(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 531 148**

(51) Int. CI.:

H04L 29/06 (2006.01)
G05B 19/41 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **30.03.2012 E 12714986 (2)**

(97) Fecha y número de publicación de la concesión europea: **24.12.2014 EP 2656580**

(54) Título: **Procedimiento y equipo de comunicación para la protección criptográfica de una comunicación de datos de un aparato de campo**

(30) Prioridad:

12.04.2011 DE 102011007199

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.03.2015

(73) Titular/es:

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

(72) Inventor/es:

FALK, RAINER

(74) Agente/Representante:

PÉREZ BARQUÍN, Eliana

PROCEDIMIENTO Y EQUIPO DE COMUNICACIÓN PARA LA PROTECCIÓN CRIPTOGRÁFICA DE UNA COMUNICACIÓN DE DATOS DE UN APARATO DE CAMPO

DESCRIPCIÓN

La presente invención se refiere a un procedimiento y a un equipo de comunicación para la protección criptográfica de una comunicación de datos de un aparato de campo.

Estado de la técnica

Los aparatos de campo industriales, como por ejemplo aparatos de control para instalaciones ferroviarias y de vías férreas, comunican cada vez con más frecuencia mediante protocolos de comunicación abiertos como TCP/IP, en lugar de mediante protocolos propietarios. Entonces los mismos utilizan redes públicas como por ejemplo Internet para transmitir datos de comunicación a una central o a otros aparatos de campo. Para proteger la transmisión de datos frente a manipulaciones, se utilizan mecanismos de protección criptográficos, por ejemplo MACsec, SSL/TSL, WS-Security o IPsec.

El documento US 2007/0056032 A1 da a conocer al respecto una técnica para proporcionar un enlace Virtual-Private-Network (enlace VPN, de red privada virtual). Allí se establece el enlace VPN con una pasarela remota (Remote-Gateway) mediante un adaptador de red con un firmware sobre una plataforma. Además se genera un evento que se comunica a un activador de red mediante una interfaz de activador de bus. En base a una solicitud del activador de red del sistema operativo, se suministran informaciones de red.

El documento WO 00/36807 da a conocer además un sistema y un procedimiento para aportar un acceso seguro a datos del sensor remotos a través de una red privada virtual codificada. El sistema utiliza una arquitectura escalable e incluye un servidor central del sensor que a través de la citada red, está conectado con una pluralidad de centros con sensores. La red privada virtual puede realizarse mediante una red con conmutación de paquetes, como Internet, pudiendo operar monitores de sensor remotos a través de un navegador de web (Web-Browser). El sistema utiliza entonces diversos servicios de autentificación y seguridad para proteger los datos del sensor.

En la publicación previa "Bus de campo, Ethernet, Internet, TCP/IP - ¿Todo está claro?" (XP002288533) se consideran finalmente aspectos generales sobre la integración de sensores de la técnica de automatización a través de Internet. No obstante, la citada integración se realiza entonces sin un VPN y sin tener en cuenta aspectos de seguridad.

A menudo, debido a la potencia de cálculo necesaria, la memoria necesaria, la autorización o la compatibilidad en sentido descendente, no pueden dotarse los propios aparatos de campo de una técnica de red de esta clase, por lo que la mayoría de las veces se utilizan aparatos externos para constituir redes privadas virtuales (VPN) para la comunicación de aparatos de campo a través de redes públicas como Internet y para poder garantizar la seguridad necesaria. Tales aparatos externos deben configurarse para la comunicación con datos criptográficos asegurados. Para ello es necesaria una clave de comunicación criptográfica secreta, con la cual puedan codificarse y decodificarse datos que se envíen y reciban a través de la VPN.

La configuración de los aparatos externos es costosa y susceptible de faltas. Una posibilidad es buscar los aparatos externos localmente y configurarlos o reconfigurarlos. Esta posibilidad requiere mucho tiempo.

