(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 532 772**

(51) Int. CI.:

G06F 21/00 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **15.12.2011 E 11805467 (5)**

(97) Fecha y número de publicación de la concesión europea: **28.01.2015 EP 2628121**

(54) Título: **Dispositivo y procedimiento para proteger un módulo de seguridad frente a intentos de manipulación en un aparato de campo**

(30) Prioridad:

14.01.2011 DE 102011002706

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
31.03.2015

(73) Titular/es:

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

(72) Inventor/es:

FALK, RAINER y
FRIES, STEFFEN

(74) Agente/Representante:

PÉREZ BARQUÍN, Eliana

DISPOSITIVO Y PROCEDIMIENTO PARA PROTEGER UN MÓDULO DE SEGURIDAD FRENTE A INTENTOS DE MANIPULACIÓN EN UN APARATO DE CAMPO

DESCRIPCIÓN

La presente invención se refiere a un dispositivo y a un procedimiento para proteger un módulo de seguridad frente a intentos de manipulación, en particular en aparatos de campo con protección tamper (frente a manipulación).

Estado de la técnica

Los aparatos de campo industriales como por ejemplo aparatos de control para instalaciones de ferrocarriles y de vías, para el control de semáforos o de indicaciones de cambios en el tráfico o para vigilar oleoductos, se encuentran la mayoría de las veces en sectores públicamente accesibles o de difícil vigilancia por parte del operador, por lo que básicamente no puede excluirse que se logre un acceso no autorizado a un aparato de campo y en base a ello puedan realizarse intentos de manipulación. En este contexto se habla también de un “tampering” cuando existen intervenciones y manipulaciones no autorizadas.

Puesto que los aparatos de campo disponen de una funcionalidad de seguridad integrada, mediante la cual se asegura criptográficamente por ejemplo la comunicación externa con centros de mando o centros de cálculo, es necesario proteger suficientemente frente a un tampering los correspondientes datos relevantes para la seguridad, que necesita el aparato de campo para un funcionamiento correcto.

Para memorizar datos relevantes para la seguridad como por ejemplo claves criptográficas de comunicación, son básicamente adecuados chips de seguridad previstos especialmente para esta función, por ejemplo circuitos integrados de seguridad, que memorizan con seguridad los datos clave y también realizan cálculos criptográficos necesarios con los datos clave internamente en el chip. El propio chip de seguridad está entonces la mayoría de las veces protegido frente a manipulación, es decir, integrado en un entorno adecuado protegido frente a manipulación.

Tales chips de seguridad no pueden dotarse desde luego de sensores de tamper externos o de sensores de manipulación con los que puedan detectarse intentos de manipulación fuera del entorno protegido frente a manipulación, en el que está integrado el propio chip. No obstante, también para tales intentos de manipulación es deseable poder garantizar que se mantienen secretos los datos relevantes para la seguridad en el chip de seguridad.

En el caso de un intento de manipulación en el aparato de campo, el responsable de desencadenar medidas de seguridad es hasta ahora la unidad de ordenador o equipo de control del aparato de campo. Para ello debe encontrarse el equipo de control en un modo de servicio activo. No obstante a menudo está conectado el equipo de control a inactivo o bien en el caso de la manipulación incluso no es capaz de funcionar o no está alimentado con suficiente corriente.

El documento US 2007/0255966 A1 da a conocer un circuito criptográfico con una memoria de datos segura y una unidad funcional del sistema, que accede a la memoria de datos.

El documento DE 10 2006 014 133 A1 da a conocer un dispositivo con una memoria de datos que está rodeado por una unidad de protección física, una unidad de borrado y una unidad de acceso, que permite un acceso externo a la memoria de datos.

El documento US 2009/0106563 A1 da a conocer un sistema que protege datos almacenados en una memoria frente a manipulación.

El documento US 2008/0222430 A1 da a conocer un sistema protegido frente a manipulación con un aparato de control y una memoria de datos segura, protegida frente a maniobras de manipulación.

Existe por lo tanto una necesidad de soluciones con ayuda de las cuales puedan desencadenarse de manera fiable, eficiente y rápida medidas de seguridad adecuadas para asegurar que se mantienen secretos datos relevantes para la seguridad en un chip de seguridad de un aparato de campo cuando se realizan intentos de manipulación en el aparato de campo.

