(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 464 665**

(21) Número de solicitud: 201390095

(51) Int. CI.:

G06F 21/41 (2013.01)

(12) SOLICITUD DE PATENTE A2

(22) Fecha de presentación:

21.06.2012

(30) Prioridad:

22.06.2011 US 13/166,648

(43) Fecha de publicación de la solicitud:

03.06.2014

(71) Solicitantes:

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

(72) Inventor/es:

SMITH, Rhett;
BRADETICH, Ryan;
EWING, Christopher;
KIPP, Nathan Paul y
YAUCHZEE, Kimberly Ann

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

(54) Título: **Sistemas y procedimientos de gestión de sesiones de comunicación seguras con dispositivos remotos**

(57) Resumen:

Según varias realizaciones, un gestor de sesiones genera, almacena y actualiza periódicamente las credenciales de inicio de sesión de cada uno de una pluralidad de IED conectados. Un operador, posiblemente a través de un dispositivo de acceso, puede proporcionar credenciales de inicio de sesión únicas al gestor de sesiones. El gestor de sesiones puede determinar el nivel de autorización del operador basándose en las credenciales de inicio de sesión del operador, que definen con qué IED puede comunicarse el operador. Según varias realizaciones, el gestor de sesiones no facilita una sesión de comunicación entre el operador y un IED objetivo. En cambio, el gestor de sesiones mantiene una primera sesión de comunicación con el operador e inicia una segunda sesión de comunicación con el IED objetivo. Por consiguiente, el gestor de sesiones puede reenviar comandos transmitidos por el operador al IED objetivo. En función del nivel de autorización del operador, un filtro de sesiones puede restringir lo que puede comunicarse entre un operador y un IED.

ES 2 464 665 A2

DESCRIPCIÓN

Sistemas y procedimientos de gestión de sesiones de comunicación seguras con dispositivos remotos.

CAMPO TÉCNICO

La presente invención se refiere, en general, a sistemas y procedimientos de gestión de sesiones de comunicación seguras. Más en particular, los sistemas y procedimientos dados a conocer en este documento pueden implementarse en pasarelas, cortafuegos y otros dispositivos de red y pueden configurarse para implementar paradigmas de control de acceso modernos a través de varios dispositivos conectados en red.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

A continuación se describen realizaciones no limitativas y no exhaustivas de la divulgación, incluidas varias realizaciones de la divulgación con referencia a las figuras, en las que:

La FIG.1 ilustra una realización de un sistema de gestión de sesiones de pasarela que incluye un gestor de sesiones, múltiples dispositivos electrónicos inteligentes (IED) y un dispositivo de acceso del operador.

La FIG. 2 ilustra una realización de un diagrama de bloques funcional de un sistema informático configurado para gestionar las credenciales de inicio de sesión y las sesiones de comunicación entre un dispositivo de acceso y uno o más IED.

La FIG. 3 ilustra una realización de un procedimiento para establecer y mantener credenciales de inicio de sesión seguras para cada uno de una pluralidad de IED.

La FIG. 4 ilustra una realización de un procedimiento para iniciar una sesión de comunicación entre un dispositivo de acceso y un gestor de sesiones.

La FIG. 5 ilustra una realización de un procedimiento para iniciar una primera sesión de comunicación entre un dispositivo de acceso y un gestor de sesiones y una segunda sesión de comunicación controlada por el acceso entre un IED y el gestor de sesiones.

Las FIG. 6A y 6B ilustran realizaciones de tablas representativas de la gestión de credenciales de un IED heredado y de un IED moderno más seguro, respectivamente.

La FIG. 7 ilustra una tabla representativa para gestionar las credenciales de inicio de sesión y las conexiones de una pluralidad de IED en una realización de un gestor de sesiones.

La FIG. 8 ilustra una tabla representativa para gestionar las credenciales de inicio de sesión y el nivel de autorización asociado concedido a cada uno de una pluralidad de dispositivos de acceso mediante un gestor de sesiones.

La FIG. 9 ilustra una tabla representativa para gestionar las credenciales de inicio de sesión y los niveles de autorización asociados concedidos a cada uno de una pluralidad de dispositivos de acceso mediante un gestor de sesiones que incluye un filtro de sesiones.

En la siguiente descripción se proporcionan numerosos detalles específicos para un entendimiento minucioso de las diversas realizaciones dadas a conocer en este documento. Los sistemas y procedimientos dados a conocer en este documento pueden llevarse a la práctica sin uno o más de los detalles específicos, o con otros procedimientos, componentes, materiales, etc. Además, en algunos casos, estructuras, materiales u operaciones ampliamente conocidos pueden no mostrarse o describirse en detalle para no oscurecer los aspectos de la invención. Además, las propiedades, estructuras o características pueden combinarse de cualquier manera adecuada en una o más realizaciones alternativas.

DESCRIPCIÓN DETALLADA

La presente divulgación proporciona sistemas y procedimientos para gestionar el acceso a una pluralidad de dispositivos electrónicos inteligentes (IED). Según varias realizaciones, las medidas de seguridad incorporadas de los IED existentes varían considerablemente. Por ejemplo, los IED heredados no pueden distinguir usuarios únicos y pueden incluir combinaciones de nombre de usuario/contraseña con una longitud y/o un conjunto de caracteres limitados. Incluso usando IED modernos, que pueden permitir la creación de numerosas

combinaciones complejas de nombre de usuario/contraseña, puede ser difícil gestionar y actualizar un elevado número de credenciales de inicio de sesión a través de una red de IED.

Según varias realizaciones dadas a conocer en este documento, un gestor de sesiones puede configurarse para gestionar y actualizar las credenciales de inicio de sesión de una pluralidad de IED conectados en red. Además, un gestor de sesiones puede gestionar una pluralidad de credenciales de inicio de sesión de dispositivo de acceso. Según varias realizaciones, un gestor de sesiones puede configurarse con una variedad de puertos de red y puede comunicarse usando una gran variedad de protocolos de comunicaciones. Por ejemplo, un gestor de sesiones puede configurarse con puertos serie y puertos de Ethernet y puede comunicarse con y/o traducir varios protocolos asociados a varios tipos de conexiones de red físicas.

Según varias realizaciones, el gestor de sesiones está configurado para establecer las credenciales de inicio de sesión para cada nivel de acceso de cada IED conectado. Además, el gestor de sesiones puede configurarse para restablecer y actualizar las credenciales de inicio de sesión en un intervalo de tiempo específico. Por ejemplo, las credenciales de inicio de sesión de cada IED conectado pueden restablecerse y actualizarse anualmente para cumplir un reglamento aplicable.

El gestor de sesiones puede configurarse para asignar credenciales de inicio de sesión a cada IED asociado que sean tan robustas como permita cada IED. Por ejemplo, un IED heredado puede permitir solamente una única combinación de nombre de usuario y contraseña con una longitud y un conjunto de caracteres limitados, mientras que un IED más moderno puede permitir múltiples nombres de usuario y/o contraseñas que tienen longitudes y/o conjuntos de caracteres más amplios.

Según varias realizaciones, un operador puede acceder a un IED remoto a través del gestor de sesiones. Puede ser necesario que el operador proporcione un nombre de usuario y una contraseña al gestor de sesiones para obtener acceso a un IED particular. Según varias realizaciones, el operador puede comunicarse con un gestor de sesiones usando un dispositivo de acceso conectado al gestor de sesiones. El gestor de sesiones puede configurarse para mantener y gestionar una pluralidad de credenciales de inicio de sesión asociadas a una pluralidad de operadores, dispositivos de acceso y/o combinaciones de los mismos. Según varias realizaciones, un gestor de sesiones puede requerir que un dispositivo de acceso, o el operador del mismo, proporcione credenciales de inicio de sesión para obtener acceso a los IED conectados en red. Un nivel de autorización puede estar asociado a cada operador, el cual especifica los IED con los que el operador puede comunicarse. Además, algunos operadores pueden tener acceso limitado a algunos IED, mientras que otros pueden tener acceso total.

Un gestor de sesiones puede incluir un filtro de sesiones configurado para suprimir la comunicación entre un operador y un IED conectado en red que no pertenezca al nivel de autorización del operador. Por ejemplo, un filtro de sesiones puede impedir que todos los operadores y/o dispositivos de acceso cambien las credenciales de inicio de sesión de un IED conectado en red. Además, un filtro de sesiones puede configurarse para suprimir los comandos enviados por un operador y/o un dispositivo de acceso a un IED particular que estén en una lista negra de comandos.

Un operador que desea iniciar una sesión de comunicación con un IED particular puede establecer contacto inicialmente con el gestor de sesiones. Después, puede requerirse que el operador y/o el dispositivo de acceso proporcionen credenciales de inicio de sesión, tales como un nombre de usuario y una/varias contraseña(s). El gestor de sesiones puede analizar las credenciales de inicio de sesión proporcionadas para determinar el nivel de autorización del operador y/o del dispositivo de acceso. Después, el operador puede especificar un IED con el que comunicarse. Si el IED especificado pertenece al nivel de autorización de las credenciales de inicio de sesión proporcionadas, el gestor de sesiones puede proporcionar credenciales de inicio de sesión apropiadas al IED especificado para iniciar una sesión de comunicación entre el IED y el gestor de sesiones. Después, el operador y/o el dispositivo de acceso pueden transmitir al gestor de sesiones un comando destinado al IED. El comando puede ser analizado por el filtro de sesiones y, si el comando enviado por el operador satisface los criterios impuestos por el filtro de sesiones, el comando puede reenviarse al IED objetivo. Asimismo, el gestor de sesiones puede reenviar información enviada por el IED objetivo al dispositivo de acceso.

Según determinadas realizaciones, un gestor de sesiones puede mantener registros de eventos de acceso, incluyendo comandos e información enviados entre dispositivos de acceso e IED y las credenciales de inicio de sesión asociadas de los operadores y/o dispositivos de acceso. Tal y como se describe en este documento, un gestor de sesiones permite la aplicación de normas y prácticas de seguridad modernas y coherentes a través de una pluralidad de IED y dispositivos de acceso conectados en red, incluso cuando algunos IED heredados y/o dispositivos de acceso no pueden ajustarse a o proporcionar prácticas de seguridad modernas.

Los operadores y/o los dispositivos de acceso pueden proporcionar credenciales de inicio de sesión a un gestor de sesiones para obtener acceso a cada uno de los IED con los que el operador está autorizado a comunicarse. Esto puede eliminar la necesidad de que un operador tenga que recordar (o posiblemente anotar, lo que crea más problemas de seguridad) las credenciales de inicio de sesión de cada uno de una pluralidad de IED. Además, en algunas industrias, tales como la generación y supervisión de energía eléctrica, el reglamento impone unos requisitos de seguridad mínimos y cambios de contraseña periódicos. El gestor de sesiones descrito en este documento puede automatizar la tarea de actualizar cientos o incluso miles de combinaciones de nombre de usuario/contraseña.

La referencia a lo largo de esta memoria descriptiva a “una realización” significa que una propiedad, estructura o característica particular descrita en relación con la realización está incluida en al menos una realización. Por tanto, la aparición de la expresión “en una realización” en varios puntos de esta memoria descriptiva no hace referencia necesariamente 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 expresiones “conectado(s)/a(s) a” y “en comunicación con” hacen referencia a cualquier forma de interacción entre dos o más componentes, incluidas interacciones mecánicas, eléctricas, magnéticas y electromagnéticas. 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 a un gestor de sesiones de pasarela a través de uno o más IED o dispositivos de conexión en red intermedios. Tales redes pueden modelarse como estructuras en árbol, como es habitual en la técnica.

Como se usa en este documento, el término IED puede referirse a cualquier dispositivo basado en microprocesador que supervise, controle, automatice y/o proteja los equipos supervisados de un sistema. Tales dispositivos pueden incluir, por ejemplo, unidades de terminal remotas, relés diferenciales, relés de distancia, relés direccionales, relés de alimentación, relés de sobrecorriente, controles de regulación de tensión, relés de tensión, relés de fallo de disyuntor, relés de generador, relés de motor, controladores de automatización, controladores de módulo, medidores, controles de reconectador, procesadores de comunicaciones, plataformas informáticas, controladores de lógica programable (PLC), controladores de automatización programable, módulos de entrada y salida, controladores de motor y similares. Los IED pueden estar conectados a una red, y la comunicación en la red puede facilitarse mediante dispositivos de interconexión que incluyen, pero sin limitarse a, multiplexores, encaminadores, concentradores, pasarelas, cortafuegos y conmutadores. Además, los dispositivos de conexión en red y de comunicación pueden estar incorporados en un IED o estar en comunicación con un IED. El término IED puede usarse de manera intercambiable para describir un IED individual o un sistema que comprende múltiples IED.

