(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 550 501**

(21) Número de solicitud: 201590028

(51) Int. CI.:

G06F 21/55 (2013.01)
G08B 13/00 (2006.01)
H04L 12/22 (2006.01)
H04L 29/02 (2006.01)

(12) PATENTE DE INVENCIÓN B1

(22) Fecha de presentación:

03.10.2013

(30) Prioridad:

12.10.2012 US 61/713,391
14.03.2013 US 13/829,047

(43) Fecha de publicación de la solicitud:

10.11.2015

(88) Fecha de publicación diferida del informe sobre el estado de la técnica:
24.02.2016

Fecha de la concesión:

22.11.2016

(45) Fecha de publicación de la concesión:

29.11.2016

(73) Titular/es:

SCHWEITZER ENGINEERING LABORATORIES, INC. (100.0%)
2350 NE Hopkins Court
99163 Pullmann WA Washington US

(72) Inventor/es:

SMITH, Rhett y
GORDON, Colin

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

(54) Título: **Detección y respuesta a acceso no autorizado a un dispositivo de comunicación**

ES 2 550 501 B1

(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 550 501**

(21) Número de solicitud: 201590028

(57) Resumen:

Detección y respuesta a acceso no autorizado a un dispositivo de comunicación.

Una pasarela de comunicación congruente con la presente revelación puede detectar un acceso físico o electrónico no autorizado e implementar acciones de seguridad en respuesta al mismo. Una pasarela de comunicación puede proporcionar un trayecto de comunicación a un dispositivo electrónico inteligente (IED), usando un puerto de comunicaciones del IED configurado para comunicarse con el IED. La pasarela de comunicación puede incluir un puerto de detección de intrusión física y un puerto de red. La pasarela de comunicación puede además incluir lógica de control configurada para evaluar una señal de detección de intrusión física. La lógica de control puede ser configurada para determinar que la señal de detección de intrusión física es indicativa de un intento de obtener acceso no autorizado a uno entre la pasarela de comunicación, el IED y un dispositivo en comunicación con la pasarela; y emprender una acción de seguridad en base a la determinación de que la indicación es indicativa del intento de obtener acceso no autorizado.

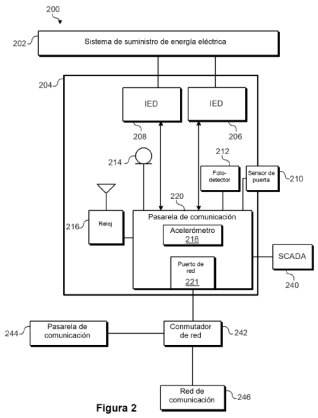

Figura 2

ES 2 550 501 B1

DESCRIPCIÓN

Detección y respuesta a acceso no autorizado a un dispositivo de comunicación

CAMPO TÉCNICO

La presente divulgación se refiere, en general, a sistemas y procedimientos para detectar y responder a un acceso no autorizado a un dispositivo de comunicación. Más específicamente, los sistemas y procedimientos revelados en la presente memoria pueden ser implementados con relación a dispositivos de red y dispositivos electrónicos inteligentes en un sistema de suministro de energía eléctrica, para detectar y responder a un acceso físico no autorizado.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Se describen realizaciones no limitantes y no exhaustivas de la revelación, incluyendo diversas realizaciones de la revelación con referencia a las figuras, en las cuales:

la **Figura 1** ilustra un diagrama unifilar simplificado de un sistema de suministro de energía eléctrica y dispositivos electrónicos inteligentes (IED) asociados, congruente con diversas realizaciones de la presente revelación.

La **Figura 2** ilustra un diagrama de bloques simplificado de un sistema para detectar y responder a un acceso no autorizado a un dispositivo de comunicación, congruente con diversas realizaciones de la presente revelación.

La **Figura 3A** ilustra una representación conceptual de un sistema que implementa una acción de seguridad como resultado de una detección de un dispositivo no autorizado, congruente con diversas realizaciones de la presente revelación.

La **Figura 3B** ilustra una representación conceptual del sistema de la **Figura 3A**, que implementa otra acción de seguridad como resultado de una detección de un dispositivo no autorizado, congruente con diversas realizaciones de la presente revelación.

La **Figura 4** ilustra un gráfico de flujo de un procedimiento para detectar acceso físico no autorizado a un recinto que contiene equipo asociado a un sistema de suministro de energía eléctrica, congruente con diversas realizaciones de la presente revelación.

En la siguiente descripción, se proporcionan numerosos detalles específicos para una comprensión exhaustiva de las diversas realizaciones reveladas en la presente memoria. Los sistemas y procedimientos revelados en la presente memoria pueden ser puestos en práctica sin uno o más de los detalles específicos, o con otros procedimientos,

componentes, materiales, etc. Además, en algunos casos, estructuras, materiales u operaciones bien conocidos pueden no ser mostrados o descritos en detalle, a fin de evitar oscurecer aspectos de la revelación. Además, las características, estructuras o características descritas pueden ser combinadas de cualquier forma adecuada en una o más realizaciones alternativas.

DESCRIPCIÓN DETALLADA

La presente revelación proporciona sistemas y procedimientos para detectar y responder al acceso no autorizado a un dispositivo de comunicación. De acuerdo a diversas realizaciones, el dispositivo de comunicación puede estar configurado para la comunicación segura con uno o más dispositivos electrónicos inteligentes (IED), un sistema de control supervisor y adquisición de datos (SCADA) y / o una red de comunicación. Los IED pueden estar configurados para monitorizar una parte de un sistema de suministro de energía eléctrica, y proporcionar control al sistema de suministro de energía eléctrica. De acuerdo a diversos algoritmos de protección y control, los IED pueden estar configurados para comunicarse con otros IED, controladores, sistemas de adquisición de datos y / o similares.

Los IED pueden estar situados cerca de centros de control, en subestaciones, o pueden estar distribuidos en el sistema de suministro de energía eléctrica. Por ejemplo, los IED pueden estar situados cerca de equipos primarios en líneas de transmisión o distribución, alejadas de la subestación. En una realización, el IED puede ser un control restablecedor en comunicación con, y proporcionando protección y control a, un restablecedor. El restablecedor puede estar situado en sitio remoto de la subestación. El IED puede estar dispuesto, por ejemplo, en un armario u otra carcasa montada sobre un poste de energía.

Los equipos situados remotamente, asociados a un sistema de suministro de energía eléctrica, plantean un riesgo de seguridad en cuanto a que usuarios no autorizados pueden ser capaces de obtener acceso físico a un recinto que contiene tales equipos. Si bien los recintos están habitualmente asegurados de forma física, usando cerrojos, cercos u otras barreras, tales barreras pueden ser superadas por un usuario no autorizado con suficiente motivación. Los equipos almacenados dentro de un recinto pueden incluir botones, interfaces hombre–máquina y otros mecanismos para cambiar configuraciones asociadas al equipo. Además, las comunicaciones pueden ser descifradas dentro de un armario, edificio u otro recinto que contenga equipos asociados a un sistema de suministro de energía eléctrica. Esto puede ser verdad, en particular, allí donde se usan sistemas heredados que

no prestan soporte en forma nativa a la comunicación cifrada. En consecuencia, un usuario no autorizado con acceso físico a un canal de comunicación no cifrado puede presentar significativas preocupaciones de seguridad.

Un posible remedio es colocar una pasarela de comunicación en el armario con el IED. El IED puede ser configurado para comunicarse solamente con la pasarela de comunicación, la cual, a su vez, puede comunicarse con el controlador, el sistema de adquisición de datos o similares. La pasarela de comunicación puede ser configurada para cifrar las comunicaciones con el controlador, el sistema de adquisición de datos y similares; sin embargo, si el armario está afectado, la pasarela de comunicaciones y / o los IED pueden quedar vulnerables al ataque.

Las comunicaciones entre los IED en un sistema de suministro de energía eléctrica pueden ser habitualmente comunicaciones fiables. Según se usa el término en la presente memoria, una comunicación fiable se refiere a un mensaje que incluye indicios de confianza. Los indicios de confianza pueden incluir, pero no se limitan a, un identificador reconocido en el mensaje que está asociado a un origen fiable, un trayecto o puerto de comunicación fiable desde el cual se recibe el mensaje, un nodo autenticado que despachó el mensaje, un mensaje cifrado capaz de ser descifrado usando una técnica (p. ej., criptografía de clave pública / privada) o un mensaje que incluye criterios de autenticación. Por supuesto, también pueden ser utilizados otros indicios de confianza con relación a diversas realizaciones, congruentes con la presente revelación.

De acuerdo a diversas realizaciones reveladas en la presente memoria, una pasarela de comunicaciones incluye la detección del acceso físico, para detectar cuándo es abierto un recinto y / o es objeto de acceso físico de otro modo. La pasarela de comunicaciones puede además ser configurada para emprender ciertas etapas cuando se detecta un acceso no autorizado a un recinto. Por ejemplo, de acuerdo a algunas realizaciones, las comunicaciones recibidas desde la pasarela después de una detección de acceso físico no autorizado pueden no ser fiables ya. En consecuencia, ciertas acciones o comandos pueden ser selectivamente descartados como resultado de la naturaleza no fiable de las comunicaciones. De acuerdo a algunas realizaciones, las comunicaciones desde una pasarela de comunicaciones que ha sido objeto de acceso sin autorización pueden ser bloqueadas enteramente. La pasarela de comunicación puede además ser configurada para registrar todas las comunicaciones después de que haya sido detectado un acceso físico no autorizado.

La referencia en toda la extensión de esta memoria descriptiva a “una realización” significa que un rasgo, estructura o característica específicos, descritos con relación a la realización, está incluido en al menos una realización. De tal modo, las apariciones de la frases “en una realización” en diversos lugares en toda la extensión de esta memoria descriptiva no necesariamente están todas refiriéndose a la misma realización. En particular “una realización” puede ser un sistema, un artículo de fabricación (tal como un medio de almacenamiento legible por ordenador), un procedimiento y / o un producto de un proceso.

Las frases “conectado con” y “en comunicación con” se refieren a cualquier forma de interacción entre dos o más componentes, incluyendo la interacción mecánica, eléctrica, magnética y electromagnética. Dos componentes pueden estar conectados entre sí, incluso aunque no estén en contacto directo entre sí, e incluso aunque pueda haber dispositivos intermedios entre los dos componentes. Por ejemplo, un IED puede estar conectado con un administrador de sesiones de pasarela a través de uno o más IED intermedios o dispositivos de red. Tales redes pueden ser modeladas como estructuras arboladas, como es común en la técnica.

Según se usa en la presente memoria, el término IED puede referirse a cualquier dispositivo basado en microprocesadores que monitoriza, controla, automatiza y / o protege equipos monitorizados dentro de un sistema. Tales dispositivos pueden incluir, por ejemplo, unidades terminales remotas, relés diferenciales, relés a distancia, relés direccionales, relés alimentadores, relés de exceso de corriente, controles reguladores de voltaje, relés de voltaje, relés de fallo de interruptor, relés generadores, relés de motor, controladores de automatización, controladores de compartimiento, contadores, controles restablecedores, procesadores de comunicaciones, plataformas de cálculo, controladores lógicos programables (PLC), controladores de automatización programables, módulos de entrada y salida, controladores de motores y similares. Los IED pueden estar conectados con una red, y la comunicación en la red puede ser facilitada por dispositivos de formación de redes, que incluyen, pero no se limitan a, multiplexadores, encaminadores, concentradores, pasarelas, cortafuegos y conmutadores. Además, los dispositivos de formación de redes y de comunicación pueden estar incorporados en un IED o pueden estar en comunicación con un IED. El término IED puede ser usado de manera intercambiable para describir un IED individual o un sistema que comprende múltiples IED.

Según se usa en la presente memoria, el término “credenciales de inicio de sesión” puede referirse a cualquier tipo de procedimiento de autenticación conocido como útil en la técnica.

Por ejemplo, las credenciales de inicio de sesión se refieren normalmente a una combinación de nombre de usuario y contraseña, codificados en ASCII; en consecuencia, los términos “credenciales de inicio de sesión” y “nombre de usuario y contraseña(s)” pueden ser usados de manera intercambiable en la presente memoria. Sin embargo, el nombre de usuario y la(s) contraseña(s) pueden ser reemplazados por cualquiera entre una amplia variedad de protocolos de autenticación y / o técnicas que incluyen protocolos criptográficos para máquinas de autenticación, procedimientos de reto–respuesta, pruebas de conocimiento nulo, contraseñas de uso único sincronizadas en el tiempo, testigos de seguridad, autenticación biométrica, contraseñas gráficas u otras, no basadas en texto, autenticación vocal y similares.

