(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 445 706**

(51) Int. CI.:

H04L 12/46 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **28.10.2010 E 10189275 (0)**

(97) Fecha y número de publicación de la concesión europea: **04.12.2013 EP 2448182**

(54) Título: **Método para la comunicación en un sistema de automatización**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.03.2014

(73) Titular/es:

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

(72) Inventor/es:

GERLACH, HENDRIK y
KÖBINGER, FRANZ

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Método para la comunicación en un sistema de automatización

La presente invención hace referencia a un método para la comunicación en un sistema de automatización, en particular para la comunicación entre redes de automatización remotas que se comunican unas con otras mediante una red central con un relé.

Por la solicitud EP 1 249 747 A1 se conoce un sistema de control para controlar desarrollos de procedimientos, así como un método para controlar los desarrollos de procedimientos. Las señales que dependen del sistema de control se hacen pasar a través de túneles, a través de mensajes de protocolo TCP/IP que se intercambian entre controladores del bus de campo y un servidor dentro de una red, donde la conversión entre información específica de los dispositivos e información basada en OPC se efectúa de forma centralizada en un servidor.

La automatización puede efectuarse también en instalaciones de menor tamaño que se encuentran separadas de una parte central del sistema de automatización. Dichas instalaciones pueden ser por ejemplo plantas purificadoras o instalaciones de energía eólica. Las instalaciones de automatización de este tipo se denominan también instalaciones remotas de automatización. Con frecuencia, las instalaciones remotas de automatización se encuentran vinculadas a la telefonía móvil. Esta vinculación puede tener lugar por ejemplo mediante UMTS o GPRS. Para ello, a modo de ejemplo, un aparato de telefonía móvil se encuentra en la instalación, donde dicho aparato se encuentra diseñado para establecer una comunicación con la parte central del sistema de automatización. Por consiguiente, la instalación remota puede ser controlada, así como también se le puede realizar el mantenimiento, desde la parte central del sistema de automatización. Por lo general, la comunicación tiene lugar vía Internet mediante canales de red privada virtual (VPN).

Por la solicitud US 7,779,461 B1 se conoce un método que permite el reenvío de datos a lo largo de túneles VPN dentro de una VPN. De este modo, los túneles VPN son estructurados con un objetivo y se determinan direcciones next-hop para el túnel VPN.

Cuando deben transmitirse datos desde una instalación remota hacia una segunda instalación remota esta transmisión se efectúa desde la primera instalación remota a través del túnel VPN hacia la parte central del sistema de automatización. Un dispositivo VPN de la parte central del sistema de automatización determina las conexiones VPN que llegan desde las instalaciones remotas. El dispositivo VPN retransmite los datos decodificados desde el túnel VPN en un dispositivo de conmutación. En el dispositivo de conmutación se desarrolla una aplicación que retransmite los datos hacia la segunda instalación remota. Esta conmutación tiene lugar en el plano de aplicación (capa 7) del modelo de capas OSI. Para cada protocolo de aplicación se requiere una aplicación propia de conmutación. La conmutación no sólo se efectúa generada de manera específica, sino también configurada de manera específica.

A este respecto, es objeto de la presente invención crear un método mejorado para la comunicación en un sistema de automatización. Asimismo, es objeto de la presente invención crear un relé mejorado para un sistema de automatización y un sistema de automatización mejorado.

El objeto de la invención se alcanzará a través de las reivindicaciones independientes. En las reivindicaciones dependientes se indican formas de ejecución de la presente invención.

Conforme a la invención se creará un método para la comunicación en un sistema de automatización. El sistema de automatización comprende al menos una primera y una segunda red, y un relé central. La primera y la segunda red pueden denominarse igualmente como instalaciones remotas. Preferentemente, el relé se encuentra en un área central del sistema de automatización. Por tanto, la primera y la segunda red, de manera preferente, se encuentran separadas espacialmente del relé central. También es posible que la primera y la segunda red no se encuentren separadas espacialmente del relé central. La primera y la segunda red, respectivamente, comprenden al menos un dispositivo de red y respectivamente al menos un dispositivo de acceso hacia la respectiva red. La puerta de enlace de acceso posibilita la comunicación de la respectiva red con el relé en el área central del sistema de automatización. A modo de ejemplo, la puerta de enlace de acceso puede comprender un aparato de telefonía móvil, donde puede establecerse una conexión de datos con el relé central. De forma alternativa o adicional, la puerta de enlace de acceso puede estar conectada al relé central mediante una línea alámbrica. Ésta puede consistir por ejemplo en una conexión DLS, por cable o telefónica.

Se establece una conexión de datos entre la puerta de enlace de acceso de la primera red con el relé central y entre la puerta de enlace de acceso de la segunda red con el relé central. Las conexiones de datos se basan respectivamente en el protocolo IP.

Se establece un primer túnel de red privada virtual (VPN) entre la puerta de enlace de acceso de la primera red y el relé, y un segundo túnel de red privada virtual VPN entre la puerta de enlace de acceso de la segunda red y el relé.

La conexión de datos y el túnel de red privada virtual se establecen respectivamente desde las puertas de enlace de acceso. La dirección de la capa de red, por ejemplo una dirección IP, del relé central, o una información equivalente como un nombre DNS, se almacena para ello en ambas puertas de enlace de acceso o puede ser determinada por las puertas de enlace de acceso, por ejemplo a través de una resolución DNS. De este modo, las conexiones de datos entre las puertas de enlace de acceso, el relé y los túneles VPN se establecen entre las puertas de enlace de acceso y el relé independientemente de la dirección actual de la capa de red de la puerta de enlace de acceso. Por consiguiente, las puertas de enlace de acceso pueden disponer de direcciones dinámicas de la capa de red, por ejemplo de direcciones IP. Asimismo, a través de la conexión mediante los túneles VPN también se considera irrelevante si en la vía de transmisión entre la respectiva puerta de enlace de acceso y el relé central se encuentra al menos un cortafuegos, al menos un router y/o al menos un dispositivo NAT, por ejemplo un proveedor de telefonía móvil.

