(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 810 150**

(51) Int. CI.:

G06F 21/44 (2013.01)
H04L 29/06 (2006.01)
H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **13.09.2017 E 17190811 (4)**

(97) Fecha y número de publicación de la concesión europea: **03.06.2020 EP 3306507**

(54) Título: **Componente para una cadena funcional crítica para la seguridad**

(30) Prioridad:

04.10.2016 DE 102016219204

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.03.2021

(73) Titular/es:

MBDA DEUTSCHLAND GMBH (100.0%)
Hagenauer Forst 27
86529 Schrobenhausen, DE

(72) Inventor/es:

WAGNER, DIETER

(74) Agente/Representante:

SALVÀ FERRER, Joan

DESCRIPCIÓN

Componente para una cadena funcional crítica para la seguridad

[0001] La presente invención se refiere a una cadena funcional crítica para la seguridad, que presenta varios componentes concatenados mediante enlaces de comunicación para proporcionar una función de seguridad.

[0002] Los sistemas que incluyen cadenas funcionales críticas para la seguridad pueden presentar una pluralidad de componentes. Para certificar o recertificar las cadenas funcionales críticas para la seguridad, la certificación se lleva a cabo a través de un organismo de certificación. La certificación de un producto o de un componente se realiza a petición del fabricante o de un distribuidor. Los procedimientos de certificación convencionales incluyen el examen técnico o la evaluación de los componentes según criterios específicos. El examen técnico puede ser realizado por un organismo de inspección reconocido por el organismo de certificación. Se comprueba el cumplimiento de los requisitos para el producto o componente en cuestión, el entorno de desarrollo, la documentación de usuario y el funcionamiento del componente en cuestión. La duración de un procedimiento de certificación depende de la complejidad de los componentes en cuestión y de la profundidad de las pruebas. El resultado del procedimiento de certificación se registra en un informe de certificación. Este informe de certificación contiene, entre otras cosas, un documento de certificado de seguridad y un informe de certificación detallado. En el caso de cambios relevantes para la seguridad de un componente o de los procesos de desarrollo del componente, el componente debe ser certificado nuevamente o recertificado. Con cada cambio dentro de una cadena funcional crítica para la seguridad, que comprende varios componentes concatenados, expira la autorización de explotación para toda la cadena funcional crítica para la seguridad, que solo puede recuperarse mediante una recertificación compleja.

[0003] El documento US 2007/0143629 A1 describe una plataforma de usuario que puede certificarse para acceder a un servicio o una aplicación en una red. El documento EP 2 814 277 A1 describe un mecanismo de verificación para componentes certificables.

[0004] Por lo tanto, es un objeto de la presente invención simplificar la certificación o recertificación de una cadena funcional crítica para la seguridad. Este objeto se logra mediante un sistema con las características especificadas en la reivindicación 1.

[0005] A continuación, se describirán en detalle las posibles realizaciones de los diversos aspectos según la invención con referencia a las figuras adjuntos.

[0006] La invención se define por las reivindicaciones adjuntas.

[0007] Muestran:

Fig. 1 un diagrama esquemático de bloques que explica el modo de funcionamiento de un procedimiento para certificar una cadena funcional crítica para la seguridad;

Fig. 2 un diagrama de flujo que ilustra un posible procedimiento ejemplar para certificar una cadena funcional crítica para la seguridad según el primer aspecto de la invención;

Fig. 3 un diagrama de flujo de señal para ilustrar un ejemplo de un procedimiento para certificar una cadena funcional crítica para la seguridad;

Las figuras 4 y 5 son representaciones esquemáticas de posibles cadenas funcionales críticas para la seguridad;

Fig. 6 muestra una representación esquemática de una realización ejemplar de un sistema en el que se puede usar el procedimiento para certificar una cadena funcional crítica para la seguridad;

Fig. 7 una representación esquemática para explicar una posible secuencia de una verificación de la certificación en el sistema que se muestra en la Fig. 6;

Fig. 8 una representación esquemática de una posible secuencia de una verificación de la certificación al renovar un componente del sistema que se muestra en la Fig. 6;

Fig. 9 una representación esquemática de una posible secuencia con resultado negativo de una verificación de la certificación de un componente renovado dentro del sistema que se muestra en la Fig. 6;

Fig. 10 una representación esquemática de un procedimiento para proporcionar un enlace de comunicación entre componentes de una cadena funcional crítica para la seguridad;

Fig. 11 un diagrama de señales para representar un ejemplo del procedimiento que se muestra en la Fig. 10 para

proporcionar un enlace de comunicación seguro entre los componentes de una cadena funcional crítica para la seguridad;

Fig. 12 representación esquemática de la activación de una interfaz entre dos componentes de una cadena funcional crítica para la seguridad;

Fig. 13 otra representación esquemática para explicar la activación de un componente periférico de una cadena funcional crítica para la seguridad;

Fig. 14 muestra una ilustración esquemática de un componente según la invención para una cadena funcional crítica para la seguridad;

Fig. 15 muestra una ilustración esquemática adicional de una realización ejemplar de un componente según la invención para una cadena funcional crítica para la seguridad;

Fig. 16 un diagrama de estructura de datos de un ejemplo de realización de certificado que puede usarse para los componentes según la invención que se muestran en las figuras 14, 15.

[0008] La Fig. 1 muestra una cadena funcional 1 que comprende varios componentes según la invención 2-1, 2-2... 2-M. Los componentes están unidos entre sí mediante enlaces de comunicación. Los componentes 2-i pueden ser componentes de hardware y/o componentes de software. En el ejemplo de realización de la Fig. 1, la cadena funcional 1 está formada por varios componentes en serie para realizar una función de seguridad. La cadena funcional 1 proporciona una función que puede poner en peligro la salud de una persona en caso de fallo. Para conectar los componentes, cada uno de ellos presenta interfaces, tal como se muestra en la Fig. 1. Estas pueden ser interfaces de hardware o interfaces de software. En el ejemplo de realización mostrado, cada uno de los componentes 2-i de la cadena funcional crítica para la seguridad 1 presenta una interfaz de componentes de salida 4-i del componente, que en cada caso está conectada con la siguiente interfaz de componentes de entrada 3-(i+1) del componente adyacente 2-(i+1) a través de un enlace de comunicación de forma inalámbrica y/o por cable 5-i. Los enlaces de comunicación 5-i son preferentemente unidireccionales, es decir, cuando se establece un enlace de comunicación, los datos o mensajes se transmiten desde una interfaz de componentes de salida a la interfaz de componentes de entrada del siguiente componente adyacente en una dirección, de modo que existe una relación de causalidad dentro de la cadena funcional crítica para la seguridad.

[0009] Los componentes 2-i de la cadena funcional crítica para la seguridad 1 pueden comunicarse bidireccionalmente con un gestor de certificados de seguridad 6, tal como se muestra en la Fig. 1. La comunicación con el administrador de certificados de seguridad 6 puede realizarse a través de conexiones de comunicación separadas en una posible realización. De forma alternativa, la comunicación con el gestor de certificados de seguridad 6 puede realizarse a través de las conexiones de comunicación 5-i. Esto puede, por ejemplo, alimentar mensajes de solicitud o solicitudes de certificados de seguridad a través de la primera interfaz de entrada 3-1 de la cadena funcional crítica para la seguridad 1 y obtener certificados de seguridad de la interfaz de componentes de salida 4-M del último componente 2-M presente dentro de la cadena de funcional crítica para la seguridad 1.

[0010] En una posible realización, el gestor de certificados de seguridad 6 forma un componente separado fuera de la cadena funcional crítica para la seguridad 1, tal como se muestra en la Fig. 1. En una realización alternativa, el gestor de certificados de seguridad 6 está integrado en uno de los componentes 2-i de la cadena funcional crítica para la seguridad 1. Para cada uno de los componentes 2- i de la cadena funcional crítica para la seguridad 1 se ha previsto como mínimo un certificado de seguridad de componentes KSZ. Además, cada interfaz de componentes, es decir, cada interfaz de componentes de entrada 3-i y cada interfaz de componentes de salida 4-i, posee un certificado de seguridad de interfaz SSZ asociado. Los certificados de seguridad de componentes KSZ y los certificados de seguridad de interfaz SSZ son certificados digitales que pueden almacenarse en un área de la memoria. El gestor de certificados de seguridad 6 tiene acceso a los certificados de seguridad de componentes KSZ de los componentes 2-i concatenados dentro de la cadena funcional 1 y a los certificados de seguridad de interfaz SSZ de las interfaces concatenadas. Esto permite una verificación central de los certificados digitales por parte del gestor de certificados de seguridad 6 de la cadena funcional crítica para la seguridad 1. El gestor de certificados de seguridad 6 puede llevar a cabo una certificación o recertificación automática central sobre la base de determinados requisitos de seguridad para la cadena funcional crítica para la seguridad 1. Si el gestor de certificados de seguridad 6 realiza correctamente la verificación del certificado de seguridad de componentes y la verificación del certificado de seguridad de interfaces, el gestor de certificados de seguridad 6 autoriza de forma automática los componentes 2-i de la cadena funcional crítica para la seguridad 1. Si la totalidad de todos los certificados, es decir, los certificados de seguridad de componentes KSZ y todos los certificados de seguridad de interfaces SSZ cumplen los requisitos de seguridad para la cadena funcional crítica para la seguridad 1, el gestor de certificados de seguridad 6 autoriza los diversos componentes 2-i de la cadena funcional crítica para la seguridad 1. Los componentes de la cadena funcional crítica para la seguridad 1 proporcionan una función de seguridad para una posible realización.

[0011] La Fig. 2 muestra un diagrama de flujo que ilustra un ejemplo de realización de un procedimiento para

certificar una cadena funcional crítica para la seguridad 1 según el primer aspecto de la invención. El procedimiento sirve para certificar o recertificar una compleja cadena funcional crítica para la seguridad 1, que tiene una pluralidad de componentes concatenados a través de enlaces de comunicación para proporcionar una función de seguridad. En la etapa S1, un gestor de certificados de seguridad 6 realiza una verificación del certificado de seguridad de componentes del componente. Los certificados de seguridad de componentes KSZ de los componentes concatenados 2-i son verificados por el gestor de certificados de seguridad 6 en base a los requisitos de seguridad especificados. Los requisitos de seguridad pueden almacenarse en un almacén de datos del gestor de certificados de seguridad 6 o introducirse a través de una interfaz. Los requisitos de seguridad pueden definirse por niveles de seguridad. Los certificados de seguridad de componentes KSZ indican un nivel de seguridad de componentes KSL del componente 2-i correspondiente dentro de la cadena funcional crítica para la seguridad 1. Además, los certificados de seguridad de interfaz SSZ de las distintas interfaces de componentes especifican cada una un nivel de seguridad de interfaz SSL de la interfaz de componentes respectiva. Durante la verificación de la certificación de seguridad de componentes en la etapa S1, el gestor del certificado de seguridad 6 comprueba si un nivel de seguridad del componente KSL, especificado en el certificado de seguridad de componentes KSZ correspondiente del componente 2-i correspondiente, es adecuado o suficiente para un nivel de seguridad de componentes KSL correspondiente del componente 2-i correspondiente requerido conforme a los requisitos de seguridad especificados.

