(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 773 786**

(51) Int. CI.:

G06F 21/44 (2013.01)
G06F 21/57 (2013.01)
G06F 21/70 (2013.01)
G06F 21/85 (2013.01)
G06F 21/82 (2013.01)
G06F 21/88 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **10.10.2017 E 17195737 (6)**

(97) Fecha y número de publicación de la concesión europea: **11.12.2019 EP 3309699**

(54) Título: **Sistema de unidad de comunicación y aparato adicional con medio de aseguramiento junto a la interfaz**

(30) Prioridad:

11.10.2016 DE 102016219756

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.07.2020

(73) Titular/es:

POWER PLUS COMMUNICATIONS AG (100.0%)
Dudenstraße 6
68167 Mannheim, DE

(72) Inventor/es:

MAYER, EUGEN y
RINDCHEN, MARKUS

(74) Agente/Representante:

ROEB DÍAZ-ÁLVAREZ, María

DESCRIPCIÓN

Sistema de unidad de comunicación y aparato adicional con medio de aseguramiento junto a la interfaz

La presente invención se refiere a una unidad de comunicación para proporcionar una función de comunicación, donde la unidad de comunicación es una puerta de enlace de medidor inteligente y la función de comunicación proporcionada comprende la dirección de la comunicación entre varias redes conectadas con la unidad de comunicación, y donde la unidad de comunicación presenta al menos una interfaz que hace posible el intercambio de datos con un aparato adicional conectable mediante una conexión por enchufe. La presente invención se refiere además a un sistema con una unidad de comunicación de este tipo y un aparato adicional.

En la práctica, se conocen aparatos que deben someterse a una certificación antes de que puedan distribuirse y/o utilizarse. Durante el procedimiento de certificación, se revisa el funcionamiento del hardware y/o software en lo referente al cumplimiento de la normativa aplicable. Tales aparatos son en particular unidades de comunicación como, por ejemplo, una puerta de enlace de medidor inteligente (SMGW), que conecta entre sí diferentes redes en un sistema de medición inteligente y que dirige el acceso a los aparatos conectados y/o los datos disponibles. Durante la certificación de una SMGW, se comprueba el cumplimiento de la normativa aplicable en materia de seguridad. En Alemania, esta son dos perfiles de protección y una Directiva Técnica (TR) de la BSI (Oficinal Federal para la Seguridad de las Tecnologías de la Información) y especificaciones del FNN (Foro Tecnología de Redes/Explotación de Redes). Las redes que la SMGW conecta entre sí son una LMN (red metrológica local) para la conexión de nodos de medición, una HAN (red de área doméstica) para aparatos de consumo, y una WAN (red de área amplia) para un acceso "desde fuera" (por ejemplo, a través de un suministrador de energía).

En tales aparatos es desventajoso que, tras una certificación finalizada, la mayoría de las modificaciones en el hardware y/o software hacen necesaria una nueva certificación de todo el aparato. De este modo, en la práctica son imposibles modificables rápidas del hardware y/o software. Un enfoque para la solución de esta problemática consiste en que el aparato eléctrico se divida en componentes que requieran certificación y que no requieran certificación. Un ejemplo de una estructura de este tipo de una SMGW se divulga en el documento EP 2 709 374 A2. Gracias a esta división, es posible que los componentes que no requieran certificación se puedan modificar sin perder la certificación.

También sería concebible la utilización de interfaces universales flexibles a las que se puedan conectar aparatos adicionales como, por ejemplo, un adaptador de interfaz para Ethernet o redes de telefonía móvil. Una interfaz de este tipo podría ser, por ejemplo, un USB (bus universal en serie). No obstante, en tales interfaces es desventajoso el riesgo de seguridad relativamente elevado aunado a ellas. Puesto que tales interfaces están configuradas para un control particularmente sencillo y universal de una gran cantidad de aparatos diferentes, no hay presentes medidas de seguridad pronunciadas, de modo que los potenciales escenarios de ataque son diversos. Con ello, la gran ventaja de estas interfaces crea simultáneamente una desventaja considerable en el presente contexto, por lo que tales interfaces universales no son utilizables para las unidades de comunicación de que se habla.

El documento WO 2012/106049 A1 divulga un equipo de seguridad a través del que está ampliada la pila de protocolo USB de un sistema de servidor de USB. Para ello, en una pila de protocolo USB ampliada está incorporado un módulo de control de seguridad. Si se conecta un nuevo aparato de USB, en una etapa de inicialización se obtiene información a través del nuevo aparato de USB. Mediante una interfaz de aplicación, se comprueba si el acceso al aparato de USB es seguro o no. Una vez que el aparato de USB se haya clasificado como seguro, se desbloquea la comunicación con el aparato de USB. La comunicación se impide hasta este momento. El usuario puede ejercer influencia sobre el comportamiento del equipo de seguridad a través de una interfaz de configuración.

Por el documento WO 2013/117404 A1, se conoce un procedimiento para la personalización de un módulo de seguridad de un medidor inteligente o de una puerta de enlace de medidor inteligente. A este respecto, el núcleo es la generación y la distribución de las claves a un módulo de seguridad que esté conectado de manera no separable con el medidor inteligente, o bien, la puerta de enlace de medidor inteligente. El módulo de seguridad está configurado en un estado inicial de tal modo que la comunicación únicamente sea posible con una instancia fiable. Mediante la instancia fiable, se ejecutan configuraciones en el módulo de seguridad y/o el medidor inteligente, o bien, puerta de enlace de medidor inteligente, respectivo/a.

El objetivo de la presente invención consiste en configurar y perfeccionar una unidad de comunicación del tipo mencionado al inicio de tal modo que funciones parciales de la unidad de comunicación sean intercambiables sin comprometer la seguridad de la unidad de comunicación y, sin embargo, garantizar una protección frente a manipulaciones.

De acuerdo con la invención, el objetivo anterior se consigue mediante las características de la reivindicación 1. Por consiguiente, la unidad de comunicación de que se habla se caracteriza por que la unidad de comunicación utiliza al menos parcialmente un aparato adicional conectado a través de la interfaz al proporcionar la función de comunicación y por qué está proporcionado al menos un medio de aseguramiento que interactúa con la unidad de comunicación de tal modo que se impide o al menos se dificulta una conexión y/o separación no autorizadas de un aparato adicional a la interfaz.

Asimismo, el sistema de conformidad con las características de la reivindicación 10 consigue el objetivo anteriormente expuesto. Este sistema comprende una unidad de comunicación y un aparato adicional que proporcionan conjuntamente una función de comunicación.

