(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 615 119**

(51) Int. CI.:

G06F 11/14 (2006.01)
G06F 11/16 (2006.01)
G06F 11/18 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **09.02.2015 E 15154334 (5)**

(97) Fecha y número de publicación de la concesión europea: **04.01.2017 EP 2911058**

(54) Título: **Procedimientos y aparatos de reducción de fallos de modo común de sistemas de control de software relacionados con seguridad nuclear**

(30) Prioridad:

12.02.2014 US 201414178820

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.06.2017

(73) Titular/es:

GE-HITACHI NUCLEAR ENERGY AMERICAS LLC (100.0%)
3901 Castle Hayne Road
Wilmington, NC 28401, US

(72) Inventor/es:

KAKUNDA, BISHARA E.;
DROBA, GREGORY S. y
MEEK, OSCAR L.

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimientos y aparatos de reducción de fallos de modo común de sistemas de control de software relacionados con seguridad nuclear

Antecedentes

Se define fallo de causa común (CCF) como un fallo de dos o más estructuras, sistemas, y/o componentes debido a un solo evento o causa específica. CCF puede incluir un fallo de dos o más estructuras, sistemas, y/o componentes causado por cualquier deficiencia latente procedente del diseño o de la fabricación, de la operación o errores de mantenimiento y/o que pueda ser provocado por cualquier evento inducido por algún fenómeno natural, operación de procedimiento de planta generadora o error humano. Fallo de modo común (CMF) es un subconjunto de CCF y se produce cuando dos o más sistemas o componentes fallan de la misma manera. Los eventos de CMF pueden incluir fallos en múltiples partes de un sistema causados por un solo fallo, particularmente fallos aleatorios debidos a condiciones ambientales, envejecimiento, eventualidades operativas anormales (AOOs), accidentes sobre la base del diseño (DBA) y similares.

Los criterios de diseño para sistemas de seguridad en una central de energía nuclear (NPP) incluyen la separación de divisiones redundantes, tales como barreras físicas y aislamiento eléctrico, para que se aplique en general como medidas de diseño para abordar las posibles vulnerabilidades relacionadas con un CMF de equipo y/o la propagación de los efectos del fallo. Las medidas de separación y de redundancia tienden a reducir al mínimo los CMFs relacionados con los componentes compartidos y/o el equipo, que protege típicamente contra fallos aleatorios en el hardware. Sin embargo, muchos defectos en el software tienden a tener fallos de modo común, ya que el software en cada división es idéntico. No obstante, se ha reconocido durante mucho tiempo la posibilidad de la vulnerabilidad de CMF y, por lo tanto, se emplea la "diversidad" a fin de satisfacer los requisitos de seguridad para las NPPs.

Como analiza Preckshot en "*Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems*", NUREG/CR-6303, NRC Job Code L1867, la "diversidad" es "un principio en los sistemas de instrumentación para detectar diferentes parámetros, mediante el uso de diferentes tecnologías, mediante el uso de diferentes lógicas o algoritmos o mediante el uso de diferentes medios de actuación para proporcionar varias maneras de detectar y responder a un evento significativo". Cuando se aplica el principio de diversidad en los sistemas de instrumentación, se pueden mitigar o reducir las preocupaciones de CMF.

El CMF puede producirse en "divisiones redundantes" del equipo de seguridad nuclear. Las divisiones redundantes son divisiones del equipo de seguridad nuclear que operan software, sistemas operativos y bibliotecas compartidos en la misma plataforma de hardware. Se pueden usar las divisiones redundantes para realizar una función de seguridad. Un CMF que se produce al mismo tiempo es de especial interés para las divisiones redundantes porque el CMF puede afectar cada una de las divisiones redundantes al mismo tiempo, y tiene la posibilidad de degradar la función de seguridad. A los inspectores de regulación nuclear les podría preocupar que los CMFs de software en los sistemas de seguridad digital anulen los beneficios de la redundancia a través de múltiples divisiones. La preocupación es que, debido a hardware y software comunes entre múltiples divisiones redundantes, un defecto de software se puede exhibir al mismo tiempo en cada una de las divisiones redundantes y se pueda evitar, por lo tanto, que el equipo realice su función de seguridad.

Para superar los CMFs en múltiples divisiones redundantes, como se analiza anteriormente, se han diseñado típicamente diversas plataformas de hardware para proporcionar protección adicional. Por ejemplo, se puede proporcionar diversidad mediante el nuevo diseño de tarjetas lógicas con dos diferentes dispositivos lógicos fabricados por diferentes proveedores, además de duplicar la lógica dentro de cada división. Tales nuevos diseños de hardware pueden ser caros y causar largas demoras en la implementación.

Por ello, existe la necesidad de proporcionar diversidad en múltiples divisiones de un equipo de seguridad nuclear y, en particular, de proporcionar diversidad en múltiples divisiones de un equipo de seguridad nuclear sin que se requiera un nuevo diseño de hardware.

El documento WO 2011/101707 A1 desvela un procedimiento para procesar datos en un procesador de datos que comprende al menos dos unidades de procesamiento de datos. El procedimiento comprende realizar diferentes etapas de procesamiento de datos en las unidades de procesamiento de datos simultáneamente durante una operación en paralelo, y reproducir los rendimientos de etapas de procesamiento de datos idénticas seleccionadas en las unidades de procesamiento de datos durante una operación redundante no sincronizada. El documento WO 98/57238 A desvela un sistema de seguridad o protección que incluye una pluralidad de divisiones de primeras señales; una pluralidad de subsistemas de seguridad o protección, cada uno de los cuales recibe una división correspondiente de las divisiones de las primeras señales y produce una pluralidad correspondiente de segundas señales desde la misma; y un subsistema de memoria reflectante para comunicar las segundas señales entre los subsistemas de seguridad o protección.

El documento US 5 613 127 A desvela un aparato procesador para funciones de control realizadas de una manera redundante que utiliza relojes separados, pero que corrige la falta de coincidencia en su sincronización, provocando

una interrupción del procesamiento a través de software a un estado de "retención" para dejar tiempo por cualquier demora a los procesadores para ponerse al día antes de iniciar una trama siguiente de procesamiento.

El documento GB 2 317 032 A desvela un sistema de seguridad contra fallos de microcontrolador que incluye un microprocesador primario acoplado a un bus y dispuesto para procesar señales no procesadas recibidas desde el bus y para proporcionar señales procesadas primarias. Una disposición de retardo retrasa tanto las señales no procesadas como las primarias procesadas en un período predeterminado, para proporcionar señales retardadas. Un microprocesador secundario está dispuesto para procesar las señales retardadas no procesadas y para proporcionar señales procesadas secundarias.

Sumario

Por lo menos una realización de ejemplo de la invención, que se define en detalle en las reivindicaciones independientes 1 y 9 adjuntas, se refiere a un sistema informático para ejecutar una tarea de acuerdo con diferentes frecuencias de reloj para reducir fallos de modo común en el sistema informático.

En una realización de ejemplo, el sistema informático incluye por lo menos una primera división y una segunda división. La primera división tiene una primera frecuencia de reloj y la segunda división tiene una segunda frecuencia de reloj. El sistema informático incluye un primer procesador configurado para ejecutar una tarea en la primera división y un segundo procesador configurado para ejecutar la tarea en la segunda división. La tarea ejecutada en la primera división opera de acuerdo con la primera frecuencia de reloj, y la tarea ejecutada en la segunda división opera de acuerdo con la segunda frecuencia de reloj.

Algunas realizaciones de ejemplo prevén que el primer procesador y el segundo procesador estén configurados además para determinar que exista una condición de disparo en por lo menos una de la primera división y la segunda división.

Las realizaciones de ejemplo prevén que la primera frecuencia de reloj tenga diferente velocidad que la segunda frecuencia de reloj.

Las realizaciones de ejemplo prevén que la tarea sea ejecutada simultáneamente en el primer procesador y en el segundo procesador.

Las realizaciones de ejemplo prevén que la primera división incluya un reloj de primera división configurado para medir un tiempo de primera división mediante el recuento de un número de registros de primera división que se hayan producido desde el tiempo de inicio deseado. Cada registro de primera división representa una cantidad de tiempo requerida para ejecutar una instrucción de programa de la tarea de acuerdo con la frecuencia de reloj de primera división. Realizaciones de ejemplo prevén que la segunda división incluya un reloj de segunda división configurado para medir un tiempo de segunda división mediante el recuento de un número de registros de segunda división que se hayan producido desde el tiempo de inicio deseado. Cada registro de segunda división representa una cantidad de tiempo requerida para ejecutar una instrucción de programa de la tarea de acuerdo con la frecuencia de reloj de segunda división.

