(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 674 923**

(51) Int. CI.:

G05B 19/042 (2006.01)
G06F 21/86 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **11.04.2012 PCT/EP2012/056517**

(87) Fecha y número de publicación internacional: **26.10.2012 WO12143271**

(96) Fecha de presentación y número de la solicitud europea: **11.04.2012 E 12717242 (7)**

(97) Fecha y número de publicación de la concesión europea: **04.04.2018 EP 2668607**

(54) Título: **Procedimiento para vigilar una protección antimanipulación así como sistema de vigilancia para un aparato de campo con protección antimanipulación**

(30) Prioridad:

18.04.2011 DE 102011007572

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.07.2018

(73) Titular/es:

SIEMENS AKTIENGESELLSCHAFT (100.0%)
Werner-von-Siemens-Strasse 1
80333 München, DE

(72) Inventor/es:

FALK, RAINER y
FRIES, STEFFEN

(74) Agente/Representante:

LOZANO GANDIA, José

PROCEDIMIENTO PARA VIGILAR UNA PROTECCIÓN ANTIMANIPULACIÓN ASÍ COMO SISTEMA DE VIGILANCIA PARA UN APARATO DE CAMPO CON PROTECCIÓN ANTIMANIPULACIÓN

DESCRIPCIÓN

La invención se refiere a un procedimiento para vigilar una protección antimanipulación, a un sistema de vigilancia para un aparato de campo con protección antimanipulación y a una utilización de un sistema de vigilancia.

Los aparatos de campo, por ejemplo en forma de instalaciones de señales de tráfico para regular el tráfico, instalaciones de señalización para trenes, sistemas de agujas, etc., están conectados usualmente con un centro de control o un puesto de enclavamientos para accionar y vigilar los mismos. La comunicación entre aparato de campo y centro de control puede realizarse entonces tanto mediante línea física, por medio de cables correspondientemente tendidos, como también inalámbricamente, mediante un enlace por radio.

Para poder detectar entonces una manipulación física en un aparato de campo por parte de un posible atacante, pueden disponerse los correspondientes sensores, por ejemplo sensores de movimiento. Para dificultar una manipulación de circuitos electrónicos en el propio aparato de campo, se conocen ya además circuitos integrados de seguridad de hardware (hardware-security) que memorizan claves criptográficas y pueden realizar operaciones criptográficas. Tales circuitos integrados disponen usualmente de una protección antimanipulación, por ejemplo en forma de sensores directamente situados sobre el circuito integrado. Éstos están configurados para detectar una apertura no autorizada del circuito integrado.

Un tal circuito integrado hardware-security se conoce ya por ejemplo como "Trusted Platform Module“ (módulo de plataforma de confianza), cuyos datos pueden bajarse en la dirección http.//de.wikipedia.org/wiki/trusted_platform_module. Tales circuitos integrados se alojan por ejemplo en PCs o notebooks.

Finalmente se conoce ya por el sector de las instalaciones de aviso de intrusión e instalaciones de alarmas para edificios la utilización de contactos en puertas y ventanas y/o detectores de movimiento, para señalizar una intrusión o una apertura no autorizada o penetración en el edificio o en una sala. En el caso de una intrusión en un edificio, se dispara por ejemplo una alarma mediante una sirena o similar y también es posible tomar contacto a la vez con una central de operaciones de la policía. Los propios sensores utilizados en instalaciones de aviso de intrusión o en instalaciones de alarmas pueden estar dotados por sí mismos de los llamados sensores antimanipulación, para proteger la instalación de alarmas frente a manipulaciones, detectando los mismos una manipulación de la instalación de aviso de intrusión o de la instalación de alarmas, en particular cuando se abre su carcasa y/o se desmonta un sensor. Los sensores antimanipulación transmiten entonces la información a la instalación de alarmas, que a su vez dispara una alarma.

Para proteger partes de una placa de circuitos o una placa de circuitos completa frente a una manipulación, se conoce ya además la práctica de atornillar sobre la placa de circuitos placas metálicas, tal que en conjunto se forme un condensador. La capacidad del mismo se vigila entonces continuamente, con lo que cuando existe una desviación respecto al valor usual de la capacidad, por ejemplo al tocar la placa metálica o al retirarla, resulta una variación de la capacidad. Cuando se detecta una variación de la capacidad, puede dispararse una alarma y borrarse una memoria de la placa de circuitos, que por ejemplo contiene datos sensibles, con lo que un atacante no consigue acceso alguno a los datos sensibles.

