(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 751 098**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **03.04.2012 PCT/EP2012/056026**

(87) Fecha y número de publicación internacional: **18.10.2012 WO12139924**

(96) Fecha de presentación y número de la solicitud europea: **03.04.2012 E 12715009 (2)**

(97) Fecha y número de publicación de la concesión europea: **04.09.2019 EP 2656581**

(54) Título: **Equipo de acoplamiento a red y procedimiento de transmisión para redes de datos basadas en paquetes en sistemas de mando de procesos o sistemas de mando de la operación**

(30) Prioridad:

14.04.2011 DE 102011007387

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.03.2020

(73) Titular/es:

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

(72) Inventor/es:

FALK, RAINER;
FRIES, STEFFEN;
SATTLER, CARSTEN y
SEIFERT, MATTHIAS

(74) Agente/Representante:

LOZANO GANDIA, José

DESCRIPCIÓN

Equipo de acoplamiento a red y procedimiento de transmisión para redes de datos basadas en paquetes en sistemas de mando de procesos o sistemas de mando de la operación

La presente invención se refiere al sector de la técnica de mando de procesos y de la técnica de mando de la operación, en particular a equipos de acoplamiento a red y procedimientos de transmisión para redes de datos de campo basadas en paquetes en sistemas de mando de procesos o sistemas de mando de la operación.

Hoy en día existe una pluralidad de sectores en los que es necesario regular secuencias y procesos complejos. Estos sectores pueden ser por ejemplo la técnica de proceso, la técnica del tráfico, la técnica de la automatización, así como la técnica de fabricación u otros sectores técnicos. En todos estos sectores técnicos se utilizan instalaciones compuestas por una pluralidad de sensores, actuadores y equipos de control. Entonces sirve la técnica de mando para hacer posible el control y vigilancia de estos sistemas complejos. En la técnica de mando se dividen las instalaciones usualmente en distintos niveles. Al respecto son de especial importancia el nivel de campo, que por ejemplo contiene actuadores y sensores, así como el nivel de mando, que a menudo se realiza a través de un puesto de mando. En instalaciones técnicas sencillas se encuentra el puesto de mando en un lugar próximo al nivel de campo. Usualmente está conectado el puesto de mando con el nivel de campo directamente a través de una red de datos. En instalaciones complejas y extendidas en el espacio se reúne el nivel de campo formando una red propia y se conecta con el puesto de mando, por ejemplo mediante una pasarela (gateway).

Al respecto las pasarelas posibilitan una comunicación entre dos redes distintas. En el caso de la técnica de mando hacen posible las mismas en particular la comunicación entre la red del nivel de campo y el puesto de mando. Entre la pasarela del nivel de campo y el puesto de mando pueden encontrarse entonces otras redes, por ejemplo redes públicas, como Internet. Esto hace posible por un lado prever el puesto de mando alejado localmente del nivel de campo y por otro lado ello exige una conexión segura entre la pasarela del nivel de campo y el puesto de mando.

Por el documento EP 1 682 952 B1 se conoce un procedimiento para el mantenimiento de aparatos de campo con un ordenador de mantenimiento del fabricante de los aparatos, acoplando un servidor de relés en una red pública, por un tiempo limitado, una red del nivel de campo con una red del nivel de mando, con lo que un ordenador de mantenimiento de la red del nivel de mando puede realizar un enlace peer-to-peer (entre iguales) con un aparato de campo en la red del nivel de campo.

Si se realizase el enlace entre el puesto de mando y la pasarela del nivel de campo sin aseguramiento a través de redes públicas, las faltas en la transmisión de datos a través de la red pública, así como también atacantes malignos, pueden falsear los datos y ello puede incidir en el control de los sensores y actuadores del nivel de campo.

Por esta razón pueden realizar las pasarelas por ejemplo una adaptación y/o conversión de mensajes de protocolo. Esta adaptación y/o conversión de mensajes de protocolo puede consistir en el encriptado de determinados mensajes de protocolo, así como en el aseguramiento de mensajes de protocolo mediante sumas de comprobación o similares.

Una aplicación de una tal pasarela se encuentra por ejemplo en el control de la técnica de mando de la operación en el tráfico ferroviario. Al respecto es usual que la unidad de mando esté espacialmente bastante alejada del nivel de campo propiamente dicho. Para garantizar una transmisión de datos segura entre el puesto de mando y los sensores y/o actuadores del nivel de campo, se realiza para la comunicación de datos entre el puesto de mando y la pasarela del nivel de campo una transmisión de datos basada en paquetes, por ejemplo basada en IP e IPSEC. Además para la comunicación entre los distintos sensores y/o actuadores y el puesto de mando se utiliza por ejemplo Profisafe como protocolo de transmisión para datos críticos para la seguridad. En el marco de esta solicitud de patente se utiliza el concepto "crítico para la seguridad" como el concepto inglés "safety critical". Esto significa que una aplicación crítica para la seguridad es una aplicación que puede originar un peligro para la salud y la vida si se presenta una falta en la instalación. Este es el caso, por ejemplo en el tráfico ferroviario, en el control de las luces de señales.