Las realizaciones de ejemplo prevén que el sistema informático incluya además un reloj de sistema configurado para medir un tiempo de sistema mediante el recuento de un número de registros de sistema que se hayan producido a partir de un tiempo de inicio deseado. El reloj de sistema tiene una frecuencia de reloj de sistema, donde cada registro de sistema representa una cantidad de tiempo requerida para ejecutar una instrucción de programa de la tarea de acuerdo con la frecuencia de reloj de sistema.

Las realizaciones de ejemplo prevén que (i) cada uno de los registros de primera división representa tanto la cantidad de tiempo requerida para ejecutar una instrucción de programa de la tarea de acuerdo con la frecuencia de reloj de primera división como un retraso en el inicio de una ejecución de una siguiente instrucción de programa de la tarea, y (ii) cada uno de los registros de segunda división representa tanto la cantidad de tiempo requerida para ejecutar una instrucción de programa de la tarea de acuerdo con la frecuencia de reloj de segunda división como un retraso en el inicio de la ejecución de la siguiente instrucción de programa de la tarea.

Las realizaciones de ejemplo prevén que el primer procesador esté configurado además para variar la ejecución de la tarea en la primera división basándose en por lo menos uno de la frecuencia de reloj de primera división y el tiempo de sistema, y el segundo procesador esté configurado además para variar la ejecución de la tarea en la segunda división basándose en por lo menos uno de la frecuencia de reloj de segunda división y el tiempo del sistema.

Las realizaciones de ejemplo prevén que cada una de la primera división y la segunda división comprenda por lo menos un instrumento configurado para obtener datos de por lo menos un sensor o una entrada; monitorizar los datos obtenidos; generar información de disparo basándose en los datos obtenidos; y realizar un procedimiento de votación divisional basándose en la información de disparo, en que el procedimiento de votación divisional se usa para detectar discrepancias de por lo menos una de la primera división y la segunda división.

Por lo menos una realización de ejemplo se refiere a un procedimiento para ejecutar una tarea para reducir fallos de modo común en un sistema informático.

En una realización de ejemplo, el procedimiento incluye dividir el sistema informático en una primera división y una segunda división. El procedimiento incluye definir una primera frecuencia de reloj para la primera división y una segunda frecuencia de reloj para la segunda división. El procedimiento incluye ejecutar la tarea en la primera división y en la segunda división. La tarea ejecutada en la primera división opera de acuerdo con la primera frecuencia de reloj, y la tarea ejecutada en la segunda división opera de acuerdo con la segunda frecuencia de reloj.

Las realizaciones de ejemplo prevén que el procedimiento incluya además determinar que exista una condición de disparo en por lo menos una de la primera división y la segunda división. Las realizaciones de ejemplo prevén que la primera frecuencia de reloj tenga diferente velocidad que la de la segunda frecuencia de reloj.

Las realizaciones de ejemplo prevén que la ejecución incluya además ejecutar simultáneamente la tarea en la primera división y en la segunda división.

Las realizaciones de ejemplo prevén que el procedimiento incluya además definir un reloj de primera división para la primera división para medir un tiempo de primera división mediante el recuento de un número de registros de primera división que se hayan producido a partir del tiempo de inicio deseado. Cada registro de primera división representa una cantidad de tiempo requerida para ejecutar una instrucción de programa de la tarea de acuerdo con la frecuencia de reloj de primera división. El procedimiento incluye además definir un reloj de segunda división para la segunda división para medir un tiempo de segunda división mediante el recuento de un número de registros de segunda división que se hayan producido a partir del tiempo de inicio deseado. Cada registro de segunda división representa una cantidad de tiempo requerida para ejecutar una instrucción de programa de la tarea de acuerdo con la frecuencia de reloj de segunda división.

Las realizaciones de ejemplo prevén que el procesador opere de acuerdo con un reloj de sistema, y el procedimiento incluye además medir un tiempo de sistema mediante el recuento de un número de registros de sistema que se hayan producido a partir de un tiempo de inicio deseado. El reloj de sistema tiene una frecuencia de reloj de sistema, en donde cada registro de sistema representa una cantidad de tiempo requerida para ejecutar una instrucción de programa de la tarea de acuerdo con la frecuencia de reloj de sistema.

Las realizaciones de ejemplo prevén que por lo menos uno de (i) cada uno de los registros de primera división representa tanto la cantidad de tiempo requerida para ejecutar una instrucción de programa de la tarea de acuerdo con la frecuencia de reloj de primera división como un retraso en el inicio de una ejecución de una siguiente instrucción de programa de la tarea, y (ii) cada uno de los registros de segunda división representa tanto la cantidad de tiempo requerida para ejecutar una instrucción de programa de la tarea de acuerdo con la frecuencia de reloj de segunda división como un retraso en el inicio de la ejecución de la siguiente instrucción de programa de la tarea.

Las realizaciones de ejemplo prevén que el procedimiento incluya además variar la ejecución de la tarea en la primera división basándose en por lo menos uno de la frecuencia de reloj de primera división y el tiempo de sistema, y variar la ejecución de la tarea en la segunda división basándose en por lo menos uno de la frecuencia de reloj de segunda división y el tiempo de sistema.

Las realizaciones de ejemplo prevén que el procedimiento incluya además obtener datos de por lo menos una entrada; monitorizar los datos obtenidos; generar información de disparo basándose en los datos obtenidos; y realizar un procedimiento de votación divisional basándose en la información de disparo, en que se usa el procedimiento de votación divisional para detectar discrepancias de por lo menos una de la primera división y la segunda división.

Por lo menos una realización de ejemplo se refiere a un procedimiento para ejecutar una tarea para reducir fallos de modo común en un sistema informático, donde el sistema informático incluye una pluralidad de divisiones, y cada de la pluralidad de divisiones tiene diferente frecuencia de reloj.

En una realización de ejemplo, el procedimiento incluye variar, mediante un procesador, una velocidad de programa de cada una de la pluralidad de divisiones, de manera que la tarea, cuando se ejecuta en una correspondiente de la pluralidad de divisiones, opera a una frecuencia de reloj de acuerdo con la correspondiente de la pluralidad de divisiones.

Breve descripción de los dibujos

Los dibujos adjuntos, los cuales se incorporan en y constituyen una parte de la memoria descriptiva, ilustran una o más realizaciones y, junto con la descripción, explican estas realizaciones. En los dibujos:

la figura 1 ilustra un sistema de monitorización que incluye múltiples divisiones redundantes de instrumentación, de acuerdo con una realización de ejemplo;

la figura 2 ilustra los componentes de un procesador contenido en instrumentos que son empleados por cada una

de las divisiones redundantes del sistema de monitorización de la figura 1, de acuerdo con una realización de ejemplo; y

la figura 3 ilustra un diagrama de temporización variable de reloj, de acuerdo con una realización de ejemplo.

Descripción detallada de las realizaciones

Se describirán ahora varias realizaciones de ejemplo más detalladamente con referencia a los dibujos adjuntos, en los cuales se muestran algunas realizaciones de ejemplo de la invención.

Se divulgan en el presente documento realizaciones ilustrativas detalladas. Sin embargo, los detalles estructurales y funcionales específicos expuestos en el presente documento son meramente representativos con el propósito de describir realizaciones de ejemplo de la presente invención. Se puede realizar esta invención, sin embargo, en muchas formas alternativas y no se debe interpretar como limitada solamente a las realizaciones expuestas en el presente documento.

Se entenderá que, aunque los términos primero, segundo, etc. se pueden utilizar aquí para describir varios elementos, estos elementos no deben estar limitados por estos términos. Estos términos solo se utilizan para distinguir un elemento de otro. Por ejemplo, un primer elemento podría llamarse un segundo elemento, y asimismo un segundo elemento podría llamarse un primer elemento, sin separarse del alcance de las realizaciones de ejemplo de la presente invención. Tal como se utiliza aquí, el término "y/o" incluye cualquiera y todas las combinaciones de uno o más de los elementos nombrados asociados.

Se entenderá que, cuando se hace referencia a que un elemento está "conectado" o "acoplado" a otro elemento, el mismo puede estar directamente conectado o acoplado al otro elemento o pueden estar presentes elementos intermedios. Por el contrario, cuando se hace referencia a que un elemento esta "directamente conectado" o "directamente acoplado" a otro elemento, no están presentes elementos intermedios. Otras palabras utilizadas para describir la relación entre los elementos deben ser interpretadas en un modo similar (por ejemplo, "entre" en comparación con "directamente entre", "adyacente" en comparación con "directamente adyacente", etc.).

La terminología utilizada en el presente documento tiene solo el propósito de describir realizaciones particulares y no pretende limitar las realizaciones de ejemplo de la invención. Como se utiliza aquí, las formas en singular "un/una" y "el/la" pretenden incluir también las formas en plural, a menos que el contexto indique claramente lo contrario. Además, se entenderá que los términos "comprende", "que comprende", "incluye" y/o "que incluye" cuando se utilizan en el presente documento, especifican la presencia de las características, números enteros, etapas, operaciones, elementos y/o componentes establecidos, pero no excluyen la presencia o adición de una o varias otras características, números enteros, etapas, operaciones, elementos, componentes y/o grupos de las mismas.