[0012] En una etapa más, S2, el gestor de certificados de seguridad 6 realiza una verificación de la certificación de seguridad de interfaces. Durante la verificación de la certificación de seguridad de interfaces, se comprueban los certificados de seguridad de interfaces SSZ de las dos interfaces de componentes 4, 3 de dos componentes adyacentes 2-i, 2-(i+1) conectadas mediante un enlace de comunicación 5 dentro de la cadena funcional crítica para la seguridad 1 para ver si los niveles de seguridad de interfaz SSL especificados son compatibles o adecuados entre sí. En una posible realización, un certificado de seguridad de interfaces SSZ de una interfaz de componentes especifica un nivel mínimo de seguridad de interfaz SSL_{MIN} y/o un nivel máximo de seguridad de interfaz SSL_{MAX} de la interfaz de componente respectiva. En una realización, en el curso de la verificación del certificado de interfaz en la etapa S2, se verifica si el nivel de seguridad de interfaces SSL-AUS ofrecido o proporcionado por la interfaz de componentes de salida 4 de un primer componente 2-i que está especificado en el certificado de seguridad de interfaz SSZ de la interfaz de componentes de salida 4-i de un componente 2-i es suficiente para un nivel de seguridad de componentes SSL-EIN requerido por una interfaz de componentes de entrada 3-(i+1) del siguiente componente 2-(i+1), que se especifica en el certificado de seguridad de interfaz SSZ de la interfaz de componentes de entrada 3-(i+1) del siguiente componente 2-(i+1). Por ejemplo, si el nivel de seguridad de interfaces SSL de la interfaz del componente de salida 4-i del primer componente 2-i es mayor o igual que el nivel de seguridad de interfaces SSL requerido por la interfaz del componente de entrada 3-(i+1) del segundo componente 2-(i+1), se realizó correctamente la verificación del certificado de seguridad de interfaz en la etapa S2 en este punto de la cadena de funcional 1. Si, por ejemplo, el nivel de seguridad de interfaces SSL ofrecido por la interfaz del componente de salida 4-i del primer componente 2-i, que está especificado en el certificado de seguridad de interfaces SSZ de la interfaz del componente de salida 4-i de un componente 2-i, tiene un valor 5, (SSL -AUS = 5) y tiene el nivel de seguridad de la interfaz SSL requerido por la interfaz del componente de entrada 3-(i+1) del siguiente componente 2-(i+1) que está especificado en el certificado de seguridad de interfaces SSZ de la interfaz del componente de entrada 3-(i+1) del segundo componente 2-(i+1) adyacente tiene un valor de 4 (SSL-EIN = 4), los dos niveles de seguridad de interfaces SSL de las dos interfaces de componente son compatibles, de modo que la validación del certificado de seguridad de la interfaz se puede realizar satisfactoriamente en este punto. Los certificados de seguridad de componentes KSZ y los certificados de seguridad de interfaces SSZ de las interfaces de componentes usados en la etapa S1, que se usan en la etapa S2, se almacenan preferentemente en una memoria de datos a prueba de manipulaciones indebidas y pueden transmitirse al gestor de certificados de seguridad 6 para su verificación.

[0013] En la etapa S3, el gestor de certificados de seguridad 6 realiza una autorización de componentes si la verificación de certificados de componentes en la etapa S1 y la verificación de certificados de seguridad de interfaces en la etapa S2 se realizan correctamente. Después de habilitar los componentes 2-i dentro de la cadena funcional crítica para la seguridad 1, los distintos componentes 2-i pueden activar sus interfaces de componentes, es decir, las interfaces de componentes de entrada 3-i y las interfaces de componentes de salida 4-i, de modo que se activa la cadena funcional crítica para la seguridad 1 en su conjunto.

[0014] La Fig. 3 muestra un diagrama de flujo de señal de un ejemplo de realización del procedimiento para certificar una cadena funcional crítica para la seguridad 1. En primer lugar, el gestor de certificados de seguridad 6 transmite una solicitud a los componentes 2-i de la cadena funcional crítica para la seguridad 1, donde el gestor de certificados de seguridad 6 solicita sus certificados digitales a los componentes de la cadena funcional crítica para la seguridad 1. El gestor de certificados de seguridad 6 puede solicitar los certificados de los componentes 2-i en paralelo o simultáneamente, tal como se muestra en la Fig. 3, o uno tras otro. En el ejemplo mostrado, gestor de certificados de seguridad 6 primero le solicita al primer componente 2-1 que transfiera su certificado de seguridad de componentes KSZ1 y los diversos certificados de seguridad de interfaces SSZ para las distintas interfaces de componentes del componente 2-1. Cada componente 2-i puede tener un número N de interfaces de componentes. En el ejemplo que se muestra en la Fig. 1, cada componente 2-i de la cadena funcional crítica para la seguridad 1 posee dos interfaces de componentes, es decir, una interfaz de componentes de entrada 3-i y una interfaz de componentes de salida 4-i. Por tanto, en el ejemplo que se muestra en la Fig. 1, cada componente 2-i posee dos certificados de seguridad de

interfaces SSZ. En general, cada componente 2-i posee un número especificado N de interfaces de componentes y un número correspondiente N de certificados de seguridad de interfaces SSZ asociados. El primer componente 2-1, que posee interfaces de componentes N1, envía un número N1 correspondiente de certificados de seguridad de interfaz SSZ al gestor de certificados de seguridad solicitante 6. El siguiente componente 2-2 transfiere su certificado de seguridad de componentes KSZ2 y N2 certificados de interfaces SSZ para sus N2 interfaces de componentes al gestor de certificados de seguridad 6 de manera correspondiente. De este modo, el gestor de certificados de seguridad 6 recibe gradualmente los certificados de seguridad de componentes KSZ y todos los certificados de seguridad de interfaz SSZ de los distintos componentes 2-i, tal como se muestra en la Fig. 3. Sobre la base de los certificados de seguridad de interfaz de componentes KSZ y los certificados de seguridad de interfaces SSZ, el gestor de certificados de seguridad 6 realiza una verificación de la certificación de seguridad. En este caso, se verifica preferentemente si un nivel de seguridad de componentes KSL del componente 2 especificado en el certificado de seguridad de componentes KSZ del componente respectivo es suficiente para el nivel de seguridad del componente conforme a los requisitos de seguridad especificados. En el curso de la verificación de la certificación de seguridad de interfaces en la etapa S2, los certificados de seguridad de interfaz SSZ de los dos componentes adyacentes dentro de la cadena funcional crítica para la seguridad 1 se verifican para determinar si los niveles de seguridad de interfaz SSL coinciden entre sí o son compatibles. Si tanto la verificación de la certificación de seguridad de componentes en la etapa S1 como la verificación de la certificación de seguridad de interfaces en la etapa S2 son satisfactorias, el gestor de certificados de seguridad 6 autoriza los componentes 2-i de la cadena funcional crítica para la seguridad 1. Para ello, el gestor de certificados de seguridad 6 puede enviar mensajes de autorización F1, F2... F_m a los diferentes componentes 2-i de la cadena funcional crítica para la seguridad 1, tal como se muestra en la Fig. 3. Si todos los certificados cumplen los requisitos de seguridad, el gestor de certificados de seguridad 6 autoriza los componentes individuales 2-i de la cadena funcional crítica para la seguridad 1. A continuación, los diversos componentes 2-i de la cadena funcional crítica para la seguridad 1 activan sus interfaces de componentes y proporcionan la función de seguridad deseada. Si un certificado digital de un componente 2-i no cumple los requisitos de seguridad requeridos, el gestor de certificados de seguridad 6 puede bloquear el componente correspondiente dentro de la cadena de funcional 1 crítica para la seguridad.

[0015] Las figuras 4 y 5 muestran otros ejemplos de sistemas o instalaciones que contienen cadenas funcionales 1 críticas para la seguridad. En el ejemplo de la Fig. 1, el sistema posee una única cadena funcional lineal crítica para la seguridad 1 con componentes de hardware o software 2-i concatenados en serie. Todos los componentes 2-i tienen una interfaz de componentes de entrada 3-i y una interfaz de componentes de salida 4-i. Tal como se muestra en la Fig. 4, cada componente puede presentar también varias interfaces de componentes. Por ejemplo, el segundo componente 2-2 posee dos interfaces de componentes de salida 4A-2, 4B-2. Esto da como resultado dos cadenas funcionales críticas para la seguridad 1 dentro del sistema, es decir, una primera cadena funcional crítica para la seguridad 1, formada a partir de los componentes encadenados 2-1, 2-2, 2-3, y una segunda cadena funcional crítica para la seguridad 1, formada a partir de los componentes encadenados 2-1, 2-2, 2-4, 2-5.

[0016] Además, los componentes también pueden presentar varias interfaces de componentes de entrada, tal como se muestra, por ejemplo, en la Fig. 5. Por ejemplo, el componente 2-5 posee dos interfaces de componentes de entrada 3A-5, 3B-5. En este sistema, hay, por lo tanto, tres cadenas funcionales críticas para la seguridad 1, es decir, una primera cadena funcional crítica para la seguridad que consiste en los componentes 2-1, 2-2, 2-3, 2-4, y una segunda cadena funcional crítica para la seguridad que consiste en los componentes 2-1, 2-2, 2-3, 2-5 y otra cadena funcional crítica para la seguridad que consiste en los componentes 2-1, 2-2, 2-5, que se prueban y certifican por separado por el gestor de certificados de seguridad 6. La autorización del sistema se produce después de que todas las cadenas funcionales 1 hayan sido comprobadas satisfactoriamente por el gestor de certificados de seguridad 6 con respecto a los requisitos de seguridad. Dentro del sistema, dos interfaces de componentes de dos componentes adyacentes se comunican entre sí. El enlace de comunicación puede ser una conexión inalámbrica, por ejemplo, WLAN, o una conexión por cable, por ejemplo, un bus de datos en serie o paralelo.

[0017] La Fig. 6 muestra un ejemplo de realización de un sistema técnico con una cadena funcional crítica para la seguridad 1 compuesta por varios componentes de hardware y software 2 concatenados. Un brazo robótico industrial de un sistema de producción cumple una función crítica para la seguridad, ya que una persona que se encuentre en las proximidades del robot industrial puede estar en peligro. El brazo robótico industrial está controlado por componentes de hardware y software que se conectan en serie en una cadena funcional. Una unidad de interfaz de usuario 2-1 está conectada a una unidad de control del sistema. Para ello, la unidad de interfaz de usuario 2-1 presenta una interfaz de componentes de salida que se conecta a una interfaz de componentes de entrada del control del sistema. El control del sistema contiene un microprocesador que ejecuta un programa de control como componente de software 2-2. El enlace de comunicación entre la interfaz de entrada de usuario 2-1 y el componente de software 2-2 se establece a través de las líneas de control y de datos 5-1. El control de sistemas del sistema controla otro componente de software 2-3 a través de una red de datos como enlace de comunicación 5-2, que se implementa en un control de brazo robótico local del sistema de producción. El componente de software 2-3 controla a su vez el brazo robótico como componente de hardware 2-4, tal como se muestra en la Fig. 6. El brazo del robot, por ejemplo, tiene en su punta un dispositivo para retirar varias herramientas o útiles para llevar a cabo los pasos de producción dentro del sistema de producción. El brazo robótico 2-4 extrae herramientas o útiles 2-5A, 2-5B de un dispositivo de sujeción de herramientas. En el ejemplo de realización del sistema de producción mostrado, la cadena funcional crítica para la

seguridad 1 comprende el componente 2-1, los dos componentes de software 2-2, 2-3 y el brazo robótico como componente de hardware 2-4. En el ejemplo mostrado, la cadena funcional crítica para la seguridad 1 puede ampliarse con un componente de hardware durante el funcionamiento, donde el componente de hardware adicional es la herramienta 2-5A o la herramienta 2-5B.

