

19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 792 101**

51 Int. Cl.:

**G06F 21/88** (2013.01)

**H04W 12/12** (2009.01)

**H04W 12/02** (2009.01)

**H04W 12/08** (2009.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **13.04.2017 PCT/EP2017/058924**

87 Fecha y número de publicación internacional: **02.11.2017 WO17186506**

96 Fecha de presentación y número de la solicitud europea: **13.04.2017 E 17721057 (2)**

97 Fecha y número de publicación de la concesión europea: **25.03.2020 EP 3449416**

54 Título: **Procedimiento y equipo para borrar información relevante para la seguridad en un aparato**

30 Prioridad:

**28.04.2016 DE 102016207238**

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

**10.11.2020**

73 Titular/es:

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

72 Inventor/es:

**FALK, RAINER**

74 Agente/Representante:

**LOZANO GANDIA, José**

ES 2 792 101 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

**DESCRIPCIÓN**

Procedimiento y equipo para borrar información relevante para la seguridad en un aparato

- 5 La invención se refiere a un equipo y a un procedimiento para borrar información relevante para la seguridad, como por ejemplo claves criptográficas contenidas en aparatos móviles o también instalados de manera fija.
- 10 Los aparatos móviles, como por ejemplo robots, objetos voladores no tripulados, vehículos autónomos, pueden almacenar datos sensibles. Estos datos sensibles se aseguran con preferencia mediante procedimientos criptográficos, tal que los mismos sólo pueden ser extraídos y leídos en texto sin codificar por entidades autorizadas. Para ello se necesitan claves criptográficas. Tales claves criptográficas se generan por ejemplo mediante una clave genérica y se memorizan en un módulo de seguridad. Tal información relevante para la seguridad debe protegerse frente al acceso de personas no autorizadas o
- 15 frente al acceso mediante equipos no autorizados, para impedir una manipulación de funciones, a menudo críticas para la seguridad, que utilizan la información crítica para la seguridad. A menudo sólo se permite la utilización de aparatos para operar una función crítica para la seguridad por parte de entidades oficiales cuando un aparato proporciona medidas de protección prescritas para informaciones relevantes para la seguridad.
- 20 Se conocen por ejemplo sensores de manipulación, como por ejemplo láminas de protección frente a perforaciones, interruptores de carcasa o sensores de luz, que detectan una manipulación del aparato y/o una manipulación de un módulo de seguridad dispuesto en el aparato e inician una función de borrado de claves.
- 25 No obstante, tales sensores de manipulación sólo protegen frente a un ataque físico directo a un tal módulo de seguridad.
- 30 Por el documento US 2009/060194 A1 se conoce un método para proteger procesadores criptográficos integrados. Mediante un perfil de servicio se comprueba si se está manipulando el sistema.
- 35 El documento US 2006/225142 A1 describe un método y un sistema para activar un borrado completo de datos confidenciales en un aparato eléctrico. Para ello se vigila el aparato, comparándose valores de diagnóstico con valores de umbral predeterminados.
- 40 En el documento US 2014/351950 A1 se describe un aparato de comunicación que cuando se detectan vibraciones, protege informaciones memorizadas.
- 45 El documento US 8 615 612 B1 describe una carcasa para un medio de memoria portátil, para protegerlo frente a influencias externas, estando dotada la carcasa de una protección anti-manipulación.
- El documento US 2010/058077 A1 describe un aparato seguro frente a manipulaciones, que cuando se produce una manipulación borra informaciones confidenciales memorizadas en el aparato.
- 50 Por el documento US 2009/249460A1 se conoce un método y un sistema para modificar el funcionamiento de un aparato electrónico cuando se produce una utilización no autorizada.
- Por el documento US 2010/249460A1 se conocen un aparato volador y un procedimiento para borrar datos, en el que se borran datos de una memoria del aparato volador tan pronto como se presenta un evento previamente definido.
- 55 Cada vez más se utilizan informaciones relevantes para la seguridad en objetos móviles, por ejemplo para la localización y navegación seguras de objetos voladores no tripulados o vehículos autónomos. Además se necesita material de codificación para diversas funciones del aparato y/u objeto, creciendo con ello la cantidad de datos relevantes para la seguridad, por lo que debe iniciarse y en particular completarse un proceso de borrado de información relevante para la seguridad ante una destrucción mecánica del aparato, por ejemplo debida a la caída, colisión, fuego dirigido al objeto. Caso contrario, existe el peligro de que sean accesibles a entes no autorizados datos sensibles del objeto móvil siniestrado. También existe el peligro de que sensores de manipulación, también denominados función de protección tamper,
- 60 de un aparato móvil siniestrado o bien de un módulo de seguridad allí contenido, ya no funcionen correctamente y ya no puedan realizar la función exigida de protección frente a manipulaciones.
- 65 Es por lo tanto el objetivo de la presente invención lograr un procedimiento y un equipo que garanticen que incluso en un accidente u otro suceso imprevisto, se borran con fiabilidad y por completo datos del aparato relevantes para la seguridad.
- El objetivo se logra mediante las medidas descritas en las reivindicaciones independientes. En las reivindicaciones secundarias se presentan ventajosos perfeccionamientos de la invención.

