(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 796 083**

(51) Int. CI.:

G05B 9/02 (2006.01)
B61L 15/00 (2006.01)
G06F 11/07 (2006.01)
G06F 11/14 (2006.01)
G06F 11/16 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **18.12.2015 E 15201096 (3)**

(97) Fecha y número de publicación de la concesión europea: **20.05.2020 EP 3035135**

(54) Título: **Procedimiento de parada de emergencia y sistema de seguridad asociado**

(30) Prioridad:

19.12.2014 FR 1462968

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.11.2020

(73) Titular/es:

CLEARSY (100.0%)
320 avenue Archimède Zone d'Activités Commerciales de la Duranne Immeuble les Pléiades III Bat à
13857 Aix-en-Provence, FR

(72) Inventor/es:

SABATIER, DENIS y
PATIN, FLORENT

(74) Agente/Representante:

SALVÀ FERRER, Joan

DESCRIPCIÓN

Procedimiento de parada de emergencia y sistema de seguridad asociado

[0001] La presente invención se refiere a un procedimiento de parada de emergencia de un elemento de seguridad de un conjunto de seguridad, comprendiendo el conjunto de seguridad el elemento de seguridad y un sistema de seguridad. La presente invención se refiere también al sistema de seguridad asociado.

[0002] En el campo de los sistemas eléctricos, se conoce el intentar buscar limitar los riesgos de averías. El estándar SIL, acrónimo de "*Security Integrity Level*", que significa nivel de integridad de seguridad, se utiliza para evaluar la fiabilidad de las funciones de seguridad de los sistemas eléctricos y electrónicos programables. Un SIL se define como un nivel relativo de reducción de riesgo inherente a una función de seguridad, o como una especificación de un objetivo de reducción de riesgo. Más sencillamente, es una medida del rendimiento esperado para una función de seguridad. El estándar SIL se define según cuatro niveles de seguridad. El nivel más alto es SIL4.

[0003] En el campo de la seguridad ferroviaria, a menudo se requiere un nivel SIL 4, por ejemplo, para frenar trenes o para abrir puertas de andén.

[0004] Para cumplir con tal nivel de seguridad, los sistemas electrónicos que controlan los elementos de seguridad que constituyen, por ejemplo, los elementos de apertura y cierre de puertas de vagones o plataformas deben ser lo más seguros posible.

[0005] Para mejorar el nivel de seguridad de un sistema electrónico, se conoce el uso de un microprocesador de control que verifica el estado de otro microprocesador en funcionamiento. El microprocesador de control desencadena una detención de los elementos de seguridad y del sistema en caso de avería del microprocesador en funcionamiento.

[0006] Sin embargo, en el caso de un fallo del microprocesador de control, existe un riesgo significativo de avería no detectada del sistema. Además, ciertos fallos del microprocesador de control evitan la activación de la detención de los elementos de seguridad.

[0007] Por lo tanto, existe la necesidad de un procedimiento de parada más fiable.

[0008] Para ello, se propone un procedimiento de parada de emergencia de un elemento de seguridad de un conjunto de seguridad según la reivindicación 1, comprendiendo el conjunto de seguridad el elemento de seguridad y un sistema de seguridad. El sistema de seguridad comprende un primer núcleo. El primer núcleo comprende dos primeros programas de cálculo capaces de realizar las mismas operaciones, y un primer programa de parada capaz de implementar una parada de emergencia. El sistema de seguridad comprende además un segundo núcleo. El segundo núcleo comprende dos segundos programas de cálculo capaces de realizar las mismas operaciones, y un segundo programa de parada capaz de implementar una parada de emergencia. El procedimiento comprende una primera etapa de realización de operaciones en los dos primeros programas de cálculo, dando lugar cada realización de operaciones en un primer programa de cálculo a un primer resultado. El procedimiento comprende además una primera etapa de comparación de los dos primeros resultados, siendo una anomalía del primer núcleo detectada si los dos primeros resultados difieren. El procedimiento comprende también una primera etapa de deducción del estado del sistema, al final de la cual, si se detecta una anomalía del primer núcleo, una tercera etapa de parada se implementa por el segundo programa de parada del segundo núcleo, si no se detecta ninguna anomalía del primer núcleo, se implementan las segundas etapas. Las segundas etapas comprenden una segunda etapa de realización de operaciones en los dos segundos programas de cálculo, dando lugar cada realización de operaciones en un segundo programa de cálculo a un segundo resultado. Las segundas etapas comprenden también una segunda etapa de comparación de los dos segundos resultados, siendo una anomalía del segundo núcleo detectada si los dos segundos resultados difieren. Las segundas etapas comprenden además una segunda etapa de deducción del estado del sistema, al final de la cual, si se detecta una anomalía del segundo núcleo, una cuarta etapa de parada se implementa por el primer programa de parada del primer núcleo, si no se detecta ninguna anomalía del segundo núcleo, las primeras etapas se repiten. Las primeras etapas y las segundas etapas se repiten siempre que no se detecte ninguna anomalía del primer núcleo o del segundo núcleo.

[0009] Según las realizaciones particulares, el procedimiento de parada de emergencia de un elemento de seguridad comprende una o más de las siguientes características, tomadas de forma aislada o en cualquier combinación técnicamente posible:

- el primer núcleo comprende programas que tienen instrucciones, tablas de constantes, registros de configuración, circuitos electrónicos y primeros elementos estáticos, comprendiendo los primeros elementos estáticos las instrucciones de los programas del primer núcleo y al menos un elemento seleccionado del grupo constituido por las tablas de constantes del primer núcleo, los registros de configuración del primer núcleo y los circuitos electrónicos del primer núcleo. El segundo núcleo comprende programas que tienen instrucciones, tablas de constantes, registros de

configuración, circuitos electrónicos y segundos elementos estáticos, comprendiendo los segundos elementos estáticos las instrucciones de los programas del segundo núcleo y al menos un elemento seleccionado del grupo constituido por las tablas de constantes del segundo núcleo, los registros de configuración del segundo núcleo y los circuitos electrónicos del segundo núcleo. El procedimiento comprende además una etapa de almacenamiento de los primeros elementos estáticos, una etapa de almacenamiento de los segundos elementos estáticos, una primera etapa de verificación de los primeros elementos estáticos, siendo una anomalía del primer núcleo detectada si los primeros elementos estáticos difieren de los primeros elementos estáticos almacenados del primer núcleo, y una segunda etapa de verificación de los segundos elementos estáticos, siendo una anomalía del segundo núcleo detectada si los segundos elementos estáticos del segundo núcleo difieren de los segundos elementos estáticos almacenados del segundo núcleo.

- el primer núcleo incluye una primera memoria y es capaz de implementar una primera serie de operaciones predeterminadas que dan lugar a un primer resultado conocido, y el segundo núcleo incluye una segunda memoria y es capaz de implementar una segunda serie de operaciones predeterminadas que dan lugar a un segundo resultado conocido, y el procedimiento comprende una etapa de almacenamiento del primer resultado conocido, una etapa de almacenamiento del segundo resultado conocido, una primera etapa de cálculo, durante la cual el primer núcleo realiza la primera serie de operaciones predeterminadas que dan lugar a un primer elemento calculado, una etapa de comparación del primer resultado conocido con el primer elemento calculado, siendo una anomalía del primer núcleo detectada si el primer elemento calculado y el primer resultado conocido difieren, una segunda etapa de cálculo, durante la cual el segundo núcleo realiza la segunda serie de operaciones predeterminadas que dan lugar a un segundo elemento calculado, y una etapa de comparación del segundo resultado conocido con el segundo elemento calculado, siendo una anomalía del segundo núcleo detectada si el segundo elemento calculado y el segundo resultado conocido difieren.

