(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 778 848**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **05.07.2017 E 17179719 (4)**

(97) Fecha y número de publicación de la concesión europea: **18.12.2019 EP 3425865**

(54) Título: **Procedimiento y dispositivo para la transmisión unidireccional sin repercusión de datos a un servidor de aplicación remoto**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.08.2020

(73) Titular/es:

SIEMENS MOBILITY GMBH (100.0%)
Otto-Hahn-Ring 6
81739 München, DE

(72) Inventor/es:

FALK, RAINER y
WIMMER, MARTIN

(74) Agente/Representante:

LOZANO GANDIA, José

DESCRIPCIÓN

Procedimiento y dispositivo para la transmisión unidireccional sin repercusión de datos a un servidor de aplicación remoto

La invención se refiere a un procedimiento, un dispositivo y un producto de programa informático para la transmisión unidireccional sin repercusión de datos desde una primera zona de red a una segunda zona de red para la evaluación en un servidor de aplicación remoto. En particular, la primera zona de red es una red relevante para la seguridad, por ejemplo, una red de seguridad de un sistema de seguridad ferroviaria o un sistema de automatización. La segunda zona de red está sujeta a requisitos de seguridad más bajos y puede ser, por ejemplo, una red de oficina o una zona de evaluación conectada a través de una red de oficina o Internet, también designada como zona de Backend o nube.

La invención se define por las reivindicaciones independientes.

Por medio de un diodo de datos o una puerta de enlace unidireccional, generalmente se debe lograr que un flujo de información sea posible solamente en una dirección, en particular entre zonas de red de diferente relevancia de seguridad. Dichas soluciones de seguridad entre zonas, también llamadas soluciones de seguridad de dominio cruzado, se han usado hasta ahora para áreas especiales de comunicación de autoridad en las que se aplican requisitos de alta seguridad y en los que existe una clasificación de seguridad de documentos o información. Mediante la solución de seguridad de dominio cruzado se implementa un intercambio seguro automatizado de documentos y mensajes, como por ejemplo correos electrónicos, entre zonas de seguridad de diferente nivel.

Dicha solución de seguridad de dominio cruzado se conoce por el documento WO 2012/170485, en el que una máquina virtual controla la transferencia de información entre dos dominios de información. Sin embargo, se requiere un componente de transmisión especial y un componente de recepción especial además del diodo de datos real, de modo que un protocolo de comunicación realmente bidireccional, como el Protocolo de Transferencia de Archivos FTP o el Protocolo de Transferencia de Hipertexto HTTP, se pueda implementar a través de un diodo de datos.

Un demonio Syslog especial provisto en un nodo transmisor también se conoce por el documento US 7,941,526 B1, en el que el nodo transmisor está conectado a un nodo receptor a través de una conexión de datos unidireccional y el demonio Syslog especial está configurado para recibir un mensaje syslog desde un transmisor syslog, insertar una parte de la información de IP del remitente de syslog en la parte de mensaje del mensaje de syslog recibido y reenviar el mensaje de syslog resultante a la conexión de datos unidireccional, de modo que el mensaje de syslog resultante se pueda enviar a través de la conexión de datos unidireccional a un receptor de syslog, que está conectado comunicativamente al nodo receptor. Esto resuelve el posible conflicto entre las aplicaciones de transmisión de datos syslog y las aplicaciones de transmisión de datos unidireccionales, que eliminan la información IP de los datos antes de que se transmitan a través de una conexión de datos unidireccional, lo que mejora aún más la seguridad de la red mediante su combinación.

El documento US 7,941,526 B1 describe además un demonio Syslog especial en un nodo de envío, en el que el nodo de envío está conectado a través de una conexión de datos de una sola vía a un nodo receptor, en el que el demonio Syslog especial está configurado para recibir un mensaje de syslog desde un transmisor syslog, para insertar una parte de la información IP del remitente de syslog en el mensaje de syslog recibido y enrutar el mensaje de syslog resultante a la conexión de datos unidireccional para que el mensaje de syslog resultante se envíe a través de la conexión de datos unidireccional a un receptor de syslog, que está conectado comunicativamente al nodo receptor. El documento WO 98/42107 A1 describe un sistema de transmisión de paquetes de datos digitales que proporciona una calidad de servicio más eficiente y más alta en aplicaciones tales como telefonía por Internet. Se usa un protocolo de transmisión para enviar datos de un primer usuario o cliente a un proveedor de servicios de Internet (ISP) local a través de líneas telefónicas estándar. En el ISP, los paquetes de datos se convierten de TCP a UDP y luego los paquetes UDP se transmiten, típicamente en un ancho de banda más alto, a otro ISP local que sirve al receptor. Los paquetes UDP se traducen de nuevo a paquetes TCP y se envían al receptor.

Cuando las redes de control industrial están vinculadas a una red de oficina, una Internet pública u otras redes de control, el foco está en la transmisión sin repercusión. Los firewalls convencionales se usan generalmente para este propósito, que restringe la comunicación de datos bidireccional según reglas de filtro configurables. Sin embargo, dichas soluciones no garantizan la falta de repercusión o la calidad requerida para las redes de control industrial. La falta de repercusión significa que al transmitir desde una zona de red con alta relevancia de seguridad a una zona de red menos segura, no se introducen datos en la zona de red relevante para la seguridad.

Se conoce un cuadro de conexión en la nube unidireccional de la compañía Waterfall, véase http://static.waterfallsecurity.com/Unidirektional-CloudConnect-Brochure.pdf. Esta solución comprende un diodo

de datos unidireccional con una unidad transmisora y una unidad receptora, que admite una amplia variedad de protocolos de red de la zona de red relevante para la seguridad, tanto en el lado receptor de la zona relevante para la seguridad como en una unidad receptora que reenvía datos a la segunda zona de red menos relevante para la seguridad.

Para los protocolos de red que se usan en zonas de red relevantes para la seguridad, generalmente se deben realizar certificaciones de seguridad para demostrar la seguridad (Safety) funcional. Esto significa que los componentes de red con dichas implementaciones de protocolo solo se pueden cambiar con una nueva certificación. Por tanto, las nuevas implementaciones de protocolo u otros protocolos difícilmente se pueden introducir en dichos componentes, o solo con gran esfuerzo y gasto. Por otro lado, los servicios de evaluación se llevan a cabo cada vez más en una zona de red central, también conocida como zona de nube o Backend, que está separada de la zona de red relevante para la seguridad y que impone diferentes demandas a los datos de entrada.

Por tanto, el objetivo de la presente invención es proporcionar una solución rentable y flexiblemente adaptable para la transmisión de datos unidireccional sin repercusión, que sea preferentemente adecuada tanto para soluciones de seguridad de dominio cruzado basadas en diodos de datos como para soluciones de puerta de enlace de datos unidireccionales sin repercusión para aplicaciones industriales.