Algo de la infraestructura que puede ser usada con las realizaciones reveladas en la presente memoria ya está disponible, tal como: ordenadores de propósito general, herramientas y técnicas de programación de ordenadores, medios de almacenamiento digital y redes de comunicaciones. Un ordenador puede incluir un procesador, tal como un microprocesador, un micro–controlador, circuitos lógicos o similares. El procesador puede incluir un dispositivo de procesamiento de propósito especial, tal como un ASIC, PAL, PLA, PLD, Formación de Compuertas Programables en el Terreno u otro dispositivo personalizado o programable. El ordenador también puede incluir un dispositivo de almacenamiento legible por ordenador, tal como memoria no volátil, memoria RAM estática, memoria RAM dinámica, ROM, CD–ROM; disco, cinta, memoria magnética, óptica o flash, u otro medio de almacenamiento legible por ordenador.

Las redes adecuadas para la configuración y / o el uso, según lo descrito en la presente memoria, incluyen una o más redes de área local, redes de área amplia, redes de área metropolitana y / o redes de “Internet” o del protocolo de Internet (IP), tales como la Máxima Malla Mundial, una Internet privada, una Internet segura, una red de valor añadido, una red privada virtual, una extranet, una intranet, o incluso máquinas autónomas que se comunican con otras máquinas por el transporte físico de medios. En particular, una red adecuada puede ser formada a partir de partes o totalidades de otras dos o más redes, incluyendo redes que usan tecnologías disímiles de hardware y de comunicación de redes. Una red puede incorporar líneas terrestres, comunicación inalámbrica y combinaciones de las mismas.

La red puede incluir software de comunicaciones o de formación de redes, tal como software disponible a partir de Novell, Microsoft, Artisoft y otros proveedores, y puede funcionar

usando TCP/IP, SPX, IPX, RS–232 y otros protocolos, sobre pares cruzados, cables coaxiales o de fibra óptica, líneas telefónicas, satélites, relés de microondas, líneas de energía de Corriente Alterna modulada, transferencia de medios físicos y / u otros medios de transmisión de datos. La red puede abarcar redes más pequeñas y / o puede ser conectable con otras redes mediante una pasarela o mecanismo similar.

Aspectos de ciertas realizaciones descritas en la presente memoria pueden ser implementadas como módulos o componentes de software. Según se usa en la presente memoria, un módulo o componente de software puede incluir cualquier tipo de instrucción de ordenador o código ejecutable por ordenador, situado dentro, o en, un medio de almacenamiento legible por ordenador. Un módulo de software, por ejemplo, puede comprender uno o más bloques físicos o lógicos de instrucciones de ordenador, que pueden estar organizadas como una rutina, un programa, un objeto, un componente, una estructura de datos, etc., que realiza una o más tareas o implementa tipos específicos de datos abstractos.

En ciertas realizaciones, un módulo de software específico puede comprender instrucciones disímiles almacenadas en distintas ubicaciones de un medio de almacenamiento legible por ordenador, que implementan conjuntamente la funcionalidad descrita del módulo. En efecto, un módulo puede comprender una única instrucción o muchas instrucciones, y puede estar distribuido sobre varios segmentos distintos de código, entre distintos programas y entre varios medios de almacenamiento legibles por ordenador. Algunas realizaciones pueden ser puestas en práctica en un entorno informático distribuido donde las tareas son realizadas por un dispositivo de procesamiento remoto enlazado a través de una red de comunicaciones. En un entorno informático distribuido, los módulos de software pueden estar situados en medios de almacenamiento legibles por ordenador, locales y / o remotos. Además, los datos ligados o representados conjuntamente en un registro de base de datos pueden ser residentes en el mismo medio de almacenamiento legible por ordenador, o entre varios medios de almacenamiento legibles por ordenador, y pueden estar enlazados entre sí en campos de un registro en una base de datos sobre una red.

Los módulos de software descritos en la presente memoria realizan tangiblemente programas, funciones y / o instrucciones que son ejecutables por uno o más ordenadores para realizar tareas según lo descrito en la presente memoria. El software adecuado, según sea aplicable, puede ser proporcionado usando las divulgaciones presentadas en la presente memoria y lenguajes y herramientas de programación, tales como XML, Java,

Pascal, C++, C, lenguajes de base de datos, API, SDK, ensambladores, firmware, micro–código y / u otros lenguajes y herramientas. Adicionalmente, el software, el firmware y el hardware pueden ser usados de forma intercambiable para implementar una función dada.

En algunos casos, características, estructuras u operaciones bien conocidas no se muestran o describen en detalle. Además, las características, estructuras u operaciones descritas pueden ser combinadas de cualquier manera adecuada en una o más realizaciones. También se entenderá inmediatamente que los componentes de las realizaciones, según lo generalmente descrito e ilustrado en las figuras en la presente memoria, podrían ser dispuestos y diseñados en una amplia variedad de configuraciones distintas. Todas las configuraciones de ese tipo están incluidas dentro del ámbito de la presente revelación.

Las realizaciones de la revelación serán óptimamente entendidas por referencia a los dibujos, en los que las partes iguales están indicadas por números iguales en toda su extensión. Los componentes de las realizaciones reveladas, según lo generalmente descrito e ilustrado en las figuras en la presente memoria, podrían ser dispuestos y diseñados en una amplia variedad de configuraciones distintas. De tal modo, la siguiente descripción detallada de las realizaciones de los sistemas y procedimiento de la revelación no está concebida para limitar el ámbito de la revelación, según lo reivindicado, sino que es meramente representativa de posibles realizaciones. En otros casos, estructuras, materiales u operaciones bien conocidos no se muestran o describen en detalle para evitar oscurecer aspectos de esta revelación. Además, las etapas de un procedimiento no necesariamente deben ser ejecutados en algún orden específico, o incluso secuencialmente, ni las etapas deben ser ejecutadas solamente una vez, a menos que se especifique lo contrario.

La **Figura 1** ilustra un diagrama unifilar simplificado de un sistema de suministro de energía eléctrica 100 y los IED asociados 104, 106, 115 y 170, congruente con ciertas realizaciones reveladas en la presente memoria. El sistema 100 incluye diversas subestaciones y los IED 104, 106, 108, 115 y 170, configurados para realizar diversas funciones. El sistema 100 está proporcionado con fines ilustrativos y no implica ninguna disposición o función específica, requerida a cualquier IED específico. En algunas realizaciones, los IED 104, 106, 108, 115 y 170 pueden ser configurados para monitorizar y comunicar información, tal como voltajes, corrientes, estado de equipos, temperatura, frecuencia, presión, densidad, absorción infrarroja, información de frecuencia de radio, presiones parciales, viscosidad, velocidad, velocidad de rotación, masa, estado de conmutación, estado de válvulas, estado de interruptores de circuitos, estado de tomas, lecturas de contadores y similares. Además, los IED 104, 106, 108, 115 y 170 pueden ser configurados para comunicar cálculos, tales como

fasores (que pueden o no estar sincronizados como sincro–fasores), sucesos, distancias de fallos, diferenciales, impedancias, reactancias, frecuencias y similares.

El sistema de suministro de energía eléctrica 100 ilustrado en la **Figura 1** puede incluir una subestación de generación 111. La subestación 111 puede incluir los generadores 110 y 112, que están conectados con un bus 118 mediante los transformadores incrementales 120 y 122. El bus 118 puede estar conectado con el bus 126 en la subestación 119, mediante la línea de transmisión 124. Aunque los equipos en la subestación 111 pueden estar monitorizados y / o controlados por diversos IED, solamente se muestra un único IED 104. El IED 104 puede ser un IED de protección de transformador para el transformador 120. El IED 104 puede estar en comunicación con un origen horario común 188 que, según se indica más adelante, puede estar distribuido en el sistema 100 usando una red de comunicaciones, o usando un origen horario universal, tal como un sistema de localización global (GPS) o similares. La utilización de un origen horario común o universal puede asegurar que los IED tengan una señal horaria sincronizada que puede ser usada para generar datos sincronizados en el tiempo, tales como los sincro–fasores.

La subestación 119 puede incluir un generador 114, que puede ser un generador distribuido, y que puede estar conectado con el bus 126 mediante el transformador incremental 118. El bus 128 puede estar conectado con un bus de distribución 132 mediante un transformador decremental 130. Diversas líneas de distribución 136 y 134 pueden estar conectadas con el bus de distribución 132. La línea de distribución 136 puede llevar a la subestación 141, donde la línea es monitorizada y / o controlada usando el IED 106, que puede abrir y cerrar selectivamente el interruptor 152. La carga 140 puede ser alimentada desde la línea de distribución 136. Además, el transformador decremental 144 puede ser usado para decrementar un voltaje para su consumo por la carga 140.

La línea de distribución 134 puede llevar a la subestación 151, y suministrar energía eléctrica al bus 148. El bus 148 también puede recibir energía eléctrica desde el generador distribuido 116 mediante el transformador 150. La línea de distribución 158 puede suministrar energía eléctrica desde el bus 148 a la carga 138, y puede incluir además el transformador decremental 142. El interruptor de circuitos 160 puede ser usado para conectar selectivamente el bus 148 con la línea de distribución 134. El IED 108 puede ser usado para monitorizar y / o controlar el interruptor de circuitos 160, así como la línea de distribución 158.

Un IED central 170 puede estar en comunicación con diversos IED 104, 106, 108 y 115, usando una red de comunicaciones de datos. Los IED 104, 106, 108 y 115 pueden ser remotos con respecto al IED central 170. Los IED remotos 104, 106, 108 y 115 pueden comunicarse por diversos medios, tales como una comunicación directa desde el IED 170 o sobre una red de comunicaciones de área amplia 162. Los IED 104, 106, 108, 115 y 170 pueden estar comunicativamente enlazados entre sí usando una red de comunicaciones de datos, y pueden además estar comunicativamente enlazados con un sistema de monitorización central, tal como un sistema de control supervisor y de adquisición de datos (SCADA) 182, un sistema de información (IS) 190 y / o un sistema de control de área amplia y de percepción de situaciones (WCSA) 180. La red de comunicaciones de datos entre los IED 104, 106, 108, 115 y 170 puede utilizar una amplia variedad de tecnologías de red, y puede comprender dispositivos de red tales como módems, encaminadores, cortafuegos, servidores de redes privadas virtuales y similares, que no se muestran en la Figura 1.

Los diversos IED en el sistema 100 pueden obtener información de energía eléctrica desde equipos monitorizados, usando transformadores potenciales (PT) para mediciones de voltaje (p. ej., el transformador potencial 156), transformadores de corriente (CT) para mediciones de corriente (p. ej., el transformador de corriente 154) y similares. Los PT y CT pueden incluir a cualquier dispositivo capaz de proporcionar salidas que puedan ser usadas por los IED para hacer mediciones potenciales y de corriente, y pueden incluir los PT y CT tradicionales, los PT y CT ópticos, bobinas de Rogowsky, sensores de efecto de sala y similares.

Cada IED puede ser configurado para acceder a un origen horario común 188. El origen horario común 188 puede ser distribuido mediante una red de comunicaciones (usando, por ejemplo, el protocolo IEEE–1588, el protocolo NTP o similares), u obtenido localmente en cada IED. El origen horario común 188 puede ser una hora universal, tal como la suministrada usando satélites del GPW, WWVB, WWV o similares. Un origen horario común puede ser usado para sincronizar en el tiempo las mediciones del sistema de energía eléctrica y / o en el cálculo de sincro–fasores. Los fasores calculados por los IED pueden incluir un sello horario que indica una hora a la cual fue hecha la medición.

El IED central 170 también puede estar en comunicación con un cierto número de otros dispositivos o sistemas. Tales dispositivos o sistemas pueden incluir, por ejemplo, un sistema WCSA 180, un sistema SCADA 182 o una Interfaz Hombre–Máquina (HMI) 187 local. La HMI local 187 puede ser usada para cambiar configuraciones, emitir instrucciones

de control, recuperar un informe de suceso, recuperar datos y similares. En algunas realizaciones, el sistema WCSA 180 puede recibir y procesar los datos alineados en el tiempo, y puede coordinar acciones de control sincronizadas en el tiempo al más alto nivel del sistema de suministro de energía eléctrica 100. El dispositivo de almacenamiento masivo 184 puede almacenar datos referidos al sistema 100 desde los IED 104, 106, 108, 115 y 170.

