(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 400 369**

(51) Int. CI.:

G05B 19/05 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **13.04.2006 E 06007864 (9)**

(97) Fecha y número de publicación de la concesión europea: **13.02.2013 EP 1717654**

(54) Título: **Dispositivo de entrada de una unidad de seguridad**

(30) Prioridad:

19.04.2005 JP 2005121673
31.03.2006 JP 2006097197

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
09.04.2013

(73) Titular/es:

OMRON CORPORATION (100.0%)
801, MINAMIFUDODO-CHO,
HORIKAWAHIGASHIIRU, SHIOKOJI-DORI,
SHIMOGOYO-KU KYOTO-SHI
KYOTO 600-8530, JP

(72) Inventor/es:

TERANISHI, KEIICHI;
MUNETA, YASUO;
KOSHIRO, CHIAKI;
IKENO, NAOAKI;
NAKAMURA, TOSHIYUKI;
SUGANUMA, HIROMU;
MATSUI, ASAHI;
YOSHIDA, KATSUFUMI;
FUJIWARA, SHOHEI y
HIOKA, TAKEHIKO

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Dispositivo de entrada de una unidad de seguridad

ANTECEDENTES DEL INVENTO

1. Campo del Invento

El presente invento se refiere a un dispositivo de entrada de una unidad de seguridad preferible como un medio de entrada de la unidad de seguridad tal como un controlador de seguridad y un terminal de seguridad remoto.

2. Descripción de la Técnica Relacionada

Se ha desarrollado una variedad de controladores de seguridad con una conciencia intensificada actualmente para trabajar con seguridad. El controlador de seguridad asegura una alta fiabilidad incorporando una función de auto-diagnóstico para la seguridad además de una función de operación aritmética lógica similar al controlador programable general (PLC) y a la función de control de I/O. Este controlador de seguridad tiene una función de controlar el lado de seguridad obligatoriamente de modo que impida que su propio control lleve a un peligro si se ha detectado una anormalidad como un resultado de la auto-diagnosis. Más específicamente, la seguridad mencionada aquí incluye una norma de seguridad especificada. La norma incluye por ejemplo, la IEC61508, una norma EN y similar. La norma IEC61508 (Comisión Electrotécnica Internacional relativa a la seguridad funcional de un sistema electrónico programable) ha definido el peligro de la probabilidad de fallo por hora (probabilidad de fallo por hora) y ha clasificado el nivel de integridad de seguridad (SIL) en cuatro etapas dependiendo de esta probabilidad. La EN (Norma Europea) evalúa la gravedad del riesgo de máquina y obliga a tomar una medida que reduzca el riesgo y la EN954-1 estipula cinco categorías de seguridad. El controlador de seguridad del presente invento satisface cualquiera de estas normas de seguridad.

Desde antes, es bien conocido un sistema de control de seguridad en el que un controlador 2 de seguridad y un esclavo 1 de seguridad están conectados con una red 3 como se ha mostrado en la fig. 11. El esclavo 1 de seguridad asegura una alta fiabilidad incorporando una función de auto-diagnóstico tanto para la entrada como para la salida además de la misma función que un esclavo en un PLC corriente. El controlador 2 de seguridad tiene la función maestra de comunicación de ejecutar una comunicación con el esclavo 1 de seguridad a través de la red y es llamado a veces maestro de seguridad. El esclavo 1 de seguridad es llamado a veces terminal de seguridad remoto y tiene una función de comunicación de red (función de esclavo controlado por el maestro) con la función maestra de comunicación del controlador 2 de seguridad. El esclavo de seguridad tiene un terminal de conexión y al menos uno de un dispositivo de entrada tal como un interruptor para emitir la señal ACTIVADO/DESACTIVADO y un dispositivo de salida que actúa como un destino de salida de la señal de control está conectado a ese terminal de conexión (aunque la fig. 11 muestra un ejemplo del dispositivo de salida mientras un interruptor SW de parada de emergencia está conectado al mismo, una cortina o persiana, un interruptor de puerta, un interruptor de 2 manos y similar pueden estar conectados. Se ha omitido la representación del dispositivo de salida. El dispositivo de salida incluye un relé de seguridad, contactor y similar). Estos dispositivos de entrada y salida cumplen con las normas de seguridad. El esclavo de seguridad genera datos de control basándose en una señal introducida desde un dispositivo de aplicación de seguridad conectado y transmite los datos de control generados al controlador de seguridad a través de la red. El esclavo de seguridad recibe los datos de control desde el controlador de seguridad mediante comunicación con el controlador de seguridad a través de la red. A continuación, el controlador 2 de seguridad recibe una señal de entrada desde un dispositivo de entrada introducida desde el esclavo 1 de seguridad a través de comunicación por red, ejecuta la operación lógica de ACTIVADO/DESACTIVADO de la señal de entrada de acuerdo con un programa lógico almacenado preliminarmente y emite una señal de salida basándose en un resultado de la operación lógica al esclavo 1 de seguridad a través de comunicación por red. El esclavo de seguridad emite la señal de salida a un dispositivo de salida. Como resultado de ejecutar tal serie de operaciones repetidamente, el controlador de seguridad controla el sistema completo. El ciclo de comunicación entre el controlador 2 de seguridad y el esclavo 1 de seguridad puede ser síncrono con el ciclo de ejecución repetitivo del controlador de seguridad o puede ser asíncrono. El dispositivo de salida está conectado a un robot operativo, a una máquina de tratamiento, a una herramienta de corte o similar y cuando el relé de seguridad del dispositivo de seguridad o un punto del contactor es ACTIVADO, el robot operativo es accionado y cuando el punto de contacto es DESACTIVADO, el robot operativo es detenido. El controlador de seguridad controla el robot operativo o similar como un objeto de control controlando el ACTIVADO/DESACTIVADO del dispositivo de salida. Es decir, si el controlador 2 de seguridad ha sido notificado de que el interruptor SW de parada de emergencia es hecho funcionar apropiadamente cuando controla un objeto de control (no mostrado) por el esclavo de seguridad a través de comunicación, DESACTIVA el dispositivo de salida o controla el estado al lado de seguridad, obligatoriamente, con el fin de impedir que el objeto de control realice una acción peligrosa de modo que adopte una medida de seguridad necesaria inmediatamente. Además si el controlador de seguridad recibe un resultado de diagnóstico que indica que el interruptor SW de parada de emergencia u otro dispositivo de entrada (no mostrado) tiene un error cuando controla un objeto de control (no mostrado), desactiva el dispositivo de salida o controla el estado al lado de seguridad, obligatoriamente, para detener la operación del objeto de control con el fin de impedir que el objeto de control realice

una acción peligrosa independientemente de si el interruptor SW de parada de emergencia es accionado o el dispositivo de entrada es ACTIVADO/DESACTIVADO, de modo que se adopte una medida de seguridad necesaria inmediatamente.

