(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 546 018**

(51) Int. CI.:

B60R 16/023 (2006.01)
B60R 25/00 (2013.01)
G06F 9/445 (2006.01)
H04L 12/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **28.11.2006 E 06819817 (5)**

(97) Fecha y número de publicación de la concesión europea: **12.08.2015 EP 1966008**

(54) Título: **Procedimiento para la distribución de módulos de software**

(30) Prioridad:

22.12.2005 DE 102005061393

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.09.2015

(73) Titular/es:

ROBERT BOSCH GMBH (100.0%)
POSTFACH 30 02 20
70442 STUTTGART, DE

(72) Inventor/es:

VON SCHWERTFUEHRER, GERIT;
NIEMANN, HOLGER;
HAGMAN, PER;
DUBS, ALEXANDER y
GRESKAMP, SIEGFRIED

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Procedimiento para la distribución de módulos de software

La invención se refiere a un procedimiento para la distribución de módulos de software, a una instalación para la distribución de módulos de software, a un programa de ordenador y a un producto de programa de ordenador.

Estado de la técnica

Existen esfuerzos para poder realizar en el futuro una distribución libre de software de aparatos de control de vehículos sobre aparatos de control presentes en el vehículo. En este caos, hay que tener en cuenta especialmente aspectos de seguridad. Una distribución totalmente libre de módulos de software en este contexto podría conducir a que cada aparato de control, sobre el que deben distribuirse los módulos de software, deba cumplir los máximos requerimientos de seguridad de los módulos de software a distribuir. Sin embargo, en este caso existe el peligro de que se asignen módulos de software relevantes para la seguridad a un aparato de control que no cumple los requerimientos de seguridad de estos módulos de software relevantes para la seguridad. Por lo demás, es concebible que los módulos de software relevantes para la seguridad no puedan ser distribuidos. Esto significaría una limitación de la distribución prevista de software.

La publicación DE 102 19 501 A1 publica un ejemplo de esta colaboración de módulos de software y módulos de hardware teniendo en cuenta aspectos críticos para la seguridad. Esta publicación se refiere a un procedimiento para la mejora de medidas de dominio de errores, en particular en sistemas de automatización, que están constituidos por al menos un módulo de CPU estándar con software integrado, al menos un módulo de la periferia a prueba de fallos y al menos un canal de comunicación para la comunicación entre el módulo de CPU estándar y el módulo de la periferia a prueba de fallos, en el que el software del módulo de CPU estándar está constituido por un sistema operativo y un programa de usuario. Durante la verificación de errores en datos críticos para la seguridad y/o la verificación de errores durante el procesamiento de datos críticos para la seguridad se utiliza dentro del módulo de CPU estándar una combinación de procesamiento diverso y codificado de datos y/o de operaciones.

El documento EP-A-1455312 publica un procedimiento y una instalación de acuerdo con el estado de la técnica más próximo.

Ante estos antecedentes, se propone un procedimiento con las características de la reivindicación 1 de la patente, una instalación con las características de la reivindicación 7 de la patente, un programa de ordenador con las características de la reivindicación 11 de la patente y un producto de programa de ordenador con las características de la reivindicación 12 de la patente.

Ventajas de la invención

En el procedimiento de acuerdo con la invención para la distribución de módulos de software sobre aparatos de control se asocian a los aparatos de control los módulos de software teniendo en cuenta las características de clasificación relevantes para la seguridad.

La instalación de acuerdo con la invención está configurada para la distribución de módulos de software sobre aparatos de control. Está previsto que esta instalación de acuerdo con la invención asocie a los aparatos de control módulos de software teniendo en cuenta características de clasificación relevantes para la seguridad.

Otras configuraciones ventajosas se deducen a partir de las reivindicaciones dependientes de la patente.

La invención se refiere, además, a un programa de ordenador con medios de codificación de programa para ejecutar todas las etapas de un procedimiento de acuerdo con la invención, cuando el programa de ordenador es ejecutado en un ordenador o en una unidad de cálculo correspondiente, en particular una instalación de acuerdo con la invención.

La invención se refiere también a un producto de programa de ordenador con medios de códigos de programa, que están registrados en un soporte de datos legible por ordenador, para realizar todas las etapas de un procedimiento de acuerdo con la invención, cuando el programa de ordenador es ejecutado en un ordenador o en una unidad de cálculo correspondiente, en particular una instalación de acuerdo con la invención.

