(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 807 605**

(51) Int. CI.:

G06F 21/57 (2013.01)
G06F 21/74 (2013.01)
B61L 27/00 (2006.01)
G05B 9/00 (2006.01)
G06F 11/07 (2006.01)
G06F 11/16 (2006.01)
B61L 15/00 (2006.01)
H04L 1/22 (2006.01)
H04L 29/08 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **04.09.2014 PCT/EP2014/068843**

(87) Fecha y número de publicación internacional: **26.03.2015 WO15039878**

(96) Fecha de presentación y número de la solicitud europea: **04.09.2014 E 14761976 (1)**

(97) Fecha y número de publicación de la concesión europea: **13.05.2020 EP 3027483**

(54) Título: **Actualización de software de componentes no críticos en sistemas distribuidos críticos para la seguridad dual**

(30) Prioridad:

19.09.2013 DE 102013218814

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.02.2021

(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

Actualización de software de componentes no críticos en sistemas distribuidos críticos para la seguridad dual

Se ha demostrado que es muy difícil o prácticamente imposible operar dispositivos de datos como, por ejemplo, computadoras personales, de tal manera que puedan funcionar sin huecos de seguridad identificables. De ello resultan problemas particulares cuando los dispositivos de datos pertenecen a un sistema crítico para la seguridad equipado con un software relevante y no relevante para la seguridad que debe ser probado en conformidad antes de su uso y aprobado en un procedimiento complejo, por ejemplo, en un sistema de seguridad de trenes o un dispositivo operativo de un sistema de enclavamiento. Después de ello, el software ya no se puede modificar. Esto se monitorea incluso automáticamente de acuerdo con el estado del arte y dichos sistemas se apagan automáticamente después de que se han detectado cambios. Cuando, después de la prueba y admisión de un sistema como este se presenta la necesidad de incorporar un software no relevante para la seguridad en dicho sistema mediante una actualización o un parche informático, entonces se debe utilizar un software aprobado, claramente identificable, o bien se debe realizar una nueva prueba para su admisión.

De la solicitud WO 03/047937 A1 se conoce un procedimiento para el control de un proceso operativo de ferrocarril crítico para la seguridad. Para la ejecución de este procedimiento se utiliza un dispositivo con un ordenador con tecnología de señal segura en el cual se implementa el software del sistema y con ordenadores comerciales sin tecnología de señales segura en los cuales está implementado un software específico de gestión ferroviaria. Allí, el ordenador seguro y los ordenadores comerciales están conectados a un sistema de comunicaciones a través del cual el ordenador seguro transmite órdenes de procesamiento a los ordenadores comerciales y recibe resultados y/o resultados intermedios desde ellos. Los ordenadores comerciales están configurados para ejecutar cada operación de procesamiento al menos dos veces de forma independiente entre sí. El ordenador seguro verifica con tecnología de señales segura la coincidencia de contenido de los resultados y/o de los resultados intermedios que le transmiten los ordenadores comerciales al menos en pares; en función del resultado de la prueba, el ordenador deriva comandos de control para los elementos del proceso e inicia su salida en el proceso a través de controladores provistos para ese propósito. Del lado del ordenador comercial están proporcionados mecanismos de verificación para la plausibilidad de las firmas de las salidas elaboradas por el mismo. Dichos mecanismos de verificación no se ejecutan con tecnología de señales segura. Por otro lado, del lado del ordenador con tecnología de señales segura están proporcionados mecanismos de verificación que se ejecutan con tecnología de señales segura.

El objeto de la presente invención consiste en especificar un procedimiento para el funcionamiento de un sistema crítico para la seguridad con el cual el sistema se pueda actualizar con costes comparativamente reducidos.

Para resolver dicho objeto resulta adecuado un procedimiento para el funcionamiento de un sistema crítico para la seguridad con al menos un primer dispositivo de datos con un software aprobado y relevante para la seguridad y con al menos un dispositivo de datos de referencia con el mismo software aprobado y relevante para la seguridad; en el cual después de una prueba de conformidad del sistema el, al menos un, primer dispositivo de datos está equipado con al menos un software adicional no relevante para la seguridad y el, al menos un, dispositivo de datos de referencia está bloqueado para modificaciones de software y todavía está equipado sólo con el software relevante para la seguridad; antes del envío de una información de datos relacionados con la seguridad mediante un dispositivo de comparación se verifica la coincidencia de las informaciones de salida del, al menos un, primer dispositivo de datos y del, al menos un, dispositivo de datos de referencia en referencia al software relevante para la seguridad y si hay una coincidencia se envía la información de datos relativos a la seguridad.