El objetivo se consigue mediante el procedimiento según la invención o el dispositivo según la invención según las reivindicaciones independientes. Los desarrollos ventajosos del procedimiento según la invención o del dispositivo según la invención se muestran en las reivindicaciones dependientes.

Según un primer aspecto, la invención se refiere a un procedimiento para la transmisión unidireccional sin repercusión de datos desde una primera zona de red a una segunda zona de red para la evaluación en un servidor de aplicación remoto, con las siguientes etapas de procedimiento: Detectar los datos que se transmiten en un formato de datos de red en la primera zona de red, transformar los datos del formato de datos de red a un formato de datos de transporte y transmitir unidireccionalmente los datos en formato de datos de transporte a la segunda zona de red, retransformar los datos desde el formato de datos de transporte y transmitir los datos a un servidor de aplicación, en el que la retransformación se lleva a cabo en una segunda zona de red separada de la primera zona de red, en el que cuando los datos de red se transforman de un formato de datos de red a un formato de datos de transporte, se lleva a cabo una conversión de formato de protocolo de un protocolo de red usado en la primera zona de red para transmitir los datos de red a un protocolo de transporte que se usa para transmitir los datos de red a la segunda zona de red, el protocolo de red permite la comunicación bidireccional y el protocolo de transporte permite solamente la comunicación unidireccional.

El procedimiento permite una solución rentable y flexiblemente adaptable para soluciones de seguridad de dominio cruzado basadas en diodos de datos, así como para soluciones de puerta de enlace unidireccionales sin repercusión para redes de control industrial, ya que el diodo de datos en sí no incluye un dispositivo de conversión que, por un lado, requiere aprobación para su uso en contacto directo con la primera zona de red relevante para la seguridad. Esto significa que las versiones no certificadas y publicadas del protocolo de red también se pueden usar para la importación de datos, que se pueden actualizar libremente. Por otro lado, es posible usar diodos de datos de bajo coste o puertas de enlace unidireccionales, por ejemplo, una llamada unidad de captura de datos, una toma de red o un conmutador de red con duplicación de puertos (Port Mirroring), para implementar la transmisión unidireccional sin interferencia. en lugar de tener que usar diodos de datos de hardware muy caros adaptados para áreas especiales de aplicaciones y redes de seguridad, así como protocolos de red.

Conforme a la solución propuesta, cuando los datos de la red se transforman de un formato de datos de red a un formato de datos de transporte, se lleva a cabo una conversión de formato de protocolo de un protocolo de red que se usa en la primera zona de red para transmitir los datos de red, a un protocolo de transporte que se usa para transmitir los datos de red a la segunda zona de red. El protocolo de red admite comunicación bidireccional, mientras que el protocolo de transporte solo admite comunicación unidireccional.

Esto tiene la ventaja de que la transmisión a través de un diodo de datos no genera ni transmite datos a la primera zona de red. Esto asegura o mejora la ausencia de repercusión del diodo de datos. En este contexto, la ausencia de repercusión significa que no se introducen datos de mensajes u otros "bits de contaminación" en la primera zona de red debido a la transmisión de los datos de transporte a la segunda zona de red.

En un modo de realización ventajoso, la información sobre el protocolo de red usado se introduce en el formato de datos de transporte.

El formato de datos de transporte incluye, por lo tanto, información suficiente sobre el protocolo de red para permitir una transformación inversa solo de esta información. De este modo se logran el desacoplamiento de la transmisión de datos entre la primera zona de red y la transmisión unidireccional de los datos en la segunda zona de red y la evaluación de los datos en una segunda zona de red remota.

En un modo de realización ventajoso, los datos se codifican de forma redundante durante la transformación y/o se añaden códigos de detección de errores a los datos.

Esto reduce el riesgo de transmisión errónea o incompleta de los datos a la segunda zona de red.

En un modo de realización ventajoso, los datos están protegidos criptográficamente durante la transformación, en particular se añade una suma de verificación criptográfica y/o los datos se encriptan.

Mediante una suma de verificación criptográfica correspondiente y/o el encriptado de los datos durante la transformación del formato de datos de red al formato de datos de transporte, los datos ya están protegidos contra la manipulación durante la transmisión a través de una unidad de transmisión unidireccional. Si el atacante no puede escuchar o ramificar los datos en formato de datos de transporte, el atacante no puede leer los datos en texto plano o manipular los datos sin ser detectado.

En un modo de realización ventajoso, se usa una conexión de comunicación protegida criptográficamente para transmitir los datos en el formato de datos de transporte a la segunda zona de red.

Por ejemplo, los datos se transmiten en el formato de datos de transporte a través de un enlace de comunicación según el protocolo de seguridad de la capa de transporte TLS dentro de la segunda zona de red. Dicha conexión de comunicación se configura preferentemente mediante una puerta de enlace de datos separada de un dispositivo de transmisión unidireccional para evitar una obligación de certificación y aprobación. De esta manera, en particular, un modo de realización del protocolo de seguridad puede actualizarse (parchearse) rápidamente si se conocen vulnerabilidades. Por tanto, se transmiten datos en el formato de datos de transporte así como datos de usuario a un servidor de aplicación, es decir, un servicio web, a través de un protocolo de red convencional. Esto garantiza que la solución sea altamente compatible con las tecnologías de Backend existentes. En lugar de o además del protocolo de seguridad de la capa de transporte TLS, también se pueden usar otros protocolos de seguridad para transmitir los datos en formato de datos de transporte a través de un enlace de comunicación dentro de la segunda zona de red, por ejemplo, IPsec/IKEv2, S/MIME, sintaxis de mensajes criptográficos (CMS), cifrado web JSON (JWE), JSON Web Signature (JWS).

Un segundo aspecto de la presente invención se refiere a un dispositivo de transmisión para la transmisión sin repercusión y unidireccional de datos desde una primera zona de red a una segunda zona de red para la evaluación en un servidor de aplicación remoto, que presenta los siguientes componentes: un dispositivo de exportación de datos que está dispuesto en la primera zona de red y que está diseñado para recopilar los datos que se transmiten en un formato de datos de red en la primera zona de red y para transformar los datos del formato de datos de red a un formato de datos de transporte, una unidad de transmisión de datos unidireccional que está diseñada para transmitir unidireccionalmente los datos en el formato de datos de transporte a la segunda zona de red, y un dispositivo de importación de datos que está diseñado para retransformar los datos desde el formato de datos de transporte al formato de datos de red y para transmitir los datos a un servidor de aplicación, en el que el dispositivo de importación de datos y los servidores de aplicaciones están dispuestos en una segunda zona de red separada de la primera zona, en el dispositivo de exportación de datos está configurado además para convertir los datos de red del formato de datos de red al formato de datos de transporte al convertir un formato de protocolo de un protocolo de red que se usa en la primera zona de red para transmitir los datos de red, en un protocolo de transporte que se usa para transmitir los datos de la red a la segunda zona de red, en el que el protocolo de red permite la comunicación bidireccional y el protocolo de transporte solo permite la comunicación unidireccional.