Existe por lo tanto la necesidad de soluciones para una configuración sencilla de un aparato VPN externo para aparatos de campo con la que quede garantizada a la vez una elevada seguridad de los datos criptográficos.

Resumen de la invención

Una forma de ejecución de la presente invención consiste por lo tanto en un procedimiento para la protección criptográfica de una comunicación de datos de un aparato de campo, con las etapas de identificación del aparato de campo mediante un equipo de comunicación en base a un código de identificación del aparato de campo, de la elección de una configuración VPN asociada al aparato de campo identificado mediante el equipo de comunicación, del establecimiento de un enlace de VPN sobre la base de la configuración VPN elegida mediante el equipo de comunicación y de la transmisión de datos de control a través del aparato de campo a un servidor VPN a través del enlace VPN establecido.

Según una forma de ejecución ventajosa incluye el procedimiento una autentificación del aparato de campo mediante el equipo de comunicación por medio de un procedimiento de autentificación.

Preferiblemente puede además realizarse una captación de señales de comprobación de sensores de manipulación asociados al aparato de campo, para vigilar la integridad del aparato de campo.

La elección de una configuración VPN mediante el equipo de comunicación puede incluir en una forma de ejecución preferente la elección de una configuración VPN archivada en una memoria del equipo de comunicación.

Alternativamente puede incluir la elección de una configuración VPN mediante el equipo de comunicación la recepción y memorización de una configuración VPN asociada en un servidor de configuración.

En una forma de ejecución ventajosa se realiza además una autentificación del aparato de campo a través del enlace VPN mediante el servidor VPN.

Según otra forma de ejecución puede vigilarse el estado de servicio del aparato de campo mediante el equipo de comunicación, una vez que se ha establecido el enlace VPN y una desconexión del enlace VPN en el caso de que el aparato de campo ya no esté conectado con el equipo de comunicación o bien esté desactivado.

La presente invención logra, según otra forma de ejecución, un equipo de comunicación para la protección criptográfica de una comunicación de datos de un aparato de campo, con una interfaz de comunicación diseñada para establecer una comunicación local con un aparato de campo conectado a la interfaz de comunicación, un equipo de cálculo, diseñado para identificar el aparato de campo a través de la interfaz de comunicación en base a un código de identificación del aparato de campo y elegir una configuración VPN asociada al aparato de campo identificado y un equipo de red diseñado para establecer un enlace VPN con un servidor VPN en base a la configuración VPN elegida, estando diseñado el enlace VPN para transmitir datos de control del aparato de campo a un servidor VPN.

Otras modificaciones y variaciones resultan de las características de las reivindicaciones dependientes.

Breve descripción de las figuras

A continuación se describirán con más precisión diversas formas de ejecución y configuraciones de la presente invención con referencia a los dibujos adjuntos, en los que muestra la

figura 1 una representación esquemática de un entorno VPN según una forma de ejecución de la invención;
figura 2 una representación esquemática de un procedimiento para la protección criptográfica de una comunicación de datos de un aparato de campo según otra forma de ejecución de la invención; y
figura 3 una representación esquemática de un equipo de comunicación para establecer una VPN según otra forma de ejecución de la invención.

Las mejoras y perfeccionamientos descritos pueden combinarse entre sí de cualquier manera, siempre que ello tenga sentido. Otras posibles mejoras, perfeccionamientos e implementaciones de la invención incluyen también combinaciones no citadas explícitamente de características de la invención descritas antes o a continuación en relación con los ejemplos de ejecución.

Los dibujos adjuntos deben proporcionar una comprensión adicional de las formas de ejecución de la invención. Los mismos visualizan formas de ejecución y sirven en relación con la descripción para clarificar principios y conceptos de la invención. Otras formas de ejecución y muchas de las ventajas citadas resultan en relación con los dibujos. Los elementos de los dibujos no se muestran necesariamente a escala uno respecto a otro. Las mismas referencias designan aquí componentes iguales o que funcionan de igual manera.

