(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 716 736**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **18.03.2016 PCT/EP2016/055915**

(87) Fecha y número de publicación internacional: **06.10.2016 WO16156063**

(96) Fecha de presentación y número de la solicitud europea: **18.03.2016 E 16711582 (3)**

(97) Fecha y número de publicación de la concesión europea: **19.12.2018 EP 3245775**

(54) Título: **Dispositivo de acoplamiento de sentido único con dispositivo de interceptación para la transmisión de datos sin retroacción**

(30) Prioridad:

31.03.2015 DE 102015205833

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.06.2019

(73) Titular/es:

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

(72) Inventor/es:

BLÖCHER, UWE;
FALK, RAINER;
REINERT, JENS;
TANG, WEN y
WIMMER, MARTIN

(74) Agente/Representante:

LOZANO GANDIA, José

DESCRIPCIÓN

DISPOSITIVO DE ACOPLAMIENTO DE SENTIDO ÚNICO CON DISPOSTIVO DE INTERCEPTACIÓN PARA LA TRANSMISIÓN DE DATOS SIN RETROACCIÓN

La invención se refiere a un dispositivo de acoplamiento de sentido único, un equipo de consulta, un procedimiento, así como un producto de programa informático para la transmisión de datos sin retroacción de al menos un dispositivo, que está dispuesto en una primera red con exigencia de seguridad elevada, a una segunda red con menor exigencia de seguridad.

Las soluciones de seguridad para la transferencia de datos entre redes con diferentes exigencias de seguridad, así denominadas soluciones de seguridad de dominio cruzado, se usan hasta ahora sólo para sectores especiales, como comunicación con autoridades, en donde tienen validez exigencias de seguridad elevadas y en donde está presente una clasificación de seguridad de los documentos o informaciones. Mediante la solución de dominio cruzado se implementa un intercambio seguro automatizado de documentos y mensajes, como por ejemplo también correos electrónicos, entre zonas de seguridad de diferente nivel. A este respecto, una exigencia decisiva es que los datos sólo se transmitan de la zona con mayores exigencias de seguridad a la zona con menores exigencias de seguridad y a este respecto no se introduzcan nuevamente nuevos datos en la transmisión en la red con mayor exigencia de seguridad, ni se modifican los datos dentro de la red con exigencia de seguridad elevada por el intercambio. A este respecto, un componente esencial es un diodo de datos, que asegura la unidireccionalidad de la comunicación de datos.

Por el documento US 2012/291089 se conoce, por ejemplo, una solución para el intercambio seguro de datos entre dos zonas de seguridad. A este respecto, una unidad de gestión de datos está conectada tanto con la primera como también la segunda zona de seguridad, que tiene en cuenta las reglas de seguridad de ambos dominios.

También se conocen diodos de datos, que implementan físicamente una comunicación de sentido único. Para el soporte de una transmisión de datos con protocolos de transmisión de datos bidireccionales, como por ejemplo TCP, se conoce permitir un canal de retorno limitado extremadamente para la transmisión de los mensajes de confirmación. Alternativamente a ello en el documento US 7,675,867, el protocolo se termina en un servidor proxy y se transmite, por ejemplo, mediante un corrector de errores hacia delante a través del recorrido de transmisión unidireccional.

Finalmente se debe indicar el documento US2015/016256-A1en el que se presenta una técnica de acoplamiento que satisface las exigencias de seguridad.

Además se menciona el documento US2003/202663-A1 que igualmente describe un sistema electrónico de envío de mensajes que trabaja con elevada seguridad.

Para garantizar un intercambio de datos sin retroacción de una red de control crítica respecto a la seguridad, por ejemplo, una red de seguridad de vía, a una red menos crítica, como por ejemplo, una red de diagnóstico o una red de oficina, con frecuencia también se deben tener en cuenta los estándares internacionales, como por ejemplo el ISO/IEC 62443, que establece una estricta exigencia respecto al intercambio de datos entre las zonas de seguridad.

Por consiguiente, el objetivo de la presente invención es proporcionar un procedimiento y dispositivos para una transmisión de datos correspondiente, que garanticen por un lado la libertad frente a retroacción de la transmisión de datos y se puedan implementar por otro lado de forma sencilla. Además se puede utilizar un dispositivo semejante o un procedimiento semejante de forma flexible en distintos sectores de aplicación.

El objetivo se consigue mediante las medidas descritas en las reivindicaciones independientes. En las reivindicaciones dependientes están representados perfeccionamientos ventajosos de la invención.

El dispositivo de acoplamiento de sentido único según la invención para la transmisión de datos sin retroacción de al menos un dispositivo, que está dispuesto en una red con exigencia de seguridad elevada, a una segunda red con menor exigencia de seguridad contiene un equipo de consulta, un equipo de escucha y un equipo de recepción. El equipo de consulta está configurado para proporcionar una primera conexión de comunicación dentro de la primera red con al menos un dispositivo y además consultar los primeros datos del al menos un dispositivo y a continuación transmitir los primeros datos a través de una segunda conexión de comunicación en un bucle de línea separado entre dos interfaces del equipo de consulta. El equipo de escucha está configurado para escuchar los datos en la segunda conexión de comunicación externa y transmitirlos al equipo de recepción, que está dispuesto en la segunda red.