Como se usa en este documento, el término “credenciales de inicio de sesión” puede referirse a cualquier tipo de procedimiento de autenticación conocido en la técnica por su utilidad. Por ejemplo, las credenciales de inicio de sesión pueden referirse habitualmente a una combinación de nombre de usuario y contraseña codificados en ASCII; por consiguiente, los términos “credenciales de inicio de sesión” y “nombre de usuario y contraseña(s)” pueden intercambiarse en este documento. Sin embargo, el nombre de usuario y la(s) contraseña(s) pueden sustituirse por cualquiera de una gran variedad de protocolos y/o técnicas de autenticación que incluyen protocolos criptográficos de máquinas de autenticación, procedimientos de respuesta a desafíos, pruebas de conocimiento cero, contraseñas de un solo uso sincronizadas en el tiempo, testigos de seguridad, autenticación biométrica, contraseñas gráficas u otras contraseñas no basadas en texto, autenticación por voz y similares.

Alguna de las infraestructuras que pueden usarse con las realizaciones dadas a conocer en este documento ya están disponibles, tales como: ordenadores de propósito general, herramientas y técnicas de programación informática, medios de almacenamiento digitales y redes de comunicaciones. Un ordenador puede incluir un procesador, tal como un microprocesador, un microcontrolador, un sistema de circuitos lógico o similares. El procesador puede incluir un dispositivo de procesamiento de propósito especial, tal como un ASIC, una PAL, una PLA, un PLD, una matriz de puertas de campo programable u otro dispositivo personalizado o programable. El ordenador también puede incluir un dispositivo de almacenamiento legible por ordenador, tal como memoria no volátil, RAM estática, RAM dinámica, ROM, CD-ROM, disco, cinta, memoria magnética, óptica, flash u otro medio de almacenamiento legible por ordenador.

Redes adecuadas para la configuración y/o el uso, como se describe en este documento, incluyen una o más redes de área local, redes de área extensa, redes de área metropolitana y/o redes "Internet" o de protocolo de Internet (IP), tal como la *World Wide Web*, 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 mediante el transporte físico de medios. En particular, una red adecuada puede estar formada por

partes o por la totalidad de dos o más redes, incluidas redes que usan hardware y tecnologías de comunicación de red diferentes. Una red puede incluir líneas terrestres, comunicación inalámbrica y combinaciones de las mismas.

La red puede incluir software de comunicaciones o de conexión en red, tal como software comercializado por Novell, Microsoft, Artisoft y otros vendedores, y puede funcionar usando TCP/IP, SPX, IPX y otros protocolos a través de cables de par trenzado, coaxiales o de fibra óptica, líneas telefónicas, satélites, retransmisores de microondas, líneas de alimentación de CA modulada, transferencia de medios físicos y/u otras "líneas" de transmisión de datos. La red puede abarcar redes más pequeñas y/o puede conectarse a otras redes a través de una pasarela o un mecanismo similar.

Aspectos de determinadas realizaciones descritas en este documento pueden implementarse como módulos o componentes de software. Tal y como se usa en este documento, un módulo o componente de software puede incluir cualquier tipo de instrucción informática o código ejecutable por ordenador ubicado en un medio de almacenamiento legible por ordenador. Un módulo de software puede comprender, por ejemplo, uno o más bloques físicos o lógicos de instrucciones informáticas que pueden organizarse como una rutina, un programa, un objeto, un componente, una estructura de datos, etc., que realiza una o más tareas o que implementa tipos de datos abstractos particulares.

En determinadas realizaciones, un módulo de software particular puede comprender diferentes instrucciones almacenadas en diferentes ubicaciones de un medio de almacenamiento legible por ordenador que implementan conjuntamente la funcionalidad descrita del módulo. De hecho, un módulo puede comprender una única instrucción o muchas instrucciones, y puede estar distribuido a través de varios segmentos de código diferentes, entre diferentes programas y a través de varios medios de almacenamiento legibles por ordenador. Algunas realizaciones pueden llevarse a la práctica en un entorno informático distribuido, donde las tareas se llevan a cabo mediante un dispositivo de procesamiento remoto conectado a través de una red de comunicaciones. En un entorno informático distribuido, módulos de software pueden estar ubicados en medios de almacenamiento legibles por ordenador locales y/o remotos. Además, los datos vinculados a o almacenados conjuntamente en un registro de una base de datos pueden residir en el mismo medio de almacenamiento legible por ordenador o en varios medios de almacenamiento legibles por ordenador, y pueden estar relacionados entre sí en campos de un registro de una base de datos a través de una red.

Los módulos de software descritos en este documento representan de manera tangible programas, funciones y/o instrucciones que pueden ejecutarse por uno o varios ordenadores para llevar a cabo las tareas descritas en este documento. Puede proporcionarse software adecuado, si procede, usando las enseñazas presentadas en este documento y lenguajes y herramientas de programación, tales como XML, Java, Pascal, C++, C, lenguajes de bases de datos, API, SDK, ensamblador, firmware, microcódigo y/u otros lenguajes y herramientas. Además, puede usarse software, firmware y hardware de manera intercambiable para implementar una función dada.

En algunos casos, características, estructuras u operaciones ampliamente conocidas no se muestran o describen en detalle. Además, las características, estructuras u operaciones descritas pueden combinarse de cualquier manera adecuada en una o más realizaciones. También se entenderá fácilmente que los componentes de las realizaciones, descritas e ilustradas de manera genérica en las figuras de este documento, pueden disponerse y diseñarse en una gran variedad de configuraciones diferentes.

Las realizaciones de la divulgación se entenderán mejor haciendo referencia a los dibujos, en los que las partes similares se designan mediante números de referencia similares a lo largo de los dibujos. Los componentes de las realizaciones dadas a conocer, descritas e ilustradas de manera genérica en las figuras de este documento, pueden disponerse y diseñarse en una gran variedad de configuraciones diferentes. Por tanto, la siguiente descripción detallada de las realizaciones de los sistemas y procedimientos de la invención no limita el ámbito de la invención reivindicada, sino que solo representa posibles realizaciones. En otros casos, estructuras, materiales u operaciones ampliamente conocidas no se muestran o se describen en detalle para no oscurecer aspectos de esta invención. Además, no es necesario que las etapas de un procedimiento se ejecuten en un orden específico, o incluso secuencialmente, ni que las etapas se ejecuten una sola vez, a no ser que se indique lo contrario.

La FIG. 1 ilustra una realización de un sistema 100 que incluye un gestor de sesiones 110, una pluralidad de dispositivos electrónicos inteligentes (IED) 161, 162, 163, 164, 165 y 166, y un dispositivo de acceso de operador 150. Como se ilustra, el gestor de sesiones 110 puede incluir múltiples puertos 120, 130 y 140. Según varias realizaciones, los puertos pueden incluir puertos serie 120 y puertos de Ethernet 130 y 140. Según otras realizaciones, un gestor de sesiones 110 puede incluir puertos ópticos, puertos USB, puertos SATA y/o puertos alternativos. Como se ilustra, los IED 161 y 162 están conectados al gestor de sesiones 110 a través de cables de Ethernet 131 y 132. Los IED 165 y 166 están conectados a través de cables de Ethernet y/o cables serie 135

y 136 al IED 162 y, en última instancia, al gestor de sesiones 110 a través del cable de Ethernet 132. Los IED 163 y 164 son IED conectados al gestor de sesiones 110 a través de cables serie 123 y 124. Según varias realizaciones, el gestor de sesiones 110 puede mantener un modelo en forma de árbol de todos los dispositivos conectados en red, de sus tipos, protocolos de comunicación e interconexiones.

Uno o más puertos del gestor de sesiones 110 pueden estar designados como un puerto maestro 140 para la comunicación con un dispositivo de acceso de operador 150, mientras que otros puertos, tales como los puertos serie 120 y/o los puertos de Ethernet 130, pueden estar reservados como puertos esclavos para la conexión de IED en dirección al usuario. Como alternativa, cualquiera de los puertos 120, 130 y 140 pueden configurarse como puertos maestros o puertos esclavos. Según otra realización alternativa, cada uno de los puertos 120, 130 y 140 pueden usarse de manera intercambiable como puertos maestros y esclavos mediante un dispositivo conectado, según sea apropiado durante varias sesiones de comunicación. Es decir, cualquiera de los IED 161 a 166 puede considerarse un dispositivo esclavo durante una sesión de comunicación en la que el dispositivo de acceso 150 está enviando comandos. Sin embargo, el mismo IED puede considerarse un dispositivo maestro durante una sesión de comunicación en la que un operador usa ese mismo IED para acceder a otro IED de la red.

Un operador del dispositivo de acceso 150 puede iniciar una sesión de comunicación con el gestor de sesiones 110 proporcionando credenciales de inicio de sesión únicas. El gestor de sesiones 110 puede analizar las credenciales de inicio de sesión para determinar qué nivel de autorización debe asignarse al operador. El nivel de autorización puede usarse para determinar los IED 161 a 166 a los puede acceder el operador y/o el nivel de acceso que tiene el operador en cada IED.

Durante la sesión de comunicación, el operador puede enviar una solicitud para comunicarse con, por ejemplo, el IED 161. El gestor de sesiones 110 puede iniciar entonces una sesión de comunicación entre el IED 161 y el gestor de sesiones 110. Después, el operador puede transmitir al gestor de sesiones 110 comandos destinados al IED 161. Después, el gestor de sesiones 110 puede reenviar los comandos al IED 161.

Según varias realizaciones, el gestor de sesiones 110 puede configurarse para actuar como un proxy para las comunicaciones con cualquiera de los IED 161 a 166. Por consiguiente, el gestor de sesiones 110 puede mantener dos sesiones de comunicación independientes: una primera sesión de comunicación con el dispositivo de acceso 150 y una segunda sesión de comunicación con uno de los IED 161 a 166. Además, el gestor de sesiones 110 puede incluir un filtro de sesiones configurado para suprimir los comandos transferidos por el dispositivo de acceso 150 a un IED objetivo que no pertenecen al nivel de autorización del operador del dispositivo de acceso 150. Por ejemplo, dado que un gestor de sesiones 110 gestiona de manera independiente las credenciales de inicio de sesión de cada uno de los IED 161 a 166, el filtro de sesiones puede suprimir automáticamente cualquier comando que trate de modificar las credenciales de inicio de sesión de cualquiera de los IED 161 a 166.

Según una realización, el gestor de sesiones 110 puede proporcionar a un operador del dispositivo de acceso 150 una lista de IED que pertenecen al nivel de autorización de las credenciales de inicio de sesión recibidas. Los IED que no pertenezcan al nivel de autorización de las credenciales de inicio de sesión recibidas pueden permanecer ocultos de manera eficaz al operador del dispositivo de acceso 150. Además, el operador del dispositivo de acceso 150 puede desconocer el número de otros IED que están conectados. Por consiguiente, el operador del dispositivo de acceso 150 solo puede tener constancia de los IED de la lista proporcionada por el gestor de sesiones 110. Un filtro de sesiones puede suprimir los comandos transmitidos a los IED listados que no pertenecen al nivel de acceso asociado al nivel de autorización del operador del dispositivo de acceso 150. Además, el filtro de sesiones puede suprimir cualquier intento por parte del operador del dispositivo de acceso 150 de comunicarse con un IED que no esté en la lista de IED proporcionada por el gestor de sesiones 110.

Según varias realizaciones, el gestor de sesiones 110 puede incluir un traductor de protocolos configurado para traducir varios protocolos de comunicaciones y medios físicos de comunicaciones. Por ejemplo, el gestor de sesiones 110 puede permitir la comunicación entre un primer dispositivo conectado al gestor de sesiones 110 mediante Ethernet y un segundo dispositivo conectado al gestor de sesiones 110 mediante una conexión serie. Por ejemplo, el dispositivo de acceso 150 puede comunicarse usando paquetes IP a través de un cable de Ethernet 145, mientras que el IED 164 puede utilizar RS-232 a través de un cable serie 124. El gestor de sesiones 110 puede realizar todas las conversiones implicadas en la comunicación, de manera que las conversiones y/o las traducciones son transparentes al operador que usa el dispositivo de acceso 150.

