(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 445 894**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **22.06.2010 E 10006472 (4)**

(97) Fecha y número de publicación de la concesión europea: **04.12.2013 EP 2400708**

(54) Título: **Dispositivo de protección de red**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.03.2014

(73) Titular/es:

SIEMENS AKTIENGESELLSCHAFT (100.0%)
Wittelsbacherplatz 2
80333 München, DE

(72) Inventor/es:

ARNOLD, JOHANN;
GERLACH, HENDRIK;
HERBERTH, HARALD;
PLAUM, REINER y
TALANIS, THOMAS

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Dispositivo de protección de red

La presente invención hace referencia a un dispositivo de protección de red para el control de las comunicaciones de un dispositivo de procesamiento de datos externo dispuesto fuera de una red de automatización con un dispositivo de automatización en la red de automatización, en donde se proporciona un protocolo de automatización para las comunicaciones con el dispositivo de automatización.

Esta clase de dispositivos de protección de red se conocen a partir del estado del arte, por ejemplo, a partir de la patente US 2008/0320582.

Las unidades de automatización se integran cada vez más, por ejemplo, en grandes redes de comunicaciones de oficinas que, sin embargo, generalmente resultan accesibles de una manera relativamente abierta. De esta manera, los aspectos de la seguridad cobran cada vez más importancia también en la tecnología de automatización. Para evitar o para reducir los accesos no autorizados a las unidades de automatización, frecuentemente se utilizan los denominados “cortafuegos” como un dispositivo de protección de red. Esta clase de cortafuegos protegen las redes que se encuentran detrás, en tanto que filtran el tráfico de datos hacia la red mencionada, en base a un conjunto de reglas (las denominadas reglas de cortafuegos). Las acciones de filtrado convencionales consisten, por ejemplo, en el bloqueo, rechazo o dejar pasar paquetes de datos.

En general, para la descripción de los procesos de comunicaciones, se utiliza frecuentemente el denominado “modelo de capas OSI”. Dentro del modelo de capas OSI, las tareas individuales en un proceso de comunicaciones se dividen generalmente en siete capas dispuestas unas sobre otras. En el caso de un denominado protocolo de comunicaciones TCP/IP, como se utiliza, por ejemplo, en el estado del arte mencionado a continuación, en este caso la capa de red IP corresponde a la capa OSI 3, mientras que la capa de transporte TCP/UDP corresponde a la capa OSI 4. Por lo tanto, la capa OSI 7 superior corresponde a la denominada “capa de aplicación”, es decir, la capa mencionada contiene los datos de comunicaciones reales que deben ser transmitidos desde el emisor hacia el receptor.

Los dispositivos de protección de red anteriormente mencionados, se conocen, por ejemplo, a partir de la publicación europea EP 2091199 A2, de la declaración de patente alemana DE 103 31 307 A1, o también a partir de la publicación de Estados Unidos US 2008/0320582 A1. Los cortafuegos revelados en dichas declaraciones de patente, toman sus decisiones de filtrado en base a la información que resulta relevante en las capas mencionadas anteriormente, la “capa OSI 3” o la “capa OSI 4”. Los cortafuegos mencionados, conocidos a partir del estado del arte, dictan sus decisiones, por ejemplo, en base a la dirección IP (dirección de origen y/o dirección de destino) (capa OSI 3), a los denominados “puertos” y/o, por ejemplo, a las clases de protocolo IP, como por ejemplo, UDP, TCP, ICMP. Por consiguiente, los cortafuegos conocidos pueden admitir o bloquear determinadas direcciones IP de destino y de origen, así como determinados puertos de destino y, de esta manera, pueden controlar el acceso a una red protegida por los cortafuegos mencionados.

Una desventaja del estado del arte mencionado, consiste en que esta clase de dispositivos de protección de red, siempre se deben adaptar a las modificaciones correspondientes en una red dispuesta detrás, y en que, por ejemplo, en una red de esta clase no se pueden recibir fácilmente unidades con direcciones IP desconocidas. Además, también resulta difícil la recepción de unidades con direcciones IP dinámicas, pero con nombres DNS que permanezcan sin modificaciones.

Por lo tanto, un objeto de la presente invención consiste en proporcionar un dispositivo de protección de red, mediante el cual se pueda proteger desde el exterior, una red de automatización industrial, de una manera flexible y simple contra un acceso no autorizado o no deseado.

Dicho objeto se resuelve mediante un dispositivo de protección de red, de acuerdo con la reivindicación 1.

Además, por un mensaje de protocolo del protocolo de automatización en relación con la presente descripción, se entiende un mensaje de acuerdo con el protocolo de automatización en una de las capas 5 o sobre dichas capas, de acuerdo con el modelo de capas OSI anteriormente mencionado. En particular, por un mensaje de protocolo se entiende un mensaje sobre la capa OSI 7, la denominada capa de aplicación.

Dado que el dispositivo de protección de red consulta el contenido del mensaje de protocolo, para decidir sobre una transmisión o una no transmisión de un mensaje de protocolo entrante, una decisión de esta clase se toma, por ejemplo, independientemente de la información de la dirección sobre el nivel de la capa 3 o de la capa 4, es decir, por ejemplo, independientemente de la dirección IP. Más bien, se llega preferentemente a la información lógica o a las direcciones, independientemente de la configuración de red física concreta. De esta manera, se pueden integrar, por ejemplo, nuevas unidades de una manera simple en una red de automatización, dado que el dispositivo de

protección de red se puede configurar de manera que en el caso de las especificaciones de seguridad, la configuración física de la red no cumple función alguna o bien, cumple una función subordinada.

Los dispositivos de protección de red correspondientes se pueden configurar, por ejemplo, de una manera más simple (se puede realizar, por ejemplo, el establecimiento de las reglas de filtrado), dado que las reglas de protocolo correspondientes también se pueden crear sin conocimientos concretos de la configuración física de la red. Un dispositivo de protección de red de esta clase, permite admitir o prohibir, por ejemplo, determinadas consultas específicas de automatización (por ejemplo, cambios de parametrización, diagnósticos, cambios de modos de funcionamiento), en donde las admisiones o bien, prohibiciones mencionadas de esta clase de consultas, pueden ser específicas, por ejemplo, del usuario o bien, del cliente. Mediante la transferencia de los criterios de selección de un dispositivo de protección de red de esta clase, a los contenidos sobre la capa OSI 4, se puede lograr una configuración más flexible y simple de un dispositivo de protección de red, para una red de automatización.

Una red de automatización puede estar conformada, por ejemplo, como una red de automatización industrial. Esta clase de redes de automatización industriales se pueden diseñar, configurar y/o proporcionar, por ejemplo, para el control y/o el ajuste de instalaciones industriales (por ejemplo, instalaciones de producción, de transporte, etc.), máquinas y/o equipos. En particular, las redes de automatización o bien, las redes de automatización industriales pueden presentar protocolos de comunicaciones en tiempo real (por ejemplo, Profinet, Profibus, Ethernet en tiempo real) para las comunicaciones, al menos, entre los componentes que participan en las tareas de control y/o de ajuste (por ejemplo, entre las unidades de control y las instalaciones y/o máquinas a controlar).

Además de un protocolo de comunicaciones en tiempo real, también se puede proporcionar, al menos, un protocolo de comunicaciones adicional (que no debe ser, por ejemplo, capaz de operar en tiempo real) en la red de automatización o bien, en la red de automatización industrial, por ejemplo, para la monitorización, la configuración, la reprogramación y/o la reparametrización de una unidad o de una pluralidad de unidades de control en la red de automatización.

Una red de automatización puede comprender, por ejemplo, comunicaciones por hilos y/o comunicaciones sin hilos.

Los dispositivos de protección de red pueden ser, por ejemplo, los denominados “cortafuegos”. Los dispositivos de protección de red pueden estar provistos, por ejemplo, además de la función de protección, con una funcionalidad de “conmutador” o de “enrutador”. Además, esta clase de funcionalidad adicional permite, por ejemplo, un redireccionamiento de mensajes entrantes y salientes, en donde la capacidad de redireccionamiento mencionada no se debe utilizar forzosamente siempre durante el funcionamiento.

Además, la función de protección puede estar provista también, por ejemplo, de una función de “puente”, en la que los mensajes se conducen, por ejemplo, siempre sin modificaciones de dirección.