Bajo el equipo de escucha se entiende a este respecto el equipo, que copia el flujo de datos, que se transmite a través de la línea de conexión escuchada, y emite la copia del flujo de datos. A este respecto no tiene lugar en particular una evaluación, procesamiento de contenido o conversión de los datos del flujo de datos. Los datos se emiten a través del equipo de recepción que está conectado con una segunda red.

Esto tiene la ventaja de que se garantiza la libertad frente a retroacción. Por otro lado, a través de la conexión de comunicación entre el equipo de consulta y uno o varios dispositivos en la primera red se pueden consultar los datos deseados y a través del equipo de escucha y el equipo de recepción se pueden poner a disposición de la segunda red. A este respecto, la primera conexión de comunicación se extiende exclusivamente dentro de la primera red y se termina en el la menos un dispositivo y el equipo de consulta.

En una configuración ventajosa de la invención, el equipo de consulta presenta una primera unidad de protocolo para la terminación del al menos un protocolo de comunicación de la primera conexión de comunicación con el al menos un dispositivo. En particular presenta una terminación del protocolo OPC UA usado con frecuencia en redes de seguridad.

Esto tiene la ventaja de que en la unidad de consulta están presentes los primeros datos directamente de forma legible, es decir, sin otra información de protocolo o también encriptación. Esto facilita evaluar o reprocesar tales datos en el equipo de recepción o en otras unidades de evaluación de la segunda red. Se pueden usar diferentes protocolos también complejos para la conexión de comunicación de manera no modificada para la consulta. Para sistemas de seguridad se usa en particular el protocolo de arquitectura uniforme de la organización OPC, denominado protocolo OPC UA. A este respecto, la conexión de comunicación o la transmisión de datos correspondiente también puede estar asegurado de forma criptográfica. Dado que la conexión se termina en el equipo de consulta, también se conocen, por ejemplo, procedimientos y claves criptográficos, estipulados en un establecimiento de conexión entre las parejas de comunicación en la unidad de protocolo. Los primeros datos transmitidos de forma encriptada se decodifican por ello en la primera unidad de protocolo del equipo de consulta y por ello se transmiten de forma desencriptada a la segunda red a través de la segunda conexión de comunicación.

En otro ejemplo de realización, el equipo de consulta presenta una segunda unidad de protocolo para la facilitación de un segundo protocolo de comunicación para la transmisión de los primeros datos a través del bucle de conexión.

Esto tiene la ventaja de que los primeros datos ya se estructuran y transmiten a través del equipo de consulta según un segundo protocolo, que está presente por ejemplo en el equipo de recepción. El equipo de recepción no necesita por consiguiente una conversión de protocolo y puede estar configurado de forma menos compleja. Por consiguiente se puede realizar en particular una transmisión de datos evaluable de forma sencilla. Por consiguiente se pueden usar protocolos de diferente flexibilidad para la primera conexión de comunicación y una transmisión normalizada a través de la segunda conexión de comunicación. Por otro lado, la segunda conexión de comunicación se puede corresponder con el protocolo que se soporta en el equipo de recepción.

En una forma de realización ventajosa, el equipo de consulta presenta una unidad de conversión para la conversión de formato de los primeros datos.

En otra forma de realización ventajosa, el equipo de consulta presenta una unidad de memoria para el almacenamiento de los primeros datos.

Esto posibilita enviar los primeros datos en un formato de datos favorable para la unidad de recepción en la segunda red a través de la segunda conexión de comunicación y almacenarlos, por ejemplo, conforme a un formato de datos usado en una base de datos. Con ello es suficiente que el equipo de recepción sólo soporte un formato de datos determinado para la recepción y el reprocesamiento de los primeros datos.

En una forma de realización ventajosa, el equipo de escucha está configurado como copiador de datos, en particular una interceptación de red.

Esto tiene la ventaja de que se garantiza la unidireccionalidad de la transmisión de datos, dado que sólo se copian los datos de la segunda conexión de comunicación, pero no se pueden introducir los datos en la segunda conexión de comunicación o indirectamente en la primera conexión de comunicación desde la segunda red. Esto asegura simultáneamente la libertad frente a retroacción, dado que no tiene lugar una modificación de los primeros datos transmitidos en la segunda conexión de comunicación y ninguna modificación de los datos transmitidos en la primera conexión de comunicación. Tampoco se pueden introducir nuevos datos adicionales en la primera conexión de comunicación o segunda conexión de comunicación. Simultáneamente esto es un procedimiento fácilmente implementable.