Con la invención es posible una clasificación de módulos de software y, por lo tanto, de software, que deben ser distribuidos sobre aparatos de control. Además, se puede realizar una clasificación de los aparatos de control con respecto a su relevancia para la seguridad o bien sus requerimientos de seguridad y una consideración de estas características de clasificación relevantes para la seguridad durante un proceso de la distribución de los módulos de software o de porciones de este software. La invención permite de acuerdo con ello una distribución especialmente selectiva de módulos de software relevantes para la seguridad sobre aparatos de control de un conjunto de aparatos de control.

En este caso existe la posibilidad de ahorrar costes de hardware en el conjunto de aparatos de control, en el caso de que no cada aparato de control esté sometido a los mismos requerimientos de seguridad. Sobre los diferentes aparatos de control dentro del conjunto de aparatos de control, por ejemplo en un vehículo, se pueden instalar de acuerdo con la distribución o asociación, respectivamente, sólo determinados módulos de software. Por lo demás, se puede evitar que los módulos de software relevantes para la seguridad sean distribuidos sobre aparatos de control, que no corresponden a los requerimientos de seguridad.

En una configuración de la invención, se dividen en primer lugar todos los módulos de software, que deben distribuirse sobre los aparatos de control, con la ayuda de características de clasificación relevantes para la seguridad. De la misma manera se dividen los aparatos de control, sobre los que deben distribuirse los módulos de software, con la ayuda de las mismas características de clasificación relevantes para la seguridad. De esta manera se clasifican y se dividen los módulos de software y los aparatos de control con respecto a una realización de requerimientos de seguridad de acuerdo con los mismos aspectos. Las características de clasificación pueden estar normalizadas de acuerdo con requerimientos de seguridad dados.

Durante la distribución de los módulos de software relevantes para la seguridad se permite una asignación de al menos un módulo de software solamente a un aparato de control, que cumple al menos las características de clasificación relevantes para la seguridad del módulo de software relevante para la seguridad. Si no se cumplen tales características de clasificación, no se puede realizar ninguna asignación.

Como características de clasificación relevantes para la seguridad se podría utilizar, por ejemplo, el nivel de integridad de la seguridad (SIL) según DIN EN 61508, que está dividido típicamente en cinco grados de SIL0 a SIL4. De esta manera, se puede asociar a un primer módulo de software o bien a una primera función de software, por ejemplo para un control de ventilador un SIL de 0 y a un segundo módulo de software o bien a una segunda función de software, que está configurado para el cálculo de un momento de deseo del conductor desde una posición del pedal el acelerador, por ejemplo un SIL de 3.

Un primer aparato de control sin redundancia de software y concepto de seguridad solamente puede recibir módulos de software de grado SIL0, un segundo aparato de control con una redundancia de software, que presenta, por ejemplo, dos procesadores y que está equipado con un concepto de seguridad, puede recibir software hasta el grado SIL3.

En este ejemplo, la segunda función de software debería distribuirse sobre el segundo aparato de control. La primera función de software podría asignarse a los dos aparatos de control. Puesto que el primer aparato de control no requiere redundancia ni concepto de seguridad, es más económico que el segundo aparato de control.

La distribución se puede desarrollar automáticamente, pero también se puede realizar manualmente y se puede emplear, por ejemplo, en el marco de software distribuido, que está presente en módulos de software y está previsto para aparatos de control en automóviles.

Otras ventajas y configuraciones de la invención se deducen a partir de la descripción y del dibujo adjunto.

Se entiende que las características mencionadas anteriormente y las características que se explican todavía a continuación no sólo se pueden aplicar en la combinación indicada en cada caso, sino también en otras combinaciones o en particular, sin abandonar el marco de la presente invención.

La invención se representa esquemáticamente con la ayuda de un ejemplo de realización en el dibujo y se describe en detalle a continuación con referencia al dibujo.

La figura 1 muestra en representación esquemática un ejemplo de realización para la distribución de módulos de software sobre aparatos de control.

En la figura 1 se representan esquemáticamente varios módulos de software 2, 4, una instalación 6 así como varios aparatos de control 8, 10 dentro de un conjunto de aparatos de control 12, por ejemplo en un vehículo o en un dispositivo electromecánico.

Está previsto que los módulos de software 2, 4 sean distribuidos teniendo en cuenta requerimientos de seguridad sobre los aparatos de control 8, 10. En este caso, hay que tener en cuenta que no se asigna ningún módulo de software 2, 4 a un aparato de control 8, 10, que no cumple sus requerimientos de seguridad.