Sin embargo, la función de un dispositivo de protección de red puede estar limitada a la propia función de protección de los mensajes del protocolo de automatización que se conducen a través del dispositivo mencionado.

Un dispositivo de protección de red se conforma de manera que, al menos, un participante en la red de automatización se encuentra protegido de acuerdo con las reglas de protocolo, ante un acceso no autorizado de terceros. En particular, el dispositivo de protección de red protege de manera correspondiente todos o, al menos, determinados participantes en la red de automatización.

El dispositivo de procesamiento de datos externo se encuentra fuera de la red de automatización, es decir, que no es un participante de la red de automatización. El dispositivo de procesamiento de datos externo se puede encontrar conectado con el dispositivo de protección de red, por ejemplo, a través de una conexión individual, o también puede formar parte de una red adicional de datos o de comunicaciones, como por ejemplo, conectada con Internet, participantes de una red LAN, de una red WAN o también de otra red de automatización adicional.

El dispositivo de procesamiento de datos externo puede comunicar a través del protocolo de automatización, por ejemplo, con, al menos, una unidad, una pluralidad de unidades o todas las unidades de automatización en la red de automatización. Un dispositivo de procesamiento de datos puede ser cualquier clase de ordenador, controlador, unidad de comunicaciones, un terminal de comunicaciones u otra unidad eléctrica o electrónica que sea capaz de realizar comunicaciones con un dispositivo de automatización, o que está diseñada, configurada y/o resulta apropiada para la tarea mencionada.

Un dispositivo de automatización puede ser, por ejemplo, un ordenador, PC y/o un controlador con tareas de control o bien, capacidades para realizar el control. En particular, un dispositivo de automatización puede ser, por ejemplo, un dispositivo de automatización industrial que se puede diseñar, configurar y/o proporcionar, por ejemplo, especialmente para el control y/o el ajuste de instalaciones industriales. En particular, esta clase de dispositivos de automatización o bien, de dispositivos de automatización industriales, pueden ser capaces de funcionar en tiempo

real, es decir, que permiten un control o bien, un ajuste en tiempo real. Para el funcionamiento mencionado, el dispositivo de automatización o bien, el dispositivo de automatización industrial puede comprender, por ejemplo, un sistema de funcionamiento en tiempo real, y/o puede soportar entre otros, al menos, un protocolo de comunicaciones capaz de operar en tiempo real, para realizar las comunicaciones (por ejemplo, Profinet, Profibus, Ethernet en tiempo real).

Un dispositivo de automatización industrial puede ser o puede comprender, por ejemplo, un controlador lógico programable, un módulo o una parte de un controlador lógico programable, un controlador lógico programable integrado en un ordenador o una PC, así como dispositivos de campo correspondientes, sensores y/o actuadores, dispositivos de entrada y/o de salida o similares, para la conexión con un controlador lógico programable.

El dispositivo de protección de red se puede conectar, por ejemplo, con la red de automatización de manera que un acceso desde el exterior a la red de automatización sólo se pueda realizar a través del dispositivo de protección de red. Además, el dispositivo de protección de red se puede integrar en la red de automatización o bien, se puede encontrar conectada con la red mencionada, de manera que también se pueda acceder, al menos, a partes de la red de automatización, sin control por parte del dispositivo de protección de red. De esta manera, el dispositivo de protección de red puede proteger, por ejemplo, sólo partes de la red de automatización o, por ejemplo, sólo controla los mensajes de determinados dispositivos de procesamiento de datos externos.

Como protocolo de automatización en el sentido de la presente invención, se entiende cualquier clase de protocolo que se proporciona, que resulta apropiado y/o que se encuentra configurado para las comunicaciones con dispositivos de automatización de acuerdo con la presente descripción. Esta clase de protocolos de automatización pueden ser, por ejemplo, el protocolo Profibus (por ejemplo, de acuerdo con IEC 61158/EN50170), un protocolo Profibus DP, un protocolo Profibus PA, un protocolo Profinet, un protocolo Profinet IO, un protocolo de acuerdo con la interfaz AS, un protocolo de acuerdo con el enlace IO, un protocolo KNX, un protocolo de acuerdo con una interfaz multipunto (Multipoint Interface, MPI), un protocolo para un acoplamiento punto a punto (Point to Point, PtP), un protocolo de acuerdo con las especificaciones de las comunicaciones S7 (el cual se proporciona y se configura, por ejemplo, para las comunicaciones de controladores lógicos programables de la empresa Siemens) o también un protocolo de Ethernet industrial o un protocolo de Ethernet en tiempo real o bien, otros protocolos específicos para las comunicaciones con unidades de automatización. Como protocolo de automatización en el sentido de la presente descripción, se puede proporcionar también cualquier combinación de los protocolos anteriormente mencionados.

Como se ha explicado anteriormente, por un mensaje de protocolo se puede entender el contenido de un mensaje de comunicaciones entre el dispositivo de procesamiento de datos externo y el dispositivo de automatización, sobre la capa OSI 4, particularmente en la capa OSI 7. Un contenido de uno de los mensajes de protocolo de esta clase, puede comprender o presentar, por ejemplo, uno o una pluralidad de comandos en un dispositivo de automatización, uno o una pluralidad de comandos que se pueden ejecutar mediante un programa de control de un dispositivo de automatización, así como consultas, datos, información, programas o bien, partes de programas, parámetros y/o índices de configuración para el dispositivo de automatización o bien, para la transmisión al dispositivo de procesamiento de datos externo. Además, el contenido del mensaje de protocolo también puede comprender o presentar información lógica de la dirección, información del equipo o información de la clase de equipo.

El dispositivo de protección de red puede estar diseñado de manera que la decisión sobre una transmisión o una no transmisión de un mensaje de protocolo, dependa entre otros de las reglas de protocolo o bien, del contenido del mensaje de protocolo. Además, el dispositivo de protección de red puede estar diseñado de manera que la decisión sobre una transmisión o una no transmisión de un mensaje de protocolo, dependa exclusivamente de las reglas de protocolo o bien, exclusivamente del contenido del mensaje de protocolo.

Un dispositivo de protección de red de acuerdo con la presente descripción, puede bloquear, rechazar (por ejemplo, bloquear con la información correspondiente) o transmitir, por ejemplo, un mensaje de protocolo de acuerdo con la presente descripción, en relación con el contenido del mensaje de protocolo, según la manera en que se deba gestionar en relación con el contenido o bien, con una parte del contenido en vista de las reglas de protocolo y eventualmente de otras reglas.

Un dispositivo de protección de red de acuerdo con la presente descripción, se puede diseñar, por ejemplo, como un cortafuegos de capa OSI 7 con reglas de protocolo de automatización correspondientes.

El dispositivo de protección de red se puede conformar, por ejemplo, de manera que en el caso de una no transmisión del mensaje de protocolo, se envíe un mensaje con información en relación con la no transmisión, en correspondencia con el protocolo de automatización, al dispositivo de procesamiento de datos externo.

Además, el mensaje con información puede comprender, por ejemplo, una información sobre la no transmisión o una información sobre la recepción correcta, por ejemplo, en el dispositivo de protección. El mensaje con información se

puede enviar, por ejemplo, mediante el propio dispositivo de protección de red, o se puede, al menos, activar también mediante el dispositivo de protección de red

De esta manera, el emisor del mensaje recibe un “acuse de recibo”, en el cual el emisor mencionado puede detectar que el mensaje ha sido transmitido correctamente, al menos, hasta el dispositivo de protección de red. De esta manera se puede evitar, por ejemplo, que el emisor del mensaje envíe nuevamente el mensaje mencionado, dado que sin un acuse de recibo se parte de la base de que el mensaje no ha sido transmitido correctamente, por ejemplo, debido a un problema de transmisión. Además, esta clase de acuses de recibo se proporcionan según el estándar en una pluralidad de protocolos de automatización, de manera que el dispositivo de protección de red también opere conforme al protocolo de automatización, en el caso en que un mensaje no sea transmitido.

Además, el dispositivo de protección de red puede estar diseñado para un modo operacional con dirección transparente. Además, para la realización del modo operacional mencionado con dirección transparente, el dispositivo de protección de red opera además como sustituto para los participantes de la red de automatización, protegidos por el dispositivo mencionado, o se encuentra configurado o bien, diseñado para dicha función.