Cabe mencionar también que, en algunas implementaciones alternativas, los hechos/funciones mencionados pueden producirse en orden distinto al indicado en las figuras. Por ejemplo, dos figuras mostradas en sucesión pueden ejecutarse en efecto de manera sustancialmente al mismo tiempo o pueden ser ejecutadas algunas veces en el orden inverso, dependiendo de los hechos o la funcionalidad implicados.

Se proporcionan detalles específicos en la siguiente descripción para proporcionar un entendimiento completo de las realizaciones de ejemplo. Sin embargo, un experto en la técnica entenderá que se pueden llevar a la práctica las realizaciones de ejemplo sin estos detalles específicos. Por ejemplo, se pueden mostrar los sistemas en diagramas de bloques para no oscurecer las realizaciones de ejemplo con detalles innecesarios. En otros casos, se pueden mostrar procedimientos, estructuras y técnicas bien conocidas sin detalles innecesarios para evitar oscurecer las realizaciones de ejemplo.

Asimismo, se indica que se pueden describir las realizaciones de ejemplo como un procedimiento representado como un esquema de flujo, un diagrama de flujo, un diagrama de flujo de datos, un diagrama de estructura o un diagrama de bloques. Aunque un diagrama de flujo puede describir las operaciones como un procedimiento secuencia, se puede realizar gran parte de las operaciones en paralelo, al mismo tiempo o simultáneamente. Por otra parte, se puede cambiar el orden de las operaciones. Se puede terminar un procedimiento cuando hayan completado sus operaciones, pero puede tener también etapas adicionales no incluidas en la figura. Un procedimiento puede corresponder a un procedimiento, una función, un procedimiento, una subrutina, un subprograma, etc. Cuando un procedimiento corresponde a una función, su terminación puede corresponder a un regreso de la función a la función de llamada o la función principal.

Además, como se expone en el presente documento, el término "memoria" puede representar uno o más dispositivos para almacenar datos, incluso memoria de acceso aleatorio (RAM), RAM magnética, memoria principal y/u otros medios legibles por máquina para almacenar información. El término "medio de almacenamiento" puede representar uno o más dispositivos para almacenar datos, incluyendo memoria de solo lectura (ROM), memoria de acceso aleatorio (RAM), RAM magnética, memoria principal, medios de almacenamiento en disco magnético, medios de almacenamiento óptico, dispositivos de memoria instantánea y/u otros medios legibles por máquina para almacenar información. El término "medio legible por ordenador" puede incluir, sin limitación, dispositivos de

almacenamiento portátiles o fijos, dispositivos de almacenamiento óptico, canales inalámbricos y otros varios medios capaces de almacenar, contener o llevar instrucción(es) y/o datos.

Además, se pueden implementar realizaciones de ejemplo mediante hardware, software, firmware, middleware, microcódigo, lenguajes de descripción de hardware o cualquier combinación de los mismos. Cuando se implementa en software, firmware, middleware o microcódigo, el código de programa o los segmentos de código, para realizar las tareas necesarias, se pueden almacenar en un medio legible por máquina u ordenador, tal como un medio de almacenamiento. Uno o varios procesadores pueden realizar las tareas necesarias.

Un segmento de código puede representar un procedimiento, una función, un subprograma, un programa, una rutina, una subrutina, un módulo, un paquete de software, una clase o cualquier combinación de instrucciones, datos estructuras o declaraciones de programa. Se puede acoplar un segmento de código a otro segmento de código o a un circuito de hardware pasando y/o recibiendo información, datos, argumentos, parámetros o contenidos de memoria. Se puede pasar, reenviar o transmitir información, argumentos, parámetros, datos, etc. a través de cualesquiera medios adecuados incluyendo el uso compartido de memoria, paso de mensajes, paso de testigos, transmisión en la red, etc.

Se describen realizaciones de ejemplo en el presente documento como implementadas en un entorno informático adecuado. Aunque no se requieren, se describirán realizaciones de ejemplo en el contexto general de instrucciones ejecutables por ordenador, tal como módulos de programa o procedimientos funcionales, que son ejecutados por uno o más procesadores de ordenador o CPU. Generalmente, los módulos de programa o los procedimientos funcionales incluyen rutinas, programas, objetos, componentes, estructuras de datos, etc. que realizan tareas particulares o implementan tipos particulares de datos. Se pueden implementar los módulos de programa y los procedimientos funcionales analizados en el presente documento mediante el uso de hardware existente en las redes de comunicación existentes. Por ejemplo, se pueden implementar módulos de programa y procedimientos funcionales analizados en el presente documento mediante el uso de hardware existente en elementos de red o nodos de control existentes. Este hardware existente puede incluir uno o más procesadores de señales digitales (DSP), circuitos integrados para aplicaciones específicas, dispositivos de compuertas programables de campo (FPGA), ordenadores o similares.

Las realizaciones de ejemplo de un sistema de monitorización y control permiten que un procesador tenga frecuencias de reloj variables en diferentes divisiones del equipo de seguridad nuclear (a las cuales se hace referencia en lo sucesivo como "divisiones"), que usa software y hardware iguales en aplicaciones relacionadas con la seguridad nuclear. Mediante la variación de la velocidad de reloj para cada división que opera y/o ejecuta la misma tarea, una temporización de programa de la tarea que se ejecute en cada división puede ser diferente. Dado que cada división ejecuta la misma tarea a diferentes velocidades, cada división es asíncrona una en relación con otra en el sistema de monitorización y control. De esta manera, se pueden reducir o mitigar de alguna otra manera los posibles fallos de modo común (CMFs) relacionados con el software.

Cabe mencionar que, aunque las realizaciones de ejemplo pueden ser aplicables a sistemas relacionados con la seguridad nuclear, las realizaciones de ejemplo pueden también ser aplicables a cualquier sistema redundante, incluyendo sin limitación un equipo nuclear no relacionado con la seguridad, equipo de aviación, equipo médico, y otros sistemas redundantes similares. Cabe mencionar también que las realizaciones de ejemplo pueden ser aplicables también a sistemas de accionamiento y/o a sistemas de control con dispositivos de control de bucle abierto o dispositivos de control de bucle cerrado.

Las realizaciones de ejemplo incluyen múltiples divisiones, cada una de las cuales emplea un procesador que permite que varíe una frecuencia de reloj de la división. Tales procesadores se usan típicamente para disminuir la frecuencia de reloj para reducir el consumo de energía, pero, cuando se aplican a sistemas de control para seguridad nuclear, se puede usar la frecuencia variable para alterar la orden de ejecución de una o más tareas o subprocedimientos en las divisiones redundantes, mitigando así un posible riesgo de CMF.

Las realizaciones de ejemplo incluyen un reloj de división. Se puede crear un reloj de división mediante el uso de un temporizador de hardware y/o un temporizador de software, que es una función fija de la frecuencia de reloj que está definida para la división. Cuando el temporizador expira, puede generarse una interrupción mediante el procesador y un sistema operativo (OS) puede contar el tiempo como un "registro". Un registro puede ser una unidad arbitraria que representa una cantidad de tiempo requerida para ejecutar una instrucción de programa de una tarea de acuerdo con la frecuencia de reloj. Por ello, un registro es una cantidad de tiempo que se requiere para que el temporizador expire, y variará con la frecuencia a la cual se sincronice el procesador.

Las realizaciones de ejemplo incluyen un OS que funciona en conjunción con el procesador que puede variar su frecuencia de reloj de procesador. El OS proporciona un servicio tradicional de planificación, donde se planifica una tarea o un subprocedimiento específicos para operar basándose en un tiempo recurrente. Además del servicio tradicional, el planificador de OS puede estar configurado para planificar una tarea o un subprocedimiento basándose en registros, en lugar de tiempo. La ejecución del mismo software en el mismo hardware en dos o más divisiones, pero con una mezcla de tareas o subprocedimientos que son fijos en el tiempo, así como fijados por registros, hará que la tarea o el subprocedimiento de tiempo fijo opere a la misma frecuencia, mientras que las

tareas o el subprocedimiento de registro fijo operarán de manera más rápida o más lenta, según determine la frecuencia de reloj. Adicionalmente, de acuerdo con realizaciones de ejemplo, cuando el OS permite que una tarea opere hasta terminar, los retrasos (por ejemplo, las demoras internas debidas a iniciar una ejecución de una siguiente instrucción de programa de una tarea) a la tarea o el subprocedimiento puede causar que varíe el orden de ejecución y/o temporización de programa entre las divisiones, incluso si el mismo software y hardware está operando y procesando las mismas señales de entrada.