Si debe tener lugar una transmisión de datos desde un primer dispositivo de red de la primera red hacia un segundo dispositivo de red de la segunda red, la señal es transmitida desde el primer dispositivo de red de la primera red mediante la puerta de enlace de acceso de la primera red a través del primer túnel VPN hacia el relé central. En el relé central la señal es enrutada desde el primer túnel VPN hacia el segundo túnel VPN. De este modo, la señal es transmitida desde el relé a través del segundo túnel VPN mediante la puerta de enlace de acceso de la segunda red hacia el segundo dispositivo de red de la segunda red.

La conmutación, del mismo modo que la determinación de las conexiones VPN, se realiza a través del relé central. Preferentemente, el enrutamiento tiene lugar en la capa de red del modelo de capas OSI. Por tanto, el enrutamiento no depende de los protocolos de aplicación utilizados.

Un sistema de automatización, por ejemplo, puede estar diseñado como un sistema industrial de automatización. Los sistemas industriales de automatización de este tipo, a modo de ejemplo, pueden estar diseñados, configurados y/o previstos para controlar y/o regular instalaciones industriales (por ejemplo instalaciones de producción, instalaciones de transporte, etc.). En particular, los sistemas de automatización, así como los sistemas industriales de automatización, pueden presentar protocolos de comunicación en tiempo real (por ejemplo Profinet, Profibus, Real-Time-Ethernet) para la comunicación, al menos entre los componentes que participan en las tareas de control y/o de regulación (por ejemplo entre las unidades de control y las instalaciones y/o máquinas a ser controladas). La transmisión protegida de los datos se encuentra cubierta igualmente a través de medios de almacenamiento.

Asimismo, junto con un protocolo de comunicación en tiempo real, puede proporcionarse también al menos un protocolo de comunicación adicional (que no necesariamente debe operar en tiempo real) en el sistema de automatización o en el sistema industrial de automatización, por ejemplo para controlar, configurar, reprogramar y/o reparametrizar una o varias unidades en el sistema de automatización.

n sistema de automatización, por ejemplo, puede contener componentes de comunicación a través de conexiones y/o componentes de conexión inalámbricos. Un sistema de automatización puede comprender además al menos un equipo de automatización.

Un equipo de automatización puede consistir por ejemplo en un ordenador, un PC y/o un controlador con tareas de control o con capacidades de control. En particular, un equipo de automatización puede consistir, a modo de ejemplo, en un equipo industrial de automatización que por ejemplo se encuentra especialmente diseñado, configurado y/o previsto para controlar y/o regular instalaciones industriales. En particular, los equipos de automatización de esta clase, así como los equipos industriales de automatización, pueden operar en tiempo real, es decir que posibilitan un control o una regulación en tiempo real. Para ello, el equipo de automatización o el equipo industrial de automatización puede comprender por ejemplo un sistema operativo en tiempo real y/o al menos, entre otros, ser respaldado por un protocolo de comunicación en tiempo real para la comunicación (por ejemplo Profinet, Profibus, Real-Time- Ethernet).

Un sistema de automatización comprende varios sensores y actuadores. Los actuadores y los sensores son controlados al menos por un dispositivo de control. Los actuadores, los sensores y al menos un dispositivo de control intercambian datos unos con otros. Para el intercambio de datos se utiliza un protocolo de automatización. Al menos un dispositivo de control controla los actuadores, los sensores y el intercambio de datos de manera que se desarrolla un proceso de fabricación mediante maquinaria, en el cual por ejemplo se fabrica un producto.

Un dispositivo industrial de automatización, por ejemplo, puede contener un controlador programable de almacenamiento, un módulo o parte de un controlador programable de almacenamiento, un controlador programable de almacenamiento integrado a un ordenador o a un PC, así como dispositivos de campo apropiados, sensores y/o

actuadores, dispositivos de entrada y/o de salida o similares para la conexión a un controlador programable de almacenamiento o similares.

Dentro del marco de la presente invención se entiende como protocolo de automatización cualquier clase de protocolo que se encuentra previsto, adaptado y/o configurado para la comunicación con equipos de automatización, conforme a la presente descripción. Los protocolos de automatización de esta clase, por ejemplo, pueden consistir en el protocolo de Profi-bus (por ejemplo conforme a IEC 61158/EN50170), un protocolo DP de Profi-bus, un protocolo PA de Profi-bus, un protocolo Profi-Net, un protocolo IO Profi-Net, un protocolo conforme a la interfaz AS, un protocolo conforme a IOLink, un protocolo KNX, un protocolo conforme a una interfaz multipunto (Multipoint-Interface, MPI), un protocolo para un acoplamiento punto a punto (Point-to-Point, PtP), un protocolo conforme a las especificaciones de la comunicación SIMATIC S7 (la cual por ejemplo se encuentra prevista y configurada por la empresa Siemens para la comunicación de controladores programables de almacenamiento) o también un protocolo ethernet industrial o protocolo en tiempo real, así como otros protocolos específicos para la comunicación con equipos de automatización. Dentro del marco de la presente descripción, como protocolo de automatización puede preverse también cualquier combinación deseada de los protocolos mencionados.