Por un modo operacional con dirección transparente se entiende un modo operacional en el cual el dispositivo de protección de red no modifica la dirección del receptor y/o del emisor del mensaje de protocolo, particularmente una dirección de la capa 3 (por ejemplo, dirección IP) o una dirección de la capa 4. En particular, se puede considerar un modo operacional en el que la dirección del emisor y del receptor del mensaje de protocolo, particularmente las direcciones anteriormente mencionadas, no se modifica mediante el dispositivo de protección de red. En una transmisión de un mensaje de protocolo desde el dispositivo de procesamiento de datos externo hacia el dispositivo de automatización, la dirección del emisor puede ser la dirección del dispositivo de procesamiento de datos externo, por ejemplo, una dirección de la capa 3 (por ejemplo, una dirección IP) del dispositivo de procesamiento de datos externo, o también una dirección en correspondencia con una capa OSI superior. La dirección del receptor puede ser, por ejemplo, la dirección de la capa 3 del dispositivo de automatización (por ejemplo, su dirección IP) o también su dirección de acuerdo con una capa OSI superior. En correspondencia, resultan válidas para mensajes desde el dispositivo de automatización hacia el dispositivo de procesamiento de datos externo.

Además, el dispositivo de protección de red puede estar conformado de manera que sus propias interfaces presenten direcciones correspondientes que, sin embargo, no se utilizan en la transmisión de un mensaje de protocolo. El dispositivo de protección de red se puede conformar de manera que sus interfaces no presenten esta clase de direcciones propias y, por ejemplo, se filtran todos los mensajes de protocolo que pasan entre una entrada de los dispositivos de protección de red y una salida correspondiente del dispositivo de protección de red, al menos, entre otros, de acuerdo con las reglas de protocolo.

Un dispositivo de protección de red de esta clase se puede acoplar de una manera simple en una red de automatización, dado que una gran cantidad de protocolos de automatización prefieren un direccionamiento directo, y la transmisión de mensajes de protocolo mediante la utilización de direcciones propias del dispositivo de protección de red, resulta más difícil o imposible de realizar.

Además, un dispositivo de protección de red de esta clase se puede integrar también de una manera simple en una red de automatización o bien, se puede acoplar a dicha red, dado que los protocolos de automatización no resultan aptos para una red Proxy, en comparación con una gran cantidad de protocolos IT. Esto significa que además de la propia dirección de destino del mensaje de protocolo, no se puede indicar la dirección de una puerta de enlace o de un dispositivo de protección de red intercalado. Mediante el acondicionamiento con dirección transparente del dispositivo de protección de red, el dispositivo mencionado puede cumplir su función de protección sin la necesidad de indicar esta clase de direcciones intermedias.

Un dispositivo de protección de red de esta clase con transparencia de dirección, se puede conformar, por ejemplo, como un denominado “puente”. Además, un dispositivo de protección de red de esta clase se puede realizar como un cortafuego para una red IP o como un cortafuego para una red IP con transparencia de dirección, mediante la utilización de Proxy ARP.

En el caso que el dispositivo de protección de red opere como un sustituto para los participantes protegidos por el dispositivo mencionado, el dispositivo desvía los mensajes de protocolo, por ejemplo, hacia los equipos protegidos. De esta manera, se puede lograr, por ejemplo, que el dispositivo de protección de red pueda analizar todos los mensajes de protocolo en los equipos protegidos por dicho dispositivo, sin la necesidad de realizar modificaciones en los equipos mencionados.

Además, el dispositivo de protección de red puede estar diseñado y configurado de manera que se pueda controlar, configurar y/o predeterminar opcionalmente un modo operacional con dirección transparente o sin dirección transparente.

De esta manera, un dispositivo de protección de red se puede adaptar de manera flexible a las propiedades de una red de automatización utilizada respectivamente y/o de un protocolo de automatización y, de esta manera, también se puede adaptar de una manera más simple a diferentes aplicaciones y redes. El control del modo operacional se puede realizar, por ejemplo, en el dispositivo de protección de red o, por ejemplo, mediante su configuración a través de un ordenador externo o de un programa de control correspondiente. Además, el dispositivo de protección de red puede estar conformado también para el control automático del modo operacional con dirección transparente o sin dirección transparente, por ejemplo, en relación con un protocolo de automatización controlado o detectado, o especificaciones o bien, determinaciones de los participantes en la red de automatización.

En un acondicionamiento ventajoso se puede prever que el contenido del mensaje de protocolo inicie una acción de automatización en el dispositivo de automatización que recibe el mensaje de protocolo o bien, se proporciona para la iniciación de una acción de automatización de esta clase. Las reglas de protocolo comprenden especificaciones que crean una dependencia de la decisión sobre una transmisión o una no transmisión del mensaje de protocolo, en relación con la acción de automatización a iniciar y/o la clase de acción de automatización a iniciar.

Un acondicionamiento o una formulación de esta clase de las reglas del protocolo, presenta la ventaja, por ejemplo, de que las reglas no dependan de la información de la dirección, de otra información de configuración y/u otra información de configuración de las redes de comunicaciones que participan. La decisión sobre un bloqueo o una transmisión del mensaje de protocolo, se dicta sólo a través de una operación o de una clase de operación del mensaje de protocolo. De esta manera, se simplifica la integración y el control y un dispositivo de protección de red de esta clase, dado que durante el control el usuario no necesita, por ejemplo, la información de la dirección o bien, de la configuración, y también en el caso de realizar modificaciones, por ejemplo, en la red de automatización, un dispositivo de protección de red no se debe adaptar en correspondencia con las modificaciones mencionadas, por ejemplo, las direcciones de equipos nuevos instalados.

Un mensaje de protocolo inicia, por ejemplo, una acción de automatización, cuando el mensaje mencionado inicia un proceso y/o una acción en o con un participante de la red de automatización. En particular, se inicia, por ejemplo, una acción de automatización mediante el mensaje de protocolo, cuando se inicia un proceso con o en un dispositivo de automatización de la red de automatización, que coopera con un control y/o un ajuste de un equipo controlado (por ejemplo, un ordenador, una máquina, una instalación, una instalación de producción o una línea de producción).

Una acción de automatización se puede realizar exclusivamente en el interior de un participante de la red de automatización, por ejemplo, también se puede realizar completamente mediante soporte lógico. Además, una acción de automatización en un participante, puede presentar también repercusiones directas y/o indirectas sobre el equipo controlado por la red de automatización o bien, sobre el equipo controlado dentro de la red de automatización.

Las acciones de automatización pueden comprender, por ejemplo:

- una conmutación del modo de funcionamiento, particularmente un inicio o una detención de un proceso, y/o

- la carga de un programa de automatización, y/o

- el establecimiento de parámetros, información y/o valores en un módulo de control o una unidad de automatización, y/o

- la lectura de parámetros, valores o información de un módulo de control o una unidad de automatización, y/o

- el control o el ajuste de un programa de automatización, o la intervención en un programa de automatización, y/o

- la activación de un sensor o de un actuador.

Además, la información a extraer o a establecer puede ser, por ejemplo, información de diagnóstico, por ejemplo, de una memoria intermedia de diagnóstico. El control o el ajuste de un programa de automatización, o la intervención en el programa mencionado, pueden consistir, por ejemplo, en el establecimiento de puntos de detención o de un desarrollo en el funcionamiento paso a paso, por ejemplo, en un funcionamiento de prueba.

Las acciones de automatización pueden ser también, por ejemplo:

- una conmutación del modo de funcionamiento, como por ejemplo, inicio, detención, etc.;

- evaluación de direccionamientos específicos de la automatización (por ejemplo, dirección S7);

- carga de programas de usuario, reparametrización de módulos de usuario y/o lectura de parámetros;

- configuración del soporte físico;

- prueba y puesta en marcha (por ejemplo, el establecimiento de puntos de detención, el control o el accionamiento de un funcionamiento paso a paso);

- un diagnóstico (por ejemplo, la lectura de una memoria intermedia de diagnóstico);

- una acción de control en el funcionamiento de producción o de prueba.

