(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 713 448**

(51) Int. CI.:

G06F 11/07 (2006.01)
G06F 9/445 (2008.01)
G06F 11/14 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **04.06.2014 PCT/EP2014/061594**

(87) Fecha y número de publicación internacional: **24.12.2014 WO14202388**

(96) Fecha de presentación y número de la solicitud europea: **04.06.2014 E 14730114 (7)**

(97) Fecha y número de publicación de la concesión europea: **28.11.2018 EP 2992426**

(54) Título: **Procedimiento para verificar un estado de funcionamiento seguro de un ordenador**

(30) Prioridad:

19.06.2013 DE 102013211504

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
21.05.2019

(73) Titular/es:

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

(72) Inventor/es:

ECKELMANN-WENDT, UWE

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Procedimiento para verificar un estado de funcionamiento seguro de un ordenador

Descripción

La invención hace referencia a un procedimiento para verificar un estado de funcionamiento seguro de un ordenador para controlar un sistema crítico para la seguridad, particularmente un sistema de seguridad ferroviario.

Los sistemas críticos para la seguridad son por lo general sistemas de control y de regulación, los cuales se utilizan, por ejemplo, en el control de enclavamiento, el control de accionamiento y de frenado para todo tipo de medios de transporte, así como en la técnica de fabricación y la instrumentación y control de procesos, o en la regulación de centrales eléctricas. En estos casos, por lo general, se detectan mediante sensores valores de medición para realizar acciones en actuadores. Con frecuencia, para estas tareas de regulación y de control deben estar garantizadas propiedades referidas a la seguridad. Los niveles de seguridad están definidos por la Norma CENELEC EN50129, que van desde SIL 0 (no seguro desde el punto de vista de la técnica de señalización) hasta SIL 4 (en alto grado seguro desde el punto de vista de la técnica de señalización).

Eventualmente, para actualizaciones de software, no se puede garantizar de manera automatizada el cumplimiento de las propiedades referidas a la seguridad, sino que se debe asegurar mediante medidas operativas. Aquí, debe ser comprobado por un operador que el ordenador o el conjunto de ordenadores que controlan el sistema crítico para la seguridad se encuentra en un estado de funcionamiento seguro. En ningún caso, la carga de software en un ordenador equivocado o un software con errores puede conducir a que el ordenador sea capacidaz de controlar el sistema crítico para la seguridad.

La siguiente descripción se refiere fundamentalmente al uso del procedimiento para verificar un estado de funcionamiento seguro de un sistema de seguridad ferroviario, sin que por ello la invención esté restringida a esta aplicación especial.

Los sistemas de seguridad ferroviarios comprenden particularmente el control de elementos de campo como por ejemplo agujas, señales, dispositivos de indicación de vía libre, y pasos a nivel. La carga de programas en el ordenador que controla es problemática, cuando antes de que finalice la prueba manual para determinar si los programas auténticos correctos se han cargado en el ordenador correcto, es posible un efecto externo, o sea un funcionamiento eficiente de los programas.

Por la solicitud DE 10 2009 009 947 A1 se conoce un procedimiento para asignar direcciones para un ordenador, en el cual la dirección se asocia a un hardware, de modo que la dirección no puede ser modificada ni eliminada por intervenciones de software.

Un procedimiento de esta clase se indica en la patente DE 10 2010 015 285 A1. Allí, el sistema genera un código de activación que no puede ser evaluado mecánicamente, el cual debe ser ingresado de manera manual en el sistema a fin de corroborar el estado seguro de funcionamiento.

Lo desventajoso del procedimiento conocido consiste ante todo en que el mismo requiere de un acuerdo de utilizar el ordenador solamente en un estado de funcionamiento seguro, de modo que la decisión respecto a si efectivamente hay un estado de funcionamiento seguro debe ser tomada por un operador. Además, no está excluido que algún programa pueda conectar el ordenador eludiendo el código de activación. Una inicialización con un programa aún sin confirmar, pero por lo demás, con capacidad de funcionamiento no se puede evitar por ejemplo en los ordenadores con diseño SIMIS. En el caso de un ordenador cargado de forma remota, el correcto proceso de carga se comprueba tras la relectura de los software cargados o de sus valores hash. Sin embargo, existe un vacío entre la carga del software y la finalización de la prueba. Durante este vacío, el ordenador puede ser ejecutado con un programa no comprobado y defectuoso, sin que resulte reconocible por fuera, y puede ya ser utilizado en este estado no seguro. La presente invención tiene por objeto especificar un procedimiento de este tipo, el cual evita que el programa cargado pueda operar hacia afuera antes de que esté comprobado que el programa no presenta errores y funciona en el ordenador previsto.