En las pasarelas actuales se utilizan, para asegurar la comunicación, además de las funciones de seguridad antes citadas, los llamados sistemas de detección de intrusión en la red, que detectan un ataque a un componente de la red. Al respecto pueden detectar estos sistemas de detección de intrusión en la red patrones de ataque conocidos, que por ejemplo significan una desviación de un comportamiento de comunicación definido como consigna para la red. En general se conocen también circuitos watchdog (de perro guardián), que vigilan un ordenador y/o el software que corre sobre el mismo y que cuando se produce una parada del sistema, arrancan de nuevo el sistema mediante una señal de reset o reposición.

Pese a las medidas preventivas de seguridad antes citadas, no queda excluido que en una pasarela, debido a un problema de software o debido a la penetración de un atacante desde el exterior a través de la pasarela, presente la pasarela un comportamiento imprevisto o no deseado.

Por ejemplo podría suceder que una pasarela genere y envíe autónomamente mensajes de red. El envío autónomo de mensajes por parte de la pasarela no origina usualmente problemas, ya que el enlace con los distintos componentes del nivel de campo se protege mediante un protocolo concebido para aplicaciones críticas para la seguridad, como por ejemplo Profisafe. Desde luego es deseable poder detectar una pasarela defectuosa o influida por un atacante y poder eventualmente eliminar la falta.

Por lo tanto el objetivo de la presente invención es proporcionar una posibilidad para operar una pasarela con gran fiabilidad.

En el marco de la invención se logra este objetivo mediante un equipo de acoplamiento a red con las características de la reivindicación 1 y un procedimiento de transmisión con las características de la reivindicación 12.

En consecuencia está previsto:

- un equipo de acoplamiento a red con las características de la reivindicación 1 y
- un procedimiento de transmisión para una red de datos de campo con las características de la reivindicación 11.

El conocimiento que sirve de base a la presente invención consiste en que, cuando la pasarela funciona sin faltas, cuando se envía un paquete de datos determinado debe recibirse un paquete de datos correspondiente, antes de que se envíe el paquete de datos a enviar.

La idea que sirve de base a la presente invención consiste pues en tener en cuenta este conocimiento y prever un equipo de acoplamiento a red que presente un dispositivo de vigilancia que realice una contabilidad relativa a la cantidad de paquetes de datos salientes y entrantes en el equipo de transmisión del equipo de acoplamiento a red. Un tal dispositivo de vigilancia comprueba para cada paquete de datos a enviar que detecta el dispositivo de vigilancia en una de las interfaces de comunicación del equipo de acoplamiento a red, si previamente se ha recibido un paquete de datos correspondiente a través de otra interfaz de comunicación del equipo de acoplamiento a red.

Mediante la utilización de un tal dispositivo de vigilancia resulta posible detectar si el equipo de acoplamiento a red funciona correctamente y sólo envía paquetes de datos para los cuales ha recibido el mismo previamente un paquete de datos correspondiente. De esta manera ha de quedar asegurado que no aparecen paquetes de datos a partir de la "nada". No obstante, si se detecta esto, entonces indica esto que hay una falta o bien una influencia sobre el equipo de acoplamiento a red.

Ventajosas variantes de configuración y perfeccionamientos resultan de las demás reivindicaciones secundarias, así como de la descripción con referencia a las figuras del dibujo.

En una forma de ejecución ventajosa identifica el dispositivo de vigilancia, en base a una dependencia en el tiempo, un paquete de datos correspondiente. La asociación de un paquete de datos enviado a un paquete de datos previamente recibido, basándose en una dependencia en el tiempo, posibilita una asociación rápida y sencilla de paquetes de datos entrantes a paquetes de datos enviados. En la pasarela puede determinarse por ejemplo para cada paquete de datos entrante después de cuántos segundos ha de enviarse un paquete de datos. Por ejemplo pueden prescribirse para ello 5 segundos, en particular también tiempos inferiores a 1 segundo, pero en particular también tiempos inferiores a 10 milisegundos o inferiores a 1 milisegundo.

En otra forma de ejecución ventajosa identifica el dispositivo de vigilancia, basándose en un contenido de datos de una cabecera de paquete, un paquete de datos correspondiente. El contenido en datos de una cabecera de paquete presenta informaciones detalladas relativas a los distintos paquetes de datos. Por ello permite la comparación de contenidos de datos de una cabecera de paquete correspondiente a un paquete de datos enviado con el contenido de una cabecera de paquete correspondiente un paquete de datos recibido, una asociación exacta del paquete de datos entrante al que se ha enviado. Los contenidos de datos de una cabecera de paquete a comparar mediante el dispositivo de vigilancia pueden presentar por ejemplo informaciones de versión, informaciones del tamaño del paquete, direcciones o similares.

En otra forma de ejecución ventajosa adicional, identifica el dispositivo de vigilancia, basándose en una dirección del remitente y/o una dirección del receptor, un paquete de datos correspondiente. Usualmente envía la unidad de mando de una instalación paquetes de datos a distintos componentes de la instalación. Por ello es posible, basándose en la dirección del remitente y la dirección del receptor de un paquete de datos, una asociación exacta de paquetes de datos entrantes a paquetes de datos enviados de la pasarela. Las direcciones del remitente y/o receptor pueden ser entonces direcciones de remitente y/o receptor de IP, pero también direcciones de remitente y receptor de otros protocolos.

