

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 745 120**

51 Int. Cl.:

G06F 11/30 (2006.01)

G06F 12/08 (2006.01)

G06F 11/26 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **21.06.2011 PCT/JP2011/064116**

87 Fecha y número de publicación internacional: **15.03.2012 WO12032829**

96 Fecha de presentación y número de la solicitud europea: **21.06.2011 E 11823308 (9)**

97 Fecha y número de publicación de la concesión europea: **07.08.2019 EP 2615551**

54 Título: **Dispositivo de inspección de anomalías, unidad central de procesamiento y método de inspección de anomalías**

30 Prioridad:

08.09.2010 JP 2010201045

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

27.02.2020

73 Titular/es:

**mitsubishi heavy industries, ltd. (100.0%)
16-5, Konan 2-chome, Minato-ku
Tokyo 108-8215, JP**

72 Inventor/es:

**NAKAIDE, MINORU y
TODA, SHINICHI**

74 Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

ES 2 745 120 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

Dispositivo de inspección de anomalías, unidad central de procesamiento y método de inspección de anomalías

5 {Campo técnico}

La presente invención se refiere a unidades de inspección de fallos, unidades centrales de procesamiento y métodos de inspección de fallos.

10 {Antecedentes de la técnica}

Las unidades centrales de procesamiento (CPU) pueden usar direcciones virtuales para acceder a una memoria física, tal como una memoria de acceso aleatorio (RAM), dividida en unidades de página (por ejemplo, de varios kilobytes cada una). Direcciones virtuales, que difieren de las direcciones físicas, son direcciones de una memoria virtual que tiene un espacio virtual continuo compuesto de regiones de memoria física discontinua. Cuando una CPU usa direcciones virtuales, por lo tanto, una unidad de gestión de memoria (en adelante abreviada como "MMU") traduce las direcciones virtuales en direcciones físicas para permitir que la CPU acceda a la memoria física.

La MMU obtiene (carga) una tabla de página, que es una tabla de traducción para traducir direcciones virtuales a direcciones físicas, desde la RAM a una memoria intermedia de traducción al lado (en adelante abreviado como "TLB") y traduce una dirección virtual para la cual la CPU ha solicitado acceso a una dirección física usando esta tabla de página.

Como se muestra en el diagrama de la figura 4, una tabla de página tiene entradas de página de memoria para acceder a diferentes páginas de memoria de una memoria física 50. Cada entrada de página de memoria contiene las direcciones virtuales y físicas de la página de memoria correspondiente. La entrada de página de memoria necesaria se obtiene de la información de la tabla de página almacenada en la memoria física 50 y se almacena en una TLB 54 proporcionado en una MMU 52.

La entrada de la página de memoria también contiene un atributo de protección de memoria que especifica, por ejemplo, "leer", "escribir", o "ejecutar". La técnica descrita en PTL 1 es una técnica que establece un valor en el bit de protección del atributo de protección de memoria de la entrada de página de memoria obtenida de la tabla de página en la MMU para evitar una tarea incontrolada si una variable global utilizada solo por una tarea es accidentalmente sobrescrita por otra tarea.

35 {Lista de citas}**{Literatura de patentes}**

40 PTL 1
Solicitud de patente japonesa no examinada, Publicación n.º HEI-10-289158

El documento US 2009-300249A divulga una acumulación de datos de registros de desplazamiento de entrada múltiple (MISR) selectiva durante el procesamiento de excepciones en el que una pluralidad de puntos de prueba se ubican en nodos de circuito predeterminados en un sistema de procesamiento. El código de prueba que incluye un conjunto de interrupciones controlables por software se ejecuta utilizando un registro de desplazamiento de entrada múltiple (MISR) para generar una firma MISR. Se determinan uno o más tipos de interrupciones controlables por software seleccionados. Durante la ejecución del código de prueba, el MISR se usa para acumular también valores de datos de la pluralidad de puntos de prueba durante el procesamiento de excepción de una o más de las interrupciones controlables por software dentro del conjunto de interrupciones controlables por software que son de uno o más tipos de interrupciones controlables por software seleccionados para generar la firma MISR. Un registro de control de prueba tiene una pluralidad de campos, cada uno para seleccionar o no seleccionar un tipo de interrupción controlable por software correspondiente.

55 {Sumario de la invención}**{Problema técnico}**

60 Por otra parte, si una CPU 56 que se muestra en la vista esquemática de la figura 4 ingresa una dirección virtual correspondiente a una dirección física inexistente a la MMU 52, la MMU 52 genera una notificación de excepción de la CPU (error de página), que es una señal que indica un acceso ilegal, a la CPU 56. Sin embargo, si un fallo en la MMU 52 impide que se envíe una notificación de excepción de la CPU a pesar de la ocurrencia de un acceso ilegal, la CPU 56 podría funcionar de manera anormal, por ejemplo, congelar (colgar), ejecutar un proceso incontrolado o alterar accidentalmente la salida a otra unidad conectada al mismo.

65 A la vista de lo anterior, un objetivo de la presente invención es proporcionar una unidad de inspección de fallos, una

unidad de procesamiento central y un método de inspección de fallos que permite la inspección para determinar si se ha producido o no un fallo que impide la detección de un acceso ilegal en una unidad de gestión de memoria al ejecutar otro programa.

5 **{Solución al problema}**

La invención se define mediante las reivindicaciones independientes adjuntas.

