(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 784 265**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **10.12.2015 PCT/EP2015/079245**

(87) Fecha y número de publicación internacional: **23.06.2016 WO16096599**

(96) Fecha de presentación y número de la solicitud europea: **10.12.2015 E 15817777 (4)**

(97) Fecha y número de publicación de la concesión europea: **12.02.2020 EP 3207683**

(54) Título: **Procedimiento y dispositivo para la captura sin repercusiones de datos**

(30) Prioridad:

18.12.2014 DE 102014226398

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.09.2020

(73) Titular/es:

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

(72) Inventor/es:

BLÖCHER, UWE;
FALK, RAINER y
WIMMER, MARTIN

(74) Agente/Representante:

LOZANO GANDIA, José

DESCRIPCIÓN

Procedimiento y dispositivo para la captura sin repercusiones de datos

La invención se refiere a un procedimiento y a un dispositivo para la captura sin repercusiones de datos de al menos un dispositivo que está dispuesto en una primera red con requerimiento de seguridad alto, en una segunda red con requerimiento de seguridad reducido.

Se usan hasta ahora soluciones de seguridad para transferir datos entre redes con requerimientos de seguridad distintos, denominadas soluciones de seguridad entre dominios (*cross domain security*), para sectores especiales, como la comunicación de organismos públicos, en los que se aplican requerimientos de seguridad altos y en los que existe una clasificación de seguridad de documentos o informaciones. Por medio de una solución entre dominios se realiza un intercambio seguro automatizado de documentos y mensajes, como por ejemplo correos electrónicos, entre zonas con requerimientos de seguridad de distinto nivel. A este respecto un componente esencial es un diodo de datos, que asegura una unidireccionalidad de la comunicación de datos, es decir también un transporte de datos únicamente en una dirección.

Para acoplar redes de control industriales, que tienen habitualmente requerimientos de seguridad altos, con una red de oficina, una internet pública u otras redes de control, a las que les basta habitualmente sólo con requerimientos de seguridad reducidos, se usan hasta ahora cortafuegos convencionales, que filtran la comunicación de datos según reglas de filtro configurables. La comunicación de datos se permite o se bloquea a este respecto dependiendo de las direcciones de los socios de comunicación y del protocolo de comunicación usado.

Por el documento WO 2012/170485 se conoce una solución de seguridad entre dominios que se basa en una solución de virtualización, en la que una máquina virtual controla la transferencia de información entre dos dominios de información.

El documento US 2010/162399 A1 da a conocer un procedimiento, un dispositivo, así como un producto de programa informático, que protege una red frente a software malicioso, recopilando y analizando datos de *xFlow* dentro de una red, para reconocer tráfico anómalo y a partir de ahí poder concluir la existencia de software malicioso. Para ello se soporta un protocolo de *xFlow* en un enrutador de red, que graba metadatos de tráfico de datos de red y adicionalmente un flujo de datos, es decir una secuencia unidireccional de paquetes con uno o varios parámetros iguales, como por ejemplo dirección de IP de origen o destino, puerto de origen/destino, protocolo de IP, etc. en un registro de *xFlow*.

Además se conoce un desacoplador de red, también denominado punto de conexión de red (*network tap*), como componente de red, para poder escuchar datos transferidos sin influir en los datos transferidos. Tales desacopladores de red se emplean en general para una monitorización de red, dado que en este caso no se influye en parámetros, como un rendimiento o una latencia, por medio de la medición.

Para entornos industriales, como por ejemplo para un sistema de protección ferroviaria, existe la necesidad de capturar sin repercusiones datos de diagnóstico en la red crítica para la seguridad y de proporcionar los mismos a una red de diagnóstico que está realizada habitualmente en una red con requerimientos de seguridad reducidos. A este respecto aparece en particular el problema de que un componente para la transferencia de datos unidireccional no puede controlar o influir activamente en la petición de una información en la red con requerimiento de seguridad alto. En el ejemplo del denominado sistema de protección ferroviaria se depende de que tenga lugar una comunicación de los datos necesarios sin su intervención o la necesaria.

Por consiguiente, el objetivo de la presente invención es proporcionar un procedimiento y un dispositivo que aseguren que datos determinados de uno o más dispositivos, que están dispuestos en una red con requerimiento de seguridad alto, puedan recuperarse y estos datos puedan transmitirse a una segunda red, sin poder requerir activamente estos datos desde la segunda red.

El objetivo se alcanza por medio de las medidas descritas en las reivindicaciones independientes. En las reivindicaciones dependientes se representan perfeccionamientos ventajosos de la invención.

El procedimiento según la invención para la captura sin repercusiones de datos de al menos un dispositivo que está dispuesto en una primera red con requerimiento de seguridad alto, en una segunda red con requerimiento de seguridad reducido, presenta como primera etapa de procedimiento requerir los datos del al menos un dispositivo de manera correspondiente a un perfil de petición por medio de una unidad de petición, que está dispuesta dentro de la primera red. A continuación se efectúa una escucha de los datos enviados desde el al menos un dispositivo en respuesta al requerimiento a la unidad de petición dentro de la primera red por medio de una unidad de escucha y una transmisión de los datos a una unidad de evaluación en la segunda red. En la misma se comparan los datos escuchados con los datos esperados según el perfil de petición y se proporciona una señal de alarma cuando los datos escuchados difieren de los datos esperados según el perfil de petición. La unidad 21 de escucha sólo puede escuchar datos que se transfieren a la primera red 11, y no puede enviar mensajes de ningún tipo a los dispositivos

16.1, 16.2, 16.3 y tampoco ningún mensaje a la unidad 14 de petición.

