

19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 457 015**

51 Int. Cl.:

**G08B 29/26** (2006.01)

**G08B 13/24** (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **10.12.2008 E 08869597 (8)**

97 Fecha y número de publicación de la concesión europea: **05.03.2014 EP 2243124**

54 Título: **Red neural de sistema de sistema de vigilancia electrónica de artículos que minimiza falsas alarmas y fallos a desactivar**

30 Prioridad:

**09.01.2008 US 971255**

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

**24.04.2014**

73 Titular/es:

**TYCO FIRE & SECURITY GMBH (100.0%)  
Victor von Bruns-Strasse 21  
8212 Neuhausen am Rheinfall, CH**

72 Inventor/es:

**ALLEN, JOHN A.;  
BERGMAN, ADAM S. y  
SOTO, MANUEL A.**

74 Agente/Representante:

**VALLEJO LÓPEZ, Juan Pedro**

**ES 2 457 015 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

Red neural de sistema de sistema de vigilancia electrónica de artículos que minimiza falsas alarmas y fallos a desactivar

5

**Campo de la invención**

La presente invención se refiere en general a sistemas de seguridad electrónica, y en particular, a un sistema de vigilancia electrónica de artículos ("EAS") mejorado y método para disminuir falsas alarmas.

10

**Antecedentes de la invención**

Los sistemas de vigilancia electrónica de artículos ("EAS") son sistemas de detección que permiten la identificación de un marcador o etiqueta en una zona de detección dada. Los sistemas EAS tienen muchos usos, pero en muchas ocasiones se usan como sistemas de seguridad para evitar hurtos en tiendas o retirada de bienes en edificios de oficinas. Los sistemas EAS vienen en muchas diferentes formas y hacen uso de un número de diferentes tecnologías.

15

Un sistema EAS típico incluye una unidad de detección electrónica, etiquetas y/o marcadores, y un desprendedor o desactivador. Las unidades de detección pueden, por ejemplo, formarse como unidades de pedestal, enterrarse bajo el suelo, montarse sobre paredes o colgarse del techo. Las unidades de detección se colocan normalmente en altas áreas de tráfico, tales como entradas y salidas de tiendas o edificios de oficinas. Las etiquetas y/o marcadores tienen características especiales y se conciben específicamente para fijarse o para embeberse en mercancías u otros objetos que se busque proteger. Cuando una etiqueta activa atraviesa una zona de detección de etiquetas, el sistema EAS hace sonar una alarma, se activa una luz y/o se activan algunos otros dispositivos de alerta adecuados para indicar la retirada de la etiqueta del área prescrita.

20

25

Los sistemas EAS comunes funcionan con estos mismos principios generales usando transeceptores, que cada uno transmite y recibe, o un transmisor y receptor separados. Normalmente el transmisor se coloca en un lado de la zona de detección y el receptor se coloca en el lado opuesto de la zona de detección. El transmisor produce una señal de excitación predeterminada en una zona de detección de etiquetas. En el caso de una tienda al por menor, esta zona de detección se forma normalmente en una salida. Cuando una etiqueta EAS entra en la zona de detección, la etiqueta tiene una respuesta característica a la señal de excitación, que puede detectarse. Por ejemplo, la etiqueta puede responder a la señal enviada mediante el transmisor usando una simple unión de semiconductor, un circuito sintonizado, compuesto de un inductor y un condensador, tiras o alambres magnéticos blandos o resonadores acústico-magnéticos de vibración ("AM"). Por ejemplo las etiquetas "AM" son dispositivos que presentan propiedades de respuesta específicas cuando se activan y desactivan. Cuando se activan, las etiquetas AM resuenan y transmiten una señal en una frecuencia resonante cuando se estimulan mediante una señal de interrogación en una frecuencia particular. El receptor posteriormente detecta esta respuesta característica. Las propiedades de las etiquetas AM "desactivadas" dan como resultado la incapacidad de transmitir una señal en la frecuencia resonante. Por diseño, la respuesta característica de la etiqueta es distintiva y no es probable que se cree mediante circunstancias naturales.

30

35

40

Una consideración en relación con el diseño y uso de tales sistemas EAS es minimizar la aparición de falsas alarmas que podrían provocar incomodidades a clientes de un usuario de sistema EAS, por ejemplo, en una tienda al por menor, o producir señales de alarma molestas y perjudiciales cuando nadie está atravesando el sistema EAS de la tienda. Existen diversos tipos de señales de falsa alarma que incluyen una "falsa" alarma que aparece cuando un comprador atraviesa el sistema EAS sin poseer ninguna mercancía que lleve etiqueta o protegida, pero, sin embargo, sonó una alarma. Otro tipo más específico aún de señal de falsa alarma es la alarma de "mercancía", que aparece cuando un comprador lleva mercancía no protegida a través del sistema EAS que, sin embargo, presenta las características de una etiqueta activa. Ejemplos de esto son artículos tales como alargadores y cables, sillas plegables y otros objetos de metal enrollados que son capaces de resonancia en la presencia del campo electromagnético de un sistema EAS. Otro tipo específico de señal de falsa alarma es la alarma "fantasma", que aparece cuando un sistema EAS hace sonar una alarma en respuesta a la detección de una señal de "ambiente", generalmente cuando nadie está atravesando el sistema EAS. Son ejemplos señales de falsa alarma producidas mediante mercancía que lleva etiqueta colocada en la visualización lo suficientemente cerca del sistema EAS para producir accidentalmente una condición de alarma o cuando se introduce temporalmente mercancía que lleva etiqueta en la zona de detección pero no sale del espacio de venta.

45

50

55

Otro tipo de falsa alarma aparece cuando existe un fallo al desactivar (evento "FTD" que aparece cuando una etiqueta está inapropiadamente desactivada o "herida"). Una etiqueta se "hiere" cuando la etiqueta no se ha desactivado completamente sino que permanece en un estado donde la etiqueta está en el umbral de ser una etiqueta válida. Por ejemplo, en sistemas EAS actuales, cuando las etiquetas AM (también denominadas en el presente documento como "sellos") se desactivan apropiadamente puede esperarse que la frecuencia del sello como se detectó mediante el receptor del sistema sea aproximadamente 59,3 kHz. El criterio de frecuencia del detector AM rechaza la detección de sellos con frecuencias mayores que 58,6 kHz. En algunos casos unos sellos parcial o

60

65

inapropiadamente desactivados pueden tener una frecuencia menor de 58,6 kHz, caso en el que el sistema inintencionadamente hará sonar la alarma (falsa alarma).

5 El documento US 5.909.178 A enseña un método para ajustar un umbral de validación para detectar un marcador en una zona de interrogación. Se obtiene ruido de fondo para adaptar el criterio de alarma para ajustar la sensibilidad.

10 El documento EP 0 435 198 A2 muestra un método para reducir la aparición de falsas alarmas en sistemas EAS. Se usa un sensor auxiliar para detectar una presencia de comprador. Este método no es apropiado para distinguir entre etiquetas válidas y las denominadas heridas.

15 El documento WO 2009/011732 A2 se refiere a un método para inhibir detección de etiquetas de vigilancia electrónica de artículos desactivadas, comprendiendo el método determinar una relación de fallo al desactivar, correspondiendo la relación de fallo al desactivar al valor de energía de detección de señal medido en la frecuencia recibida válida de la etiqueta dividido por el valor de energía de desactivación de señal medido en la frecuencia desactivada esperada de la etiqueta. El documento WO 20091011732 constituye la técnica anterior para el fin de la evaluación de la novedad exclusivamente.

20 El documento US 4.249.167 desvela crear dos diferentes frecuencias en una zona de interrogación. Ambas frecuencias son frecuencias válidas de las etiquetas bajo vigilancia para crear bandas laterales en la zona de interrogación. Estas bandas laterales se mezclan con una de las dos diferentes frecuencias para obtener al menos una frecuencia base igual a la diferencia entre las frecuencias de bandas laterales y una de las dos diferentes frecuencias. De esta manera se evitan las falsas alarmas.

