(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 569 518**

(51) Int. CI.:

G06F 11/16 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **29.04.2003 E 03732589 (1)**

(97) Fecha y número de publicación de la concesión europea: **03.02.2016 EP 1573543**

(54) Título: **Aparato de procesamiento o de control intrínsecamente seguro**

(30) Prioridad:

03.05.2002 IT SV20020018

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.05.2016

(73) Titular/es:

ALSTOM FERROVIARIA S.P.A. (100.0%)
VIA O. MORENO, 23
12038 SAVIGLIANO (CUNEO), IT

(72) Inventor/es:

MANONI, VITTORIO

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Aparato de procesamiento o de control intrínsecamente seguro

Esta invención se refiere a un aparato de procesamiento o de control intrínsecamente seguro según el preámbulo de la reivindicación 1.

Actualmente, los sistemas ferroviarios regulares están controlados por aparatos de control basados en ordenador.

Esta disposición proporciona considerables ventajas relacionadas con la lógica del sistema. La lógica del sistema es reproducida por un conjunto de algoritmos, y en particular por un conjunto de ecuaciones booleanas. Los estados de los diversos elementos de maniobras tales como señales, conmutadores, circuitos de vía, etc. se controlan en forma de variables booleanas, a partir de las cuales el ordenador determina el estado que dichos elementos deberán adoptar en vista de la llegada de un tren o de una nueva situación. Los nuevos estados se disponen asimismo como variables booleanas a transmitir como datos digitales a los accionadores locales de los diferentes elementos de maniobras, accionadores que transforman las variables recibidas en correspondientes señales de control a transmitir a los elementos accionados por los mismos.

En este caso, esta tarea de cálculo requiere cierta potencia, pero no requiere de hecho una construcción de hardware dedicada de la unidad de procesamiento. Por lo tanto, se obtendrían ventajas de la utilización de unidades de procesamiento consistentes en hardware comercial, no específico de la aplicación.

Sin embargo, la utilización de hardware comercial no se recomienda actualmente para unidades de control central de sistemas ferroviarios, que requieren niveles de seguridad intrínseca en la determinación de controles vitales.

Se encuentra un problema similar en los dispositivos de control de unidades operativas, tales como los subsistemas gráficos digitales, que sustituyen los bien conocidos paneles, o en subsistemas de entrada de datos, tales como teclados, o en el control de otras unidades operativas que requieren la utilización de unidades de procesamiento dedicadas.

Se conoce por el documento US 4.553.200 un aparato seguro de procesamiento o de control acorde con el preámbulo de la reivindicación 1. De acuerdo con este documento, las funciones de un procesador principal se controlan vitalmente mediante un controlador vital. El procesador principal genera palabras de control, denominadas palabras de comprobación, durante la ejecución de un programa. Las palabras de comprobación son examinadas por el controlador vital para determinar la corrección de la secuencia de palabras de comprobación generada por el procesador principal. El controlador vital comprende un procesador convencional que ejecuta un programa para examinar la secuencia de palabras de comprobación, y activa o desactiva la salida del procesador principal en función de si la secuencia de palabras de comprobación es o no correcta. El procesador principal y el procesador del controlador vital son procesadores convencionales. El controlador vital no está diseñado para ejecutar tareas con el fin de estimar los riesgos de una obsolescencia de los datos en la memoria caché del procesador principal.

En todos los casos anteriores, existen dos niveles de problemas. En primer lugar, es necesario forzar de manera segura la salida de la unidad de control a un estado de seguridad siempre que se produzcan fallos en alguna unidad involucrada en la generación de salida de datos de control. Un segundo aspecto consiste en que los procesadores ultrarrápidos disponibles actualmente tienen una memoria caché que puede almacenar los datos de entrada de ciclos de procesamiento ocurridos antes del ciclo en curso por lo que, como resultado de fallos aleatorios o sistemáticos, las unidades de procesamiento del microprocesador pueden generar datos de control de salida a partir de datos de entrada relativos a ciclos pasados, obsoletos, lo que tiene como resultado consecuencias graves.

La invención está destinada a dar a conocer un aparato de control intrínsecamente seguro que pueda utilizar hardware no seguro, de bajo coste y alta potencia, para ejecutar cálculos relacionados con la lógica del sistema, es decir para determinar los datos de control del sistema a partir de datos de entrada, asegurando al mismo tiempo la ejecución intrínsecamente segura de funciones vitales.

La invención consigue los objetivos anteriores disponiendo un aparato acorde con el preámbulo de la reivindicación 1, que comprende además la combinación de características de la parte caracterizante de la reivindicación 1.

En este caso, la primera unidad de procesamiento se compone de un hardware comercial no intrínsecamente seguro, mientras que la unidad de comprobación y protección está fabricada de un hardware dedicado propietario y proporciona funciones de comprobación en la primera unidad de procesamiento, que permiten comprobar la corrección de todas las operaciones diseñadas para actuar sobre las funciones vitales del sistema, siempre que se detecten fallos de funcionamiento.

Se pueden disponer varios modos de comprobación y ejecución de funciones, para conseguir el nivel de seguridad deseado. Estos modos dependen de las funciones previstas de la unidad de procesamiento y de las unidades operativas controladas por ésta.

Sin embargo, para proporcionar mayor flexibilidad y reducir costes de fabricación, se han proporcionado unidades de comprobación y protección con un subsistema de comprobación, un subsistema de protección y una unidad para la

interconexión con la unidad o unidades operativas, lo que varía en función del hardware de las unidades operativas. Los subsistemas de comprobación y protección son siempre sustancialmente idénticos en lo que se refiere a su construcción. Sin embargo, los programas de comprobación de las unidades de procesamiento pueden ser diferentes.

De acuerdo con una realización preferida, la unidad de comprobación y protección funcional tiene dos unidades independientes con dos procesadores independientes y se compone de una subunidad de comprobación, que lleva a cabo funciones de comprobación funcional sobre la primera unidad de procesamiento, ejecutando un programa de comprobación, y de una subunidad de protección que lleva a cabo solamente funciones de verificación sobre palabras de comprobación y sobre la secuencia de las mismas, y que controla en las unidades la activación/desactivación de las funciones vitales de la unidad remota.

Para asegurar un funcionamiento intrínsecamente seguro, la subunidad de comprobación está programada asimismo de tal modo que genera un flujo de palabras de comprobación que describe su estado funcional y que están relacionadas únicamente con las etapas de comprobación ejecutadas, palabras de comprobación que son transmitidas a la subunidad de protección para una comprobación de corrección y de secuencia.

Sin embargo, para evitar la posibilidad de utilizar datos de entrada de ciclos de procesamiento anteriores, la subunidad de comprobación está programada de tal modo que genera una única marca de tiempo para cada ciclo de ejecución del programa de procesamiento de la primera unidad de procesamiento. Esta marca de tiempo se cambia/incrementa en cada inicio del ciclo de procesamiento de la primera unidad de procesamiento y es transmitida por la subunidad de comprobación a la primera unidad de procesamiento en el inicio de cada ciclo de procesamiento de esta primera unidad de procesamiento.

La primera unidad de procesamiento tiene una memoria para los datos de entrada a procesar, habitualmente la memoria caché del procesador, cuyos datos se marcan con la marca de tiempo del ciclo de procesamiento actual, mientras que todos los datos de entrada marcados con las marcas de tiempo de ciclos de procesamiento anteriores se eliminan de la memoria. Por lo tanto, la memoria se actualiza o restablece en cada ciclo de procesamiento, y solamente se mantienen los datos marcados con la marca de tiempo del ciclo actual, mientras que los datos de ciclos anteriores son eliminados.

Con el fin de que los datos de entrada se procesen por lo menos una vez, una mejora de la invención dispone que todos los datos introducidos en la primera unidad de procesamiento se marquen con las marcas de tiempo de los ciclos tanto actual como siguiente, y que se procesen tanto en el ciclo actual como en el siguiente.

La condición de seguridad se puede obtener, por ejemplo, disponiendo que la unidad de comprobación y protección actúe sobre una interfaz para transmitir/amplificar la salida de datos de control de la unidad de procesamiento, en cuanto se detecta el fallo de funcionamiento de la unidad de procesamiento, impidiendo de ese modo la transmisión de datos a la unidad operativa.

Éste puede ser el caso de un subsistema de procesamiento de gráficos para el control de monitores de video. Mientras la unidad de procesamiento lleva a cabo la tarea de transformar los datos de entrada en símbolos gráficos relacionados con datos de entrada y de generar señales de control de monitor de video, por medio de adaptadores gráficos asociados al mismo, la unidad de comprobación y protección comprueba las etapas de proceso ejecutadas por la unidad de procesamiento, en base al flujo de palabras de comprobación y, si siempre que se detecte una inconsistencia, impide cualquier transmisión/amplificación de la salida de datos de visualización de la unidad de procesamiento a los monitores de video. En este caso, los adaptadores gráficos no están conectados directamente a entradas de monitor de video, sino a través de una interfaz de transmisión/amplificación de la unidad de comprobación y protección, que está controlada por la propia unidad de comprobación y protección.

Se puede disponer una disposición similar para la comprobación de seguridad intrínseca de datos o controles introducidos desde un teclado. En este caso, la comprobación funcional se lleva a cabo directamente desde el teclado y el control se transmite solamente a la unidad de procesamiento si la comprobación de corrección desde el teclado ha tenido resultados positivos. Si se ha obtenido un resultado negativo se desactiva el teclado, o la conexión entre el teclado y la unidad de procesamiento. En este ejemplo, la unidad de procesamiento tiene la función de recibir el control de entrada del teclado y de generar una imagen en el monitor de video.

Para esta función de eco, en la realización que se describe y se muestra en la presente memoria, el control de los monitores de video y la utilización de los teclados están implementados para una única subunidad de procesamiento, con una única unidad de comprobación y protección.

Otro ejemplo de aplicación del aparato de control de seguridad intrínseca de la invención consiste en un ordenador lógico central, es decir un ordenador cuya función es controlar todo el sistema, mientras que las funciones secundarias, tales como funciones gráficas y de entrada de teclado están asignadas a subunidades de procesamiento tal como la mencionada anteriormente.

Cuando se utilizan estos ordenadores, y por razones de seguridad, el proceso se lleva a cabo en dos canales independientes, con un control sincronizado. Esto tiene la finalidad de asegurar que el conjunto requerido de datos

de control está siempre listo a la salida, y que está inmediatamente operativo y efectivo un canal de procesamiento en cuanto se produce un fallo en el otro canal. Por lo tanto, tanto las entradas como el procesamiento se manejan en paralelo, mientras que la transmisión de datos de salida se permite solamente desde una de las dos unidades de procesamiento.

Una vez más, el procesamiento se lleva a cabo por una unidad de microprocesador basada en hardware comercial, mientras que la unidad de comprobación y protección no sólo comprueba que cada unidad de procesamiento funciona correctamente, sino que determina asimismo qué canal está activado actualmente para la transmisión de datos de salida, mientras mantiene el otro canal de procesamiento en estado listo y operativo. La redundancia de los canales de cálculo es controlada de manera intrínsecamente segura por la unidad de comprobación y protección.

Es posible y recomendable disponer unidades de comprobación y protección independientes para cada una de las dos unidades de procesamiento paralelas, unidades de comprobación y protección que comunican entre sí para controlar la sincronización de las funciones de cálculo de ambos canales de procesamiento y controlar la redundancia de los datos de salida, tal como se ha mencionado anteriormente, incluso en la salida.

Otras mejoras de la invención constituirán el tema de las reivindicaciones dependientes.

Las características de la invención y las ventajas derivadas de la misma resultarán más evidentes a partir de la siguiente descripción de unas pocas realizaciones no limitativas, que se muestran en los dibujos adjuntos, en los cuales:

La figura 1 muestra un diagrama de un típico sistema de estación, controlado por un sistema informático.

La figura 2 muestra un subsistema de procesamiento de gráficos y entrada de teclado para la denominada interfaz virtual hombre máquina (VMMI, Virtual Man-Machine Interface) que da a conocer esta invención, y que comprende una unidad de procesamiento y una unidad de comprobación y protección.

La figura 3 muestra un diagrama de bloques más detallado de la unidad de comprobación y protección del subsistema VMMI que se muestra en la figura 2.

La figura 4 y la figura 5 muestran diagramas de bloques más detallados de los subsistemas de comprobación y de protección que forman la unidad de protección y de comprobación que se muestra en la figura 3.

La figura 6 muestra un diagrama de bloques de la sección de aplicación, es decir la interfaz con las unidades remotas de la unidad de comprobación y protección, que se muestra en las figuras anteriores.

La figura 7 muestra un diagrama de bloques de la arquitectura de ordenador lógico central (CLC, Central Logic Computer), que incluye dos canales paralelos de cálculo, un ordenador lógico central N (CLC N) y un ordenador lógico central B (CLC B), cada uno de los cuales tiene una unidad de comprobación y protección, diseñada para controlar de manera intrínsecamente segura la redundancia de los dos canales de cálculo.

La figura 8 muestra un diagrama de bloques más detallado de la arquitectura de las dos unidades de comprobación y protección, denominadas unidades de control vital del ordenador lógico central (CLCVCU, Central Logic Computer Vital Control Units).

La figura 9 muestra un diagrama más detallado de la figura 8.

La figura 10 muestra un diagrama de flujo de los datos del ordenador lógico central (CLC) entre los dos canales de procesamiento (CLC N y CLC B).

La figura 11 muestra un diagrama de bloques detallado de la tarjeta de comprobación y protección de la unidad de comprobación y protección de una de las dos unidades de procesamiento del ordenador lógico central.

La figura 12 muestra un diagrama de tiempo de las etapas decisivas del ciclo de procesamiento del ordenador lógico central de respaldo en caliente, de dos canales.

Aunque el ejemplo de las figuras se refiere a unidades de procesamiento y/o de control de un sistema de estación ferroviaria, no se deberá interpretar que esta invención está limitada por el mismo, dado que es aplicable a cualquier aparato de procesamiento que tenga que llevar a cabo funciones intrínsecamente seguras y utilice hardware no intrínsecamente seguro para desarrollar algoritmos de procesamiento.

Haciendo referencia a la figura 1, el sistema que se muestra en el diagrama de bloques comprende múltiples elementos de maniobras, tales como circuitos de vías, señales, conmutadores y otros elementos accionadores remotos, por ejemplo módulos 2, 2', 2'' de generación/recepción de códigos (MGRC), que controlan los circuitos de las vías, un módulo 3 de gestión de entrada/salida vitales (VIOMM, vital input/output management module), ordenadores de lógica de zona (ZLC, zone logic computers) 4, 4', 44'', que comunican con un ordenador lógico central (CLC). La comunicación se produce por medio de diferentes tipos de redes, indicadas por los numerales 5 y 6, y definidas como Fnet (Field Network, red de campo) y Znet (Zone Network, red de zona) respectivamente. El ordenador lógico central 1 comunica además con un terminal de operador 7, o OT, con un sistema 8 de

mantenimiento y diagnósticos, denominado MDS-GS y con una o varias interfaces vitales hombre máquina 9, 9', denominadas VMMI. En este caso, la comunicación se produce mediante una red de comunicación 10 indicada como Cnet (Central Network, red central).

Tal como resulta evidente y se describirá en mayor detalle a continuación, el ordenador lógico central 1 (CLC) tiene un funcionamiento de respaldo en caliente de doble canal. Esto significa que, tal como se muestra en la figura 1, el ordenador 1 se compone de dos ordenadores lógicos centrales 101, 201 (CLC N y CLC B) que llevan a cabo funciones paralelas de recogida de datos de entrada desde accionadores o unidades remotas 2, 2', 2'', 3, 4, 4', 4'', 7, 8, 9 y procesamiento de las mismas para generar datos de salida. Además, controlan las comunicaciones en las diferentes redes de comunicación 5, 6, 10 con diferentes protocolos y diferentes modos de seguridad.

Las salidas de los dos canales de procesamiento de los ordenadores lógicos centrales 101, 201 se controlan con una operación de respaldo seguro y en caliente, que significa que ambos ordenadores adquieren datos de entrada y los procesan, pero uno de los dos ordenadores no es activado para transmitir datos de salida. Sin embargo, el ordenador desactivado está dispuesto para asumir la función del ordenador activado, ya sea cuando se le ordena hacerlo o cuando se produzca un fallo de funcionamiento en el ordenador activado.

Además, varios subsistemas o accionadores dedicados entre los descritos en la presente memoria pueden tener una estructura de hardware/software según esta invención, es decir, comprender una unidad de procesamiento basada en hardware comercial no intrínsecamente seguro, que está asociada con una unidad de comprobación y protección que comprueba la ejecución adecuada de funciones mediante la unidad de procesamiento y, después de esta comprobación del funcionamiento adecuado, actúa sobre interfaces o accionadores diseñados para determinar la recuperación segura de las unidades remotas u operativas controladas por la unidad de procesamiento, teniendo de ese modo el conjunto de hardware y software de procesamiento no intrínsecamente seguro y el hardware y software de comprobación y protección funcionando en un modo intrínsecamente seguro.

Un primer ejemplo de estos subsistemas de procesamiento dedicados, según la invención, es el subsistema de interfaz vital hombre máquina (VMMI), que está indicado por los numerales 9, 9' en la figura 1, y se muestra en mayor detalle en el diagrama de la figura 2.

El sistema se compone de una unidad de procesamiento (unidad de procesamiento de gráficos, GPU) 109. Esta unidad de procesamiento está diseñada especialmente para la comunicación, el procesamiento y la generación de imágenes. La unidad de gráficos GPU 109 utiliza hardware comercial y tiene una arquitectura multiprocesador basada en un bus de interfaz de componentes periféricos compacta (CPCI, Compact Peripheral Component Interface). Esta disposición permite utilizar la capacidad de cálculo, flexibilidad y configurabilidad del subsistema, reduciendo al mismo tiempo los costes de desarrollo y fabricación. La unidad GPU 109 es asimismo adaptable a cualesquiera desarrollos y mejoras futuras, en vista de las expectativas de desarrollo de los dispositivos basados en bus CPCI. La unidad GPU no tiene características intrínsecamente seguras.

La interacción con otros subsistemas del sistema, tal como se muestra en la figura 1, se proporciona por un canal Ethernet 10/100 Mbit/s que es redundante en cuanto a disponibilidad, y permite conectar al subsistema de la línea CNET 10 del sistema. La información del subsistema se proporciona al operador por medio de pantallas gráficas 11. Cada subsistema de VMMI 9 puede manejar hasta dos pantallas gráficas independientes 11, 11'; cada pantalla gráfica puede representar un cuadro sinóptico o ciertas especificaciones definidas en la etapa de configuración. Si se requiere un mayor número de pantallas o estaciones de trabajo de operador, el sistema se configurará de tal modo que tenga múltiples interfaces vitales VMMI 9, tal como se muestra en la figura 1.

La interfaz de operador presenta además un teclado funcional 12, que permite entradas de control vital y no vital.

La información de estado del subsistema y los resultados de las pruebas de autodiagnóstico se transmiten a través de la red CNET 10. Una poca información de diagnóstico concisa, particularmente en relación con el teclado funcional, se transmite al operador por medio de una pantalla alfanumérica, que está integrada en el teclado funcional 12.

La unidad de procesamiento de gráficos 109 se compone, a su vez, de varios módulos que realizan varias funciones.

209 indica una unidad de alimentación que proporciona las tensiones requeridas a las diversas unidades.

Las tarjetas VMMIMAIN 1 y VMMIMAIN 2 (Vital Man Machine Interface Main, interfaz vital hombre máquina principal), indicadas por los numerales 309 y 309', son tarjetas CPCI 6U de una sola ranura, que están definidas como CPU periféricas. Estas tarjetas son idénticas, excepto por el hecho de que solamente una de ellas está conectada a la unidad de comprobación y protección 119, denominada IPU (Interface and Peripheral Unit, unidad de interfaz y periféricos). Habitualmente, las tarjetas utilizan un procesador Intel Pentium, o superior.