Descripción detallada de la invención

La figura 1 muestra una representación esquemática de un entorno VPN 10 según una forma de ejecución de la invención. El entorno VPN 10 incluye un aparato de campo 11. El aparato de campo 11 puede ser por ejemplo un aparato de control para una instalación ferroviaria o de vías férreas, por ejemplo para agujas de control, una barrera o una señal. El aparato de campo 11 puede no obstante ser cualquier otro aparato situado alejado, como por ejemplo una estación meteorológica o un semáforo. Para que el aparato de campo 11 pueda intercambiar con una estación central 17, como por ejemplo un puesto de enclavamiento, mensajes de control y datos de control, existe un equipo de comunicación 12 conectado con el aparato de campo 11 y que comunica a través de una red 15 con una estación interlocutora 16, conectada a su vez con la estación central 17. El equipo de comunicación 12 puede estar constituido como aparato externo o bien estar integrado en el aparato de campo 11.

La transmisión de los datos de control se realiza a través de la red 15, que puede ser una red pública, como por ejemplo Internet, una red de telefonía móvil, como por ejemplo GPRS, UMTS, LTE o WiMAX,

una red inalámbrica como por ejemplo WLAN, una red ethernet, una red token-ring, una red DSL u otra red comparable. Los datos de control que se transmiten a través de la red 15 están sometidos por lo tanto a ataques potenciales. Por ello se ha establecido para la comunicación entre el equipo de comunicación 12 y la estación interlocutora 16 una red privada virtual 15a (VPN), a través de la cual puedan enviarse y recibirse datos con protección criptográfica mediante la codificación correspondiente. Para la codificación puede utilizarse cualquiera de las técnicas de codificación conocidas, como por ejemplo IPsec, IKE, EAP, SSL/TLS, MACsec, L2TP, PPTP, PGP, S/MIME o técnicas similares. La codificación puede estar configurada entonces como un cálculo de una suma de comprobación criptográfica (Message Authentication Code, Digitale Signatur; código de autentificación del mensaje, firma digital) y la decodificación como la comprobación de una suma de comprobación criptográfica.

El equipo de comunicación 12 dispone por lo tanto de una (o varias) claves de comunicación, con las que se codifican criptográficamente los datos de control del aparato de campo 11 a enviar y se decodifican criptográficamente los datos a recibir para el aparato de campo 11. Una clave de comunicación puede utilizarse directamente. Igualmente puede utilizarse la clave de comunicación en un protocolo de acuerdo de autentificación y de claves, como por ejemplo en el protocolo IKE, para establecer una clave de sesión. La clave de sesión establecida puede entonces utilizarse para la transmisión protegida criptográficamente de mensajes de control o datos de control con la estación interlocutora 16.

El entorno VPN 10 incluye además un servidor de configuración 18, que dispone de las llamadas funciones “bootstrapping” (da autoarranque), por ejemplo un servidor de autentificación. El bootstrapping designa una transmisión entre aparatos terminales y servidores previamente desconocidos entre si, que permite la autentificación unilateral o mutua y a raíz de ello el intercambio de claves secretas, con lo que es posible un mayor aprovechamiento de aplicaciones que presuponen una autentificación y una relación de comunicación asegurada. El servidor de configuración 18 dispone de una dirección, por ejemplo de una dirección IP o de una URL, que puede estar fijamente programada o variable mediante ajuste en el equipo de comunicación 12. En una forma de ejecución la dirección del servidor de configuración 18 es una dirección del fabricante del equipo de comunicación 12. En otra forma de ejecución la dirección del servidor de configuración 18 es una dirección del operador del equipo de comunicación 12. No obstante es posible también determinar mediante otra dirección del equipo de comunicación 12 primeramente otra dirección del servidor 19 competente para el correspondiente equipo de comunicación 12 y a continuación construir la otra dirección para establecer un enlace bootstrapping con el servidor de comunicación 18. También puede ser factible consultar un banco de datos para la elección del servidor de configuración 18 perteneciente en cada caso a un equipo de comunicación 12. Además puede ser factible hacer depender la elección de la dirección del correspondiente servidor de configuración 18 de un lugar de estancia físico del aparato de campo 11, por ejemplo de datos de navegación por satélite como datos GPS o GA-LILEO u otras coordenadas espaciales. También puede ser factible que el servidor de configuración 18 competente para la configuración del equipo de comunicación 12 se determine mediante un número de identificación memorizado en el equipo de comunicación 12 y/o en el aparato de campo 11, por ejemplo una dirección MAC. El servidor de configuración 18 puede estar integrado también en la estación interlocutora 16, o también puede ser factible que la estación interlocutora 16 disponga de la correspondiente funcionalidad bootstrapping. En una variante puede estar conectado el servidor de configuración 18 también directamente con el equipo de comunicación 12. Debe quedar claro que es posible una pluralidad de posibilidades adicionales para la asignación de un servidor de configuración 18 para el correspondiente equipo de comunicación 12.