[0018] La Fig. 7 muestra esquemáticamente el sistema de producción mostrada en la Fig. 6 para explicar el procedimiento de certificación. Cada componente 2-i de la cadena funcional crítica para la seguridad 1 dispone al menos de un certificado de seguridad con el número de versión V1.0. Los diferentes componentes 2-i representan componentes relevantes para la seguridad dentro de la cadena funcional crítica para la seguridad 1, que están concatenados o enlazados en serie. El gestor de certificados de seguridad 6 comprueba los diferentes certificados de seguridad de los diferentes componentes relevantes para la seguridad. El gestor de certificados de seguridad 6 solicita los certificados de seguridad digitales correspondientes de los componentes individuales relevantes para la seguridad 2-i, por ejemplo, de la unidad de interfaz de usuario 2-1. Los certificados de seguridad comprenden certificados de seguridad de componentes KSZ y certificados de seguridad de interfaz SSZ. En otra etapa, los certificados digitales solicitados y transferidos al gestor de certificados de seguridad 6 son comprobados por el gestor de certificados de seguridad 6 con respecto al cumplimiento de los requisitos de seguridad especificados.

[0019] Una vez finalizada de manera satisfactoria la verificación de la certificación de seguridad de componentes y la verificación de la certificación de seguridad de la interfaz del componente respectivo, se autoriza el componente 2-1 relevante para la seguridad. Tan pronto como todos los componentes han sido verificados por el gestor de certificados de seguridad 6, se activan las distintas interfaces de componentes de los componentes relevantes para la seguridad 2-i, con lo cual la cadena funcional crítica para la seguridad 1 está lista para funcionar. El proceso de certificación de la cadena funcional crítica para la seguridad 1 puede tener lugar, por ejemplo, durante la puesta en marcha del sistema de producción que se muestra en la Fig. 6. La certificación de la cadena funcional crítica para la seguridad 1 se realiza preferentemente de forma automática en respuesta a un hecho desencadenante detectado. Para una posible realización, el hecho desencadenante es la puesta en servicio de al menos un componente 2-i dentro de la cadena funcional 1 crítica para la seguridad. En otra una posible realización, el hecho desencadenante para el proceso de certificación es un cambio del estado operativo de al menos un componente 2-i dentro de la cadena funcional crítica para la seguridad 1. Preferentemente, el hecho desencadenante es registrado automáticamente por el gestor de certificados de seguridad 6. El gestor de certificados de seguridad 6 realiza el proceso de certificación durante la puesta en funcionamiento o cuando se pone en marcha el sistema de producción. Además, el gestor de certificados de seguridad 6 supervisa preferentemente los distintos componentes relevantes para la seguridad dentro de la cadena funcional crítica para la seguridad 1, con el fin de detectar automáticamente un cambio relevante en el estado operativo e iniciar el proceso de certificación. Además, en una posible realización, los sensores pueden detectar que un componente 2 dentro de la cadena funcional crítica para la seguridad 1 es sustituido o cambiado por otro componente. Además, el gestor de certificados de seguridad 6 puede reconocer en una posible realización la ejecución de un proceso de actualización de software para un componente de software dentro de la cadena funcional crítica para la seguridad 1 e iniciar el proceso de certificación.

[0020] La Fig. 8 muestra esquemáticamente un proceso de recertificación según el procedimiento de certificación después de una actualización de software del componente de software 2-2 del sistema de producción. Con la ayuda del procedimiento de certificación según la invención, la verificación de la certificación de componentes 2-2 del software relevante para la seguridad se realiza de forma automática. En el caso de una actualización de software del componente de software, el componente de software se recertifica de forma aislada dentro de la cadena funcional crítica para la seguridad 1 mediante el procedimiento según la invención. Recibirá un nuevo certificado digital con el número de versión V1.1. Tan pronto como el nuevo componente de software, en particular actualizado, de la cadena funcional 1 haya recibido del gestor de certificados de seguridad 6 un certificado con el número de versión V1.1, esto se verifica de forma automática conforme a los requisitos de seguridad del sistema. Después de una recertificación satisfactoria, los diferentes componentes 2-i del sistema son autorizados por el gestor de certificados de seguridad 6 y las interfaces de los componentes asociados se activan automáticamente para que la cadena de funcional 1 esté lista para funcionar dentro del sistema.

[0021] La Fig. 9 muestra una verificación de la certificación con resultado negativo según el procedimiento de certificación. En el ejemplo, el componente de software 2-2 se actualiza de nuevo. En la actualización del componente 2-2, el componente es primero recertificado de forma aislada y recibe un certificado de seguridad con el número de versión V1.2, tal como se muestra en la Fig. 9. Tan pronto como el componente de software 2-2 nuevo o actualizado sea instalado dentro de la cadena funcional crítica para la seguridad 1, el nuevo certificado de seguridad V1.2 del componente relevante para la seguridad 2-2 es consultado por el gestor de certificados de seguridad 6 y comprobado de forma automáticamente conforme a los requisitos de seguridad especificados del sistema. En el ejemplo mostrado, el nuevo certificado V1.2 no cumple los requisitos de seguridad, por lo que el gestor de certificados de seguridad 6 desactiva automáticamente los componentes 2-i de la cadena funcional crítica para la seguridad 1. A continuación, puede tener lugar un tratamiento de errores. Los requisitos de seguridad para la cadena funcional crítica para la seguridad 1 pueden, por ejemplo, redefinirse y almacenarse en el gestor de certificados de seguridad 6.

[0022] Los certificados de seguridad de componentes KSZ y los certificados de seguridad de interfaces SSZ

presentan en una posible realización cada uno el nivel de seguridad SL. Los niveles de seguridad de los componentes KSL, que están especificados en los certificados de seguridad de componentes KSZ de los componentes 2-i, y/o los niveles de seguridad de interfaz SSL, que están especificados en los certificados de seguridad de interfaz SSZ de las interfaces de los componentes 2-i, están preconfigurados para los respectivos componentes relevantes para la seguridad en una posible realización. En una realización alternativa, el nivel de seguridad de componentes KSL y/o el nivel de seguridad de interfaz SSL puede cambiar en función de las condiciones ambientales y/o de los estados de funcionamiento de los componentes 2-i dentro de la cadena funcional crítica para la seguridad 1. Por ejemplo, un componente relevante para la seguridad 2-i posee un alto nivel de seguridad de componentes KSL1 en el primer estado operativo del componente 2-i y un bajo nivel de seguridad de componentes KSL2 en otro estado operativo. Además, el estado operativo de un componente 2-i también puede afectar al nivel de seguridad de interfaces SSL de las distintas interfaces de ese componente. Por ejemplo, una interfaz de componentes de un componente 2-i posee un nivel de seguridad de interfaz SSL1 relativamente alto en un primer estado operativo del componente y un nivel de seguridad de interfaz SSL2 relativamente bajo en otro estado operativo del componente. El nivel de seguridad de componentes KSL y el nivel de seguridad de interfaz SSL pueden, por lo tanto, puede cambiar dinámicamente con esta versión en función de los estados operativos y/o de las condiciones ambientales. En una posible realización, las condiciones ambientales del sistema son registradas sensorialmente por el gestor del certificado de seguridad 6. Las condiciones ambientales comprenden, por ejemplo, parámetros ambientales físicos tales como la temperatura o la presión. Las condiciones ambientales también pueden comprender la posición o ubicación del componente o de todo el sistema, que también tienen influencia sobre los requisitos de seguridad utilizados. Por ejemplo, un sistema en un primer intervalo de temperatura requiere un nivel de seguridad diferente al de un sistema en un intervalo de temperatura diferente. Un componente ubicado en una primera ubicación puede tener requisitos de seguridad más altos que un componente que se encuentra en otra ubicación. En una realización, los componentes 2-i concatenados en la cadena funcional 1 están instalados de forma permanente y situados en el mismo lugar. En una realización alternativa, los componentes 2-i concatenados dentro de la cadena funcional 1 cambian su posición actual con respecto a los demás. Estos componentes se conectan preferentemente con componentes adyacentes a través de enlaces de comunicación inalámbricos, donde el movimiento del componente 2-i puede cambiar el nivel de seguridad de componentes KSL del componente y/o el nivel de seguridad de interfaz SSL de las diversas interfaces del componente 2-i en cuestión. En una realización, el nivel de seguridad de componentes KSL y el nivel de seguridad de interfaz SSL se reducen o disminuyen con el tiempo. Esto refleja, por ejemplo, el tiempo de funcionamiento del componente. Por ejemplo, el nivel de seguridad de componentes KSL de un componente se reduce anualmente. A partir de un determinado momento, el nivel de seguridad de componentes KSL del componente ya no satisface el nivel de seguridad de este componente conforme a los requisitos de seguridad especificados del sistema. Entonces se puede indicar, por ejemplo, que el componente en cuestión debe ser reparado o reemplazado y que el sistema debe ser recertificado.

[0023] Los certificados de seguridad de componentes KSZ de un componente se almacenan en una memoria de datos a prueba de manipulaciones indebidas y son leídos por el gestor de certificados de seguridad 6. El certificado de seguridad de componentes KSZ de un componente 2 contiene diversas informaciones que pueden variar según la aplicación. En una posible realización, el certificado de seguridad de componentes KSZ de un componente 2 dentro de la cadena funcional crítica para la seguridad 1 presenta algunos de los siguientes campos de datos, es decir, un número de versión V y una fecha de caducidad, que son comprobados por el gestor del certificado de seguridad 6 para determinar si el certificado sigue siendo válido. El emisor del certificado de seguridad de componentes KSZ se especifica en otro campo de datos. El certificado indicará preferentemente un tipo de componente en cuestión, por ejemplo, si se trata de un componente de software o de un componente de hardware. Además, está preferentemente incluido un nivel de seguridad de componentes KSL del componente 2 respectivo. El nivel de seguridad puede configurarse de forma permanente o modificarse, por ejemplo, en función de las condiciones ambientales o de los estados de funcionamiento de los componentes 2. El certificado de seguridad de componentes KSZ comprende preferentemente una identificación del fabricante del componente. Por ejemplo, en un equipo determinado, solo pueden estar autorizados componentes de un fabricante determinado. Además, el certificado de seguridad de componentes KSZ contiene preferentemente una identificación única del componente en cuestión. Además, el certificado de seguridad de componentes KSZ incluye certificados de seguridad de interfaz SSZ proporcionados para interfaces de componentes del componente con los niveles de seguridad de interfaz correspondientes. Además, el certificado de seguridad de componentes KSZ también comprende preferentemente los certificados de seguridad de interfaz SSZ requeridos para las interfaces de componentes de entrada del componente con un nivel de seguridad de interfaz SSL de la interfaz de componentes de entrada requerido en cada caso. Esto le permite al gestor del certificado de seguridad 6 comprobar si los niveles de seguridad coinciden o son compatibles. Además, el certificado de seguridad de interfaz de componentes KSZ del componente 2 puede incluir varios parámetros de configuración del componente en cuestión. Por ejemplo, los parámetros de configuración pueden especificar una potencia láser autorizada de un brazo robótico dentro de la línea de producción. Un brazo robótico, por ejemplo, solo tiene permiso de funcionamiento para 50 KW, incluso si técnicamente ofrece una potencia de 100 KW. Cada componente 2 dentro de la cadena funcional crítica para la seguridad 1 lleva su documentación de autorización en forma de un certificado digital de seguridad de componentes KSZ. Preferentemente, el certificado digital asociado se almacena para cada componente 2 en un área de memoria infalsificable prevista especialmente. Este solo puede ser leído y comprobado por un gestor de certificados 6 de seguridad previsto a tal efecto. Con la ayuda de certificados digitales de lectura electrónica, la certificación o recertificación de la cadena funcional crítica para la seguridad 1 también puede llevarse a cabo de forma

automática durante el tiempo de ejecución.