El dispositivo de importación de datos y el servidor de aplicación no necesariamente tienen que estar dispuestos en una zona de red común. También pueden estar dispuestos en diferentes zonas de red que son diferentes de la primera zona de red. Esto hace posible implementar una implementación menos compleja y menos costosa de un diodo de datos unidireccional sin repercusión para aplicaciones industriales y una solución de seguridad de dominio cruzado basada en un diodo de datos.

En un modo de realización ventajoso, el dispositivo de transmisión está diseñado para llevar a cabo el procedimiento reivindicado.

En un modo de realización ventajoso, el dispositivo de importación de datos está diseñado para llevar a cabo al menos una transformación adicional de los datos del formato de datos de red a un formato de datos adicional.

Como resultado, el formato de datos ya se puede adaptar en la unidad de importación de datos para su evaluación por aplicaciones de aplicación o el servidor de aplicación. Por tanto, los datos pueden estar disponibles de manera flexible para diferentes aplicaciones de aplicación o servidores de aplicación.

En un modo de realización ventajoso, el dispositivo de importación de datos está diseñado como parte del servidor de aplicación.

Además de un dispositivo de importación de datos que está separado espacialmente del servidor de aplicación y que está conectado a la primera zona de red dentro de la segunda zona de red, por ejemplo a través de Internet pública o una red de oficina, el dispositivo de importación de datos también se puede combinar ventajosamente como parte del servidor de aplicación. Esto reduce el número de componentes que se deben accionar y, por tanto, mantener y, por tanto, se pueden accionar de manera más rentable.

En un modo de realización ventajoso, el dispositivo de exportación de datos tiene una unidad de memoria para almacenar persistentemente los datos en la primera zona de red.

Por tanto, estos datos pueden recopilarse en la primera zona de red y usarse, por ejemplo, como datos de registro para la reconstrucción de la transmisión de datos en la primera zona de red.

En un modo de realización ventajoso, una toma de red, un puerto espejo de un conmutador de red o un diodo de datos pueden usarse como una unidad de transmisión de datos unidireccional. Una toma de red también puede denominarse unidad de captura de datos (DCU). El uso de un puerto espejo de un conmutador de red también se conoce como Port Mirroring.

Estas versiones de una unidad de transmisión de datos tienen propiedades particularmente buenas con respecto a la falta de repercusión.

En un modo de realización ventajoso, el dispositivo comprende adicionalmente una puerta de enlace de datos, que está diseñada para establecer una conexión de comunicación protegida criptográficamente para la transmisión de los datos en el formato de datos de transporte, al dispositivo de importación de datos.

Un tercer aspecto de la invención se refiere a un producto de programa informático, que se puede cargar directamente en la memoria de un ordenador digital, y comprende las partes de código de programa que son apropiadas para realizar las etapas del procedimiento según una de las reivindicaciones 1-7.

Ejemplos de realización del dispositivo según la invención y del procedimiento según la invención están representados a modo de ejemplo en los dibujos y se explican más en detalle mediante la descripción siguiente. Muestran:

La figura 1 una puerta de enlace de seguridad de dominio cruzado convencional según el estado de la técnica en una representación esquemática;

La figura 2 una puerta de enlace de datos sin repercusión para redes de control según el estado de la técnica en una representación esquemática;

La figura 3 un primer ejemplo de realización de un dispositivo de transmisión según la invención, en particular para redes de control, en una representación esquemática;

La figura 4 un segundo ejemplo de realización de un dispositivo de transmisión según la invención con un dispositivo de importación de datos integrado en un servidor de aplicación en una representación esquemática;

La figura 5 un tercer ejemplo de realización de un dispositivo de transmisión según la invención, diseñado como una puerta de enlace de seguridad de dominio cruzado en una representación esquemática;

La figura 6 un cuarto ejemplo de realización de un dispositivo de transmisión según la invención como una puerta de enlace de seguridad de dominio cruzado en una representación esquemática; y

La figura 7 un ejemplo de realización del procedimiento según la invención como un diagrama de desarrollo.

Las partes correspondientes entre sí están provistas en todas las figuras con las mismas referencias.

La figura 1 muestra una puerta de enlace de seguridad convencional de dominio cruzado 12 con dos enlaces de comunicación unidireccionales 1, 2 basados en los diodos de datos 8, 18. Las zonas de red conectadas 11, 13 se clasifican de manera diferente, de modo que, por un lado, hay una zona de red 13 con un bajo requisito de seguridad y, por otro lado, una zona de red 11 con un alto requisito de seguridad 11. Una transferencia de datos en el enlace de comunicación unidireccional 1 a partir de la segunda zona de red 13 con una clasificación de seguridad "interna" es posible en la dirección de la primera zona de red 11 con requisitos de alta seguridad y una clasificación como "confidencial", siempre que un escáner de virus 16 no reconozca el contenido de los datos como malicioso. El uso del diodo de datos 18 requiere un convertidor bidireccional a unidireccional 15 para convertir un protocolo de comunicación bidireccional, por ejemplo un protocolo de control de transmisión TCP, en un protocolo de comunicación unidireccional, por ejemplo el protocolo de datagramas de usuario UDP, para la transmisión a través del diodo de datos 18. Después del diodo de datos 18, el protocolo unidireccional debe

convertirse de nuevo en un protocolo de comunicación bidireccional mediante un convertidor de protocolo unidireccional a bidireccional 14.

En la dirección opuesta en el enlace de comunicación unidireccional 2 desde la primera zona de red 11 a la segunda zona de red 13, la transferencia de datos solo es posible si los datos a transmitir o un documento a transmitir puede desclasificarse con éxito en un dispositivo de desclasificación 7, por ejemplo, de la clasificación en "Confidencial" a "Interno" según reglas de desclasificación predefinidas. Los datos se transforman luego en un convertidor bidireccional a unidireccional 5 y se transfieren a través del diodo de datos 8 a un convertidor unidireccional a bidireccional 4 y se retransforman. Los datos en sí son enviados o recibidos por el usuario C1 en la primera zona de red 11 o el usuario C2 en la segunda zona de red 13.

La figura 2 muestra ahora una solución convencional por medio de una puerta de enlace de datos unidireccional sin repercusión 22 para la exportación unidireccional sin repercusión de datos desde una red de seguridad, que aquí corresponde a una primera zona de red 21, a un servidor de aplicación 29, que está conectado a través de una red pública 24, por ejemplo, Internet o red de oficinas. La red pública 24 y el servidor de aplicación de Backend 29 se encuentran, por tanto, en una segunda zona de red 23.