Conforme a la invención, el procedimiento comprende los pasos indicados en la reivindicación 1.

El sello electrónico de inicialización transferido por separado complementa la comprobación del código de programa y del número de identificación de ordenador, según el primer paso del procedimiento conforme a la invención. El procedimiento posibilita la prueba del correcto almacenamiento de programa, de la versión del programa y de otras condiciones de programa, antes de que el programa pueda operar efectivamente. El ordenador se puede utilizar para el control del sistema crítico para la seguridad, sólo cuando los valores vinculados en el paso 3 para el sello electrónico de inicialización, el código de programa y el número de identificación de ordenador son consistentes, o

sea se corresponden con los valores esperados. Una inicialización del ordenador sin el sello electrónico de inicialización transferido no arroja un código de activación correcto, porque sólo el sello electrónico de inicialización suministrado cuasi posteriormente permite probar si se ha cargado correctamente en la memoria de programa el programa correcto en el ordenador correcto. Después de una coincidencia con los valores vinculados esperados se realiza una activación controlada del módulo de salida del ordenador. El módulo de salida del ordenador, o sea un módulo de hardware, debe ser activado antes de que el programa de ordenador pueda operar hacia afuera. El sello electrónico de inicialización requerido para esta activación no evita en sí la ejecución del programa, sino que establece sólo una condición que permite o evita un efecto externo del programa de ordenador.

La vinculación para calcular el código de activación se realiza en un área de memoria de programa no transferible del ordenador, para asegurar con ello, que ningún programa del ordenador pueda conectar efectivamente el ordenador con tecnología de seguridad, eludiendo la generación del código de activación prevista. El código de activación establece el valor inicial para las propiedades de hardware, sin las cuales el ordenador no puede operar hacia afuera. Si el código de activación no es correcto, el ordenador no puede ejecutarse efectivamente en referencia al control del sistema crítico de seguridad, pero puede aún comunicar por ejemplo con dispositivos de carga de programas a través de las conexiones de datos comprobadas, o sea puede enviar y recibir datos. En principio, el código de activación debe presentar propiedades, las cuales se reconocen mediante el hardware del ordenador, para activar el ordenador en un modo efectivo. El procedimiento permite una conexión controlada de los "puertos de salida" del ordenador para que el ordenador pueda actuar en su entorno. Si bien el programa de ordenador opera sin dicho código de activación, las salidas al sistema crítico para la seguridad se pierden porque el hardware no reacciona a las mismas.

Después de la carga del programa de ordenador, el ordenador es operable en una medida restringida, pero todavía no puede actuar hacia afuera, ya que aún no está cargado el sello electrónico de inicialización. Primero se relee el programa de operador, o su código de programa, o bien, su valor hash y se compara con el primer valor esperado. Allí el ordenador también se identifica inequívocamente por su número de identificación de ordenador específico. Cuando del ordenador esperado se puede releer el esperado valor hash de programa de ordenador, en el área de memoria de programa no transferible del ordenador se almacena el sello electrónico de inicialización válido sólo para ese ordenador y sólo para ese programa de ordenador. Por un área de memoria de programa no transferible se entiende un área en la cual el programa no puede ser transferido, aunque sí se pueden almacenar valores y evaluarlos o procesarlos. Esta área de memoria de programa no transferible calcula el valor hash del programa de ordenador, su inequívoco número de identificación y el sello electrónico de inicialización para formar el código de activación. Este valor calculado es entonces un código de activación efectivo sólo cuando el programa de ordenador, el número de identificación de ordenador y el sello electrónico de inicialización se corresponden. El código de activación se envía después al hardware del módulo de salida del ordenador, con lo cual se asegura que sólo ese hardware (y no un software) puede conectar eficientemente el ordenador.