En otra forma de ejecución ventajosa identifica el dispositivo de vigilancia, basándose en datos útiles, un paquete de datos correspondiente. Dado que la unidad de mando transmite a los distintos sensores o actuadores de una instalación de técnica de automatización usualmente distintos datos, puede realizarse eficientemente una identificación de los paquetes de datos entrantes y emitidos por la pasarela en base a los datos útiles. Al respecto pueden trasmitirse los datos útiles encriptados o sin encriptar. Cuando se reciben de la pasarela datos útiles encriptados y se envían sin modificar como datos útiles encriptados, entonces es fácilmente posible comparar los datos útiles encriptados, sin desencriptarlos. Si por el contrario se recibe de la pasarela un paquete de datos con datos útiles encriptados, que envía la pasarela por ejemplo sin encriptar sobre el bus de datos, entonces debe realizar igualmente el dispositivo de vigilancia el desencriptado del paquete de datos, para poder comparar los contenidos del paquete.

En otra forma de ejecución ventajosa presenta al menos una de las interfaces de comunicación una interfaz de Ethernet, una interfaz de Profibus, una interfaz de teléfono móvil, una interfaz de UMTS, una interfaz WLAN, una interfaz LTE, una interfaz CAN, una interfaz Flexray, una interfaz de comunicación HART, otra interfaz de bus de campo u otra interfaz SPI o bien una interfaz I^2C. La utilización de distintas interfaces de comunicación, que se utilizan hoy en día usualmente en instalaciones de técnica de automatización tanto en el nivel de campo como también en el nivel del puesto de mando, hace posible una utilización flexible del equipo de acoplamiento a red en las más diversas aplicaciones y campos de utilización.

En otra forma de ejecución ventajosa adicional, está configurado el dispositivo de vigilancia para hacer el rearranque o la desconexión del equipo de transmisión en el caso de que para un número que puede determinarse de paquetes de datos enviados a través de la interfaz de comunicación del equipo de acoplamiento a red no se haya recibido ningún paquete de datos correspondiente a través de otra interfaz de comunicación del equipo de acoplamiento a red. Puesto que el código de programa que ejecuta la pasarela está archivado en una memoria flash que no puede reescribirse y este código de programa se carga al arrancar el equipo de acoplamiento a red en una memoria RAM, desde la cual se ejecuta a partir de este código, origina un rearranque del equipo de acoplamiento a red la nueva carga en la RAM del código de programa inicialmente escrito en la memoria flash. De esta manera pueden retrotraerse modificaciones realizadas debido a una RAM defectuosa o mediante una penetración desde el exterior en el código de programa en la memoria RAM. Si además se configura de forma flexible la cantidad de faltas en la comunicación de datos del equipo de acoplamiento a red que origina un rearranque del equipo de acoplamiento a red, entonces es posible adaptar el equipo de acoplamiento a red a distintas exigencias. La cantidad de paquetes de datos que pueden tolerarse, que envía una interfaz de comunicación del equipo de acoplamiento a red, en correspondencia a los cuales no se ha recibido ningún paquete de datos, puede fijarse en aplicaciones muy críticas por ejemplo igual a 1 y en otras aplicaciones puede fijarse este número también en un valor más alto, por ejemplo en 5, 10 ó 20.

En otra forma de ejecución ventajosa, presenta el dispositivo de vigilancia una interfaz de comunicación de alarmas y está constituido para emitir una señal de alarma a través de la interfaz de comunicación de alarmas cuando a un número que puede fijarse de paquetes de datos enviados a través de una interfaz de comunicación del equipo de acoplamiento a red no se ha recibido ningún paquete de datos correspondiente a través de otra interfaz de comunicación del equipo de acoplamiento a red. Si se prevé en el dispositivo de vigilancia una interfaz de comunicación de alarmas, puede informar el dispositivo de vigilancia a través de esta interfaz de comunicación de alarmas por ejemplo al operador de un puesto de mando que está acoplado con la pasarela a través de una red de datos pública, sobre la aparición de un comportamiento defectuoso en la pasarela. De esta manera le resulta posible al operador del puesto de mando prever medidas para solucionarlo. La interfaz de comunicación de alarmas del dispositivo de vigilancia puede realizarse entonces igualmente mediante una red de datos basada en paquetes. Pero en otras formas de ejecución puede presentar la interfaz de comunicación de alarmas del dispositivo de vigilancia también una interfaz de teléfono móvil, por ejemplo una interfaz UMTS o una interfaz LTE. En otras formas de ejecución más, puede estar realizada la interfaz de comunicación de alarmas en forma de una indicación auditiva o visual en el equipo de acoplamiento a red. Esto puede realizarse por ejemplo mediante altavoces o una pantalla gráfica.

En otra forma de ejecución ventajosa está constituido el dispositivo de vigilancia como un módulo lógico reconfigurable, FPGA, un microprocesador, un circuito eléctrico específico de la aplicación o un equipo de ordenador programable. Esto hace posible una estructura eficiente del dispositivo de vigilancia y con ello también una integración eficiente y fácil del dispositivo de vigilancia en el equipo de acoplamiento a red.

En otra forma de ejecución ventajosa está constituido el dispositivo de vigilancia como un producto de programa de computadora, que está previsto en el equipo de transmisión. Cuando esta previsto el dispositivo de vigilancia como un producto de programa de computadora, puede integrarse el mismo fácilmente en equipos de transmisión existentes. Además es fácil portar un producto de programa de computadora a otra arquitectura de hardware si debe utilizarse el dispositivo de vigilancia en distintos equipos de transmisión. Entonces puede implementarse el dispositivo de vigilancia en un lenguaje de

programación procedimental, como por ejemplo C o un lenguaje de programación orientado al objeto, como por ejemplo Java o C++.

