(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 775 879**

(51) Int. CI.:

G06F 21/31 (2013.01)
G06F 21/57 (2013.01)
G06F 21/71 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **28.08.2017 E 17188151 (9)**

(97) Fecha y número de publicación de la concesión europea: **18.12.2019 EP 3451215**

(54) Título: **Equipo de hardware y procedimiento para operar y fabricar un equipo de hardware**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.07.2020

(73) Titular/es:

SIEMENS AKTIENGESELLSCHAFT (100.0%)
Werner-von-Siemens-Straße 1
80333 München, DE

(72) Inventor/es:

FALK, RAINER;
FEIST, CHRISTIAN PETER y
ZWANZGER, JOHANNES

(74) Agente/Representante:

LOZANO GANDIA, José

DESCRIPCIÓN

Equipo de hardware y procedimiento para operar y fabricar un equipo de hardware

La presente invención se refiere a un equipo de hardware, un procedimiento para operar un equipo de hardware y un procedimiento para fabricar un equipo de hardware.

Un equipo de hardware, como por ejemplo un aparato de control industrial, se protege a menudo frente a ataques o manipulaciones por parte de usuarios no autorizados. La protección del equipo de hardware puede denominarse también protección de integridad. La protección de integridad del equipo de hardware a menudo no puede configurarse tal que pueda modificarse sobre el equipo de hardware.

El documento US 2009/0089569 A1 da a conocer un sistema que puede arrancar un sistema operativo de varias formas, para hacer posible que los usuarios tengan un acceso rápido a determinadas funcionalidades, seguridades y aplicaciones de un aparato móvil.

El documento US 2016/0179554 A1 da a conocer un equipo para inicializar una plataforma. Además, da a conocer el documento CN 102 045 449 A un entorno de multisistema operativo para un smartphone.

Partiendo de esta base, consiste el objetivo de la presente invención en lograr un procedimiento mejorado para operar un equipo de hardware. Otro objetivo consiste en proporcionar un equipo de hardware mejorado. Además, debe proporcionarse un procedimiento mejorado para fabricar un equipo de hardware.

Estos objetivos se logran mediante un procedimiento para operar un equipo de hardware según la reivindicación 1, así como mediante un equipo de hardware según la reivindicación 8. Determinados aspectos de la invención se describen en las reivindicaciones secundarias.

En determinadas formas de ejecución se propone un procedimiento para operar un equipo de hardware que es adecuado para ejecutar varias funciones diferentes. El procedimiento incluye:

Memorización en el equipo de hardware de varios perfiles de protección de integridad para el equipo de hardware, pudiendo asignarse cada perfil de protección de integridad a una de las varias funciones distintas y definiendo cada perfil de protección de integridad medidas de seguridad para proteger un hardware y un software del equipo de hardware frente a manipulaciones;
elección de un perfil de protección de integridad de entre los varios perfiles de protección de integridad como un perfil de protección de integridad elegido, teniendo en cuenta una función a ejecutar mediante el equipo de hardware de entre las varias funciones diferentes y
ejecución de las medidas de seguridad del perfil de protección de integridad elegido.

Además, según una forma de ejecución se propone un equipo de hardware que es adecuado para ejecutar varias funciones distintas. El equipo de hardware incluye:

Un equipo de memoria para memorizar varios perfiles de protección de integridad para el equipo de hardware, pudiendo asignarse cada perfil de protección de integridad a una de las varias funciones diferentes y definiendo cada perfil de protección de integridad medidas de seguridad para proteger un hardware y un software del equipo de hardware frente a manipulaciones;
un equipo de determinación, para determinar un perfil de protección de integridad elegido, que ha sido elegido de entre los varios perfiles de protección de integridad teniendo en cuenta una función a ejecutar mediante el equipo de hardware de entre las varias funciones diferentes y
un equipo de seguridad para ejecutar las medidas de seguridad del perfil de protección de integridad elegido.

El equipo de hardware es en particular adecuado para operar según el procedimiento antes descrito y que se describe a continuación. El concepto "operar" incluye tanto la fabricación del equipo de hardware como también la configuración y la utilización del equipo de hardware.

El equipo de hardware puede ser un aparato de campo, un aparato de Internet de las cosas, un aparato de control o similares. En particular es el equipo de hardware un sistema embebido. El equipo de hardware incluye en particular una parte de hardware y una parte de software. La parte del software, denominada a continuación también "software", puede incluir por ejemplo códigos ejecutables, así como datos memorizados en el equipo de hardware. La parte de hardware, denominada a continuación también "hardware", puede incluir por ejemplo una carcasa del equipo de hardware, así como una memoria física del equipo de hardware.

El equipo de hardware puede ser en particular adecuado para ejecutar distintas funciones. Las funciones posibles pueden incluir por ejemplo controlar, memorizar o calcular. Por ejemplo, puede realizarse el equipo de hardware tanto como servidor como también como cliente para una red.

Al equipo de hardware pueden estar asociados varios perfiles de protección de integridad, que definen en cada caso medidas de seguridad para proteger tanto el hardware como también el software. Las mismas están memorizadas en el equipo de memoria, que en particular está configurado como una memoria de datos no volátil. En particular sirven las medidas de seguridad de los correspondientes perfiles de protección de integridad para la protección de integridad del equipo de hardware. Bajo protección de integridad del equipo de hardware puede entenderse por ejemplo impedir y/o detectar manipulaciones y/o ataques al equipo de hardware por parte de usuarios malignos y/o no autorizados.

Los perfiles de protección de integridad pueden estar asociados a las distintas funciones o bien ser independientes de las funciones. Además, pueden diferenciarse entre sí los perfiles de protección de integridad por ejemplo mediante su nivel de seguridad, por ejemplo "alto", "medio", "bajo".

De entre los perfiles de protección de integridad puede elegirse el perfil de protección de integridad a elegir en dependencia de la función que ha de ejecutar el equipo de hardware. Si el equipo de hardware por ejemplo debe utilizarse en un entorno que exige una elevada seguridad, por ejemplo, como una memoria de claves, puede elegirse un perfil de protección de integridad que garantice una elevada protección de integridad al equipo de hardware. Si el equipo de hardware ha de utilizarse en un entorno en el que la integridad del equipo de hardware no es relevante, por ejemplo, en una estructura de tests o en una zona de acceso protegido, puede elegirse un perfil de protección de integridad que garantice una baja protección de integridad al equipo de hardware.