10 Una unidad de inspección de fallos según un primer aspecto de la presente invención es una unidad de inspección de fallos provista para una unidad central de procesamiento conectada a una unidad de gestión de memoria. La unidad de gestión de memoria traduce una dirección física que es una dirección de una memoria física a una dirección virtual que es una dirección de una memoria virtual y emite una primera señal que indica un acceso ilegal si la memoria física es inaccesible con la dirección física a la que la dirección virtual se traduce. La unidad central de procesamiento envía la dirección virtual a la unidad de gestión de memoria, permite que se ingrese la primera señal y finaliza un programa que se ejecuta si se ingresa la primera señal. La unidad de inspección de fallos incluye medios de cambio para cambiar un modo de funcionamiento de la unidad de procesamiento central a un modo de prueba en el que la unidad de procesamiento central no termina un programa que se está ejecutando incluso si la unidad de gestión de memoria emite la primera señal; medios de salida para emitir una segunda señal para hacer que la unidad de gestión de memoria emita la primera señal a la unidad de gestión de memoria en el modo de prueba; y medios de detección para detectar si la primera señal se introduce o no después de que los medios de salida emiten la segunda señal a la unidad de gestión de memoria.

25 En la configuración anterior, la unidad de inspección de fallos se proporciona para la unidad central de procesamiento conectada a la unidad de gestión de memoria.

30 La unidad de gestión de memoria traduce una dirección física que es una dirección de una memoria física a una dirección virtual que es una dirección de una memoria virtual y emite una primera señal que indica un acceso ilegal si la memoria física es inaccesible con la dirección física a la que la dirección virtual se traduce. La memoria física es, por ejemplo, una memoria RAM, mientras que la memoria virtual es una memoria que tiene un espacio virtual continuo compuesto de regiones de memoria física discontinua. La unidad central de procesamiento envía la dirección virtual a la unidad de gestión de memoria, permite que se ingrese la primera señal y finaliza un programa que se ejecuta si se ingresa la primera señal.

35 Los medios cambiantes cambian el modo operativo de la unidad central de procesamiento al modo de prueba, en el que la unidad central de procesamiento no termina un programa que se está ejecutando incluso si la unidad de gestión de memoria emite la primera señal.

40 Después de cambiar el modo operativo al modo de prueba, los medios de salida emiten una segunda señal para hacer que la unidad de gestión de memoria emita la primera señal a la unidad de gestión de memoria. Es decir, la segunda señal es una señal para acceder ilegalmente a la memoria física.

Después de que los medios de salida emiten la segunda señal a la unidad de gestión de memoria, el medio de detección detecta si se introduce o no la primera señal.

45 Por lo tanto, después de cambiar el modo de funcionamiento de la unidad central de procesamiento al modo de prueba, se emite una segunda señal para acceder ilegalmente a la memoria física, y se detecta si se ingresa o no una primera señal que indica un acceso ilegal, que permite la inspección para determinar si se ha producido o no un error que impide la detección de un acceso ilegal en la unidad de gestión de memoria al ejecutar otro programa.

50 Preferentemente, en un primer aspecto, los medios de cambio restablecen el modo de prueba si se ingresa la primera señal en el modo de prueba, y los medios de detección detectan que la primera señal se ingresa si se restablece el modo de prueba.

55 En la configuración anterior, los medios de cambio restablecen el modo de prueba si se ingresa la primera señal en el modo de prueba, y los medios de detección detectan que la primera señal se ingresa si se restablece el modo de prueba.

60 Por lo tanto, porque el modo de prueba se reinicia inicialmente si la primera señal se ingresa en el modo de prueba, se puede evitar un período de tiempo prolongado innecesariamente durante el cual el modo operativo se establece en el modo de prueba.

65 Preferentemente, en un primer aspecto, la segunda señal es una señal que especifica una dirección virtual que no existe en la memoria virtual, una señal que especifica una dirección física que no existe en la memoria física, o una señal para ejecutar un acceso, a la dirección virtual, que viola un atributo de protección de memoria establecido en una entrada de página de memoria para acceder a la memoria física. En la configuración anterior, porque la segunda señal es una señal que especifica una dirección virtual que no existe en la memoria virtual, una señal que especifica

una dirección física que no existe en la memoria física, o una señal para ejecutar un acceso que viola un atributo de protección de memoria, se puede generar fácilmente una señal para acceder ilegalmente a la memoria física.

5 Una unidad de procesamiento central de acuerdo con un segundo aspecto de la presente invención es una unidad de procesamiento central que incluye la unidad de inspección de fallos descrita anteriormente y que finaliza un programa que se ejecuta si los medios de detección de la unidad de inspección de fallos detectan que no se recibe ninguna primera señal desde la unidad de gestión de memoria.

10 En la configuración anterior, la unidad central de procesamiento incluye la unidad de inspección de fallos descrita anteriormente. La unidad central de procesamiento termina un programa que se ejecuta si los medios de detección de la unidad de inspección de fallos detecta que no se ingresa ninguna primera señal desde la unidad de gestión de memoria.

15 El caso en el que no se ingresa la primera señal desde la unidad de gestión de memoria es el caso en que se produjo un fallo que impide la detección de un acceso ilegal por parte de la unidad central de procesamiento en la unidad de gestión de memoria. En ese caso, si la unidad central de procesamiento continúa ejecutando el programa y ejecuta un acceso ilegal, la unidad central de procesamiento podría funcionar de manera anormal, por ejemplo, congelar, ejecutar un proceso incontrolado o alterar accidentalmente la salida a otra unidad conectada al mismo.

