(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 992 251**

(51) Int. CI.:

G06F 21/57 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **05.05.2021 E 21172207 (9)**

(97) Fecha y número de publicación de la concesión europea: **21.08.2024 EP 3907638**

(54) Título: **Controlador de arranque seguro para un sistema de a bordo, sistema de a bordo y procedimiento de arranque seguro asociados**

(30) Prioridad:

05.05.2020 FR 2004434

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.12.2024

(73) Titular/es:

THALES (100.0%)
Tour Carpe Diem, Place des Corolles - Esplanade Nord
92400 Courbevoie, FR

(72) Inventor/es:

MONNIER, STÉPHANE

(74) Agente/Representante:

PONTI & PARTNERS, S.L.P.

DESCRIPCIÓN

Controlador de arranque seguro para un sistema de a bordo, sistema de a bordo y procedimiento de arranque seguro asociados

[0001] La presente invención se refiere a un controlador de arranque seguro.

[0002] La presente invención se refiere también a un sistema de a bordo y a un procedimiento de arranque seguro, asociados a este controlador de arranque seguro.

[0003] El sistema de a bordo según la invención es especialmente un sistema de aviónica.

[0004] El documento US 2016/300064 A1 describe un procesador seguro para la inicialización de un SOC (del inglés «System On a Chip»).

[0005] El documento US 2005/091522 A1 describe un dispositivo de seguridad informática que comprende un procesador que es independiente de una CPU anfitriona para controlar el acceso entre la CPU anfitriona y un dispositivo de almacenamiento.

[0006] En el campo de los sistemas de a bordo y especialmente en el campo de los sistemas de aviónica, la ciberseguridad se convierte en uno de los elementos clave de la arquitectura. Para responder a numerosos escenarios de amenazas, los sistemas de a bordo actuales deben poder garantizar la autenticidad y la integridad del conjunto de sus componentes.

[0007] Los mecanismos de verificación de las signaturas de estos componentes en el arranque del sistema permiten responder a esta problemática.

[0008] Sin embargo, para poder integrar mecanismos de arranque seguros de los sistemas de a bordo es necesario en general modificar las arquitecturas existentes. De hecho, para poder asegurar un arranque seguro es necesario intervenir desde las primeras etapas del arranque del sistema de a bordo, imponiendo así una reactivación de los componentes de software de bajo nivel para poder lanzar los mecanismos de verificaciones de signaturas.

[0009] Esta reactivación es tanto más molesta cuando las componentes de bajo nivel presentan componentes COTS («componentes comerciales de venta al público»).

[0010] Según los procedimientos del estado de la técnica, para asegurar un arranque seguro existen mecanismos de tipo certificados o de cadena de confianza.

[0011] En particular, según este segundo caso, en el arranque de un sistema de a bordo, una componente de hardware verifica y lanza un software de arranque que verifica y lanza un sistema operativo que, a su vez, verifica y lanza aplicaciones alojadas por este sistema operativo.

[0012] Sin embargo, en los dos casos, los impactos en la arquitectura existente del sistema de a bordo no son insignificantes e imponen en general una reactivación de al menos varias componentes de este sistema de a bordo.

[0013] En particular, los mecanismos existentes no permiten integrar un mecanismo de arranque seguro en una componente de un sistema de a bordo sin modificar al menos algunas otras componentes de este sistema.

[0014] Ahora bien, dicha modificación de las otras componentes del sistema puede implicar la necesidad de su recertificación, lo que representa un proceso muy complejo y costoso. Así sucede especialmente cuando estas componentes presentan un nivel de criticidad DAL (del inglés «*Development Assurance Level*») elevado, como por ejemplo el nivel DAL A.

[0015] La presente invención tiene como objeto proponer un controlador de arranque seguro que permita implementar un mecanismo de arranque seguro de una componente cualquiera de un sistema de a bordo, sin modificar las otras componentes de este sistema y, en su caso, sin necesidad de recertificación de estas otras componentes.

[0016] Para este fin, la invención tiene por objeto un controlador según la reivindicación 1.

[0017] Según otras características de la invención, el controlador es según cualquiera de las reivindicaciones 2 a 6.

[0018] La invención tiene también por objeto un sistema de a bordo según la reivindicación 7.

[0019] La invención tiene también por objeto un procedimiento de arranque según la reivindicación 8.

[0020] Estas características y ventajas de la invención resultarán evidentes a partir de la lectura de la descripción que se ofrece a continuación, proporcionada únicamente a modo de ejemplo no limitativo, hecha en referencia a la figura única, denominada también figura 1 [Fig. 1], donde se ha ilustrado esquemáticamente un sistema de a bordo según la invención.

