(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 345 115**

(51) Int. Cl.:
G06F 11/20 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06126461 .0**
(96) Fecha de presentación : **19.12.2006**
(97) Número de publicación de la solicitud: **1936502**
(97) Fecha de publicación de la solicitud: **25.06.2008**

(54) Título: **Un procedimiento para asegurar la función de salvaguardar en un sistema eléctrico de un vehículo, y sistema eléctrico correspondiente.**

(45) Fecha de publicación de la mención BOPI:
15.09.2010

(45) Fecha de la publicación del folleto de la patente:
15.09.2010

(73) Titular/es: **SAAB AB.**
581 88 Linköping, SE

(72) Inventor/es: **Jansson, Tomas y**
Holmlund, Lars

(74) Agente: **Carpintero López, Mario**

DESCRIPCIÓN

Un procedimiento para asegurar la función de salvaguardar en un sistema electrónico de un vehículo, y sistema eléctrico correspondiente.

Campo de la invención

La presente invención se refiere a un procedimiento para asegurar la función de salvaguarda en un sistema eléctrico, y a un sistema eléctrico para un vehículo. Específicamente, la presente invención se refiere a un sistema eléctrico redundante con una función de salvaguarda de acuerdo con el preámbulo de las reivindicaciones 1 y 9 independientes anexas.

Antecedentes de la invención

En el campo de la aviónica, siempre ha sido de alta prioridad y de gran interés centrarse en la fiabilidad de los sistemas eléctricos. Por supuesto, es de gran importancia que cada sistema sea fiable en un vehículo aéreo con el fin de obtener la función de vuelo apropiadamente. Genéricamente, la fiabilidad ha sido resuelta mediante la provisión de sistemas de salvaguarda respecto a los sistemas principales, mientras que el sistema de salvaguarda se hace cargo del control cuando se establece que un sistema principal está fuera de funcionamiento. En algunos de los sistemas eléctricos de un vehículo aéreo, tal como los sistemas de control de vuelo y similares, es importante que no se introduzca ningún retardo durante la transferencia de control, ejecutándose la salvaguarda generalmente en tales sistemas en paralelo con el sistema principal. Esto significa que el sistema de salvaguarda es sustancialmente una réplica del sistema principal, tanto en hardware como en software, y que el sistema de salvaguarda debe actualizar los parámetros del sistema de la misma manera que el sistema principal, lo que se traduce en altos costes debido a la duplicación del hardware y similar. La fiabilidad es, por lo tanto, un parámetro que se encuentra bajo continuo desarrollo con el fin de resolver el problema y mantener los costes al mínimo. Se debe entender que el coste de la duplicación del hardware y similar, es muy alto y es algo que debe ser evitado, si es posible, durante las nuevas construcciones así como durante el desarrollo de los sistemas ya existentes.

En los sistemas actuales, la fiabilidad se resuelve ya sea proporcionando componentes de muy alta fiabilidad o ya sea con hardware redundante, como se ha definido anteriormente, y la duplicación de la funcionalidad con diferentes programas. Los sistemas redundantes, no solo generan altos costes, sino que también introducen un factor que afecta negativamente a la tasa de fallos, puesto que se introducen nuevos componentes que también pueden fallar. También, resulta muy costoso crear soluciones de software para aplicaciones especialmente adaptadas, en las que cada programa de software de aplicación está adaptado con rutinas y procedimientos que monitorizan otro software de aplicación. Resulta por lo tanto deseable en la industria de la aviónica proporcionar una alta fiabilidad de las funciones del sistema a bajo coste y bajo volumen, con el fin de evitar llenar el aeroplano con equipamiento de salvaguarda. Es además deseable proporcionar funciones de fiabilidad en un sistema que genere un bajo incremento de peso con el fin de que se mantenga el consumo de combustible tan bajo como sea posible, que la menor carga útil genere menos peso total, lo que da como resultado que el aeroplano consuma menos combustible, y que el esfuerzo sobre el cuerpo del aeroplano se reduzca.

Se conoce el hecho de conmutar de una unidad de hardware a otra unidad de hardware en un sistema eléctrico cuando una unidad de hardware falla, con el fin de obtener una alta fiabilidad del sistema. El documento de Patente GB 2.410.573 se refiere a un sistema redundante en el que dos estaciones de aplicación similares conmutan información; el estado de la primera aplicación es transferido a la segunda aplicación a intervalos regulares, con el fin de transferir el control a la segunda aplicación cuando la primera aplicación falla. La estación de aplicación que ejecuta la salvaguarda constantemente, comprende un hardware y un software que incrementan los costes, el peso y el volumen, con el fin de ser introducidos en un sistema eléctrico de un vehículo.

El documento EP0760503 muestra un sistema de servidor de red controlador de averías, en el que múltiples servidores actúan simultáneamente como servidores de salvaguarda cada uno con los otros, incluso mientras están proporcionando sus propios servicios de servidor al sistema.

El documento US 4 590 554 describe un sistema de ordenador en paralelo que tiene un procesador de tarea primaria, un segundo procesador de tarea primaria, y un procesador de tarea secundaria que actúa como salvaguarda para el segundo procesador de tarea primaria.

En vista de lo anterior, un objeto consiste en proporcionar un sistema eléctrico redundante, que no afecte a los costes, al peso y al volumen tanto como los sistemas convencionales.

Sumario de la invención

Con el fin de lograr el citado objeto de la invención se proporciona un sistema y un procedimiento de acuerdo con las reivindicaciones 1 y 9 independientes anexas.

La presente invención divulga un sistema eléctrico para un vehículo que comprende un portador de información digital para transferencia de datos digitales; un primer dispositivo (1) de computación dispuesto para ejecutar un primer

software de aplicación instalado en el primer dispositivo de computación; y un segundo dispositivo de computación dispuesto para ejecutar un segundo software de aplicación, diferente de dicho primer software de aplicación, instalado en el segundo dispositivo de computación. El segundo dispositivo de computación comprende además un software de aplicación de salvaguarda instalado en el segundo dispositivo de computación, idéntico al primer software de aplicación, en el que el segundo dispositivo de computación está configurado para iniciar una ejecución del software de aplicación de salvaguarda instalado, cuando se produce un error en el primer dispositivo de computación, en paralelo con la ejecución del segundo software de aplicación. El primer software de aplicación, el segundo software de aplicación y el software de aplicación de salvaguarda, están dispuestos de modo que se ejecutan en partes de memoria separadas.

El sistema eléctrico puede incluir además el segundo dispositivo de computación que comprende un primer programa de instrucción, en el que el primer programa de instrucción está dispuesto para ejecutar la segunda aplicación en el segundo dispositivo de computación; y un segundo programa de instrucción, en el que el segundo programa de instrucción está dispuesto para ejecutar la segunda aplicación y la aplicación de salvaguarda.

Además, el sistema eléctrico de acuerdo con la invención incluye una configuración, en la que el segundo dispositivo de computación está dispuesto de modo que ejecuta el primer programa de instrucción cuando el sistema eléctrico está operando de manera normal, es decir, cuando el primer software de aplicación se está ejecutando apropiadamente en el primer dispositivo de computación, y el segundo dispositivo de computación está dispuesto para ejecutar el segundo programa de instrucción cuando el sistema eléctrico está operando en modo de salvaguarda, es decir, cuando el primer software de aplicación ha fallado en el sistema.

Adicionalmente, el sistema eléctrico puede divulgar además que el segundo dispositivo de computación esté configurado para activar un proceso de reprogramación en un sistema operativo del segundo dispositivo de computación, dispuesto para conmutar desde el primer programa de instrucción al segundo programa de instrucción cuando se detecta un error en el primer dispositivo de computación.

El sistema eléctrico conforme a la invención puede divulgar además que el segundo dispositivo de computación esté dispuesto con una función de monitorización configurada para activar el proceso de reprogramación en el segundo dispositivo de computación.

La invención puede comprender además un segundo dispositivo de computación que esté dispuesto con una función de monitorización para monitorizar al menos el primer dispositivo de computación.

