(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 347 519**

(51) Int. Cl.:
G06F 21/02 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **00103666 .4**
(96) Fecha de presentación : **22.02.2000**
(97) Número de publicación de la solicitud: **1031906**
(97) Fecha de publicación de la solicitud: **30.08.2000**

(54) Título: **Procedimiento y disposición de acoplamiento para prevenir el acceso no autorizado a un microprocesador.**

(30) Prioridad: **26.02.1999 FI 19990414**

(45) Fecha de publicación de la mención BOPI:
02.11.2010

(45) Fecha de la publicación del folleto de la patente:
02.11.2010

(73) Titular/es: **Nokia Corporation**
Keilalahdentie 4
02150 Espoo, FI

(72) Inventor/es: **Laiho, Kimmo y**
Kaunisto, Ismo

(74) Agente: **López Bravo, Joaquín Ramón**

DESCRIPCIÓN

La invención se refiere, en general, a la tecnología de protección de circuitos electrónicos y sus programas almacenados contra el acceso no autorizado. Especialmente, la invención se refiere a la tecnología de prevenir el uso no autorizado de una cierta interfaz a un procesador.

Un microprocesador (o "procesador" para abreviar) puede comprender una denominada interfaz de depuración para proporcionar un amplio control sobre las operaciones del procesador. La interfaz de depuración se puede usar para, por ejemplo, descargar y cargar programas, leer contenidos de los registros internos del procesador y realizar la ejecución paso por paso de los programas almacenados. En general, puede decirse que en un dispositivo electrónico controlado por procesador ofrece un acceso más o menos directo a todas estas características funcionales del procesador que pueden ser propiedad del fabricante y/o del operador autorizado del dispositivo. Por tanto, los fabricantes están buscando con impaciencia soluciones que evitarían el uso no autorizado de la interfaz de depuración. En función de la estructura del procesador puede haber también otras interfaces de procesador que deberían protegerse de forma similar.

Una fuerza bruta alternativa para proteger una interfaz es eliminar físicamente los vástagos externos o cortar las conexiones desde ellos a los correspondientes acoplamientos internos en los dispositivos que van desde la producción en serie al mercado. Por tanto, la interfaz de depuración sólo estaría disponible en prototipos y en unidades de prueba. La desventaja está clara: La interfaz de depuración no está disponible cuando, por ejemplo, una unidad disponible comercialmente debe ponerse en servicio o repararse.

El documento de la técnica anterior EP-A-O-897 144 divulga un procedimiento y un aparato para proporcionar protección frente al acceso en un procesador de datos. La solución se basa en comparar los datos de acceso y las señales control con valores de comparación previamente definidos y en responder a una falta de coincidencia realizando una reinicialización del hardware.

El documento de la técnica anterior EP-A- 831 399 divulga un circuito temporizador de vigilancia (en inglés “perro guardián”), cuyo propósito es controlar que un procesador está funcionando de un modo deseado. Las situaciones de error, generadas por interferencias electromagnéticas, radiación externa o fallos de software, producen un funcionamiento anormal del procesador y, en consecuencia, alertan al circuito de vigilancia, que responde reiniciando el procesador.

Es un objeto de la presente invención proporcionar un procedimiento y una disposición de acoplamiento para prevenir el uso no autorizado de determinadas interfaces en un procesador. También es un objeto de la invención que el conjunto no necesariamente impide el uso autorizado de las interfaces protegidas. Un objeto adicional de la invención es implementar la protección sin un gran número de componentes adicionales.

Los objetos de la invención se consiguen mediante la asociación del uso de la interfaz de depuración con un cambio en ciertas rutinas realizadas por el procesador, disponiendo la detección de tal cambio fuera del procesador y uniendo la detección con la inhabilitación de una gran parte de la operación del procesador si no se ha activado cierto procedimiento de habilitación.

El procedimiento de acuerdo con la invención se caracteriza por las etapas mencionadas en la parte de caracterización de la reivindicación independiente dirigida a un procedimiento.

Adicionalmente, la invención se aplica a un dispositivo que está caracterizado por los rasgos mencionados en la parte de caracterización de la reivindicación independiente dirigida a un dispositivo.

