

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 786 316**

51 Int. Cl.:

G08B 25/14 (2006.01)

G06Q 10/06 (2012.01)

G08B 31/00 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **29.12.2015 PCT/GB2015/054174**

87 Fecha y número de publicación internacional: **07.07.2016 WO16108047**

96 Fecha de presentación y número de la solicitud europea: **29.12.2015 E 15820244 (0)**

97 Fecha y número de publicación de la concesión europea: **29.01.2020 EP 3241201**

54 Título: **Sistema de supervisión remoto de múltiples alarmas**

30 Prioridad:

29.12.2014 GB 201423300

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

09.10.2020

73 Titular/es:

**FIREANGEL SAFETY TECHNOLOGY LIMITED
(100.0%)**

**Unit 10, Vanguard Centre, Sir William Lyons Road
Coventry CV4 7EZ, GB**

72 Inventor/es:

**RUTTER, NICHOLAS;
BOLGER, CHRIS y
BRIGHAM, PETER**

74 Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

ES 2 786 316 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

Sistema de supervisión remoto de múltiples alarmas

5 Campo de la invención

Esta invención se refiere a un sistema para supervisar remotamente alarmas de seguridad en una ubicación de instalación, y determinar y notificar un nivel de riesgo asociado. Las alarmas de seguridad pueden incluir detectores de calor, detectores de monóxido de carbono, detectores de humo y otras alarmas de seguridad. Más específicamente, la presente invención se refiere a sistemas y métodos que usan lógica de decisión para gestionar la emisión de notificaciones de alerta basándose en un historial de datos de eventos de alarma, en los que los datos de eventos de alarma comprenden activación de una alarma, procedimientos de prueba en la alarma o incluso un mal funcionamiento de la alarma.

15 Antecedentes

Una disposición convencional en, por ejemplo, una residencia doméstica, implica alarmas de seguridad autónomas. Cuando se activan, como consecuencia del catalizador pertinente o procedimiento de prueba de alarma, funciona una alarma audible y/o visual; esto se conoce como un evento de alarma. Un evento de alarma alerta a los habitantes o individuos cercanos para que adopten una acción. También se conoce tener alarmas, en particular alarmas contra humo, conectadas al parque de bomberos más cercano a través de la red de teléfono. En este caso, la activación de la alarma de humo en la residencia, escuela, oficina o fábrica provocará que se desencadene una función de alerta asociada en el parque de bomberos.

El documento US 8.988.232 B1 divulga un método de determinación de una cantidad de tiempo durante el cual está presente una condición peligrosa, y generación de un resultado en respuesta a si la cantidad de tiempo ha alcanzado o no al menos una duración umbral. El documento US2011/0254681A1 se refiere a un método para verificación de alarma que incluyen las etapas de recopilación de datos que representa un evento de alarma potencial y aplicación de los datos recopilados a un módulo de verificación de alarma.

La hora y fecha de un evento de alarma y la ubicación y tipo de alarma que se activó, son datos que son únicos para cada evento de alarma. Tal información tiene un valor considerable que tiene que reconocerse o utilizarse en sistemas de alarma convencionales.

Es un objetivo de la presente invención proporcionar un sistema de supervisión de alarma de seguridad que utiliza información de evento de alarma histórica para determinar un factor de riesgo para una ubicación particular y para comunicar este factor de riesgo a una tercera parte.

Sumario de la invención

De acuerdo con un primer aspecto de la presente invención, se proporciona un sistema de supervisión de alarma remoto como se define en la reivindicación 1.

El sistema de supervisión de alarma remoto se configura para registrar y procesar datos de eventos de alarma, el sistema de alarma que comprende: una instalación de alarma que comprende uno o más dispositivos de alarma en conexión con una interfaz, en el que la interfaz se configura para recibir datos de eventos de alarma; un servidor en comunicación con la interfaz, en el que el servidor se configura para recibir y procesar datos de eventos de alarma de la interfaz; y uno o más dispositivos de cliente en red en comunicación con el servidor, en el que el servidor se configura para transmitir un mensaje al dispositivo de cliente en red, basándose dicho mensaje en los datos de eventos de alarma procesados. El servidor se configura para provocar una respuesta diferente para el mismo evento de alarma dependiendo de un nivel de riesgo asignado a la instalación de alarma.

En las realizaciones del primer aspecto, los datos de eventos de alarma procesados se basan en un análisis del patrón y/o la frecuencia de eventos de alarma y una evaluación de un nivel de riesgo basándose en los resultados de análisis.

Se entenderá que la frecuencia de eventos de alarma puede basarse en datos de eventos de alarma históricos, es decir, un historial o registro de eventos de alarma pasados, del uno o más dispositivos de alarma.

En las realizaciones, los datos de eventos de alarma procesados se basan en un análisis del tipo de eventos de alarma y una evaluación de un nivel de riesgo basándose en los resultados de análisis.

Como se especifica a continuación, datos de eventos de alarma pueden incluir la fecha y hora del evento, un identificador del dispositivo de alarma que detecta el evento y también la naturaleza del evento, tal como una activación de la alarma, un procedimiento de prueba en la alarma o incluso un mal funcionamiento de la alarma. Datos de eventos de alarma pueden incluir la fecha y hora en que se silencia una alarma (por ejemplo, después de

una alerta molesta o prueba), o el tiempo transcurrido entre un evento de alarma y la alarma silenciándose.

La conexión entre el uno o más dispositivos de alarma y la interfaz puede ser una conexión de red inalámbrica.