[0021] En particular, en esta figura, el sistema de a bordo se designa por la referencia 10 y presenta especialmente un sistema de aviónica.

[0022] En un ejemplo particular de la invención, este sistema de aviónica presenta un conmutador de una red de aviónica. Según otros ejemplos de la invención, este sistema de aviónica presenta cualquier otro sistema de una aeronave.

[0023] Ventajosamente, el sistema de a bordo 10 es un sistema crítico de un nivel de criticidad DAL (del inglés «*Development Assurance Level*») determinado.

[0024] Como puede verse en la figura, el sistema de a bordo 10 comprende un módulo operativo 12, un módulo de verificación 14, un módulo de configuración 16 y un controlador de arranque 18.

[0025] El sistema de a bordo 10 comprende también recursos de hardware que permiten implementar el funcionamiento de sus diferentes componentes 12 a 18.

[0026] Estos recursos de hardware son conocidos de por sí y comprenden especialmente un procesador 20, un espacio de almacenamiento 22 y una memoria de acceso aleatorio 24.

[0027] En particular, el espacio de almacenamiento 22 presenta por ejemplo una memoria de tipo FLASH que permite almacenar en diferentes direcciones diferentes funciones ejecutables por el procesador 20. Estas funciones presentan así elementos de software.

[0028] Especialmente, el espacio de almacenamiento 22 define una zona de arranque 32 que define una función que será ejecutada por el procesador 20 en el arranque del sistema 10. Dicha función es, por tanto, ejecutable en el arranque según la terminología utilizada a continuación.

[0029] En particular, esta zona de arranque 32 presenta una dirección de memoria predefinida a la que se refiere el procesador 20 en el arranque del sistema 10.

[0030] La zona de arranque 32 contiene así una función ejecutable en el arranque por el procesador 20 o al menos una referencia a una dirección de memoria que almacena esta función, cuando se presenta en la forma de un software. Cuando la función ejecutable en el arranque se implementa al menos parcialmente en la forma de una componente de hardware, la zona de arranque 32 contiene entonces una referencia hacia esta componente.

[0031] La memoria de acceso aleatorio 24 es también conocida de por sí y presenta en particular una memoria intermedia de intercambio entre las diferentes componentes del sistema de a bordo 10.

[0032] Como también es conocido de por sí, la memoria de acceso aleatorio 24 permite almacenar al menos temporalmente datos de intercambio cuando el sistema de a bordo 10 recibe alimentación.

[0033] En algunos ejemplos de realización, la memoria de acceso aleatorio 24 permite también almacenar datos de intercambio durante las interrupciones, denominadas cortas, de corriente en el curso de las cuales recibe alimentación, por ejemplo, de una componente interior del sistema de a bordo 10 que presenta una reserva de energía. Dicha componente permite, por ejemplo, hacer que el sistema de a bordo 10 sea insensible a este tipo de perturbaciones.

[0034] El módulo operativo 12 integra una función operativa del sistema de a bordo 10.

[0035] Esta función operativa es implementada por el sistema de a bordo 10 y especialmente por el procesador 20. En el ejemplo descrito, esta función operativa se presenta, por ejemplo, en la forma de un software que se almacena así, por ejemplo, en el espacio de almacenamiento 22.

[0036] En el ejemplo de realización donde el sistema de a bordo 10 presenta un conmutador de una red de aviónica, la función operativa asegurada por el módulo operativo 12 presenta por ejemplo las transmisiones de los datos de mantenimiento.

[0037] El módulo de configuración 16 permite definir parámetros de funcionamiento del sistema 10.

[0038] Así, por ejemplo, este módulo de configuración 16 define una pluralidad de parámetros de funcionamiento de al menos algunas de las componentes del sistema 10.

[0039] En el ejemplo de realización donde el sistema de a bordo 10 presenta un conmutador, el módulo de configuración 16 presenta especialmente una tabla de configuración que define el encaminamiento de los datos entre diferentes puertos de entrada y de salida de este conmutador.

[0040] Ventajosamente, según la invención, este módulo de configuración 16 se presenta en la forma de una memoria no volátil tal como una memoria de tipo FLASH.

[0041] El módulo de verificación 14 integra una función de verificación de diferentes componentes del sistema de a bordo 10.

[0042] En particular, esta función de verificación permite verificar la autenticidad y la integridad de cada una de estas componentes, según por ejemplo procedimientos conocidos de por sí.