La instalación 6 está configurada para asociar a los aparatos de control 8, 10 módulos de software 2, 4 teniendo en cuenta características de clasificación relevantes para la seguridad. A tal fin, los módulos de software 2, 4y los aparatos de control 8, 10 son clasificados a través de la instalación 6 y son divididos con la ayuda de las características de clasificación. A tal fin se utilizan como característica de clasificación los niveles de integridad de la seguridad. En este caso se verifica a través de la instalación 6, qué característica de clasificación cumple, respectivamente, un aparato de control 8, 10, de manera que se asignan a este aparato de control 8, 10 módulos de

software 2, 4 correspondientes en función de las características de clasificación cumplidas.

En el presente ejemplo de realización se clasifican a través de la instalación 6 un primer módulo de software 2 y un primer aparato de control 8 y de esta manera se verifica el cumplimiento de características de clasificación relevantes para la seguridad. Como escala se utiliza en este caso el nivel de integridad de la seguridad distribuido en varios grados o escalones relevantes para la seguridad. En este caso, el primer aparato de control 8 cumple los requerimientos de seguridad del primer módulo de software 2, puesto que el nivel de integridad de la seguridad del primer aparato de control 8 es al menos de la misma magnitud que el nivel de integridad de la seguridad del primer módulo de software 2. Por lo tanto, el primer módulo de software es asignado al primer aparato de control 8 y es instalado en este primer aparato de control 8.

Con la presente invención es posible una distribución libre de módulos de software 2, 4 y, por lo tanto, de software de aparatos de control de vehículos sobre los aparatos de control 8, 10 presentes en el vehículo. En este caso, se pueden tener en cuenta ahora especialmente aspectos de seguridad. Por lo tanto, en el caso de una distribución totalmente libre de módulos de software 2, 4 no es necesario ya que cada aparato de control 8, 10, sobre el que deben distribuirse los módulos de software 2, 4, deban cumplirse los requerimientos de seguridad de los módulos de software 2, 4 a distribuir.

Tampoco existe ya el peligro de que se asignen módulos de software 2, 4 relevantes para la seguridad a un aparato de control 8, 10, que no cumple los requerimientos de seguridad de estos módulos de software 2, 4 relevantes para la seguridad. Los módulos de software 2, 4 se pueden distribuir ahora de forma selectiva teniendo en cuenta las características de clasificación relevantes para la seguridad.

REIVINDICACIONES

1.- Procedimiento para la distribución de módulos de software (2, 4) con diferentes requerimientos de seguridad sobre aparatos de control, (8, 10), que se diferencian con respecto al cumplimiento de los requerimientos de seguridad, caracterizado porque se asignan a los aparatos de control (8, 10) los módulos de software (2, 4) teniendo en cuenta características de clasificación relevantes para la seguridad.

2.- Procedimiento de acuerdo con la reivindicación 1, en el que los módulos de software (2, 4) son clasificados y son distribuidos con la ayuda de las características de clasificación.

3.- Procedimiento de acuerdo con la reivindicación 1 ó 2, en el que los aparatos de control (8, 10) son clasificados y son distribuidos con la ayuda de las características de clasificación.

4.- Procedimiento de acuerdo con una de las reivindicaciones anteriores, en el que se verifica qué características de seguridad cumple, respectivamente, un aparato de control (8, 10), de manera que se asigna a este aparato de control (8, 10) al menos un módulo de software (2, 4) en función de las características de clasificación cumplidas.

5.- Procedimiento de acuerdo con una de las reivindicaciones anteriores, en el que como característica de clasificación se utilizan niveles de integridad de la seguridad.

6.- Procedimiento de acuerdo con una de las reivindicaciones anteriores, que se realiza para aparatos de control (8, 10) de un vehículo, en el que los aparatos de control (8, 10) realizan por medio de los módulos de software (2, 4) funciones del vehículo, por ejemplo el control de un ventilador o el cálculo de un momento de deseo del conductor desde una posición del pedal del acelerador.

7.- Instalación, que está configurada para la distribución de módulos de software (2, 4) sobre aparatos de control (8, 10), caracterizada porque la instalación asocia módulos de software (2, 4) a los aparatos de control (8, 10) teniendo en cuenta características de clasificación relevantes para la seguridad.

8.- Instalación de acuerdo con la reivindicación 7, que está configurada para clasificar módulos de software (2, 4) y para distribuidos con la ayuda de las características de clasificación.

9.- Instalación de acuerdo con la reivindicación 7 u 8, que está configurada para clasificar los aparatos de control (8, 10) y distribuirlos con la ayuda de las características de clasificación.

10.- Instalación de acuerdo con una de las reivindicaciones 7 a 9, que está configurada para verificar qué características de clasificación cumple, respectivamente, un aparato de control (8, 10), y para signar a este aparato de control (8, 10) al menos un módulo de software (2, 4) en función de las características de clasificación cumplidas.