5 Cada uno del uno o más dispositivos de alarma puede configurarse para almacenar datos de eventos de alarma, incluyendo los datos de eventos de alarma activación de una alarma, procedimientos de prueba en la alarma o un mal funcionamiento de la alarma, para su transmisión al servidor.

10 Esto permite que datos de eventos de alarma se retransmitan una vez que se ha establecido una conexión fiable con el servidor.

El uno o más dispositivos de alarma pueden almacenar datos de eventos de alarma dentro de cada dispositivo de alarma antes de la transmisión de los datos de evento de alarma a la interfaz.

15 El análisis del patrón y/o la frecuencia de eventos de alarma pueden tener en cuenta eventos de alarma no peligrosos.

20 Eventos de alarma no peligrosos incluyen funciones de test, y el silenciamiento de alarmas en una situación no peligrosa. Eventos de alarma no peligrosos pueden incluir el tiempo entre un evento de alarma y la activación de la función de silenciamiento. Eventos de alarma no peligrosos pueden incluir datos de sensor de antecedentes, tales como un patrón de la actividad de sensor.

Esto aumenta la autonomía de un dispositivo de alarma.

25 De acuerdo con un segundo aspecto de la presente invención, se proporciona adicionalmente un servidor como se define en la reivindicación 6.

30 El servidor se configura para procesar datos de eventos de alarma, para recibir datos de eventos de alarma desde una instalación de alarma a través de una interfaz; analizar el patrón, frecuencia y/o tipo de eventos de alarma; comparar los datos analizados con criterios predeterminados; y transmitir un mensaje al dispositivo de cliente en red basándose en los resultados de comparación. El servidor se configura para provocar una respuesta diferente para el mismo evento de alarma dependiendo de un nivel de riesgo asignado a la instalación de alarma.

35 En las realizaciones del segundo aspecto, la etapa de comparación de los datos de eventos de alarma analizados con los criterios predeterminados resulta en un nivel de riesgo específico para la instalación.

Los criterios predeterminados pueden incluir datos históricos almacenados específicos para la instalación asociada.

40 La etapa de comparación de los datos de eventos de alarma analizados con los criterios predeterminados puede resultar en un nivel de riesgo específico para la instalación.

Los criterios predeterminados pueden incluir datos históricos almacenados específicos para la instalación asociada.

45 Los criterios predeterminados pueden incluir análisis continuo del patrón, frecuencia y/o tipo de los datos de evento de alarma de la instalación asociada.

El servidor puede tener en cuenta el número de eventos de alarma no peligrosos cuando se analiza el patrón y/o la frecuencia de eventos de alarma.

50 De acuerdo con un tercer aspecto de la presente invención, se proporciona un método para supervisar remotamente alarmas como se define en la reivindicación 9.

55 El método comprende las etapas de: recepción de datos de eventos de alarma en una interfaz desde uno o más dispositivos de alarma comprendidos en una instalación de alarma; transferencia de datos de eventos de alarma desde la interfaz a un servidor; procesamiento de los datos de eventos de alarma en el servidor; y transmisión de un mensaje a al menos un dispositivo de cliente en red basándose en los datos de eventos de alarma procesados. El método comprende la etapa del servidor que provoca una respuesta diferente para el mismo evento de alarma dependiendo de un nivel de riesgo asignado a la instalación de alarma.

60 Como se expone en más detalle a continuación, una interfaz puede ser integral con un dispositivo de alarma.

En las realizaciones del tercer aspecto, la etapa de procesamiento de los datos de eventos de alarma puede comprender analizar el patrón, frecuencia y/o tipo de eventos de alarma, y evaluar el nivel de riesgo basándose en los resultados de análisis.

65 El método para supervisar remotamente alarmas de seguridad puede comprender adicionalmente la etapa de

almacenamiento de datos de eventos de alarma localmente en el uno o más dispositivos de alarma para su transmisión al servidor.

5 El método para supervisar remotamente alarmas de seguridad puede comprender adicionalmente las etapas de:
almacenamiento de datos de eventos de alarma localmente en el uno o más dispositivos de alarma; y transmisión de
datos de eventos de alarma desde los dispositivos de alarma a la interfaz.

10 En el método para supervisar remotamente alarmas de seguridad, la etapa de análisis del patrón y/o la frecuencia de
eventos de alarma pueden tener en cuenta el número de eventos de alarma no peligrosos.

De esta manera, se consigue de forma eficiente una supervisión automatizada remota de alarmas de seguridad de
forma continua.

15 Características de las realizaciones del primer, segundo y tercer aspectos pueden combinarse. Por ejemplo, etapas
de método de acuerdo con realizaciones del tercer aspecto pueden efectuarse usando configuraciones de las
realizaciones del primer aspecto.

Descripción de las figuras

20 Realizaciones de la invención se describirán ahora, a modo de ejemplo, con referencia a los dibujos adjuntos, en los
que:

25 La Figura 1 es una ilustración esquemática de un sistema de supervisión de alarma de acuerdo con una
realización de la presente invención; y

La Figura 2 es un diagrama de proceso de las etapas realizadas en el servidor por el algoritmo de la presente
invención.

Descripción

30 La Figura 1 ilustra esquemáticamente el sistema de supervisión de alarma 10 de la presente invención. Una o más
alarmas 12 (en la Figura 1: cuatro dispositivos de alarma 12) instaladas en una o más ubicaciones comprenden una
red de alarma. Datos de la red de alarma se transmiten a través de una interfaz 14 a una red de telecomunicaciones
móvil 16 tal como GSM, UMTS o a través de TCP/IP. La interfaz puede ser por cable y/o inalámbrica. Un servidor
35 basado en la nube 18 recibe posteriormente los datos.