La figura 1 ilustra un sistema 100 de monitorización que incluye múltiples divisiones redundantes, de acuerdo con una realización de ejemplo. El sistema 100 de monitorización y control incluye divisiones 105-1 - 105-N (donde $N \geq 2$) (a las cuales se hace referencia en los sucesivo como "divisiones 105"). Adicionalmente, cada una de las divisiones 105 incluye instrumentos 110-1 - 110-N e instrumentos 115-1 - 115-N (donde $N \geq 2$) (a los cuales se hace referencia en lo sucesivo como "instrumentos 110-115"). La figura 1 es una representación de un sistema con múltiples divisiones, cada una de las cuales tiene múltiples instrumentos, y donde cada instrumento tiene por lo menos un procesador.

El sistema 100 de monitorización puede considerarse un sistema de monitorización "redundante" porque cada una de las divisiones 105 tiene instrumentos y/o componentes iguales o similares. Aunque cada una de las divisiones 105 incluye instrumentos iguales o similares, cada una de las divisiones 105 puede operar de acuerdo con diferentes frecuencias de reloj. Cada una de las divisiones 105 mide un tiempo (es decir un "tiempo de división") mediante el recuento de un número de registros que se hayan producido a partir de un tiempo de inicio deseado. Cada registro representa una cantidad de tiempo requerida para ejecutar una instrucción de programa de una tarea deseada. Puesto que cada división tiene una frecuencia de reloj diferente, una cantidad de tiempo requerida para ejecutar una tarea dada en cada división será también diferente. En consecuencia, un registro medido en una división representará una cantidad de tiempo diferente de otro registro medido en otra división. En varias realizaciones, las divisiones 105 del sistema 100 de monitorización puede ejecutar simultáneamente la misma tarea. En tales realizaciones, la velocidad a la cual se ejecuta la tarea variará dependiendo de la frecuencia de reloj de la división en la cual se ejecuta la tarea.

Adicionalmente, el sistema 100 de monitorización puede considerarse también un sistema de monitorización redundante porque, como se describe con detalle a continuación, cuando el número mínimo de las divisiones 105 (como se determina mediante la lógica de votación por ejemplo dos-de-cuatro) está indicado como una "disparo" y/o un "fallo", entonces el sistema puede desconectar un componente, dispositivo, sistema o, en algunas realizaciones, todo un NPP. Los términos "disparo" y/o "fallo" (o alternativamente una "disparo de reactor", "interrupción de emergencia", "inicio" y similares) pueden referirse a cualquier inicialización y/o activación de un procedimiento de apagado y/o accionamiento con respecto a un componente deseado, dispositivo, sistema y/o NPP. Por ejemplo, en el sistema 100 de monitorización, si una división (por ejemplo, la división 1) falla o está de alguna otra manera en estado de fallo y es incapaz de enviar una señal de disparo, una segunda división (por ejemplo, la división N), la cual puede estar configurada para monitorizar todas las condiciones de disparo, cuando se requieren, puede enviar la señal de disparo. Se puede usar la señal de disparo para tomar la división desconectada y/o fallada fuera de línea. De acuerdo con realizaciones de ejemplo en donde un sistema está configurado con cuatro divisiones, cada división puede recibir entradas de disparo de una de las otras divisiones y realizar un procedimiento de votación, con lo cual las divisiones votan si el sistema debe accionar un dispositivo externo (por ejemplo, interrumpir de emergencia el NPP). Una entrada fallida de una división puede ser considerada una disparo por las otras divisiones en un sistema a prueba de fallos o puede ser ignorada en otros sistemas.

Como se muestra en la figura 1, solamente dos divisiones 105 están presentes. Sin embargo, de acuerdo con varias realizaciones, cualquier número de divisiones, mayor a dos, puede estar presente. Adicionalmente, en varias realizaciones, las divisiones pueden ser dispositivos en red o pueden proporcionarse como un solo dispositivo.

De acuerdo con varias realizaciones, cada uno de los instrumentos 110-1 - 110-N (en donde $N \geq 2$) (a los cuales se hace referencia en lo sucesivo como "instrumentos 110") es un dispositivo físico de hardware para ordenador capaz de comunicarse con uno o más de otros dispositivos en lo sucesivo como "instrumentos 110") es un dispositivo físico de hardware para ordenador capaz de comunicarse con uno o más de otros dispositivos para ordenador capaz de comunicarse con uno o más de otros dispositivos de computación de hardware a través de una interfaz de comunicaciones, y los instrumentos 110 pueden incluir memoria, uno o más procesadores, y otros componentes de hardware similares. Los instrumentos 110 pueden estar configurados para enviar/recibir datos a/de otros dispositivos de hardware, tales como uno o más sensores (no mostrados), a través de una conexión óptica, alámbrica y/o inalámbrica (no mostrada). Por ejemplo, los instrumentos 110 pueden incluir uno o más dispositivos de hardware y/o componentes de software para medir y analizar un número y nivel de energía de neutrones haciendo colisión con uno o más detectores de neutrones asociados (no mostrados). De acuerdo con ello, los instrumentos 110 pueden actuar como un "portal" que recibe una o más señales de uno o más sensores, filtra y/o procesa las una o más señales recibidas, y reenvía las señales filtradas y/o procesadas a los instrumentos 115-1 - 115-N (donde $N \geq 2$) (a los cuales se hace referencia en lo sucesivo como "instrumentos 115").

De acuerdo con varias realizaciones, cada uno de los instrumentos 115 es un dispositivo físico de hardware para ordenador que realiza un procedimiento de votación basándose en la información de disparo recibida del instrumento 110 ubicado en la división 1 y/o la información de disparo recibida de otras divisiones. Para ello, los

instrumentos 115 pueden incluir uno o más dispositivos de hardware (por ejemplo, memoria, uno o más procesadores, y otros componentes de hardware similares) y/o componentes de software para llevar a cabo un procedimiento de votación, tal como un procedimiento de votación de dos-de-cuatro para un sistema de monitorización que tiene cuatro divisiones. Se usa el procedimiento de votación para determinar si una o más de las divisiones 105 está en una condición de disparo (o alternativamente, "desconectada"). Se usa a menudo un procedimiento de votación (o alternativamente, un sistema lógico de votación) para detectar discrepancias y/o inconsistencias en sistemas redundantes. En un sistema de votación, si una señal u otro mecanismo de votación similar no está disponible, se puede determinar que el sistema de votación entre en un modo degradado. Por ejemplo, si una división experimenta un CMF o de alguna otra manera está en peligro, una señal de la división puede ser detenida o de alguna otra manera interrumpida. Sin la señal de la división, o cuando se determina que se debe interrumpir la señal, el sistema de votación puede determinar que la división esté en condición de disparo. Si uno de los instrumentos 115 determina que se ha desconectado un número mínimo requerido de las divisiones 105, entonces el instrumento puede iniciar un procedimiento de disparo, de manera que el NPP u otro sistema similar se paraliza y/o desconecta. En varias realizaciones, en lugar de paralizar o excluir un sistema, un procedimiento de disparo puede iniciar uno o más sistemas y/o procedimiento de seguridad adicionales. En varias realizaciones, el procedimiento de disparo puede incluir emitir una notificación (o alternativamente, "marcado"), o puede implicar generar o de alguna otra manera definir un registro de base de datos u otra inscripción similar que contenga información que indique que existe una condición de disparo.

Debe indicarse que los instrumentos instrumento 110, instrumento 115, etc., se pueden agrupar entre sí o disponer de alguna otra manera, de manera lógica y/o física, basándose en un sistema deseado o una aplicación deseada. Como se muestra en la figura 1, únicamente un solo instrumento 110 y un solo instrumento 115, están presentes dentro de cada una de las divisiones 105. De acuerdo con varias realizaciones, las divisiones 105 pueden incluir cualquier número de los instrumentos 110-115. Adicionalmente, en varias realizaciones, puede haber muchos más instrumentos y/o componentes que los mostrados en la figura 1, tal como un dispositivo de control o un grupo de dispositivos de control, que gestione, mande, dirija y/o regule los varios instrumentos de las múltiples divisiones del sistema de monitorización 100. Sin embargo, no es necesario mostrar todos estos instrumentos y/o componentes generalmente convencionales a fin de exponer las realizaciones de ejemplo. Además, cabe mencionar que las realizaciones de ejemplo no están limitadas al sistema de votación que se describe y que pueden usar cualquier sistema lógico de votación por mayoría para iniciar una función de seguridad y/o un accionamiento de salvaguarda.

