(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 739 153**

(51) Int. CI.:

B61L 1/20 (2006.01)
G06F 21/57 (2013.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **24.03.2016 PCT/EP2016/056565**

(87) Fecha y número de publicación internacional: **06.10.2016 WO16156207**

(96) Fecha de presentación y número de la solicitud europea: **24.03.2016 E 16714339 (5)**

(97) Fecha y número de publicación de la concesión europea: **01.05.2019 EP 3253638**

(54) Título: **Procedimiento para monitorizar un componente de red así como disposición con un componente de red y un dispositivo de monitorización**

(30) Prioridad:

27.03.2015 DE 102015205607

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.01.2020

(73) Titular/es:

SIEMENS MOBILITY GMBH (100.0%)
Otto-Hahn-Ring 6
81739 München, DE

(72) Inventor/es:

BRABAND, JENS

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Procedimiento para monitorizar un componente de red así como disposición con un componente de red y un dispositivo de monitorización

Una monitorización de un componente de red de una red de comunicación puede ser necesaria o conveniente por diferentes motivos. Así, por ejemplo, la norma alemana DIN EN 50159 describe requisitos de una comunicación relevante en cuanto a la seguridad en sistemas de transmisión en el campo de aplicaciones ferroviarias. En el marco de la arquitectura predeterminada a este respecto existe la necesidad de que aplicaciones relevantes en cuanto a la seguridad y/o funciones de transmisión relevantes en cuanto a la seguridad monitoricen aquellas funciones o componentes implementados incluso no en forma de un dispositivo relevante en cuanto a la seguridad, en las que se apoye la respectiva aplicación relevante en cuanto a la seguridad.

Por el documento EP 2 442 519 A1 se conoce un procedimiento para la autenticación de una unidad de red. Cuando se autentica la unidad de red, se incorpora un resultado de comprobación de integridad en un entorno identificado como fiable de la unidad de red. Este su usa para iniciar una petición de autenticación o para notificar un éxito de autenticación.

Por el documento EP 1 126 655 A1 se conoce un procedimiento para asegurar la autenticidad de hardware y software en un sistema interconectado. El sistema interconectado presenta componentes de sistema conectados a través de un bus de sistema con módulos de hardware y software. Los componentes de sistema presentan en cada caso una característica de autenticación para los módulos de hardware y en cada caso una característica de autenticación o aseguramiento de la integridad adicional para los módulos de software. En el bus de sistema se enciende un módulo de comprobación central para comprobar las características de autenticación y/o las características de aseguramiento de la integridad.

La presente invención se basa en el objetivo de indicar un procedimiento especialmente eficiente y al mismo tiempo implementable de manera comparativamente sencilla para monitorizar un componente de red.

Este objetivo se alcanza según la invención mediante un procedimiento para monitorizar un componente de red, en el que por parte del componente de red usando datos específicos para un estado del componente de red se realiza un cálculo que comprueba el funcionamiento correcto del componente de red. Por parte del componente de red se realiza el cálculo que comprueba el funcionamiento del componente de red en forma de una encriptación de los datos específicos para el estado del componente de red. Los datos encriptados se transmiten desde el componente de red como resultado de cálculo al dispositivo de monitorización. El dispositivo de monitorización comprueba mediante el resultado de cálculo transmitido el estado del componente de red así como el funcionamiento correcto del mismo así como la encriptación llevada a cabo por parte del componente de red. Desde el dispositivo de monitorización se transmite un mensaje de petición con una clave de prueba específica para el respectivo mensaje de petición al componente de red. Por parte del componente de red se encriptan los datos específicos para el estado del componente de red para garantizar la actualidad del cálculo por medio de la clave de prueba.

Según la primera etapa del procedimiento según la invención para monitorizar un componente de red se realiza por parte del componente de red usando datos específicos para un estado del componente de red un cálculo que comprueba el funcionamiento correcto del componente de red. A este respecto, en el caso del cálculo que comprueba el funcionamiento correcto del componente de red puede tratarse básicamente de un cálculo correspondiente de cualquier tipo. A este respecto, el cálculo está diseñado preferiblemente de tal manera que al menos una parte de la funcionalidad relevante en cuanto a la seguridad del componente de red se comprueba mediante el cálculo en el sentido de que un funcionamiento incorrecto con respecto a la funcionalidad o funcionalidades en cuestión conducirían a un resultado de cálculo falsificado.