Del modo de acuerdo con la invención, en primer lugar se ha reconocido que (a pesar de las problemáticas en cuanto a seguridad existentes en principio) se pueden utilizar no obstante interfaces universales para proporcionar una intercambiabilidad de las funciones de comunicación también en unidades de comunicación que requieran certificación. Entonces, tales interfaces permiten una externalización particularmente sencilla de al menos partes de la función de comunicación de la unidad de comunicación a un aparato adicional conectado a través de la interfaz. Si este aparato adicional es activado a través de software y/o hardware certificado, el aparato adicional se puede sustituir con facilidad y sin la pérdida de la certificación de la unidad de comunicación. Para eliminar o al menos para atenuar considerablemente las problemáticas en materia de seguridad, de acuerdo con la invención se proporciona además al menos un medio de aseguramiento que impide o al menos dificulta una conexión y/o separación no autorizadas de un aparato adicional a la interfaz. De este modo, se crea un sistema de unidad de comunicación y aparato adicional que también se puede utilizar durante el manejo de datos sensibles. A este respecto, también se pueden combinar diferentes medios de seguridad, de modo que se puede reforzar recíprocamente el efecto protector de los medios de aseguramiento individuales.

Gracias al medio de aseguramiento, se puede impedir de manera efectiva una tentativa de conexión y/o separación de un aparato adicional, ya que siempre se debe eludir al menos un medio de aseguramiento. Con la elección adecuada del medio de aseguramiento, se puede dificultar la conexión y/o la separación del aparato adicional de tal modo que se tenga que emplear mucho esfuerzo para poner en funcionamiento un aparato adicional no autorizado. A este respecto, un medio de aseguramiento puede actuar de tal modo que un aparato adicional conectado una vez con la interfaz de la unidad de comunicación se pueda separar entonces únicamente si se elude o destruye el medio de aseguramiento. De manera alternativa o adicional, un medio de aseguramiento puede evitar la conexión de un aparato adicional no admisible y/o impedir el funcionamiento de un aparato adicional no admisible conectado. En todos los casos, los medios de aseguramiento actúan sobre el sistema de unidad de comunicación y aparato adicional de tal modo que se puedan reducir significativamente o incluso eliminar por completo los riesgos de seguridad por la conexión no autorizada de aparatos adicionales que puedan comprometer la seguridad.

El término "aparato adicional" ha de entenderse en el sentido de que el aparato adicional no sea parte constituyente de la unidad de comunicación, sino que esté dispuesto externamente con respecto a la unidad de comunicación. Esto significa por lo general que la unidad de comunicación y el aparato adicional estén alojados en carcasas separadas y que un conector enchufable accesible desde fuera de la unidad de comunicación proporcione acceso a la electrónica de la unidad de comunicación para el intercambio de datos a través de la interfaz. En la mayoría de los casos, el conector enchufable estará formado junto a la unidad de comunicación mediante una hembrilla, mientras que el conector enchufable estará conformado junto al aparato adicional como conector macho correspondiente. Generalmente, el conector macho del aparato adicional podría estar dispuesto al final de un cable de conexión que establezca una conexión entre el conector macho y el aparato adicional.

El término "unidad de comunicación" también ha de entenderse de manera general. En principio, la unidad de comunicación podría estar formada por cualquier aparato que proporcione una función de comunicación. Una función de comunicación significa que datos, generalmente en forma empaquetada, se intercambian con uno o más aparatos conectados. Los datos intercambiados pueden generarse en la propia unidad de comunicación o almacenarse en ella. No obstante, los datos intercambiados también pueden provenir de otro aparato que esté conectado con la unidad de comunicación. Entonces, la unidad de comunicación también puede asumir únicamente tareas de coordinación. Por la práctica, se conocen numerosas unidades de comunicación correspondientes. La enseñanza de acuerdo con la invención es especialmente adecuada para su utilización en unidades de comunicación que deban someterse al menos parcialmente a una certificación. La unidad de comunicación se utiliza preferentemente en relación con sistemas de medición, en particular, un llamado sistema de medición inteligente. Una unidad de comunicación excepcionalmente preferida está formada por una puerta de enlace de medidor inteligente (SMGW) en la que la función de comunicación proporcionada comprenda la dirección entre varias redes conectadas con la unidad de comunicación. Aquí también queda englobada la dirección del acceso a datos presentes dentro de las redes y/o dentro de la SMGW.

También el término "conexión por enchufe" ha de entenderse igualmente de manera general. En este sentido, es esencial que contactos de un primer conector enchufable establezcan en el estado enchufado una conexión eléctrica con contactos correspondientes de un segundo conector enchufable. A este respecto, es irrelevante cuántos contactos presentan los conectores enchufables y cómo están formados los contactos. De hecho, el diseño respectivo de los contactos dependerá de la interfaz empleada, del escenario de uso, del entorno de funcionamiento, de la tasa de transmisión de datos a través de la interfaz y/o de condiciones básicas similares. Asimismo, es irrelevante lo "firme" que sea la conexión por enchufe, es decir, si el primer y el segundo conector enchufable únicamente están enchufados entre sí y se pueden soltar simplemente tirando de uno de los conectores enchufables, o si antes se debe(n) soltar todavía un elemento de enclavamiento o varios elementos de enclavamiento. Por la práctica, se conocen suficientemente conexiones por enchufe adecuadas.

Preferentemente, el al menos un medio de aseguramiento actúa de manera mecánica, eléctrica y/o lógica. Un medio de aseguramiento que actúe mecánicamente puede, por ejemplo, interactuar con la carcasa de la unidad de comunicación de tal modo que un cable de conexión entre la unidad de comunicación y el aparato adicional no se pueda separar de la conexión por enchufe con la interfaz de la unidad de comunicación antes de la destrucción del medio de aseguramiento. De este modo, se genera al menos un obstáculo psicológico eficaz para separar el aparato adicional de la unidad de comunicación. Así, se frustran las tentativas de separación en la mayoría de los casos. Además, de este modo es reconocible todo tipo de manipulación de una conexión entre la unidad de comunicación y el aparato adicional. Un medio de aseguramiento que actúe mecánicamente podría impedir adicional o alternativamente el acceso a la conexión por enchufe por completo. Ha de señalarse que en este contexto no se entiende por medio de aseguramiento que actúe mecánicamente un conector enchufable configurado de manera específica. Es más, no ha de influenciarse la universalidad de la conexión por enchufe. Así, por ejemplo una pestaña de codificación adicional junto a uno de los conectores enchufables de la conexión por enchufe no se consideraría medio de aseguramiento en el sentido de la enseñanza reivindicada.