Una ventaja fundamental del procedimiento conforme a la invención consiste en que ofrece la posibilidad de actualizar o complementar con posterioridad en el sistema crítico para la seguridad, es decir, después de la admisión, un software no relevante para la seguridad sin necesidad de realizar una nueva prueba de conformidad con una nueva aprobación.

Para garantizar la seguridad resulta ventajoso en un sistema con una pluralidad de primeros dispositivos de datos y una pluralidad de dispositivos de datos de referencia, emitir informaciones de datos relacionados con la seguridad cuando una verificación de las informaciones de salida de los primeros dispositivos de datos y los dispositivos de datos de referencia con respecto al software relevante para la seguridad ha demostrado que existe una coincidencia en cada caso con respecto a una mayoría cualificada de los primeros dispositivos de datos y de los dispositivos de datos de referencia.

El procedimiento conforme a la invención ofrece la posibilidad ventajosa de utilizar un software de protección de datos como software adicional, el cual puede consistir, en particular, en un software de protección contra virus o contra programas malignos en general.

Además, el procedimiento conforme a la invención permite ventajosamente que se utilice un software externo como software adicional, que incluye, por ejemplo, un software disponible comercialmente, un software no desarrollado por el propio desarrollador del sistema crítico para la seguridad o un software no verificado.

En referencia al tipo del software no relevante para la seguridad, el procedimiento conforme a la invención no está sujeto a ninguna restricción.

En una forma de realización particularmente ventajosa del procedimiento conforme a la invención, antes de la prueba de conformidad, el, al menos un, primer dispositivo de datos está equipado con al menos un software adicional no relevante para la seguridad de tal manera que el programa y los datos están separados entre sí; en donde como datos se utilizan datos de prueba con un código; después de la prueba de conformidad, el, al menos un, primer dispositivo de datos es provisto de datos actualizados en el mismo programa usando el código después de la verificación de la validez de los datos actualizados. El código puede tratarse de una firma. Esta forma de realización del procedimiento conforme a la invención se caracteriza porque se evitan con gran fiabilidad perturbaciones en funcionamiento del sistema crítico para la seguridad actualizando el software adicional.

Esta forma de realización del procedimiento conforme a la invención también se puede utilizar independientemente de un sistema crítico para la seguridad con al menos un primer dispositivo de datos con software aprobado y relevante para la seguridad y con al menos un dispositivo de datos de referencia con el mismo software aprobado y relevante para la seguridad, es decir, también en un sistema crítico para la seguridad con un dispositivo de datos en el sentido del primer dispositivo de datos mencionado anteriormente o con múltiples dispositivos de datos.

Para la actualización sin alteraciones del software adicional también contribuye ventajosamente cuando, en el caso del software de protección de datos como software adicional, se garantiza que la funcionalidad del programa no pueda verse afectada por los datos.

En este mismo sentido resulta ventajoso cuando al utilizar el software adicional, la validez del código de los datos de dicho software adicional se verifica mediante el software relevante para la seguridad.

El sistema crítico para la seguridad puede consistir en sistemas de diversos tipos, incluidos entre otros, sistemas de seguridad de trenes o sistemas de control para enclavamientos. Resulta particularmente ventajoso cuando como sistema crítico para la seguridad se utiliza un sistema de seguridad de trenes y como al menos un primer dispositivo de datos se utiliza una computadora operativa y como dispositivo de comparación se usa un enclavamiento.

Para explicaciones adicionales de la invención, en la figura está representada esquemáticamente una disposición con un primer dispositivo de datos y un dispositivo de datos de referencia.

La figura muestra un primer dispositivo de datos 1, que puede consistir en una computadora operativa de un sistema de seguridad de trenes. El primer dispositivo de datos 1 contiene software aprobado y relevante para la seguridad 2. Un dispositivo de datos de referencia 4, que también está equipado con el software aprobado relevante para la seguridad 2, está conectado con el primer dispositivo de datos 1 a través de una conexión de datos 3.

El primer dispositivo de datos 1 está conectado, a través de un canal de datos 5 y el dispositivo de datos de referencia 4, a través de un canal de datos adicional 6 con un dispositivo de comparación 7, cuya función es asumida en un sistema de seguridad de trenes por un enclavamiento que no está representado, u otro comparador orientado a la seguridad.