## ES 2 792 101 T3

El procedimiento correspondiente a la invención para borrar informaciones relevantes para la seguridad en un aparato presenta las siguientes etapas del procedimiento:

- 5
- averiguación de al menos un parámetro de movimiento del aparato a lo largo del tiempo,
  - vigilancia del parámetro de movimiento averiguado a lo largo del tiempo en función de al menos un patrón de movimiento predeterminado y
  - activación de un proceso de borrado de la información relevante para la seguridad cuando el parámetro de movimiento averiguado corresponda a lo largo del tiempo al patrón de movimiento
- 10

Los aparatos móviles presentan, en escenarios de accidente típicos, también patrones de movimiento típicos. Así pasa un objeto volador, cuando falla el accionamiento, a un vuelo en descenso típico de una caída o bien llega por debajo de una altura predeterminada sobre tierra con una velocidad superior a un valor límite predeterminado. Los correspondientes patrones de movimiento se memorizan en el objeto volador como patrones de movimiento predeterminados. Mediante la vigilancia del parámetro de movimiento que se averigua, puede detectarse con gran seguridad un accidente y/o una destrucción del aparato e iniciarse a tiempo, antes de la destrucción del aparato, el borrado de la información relevante para la seguridad. El proceso de borrado puede así completarse antes de la destrucción del aparato y/o del módulo de seguridad sobre el que está memorizada la información relevante para la seguridad. Así puede asegurarse con elevada probabilidad que incluso en eventos imprevistos que originan una destrucción mecánica del aparato, se borra del aparato la información relevante para la seguridad, no siendo ya por lo tanto accesible.

- 15
- 20
- 25
- En una forma de ejecución ventajosa, se averigua como parámetro de movimiento una posición, una velocidad, una aceleración o una orientación del aparato.

- 30
- Así puede vigilarse por ejemplo, mediante la indicación de la posición, la altura del aparato sobre tierra y, cuando la altura es inferior a una altura mínima o al sobrepasarse una altura máxima, activar el proceso de borrado. De la misma manera puede suponerse que existe un accidente o un comportamiento incorrecto del aparato cuando se sobrepasa una aceleración máxima. Averiguando la aceleración como parámetro de movimiento, puede detectarse por ejemplo una manipulación incluso en aparatos instalados fijos y activarse el proceso de borrado.

- 35
- En una forma de ejecución ventajosa, se activa el proceso de borrado cuando el parámetro de movimiento, de los que al menos hay uno, se corresponde con el patrón de movimiento predeterminado, al menos durante un tiempo predeterminado y/o con una exactitud predeterminada.

- 40
- De esta manera queda asegurado que no origina un borrado prematuro y/o innecesario de la información relevante para la seguridad una oscilación breve, o que se presenta estadísticamente, del parámetro de movimiento averiguado.

- 45
- En una forma de ejecución ventajosa, el patrón de movimiento predeterminado es una trayectoria de movimiento del aparato.

- 50
- Una trayectoria de movimiento designa una curva espacial, a lo largo de la cual se mueve el aparato, por ejemplo el centro de gravedad del aparato. Mediante la vigilancia del movimiento del aparato en comparación con trayectorias de movimiento predeterminadas, que caracterizan patrones de movimiento inadmisibles y/o típicos de un accidente, puede también detectarse una desviación del aparato respecto a la trayectoria debido a una manipulación y, cuando se trata de aparatos muy críticos para la seguridad, activar esto ya un borrado de la información relevante para la seguridad.

- 55
- En una forma de ejecución ventajosa, caracteriza un patrón de movimiento predeterminado un modo de funcionamiento especial del aparato.

- 60
- Si por ejemplo el parámetro de movimiento trazado es idéntico a la trayectoria de movimiento de un modo de funcionamiento especial, que caracteriza por ejemplo un aterrizaje de emergencia, una parada de emergencia o una función de evasión para limitar los daños de un accidente, entonces puede iniciarse y completarse el proceso de borrado también en este caso.