Mediante el dispositivo de acoplamiento de sentido único se implementa por consiguiente una protección de tres escalones de la transmisión de datos sin retroacción. La conexión de comunicación cerrada forma el primer escalón en la primera red crítica respecto a la seguridad. La segunda conexión de comunicación constituye el segundo escalón. Ésta está separada físicamente de la primera conexión de comunicación y otros recorridos de transmisión de red en la primera red. Por consiguiente se excluye o al menos minimiza un entremezclado de los mensajes de la segunda conexión de comunicación en la primera conexión de comunicación. También se evita una influencia de los parámetros de calidad de transmisión de una transmisión de datos en la primera red, como por ejemplo, tiempos de retardo para un acceso a un canal. En general la unidad de consulta está dispuesta en una zona protegida y/o cerrada, por ejemplo, un armario de conmutación. Por consiguiente se dificulta una manipulación de la segunda conexión de comunicación.

El equipo de escucha configurado como interceptación de red o copiador de datos, que elabora una copia no modificada de los primeros datos y posibilita una transmisión desacoplada de la primera red a la segunda red, constituye el tercer escalón. Una infiltración de mensajes en el bucle de conexión a través de la unidad de escucha no es posible y no está prevista.

Si el dispositivo de acoplamiento de sentido único según la invención no se implementa en un área cerrada, por ejemplo, dentro de un armario de conmutación o dentro de un rack de red, se puede realizar de forma asegurada criptográficamente una transmisión de los primeros datos a través de la segunda conexión de comunicación, de modo que se dificulta o no es posible una escucha de los primeros datos.

Una unidad de consulta según la invención para la transmisión sin retroacción de los primeros datos del al menos un dispositivo en una primera red está configurada para proporcionar una primera conexión de comunicación dentro de la primera red con al menos un dispositivo y consultar por ello los primeros datos del la menos un dispositivo y a continuación transmitir los primeros datos a través de una segunda conexión de comunicación en un bucle de línea separado de una interfaz de salida del equipo de consulta directamente a una interfaz de entrada del equipo de consulta.

Esto tiene la ventaja de que el equipo de consulta está completamente integrado en la primera red y sirve para la consulta o también recopilación de informaciones de los dispositivos dentro de la primera red. Por consiguiente se pueden determinar los primeros datos, como por ejemplo una información de estado de instalaciones de seguridad dentro de la red de control de vía fuertemente asegurada. Por otro lado, a través de la segunda conexión de comunicación separada es posible una transmisión sencilla y sin retroacción en una segunda red con menores exigencias de seguridad. A este respecto, la primera y la segunda conexión de comunicación están separadas una de otra y por consiguiente ya constituyen dentro de la primera red un desacoplamiento completo de la primera red. Este desacoplamiento es igualmente la base para un uso flexible del equipo de consulta en redes aseguradas con primeros protocolos de comunicación diferentes.

El procedimiento según la invención para la transmisión de datos sin retroacción de al menos un dispositivo, que está dispuesto en una primera red con exigencia de seguridad elevada, a una segunda red con exigencia de seguridad baja presenta las siguientes etapas del procedimiento.

Una facilitación de una primera conexión de comunicación dentro de la primera red, una consulta y recepción de los primeros datos por al menos un dispositivo a través de la conexión de comunicación, una transmisión de los primeros datos a través de una segunda conexión de comunicación, una escucha de los primeros datos en la segunda conexión de comunicación y una transferencia de los primeros datos a la segunda red con exigencia de seguridad baja.

Mediante el procedimiento según la invención se transmiten los primeros datos desde una red relevante respecto a la seguridad sin retroacción a una segunda red con menor exigencia de seguridad. Esto se implementa de forma especialmente flexible y sencilla mediante la separación de la transmisión de datos a través de la primera conexión de comunicación y una segunda conexión de comunicación separada dentro de la primera red. Además, mediante la escucha se garantiza una transmisión fiable en sólo una dirección y concretamente de la primera red a la segunda red.

En un ejemplo de realización ventajoso se usa un primer protocolo de comunicación para la conexión de comunicación con el al menos un dispositivo, en particular el protocolo OPC UA, y/o se usa un segundo protocolo de comunicación para la transmisión de los primeros datos a través de la segunda conexión de comunicación.

Los diferentes protocolos en las dos conexiones de comunicación posibilitan un uso flexible del procedimiento en diferentes sectores de aplicación o redes de aseguramiento y automatización. Además, por ejemplo, siempre se puede usar un segundo protocolo de comunicación igual para la simplificación de la evaluación en una segunda red. Los primeros datos se convierten por ello de un primer protocolo de comunicación a un segundo protocolo de comunicación.

En una forma de realización ventajosa, el formato de los primeros datos se convierte en un equipo de consulta y/o los primeros datos se almacenan en una unidad de memoria.

Esto posibilita un manejo flexible de los primeros datos, en particular los primeros datos se pueden transformar ya en la primera red en un formato datos favorable para la evaluación en la segunda red. El almacenamiento de los datos posibilita una recopilación de los datos y sólo una transmisión temporal de los primeros datos a la segunda red. Una segunda conexión de datos y medios para la escucha no deben estar presentes por ello de forma continua.

En una forma de realización ventajosa, los primeros datos se transmiten de forma encriptada en la conexión de comunicación y se desencriptan antes de la transmisión en la segunda conexión de comunicación.

Esto tiene la ventaja de que los primeros datos, que se transmiten de forma encriptada en la red de comunicación, también se pueden consultar para una evaluación en la segunda red.