Debe tenerse en cuenta que el método según las formas de ejecución de la invención no se encuentra limitado a un sistema de automatización, sino que también puede utilizarse para otros sistemas con al menos una primera y una segunda red.

De acuerdo con las formas de ejecución de la invención, el enrutamiento de la señal consiste en un enrutamiento IP.

De acuerdo con formas de ejecución de la invención, la autorización del primer dispositivo de red para la comunicación es controlada con el relé. Además, el control de la autorización del primer dispositivo de red para la comunicación se controla con el segundo dispositivo de red. Si el primer dispositivo de red no está autorizado para la comunicación con el relé y/o con el segundo dispositivo de red, se impide entonces el enrutamiento de la señal y la transmisión de la señal hacia el segundo dispositivo de red. Los controles de las respectivas autorizaciones del primer dispositivo de red se efectúan igualmente en el relé central. A modo de ejemplo, puede aplicarse para ello una así llamada política de túnel en el extremo del túnel VPN. Por ejemplo, puede controlarse si en general todos los dispositivos de campo de la primera red están autorizados para la comunicación con los dispositivos de red de la segunda red. De forma alternativa o adicional puede controlarse qué puertas de enlace de datos de la primera y/o de la segunda red están autorizadas para establecer un túnel VPN hacia el relé central. Esto puede realizarse por ejemplo mediante certificados o claves precompartidas (preshared keys).

De forma alternativa o adicional, en el relé central puede implementarse también una así llamada política de acceso. Esto significa que se controla si el primer dispositivo de red en la primera red está autorizado para la comunicación con un dispositivo de red en la segunda red o también para la comunicación con el relé central. Esto puede efectuarse por ejemplo a través del control de la dirección de la capa de red del primer dispositivo de red.

Los controles de las respectivas autorizaciones se consideran ventajosos cuando debe restringirse el tráfico de datos mediante el respectivo túnel VPN. Esto puede tener lugar por ejemplo a través de un cortafuegos que se encuentra situado aguas abajo en el punto de demarcación VPN en la puerta de enlace de acceso y/o en el relé central.

De acuerdo con las formas de ejecución de la invención, el establecimiento de al menos una de las dos conexiones de datos desde la primera red hacia el relé y desde la segunda red hacia el relé tiene lugar a través de la respectiva puerta de enlace de acceso. Por tanto, la respectiva puerta de enlace de acceso da inicio al establecimiento de las dos conexiones de datos.

De acuerdo con las formas de ejecución de la invención, el establecimiento de la conexión de datos desde la segunda red hacia el relé central y el establecimiento del segundo túnel VPN se inician a través de una señalización mediante un canal de datos desde el primer dispositivo de red de la primera red hacia el segundo dispositivo de red de la segunda red. En el caso de que el primer dispositivo de red desee establecer una conexión de datos con el segundo dispositivo de red, pero el segundo dispositivo de red no hubiera iniciado aún una conexión hacia el relé central, el primer dispositivo de red, a través de una señalización, puede iniciar el establecimiento de la conexión desde la puerta de enlace de acceso de la segunda red hacia el relé central. Esto puede considerarse como ventajoso cuando por ejemplo el primer dispositivo de red desea comunicarse con el segundo dispositivo de red, aunque el segundo dispositivo no posea una conexión hacia el relé central. A modo de ejemplo, la señalización puede tener lugar mediante una red de telefonía móvil.

De acuerdo con las formas de ejecución de la invención, la señalización consiste en un mensaje de texto o en una llamada telefónica transmitidos mediante una conexión de un teléfono móvil. El mensaje de texto, por ejemplo, puede ser un SMS protegido contra un uso incorrecto. La protección contra uso incorrecto, a modo de ejemplo, puede tener lugar a través de una transmisión, encriptación y/o firma protegidas.

De acuerdo con las formas de ejecución de la invención, el enrutamiento tiene lugar en la capa de red del modelo de capas OSI.

De acuerdo con la invención, a través del relé se efectúa un registro de las señales transmitidas.

De acuerdo con la invención, un usuario del primer dispositivo de red en la primera red se autentifica con datos de autentificación. Los datos de autentificación pueden ser por ejemplo un nombre de usuario y una contraseña. Los datos de autentificación son transmitidos antes de la señal desde la puerta de enlace de acceso de la primera red hacia el relé central. La autorización del usuario para la comunicación con el segundo dispositivo de red en la segunda red es controlada mediante datos de políticas. Por lo tanto se efectúa un control de la autorización del usuario. Además, la autorización del usuario para la comunicación con el segundo dispositivo de red en la segunda red es controlada mediante una política de acceso. El control de la autorización del usuario puede tener lugar en los mismos lugares en el relé central, del mismo modo que el control anteriormente descrito de la autorización del primer dispositivo de red. La autentificación de un usuario con los datos de autentificación puede tener lugar en el punto de reforzamiento (enforcement point) para la política de acceso en el relé central.

Después de efectuada la autentificación, a cada usuario se le puede asignar un conjunto de reglas de política de acceso que controla sus derechos de acceso y representa una parte de toda la política de acceso. Esto puede tener lugar por ejemplo a través de un cortafuegos que se encuentra situado aguas abajo en el punto de demarcación VPN en la puerta de enlace de acceso.

Expresado de otro modo, la autentificación del usuario se efectúa en el relé central. Después de finalizada exitosamente la autentificación del usuario, al dispositivo de red utilizado por el usuario se le asigna una política de acceso que permite y/o prohíbe una comunicación de ese dispositivo de red con otros dispositivos de red en el sistema de automatización. La política de acceso asignada a ese dispositivo de red es apropiada con respecto al usuario autentificado.