El IED central 170 puede además incluir una entrada horaria, que puede recibir una señal horaria desde un origen horario central de IED 186. El origen horario central de IED 186 también puede ser usado por el IED central 170 para información y datos de sellos horarios. La sincronización en el tiempo puede ser útil para la organización de los datos y la toma de decisiones en tiempo real, así como el análisis posterior a sucesos. La sincronización en el tiempo puede además ser aplicada a las comunicaciones de red. En ciertas realizaciones, el origen horario central de IED 186 y el origen horario común 177 pueden ser el mismo origen horario. El origen horario común 188 puede ser cualquier origen horario que sea una forma aceptable de sincronización en el tiempo, incluyendo, pero sin limitarse a, un oscilador de cristal compensado en temperatura y controlado por voltaje, osciladores de Rubidio y Cesio, con o sin bucles bloqueados en fase digital, tecnología de sistemas micro–electromecánicos (MEMS), que transfiere los circuitos resonantes desde los dominios electrónicos a los mecánicos, o un receptor del GPS con descodificación horaria. A falta de un origen horario común disponible para todos los IED, el IED central 170 puede servir como un origen horario común distribuyendo una señal de sincronización en el tiempo.

El sistema de información 190 incluye generalmente hardware y software para permitir la comunicación de redes, la seguridad de redes, la administración de usuarios, la administración de Internet e intranet, el acceso de redes remotas y similares. El sistema de información 190 puede generar información acerca de la red para mantener y sostener una red de comunicaciones fiable, de calidad y segura, ejecutando lógica comercial en tiempo real sobre sucesos de seguridad de redes, realizar diagnósticos de red, optimizar prestaciones de red y similares.

Las comunicaciones de datos entre los IED 104, 106, 108, 115 y 170 pueden ocurrir usando una amplia variedad de protocolos de comunicación y formatos de datos. De acuerdo a algunas realizaciones, los protocolos de comunicación y los formatos de datos pueden ser de propiedad industrial en algunos casos, y estandarizados en algunos casos. Los IED 104, 106, 108, 115 y 170 también pueden comunicar información de configuración, información

de identificación de IED, información de comunicaciones, información de estado, información de alarma y similares.

Los IED 104, 106, 108 y 115 pueden ser desplegados en áreas pobladas y, en consecuencia, pueden ser colocados en proximidad física con el público general. Por ejemplo, el sistema 100 puede ser situado en un entorno urbano con una pluralidad de subestaciones 111, 119, 141 y 151 ubicadas por toda una ciudad. En consecuencia, el control del acceso físico a las subestaciones y a los IED plantea dificultades. Un actor no autorizado puede intentar obtener acceso físico a las subestaciones 111, 119, 141 y 151 y / o a su equipo constituyente. Tras obtener acceso físico a una de las subestaciones 111, 119, 141 y 151, los IED en las subestaciones pueden estar expuestos a amenazas tales como pulsación de botones, conexión con puertos de comunicación o similares.

La obtención de acceso físico a los enlaces de comunicación en las subestaciones 111, 119, 141 y 151 puede permitir a un usuario no autorizado evitar ciertas medidas de seguridad concebidas para impedir el acceso no autorizado a las comunicaciones entre los IED 104, 106, 108, 115 y 170. Las comunicaciones entre los IED 104, 106, 108, 115 y 170 pueden ser habitualmente comunicaciones fiables. En consecuencia, las comunicaciones pretendidamente originadas desde una ubicación fiable, una red fiable o un origen fiable pueden ser más fácilmente explotadas por un usuario no autorizado para implementar cambios en configuraciones de IED, disparar alarmas o perturbar de otro modo el funcionamiento del sistema 100.

La **Figura 2** ilustra un diagrama de bloques simplificado de un sistema 200 para la detección y respuesta a un acceso no autorizado a un IED u otro dispositivo de comunicaciones. Un recinto 204 puede ser usado para confinar diversos dispositivos tales como los IED 206 y 208, el reloj 216 y la pasarela de comunicaciones 220. De acuerdo a algunas realizaciones, el recinto 204 puede comprender un armario montado sobre postes, una estructura autónoma u otro recinto configurado para alojar infraestructura asociada a un sistema de suministro de energía eléctrica 202.

Los IED 206 y 208 pueden estar en comunicación eléctrica con el sistema de suministro de energía eléctrica 202 para proporcionar protección, control, lecturas y / o automatización al mismo. Los IED 206 y 208 pueden estar en comunicación con la pasarela de comunicaciones 220, que puede estar en comunicación segura con el sistema SCADA 240 y / o una red de comunicaciones 246. La pasarela de comunicación 220 puede incluir un puerto de red 221, que puede estar en comunicación con el conmutador de red 242. La red

de comunicaciones 246 puede facilitar las comunicaciones con otros IED mediante otras pasarelas de comunicaciones. Un conmutador de red puede existir entre la pasarela de comunicación 220 y la red de comunicación 246. Otras pasarelas de comunicaciones 244 también pueden estar en comunicación con el conmutador de red 242.

El reloj 216 puede estar en comunicación con un origen horario común tal como un sistema global de satélites de navegación (GNSS), un origen horario (p. ej., un origen horario proporcionado por un GPS), una emisión de WWVB o WWV, u otro origen horario común. El reloj 216 puede proporcionar una señal horaria a la pasarela de comunicación 220, la cual puede, a su vez, proporcionar una señal horaria a los IED 206 y 208.

Para detectar un acceso no autorizado al recinto 204, la pasarela de comunicación 220 puede además estar en comunicación con un sensor de puerta 210, configurado para detectar una apertura de una puerta del recinto 204, usando cualquier mecanismo adecuado de detección. En algunas realizaciones, el sensor de puerta 210 puede ser un perno de puerta de armario cableado con una entrada de contacto de la pasarela de comunicación 220. En realizaciones adicionales, el sensor de puerta 210 puede ser un sensor magnético o un conmutador de perno a presión, cableado con una entrada de contacto de la pasarela de comunicación 220. El sensor de puerta 210 puede ser configurado para señalizar a la pasarela de comunicación 220 si detecta la apertura de una puerta del recinto 204.

Además, para detectar el acceso no autorizado al recinto 204, la pasarela de comunicación 220 puede estar en comunicación con un foto–detector 212. El foto–detector 212 puede detectar cuando el recinto 204 está abierto por un cambio en la iluminación dentro del recinto 204. En ciertas realizaciones, el foto–detector 212 puede ser capaz de detectar cambios en la densidad lumínica. El foto–detector 212 puede ser configurado para señalizar a la pasarela de comunicación 220 cuando se detecta luz.

La pasarela de comunicación 220 puede estar en comunicación con un micrófono 214. El micrófono 214 puede detectar atributos de frecuencia y amplitud, para detectar una alteración física, así como sucesos que ocurren en el sistema de energía. Es decir, el micrófono 214 puede detectar sonidos y comunicar señales eléctricas que representan tales sonidos a la pasarela de comunicación 220. La pasarela de comunicación 220 puede incluir atributos sonoros predeterminados tales que puedan permitir a la pasarela de comunicación 220 diferenciar entre sonidos que significan un acceso físico no autorizado (tales como cortes de metal o rotura de cerraduras), sonidos que significan sucesos en el sistema de

energía eléctrica (tales como apertura de interruptores, cambio de posición de tomas y similares), sonidos asociados a un fenómeno natural (tal como la lluvia, el granizo, el trueno, etc.) y sonidos asociados a condiciones ambientales (tales como tráfico, bocinas, etc.). En otra realización, el micrófono 214 puede ser capaz de diferenciar sucesos distintos, y de señalizar a la pasarela de comunicación 220 cuando es detectado un sonido correspondiente a un acceso no autorizado. De acuerdo a algunas realizaciones, el sonido detectado por el micrófono 214 puede ser transmitido a una estación monitora central a fin de que un operador pueda escuchar los sonidos y tomar una determinación en cuanto a si tales sonidos son o no indicativos de un intento de obtener acceso no autorizado.

La pasarela de comunicación 220 incluye un acelerómetro 218 para detectar el movimiento. El acelerómetro 218 puede ser capaz de proporcionar una señal a la pasarela de comunicación 220, correspondiente al movimiento. De acuerdo a algunas realizaciones, el acelerómetro 218 puede comprender un dispositivo externo a la pasarela de comunicación 220. La pasarela de comunicación 220 puede usar la señal para detectar cuándo está presente un movimiento correspondiente a un acceso no autorizado. Por ejemplo, impactos físicos repetidos pueden corresponder a golpear el recinto 204 en un intento de romper una cerradura y obtener acceso. En otra realización, el acelerómetro 218 detecta fenómenos naturales y / o condiciones ambientales, tales como terremotos o grandes tormentas, que pueden ser retro–alimentados al sistema de control de modo que las operaciones puedan hacer los ajustes adecuados a las configuraciones del sistema de energía. Además, algunas realizaciones congruentes con la presente revelación pueden ser montadas en un poste utilitario. Los accidentes automovilísticos pueden dar ocasionalmente como resultado colisiones con postes utilitarios y, en consecuencia, un acelerómetro puede ser activado en el caso de que el poste en el cual está montado el dispositivo sea golpeado por un automóvil.

Dado que fenómenos naturales o condiciones ambientales (p. ej., un terremoto o colisión de vehículos puede activar un acelerómetro, el trueno puede activar un micrófono, etc.) pueden activar uno o más detectores de intrusiones físicas, ciertas realizaciones congruentes con la presente revelación pueden identificar indicaciones alternativas de acceso no autorizado antes de implementar una acción de seguridad. De acuerdo a una realización, las señales de detección pueden ser comparadas en base a la proximidad física de los dispositivos. Por ejemplo, en la medida en que un terremoto activa un acelerómetro en una ubicación, los dispositivos cercanos pueden ser similarmente activados. De manera similar, el clima extremo puede también afectar a múltiples dispositivos en la misma vecindad geográfica, y

por tanto una comparación de información entre tales dispositivos puede proporcionar una indicación alternativa de si una señal de detección recibida desde un sistema de detección de intrusiones corresponde a un intento de obtener acceso no autorizado o a fenómenos naturales.

Además de monitorizar condiciones físicas (p. ej., luz, sonido, movimiento, etc.), los patrones en los datos transmitidos a o desde la pasarela de comunicación 220 también pueden ser analizados a fin de determinar intentos de obtener acceso físico no autorizado. Cuando la pasarela de comunicación 220 detecta un cambio en la comunicación en uno de los puertos, puede ser debido a un intento de acceso no autorizado. Por ejemplo, si un medio de comunicación de un IED es quitado de su puerto, la comunicación por ese puerto cambiará con respecto a su línea de referencia. La pasarela de comunicación 220 puede luego detectar un intento de acceso no autorizado. En consecuencia, la pasarela de comunicación 220 puede ser configurada para detectar cuando un actor no autorizado desenchufa un cable activo, enchufa otro cable y / o comienza a usar el canal de comunicación.

La pasarela de comunicación 220 puede incluir una pluralidad de puertos de comunicación (p. ej., el puerto de red 221, un puerto para la comunicación con un sistema SCADA 240, puertos para recibir entrada desde el foto–detector 212, el sensor de puerta 210 y el micrófono 214, etc.). Los puertos de comunicación pueden ser realizados en una amplia variedad de formas, incluyendo puertos en serie, puertos USB, puertos Ethernet, puertos IEEE 1394, etc. De acuerdo a algunas realizaciones, cada uno entre el foto–detector 212, el sensor de puerta 210 y el micrófono 214 puede estar en comunicación con un puerto de comunicación asociado a la pasarela de comunicación 220. De acuerdo a otras realizaciones, la pasarela de comunicación 220 puede incluir diversos sensores (p. ej., micrófono, foto–detector, etc.) como componentes integrados. De acuerdo a diversas realizaciones, los elementos configurados para detectar acceso no autorizado pueden ser mencionados como detectores de intrusiones físicas.

La pasarela de comunicación 220 puede monitorizar cada uno de sus puertos de comunicaciones, y establecer una línea de referencia para la comunicación por cada puerto. Por ejemplo, un puerto en comunicación con el reloj 216 establecerá una línea de referencia de comunicación, correspondiente a una señal desde el reloj 216. Los puertos en comunicación con los IED 206 y 208 pueden establecer una línea de referencia distinta. Además, los puertos que no son usados establecerán otra línea de referencia más. Una

línea de referencia puede comprender un cierto número de factores, tales como el tipo de datos, el volumen de datos, etc. Por ejemplo, una línea de referencia puede mostrar que un puerto específico tiene, históricamente, una muy baja velocidad de transmisión de datos. La actividad durante un periodo específico puede ser comparada con la línea de referencia a fin de determinar si tal actividad es congruente con la línea de referencia o constituye un alejamiento de la línea de referencia. Un alejamiento significativo de la velocidad histórica de datos puede indicar un alejamiento de la línea de referencia y, en consecuencia, puede sugerir una condición anormal, tal como un acceso no autorizado.