[0024] Con el sistema que se muestra en la Fig. 6, la cadena funcional crítica para la seguridad 1 se puede acortar o ampliar de manera dinámica. Por ejemplo, la cadena funcional crítica para la seguridad 1 se amplía con la inclusión de la herramienta 2-5A. Esta representa preferentemente un hecho desencadenante que desencadena un proceso de certificación por parte del gestor de certificados de seguridad 6. El gestor de certificados de seguridad 6 lleva a cabo una recertificación de la cadena funcional crítica para la seguridad 1 ampliada. Con la entrega de la herramienta 2-5A, la cadena funcional 1 se acorta por un componente de hardware. En una posible realización, esto puede desencadenar un proceso de recertificación nuevo durante el funcionamiento del sistema.

[0025] Un usuario también puede ser incluido en el proceso de recertificación. Por ejemplo, el usuario U puede ser considerado como un componente que dispone de un certificado de seguridad. El certificado de seguridad de una persona o de un usuario difiere de un certificado de seguridad de un componente de hardware o software convencional. Por ejemplo, el gestor de certificados de seguridad 6 puede comprobar de forma automática si el usuario en cuestión tiene un nivel de seguridad para manejar la interfaz de usuario 2-1 del sistema. En esta realización, los usuarios u operadores participan automáticamente en el proceso de certificación o recertificación. El procedimiento de certificación para la certificación de una cadena funcional crítica para la seguridad 1 según el primer aspecto de la invención permite reducir significativamente el esfuerzo para la certificación de una cadena funcional crítica para la seguridad 1. Con el procedimiento de certificación, los componentes de una cadena funcional crítica para la seguridad 1 crítica pueden sustituirse sin tener que volver a certificar toda la cadena funcional. En caso de que se produzca un cambio en la cadena funcional crítica para la seguridad 1, la certificación puede llevarse a cabo de forma automática en el menor tiempo posible mediante el procedimiento de recertificación según la invención, sin que expire la autorización de explotación del sistema.

[0026] Según un segundo aspecto de la invención, se crea un procedimiento para proporcionar una conexión de comunicación segura KVB entre componentes 2 de una cadena funcional 1 crítica para la seguridad, por ejemplo, una conexión de comunicación 5-i seguro según la Fig. 1. En el ámbito de las cadenas funcionales críticas para la seguridad, actualmente no existe ningún concepto uniforme que indique cómo deben comunicarse entre sí los componentes relevantes para la seguridad 2-i de las cadenas funcionales 1 críticas para la seguridad dentro de un sistema. El procedimiento de proporcionar un enlace de comunicaciones seguro puede reducir de manera significativa el esfuerzo necesario para recertificar el enlace de comunicación. Antes de la puesta en marcha del sistema, todas las cadenas funcionales críticas para la seguridad 1 del sistema se encuentran en un estado de funcionamiento seguro, preferentemente aislado, en particular, conectado a tierra. Los diferentes componentes 2 dentro de la cadena de funcional crítica para la seguridad 1 presentan un estado de funcionamiento seguro predefinido, de modo que no se puede producir ninguna comunicación espontánea no deseada entre los distintos componentes.

[0027] En el procedimiento para proporcionar un enlace de comunicación seguro entre los componentes 2 de una cadena funcional crítica para la seguridad 1, los token T idénticos se transmiten primero en la etapa S4 por el gestor de certificados de seguridad 6 a los componentes adyacentes dentro de la cadena funcional crítica para la seguridad 1, tal como se muestra en la Fig. 10. Los dos componentes adyacentes presentan cada uno una interfaz de componentes para un enlace de comunicación con el otro componente adyacente. En la etapa S5 se activan las interfaces de componentes de los dos componentes adyacentes dentro de la cadena funcional crítica para la seguridad 1 para establecer el correspondiente enlace de comunicación entre los dos componentes adyacentes. A continuación, en otra etapa S6, los token T recibidos del gestor de certificados de seguridad 6 por los dos componentes vecinos se intercambian a través del enlace de comunicación establecido. El enlace de comunicación establecido entre los dos componentes adyacentes de la cadena funcional crítica para la seguridad 1 se mantiene en la etapa S7 si los token T intercambiados a través del enlace de comunicación entre los dos componentes adyacentes son idénticos a los token T recibidos del gestor del certificado de seguridad 6. En una posible realización, los token transmitidos a los dos componentes vecinos de la cadena funcional crítica para la seguridad 1 poseen un tiempo de caducidad. El enlace de comunicación entre los dos componentes adyacentes de la cadena funcional crítica para la seguridad 1 puede terminarse automáticamente una vez transcurrido el tiempo de caducidad del token T conforme a un nivel de seguridad especificado, en particular, mediante desactivación de una interfaz. Los datos transmitidos a través del enlace de comunicación establecido entre los dos componentes se transmiten preferentemente cifrados según un nivel de seguridad. El nivel de seguridad puede ser un nivel de seguridad de componentes KSL de un componente 2, que se especifica en un certificado de seguridad de componentes KSZ del componente 2 correspondiente. El nivel de seguridad también puede ser el nivel de seguridad de una interfaz de componentes del componente en cuestión especificado en el certificado de seguridad SSZ de la interfaz de componente. El gestor de certificados de seguridad 6 envía preferentemente una lista TAN a los componentes 2 de la cadena funcional crítica para la seguridad 1 después de la autorización de todos los componentes de la cadena funcional crítica para la seguridad 1. La lista TAN enviada es utilizada por los componentes 2-i para encriptar y/o descifrar los datos transmitidos a través del enlace de comunicación. La lista TAN enviada presenta preferentemente un número de lista y un número específico de números TAN que se pueden utilizar una sola vez para la comunicación. No se requiere encriptación para las interfaces analógicas. Si los números de transacción dentro de la lista de TAN se acaban, la cadena funcional crítica para la seguridad 1 puede informar esta circunstancia al gestor de certificados de seguridad 6, que envía una nueva lista TAN a los componentes. Un mensaje transmitido por el gestor de certificados de seguridad 6 puede incluir una ID de

mensaje, una marca de tiempo, una suma de comprobación sobre los contenedores de datos descifrados, un número de lista de la lista de TAN enviada, un elemento de la lista de TAN y un contenedor de datos cifrados. El número de lista TAN y el número de elemento TAN forman parte de cada mensaje transmitido a través del enlace de comunicación con fines de registro. El número TAN se puede seleccionar de la lista TAN de forma secuencial o mediante un número pseudoaleatorio. Cada número TAN se usa preferentemente una sola vez. La longitud del número TAN determina la calidad del cifrado. Una suma de control sobre el contenedor de datos se cifra con el número TAN y se puede transmitir al interlocutor de comunicación o al componente adyacente. El destinatario compara entonces su lista TAN/posición TAN con la del mensaje recibido. El mensaje recibido se considerará válido después de una comprobación CRC correcta y será procesado posteriormente por el componente. Si los dos parámetros no son idénticos, el mensaje es descartado por el componente, donde el gestor de certificados de seguridad 6 puede activar una advertencia.

[0028] La Fig. 11 muestra un diagrama de flujo de señal para explicar el modo de funcionamiento del procedimiento según la invención para proporcionar un enlace de comunicación seguro entre componentes de una cadena funcional crítica para la seguridad 1 según el segundo aspecto de la invención. El gestor de certificados de seguridad 6 transfiere primero un token T, T' idéntico a dos componentes adyacentes 2-1, 2-j de la cadena funcional crítica para la seguridad 1, tal como se muestra en la Fig. 1, por ejemplo. Las interfaces previstas de los dos componentes adyacentes 2-i, 2-j sirven para establecer un enlace de comunicación KVB entre los dos componentes adyacentes, tal como se muestra en la Fig. 11. Primero, el primer componente 2-i activa una interfaz de componentes de salida y el segundo componente adyacente 2j activa una interfaz de componentes de entrada para establecer la conexión de comunicación KVB entre los dos componentes. A esto le sigue un intercambio de los token T, T ', respectivamente, obtenidos del gestor de certificados de seguridad 6 por los dos componentes 2-i, 2-j a través de la conexión de comunicación KVB establecida. Se comprueba, por un lado, mediante el primer componente 2-i y, por otro lado, mediante el segundo componente 2-j, si el token T intercambiado con el otro componente es idéntico al original recibido. Si los token T intercambiados a través del enlace de comunicación KVB entre los dos componentes adyacentes 2-i, 2-j son idénticos a los token obtenidos del gestor de certificados de seguridad 6, el enlace de comunicación KVB establecido entre los dos componentes adyacentes de la cadena funcional crítica para la seguridad 1 se mantiene, tal como se muestra en la Fig. 11. Los datos pueden intercambiarse preferentemente de forma encriptada a través del enlace de comunicación KVB. Si el primer componente 2-i llega a la conclusión de que el token T recibido por el otro componente 2-j y el token T originalmente obtenido por el gestor de certificados de seguridad 6 se desvían, puede desactivar su interfaz de componentes de salida para suprimir la conexión de comunicación KVB establecida. De manera similar, el segundo componente 2-j puede verificar si el token T que recibió a través de la conexión de comunicación es idéntico al token T' obtenido del gestor de certificados de seguridad 6. Si este no es el caso, el segundo componente 2-j puede desactivar su interfaz de componentes de entrada para que la conexión de comunicación KVB se suprima de forma automática y/o se transmita un mensaje de error al gestor de certificados de seguridad.

[0029] El gestor de certificados de seguridad 6 del sistema puede activar las conexiones de comunicación KVB gradualmente hasta que se alcancen los componentes periféricos del sistema. Los componentes periféricos son los componentes en los límites del sistema de la instalación o del sistema. La Fig. 13 muestra esquemáticamente la activación de una interfaz de componentes de un componente periférico, por ejemplo, los componentes 2-1, 2-4. El gestor de certificados de seguridad 6 envía el token T al componente periférico, que es una interfaz de componente para el mundo exterior, es decir, en el límite del sistema, activado, tal como se muestra esquemáticamente en la Fig. 13.