Después de finalizada exitosamente la autentificación del usuario, por consiguiente, para el primer dispositivo de red se configura una autorización para la comunicación con el segundo dispositivo de red.

Además, los datos de autentificación pueden utilizarse para la autentificación de dispositivos de las puertas de enlace de acceso. Los datos de autentificación para una autentificación de dispositivos de las puertas de enlace de acceso, a modo de ejemplo, pueden consistir en certificados o en claves precompartidas (preshared keys).

Los dispositivos de red, durante el control de las políticas de túnel y de acceso, se identifican mediante sus direcciones de la capa de red.

En cuanto a otro aspecto, la presente invención hace referencia a un relé para un sistema de automatización. El relé comprende medios para la comunicación con la puerta de enlace de acceso de la primera red y con la puerta de enlace de acceso de la segunda red. Estos medios pueden consistir por ejemplo en una interfaz, mediante la cual la puerta de enlace de acceso puede comunicarse a través de una conexión de telefonía móvil, de una conexión telefónica o de una conexión de Internet. Además, el relé comprende medios para establecer un túnel VPN entre la puerta de enlace de acceso de la primera red y el relé, y un segundo túnel VPN entre la puerta de enlace de acceso de la segunda red y el relé. Estos medios pueden consistir por ejemplo en un procesador que ejecuta un programa, el cual induce al procesador a determinar las conexiones VPN que provienen de las puertas de enlace de acceso de las dos redes.

El relé presenta además medios para recibir una señal protegida desde un primer participante de la red en la primera red mediante la puerta de enlace de acceso de la primera red a través del primer túnel VPN. Asimismo, la señal del primer dispositivo de red puede ser recibida igualmente mediante la interfaz de la puerta de enlace de acceso.

El relé comprende también medios para el enrutamiento de la señal. Por ejemplo, el enrutamiento puede ser ejecutado a través del procesador y, de manera preferente, tiene lugar en la capa de red del modelo de capas OSI. Asimismo, el relé comprende medios para la transmisión de la señal, protegida a través del túnel VPN, desde el relé a través del segundo túnel VPN mediante la puerta de enlace de acceso de la segunda red hacia el segundo dispositivo de red de la segunda red. La señal puede ser transmitida por ejemplo a través del procesador mediante la interfaz del relé.

En cuanto a otro aspecto, la presente invención hace referencia a un sistema de automatización con un relé central acorde a las formas de ejecución de la invención.

A continuación se explican en detalle formas de ejecución de la invención mediante los dibujos. Las figuras muestran:

Figura 1: una representación esquemática de un sistema de automatización con dos redes, respectivamente con una puerta de enlace de datos y un área central del sistema de automatización con un relé central;

Figura 2: un diagrama de bloques de un sistema de automatización con dos redes y un relé central; y

Figura 3: un diagrama de flujo de un método acorde a las formas de ejecución de la invención.

Los elementos de las siguientes figuras que se corresponden se encuentran indicados con los mismos símbolos de referencia.

La figura 1 muestra una representación esquemática de un sistema de automatización 100 con una primera red 102 y una segunda red 104. En un área central 108 del sistema de automatización 100 se encuentra un relé central 106. La primera red 102 comprende un primer dispositivo de red 114, un segundo dispositivo de red 116 y un tercer dispositivo de red 118. La segunda red 104 comprende un primer dispositivo de red 110 y un segundo dispositivo de red 112. Debe tenerse en cuenta que tanto la primera red como la segunda red pueden comprender más o menos dispositivos de red que los aquí representados.

La primera red 102 comprende además una primera puerta de enlace de acceso 120 y la segunda red 104 una segunda puerta de enlace de acceso 122.

A modo de ejemplo, los dispositivos de red 110 - 118 pueden consistir en equipos de automatización como por ejemplo controladores programables de almacenamiento. El dispositivo de red 118, por ejemplo, es un ordenador que se encuentra igualmente en la primera red 102.

Las dos puertas de enlace de acceso 120 y 122, mediante un punto de acceso 124 de una red de telefonía móvil, establecen una conexión hacia el relé central 106. De forma alternativa, la conexión puede tener lugar también mediante una conexión por cable, como por ejemplo una conexión telefónica. Cuando se encuentra establecida la conexión entre las puertas de enlace de acceso 120 y 122 con el relé central 106, las puertas de enlace de acceso 120 y 122 establecen un túnel VPN entre la respectiva puerta de enlace de acceso y el relé central 106. Se encuentra presente por tanto una conexión entre la puerta de enlace de acceso 120 de la primera red 102 y el relé central 106, y una conexión entre la puerta de enlace de acceso 122 de la segunda red 104 con el primer relé 106. Además se establece un túnel VPN entre la puerta de enlace de acceso 120 de la primera red 102 y el relé central 106, y otro túnel VPN entre la puerta de enlace de acceso 122 de la segunda red 104 con el relé central 106.

Por ejemplo, si el tercer dispositivo de red 118 de la primera red 102 desea transmitir una señal en el primer dispositivo de red 110 de la segunda red 104, esa señal es transmitida primero desde el tercer dispositivo de red 118 de la primera red 102 en la puerta de enlace de acceso 120 de la primera red 102. La puerta de enlace de acceso 120 transmite la señal entonces mediante el túnel VPN hacia el relé central 106. En el relé central 106, la señal es enrutada en la capa de red del modelo de capas OSI y es transmitida a través del túnel VPN en la puerta de enlace de acceso 122 de la segunda red 104. La puerta de enlace de acceso 122 de la segunda red 104 transmite a su vez la señal hacia el primer dispositivo de red 110 de la segunda red 104. Por lo tanto, es posible la transmisión de una señal desde cada dispositivo de red de la primera red 102 hacia cada dispositivo de red de la segunda red 104 y viceversa. La transmisión de señal se efectúa respectivamente mediante los túneles VPN que se encuentran entre las puertas de enlace de acceso 120 y 122 y el relé central 106. El enrutamiento de la señal tiene lugar en el relé 106 en la capa de red del modelo de capas OSI, de manera que la conmutación tiene lugar de forma independiente con respecto a un protocolo de aplicación.