La invención se refiere además a un sistema eléctrico en el que el primer dispositivo de computación está enviando continuamente la condición de ejecución del primer software de aplicación, y en el que la función de monitorización está configurada para monitorizar datos enviados por el bus de datos, y cuando no se detecta una condición de ejecución esperada procedente del primer dispositivo de computación en el bus de sistema, la función de monitorización está configurada para instruir al segundo dispositivo de computación para que inicie la ejecución del tercer software de aplicación.

Adicionalmente, el sistema eléctrico de acuerdo con la presente invención puede ser un sistema no-crítico que sea no-sensible a retardos.

La invención divulga además un procedimiento para asegurar la función de salvaguarda en un sistema eléctrico de un vehículo que comprende un portador de información digital para transferencia de datos digitales; un primer dispositivo de computación dispuesto para ejecutar un primer software de aplicación instalado en el primer dispositivo de computación, y un segundo dispositivo de computación dispuesto para ejecutar un segundo software de aplicación instalado en el segundo dispositivo de computación, diferente del citado primer software de aplicación, y un tercer software de aplicación de salvaguarda, idéntico al primer software de aplicación. El procedimiento comprende las etapas de: determinar que se ha producido un error en el primer dispositivo de computación, e iniciar la ejecución de la aplicación de salvaguarda en una primera parte de memoria del segundo dispositivo de computación en paralelo, mientras se ejecuta de forma continua el segundo software de aplicación en una segunda parte de la memoria separada de la primera parte de memoria.

El proceso de iniciación del procedimiento puede comprender además la etapa de conmutar desde un programa de instrucción original que se ejecuta en el segundo dispositivo de computación, a un segundo programa de instrucción.

El procedimiento puede comprender además la etapa de monitorizar el portador de información digital utilizando una función de monitorización que se ejecuta en el segundo dispositivo de computación, realizando dicha función de monitorización también la citada etapa de determinación.

Además, la invención divulga un procedimiento en el que la función de monitorización puede monitorizar además las condiciones de ejecución del primer software de aplicación enviado en la información digital desde el primer dispositivo.

El procedimiento de acuerdo con la presente invención puede divulgar además una realización en la que la función de monitorización determina además que se ha producido un error en el primer dispositivo de computación cuando no se monitoriza ninguna condición de ejecución del primer software de aplicación en el portador de información digital.

El procedimiento puede comprender además, después de dicha etapa de iniciación, las etapas de: determinar que el primer software de aplicación está a nivel alto y ejecutándose en el primer dispositivo de computación, y conmutar de nuevo al estado de ejecución original que realiza la primera aplicación en el proceso cuando se determina que el primer software de aplicación está a nivel alto y ejecutándose de nuevo en el primer dispositivo de computación.

Utilizando estructuras de hardware ya existentes y utilizando el exceso de capacidad que existe en el hardware existente, se puede omitir la introducción de hardware duplicado. La presente invención es especialmente adecuada para sistemas eléctricos críticos de no-retardo, tal como los sistemas de comunicaciones, sistemas de contra-medición, sistemas de navegación, sistemas de comunicación interna, sistemas de presentación y similares, en los que se acepta un retardo de poca importancia en la función de mantenimiento cuando se produce un fallo. En estos sistemas, el coste de introducir duplicación de hardware es extremadamente alto, mientras que la fiabilidad puede, de hecho, descender en cuanto a prioridad en estos sistemas, dando como resultado la carencia de una función de salvaguarda.

La presente invención da como resultado una fiabilidad incrementada, alcanzada con un mínimo de incremento de costes y sin incremento de volumen ni peso.

Breve descripción de los dibujos

La invención, junto con otros objetivos y ventajas de la misma, puede ser mejor comprendida mediante referencia a la descripción que sigue tomada junto con los dibujos que se acompañan, en los que:

Las Figuras 1A-1B ilustran una vista general esquemática de un proceso de una realización de la presente invención;

las Figuras 2A-2B ilustran una vista general similar de un proceso de una realización diferente de la presente invención;

la Figura 3 muestra un diagrama de flujo esquemático de la conmutación a una función de salvaguarda de acuerdo con una realización de la presente invención;

las Figuras 4A-4B ilustran un proceso de una realización de la presente invención en cada dispositivo de computación, y

la Figura 5 ilustra un proceso de una realización de la presente invención cuando se lleva a cabo un reinicio con éxito.

Descripción detallada de realizaciones de la invención

Las realizaciones de la presente invención van a ser descritas de manera más completa en lo que sigue, con referencia a los dibujos que se acompañan, en los que se muestran realizaciones de la presente invención. Esta invención puede ser, sin embargo, materializada de muchas formas diferentes, y no deben entenderse como limitada a las realizaciones que aquí se exponen. Más bien, estas realizaciones se proporcionan de modo que esta descripción sea minuciosa y completa, y transmitirá de manera completa el alcance de la invención a los expertos en la materia. Los mismos números se refieren a iguales elementos a través de la misma.

La terminología aquí utilizada es a efectos de descripción de realizaciones particulares únicamente, y no se pretende que limite la invención. Según se utiliza aquí, las formas en singular “un”, “una” y “el”, “la”, se pretende que incluyan también las formas en plural, a menos que el contexto indique claramente lo contrario. Se comprenderá además que los términos “comprende”, “comprendiendo”, “incluye” y/o “incluyendo”, cuando se utilicen aquí, especifican la presencia de características constatadas, entidades completas, etapas, operaciones, elementos y/o componentes, pero no excluyen la presencia o la adición de una o más de otras características, entidades completas, etapas, operaciones, elementos, componentes y/o grupos de los mismos.

A menos que se defina de otro modo, todos los términos (incluyendo los términos técnicos y científicos), que aquí se utilizan, tienen el mismo significado que el entendido normalmente por un experto en la materia a la que pertenece esta invención. Se comprenderá además que los términos aquí utilizados deben ser interpretados como que tienen un significado que es compatible con su significado en el contexto de esta descripción y de la técnica relevante, y no deberán ser interpretados en sentido idealizado o excesivamente formal, a menos que se definan expresamente de esa manera.

La presente invención se describe en lo que sigue con referencia a diagramas de bloques y/o a ilustraciones de diagramas de flujo de procedimientos y/o aparatos (sistemas) de acuerdo con realizaciones de la invención. Se comprende que diversos bloques de los diagramas de bloques y/o ilustraciones de diagramas de flujo, y combinaciones de bloques en los diagramas de bloques y/o ilustraciones de diagramas de flujo, pueden ser implementados mediante instrucciones de programa de ordenador. Estas instrucciones de programa de ordenador pueden ser proporcionadas a un ordenador de propósito general, un ordenador de propósito especial, y/u otro aparato programable de procesamiento de datos para producir una máquina, de tal modo que las instrucciones, que se ejecuten por medio del procesador del ordenador y/o del aparato programable de procesamiento de datos, crean medios para im-

plementar las funciones/actos especificados en los diagramas de bloques y/o en el bloque o bloques del diagrama de flujo.

Estas instrucciones de programa de ordenador pueden estar también almacenadas en una memoria legible con ordenador que puede dirigir un ordenador u otro aparato programable de procesamiento de datos para que funcione de una manera particular, de tal modo que las instrucciones almacenadas en la memoria legible con ordenador producen un artículo de fabricación que incluye instrucciones que implementan la función/ acto especificado en los diagramas de bloques y/o en el bloque o bloques del diagrama de flujo.

Las instrucciones de programa de ordenador pueden estar cargadas también en un ordenador u otro aparato programable de procesamiento de datos de modo que provoquen que una serie de etapas operativas se lleven a cabo en el ordenador u otro aparato programable para producir un proceso implementado por ordenador, de tal modo que las instrucciones que se ejecuten en el ordenador u otro aparato programable proporcionen etapas para implementar las funciones/actos especificados en los diagramas de bloques y/o en el bloque o bloques de diagrama de flujo.