Por una captura sin repercusiones de datos ha de entenderse a este respecto que por medio de la transferencia de la primera red relevante en cuanto a seguridad a la segunda red menos relevante en cuanto a seguridad no se introducen datos o interferencias de ningún tipo en la primera red relevante en cuanto a seguridad.

Por medio del requerimiento de los datos de manera correspondiente a un perfil de petición preestablecido, que se conoce tanto en la unidad de petición como en la unidad de evaluación, puede establecerse unívocamente si todos los datos necesarios se transfirieron a la segunda red y, por consiguiente, garantizarse una función correcta. Al proporcionar una señal de alarma puede averiguarse y monitorizarse por ejemplo una tasa de errores en el requerimiento y/o en la escucha y/o en la transmisión. Esto está asegurado por medio de una escucha exclusiva de los datos. La escucha puede realizarse en este caso por ejemplo por medio de un desacoplador de red, es decir un punto de conexión de red.

En una forma de realización ventajosa del procedimiento según la invención, se visualiza por medio de la señal de alarma un aviso de alarma en la unidad de evaluación y/o en un dispositivo de diagnóstico en una red de diagnóstico. Adicional o alternativamente a esto se crea una entrada en un informe de monitorización, también denominado archivo de registro, y/o se desencadena una reacción activa en la unidad de escucha o en la unidad de petición.

A este respecto como reacción activa puede considerarse por ejemplo el comienzo de un reinicio de la unidad de escucha o puede provocarse por ejemplo una interrupción de la alimentación eléctrica de la unidad de petición, de modo que se efectúa un reinicio de la unidad de petición y se generan de nuevo peticiones según el perfil de petición. Por consiguiente, puede realizarse una medida para anular una interferencia. Por lo demás la funcionalidad de la unidad de petición y de la unidad de escucha puede monitorizarse continuamente por medio de una entrada en un informe de monitorización o por medio de un aviso de alarma. De este modo puede establecerse en particular una señal de alarma cuando se realiza una petición frecuentemente de manera no permitida, cuando se realiza una petición de manera demasiado infrecuente, cuando no se realiza una petición de datos necesarios o cuando se realiza una petición de datos no permitidos.

En una forma de realización ventajosa adicional, se bloquea por medio de la señal de alarma una retransmisión de los datos escuchados por medio de la unidad de evaluación o una lectura de los datos escuchados desde la unidad de evaluación.

Esto impide que se tengan en cuenta datos incorrectos o no permitidos para la evaluación y el diagnóstico.

En una variante del procedimiento según la invención, el perfil de petición presenta reglas de petición distintas para tipos de datos distintos y/o para tipos distintos de dispositivos y/o para dispositivos individuales en sí mismos.

De este modo pueden generarse y evaluarse valores de diagnóstico pertinentes dependiendo de los distintos tipos de datos y/o las propiedades de los dispositivos individuales o tipos de dispositivo. De este modo pueden ajustarse por ejemplo en cada caso reglas de petición iguales para tipos de dispositivo iguales, como por ejemplo barreras de paso a nivel, o reglas de petición iguales para todas las señales de trenes o semáforos.

En una variante adicional, el perfil de petición presenta una regla de petición unificada para tipos de datos distintos y/o para tipos de dispositivo distintos y/o para los dispositivos individuales en sí mismos.

Esto posibilita el uso de una unidad de petición construida de manera sencilla y menos compleja. La unidad de petición también puede pasar a un modo con regla de petición unificada cuando por ejemplo la cantidad de datos averiguados como erróneos aumenta, de modo que puede conservarse una posibilidad de diagnóstico de emergencia.

En una variante del procedimiento según la invención, se memorizan en memoria intermedia los datos escuchados en la unidad de evaluación y sólo se transmiten al dispositivo de diagnóstico después de una comprobación satisfactoria.

En una variante del procedimiento según la invención, existe entonces una comprobación satisfactoria cuando los datos escuchados corresponden al perfil de petición y/o si los datos escuchados presentan una suma de comprobación criptográfica válida.

Esto tiene la ventaja de que sólo se reenvían y, por consiguiente, se tienen en cuenta para la evaluación datos relevantes y/o transferidos con contenido inalterado y transferidos desde un dispositivo permitido, autorizado.

En una variante del procedimiento según la invención, se transmite, en el caso de una comprobación no satisfactoria, un valor de sustitución o un aviso de error al dispositivo de diagnóstico.

Esto, a pesar de un valor de datos falseado o no relevante, permite una evaluación buena y continua, en particular por medio del uso de un valor de sustitución. En el caso del aviso de un error puede averiguarse en particular de manera sencilla la tasa de errores.

En un ejemplo de realización adicional del procedimiento según la invención, una información de validez se asocia a los datos escuchados después de una comprobación en la unidad de evaluación.

Esto posibilita una valoración de los datos también en el caso de una memorización más larga o facilita gestionar los datos escuchados, archivando o borrando por ejemplo el conjunto de datos después de expirar el periodo de validez.

En una variante del procedimiento según la invención, los datos escuchados sólo se transmiten entonces al ordenador de diagnóstico, si se recibieron los datos escuchados en un intervalo de tiempo predeterminado después de la petición asociada en la unidad de evaluación.

De este modo se reduce la cantidad de datos capturados que no pertenecen a un perfil de petición actual. Además con ello datos que un dispositivo no permitido o un atacante introdujo en la primera red pueden reconocerse al menos parcialmente y no consultarse para la evaluación.

