse la presencia humana utilizando el sensor de CO₂. La concentración de CO₂ en el contenedor 105, por ejemplo, puede aumentar en un sistema cerrado tal como el contenedor 105 cuando está presente un ser humano. El sensor de CO₂ puede comprender dos diodos de emisión de luz (LED, por sus siglas en inglés), un LED puede emitir luz en una región de espectro pequeña donde el CO₂ muestra una gran absorción y el otro LED puede emitir luz en una región de espectro donde el CO₂ no muestra absorción alguna. Mediante la pulsación de estos LED en secuencia y el monitoreo de la transmisión de luz a través de una cavidad que contiene una muestra de aire del contenedor 105, puede calcularse la concentración de CO₂ en el contenedor 105. Debido a que es posible preestablecer la velocidad a la cual la concentración de dióxido de carbono se incrementa ante la presencia humana, la comparación de concentraciones de CO₂ del contenedor 105 con estas mediciones preestablecidas puede indicar si hay un ser humano presente en el contenedor 105.

Además, los sensores 120 también pueden incluir un sensor de puerta abierta en combinación con los medios de detección de la invención. El estado de la puerta del contenedor puede monitorearse utilizando sensores ópticos que pueden comprender dos partes: una fuente de luz LED; y un fotodetector pareados que puede ser sensible a la luz desde la fuente de luz LED. Puede instalarse una parte dentro del contenedor 105 en una pared y la otra parte puede instalarse en el panel de la puerta del contenedor 105. Las dos partes pueden operar de modo tal que la luz de la fuente de luz LED puede incidir en el fotodetector cuando se cierra la puerta. Puede utilizarse una película de control de luz para limitar el campo de visión del fotodetector de modo tal que puedan detectarse pequeños cambios en la posición de la puerta.

Un evento de apertura de la puerta puede detectarse cuando el cambio en el nivel de luz en el fotodetector excede un valor umbral. En otras palabras, si la puerta del contenedor 105 se abriera un poco, no se detectaría un evento de apertura de la puerta. Sin embargo, si la puerta del contenedor 105 se abriera tanto que cambiara el nivel de luz en el fotodetector tanto como para exceder el valor umbral, podría detectarse un evento de apertura de la puerta. Por ejemplo, cambios pequeños en la ubicación de la puerta pueden no indicar que se está abriendo la puerta. Si, en cambio, la puerta se mueve mucho, esto puede indicar que se está abriendo la puerta. En el ejemplo de contenedor de transporte, los contenedores pueden estar apilados, lo cual puede hacer que las puertas en algunos contenedores se abran un poco debido a la hinchazón. Dado que esta protuberancia puede ocurrir de manera habitual y no indicar manipulación, un evento de apertura de la puerta puede no indicarse mediante la hinchazón de la puerta debido a que los contenedores están apilados. Además, la utilización de códigos de impulsos generados de manera aleatoria entre la fuente de luz LED y el fotodetector pareado para consultar el sensor de apertura de la puerta puede hacer que la manipulación sea más difícil. Estos códigos pueden generarse de manera pseudo-aleatoria de modo tal que el transmisor y receptor pueden sincronizarse sin una conexión con cables entre ellos.

Como se indicara con anterioridad, el sensor de puerta puede comprender dos partes (es decir, dos módulos). Una parte puede incluir un LED que emite luz de 950nm de longitud de onda en un haz estrecho con una divergencia de menos de 10 grados. La otra parte puede incluir un fotodetector de silicio de bajo perfil con una lámina de película de control de luz que cubre el detector. La película de control de luz puede comprender, pero no se limita a, una implementación modificada de las láminas plásticas transparentes de microrejillas integradas utilizadas, por ejemplo, para cubrir terminales de visualización informáticas y proporcionar privacidad en entornos públicos.

Para la aplicación del sensor de puerta, la película antes mencionada puede fabricarse de modo tal que puede restringir la transmisión de luz a un ángulo de menos de 10 grados. Los dos módulos del sensor de puerta pueden instalarse de modo tal que cuando la puerta se cierra, la luz del LED puede incidir en y detectarse mediante el fotodetector. Por ejemplo, cuando la puerta se abre, el ángulo interior de incrementa. En consecuencia, la cantidad de luz detectada aumenta a medida que el haz de luz rota fuera del campo de visión del detector que puede definirse mediante la película de control de luz. Puede utilizarse un umbral de detección para el fotodetector para definir cuándo se considera que la puerta está abierta. Además, en lugar de iluminación continua, la luz del LED puede ser intermitente utilizando un esquema de señalización de modulación por intervalo entre impulsos. Esto puede evitar la falsificación activa de la identificación de la fuente de LED para generar un estado de "puerta cerrada" falso.

Además, los sensores 120 también pueden incluir un sensor de movimiento en combinación con los medios de detección de la invención. El movimiento del contenedor 105 puede comprender, por ejemplo, un acelerómetro de baja potencia de doble eje. El acelerómetro puede detectar cambios en la velocidad a lo largo de cada eje. Estos datos de cambio de velocidad pueden estar integrados para descubrir la velocidad del contenedor 105. Por ejemplo, una velocidad que no es cero puede indicar que el contenedor 105 está en movimiento. Además, los sensores 120 también pueden indicar sensores para monitorear condiciones del entorno dentro del contenedor 105 tal como temperatura y humedad.

Los datos de los sensores 120 pueden transmitirse al controlador 125 que a su vez puede procesar y transmitir los datos a través de la red 110 al procesador 115. El procesador 115 puede procesar los datos antes de tomar una decisión de emitir una alerta de seguridad. En otra realización, el controlador 125 puede procesar los datos antes de tomar una decisión de emitir una alerta de seguridad y pasar cualquier alerta al procesador 115. Este enfoque integrado para detectar amenazas de seguridad puede mejorar la probabilidad de detección de amenazas de alta seguridad para el contenedor 105 y al mismo tiempo minimizar los riesgos de falsa alarma. Además, pueden incorporarse técnicas para mejorar la resistencia a la manipulación del sensor 120 a los sensores 120 y al controlador 125. El sistema 100 también puede tener una interfaz con otros sensores que pueden proporcionar utilidad a los expedidores. Estos otros sensores pueden comprender, pero sin limitarse a, lectores de etiquetas de identificación por radio frecuencia (RFID, por sus siglas en inglés). La capacidad de leer etiquetas RFID en productos u otros elementos a medida que se introducen o extraen del contenedor 105 puede ser una ventaja importante. Por ejemplo, el controlador 125 o procesador 115 puede monitorear y registrar todos los productos u otros elementos que se introdujeron en o se extrajeron del contenedor 105.

Un sistema para determinar intrusiones en el recinto y otra información del recinto puede consistir en un almacenamiento de memoria y una unidad de procesamiento acoplada al almacenamiento de memoria. La unidad de procesamiento puede ser operativa para recibir datos de una pluralidad de sensores asociados con el recinto, donde al menos uno de la pluralidad de sensores comprende, al menos, uno de los siguientes tipos de sensores: ultrasónico, acústico, de línea de transmisión electromagnética (EMTL), movimiento del contenedor, detección de humanos y estado de la puerta. Además, la unidad de procesamiento puede ser operativa para analizar los datos para determinar si se ha producido un evento de intrusión del recinto. La unidad de procesamiento también puede ser operativa para emitir una alerta cuando se determina que se ha producido el evento de intrusión.

La memoria antes mencionada, unidad de procesamiento y otros componentes pueden implementarse en un sistema de seguridad, tal como el sistema de seguridad 100 a modo de ejemplo de las figuras 1 y 2. Puede utilizarse cualquier combinación adecuada de hardware, software y/o firmware para implementar la memoria, unidad de procesamiento u otros componentes. Por ejemplo, la memoria, unidad de procesamiento u otros componentes pueden implementarse con cualquier procesador 115 o controlador 125, en combinación con el sistema 100. El sistema, procesador y controlador antes mencionados son a modo de ejemplo y otros sistemas, procesadores y controladores pueden constituir la memoria, unidad de procesamiento u otros componentes antes mencionados, conforme a realizaciones de la presente invención.

La figura 3 muestra el procesador 115 de la figura 1 en más detalle. Como se muestra en la figura 3, el procesador 115 puede incluir una unidad de procesamiento 325 y una memoria 330. La memoria 330 puede incluir un módulo de software 335 y una base de datos 340. Mientras se ejecuta la unidad de procesamiento 325, el módulo de software 335 puede realizar procesos de seguridad, incluyendo, por ejemplo, uno o más de los pasos del método 400 descrito con posterioridad con respecto a la figura 4. Además, también cualquier combinación de módulo de software 335 y base de datos 340 puede ejecutarse en o residir en el controlador 125, tal como se muestra en la figura 1. El controlador 125 puede comprender una configuración similar al procesador 115.

El procesador 115 o el controlador 125 ("los procesadores") incluidos en el sistema 100 pueden implementarse utilizando un ordenador personal, un ordenador en red, un ordenador central u otras estaciones de trabajo basadas en microordenadores similares. Los procesadores pueden comprender cualquier tipo de entorno operativo informático, tal como dispositivos portátiles, sistema multiprocesadores, dispositivos electrónicos emisores programables o basados en microprocesadores, miniordenadores, ordenadores centrales y similares. Los procesadores también pueden realizarse en entornos informáticos distribuidos donde las tareas son realizadas mediante dispositivos de procesamiento remotos. Además, cualquiera de los procesadores puede consistir en un terminal móvil, tal como un teléfono inteligente, un teléfono celular, un teléfono celular que utiliza el protocolo de aplicaciones inalámbricas (WAP, por sus siglas en inglés), asistente digital personal (PDA), localizador inteligente, ordenador portátil, un ordenador portátil de mano, un teléfono convencional o una máquina de fax. Los sistemas y dispositivos antes mencionados son ejemplos y los procesadores pueden consistir en otros sistemas y dispositivos.

La red 110 puede consistir en, por ejemplo una red de área local (LAN, por sus siglas en inglés) o una red de área extensa (WAN, por sus siglas en inglés). Tales entornos de red pueden utilizarse en oficinas, redes informáticas en toda una empresa, intranets e Internet. Cuando se utiliza una red LAN como la red 110, puede utilizarse una interfaz de red ubicada en cualquiera de los procesadores para interconectar cualquiera de los procesadores. Cuando la red 110 se implementa en un entorno de red WAN, tal como Internet, los procesadores normalmente

pueden incluir un módem interno o externo (no se muestra) u otros elementos para establecer comunicaciones por la red WAN. Además, al utilizar la red 110, los datos enviados a través de la red 110 pueden cifrarse para garantizar la seguridad de los datos utilizando técnicas de cifrado/decodificación.

Además de utilizar un sistema de comunicaciones de línea 110, puede utilizarse un sistema de comunicaciones inalámbrico, o una combinación de sistema de línea e inalámbrico como la red 110 para, por ejemplo, intercambiar páginas web por Internet, intercambiar correos electrónicos por Internet o para utilizar otros canales de comunicaciones. Puede definirse inalámbrico como la transmisión de radio a través de ondas de aire. Sin embargo, pueden utilizarse otras técnicas de comunicaciones diferentes para proporcionar transmisión inalámbrica, incluyendo por infrarrojos con línea de visión directa, celular, microondas, satelital, radiotransmisión de paquetes y radio de espectro ensanchado. Los procesadores en el entorno inalámbrico pueden ser cualquier terminal móvil, tal como los terminales móviles descritos con anterioridad. Los datos inalámbricos pueden incluir, pero no se limitan a, localización, mensajes de texto, correos electrónicos, acceso a Internet y otras aplicaciones de datos especializadas con o sin transmisión de voz. Por ejemplo, los procesadores pueden comunicarse a través de una interfaz inalámbrica, como por ejemplo, una interfaz celular (por ejemplo, un sistema general de paquetes vía radio (GPRS, por sus siglas en inglés), Velocidades de Datos Mejoradas para la evolución de GSM (EDGE, por sus siglas en inglés), sistema global para comunicaciones móviles (GSM, por sus siglas en inglés)), una interfaz de red de área local inalámbrica (por ejemplo, WLAN, IEEE 802, WiFi, WiMax), una interfaz bluetooth, otra interfaz de comunicaciones por RF y/o una interfaz óptica.

El sistema 100 también puede transmitir datos mediante métodos y procesos diferentes a, o en combinación con, la red 110. Estos métodos y procesos pueden incluir, pero no se limitan a, la transferencia de datos a través de disquetes, tarjetas de memoria, CD/DVD ROM, fax, correo convencional, un sistema de respuesta de voz interactiva (IVR, por sus siglas en inglés), o mediante voz a través de una red telefónica pública conmutada.

La figura 4 es un diagrama de flujo que establece las etapas generales involucradas en un método 400 para determinar intrusiones al recinto y otra información del recinto. El método 400 puede implementarse utilizando un procesador 115 o controlador 125 como se describe en más detalle con referencia a la figura 1. Formas de implementar las etapas del método 400 se describirán en más detalle con posterioridad. El método puede comenzar en el bloque inicial 405 y proceder al paso 410 donde el controlador 125 puede recibir datos de una pluralidad de sensores 120 ubicados dentro de un recinto (por ejemplo, el contenedor 105). Por ejemplo, al menos uno de la pluralidad de sensores puede consistir en al menos uno de los siguientes tipos de sensores: ultrasónico, acústico, de línea de transmisión electromagnética (EMTL), movimiento del contenedor, detección de humanos y estado de la puerta, como se describe, por ejemplo, en más detalle a continuación.

Del paso 410, donde el controlador 125 recibe los datos desde la pluralidad de sensores 120 ubicada dentro del recinto, el método 400 puede avanzar al paso 420 donde el controlador 125 puede analizar los datos para determinar si ha ocurrido un evento de intrusión al recinto. Por ejemplo, el análisis de los datos puede incluir determinar si el evento de intrusión al recinto comprende al menos uno de los siguientes: el recinto ha sido penetrado, cualquiera de la pluralidad de sensores ha sido manipulado, y se ha detectado la presencia de un humano en el recinto. Además, puede utilizarse la fusión de sensores, como se describe en más detalle a continuación, para analizar los datos.

Una vez que el controlador 125 analiza los datos para determinar si ha ocurrido el evento de intrusión al recinto en el paso 420, el método 400 puede continuar al paso 430 donde el controlador 125 puede emitir una alerta si se determina que ha ocurrido el evento de intrusión. Por ejemplo, emitir la alerta puede consistir en emitir la alerta indicando los contenidos del recinto y la ubicación del recinto. Los contenidos del recinto pueden determinarse mediante etiquetas de identificación por radio frecuencia (RFID) ubicadas en los contenidos del recinto. Además, la ubicación del recinto puede determinarse mediante un sensor de movimiento ubicado en el recinto como se describe con posterioridad. Después de que el controlador 125 emite la alerta en el paso 430, el método 400 puede terminar en el paso 440.