Los datos desde la una o más alarmas 12 se denominan como datos de eventos de alarma. Los datos de eventos de
alarma especifican la fecha y hora del evento y también la naturaleza del evento, tal como una activación de la
alarma, un procedimiento de prueba en la alarma o incluso un mal funcionamiento de la alarma.

40 Se entenderá que una alarma 12 puede incorporarse en forma de un detector capaz de determinar un cambio en
una condición ambiental. La condición ambiental puede ser un nivel de temperatura (calor), nivel de monóxido de
carbono, nivel de humo u otra condición. El detector puede ser capaz de supervisar una pluralidad de condiciones
ambientales. Si la condición ambiental está fuera de límites permisibles, la alarma indica esto localmente mediante
45 una señal, que puede ser audible y/o visual, en forma de un evento de alarma anteriormente mencionado.

Un detector es capaz de supervisar su estado. El estado puede indicar que el detector está operando dentro de
parámetros predeterminados, o que se ha producido un fallo. El estado puede incluir estado de potencia y/o estado
de sensor. Por ejemplo, un detector puede supervisar si su fuente de alimentación está o no interrumpida. Un
50 detector puede supervisar si un nivel de batería está demasiado bajo. Un detector puede supervisar si un nivel de
batería está bajando a una tasa más rápida de la esperada. Un detector puede supervisar el rendimiento de
sensores ópticos. La información de estado puede incluirse en los datos de eventos de alarma. Esta puede usarse
en la determinación de un patrón en datos de eventos de alarma.

55 La alarma es un dispositivo autónomo. Por "autónomo", se entiende que la alarma puede operar como un dispositivo
independiente, independientemente de si o se conecta o no a un servidor basado en la nube 18. Sin embargo, si se
establece una conexión de datos entre la alarma y el servidor 18, pueden transmitirse datos de eventos de alarma
desde el dispositivo de alarma al servidor 18.

60 Los datos se procesan a través de una aplicación ejecutándose en el servidor 18 en el que se analizan variables
tales como el número de eventos de alarma durante un periodo de tiempo.

Un análisis puede tener en cuenta el tipo de la alarma. El tipo de alarma puede determinarse mediante la sustancia o
condición supervisada por la alarma. Esta puede incluir humo, calor, monóxido de carbono, temperaturas extremas,
65 niveles de gas, niveles de contaminación u otros.

Un análisis puede tener en cuenta la ubicación de una alarma dentro de la propiedad. Por ubicación, se quiere decir el área supervisada por el detector. Por ejemplo, la ubicación puede ser un nivel de planta supervisado por la alarma. La ubicación puede clasificarse por uso, o uso previsto. Una ubicación puede ser un área de cocina. Por ejemplo, alertas falsas debido a humo de una tostadora pueden calificarse de forma diferente en un área de cocina que un área distinta de la cocina. Una ubicación puede ser un área húmeda. Por ejemplo, alertas falsas debido a vapor pueden calificarse de forma diferente en un baño.

5

Un análisis puede tener en cuenta el número de lote de un dispositivo de alarma o su estado.

10 Sometido a los resultados de tal análisis, se genera automáticamente un mensaje 20 y transmite a través de correo electrónico, mensaje de texto o medios electrónicos similares a un dispositivo de cliente en red 22 de un receptor predeterminado. El dispositivo de cliente en red 22 puede ser un ordenador de sobremesa, un portátil, una tableta o teléfono inteligente o similar. El dispositivo de cliente en red 22 puede ser un dispositivo distinto de la alarma 12.

15 La aplicación ejecutándose en el servidor 18 se configura para analizar datos de un único tipo de alarma 12 en una o más ubicaciones tales como un edificio residencial, escuela, oficina o fábrica para crear un historial de eventos de alarma. Además, la aplicación ejecutándose en el servidor 18 se configura para analizar también datos de múltiples tipos de alarma 12 dentro de una única ubicación para crear un historial de eventos de alarma.

20 La aplicación se configura para analizar el historial de eventos de alarma para determinar si algún patrón es evidente. Patrones de eventos de alarma repetidos desde una única ubicación dentro de un periodo de tiempo predeterminado puede indicar un problema en esa ubicación que necesita abordarse. Específicamente, un cierto patrón se refiere a un cierto grado de riesgo en una ubicación, mientras que un patrón diferente se refiere a un grado diferente de riesgo en una ubicación. Si el riesgo en una cierta ubicación excede un nivel predeterminado, a continuación se envía automáticamente un mensaje adecuado 20 a un receptor predeterminado, es decir, a una tercera parte, para recibirse en su teléfono móvil, línea terrestre, tableta, P.C. u otros medios de telecomunicaciones 22. El nivel predeterminado puede variar instalación por instalación, dependiendo de factores en cada instalación.

25

30 El receptor predeterminado o tercera parte responsable puede ser, a modo de ejemplo, servicios de atención comunitaria de bomberos y salvamento o un familiar del propietario de la alarma de incendios o un servicio de mantenimiento de alarma. El receptor predeterminado o tercera parte responsable puede ser una persona o entidad con un interés o con una obligación de supervisar un número de edificios simultáneamente, tal como un arrendador privado, un arrendador social, un administrador de propiedad, una autoridad local o una asociación de viviendas. El receptor predeterminado o tercera parte responsable puede ser un cuidador o un familiar.