[0043] Especialmente, en el ejemplo de realización descrito, la función de verificación permite verificar la autenticidad y la integridad del módulo de configuración 16, y especialmente de la tabla de configuración en el caso del conmutador, así como la autenticidad y la integridad del módulo operativo 12 analizando por ejemplo las signaturas de este con algoritmos criptográficos de tipo SHA (del inglés «*Secure Hash Algorithm*») o RSA (así denominado por sus autores Ronald Rivast, Adi Shamir y Leonard Adleman) u otros.

[0044] Ventajosamente, según la invención, el módulo de verificación 14 permite implementar su función de verificación con respecto a cada una de las componentes del sistema de a bordo 10 en el arranque de este sistema, como se explicará en detalle más adelante.

[0045] El módulo de verificación 14 se presenta, por ejemplo, en la forma de una componente de hardware por ejemplo de una componente FPGA («*Field Programmable Array*» en inglés) o bien en la forma de un software.

[0046] En este último caso, la función de verificación integrada en el módulo de verificación 14 se almacena por ejemplo en el espacio de almacenamiento 22.

[0047] El controlador de arranque seguro 18 según la invención permite implementar un arranque seguro del sistema 10 como se explicará en detalle más adelante en referencia al procedimiento de arranque según la invención.

[0048] En particular, para ello, el controlador 18 permite, durante cada arranque del sistema de a bordo 10, determinar el tipo de arranque del sistema. Especialmente, el controlador 18 permite determinar si se trata de un arranque en frío del sistema 10 o de un arranque en caliente.

[0049] En particular, en todo lo que sigue, por arranque en frío o primer arranque se entiende un arranque después de una pérdida al menos parcial de los datos de intercambio de la memoria de acceso aleatorio 24. Este arranque se reproduce especialmente después de un corte prolongado de corriente o después de una parada del sistema 10. Un arranque en frío se lleva a cabo también durante cualquier primer arranque del sistema, es decir, durante el primer arranque del sistema después de su ensamblaje y/o instalación.

[0050] Como oposición al arranque en frío, por arranque en caliente se entiende un arranque del sistema 10 después de un corte corto de corriente. En general, durante dicho arranque en caliente del sistema, los datos de la memoria de acceso aleatorio 24 no se pierden.

[0051] Para determinar el tipo de arranque, el controlador 18 es capaz, por ejemplo, de consultar el estado de un registro de arranque modificable por un controlador de alimentación. En particular, en función por ejemplo de la duración del corte de corriente, este controlador de alimentación es capaz de modificar el estado de este registro para un valor determinado.

[0052] El controlador 18 permite también modificar la zona de arranque 32 según el tipo de arranque determinado, como se explicará más adelante.

[0053] El controlador 18 se presenta, por ejemplo, en la forma de una componente de hardware, especialmente en la forma de una componente FPGA.

[0054] Ventajosamente según la invención, su nivel de criticidad DAL es equivalente al del módulo de verificación 14 y es superior en criticidad al módulo operativo 12. Por ejemplo, el controlador 18 y el módulo de verificación 14 pueden presentar el nivel de criticidad DAL A mientras que el módulo operativo 12 puede presentar un nivel de criticidad más bajo (DAL B o DAL C o incluso DAL D o DAL E) o igual al nivel de criticidad DAL A.

[0055] A continuación, se explicará el procedimiento de arranque seguro del sistema de a bordo 10 según la invención.

[0056] Inicialmente, se considera que el sistema 10 está en el punto de ser arrancado.

[0057] Así, en primer lugar, el procedimiento comprende una etapa inicial durante la cual el controlador 18 determina el tipo de arranque.

[0058] Cuando el controlador 18 determina que se trata de un arranque en frío, durante una etapa siguiente, hace ejecutable en el arranque la función de verificación para realizar una verificación de la autenticidad y de la integridad de la función operativa, así como del módulo de configuración 16.

[0059] En particular, para hacer ejecutable la función de verificación, el controlador 18 coloca la función de verificación o una referencia de la misma en la zona de arranque 32.

[0060] Además, para hacer visible la función operativa a la función de verificación, el controlador 18 asocia a esta función operativa una dirección de memoria en el espacio de almacenamiento 22.

[0061] A continuación, el controlador 18 recupera un resultado de verificación efectuada por la función de verificación.

[0062] Cuando durante la etapa inicial el controlador 18 determina que se trata de un arranque en caliente, durante una etapa siguiente, este controlador 18 verifica en primer lugar el resultado de la verificación suministrado por la función de verificación durante el arranque en frío.