Por el documento WO 2004/078787 A1 del 16 de septiembre de 2004 se conoce un procedimiento en el que el objeto a transportar está rodeado por un embalaje seguro frente a la manipulación, que registra con firma sucesos relevantes en cuanto a la manipulación (tamper) durante el transporte y con ello atestigua al receptor mediante un certificado que el objeto transportado ha sido correctamente tratado. Un objetivo de la presente invención es proporcionar un procedimiento para vigilar una protección antimanipulación de un aparato de campo y un sistema de vigilancia para un aparato de campo con protección antimanipulación, en el cual sea posible una protección antimanipulación de manera sencilla y económica. A la vez deben poder reequiparse con las mismas de manera flexible una pluralidad de aparatos distintos y ser adaptables y proporcionar un nivel de seguridad deseado frente a manipulación física.

Este objetivo se logra mediante un procedimiento para vigilar una protección antimanipulación de un aparato de campo, que incluye las etapas de comprobación de si se ha realizado una manipulación en el aparato de campo, emisión de un certificado de no-manipulación, si el resultado obtenido de la comprobación es negativo, transmisión del certificado de no-manipulación, comprobación del certificado de no-manipulación mediante un equipo registrador, determinación de un estado activo del aparato de campo mediante el equipo registrador, si el certificado de no-manipulación es válido, comprobación del aparato de campo mediante un equipo de vigilancia mediante consulta del estado del aparato de campo y

transmisión de datos del aparato de campo al equipo de vigilancia, aceptación de los datos del aparato de campo mediante el equipo de vigilancia, si el aparato de campo se encuentra en un estado activo.

Este objetivo se logra igualmente mediante un sistema de vigilancia para un aparato de campo con protección antimanipulación, en particular adecuado para realizar un procedimiento de acuerdo con al menos una de las reivindicaciones 1-5, que incluye un equipo de vigilancia de manipulación, que está configurado para vigilar el aparato de campo para la protección antimanipulación, un equipo registrador para registrar y vigilar el estado del aparato de campo, un equipo de vigilancia para controlar y vigilar el aparato de campo, estando configurado el equipo de vigilancia de manipulación para comprobar si se ha realizado una manipulación en el aparato de campo y emite un certificado de no-manipulación si se ha detectado un resultado de la comprobación negativo y estando configurado el equipo registrador para comprobar el certificado de no-manipulación y determinar un estado activo del aparato de campo cuando el certificado de no-manipulación es válido y estando configurado el equipo de vigilancia para comprobar un estado del aparato de campo y estando configurado el equipo de vigilancia para aceptar datos del aparato de campo en el caso de que se dé un estado activo del aparato de campo.

Este objetivo se logra igualmente utilizando un sistema de vigilancia según al menos una de las reivindicaciones 6 - 10 para vigilar una instalación de tráfico o para vigilar una estación transformadora.

Una ventaja que con ello se logra es que una protección antimanipulación puede incorporarse posteriormente de manera sencilla y sin un gasto importante, en particular también en aparatos de campo ya existentes. Una ventaja adicional es que los aparatos de campo a vigilar pueden desarrollarse y fabricarse sin que tengan que tenerse en cuenta medidas de protección antimanipulación configuradas especialmente en el propio aparato de campo. Mediante el procedimiento para vigilar la protección antimanipulación se bloquea también solamente el aparato de campo y/o una clave de seguridad archivada en el aparato de campo, con lo que cuando eventualmente se lean datos desde una memoria del aparato de campo, en particular la clave de seguridad elegida, por parte de un atacante, no aportan a éste utilidad alguna. Una ventaja adicional es que una tal vigilancia de una protección antimanipulación puede utilizarse para muchas clases distintas de aparatos de campo, lo cual reduce considerablemente los costes de fabricación de los correspondientes aparatos de campo. La protección antimanipulación debe desarrollarse sólo una vez y no separadamente para cada tipo de aparatos de campo. Además no se necesita una comunicación directa entre el equipo de vigilancia de manipulación y el aparato de campo. También esto ahorra costes de fabricación.

Otros perfeccionamientos ventajosos de la invención se describen en las reivindicaciones secundarias.

Convenientemente se realiza la transmisión del certificado de no-manipulación al equipo registrador mediante el aparato de campo. De esta manera no se necesita ninguna interfaz adicional para transmitir el certificado de no-manipulación, sino que pueden utilizarse canales de comunicación o líneas de comunicación ya existentes para el aparato de campo. En particular se reduce por lo tanto el coste de fabricación de un equipo de vigilancia de manipulación para el aparato de campo.

Ventajosamente se realiza la transmisión del certificado de no-manipulación esencialmente a la vez que la transmisión de los datos del aparato de campo, transmitiéndose en particular el certificado de no-manipulación y los datos del aparato de campo a un equipo de control común que incluye el equipo registrador y el equipo de vigilancia. La ventaja que con ello se logra es que así puede comprobarse de manera especialmente rápida y fiable si ha tenido lugar una manipulación física del aparato de campo.