[0030] Según un tercer aspecto, la invención también proporciona un componente 2-i para una cadena funcional crítica para la seguridad 1, tal como se muestra esquemáticamente en las figuras 14, 15. El componente 2-i posee un certificado de seguridad de componente KSZ asociado que se almacena en un área de memoria a prueba de manipulaciones asociada de una memoria de datos y puede ser verificado por un gestor de certificados de seguridad 6 para habilitar el componente 2-i dentro de la cadena funcional crítica para la seguridad 1. En una realización preferida de la invención del componente según la invención, el certificado de seguridad de componentes KSZ almacenado puede ser leído por el gestor de certificados de seguridad 6 del sistema y puede verificarse su validez en función de los requisitos de seguridad especificados. El área de memoria para almacenar el certificado de seguridad de componentes del componente está previsto preferentemente en una memoria de datos a prueba de manipulación indebida que está integrada en el componente, tal como se muestra en las figuras 14, 15. La memoria de datos integrada en el componente, que está prevista para almacenar el certificado de seguridad de componentes KSZ, es preferentemente un módulo de plataforma confiable 7, tal como se muestra en las figuras 14, 15. En una variante de realización alternativa, el área de memoria para almacenar el certificado de seguridad de componentes KSZ del componente 2 se ubica en una memoria de datos a prueba de manipulaciones indebidas que no está integrada en el componente 2, sino que forma una memoria de datos externa, preferentemente referenciada por una dirección de memoria y a la que tiene acceso el gestor de certificados de seguridad 6. Tal como se muestra en la Fig. 4, el módulo de plataforma confiable 7 del componente 2 puede contener el certificado de seguridad de componentes KSZ asociado del componente 2-i, que puede ser leído para su verificación por el gestor de certificados de seguridad 6.

[0031] En el módulo de plataforma confiable 7-i del componente según la invención 2, además del certificado de seguridad de componente KSZ, también puede haber certificados de seguridad de interfaz de componentes SSZ

que el gestor de certificados de seguridad 6 puede leer para verificar.

[0032] La Fig. 16 muestra de manera esquemática una estructura de datos de un ejemplo de realización de un certificado de seguridad de componentes KSZ, ya que puede almacenarse en una memoria de datos 7 a prueba de manipulación indebida del componente 2 según la invención. El certificado de seguridad de componentes KSZ del componente 2 comprende un número de versión del certificado de seguridad de componentes, una fecha de emisión del certificado de seguridad de componentes, un emisor del certificado de seguridad del componentes, un tipo de componentes del componente, un nivel de seguridad de componentes KSL del componente, una identificación del fabricante para identificar al fabricante del componente, una identificación de componentes del componente, certificados de seguridad de interfaz SSZ para las interfaces de componentes de salida del componente con un nivel de seguridad de interfaz SSL de la respectiva interfaz de componentes de salida provista en el mismo, certificados de seguridad de interfaz SSZ para interfaces de componentes de entrada del componente con un nivel de seguridad de interfaz respectivo requerido de la interfaz de componentes de entrada respectiva y parámetros de configuración del componente en cuestión.

[0033] En una posible realización, se proporciona un certificado de seguridad de interfaz SSZ asociado para cada interfaz de componente del componente según la invención 2 y se almacena a prueba de manipulaciones en el módulo de plataforma confiable 7 del componente. En el sistema según la invención, tal como se ilustra esquemáticamente a modo de ejemplo en la Fig. 1, un gestor de certificados de seguridad 6 central puede verificar los certificados de seguridad de todos los componentes e interfaces. Los componentes 2 de una instalación o de un sistema pueden comunicarse entre sí en una variante de realización a través de una interfaz segura, donde el sistema se activa solo cuando todas las cadenas funcionales críticas para la seguridad 1 cumplen con los requisitos de seguridad. El número de niveles de seguridad utilizados puede variar. Los certificados de seguridad digital, en una posible variante de realización pueden ser los certificados de seguridad de clave pública. En una posible realización, los certificados digitales pueden ser emitidos por una autoridad de certificación. Los certificados de seguridad digital que se usan en el sistema según la invención, es decir, los certificados de seguridad de componentes KSZ y los certificados de seguridad de interfaz SSZ representan conjuntos de datos digitales que confirman ciertas propiedades de los objetos o componentes, donde la autenticidad e integridad de la información se puede verificar mediante métodos criptográficos. El sistema es, por ejemplo, un sistema industrial con al menos una cadena funcional crítica para la seguridad 1, que consiste en varios componentes 2-i concatenados. Este puede ser un sistema con una gran cantidad de componentes de hardware y/o software concatenados. Además, el sistema puede ser, por ejemplo, un vehículo con una pluralidad de componentes de software y/o hardware integrados en él. La invención proporciona además un gestor de certificados de seguridad 6 para dicha cadena funcional crítica para la seguridad 1, donde el gestor de certificados de seguridad 6 autoriza automáticamente la cadena funcional crítica para la seguridad 1 después de verificar satisfactoriamente los certificados de seguridad de componentes KSZ y los certificados de seguridad de interfaz de componentes SSZ. El gestor de certificados de seguridad 6 puede ser parte del sistema complejo o estar conectado con el sistema a ser certificado. En una variante de realización, el gestor de certificados de seguridad 6 está conectado a través de una red de datos con un sistema remoto que va a ser certificado. Además, el gestor de certificados de seguridad 6 también puede estar implementado en un servidor local del sistema. Además, el gestor de certificados de seguridad 6 puede estar integrado en otra variante de realización en un componente 2-i de la propia cadena funcional crítica para la seguridad 1. En otra variante de realización, el gestor de certificados de seguridad 6 también forma un componente, es decir, el gestor de certificados de seguridad 6 puede ejecutar una autocomprobación en una variante de realización para verificar si aún cumple con los requisitos de seguridad dados.

Lista de referencias

[0034]

1 Cadena funcional
2 Componente
3 Interfaz del componente de entrada
4 Interfaz del componente de salida
5 Conexiones de comunicación
6 Gestor de certificados de seguridad
7 Memoria de datos a prueba de manipulaciones

REIVINDICACIONES

1. Sistema, con:

un administrador de certificados de seguridad (6); y al menos una cadena funcional crítica para la seguridad (1) que presenta una pluralidad de componentes (2) que están unidos entre sí a través de enlaces de comunicación, KVB, cada uno de los cuales tiene un certificado de seguridad de componentes asociado, KSZ, que se almacena en un área de memoria a prueba de manipulación asociada de una memoria de datos (7) y para liberar el componente (2) dentro de la cadena funcional crítica para la seguridad (1) puede verificarse por parte del gestor de certificados de seguridad (6),
donde el certificado de seguridad de interfaces del KSZ, SSZ, para interfaces del componente de salida del componente (2) con un nivel de seguridad de interfaz especificado en el mismo, SSL, presenta la interfaz del componente de salida respectiva, así como el SSZ para las interfaces del componente de entrada del componente (2) con un SSL de entrada respectivo requerido en la interfaz de componente, el administrador de certificados de seguridad (6) está diseñado al efecto para verificar, si un nivel de seguridad de componentes KSL, que se especifica en el KSZ de los componentes concatenados (2), es suficiente para un nivel de seguridad de componentes, KSL, del componente relevante (2) requerido según los requisitos de seguridad especificados, y si en el SSZ de las interfaces de componentes de entrada y salida conectadas a través de un enlace de comunicación, KVB, de cada SSL especificado de dos componentes adyacentes (2) dentro de la cadena funcional crítica para la seguridad (1) son compatibles entre sí, y
el gestor de certificados de seguridad (6) está diseñado para liberar automáticamente la cadena funcional crítica para la seguridad (1) si la verificación de todos los KSL y SSL es satisfactoria.

2. Sistema según la reivindicación 1, donde el gestor de certificados de seguridad (6) puede leer el KSZ almacenado y su validez puede verificarse en función de requisitos de seguridad predeterminados.

3. Sistema según la reivindicación 1 o 2, donde el área de memoria para almacenar el KSZ del componente (2) se proporciona en una memoria de datos a prueba de manipulaciones (7) que está integrada en los componentes (2) o está previsto en una memoria externa a prueba de manipulaciones, a la que hace referencia una dirección de memoria.

4. Sistema según la reivindicación 3, donde la memoria de datos (7) integrada en los componentes (2) para almacenar el KSZ presenta un módulo de plataforma confiable, TPM.

5. Sistema según una de las reivindicaciones 1 a 4, donde el KSZ de los componentes (2) comprende:

- un número de versión del KSZ,
- una fecha de emisión del KSZ,
- un emisor del KSZ,
- un tipo del componente,
- una identificación del fabricante para la identificación del fabricante del componente,
- una identificación del componente del componente,
- parámetros de configuración del componente.