El dispositivo según la invención para la captura sin repercusiones de datos de al menos un dispositivo que está dispuesto en una primera red con requerimiento de seguridad alto, en una segunda red con requerimiento de seguridad reducido, contiene una unidad de petición que está dispuesta dentro de la primera red y configurada para requerir datos del al menos un dispositivo de manera correspondiente a un perfil de petición. Contiene una unidad de escucha que está dispuesta dentro de la primera red y está configurada para escuchar datos que se enviaron desde el al menos un dispositivo en respuesta al requerimiento y para transmitir los mismos a una unidad de evaluación. El dispositivo comprende además una unidad de evaluación que está dispuesta en la segunda red y configurada para comparar los datos escuchados con los datos esperados según el perfil de petición y una unidad de alarma que está configurada para proporcionar una señal de alarma cuando los datos escuchados difieren de los datos esperados según el perfil de petición.

Por consiguiente, este dispositivo posibilita estimular datos dirigidos por medio de una petición en el dispositivo y comparar los datos después de la transferencia a la segunda red menos segura con el mismo perfil de petición que se conoce en la unidad de evaluación, y por consiguiente asegurar que es posible una evaluación fiable de los datos.

En una forma de realización ventajosa del dispositivo según la invención, la unidad de escucha y/o la unidad de petición están configuradas para reconocer una señal de alarma y reiniciarse posteriormente de manera autónoma o la unidad de evaluación está configurada para bloquear una retransmisión o una lectura de los datos escuchados después de reconocer la señal de alarma.

En una variante del dispositivo según la invención, la unidad de evaluación está configurada para memorizar datos escuchados para realizar una comprobación de los datos y para transmitir los datos a un dispositivo de diagnóstico sólo después de una comprobación satisfactoria.

En una variante adicional del dispositivo según la invención, la unidad de evaluación está configurada para comprobar si los datos escuchados corresponden al perfil de petición y/o o los datos escuchados presentan una suma de comprobación criptográfica válida, y para transmitir únicamente los datos comprobados satisfactoriamente al dispositivo de diagnóstico o para transmitir, en el caso de una comprobación no satisfactoria, un valor de sustitución o un mensaje de error al dispositivo de diagnóstico.

Además se reivindica un producto de programa informático con instrucciones de programa para realizar el procedimiento mencionado anteriormente.

La invención se determina por medio de las reivindicaciones adjuntas.

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

la figura 1, un ejemplo de realización del procedimiento según la invención en forma de diagrama de flujo;

la figura 2, un primer ejemplo de realización del dispositivo según la invención en un entorno de automatización a modo de ejemplo en representación esquemática; y

la figura 3, un segundo ejemplo de realización del dispositivo según la invención con datos memorizados en memoria intermedia en una unidad de evaluación en representación esquemática.

Las partes correspondientes entre sí están dotadas en todas figuras de signos de referencia iguales.

Mediante un diagrama de flujo en la figura 1 se explica más detalladamente ahora el procedimiento según la invención. En el estado 1 de partida hay una primera red con requerimientos de seguridad altos así como una segunda red con requerimientos de seguridad reducidos. Los datos que se transfieren a la primera red deben transmitirse ahora sin repercusiones a la segunda red, es decir sin variar los datos transferidos a la primera red, generar datos nuevos en la primera red o ejercer otra influencia en esta primera red. Los datos se crean en la primera red por al menos un dispositivo y dan por ejemplo información sobre el estado de funcionamiento de la una o las varias unidades. Además en la primera red se encuentra una unidad de escucha que está configurada por ejemplo como desacoplador de red o como diodo de datos de otro tipo constructivo. Los datos transferidos a la primera red se duplican por ejemplo y el duplicado se transmite a los componentes en la segunda red, en particular a una unidad de evaluación.

En la primera red se encuentra además una unidad de petición, que presenta un perfil de petición que contiene por ejemplo peticiones predeterminadas y un esquema temporal relativo al momento en que deben enviarse estas peticiones a los dispositivos en la primera red. El mismo perfil de petición existe en una unidad de evaluación que está dispuesta en la segunda red. En la primera etapa de procedimiento 2, la unidad de petición requiere datos dentro de la primera red del al menos un dispositivo de manera correspondiente al perfil de petición que está memorizado en la unidad de petición. Este requerimiento puede efectuarse por ejemplo por medio de la emisión de mensajes de petición, también mensajes de solicitud (*request*), que o bien están dirigidos directamente a dispositivos individuales o bien se reciben desde varios dispositivos y se evalúan como mensajes de multidifusión (*multicast*) o radiodifusión (*broadcast*). Como reacción a estos mensajes de petición el uno o los varios dispositivos envían de vuelta los datos requeridos a la unidad de petición por ejemplo en mensajes de respuesta.

Los datos enviados de vuelta se escuchan ahora en la etapa de procedimiento 3 por medio de una unidad de escucha dentro de la primera red y se transmiten a una unidad de evaluación en la segunda red. A este respecto la unidad de escucha puede transmitir por ejemplo por sí misma únicamente aquellos mensajes de respuesta de los dispositivos en la segunda red que corresponden a una respuesta a los mensajes de petición enviados. No obstante, también puede escucharse el tráfico de datos total que está enviado desde un dispositivo y dirigido a la unidad de petición. No obstante, la unidad de escucha también puede escuchar o evaluar únicamente el tráfico de datos o el tipo de mensaje determinado que se envía en un intervalo de tiempo predeterminado después de que el dispositivo envíe el mensaje de petición a la unidad de petición.

En particular la limitación del tiempo de escucha a un intervalo de tiempo después del mensaje de petición emitido puede impedir que se capture un mensaje de respuesta no enviado de vuelta para una petición actual, pero cuyo formato es igual al de una respuesta al mensaje de petición. Por consiguiente, tales mensajes de respuesta y los datos contenidos de manera correspondiente no falsean una evaluación posterior.