Detección ultrasónica de transgresión de la seguridad

Los sensores ultrasónicos dentro de los sensores 120 pueden operarse como un subsistema ultrasónico de detección de transgresión de la seguridad, utilizado en combinación con los medios de detección de la invención. El subsistema ultrasónico de detección de transgresión de la seguridad puede comprender, como se indica con anterioridad, ultrasónicos activos, pasivos y/o una combinación de ultrasónicos activos y pasivos utilizando el mismo conjunto de sensores ultrasónicos. Pueden montarse múltiples sensores ultrasónicos en cada superficie del contenedor. En el modo pasivo, cada sensor puede monitorear de manera independiente, por ejemplo, señales ultrasónicas entre aproximadamente 50kHz y 500kHz. Estas señales pueden analizarse mediante el controlador 125 o el procesador 115, por ejemplo, en el dominio de frecuencia en términos de relaciones de energías en diferentes bandas de frecuencia. Cada una de estas relaciones, por ejemplo, puede indicarse como una característica, y puede definirse como se indica a continuación:

$$\text{Característica } (f_1, f_2, f_3, f_4) = 10 \log_{10} \left[\frac{\int_{f_1}^{f_2} X^2(f) df}{\int_{f_3}^{f_4} X^2(f) df} \right]$$

5 Aquí, f_1 , f_2 , f_3 y f_4 pueden delinear los rangos de frecuencia de interés. Múltiples características pueden fusionarse para discriminar sonidos provocados por transgresiones de la seguridad de sonidos no peligrosos (es decir, que no indiquen transgresiones de la seguridad). Además, estas señales pueden analizarse mediante el controlador 125 o procesador 115 en, por ejemplo, el dominio de tiempo o tiempo-frecuencia.

10 En el modo activo, pueden operar sensores ultrasónicos, por ejemplo, en pares de transceptores donde la señal recibida consulte la superficie del contenedor para buscar evidencia de una transgresión de la seguridad. Las señales pueden compararse con referencias, tanto fijas como adaptativas, para detectar cambios que pueden indicar una transgresión de la seguridad. Estas señales, por ejemplo, pueden analizarse mediante el controlador 125 o procesador 115 en el dominio de frecuencia, tiempo o tiempo-frecuencia en el modo activo. En el dominio de tiempo, la coherencia temporal local (también conocida como la correlación cruzada normalizada local) puede ser una medición de cambios que sean sensibles a cambios en la forma de onda pero no tiempos de llegada; puede darse en las ecuaciones a continuación:

$$R_{xy}^T(\tau, t) = \frac{1}{T} \int_{t-\frac{T}{2}}^{t+\frac{T}{2}} x(s)w(s-t)y(s+\tau)w(s+\tau-t)ds$$

$$\gamma_{xy}^T(\tau, t) = \frac{R_{xy}^T(\tau, t)}{\sqrt{R_{xx}^T(0, t)R_{yy}^T(0, t)}}$$

= Coherencia temporal local

$$C_{xy}(t) = \max_{\tau} |\gamma_{xy}^T(\tau, t)|$$

= Coherencia máxima

$$P = \overline{1 - C_{xy}(t)}$$

15 Aquí el parámetro P , que puede calcularse a partir de la coherencia temporal local, puede utilizarse para evaluar cambios entre dos señales y así detectar una transgresión de la seguridad.

20 Un subsistema ultrasónico de detección de transgresión de la seguridad 500, que se muestra en la figura 5, comprende un controlador 505 de procesamiento de señal digital (DSP, por sus siglas en inglés), un trayecto de adquisición para la adquisición de datos ultrasónicos pasivos, un trayecto de adquisición para la adquisición de datos ultrasónicos activos, y enlaces de comunicación con el controlador 125. El subsistema ultrasónico de detección de transgresión de la seguridad 500 puede tener tres modos de operación para reducir el consumo de energía: (1) un modo de reposo donde todo el subsistema puede colocarse en un estado de energía casi cero; (2) un estado de energía mínima donde sólo las funciones ultrasónicas pasivas pueden ser operativas; y (3) un estado de energía superior durante interrogaciones ultrasónicas activas. El subsistema ultrasónico de detección de transgresión de la seguridad 500 puede ubicarse en una placa de circuito impreso en un recinto principal para componentes electrónicos salvo los sensores ultrasónicos 510 que se muestran en más detalle en la figura 5. Cada uno de los sensores ultrasónicos 510 puede comprender un elemento piezoeléctrico activo 605 combinado con componentes electrónicos de sensor que pueden integrarse en un estuche moldeado. Los componentes electrónicos de sensor pueden incluir un generador de impulsos miniaturizado y un amplificador receptor 615 para la operación activa y pasiva. El diseño puede incorporarse enviando energía y señales a través de tres líneas que se muestran conectadas al sensor ultrasónico 510 en la figura 6.

35 Para la operación pasiva, puede proporcionarse energía a la línea izquierda inferior en la figura 6 para energizar sólo el amplificador receptor pasivo, por ejemplo. Las señales ultrasónicas pasivas pueden transmitirse a un banco de filtros de frecuencia /comparadores de muestreo y retención 515 en el subsistema de detección de transgresión de la seguridad ultrasónico 500 que se muestra en la figura 5. Como una opción, DSP 505 puede energizar después las otras dos líneas a la izquierda en la figura 6 y utilizar el trayecto de datos ultrasónicos activos para digitalizar señales ultrasónicas pasivas en caso de que se requieran características de señales más complejas.

Para la operación activa, la energía puede bloquearse a los componentes electrónicos ultrasónicos pasivos (línea inferior a la izquierda en la figura 6) y suministrarse a las dos líneas (dos líneas superiores a la izquierda en la figura 6) que pueden energizar y proporcionar señales de control al generador de impulsos ultrasónicos activos 610 y receptor 615. Los circuitos de componentes electrónicos activos para cada sensor 510 pueden configurarse, por ejemplo, como generador de impulsos solamente, generador de impulsos/receptor o receptor solamente. Para la operación ultrasónica activa normal, cada sensor 510 puede configurarse como un generador de impulsos o como un receptor. El modo de operación generador de impulsos/receptor (impulso/eco) puede retenerse para asistir con el diagnóstico del subsistema de sensores y la posible utilización del sistema en un modo degradado de operación con sólo un sensor.

Entre 4 y 8 sensores ultrasónicos pueden integrarse juntos en ensamblajes de cable moldeado prefabricados con elementos transductores y electrónicos empaquetados como elementos con forma de "botón" moldeados en puntos de sujeción de sensores y bifurcación de cables. Los cables pueden estar incluidos en un mazo de cables blindado con forro de goma.

Detección de transgresión de la seguridad electromagnética

La detección ultrasónica de transgresión de la seguridad antes mencionada puede no ser efectiva en suelos del contenedor hechos de, por ejemplo, material no metálico tal como contrachapado ya que las ondas ultrasónicas pueden no propagarse bien en materiales no metálicos (por ejemplo, madera). Además, el suelo puede estar sujeto a amenazas habituales y no habituales adicionales, tales como penetraciones de clavos utilizados para asegurar el cargamento que no ocurren en otras superficies como las paredes o el techo. Por lo tanto, de manera consistente con realizaciones de la invención, puede utilizarse un proceso de línea de transmisión electromagnética (EMTL) en el suelo del contenedor 105. El proceso EMTL puede utilizarse sobre cualquier material en el cual las ondas ultrasónicas no se propaguen bien.

De manera consistente con realizaciones de la invención, transgresiones de la seguridad mayores a nueve pulgadas cuadradas de superficie pueden detectarse con una probabilidad de detección mayor al 82% y dentro de los dos minutos de la ocurrencia. La tasa de falsa alarma correspondiente es menor a 0,003 falsas alarmas por viaje. El sensor EMTL puede ser apropiado para la instalación en contenedores nuevos y usados en menos de dos horas para, por ejemplo, permitir una utilización generalizada. Debido a las amenazas de características únicas impuestas al suelo, un sensor EMTL puede no ser sensible a los clavos insertados a través del suelo para asegurar el cargamento, daños en el suelo asociados al uso habitual, y condiciones de carga. El entorno marítimo puede requerir que el sensor no sea sensible a la humedad en el contenedor ni al contenido de humedad en el suelo. El consumo general de energía promedio puede ser menor a 70mW.

El sensor EMTL puede comprender una rejilla de cintas conductoras paralelas que pueden estar instaladas en el suelo del contenedor 105 entre dos secciones de contrachapado para formar una línea de transmisión electromagnética. El espaciado de los conductores y la construcción de la rejilla puede ser tal que colocar clavos en el suelo u otros daños asociados con la utilización habitual pueden no alterar de manera significativa (por ejemplo, ni mediante la interrupción ni mediante el corte) los conductores en la rejilla. Sin embargo, hacer un orificio, por ejemplo, con una superficie mayor de nueve pulgadas cuadradas puede romper la rejilla y cambiar de este modo las características de la línea de transmisión. Estos cambios pueden detectarse mediante la medición del patrón de onda estacionaria de tensión en la línea de transmisión. Un patrón de onda estacionaria puede inducirse en una línea de transmisión cuando es conducida a una frecuencia constante y pueden ocurrir reflexiones en el final de la línea. Este patrón puede caracterizarse por la ubicación de los puntos de tensión máxima y mínima, la separación entre esos puntos, y la relación entre los valores de tensión máxima y mínima, que se conoce como VSWR (relación de onda estacionaria de tensión). Estas características de transmisión pueden medirse mediante la detección de la tensión en la línea en diferentes ubicaciones a lo largo de la rejilla en varias frecuencias diferentes. Estas frecuencias pueden aplicarse como ráfagas de RF cortas en el rango de frecuencia de 1MHz a 50MHz como se muestra en la figura 7. El ciclo de trabajo para la generación de señal puede ser aproximadamente 0,001%. Por lo tanto, el consumo de energía promedio en el tiempo para este ejemplo puede ser menor a 500µW para un suelo completamente instrumentado en un contenedor de 40 pies, por ejemplo.

Cada interrogación del sensor EMTL puede utilizar varias frecuencias predeterminadas seleccionadas de manera aleatoria de una base de datos interna. El controlador 125 puede consultar los detectores de valores máximos y comparar los valores con umbrales apropiados para cada frecuencia. Cuando se detectan diferencias que pueden indicar una potencial transgresión de la seguridad, pueden generarse frecuencias adicionales para caracterizar completamente la rejilla. Este patrón puede compararse con datos almacenados previamente para determinar si ha ocurrido una transgresión de la seguridad. Puede utilizarse un algoritmo de tasa de cambio para añadir robustez a este proceso de detección. Si los resultados indican que ha ocurrido una transgresión de la seguridad, puede generarse una condición de alarma junto con un nivel de seguridad para esa alerta. El análisis antes mencionado puede realizarse mediante el controlador 125, el procesador 115 o cualquier elemento capaz de realizar esta función.

El diseño para este subsistema EMTL se ilustra en la figura 8. Un generador de frecuencia controlado 805 puede utilizarse para crear señales de RF que conducen las líneas de transmisión en una rejilla EMTL 810. La rejilla EMTL 810 puede comprender conductores paralelos (por ejemplo, líneas de transmisión) que pueden estar espaciados de modo tal que la rejilla EMTL 810 pueda satisfacer, por ejemplo, el objetivo de detección de transgresión de la seguridad de nueve pulgadas cuadradas antes expuesto mientras se minimizan las falsas alarmas. El objetivo de detección de transgresión de la seguridad de nueve pulgadas cuadradas es un ejemplo y pueden utilizarse otros objetivos. Pueden utilizarse múltiples amplificadores de detección de voltaje 815 con detectores de valores máximos 820 para medir la tensión, por ejemplo, en la rejilla EMTL 180 en diferentes puntos del suelo. Estas mediciones pueden procesarse mediante el procesador 115, controlador 125 o un controlador EMTL 825 que puede contener memoria para almacenar interrogaciones de rejilla anteriores.

Un diagrama de bloques del hardware que ilustra un ejemplo del diseño de hardware para un subsistema EMTL 900 se muestra en la figura 9. Por ejemplo, después de que el controlador 905 selecciona cada frecuencia de interrogación, puede generarse una forma de onda corta de tal frecuencia y almacenarse en un componente FIFO 910. Una vez que la forma de onda completa se ha almacenado en el componente FIFO 910, puede convertirse en una señal analógica mediante un conversor digital a analógico 915 y acoplarse en una rejilla de línea de transmisión 920. Diferentes puntos en la rejilla de línea de transmisión 920 pueden conectarse a una matriz de conmutación 925 que puede efectuar un ciclo por cada punto de medición. La señal de cada punto seleccionado puede pasarse a través de un amplificador de frecuencia controlado 930 que puede amplificar la señal de interés y bloquear el ruido de banda. Un circuito de muestreo y retención 935 puede utilizarse para acumular la salida del amplificador de frecuencia controlado 930 hasta que la forma de onda se ha transmitido completamente. Ese circuito puede conectarse a un conversor analógico-digital (A/D) 940 que puede digitalizar el valor de la señal almacenado del circuito de muestreo y retención 935 y pasarlo al controlador 905. El controlador 905 puede comparar el resultado con los valores de mediciones previas a la misma frecuencia para determinar si se ha producido una transgresión de la seguridad.

25 Detección de movimiento en el contenedor

En combinación con los medios de detección de la invención, la detección de cualquier movimiento del contenedor 105, ya sea que el movimiento se produzca, por ejemplo, por tren, barco o camión, puede lograrse mediante el monitoreo continuo de la velocidad horizontal del contenedor 105. Por ejemplo, el procesador 115 o controlador 125 pueden registrar cambios en el estado de movimiento del contenedor 105 donde una velocidad umbral (por ejemplo, 1 milla/hora) puede determinar si el contenedor 105 se mueve o no.

La velocidad puede medirse, por ejemplo, realizando mediciones de reemplazo de la distancia o aceleración y diferenciando o integrando, respectivamente, aquellos valores con respecto al tiempo. Por ejemplo, los valores de aceleración pueden utilizarse para calcular la velocidad. Dos acelerómetros pueden orientarse de modo tal que sus ejes de detección sean ortogonales uno al otro y horizontales con respecto al suelo. Los dos componentes de aceleración medidos pueden integrarse con respecto al tiempo y los componentes de velocidad resultantes se utilizan para calcular la raíz cuadrada de la suma de los cuadrados para obtener la velocidad. Los acelerómetros utilizados, por ejemplo, puede tener un rango de medición de $\pm 2g$ y anchos de banda de frecuencia de 50-60Hz. Si el consumo de energía es fundamental, los acelerómetros capacitivos con micromaquinado superficial pueden proporcionar el menor consumo de energía y satisfacer cualquier requerimiento de medición.