- el primer núcleo comprende un primer reloj, y el segundo núcleo comprende un segundo reloj, incluyendo el procedimiento una primera etapa de control del desfase de los relojes, implementada por el segundo núcleo, siendo una anomalía del primer núcleo detectada si el desfase del primer reloj, con respecto al segundo reloj, es superior o igual a un umbral de tolerancia predeterminado, y una segunda etapa de control del desfase de los relojes implementada por el primer núcleo, siendo una anomalía del segundo núcleo detectada si el desfase del segundo reloj, con respecto al primer reloj, es superior o igual a un umbral de tolerancia predeterminado.

- cada primer programa de cálculo comprende un primer programa, generando una ejecución nominal de dicho al menos un primer programa variaciones de los datos de un primer conjunto de datos, y cada segundo programa de cálculo comprende un segundo programa, generando una ejecución nominal de dicho al menos un segundo programa variaciones de los datos de un segundo conjunto de datos, y en el que las primeras etapas se aplican para todas las variaciones del primer conjunto de datos que la ejecución nominal de dicho al menos un primer programa es capaz de generar, siendo cada variación una realización de operación, y las segundas etapas se aplican para todas las variaciones del segundo conjunto de datos que la ejecución nominal de dicho al menos un segundo programa es capaz de generar, siendo cada variación una realización de operación.

- la primera etapa de comparación de los dos primeros resultados se implementa por el segundo núcleo y la segunda etapa de comparación de los dos segundos resultados se implementa por el primer núcleo.

- el primer núcleo comprende, además, una primera memoria y el segundo núcleo comprende, además, una segunda memoria, y en el que el primer programa de parada incluye un primer programa de borrado de al menos una parte del contenido de la primera memoria, el segundo programa de parada incluye un segundo programa de borrado de la segunda memoria, la tercera etapa de parada incluye una etapa de borrado de al menos una parte del contenido de la segunda memoria del segundo núcleo por el segundo núcleo, y la cuarta etapa de parada incluye una etapa de borrado de al menos una parte del contenido de la primera memoria del primer núcleo por el primer núcleo.

- la tercera etapa de parada incluye una etapa de parada de transmisión de una instrucción de continuación al primer núcleo, y la cuarta etapa de parada incluye una etapa de parada de transmisión de una instrucción de continuación al segundo núcleo.

- cada primer resultado incluye una pluralidad de datos ordenados según un índice creciente, correspondiendo cada dato a un índice idéntico para los dos primeros programas de cálculo, comprendiendo la primera etapa de comparación una comparación para cada índice de los datos de cada primer programa de cálculo asociados con el índice particular, siendo una anomalía del primer núcleo detectada si los valores difieren, y en el que cada segundo resultado incluye una pluralidad de datos ordenados según un índice creciente, correspondiendo cada dato a un índice idéntico para los dos segundos programas de cálculo, comprendiendo la segunda etapa de comparación una comparación para cada índice de los datos de cada segundo programa de cálculo asociados con el índice particular, siendo una anomalía del segundo núcleo detectada si los valores difieren.

[0010] La invención se refiere también a un sistema de seguridad según la reivindicación 10, comprendiendo el sistema de seguridad un primer núcleo que comprende dos primeros programas de cálculo capaces de realizar las mismas operaciones, y un primer programa de parada capaz de implementar una parada de emergencia. El sistema de seguridad comprende también un segundo núcleo que comprende dos segundos programas de cálculo capaces de realizar las mismas operaciones, y un segundo programa de parada capaz de implementar una parada de emergencia. El sistema de seguridad es capaz de implementar el procedimiento de parada de emergencia que se ha descrito anteriormente.

[0011] Otras características y ventajas de la invención se desprenderán de la lectura de la descripción que se ofrece a continuación de realizaciones de la invención, proporcionada a modo de ejemplo únicamente y en referencia a los dibujos que son:

- figura 1, un diagrama de un conjunto de seguridad que incluye un sistema de seguridad según la invención, y
- figura 2, un diagrama de flujo de un ejemplo de implementación de un procedimiento de parada de emergencia del elemento de seguridad del conjunto de seguridad de la figura 1 según una primera realización.

[0012] En la figura 1 se muestra un conjunto de seguridad 1. El conjunto de seguridad 1 comprende un elemento de seguridad 2 y un sistema de seguridad 4 para el procesamiento de datos, según la invención.

[0013] El sistema de seguridad 4 y el elemento de seguridad 2 son distintos y están físicamente separados. El sistema de seguridad 4 y el elemento de seguridad 2 son capaces, por ejemplo, de intercambiar datos por medio de un bus de intercambio de datos 6.

[0014] El elemento de seguridad 2 es, por ejemplo, un elemento de apertura y cierre de puertas de vagones.

[0015] El elemento de seguridad 2 presenta, por ejemplo, un estado operativo de seguridad y un estado de parada de seguridad. Por ejemplo, en el estado de parada de seguridad del elemento de seguridad 2, se corta la alimentación del elemento de seguridad 2. Además, el elemento de seguridad 2 es capaz de mantenerse en el estado de parada de seguridad, una vez que el elemento de seguridad 2 está en el estado de parada de seguridad.

[0016] El sistema de seguridad 4 es capaz de garantizar un funcionamiento seguro del elemento de seguridad 2 del conjunto de seguridad 1.

[0017] Para ello, el sistema de seguridad 4 es particularmente capaz de implementar un procedimiento de parada de emergencia del elemento de seguridad 2. La parada de emergencia del elemento de seguridad 2 permite el paso del elemento de seguridad 2 al estado de parada de seguridad.

[0018] El sistema de seguridad 4 comprende un primer núcleo 10_1 y un segundo núcleo 10_2.

[0019] El primer núcleo 10_1 y el segundo núcleo 10_2 son distintos y están físicamente separados. Como alternativa, los núcleos 10_1, 10_2 pertenecen al mismo procesador.

[0020] El primer núcleo 10_1 es capaz de intercambiar datos con el segundo núcleo 10_2 por medio de un enlace de intercambio de datos 14, por ejemplo, un bus de intercambio de datos.

[0021] El segundo núcleo 10_2 es idéntico al primer núcleo 10_1.

[0022] Para simplificar la descripción, solo se describirá en detalle el primer núcleo 10_1.

[0023] El primer núcleo 10_1 es capaz de procesar datos. Por ejemplo, el primer núcleo 10_1 es un procesador, particularmente un microprocesador. El primer núcleo 10_1 comprende programas que tienen instrucciones, tablas de constantes, registros de configuración y circuitos electrónicos.

[0024] El siguiente ejemplo permite ilustrar cada uno de estos términos para proporcionar una definición.

[0025] En el ejemplo, un procesador comprende un programa destinado a activar un puerto de salida cada vez que el procesador recibe un cierto número en un bus serie.

[0026] Un bus serie es un conjunto de enlaces físicos que permiten transmitir información bit a bit.

[0027] El programa de ejemplo comprende las siguientes instrucciones: "leer el valor recibido en el bus serie", "si el valor es inferior al valor umbral, configurar el puerto de salida en 1".

[0028] La tabla de constantes comprende, por ejemplo, los valores de umbral necesarios para el programa y los otros valores de constantes necesarios durante la inicialización del programa.

[0029] El circuito electrónico es un elemento de hardware capaz de recibir y ejecutar las instrucciones del programa.

[0030] En el ejemplo, un circuito electrónico es capaz de recibir el número del bus serie y activar el puerto de salida del procesador.

[0031] Un registro es una memoria legible por el circuito electrónico que comprende la información necesaria

para que el circuito electrónico interprete las instrucciones.

[0032] Se denominan registros de configuración los registros cuyo contenido permite ajustar los elementos de hardware.