25 El documento EP 0 410 245 A2 desvela un sistema de vigilancia electrónica de artículos multimodo. El transceptor puede funcionar en dos modos diferentes.

Lo que se necesita es un método y sistema que pueda usarse para reducir o eliminar falsas alarmas en zonas de detección de sistema EAS especialmente cuando las etiquetas no se han desactivado apropiadamente.

### 30 **Sumario de la invención**

La presente invención proporciona ventajosamente un método, sistema y producto de programa informático para gestionar falsas alarmas en un sistema de seguridad. En una realización, la presente invención proporciona el método para gestionar falsas alarmas en un sistema de seguridad en el que se establece una zona de detección. Un evento de alarma se acciona basándose en la detección de una etiqueta en la zona de detección usando una sensibilidad de accionador de alarma inicial. La sensibilidad de accionador de alarma inicial se basa en un conjunto inicial de uno o más criterios de detección. El conjunto de criterios de detección se modifica para ajustar la sensibilidad de accionador de alarma del sistema de seguridad. El conjunto de criterios de detección incluye un umbral de frecuencia y un umbral de relación de nivel de energía y en el que el evento de alarma se acciona si una relación de primer nivel de frecuencia detectado a una primera frecuencia, que es la frecuencia recibida válida de dicha etiqueta, a un segundo nivel de energía detectado a una segunda frecuencia, que es la frecuencia desactivada esperada de dicha etiqueta, es mayor que un umbral de relación de nivel de energía predeterminado. Se reduce un intervalo de frecuencias de accionador de alarma válidas cuando una frecuencia media detectada para etiquetas que producen una alarma es mayor que el umbral de frecuencia.

45 De acuerdo con otro aspecto, la presente invención proporciona un sistema para gestionar falsas alarmas. Un transmisor produce un campo de interrogación aplicado en una zona de detección. Un procesador funciona o acciona un evento de alarma en respuesta a la detección de una etiqueta en la zona de detección usando una sensibilidad de accionador de alarma inicial en la que la sensibilidad de accionador de alarma inicial se basa en un conjunto inicial de uno o más criterios de detección, y modificar el conjunto de criterios de detección para ajustar la sensibilidad de accionador de alarma del sistema de seguridad. El conjunto de criterios de detección incluye un umbral de frecuencia y un umbral de relación de nivel de energía y en el que el evento de alarma se acciona si una relación de primer nivel de frecuencia detectado a una primera frecuencia, que es la frecuencia recibida válida de dicha etiqueta, a un segundo nivel de energía detectado a una segunda frecuencia, que es la frecuencia desactivada esperada de dicha etiqueta, es mayor que un umbral de relación de nivel de energía predeterminado. El procesador funciona adicionalmente para reducir un intervalo de frecuencias de accionador de alarma válidas cuando una frecuencia media detectada para etiquetas que producen una alarma es mayor que el umbral de frecuencia.

60 De acuerdo con otro aspecto, la presente invención proporciona un producto de programa informático que incluye un medio que puede usar un ordenador que tiene un programa legible por ordenador para un sistema de seguridad que cuando se ejecuta en un ordenador produce que el ordenador realice un método que incluye el establecimiento de una zona de detección. Un evento de alarma se acciona basándose en la detección de una etiqueta en la zona de detección usando una sensibilidad de accionador de alarma inicial. La sensibilidad de accionador de alarma inicial se basa en un conjunto inicial de uno o más criterios de detección. El conjunto de criterios de detección se modifica para ajustar la sensibilidad de accionador de alarma del sistema de seguridad. El conjunto de criterios de detección incluye un umbral de frecuencia y un umbral de relación de nivel de energía y en el que el evento de alarma se

acciona si una relación de primer nivel de frecuencia detectado a una primera frecuencia, que es la frecuencia recibida válida de dicha etiqueta, a un segundo nivel de energía detectado a una segunda frecuencia, que es la frecuencia desactivada esperada de dicha etiqueta, es mayor que un umbral de relación de nivel de energía predeterminado. Se reduce un intervalo de frecuencias de accionador de alarma válidas cuando una frecuencia media detectada para etiquetas que producen una alarma es mayor que el umbral de frecuencia.

Se expondrán aspectos adicionales de la invención en parte en la descripción que sigue, y en parte serán obvios a partir de la descripción, o pueden aprenderse poniendo en práctica la invención. Los aspectos de la invención se llevarán a cabo y obtendrán por medio de los elementos y combinaciones particularmente señalados en las reivindicaciones adjuntas. Se ha de entender que tanto la descripción general anterior y la siguiente descripción detallada son a modo de ejemplo y explicatorias únicamente y no son restrictivas de la invención, según se reivindica.

### Breve descripción de los dibujos

Un entendimiento más completo de la presente invención, y las consiguientes ventajas y características de la misma, serán más fácilmente entendibles por referencia a la siguiente descripción detallada cuando se considera en relación con los dibujos adjuntos en los que:

La Figura 1 es un diagrama de bloques de un sistema de vigilancia electrónica de artículos construido de acuerdo con los principios de la presente invención;

La Figura 2 es un diagrama de bloques de un registrador de datos a modo de ejemplo del sistema de vigilancia electrónica de artículos de la Figura 1, que se construye de acuerdo con los principios de la presente invención;

La Figura 3 es un diagrama de flujo de un proceso de reducción de falsa alarma a modo de ejemplo de acuerdo con los principios de la presente invención;

La Figura 4 es un diagrama que muestra el ajuste del intervalo de frecuencia de activación de alarma de acuerdo con los principios de la presente invención;

La Figura 5 es un diagrama de flujo de un proceso de ajuste del intervalo de frecuencia de activación de alarma de acuerdo con los principios de la presente invención; y

La Figura 6 es un diagrama de flujo de un proceso de activación de alarma basado en energía de acuerdo con los principios de la presente invención.

### Descripción detallada de la invención

Con referencia ahora a las figuras de los dibujos en las que designadores de referencia similares se refieren a elementos similares, se muestra en la Figura 1 un diagrama de un sistema a modo de ejemplo construido de acuerdo con los principios de la presente invención y designado generalmente como "100". El sistema de vigilancia electrónica de artículos ("EAS") 100 incluye las unidades de detección EAS 102, 104 situadas generalmente en paralelo y a una distancia espaciada entre sí, el controlador del sistema EAS 106 en comunicación con las unidades de detección EAS 102, 104, y el registrador de datos 108 en comunicación con el controlador 106 EAS mediante una red 110 EAS. La unidad de detección EAS 102 puede incluir un transmisor 112 y una antena de transmisión 114 para producir los campos electromagnéticos que se usan en relación con tales sistemas para detectar la presencia de una etiqueta (no mostrado) fijada a mercancía a proteger. La unidad de detección EAS 104 restante incluye un receptor 116 y una antena de recepción 118, que después funciona para detectar una perturbación (resultante de la presencia de una etiqueta activa) en los campos electromagnéticos producidos mediante la unidad de detección EAS 102, que puede usarse para hacer sonar una alarma apropiada. El sistema EAS 100 puede crear una zona de detección 120 en espacios, por ejemplo, espacios de venta de una tienda, una salida de tienda, etc.

En otra realización, se proporciona una única unidad de detección EAS 102 que usa un transceptor 112 y una antena de transceptor 114 para establecer la zona de detección 120 generando los campos electromagnéticos que se usan para detectar la presencia de etiquetas fijadas a mercancía a proteger. En esta realización, el transceptor 112 y la antena de transceptor 114 también funcionan para recibir una perturbación en el campo electromagnético producido de la unidad de detección EAS 102. Por ejemplo, aunque la Figura 1 muestra la unidad de detección EAS 102 desplegada en un pedestal, el transceptor 112 y/o la antena de transceptor 114 o ambos pueden desplegarse, por ejemplo, en una puerta o en una salida de tienda. En esta realización, la antena de transceptor 114 radia el campo electromagnético o de frecuencia de radio apropiado para producir la zona de detección 120.