El perfil de protección de integridad puede elegirse y/o fijarse tal que no pueda modificarse ya durante la fabricación, en particular mientras se proyecta. Además, es posible modificar el perfil de protección de integridad durante la utilización u operación del equipo de hardware según se desee.

La protección de integridad del equipo de hardware puede determinarse mediante las medidas de seguridad del perfil de protección de integridad elegido. La ejecución de las medidas de seguridad puede servir para proteger la integridad del equipo de hardware. En particular puede configurarse flexible la protección de integridad del equipo de hardware. Así puede aumentarse la seguridad del equipo de hardware.

Mediante la elección adecuada del perfil de protección de integridad puede además evitarse por ejemplo que se ejecuten medidas de seguridad cuyo cálculo es costoso, que en particular son usuales cuando la protección de la integridad es alta, aún cuando no sean necesarias las mismas. La protección de integridad del equipo de hardware puede adaptarse con miras a una utilización y/o función del equipo de hardware.

Según una forma de ejecución, incluye la realización de las medidas de seguridad, al menos:

ejecución de un arranque seguro del equipo de hardware;
comprobación de que los datos que están memorizados en el equipo de hardware son correctos;
comprobación de procesos que corren en el equipo de hardware;
ejecución de un "Mandatory Access Control" (control de acceso obligatorio) en el equipo de hardware;
virtualización de recursos del sistema operativo y/o recursos de hardware;
averiguación de si se realiza una manipulación en el equipo de hardware y/o
vigilancia de sensores tamper del equipo de hardware, que captan características físicas del equipo de hardware.

Mediante la ejecución de las medidas de seguridad puede protegerse la integridad del equipo de hardware. Por ejemplo, pueden definir las medidas de seguridad premisas para un arranque seguro del equipo de hardware, tal que el equipo de hardware pueda arrancarse con seguridad con ayuda de las medidas de seguridad. En particular puede comprobarse como parte de la protección de la integridad durante el arranque del equipo de hardware la firma del firmware, con lo que sólo se carga durante el arranque un firmware firmado correctamente.

Además, puede comprobarse como parte de la protección de integridad que los datos que están memorizados en el equipo de hardware son correctos. Esto incluye tanto datos que son específicos del equipo de hardware como también datos archivados en una memoria fijamente instalada o que puede eliminarse en el equipo de hardware. En particular se comprueba la integridad y/o invariabilidad de los datos memorizados durante el funcionamiento. Para ello pueden formarse valores hash de los datos memorizados y comprobarse si coinciden con valores de referencia memorizados en el equipo de hardware.

Además, pueden comprobarse los procesos que corren en el equipo de hardware como parte de la protección de integridad. En particular puede detectar el equipo de hardware cuándo corre un proceso que según una lista blanca previamente almacenada no es admisible.

Como parte de la protección de integridad puede estar definido también un "Mandatory Access Control", es decir, un control de acceso de software a recursos que proporciona y/o gestiona un sistema operativo del equipo de hardware. Tales recursos pueden ser por ejemplo una interfaz de red o un sistema de ficheros. El control de accesos puede realizarse por ejemplo con ayuda de SELinux, AppArmor, SMACK y/o TOMOYO.

La protección de integridad puede incluir también la virtualización de recursos del sistema operativo y/o recursos de hardware, como por ejemplo contenedores de software o máquinas virtuales.

Los recursos virtualizados representan por ejemplo una reproducción de un recurso de hardware o de software correspondiente mediante un objeto similar del mismo tipo con ayuda de una capa de abstracción a modo de una capa de abstracción de hardware. En este sentido pueden entonces reunirse o repartirse con flexibilidad recursos virtuales. Con ayuda de los recursos virtuales puede en particular probarse, protegerse y/o modificarse por medio de una prueba el equipo de hardware o sus funciones.

En particular ofrecen los recursos del sistema operativo y/o recursos de hardware, en su forma virtualizada, también una protección mejorada que puede configurarse. Por ejemplo, puede prescribirse que sólo puedan arrancarse los correspondientes contenedores de software sin acceso a la red. Se puede hablar entonces, en un contenedor de software, de un recurso virtual.

Además, puede determinarse como parte de la protección de integridad si se realiza una manipulación y/o un ataque al equipo de hardware. La determinación de si se realiza una manipulación y/o un ataque puede realizarse con ayuda de las vigilancias y/o comprobaciones antes descritas y que se describen a continuación, por ejemplo, con ayuda de una prueba de los procesos en marcha.

Además, pueden vigilarse como parte de la protección de integridad sensores tamper del equipo de hardware. Esto sensores tamper miden en particular características físicas del hardware, como por ejemplo vibraciones de la carcasa, movimientos de la carcasa y/o ruidos en el equipo de hardware. De esta manera puede protegerse el equipo de hardware también frente a ataques físicos, por ejemplo, frente a una apertura o movimiento de la carcasa. Además, pueden fijarse valores de umbral, que son vigilados por sensores tamper, en función del perfil de protección de integridad elegido. En particular se determina mediante los valores de umbral el "grado de sensibilidad" de los sensores tamper.

Según otra forma de ejecución, incluye la ejecución de las medidas de seguridad una vigilancia lógica y una vigilancia física del equipo de hardware.

En particular sirve la protección de integridad prescrita por el perfil de protección de integridad elegido tanto para la vigilancia de la integridad lógica del equipo de hardware a nivel de software como también para la vigilancia de integridad física, también vigilancia de tamper, del equipo de hardware a nivel de hardware. La protección de la integridad lógica y la protección de la integridad física están entonces en particular integradas en un concepto total formado unitariamente mediante el perfil de protección de integridad elegido, con lo que pueden interactuar procedimientos de protección de integridad lógicos y físicos, para garantizar una elevada protección continua de la integridad del equipo de hardware.

Según otra forma de ejecución, incluye el procedimiento además:

Memorización de datos de verificación en el equipo de hardware;
recepción de datos de autentificación por el equipo de hardware de un usuario que quiere elegir un perfil de protección de integridad de entre los varios perfiles de protección de integridad;
determinación de si los datos de autentificación coinciden con los datos de verificación y
si los datos de autentificación coinciden con los datos de verificación, autorización de la elección del perfil de protección de identidad.

Para la elección y/o utilización del perfil de protección de integridad elegido, puede ser necesario que el usuario se autentifique con datos de autentificación en el equipo de hardware. Los datos de autentificación pueden ser por ejemplo un código de configuración específico del aparato, compuesto por una secuencia de números. Los datos de autentificación pueden también ser datos específicos del usuario, que sirven para autentificar al usuario, por ejemplo, personal del servicio de atención (service). En determinadas formas de ejecución han de entenderse los datos de autentificación como un código de licencia.