En la figura 2 se muestra un diagrama de bloques del sistema de automatización 100 con la primera red 102 y la segunda red 104. Se representa además el relé central 106. En la primera red 102 se encuentra la puerta de enlace de acceso 120 y en la segunda red 104 la puerta de enlace de acceso 122. Las puertas de enlace 120 y 122, respectivamente, se encuentran configuradas para establecer una conexión y un túnel VPN con el relé central 106. La puerta de enlace de acceso 120 establece el túnel 202 VPN hacia el relé central y la puerta de enlace de acceso 122 el túnel VPN 200. El sistema de automatización 100 puede también comprender más redes que la primera red 102 y la segunda red 104. Para ello, el relé central 106 comprende medios para establecer al menos un túnel VPN adicional 204.

El relé central 106 comprende además un procesador 206 y una memoria de datos 208. Un programa 210 en la memoria de datos 208 se encuentra diseñado para inducir al procesador a establecer una comunicación con las puertas de enlace de acceso, para establecer los túneles VPN, para recibir señales desde los dispositivos de red, para el enrutamiento de las señales y para transmitir las señales.

Al recibir una señal de un dispositivo de red de la primera red 102 mediante la puerta de enlace de acceso 120 a través del túnel VNP 202, la autorización del dispositivo de red para la comunicación con el relé central es controlada en el punto final del túnel 212. A modo de ejemplo, el control puede ser efectuado a través del procesador 206. Aquí

puede efectuarse también el control de los datos de autentificación del usuario. Mediante los datos de autentificación de un usuario puede controlarse si el usuario está autorizado para la comunicación con el relé central 106.

Una autentificación del usuario, por ejemplo, puede desarrollarse del siguiente modo. Primero se establece el túnel 202. Aquí se controla si está permitido el establecimiento de un túnel VPN hacia el relé. Para ello se controlan certificados o claves precompartidas (preshared keys).

A continuación, la comunicación se controla en el túnel. Esto concierne al intercambio de datos o de señales entre un dispositivo de red de la primera red 102 y un dispositivo de red de la segunda red 104. Debe tenerse en cuenta que el túnel ya se ha establecido. Una política de túnel controla qué direcciones de capa de red, por ejemplo direcciones IP, y/o qué subredes pueden intercambiar señales con otras direcciones de capa de red y/o subredes. Por ejemplo, puede determinarse que la primera red 102 puede intercambiar señales con la segunda red 104. También puede determinarse que la primera red 102 puede intercambiar señales con una tercera red (lo cual no se encuentra aquí representado).

En los puntos de reforzamiento de políticas 218-222 pueden controlarse los datos de autentificación del usuario. En base a esa autentificación del usuario se determinan autorizaciones de acceso para el respectivo dispositivo de campo. Expresado de otro modo, en caso de una autorización exitosa del usuario para el dispositivo de red, con la cual ha autentificado el usuario, se determinan autorizaciones de acceso para ese usuario. Por ejemplo, un dispositivo de red de la primera red no está autorizado para el intercambio de señales con la segunda red. Después de una autentificación exitosa del usuario puede determinarse que ese dispositivo de red está autorizado para el intercambio de señales con la segunda red. Por tanto, la autorización se determina para la dirección fuente de la capa de red.

También el túnel VPN 200 dispone de un punto final del túnel 214. Aquí igualmente se controla si un dispositivo de red de la segunda red 104 está autorizado para la comunicación con el relé central 106. El relé central 106 comprende un punto final del túnel para cada túnel VPN. Por ejemplo, para el túnel 204 éste es el punto final del túnel 216.

En cada punto final del túnel 212-216 se encuentra también un punto de reforzamiento para la respectiva política del túnel.

Inmediatamente después de los puntos finales del túnel 212 - 216 pueden efectuarse otros controles de autorización. Aquí pueden implementarse otras políticas de acceso, como por ejemplo un control de la autorización del dispositivo de red que ha iniciado la transmisión de la señal, para la comunicación con el dispositivo de red -objetivo de la señal. Estos controles adicionales, para el túnel VPN 202, tienen lugar en el punto de reforzamiento de políticas 218, para el túnel VPN 200 en el punto de reforzamiento de políticas 220 y para el túnel VPN potencial 204 en el punto de reforzamiento de políticas 222.

En el relé central 106 tiene lugar además un enrutamiento 224 de la señal. Preferentemente, el enrutamiento tiene lugar en la capa de red del modelo de capas OSI. Esto se considera ventajoso, puesto que la señal puede ser enrutada de forma independiente con respecto a la aplicación que ha transmitido la señal. A modo de ejemplo, el enrutamiento puede tener lugar desde un primer dispositivo de red de la primera red 102 hacia un segundo dispositivo de red de la segunda red 104. Después del enrutamiento, las señales que fueron recibidas mediante el primer túnel 202 son transmitidas mediante el segundo túnel VPN 200 en la puerta de enlace de acceso 122 de la segunda red 104. La puerta de enlace de acceso 122 de la segunda red 104 transmite a su vez la señal en el segundo dispositivo de red de la segunda red 104.