Los medios de aseguramiento que actúan eléctricamente actúan de tal modo que el conector enchufable se desactiva eléctricamente con respecto a la interfaz de la unidad de comunicación. Esto puede significar, por ejemplo, que señales de comunicación que un aparato adicional desearía enviar a través de la conexión por enchufe a la interfaz de la unidad de comunicación no se conduzcan a la electrónica de la unidad de comunicación, sino que se separen eléctricamente de la electrónica. No obstante, esto puede significar también que se desactive un suministro de energía aplicado a la interfaz. Esto se puede poner en práctica en particular en configuraciones de la interfaz en las que a un aparato adicional conectado se le suministre energía eléctrica a través de la interfaz. También de este modo, se impediría un funcionamiento del aparato adicional junto a la unidad de comunicación. En el diseño más sencillo de tales medios de aseguramiento que actúan eléctricamente, estos medios de aseguramiento están implementados mediante interruptores mecánicos o electrónicos.

Con medios de aseguramiento que actúen de manera lógica, la activación de un aparato adicional a través de la interfaz se puede limitar a un aparato adicional o a un grupo de aparatos adicionales determinados por completo. Los grupos de aparatos adicionales pueden estar formados, por ejemplo, por aparatos de un fabricante determinado, un modelo de aparato determinado, un tipo de aparato determinado, o una clase determinada de aparatos adicionales (como un adaptador de interfaz LAN o un adaptador de comunicación de línea de alimentación). El experto en la materia reconocerá directamente cómo pueden estar formados tales grupos de aparatos adicionales.

En principio, los medios de aseguramiento mencionados anteriormente se pueden combinar del modo deseado para aumentar en mayor medida la protección contra una separación y/o conexión no autorizadas de un aparato adicional. Así, podrían, por ejemplo, utilizarse simultáneamente un medio de aseguramiento que actúe de manera lógica y un medio de aseguramiento que actúe de manera mecánica. En este caso, el medio de aseguramiento que actúe de manera lógica podría encargarse de que únicamente se active un aparato adicional determinado por completo o una clase determinada por completo de aparatos adicionales. El medio de aseguramiento que actúe de manera mecánica podría impedir que un aparato adicional conectado una vez únicamente se pueda separar de nuevo tras la destrucción del medio de aseguramiento.

En un diseño particularmente preferido, la unidad de comunicación comprende un controlador del servidor de seguridad que sirve de medio de aseguramiento que actúa de manera eléctrica y/o lógica. A este respecto, el controlador del servidor de seguridad dirige el intercambio de datos a través de la interfaz y es comparable en esta función básica con un controlador de servidor convencional sin medio de aseguramiento. Si, a modo de ejemplo, la interfaz está formada por USB (bus universal en serie), el controlador del servidor de seguridad sería un controlador de servidor de USB que haya sido complementado en funciones de seguridad, esto es, los medios de aseguramiento utilizados de acuerdo con la invención. A este respecto, el controlador del servidor de seguridad puede estar implementado en una unidad cerrada por completo, por ejemplo, un IC (circuito integrado). No obstante, también es concebible que el controlador del servidor de seguridad esté formado por un controlador de servidor "estándar" y que un módulo adicional complemente las funciones de seguridad. En este caso, el controlador del servidor de seguridad podría estar formado, por ejemplo, por dos IC conectados entre sí. Sin embargo, el controlador del servidor de seguridad es preferentemente una unidad cerrada.

El controlador del servidor de seguridad está configurado para activar o rechazar un aparato adicional conectado con la interfaz en función de datos de configuración. Los datos de configuración pueden estar almacenados en una memoria, preferentemente una memoria no volátil, donde esta memoria puede ser parte constituyente del controlador del servidor de seguridad o estar asociada al controlador del servidor de seguridad. Los datos de configuración pueden estar configurados de manera modificable por un administrador, de modo que se puede ejercer influencia sobre los aparatos adicionales conectables. Aquello que fijan los datos de configuración depende de la función respectiva que cumpla un medio de aseguramiento implementado en el controlador del servidor de seguridad.

En un diseño preferido, el controlador del servidor de seguridad está configurado para desactivar la interfaz. En este sentido, los datos de configuración pueden definir una desactivación correspondiente de la interfaz. Una desactivación podría significar que no se responda a ninguna señal de comunicación que se envíe a través de la interfaz al controlador del servidor de seguridad. Entonces, el controlador del servidor de seguridad ignoraría todas las peticiones

enviadas a través de la interfaz. No obstante, la desactivación puede llegar también hasta tal punto que el controlador del servidor de seguridad desactive las etapas excitadoras para la interfaz o incluso se apague por completo. De esta forma, se puede asegurar que, en el caso de una comunicación no deseada a través de la interfaz, ningún aparato adicional conectado pueda forzar una comunicación a través de manipulaciones.

En otro perfeccionamiento del controlador del servidor de seguridad, este puede estar configurado para desconectar una tensión de alimentación proporcionada a través de la interfaz para un aparato adicional conectado. Algunas interfaces como, por ejemplo, con USB, proporcionan una tensión de alimentación que suministra la energía necesaria a un aparato adicional conectado a la interfaz. Mediante la desactivación de esta tensión de alimentación, el aparato adicional no obtendría el suministro de energía necesario, de modo que no funcionaría un aparato adicional conectado a modo de prueba. De hecho, la tensión de alimentación también podría proporcionarse entonces de otro modo en un ensayo de manipulación, por ejemplo, mediante un aparato de alimentación separado, pudiendo en efecto ignorarse así de manera efectiva un aparato adicional conectado a modo de prueba.

En otro perfeccionamiento, el controlador del servidor de seguridad está configurado para obtener datos de identificación de un aparato adicional conectado con la interfaz. Estos datos de identificación pueden contener tanto información individual relativa al aparato adicional como información de carácter general. Así, en los datos de identificación podría estar expresado, por ejemplo, el fabricante del aparato adicional. Por otro lado, podría estar almacenado qué tipo de aparato o clase de aparato tiene el aparato adicional. Los datos de identificación individuales pueden comprender el número de serie, una dirección MAC (control de acceso a los medios), una ID de hardware, un certificado, u otra información que haga posible la identificación biunívoca del aparato adicional.