[0063] Cuando este resultado es positivo, es decir, cuando la verificación se consigue, durante una etapa siguiente, el controlador 18 hace ejecutable en el arranque la función operativa integrada en el módulo operativo 12.

[0064] Para ello, como en el caso anterior, el controlador 18 coloca esta función operativa o una referencia a la misma en la zona de arranque 22 sustituyendo así la función de verificación o una referencia a la misma en esta zona.

[0065] En este caso, el arranque del sistema de a bordo 10 se realiza entonces sin la ejecución de la función de verificación.

[0066] Se entiende así que la presente invención presenta un cierto número de ventajas.

[0067] En primer lugar, está claro que el controlador según la invención permite gestionar la ejecución en el arranque de diferentes componentes del sistema según el tipo del arranque.

[0068] Así, durante un arranque en frío, el controlador hace ejecutable la función de verificación que verifica entonces las otras componentes del sistema de a bordo y especialmente la función operativa y el módulo de configuración.

[0069] Cuando se trata de uno de los arranques en caliente siguientes, el controlador según la invención hace ejecutable la función operativa sin ejecutar la función de verificación. Esto permite así integrar un mecanismo de arranque seguro en un sistema de a bordo sin modificar las otras componentes de este sistema.

[0070] De hecho, dado que la función operativa y la función de verificación son ejecutadas independientemente una de la otra en el arranque del sistema, la función operativa no tiene necesidad de integrar un mecanismo de arranque seguro específico. Esta seguridad es garantizada por la función de verificación durante el arranque en frío del sistema.

[0071] Se permite así evitar la necesidad de recertificación de las componentes no modificadas del sistema de a bordo, lo que resulta especialmente ventajoso cuando este sistema es de un nivel de criticidad elevado como, por ejemplo, el nivel DAL A. Así, la invención permite reducir considerablemente el coste y la complejidad del proceso de integración de una nueva componente en dicho sistema de a bordo.

REIVINDICACIONES

1. Controlador de arranque (18) seguro para un sistema de a bordo (10), comprendiendo el sistema de a bordo (10) además un módulo operativo (12) que integra una función operativa del sistema (10), y un módulo de verificación (14) que integra una función de verificación de diferentes componentes del sistema (10);
estando el controlador (18) configurado para:

- en un arranque en frío del sistema (10), hacer ejecutable en el arranque la función de verificación para realizar una verificación de funcionamiento que comprende una verificación de la autenticidad y de la integridad de la función operativa;
- cuando se completa la verificación de funcionamiento, en cada arranque en caliente después de dicho arranque en frío del sistema (10), hacer ejecutable en el arranque la función operativa,

donde el arranque en frío corresponde a un reinicio del sistema (10) después de un corte de alimentación que conduce a una pérdida de al menos una parte de los datos contenidos en una memoria de acceso aleatorio (24) del sistema (10),
estando el controlador (18) configurado además para consultar el estado de un registro de arranque modificable por un controlador de alimentación del sistema de a bordo (10) para determinar el tipo de arranque elegido entre un arranque en caliente y un arranque en frío.

2. Controlador (18) según la reivindicación 1, configurado para hacer ejecutable en el arranque una función colocando esta función o una referencia a la misma en una zona de arranque (32) reservada del sistema (10).

3. Controlador (18) según la reivindicación 1 o la reivindicación 2, que se presenta en la forma de una componente de hardware, preferentemente en la forma de una componente FPGA.

4. Controlador (18) según cualquiera de las reivindicaciones anteriores, implementado según el mismo nivel de criticidad que el módulo de verificación (14), siendo este nivel de criticidad superior o igual al nivel de criticidad del módulo operativo (12).

5. Controlador (18) según cualquiera de las reivindicaciones anteriores, configurado además para, en el arranque en frío del sistema, asociar a la función operativa una dirección de memoria accesible por la función de verificación.

6. Controlador (18) según cualquiera de las reivindicaciones anteriores, donde el sistema de a bordo (10) comprende además un módulo de configuración (16);
comprendiendo además dicha verificación de funcionamiento una verificación de la autenticidad y de la integridad del módulo de configuración (16).

7. Sistema de a bordo (10) que comprende:

- un módulo operativo (12) que integra una función operativa del sistema (10);
- un módulo de verificación (14) que integra una función de verificación de diferentes componentes del sistema (10);
- un controlador de arranque seguro (18) según cualquiera de las reivindicaciones anteriores.