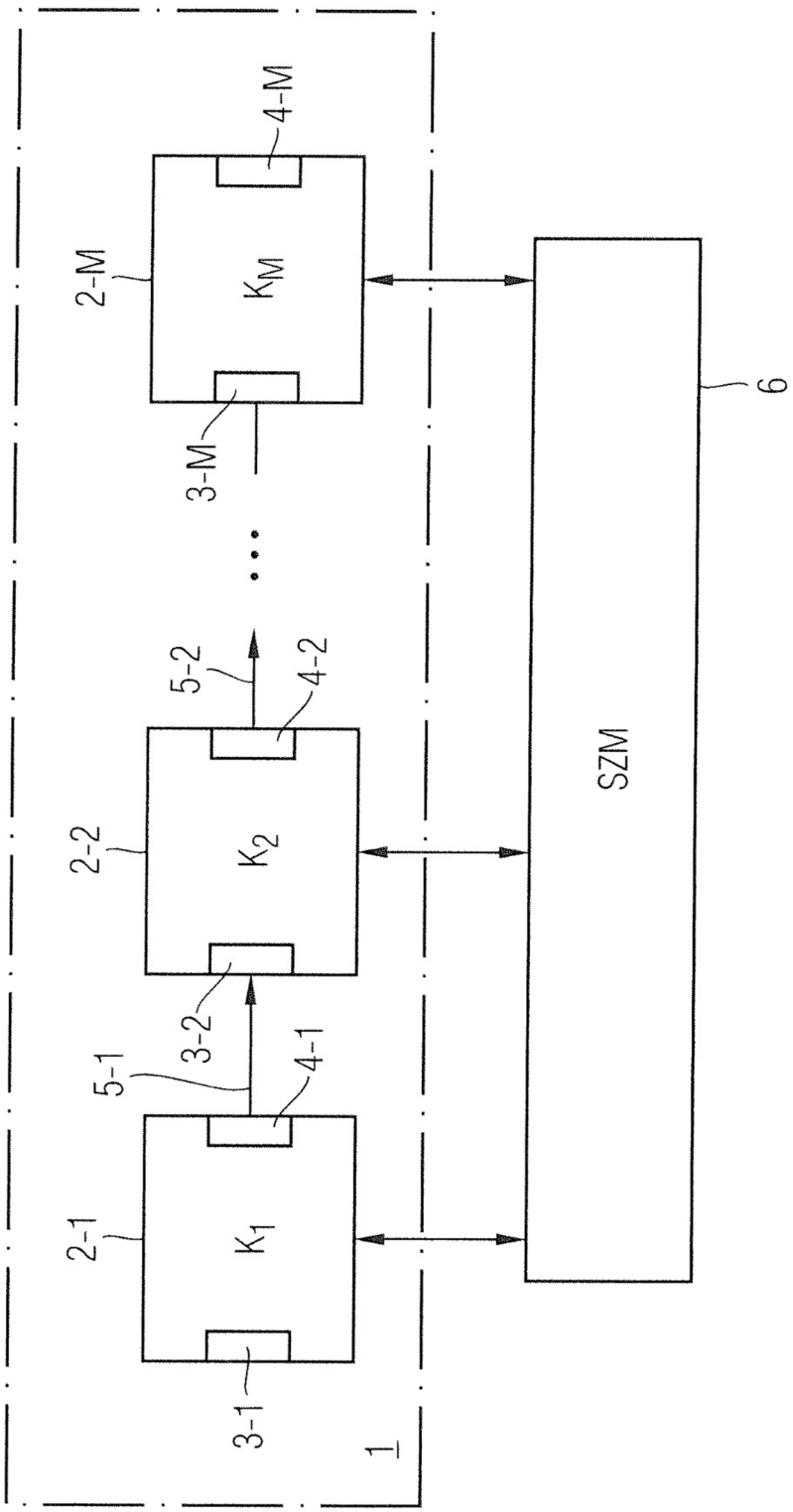

Fig. 1

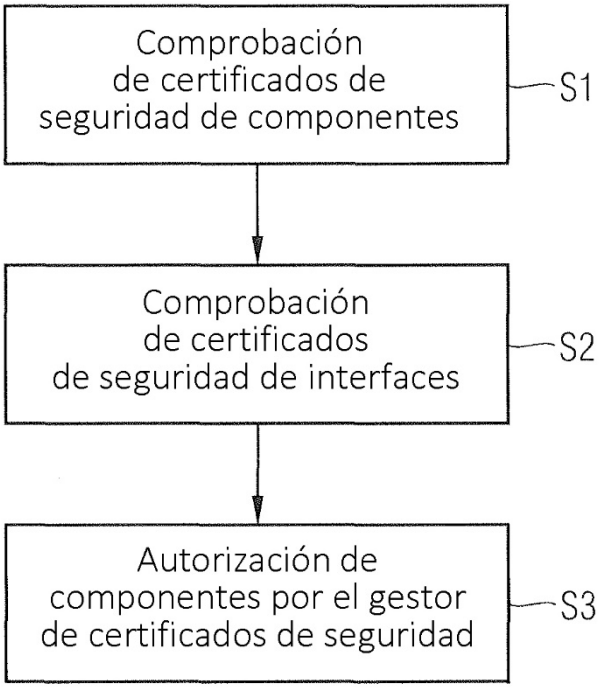
Comprobación de certificados de seguridad de componentes
S1
Comprobación de certificados de seguridad de interfaces
S2
Autorización de componentes por el gestor de certificados de seguridad
S3

Fig. 2

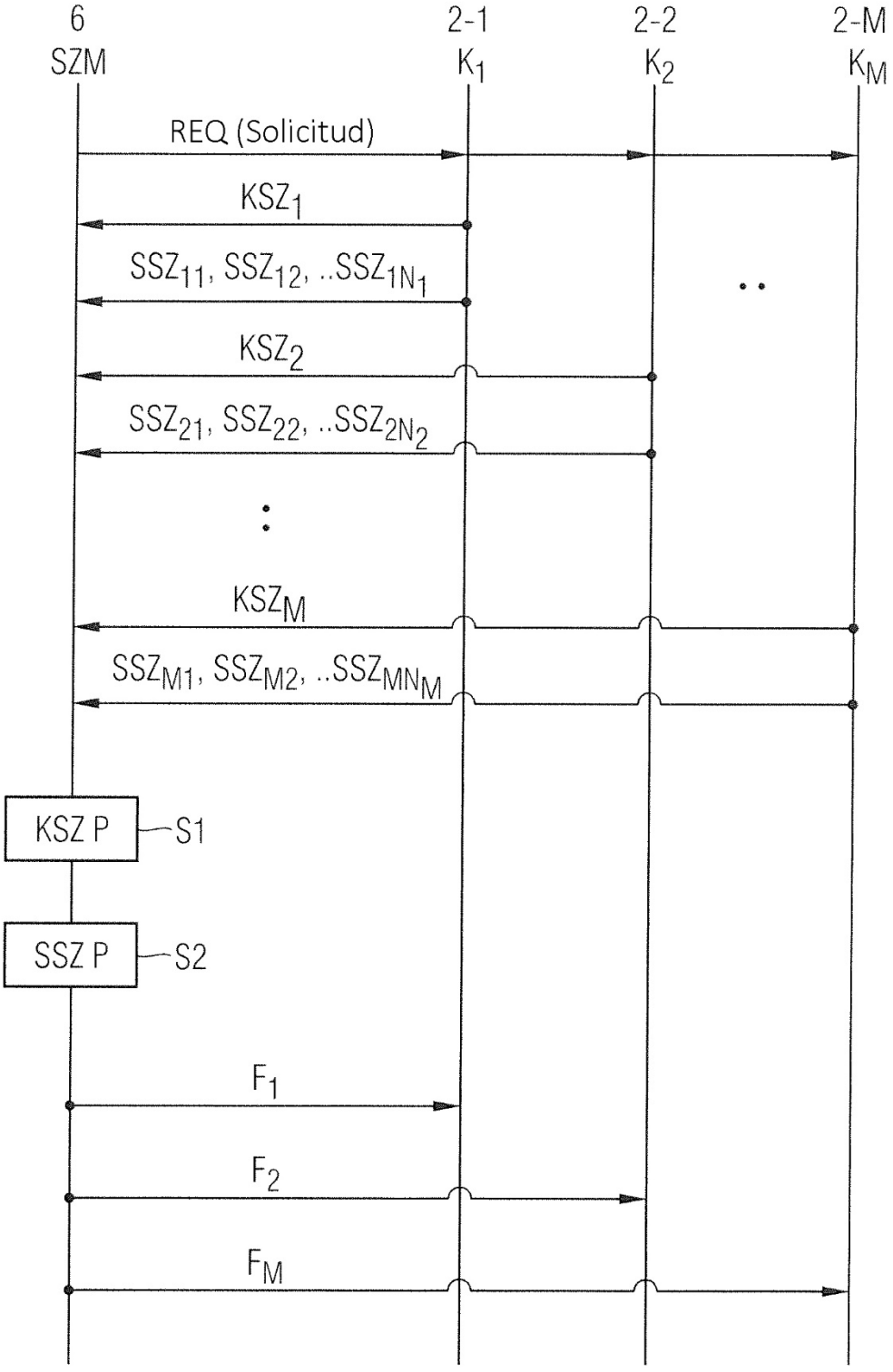
6
SZM
2-1
K1
2-2
K2
2-M
KM
REQ (Solicitud)
KSZ1
SSZ11, SSZ12, ..SSZ1N1
KSZ2
SSZ21, SSZ22, ..SSZ2N2
KSZM
SSZM1, SSZM2, ..SSZMNM
KSZ P
S1
SSZ P
S2
F1
F2
FM

Fig. 3

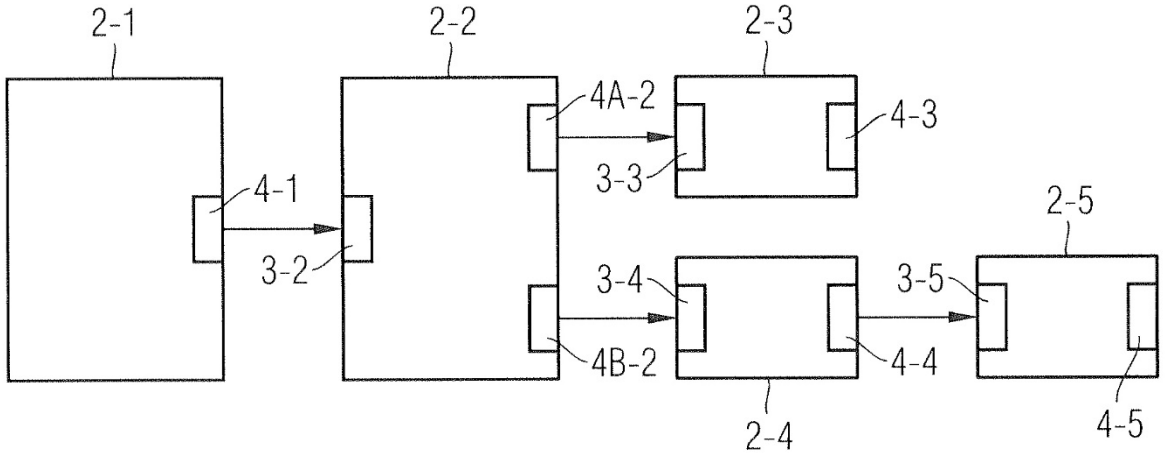
2-1
2-2
2-3
4A-2
4-3
4-1
3-3
2-5
3-4
3-5
3-2
4B-2
4-4
2-4
4-5

Fig. 4

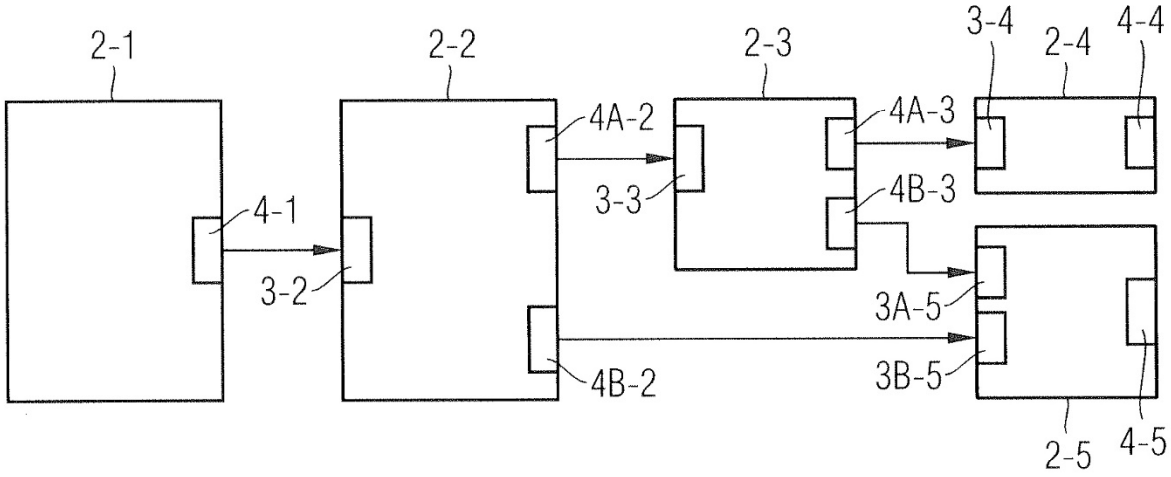
2-1
2-2
2-3
3-4
2-4
4-4
4A-2
4A-3
4-1
3-3
4B-3
3-2
3A-5
4B-2
3B-5
2-5
4-5