Para una descripción más detallada del procedimiento conforme a la invención, se supone que la disposición recién descrita ha sido sometida a una prueba de conformidad y a una aprobación en este estado. Cuando dicha disposición se equipa posteriormente, por ejemplo, con un software adicional 8 en forma de un programa antivirus, entonces el dispositivo de datos de referencia 4 se bloquea en simultáneo para modificaciones de software; el mismo todavía sólo está equipado con un software relevante para la seguridad 2.

Cuando el dispositivo de comparación 7 debe emitir información de datos relacionados con la seguridad D, entonces las informaciones de salida A1 y Ar del primer dispositivo de datos y del dispositivo de datos de referencia 4 son registradas previamente por el dispositivo de comparación 7; dichas informaciones de salida A1 y Ar se verifican en referencia al software 2 relevante para la seguridad, y cuando el software 2 relevante para la seguridad coincide se emite la información de datos relacionados con la seguridad D.

Además del software adicional no relevante 8, el primer dispositivo de datos también puede estar provisto de otro software adicional no relevante para la seguridad 9, que en el caso de un sistema de seguridad de trenes puede ser, por ejemplo, cualquier software para el monitoreo de video de un sistema de estación de trenes, o de otro software adicional 10, que puede representar un software para el sistema de monitoreo de los pasos a nivel.

En este caso, el primer dispositivo de datos 1 se puede equipar con el respectivo software adicional 8, 9 y 10 de una manera no mostrada de tal modo que el programa y los correspondientes datos estén respectivamente separados. Antes de la prueba de conformidad o admisión, los respectivos programas están almacenados en el primer dispositivo de datos 1 con datos de prueba y un código. Lo mismo resulta válido, por supuesto, para el software 2 relevante para la seguridad en referencia al primer dispositivo de datos 1 y al dispositivo de datos de referencia 4.

Cuando, después de la prueba de conformidad, el primer dispositivo de datos debe actualizarse con respecto, por ejemplo, al software adicional 8, entonces el primer dispositivo de datos 1 recibe datos actualizados con respecto a dicho software. Allí, el código se utiliza de manera independiente de la transferencia de los datos actualizados y se verifica en referencia a la coincidencia. También se verifica la validez de los datos actualizados. De esta manera se garantiza que los datos del software adicional no puedan modificar la funcionalidad del programa del software adicional.

El software adicional también se puede actualizar siempre y cuando se garantice que la actualización no pueda anular los mecanismos de seguridad descritos previamente, en particular, cuando se puede excluir una influencia en el dispositivo de referencia 4 a través de la conexión de datos 3.

REIVINDICACIONES

1. Procedimiento para el funcionamiento de un sistema crítico para la seguridad con al menos un primer dispositivo de datos (1) con un software aprobado y relevante para la seguridad (2) y con al menos un dispositivo de datos de referencia (4) con el mismo software aprobado y relevante para la seguridad (2), en el cual después de una prueba de conformidad del sistema el, al menos un, primer dispositivo de datos (1) está equipado con al menos un software adicional no relevante para la seguridad (8, 9, 10) y el, al menos un, dispositivo de datos de referencia (4) está bloqueado para modificaciones de software y todavía está equipado sólo con el software relevante para la seguridad (2), antes del envío de una información de datos relacionados con la seguridad (D) mediante un dispositivo de comparación (7) se verifica la coincidencia de las informaciones de salida (A1, Ar) del, al menos un, primer dispositivo de datos (1) y del, al menos un, dispositivo de datos de referencia (4) en referencia al software relevante para la seguridad (2) y si hay una coincidencia se envía la información de datos relativos a la seguridad (D).

2. Procedimiento según la reivindicación 1,

caracterizado porque,

en el caso de una pluralidad de primeros dispositivos de datos y una pluralidad de dispositivos de datos de referencia, se emiten informaciones de datos relacionados con la seguridad cuando una verificación de las informaciones de salida de los primeros dispositivos de datos y los dispositivos de datos de referencia con respecto al software relevante para la seguridad ha demostrado que existe una coincidencia en cada caso con respecto a una mayoría cualificada de los primeros dispositivos de datos y de los dispositivos de datos de referencia.

3. Procedimiento según la reivindicación 1 ó 2,

caracterizado porque,

como software adicional se utiliza un software de protección de datos (8).

4. Procedimiento según una de las reivindicaciones precedentes,

caracterizado porque,

como software adicional se utiliza un software externo (9,10).