Además, el dispositivo de protección de red puede comprender reglas de protocolo que crean una dependencia de la decisión sobre la transmisión o la no transmisión del mensaje de protocolo, entre otros o también exclusivamente en relación con especificaciones de tiempo y/o de lugar. Esta clase de especificaciones pueden ser, por ejemplo, horas del día o también horas de funcionamiento en conjunto o similares. De esta manera, en un funcionamiento de automatización se pueden realizar, por ejemplo, modificaciones o controles individuales, sólo durante determinadas horas del día o también horas de la noche, por ejemplo, durante un turno de día. De esta manera se puede lograr, por ejemplo, que no se realicen intervenciones en un equipo controlado, por ejemplo, en una instalación de producción que por las noches sólo presenta un personal reducido.

Las especificaciones de lugar pueden ser, por ejemplo, determinadas construcciones, salas o también ubicaciones geográficas. De esta manera se puede prever, por ejemplo, la realización de determinadas modificaciones en una red de automatización sólo desde una central de control especial, y no directamente de, por ejemplo, un taller de fabricación. También de esta manera, mediante un dispositivo de protección de red de esta clase se puede incrementar la susceptibilidad a los errores.

Además, las reglas de protocolo pueden comprender especificaciones que crean una dependencia de la decisión sobre la transmisión o la no transmisión del mensaje de protocolo, o exclusivamente en relación con un estado operacional de un elemento o de una pluralidad de elementos de la red de automatización, o de un dispositivo o de una pluralidad de dispositivos conectados con la red de automatización. Esta clase de dispositivos pueden ser, por ejemplo, un equipo controlado o una máquina controlada o bien, actuadores controlados en general y/o sensores de lectura.

De esta manera, el dispositivo de protección de red puede estar configurado, por ejemplo, de manera que se admita la escritura de una determinada palabra de datos sólo en un estado de funcionamiento o bien, un estado de la instalación de “puesta en marcha” de una instalación controlada, mientras que en un estado de “funcionamiento de producción” de la instalación sólo se admite la lectura de la palabra de datos correspondiente.

Las opciones de acondicionamiento anteriormente mencionadas de las reglas de protocolo, considerando una acción de automatización iniciada por un mensaje de protocolo, de una manera diferente hasta el momento, permiten la definición de reglas que no se encuentran sujetas a direcciones IP y/o puertos y/o clases de protocolo IP, como resulta convencional en el caso de los cortafuegos de hasta el momento, sino que se encuentran orientadas a determinados objetivos de acción en relación con la técnica de automatización. De esta manera, se logra una independencia parcial o también completa del dispositivo de protección de red, de configuraciones físicas especiales de una red externa o de una red de automatización. La independencia mencionada facilita el control de un dispositivo de protección de red de esta clase y/o reduce la susceptibilidad a errores o bien, mejora la acción de protección mediante un dispositivo de protección de red de esta clase. Además, el dispositivo de protección de red también se puede adaptar de una manera más simple a las modificaciones correspondientes en la red protegida o conectada.

En otro acondicionamiento ventajoso, las reglas de protocolo almacenadas en el dispositivo de protección de red comprenden especificaciones que crean una dependencia de la decisión sobre la transmisión o la no transmisión del mensaje de protocolo, además en relación con un emisor y/o un cliente y/o un receptor del mensaje de protocolo. En este caso, el emisor, el cliente y/o el receptor se pueden caracterizar por su dirección, por ejemplo, su dirección IP o por una dirección lógica, o por un nombre de equipo o una denominación de equipo o bien, por otros medios. Una dirección puede ser, por ejemplo, una dirección de la capa 3, una dirección de la capa 4, o también una dirección de acuerdo con una capa por encima de la capa 4, particularmente una dirección de la capa 7.

De esta manera, se pueden obtener de una mejor manera y más simple, reglas para la protección de una red de automatización, dado que se pueden limitar determinados mensajes de protocolo, por ejemplo, también más allá de su contenido, mediante la información del receptor y/o del emisor, o particularmente también mediante determinadas combinaciones del emisor y del receptor.

Además, el emisor y el receptor pueden estar sujetos, por ejemplo, también a las clases, a las categorías y/o a los clústeres de equipo. De esta manera, por ejemplo, las reglas de protocolo pueden comprender especificaciones que a una categoría determinada de emisores y/o clientes, le permiten enviar determinados mensajes de protocolo a un dispositivo de automatización determinado o a una categoría o clase determinada de dispositivos de automatización. La clase mencionada de emisores o clientes, pueden ser, por ejemplo, un administrador de la puesta en funcionamiento, un "sistema de control y monitorización", un controlador, un técnico de automatización, un técnico de servicio o un operador de la instalación. De esta manera, pueden existir diferentes opciones para diferentes categorías de emisores y/o clientes de los mensajes de protocolo, para acceder a la red de automatización y para intervenir en la red mencionada.

Además, el dispositivo de protección de red se puede ocupar, por ejemplo, de la reducción de errores correspondientes al operador, dado que, por ejemplo, sólo las personas instruidas en correspondencia, son capaces de enviar los mensajes de protocolo correspondientes, posiblemente críticos (y, por ejemplo, los comandos de control sujetos a dichos mensajes) a un dispositivo de automatización en la red de automatización. Una clasificación de las categorías del emisor o del cliente, se puede configurar y controlar, por ejemplo, mediante un acceso correspondiente de las personas correspondientes, al dispositivo de procesamiento de datos externo, por ejemplo, a través de una denominada "cuenta de usuario" con una contraseña.

Las reglas de protocolo almacenadas en el dispositivo de protección de red pueden comprender además especificaciones que crean una dependencia de la decisión sobre una transmisión o una no transmisión del mensaje de protocolo, además en relación con la existencia de un código de seguridad asociado a un emisor y/o a un cliente del mensaje de protocolo. Además, se puede prever que el mensaje de protocolo no se transmita cuando no se encuentra presente el código de seguridad asociado al emisor y/o al cliente del mensaje de protocolo. Esta clase de códigos de seguridad pueden ser, por ejemplo, la introducción de una contraseña, por ejemplo, para la autentificación de un emisor o de un usuario en el dispositivo de procesamiento de datos electrónico, o también una contraseña correspondiente que se debe ingresar, por ejemplo, cuando se envía el mensaje de protocolo.

Además, se puede proporcionar, por ejemplo, un código de seguridad correspondiente también en una tarjeta de memoria, una tarjeta chip o en otra memoria electrónica que, por ejemplo, un usuario o un emisor de un mensaje de protocolo correspondiente debe acoplar en el dispositivo de procesamiento de datos, o en un equipo conectado con el dispositivo de procesamiento de datos que envía el mensaje de protocolo.

De esta manera, se puede controlar de una manera más simple y mejor, la transmisión de los mensajes de protocolo o bien, se puede reglamentar mediante el dispositivo de protección de red, dado que determinadas acciones, por ejemplo, en la red de automatización, se pueden limitar a un círculo de personas muy bien definido y controlado.

Además, las reglas de protocolo almacenadas en el dispositivo de protección de red pueden comprender especificaciones que crean una dependencia de la decisión sobre la transmisión o la no transmisión del mensaje de protocolo, además en relación con una autentificación de un emisor y/o de un cliente del mensaje de protocolo. Una autentificación de esta clase se puede realizar, por ejemplo, a través de uno de los códigos de seguridad mencionados anteriormente, como por ejemplo, una contraseña. Las opciones anteriormente mencionadas en relación con la limitación de la transmisión de mensajes de protocolo, al menos, entre otros, mediante la consideración de un código de seguridad de esta clase o de una autentificación de esta clase, permiten, por ejemplo, una protección muy eficiente contra el acceso a la red de automatización desde el exterior, mediante un dispositivo de protección de red asociado a la red de automatización. Las opciones mencionadas simplifican tanto la configuración de la propia red de automatización, así como la configuración de una red de comunicaciones externa que autoriza un acceso a la red de automatización, dado que esta clase de comprobaciones de seguridad se ejecutan en el dispositivo de protección de red y, de esta manera, libera, por ejemplo, a otras unidades en la red de automatización (por ejemplo, módulos de control) de una tarea de esta clase.

El objeto anteriormente mencionado se resuelve además mediante un método para el control de las comunicaciones de un dispositivo de procesamiento de datos externo, que se encuentra fuera de una red de automatización, con un dispositivo de automatización en la red de automatización, a través de un dispositivo de protección de red de acuerdo con la presente descripción, que comprende las siguientes etapas:

a) recepción de un mensaje de protocolo del protocolo de automatización del dispositivo de procesamiento de datos externo, por parte del dispositivo de protección de red, y

b) transmisión del mensaje de protocolo cuando el contenido del mensaje de protocolo corresponde a las especificaciones de las reglas de protocolo para la transmisión, y/o la no transmisión del mensaje de protocolo cuando el contenido del mensaje de protocolo no corresponde con las especificaciones de las reglas de protocolo para la transmisión.