En otra forma de ejecución ventajosa está previsto en el equipo de acoplamiento de red un zócalo o un equipo de conexión, estando previsto el dispositivo de vigilancia en una placa de circuitos separada, que puede alojarse en el zócalo o que puede acoplarse con el equipo de conexión. Si está previsto el dispositivo de vigilancia en una placa de circuitos separada, entonces es posible una sustitución sencilla y flexible de esta placa de circuitos y con ella del dispositivo de vigilancia en un equipo de acoplamiento a red. Esto es especialmente ventajoso cuando el dispositivo de vigilancia está realizado por razones de seguridad en un módulo semiconductor, que sólo puede configurarse o programarse una única vez. Si estuviera integrado o por ejemplo soldado un tal módulo fijamente en un equipo de acoplamiento a red, entonces sería difícilmente posible sustituir este módulo. Pero una placa de circuitos separada que contiene el dispositivo de vigilancia puede sustituirse fácilmente en todo momento.

En otras formas de ejecución presenta el dispositivo de vigilancia en cada caso una interfaz con las interfaces de comunicación del equipo de acoplamiento a red, para desconectar las interfaces de comunicación del equipo de acoplamiento a red. Esto hace posible desactivar un equipo de acoplamiento a red incluso cuando el equipo de transmisión no reacciona a órdenes de desconexión. En un tal caso seguiría enviando el equipo de transmisión paquetes de datos, pero las interfaces de comunicación no retransmitirían estos paquetes de datos.

El dispositivo de vigilancia puede integrarse con el equipo de transmisión conjuntamente en una carcasa. En un tal caso puede captar el dispositivo de vigilancia la comunicación de datos del equipo de transmisión entre las interfaces de comunicación y el equipo de transmisión de datos. En otra forma de ejecución puede captar el dispositivo de vigilancia la comunicación del equipo de transmisión también entre las interfaces de comunicación y la correspondiente red. Si capta el dispositivo de vigilancia la comunicación de datos en el equipo de transmisión entre el equipo de transmisión y las interfaces de comunicación, entonces presenta el dispositivo de vigilancia una interfaz que está constituida para captar esa comunicación. Ésta es usualmente una interfaz SPI o una interfaz I^2C. Para la comunicación de datos entre el equipo de transmisión y las interfaces de comunicación pueden utilizarse también otras interfaces. Éstas pueden ser por ejemplo enlaces de datos digitales paralelos o serie. Si capta el dispositivo de vigilancia el tráfico en la red del equipo de transmisión entre las interfaces de comunicación del equipo de acoplamiento a red y las redes propiamente dichas, entonces presenta el dispositivo de vigilancia elementos de acoplamiento que permiten al dispositivo de vigilancia captar directamente el tráfico de red correspondiente a las redes de datos. Al respecto puede tratarse por ejemplo de una interfaz Ethernet, una interfaz Profibus, una interfaz de fibra de vidrio o similares. Un dispositivo de vigilancia puede estar previsto en una carcasa propia, que por ejemplo presenta conexiones de Ethernet, para poder conectar el equipo de vigilancia con un conmutador o un enrutador al que está conectado el equipo de acoplamiento a red.

Las variantes y perfeccionamientos antes citados pueden combinarse entre sí de cualquier forma, siempre que ello tenga sentido. Otras posibles variantes, perfeccionamientos e implementaciones de la invención incluyen también la combinación no explícitamente citada de características de la invención antes descritas o descritas a continuación relativas a los ejemplos de ejecución. En particular añadirá el especialista al respecto también aspectos individuales como mejoras o complementos relativos a la correspondiente forma básica de la presente invención.

La presente invención se describirá a continuación más en detalle en base a los ejemplos de ejecución indicados en las figuras esquemáticas de los dibujos. Al respecto se muestra en:

figura 1 un esquema de circuitos en bloques de una forma de ejecución de un equipo de acoplamiento a red correspondiente a la invención;
figura 2 un diagrama secuencial de una forma de ejecución de un procedimiento de transmisión correspondiente a la invención;
figura 3 una forma de ejecución de un equipo de acoplamiento a red correspondiente a la invención, que está acoplado con un bus de campo y una unidad de mando.

En las figuras de los dibujos se han dotado los elementos, características y componentes iguales y los que tienen las mismas funciones en cada caso de las mismas referencias, salvo indicación en contra.

La figura 1 muestra un esquema de circuitos en bloques de una forma de ejecución de un equipo de acoplamiento a red correspondiente a la invención.

Al respecto se representa en la figura 1 con la referencia 1 un equipo de acoplamiento a red, que presenta dos interfaces de comunicación 2 y 3, que están acopladas con un equipo de transmisión 4. Además presenta el equipo de acoplamiento a red 1 en la figura 1 un dispositivo de vigilancia 5. El dispositivo de vigilancia 5 está acoplado con la línea de transmisión de datos 6, que conecta la interfaz de comunicación

2 con el equipo de transmisión 4. Además está acoplado el dispositivo de vigilancia 5 con la línea de transmisión de datos 7, que conecta la interfaz de comunicación 3 con el equipo de transmisión 4.

