(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 385 195**

(51) Int. CI.:
G05B 19/05 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **10154186 .0**
(96) Fecha de presentación: **22.02.2010**
(97) Número de publicación de la solicitud: **2228699**
(97) Fecha de publicación de la solicitud: **15.09.2010**

(54) Título: **Unidad de E/S y controlador industrial**

(30) Prioridad:
12.03.2009 JP 2009059324
19.01.2010 JP 2010009338

(45) Fecha de publicación de la mención BOPI:
19.07.2012

(45) Fecha de la publicación del folleto de la patente:
19.07.2012

(73) Titular/es:
OMRON CORPORATION
801, MINAMIFUDODO-CHO
HORIKAWAHIGASHIIRU SHIOKOJI-DORI
SHIMOGYO-KU
KYOTO-SHI, KYOTO 600-8530, JP

(72) Inventor/es:
Yoshida, Katsufumi y
Nakamura, Toshiyuki

(74) Agente/Representante:
Lehmann Novo, Isabel

DESCRIPCIÓN

Unidad de E/S y controlador industrial

Antecedentes de la invención

Esta solicitud se basa en las Solicitudes de Patente Japonesas números 2009-059324 y 2010-009338 presentadas a la Oficina de Patentes de Japón el 12 de marzo de 2009 y el 19 de enero de 2010, respectivamente.

Campo de la técnica

La presente invención está relacionada con una unidad de E/S y un controlador industrial y, en particular, con una función de diagnóstico de un dispositivo de E/S conectado a la unidad de E/S.

Técnica asociada

Un sistema de red en FA (Automatización de Plantas) dispone de uno o una pluralidad de PLC (Controlador de Lógica Programable) responsable del control de un dispositivo de entrada y un dispositivo de salida de un robot industrial y otros medios de producción dispuestos en el interior de una planta de producción, y un dispositivo cuyo funcionamiento es controlado por el PLC, conectado a una red de un sistema de control. El PLC y el dispositivo se comunican a través de la red del sistema de control para transmitir y recibir datos de ENTRADA y datos de SALIDA (denominados de aquí en adelante en la presente solicitud como datos de E/S), y controlar los medios de producción.

Más específicamente, el control en la unidad de la CPU del PLC introduce una señal de CONEXIÓN o una señal de DESCONEXIÓN del dispositivo de entrada, mediante un programa de usuario lleva a cabo las operaciones lógicas en función de la información de CONEXIÓN/DESCONEXIÓN introducida y envía el resultado de la operación al dispositivo de salida. Dicho resultado se transforma en una orden de operación para el dispositivo de salida con el fin de operar el dispositivo de salida, controlándose de este modo los medios de producción.

Existe una demanda para la realización del diagnóstico en el momento apropiado en el dispositivo de E/S como, por ejemplo, el dispositivo de entrada y el dispositivo de salida. Dicho diagnóstico incluye, en general, la conexión de un dispositivo de monitorización al PLC y monitorizar la memoria E/S del PLC almacenando los datos de E/S del dispositivo de E/S para confirmar el estado del dispositivo de E/S y determinar si el dispositivo de E/S está funcionando correctamente.

Se conoce un sistema de diagnóstico divulgado en la Publicación de la Patente Japonesa sin Examinar número 2005-243008 para realizar el diagnóstico en la parte de entrada del dispositivo y en la parte de salida del dispositivo. Dicho sistema de diagnóstico crea un algoritmo de diagnóstico adaptado al dispositivo de entrada y al dispositivo de salida, que se convierten en el objetivo, utilizando un dispositivo utilizado como herramienta de configuración, y descarga y configura el algoritmo de diagnóstico creado en el dispositivo de entrada y en el dispositivo de salida. En el momento del funcionamiento real, el dispositivo de entrada y similares ejecutan el algoritmo de diagnóstico para determinar la presencia de anomalías, y circunstancias similares, y envía el resultado del diagnóstico a través de la red. El algoritmo de diagnóstico incluye un programa de aplicación de diagnóstico, y los parámetros utilizados cuando se ejecuta el programa de aplicación. El diagnóstico realizado en esta solicitud incluye la medición del tiempo desde el momento en el que se activa un sensor o el dispositivo de entrada hasta que el dispositivo de salida actúa, el tiempo de funcionamiento del dispositivo de salida, y similares, y la determinación de si el resultado de la medición se encuentra, o no, dentro de un rango de valores de referencia.

Recientemente se ha introducido un sistema a prueba de fallos (seguro) para el control mediante el PLC. Esto es, además del PLC y cada dispositivo por sí mismo, la red que conecta el PLC y el dispositivo también se configura para incorporar la función de seguridad. La función de seguridad garantiza la seguridad de un trabajador cuando se pulsa un botón de parada de emergencia o cuando un sensor de una cortina de luz o dispositivos similares detectan la entrada de una persona (parte del cuerpo), y se duplican la CPU y otras unidades de proceso, de modo que el sistema a prueba de fallos funciona incluso cuando se produce un fallo en una unidad de control asociada con la seguridad y el sistema pasa al modo de seguridad para parar el funcionamiento.

Este tipo de sistema de control de seguridad incluye un controlador de seguridad que cumple con el estándar de seguridad, un terminal remoto de seguridad, y un dispositivo de E/S, y se utiliza con una máquina de corte, una máquina de desconexión, un equipo robotizado de fabricación, y equipos similares. El controlador de seguridad incorpora una función de autodiagnóstico en términos de seguridad además de la función de operación lógica similar al controlador programable general (PLC) y la función de control de entrada/salida para asegurar una alta seguridad y fiabilidad del control. El controlador de seguridad tiene una función (función a prueba de fallos) para forzar la realización de un control de seguridad de modo que su control no dé lugar a ningún peligro cuando el resultado del autodiagnóstico detecte algún funcionamiento anómalo. El terminal remoto de seguridad también tiene una función de autodiagnóstico, y tiene una función a prueba de fallos para realizar un control de modo que su control no dé

lugar a ningún peligro cuando el resultado del autodiagnóstico detecte algún funcionamiento anómalo. De este modo, el sistema de control de seguridad previene que el funcionamiento de un equipo robotizado de fabricación y equipos similares den lugar a ningún peligro.

Tal como se utiliza en la presente solicitud, seguridad tiene más específicamente un significado que incluye un estándar de seguridad normalizado. El estándar de seguridad incluye, por ejemplo, el estándar 61508 del IEC y el estándar EN. En el 61508 del IEC (Comisión Electrotécnica internacional asociada a la seguridad de funcionamiento de un sistema electrónico programable), se define una probabilidad de de fallo peligroso por unidad de tiempo (Probabilidad de Fallo por Hora) y, en función de dicha probabilidad, un nivel SIL (Nivel de Integridad de Seguridad) clasifica dicho sistema en cuatro niveles. En el estándar EN, es obligatorio tanto evaluar la magnitud del riesgo de la máquina como llevar a cabo contramedidas para reducir el riesgo, y en el ISO 13849-1 se definen cinco categorías de seguridad. El controlador de seguridad, el sistema de control de seguridad, y similares, tal y como se denominan en la presente solicitud, corresponden a dicho estándar de seguridad. El sistema de control de seguridad se denomina, algunas veces, como “sistema de control de seguridad” y el controlador de seguridad se denomina, algunas veces, como “controlador de seguridad” o “dispositivo de control de seguridad”.

Si el controlador de seguridad es de tipo componente, cada unidad se conecta a un bus interno común para comunicarse a través del bus con la unidad de la CPU responsable del control del controlador de seguridad en su conjunto, y para intercambiar datos. La unidad de E/S acoplada también incluye un terminal de conexión, donde el dispositivo de entrada para la aplicación de seguridad o el dispositivo de salida para la aplicación de seguridad se conecta al terminal de conexión. El controlador de seguridad introduce la señal de entrada del dispositivo de entrada recibida desde el terminal remoto de seguridad a través de la comunicación de red, o la señal de entrada del dispositivo de entrada conectado a la unidad de E/S acoplada, y realiza la operación lógica en función de la CONEXIÓN/DESCONEXIÓN de la señal de entrada mediante un programa lógico almacenado previamente. En función del resultado de la operación, la señal de salida se envía al terminal remoto de seguridad y a la unidad de E/S. La unidad de E/S y unidades similares envían la señal de salida al dispositivo de salida. El conjunto de operaciones se ejecutan repetidamente de modo que el sistema completo, incluyendo el equipo robotizado de fabricación, puede ser controlado por el controlador de seguridad.

Con antelación, un programador crea el programa lógico, que se convierte en el núcleo del proceso de operación lógica en el controlador de seguridad o en la unidad de la CPU. La descripción de la programación en la creación del programa puede ser un diagrama de escalera, un diagrama de bloques de funciones, un diagrama de funciones secuenciales, texto estructurado, lista de instrucciones, y otros. El lenguaje de programación puede ser un lenguaje interpretado, lenguaje de script, lenguaje ensamblador, lenguaje de alto nivel, Java (marca registrada), y similares. Un código fuente escrito con dicho lenguaje de programación es sometido a un proceso como por ejemplo ensamblaje y compilación y, a continuación, lo ejecuta la CPU.