El sistema de gestión de sesiones de pasarela 100 incluye un único dispositivo de acceso 150; sin embargo, según realizaciones alternativas, un número cualquiera de dispositivos de acceso puede estar en comunicación con el gestor de sesiones 110. Además, según varias realizaciones, un dispositivo de acceso puede ser un IED. Por consiguiente, cualquiera de los IED 161 a 166 puede configurarse para realizar además las funciones de un

dispositivo de acceso. Además, el gestor de sesiones 110 puede incluir cualquier número de puertos cableados y/o inalámbricos, puede utilizar cualquier número de protocolos y/o puede incluir un dispositivo de acceso incorporado. Un ordenador, un servidor u otro dispositivo electrónico, incluido un IED, puede modificarse usando hardware, firmware y/o software para realizar las funciones del gestor de sesiones 110, como se describe en este documento.

La FIG. 2 ilustra una realización de un diagrama de bloques funcional de un sistema informático 200 configurado para funcionar como un gestor de sesiones. El sistema informático 200 puede configurarse para gestionar sesiones de comunicación entre uno o más dispositivos de acceso y uno o más IED. Como se ilustra, el sistema informático 200 puede incluir un procesador 230, una memoria (RAM) 240, una interfaz de red 250 y un medio de almacenamiento legible por ordenador 270, todos conectados a través de un bus de sistema 220.

El procesador 230 puede configurarse para procesar las comunicaciones recibidas a través de la interfaz de red 250 y puertos de entrada/salida 290. El procesador 230 puede funcionar usando cualquier número de velocidades y arquitecturas de procesamiento. El procesador 230 puede configurarse para llevar a cabo varios algoritmos y cálculos descritos en este documento. El procesador 230 puede realizarse como un circuito integrado de propósito general, un circuito integrado de aplicación específica, una matriz de puertas de campo programable y otros dispositivos de lógica programable.

La interfaz de red 250 y los puertos de entrada/salida 290 pueden permitir la comunicación entre el sistema informático 200 y una pluralidad de IED y dispositivos de acceso de operador conectados. La interfaz de red 250 puede realizarse usando varias interfaces para varios tipos de medios físicos (por ejemplo, cable de fibra óptica, de par trenzado o coaxial). Además, la interfaz de red 250 puede configurarse para permitir comunicaciones según varios protocolos y velocidades de comunicación. Según varias realizaciones, múltiples interfaces de red pueden utilizarse para permitir la comunicación con múltiples IED u otros componentes de red.

Los puertos de entrada/salida 290 pueden configurarse para permitir la comunicación entre el sistema informático 200 y una pluralidad de otros dispositivos, tales como IED. Los puertos de entrada/salida 290 pueden realizarse, por ejemplo, como conexiones RS-232, conexiones USB, IEEE 1394 y similares. Una pluralidad de puertos de entrada/salida 290 puede proporcionarse para facilitar la comunicación con una pluralidad de dispositivos.

Según varias realizaciones, el medio de almacenamiento legible por ordenador 270 puede incluir módulos 280 a 292. Según varias realizaciones, cada uno de los módulos 280 a 292 puede implementarse de manera alternativa usando hardware, firmware, software o una combinación de los mismos.

Un módulo de topología 280 puede configurarse para identificar y mantener un registro de las interconexiones entre cada dispositivo conectado en red, incluidos IED, dispositivo(s) de acceso y/u otros elementos de red. Según varias realizaciones, cuando un dispositivo de acceso realiza una solicitud de conexión, el módulo de topología 280 puede configurarse para determinar una trayectoria de comunicación que puede incluir uno o más IED u otros dispositivos de red intermedios, y crear una trayectoria de comunicación que puede utilizarse para las comunicaciones con el IED solicitado. Si múltiples dispositivos de red están incluidos en la trayectoria de comunicación, el sistema informático 200 puede conectarse a cada dispositivo intermedio de manera sucesiva para iniciar una sesión de comunicación con el IED solicitado.

Un módulo de gestión de credenciales de IED 282 puede configurarse para generar y establecer credenciales seguras para uno o más IED conectados al sistema informático 200. Según varias realizaciones, el módulo de gestión de credenciales de IED 282 puede configurarse para establecer credenciales de inicio de sesión aleatorias para cada IED y almacenarlas en una tabla interna. Según algunas realizaciones, si un IED soporta más de un nivel de acceso, el módulo de gestión de credenciales de IED 282 puede establecer credenciales de inicio de sesión para cada nivel de acceso. Además, el módulo de gestión de credenciales de IED 282 puede configurarse para supervisar la antigüedad de las credenciales de inicio de sesión asociadas a cada IED y actualizarlas en un intervalo de tiempo especificado. Por ejemplo, las credenciales de inicio de sesión pueden actualizarse semanal, mensual o anualmente.

Un módulo de gestión de credenciales de dispositivo de acceso 284 puede configurarse para gestionar las credenciales de inicio de sesión de uno o más dispositivos de acceso y/u operadores. Cada dispositivo de acceso y/u operador pueden tener credenciales de inicio de sesión únicas. Según una realización, las credenciales de inicio de sesión comprenden un nombre de usuario y al menos una contraseña. Como alternativa, cada credencial de inicio de sesión puede incluir cualquiera de una gran variedad de mecanismos de autenticación. El módulo de gestión de credenciales de dispositivo de acceso 284 puede configurarse para instar a un operador y/o un dispositivo de acceso a que restablezcan y/o actualicen las credenciales de inicio de sesión únicas en intervalos de tiempo especificados. Como alternativa, el módulo de gestión de credenciales de

dispositivo de acceso 284 puede configurarse para seleccionar y actualizar automáticamente las credenciales de inicio de sesión de dispositivos de acceso y/u operadores.

Un módulo de gestión de control de acceso 286 puede configurase para determinar el nivel de autorización de un dispositivo de acceso y/o de un operador en función de las credenciales de inicio de sesión proporcionadas. Por ejemplo, cuando un operador trata de iniciar una sesión de comunicación con el sistema informático 200 a través de un dispositivo de acceso, puede requerirse que el operador proporcione credenciales de inicio de sesión únicas. El módulo de gestión de control de acceso 286 puede determinar con qué IED conectados en red puede comunicarse el operador. Además, el módulo de gestión de control de acceso 286 puede configurarse para generar una lista negra de comandos que el operador no debe poder transmitir a IED específicos y/o con qué nivel de acceso un operador debería poder comunicarse con un IED. Asimismo, el módulo de gestión de control de acceso 286 puede configurarse para generar una lista blanca de comandos que el operador puede transmitir a IED específicos.

Además, el módulo de gestión de control de acceso 286 puede soportar comandos virtuales definidos por el usuario. Según varias realizaciones, un comando virtual puede incluir un conjunto de comandos personalizados configurados para solicitar datos de un IED y después devolver los datos solicitados en un formato especificado por el usuario. Por ejemplo, un IED solo puede soportar un conjunto específico de comandos básicos. El módulo de gestión de control de acceso 286 puede permitir a un operador definir un comando virtual personalizado como un conjunto de comandos básicos que deben llevarse a cabo en una secuencia predefinida. Un operador puede introducir un comando virtual y el módulo de gestión de control de acceso 286 puede transmitir después a un IED el conjunto predefinido de comandos básicos en la secuencia predefinida. Además, los datos pueden devolverse al operador o al dispositivo de acceso en un formato especificado por el usuario.

Los comandos transmitidos por un operador a un IED objetivo pueden ser suprimidos por un módulo de filtrado de sesiones 288 si los comandos superan el nivel de autorización del operador. Por ejemplo, los comandos transmitidos por un operador destinados a un IED que están en una lista negra generada por el módulo de gestión de control de acceso 286 pueden suprimirse. Como alternativa, los comandos transmitidos por un operador pueden suprimirse si no están en una lista blanca generada por el módulo de gestión de control de acceso 286. Según una realización, los comandos que tratan de modificar las credenciales de inicio de sesión de los IED conectados en red son suprimidos por un filtro de sesiones. El módulo de gestión de control de acceso 286 también puede configurarse para suprimir comandos que puedan dar como resultado la interrupción del servicio eléctrico o daños en un sistema de suministro eléctrico.

Según varias realizaciones, los IED, los equipos de red y/o los dispositivos de acceso pueden comunicarse con el sistema informático 200 usando una gran variedad de protocolos y hardware físico. Un módulo de traducción de protocolos 291 puede configurarse para traducir comandos recibidos en un protocolo con el fin de reenviarlos a un IED en otro protocolo, y viceversa. Por ejemplo, el módulo de traducción de protocolos 291 puede traducir datos TCP/IP transmitidos mediante Ethernet o fibra óptica a RS-232 a través de un cable serie.

Además, un módulo de registro de eventos de acceso 292 puede configurarse para registrar eventos de acceso y credenciales de inicio de sesión asociadas. Según varias realizaciones, los eventos de acceso pueden incluir inicio o finalización de sesión con o sin éxito, comandos transmitidos, comandos recibidos, comandos suprimidos, información recibida, información solicitada, información transmitida y/u otras transmisiones de datos entre un dispositivo de acceso, un gestor de sesiones y/o un IED. Según varias realizaciones, el tipo y la cantidad de información registrada pueden configurarse por un operador para ajustarse a una necesidad particular.

La FIG. 3 ilustra una realización de un procedimiento 300 para establecer y mantener credenciales de inicio de sesión seguras para cada uno de una pluralidad de IED. Cada uno de la pluralidad de IED se conecta a un gestor de sesiones, en 310. Según varias realizaciones, los IED pueden conectarse a un gestor de sesiones usando cualquiera de una gran variedad de conexiones físicas o usando una conexión inalámbrica. El gestor de sesiones puede incluir un gestor de conexiones que determina el modelo y el protocolo para la comunicación con cada uno de los IED conectados, en 320. Por ejemplo, puede mantenerse un modelo en árbol que represente la topología de una pluralidad de IED conectados en red.

Según varias realizaciones, el gestor de sesiones puede ser capaz de usar y traducir una gran variedad de protocolos de comunicación, incluidos el protocolo RS-232 y protocolos de datos basados en paquetes. El gestor de conexiones también puede determinar una trayectoria de comunicación hacia cada IED conectado, en 330.

Un gestor de credenciales puede establecer credenciales de inicio de sesión seguras para varios niveles de autorización de cada IED conectado, en 340. Según varias realizaciones, cada IED puede requerir que se proporcionen credenciales de inicio de sesión, tales como un nombre de usuario y una contraseña, para acceder

al IED. Por ejemplo, un IED puede configurarse para supervisar partes de un sistema de distribución de energía y controlar automáticamente un disyuntor. El IED puede requerir que un operador proporcione un nombre de usuario y una contraseña para impedir un acceso no autorizado.

El gestor de credenciales también puede supervisar la antigüedad de las credenciales de inicio de sesión de cada uno de la pluralidad de IED y modificar las credenciales de inicio de sesión en un intervalo de tiempo especificado, en 350. Por ejemplo, reglamentos federales pueden obligar que las credenciales de inicio de sesión del IED se restablezcan anualmente. Al restablecerse automáticamente las credenciales de inicio de sesión de todos los IED conectados en red en un intervalo de tiempo especificado, el gestor de sesiones puede automatizar lo que de otro modo sería un proceso manual complejo y lento.

Según varias realizaciones, el gestor de credenciales puede generar credenciales de inicio de sesión aleatorias para cada IED conectado y almacenar las credenciales en una base de datos interna. Los IED heredados no pueden ofrecer los mismos controles de seguridad que los IED modernos. Por ejemplo, un IED heredado solo puede permitir una única credencial de inicio de sesión, tal como una única combinación de nombre de usuario/contraseña que concede un acceso no restringido al IED. Por el contrario, los IED más modernos pueden permitir múltiples combinaciones de nombre de usuario/contraseñas que tienen niveles de acceso configurables. Además, la longitud y el conjunto de caracteres disponibles para crear credenciales de inicio de sesión pueden variar considerablemente de un IED a otro. El gestor de credenciales puede configurarse para interactuar de manera apropiada con cada tipo de IED, independientemente de las normas de seguridad usadas por el IED particular.