- 65
- En una forma de ejecución ventajosa se averigua el parámetro de movimiento de un medio del entorno del aparato.

Por ejemplo puede averiguarse y vigilarse la velocidad con la que fluye el aire en la superficie de un objeto volador o a una cierta distancia de un objeto volador y con ello detectarse una entrada en pérdida, que origina o caracteriza una caída y activarse un borrado a tiempo de los datos relevantes para la seguridad.

- 5 El equipo correspondiente a la invención para borrar información relevante para la seguridad en un aparato incluye una unidad de detección, configurada para averiguar un parámetro del movimiento del aparato, una unidad de vigilancia que está configurada para vigilar el parámetro de movimiento averiguado a lo largo del tiempo en función de al menos un patrón de movimiento predeterminado y una
- 10 unidad de borrado, que está configurada para activar un proceso de borrado de la información relevante para la seguridad cuando el parámetro de movimiento averiguado corresponde a lo largo del tiempo al patrón de movimiento predeterminado.
- 15 La información relevante para la seguridad de un tal equipo puede así borrarse con elevada probabilidad ya antes de una destrucción mecánica y así impedirse una averiguación no permitida de esta información tras un evento imprevisto.
- En una forma de ejecución ventajosa, presenta la unidad de detección al menos un sensor, con preferencia un sensor inercial, un sensor de aceleración, un sensor de campo magnético o un sensor de posición, que averigua el parámetro de movimiento, de los que al menos hay uno.
- 20 En una forma de ejecución ventajosa, puede conectarse directamente la unidad de borrado con un módulo de seguridad, que memoriza información relevante para la seguridad.
- 25 Mediante una unión directa entre unidad de borrado y un módulo de seguridad, que memoriza información relevante para la seguridad, puede optimizarse el tiempo de retardo entre un proceso de borrado y la realización del proceso de borrado propiamente dicho. Igualmente aumenta la fiabilidad de la activación del proceso de borrado, ya que no existe ninguna línea de conexión entre unidad de borrado y módulo de seguridad que pueda dañarse en un accidente y afectar a una recepción de una señal de borrado en la unidad de borrado.
- 30 Un aparato correspondiente a la invención, que es un aparato móvil o un aparato instalado fijamente, incluye un equipo correspondiente para borrar información relevante para la seguridad.
- 35 En particular los aparatos móviles pueden dañarse al chocar con un cuerpo sólido y/o superficie o al penetrar en otro medio, por ejemplo agua, sin que la protección frente a manipulación existente lo detecte y active el borrado de la información relevante para la seguridad. Además pueden detectarse con fiabilidad mediante los citados sensores vibraciones o variaciones bruscas en el movimiento, que en aparatos instalados fijamente permiten deducir que existe un daño o también una sustracción no permitida del aparato. En ambos casos puede activarse el borrado basándose en esta información.
- 40 Además se reivindica un producto de programa informático que puede cargarse directamente en una memoria de una computadora digital y que incluye partes de código de programa que son adecuadas para ejecutar las etapas del procedimiento. Además se reivindica un soporte de datos que memoriza el producto de programa de computadora.
- 45 En los dibujos se representan, a modo de ejemplo, ejemplos de ejecución del procedimiento correspondiente a la invención, así como del equipo correspondiente a la invención y se describirán más en detalle en base a la siguiente descripción. Se muestra en:
- 50 figura 1 un ejemplo de ejecución general del procedimiento correspondiente a la invención, como diagrama secuencial;
- figura 2 un segundo ejemplo de ejecución del procedimiento correspondiente a la invención, como diagrama secuencial;
- 55 figura 3 un ejemplo de ejecución de un equipo correspondiente a la invención, en representación de bloques;
- figura 4 un ejemplo de ejecución de un aparato correspondiente la invención con un equipo correspondiente a la invención, en representación de bloques y
- figura 5 un ejemplo de ejecución de un patrón de movimiento predeterminado.
- Las partes que se corresponden entre sí se han dotado en todas las figuras de las mismas referencias.
- 60 Una pluralidad de aparatos con microprocesadores, como por ejemplo computadoras, pero también robots, objetos voladores, vehículos o también aparatos de campo en instalaciones de automatización, utilizan procedimientos criptográficos para comunicarse con interlocutores de comunicación de forma protegida frente a la manipulación y/o por ejemplo para poder utilizar aplicaciones de navegación por radio con señales fiables y seguras frente a la manipulación. Para ello se memorizan en el correspondiente aparato o en un equipo especial, que está dispuesto en el aparato, informaciones relevantes para la seguridad, como por ejemplo claves criptográficas utilizadas en los procedimientos criptográficos.
- 65 Con el procedimiento correspondiente a la invención, tal como se representa en la figura 1, queda garantizado que se borra información relevante para la seguridad a tiempo antes de que quede inutilizado