5. Procedimiento según una de las reivindicaciones precedentes,

caracterizado porque,

antes de la prueba de conformidad, el, al menos un, primer dispositivo de datos está equipado con al menos un software adicional no relevante para la seguridad de tal manera que el programa y los datos están separados entre sí; en donde como datos se utilizan datos de prueba con un código y, después de la prueba de conformidad, el, al menos un, primer dispositivo de datos es provisto de datos actualizados en el mismo programa usando el código después de la verificación de la validez de los datos actualizados.

6. Procedimiento según la reivindicación 5,

caracterizado porque,

cuando se utiliza el software adicional, la validez del código de los datos de dicho software adicional se verifica mediante el software relevante para la seguridad.

7. Procedimiento según una de las reivindicaciones 5 ó 6,

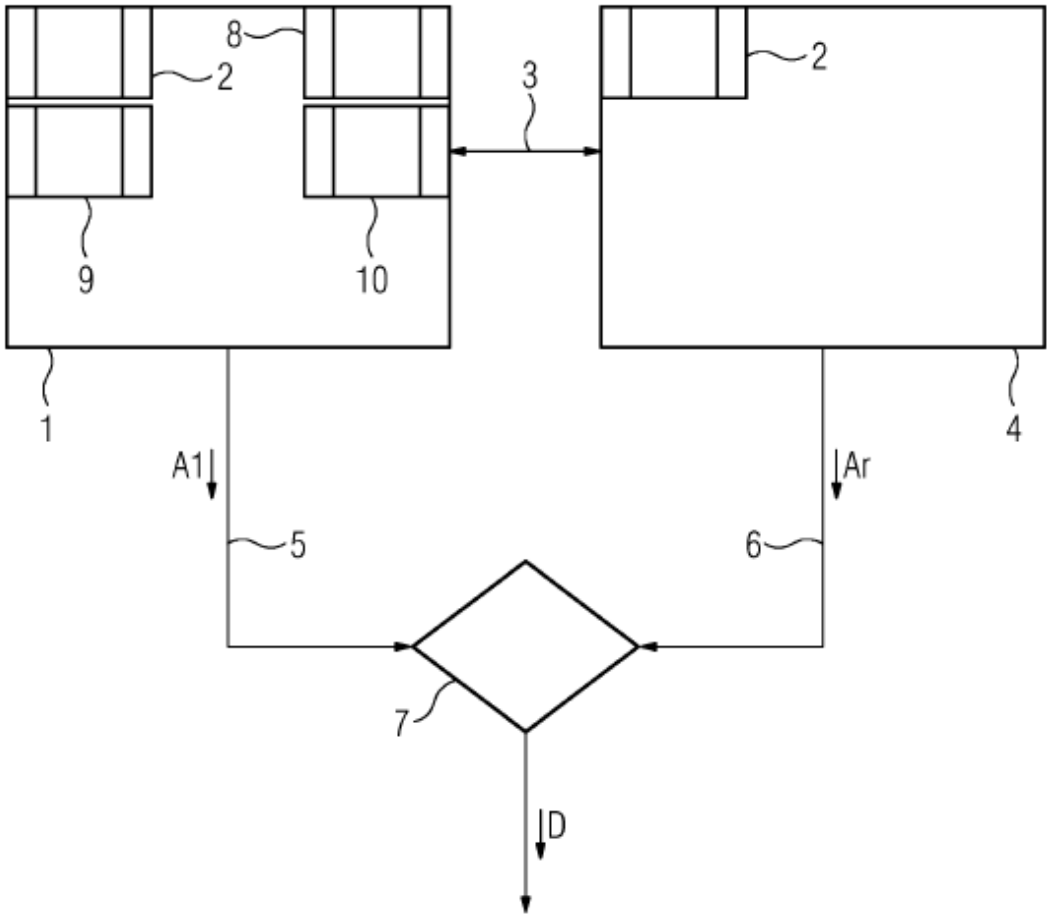
caracterizado porque,

para la actualización del software adicional (8, 9, 10), el primer dispositivo de datos (1) es provisto de datos actualizados de dicho software adicional utilizando el código de manera independiente de la transferencia de los datos actualizados.

8. Procedimiento según una de las reivindicaciones precedentes,

caracterizado porque,

como sistema crítico para la seguridad se utiliza un sistema de seguridad de trenes y como al menos un primer dispositivo de datos se utiliza una computadora operativa y como dispositivo de comparación se utiliza un enclavamiento.


8
2
3
2
9
10
1
4
A1
Ar
5
6
7
D