Tras la extracción de los datos de identificación del aparato adicional, el controlador del servidor de seguridad puede comparar los datos de identificación obtenidos de tal modo con datos de configuración. Basándose en el resultado de la comparación, se puede permitir o denegar una comunicación con el aparato adicional conectado a través de la interfaz. En los datos de configuración puede estar almacenada (de manera correspondiente a la granularidad de la dirección de los accesos) información de identificación que haga posible una decisión acerca de la activación o rechazo del aparato adicional. Así, puede estar definido, por ejemplo, qué clases de aparato pueden conectarse con la interfaz de la unidad de comunicación y/o qué aparatos adicionales completamente específicos pueden activarse por medio de sus números de serie. A este respecto, la comparación puede efectuarse mediante un sencillo ajuste de los datos de identificación con los datos de configuración. Si los datos de configuración contienen información idéntica a la de los datos de identificación, se autorizaría el control del aparato adicional conectado. De lo contrario, se denegaría el acceso. No obstante, también sería concebible si, por ejemplo, los datos de identificación comprenden un certificado, que el controlador del servidor de seguridad ejecute con el certificado operaciones de codificación y de descodificación y que la comparación de los datos de configuración se realice de este modo. Así, los datos de configuración podrían comprender, por ejemplo, una información codificada que se descodifique con el certificado almacenado en el aparato adicional. Solo si se logra la descodificación, la comparación de los datos de identificación con los datos de configuración conduciría a un resultado positivo y, de este modo, permitiría el acceso al aparato adicional.

En los datos de configuración puede estar almacenado de manera adicional qué "derechos" tiene un aparato adicional conectado identificado. Así, podría estar definido que únicamente se puedan enviar datos al aparato adicional y que únicamente acuses de recibo puedan ser evaluados por el aparato adicional. De manera alternativa o adicional, el tipo de comunicación entre el controlador del servidor de seguridad y el aparato adicional podría estar restringido por los datos de configuración. Así, sería concebible que únicamente estén permitidos determinados modos de funcionamiento, determinadas tasas de transmisión de datos y/o determinadas operaciones.

El controlador del servidor de seguridad puede presentar adicionalmente un contador o al controlador del servidor de seguridad puede estar asociado un contador. Este contador podría detectar la cantidad de diferentes aparatos adicionales conectados con la interfaz, donde, con cada aparato adicional no conectado todavía anteriormente con el controlador del servidor de seguridad, se modifique la lectura del contador. Es irrelevante en gran medida si en este sentido se lleva a cabo un aumento o una reducción de la lectura del contador. Únicamente es esencial que con cada conexión de otro aparato adicional se cuente en la misma dirección. Sin que suponga una restricción de carácter general, a continuación se da por hecho que la lectura del contador se aumenta en cada caso. Al alcanzarse o superarse un valor contado predefinido del contador, se puede denegar la comunicación con un aparato adicional conectado a través de la interfaz. Así, se puede impedir de manera aún más efectiva la conexión manipulativa de un aparato adicional, ya que el contador se debe poner a cero de manera activa en cada caso.

Al utilizarse un contador, puede ser razonable almacenar los datos de identificación, preferentemente datos de identificación individuales, extraídos de un aparato adicional. Esto es de importancia en particular entonces si el valor contado predefinido ha de permitir una conexión de varios aparatos adicionales diferentes. De esta forma, se puede reconocer si un aparato adicional ya estaba conectado o no con anterioridad. Al reconocerse un aparato adicional conectado, el controlador del servidor de seguridad extraería en primer lugar datos de identificación del aparato adicional. A continuación, los datos de identificación se compararían con datos de identificación almacenados. Si los datos de identificación recién extraídos no están aún almacenados, los datos de identificación extraídos podrían almacenarse y aumentarse o reducirse el contador. No hasta después de ello, se comprobaría si el aparato adicional puede ser conectado a la interfaz de la unidad de comunicación. Mediante este enfoque, también se contarían los

aparatos adicionales conectados a modo de prueba.

De manera adicional o alternativa, el controlador del servidor de seguridad puede comprender un módulo de autenticación. De esta forma, el controlador del servidor de seguridad puede denegar una comunicación con un aparato adicional conectado hasta una autenticación efectiva. Una autenticación de este tipo puede realizarse, por ejemplo, a través de una cadena de caracteres que garantice en el sentido de una contraseña una autenticación en el controlador del servidor de seguridad. También sería concebible que un certificado esté almacenado en el aparato adicional y que el controlador del servidor de seguridad excluya este certificado y lo utilice para una autenticación. Sería concebible que el certificado forme parte de un par de claves del que una parte esté almacenada en el controlador del servidor de seguridad y la otra parte esté almacenada en el aparato adicional. La autenticación sería exitosa solo si las dos partes encajan. Por la práctica, se conocen suficientemente procedimientos de autenticación correspondientes.

En principio, la interfaz de la unidad de comunicación puede estar formada de las maneras más diversas. Es esencial que la interfaz sea enchufable en caliente, es decir, que un aparato adicional pueda conectarse con la unidad de comunicación durante el funcionamiento en marcha de la unidad de comunicación. No obstante, estas interfaces están muy extendidas. Para garantizar un conector enchufable tan compacto como sea posible y una conexión a prueba de averías del aparato adicional, la interfaz está configurada preferentemente en serie. A este respecto, la interfaz está configurada como bus en serie de manera particularmente preferida. Un diseño particularmente preferido de un bus en serie de este tipo es un USB (bus universal en serie). Es en gran medida irrelevante qué versión de USB se utiliza. La elección del estándar dependerá esencialmente de qué tasas de transmisión de datos entre la unidad de comunicación y el aparato adicional se hayan de poner en práctica. No obstante, en una variante preferida, se utiliza USB 3, allí en particular USB 3.1. El USB 3.1 tiene la ventaja decisiva consistente en que en el estándar sea conocida una variante atornillable en la que uno o dos tornillos aseguren el conector de corte en el sentido de un elemento de enclavamiento contra la extracción del conector macho desde la hembrilla.

Para proporcionar un medio de aseguramiento que actúe mecánicamente, en la carcasa de la unidad de comunicación podría estar realizado ojete o una vía de paso a través del cual/de la cual sea conducible un precinto para asegurar el conector enchufable entre el aparato adicional y la unidad de comunicación.

Mediante la combinación de una unidad de comunicación de acuerdo con la invención con un aparato adicional se puede formar un sistema de acuerdo con la invención. El aparato adicional está conectado a través de una conexión por enchufe con una interfaz de la unidad de comunicación y asume una parte de la función de comunicación de la unidad de comunicación. De este modo, las unidades de combinación y el aparato adicional cumplen conjuntamente una función de comunicación que ha de proporcionarse.

El aparato adicional puede asumir repetidamente funciones de comunicación. No obstante, la función de comunicación es preferentemente un empalme a una red conectada por cable o basada en radio. En este caso, el aparato adicional actúa como adaptador de interfaz. Diseños preferidos de tales redes son Ethernet, WLAN (red de área local inalámbrica), la telefonía móvil, en particular, GSM (sistema global para las comunicaciones móviles), UMTS (sistema universal de telecomunicaciones móviles) o LTE (evolución a largo plazo). La red también podría estar tendida por comunicación de línea de alimentación, es decir, los datos se transmiten mediante señales de línea de alimentación moduladas de manera específica a través de líneas de suministro de energía convencionales. Por el estado de la técnica, se conocen suficientemente técnicas y redes correspondientes.