el aparato para funcionar. En el estado inicial 10 del procedimiento, se encuentran informaciones relevantes para la seguridad en un aparato. Las mismas pueden estar memorizadas por ejemplo en un módulo de seguridad. Entonces se averigua continuamente en la etapa 11 del procedimiento al menos un parámetro de movimiento del aparato a lo largo del tiempo. Un tal parámetro de movimiento puede caracterizar por ejemplo la posición del aparato, la velocidad, la aceleración o también la orientación del aparato. Se registra así por ejemplo una trayectoria del movimiento del aparato. Una tal trayectoria de movimiento es por ejemplo una trayectoria en el espacio bidimensional, tal como se representa en la figura 5, o también una curva espacial en un sistema de coordenadas tridimensional, a lo largo de la cual se mueve por ejemplo el centro de gravedad del aparato o del equipo. Además de la posición o del punto del aparato en el espacio, puede averiguarse también su velocidad o su aceleración, o también la orientación del aparato.

Los parámetros de movimiento pueden averiguarse mediante el aparato. Para ello pueden utilizarse en una variante sensores de choque (crash) del aparato, que por ejemplo activan como función adicional un airbag o pretensor del cinturón. En otra variante contiene el aparato un módulo de seguridad, que independiente o adicionalmente a sensores del aparato contiene sensores. Un tal módulo de seguridad tiene la ventaja de que puede integrarse con poco coste en un aparato, ya que el mismo presenta la funcionalidad correspondiente a la invención como función integrada.

En la etapa 12 del procedimiento se vigila igualmente de forma continua el parámetro de movimiento averiguado a lo largo del tiempo frente a al menos un patrón de movimiento predeterminado. El patrón de movimiento predeterminado puede ser en particular también una trayectoria de movimiento del aparato. En particular pueden corresponder trayectorias de movimiento predeterminadas a un modo de funcionamiento especial del aparato, como por ejemplo un aterrizaje de emergencia, una parada de emergencia, o una función de evasión para limitar los daños en un accidente.

Los patrones de movimiento predeterminados pueden extenderse a lo largo de un tiempo de distinta duración. La duración puede ser desde uno o varios milisegundos hasta varios segundos o incluso minutos. Por ejemplo puede ser ya un patrón de movimiento que se sobrepase por breve tiempo una velocidad máxima predeterminada. Un patrón de movimiento predeterminado puede ser igualmente un perfil de alturas o por ejemplo una altura constante sobre una superficie, tal que al pasar a ser la altura inferior a esta altura mínima, se active un proceso de borrado de la información relevante para la seguridad; véase la etapa 13 del procedimiento. Entonces puede además hacerse depender el proceso de borrado de que se alcance o sobrepase un valor de umbral predeterminado al menos durante un tiempo predeterminado. Esto evita que breves oscilaciones, que pueden ser debidas eventualmente sólo a efectos estadísticos o a errores de medida en sensores, activen el proceso de borrado y con ello por ejemplo ya no puedan ejecutarse funciones importantes en el aparato.

Por otro lado, debe elegirse la duración predeterminada de la coincidencia del patrón de movimiento averiguado con el patrón de movimiento predeterminado tal que permanezca un tiempo suficiente para poder ejecutar y completar el proceso de borrado.

En una variante puede averiguarse también un parámetro de movimiento de un medio del entorno del aparato. Por ejemplo puede medirse la velocidad del flujo de aire sobre la superficie del aparato o partes del aparato y compararse con una trayectoria de movimiento predeterminada para el medio. Igualmente puede por ejemplo medirse la presión en la superficie del aparato. Pueden utilizarse entonces uno o varios sensores por ejemplo en distintos lugares o sobre la superficie del aparato o también dentro del aparato para detectar parámetros de movimiento.