[0033] En el ejemplo, el registro de configuración incluye la velocidad a la que el circuito debe recibir los valores en el bus serie. Durante la inicialización del procesador, la información de velocidad se carga en el registro de configuración desde la tabla de constantes.

[0034] Además, el primer núcleo 10_1 comprende dos primeros programas de cálculo 16_1, 18_1, un primer reloj H_1 y una primera memoria M_1.

[0035] El primer núcleo 10_1 es capaz de garantizar la parada de emergencia del elemento de seguridad 2.

[0036] El primer núcleo 10_1 es capaz de detectar una anomalía, como se describirá más adelante.

[0037] Además, el primer núcleo 10_1 es capaz de transmitir una instrucción de continuación al segundo núcleo 10_2. Una instrucción de continuación es una instrucción para que el núcleo que la recibe continúe en funcionamiento.

[0038] Además, el primer núcleo 10_1 es capaz de continuar en funcionamiento después de la recepción de una instrucción de continuación.

[0039] Los dos primeros programas de cálculo 16_1, 18_1 son capaces de realizar las mismas operaciones de procesamiento de datos con el fin de garantizar una redundancia. En otras palabras, desde un punto de vista funcional, los dos primeros programas de cálculo 16_1, 18_1 son réplicas exactas entre sí.

[0040] Los dos primeros programas de cálculo 16_1, 18_1 son capaces de realizar las mismas operaciones de forma independiente, es decir, sin utilizar los datos procesados por el otro.

[0041] Los primeros programas de cálculo 16_1, 18_1 son, por ejemplo, idénticos e incluyen los mismos componentes de software y/o hardware.

[0042] Cada primer programa de cálculo 16_1, 18_1 incluye un módulo de comparación 20, al menos un primer programa P_1 y un primer programa de parada PA_1.

[0043] El módulo de comparación 20 es capaz de comparar dos datos y de detectar una anomalía si los datos difieren.

[0044] Una ejecución nominal de dicho al menos un primer programa P_1 por cada primer programa de cálculo 16_1, 18_1 es una realización de operaciones que genera una variación de un primer conjunto de datos.

[0045] El primer programa de parada PA_1 permite garantizar una parada del elemento de seguridad 2 en caso de emergencia, por ejemplo, cuando se detecta una anomalía.

[0046] El primer programa de parada PA_1 es capaz de transmitir instrucciones de parada de emergencia al elemento de seguridad 2. Las instrucciones de parada de emergencia permiten el paso del elemento de seguridad 2 al estado de parada de seguridad.

[0047] Además, el primer programa de parada PA_1 es capaz de detener la transmisión de la instrucción de continuación al segundo núcleo 12_1.

[0048] El primer programa de parada PA_1 incluye, ventajosamente, un primer programa de borrado de al menos una parte del contenido de los primeros programas de cálculo 16_1, 18_1 y de al menos una parte del contenido de la primera memoria M_1.

[0049] El primer reloj H_1 es capaz de emitir una señal regular. El primer reloj permite, por ejemplo, la cadencia de los programas del primer núcleo 10_1.

[0050] La primera memoria M_1 se comparte para los dos primeros programas de cálculo 16_1, 18_1. Como alternativa, el primer núcleo 10_1 incluye una primera memoria M_1 distinta asociada a cada primer programa de cálculo 16_1, 18_1.

[0051] La primera memoria M_1 es capaz de almacenar los primeros elementos estáticos del primer núcleo 10_1.

[0052] El término " elementos estáticos" designa los elementos que se supone que no varían en el primer núcleo 10_1 o en el segundo núcleo 10_2. Estos elementos estáticos son, por ejemplo, instrucciones de registro que permiten realizar operaciones básicas, como sumas, multiplicaciones o similares.

[0053] Los primeros elementos estáticos comprenden las instrucciones de los programas del primer núcleo 10_1 y al menos un elemento seleccionado del grupo constituido por las tablas de constantes del primer núcleo 10_1, los registros de configuración del primer núcleo 10_1 y los circuitos electrónicos del primer núcleo 10_1.

[0054] En una variante, los primeros elementos estáticos comprenden al mismo tiempo, las instrucciones de los programas del primer núcleo 10_1, las tablas de constantes del primer núcleo 10_1, los registros de configuración del primer núcleo 10_1 y los circuitos electrónicos del primer núcleo 10_1.

[0055] El primer núcleo 10_1 incluye en su primera memoria M_1 una primera serie de instrucciones informáticas para realizar las operaciones predeterminadas que dan lugar a un primer resultado conocido.

[0056] Además, el primer núcleo 10_1 es capaz de implementar la primera serie de operaciones predeterminadas, en cada primer programa de cálculo 16_1 y 18_1. La primera serie de operaciones predeterminadas realizadas por el primer núcleo 10_1, dan lugar a un primer elemento calculado.

[0057] Las mismas observaciones sobre los elementos del primer núcleo 10_1 descritos anteriormente, en los que los números de referencia que terminan con _1 se reemplazan por números de referencia que terminan con _2 y los términos "primero", "primero" y "primeros" se reemplazan por los términos "segundo" y "segundo", se aplican a los elementos del segundo núcleo 10_2.

[0058] Cada núcleo 10_1, 10_2 es capaz de garantizar, independientemente del otro núcleo 10_1 y 10_2, la parada de emergencia del elemento de seguridad 2.

[0059] El funcionamiento del sistema de seguridad 4 se describe ahora en referencia a la figure 2, que es un diagrama de flujo de un ejemplo de implementación de una primera realización del procedimiento de parada de emergencia del sistema de seguridad 4 según la invención.

[0060] El procedimiento de parada de emergencia comprende una etapa de inicialización 28, primeras etapas 90, segundas etapas 190, una tercera etapa de parada 300 y una cuarta etapa de parada 400.

[0061] La etapa de inicialización 28 comprende las siguientes subetapas; un almacenamiento de los primeros elementos estáticos 30, un almacenamiento del primer resultado conocido 40, un almacenamiento de los segundos elementos estáticos 50 y un almacenamiento del segundo resultado conocido 60.

[0062] Cada subetapa de almacenamiento 30, 40, 50, 60 se implementa ventajosamente solo una vez.

[0063] En el almacenamiento, los primeros elementos estáticos 30, los primeros elementos estáticos se almacenan, por ejemplo, en la primera memoria M_1. Como alternativa, los primeros elementos estáticos se almacenan en la segunda memoria M_2.

[0064] En el almacenamiento del primer resultado conocido 40, el primer resultado conocido se almacena, por ejemplo, en la primera memoria M_1. Como alternativa, el primer resultado conocido se almacena en la segunda memoria M_2.

[0065] En el almacenamiento de los segundos elementos estáticos 50, los segundos elementos estáticos se almacenan, por ejemplo, en la segunda memoria M_2. Como alternativa, los segundos elementos estáticos se almacenan en la primera memoria M_1.

[0066] En el almacenamiento del segundo resultado conocido 60, el segundo resultado conocido se almacena, por ejemplo, en la segunda memoria M_2. Como alternativa, el segundo resultado conocido se almacena en la primera memoria M_1.

[0067] Las primeras etapas 90 comprenden una primera etapa de realización de operaciones 100, una primera etapa de transmisión 110, una primera etapa de comparación 120 y una primera etapa de deducción 130, una primera etapa de verificación de los primeros elementos estáticos 140, una primera etapa de cálculo 150 que da lugar a un primer elemento calculado, una etapa de comparación del primer resultado conocido con el primer elemento calculado 160 y una primera etapa de control del desfase de los relojes 170.

[0068] La primera etapa de realización de operaciones 100 para el procesamiento de datos se implementa en los dos primeros programas de cálculo 16_1, 18_1. Por lo tanto, cada uno de los primeros programas de cálculo 16_1, 18_1 realiza la misma serie de operaciones.