20 En consecuencia, en la presente invención, la unidad central de procesamiento finaliza la ejecución de un programa si el modo operativo se establece en el modo de prueba y se detecta que no se ingresa la primera señal y, por lo tanto, se puede evitar que la unidad central de procesamiento funcione de manera anormal.

25 Un método de inspección de fallos de acuerdo con un tercer aspecto de la presente invención es un método de inspección de fallos provisto para una unidad central de procesamiento conectada a una unidad de gestión de memoria. La unidad de gestión de memoria traduce una dirección física que es una dirección de una memoria física a una dirección virtual que es una dirección de una memoria virtual y emite una primera señal que indica un acceso ilegal si la memoria física es inaccesible con la dirección física a la que la dirección virtual se traduce. La unidad central de procesamiento envía la dirección virtual a la unidad de gestión de memoria, permitiendo que se ingrese la primera señal y finaliza un programa que se ejecuta si se ingresa la primera señal. El método de inspección de fallos incluye una primera etapa para cambiar un modo operativo de la unidad de procesamiento central a un modo de prueba en el que la unidad de procesamiento central no finaliza un programa que se está ejecutando incluso si la unidad de gestión de memoria emite la primera señal; una segunda etapa para emitir una segunda señal para hacer que la unidad de gestión de memoria emita la primera señal a la unidad de gestión de memoria en el modo de prueba; y una tercera etapa para detectar si la primera señal se introduce o no después de que la segunda señal se envíe a la unidad de gestión de memoria.

40 En la configuración anterior, después de cambiar el modo de funcionamiento de la unidad central de procesamiento al modo de prueba, se emite una segunda señal para acceder ilegalmente a la memoria física, y se detecta si se ingresa o no una primera señal que indica un acceso ilegal, que permite la inspección para determinar si se ha producido o no un error que impide la detección de un acceso ilegal en la unidad de gestión de memoria al ejecutar otro programa.

45 La presente invención proporciona el efecto ventajoso de permitir la inspección en cuanto a si se ha producido o no un fallo que impide la detección de un acceso ilegal en una unidad de gestión de memoria al ejecutar otro programa.

{Breve descripción de los dibujos}

50 {Figura 1}
La figura 1 es un diagrama que muestra la configuración eléctrica relevante de un sistema de procesamiento de información de acuerdo con una realización de la presente invención.

{Figura 2}
La figura 2 es un diagrama esquemático que muestra la configuración de la información de la tabla de página almacenada en una RAM de acuerdo con la realización de la presente invención.

55 {Figura 3}
La figura 3 es un diagrama de flujo que muestra el flujo de procesamiento de un programa de inspección de fallos de acuerdo con la realización de la presente invención.

60 {Figura 4}
La figura 4 es un diagrama esquemático utilizado para ilustrar el procesamiento en una MMU en la técnica relacionada.

{Descripción de las realizaciones}

65 Una realización de una unidad de inspección de fallos, una unidad central de procesamiento y un método de inspección de fallos se describirán a continuación de acuerdo con la presente invención con referencia a los dibujos.

Se describirá a continuación una realización de la presente invención.

La figura 1 es un diagrama de bloques que muestra la configuración eléctrica de un sistema de procesamiento de información 10 según esta realización.

5 El sistema de procesamiento de información 10 incluye una CPU 12 responsable del funcionamiento de todo el sistema de procesamiento de información 10, una RAM 14 que es una memoria física utilizada como, por ejemplo, un área de trabajo cuando la CPU 12 ejecuta varios programas, una memoria de solo lectura (ROM) 16 en la que
10 varios programas, diversa información (datos), etc. se almacenan de antemano, y una unidad de disco duro (HDD) 18 que sirve como medio de almacenamiento para almacenar diversos programas y diversa información. Los medios de almacenamiento utilizados no se limitan al HDD 18 sino que pueden ser otros medios de almacenamiento que pueden almacenar datos, como una ROM flash.

15 La CPU 12 incluye una sección 22 de ejecución de programas para ejecutar un programa y una sección 24 de manejo de excepciones que termina un programa que se ejecuta si se ingresa una notificación de excepción de la CPU.

20 La CPU 12 también está conectada a través de un bus interno 40 a una MMU 20 que traduce una salida de dirección virtual desde la CPU 12 a una dirección física basada en una tabla de traducción (en lo sucesivo denominada "tabla de página") para traducir direcciones virtuales a físicas direcciones.

25 Como se muestra en la figura 2, la tabla de página contiene una pluralidad de entradas de página de memoria (entrada de página de memoria #1 a entrada de página de memoria #N) proporcionadas para diferentes unidades de página (páginas de memoria #1 a #N (N es un número entero)) en la RAM 14, que es una memoria física. Cada
30 entrada de página de memoria contiene las direcciones virtuales y físicas de la página de memoria correspondiente y un atributo de protección de memoria que especifica, por ejemplo, "leer", "escribir", "ejecutar", o "modo superusuario" lo que indica que solo se acepta el acceso de un usuario con derechos de acceso completos.

35 La MMU 20 incluye una TLB 26, una sección de traducción de direcciones 28 y una sección de protección de memoria 30.

40 La TLB 26 almacena información de la tabla de página que indica una tabla de página. De manera más específica, la TLB 26 obtiene y almacena la entrada de página de memoria necesaria de la información de la tabla de página almacenada en la RAM 14 dependiendo del programa ejecutado por la CPU 12.

45 La sección de traducción de direcciones 28 traduce la dirección virtual a una dirección física utilizando la información de la tabla de página obtenida en la TLB 26.