En la unidad de evaluación se comparan a continuación en la etapa de procedimiento 4 los datos escuchados con los datos esperados según el perfil de petición. Es decir, se comparan por ejemplo los mensajes de respuesta con los mensajes de petición emitidos y el mensaje de respuesta se acepta únicamente cuando puede averiguarse un mensaje de petición para un mensaje de respuesta.

Si los datos o los mensajes de respuesta escuchados difieren de los datos o los mensajes de respuesta esperados según el perfil de petición, la unidad de evaluación proporciona una señal de alarma, véase la etapa de procedimiento 5. A este respecto, en el caso de una única diferencia, es decir cuando ya no puede encontrarse ningún mensaje de petición asociado para un mensaje de respuesta, puede proporcionarse una señal de alarma o, no obstante, también pueden definirse valores de umbral predeterminados con respecto a una cantidad máxima de datos que difieren y sólo después de que se supere el valor de umbral se proporciona una señal de alarma.

Como reacción a la señal de alarma puede visualizarse un aviso de alarma en la unidad de evaluación y/o en un dispositivo de diagnóstico, al que se transmiten los datos por ejemplo para una evaluación adicional. No obstante, también puede crearse por medio de la señal de alarma una entrada en un informe de monitorización, un denominado archivo de registro (*logfile*), en el dispositivo de escucha o en la unidad de evaluación o incluso en el dispositivo de diagnóstico. También puede crearse un aviso de error para personal de servicio, por ejemplo, en forma de un tono de advertencia o una señal luminosa o una visualización en un monitor de monitorización. Es posible además desencadenar una reacción activa a la señal de alarma. De esta manera puede efectuarse por ejemplo el reinicio de la unidad de petición por medio de la interrupción de la alimentación eléctrica. Por consiguiente, esto permite un acceso indirecto a componentes en la primera red. De este modo puede reiniciarse el proceso de petición, es decir la emisión de mensajes de petición en la unidad de petición. También es posible, dependiendo de la señal de alarma, retransmitir o bloquear datos escuchados o permitir o impedir un acceso de lectura a datos escuchados desde la unidad de evaluación.

El perfil de petición puede definir reglas de petición distintas para una comunicación observada de tipos distintos. Por ejemplo si en el perfil de petición están contenidas reglas de petición distintas para tipos de datos distintos y/o para tipos distintos de dispositivos, como por ejemplo para tipos de aparato distintos y/o para los dispositivos individuales en sí mismos, entonces puede estar introducido un intervalo de consulta más largo en el perfil de petición por ejemplo para todas las barreras de paso a nivel en una red de control de ferrocarriles como por ejemplo

para un equipo de señalización.

Por otro lado, el perfil de petición también puede contener una regla de petición unificada para tipos de datos distintos, tipos de dispositivo distintos o para los dispositivos individuales en sí mismos. Un esquema sencillo de este tipo también puede soportarse por ejemplo por medio de unidades de petición poco complejas.

En particular los datos escuchados pueden memorizarse en memoria intermedia en la unidad de escucha o en la unidad de evaluación. Antes de una retransmisión o una lectura de datos desde la unidad de evaluación y de una transmisión a la unidad de diagnóstico se comprueban en primer lugar los datos escuchados. Puede realizarse una comprobación por un lado con respecto al perfil de petición. No obstante, también puede comprobarse la validez de una suma criptográfica de comprobación que los propios dispositivos formaron mediante los datos o los mensajes de respuesta enviados y que se transmitió con el mensaje de respuesta a la unidad de petición. Para ello, sin embargo, debe existir en la unidad de evaluación una clave criptográfica usada en el dispositivo o en el caso de un sistema criptográfico asimétrico por ejemplo una clave pública adecuada para una clave privada del dispositivo.

Si una comprobación de este tipo no se desarrolla satisfactoriamente, se transmite preferiblemente un valor de sustitución o un aviso de error a la unidad de diagnóstico. Por consiguiente, se comprueba si los datos memorizados en memoria intermedia se transmitieron de una manera que corresponde al perfil de petición preestablecido. Después de la transmisión de los datos el procedimiento en la etapa de procedimiento 6 está finalizado.

El procedimiento descrito posibilita asegurar un modo de funcionamiento correcto de la transferencia de datos, sin que sea necesario un acceso directo a los componentes en la primera red, relevante en cuanto a seguridad. Si se establece una diferencia de los datos averiguados con respecto al perfil de petición predeterminado, entonces esto es un indicio de una captura errónea por ejemplo de datos de diagnóstico y posibilita, por un lado, reconocer tales datos como no correctos y tener en cuenta esto en la valoración y la pertinencia de los datos. Además, pueden desencadenarse medidas para subsanar un error de este tipo.

En la figura 2 se describe ahora un dispositivo 10 correspondiente para capturar sin repercusiones datos por medio de una comunicación unidireccional con el ejemplo de una red de protección de funcionamiento. En el caso de la red de protección de funcionamiento puede tratarse de una red de automatización ferroviaria, una red de control de vehículos, una red de automatización de energía, una red de automatización de fabricación, una red de automatización de procesos o similares. La primera red 12 representada en la figura 2 corresponde a este respecto a la red de protección de funcionamiento que presenta requerimientos de seguridad altos con respecto a una transferencia de datos y una autorización de acceso. Los dispositivos 16.1, 16.2, 16.3 en una red de protección de funcionamiento de este tipo pueden ser en particular ordenadores de control y aparatos de campo con sensores o accionadores conectados. Los mismos están enlazados mediante la primera red 12 con requerimientos de seguridad altos, por ejemplo, mediante circuitos 18 de enlace o también mediante enlaces de comunicación inalámbricos, por ejemplo, una WLAN. Los dispositivos 16.1, 16.2, 16.3 se comunican por ejemplo mediante un protocolo de máquina a máquina (M2M), como una arquitectura unificada de OPC especificada por la organización OPC, denominada de manera abreviada UA de OPC, que especifica mensajes específicos para transferir por ejemplo avisos de alarma o estado entre redes industriales.