Un dispositivo de transmisión de datos 25 en la primera zona de red 21 recopila datos de diagnóstico de, por ejemplo, dispositivos de control S1 y transmite la imagen de datos actual, por ejemplo, como un archivo o como un objeto de datos binarios, también llamado blob binario, cíclicamente a un dispositivo de recepción de datos 27 a través de una unidad de transmisión de datos 26 que garantiza la ausencia de repercusión.

El dispositivo de transmisión de datos 25 también puede denominarse proveedor de datos unidireccional o editor unidireccional (Oneway-Data-Provider o Oneway-Publisher). Un dispositivo receptor de datos 27 recibe los datos transmitidos a través de la unidad de transmisión de datos unidireccional 26 y también puede denominarse receptor unidireccional o suscriptor unidireccional (Oneway-Recipient o Oneway-Subscriber). El dispositivo de transmisión de datos 25 comprende una función de exportación unidireccional para hacer que el stock de datos esté disponible para el dispositivo de recepción de datos 27, por ejemplo, como un objeto de datos binarios. El dispositivo receptor de datos 27 tiene una función de importación para importar e interpretar el stock de datos recibido y transmitir los datos de diagnóstico contenidos en el mismo, por ejemplo a través de una puerta de enlace de datos 28, al servidor de aplicación 29. Los programas de aplicación 30, 31, 32 para evaluar los datos transmitidos están contenidos en el servidor de aplicación 29.

La figura 3 muestra ahora un ejemplo de realización según la invención de un dispositivo 102 de transmisión de datos sin repercusión en un entorno industrial correspondiente a la figura 2. En este caso, los datos de los usuarios o dispositivos de control S1 deben transmitirse en una primera zona de red 21 a una segunda zona de red 23 para la evaluación en un servidor de aplicación 29. La transmisión tiene lugar dentro de la segunda zona de red 23, por ejemplo a través de una segunda puerta de enlace de datos 28 y a través de una red pública 24 con poca relevancia de seguridad.

El dispositivo de transmisión unidireccional 102 comprende un dispositivo de exportación de datos 105, una unidad de transmisión de datos unidireccional 106 y un dispositivo de importación de datos 107, que se diseña por separado del dispositivo de exportación de datos 105 y de la unidad de transmisión de datos 106 en la segunda zona de red 23. El dispositivo de importación de datos 107 está dispuesto, por ejemplo, en una zona de aplicación, a menudo también denominada nube.

En el dispositivo de exportación de datos 105, los datos a transmitir se almacenan de forma persistente dentro de la primera zona de red 21, por ejemplo, en una memoria de datos. Los datos se transmiten dentro de la primera zona de red 21 a través de una conexión de red según un protocolo de red. Los datos están en un formato de datos de red 110. Los protocolos de red típicos de la primera zona de red 21 son, por ejemplo, el protocolo OPC Unified Architecture (OPC UA) para la transmisión de datos de la máquina o un protocolo syslog para la transmisión de mensajes de registro.

En una unidad de exportación de datos 105, que se asigna a la primera zona de red, los datos ahora se registran en el formato de datos de red 110 y se transforman a un formato de datos de transporte 111 correspondiente a un protocolo de transporte. Aquí, tiene lugar una conversión de un protocolo de red bidireccional a un formato de datos de transporte 111, que es adecuado para la transmisión a través del enlace unidireccional por la unidad de transmisión de datos unidireccional 106. Además de una conversión de formato de protocolo, los datos se codifican opcionalmente de forma redundante para que sea posible corregir los errores de transmisión, y se añaden códigos de detección de errores o sumas de verificación criptográficas para que los errores de transmisión o .la manipulación puedan identificarse y/o los datos se encripten.

El formato de datos de transporte 111 contiene información sobre el protocolo de red usado en la primera zona de red 21. Como resultado, el dispositivo de importación de datos 107 puede realizar una retransformación del formato de datos de transporte al formato de datos de red.

Por ejemplo, un encabezado de un paquete de datos en formato de datos de transporte 111 contiene metadatos, que además de la información sobre el protocolo de red, una marca de tiempo, información original tal como una dirección IP. Los datos disponibles en el formato de datos de transporte 111 se dividen, preferentemente, en paquetes de datos parciales más pequeños para el desacoplamiento por la unidad de transmisión de datos 106. Cada paquete de datos parcial contiene metadatos adicionales, como por ejemplo un identificador de transferencia, un identificador de transmisor que admite una función de publicación-suscripción en el lado receptor, así como un número de paquete o sumas de verificación para detectar errores de transmisión y/o integridad. Estos paquetes de datos parciales terminan en el lado de salida de la unidad de transmisión de datos 106 o en la segunda puerta de enlace de datos 28, los datos se convierten al formato de transferencia de datos 111 y se emiten.

Se puede llevar a cabo una conversión de formato de datos adicional en el dispositivo de importación de datos 107 para adaptar los datos de forma correspondiente a los requisitos de un servicio de evaluación posterior.

El formato de datos que emite el dispositivo de importación de datos 107 puede corresponder al formato de datos en la primera zona de red 21. Sin embargo, también es posible que el formato de datos emitido por el dispositivo de importación de datos 107 sea diferente del formato de datos en la primera zona de red 21. Por ejemplo, se puede usar OPC UA como formato de datos en la primera zona de red 21, mientras que el dispositivo de importación de datos 107 genera un formato de datos JSON.

En una variante, el dispositivo de importación de datos 107 emite los datos si la suma de verificación de los datos recibidos asignados se puede verificar correctamente. En una variante adicional, el dispositivo de importación de datos 107 emite los datos junto con información adicional que indica si la suma de verificación de los datos recibidos asignados es correcta.

La unidad de transmisión de datos unidireccional 106 ahora transmite los datos en el formato de datos de transporte 111 y los envía, por ejemplo, a una puerta de enlace de datos 28 que establece una conexión segura con la unidad de importación de datos 107. Por ejemplo, una conexión TLS convencional según el protocolo de seguridad de la capa de transporte se puede usar como una conexión de datos segura. En esta conexión TLS, los datos permanecen en el formato de datos de transporte 111.

La unidad de transmisión de datos unidireccional 106 se puede diseñar como un dispositivo de desacoplamiento de datos, por ejemplo, una toma de red o una unidad de captura de datos de red, a través de un puerto espejo de un conmutador de red, que también pasa los datos presentes en el puerto espejo de forma idéntica a un puerto de salida, o mediante un diodo de red con, por ejemplo, una fibra óptica, para transmisión de datos unidireccional. La unidad de transmisión de datos unidireccional 106 hace que los datos estén disponibles fuera de la primera zona de red 21 cerrada y crítica para la seguridad.