En la figura 2 se representa la secuencia del procedimiento en base al ejemplo de la vigilancia de la aceleración de un aparato. El punto de partida del procedimiento es el estado 20, en el que un aparato, por ejemplo con un módulo de seguridad, presenta un sensor de aceleración o un sensor inercial, que mide continuamente o a intervalos de tiempo predeterminados la aceleración del aparato y en particular del módulo de seguridad. En el módulo de seguridad se generan por ejemplo materiales de codificación criptográfica para diversas aplicaciones del aparato. En la etapa 21 del procedimiento se memoriza un tal material de codificación o también cualquier otra información relevante para la seguridad. En la etapa 22 del procedimiento se averigua la aceleración del aparato o también en especial del módulo de seguridad. En la etapa 23 del procedimiento se compara la aceleración averiguada por ejemplo frente a un valor de aceleración máximo predeterminado. Si la aceleración averiguada es a lo largo de un periodo de tiempo predeterminado mayor que un valor de aceleración máximo predeterminado, se activa a continuación en la etapa 24 del procedimiento el borrado de una memoria de codificación y con ello de todas las informaciones relevantes para la seguridad memorizadas en un aparato. Esto se señala mediante la flecha que conduce a la etapa 21 del procedimiento. El proceso de borrado se ejecuta entonces en lugar de la memorización de material de codificación como etapa 21 del procedimiento. Si la aceleración  $a(t)$  medida en el instante  $t$  es inferior al valor máximo predeterminado  $a_{max}$ , entonces se origina solamente otra detección de la aceleración. Esto se señala mediante la flecha de la etapa 23 del procedimiento a la etapa 22 del procedimiento.

La vigilancia de los parámetros de movimiento medidos se realiza en particular también a lo largo de un periodo de tiempo y un borrado de la información relevante para la seguridad sólo se activa cuando la evolución en el tiempo que resulta para el parámetro de movimiento detectado corresponde a un patrón de movimiento o una trayectoria de movimiento correspondiente predeterminados o a una evolución predeterminada del parámetro de movimiento o bien se desvía del patrón de movimiento o de la trayectoria del movimiento predeterminados.

La figura 3 muestra un equipo para borrar información relevante para la seguridad de un aparato. El equipo incluye una unidad de detección 31. La unidad de detección 31 puede contener uno o también varios sensores, por ejemplo un sensor inercial, que miden una aceleración o una velocidad de giro de un cuerpo. Tales sensores inerciales se utilizan por ejemplo en sistemas de navegación por inercia para aplicarlos en aeronaves o cohetes para la navegación aérea.

La unidad de detección 31 puede también estar configurada en varias partes y en diversos lugares en el aparato o sobre el mismo. Por ejemplo pueden estar montados varios sensores de posición o sensores de velocidad para detectar al menos un parámetro de movimiento en el aparato 30 o sobre el mismo.

Una unidad de vigilancia 32 vigila un movimiento averiguado a lo largo del tiempo en comparación con un patrón de movimiento predeterminado y registra con preferencia el mismo. Una unidad de borrado 33 activa un proceso de borrado de la información relevante para la seguridad cuando se cumplen criterios predeterminados. La unidad de vigilancia 32 y la unidad de borrado 33 están integradas en el equipo 30, por ejemplo en un detector de impacto.

El equipo 30 representado en la figura 3 es por ejemplo un módulo de seguridad con una interfaz externa 37, por ejemplo hacia un bus serie de datos según el I2C, una USB, un RS232 o el estándar SPI. A través de la interfaz 37 puede conectarse el equipo 30 por ejemplo con un aparato de campo, un aparato de control, un receptor de navegación por satélite o un sistema de computadora. El procesador de órdenes 36 ejecuta órdenes recibidas, como por ejemplo para codificar o decodificar datos, para firmar o para comprobar una firma, para calcular o para comprobar una suma de comprobación criptográfica o también para generar una secuencia pseudoaleatoria criptográfica.

El procesador de órdenes 36 utiliza para ello una unidad de codificación 35, denominada también criptomáquina, que realiza criptoalgoritmos simétricos, como por ejemplo AES, procedimientos criptográficos asimétricos, como por ejemplo RSA, Diffie-Hellman Key Exchange (intercambio de claves) o ECC, algoritmos para la firma digital, como DSA o ECDSA, funciones hash criptográficas, como por ejemplo HMAC o funciones de deducción de claves, como por ejemplo KDF. Además se incluye una memoria de claves 34. La unidad de borrado 33 está conectada con la memoria de claves 34 y envía una orden de borrado a la memoria de claves 34, que origina allí un borrado de todas las informaciones relevantes para la seguridad.

El sensor de aceleración 31 averigua continuamente la aceleración del equipo 30 o bien de un aparato 40, en el que está dispuesto el equipo 30 y registra así una trayectoria de movimiento 50, tal como se representa a modo de ejemplo en la figura 5. La trayectoria de movimiento 50 corresponde por ejemplo a una curva de localización  $x(t)$  de un objeto, que cae desde una altura  $x_0$  exclusivamente bajo la acción de la gravedad. Si se detecta a lo largo de un periodo de tiempo de por ejemplo  $t_B$  un patrón de movimiento 50 correspondiente mediante la unidad de vigilancia 32, activa la unidad de borrado 33 el proceso de borrado. Correspondientemente puede vigilarse como criterio de borrado el que se alcance una aceleración máxima, aquí denominada  $a_{max}$ , a lo largo del periodo de tiempo predeterminado, como valor de umbral. Un periodo de vigilancia  $t_B$  está elegido entonces tal que un patrón de movimiento predeterminado puede diferenciarse también con seguridad de un movimiento inusual aleatorio.