En una forma de realización ventajosa, los datos se transmiten de forma desencriptada en la segunda conexión de comunicación.

Por consiguiente el equipo de consulta para el segundo dispositivo de comunicación y en particular el equipo de recepción no deben proporcionar medios de encriptación. Por consiguiente se pueden usar equipos de consulta o recepción menos complejos.

En una variante de realización alternativa, los datos se encriptan para la transmisión en una segunda conexión de comunicación con un procedimiento criptográfico predeterminado.

Esto protege la transmisión de datos adicionalmente frente a una escucha ilícita o una manipulación de la transmisión de datos, en particular cuando un dispositivo de acoplamiento de sentido único semejante no está dispuesto en una zona protegida, como por ejemplo dentro de un armario de conmutación o dentro de un rack de red, sino de forma accesible desde fuera.

A este respecto, en particular se puede establecer un procedimiento de encriptación determinado entre el equipo de consulta y equipo de recepción y usarse este procedimiento de encriptación determinado siempre para la transmisión a través de la segunda conexión de comunicación.

En una forma de realización ventajosa, los datos se almacenan en una base de datos de evaluación en la segunda red y se retransmiten a petición o automáticamente a un dispositivo de evaluación.

Esto tiene la ventaja que sólo se debe proporcionar temporalmente una conexión activa entre la unidad de recepción y un equipo de evaluación. Los datos recibidos de la primera red también se pueden evaluar a intervalos de supervisión deseados.

Se reivindica un producto de programa informático según la invención, que se puede cargar directamente en una memoria de un ordenador digital y comprende partes de código de programa que son apropiadas para realizar las etapas del procedimiento.

Ejemplos de realización del dispositivo de acoplamiento de sentido único según la invención, el equipo de consulta según la invención, así como el procedimiento según la invención están representados a modo de ejemplo en los dibujos y se explican más en detalle mediante la descripción siguiente. Muestran:

Figura 1 un ejemplo de realización de un dispositivo de acoplamiento de sentido único dispuesto en el lugar de acoplamiento entre una primera y una segunda red en representación esquemática;

Figura 2 un ejemplo de realización de un equipo de consulta según la invención en representación esquemática;

Figura 3 un ejemplo de realización del procedimiento según la invención en forma de un diagrama de desarrollo, y

Figura 4 un ejemplo de realización del procedimiento según la invención mediante un dispositivo de acoplamiento de sentido único según la invención en forma de un diagrama de flujo de mensajes.

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

La figura 1 muestra un caso de aplicación para un dispositivo de acoplamiento de sentido único, por ejemplo, del sector de la automatización de vía. También hay escenarios de aplicación similares en la técnica de control de vehículos, en la automatización de energía, en la automatización de fabricación o en la automatización de procesos. En la primera red con requisitos de seguridad elevados, los dispositivos 20, 21, 22, como por ejemplo ordenadores de control con equipos de campo, están conectados a través de una primera conexión de comunicación 19 con un equipo de consulta 14 y envían informaciones a un equipo de consulta 14. En el caso de aplicación se deben transferir ahora, por ejemplo, informaciones de estado de los dispositivos 20, 21, 22 a un sistema de diagnóstico / monitorización, representado en la figura 1 por el equipo de evaluación 18. A este respecto, el equipo de evaluación 18 está unido en una segunda red 12 con bajas exigencias de seguridad, como por ejemplo una red de oficina o una red pública. Desde puntos de vista técnicos de seguridad se debe garantizar que se implemente una comunicación de sentido único dirigida, que impida que los datos potencialmente perjudiciales, como por ejemplo virus, lleguen desde la segunda red con bajas exigencias de seguridad 12 a la primera red 11 crítica respecto a la seguridad. La comunicación dentro de la primera red se puede realizar, por ejemplo, a través de un protocolo OPC UA, que se usa con frecuencia en las redes de automatización de vía.

Bajo una transmisión sin retroacción de los datos se entiende una comunicación de sentido único unidireccional, que impide que los datos potencialmente perjudiciales lleguen desde la segunda red a la primer red 11 crítica respecto a la seguridad. Una transmisión óptima sin retroacción se produce luego cuando no se introducen datos desde la segunda red 12 en la primera red 11 y tampoco datos a través de un dispositivo de acoplamiento en la primera red 11.

El dispositivo de acoplamiento de sentido único 10 representado implementa una transmisión sin retroacción semejante de datos y comprende un equipo de consulta 14, un equipo de escucha 15 y un equipo de recepción 13. Para ello está dispuesto un equipo de consulta 14 en la primera red 11, que proporciona unas primeras conexiones de comunicación 19 con los dispositivos 20, 21, 22. La facilitación de las primeras conexiones de comunicación 19 comprende el establecimiento de la conexión a través de todas las capas de protocolo conforme a una pila de protocolo OSI del protocolo de comunicación usado en la primera red 11. Esto incluye, por ejemplo, una autentificación mutua de los dispositivos 20, 21, 22 y del equipo de consulta 14 y una transmisión protegida criptográficamente de los primeros datos transmitidos. A este respecto, por ejemplo, para la transmisión segura se pueden transmitir los datos de forma encriptada a través de la conexión de comunicación.