Además, el dispositivo de protección de red, el mensaje de protocolo, el contenido del mensaje de protocolo, así como las reglas de protocolo y las especificaciones creadas en las reglas de protocolo mencionadas, se pueden conformar, por ejemplo, de acuerdo con la presente descripción.

Además de las etapas del método mencionadas anteriormente, se puede prever también que en el caso de una no transmisión del mensaje de protocolo, se envíe un mensaje con información en relación con la no transmisión, en correspondencia con el protocolo de automatización, al dispositivo de procesamiento de datos externo. En este caso, por otra parte, el mensaje con información se puede conformar de acuerdo con la presente descripción.

Por otra parte, mediante un método de esta clase se puede lograr una adaptación más simple o bien, una modificación o también una configuración de una red de automatización, en relación con una protección contra el acceso mediante dispositivos de procesamiento de datos externos, dado que las reglas para la transmisión o la no transmisión dependen, al menos, entre otros, del contenido de un mensaje de protocolo enviado, por ejemplo, por el dispositivo de procesamiento de datos externo al dispositivo de automatización. Además, el contenido del mensaje de protocolo se obtiene mediante el contenido de dicho mensaje sobre una capa OSI 4, particularmente el contenido dentro de la capa de aplicación (capa OSI 7). De esta manera, las reglas de transmisión se pueden formular en el dispositivo de protección de red, por ejemplo, al menos, parcialmente o también de una manera completamente independiente de la configuración física concreta de la red de automatización (por ejemplo, las direcciones IP o las direcciones MAC utilizadas en la red mencionada).

Por consiguiente, la presente invención hace referencia a un dispositivo de protección de red, que puede comprender y decodificar los protocolos específicos de la automatización (en la presente descripción también se denomina protocolo de automatización). De esta manera, el dispositivo de protección de red mencionado es capaz de decodificar e identificar las solicitudes, ordenes o consultas específicas de la automatización, y de permitir o prohibir su transmisión hacia la red de automatización asegurada mediante el dispositivo de protección de red o bien, hacia el dispositivo de automatización que se encuentra en su interior.

Mediante un dispositivo de protección de red de esta clase, de una manera diferente hasta el momento, se pueden definir reglas que no se encuentran sujetas exclusivamente a direcciones IP y/o a puertos y/o a clases de protocolo IP, como resulta convencional en el caso de los cortafuegos de hasta el momento. De esta manera, por primera vez se puede filtrar, al menos, en base a determinados objetivos de acción en relación con la técnica de automatización, ya sea de manera exclusiva o, al menos, entre otras opciones.

Cuando el protocolo de automatización soporta un método apropiado para la autentificación de los usuarios correspondientes (por ejemplo, mediante una contraseña o un hash de contraseñas), el dispositivo de protección de red debe comprobar también la autentificación mencionada, sin que el dispositivo de automatización receptor deba conocer y/o soportar la dicha autentificación.

El dispositivo de protección de red comprueba los mensajes específicos de la automatización, dentro del mensaje de protocolo de acuerdo con sus reglas. Las reglas se obtienen a partir de los objetivos de acción admitidos y prohibidos. Cuando las reglas determinan que el mensaje puede pasar, dicho mensaje se transmite, de lo contrario se rechaza. En comparación con los cortafuegos convencionales o bien, los dispositivos de protección de red convencionales, generalmente no se puede desechar simplemente un mensaje, dado que los protocolos de automatización convencionales o los protocolos específicos de la automatización, convencionalmente operan sobre niveles superiores del protocolo (superior a la capa OSI 4, convencionalmente sobre la capa OSI 7) y por lo tanto esperan acuses de recibo para las tareas correspondientes. Ante la ausencia de esta clase de mensajes de acuse de recibo o de información de acuerdo con el protocolo de automatización, se pueden presentar los denominados “tiempos de espera” y eventualmente se pueden presentar incluso interferencias considerables en las comunicaciones. Por este motivo, el dispositivo de protección de red debe ser capaz eventualmente también de generar mensajes con información o bien, acuses de recibo conforme al protocolo de automatización. En tanto que se pueda realizar el proceso mencionado en el protocolo de automatización, se puede tratar o bien, se debe tratar de acuses de recibo negativos que se presentan en forma de un mensaje con información correspondiente.

Un problema adicional de los protocolos de automatización actuales consiste en que en comparación con una gran cantidad de protocolos IT, por ejemplo, en el ámbito de oficinas, no resultan aptos para una red Proxy. Es decir, que además de la dirección de destino, no se puede indicar la dirección de una “puerta de enlace” correspondiente o de un dispositivo de protección adicional intercalado (mientras que, por ejemplo, HTTP permite un servidor denominado Proxy HTTP).

Por este motivo, el dispositivo de protección de red puede estar conformado de manera ventajosa, con dirección transparente. La conformación mencionada se puede realizar, por ejemplo, mediante el hecho de que el dispositivo de soporte opera como un sustituto para todos los dispositivos de automatización protegidos por dicho dispositivo, en la red de automatización (por ejemplo, de manear definida por una lista de equipos). Además, el dispositivo mencionado desvía hacia él mismo, el tráfico que se dirige hacia los equipos protegidos. De esta manera, el

dispositivo de soporte puede analizar todos los mensajes, sin que se deban realizar modificaciones en los dispositivos de automatización correspondientes.

Los objetivos de acción admitidos o no admitidos, mencionados anteriormente, se pueden definir de una forma familiar para un técnico de automatización (que configura, por ejemplo, una red de comunicaciones o de automatización de esta clase). Los objetivos hacen referencia a los dispositivos de automatización correspondientes (por ejemplo, equipos con una función determinada o con determinados nombres, módulos o programas de automatización), es decir, que hacen referencia a aquellos objetos que resultan conocidos para el técnico de automatización a partir de su área de trabajo.

Ejemplos para esta clase de reglas son:

- permitir a un administrador de la puesta en funcionamiento, la modificación de la palabra de datos 10 en el módulo de datos 100;

- permitir a un sistema de control y de monitorización, la lectura de todas las palabra de datos del módulo de datos 200;

- permitir a un controlador la modificación de todos los módulos de datos en la fase de puesta en funcionamiento de la instalación;

- permitir al controlador 1 la lectura de todos los módulos en la fase operativa;

- permitir al controlador 2 la detención y el inicio del grupo constructivo 1;

- permitir al controlador 3 la modificación de la configuración del grupo constructivo 3.

Si un dispositivo de protección de red se conforma o se configura o bien, se controla con dirección transparente, un dispositivo de protección de red de esta clase se puede integrar también posteriormente en una red existente. En este caso, no resulta necesario realizar una nueva planificación o bien, se pueden reducir de manera considerable los trabajos relacionados. Dado que el dispositivo de protección de red opera de manera transparente, también se pueden utilizar sin modificar protocolos de automatización no aptos para red Proxy. Además, un dispositivo de protección de red conformado con dirección transparente de esta manera, no se puede descubrir mediante medios auxiliares, como por ejemplo, un rastreo de ruta (“Traceroute”), hecho que dificulta esencialmente una intervención en el dispositivo de protección de red desde el exterior.

A continuación, la presente invención se explica en detalle, por ejemplo, en relación con las figuras adjuntas.

Muestran:

Figura 1 Ejemplo para una red de automatización, a la cual se conecta un ordenador externo a través de un cortafuego;

Figura 2a Diagrama de la transmisión de mensajes para un cortafuego, sin transparencia de dirección;

Figura 2b Diagrama de la transmisión de mensajes para un cortafuego, con transparencia de dirección.

La figura 1 muestra una red de automatización 100 con un controlador lógico programable ("Programmable Logic Controller" (PLC)) 190, el cual se encuentra conectado con un cortafuegos 110 a través de un cable Ethernet 126, en donde el cortafuegos 110 es un ejemplo de un dispositivo de protección de red de acuerdo con la presente descripción. El cortafuego 110 se utiliza para la protección de la red de automatización 100 dispuesta detrás, y filtra en correspondencia con los mensajes que provienen desde el exterior de la red de automatización 100. La figura 1 muestra un ordenador (PC) 200 fuera de la red de automatización 100, que se encuentra conectado con el cortafuego a través de un cable Ethernet 116.