En la figura 4 se representa un aparato 40, que contiene un equipo para borrar informaciones relevantes para la seguridad. El aparato es por ejemplo un aparato de campo, un aparato de control, un receptor de navegación por satélite o un sistema de computadora. Los aparatos citados son simplemente un surtido de aparatos en los que puede integrarse el equipo. El aparato 40 presenta unidades funcionales 43 específicas del aparato, así como por ejemplo un módulo de seguridad 41 en el que está contenida la memoria de claves 34. Una unidad de detección 31, que incluye uno o varios sensores para detectar al menos un parámetro de movimiento, está conectada con una unidad de vigilancia 32, que compara el parámetro de movimiento detectado y registrado a lo largo del tiempo con uno o varios patrones de movimiento predeterminados y cuando se sobrepasa un valor de umbral o cuando hay coincidencia con un patrón de movimiento predeterminado, hace que por ejemplo la unidad de borrado 33 envíe una señal de borrado a través de la interfaz 42 a la memoria de claves 34 en el módulo de seguridad 41.

El equipo para borrar informaciones relevantes para la seguridad puede estar integrado así de distintas formas en un aparato. Las distintas unidades del equipo pueden estar implementadas por ejemplo todas en un módulo de seguridad, tal como se muestra en la figura 3, pero también distribuidas en un aparato, tal como muestra la figura 4. Los bloques funcionales representados pueden estar realizados en funciones basadas en hardware o como funciones basadas en software. El equipo 30 puede estar constituido por

5 ejemplo como un módulo de seguridad o criptocontrolador con sensor MEMS (sistema mecánico microelectrónico) integrado como sensor de aceleración y un sensor de choque (crash) integrado, que constituye la unidad de vigilancia 32. El aparato 40 puede incluir por ejemplo un aparato de campo con un sensor de aceleración MEMS, que ejecuta un borrado automático de material codificado si la aceleración detectada sobrepasa un valor de umbral predeterminado durante un tiempo predeterminado.

Todas las características descritas y/o dibujadas pueden combinarse ventajosamente entre sí en el marco de la invención. La invención no está limitada a los ejemplos de ejecución descritos.

**REIVINDICACIONES**

- 5 1. Procedimiento para borrar información relevante para la seguridad en un aparato, con las etapas del procedimiento:
- averiguación continua (11) de al menos un parámetro de movimiento del aparato (40) a lo largo del tiempo,
  - 10 • vigilancia continua (12) del parámetro de movimiento averiguado a lo largo del tiempo en función de al menos un patrón de movimiento predeterminado, siendo el patrón de movimiento predeterminado una trayectoria de movimiento (50) del aparato (40) y
  - 15 • activación (13) de un proceso de borrado de la información relevante para la seguridad cuando el parámetro de movimiento averiguado corresponda a lo largo del tiempo al patrón de movimiento predeterminado, de los que al menos hay uno, activándose el proceso de borrado cuando el parámetro de movimiento, de los que al menos hay uno, se corresponde con el patrón de movimiento predeterminado, al menos durante un tiempo predeterminado (tB).
- 20 2. Procedimiento según la reivindicación 1, en el que como parámetro de movimiento se averigua una posición, una velocidad, una aceleración o una orientación del aparato (40).
- 25 3. Procedimiento según una de las reivindicaciones precedentes, en el que el proceso de borrado se activa cuando el parámetro de movimiento, de los que al menos hay uno, se corresponde con el parámetro de movimiento predeterminado adicionalmente con una exactitud predeterminada.
- 30 4. Procedimiento según una de las reivindicaciones precedentes, en el que la trayectoria de movimiento predeterminada caracteriza un modo de funcionamiento especial del aparato (40).
- 35 5. Procedimiento según una de las reivindicaciones precedentes, en el que se averigua el parámetro de movimiento de un medio del entorno del aparato (40).
- 40 6. Equipo (30) para borrar información relevante para la seguridad en un aparato (40), que incluye:
- una unidad de detección (31), configurada para averiguar continuamente al menos un parámetro del movimiento del aparato (40),
  - una unidad de vigilancia (32), que está configurada para vigilar continuamente los parámetros de movimiento averiguados a lo largo del tiempo en función de al menos un patrón de movimiento predeterminado, siendo el parámetro de movimiento predeterminado una trayectoria de movimiento (50) del aparato (40) y
  - 45 • una unidad de borrado (33), que está configurada para activar un proceso de borrado de la información relevante para la seguridad cuando el parámetro de movimiento averiguado corresponde a lo largo del tiempo al patrón de movimiento predeterminado, activándose el proceso de borrado cuando el parámetro de movimiento, de los que al menos hay uno, se corresponde con el patrón de movimiento predeterminado, al menos durante un tiempo predeterminado (tB).
- 50 7. Equipo (30) según la reivindicación 6, en el que la unidad de detección presenta al menos un sensor, con preferencia un sensor inercial, un sensor de aceleración, un sensor de campo magnético o un sensor de posición, que averigua el parámetro de movimiento, de los que al menos hay uno.
- 55 8. Equipo (30) según la reivindicación 6 ó 7, en el que puede conectarse directamente al menos la unidad de borrado con un módulo de seguridad, que memoriza información relevante para la seguridad.
- 60 9. Aparato (40) que incluye un equipo según una de las reivindicaciones 6-8, siendo el aparato (40) un aparato móvil o un aparato instalado fijamente.
- 65 10. Producto de programa informático que puede cargarse directamente en una memoria de una computadora digital, que incluye partes de código de programa que ejecutan las etapas del procedimiento según una de las reivindicaciones 1 a 5.
11. Soporte de datos, que almacena el producto de programa informático según la reivindicación 10.