En el marco del procedimiento según la invención, el cálculo que comprueba el funcionamiento correcto del componente de red tiene lugar usando datos específicos para un estado del componente de red. Esto significa que el cálculo tiene lugar de tal manera que diferencias con respecto a los datos específicos para el estado del componente de red con una probabilidad que roza la seguridad o al menos suficiente para el respectivo caso de aplicación influyen en el resultado de cálculo.

Según la segunda etapa del procedimiento según la invención, el resultado de cálculo se transmite desde el componente de red a un dispositivo de monitorización. A este respecto, la transmisión del resultado de cálculo puede tener lugar de cualquier manera en sí conocida. Esto incluye en particular una transmisión por cable o inalámbrica, por ejemplo, por radio, del resultado de cálculo desde el componente de red al dispositivo de monitorización.

Según la tercera etapa del procedimiento según la invención, luego se comprueban por el dispositivo de monitorización mediante el resultado de cálculo transmitido el estado del componente de red así como el funcionamiento correcto del mismo. Esto significa que el dispositivo de monitorización conoce un valor esperado para el resultado de cálculo o el propio dispositivo de monitorización puede realizar el cálculo realizado por el componente de red y con ello comprobar el resultado de cálculo. Para ello es necesario que el dispositivo de monitorización conozca también los datos específicos para el estado del componente de red, que se usan durante el cálculo, o que el dispositivo de monitorización conozca qué valor deben presentar los datos específicos para el estado del componente de red. Por consiguiente, mediante el

resultado de cálculo transmitido es posible comprobar desde el dispositivo de monitorización tanto el estado del componente de red como el funcionamiento correcto del componente de red. Así, el resultado de cálculo determinado por el componente de red coincide entonces exclusivamente con el resultado de cálculo esperado o calculado por el dispositivo de monitorización, cuando el componente de red ha realizado correctamente el cálculo que comprueba su funcionamiento correcto. Para ello es además necesario que también los datos específicos para el estado del componente de red sean correctos en el sentido de que correspondan a los datos esperados por el dispositivo de monitorización.

Por consiguiente, como resultado, el procedimiento según la invención posibilita comprobar de manera comparativamente sencilla tanto el estado del componente de red monitorizado como el funcionamiento correcto del mismo.

Según una forma de realización especialmente preferida, el procedimiento según la invención está perfeccionado de tal manera que desde el dispositivo de monitorización se transmite un mensaje de petición con al menos un parámetro específico para el respectivo mensaje de petición al componente de red y por parte del componente de red durante la realización del cálculo que comprueba el funcionamiento del componente de red para garantizar la actualidad del cálculo se usa el al menos un parámetro específico para el respectivo mensaje de petición. Esto ofrece la ventaja de que por parte del dispositivo de monitorización se garantiza que el resultado de cálculo transmitido por el componente de red se ha calculado realmente de manera actual por el componente de red. De este modo, por parte del dispositivo de monitorización pueden reconocerse, por ejemplo, errores en el sentido de que hay una alteración o un fallo de funcionalidad del componente de red, pero esta alteración o este fallo se enmascara porque el componente de red recurre a un resultado de cálculo determinado en un momento anterior y lo transmite al dispositivo de monitorización. Dado que desde el dispositivo de monitorización se transmite un mensaje de petición con al menos un parámetro específico para el respectivo mensaje de petición al componente de red y este al menos un parámetro se usa por parte del componente de red durante la realización del cálculo que comprueba el funcionamiento del componente de red, por consiguiente se garantiza la actualidad del cálculo del resultado de cálculo. A este respecto, el al menos un parámetro específico para el respectivo mensaje de petición se usa por parte del componente de red de manera análoga a los datos específicos para el estado del componente de red a su vez en el cálculo, de tal manera que diferentes parámetros conducen con una probabilidad suficientemente alta a diferentes resultados de cálculo.