La FIG. 4 ilustra una realización de un procedimiento 400 para iniciar una sesión de comunicación entre un dispositivo de acceso y un gestor de sesiones. En 410, un dispositivo de acceso inicia una sesión de comunicación con un gestor de sesiones. Un gestor de control de acceso incorporado en el gestor de sesiones solicita que el dispositivo de acceso proporcione credenciales de inicio de sesión, en 420. El dispositivo de acceso y/o un operador del mismo proporcionan las credenciales de inicio de sesión, en 430. Según varias realizaciones, el gestor de control de acceso puede solicitar las credenciales de inicio de sesión para la máquina que está usándose como dispositivo de acceso, las credenciales de inicio de sesión del operador del dispositivo de acceso o ambas. Por tanto, según algunas realizaciones, un gestor de sesiones solo puede ser accesible para dispositivos de acceso conocidos por el gestor de sesiones. Como alternativa, el gestor de sesiones puede permitir el acceso siempre que el operador del dispositivo de acceso pueda proporcionar credenciales de inicio de sesión autorizadas.

Después, el gestor de control de acceso puede determinar el nivel de autorización del dispositivo de acceso para la sesión de comunicación iniciada basándose en las credenciales de inicio de sesión recibidas, en 440. Es decir, el gestor de sesiones puede proporcionar acceso a los IED conectados en red, basándose en las credenciales de inicio de sesión del dispositivo de acceso y/o del operador. Por ejemplo, un operador dado puede tener varios niveles de acceso a cada uno de los IED conectados en red. El operador puede tener acceso total a algunos IED y acceso limitado a algunos IED, y puede impedirse completamente que interactúe con otros IED.

El gestor de sesiones puede reenviar comunicaciones entre el dispositivo de acceso y un IED objetivo que pertenezca al nivel de autorización determinado, en 450. Según varias realizaciones, el gestor de sesiones no facilita una sesión de comunicación entre el dispositivo de acceso y un IED. En cambio, el gestor de sesiones puede mantener una primera sesión de comunicación con el dispositivo de acceso e iniciar una segunda sesión de comunicación con un IED objetivo. Por consiguiente, el gestor de sesiones reenvía comandos transmitidos por el dispositivo de acceso en la primera sesión de comunicación a un IED objetivo en la segunda sesión de comunicación, siempre que el IED objetivo pertenezca al nivel de autorización determinado.

Según varias realizaciones, un gestor de sesiones puede mantener una primera sesión de comunicación con un dispositivo de acceso y múltiples sesiones de comunicación con varios IED objetivo. Además, un gestor de sesiones puede facilitar comunicaciones entre múltiples dispositivos de acceso y múltiples IED simultáneamente. Es decir, múltiples dispositivos de acceso pueden utilizar la funcionalidad del gestor de sesiones sin que tengan constancia necesariamente unos de otros. Por ejemplo, dos dispositivos de acceso pueden comunicarse simultáneamente con un único IED o con dos IED diferentes. Según varias realizaciones, un acceso concurrente o simultáneo se proporciona a través de un único puerto de comunicación. Por ejemplo, un único puerto de Ethernet puede soportar comunicaciones entre múltiples dispositivos de acceso y el gestor de sesiones y/o un IED.

La FIG. 5 ilustra una realización de un procedimiento 500 para iniciar una primera sesión de comunicación entre un dispositivo de acceso y un gestor de sesiones, y una segunda sesión de comunicación controlada por acceso entre un IED y el gestor de sesiones. En 510, un dispositivo de acceso proporciona credenciales de inicio de

sesión a un gestor de sesiones para iniciar una sesión de comunicación. El gestor de control de acceso del gestor de sesiones determina el nivel de autorización del dispositivo de acceso basándose en las credenciales recibidas, en 520. El nivel de autorización concedido puede depender de las credenciales de inicio de sesión de la máquina física usada como dispositivo de acceso, de las credenciales de inicio de sesión de un operador del dispositivo de acceso, o de una combinación de las mismas.

Según varias realizaciones, un gestor de sesiones proporciona varios niveles de acceso a cada IED conectado, dependiendo del nivel de autorización del dispositivo de acceso y/o del operador. Según algunas realizaciones, un gestor de sesiones puede utilizar los niveles de acceso diferenciados e incorporados de los IED modernos para proporcionar un acceso limitado por dispositivo de acceso a algunos IED. Además, un gestor de sesiones puede incluir un filtro de sesiones configurado para suprimir comandos y comunicaciones entre un dispositivo de acceso y un IED que no pertenezcan al nivel de autorización del dispositivo de acceso y/o del operador del mismo.
Por ejemplo, puede ser deseable otorgar a un operador particular privilegios administrativos para algunos IED, privilegios de un operador de alto nivel para otros IED y privilegios de un operador de bajo nivel para otros IED. Si el operador desea comunicarse con un IED particular, el gestor de sesiones puede iniciar una sesión de comunicación con el IED que corresponda al nivel de autorización del operador. Un modelo de este tipo funciona siempre que el IED soporte diferentes niveles de acceso. En los IED heredados que no soportan diferentes niveles de acceso, un filtro de sesiones incorporado en el gestor de sesiones puede suprimir comunicaciones que no pertenezcan al nivel de autorización del dispositivo de acceso. Por consiguiente, un gestor de sesiones puede proporcionar de manera eficaz IED heredados con diferentes niveles de acceso mediante el uso de un filtro de sesiones.

En 520 puede determinarse el nivel de autorización y, en 530, el dispositivo de acceso puede solicitar que el gestor de sesiones reenvíe comandos a un IED conectado. En 540, un filtro de sesiones puede determinar si los comandos pertenecen al nivel de autorización del dispositivo de acceso para el IED objetivo. Si la solicitud pertenece al nivel de autorización del dispositivo de acceso, en 550, el gestor de sesiones puede reenviar el comando al IED objetivo, en 570. Sin embargo, si la solicitud no pertenece al nivel de autorización del dispositivo de acceso, en 550, el gestor de sesiones puede rechazar la solicitud de reenvío del comando, en 560.

Según varias realizaciones, un gestor de sesiones puede incluir un subsistema de registro. Por consiguiente, el subsistema de registro puede registrar eventos de acceso y credenciales de inicio de sesión asociadas, en 580. Según varias realizaciones, los eventos de acceso registrados pueden incluir cualquier inicio o finalización de sesión con o sin éxito, comandos transmitidos, comandos recibidos, comandos suprimidos, información recibida, información solicitada, información transmitida y/u otras transmisiones de datos entre un dispositivo de acceso, un gestor de sesiones y/o un IED. Según varias realizaciones, el tipo y la cantidad de información registrada pueden adaptarse para ajustarse a una necesidad particular.

Las FIG. 6A y 6B ilustran realizaciones de tablas representativas de la gestión de credenciales de un IED heredado 600 y de un IED moderno 650 más seguro. Como se ha descrito anteriormente, un IED moderno 650 puede permitir diferentes niveles de acceso en función de las credenciales de inicio de sesión, mientras que un IED heredado 600 no puede proporcionar acceso alguno o puede proporcionar un acceso ilimitado. Como se ilustra en la FIG. 6A, un IED heredado puede proporcionar un acceso total a todos los sistemas y archivos tras la autenticación usando un nombre de usuario y una contraseña. Además, la longitud y el conjunto de caracteres usados para crear el nombre de usuario y la contraseña pueden ser limitados.

Por el contrario, un IED mejorado 650 puede permitir múltiples combinaciones de nombre de usuario y contraseña, cada una con diferentes niveles de acceso. Como se ilustra en la FIG. 6B, los posibles niveles de acceso pueden incluir variaciones en la capacidad del operador de leer y escribir en los sistemas y archivos presentes en el IED. Las FIG. 6A y 6B son simplemente ejemplos de posibles combinaciones de nombre de usuario, contraseña y nivel de acceso. Según varias realizaciones, los IED pueden utilizar paradigmas alternativos de credenciales de inicio de sesión y pueden incluir más niveles de acceso definidos.

La FIG. 7 ilustra una tabla representativa 700 para gestionar las contraseñas y las conexiones de una pluralidad de IED en una realización de un gestor de sesiones. Como se ha descrito anteriormente, un gestor de sesiones puede gestionar las credenciales de inicio de sesión, el tipo, la conexión y los niveles disponibles de acceso para cada uno de una pluralidad de IED conectados. El gestor de sesiones puede generar y actualizar automáticamente las credenciales de inicio de sesión para múltiples niveles de acceso (cuando sea posible) de cada IED conectado. Como se ilustra en la primera columna de la tabla 700, los IED 1 a N pueden conectarse al gestor de sesiones. Los IED 1 y N pueden ser dispositivos heredados (segunda columna) conectados a través de cables serie (tercera columna). Estos IED heredados solo pueden soportar un único nivel de acceso equivalente al de un administrador (cuarta columna). Por consiguiente, un nombre de usuario (quinta columna) y una

contraseña (sexta columna) pueden generarse, almacenarse y actualizarse periódicamente para cada IED.

Los IED 2 y 3 (primera columna) pueden ser IED mejorados o modernos (segunda columna) conectados al gestor de sesiones a través de Ethernet (tercera columna). Como se ilustra, el IED 2 puede soportar cinco niveles de acceso (cuarta columna) predefinidos como administrador, nivel alto, nivel medio, nivel bajo y personalizado. El IED 3 también puede soportar numerosos niveles de acceso (cuata columna), cada uno de los cuales puede personalizarse. El gestor de sesiones puede generar, almacenar y actualizar periódicamente nombres de usuario y contraseñas para cada nivel de acceso de IED 2 y para cualquier número de niveles de acceso de IED 3.

La FIG. 8 ilustra una tabla representativa 800 para gestionar las credenciales de inicio de sesión y el nivel de autorización asociado concedido a cada uno de una pluralidad de operadores mediante un gestor de sesiones. La primera y la segunda columna de la tabla 800 representan el dispositivo de acceso y/o las credenciales de inicio de sesión del operador. Según varias realizaciones, cada operador puede tener un nombre de usuario único, mostrados en la primera columna de la tabla 800 como Operador 1 a Operador N, y una contraseña única, mostradas en la segunda columna de la tabla 800. Las credenciales de inicio de sesión de un dispositivo de acceso y/o de un operador pueden comprender cualquier número de esquemas de autenticación posibles, y no están limitadas a combinaciones de nombre de usuario/contraseña.

Un nivel de autorización para cada IED conectado está asociado a cada credencial de inicio de sesión del operador. Usando la primera fila como ejemplo, el nivel de autorización asociado a las credenciales de inicio de sesión “Operador 1” y “Contraseña 1” proporciona acceso de administrador al IED 1, acceso de nivel medio al IED 2, acceso de nivel bajo al IED 3 y acceso administrativo al IED N. Como otro ejemplo, el operador asociado al nombre de usuario “Operador 3” y a la contraseña “Contraseña 3” solo tiene acceso de nivel bajo tanto al IED 2 como al IED 3.

Como se ha descrito anteriormente, los IED heredados no pueden proporcionar diferentes niveles de acceso. Por consiguiente, a todos los operadores de la FIG. 8 se les concede acceso de administrador tanto al IED 1 como al IED 2 ya que la otra alternativa posible es no concederles acceso.

La FIG. 9 ilustra una tabla representativa 900 para gestionar credenciales de inicio de sesión y niveles de autorización asociados concedidos a cada uno de una pluralidad de dispositivos de acceso mediante un gestor de sesiones que incluye un filtro de sesiones. Según varias realizaciones y como se ha descrito anteriormente, un filtro de sesiones puede proporcionar de manera eficaz a los IED heredados diferentes niveles de acceso. Por ejemplo, el IED 1 y el IED N se muestran como dispositivos heredados (tercera columna). Por consiguiente, el único nivel de acceso disponible para el IED 1 y el IED N es o bien administrador o ninguno (véase la cuarta columna de las FIG. 7 y 9). Nuevamente, usando un filtro de sesiones para suprimir comandos específicos, puede parecer que un IED heredado soporta diferentes niveles de acceso.