Conforme a la reivindicación 2, está previsto que el módulo de salida del ordenador compare la dirección del área de la memoria de programa que ha generado el código de activación, con un valor teórico. De esta manera se asegura adicionalmente que el código de activación proviene del área de memoria de programa no transferible, prevista para ello, y que no es algún otro segmento de programa el que suministra el código de activación al hardware del módulo de salida. Un código de activación de este tipo que eluda el área de memoria de programa no transferible, no es aceptado por el módulo de salida. El módulo de salida evalúa para ello la dirección de programa física del origen del código de activación.

Preferentemente, conforme a la reivindicación 3, el área de memoria de programa no transferible está proporcionada en un PLD (programmable logic device/ dispositivo de lógica programable) del CPU (central processing unit/ unidad central de procesamiento) del ordenador. El PLD el CPU calcula el código de activación, conforme a un algoritmo programado a partir del código de programa del programa de ordenador, del número de identificación de ordenador y del sello electrónico de inicialización. En este caso, debe resultar un valor previamente conocido para el código de activación, el cual se puede transferir al módulo de salida sólo por el código ejecutado en el PLD. En los ordenadores SIMIS, el código de activación puede ser el código de inicialización para la liberación de tiempo cíclico, que debe comprender cada hardware de CPU SIMIS como propiedad "Watchdog" (perro guardián).

Conforme a la reivindicación 4, está previsto que después de cada cambio del sello electrónico de inicialización, particularmente ante una recarga del programa de ordenador, el área de memoria de programa no transferible calcule el código de liberación; en donde el sello electrónico de inicialización eventualmente presente se elimina y un sello electrónico de inicialización actual debe ser almacenado. De esta manera se consigue una seguridad adicional en cada cambio del sello electrónico de inicialización y no solamente en la primera carga del programa de ordenador. El código de activación debe ser recalculado al menos en cada cambio del sello electrónico. Recalcular el código solamente en la recarga del programa no es suficiente, porque entonces probablemente no se haría efectiva una eliminación del sello electrónico de inicialización en el código de activación calculado.

El sello electrónico de inicialización no necesita ser borrado con cada inicialización del ordenador, sino sólo cuando se realiza una recarga del programa de ordenador, porque en un reinicio el valor hash del programa y el número de identificación de programa no están modificados, de modo que el ordenador puede iniciar con el mismo sello electrónico de inicialización tantas veces como se desee. En consecuencia, el sello electrónico no tiene que borrarse después de un único uso.

Para obtener las mismas condiciones con un programa idéntico tras una recarga, se evita una actuación de tecnología de seguridad del ordenador antes de que el sello electrónico de inicialización haya sido transferido.

Si el mismo programa hubiera sido cargado nuevamente sin haber eliminado el sello electrónico de inicialización, entonces actuaría el antiguo sello electrónico de inicialización que no fue eliminado. Esto es particularmente indeseado cuando la intención es cargar un nuevo programa con el fin de corregir errores, pero sin embargo se ha cargado por equivocación el antiguo programa nuevamente, el cual se hace efectivo de forma inmediata. Sin que resulte reconocible, ya que el antiguo sello electrónico de inicialización no había sido borrado, no se pudo hacer efectiva una corrección de errores. En caso de que esto se descubra con la relectura y la prueba, existe sin embargo una ventana temporal en la cual no puede evitarse el efecto del programa. Entonces el programa opera con los antiguos errores y la situación es la misma que antes de la carga. Esto es peligroso si el efecto del error implicara que se deba evitar obligatoriamente el desarrollo del antiguo programa.

Cuando conforme a la reivindicación 5, para el ordenador se permite sólo un número limitado de inicializaciones del ordenador, o sea de arranques; también resulta necesario eliminar el sello electrónico de inicialización, por ejemplo, tras la carga de una versión de prueba que no debe ser utilizada de manera permanente. Para ello, el código de activación calculado a partir del valor hash, número de identificación de ordenador y sello electrónico de inicialización puede a través de otro valor teórico aparte activar la eliminación del sello electrónico de inicialización.