35

40 El nivel predeterminado puede incorporarse en forma de un umbral de riesgo. Un umbral de riesgo diferente puede asociarse con diferentes instalaciones. Por ejemplo, si uno o más dispositivos de alarma 12 se instalan en la cocina de inmuebles residenciales y si más de un evento de alarma humo se registra en el periodo de 10 días, entonces se enviará una alerta a uno o más dispositivos de comunicación 22 de la tercera parte. Por ejemplo, si el ocupante es una persona mayor que vive sola, entonces el cuidador asignado o familiar recibirá la alerta. La alerta puede comprender diversos tipos y niveles de información; la alerta puede especificar la naturaleza y veces de los eventos de alarma, o la alerta puede especificar simplemente que se requiere una comprobación del inmueble contactando o visitando al ocupante.

45 Análogamente, pueden asociarse diferentes umbrales de riesgo para instalaciones dependiendo del tamaño, condición y/o antigüedad de una propiedad, el número de ocupantes, la ocupación de los ocupantes (por ejemplo, estudiante, pensionista), la edad de ocupantes, registros médicos, salud mental, drogodependencia, o cualquier combinación de estos factores.

50 La interfaz 14 funciona para transferir datos de eventos de alarma desde la red de alarma a la internet o red de telecomunicaciones móvil 16. La interfaz 14 puede ser inalámbrica o realizarse en hardware. Por ejemplo, la interfaz 14 puede comprender un módem de banda ancha o concentrador doméstico, o cualquier otro medio de transferencia de datos desde los sistemas de alarma 12 a la internet o red de telecomunicaciones móvil 16.

55 Una única ubicación, tal como una residencia, edificio de escuela, edificio de oficinas o fábrica puede tener instaladas varias alarmas de seguridad. Estas alarmas 12 pueden tener diversas posiciones dentro de un edificio y pueden instalarse diversos tipos de alarma de seguridad. Cada alarma 12 puede identificarse inequívocamente en el sistema de supervisión de la presente invención. Un registro de eventos de alarma puede almacenarse en un microchip dentro de cada dispositivo de alarma 12 y transmitirse a continuación periódicamente a la interfaz 14. Como alternativa, cada evento de alarma que se produce en un dispositivo de alarma 12 puede transmitirse instantáneamente a la interfaz 14.

60

65 Se conoce que alarmas de seguridad tienen una función de prueba de dispositivo, que comprende un botón que puede presionarse para establecer que el dispositivo está funcionando correctamente. Por lo tanto, un evento de alarma que puede supervisarse usando la presente invención es la activación de la función de prueba de una alarma. Por ejemplo, puede ser de ayuda que la tercera parte responsable conozca que su dependiente anciano

está presionando repetidamente el botón de prueba, es decir, con una mayor frecuencia de la que se esperaría normalmente, ya que esto puede indicar que la persona anciana está preocupada del funcionamiento de la alarma provocándoles de esta manera preocupación o estrés.

5 Cuando se produce un evento de alarma de seguridad de forma inapropiada, esto puede denominarse como una alarma molesta. Un ejemplo de una alarma molesta de este tipo es la activación de una alarma de humo por humos de cocina normales. En consecuencia, el usuario presionaría el botón de reinicio en el cuerpo de alarma para silenciar la alarma, ya que no hay un peligro inminente. La presente invención puede registrar el lapso de tiempo entre el evento de alarma de seguridad y la activación de la función de reinicio. El experto entenderá que tales datos de comportamiento son valiosos para analizar el factor de riesgo en una ubicación. Por ejemplo, una alarma molesta puede notarse y silenciarse rápidamente por el usuario presionando el botón de reinicio, o una alarma molesta puede reiniciarse únicamente después de un periodo prolongado, o no. En cualquier ejemplo, la cantidad de tiempo que lleva reiniciar la alarma en combinación con otros factores (tal como la ubicación de instalación) se usa para determinar un nivel de riesgo en una ubicación.

15 Cada alarma de seguridad 12 instalada en el sistema 10 de la presente invención está provista de la instalación para almacenar un registro de eventos de alarma en una memoria no volátil dentro de la electrónica de alarma ubicada dentro de la carcasa de la alarma. Además, cada alarma de seguridad 12 tiene la instalación para transmitir los datos de eventos de alarma a través de una red inalámbrica.

20 La Figura 2 ilustra las etapas de un método para procesar los datos de eventos de alarma. La primera etapa 24 comprende la recepción de datos de eventos de alarma desde la interfaz. La segunda etapa 26 comprende un análisis del patrón, frecuencia y/o tipo de eventos de alarma. En la tercera etapa 28, los resultados de análisis se comparan con criterios de riesgo predeterminados. La cuarta etapa 30 comprende transmitir un mensaje a un dispositivo de cliente en red específico de una tercera parte especificando un nivel de riesgo en la instalación y/o acción a tomar por la tercera parte.

25 Las etapas de método citadas en la Figura 2 se realizan por un algoritmo de la presente invención ejecutándose en el servidor basado en la nube 18.

30 Se prevé que una única entidad comercial puede proporcionar todo el servicio con respecto a la presente invención. Específicamente, se prevé proporcionar e instalar la alarma de seguridad o alarmas en uno o más inmuebles y proporcionar la infraestructura de red para soportar la función de supervisión remota. Además, realizaciones de la invención permiten determinar, y posteriormente actualizar, los criterios de riesgo predeterminados con respecto a cada instalación de alarma. Esto puede conseguirse a través de consulta con la tercera parte responsable, que, en muchos casos, puede también ser el cliente o gestor de la entidad comercial. Igualmente, diferentes entidades comerciales pueden proporcionar diversas partes de la instalación de alarma y servicio de supervisión remoto.