Resumen de la invención

Una idea de la presente invención es prever una interfaz intermedia entre un equipo de control de un aparato de campo y un módulo de seguridad tradicional, que vigila el intercambio de datos relevantes para la seguridad entre el equipo de control y el módulo de seguridad y que cuando existan intentos de manipulación en el aparato de campo pueda desencadenar autónomamente las medidas necesarias para mantener secretos los datos relevantes para la seguridad. La interfaz intermedia emula tanto para el

equipo de control como también para el módulo de seguridad un interlocutor de comunicación tradicional, con lo que no son necesarias modificaciones en los protocolos de comunicación existentes.

Una forma de ejecución de la presente invención según la reivindicación 1 consiste por lo tanto en un dispositivo para proteger un módulo de seguridad frente a intentos de manipulación en un aparato de campo, con un equipo de control diseñado para controlar el aparato de campo, un módulo de seguridad diseñado para mantener disponibles datos clave criptográficos para su utilización mediante el equipo de control y un equipo de interfaz conectado entre el equipo de control y el módulo de seguridad, que posibilita una comunicación entre el equipo de control y el módulo de seguridad y que está diseñado para permitir al equipo de control el acceso a los datos clave criptográficos que se mantienen disponibles en el módulo de seguridad y, cuando hay un intento de manipulación en el aparato de campo, impedir el acceso a los datos clave criptográficos. Esto ofrece la ventaja de poder equipar aparatos de campo con módulos de seguridad tradicionales de manera eficiente y económica, sin tener que modificar componentes existentes del aparato de campo.

Según una forma de ejecución preferente incluye el dispositivo sensores de manipulación, conectados con el equipo de interfaz y que están diseñados para detectar intentos de manipulación en el aparato de campo o en un entorno protegido frente a manipulación del módulo de seguridad y señalizarlo al equipo de interfaz. Así puede iniciar el equipo de interfaz autónomamente y sin apoyo del equipo de control medidas de seguridad adecuadas en intentos de manipulación. En particular en el estado inactivo del equipo de control pueden así desencadenarse rápida y fiablemente medidas de seguridad para asegurar los datos clave criptográficos.

Preferiblemente el equipo de interfaz es un módulo de hardware, por ejemplo un módulo lógico programable. Esto ofrece la ventaja de que el equipo de interfaz puede configurarse compacto, económico y cumpliendo su finalidad con un funcionamiento adecuado.

Según una forma de ejecución ventajosa incluye el dispositivo además una fuente de alimentación, conectada con el equipo de interfaz y que está diseñada para alimentar eléctricamente, al menos temporalmente, el equipo de interfaz. Esto tiene la ventaja de que cuando se detectan intentos de manipulación no tiene que activarse primeramente el equipo de control para desencadenar medidas de seguridad. Es especialmente ventajoso que también cuando se interrumpan alimentaciones eléctricas de otro tipo del aparato de campo y/o del equipo de control, el equipo de interfaz permanezca alimentado eléctricamente hasta que puedan haberse llevado a cabo medidas de seguridad adecuadas para mantener secretos los datos clave criptográficos en el módulo de seguridad.

La presente invención logra además un procedimiento según la reivindicación 8 para proteger un módulo de seguridad frente a intentos de manipulación en un aparato de campo, con las etapas: Enviar una petición de un equipo de control del aparato de campo relativa a datos clave criptográficos de un módulo de seguridad a un equipo de interfaz;
comprobar en el equipo de interfaz si se ha detectado un intento de manipulación en el aparato de campo;
transmitir los datos clave criptográficos del módulo de seguridad al equipo de control mediante el equipo de interfaz, si no se ha detectado ningún intento de manipulación; e
impedir la transmisión de los datos clave criptográficos del módulo de seguridad al equipo de control a través del equipo de interfaz, si se ha detectado un intento de manipulación.

Ventajosamente se realiza además un borrado de los datos clave criptográficos en el módulo de seguridad mediante el equipo de interfaz cuando se ha detectado un intento de manipulación. De esta manera puede imposibilitarse ventajosamente que lean datos clave criptográficos en el módulo de seguridad personas no autorizadas, si se ha realizado una manipulación en el aparato de campo.

Según una forma de ejecución, se impide y/o bloquea la autentificación del equipo de control frente al módulo de seguridad o una comunicación del equipo de control con el módulo de seguridad a través del equipo de interfaz. Con ello puede evitarse un acceso posiblemente no autorizado a los datos clave criptográficos, cuando existe una sospecha de manipulación.

La invención logra además un aparato de campo según la reivindicación 15 con un dispositivo correspondiente a la invención para proteger un módulo de seguridad frente a intentos de manipulación.