[0069] Cada realización de operaciones en un primer programa de cálculo 16_1, 18_1 da lugar a un primer resultado.

[0070] Por ejemplo, cada primer programa de cálculo 16_1, 18_1 ejecuta el primer programa P_1 y cada variación del primer conjunto de datos da lugar a un primer resultado.

[0071] En un primer ejemplo ilustrativo, si la operación a realizar es "2 + 3", el primer resultado es "5". Cada primer programa de cálculo 16_1, 18_1 da lugar, tras la operación "2 + 3", en funcionamiento nominal al mismo primer resultado "5".

[0072] En la primera realización del procedimiento durante la primera etapa de transmisión 110, los dos primeros resultados obtenidos se transmiten del primer núcleo 10_1 al segundo núcleo 10_2.

[0073] En el primer ejemplo ilustrativo, los primeros resultados "5" y "5" de cada primer programa de cálculo 16_1, 16_2 se transmiten al segundo núcleo 10_2.

[0074] En la primera realización del procedimiento, la primera etapa de comparación 120 se implementa por el segundo núcleo 10_2. En particular, la primera etapa de comparación se realiza por los módulos de comparación 20 de cada segundo programa de cálculo 16_2, 18_2.

[0075] Durante la primera etapa de comparación 120, se detecta una anomalía del primer núcleo 10_1 si los primeros resultados proporcionados por los dos primeros programas de cálculo 16_1, 18_1 difieren.

[0076] En el primer ejemplo ilustrativo, si los primeros resultados son, por ejemplo, "5" para un primer programa de cálculo 16_1, 18_1 y "6" para el otro primer programa de cálculo 16_1, 18_1, se detecta una anomalía del primer núcleo 10_1. Tal anomalía indica que los dos primeros programas de cálculo 16_1, 18_1 ya no son réplicas exactas entre sí porque los dos primeros programas de cálculo 16_1, 18_1 no obtienen el mismo resultado.

[0077] Por ejemplo, cada primer resultado contiene una pluralidad de datos correspondientes a diversos resultados variables resultantes de las operaciones del primer programa de cálculo asociado 16_1, 18_1. Por ejemplo, cada primer resultado incluye una pluralidad de datos ordenados según un índice creciente, correspondiendo cada dato a un índice idéntico para los dos primeros programas de cálculo 16_1, 18_1. La primera etapa de comparación 120 comprende una comparación para cada índice de los datos de cada primer programa de cálculo 16_1, 18_1 asociados con el índice, detectándose una anomalía del primer núcleo 10_1 si los valores difieren.

[0078] En un segundo ejemplo ilustrativo, si las operaciones a realizar son "2 + 3", entonces "1+5". Cada primer programa de cálculo 16_1, 18_1 da lugar, tras las operaciones en funcionamiento nominal, al mismo primer resultado, una lista ordenada "[5, 6]". Si los primeros resultados son, por ejemplo, "[5,6]" para un primer programa de cálculo 16_1, 18_1 y "[5,7]" para el otro primer programa de cálculo 16_1, 18_1, se detectará una anomalía del primer núcleo 10_1 porque los valores de los datos correspondientes al segundo índice, "6" y "7", difieren.

[0079] La primera etapa de deducción del estado del sistema de seguridad 130, es una etapa de orientación del procedimiento, ya sea hacia la tercera etapa de parada 300 o hacia las segundas etapas 190.

[0080] Al final de la primera etapa de deducción 130, si no se detecta ninguna anomalía del primer núcleo 10_1, entonces se implementa el conjunto de las segundas etapas 190.

[0081] La primera etapa de verificación de los primeros elementos estáticos 140 se implementa después de la etapa de almacenamiento de los primeros elementos estáticos 30.

[0082] En el transcurso de la primera etapa de verificación de los primeros elementos estáticos 140, se detecta una anomalía del primer núcleo 10_1 si los primeros elementos estáticos difieren de los elementos estáticos almacenados del primer núcleo 10_1.

[0083] Tal anomalía indica, por ejemplo, que el primer núcleo 10_1 tiene un defecto al haber modificado un primer elemento estático, por ejemplo, un circuito electrónico defectuoso.

[0084] Ventajosamente, la primera etapa de verificación de los primeros elementos estáticos 140 se repite siempre que no se detecte ninguna anomalía.

[0085] La primera etapa de cálculo 150 se implementa por el primer núcleo 10_1. La primera etapa de cálculo 150 se realiza después de la etapa de almacenamiento del primer resultado conocido 40.

[0086] En la primera etapa de cálculo 150, el primer núcleo 10_1 realiza la primera serie de operaciones

predeterminadas dando lugar a un primer elemento calculado.

[0087] En un tercer ejemplo ilustrativo, la serie de operación predeterminada es "hacer la operación "2+1", después multiplicar el resultado de esta operación por 3", fijándose y seleccionándose las cifras "1", "2", y "3" con el objetivo de controlar el correcto funcionamiento de las operaciones de suma y de multiplicación. El resultado conocido y almacenado es "9". Las operaciones se realizan por el primer núcleo 10_1 y dan como resultado el número "9" en funcionamiento nominal.

[0088] La etapa de comparación del primer resultado conocido con el primer elemento calculado 160 se implementa ventajosamente cada vez que se realiza la primera etapa de cálculo 150.

[0089] En la etapa de comparación del primer resultado conocido con el primer elemento calculado 160, se detecta una anomalía del primer núcleo 10_1 si el primer elemento calculado y el primer resultado conocido difieren.

[0090] En el tercer ejemplo ilustrativo, si el primer elemento calculado "8", se detectará una anomalía después de la comparación con el resultado "9" registrado. Esta anomalía podría, por ejemplo, ser el resultado de defectos del primer núcleo 10_1 que impiden la correcta realización de sumas o multiplicaciones.

[0091] Ventajosamente, la primera etapa de cálculo 150 y la etapa de comparación del primer resultado conocido con el primer elemento calculado 160, se repiten siempre que no se detecte ninguna anomalía.

[0092] La primera etapa de control del desfase de los relojes 170 se implementa por el primer núcleo 10_1.

[0093] En la primera etapa de control del desfase de los relojes 170, se detecta una anomalía del primer núcleo 10_1 si el desfase del primer reloj H_1 con respecto al segundo reloj H_2 es superior o igual a un umbral de tolerancia predeterminado.

[0094] Ventajosamente, la primera etapa de control del desfase de los relojes 170 se repite siempre que no se detecte ninguna anomalía.

[0095] Las mismas observaciones sobre las primeras etapas 90 descritas anteriormente se aplican a las segundas etapas 190. Los índices de referencia se han aumentado en 100.

[0096] Las segundas etapas 190 comprenden una segunda etapa de realización de operaciones 200, una segunda etapa de transmisión 210, una segunda etapa de comparación 220, una segunda etapa de deducción del estado del sistema de seguridad 230, una segunda etapa de verificación de los segundos elementos estáticos 240, una segunda etapa de cálculo 250 que da lugar a un segundo elemento calculado y una etapa de comparación del segundo resultado conocido con el segundo elemento calculado 260 y una segunda etapa de control del desfase de los relojes 270.

[0097] La segunda etapa de realización de operaciones 200 para el procesamiento de datos se implementa en los dos segundos programas de cálculo 16_2, 18_2. Cada uno de los segundos programas de cálculo 16_2, 18_2 realiza la misma serie de operaciones.

[0098] Cada realización de operaciones en un segundo programa de cálculo 16_2, 18_2 da lugar a un segundo resultado.

[0099] Por ejemplo, cada segundo programa de cálculo 16_1, 18_1 ejecuta el segundo programa P_2 y cada variación del primer conjunto de datos da lugar a un segundo resultado.