El equipo de consulta presenta para ello una interfaz de red 6, en la que se termina la conexión de comunicación. La unidad de consulta 14 está configurada para consultar los primeros datos en los dispositivos 20, 21, 22. Para esta comunicación se usa, por ejemplo, el protocolo OPC UA. Dado que la conexión de comunicación se termina según el protocolo de comunicación completamente en el equipo de consulta 14, allí están presentes los primeros datos ahora de forma desencriptada y por consiguiente interpretable.

Según está representado en la figura 2, el equipo de consulta 14 comprende junto a la interfaz de red 6 una unidad de consulta 1, que recoge información sobre los datos a determinar de los dispositivos deseados, como por ejemplo instante de la consulta y tipo de los datos deseados. En una primera unidad de protocolo 2 se proporcionan todos los medios para el establecimiento de una primera conexión 19 dentro de la primera red 11. Una segunda unidad de protocolo 3 comprende todos los medios para el establecimiento de una segunda conexión de comunicación 23 diferente de la primera conexión de comunicación 19 a través de un bucle de línea separado 8. Una unidad de conversión 4 proporciona medios para convertir el formato de datos de los primeros datos entrantes a través de la primera conexión de comunicación 19 en otro formato predeterminado, en el que los primeros datos se depositan entonces en una unidad de memoria 5 y/o se transmiten a través de la segunda conexión de comunicación 23. La conexión de bucle separada 8 está configurada entre una interfaz de salida 7 y una interfaz de entrada 8 de la unidad de consulta 14. La conexión de bucle 8 puede estar configurada externamente, es decir, discurrir fuera del equipo de consulta 14. Pero la conexión de bucle 8 también puede estar configurada dentro del equipo de consulta 14, en particular cuando está configurado como equipo combinado de forma integrada con la unidad de escucha 15. La conexión de bucle 8 comienza y termina por consiguiente directamente en el equipo de consulta 14, sin que se atraviesen otras unidades o componentes por la conexión de bucle 8. A este respecto, la conexión de bucle está formada a través de una interfaz de salida 7 y una interfaz de entrada 8 de la unidad de consulta 14, que no coinciden con la interfaz de red 6. Los primeros datos se pueden almacenar opcionalmente en una base de datos de consulta 17, que está configurada como componente integral o como base de datos externa conectada.

El dispositivo de acoplamiento de sentido único 10 comprende, según está representado en la figura 1, además un equipo de escucha 15 con una unidad de acoplamiento 10, que está configurada por ejemplo como una interceptación de red o un copiador de datos. A este respecto, por ejemplo, la corriente de datos se duplica y se retransmites a través de una conexión separada con una unidad de recepción 13, mientras que el flujo de datos original fluye de forma no modificada en la conexión de bucle 8 hacia el equipo de consulta 14. Este equipo de escucha representa el lugar de conexión directo entre la primer red 11 y segunda red 12. Dado que mediante la unidad de acoplamiento 10 sólo es posible una copia de los datos de la segunda conexión de comunicación, pero no una introducción de datos en la segunda conexión de comunicación 23, la comunicación de sentido único se produce partiendo de la primera red 11 relevante respecto a la seguridad hacia la segunda red 12 menos relevante respecto a la seguridad.

Copiadores de datos o interceptaciones de red semejantes se conocen por sistemas de supervisión de red o también por sistemas de reconocimiento de penetración y representan por consiguiente una transmisión de datos unidireccional sencilla y fiable. Con la unidad de recepción 13 puede estar unida opcionalmente una base de datos de evaluación 17, en la que se alimentan los primeros datos escuchados o copiados. La base de datos de evaluación 17 puede estar configurada asimismo como componente integrado del equipo de recepción.

Los primeros datos recibidos en el equipo de recepción 13 se pueden transmitir por un mecanismo de empuje, es decir, por una retransmisión activa en el sentido de un enfoque de publicación y suscripción al equipo de evaluación 18 o consultarse en el caso de un almacenamiento intermedio en la base de datos de evaluación 16 mediante un mecanismo de tire del equipo de evaluación 18 de forma activa en el equipo de recepción 13 o la base de datos de evaluación 16.

De manera similar los primeros datos consultados por la unidad de consulta 14 en la primera red 11 se pueden almacenar de forma intermedia en una base de datos de consulta 17 y transmitirse, por ejemplo, a intervalos regulares o a intervalos temporales predeterminados a través de la segunda conexión de comunicación 8.

El dispositivo de acoplamiento de sentido único 10 descrito representa una implementación económica mediante el uso del equipo de escucha 15 en lugar de las conexiones de sentido único especial mediante diodos de datos. Gracias a la separación de la primera conexión de comunicación 19 y la segunda conexión de comunicación 23 en referencia a los protocolos y presentación de datos usados se puede usar el dispositivo de acoplamiento de sentido único 10 de

forma flexible para diferentes sectores de aplicación y protocolos de aplicación. La transferencia de los primeros datos a través de, por ejemplo, la interceptación de red se puede realizar a través de un protocolo lo más sencillo posible. Los protocolos más complejos, como por ejemplo OPC UA, están limitados a la primera conexión de comunicación 19 y se terminan en el equipo de consulta 14, en particular en la primera unidad de protocolo 2. Los primeros datos se pueden depositar, por ejemplo, en forma de un documento XML. Esto hace la solución escalable en referencia a su uso para otros sectores de aplicación y el uso de diferentes protocolos en las redes circundantes.