Si los datos de autentificación coinciden con los datos de verificación memorizados en el equipo de hardware, en particular si los mismos son idénticos entre sí, se autoriza la elección del perfil de protección de integridad mediante el equipo de hardware. En particular pueden liberarse los procedimientos de protección de integridad definidos por los perfiles de protección de integridad, puede autorizarse una desactivación de un perfil de protección de integridad y/o puede autorizarse un cambio de un perfil de protección de integridad.

En formas de ejecución no se autoriza la elección del perfil de protección de integridad si los datos de autentificación recibidos no coinciden con los datos de verificación.

Una modificación del perfil de protección de integridad sólo es posible en particular cuando se reciben los datos de autentificación correctos. De esta manera puede protegerse el equipo de hardware, porque sólo usuarios autorizados pueden elegir y/o modificar el perfil de protección de integridad del equipo de hardware. En particular se impide que una vigilancia de integridad se desactive de manera no deseada, lo cual pondría en peligro la seguridad del equipo de hardware.

Según otra forma de ejecución incluye el procedimiento además:

si se averigua que tiene lugar una manipulación del equipo de hardware, se ejecuta una función de emergencia mediante el equipo de hardware, incluyendo la función de emergencia:

Emisión de una señal de aviso;
desconexión del equipo de hardware;
ejecución de un programa de funcionamiento en emergencia;
borrado de datos memorizados en el equipo de hardware;
desactivación del equipo de hardware;
desactivación de interfaces del equipo de hardware y/o
señalización de la manipulación del equipo de hardware mediante un contacto de aviso.

El equipo de hardware es en particular adecuado para detectar una manipulación y/o un ataque al equipo de hardware y, cuando se detecta la manipulación y/o el ataque, ejecutar en el marco de la función de emergencia medidas adecuadas para señalizar la manipulación y/o el ataque y mantener limitadas las repercusiones de la manipulación y/o del ataque. Las medidas adecuadas pueden entonces ser parte de las medidas de seguridad del perfil de protección de integridad elegido.

La ejecución de la función de emergencia puede dar lugar a que el equipo de hardware emita la señal de aviso. La señal de aviso puede ser una alarma. Además, puede ser la señal de aviso un aviso de peligro. La señal de aviso puede además enviarse desde el equipo de hardware a un equipo de vigilancia, para señalizar al mismo la manipulación detectada.

Además, puede desconectar y/o desactivar la función de emergencia el equipo de hardware, con lo que puede impedirse una manipulación. Puede además ejecutarse el programa de funcionamiento en emergencia en el equipo de hardware. El programa de funcionamiento en emergencia es por ejemplo un programa que sólo ejecuta las funciones necesarias del equipo de hardware y detiene funciones sensibles del equipo de hardware. De esta manera pueden mantenerse limitadas las repercusiones de la manipulación y/o del ataque y puede garantizarse la seguridad del equipo de hardware.

Además, pueden borrarse datos memorizados en el equipo de hardware, en particular datos relevantes para la seguridad. De esta manera puede impedirse que un usuario no autorizado que realiza la manipulación lea y/o copie los datos memorizados en el equipo de hardware.

Mediante la desactivación de interfaces del equipo de hardware puede además impedirse que el usuario no autorizado manipule a través de estas interfaces el equipo de hardware, en particular lea datos memorizados en el equipo de hardware.

Además, puede indicar ópticamente el equipo de hardware la manipulación mediante un contacto de aviso. En particular puede visualizarse en el contacto de aviso qué infracciones de la integridad se detectan.

Según otra forma de ejecución se introduce un producto de programa de computadora que origina en un equipo controlado por programa la ejecución del procedimiento descrito anteriormente y en lo que sigue.

Un producto de programa de computadora, como por ejemplo un medio de programa de computadora, puede proporcionarse o suministrarse por ejemplo como medio de memoria, como por ejemplo tarjeta de memoria, lápiz USB, CD-ROM, DVD o también en forma de un fichero que puede descargarse desde un servidor en una red. Esto puede realizarse por ejemplo en una red de comunicación inalámbrica mediante la transmisión de un fichero correspondiente con el producto de programa de computadora o el medio de programa de computadora.

Según otra forma de ejecución, el equipo de hardware es un sistema embebido.

Según otra forma de ejecución incluye el equipo de hardware además un equipo de elección para elegir el perfil de protección de integridad que se desee elegir, estando configurado el equipo de elección como una interfaz del equipo de hardware, como un conmutador y/o como un módulo codificador.

La interfaz del equipo de hardware puede ser por ejemplo un teclado, una interfaz de Internet y/o una pantalla (display), mediante los cuales pueden introducirse datos elegidos para elegir el perfil de protección de integridad. Los datos de elección pueden proporcionarse al equipo de hardware también por ejemplo mediante el Ethernet, IP, WLAN, ZigBee, IEEE 802.15.4 o Bluetooth.
El interruptor puede ser por ejemplo un interruptor DIP o un jumper. La elección del perfil de protección de integridad puede realizarse en función del jumper insertado y/o del interruptor DIP insertado.

Además, puede realizarse la elección del perfil de protección de integridad en función del módulo codificador insertado.

Según otra forma de ejecución incluye el equipo de hardware al menos una primera y una segunda unidad, sucediendo que

los perfiles de protección de integridad incluyen primeros y segundos perfiles de protección de integridad;
los primeros perfiles de protección de integridad están asociados a la primera unidad, definiendo cada primer perfil de protección de integridad primeras medidas de seguridad para proteger un hardware y un software de la primera unidad frente a manipulaciones,
estando asociados los segundos perfiles de protección de integridad a la segunda unidad, definiendo cada segundo perfil de protección de integridad primeras medidas de seguridad para proteger un hardware y un software de la segunda unidad frente a manipulaciones,
incluyendo el equipo de determinación un primer equipo de determinación para elegir un primer perfil de protección de integridad de los varios primeros perfiles de protección de integridad como un primer perfil de protección de integridad elegido y un segundo equipo de determinación para elegir un segundo perfil de protección de integridad de los varios segundos perfiles de protección de integridad como un segundo perfil de protección de integridad elegido y
estando equipado el equipo de seguridad para ejecutar las medidas de seguridad del primer perfil de protección de integridad elegido en la primera unidad y las medidas de seguridad del segundo perfil de protección de integridad elegido en la segunda unidad.