Un relé de seguridad y un interruptor como dispositivo de salida conectado a la unidad de E/S y al terminal remoto de seguridad se conectan al equipo robotizado de fabricación, equipo de procesado, equipo de desconexión, y equipos similares. El equipo robotizado de fabricación y equipos similares funcionan en tanto en cuanto el contacto principal del relé y el interruptor se encuentra CONECTADO, y el equipo robotizado de fabricación y equipos similares dejan de funcionar cuando el contacto se encuentra DESCONECTADO. Por lo tanto, el controlador de seguridad lleva a cabo el control asociado a la detención de la operación del robot y equipos similares para que sea controlado en última instancia por el control de CONEXIÓN/DESCONEXIÓN del dispositivo de salida. Describiéndolo con un ejemplo específico, cuando se introduce una señal que indica que se ha activado normalmente el conmutador de parada de emergencia, el controlador de seguridad desconecta el dispositivo de salida (relé e interruptor) de modo que el equipo sujeto a control no realiza una operación peligrosa o fuerza que el control pase al modo de seguridad y realiza inmediatamente las acciones de seguridad necesarias. Cuando se recibe un resultado de diagnóstico que indica que el conmutador de parada de emergencia u otro dispositivo de entrada que no funciona correctamente, el controlador de seguridad desconecta el dispositivo de salida para parar el funcionamiento de modo que el equipo sujeto a control no lleva a cabo una operación peligrosa independientemente de la presencia del funcionamiento del conmutador de parada de emergencia o el estado de conexión/desconexión del dispositivo de entrada.

El sistema de control de seguridad necesita diagnosticar si funciona normalmente el dispositivo de seguridad como por ejemplo el dispositivo de entrada y el dispositivo de salida conectados al PLC directamente o a través de la red, para hacer la transición al estado seguro de modo fiable en el momento en el que se produzca una emergencia. Para realizar dicho diagnóstico es necesario un algoritmo de diagnóstico único muy avanzado adaptado al dispositivo de entrada y al dispositivo de salida de cada a aplicación de seguridad (de aquí en adelante denominados de forma conjunta como “dispositivo de seguridad”), y no únicamente la medición del tiempo de funcionamiento y parámetros similares como en el algoritmo de diagnóstico divulgado en la Publicación de Patente de Japón sin Examinar número 2005-243008. Por lo tanto, se adopta una configuración en la que se prepara un controlador de diagnóstico dedicado adaptado a cada dispositivo de seguridad, y en la que el controlador de diagnóstico adaptado al dispositivo de seguridad relevante se coloca entre el PLC y el dispositivo de seguridad.

La invención divulgada en la Publicación de Patente de Japón sin Examinar número 2005-243008 almacena un algoritmo de diagnóstico en un dispositivo de entrada y en un dispositivo de salida y, de este modo, el algoritmo de diagnóstico se debe descargar de nuevo a un dispositivo de entrada de sustitución y dispositivos similares desde un dispositivo utilizado como herramienta de configuración si falla y se sustituye el dispositivo de entrada y similares, por lo tanto, la invención resulta inconveniente.

Además, cuando se crea el algoritmo de diagnóstico en el dispositivo utilizado como herramienta de configuración, esto resulta efectivo cuando se crea un algoritmo de diagnóstico flexible, pero es incómodo cuando crece el número de algoritmos de diagnóstico y la configuración de parámetros y, más aún, es posible que no se realice un diagnóstico correcto debido a un error humano como por ejemplo un error en la configuración de parámetros. Por otra parte, en el algoritmo de diagnóstico del dispositivo de seguridad, en particular, es muy incómoda la creación de un algoritmo de diagnóstico que incluye la configuración de parámetros debido a sus propiedades y, cuando se tienen en cuenta los errores humanos, no se puede garantizar el estado de seguridad. En los documentos EP 1717654 A2 y EP 1703348 A2 se describen otras aproximaciones a la técnica anterior.

Como un problema específico del sistema de control de seguridad descrito más arriba, es necesario preparar un controlador dedicado para realizar el diagnóstico del dispositivo de seguridad para cada dispositivo de seguridad, y es necesario incorporarlo independientemente del dispositivo de seguridad y del PLC. Por lo tanto, en la fabricación y almacenamiento de una pluralidad de diferentes tipos de controladores dedicados son necesarias tareas incómodas, un aumento en los pasos de trabajo cuando se construye un sistema de control de seguridad en un emplazamiento, y un lugar para la instalación del controlador dedicado.

Resumen

De acuerdo con un aspecto de la presente invención, para resolver los problemas descritos más arriba, una unidad de E/S de acuerdo con la presente invención es (1) una unidad de E/S para un controlador industrial que incluye un terminal de conexión para conectar un dispositivo de E/S como dispositivo de entrada y dispositivo de salida, y una unidad de control para recibir/enviar una señal de E/S con el dispositivo de E/S. La unidad de E/S incluye: una unidad de almacenamiento para almacenar una pluralidad de algoritmos de diagnóstico correspondiéndose cada uno a un dispositivo de E/S diferente; una unidad de almacenamiento de información de especificación para almacenar la información de especificación para especificar el algoritmo de diagnóstico que se debe utilizar entre la pluralidad de algoritmos de diagnóstico; una unidad de diagnóstico para realizar un diagnóstico del dispositivo de E/S conectado al terminal de conexión utilizando el algoritmo de diagnóstico especificado por la información de especificación almacenada en la unidad de almacenamiento de información de especificación entre la pluralidad de algoritmos de diagnóstico; y una unidad para ejecutar un proceso de anomalías cuando el resultado del diagnóstico de la unidad de diagnóstico indica alguna anomalía. (2) Se pueden proporcionar varios terminales de conexión, y la información de especificación puede configurarse para cada terminal de conexión.

En el modo de realización, el terminal de conexión se corresponde con “terminales 13c, 14c de entrada/salida”. En el modo de realización, la unidad de almacenamiento de información de especificación se corresponde con el “registro 21”. En el modo de realización, la unidad de almacenamiento se corresponde con los “ASIC 13a, 14a”. El proceso de anomalías incluye varios procesos como, por ejemplo, detener de la operación por sí mismo, notificar la anomalía a la unidad de la CPU, almacenar la anomalía ocurrida, y realizar el proceso de anomalías en el sistema de control de seguridad. En el modo de realización, la información de especificación se corresponde con “información de configuración del algoritmo de diagnóstico”. En el modo de realización, el controlador industrial se materializa mediante un controlador de seguridad que cumple con la normativa de seguridad, que además de la propiedad de alta velocidad, función de alto nivel, y ampliación de la funcionalidad del ordenador personal denominado controlador programable general (PLC) y un PAC (Controlador de Automatización Programable), incluye varios tipos de controladores además del controlador de alta precisión y durabilidad del PLC. En el modo de realización, la unidad de E/S se corresponde con la unidad Slice I/O (unidad Slice 13 de Entrada, unidad Slice 14 de Salida).

A la unidad de E/S se le proporciona una pluralidad de algoritmos de diagnóstico, uno de los cuales se especifica mediante la información de especificación y, de este modo, se puede facilitar la configuración en la herramienta de configuración. Inicialmente, el algoritmo de diagnóstico se puede almacenar y mantener en origen en lugar de utilizar el dispositivo utilizado como herramienta de configuración y similares y, de este modo, la tarea de configuración para hacer que opere la función de diagnóstico, se puede llevar a cabo fácilmente debido a que la información de especificación únicamente necesita configurarse incluso cuando se cambie con el mismo tipo de unidad de E/S debido a un fallo y similares. Como en una unidad de E/S se dispone una pluralidad de algoritmos de diagnóstico, el controlador dedicado, que es necesario para cada dispositivo de seguridad (dispositivo de E/S) en el sistema de control de seguridad, se convierte en innecesario, y con una única unidad de E/S se puede dar respuesta a una pluralidad de dispositivos de seguridad. Como el algoritmo de diagnóstico se mantiene en la unidad de E/S, el algoritmo de diagnóstico puede permanecer almacenado incluso si se sustituye con el mismo tipo de dispositivo de E/S con un fallo.

(3) El controlador industrial de acuerdo con la presente invención incluye la unidad de E/S de acuerdo con (1) o (2), y

una unidad de la CPU, en donde la unidad de la CPU tiene una función de almacenamiento y mantenimiento de la información de especificación, y de configuración de la información de especificación almacenada y mantenida para la unidad de E/S. De este modo, la unidad de la CPU puede realizar la configuración de la información de especificación con respecto a la unidad de E/S cuando se sustituye con una unidad de E/S nueva cuando ocurra un fallo en la unidad de E/S y, por lo tanto, la unidad de E/S se puede configurar fácilmente con la misma configuración que en el estado anterior del fallo sin utilizar el dispositivo utilizado como herramienta de configuración.

(4) La unidad de la CPU puede tener información de conexión de la unidad de E/S para la información de identificación de la especificación y una posición de colocación de la unidad de E/S que se va a conectar; y la unidad de la CPU puede tener una función de búsqueda de la información de conexión de la unidad de E/S y de transmisión de la información de especificación cuando se confirma una unidad de E/S sin errores en la configuración de la información de especificación en la unidad de E/S. Por consiguiente, en la medida de lo posible se impide una configuración errónea en diferentes unidades de E/S.