Fig. 5

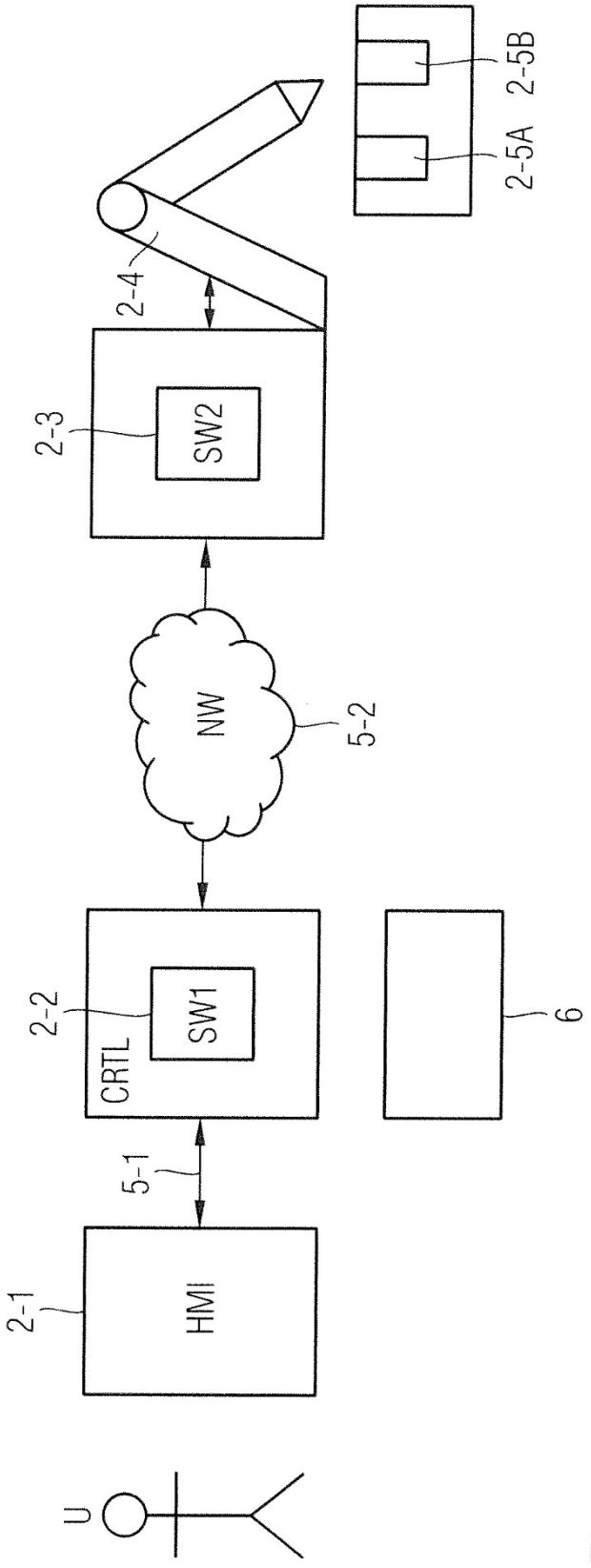

Fig. 6

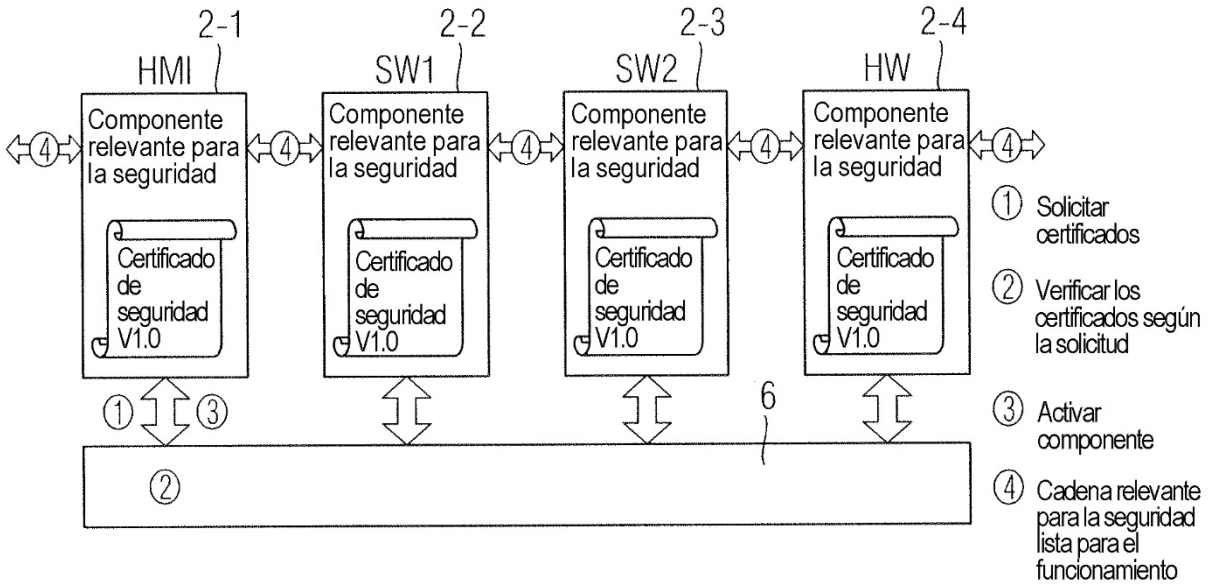
2-1
HMI
2-2
SW1
2-3
SW2
2-4
HW
Componente relevante para la seguridad
Certificado de seguridad V1.0
6
① Solicitar certificados
② Verificar los certificados según la solicitud
③ Activar componente
④ Cadena relevante para la seguridad lista para el funcionamiento

Fig. 7

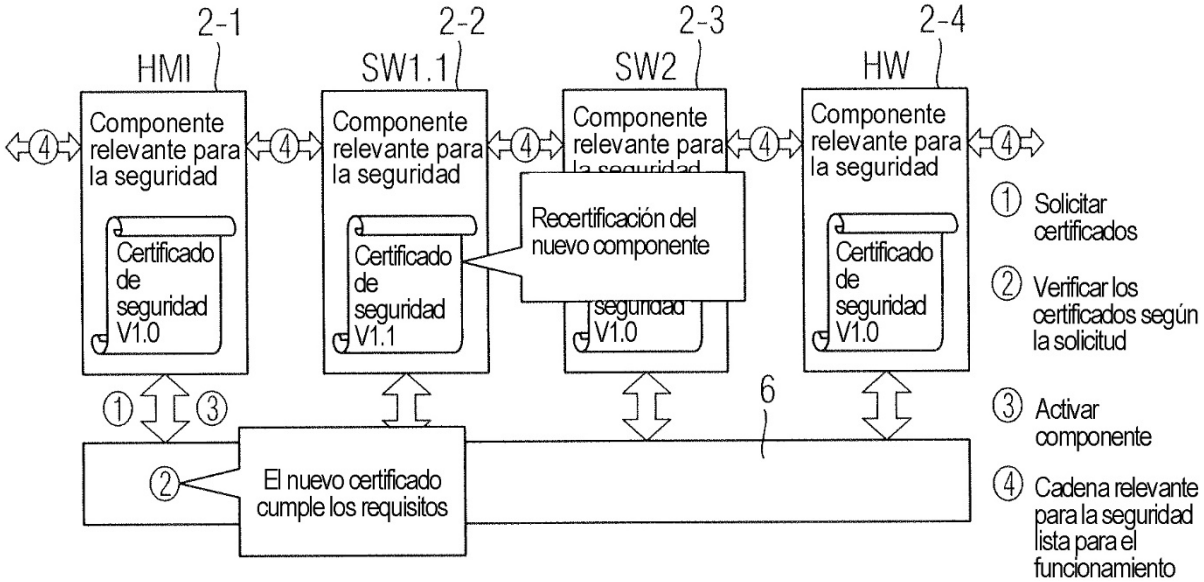
2-1
HMI
2-2
SW1.1
2-3
SW2
2-4
HW
Componente relevante para la seguridad
Certificado de seguridad V1.0
Certificado de seguridad V1.1
Recertificación del nuevo componente
El nuevo certificado cumple los requisitos
6
① Solicitar certificados
② Verificar los certificados según la solicitud
③ Activar componente
④ Cadena relevante para la seguridad lista para el funcionamiento

Fig. 8

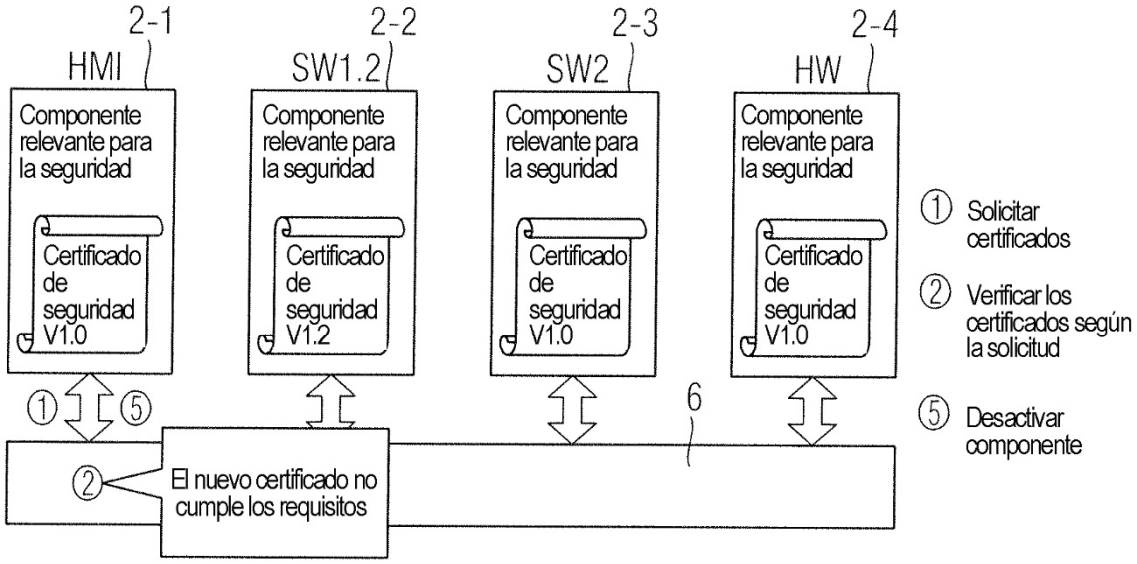
2-1
HMI
Componente relevante para la seguridad
Certificado de seguridad V1.0
2-2
SW1.2
Componente relevante para la seguridad
Certificado de seguridad V1.2
2-3
SW2
Componente relevante para la seguridad
Certificado de seguridad V1.0
2-4
HW
Componente relevante para la seguridad
Certificado de seguridad V1.0
6
① Solicitar certificados
② Verificar los certificados según la solicitud
⑤ Desactivar componente
① ⑤
②
El nuevo certificado no cumple los requisitos

Fig. 9

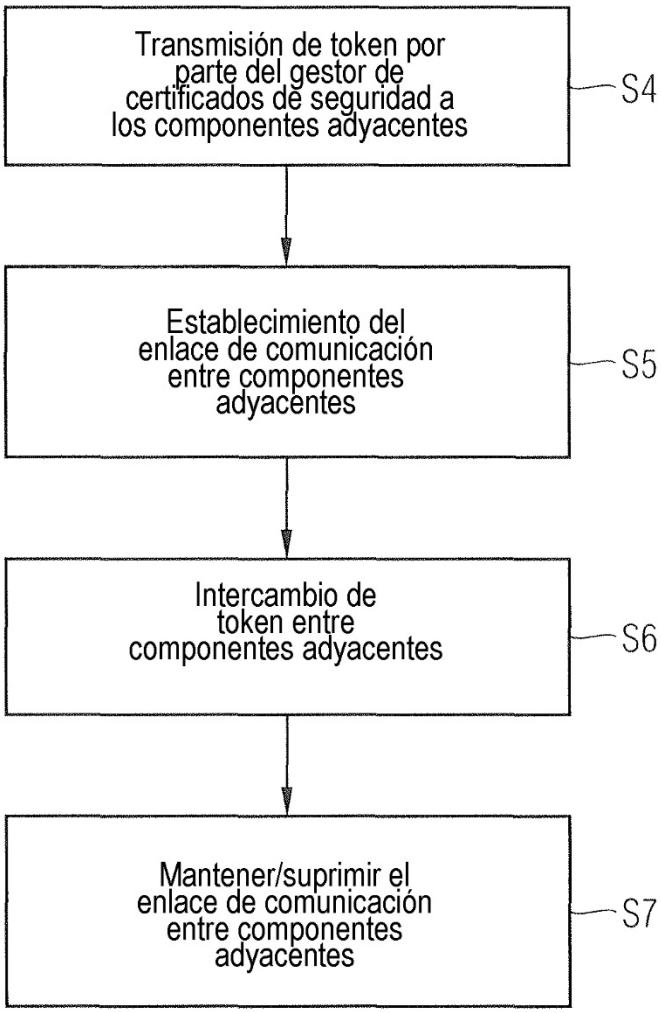
Transmisión de token por parte del gestor de certificados de seguridad a los componentes adyacentes
S4
Establecimiento del enlace de comunicación entre componentes adyacentes
S5
Intercambio de token entre componentes adyacentes
S6
Mantener/suprimir el enlace de comunicación entre componentes adyacentes
S7