Conforme a la reivindicación 6 está previsto de manera preferida que la eliminación del sello electrónico de inicialización posibilite la recarga del programa de ordenador. De esta manera, el nuevo programa se puede cargar sólo entonces cuando ya no hay un sello electrónico de inicialización válido almacenado. El sello electrónico de inicialización debe entonces inevitablemente estar eliminado para preparar la carga. Ya que debe haber un mecanismo para proporcionar el sello electrónico de inicialización, se puede utilizar también el mismo mecanismo para destruir el sello electrónico de inicialización. La destrucción del sello electrónico de inicialización con el mismo proceso que genera el sello electrónico, evita de manera eficaz el funcionamiento de tecnología de seguridad de un programa reconocido como defectuoso. Romper el sello electrónico puede resultar entonces apropiado en términos de tecnología de seguridad incluso sin una (inmediata) nueva carga de programa.

Aunque también es posible una variante desarmada; en donde conforme a la reivindicación 7, el sello electrónico de inicialización se cargue junto con el programa de ordenador. Para ordenadores que no tienen gran responsabilidad en la seguridad, o ninguna, el sello electrónico de inicialización se transfiere al mismo tiempo que el programa de ordenador, o el código de programa, y no se envía con posterioridad después de la prueba en relación al primer valor esperado. Por el inequívoco número de identificación de ordenador, está siempre garantizado que el programa se encuentra en el ordenador correcto; en donde el programa de ordenador está vinculado al ordenador determinado por la formación del código de activación. Sin embargo, cuasi por descuido se podría cargar una versión de programa, aunque válida, obsoleta o demasiado nueva. Por la omisión del paso de prueba, no se puede excluir una inseguridad residual a causa de la transferencia de sello electrónico de inicialización que no se realizó por separado.

Si el procedimiento se llevara adelante sin eliminar el sello electrónico de inicialización, sería concebible que por descuido se pudiera omitir una actualización necesaria de programa. Este riesgo residual debe evaluarse en relación a los requerimientos de tecnología de seguridad al igual que el riesgo residual de transferir el sello electrónico de inicialización con la carga de programa.

REIVINDICACIONES

1. Procedimiento para verificar un estado de funcionamiento seguro de un ordenador para controlar un sistema crítico para la seguridad, particularmente un sistema de seguridad ferroviario, caracterizado por los siguientes pasos:

• se releen una combinación de un programa de ordenador cargado, o de su código de programa o de su valor de hash y de un número de identificación de ordenador; y se comparan con los primeros valores esperados;

• un sello electrónico de inicialización válido solamente para la combinación proporcionada de programa de ordenador, código de programa o valor de hash y de número de identificación de ordenador se almacena en un área de memoria de programa no transferible del ordenador; y

• el área de memoria de programa no transferible del ordenador está proporcionada en un PLD (programmable logic device/ dispositivo de lógica programable) del CPU (central processing unit/ unidad central de procesamiento), y el PLD calcula el sello electrónico de inicialización con la combinación de programa de ordenador, código de programa o valor hash y de número de identificación de ordenador para formar un código de activación, el cual si hay coincidencia con un segundo valor esperado se envía al hardware de un módulo de salida del ordenador y el cual activa el último.

2. Procedimiento según la reivindicación 1, caracterizado porque el módulo de salida del ordenador compara la dirección del área de la memoria de programa que ha generado el código de activación, con un valor teórico.

3. Procedimiento según una de las reivindicaciones precedentes, caracterizado porque después de cada cambio del sello electrónico de inicialización, particularmente con una recarga del programa de ordenador, el área de memoria de programa no transferible calcula el código de liberación; en donde el sello electrónico de inicialización eventualmente presente se elimina y un sello electrónico de inicialización actual debe ser almacenado.

4. Procedimiento según la reivindicación 3, caracterizado porque el sello electrónico de inicialización se elimina después un determinado número de inicializaciones del ordenador.

5. Procedimiento según la reivindicación 3 ó 4, caracterizado porque la eliminación del sello electrónico de inicialización posibilita la recarga del programa de ordenador.

6. Procedimiento según una de las reivindicaciones precedentes, caracterizado porque el sello electrónico de inicialización se carga junto con el programa de ordenador.