Los sensores de velocidad basados en acelerómetros pueden sufrir errores de deriva de velocidad, la magnitud de los cuales puede incrementarse con el tiempo. Esta deriva puede producirse por errores sistemáticos de gravedad nula que pueden depender de la temperatura. La magnitud del error puede variar de un acelerómetro a otro. Por lo tanto, los acelerómetros utilizados para la navegación inercial pueden utilizarse como refuerzos temporarios de otros sensores más precisos tales como los que utilizan el sistema de posicionamiento global (GPS, por sus siglas en inglés) que pueden ser menos propensos a pérdidas de medición. En aplicaciones donde el acelerómetro puede ser el sensor principal, puede utilizarse otra entrada de sensor para corregir periódicamente el valor medido (por ejemplo, realizando mediciones a distancia a los alrededores o rastreando mediante movimiento los objetos en imágenes de vídeo). Cuando no se utilizan sensores externos al contenedor 105, la corrección de cualquier error que depende de la temperatura puede lograrse mediante la detección de la temperatura del acelerómetro y la corrección de la señal medida en el software. En escalas de tiempo corto, los errores de velocidad de fuentes de ruido y acoplamiento cruzado de componentes de aceleración pueden corregirse con filtración digital de frecuencia muy baja.

Un diagrama de bloques de un subsistema de detección de movimiento del contenedor 1000 se muestra en la figura 10. El controlador 1005 para el subsistema puede ser responsable de sincronizar las mediciones de temperatura y aceleración y el cálculo de la corrección de errores de desviación de gravedad nula y velocidad. La figura 11 es un diagrama de flujo de un método 1100 para la detección de movimiento del contenedor que puede realizarse en software ejecutado, por ejemplo, en el procesador 115, o el controlador 125, o ambos. El método 1100 es un ejemplo y pueden utilizarse otros procesos.

Detección de humanos

En combinación con los medios de detección de la invención, la detección de presencia de animales o humanos dentro del contenedor 105 puede lograrse monitoreando la tasa de cambio de concentración de CO₂ de la atmósfera interior del contenedor 105. Las mediciones de la concentración de CO₂ pueden realizarse mediante el sistema 100 cada 10 minutos. Si la concentración de CO₂ incrementa de modo tal que durante el transcurso de dos horas, por ejemplo, se excede un umbral de tasa de cambio, el sistema 100 puede iniciar una alerta de evento de detección de humanos. El umbral de tasa de cambio puede comprender, por ejemplo, 3,3%/min. y 1,6%/min. para contenedores de 20' y 40' respectivamente.

Los procesos utilizados para medir la concentración de CO₂ pueden basarse en un proceso de análisis infrarrojo no dispersivo (NDIR, por sus siglas en inglés) de detección de gas. En el proceso NDIR, la luz IR de la fuente de banda ancha, tal como un filamento calentado, puede pasarse a través de una muestra de la mezcla de gas a analizarse, y detectarse con dos fotodetectores separados. Toda molécula de CO₂ dentro de la mezcla de gas puede absorber radiación IR que tiene longitudes de onda entre 4,18 y 4,33µm como se muestra en el gráfico en la figura 12. La cantidad de radiación absorbida puede depender de la concentración de CO₂ dentro de la mezcla de gas y la longitud del trayecto óptico de la luz cuando pasa a través de la muestra de gas y llega a uno de los fotodetectores. Pueden utilizarse filtros ópticos de paso banda con cada fotodetector para aislar diferentes partes del espectro de luz. El paso banda de un filtro puede confinarse a la banda de absorción de CO₂ antes mencionada mientras que el paso banda del otro filtro puede centrarse en 3,6µm. Dado que el CO₂ puede no absorber la energía en esta segunda longitud de onda, esta respuesta del fotodetector puede utilizarse como un valor testigo para medir la transmisión óptica ambiente de la mezcla de gas. Una relación de las respuestas eléctricas de los dos fotodetectores puede estar relacionada directamente con la concentración de CO₂ de la mezcla de gas y ser independiente de la transmisión de la mezcla de gas.

En lugar de una fuente IR de banda ancha y dos fotodetectores filtrados, otras realizaciones pueden incluir un subsistema de detección humano 1300 que puede utilizar dos fuentes LED IR de onda media (MWIR, por sus siglas en inglés) y un fotodetector no filtrado para detectar la luz transmitida como se muestra en la figura 13. Un LED MWIR 1305 puede emitir a 4,2µm y otro LED MWIR 1310 puede emitir a 3,6µm donde el fotodetector tiene suficiente sensibilidad en ambas longitudes de onda. Una vez más, una relación entre la respuesta del fotodetector a la radiación 4,2µm transmitida y la respuesta a 3,6µm puede estar directamente relacionada con la concentración de CO₂ de la mezcla de gas. Un beneficio de este proceso para la detección de CO₂ frente al proceso precedente que se describe con anterioridad es que puede reducirse el consumo de energía promedio. Por ejemplo, LED MWIR 1305 y 1310 puede ser pulsado brevemente durante cada periodo de medición a diferencia de la fuente de filamento calentado que puede requerir un tiempo de calentamiento de alrededor de varios segundos de duración. Otro beneficio de este enfoque puede ser que el rango de temperatura de operación puede ser mucho mayor que en los procesos antes mencionados.

La figura 14 muestra una transmisión del trayecto de 10cm calculada para una banda de absorción de CO₂ de 4,3µm. La longitud del trayecto óptico que separa los LED del fotodetector puede ser de 10cm. Para esta longitud de trayecto, la transmisión en la banda de absorción de 4,3µm puede variar linealmente con la concentración de CO₂ como se muestra en la figura 14. Un incremento de 50ppm en CO₂ puede resultar en una disminución de 1% en la transmisión que puede requerir un SNR de 20dB para detectarlo.

Un controlador 1315 para el subsistema de detección de humanos 1300 puede ser responsable de sincronizar tanto los eventos de impulso LED como la digitalización de las señales de respuesta del fotodetector y de calcular la concentración de CO₂. Un diagrama de flujo de un método 1500 para la operación del subsistema de detección de humanos 1300 se muestra en la figura 15. El método 1500 puede implementarse en software, por ejemplo, mediante el controlador 125 o procesador 115; sin embargo, pueden utilizarse otros métodos. Además de la medición de la respuesta del fotodetector a los eventos de impulso LED, la respuesta al nivel de luz de fondo precedente a los eventos de impulso LED puede medirse para eliminar el valor de señal de fondo de los valores de señal del evento de impulso durante el cálculo de la transmisión de banda de absorción de CO₂.

Detección del estado de la puerta

En combinación con los medios de detección de la invención, puede proporcionarse un sensor óptico en una puerta dentro de un subsistema de estado de puerta 1600 como se muestra en la figura 16. El subsistema de estado de puerta 1600 puede utilizarse para detectar el estado de la puerta en el contenedor 105. Un enfoque óptico puede proporcionar varias ventajas, incluyendo un consumo de energía muy bajo, alta probabilidad de detección y resistencia a la manipulación, por ejemplo. Un sensor de puerta puede comprender dos componentes que pueden estar montados en la interfaz puerta-contenedor. Un componente puede montarse en la puerta del contenedor 105. Este componente puede incluir un transmisor LED de baja divergencia 1605 que opera a una longitud de onda de 950nm junto con el circuito impulsor 1610 para el LED. Un controlador de subsistema 1615, que puede estar conectado al transmisor mediante un cable ubicado debajo de la puerta, puede generar un impulso digital cada vez que se supone que el transmisor debe estar activado. Después de recibir un impulso del controlador 1615, el circuito

impulsor 1610 puede proporcionar un impulso de corriente individual al LED 1605 que puede ser de un microsegundo de duración y 100 miliamperios de amplitud. La duración y amplitud de esta señal puede ajustarse a través de pequeños cambios en el diseño del circuito impulsor 1610. Debido a que la combinación de LED 1605/circuito impulsor 1610 puede ser capaz de transmitir impulsos cortos a frecuencias relativamente altas, el controlador del subsistema 1615 puede generar códigos de impulsos variados de manera aleatoria que pueden hacer que se sustituya una fuente falsa para permitir que la puerta se abra sin que se detecte.

Un segundo componente puede montarse en la pared del contenedor 105. El segundo componente puede incluir un fotodiodo de silicio de bajo perfil 1620 que puede ser sensible a la longitud de onda del LED 1605. Cuando la puerta está en posición cerrada, la luz del transmisor (es decir, el primer componente) puede incidir en el detector (es decir, el segundo componente). Cuando la puerta se abre, el ángulo de incidencia entre el transmisor y el receptor puede incrementarse de manera proporcional al incremento en ángulo entre la puerta y la interfaz de puerta. Este cambio en el ángulo puede explotarse a través de la utilización de un revestimiento de película de control de luz 1650 en el receptor como se muestra en más detalle en la figura 17. La película de control de luz 1650 puede comprender dos láminas plásticas delgadas que intercalan rejillas verticales pequeñas entre ellas.

La película de control de luz 1650 puede hacer que la salida del fotodiodo 1620 dependa en gran medida del ángulo de incidencia entre el transmisor y el receptor. Como resultado, la salida del receptor puede reducirse rápidamente a medida que se abre la puerta y el ángulo entre el transmisor y el receptor disminuye. Este cambio en la salida del receptor puede medirse de manera electrónica y compararse con un valor umbral almacenado para determinar si la puerta se ha abierto. El valor umbral, por ejemplo, puede basarse en una abertura de 44mm que puede permitirse debido al apilado de contenedores. Una abertura de 44mm puede traducirse en un ángulo de dos grados entre la puerta y la interfaz del contenedor. Un cambio de dos grados en el ángulo de incidencia puede resultar en un cambio en la salida del receptor de aproximadamente 5%, que puede estar en un rango detectable para este sensor. La utilización de un valor umbral puede permitir ajustes simples si la experiencia operativa indica que 44mm no es una desviación adecuada debido al apilado de contenedores. Además, la dependencia angular puede ocurrir en una sola dirección, lo cual puede reducir los requerimientos de alineación para los sensores instalados. Para poder comparar la salida del receptor con el valor umbral, primero puede amplificarse mediante un amplificador 1625 y después convertirse en una señal digital utilizando un conversor de analógico a digital 1630. Un conversor A/D 1630 puede conectarse directamente al controlador 1615 que puede realizar el procesamiento.

Para minimizar los efectos del apilado de contenedores, los sensores pueden instalarse en el mismo lugar que las bisagras de las puertas dado que la bisagra puede limitar el movimiento de la puerta. Pueden utilizarse múltiples sensores (por ejemplo, tres sensores 1655, 1660 y 1665) en cada puerta para proporcionar redundancia en caso de fallas accidentales o maliciosas. Aunque algunos contenedores pueden utilizar más de tres bisagras, sensores adicionales no pueden proporcionar suficientes mejoras en la probabilidad de detección o falsa alarma que justifiquen el coste adicional. Los cables que conectan cada componente de sensor al controlador del subsistema 1615 pueden transportar tanto energía como señales digitales hacia y desde los sensores 1655, 1660 y 1665. Estos cables pueden ser parte de un mazo de cables para minimizar la complejidad de instalación. Pueden utilizarse cables blindados para reducir el riesgo de daños accidentales o intencionales al cable. El enrutado del cable en las partes corrugadas del contenedor 105 donde sea posible también puede limitar el impacto del cable en el contenedor.

Para minimizar la complejidad de la instalación, los dos componentes sensores pueden fabricarse como una parte física con un material plástico perforado que separa los dos sensores. Una vez que los sensores se han asegurado al contenedor, el plástico que mantiene las dos partes unidas puede cortarse y eliminarse, lo cual permitirá que la puerta se mueva libremente. Esta construcción puede asegurar que los sensores se alineen de manera adecuada durante la instalación. El empaquetado del sensor puede ser robusto pero no molesto para evitar afectar las operaciones del contenedor. Ambos componentes pueden empaquetarse en pequeños alojamientos metálicos que sean lo suficientemente resistentes para soportar impactos producidos por los movimientos de la carga en el contenedor. El diámetro del LED puede ser de 5mm y el grosor del fotodiodo puede ser de menos de 1mm. Esto puede permitir que cada componente sea de bajo perfil. Esta construcción, junto con la naturaleza curva de los alojamientos, puede reducir el riesgo de que el cargamento o el equipo de carga quite accidentalmente los sensores de la pared.

Como se muestra en la figura 18, el método 1800 puede describir un proceso para operar los sensores de estado de la puerta. Para evitar la introducción de un transmisor falso, puede utilizarse un código de impulsos generado de manera aleatoria para cada interrogación del sensor. Este código de impulsos puede comprender cuatro bits durante los cuales el transmisor puede estar encendido o apagado, lo cual da como resultado dieciséis combinaciones diferentes. Un impulso de arranque puede utilizarse para indicar el comienzo de una nueva interrogación además de los cuatro bits del código de impulsos. Después de que se ha transmitido el impulso de arranque, la salida del receptor puede amplificarse y convertirse en un valor digital mediante el conversor A/D. Si esta salida no excede el valor umbral mínimo, el estado de la puerta puede cambiarse a abierto y transmitirse al controlador 125. Si está por encima del mínimo, se transmite el resto del código de impulsos. Cada bit puede compararse con el nivel umbral para determinar si el bit transmitido estaba en estado de encendido o apagado. Después de que se ha transmitido

completamente el código de impulsos, el código de impulsos recibido puede compararse con el código de impulsos esperado en el controlador del subsistema 1615 para determinar si el código correcto se ha recibido. Si no se ha recibido el código correcto, puede generarse una alarma de manipulación para indicar que ha ocurrido un intento de derrotar el sistema. Un estado de abertura de la puerta sólo puede declararse si los tres sensores en una puerta dada indican que está abierta. Esto puede proporcionar más inmunidad contra errores del apilado de contenedores. Estos códigos de impulsos pueden generarse de una manera pseudoaleatoria de modo tal que el receptor conozca qué código esperar del transmisor en un momento dado. Esto puede eliminar la necesidad de conectar un cable entre el transmisor ubicado en la puerta y el receptor ubicado en la pared del contenedor.

Un esquema de modulación de generación pseudoaleatoria de números (GPAN) puede utilizarse para eliminar la necesidad de un cable que conecte el componente transmisor y el receptor y también para evitar la manipulación por medio de la introducción de una fuente LED externa. GPAN puede utilizar una secuencia pseudoaleatoria que puede poblarse en la fábrica y ser conocida sólo por el transmisor y receptor y puede permitir que el receptor conozca qué código se espera en un momento en particular sin una conexión por cables con el transmisor. La unidad transmisora puede generar una secuencia de bits pseudoaleatoria de larga longitud utilizando un registro de desplazamiento con retroalimentación lineal que puede incluir eventos de re-sincronización entrelazados de manera aleatoria. Estos eventos de re-sincronización pueden parecer una continuación del flujo de bits aleatorio generado normalmente, pero pueden ser reconocidos por el receptor y pueden permitir al receptor sincronizar con el flujo de bits transmitido sin necesidad de probar de manera exhaustiva todas las secuencias de bits posibles. La tasa promedio de eventos de re-sincronización puede controlarse mediante el diseño.