La figura 2 ilustra los componentes de un instrumento 200 (por ejemplo, los instrumentos 110 y/o instrumentos 115) que se emplean por la una o más divisiones (por ejemplo, las divisiones 105) de un sistema de monitorización (por ejemplo, el sistema 100 de monitorización), de acuerdo con una realización de ejemplo. Como se muestra, el instrumento 200 incluye un procesador 210, un bus 220, una interfaz 230 de entrada/salida y una memoria 255. Durante la operación, la memoria 255 incluye un sistema operativo 260, el cual incluye un reloj de división 261, un reloj 262 de sistema y un planificador 263; y el procesador 210 incluye las tareas 1-N (donde N es un número entero mayor o igual a 2). En algunas realizaciones, el instrumento 200 puede incluir muchos más componentes que los mostrados en la figura 2. Sin embargo, no es necesario mostrar todos estos componentes generalmente convencionales para exponer las realizaciones de ejemplo.

La memoria 255 puede ser un medio de almacenamiento legible por ordenador que incluye generalmente una memoria de acceso aleatorio (RAM), una memoria de solo lectura (ROM), y un dispositivo permanente de almacenamiento en masa, tal como una unidad de disco. La memoria 255 almacena también un sistema operativo 260, el cual incluye un reloj 261 de división, un reloj 262 de sistema, y un planificador 263.

El reloj 261 de división puede medir un tiempo de división que se puede implementar como un recuento de un número de registros de división que se hayan producido a partir de un tiempo y/o fecha de partida deseada. Una velocidad del reloj 261 de división se basa en una frecuencia de reloj que está definida para la división en la cual el instrumento 200 está instalado o con la cual está asociado de alguna otra manera. El reloj 262 de sistema puede medir un tiempo de sistema que se puede implementar como un recuento de un número de registros de sistema que se hayan producido a partir de un tiempo y/o fecha de partida deseada. Una velocidad del reloj 262 de sistema se basa en una frecuencia de reloj que está definida para el sistema de monitorización (por ejemplo, el sistema 100 de monitorización) con el cual está asociado el instrumento 200. El número de registros que representa el tiempo de sistema puede ser diferente en uno o más procesadores ubicados en cada división, y el tiempo de sistema puede ser una función de la velocidad a la cual se ejecutan o sincronizan el uno o más procesadores. Adicionalmente, cabe mencionar que los procesadores que tienen diferentes velocidades de reloj realizando las mismas tareas son inherentemente asíncronas, puede causar que la frecuencia de barrido a través de cada programa de aplicación opera a diferente frecuencia. Puesto que las operaciones de tarea se ejecutan de manera asíncrona, es poco probable que ocurran anomalías causadas por cierta secuencia de eventos en ambas divisiones.

Se pueden implementar las frecuencias de reloj para cada una del reloj 261 de división y el reloj 262 de sistema mediante el uso de cristales de oscilador, sistemas de control de bucles de bloqueo de fase, y/o cualquier otro dispositivo similar que genere una señal de referencia fija. Adicionalmente, cada cristal de oscilador, sistemas de control de bucles de bloqueo de fase, y/u otro dispositivo similar puede operar a diferentes frecuencias. Además, en varias realizaciones, el procesador 210 puede estar configurado para variar una velocidad de la frecuencia de reloj del reloj 261 de división basándose en la frecuencia del cristal de oscilador, sistema de control de bucles de bloqueo

de fase y algún otro dispositivo similar. En tales realizaciones, cada cristal de oscilador, sistemas de control de bucles de bloqueo de fase y/u otro dispositivo similar puede operar a la misma frecuencia, pero puede tener una frecuencia de reloj que sea variada por el procesador 210.

En varias realizaciones, cada uno del reloj 261 de división y del reloj 262 de sistema se puede implementar como temporizador programable de intervalos que interrumpe el procesador 210, el cual comienza entonces una interrupción de temporizador. En tales realizaciones, una vez que expira y/o termina una interrupción de temporizador para el reloj 261 de división, se le añade un registro de división al reloj 261 de división, y una vez que expira y/o termina una interrupción de temporizador para el reloj 262 de sistema, un registro de sistema al reloj 262 de sistema.

El planificador 263 puede implementar un procedimiento de planificación mediante el cual se les da acceso a tareas (por ejemplo, las tareas 1-N), subprocedimientos, procedimientos, y/o flujos de datos a los recursos del instrumento 200 (por ejemplo, el tiempo de operación en el procesador 210 y similares).

Adicionalmente, la memoria 255 puede incluir código de programa para arrancar, comenzar y/o inicializar el instrumento 200. Estos componentes de software pueden cargarse también desde un medio separado de almacenamiento legible por ordenador a la memoria 255 mediante el uso de un mecanismo de accionamiento (no mostrado). Este medio separado de almacenamiento legible por ordenador puede incluir una unidad de disquete, un disco, una cinta, una unidad de DVD/CD-ROM, una tarjeta de memoria y/u otro medio similar de almacenamiento legible por ordenador (no mostrado). En algunas realizaciones, se pueden cargar componentes de software a la memoria 255 de un dispositivo remoto de almacenamiento de datos (por ejemplo, los bases de datos 125A-D) a través de la interfaz 230 de entrada/salida, más bien que por un medio de almacenamiento legible por ordenador.

El procesador 210 puede estar configurado para llevar a cabo instrucciones de un programa informático mediante la realización de operaciones básicas aritméticas, lógicas y de entrada/salida del sistema. La memoria 255 puede proporcionar instrucciones al procesador 210 a través del bus 220. El procesador 210 está configurado para ejecutar el código de programa para las tareas 1-N. Se puede almacenar tal código de programa en un dispositivo de almacenamiento (por ejemplo, la memoria 255).

El bus 220 hace posible la comunicación y la transferencia de datos entre los componentes del elemento de red 200. El bus 220 puede comprender un bus en serie de alta velocidad, un bus paralelo, una red de área de almacenamiento (SAN) y/u otra tecnología de comunicación adecuada.

La interfaz 230 de entrada/salida es un componente de hardware para ordenador que conecta el instrumento 200 a los otros instrumentos en la división en la cual está implementado el instrumento 200, y/o a uno o más instrumentos de otras divisiones. La interfaz 230 de entrada/salida está configurada para recibir una o más señales de entrada de uno o más dispositivos de entrada y dar salida a una o más señales de salida a uno o más instrumentos y/o componentes. La interfaz 230 de entrada/salida puede conectar el instrumento 200 a otros instrumentos a través de una conexión óptica, alámbrica y/o inalámbrica.

La figura 3 ilustra un diagrama de temporización variable de reloj 300, de acuerdo con una realización de ejemplo. El diagrama de temporización variable de reloj 300 incluye divisiones 305-1 y 305-2; tiempo de sistema 307; tiempo de división 312-1 - 312-2; tiempo de inactividad 317-1 - 317-2; tiempo de división 312-1 - 312-2; tiempo de inactividad 317-1 - 317-2; instrucciones de programa 306-1 - 306-2; instrucciones de sistema 311-1 - 311-2; momentos 310-1 310-2, 315-1 - 315-2, 320-1 - 320-2, 325-1 - 325-2, 330-1 - 330-2, 335-1 - 335-2, 340-1 - 340-2, 345-1 - 345-2, y 350-1 - 350-2; y registros de división 313-1 - 313-2, 318-1 - 318-2, 323-1 - 323-2, 328-1 - 328-2, 333-1 - 333-2, 338-1 - 338-2, 343-1, y 348-1; y registros de sistema 355 - 360.

De acuerdo con varias realizaciones, las divisiones 305-1 - 305-2 tienen los instrumentos iguales o similar a los de las divisiones 1-4 como se analiza anteriormente con respecto a las figuras 1A-1B, cada una de las cuales tiene los componentes iguales o similar, como el instrumento 200, como se describe anteriormente con respecto a la figura 2. El diagrama de temporización variable de reloj 300 muestra la temporización de los eventos que se producen en cada una de las divisiones 305-1 y 305-2. El tiempo de sistema 307 muestra una temporización de los eventos que ocurren (por ejemplo, la ejecución de las tareas de sistema) en relación con un sistema de monitorización (por ejemplo, el sistema 100 de monitorización). El tiempo de sistema 307 opera de acuerdo con un reloj de sistema que es operado por un dispositivo de control del sistema de monitorización. El tiempo de división 312-1 muestra una temporización de los eventos que se producen (por ejemplo, las instrucciones de programa que son ejecutadas por la división 305-1) en relación con la división 305-1. El tiempo de división 312-1 opera de acuerdo con un reloj de división que está definido para la división 305-1. El tiempo de división 312-2 muestra una temporización de los eventos que ocurren (por ejemplo, las instrucciones de programa que son ejecutadas por la división 305-2) en relación con la división 305-2. El tiempo de división 312-2 opera de acuerdo con un reloj de división que está definido para la división 305-2. El tiempo de inactividad 317-1 muestra una temporización de inactividad en relación con la división 305-1. El tiempo de inactividad 317-2 muestra una temporización de inactividad en relación con la división 305-2. El término "inactividad" puede referirse a un retraso en el inicio de una ejecución de una siguiente instrucción de programa de una tarea.