En el sistema de control de seguridad de tipo maestro/esclavo en el que el controlador de seguridad es un puesto maestro de comunicación y el esclavo de seguridad es un puesto esclavo de comunicación como se ha mostrado en la fig. 11, si un resultado de diagnóstico que indica que un terminal de entrada al que está conectado un interruptor (SW) de aplicación de seguridad que cumple la norma de seguridad tiene un error como resultado de la operación de la función de auto-diagnóstico del esclavo 1 de seguridad, se adoptan algunas contramedidas selectivamente por el lado del esclavo de seguridad con el fin de garantizar la seguridad de la operación en el lado del maestro de seguridad.

Una primera contramedida en el lado del esclavo de seguridad es establecer el valor de los datos de control (datos de entrada cuya seguridad está asegurada) que han de ser transmitidos al maestro 2 de seguridad correspondiente al terminal para DESACTIVAR (“BAJO”) obligatoriamente y transmitir DESACTIVADO (“BAJO”) al controlador 2 de seguridad. Una segunda contramedida es bloquear los datos de control erróneo que están siendo transmitidos al controlador de seguridad cortando la comunicación a través de la red.

De acuerdo con la primera contramedida, si se ha diagnosticado que el interruptor (SW) de aplicación de seguridad tiene un error en el lado del esclavo 1 de seguridad, el valor de los datos de control correspondiente al interruptor (SW) de aplicación de seguridad es obligatoriamente establecido al estado DESACTIVADO (“BAJO”) del mismo modo que cuando el interruptor de aplicación de seguridad es apretado y por consiguiente, el lado del controlador 2 de seguridad que recibe los datos de control puede adoptar inmediatamente una medida de seguridad necesaria.

Sin embargo, de acuerdo con la primera contramedida, el lado del maestro 2 de seguridad no puede determinar si cuando el valor de los datos de control está en estado DESACTIVADO (”BAJO”), está en el estado DESACTIVADO (“BAJO”) como resultado de que el interruptor (SW) de aplicación de seguridad está siendo apretado realmente o está en estado DESACTIVADO (“BAJO”) como resultado de estar obligatoriamente establecido al estado porque el resultado del diagnóstico indica que existe un error. Por ello, el lado del maestro de seguridad que recibe los datos de control tiene un problema tal que no puede adoptar una contramedida suficiente porque requiere tiempo y trabajo restaurar el sistema después eso. La razón es porque incluso si el sistema es detenido como resultado de que el interruptor SW de parada de emergencia está siendo apretado apropiadamente, si el sistema es detenido porque el interruptor de parada de emergencia es apretado apropiadamente o debido a que no se ha podido determinar automáticamente un problema, es imposible discriminar si no se requiere nada más que liberar el interruptor de parada de emergencia o es necesario comprobar cualquier error y así, ocurre una necesidad de comprobación cada vez, de modo que requiere tiempo restaurar el sistema cada vez que el sistema de detiene.

De acuerdo con la segunda contramedida, debido a que el valor de los datos de control es establecido al estado DESACTIVADO (“BAJO”) obligatoriamente debido a la ausencia de datos de recepción en el lado del maestro de seguridad, el valor de los datos de control correspondiente al interruptor (SW) de aplicación de seguridad en el lado del maestro 2 de seguridad es establecido al estado DESACTIVADO (“BAJO”) obligatoriamente del mismo modo que cuando el interruptor de aplicación de seguridad es apretado cerrando la comunicación en el lado del esclavo 1 de seguridad, el lado del controlador 2 de seguridad puede adoptar inmediatamente una medida de seguridad necesaria para el sistema.

Sin embargo, la segunda contramedida tiene un problema tal que no puede buscarse una razón hasta que se lee la historia del error después de que se haya detenido el sistema y que necesita tiempo para el trabajo de restauración del sistema. La razón es que debido a que es imposible determinar automáticamente si el sistema se ha detenido porque el interruptor SW de parada de emergencia es apretado apropiadamente o porque el sistema tiene problemas, es imposible discriminar si no se requiere nada más que liberar el interruptor de parada de emergencia o es necesario eliminar una causa de un error en la red y por consiguiente, ocurre una necesidad de comprobación cada vez, de forma que se necesita tiempo para la restauración del sistema cada vez que el sistema se detiene.

Un esclavo de seguridad de acuerdo con el preámbulo de la reivindicación 1 es conocido a partir de los documentos FR 2.681.160 A1 y EP 1.396.771 A.

RESUMEN DEL INVENTO

El presente invento ha sido conseguido en vista de los problemas antes descritos en un sistema de control de seguridad convencional y un objeto del invento es proporcionar un dispositivo de entrada de unidad de seguridad que permita que un resultado del diagnóstico de error mencionado por una unidad de seguridad tal como un controlador de seguridad, el esclavo de seguridad en un proceso de generar datos de control desde una señal de entrada bruta desde un interruptor de aplicación de seguridad o similar, sea adoptado por el lado del controlador que utiliza dichos datos de control de modo que se consigan una variedad de controles de seguridad basándose en los datos de control.

El invento es según se ha definido en la reivindicación 1. De acuerdo con un primer aspecto, se ha proporcionado una unidad esclava de seguridad que con un dispositivo de entrada basado en una especificación de seguridad y activado cuando existe un peligro conectado al mismo, recibe una señal acerca de la presencia/ausencia de una acción procedente del dispositivo de entrada como una entrada, maneja la señal como una señal de entrada y está conectada a un controlador de seguridad basado en la especificación de seguridad a través de una red de modo que transmite la señal de entrada a un maestro de comunicación en el lado del controlador de seguridad, que comprende: una parte de terminal de entrada que tiene uno o dos o más terminales de entrada alimentados con una señal de entrada procedente del dispositivo de entrada basado en la especificación de seguridad; una parte de diagnóstico de error que busca información de un resultado de auto-diagnóstico del dispositivo de entrada conectado a cada terminal de entrada de la parte del terminal de salida individualmente; y un dispositivo de tratamiento que maneja un resultado de diagnosis de error de la parte de diagnóstico de error como datos de estado, considera un valor lógico acerca de la presencia o ausencia de cualquier acción bruta del dispositivo de entrada, que es una señal de entrada dada a la parte del terminal de entrada, como indicando la presencia de acción obligatoriamente si el resultado de la diagnosis de error por la parte de diagnóstico de error es la presencia de un error, mientras que si el resultado del diagnóstico de error por la parte de diagnóstico de error es normal, mantiene el valor lógico acerca de la presencia o ausencia de la acción bruta, maneja el valor lógico como los datos de control y transmite los datos de control y los datos de estado a la par a una parte maestra de comunicación del controlador de seguridad.