Fusión de sensores

Los datos del sensor ultrasónico pueden fusionarse en múltiples niveles (por ejemplo, tres) como se muestra en las figuras 19 y 20. En primer lugar, en el nivel del sensor, los sensores activos pueden fusionarse con datos del sensor de temperatura para obtener un resultado de sensor activo para cada superficie de contenedor (por ejemplo, paredes, techos, puertas). De manera similar, los datos de sensor pasivo pueden fusionarse para obtener un resultado pasivo para cada superficie. En segundo lugar, en el nivel de superficie, los resultados activos y pasivos pueden fusionarse. Finalmente, en el nivel del contenedor, los datos del sensor ultrasónico activo y pasivo de cada superficie pueden fusionarse con los resultados del sensor EMTL junto con información del sensor de movimiento y humedad para obtener un resultado general de transgresión de la seguridad del contenedor. Esta jerarquía de fusión se muestra en las figuras 19 y 20 donde el círculo con una "X" indica fusión. Los algoritmos de fusión reales pueden utilizar simples estrategias de votación o redes neuronales complejas por ejemplo.

Resistencia a la manipulación

En combinación con los medios de detección de la invención, pueden incorporarse mecanismos resistentes a la manipulación en cada uno de los subsistemas de sensores. Por ejemplo, el sensor de estado de la puerta puede utilizar un código óptico generado de manera aleatoria para evitar la introducción de un transmisor falso para estimular la señal de puerta cerrada. Otros subsistemas, incluyendo los sensores ultrasónicos y EMTL, pueden utilizar señales variables con el tiempo que pueden ser difíciles de falsificar. Además, el cableado puede contener un bucle de continuidad interno que puede interrogarse para garantizar que el cable sigue conectado apropiadamente. Esto puede proporcionar una alerta temprana en caso de que se produzca un intento de cortar un cable.

Pueden instalarse baterías del sistema en el controlador 125 para evitar su extracción por parte de personas no autorizadas. La alimentación del sistema puede activarse a través de un mecanismo de interruptor irreversible que puede evitar que el sistema sea apagado sin acceder a un controlador del alojamiento del recinto seguro. Además, todas las placas de circuito pueden tener recubrimientos protectores o estar embebidos en encapsulado para protección contra condiciones ambientales (por ejemplo, intencionales o no) y resistencia a la explotación y manipulación.

El controlador 125 puede estar ambientalmente sellado utilizando un proceso de moldeado con aire a presión para evitar problemas causados por gases o humedad. Además, el controlador 125 puede estar montado en el contenedor 105 utilizando una placa base fabricada a partir de aluminio balístico o un material similar que puede ser difícil de penetrar sin herramientas especializadas. La integridad del montaje del controlador 125 puede monitorearse utilizando un sensor similar a aquellos que son utilizados para detectar el estado de la puerta, y cualquier intento de penetración puede dar como resultado un informe de alerta.

En general, los módulos de programa pueden incluir rutinas, programas, componentes, estructuras de datos y otros tipos de estructuras que pueden realizar tareas particulares o que pueden implementar tipos de datos abstractos particulares. Además, las realizaciones de la invención y los medios de detección alternativos en combinación con ellas pueden realizarse con otras configuraciones de sistema informático, incluyendo dispositivos de mano, sistemas multiprocesadores, elementos electrónicos de consumidor programables o basados en microprocesador, miniordenadores, ordenadores centrales, y similares. Las realizaciones antes mencionadas también pueden realizarse en entornos informáticos distribuidos donde las tareas se realizan mediante dispositivos de procesamiento

remotos que se conectan a través de una red de comunicaciones. En un entorno informático distribuido, los módulos de programas pueden estar ubicados en dispositivos, locales o remotos, de almacenamiento de memoria.

Además, las realizaciones de la invención y los medios de detección alternativos utilizados en combinación con ellas pueden realizarse en un circuito eléctrico que comprende elementos electrónicos discretos, chips electrónicos integrados o empaquetados que contienen puertas lógicas, un circuito que utiliza un microprocesador, o un solo chip que contiene elementos electrónicos o microprocesadores. Las realizaciones antes mencionadas también se realizan utilizando otras tecnologías capaces de realizar operaciones lógicas, tales como, por ejemplo, Y, O y NO, incluyendo, pero sin limitarse a, tecnologías mecánicas, ópticas, fluidicas, y cuánticas. Además, las realizaciones antes indicadas pueden realizarse dentro de un ordenador para fines generales o en cualquier otro circuito o sistema.

Las realizaciones de la invención y los medios de detección alternativos utilizados en combinación con ellas, por ejemplo, pueden implementarse como un proceso informático (método), un sistema informático, o como un artículo de fabricación, tal como un producto de programa informático o soporte magnético. El producto de programa informático puede ser un medio de almacenamiento informático legible por un sistema informático y que codifica un programa informático de instrucciones para ejecutar un proceso informático. El producto de programa informático también puede ser una señal propagada en una portadora legible por un sistema informático y que codifica un programa informático de instrucciones para ejecutar un proceso informático. Por lo tanto, la presente invención, puede realizarse en hardware y/o software (incluyendo, firmware, software residente, microcódigo, etc.). En otras palabras, las realizaciones antes indicadas pueden tomar la forma de un producto de programa informático en un medio de almacenamiento legible por ordenador o utilizable por un ordenador que tiene un código de programa legible por ordenador o utilizable por un ordenador en el medio para su utilización por o en conexión con un sistema de ejecución de instrucciones. Un medio legible por ordenador o utilizable por un ordenador puede ser cualquier medio que contiene, almacena, comunica, propaga o transporta el programa para su utilización por o en conexión con el sistema de ejecución de instrucciones, aparato o dispositivo.

El medio legible por ordenador o utilizable por un ordenador puede ser, por ejemplo pero sin limitarse a, un sistema, aparato, dispositivo o medio de propagación electrónico, óptico, electromagnético, infrarrojo o semiconductor. Como ejemplos de medios legibles por ordenador más específicos (una lista no exhaustiva), el medio legible por ordenador puede incluir lo siguiente: una conexión eléctrica que tiene uno o más cables, un disquete portátil, una memoria de acceso aleatorio (RAM), una memoria de sólo lectura (ROM), una memoria de sólo lectura programable y borrrable (EPROM, por sus siglas en inglés, o memoria Flash), una fibra óptica, y un disco compacto de sólo lectura portátil (CD-ROM). Debe tenerse en cuenta que el medio legible por ordenador o utilizable por un ordenador podría ser papel o cualquier otro medio adecuado en el cual el programa está impreso, ya que el programa puede capturarse de manera electrónica, a través de, por ejemplo, el escaneado óptico del papel u otro medio, y después compilarse, interpretarse, o de otro modo procesarse de manera adecuada, si es necesario, y después almacenarse en una memoria para ordenador.

Las realizaciones de la invención y los medios de detección alternativos utilizados en combinación con ellas, por ejemplo, se describen con anterioridad con referencia a diagramas de bloques y/o ilustraciones operativas de métodos, sistemas y productos de programas informáticos según realizaciones de la invención. Las funciones/acciones indicadas en los bloques pueden ocurrir en un orden diferente del que se muestra en los diagramas de flujo. Por ejemplo, dos bloques mostrados de manera sucesiva pueden ejecutarse sustancialmente al mismo tiempo o a veces los bloques pueden ejecutarse en orden invertido, según las funciones/acciones involucradas.

Aunque se han descrito ciertas realizaciones de la invención, pueden existir otras realizaciones. Además, aunque las realizaciones de la presente invención se describieron como asociadas con datos almacenados en la memoria y otros medios de almacenamiento, los datos también pueden almacenarse en o leerse de otros tipos de medios legibles por ordenador, tales como dispositivos de almacenamiento secundarios, como discos duros, disquetes, o un CD-ROM, una onda portadora de Internet, u otras formas de RAM o ROM. Además, las etapas de los métodos revelados pueden modificarse de cualquier forma, incluso re-ordenando las etapas y/o insertando o borrando etapas, sin alejarse de la invención.

Mientras que la especificación incluye ejemplos, el alcance de la invención se indica mediante las siguientes reivindicaciones. Además, mientras que la especificación se ha descrito en un lenguaje específico de las funciones estructurales y/o acciones metodológicas, las reivindicaciones no se limitan a las funciones o actos descritos con anterioridad. En cambio, las funciones y acciones específicas descritas con anterioridad se revelan como ejemplo de las realizaciones de la invención.

REIVINDICACIONES

1. Método de determinación de transgresión de la seguridad de una estructura, el método comprende:
- 5 proporcionar a dicha estructura (105) un sensor (120) que comprende un primer elemento conductivo y un segundo elemento conductivo sustancialmente paralelo a dicho primer elemento conductivo, dichos primer y segundo elementos constituyen una línea de transmisión electromagnética;
- dirigir dicho sensor (120) con al menos una señal de frecuencia constante de modo tal que se induzca un patrón de onda estacionaria en el sensor (120) mediante la reflexión de dicha al menos una señal de frecuencia constante a partir de un punto de terminación del sensor;
- medir al menos una característica del sensor (120) causada por el patrón de onda estacionaria de tensión; y
- 10 determinar que ha ocurrido una transgresión de la seguridad en la estructura (105) cuando la al menos una característica medida difiere de un valor previamente determinado en una cantidad predeterminada.
2. Método conforme a la reivindicación 1, que comprende el primer elemento conductivo y el segundo elemento conductivo del sensor (120) en una configuración de rejilla.
3. Método conforme a la reivindicación 1, en donde el primer elemento conductivo y el segundo elemento conductivo están intercalados entre dos capas que comprenden la estructura (105).
- 15 4. Método conforme a la reivindicación 1, en donde determinar que la transgresión de la seguridad ha ocurrido comprende determinar que ha ocurrido una transgresión de la seguridad que consiste en una abertura mayor a nueve pulgadas cuadradas en la estructura (105).
5. Método conforme a cualquiera de las reivindicaciones precedentes, en donde medir la al menos una característica comprende medir al menos uno de los siguientes elementos: una ubicación de un punto de tensión máximo y una ubicación de un punto de tensión mínimo, la separación entre la ubicación del punto de tensión máximo y la ubicación del punto de tensión mínimo, y una relación entre una tensión máxima en el punto de tensión máximo y una tensión mínima en el punto de tensión mínimo.
- 20 6. Sistema de determinación de transgresión de la seguridad de una estructura, el sistema comprende:
- 25 un sensor (120) provisto en la estructura (105) que comprende un primer elemento conductivo y un segundo elemento conductivo sustancialmente paralelo a dicho primer elemento conductivo, dichos primer y segundo elementos constituyen una línea de transmisión electromagnética;
- un almacenamiento de memoria (330); y
- 30 una unidad de procesamiento (325) acoplada al almacenamiento de memoria (330), en donde la unidad de procesamiento (325) es operativa para:
- dirigir dicho sensor (120) con al menos una señal de frecuencia constante de modo tal que se induzca un patrón de onda estacionaria en el sensor (120) mediante la reflexión de dicha al menos una señal de frecuencia constante a partir de un punto de terminación del sensor;
- medir al menos una característica del sensor (120) causada por el patrón de onda estacionaria de tensión; y
- 35 determinar que ha ocurrido una transgresión de la seguridad en la estructura (105) cuando la al menos una característica medida difiere de un valor previamente determinado en una cantidad predeterminada.
7. Sistema conforme a la reivindicación 6, en donde el primer elemento conductivo y el segundo elemento conductivo están en una configuración de rejilla.
8. Sistema conforme a la reivindicación 6, en donde la estructura (105) consiste en un recinto.
- 40 9. Sistema conforme a la reivindicación 8, en donde la estructura (105) consiste en un contenedor de transporte.
10. Sistema conforme a la reivindicación 9, en donde la estructura (105) consiste en el suelo de un contenedor de transporte.

11. Sistema conforme a la reivindicación 10, en donde la estructura (105) consiste en el suelo de un contenedor de transporte que consta de uno de los siguientes materiales: madera y material no metálico.
12. Sistema conforme a la reivindicación 6, en donde el primer elemento conductor y el segundo elemento conductor están intercalados entre dos capas que comprenden la estructura.
- 5 13. Sistema conforme a la reivindicación 6, en donde la transgresión de la seguridad consiste en una abertura mayor a nueve pulgadas cuadradas en la estructura (105).
- 10 14. Sistema conforme a la reivindicación 6, en donde la al menos una característica comprende al menos uno de los siguientes elementos: una ubicación de un punto de tensión máximo y una ubicación de un punto de tensión mínimo, la separación entre la ubicación del punto de tensión máximo y la ubicación del punto de tensión mínimo, y una relación entre una tensión máxima en el punto de tensión máximo y una tensión mínima en el punto de tensión mínimo.