En principio, es concebible que el aparato adicional esté formado por aparatos adicionales habituales en el mercado para su conexión a la interfaz de la unidad de comunicación. Si la interfaz está formada, por ejemplo, por USB, y la red a conectar está formada por Ethernet, hay disponibles comercialmente adaptadores USB a Ethernet que se pueden utilizar en principio como aparato adicional en el sistema de acuerdo con la invención. No obstante, es esencial que los medios de aseguramiento proporcionados por la unidad de comunicación funcionen de manera suficientemente segura. Esto significa, por ejemplo, que el aparato adicional proporcione datos de identificación suficientemente apropiados para la extracción a través de un controlador del servidor de seguridad. No obstante, también sería concebible que se utilicen aparatos adicionales configurados de manera específica, los cuales estén complementados por memorias con datos de identificación correspondientes o comprendan los módulos para proporcionar una autenticación segura.

El sistema puede comprender además un precinto que actúe como medio de aseguramiento. A este respecto, el precinto puede impedir el acceso a un conector enchufable junto a la unidad de comunicación, que se suelte el conector enchufable y/o que se suelte un elemento de enclavamiento instalado junto al conector enchufable. Para ello, se puede utilizar adicionalmente un ojete o una vía de paso en la carcasa de la unidad de comunicación.

A este respecto, la unidad de comunicación y el aparato adicional están dispuestos preferentemente en carcasas separadas. De este modo, se puede mejorar en mayor medida la modularidad deseada.

En un perfeccionamiento del sistema, podría estar prevista allí una unidad de configuración que permita una adaptación de datos de configuración para la unidad de comunicación. A este respecto, la unidad de configuración

puede estar configurada de tal modo que la unidad de configuración sea conectada localmente a la unidad de comunicación por un técnico del servicio si ha de efectuarse una modificación de datos de configuración. No obstante, la unidad de configuración está dispuesta preferentemente alejada de la unidad de comunicación y permite con ello la administración remota de la unidad de comunicación. A este respecto, se puede utilizar una unidad de configuración para varias unidades de comunicación. Para la protección de modificaciones no autorizadas de los datos de configuración, se podrían adoptar medidas de seguridad especiales. Así, sería concebible que entre la unidad de configuración y la/las unidad(es) de comunicación se estructure una conexión codificada, por ejemplo, como conexión SSL (capa de conexiones seguras) o como túnel VPN (red privada virtual). Solo si llegan datos a través de una conexión de este tipo, la unidad de comunicación aceptará las modificaciones. De manera adicional, puede estar previsto además, por ejemplo, un inicio de sesión en el que el técnico del servicio se autentifique con un nombre de usuario y una contraseña.

Ahora hay diferentes posibilidades de configurar y perfeccionar la enseñanza de la presente invención de manera ventajosa. Para ello, se remite por un lado a las reivindicaciones subordinadas a las reivindicaciones independientes y, por otro lado, a la siguiente explicación de las formas de realización preferidas de la invención por medio del dibujo. En relación con la explicación de los ejemplos de realización preferidos de la invención por medio del dibujo, también se explican en general realizaciones y perfeccionamientos preferidos de la enseñanza. En el dibujo, muestran

Fig. 1 un diagrama de bloques con diferentes unidades funcionales de una puerta de enlace de medidor inteligente con un puerto USB-C,

Fig. 2 un diagrama de bloques con diferentes unidades funcionales de una puerta de enlace de medidor inteligente de acuerdo con la invención con un puerto USB y un controlador del servidor de seguridad para el aseguramiento eléctrico y/o lógico contra la manipulación con un adaptador de Ethernet conectado,

Fig. 3 un diagrama de bloques correspondiente a la figura 2, donde, en lugar del adaptador de Ethernet, está conectado como aparato adicional un adaptador de interfaz LTE.

La figura 1 muestra un diagrama de bloques con diferentes unidades funcionales de una puerta de enlace de medidor inteligente (SMGW). La SMGW 1 se compone de una carcasa 2, representada simbólicamente como rectángulo, en la que está dispuesta la electrónica de la SMGW 1 sobre cuatro placas en total. Una placa base 3 sirve para la conexión de una placa de suministro de energía 4, una placa de línea de alimentación de banda ancha 5 ("placa BPL") y un módulo de integración de SMGW 6 ("placa IMI"). La placa de suministro de energía 4 comprende un terminal de suministro de energía 7 al que es conectable un suministro de energía. Un suministro de energía de este tipo puede estar formado, por ejemplo, por una red monofásica de tensión alterna con un valor eficaz de 230V. La placa de suministro de energía 4 genera una o varias tensiones que son necesarias para el funcionamiento de la SMGW 1 a partir de la tensión aplicada en el terminal de suministro de energía 7. Las tensiones generadas se distribuyen a través de la placa base 3 a las otras placas de la SMGW 1. En el módulo de integración de SMGW 6 están implementados todos los componentes de la SMGW 1 que requieren una certificación.

Por lo tanto, el módulo de integración de SMGW 6 presenta dos puertos Ethernet 8, 9, que pueden proporcionar una conexión a la HAN y la LMN. La conexión a la WAN está formada a través de la placa BPL 5. A este respecto, la placa BPL 5 puede utilizar para la comunicación primariamente línea de alimentación de banda ancha, es decir, los datos que han de transmitirse se transmiten a través del suministro de energía conectado con el terminal de suministro de energía 7.

La placa BPL 5 presenta un puerto USB 10 al que es conectable un aparato adicional. El puerto USB 10 forma una interfaz para conectar un aparato adicional mediante una conexión por enchufe. Este aparato adicional no señalado en este caso puede estar formado, a modo de ejemplo, por un adaptador USB a Ethernet. Mediante el aparato adicional, se puede proporcionar una vía de comunicación secundaria a la WAN. El puerto USB 10 está realizado preferentemente como puerto USB-C con atornillamiento, es decir, la hembrilla de USB-C junto a la SMGW presenta una o dos hembrillas roscadas en las cuales se puede enroscar en cada caso un tornillo junto al conector macho de USB-C como elementos de enclavamiento. Un precinto no indicado en este caso puede actuar de medio de aseguramiento que actúe mecánicamente y asegurar el conector macho de USB contra la separación y el recambio no autorizados del aparato adicional. De manera adicional o alternativa, es concebible que la carcasa de la SMGW presente un ojete o una vía de paso a través del cual/de la cual esté conducido un precinto. A este respecto, el precinto podría conducirse a través del ojete o, en su caso, la vía de paso, adicionalmente al aseguramiento del elemento de enclavamiento. Como alternativa, el precinto podría estar conducido alrededor del cable de conexión de USB, de modo que se impida la extracción del conector macho de USB (con o sin elementos de enclavamiento). De este modo, puede estar formado un ejemplo de realización de un sistema de acuerdo con la invención.