FIG 1

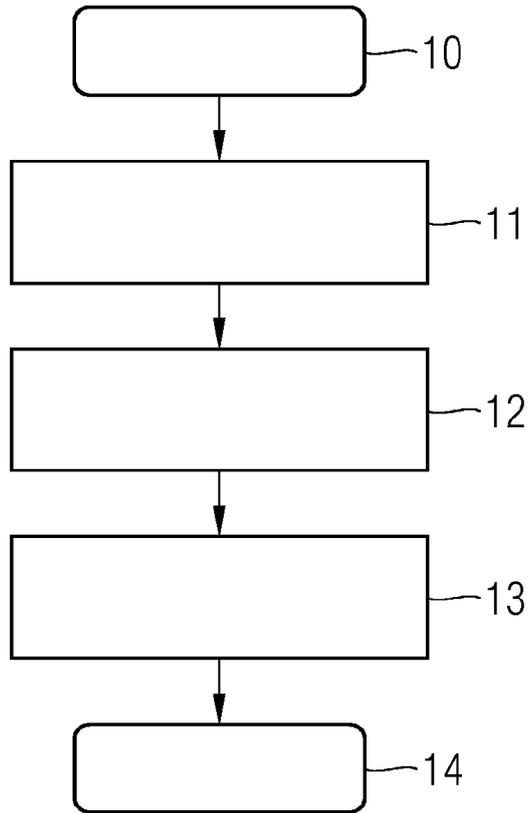


FIG 2

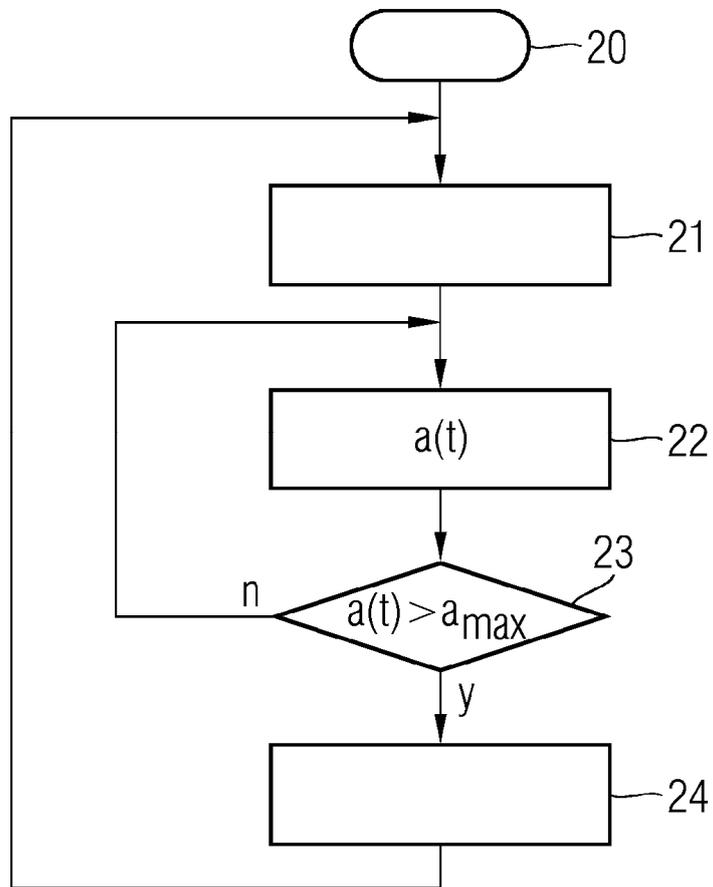