El estado en el que es activado el dispositivo de entrada basado en la especificación de seguridad cuando existe un peligro corresponde a un estado ACTIVADO en la realización o “BAJO” en el valor lógico de los datos de control. La ausencia de acción corresponde al estado DESACTIVADO en la realización o “ALTO” en el valor lógico de los datos de control. La red entre la unidad esclava de seguridad y el controlador de seguridad ha sido llamada red de campo de seguridad.

De acuerdo con un segundo aspecto, se ha proporcionado un sistema de control en el que un controlador de seguridad basado en la especificación de seguridad que tiene una parte maestra de comunicación y una unidad esclava de seguridad para la seguridad están conectados a través de una red, en que la unidad esclava de seguridad comprende: una parte de terminal de entrada que tiene un terminal de entrada y a la que un dispositivo de entrada basado en la especificación de seguridad es conectado a través del terminal de entrada y recibe un señal acerca de la presencia o ausencia de acción procedente del dispositivo de entrada como una entrada y maneja la señal como una señal de entrada; una parte de diagnóstico de error que busca información de un resultado de auto-diagnóstico de cada dispositivo de entrada conectado a cada terminal de entrada individualmente; y un dispositivo de tratamiento que maneja un resultado de diagnosis de error de la parte de diagnóstico de error como datos de estado, considera un valor lógico acerca de la presencia o ausencia de cualquier acción bruta del dispositivo de entrada introducido por la parte de terminal de entrada como indicando la presencia de la acción obligatoriamente si el resultado de diagnosis de error por la parte de diagnóstico de error es la presencia de un error, mientras que si el resultado de diagnosis de error por la parte de diagnóstico de error es normal, mantiene el valor lógico acerca de la presencia o ausencia de la acción bruta, maneja el valor lógico como los datos de control y transmite los datos de control y los datos de estado a la par a una parte maestra de comunicación del controlador de seguridad, en que el controlador de seguridad recibe un par de datos de los datos de control y de los datos de estado desde el esclavo de seguridad a través de la parte maestra de comunicación y cuando los datos de control recibidos indican un estado acerca de la presencia de la acción, determina si ese estado se origina a partir de que el valor lógico bruto indica la presencia de la acción o porque la presencia de la acción es inducida de forma obligaría debido a un error, basándose en los valores lógicos de los datos de control y datos de estado.

La presencia de acción del dispositivo de entrada basado en la especificación de seguridad corresponde a un estado ACTIVADO en la realización o ”BAJO” en el valor lógico de los datos de control. La ausencia de acción corresponde a un estado DESACTIVADO en la realización o “ALTO” en el valor lógico de los datos de control.

De acuerdo con un tercer aspecto, se ha proporcionado un controlador de seguridad que con un dispositivo de entrada basado en una especificación de seguridad y activado cuando existe un peligro, recibe una señal acerca de la presencia/ausencia de acción como una entrada, se conecta a una unidad de entrada que maneja esa señal como una señal de entrada a través de un bus interno, mientras la unidad CPU introduce una señal de entrada de la unidad de entrada, y ejecuta un control lógico de seguridad basándose en la señal de entrada, en que la unidad de entrada incluye: una parte de terminal de entrada que tiene uno o dos o más terminales de entrada alimentados con una señal de entrada desde el dispositivo de entrada basado en la especificación de seguridad; una parte de diagnóstico de error que busca información de un resultado de auto-diagnosis del dispositivo de entrada conectado a cada terminal de entrada de la parte de terminal de entrada individualmente; y un dispositivo de tratamiento que maneja un resultado de diagnosis de error de la parte de diagnóstico de error como datos de estado, considera un valor lógico acerca de la presencia o ausencia de cualquier acción bruta del dispositivo de entrada, que es una señal de entrada dada a la parte de terminal de entrada, como la presencia de acción obligatoriamente si el resultado de diagnosis de error por la parte de diagnóstico de error es la presencia de un error, mientras que si el resultado de la diagnosis de error por la parte de diagnóstico de error es normal, mantiene el valor lógico acerca de la presencia o ausencia de la acción bruta, maneja el

valor lógico como los datos de control y transmite los datos de control y los datos de estado a la par a la unidad CPU a través del bus interno y la unidad CPU incluye una parte de tratamiento central que con un par de datos de los datos de control y de los datos de estado introducidos desde la unidad de entrada, cuando los datos de control introducidos indican un estado acerca de la presencia de acción, determina si el estado se origina a partir de que el valor lógico bruto indica la presencia de acción o porque la presencia de la acción es inducida obligatoriamente debido a un error, basándose en los valores lógicos de los datos de control y de los datos de estado.

De acuerdo con un cuarto aspecto, se ha proporcionado un dispositivo de entrada de unidad de seguridad que comprende: una parte del terminal de entrada que tiene uno o dos o más terminales de entrada alimentados con una señal de entrada desde un dispositivo de entrada basado en una especificación de seguridad; una parte de diagnóstico de error utilizada para diagnosticar la presencia o ausencia de un error en cada terminal de entrada de la parte del terminal de entrada; un dispositivo de diagnóstico de error para diagnosticar la presencia o ausencia de un error en cada terminal de entrada de la parte del terminal de entrada utilizando la parte de diagnosis de error; y un dispositivo de entrada que convierte una señal de entrada que tiene un valor lógico bruto proporcionada a cada terminal de entrada de la parte de terminal de entrada para controlar datos que tienen un valor lógico cuya seguridad está garantizada por la referencia a un resultado de diagnosis de error con el dispositivo de diagnosis de error.

El dispositivo de entrada contiene una función que emite unos datos de estado que indican el resultado de la diagnosis de error mencionado cuando los datos de entrada son convertidos a los datos de control y los datos de control obtenidos por esa conversión a la par.

Por tanto, cuando el valor lógico de los datos de control es “BAJO”, si se origina porque el valor lógico bruto es “BAJO” o porque “BAJO” es establecido obligatoriamente debido a un error puede ser determinado a partir de un valor lógico de los datos de estado que forman un par con los datos de control.

Con tal estructura, el dispositivo de entrada contiene una función que emite los datos de estado que indican el resultado de la diagnosis de error mencionado cuando la señal de entrada es convertida a los datos de control y los datos de control obtenidos por la conversión a la par. Como consecuencia, el resultado de la diagnosis de error mencionado en el proceso de tratamiento de entrada para generar los datos de control desde la señal de entrada bruta puede ser mencionado por un lado que utiliza los datos de control consiguiendo por ello una variedad de controles de seguridad basándose en los datos de control.

El lado que utiliza los datos de control mencionados aquí no siempre significa un acoplamiento que ha de ser conectado a través de comunicación. Por ejemplo, si la unidad de seguridad correspondiente es un controlador de seguridad o un terminal de seguridad remoto, es un tratamiento principal (tratamiento de ejecución de programa de usuario, tratamiento de servicio de sistema y similar) inherente del dispositivo que ha de ser ejercido dentro de cada uno.

En una realización preferida del dispositivo de entrada antes mencionado, el valor lógico de los datos de estado es “BAJO” cuando existe un error y “ALTO” cuando no existe ningún error.