El procedimiento está diseñado según la invención está diseñado además de tal manera que por parte del componente de red se realiza un cálculo que comprueba el funcionamiento del componente de red en forma de una encriptación de los datos específicos para el estado del componente de red, los datos encriptados se transmiten desde el componente de red como resultado de cálculo al dispositivo de monitorización y el dispositivo de monitorización comprueba mediante el resultado de cálculo transmitido el estado del componente de red así como la encriptación llevada a cabo por parte del componente de red. En particular, con respecto a tales componentes de red, que en una red de comunicación son responsables de la encriptación, existe la necesidad de que por parte de componentes o aplicaciones relevantes en cuanto a la seguridad se lleve a cabo una monitorización de la función del componente de red. El procedimiento según la invención posibilita en este contexto comprobar tanto el cálculo en forma de la encriptación como tal como el estado del componente de red mediante los datos específicos para el estado del componente de red. De este modo pueden descubrirse, por ejemplo, también aquellos casos de error, en los que el componente de red básicamente puede realizar la encriptación correcta de mensajes, pero la funcionalidad en cuestión está desconectada por configuración completamente o también en función de la situación, por ejemplo, con respecto a determinados emisores y/o receptores.

El procedimiento está diseñado según la invención además de tal manera que desde el dispositivo de monitorización se transmite un mensaje de petición con una clave de prueba específica para el respectivo mensaje de petición al componente de red y por parte del componente de red se encriptan los datos específicos para el estado del componente de red para garantizar la actualidad del cálculo por medio de la clave de prueba. De manera análoga al perfeccionamiento preferido descrito anteriormente con respecto a la transmisión de un mensaje de petición con al menos un parámetro específico para el respectivo mensaje de petición se posibilita mediante la transmisión de un mensaje de petición con una clave de prueba específica para el respectivo mensaje de petición desde el dispositivo de monitorización al componente de red según la invención, garantizar que el cálculo en forma de la encriptación se realice actualmente por el componente de red y se reconoce de manera fiable una transmisión concebible de un resultado de cálculo determinado en un momento anterior por el dispositivo de monitorización.

Según una forma de realización especialmente preferida adicional del procedimiento según la invención, como datos específicos para el estado del componente de red se usan datos de configuración del componente de red. Esto es ventajoso, dado que los datos de configuración son habitualmente muy adecuados para especificar el estado de un componente de red. Por consiguiente, de este modo se posibilita al dispositivo de monitorización, mediante el resultado de cálculo transmitido desde el componente de red, reconocer posibles errores en los datos de configuración del componente de red.

Alternativa o adicionalmente a la forma de realización descrita anteriormente, el procedimiento según la invención ventajosamente también puede estar configurado de tal manera que como datos específicos para el estado del componente de red se usen informaciones de estado del componente de red. A este respecto, en el caso de las informaciones de estado del componente de red puede tratarse de informaciones de estado de cualquier tipo. Esto incluye, por un lado, informaciones de estado comparativamente sencillas del tipo “activo” o “inactivo”; por otro lado las

informaciones de estado también pueden ser claramente más detalladas y más amplias. A este respecto, únicamente es una condición previa que las informaciones de estado o valores esperados en cuestión se conozcan para estas informaciones de estado por parte del dispositivo de monitorización.

Alternativa o adicionalmente a los dos perfeccionamientos preferidos mencionados anteriormente, el procedimiento según la invención puede transcurrir ventajosamente también de tal manera que como datos específicos para el estado del componente de red se usen datos específicos para software del componente de red. A este respecto, en el caso de los datos específicos para software del componente de red puede tratarse de una parte del software o también de todo el software del componente de red. A través de los datos correspondientes puede calcularse de manera en sí conocida, por ejemplo, un valor hash, que identifica unívocamente el software o la versión de software del componente de red. Por consiguiente, de este modo se posibilita por parte del dispositivo de monitorización basándose en el resultado de cálculo transmitido reconocer eventuales desviaciones del software del componente de red con respecto al software esperado o previsto por parte del dispositivo de monitorización.