Asimismo, el relé central 106 dispone de un componente de registro 226. El componente de registro 226 está diseñado para registrar las señales transmitidas. De forma alternativa o adicional, mediante las señale transmitidas, puede registrarse también información de los puntos finales de los túneles y de los puntos de reforzamiento Ésta puede tratarse por ejemplo de información relativa a cuándo una señal fue transmitida, desde dónde y hacia dónde y/o relativa a cuándo una señal no fue transmitida y por qué. Por ejemplo en el caso del punto final del túnel 212 puede tratarse de información sobre cuándo se intentó establecer un túnel y si el intento fue exitoso, cuándo y por qué fue establecido el túnel, cuántos datos se transmitieron mediante el túnel y/o qué grado de encriptación posee el túnel. Para el punto de reforzamiento de políticas 218 esta información podría referirse a qué usuario fue autentificado exitosamente, cuándo y dónde, qué usuario no fue autentificado con éxito y/o qué accesos fueron o no permitidos.

Esto puede ser ventajoso para poder realizar el seguimiento de transmisiones de señal, del establecimiento de un túnel y/o también de la acciones de los puntos de reforzamiento de políticas. Por tanto, cada transmisión de señal, cada establecimiento o intento de establecer un túnel y cada acción en los puntos de reforzamiento de políticas pueden registrarse dentro del relé central. A los fines de una simplificación, en la figura 2 se indican sólo las conexiones desde el punto final del túnel 214 y desde el punto de reforzamiento de políticas 220 hacia el

componente de registro 226. Las mismas conexiones se presentan también desde los puntos finales de los túneles 216 y 212 y desde los puntos de reforzamiento de políticas 218 y 222 hacia el componente de registro.

La figura 3 muestra un diagrama de flujo de un método acorde a las formas de ejecución de la invención. En un primer paso S1 se establece una conexión de datos entre la puerta de enlace de acceso de la primera red y el relé central. Además, el paso S1 comprende el establecimiento de una conexión de datos entre la puerta de enlace de acceso de la segunda red y el relé central. De este modo, en el paso S2 se establece un primer túnel VPN entre la puerta de enlace de acceso de la primera red y el relé. Asimismo, en el paso S2 se establece otro segundo túnel VPN entre la puerta de enlace de acceso de la segunda red y el relé.

En el paso S3 una señal se transmite desde un primer dispositivo de red de la primera red mediante la puerta de enlace de acceso de la primera red a través del primer túnel VPN hacia el relé central. En el paso S4 la señal es enrutada dentro del relé central desde el primer túnel VPN hacia el segundo túnel VPN. De este modo, la señal es transmitida en el paso S5 desde el relé a través del segundo túnel VPN mediante la puerta de enlace de acceso de la segunda red hacia el segundo dispositivo de red de la segunda red.

Lista de referencias

100 sistema de automatización

102 primera red

104 segunda red

106 relé central

108 área central

110 primer dispositivo de red (en la segunda red)

112 segundo dispositivo de red (en la segunda red)

114 primer dispositivo de red (en la primera red)

116 segundo dispositivo de red (en la primera red)

118 tercer dispositivo de red (en la primera red)

120 puerta de enlace de acceso (de la primera red)

122 puerta de enlace de acceso (de la segunda red)

124 punto de acceso

200 túnel VPN

202 túnel VPN

204 túnel VPN

206 procesador

208 memoria de datos

210 programa

212 punto final del túnel con punto de reforzamiento de la política del túnel

214 punto final del túnel con punto de reforzamiento de la política del túnel

216 punto final del túnel con punto de reforzamiento de la política del túnel

218 punto de reforzamiento de la política de acceso

220 punto de reforzamiento de la política de acceso

222 punto de reforzamiento de la política de acceso

224 enrutamiento

226 registro

REIVINDICACIONES

1. Método para la comunicación en un sistema de automatización (100), donde el sistema de automatización comprende al menos una primera red (102) y una segunda red (104) y un relé central (106), donde la primera y la segunda red comprenden respectivamente al menos un dispositivo de red (110; 112; 114; 116; 118) y respectivamente al menos una puerta de enlace de acceso (120; 122) hacia la respectiva red, donde el método comprende los siguientes pasos:

- establecimiento (S1) respectivamente de una conexión de datos entre la puerta de enlace de acceso de la primera red con el relé central y entre la puerta de enlace de acceso de la segunda red con el relé central, donde la conexión de datos se basa en el protocolo IP,

- establecimiento (S2) de un primer túnel de red privada virtual (202) entre la puerta de enlace de acceso de la primera red y el relé, y de un segundo túnel de red privada virtual (200) entre la puerta de enlace de acceso de la segunda red y el relé,

- registro de las señales transmitidas a través del relé,

- autentificación de un usuario del primer dispositivo de red con datos de autentificación,

- transmisión (S3) de una señal desde el primer dispositivo de red de la primera red mediante la puerta de enlace de acceso de la primera red a través del primer túnel de red privada virtual hacia el relé central,

- enrutamiento (S4; 224) de la señal dentro del relé central desde el primer túnel de red privada virtual hacia el segundo túnel de red privada virtual,

- transmisión (S5) de la señal desde el relé a través del segundo túnel de red privada virtual mediante la puerta de enlace de acceso de la segunda red hacia un segundo dispositivo de red de la segunda red.

2. Método conforme a la reivindicación 1, donde el enrutamiento de la señal consiste en un enrutamiento IP de la señal.

3. Método conforme a una de las reivindicaciones precedentes, donde el método comprende además los siguientes pasos:

- control de la autorización del primer dispositivo de red para la comunicación con el relé,

- control de la autorización del primer dispositivo de red para la comunicación con el segundo dispositivo de red,

- prevención del enrutamiento de la señal y de la transmisión de la señal hacia el segundo dispositivo de red cuando el primer dispositivo de red no está autorizado para la comunicación con el relé y/o con el segundo dispositivo de red.