35 Puede asignarse un perfil de riesgo tras la instalación de un dispositivo de alarma. El mismo perfil de riesgo puede asignarse a un grupo de dispositivos de alarma basándose en criterios de clasificación similares. Por ejemplo, el perfil de riesgo puede asignarse sobre la base de factores que incluyen si los dispositivos de alarma 12 pertenecen o no al mismo sistema de alarma 10, la propiedad tipo (por ejemplo, residencial o comercial), la ubicación dentro de una propiedad, y cualquiera de los criterios anteriormente listados, tal como número, ocupación y/o número y edad de ocupantes. Los factores pueden basarse en políticas de servicios de bomberos y salvamento y/o en consideraciones regionales. El perfil de riesgo puede establecerse manualmente. Puede ser adecuado usar uno de tres niveles de riesgo, tales como "bajo", "medio", "alto". Puede establecerse cualquier número de niveles de riesgo como apropiado para un tipo de instalación o según se requiera por una tercera parte.

40 Ya que la aplicación se configura para determinar patrones de eventos de alarma a partir de un análisis de eventos de alarma históricos, esto permite que el perfil de riesgo para una instalación dada se ajuste basándose en un patrón de eventos de alarma. Por ejemplo, a una instalación con un perfil de riesgo inicialmente bajo puede asignarse un perfil de riesgo mayor cuando se observa una mayor frecuencia de eventos de alarma.

45 Análogamente, un cambio en un patrón de eventos de alarma puede indicar un problema subyacente que, en sí mismo, no es suficientemente crítico para suscitar una alerta de peligro local, pero que justifica una notificación a una tercera parte. Por ejemplo, una persona anciana puede probar habitualmente un dispositivo de alarma una vez por semana como parte de su rutina (por ejemplo, cada viernes por la mañana). Una desviación de la rutina (por ejemplo, prueba irregular en diferentes momentos del día y pruebas inusualmente frecuentes durante toda la semana) puede indicar un problema de salud subyacente, tal como la enfermedad de Alzheimer incipiente. Una desviación de la rutina puede ser apreciable por un cambio del patrón de eventos de alarma (y/o frecuencia). Un algoritmo puede recoger un cambio de este tipo y emitir un mensaje de notificación a una tercera parte.

50 Análogamente, un algoritmo puede tener en cuenta un cambio en la duración requerida para silenciar una alarma molesta, como se ha descrito anteriormente. Por ejemplo, puede esperarse que una alarma molesta se silencie dentro de un corto periodo de tiempo (por ejemplo, dentro de menos de un minuto). Si el tiempo de respuesta se desvía de un intervalo esperado (por ejemplo, se tarda mucho más de un minuto en silenciar una alarma molesta),

esto puede indicar un problema subyacente.

El algoritmo puede tener en cuenta una combinación de dos o más desencadenantes diferentes (por ejemplo, tanto un cambio en comportamiento de pruebas como un cambio en el tiempo de respuesta a una alarma molesta), o cualquier número de tipos de eventos de alarma.

El algoritmo puede proporcionar como parte de la alerta notificación una salida que sugiere un nivel de riesgo más apropiado, por ejemplo, un nivel de riesgo mayor (de bajo a medio, de bajo a alto o de medio a alto), para que una tercera parte lo establezca manualmente.

Para ilustrar esto mejor con un ejemplo, a una instalación puede asignarse uno de tres niveles de riesgo, tal como riesgo bajo, riesgo medio o riesgo alto. Un evento de alarma provocará una respuesta diferente dependiendo del nivel de riesgo de la instalación. Por ejemplo, en una instalación de riesgo bajo, puede registrarse un evento de alarma sin que se envíe un mensaje 22 a una tercera parte. En una instalación de riesgo medio, el mismo evento de alarma puede provocar que el sistema de alarma genere un mensaje de notificación a un encargado. En una instalación de riesgo alto, el mismo evento de alarma puede provocar que el sistema de alarma alerte a un servicio de bomberos y salvamento.

Para proporcionar un ejemplo para una instalación de riesgo bajo, un evento de alarma típico puede ser una alerta de humo en una cocina. Una alarma de humo en un alojamiento para estudiantes puede clasificarse como una instalación de riesgo bajo. Si se detecta un único evento de alarma de humo (por ejemplo, una alarma molesta) por un único dispositivo de alarma, esto se registrará como un evento de alarma por el servidor, pero no se envía ningún mensaje de alarma 20 a una tercera parte. Si, sin embargo, se detectan dos o más eventos de alarma de humo dentro de una ventana temporal predeterminada, o por dos dispositivos de alarma en proximidad cercana, esto puede indicar un problema y el servidor emitirá un mensaje de alarma 20 para alertar a una tercera parte. Por ejemplo, puede alertarse a un encargado de un caso de repetición de alarma de humo.

Para proporcionar un ejemplo de una instalación de riesgo alto, una alarma de humo en la casa de una persona vulnerable puede clasificarse como una instalación de riesgo alto. En ese caso, el único evento de alarma de humo por un único dispositivo de alarma se retransmite como una alerta a una tercera parte. Por ejemplo, una alerta puede retransmitirse directamente a un servicio de bomberos y salvamento.

Como se ha expuesto anteriormente, datos de eventos de alarma pueden incluir condiciones no peligrosas, tal como procedimientos de prueba o mensajes de estado que indican un mal funcionamiento de un dispositivo de alarma. El dispositivo de alarma puede configurarse para no indicar un mensaje de aviso de la condición no peligrosa si los datos de eventos de alarma pueden retransmitirse a un servidor.

Para proporcionar otro ejemplo, si un dispositivo de alarma se silencia repetidamente, es decir, con una mayor frecuencia de la que se esperaría normalmente, el sistema de alarma permite que cada silenciamiento se registre como un evento de alarma. Dependiendo del perfil de riesgo, puede enviarse una prealerta o alerta en forma de un mensaje 20 a una tercera parte si el número de eventos de silenciamiento se produce con demasiada frecuencia (por ejemplo, más de 3 veces un día).