Una configuración VPN incluye por ejemplo informaciones sobre la dirección del servidor de configuración 18, la dirección de la estación interlocutora 16, una clave pública o bien un certificado digital de la estación interlocutora 16, el protocolo VPN a utilizar, una descripción de los ajustes de seguridad, por ejemplo de la clave y del módulo para el correspondiente enlace VPN 15a y/o reglas de filtrado sobre el tráfico de datos admisible. Estas informaciones pueden estar presentes textualmente, por ejemplo como par de valores de atributo o como documento XML. Puede ser también factible establecer varios enlaces VPN 15a para un aparato de campo 11, para realizar por ejemplo distintas clases de tráfico, por ejemplo control, vigilancia, acceso al mantenimiento y funciones similares en enlaces VPN 15a separados.

En una variante pueden incluir la configuración VPN también un número de identificación del aparato de campo 11, por ejemplo una dirección MAC del aparato de campo 11, un número EAN, un número de serie del fabricante o una información de identificación similar. Este número de identificación puede leerse por ejemplo de una placa de características electrónica del aparato de campo 11 mediante RFID o bien mediante una interfaz de comunicación del aparato de campo 11. Por ejemplo puede incluir el aparato de campo 11 una clave de aparato o un certificado digital del aparato, por ejemplo según el estándar ITU-T X.509. En este caso pueden utilizarse del certificado del aparato por ejemplo valores derivados de una función hash o campos individuales o atributos del certificado del aparato como número de identificación del aparato de campo 11.

Además puede estar previsto que cada configuración VPN lleve asociado un código de identificación VPN, que se codifique en una configuración VPN o que pueda derivarse de la misma, por ejemplo utilizando parámetros o campos individuales de la descripción de la configuración o valores derivados de

ello mediante una función hash. El código de identificación VPN puede utilizarse para consultar en el servidor de configuración 18 a qué aparato del campo 11 está asignada la correspondiente configuración VPN. A la configuración VPN puede asociársele mediante un código de identificación VPN un número de identificación de un aparato de campo 11 y darlo a conocer al servidor de configuración 18. Para ello envía el equipo de comunicación 12 un mensaje de registro con el código de identificación VPN y el número de identificación asociado del aparato de campo 11 al servidor de configuración 12 y/o a la estación interlocutora 16.

La figura 2 muestra una representación esquemática de un procedimiento 30 para la protección criptográfica de una comunicación de datos del aparato de campo con ayuda de un equipo de comunicación.

En una primera etapa 31 se realiza la identificación de un aparato de campo conectado al equipo de comunicación. La identificación puede incluir por ejemplo la lectura de un número de identificación asociado al aparato de campo. Preferiblemente puede realizarse a la vez que la identificación del aparato de campo un autentificación del aparato de campo, por ejemplo con ayuda de un procedimiento Challenge-Response (reto-respuesta), en el que los datos de comprobación, el llamado “reto” se transmita mediante el equipo de comunicación al aparato de campo y mediante el aparato de campo se genere a partir del challenge un valor de comprobación, cuya coincidencia con una respuesta esperada, la llamada “Response”, se determine mediante el equipo de comunicación, para poder verificar la autenticidad del aparato de campo. Mediante la autentificación del aparato de campo puede asegurarse ventajosamente que los datos enviados a través de un enlace VPN pueden asociarse inequívocamente a un determinado aparato de campo.