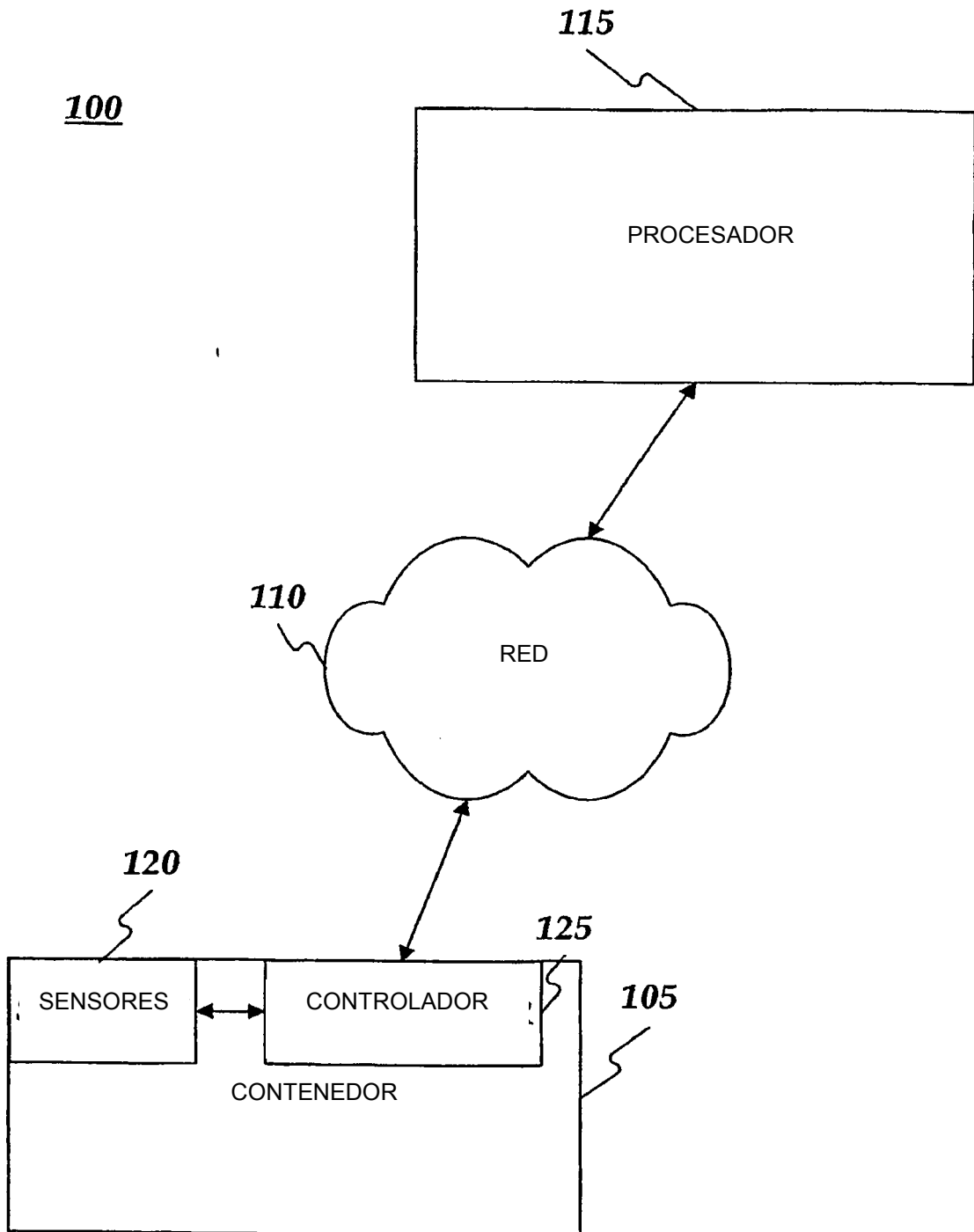


FIG. 1

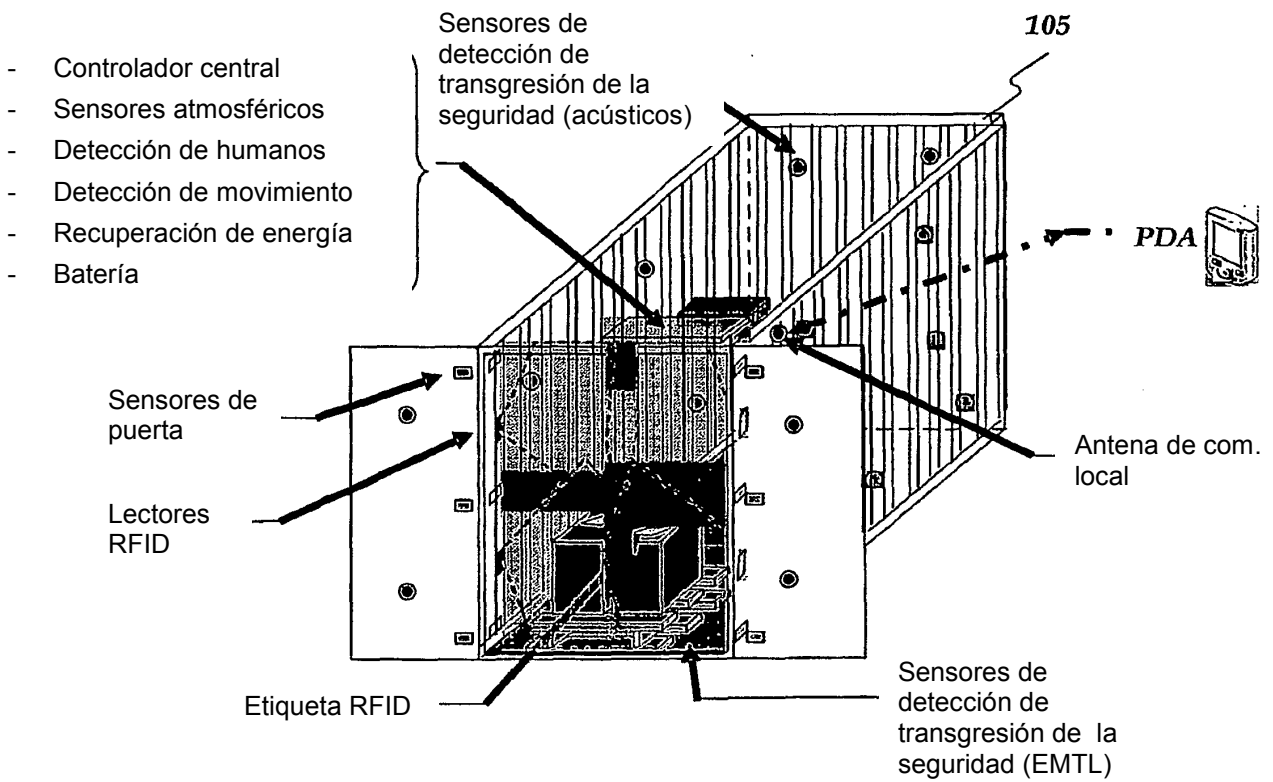


FIG. 2

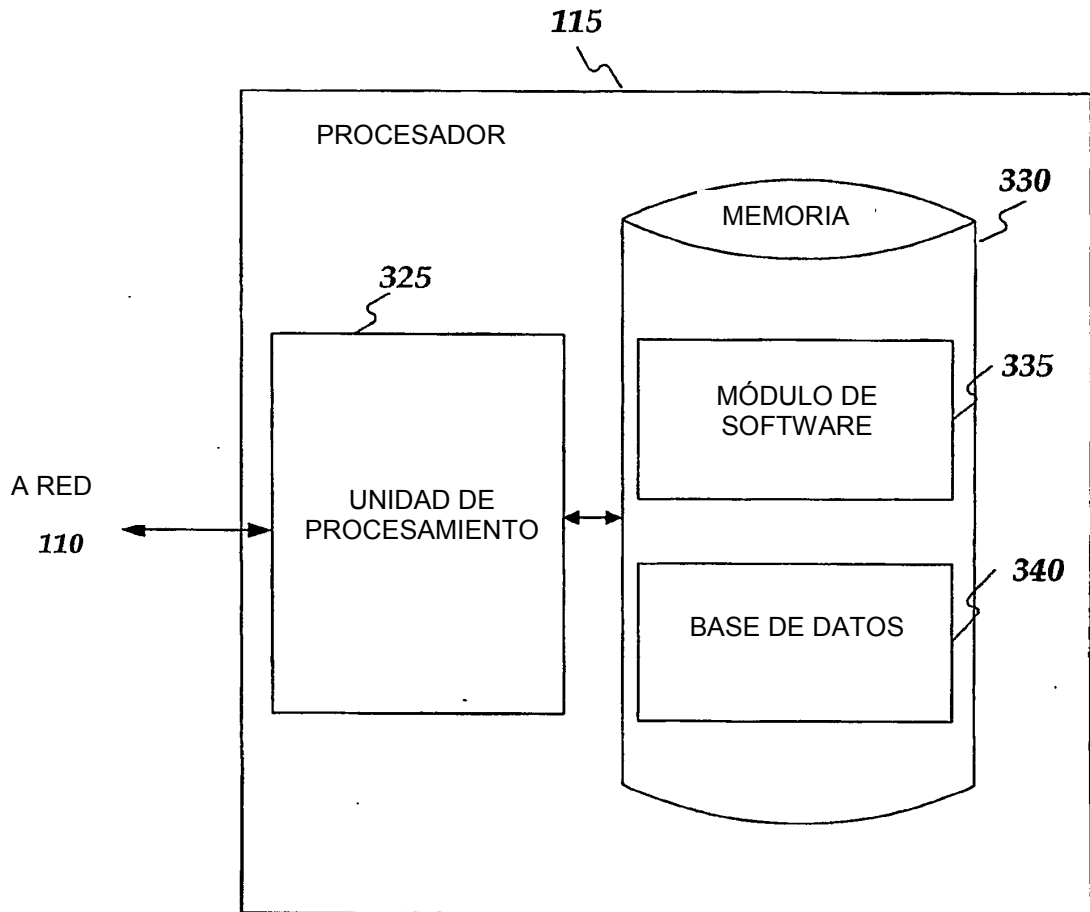


FIG. 3

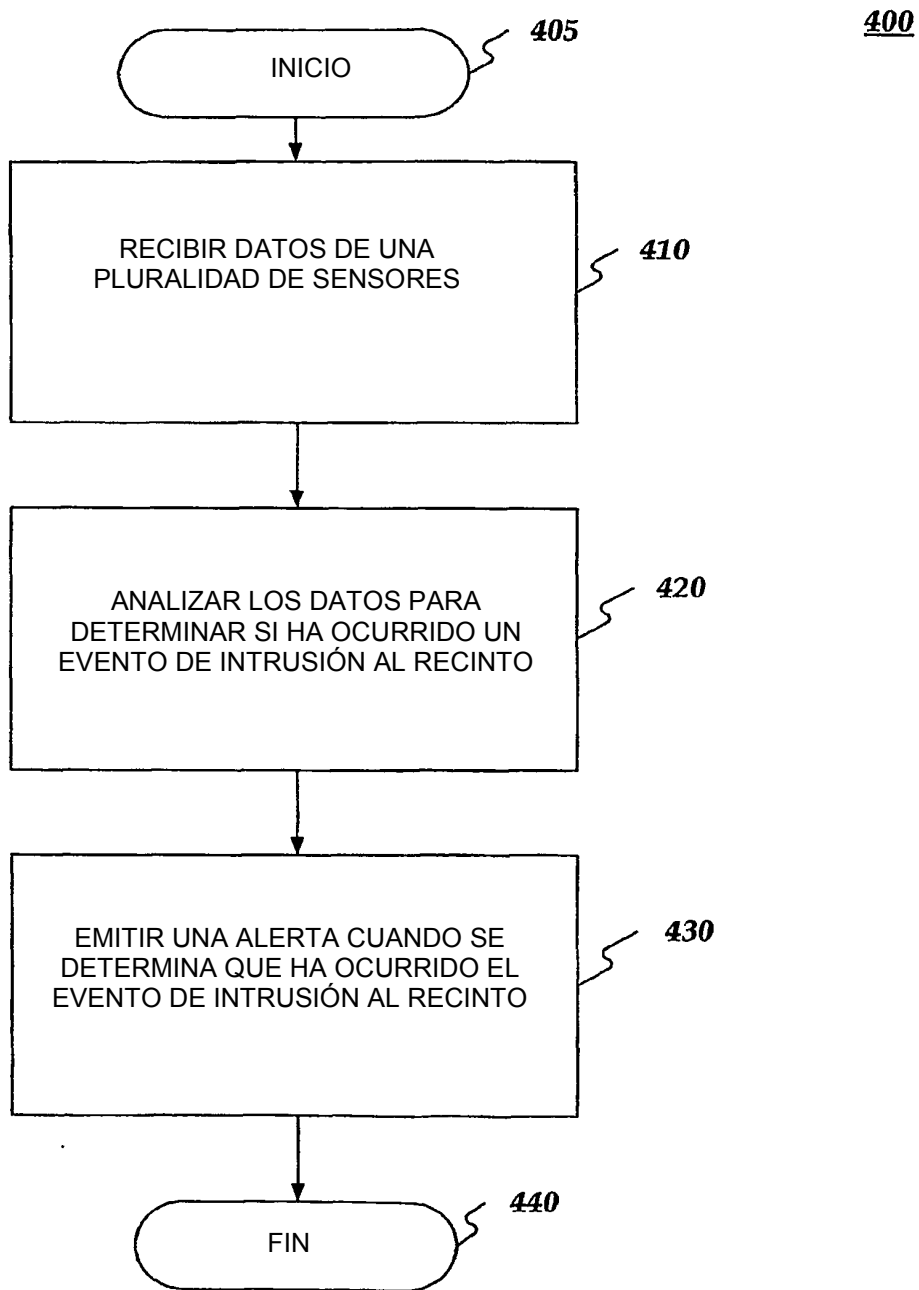


FIG. 4

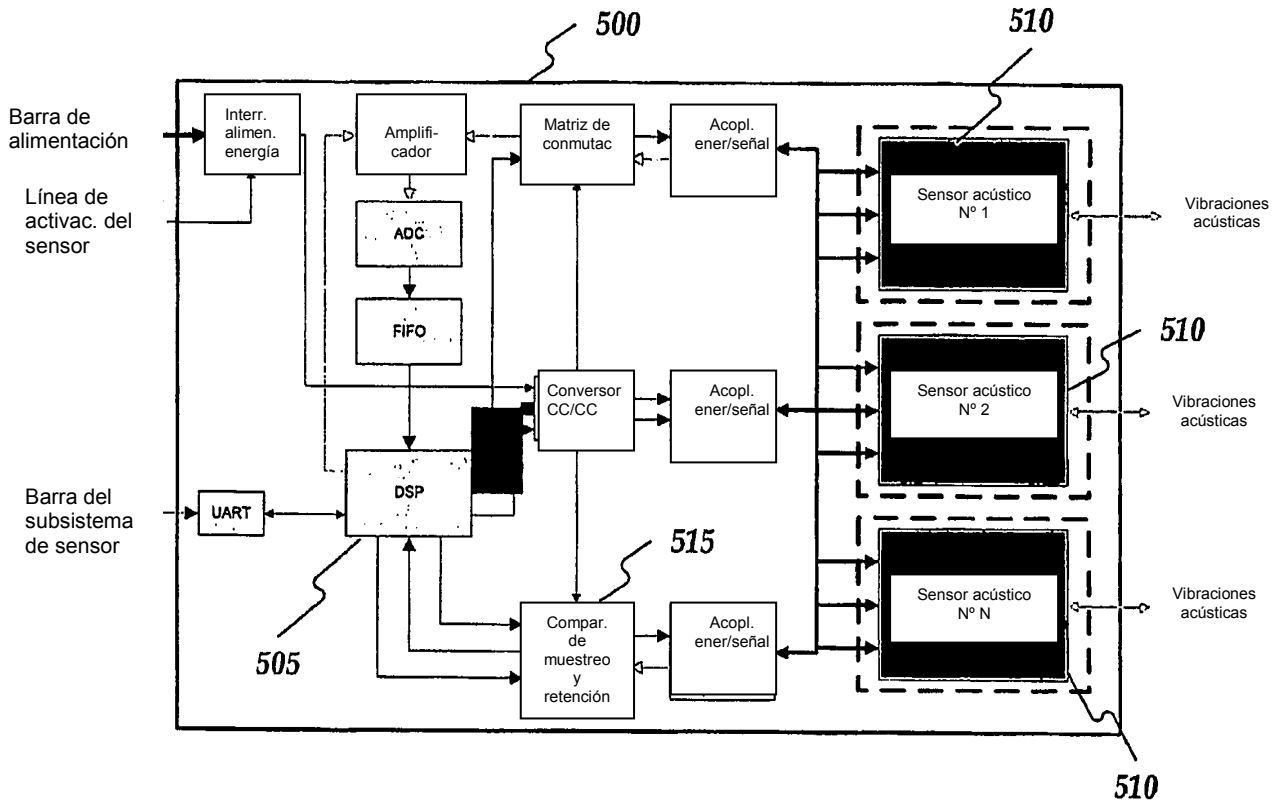


FIG. 5