(5) La unidad de la CPU puede tener una función para configurar la unidad de E/S para su funcionamiento cuando la información de especificación se transmite con normalidad a la unidad de E/S. En este modo de realización, la determinación de si se ha transmitido o no con normalidad se realiza mediante la coincidencia o no de los valores de la suma de comprobación, pero se pueden utilizar otros métodos. Esto resulta seguro ya que la unidad de E/S no funciona si el algoritmo de diagnóstico no está configurado correctamente.

(6) La unidad de E/S puede tener una función de determinar de si la información de especificación se ha recibido o no con normalidad desde la unidad de la CPU, y de deshabilitar el funcionamiento de la unidad de control cuando no se recibe con normalidad. En este modo de realización, la determinación se realiza mediante la coincidencia o no de los valores de la suma de comprobación, pero se pueden utilizar otros métodos. Esto resulta seguro ya que la unidad de E/S no funciona si el algoritmo de diagnóstico no está configurado correctamente.

(7) La unidad de la CPU puede tener una función de inicio de la configuración de la unidad de E/S mediante una puesta en marcha, pulsando un interruptor, o mediante la recepción de una instrucción de ejecución desde un dispositivo utilizado como herramienta de configuración conectado a la unidad de la CPU como activador.

La presente invención puede conectar una pluralidad de dispositivos de seguridad con una única unidad de E/S y, de este modo, puede reducir los miembros de mantenimiento. No es necesario el restablecimiento mediante la herramienta de configuración y los cambios se pueden realizar en el momento de fallo de la unidad de E/S y, por lo tanto, se puede moderar el tiempo de inactividad del sistema completo. En la aplicación práctica del sistema de control de seguridad, se puede garantizar la seguridad del dispositivo de seguridad, del algoritmo de, etc. En otras palabras, suponiendo que se garantiza la seguridad del algoritmo de diagnóstico ya disponible en la unidad de E/S, únicamente es necesario especificar la información de especificación como, por ejemplo, un número y, de este modo no es necesario incluir autenticación de seguridad en el diseño del algoritmo de diagnóstico.

Breve descripción de los dibujos

La Fig. 1 es una vista que muestra un modo de realización preferido de un controlador de seguridad, que es un modo de un controlador programable de acuerdo con la presente invención;

La Fig. 2 es una vista que muestra una configuración interna de una unidad Slice I/O;

La Fig. 3 es una vista que muestra una configuración interna de una unidad de CPU;

La Fig. 4 es una vista que muestra un ejemplo de una estructura de datos en una memoria no volátil;

La Fig. 5 es un diagrama de flujo que muestra una función para realizar un proceso de almacenamiento de datos configurados en la memoria no volátil; y

La Fig. 6 es un diagrama de flujo que muestra una función para realizar un proceso de configuración en la unidad Slice I/O.

Descripción detallada

La Fig. 1 muestra un modo de realización apropiado de un controlador 10 de seguridad, que es un modo de un controlador programable de acuerdo con la presente invención.

El controlador 10 de seguridad incorpora una función de autodiagnóstico en términos de seguridad además de una función de operación lógica y una función de control de entrada/salida parecidas a las de un controlador programable general (PLC), de modo que se puede asegurar una alta seguridad y fiabilidad en el control. El controlador de seguridad tiene una función (función a prueba de fallos) para forzar la realización de un control de seguridad de modo que su control no dé lugar a ningún peligro cuando el resultado del autodiagnóstico detecte alguna anomalía.

El controlador 10 de seguridad es de tipo componente y en la Fig. 1 se muestra una configuración en la que se acoplan una unidad 11 de comunicación, una unidad 12 de la CPU, una unidad Slice 13 de Entrada, una unidad Slice 14 de Salida, y una unidad terminadora 15, pero esto no impide que se acoplen otros tipos distintos de unidades. El número de instalación de cada unidad es arbitrario. Cada unidad se conecta mediante un bus interno (bus PLC) 10a, e intercambia datos mediante la comunicación del bus con la unidad 12 de la CPU responsable del control del controlador de seguridad en su conjunto.

La unidad 11 de comunicación se conecta a un bus 2 de campo, y se comunica con equipos externos y dispositivos conectados al bus 2 de campo. En relación con la presente invención, la unidad 11 de comunicación tiene una función de comunicación con un dispositivo 1 utilizado como herramienta de configuración conectado al bus 2 de campo. Una MPU 11a de la unidad 11 de comunicación tiene una función de control de la transmisión y recepción de datos con el dispositivo 1 utilizado como herramienta de configuración, y envío de los datos recibidos desde el dispositivo 1 utilizado como herramienta de comunicación a la unidad de la CPU 12. Obviamente, la MPU 11a ejecuta una función normal que actúa como la unidad 11 de comunicación.

La unidad Slice I/O como por ejemplo la unidad Slice 13 de de Entrada y la unidad Slice 14 de Salida incluyen los ASIC 13a, 14a para ejecutar procesos como unidad de E/S. Los procesos en los ASIC 13a, 14a incluyen la entrada/salida de una señal de E/S con un dispositivo de seguridad conectado (dispositivo 5 de entrada de seguridad, dispositivo 6 de salida de seguridad), y la transmisión/recepción de datos de E/S respecto a la unidad 12 de la CPU a través del bus interno 10a. La unidad Slice I/O cumple las normas de seguridad y, por lo tanto, los ASIC 13a, 14a están duplicados. Aunque no se ilustra, se pueden disponer la MPU para la ejecución del proceso de funcionamiento que un ASIC no puede realizar, la RAM utilizada como memoria de trabajo cuando la MPU ejecuta la operación, y otras memorias.

La unidad Slice 13 de Entrada está conectada con el dispositivo 5 de entrada de seguridad, a través de un circuito 13b de entrada, y mediante el circuito 13b de entrada se recupera la señal de ENTRADA desde el dispositivo 5 de entrada de seguridad para el ASIC 13a. La unidad Slice 14 de Salida se conecta con el dispositivo 6 de salida de seguridad a través de un circuito 14b de salida, y mediante el circuito 14b de salida se proporciona la señal de SALIDA producida por el ASIC 14a al dispositivo 6 de salida de seguridad. Como se muestra en la Fig. 2, los dispositivos 5, 6 de seguridad se conectan a los terminales 13c, 14c de entrada/salida dispuestos en una posición predeterminada de cada unidad 13, 14 y transmiten y reciben la señal de E/S con los ASIC 13a, 14a a través de los circuitos 13b, 14b de entrada/salida.

En la presente invención, los ASIC 13a, 14a almacenan y mantienen, con anterioridad, una pluralidad de tipos (N) de algoritmos 20 de diagnóstico. La pluralidad de tipos (N) de algoritmos 20 de diagnóstico corresponde, respectivamente, a varios tipos de dispositivos de seguridad que se pueden conectar. En el presente modo de realización, la pluralidad de algoritmos 20 de diagnóstico se especifica unívocamente mediante un número. Esto es, los ASIC 13a, 14a tienen una función para ejecutar, en un momento apropiado, un algoritmo de diagnóstico especificado por el número almacenado en un registro interno 21, y realizar un diagnóstico sobre el dispositivo de seguridad conectado. Cuando se determina que el resultado del diagnóstico es anómalo, la unidad Slice I/O ejecuta un proceso de anomalías definido anteriormente. El proceso de anomalías puede detener el funcionamiento por sí mismo, notificar la anomalía a la unidad 12 de la CPU, o almacenar la anomalía que ha ocurrido. La función de ejecución del proceso de anomalías se puede incorporar en el ASIC, o la puede realizar la MPU que se monta por separado.

Por lo tanto, la unidad Slice I/O del presente modo de realización tiene una función de diagnóstico de una pluralidad de dispositivos de seguridad y especifica el algoritmo de diagnóstico que se utiliza selectivamente y, de este modo, no tiene una configuración compleja. Debido a que el funcionamiento de la función de diagnóstico especificada se realiza de acuerdo con la configuración de parámetros desde la unidad 12 de la CPU, no se interpone el factor humano y no se produce ningún fallo debido a un error de configuración humano.

Como se muestra en la Fig. 3, la unidad 12 de la CPU incluye una MPU 12a de comunicación, una MPU Slice 12b, una interfaz 12c de la unidad de comunicación, una memoria no volátil 12d y un controlador 12e USB. Como la unidad 12 de la CPU es compatible desde el punto de vista de la seguridad, la MPU 12a de comunicación, la MPU Slice 12b y la memoria no volátil 12d están duplicadas.

La interfaz 12c de la unidad de comunicación es una interfaz para transmitir y recibir datos en relación con la unidad 11 de comunicación. La MPU 12a de comunicación tiene una función para transmitir y recibir datos en relación con la MPU 11a de la unidad 11 de comunicación, y para almacenar los datos de configuración desde el dispositivo 1 utilizado como herramienta de configuración recibidos a través de la unidad 11 de comunicación en la memoria 12d no volátil como, por ejemplo, una EEPROM. La unidad 12 de la CPU incluye el controlador 12e USB y, de este modo, está conectado directamente con el dispositivo 1 utilizado como herramienta de configuración mediante una conexión USB, y puede obtener los datos de configuración del dispositivo 1 utilizado como herramienta de configuración sin pasar a través de la unidad 11 de comunicación y almacenarlos en la memoria 12d no volátil.