Convenientemente se realiza la transmisión del certificado de no-manipulación mediante Internet y/o mediante al menos una red de telefonía móvil y/o mediante al menos una red por satélite. La ventaja que con ello se logra es que así, de manera sencilla, en particular cuando se utilizan varias clases de transmisión en paralelo, queda garantizada una transmisión lo más fiable posible. A la vez pueden utilizarse vías de transmisión usuales, que son económicas, ya que los equipos necesarios para la transmisión están disponibles en grandes cantidades.

Convenientemente se realizan al menos las etapas de comprobar si se ha realizado una manipulación en el aparato de campo, emitir un certificado de no-manipulación, si el resultado de la comprobación es negativo y transmitir el certificado de no-manipulación, a intervalos de tiempo regulares. La ventaja es entonces que con ello se determina así de manera fiable, cuando no existe la transmisión del certificado de no-manipulación, el estado del correspondiente aparato de campo como inactivo.

Ventajosamente está dispuesto en el sistema de vigilancia un equipo de control, que incluye el equipo registrador y el equipo de vigilancia. La ventaja que con ello se logra es que de esta manera no tiene que tenderse ninguna interfaz externa adicional o cable o similar para comprobar el certificado de no-manipulación. A la vez pueden transmitirse datos del aparato de campo y el certificado de no-manipulación por los canales de comunicación ya existentes entre aparato de campo y equipo de vigilancia, lo cual simplifica considerablemente el manejo, control y vigilancia del aparato de campo.

Convenientemente el equipo de control está configurado en forma de un puesto de control SCADA o de un sistema ERP. La ventaja que con ello se logra es que de esta manera se proporciona de manera sencilla y fiable un equipo de control. Además está configurado un tal equipo de control no sólo para vigilar una protección antimanipulación de un aparato de campo, sino que puede también realizar tareas adicionales como por ejemplo una visualización, una regulación o similares de otros sistemas o equipos.

Convenientemente incluye al menos uno de los equipos una interfaz de comunicación hacia Internet, hacia una red de telefonía móvil y/o hacia una red por satélite. La ventaja que con ello se logra es que así, en particular cuando se utilizan varias redes de transmisión en paralelo, queda garantizada una transmisión lo más fiable posible. A la vez pueden utilizarse vías de transmisión ya existentes, que son económicas, ya que los equipos necesarios para la transmisión se encuentran disponibles fácilmente.

Ventajosamente presenta el equipo de vigilancia de manipulación una fuente de energía autónoma. De esta manera se reduce una manipulación física del propio equipo de vigilancia de manipulación. A la vez aumenta la seguridad frente a fallos del equipo de vigilancia de manipulación, ya que no se necesita una fuente de energía externa y de esta manera cuando hay un fallo de la corriente el equipo de vigilancia de manipulación sigue vigilando a pesar de ello el aparato de campo.

Otras características y ventajas de la invención resultan de la siguiente descripción de ejemplos de realización en base al dibujo.

Al respecto muestra de forma esquemática la

figura 1 un sistema de vigilancia para un aparato de campo con protección antimanipulación según una primera forma de realización de la presente invención;
figura 2 un sistema de vigilancia para un aparato de campo con protección antimanipulación según una segunda forma de realización de la presente invención;
figura 3 un sistema de vigilancia para un aparato de campo con protección antimanipulación según una tercera forma de realización de la presente invención;
figuras 4a,4b equipos de vigilancia de manipulación según una primera y segunda formas de realización;
figura 5 un procedimiento para vigilar una protección antimanipulación de un aparato de campo según una primera forma de realización de la presente invención.

La figura 1 muestra un sistema de vigilancia para un aparato de campo con protección antimanipulación según una primera forma de realización de la presente invención.

En la figura 1 designa la referencia 1 un aparato de campo. El aparato de campo 1 está conectado con un equipo de vigilancia de manipulación 2, que está configurado para vigilar el aparato de campo 1 en cuanto a si el aparato de campo 1 se manipula físicamente. El aparato de campo 1 está conectado además con un equipo registrador 3 para registrar y vigilar el estado del aparato de campo 1. El equipo registrador 3 intercambia a su vez datos con un equipo de vigilancia 4 para controlar y vigilar el aparato de campo 1. El equipo de vigilancia 4 está conectado según la figura 1 a través de Internet 20 con el aparato de campo 1.

El equipo de vigilancia de manipulación 2 expide, si no se ha detectado ninguna manipulación física ni un suceso de manipulación, un certificado de no-manipulación o una aserción de no-manipulación (Non-Tampering-Assertion) NTA y transmite (referencia 10) el mismo al aparato de campo 1 protegido mediante el equipo de vigilancia de manipulación 2. La aserción de no-manipulación se transmite a continuación (referencia 11) por ejemplo a un equipo registrador 3 configurado en forma de un Device-Registry-Server (servidor de registro del aparato). Éste bloquea el aparato de campo 1, cuya característica de seguridad o cuyas Security Credentials (credenciales de seguridad), existentes por ejemplo en forma de certificados, claves, palabras de paso o cuentas del aparato de campo, en el caso de que durante un determinado espacio de tiempo no exista en el Device-Registry-Server 3 ninguna aserción de no-manipulación expedida por el equipo de vigilancia de manipulación 2 asociado al aparato de campo 1 ni se transmita al mismo. Entonces se determina que el estado del aparato de campo 1 es inactivo.