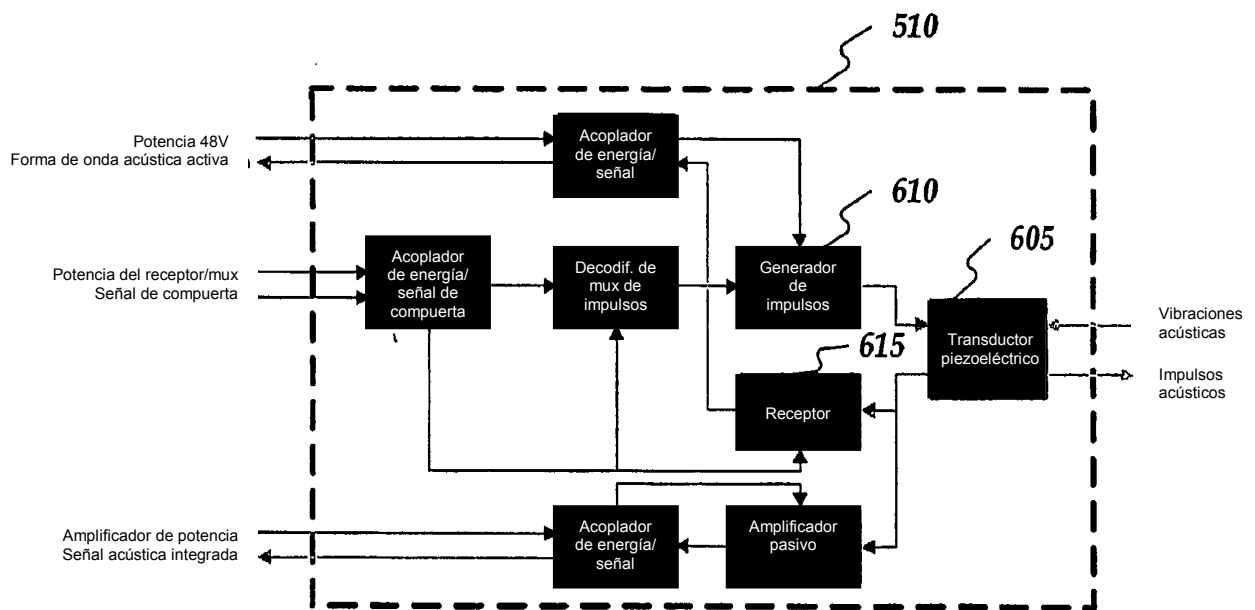


FIG. 6

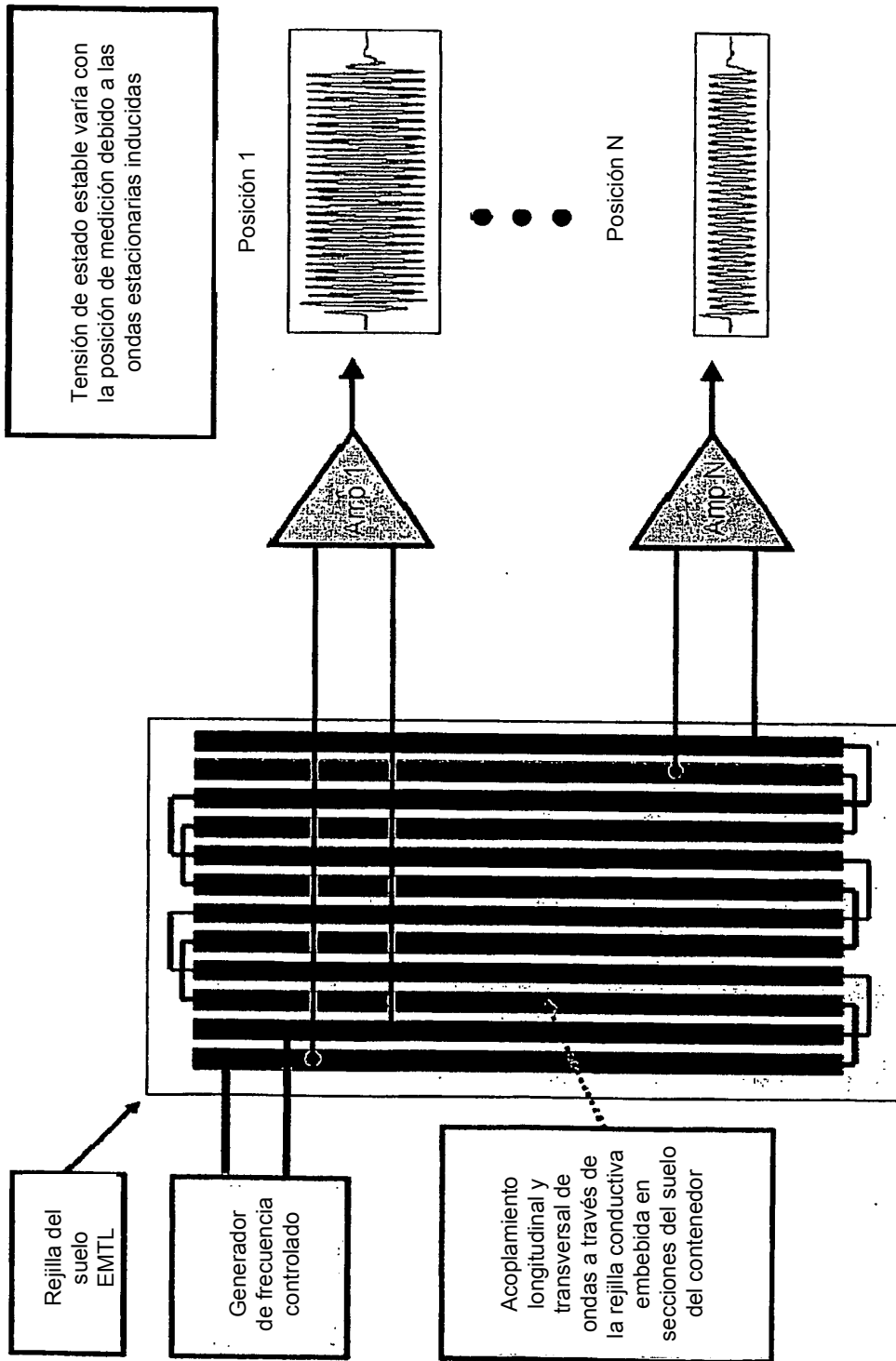


FIG. 7

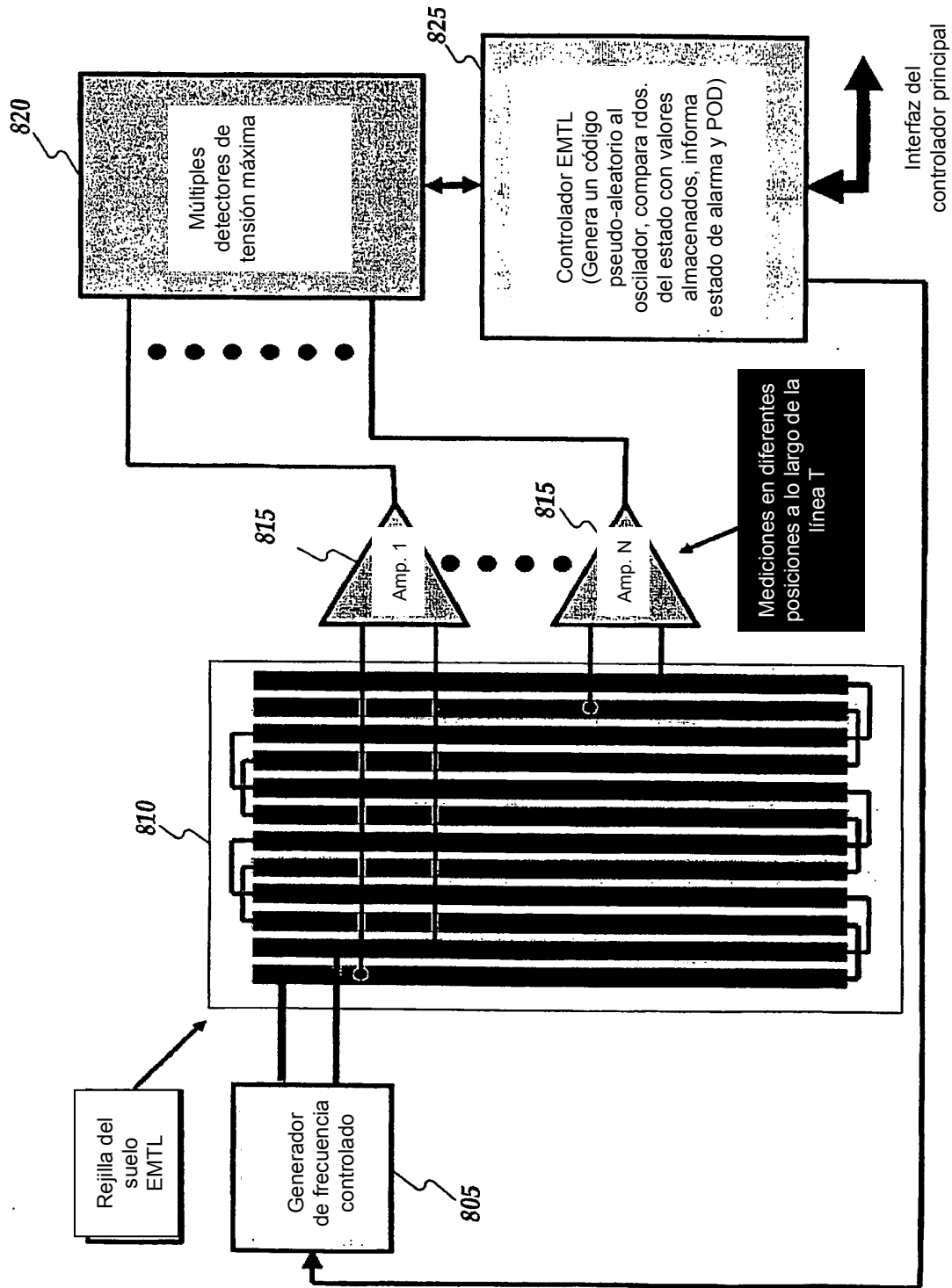


FIG. 8

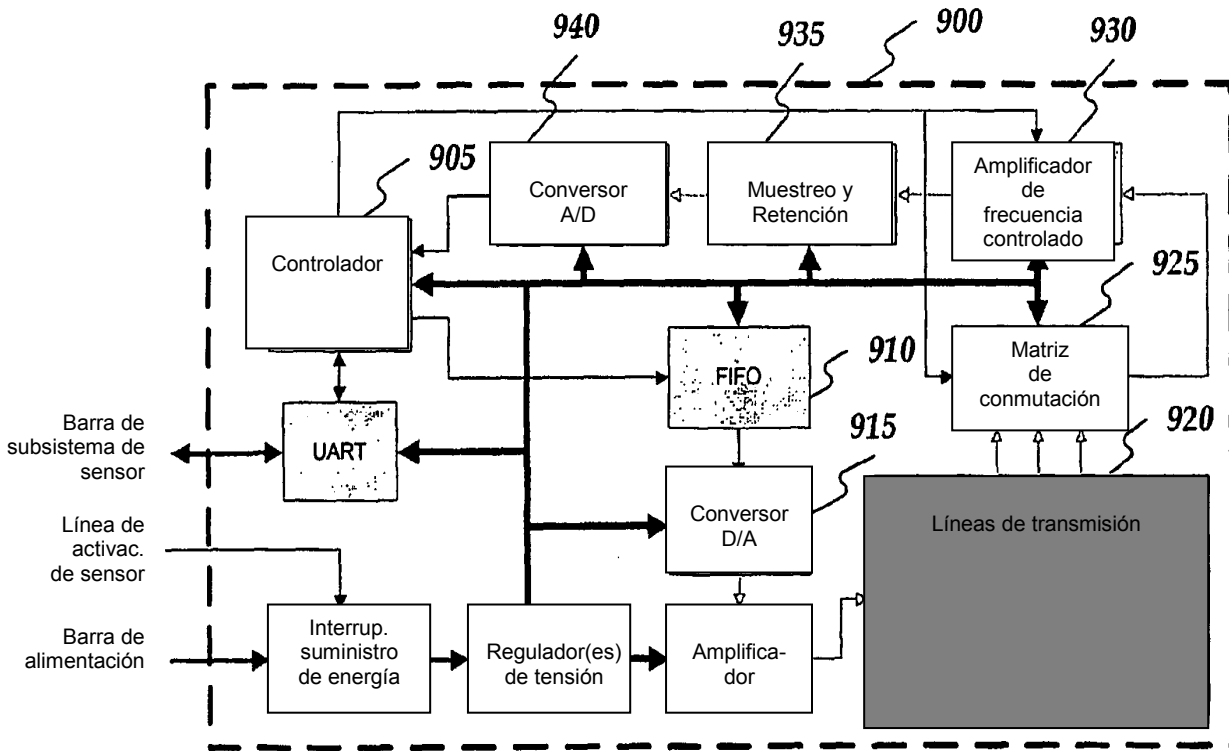


FIG. 9

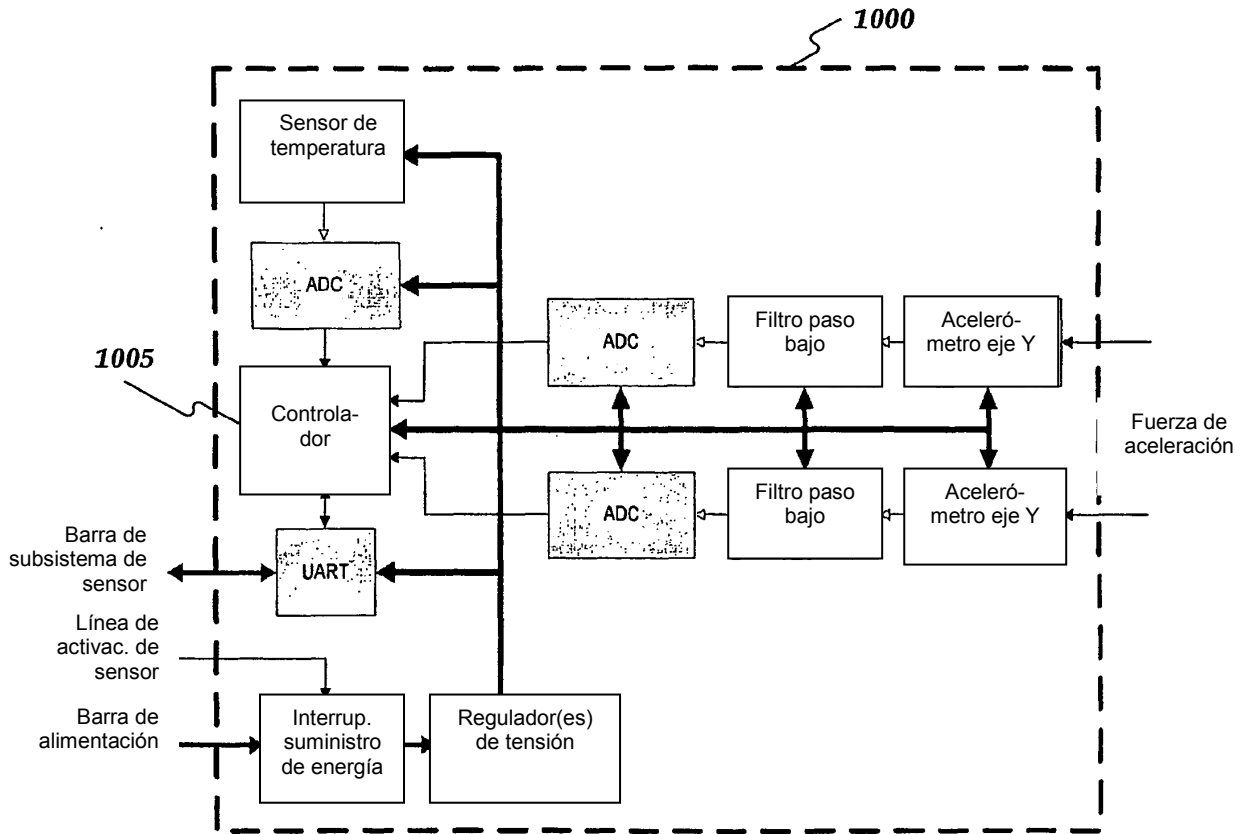


FIG. 10

