(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 532 771**

(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 11805465 (9)**

(97) Fecha y número de publicación de la concesión europea: **28.01.2015 EP 2622527**

(54) Título: **Procedimiento y dispositivo para proporcionar una clave criptográfica para un aparato de campo**

(30) Prioridad:

14.01.2011 DE 102011002703

(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

PROCEDIMIENTO Y DISPOSITIVO PARA PROPORCIONAR UNA CLAVE CRIPTOGRÁFICA PARA UN APARATO DE CAMPO

DESCRIPCIÓN

La invención se refiere a un procedimiento y a un dispositivo para proporcionar una clave criptográfica para un aparato de campo, en particular un aparato de campo industrial.

Los aparatos de campo industriales que cumplen funciones de control, por ejemplo un control de válvula, disponen en muchos casos de sensores y actuadores o de otros subsistemas. Para proteger una comunicación de datos frente a manipulaciones, es necesario memorizar de forma protegida en los aparatos de campo claves y/o credenciales criptográficas. Para tales aparatos de campo, que están instalados a menudo en zonas en las que son accesibles a atacantes, es necesario proteger estos aparatos de campo frente a manipulaciones físicas. Por ello se memorizan hasta ahora en aparatos de campo tradicionales datos sensibles, en particular claves criptográficas, en una zona que ofrece localmente una cierta protección frente a manipulaciones, por ejemplo en una carcasa especialmente protegida, que dispone por ejemplo de una llamada malla de alambre o bien wire mesh o bien una rejilla conductora de seguridad, es decir, un sistema sensórico de red de alambre que cuando hay una manipulación en la carcasa detecta esta manipulación y dado el caso origina un borrado automático de los datos memorizados. Tales sensores se denominan también sensores tamper (de manipulación). En general se conoce así una vigilancia tamper mediante sensores tamper, en la que los sensores tamper necesitan no obstante por lo general una alimentación eléctrica. Se conocen medidas de protección físicas que dificultan un tampering (manipulación), por ejemplo carcasas especiales o unidades constructivas encapsuladas. Una tal vigilancia tamper local necesita no obstante una alimentación eléctrica permanente o bien una batería tampón. En el caso de que la energía eléctrica disponible mediante la batería decaiga, queda la vigilancia tamper fuera de servicio. Además, en esta forma de proceder tradicional debe dotarse cada aparato de campo de una tal vigilancia tamper o de una tal protección tamper separada, con lo que el coste técnico es relativamente alto.

Un tal proceder se conoce por ejemplo por “SEKEN: secure and efficient key exchange for sensor networks” (SEKEN: Intercambio de claves seguro y eficiente para redes de sensores”), Kamran Jamshaid, Loren Schwiebert, 2004 IEEE CONFERENCIA INTERNACIONAL SOBRE PRESTACIONES, COMPUTACIÓN Y COMUNICACIONES, PHOENIX, AZ ABRIL 15-17, 2004, ISBN: 978-0-7803-8396-8.

Por lo tanto es una tarea de la presente invención lograr un procedimiento y un dispositivo que ofrezca una protección potente tamper o frente a manipulación para aparatos de campo y que a la vez evite los inconvenientes de los equipos tradicionales de vigilancia y protección tamper utilizados hasta ahora.

Esta tarea se resuelve en el marco de la invención mediante un dispositivo de seguridad con las características indicadas en la reivindicación 1.

La invención logra un dispositivo de seguridad para proporcionar una clave criptográfica para un aparato de campo,
estando el dispositivo de seguridad conectado con al menos un sensor tamper asociado al aparato de campo, que cuando detecta una manipulación física realizada en el aparato de campo emite un aviso de manipulación,
proporcionándose la clave criptográfica al aparato de campo mediante el dispositivo de seguridad sólo cuando el dispositivo de seguridad no recibe ningún aviso de manipulación de los sensores tamper asociados al aparato de campo.

El dispositivo de seguridad no está montado en el aparato de campo a vigilar, sino conectado mediante una red con el aparato de campo, es decir, la vigilancia tamper del aparato de campo no se realiza localmente, sino de forma remota mediante un dispositivo de seguridad situado alejado. Por lo tanto no es necesaria en la vigilancia tamper correspondiente a la invención una alimentación eléctrica duradera y/o permanente, por ejemplo mediante una batería tampón en el aparato de campo. Además en la vigilancia tamper correspondiente a la invención mediante el dispositivo de seguridad según la invención el coste técnico es relativamente bajo, ya que los correspondientes aparatos de campo no tienen que dotarse de una protección tamper local.

En una forma de ejecución posible del dispositivo de seguridad correspondiente a la invención, están conectados los sensores tamper inalámbricamente o mediante hilos con el dispositivo de seguridad.

Una conexión inalámbrica de los sensores tamper con el dispositivo de seguridad permite una instalación sencilla del aparato de campo y reduce así el coste técnico para la implementación.

En otra forma de ejecución posible del dispositivo de seguridad correspondiente a la invención, están montados los sensores tamper directamente en el aparato de campo o bien integrados en el aparato de campo.

En otra forma de ejecución posible del dispositivo de seguridad correspondiente a la invención están montados los sensores tamper en una carcasa cerrada y/o en un armario de maniobra en el que se encuentra el correspondiente aparato de campo.