Las instrucciones de programa 306-1 - 306-9 representan instrucciones de programa de una tarea, las cuales son ejecutadas por una correspondiente división. Como se muestra en la figura 3, cada una de las divisiones 305-1 - 305-2 ejecuta la misma tarea, y así, cada una de las divisiones 305-1 - 305-2 ejecuta las mismas instrucciones de programa. Como se muestra, las instrucciones de programa 306-1 - 306-9 son ejecutadas por la división 305-1, y las instrucciones de programa 306-1 - 306-7 son ejecutadas por la división 305-2. Adicionalmente, algunas de las instrucciones de programa 306-1 - 306-9 pueden depender de una instrucción de sistema 311-1 - 311-3 ejecutada por el sistema de monitorización. Cada una de las instrucciones de programa 306-1 - 306-9 puede incluir uno o más operaciones de gestión de datos, una o más operaciones aritméticas y/o lógicas, una o más operaciones de flujo de control y/o una o más operaciones adicionales similares. Cada una de las instrucciones de programa 306-1 - 306-9 puede tener una longitud de instrucción de programa de cualquier tamaño. Cada una de las instrucciones de programa 306-1 - 306-9 puede tener una longitud igual o similar de instrucción de programa, o puede tener longitudes variables de instrucción de programa.

Las instrucciones de sistema 311-1 - 311-2 representan instrucciones de programa de la tarea, que son ejecutadas por un procesador central del sistema de monitorización. Como se muestra, las instrucciones de sistema 311-1 - 311-3 son ejecutadas por el sistema de monitorización y dependen de una instrucción de programa ejecutada por la división 305-1 y dependen también de una instrucción de programa ejecutada por la división 305-2. Cada una de las instrucciones de sistema 311-1 - 311-2 puede incluir una o más operaciones de manejo de datos, una o más operaciones aritméticas y/o lógicas, una o más operaciones de flujo de control y/o una o más operaciones adicionales similares. Cada una de las instrucciones de sistema 311-1 - 311-3 puede tener una longitud de instrucción de programa de cualquier tamaño. Cada una de las instrucciones de sistema 311-1 - 311-3 puede tener una longitud igual o similar de instrucción de programa, o puede tener longitudes variables de instrucción de programa.

De acuerdo con varias realizaciones, los momentos 310-1 - 310-5 2, 315-1 - 315-2, 320-1 - 320-2, 325-1 - 325-2, 330-1 - 330-2, 335-1 - 335-2, 340-1 - 340-2, 345-1 - 345-2, y 350-1 - 350-2 representan un tiempo en el cual una instrucción de programa 306-1 - 306-2 es ejecutada por las divisiones 305-1 - 305-2.

De acuerdo con varias realizaciones, los registros de división 313-1 - 313-2, 318-1 - 318-2, 323-1 - 323-2, 328-1 - 328-2, 333-1 - 333-2, 338-1 - 338-2, 343-1, y 348-1 representan una cantidad de tiempo (o alternativamente, un intervalo de tiempo) requerida para ejecutar una instrucción de programa de la tarea en una correspondiente división. Las frecuencias de reloj definidas para cada una de las divisiones 305-1 - 305-2 definen una frecuencia a la cual cada instrucción de programa 306-1 - 306-2 es ejecutada en las divisiones 305-1 - 305-2. Cada una de las divisiones 305-1 - 305-2 mide un tiempo de división 312-1 - 312-2 mediante el recuento de un número de registros que se hayan producido a partir de un tiempo de inicio deseado.

Como se muestra en la figura 3, la división 305-1 tiene un menor registro entre las instrucciones de programa de ejecución en relación con la división 305-2. Así, la división 305-1 tiene una mayor frecuencia de reloj que la división 305-2. De acuerdo con ello, la división 305-1 es capaz ejecutar más instrucciones de programa que la división 305-2 en una cantidad de tiempo deseada. A manera de ejemplo, la división 305-1 puede tener una frecuencia de reloj de 60 megahertzios (MHz) y la división 305-2 puede tener una frecuencia de reloj de 50 MHz y, así, como se muestra en la figura 3, la división 305-1 ejecuta nueve instrucciones de programa (por ejemplo, las instrucciones de programa 306-1 - 306-9), mientras que la división 305-2 ejecuta siete instrucciones de programa (por ejemplo, las instrucciones de programa 306-1 - 306-7) en la misma cantidad de tiempo. Cabe mencionar que el número de instrucciones de programa ejecutadas por ciclo de reloj puede no ser constante para cada una de las divisiones 305-1 - 305-2. El número de instrucciones de programa ejecutadas por ciclo de reloj puede depender de una arquitectura de hardware que esté siendo empleada por la división en la cual la tarea se está ejecutando, cómo actúe recíprocamente cada instrucción de programa con el procesador de la división y/o un dispositivo de control del sistema de monitorización, y/o un tiempo de retraso en el inicio de una ejecución de una siguiente instrucción de programa.

Adicionalmente, en varias realizaciones de ejemplo, un dispositivo de control del sistema de monitorización (no mostrado) puede variar las frecuencias de reloj de cada una de las divisiones 305-1 - 305-2, de manera que la división 305-2 tenga una mayor frecuencia que la de la división 305-1 (no mostrada).

De acuerdo con varias realizaciones, los registros de sistema 355 - 360 representan una cantidad de tiempo (o alternativamente, un intervalo de tiempo) requerida para ejecutar una instrucción de programa de la tarea por un dispositivo de control del sistema de monitorización. Las frecuencias de reloj definidas para el sistema de monitorización definen una frecuencia a la cual cada instrucción de programa es ejecutada por el dispositivo de control el sistema de monitorización. El sistema de monitorización mide un tiempo de sistema 307 mediante el recuento de un número de registros de sistema que se hayan producido a partir de un tiempo de inicio deseado. Puesto que el tiempo de sistema 307 es el mismo para cada división, el tiempo de sistema puede servir de tiempo de referencia para cada una de las divisiones en el sistema de monitorización.

De acuerdo con varias realizaciones, los registros de división 313-1 - 313-2, 318-1 - 318-2, 323-1 - 323-2, 328-1 - 328-2, 333-1 - 333-2, 338-1 - 338-2, 343-1 y 348-1 pueden incluir también un tiempo de ejecución y un tiempo de retraso (o alternativamente, un tiempo de espera) en el inicio de una ejecución de una siguiente instrucción de programa. En tales realizaciones, un registro (por ejemplo,) puede estar representado por el tiempo de ejecución

más un tiempo de retraso. Por ejemplo, como se muestra en la figura 3, el registro de división 313-2 está representado por el tiempo de ejecución 365 y el tiempo de retraso 370. Incorporando un tiempo de retraso a un registro, se puede expandir la operación asíncrona de cada división de la división de monitorización, y así, el CMF relacionado con el software puede reducirse, mitigarse o de alguna otra manera evitarse aún más. Cabe mencionar que, además de cada división que opere de acuerdo con diferente frecuencia de reloj, en varias realizaciones, cada división puede tener diferente tiempo de retraso.

Como se apreciará, los procedimientos y aparatos de acuerdo con las realizaciones de ejemplo tienen varias ventajas. En primer lugar, las realizaciones de ejemplo permiten variar una velocidad de reloj para cada división de un sistema de monitorización, de manera que las tareas que se ejecutan en diferentes divisiones tienen diferente temporización de programa, lo cual permite que cada división sea asíncrona una en relación con otra en el sistema de monitorización, reduciendo y/o mitigando así los CMF relacionados con el software. En segundo lugar, las realizaciones de ejemplo son rentables porque las realizaciones de ejemplo permiten usar múltiples divisiones redundantes de aplicaciones relacionadas con la seguridad nuclear sin nuevos diseños de hardware.

Esta descripción escrita usa ejemplos de la materia objeto descrita para permitir que cualquier persona experta en la técnica practique la misma, incluyendo el hacer o usar cualesquiera dispositivos o sistemas y efectuando cualquiera de los procedimientos incorporados. El alcance patentable de la materia objeto es definido por las reivindicaciones.