[0100] En la primera realización del procedimiento, durante de la segunda etapa de transmisión 210, los dos segundos resultados obtenidos se transmiten del segundo núcleo 10_2 al primer núcleo 10_1.

[0101] En la primera realización del procedimiento, la segunda etapa de comparación 220 se implementa por el primer núcleo 10_1.

[0102] En la segunda etapa de comparación 220, se detecta una anomalía del segundo núcleo 10_2 si los segundos resultados, proporcionados por los dos segundos programas de cálculo 16_2, 18_2, difieren.

[0103] Por ejemplo, cada segundo resultado contiene una pluralidad de datos correspondientes a diversos resultados variables resultantes de las operaciones del segundo programa de cálculo asociado 16_2, 18_2. Cada segundo resultado incluye una pluralidad de datos ordenados según un índice creciente, correspondiendo cada dato a un índice idéntico para los dos segundos programas de cálculo 16_2, 18_2. La segunda etapa de comparación 220 comprende una comparación para cada índice de los datos de cada segundo programa de cálculo 16_2, 18_2 asociados con el índice, detectándose una anomalía del segundo núcleo 10_2 si los valores difieren.

[0104] La segunda etapa de deducción del estado del sistema de seguridad 230, es una etapa de orientación del procedimiento, ya sea hacia la cuarta etapa de parada 400 o hacia las primeras etapas 90.

[0105] Al final de la segunda etapa de deducción 230, si no se detecta ninguna anomalía del segundo núcleo 10_2, las primeras etapas 90 se repiten. El conjunto de las primeras etapas 90 se implementa de nuevo, por ejemplo, a partir de la primera etapa de realización de operaciones 100 para el tratamiento de datos.

[0106] Por lo tanto, el procedimiento se repetirá siempre que no se detecte ninguna anomalía del primer núcleo 10_1 o del segundo núcleo 10_2.

[0107] La segunda etapa de verificación de los elementos estáticos 240 se implementa después de la etapa de almacenamiento de los segundos elementos estáticos 50.

[0108] En el transcurso de la segunda etapa de verificación de los segundos elementos estáticos 240, se detecta una anomalía del segundo núcleo 10_2 si los segundos elementos estáticos difieren de los elementos estáticos almacenados del segundo núcleo 10_2.

[0109] Ventajosamente, la segunda etapa de verificación de los segundos elementos estáticos 240 se repite siempre que no se detecte ninguna anomalía.

[0110] La segunda etapa de cálculo 250 se implementa por el segundo núcleo 10_2. La segunda etapa de cálculo 250 se realiza después de la etapa de almacenamiento del segundo resultado conocido 60.

[0111] En la segunda etapa de cálculo 250, el segundo núcleo 10_2 realiza la segunda serie de operaciones predeterminadas que dan lugar a un segundo elemento calculado.

[0112] La etapa de comparación del segundo resultado conocido con el segundo elemento calculado 260 se implementa ventajosamente cada vez que se realiza la segunda etapa de cálculo 250.

[0113] En la etapa de comparación del segundo resultado conocido con el segundo elemento calculado 260, se detecta una anomalía del segundo núcleo 10_2 si el segundo elemento calculado y el segundo resultado conocido difieren.

[0114] Ventajosamente, la segunda etapa de cálculo 250 y la etapa de comparación del segundo resultado conocido con el segundo elemento calculado 260 se repiten siempre que no se detecte ninguna anomalía.

[0115] La segunda etapa de control del desfase de los relojes 270 se implementa por el segundo núcleo 10_2.

[0116] En la segunda etapa de control del desfase de los relojes 270, se detecta una anomalía del segundo núcleo 10_2 si el desfase del segundo reloj H_2 con respecto al primer reloj H_1 es superior o igual a un umbral de tolerancia predeterminado.

[0117] Ventajosamente, la segunda etapa de control del desfase de los relojes 270 se repite siempre que no se detecte ninguna anomalía.

[0118] Además, una instrucción de continuación se transmite regularmente al primer núcleo 10_1 por el segundo núcleo 10_2 siempre que no se detecte ninguna anomalía.

[0119] Además, una instrucción de continuación se transmite regularmente al segundo núcleo 10_2 por el primer núcleo 10_2 siempre que no se detecte ninguna anomalía.

[0120] Una anomalía del primer núcleo 10_1 es detectable al final de la primera etapa de deducción 130 del estado del sistema de seguridad 4. Cuando se detecta tal anomalía del primer núcleo 10_1, la tercera etapa de parada 300 se implementa por el segundo programa de parada del segundo núcleo 10_2.

[0121] En la tercera etapa de parada 300, se ejecuta el segundo programa de parada PA_2. El elemento de seguridad 2 se pone en el estado de parada de seguridad por el segundo núcleo 10_2.

[0122] La tercera etapa de parada 300 incluye una etapa de parada de la transmisión de la instrucción de continuación al primer núcleo 10_1.

[0123] Además, la tercera etapa de parada del sistema de seguridad 300 incluye ventajosamente una etapa de borrado de la memoria del segundo núcleo 10_2 o de al menos una parte del contenido de los segundos programas de cálculo 16_2, 18_2 por el segundo núcleo 10_2. Tal borrado permite limitar los riesgos de reinicio involuntario del

conjunto de seguridad 1 y, en particular, del elemento de seguridad 2 después de una parada.

[0124] Si el primer núcleo 10_1 detecta la ausencia de instrucción de continuación, entonces la cuarta etapa de parada 400 se implementará por el primer núcleo 10_1, si es capaz de ejecutarla.

[0125] Una anomalía del segundo núcleo 10_2 es detectable al final de la segunda etapa de deducción 230 del estado del sistema de seguridad 4. Cuando se detecta tal anomalía del segundo núcleo 10_2, la cuarta etapa de parada 400 se implementa por el primer programa de parada del primer núcleo 10_1.

[0126] En la cuarta etapa de parada 400, se ejecuta el primer programa de parada PA_1. El elemento de seguridad 2 se pone en el estado de parada de seguridad por el primer núcleo 10_1.

[0127] La cuarta etapa de parada 400 incluye una etapa de parada de la transmisión de la instrucción de continuación al segundo núcleo 10_2.

[0128] Además, la cuarta etapa de parada 400 del sistema de seguridad 4 incluye ventajosamente una etapa de borrado de la memoria del primer núcleo 10_1 o de al menos una parte del contenido de los primeros programas de cálculo 16_1, 18_1 por el primer núcleo 10_1.

[0129] Si el segundo núcleo 10_2 detecta la ausencia de instrucción de continuación, la tercera etapa de parada 300 se implementará entonces por el segundo núcleo 10_2, si es capaz de ejecutarla.

[0130] Por lo tanto, la primera realización del procedimiento de parada de emergencia del sistema de seguridad 4 según la invención se refiere a un procedimiento en el que la primera etapa de comparación 120 y la segunda etapa de comparación 220 se realizan de forma remota, es decir, en el núcleo 10_1, 10_2, que no es el núcleo 10_1, 10_2 en el que se han obtenido los resultados de las unidades de cálculo 16_1, 18_1, 16_2, 18_2 a comparar.

[0131] Ahora se describirá una segunda realización del procedimiento de parada de emergencia del sistema de seguridad 4 según la invención.

[0132] El procedimiento de parada de emergencia según la segunda realización es similar al procedimiento según la primera realización, excepto con respecto a las diferencias que se expondrán a continuación.

[0133] El procedimiento de parada de emergencia de la segunda realización difiere del procedimiento de la primera realización descrita en que la primera etapa de comparación 120 y la segunda etapa de comparación 220 se realizan localmente, es decir, en el núcleo 10_1, 10_2 en el que se han obtenido los resultados de los programas de cálculo 16_1, 18_1, 16_2 18_2.