Preferiblemente, el procedimiento según la invención también puede estar perfeccionado de tal manera que el dispositivo de monitorización y el componente de red lleven a cabo una autenticación mutua. Esto es ventajoso, dado que de este modo se garantiza con respecto al respectivo otro componente la identidad del componente de red así como del dispositivo de monitorización. De este modo se evitan problemas de seguridad o posibilidades de ataque de lo contrario concebibles con respecto al dispositivo de monitorización y/o al componente de red o la comunicación entre estos dos componentes.

Según una forma de realización especialmente preferida adicional del procedimiento según la invención, desde el componente de red junto con el resultado de cálculo se transmite al menos un parámetro del componente de red al dispositivo de monitorización. En el caso del parámetro correspondiente puede tratarse, por ejemplo, de la frecuencia de intentos de notificación sin éxito o mensajes no autenticados. Mediante la transmisión adicional del al menos un parámetro del componente de red al dispositivo de monitorización existe por parte del mismo ventajosamente la posibilidad de obtener, además del estado del componente de red así como el funcionamiento correcto del mismo, también informaciones de parámetros no conocidos previamente por el dispositivo de monitorización y tenerlos en cuenta en el marco de la monitorización del componente de red.

Preferiblemente, el procedimiento según la invención también puede estar diseñado de tal manera que el al menos un parámetro del componente de red que debe transmitirse por el componente de red al dispositivo de monitorización se notifique conjuntamente por el dispositivo de monitorización. Esto ofrece la ventaja de que el propio dispositivo de monitorización con respecto al componente de red puede especificar qué parámetro o qué parámetros debe o deben transmitirse desde el componente de red junto con el resultado de cálculo al dispositivo de monitorización.

A este respecto, el procedimiento según la invención puede estar configurado preferiblemente de tal manera que el al menos un parámetro comprenda una indicación con respecto a casos de error registrados por el componente de red. Esto es ventajoso, dado que el dispositivo de monitorización se pone en la posición de, en el marco de la monitorización del componente de red, tener en cuanto el número, el tipo y/o la frecuencia de casos de error registrados por el componente de red.

La presente invención se refiere por lo demás a una disposición con un componente de red así como a un dispositivo de monitorización.

En cuando a la disposición, la presente invención se basa en el objetivo de indicar una disposición, que respalde un procedimiento especialmente eficiente y al mismo tiempo que pueda implementarse de manera comparativamente sencilla para monitorizar un componente de red.

Este objetivo se alcanza según la invención mediante una disposición con las características de la reivindicación independiente 10.

Las ventajas de la disposición según la invención corresponden esencialmente a aquellos del procedimiento según la invención, de modo que a este respecto se remite a las explicaciones anteriores correspondientes. Lo mismo es válido en cuanto a los perfeccionamientos preferidos de la disposición según la invención con respecto a los perfeccionamientos preferidos correspondientes del procedimiento según la invención, de modo que también a este respecto se remite a las realizaciones anteriores correspondientes.

Según una forma de realización especialmente preferida de la disposición según la invención, el componente de red y el dispositivo de monitorización están configurados para realizar el procedimiento según una de las reivindicaciones 1 a 9.

A continuación se explicará más detalladamente la invención mediante ejemplos de realización. Para ello, muestra

la figura para explicar un ejemplo de realización del procedimiento según la invención en un diagrama esquemático un ejemplo de realización de la disposición según la invención.

En la figura puede reconocerse un componente 10 de red, que presenta un dispositivo 11 de control, un dispositivo 12 de almacenamiento así como una conexión 13 de comunicación interna que los comunica. Además se representa un

dispositivo 20 de monitorización, que comprende un dispositivo 21 de control. El dispositivo 21 de control del dispositivo 20 de monitorización está unido a través de una conexión 30 de comunicación con el dispositivo 11 de control del componente 10 de red. A este respecto, en el caso de los dispositivos 11 y 21 de control correspondientes puede tratarse, por ejemplo, de procesadores o unidades de cálculo en sí conocidos.