Entonces puede comprobar también el equipo de comunicación si el aparato de campo está conectado directamente, por ejemplo comprobando la conectividad Layer 2 (capa 2) o midiendo el tiempo de recorrido de las señales transmitidas. Así puede evitarse que el equipo de comunicación se aleje de su lugar de utilización propiamente dicho. Además puede comprobar el equipo de comunicación la integridad del aparato de campo. Además puede recibir el equipo de comunicación señales de comprobación de dispositivos del aparato de campo o de una carcasa en la que está colocado el aparato de campo e investigar manipulaciones o intervenciones exteriores indeseadas eventualmente existentes. Las señales de comprobación pueden entonces por ejemplo ser iniciadas por sensores de manipulación en o junto a la carcasa o en el propio aparato de campo.

En una segunda etapa 32 se realiza la elección de una o dado el caso varias configuraciones VPN para establecer uno o dado el caso varios enlaces VPN mediante el equipo de comunicación a través del que el aparato de campo puede intercambiar datos de control con un servidor VPN y/o una estación interlocutora VPN. Al respecto puede utilizarse por ejemplo una configuración VPN memorizada en el equipo de comunicación. El equipo de comunicación puede disponer para ello de una memoria en la que están instaladas previamente o preconfiguradas configuraciones VPN. Las configuraciones VPN memorizadas pueden comprobarse en cuanto a la asociación con el aparato de campo identificado en la etapa 31. Si entonces debe determinarse una configuración VPN asociada al aparato de campo, entonces puede elegirse esta configuración VPN. Entonces puede comprobarse también alternativamente si la configuración VPN elegida sigue siendo válida en ese momento.

Alternativamente puede conectarse en la etapa 32, para elegir una configuración VPN, un servidor de configuración, al que se transmiten los datos de identificación determinados para el aparato de campo. El servidor de configuración puede entonces, en función de los datos de identificación del aparato de campo transmitidos, buscar una configuración VPN en un banco de datos o crearla dinámicamente en especial para el aparato de campo identificado y ponerla a disposición del equipo de comunicación. La comunicación del equipo de comunicación con el servidor de configuración puede entonces realizarse de forma asegurada, autentificándose el equipo de comunicación, mediante una red pública, como por ejemplo Internet o una red de telefonía móvil respecto al servidor de configuración. Esto puede realizarse por ejemplo mediante una clave de comunicación prevista especialmente en el servidor de comunicación, con lo que el equipo de comunicación puede comunicar por ejemplo mediante SSL/TLS o bien IPsec.

El servidor de configuración transmite una configuración VPN asociada al aparato de campo con los correspondientes datos de configuración VPN al equipo de comunicación. El equipo de comunicación puede memorizar esta configuración VPN y asociarla internamente al aparato de campo identificado.

En una tercera etapa 33 se establece un enlace VPN con un servidor VPN a través de una red, como por ejemplo Internet, una red de telefonía móvil o una red similar. El enlace VPN se establece entonces mediante el equipo de comunicación según la configuración VPN elegida. Entonces pueden establecerse por ejemplo también varios enlaces VPN según diversas configuraciones VPN para el mismo aparato de campo. Mediante el enlace VPN establecido puede realizarse por ejemplo una identificación y/o autentificación del aparato de campo mediante el servidor VPN. Cuando entonces coincide la identificación del aparato de campo con el aparato de campo asociado a esta configuración VPN, puede liberarse el enlace VPN por parte del servidor VPN.