El desarrollo técnico de sistemas de aviónica ha conducido a un incremento en el uso de dispositivos de ordenador estandarizados en los que se realizan diferentes tipos de funciones como software de aplicación. Los dispositivos de ordenador comunican entre sí mediante enlaces de datos, por ejemplo buses de datos alámbricos o inalámbricos. En lo que sigue, se va a describir un procedimiento sobre cómo lograr una fiabilidad incrementada en un sistema de aviónica sin añadir hardware o software extra. La solución utiliza la capacidad, por ejemplo procesamiento y memoria y similar, de un dispositivo de ordenador ya existente. En sistemas de aviónica, es importante aislar por completo las porciones de un sistema entre sí, por ejemplo el sistema de control de cabina del piloto debe ser predecible y conocido en todo momento. Esto se consigue utilizando un sistema operativo de partición. Un sistema operativo de partición divide la memoria y el tiempo de CPU entre particiones asignadas estáticamente de una manera fija, de modo que cada partición posea una cierta cantidad de memoria y de tiempo de CPU asignada a la misma, que no puede ser incrementada ni reducida.

Las Figuras 1A y 1B ilustran esquemáticamente un proceso para hacerse cargo de la función de un software de aplicación en caso de que falle la aplicación principal, de acuerdo con una realización de la presente invención. En el ejemplo ilustrado, un primer dispositivo 1 de computación y un segundo dispositivo 2 de computación están conectados a un bus 3 de datos. El bus 3 de datos puede ser una LAN que trabaje con protocolos Ethernet o similares, pero podría ser también un enlace de comunicación inalámbrica. Un primer software P1 de aplicación, está dispuesto en el primer dispositivo 1 de computación, y una salvaguarda, señalada como P1' se encuentra almacenada en el segundo dispositivo 2 de computación. El primer software P1 de aplicación está activo en la Figura 1A, es decir, a nivel alto y ejecutándose, mientras que el primer software P1' de aplicación del segundo dispositivo de computación está pasivo, es decir, a nivel bajo y en estado de "desconexión".

En el segundo ordenador, se ha dispuesto un segundo software P2 de aplicación, diferente del primer software P1. Como ejemplo, el primer software P1 de aplicación puede ser una aplicación que presente datos de vuelo tal como la velocidad de viento que se está utilizando normalmente, y el segundo software de aplicación puede ser una aplicación que presente una alimentación de vídeo procedente de una cámara externa, tal como una cámara de tren de aterrizaje. En el segundo dispositivo 2 de computación, la función 5 de monitorización ha sido instalada en un sistema operativo 7 (SO) particionado del segundo dispositivo 2 de computación, y la función de monitorización realiza la monitorización de todos los demás dispositivos de computación, en la figura el primer dispositivo 1 de computación, por ejemplo la función 5 de monitorización puede monitorizar todos los datos del bus 3 que llegan desde el primer software P1 de aplicación a través del sistema operativo 6 de partición del primer dispositivo de computación. La función de monitorización va a ser descrita con mayor detalle en lo que sigue. Cuando la función 5 de monitorización del segundo dispositivo 2 de monitorización detecta un error en el primer dispositivo 1 de monitorización, que indica que la primera aplicación P1 no está operando, el sistema operativo 7 de partición del segundo dispositivo 2 de computación inicia un esquema de ejecución alternativo. Se debe apreciar que en la realización ilustrada, se utiliza un sistema operativo de partición, sin embargo, en un entorno diferente, el sistema operativo puede ser un sistema operativo diferente tal como un sistema de operación de proceso o similar. Sin embargo, se prefiere el sistema particionado que divide la memoria y el tiempo de CPU entre particiones asignadas estáticamente de una manera fija, con el fin de conseguir un margen de fiabilidad seguro para el sistema.

En cada uno de los sistemas de partición ilustrados, se ha mostrado un BSP (paquete de soporte de a bordo) 8, 9. El BSP 8, 9 contiene rutinas para inicializar y controlar el hardware en el sistema de interés. El BSP está capacitado para procesar múltiples aplicaciones de forma simultánea, y sus principales responsabilidades son:

- servir de interfaz con el software de inicio y parada,

- establecer un mapa virtual de direcciones para E/S del ordenador de a bordo,

- servir de interfaz con un controlador de interrupciones,

- proporcionar rutinas de servicio por defecto, para interrupciones de señalización de error,

- servir de interfaz con un controlador de PCI, y

- servir de interfaz con un tiempo de sistema (temporizador de variación).

Se debe comprender además que los dispositivos de computación comprenden hardware adicional indicado como hardware en las Figuras.

El esquema de ejecución alternativa del segundo dispositivo 2 de computación incluye el software P1' de aplicación idéntico, así como el software P2 de aplicación, y se utiliza a efectos de iniciar la aplicación idéntica en el segundo dispositivo 2 de computación para ejecutar, por ejemplo, la aplicación que está presentando la velocidad de viento del vuelo. Con ello, se omite la primera aplicación P1 que se ejecuta en el primer dispositivo 1 de computación del proceso de ejecución del sistema. Este proceso de reprogramación, cambio de programa de instrucción, está predefinido en el segundo dispositivo 2 de computación. El primer software P1' de aplicación que se ejecuta en el segundo dispositivo 2 de computación, es activado por este proceso de reprogramación, y el software P1' de aplicación asume el control como aplicación de partición activa, y el software P1 de aplicación, previamente activo, se sitúa mediante el BSP en un estado bajo, como se ha ilustrado en la Figura 1B. Se debe entender aquí que el BSP del primer dispositivo de computación puede reiniciar la aplicación. Si el primer software P1 de aplicación, después de este reinicio, funciona apropiadamente, el segundo dispositivo 2 de computación registra que la aplicación está a nivel alto y se ejecuta de nuevo y cambia a su esquema de ejecución original, dando como resultado que el primer dispositivo de computación sea implementado de nuevo en el sistema. En una realización alternativa, el sistema como tal falla, y el primer dispositivo de computación queda por tanto inactivo.

En las Figuras 2A-2B se ha ilustrado un proceso similar. Sin embargo, en las Figuras 2A, 2B, el sistema eléctrico está expandido por introducción de una aplicación de salvaguarda al segundo software P2 de aplicación, es decir, se ha introducido un software P2' de aplicación idéntico en el primer dispositivo 1 de computación. En la Figura 2A, el primer software P1 de aplicación está ejecutándose de un modo normal en el primer dispositivo 1 de computación y en el segundo software P2 de aplicación está ejecutándose de un modo normal en el segundo dispositivo 2 de computación. En la Figura 2B, fallan tanto el primer software P1 de aplicación que se está ejecutando en el primer dispositivo 1 de computación, como el segundo software P2 de aplicación que se está ejecutando en el segundo dispositivo 2 de computación, y el primer software P1' de aplicación que se ejecuta en el segundo dispositivo 2 de computación y el segundo software P2' de aplicación que se ejecuta en el primer dispositivo 1 de computación, son activados en el sistema. Esto se hace mediante procesos de reprogramación predefinidos, es decir, haciendo que se ejecuten esquemas alternativos de ejecución de instrucción tanto en el primer dispositivo de computación como en el segundo dispositivo de computación. Según se ha ilustrado en las Figuras 2A-2B, la primera unidad de computación posee una función 4 de monitorización instalada en la misma a efectos de detectar que el segundo software P2 de aplicación ha fallado en el segundo dispositivo 2 de computación. El proceso ilustrado en las Figuras 2A y 2B es, obviamente, posible solamente si las aplicaciones P1 y P2 caen internamente en el dispositivo de computación y sin que se deba a fallo de hardware del dispositivo de computación. Se debe apreciar aquí que el número de aplicaciones de partición que se ejecuta en un dispositivo de computación puede ser mucho más alto que en el ejemplo ilustrado. Por ejemplo, en el segundo dispositivo de computación se pueden instalar muchos programas alternativos de software de aplicación, P1', P3', P4', y así sucesivamente. El número está limitado únicamente por el procesador y por la capacidad de memoria del segundo dispositivo de computación. Instalando la misma aplicación dos ves, es decir, en dos dispositivos de computación separados, se logra un grado de fiabilidad más alto sin necesidad de desarrollar dos aplicaciones diferentes. Además, se utiliza el exceso de capacidad de memoria y de computación que existe, puesto que los dispositivos de computación que están estandarizados hoy en día y que se utilizan generalmente, tienen grandes capacidades de memoria y de computación.