En el marco del ejemplo de realización descrito se asume que en el caso del dispositivo 20 de monitorización se trata de un dispositivo relevante en cuanto a la seguridad, que puede implementarse, por ejemplo, según los requisitos a este respecto de la norma DIN EN 50159. Con respecto al componente 10 de red se asume que este proporciona técnica criptográfica relevante en cuanto a la seguridad, es decir, por ejemplo, por parte del dispositivo 20 de monitorización se encriptan los mensajes proporcionados. Sin embargo, a este respecto, el propio componente 10 de red no está implementado ni realizado como dispositivo relevante en cuanto a la seguridad, de modo que básicamente no puede excluirse un funcionamiento incorrecto del componente 10 de red. Por este motivo es necesario que se monitorice la función del componente 10 de red mediante el dispositivo 20 de monitorización.

Se indica que el componente 10 de red así como el dispositivo 20 de monitorización comprenden por regla general tanto medios técnicos de hardware como medios técnicos de software. A este respecto, en función de las respectivas circunstancias existe también la posibilidad que el componente 10 de red así como el dispositivo 20 de monitorización usen total o al menos parcialmente el mismo hardware y por consiguiente están caracterizados esencialmente por componentes de software correspondientes. Con respecto a la arquitectura conocida por la norma DIN EN 50159, esto puede tener lugar, por ejemplo, de modo que el dispositivo de monitorización se instala en forma de un módulo adicional o de una capa de software adicional entre la función de transmisión relevante en cuanto a la seguridad y la técnica criptográfica relevante en cuanto a la seguridad o también entre la aplicación relevante en cuanto a la seguridad y la función de transmisión relevante en cuanto a la seguridad.

Para poder comprobar ahora por parte del dispositivo 20 de monitorización el funcionamiento del componente 10 de red de manera especialmente fiable y al mismo tiempo comparativamente sencilla, por parte del dispositivo 20 de monitorización en una primera etapa de procedimiento o un primer mensaje s1 puede transmitirse un mensaje de petición con al menos un parámetro específico para el respectivo mensaje de petición al componente 10 de red. A este respecto, el mensaje de petición corresponde en su función a una especie de “*safety ping*”, dado que a través de la misma se desencadena una comprobación del funcionamiento correcto del componente 10 de red.

En el marco del ejemplo de realización descrito se asume que el mensaje de petición como parámetros específicos para el respectivo mensaje de petición contiene una clave de prueba específica para el respectivo mensaje de petición.

Por parte del componente 10 de red se realiza ahora usando datos específicos para un estado del componente 10 de red un cálculo que comprueba el funcionamiento correcto del componente de red. Esto se indica en la figura mediante una etapa s2 de procedimiento asociada al dispositivo 11 de control así como las etapas 2a y s2b de procedimiento que incluyen el dispositivo de almacenamiento. A este respecto, como datos específicos para el estado del componente 10 de red pueden consultarse o leerse por parte del dispositivo 11 de control desde el dispositivo 12 de almacenamiento datos de configuración del componente 10 de red, informaciones de estado del componente 10 de red y/o datos específicos para el software del componente 10 de red.

Por parte del componente 10 de red o su dispositivo 11 de control se realiza ahora un cálculo que comprueba el funcionamiento del componente 10 de red en forma de una encriptación de los datos específicos para el estado del componente de red. A este respecto, el cálculo se selecciona preferiblemente de tal manera que mediante el mismo se posibilita una comprobación al menos en su mayor parte de al menos la función relevante en cuanto a la seguridad, es decir una cobertura de función lo más amplia posible, del componente 10 de red. Siempre que no sea posible una cobertura de función completa o suficiente para el respectivo caso de aplicación por medio de un cálculo, entonces a este respecto pueden vincularse los resultados de diferentes cálculos.