A diferencia del estado de la técnica, fuera de la unidad de transmisión de datos unidireccional 106, el formato de datos de transporte 111 no se reconvierte en el formato de datos de red 110, sino que se retransmite en el formato de datos de transporte 111.

En la unidad de importación de datos 107, los datos en el formato de datos de transferencia 111 se retransforman al formato de datos de red 110 y se ponen a disposición de un programa de evaluación 30, 31, 32 en un servidor de aplicación 29.

La figura 4 muestra un modo de realización adicional de un dispositivo de transmisión unidireccional 202, en el que el dispositivo de importación de datos 207 se implementa como integrado en un servidor de aplicación 203. El dispositivo de importación de datos 207 también puede cargarse como una aplicación en la nube en un servidor de aplicación 203 y ejecutarse allí. En dicho servidor de aplicación 203, por ejemplo, un Backend de IoT, la funcionalidad se puede implementar en forma de una aplicación en la nube.

La figura 5 muestra un modo de realización del dispositivo de transmisión unidireccional 312 en una solución de puerta de enlace de seguridad de dominio cruzado. Aquí, en la segunda zona de red 313, se usa un convertidor unidireccional a bidireccional remoto 304 basado en Internet, que corresponde a los dispositivos de importación de datos 105 de un dispositivo de transmisión unidireccional 102, para un enlace de transmisión 2 desde la primera zona de red 311 a la segunda zona de red 313. Como en los modos de realización ejemplares anteriores, el convertidor unidireccional a bidireccional 304 es un componente lógico del dispositivo de transmisión 312, pero está espacialmente separado de un convertidor bidireccional a unidireccional 305 y un diodo de datos 308. En una variante adicional (no mostrada), los datos transmitidos unidireccionalmente se transmiten (tunelizados) durante la transmisión a través del enlace de transmisión 2 a la segunda zona de red 313 a través de una conexión de comunicación de datos bidireccional al convertidor unidireccional a bidireccional 304 basado en Internet. Para este propósito, se puede proporcionar un componente de tunelización separado (no mostrado), que está dispuesto entre el diodo de datos 308 y el enlace de transmisión 2. Este puede, por ejemplo, transmitir tramas UDP transmitidas unidireccionalmente a través de un canal de comunicación TCP o un canal de comunicación TLS.

Del mismo modo, un convertidor bidireccional a unidireccional 315, correspondiente a un dispositivo de exportación de datos 105, se usa como una unidad separada en la segunda zona de red 313 para el enlace de transmisión 1 desde la segunda zona de red 313 a la primera zona de red 311. Un convertidor unidireccional a bidireccional 304, 312 realiza la conversión unidireccional a bidireccional 304, 312, y corresponde a un dispositivo de exportación de datos 105 en las figuras 3 y 4. Del mismo modo, un escáner de virus 316 puede diseñarse como un servicio de red.

Los convertidores unidireccional a bidireccional 304 o los convertidores bidireccional a unidireccional 315 tienen, por tanto, un diseño más simple ya que solo se debe implementar una función de recepción o función de transmisión. Esto permite, en particular, una extensión simple para nuevos protocolos o el cierre de puntos débiles en las pilas de protocolos usadas del convertidor unidireccional a bidireccional 304 o el convertidor bidireccional a unidireccional 315.

A diferencia del estado de la técnica, como se sabe por las soluciones de seguridad de dominio cruzado basadas en diodos de datos de hardware, no es necesaria la reconversión después de la transmisión unidireccional antes de que los datos se transmitan, por ejemplo, a un sistema de Backend basado en la nube que está dispuesto en una segunda zona de red 313, 413 con un requisito de seguridad menor. En cambio, la transmisión puede transmitirse al sistema de Backend basado en la nube a través de una conexión de red convencional y solo allí transformarse y transmitirse a un servidor de aplicación para su evaluación. Como resultado, se pueden usar servicios redundantes basados en la nube, por ejemplo con conmutación por error automática, en el servidor de aplicación. La implementación del procedimiento por medio de dicha implementación técnica comprende, por lo tanto, menos componentes que deben mantenerse y también certificarse, de modo que la solución es menos compleja que los procedimientos convencionales. Esto hace que el procedimiento y el dispositivo correspondiente sean más rentables y más fáciles de integrar en las infraestructuras existentes.

La figura 6 muestra una variante en la cual el convertidor unidireccional a bidireccional 414, que corresponde al convertidor unidireccional a bidireccional integrado 314 en la figura 5, y el convertidor bidireccional a unidireccional 405, que corresponde al convertidor bidireccional a unidireccional integrado 305 en la figura 5, se implementan en la primera zona de red 403, por ejemplo, como parte de un centro de datos de alta seguridad. Aquí también, en una variante de implementación adicional, se puede proporcionar un componente de tunelización adicional para los diodos de datos 408, 418, que convierte los datos transmitidos unidireccionalmente en un enlace de comunicación bidireccional, por así decirlo, tunelizado.

La figura 7 muestra las etapas del procedimiento individual para la transmisión unidireccional sin repercusión de datos desde una primera zona de red 21, 311, 411 a una segunda zona de red 23, 313, 413 para evaluación en un servidor de aplicación remoto 29, 203. En una primera etapa de procedimiento 501, los datos que se transmiten en un formato de datos de red en la primera zona de red 21, 311, 411 se registran en esta primera zona de red 21, 311, 411. En la etapa de procedimiento 502, los datos se transforman de un formato de datos de red a un formato de datos de transporte y, en la etapa de procedimiento 503, se transmiten unidireccionalmente en el formato de datos de transporte 111 a la segunda zona de red 23, 313, 413. En la segunda zona de red 23, 313, 413, los datos se retransforman 504 desde el formato de datos de transporte al formato de datos de red. Esta retransformación tiene lugar en una segunda zona de red separada de la primera zona de red y transmite los datos en formato de datos de red a un servidor de aplicación, véase la etapa 505 para la evaluación.

Todas las características descritas y/o dibujadas se pueden combinar ventajosamente entre sí en el marco de la invención. La invención no está limitada a los ejemplos de realización descritos.