4. Método conforme a una de las reivindicaciones precedentes, donde el establecimiento de una de las dos conexiones de datos desde la primera red hacia el relé y desde la segunda red hacia el relé tiene lugar a través de la respectiva puerta de enlace de acceso.

5. Método conforme a una de las reivindicaciones precedentes, donde el establecimiento del primer y del segundo túnel de red privada virtual es iniciado a través de la respectiva puerta de enlace de acceso.

6. Método conforme a una de las reivindicaciones precedentes, donde el establecimiento de la conexión de datos desde la segunda red hacia el relé central y el establecimiento del segundo túnel de red privada virtual es iniciado a través de una señalización mediante un canal de datos desde el primer dispositivo de red hacia el segundo dispositivo de red de la segunda red o a través de una señalización mediante un canal de datos desde la primera puerta de enlace de acceso hacia la segunda puerta de enlace de acceso.

7. Método conforme a la reivindicación 6, donde la señalización consiste en un mensaje de texto o en una llamada telefónica transmitidos mediante una conexión de un teléfono móvil.

8. Método conforme a una de las reivindicaciones precedentes, donde el enrutamiento tiene lugar en una capa de red.

9. Método conforme a una de las reivindicaciones precedentes, donde el método comprende además los siguientes pasos:

- control de la autorización del usuario para la comunicación con el segundo dispositivo de red mediante los datos de autentificación, y

- configuración de una autorización del primer dispositivo de red para la comunicación con el segundo dispositivo de red.

10. Relé (106) para un sistema de automatización, donde el relé comprende

- medios (206) para la comunicación con una puerta de enlace de acceso de la primera red y con una puerta de enlace de acceso de la segunda red, donde la comunicación se basa en el protocolo IP,

- medios (212; 216; 214) para el establecimiento de un primer túnel de red privada virtual entre la puerta de enlace de acceso de una primera red y el relé, y de un segundo túnel de red privada virtual entre la puerta de enlace de acceso de la segunda red y el relé,

- medios (212) para recibir una señal desde un primer dispositivo de red en la primera red mediante la puerta de enlace de acceso de la primera red a través del primer túnel de red privada virtual,

- medios (224) para el enrutamiento de la señal, y

- medios (214) para la transmisión de la señal desde el relé a través del segundo túnel de red privada virtual mediante la puerta de enlace de acceso de la segunda red hacia un segundo dispositivo de red de la segunda red,

- medios para el registro (226) de las señales transmitidas,

- medios para la autentificación de un usuario del primer dispositivo de red con datos de autentificación.

11. Relé conforme a la reivindicación 10, donde el relé está diseñado para ejecutar un método según una de las reivindicaciones 1-9.

12. Sistema de automatización (100) con al menos una primera red (102), una segunda red (104) y un relé (106) según una de las reivindicaciones 10 u 11, donde la primera y la segunda red respectivamente comprenden al menos un dispositivo de red y respectivamente al menos una puerta de enlace de acceso (120; 122).

13. Sistema de automatización conforme a la reivindicación 12, donde el sistema de automatización está diseñado para ejecutar un método según una de las reivindicaciones 1-9.

FIG 1

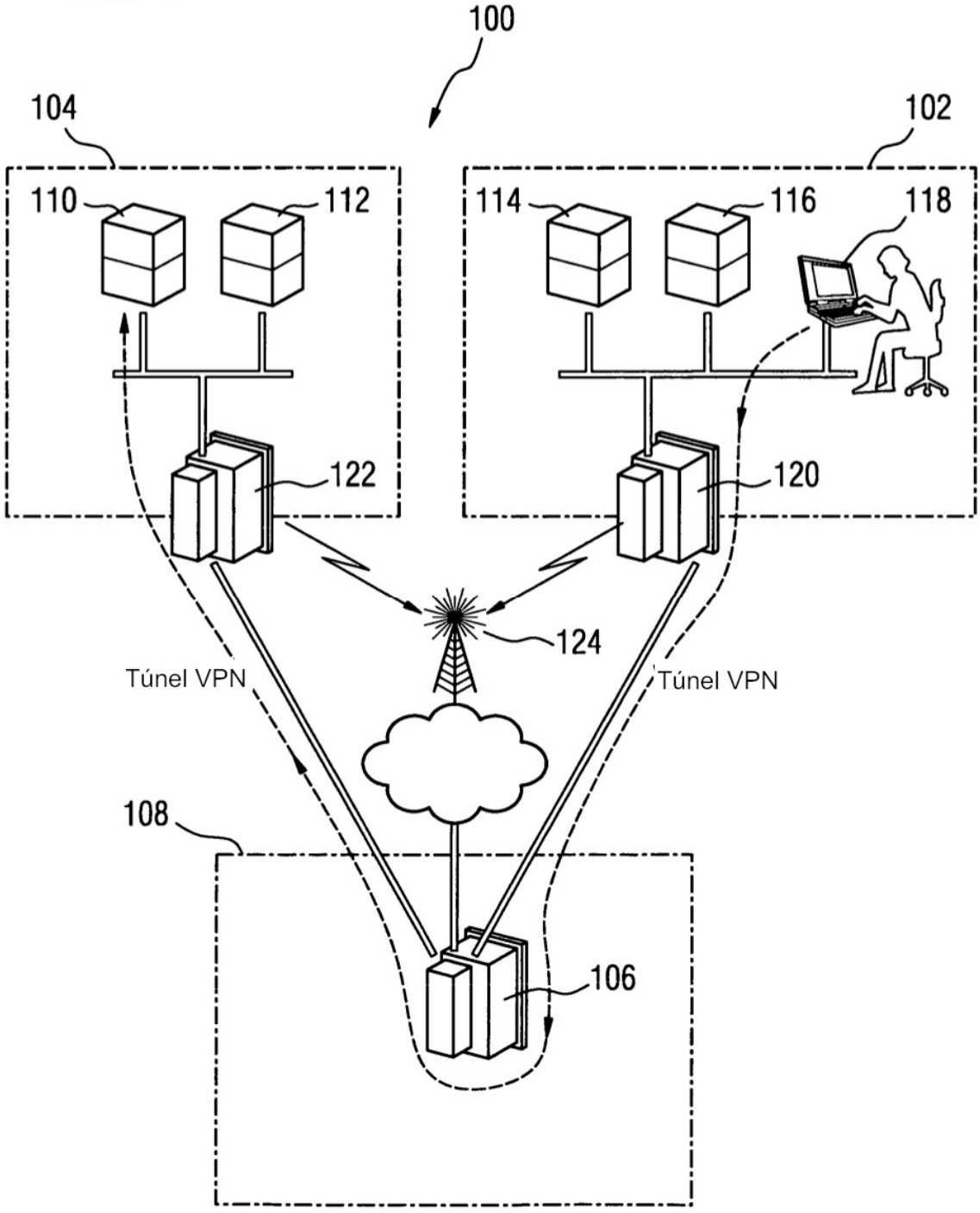
100
104
102
110
112
114
116
118
122
120
124
Túnel VPN
Túnel VPN
108
106