La primera y la segunda unidad pueden ser partes del equipo de hardware, a las que están asociados respectivos perfiles de protección de integridad propios. La integridad de la primera y segunda unidad pueden protegerse con independencia una de otra. Puede además quedar asegurado que cada una de las unidades está configurada correctamente, en particular en cuanto a funciones a ejecutar por la unidad. De esta manera puede aumentarse la seguridad de las distintas unidades, así como también la seguridad del equipo de hardware completo.

En determinadas formas de ejecución incluye el equipo de hardware otras unidades, por ejemplo una tercera y cuarta unidad, que incluyen otros perfiles de protección de integridad que pueden elegirse, que son adecuados para proteger las otras unidades.

Las formas de ejecución y características descritas para el procedimiento propuesto para operar el equipo de hardware son válidas correspondientemente para el equipo de hardware propuesto.

Según otra forma de ejecución, se propone un procedimiento para fabricar un equipo de hardware que incluye las etapas de procedimiento correspondientes al procedimiento que se ha descrito y se describe en lo que sigue.

En particular puede realizarse la elección del perfil de protección de integridad ya durante la fabricación del equipo de hardware. El perfil de protección de integridad puede fijarse por ejemplo durante la fabricación del equipo de hardware tal que sea invariable. En este caso pueden borrarse todos los perfiles de protección de integridad no elegidos.

Otras posibles implementaciones de la invención incluyen también combinaciones no citadas explícitamente de características o formas de ejecución antes descritas o que se describen a continuación relativas a los ejemplos de ejecución. Al respecto añadirá el especialista también aspectos individuales como mejoras o complementos al equipo de hardware, al procedimiento para operar el equipo de hardware y al procedimiento para fabricar el equipo de hardware.

Otras ventajosas variantes de ejecución y aspectos ventajosos de la invención son objeto de las reivindicaciones secundarias, así como de los ejemplos de ejecución descritos a continuación. En lo que sigue se describirán más en detalle formas de ejecución preferidas, con referencia a las figuras adjuntas.

La figura 1 muestra un equipo de hardware según una primera forma de ejecución;
la figura 2 muestra un procedimiento para operar un equipo de hardware según una primera forma de ejecución;
la figura 3 muestra un procedimiento para operar un equipo de hardware según una segunda forma de ejecución y

la figura 4 muestra un equipo de hardware según una segunda forma de ejecución.

En las figuras se han dotado los mismos elementos o elementos que tienen la misma función de las mismas referencias, siempre que no se haya indicado otra cosa.

La figura 1 muestra un equipo de hardware 1 según una primera forma de ejecución. El equipo de hardware 1 incluye un equipo de memoria 2, un equipo de determinación 3, un equipo de seguridad 4 y una interfaz 6, que están unidos entre sí mediante un bus interno 5.

El equipo de hardware 1 está concebido tal que el mismo puede ejecutar varias funciones distintas. Las funciones incluyen aquí un control de aparatos de campo en una instalación industrial y una memorización de datos relevantes de aparatos de campo.

En el equipo de memoria 2, que está realizado como una memoria RAM no volátil, están memorizados varios perfiles de protección de integridad P1-P4. Los perfiles de protección de integridad P1-P4 definen en cada caso distintas medidas de seguridad para proteger un hardware y un software del equipo de hardware.

Los perfiles de protección de integridad P1 y P2 son especialmente adecuados para proteger el equipo de hardware 1 cuando éste se utiliza para controlar los aparatos de campo en la instalación industrial. El perfil de protección de integridad P1 es al respecto más seguro que el perfil de protección de integridad P2, pero más complejo de ejecutar en cuanto a técnica de cálculo.

Los perfiles de protección de integridad P3 y P4 son especialmente adecuados para proteger el equipo de hardware 1, cuando éste se utiliza para memorizar datos relevantes de los aparatos de campo. El perfil de protección de integridad P3 es entonces más seguro que el perfil de protección de integridad P4, pero más complejo de ejecutar en cuanto a técnica de cálculo.

El equipo de hardware 1 es adecuado según un procedimiento representado en la figura 2 para operar un equipo de hardware 1 según una primera forma de ejecución. El procedimiento se describirá a continuación con referencia a las figuras 1 y 2.

En una etapa de preparación S0 se aporta el equipo de hardware 1 representado en la figura 1. En una etapa S1 se memorizan los varios perfiles de protección de identidad P1-P4 en el equipo de memoria 2. La memorización de los perfiles de protección de integridad P1-P4 se realiza durante la fabricación del equipo de hardware 1.

En una etapa S2 se elige un perfil de protección de integridad de entre los varios perfiles de protección de integridad P1-P4 como un perfil de protección de integridad elegido. La elección del perfil de protección de integridad a elegir se realiza mediante un usuario, no representado, del equipo de hardware 1 a través de la interfaz 6. La interfaz 6 es aquí un touchscreen, que muestra los perfiles de protección de integridad P1-P4 disponibles para la elección. El usuario elige el perfil de protección de integridad a elegir a través del touchscreen 6. La elección del perfil de protección de integridad a elegir se realiza teniendo en cuenta la función que ha de ejecutar el equipo de hardware 1. Si el equipo de hardware 1 ha de utilizarse para controlar los aparatos de campo en la instalación industrial, se eligen con preferencia los perfiles de protección de integridad P1 o P2. Si el equipo de hardware 1 ha de utilizarse para memorizar los datos relevantes de los aparatos de campo, se eligen con preferencia los perfiles de protección de integridad P3 o P4. En el equipo de hardware 1 repercute la elección del perfil de protección de integridad en que el equipo de determinación 3 determina el perfil de protección de integridad a elegir a partir de los perfiles de protección de integridad P1-P4 y proporciona el mismo al equipo de seguridad 4.

En una etapa S3 se ejecutan las medidas de seguridad del perfil de protección de integridad elegido mediante el equipo de seguridad 4. La ejecución de las medidas de seguridad incluye la ejecución de un arranque seguro del equipo de hardware 1.

El perfil de protección de integridad a ejecutar puede elegirse de entre los perfiles de protección de integridad P1-P4, tal que ello sea óptimo para la función a ejecutar mediante el equipo de hardware 1. De esta manera se protege la integridad del equipo de hardware 1 y aumenta la seguridad del equipo de hardware.

Las etapas S0, S1, S2 y S3 pueden también ejecutarse en el marco de un procedimiento para fabricar el equipo de hardware 1, tal que el perfil de protección de integridad a elegir se elija ya durante la fabricación del equipo de hardware 1.