11.- Programa de ordenador con medios de codificación de programa para realizar todas las etapas de un procedimiento de acuerdo con una de las reivindicaciones 1 a 6, cuando el programa de ordenador es ejecutad en un ordenador o una unidad de cálculo correspondiente, en particular una instalación (6) de acuerdo con una de las reivindicaciones 7 a 10.

12.- Producto de programa de ordenador con medios de códigos de programas, que están registrados en un soporte de datos legible por ordenador, para realizar todas las etapas de un procedimiento de acuerdo con una de las reivindicaciones 1 a 6, cuando el programa de ordenador es ejecutado en un ordenador o una unidad de cálculo correspondiente, en particular unas instalación (6) de acuerdo con una de las reivindicaciones 7 a 10.

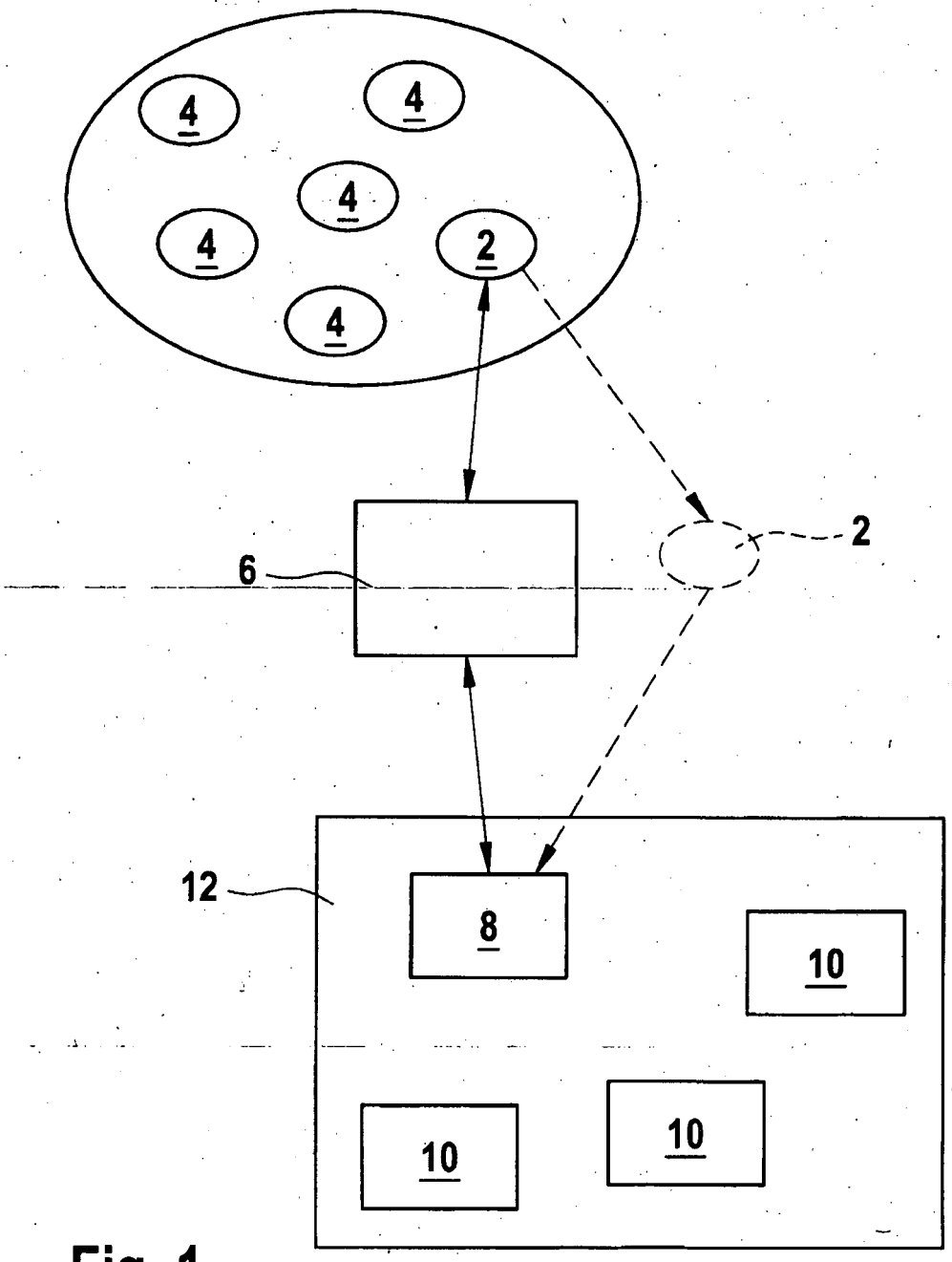

Fig. 1