REIVINDICACIONES

1. Procedimiento para la transmisión unidireccional sin repercusión de datos desde una primera zona de red (21, 311, 411) a una segunda zona de red (23, 313, 413) para la evaluación en un servidor de aplicación remoto (29, 203), realizada por un dispositivo de transmisión y con las etapas de procedimiento:

- capturar (501) los datos que se transmiten en un formato de datos de red (110) en la primera zona de red (21, 311, 411),

- transformar (502) los datos del formato de datos de red (110) en un formato de datos de transporte (111),

- transmitir unidireccionalmente (503) los datos en el formato de datos de transporte (111) a la segunda zona de red (23, 313, 413),

- retransformar (504) los datos del formato de datos de transporte (111) al formato de datos de red (110), y

- transmitir los datos (505) a un servidor de aplicación (29, 203),

en el que la retransformación (504) se lleva a cabo en una segunda zona de red (23, 313, 413) que está espacialmente separada de la primera zona de red (21, 311, 411),

caracterizado por que

durante la transformación (502) de los datos de red del formato de datos de red (110) al formato de datos de transporte (111) se lleva a cabo una conversión de formato de protocolo de un protocolo de red usado en la primera zona de red (21, 311, 411) para transmitir los datos de red a un protocolo de transporte usado para la transmisión de los datos de red a la segunda zona de red (23, 313, 413), en la que el protocolo de red permite la comunicación bidireccional y el protocolo de transporte permite solamente la comunicación unidireccional.

2. Procedimiento según la reivindicación 1, en el que la información sobre el protocolo de red usado se introduce en el formato de datos de transporte (111).

3. Procedimiento según una de las reivindicaciones anteriores, en el que durante la transformación (502) los datos se codifican de forma redundante y/o se añaden códigos de detección de errores a los datos.

4. Procedimiento según una de las reivindicaciones anteriores, en el que los datos se protegen criptográficamente durante la transformación (502), en particular añadiendo una suma de verificación criptográfica y/o encriptando los datos.

5. Procedimiento según una de las reivindicaciones anteriores, en el que se usa un enlace de comunicación (109) protegido criptográficamente para transmitir los datos en el formato de datos de transporte (111) a la segunda zona de red (23, 313, 413).

6. Procedimiento según una de las reivindicaciones anteriores, en el que la primera zona de red (21, 311, 411) es una red con requisitos de alta seguridad y la segunda zona de red (23, 313, 413) es una red con requisitos de baja seguridad.

7. Dispositivo de transmisión para la transmisión unidireccional sin repercusión de datos desde una primera zona de red (21, 311, 411) a una segunda zona de red (23, 313, 413) para la evaluación en un servidor de aplicación remoto (29, 203, 316, 416), que comprende:

− un dispositivo de exportación de datos (105, 305, 405) que está dispuesto en la primera zona de red (21, 311, 411) y que está diseñado para registrar los datos que se transmiten en un formato de datos de red (110) en la primera zona de red (21, 311, 411), y para transformar los datos del formato de datos de red (110) a un formato de datos de transporte (111),

− una unidad de transmisión unidireccional de datos (106, 308, 408), que está diseñada para transmitir unidireccionalmente los datos en formato de datos de transporte (111) a la segunda zona de red (23, 313, 413)

− un dispositivo de importación de datos (107, 207, 304, 404) que está diseñado para retransformar los datos del formato de datos de transporte (111) al formato de datos de red (110) y transmitir los datos a un servidor de aplicación (29, 203), en el que el dispositivo de importación de datos y el servidor de aplicación

(29, 203, 316, 416) están dispuestos en una segunda zona de red (23, 313, 413) espacialmente separada de la primera zona (21, 311, 411),

caracterizado por que

el dispositivo de exportación de datos (105, 305, 405) está configurado además para, durante la transformación de los datos de red del formato de datos de red (110) al formato de datos de transporte (111), llevar a cabo una conversión de formato de protocolo de un protocolo de red usado en la primera zona de red (21, 311, 411) para transmitir los datos de red a un protocolo de transporte usado para la transmisión de los datos de red a la segunda zona de red (23, 313, 413), en la que el protocolo de red permite la comunicación bidireccional y el protocolo de transporte permite solamente la comunicación unidireccional.

8. Dispositivo según la reivindicación 7, en el que el dispositivo está diseñado para llevar a cabo el procedimiento según las reivindicaciones 1 a 6.

9. Dispositivo según una de las reivindicaciones 7 a 8, en el que el dispositivo de importación de datos (107, 207) está diseñado para llevar a cabo al menos una transformación adicional de los datos del formato de datos de red (110) a un formato de datos adicional.

10. Dispositivo según una de las reivindicaciones 7 a 9, en el que el dispositivo de importación de datos (207) está diseñado como parte del servidor de aplicación (203).

11. Dispositivo según una de las reivindicaciones 7 a 10, en el que el dispositivo de exportación de datos (105, 205) presenta una unidad de memoria para almacenar de forma persistente los datos en la primera zona de red (21).

12. Dispositivo según una de las reivindicaciones 7 a 11, en el que una toma de red, un puerto espejo de un conmutador de red o un diodo de datos puede usarse como la unidad de transmisión de datos unidireccional (106, 308, 408).

13. Dispositivo según una de las reivindicaciones 7 a 12, que comprende una puerta de enlace de datos (28) que está diseñada de modo que establece una conexión de comunicación protegida criptográficamente para la transmisión de los datos, en particular en el formato de datos de transporte, al dispositivo de importación de datos (107, 207).

14. Producto de programa informático, que se puede cargar directamente en una memoria de un ordenador digital, que comprende las partes de código de programa que son apropiadas para realizar las etapas del procedimiento según una de las reivindicaciones 1 a 6.