Puede utilizarse una amplia variedad de técnicas a fin de determinar que un actor no autorizado ha comenzado a usar el canal de comunicación. Por ejemplo, la autenticación de direcciones de MAC puede ser una manera de determinar la presencia de un dispositivo recientemente conectado. Cuando se hacen cambios autorizados, una dirección de MAC asociada al dispositivo a añadir puede ser especificada de antemano, de modo que las indicaciones del dispositivo autorizado recientemente añadido sean aceptadas y no den origen a una indicación de acceso no autorizado. De acuerdo a otras realizaciones, los criterios tales como las direcciones de IP, los protocolos de comunicaciones, los números de puertos de comunicación, etc., pueden ser usados a fin de detectar un dispositivo no autorizado recientemente añadido. Más aún, las tecnologías tales como USB, IEEE 1394, eSATA y similares pueden ser usadas para reconocer cuándo son conectados nuevos dispositivos a un sistema por primera vez. Los dispositivos conectados usando USB, IEEE 1394 y eSATA, y tecnologías similares, pueden ser denominados dispositivos periféricos. Si la conexión de un dispositivo de ese tipo es inesperada, el dispositivo recientemente conectado puede ser designado como un dispositivo no autorizado y pueden ser emprendidas una o más acciones de seguridad.

En consecuencia, la pasarela de comunicación 220 puede incluir varios procedimientos para detectar un acceso físico no autorizado. La pasarela de comunicación 220 puede ser configurable para minimizar las falsas detecciones positivas, requiriendo más de una señal que indique un acceso no autorizado. De acuerdo a una realización, la pasarela de comunicación 220 puede requerir al menos dos señales (p. ej., una señal tanto del sensor de puerta como del foto–detector) para determinar un acceso físico no autorizado. En otra realización, la pasarela de comunicación 220 puede requerir ciertas combinaciones de señales para determinar un acceso físico no autorizado.

Una vez que es detectado un acceso físico no autorizado, la pasarela de comunicaciones

220 puede emprender una o más acciones. En una realización, la pasarela de comunicación 220 puede tener la capacidad de configurar un perfil normal de ciber–seguridad y un perfil elevado de ciber–seguridad. En base a la detección de un ciber–ataque o una alteración física, la pasarela de comunicación 220 puede ajustar el perfil automáticamente como perfil elevado. Por ejemplo, si el sensor de puerta determina que la puerta ha sido abierta, y no hay pedidos de trabajo planificado para ese armario, el perfil de ciber–seguridad puede avanzar al estado elevado desde el estado normal, en un intento de restringir un compromiso adicional del sistema mayor.

En una realización, cuando la pasarela de comunicaciones 220 detecta un acceso no autorizado, puede alertar a los dispositivos de red flujo arriba (tales como el conmutador de red 242, la pasarela de comunicaciones 244 y la red de comunicaciones 246) en cuanto a que las comunicaciones desde el recinto 204 no pueden ya ser fiables, y poner en cuarentena todas las comunicaciones desde el recinto 204 y / o los dispositivos flujo arriba desde el recinto 204. Una alerta de ese tipo puede ser generada en cuanto sea detectado el acceso no autorizado, y la ciber–respuesta puede ser configurable en el dispositivo de comunicación flujo arriba, para terminar todas las comunicaciones, registrar todo el tráfico y / o continuar las operaciones habituales pero alertar a los dispositivos flujo arriba en cuanto al acceso no autorizado.

La pasarela de comunicación 220 puede ser capaz de prevalencia supervisora, de acuerdo a ciertas realizaciones congruentes con la presente revelación. Es decir, si está planificado el acceso autorizado al recinto 204, la detección de accesos no autorizados puede ser suspendida temporalmente. Además, las respuestas al acceso físico no autorizado pueden ser suspendidas temporalmente. Tal prevalencia puede ser lograda mediante un sistema SCADA o el acceso de ingeniería, de acuerdo a diversas realizaciones. Una prevalencia puede ser adecuada allí donde un suceso no planificado requiere acceso físico a un recinto. De acuerdo a un ejemplo, una prevalencia puede ser adecuada en un caso donde un vehículo ha chocado con el poste utilitario sobre el cual está ubicado un recinto. El personal de mantenimiento puede prevalecer sobre una acción de seguridad a fin de permitir que una parte del sistema de suministro de energía eléctrica sea descargada mientras se aborda el accidente.

De acuerdo a la realización ilustrada en la **Figura 2**, la pasarela de comunicación 220 puede ser físicamente distinta a los IED 208 y 208; sin embargo, de acuerdo a realizaciones alternativas, cierta funcionalidad asociada a la pasarela de comunicación 220 puede ser

incorporada a un IED. De acuerdo a tales realizaciones, un IED puede comprender una pluralidad de puertos configurados para recibir entrada desde sensores de diversos tipos (p. ej., micrófono, un sensor de puerta, un foto–detector, un acelerómetro, etc.). Además, un IED de ese tipo puede comprender puertos configurados para la comunicación con una red y / o un sistema SCADA.

La **Figura 3A** ilustra una representación conceptual de un sistema 300 que implementa una acción de seguridad como resultado de una detección de un dispositivo no autorizado 328, congruente con diversas realizaciones de la presente revelación. De acuerdo a la realización ilustrada en la **Figura 3A**, los IED 310, 312 y 314 están en comunicación, respectivamente, con las pasarelas de comunicación 316, 318 y 320. Cada una de las pasarelas de comunicación 316, 318, 320 está en comunicación con una red 326. Además, el sistema SCADA 322 y el sistema de información 324 también están en comunicación con la red 326. De acuerdo a realizaciones alternativas, los IED 310, 312 y 314 pueden estar físicamente integrados con las pasarelas de comunicación 316, 318 y 320, respectivamente.

A fin de conectar el dispositivo no autorizado 328 con la pasarela de comunicación 316, el acceso físico a la pasarela de comunicación 316 puede ser necesario. En consecuencia, una o más señales de detección de intrusión física (p. ej., luz de la apertura del armario, sonido asociado a la apertura de una puerta de armario, el salto de un sensor de puerta, etc.) pueden ser generadas como resultado de obtener un actor no autorizado acceso físico a la pasarela de comunicación 316. La conexión del dispositivo no autorizado 328 con la pasarela de comunicación 316 puede además proporcionar una indicación alternativa de acceso no autorizado. Por ejemplo, la pasarela de comunicación 316 puede determinar que una dirección de MAC asociada al dispositivo no autorizado 328 no está reconocida.

Como resultado de los sistemas de detección de intrusiones físicas y de la indicación alternativa de un acceso no autorizado proporcionada por la conexión del dispositivo no autorizado 328 con la pasarela de comunicación 316, el sistema 300 puede implementar una acción de seguridad. En una realización específica ilustrada en la **Figura 3A**, la comunicación desde la pasarela de comunicación 316 puede ser considerada sospechosa o no fiable, según lo indicado por los signos de interrogación 330. Como se ha descrito anteriormente, la comunicación entre los diversos dispositivos en el sistema 300 puede ser habitualmente fiable; sin embargo, tras la detección de un acceso no autorizado, los dispositivos flujo arriba desde la pasarela de comunicación 316 pueden ser notificados del acceso no autorizado y, en consecuencia, pueden no fiarse ya más de las comunicaciones

recibidas desde la pasarela de comunicaciones 316. Como se ha indicado anteriormente, uno de los indicios sobre los cuales ciertas comunicaciones pueden ser fiables es la recepción desde un nodo conocido, o dispositivo fiable en una red. A continuación de la detección de un acceso no autorizado, el nodo asociado a la pasarela de comunicación 316 puede ya no ser considerado fiable. En consecuencia, las comunicaciones desde la pasarela de comunicación 316 y los dispositivos flujo arriba desde la pasarela de comunicación 316 pueden ya no ser fiables (p. ej., el IED 310 y el dispositivo no autorizado a 328).

Pueden ser utilizados diversos protocolos para diferenciar entre comunicaciones fiables y no fiables, de acuerdo a realizaciones congruentes con la presente revelación. Esto puede permitir a la red ajustar los criterios y a todos los aparatos adoptar posiciones de ciber–defensa. En una realización, las pasarelas de comunicación 316, 318 y 320 pueden ser configuradas para usar un protocolo de control de acceso de red (p. ej., el IEEE 802.1X) para alertar a los otros aparatos de red sobre un intento de obtener acceso físico no autorizado a un recinto. El protocolo 802.1X puede proporcionar el control de acceso a la red y la autenticación de clientes, en base a puertos, en la capa física del modelo OSI de formación de redes de ordenadores. En otro ejemplo, una indicación de un acceso físico no autorizado puede ser transmitida mediante un sistema SCADA. Un punto SCADA puede ser correlacionado con un indicador de intrusión física a continuación de la detección de un acceso físico no autorizado. Las comunicaciones asociadas a un indicador de intrusión física pueden ser consideradas no fiables por el sistema SCADA.

La **Figura 3B** ilustra una representación conceptual del sistema de la **Figura 3A**, en el cual un cortafuegos 332 está colocado entre la pasarela de comunicación 316 y otros dispositivos de comunicación en el sistema 300, como resultado de una detección de un dispositivo no autorizado 328, congruente con diversas realizaciones de la presente revelación. El sistema 300, según lo ilustrado en la **Figura 3B**, puede funcionar de manera similar al sistema 300, según lo descrito anteriormente con relación a la **Figura 3A**; sin embargo, en la **Figura 3B**, el sistema 300 puede ser configurado para implementar una acción de seguridad alternativa como resultado de una detección del dispositivo no autorizado 328. El cortafuegos 332 puede ser configurado para bloquear las comunicaciones entrantes desde la pasarela de comunicación 316, el dispositivo no autorizado 328 y el IED 310. Se puede permitir pasar a través del cortafuegos 332 a las comunicaciones dirigidas a la pasarela de comunicación 316 y al IED 310. En otras palabras, el cortafuegos 332 puede permitir que pase la comunicación flujo abajo, pero el cortafuegos 332 puede bloquear la comunicación flujo arriba.

De acuerdo a otras realizaciones adicionales, el sistema 300, según lo ilustrado en la **Figura 3A** y la **Figura 3B**, puede implementar acciones de seguridad alternativa tras la detección del dispositivo no autorizado 328. Por ejemplo, el sistema 300 puede poner en cuarentena las comunicaciones flujo arriba desde la pasarela de comunicación 316. En otro ejemplo, el sistema 300 puede simular respuestas a las comunicaciones recibidas desde el dispositivo no autorizado 328 sin implementar ningún cambio en base a tales comunicaciones.

La **Figura 4** ilustra un gráfico de flujo de un procedimiento 400 para detectar acceso físico no autorizado a un recinto que contiene equipos asociados a un sistema de suministro de energía eléctrica, congruente con diversas realizaciones de la presente revelación. Un sistema de detección de intrusiones puede comprender uno o más componentes configurados para detectar acceso físico a un recinto. Según se describe con relación a diversas realizaciones anteriormente, tales componentes pueden incluir un micrófono, un sensor lumínico, un sensor de puerta, un acelerómetro, etc.

En 402, un sistema de detección de intrusiones puede ser activado. El procedimiento 400 puede esperar la recepción de una señal de detección desde el sistema de detección de intrusiones en 404. Una vez que se recibe una señal de detección, en 406, el procedimiento 400 puede determinar si la señal de detección es indicativa o no de un acceso no autorizado. Como se ha descrito anteriormente, los fenómenos naturales o ambientales pueden activar una señal de detección; sin embargo, el procedimiento 400 puede determinar en 406 que la señal de detección no es indicativa de un acceso no autorizado. Si se toma tal determinación, el procedimiento 400 puede volver a 404 y esperar la detección de una señal posterior.

Ciertas realizaciones pueden requerir que se satisfaga un umbral de confirmación de acceso no autorizado. De acuerdo a tales realizaciones, en 408, el procedimiento 400 puede determinar si se satisface o no el umbral de confirmación de acceso no autorizado. Una amplia variedad de información puede ser analizada a fin de determinar si se satisface o no el umbral de confirmación antes de implementar una acción de seguridad. De acuerdo a algunas realizaciones, el umbral de confirmación de acceso no autorizado puede ser satisfecho por una indicación de sensor alternativo. Por ejemplo, la señal de detección recibida en 404 puede estar basada en sonido detectado por un micrófono. Una indicación alternativa puede ser proporcionada por un sensor de puerta que indica que una puerta, o un panel, del recinto ha sido abierta. Según lo ilustrado por este ejemplo, indicaciones

alternativas pueden ser proporcionadas por múltiples componentes sensores asociados a un único recinto. Las realizaciones que se apoyan en indicaciones alternativas pueden proporcionar alguna protección ante una falsa alarma provocada por un único sensor estropeado.