REIVINDICACIONES

1. Un sistema (100) informático para ejecutar una tarea de acuerdo con diferentes frecuencias de reloj para reducir fallos de modo común en el sistema informático, comprendiendo el sistema informático:

por lo menos una primera división (105-1) y una segunda división (105-N), teniendo la primera división una primera frecuencia de reloj y teniendo la segunda división una segunda frecuencia de reloj, incluyendo cada una de la primera división (105-1) y la segunda división (105-N) un respectivo instrumento (110, 115);
un primer procesador configurado para ejecutar una tarea en la primera división (105-1) de acuerdo con la primera frecuencia de reloj; y
un segundo procesador configurado para ejecutar la tarea en la segunda división (105-N) de acuerdo con la segunda frecuencia de reloj,
en el que cada respectivo instrumento (110, 115) de la primera división (105-1) y la segunda división (105-2) está configurado para:

determinar si una o más de las divisiones está en una condición de disparo, en el que una condición de disparo es indicativa de una inicialización y/o activación de un procedimiento de apagado y/o accionamiento, basándose en la detección de una discrepancia de al menos una de la primera división (105-1) y la segunda división (105-2);
determinar si una división está en un estado de fallo y no puede enviar una señal de disparo; y
accionar el dispositivo externo basándose en una determinación, basándose en un procedimiento de votación, de que existe al menos una condición de disparo y un estado de fallo.

2. El sistema (100) informático de la reivindicación 1, en el que la primera frecuencia de reloj tiene una velocidad diferente de la segunda frecuencia de reloj.

3. El sistema (100) informático de cualquier reivindicación anterior, en el que la tarea se ejecuta simultáneamente en la primera división y en la segunda división.

4. El sistema (100) informático de cualquier reivindicación anterior, que comprende, además:

la primera división (105-1) comprende un reloj (261) de primera división configurado para medir un tiempo de primera división mediante el recuento de un número de registros de primera división que se hayan producido a partir del tiempo de inicio deseado, en que cada registro de primera división representa una cantidad de tiempo requerida para ejecutar una instrucción de programa de la tarea de acuerdo con la frecuencia de reloj de primera división, y
la segunda división (105-N) comprende un reloj de segunda división configurado para medir un tiempo de segunda división mediante el recuento de un número de registros de segunda división que se hayan producido a partir del tiempo de inicio deseado, en que cada registro de segunda división representa una cantidad de tiempo requerida para ejecutar una instrucción de programa de la tarea de acuerdo con la frecuencia de reloj de segunda división.

5. El sistema (100) informático de la reivindicación 4, que comprende, además:

un reloj (262) de sistema configurado para medir un tiempo de sistema mediante el recuento de un número de registros de sistema que se hayan producido a partir de un tiempo de inicio deseado, teniendo el reloj de sistema una frecuencia de reloj de sistema, representando cada registro de sistema una cantidad de tiempo requerida para ejecutar una instrucción de programa de la tarea de acuerdo con la frecuencia de reloj de sistema.

6. El sistema (100) informático de la reivindicación 5, en el que por lo menos uno de

(i) cada uno de los registros de primera división representa tanto la cantidad de tiempo requerida para ejecutar una instrucción de programa de la tarea de acuerdo con la frecuencia de reloj de primera división como un retraso en el inicio de una ejecución de una siguiente instrucción de programa de la tarea, y
(ii) cada uno de los registros de segunda división representa tanto la cantidad de tiempo requerida para ejecutar una instrucción de programa de la tarea de acuerdo con la frecuencia de reloj de segunda división como un retraso en el inicio de la ejecución de la siguiente instrucción de programa de la tarea.

7. El sistema (100) informático de la reivindicación 5 o 6, en el que
el primer procesador está configurado, además, para variar la ejecución de la tarea en la primera división basándose en por lo menos uno de la frecuencia de reloj de primera división y el tiempo de sistema; y
el segundo procesador está configurado además para variar la ejecución de la tarea en la segunda división basándose en por lo menos uno de la frecuencia de reloj de segunda división y el tiempo de sistema.

8. El sistema (100) informático de cualquier reivindicación anterior, en el que
los instrumentos (110, 115) están también configurados para realizar un procedimiento de votación divisional basándose en la información de disparo, utilizándose el procedimiento de votación divisional para detectar discrepancias de por lo menos una de la primera división y la segunda división.

9. Un procedimiento para ejecutar una tarea para reducir fallos de modo común en un sistema informático, comprendiendo el procedimiento:

dividir el sistema (100) informático en una primera división (105-1) y una segunda división (105-N), incluyendo cada una de la primera división (105-1) y la segunda división (105-N) un respectivo instrumento (110, 115);
definir una primera frecuencia de reloj para la primera división y una segunda frecuencia de reloj para la segunda división;
ejecutar la tarea en la primera división (105-1) usando un primer procesador de acuerdo con una primera frecuencia de reloj;
ejecutar la tarea en la segunda división (105-2) usando un segundo procesador de acuerdo con una segunda frecuencia de reloj;
en el que cada respectivo instrumento (110, 115) de la primera división (105-1) y la segunda división (105-2) es capaz de:

determinar si una o más de las divisiones está en una condición de disparo, en el que una condición de disparo es indicativa de una inicialización y/o activación de un procedimiento de apagado y/o accionamiento, basándose en la detección de una discrepancia de al menos una de la primera división (105-1) y la segunda división (105-2);
determinar si una división está en un estado de fallo y no puede enviar una señal de disparo; y
accionar un dispositivo externo basándose en una determinación, basándose en un procedimiento de votación, de que existe al menos una condición de disparo y un estado de fallo.

10. El procedimiento de la reivindicación 9, en el que la ejecución también comprende:

ejecutar simultáneamente la tarea en la primera división (105-1) y en la segunda división (105-N).

11. El procedimiento de la reivindicación 9 o la reivindicación 10, en el que el procesador opera de acuerdo con un reloj (262) de sistema, y el procedimiento también comprende:

definir un reloj de primera división para la primera división (105-1) para medir un tiempo de primera división mediante el recuento de un número de registros de primera división que se hayan producido a partir del tiempo de inicio deseado, representando cada registro de primera división una cantidad de tiempo requerida para ejecutar una instrucción de programa de la tarea de acuerdo con la frecuencia de reloj de primera división, y
definir un reloj de segunda división para la segunda división (105-N) para medir un tiempo de segunda división mediante el recuento de un número de registros de segunda división que se hayan producido a partir del tiempo de inicio deseado, representando cada registro de segunda división una cantidad de tiempo requerida para ejecutar una instrucción de programa de la tarea de acuerdo con la frecuencia de reloj de segunda división.

12. El procedimiento de la reivindicación 11, que comprende, además:

medir un tiempo de sistema mediante el recuento de un número de registros de sistema que se hayan producido a partir de un tiempo de inicio deseado, en que el reloj de sistema tiene una frecuencia de reloj de sistema, cada registro de sistema representa una cantidad de tiempo requerida para ejecutar una instrucción de programa de la tarea de acuerdo con la frecuencia de reloj de sistema.

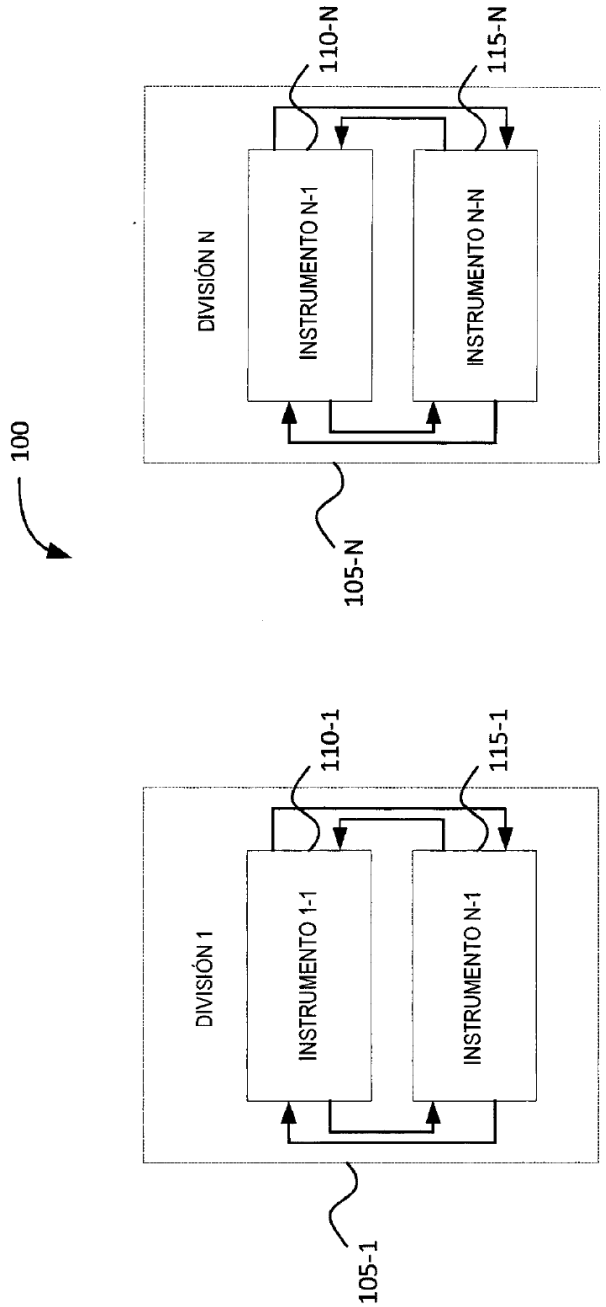
100
110-N
115-N
DIVISIÓN N
INSTRUMENTO N-1
INSTRUMENTO N-N
105-N
110-1
115-1
DIVISIÓN 1
INSTRUMENTO 1-1
INSTRUMENTO N-1
105-1