En otra forma de ejecución posible del dispositivo de seguridad correspondiente a la invención, se proporciona la clave criptográfica al correspondiente aparato de campo cuando el mismo se anuncia a una red sólo tras una autentificación con éxito frente al dispositivo de seguridad.

En otra forma de ejecución posible del dispositivo de seguridad correspondiente a la invención, utiliza el aparato de campo la clave criptográfica proporcionada para la codificación o decodificación de mensajes que intercambia el aparato de campo con otros aparatos de campo o con un nodo de pasarela (gateway) de la red.

Además es posible que el aparato de campo utilice la clave criptográfica proporcionada para decodificar datos memorizados localmente en el aparato de campo.

En otra forma de ejecución posible del dispositivo de seguridad correspondiente a la invención, presenta el mismo una unidad lectora, que recibe avisos inalámbricamente de los sensores tamper.

En una forma de ejecución posible del dispositivo de seguridad correspondiente a la invención, los sensores tamper son sensores activos, que disponen de una alimentación eléctrica propia.

En una forma de ejecución alternativa preferente los sensores tamper son sensores pasivos, que no disponen de una alimentación eléctrica propia.

Los sensores tamper sirven para detectar manipulaciones físicas, que puede realizar un atacante en el aparato de campo.

En una forma de ejecución posible son estos sensores tamper interruptores eléctricos o magnéticos para detectar una abertura en una carcasa o en un armario de maniobra.

Además los sensores tamper pueden ser sensores para captar radiación electromagnética.

Los sensores pueden ser en particular sensores de luz y/o sensores de barrera luminosa.

En otra forma de ejecución posible incluyen los sensores tamper también sensores para detectar haces de iones.

En otra forma de ejecución posible presentan los sensores tamper también sensores de temperatura para detectar una variación de temperatura.

En otra forma de ejecución posible presentan los sensores tamper también sensores de aproximación.

En otra forma de ejecución posible presentan los sensores tamper también sensores de vibración, que detectan una variación de posición.

En otra forma de ejecución posible presentan los sensores tamper también mallas de alambre, previstas en una envolvente encapsulada o bien en una carcasa encapsulada.

Son posibles otros tipos de sensores tamper, que pueden presentar un efecto físico que aparece cuando tiene lugar una manipulación física.

Preferiblemente se utilizan en el dispositivo de seguridad correspondiente a la invención sensores tamper pasivos, que no necesitan ninguna alimentación eléctrica propia.

En una forma de ejecución posible del dispositivo de seguridad correspondiente a la invención obtienen estos sensores tamper pasivos en cada momento su energía para generar el aviso de manipulación al dispositivo de seguridad de una energía que resulta de la manipulación física. Si se encuentra por ejemplo un sensor tamper sobre una luna de vidrio, que se golpea con un martillo, puede obtenerse en una posible forma de ejecución un sensor tamper que para generar el aviso de manipulación obtiene la energía necesaria de la energía mecánica que aparece debido al golpe del martillo.

En una forma de ejecución alternativa obtienen los sensores tamper pasivos en cada caso su energía para generar el aviso de manipulación al dispositivo de seguridad de un campo emitido por el dispositivo de seguridad, en particular de un campo electromagnético.

En una ejecución posible del dispositivo de seguridad correspondiente a la invención, están codificados los sensores tamper correspondientes al aparato de campo en un certificado digital de aparato correspondiente al aparato de campo.

La invención logra además un procedimiento para proporcionar una clave criptográfica para un aparato de campo tal que se proporciona la clave criptográfica al aparato de campo mediante un dispositivo de seguridad sólo si el dispositivo de seguridad no recibe dentro de un periodo de tiempo predeterminado un aviso de manipulación que señalice una manipulación física realizada en el aparato de campo de ningún sensor tamper asociado al aparato de campo.

En una posible forma de ejecución del procedimiento correspondiente a la invención, sólo se proporciona la clave criptográfica al aparato de campo una vez realizada la autentificación del aparato de campo frente al dispositivo de seguridad.

En otra forma de ejecución posible del procedimiento correspondiente a la invención, obtienen los sensores tamper la energía para generar un aviso de manipulación de una energía que aparece durante la manipulación o de un campo emitido por el dispositivo de seguridad.

En una forma de ejecución posible del procedimiento correspondiente a la invención, la clave criptográfica proporcionada es una clave de sesión, que utiliza el aparato de campo para la comunicación con otro aparato de campo o con una pasarela de la red.

En otra forma de ejecución posible del procedimiento correspondiente a la invención, decodifica el aparato de campo con ayuda de la clave criptográfica proporcionada datos memorizados de forma codificada en el aparato de campo.

A continuación se describirán más en detalle formas de ejecución posibles del dispositivo de seguridad correspondiente a la invención para proporcionar una clave criptográfica para un aparato de campo con referencia a las figuras adjuntas.

Se muestra en:

figura 1 un ejemplo de ejecución de un sistema que dispone de un dispositivo de seguridad para proporcionar claves criptográficas para aparatos de campo según la invención;
figura 2 un diagrama de señales para representar la forma de funcionamiento del procedimiento correspondiente a la invención para proporcionar claves criptográficas para un aparato de campo,
figura 3 un ejemplo de ejecución de otro sistema que dispone de un dispositivo de seguridad para proporcionar una clave criptográfica para un aparato de campo según la invención.