50 La sección de protección de memoria 30 detecta si hay o no acceso ilegal, lo que indica que la memoria física es inaccesible con la dirección física a la que la sección de traducción de direcciones 28 traduce la dirección virtual y, si detecta algún acceso ilegal, genera una notificación de excepción de la CPU, que es una señal que indica un acceso ilegal, a la CPU 12.

55 La información de la tabla de página se almacena por adelantado en el HDD 18, y cuando el sistema de procesamiento de información 10 comienza a funcionar, la información se envía desde el HDD 18 a la RAM 14 y se almacena allí. La información de la tabla de página almacenada en la RAM 14 se obtiene en la TLB 26 dependiendo del programa ejecutado por la CPU 12.

60 El sistema de procesamiento de información 10 también incluye una sección de entrada de operación 32 que está compuesta de, por ejemplo, un teclado y un ratón y que acepta la entrada de varias operaciones y una sección de visualización de imágenes 34, como una pantalla de cristal líquido. La sección de entrada de operación 32 no se limita a un teclado y ratón, sino que puede ser otro dispositivo de entrada, tal como botones pulsadores, que acepta la entrada de operaciones al sistema de procesamiento de información 10. Además, la sección de visualización de imágenes 34 no está limitada a una pantalla de cristal líquido sino que puede ser otro dispositivo de visualización,
65 tales como diodos emisores de luz (LED), que puede notificar a un usuario del sistema de procesamiento de información 10 sobre información diversa.

El sistema de procesamiento de información 10 incluye además una sección de procesamiento de entrada / salida 38 que está conectada a través de una línea de comunicación 36 a un sistema externo tal como otro sistema de procesamiento de información u otro sistema que es controlado por el sistema de procesamiento de información 10 y que realiza entrada y salida de diversa información entre el sistema de procesamiento de información 10 y el sistema externo.

65 La línea de comunicación 36 es, por ejemplo, una red de área amplia proporcionada por un operador de telecomunicaciones, una red de comunicación local, como una red de área local (LAN), o una ruta externa, y puede ser cableada o inalámbrica.

- La MMU 20, la RAM 14, la ROM 16, el HDD 18, la sección de entrada de operación 32, la sección de visualización de imágenes 34 y la sección de procesamiento de entrada / salida 38 están conectadas eléctricamente entre sí a través de un bus interno 40. Por lo tanto, a través de la MMU 20, la CPU 12 puede, por ejemplo, acceder a la RAM 14, la ROM 16 y el HDD 18, determinar el estado de la sección de entrada de operación 32 que se está operando, visualizar una imagen en la sección de visualización de imágenes 34, y enviar y recibir diversa información hacia y desde el sistema externo a través de la sección de procesamiento de entrada / salida 38.
- Como se ha descrito anteriormente, si la CPU 12 ingresa una dirección virtual correspondiente a una dirección física inexistente a la MMU 20, la MMU 20 envía una notificación de excepción de la CPU a la CPU 12. Sin embargo, si un fallo en la MMU 20 impide que se envíe una notificación de excepción de la CPU a pesar de la ocurrencia de un acceso ilegal, la CPU 12 podría funcionar de manera anormal, por ejemplo, congelar, ejecutar un proceso incontrolado o alterar accidentalmente la salida a otra unidad conectada al mismo.
- En consecuencia, el sistema de procesamiento de información 10 según esta realización ejecuta un proceso de inspección de fallos para inspeccionar si se ha producido o no un fallo que impide la detección de un acceso ilegal en la unidad de gestión de memoria mientras se ejecuta otro programa.
- A continuación, se describirá el funcionamiento del sistema de procesamiento de información 10 de acuerdo con esta realización.
- La figura 3 es un diagrama de flujo que muestra el flujo de procesamiento de un programa de inspección de fallos ejecutado por la CPU 12 cuando se ingresa una instrucción para ejecutar el proceso de inspección de fallos a través de la sección de entrada de operación 32, el programa se almacena en una región predeterminada en el HDD 18 de antemano. Cuando se ingresa una instrucción para ejecutar el proceso de inspección de fallos, el programa de inspección de fallos se envía desde el HDD 14 a la RAM 14 y se almacena en el mismo. Al comenzar el programa de inspección de fallos, la información de la tabla de página correspondiente al programa de inspección de fallos se obtiene en la TLB 26.
- En la etapa 100, el modo de funcionamiento se cambia a un modo de prueba. El modo de prueba es un modo operativo en el que la CPU 12 no finaliza un programa que se está ejecutando incluso si una notificación de excepción de la CPU se emite desde la MMU 20 y se ingresa a la CPU 12. Como un ejemplo, si el modo operativo se cambia al modo de prueba, la CPU 12 de acuerdo con esta realización establece un indicador que indica que el modo operativo está configurado en el modo de prueba.
- En la siguiente etapa 102, un acceso ilegal a la RAM 14, que es una memoria física, es ejecutado.
- En esta etapa, para ejecutar un acceso ilegal, la CPU 12 envía a la MMU 20 una señal de dirección que especifica una dirección virtual que no existe en la memoria virtual, una señal de dirección que especifica una dirección virtual correspondiente a una dirección física que no existe en la RAM 14, o una señal de dirección para ejecutar un acceso, a una dirección virtual, que viola un atributo de protección de memoria establecido en la entrada de la página de memoria para acceder a la memoria física.
- Los ejemplos de señales de dirección para ejecutar un acceso que viola un atributo de protección de memoria incluyen señales para escribir en la dirección virtual de una página de memoria que no tiene atributo de escritura, señales para ejecutar el contenido de la dirección virtual de una página de memoria que no tiene atributo de ejecución (recuperar un código de instrucción de la dirección virtual), y señales para acceder a la dirección virtual de una página de memoria que no tiene atributo de modo de superusuario en un modo de usuario normal.
- Cuando se introduce la señal de dirección anterior, la MMU 20 traduce la dirección virtual a una dirección física basada en la información de la tabla de página obtenida en la TLB 26. Sin embargo, dado que la señal de dirección de entrada da como resultado un acceso ilegal, la MMU 20 envía una notificación de excepción de la CPU a la CPU 12 si la MMU 20 está funcionando normalmente.
- En la siguiente etapa 104, se determina si se ingresa o no una notificación de excepción de la CPU dentro de un período de tiempo predeterminado, y el programa continúa a la etapa 106 si la determinación es afirmativa y continúa a la etapa 108 si la determinación es negativa.
- En la etapa 106, el modo de prueba se reinicia. Por lo tanto, el modo de funcionamiento de la CPU 12 se cambia a un modo de funcionamiento normal en el que la CPU 12 finaliza un programa que se ejecuta si se introduce una notificación de excepción de la CPU. Junto con restablecer el modo de prueba, la CPU 12 de acuerdo con esta realización restablece el indicador que indica que el modo operativo está configurado en el modo de prueba.
- En la siguiente etapa 108, se determina si el modo de prueba se ha reiniciado o no, y el programa finaliza si la determinación es afirmativa y continúa con la etapa 110 si la determinación es negativa. La CPU 12 de acuerdo con esta realización realiza una determinación afirmativa si el indicador que indica que el modo de funcionamiento está