Un dispositivo electrónico controlado por procesador comprende también otros componentes, entre los cuales puede haber otro circuito que es programable en el sentido de que se puede disponer de modo que espere ciertas señales de entrada y reaccione a ellas con cierta respuesta. De acuerdo con la invención, tal circuito externo se dispone de modo que actúe como un denominado perro guardián: el procesador cuya(s) interfaz(ces) se deben proteger tiene que "acariciar al perro guardián" con regularidad o dar una cierta señal de entrada al circuito externo con el fin de evitar la inhabilitación de al menos una gran parte de las operaciones del procesador. El procesador también está dispuesto de modo que asocie el uso de una interfaz protegida con el retraso o atasco de la emisión de dichas entradas, por que normalmente un intento de usar la interfaz protegida tendrá como resultado la inhabilitación de al menos una gran parte de la operación del procesador. Un usuario autorizado conoce una orden o procedimiento secreto que evitará que el circuito externo reaccione o anule la reacción de modo que el procesador se mantenga operativo.

El concepto de “acariciar al perro guardián” puede también entenderse de forma inversa: en condiciones normales, el procesador no envía entradas al circuito externo, lo que mantiene el procesador habilitado. Un intento de usar la(s) interfaz(ces) protegida(s) hace que el procesador emita una alarma al circuito externo que, a su vez, inhabilita al menos una gran parte de la operación del procesador. Una orden o procedimiento de liberación está disponible para los usuarios autorizados para evitar que la alarma cause la inhabilitación.

Los nuevos rasgos que se consideran característicos de la invención se exponen en particular en las reivindicaciones adjuntas. No obstante, la propia invención, tanto en cuanto a su construcción como a su procedimiento de operación, junto con objetos adicionales y ventajas de la misma, se entenderá mejor a partir de la siguiente descripción de formas de realización específicas cuando se leen en relación con las figuras adjuntas.

Las Figuras 1a-1c ilustran el principio de una primera forma de realización de la invención,

Las Figuras 2-a2c ilustran el principio de una segunda forma de realización de la invención,

La Figura 3 Ilustra la disposición de un circuito que implementa el principio de las Figuras 1a-1c y

La Figura 4 ilustra un dispositivo electrónico de acuerdo con una forma de realización de la invención.

Partes similares en las figuras se designan con los mismos indicadores de referencia.

Las Figuras 1a a 1c muestran un procesador 101 con una interfaz 102 que debería protegerse contra el acceso no autorizado. Otra parte del conjunto es un circuito de vigilancia 103. En condiciones normales, cuando no hay intentos de usar la interfaz 102, el procesador envía con regularidad un poco de información de entrada al circuito de vigilancia de acuerdo con la flecha “PAT”. Como resultado, el circuito de vigilancia 103 habilita la operación del procesador 101 de acuerdo con la flecha “HABILITAR”. El procesador 101 se ha construido y programado de tal modo que cuando se efectúa un intento de usar la interfaz protegida 102 como en la Figura 1b, el procesador se detiene o retrasa el envío de entradas al circuito de vigilancia 103. Este último normalmente responde inhabilitando al menos una gran parte de las operaciones del procesador. La Figura 1c ilustra una situación en la que el intento de usar la interfaz protegida 102 se acompaña de una orden de liberación al circuito de vigilancia. La orden de liberación evita que el circuito de vigilancia 103 inhabilite el procesador 101 de modo que el usuario que sepa la orden de liberación correcta pueda proseguir usando la interfaz protegida, por ejemplo para depurar cualquier software recién cargado en el procesador.

Las Figuras 2a a 2c muestran de nuevo un procesador y un circuito de vigilancia que ahora se han designado 101’ y 103’ respectivamente porque su operación difiere ligeramente de la del procesador 101 y el circuito de vigilancia 103 de las Figuras 1a a 1c. Cuando no se efectúan intentos de usar la interfaz protegida 102, el procesador 101’ no envía al circuito de vigilancia 103’ ninguna entrada relacionada con la interfaz protegida como en a Figura 2a. Un

intento de usar la interfaz protegida hace que se emita una alarma al circuito de vigilancia 103' de acuerdo con la Figura 2b, lo que inhabilita al menos una gran parte de la operación del procesador 101'. Si el intento de uso de la interfaz protegida se acompaña de una cierta orden de liberación como en la Figura 2c, el circuito de vigilancia 103' ignora la alarma y permite que continúe la operación habilitada del procesador 101'.