En la figura 1 se representa el cortafuego 110 dentro del símbolo para el cortafuego 110 de la estructura de capa OSI. Se muestra una capa IP 140, que en el modelo OSI corresponde a una capa OSI 3. Además, sobre dicha capa, se representa una capa TCP/UDP 150 que corresponde a una capa OSI 4. Como capa superior en el modelo de capas representado del cortafuego 110, se representa una capa de aplicación 160 que corresponde a una capa OSI 7. En el interior de la capa IP 140 y de la capa TCP 150, se representa un dispositivo de protección 152 de la capa 3 + 4, que simboliza una función de filtro de la capa 3+4 del cortafuego 110.

En el interior de la capa de aplicación 160 se representa un protocolo Proxy 162 del lado del ordenador (por ejemplo, para un denominado protocolo S7 para dispositivos de automatización Siemens) y un segundo protocolo Proxy 164 del lado del PLC (por ejemplo, también para el protocolo S7). Entre el protocolo Proxy del ordenador 162 y el protocolo Proxy del PLC 164, se representa un dispositivo de protección de aplicación 166, a través del cual se realiza un filtrado de los mensajes de protocolo a comprobar mediante el cortafuego 110, en el nivel de aplicación (por ejemplo, nivel de protocolo S7).

La línea Ethernet 116 desde el ordenador 200 hacia el cortafuego 110, se encuentra conectada con una interfaz 202, que presenta una dirección IP del ordenador 204 "192.168.1.55". El cable Ethernet 116 se encuentra conectado en el cortafuego 110 en una conexión exterior 112, con una dirección IP 114 "192.168.1.1". El cable Ethernet 126 se encuentra conectado con una interfaz interior 122 del cortafuego 110, con una dirección IP 124 "10.0.0.1". Además, el cable Ethernet 126 mencionado se encuentra conectado con el PLC 190, mediante una interfaz 192, con una dirección IP 194 "10.0.0.99". Las direcciones mencionadas han sido establecidas y configuradas en la instalación de dicha red, como se representa en la figura 1.

La flecha 168 desde el ordenador 200 hasta la capa de aplicación 160 del cortafuego 110, simboliza el recorrido de un mensaje de protocolo de acuerdo con el protocolo S7, como se puede utilizar, por ejemplo, para las comunicaciones con controladores lógicos programables o con dispositivos de automatización similares de la empresa Siemens, desde el ordenador 200 hasta el interior de la capa de aplicación 160 del cortafuego 110. De acuerdo con el procedimiento en correspondencia con el modelo de capas OSI, el propio mensaje de protocolo se encapsula de acuerdo con el protocolo S7 en el ordenador 200, en correspondencia con las especificaciones de la capa de transporte (capa 4) y después de la capa de red (capa 3), y a continuación se transmite al cortafuego 110 a través del cable Ethernet 116.

En dicho punto el mensaje se desencapsula nuevamente mediante su capa IP 140 y, a continuación, su capa de transporte 150, y el propio mensaje de protocolo S7 se transmite a la capa de aplicación 160, y en dicho punto se transmite al protocolo Proxy 162 del lado del ordenador. El protocolo Proxy puede analizar el contenido del mensaje de protocolo S7, y transmite los resultados del análisis al dispositivo de protección de la capa 7 166, es decir, cuales son las reglas que contiene, cuales son los objetivos de acción permitidos en relación con la técnica de automatización, y cuales no están permitidos. En vista de ello, se dicta una decisión en el dispositivo de protección de la capa 7 166, que consiste en si en el cortafuego 110 el mensaje transmitido para el PLC 190 se puede transmitir de acuerdo con las especificaciones en el dispositivo de protección 166, o si se debe bloquear.

Esta clase de reglas pueden comprender, por ejemplo:

- se permite o se prohíbe una conmutación del modo de funcionamiento, como por ejemplo, inicio, detención, ejecución, etc.;

- determinadas direcciones de protocolo o grupos de direcciones de protocolo (en el presente ejemplo, por ejemplo, las direcciones S7) están autorizadas a transmitir mensajes de protocolo hacia la red de automatización, otras no;

- se admite o no la carga de programas de usuario;

- se admite o no la parametrización o la reparametrización de módulos de usuario;

- se admite o no la lectura de parámetros o la escritura de parámetros;

- se admite o no la configuración de determinado soporte físico o de todos los soportes físicos;

- se admiten o no acciones de prueba y de puesta en funcionamiento (por ejemplo, el establecimiento de puntos de detención, el control de un funcionamiento paso a paso, o la ejecución de un funcionamiento paso a paso);

- se admiten o no acciones de diagnóstico (por ejemplo, la lectura de una memoria intermedia de diagnóstico);

- se admiten o no acciones de control en el funcionamiento de producción.

Las reglas de filtrado en el dispositivo de protección 166 de la capa 7, pueden comprender, por ejemplo, cualquier combinación de los elementos de las reglas o bien, de los módulos mencionados anteriormente. Las combinaciones mencionadas pueden ser, por ejemplo:

- permitir a un administrador de la puesta en funcionamiento, la modificación de determinadas palabras de datos en un módulo de datos determinado del PLC 190;

- permitir a un sistema de control y de monitorización, la lectura de todas las palabra de datos de otro módulo de datos en el PLC 190;

- permitir a un controlador durante el estado: “puesta en funcionamiento” del PLC 190 y de una instalación conectada con dicho PLC (no representada en la figura 1) la modificación de todos los módulos de datos;

- permitir a un primer controlador en un estado de “funcionamiento” del PLC 190 y de la instalación conectada con dicho PLC, la lectura de todos los módulos de datos;

- permitir a un segundo controlador la detención y el inicio de un primer grupo constructivo del PLC 190 (o la realización de conmutaciones a otros modos de funcionamiento);

- permitir a un tercer controlador la modificación de la configuración de otro grupo constructivo del PLC 190.

Si el mensaje de protocolo S7 transmitido por el ordenador 200, es admisible de acuerdo con el dispositivo de protección 166 de la capa 7, el mensaje mencionado se transmite al protocolo Proxy 164 del lado del PLC, y desde dicho protocolo se transmite, después del empaquetado correspondiente, a través de la capa de transporte 150 y la capa de red 140, mediante el cable Ethernet 126 al PLC 190.

Si el mensaje no es admisible de acuerdo con las reglas en el dispositivo de protección 166 de la capa 7, el cortafuego 110 reenvía un mensaje de acuse de recibo de acuerdo con el protocolo S7 al ordenador 200, para indicar que el mensaje ha sido recibido correctamente por el cortafuego 110 y/o que ha sido bloqueado. De esta manera, el ordenador 200 recibe, por ejemplo, un mensaje sobre la correcta transmisión del mensaje de protocolo S7 a la red de automatización 100, y/o la información que indica que el mensaje mencionado no se ha convertido en dicho punto.

El flujo de mensajes desde la capa de aplicación 160 del cortafuego 110 hasta el PLC 190, se simboliza en la figura 1 mediante una segunda flecha 169.

Además de la función de protección en la capa de aplicación 160, el cortafuego 110 presenta el dispositivo de protección adicional 152 de la capa 3+4, mediante el cual se puede realizar, por ejemplo, un filtrado adicional o alternativo de mensajes desde el ordenador 200 hacia el PLC 190 en el nivel IP (por ejemplo, la admisión o la no admisión de determinadas direcciones IP, como emisor y/o receptor) o en el nivel TCP. Además, el cortafuego 110 se puede accionar, por ejemplo, tanto como un cortafuegos elemental de la capa 7, en el cual sólo se encuentra activo el dispositivo de protección 166 en la capa 7 160, así como un cortafuegos elemental de la capa 3+4 en el que sólo se encuentra activo el dispositivo de protección 152 de la capa 3+4, así como un cortafuego combinado en el que se utilizan ambos dispositivos de protección. El cortafuego 110 se puede parametrizar de manera que los tres modos de funcionamiento mencionados se pueden controlar y predeterminar mediante una parametrización de esta clase.