FIG. 1

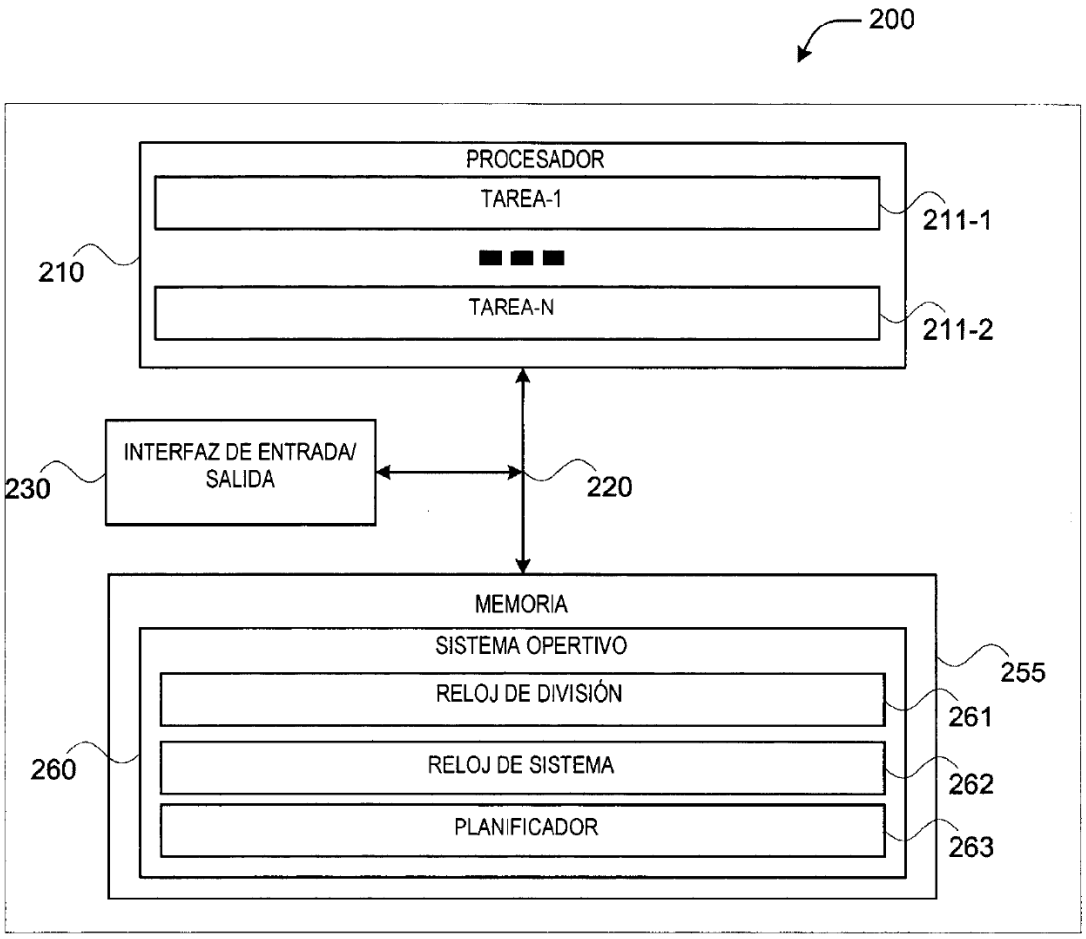
200
PROCESADOR
TAREA-1
211-1
210
TAREA-N
211-2
INTERFAZ DE ENTRADA/ SALIDA
230
220
MEMORIA
SISTEMA OPERTIVO
255
RELOJ DE DIVISIÓN
261
260
RELOJ DE SISTEMA
262
PLANIFICADOR
263

FIG. 2

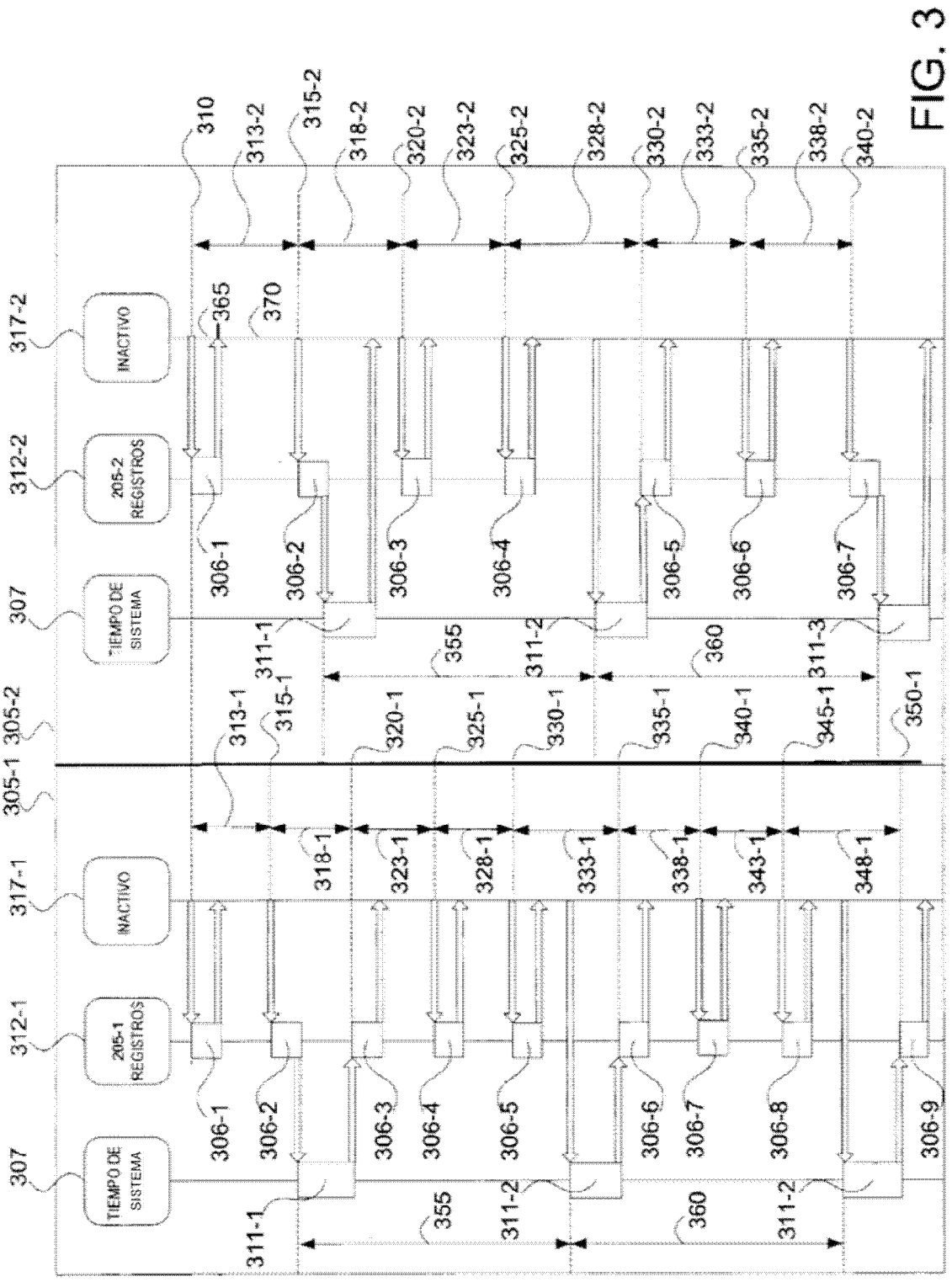
TIEMPO DE SISTEMA
205-1 REGISTROS
INACTIVO
TIEMPO DE SISTEMA
205-2 REGISTROS
INACTIVO
307
312-1
317-1
305-1
305-2
307
312-2
317-2
306-1
306-2
306-3
306-4
306-5
306-6
306-7
306-8
306-9
310
313-1
313-2
315-1
315-2
318-1
318-2
320-1
320-2
323-1
323-2
325-1
325-2
328-1
328-2
330-1
330-2
333-1
333-2
335-1
335-2
338-1
338-2
340-1
340-2
343-1
345-1
348-1
350-1
355
360
365
370
311-1
311-2
311-3

FIG. 3