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

Breve descripción de las figuras

Se describirán a continuación más en detalle diversas formas de ejecución y configuraciones de la presente invención, con referencia a los dibujos adjuntos, en los cuales muestra la

figura 1 una representación esquemática de un aparato de campo con un dispositivo para proteger un módulo de seguridad según una forma de ejecución de la invención;

figura 2 una representación esquemática de un aparato de campo con un dispositivo para proteger un módulo de seguridad según otra forma de ejecución de la invención;
figura 3 un esquema de un procedimiento para la comunicación con un dispositivo para proteger un módulo de seguridad según otra forma de ejecución de la invención; y
figura 4 una representación esquemática de un procedimiento para proteger un módulo de seguridad según otra forma de ejecución de la invención.

Las mejoras y perfeccionamientos descritos pueden combinarse entre sí de cualquier forma, 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 relativas a los ejemplos de ejecución.

Los dibujos adjuntos deben trasmitir una comprensión adicional de las formas de ejecución de la invención. Los mismos muestran formas de ejecución y sirven en relación con la descripción para explicar principios y conceptos de la invención. Otras formas de ejecución y muchas de las ventajas citadas resultan de los dibujos.

Los elementos de los dibujos no se muestran necesariamente a la misma escala uno que otro. Las mismas referencias designan aquí componentes iguales o de similar funcionamiento.

Descripción detallada de la invención

En lo que sigue pueden incluir los sensores de manipulación en el sentido de esta descripción todos los equipos de detección que captan intervenciones físicas en el aparato vigilado y que pueden transmitir las correspondientes señalizaciones a los equipos de cálculo o control asociados. Por ejemplo pueden detectar tales equipos de detección alteraciones del estado normal relativas a luz, radiaciones iónicas, temperatura, presión, resistencia eléctrica, tensión eléctrica o efectos físicos similares que implica una intervención tamper o bien una manipulación del aparato vigilado. Los sensores de manipulación en el sentido de esta descripción pueden incluir por lo tanto por ejemplo interruptores, láminas tamper (por ejemplo un llamado “wire mesh” o una lámina de malla conductora de seguridad), barreras de luz, configuraciones capacitivas, superficies de sensor sensibles a la luz o equipos similares. Debe quedar claro que también otros equipos de captación con funcionalidad similar pueden ser sensores de manipulación en el sentido de esta descripción.

La figura 1 muestra una representación esquemática de un aparato de campo 10 con un dispositivo para proteger un módulo de seguridad 7. El aparato de campo 10 puede ser por ejemplo un aparato de control para una instalación de ferrocarriles o de vías, por ejemplo para un cambio de agujas, una barrera o una señal. El aparato de campo 10 puede no obstante ser cualquier otro aparato remoto, como por ejemplo un dispositivo de vigilancia de un oleoducto, una estación meteorológica o un semáforo. El aparato de campo 10 incluye un equipo de control 1, que por un lado puede controlar tareas funcionales del aparato de campo 10 y por otro procesos de comunicación dentro del aparato de campo 10 o con el mundo exterior. Un equipo de entrada/salida 2 puede estar previsto para conectar el equipo de control 1 por ejemplo con una estación central como un centro de mando o un centro de cálculo. Mediante el equipo de entrada/salida 2 puede comunicar el aparato de campo 10 con el mundo exterior utilizando claves criptográficas.

Pueden enviarse y recibirse datos con protección criptográfica por ejemplo mediante la correspondiente codificación con ayuda del equipo de entrada/salida 2. Para la codificación puede utilizarse cualquier técnica de codificación conocida como por ejemplo IPsec, SSL/TLS, MACsec, L2TP, PPTP, PGP, S/MIME o una técnica similar con la correspondiente gestión de claves, como por ejemplo IKE, EAP u otro procedimiento. Para ello incluye el aparato de campo 10 conexiones de comunicación 3, que conectan el equipo de entrada/salida 2 con el mundo exterior.

Al equipo de entrada/salida 2 puede estar conectado por ejemplo un sensor de manipulación 5, que puede detectar o reconocer intentos de manipulación o intervenciones no autorizadas en el aparato de campo 10. Cuando se detecta un intento de manipulación, el sensor de manipulación 5 transmite mediante el equipo de entrada/salida 2 la correspondiente señal al equipo de control 1, que a continuación puede tomar las correspondientes medidas de aseguramiento.

El aparato de campo 10 puede incluir además un equipo de memoria 4, conectado con el equipo de control 1. El equipo de memoria 4 puede ser por ejemplo un módulo de memoria, en el que pueden memorizarse de manera duradera y reescribible ajustes de configuración del aparato de campo 10, por ejemplo una EEPROM serie, una memoria flash o un equipo de memoria equivalente.