En particular, no es necesario que el dispositivo de alarma haga sonar una alerta. Por ejemplo, puede generarse un mensaje 20 porque un botón de prueba se presiona con demasiada frecuencia. En sistemas de alarma con dispositivos de alarma aislados, no se conocía hasta ahora la utilización de tales datos de eventos de alarma en la determinación de un factor de riesgo. El sistema de alarma de la presente invención permite que se incluyan datos de eventos de alarma de condiciones no peligrosas en la determinación de si un peligro está o no presente.

Eventos de alarma no peligrosos pueden incluir datos de sensor de antecedentes, tales como un patrón de la actividad de sensor. Por ejemplo, un sensor de un dispositivo de alarma puede supervisar un nivel de peligro, y puede configurarse forma rutinaria para hacer sonar una alerta si el nivel de peligro excede un nivel de umbral predeterminado ("nivel desencadenador"). Los datos de eventos de alarma pueden incluir datos de sensor de fondo que estaban por debajo de nivel desencadenador. Por ejemplo, los datos de eventos de alarma pueden incluir la hora, fecha y otros datos de dispositivo de alarma para cada vez que el nivel de peligro excedió el 50 %, o 2/3, del nivel desencadenador. Como tal, el patrón de la actividad de sensor puede elevarse por encima del ruido de fondo, pero no lo suficientemente alto para desencadenar una alerta localmente. Por lo tanto, no se esperará que el nivel de peligro provoque que un dispositivo de alarma haga sonar una alarma localmente. Sin embargo, el patrón puede analizarse por el servidor como significativo para justificar la notificación a una tercera parte. El servidor puede, por consiguiente, enviar una notificación a una tercera parte. Esto proporciona una oportunidad para que la tercera parte investigue el problema.

Por ejemplo, un número creciente de eventos de alarma no peligrosos puede indicar un deterioro de un entorno y puede justificar llamar a un ingeniero de servicio o encargado para inspeccionar la situación en el inmueble.

En las realizaciones en las que el número de lote del dispositivo de alarma se tiene en cuenta en el análisis del factor

de riesgo, esto permite determinar si se produce o no un número repetido de eventos de falsa alarma en un lote particular de dispositivos de alarma.

5 Esto puede indicar una degradación en el rendimiento de detector. Análogamente, patrones pueden ser indicativos de si se han efectuado o no pruebas planificadas en los intervalos requeridos, o si un nivel de batería está demasiado bajo.

10 De este modo, pueden detectarse condiciones de fallo que no son críticas para la operación normal del dispositivo de alarma. Esto permite que se inicie el servicio o puede fomentarse un mantenimiento dirigido de detectores de acuerdo con su clasificación (por ejemplo, ubicación, número de lote, edad de ocupantes, etc.).

15 La lógica de decisión puede considerar el historial de eventos de alarma de los últimos 3, 4, 5, 6 días o de la última semana. La lógica de decisión puede considerar el historial de eventos de alarma de las últimas dos, tres, cuatro semanas o del último mes. La lógica de decisión puede tener en cuenta diferentes días de la semana o momentos del año. Por ejemplo, un alojamiento para estudiantes puede usarse para estudiantes durante el tiempo de semestre y como alojamiento para invitados durante una temporada vacacional. El perfil de riesgo puede establecerse a un nivel durante el tiempo de semestre, cuando se espera que los estudiantes ocupen el alojamiento, y otro nivel cuando los invitados están presentes durante la temporada vacacional.

20 El experto entenderá que son posibles numerosas modificaciones y variaciones a las realizaciones ilustrativas dentro del alcance de la presente invención. Por ejemplo, dos o más características del sistema de alarma ilustrado en la Figura 1 pueden combinarse en una única unidad. Esto incluye la combinación de una alarma 12 que incluye una interfaz 14 dentro de la carcasa de alarma. En otras palabras, la interfaz 14 puede constituirse mediante el establecimiento de comunicación entre un dispositivo de alarma 12 y el servidor 18, como se ilustra en la Figura 1.
25 La interfaz 14 puede ser integral con un dispositivo de alarma 12, de tal forma que cada dispositivo de alarma 12 tiene, a través de una interfaz integral 14, un canal de comunicación directo a través de la red 16 con el servidor 18. La interfaz 14 de un dispositivo de alarma 12 puede servir como intermediario para retransmitir datos desde uno o más otros dispositivos de alarma 12 de un sistema de alarma. Esto permite que datos de dispositivos de alarma sin conexión directa a un servidor se retransmitan a través de uno o más dispositivos de alarma que están en
30 comunicación directa con el servidor 18.

Como tal, la interfaz 14 puede configurarse para almacenar datos de eventos de alarma de una pluralidad de dispositivos de alarma 12.

35 Adicionalmente, los criterios de riesgo predeterminados pueden reevaluarse de forma continua, o bien automáticamente a través de la aplicación ejecutándose en el servidor o con la adición de entrada manual. Modificaciones y variaciones a los algoritmos que comprende la aplicación son un aspecto integral de la presente invención.

40 Se entenderá que cuando la presente memoria descriptiva se refiere a una lógica de decisión en una realización, la lógica de decisión puede incorporarse en la forma de un algoritmo. Realizaciones de la invención pueden comprender un procesador e instrucciones de software implementadas por el procesador para aplicar la lógica de decisión o algoritmo.