Con esta estructura, el valor lógico de los datos de estado no cambia a “ALTO” que indica la ausencia de un error hasta que es ajustado a la ausencia de error positivamente confirmando que no existe error realmente, porque el valor lógico que indica ausencia de error es ajustado a un valor lógico (“ELEVADO”) en el lado de energía elevada. Como consecuencia, los datos de estado obtienen una alta fiabilidad, de modo que se impide que los datos de estado que indican ausencia de error, sean enviados por error en un estado no diagnosticado justo después de que la alimentación es ACTIVADA.

De acuerdo con una realización preferida, mientras el dispositivo de entrada refleja un valor lógico bruto proporcionado al terminal de entrada sobre los datos de control como sucede cuando el resultado de la diagnosis de error indica ausencia de error, el dispositivo de entrada establece obligatoriamente el valor lógico de los datos de control a “BAJO” de manera obligatoria independientemente del valor lógico bruto proporcionado al terminal de entrada.

Tal configuración permite que una señal de entrada que tiene un valor lógico bruto proporcionada a cada terminal de entrada de la parte de terminal de entrada sea convertida a datos de control que tienen un valor lógico cuya seguridad está garantizada por referencia al resultado de la diagnosis de error por el dispositivo de diagnóstico de error.

De acuerdo con un quinto aspecto, se ha proporcionado una unidad esclava de seguridad que comprende: una parte de terminal de entrada que tiene uno o dos o más terminales de entrada alimentados con una señal de entrada desde un dispositivo de entrada basado en la especificación de seguridad; una parte de diagnóstico de error utilizada para diagnosticar la presencia o ausencia de un error en cada terminal de entrada de la parte de terminal de entrada; un dispositivo de diagnosis de error para diagnosticar la presencia o ausencia de un error en cada terminal de entrada de la parte del terminal de entrada utilizando la parte de diagnosis de error; y un dispositivo de entrada que convierte una señal de entrada que tiene un valor lógico bruto proporcionada a cada terminal de entrada de la parte del terminal de entrada a datos de control que tienen un valor lógico cuya seguridad está garantizada por referencia a un resultado de

la diagnosis de error con el dispositivo de diagnóstico de error, y emite los datos de control obtenidos por esa conversión con datos de estado que indican el resultado de la diagnosis de error referido a la conversión a la par a la red; y un dispositivo de transmisión para transmitir los datos de control obtenidos desde el dispositivo de entrada con los datos de estado que forman un par con ellos a la red, en el que el acoplamiento de la transmisión a través de la red es capaz de determinar si, cuando el valor lógico de los datos de control recibidos es “BAJO”, se origina porque el valor lógico bruto es “BAJO” o porque “BAJO” es obligatoriamente establecido debido a un error en el terminal a partir de un valor lógico de los datos de estado que forman un par con los datos de control.

Con tal configuración, el dispositivo de entrada contiene una función que emite los datos de estado que indican el resultado de la diagnosis de error mencionado cuando la señal de entrada es convertida a los datos de control con los datos de control obtenidos por la conversión a la par. Como consecuencia, el resultado de la diagnosis de error mencionado en el proceso del tratamiento de entrada para generar los datos de control a partir de una señal de entrada bruta puede ser mencionado porque por un lado utiliza los datos de control (por ejemplo, maestro de seguridad conectado a través de red o similar), de modo que puede conseguirse una variedad de controles de seguridad basándose en los datos de control sobre el lado de recepción a través de la red.

De acuerdo con una realización preferida, el valor lógico de los datos de estado es “BAJO” cuando existe un error y “ALTO” cuando no existe ningún error.

Con esta estructura, el valor lógico de los datos de estado no cambia a “ALTO” indicando la ausencia de un error hasta que es ajustado a la ausencia de error confirmando positivamente que no existe ningún error realmente, porque el valor lógico que indica la ausencia de error es establecido a un valor lógico (“ALTO”) en el lado de energía elevada. Como consecuencia, los datos de estado obtienen una alta fiabilidad, de modo que se impide que los datos de estado que indican la ausencia de error, sean enviados a un acoplamiento de transmisión (por ejemplo, maestro de seguridad conectado a través de la red o similar) por error en un estado no diagnosticado justo después de que la alimentación es ACTIVADA.

De acuerdo con una realización preferida, mientras el dispositivo de entrada refleja un valor lógico bruto proporcionado al terminal de entrada en los datos de control como sucede cuando el resultado de la diagnosis de error indica la ausencia de error, el dispositivo de entrada establece el valor lógico de los datos de control a “BAJO” obligatoriamente de manera independiente del valor lógico bruto proporcionado al terminal de entrada.

Tal configuración permite que una señal de entrada que tiene un valor lógico bruto proporcionado a cada terminal de entrada de la parte del terminal de entrada sea convertida a datos de control que tienen un valor lógico cuya seguridad está garantizada por referencia al resultado de la diagnosis de error por el dispositivo de diagnóstico de error y emitida. Como consecuencia, un acoplamiento de transmisión (maestro de seguridad o similar) conectado a través de comunicación puede adoptar una medida de seguridad apropiada enviando esto al acoplamiento.

De acuerdo con un sexto aspecto, se ha proporcionado un controlador de seguridad que comprende: una parte de terminal de entrada que tiene uno o dos o más terminales de entrada alimentados con una señal de entrada procedente de un dispositivo de entrada basado en una especificación de seguridad; una parte de diagnóstico de error utilizada para diagnosticar la presencia o ausencia de un error en cada terminal de entrada de la parte de terminal de entrada; un dispositivo de diagnosis de error para diagnosticar la presencia o ausencia de un error en cada terminal de entrada de la parte de terminal de entrada utilizando la parte de diagnosis de error; y un dispositivo de entrada que convierte una señal de entrada que tiene un valor lógico bruto proporcionada a cada terminal de entrada de la parte de terminal de entrada a datos de control que tienen un valor lógico cuya seguridad está garantizada por referencia a un resultado de diagnosis de error con el dispositivo de diagnosis de error, y emite los datos de control obtenidos por esa conversión con datos de estado que indican el resultado de la diagnosis de error referido a la conversión en par a la red; y un dispositivo de transmisión para transmitir los datos de control obtenidos desde el dispositivo de entrada con los datos de estado formando un par con ellos a la red, en el que el acoplamiento de la transmisión a través de la red es capaz de determinar si, cuando el valor lógico de los datos de control recibidos es “BAJO”, se origina porque el valor lógico es “BAJO” o porque “BAJO” es establecido obligatoriamente debido a un error en el terminal a partir de un valor lógico de los datos de estado que forman un par con los datos de control.