La MPU Slice 12b tiene una función de transmisión y recepción de datos en relación con la unidad Slice 13 de Entrada y la unidad Slice 14 de Salida, y de ejecución de varios tipos de procesos de operación en función de los datos adquiridos. En relación con la presente invención, la MPU Slice 12b establece los datos configurados (número que especifica el algoritmo de diagnóstico a utilizar) para la ejecución del algoritmo de diagnóstico en el registro 21 de la unidad Slice 13 de Entrada y la unidad Slice 14 de Salida. La MPU Slice 12b envía la señal de entrada del dispositivo 4 de entrada de seguridad conectado a la unidad Slice 13 de Entrada, realiza la operación lógica sobre la conexión/desconexión de la señal de entrada mediante el programa lógico almacenado con antelación para obtener la señal de salida, y envía a la unidad Slice 14 de Salida la señal de salida en función del resultado de la operación.

La memoria 12d no volátil almacena los datos de configuración de la unidad de la CPU que se muestran en la Fig. 4. Los datos de configuración de la unidad de la CPU se descargan del dispositivo 1 utilizado como herramienta de configuración y se almacenan. Los datos de configuración de la unidad de la CPU incluyen información de configuración de la unidad de la CPU, información de conexión de la unidad Slice I/O, e información de configuración de la unidad Slice I/O.

La información de configuración de la unidad de la CPU es un parámetro de configuración de la propia unidad de la CPU. La información de conexión de la unidad Slice I/O es información de identificación para especificar la unidad Slice I/O conectada, e incluye un número de unidad para especificar la posición y el tipo (información de identificación: ID) de la unidad Slice I/O incorporada. La unidad 12 de la CPU (MPU Slice 12b) obtiene la información de identificación de la unidad Slice I/O realmente acoplada, compara la información de identificación obtenida con la información de conexión de la unidad Slice I/O, y comprueba si se ha colocado en la posición correcta la unidad Slice I/O correcta. Si se incorpora una unidad Slice I/O distinta de la información de configuración, la CPU 12 impide la operación de la unidad Slice I/O. Esto es, la unidad 12 de la CPU tiene una función de conexión/desconexión de la operación de la unidad Slice I/O.

La información de configuración de la unidad Slice I/O incluye la información de configuración del algoritmo de diagnóstico, i.e., la información de especificación para especificar el algoritmo de diagnóstico utilizado en función del dispositivo de seguridad conectado al terminal de entrada/salida en cada unidad Slice I/O. En otras palabras, a la unidad Slice I/O se le puede conectar una pluralidad de dispositivos 5, 6 de seguridad y, en particular, si se incorporan distintos tipos de dispositivos de seguridad, el algoritmo de diagnóstico a utilizar es distinto para cada dispositivo de seguridad. El algoritmo de diagnóstico a utilizar se configura para cada terminal de entrada/salida de la unidad Slice I/O. La información de configuración del algoritmo de diagnóstico es específicamente un número que identifica uno entre una pluralidad de algoritmos de diagnóstico almacenados en el ASIC. La CPU 12 (MPU Slice 12b) establece la información en el registro 21 de los ASIC 13a, 14a de cada unidad Slice I/O para especificar el algoritmo de diagnóstico a utilizar en función de la información de configuración de la unidad Slice I/O. El registro 21 almacena la información para especificar el algoritmo de diagnóstico a utilizar para cada terminal de entrada/salida.

Aunque no se ilustra, la unidad 12 de la CPU también incluye una ROM del sistema y una parte de almacenamiento del programa de usuario para almacenar un programa que va a ejecutar la MPU, RAM que funciona como memoria de trabajo y una memoria de E/S cuando se realiza la operación, etc.

Las funciones del dispositivo 1 utilizado como herramienta de configuración y la unidad 12 de la CPU se describirán a continuación al mismo tiempo que se describe el procedimiento del proceso (proceso de configuración desde el dispositivo 1 utilizado como herramienta de configuración en relación con la unidad 12 de la CPU) para almacenar los datos de configuración en la memoria no volátil 12d haciendo referencia a la Fig. 5.

El usuario utiliza el dispositivo 1 de configuración para transmitir la orden de inicio desde el dispositivo 1 utilizado como herramienta de configuración a la unidad 12 de la CPU. Al recibir una orden de inicio de la configuración transmitida por el dispositivo 1 utilizado como herramienta de configuración (S1), la unidad 12 de la CPU crea y transmite una respuesta en función de la misma (S2).

Al recibir la respuesta desde la unidad 12 de la CPU, el dispositivo 1 utilizado como herramienta de configuración transmite la información de configuración de la unidad de la CPU. Al recibir la información de configuración de la unidad de la CPU transmitida desde el dispositivo 1 utilizado como herramienta de configuración (S3), la unidad 12 de la CPU crea y transmite la respuesta asociada (S4). La información de configuración de la unidad de la CPU recibida se amacena y mantiene temporalmente en una memoria intermedia o similar.

Al recibir la respuesta desde la unidad 12 de la CPU, el dispositivo 1 utilizado como herramienta de configuración transmite la información de conexión de la unidad Slice I/O. Al recibir la información de conexión de la unidad Slice I/O transmitida desde el dispositivo 1 utilizado como herramienta de configuración (S5), la unidad 12 de la CPU crea y transmite la respuesta en función de la misma (S6). La información de conexión de la unidad Slice I/O recibida se almacena y mantiene temporalmente en una memoria intermedia o similar.

Al recibir la respuesta desde la unidad 12 de la CPU, el dispositivo 1 utilizado como herramienta de configuración transmite la orden de suma de comprobación de la información de configuración de la unidad Slice o de la información transmitida y, de este modo, la unidad 12 de la CPU espera a la recepción de la orden de recepción

(S7), y si la orden recibida es la información de configuración de la unidad Slice I/O, crea y transmite la respuesta (S8). La información de configuración de la unidad Slice I/O se almacena y mantiene temporalmente en la memoria intermedia o similar.

Si la orden recibida es la orden de suma de comprobación, la unidad 12 de la CPU obtiene el valor de la suma de comprobación de la información de configuración recibida que está almacenada y mantenida temporalmente (S9), y la compara con el valor de la suma de comprobación recibido desde el dispositivo 1 utilizado como herramienta de configuración (S10). Si no coinciden los valores de las sumas de comprobación, la unidad 12 de la CPU transmite una respuesta de anomalía al dispositivo 1 utilizado como herramienta de configuración y el proceso termina (S12). Si los valores de la suma de comprobación coinciden en la decisión de bifurcación del paso S10 del proceso, la unidad 12 de la CPU transmite al dispositivo 1 utilizado como herramienta de configuración el valor de suma de comprobación calculado (S10).

El dispositivo 1 utilizado como herramienta de configuración compara el valor de la suma de comprobación (valor de la suma de comprobación transmitido) obtenido y transmitido anteriormente en relación con la unidad 12 de la CPU y el valor de la suma de comprobación (valor de la suma de comprobación de recepción) transmitido desde la unidad 12 de la CPU (S13), y finaliza el proceso si los valores de las sumas de comprobación no coinciden. Si los valores de las sumas de comprobación coinciden, el dispositivo 1 utilizado como herramienta de configuración transmite un orden de confirmación de coincidencia de los datos.

Al recibir la orden de confirmación de coincidencia de los datos (S14), la unidad 12 de la CPU guarda varios tipos de información que estaban almacenados temporalmente en la memoria no volátil 12d (S15) y finaliza el proceso después de transmitir la respuesta (S16). Si se termina la parte del proceso del dispositivo 1 utilizado como herramienta de configuración cuando el resultado de la comparación de los valores de las sumas de comprobación no coinciden en el dispositivo 1 utilizado como herramienta de configuración, como en la figura, la unidad 12 de la CPU descarta el almacenamiento temporal de datos y no guarda los datos en la memoria no volátil 12d cuando no recibe la orden de confirmación de coincidencia de datos incluso después de que haya transcurrido un período de tiempo constante. Si en la decisión de bifurcación del paso S13 del proceso no coinciden los valores de las sumas de comprobación, el dispositivo 1 utilizado como herramienta de configuración transmite la orden de que los datos no coinciden y, la unidad 12 de la CPU, después de recibir la orden de que los datos no coinciden, descarta el almacenamiento temporal de datos y no guarda los datos en la memoria no volátil 12d.

De este modo, se realiza la comprobación mediante el valor de la suma de comprobación por parte de la unidad 12 de la CPU y por parte de la herramienta 1 de configuración, y se guarda legítimamente cuando coincide en ambas partes y, de este modo, se mejora la precisión de la información que se almacena en la memoria no volátil 12d.

A continuación se describirán las funciones del dispositivo 1 utilizado como herramienta de configuración y de la unidad 12 de la CPU al mismo tiempo que se describe el procedimiento del proceso (proceso de configuración desde la unidad 12 de la CPU a la unidad Slice I/O) para almacenar en la unidad Slice I/O la información de configuración de la unidad Slice I/O almacenada en la memoria no volátil 12d haciendo referencia a la Fig. 6.