La Figura 3 es un ejemplo de una disposición de acoplamiento que se puede usar para implementar el principio de las Figuras 1a a 1c. El conjunto comprende un procesador 101 con una interfaz de depuración 102 a proteger, así como un coprocesador 103 que actúa como circuito de vigilancia. La interfaz de depuración está acoplada a un conector 301 en Modo de Depuración de fondo. Los otros bloques funcionales del procesador 101 mostrados son el bloque de interfaz I^2C 302 y el bloque de alimentación 303. El primero es un bloque interfaz conocido como tal: La interfaz I^2C es *de facto* un bus estándar industrial para el acoplamiento de elementos de circuito programables. El bloque de Alimentación 303 es responsable de proporcionar tensión de funcionamiento a al menos una gran parte del procesador 101. Está acoplado a una fuente de alimentación a través de un conmutador 304 y también tiene otros, de los que se ha mostrado una entrada de reinicio. Algunos de los bloques de funcionamiento específicamente mostrados del co-procesador 103 son el bloque de interfaz I^2C 305, el bloque de salida de señal de reinicio 306, el bloque de salida de señal en espera 307 y el bloque de entrada de órdenes 308. De estos, el primero es para comunicar con el procesador principal 101, el bloque de señal de salida de reinicio 306 es para enviar órdenes de reinicio al procesador principal 101, el bloque de salida de señal en espera 307 es para controlar el conmutador 304 y el bloque de entrada de órdenes 308 es para recibir órdenes de fuentes externas como de un receptor de infrarrojos 309. También hay un bloque de vigilancia 301 cuya implementación y operación se describen con mayor detalle más adelante.

Mientras la señal de reinicio del bloque 306 para bloquear 303 permanece activada, el procesador 101 no está operativo. Una vez que la señal de reinicio se libera, se requiere que el procesador 101 comience a proporcionar con regularidad una cierta señal a través de la conexión I^2C desde el bloque 302 al bloque 305. El requisito se cumple asegurando que hay un conjunto correspondiente de instrucciones en el programa que el procesador ejecuta. Esto implementa la función de "acariciar al perro guardián". Otro conjunto de instrucciones en el programa del procesador principal es responsable de detener la emisión de las señales de "acariciar al perro guardián" en cuanto se detecte un intento de uso de la interfaz de depuración 102.

Hay múltiples formas conocidas de realizar una función de vigilancia como tal en el co-procesador 103. Una simple implementación se basa en un registro de vigilancia dentro del

bloque 310. Cada vez que el co-procesador recibe una señal de “acariciar” a través de la interfaz I^2C, reinicia el valor de tal registro a cero o a otro valor fijo adecuado. Entre las señales de caricias, el co-procesador incrementa (o disminuye) con regularidad el valor del registro de vigilancia. Si el valor alcanza un cierto límite, el co-procesador lo toma como una indicación de que el procesador principal ya no está respondiendo. De acuerdo con el principio de las Figuras 1a a 1c transmite a través del bloque de salida de la señal en espera 307 una señal que abre el conmutador 304. Por tanto, el procesador principal se apaga completamente. En un modo de operación típico, el co-procesador activa simultáneamente la señal de reinicio para bloquear 303.

La recuperación desde la condición de en espera/reinicio se produce según se determine en el programa ejecutado por el co-procesador 103. Un modo de operación factible es tal cuando el co-procesador espera un cierto intervalo de retraso, después libera la señal de en espera, lo que hace que el conmutador 304 se cierre y, después, libera la señal de reinicio. Si el usuario no autorizado todavía está intentando usad la interfaz de depuración, el procesador principal ni siquiera comienza a enviar señales de “acariciar al perro guardián” de modo que el registro de vigilancia en el co-procesador alcanzará pronto su valor límite de nuevo, lo que produce otro ciclo de apagado del procesador. El procesador 101 solo puede retomar el funcionamiento normal después de que se han detenido los intentos no autorizados para usar la interfaz de depuración 102.