FIG 1

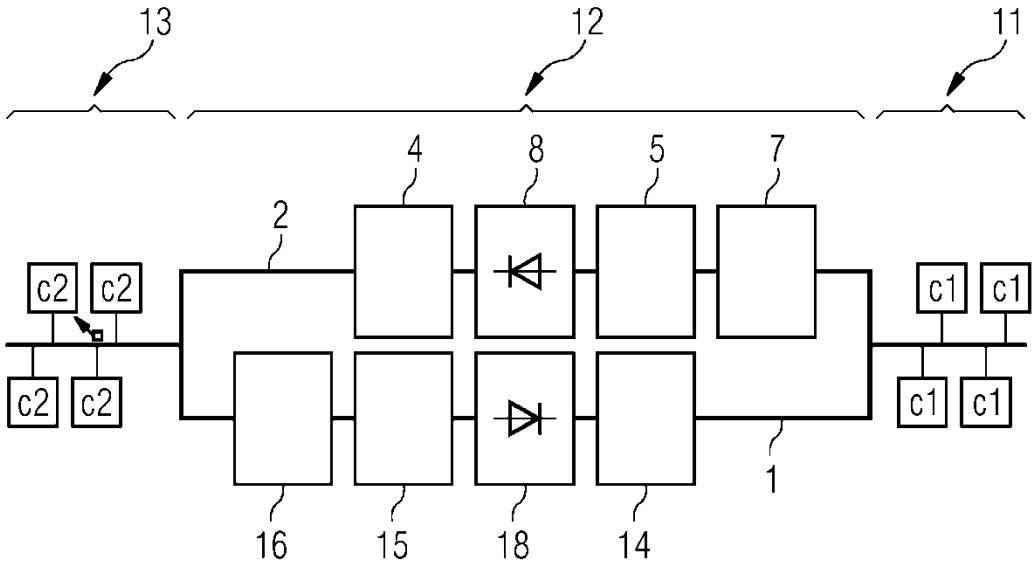

13
12
11
4
8
5
7
2
c2
c2
c2
c2
c1
c1
c1
c1
1
16
15
18
14

FIG 2

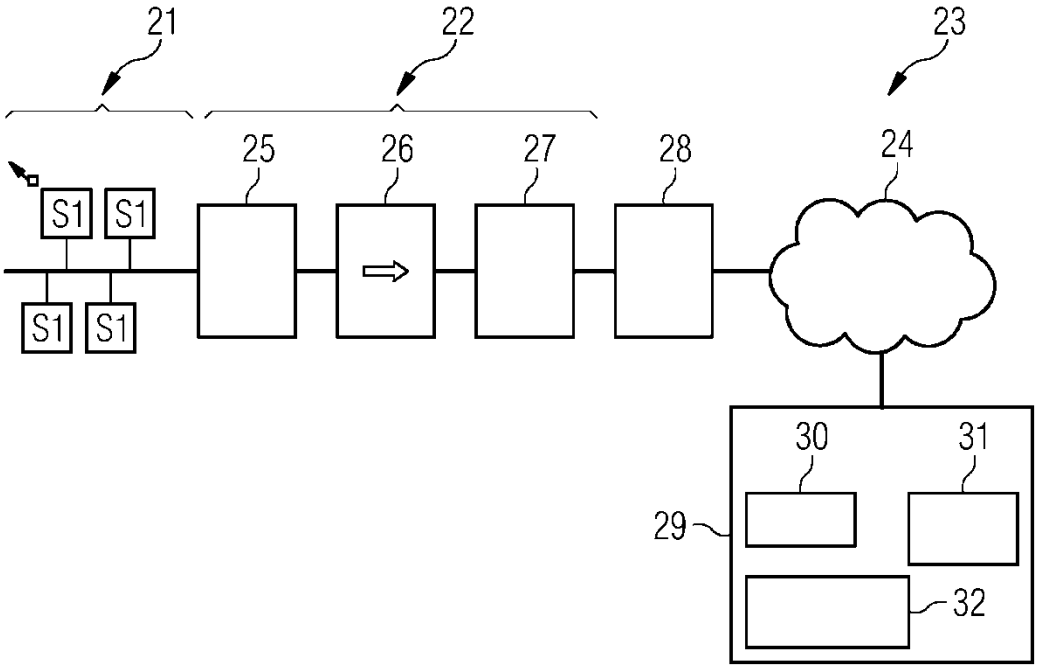

21
22
23
25
26
27
28
24
S1
S1
S1
S1
30
31
29
32

FIG 3

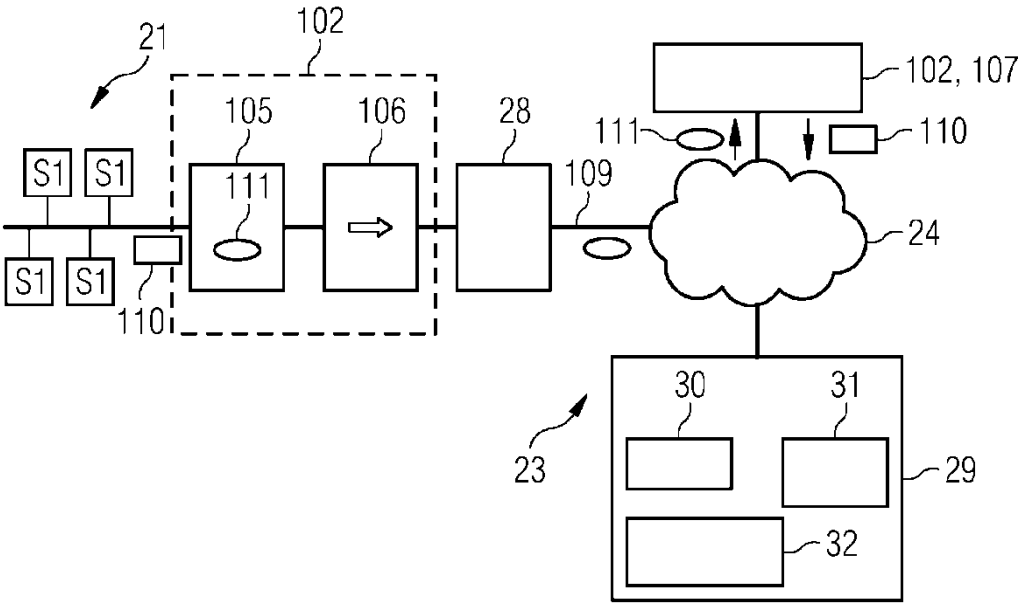
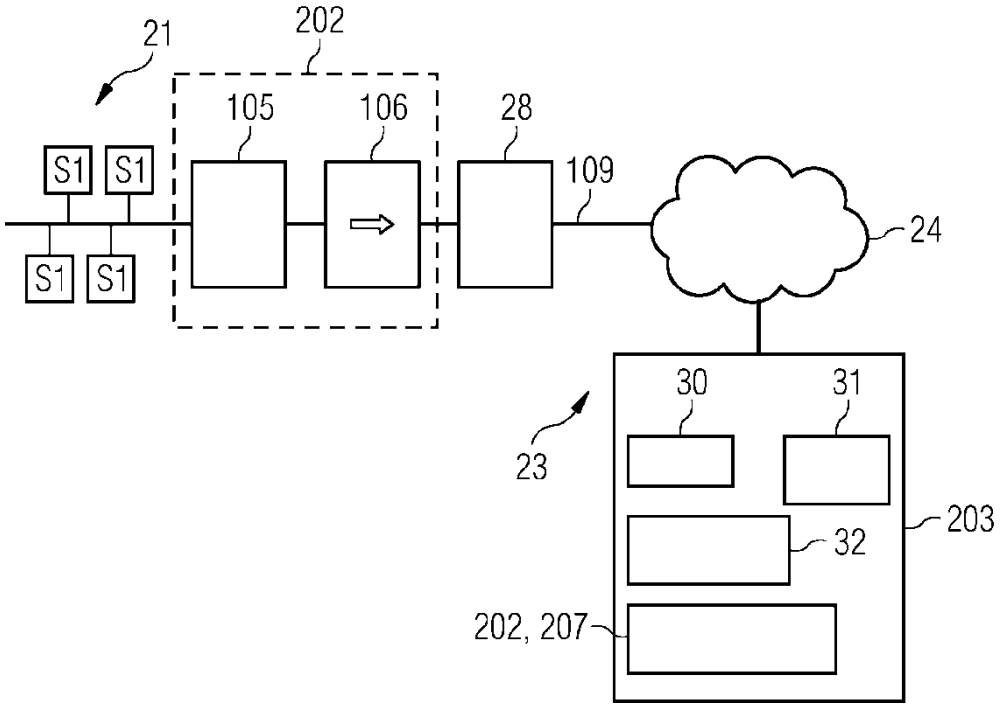