REIVINDICACIONES

1. Un sistema de supervisión de alarma remoto (10) para registrar y procesar datos de eventos de alarma, comprendiendo el sistema de alarma (10):
- 5 una instalación de alarma que comprende uno o más dispositivos de alarma (12) en conexión con una interfaz (14), en donde la interfaz (14) está configurada para recibir datos de eventos de alarma; un servidor (18) en comunicación con la interfaz (14), en donde el servidor (18) está configurado para recibir y procesar datos de eventos de alarma de la interfaz (14); y
- 10 uno o más dispositivos de cliente en red (22) en comunicación con el servidor (18), en donde el servidor (18) está configurado para transmitir un mensaje (20) al dispositivo de cliente en red (22), basándose dicho mensaje (20) en los datos de eventos de alarma procesados;
- 15 **caracterizado por que** el servidor (18) está configurado para provocar una respuesta diferente para el mismo evento de alarma dependiendo de un nivel de riesgo asignado a la instalación de alarma.
2. El sistema de alarma (10) de acuerdo con la reivindicación 1, en el que los datos de eventos de alarma procesados se basan en un análisis del patrón y/o de la frecuencia de eventos de alarma y/o en un análisis del tipo de eventos de alarma, y en donde el sistema de alarma (10) está configurado para ajustar el nivel de riesgo basándose en un patrón de eventos de alarma.
- 20 3. El sistema de alarma (10) de acuerdo con la reivindicación 2, en el que el análisis del patrón y/o de la frecuencia de eventos de alarma tiene en cuenta eventos de alarma no peligrosos.
- 25 4. El sistema de alarma (10) de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que cada uno del uno o más dispositivos de alarma (12) está configurado para almacenar datos de eventos de alarma, incluyendo los datos de eventos de alarma activación de una alarma, procedimientos de prueba en la alarma o un mal funcionamiento de la alarma, para su transmisión al servidor (18).
- 30 5. El sistema de alarma (10) de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que la interfaz (14) es parte integral del dispositivo de alarma (12).
6. Un servidor (18) para procesar datos de eventos de alarma, el servidor (18) configurado para:
- 35 recibir datos de eventos de alarma desde una instalación de alarma a través de una interfaz (14); analizar el patrón, la frecuencia y/o el tipo de eventos de alarma; comparar los datos analizados con criterios predeterminados; y transmitir un mensaje (20) al dispositivo de cliente en red (22) basándose en los resultados de la comparación, en donde el servidor (18) está configurado adicionalmente para provocar una respuesta diferente para el mismo evento de alarma dependiendo de un nivel de riesgo asignado a la instalación de alarma.
- 40 7. El servidor (18) de acuerdo con la reivindicación 6, en el que la etapa de comparación de los datos de eventos de alarma analizados con los criterios predeterminados resulta en un nivel de riesgo específico para la instalación, y en donde, opcionalmente, los criterios predeterminados incluyen datos históricos almacenados específicos para la instalación asociada, y/o en donde los criterios predeterminados incluyen análisis continuo del patrón, de la frecuencia y/o del tipo de los datos de evento de alarma de la instalación asociada.
- 45 8. El servidor (18) de acuerdo con las reivindicaciones 6 o 7, en el que en el análisis del patrón y/o de la frecuencia de eventos de alarma, el servidor (18) tiene en cuenta el número y/o el tipo de eventos de alarma no peligrosos.
- 50 9. Un método para supervisar remotamente alarmas, que comprende las etapas de:
- recepción de datos de eventos de alarma en una interfaz (14) desde uno o más dispositivos de alarma (12) comprendidos en una instalación de alarma;
- 55 transferencia de datos de eventos de alarma de la interfaz (14) a un servidor (18); procesamiento de los datos de eventos de alarma en el servidor (18); y transmisión de un mensaje (20) a al menos un dispositivo de cliente en red (22) basándose en los datos de eventos de alarma procesados, en donde el método comprende adicionalmente que el servidor (18) provoque una respuesta diferente para el mismo evento de alarma dependiendo de un nivel de riesgo asignado a la instalación de alarma (12).
- 60 10. El método de acuerdo con la reivindicación 9, en el que la etapa de procesamiento de los datos de eventos de alarma comprende:
- 65 analizar el patrón, la frecuencia y/o el tipo de eventos de alarma; evaluar el nivel de riesgo basándose en los resultados de análisis y, opcionalmente, comprendiendo adicionalmente la etapa de:

almacenar datos de eventos de alarma localmente en el uno o más dispositivos de alarma (12) para su transmisión al servidor (18).

5 11. El método de acuerdo con la reivindicación 10, que comprende ajustar el nivel de riesgo basándose en un patrón de eventos de alarma.

12. El método de acuerdo con las reivindicaciones 10 u 11, en el que la etapa de análisis del patrón y/o de la frecuencia de eventos de alarma tiene en cuenta el número y/o el tipo de eventos de alarma no peligrosos.