El equipo de acoplamiento a red 1 de la figura 1 está alojado en un armario de maniobra, que por ejemplo está emplazado en una zona de operación de una estación de ferrocarril. La interfaz de comunicación 2 conecta el equipo de acoplamiento a red 1 mediante una conexión Ethernet con una red de datos pública, en particular Internet 8, tal como se representa en la figura 3. La interfaz de comunicación 3 conecta el equipo de acoplamiento a red 1 por ejemplo con una red de datos de campo 12 de una estación ferroviaria, que se basa en Profibus. En otras formas de ejecución puede conectar la interfaz de comunicación 2 el equipo de acoplamiento a red 1 por ejemplo a través de un enlace WLAN, un enlace UMTS, un enlace LTE u otro enlace de datos con Internet 8. La interfaz de comunicación 3 puede ser, en vez de una interfaz Profibus, igualmente una interfaz Ethernet, pero también una interfaz de bus CAN, una interfaz Flexray, una interfaz LIN, una interfaz RS232, una interfaz de radio, por ejemplo una interfaz ZigBee, una interfaz Bluetooth, una interfaz NFC o una interfaz WLAN.

El equipo de transmisión 4 de la figura 1 es una computadora u ordenador con un procesador x86, que como sistema operativo por ejemplo ejecuta un sistema operativo basado en Linux. El sistema operativo está memorizado entonces con preferencia en una memoria flash, que sólo puede escribirse con herramientas especiales. Cuando se conecta el equipo de transmisión 4, carga el equipo de transmisión 4 el sistema operativo desde la memoria flash en una memoria RAM, desde la cual se ejecuta el sistema operativo. En otras formas de ejecución está integrado el equipo de transmisión 4 en un sistema de computadora embebido (embedded), que se basa en un procesador ARM y que ejecuta un Embedded Lynux, que es adecuado para tales procesadores ARM. En otras formas de ejecución no está memorizado el sistema operativo en una memoria flash, sino sobre un soporte de datos externo, como por ejemplo un CD o una memoria USB que no puede reescribirse.

Las líneas de transmisión de datos 6 y 7 son líneas de transmisión de datos que constituyen un bus SPI entre el equipo de transmisión 4 y las interfaces de comunicación 2 y 3. En otras formas de ejecución pueden ser estas líneas de transmisión de datos líneas de bus I^2C o líneas de transmisión de datos digitales directas serie y/o paralelo.

El dispositivo de vigilancia 5 de la figura 1 puede ser un FPGA, que está configurado para vigilar el tráfico de datos sobre las líneas de transmisión de datos 6 y 7. El FPGA 5 está montado entonces con preferencia sobre una tarjeta insertable, que se asienta en un zócalo del equipo de acoplamiento a red 1.

En otras formas de ejecución está constituido el dispositivo de vigilancia 5 como sistema de computadora embedded o como ASIC.

La figura 2 muestra un diagrama secuencial de una forma de ejecución de un procedimiento de transmisión correspondiente a la invención.

En la figura 2 se transmiten en una primera etapa S1 paquetes de datos a través de un equipo de transmisión 4 de un equipo de acoplamiento a red 1. Al respecto se reciben los datos a través de una interfaz de comunicación 2, 3 del equipo de acoplamiento a red 1 y se envían mediante otra interfaz de comunicación 3, 2 del equipo de acoplamiento a red 1. El envío de los datos significa en el contexto de la presente invención que los datos se transmiten a través de una de las interfaces de comunicación 2, 3 del equipo de acoplamiento a red 1.

En una segunda etapa S2 se vigila si para un paquete de datos enviado a través de una interfaz de comunicación 2, 3 del equipo de acoplamiento a red 1 se ha recibido un paquete de datos correspondiente al mismo a través de otra interfaz de comunicación 3, 2 del equipo de acoplamiento a red 1. El equipo de transmisión 4 se vigila mediante el dispositivo de vigilancia 5 en cuanto a si el equipo de transmisión 4 genera paquetes de datos autónomamente y transmite los mismos a través de las interfaces de comunicación 2, 3. Puesto que el equipo de transmisión 4 tiene una función de pasarela (gateway), no debe generar el equipo de transmisión 4 ningún paquete de datos autónomamente. En este contexto se refiere la vigilancia con preferencia sólo a una determinada clase de paquetes de datos, es decir, a aquellos paquetes de datos que cumplen con un determinado criterio. En particular puede referirse la vigilancia a mensajes críticos para la seguridad. Tales mensajes o paquetes de datos críticos para la seguridad pueden ser por ejemplo paquetes de datos del protocolo Profisafe. Así puede generar el equipo de transmisión 4 autónomamente paquetes por ejemplo para un sistema de gestión, para mantenimiento a distancia, sin que el dispositivo de vigilancia 5 lo detecte como defectuoso. Pueden utilizarse también otros protocolos de seguridad, como por ejemplo el protocolo de seguridad abierto (Open-Safety), el protocolo de seguridad CA-Nopen, el protocolo de seguridad CIP y/o el protocolo de seguridad IN-TER-BUS. También pueden transmitirse mensajes de vigilancia relevantes para la seguridad (safety-relevants) y/o mensajes de control safety-relevant mediante un protocolo de control tradicional como por ejemplo Profinet o mediante un protocolo de comunicación general como IP, TCP, UDP, HTTP, RPC, DCOM o un Web-Service.