La unidad 12 de la CPU tiene una función de transmisión a la unidad Slice I/O del parámetro de configuración almacenado mediante un arranque, la pulsación de un interruptor o la recepción de una orden de ejecución desde el dispositivo utilizado como herramienta de configuración que actúa como activador. En otras palabras, cuando se produce dicha activación (S21), la unidad 12 de la CPU extrae la información de conexión de la unidad Slice I/O y la información de configuración de la unidad Slice I/O almacenadas en la memoria no volátil 12d (S22).

La unidad 12 de la CPU obtiene la posición de conexión y la información de reconocimiento de la unidad Slice I/O que se encuentra realmente conectada, y la compara con la información de conexión de la unidad Slice I/O leída (S23). El proceso termina cuando el resultado de la comparación es negativo y la unidad 12 de la CPU transmite la información de configuración correspondiente de la unidad Slice I/O a una unidad de E/S predeterminada (S24) de acuerdo con la información de conexión de la unidad Slice I/O leída cuando el resultado de la comparación indica coincidencia. La unidad Slice I/O predeterminada de destino comienza, por orden de importancia, en la unidad que tenga un número de unidad pequeño. Esto no excluye la transmisión en órdenes distintos.

La unidad Slice I/O devuelve la respuesta después de recibir la información de configuración de la unidad Slice I/O y, por lo tanto, la unidad 12 de la CPU espera la recepción de la respuesta. Al recibir la respuesta (S25), la unidad 12 de la CPU transmite el valor de la suma de comprobación (S26).

La unidad Slice I/O que recibió el valor de la suma de comprobación calcula el valor de la suma de comprobación a partir de la información de configuración de la unidad Slice I/O recibida con antelación (S27), y la compara con el valor de la suma de comprobación recibido (S28). Si los valores de las sumas de comprobación no coinciden, la unidad Slice I/O transmite una respuesta de anomalía a la unidad 12 de la CPU, y si los valores de la suma de comprobación coinciden transmite el valor de la suma de comprobación calculado a la unidad 12 de la CPU.

Al recibir una respuesta de anomalía (S30), la unidad 12 de la CPU pone en estado DESACTIVADO el indicador de

coincidencia de la unidad Slice I/O (S33). Al recibir el valor de la suma de comprobación transmitido desde la unidad Slice I/O (S29), la unidad 12 de la CPU compara el valor de la suma de comprobación (valor de la suma de comprobación de transmisión) obtenido y transmitido con antelación con el valor de la suma de comprobación (valor de la suma de comprobación de recepción) transmitido desde la unidad Slice I/O (S31). Si los valores de la suma de comprobación coinciden, la unidad 12 de la CPU pone en estado ACTIVADO el indicador de coincidencia en la configuración de la unidad Slice I/O (S32). Si los valores de la suma de comprobación no coinciden, la unidad 12 de la CPU pone en estado DESACTIVADO el indicador de coincidencia en la configuración de la unidad Slice I/O (S33).

Se determina si se completa o no la configuración en todas las unidades Slice I/O (S34), donde el proceso vuelve al paso S24 de proceso si existe una unidad sin configurar, y realiza la transmisión a la próxima unidad Slice I/O. Si se completa la configuración de todas las unidades Slice I/O, la unidad 12 de la CPU realiza el proceso de inicio en la unidad Slice I/O cuyo indicador de coincidencia se encuentra en el estado activado (S35).

De este modo, únicamente se inicia la unidad Slice I/O correcta tal y como se ha indicado en la información de conexión de la unidad Slice I/O, siendo la unidad Slice I/O tal que en el registro 21 se encuentra registrado el número del algoritmo de diagnóstico correcto tal y como se indica en la información de configuración de la unidad Slice I/O, gracias a lo cual la unidad puede funcionar de modo seguro. El momento de grabación de la información de configuración de la unidad Slice I/O (número que especifica el algoritmo de diagnóstico a utilizar) transmitida desde la unidad 12 de la CPU al registro 21 depende de si coinciden los valores de comprobación en la unidad Slice I/O. Se puede recibir la información desde la unidad 12 de la CPU y grabarla en el registro 21 antes de realizar la comprobación de coincidencia. Incluso si la información se almacena en el registro 21 al recibirse, la unidad Slice I/O no se puede iniciar en el paso S35 del proceso a menos que, en última instancia, coincidan los valores de las sumas de comprobación tanto por parte de la unidad 12 de la CPU como por parte de la unidad Slice I/O y, de este modo, no surjan problemas incluso si la información se registra por adelantado en el registro.

De acuerdo con el presente modo de realización, la información para especificar el algoritmo de diagnóstico a utilizar en cada unidad Slice I/O (información de configuración de la unidad Slice I/O) se guarda en la memoria no volátil 12d de la unidad 12 de la CPU. Por lo tanto, incluso si se sustituye la unidad Slice I/O, se puede registrar desde la unidad de la CPU la información de configuración para especificar el algoritmo de diagnóstico a utilizar en la unidad Slice I/O recién incorporada si se instala una unidad Slice I/O del mismo tipo.

Por lo tanto, cuando se registra dicha información de configuración, es menos probable que ocurra un error humano y se puede mantener el entorno de seguridad de modo fácil y fiable.

Cuando se sustituye el tipo de dispositivo de seguridad, se puede realizar fácilmente la configuración simplemente volviendo a grabar la información de configuración almacenada en el registro que contiene la información de configuración (el número) que especifica el algoritmo de diagnóstico correspondiente al nuevo dispositivo de seguridad.

En el modo de realización descrito más arriba, se ha descrito un ejemplo de su aplicación a un controlador de seguridad compatible con las normas de seguridad, pero la presente invención no se limita con ello y se puede aplicar a un controlador programable normal (unidad de E/S).

REIVINDICACIONES

1. Una unidad (13, 14) de E/S para un controlador industrial, incluyendo la unidad (13, 14) de E/S un terminal (13c, 14c) de conexión para conectar un dispositivo (5, 6) de E/S como un dispositivo de entrada y como un dispositivo de salida, e incluyendo, además, una unidad de control para recibir/enviar una señal de E/S en relación con el dispositivo (5, 6) de E/S; caracterizándose la unidad (13, 14) de E/S por comprender:

una unidad (13a, 14a) de almacenamiento para almacenar una pluralidad de algoritmos (20) de diagnóstico, correspondiéndose cada uno con un dispositivo (5, 6) de E/S distinto;

una unidad (21) de almacenamiento de la información de especificación para almacenar la información de especificación para especificar los algoritmos (20) de diagnóstico a utilizar entre la pluralidad de algoritmos (20) de diagnóstico;

una unidad de diagnóstico para realizar un diagnóstico del dispositivo (5, 6) de E/S conectado al terminal (13c, 14c) de conexión utilizando el algoritmo (20) de diagnóstico especificado por la información de especificación almacenada en la unidad (21) de almacenamiento de la información de especificación de la pluralidad de algoritmos (20) de diagnóstico; y

una unidad para ejecutar un proceso de anomalía cuando un resultado del diagnóstico de la unidad de diagnóstico es anómalo.

2. La unidad (13, 14) de E/S de acuerdo con la reivindicación 1, caracterizada por que:

la unidad (13, 14) de E/S incluye una pluralidad de terminales de conexión; y la unidad (21) de almacenamiento de la información de especificación se adapta para almacenar la información de especificación que se establece para cada uno de los terminales de conexión.

3. Un controlador industrial que comprende la unidad (13, 14) de E/S de acuerdo con la reivindicación 1 ó 2, y una unidad (12) de CPU, caracterizada por que:

la unidad (12) de CPU tiene una función de almacenamiento y mantenimiento de la información de especificación, y de asignar la información de especificación almacenada y mantenida a la unidad (13, 14) de E/S.

4. El controlador industrial de acuerdo con la reivindicación 3, caracterizado por que:

la unidad (12) de la CPU tiene una función de almacenamiento y mantenimiento de la información de conexión de la unidad de E/S para especificar la información de identificación y una posición de colocación de la unidad (13, 14) de E/S que se va a conectar; y