El umbral de confirmación de acceso no autorizado también puede ser satisfecho usando información proporcionada por componentes sensores asociados a otros recintos, de acuerdo a diversas realizaciones. Por ejemplo, un terremoto puede activar acelerómetros asociados a sistemas de detección de intrusiones en distintas ubicaciones. De acuerdo a diversas realizaciones, en la medida en que múltiples acelerómetros asociados a sistemas de detección de intrusiones en proximidad física generan señales de detección a aproximadamente la misma hora, tales señales pueden ser comparadas a fin de deducir que los fenómenos naturales activaron las señales. Según lo ilustrado por este ejemplo, indicaciones alternativas pueden ser proporcionadas por componentes sensores dispersos entre múltiples recintos.

De acuerdo a más realizaciones adicionales, el umbral de confirmación de acceso no autorizado puede ser satisfecho en base a una evaluación de un intervalo de confianza asociado a una señal de detección específica. Por ejemplo, una señal de un sensor de puerta puede estar asociada a un intervalo de confianza mayor que una señal desde un micrófono. En consecuencia, en algunas realizaciones, una señal de detección basada en un sensor de puerta puede ser suficiente para satisfacer el umbral de confirmación, pero una señal desde un micrófono puede ser insuficiente para satisfacer el umbral de confirmación sin una indicación alternativa (p. ej., entrada desde un acelerómetro, confirmación visual de una persona no autorizada, en base a la inspección de una imagen obtenida usando una cámara, confirmación de un operador en una estación monitora central en cuanto a que el sonido corresponde a un intento de obtener acceso físico no autorizado, etc.).

En 410, una acción de seguridad puede ser implementada en base a un acceso no autorizado. Puede ser implementada una amplia variedad de acciones de seguridad. Por ejemplo, de acuerdo a algunas realizaciones, un cortafuegos puede ser configurado para bloquear las comunicaciones flujo arriba, originadas en un dispositivo de comunicación ubicado en un recinto que ha sido objeto de acceso sin autorización. De acuerdo a otras realizaciones, las comunicaciones para un dispositivo de comunicación ubicado en un recinto que ha sido objeto de acceso sin autorización pueden ser indicadas como no fiables. En una realización, la acción de seguridad puede incluir activar contactos de salida, en base

a la detección de un acceso no autorizado. Por ejemplo, los contactos de salida pueden activar una luz, una sirena o incluso una cámara. Una cámara activada como parte de una acción de seguridad puede además ser configurada para transmitir un flujo de vídeo o imágenes fijas a una estación monitora central. De acuerdo a algunas realizaciones, la acción de seguridad puede comprender impedir el acceso de ingeniería o el acceso al nivel del administrador al IED.

En 412, el procedimiento 400 puede determinar si ha sido resuelta o no la cuestión del acceso no autorizado. La resolución del acceso no autorizado puede lograrse despachando personal de servicio para inspeccionar el recinto, realizar pruebas de diagnóstico, revisar vídeo o imágenes de la cámara, o restringir cambios de configuraciones asociadas a equipos ubicados en el recinto. Tras la determinación de que la cuestión del acceso no autorizado ha sido resuelta, el procedimiento 400 puede volver a 404 y esperar la detección de otras señales que indiquen un acceso físico no autorizado.

Si bien han sido ilustradas y descritas realizaciones y aplicaciones específicas de la revelación, ha de entenderse que la revelación no está limitada a la configuración y componentes precisos revelados en la presente memoria. Diversas modificaciones, cambios y variaciones, evidentes para los expertos en la técnica, pueden ser hechos en la disposición, operación y detalles de los procedimientos y sistemas de la revelación, sin apartarse del espíritu y el ámbito de la revelación.

REIVINDICACIONES

1. Un dispositivo de comunicación configurado para proporcionar un trayecto de comunicación a un dispositivo electrónico inteligente (IED), y configurado para detectar y remediar un acceso no autorizado, comprendiendo el dispositivo de comunicación:
un puerto de comunicaciones de IED, configurado para comunicarse con un IED;
un puerto de red configurado para transmitir información recibida desde el IED mediante una red, y para transmitir información recibida desde la red al IED; y
lógica de control en comunicación con el puerto de comunicaciones del IED y el puerto de red, estando la lógica de control configurada para:
recibir una señal de detección de intrusión;
determinar que la señal de detección de intrusión es indicativa de un intento de obtener acceso no autorizado a uno entre el dispositivo de comunicación, el IED y un dispositivo en comunicación con el dispositivo de comunicación; y
emprender una acción de seguridad en base a la determinación de que la señal de detección de intrusión es indicativa del intento de obtener acceso no autorizado.

2. El dispositivo de comunicación de la reivindicación 1, en el que la lógica de control está adicionalmente configurada para generar una línea de referencia, representativa de la comunicación en uno entre el puerto de red y el puerto de comunicaciones del IED, y la señal de detección de intrusión comprende una divergencia de comunicación, con respecto a la línea de referencia, en uno entre el puerto de red y el puerto de comunicaciones del IED.

3. El dispositivo de comunicación de la reivindicación 2, en el que la lógica de control está adicionalmente configurada para recibir la señal de detección de intrusión, donde dicha señal comprende una comunicación originada en uno entre una dirección no autorizada de control de acceso a máquina, una dirección no autorizada del protocolo de Internet, un puerto no autorizado y un dispositivo periférico no autorizado.

4. El dispositivo de comunicación de la reivindicación 1, que comprende adicionalmente un puerto de detección de intrusión física; y en el que la señal de detección de intrusión comprende una señal de detección de intrusión física que incluye una salida de al menos uno entre un sensor de puerta y un sensor lumínico.

5. El dispositivo de comunicación de la reivindicación 1, que comprende adicionalmente:

un puerto de detección de intrusión física; y

un micrófono en comunicación con el puerto de detección de intrusión física;

en el que la lógica de control está adicionalmente configurada para diferenciar los sonidos recibidos por el micrófono, correspondientes a un acceso no autorizado, de los sonidos correspondientes a un fenómeno natural y a condiciones ambientales.

6. El dispositivo de comunicación de la reivindicación 1, que comprende adicionalmente:

un puerto de detección de intrusión física; y

un micrófono en comunicación con el puerto de detección de intrusión física;

en el que la lógica de control está adicionalmente configurada para:

transmitir un sonido recibido mediante el micrófono a una estación monitora central, mediante el puerto de red, y

recibir, mediante el puerto de red, una indicación desde la estación monitora central, en cuanto a que el sonido recibido mediante el micrófono es indicativo de un acceso no autorizado.

7. El dispositivo de comunicación de la reivindicación 1, que comprende adicionalmente:

un puerto de detección de intrusión física; y

un acelerómetro en comunicación con el puerto de detección de intrusión física, estando el acelerómetro configurado para detectar una aceleración, en el que la lógica de control está adicionalmente configurada para:

diferenciar entre una aceleración correspondiente a un acceso no autorizado de una aceleración correspondiente a un fenómeno natural, y de una aceleración correspondiente a una condición ambiental.

8. El dispositivo de comunicación de la reivindicación 7, en el que la lógica de control está adicionalmente configurada para comunicar a una estación monitora central información con respecto a la condición ambiental, para permitir a la estación monitora central implementar una estrategia de control en respuesta a la condición ambiental.

9. El dispositivo de comunicación de la reivindicación 1, que comprende adicionalmente:

una cámara en comunicación con la lógica de control;

en el que la lógica de control está adicionalmente configurada para transmitir imágenes capturadas por la cámara a una estación monitora central, mediante el

puerto de red, en base a la determinación de que la señal de detección de intrusión es indicativa del intento de obtener acceso no autorizado.

10. El dispositivo de comunicación de la reivindicación 1, en el que la lógica de control está adicionalmente configurada para suspender temporalmente la acción de seguridad al recibir una orden de supervisión prevaleciente.

11. El dispositivo de comunicación de la reivindicación 1, en el que la acción de seguridad comprende asignar automáticamente un perfil de alta seguridad al dispositivo de comunicación

12. El dispositivo de comunicación de la reivindicación 1, en el que la lógica de control está adicionalmente configurada para emprender la acción de seguridad, donde dicha acción comprende alertar a un sistema de control supervisor y adquisición de datos en cuanto al intento de obtener acceso no autorizado.

13. El dispositivo de comunicación de la reivindicación 1, en el que la lógica de control está adicionalmente configurada para emprender la acción de seguridad, donde dicha acción comprende alertar a dispositivos de red flujo arriba en cuanto al intento de obtener acceso no autorizado.

14. El dispositivo de comunicación de la reivindicación 13, en el que alertar a dispositivos de red flujo arriba comprende que la lógica de control está adicionalmente configurada para invocar un protocolo de control de acceso a la red.

15. El dispositivo de comunicación de la reivindicación 1, en el que la lógica de control está adicionalmente configurada para emprender la acción de seguridad, donde dicha acción comprende activar un dispositivo de seguridad.

16. El dispositivo de comunicación de la reivindicación 1, en el que la lógica de control está adicionalmente configurada para inhabilitar temporalmente la acción de seguridad para un acceso autorizado.

17. El dispositivo de comunicación de la reivindicación 1, en el que la lógica de control está adicionalmente configurada para recibir una segunda indicación que es indicativa del intento de obtener acceso no autorizado, antes de emprender la acción de

seguridad.

18. El dispositivo de comunicación de la reivindicación 17, en el que la lógica de control está adicionalmente configurada para generar una línea de referencia, representativa de la comunicación en uno entre el puerto de red y el puerto de comunicaciones del IED, y la segunda indicación comprende una divergencia de comunicación, con respecto a la línea de referencia, en uno entre el puerto de red y el puerto de comunicaciones del IED.

19. El dispositivo de comunicación de la reivindicación 17, en el que la lógica de control está adicionalmente configurada para recibir la señal de detección de intrusión en base a la entrada recibida desde un primer componente sensor, y para recibir la segunda indicación en base a la entrada recibida desde un segundo componente sensor.

20. El dispositivo de comunicación de la reivindicación 19, en el que la lógica de control está adicionalmente configurada para recibir la segunda indicación mediante el puerto de red desde un dispositivo remoto en comunicación con la red.

21. Un procedimiento para detectar y remediar un acceso no autorizado a equipos asociados a un sistema de suministro de energía eléctrica, contenido en un recinto, comprendiendo el procedimiento:
comunicar información con un IED mediante un puerto de comunicaciones del IED;
transmitir información, recibida desde el IED, a una red, mediante un puerto de red;
transmitir al IED información recibida desde la red;
recibir una señal de detección de intrusión;
determinar que la señal de detección de intrusión es indicativa de un intento de obtener acceso no autorizado a uno entre un dispositivo de comunicación y un dispositivo en comunicación con el dispositivo de comunicación; y
emprender una acción de seguridad en base a la determinación de que la señal de detección de intrusión es indicativa del intento de obtener acceso no autorizado.

22. El procedimiento de la reivindicación 21, que comprende adicionalmente:
generar una línea de referencia, representativa de la comunicación en uno entre el puerto de red y el puerto de comunicaciones del IED;
en el que la señal de detección de intrusión comprende una divergencia de comunicación, con respecto a la línea de referencia, en uno entre el puerto de red y el

puerto de comunicaciones del IED.

23. El procedimiento de la reivindicación 21, en el que la acción de seguridad comprende asignar automáticamente un perfil de alta seguridad al dispositivo de comunicación.

24. El procedimiento de la reivindicación 21, en el que la acción de seguridad comprende alertar a un sistema de control supervisor y adquisición de datos en cuanto al intento de obtener acceso no autorizado.

25. El procedimiento de la reivindicación 21, en el que la acción de seguridad comprende alertar a los dispositivos de red flujo arriba en cuanto al intento de obtener acceso no autorizado.

26. El procedimiento de la reivindicación 21, en el que la acción de seguridad comprende activar un dispositivo de seguridad.

27. El procedimiento de la reivindicación 21, que comprende adicionalmente:
recibir una segunda indicación que es indicativa del intento de obtener acceso no autorizado, antes de emprender la acción de seguridad.

28. El procedimiento de la reivindicación 27, que comprende adicionalmente:
generar una línea de referencia, representativa de la comunicación en uno entre el puerto de red y el puerto de comunicaciones del IED, y la segunda indicación comprende una divergencia de comunicación, con respecto a la línea de referencia, en uno entre el puerto de red y el puerto de comunicaciones del IED.