La figura 2a muestra un diagrama de la transmisión de mensajes, en el sistema representado en la figura 1, en el caso de un modo operacional sin dirección transparente del cortafuego 110. Además, desde el ordenador 200 hacia el cortafuego 110, se envía un mensaje de protocolo S7 con una dirección de destino "192.168.1.1" de la interfaz del ordenador 112 del cortafuego 110, y una dirección de origen "192.168.1.55" de la interfaz 202 del ordenador 200, lo cual se simboliza en la figura 2a mediante la flecha 168.

En el caso representado en la figura 2a, el mensaje de protocolo S7 es admitido por el cortafuego, y se transmite al PLC 190, lo cual se representa mediante la flecha 169 que corresponde a la flecha 169 de la figura 1. El mensaje mencionado se transmite de manera lógica desde la interfaz del PLC 122 del cortafuego 110, hacia la interfaz de entrada 192 del PLC 190 y, por lo tanto, presenta una dirección de origen "10.0.0.1" de la interfaz del cortafuego 122, y una dirección del receptor "10.0.0.99" de la interfaz 192 del PLC 190. En el caso de dicho modo operacional no transparente, en el interior del cortafuego 110 se cambia la dirección en correspondencia con las interfaces de origen y destino, relevantes de acuerdo con la transmisión.

La figura 2b muestra la misma transmisión de mensajes en el caso de un modo operacional del cortafuego 110 con dirección transparente. En este caso, el mensaje de protocolo S7 se envía de manera lógica directamente desde el ordenador 200 y su interfaz 202, a la interfaz de entrada 192 del PLC 190 y, por lo tanto, como dirección de origen tanto para el mensaje desde el ordenador 200 hacia el cortafuego 110, así como desde el cortafuego 110 hacia el PLC 190, se utiliza respectivamente la dirección IP "192.168.1.55" de la interfaz del ordenador 202. En correspondencia, como dirección de destino se utiliza respectivamente la dirección IP "10.0.0.99" de la interfaz de entrada 192 del PLC 190. No se realiza modificación alguna de las direcciones mencionadas en el interior del cortafuego. En este caso transparente, en la constelación representada, el cortafuego 110 se comporta, por ejemplo, como un denominado "puente". No se modifican ni el propio mensaje de protocolo S7 ni los parámetros relevantes de la capa de red 140.

En el caso de un funcionamiento con dirección transparente del dispositivo de protección de red o bien, del cortafuego 110, también se puede utilizar el cortafuego 110 o bien, en general un dispositivo de protección de red de acuerdo con la presente descripción, también en las denominadas redes no segmentadas. Mediante la expresión “no segmentada”, en el presente contexto se refiere a que, por ejemplo, tanto el dispositivo de procesamiento de datos externo, por ejemplo, el ordenador 200 de las figuras 1 y 2, el cortafuego 110 o bien, en general el dispositivo de protección de red de acuerdo con la presente descripción, así como el dispositivo de automatización de acuerdo con la presente descripción, y en el presente ejemplo el PLC 190, se encuentran en la misma subred IP. En este caso, el dispositivo de protección no resulta visible ni para el dispositivo de procesamiento de datos externo / el ordenador 200, así como para el dispositivo de automatización / el PLC 190 en el nivel del protocolo IP (capa OSI 3). Para cambiar el comportamiento mencionado, el dispositivo de protección de red / el cortafuego 110 puede utilizar, por ejemplo, los mecanismos de los denominados "Proxy ARP".

La presente invención describe un dispositivo de protección de red para una red de automatización, que permite analizar el contenido de los mensajes de protocolo de un protocolo de automatización utilizado, y filtrar en virtud del contenido o bien, de los objetivos de acción obtenidos a partir del contenido mencionado. De esta manera, se simplifica el control del dispositivo de protección de red para un usuario y, de esta manera, también se torna más seguro y más claro. Además, el modo operacional del dispositivo de protección de red es independiente o bien, más independiente de la configuración física de las redes que participan, por ejemplo, de la red de automatización protegida y/o de los dispositivos y redes exteriores conectados con la red mencionada. De esta manera, también se pueden realizar modificaciones en las redes mencionadas, por ejemplo, el cambio de equipos, la modificación de direcciones o el montaje adicional de equipos, sin la necesidad de adaptar el dispositivo de protección de red individualmente a cada modificación mencionada. La opción mencionada también incrementa la flexibilidad y, de esta manera, también la seguridad de un dispositivo de protección de red de esta clase.

REIVINDICACIONES

1. Dispositivo de protección de red (110) para el control de las comunicaciones de un dispositivo de procesamiento de datos externo (200) fuera de una red de automatización (100) con un dispositivo de automatización (190) en la red de automatización (100), en donde para las comunicaciones con el dispositivo de automatización (190) se proporciona un protocolo de automatización, en donde en el dispositivo de protección de red (110) se almacenan o se pueden almacenar reglas de protocolo, en donde las reglas de protocolo comprenden especificaciones que crean una dependencia de la decisión sobre una transmisión o una no transmisión de un mensaje de protocolo del protocolo de automatización, en relación con un contenido del mensaje de protocolo, y en donde el dispositivo de protección de red (110) se conforma para la decisión sobre una transmisión o una no transmisión de un mensaje de protocolo entrante del protocolo de automatización que corresponde a las especificaciones de las reglas de protocolo, **caracterizado porque** las reglas de protocolo almacenadas en el dispositivo de protección de red (110) comprenden especificaciones que crean una dependencia de la decisión sobre la transmisión o la no transmisión del mensaje de protocolo, además en relación con un estado operacional de un elemento o de una pluralidad de elementos (110, 190) de la red de automatización (100), o de un dispositivo o de una pluralidad de dispositivos conectados con la red de automatización.

2. Dispositivo de protección de red de acuerdo con la reivindicación 1, **caracterizado porque** el dispositivo de protección de red (110) se conforma de manera que en el caso de una no transmisión del mensaje de protocolo, se envía un mensaje con información en relación con la no transmisión, en correspondencia con el protocolo de automatización, al dispositivo de procesamiento de datos externo (200).

3. Dispositivo de protección de red de acuerdo con la reivindicación 1 ó 2, **caracterizado porque** el dispositivo de protección de red (110) está diseñado para un modo operacional con dirección transparente, particularmente porque para la realización del modo operacional con dirección transparente, el dispositivo de protección de red (110) opera como sustituto para los participantes (190) de la red de automatización (100), protegidos por el dispositivo mencionado.

4. Dispositivo de protección de red de acuerdo con una de las reivindicaciones 1 a 3, **caracterizado porque** el dispositivo de protección de red (110) se diseña y se configura de manera que se pueda controlar, configurar y/o predeterminar opcionalmente un modo operacional con dirección transparente o con dirección no transparente.

5. Dispositivo de protección de red de acuerdo con una de las reivindicaciones 1 a 4, **caracterizado porque** el contenido del mensaje de protocolo está configurado para la iniciación de una acción de automatización en el dispositivo de automatización (190) que recibe el mensaje de protocolo, y porque las reglas del protocolo comprenden especificaciones que crean una dependencia de la decisión sobre una transmisión o una no transmisión del mensaje de protocolo, en relación con la acción de automatización a iniciar y/o la clase de acción de automatización a iniciar.

6. Dispositivo de protección de red de acuerdo con la reivindicación 5, **caracterizado porque** la acción de automatización comprende:

- una conmutación del modo de funcionamiento, particularmente un inicio o una detención de un proceso, y/o

- la carga de un programa de automatización, y/o

- el establecimiento de parámetros, información o valores en un módulo de control o una unidad de automatización, y/o

- la lectura de parámetros, valores o información de un módulo de control o una unidad de automatización, y/o

- el control o el ajuste de un programa de automatización, o la intervención en un programa de automatización, y/o

- la activación de un sensor o de un actuador.

7. Dispositivo de protección de red de acuerdo con una de las reivindicaciones 1 a 6, **caracterizado porque** las reglas de protocolo almacenadas en el dispositivo de protección de red (110) comprenden especificaciones que crean una dependencia de la decisión sobre la transmisión o la no transmisión del mensaje de protocolo, además en relación con especificaciones de tiempo y/o de lugar.

8. Dispositivo de protección de red de acuerdo con una de las reivindicaciones 1 a 7, **caracterizado porque** las reglas de protocolo almacenadas en el dispositivo de protección de red (110) comprenden especificaciones que crean una dependencia de la decisión sobre la transmisión o la no transmisión del mensaje de protocolo, además en relación con un emisor y/o un cliente y/o un receptor del mensaje de protocolo.