Tal como puede observarse en la figura 1, dispone el sistema 1 representado en la figura 1 de un dispositivo de seguridad 2 para proporcionar claves o credenciales criptográficas para diversos aparatos de campo 3-i. En el ejemplo representado se encuentran tres aparatos de campo 3-1, 3-2, 3-3 en un armario de maniobra 4, indicado mediante línea discontinua. El dispositivo de seguridad 2 está conectado mediante una red 5 con un equipo lector 6. El equipo lector 6 puede ser por ejemplo un lector RFID (RR), conectado a través de la red 5 con el dispositivo de seguridad 2. Además está conectado el dispositivo de seguridad 2 en el ejemplo de ejecución representado en la figura 1 a través de la red 5 con una pasarela 7, que puede comunicar con los diversos aparatos de campo 3-i. En el ejemplo de ejecución representado en la figura 1 se encuentra un aparato de campo 3-4 fuera del armario de maniobra 4. Los aparatos de maniobra pueden ser por ejemplo nodos sensores de una red de sensores. En el ejemplo de ejecución representado disponen algunos nodos sensores o aparatos de campo de sensores tamper propios 8-i. Así dispone por ejemplo el aparato de campo 3-3 dentro del armario de maniobra 4 de un sensor tamper propio 8-3. Además dispone el aparato de campo 3-4 fuera del armario de maniobra 4 de un correspondiente sensor tamper propio 8-4. En el armario de maniobra 4 están montados en el ejemplo de ejecución representado otros sensores tamper 9-1, 9-2. Estos sensores tamper 9-1, 9-2 no están así directamente montados en aparatos de campo 3-i, sino en una carcasa o bien un armario de maniobra 4 en el que se encuentran los aparatos de campo. En el ejemplo de ejecución representado en la figura 1 están montados en el armario de maniobra 4 dos sensores tamper 9-1, 9-2 de este tipo. Los sensores tamper 8-i, 9-i pueden ser consultados en el ejemplo de ejecución representado en la figura 1 por el equipo lector 6. Los sensores 8-i, 9-i pueden ser por ejemplo sensores tamper pasivos, que obtienen su energía para generar un aviso de manipulación por ejemplo de un campo electromagnético emitido por el equipo lector 6. Los sensores tamper 8-3, 8-4 están montados directamente en el aparato de campo a vigilar o bien nodo sensor 3-3, 3-4, pudiendo estar montados los mismos en la carcasa del aparato de campo o estar integrados en el propio aparato de campo. Los sensores tamper 9-1, 9-2 están montados por ejemplo en lunas de vidrio de un armario de maniobra 4 y detectan una manipulación física en la correspondiente luna de vidrio del armario de maniobra 4. En el ejemplo de ejecución representado en la figura 1 comunican los sensores tamper 8-i, 9-i con el equipo lector 9 inalámbricamente. Alternativamente pueden transmitir los sensores tamper un aviso de manipulación al dispositivo de seguridad 2 también a través de hilos. El dispositivo de seguridad 2 está conectado con al menos un sensor tamper 3-i asociado al correspondiente aparato de campo. Entonces pueden estar asociados a un aparato de campo uno o varios sensores tamper. Por ejemplo están asociados al nodo sensor 3-3 en el ejemplo de ejecución representado, además del sensor tamper 8-3 directamente montado, también ambos sensores tamper 9-

1, 9-2, ya que el aparato de campo 3-3 se encuentra dentro del armario de maniobra 4 que a su vez es vigilado mediante ambos sensores tamper 9-1, 9-2. El aparato de campo 3-1 y/o el nodo sensor que no disponen de ningún sensor tamper propio llevan asociados esencialmente los sensores tamper 9-1, 9-2 del armario de maniobra 4. El nodo sensor 3-4 previsto fuera del armario de maniobra 4 dispone de un sensor tamper propio 8-4, igualmente asociado al mismo.

En una forma de ejecución posible dispone el dispositivo de seguridad 2 de una memoria de datos y gestiona una lista de los sensores tamper asociados a los correspondientes aparatos de campo 3-i. Un sensor tamper asociado a un aparato de campo 3-i envía cuando detecta una manipulación física realizada en el aparato de campo 3-i un aviso de manipulación, por ejemplo un aviso de suceso tamper o bien evento tamper TE, que por ejemplo se retransmite mediante el equipo lector 6 al dispositivo de seguridad 2. Cuando se anuncia un aparato de campo 3-i al dispositivo de seguridad 2, por ejemplo a través de la pasarela 7, sólo se le proporcionan al correspondiente aparato de campo 3-i las claves y/o credenciales criptográficas necesarias mediante el dispositivo de seguridad 2 si el dispositivo de seguridad 2 no ha recibido de ninguno de los sensores tamper 3-i asociados al aparato de campo hasta entonces un aviso de manipulación y/o un aviso de evento tamper TE. En una variante se revoca la clave y/o credencial criptográfica ya proporcionada a un aparato de campo 3-i en el caso de que el dispositivo de seguridad 2 reciba de uno de los sensores tamper asociados al aparato de campo 3-i un aviso de manipulación y/o un aviso de evento tamper TE. Para ello puede proporcionar el dispositivo de seguridad 2 un mensaje de revocación asociado a la clave proporcionada y/o a la credencial proporcionada. En una forma de ejecución posible se proporcionan las claves criptográficas al correspondiente aparato de campo 3-i sólo durante un determinado periodo de tiempo y caducan una vez transcurrido un tiempo determinado. En una forma de ejecución posible se proporcionan las claves criptográficas a los aparatos de campo 3-i al anunciarse a una red mediante el dispositivo de seguridad 2 sólo tras una autentificación con éxito del correspondiente aparato de campo 3-i frente al dispositivo de seguridad 2. La clave criptográfica proporcionada puede ser por ejemplo una clave de sesión o bien Session Key SK. Esta clave criptográfica proporcionada puede utilizarla el aparato de campo 3-i para codificar o decodificar mensajes que se intercambian entre los aparatos de campo. Además es posible utilizar la clave criptográfica proporcionada también para decodificar datos archivados codificadamente en el aparato de campo 3-i. Los sensores tamper representados en la figura 1 pueden ser sensores tamper de lo más diverso, que detectan diversas manipulaciones físicas, en particular interruptores eléctricos o magnéticos, sensores para detectar radiación electromagnética, sensores para detectar radiaciones iónicas, sensores de temperatura, sensores de aproximación, sensores de movimiento, sensores de vibración o sensores de malla de alambre. Preferiblemente se utilizan como sensores tamper 8-i, 9-i sensores tamper pasivos, que no tienen que disponer de una alimentación eléctrica propia.