29. Un dispositivo electrónico inteligente (IED) configurado para detectar y remediar un acceso no autorizado, comprendiendo el IED:
un puerto de comunicaciones del IED, configurado para comunicarse con equipos monitorizados en comunicación eléctrica con un sistema de suministro de energía eléctrica;
un puerto de red configurado para transmitir información recibida desde el equipo monitorizado, mediante una red, y para transmitir información recibida desde la red al equipo monitorizado; y
lógica de control en comunicación con el puerto de comunicaciones del IED y el puerto de red, configurada para:

recibir una señal de detección de intrusión;

determinar que la señal de detección de intrusión física es indicativa de un intento de obtener acceso no autorizado a uno entre el IED y un dispositivo en comunicación con el IED; y

emprender una acción de seguridad en base a la determinación de que la indicación es indicativa del intento de obtener acceso no autorizado.

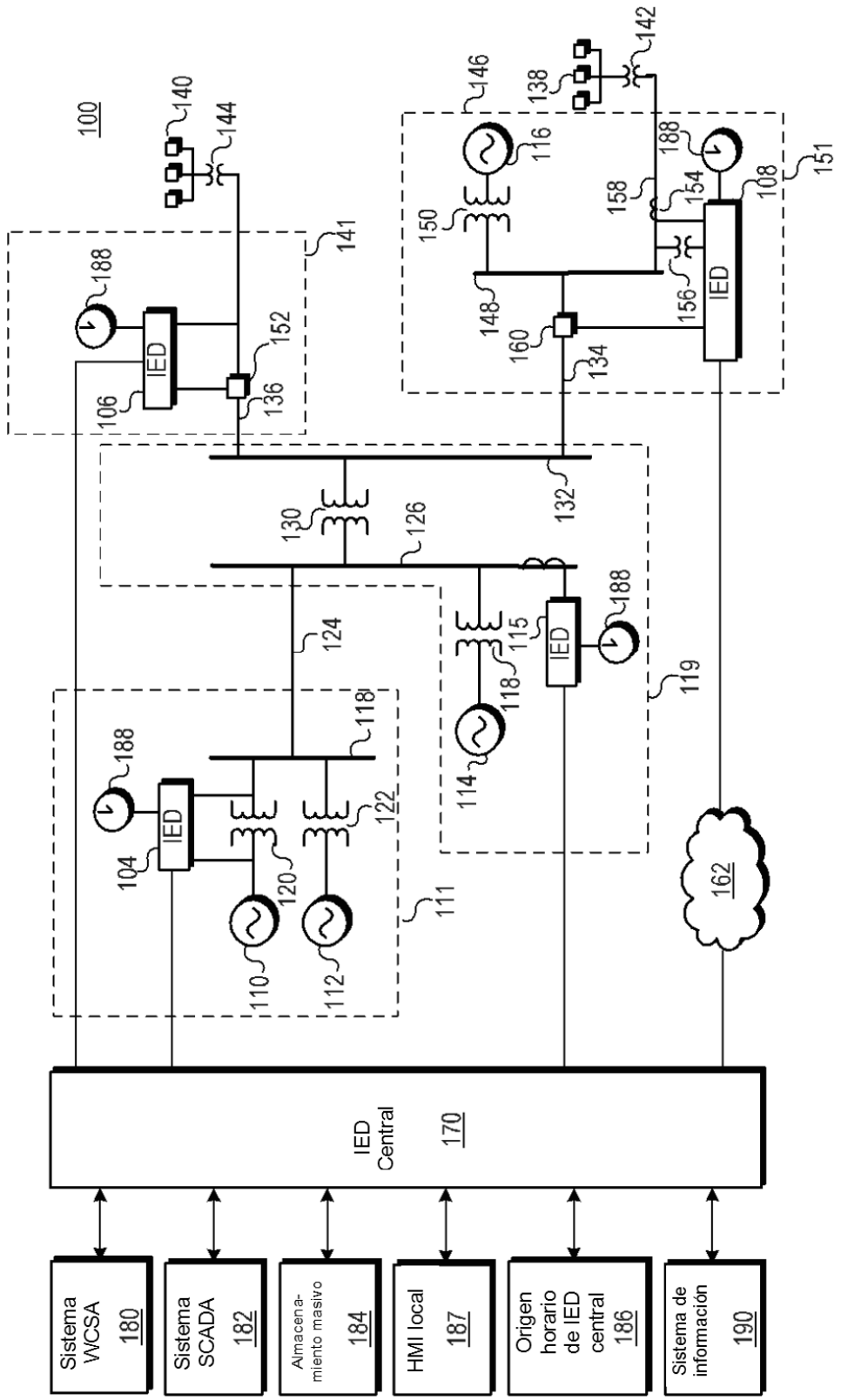
100
140
144
141
188
IED
106
152
136
146
116
142
138
188
158
154
108
151
150
148
160
156
IED
134
132
130
126
124
188
IED
115
118
119
104
120
122
118
114
110
112
111
162
IED Central
170
Sistema WCSA
180
Sistema SCADA
182
Almacena-miento masivo
184
HMI local
187
Origen horario de IED central
186
Sistema de infomación
190

Figura 1

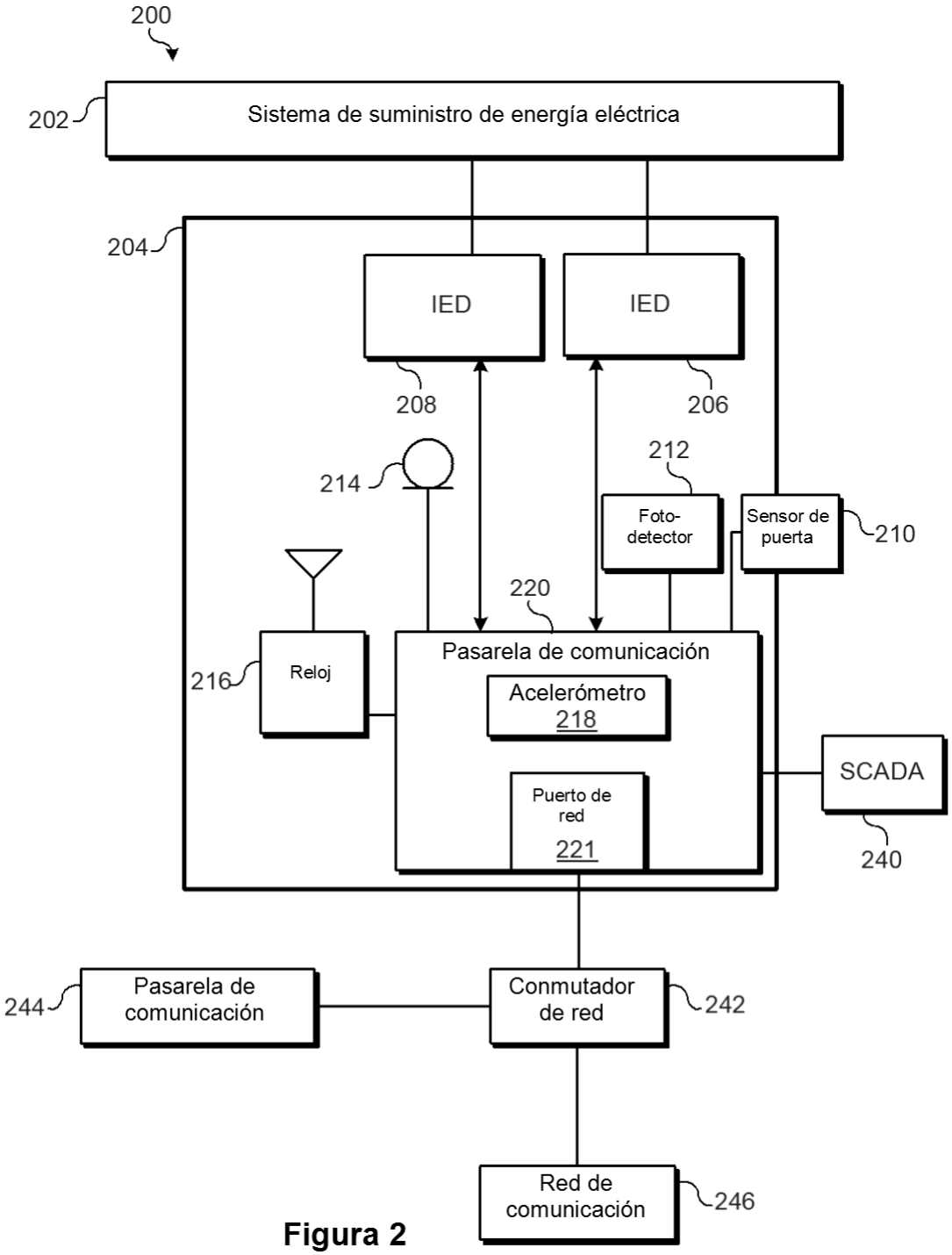
200
202
Sistema de suministro de energía eléctrica
204
IED
IED
208
206
212
214
Foto-detector
Sensor de puerta
210
220
Reloj
216
Pasarela de comunicación
Acelerómetro 218
Puerto de red 221
SCADA
240
244
Pasarela de comunicación
Conmutador de red
242
Red de comunicación
246