Según se ha expuesto en lo que antecede, una realización de la presente invención comprende una función 5 de monitorización, la cual va a ser descrita ahora con referencia a las Figuras 1A-1B y a la Figura 4. La función 5 de monitorización tiene solamente una tarea, que consiste en monitorizar las condiciones de estado de otras aplicaciones en otros dispositivos de computación conectados al bus 3 de sistema. Con el fin de definir el número de programas de instrucción, mencionados en lo que antecede como esquemas de ejecución, se ha diseñado una tabla en cada dispositivo de computación, véase la tabla 1. Según se muestra en la tabla 1, el número de programas de instrucción está basado en el número de aplicaciones de salvaguarda instaladas en el dispositivo de computación. La tabla esquemática ha sido ilustrada en lo que sigue con referencia a las realizaciones de las Figuras 1A-1B. En un ejemplo, en el que un dispositivo de computación comprende dos aplicaciones de salvaguarda (no representadas), la tabla podría divulgar un dispositivo de computación que comprende cuatro programas de instrucción, un primer programa de instrucción (sin aplicaciones de salvaguarda), un segundo programa de instrucción (primera aplicación de salvaguarda), un tercer programa de instrucción (segunda aplicación de salvaguarda) y un cuarto programa de instrucción (primera y segunda aplicaciones de salvaguarda). Cada programa de instrucción posee un criterio de activación que define cuándo conmutar programas de instrucción en cada dispositivo de computación. El dispositivo de computación cambia el programa de instrucción tan pronto como sea posible cuando se satisface/cumple el criterio de activación. Se debe apreciar aquí que el momento para iniciar un cambio de un programa de instrucción puede estar relacionado con la aplicación de salvaguarda.

TABLA 1

Dispositivo de computación	Núm. de aplicaciones	Programa de instrucción
1	1	1
2	2	2

La tabla 1 define el primer dispositivo de computación y el segundo dispositivo de computación en la columna de la izquierda. En la columna central se define que el primer dispositivo de computación tiene una aplicación P1 instalada y el segundo dispositivo de computación tiene dos aplicaciones P2, P1' instaladas. Finalmente, la columna de la derecha define que el primer dispositivo de computación actúa de acuerdo con un programa de instrucción original y el segundo dispositivo de computación actúa en modo normal de acuerdo con un primer programa de instrucción, pero en caso de fallo, el segundo dispositivo de computación dispone de un segundo programa de instrucción, es decir, el segundo dispositivo de computación posee dos programas de instrucción según se define en la columna de la derecha.

Haciendo referencia a la Figura 3, se muestra una vista general esquemática del proceso de ejecución de la función de salvaguarda de un sistema eléctrico. El sistema eléctrico es un sistema no crítico en tiempo real, tal como un sistema de comunicaciones, un sistema de comunicaciones internas, o similar. En el ejemplo ilustrado, el sistema eléctrico es un sistema de comunicaciones internas.

En la etapa 20, un programa de software de aplicación en un primer dispositivo de computación del sistema de comunicación interno, se está ejecutando en modo normal, es decir, el sistema está trabajando normalmente. En el ejemplo ilustrado, el software de aplicación es un programa de software de aplicación de vídeo para presentar una película a bordo.

En la etapa 22, la función de monitorización de un segundo dispositivo de computación detecta un error en la aplicación, tal como un valor esperado de una condición de ejecución sobre un bus de datos entre dos dispositivos de computación que no se ha detectado, o similar. Aquí se comprenderá que en una realización alternativa de la invención, la función de monitorización puede estar también al nivel más alto del sistema, tal como una función de monitorización global en un dispositivo de control central. En el segundo dispositivo de computación, se está ejecutando continuamente un segundo programa de software de aplicación, que es un programa de software de aplicación de comunicación interna que permite la comunicación entre la cabina del piloto y otras partes del aeroplano.

En la etapa 24, el segundo dispositivo de computación inicia un proceso de reprogramación que ha sido predeterminado por un operador previamente. El proceso de reprogramación cambia el esquema de ejecución del software de aplicación en el segundo dispositivo de computación, dando como resultado que el segundo dispositivo de computación inicie el programa de comunicación interna de salvaguarda instalado. La conmutación puede dar como resultado un retardo del sistema mediante un pequeño período de tiempo respecto al tiempo que necesita para iniciar la aplicación de salvaguarda. Este retardo se verá solamente como una perturbación de imagen en la película. Se debe apreciar aquí que el segundo programa de software de aplicación se está ejecutando continuamente durante el proceso de reprogramación.

Una realización del proceso de conmutación a una función de salvaguarda en un ejemplo de sistema como el mostrado en la Figura 1A, ha sido ilustrada en las Figuras 4A-4B, en las que la Figura 4A muestra las etapas llevadas a cabo en el primer dispositivo 1 de computación, y la Figura 4B muestra las etapas llevadas a cabo en el segundo dispositivo 2 de computación. Un primer software P1 de aplicación está instalado en una memoria del primer dispositivo 1 de computación, y un segundo software P2 de aplicación y un software P1' de aplicación de salvaguarda, que es idéntico al primer software P1 de aplicación del primer dispositivo 1 de computación, están instalados en una memoria del segundo dispositivo 2 de computación. Se debe apreciar aquí que las aplicaciones de memoria están separadas de acuerdo con un sistema de partición, es decir, los programas de software de aplicación no están influenciados cada uno por el otro debido al hecho de que los programas de software de aplicación se ejecutan en partes de memoria separadas. Las condiciones de ejecución de las aplicaciones de software se definen como sigue:

CD1.P1.Start_Up - La aplicación P1 se está iniciando, es decir, el primer dispositivo 1 de computación está iniciando la ejecución de la aplicación P1;

CD1.P1.Running_OK - La aplicación P1 se está ejecutando 1 satisfactoriamente en el primer dispositivo de computación;

CD2.P1'.Start_Up - La aplicación P1' se está iniciando, es decir, el segundo dispositivo 2 de computación está iniciando la ejecución de la aplicación P1';

CD2.P1'.Running_OK - La aplicación P1' se está ejecutando satisfactoriamente en el segundo dispositivo 2 de computación;

CD2.P2.Start_Up - La aplicación P2 se está iniciando, es decir, el segundo dispositivo 2 de computación está iniciando la ejecución de la aplicación P2, y

CD2.P2.Running_OK - La aplicación P2 se está ejecutando satisfactoriamente en el segundo dispositivo 2 de computación.

En la etapa 30 de la Figura 4A, el primer dispositivo 1 de computación ha sido activado y P1 empieza a ejecutarse y transmite una condición de terminación de ejecución de inicio CD 1.P1.Start_Up por el bus 3 de datos, y tan pronto como la primera aplicación P1 está a nivel alto y ejecutándose en una condición de estado normal, la aplicación P1 está transmitiendo su condición de ejecución CD1.P1.Running_OK por el bus 3 de sistema. Puesto que el primer dispositivo de computación está configurado solamente con una aplicación activa y sin ninguna aplicación de salvaguarda pasiva, solamente dispone de un programa de instrucción como se ha expuesto en lo que antecede.

En la etapa 31, el segundo dispositivo de computación se activa y el segundo dispositivo de computación empieza a funcionar de acuerdo con el programada de instrucción 1 original (véase la tabla 2 que sigue, la cual revela programas de instrucción en el segundo dispositivo de computación). Es decir, solamente la segunda aplicación P2 está ejecutándose en el segundo dispositivo de computación. De manera similar a la primera aplicación P1 en el primer dispositivo de computación, la segunda aplicación P2 transmite durante el inicio la condición de inicio CD2.P2.Start_Up por el bus 3 de sistema. Tan pronto como P2 está a nivel alto y se está ejecutando en modo normal, la segunda aplicación P2 transmite su condición de ejecución CD2.P2.Running_OK por el bus 3 de sistema.

En la etapa 32, una función 5 de monitorización del segundo dispositivo 2 de computación está monitorizando el bus 3 de sistema con el fin de detectar cuándo se cumple un criterio de conmutación de programa de instrucción.

En la etapa 33 de la Figura 4A, el primer dispositivo 1 de computación falla en cuanto a la ejecución debido, por ejemplo, a un fallo de hardware, pérdida de potencia o similar, y el primer dispositivo 1 de computación detiene la transmisión de la condición de ejecución CD1.P1.Running_OK por el bus de sistema.