El aparato de campo 10 incluye además un módulo de seguridad 7, en el que pueden estar archivados datos relevantes para la seguridad, como por ejemplo datos clave criptográficos para que los utilice el equipo de control 1. El módulo de seguridad 7 puede ser por ejemplo un circuito integrado, que dispone de una protección tamper pasiva, por ejemplo una capa de pasivación o sensores de manipulación en el propio módulo de seguridad 7. El módulo de seguridad 7 puede estar asegurado por ejemplo frente a

intentos de manipulación exteriores por medio de medidas que detectan y corrigen errores para la memoria y la comunicación por bus, codificación interna de datos, máscaras de cableado irregulares o memorización de datos físicamente asegurada. Como módulo de seguridad 7 pueden utilizarse por ejemplo chips de seguridad tradicionales que pueden obtenerse en el comercio.

El aparato de campo 10 incluye un equipo de interfaz 6, conectado entre el equipo de control 1 y el módulo de seguridad 7 y que posibilita y vigila la comunicación entre el equipo de control 1 y el módulo de seguridad 7 como una especie de hardware-firewall (cortafuegos de hardware). El equipo de interfaz puede incluir por ejemplo un circuito integrado, un módulo lógico programable, como un GAL (Generic Array Logic, matriz lógica genérica), CPLD (Complex Programmable Logic Device, aparato lógico programable complejo) o FPGA (Field Programmable Gate Array, matriz de puertas programables en campo), ASIC (Application Specific Integrated Circuit, circuito integrado de aplicación específica) o bien un microprocesador. El equipo de interfaz 6 puede estar acoplado por ejemplo mediante una interfaz de datos, como por ejemplo USB, un bus de datos serie como I2C o una interfaz de tarjeta de chip con el equipo de control 1. El aparato de campo 1 puede incluir además un sensor de manipulación 8, conectado al equipo de interfaz 6 y que puede detectar intentos de manipulación en el aparato de campo 10 o en partes del aparato de campo 10 y puede transmitir las correspondientes señales de manipulación al equipo de interfaz 6. Cuando detecta un intento de manipulación el sensor de manipulación 8, puede tomar el equipo de interfaz 6 autónomamente medidas de aseguramiento adecuadas, para garantizar que se mantienen secretos los datos clave criptográficos en el módulo de seguridad 7. Es posible que esté previsto el sensor de manipulación 8 en lugar del sensor de manipulación 5 en el aparato de campo 10. Pero también es posible disponer ambos sensores de manipulación 5 y 8 en el aparato de campo 10.

El aparato de campo 10 puede incluir además una fuente de alimentación (no mostrada) que alimenta eléctricamente el equipo de interfaz 6, incluso cuando el aparato de campo 10 o el equipo de control 6 estén desconectados, inactivos o sustituidos permanente o temporalmente por otra fuente de alimentación. Por ejemplo puede presentar la fuente de alimentación una batería, un acumulador, un condensador de doble capa, como por ejemplo un goldcap, un ultracap o un supercap o una fuente de alimentación similar. La fuente de alimentación puede estar diseñada para alimentar eléctricamente el equipo de interfaz 6 al menos temporalmente. Al respecto puede estar previsto garantizar la alimentación eléctrica del equipo de interfaz 6 al menos hasta que el equipo de interfaz 6 haya tomado o completado en el caso de un intento de manipulación medidas de aseguramiento adecuadas para mantener secretos los datos relevantes para la seguridad en el módulo de seguridad 7. También es posible integrar la fuente de alimentación en el equipo de interfaz 6.

La figura 2 muestra una representación esquemática de un aparato de campo 20 con un dispositivo para proteger un módulo de seguridad 7. El aparato de campo 20 se diferencia del aparato de campo 10 descrito y mostrado en la figura 1 en que el equipo de interfaz 6 y el módulo de seguridad 7 están integrados en un entorno común 21 protegido frente a manipulación. El entorno 21 puede presentar por ejemplo una protección frente a manipulación física completa o parcial, por ejemplo mediante encapsulado con resina epoxi. Puede estar previsto además otro sensor de manipulación 28, dispuesto dentro del entorno 21 protegido frente a manipulación y que puede detectar una manipulación, por ejemplo una penetración en la masa del encapsulado. El sensor de manipulación 28 puede incluir por ejemplo una lámina especial, una llamada “tamper-mesh” y/o “wire mesh”. Tales láminas incluyen mallas de vías conductoras, que pueden pegarse alrededor de aparatos a proteger. Un intento de manipulación de un entorno 21 protegido de esta manera provoca interrupciones y/o cortocircuitos, que generan la correspondiente señal. No obstante debe quedar claro que es posible una pluralidad de configuraciones para el sensor de manipulación 28.