La figura 3 muestra un diagrama de bloques de una forma de ejecución de un equipo de acoplamiento a red 1 correspondiente a la invención, que a través de una interfaz de comunicación 2 está acoplado con Internet 8 y a través de la misma indirectamente con una unidad de control 9. Además está acoplado el equipo de acoplamiento a red 1 representado en la figura 3 mediante una interfaz de comunicación de alarmas 13 del dispositivo de vigilancia 5 con la unidad de mando 9. Mediante la interfaz de comunicación 3 está conectado el equipo de acoplamiento a red 1 de la figura 3 con una red de datos Profibus, que representa la red de datos de campo de una estación ferroviaria. A través de esta red de datos de campo 12 está acoplado el equipo de acoplamiento a red 1 con un sistema de cambio de vías 10 y una señalización 11 de la estación ferroviaria.

El equipo de acoplamiento a red 1 de la figura 3 se diferencia del equipo de acoplamiento a red 1 de la figura 1 en que el dispositivo de vigilancia 5 presenta además enlaces tanto con las interfaces de comunicación 2 y 3 como también con el equipo de transmisión 4. Además no está conectado el dispositivo de vigilancia 5 con las líneas de transmisión 6 y 7 entre las interfaces de comunicación 2, 3 y el equipo de transmisión 4, sino con las líneas de enlace que conectan las interfaces de comunicación 2 y 3 con las correspondientes redes 8 y 12. Las líneas de enlace entre el dispositivo de vigilancia 5 y las interfaces de comunicación 2 y 3, así como el equipo de transmisión 4, sirven para, cuando se presenta una falta, desconectar los mismos o realizar el rearranque. En la forma de ejecución representada en la figura 3 están realizadas estas líneas como líneas digitales simples, que como señal pueden transmitir un cero o un uno, significando un uno que el aparato allí conectado, es decir, las interfaces de comunicación 2, 3 o el equipo de transmisión 4, debe/n desconectarse o debe ejecutarse un rearranque.

En la figura 3 se representa con la referencia 8 Internet, en forma de una nube. El equipo de acoplamiento a red 1 puede estar acoplado también indirectamente a través de otras redes con Internet 8. Entonces no está conectado el equipo de acoplamiento a red 1 necesariamente a través de una línea de Ethernet con los mismos entre el equipo de acoplamiento a red 1 y redes basadas en Internet 8. Por ejemplo puede estar conectado el equipo de acoplamiento a red 1 a través de una interfaz WLAN o a través de una interfaz UMTS con estas redes. Para lograr una transmisión de datos segura entre la unidad de mando 9 y el equipo de acoplamiento a red 1, puede tener lugar por ejemplo una comunicación basada en IPV4 protegida con IPSEC. En otras formas de ejecución puede no obstante tener lugar también una comunicación basada en IPV6, que se protege mediante IPSEC u otros mecanismos de aseguramiento.

La comunicación entre el equipo de acoplamiento a red 1 y la red de datos de campo 12 de la estación ferroviaria tiene lugar usualmente sin encriptar, puesto que en las estaciones ferroviarias se utilizan ya una pluralidad de aparatos de campo 10, 11, como por ejemplo el sistema de cambio de vías 10 y la señalización 11, que no permiten un encriptado de la transmisión de datos. Desde luego en otras formas de ejecución puede tener lugar también una transmisión de datos encriptada sobre la red de datos de campo 12. En particular está configurado el equipo de acoplamiento a red 1 tal que el mismo puede establecer con determinados aparatos de campo 10, 11 un enlace encriptado y con otros aparatos de campo 10, 100 un enlace no encriptado. Usualmente se transmiten desde la unidad de mando 9 a través de Internet 8 órdenes de mando al equipo de acoplamiento a red 1, que transmite las mismas a los distintos aparatos de campo 10, 11 a través de la red de datos de campo 12. En la dirección contraria transmiten los aparatos de campo 10, 11 a través de la red de datos de campo 12 avisos de estado al equipo de acoplamiento a red 1, que retransmite los mismos a través de Internet 8 a la unidad de mando 9.

En el ejemplo de ejecución representado en la figura 3 identifica el dispositivo de vigilancia 5 los paquetes de datos entrantes pertenecientes a un paquete de datos correspondiente enviado, comparando el instante de llegada del paquete de datos recibido con el de envío del paquete de datos a enviar, así como comparando campos de la cabecera del paquete, que por ejemplo presentan informaciones sobre la versión, informaciones sobre la dirección o similares. En otras formas de ejecución identifica el dispositivo de vigilancia 5 paquetes de datos que se corresponden en base al tamaño del paquete recibido y el del correspondiente paquete de datos a enviar. Al respecto no tiene por qué ser igual el tamaño de los paquetes, sino que pueden presentar, basándose por ejemplo en un encriptado mediante el equipo de acoplamiento a red 1, una determinada diferencia conocida en cuanto a tamaño. En otra forma de ejecución más, identifica el dispositivo de vigilancia 5 paquetes de datos entrantes y paquetes de datos a enviar, que se corresponden entre sí en base a diferencias predeterminadas. Así por ejemplo para un determinado paquete de datos entrante no encriptado debe generarse un paquete de datos a enviar encriptado de una determinada manera. De esta manera puede asegurarse también que el equipo de acoplamiento a red 1 y/o el equipo de transmisión 4 del equipo de acoplamiento a red 1 lleva a cabo medidas de seguridad previstas.