Las tarjetas VMMIMAIN 309, 309' pueden utilizar potencialmente diversos sistemas operativos. El nivel de seguridad requerido para operaciones vitales de procesamiento llevadas a cabo por la unidad de VMMIMAIN prohíbe la utilización de un sistema operativo multitarea, siendo las operaciones estrictamente cíclicas y secuenciales. Por lo tanto, se requiere un entorno DOS para esta tarjeta.

Las tarjetas CPU periféricas tienen un puente particular, denominado puente no transparente (ver, por ejemplo, DEC21554) que permite que el sistema sea visto por el bus CPCI 409 como un solo agente PCI. El bus PCI es accedido por medio de un puente que puede generar ciclos de "lectura de línea" y "lectura múltiple" PCI, que proporcionan un alto rendimiento de lectura de bloques de datos del bus CPCI.

Una interfaz EIDE (no mostrada) permite que las unidades VMMIMAIN 309, 309' sean conectadas a un disco duro EIDE para arranque de fábrica y configuración BIOS. Alternativamente, la configuración BIOS se puede realizar por medio de una interfaz de disquete. Está disponible un canal 509 RS232 EIA RS232 en serie para permitir la conexión con el conjunto de IPU 119.

Las tarjetas VMMIMAIN 309, 309' están diseñadas para llevar a cabo las funciones siguientes:

- Capa de seguridad FSFB/2. FSFB/2 es una capa del protocolo de comunicación que se utiliza para transmitir información vital entre los diferentes subsistemas, tal como se muestra en la figura 1.

- Reconstrucción de imagen de memoria de pantalla en función de la vista seleccionada y del estado de los elementos de maniobras, recibido por el subsistema CLC 1.

- Comprobar la imagen visualizada actualmente, en base al valor de la palabra de código y al estado de la memoria de pantalla.

- Eco de entrada. Visualizar el eco de las pulsaciones tecleadas por el operador en el teclado funcional 12.

- Análisis sintáctico y construcción de control. La VMMIMAIN comprueba que la secuencia de pulsaciones pertenece una secuencia de control válida y, tras el reconocimiento de la pulsación ENTRAR, conforma y transmite al área de eco el control visualizado actualmente.

- Comprobación de integridad de los datos de configuración. En cada ciclo se vuelve a comprobar si hay corrupción en una parte de los datos de configuración.

Funciones de diagnóstico

La tarjeta de comunicación vital hombre máquina (VMMICOM, Vital Man Machine Communication), indicada por el numeral 609 en la figura 2, es una tarjeta CPCI 6U de una ranura, definida como una CPU de sistema. La tarjeta VMMICOM 609 está asignada todas las funciones de comprobación en comunicaciones de bajo nivel con subsistemas externos, incluyendo el almacenamiento masivo. La disponibilidad de una ranura PMC o PC-MIP (no mostrada en detalle) es una característica preferida. El bus PCI es accedido por medio de un puente que puede generar ciclos de "lectura de línea" y "lectura múltiple" PCI, que proporcionan un alto rendimiento de lectura de bloques de datos del bus CPCI 409. La tarjeta lleva a cabo la función de controlar los accesos al bus CPCI 409. Una interfaz EIDE (no mostrada) permite que las tarjetas VMMICOM 609, 309' sean conectadas a un disco duro EIDE para el arranque de fábrica de la tarjeta y la configuración BIOS. Alternativamente, la configuración BIOS se puede realizar por medio de interfaces de disquete. La tarjeta VMMICOM 609 requiere una gran área de memoria para el intercambio de páginas de pantalla. La sección de intercambio permite almacenar las páginas de pantalla que no se visualizan actualmente; esta unidad no tiene necesariamente una correspondencia física, biunívoca, con un componente, pero no sólo se puede disponer como una expansión de memoria del bus CPCI, sino que se asigna asimismo como un recurso interno, a cada unidad de VMMICOM 609 y unidad de VMMIMAIN 309, 309'. La sección de intercambio se tiene que componer de RAM y tener un tamaño tal como para contener 15 MB para que se visualice cada vista de estación.

La unidad de memoria de interfaz vital hombre máquina (VMMIMU, Vital Man Machine Interface Memory Unit), indicada por 709, está diseñada para soportar dispositivos para almacenar datos de configuración del subsistema y del código de aplicación utilizado por los diferentes microprocesadores de la sección de procesamiento de gráficos GPU 9. En una realización preferida particular, los dispositivos de almacenamiento satisfacen los siguientes requisitos mínimos: formato PCMCIA II; velocidad de transferencia de datos hacia/desde flash = 4 MB/s; tamaño de hasta 1 GB, que puede variar en función de la aplicación. La tarjeta VMMIMU puede estar dispuesta en un formato CPCI 6U, 3U, con el panel 6U estando ajustado en la misma, o en un formato PCI subordinado (PMC o PC-MIP).

La tarjeta VMMIMU 709 permite el acceso frontal a 2 discos flash ATA 2 en un formato de tarjeta de memoria PCMCIA II (no mostrado). Los dos discos flash contienen por separado los datos de configuración del sistema y el software de aplicación, asegurando de ese modo la independencia entre datos de código y datos de aplicación.

Se accede al almacenamiento masivo, en modo sólo lectura, cuando el subsistema se conecta o en durante un restablecimiento.

La tarjeta controladora CNET 809 pone a disposición la interfaz 10/100 baseT Ethernet redundante, y permite la conexión de la unidad de procesamiento de gráficos GPU 9 con el conmutador central de la red CNET, asegurando de ese modo la redundancia física de la línea de comunicación. La tarjeta CNET puede estar dispuesta en un formato CPCI 6U, 3U, con el panel 6U estando montado en la misma, o en un formato PCI subordinado (PMC o PC-MIP). No está instalado ningún software de aplicación en la tarjeta controladora CNET. La redundancia de conexión

está controlada totalmente mediante controladores de bajo nivel, asociando una única dirección de IP, correspondiente a una única pila lógica TCP, a ambos canales, por lo que esta función no necesita estar controlada mediante un software de aplicación.

La tarjeta SVGA 909, 909' está diseñada para transferir el video procesado por la VMMIMAIN 309, 309' a pantallas gráficas 11, 11', y es un recurso exclusivo de la tarjeta VMMIMAIN 309, 309'. Preferentemente, los controladores de video en uso satisfacen los siguientes requisitos mínimos: SGRAM (Synchronous Graphics RAM, RAM síncrona gráfica) de 4 MB, una resolución de 1600x1200 píxeles y 256 colores (8 bits por píxel); una interfaz PCI (formato PMC, PC-MIP o CPCI). La conexión está dispuesta en la parte frontal, por medio de un conector RS343A VAG estándar.

Las tarjetas SVGA 909 se conectan con las salidas de los monitores 11, 11' por medio de una interfaz de comunicación que es supervisada por la unidad de comprobación y protección.

La unidad de comprobación y protección IPU 119 está diseñada especialmente para funciones de protección y utiliza hardware propietario, ad hoc, a diferencia de la unidad de procesamiento de gráficos GPU 109. Esta disposición está determinada por la necesidad de obtener un macro-componente seguro que pueda llevar a cabo funciones de protección, y por la necesidad de implementar ciertas soluciones de hardware con modos vitales que no puede asegurar el hardware comercial, tal como se describe más adelante. La unidad de comprobación y protección 119 está diseñada para controlar los resultados de procesamiento de la unidad de procesamiento GPU y para proteger el sistema contra fallos relacionados con seguridad. Ésta incluye algunas funciones de hardware intrínsecamente seguras, por lo que se compone de tarjetas fabricadas especialmente.

Por lo tanto, mientras que la unidad de procesamiento de gráficos GPU, indicada por el numeral 109, solamente lleva a cabo funciones de comprobación, la unidad de comprobación y protección IPU, indicada por el numeral 119, lleva a cabo todas las funciones de protección, así como las funciones de comprobación relacionadas con la gestión de las pantallas 11, 11' y de la tarjeta funcional 12.

La unidad de comprobación y protección, que se denomina unidad de interfaz y periféricos (IPU) está indicada por el numeral 119 como una fuente de alimentación 219 y dos módulos principales: el módulo de unidad de control vital de interfaz vital hombre máquina (VMMIVCU, Vital Man Machine Interface Vital Control Unit), indicado como 319, y el módulo de aplicación de interfaz vital hombre máquina (VMMIAP, Vital Man Machine Interface Application module), indicado por el numeral 419.

El módulo VMMIVCU 319 es un módulo propietario está diseñado para funciones tanto de comprobación como de protección. Este módulo tiene la función de concentrar todas las palabras de comprobación proporcionadas por el subsistema, comprobar la secuencia adecuada de las mismas y proporcionar a la GPU una marca de tiempo apropiada, así como una contribución vital para el comportamiento de las operaciones de procesamiento de gráficos, contribución vital que se utiliza posteriormente durante la transmisión de variables vitales remotas para certificar un funcionamiento adecuado; la VMMIVCU controla la interfaz RS232 en serie 509 para la conexión de la unidad de procesamiento de gráficos GPU 9 y la interfaz no vital con el teclado funcional 12;

La VMMIVCU está interconectada con el módulo 419 aplicación del VMMIAP por medio de un puerto digital de propósito general 719. El módulo de VMMIAP 419 permite especializar la IPU para la aplicación específica de interfaz vital hombre máquina VMMI. Particularmente, el módulo actúa como una interfaz física con el teclado funcional, tal como se muestra mediante el bloque funcional 519, y con las pantallas gráficas, tal como se muestra mediante los bloques funcionales 619, 619'. El módulo de VMMIAP recibe directamente tensiones para los monitores de video 11, 11' y la interfaz al teclado funcional 12 desde la sección de protección sobre el módulo de VMMIVCU 319, tal como se describe en mayor detalle a continuación.

Las figuras 3 a 5 muestran en mayor detalle las estructuras y características de las unidades componentes de la unidad de comprobación y protección 119.

Tal como resulta evidente a partir de estas figuras, el módulo de comprobación y protección VMMIVCU 319 se compone de dos secciones independientes, una primera sección de comprobación 1319 y otra sección, denominada controlador de potencia vital 2 (VITAL POWER CONTROLLER 2, VPC2) que está dedicada a la función de protección y está indicada mediante el numeral 2319. El principio de esta arquitectura de unidad de microprocesador intrínsecamente segura se conoce, por ejemplo, por la memoria US 4.553.200, que se contempla como parte de esta descripción.

En la figura 4, los bloques funcionales del módulo de VMMIVCU 319 que pertenecen a la sección de comprobación 1319 se muestran en gris.

La lógica de procesamiento de la VMMIVCU se obtiene físicamente por medio de un procesador Intel 80386, indicado por el numeral 20. Esta disposición proporciona a la potencia de procesamiento necesaria, utilizando un procesador de arquitectura simple. La lógica de procesamiento de la VMMIVCU lleva a cabo las funciones siguientes:

Sincronizar los procesos de las unidades de procesamiento de gráficos GPU, y de la unidad de comprobación y protección IPU 119. Cada ciclo de procesamiento, la lógica de la VMMIVCU 319 produce una marca de tiempo vital, que se denomina VSN (Vital Sequence Number, número de secuencia vital) del subsistema. El VSN es un valor que progresa, un ciclo tras otro, por medio de una sucesión predeterminada de estados. El VSN es utilizado como una referencia temporal por todos los módulos de la sección de comprobación, tanto de la unidad de procesamiento de gráficos GPU como de la unidad de comprobación y protección IPU. Tal como se explica mejor en la descripción funcional, la marca de tiempo VSN proporciona protección contra la presencia de datos obsoletos en los procesadores que utilizan una memoria caché, y en particular en la tarjeta de VMMIMAIN 309, 309'.

La comunicación con la unidad de procesamiento GPU 109 se produce por medio de la línea de comunicación RS232 asíncrona dedicada y proporciona la transmisión de la información siguiente:

desde la GPU a la IPU: las palabras de comprobación producidas por algoritmos vitales residentes en GEA. La CPU 20 refleja esta información al módulo de protección VCP2 2319;

desde la IPU a la GPU: todos los datos obtenidos del teclado funcional, así como la marca de tiempo VSN generada por la unidad de comprobación y protección IPU en cada ciclo de procesamiento.

La CPU 386 20 transmite las palabras de comprobación producidas por los algoritmos contenidos en la unidad de procesamiento de gráficos GPU y la unidad de comprobación y protección IPU, por medio de una memoria de dos puertos 22, a la sección de protección VPC2 2319. Los accesos de memoria están sincronizados con la ayuda de indicadores;

La sección de comprobación 1319 comunica con el módulo de aplicación (VMMIAP) 419. Esta comunicación se produce a través de un puerto digital paralelo de propósito general 719 y la información intercambiada incluye: el estado codificado de la tecla ENTRAR, obtenido por el VMMIAP; el resultado de las pruebas de diagnóstico no vitales llevadas a cabo sobre amplificadores de video.

Se obtiene la comunicación mediante la línea de comunicación RS232 asíncrona dedicada 23 y proporciona la transmisión de la siguiente información: los datos de pulsaciones no vitales, obtenidos por la VMMIVCU desde el teclado funcional 12; los datos dirigidos a la pantalla del teclado funcional 12, proporcionados por la VMMIVCU;

Está dispuesto asimismo un divisor polinomial 24, para llevar a cabo funciones de división polinomial por hardware. Esta función es utilizada ampliamente por algoritmos dedicados de generación de palabras de comprobación (ver la memoria US 4.553.200) y se utiliza asimismo, tal como se describe a continuación en mayor detalle, para generar marcas de tiempo VSN. La implementación por hardware del algoritmo de división polinomial permite acelerar todos los algoritmos vitales que residen en la lógica de la VMMIVCU.

Se utiliza una EEPROM flash 25 para contener el código de aplicación y los datos de configuración utilizados por la lógica de procesamiento de la VMMIVCU.

La memoria de dos puertos 22 actúa como una interfaz física entre la lógica de comprobación 1319 y la lógica de protección 2319. La información intercambiada a través de este área, así como ciertos parámetros de configuración e indicadores de sincronización, son solamente las palabras de comprobación producidas por los algoritmos que residen en las diferentes lógicas de la sección de comprobación.

El módulo de VMMIVCU 319 tiene unos pocos puertos de E/S para funciones no vitales, tales como el control de estado de abordo y LEDs de diagnósticos, y como puertos para la descarga de SW.

En la figura 5, los bloques funcionales de la sección de protección 2319 se muestran en gris. Esta sección incluye el módulo VPC2 que se interconecta con la CPU 20 de la sección de comprobación por medio de una memoria de dos puertos. El componente VPC2 tiene solamente la función de proporcionar tensión de salida vital si está presente en su entrada el flujo previsto de palabras de comprobación; este componente consiste en un microprocesador 8085 que ejecuta la lógica de comprobación de palabras de comprobación 30 (figura 3) y un filtro vital intrínsecamente seguro 31.

Como resultado de la validación mediante la lógica residente en el microprocesador 30, se generan dos señales hacia el filtro vital 31, que tienen características precisas de forma de onda (ondas cuadradas con diferentes frecuencias y ciclos de trabajo). Estas señales son utilizadas por el filtro vital para la generación de potencia 32, de 1,5 W a 12V.

La tensión vital se genera solamente si la sección de comprobación proporciona cíclicamente, cada 50 ms, las denominadas palabras de comprobación, utilizando la memoria compartida 22.

En cada ciclo de 50 ms, denominado ciclo de re-comprobación, la sección de protección 2319 obtiene las diversas palabras de comprobación proporcionadas por la sección de comprobación 1319 y procesa palabras de comprobación proporcionando al mismo tiempo la tensión vital, en base a su valor, actuando sobre el filtro activo.

Como resultado de la validación mediante la lógica residente en el microprocesador 8085, se generan dos señales hacia el filtro vital 31, que tienen características precisas de forma de onda (ondas cuadradas con diferentes frecuencias y ciclos de trabajo, a 5 kHz y 500 Hz respectivamente, que tienen una relación de fases bien definida). Estas señales se utilizan para generar una tensión vital utilizada por el VMMIAP. Cada 50 ms, las formas de onda se regeneran cíclicamente en base a las palabras de comprobación recibidas por la sección de comprobación.

Durante la comprobación de corrección o consistencia, la lógica de verificación de palabras de comprobación consume palabras de comprobación de manera destructiva, asegurando de ese modo que un conjunto determinado no puede ser utilizado más de una vez. El bloque 31 de filtro vital activo (AVF, Active Vital Filter) garantiza la disposición de la frecuencia de salida de 5 kHz (la señal de activación es transmitida solamente al VG (Vital Generator, generador vital) 32 si las dos frecuencias de entrada procedentes de la lógica de verificación de palabras de comprobación tienen las características esperadas de frecuencia y ciclo de trabajo. El bloque está realizado con circuitos analógicos de seguridad intrínseca. La salida del filtro activo se utiliza como una señal de activación para el generador vital (VG) 32; éste es un suministro de potencia que se supone genera una tensión vital de +12,5 VDC, con una salida continua disponible máxima de 1,5 W. En el generador está implementado un circuito de conversión CC-CC de seguridad intrínseca, que tiene características tales que asegura solamente la generación de tensión vital cuando el filtro activo 31 proporciona una señal de activación.

El módulo de aplicación de interfaz vital hombre máquina (VMMIAP) 419 consiste en una tarjeta propietaria que lleva a cabo funciones específicas de aplicación de VMMI. En particular, esta tarjeta controla la adquisición del estado de la tecla ENTRAR desde el teclado funcional; el suministro de alimentación al teclado funcional 12; y asegura el aislamiento de las interfaces con el operador, cuando no hay tensión vital.

El módulo 419 de aplicación del VMMIAP recibe de la sección de protección 2319 la tensión generada de forma segura como una autorización de funcionamiento del subsistema. Este módulo utiliza la tensión vital para hacer funcionar amplificadores de video 619, 619' y los circuitos de interfaz 519 con la tecla ENTRAR del teclado funcional 12.

Cuando la sección de protección 2319 no proporciona autorización, el módulo 419 asegura que si se detecta un conjunto de palabras de comprobación erróneas, la tensión vital cae por debajo de un umbral predeterminado dentro de un tiempo máximo de 400 ms. Esto permite: cancelar una imagen errónea en un tiempo de respuesta predeterminado de 1 s, que incluye los tiempos de ciclo del subsistema, y desactivar controles vitales, desactivándose los circuitos de detección del estado de la tecla ENTRAR.

La interfaz con la tarjeta VMMIVCU se compone de un puerto de E/S digital 719 del VMMIAP de propósito general (figura 2).

En la figura 6 se muestra un diagrama de bloques funcional del bloque 419 de aplicación del VMMIAP, que destaca en gris los bloques funcionales relacionados con la seguridad.

El numeral 27 indica los circuitos de preparación de la tensión vital asignados al VMMIAP 419. Estos circuitos tienen solamente la función de generar tensiones específicas para amplificadores de video 619, 619' y para la interfaz con las teclas vitales del teclado funcional 12, desde la tensión vital de 12 V generada por el VPC2 2319 al módulo 319 de la VMMIVCU. La interfaz vital 519 con el teclado funcional 12 está diseñada para interactuar con un circuito de codificación de la tecla ENTRAR, que no se muestra en detalle y está montado en el teclado funcional 12 para detectar el estado de la misma. El teclado funcional 12 tiene tanto controles de funcionamiento normal como controles de emergencia. Las teclas están divididas en conjuntos homogéneos, en función de sus funciones; los diversos conjuntos están dispuestos de izquierda a derecha, según una lógica de entrada de control. La lógica de adquisición del estado de la tecla ENTRAR está diseñada con criterios intrínsecamente seguros. El FK integra además una pantalla alfanumérica, dos timbres y una tecla de activación de tres posiciones. La arquitectura del teclado funcional se compone de tres tableros diferentes, conectados por un cable plano, un tablero que contiene los botones y la tecla; un tablero que contiene la pantalla LCD; un tablero de control que es una CPU y utiliza el microprocesador Intel 80C51FA1 de 16 MHz.

La interfaz se compone físicamente de 4 líneas EIA en serie 422, que se utilizan como sigue:

INV_OPEN: codificación de 32 bits de estado de tecla abierto.