En el ejemplo mostrado del aparato de campo 20 no están alojados los sensores de manipulación 5 y 8 en el entorno 21 protegido frente a manipulación. No obstante también es posible integrar uno o ambos de los sensores de manipulación 5 y 8 en el entorno 21 protegido frente a manipulación. Tampoco el equipo de control 1 ni los demás componentes del aparato de campo 20 están integrados en el entorno 21 protegido frente a manipulación. Debido a ello no tienen que encapsularse por ejemplo componentes sensibles, lo cual hace que el entorno 21 protegido frente a manipulación sea de realización compacta y económica.

La figura 3 muestra un esquema de un procedimiento para la comunicación con un dispositivo para proteger un módulo de seguridad. El procedimiento 30 puede entonces realizarse en particular mediante un aparato de campo según una configuración correspondiente a una de las figuras 1 ó 2.

En una primera etapa 31 transmite el equipo de control 1 una petición con una autentificación al equipo de interfaz 6. La autentificación puede presentar por ejemplo un código de activación, un PIN o un contenido similar, con el que el equipo de control 1 puede autentificarse frente al módulo de seguridad 7. Entonces actúa el equipo de interfaz 6 como receptor y emula así el módulo de seguridad 7 frente al equipo de control 1. En una segunda etapa 32 retransmite el equipo de interfaz 6 la petición al módulo de seguridad 7, siempre que no se haya detectado ningún intento de manipulación y la comunicación entre el equipo de control 1 y el módulo de seguridad 7 se catalogue como segura.

Tras una autentificación del equipo de control 1 en el módulo de seguridad 7, envía el módulo de seguridad 7 en una tercera etapa 33 una respuesta de confirmación al equipo de interfaz 6, que en una cuarta etapa 34 se retransmite al equipo de control 1. Tras la autentificación envía el equipo de control 1 en una quinta etapa 35 un valor aleatorio, un llamado challenge (reto), al equipo de interfaz 6, que en una sexta etapa 36 retransmite el equipo de interfaz 6 al módulo de seguridad 7. En el módulo de seguridad 7 se procesa a continuación con ayuda de un cálculo criptográfico el challenge (reto), utilizando los datos clave criptográficos, para generar por ejemplo una clave de comunicación. El cálculo puede incluir por ejemplo una codificación, un cálculo de una suma de prueba criptográfica, una formación de valor hash, un cálculo de una firma digital o un cálculo similar. El resultado del cálculo se transmite en una séptima etapa 37 desde el módulo de seguridad 7 al equipo de interfaz 6, que retransmite el resultado en una octava etapa 38 al equipo de control 1. El resultado del cálculo puede utilizarse por ejemplo para establecer enlaces de comunicación protegidos criptográficamente mediante el equipo de control 1.

La secuencia 30 mostrada para el procedimiento es válida para el caso de que la conexión entre el equipo de control 1 y el módulo de seguridad 7 sea catalogada por el equipo de interfaz 6 como segura, es decir, que no haya detectado el equipo de interfaz 6 ningún intento de manipulación. Tan pronto como se detecta un intento de manipulación en cualquier instante durante la comunicación entre el equipo de control 1 y el módulo de seguridad 7, puede estar diseñado el equipo de interfaz 6 para impedir la transmisión de datos entre el equipo de control 1 y el módulo de seguridad 7. Entonces es posible impedir por completo la transmisión de datos entre el equipo de control 1 y el módulo de seguridad 6, o bien sólo impedir la transmisión de determinados datos. En este último caso analiza el equipo de interfaz 6 los datos recibidos cuando se ha detectado una manipulación, y sólo los retransmite cuando cumplen un criterio de prueba predeterminado. De esta manera es posible incluso cuando se ha detectado una manipulación, una utilización parcial del módulo de seguridad 7 mediante el equipo de control 1.