Por ejemplo, el operador de la segunda fila asociado al nombre de usuario “Operador 2” (primera columna) y a la contraseña “Contraseña 2” (segunda columna) tiene acceso de administrador al IED 1 y al IED 2 (cuarta columna). Sin embargo, el filtro de sesiones suprime comandos de manera que el operador es en términos prácticos un operador de nivel alto del IED 1 y un operador de nivel medio del IED N. Según varias realizaciones, un filtro de sesiones puede configurarse para suprimir todos los comandos relacionados con modificaciones de las credenciales de inicio de sesión de los propios IED.

La descripción anterior proporciona numerosos detalles específicos para ofrecer un entendimiento minucioso de las realizaciones descritas en este documento. Sin embargo, los expertos en la técnica reconocerán que uno o más de los detalles específicos pueden omitirse, modificarse y/o sustituirse por un proceso o sistema similar.

REIVINDICACIONES

1.- Un procedimiento de gestión de credenciales de inicio de sesión y sesiones de comunicación de una pluralidad de dispositivos electrónicos inteligentes (IED), que comprende:

conectar cada uno de una pluralidad de IED a un gestor de sesiones;

generar una pluralidad de credenciales de inicio de sesión para cada uno de la pluralidad de IED usando el gestor de sesiones;

almacenar la pluralidad de credenciales de inicio de sesión en una base de datos accesible mediante el gestor de sesiones;

supervisar la antigüedad de la pluralidad de credenciales de inicio de sesión de cada IED conectado usando el gestor de sesiones; y

actualizar la pluralidad de credenciales de inicio de sesión de cada IED conectado en un intervalo de tiempo especificado usando el gestor de sesiones.

2.- El procedimiento según la reivindicación 1, en el que cada una de la pluralidad de credenciales de inicio de sesión comprende un nombre de usuario y una contraseña.

3.- El procedimiento según la reivindicación 1, en el que generar la pluralidad de credenciales de inicio de sesión para cada uno de la pluralidad de IED comprende generar credenciales de inicio de sesión únicas para una pluralidad de niveles de acceso de al menos uno de la pluralidad de IED.

4.- El procedimiento según la reivindicación 1, en el que conectar cada uno de la pluralidad de IED comprende conectar cada IED al gestor de sesiones usando al menos uno de entre un cable de Ethernet, un cable serie, un cable coaxial, un cable óptico y una conexión inalámbrica.

5.- El procedimiento según la reivindicación 1, que comprende además:

asociar una pluralidad de credenciales de inicio de sesión de operador a una pluralidad de operadores, teniendo cada una de la pluralidad de credenciales de inicio de sesión de operador un nivel de autorización que especifica el nivel de acceso del operador asociado.

6.- Un procedimiento según la reivindicación 5, que comprende además:

recibir una de la pluralidad de credenciales de inicio de sesión de operador mediante el gestor de sesiones;

determinar el nivel de autorización de las credenciales de inicio de sesión de operador recibidas usando el gestor de sesiones; y

crear una primera sesión de comunicación entre el gestor de sesiones y un dispositivo de acceso de operador.

7.- El procedimiento según la reivindicación 6, que comprende además:

recibir una solicitud desde el dispositivo de acceso de operador para comunicarse con un IED conectado que pertenece al nivel de autorización de las credenciales de inicio de sesión de operador recibidas;

iniciar por medio del gestor de sesiones una segunda sesión de comunicación entre el gestor de sesiones y el IED solicitado mediante el gestor de sesiones proporcionando credenciales de inicio de sesión del IED solicitado; y

retransmitir de manera selectiva por medio del gestor de sesiones las comunicaciones recibidas desde el dispositivo de acceso de operador en la primera sesión de comunicación al IED solicitado en la segunda sesión de comunicación.

8.- El procedimiento según la reivindicación 6, que comprende además:

suprimir las comunicaciones entre el operador y el IED que superen el nivel de autorización del operador.

9.- El procedimiento según la reivindicación 6, que comprende además registrar eventos de acceso asociados a las credenciales de inicio de sesión del operador usando el gestor de sesiones.

10.- El procedimiento según la reivindicación 6, que comprende además que el gestor de sesiones:

proporcione al dispositivo de acceso de operador una lista de IED conectados;

reciba una solicitud desde el dispositivo de acceso de operador para comunicarse con uno de los IED listados que pertenecen al nivel de autorización de las credenciales de inicio de sesión de operador recibidas;

inicie una segunda sesión de comunicación entre el gestor de sesiones y el IED solicitado mediante el gestor de sesiones proporcionando credenciales de inicio de sesión del IED solicitado; y

retransmita de manera selectiva las comunicaciones recibidas desde el dispositivo de acceso de operador en la primera sesión de comunicación al IED solicitado en la segunda sesión de comunicación.

11.- El procedimiento según la reivindicación 10, en el que la lista comprende solamente los IED que pertenecen al nivel de autorización de las credenciales de inicio de sesión de operador recibidas.

12.- El procedimiento según la reivindicación 1, que comprende además traducir un primer protocolo de datos en un segundo protocolo de datos.

13.- Un gestor de sesiones para gestionar credenciales de inicio de sesión y sesiones de comunicación de una pluralidad de dispositivos electrónicos inteligentes (IED), que comprende:

un bus;

un procesador en comunicación con el bus;

una pluralidad de puertos en comunicación con el bus y configurados para permitir la conexión de una pluralidad de IED con el gestor de sesiones; y

un medio de almacenamiento legible por ordenador en comunicación con el bus, comprendiendo el medio de almacenamiento legible por ordenador:

un módulo de gestión de credenciales de IED que puede ejecutarse en el procesador y que está configurado para:

generar credenciales de inicio de sesión para cada IED conectado;

almacenar las credenciales de inicio de sesión de los IED conectados en una base de datos accesible al gestor de sesiones;

supervisar la antigüedad de las credenciales de inicio de sesión de cada IED conectado; y

actualizar las credenciales de inicio de sesión de cada IED conectado en un intervalo de tiempo especificado.

14.- El gestor de sesiones según la reivindicación 13, en el que cada una de la pluralidad de credenciales de inicio de sesión comprende un nombre de usuario y una contraseña.

15.- El gestor de sesiones según la reivindicación 13, en el que el módulo de gestión de credenciales de IED está configurado para generar credenciales de inicio de sesión para una pluralidad de niveles de acceso de al menos uno de la pluralidad de IED.

16.- El gestor de sesiones según la reivindicación 13, en el que la pluralidad de puertos comprende al menos uno de entre un puerto de Ethernet, un puerto serie, un puerto coaxial, un puerto óptico y un puerto inalámbrico.

17.- El gestor de sesiones según la reivindicación 13, en el que el medio de almacenamiento legible por ordenador comprende además:

un módulo de gestión de credenciales de dispositivo de acceso que puede ejecutarse en el procesador y que

está configurado para asociar una pluralidad de credenciales de inicio de sesión de operador a una pluralidad de operadores, teniendo cada una de la pluralidad de credenciales de inicio de sesión de operador un nivel de autorización que especifica el nivel de acceso de al menos uno de la pluralidad de IED.

18.- El gestor de sesiones según la reivindicación 17, en el que el medio de almacenamiento legible por ordenador comprende además:

un módulo de gestión de control de acceso que puede ejecutarse en el procesador y que está configurado para:

recibir una de la pluralidad de credenciales de inicio de sesión de operador desde un dispositivo de acceso de operador;

determinar el nivel de autorización de las credenciales de inicio de sesión de operador; y

crear una primera sesión de comunicación entre el gestor de sesiones y el dispositivo de acceso de operador.

19.- El gestor de sesiones según la reivindicación 18, en el que el módulo de gestión de control de acceso está configurado además para:

recibir una solicitud desde el dispositivo de acceso de operador para comunicarse con un IED que pertenece al nivel de autorización de las credenciales de inicio de sesión de operador recibidas;

iniciar una segunda sesión de comunicación entre el gestor de sesiones y el IED solicitado mediante el gestor de sesiones proporcionando las credenciales de inicio de sesión del IED solicitado; y

retransmitir las comunicaciones recibidas desde el dispositivo de acceso de operador en la primera sesión de comunicación al IED solicitado en la segunda sesión de comunicación.

20.- El gestor de sesiones según la reivindicación 18, en el que el medio de almacenamiento legible por ordenador comprende además:

un módulo de filtrado de sesiones que puede ejecutarse en el procesador y que está configurado para suprimir las comunicaciones que superen el nivel de autorización determinado de las credenciales de inicio de sesión de operador proporcionadas.

21.- El gestor de sesiones según la reivindicación 17, en el que el medio de almacenamiento legible por ordenador comprende además:

un módulo de registro de eventos de acceso que puede ejecutarse en el procesador y que está configurado para registrar eventos de acceso asociados a las credenciales de inicio de sesión de operador proporcionadas.

22.- El gestor de sesiones según la reivindicación 18, en el que el módulo de gestión de control de acceso está configurado además para:

proporcionar al dispositivo de acceso de operador una lista de IED;

recibir una solicitud desde el dispositivo de acceso de operador para comunicarse con uno de los IED listados que pertenecen al nivel de autorización de las credenciales de inicio de sesión de operador recibidas;

iniciar una segunda sesión de comunicación entre el gestor de sesiones y el IED solicitado mediante el gestor de sesiones proporcionando las credenciales de inicio de sesión del IED solicitado;

retransmitir las comunicaciones recibidas desde el dispositivo de acceso de operador en la primera sesión de comunicación al IED solicitado en la segunda sesión de comunicación.

23.- El gestor de sesiones según la reivindicación 22, en el que la lista comprende solamente los IED que pertenecen al nivel de autorización de las credenciales de inicio de sesión de operador recibidas.

24.- El gestor de sesiones según la reivindicación 13, en el que el medio de almacenamiento legible por ordenador comprende además:

un módulo de traducción de protocolos que puede ejecutarse en el procesador y que está configurado para traducir un primer protocolo de datos en un segundo protocolo de datos.

25.- Un gestor de sesiones para gestionar las credenciales de inicio de sesión y las sesiones de comunicación de una pluralidad de dispositivos electrónicos inteligentes (IED), que comprende:

conectar cada uno de una pluralidad de IED a un gestor de sesiones;

medios para generar una pluralidad de credenciales de inicio de sesión para cada uno de los IED conectados usando el gestor de sesiones;

medios para almacenar la pluralidad de credenciales de inicio de sesión en una base de datos accesible mediante el gestor de sesiones;

medios para recibir una credencial de inicio de sesión de operador desde un dispositivo de acceso de operador mediante el gestor de sesiones;

medios para determinar el nivel de autorización de la credencial de inicio de sesión de operador recibida usando el gestor de sesiones;

medios para crear una primera sesión de comunicación entre el gestor de sesiones y un dispositivo de acceso de operador;

medios para recibir una solicitud desde el dispositivo de acceso de operador para comunicarse con un IED conectado que pertenece al nivel de autorización de la credencial de inicio de sesión de operador recibida;

medios para iniciar una segunda sesión de comunicación entre el gestor de sesiones y el IED solicitado mediante el gestor de sesiones proporcionando la credencial de inicio de sesión del IED solicitado; y

medios para suprimir las comunicaciones entre el dispositivo de acceso de operador y el IED solicitado que superen el nivel de autorización del operador.