Siempre que por medio del cálculo que comprueba el funcionamiento correcto del componente de red se compruebe únicamente una funcionalidad parcial del componente de red, dentro de un tiempo de divulgación de fallo predeterminada o predeterminable pueden realizarse de manera correspondiente cálculos adicionales, para conseguir como resultado en total una cobertura lo más completa posible de al menos las funcionales relevantes en cuanto a la seguridad o funcionalidad del componente 10 de red.

Los datos encriptados se transmiten desde el componente 10 de red en un etapa s3 de procedimiento como resultado de cálculo al dispositivo 20 de monitorización. Este o su dispositivo 21 de control comprueba ahora mediante el resultado de cálculo transmitido el estado del componente 10 de red así como la encriptación llevada a cabo por parte del componente 10 de red. Esto significa que para el dispositivo 20 de monitorización mediante el resultado de cálculo recibido y teniendo en cuenta un valor esperado para este resultado de cálculo, que puede haber calculado, por ejemplo, el propio dispositivo 20 de monitorización, es posible una comprobación amplia de la funcionalidad del componente 10 de red. Esto se refiere tanto a la correcta realización de la encriptación por medio de la clave de prueba como al valor de los datos específicos para el estado del componente de red. La comprobación correspondiente está asociada en la figura al dispositivo 21 de control y está identificada con el signo de referencia s4.

Dado que el dispositivo 20 de monitorización en la etapa s1 de procedimiento ha transmitido un mensaje de petición con la clave de prueba específica para el mensaje de petición en cuestión al componente 10 de red, se garantiza ventajosamente que el componente 10 de red haya calculado realmente de manera actual el resultado de cálculo y no recurra posiblemente a un resultado de cálculo anterior. Para aumentar la seguridad, el dispositivo 20 de monitorización y el componente 10 de red realizan además preferiblemente una autenticación mutua, que no se representa en la figura por motivos de claridad.

Desde el componente 10 de red puede transmitirse en el marco de la etapa s3 de procedimiento ventajosamente junto con el resultado de cálculo al menos un parámetro del componente 10 de red al dispositivo 20 de monitorización. Dado que el al menos un parámetro en cuestión se transmite directamente al dispositivo 20 de monitorización, se posibilita al mismo obtener informaciones adicionales sobre el componente 10 de red. En el caso del parámetro correspondiente puede tratarse, por ejemplo, de una indicación con respecto a casos de error registrados por el componente 10 de red, por ejemplo, en forma de la frecuencia de intentos de notificación sin éxito o la frecuencia de mensajes no autenticados. Siempre que se obtenga a este respecto una tendencia negativa o se supere un valor umbral, entonces por parte del dispositivo de monitorización puede tomarse una medida apropiada, por ejemplo, en el sentido de que se emita un aviso a una aplicación. Preferiblemente, al componente 10 de red, por ejemplo, en el marco de la etapa s1 de procedimiento se le puede notificar conjuntamente desde el dispositivo 20 de monitorización, qué parámetro o qué parámetros deben transmitirse desde el componente 10 de red junto con el resultado de cálculo al dispositivo 20 de monitorización.

Se indica que el componente 10 de red puede producir adicional o alternativamente también cualquier otra funcionalidad. Esto significa que en el caso del componente 10 de red puede tratarse de cualquier participante en una red de comunicación. También para un participante de este tipo, el procedimiento descrito anteriormente posibilita llevar a cabo una comprobación amplia de la funcionalidad del participante o del componente 10 de red correspondiente. Para ello, el componente 10 de red realiza preferiblemente una función lo más compleja posible como cálculo. Esta puede consistir, por ejemplo, en que se calcule una función *hash*, cuyo valor inicial depende de un código formado de manera actual a través del software y los datos específicos para el estado del componente 10 de red.

El procedimiento descrito anteriormente mediante ejemplos de realización así como la disposición asociada posibilitan ventajosamente una monitorización fiable del componente 10 de red mediante el dispositivo 20 de monitorización. Esto es relevante en particular en aquellos casos, en los que el componente 10 de red produce una función relevante en cuanto a la seguridad, pero sin estar implementado en sí mismo como dispositivo relevante en cuanto a la seguridad correspondiente, por ejemplo, según la norma DIN EN 50159. Por consiguiente, mediante una monitorización correspondiente, que transcurre preferiblemente de manera cíclica por medio del dispositivo 20 de monitorización se posibilita ventajosamente también la utilización de tales componentes de red 10 para aplicaciones relevantes en cuanto a la seguridad, por ejemplo, en el sector ferroviario.