Las figuras 2 y 3 muestran otro diseño de una unidad de comunicación de acuerdo con la invención. La placa BPL 5 presenta de nuevo un puerto USB 10, que está realizado como USB-C u otra variante de USB. Para dirigir la comunicación a través del puerto USB 10, la placa BPL presenta adicionalmente un controlador del servidor de seguridad 11 que en su función básica se corresponde con un controlador de servidor de USB. De manera adicional,

en el controlador del servidor de seguridad están implementados medios de aseguramiento con los que se puede impedir de manera dirigida la conexión, o bien, el funcionamiento, de aparatos adicionales 12 no admisibles. La figura 2 muestra una variante en la que el aparato adicional 12 está formado por un adaptador USB-Ethernet (USB2ETH). En la figura 3, hay una segunda variante con un adaptador USB-LTE (USB2LTE) con antena correspondiente como aparato adicional 12'.

Con ello, la hembrilla de USB puede constituir el límite del hardware de un aparato certificado. Por el lado del software, un controlador de servidor es el punto que integra los diferentes tipos de adaptadores y posibilita la comunicación. A la propia hembrilla se pueden conectar diferentes adaptadores, que a su vez proporcionan diferentes interfaces [por ejemplo, Ethernet, GSM (sistema global para las comunicaciones móviles), LTE (evolución a largo plazo), etc.].

En lo relativo a otros diseños ventajosos de la unidad de comunicación de acuerdo con la invención, o bien, del sistema de acuerdo con la invención, para la evitación de repeticiones se remite a la parte general de la descripción y a las reivindicaciones adjuntas.

Finalmente, ha de señalarse expresamente que los ejemplos de realización descritos anteriormente sirven únicamente para exponer la enseñanza reivindicada, pero no la limitan a los ejemplos de realización.

Lista de referencias

1	Puerta de enlace de medidor inteligente
2	Carcasa
3	Placa base
4	Placa de suministro de energía
5	Placa BPL
6	Módulo de integración de SMGW
7	Terminal de suministro de energía
8	Puerto Ethernet
9	Puerto Ethernet
10	Puerto USB
11	Controlador del servidor de seguridad
12	Aparato adicional

REIVINDICACIONES

1. Unidad de comunicación para proporcionar una función de comunicación, donde la unidad de comunicación es una puerta de enlace de medidor inteligente (1) y la función de comunicación proporcionada comprende la dirección de la comunicación entre varias redes conectadas con la unidad de comunicación, y donde la unidad de comunicación presenta al menos una interfaz que hace posible un intercambio de datos con un aparato adicional (12, 12') conectable mediante una conexión por enchufe,
caracterizada por que la unidad de comunicación utiliza al menos parcialmente un aparato adicional (12, 12') conectado a través de la interfaz (10) al proporcionar la función de comunicación y por que está proporcionado al menos un medio de aseguramiento que interactúa con la unidad de comunicación de tal modo que se impide o al menos se dificulta una conexión y/o separación no autorizadas de un aparato adicional (12, 12') a la interfaz.

2. Unidad de comunicación según la reivindicación 1, caracterizada por que el al menos un medio de aseguramiento actúa de manera mecánica, eléctrica y/o lógica.

3. Unidad de comunicación según la reivindicación 1 o 2, caracterizada por un controlador del servidor de seguridad (11) que actúa como medio de aseguramiento y dirige un intercambio de datos a través de la interfaz (10), donde el controlador del servidor de seguridad (11) está configurado para activar o rechazar un aparato adicional (12, 12') conectado con la interfaz (10) en función de datos de configuración.

4. Unidad de comunicación según la reivindicación 3, caracterizada por que el controlador del servidor de seguridad (11) está configurado para desactivar la interfaz (10) y/o desconectar una tensión de alimentación proporcionada a través de la interfaz (10) para un aparato adicional (12, 12') conectado.

5. Unidad de comunicación según la reivindicación 3 o 4, caracterizada por que el controlador del servidor de seguridad (11) está configurado para identificar un aparato adicional (12, 12') conectado con la interfaz (10) y/o su tipo de aparato, comparar datos de identificación obtenidos de tal modo con datos de configuración, y permitir o denegar una comunicación con el aparato adicional (12, 12') conectado a través de la interfaz (10) basándose en el resultado de la comparación, donde los datos de configuración comprende(n) preferentemente una clase de aparato y/o un número de identificación de un aparato adicional permitido.

6. Unidad de comunicación según una de las reivindicaciones 3 a 5, caracterizada por que el controlador del servidor de seguridad (11) presenta un contador o por que al controlador del servidor de seguridad (11) está asociado un contador, donde el contador detecta la cantidad de diferentes aparatos adicionales (12, 12') conectados con la interfaz (10) y donde el controlador del servidor de seguridad (11) está configurado para permitir o denegar una comunicación con el aparato adicional conectado a través de la interfaz al alcanzarse o superarse un valor contado predefinido del contador.

7. Unidad de comunicación según una de las reivindicaciones 3 a 6, caracterizada por que el controlador del servidor de seguridad (11) comprende un módulo de autenticación, donde el controlador del servidor de seguridad (11) está configurado para permitir una comunicación con un aparato adicional (12, 12') conectado no hasta después de una autenticación efectiva.

8. Unidad de comunicación según una de las reivindicaciones 1 a 7, caracterizada por que la interfaz (10) está formada por un bus en serie, preferentemente por USB (bus universal en serie).

9. Unidad de comunicación según una de las reivindicaciones 1 a 8, caracterizada por que los medios de aseguramiento comprenden un ojete o una vía de paso a través del/de la cual es conducible un precinto para asegurar el conector enchufable.

10. Sistema con una unidad comunicación según una de las reivindicaciones 1 a 9 y con un aparato adicional, donde el aparato adicional (12, 12') está conectado a través de una conexión por enchufe con una interfaz (10) de la unidad de comunicación y donde la unidad de comunicación y el aparato adicional (12, 12') proporcionan conjuntamente una función de comunicación.