La independencia de la comunicación encriptada, en particular dentro de la primera red 11, representa otra ventaja. Si la comunicación se realiza en la primera red y/o en la segunda red 12 usando protocolos de seguridad, como por ejemplo SSL/TLS, en el lugar de acoplamiento deben estar presentes, véase la línea a trazos en la figura 1, informaciones clave para el desencriptado de la comunicación, si la interceptación de red está colocada directamente en la primera red 11. En el enfoque de solución descrito se favorece una comunicación encriptada. El encriptado en la primera red 11 se termina en el equipo de consulta 14. La transmisión a través de la segunda conexión de comunicación 23 se realiza de forma desencriptada o se puede transmitir de nuevo de forma encriptada mediante un encriptado compatible entre el equipo de consulta 14 y el equipo de recepción 13.

En la figura 3 se representan las etapas del procedimiento individuales del procedimiento según la invención. En la primera etapa del procedimiento 31 se proporciona una primera conexión de comunicación 19 dentro de la primera red 11. En la etapa del procedimiento 32 se consultan ahora los primeros datos a través de la primera conexión de comunicación de los dispositivos 20, 21, 22 u otros dispositivos en la primera red 11. Para ello un equipo de consulta 14 puede contener perfiles de consulta predeterminados. En la etapa del procedimiento 33 se reciben los primeros datos consultados a través de la conexión de comunicación 19 en la unidad de consulta 14. A este respecto, la primera conexión de comunicación 19 se termina conforme al protocolo de comunicación usado y en particular se realiza una autentificación de los dispositivos 20, 21, 22 o del equipo de consulta 14 y se desencriptan de nuevo los primeros datos transmitidos de forma encriptada. En la etapa del procedimiento 34 se transmiten ahora los primeros datos a través de una conexión de bucle separada 8, por ejemplo externa. La conexión de bucle 8 se sitúa concretamente dentro de la zona de la red 11, no obstante, está separada físicamente de la primera conexión de comunicación 19. En la etapa del procedimiento 35 se escuchan los primeros datos en la conexión de bucle externo 8 y en la etapa del procedimiento 36 se transfieren a una segunda red 12 con exigencia de seguridad baja 12.

La fig. 4 muestra ahora el procedimiento mediante una red de seguridad en una instalación de seguridad de vía con dispositivos de seguridad 20, 21, 22. Entre los dispositivos 20, 21, 22 individuales y el equipo de consulta 14 está proporcionada respectivamente una primera conexión de comunicación 19, que termina en el equipo de consulta 14 en la interfaz de red 6. El equipo de consulta 14 representa aquí un cliente OPC UA. A través de la primera conexión de comunicación 19 se envían los mensajes de consulta 40 a los dispositivos 20, 21, 22 y los primeros datos exigidos se devuelven en mensajes de repuesta 41 al equipo de consulta 14. Los primeros datos contenidos en los mensajes de repuesta 41 se extraen mediante la primera unidad de protocolo 2 y se convierten en otra representación (por ejemplo, en un lenguaje de marcado extensible, denominado de forma acortada XML). Los primeros datos se estructuran mediante la segunda unidad de protocolo 3 conforme a un segundo protocolo de comunicación de la segunda conexión de comunicación 23 y se emiten a través de la interfaz de salida 7 para la transmisión a través de la conexión de bucle 8 y se reciben de nuevo en la interfaz de salida 9, véase la flecha 43. En la conexión de bucle 8 entre una interfaz de salida 7 y una interfaz de entrada 9 se copia la conexión de comunicación por el equipo de escucha 15, véase la flecha 44 a trazos y se transmite a la unidad de recepción 13, véase la flecha 45. A través de la propiedad física de la interceptación de red se garantiza que se realice esto sin retroacción, es decir, que no sea posible un flujo de información en la dirección opuesta de la segunda red a la primera red 11.

El equipo de recepción 13 actúa, por ejemplo, como servidor OPC UA. Pero el equipo de recepción 13 puede soportar un protocolo más sencillo y procesar el mensaje 43 transmitido en el primer protocolo de comunicación en la segunda conexión de comunicación 23 o el mensaje reenviado 45. Una consulta de un equipo de evaluación 18 se puede responder ahora en base a los primeros datos almacenados en la base de datos de evaluación o en el equipo de recepción 13.

Una ventaja esencial de esta construcción consiste en que se puede realizar una integración del dispositivo de acoplamiento de sentido único en redes de control existentes, sin que sea necesaria una modificación o adaptación de los componentes existentes. A este respecto, el dispositivo de acoplamiento de sentido único puede estar configurado como equipo de consulta 14, equipo de escucha 15 y equipo de recepción 13 separados físicamente o como un único dispositivo integrado.