21
102
105
106
28
111
110
102, 107
S1
S1
S1
S1
111
109
24
110
30
31
23
29
32

FIG 4


21
202
105
106
28
S1
S1
S1
S1
109
24
30
31
23
203
32
202, 207

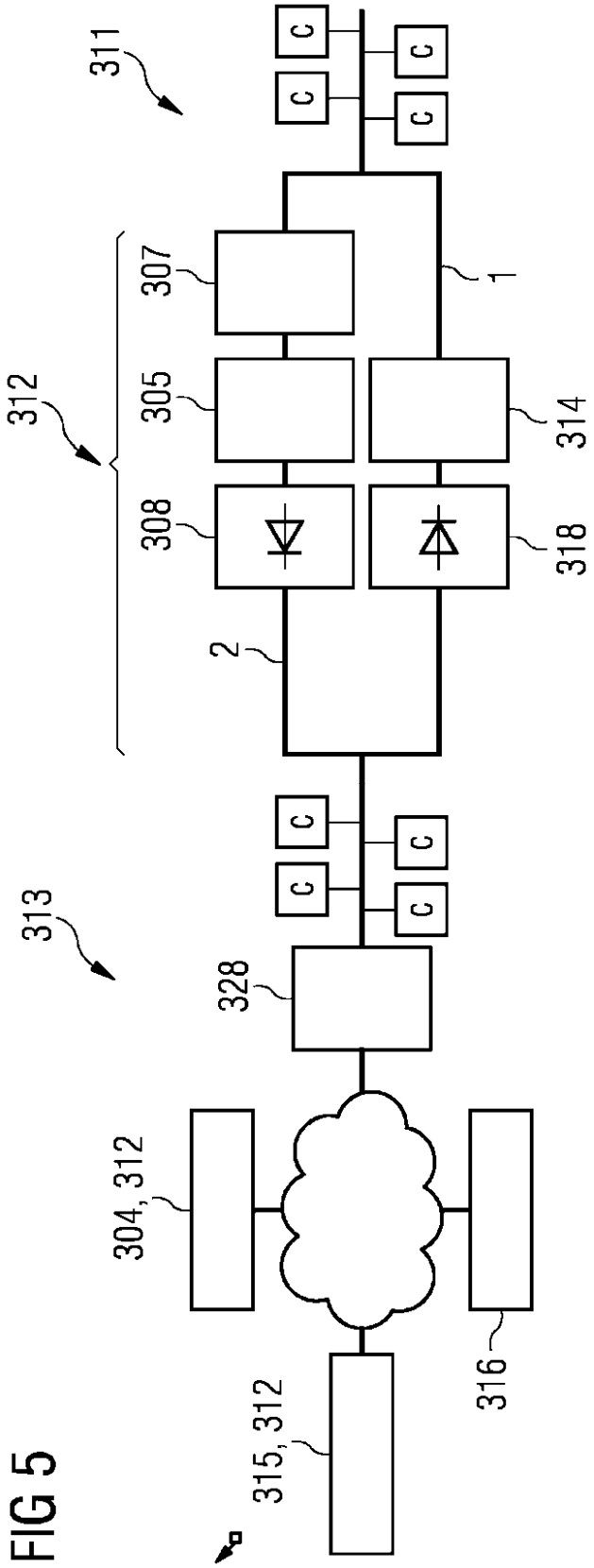

311
C
C
C
C
307
1
312
305
314
308
318
2
313
C
C
C
C
328
304, 312
316
315, 312

FIG 5

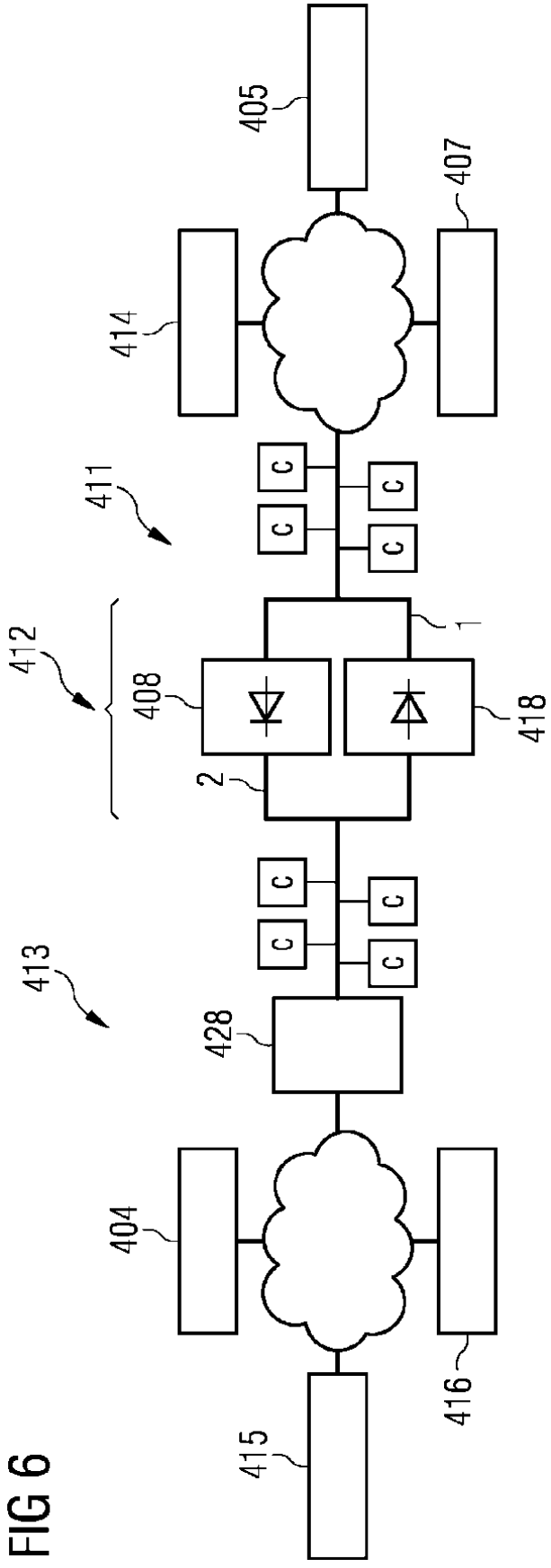


FIG 6

FIG 7