REIVINDICACIONES

1. Procedimiento para monitorizar un componente (10) de red,

- en el que por parte del componente (10) de red usando datos específicos para un estado del componente (10) de red se realiza (s2) un cálculo que comprueba el funcionamiento correcto del componente (10) de red,

- en el que por parte del componente (10) de red se realiza el cálculo que comprueba el funcionamiento del componente (10) de red en forma de una encriptación de los datos específicos para el estado del componente (10) de red,

- en el que los datos encriptados se transmiten (s3) desde el componente (10) de red como resultado de cálculo al dispositivo (20) de monitorización,

- en el que el dispositivo (20) de monitorización comprueba mediante el resultado de cálculo transmitido el estado del componente (10) de red así como el funcionamiento correcto del mismo así como la encriptación llevada a cabo por parte del componente (10) de red,

- en el que desde el dispositivo (20) de monitorización se transmite un mensaje de petición con una clave de prueba específica para el respectivo mensaje de petición al componente (10) de red, y

- en el que por parte del componente (10) de red se encriptan los datos específicos para el estado del componente (10) de red para garantizar la actualidad del cálculo por medio de la clave de prueba.

2. Procedimiento según la reivindicación 1,

- en el que desde el dispositivo (20) de monitorización se transmite (s1) un mensaje de petición con al menos un parámetro específico para el respectivo mensaje de petición al componente (10) de red, y

- en el que por parte del componente (10) de red durante la realización del cálculo que comprueba el funcionamiento del componente (10) de red para garantizar la actualidad del cálculo se usa el al menos un parámetro específico para el respectivo mensaje de petición.

3. Procedimiento según una de las reivindicaciones anteriores, en el que como datos específicos para el estado del componente (10) de red se usan datos de configuración del componente (10) de red.

4. Procedimiento según una de las reivindicaciones anteriores, en el que como datos específicos para el estado del componente (10) de red se usan informaciones de estado del componente (10) de red.

5. Procedimiento según una de las reivindicaciones anteriores, en el que como datos específicos para el estado del componente (10) de red se usan datos específicos para el software del componente (10) de red.

6. Procedimiento según una de las reivindicaciones anteriores, en el que el dispositivo (20) de monitorización y el componente (10) de red llevan a cabo una autenticación mutua.

7. Procedimiento según una de las reivindicaciones anteriores, en el que desde el componente (10) de red junto con el resultado de cálculo se transmite al menos un parámetro del componente (10) de red al dispositivo (20) de monitorización.

8. Procedimiento según la reivindicación 7, en el que el al menos un parámetro del componente (10) de red que debe transmitirse desde el componente (10) de red al dispositivo (20) de monitorización se notifica conjuntamente por el dispositivo (20) de monitorización.

9. Procedimiento según la reivindicación 7 o 8, en el que el al menos un parámetro comprende una indicación con respecto a casos de error registrados por el componente (10) de red.

10. Disposición con un componente (10) de red y con un dispositivo (20) de monitorización,

- estando configurado el componente (10) de red

  - para realizar un cálculo que comprueba el funcionamiento correcto del componente (10) de red en forma de una encriptación de datos específicos para el estado del componente (10) de red así como

  - para transmitir los datos encriptados como resultado de cálculo al dispositivo (20) de monitorización, y