La figura 4 muestra una representación esquemática de un procedimiento 40 para proteger un módulo de seguridad, como por ejemplo el módulo de seguridad 7 de las figuras 1 a 3. En una primera etapa 41 se envía al equipo de interfaz 6 una petición de un equipo de control 1 de un aparato de campo, como por ejemplo de los aparatos de campo 10 ó 20 de las figuras 1 ó 2, relativa a datos clave criptográficos del módulo de seguridad 7. En el equipo de interfaz 6 se comprueba a continuación en una etapa 42 si se ha detectado un intento de manipulación en el aparato de campo. Para ello puede vigilarse continuamente la presencia de una señal de manipulación mediante un sensor de manipulación conectado al equipo de interfaz 6, como por ejemplo los sensores de manipulación 8 y 28 de la figura 2. Si no se ha detectado ningún intento de manipulación, pueden transmitirse datos clave criptográficos del módulo de seguridad 7 al equipo de control 1 a través del equipo de interfaz 6 en una etapa 43 según el procedimiento de la figura 3. Pero si se ha detectado un intento de manipulación, se impide en una etapa 44 la transmisión de los datos clave criptográficos del módulo de seguridad 7 al equipo de control 1 a través del equipo de interfaz 6. La obstaculización puede por ejemplo hacerse bloqueando por completo la comunicación entre el equipo de control 1 y el módulo de seguridad 7 a través del equipo de interfaz 6 o bien limitándola en partes. Puede realizarse por ejemplo la correspondiente catalogación en función de la gravedad del intento de manipulación. También es posible que no se retransmitan los correspondientes códigos de autentificación, como por ejemplo un PIN, a través del equipo de interfaz 6 al módulo de seguridad 7 mientras no quede garantizada la seguridad de la comunicación. Puede estar previsto también que el equipo de interfaz 6, si se ha detectado un intento de manipulación, envíe una orden de bloqueo al módulo de seguridad 7, para impedir la emisión de cualquier dato relevante para la seguridad a través del módulo de seguridad 7 ya mediante el propio módulo de seguridad 7.

En otra etapa 45 es posible que el equipo de interfaz 6 borre los datos clave criptográficos en el módulo de seguridad 7 mediante una orden de borrado físicamente desde el módulo de seguridad 7, en el caso de que exista un intento de manipulación. De esta manera puede asegurarse que incluso cuando haya una ampliación o lectura no autorizada del módulo de seguridad, se han borrado ya todos los datos relevantes para la seguridad.

Puede estar previsto que estén memorizadas de antemano las correspondientes medidas de seguridad en función de la gravedad o de la catalogación de un posible intento de manipulación ya como medidas de emergencia en el equipo de interfaz 6, con lo que en el caso de un intento de manipulación pueden desencadenarse sin demora todas las medidas de aseguramiento. El equipo de interfaz 6 puede así reaccionar muy rápidamente a un intento de manipulación. En particular cuando el equipo de interfaz 6 pueda ser alimentado al menos temporalmente de forma continua mediante una fuente de alimentación, no es necesario esperar primeramente a una activación del equipo de control 1 para iniciar medidas de aseguramiento. También en un fallo del equipo de control 1, por ejemplo al faltar la alimentación eléctrica o al romperse el equipo de control 1, pueden realizarse todas las medidas de aseguramiento autónomamente mediante el equipo de interfaz 6.

REIVINDICACIONES

1. Dispositivo para proteger un módulo de seguridad (7) frente a intentos de manipulación en un aparato de campo (10; 20), con:
un equipo de control (1) diseñado para
controlar el aparato de campo (10; 20); y
un módulo de seguridad (7) diseñado para
mantener disponibles datos clave criptográficos para su utilización mediante el equipo de control (1);
caracterizado por un equipo de interfaz (6) conectado entre el equipo de control (1) y el módulo de seguridad (7) y que posibilita una comunicación entre el equipo de control (1) y el módulo de seguridad (7),
y que está diseñado para posibilitar al equipo de control (1) el acceso a los datos clave criptográficos que se mantienen disponibles en el módulo de seguridad (7) e impedir el acceso a los datos clave criptográficos cuando hay un intento de manipulación en el aparato de campo (10; 20).

2. Dispositivo según la reivindicación 1, además con:
un primer sensor de manipulación (8), conectado al equipo de interfaz (6) y que está diseñado para detectar intentos de manipulación en el aparato de campo (10; 20) e indicarlos al equipo de interfaz (6).

3. Dispositivo según la reivindicación 1 ó 2,
en el que el módulo de seguridad (7) y el equipo de interfaz (6) están integrado en un entorno protegido frente a manipulación (21).

4. Dispositivo según la reivindicación 3, además con:
un segundo sensor de manipulación (28), que está conectado con el equipo de interfaz (6), que está integrado en el entorno protegido frente a manipulación (21) y que está diseñado para detectar intentos de manipulación en el entorno protegido frente a manipulación (21) e indicarlos al equipo de interfaz (6).