Figura 2

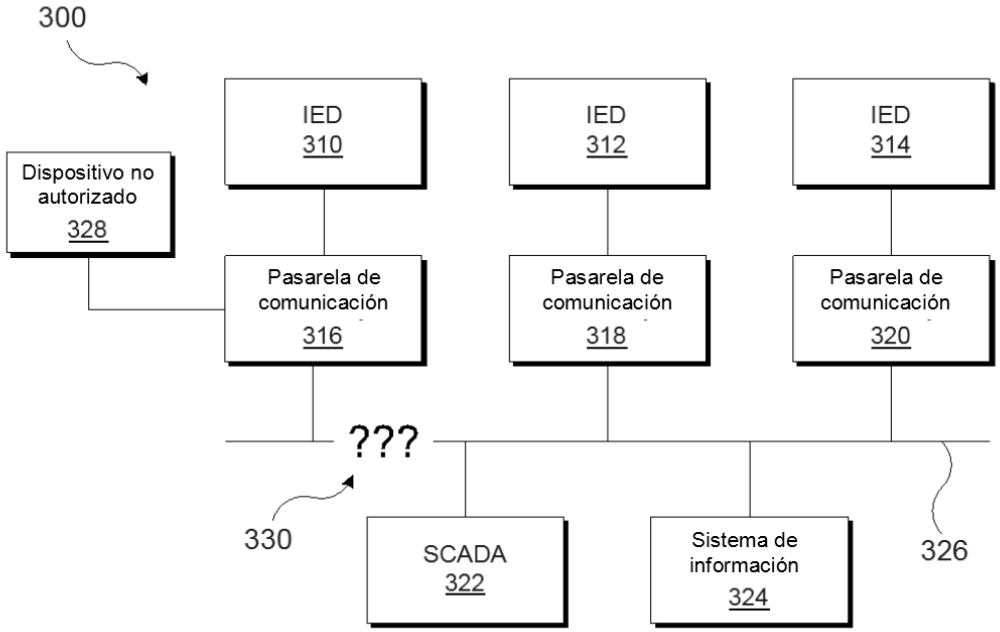

Figura 3A

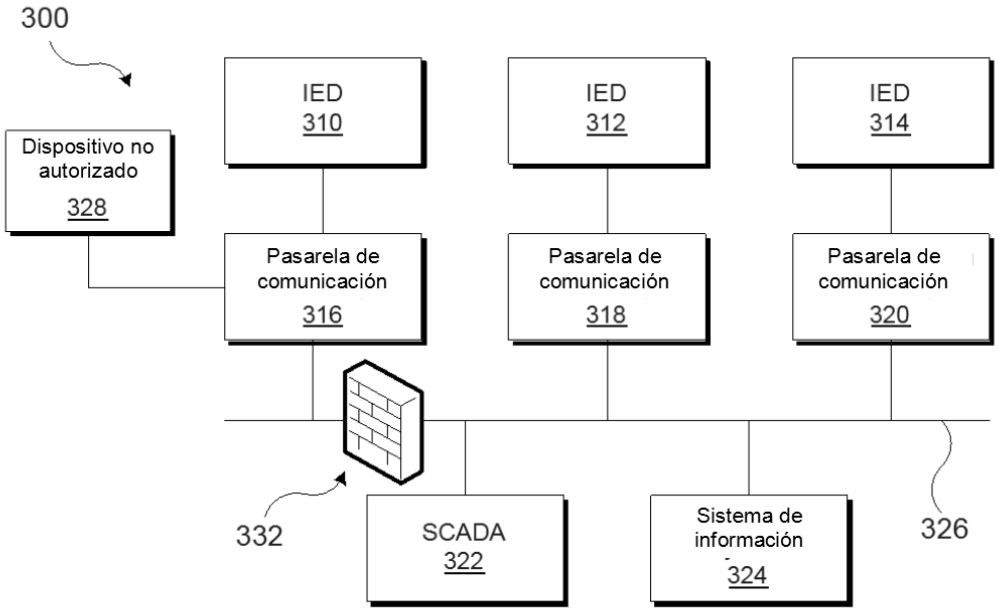

Figura 3B

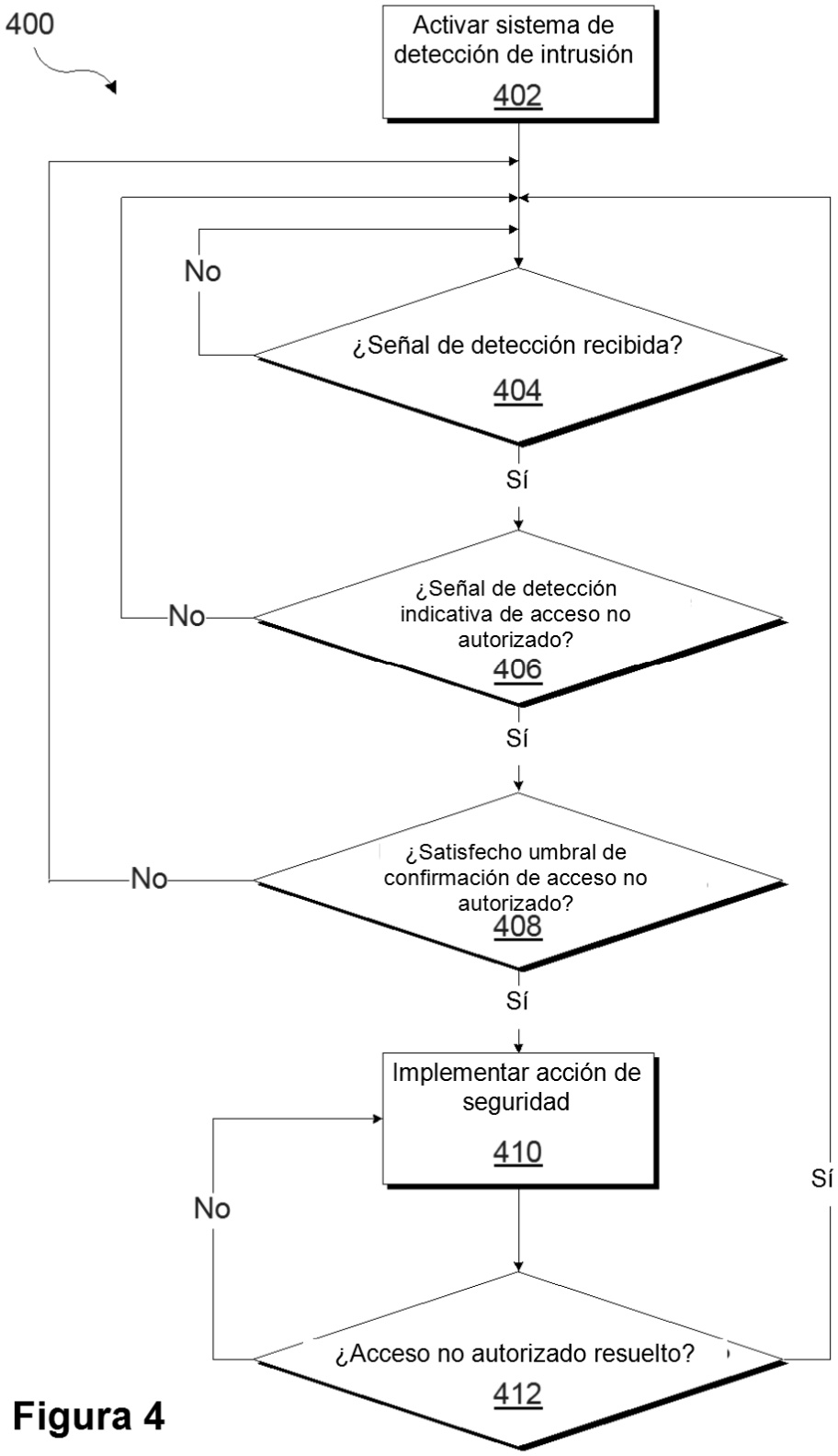
400
Activar sistema de detección de intrusión
402
No
¿Señal de detección recibida?
404
Sí
No
¿Señal de detección indicativa de acceso no autorizado?
406
Sí
No
¿Satisfecho umbral de confirmación de acceso no autorizado?
408
Sí
Implementar acción de seguridad
410
No
Sí
¿Acceso no autorizado resuelto?
412

Figura 4

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201590028

(22) Fecha de presentación de la solicitud: 03.10.2013

(32) Fecha de prioridad: **12-10-2012**
14-03-2013

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** Ver Hoja Adicional

DOCUMENTOS RELEVANTES

Categoría	(56) **Documentos citados**	**Reivindicaciones afectadas**
X	US 2004193329 A1 (RANSOM DOUGLAS S et al.) 30.09.2004, párrafos 24,33,38,39,49,50,56,87-89,207-221; figuras 1,2a,13.	1-3,11-15,17-29
Y		4-10,16
Y	US 5986543 A (JOHNSON SAM) 16.11.1999, columna 2, líneas 21-52; columna 4, líneas 39-51; columna 7, líneas 46-56; columna 8, líneas 58-65; columna 11, línea 66 – columna 12, línea 9; columna 13, línea 63 – columna 14, línea 58; figuras 2,4a,6-8f.	4,6,10
Y	WO 0075900 A1 (STRATEGIC VISTA INTERNAT INC et al.) 14.12.2000, página 3, línea 2 – página 5, línea 30; página 6, líneas 9-19; página 9, líneas 7-12; página 15, líneas 14-18; página 17, línea 22 – página 18, línea 25; figura 1.	5,9,16
Y	WO 2011073241 A1 (EYASI TRADING GROUP LC et al.) 23.06.2011, párrafos 32-36,60; figuras 1,2,7.	7,8

Categoría de los documentos citados
X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado
☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	**Examinador**	**Página**
12.02.2016	M. J. Lloris Meseguer	1/7

CLASIFICACIÓN OBJETO DE LA SOLICITUD

G06F21/55 (2013.01)
G08B13/00 (2006.01)
H04L12/22 (2006.01)
H04L29/02 (2006.01)

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

G06F, G08B, H04L

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC, WPI

Fecha de Realización de la Opinión Escrita: 12.02.2016

Declaración

Novedad (Art. 6.1 LP 11/1986)	Reivindicaciones	1-28	**SI**
	Reivindicaciones	29	**NO**
Actividad inventiva (Art. 8.1 LP11/1986)	Reivindicaciones		**SI**
	Reivindicaciones	1-29	**NO**

Se considera que la solicitud cumple con el requisito de aplicación industrial. Este requisito fue evaluado durante la fase de examen formal y técnico de la solicitud (Artículo 31.2 Ley 11/1986).

Base de la Opinión.-

La presente opinión se ha realizado sobre la base de la solicitud de patente tal y como se publica.

1. Documentos considerados.-

A continuación se relacionan los documentos pertenecientes al estado de la técnica tomados en consideración para la realización de esta opinión.

Documento	Número Publicación o Identificación	Fecha Publicación
D01	US 2004193329 A1 (RANSOM DOUGLAS S et al.)	30.09.2004
D02	US 5986543 A (JOHNSON SAM)	16.11.1999
D03	WO 0075900 A1 (STRATEGIC VISTA INTERNAT INC et al.)	14.12.2000
D04	WO 2011073241 A1 (EYASI TRADING GROUP LC et al.)	23.06.2011

2. Declaración motivada según los artículos 29.6 y 29.7 del Reglamento de ejecución de la Ley 11/1986, de 20 de marzo, de Patentes sobre la novedad y la actividad inventiva; citas y explicaciones en apoyo de esta declaración

De todos los documentos recuperados del estado de la técnica, se considera que el documento D01 es el más próximo a la solicitud que se analiza. A continuación se comparan las reivindicaciones de la solicitud con el documento D01.

Reivindicación 1
El documento D01 describe un sistema para la gestión del suministro de energía eléctrica, en un sistema de distribución de energía eléctrica, que comprende múltiples dispositivos electrónicos inteligentes (IED) distribuidos por el sistema, para gestionar el flujo y el consumo de energía (ver figuras 1 y 2a).
Los dispositivos electrónicos inteligentes (IED) pueden comprender (ver figura 13 y párrafos 89, 210 y 219) un dispositivo de comunicación para permitir la comunicación del IED, con otros dispositivos, a través de una red y configurado para detectar y actuar en el caso de que se produzca un acceso no autorizado, que puede afectar a la integridad del sistema. La identificación de un acceso no autorizado se puede realizar monitorizando patrones de acceso y comportamientos en un IED determinado, en redes de dispositivos IED o en un sistema completo de dispositivos IED.
La monitorización se puede realizar mediante la supervisión del tráfico en la red y su análisis, para detectar una actividad inusual e intentos de acceso, empleando reglas que determinan los distintos niveles de acceso (quién puede acceder a qué) o revisando los eventos ocurridos; pudiendo emplear técnicas estadísticas o inteligencia artificial.
En caso de detectar un intento de obtener acceso no autorizado, el dispositivo de comunicación activa una acción de seguridad (ver párrafos 219-221).

La invención definida en la reivindicación 1 difiere del documento D01 en que el dispositivo de comunicación podría ser físicamente distinto a los IED y no estar incorporado en un IED. Sin embargo, esta diferencia se considera un modo de realización particular, por lo que no se considera que la reivindicación 1 cumpla el requisito de actividad inventiva conforme al artículo 8.1 LP.

Reivindicaciones 2 y 3
El documento D01 indica que el dispositivo de comunicación puede determinar que se ha producido el intento de obtener acceso no autorizado a partir de la supervisión del tráfico de la red y del análisis del mismo para detectar actividades inusuales e intentos de acceso, empleando reglas que determinan los distintos niveles de acceso (quién puede acceder a qué) o revisando los eventos ocurridos; pudiendo emplear técnicas estadísticas o inteligencia artificial (ver párrafos 89, 219).
A la vista de lo que se conoce del documento D01, no se considera que requiera ningún esfuerzo inventivo para un experto en la materia desarrollar un dispositivo como el descrito en las reivindicaciones 2 y 3. Por consiguiente, no se considera que estas reivindicaciones cumplan el requisito de actividad inventiva conforme al artículo 8.1 LP.

Reivindicación 4
La invención definida en la reivindicación 4 difiere del documento D01 en que indica que el dispositivo comprende adicionalmente un puerto de detección de intrusión física; y en el que la señal de detección de intrusión comprende una señal de detección de intrusión física que incluye una salida de al menos uno entre un sensor de puerta y un sensor lumínico. De esta manera el dispositivo puede detectar una intrusión física a partir de las medidas realizadas por un sensor de puerta o un sensor lumínico. El problema técnico objetivo que resuelve así la reivindicación es poder detectar una intrusión física a partir de las medidas realizadas por un sensor de puerta o un sensor lumínico.

El documento D02 describe un sistema de seguridad para detectar una intrusión física en una zona protegida, en particular, una intrusión en un vehículo. El sistema de seguridad comprende una unidad de control y comunicación (201) que determina que se ha producido una intrusión física a partir de las medidas realizadas por un sensor de puerta (205).

Por tanto, el problema técnico objetivo mencionado anteriormente se encuentra resuelto en el documento D02. En consecuencia, la reivindicación 4 carece de actividad inventiva según el artículo 8.1 LP.

Reivindicación 5

La invención definida en la reivindicación 5 difiere del documento D01 en que indica que el dispositivo comprende adicionalmente un puerto de detección de intrusión física; y un micrófono en comunicación con el puerto de detección de intrusión física. Estando la lógica de control configurada para diferenciar los sonidos recibidos por el micrófono, correspondientes a un acceso no autorizado, de los sonidos correspondientes a un fenómeno natural y a condiciones ambientales. El problema técnico objetivo que resuelve así la reivindicación es poder diferenciar en el dispositivo entre sonidos que pueden corresponder a un acceso no autorizado de sonidos que pueden corresponder a un fenómeno natural y a condiciones ambientales.