El equipo de hardware 1 es además adecuado para operar según un procedimiento representado en la figura 3 para operar un equipo de hardware 1 según una segunda forma de ejecución. El procedimiento según la segunda forma de ejecución es una ampliación del procedimiento según la primera forma de ejecución y se describirá a continuación con referencia a las figuras 1 y 3.

Primeramente, se ejecutan las etapas S0 y S1 ya descritas. En una etapa S11 se memorizan datos de verificación en el equipo de hardware 1. Los mismos se memorizan durante la fabricación del equipo de hardware 1 en el equipo de memoria 2. Los datos de verificación están configurados como una secuencia de números.

En una etapa S 12 recibe el equipo de hardware 1 datos de autentificación del usuario que desearía elegir un perfil de protección de integridad para el equipo de hardware 1, a través de la interfaz 6. Los datos de autentificación son una secuencia de números que introduce el usuario como palabra de paso en el equipo de hardware 1, para poder elegir un perfil de protección de integridad P1-P4.

En una etapa S 13 determina el equipo de hardware 1 si los datos de autentificación recibidos coinciden con los datos de verificación memorizados. Si los datos de autentificación recibidos coinciden con los datos de verificación memorizados, permite el equipo de hardware 1 en una etapa S 14 la elección de un perfil de protección de integridad P1-P4. Es decir, el equipo de hardware 1 autoriza al usuario a elegir un perfil de protección de integridad P1-P4.

Evidentemente si los datos de autentificación recibidos no coinciden con los datos de verificación memorizados, impide el equipo de hardware 1 en una etapa S 15 la elección de un perfil de protección de integridad P1-P4. El usuario no puede en este caso modificar el perfil de protección de integridad P1-P4 hasta que introduzca los datos de autentificación correctos. En la etapa S 15 se emite adicionalmente a través de la interfaz 6 un aviso de alarma al usuario.

Si se admite la elección del perfil de protección de integridad P1-P4 en la etapa S 14, se ejecutan las etapas S2 y S3 ya antes descritas.

La etapa S3 incluye en la forma de ejecución representada en la figura 3 las etapas S4 y S5. En la etapa S4 determina el equipo de hardware 1, con ayuda de las medidas de seguridad del perfil de protección de integridad elegido, si tiene lugar una manipulación en el equipo de hardware 1. Para ello comprueba el equipo de hardware 1 con ayuda de las medidas de seguridad los procesos que corren en el equipo de hardware 1 y la integridad de los datos memorizados en el equipo de hardware 1. De esta manera se comprueba la integridad del software del equipo de hardware 1.

Además, vigila el equipo de hardware 1 con ayuda de las medidas de seguridad sensores tamper no representados del equipo de hardware 1. Los sensores tamper incluyen una lámina de protección antiperforación. De esta manera pueden detectarse también infracciones físicas de la integridad.

La etapa S4 se ejecuta periódicamente mientras no se detecte ninguna manipulación. Si se determina en la etapa S4 una manipulación, se ejecuta en la etapa S5 una función de emergencia definida por las medidas de seguridad del perfil de protección de integridad elegido. Al ejecutar la función de emergencia se borran todos los datos memorizados en el equipo de hardware 1, con lo que se garantiza la seguridad del equipo de hardware 1.

La figura 4 muestra un equipo de hardware 10 según una segunda forma de ejecución.

El equipo de hardware 10 es un sistema Linux embebido. El equipo de hardware 10 incluye una unidad de procesador 15, una memoria de configuración 25 para memorizar datos elegidos para un perfil de protección de integridad, una interfaz de red 26 para el intercambio de datos con aparatos de campo a través de una conexión Ethernet 28, una interfaz de entrada/salida 27 para acceder a módulos periféricos, como la interfaz de red 26 y los sensores tamper 30 y una fuente de alimentación 31 para alimentar eléctricamente el equipo de hardware 10.

La unidad de procesador 15 es adecuada para ejecutar aplicaciones de contenedor 17, que se implementan mediante un sistema de tiempo de ejecución (” Runtime Engine, RTE”), así como para ejecutar aplicaciones de usuario 19 regulares.

El procesador 15 incluye un kernel (núcleo) Lynux 16, con un monitor de integridad kernel 11 como una primera unidad. El monitor de integridad kernel 11 incluye un primer equipo de memoria 12, en el que están memorizados perfiles de protección de integridad kernel PK1 - PK3 como primeros perfiles de protección de integridad. Los perfiles de protección de integridad kernel PK1 - PK3 incluyen medidas de seguridad para proteger el software y el hardware del monitor de integridad kernel 11. Además, incluye el monitor de integridad kernel 11 un primer equipo de determinación 13.

La unidad de procesador 15 incluye además un monitor de integridad del usuario 21, como una segunda unidad con un segundo equipo de memoria 22, en el que están memorizados perfiles de protección de integridad del usuario PU1 - PU3 como segundos perfiles de protección de integridad y con un segundo equipo de determinación 23. Los perfiles de protección de integridad del usuario PU1 - PU3 incluyen medidas de seguridad para proteger el software y el hardware del monitor de integridad del usuario 21.

El equipo de hardware 10 es adecuado para funcionar según el procedimiento de las figuras 2 y 3. Las etapas del procedimiento descritas con referencia a las figuras 1 a 3 se ejecutan entonces separadamente para el monitor de integridad kernel 11 y el monitor de integridad del usuario 21. Al respecto se realiza en particular una elección del perfil de protección de integridad kernel PK1-PK3 independientemente de la elección del perfil de integridad del usuario PU1 - PU3. También están memorizados para permitir la elección del perfil de protección de integridad kernel PK1-PK3 y del perfil de integridad del usuario PU1 - PU3 en el monitor de integridad kernel 11 y en el monitor de integridad del usuario 21, distintos datos de verificación, que deben coincidir con distintos datos de autentificación recibidos.

A continuación, se describe el funcionamiento del equipo de hardware 10 con referencia a las figuras 2 y 4.

En la etapa S0 se aporta el equipo de hardware 10. En la etapa S1 se memorizan los perfiles de protección de integridad kernel PK1-PK3 en el primer equipo de memoria 12 y los perfiles de protección de integridad del usuario PU1 - PU3 en el segundo equipo de memoria 22.

En la etapa S2 se elige en cada caso un perfil de protección de integridad de entre los perfiles de protección de integridad kernel PK1-PK3 y a partir de los perfiles de protección de integridad del usuario PU1 - PU3. Para realizar la elección, reciben el monitor de integridad kernel 11 y el monitor de integridad del usuario 21 en cada caso datos para la elección de la memoria de configuración 25, que es una memoria EEPROM. El primer y el segundo equipo de determinación 13, 23 determinan, teniendo en cuenta los datos de elección recibidos, el perfil de protección de integridad kernel elegido y el perfil de protección de integridad del usuario elegido.