En la etapa 34 de la Figura 4B, la función 5 de monitorización del segundo dispositivo 2 de computación detecta una pérdida del primer dispositivo 1 de computación o de la aplicación P1 cuando no recibe una condición de ejecución CD1.P1.Running_OK por el bus de sistema. En la etapa 36, el segundo dispositivo 2 de computación activa un proceso de reprogramación de la ejecución de programa de instrucción en el segundo dispositivo 2 de computación, desde el primer programa de instrucción M1 hasta el segundo programa de instrucción M2. Se debe apreciar aquí que el intervalo entre la transmisión de las condiciones de ejecución puede variar desde muy frecuente, por ejemplo 100 veces por segundo, hasta por ejemplo una vez por minuto, o similar. Con el fin de detectar que se ha perdido la condición de ejecución, la función de monitorización sabe cuándo debe esperar una condición de ejecución del primer dispositivo 1 de computación por el bus 3 de sistema mediante criterios predefinidos en la tabla que sigue.

El momento de la reprogramación es acorde con las condiciones de reprogramación según se expone en la tabla 2 que sigue, indicado como T en las Figuras 1A-1B, definido en el sistema operativo del segundo dispositivo 2 de computación. Durante el proceso de reprogramación, la segunda aplicación P2 continúa transmitiendo la condición de ejecución CD2.P2.Running_OK por el bus 3 de sistema.

En la etapa 38, la aplicación P1' de salvaguarda se activa y el sistema 7 operativo está emitiendo la condición CD2.P1'.Start_Up. Tan pronto como la aplicación P1' está a nivel alto y ejecutando la aplicación de salvaguarda, empieza a transmitir CD2.P1'.Running_OK. La función de monitorización está monitorizando las condiciones de conmutación de programa de instrucción dentro del dispositivo de computación, teniendo en cuenta ambas señales de instante de inicio y de condición sobre el bus de sistema, tal y como se ve en la tabla 2.

TABLA 2

Programa de instrucción en el segundo dispositivo 2 de computación

Programa de instrucción	Criterios de activación	Condiciones de reprogramación	Aplicaciones ejecutadas
M1 (normal)	Inicio normal	Ninguna	P2
M2	Ninguna señal de CD1.P1.Running_OK y X segundos después de "Activación"	Al final del cuadro de instrucción en curso para P2	P2 y P1'

M1	M2 está activo y CD1.P1.Start_Up-señal	Al final del cuadro de instrucción en curso para P2	P2

Haciendo ahora referencia a la tabla 2, los criterios de activación para la activación del proceso de reprogramación desde el programa de instrucción 1, MS1, hasta el programa de instrucción 2, MS2, consisten en que no se detecta ninguna condición de ejecución esperada procedente del primer dispositivo 1 de computación, y que han pasado X segundos desde "activación". Según se ha expuesto en lo que antecede, el primer dispositivo de computación envía una condición de inicio, CD1.P1.Start_Up, por el bus de datos, y de acuerdo con esta realización de la invención, el segundo dispositivo de computación tiene un reloj interno que monitoriza cuántos segundos han pasado desde que fue monitorizada la condición de inicio. Este requisito se implementa con el fin de permitir que el primer dispositivo de computación inicie la primera aplicación P1 sin que el segundo dispositivo 2 de computación tenga que determinar erróneamente que la primera aplicación está a nivel bajo. Esto podría dar como resultado que el sistema empiece a hacer que la aplicación bascule adelante y atrás entre los dos dispositivos incluso aunque la primera aplicación esté trabajando.

Si la función 5 de monitorización ha determinado que el primer software P1 de aplicación está a nivel bajo/ha fallado, la función 5 de monitorización activa el proceso de reprogramación en el segundo dispositivo 2 de computación, dando como resultado que el esquema 1 de instrucción sea conmutado al esquema 2 de instrucción. Sin embargo, cuando ha de hacerse la conmutación, se determina de acuerdo con las condiciones de reprogramación predeterminadas, como se aprecia en la columna titulada "Condiciones de reprogramación" en la tabla 2. Según se aprecia en la tabla 2, la conmutación, cuando se determina que debe llevarse a cabo una conmutación, se inicia al final del cuadro de instrucción de P2, con el fin de evitar la interrupción en la ejecución del segundo software P2 de aplicación. Al tratar de evitar interrupciones en la ejecución de la aplicación P2, se puede evitar la generación de datos erróneos a partir de la segunda aplicación, o como en la Figura 2, la función 4 de monitorización del primer dispositivo 1 de computación determina que P2 ha fallado. Se debe apreciar aquí que la conmutación puede ser realizada, en otra realización, al comienzo de la ejecución de P2. El segundo software de aplicación se ejecuta de forma ininterrumpida en el segundo dispositivo de computación cuando se lleva a cabo la conmutación de programa de instrucción. El sistema operativo de la invención está capacitado para cambiar el esquema de ejecución del dispositivo de computación, y está capacitado para transmitir la condición de ejecución de diferentes aplicaciones a diferentes frecuencias. Por ejemplo, haciendo de nuevo referencia a la Figura 1, el SO del segundo dispositivo de computación transmite cuatro condiciones de ejecución del segundo programa P2 de software de aplicación por segundo, y dos condiciones de ejecución del programa P1' de software de aplicación de salvaguarda por segundo, dando como resultado una secuencia de condiciones de ejecución transmitidas desde el SO del segundo dispositivo 2 de computación, como sigue: Run_P2, Run_P2, Run_P1', RUN_P2, Run_P2, Run_P1'.

En una realización de la invención, se prefiere que el programa de software de aplicación se ejecute en el dispositivo de computación previsto, el primer dispositivo 1 de computación en el ejemplo. Esta característica deseada implica una realización en la que el sistema está capacitado para conmutar de nuevo si el primer programa P1 de software de aplicación empieza a trabajar de nuevo. Una realización de un proceso conforme a todo esto, se ha mostrado en la Figura 5.

En la etapa 40 de la Figura 5, se realiza un reinicio. Se debe apreciar aquí que la iniciación del reinicio/recomienzo puede ser llevada a cabo inmediatamente después del fallo del primer dispositivo de computación, o con un retardo. Es decir, la iniciación del reinicio puede ser llevada a cabo durante el, o después del, proceso de reprogramación en el primer dispositivo de computación. Según se ha definido en la etapa 42, el primer dispositivo de computación inicia la activación del primer software P1 de aplicación después de que ha comenzado el reinicio. En la etapa 44, el primer dispositivo de computación, tan pronto como empieza a ejecutar de nuevo la aplicación después de una interrupción, empieza la transmisión de la condición de inicio de ejecución CD1.P1.Start_Up, y tan pronto como la aplicación P1 está a nivel alto y ejecutándose en estado normal, el primer dispositivo de computación empieza a transmitir su condición de ejecución CD1.P1.Running_OK por el bus 3 de sistema.

Con referencia a la realización de la Figura 5 y a la tabla 2, se muestran las etapas de función del segundo dispositivo de computación. En la etapa 46, la función 5 de monitorización, en el segundo dispositivo 2 de computación, detecta el comienzo de la condición de inicio CD1.P1.Start_Up procedente del primer dispositivo de computación en el bus de sistema. En la etapa 48, se activa el segundo dispositivo 2 de computación, si el segundo dispositivo 2 de computación está funcionando de acuerdo con el programa 2 de instrucción, un proceso de reprogramación del programador maestro desde el programa 2 de instrucción MS2 al programa 1 de instrucción MS1, de acuerdo con la tabla 2. Esto da como resultado, a su vez, que la aplicación P1' de salvaguarda se desactive como se expone en la etapa 50.

Se debe apreciar aquí que el número de reinicios o recomienzos puede estar limitado, por ejemplo, a 3, 10 ó 30 veces, con el fin de evitar que el dispositivo de computación esté realizando un bucle sin fin cuando exista un fallo de hardware en el dispositivo de computación.

La presente invención resulta muy adecuada para redes que utilizan concentradores de datos digitales que multiplexan corrientes de datos procedentes de un número de unidades de computación, en una única corriente de datos que

comprende información de datos digitales procedentes de un número de dispositivos de computación. La función de monitorización de la presente invención se utiliza entonces para monitorizar la corriente de datos digitales.