Fig. 10

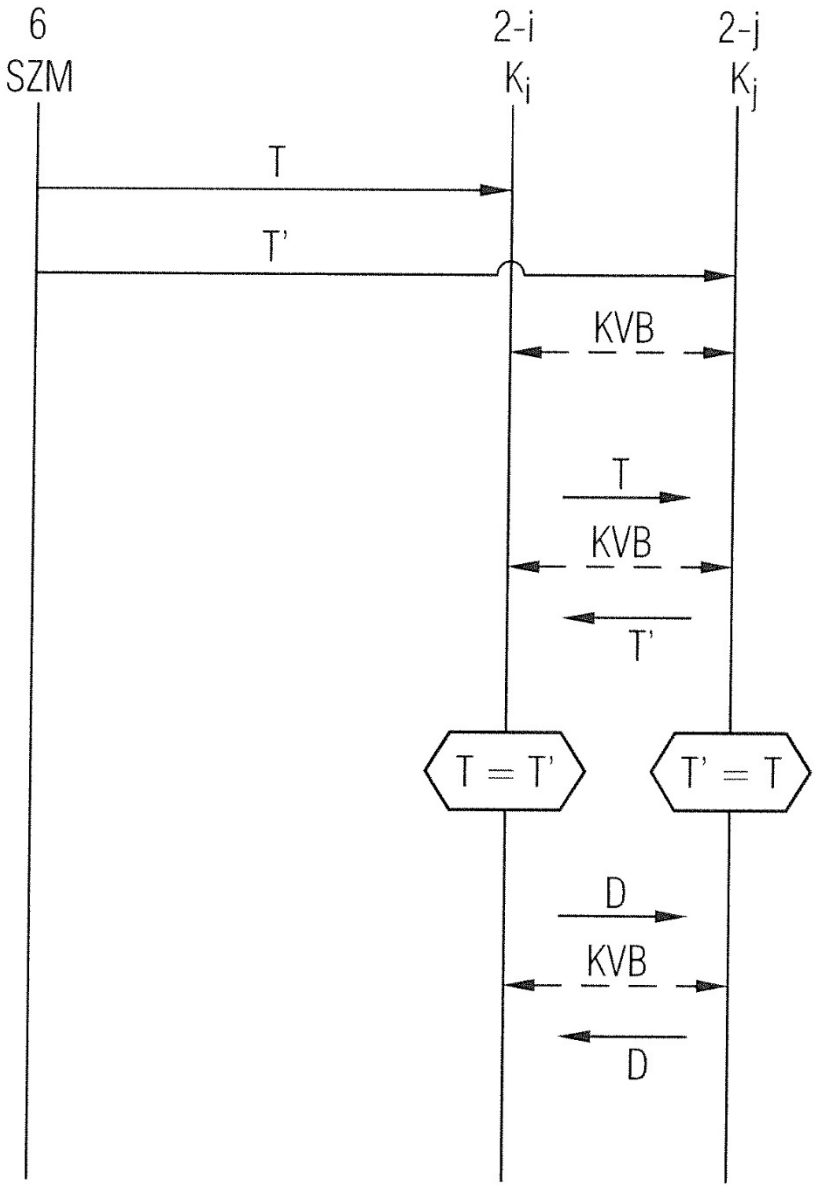

Fig. 11

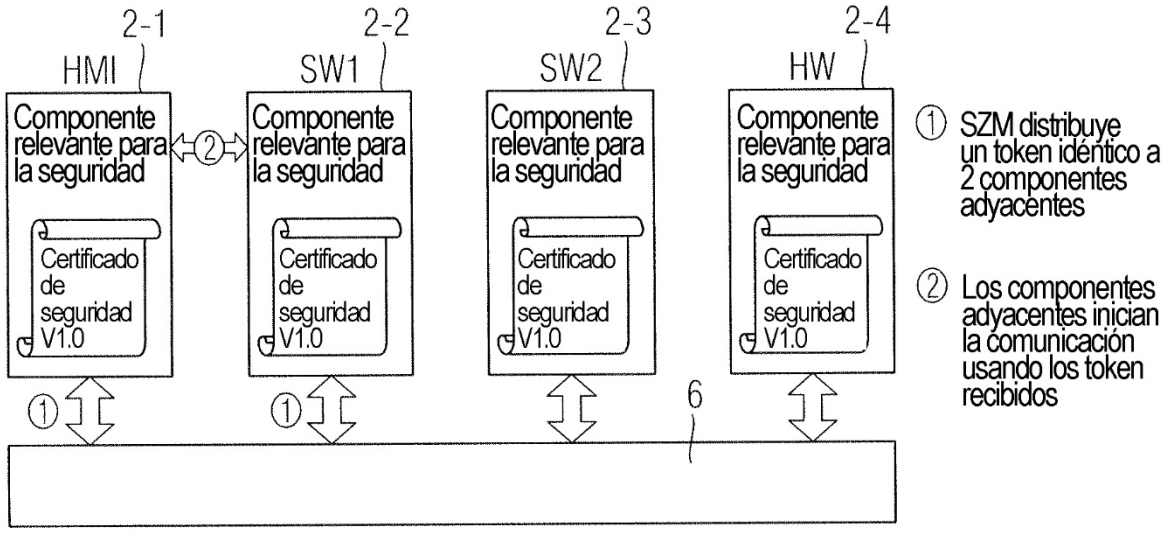
2-1
HMI
2-2
SW1
2-3
SW2
2-4
HW
Componente relevante para la seguridad
Certificado de seguridad V1.0
6
① SZM distribuye un token idéntico a 2 componentes adyacentes
② Los componentes adyacentes inician la comunicación usando los token recibidos

Fig. 12

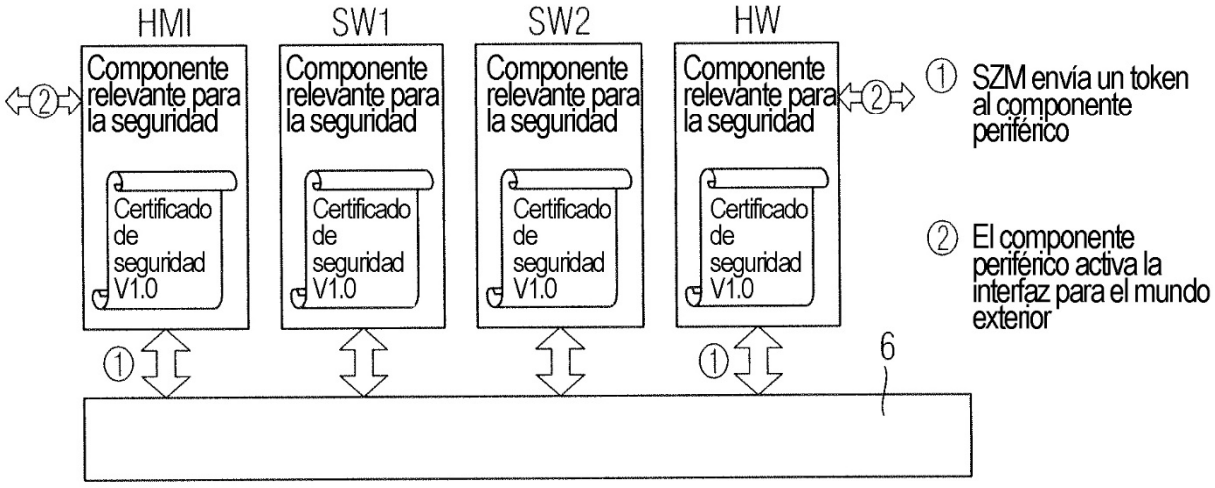
HMI
SW1
SW2
HW
Componente relevante para la seguridad
Certificado de seguridad V1.0
6
① SZM envía un token al componente periférico
② El componente periférico activa la interfaz para el mundo exterior

Fig. 13

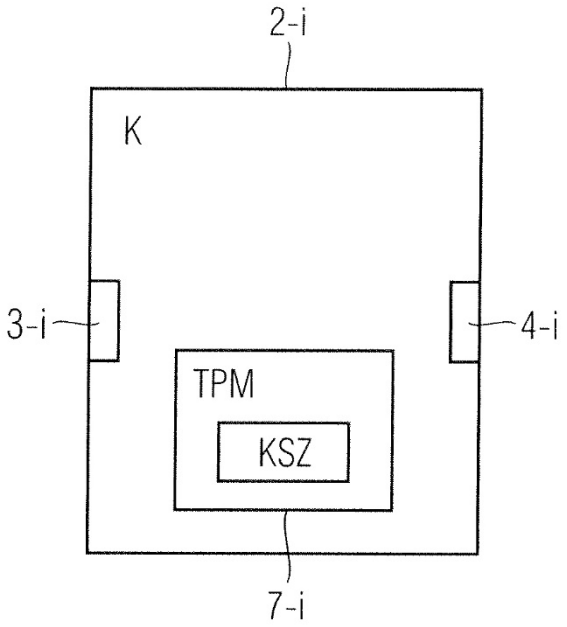

Fig. 14

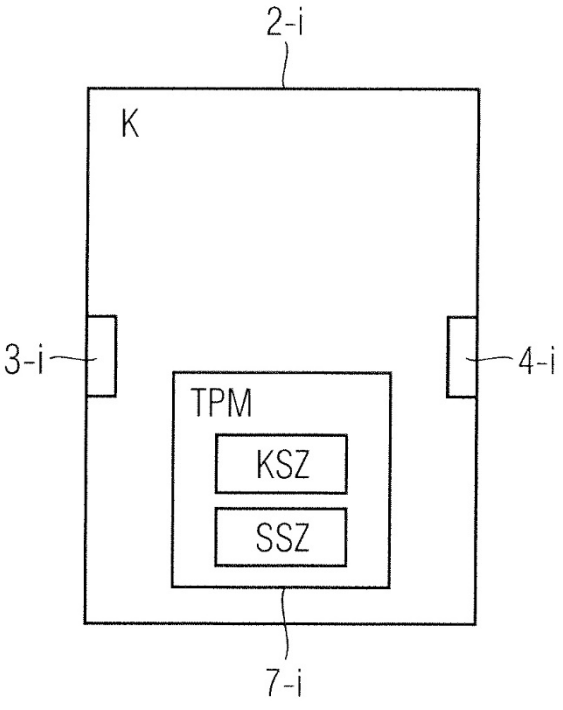

Fig. 15


KSZ
N.º VER
Fecha
Emisor
Tipo de componente
Nivel de seguridad de los componentes
Identificación del fabricante
Identificación de componentes
Certificados de seguridad de interfaces para interfaces de componentes de SALIDA
Certificados de seguridad de interfaces para interfaces de componentes de ENTRADA
Parámetros de configuración

Fig. 16