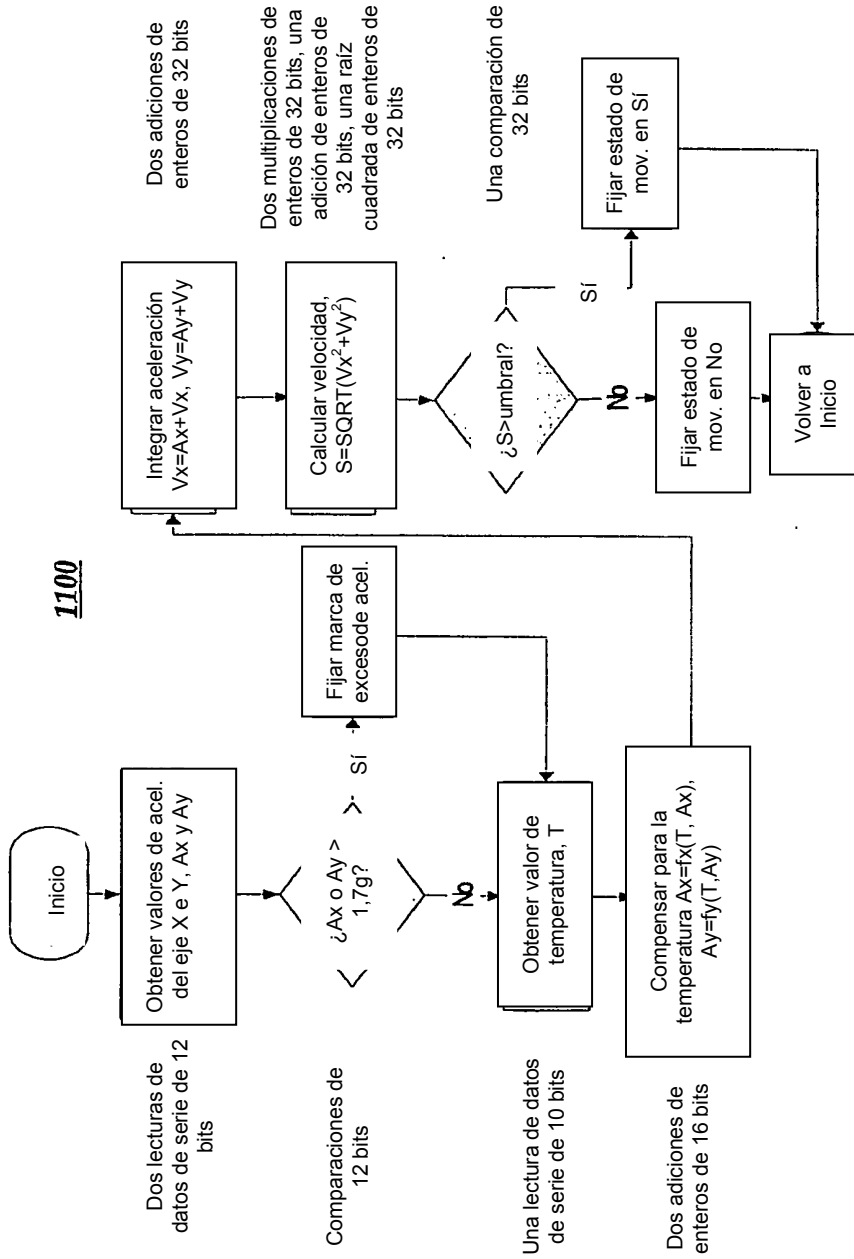


FIG. 11

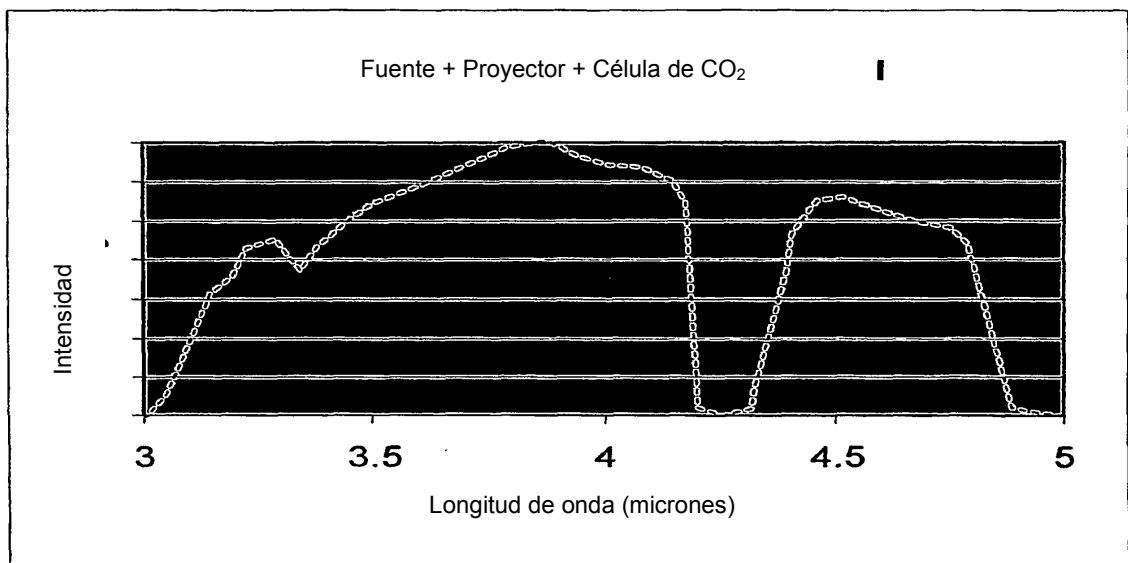


FIG. 12

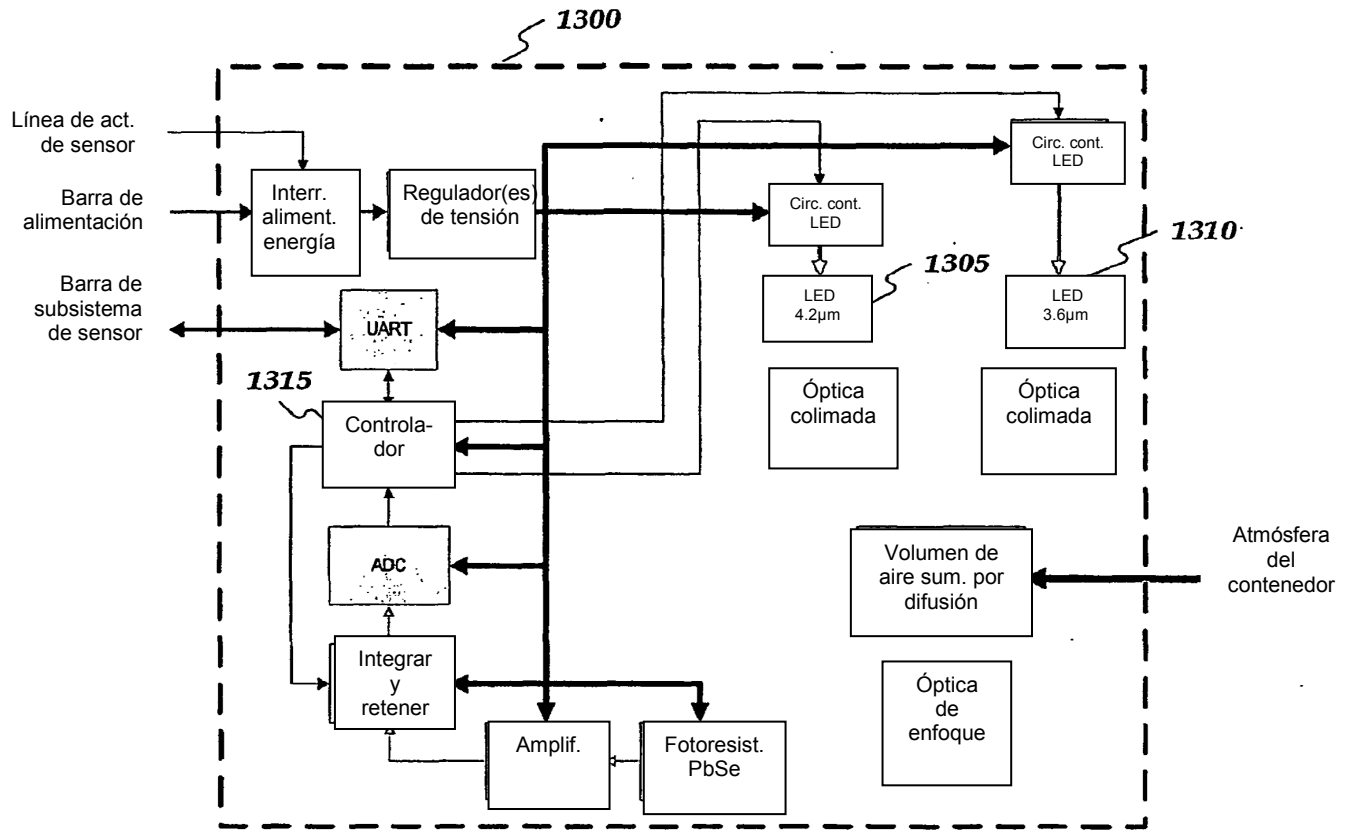


FIG. 13

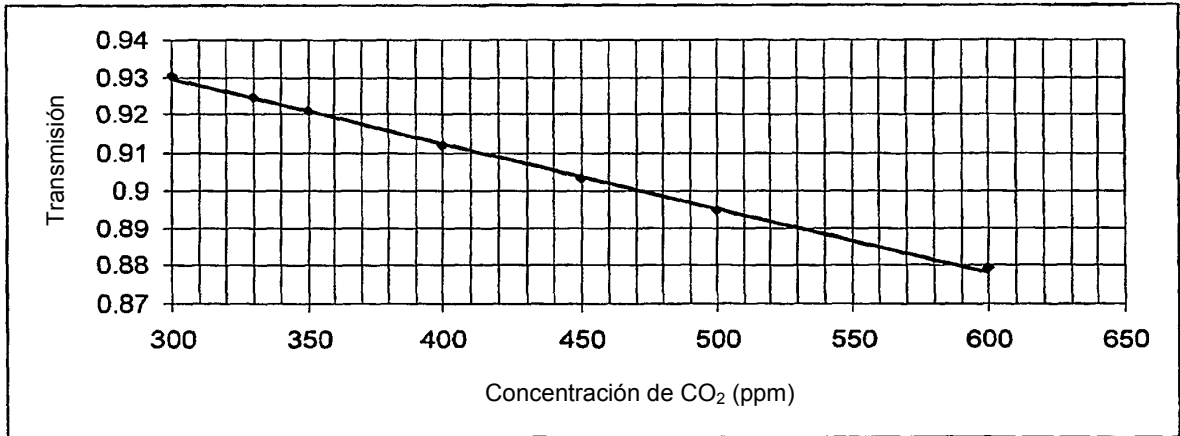


FIG. 14

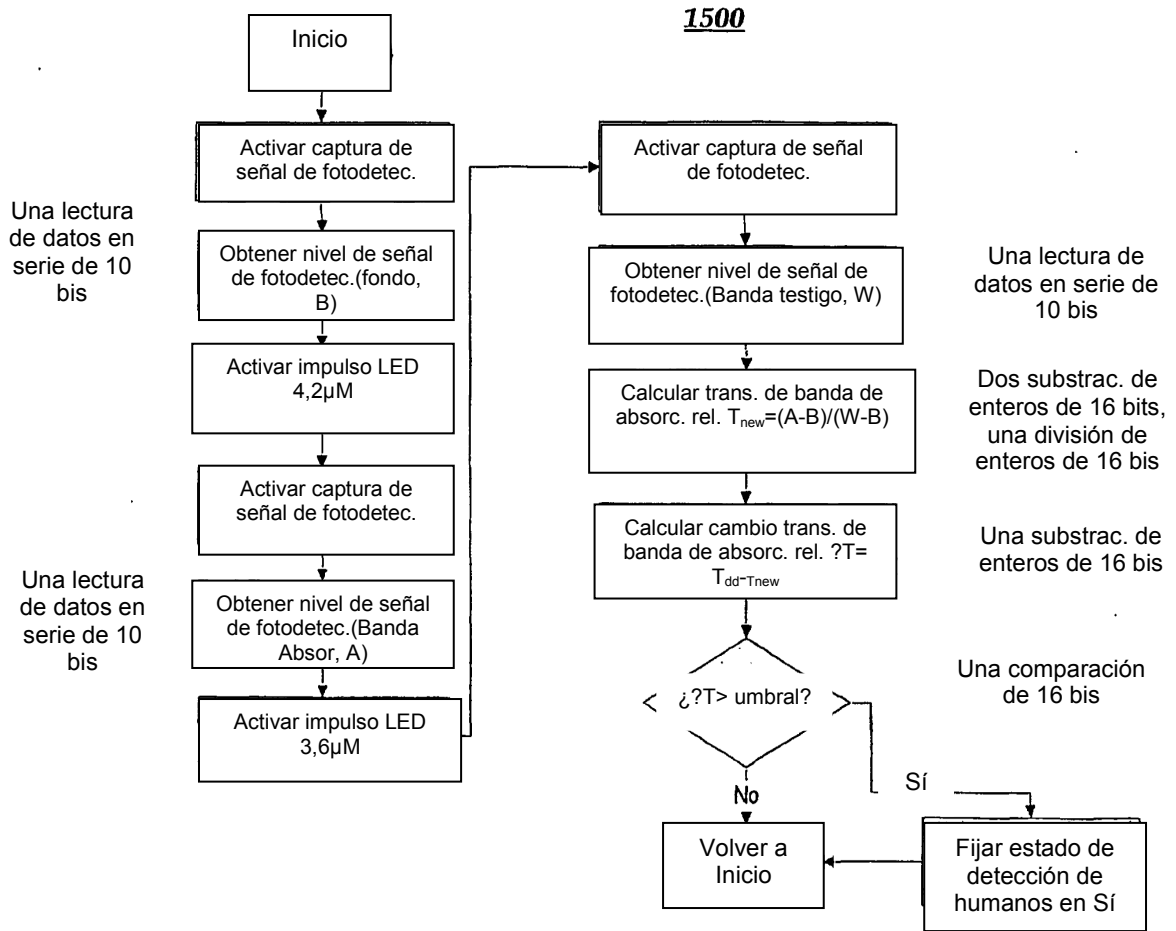


FIG. 15