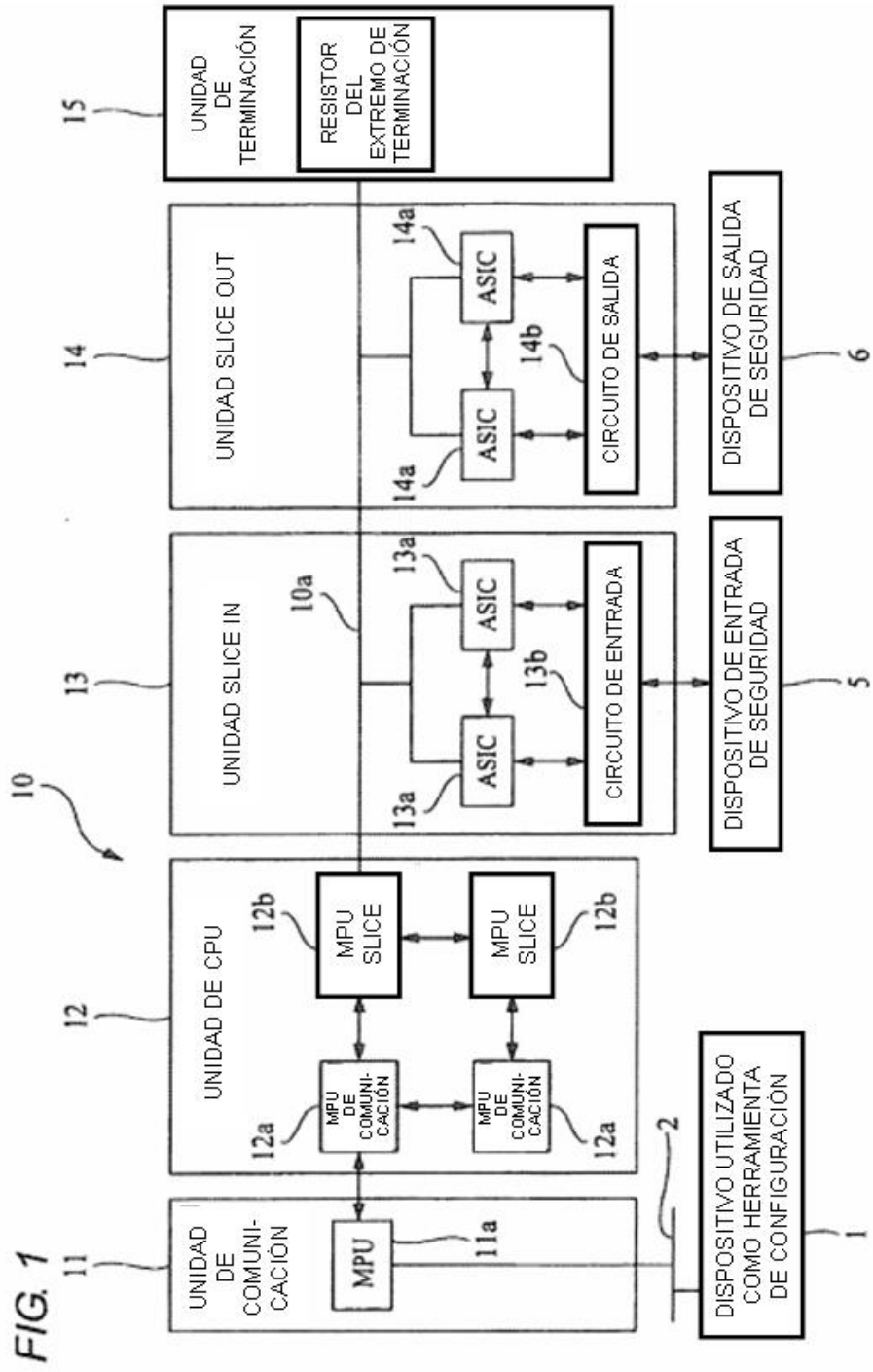
la unidad (12) de la CPU tiene una función de referencia de la información de conexión de la unidad de E/S y transmisión de la información de especificación cuando se confirma como correcta una unidad (13, 14) de E/S al asignar la información de especificación a la unidad (13, 14) de E/S.

5. El controlador industrial de acuerdo con la reivindicación 3 ó 4, caracterizado por que la unidad (12) de la CPU tiene una función de establecer que la unidad (13, 14) de E/S es operable cuando la información de especificación se transmite normalmente a la unidad (13, 14) de E/S.

6. El controlador industrial de acuerdo con cualquiera de las reivindicaciones 3 a 5, caracterizado por que la unidad (13, 14) de E/S tiene una función para determinar si, desde la unidad (12) de la CPU, se recibe normalmente o no la información de especificación, y para desactivar el funcionamiento de la unidad de control cuando no se recibe normalmente la información de especificación.

7. El controlador industrial de acuerdo con cualquiera de las reivindicaciones 3 a 6, caracterizado porque la unidad (12) de la CPU tiene una función de inicio de la configuración de la unidad (13, 14) de E/S mediante una puesta en marcha, pulsando un interruptor, o mediante la recepción de una orden de ejecución desde un dispositivo utilizado como herramienta de configuración conectado a la unidad (12) de la CPU que actúa como activador.

FIG. 1


DISPOSITIVO UTILIZADO COMO HERRAMIENTA DE CONFIGURACIÓN
1
2
UNIDAD DE COMUNI-CACIÓN
11
MPU
11a
UNIDAD DE CPU
12
MPU DE COMUNI-CACIÓN
12a
MPU SLICE
12b
10
UNIDAD SLICE IN
13
10a
ASIC
13a
13b
CIRCUITO DE ENTRADA
DISPOSITIVO DE ENTRADA DE SEGURIDAD
5
UNIDAD SLICE OUT
14
14a
14b
CIRCUITO DE SALIDA
DISPOSITIVO DE SALIDA DE SEGURIDAD
6
UNIDAD DE TERMINACIÓN
15
RESISTOR DEL EXTREMO DE TERMINACIÓN

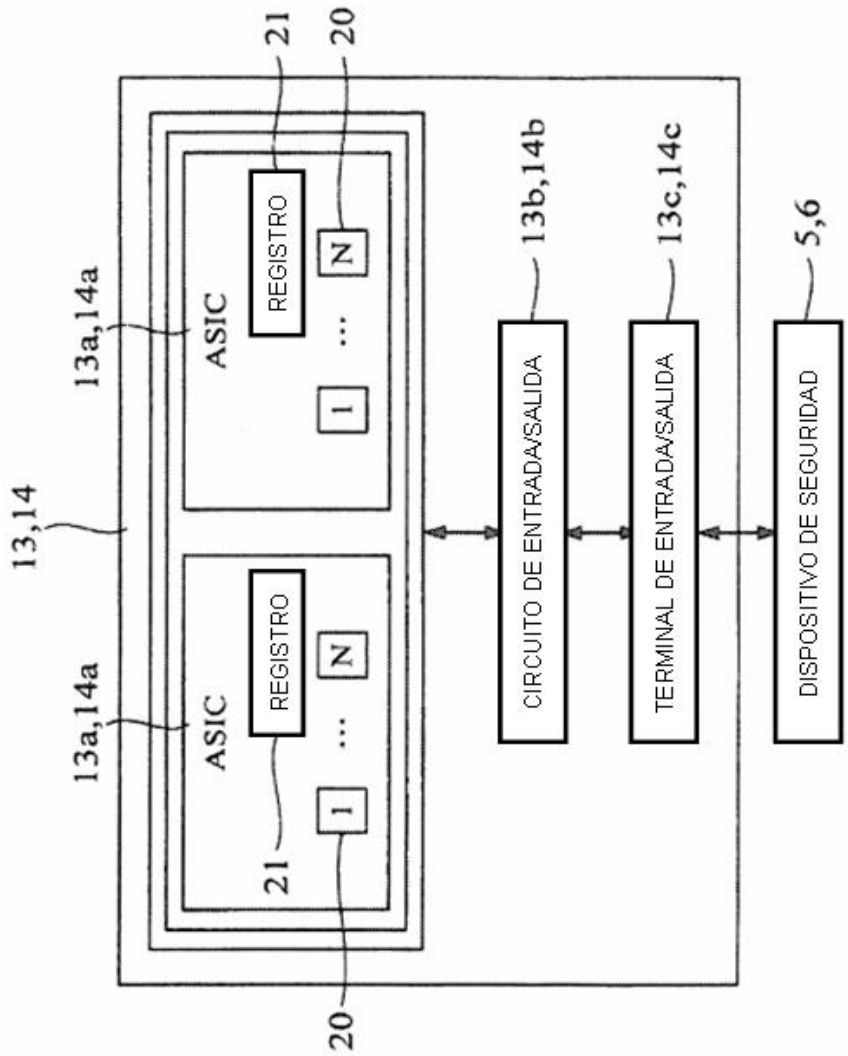

13,14
13a,14a
ASIC
REGISTRO
1
...
N
21
20
13b,14b
CIRCUITO DE ENTRADA/SALIDA
13c,14c
TERMINAL DE ENTRADA/SALIDA
5,6
DISPOSITIVO DE SEGURIDAD