establecido en el modo de prueba está establecido y realiza una determinación negativa si el indicador no está establecido.

5 Es decir, el caso en que se reinició el modo de prueba es el caso en que la MMU 20 ha enviado una notificación de excepción de la CPU a la CPU 12. A la inversa, el caso en el que el modo de prueba no se ha restablecido es el caso en que la MMU 20 no ha emitido ninguna notificación de excepción de la CPU a la CPU 12, indicando que se ha producido un fallo que impide la detección de un acceso ilegal en la MMU 20.

10 En la etapa 110, se determina si hay algún programa en ejecución o no, y el programa continúa con la etapa 112 si la determinación es afirmativa y continúa con la etapa 114 si la determinación es negativa.

En la etapa 112, el programa que ejecuta la sección de ejecución del programa 22 finaliza.

15 En la etapa 114, el programa finaliza después de que se ejecuta un procedimiento de notificación para notificar al usuario sobre la ocurrencia de un fallo que impide la detección de un acceso ilegal en la MMU 20 y, si se termina un programa que se está ejecutando, también sobre el nombre y otra información sobre el programa terminado, mostrándolos en la pantalla de la sección de visualización de imágenes 34.

20 Como se ha descrito anteriormente, la CPU 12 de acuerdo con esta realización cambia el modo operativo al modo de prueba, en el que no finaliza la ejecución de un programa incluso si la MMU 20 emite una notificación de excepción de la CPU, emite una señal para hacer que la MMU 20 envíe una señal de notificación de excepción de la CPU a la MMU 20, y detecta si una notificación de excepción de la CPU se ingresa o no desde la MMU 20.

25 Por lo tanto, la CPU 12 de acuerdo con esta realización puede inspeccionar si se ha producido o no un fallo que impide la detección de un acceso ilegal en la MMU 20 al ejecutar otro programa.

30 Además, porque la CPU 12 según esta realización restablece el modo de prueba si se ingresa una notificación de excepción de la CPU en el modo de prueba y detecta que se ingresa una notificación de excepción de la CPU en función del hecho de que el modo de prueba se reinicia, se puede evitar un período de tiempo prolongado innecesariamente durante el cual el modo operativo se establece en el modo de prueba.

35 Además, porque la CPU 12 de acuerdo con esta realización usa, como la señal para hacer que la MMU 20 emita una señal de notificación de excepción de la CPU, una señal de dirección que especifica una dirección virtual que no existe en la memoria virtual, una señal de dirección que especifica una dirección física que no existe en la memoria física, o una señal de dirección para ejecutar un acceso, a una dirección virtual, que viola un atributo de protección de memoria establecido en la entrada de la página de memoria para acceder a la memoria física, se puede generar fácilmente una señal para acceder ilegalmente a la memoria física.

40 Además, porque la CPU 12 de acuerdo con esta realización termina un programa que se ejecuta si el modo operativo se establece en el modo de prueba y se detecta que no se ingresa ninguna notificación de excepción de la CPU, se puede evitar que la CPU 12 funcione de manera anormal.

45 Aunque la presente invención se ha descrito anteriormente usando la realización anterior, el alcance técnico de la presente invención no se limita al alcance descrito en la realización anterior. Se pueden agregar varias modificaciones y mejoras a la realización anterior sin apartarse del espíritu de la invención, y el alcance técnico de la presente invención abarca realizaciones con tales modificaciones y mejoras.

50 Por ejemplo, aunque la realización anterior ilustra el caso en el que se detecta que la notificación de excepción de la CPU se emite desde la MMU 20 en función del hecho de que se restablece el modo de prueba, la presente invención no se limita a esto, pero se puede practicar en una realización en la que se detecta que la notificación de excepción de la CPU se emite desde la MMU 20 detectando la notificación de excepción de la CPU en sí misma.

55 Además, aunque la realización anterior ilustra el caso donde la memoria física es la RAM 14, la presente invención no se limita a esto, pero se puede practicar en una realización en la que la memoria física es la RAM 14 y el HDD 18.