En la etapa S3 se ejecutan las medidas de seguridad prescritas mediante el perfil de protección de integridad kernel elegido, para proteger la integridad de recursos kernel por parte del monitor de integridad kernel 11 y las medidas de seguridad prescritas por el perfil de protección de integridad del usuario elegido, para proteger la integridad de recursos de usuario mediante el monitor de integridad del usuario 21.

En el marco de la protección de integridad mediante el monitor de integridad kernel 11 y mediante el monitor de integridad del usuario 21, se determina con ayuda de las correspondientes medidas si determinados procesos, por ejemplo, unas determinadas aplicaciones de contenedor 17, tienen autorización para correr o no.

Además, puede detectarse si se realiza una manipulación sobre el equipo de hardware 10. Para ello se comprueban los procesos que corren en el equipo de hardware 10 y se vigilan los sensores tamper 30. Los sensores tamper 30 incluyen una lámina de protección antiperforación y un sensor de movimiento.

Si se detecta una manipulación, se desactiva la interfaz de red 26 mediante un cable de interfaz 33 y se pone a cero la unidad de procesador 15 mediante un cable de reset 32, borrándose los datos memorizados en la unidad de procesador 15. Además, cuando se detecta la manipulación, se emite a través de la interfaz de entrada/salida 27 una señal de conmutación a través de un contacto de aviso 29.

Aún cuando la presente invención se ha descrito en base a ejemplos de ejecución, la misma puede modificarse de múltiples formas. El equipo de hardware puede ser un equipo cualquiera, como por ejemplo un aparato de campo. La cantidad de perfiles de protección de integridad que están memorizados en el equipo de hardware puede elegirse a discreción. Las medidas de seguridad que están definidas mediante los perfiles de protección de integridad pueden ampliarse a discreción. Además, puede presentar el equipo de hardware cualquier número de unidades, cada una de las cuales se protege con un perfil de protección de integridad específico de la unidad, el cual ha sido elegido de entre una pluralidad de perfiles de protección de integridad específicos de la unidad.

REIVINDICACIONES

1. Procedimiento para operar un equipo de hardware (1, 10) que es adecuado para ejecutar varias funciones diferentes y que incluye:
Memorización (S1) en el equipo de hardware (1, 10) de varios perfiles de protección de integridad (P1 – P4) para el equipo de hardware (1, 10), pudiendo asignarse cada perfil de protección de integridad (P1 – P4) a una de las varias funciones distintas y definiendo cada perfil de protección de integridad (P1 – P4) medidas de seguridad para proteger un hardware del equipo de hardware (1, 10) frente a manipulaciones;
elección (S2) de un perfil de protección de integridad de entre los varios perfiles de protección de integridad (P1 – P4) como un perfil de protección de integridad elegido a través de una interfaz (6), teniendo en cuenta una función a ejecutar mediante el equipo de hardware (1, 10) de entre las varias funciones diferentes y
ejecución (S3) de las medidas de seguridad del perfil de protección de integridad elegido;
caracterizado porque la ejecución de las medidas de seguridad incluye al menos:
vigilancia de sensores tamper (30) del equipo de hardware (1, 10), que captan características físicas del equipo de hardware (1, 10).

2. Procedimiento según la reivindicación 1,
en el que cada perfil de protección de integridad (P1 – P4) define además medidas de seguridad para proteger un software del equipo de hardware (1, 10) frente a manipulaciones.

3. Procedimiento según la reivindicación 2,
en el que la realización de las medidas de seguridad incluye al menos:
ejecución de un arranque seguro del equipo de hardware (1, 10);
comprobación de que los datos que están memorizados en el equipo de hardware (1, 10) son correctos;
comprobación de procesos que corren en el equipo de hardware (1, 10);
ejecución de un "Mandatory Access Control" en el equipo de hardware (1, 10);
virtualización de recursos del sistema operativo y/o recursos de hardware y/o
averiguación (S4) de si se realiza una manipulación en el equipo de hardware (1, 10).

4. Procedimiento según una de las reivindicaciones 1 a 3,
en el que la ejecución de las medidas de seguridad incluye una vigilancia lógica y una vigilancia física del equipo de hardware (1, 10).

5. Procedimiento según una de las reivindicaciones 1 a 4,
que incluye, además:
Memorización (S11) de datos de verificación en el equipo de hardware (1, 10);
recepción (S12) de datos de autentificación por el equipo de hardware (1, 10) de un usuario que quiere elegir un perfil de protección de integridad de entre los varios perfiles de protección de integridad (P1 – P4);
determinación (S13) de si los datos de autentificación coinciden con los datos de verificación y
si los datos de autentificación coinciden con los datos de verificación, autorización (S14) de la elección del perfil de protección de identidad.

6. Procedimiento según una de las reivindicaciones 1 a 5,
que incluye, además:
si se averigua que tiene lugar una manipulación del equipo de hardware (1, 10), ejecución (S5) de una función de emergencia mediante el equipo de hardware (1, 10), incluyendo la función de emergencia:
Emisión de una señal de aviso;
desconexión del equipo de hardware (1, 10);
ejecución de un programa de funcionamiento en emergencia;
borrado de datos memorizados en el equipo de hardware (1, 10);
desactivación del equipo de hardware (1, 10);
desactivación de interfaces (6, 26, 27) del equipo de hardware (1, 10) y/o
señalización de la manipulación del equipo de hardware (1, 10) mediante un contacto de aviso (29).

7. Procedimiento según una de las reivindicaciones 1 a 6,
en el que la elección (S2) del perfil de protección de integridad se realiza mientras se fabrica el equipo de hardware (1, 10).

8. Equipo de hardware (1, 10) que es adecuado para ejecutar varias funciones diferentes,
que incluye:
Un equipo de memoria (2) para memorizar varios perfiles de protección de integridad (P1 – P4) para el equipo de hardware (1, 10), pudiendo asignarse cada perfil de protección de integridad (P1 – P4) a una de las varias funciones diferentes y definiendo cada perfil de protección de integridad

(P1 – P4) medidas de seguridad para proteger un hardware del equipo de hardware (1, 10) frente a manipulaciones;
un equipo de determinación (3), para determinar un perfil de protección de integridad elegido, que ha sido elegido de entre los varios perfiles de protección de integridad (P1 – P4) teniendo en cuenta una función a ejecutar mediante el equipo de hardware (1, 10) de entre las varias funciones diferentes y
un equipo de seguridad (4) para ejecutar las medidas de seguridad del perfil de protección de integridad elegido;
caracterizado porque la realización de las medidas de seguridad incluye al menos una vigilancia de sensores tamper (30) del equipo de hardware (1, 10), que captan características físicas del equipo de hardware (1, 10).