FIG. 2

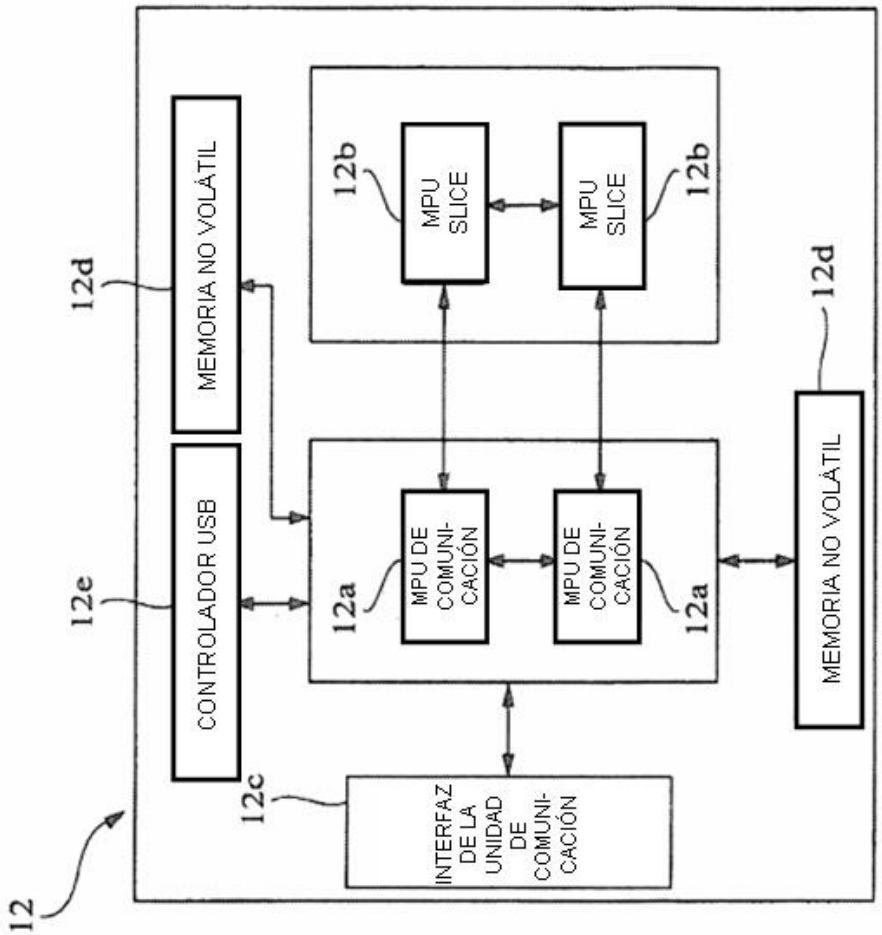

12
12c
INTERFAZ DE LA UNIDAD DE COMUNI-CACIÓN
12e
CONTROLADOR USB
12d
MEMORIA NO VOLÁTIL
12a
MPU DE COMUNI-CACIÓN
MPU DE COMUNI-CACIÓN
12a
12b
MPU SLICE
MPU SLICE
12b
12d
MEMORIA NO VOLÁTIL

FIG. 3

FIG. 4

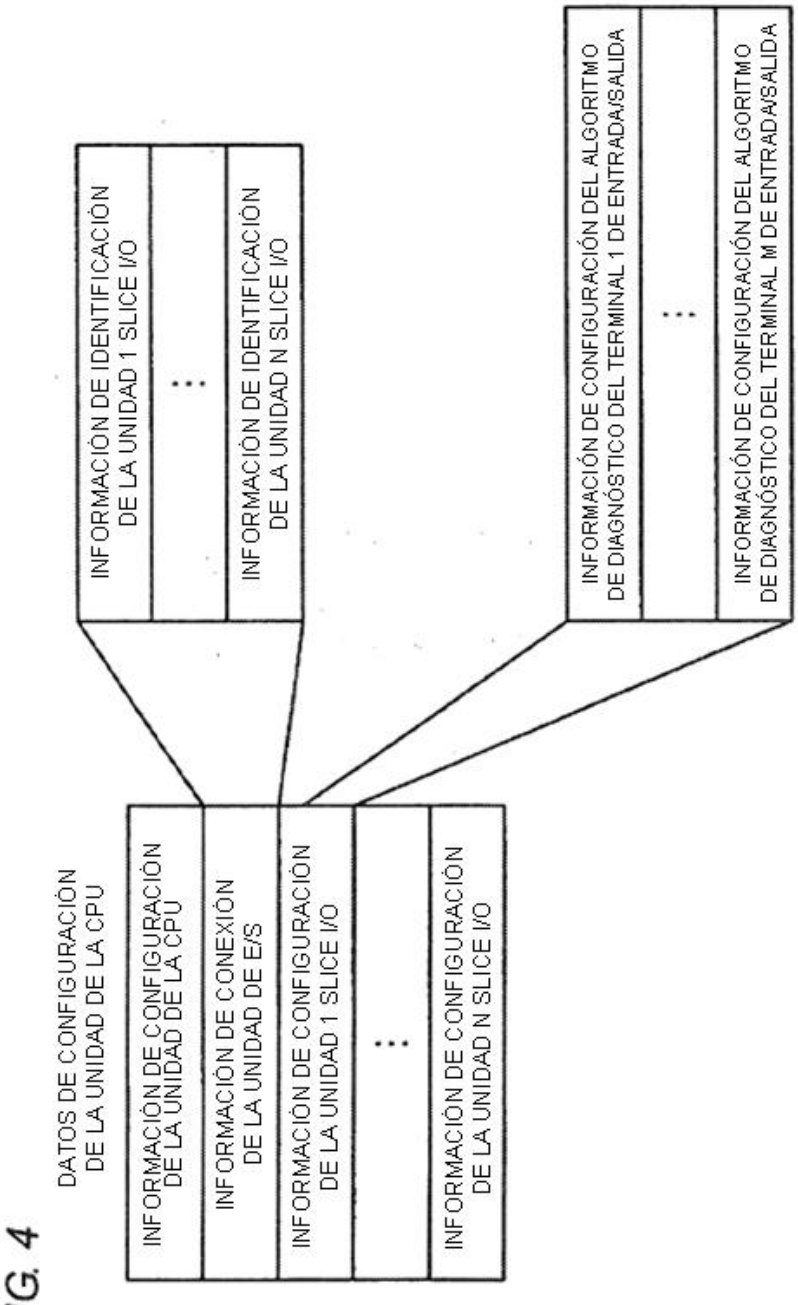

DATOS DE CONFIGURACIÓN DE LA UNIDAD DE LA CPU
INFORMACIÓN DE CONFIGURACIÓN DE LA UNIDAD DE LA CPU
INFORMACIÓN DE CONEXIÓN DE LA UNIDAD DE E/S
INFORMACIÓN DE CONFIGURACIÓN DE LA UNIDAD 1 SLICE I/O
...
INFORMACIÓN DE CONFIGURACIÓN DE LA UNIDAD N SLICE I/O
INFORMACIÓN DE IDENTIFICACIÓN DE LA UNIDAD 1 SLICE I/O
...
INFORMACIÓN DE IDENTIFICACIÓN DE LA UNIDAD N SLICE I/O
INFORMACIÓN DE CONFIGURACIÓN DEL ALGORITMO DE DIAGNÓSTICO DEL TERMINAL 1 DE ENTRADA/SALIDA
...
INFORMACIÓN DE CONFIGURACIÓN DEL ALGORITMO DE DIAGNÓSTICO DEL TERMINAL M DE ENTRADA/SALIDA