FIG 3

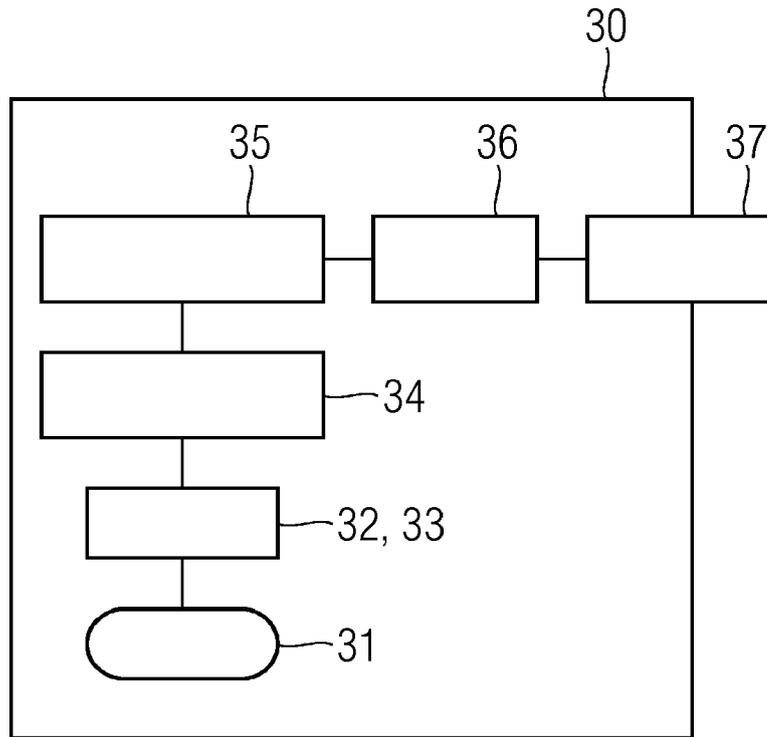


FIG 4

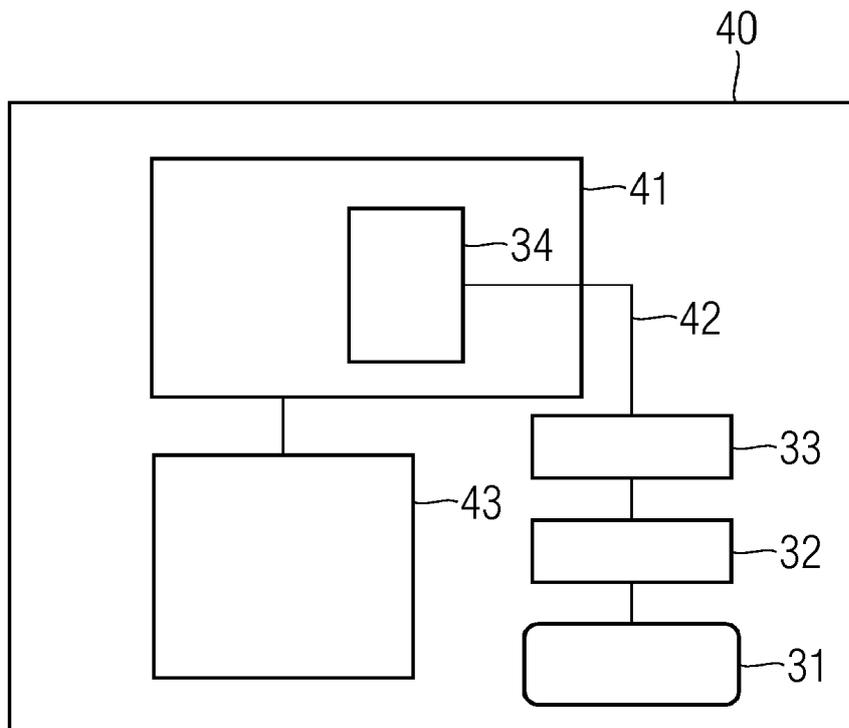


FIG 5