El procesamiento de datos y señales desarrollado mediante las unidades de detección EAS 102, 104 del sistema EAS 100 se consigue mediante un controlador de sistema EAS 106 asociado con el sistema EAS 100 que puede ser una unidad independiente o una unidad integrada, por ejemplo, situada en los transceptores/receptores 112, 116. En ciertas realizaciones, el controlador 116 ejecuta uno o más procesos asociados con aplicaciones EAS. En esta realización, el controlador 106 se usa para analizar señales de detección recibidas mediante el receptor 116 para determinar la presencia de una etiqueta en la zona de detección 120 entre las unidades de detección EAS 102 y 104. El controlador 106 ejecuta instrucciones y manipula datos para realizar las operaciones del sistema EAS 100 y puede ser, por ejemplo, una unidad de procesamiento central ("CPU") un circuito integrado específico de la aplicación ("ASIC") o un campo de matriz de puertas programables ("FPGA"). El controlador 106 también controla la

activación o habilitación de los transmisores, por ejemplo, el transmisor 112, para todas las diversas configuraciones del sistema EAS 100.

5 El sistema EAS 100 incluye un registrador de datos 108, que es una unidad que rastrea la cantidad y tipo de eventos de alarma que aparecen en la zona de detección 120. El registrador de datos 108 de la Figura 2 incluye uno o más procesadores, tales como el procesador 204. El procesador 204 está conectado a una infraestructura de comunicación 202, por ejemplo, un bus de comunicaciones, barra de transición o red cableada/inalámbrica. Se describen diversas realizaciones de software en términos de este registrador de datos 108 a modo de ejemplo. Después de leer esta descripción, será evidente para los expertos en la materia cómo implementar la invención usando otros sistemas informáticos y/o arquitecturas basadas en ordenador.

15 El registrador de datos 108 puede incluir una interfaz de usuario 208 que envía gráficos, texto y otros datos desde la infraestructura de comunicación 202 (o desde una memoria intermedia de tramas no mostrada) para presentación en la unidad de visualización 210. La interfaz de usuario 208 sirve como un dispositivo de entrada para interacción humana. En ciertas realizaciones, el controlador 106 puede recibir comandos desde el operador a través de la interfaz de usuario 208, así como otros dispositivos de entrada, tales como un ratón o teclado. Por ejemplo, el registrador de datos 108 puede tener una serie de botones en la periferia de la interfaz de usuario 208 que permiten a un operador introducir un código de motivo para un evento de alarma.

20 El registrador de datos 108 también incluye una memoria principal 206, preferentemente memoria de acceso aleatorio (RAM), y puede también incluir una memoria secundaria 212. La memoria secundaria 212 puede incluir, por ejemplo, un mecanismo de disco duro 214 y/o un mecanismo de almacenamiento extraíble 216, que representa un mecanismo de disco flexible, un mecanismo de cinta magnética, un mecanismo de disco óptico, mecanismo/memoria flash, etc. El mecanismo de almacenamiento extraíble 216 lee desde y/o escribe en una unidad de almacenamiento extraíble 218 de una manera bien conocida para los expertos en la materia. La unidad de almacenamiento extraíble 218 representa, por ejemplo, memoria flash, un disco flexible, cinta magnética, disco óptico, etc., que se lee mediante y se escribe mediante el mecanismo de almacenamiento extraíble 216. Como se apreciará, la unidad de almacenamiento extraíble 218 incluye un medio de almacenamiento que puede usar un ordenador que tiene almacenado en el mismo software informático y/o datos.

30 En realizaciones alternativas, la memoria secundaria 212 puede incluir otros medios similares para permitir a programas informáticos u otras instrucciones cargarse en el registrador de datos 108. Tales medios pueden incluir, por ejemplo, una unidad de almacenamiento extraíble 222 y una interfaz 220. Ejemplos de tales puede incluir un cartucho de programa e interfaz de cartucho (tales como aquellos encontrados en dispositivos de videojuegos), un chip de memoria extraíble (tal como una flash, EPROM o PROM) y zócalo asociado, y otras unidades de almacenamiento extraíble 222 e interfaces 220 que permiten al software y datos transferirse desde la unidad de almacenamiento extraíble 222 al registrador de datos 108.

40 El registrador de datos 108 puede también incluir una interfaz de comunicaciones 224. La interfaz de comunicaciones 224 permite al software y datos transferirse entre el registrador de datos 108 y dispositivos externos, por ejemplo, el controlador de sistema EAS 106. Ejemplos de la interfaz de comunicaciones 224 pueden incluir un módem, una interfaz de red (tal como una tarjeta Ethernet), un puerto de comunicaciones, una ranura y tarjeta PCMCIA, etc. El software y datos transferidos mediante la interfaz de comunicaciones 224 están en la forma de señales que pueden ser, por ejemplo, electrónicas, electromagnéticas, ópticas u otras señales capaces de recibirse mediante la interfaz de comunicaciones 224. Estas señales se proporcionan a la interfaz de comunicaciones 224 mediante una ruta o canal 226 de comunicaciones. El canal 226 lleva señales y puede implementarse usando alambre o cable, fibra óptica, una línea telefónica, un enlace telefónico celular, un enlace RF y/u otros canales de comunicaciones. En una realización, el registrador de datos 108 se comunica con el controlador de sistema EAS 106 mediante una red, por ejemplo, la red 110 EAS que puede incluir pero sin limitación diversas interfaces o normas de enlace de datos tales como la norma 232 recomendada ("RS-232"), norma 485 recomendada ("RS-485"), bus serie universal ("USB"), protocolo de control de transmisión Ethernet /protocolo de internet ("TCP/IP"), etc.

55 Las expresiones "medio de programa informático", "medio que puede usar un ordenador" y "medio legible por ordenador" se una para referirse en general a medios tales como una memoria principal 206 y una memoria secundaria 212, mecanismo de almacenamiento extraíble 216, un disco duro instalado en el mecanismo de disco duro 214 y señales. Estos productos de programa informático son medios para proporcionar software al registrador de datos 108. El medio legible por ordenador permite al registrador de datos 108 leer datos, instrucciones, mensajes o paquetes de mensaje, y otra información legible por ordenador desde el medio legible por ordenador. El medio legible por ordenador, por ejemplo, puede incluir memoria no volátil, tal como flexible, ROM, memoria flash, memoria de mecanismo de disco, CD-ROM y otro almacenamiento permanente. Es útil, por ejemplo, para transportar información, tal como datos e instrucciones informáticas, entre sistemas informáticos. Adicionalmente, el medio legible por ordenador puede comprender información legible por ordenador en un medio de estado transitorio tal como un enlace de red y/o una interfaz de red, incluyendo una red cableada o una red inalámbrica que permite al registrador de datos 108 leer tal información legible por ordenador.

Los programas informáticos (también denominados lógica de control informática) se almacenan en memoria principal 206 y/o memoria secundaria 212. Los programas informáticos pueden también recibirse mediante la interfaz de comunicaciones 224. Tales programas informáticos, cuando se ejecutan, posibilitan al registrador de datos 108 realizar las características de la presente invención como se analiza en el presente documento. En particular, los programas informáticos, cuando se ejecutan, posibilitan al procesador 204 realizar las características del registrador de datos 108.

La Figura 3 es un diagrama de flujo que ilustra un método a modo de ejemplo para gestión de falsa alarma del sistema EAS 100 que usa un registrador de datos 108. El método a modo de ejemplo se analiza con referencia al sistema EAS 100, sin embargo, cualquier otro sistema adecuado o porción de un sistema puede usar realizaciones apropiadas del método para recuperar y procesar información EAS registrada para gestionar la sensibilidad de las unidades de detección EAS 102,104 en la zona de detección EAS 120. Generalmente, el método para gestión de falsa alarma describe una etiqueta que entra en una zona de detección 120 para generar un evento de alarma.

En la etapa S302, se realiza una determinación de si ha aparecido o no un evento de alarma, tal como cuando una etiqueta fijada a un objeto, por ejemplo, una pieza de mercancía, entra en la zona de detección 120. Si no se detecta evento de alarma, a continuación se repite la etapa S302 hasta que aparece un evento de alarma. Una vez que aparece un evento de alarma, se investiga el evento de alarma (etapa S304) mediante, por ejemplo, los empleados de la compañía que despliega el sistema de seguridad 100.