60 Además, aunque la realización anterior ilustra el caso en el que el procedimiento de notificación proporciona una notificación en una pantalla de imagen, la presente invención no se limita a esto, pero se puede practicar, por ejemplo, en una realización en la cual, si una impresora está conectada a la sección de procesamiento de entrada / salida 38, la impresora envía una notificación formando un mensaje que contiene la notificación como una imagen en, por ejemplo, un medio de papel, o en una realización en la que un altavoz (no mostrado) da una notificación en forma de sonido.

{Lista de signos de referencia}

- 10 sistema de procesamiento de información
- 12 CPU

- 14 RAM
- 20 MMU
- 24 sección de manejo de excepciones

REIVINDICACIONES

1. Una unidad de inspección de fallos provista para una unidad central de procesamiento (12) conectada a una unidad de gestión de memoria (20), comprendiendo la unidad central de procesamiento (12) la unidad de inspección de fallos, la unidad de gestión de memoria (20) está configurada para traducir una dirección física que es una dirección de una memoria física (14) a una dirección virtual que es una dirección de una memoria virtual y generar una primera señal que indica un acceso ilegal si la memoria física (14) es inaccesible con la dirección física a la que se traduce la dirección virtual, la unidad central de procesamiento (12) está configurada para enviar la dirección virtual a la unidad de gestión de memoria (20), permitir que se ingrese la primera señal y terminar un programa que se ejecuta si se ingresa la primera señal, comprendiendo la unidad de inspección de fallos:

un medio de cambio para cambiar un modo de funcionamiento de la unidad de procesamiento central (12) a un modo de prueba en el que la unidad de procesamiento central (12) no finaliza un programa que se está ejecutando incluso si la unidad de gestión de memoria (20) emite la primera señal;
 la unidad de inspección de fallos se **caracteriza además por:**

un medio de salida para la salida, mientras la unidad central de procesamiento (12) está operando en el modo de prueba, una segunda señal a la unidad de gestión de memoria (20) para hacer que la unidad de gestión de memoria (20) emita la primera señal; y
 un medio de detección para detectar si la primera señal se introduce o no en la unidad central de procesamiento (12) después de que el medio de salida emite la segunda señal a la unidad de gestión de memoria (20).

2. La unidad de inspección de fallos según la reivindicación 1, en la que los medios de cambio están configurados para restablecer el modo de prueba si la primera señal se introduce en el modo de prueba; y el medio de detección está configurado para detectar que se ingresa la primera señal si se restablece el modo de prueba.

3. La unidad de inspección de fallos según las reivindicaciones 1 o 2, en la que la segunda señal es una señal que especifica una dirección virtual que no existe en la memoria virtual, una señal que especifica una dirección física que no existe en la memoria física (14), o una señal para ejecutar un acceso, a la dirección virtual, que viola un atributo de protección de memoria establecido en una entrada de página de memoria para acceder a la memoria física (14).

4. Una unidad central de procesamiento (12) que comprende la unidad de inspección de fallos de acuerdo con una de las reivindicaciones 1 a 3, la unidad central de procesamiento (12) está configurada para terminar un programa que se está ejecutando si los medios de detección de la unidad de inspección de fallos detectan que no se ingresa la primera señal desde la unidad de gestión de memoria (20).

5. Un método de inspección de fallos provisto para una unidad central de procesamiento (12) conectada a una unidad de gestión de memoria (20), la unidad de gestión de memoria (20) está configurada para traducir una dirección física que es una dirección de una memoria física (14) a una dirección virtual que es una dirección de una memoria virtual (14) y emitir una primera señal que indica un acceso ilegal si la memoria física (14) es inaccesible con la dirección física a la que se traduce la dirección virtual, la unidad central de procesamiento (12) está configurada para enviar la dirección virtual a la unidad de gestión de memoria (20), permitir que se ingrese la primera señal y terminar un programa que se ejecuta si se ingresa la primera señal, comprendiendo el método de inspección de fallos:

una primera etapa para cambiar un modo operativo de la unidad central de procesamiento (12) a un modo de prueba en el que la unidad central de procesamiento (12) no finaliza un programa que se ejecuta incluso si la unidad de gestión de memoria (20) emite la primera señal;
 el método de inspección de fallos se **caracteriza además por:** una segunda etapa de salida, mientras la unidad central de procesamiento (12) está operando en el modo de prueba, una segunda señal de la unidad central de procesamiento (12) a la unidad de gestión de memoria (20) para hacer que la unidad de gestión de memoria (20) emita la primera señal; y una tercera etapa para detectar si la primera señal se introduce o no en la unidad central de procesamiento (12) después de que la segunda señal se envíe a la unidad de gestión de memoria (20).