FIG. 1

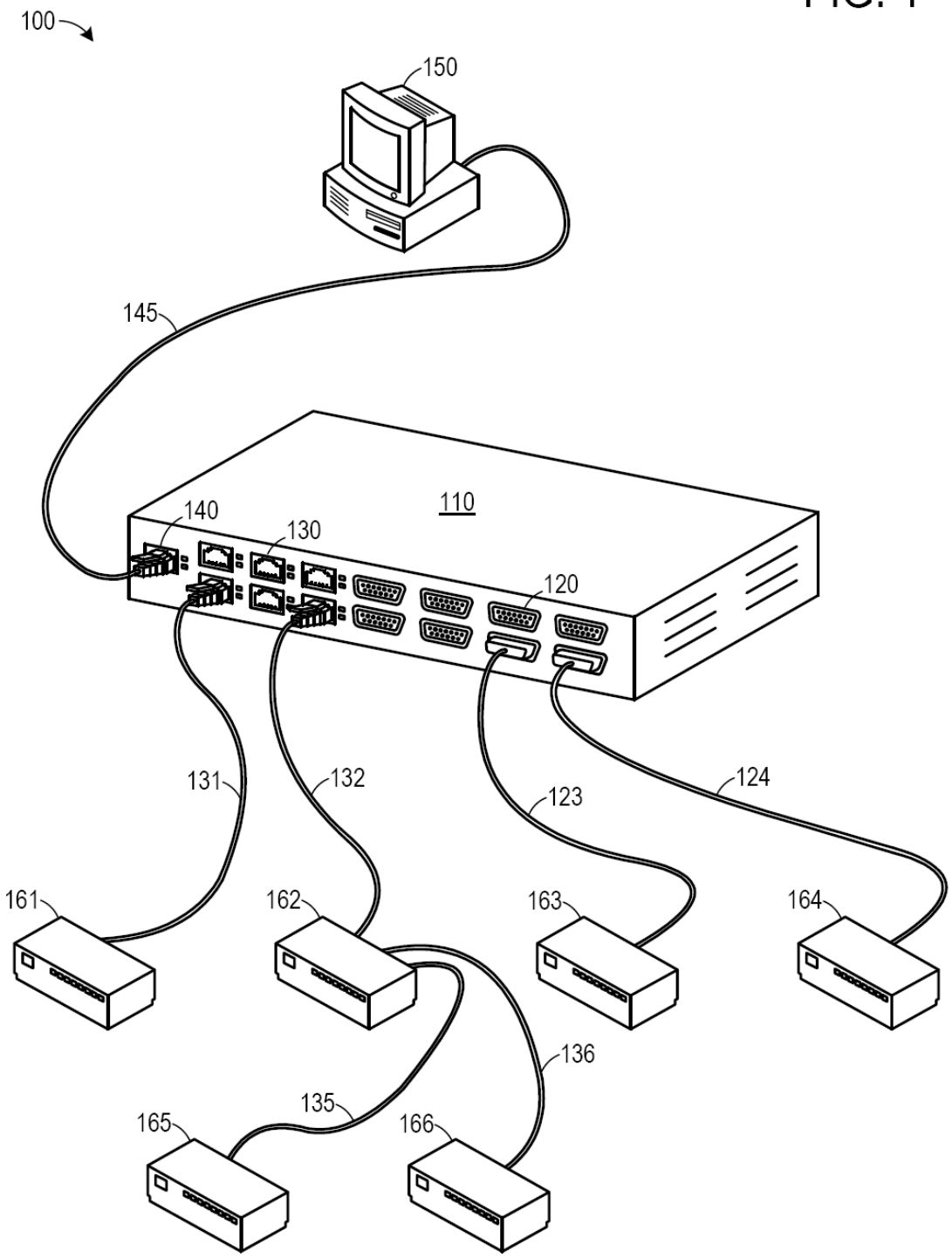

100
150
145
110
140
130
120
131
132
123
124
161
162
163
164
136
135
165
166

FIG. 2

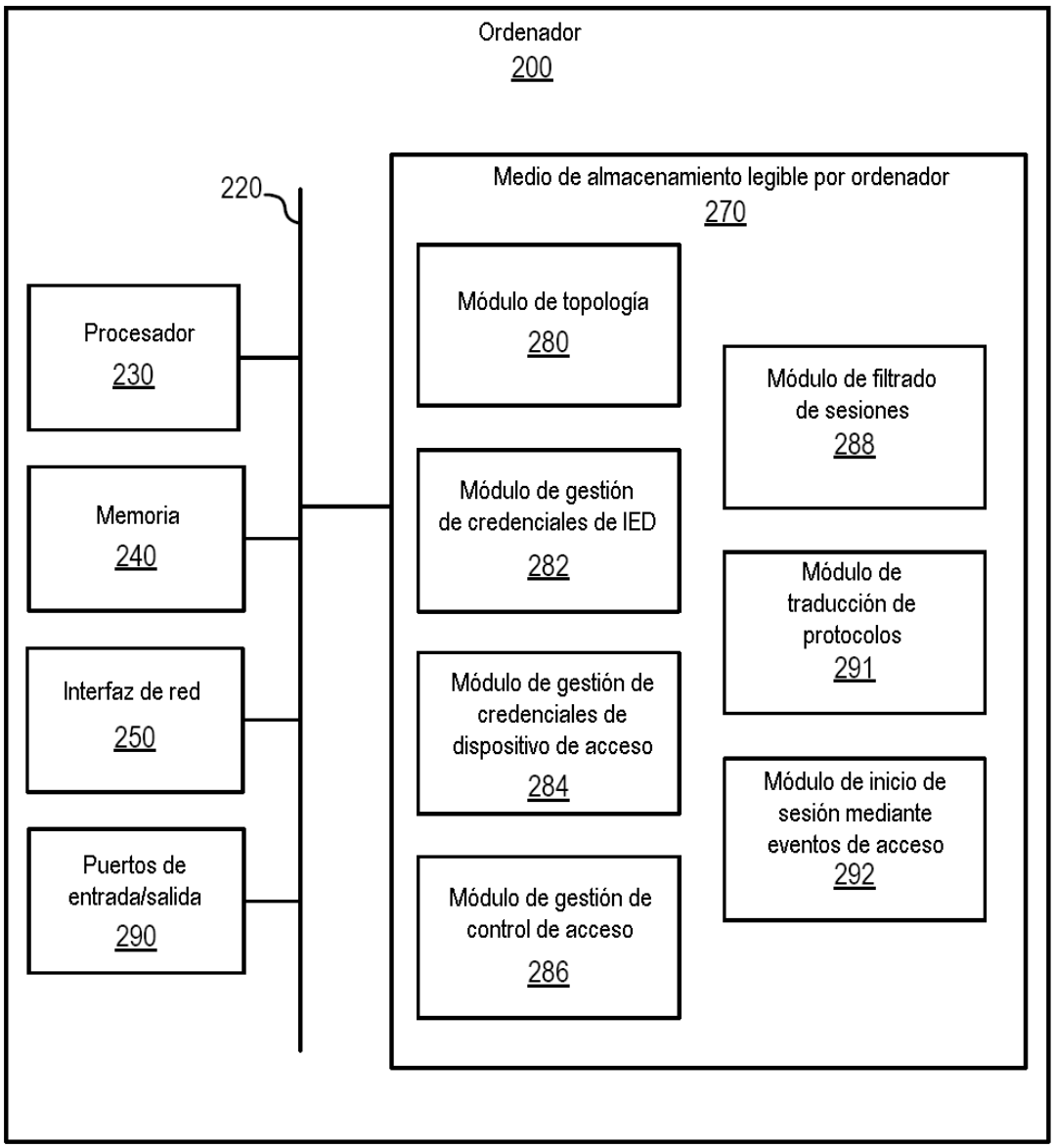

Ordenador
200
220
Procesador
230
Memoria
240
Interfaz de red
250
Puertos de entrada/salida
290
Medio de almacenamiento legible por ordenador
270
Módulo de topología
280
Módulo de gestión de credenciales de IED
282
Módulo de gestión de credenciales de dispositivo de acceso
284
Módulo de gestión de control de acceso
286
Módulo de filtrado de sesiones
288
Módulo de traducción de protocolos
291
Módulo de inicio de sesión mediante eventos de acceso
292

FIG. 3

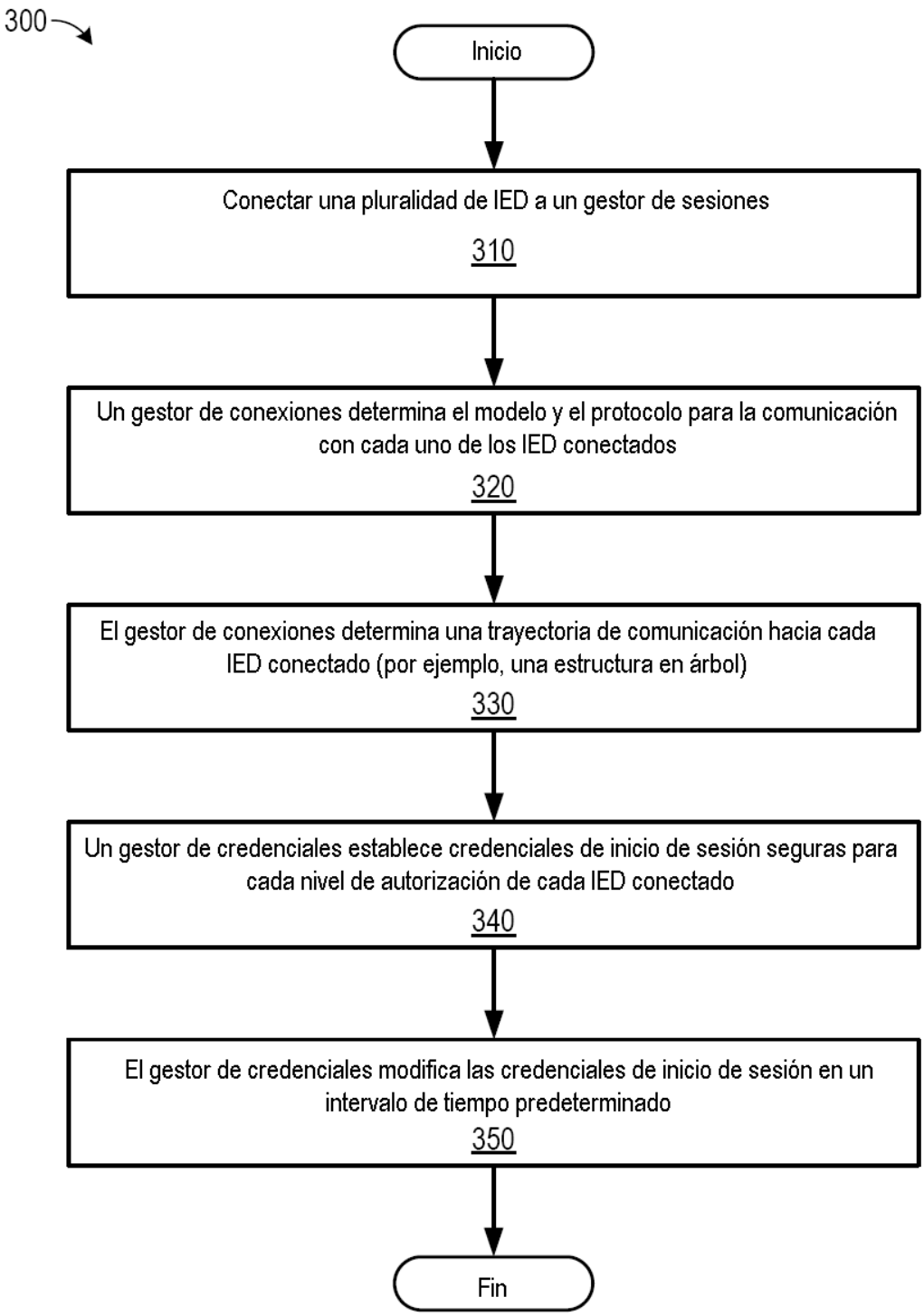

300
Inicio
Conectar una pluralidad de IED a un gestor de sesiones
310
Un gestor de conexiones determina el modelo y el protocolo para la comunicación con cada uno de los IED conectados
320
El gestor de conexiones determina una trayectoria de comunicación hacia cada IED conectado (por ejemplo, una estructura en árbol)
330
Un gestor de credenciales establece credenciales de inicio de sesión seguras para cada nivel de autorización de cada IED conectado
340
El gestor de credenciales modifica las credenciales de inicio de sesión en un intervalo de tiempo predeterminado
350
Fin