Con tal configuración, el dispositivo de entrada contiene una función que emite los datos de estado que indican el resultado de la diagnosis de error referido a cuando la señal de entrada es convertida a los datos de control con los datos de control obtenidos por la conversión en par. Como consecuencia, el resultado de la diagnosis de error referido al proceso de tratamiento de entrada para generar los datos de control a partir de una señal de entrada bruta puede ser referido por un lado a que utiliza los datos de control (por ejemplo, un maestro de seguridad conectado a través de la red o similar), de modo que puede conseguirse una variedad de controles basándose en los datos de control en el lado de recepción a través de la red.

De acuerdo con una realización preferida, el valor lógico de los datos de estado es “BAJO” cuando existe un error y “ALTO” cuando no existe ningún error.

Con esta estructura, el valor lógico de los datos de estado no cambia a “ALTO” que indica la ausencia de un error hasta que es ajustado a la ausencia de error positivamente confirmando que no existe ningún error realmente, porque el valor lógico que indica la ausencia de error es ajustado a un valor lógico (“ALTO”) en el lado de energía elevada. Como consecuencia, los datos de estado obtienen una alta fiabilidad, de modo que los datos de estado que indican la ausencia de error se impide que sean enviados a un acoplamiento de transmisión (por ejemplo, un maestro de seguridad conectado a través de la red o similar) por error en un estado no diagnosticado justo después de que la alimentación es ACTIVADA.

De acuerdo con una realización preferida, mientras el dispositivo de entrada refleja un valor lógico bruto proporcionado al terminal de entrada en los datos de control como sucede cuando el resultado de la diagnosis de error indica ausencia de error, el dispositivo de entrada establece el valor lógico de los datos de control a “BAJO” obligatoriamente de manera independiente del valor lógico bruto proporcionado al terminal de entrada.

Tal configuración permite que una señal de entrada que tiene un valor lógico bruto proporcionado a cada terminal de entrada de la parte de terminal de entrada sea convertida a datos de control que tienen un valor lógico cuya seguridad está garantizada por referencia al resultado de la diagnosis de error y emitida. Como consecuencia, un acoplamiento de transmisión (maestro de seguridad o similar) conectado a través de comunicación puede adoptar una medida de seguridad apropiada enviando esto al acoplamiento.

De acuerdo con un séptimo aspecto, se ha proporcionado un sistema de control de seguridad en el que un controlador de seguridad que funciona como un maestro de seguridad y una unidad de seguridad remota que funciona como un esclavo de seguridad están conectados a través de una red, en que la unidad de seguridad remota que comprende una parte de terminal de entrada tiene uno o dos o más terminales de entrada alimentados con una señal de entrada procedente de un dispositivo de entrada basado en una especificación de seguridad; una parte de diagnóstico de error utilizada para diagnosticar la presencia o ausencia de un error en cada terminal de entrada de la parte del terminal de entrada; un dispositivo de diagnóstico de error para diagnosticar la presencia o ausencia de un error en cada terminal de entrada de la parte del terminal de entrada que utiliza la parte de diagnosis de error; y un dispositivo de entrada que convierte una señal de entrada que tiene un valor lógico bruto proporcionada a cada terminal de entrada de la parte de terminal de entrada a datos de control que tienen un valor lógico cuya seguridad está garantizada por referencia a un resultado de la diagnosis de error con el dispositivo de diagnosis de error, y emite los datos de control obtenidos por esa conversión con datos de estado que indican el resultado de la diagnosis de error referida a la conversión en par a la red; y un dispositivo de transmisión para transmitir los datos de control obtenidos desde el dispositivo de entrada con los datos de estado que forman un par con ellos a la red, en el que el controlador de seguridad incluye un dispositivo de recepción para recibir datos de control y datos de estado que forman un par con ellos desde la red y un dispositivo reproductor de datos de entrada para reproducir datos de entrada basándose en los datos de control y los datos de estado que forman un par con ellos.

Con tal configuración, el lado de la unidad de seguridad remota es provisto con un dispositivo de transmisión que tiene una función para transmitir los datos de control obtenidos desde el dispositivo de entrada y los datos de estado que forman un par con ellos a la red y por otro lado, el lado del controlador de seguridad es provisto con un dispositivo de recepción para recibir los datos de control y los datos de estado que forman un par con ellos desde la red y un dispositivo reproductor de datos de entrada para reproducir datos de entrada basándose en los datos de control y los datos de estado que forman un par con ellos. Como consecuencia, el resultado de la diagnosis del lado de la unidad de seguridad remota puede ser utilizado efectivamente en el lado del control de seguridad, consiguiendo por ello un control de seguridad más fiable.

Como se ha descrito previamente, se prefiere que el valor lógico de los datos de estado sea “BAJO” cuando existe un error y “ALTO” cuando no existe ningún error. Además, preferiblemente, mientras el dispositivo de entrada refleja un valor lógico bruto proporcionado al terminal de entrada en los datos de control como sucede cuando el resultado de la diagnosis de error indica ausencia de error, el dispositivo de entrada establece el valor lógico de los datos de control a "BAJO" de manera obligatoria independientemente del valor lógico bruto proporcionado al terminal de entrada.

El presente invento permite que el resultado de la diagnosis de error referido en el proceso de tratamiento de entrada para generar los datos de control a partir de una señal de entrada bruta sea referido en un lado que utiliza los datos de control en la unidad de seguridad tales como el maestro de seguridad y el esclavo de seguridad consiguiendo así una variedad de controles de seguridad basándose en los datos de control.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La fig. 1 es un diagrama de configuración de un sistema de control de seguridad;

La fig. 2 es un diagrama de bloques que muestra la estructura de hardware interna del esclavo de seguridad de entrada;

La fig. 3 es un diagrama de bloques que muestra la estructura de hardware interna del controlador de seguridad (maestro de seguridad);

La fig. 4 es un diagrama explicativo de temporización de comunicación entre un puesto maestro y un puesto esclavo;

La fig. 5 es un diagrama de flujo general que muestra un contenido de tratamiento del aparato del presente invento;

La fig. 6 es un diagrama de flujo que muestra el detalle de tratamiento inicial;

La fig. 7 es un diagrama de flujo que muestra el detalle de tratamiento de entrada;

La fig. 8 es un diagrama de tiempos que muestra una transición de estado cuando se ha determinado que existe un error como un resultado de diagnosis en el tratamiento inicial (en el caso en que el estado es “ALTO” = “normal”);

La fig. 9 es un diagrama de tiempos que muestra una transición de estado cuando se ha determinado que existe un error como un resultado de diagnosis después de que se haya iniciado la operación (en el caso en que el estado es “ALTO” = “normal”);

La fig. 10 es un diagrama de tiempos que muestra una transición de estado cuando se ha determinado que existe un error como un resultado de diagnosis después de que se haya iniciado la operación (en el caso en el que el estado es “BAJO” = “normal”); y

La fig. 11 es un diagrama para explicar un problema en el sistema de control de seguridad de tipo maestro/esclavo.