En la etapa S306, se determina la causa del evento de alarma y esa causa del evento de alarma se registra en la etapa S308. En una realización, los investigadores, por ejemplo, empleados de la compañía que despliega el sistema de seguridad 100, determinan la causa del evento de alarma, que puede ser, por ejemplo, un fallo al desactivar ("FTD"), una falsa alarma, por ejemplo, una falsa alarma de mercancía o una alarma válida, por ejemplo, una alarma producida mediante retirada no autorizada de un objeto de las instalaciones de la compañía. Cada uno de los tipos de evento de alarma puede tener un "código de motivo" asignado, que permite al investigador introducir en o seleccionar desde el registrador de datos 108 para registrar de este modo la causa apropiada del evento de alarma. Una vez que se ha registrado la información para el evento de alarma en (o recibido mediante) el registrador de datos 108, esta información se envía de vuelta al controlador de sistema EAS 106 en tiempo real o retardado para análisis y almacenamiento. Por ejemplo, se investiga y determina un elemento de alarma para ser el resultado de una falsa alarma y se introduce un código de motivo para una falsa alarma en el registrador de datos 108, por ejemplo, mediante un investigador. En la etapa S310, el código de motivo e información relacionada con el evento de alarma se transmiten al controlador de sistema EAS 106 para procesamiento y análisis.

Si se determina que ha habido demasiadas falsas alarmas (etapa S312) a continuación el sistema puede ajustarse para cambiar su sensibilidad de accionador de alarma a un nivel que es menos sensible permitiendo menos falsas alarmas. Si no hay demasiadas falsas alarmas o fallos al desactivar, el proceso vuelve a la etapa S302 para esperar para el siguiente evento de alarma.

De acuerdo con una realización, el ajuste puede realizarse manualmente usando el registrador de datos 108 anteriormente analizado. En otra realización analizada a continuación en detalle, puede reducirse la sensibilidad de accionador de alarma reduciendo las frecuencias permisibles para un evento de alarma. En otras palabras, el umbral de frecuencia se ajusta automáticamente para evitar eventos de alarma en la frecuencia de las falsas alarmas registradas. En otra realización más también analizada a continuación el sistema EAS puede elevar automáticamente el umbral de relación de señal a ruido ("SNR") en un intento para reducir la probabilidad de otro falso evento. De acuerdo con ambas de estas realizaciones, el ajuste del sistema es automático y no necesita emplear el uso del registrador de datos 108. Como tal, se dispone el controlador de sistema EAS 106 para funcionar sin intervención manual ni ajuste manual.

Un ejemplo de rastreo de la frecuencia de sello estimada para cada alarma mientras se registra la tasa de alarma se explica con referencia al diagrama de frecuencia de la Figura 4 y el proceso de ajuste automático mostrado en la Figura 5. Los detectores AM actuales usan algoritmos de estimación de frecuencia para estimar la frecuencia real de etiquetas AM cuando se detectan mediante el sistema. La presente invención compara esta estimación de frecuencia con un intervalo inicial predeterminado de frecuencias válidas 402 ( $F_{\min}$ ,  $F_{\max}$ ). Por ejemplo se establece una  $F_{\min}$  y  $F_{\max}$  iniciales (Etapa S502). Como se muestra en la Figura 4,  $F_{\min}$  en la Figura 4 es 57,7 kHz y se muestra la  $F_{\max}$  inicial como 58,6 kHz. Esto supone que una frecuencia recibida preferida para una etiqueta activada es 58,0 kHz. Si la frecuencia de etiqueta estimada cae en el intervalo válido (etapa S504), entonces la etiqueta se considera válida y el sistema hace sonar la alarma (etapa S506). De otra manera la etiqueta se considera desactivada o fuera del intervalo de frecuencia. Son conocidos métodos para estimar la frecuencia de una señal recibida, tal como la señal que corresponde a una etiqueta AM, y están fuera del alcance de la presente invención.

Como se ha observado anteriormente, la presente invención, tal como mediante el controlador 106, rastrea la frecuencia de etiqueta estimada para cada alarma mientras registra la tasa de alarma (etapa S508). El controlador 106 también rastrea la frecuencia media estimada ( $F_{\text{med}}$ ) de las etiquetas que produjeron una alarma. Si se detecta un aumento considerable en la tasa de alarma por encima de un umbral de tasa de alarma predeterminado (etapa S510), el controlador 106 compara la frecuencia media estimada ( $F_{\text{med}}$ ) de etiquetas que producen alarmas con un

FTD Umbral de Frecuencia ( $F_{umb}$ ) (etapa S512). Si la media estimada es superior que el Umbral FTD el sistema automáticamente disminuirá la máxima frecuencia ( $F_{m\acute{a}x}$ ) de la frecuencia válida para crear un nuevo intervalo 404 actualizado (etapa S514) estableciendo el máximo valor 406 actualizado ( $F_{m\acute{a}x}$  actualizado) para que sea menor que el Umbral FTD.

5 Por ejemplo, la frecuencia natural, también denominada como frecuencia característica, de una etiqueta viva es aproximadamente 58 kHz. En consecuencia, se conciben plataformas de detección para que tengan una frecuencia de funcionamiento que varía desde aproximadamente 57,7 kHz a 58,3 kHz. Cuando una etiqueta se desactiva apropiadamente, la frecuencia característica de la etiqueta desactivada se desplaza normalmente al intervalo de 59-10 60 kHz, que está fuera efectivamente del intervalo de detección y por lo tanto ya no acciona un evento de alarma. Sin embargo, una etiqueta parcialmente desactivada, o etiqueta "herida" puede tener su frecuencia característica desplazada al intervalo de 58,7-59 kHz y por lo tanto puede detectarse potencialmente si la energía es suficientemente grande en los nuevos atributos espectrales de la etiqueta, por ejemplo, la frecuencia característica de la etiqueta. Por consiguiente, disminuyendo el intervalo de frecuencia de lo que se considera una etiqueta 15 activada válida, ya no se consideran las etiquetas heridas que de otra manera harían sonar la alarma de manera falsa al sistema, incluso con etiquetas inapropiadamente válidas. Se observa que esta disposición es más precisa en entornos de alta relación de señal a ruido ("SNR"), puesto que la precisión de los algoritmos de estimación de frecuencia disminuye con una disminución en SNR.

20 Como se ha indicado anteriormente, la presente invención también proporciona una disposición mediante la cual el método de fallo al desactivar se basa en ajustar el criterio de detección. De acuerdo con la invención, el criterio de detección se basa adicionalmente en una comparación de los niveles de energía a ciertas frecuencias de detección de etiqueta. El efecto es que esta realización es menos sensible a cambios en SNR e incluso a pobres entornos SNR debido a que el sistema se ajusta de una manera que no considera ruido debido a que está generalmente 25 presente el mismo nivel de ruido en el nivel de energía de frecuencias controladas. Se describe una descripción de activación de alarma basada en energía con referencia a la Figura 6.

De acuerdo con la invención, se establece una relación FTD (etapa S602). Esta relación, descrita en detalle más adelante, se usa como una base para determinar si el nivel de energía a una primera frecuencia es suficientemente 30 grande para accionar una alarma.

En funcionamiento, el controlador de sistema EAS 106 calcula (etapa S604) y compara la energía de etiqueta recibida a dos frecuencias diferentes. De acuerdo con la invención, la primera frecuencia ( $f_1$ ) es la frecuencia recibida válida de una etiqueta, por ejemplo, 58 kHz, y la segunda frecuencia ( $f_2$ ) es la frecuencia desactivada 35 esperada de un sello, por ejemplo, 59,3 kHz. Sin embargo, en entornos de baja SNR, incluso aunque pueda existir suficiente energía 58 kHz para accionar una alarma, si se observa más energía de sello a 59,3 kHz como se compara con 58 kHz entonces el sistema considera el sello para desactivarse y no hará sonar la alarma.