9. Dispositivo de protección de red de acuerdo con una de las reivindicaciones 1 a 8, **caracterizado porque** las reglas de protocolo almacenadas en el dispositivo de protección de red (110) comprenden especificaciones que crean una dependencia de la decisión sobre la transmisión o la no transmisión del mensaje de protocolo, además en relación con la presencia de un código de seguridad asociado a un emisor y/o a un cliente del mensaje de protocolo, particularmente porque el mensaje de protocolo no se transmite cuando no se encuentra presente el código de seguridad asociado al emisor o al cliente del mensaje de protocolo.

10. Dispositivo de protección de red de acuerdo con una de las reivindicaciones 1 a 9, **caracterizado porque** las reglas de protocolo almacenadas en el dispositivo de protección de red (110) comprenden especificaciones que crean una dependencia de la decisión sobre la transmisión o la no transmisión de un mensaje de protocolo, además en relación con una autentificación de un emisor y/o de un cliente del mensaje de protocolo.

11. Dispositivo de protección de red de acuerdo con una de las reivindicaciones 1 a 10, **caracterizado porque** las reglas de protocolo almacenadas en el dispositivo de protección de red (110) comprenden especificaciones que crean una dependencia de la decisión sobre una transmisión o no transmisión de un mensaje de protocolo, desde el dispositivo de procesamiento de datos externo (200) al dispositivo de automatización (190) en la red de automatización, además en relación con una dirección IP del mensaje de protocolo, un protocolo IP del mensaje de protocolo y/o un “puerto”.

FIG 1

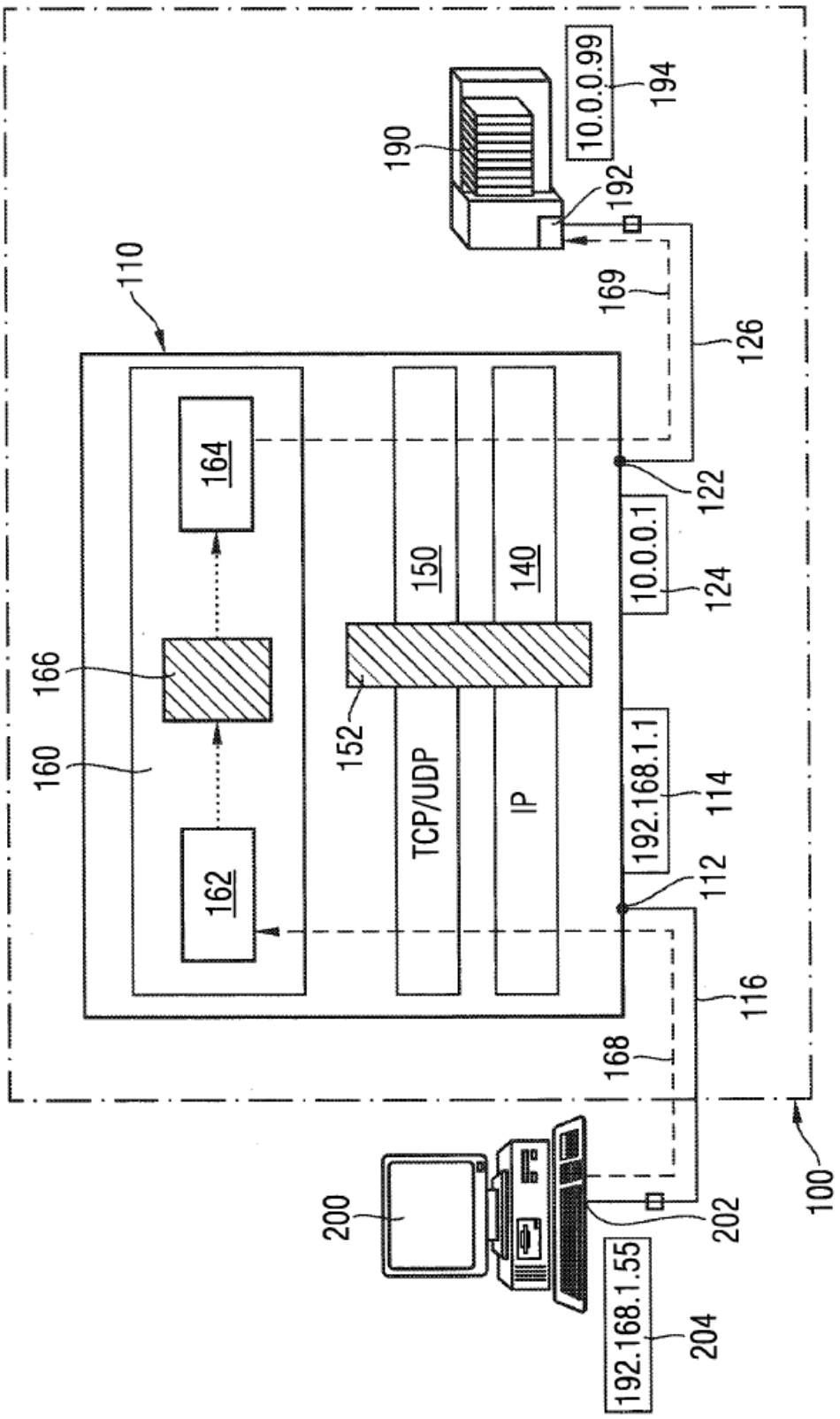

100
110
190
10.0.0.99
194
192
169
126
122
10.0.0.1
124
164
166
160
162
150
140
152
TCP/UDP
IP
192.168.1.1
114
112
116
168
200
202
192.168.1.55
204

FIG 2A

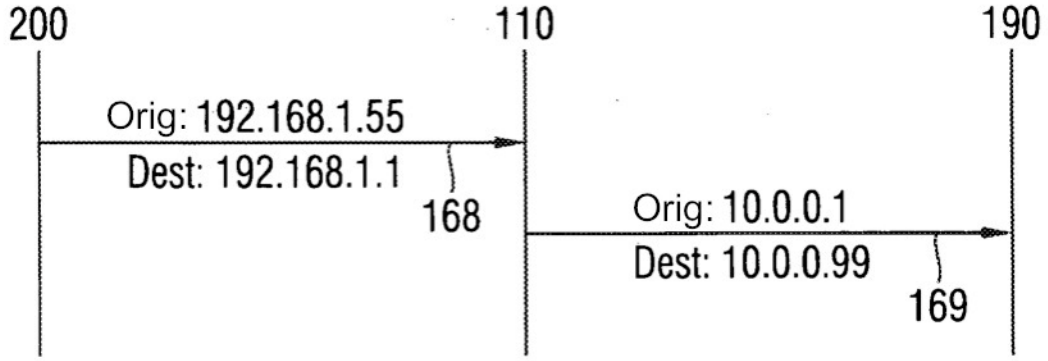
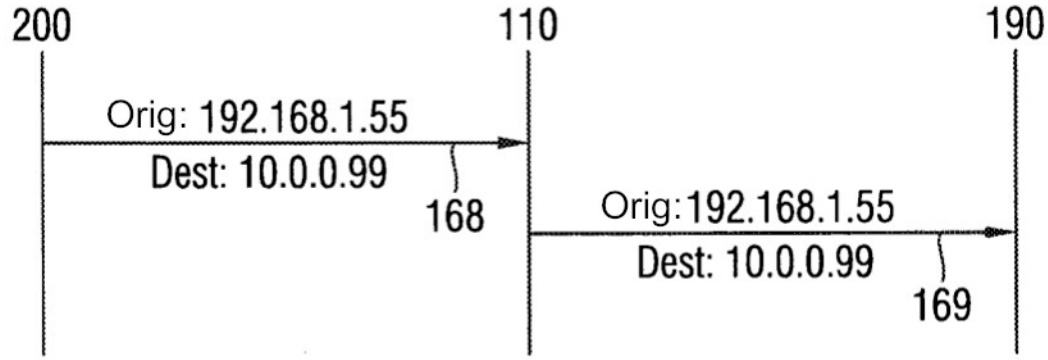

200
110
190
Orig: 192.168.1.55
Dest: 192.168.1.1
168
Orig: 10.0.0.1
Dest: 10.0.0.99
169

FIG 2B


200
110
190
Orig: 192.168.1.55
Dest: 10.0.0.99
168
Orig:192.168.1.55
Dest: 10.0.0.99
169