En el ejemplo representado el dispositivo 10 lee sin repercusiones ahora por ejemplo datos de diagnóstico de los dispositivos 16.1, 16.2, 16.3 de la primera red 12 y los transfiere a un dispositivo 19 de diagnóstico en una red 15 de diagnóstico, que está dispuesta en una segunda red 11 con requerimientos de seguridad reducidos. El dispositivo 10 contiene una unidad 14 de petición, una unidad 21 de escucha, una unidad 13 de evaluación, así como una unidad 24 de alarma.

La unidad 14 de petición está dispuesta en la primera red 12 y envía peticiones a los distintos dispositivos 16.1, 16.2, 16.3. La unidad 14 de petición emite estas peticiones, por ejemplo, mensajes de petición de UA de OPC, según un perfil 17' de petición preestablecido. El perfil 17' de petición puede haberse introducido por ejemplo por medio de un técnico de servicio en la unidad 14 de petición o puede haberse configurado en la producción o la instalación en la primera red 12 en la unidad 14 de petición.

Después de la recepción de un mensaje de petición de este tipo en el dispositivo 16.1, 16.2, 16.3, el dispositivo 16.1, 16.2, 16.3 responde con un mensaje de respuesta, también denominado contestación (*response*). Estos mensajes de respuesta o también la información contenida en los mismos corresponden a los datos ya mencionados.

La comunicación unidireccional se lee por medio de la unidad 21 de escucha de la primera red 12 por medio de la escucha del tráfico de datos por ejemplo en el circuito 18 de enlace y se transfiere a la unidad 13 de evaluación. La unidad 13 de evaluación está dispuesta de manera preferida ya en la segunda red 11, como por ejemplo una red de oficina con requerimientos de seguridad reducidos. El límite entre la primera red 12 y la segunda red 11 se representa por medio de la línea punteada en la figura 2 e igualmente en la figura 3.

La unidad 21 de escucha sólo puede escuchar datos que se transfieren a la primera red 11, para garantizar que no hay repercusiones. No puede enviar mensajes de ningún tipo a los dispositivos 16.1, 16.2, 16.3 y tampoco ningún

mensaje a la unidad 14 de petición. Puede escuchar por ejemplo el tráfico de datos total transferido en el circuito 18 de enlace o sólo mensajes de la comunicación de UA de OPC, respecto a los cuales la unidad 14 de petición realizó la petición.

La unidad 13 de evaluación en la segunda red 11 comprueba los mensajes de la comunicación de UA de OPC o el tráfico de datos escuchados contra un perfil 17 de petición que corresponde al perfil 17' de petición en la unidad 14 de petición. Dependiendo de si la comunicación de UA de OPC escuchada corresponde a este perfil de petición, se proporcionan los datos escuchados al ordenador 19 de diagnóstico. En particular puede lograrse de este modo que sólo se reenvíen datos escuchados que corresponden al perfil 17, 17' de petición. De este modo puede impedirse en particular que se traslade una comunicación no permitida u obsoleta. También puede lograrse que sólo se transfieran datos si se observó un mensaje 20.1, 20.2, 20.3 de petición asociado.

La unidad de evaluación presenta en el ejemplo de realización representado en este caso una unidad 24 de alarma integrada que, en el caso de una comprobación no satisfactoria de los datos escuchados, proporciona una señal de alarma. La señal de alarma puede implementarse en la propia unidad 13 de evaluación, por ejemplo, como entrada en un informe de monitorización de la unidad 13 de evaluación. La señal de alarma también puede desencadenar la generación de un aviso de error, que se envía a la unidad 19 de diagnóstico.

El dispositivo 19 de diagnóstico puede realizar peticiones a la unidad 13 de evaluación por ejemplo igualmente mediante una petición de UA de OPC. Esto se designa habitualmente como una extracción de mensajes. Dependiendo de si se observó una comunicación de datos adecuada que cumple el perfil 17, 17' de petición, se proporcionan los datos correspondientes. En el caso de una vulneración del perfil 17, 17' de petición puede notificarse un valor de sustitución o un error. Igualmente pueden proporcionarse activamente los datos por medio de la unidad 13 de evaluación de la unidad 19 de diagnóstico. Esto también se designa como modo de inserción.

Para soportar el mecanismo de extracción la unidad 13 de evaluación pueden memorizar en memoria intermedia datos escuchados desde la primera red 12. Esto se describe ahora mediante una representación ampliada de la unidad 13 de evaluación en la figura 3.

Los datos escuchados, en este caso por ejemplo las entradas de comunicación de UA de OPC, pueden ponerse a disposición por ejemplo en una memoria 22 de datos local. A este respecto se registra por ejemplo cada mensaje X, A, B de petición en la columna Y junto con la información sobre a quién iba dirigido el mensaje de petición. En la columna Z se memorizan los mensajes de respuesta o datos notificados en un mensaje de respuesta a la unidad 14 de petición. En la columna t(Z) se registra el tiempo de recepción del mensaje de respuesta. Los mensajes X, A, B de petición registrados en la memoria 22 de datos local se marcan en la parte derecha de la figura 3, que representa la primera red 11, como mensaje A, B, X de petición de la unidad 14 de petición a los dispositivos 16.1, 16.2. Los mensajes de respuesta correspondientes se marcan por motivos de claridad sin signos de referencia propios. Los mensajes de respuesta y/o también los mensajes de petición se toman mediante la unidad 21 de escucha en la primera red 12 por ejemplo de circuitos de enlace.