FIG 2

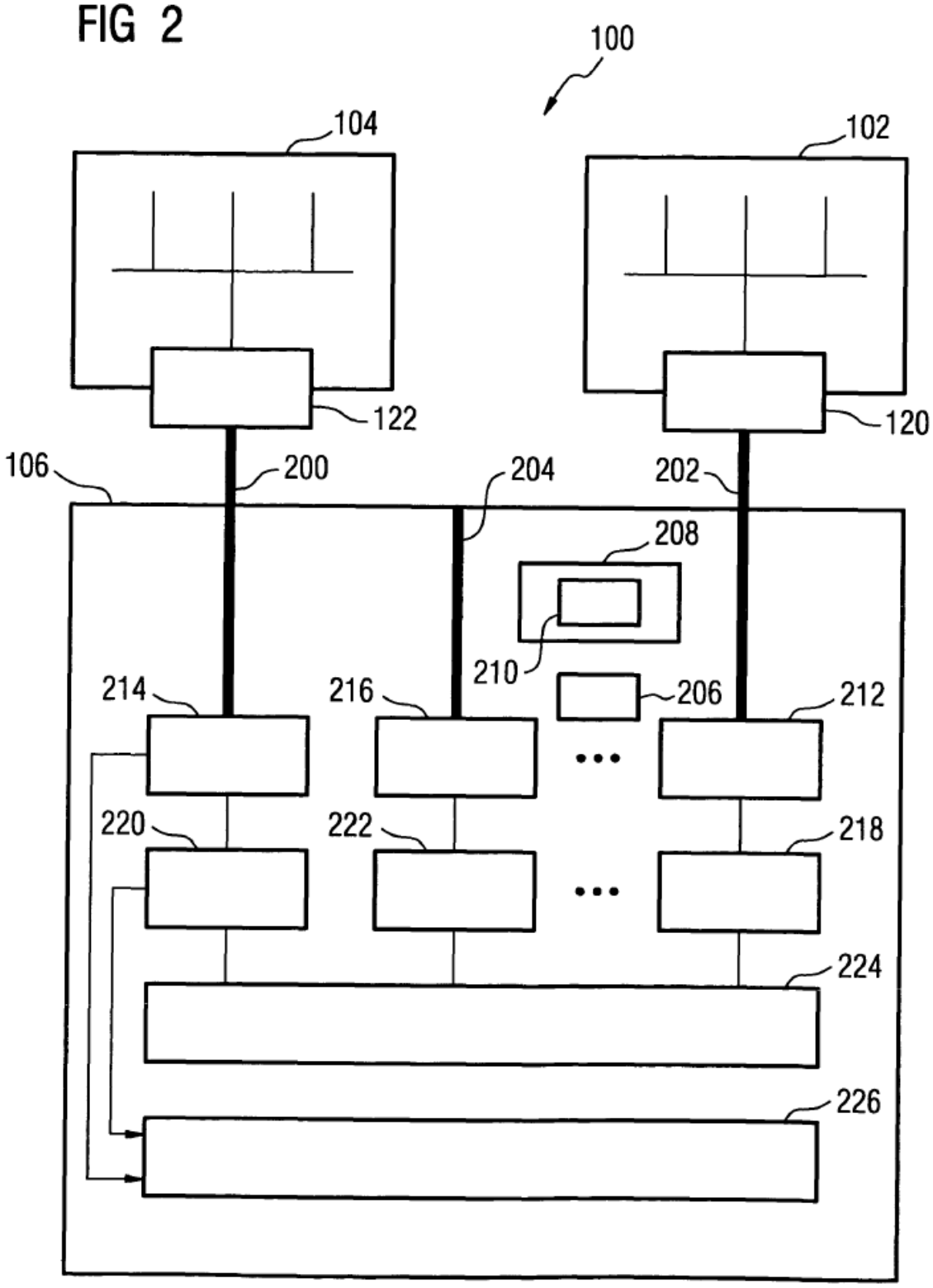
100
104
102
122
120
106
200
204
202
208
210
214
216
206
212
220
222
218
224
226

FIG 3