11. Sistema según la reivindicación 10, caracterizado por que el aparato adicional (12, 12') es un adaptador de interfaz para conectar la unidad de comunicación a una red conectada por cable o red inalámbrica, donde la red está formada preferentemente por Ethernet, WLAN (red de área local inalámbrica), telefonía móvil, en particular, GSM (sistema global para las comunicaciones móviles), UMTS (sistema universal de telecomunicaciones móviles) o LTE (evolución a largo plazo), o comunicación de línea de alimentación.

12. Sistema según la reivindicación 10 u 11, caracterizado por un precinto que actúa como medio de aseguramiento, donde el precinto impide un acceso a un conector enchufable junto a la unidad de comunicación, o donde el precinto impide que se suelte el conector enchufable, o donde el precinto asegura un elemento de enclavamiento al conector enchufable contra la soltura del elemento de enclavamiento.

13. Sistema según una de las reivindicaciones 10 a 12, caracterizado por que la unidad de comunicación y el aparato adicional están alojados en carcasas separadas y/o por que el aparato adicional es sustituible en principio.

14. Sistema según una de las reivindicaciones 10 a 13, caracterizado por que el sistema presenta adicionalmente una unidad de configuración mediante la cual son modificables datos de configuración dentro de la unidad de comunicación.

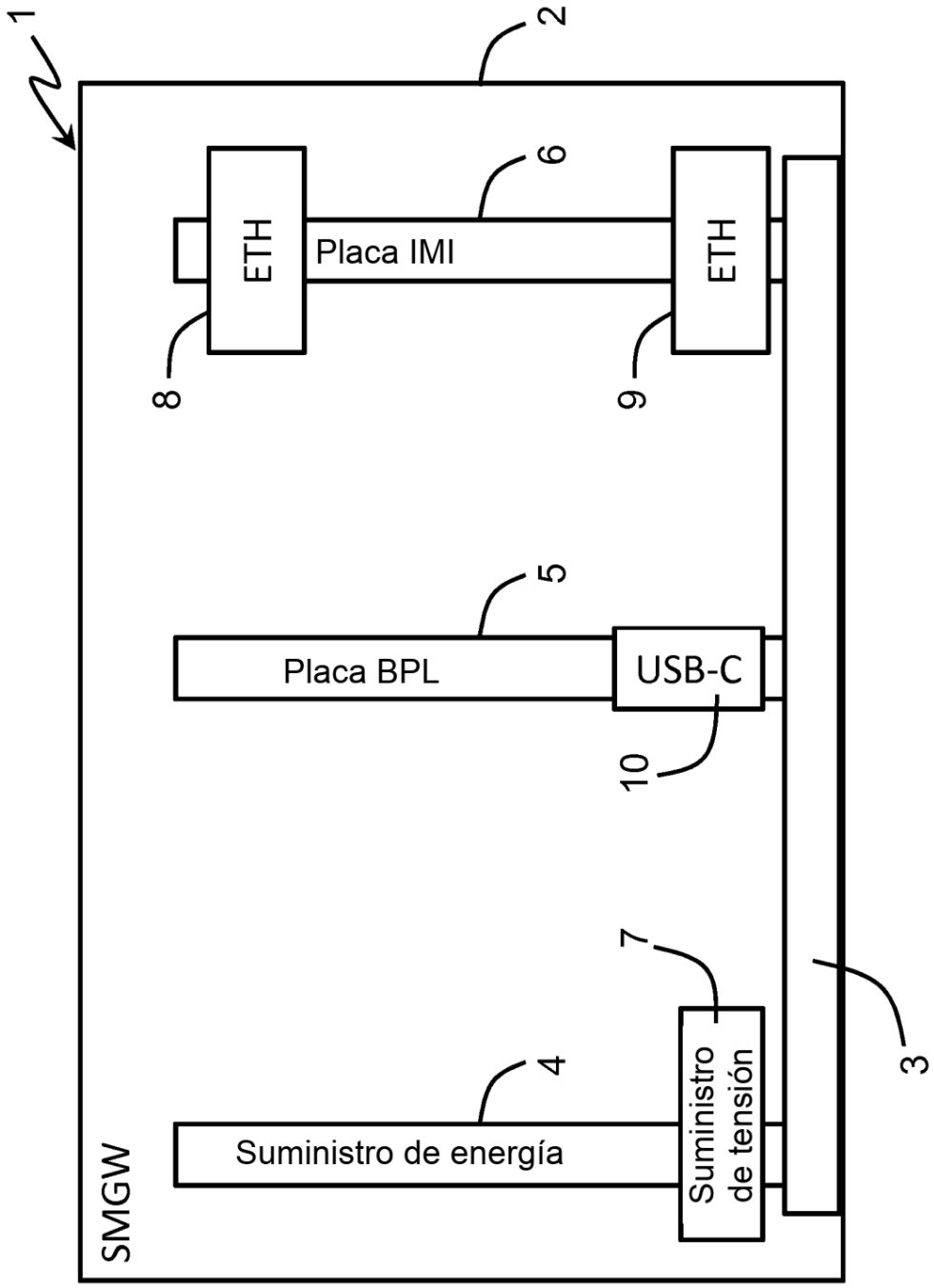
1
2
6
ETH
Placa IMI
ETH
8
9
5
Placa BPL
USB-C
10
7
3
4
Suministro de energía
Suministro de tensión
SMGW