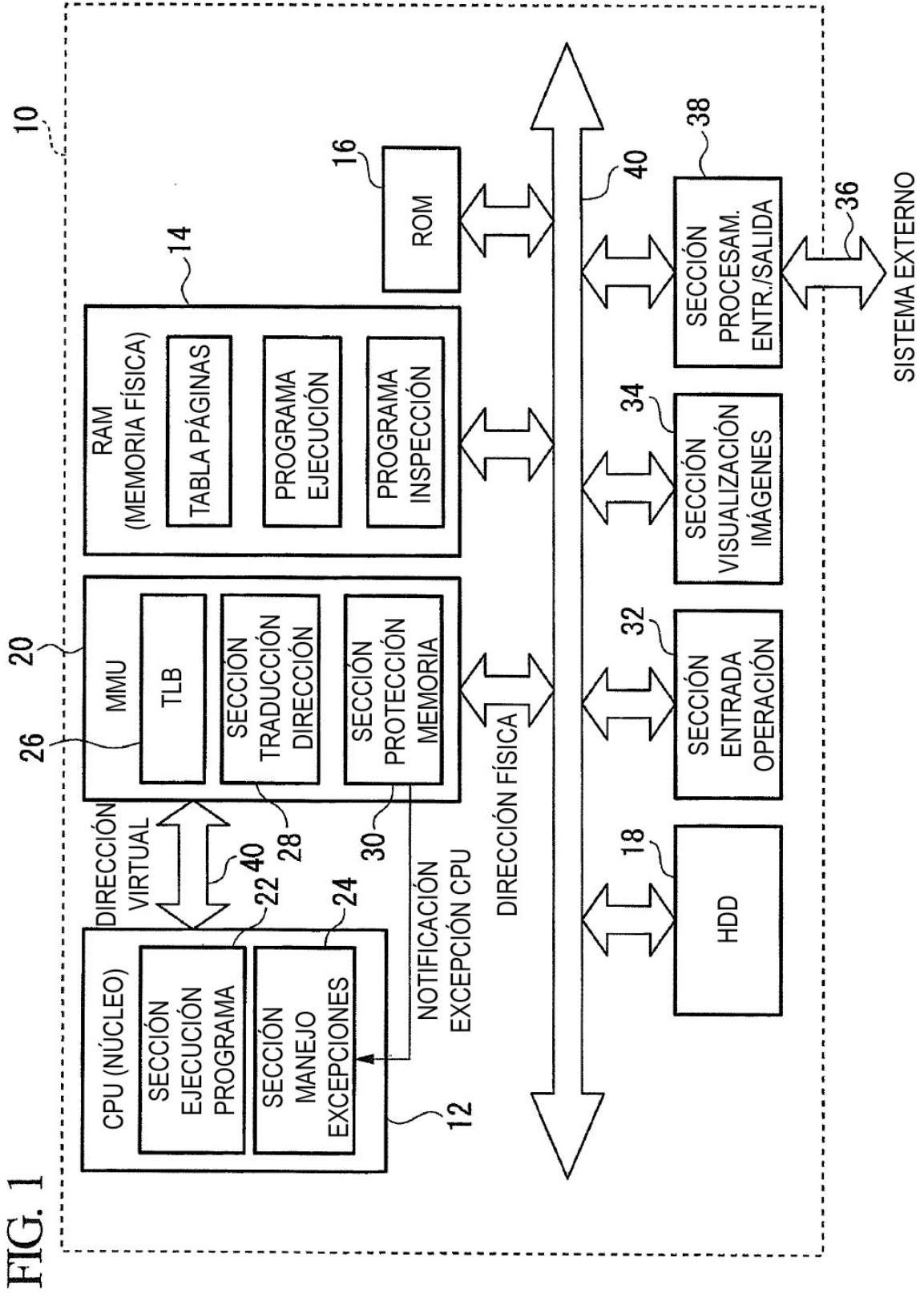


FIG. 1

FIG. 2

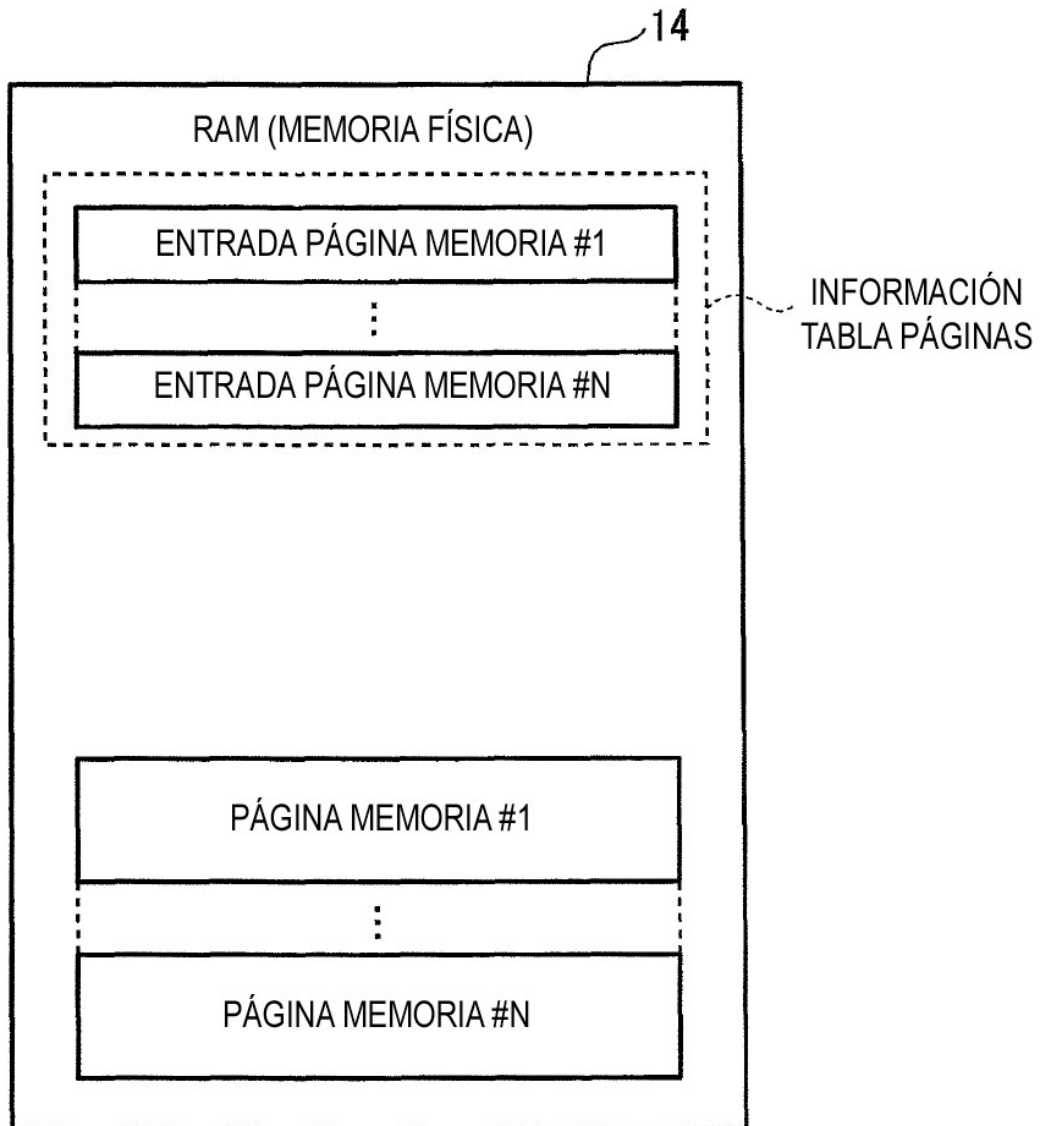