DESCRIPCIÓN DETALLADA DE LAS REALIZACIONES PREFERIDAS

A continuación, se describirá con detalle la realización preferida del sistema de control de seguridad del presente invento con referencia a los dibujos adjuntos.

La fig. 1 muestra un diagrama de estructura del sistema de control de seguridad del presente invento. Como se ha mostrado en la misma figura, este sistema de control de seguridad está constituido conectando una pluralidad de esclavos 1 de seguridad con un controlador 2 de seguridad a través de la red 3. Como el esclavo 1 de seguridad de este ejemplo, se ha indicado un esclavo 1A de seguridad de entrada, un esclavo 1B de seguridad de salida y un esclavo 1C de seguridad de I/O. A continuación, un dispositivo de entrada 4 está conectado al esclavo 1A de seguridad de entrada, un dispositivo de salida 5 está conectado al esclavo 1B de seguridad de salida y el dispositivo de salida 4 y el dispositivo de salida 5 están conectados al esclavo 1C de seguridad de I/O.

Estos dispositivos de entrada 4 y dispositivo de salida 5 han sido diseñados basándose en una especificación de seguridad. El dispositivo de entrada es, por ejemplo, un interruptor de parada de emergencia, una cortina o persiana, un interruptor de puerta, o un interruptor de 2 manos y el dispositivo de salida es, por ejemplo, un relé o contactor de seguridad. Estos dispositivos son los mismos que los convencionales.

El esclavo 1A de seguridad de entrada, el esclavo 1B de seguridad de salida y el esclavo 1C de seguridad de I/O tienen una función de ejecutar la acción de comunicación a la función maestra de comunicación, una función de ejecutar la acción de entrada a un dispositivo de entrada conectado, una función de ejecutar una acción de salida a un dispositivo de salida conectado y una función de ejecutar la auto-diagnosis relativa a los terminales de entrada y salida como una unidad esclava de un controlador programable ordinario (en lo sucesivo denominado como PLC. Mientras tanto, un PLC ordinario se refiere a un controlador utilizado para un propósito ordinario y no incluye un controlador de seguridad). La función de auto-diagnóstico proporcionada en cada esclavo de seguridad I/O tiene una función de diagnosticar si su propia parte de terminal de entrada tiene algún error y puede ejecutar auto-diagnosis acerca de distintas funciones tales como la función de comunicación y la auto-diagnosis acerca de si el cableado entre el terminal de I/O y el dispositivo de I/O está cortocircuitado o roto. Como otro ejemplo, la función de auto-diagnóstico puede ser una función en la que con un terminal de salida de prueba diferente del terminal de I/O previsto en cada esclavo de seguridad de I/O, una señal es enviada apropiadamente desde el terminal de salida de prueba a un dispositivo de I/O correspondiente y se comprueba si la señal es enviada de nuevo apropiadamente o no a través del dispositivo de entrada correspondiente de modo que vigile si la entrada correspondiente es normal o no.

El controlador 2 de seguridad tiene una variedad de funciones de auto-diagnóstico así como una función similar a un cuerpo principal incorporado de CPU de un PLC ordinario. En este ejemplo, el controlador 2 de seguridad incluye una unidad de entrada 2A y una unidad de salida 2B, que están conectadas entre sí. Estas unidades son a veces denominadas unidad local. La unidad de entrada 2A y la unidad de salida 2B están conectadas a un bus interno del controlador de seguridad de modo que se ejecute la comunicación por bus con la unidad CPU. A continuación, un dispositivo de entrada 4 diseñado basándose en una especificación de seguridad es conectado a la unidad de entrada 2A y un dispositivo de salida 5 diseñado basándose en una especificación es conectado a la unidad de salida 2B.

La fig. 2 muestra un diagrama de bloques que indica la estructura del hardware interno del esclavo 1A de seguridad de entrada. Como se ha mostrado en la misma figura, el esclavo 1A de seguridad de entrada incluye una parte 101 del terminal de entrada, una parte 102 de diagnóstico de error del terminal, una parte 103 de tratamiento central y una parte 104 de transmisión de datos.

La parte 101 del terminal de entrada tiene uno o dos o más terminales de entrada (terminal 1, terminal 2, … terminal n) a los que se proporciona una señal de salida desde el dispositivo de entrada 4 diseñado basándose en la especificación de seguridad. Cada terminal está constituido por uno o dos o más terminales. El dispositivo de entrada está diseñado sobre la especificación de seguridad y más específicamente, se ha empleado el interruptor de aplicación de seguridad. El interruptor de parada de emergencia de la aplicación de seguridad es apretado cuando ocurre un estado peligroso, de modo que su punto de contacto es abierto a DESACTIVADO y una señal BAJA es emitida. Por el contrario, en un estado de seguridad, el interruptor no es apretado de modo que su punto de contacto es cerrado a la señal de ACTIVADO (señal ALTA). De esta manera, el interruptor de la aplicación de seguridad está diseñado a una salida BAJA cuando ocurre un estado peligroso.

La parte 102 de diagnóstico de error del terminal es utilizada para diagnosticar la presencia o ausencia de un error en cada terminal de entrada (terminal 1, terminal 2, ... terminal n) de la parte 101 del terminal de entrada e incluye una variedad de circuitos de auto-diagnóstico como se ha descrito, por ejemplo, en la Solicitud de Patente Japonesa abierta al público nº 2004-297997. Los errores de cada terminal de entrada mencionados aquí incluyen no sólo errores en los dispositivos de entrada conectados al terminal sino también un error del terminal y otros distintos errores. La parte 102 de diagnóstico de error del terminal puede ser construida para diagnosticar un error en cada dispositivo de entrada introduciendo una señal de anormalidad como resultado de la auto-diagnosis, si el dispositivo de entrada tiene la función de auto-diagnóstico, a través de cada terminal. Además, la parte 102 de diagnóstico de error del terminal puede ser construida para diagnosticar un error en cada terminal individualmente si hay una anormalidad en el cableado entre el terminal y el dispositivo de entrada. En conclusión, puede adoptarse cualquier estructura si puede obtener un estado de presencia o ausencia de error individualmente para un terminal de un sistema. Mientras tanto, el esclavo 1B de seguridad de salida puede ser construido para detectar un estado de presencia o ausencia de error individualmente para un terminal de salida de un sistema. Por ejemplo, puede ser construido para obtener un resultado de auto-diagnosis de un dispositivo de salida en sí mismo si el dispositivo de salida tiene la función de auto-diagnóstico o detecta la rotura o cortocircuito de cableado entre el terminal y el dispositivo de salida. El esclavo 1C de seguridad de I/O puede ser construido para detectar un estado de presencia o ausencia de error individualmente para un terminal de entrada o un terminal de salida de un sistema.