INV_CLOSED: codificación de 32 bits de estado de tecla cerrado.

BIT_CLOCK, WORD_CLOCK: utilizado para transmitir información de sincronismo (bits y palabras).

El suministro de potencia a los receptores diferenciales utilizados para el canal de datos es proporcionado por el VPC2. Por lo tanto, un fallo del VPC2 impide la generación de controles vitales, interceptando la codificación del estado de la tecla ENTRAR. La tarjeta VMMIAP 419 transfiere la tensión de 5 V al teclado funcional 12. Los amplificadores 619, 619' tienen la función de amplificar las señales de video R/G/B transmitidas a los monitores de video. Estos se hacen funcionar mediante la tensión vital generada por el VPC2 2319. La ausencia de tensión vital hace que las señales de video desaparezcan. El módulo de VMMIAP 419 contiene 6 amplificadores 619, 619', por lo que puede controlar las señales de componentes de tres colores para dos pantallas gráficas.

El VMMIAP 419 incluye asimismo un módulo 29 de diagnóstico de la señal de video, que muestrea el nivel de la señal a la salida de los amplificadores de video 619, 619', sincronizado con la señal de sincronización de video en cuanto se actualiza la primera línea de píxeles del video. Esta línea se controla asimismo con un color blanco brillante asignado por el software de aplicación; al leer la señal de video generada cuando se visualiza la primera línea, se realiza un equilibrio de color adecuado.

El funcionamiento del sistema indicado anteriormente es como sigue:

El sistema puede visualizar las vistas sinópticas que el operador selecciona por medio del teclado funcional. Las vistas son reconstruidas por la unidad de procesamiento de gráficos GPU 109 en base a los datos recibidos por el ordenador lógico central CLC, indicado por el numeral 1 en la figura 1. El teclado funcional permite generar controles vitales y no vitales, cuyo eco se visualiza en los monitores, y que se transmiten a la unidad de procesamiento de gráficos GPU 109 para su transmisión al ordenador lógico central CLC 1.

Durante este proceso, la unidad de comprobación y protección 119 de la VMMIVCU lleva a cabo operaciones de comprobación y protección. En primer lugar, durante cada ciclo de procesamiento del ordenador lógico central, que dura aproximadamente 500 ms, se generan palabras de comprobación de certificación cada 50 ms para datos transmitidos a la unidad de procesamiento de gráficos GPU 109, así como palabras de comprobación para la re-comprobación de las vistas gráficas reconstruidas a partir de éstos y presentes en la memoria de pantalla. La unidad de procesamiento de gráficos ejecuta además una operación de volver a comprobar los datos de configuración del sistema, y el código de procesamiento de aplicación contenido en las memorias de VMMIMU, y genera una palabra de comprobación invariante interna. Se genera asimismo una palabra de comprobación invariante como resultado de una comprobación de consistencia de los datos de entrada frente a los datos visualizados por los monitores 11, es decir, los datos de salida de la unidad de procesamiento. Todas las palabras de comprobación son además asociadas, es decir marcadas, con la marca de tiempo VSN del ciclo de procesamiento en ejecución. Las palabras de comprobación generadas de este modo se transmiten mediante la sección de comprobación 1319 de la unidad de comprobación y protección de la VMMIVCU a la sección de protección VPC2 2319, que solamente lleva a cabo una verificación de palabras de comprobación. Si las palabras de comprobación son incorrectas, la sección de protección corta la tensión vital a los amplificadores 619, 619' que reciben señales de los controladores gráficos SVGA 909 de la unidad de procesamiento de gráficos 109, impidiendo de ese modo que estas señales sean visualizadas.

Las marcas de tiempo VSN tienen el efecto de impedir que permanezcan en la memoria caché del procesador de la unidad de procesamiento de gráficos datos de ciclos de procesamiento anteriores, de manera que los datos de salida calculados por la unidad de procesamiento de gráficos no puedan ser inconsistentes con la situación actual. En este caso, las marcas de tiempo VSN permiten evitar este inconveniente. Los datos vitales se asignan a un número VSN en un esquema XOR, que identifica exclusivamente el ciclo de procesamiento actual. Por lo tanto, la vida útil de los datos marcados será igual al ciclo de procesamiento.

Esta función se lleva a cabo mediante un generador de marcas de tiempo que es una característica de la sección de comprobación. La generación de marcas de tiempo y la comunicación de las mismas a la unidad de procesamiento de gráficos y/o a la unidad de control del teclado funcional 12 representan el inicio de un nuevo ciclo de procesamiento, y permiten la sincronización de los diversos procesos del sistema.

La marca de tiempo VSN pertenece a una secuencia pseudoaleatoria generada por sucesivas divisiones polinomiales a partir de una semilla asignada. Este modo de generación asegura la variación de un número suficiente de bits entre dos VSN sucesivos.

Se generan marcas de tiempo en un modo de cálculo redundante con un diagnóstico de ruptura del tiempo vital. La detección del funcionamiento adecuado del generador de marcas de tiempo VSN está basada en las propiedades algebraicas de la operación de división polinomial de cadena binaria, que consiste en que la función de división polinomial sobre una cadena de N bits se puede simular mediante un cálculo matricial. En este caso, los algoritmos de comprobación incluyen la determinación de una palabra de comprobación invariante y la transmisión de la misma a la sección de protección, de manera que ésta certifica el funcionamiento adecuado del generador de marcas VSNG.

En relación con el teclado funcional, se generan palabras de comprobación que estiman la corrección de la tecla ENTRAR, es decir la tecla que pulsa el operador para indicar su voluntad de transmitir un control vital. En este caso, el control vital se marca en tiempo y se valida mediante la sección de protección antes de ser transmitido a la unidad de procesamiento de gráficos GPU 109 para ser transmitido posteriormente al ordenador lógico central CLC 1. Las marcas de tiempo aseguran que el control transmitido está sincronizado con el ciclo de procesamiento de la unidad de procesamiento de gráficos GPU 109 y con el ordenador lógico central CLC 1. Si se descubre que la marca de tiempo de control es inconsistente con una de las unidades de procesamiento de gráficos, entonces el control no se transmite o ejecuta. El control se vuelve a comprobar además y, como resultado, se generan las palabras de comprobación, asimismo generando palabras de código en función de las pulsaciones del teclado funcional, que se envían como tales a la unidad de protección para su validación. Si las palabras de comprobación son erróneas, la sección de protección actúa sobre el generador de potencia del módulo de VMMIAP 419 y corta la tensión vital al teclado.

De nuevo haciendo referencia a la figura 1, el subsistema de ordenador lógico central CLC, indicado por el numeral 1, está diseñado especialmente para el procesamiento seguro de la lógica del sistema, en base al estado de los elementos de maniobras 2, 2', 2", 3, 4, 4', 4" y a los controles introducidos por los operadores 7, 9, 9'.

El subsistema CLC 1 se diseñó como una aplicación general para satisfacer todos los requisitos de control para maniobras físicamente diferentes, posiblemente gestionadas por diferentes diagramas de criterios. Por lo tanto, el sistema fue diseñado para ejecutar cualquier lógica del sistema definida por ecuaciones booleanas. Éste es un subsistema cíclico, y el tiempo de ciclo en el que se basa la actualización del estado de salida vital se denomina ciclo principal y dura 500 ms. Las ecuaciones booleanas utilizadas para determinar la lógica de un cierto sistema se definen en fábrica, en función de la topografía de la estación, y de reglas de manipulación aplicables, y son traducidas además a estructuras de datos, por medio de herramientas de configuración especiales. La estructura de datos relacionada con las ecuaciones permite configurar el subsistema para cualquier aplicación sin necesidad de realizar cambios en el software de procesamiento. El CLC 1 está conectado con los otros subsistemas mediante las redes CNET 10, ZNET 6 y FNET 5. A través de estos canales, y utilizando protocolos propietarios adecuados a nivel de aplicación, el CLC 1 puede intercambiar con los mismos variables relacionadas con la lógica e información de diagnóstico. El ordenador lógico central 1 es una unidad esencial para llevar a cabo las funciones principales del sistema. Por lo tanto, para proporcionar una alta disponibilidad, éste se compone de dos unidades de procesamiento simétricas 101, 201, dispuestas en una configuración de respaldo en caliente, tal como se muestra en las figuras 1, y 7 a 10. Las dos unidades de procesamiento 101, 201 se denominan CLC N (ordenador lógico central - normal) y CLC B (ordenador lógico central - respaldo). Las dos unidades de procesamiento 101, 201 pueden llevar a cabo de forma individual y segura las funciones del CLC 1, y en particular la adquisición de entradas en paralelo y la solución independiente de las ecuaciones booleanas, pero los resultados de las mismas se transmiten solamente de manera mutuamente excluyente desde una de las dos unidades de procesamiento 101, 201.

Cada unidad de procesamiento 101, 201 puede adoptar los siguientes estados operacionales:

Operativo: la unidad de procesamiento operativa es la que determina el nuevo estado de las variables de salida, en base a los datos recibidos, y transmite estas variables a las unidades remotas 2, 3, 4, 7, 8, 9;

Disponible: la unidad de procesamiento disponible lleva a cabo las mismas operaciones que la unidad operativa, excepto que, una vez que se han resuelto las ecuaciones, alinea sus salidas y su estado interno con los de su unidad de procesamiento gemela y se impide que transmita las salidas a las unidades remotas. Siempre que la unidad de procesamiento "operativa" falla, esta unidad está lista para sustituirla, y para entrar en el modo "operativo".

Inactivo: este estado describe la inicialización de una unidad de procesamiento, y puede ser adoptado por una unidad como resultado de la detección de un fallo, o cuando el sistema se conecta;

Apagado: sistema desconectado.

El ordenador lógico central CLC 1 incluye un dispositivo que permite asociar el estado "operativo" a solamente una de las dos unidades de procesamiento 101, 201, N y B, de tal modo que la transmisión de variables vitales solamente puede estar controlada por una de las dos unidades, mientras que la otra está alineada con la primera.

Con un funcionamiento normal, cada unidad de procesamiento 101, 201 genera variables de estado externas e internas de manera independiente. Las variables anteriores pueden diferir debido a que pueden ser utilizados diferentes valores de entrada, dado que el proceso de adquisición de entrada es totalmente independiente. Para evitar este desajuste de la lógica del sistema y asegurar la continuidad del funcionamiento cuando se conmuta entre las dos unidades de procesamiento, estas últimas intercambian mutuamente de manera cíclica las variables de estado externas e internas determinadas por cada una de ellas, y seleccionan y utilizan el mismo conjunto de variables, que pueden ser el conjunto generado localmente o el conjunto recibido desde la otra unidad.

Las funciones de intercambio de datos y de alineamiento utilizan unidades de comunicación dedicadas internas que conectan las dos unidades de procesamiento CLC N 101 y CLC B 201. El proceso de conmutación, es decir, la transición de la unidad de procesamiento desde el estado "disponible" al estado "operativo" se puede producir como resultado de:

un fallo: la unidad de procesamiento 101, 201 anteriormente "disponible" detecta un 'fallo' en la unidad de procesamiento anteriormente "operativa" (101, 201), y ocupa su lugar;

una solicitud: la unidad de procesamiento 101, 201 en el estado "disponible" conmuta al estado "operativo" y viceversa. Esto se determina mediante un control de conmutación manual, local o remoto, o como resultado de una solicitud automática que se proporciona para impedir que una unidad de procesamiento 101, 201 permanezca en el estado "disponible" más allá de un cierto periodo, lo que puede obstaculizar la plena detectabilidad de fallos latentes en la unidad no utilizada. La solicitud automática provoca asimismo una conmutación cuando la unidad "operativa" está en una situación de funcionamiento "peor" que la unidad "disponible". En este caso, la unidad "operativa" 101, 201 solicitará la conmutación para utilizar los datos producidos por la unidad de procesamiento 101, 201 con menor grado de degradación.

Los anteriores modos de control de redundancia se muestran gráficamente en el esquema de la figura 10.

El ordenador lógico central CLC 1 incluye una interfaz de diagnóstico básico denominada BDI e indicada por el numeral 301. Por medio de esta interfaz, el operador puede reunir información básica acerca del estado de las unidades de procesamiento, el CLC N 101 y el CLC B 201, y puede configurar una de éstas al estado "operativo".

El subsistema soportará funciones de diagnóstico para permitir la detección de fallos. Además, el ordenador lógico central CLC 1 gestionará variables de registro histórico de eventos, ya cableadas en la lógica, y unas pocas variables de monitorización que son útiles para una comprobación de funcionamiento adecuado. Esta información será transferida al sistema de diagnóstico y mantenimiento MDS GS 8, junto con la información de diagnóstico general del ordenador lógico central CLC y otros nodos conectados a las redes ZNET 5 y FNET 6, que no pueden comunicar directamente con el sistema de diagnósticos y mantenimiento DMS GS 8.

El ordenador lógico central CLC 1 tendrá interfaces para conectarlas con la red redundante CNET 10, y con múltiples redes redundantes ZNET 5 y FNET 6. Por medio de estas redes, tanto la unidad de procesamiento 101 CLC N como la unidad de procesamiento 201 CLC B obtienen en paralelo entradas remotas vitales y no vitales desde los diferentes nodos y desde las diferentes unidades remotas 2, 3, 4, 7, 9, y transmiten a éstas el valor de las salidas determinadas cíclicamente. Cabe señalar que la fase de transmisión está diseñada solamente para la unidad de procesamiento 101, 201 "operativa".

Obviamente, cada unidad de procesamiento 101, 201 podrá conectar con cualquiera de las líneas que forman cada red. Las redes CNET, ZNET y FNET son redes de comunicación cerradas, y son compartidas solamente por aplicaciones propietarias. Esta disposición permite reducir las intrusiones no autorizadas y realizar predicciones del tráfico de red.

La utilización de una arquitectura redundante para el ordenador lógico central CLC 1 involucra la necesidad de asociar un 'estado' de funcionamiento a cada una de las dos unidades de procesamiento que lo componen, el CLC normal 101 y el CLC de respaldo 201. Este estado tiene que ser detectado de manera segura por cada unidad de procesamiento 101, 201, dado que esta función involucra la selección de los datos producidos por la sección local de cálculo o por la de la otra unidad de procesamiento. Además, se impedirá que las unidades de procesamiento 101, 201 evalúen de manera no alineada.

Para controlar la redundancia, cada unidad de procesamiento 101, 201 está dotada de un circuito de protección VPC2, indicado por el numeral 2319, que es idéntico al circuito de la sección de protección 2319 del ejemplo anterior, y de un conmutador estático, indicado por el numeral 401 en la figura 8. Cada sección de protección VPC2 2319 recibe en su entrada las diversas certificaciones para confirmar el funcionamiento adecuado de las partes vitales de cada unidad de procesamiento y proporciona a su salida una tensión vital. Si el flujo de certificación es correcto, sin interrupciones, las unidades de procesamiento 101, 201 proporcionan una tensión vital de salida a su propia sección de protección VPC2 2319, pero después de éstas está dispuesto un conmutador estático 401 para permitir solamente la salida de tensión a una de las dos unidades de procesamiento 101, 201. Por lo tanto, se obtienen dos bifurcaciones, en las que puede o no estar presente una tensión vital, y la detección de esta tensión después del conmutador 401 permite determinar si la unidad de procesamiento 101, 201 está o no en el estado "operativo".

Las figuras 7 a 9 describen en mayor detalle la arquitectura que permite las funciones anteriores.

El ordenador lógico central CLC 1 es un subsistema redundante compuesto de dos unidades de procesamiento 101, 201 lógicas, denominadas CLC N y CLC B, que son idénticas tanto en relación con el hardware como con el software. Estas unidades se pueden diferenciar solamente por medio de un identificador HW adecuado, que es releído mediante procedimientos de software.

Tal como se ha descrito anteriormente, las dos unidades de procesamiento 101, 201 pueden llevar a cabo las diversas funciones incluso cuando la unidad gemela está ausente (un funcionamiento independiente).

Cada unidad de procesamiento 101, 201 se compone, a su vez, de dos conjuntos, denominados: unidad de procesamiento lógico (LPU, Logic Processing Unit), indicada por el numeral 40, y unidad de protección y sincronización (PSU, Protection and Synchronization Unit), indicada por el numeral 41, que están interconectadas adecuadamente, y diseñadas cada una para una tarea particular.

El conjunto de LPU 40 lleva a cabo funciones de comunicación y resolución de ecuaciones, y consiste en tarjetas comerciales basadas en buses CPCI (interfaz de componentes periféricos compacta), que están equipados con microprocesadores Intel Pentium. Esta disposición permite utilizar la potencia de cálculo, flexibilidad y configurabilidad del subsistema, reduciendo al mismo tiempo los costes de desarrollo y fabricación. Este conjunto es adaptable asimismo a cualesquiera mejoras y desarrollos futuros, en vista de las expectativas de desarrollo de gran disponibilidad de los dispositivos basados en bus CPCI.

El conjunto PSU es una unidad de comprobación y protección 41 que lleva a cabo funciones de comprobación y protección, y se compone de tarjetas dedicadas basadas en microprocesadores INTEL 80385 y 8085. Esta disposición surge por la necesidad de implementar ciertas soluciones de hardware con modos vitales que no pueden

ser asegurados por hardware comercial. Una tarea básica del conjunto PSU 41 es sincronizar sus respectivas unidades de procesamiento 101, 201 y comprobar el funcionamiento adecuado de las mismas, incluyendo su alineamiento con la otra unidad de procesamiento.

La unidad LPU 40 obtiene de su unidad de comprobación y protección PSU las señales de activación necesarias para el funcionamiento adecuado y transmite a ésta el resultado de sus funciones.

El conjunto LPU o unidad informática 40 es la sección de unidad de procesamiento que calcula la lógica del sistema ferroviario, mientras que los resultados de este cálculo se certifican mediante palabras de comprobación que se transfieren, a su vez, a la unidad de comprobación y protección PSU 41 para su validación.

La arquitectura de la unidad de comprobación y validación corresponde sustancialmente a la de la misma unidad que se ha descrito haciendo referencia a la realización de las figuras 2 a 6, y se compone de una sección de protección y de una sección de hardware y software de aplicación específica, siendo la aplicación en este caso el control de redundancia de los dos canales informáticos proporcionados por las dos unidades informáticas LPU.

Ambas unidades de procesamiento, CLC N 101 y CLC B 202, tienen interfaces para la conexión del subsistema con la red redundante CNET 10, y con múltiples redes redundantes ZNET 5 y FNET 6. Por medio de estas redes, las dos unidades de procesamiento 101, 201 obtienen en paralelo entradas remotas vitales y no vitales de los diferentes nodos y de las diferentes unidades remotas, mientras que solamente se activa la transmisión de la unidad de procesamiento "operativa".

La figura 7 muestra las tarjetas o subunidades individuales que componen cada una de las unidades de procesamiento 101, 201. La tarjeta controladora FNET 140 es de hecho una tarjeta de soporte de PMC, que puede alojar hasta dos módulos de alojamiento PMC, para su utilización para la conexión con dos redes ZNET redundantes, o bien con dos redes FNET redundantes, dado que utilizan el mismo tipo de soporte de transmisión y el mismo modo de comunicación.

El ordenador lógico central CLC 1 contiene otras interfaces para la conexión entre las unidades de procesamiento N 101 y B 201, interfaces que permiten el intercambio de datos resultantes, el procedimiento de alineamiento y el sincronismo entre las dos partes.

Además, el ordenador lógico central CLC 1 tiene una interfaz 310 de operador BDI local que tiene que estar conectada adecuadamente para el control de los dispositivos, y de las entradas y salidas no vitales que lo componen.

El sistema tiene un dispositivo que puede diferenciar, durante la configuración, el ordenador lógico central CLC 1 en las dos unidades de procesamiento CLC N 101 y CLC B 201. Esta función está proporcionada por un identificador de hardware externo (puente), accesible sin extraer las tarjetas, que permite identificar nominalmente los dos aparatos. Este identificador es el único elemento de diferenciación de las dos unidades de procesamiento 101, 201, que por lo además podrían ser idénticas, en términos tanto de HW como de SW. Cada unidad de procesamiento incluirá HW de seguridad intrínseca, para la adquisición vital de esta entrada, de tal modo que el software de procesamiento puede asociar el nombre a la unidad de procesamiento 101, 201 en la que está cargado.