El equipo de recepción 13 detecta los datos de diagnóstico de los dispositivos 20, 21, 22. Esto se puede realizar p. ej. mediante OPC UA, Telnet, SNMP, FTP, SCP, http o similares. Por ejemplo, la unidad de consulta 14 puede consultar cíclicamente, p. ej. por disparo mediante un temporizador interno, los primeros datos de los dispositivos y recopilarlos en la base de datos de consulta 17 de la unidad de consulta 14. Asimismo es posible que se forme un fichero 42, que contiene los valores de datos modificados, convertidos en particular en otro formato. La unidad de consulta 13 transmite este fichero 42 entre dos interfaces de red 7, 9 de la unidad de consulta 14 p. ej. a través de FTP o http. Es decir, la unidad de consulta 14 transmite el fichero a sí misma. Esta transmisión se escucha sin retroacción a través del equipo de consulta 15.

La transmisión de consulta escuchada se transmite del equipo de escucha 15 a la unidad de recepción. La transmisión del fichero se puede realizar en un mensaje. En general es posible asimismo que la transmisión se realice en fragmentos, es decir, tramos. Entonces el equipo de recepción 13 debe unir los fragmentos. El fichero 42 puede comprender una o varias sumas de comprobación que se forma, por ejemplo, como una firma digital a través de CRC. El fichero 42 puede estar codificado de forma redundante, de modo que se pueden corregir los errores de transmisión. Para ello se pueden usar igualmente procedimientos de corrección de errores, según se conocen p. ej. en la transmisión http.

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. Dispositivo de acoplamiento de un sentido para la transmisión de datos sin retroacción de una primera red (11) con exigencia de seguridad elevada a una segunda red (12) con exigencia de seguridad baja, que contiene un equipo de consulta (14), un equipo de escucha (15) y un equipo de recepción (13), en donde

el equipo de consulta (14) está configurado para proporcionar una primera conexión de comunicación (19) dentro de la primera red (12) con al menos un dispositivo (20, 21, 22) y además consultar primeros datos del al menos un dispositivo (20, 21, 22) y a continuación transmitir los primeros datos a través de una segunda conexión de comunicación (23) en un bucle de línea (8) separado y que discurre fuera del equipo de consulta (14) de una interfaz de salida del equipo de consulta (14) directamente a la interfaz de entrada del equipo de consulta (14), y

el equipo de escucha (15), que está configurado para escuchar los datos en el bucle de línea separado (8) y transferirlos a un equipo de recepción (13) que está dispuesto en la segunda red (12).

2. Dispositivo de acoplamiento de sentido único según la reivindicación 1, en donde el equipo de consulta (14) presenta una primera unidad de protocolo (2) para la facilitación de un primer protocolo de comunicación para la conexión de comunicación (19) con el al menos un dispositivo (20, 21, 22), en particular del protocolo OPC UA.

3. Dispositivo de acoplamiento de sentido único según la reivindicación 1 o 2, en donde el equipo de consulta (14) presenta una segunda unidad de protocolo (3) para la facilitación de un segundo protocolo de comunicación para la transmisión de los primeros datos a través del bucle de conexión (8).

4. Dispositivo de acoplamiento de sentido único según una de las reivindicaciones 1 a 3, en donde el equipo de consulta (14) presenta una unidad de conversión (4) para la conversión de formato para los primeros datos.

5. Dispositivo de acoplamiento de sentido único según una de las reivindicaciones 1 a 4, en donde el equipo de consulta (14) presenta una unidad de memoria (5) para el almacenamiento de los primeros datos.

6. Dispositivo de acoplamiento de sentido único según una de las reivindicaciones 1 a 5, en donde el equipo de escucha (15) está configurado como copiador de datos.

7. Procedimiento para la transmisión de datos sin retroacción de una primera red (11) con exigencia de seguridad elevada en una segunda red (12) con exigencia de seguridad baja con las etapas del procedimiento:

- facilitación (31) de una primera conexión de comunicación (19) dentro de la primera red (12), consulta (32) y recepción (33) de los primeros datos del al menos un dispositivo (20, 21, 22) en la primera red (11) a través de la primera conexión de comunicación (19),

- transmisión (34) de los primeros datos en una segunda conexión de comunicación (23) a través de un bucle de línea (8) separado y que discurre fuera del equipo de consulta (14) de una interfaz de salida del equipo de consulta (14) directamente a una interfaz de entrada dentro de la primera red (11),

- escucha (35) de los primeros datos en el bucle de línea separado (8), y

- transferencia (36) de los primeros datos a una segunda red (12) con menor exigencia de seguridad.

8. Procedimiento según la reivindicación 7, en donde un primer protocolo de comunicación, en particular del protocolo OPC UA, se usa para la conexión de comunicación (19) con el al menos un dispositivo (20, 21, 22), y/o

un segundo protocolo de comunicación se usa para la transmisión de los primeros datos a través del bucle de línea separado (8).

9. Procedimiento según la reivindicación 7 u 8, en donde el formato de los primeros datos se convierte en un equipo de consulta (14), y/o

los primeros datos se almacenan en una unidad de memoria (5).