Realizaciones alternativas de la invención pueden incluir una unidad central de control que monitorice todo el tráfico por un bus de datos, y conmute el dispositivo de computación cuando se detecte un error. La unidad central puede tener un primer programa de instrucción y un número de programas alternativos. Sin embargo, en una realización de la invención, la unidad central de control funciona únicamente como unidad de monitorización que activa el cambio de programa de instrucción en los dispositivos de computación.

El sistema puede comprender funciones de monitorización interna que determinen si la aplicación está produciendo datos erróneos, o similar. Esta característica puede dar como resultado que el SO del dispositivo de computación determine que la primera aplicación P1 ha fallado. El SO puede entonces detener la transmisión de la condición de ejecución, o transmitir CD.P1.Running_NotOK, dando como resultado que los criterios de activación, en el segundo dispositivo de computación, puedan estar recibiendo un CD.P1.Running_NotOK.

En una realización alternativa, un número de programas idénticos de software de aplicación han sido instalados en un número de dispositivos de computación, dando como resultado una realización en la que P1 está instalado en el dispositivo 1 de computación, P1' en el dispositivo 2, P1" en un tercer dispositivo, y así sucesivamente. Esto da como resultado que un criterio de activación en la función de monitorización en el tercer dispositivo consiste en que no se detecta ninguna condición de ejecución de P1 ni de P1' en el bus de datos digitales. Se puede utilizar una amplia gama de realizaciones con diferentes configuraciones, tal como una realización en la que un segundo dispositivo de computación tenga un número de aplicaciones de salvaguarda instaladas en el mismo, por ejemplo P1', P3', P4'.

En lo que antecede se han descrito los principios, las realizaciones preferidas y los modos de operación de la presente invención. Sin embargo, la descripción debe ser considerada como ilustrativa en vez de cómo restrictiva, y no como limitada a las realizaciones particulares que se han expuesto con anterioridad. Se debe apreciar, por lo tanto, que se pueden introducir variaciones en esas realizaciones por parte de los expertos en la materia sin apartarse del alcance de la presente invención, según se define mediante las reivindicaciones siguientes.

REIVINDICACIONES

1. Un sistema eléctrico para un vehículo, que comprende:

- un portador (3) de información digital para transferencia de datos digitales;

- un primer dispositivo (1) de computación, dispuesto para ejecutar un primer software (P1) de aplicación instalado en el primer dispositivo (1) de computación, y

- un segundo dispositivo (2) de computación dispuesto para ejecutar un segundo software (P2) de aplicación, diferente de dicho primer software (P1) de aplicación, instalado en el segundo dispositivo de computación y que comprende además un software (P1') de aplicación de salvaguarda instalado en el segundo dispositivo (2) de computación, idéntico al primer software (P1) de aplicación, en el que el segundo dispositivo (2) de computación está configurado para iniciar una ejecución del software (P1') de aplicación de salvaguarda instalado, cuando se produce un error en el primer dispositivo (1) de computación, en paralelo con la ejecución del segundo software (P2) de aplicación, con lo que el primer y el segundo dispositivos de computación comprenden un sistema operativo de partición dispuesto para dividir la memoria y el tiempo de CPU entre particiones asignadas estáticamente de una manera fija, de manera que cada partición tenga una cierta cantidad de memoria y de tiempo de CPU asignada a la misma, que no puede ser incrementada ni disminuida, y con lo que el primer software (P1) de aplicación, el segundo software (P2) de aplicación y el software (P1') de aplicación de salvaguarda están dispuestos para ser ejecutados en particiones separadas.

2. Un sistema eléctrico de acuerdo con la reivindicación 1, en el que el segundo dispositivo de computación comprende un primer programa de instrucción (M1), en el que el primer programa de instrucción está dispuesto para ejecutar la segunda aplicación (P2) en el segundo dispositivo (2) de computación; y un segundo programa de instrucción (M2), en el que el segundo programa de instrucción está dispuesto para ejecutar la segunda aplicación (P2) y la aplicación (P1') de salvaguarda.

3. Un sistema eléctrico de acuerdo con la reivindicación 2, en el que el segundo dispositivo (2) de computación está dispuesto para ejecutar el primer programa de instrucción cuando el sistema eléctrico está funcionando en un modo normal, es decir, cuando el primer software (P1) de aplicación está ejecutándose apropiadamente en el primer dispositivo (1) de computación, y el segundo dispositivo de computación está dispuesto para ejecutar el segundo programa de instrucción cuando el sistema eléctrico está funcionando en modo de salvaguarda, es decir, cuando el primer software (P1) de aplicación ha fallado en el sistema.

4. Un sistema eléctrico de acuerdo con la reivindicación 3, en el que el segundo dispositivo (2) de computación está configurado para activar un proceso de reprogramación en un sistema operativo del segundo dispositivo (2) de computación, dispuesto para conmutar desde el primer programa de instrucción (MS1) al segundo programa de instrucción (MS2) cuando se detecta un error en el primer dispositivo (1) de computación.

5. Un sistema eléctrico de acuerdo con la reivindicación 4, en el que el segundo dispositivo (2) de computación está dispuesto con una función (5) de monitorización, configurada para activar el proceso de reprogramación en el segundo dispositivo (2) de computación.

6. Un sistema eléctrico de acuerdo con cualquiera de las reivindicaciones 1-5, en el que el segundo dispositivo (2) de computación está dispuesto con una función (5) de monitorización, para monitorizar al menos el primer dispositivo (1) de computación.

7. Un sistema eléctrico de acuerdo con la reivindicación 6, en el que el primer dispositivo de computación está enviando continuamente la condición de ejecución del primer software (P1) de aplicación, y en el que la función (4) de monitorización está configurada para monitorizar datos enviados por el bus (3) de datos, y cuando no se detecta en el bus (3) de sistema una condición de ejecución esperada procedente del primer dispositivo (1) de computación, la función de monitorización está configurada para dar instrucciones al segundo dispositivo (2) de computación para que inicie la ejecución del tercer software (P1') de aplicación.

8. Un sistema eléctrico de acuerdo con la reivindicación 1, en el que el sistema eléctrico es un sistema no-crítico que no es sensible a los retardos.

9. Un procedimiento para asegurar la función de salvaguarda en un sistema eléctrico de un vehículo que comprende un portador (3) de información digital para transferencia de datos digitales, un primer dispositivo (1) de computación dispuesto para ejecutar un primer software (P1) de aplicación instalado en el primer dispositivo (1) de computación, y un segundo dispositivo (2) de computación dispuesto para ejecutar un segundo software (P2) de aplicación instalado en el segundo dispositivo de computación, diferente de dicho primer software (P1) de aplicación, y un tercer software (P1') de aplicación de salvaguarda, idéntico al primer software de aplicación, en el que el primer y el segundo dispositivos de computación comprenden un sistema operativo de partición dispuesto para dividir la memoria y el tiempo de CPU entre particiones asignadas estáticamente de una manera fija, de modo que cada partición tenga una cierta cantidad de memoria y de tiempo de CPU asignada a la misma, que no puede ser ni incrementada ni reducida, comprendiendo dicho procedimiento las etapas de:

- determinar que se ha producido un error en el primer dispositivo de computación, e

- iniciar una ejecución de la aplicación de salvaguarda en una primera partición que tiene una cierta cantidad de memoria y de tiempo de CPU asignada a la misma, en paralelo mientras se está ejecutando continuamente el segundo software (P2) de aplicación en una segunda partición que tiene una cierta cantidad de memoria y de tiempo de CPU asignada a la misma.

10. Un procedimiento de acuerdo con la reivindicación 9, en el que el proceso de iniciación comprende la etapa de conmutar desde un programa de instrucción original que se ejecuta en el segundo dispositivo de computación, a un segundo programa de instrucción.

11. Un procedimiento de acuerdo con cualquiera de las reivindicaciones 9-10, en el que el procedimiento comprende además la etapa de:

- monitorizar el portador de información digital utilizando una función de monitorización que se ejecuta en el segundo dispositivo de computación, realizando también dicha función de monitorización la citada etapa de determinación.

12. Un procedimiento de acuerdo con la reivindicación 11, en el que la función de monitorización realiza además la monitorización de las condiciones de ejecución del primer software (P1) de aplicación enviadas en la información digital desde el primer dispositivo de computación.