De acuerdo con esta realización se calcula una relación FTD (etapa S606) para comprar los niveles de energía de 40 etiqueta recibidos a las dos frecuencias. Por ejemplo, relación FTD = energía  $f_1$  / energía  $f_2$ . Usando los valores a modo de ejemplo anteriormente proporcionados, relación FTD = energía 58 kHz / energía 59,3 kHz.

La relación se compara a continuación con un umbral de relación FTD predeterminado. El umbral de relación FTD es la mínima cantidad de energía que debe estar presente en  $f_1$  por encima del nivel de energía en  $f_2$  para accionar 45 una alarma. Si la relación FTD es superior que el umbral de relación FTD (etapa S608), se determina que la energía de sello en  $f_1$  (58 kHz) es superior que en  $f_2$  (59,3 kHz) y el controlador 106 activa una alarma (etapa 610).

Por ejemplo, para reducir alarmas FTD debido a frecuencias de etiqueta cercanas a 58,6 kHz, el controlador 106 puede rastrear inicialmente la energía media en  $f_2$  (59,3 kHz) para etiquetas que accionaron una alarma, mientras 50 que también rastrea la tasa de alarma (etapa S612). Si se detecta un considerable aumento en la tasa de alarma por encima de una tasa de alarma umbral (etapa S614), el controlador 106 evalúa el nivel de energía en la media de  $f_2$  (59,3 kHz) y determinan si el nivel de energía en  $f_2$  (59,3 kHz) aumentó durante las alarmas (etapa S616). Si el nivel de energía aumentó, se incrementa el umbral FTD en una cantidad predeterminada para reducir falsas alarmas (etapa S618). El resultado es que se disminuye la sensibilidad del sistema para reducir las instancias de falsas 55 alarmas.

El ajuste de la sensibilidad de detección del sistema EAS comparando y a continuación ajustando umbrales de nivel de energía y reduciendo las frecuencias permisibles para un evento de alarma se incluye como criterio de detección de acuerdo con la presente invención. El uso de tal criterio de detección se aplica ventajosamente a tanto el 60 problema de fallo al desactivar y los inconvenientes de falsa alarma. Como observación, aunque se describen las funciones para ajuste automático de la frecuencia umbral del accionador de alarma y relaciones de nivel de energía con referencia al controlador 106 del sistema EAS, se entiende que estas funciones no necesitan realizarse únicamente mediante el controlador 106. Se entiende que un dispositivo informático separado puede estar en comunicación electrónica con el controlador 106 y que este dispositivo informático separado puede programarse 65 para realizar las funciones para ajuste automático de los accionadores de alarma descritos en el presente documento.

La presente invención proporciona y define ventajosamente un sistema comprensivo y método para reducir falsas alarmas y fallos al desactivar en un sistema EAS que usa tecnologías de registro de datos en tiempo real.

5 La presente invención puede realizarse en hardware, software o una combinación de hardware y software. Una implementación del método y sistema de la presente invención puede realizarse en una manera centralizada en un sistema informático o en una manera distribuida donde se dispersan diferentes elementos a través de varios sistemas informáticos interconectados. Cualquier tipo de sistema informático, u otro aparato adaptado para realizar los métodos descritos en el presente documento, es adecuado para realizar las funciones descritas en el presente documento.

10 Una combinación típica de hardware y software podría ser un sistema informático de fin general o especializado que tenga uno o más elementos de procesamiento y un programa informático almacenado en un medio de almacenamiento que, cuando se carga y ejecuta, controla el sistema informático de manera que realiza los métodos descritos en el presente documento. La presente invención puede también embeberse en un producto de programa informático, que comprende todas las características que posibilitan la implementación de los métodos descritos en el presente documento, y que, cuando se cargan en un sistema informático puede realizar estos métodos. El medio de almacenamiento se refiere a cualquier dispositivo de almacenamiento volátil o no volátil.

15 El programa informático o aplicación en el presente contexto significa cualquier expresión, en cualquier lenguaje, código o notación, de un conjunto de instrucciones pretendidas para producir que un sistema que tiene una capacidad de procesamiento de información para realizar una función particular directamente o después o ambas de las siguientes a) conversión a otro lenguaje, código o notación; b) reproducción en una forma de material diferente. Además, a menos que anteriormente se haga mención de lo contrario, debería observarse que todos los dibujos adjuntos no son a escala. Significativamente, esta invención puede realizarse en otras formas específicas sin alejarse del espíritu o atributos esenciales de la misma, y por consiguiente, debería hacerse referencia a las siguientes reivindicaciones, en lugar de a la anterior memoria descriptiva, como indica el alcance de la invención.

20 Se apreciara por los expertos en la materia que la presente invención no está limitada a lo que se ha mostrado y descrito particularmente anteriormente en el presente documento. Son posibles diversas modificaciones y variaciones a la luz de las anteriores enseñanzas sin alejarse de los atributos esenciales de las mismas, y por consiguiente, debería hacerse referencia a las siguientes reivindicaciones, en lugar de a la anterior memoria descriptiva, como indica el alcance de la invención.



## REIVINDICACIONES

1. Un método para gestionar falsas alarmas por un sistema de vigilancia electrónica de artículos (100), comprendiendo el método: establecer una zona de detección (120); accionar un evento de alarma, el evento de alarma basado en la detección de una etiqueta en la zona de detección (120) usando una sensibilidad de accionador de alarma inicial, estando basada la sensibilidad de accionador de alarma inicial en un conjunto inicial de uno o más criterios de detección; y modificar el conjunto de criterios de detección para ajustar la sensibilidad de accionador de alarma del sistema de seguridad (100), en el que el conjunto de criterios de detección incluye un umbral de frecuencia y un umbral de relación de nivel de energía y en el que se acciona el evento de alarma si una relación de primer nivel de energía detectado a una primera frecuencia (f1), que es la frecuencia recibida válida de dicha etiqueta, a un segundo nivel de energía detectado a una segunda frecuencia (f2), que es la frecuencia desactivada esperada de dicha etiqueta, es mayor que un umbral de relación de nivel de energía predeterminado, **caracterizado por que** se reduce un intervalo de frecuencias de accionador de alarma válidas cuando una frecuencia media detectada para etiquetas que producen una alarma es mayor que el umbral de frecuencia.
2. El método de la reivindicación 1, que comprende adicionalmente determinar un motivo para el evento de alarma.
3. El método de la reivindicación 1, que comprende adicionalmente recibir un código de motivo, incluyendo el código de motivo información relacionada con el evento de alarma.
4. El método de la reivindicación 3, en el que modificar el conjunto de criterios de detección incluye: procesar información de código de motivo para determinar uno o más de los criterios de detección a modificar; y almacenar el uno o más criterios de detección modificados.
5. El método de la reivindicación 1, en el que se ajusta la sensibilidad de accionador de alarma para aumentar la sensibilidad de accionador de alarma del sistema de seguridad (100), aumentar la sensibilidad de accionador de alarma del sistema de seguridad (100) incluye aumentar el umbral de relación de nivel de energía predeterminado.
6. Un sistema de vigilancia electrónica de artículos adaptado para gestionar falsas alarmas (100), comprendiendo el sistema: un transmisor (112) que produce un campo de interrogación aplicado en una zona de detección (120); un procesador (106), funcionando el procesador (106) para: accionar un evento de alarma en respuesta a la detección de una etiqueta en la zona de detección (120) usando una sensibilidad de accionador de alarma inicial, estando basada la sensibilidad de accionador de alarma inicial en un conjunto inicial de uno o más criterios de detección; y modificar el conjunto de criterios de detección para ajustar la sensibilidad de accionador de alarma del sistema de seguridad (100), en donde el conjunto de criterios de detección incluye un umbral de frecuencia y un umbral de relación de nivel de energía y en donde el procesador (106) funciona para accionar el evento de alarma si una relación de primer nivel de energía detectado a una primera frecuencia (f1), que es la frecuencia recibida válida de dicha etiqueta, a un segundo nivel de energía detectado a una segunda frecuencia (f2), que es la frecuencia desactivada esperada de dicha etiqueta, es mayor que un umbral de relación predeterminado, **caracterizado por que** el procesador (106) funciona adicionalmente para reducir un intervalo de frecuencias de accionador de alarma válidas cuando una frecuencia media detectada para etiquetas que producen una alarma es mayor que el umbral de frecuencia.
7. El sistema de la reivindicación 6, en el que el procesador (106) funciona adicionalmente para determinar la causa del evento de alarma.
8. El sistema de la reivindicación 6, en el que modificar el conjunto de criterios de detección incluye: procesar información de código de motivo para determinar uno o más de los criterios de detección para modificar; y almacenar el uno o más criterios de detección modificados.
9. El sistema de la reivindicación 6, en el que el procesador (106) funciona adicionalmente para ajustar la sensibilidad de accionador de alarma aumentando la sensibilidad de accionador de alarma del sistema de seguridad, aumentar la sensibilidad de accionador de alarma del sistema de seguridad incluye aumentar el umbral de relación de nivel de energía predeterminado.
10. Un producto de programa informático que comprende un medio que puede usar un ordenador que tiene un programa legible por ordenador para un sistema de vigilancia electrónica de artículos que cuando se ejecuta en un ordenador hace que el ordenador realice un método que comprende: establecer una zona de detección; accionar un evento de alarma, usando el evento de alarma basado en la detección de una etiqueta en la zona de detección una sensibilidad de accionador de alarma inicial, estando basada la sensibilidad de accionador de alarma inicial en un conjunto inicial de uno o más criterios de detección; y modificar el conjunto de criterios de detección para ajustar la sensibilidad de accionador de alarma del sistema de seguridad (100), en donde el conjunto de criterios de detección incluye un umbral de frecuencia y un umbral de relación de nivel de energía, y en donde se acciona el evento de alarma si una relación de primer nivel de energía detectado a una primera frecuencia (f1), que es la frecuencia recibida válida de dicha etiqueta, a un segundo nivel de energía detectado a una segunda frecuencia (f2), que es la frecuencia desactivada esperada de dicha etiqueta, es mayor que un umbral de relación de nivel de energía