En una forma de ejecución preferente obtienen los sensores tamper pasivos 8-i, 9-i su energía para generar un aviso de manipulación al dispositivo de seguridad 2 de la energía que resulta de la manipulación física. Si se golpea por ejemplo la luna de vidrio del armario de maniobra 4 en el que se encuentra el sensor tamper 9-i, puede obtenerse en una forma de ejecución posible de este sensor tamper a partir de la vibración mecánica una energía que le permite emitir un aviso de manipulación y/o aviso de suceso tamper TE al equipo lector 6.

En una forma de ejecución alternativa obtienen los sensores tamper pasivos su energía para generar el aviso de manipulación al dispositivo de seguridad 2 de un campo electromagnético irradiado, que por ejemplo emite el equipo lector 6.

El dispositivo de seguridad 2 sirve para proporcionar, es decir para suministrar o acordar una clave o credencial criptográfica a un aparato de campo 3-i con una interfaz de comunicación, por ejemplo Ethernet, IP, W-LAN o similar. Entonces se autentifica el aparato de campo 3-i preferiblemente frente al dispositivo de seguridad 2. El aparato de campo 3-i necesita una clave criptográfica durante su funcionamiento. Entonces aporta la clave criptográfica el dispositivo de seguridad 2 preferiblemente cuando se anuncia a la red el correspondiente aparato de campo, por ejemplo mediante Ethernet o mediante una interfaz de radio, en particular W-LAN, RFID, IEEE802.15.4.

El dispositivo de seguridad 2 vigila adicionalmente sensores externos tamper o de manipulación, estando asociados estos sensores tamper en cada caso a uno o varios aparatos de campo. Una clave y/o credencial criptográfica sólo se proporciona a un aparato de campo 3-i mediante el dispositivo de seguridad 2 cuando ningún sensor de manipulación y/o tamper relevante para el correspondiente aparato de campo 3-i detecta o bien ha detectado en un periodo de tiempo de vigilancia anterior un suceso tamper TE.

Los sensores de manipulación y/o tamper pueden estar conectados inalámbricamente con el dispositivo de seguridad 2. Al respecto es posible que los sensores tamper comuniquen inalámbricamente, por ejemplo mediante RFID o IEEE802.15.4. Los sensores tamper pueden ser en particular sensores tamper pasivos, es decir, sensores sin alimentación eléctrica propia o tamponamiento de batería. Los sensores tamper pasivos pueden obtener la energía necesaria para el funcionamiento de un campo emitido por el dispositivo de seguridad 2. Al respecto puede tratarse de un campo de un lector RFID o también de un campo emitido a través de una antena, sin que el equipo lector esté conectado. Además es posible que

los sensores tamper obtengan por sí mismos su energía necesaria a partir del suceso a vigilar, es decir, por ejemplo puede estar equipado un sensor de invasión o bien sensor tamper como sensor eléctrico, en el que se genera energía eléctrica mediante presión. Esta energía generada puede utilizarse para la comunicación del sensor tamper. Un tal sensor tamper puede existir separadamente, por ejemplo para montarlo en una chapaleta de mantenimiento. Además es posible que un tal sensor tamper esté integrado en un aparato de campo 3-i.

En una forma de ejecución posible, puede trasmitir en una comunicación de un aparato de campo con el dispositivo de seguridad 2 el aparato de campo al dispositivo de seguridad 2 una información sobre qué sensores tamper o sensores de manipulación ha de vigilar el dispositivo de seguridad 2 para este aparato de campo 3-i. Especialmente para sensores tamper integrados en el aparato de campo, puede estar codificada esta información en un certificado digital de aparato correspondiente aparato de campo 3-i. Alternativamente puede consultar el dispositivo de seguridad 2 estos datos también en un banco de datos central, que por ejemplo se pone a disposición en base a una identificación del aparato, por ejemplo mediante un certificado digital.

En una forma de ejecución posible borra el aparato de campo 3-i los datos secretos y/o datos sensibles memorizados en el aparato de campo tan pronto como el aparato de campo 3-i cambia a un estado de servicio inactivo, en particular tras detectar una manipulación física en el correspondiente aparato de campo.