En una forma de ejecución a modo de ejemplo, puede utilizarse el equipo de acoplamiento a red 1 en otros sistemas de mando el procesos, es decir, por ejemplo un sistema para una estación ferroviaria. En particular puede utilizarse el equipo de acoplamiento a red 1 en cualquier clase de instalación de procesos de la técnica de automatización que exija el mando de distintos actuadores y sensores mediante una unidad de mando. Ejemplos de tales instalaciones técnicas de proceso pueden ser instalaciones de control del tráfico, instalaciones de centrales generadoras, instalaciones de automatización en naves de

fabricación, redes de a bordo de trenes, buques o aeronaves, redes de automatización del hogar o por ejemplo redes de aparatos de la técnica médica dentro de hospitales que deben controlarse en un puesto de mando.

Aún cuando la presente invención se ha descrito antes en base a ejemplos de ejecución preferidos, la misma no queda limitada a estos ejemplos, sino que puede modificarse de forma diversa. En particular puede variar o modificarse la invención de forma diversa sin desviarse del núcleo de la invención.

REIVINDICACIONES

1. Equipo de acoplamiento a red (1) para una red de datos del nivel de campo basada en paquetes, con:
   - al menos dos interfaces de comunicación (2, 3), que pueden acoplarse en cada caso con una red de datos (8, 12) y
   - un equipo de transmisión (4) integrado, que está acoplado con las interfaces de comunicación (2, 3) del equipo de acoplamiento a red (1) y que está configurado para transmitir paquetes de datos entre las interfaces de comunicación (2, 3), presentando el equipo de acoplamiento a red (1) un dispositivo de vigilancia (5) que está acoplado con las interfaces de comunicación (2, 3) del equipo de acoplamiento a red (1), estando configurado el dispositivo de vigilancia (5) para vigilar si para un paquete de datos enviado a través de una interfaz de comunicación (2, 3) del equipo de acoplamiento a red (1) se ha recibido un paquete de datos correspondiente al mismo a través de otra interfaz de comunicación (3, 2) del equipo de acoplamiento a red (1).,

   caracterizado porque se vigila si el equipo de transmisión (4) ha generado autónomamente el paquete de datos transmitido a través de la interfaz de comunicación (2, 3),
   presentando el dispositivo de vigilancia (5) una interfaz de comunicación de alarmas (13) y estando constituido para emitir una señal de alarma a través de la interfaz de comunicación de alarmas (13) cuando a un número que puede fijarse de paquetes de datos enviados a través de una interfaz de comunicación (2, 3) del equipo de acoplamiento a red (1) no se ha recibido ningún paquete de datos correspondiente a través de otra interfaz de comunicación (3, 2) del equipo de acoplamiento a red (1).

2. Equipo de acoplamiento a red según la reivindicación 1,
   caracterizado porque el dispositivo de vigilancia (5), basándose en una dependencia en el tiempo, identifica un paquete de datos correspondiente.

3. Equipo de acoplamiento a red según al menos una de las reivindicaciones 1 y 2,
   caracterizado porque el dispositivo de vigilancia (5), basándose en un contenido de datos de una cabecera de paquete, identifica un paquete de datos correspondiente.

4. Equipo de acoplamiento a red según al menos una de las reivindicaciones 1 a 3,
   caracterizado porque el dispositivo de vigilancia (5), basándose en una dirección del remitente y/o una dirección del receptor, identifica un paquete de datos correspondiente.

5. Equipo de acoplamiento a red según al menos una de las reivindicaciones 1 a 4,
   caracterizado porque el dispositivo de vigilancia (5), basándose en datos útiles, identifica un paquete de datos correspondiente.

6. Equipo de acoplamiento a red según al menos una de las reivindicaciones 1 a 5,
   caracterizado porque al menos una de las interfaces de comunicación (2, 3) presenta una interfaz de Ethernet, una interfaz de Profibus, una interfaz de teléfono móvil, una interfaz de UMTS, una interfaz WLAN, una interfaz LTE, una interfaz CAN, una interfaz Flexray, una interfaz de comunicación HART, otra interfaz de bus de campo u otra interfaz SPI o bien una interfaz I^2C.

7. Equipo de acoplamiento a red según al menos una de las reivindicaciones 1 a 6,
   caracterizado porque el dispositivo de vigilancia (5) está configurado para hacer el rearranque o la desconexión del equipo de transmisión (4) en el caso de que para un número que puede determinarse de paquetes de datos enviados a través de una interfaz de comunicación (2, 3) del equipo de acoplamiento a red (1) no se haya recibido ningún paquete de datos correspondiente a través de otra interfaz de comunicación (3, 2) del equipo de acoplamiento a red (1).

8. Equipo de acoplamiento a red según al menos una de las reivindicaciones 1 a 7,
   caracterizado porque el dispositivo de vigilancia (5) está configurado como un módulo lógico reconfigurable, un FPGA, un microprocesador o un equipo de ordenador programable.

9. Equipo de acoplamiento a red según al menos una de las reivindicaciones 1 a 8,
   caracterizado porque el dispositivo de vigilancia (5) está constituido como un producto de programa de software, que está previsto en el equipo de transmisión (4).

10. Equipo de acoplamiento a red según al menos una de las reivindicaciones 1 a 9,
    con un zócalo o un equipo de conexión,
    en el que el dispositivo de vigilancia (5) está previsto en una placa de circuitos separada, que puede alojarse en el zócalo o que puede acoplarse con el equipo de conexión.