Un usuario depurador autorizado del sistema de la Figura 3 tiene un transmisor de infrarrojos que se ha programado para transmitir una palabra que es un código secreto. Si el co-procesador 103 recibe la palabra en código a través de su bloque de entrada de órdenes 308, detiene el incremento (o la disminución) del valor del registro de vigilancia en el bloque 310 o inhabilita la emisión de las señales de reinicio y de en espera desde los bloques 306 y 307 con independencia del valor del registro de vigilancia. Estas funciones se realizan de nuevo del modo más ventajoso a través de conjuntos correspondientes de instrucciones en el programa ejecutado por el co-procesador. A través de una programación similar, el co-procesador también puede disponerse de modo que libere una señal ya emitida de reinicio y/o de en espera como respuesta a una cierta orden secreta o palabra en código.

Con el fin de mantener la(s) palabra(s) en código en secreto y de prevenir el acceso no autorizado al co-procesador, normalmente se requiere que el co-procesador no tenga una interfaz de depuración propia y/o que el reconocimiento de la(s) palabra(s) en código se base en el hardware del co-procesador en lugar de en el software.

La disposición del acoplamiento de la Figura 3 se generaliza fácilmente para implementar el principio de las Figuras 2a a 2c: la interfaz I^2C ahora se usa para transportar la

señal de alarma y se puede ignorar el registro de vigilancia 310. Cuando una señal de alarma se recibe en el co-procesador, fija el procesador principal en el modo en espera cortando la línea de alimentación principal con el conmutador 304. La recuperación tiene lugar después de que la señal de alarma ya no está activa. No obstante, el principio descrito previamente se considera más ventajoso porque también se introduce la condición de en espera si el procesador deja de responder por alguna otra razón.

La Figura 4 ilustra un ejemplo de dispositivo electrónico en el que se puede aplicar la invención. El dispositivo es un terminal multimedia 104 en el que un receptor de radiofrecuencia 402 está dispuesto para recibir una (serie de) señal(es) de radiofrecuencia y convertirla(s) en una (serie de) corriente(s) de banda base. Se unas un bloque procesador de señales 403 para convertir adicionalmente la(s) corriente(s) de banda base en señales de salida de vídeo, audio y datos. Existe una interfaz de depuración al bloque de procesamiento de la señal para realizar las funciones de depuración típicas. Un bloque de control de la alimentación 404 es responsable de proporcionar la tensión y las señales de reinicio a los otros bloques. Si la disposición de acoplamiento de la Figura 3 se realiza como parte de ese dispositivo de ejemplo, el bloque de control de la alimentación 404 aloja el co-procesador y los bloques receptores de IR y el bloque de procesamiento de señales está constituido principalmente por el procesador 101.

Cabe destacar que la invención no requiere que el procesador principal y el co-procesador sean entidades físicamente separadas. Pueden estar realizadas dentro de un único chip o en chip paralelos en un módulo denominado multi-chip. De hecho, la continua miniaturización de la electrónica de procesamiento de señales ciertamente exige potenciar de forma continua las proporciones de integración, por lo que una aplicación muy plausible de la invención es integrar el procesador y las funciones de vigilancia en una única entidad física.

Asimismo son posibles otras modificaciones de las formas de realización de la invención previamente divulgadas sin desviarse del alcance de las reivindicaciones adjuntas. Por ejemplo, en una forma de realización de la invención muy sencilla, el fabricante de un dispositivo electrónico puede desear que la interfaz de depuración no esté disponible para usar en absoluto en un dispositivo completamente ensamblado, mientras que el receptor de IR u otra entrada de orden para las órdenes de liberación autorizadas pueden quedarse fuera de las formas de realización de la invención descritas. Los autores también han hecho referencia a un apagado completo del procesador como respuesta al uso detectado de una interfaz protegida; es posible inhabilitar únicamente una parte de las operaciones del procesador y dejar, por ejemplo, refrescando la memoria interna y otras funciones operativas de este tipo que mantienen la facilidad del funcionamiento del procesador.

REIVINDICACIONES

1. Un procedimiento para prevenir el uso no autorizado de una cierta interfaz protegida (102) en y hacia un procesador (101, 101'), **que se caracteriza porque** comprende:

a1) generar dentro del procesador (101, 101') una indicación (NO PAT, ALARM) de intento de uso de la interfaz protegida,

a2) Transmitir la indicación generada a otro componente (103, 103') y

b) como respuesta a dicha indicación, detectar dentro de dicho otro componente (103, 103') si se ha recibido una palabra secreta en código (LIBERAR) a una orden de entrada de ese otro componente, y si no se ha recibido una palabra secreta en código, generando una señal de inhabilitación dentro de ese otro componente y usando dicha señal de inhabilitación para inhabilitar (INHABILITAR) al menos una gran parte de las operaciones del procesador.