[0134] El procedimiento de parada de emergencia de la segunda realización difiere del procedimiento de parada de emergencia de la primera realización en que la primera etapa de comparación 120 se implementa por el primer núcleo 10_1. La primera etapa de comparación 120 se realiza por el módulo de comparación de cada primer programa de cálculo 16_1, 18_1.

[0135] El procedimiento de parada de emergencia de la segunda realización difiere también del procedimiento de la primera realización en que el procedimiento de parada de emergencia comprende:

- una primera etapa de generación de un primer mensaje que indica si se ha detectado una anomalía del primer núcleo 10_1,
- una primera etapa de transmisión del primer mensaje.

[0136] La etapa de generación del primer mensaje se implementa, por ejemplo, por el módulo de comparación 20 de cada primer programa de cálculo 16_1, 18_1.

[0137] En la primera etapa de transmisión del primer mensaje, el primer mensaje se transmite del primer núcleo 10_1 al segundo núcleo 10_2.

[0138] Después de la primera etapa de transmisión del primer mensaje, la tercera etapa de parada 300 se implementa por el segundo núcleo 10_2 si el primer mensaje indica que se ha detectado una anomalía del primer núcleo 10_1.

[0139] El procedimiento de parada de emergencia de la segunda realización difiere también del procedimiento de la primera realización en que se implementa la segunda etapa de comparación 220.

[0140] El procedimiento de la segunda realización difiere también del procedimiento de parada de emergencia de la primera realización en que el procedimiento de parada de emergencia comprende:

- una segunda etapa de generación de un segundo mensaje que indica si se ha detectado una anomalía del segundo núcleo 10_2,
- una segunda etapa de transmisión del segundo mensaje.

[0141] En la segunda etapa de transmisión del segundo mensaje, el segundo mensaje se transmite del segundo núcleo 10_2 al primer núcleo 10_1.

[0142] Después de la segunda etapa de transmisión del segundo mensaje, la cuarta etapa de parada 400 se implementa por el primer núcleo 10_1, si el segundo mensaje indica que se ha detectado una anomalía del segundo núcleo 10_2.

[0143] Este procedimiento de parada de emergencia según la segunda realización permite limitar la cantidad de datos a transmitir entre el primer núcleo 10_1 y el segundo núcleo 10_2 dado que la detección de diferencias se realiza localmente.

[0144] El procedimiento de parada de emergencia que se acaba de describir en dos realizaciones permite una parada de seguridad del elemento de seguridad 2. De hecho, cuando se detecta una anomalía de un núcleo 10_1, 10_2, la parada se realiza por el otro núcleo. Por lo tanto, la parada está controlada por el núcleo que no es el núcleo para el que se ha detectado una anomalía. Esto hace posible tener una parada segura ya que el riesgo de que el núcleo que realiza la parada también sea defectuoso es bajo.

[0145] Como alternativa, el conjunto de seguridad 1 comprende varios elementos de seguridad 2.

[0146] Ventajosamente, el procedimiento incluye una etapa de recuperación implementada por el primer núcleo 10_1 antes de la primera etapa de deducción 130, si, tras la etapa de comparación 120, se detecta una anomalía.

[0147] Durante la etapa de recuperación, el primer núcleo 10_1 se apaga y se vuelve a encender para que los dos primeros programas de cálculo 16_1 y 18_1 se reinicien. A continuación, las primeras etapas de realización de operaciones 100 y de comparación 120 se repiten una vez. Después, se implementa la primera etapa de deducción 130.

[0148] Además, la tercera etapa de parada 300 comprende una etapa de espera durante la cual se repiten las etapas de realización de operaciones 100 y de comparación 120.

[0149] Ventajosamente, el procedimiento incluye una segunda etapa de recuperación implementada por el segundo núcleo 10_2 antes de la segunda etapa de deducción 230, si, tras la segunda etapa de comparación 220, se detecta una anomalía.

[0150] Durante la etapa de recuperación, el segundo núcleo 10_2 se apaga y se vuelve a encender para que los dos segundos programas de cálculo 16_2 y 18_2 se reinicien. A continuación, las segundas etapas de realización de operaciones 200 y de comparación 220 se repiten una vez. Después, se implementa la segunda etapa de deducción 230.

[0151] Además, la cuarta etapa de parada 400 comprende una etapa de espera durante la cual se repiten las etapas de realización de operaciones 200 y de comparación 220.

REIVINDICACIONES

1. Procedimiento de parada de emergencia de un elemento de seguridad (2) de un conjunto de seguridad (1), comprendiendo el conjunto de seguridad (1) el elemento de seguridad (2) y un sistema de seguridad (4), comprendiendo el sistema de seguridad (4):

- un primer núcleo (10_1) que comprende:

  - ○ dos primeros programas de cálculo (16_1, 18_1) capaces de realizar las mismas operaciones, y
  - ○ un primer programa de parada (PA_1) capaz de implementar una parada de emergencia, y

- un segundo núcleo (10_2) que comprende:

  - ○ dos segundos programas de cálculo (16_2, 18_2) capaces de realizar las mismas operaciones, y
  - ○ un segundo programa de parada (PA_2) capaz de implementar una parada de emergencia,

comprendiendo el procedimiento la implementación de primeras etapas (90):

- una primera etapa de realización de operaciones (100) en los dos primeros programas de cálculo (16_1, 18_1), dando lugar cada realización de operaciones en un primer programa de cálculo (16_1, 18_1) a un primer resultado,
- una primera etapa de comparación (120) de los dos primeros resultados, siendo una anomalía del primer núcleo (10_1) detectada si los dos primeros resultados difieren,
- una primera etapa de deducción (130) del estado del sistema de seguridad (4), al final de la cual:

  - ○ si se detecta una anomalía del primer núcleo (10_1), se implementa una tercera etapa de parada (300) por el segundo programa de parada (PA_2) del segundo núcleo (10_2),
  - ○ si no se detecta ninguna anomalía del primer núcleo (10_1), se implementan las segundas etapas (190),

comprendiendo las segundas etapas (190):

- una segunda etapa de realización de operaciones (200) en los dos segundos programas de cálculo (16_2, 18_2), dando lugar cada realización de operaciones en un segundo programa de cálculo (16_2, 18_2) a un segundo resultado,
- una segunda etapa de comparación (220) de los dos segundos resultados, siendo una anomalía del segundo núcleo (10_2) detectada si los dos segundos resultados difieren,
- una segunda etapa de deducción (230) del estado del sistema de seguridad (4), al final de la cual:

  - ○ si se detecta una anomalía del segundo núcleo (10_2), se implementa una cuarta etapa de parada (400) por el primer programa de parada (PA_1) del primer núcleo (10_1),
  - ○ si no se detecta ninguna anomalía del segundo núcleo (10_2), las primeras etapas (90) se repiten,

repitiéndose las primeras etapas (90) y las segundas etapas (190) siempre que no se detecte ninguna anomalía del primer núcleo (10_1) o del segundo núcleo (10_2).