11. Procedimiento de transmisión para una red de datos del nivel de campo basada en paquetes, con la etapa:

transmisión (S1) de paquetes de datos a través de un equipo de transmisión (4) de un equipo de acoplamiento a red (1), que se reciben a través de una interfaz de comunicación (2, 3) del equipo de acoplamiento a red (1) y se envían a través de otra interfaz de comunicación (3, 2) del equipo de acoplamiento a red (1), incluyendo la etapa:

vigilancia (S2) de si para un paquete de datos enviado a través de una interfaz de comunicación (2, 3) del equipo de acoplamiento a red (1) se ha recibido un paquete de datos correspondiente al mismo a través de otra interfaz de comunicación (3, 2) del equipo de acoplamiento a red (1),

caracterizado porque se vigila si el equipo de transmisión (4) ha generado autónomamente el paquete de datos transmitido a través de la interfaz de comunicación (2, 3), y

envío de una señal de alarma en el caso de que para un número que puede determinarse de paquetes de datos enviados a través de una interfaz de comunicación (2, 3) del equipo de acoplamiento a red (1) no se haya recibido ningún paquete de datos correspondiente a través de otra interfaz de comunicación (3, 2) del equipo de acoplamiento a red (1).

12. Procedimiento de transmisión según la reivindicación 11,
en el que la vigilancia para al menos una elección de paquetes de datos
presenta la identificación de un paquete de datos correspondiente en base a una dependencia en el tiempo y/o
presenta la identificación de un paquete de datos correspondiente en base a un contenido de datos de una cabecera de paquete y/o
presenta la identificación de un paquete de datos correspondiente en base a una dirección del remitente y/o una dirección del receptor y/o
presenta la identificación de un paquete de datos correspondiente basándose en datos útiles.

13. Procedimiento de transmisión según al menos una de las reivindicaciones 11 y 12,
en el que el equipo de transmisión (4) del equipo de acoplamiento a red (1) rearranca o desconecta en el caso de que para un número que puede determinarse de paquetes de datos enviados a través de una interfaz de comunicación (2, 3) del equipo de acoplamiento a red (1) no se haya recibido ningún paquete de datos correspondiente a través de otra interfaz de comunicación (3, 2) del equipo de acoplamiento a red (1).

FIG 1

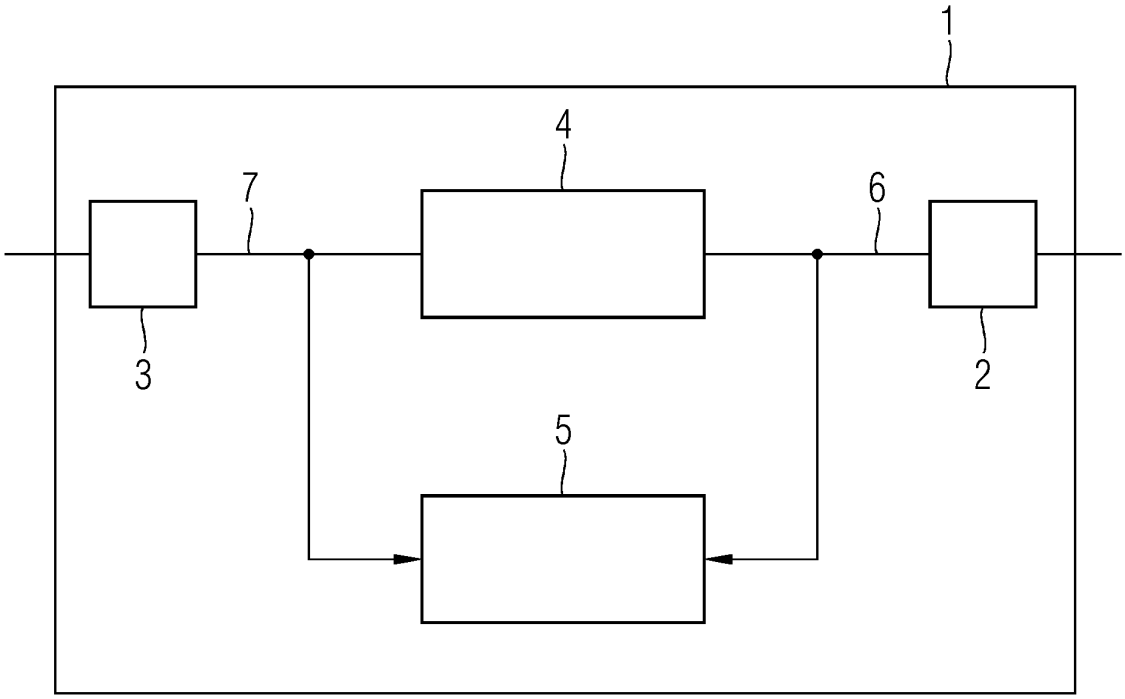

FIG 2

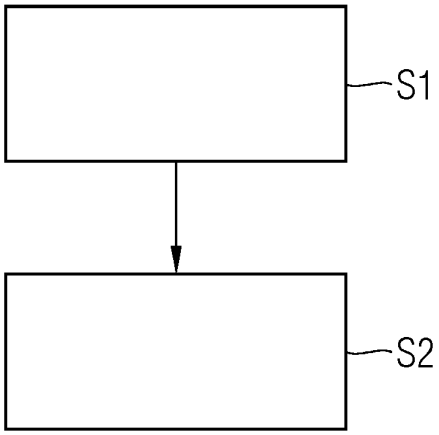

FIG 3