Desde el punto de vista del aparato de campo 3-i, que mientras tanto se encontraba en un estado de servicio inactivo, por ejemplo sin alimentación eléctrica, puede en consecuencia consultar posteriormente este aparato de campo en el dispositivo de seguridad 2 si los correspondientes sensores de manipulación y/o tamper continuamente, es decir, durante todo el periodo de vigilancia, no han detectado ninguna manipulación. Siempre que no exista ninguna manipulación, recibe el aparato de campo 3-i del dispositivo de seguridad 2 parámetros secretos o claves criptográficas que el mismo necesita para asumir un funcionamiento regular.

La figura 2 muestra un diagrama de señales para explicar el procedimiento correspondiente a la invención para proporcionar una clave criptográfica para un aparato de campo 3-i. En el ejemplo de ejecución representado vigila el dispositivo de seguridad 2 una pluralidad de sensores tamper 8-i distintos, asociados a diversos aparatos de campo 3-i, 3-j. En el ejemplo representado en la figura 2 recibe el dispositivo de seguridad 2 primeramente de un sensor tamper 8-k asociado a un aparato de campo 3-k un aviso de manipulación o bien aviso de suceso tamper TE.

A continuación transmite otro aparato de campo 3-i un mensaje de autentificación, por ejemplo codificado con una clave de aparato correspondiente al aparato, a través de la pasarela 7 al dispositivo de seguridad 2, para registrarse o anunciarse. El dispositivo de seguridad 2 comprueba el mensaje de anuncio recibido en cuanto a si el nodo o el aparato de campo 3-i que se anuncia tiene derecho a utilizar la red. Además comprueba el dispositivo de seguridad si en un sensor tamper asociado al aparato de campo 3-i existe un aviso de manipulación. Si no existe ningún aviso de manipulación y la autentificación del aparato de campo 3-i tiene éxito, recibe el aparato de campo 3-i que realiza la consulta un mensaje Accept o bien OK y la correspondiente clave de sesión o Session Key SK para proteger su comunicación en la red. De la misma manera se anuncia en el ejemplo representado en la figura 2 otro aparato de campo 3-j al dispositivo de seguridad 2 y recibe igualmente una clave de sesión o Session Key SK. En una forma de ejecución posible, la clave de sesión SK es válida en toda la red. A continuación pueden realizar ambos aparatos de campo 3-i, 3-j con ayuda de la clave de sesión SK recibida una comunicación criptográfica protegida entre sí, tal como se representa en la figura 2.

Cuando se anuncia en el ejemplo de ejecución representado en la figura 2 otro nodo o bien otro aparato de campo 3-k al dispositivo de seguridad 2, detecta el dispositivo de seguridad 2 que para este nodo existe ya un aviso de manipulación y/o aviso de suceso tamper TE y rechaza el nodo o bien el aparato de campo 3-k. En una forma de ejecución posible, activa automáticamente el mensaje de rechazo (reject) en el nodo 3-k que realiza la consulta un borrado de datos sensibles.

La figura 3 muestra otro ejemplo de aplicación para un dispositivo de seguridad 2 según la invención. En el ejemplo representado en la figura 3 se encuentra el dispositivo de seguridad 2 en una subestación 10, por ejemplo una caseta transformadora de una red distribuidora de energía. La subestación 10 dispone de una red 11 a la que están conectados en el ejemplo representado diversos aparatos de campo 12-1, 12-2, 12-3 en un primer armario de maniobra 4-1 y otros aparatos de campo 13-1, 13-2 en un segundo armario de maniobra 4-2. El primer armario de maniobra 4-1 dispone de un sensor tamper 14 y el segundo armario de maniobra 4-2 dispone de un sensor tamper 15. En el ejemplo representado se encuentran los aparatos de campo 12-1, 12-2, 12-3 en el primer armario de maniobra 4-1 conectados entre sí mediante un bus, por ejemplo un bus Ethernet 16 y están conectados con otros aparatos de campo y/o aparatos de control 17-1, 17-2 mediante el bus 16. Además la red 11 está conectada mediante un PC de estación 18 y un módem 19 a un servidor remoto, por ejemplo para fines de mantenimiento a distancia. Además está conectada a la red 11 en el ejemplo representado una unidad DCF77 20. La estación de red local 10 puede presentar para su propia protección otro sensor tamper 21, montado por ejemplo en una puerta de

la estación de red local. En los aparatos de campo previstos en un armario de maniobra pueden estar montados adicionalmente sensores tamper propios. Por ejemplo presenta el aparato de campo 12-2 en el armario de maniobra 4-1 un sensor tamper 22 y el aparato 17-2 presenta un sensor tamper 23.

Un aparato de campo lleva preferiblemente asociados aquellos sensores tamper que son relevantes en un acceso físico directo al aparato de campo. En el ejemplo representado en la figura 3 son por ejemplo relevantes para una manipulación física en el aparato de campo 12-2 los sensores tamper 22, 14, 21, ya que un atacante primeramente tiene que abrir la puerta de la estación de red local 21 y a continuación forzar el armario de maniobra 4-1, para poder realizar a continuación directamente en el aparato de campo 12-2 una manipulación física.