El documento D03 describe un sistema de seguridad que puede activar una alarma (ver figura 1). El sistema comprende una unidad de control central (20) que activa una condición de alarma en función de las señales recibidas de una serie de unidades periféricas (40). Estas unidades (40) pueden incluir sensores (42) para detectar una intrusión física. En particular, pueden comprender un micrófono, enviándose a la unidad de control central (20) el nivel de sonido detectado. La unidad de control central diferencia entre sonidos que pueden corresponder a un acceso no autorizado de sonidos que pueden corresponder a condiciones ambientales; activando una condición de alarma sólo cuando los niveles de sonido detectados superen un umbral establecido (ver página 18, líneas 7-12).

Por tanto, el problema técnico objetivo mencionado anteriormente se encuentra resuelto en el documento D03. En consecuencia, la reivindicación 5 carece de actividad inventiva según el artículo 8.1 LP.

Reivindicación 6

La invención definida en la reivindicación 6 difiere del documento D01 en que indica que el dispositivo comprende adicionalmente un puerto de detección de intrusión física; y un micrófono en comunicación con el puerto de detección de intrusión física. Estando la lógica de control configurada para transmitir un sonido recibido mediante el micrófono a una estación monitora central, mediante el puerto de red, y recibir, mediante el puerto de red, una indicación desde la estación monitora central, en cuanto a que el sonido recibido mediante el micrófono es indicativo de un acceso no autorizado.
De esta manera el dispositivo puede detectar una intrusión física a partir de los sonidos captados por un micrófono, que son enviados a una estación monitora central, que es la que determina e indica al dispositivo si se ha producido una intrusión física. El problema técnico objetivo que resuelve así la reivindicación es poder detectar una intrusión física a partir de los sonidos captados por un micrófono, que son enviados a una estación monitora central, que es la que determina e indica si se ha producido una intrusión física.

El documento D02 describe un sistema de seguridad para detectar una intrusión física en una zona protegida, en particular, una intrusión en un vehículo. El sistema de seguridad comprende una unidad de control y comunicación (201) que puede enviar a una estación monitora (103) los sonidos captados por un micrófono (211c), determinándose en la estación monitora (103) si estos sonidos son indicativos de una intrusión física y, en tal caso, enviando una señal de control al vehículo.

Por tanto, el problema técnico objetivo mencionado anteriormente se encuentra resuelto en el documento D02. En consecuencia, la reivindicación 6 carece de actividad inventiva según el artículo 8.1 LP.

Reivindicaciones 7 y 8

La invención definida en la reivindicación 7 difiere del documento D01 en que indica que el dispositivo comprende adicionalmente un puerto de detección de intrusión física; y un acelerómetro, configurado para detectar una aceleración, en comunicación con el puerto de detección de intrusión física. Estando la lógica de control configurada para diferenciar entre una aceleración correspondiente a un acceso no autorizado de una aceleración correspondiente a un fenómeno natural, y de una aceleración correspondiente a una condición ambiental.
El problema técnico objetivo que resuelve así la reivindicación es poder diferenciar en el dispositivo entre aceleraciones que pueden ser debidas a un acceso no autorizado de aceleraciones que pueden corresponder a un fenómeno natural y a condiciones ambientales.

El documento D04 describe un sistema y un método para detectar una intrusión en un área cerrada, a partir de las medidas de aceleración tomadas por un acelerómetro (ver figura 1). El sistema, (ver párrafo 60) a partir de las medidas tomadas, es capaz de distinguir entre aceleraciones debidas a una intrusión de aceleraciones causadas por un fenómeno natural o condiciones ambientales (como el viento o movimientos de baja frecuencia).

Por tanto, el problema técnico objetivo mencionado anteriormente se encuentra resuelto en el documento D04. En consecuencia, la reivindicación 7 carece de actividad inventiva según el artículo 8.1 LP.

La invención definida en la reivindicación 8 difiere del documento D01 en que indica que la lógica de control está configurada para comunicar a una estación monitora central información con respecto a la condición ambiental, para permitir a la estación monitora central implementar una estrategia de control en respuesta a la condición ambiental.
El problema técnico objetivo que resuelve así la reivindicación es poder adaptar la estrategia de control de la estación monitora central, en función de la información relativa a las condiciones ambientales, recibida del dispositivo.

El documento D04 indica que los módulos sensores empleados (acelerómetros), que pueden tener medios de procesamiento, se comunican con un módulo principal que analiza los datos recibidos (ver párrafo 36). Los módulos sensores comunican los movimientos de baja frecuencia al módulo principal, que establece un nivel superior para comparación. Cuando el nivel del impacto detectado excede a este nivel superior, se considera que se ha producido una intrusión (ver párrafo 60).

Por tanto, el problema técnico objetivo mencionado anteriormente se encuentra resuelto en el documento D04. En consecuencia, la reivindicación 8 carece de actividad inventiva según el artículo 8.1 LP.

Reivindicación 9

La invención definida en la reivindicación 9 difiere del documento D01 en que indica que el dispositivo comprende adicionalmente una cámara. Estando la lógica de control configurada para transmitir imágenes capturadas por la cámara a una estación remota central, mediante el puerto de red, en base a la determinación de que la señal de detección de intrusión es indicativa del intento de obtener acceso no autorizado.
El problema técnico objetivo que resuelve así la reivindicación es poder obtener, en una estación remota central, las imágenes capturadas por una cámara cuando se considera que se ha producido un acceso no autorizado.

El documento D03 describe un sistema de seguridad que puede activar una alarma (ver figura 1). El sistema comprende una unidad de control central (20) que activa una condición de alarma en función de las señales recibidas de una serie de unidades periféricas (40). Estas unidades (40) pueden incluir sensores (42) para detectar una intrusión física. En particular, también pueden comprender una cámara de video en comunicación con la unidad de control central (20), pudiendo acceder a las imágenes tomadas, de manera remota, a través de la comunicación con la unidad de control central (20) (ver página 17, líneas 22-26). En caso de detectarse una condición de alarma, el sistema de seguridad procesa la señal de video, permitiendo ver los eventos ocurridos a un servicio de monitorización, con objeto de dar respuesta a una situación de alarma (ver página 3, líneas 22-26).

Por tanto, el problema técnico objetivo mencionado anteriormente se encuentra resuelto en el documento D03. En consecuencia, la reivindicación 9 carece de actividad inventiva según el artículo 8.1 LP.

Reivindicación 10

La invención definida en la reivindicación 10 difiere del documento D01 en que indica que la lógica de control del dispositivo está configurada para suspender temporalmente la acción de seguridad al recibir una orden de supervisión prevaleciente.
El problema técnico objetivo que resuelve así la reivindicación es poder desactivar temporalmente la acción de seguridad en el dispositivo, a partir de una orden recibida.

El documento D02 indica que si la estación monitora (103) determina que el usuario es un usuario autorizado, la estación monitora (103) puede enviar una señal al sistema de seguridad para suspender temporalmente la acción de seguridad (ver figura 7).

Por tanto, el problema técnico objetivo mencionado anteriormente se encuentra resuelto en el documento D02. En consecuencia, la reivindicación 10 carece de actividad inventiva según el artículo 8.1 LP.

Reivindicaciones 11 y 12

El documento D01 indica que el dispositivo de comunicación puede considerar no responder a ciertos tipos de peticiones si considera que se puede estar produciendo un ataque (ver párrafo 219). El documento D01 también indica que, en caso de detectarse un ataque, el dispositivo de comunicación puede informar del mismo a un servidor central (ver párrafo 219). A la vista de lo que se conoce del documento D01, no se considera que requiera ningún esfuerzo inventivo para un experto en la materia desarrollar un dispositivo como el descrito en las reivindicaciones 11 y 12. Por consiguiente, no se considera que estas reivindicaciones cumplan el requisito de actividad inventiva conforme al artículo 8.1 LP.

Reivindicaciones 13 y 14

El documento D01 indica que el dispositivo de comunicación puede emplear alarmas antirrobo que están configuradas para alertar a todo el sistema de que se está produciendo un ataque (ver párrafos 219 y 220). Como ya se ha indicado, el documento D01 también indica que el dispositivo de comunicación puede considerar no responder a ciertos tipos de peticiones si considera que se puede estar produciendo un ataque (ver párrafo 219), como podría ser en el caso de que se haya activado una alarma antirrobo. A la vista de lo que se conoce del documento D01, no se considera que requiera ningún esfuerzo inventivo para un experto en la materia desarrollar un dispositivo como el descrito en las reivindicaciones 13 y 14. Por consiguiente, no se considera que estas reivindicaciones cumplan el requisito de actividad inventiva conforme al artículo 8.1 LP.

Reivindicación 15
El documento D01 indica que en caso de detectar un intento de obtener acceso no autorizado, el dispositivo de comunicación activa una acción de seguridad (ver párrafos 219-220) que puede consistir en activar una alarma antirrobo. Por tanto, se puede concluir que, a la vista del documento D01, la reivindicación 15 no cumple el requisito de actividad inventiva según el artículo 8.1 LP.

Reivindicación 16
La invención definida en la reivindicación 16 difiere del documento D01 en que indica que la lógica de control está adicionalmente configurada para inhabilitar temporalmente la acción de seguridad para un acceso autorizado.
El problema técnico objetivo que resuelve así la reivindicación es poder inhabilitar temporalmente la acción de seguridad del dispositivo, cuando se produce un acceso autorizado.

El documento D03 indica que el sistema de seguridad puede estar programado para permanecer inactivo hasta que un operador del servicio de monitorización lleve a cabo un diagnóstico del sistema (ver página 18, líneas 23-25); es decir, se inhabilita temporalmente cuando se produce un acceso por parte de un operador del servicio de monitorización.

Por tanto, el problema técnico objetivo mencionado anteriormente se encuentra resuelto en el documento D03. En consecuencia, la reivindicación 16 carece de actividad inventiva según el artículo 8.1 LP.

Reivindicaciones 17 y 18
El documento D01 indica que el dispositivo de comunicación puede emplear una combinación de varias técnicas o métodos para identificar a posibles intrusos, antes de activar una acción de seguridad. Uno de estos métodos para determinar que se ha producido el intento de obtener acceso no autorizado puede consistir en la supervisión del tráfico de la red y del análisis del mismo para detectar actividades inusuales e intentos de acceso (ver párrafos 219-220). A la vista de lo que se conoce del documento D01, no se considera que requiera ningún esfuerzo inventivo para un experto en la materia desarrollar un dispositivo como el descrito en las reivindicaciones 17 y 18. Por consiguiente, no se considera que estas reivindicaciones cumplan el requisito de actividad inventiva conforme al artículo 8.1 LP.

Reivindicaciones 19 y 20
El documento D01 indica que el dispositivo de comunicación puede determinar una intrusión y activar una acción de seguridad a partir de la supervisión del tráfico de la red y del análisis del mismo junto con la activación de una alarma antirrobo (ver párrafos 219-220). En este último caso, la activación de la alarma antirrobo puede haberse recibido desde otro dispositivo de comunicación, conectado en red (ver párrafos 219-220). A la vista de lo que se conoce del documento D01, no se considera que requiera ningún esfuerzo inventivo para un experto en la materia desarrollar un dispositivo como el descrito en las reivindicaciones 19 y 20. Por consiguiente, no se considera que estas reivindicaciones cumplan el requisito de actividad inventiva conforme al artículo 8.1 LP.

Reivindicaciones 21-28
Las reivindicaciones 21-28 son reivindicaciones relativas a un procedimiento para detectar y remediar un acceso no autorizado a equipos asociados a un sistema de suministro de energía eléctrica, contenido en un recinto, que presentan un contenido equivalente a las reivindicaciones 1, 2, 11-13,15, 17 y 18, relativas a un dispositivo de comunicación configurado para proporcionar una comunicación a un dispositivo electrónico inteligente (IED), y configurado para detectar y remediar un acceso no autorizado. Dado que no se considera que las reivindicaciones de dispositivo cumplan el requisito de actividad inventiva conforme al artículo 8.1 LP, tampoco se considera que las reivindicaciones 21-28 de procedimiento cumplan el requisito de actividad inventiva conforme al artículo 8.1 LP.

Reivindicación 29
La reivindicación 29 que es relativa a un dispositivo electrónico inteligente (IED), configurado para detectar y remediar un acceso no autorizado, presenta un contenido similar a la reivindicación 1, con la diferencia de que en la reivindicación 1 la lógica de control puede incorporarse en un dispositivo de comunicación físicamente distinto a los IED. Sin embargo, en la reivindicación 29 esta lógica de control sí que se encuentra incorporada en el IED. El documento D01 también indica esta forma de realización por lo que las características descritas en la reivindicación 29 quedan divulgadas por dicho documento. En consecuencia, no se considera que la reivindicación 29 cumpla el requisito de novedad conforme al artículo 6.1 LP.