En la unidad 13 de evaluación, que está dispuesta por ejemplo en la segunda red 11, pueden compararse ahora con el perfil 17 de petición estos mensajes de petición y mensajes de respuesta efectuados realmente. Igualmente puede averiguarse mediante el tiempo de detección del mensaje de respuesta si el mensaje de respuesta se recibió en una ventana temporal preestablecida después de un instante de envío del mensaje de petición. Si los mensajes de petición coinciden con el perfil 17, 17' de petición predeterminado y/o se han recibido los mensajes de respuesta pertenecientes a los mismos en el intervalo de tiempo predeterminado, entonces se transmiten los mismos por ejemplo mediante una red 15 de diagnóstico al dispositivo 19 de diagnóstico. El dispositivo 19 de diagnóstico puede consultar datos detectados de la unidad 13 de evaluación. No obstante, la unidad 13 de evaluación también puede enviar automáticamente datos de diagnóstico por ejemplo en un intervalo de tiempo predeterminado al dispositivo 19 de diagnóstico.

Todas las características descritas y/o esbozadas pueden combinarse entre sí de manera ventajosa en el marco de la invención. La invención no se limita a los ejemplos de realización descritos. En particular la invención no se limita a la red de diagnóstico usada como ejemplo, por ejemplo, de un sistema de protección ferroviaria, sino que también puede emplearse en otros entornos industriales.

A este respecto la unidad 14 de petición también puede estar configurada como unidad físicamente independiente de la unidad de escucha, de la unidad de evaluación, así como de la unidad de alarma. La unidad 21 de escucha puede estar configurada igualmente como unidad físicamente independiente o por el contrario integrada con la unidad 13 de evaluación y la unidad 24 de alarma.

REIVINDICACIONES

1. Procedimiento para capturar datos de al menos un dispositivo (16.1, 16.2, 16.3), que está dispuesto en una primera red (12) con requerimiento de seguridad alto, en una segunda red (11) con requerimiento de seguridad reducido, por medio de un dispositivo que contiene una unidad (14) de petición, una unidad (21) de escucha, una unidad (13) de evaluación y una unidad (24) de alarma, con las etapas de procedimiento de:

- requerir (2) los datos del al menos un dispositivo (16.1, 16.2, 16.3) de manera correspondiente a un perfil (17) de petición por medio de la unidad (14) de petición, que está dispuesta dentro de la primera red (12),

- escuchar (3) los datos enviados desde el al menos un dispositivo (16.1, 16.2, 16.3) en respuesta al requerimiento a la unidad (14) de petición dentro de la primera red (12) por medio de la unidad (21) de escucha, que está dispuesta dentro de la primera red (12), y transmitir los datos a la unidad (13) de evaluación que está dispuesta en la segunda red (11),

- comparar (4) los datos escuchados con los datos esperados según el perfil (17, 17') de petición por medio de la unidad de evaluación, y

- proporcionar (5) una señal de alarma por medio de la unidad de alarma, si los datos escuchados difieren de los datos esperados según el perfil (17, 17') de petición,

en el que el perfil (17, 17') de petición contiene peticiones predeterminadas y un esquema temporal relativo al momento en que estas peticiones deben enviarse al al menos un dispositivo en la primera red, la unidad (21) de escucha sólo puede escuchar datos que se transfieren a la primera red (11) y no puede enviar mensajes de ningún tipo a los dispositivos (16.1, 16.2, 16.3) y tampoco ningún mensaje a la unidad (14) de petición, y la unidad (13) de evaluación comprueba los datos escuchados contra un perfil (17) de petición que corresponde al perfil (17') de petición en la unidad (14) de petición, y reenvía sólo datos escuchados que corresponden al perfil (17, 17') de equipo a un ordenador (19) de diagnóstico dispuesto en la segunda red (11).

2. Procedimiento según la reivindicación 1, en el que se visualiza por medio de la señal de alarma un aviso de alarma en la unidad (13) de evaluación y/o en un dispositivo (19) de diagnóstico en una red (15) de diagnóstico y/o se crea una entrada en un informe de monitorización y/o se desencadena una reacción activa en la unidad (21) de escucha y/o una reacción activa en la unidad (14) de petición.

3. Procedimiento según la reivindicación 2, en el que se bloquea por medio de la señal de alarma una retransmisión de los datos escuchados por medio de la unidad (13) de evaluación o una lectura de los datos escuchados desde la unidad (13) de evaluación.

4. Procedimiento según cualquiera de las reivindicaciones 1 a 3, en el que el perfil (17) de petición presenta reglas de petición distintas para tipos de datos distintos y/o para tipos distintos de dispositivos y/o para dispositivos (16.1, 16.2, 16.3) individuales.

5. Procedimiento según cualquiera de las reivindicaciones 1 a 4, en el que el perfil (17) de petición presenta una regla de petición unificada para tipos de datos distintos y/o para tipos de dispositivo distintos y/o para los dispositivos (16.1, 16.2, 16.3) individuales en sí mismos.

6. Procedimiento según cualquiera de las reivindicaciones 2 a 5, en el que los datos escuchados se memorizan en memoria intermedia en la unidad (13) de evaluación y sólo se transmiten al dispositivo (19) de diagnóstico después de una comprobación satisfactoria.

7. Procedimiento según la reivindicación 6, en el que existe entonces una comprobación satisfactoria cuando los datos escuchados corresponden al perfil (17, 17') de petición y/o cuando los datos escuchados presentan una suma de comprobación criptográfica válida.