Tal como se ha mencionado anteriormente, la unidad LPU 40 tiene las funciones principales de comunicar con los subsistemas externos, procesar la lógica del sistema e intercambiar con el subsistema redundante las variables calculadas. Todas estas funciones, que se consideran vitales, se certifican mediante una palabra de comprobación transferida a la unidad de comprobación y protección PSU 41.

La unidad LPU 40 tiene las interfaces siguientes:

una interfaz Ethernet externa de 10/100 Mbit/s de dos puertos, que se utiliza para conectar la red central CNET 10 del sistema, controlada lógicamente por la tarjeta CLCCOM (Central Logic Computer Commmunication, comunicación del ordenador lógico central) 42 y montada en la tarjeta de "controlador CNET" 43;

múltiples interfaces RS485 redundantes externas, para la conexión a las redes ZNET y FNET 5 y 6, que están controladas lógicamente por la tarjeta CLCCOM 42 y montadas en múltiples tarjetas de soporte de PMC (incluyendo la CLCCOM);

una interfaz Ethernet externa de 10/100 Mbit/s 44, que se utiliza para intercambiar datos con la unidad de LPU B (o N) 40, controlada por la tarjeta de CLCMAIN (Central Logic Computer Main, ordenador lógico central principal) 45;

una interfaz RS232 en serie interna 46 para la conexión a la unidad de comprobación y protección PSU 41, controlada por la tarjeta CLCMAIN 45.

La configuración básica incluye las siguientes tarjetas, todas equipadas con una interfaz de bus CPCI:

La tarjeta CLCCOM 42 está diseñada para funciones de comunicación de protocolo de bajo nivel para las diversas redes redundantes (CNET, FNET, ZNET) y tiene además que soportar un módulo de alojamiento PMC;

el soporte de PMC es utilizado para añadir hasta dos módulos de alojamiento PMC, es decir, pequeñas tarjetas comerciales que pueden manejar dos redes redundantes cada una, por medio de una interfaz RS485;

La tarjeta CLCMAIN 25 está diseñada para codificar y descodificar variables remotas (es decir, el nivel de transporte del protocolo en uso), para calcular la lógica del sistema y para intercambio de datos;

La tarjeta controladora CNET 43 es una controladora Ethernet de dos puertos de 10/100 Mbit. La tarjeta controladora CNET 43 se utiliza para la conexión con la red CNET 10 y está controlada, a través de la CPCI, por medio de la tarjeta CLCCOM 42.

La tarjeta CLCMU 47 se utiliza como soporte para el almacenamiento masivo de la unidad LPU 40.

Todos los componentes de la unidad LPU 40 están disponibles en el mercado. Esto permite escalar la potencia de cálculo en función de las necesidades reales del sistema y utilizar una arquitectura actualizable en vista de las futuras innovaciones relacionadas con CPCI.

La tarjeta CLCCOM 42 es una única tarjeta Eurocard 6U equipada con un microprocesador INTEL Pentium o superior. Está diseñada especialmente para la función vital NON de completar el protocolo de comunicación de bajo nivel con redes centrales de comunicación externas. El intercambio de datos con los nodos o las unidades remotas conectadas a la red CNET 10 puede estar basado en el protocolo UDP/IP, mientras que el intercambio de datos con los nodos o las unidades remotas conectadas a las redes ZNET y FNET 5 y 6 se basa en el protocolo HDLC, en modo maestro-esclavo, con la CLCCOM actuando como maestro. Las transmisiones a través de las redes estarán controladas exclusivamente por la CLCCOM de una de las dos unidades de procesamiento 101, 201, N o B, es decir la "operativa", mientras que ambas tarjetas reciben simultáneamente datos del exterior.

La tarjeta introducida en un bastidor con un bus CPCI lleva a cabo asimismo funciones de monitorización y arbitraje sobre el bus (tarjeta "de sistema") y gestiona la fase de configuración inicial.

La tarjeta CLCCOM 42 realiza asimismo la función de tarjeta de soporte de PMC, con la tarea de soportar físicamente un módulo de expansión de alojamiento PMC que puede controlar dos redes redundantes, del tipo ZNET o FNET, 5 ó 6, por medio de una conexión RS485. Si el sistema está configurado teniendo múltiples redes ZNET y FNET, el CLC se conecta a las mismas por medio de módulos PMC adicionales montados en tarjetas de soporte de PMC especiales. Estas tarjetas y la tarjeta controladora CNET 43 están controladas lógicamente por la CLCCOM, que por lo tanto es responsable de todas las funciones de monitorización en las comunicaciones de bajo nivel con los subsistemas externos.

Desde un punto de vista funcional, la tarjeta CLCCOM 42 está dedicada especialmente a funciones no vitales. La función de protección de datos vitales, en los sentidos tanto de transmisión como de recepción, está asignada a la tarjeta CLCMAIN 45.

El sistema operativo VxWorks 5.X, de la firma Wind River, está instalado en la tarjeta CLCCOM: la utilización de un sistema operativo comercial no tiene impacto directo en la seguridad, dado que no se asignan funciones vitales a la tarjeta. La CLCCOM interactúa solamente con las otras tarjetas de la unidad LPU por medio del bus CPCI.

La tarjeta CLCMAIN 45 es una sola tarjeta Eurocard 6U equipada con una CPU INTEL Pentium o superior. Habitualmente, tiene las siguientes funciones principales:

Gestión a nivel de aplicación de protocolos de comunicación propietarios que se utilizan para transmitir datos en las redes CNET, FNET y ZNET;

Procesamiento de lógica del sistema;

Intercambio de datos entre las unidades LPU N y B, es decir, de aquellos que pertenecen a las unidades de procesamiento N y B;

Intercambio de datos con la correspondiente unidad de comprobación y protección PSU 41, es decir, transmisión de certificaciones que confirman el funcionamiento correcto de las funciones vitales individuales y recepción de toda la información sobre alineamiento lógico y marcas de tiempo;

Funciones de diagnóstico

La tarjeta CLCMU 47 está diseñada para almacenar datos de configuración de subsistemas y el código de aplicación utilizado por los diferentes microprocesadores. Se accede al almacenamiento masivo, en modo sólo lectura, cuando el subsistema se conecta o durante un restablecimiento.

La tarjeta CLCMU 47 es una única tarjeta Eurocard 6U que aloja dos discos flash de tarjeta de memoria PCMCIA, que contienen por separado los datos de configuración del sistema y el software de aplicación, asegurando de ese modo la independencia entre los datos de código y los datos de aplicación. Alternativamente, la función llevada a cabo por la tarjeta CLCMU 47 puede ser realizada por la tarjeta CLCCOM 42, por medio de un módulo de alojamiento PMC, utilizado en otro caso para comunicaciones de línea en serie.

Los datos de software y/o de configuración se actualizan reprogramando memorias flash. Esto se puede realizar en la fábrica o in situ, utilizando una herramienta de desarrollo portátil.

La unidad de comprobación y protección PSU 41 está diseñada para comprobar y proteger actividades vitales, y para controlar la redundancia de las dos unidades de procesamiento 101, 201. La unidad de comprobación y protección PSU 41 tiene asimismo la función de controlar entradas y salidas locales, incluyendo las del panel BDI 401, de obtener el identificador HW y de detectar la tensión vital suministrada por su propia unidad LPU 40 y por la LPU gemela.

La función de protección proporcionada en la unidad de comprobación y protección PSU 41 utiliza las certificaciones (palabras de comprobación) producidas por todos los algoritmos de las unidades de procesamiento 101, 201, tanto los producidos por la propia unidad de comprobación y protección PSU 41 como los producidos por su propia unidad informática LPU 40. Cuando el flujo previsto de palabras de comprobación falta o está modificado, la función de protección impide cualquier generación de tensión vital.

Otra función importante de la unidad de comprobación y protección PSU 41 es el control de redundancia, que implica una comprobación del alineamiento entre las dos unidades de procesamiento de respaldo en caliente 101, 201. Esta disposición impide la posibilidad de que una unidad de procesamiento de respaldo 101, 201 que cambia al estado "operativo" incurra en un fallo de alineamiento, y provoque por lo tanto una discontinuidad lógica en el sistema.

La unidad de comprobación y protección PSU 41 tiene asimismo la función de generar un valor pseudoaleatorio, denominado VSN, que es utilizado como una marca de tiempo. Este valor identifica de manera única el ciclo de procesamiento actual y se utiliza para marcar los datos vitales en el conjunto de cálculo LEA 40, dado que la presencia de HW comercial que utiliza una memoria caché no permite asegurar una actualización continua de variables cada ciclo.

La unidad de comprobación y protección PSU 41 tiene las siguientes interfaces internas:

la interfaz en serie RS232 46 para la conexión con la unidad informática LPU 40 de la correspondiente unidad de procesamiento, interfaz que está controlada por la sección de control CLCVCU (unidad de control vital del ordenador lógico central) 141;

la interfaz en serie RS485, que se utiliza para controlar el alineamiento y la sincronización lógica con la unidad de comprobación y protección PSU remota, estando controlada esta interfaz por la CLCVCU 141;

un canal 49, que se utiliza para transmitir y recibir sincronismo de hardware con la otra unidad de procesamiento, controlada por la CLCVCU 141.

La unidad de comprobación y protección PSU 41 se compone físicamente de las tarjetas siguientes:

Una unidad de control vital del ordenador lógico central (CLCVCU) 141, que está diseñada para funciones de comprobación y protección, con la función de concentrar todas las palabras de comprobación proporcionadas por las unidades de procesamiento 101, 201 a las que pertenece, para comprobar la secuencia de las mismas, para controlar la redundancia y para dotar a la unidad informática LPU 40 de la marca de tiempo VSN correcta y de la contribución vital, a utilizar posteriormente cuando se transmitan variables vitales remotas para certificar el funcionamiento adecuado de las mismas;

Una tarjeta 241 de aplicación de ordenador lógico central (CLCAP, Central Logic Computer Application), a través de la cual se proporcionan ciertas soluciones de hardware específicas por subsistema. En particular, este módulo actúa como una interfaz con el panel de BDI 401, y como una interfaz para leer el identificador del HW y para detectar la tensión vital. Además, esta tarjeta contiene algunos de los circuitos diseñados para control de redundancia no vital.

Tal como resulta evidente a partir de la figura 8, la tarjeta CLCVCU tiene la misma, o sustancialmente la misma construcción y funciones que la VMMIVCU descrita en la realización anterior de las figuras 1 a 6. La estructura y gestión de palabras de comprobación, incluyendo disposiciones de validación, se describe en detalle, por ejemplo, en la memoria US 4.553.200, mencionada anteriormente en relación con la realización anterior. La tarjeta CLCVCU 141 es una única tarjeta Eurocard 6U con una construcción dedicada, es decir no basada en hardware comercial, que lleva a cabo funciones de comprobación y protección. La sección de comprobación tiene la función de:

gestionar entradas y salidas no vitales;

controlar la adquisición del identificador de HW y de la tensión vital utilizando circuitos HW de seguridad intrínseca, impresos en la tarjeta CLCAP 241;

gestionar palabras de comprobación y pasarlas a la sección de protección, con un sincronismo bien definido;

actualizar el valor de la marca de tiempo VSN en cada ciclo;

transmitir la señal de inclusión a la sección de protección;

controlar la redundancia y toda la lógica de alineamiento y detección de estados, utilizando asimismo los circuitos impresos en la tarjeta CLCAP 241;

controlar la lógica de conmutación no vital, por medio de un conmutador estático que, con una de las unidades de procesamiento de respaldo 101, 201, activa solamente la transmisión de tensión vital a una de las dos unidades de procesamiento 101, 201 paralelas;

generar la señal vital de activación a transmitir con las variables vitales remotas;

controlar las comunicaciones con la unidad informática LPU 40, y más precisamente con la tarjeta CLCMAIN 45;

controlar el intercambio de información con la CLCVCU 141 de la otra unidad de procesamiento 101, 201, incluyendo la señal de sincronismo de HW.

La señal de protección se obtiene asimismo utilizando el circuito VPC2 indicado anteriormente, con el que se puede generar una tensión vital solamente si la sección de comprobación proporciona cíclicamente las palabras de comprobación correctas, utilizando una memoria compartida, y la señal de inclusión, por medio de un conmutador situado en la tarjeta CLCAP 241 y controlado por la CLCVCU 141. Por lo tanto, habitualmente la sección de protección, en cada ciclo de nueva comprobación, es decir cada 50 ms:

obtiene las diversas palabras de comprobación proporcionadas por la sección de comprobación;

procesa palabras de comprobación y proporciona una tensión vital en base al valor de las mismas y a la señal de inclusión.

En la figura 8, la tarjeta CLCVCU de HW se ha dividido en varios bloques funcionales diferentes, agrupados en secciones de comprobación y de protección, bloques que se considerarán individualmente a continuación.

La lógica de comprobación 141 de la CLCVCU se obtiene físicamente por medio de un procesador Intel 80386.

La lógica de comprobación de la CLCVCU lleva a cabo las funciones siguientes:

Sincronizar los procesos de la unidad informática LPU 40 y de la unidad de comprobación y protección PSU 41. En cada ciclo de procesamiento, la lógica de comprobación produce una nueva marca de tiempo VSN (número de secuencia vital) que define el avance temporal del subsistema. Los valores de VSN progresan, ciclo a ciclo, a través de una sucesión predeterminada de estados, utilizando un divisor polinomial (PD, Polynomial Divider). Los valores de marca de tiempo VSN proporcionan protección contra la presencia de datos obsoletos en los procesadores que utilizan una memoria caché, tales como el Pentium utilizado en el CLCMAIN 45 en la unidad informática LPU 40. (Se debe observar que el procesador 80386 no tiene memoria caché).

Sincronización de hardware de los dos microprocesadores 80386 en las tarjetas de comprobación y protección CLCVCU de las dos unidades de procesamiento 101, 201 utilizando una conexión dedicada.

Comunicación con la unidad informática LPU 40. La comunicación con la unidad informática LPU 40 se produce en la línea de comunicación RS232 asíncrona propietaria, permitiendo la transmisión de la siguiente información:

de la unidad informática LPU 40 a la unidad de comprobación y protección PSU 41, las palabras de comprobación producidas por los algoritmos vitales residentes en la unidad informática LPU, así como información de diagnóstico adicional;

de la PSU unidad de protección y de comprobación 41 a la unidad informática LPU 40: el valor de marca de tiempo del número de secuencia vital (VSN) actualizado cíclicamente, las variables vitales necesarias para el cálculo adecuado de lógica del sistema y para la transmisión de variables vitales remotas, información de estado y otros datos de diagnóstico.

La verificación y comunicación de palabras de comprobación con el VPC2 indicado por el mismo numeral 2319 que en la realización anterior. La lógica de comprobación 1319 transmite las palabras de comprobación producidas por los algoritmos contenidos en la unidad informática LPU 40 y en el conjunto de comprobación y protección PSU 41, a través de una memoria de dos puertos, a la sección de protección VPC2 2319. Los accesos a la memoria de dos puertos se sincronizan con la ayuda de indicadores.

Detección de estado de entradas no vitales locales y control de salidas no vitales locales, con la ayuda de circuitos especiales impresos en la tarjeta de aplicación CLCAP 241.

Detección de estado de entradas vitales, con la ayuda de circuitos especiales impresos en la tarjeta de aplicación CLCAP 241.

Comunicación con el módulo de aplicación por medio de circuitos especiales impresos en la CLCAP 241. Esta comunicación se produce a través de un bus interno, y la información intercambiada incluye:

variables de estado para entradas y salidas no vitales;

la variable de inclusión y la comprobación vital de la misma;

las variables vitales utilizadas para detectar la presencia de tensión vital en la bifurcación local y en la bifurcación remota;

la variable vital asociada con la función de relectura del identificador de HW, así como otras posibles variables asociadas con el estado de entradas vitales adicionales;

solicitud de conmutación e información relacionada con la redundancia;

En general, la lógica de comprobación en el 80386 certifica las operaciones de todo el subsistema y controla la redundancia de las mismas.

La sección de comprobación 1319 de la tarjeta CLCVCU 141 de la unidad de comprobación y protección PSU 41 incluye además:

Una EEPROM flash 25 que, como memoria no volátil, es utilizada para contener el código de aplicación y los datos de configuración utilizados por la lógica de procesamiento de la tarjeta de comprobación y protección CLCVCU 141.

Un divisor polinomial PD. Este dispositivo lleva a cabo la función de división polinomial utilizando hardware. Esta función es ampliamente utilizada, por ejemplo para la generación de marcas de tiempo VSN, es decir para la función de generador de VSN (VSNG, VSN Generator), o para la generación de palabras de comprobación. Al implementar el algoritmo de división polinomial en forma de hardware, se proporciona una aceleración de los algoritmos vitales que residen en la tarjeta CLCVCU 141.

Una memoria de dos puertos. La memoria de dos puertos actúa como una interfaz física entre la lógica de comprobación 1319 y la lógica de protección 2139. La información intercambiada a través de este área, así como ciertos parámetros de configuración e indicadores de sincronización, son las palabras de comprobación producidas por los algoritmos que residen en las diferentes lógicas de la sección de comprobación. 1319

Una interfaz de comunicación RS232 46. Esta interfaz permite comunicaciones con la unidad informática LPU 40, y más precisamente con la tarjeta CLCMAIN 45 de la misma. Se utiliza un protocolo propietario y se controla la transmisión mediante la propia tarjeta CLCVCU 141.

Una interfaz de comunicación RS485 48, 49. Esta interfaz permite la comunicación entre las dos tarjetas CLCVCU 141 de las dos unidades de procesamiento 101, 201 y es utilizada para el intercambio de información relativa al proceso de alineamiento de lógicas entre estas dos unidades de procesamiento 101, 201.

Un puerto E/S hacia la tarjeta de aplicación CLCAP 241. Esta interfaz controla la recepción y transmisión de datos, desde y hacia la tarjeta CLCAP 241, a través de un bus interno adecuado.

La sección de protección (VPC2) 2319. La sección de protección proporciona solamente una tensión vital de salida cuando se detecta en su entrada el flujo previsto de palabras de comprobación. Consiste en un microprocesador 8085 y un filtro vital intrínsecamente seguro. Como resultado de la validación mediante la lógica residente en el microprocesador 8085, se generan dos señales hacia el filtro vital, que tienen características precisas de forma de onda (ondas cuadradas con frecuencias y ciclos de trabajo diferentes), y se utilizan para generar una tensión detectable por medio de la tarjeta de aplicación CLCAP 241. La salida de potencia del filtro vital es de 1,5 W a 12,5 V. Cada 50 ms, las formas de onda se regeneran cíclicamente en base a las palabras de comprobación recibidas por la sección de comprobación, intercambiando datos con la "memoria de dos puertos". Además, la parte de filtro activo, situada en la unidad de protección VPC2 2319 para generar la tensión vital, requiere asimismo una señal de activación, definida como Inclusión 51, con la que se puede controlar la función de respaldo en caliente. Debido al hecho de que solamente una de las dos unidades de procesamiento puede transmitir tensión vital, esta unidad, antes de su comprobación, es controlada por un conmutador estático 401 que permite conectar una de las dos unidades de procesamiento 101, 201, N o B, a una carga simulada 50.

El conmutador estático 401 está controlado mediante un circuito que está distribuido en ambas tarjetas de aplicación CLCAP 241 y mediante una lógica interna o transmitiendo controles desde la sección de comprobación 1319.