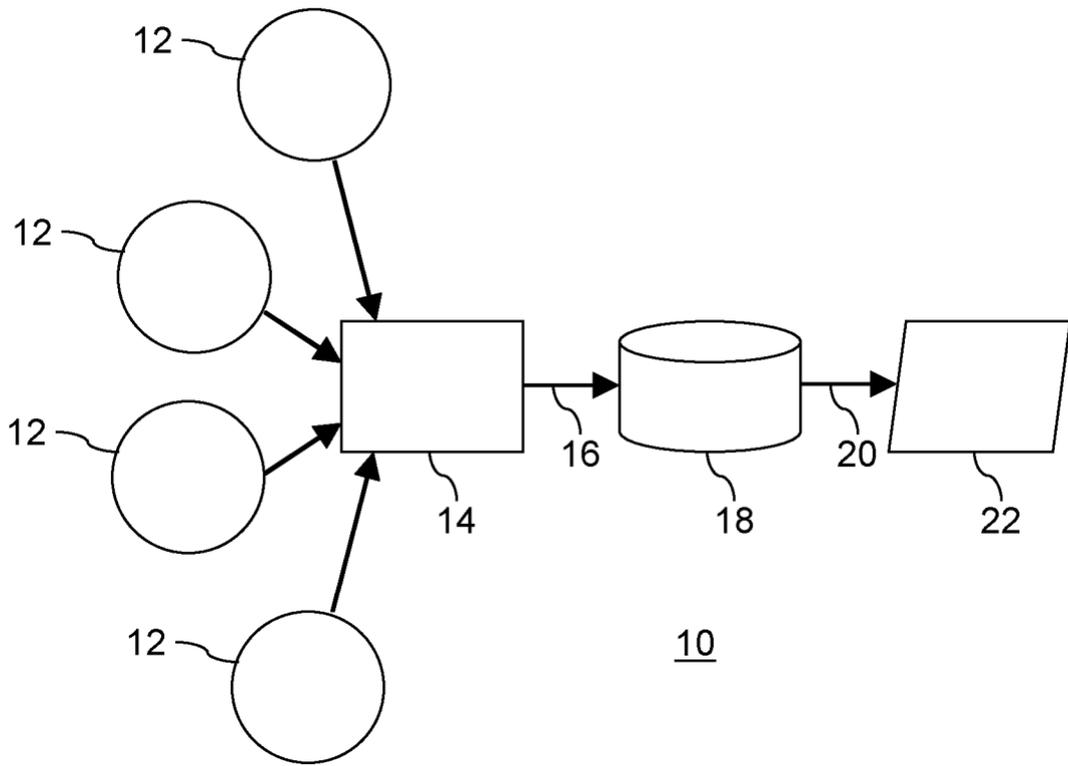


Fig. 1

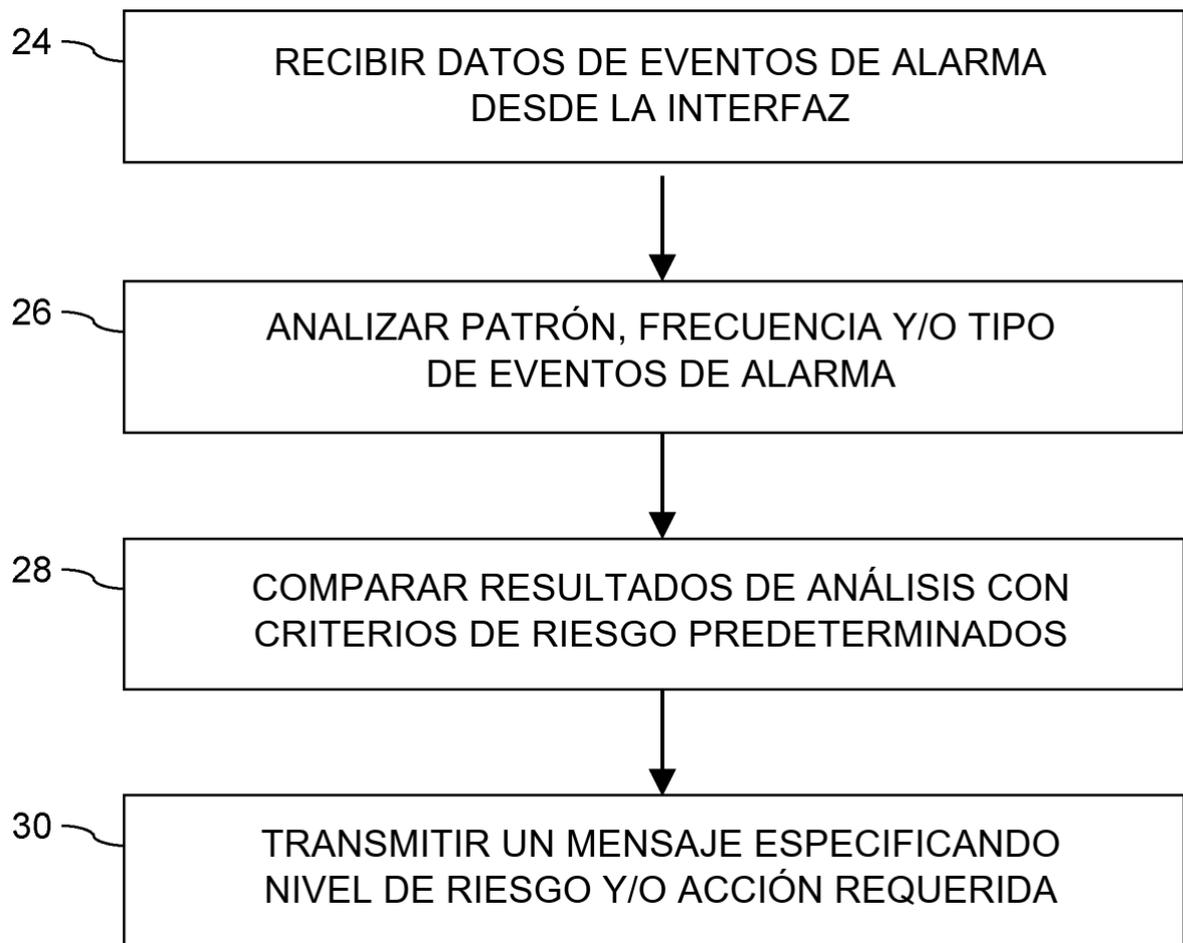


Fig. 2