Si existe una aserción de no-manipulación válida, se memoriza el estado del aparato de campo 1 como activo en el equipo registrador 3. Ya durante ello y/o a continuación transmite el aparato de campo 1 (referencia 12) datos del aparato de campo, por ejemplo datos de control o datos de acuse de recibo del aparato de campo 1 al equipo de vigilancia 4. El equipo de vigilancia 4 puede estar configurado por ejemplo como ordenador de control, como control programable en memoria, como puesto de control SCADA, como sistema ERP o similares. El equipo de vigilancia 4 comprueba ahora en otra etapa (referencia 13) si el estado del aparato de campo 1 es activo. Para ello consulta el equipo de vigilancia 4 el estado del aparato de campo 1 en el equipo registrador 3. El equipo registrador 3 transmite (referencia 14) el estado al equipo de vigilancia 4. Si el estado del aparato de campo 1 es válido, acepta el equipo de vigilancia 4 los datos del aparato de campo transmitidos desde el aparato de campo 1 al equipo de vigilancia 4 y puede transmitir datos de control para el aparato de campo (referencia 15).

Si ha realizado por ejemplo un atacante una manipulación física en el aparato de campo 1, el equipo de vigilancia de manipulación 2 detecta esto. El equipo de vigilancia de manipulación 2 no expide a continuación ninguna otra aserción de no-manipulación y por lo tanto tampoco se transmite ninguna aserción de no-manipulación al aparato de campo 1. Entonces si no recibe el equipo registrador 3 ninguna aserción de no-manipulación del aparato de campo 1, se memoriza como inactivo el estado del aparato de campo 1 en el equipo registrador 3 tras un espacio de tiempo que puede predeterminarse. Incluso cuando con ello lograse un atacante leer claves para encriptar del propio aparato de campo 1 mediante una manipulación física, no puede utilizar el mismo estas claves para acceder al equipo de vigilancia 4, ya que el equipo de vigilancia 4 reconoce o ha reconocido previamente, consultando en el equipo registrador 3, el estado del aparato de campo 1 como inactivo y con ello no acepta ya del aparato de campo 1 ningún dato del aparato de campo y tampoco se transmite ningún dato de control al aparato de campo 1.

La figura 2 muestra un sistema de vigilancia para un aparato de campo con protección antimanipulación según una segunda forma de realización de la presente invención.

Esencialmente muestra la figura 2 un sistema de vigilancia de acuerdo con la figura 1. A diferencia de la figura 1, están reunidos el equipo registrador 3 y el equipo de vigilancia 4 para el aparato de campo 1 en un equipo de control 34. Si ha recibido el aparato de campo 1 una aserción de no-manipulación del equipo de vigilancia de manipulación 2, transmite el aparato de campo 1 tanto datos del aparato de campo como también la aserción de no-manipulación a través de Internet 20 al equipo de control 34. El equipo de control 34 comprueba primeramente la aserción de no-manipulación que ha transmitido el aparato de campo 1. Si la misma es válida, acepta también el equipo de control 34 los datos del aparato de campo transmitidos.

La figura 3 muestra un sistema de vigilancia para un aparato de campo con protección antimanipulación según una tercera forma de realización de la presente invención.

La figura 3 muestra esencialmente un sistema de vigilancia según la figura 1. A diferencia del sistema de vigilancia de la figura 1 no transmite el equipo de vigilancia de manipulación 2, cuando el mismo ha detectado una manipulación física en el aparato de campo, la aserción de no-manipulación, al aparato de campo 1, sino directamente al equipo registrador 3, a través de Internet 20, como se muestra en la figura 3. Pero es igualmente posible transmitir la aserción de no-manipulación a través de WLAN, según las figuras 1-5, por medio de una red de telefonía móvil, en particular GSM, UMTS, LTE, Wimax, CDMA o similares. La ventaja que así se logra es que con ello no tiene que modificarse el aparato de campo, sino que puede comunicar el equipo de vigilancia de manipulación 2 independientemente del aparato de campo 1 con el equipo registrador 3, con lo que en el aparato de campo 1 no tiene que proporcionarse ninguna interfaz para la comunicación con el equipo de vigilancia de manipulación 2.

Las figuras 4a, 4b muestran equipos de vigilancia de manipulación según un primer y un segundo ejemplos de realización.