La parte 103 de tratamiento central incluye un microprocesador, ROM, RAM y similar con el fin de controlar completamente al esclavo 1A de seguridad de entrada. La parte 104 de transmisión de datos es utilizada para transmitir datos de control que serán descritos más tarde para el controlador 2 de seguridad a través de la red 3. En caso del esclavo 1C de seguridad de I/O, su parte 104 de transmisión de datos es una parte 104 de transmisión de datos que tiene ambas funciones para transmitir y recibir datos. En caso del esclavo 1B de seguridad de salida, es una parte 104 de transmisión de datos que tiene una función de recepción de datos.

La fig. 3 muestra un diagrama de bloques que indica la estructura del hardware del terminal del controlador 2 de seguridad. Como se ha indicado en la misma Figura, el maestro 2 de seguridad incluye una parte 2A de terminal de entrada, una parte 202A de diagnóstico de error del terminal, una parte 2B de terminal de salida, una parte 202B de diagnóstico de error del terminal, una parte 203 de tratamiento central y una parte 204 de transmisión/recepción de datos.

La parte 2A del terminal de entrada está provista con uno o dos o más terminales de entrada (terminal 1, terminal 2, … terminal m) que es alimentada con una señal de entrada procedente del dispositivo de entrada 4 designado sobre la especificación de seguridad.

La parte 202A de diagnóstico de error del terminal es utilizada para diagnosticar la presencia o ausencia de error en cada terminal de entrada (terminal 1, terminal 2, … terminal m) de la parte 2A del terminal de entrada y constituida de distintas clases de circuitos de diagnóstico de error como el esclavo de seguridad antes mencionado. Un objeto para la diagnosis de error es no sólo el dispositivo de entrada 4 sino también la propia parte 2A del terminal de entrada y otras distintas clases de sujetos. Es decir, esta parte 202A de diagnóstico de error del terminal diagnostica si existe o no algún error en cada terminal de entrada buscando en un resultado de auto-diagnóstico de un dispositivo de entrada correspondiente a cada terminal. Diagnostica cada terminal individualmente acerca de si existe o no alguna anormalidad en el cableado entre el terminal de entrada y el dispositivo de entrada. En conclusión, diagnostica sobre un estado de presencia o ausencia de error para cada terminal de un sistema.

La parte 2B del terminal de salida está provista con uno o dos o más terminales de salida (terminal 1, terminal 2, … terminal m) que proporciona una señal de salida al dispositivo de salida 5 diseñado basándose en la especificación de seguridad.

La parte 202B de diagnóstico de error del terminal es utilizada para diagnosticar la presencia o ausencia de un error en cada terminal de salida (terminal 1, terminal 2, … terminal m) de la parte 2B de terminal de salida. Si un dispositivo de salida correspondiente a cada terminal tiene función de auto-diagnóstico, esta parte 202B de diagnóstico de error del terminal busca en cada resultado de auto-diagnosis desde cada dispositivo de modo que diagnostique cada dispositivo de salida para algún error. Además, diagnostica cada terminal individualmente para ver si existe algún error en el cableado entre el terminal de salida y el dispositivo de salida. Es decir, diagnostica si cada terminal de un sistema individualmente para comprobar si existe algún error (estado) como el sistema de entrada. Es decir, la parte de diagnóstico de error del terminal en el lado del esclavo de seguridad y la parte de diagnóstico de error del terminal en el lado del controlador de seguridad puede ser así construida con la misma función.

La parte 203 de tratamiento central está constituida principalmente de un microprocesador para controlar la operación completa del controlador 2 de seguridad. Está provista con ROM; RAM (no mostrados) y similares externamente. La parte de tratamiento central del controlador 2 de seguridad incluye una función de operación lógica que utiliza un programa de usuario, una función de control de I/O conectada al controlador de seguridad, función de auto-diagnóstico, y la función para ejecutar comunicación de red con el esclavo de seguridad de entrada y similar. La parte 204 de transmisión/recepción de datos es utilizada para ejecutar la transmisión/recepción de unos datos de protocolo de comunicación específico entre el esclavo 1A de seguridad de entrada, el esclavo 1B de seguridad de salida y el esclavo 1C de seguridad de I/O.

A continuación, se ha mostrado esquemáticamente en la fig. 4 un diagrama explicativo de temporización de comunicación entre el puesto maestro y el puesto esclavo. Como se ha indicado en la misma figura, el puesto maestro y el puesto esclavo tienen sus propios ciclos de control inherentes y los datos son transmitidos y recibidos entre estos en una temporización de transmisión asíncrona con un ciclo de ejecución repetida del controlador 2 de seguridad. El lado del controlador de seguridad almacena datos recibidos en una memoria tampón de comunicación (no mostrada) temporalmente y refresca su información de almacenamiento en una memoria de datos de operación durante la ejecución repetida. En este ejemplo, “datos de control” y “datos de estado”, que serán descritos más tarde, están sido incluidos en esos datos.

A continuación, se ha mostrado en la fig. 5 un diagrama de flujo general que muestra el contenido de tratamiento del dispositivo del presente invento. El tratamiento completo del dispositivo del invento está ampliamente dividido al tratamiento inicial que ha de ser ejecutado justo después de que se active la alimentación (operación 501), el tratamiento de entrada (operación 502) que ha de ser ejecutado como un tratamiento regular que sigue al tratamiento inicial y al tratamiento principal (operación 503) que ha de ser ejecutado siguiendo al tratamiento de entrada (operación 503).

El contenido del tratamiento principal (operación 503) difiere dependiendo de si el dispositivo del presente invento es conseguido como el esclavo 1A de seguridad de entrada, el esclavo 1C de seguridad de I/O o el maestro 2 de seguridad del controlador de seguridad. En caso del esclavo 1 de seguridad, una acción de introducir una señal desde el dispositivo de entrada corresponde al tratamiento de entrada. A continuación, una acción de comunicar a la función maestra de comunicación del controlador 2 de seguridad, una acción de emitir datos de control introducidos por comunicación al dispositivo de salida y una acción de ejecutar la auto-diagnosis acerca de cada terminal corresponde al tratamiento principal. En caso del controlador 2 de seguridad, una acción de refrescar una señal procedente de la unidad de entrada o del esclavo de seguridad corresponde al tratamiento de entrada y una acción de emitir un resultado de operación al esclavo de seguridad a través del tratamiento de operación lógica y comunicación y una acción de ejecutar auto-diagnosis corresponde al tratamiento principal.

A continuación, se ha mostrado en la fig. 6 un diagrama de flujo que indica el detalle del tratamiento inicial de la parte de tratamiento central del lado del controlador de seguridad. El tratamiento inicial de la parte de tratamiento central del lado del esclavo de seguridad es el mismo y toma la operación del diagrama de flujo mostrada en la fig. 6. La descripción es aquí común para ellos. Si el tratamiento es iniciado en la misma figura, en la operación 601, el establecimiento inicial con datos de control = DESACTIVADO (“BAJO”) y datos de estado = DESACTIVADO (“BAJO”) es realizado para cada terminal. El tratamiento de ajuste inicial es realizado para todos los terminales 101 equipados en el esclavo 1 de seguridad y todos los terminales 2A, 2B equipados en el controlador 2 de seguridad por separado.