9. Equipo de hardware según la reivindicación 8,
que es adecuado para ejecutar el procedimiento según una de las reivindicaciones 1 a 6.

10. Equipo de hardware según la reivindicación 8 ó 9,
que es un sistema embebido.

11. Equipo de hardware según una de las reivindicaciones 8 a 10,
que incluye además un equipo de elección para elegir el perfil de protección de integridad que se desee elegir, estando configurado el equipo de elección como una interfaz (6, 26) del equipo de hardware (1, 10), como un conmutador y/o como un módulo codificador.

12. Equipo de hardware según una de las reivindicaciones 8 a 9 con al menos una primera y una segunda unidad (11, 21),
en el que
los perfiles de protección de integridad (P1 – P4) incluyen primeros y segundos perfiles de protección de integridad (PK1 – PK3, PU1, PU3);
los primeros perfiles de protección de integridad (PK1 – PK3) están asociados a la primera unidad (11), definiendo cada primer perfil de protección de integridad (PK1 – PK3) primeras medidas de seguridad para proteger un hardware de la primera unidad (11) frente a manipulaciones;
estando asociados los segundos perfiles de protección de integridad (PU1, PU3) a la segunda unidad (21), definiendo cada segundo perfil de protección de integridad (PU1, PU3) segundas medidas de seguridad para proteger un hardware de la segunda unidad (21) frente a manipulaciones;
incluyendo el equipo de determinación (3) un primer equipo de determinación (13) para elegir un primer perfil de protección de integridad de los varios primeros perfiles de protección de integridad (PK1 – PK3) como un primer perfil de protección de integridad elegido y un segundo equipo de determinación (23) para elegir un segundo perfil de protección de integridad de los varios segundos perfiles de protección de integridad (PU1, PU3) como un segundo perfil de protección de integridad elegido y
estando preparado el equipo de seguridad (4) para ejecutar las medidas de seguridad del primer perfil de protección de integridad elegido en la primera unidad (11) y las medidas de seguridad del segundo perfil de protección de integridad elegido en la segunda unidad (21).

13. Equipo de hardware según una de las reivindicaciones 8 a 12,
en el que cada perfil de protección de integridad (P1 – P4), cada primer perfil de protección de integridad (PK1 – PK3) y/o cada segundo perfil de protección de integridad (PU1, PU3) define además medidas de seguridad para proteger un software del equipo de hardware (1, 10) frente a manipulaciones.

14. Producto de programa de computadora que origina en un equipo de hardware según una de las reivindicaciones 8 a 13 la ejecución del procedimiento según una de las reivindicaciones 1 a 7.