En una cuarta etapa 34 se realiza la transmisión de datos de control del aparato de campo al servidor VPN a través del enlace VPN establecido mediante el equipo de comunicación para el aparato de campo. A la vez pueden transmitirse datos de control desde el servidor VPN a través del enlace VPN al aparato de campo. Entonces se transmiten los datos de control en cada caso mediante el equipo de comunicación que mantiene el enlace VPN. El equipo de comunicación puede estar para ello diseñado para mantener el enlace VPN mientras el aparato de campo permanezca conectado con el equipo de comunicación. Para ello puede realizar el equipo de comunicación preferiblemente de forma periódica una comprobación de la conexión local con el aparato de campo. Tan pronto como el aparato de campo ya no está conectado o está desactivado, puede desconectar o desactivar el equipo de comunicación el enlace VPN.

El servidor VPN puede realizar mediante la configuración VPN una asociación inequívoca con un aparato de campo. Para ello puede el mismo ajustar la configuración VPN con una lista predeterminada o bien puede bajarse los datos de configuración VPN del servidor de configuración. El servidor VPN puede realizar durante la comunicación con el aparato de campo a través del enlace VPN un infiltrado del tráfico de datos tal que sólo se retransmitan al aparato de campo paquetes de datos que pueden asociarse inequívocamente a un ordenador de control, como por ejemplo un puesto de enclavamiento. Para ello pueden evaluarse informaciones de identificación contenidas en los paquetes de datos, por ejemplo direcciones MAC, direcciones IP, nombres DNS, SPI-URI (Session Initiation Protocol Uniform Ressource Identifier, identificador uniforme de recursos para protocolo de iniciación de sesión) o informaciones similares.

El equipo de comunicación puede establecer también en una forma de ejecución enlaces VPN para varios aparatos de campo, pudiendo establecerse bien un enlace VPN para cada uno de los aparatos de campo o bien formando los aparatos de campo un grupo de aparatos de campo que pueden comunicar mediante un enlace VPN asociado al grupo de aparatos de campo. Entonces funcionan todos los aparatos de campo del grupo de aparatos de campo frente al equipo de comunicación y/o el servidor VPN como un aparato de campo (virtual).

La figura 3 muestra una representación esquemática de un equipo de comunicación 12 con un equipo de cálculo 21, una interfaz de comunicación 22, una memoria 23 y un equipo de red 24.

El equipo de comunicación 12 puede comunicar mediante la interfaz de comunicación 22 con un aparato de campo 11. En particular puede realizar el equipo de comunicación 12 mediante la interfaz de comunicación 22 una identificación y dado el caso una autentificación del aparato de campo 11. En la memoria 23 pueden instalarse previamente configuraciones VPN y/o memorizarse configuraciones VPN recibidas de un servidor de configuración. La memoria 23 puede incluir por ejemplo una zona de memoria 23a asegurada, en la que están archivados datos de configuración o bien claves de comunicación para una comunicación asegurada del equipo de comunicación 12 con un servidor de comunicación. La memoria 23 puede ser por ejemplo un módulo de memoria en el que de manera duradera y reescribible pueden archivarse ajustes de configuración del equipo de comunicación 12, por ejemplo una EEPROM serie, una memoria flash o un equipo de memoria comparable.

El equipo de cálculo 21 puede estar diseñado para recibir señales de comprobación de sensores de manipulación 11b, que pueden estar dispuestos en el aparato de campo 11 o en una carcasa 11a en la que puede estar dispuesto el aparato de campo 11. El sensor 11b puede ser por ejemplo un sensor "tamper", es decir, un sensor que puede detectar una manipulación física en el aparato de campo 11, en partes del aparato de campo 11 o en la carcasa 11a. El equipo de cálculo 21 puede realizar además la identificación y autentificación del aparato de campo 11, así como establecer y vigilar un enlace VPN 15a con un servidor VPN en función de una configuración VPN elegida para el aparato de campo 11.

El equipo de comunicación 12 incluye un equipo de red 24, mediante el que puede establecerse un enlace VPN 15a con un servidor VPN. Entonces puede establecerse el enlace VPN 15a por ejemplo a través de Internet, una red de telefonía móvil como por ejemplo GPRS, UMTS, LTE o WiMAX, una red inalámbrica, como por ejemplo WLAN, una red Ethernet, una red Token-Ring u otra red comparable.