8. Procedimiento según la reivindicación 6 ó 7, en el que en el caso de una comprobación no satisfactoria se transmite un valor de sustitución o un aviso de error al dispositivo (19) de diagnóstico.

9. Procedimiento según cualquiera de las reivindicaciones 1 a 8, en el que se asocian los datos escuchados en la unidad (13) de evaluación después de comprobar una información de validez.

10. Procedimiento según cualquiera de las reivindicaciones 1 a 9, en el que los datos escuchados sólo se transmiten entonces al ordenador (19) de diagnóstico si se recibieron los datos escuchados en un intervalo de tiempo predeterminado después de la petición asociada en la unidad (13) de evaluación.

11. Dispositivo para capturar datos de al menos un dispositivo (16.1, 16.2, 16.3), que está dispuesto en una primera red (12) con requerimiento de seguridad alto, en una segunda red (11) con requerimiento de seguridad reducido, que contiene

- una unidad (14) de petición, que está dispuesta dentro de la primera red (12) y configurada para requerir datos del al menos un dispositivo (16.1, 16.2, 16.3) de manera correspondiente a un perfil (17, 17') de petición,

- una unidad (21) de escucha, que está dispuesta dentro de la primera red (12) y configurada para escuchar datos que se enviaron desde el al menos un dispositivo (16.1, 16.2, 16.3) en respuesta al requerimiento y transmitir los mismos a una unidad (13) de evaluación y no enviar mensajes de ningún tipo a los dispositivos (16.1, 16.2, 16.3) y tampoco ningún mensaje a la unidad (14) de petición,

- una unidad (13) de evaluación, que está dispuesta en la segunda red (11) y configurada para comparar los datos escuchados con los datos esperados según el perfil (17, 17') de petición, y comprueba los datos escuchados contra un perfil (17) de petición que corresponde al perfil (17') de petición en la unidad (14) de petición, y para reenviar sólo datos escuchados que corresponden al perfil (17, 17') de equipo a un ordenador (19) de diagnóstico dispuesto en la segunda red, y

- una unidad (24) de alarma, que está configurada para proporcionar una señal de alarma cuando los datos escuchados difieren de los datos esperados según el perfil (17, 17') de petición, en el que el perfil de petición contiene peticiones predeterminadas y un esquema temporal relativo al momento en que estas peticiones deben enviarse al al menos un dispositivo en la primera red.

12. Dispositivo según la reivindicación 11, en el que la unidad (21) de escucha y/o la unidad (14) de petición están configuradas para reconocer una señal de alarma y para reiniciarse de manera autónoma a continuación o la unidad (13) de evaluación está configurada para bloquear una retransmisión o una lectura de los datos escuchados después del reconocimiento de la señal de alarma.

13. Dispositivo según cualquiera de las reivindicaciones 11 ó 12, en el que la unidad (13) de evaluación está configurada para memorizar datos escuchados, para realizar una comprobación de los datos y para transmitir los datos a un dispositivo (19) de diagnóstico sólo después de una comprobación satisfactoria.

14. Dispositivo según la reivindicación 13, en el que la unidad (13) de evaluación está configurada para comprobar si los datos escuchados corresponden al perfil (17, 17') de petición y/o si los datos escuchados presentan una suma de comprobación criptográfica válida, y para transmitir únicamente los datos comprobados satisfactoriamente al dispositivo (19) de diagnóstico o para transmitir, en el caso de una comprobación no satisfactoria, un valor de sustitución o un mensaje de error al dispositivo (19) de diagnóstico.

15. Producto de programa informático con instrucciones de programa para realizar un procedimiento según las reivindicaciones 1-10.

FIG 1

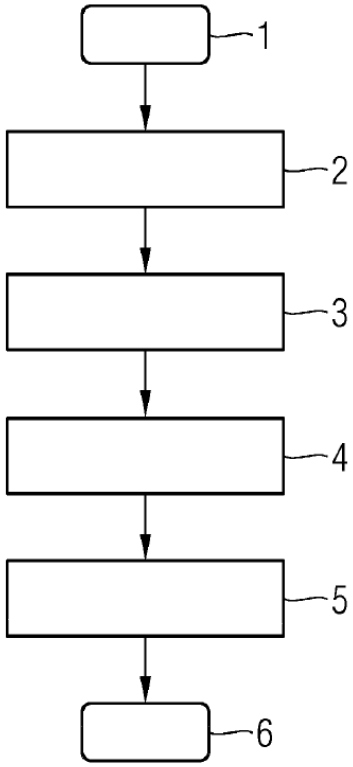
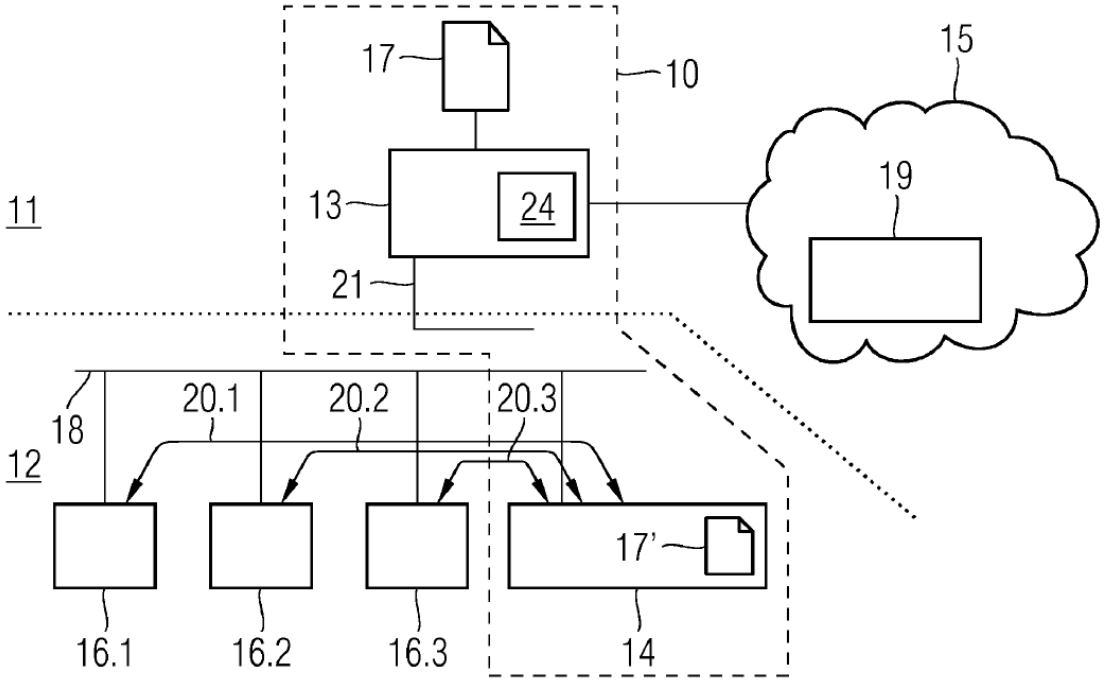