En una variante posible del procedimiento correspondiente a la invención se toman en función del correspondiente suceso tamper TE diversas medidas. Por ejemplo, cuando las exigencias de seguridad son especialmente elevadas, ya al penetrar en la estación de red local 10 con el correspondiente aviso de manipulación mediante el sensor tamper 21 se catalogan todos los aparatos de campo que se encuentran dentro de la estación de red local 10 como amenazados y no reciben a través del dispositivo de seguridad 2 ninguna clave criptográfica y/o credencial criptográfica. Alternativamente se catalogan aparatos de campo mediante el dispositivo de seguridad 2 como amenazados sólo cuando los mismos se ven afectados directamente. Por ejemplo se catalogan los aparatos de campo 12-1, 12-2, 12-3 así como los aparatos 17-1, 17-2 como amenazados y ya no reciben ninguna clave criptográfica del dispositivo de seguridad 2 cuando el sensor tamper 14 señaliza una penetración en el correspondiente armario de maniobra 4-1. En otra variante se cataloga un aparato de campo como amenazado sólo cuando se detecta directamente de forma inmediata en el aparato de campo una manipulación física. En el ejemplo de ejecución representado en la figura 3 se cataloga por ejemplo el aparato de campo 12-2 como amenazado sólo cuando también adicionalmente el sensor tamper 22 señaliza un suceso tamper TE al dispositivo de seguridad 2. En esta variante de ejecución sigue a continuación un bloqueo de la puesta a disposición de claves criptográficas para el aparato de campo 12-2 sólo una vez que el dispositivo de seguridad 2 ha reconocido el correspondiente aviso de manipulación procedente del sensor tamper 21 y también del sensor tamper 14 y adicionalmente del sensor tamper 22.

En otra posible forma de ejecución siguen a continuación diversas medidas, en función de los diversos avisos de manipulación de los sensores tamper asociados al aparato de campo. Por ejemplo, se coloca el dispositivo de seguridad 2 en un aviso de manipulación debido al sensor tamper 21 primeramente sólo en un modo de servicio de alarma, sin que se realicen otras medidas. Si a continuación por ejemplo se manipula el armario de maniobra 4-1 y recibe el dispositivo de seguridad 2 del sensor tamper 14 el correspondiente aviso de manipulación, se catalogan todos los aparatos de campo allí contenidos como amenazados y no reciben ningún material criptográfico y/o se bloquean las claves criptográficas ya otorgadas.

En una tercera etapa, sólo cuando 2B el correspondiente sensor tamper 22 montado directamente en el aparato de campo 12-2 señaliza un aviso de manipulación en el correspondiente aparato de campo, borra a continuación el dispositivo de seguridad 12 adicionalmente de forma automática los datos sensibles memorizados en el aparato de campo, en particular las claves criptográficas. En esta variante de ejecución tiene lugar así una reacción multietapa en función de la profundidad de penetración del agresor. El procedimiento correspondiente a la invención o bien el dispositivo de seguridad 2 correspondiente a la invención para proporcionar una clave criptográfica para un aparato de campo, pueden utilizarse de manera polivalente. Por ejemplo puede utilizarse el dispositivo de seguridad 2 para vigilar una instalación industrial, por ejemplo un oleoducto o una estación distribuidora de energía, por ejemplo una estación de red local. Además es adecuado el dispositivo de seguridad 2 correspondiente a la invención por ejemplo para su utilización en la técnica del transporte, por ejemplo en armarios de maniobra de semáforos y similares. Otros ejemplos son enclavamientos, agujas y señales de marcha en el sector de los ferrocarriles. Además es adecuado el dispositivo de seguridad 2 correspondiente a la invención en particular para la vigilancia de edificios y para otras infraestructuras cuya protección se considera crítica.

En una variante de ejecución posible conoce el aparato de campo correspondiente los sensores tamper asociados a los diversos aparatos de campo o bien están codificados los mismos y se anuncian en un modo de servicio determinado primeramente al dispositivo de seguridad 2. En una forma de ejecución posible gestiona el dispositivo de seguridad 2 la correspondiente lista de sensores tamper asociados a los respectivos aparatos de campo. En una forma de ejecución posible se actualiza automáticamente esta lista cuando se realizan trabajos de mantenimiento y/o reparación en la correspondiente instalación. El dispositivo de seguridad 2 correspondiente a la invención puede además utilizarse también en instalaciones industriales correspondientes a otros sectores, por ejemplo en el ámbito de los vehículos, para vigilar manipulaciones en componentes del vehículo. La comunicación del dispositivo de seguridad 2 con los sensores tamper puede realizarse, tal como se representa en la figura 3, mediante hilos a través de una red 11 o bien, tal como se representa en la figura 1, al menos parcialmente de forma inalámbrica.

REIVINDICACIONES

1. Dispositivo de seguridad (2) para proporcionar una clave criptográfica para un aparato de campo (3), **caracterizado porque** el dispositivo de seguridad (2) está conectado con al menos un sensor tamper (8, 9) asociado al aparato de campo (3), que al detectarse una manipulación física realizada en el aparato de campo (3) emite un aviso de manipulación,
en el que el dispositivo de seguridad (2) proporciona la clave criptográfica al aparato de campo (3) sólo cuando el dispositivo de seguridad (2) no recibe de los sensores tamper (8, 9) asociados al aparato de campo (3) ningún aviso de manipulación.

2. Dispositivo de seguridad según la reivindicación 1,
en el que los sensores tamper (8, 9) están conectados inalámbricamente o mediante hilos con el dispositivo de seguridad (2).