predeterminado, en donde se ajusta la sensibilidad de accionador de alarma para aumentar la sensibilidad de accionador de alarma del sistema de seguridad (100), incluyendo aumentar la sensibilidad de accionador de alarma del sistema de seguridad (100) aumentar el umbral de relación de nivel de energía predeterminado, **caracterizado por que** se reduce un intervalo de frecuencias de accionador de alarma válidas cuando una frecuencia media detectada para etiquetas que producen una alarma es mayor que el umbral de frecuencia.

5

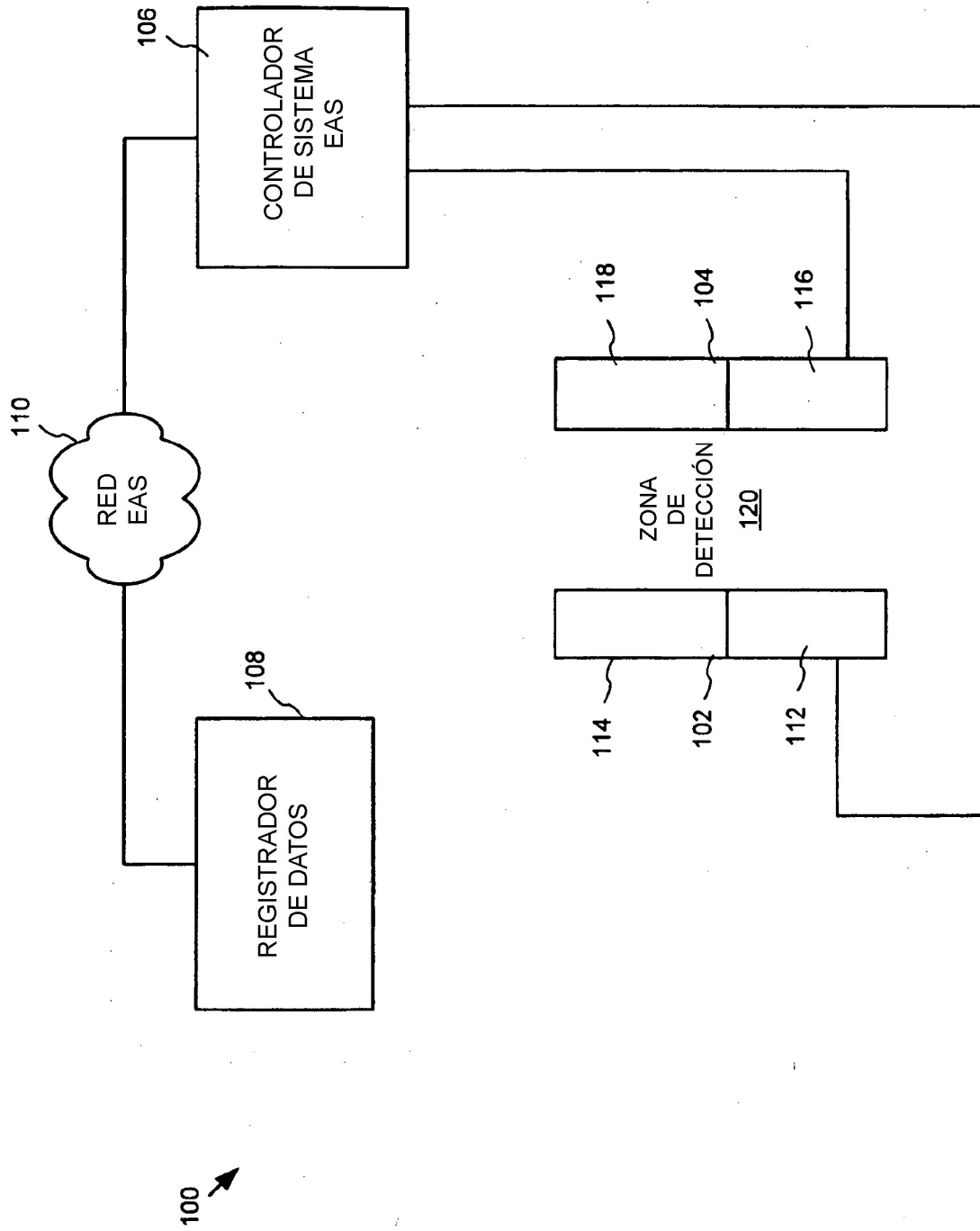
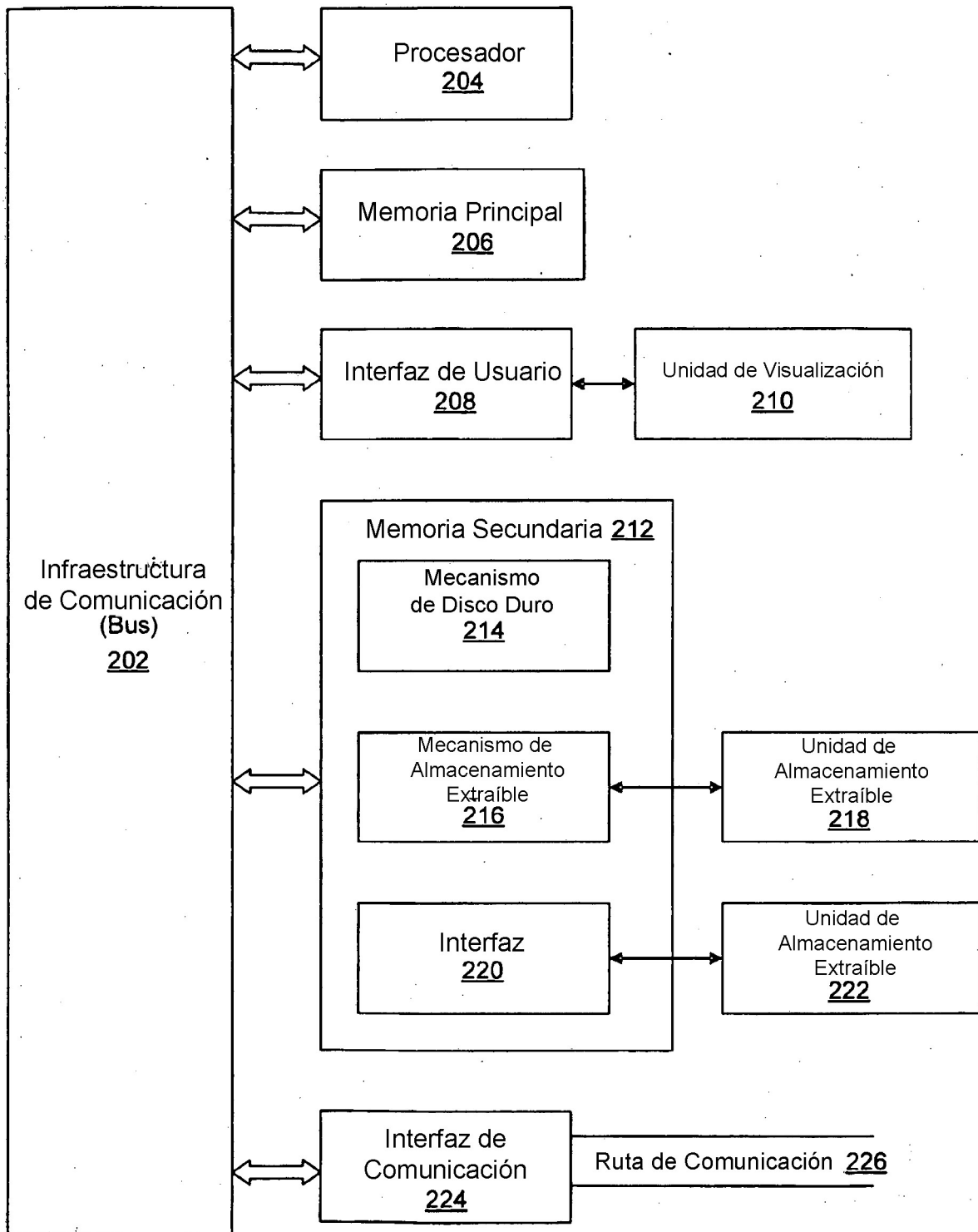