En las figuras 4a y 4b designa la referencia 2 respectivos equipos de vigilancia de manipulación. El correspondiente equipo de vigilancia de manipulación 2 incluye entonces un ordenador de control 100, que está conectado con una memoria flash 101 y una memoria RAM 102. La memoria flash 101 sirve como memoria de configuración para el equipo de vigilancia de manipulación, mientras que la memoria RAM 102 sirve como memoria de trabajo para el ordenador de control 100. Además está dispuesta una fuente de alimentación 103, que con preferencia está configurada tal que por ejemplo la fuente de alimentación 103 está configurada tamponada o como Supercap (supercondensador) o la misma puede proporcionar energía mediante Energy-Harvesting (cosecha o recuperación de energía), para poder aprovechar por ejemplo en fallos de la corriente la temperatura ambiente, oscilaciones o vibraciones del aire y hacer posible así una vigilancia continua de un aparato de campo 1. Otra ventaja adicional al respecto es que también puede operar el correspondiente equipo de vigilancia de manipulación 2 fiablemente sin una fuente de alimentación externa. El correspondiente equipo de vigilancia de manipulación 2 incluye en cada caso un equipo de entrada/salida 104, que está conectado con sensores 104a para la vigilancia de manipulación. Los sensores 104a están dispuestos en particular fuera de la carcasa del correspondiente equipo de vigilancia de manipulación 2. El correspondiente equipo de vigilancia de manipulación 2, al estar configurado para la tarea especial de la vigilancia de manipulación del aparato de campo 1, puede optimizarse en cuanto a su consumo de energía. El ordenador de control 100 puede encontrarse entonces por ejemplo durante la mayoría del tiempo en un llamado modo de reposo. Si se detecta un evento de manipulación mediante el equipo de vigilancia de manipulación 2, se activa de nuevo el ordenador de control 100.

El equipo de vigilancia de manipulación 2 vigila mediante sensores 104a si tiene lugar una manipulación, es decir, una manipulación física del aparato de campo 1. Los sensores pueden estar configurados entonces por ejemplo como sensores de movimiento, sensores de luz, contactos, mallas de alambre o similares. Mientras no detecta el equipo de vigilancia de manipulación 2 ninguna manipulación física, expide el equipo de vigilancia de manipulación una aserción de no-manipulación. La aserción de no-

manipulación puede estar configurada entonces por ejemplo como estructura de datos, que contiene un número de identificación del equipo de vigilancia de manipulación 2 y una indicación de tiempo y/o un valor numérico. La estructura de datos puede entonces codificarse y estar dotada de una suma de prueba criptográfica, por ejemplo en forma de una firma digital o de un Message Authentication Code. La suma de prueba criptográfica puede calcularse mediante una clave criptográfica memorizada en el equipo de vigilancia de manipulación 2 y proporcionarse mediante la interfaz 105. La interfaz 105 está configurada en la figura 4a con línea física y por el contrario en la figura 4b está configurada la misma inalámbrica.

Una aserción de no-manipulación puede contener entonces también al menos una de las siguientes informaciones: Una información de identificación del equipo de vigilancia de manipulación 2, adicionalmente informaciones relativas al aparato de campo 1 que se vigila mediante el equipo de vigilancia de manipulación 2, un estado del aparato de campo 1, una información sobre una manipulación física, por ejemplo una indicación relativa a una apertura de la carcasa a una temperatura cuando la diferencia de temperaturas es demasiado alta o similares y además una información de tiempo y/o una firma para la autentificación y aseguramiento de la integridad.

La figura 5 muestra un procedimiento para vigilar una protección antimanipulación de un aparato de campo según una primera forma de realización de la presente invención.

En la figura 5 designa la referencia S1 la etapa de comprobación de si se ha realizado una manipulación en el aparato de campo 1, la referencia S2 la etapa de emisión de un certificado de no-manipulación, si el resultado de la comprobación ha sido negativo, la referencia S3 la etapa de transmisión del certificado de no-manipulación, la referencia S4 la etapa de comprobación del certificado de no-manipulación mediante un equipo registrador, la referencia S5 la etapa de determinación mediante el equipo registrador 3 de que el aparato de campo se encuentra en un estado activo si el certificado de no-manipulación es válido, la referencia S6 la etapa de comprobación del aparato de campo 1 mediante un equipo de vigilancia 4, mediante transmisión del estado del aparato de campo 1 y la referencia S7 la etapa de transmisión de datos del aparato de campo al equipo de vigilancia 4, así como la referencia S8 la etapa de aceptación de los datos del aparato de campo por parte del equipo de vigilancia 4 como un estado activo, si el aparato de campo 1 se encuentra en un estado activo.

Aún cuando la presente invención se ha descrito antes en base a ejemplos de realización preferidos, la misma no queda limitada a ello, sino que puede modificarse de manera diversa.