La placa de aplicación CLCAP 241 lleva a cabo funciones específicas del CLC utilizando soluciones propietarias, es decir de hardware no comercial, sin utilizar microprocesadores y, en muchos casos, se tiene incluso que es la interfaz de circuitos de algunas funciones proporcionadas por la tarjeta de comprobación y protección CLCVCU 141. Particularmente, el módulo comprende:

el conmutador de inclusión 51, desde el cual el filtro vital de la sección de protección VPC2 2319 recibe la señal de inclusión;

los circuitos AOVD 52 utilizados para la adquisición segura de tensión vital;

los circuitos 54 para la adquisición segura de identificador de HW (así como otras entradas vitales);

los circuitos 53 para el control no vital de entrada y de salida.

Las figuras 9 y 10 muestran la lógica y el desglose de circuito de las tarjetas de comprobación y protección CLCVCU 141 y las tarjetas de aplicación CLCAP 241, donde los bloques oscuros pertenecen a la tarjeta de aplicación CLCAP 241. La "carga simulada" 50 que se muestra en las figuras, ejemplifica la parte terminal de las dos bifurcaciones de tensión vital, que necesita alguna carga simulada, manteniendo al mismo tiempo el aislamiento eléctrico. El "control de redundancia", indicado en general como 60 en la figura 9, se interpuso entre las dos unidades de procesamiento 101, 201, dado que el circuito está distribuido entre las dos tarjetas CLCAP(N) y CLCAP(B), tal como resulta evidente por la figura 10.

El conmutador de inclusión 51 es un conmutador estático que recibe un control de inclusión en su entrada desde la lógica de ordenador 1319 de la sección de comprobación situada en el 80386 y, en base a este control, transmite la señal de inclusión que permite el funcionamiento adecuado del filtro activo. A continuación, se vuelve a comprobar el valor de inclusión transmitido, para permitir que la lógica de ordenador 1319 compruebe su corrección. La señal proporcionada por este conmutador se vuelve a comprobar mediante HW de seguridad intrínseca, que asegura la adquisición segura del estado de salida no excitado.

La tarjeta AOVD 52 incluye dispositivos que permiten la detección segura de la situación de corte de alimentación después del conmutador 401. La unidad de comprobación y protección PSU 41 de cada unidad de procesamiento 101, 201 tiene un dispositivo AOVD, diseñado para detectar tensión vital a la salida de su bifurcación y a la salida de la bifurcación de la unidad de procesamiento gemela 152, 252. La detección del estado de corte de alimentación permite certificar el posible fallo de una unidad de procesamiento 101, 201 y el funcionamiento adecuado del control de redundancia.

La unidad de control de redundancia, que se muestra en general en la figura 9, donde está indicada por el numeral 60, se compone de un circuito que está distribuido habitualmente en dos módulos de aplicación, tal como se indica con 160 en la figura 10, y está diseñada para el control de operaciones de conmutación entre las dos unidades de procesamiento 101, 201 CLC N/B.

La conmutación se puede producir como resultado de un "fallo" o de una "solicitud". En el primer caso, el "control de redundancia" detecta la falta de tensión vital a continuación de los generadores de potencia y fuerza automáticamente el estado cerrado del conmutador estático 401 de la unidad de procesamiento 101, 201 que no estaba suministrando tensión a la tarjeta de aplicación CLCAP 241. En el segundo caso, la lógica que reside en el 80396 de la sección de comprobación 1319 controla el conmutador estático 401 de una de las dos unidades de procesamiento 101, 201 al estado cerrado, tras una solicitud manual (transmitida por medio de un panel BDI 301) o en base a lógica interna.

La función de control de redundancia puede tener un funcionamiento independiente siempre que se detecte tensión, ya sea a la salida de la bifurcación de la unidad de procesamiento N 101 o a la salida de la bifurcación de la unidad de procesamiento B 201, transmitiendo directamente un control de bloqueo sobre el generador de potencia vital de la sección de protección 2319.

El módulo de aplicación integra los dispositivos 54 que se utilizan para la adquisición segura del identificador de HW de cada unidad de procesamiento 101, 201, y se indican en las figuras 9 y 10 como ID HW N e ID HW B, y con el numeral 54. Estos dispositivos pueden detectar vitalmente el identificador de cada unidad de procesamiento 101, 201, releyendo adecuadamente puertos configurados de puentes externos que permiten diferenciar las dos unidades de procesamiento 101, 201 CLC N y B. Los puentes están conectados a la placa base del bastidor en el que están conectadas las tarjetas CLCVCU y CLCAP 141 y 241.

El modo de aplicación CLCAP 241 integra puertos no vitales de entrada y de salida que se utilizan para la adquisición de los botones del panel BDI 301 y para controlar las luces y los timbres dispuestos en el mismo panel, con la finalidad de la aplicación CLC.

Las figuras 11 y 12 representan el funcionamiento del ordenador lógico central CLC 1 en forma gráfica. El ordenador lógico central CLC 1 tiene un funcionamiento cíclico cuyo periodo equivale a un ciclo principal, que dura 500 ms. En cada ciclo principal, el ordenador lógico central tiene que llevar a cabo todas sus funciones, y especialmente recibir datos desde nodos remotos, es decir unidades remotas, determinar el nuevo estado de salida, comprobar y certificar su propio funcionamiento y transmitir el nuevo estado de salida a los diferentes nodos remotos, es decir unidades remotas. Se asocia un valor de tiempo VSN diferente, o marca de tiempo, a cada ciclo principal, utilizando un algoritmo generador de secuencias pseudoaleatorias. El valor de marca de tiempo VSN está asociado con las variables vitales utilizadas en las unidades informáticas LPU 40 de las dos unidades de procesamiento 101, 201, para asegurar la actualidad de los datos incluso cuando se utiliza HW comercial.

En la arquitectura del sistema indicada anteriormente, el ordenador lógico central CLC 1 tiene una configuración de respaldo en caliente, para conseguir una elevada disponibilidad de misiones del subsistema. El respaldo en caliente (para unidades de procesamiento 101, 201 CLCN/CLCB) requiere lo siguiente:

Las unidades de procesamiento 101, 201 CLCN y CLCB tienen un funcionamiento independiente seguro;

Las unidades de procesamiento 101, 201 CLCN y CLCB se alinean continuamente para asegurar la continuidad de funcionamiento cuando se conmuta entre ambas;

las situaciones de fallo que provocan la pérdida de ambas unidades de procesamiento 101, 201 CLCN y CLCB son lo suficientemente excepcionales.

El control de redundancia en las unidades de procesamiento 101, 201 CLCN/CLCB implica que estas unidades de procesamiento 101, 201 funcionan en paralelo por medio de fases de adquisición de entrada y cálculo de lógica del sistema. Sin embargo, la transmisión de las salida se asigna, para cada ciclo, solamente a una de las unidades de procesamiento 101 ó 201, es decir a aquella que detecta una tensión vital en su propia bifurcación y no detecta ninguna en la bifurcación de la otra unidad de procesamiento 101, 201 gemela. Esta condición corresponde a la definición de estado "operativo" de la unidad de procesamiento 101, 201. La otra unidad de procesamiento 101, 201 solamente es funcional y está "disponible" si está alineada adecuadamente con la "operativa".

La figura 10 muestra el ciclo de procesamiento del ordenador lógico central CLC 1 en forma gráfica.

A continuación se describen las funciones principales a completar en cada ciclo principal, tal como se indica en la figura 10.

Recepción de entrada

La fase de recepción implica una operación de descodificación sobre los datos recibidos desde subsistemas externos y la adquisición de entradas locales. Esta etapa se lleva a cabo en paralelo y en modo independiente por las dos unidades de procesamiento 101, 201 CLC N y CLC B, y todas las variables relevantes de ecuaciones booleanas se marcan con la marca de tiempo del ciclo en curso (VSNi). Cada unidad de procesamiento 101, 201 comprueba las variables vitales recibidas desde cada nodo remoto, es decir desde cada unidad remota; cuando se detecta una recepción errónea o fallida, estas variables tienen que ser normalizadas, es decir ajustadas a un estado restrictivo para el sistema. La recepción de variables vitales se certificará y la palabra de comprobación generada será utilizada como una confirmación de funcionamiento adecuado de la unidad de procesamiento. Se obtienen datos de entrada mediante las unidades informáticas LPU 40, a las que la unidad de comprobación y protección PSU 41 transmite marcas de tiempo generadas por la misma al inicio del ciclo de procesamiento principal del ordenador lógico central CLC 1. Sin embargo, la unidad informática LPU 40 calcula variables de entrada y datos de memoria relacionados con la configuración del sistema, y genera palabras de comprobación a transmitir a la unidad de comprobación y protección PSU 41, es decir a la tarjeta de comprobación 141 para validación, a través de la sección de protección 2319, que reside en la propia tarjeta CLCVCU 141. Un flujo erróneo de palabras de comprobación recibidas y validadas por la sección de protección 2319 desencadena un procedimiento de seguridad, tal como se ha mencionado anteriormente.

Cálculo de lógica

El cálculo de lógica consiste en el procesamiento seguro de ecuaciones booleanas que describen la lógica del sistema específico. Las entradas utilizadas por la lógica son las entradas adquiridas por la función de "recepción de entrada" y las variables de estado internas obtenidas a partir del ciclo de procesamiento anterior, es decir las marcadas con la marca de tiempo del ciclo anterior. Se utilizan algunas variables temporales, denominadas variables actuales (CR, current variables), para la resolución de las ecuaciones. Todas las variables de entrada de las ecuaciones se marcan con el VSNi y se calcula la lógica independientemente del estado de las dos unidades de procesamiento 101, 201. La lógica es calculada por las unidades informáticas LPU 40 de las dos unidades de procesamiento, bajo la supervisión de la unidad de comprobación y protección PSU 41, en relación con las marcas de tiempo y con las palabras de comprobación generadas cíclicamente durante el ciclo. Habitualmente, un ciclo de generación y verificación de palabras de comprobación es un submúltiplo de la duración del ciclo principal, es decir del orden de unos 50 ms.

Las variables vitales de salida y de estado (denominadas asimismo VAR/AL) obtenidas a partir de la función de cálculo ejecutada en las unidades informáticas LPU 30 se marcan adecuadamente no con el valor VSNi actual, sino con una marca de tiempo, es decir la marca de tiempo futura, es decir VSN i+1, y con un valor que está asociado con el nombre de la unidad de procesamiento generadora (CLCN o CLCB) 101, 201.

La función de cálculo genera una palabra de comprobación que contribuye a certificar el funcionamiento adecuado de las unidades informáticas LPU 40, y la proporciona a la unidad de comprobación y protección PSU 41.

Intercambio de VAL/AL (variables vitales de salida y de estado) y DL (Degradation Level, nivel de degradación).

Las variables de VAL/AL se intercambian mutuamente entre las dos unidades informáticas LPU 40 antes de cualquier utilización de las mismas. Las variables de intercambio se marcan en función del nombre de la unidad de procesamiento 101, 201 generadora y de la contribución temporal VSNi+1.

Además de las variables de alineamiento, las dos unidades de procesamiento 101, 201 CLCN y CLCB intercambian información acerca de su estado de funcionamiento, y más exactamente del valor de su nivel de degradación (DL).

Progreso de VSN, selección de conjuntos de datos y generación de máscara de inclusión.

Al comienzo de cada ciclo principal, la unidad de comprobación y protección PSU 41 transmite el nuevo valor de marca de tiempo (VSNi+1) a la unidad informática LPU 40, y este valor es utilizado para marcar las nuevas variables recibidas de unidades remotas.

En cada ciclo principal, cada unidad de procesamiento 101, 201 tiene dos conjuntos de datos: uno de éstos está determinado por la función de cálculo de su propia unidad informática LPU 40, y el otro está determinado por la unidad informática LPU 40 de la otra unidad de procesamiento 101, 201 gemela. En base a la evaluación de su propio estado ("operativo", "disponible" y "apagado"), cada una de las dos unidades de procesamiento 101, 202 seleccionará uno de los dos conjuntos de datos, del que extrae las variables de salida remotas vitales a transmitir y las variables de estado internas a utilizar para el siguiente cálculo. Esta selección deberá satisfacer los criterios siguientes:

si la unidad de procesamiento 101, 201 está en el estado "disponible", entonces selecciona los datos generados por la otra unidad de procesamiento 101, 201;

en todos los demás casos, la unidad de procesamiento 101, 201 selecciona datos generados localmente.

En base a esta selección, se genera una máscara de datos que permitirá que la unidad de procesamiento 101, 201 "emita" el conjunto de variables adecuado. Asimismo, un funcionamiento adecuado es la única condición para que la unidad de procesamiento 101, 201 "operativa" genere una máscara de inclusión, es decir una señal de activación de transmisión vital, mientras que en la unidad de procesamiento 101, 201 "disponible" está limitada asimismo a una condición de alineamiento adecuada. En cualquier caso, solamente la unidad de procesamiento 101, 201 "operativa" se asigna a la tarea de transmitir variables vitales a nodos remotos, es decir a unidades remotas.

Eliminación de la máscara

Una vez que se ha seleccionado el conjunto disponible que se debe utilizar, y antes de transmitir variables vitales remotas, mediante las redes CNET, ZNET y FNET, se eliminará en estas variables la máscara de datos y éstas contendrán solamente la marca de tiempo actual (VSNi+1). Esta operación se lleva a cabo mediante la función de eliminación de la máscara.

Transmisión de salida

La etapa de transmisión de salida incluye tanto el nivel de aplicación como niveles inferiores. Para salidas del nivel de aplicación vital, se utiliza un protocolo de seguridad, y la contribución del tiempo actual (VSN) así como la máscara de inclusión se asocian a estas salidas. Si las variables a transmitir son de tipo no vital, puede ser utilizado un protocolo de transmisión no seguro. En unos pocos casos, estas variables pueden estar en sí mismas controladas por un protocolo de transmisión seguro. La información de diagnóstico se transmite utilizando un protocolo dedicado, definido como DIAGL.

Estados y transiciones

El control de redundancia entre las unidades de procesamiento CLC N y CLC B, 101 y 201, requiere una definición de los posibles estados de funcionamiento de las unidades de procesamiento 101, 201 individuales. Tal como se ha indicado anteriormente, se han definido los estados siguientes:

"Apagado"

"Inactivo"

"Operativo"

"Disponible"

Los requisitos lógicos del ordenador central CLC disponen que solamente una unidad de procesamiento 101, 201 está en el estado "operativo", y que la otra puede permanecer "disponible" si es alineada cíclicamente con la unidad de procesamiento 101, 201 "operativa". La determinación de estados para cada unidad de procesamiento 101, 201 está asociada físicamente con la presencia o ausencia de tensión vital a la salida de los conmutadores estáticos 401 en ambas tarjetas de comprobación y protección CLCVCU 141 de la unidad de comprobación y protección PSU 41. Gracias a circuitos especiales, denominados AOVD (Absence Of Voltage Detection, ausencia de detección de tensión) 52 y a un procedimiento denominado prueba de AOVD local (LAT, Local AOVD Test) y prueba de AOVD remota (RAT, Remote AOVD Test), que puede determinar de manera segura la ausencia de tensión en la bifurcación local y en la bifurcación remota, puede ser detectado el estado de cada una de las dos unidades de procesamiento 101, 201 gemelas. Si se asocia un valor "0" a la ausencia de tensión y un valor "1" a la presencia de tensión, los estados admitidos son:

LAT/RAT	Descripción
0-0	Los dos subsistemas están inactivos
1-0	El subsistema local está en el estado "operativo", mientras que el subsistema remoto está "inactivo" o "disponible".
0-1	El subsistema remoto está en el estado "operativo", mientras que el subsistema local está "inactivo" o "disponible".
(1-1)	Un caso que genera una palabra de comprobación de restablecimiento, admitido solamente durante unos pocos milisegundos.

Tal como se ha mencionado anteriormente, solamente una unidad de procesamiento 101, 201 puede estar en el estado "operativo", de manera que no se admite el resultado de prueba LAT/RAT = 1-1. Este estado se puede producir solamente durante unos pocos milisegundos en la fase de conmutación; si permanece y es detectado por la prueba LAT/RAT, provocará la generación de una palabra de comprobación errónea y el restablecimiento del ordenador lógico central.

La unidad de procesamiento 101, 201 "disponible" puede cambiar al estado "operativo" por medio de la operación de conmutación, que se puede llevar a cabo como resultado de un "fallo" o de una "solicitud". El modo de conmutación será tal que asegure la continuidad de los estados de salida vitales.

Si la conmutación es el resultado de un fallo, la unidad de procesamiento 101, 201 "disponible", cuando está alineada adecuadamente, se cambia automáticamente al estado "operativo", siempre que la otra unidad de procesamiento 101, 202, como resultado de su fallo, abandone el estado "operativo" para pasar al estado "inactivo".

Cuando la conmutación es el resultado de una solicitud, se proporciona un control manual, es decir un botón en el panel BDI, mediante el cual se puede cambiar una unidad de procesamiento 101, 201 del estado "disponible" al estado "operativo", mientras que la otra unidad de procesamiento se cambia automáticamente del estado "operativo" al estado "disponible". Durante el proceso de encendido, puede ser utilizado el mismo botón para seleccionar la unidad de procesamiento que se debe cambiar al estado "operativo". La operación de conmutación puede ser asimismo solicitada por la lógica debido a razones de diagnóstico, o para hacer que la unidad de procesamiento 101, 201 funcione de manera más eficiente. De hecho, se asocia un nivel de degradación (DL) a cada unidad de procesamiento 101, 201 CLCN y CLCB, por lo que se insta una conmutación a petición cuando la unidad de procesamiento 101, 201 "operativa" detecta un nivel de degradación (DL) que es mayor que el de la unidad "disponible". (Cuanto mayor es el DL, mayor es el nivel de no disponibilidad de la unidad de procesamiento 101, 201.)

La figura 11 muestra las diversas transiciones entre estados.

El principio inventivo se muestra claramente en la descripción de las diferentes realizaciones.

Dispositivos basados en microprocesador con arquitecturas no intrínsecamente seguras reciben la característica de intrínsecamente seguros asociándolos con dispositivos de procesamiento adicionales intrínsecamente seguros, que están diseñados para comprobar el proceso del primer dispositivo en todas las fases relevantes, es decir vitales. Los primeros dispositivos de procesamiento están programados y construidos para llevar a cabo procesamiento lógico para funciones de control y/o de monitorización, y para llevar a cabo otras funciones, tal como generación de imágenes a partir de datos de entrada o generación de control de entrada o, tal como en el caso de la última realización, para calcular algoritmos que generan datos de salida o controles en base a datos de entrada o controles en base a lógicas predeterminadas y previamente programadas. Las primeras unidades de procesamiento están programadas además para llevar a cabo etapas de generación de palabras de comprobación, para la transmisión cíclica de palabras de comprobación a las unidades de comprobación y protección asociadas. A continuación, solamente las últimas llevan a cabo la función de comprobar el flujo de funcionamiento de las primeras unidades de procesamiento y validación de palabras de comprobación, y generan datos de comprobación vital que se transmiten a las primeras unidades de procesamiento para permitir la ejecución de los ciclos de procesamiento y/o llevar a cabo operaciones de seguridad que bloquean o conmutan las salidas de las unidades de procesamiento a condiciones o conjuntos de datos en salidas de seguridad predeterminadas.

Las unidades de comprobación y protección se componen de dos secciones de microprocesador, estando una diseñada exclusivamente para el control funcional de las unidades de procesamiento, y estando la otra diseñada exclusivamente para la comprobación y validación de las palabras de comprobación recibidas. En principio, esta arquitectura se conoce ya a partir del documento que se ha mencionado varias veces en la presente memoria. Las unidades de comprobación y protección incluyen asimismo secciones específicas de aplicación, que están diseñadas para aplicaciones objetivo de la unidad de procesamiento, y aseguran que se llevan a cabo funciones de seguridad específicas para dichas aplicaciones, cuando se detectan fallos en el flujo de palabras de comprobación,

tal como apagar los monitores, o cuando se conmutan señales de activación de transmisión de una a otra de las unidades de procesamiento de lógica del ordenador central de dos canales. La arquitectura de la unidad de comprobación y procesamiento permite obtener sustancialmente la misma sección de comprobación y protección para cualquier tipo de aplicación, sustancialmente con el mismo programa de comprobación y procesamiento, estando al mismo tiempo la unidad de comprobación y procesamiento adaptada para el uso específico, gracias a la sección de aplicación, que está diseñada expresamente para satisfacer las especificaciones del hardware que depende de las unidades de procesamiento o está servido por éstas.