2. Un procedimiento de acuerdo con la reivindicación 1, **que se caracteriza porque** comprende antes a1) transmisión regular de una corriente de señales (PAT) desde el procesador a este otro componente y a1) y a2) corresponden a retrasar o detener la generación y la transmisión de dicha corriente de señales (NO PAT).

3. Un procedimiento de acuerdo con la reivindicación 1, **que se caracteriza porque** dicha inhabilitación en b) corresponde a cambiar el procesador a un estado en espera.

4. Un procedimiento de acuerdo con la reivindicación 3, **que se caracteriza porque** dicho cambio se consigue desconectando la energía de operación de una gran parte del procesador.

5. Un procedimiento de acuerdo con la reivindicación 1, **que se caracteriza porque** a1) y a2) corresponden a fijar una señal de alarma específica (ALARMA) en un estado de activo.

6. Un procedimiento de acuerdo con la reivindicación 1, **que se caracteriza porque** comprende después de b): Detectar dentro de ese otro componente si se ha recibido una palabra secreta en código (LIBERAR) a una entrada de orden de ese otro componente y si se a recibido una palabra secreta en código (LIBERAR), rehabilitando la parte inhabilitada de la operación del procesador.

7. Un dispositivo que comprende

- un procesador (101, 101') y
- dentro del procesador una primera interfaz (102) al procesador, y una segunda interfaz (302), **que se caracteriza por** prevenir el uso no autorizado de la primera interfaz que el dispositivo electrónico comprende
- otro componente (103) acoplado a dicha segunda interfaz,
- dentro del procesador (101, 101 '), medios para generar una indicación (NO PAT, ALARMA) de intento de uso de la primera interfaz y medios para transmitir dicha indicación a ese otro componente mediante dicha segunda interfaz (302),
- dentro de este otro componente, medios (310, 307) para generar, sobre la base de una indicación recibida, una señal de inhabilitación para inhabilitar (INHABILITAR) al menos una parte de la operación del procesador, y
- dentro de este otro componente, una entrada de órdenes y medios para detectar si se ha recibido una palabra secreta en código (308) a dicha entrada de órdenes, y medios para inhabilitar la emisión de dicha señal de inhabilitación al procesador como respuesta a la detección de que dicha palabra secreta en código no se ha recibido.

8. Un dispositivo de acuerdo con la reivindicación 7, **que se caracteriza porque** comprende un conmutador (304), que responde a dicha señal de inhabilitación, para apagar de forma selectiva la energía de operación de una parte del procesador.

9. Un dispositivo de acuerdo con la reivindicación 7, **que se caracteriza porque** comprende

- dentro de este otro componente un registro de vigilancia (310) y medios para cambiar con regularidad el valor de dicho registro de vigilancia de forma monótona en una dirección determinada,
- dentro del procesador medios (302) para reiniciar con regularidad dicho registro de vigilancia a un valor constante determinado a través de dicha segunda interfaz,
- dentro de ese otro componente, medios para comparar con regularidad el valor de dicho registro de vigilancia frente a cierto valor limitante que reside en dicha dirección determinada a partir de dicho valor constante,

- dentro de este otro componente, medios para generar, como respuesta a una igualdad detectada o que supera el valor del registro de vigilancia al valor limitante, dicha señal de inhabilitación (307).

10. Un dispositivo de acuerdo con la reivindicación 7, **que se caracteriza porque** dichos medios para detectar si se ha recibido una palabra secreta en código están acoplados a un receptor inalámbrico (309) para recibir órdenes por una conexión inalámbrica.

11. Un dispositivo de acuerdo con la reivindicación 7, **que se caracteriza porque** ese otro componente (103) es un co-procesador responsable de proporcionar las señales de tensión y reinicio a las otras partes del dispositivo.