El equipo de vigilancia de manipulación puede está realizado por ejemplo como aparato separado, que está dispuesto en el aparato de campo a vigilar o en una pluralidad de aparatos de campo a vigilar. El equipo de vigilancia de manipulación puede estar realizado entonces como la llamada unidad intermedia, es decir estar fijado entre el aparato de campo a vigilar y una configuración fija, por ejemplo una pared, una barra o similar. El equipo de vigilancia de manipulación puede estar realizado en una carcasa separada adicional, por ejemplo para una placa de circuitos. Es igualmente posible alojar o integrar el equipo de vigilancia de manipulación y los sensores dado el caso existentes para un equipo de vigilancia antimanipulación en el propio aparato de campo a vigilar.

Bajo certificado de no-manipulación ha de entenderse en la descripción y en particular en las reivindicaciones no sólo esencialmente un mensaje de confirmación de no-manipulación o una aserción de no-manipulación, sino igualmente también un mensaje que indica que se ha realizado una manipulación física en el aparato de campo a vigilar. Si se detecta una manipulación física, puede expedirse entonces un certificado de manipulación, si el resultado determinado en la comprobación era positivo. Para poder procesar el mismo en el sentido de la invención, en particular tal como se expone en las reivindicaciones y en las descripciones de las figuras, pueden estar configurados correspondientemente el aparato de campo, el equipo de vigilancia y el equipo registrador.

El equipo registrador puede estar configurado además tal que el mismo esté conectado con una entidad certificadora. La entidad certificadora puede proporcionar entonces al equipo registrador una lista de revocación de certificados o Certificate Revocation List, en la que consta un certificado del aparato de campo correspondiente al aparato de campo vigilado por el equipo de vigilancia antimanipulación. Alternativamente puede proporcionar el certificado del aparato de campo un respondedor de protocolo de comprobación del estado de un certificado en línea (Online Certificate Status Protocol). Esto hace posible una transmisión online de la lista de revocación de certificados.

REIVINDICACIONES

1. Procedimiento para vigilar una protección antimanipulación de un aparato de campo (1) que incluye las etapas:
comprobación (S1) mediante un equipo de vigilancia de manipulación (2) de si se ha realizado una manipulación en el aparato de campo (1),
emisión (S2) de un certificado de no-manipulación mediante un equipo de vigilancia de manipulación (2), si el resultado obtenido de la comprobación es negativo,
transmisión (S3) del certificado de no-manipulación,
comprobación (S4) del certificado de no-manipulación mediante un equipo registrador (3),
determinación (S5) de un estado activo del aparato de campo (1) mediante el equipo registrador (3), si el certificado de no-manipulación es válido,
comprobación (S6) del aparato de campo (1) mediante un equipo de vigilancia (4) mediante consulta del estado del aparato de campo (1) y
transmisión (S7) de datos del aparato de campo al equipo de vigilancia (4),
aceptación (S8) de los datos del aparato de campo mediante el equipo de vigilancia (4), si el aparato de campo (1) se encuentra en un estado de activo.

2. Procedimiento de acuerdo con la reivindicación 1,
caracterizado porque la transmisión (S3) del certificado de no-manipulación al equipo registrador (3) se realiza mediante el aparato de campo (1).

3. Procedimiento de acuerdo con al menos una de las reivindicaciones 1-2,
caracterizado porque la transmisión del certificado de no-manipulación se realiza esencialmente a la vez que la transmisión de los datos del aparato de campo, transmitiéndose en particular el certificado de no-manipulación y los datos del aparato de campo a un equipo de control común que incluye el equipo registrador (3) y el equipo de vigilancia (4).

4. Procedimiento de acuerdo con al menos una de las reivindicaciones 1-3,
caracterizado porque la transmisión (S3) se realiza mediante Internet (20) y/o mediante al menos una red de telefonía móvil y/o mediante al menos una red por satélite.

5. Procedimiento de acuerdo con al menos una de las reivindicaciones 1-4,
caracterizado porque al menos las etapas de comprobar (S1) si se ha realizado una manipulación en el aparato de campo (1), emitir (S2) un certificado de no-manipulación, si el resultado de la comprobación es negativo y transmitir (S3) el certificado de no-manipulación, se realizan a intervalos de tiempo regulares.

6. Sistema de vigilancia para un aparato de campo con protección antimanipulación, en particular adecuado para realizar un procedimiento de acuerdo con al menos una de las reivindicaciones 1-5,
que incluye un equipo de vigilancia de manipulación (2), que es adecuado para vigilar el aparato de campo (1) para la protección antimanipulación,
un equipo registrador (3) para registrar y vigilar el estado del aparato de campo (1),
un equipo de vigilancia (4) para controlar y vigilar el aparato de campo (1), en el que
el equipo de vigilancia de manipulación (2) está configurado para comprobar si se ha realizado una manipulación en el aparato de campo (1) y emite un certificado de no-manipulación si el resultado de la comprobación es negativo y en el que
el equipo registrador (3) está configurado para comprobar el certificado de no-manipulación y determinar un estado activo del aparato de campo (1) cuando el certificado de no-manipulación es válido y en el que
el equipo de vigilancia (4) está configurado para comprobar un estado del aparato de campo (1) y en el que
el equipo de vigilancia (4) está configurado para aceptar datos del aparato de campo en el caso de que se dé un estado activo del aparato de campo (1).