Obviamente, la invención no se limita la descripción y a las figuras anteriores, sino que se puede variar considerablemente, especialmente en relación con su construcción, sin apartarse de las explicaciones inventivas dadas a conocer anteriormente y reivindicadas a continuación.

REIVINDICACIONES

1. Un aparato de procesamiento o de control intrínsecamente seguro que tiene una unidad de procesamiento con

- un primer procesador y una memoria que contiene un programa predeterminado de procesamiento de datos y/o de control;

- por lo menos un puerto de entrada para datos de entrada recibidos desde por lo menos una unidad remota;

- por lo menos un puerto de salida para datos de salida a transmitir a por lo menos una unidad remota bajo el control de dicha primera unidad de procesamiento;

caracterizado por que

- la primera unidad de procesamiento comprende además medios para generar códigos únicos para la comprobación funcional de las etapas de procesamiento o recepción o transmisión que se llevan a cabo (denominadas palabras de comprobación) y un puerto para la transmisión de las palabras de comprobación generadas en cada etapa;

- está dispuesta además una unidad de comprobación y protección funcional, que consiste en una segunda unidad de procesamiento segura, con una memoria que contiene un programa para comprobar las etapas funcionales de la primera unidad de procesamiento y un programa para comprobar la corrección de los códigos de control funcionales (denominados palabras de comprobación) y la secuencia temporal de los mismos;

- unidad de comprobación y protección funcional que comunica, mediante un puerto de transmisión recepción, con la primera unidad de procesamiento, y genera señales de activación para ésta cuando las palabras de comprobación son correctas;

- mientras que dicha unidad de comprobación y protección funcional genera señales para desactivar la actividad de la primera unidad de procesamiento y/o para forzar a la primera unidad de procesamiento a la transmisión de datos de salida predeterminados para un control seguro de la unidad remota, o la mencionada unidad de comprobación y protección funcional genera por sí misma datos de salida predeterminados para un control seguro de la unidad remota o señales para activar/desactivar funciones vitales de la unidad remota o de la primera unidad de procesamiento que son transmitidas a la unidad remota y/o a la primera unidad de procesamiento;

unidad de comprobación y protección que está dotada de dos procesadores independientes, siendo uno de los dos procesadores para la ejecución de dicho programa para comprobar las etapas funcionales de la primera unidad de procesamiento y siendo el otro de dichos dos procesadores para ejecutar el mencionado programa para comprobar la corrección de los códigos de control funcionales (denominados palabras de comprobación) y la secuencia temporal de los mismos.

2. Un aparato según la reivindicación 1, caracterizado por que la unidad de comprobación y protección funcional tiene dos unidades independientes con dos procesadores independientes y se compone de una subunidad de comprobación, que lleva a cabo funciones de comprobación funcional sobre la primera unidad de procesamiento, ejecutando un programa de comprobación, y una subunidad de protección que solamente lleva a cabo funciones de verificación sobre palabras de comprobación y sobre la secuencia de las mismas, y que controla las unidades para la activación/desactivación de las funciones vitales de la unidad remota.

3. Un aparato según la reivindicación 2, caracterizado por que la subunidad de comprobación está programada asimismo de tal modo que genera por sí misma un flujo de palabras de comprobación que describen su estado funcional y que están relacionadas únicamente con las etapas de comprobación ejecutadas, palabras de comprobación que se transmiten a la subunidad de protección para una comprobación de corrección y de secuencia.

4. Un aparato según la reivindicación 2, caracterizado por que la subunidad de comprobación está programada para generar datos vitales de activación para la primera unidad de procesamiento, y para transmitirlos a la misma con el fin de permitir la consecución adecuada de sus funciones.

5. Un aparato según la reivindicación 2, caracterizado por que la primera unidad de procesamiento ejecuta sucesivos ciclos de procesamiento que tienen una duración predeterminada, y por que la subunidad de comprobación está programada de tal modo que genera una única marca de tiempo para cada ciclo de ejecución del programa de procesamiento de la primera unidad de procesamiento, marca de tiempo que cambia/aumenta en cada comienzo del ciclo de procesamiento de la primera unidad de procesamiento, estando dispuesta una línea de comunicación entre la subunidad de comprobación y la primera unidad de procesamiento, a través de la cual la unidad de procesamiento transmite la marca de tiempo al inicio de cada ciclo de procesamiento.

6. Un aparato según la reivindicación 5, caracterizado por que la unidad de comprobación y protección inicia el ciclo de procesamiento de la primera unidad de procesamiento transmitiendo la marca de tiempo actual.

7. Un aparato según una o varias de las reivindicaciones anteriores, caracterizado por que la primera unidad de procesamiento tiene una memoria para los datos de entrada a procesar, habitualmente la memoria caché del procesador, datos que se marcan con la marca de tiempo del ciclo de procesamiento actual, mientras que todos los datos de entrada marcados con marcas de tiempo de ciclos de procesamiento anteriores se borran de la memoria.

8. Un aparato según una o varias de las reivindicaciones anteriores 4 a 7, caracterizado por que todos los datos introducidos en la primera unidad de procesamiento se marcan con las marcas de tiempo de los ciclos tanto actual como siguiente, para el procesamiento repetido de los mismos mediante la primera unidad de procesamiento.

9. Un aparato según una o varias de las reivindicaciones anteriores, caracterizado por que la unidad de comprobación y protección funcional tiene interfaces de comprobación vital desde la unidad remota.

10. Un aparato según la reivindicación 9, caracterizado por que las interfaces de comprobación vital se componen de unidades para transmitir y/o amplificar todas las salidas de datos desde la primera unidad de procesamiento, siendo dichas unidades de transmisión y/o amplificación activadas/desactivadas por la unidad de comprobación y protección, en base al resultado de la verificación de la corrección y de la secuencia de las palabras de comprobación.

11. Un aparato según la reivindicación 10, caracterizado por que las interfaces de comprobación vital de las unidades remotas se componen de fuentes de alimentación para dichas unidades remotas, que se controlan para el suministro de tensión vital mediante la unidad de comprobación y protección, en base al resultado de la verificación de la corrección y de la secuencia de las palabras de comprobación.

12. Un aparato según una o varias de las reivindicaciones anteriores, caracterizado por que la primera unidad de procesamiento tiene unidades de control de la unidad remota, que transmiten datos de salida a la unidad remota por medio de interfaces de transmisión/amplificación de la unidad de comprobación y protección.

13. Un aparato según una o varias de las reivindicaciones anteriores, caracterizado por que tiene dos primeras unidades de procesamiento en las que se ejecutan programas para controlar y comprobar por lo menos una unidad remota y/o múltiples unidades remotas diferentes y/o por lo menos parcialmente idénticas, estando asociada una unidad de comprobación y protección dedicada a cada una de dichas dos primeras unidades de procesamiento, y siendo idénticas dichas dos primeras unidades de procesamiento y estando programadas con el mismo programa de procesamiento, programa de procesamiento que se ejecuta simultáneamente y en paralelo mediante dichas dos unidades de procesamiento, mientras que están dispuestos medios para sincronizar las unidades de comprobación y protección y una interfaz de activación, que se utiliza para activar la transmisión de datos de salida de cada una de dichas dos primeras unidades de procesamiento a la unidad o unidades remotas, interfaz de activación que tiene un funcionamiento intrínsecamente seguro y activa el estado operativo para la unidad de transmisión de solamente una de dichas dos primeras unidades de procesamiento.

14. Un aparato según la reivindicación 13, caracterizado por que cada unidad de comprobación y protección, asociada a una de dichas dos primeras unidades de procesamiento respectivamente, incluye una subunidad para detectar tensión vital en la unidad de transmisión de cada una de las dos primeras unidades de procesamiento y un conmutador estático, para suministrar tensión vital a las unidades de transmisión, estando dotadas cada una de las subunidades de detección de tensión vital de sensores de detección de tensión vital, para detectar la tensión vital en ambas unidades de transmisión de dichas dos primeras unidades de procesamiento.

15. Un aparato según la reivindicación 14, caracterizado por que cada una de las subunidades de comprobación y protección tiene una unidad de control de redundancia, que tiene entradas para datos de presencia de tensión vital procedentes de las dos subunidades de detección de tensión vital, asociadas con una de las dos subunidades de comprobación y protección respectivamente, y salidas para controlar el corte del suministro de tensión vital a una de las dos unidades de transmisión, en función de los datos de presencia de tensión vital recibidos.

16. Un aparato según una o varias de las reivindicaciones anteriores, caracterizado por que genera imágenes correspondientes a los datos recibidos desde por lo menos una o varias unidades remotas, estando programada la primera unidad de procesamiento para la recepción de datos, la interpretación de datos en relación con un mapa de configuración del sistema de unidades remotas almacenado en la misma, y para la generación de datos de reconstrucción de imágenes a partir de datos de entrada, consistiendo dicha primera unidad de procesamiento en una tarjeta de microprocesador y uno o varios adaptadores gráficos, mientras que la unidad de comprobación y protección tiene una tarjeta para amplificar/transmitir las señales del adaptador gráfico a monitores de video, estando conectadas las salidas de los adaptadores gráficos de la unidad de procesamiento a dicha tarjeta de amplificación/transmisión, estando conectada esta última a un suministro de tensión vital a través de un conmutador vital controlado por la sección de protección en base a la corrección de las palabras de comprobación recibidas.

17. Un aparato según una o varias de las reivindicaciones anteriores 14 a 16, caracterizado por que la unidad de procesamiento es un generador de controles a partir de entradas de teclado, estando el teclado conectado a una unidad de procesamiento para transformar controles gráficos o alfanuméricos en datos de control y para transmitirlos a una unidad de procesamiento que forma una sección de la unidad de comprobación y protección, cuya interfaz

está conectada al suministro de tensión vital por medio de un conmutador vital controlado por la unidad de comprobación y protección.

18. Un aparato según la reivindicación 17 cuando depende de la reivindicación 16, caracterizado por que la unidad de procesamiento es un adaptador de procesamiento de gráficos según la reivindicación 16, que genera en la pantalla ecos de controles de entrada de teclado, estando dotada la unidad de comprobación y protección de una tarjeta de interfaz para la conexión de los adaptadores gráficos de las unidades de procesamiento a monitores, y de una interfaz para la conexión del teclado de control con la unidad de procesamiento.

19. Un aparato según las reivindicaciones 13 a 15, caracterizado por que las dos unidades de procesamiento son dos ordenadores lógicos centrales paralelos, cada uno de los cuales forma uno de los dos canales de procesamiento paralelos de un ordenador lógico central, diseñado en particular para el control de sistemas de estación ferroviaria.

20. Un aparato según la reivindicación 19, caracterizado por que cada una de las dos unidades de procesamiento está conectada a una unidad de comprobación y protección, dichas unidades comunicando para una comprobación de sincronización, mediante comparar las marcas de tiempo generadas por las mismas, y estando conectadas dichas unidades de comprobación y protección a sensores de tensión vital que detectan la tensión vital en dos unidades de transmisión de datos de salida, estando integradas cada una de las últimas en una de las dos unidades de procesamiento, y activando dicha unidad de comprobación y protección la unidad de transmisión de solamente una de las dos unidades de procesamiento, en base al resultado de la detección de tensión vital en la misma, y en base a la verificación de las palabras de comprobación procedentes de las dos unidades de procesamiento.

21. Un aparato según una o varias de las reivindicaciones anteriores, caracterizado por que forma parte de un sistema que comprende una o varias unidades remotas, que son por lo menos parcialmente diferentes y/o por lo menos parcialmente idénticas, y comunican con al aparato, a saber con la unidad de procesamiento del mismo, teniendo dicho aparato una memoria para almacenar datos de configuración del sistema y una memoria para un programa de gestión de la unidad de procesamiento, y teniendo un programa para comprobar los datos de configuración y/o el programa de procesamiento, que genera palabras de comprobación de corrección de los datos de configuración y del código del programa de procesamiento, que se envían para comprobar la corrección a la unidad de comprobación y protección funcional, comprobándose los datos de configuración y/o el código del programa de procesamiento en conjuntos parciales y sucesivos de datos y/o de código, dispuestos en un número predeterminado de ciclos sucesivos de ejecución del programa.

22. Un aparato según una o varias de las reivindicaciones anteriores, caracterizado por que se ejecutan múltiples ciclos sucesivos para la generación de palabras de comprobación funcionales y la verificación de palabras de comprobación, los cuales se repiten a frecuencias correspondientes a submúltiplos de la duración total del ciclo de procesamiento.

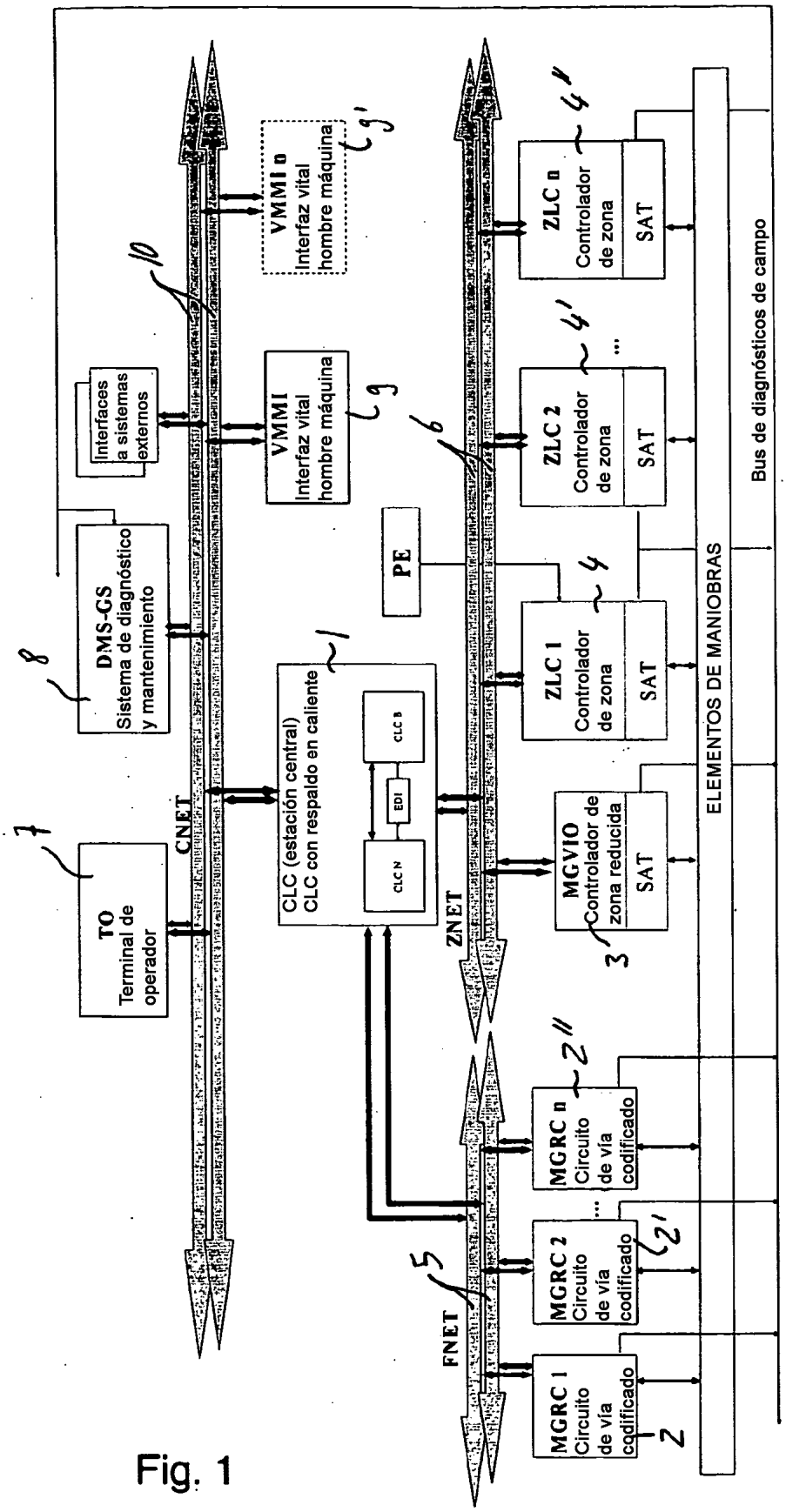
TO
Terminal de operador
CNET
DMS-GS
Sistema de diagnóstico y mantenimiento
Interfaces a sistemas externos
CLC (estación central)
CLC con respaldo en caliente
CLC N
EDI
CLC B
VMMI
Interfaz vital hombre máquina
VMMI n
Interfaz vital hombre máquina
PE
ZNET
MGV1O
Controlador de zona reducida
SAT
ZLC 1
Controlador de zona
ZLC 2
Controlador de zona
ZLC n
Controlador de zona
ELEMENTOS DE MANIOBRAS
Bus de diagnósticos de campo
FNET
MGRC 1
Circuito de vía codificado
MGRC 2
Circuito de vía codificado
MGRC n
Circuito de vía codificado

Fig. 1

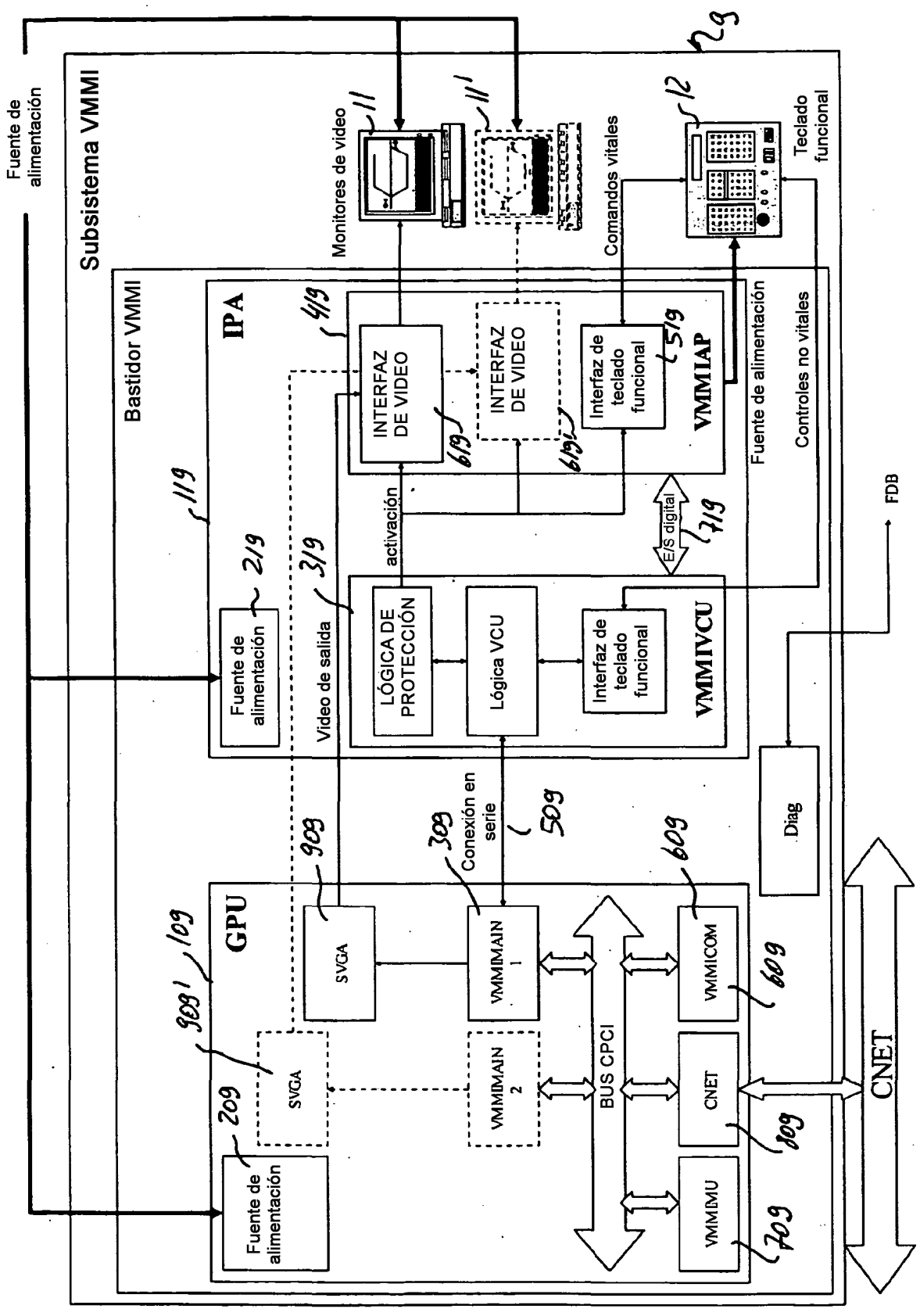
Fuente de alimentación
Subsistema VMMI
Bastidor VMMI
IPA
GPU
Monitores de video
Comandos vitales
Teclado funcional
Fuente de alimentación
Controles no vitales
INTERFAZ DE VIDEO
INTERFAZ DE VIDEO
Interfaz de teclado funcional
VMMIAP
activación
E/S digital
FDB
Fuente de alimentación
Video de salida
LÓGICA DE PROTECCIÓN
Lógica VCU
Interfaz de teclado funcional
VMMIVCU
Diag
Conexión en serie
SVGA
VMMIMAIN 1
VMMICOM
SVGA
VMMIMAIN 2
BUS CPCI
CNET
CNET
Fuente de alimentación
VMMIMU