REIVINDICACIONES

1. Procedimiento (30) para la protección criptográfica de una comunicación de datos de un aparato de campo (11), con las etapas:
identificación del aparato de campo (11) mediante un equipo de comunicación (12) sobre la base de un código de identificación del aparato de campo (11); elección de una configuración VPN asociada al aparato de campo (11) identificado mediante el equipo de comunicación (12);
establecimiento de un enlace de VPN (15a) sobre la base de la configuración VPN elegida mediante el equipo de comunicación (12); y transmisión de datos de control a través del aparato de campo (11) a un servidor VPN (16) a través del enlace VPN establecido.

2. Procedimiento (30) según la reivindicación 1, además con la etapa:
autentificación del aparato de campo (11) mediante el equipo de comunicación (12) por medio de un procedimiento de autentificación.

3. Procedimiento (30) según una de las reivindicaciones 1 y 2, además con la etapa:
captación de señales de comprobación de sensores de manipulación asociados al aparato de campo (11), para vigilar la integridad del aparato de campo.

4. Procedimiento (30) según una de las reivindicaciones 1 a 3,
en el que la elección de una configuración VPN mediante el equipo de comunicación (12) incluye la elección de una configuración VPN archivada en una memoria (23) del equipo de comunicación (12).

5. Procedimiento (30) según una de las reivindicaciones 1 a 3,
en el que la elección de una configuración VPN mediante el equipo de comunicación (12) incluye la recepción y memorización de una configuración VPN asociada en un servidor de configuración (18).

6. Procedimiento (30) según una de las reivindicaciones 1 a 5, además con la etapa:
autentificación del aparato de campo (11) a través del enlace VPN (15a) mediante el servidor VPN (16).

7. Procedimiento según una de las reivindicaciones 1 a 6, además con la etapa:
vigilancia del estado de servicio del aparato de campo (11) mediante el equipo de comunicación (12), una vez que se ha establecido el enlace VPN (15a); y
desconexión del enlace VPN (15a) en el caso de que el aparato de campo (11) ya no esté conectado con el equipo de comunicación (12) o bien esté desactivado.

8. Equipo de comunicación (12) para la protección criptográfica de una comunicación de datos de un aparato de campo (11), con:
una interfaz de comunicación (22) diseñada para establecer una comunicación local con un aparato de campo (11) conectado a la interfaz de comunicación (22);
un equipo de cálculo (21), diseñado para identificar el aparato de campo (11) a través de la interfaz de comunicación (22) en base a un código de identificación del aparato de campo (11), y para elegir una configuración VPN asociada al aparato de campo identificado; y
un equipo de red (24), diseñado para establecer un enlace VPN (15a) con un servidor VPN (16) en base a la configuración VPN elegida, estando diseñado el enlace VPN (15a) para transmitir datos de control del aparato de campo (11) al servidor VPN (16).

9. Equipo de comunicación (12) según la reivindicación 8,
en el que el equipo de cálculo (21) está diseñado además para autentificar el aparato de campo (11) mediante un procedimiento de autentificación.

10. Equipo de comunicación (12) según una de las reivindicaciones 8 y 9,
en el que el equipo de cálculo (21) está diseñado además para recibir señales de comprobación de sensores de manipulación (11b) asociados al aparato de campo (11) para vigilar la integridad del aparato de campo (11).

11. Equipo de comunicación (12) según una de las reivindicaciones 8 a 10, además con:
una memoria (23) en la que está archivada una pluralidad de configuraciones VPN, de entre las cuales el equipo de cálculo (21) elige una configuración VPN.

12. Equipo de comunicación (12) según una de las reivindicaciones 8 a 10,
en el que el equipo de cálculo (21) está diseñado además para recibir una configuración VPN asociada al aparato de campo (11) de un servidor de configuración (18) a través del equipo de red (24).