7. Sistema de vigilancia de acuerdo con la reivindicación 6,
caracterizado porque está dispuesto un equipo de control (34) que incluye un equipo registrador (3) y el equipo de vigilancia (4).

8. Sistema de vigilancia de acuerdo con al menos una de las reivindicaciones 6-7,
caracterizado porque el equipo de control (34) está configurado en forma de un puesto de control SCADA o de un sistema ERP.

9. Sistema de vigilancia de acuerdo con al menos una de las reivindicaciones 6-8,
caracterizado porque al menos uno de los equipos (2, 3, 4, 34) incluye una interfaz de comunicación hacia Internet, hacia una red de telefonía móvil y/o hacia una red por satélite.

10. Sistema de vigilancia de acuerdo con al menos una de las reivindicaciones 6-9, **caracterizado porque** el equipo de vigilancia de manipulación (4) presenta una alimentación de energía autónoma.

11. Utilización de un sistema de vigilancia de acuerdo con al menos una de las reivindicaciones 6 - 10 para vigilar una instalación de tráfico o para vigilar una estación transformadora.

FIG 1

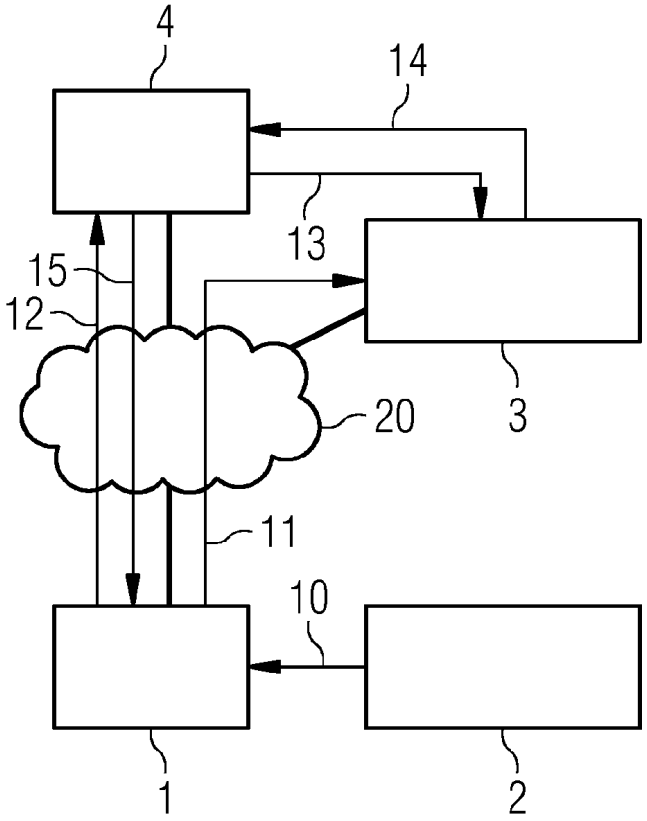

FIG 2

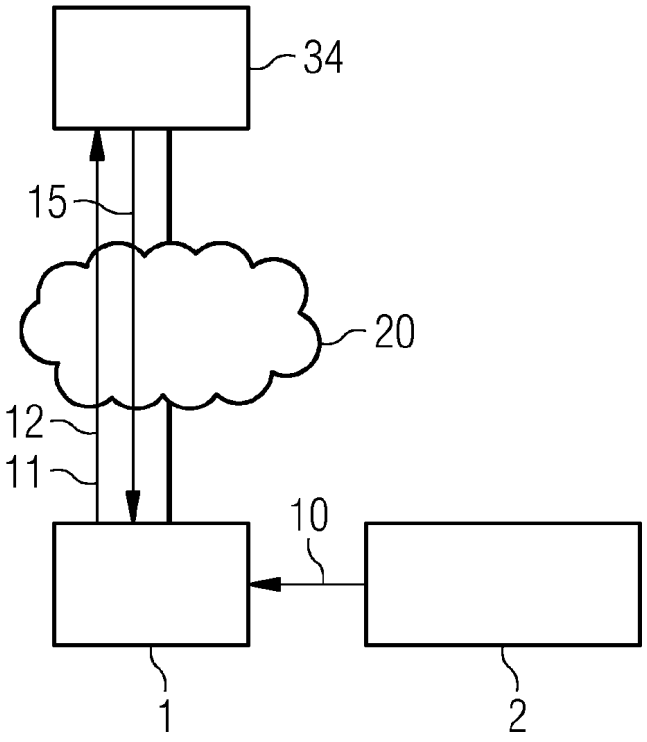

FIG 3

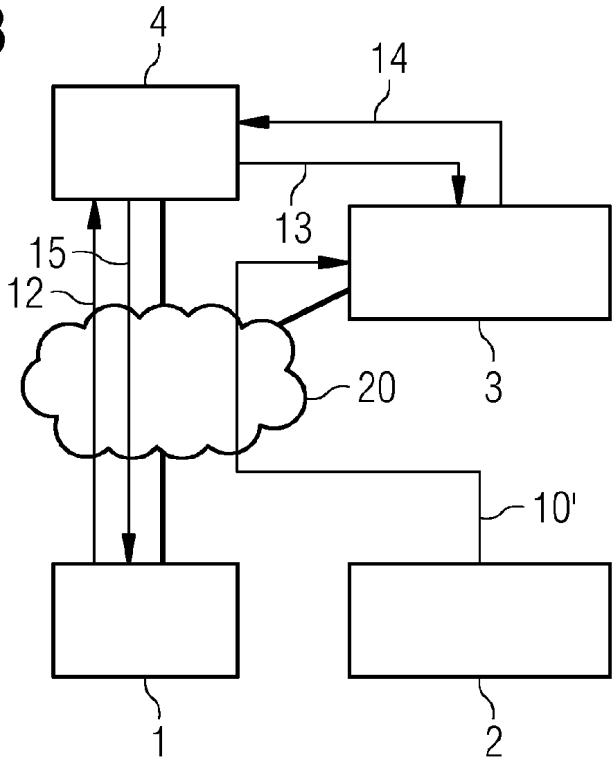

FIG 4a

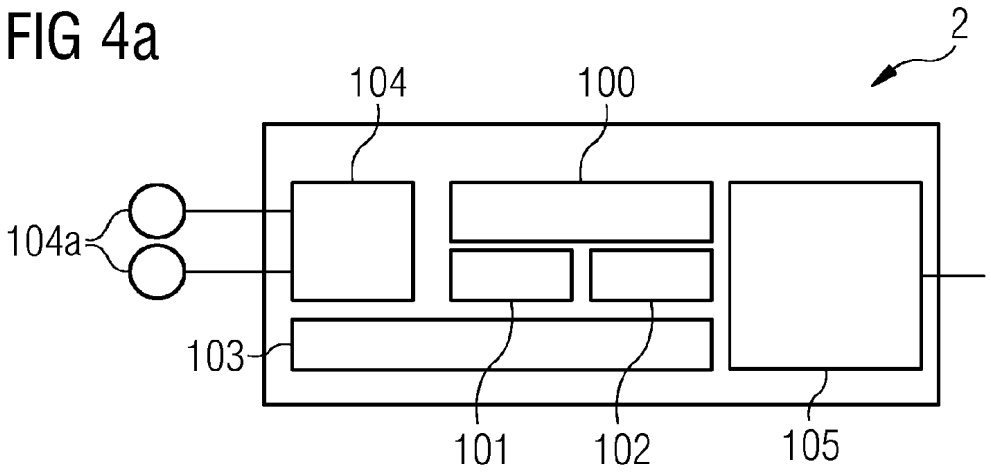

FIG 4b

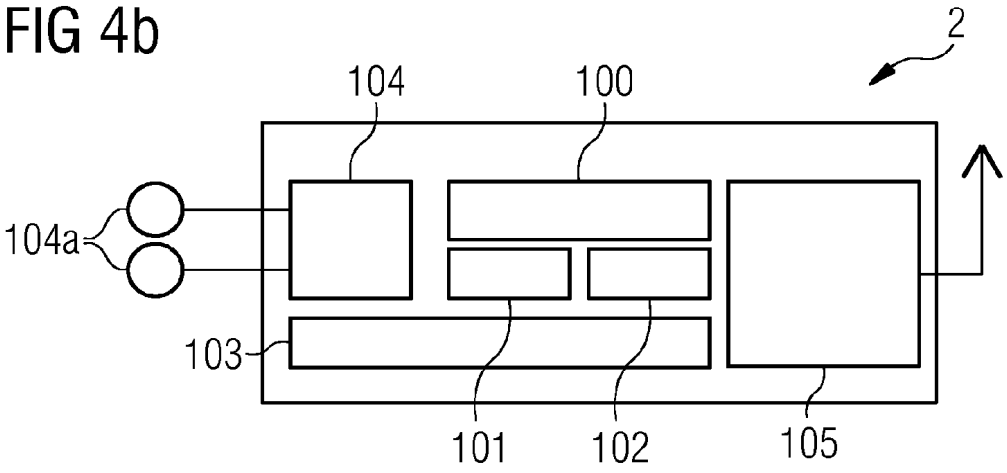

FIG 5