FIG. 4

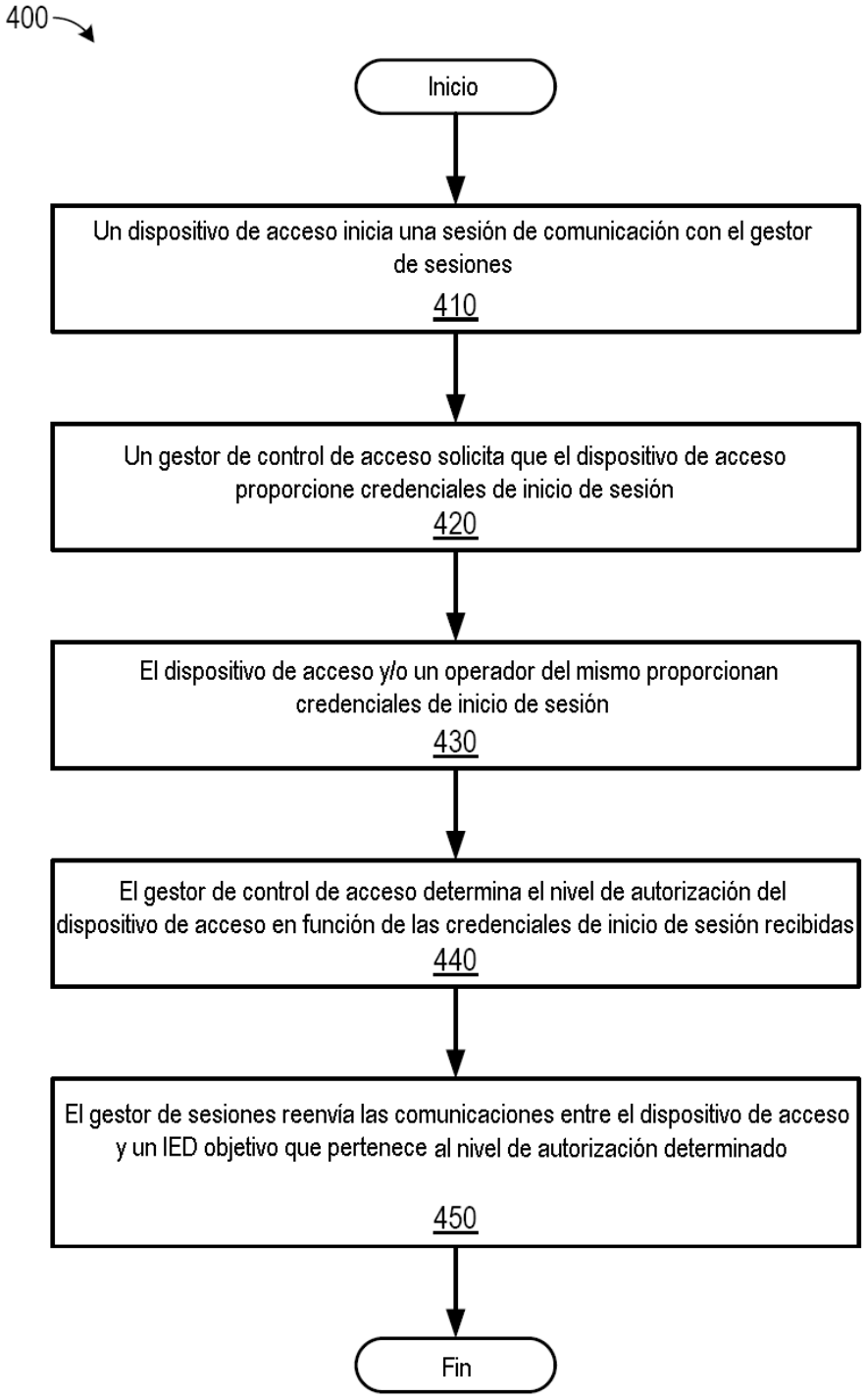
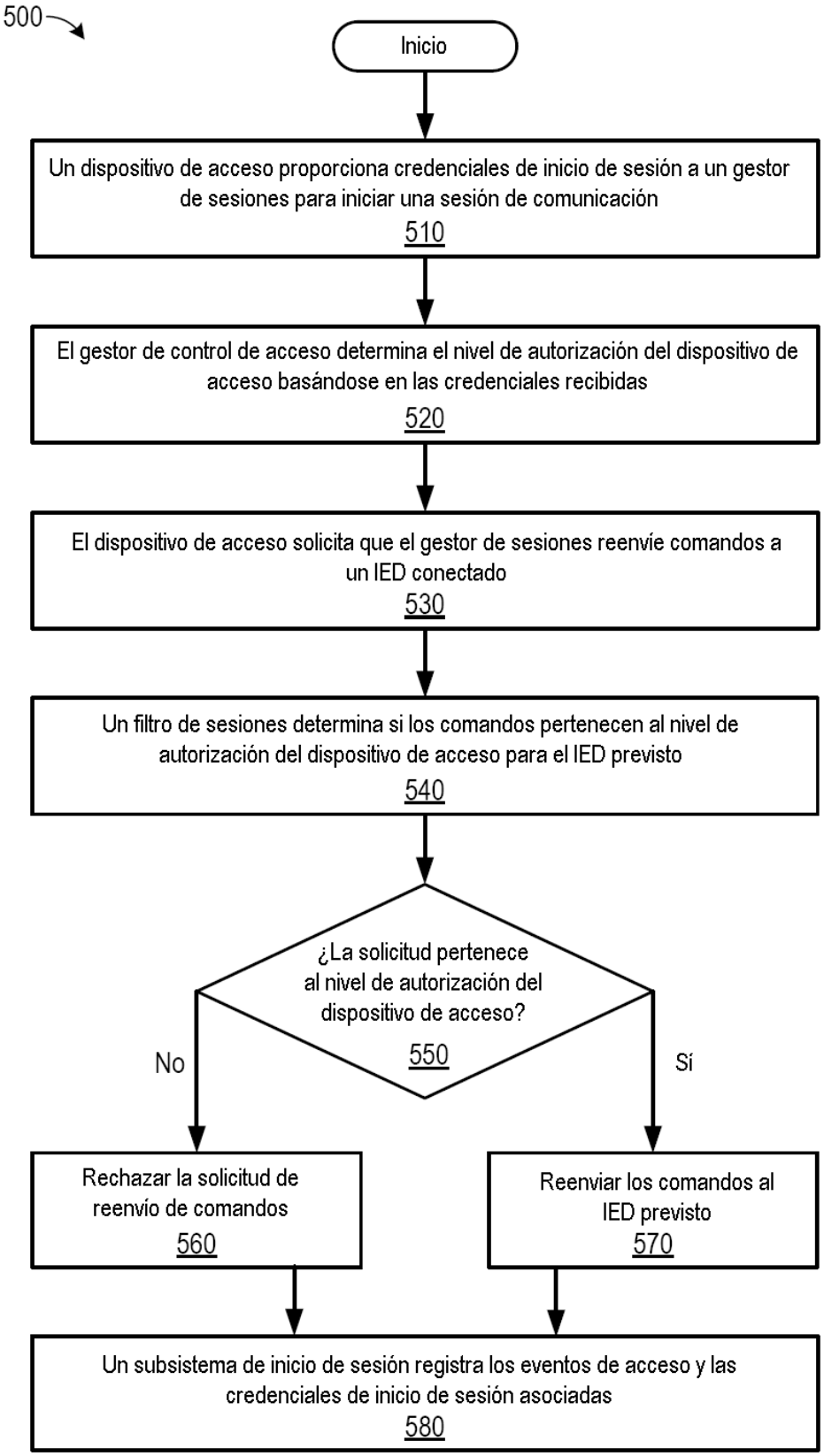

400
Inicio
Un dispositivo de acceso inicia una sesión de comunicación con el gestor de sesiones
410
Un gestor de control de acceso solicita que el dispositivo de acceso proporcione credenciales de inicio de sesión
420
El dispositivo de acceso y/o un operador del mismo proporcionan credenciales de inicio de sesión
430
El gestor de control de acceso determina el nivel de autorización del dispositivo de acceso en función de las credenciales de inicio de sesión recibidas
440
El gestor de sesiones reenvía las comunicaciones entre el dispositivo de acceso y un IED objetivo que pertenece al nivel de autorización determinado
450
Fin

FIG. 5


500
Inicio
Un dispositivo de acceso proporciona credenciales de inicio de sesión a un gestor de sesiones para iniciar una sesión de comunicación
510
El gestor de control de acceso determina el nivel de autorización del dispositivo de acceso basándose en las credenciales recibidas
520
El dispositivo de acceso solicita que el gestor de sesiones reenvíe comandos a un IED conectado
530
Un filtro de sesiones determina si los comandos pertenecen al nivel de autorización del dispositivo de acceso para el IED previsto
540
¿La solicitud pertenece al nivel de autorización del dispositivo de acceso?
550
No
Sí
Rechazar la solicitud de reenvío de comandos
560
Reenviar los comandos al IED previsto
570
Un subsistema de inicio de sesión registra los eventos de acceso y las credenciales de inicio de sesión asociadas
580

600

IED heredado (baja seguridad)		
Operador	**Contraseña**	**Nivel de acceso**
Administrador	Contraseña	Acceso total a todos los sistemas y archivos

FIG. 6A

650

IED mejorado (mayor seguridad)		
Operadores	**Contraseña**	**Nivel de acceso**
Administrador	Contraseña 0	Acceso total a todos los sistemas y archivos
Operador de nivel alto	Contraseña 1	Acceso de lectura y escritura a la mayoría de sistemas y archivos
Operador de nivel medio	Contraseña 2	Acceso de lectura y escritura en algunos sistemas y archivos
Operador de nivel bajo	Contraseña 3	Acceso de solo lectura en algunos sistemas y archivos
Operador de nivel personalizado	Contraseña 4	Acceso personalizado