2. Procedimiento de parada según la reivindicación 1, en el que el primer núcleo (10_1) comprende:

- programas que tienen instrucciones,
- tablas de constantes,
- registros de configuración,
- circuitos electrónicos, y
- primeros elementos estáticos (30), comprendiendo los primeros elementos estáticos las instrucciones de los programas del primer núcleo (10_1) y al menos un elemento seleccionado del grupo constituido por:

  - ○ las tablas de constantes del primer núcleo (10_1),
  - ○ los registros de configuración del primer núcleo (10_1) y
  - ○ los circuitos electrónicos del primer núcleo (10_1),

y en el que el segundo núcleo (10_2) comprende:

- programas que tienen instrucciones,
- tablas de constantes,
- registros de configuración,
- circuitos electrónicos y
- segundos elementos estáticos (50), comprendiendo los segundos elementos estáticos las instrucciones de los programas del segundo núcleo (10_2) y al menos un elemento seleccionado del grupo constituido por:

- ○ las tablas de constantes del segundo núcleo (10_2),
- ○ los registros de configuración del segundo núcleo (10_2) y
- ○ los circuitos electrónicos del segundo núcleo (10_2),

y en el que el procedimiento comprende, además:

- una etapa de almacenamiento de los primeros elementos estáticos (30),
- una etapa de almacenamiento de los segundos elementos estáticos (50),
- una primera etapa de verificación de los primeros elementos estáticos (140), siendo una anomalía del primer núcleo (10_1) detectada si los primeros elementos estáticos difieren de los primeros elementos estáticos almacenados del primer núcleo (10_1), y
- una segunda etapa de verificación de los segundos elementos estáticos (240), siendo una anomalía del segundo núcleo (10_2) detectada si los segundos elementos estáticos del segundo núcleo (10_2) difieren de los segundos elementos estáticos almacenados del segundo núcleo (10_2).

3. Procedimiento de parada según la reivindicación 1 o 2, en el que el primer núcleo (10_1) incluye una primera memoria (M_1) y es capaz de implementar una primera serie de operaciones predeterminadas que dan lugar a un primer resultado conocido,
y en el que el segundo núcleo (10_2) incluye una segunda memoria (M_2) y es capaz de implementar una segunda serie de operaciones predeterminadas que dan lugar a un segundo resultado conocido,
y comprendiendo el procedimiento:

- una etapa de almacenamiento del primer resultado conocido (40),
- una etapa de almacenamiento del segundo resultado conocido (60),
- una primera etapa de cálculo (150), durante la cual el primer núcleo (10_1) realiza la primera serie de operaciones predeterminadas que dan lugar a un primer elemento calculado,
- una etapa de comparación del primer resultado conocido con el primer elemento calculado (160), siendo una anomalía del primer núcleo (10_1) detectada si el primer elemento calculado y el primer resultado conocido difieren,
- una segunda etapa de cálculo (250), durante la cual el segundo núcleo (10_2) realiza la segunda serie de operaciones predeterminadas que dan lugar a un segundo elemento calculado, y
- una etapa de comparación del segundo resultado conocido con el segundo elemento calculado (260), siendo una anomalía del segundo núcleo (10_2) detectada si el segundo elemento calculado y el segundo resultado conocido difieren.

4. Procedimiento de parada según cualquiera de las reivindicaciones 1 a 3, en el que el primer núcleo (10_1) comprende un primer reloj (H_1), y el segundo núcleo (10_2) comprende un segundo reloj (H_2), incluyendo el procedimiento:

- una primera etapa de control del desfase de los relojes (170), implementada por el segundo núcleo (10_2), siendo una anomalía del primer núcleo (10_1) detectada si el desfase del primer reloj (H_1), con respecto al segundo reloj (H_2), es superior o igual a un umbral de tolerancia predeterminado,
- una segunda etapa de control del desfase de los relojes (270) implementada por el primer núcleo (10_1), siendo una anomalía del segundo núcleo (10_2) detectada si el desfase del segundo reloj (H_2), con respecto al primer reloj (H_1), es superior o igual a un umbral de tolerancia predeterminado.

5. Procedimiento de parada según cualquiera de las reivindicaciones 1 a 4, en el que cada primer programa de cálculo (16_1, 18_1) comprende un primer programa (P_1), generando una ejecución nominal de dicho al menos un primer programa (P_1) variaciones de los datos de un primer conjunto de datos,
y cada segundo programa de cálculo (16_2, 18_2) comprende un segundo programa (P_2), generando una ejecución nominal de dicho al menos un segundo programa (P_2) variaciones de los datos de un segundo conjunto de datos,
y en el que las primeras etapas (90) se aplican para todas las variaciones del primer conjunto de datos que la ejecución nominal de dicho al menos un primer programa (P_1) es capaz de generar, siendo cada variación una realización de operación, y las segundas etapas (190) se aplican para todas las variaciones del segundo conjunto de datos que la ejecución nominal de dicho al menos un segundo programa (P_2) es capaz de generar, siendo cada variación una realización de operación.

6. Procedimiento de parada según cualquiera de las reivindicaciones 1 a 5, en el que la primera etapa de comparación (120) de los dos primeros resultados se implementa por el segundo núcleo (10_2) y la segunda etapa de comparación (220) de los dos segundos resultados se implementa por el primer núcleo (10_1).

7. Procedimiento de parada según cualquiera de las reivindicaciones 1 a 6, en el que el primer núcleo (10_1) comprende, además, una primera memoria (M_1), y el segundo núcleo (10_2) comprende, además, una segunda memoria (M_2), y en el que:

- el primer programa de parada (PA_1) incluye un primer programa de borrado de al menos una parte del contenido de la primera memoria (M_1),
- el segundo programa de parada (PA_2) incluye un segundo programa de borrado de la segunda memoria (M_2),
- la tercera etapa de parada (300) incluye una etapa de borrado de al menos una parte del contenido de la segunda memoria (M_2) del segundo núcleo (10_2) por el segundo núcleo (10_2), y
- la cuarta etapa de parada (400) incluye una etapa de borrado de al menos una parte del contenido de la primera memoria (M_1) del primer núcleo (10_1) por el primer núcleo (10_1).

8. Procedimiento de parada según cualquiera de las reivindicaciones 1 a 7, en el que la tercera etapa de parada (300) incluye una etapa de parada de transmisión de una instrucción de continuación al primer núcleo (10_1), y la cuarta etapa de parada (400) incluye una etapa de parada de transmisión de una instrucción de continuación al segundo núcleo (10_2).

9. Procedimiento de parada según cualquiera de las reivindicaciones 1 a 8, en el que cada primer resultado incluye una pluralidad de datos ordenados según un índice creciente, correspondiendo cada dato a un índice idéntico para los dos primeros programas de cálculo (16_1, 18_1), comprendiendo la primera etapa de comparación (120) una comparación para cada índice de los datos de cada primer programa de cálculo (16_1, 18_1) asociados con el índice particular, siendo una anomalía del primer núcleo (10_1) detectada si los valores difieren, y en el que cada segundo resultado incluye una pluralidad de datos ordenados según un índice creciente, correspondiendo cada dato a un índice idéntico para los dos segundos programas de cálculo (16_2, 18_2), comprendiendo la segunda etapa de comparación (220) una comparación para cada índice de los datos de cada segundo programa de cálculo (16_2, 18_2) asociados con el índice particular, siendo una anomalía del segundo núcleo (10_2) detectada si los valores difieren.

10. Sistema de seguridad (4), comprendiendo el sistema de seguridad (4):

- un primer núcleo (10_1) que comprende:
  - dos primeros programas de cálculo (16_1, 18_1) capaces de realizar las mismas operaciones, y
  - un primer programa de parada (PA_1) capaz de implementar una parada de emergencia, y
- un segundo núcleo (10_2) que comprende:
  - dos segundos programas de cálculo (16_2, 18_2) capaces de realizar las mismas operaciones, y
  - un segundo programa de parada (PA_2) capaz de implementar una parada de emergencia,

siendo el sistema de seguridad (4) capaz de implementar el procedimiento de parada de emergencia según cualquiera de las reivindicaciones 1 a 9.