FIG. 1



**FIG. 2**

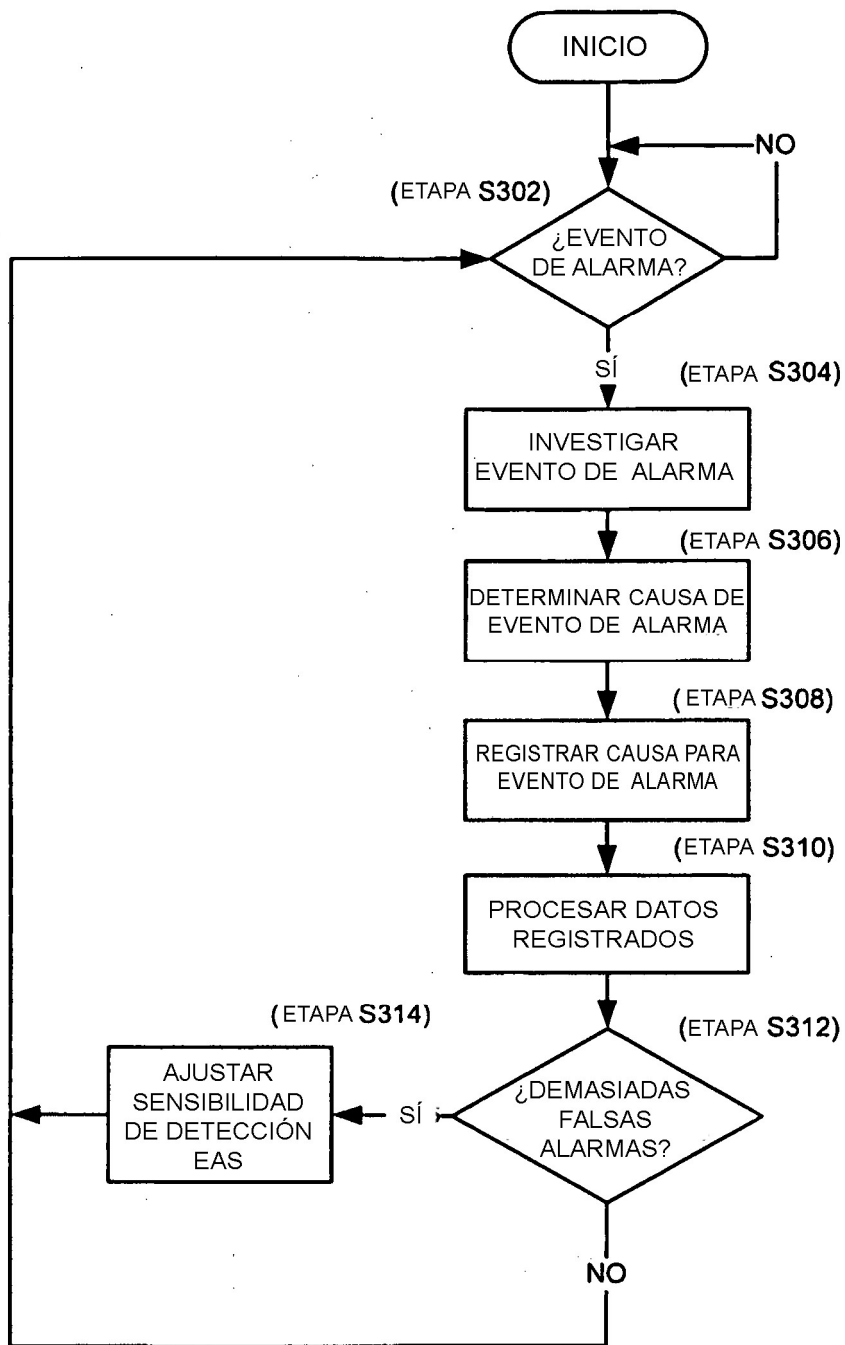
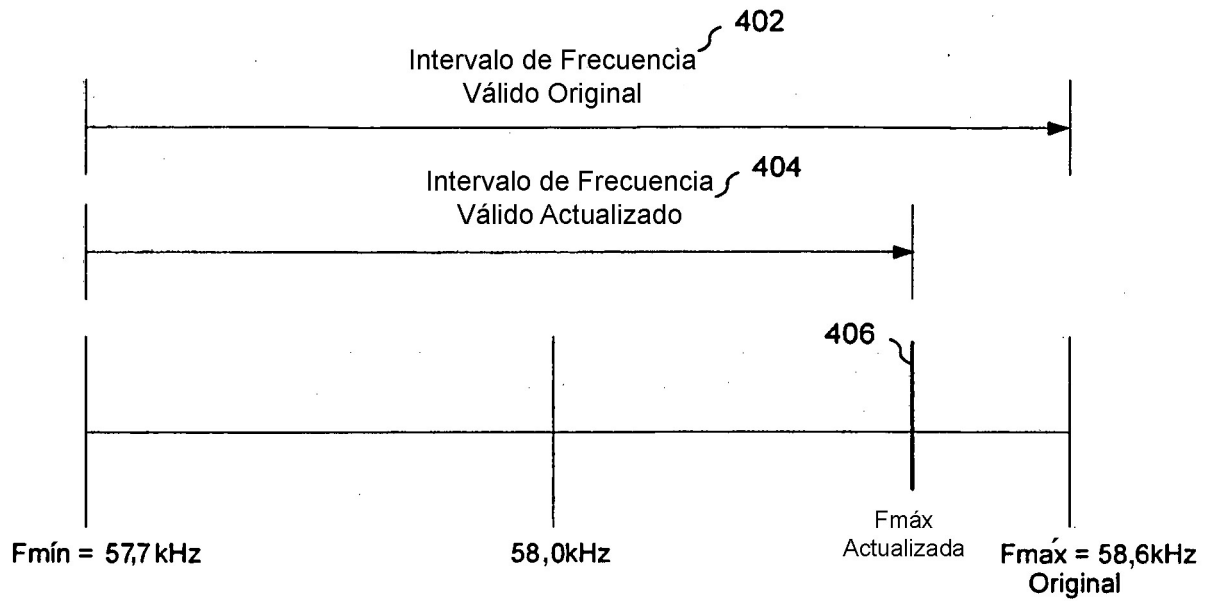