FIG. 3

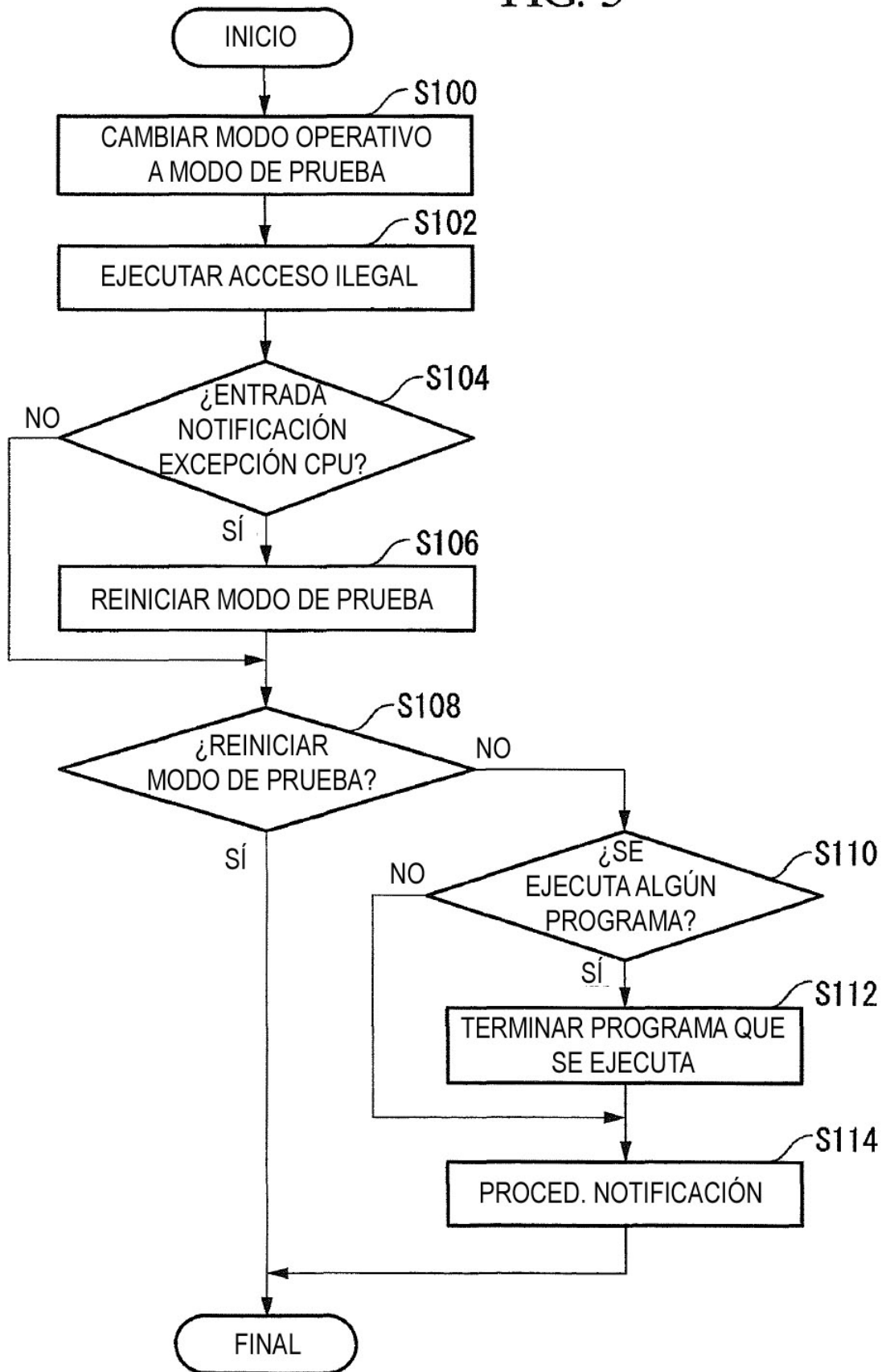


FIG. 4