10. Procedimiento según una de las reivindicaciones 7 a 9, en donde los primeros datos se transmiten de forma encriptada en la primera conexión de comunicación (19) y se desencriptan antes de la transmisión en el bucle de conexión (8).

11. Procedimiento según la reivindicación 10, en donde los datos se transmiten de forma desencriptada en el bucle de conexión (8).

12. Procedimiento según la reivindicación 10, en donde los datos para la transmisión en el bucle de conexión (8) se transmiten de forma encriptada.

13. Procedimiento según una de las reivindicaciones 7 a 12, en donde los primeros datos se almacenaban en una base de datos de evaluación (16) en la segunda red y se retransmiten de forma recuperable o automática de la base de datos de evaluación a un equipo de evaluación (18).

14. Producto de programa informático, que se puede cargar directamente en la 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 7 a 13.

FIG 1

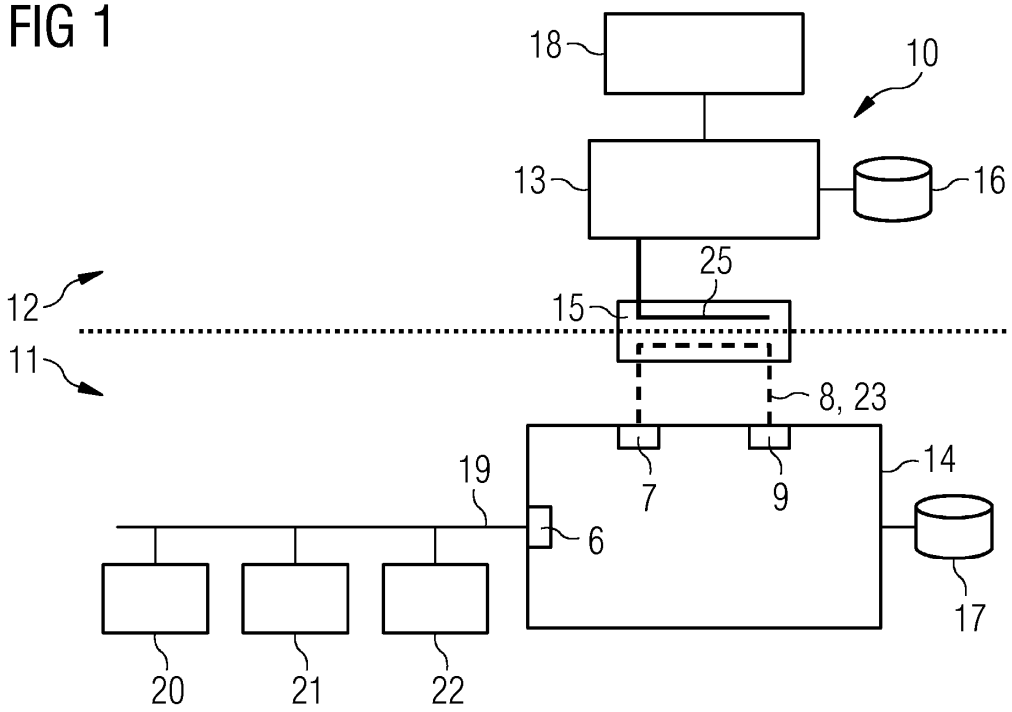

FIG 2

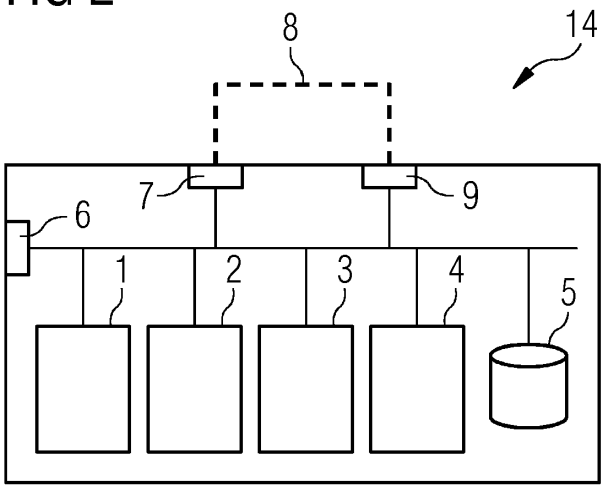

FIG 3

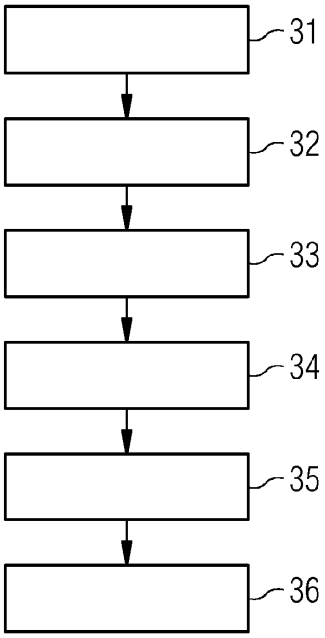

FIG 4