13. Equipo de comunicación (12) según una de las reivindicaciones 8 a 12,

en el que el equipo de cálculo (21) está diseñado además para vigilar el estado de servicio del aparato de campo (11) y desconectar un enlace VPN (15a) establecido cuando el aparato de campo (11) ya no está conectado con el equipo de comunicación (12) o está desactivado.

FIG 1

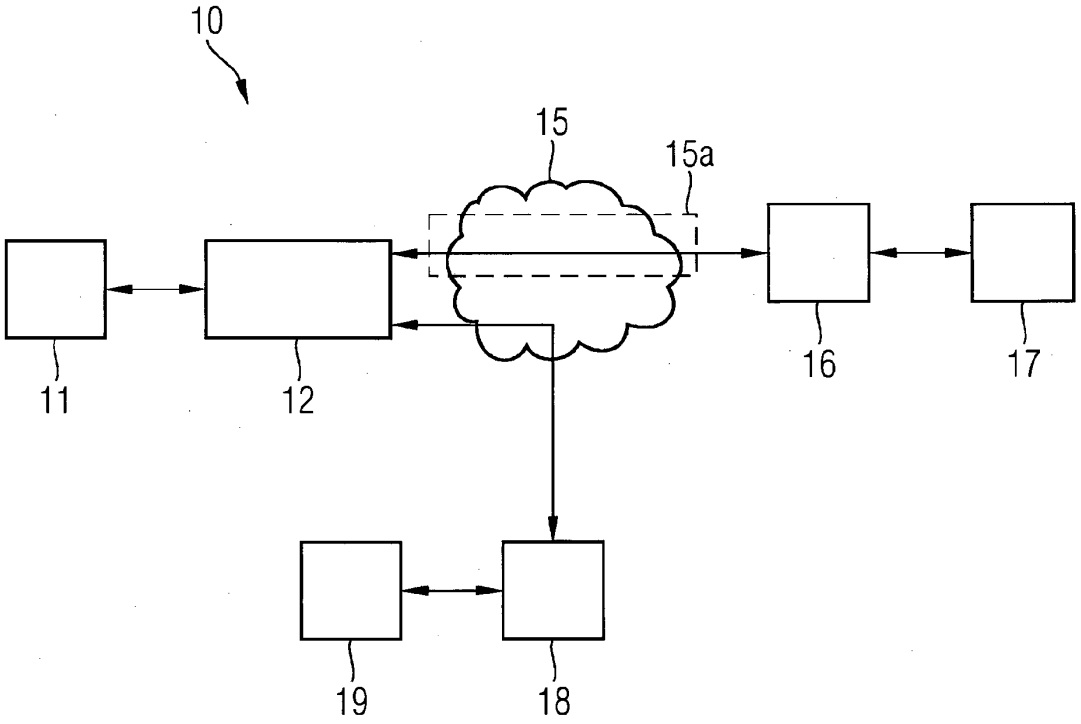

FIG 2

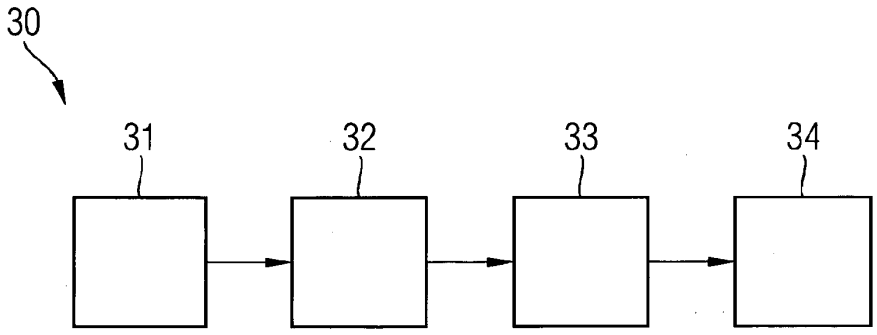

FIG 3