FIG. 6B

FIG. 7

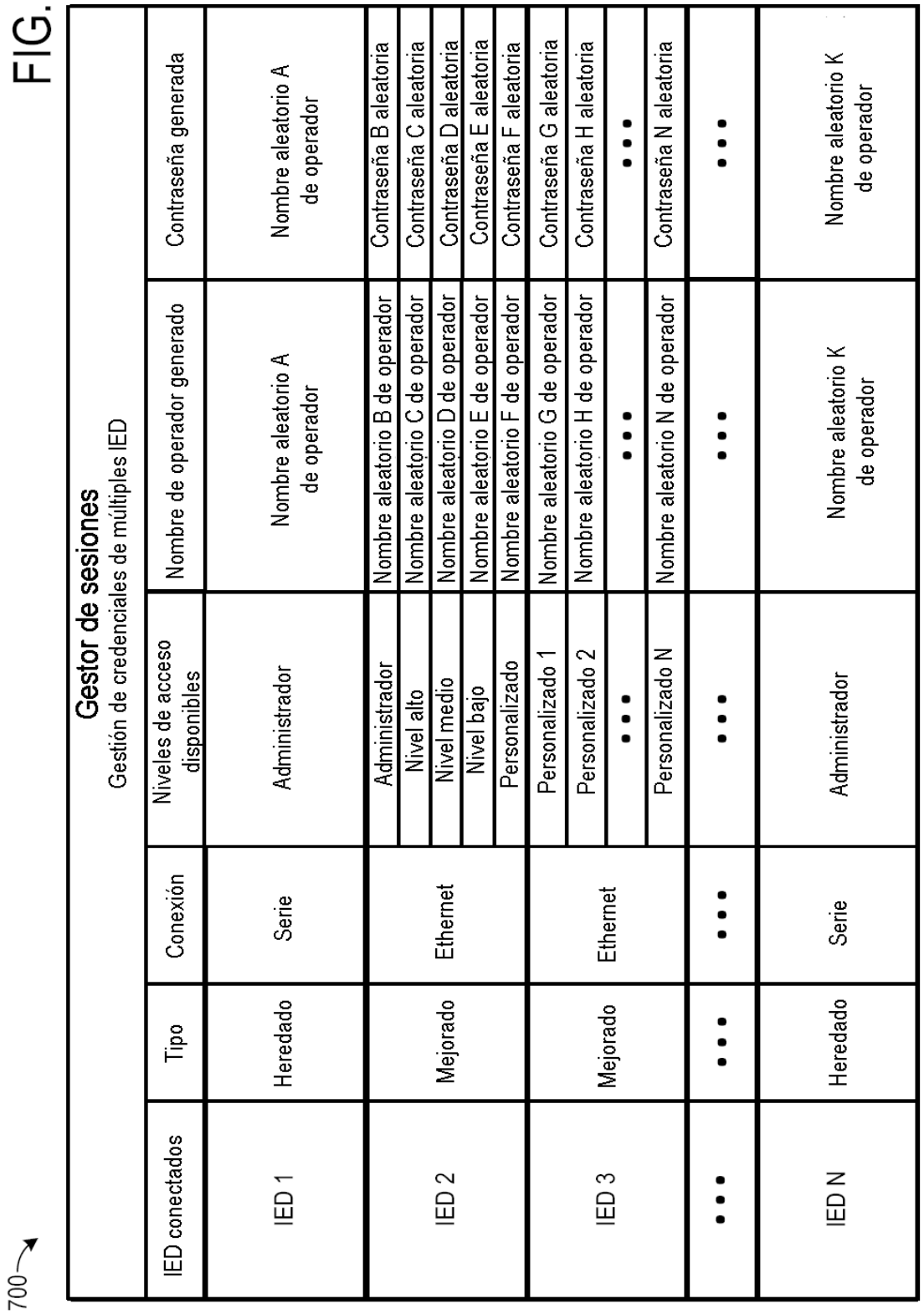

700
Gestor de sesiones
Gestión de credenciales de múltiples IED
IED conectados
Tipo
Conexión
Niveles de acceso disponibles
Nombre de operador generado
Contraseña generada
IED 1
Heredado
Serie
Administrador
Nombre aleatorio A de operador
Nombre aleatorio A de operador
IED 2
Mejorado
Ethernet
Administrador
Nivel alto
Nivel medio
Nivel bajo
Personalizado
Nombre aleatorio B de operador
Nombre aleatorio C de operador
Nombre aleatorio D de operador
Nombre aleatorio E de operador
Nombre aleatorio F de operador
Contraseña B aleatoria
Contraseña C aleatoria
Contraseña D aleatoria
Contraseña E aleatoria
Contraseña F aleatoria
IED 3
Mejorado
Ethernet
Personalizado 1
Personalizado 2
• • •
Personalizado N
Nombre aleatorio G de operador
Nombre aleatorio H de operador
• • •
Nombre aleatorio N de operador
Contraseña G aleatoria
Contraseña H aleatoria
• • •
Contraseña N aleatoria
• • •
• • •
• • •
• • •
• • •
IED N
Heredado
Serie
Administrador
Nombre aleatorio K de operador
Nombre aleatorio K de operador

FIG. 8

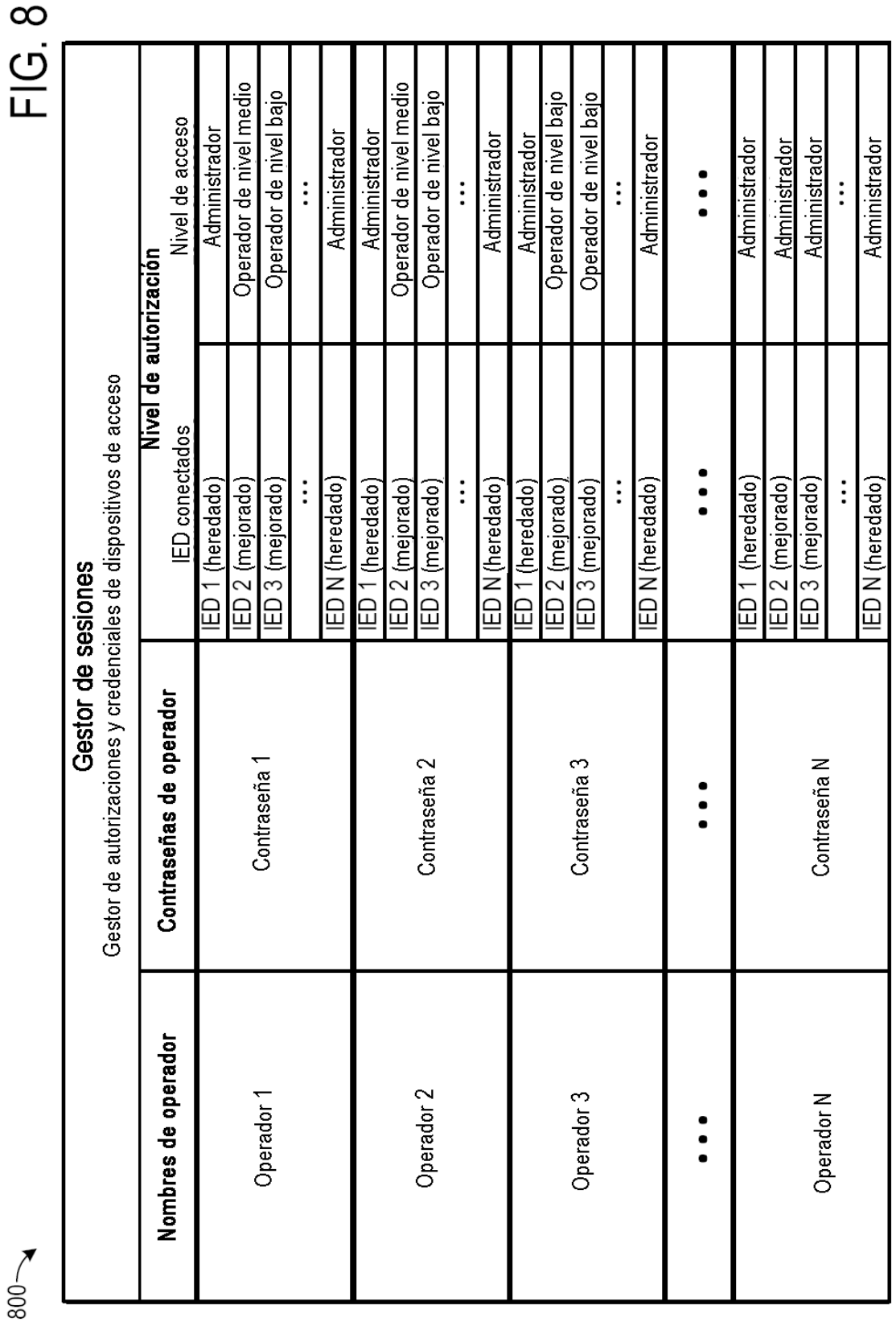
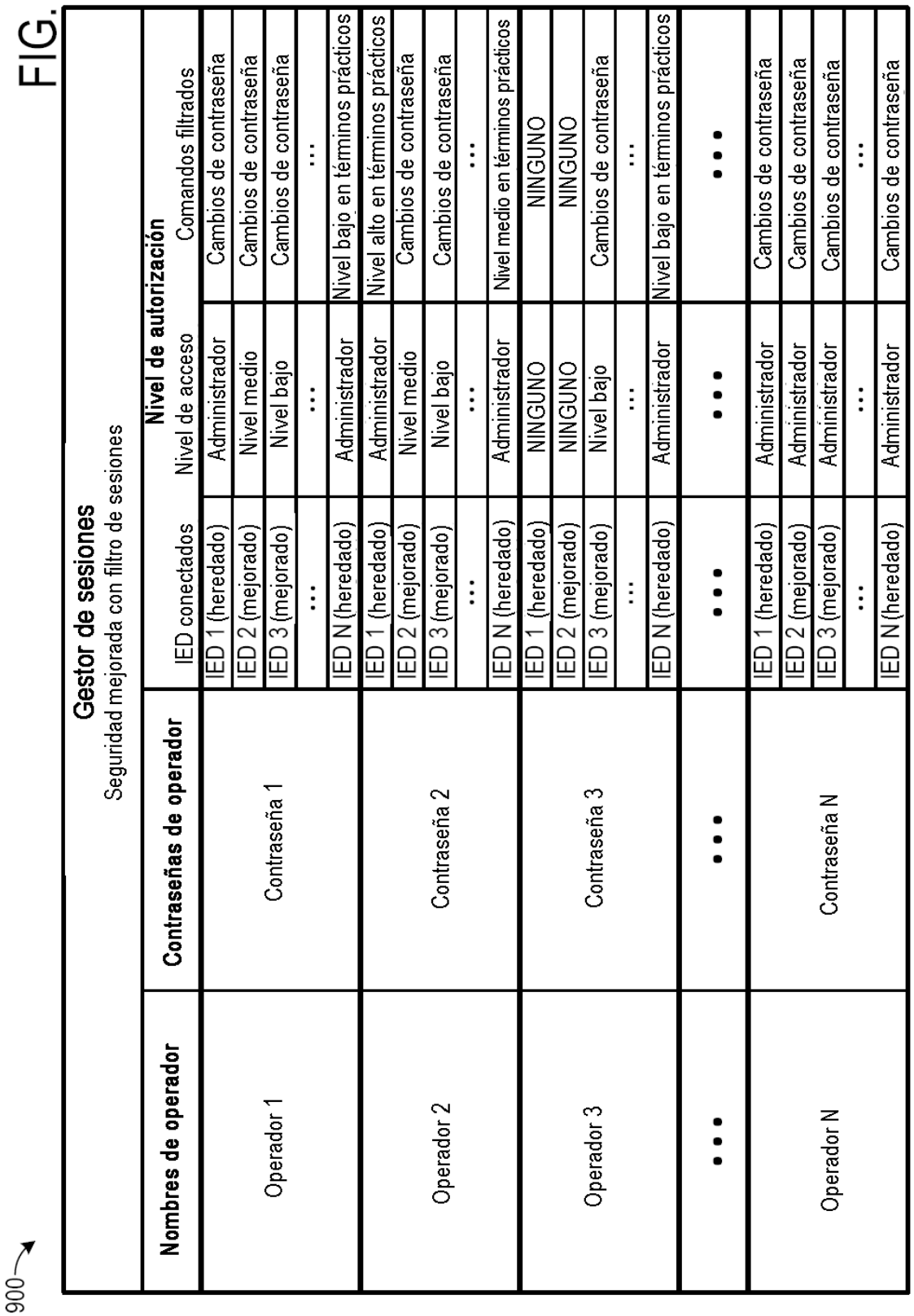

800
Gestor de sesiones
Gestor de autorizaciones y credenciales de dispositivos de acceso
Nombres de operador
Contraseñas de operador
Nivel de autorización
IED conectados
Nivel de acceso
Operador 1
Contraseña 1
IED 1 (heredado)
Administrador
IED 2 (mejorado)
Operador de nivel medio
IED 3 (mejorado)
Operador de nivel bajo
...
IED N (heredado)
Administrador
Operador 2
Contraseña 2
IED 1 (heredado)
Administrador
IED 2 (mejorado)
Operador de nivel medio
IED 3 (mejorado)
Operador de nivel bajo
...
IED N (heredado)
Administrador
Operador 3
Contraseña 3
IED 1 (heredado)
Administrador
IED 2 (mejorado)
Operador de nivel bajo
IED 3 (mejorado)
Operador de nivel bajo
...
IED N (heredado)
Administrador
• • •
• • •
• • •
Operador N
Contraseña N
IED 1 (heredado)
Administrador
IED 2 (mejorado)
Administrador
IED 3 (mejorado)
Administrador
...
IED N (heredado)
Administrador

FIG. 9


900
Gestor de sesiones
Seguridad mejorada con filtro de sesiones
Nombres de operador
Contraseñas de operador
Nivel de autorización
IED conectados
Nivel de acceso
Comandos filtrados
Operador 1
Contraseña 1
IED 1 (heredado)
Administrador
Cambios de contraseña
IED 2 (mejorado)
Nivel medio
Cambios de contraseña
IED 3 (mejorado)
Nivel bajo
Cambios de contraseña
...
IED N (heredado)
Administrador
Nivel bajo en términos prácticos
Operador 2
Contraseña 2
IED 1 (heredado)
Administrador
Nivel alto en términos prácticos
IED 2 (mejorado)
Nivel medio
Cambios de contraseña
IED 3 (mejorado)
Nivel bajo
Cambios de contraseña
...
IED N (heredado)
Administrador
Nivel medio en términos prácticos
Operador 3
Contraseña 3
IED 1 (heredado)
NINGUNO
NINGUNO
IED 2 (mejorado)
NINGUNO
NINGUNO
IED 3 (mejorado)
Nivel bajo
Cambios de contraseña
...
IED N (heredado)
Administrador
Nivel bajo en términos prácticos
• • •
• • •
• • •
• • •
Operador N
Contraseña N
IED 1 (heredado)
Administrador
Cambios de contraseña
IED 2 (mejorado)
Administrador
Cambios de contraseña
IED 3 (mejorado)
Administrador
Cambios de contraseña
...
IED N (heredado)
Administrador
Cambios de contraseña