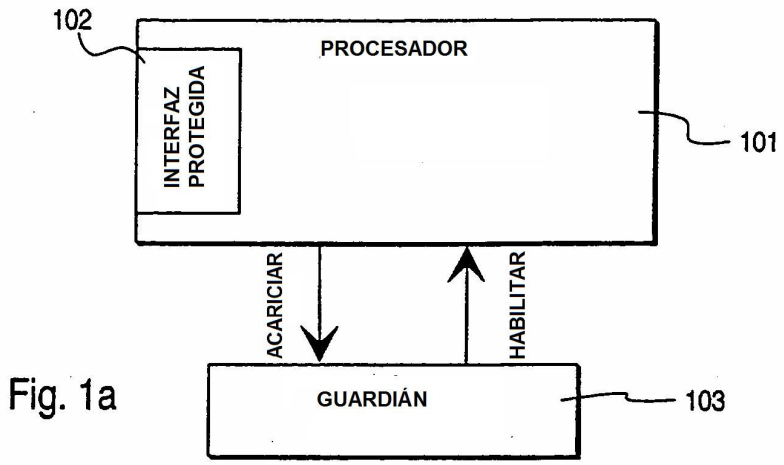

Fig. 1a

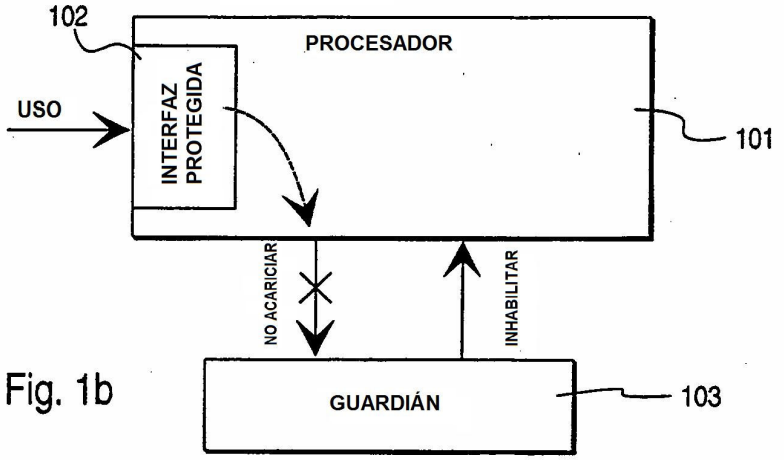

Fig. 1b

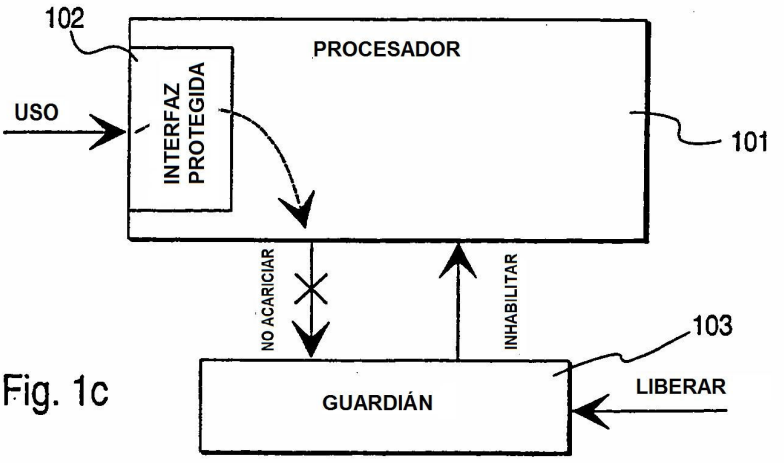

Fig. 1c

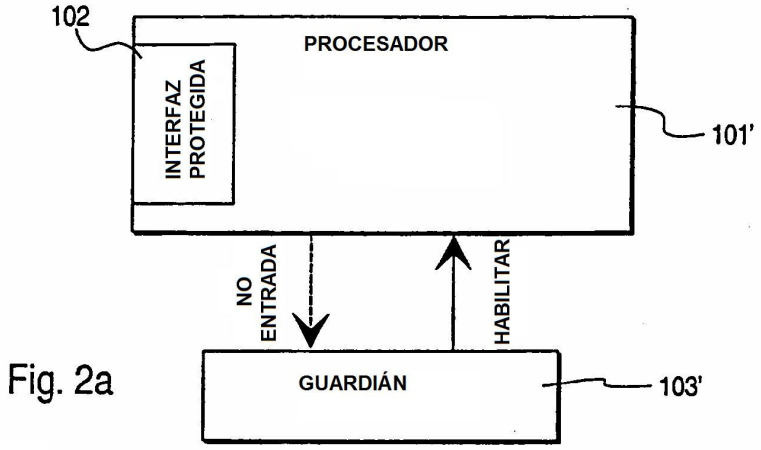

Fig. 2a

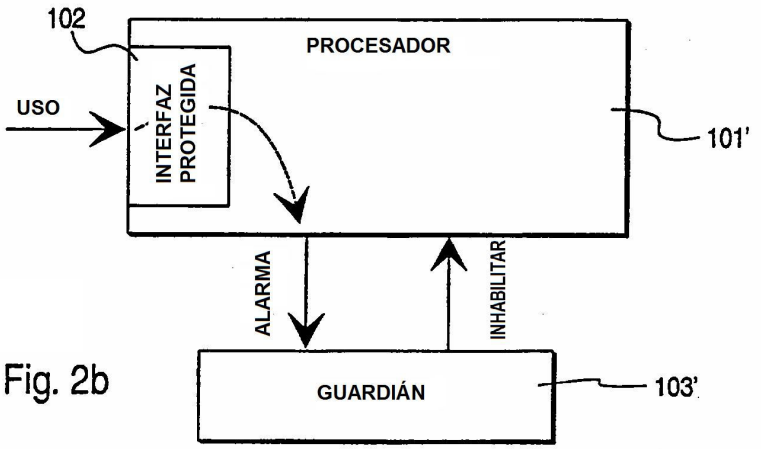

Fig. 2b