FIG. 3



**FIG. 4**

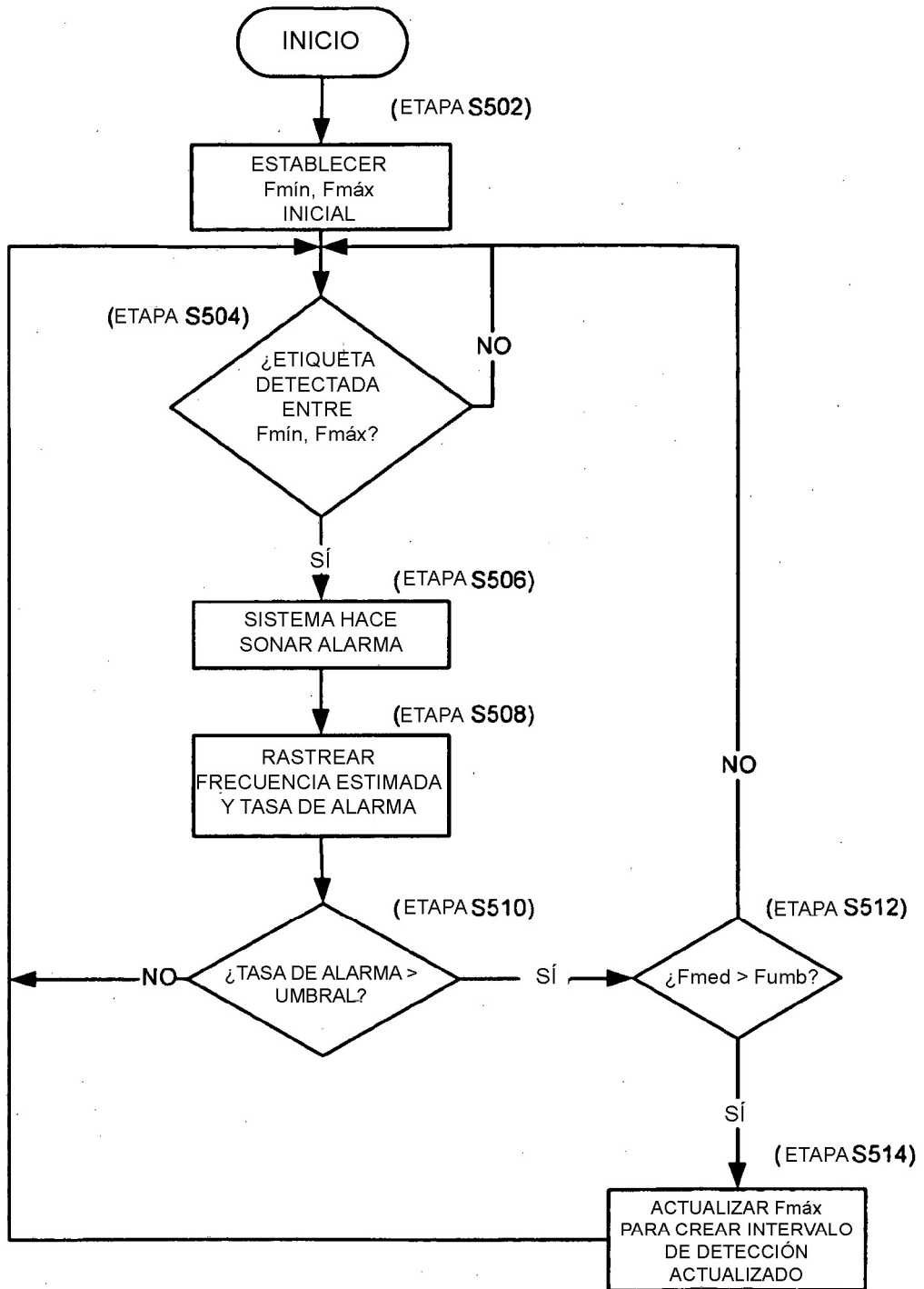


FIG. 5

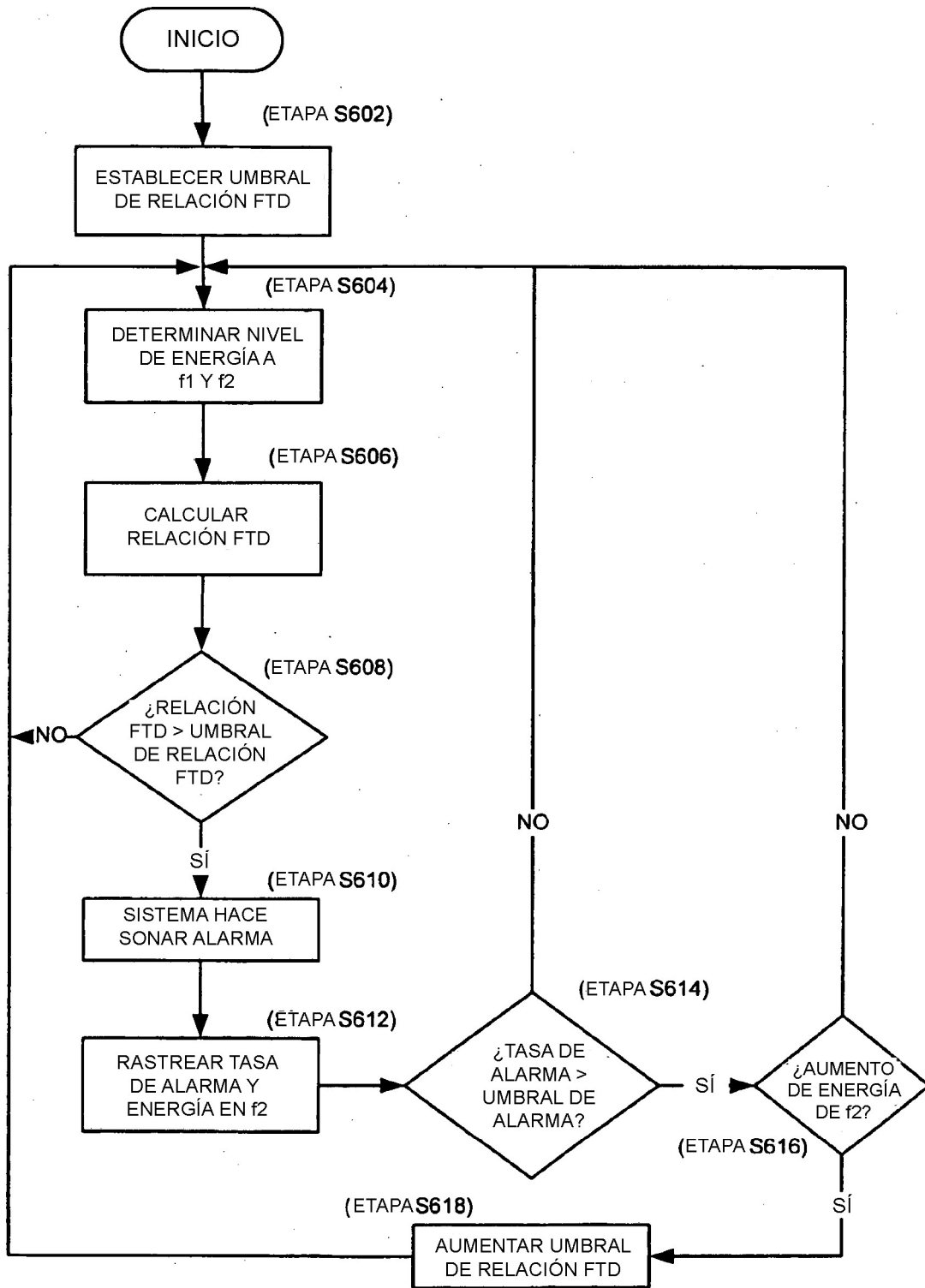


FIG. 6