13. Un procedimiento de acuerdo con la reivindicación 12, en el que la función de monitorización determina además que se ha producido un error en el primer dispositivo de computación cuando ninguna condición de ejecución del primer software (P1) de aplicación es monitorizada en el portador de información digital.

14. Un procedimiento de acuerdo con cualquiera de las reivindicaciones 9-13, en el que el procedimiento comprende además, después de la citada etapa de iniciación, las etapas de:

a. determinar que el primer software de aplicación está a nivel alto y ejecutándose en el primer dispositivo de computación, y

b. conmutar de nuevo al estado de ejecución original que realiza la primera aplicación en el proceso cuando se determina que el primer software de aplicación está a nivel alto y ejecutándose de nuevo en el primer dispositivo de computación.

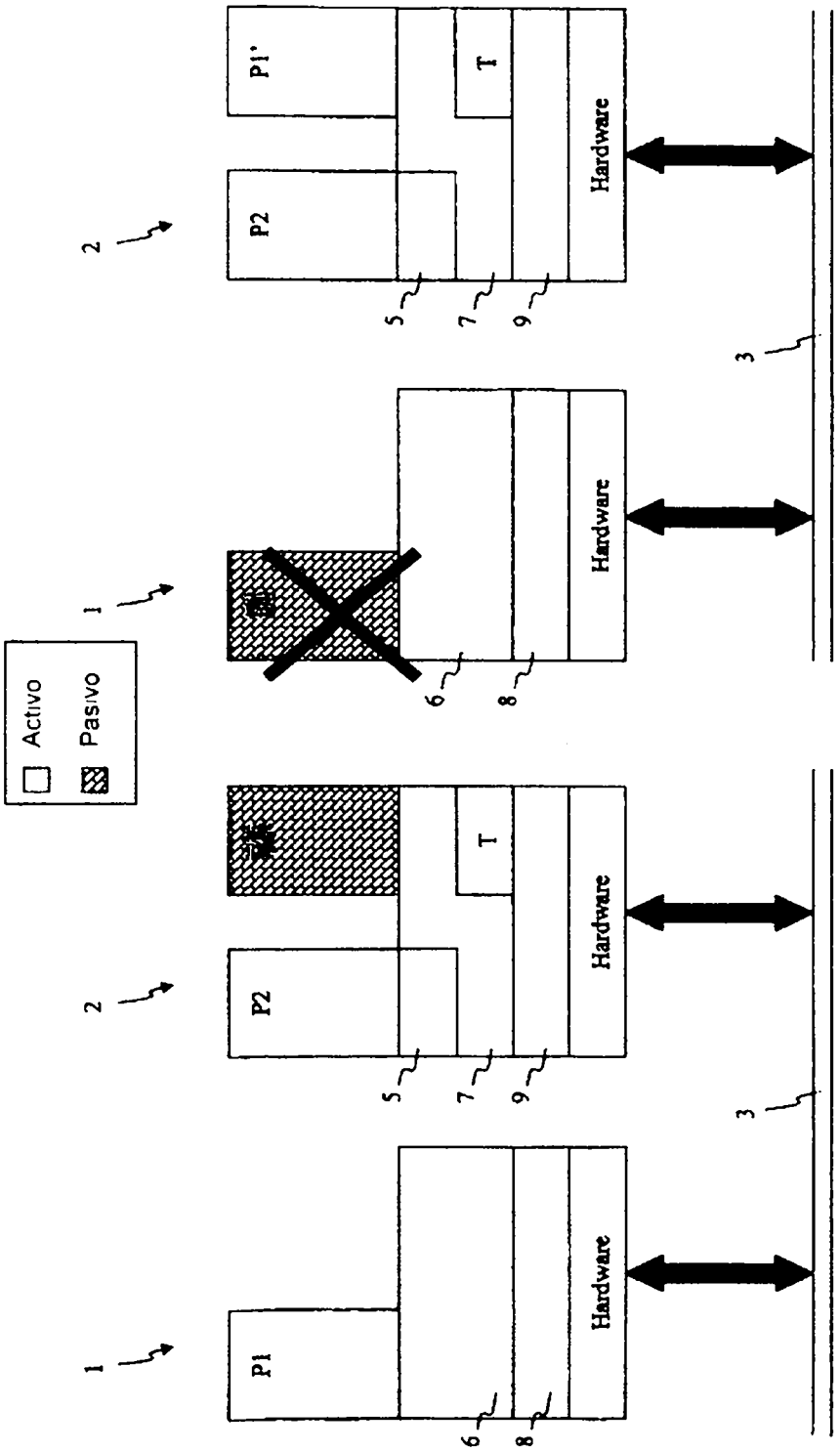

FIG. 1A

FIG. 1B

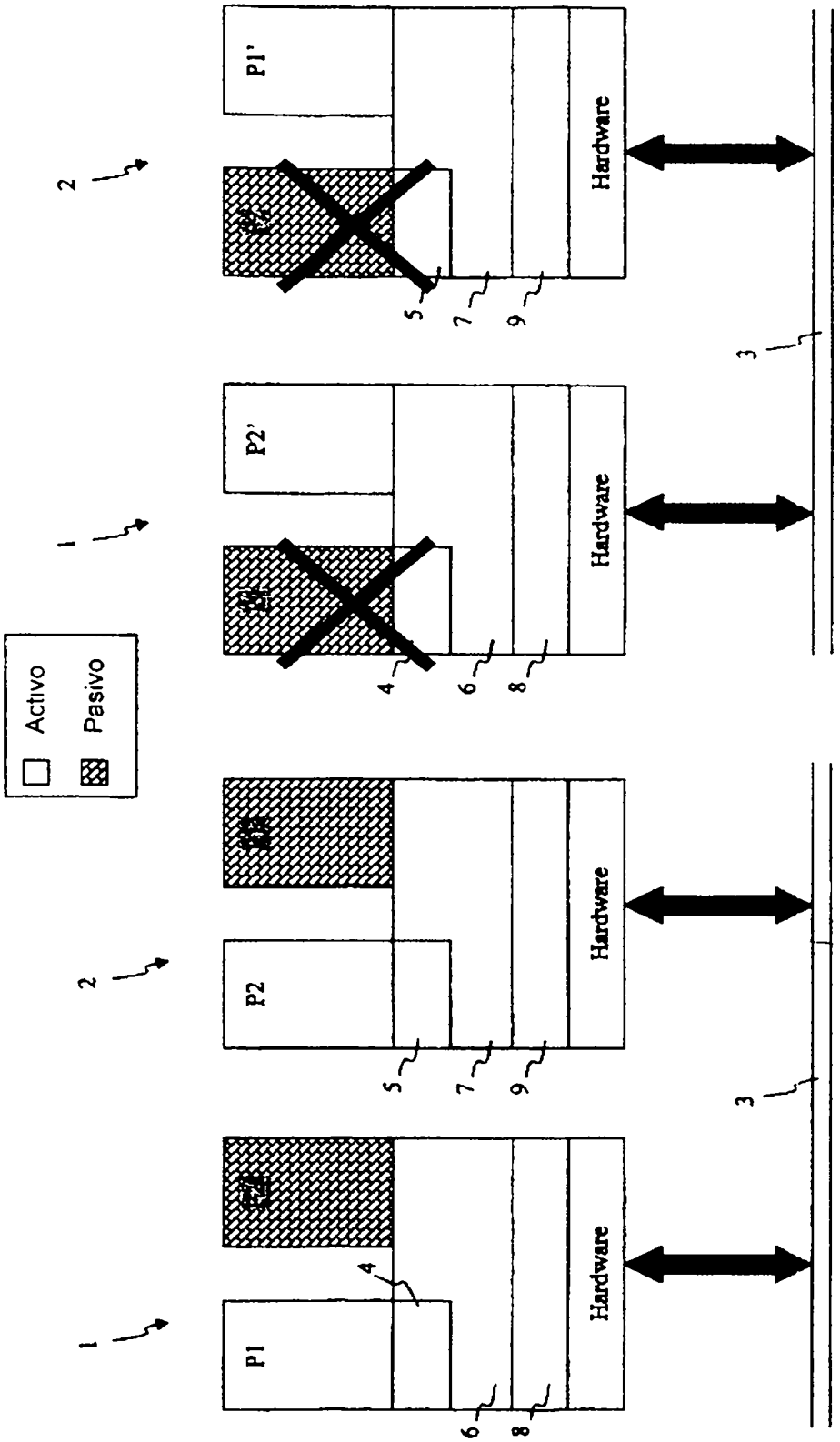

FIG. 2A

FIG. 2B

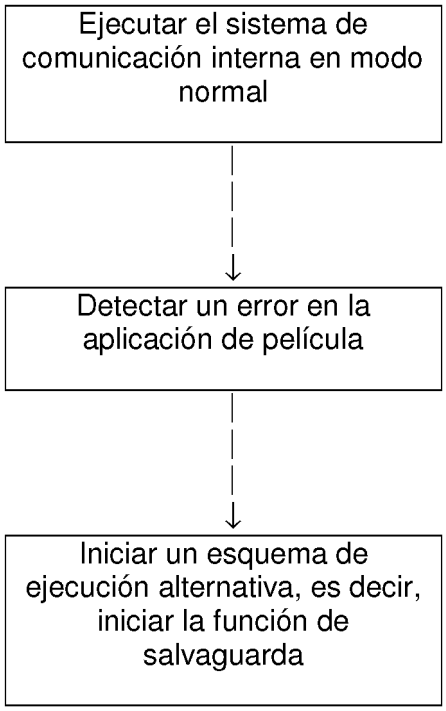
Ejecutar el sistema de comunicación interna en modo normal
Detectar un error en la aplicación de película
Iniciar un esquema de ejecución alternativa, es decir, iniciar la función de salvaguarda

FIG. 3

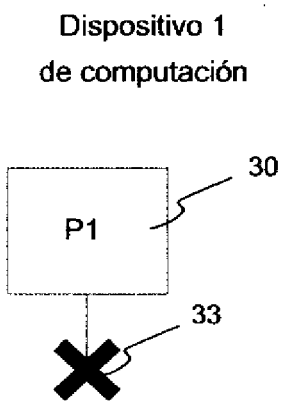
Dispositivo 1
de computación
P1
30
33

FIG. 4A

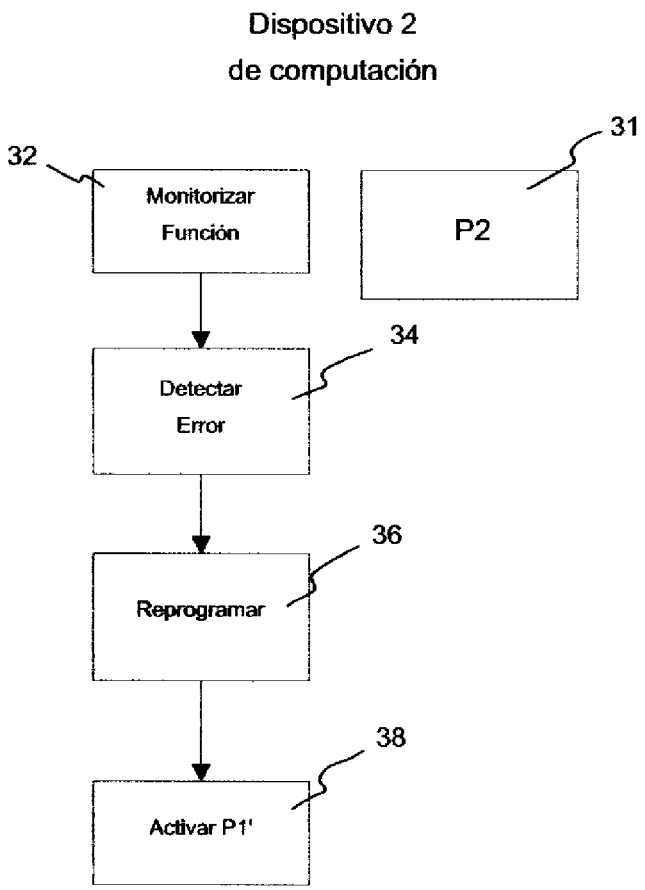
Dispositivo 2
de computación
32
Monitorizar
Función
31
P2
34
Detectar
Error
36
Reprogramar
38
Activar P1'

FIG. 4B

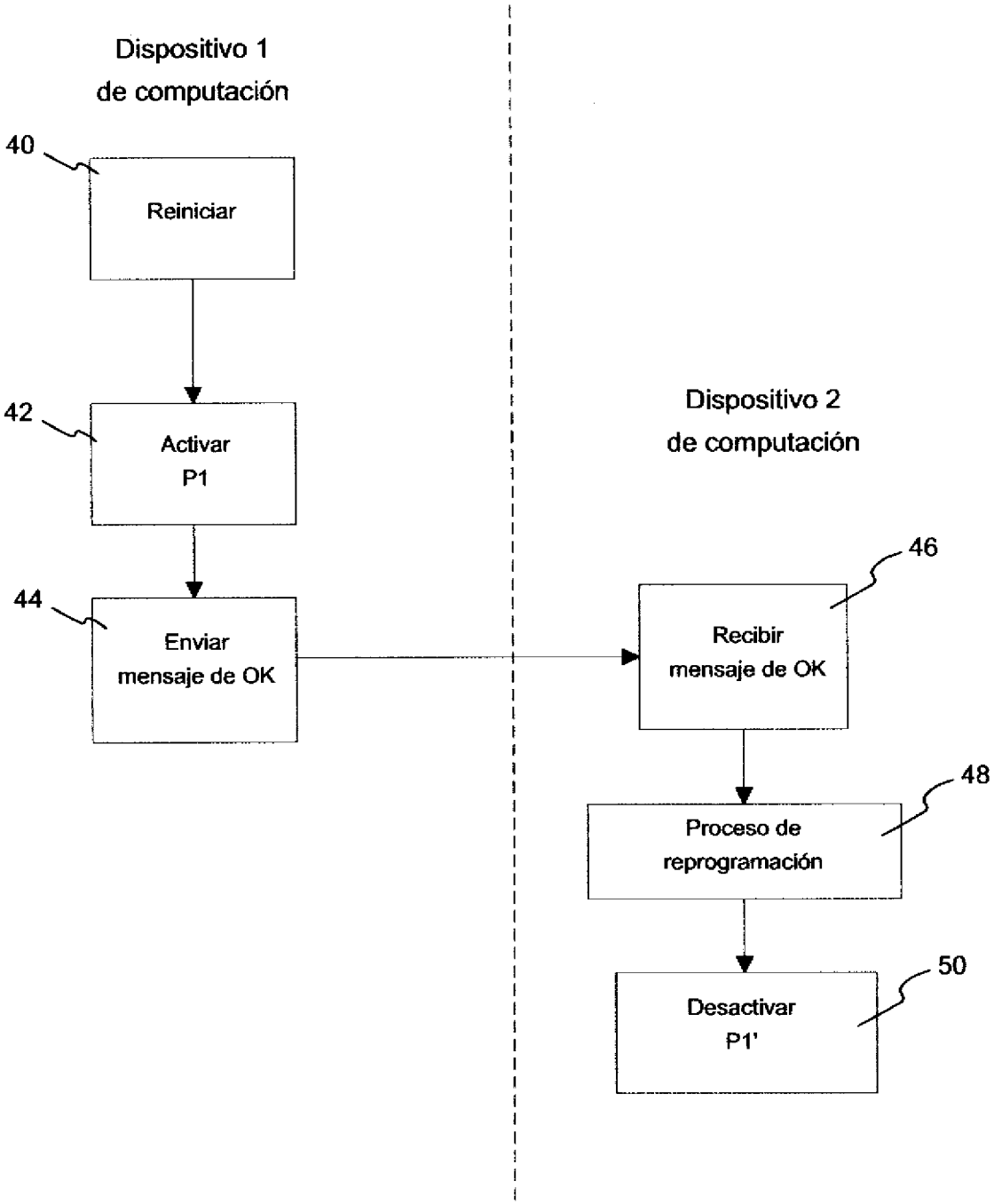
Dispositivo 1
de computación
40
Reiniciar
42
Activar
P1
44
Enviar
mensaje de OK
Dispositivo 2
de computación
46
Recibir
mensaje de OK
48
Proceso de
reprogramación
50
Desactivar
P1'

FIG. 5