Fig. 1

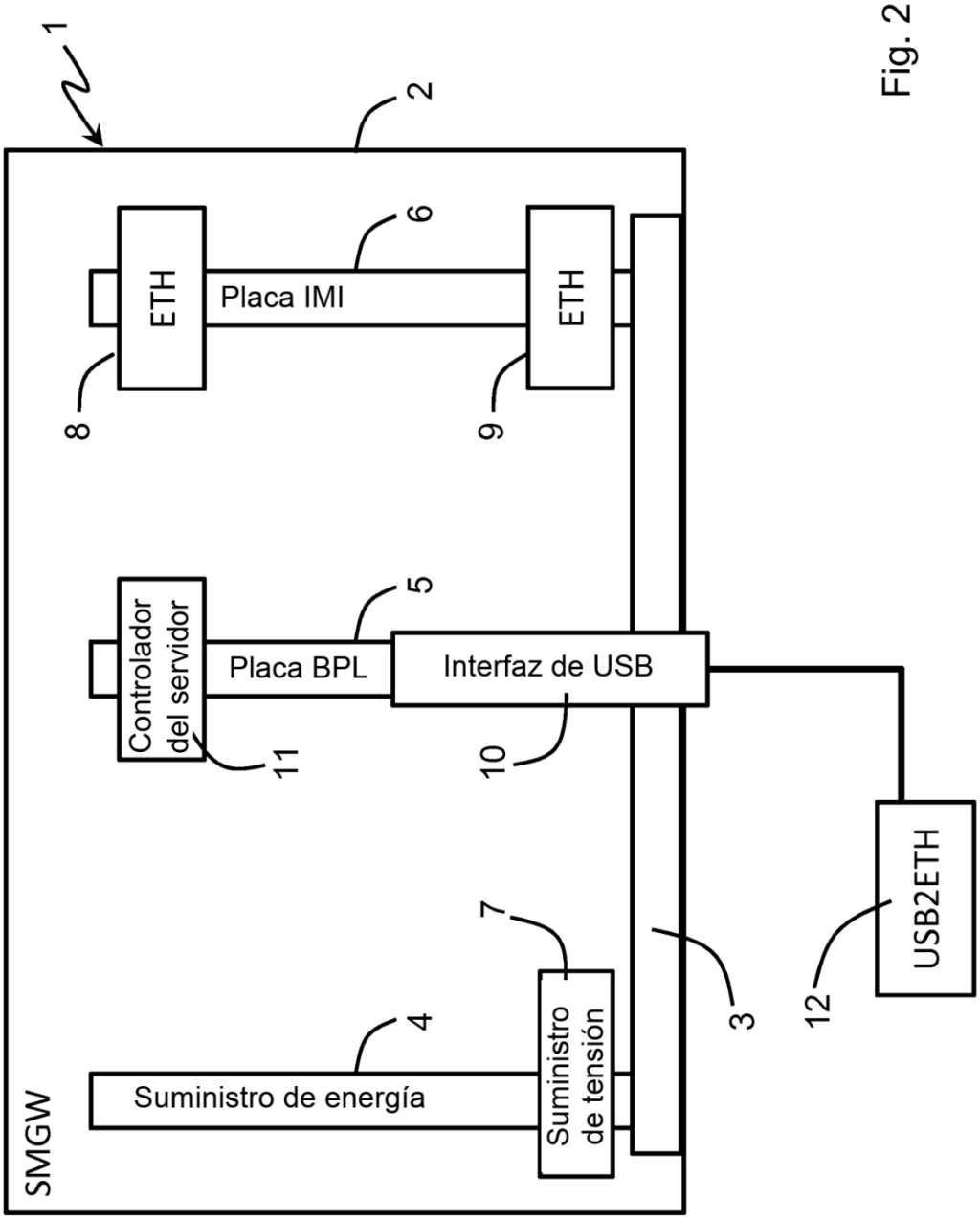
1
2
6
ETH
Placa IMI
ETH
8
9
5
Controlador del servidor
Placa BPL
Interfaz de USB
11
10
7
Suministro de tensión
4
Suministro de energía
SMGW
3
12
USB2ETH

Fig. 2

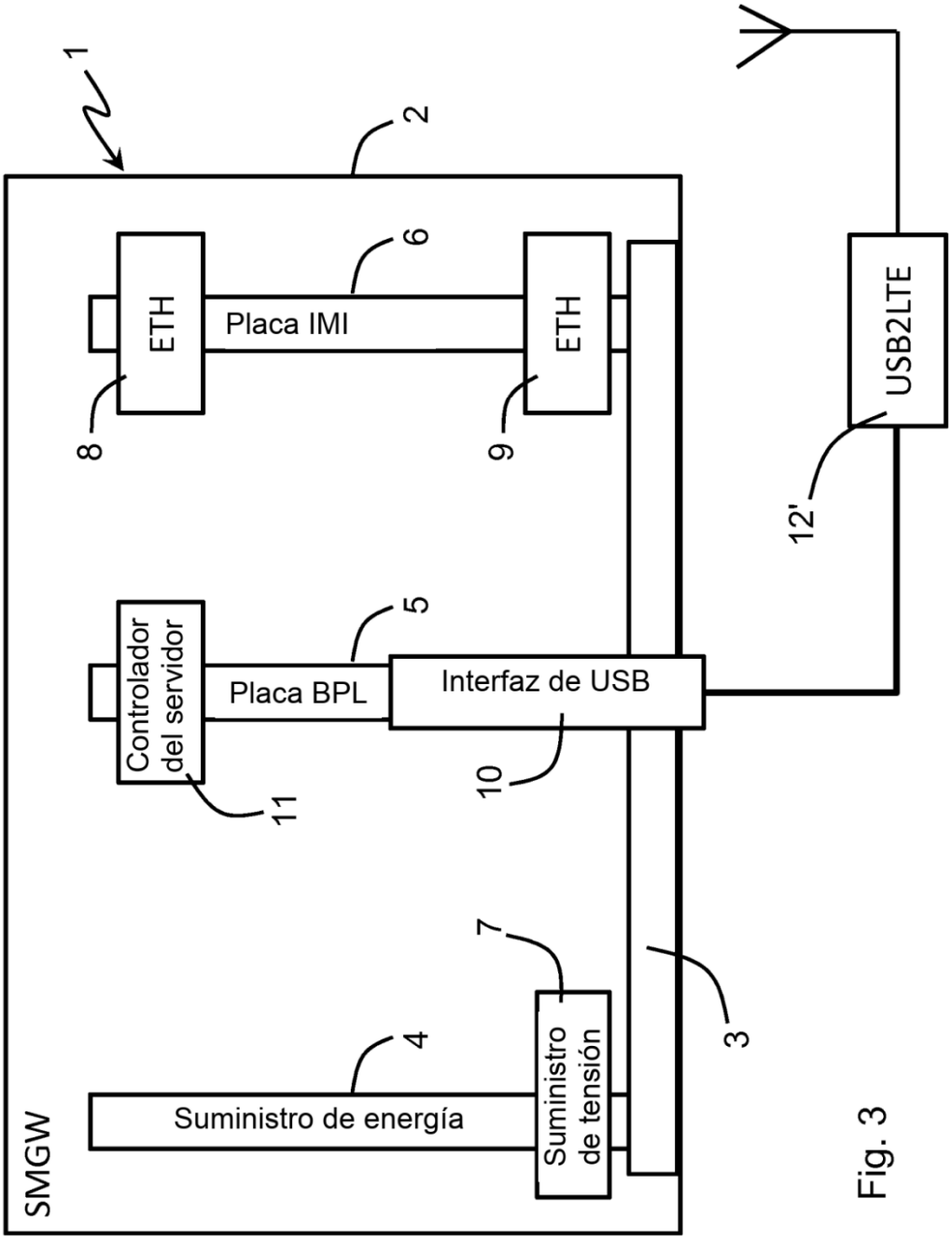
1
2
6
ETH
Placa IMI
ETH
8
9
USB2LTE
12'
5
Controlador del servidor
Placa BPL
Interfaz de USB
10
11
7
3
4
Suministro de energía
Suministro de tensión
SMGW

Fig. 3