8. Procedimiento de arranque seguro del sistema de a bordo (10) según la reivindicación 7;
comprendiendo el procedimiento la etapa siguiente:

- en un arranque en frío del sistema de a bordo (10), hacer ejecutable en el arranque la función de verificación para realizar una verificación de funcionamiento que comprende una verificación de la autenticidad y de la integridad de la función operativa; o
- cuando se completa la verificación de funcionamiento, en cada arranque en caliente después de dicho arranque en frío del sistema (10), hacer ejecutable en el arranque la función operativa.

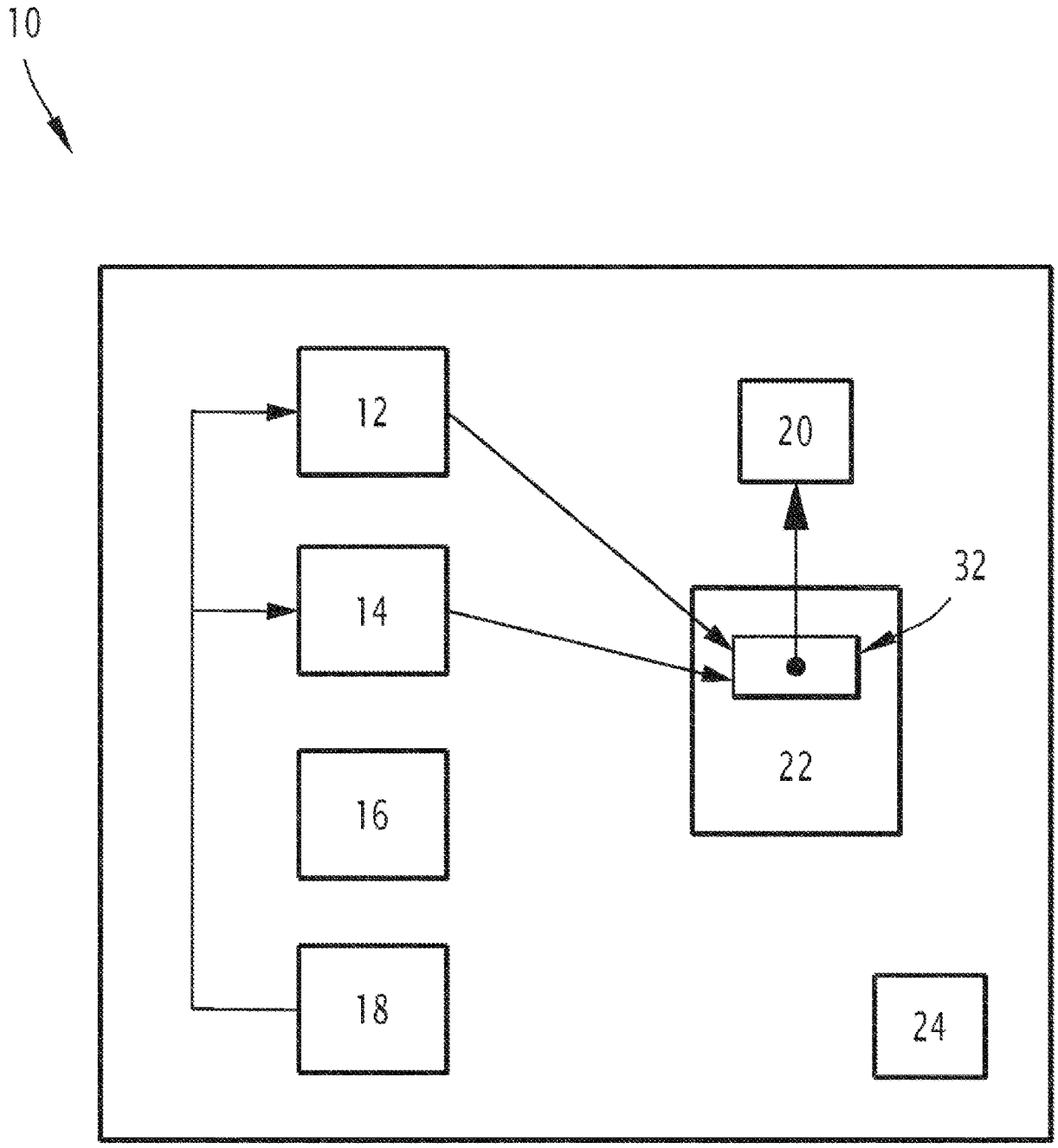

FIG.1