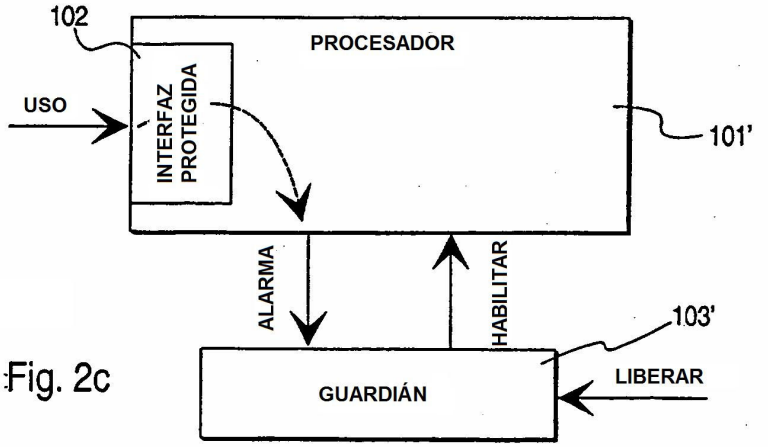

Fig. 2c

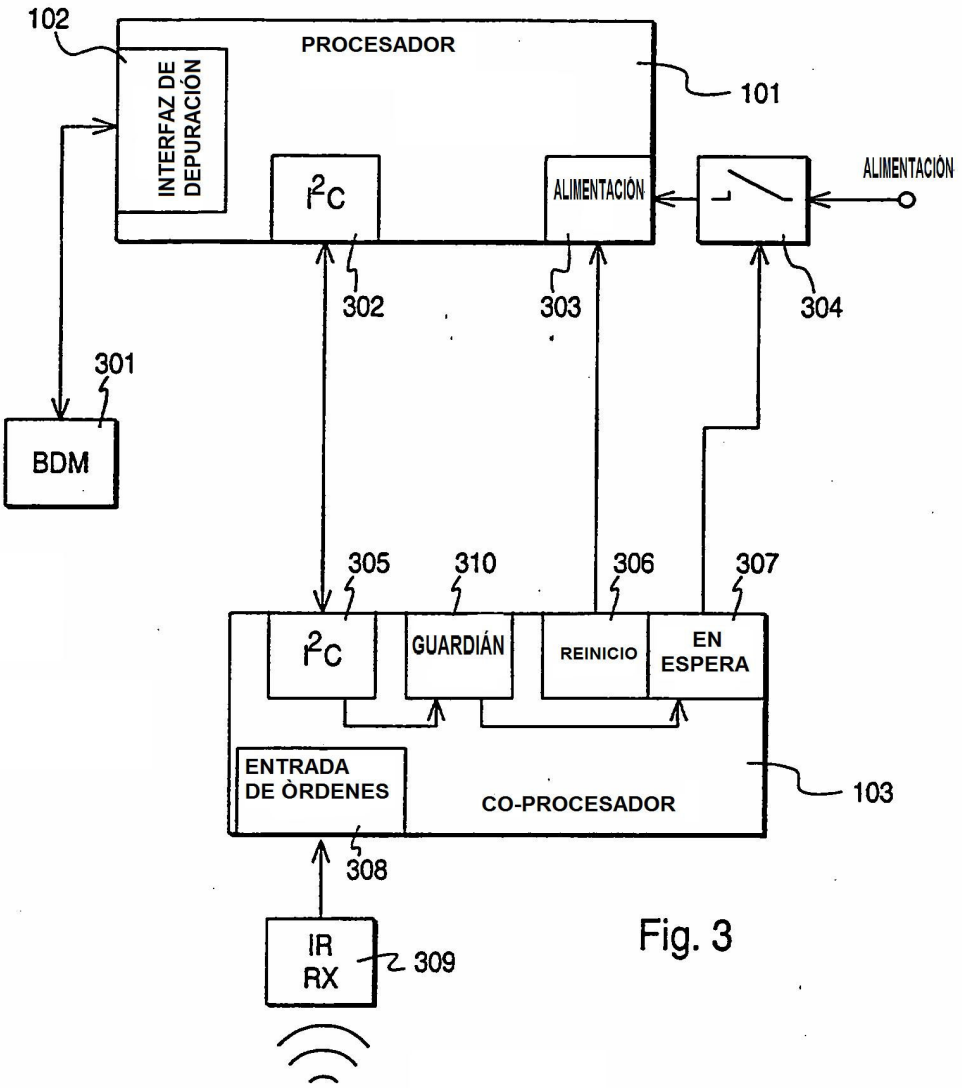
102
PROCESADOR
101
INTERFAZ DE DEPURACIÓN
I²C
ALIMENTACIÓN
ALIMENTACIÓN
302
303
304
301
BDM
305
310
306
307
I²C
GUARDIÁN
REINICIO
EN ESPERA
ENTRADA DE ÒRDENES
CO-PROCESADOR