5. Dispositivo según una de las reivindicaciones precedentes, además con:
un equipo de entrada/salida (2), conectado con el equipo de control (1) y que está diseñado para proporcionar una comunicación externa al equipo de control (1),
un tercer sensor de manipulación (5), que está conectado con el equipo de entrada/salida (2) y que está diseñado para detectar intentos de manipulación en el aparato de campo (10; 20) e indicarlos al equipo de control (1),
un equipo de memoria (4), conectado con el equipo de control (1) y diseñado para memorizar datos utilizados en el equipo de control (1)

6. Dispositivo según una de las reivindicaciones precedentes,
en el que el equipo de interfaz (6) es un módulo lógico programable.

7. Dispositivo según una de las reivindicaciones precedentes, además con:
una fuente de alimentación, conectada con el equipo de interfaz (6) y que está diseñada para alimentar eléctricamente, al menos temporalmente, el equipo de interfaz (6).

8. Procedimiento para proteger un módulo de seguridad (7) frente a intentos de manipulación en un aparato de campo (10; 20), con las etapas:
enviar a un equipo de interfaz (6) una petición de un equipo de control (1) en el aparato de campo (10; 20) relativa a datos clave criptográficos de un módulo de seguridad (7);
comprobar en el equipo de interfaz (6) si se ha detectado un intento de manipulación en el aparato de campo (10; 20);
transmitir los datos clave criptográficos del módulo de seguridad (7) al equipo de control (1) mediante el equipo de interfaz (6), si no se ha detectado ningún intento de manipulación; e
impedir la transmisión de los datos clave criptográficos del módulo de seguridad (7) al equipo de control (1) mediante el equipo de interfaz (6), si se ha detectado un intento de manipulación.

9. Procedimiento según la reivindicación 8, además con la etapa:
borrado de los datos clave criptográficos en el módulo de seguridad (7) mediante el equipo de interfaz (6), cuando se ha detectado un intento de manipulación.

10. Procedimiento según la reivindicación 8 ó 9,
en el que el envío de la petición incluye una autentificación del equipo de control (1) frente al módulo de seguridad (7).

11. Procedimiento según la reivindicación 10,
en el que la evitación de la transmisión incluye impedir la autentificación del equipo de control (1) frente al módulo de seguridad (7) mediante el equipo de interfaz (6).

12. Procedimiento según una de las reivindicaciones 8 a 11,
en el que la evitación de la transmisión incluye un bloqueo de la comunicación del equipo de control (1) con el módulo de seguridad (7) mediante el equipo de interfaz (6).

13. Procedimiento según una de las reivindicaciones 8 a 12,
en el que la comprobación en el equipo de interfaz (6) de si se ha detectado un intento de manipulación en el aparato de campo (10; 20) incluye la evaluación de un sensor de manipulación (8; 28) conectado con el equipo de interfaz (6).

14. Procedimiento según una de las reivindicaciones 8 a 13, además con la etapa:
alimentación eléctrica, al menos temporal, del equipo de interfaz (6) mediante una fuente de alimentación, cuando la alimentación eléctrica del equipo de control (1) y/o del aparato de campo (10; 20) está interrumpida o el equipo de control (1) está conectado a inactivo.