3. Dispositivo de seguridad según la reivindicación 1 ó 2,
en el que los sensores tamper (8, 9) están conectados directamente al aparato de campo (3) o bien están montados en una carcasa cerrada y/o armario de maniobra (4) en el que se encuentra el aparato de campo (3).

4. Dispositivo de seguridad según la reivindicación 1-3,
en el que el dispositivo de seguridad (2) proporciona la clave criptográfica al aparato de campo (3) cuando el mismo se anuncia a una red sólo tras la autentificación con éxito del aparato de campo (3) frente al dispositivo de seguridad (2).

5. Dispositivo de seguridad según la reivindicación 1-4,
en el que el aparato de campo (3) utiliza la clave criptográfica proporcionada por el dispositivo de seguridad (2) para codificar o decodificar mensajes que intercambia el aparato de campo (3) con otros aparatos de campo o un nodo de pasarela (7) de una red.

6. Dispositivo de seguridad según una de las reivindicaciones precedentes 1-5,
en el que el dispositivo de seguridad (2) presenta una unidad lectora (6) que recibe avisos de los sensores tamper inalámbricamente.

7. Dispositivo de seguridad según la reivindicación 1-6,
en el que los sensores tamper (8, 9) conectados con el dispositivo de seguridad (2) son sensores activos o pasivos para detectar manipulaciones físicas en el aparato de campo (3),
presentando los sensores tamper (8, 9) en particular
   - interruptores eléctricos o magnéticos,
   - sensores para detectar radiación electromagnética,
   - sensores para detectar radiaciones iónicas,
   - sensores de temperatura para detectar variaciones de temperatura,
   - sensores de aproximación para detectar la aproximación de un objeto,
   - sensores de movimiento o
   - sensores de red de alambre.

8. Dispositivo de seguridad según la reivindicación 1-7,
en el que los sensores tamper pasivos obtienen en cada caso su energía para generar el aviso de manipulación al dispositivo de seguridad (2) de una energía que resulta de la manipulación física.

9. Dispositivo de seguridad según la reivindicación 1-7,
en el que los sensores tamper pasivos obtienen en cada caso su energía para generar el aviso de manipulación al dispositivo de seguridad (2) del campo irradiado por el dispositivo de seguridad (2).

10. Dispositivo de seguridad según una de las reivindicaciones precedentes 1-9,
en el que los sensores tamper asociados al correspondiente aparato de campo (3) se señalizan mediante el aparato de campo (3) al dispositivo de seguridad (2) o bien son consultados por el dispositivo de seguridad (2) en un banco de datos en base a un ID de aparato correspondiente al respectivo aparato de campo (3).

11. Dispositivo de seguridad según la reivindicación 10,
en el que están codificados los sensores tamper asociados al aparato de campo (3) en un certificado digital de aparato del correspondiente aparato de campo (3).

12. Procedimiento para proporcionar una clave criptográfica para un aparato de campo (3),
en el que la clave criptográfica sólo se proporciona al aparato de campo (3) mediante un dispositivo de seguridad (2) cuando el dispositivo de seguridad (2) no recibe de ninguno de los sensores tamper asociados al aparato de campo (3) dentro de un periodo de tiempo predeterminado ningún aviso de manipulación que señalice una manipulación física realizada en el aparato de campo (3).

13. Procedimiento según la reivindicación 12,
en el que la clave criptográfica se proporciona al aparato de campo (3) mediante el dispositivo de seguridad (2) sólo una vez realizada la autentificación con éxito del aparato de campo (3) frente al dispositivo de seguridad (3).

14. Procedimiento según la reivindicación 12 ó 13,
en el que los sensores tamper (8, 9) obtienen la energía para generar un aviso de manipulación de una energía que aparece durante la manipulación o de un campo irradiado por el dispositivo de seguridad (2).

15. Procedimiento según la reivindicación 12-14,
en el que la clave criptográfica proporcionada por el dispositivo de seguridad (2) es una clave de sesión (SK), que utiliza el aparato de campo (3) para la comunicación con otros aparatos de campo (3) o una gateway o pasarela (7) de una red.