Fig. 2

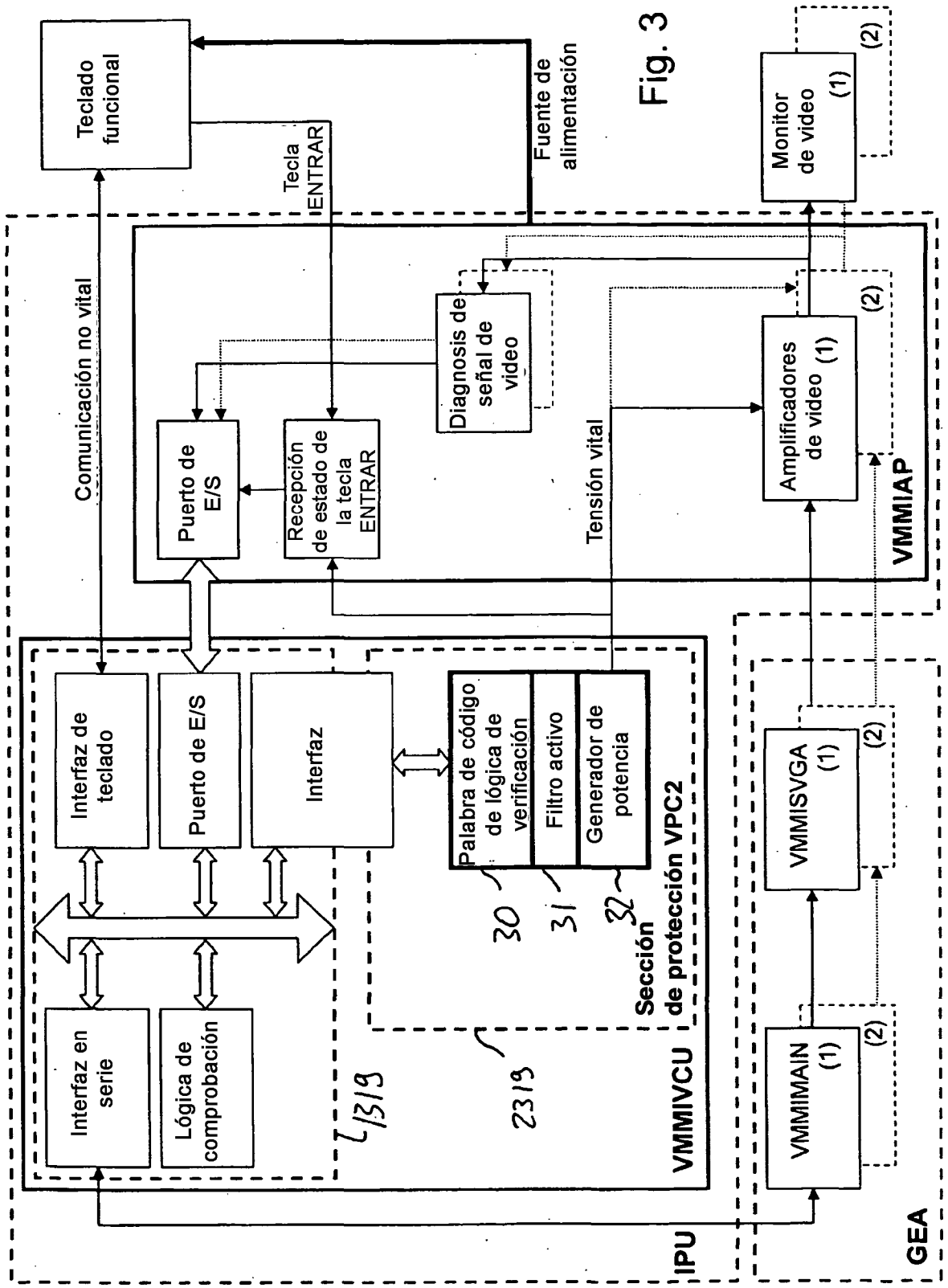
Teclado funcional
Tecla ENTRAR
Fuente de alimentación
Monitor de video (1) (2)
Comunicación no vital
Diagnosis de señal de video
Puerto de E/S
Recepción de estado de la tecla ENTRAR
Tensión vital
Amplificadores de video (1) (2)
VMMIAP
Interfaz de teclado
Puerto de E/S
Interfaz
Palabra de código de lógica de verificación
Filtro activo
Generador de potencia
30
31
32
Sección de protección VPC2
VMMIVCU
2319
Interfaz en serie
Lógica de comprobación
VMMISVGA (1) (2)
VMMIMAIN (1) (2)
IPU
GEA

Fig. 3

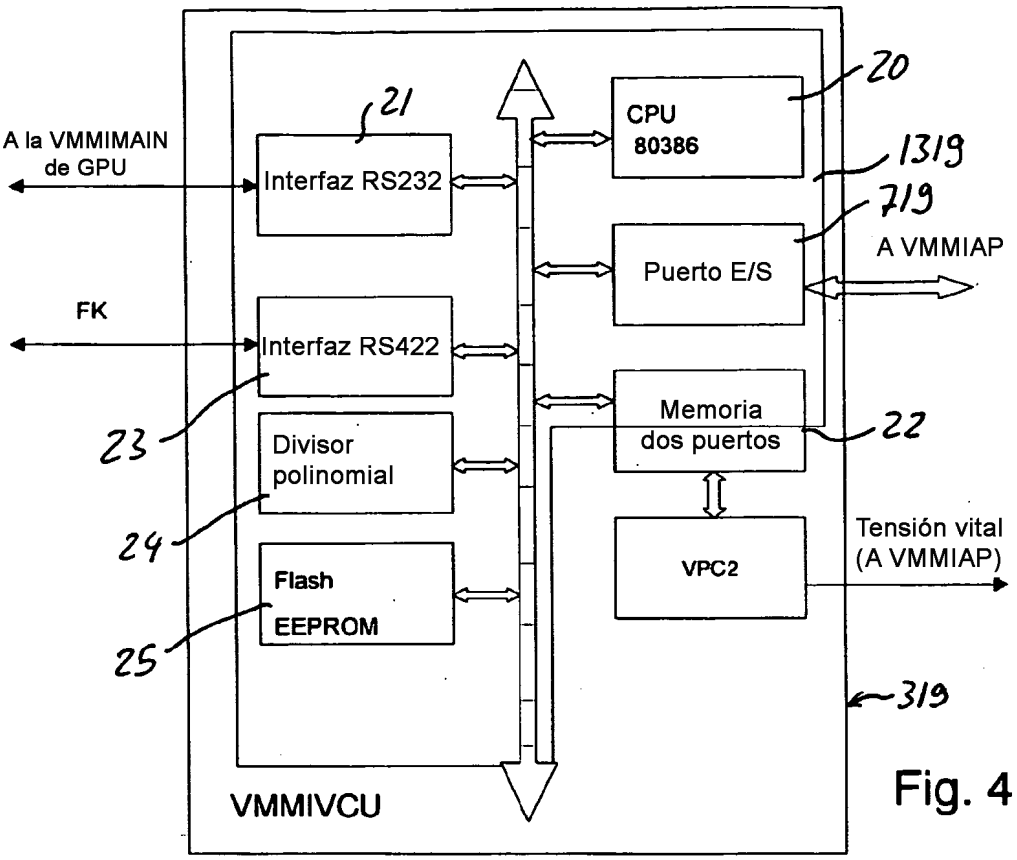
A la VMMIMAIN de GPU
FK
Interfaz RS232
Interfaz RS422
Divisor polinomial
Flash EEPROM
CPU 80386
Puerto E/S
Memoria dos puertos
VPC2
A VMMIAP
Tensión vital (A VMMIAP)
VMMIVCU
20
21
23
24
25
1319
719
22
319

Fig. 4

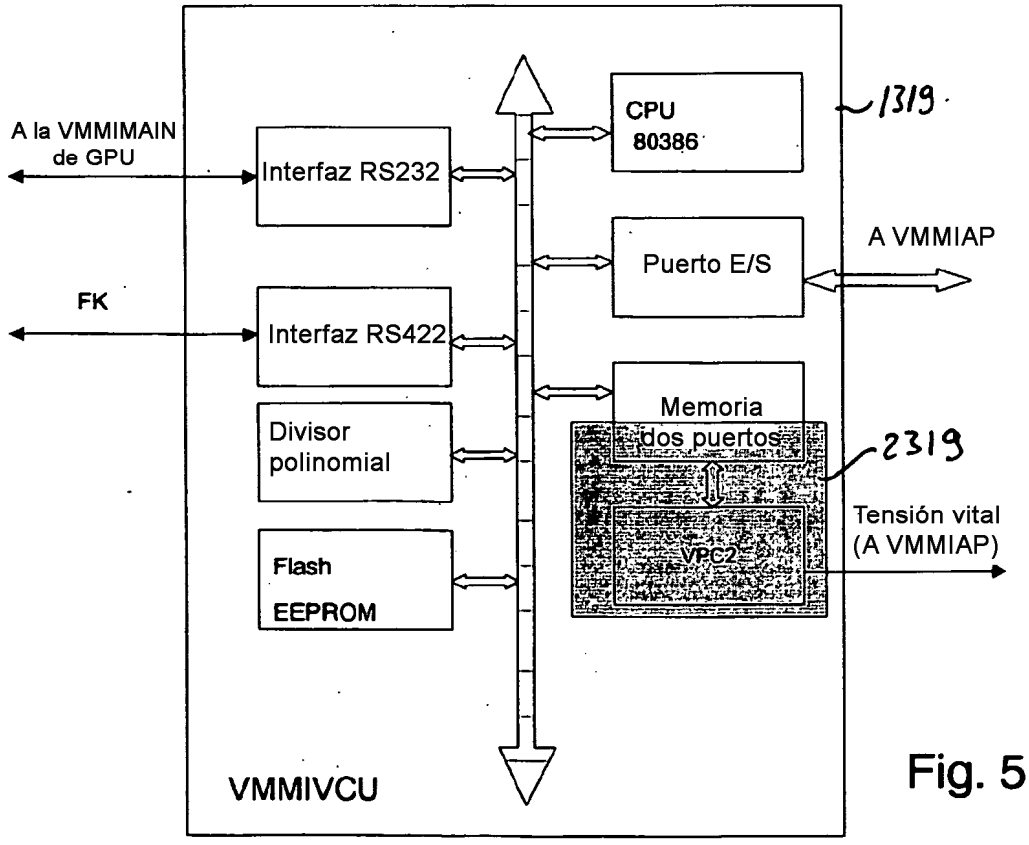
A la VMMIMAIN de GPU
FK
Interfaz RS232
Interfaz RS422
Divisor polinomial
Flash EEPROM
CPU 80386
Puerto E/S
Memoria dos puertos
VPC2
A VMMIAP
Tensión vital (A VMMIAP)
VMMIVCU
1319
2319

Fig. 5

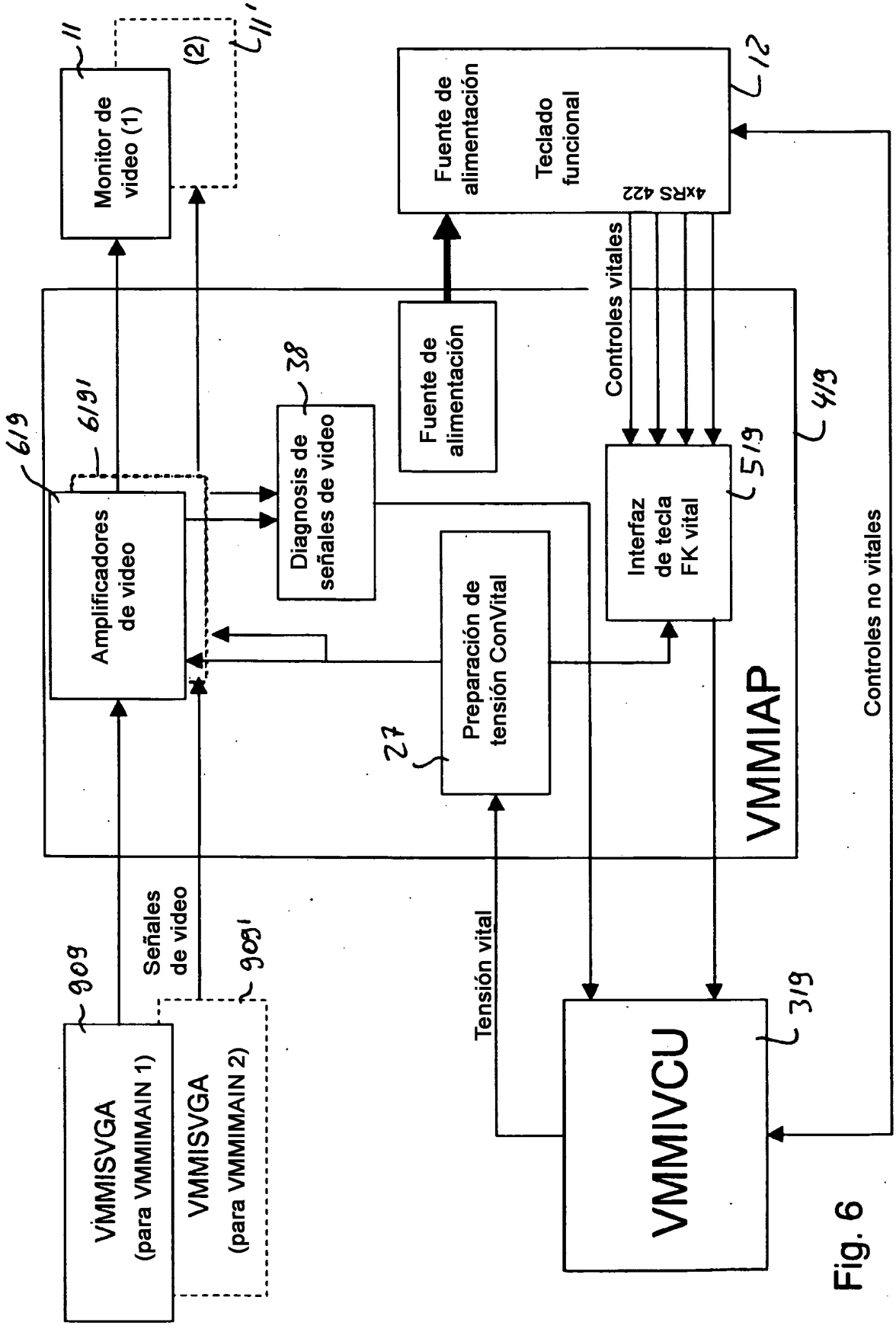
11
(2)
11'
Monitor de video (1)
Fuente de alimentación
Teclado funcional
12
4xRS 422
Controles vitales
619
619'
38
Diagnosis de señales de video
Fuente de alimentación
Amplificadores de video
Preparación de tensión ConVital
27
Interfaz de tecla FK vital
519
419
VMMIAP
Controles no vitales
Señales de video
909
909'
VMMISVGA (para VMMIMAIN 1)
VMMISVGA (para VMMIMAIN 2)
Tensión vital
VMMIVCU
319

Fig. 6

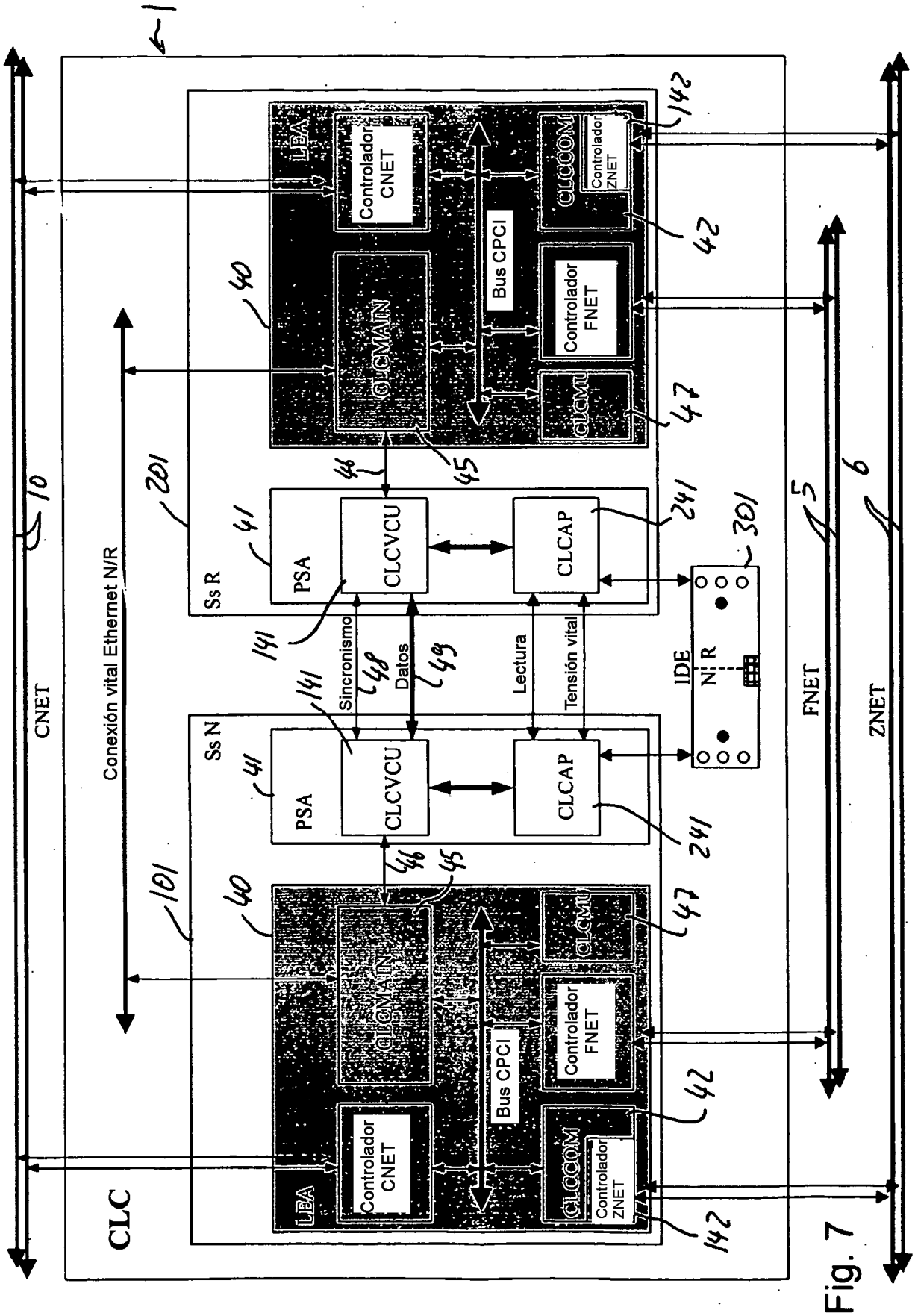
CLC
CNET
Conexión vital Ethernet N/R
FNET
ZNET
Ss R
Ss N
PSA
CLCVCU
CLCAP
Sincronismo
Datos
Lectura
Tensión vital
IDE
N: R
LEA
Controlador CNET
CLCCOM
Controlador ZNET
Bus CPCI
CLCMAIN
Controlador FNET
CLCMU