FIG. 5

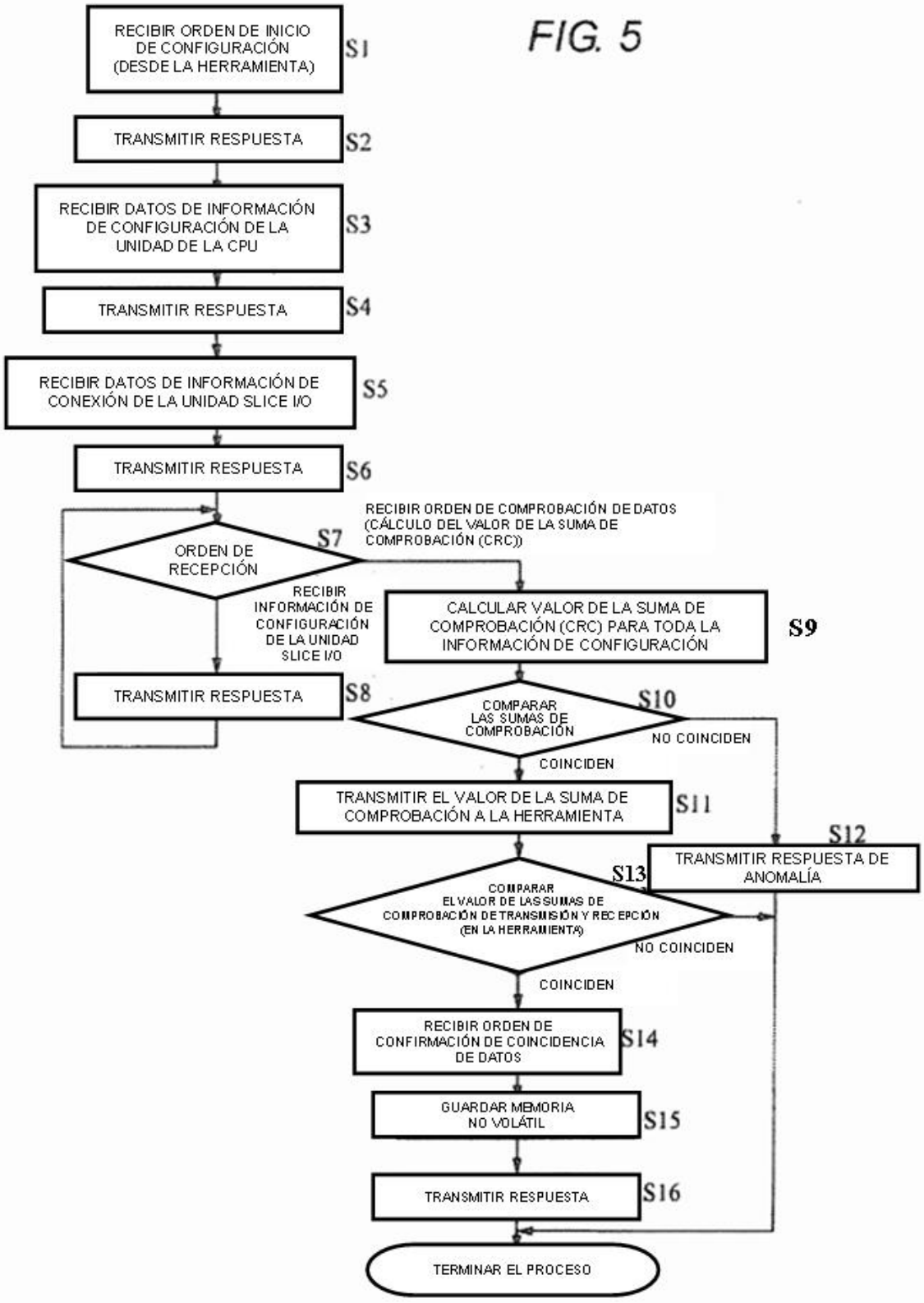
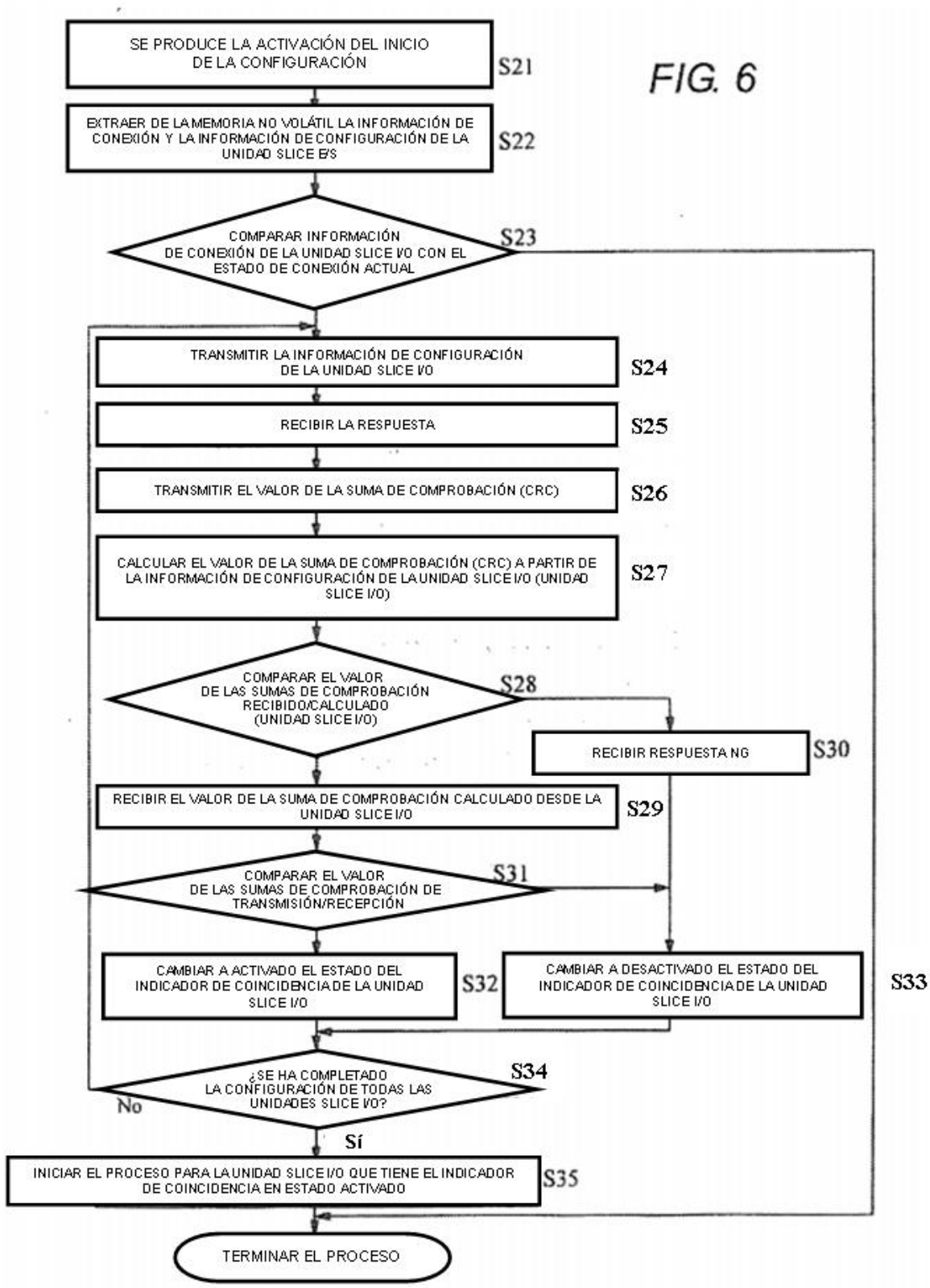

RECIBIR ORDEN DE INICIO DE CONFIGURACIÓN (DESDE LA HERRAMIENTA)
S1
TRANSMITIR RESPUESTA
S2
RECIBIR DATOS DE INFORMACIÓN DE CONFIGURACIÓN DE LA UNIDAD DE LA CPU
S3
TRANSMITIR RESPUESTA
S4
RECIBIR DATOS DE INFORMACIÓN DE CONEXIÓN DE LA UNIDAD SLICE I/O
S5
TRANSMITIR RESPUESTA
S6
ORDEN DE RECEPCIÓN
S7
RECIBIR ORDEN DE COMPROBACIÓN DE DATOS (CÁLCULO DEL VALOR DE LA SUMA DE COMPROBACIÓN (CRC))
RECIBIR INFORMACIÓN DE CONFIGURACIÓN DE LA UNIDAD SLICE I/O
TRANSMITIR RESPUESTA
S8
CALCULAR VALOR DE LA SUMA DE COMPROBACIÓN (CRC) PARA TODA LA INFORMACIÓN DE CONFIGURACIÓN
S9
COMPARAR LAS SUMAS DE COMPROBACIÓN
S10
NO COINCIDEN
COINCIDEN
TRANSMITIR EL VALOR DE LA SUMA DE COMPROBACIÓN A LA HERRAMIENTA
S11
S12
TRANSMITIR RESPUESTA DE ANOMALÍA
S13
COMPARAR EL VALOR DE LAS SUMAS DE COMPROBACIÓN DE TRANSMISIÓN Y RECEPCIÓN (EN LA HERRAMIENTA)
NO COINCIDEN
COINCIDEN
RECIBIR ORDEN DE CONFIRMACIÓN DE COINCIDENCIA DE DATOS
S14
GUARDAR MEMORIA NO VOLÁTIL
S15
TRANSMITIR RESPUESTA
S16
TERMINAR EL PROCESO

FIG. 6


SE PRODUCE LA ACTIVACIÓN DEL INICIO DE LA CONFIGURACIÓN
S21
EXTRAER DE LA MEMORIA NO VOLÁTIL LA INFORMACIÓN DE CONEXIÓN Y LA INFORMACIÓN DE CONFIGURACIÓN DE LA UNIDAD SLICE E/S
S22
COMPARAR INFORMACIÓN DE CONEXIÓN DE LA UNIDAD SLICE I/O CON EL ESTADO DE CONEXIÓN ACTUAL
S23
TRANSMITIR LA INFORMACIÓN DE CONFIGURACIÓN DE LA UNIDAD SLICE I/O
S24
RECIBIR LA RESPUESTA
S25
TRANSMITIR EL VALOR DE LA SUMA DE COMPROBACIÓN (CRC)
S26
CALCULAR EL VALOR DE LA SUMA DE COMPROBACIÓN (CRC) A PARTIR DE LA INFORMACIÓN DE CONFIGURACIÓN DE LA UNIDAD SLICE I/O (UNIDAD SLICE I/O)
S27
COMPARAR EL VALOR DE LAS SUMAS DE COMPROBACIÓN RECIBIDO/CALCULADO (UNIDAD SLICE I/O)
S28
RECIBIR RESPUESTA NG
S30
RECIBIR EL VALOR DE LA SUMA DE COMPROBACIÓN CALCULADO DESDE LA UNIDAD SLICE I/O
S29
COMPARAR EL VALOR DE LAS SUMAS DE COMPROBACIÓN DE TRANSMISIÓN/RECEPCIÓN
S31
CAMBIAR A ACTIVADO EL ESTADO DEL INDICADOR DE COINCIDENCIA DE LA UNIDAD SLICE I/O
S32
CAMBIAR A DESACTIVADO EL ESTADO DEL INDICADOR DE COINCIDENCIA DE LA UNIDAD SLICE I/O
S33
¿SE HA COMPLETADO LA CONFIGURACIÓN DE TODAS LAS UNIDADES SLICE I/O?
S34
No
Sí
INICIAR EL PROCESO PARA LA UNIDAD SLICE I/O QUE TIENE EL INDICADOR DE COINCIDENCIA EN ESTADO ACTIVADO
S35
TERMINAR EL PROCESO