FIG 1

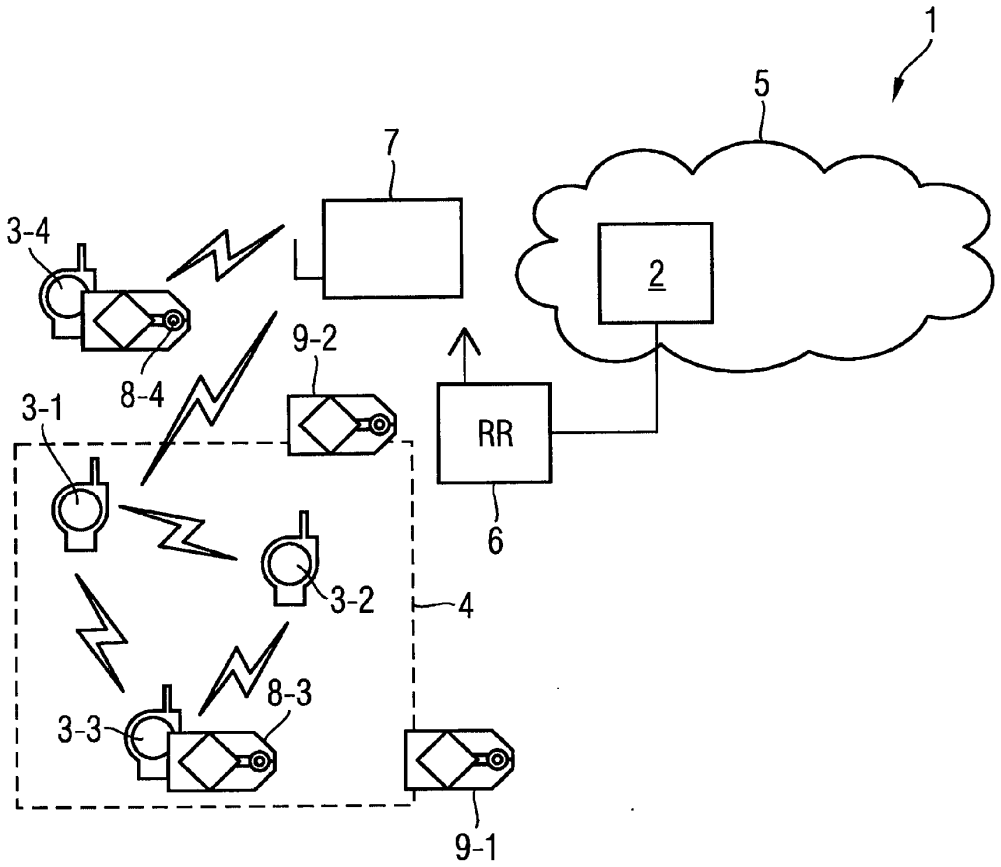

FIG 2

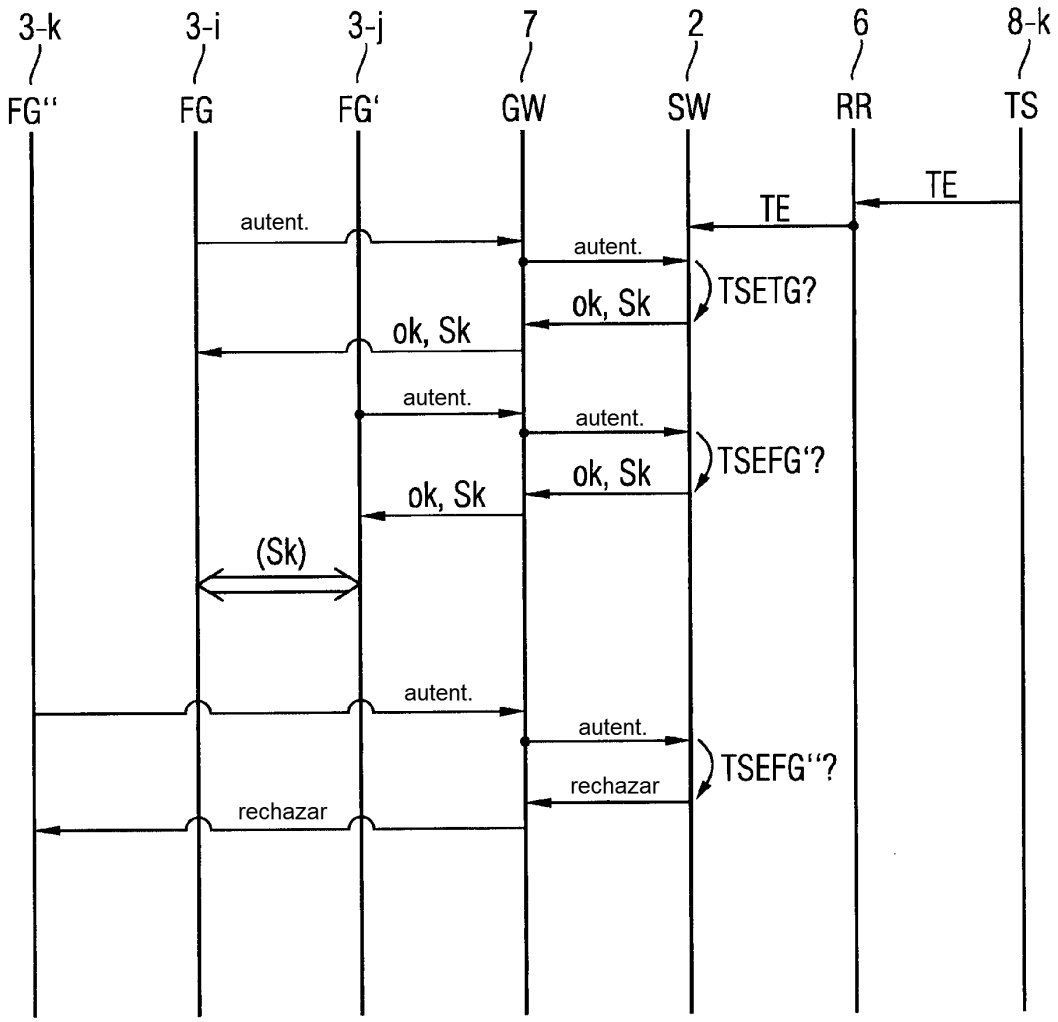
3-k
FG''
3-i
FG
3-j
FG'
7
GW
2
SW
6
RR
8-k
TS
TE
TE
autent.
autent.
TSETG?
ok, Sk
ok, Sk
autent.
autent.
TSEFG''?
ok, Sk
ok, Sk
(Sk)
autent.
autent.
TSEFG''?
rechazar
rechazar

FIG 3