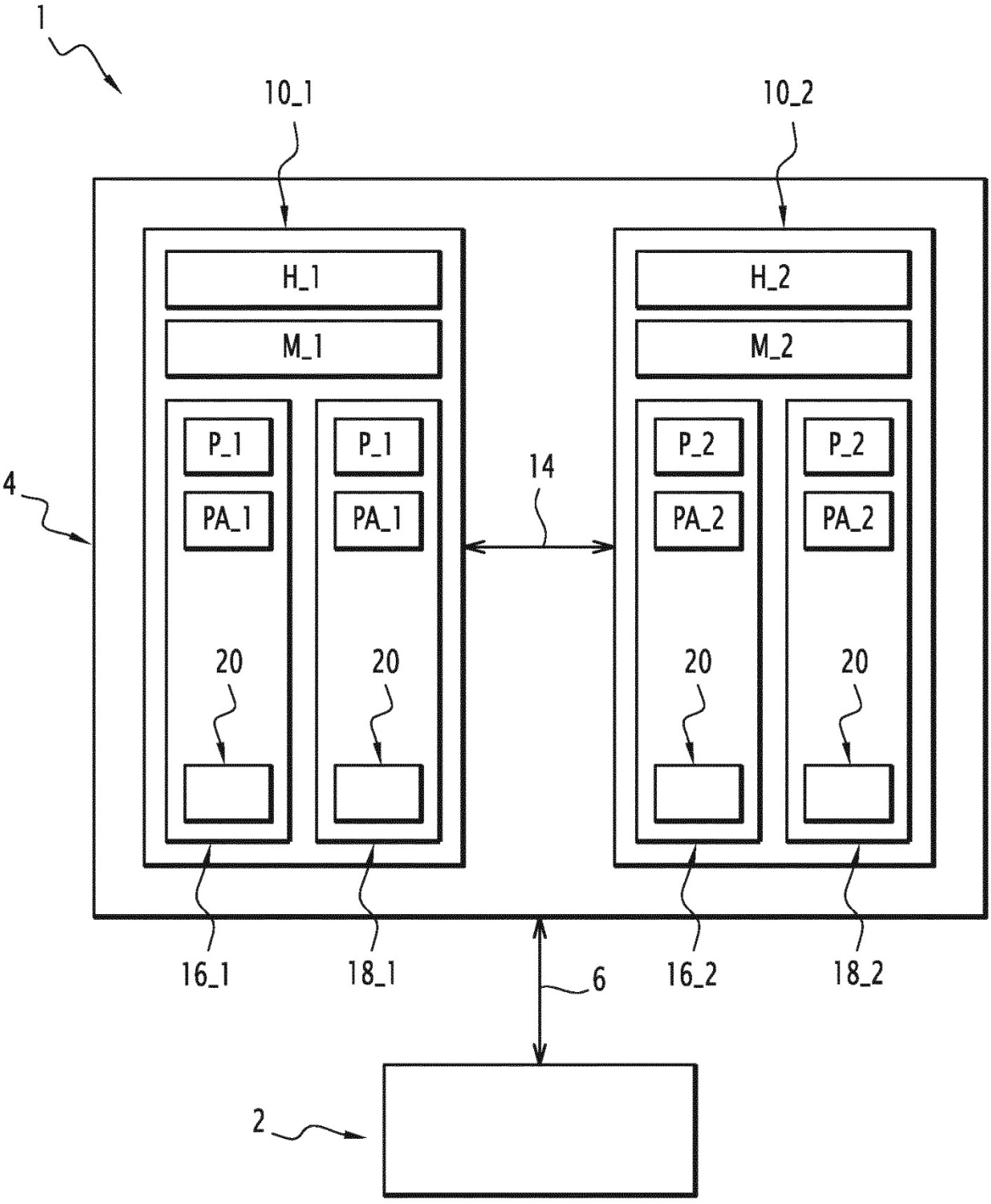
1
10_1
10_2
H_1
M_1
H_2
M_2
P_1
PA_1
P_1
PA_1
P_2
PA_2
P_2
PA_2
4
14
20
20
20
20
16_1
18_1
6
16_2
18_2
2

FIG.1

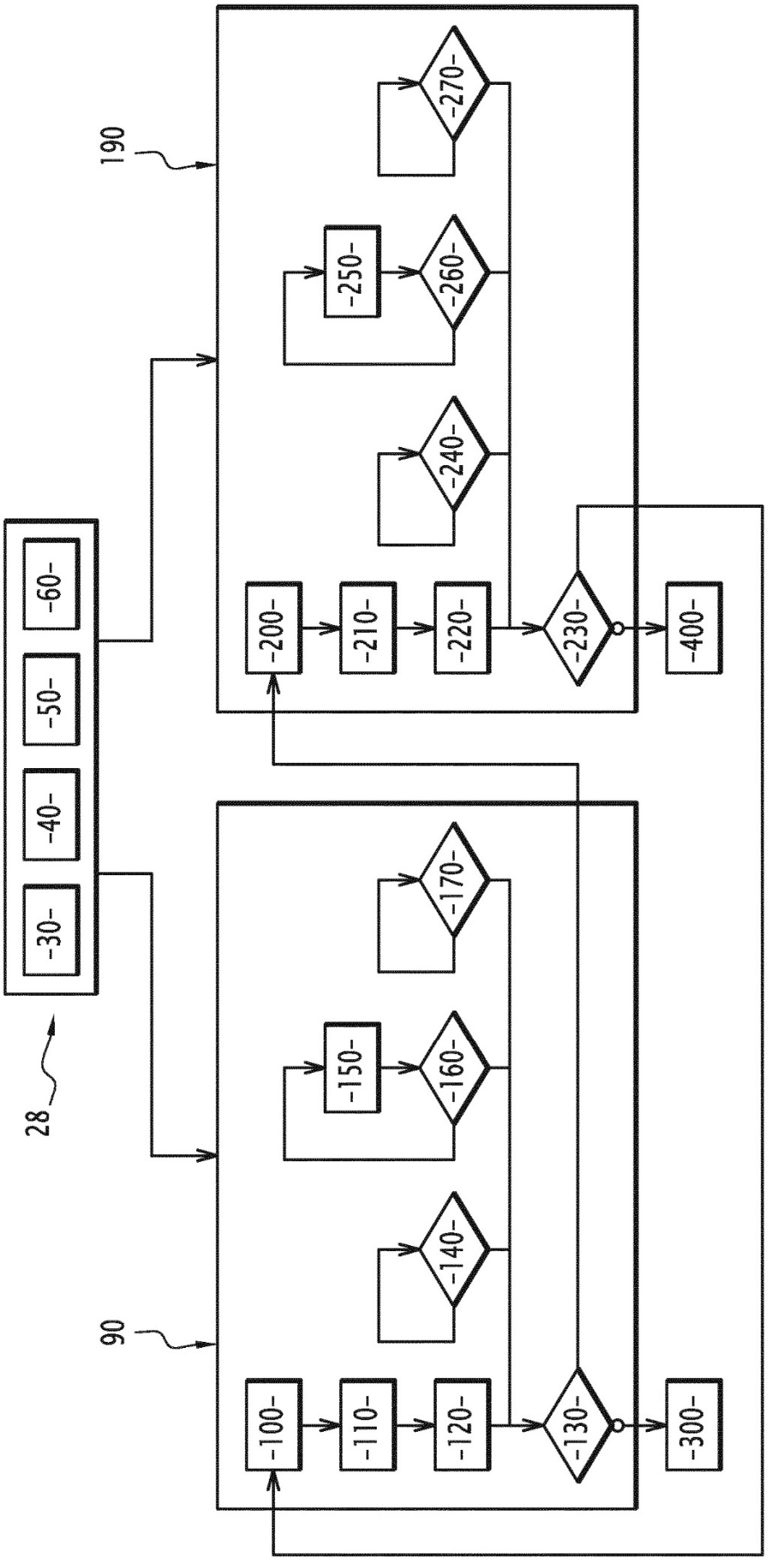
190
-270-
-250-
-260-
-240-
-200-
-210-
-220-
-230-
-400-
-60-
-50-
-40-
-30-
28
-170-
-150-
-160-
-140-
90
-100-
-110-
-120-
-130-
-300-

FIG.2