15. Aparato de campo (10; 20) con un dispositivo según una de las reivindicaciones 1 a 7.

FIG 1

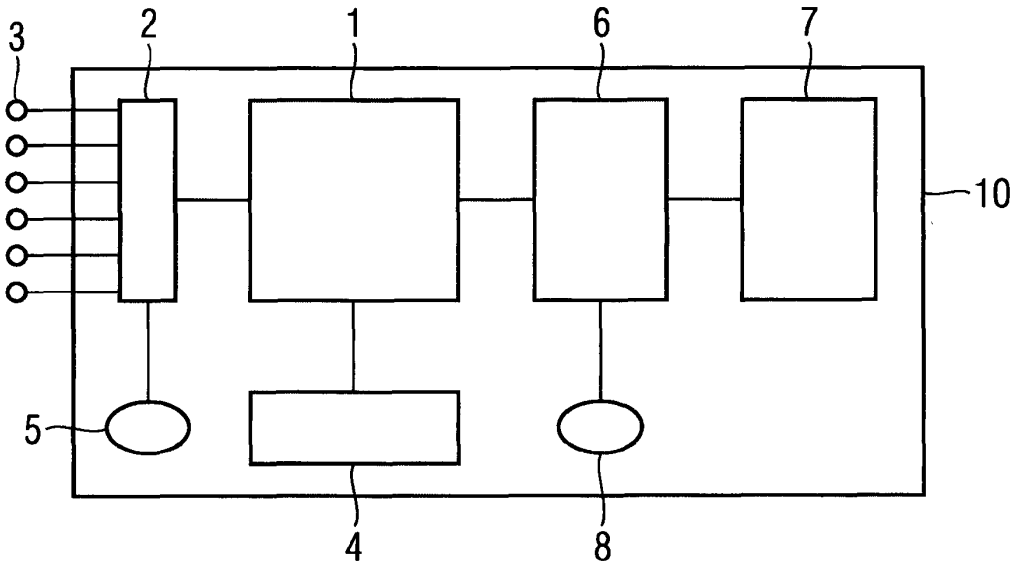

FIG 2

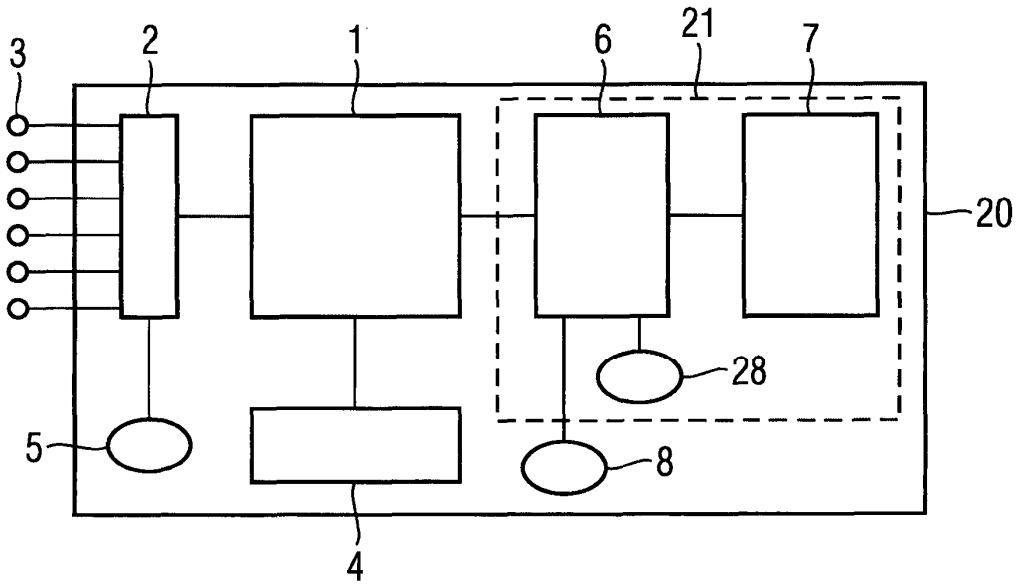

FIG 3

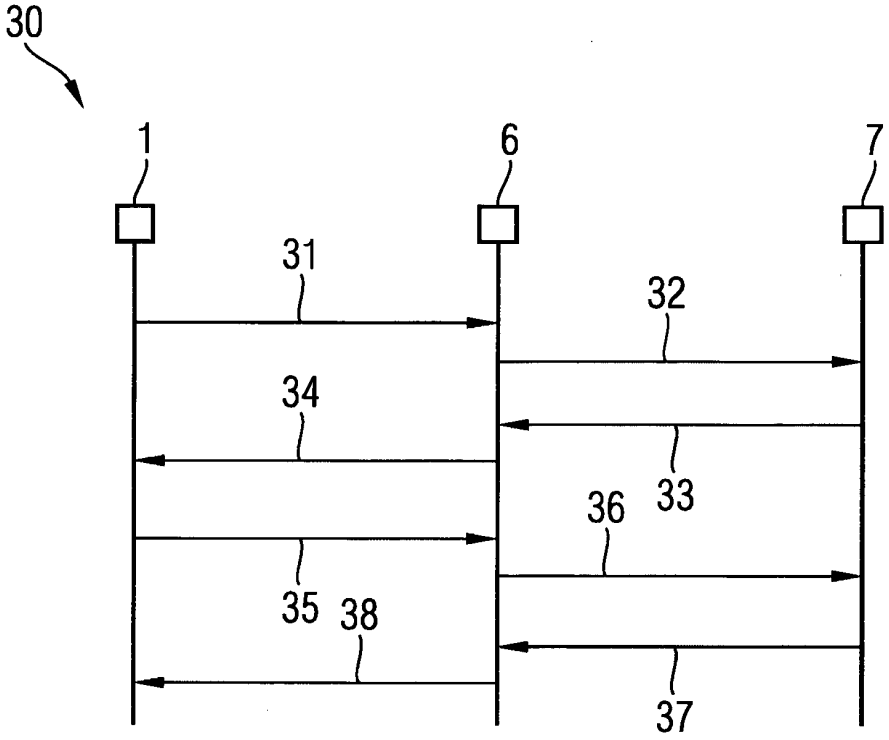

FIG 4