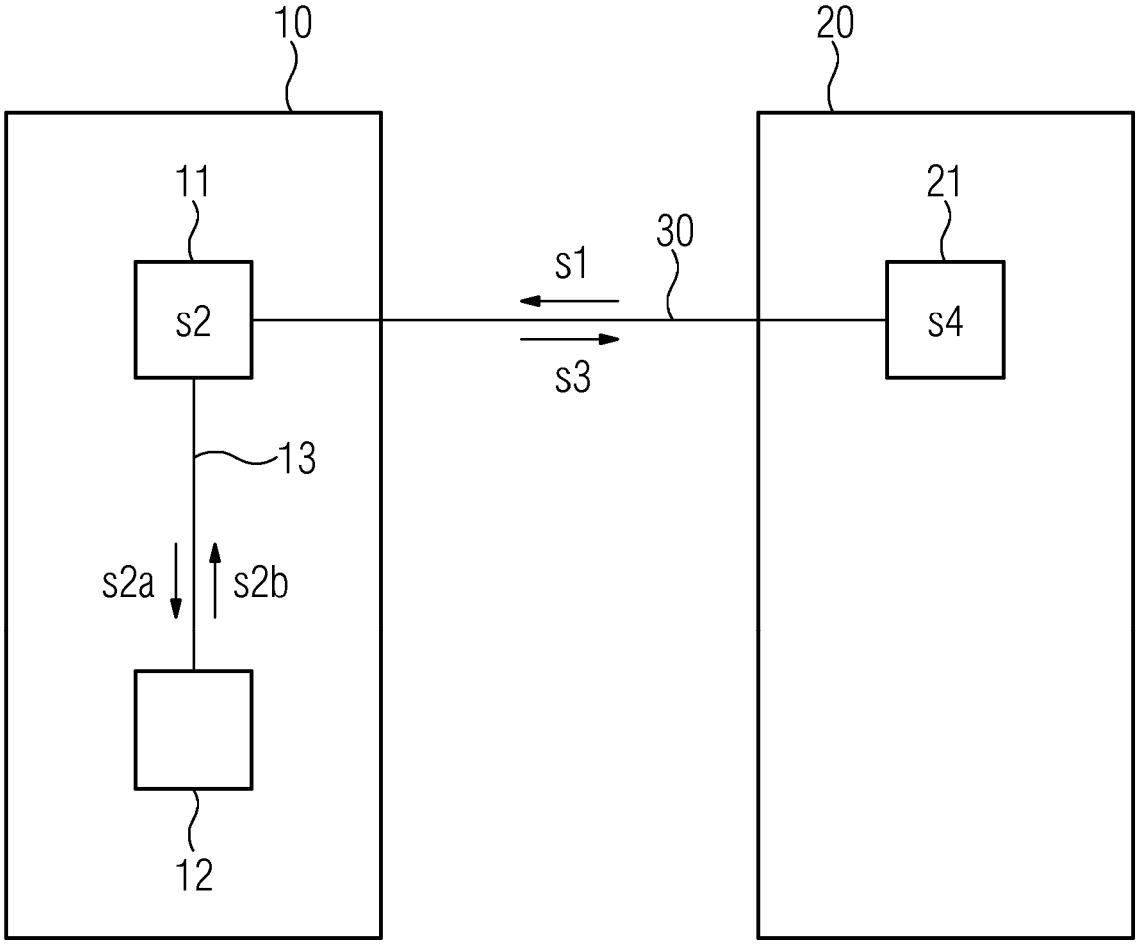
- estando configurado el dispositivo (20) de monitorización

  - para comprobar el estado del componente (10) de red así como la encriptación llevada a cabo por parte del componente (10) de red así como el funcionamiento correcto del mismo mediante el resultado de cálculo transmitido,

- estando configurado el dispositivo (20) de monitorización de tal manera que desde el dispositivo (20) de monitorización se transmite un mensaje de petición con una clave de prueba específica para el respectivo mensaje de petición al componente (10) de red,

- estando configurado el componente (10) de red de tal manera que por parte del componente (10) de red se encriptan los datos específicos para el estado del componente (10) de red para garantizar la actualidad del cálculo por medio de la clave de prueba.

11. Disposición según la reivindicación 10, en la que el componente (10) de red y el dispositivo (20) de monitorización están configurados para la realización del procedimiento según una de las reivindicaciones 1 a 9.


10
20
11
21
30
s1
s2
s4
s3
13
s2a
s2b
12