FIG 1

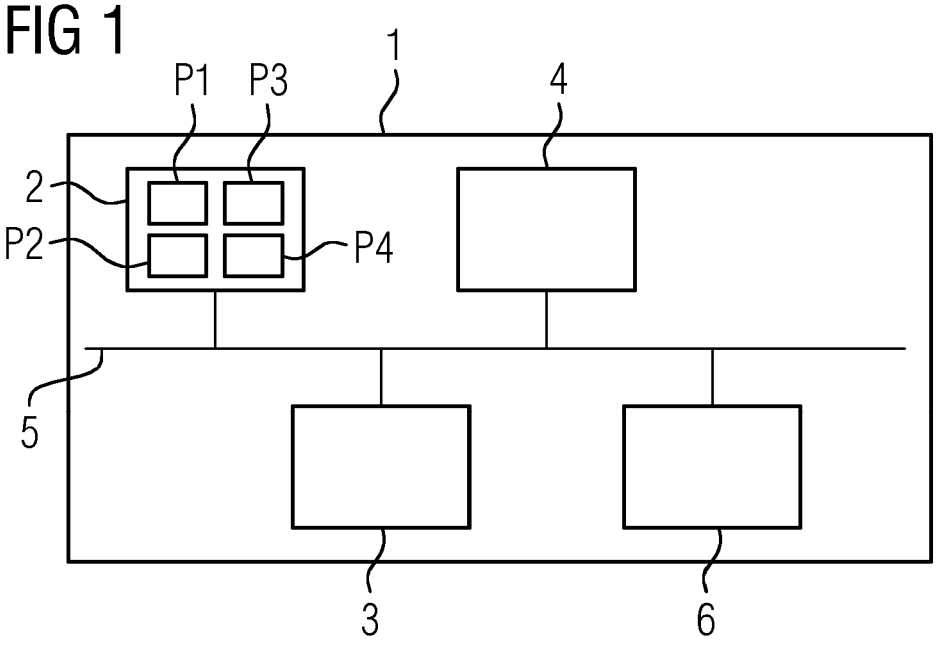


FIG 2

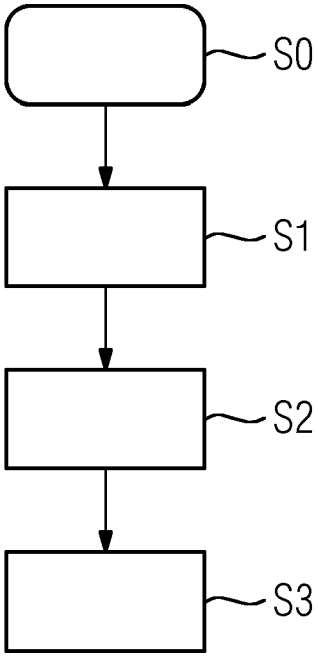


FIG 3

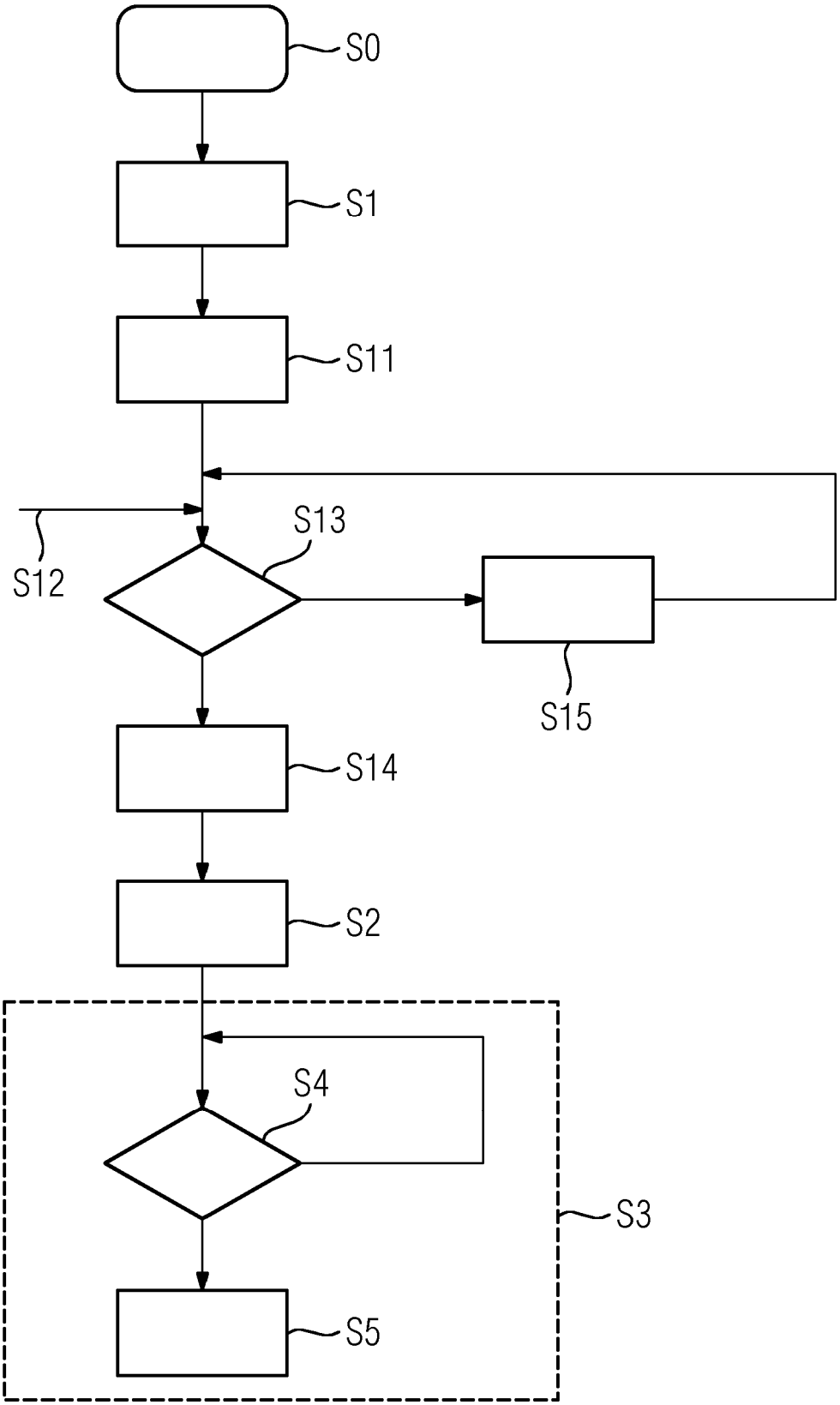
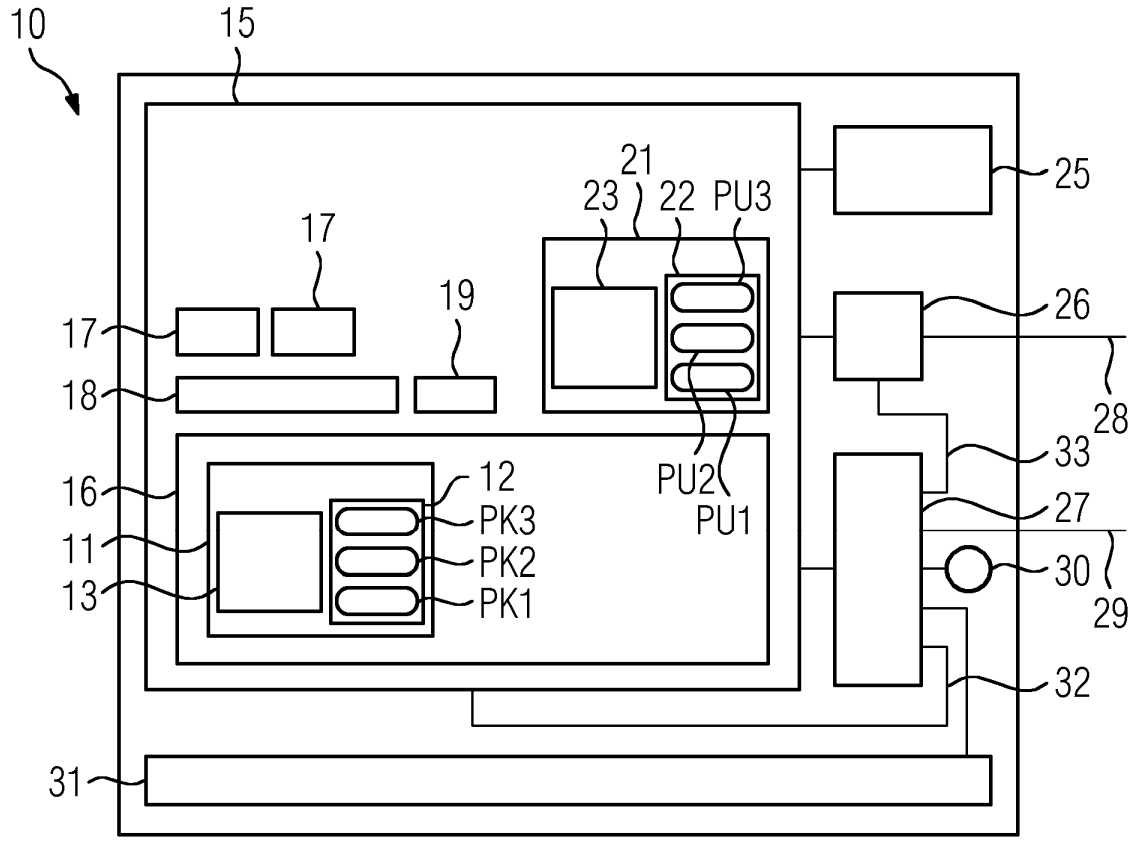


FIG 4


10
15
21
23
22
PU3
25
17
19
17
26
18
28
33
16
12
PU2
27
PK3
11
PU1
PK2
30
13
PK1
29
32
31