FIG 2



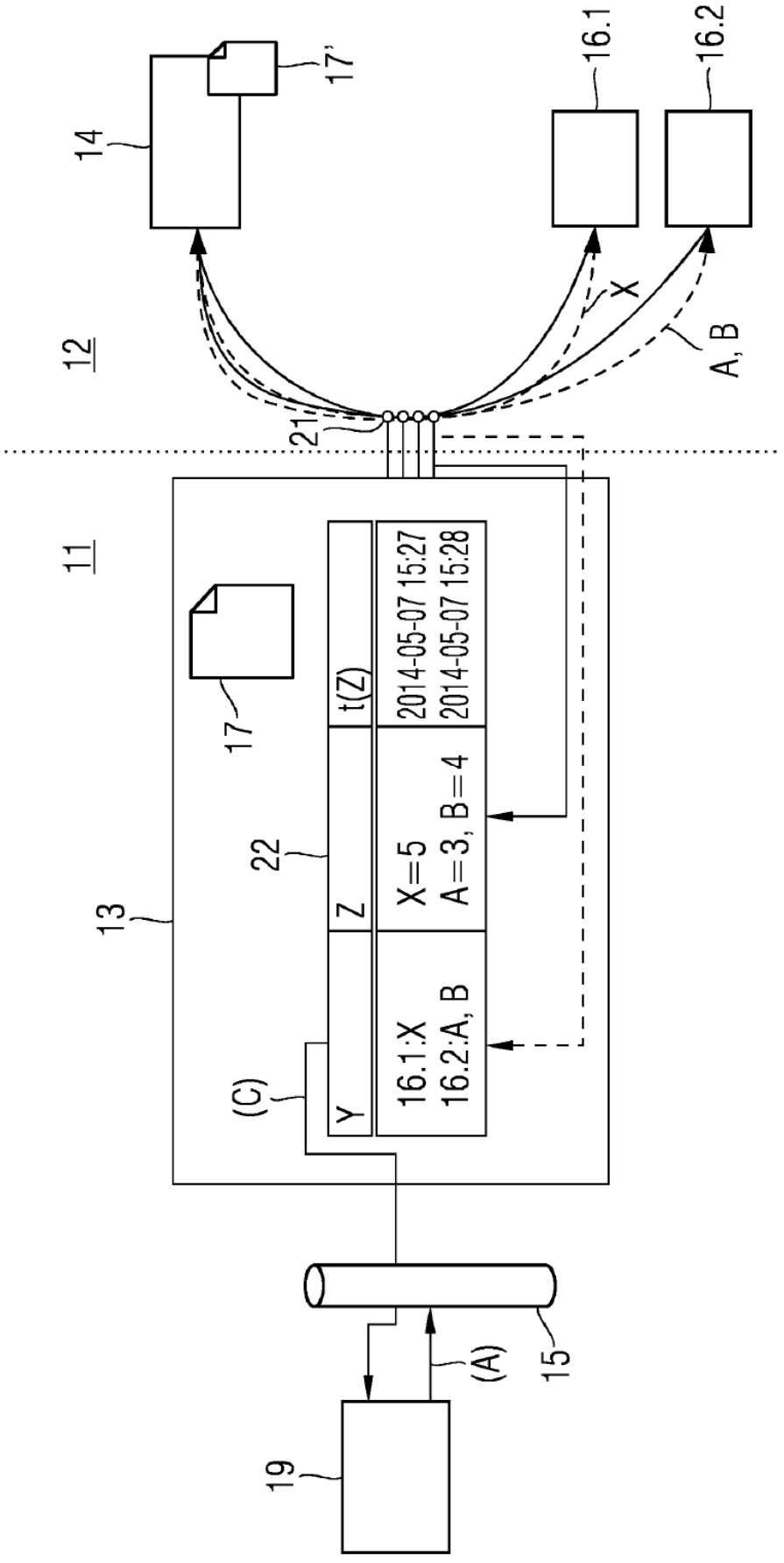

14
17'
16.1
16.2
12
X
A, B
21
11
17
t(Z)
2014-05-07 15:27
2014-05-07 15:28
22
Z
X=5
A=3, B=4
13
Y
16.1:X
16.2:A, B
(C)
(A)
15
19

FIG 3