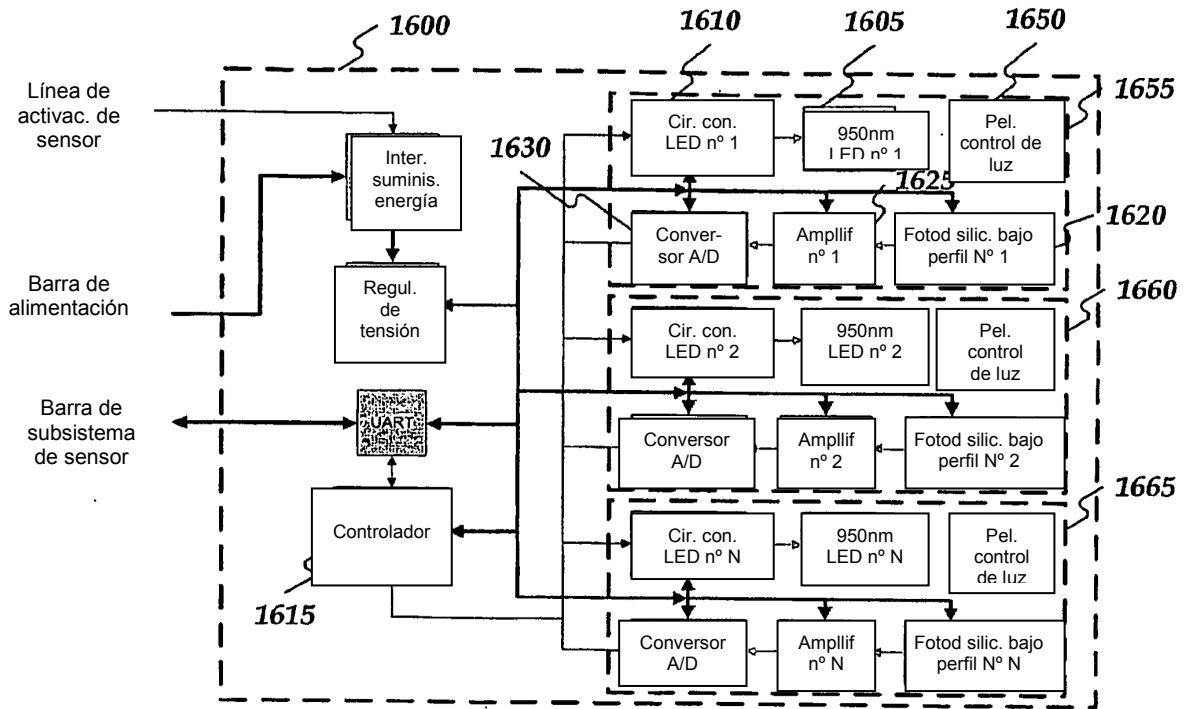


FIG. 16

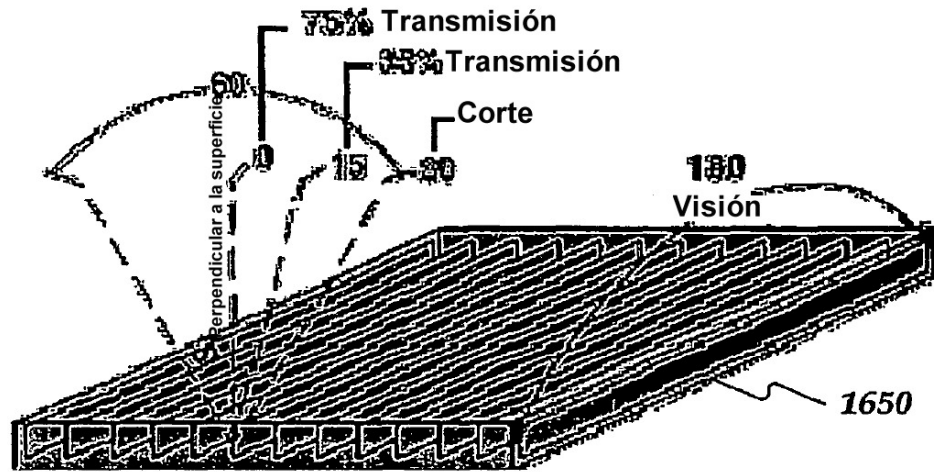


FIG. 17

1800

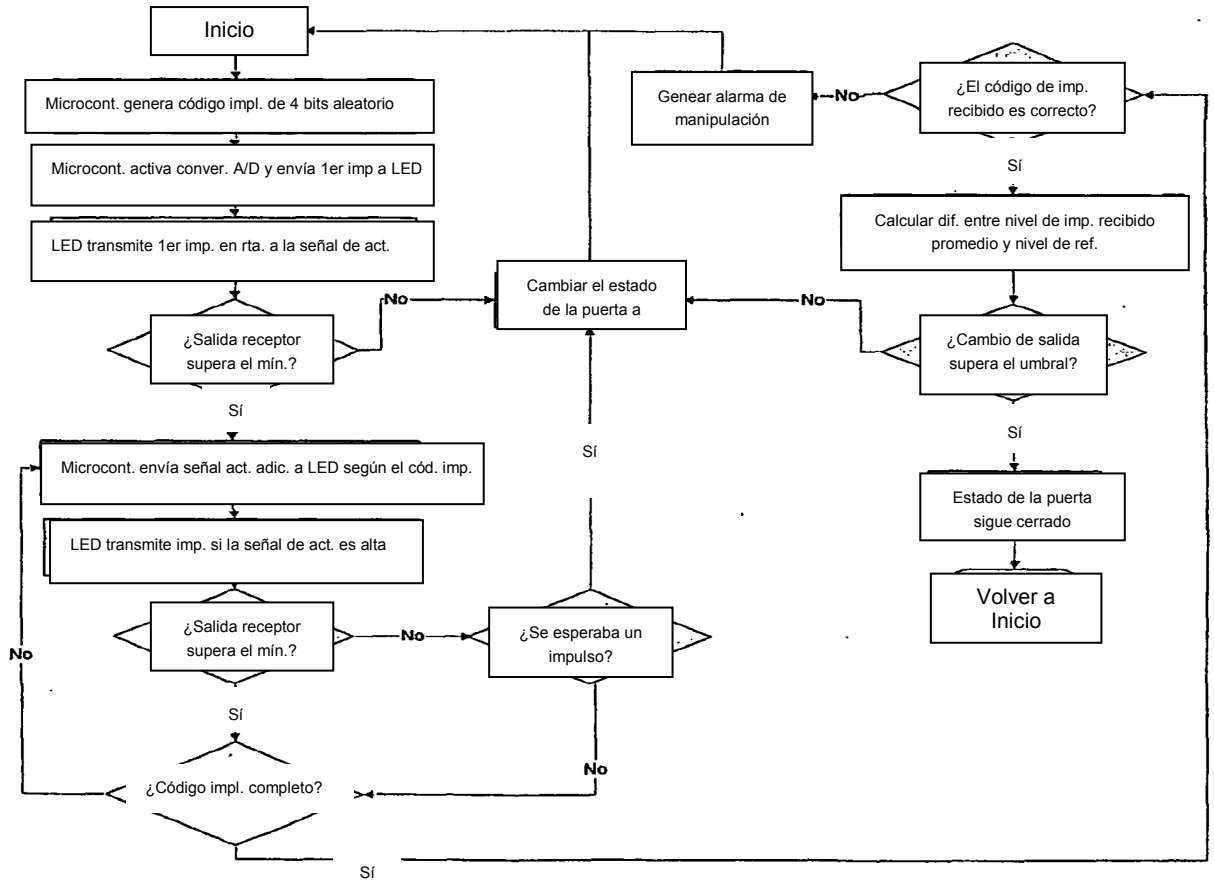


FIG. 18

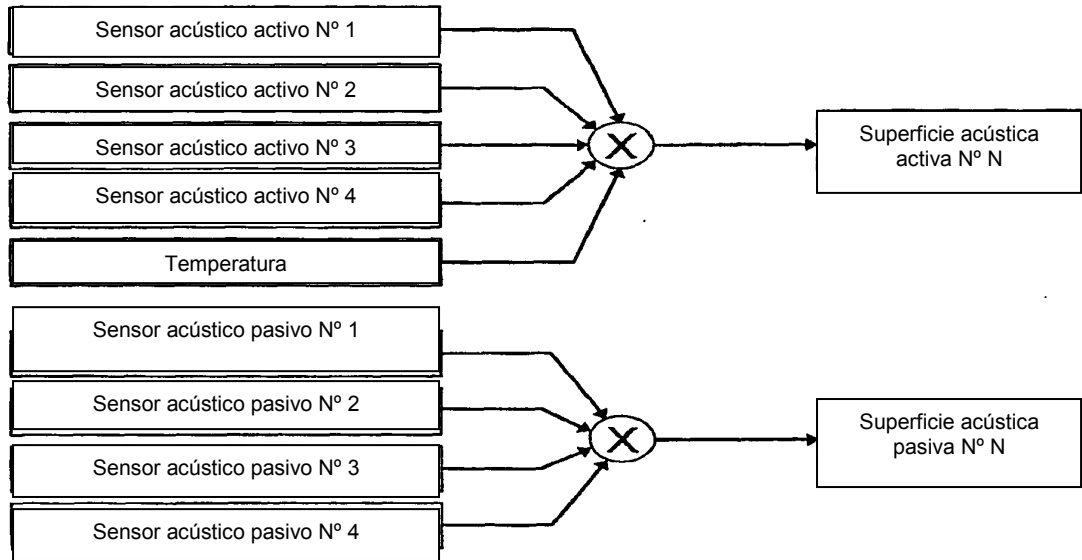


FIG. 19

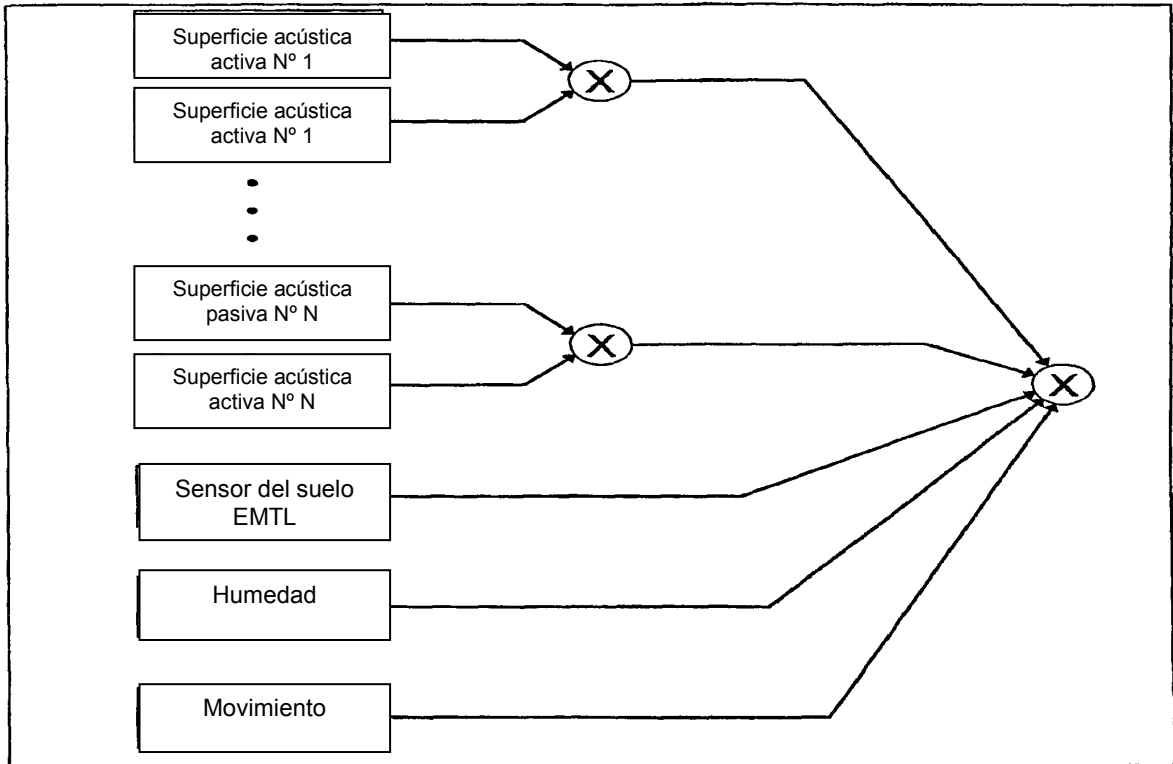


FIG. 20