103
308
IR RX
309

Fig. 3

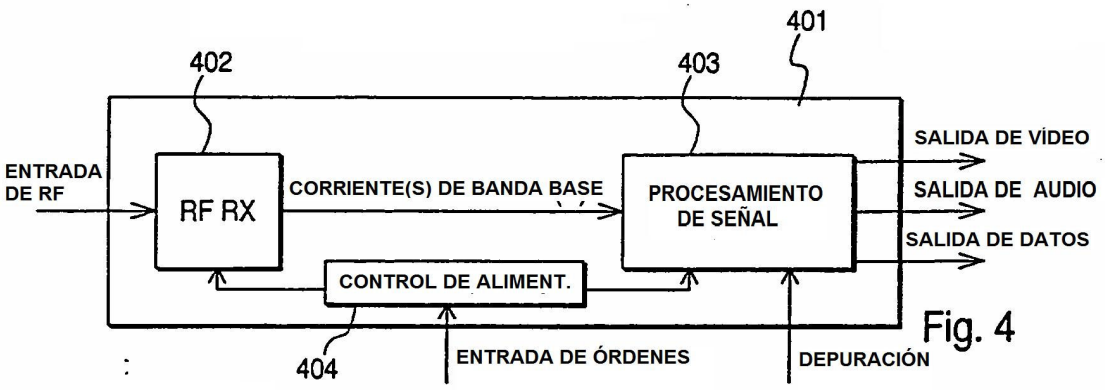
401
402
403
ENTRADA DE RF
RF RX
CORRIENTE(S) DE BANDA BASE
PROCESAMIENTO DE SEÑAL
SALIDA DE VÍDEO
SALIDA DE AUDIO
SALIDA DE DATOS
CONTROL DE ALIMENT.
404
ENTRADA DE ÓRDENES
DEPURACIÓN

Fig. 4