Fig. 7

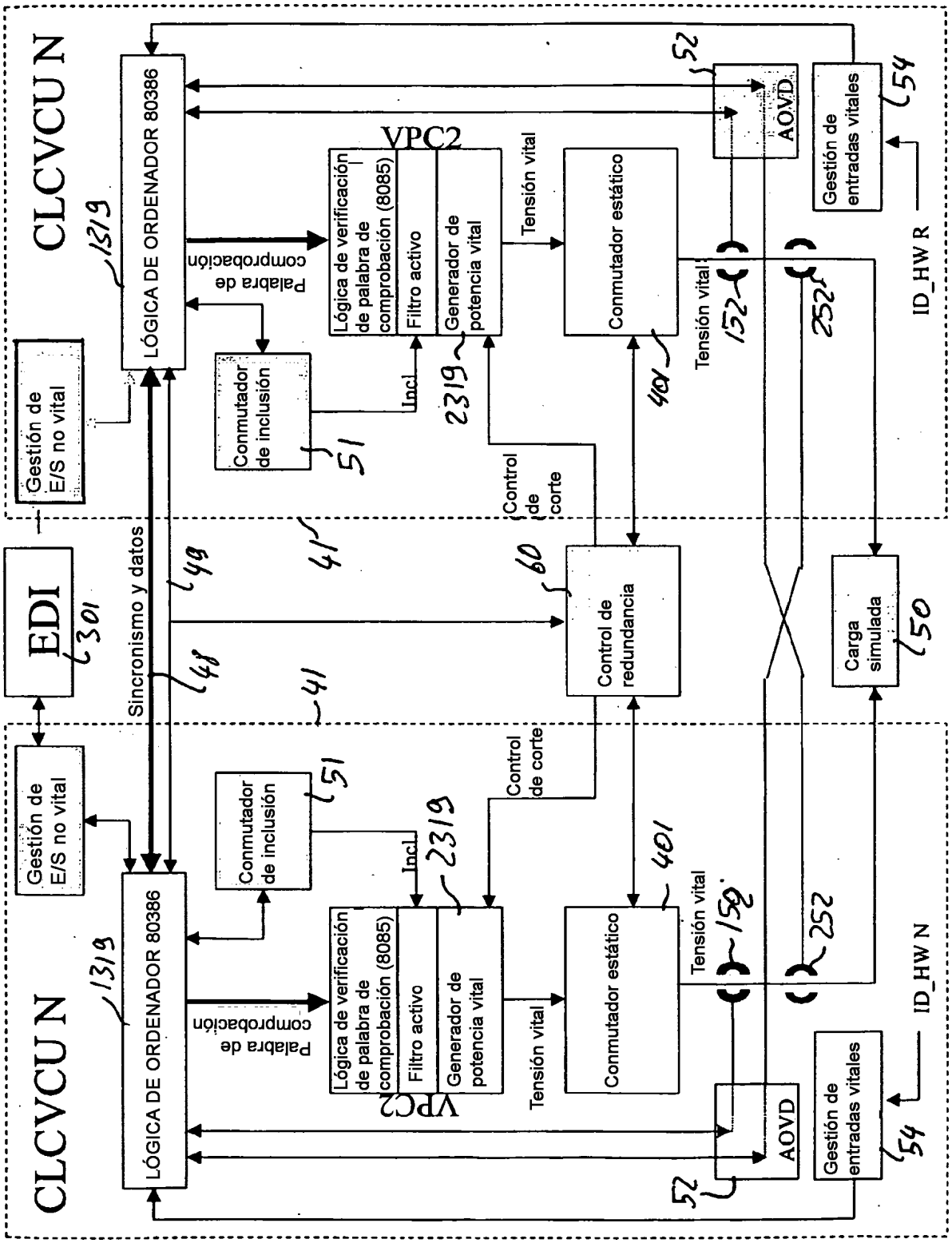
CLCVCU N
LÓGICA DE ORDENADOR 80386
1319
Gestión de E/S no vital
Palabra de comprobación
Conmutador de inclusión
Incl
51
Lógica de verificación de palabra de comprobación (8085)
Filtro activo
Generador de potencia vital
VPC2
2319
Tensión vital
Conmutador estático
401
Tensión vital
152
252
AOVD
52
Gestión de entradas vitales
54
ID_HW R
Control de corte
41
Sincronismo y datos
49
EDI
301
60
Control de redundancia
Carga simulada
150
CLCVCU N
ID_HW N

Fig. 8

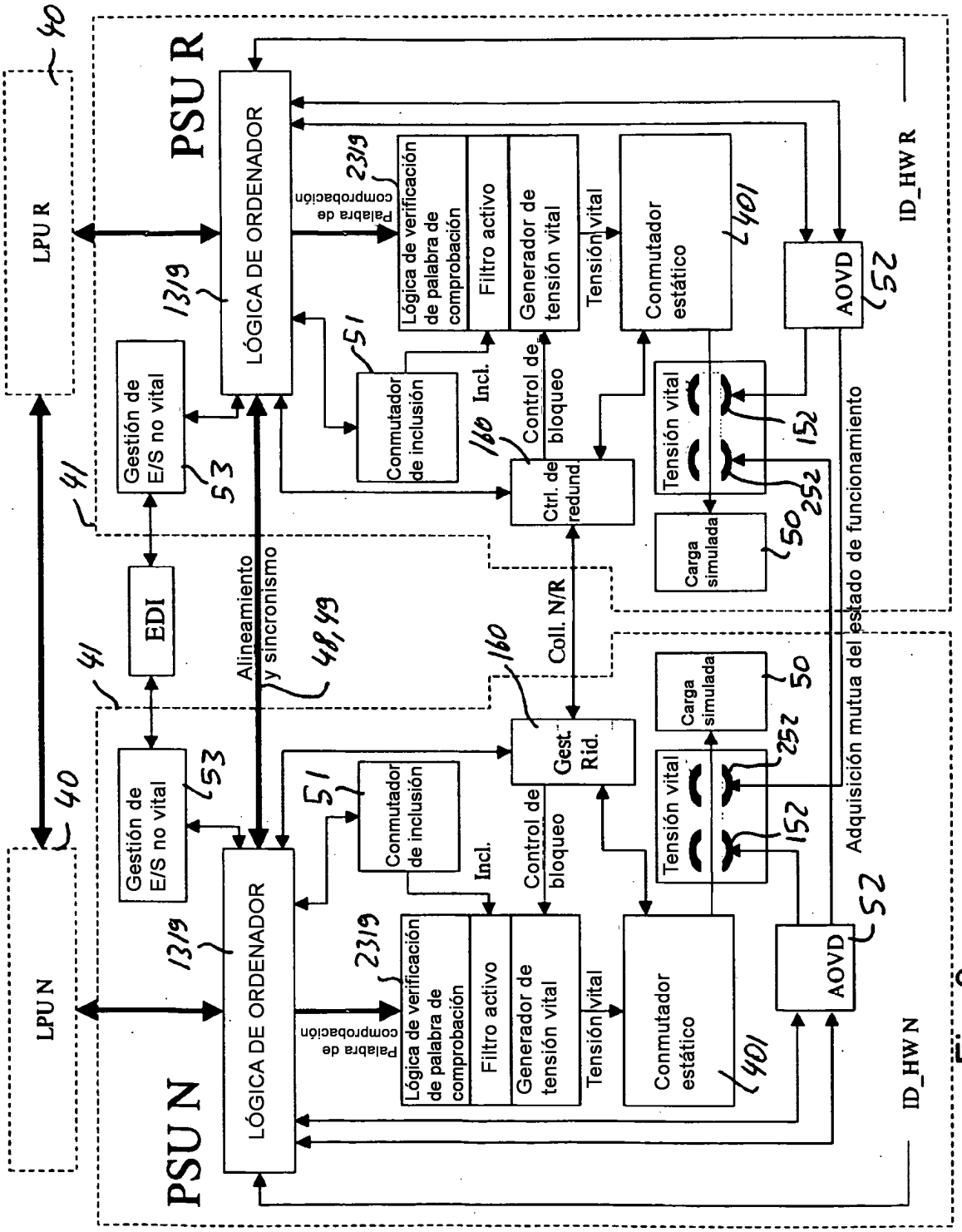
LPU R
LPU N
PSU R
PSU N
LÓGICA DE ORDENADOR
Gestión de E/S no vital
EDI
Alineamiento y sincronismo
Conmutador de inclusión
Incl.
Control de bloqueo
Ctrl. de redund.
Coll. N/R
Gest. Rid.
Lógica de verificación de palabra de comprobación
Palabra de comprobación
Filtro activo
Generador de tensión vital
Tensión vital
Conmutador estático
AOVD
Carga simulada
Adquisición mutua del estado de funcionamiento
ID_HW R
ID_HW N

Fig. 9

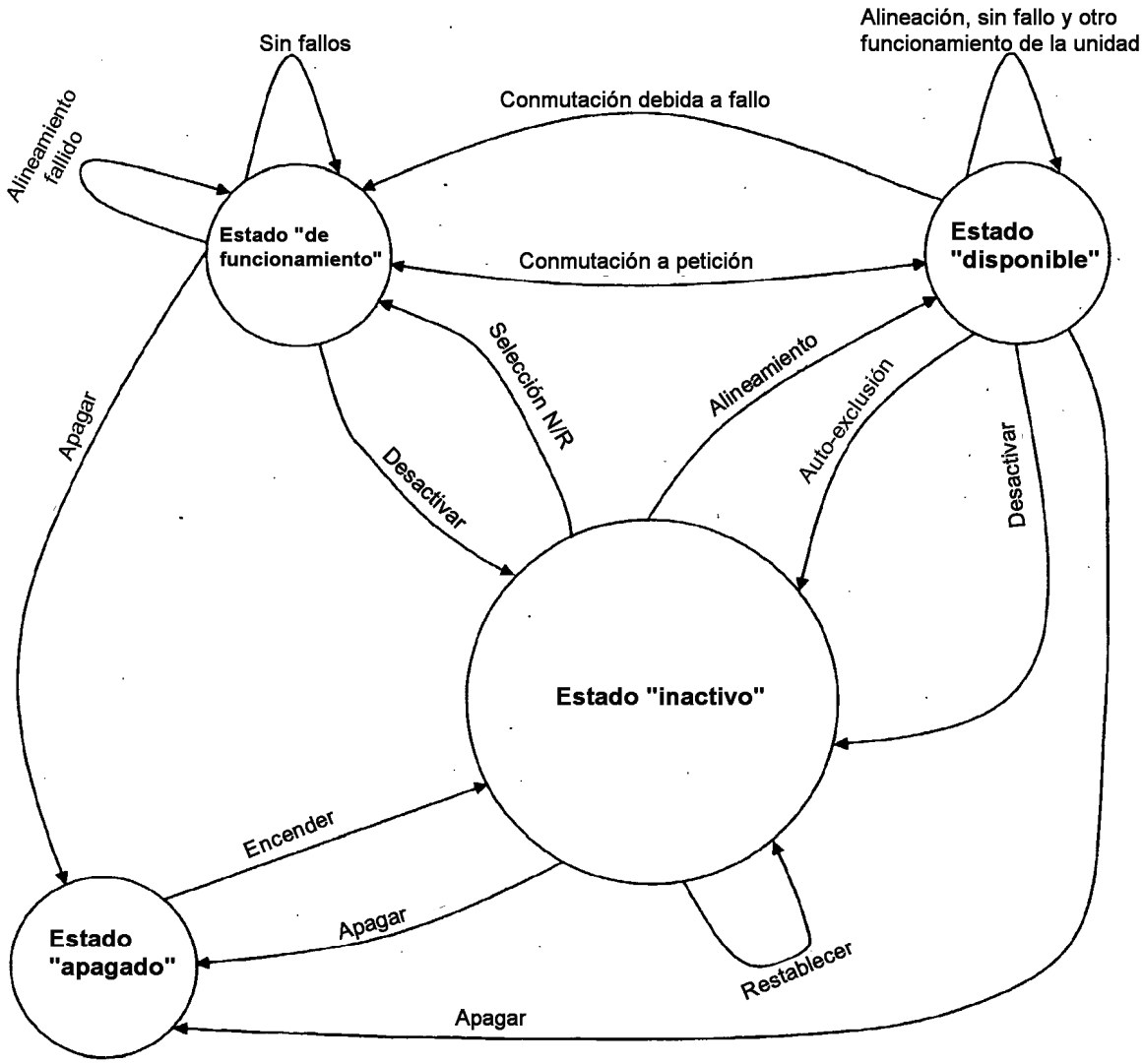
Sin fallos
Alineación, sin fallo y otro funcionamiento de la unidad
Conmutación debida a fallo
Alineamiento fallido
Estado "de funcionamiento"
Conmutación a petición
Estado "disponible"
Selección N/R
Alineamiento
Auto-exclusión
Desactivar
Desactivar
Apagar
Estado "inactivo"
Encender
Apagar
Estado "apagado"
Restablecer
Apagar

Fig. 10

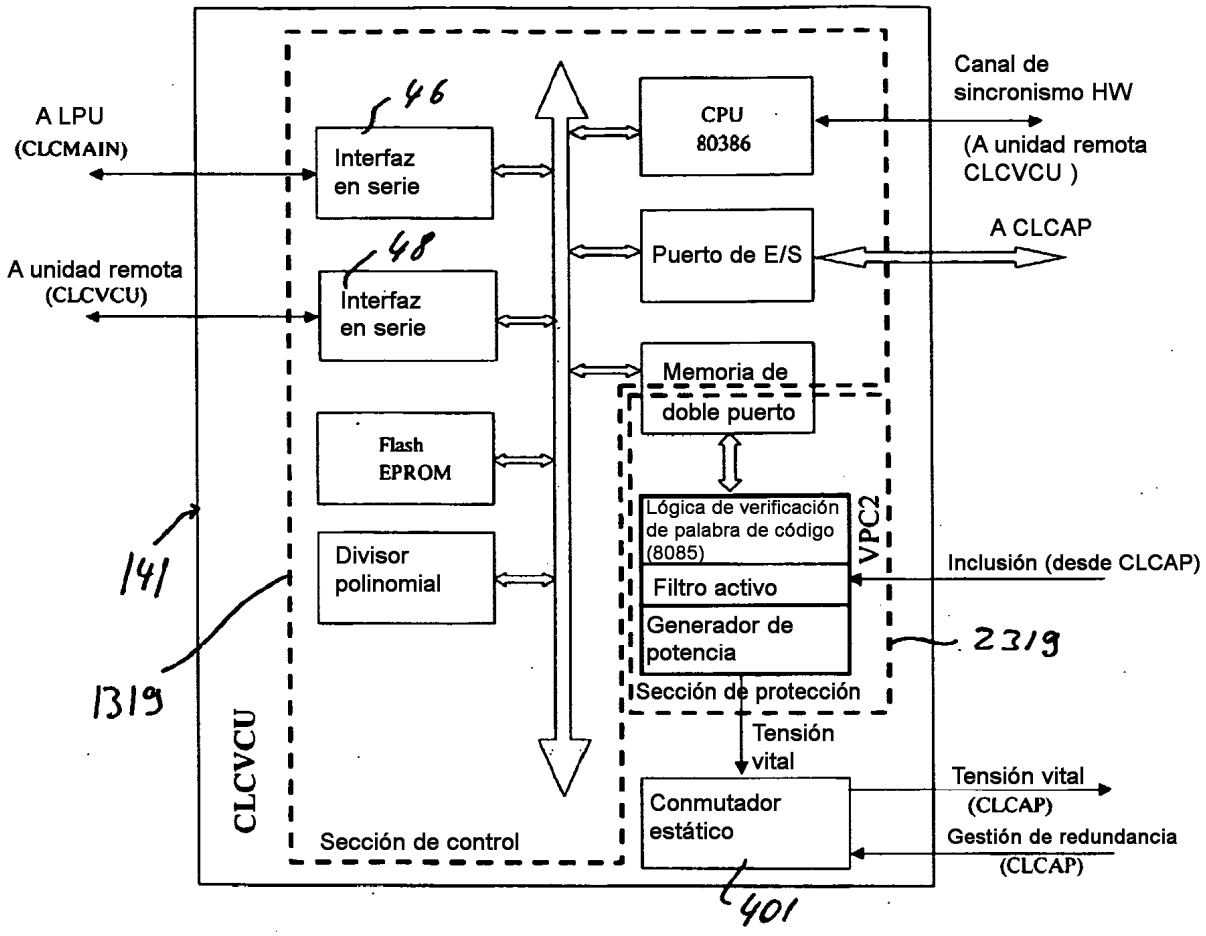
A LPU
(CLCMAIN)
A unidad remota
(CLCVCU)
46
Interfaz
en serie
48
Interfaz
en serie
Flash
EPROM
Divisor
polinomial
141
1319
CLCVCU
Sección de control
CPU
80386
Puerto de E/S
Memoria de
doble puerto
Lógica de verificación
de palabra de código
(8085)
Filtro activo
Generador de
potencia
VPC2
Sección de protección
2319
Tensión
vital
Conmutador
estático
401
Canal de
sincronismo HW
(A unidad remota
CLCVCU)
A CLCAP
Inclusión (desde CLCAP)
Tensión vital
(CLCAP)
Gestión de redundancia
(CLCAP)

Fig. 11

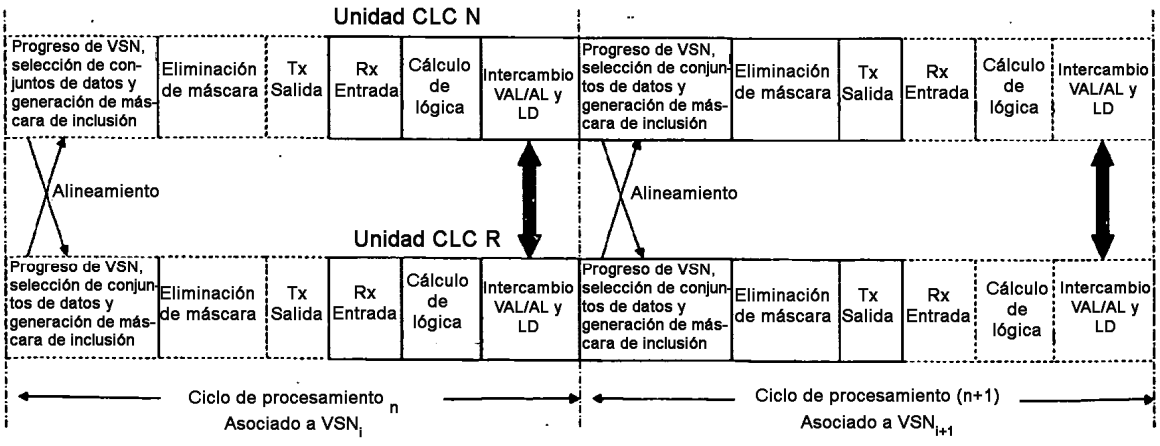
Unidad CLC N
Progreso de VSN, selección de conjuntos de datos y generación de máscara de inclusión
Eliminación de máscara
Tx Salida
Rx Entrada
Cálculo de lógica
Intercambio VAL/AL y LD
Alineamiento
Unidad CLC R
Ciclo de procesamiento n
Asociado a VSN$_i$
Ciclo de procesamiento (n+1)
Asociado a VSN$_{i+1}$

Fig. 12