En una operación subsiguiente 602, el tratamiento diagnóstico de diagnosticar un error en cada terminal de entrada de la parte de terminal de entrada que utiliza la parte de diagnóstico de error (parte 102 de diagnóstico de error del terminal en caso del esclavo de seguridad y parte 202A de diagnóstico de error de terminal en caso del maestro de seguridad) para cada terminal es ejecutado por separado. Como se ha descrito previamente, este tratamiento de diagnóstico de error diagnostica no sólo un error en el dispositivo de entrada 4 sino también un error en cada terminal y una variedad de errores.

En la operación 603, se determina si existe un error o no basándose en un resultado del tratamiento de diagnóstico (operación 602). Si se ha determinado que existe un error, el procedimiento prosigue a la operación 604 y si se ha determinado que no existe error, el procedimiento prosigue a la operación 605.

En la operación 604, los datos de control = DESACTIVADOS (“BAJOS”) y los datos de estado = DESACTIVADOS (“BAJOS”) son establecidos para un terminal de entrada que se ha determinado que tiene un error. Los datos de estado = DESACTIVADOS significa que existe un error. Por el contrario, en la operación 605, los datos de control inicial = DESACTIVADOS (“BAJOS”) y los datos de estado = ACTIVADOS (“ALTOS”) son establecidos para un terminal de entrada que se ha determinado que no tiene ningún error. Los datos de estado = ACTIVADOS significa que no existe ningún error.

Como un resultado de ejecutar el tratamiento inicial de este modo, cuando se ha iniciado un tratamiento regular subsiguiente, el estado de los datos es DESACTIVADO debido a que cada dispositivo de entrada no es operado en la etapa inicial independientemente de si existe un error o no. Así, el valor lógico de los datos de control es DESACTIVADO (“BAJO”). Si existe un error o no en el dispositivo de entrada y si existe un error o no en el cableado (cortocircuito, desconexión y similar) se diagnostica para cada terminal y el valor lógico de los datos de estado que le acompañan es establecido a DESACTIVADO (“BAJO”) cuando existe un error y ACTIVADO (“ALTO”) cuando no existe error. Así, un significado del valor lógico DESACTIVADO (“BAJO”) de los datos de control justo después de que empiece la operación puede ser notificado a un control subsiguiente haciendo referencia al valor de estos datos de estado. En caso del esclavo 1 de seguridad, los datos de control inicial que se refieren a la operación de ACTIVADO/DESACTIVADO de cada dispositivo de entrada y los datos de estado que son un resultado de diagnóstico de cada terminal de entrada pueden ser transmitidos en combinación apropiadamente al controlador 2 de seguridad como un destino de transmisión. En caso de la unidad de entrada 2A del controlador de seguridad, los datos de control y los datos de estado de cada terminal de entrada pueden ser transmitidos apropiadamente a la unidad CPU del controlador 2 de seguridad como un destino de transmisión.

Adicionalmente, debido a que “no hay error” corresponde a “ALTO” en un lado de energía elevada del valor lógico de los datos de estado, los datos de estado no indican que no hay error excepto cuando se ha determinado que no existe error como un resultado del tratamiento de diagnóstico (operación 602), de modo que los datos de estado indican una alta fiabilidad.

Se ha mostrado en la fig. 7 un diagrama de flujo que indica el detalle del tratamiento de entrada. Esta fig. 7 indica el tratamiento en el controlador de seguridad y el tratamiento en el esclavo de seguridad. Es decir, ambos ejecutan una operación común. Cuando el tratamiento es iniciado en la misma figura, en la operación 701, se ejecutan la lectura de los datos de entrada y el tratamiento de diagnóstico, lo que representan una condición operativa real de un dispositivo de entrada conectado. El contenido de este tratamiento de diagnóstico es el mismo que el tratamiento de diagnóstico (operación 602) descrito con referencia a la fig. 6 previamente y si existe un error o no es comprobado introduciendo una señal de un resultado de la auto-diagnosis en el lado del dispositivo de entrada o si existe un error o no en el cableado es diagnosticado. Las operaciones necesarias para que el esclavo introduzca una señal del resultado de la auto-diagnosis realizada por el dispositivo de entrada conectado al esclavo y para que el controlador de seguridad introduzca una señal del resultado de la auto-diagnosis realizada por el dispositivo de entrada conectado al controlador de seguridad. Mientras tanto, si existe un error o no en el cableado es ejecutado por la parte 102 de diagnóstico de error del terminal en caso del esclavo 1A de seguridad y por la parte 202A de diagnóstico de error del terminal en caso del controlador 2 de seguridad.

En la operación 702, se ha determinado si existe un error o no basándose en un resultado del tratamiento de diagnóstico. Cuando la parte 202A de diagnóstico de error del terminal recibe un señal del resultado del auto-diagnóstico del lado del dispositivo de entrada como una entrada o detecta la presencia o ausencia de un error en el cableado, el controlador 2 de seguridad determina que existe un error. Cuando la parte 102 de diagnóstico de error del terminal detecta que una señal del resultado del auto-diagnóstico en el lado del dispositivo de entrada es introducida o existe un error en el cableado, el esclavo 1 de seguridad determina que existe un error. Si se ha determinado que existe un error, el procedimiento prosigue a la operación704 y si se ha determinado que no existe ningún error, el procedimiento prosigue a la operación703.

En la operación 704, se establece que los datos de control = DESACTIVADO (“BAJO”) y los datos de estado = DESACTIVADO (“BAJO”). Los datos de control = DESACTIVADO (“BAJO”) significa que el estado de los datos es DESACTIVADO obligatoriamente como resultado de diagnosticar que existe un error y los datos de estado = ACTIVADO (“BAJO”) significa que se ha diagnosticado que existe un error. En la operación 703, se determina si el valor lógico de una señal de entrada en una condición operativa real leída desde el terminal de entrada es ACTIVADO (“ALTO”) o DESACTIVADO (“BAJO”). Debido a que el dispositivo de entrada no es hecho funcionar en la etapa inicial, sus estados de datos son mantenidos todos DESACTIVADOS y sin embargo, el estado ACTIVADO/DESACTIVADO es determinado basándose en la condición operativa real o condición de control de cada dispositivo de entrada después de eso.

Si se ha determinado que los datos de control = DESACTIVADO (“BAJO”), el procedimiento prosigue a la operación 705 y si se ha determinado que los datos de control = ACTIVADO (“ALTO), el procedimiento prosigue a la operación 706.

En la operación 705, se establece que los datos de control = DESACTIVADOS (“BAJOS”) y los datos de estado = ACTIVADOS (“ALTOS”). Los datos de estado = ACTIVADOS (“ALTOS”) significa que se ha diagnosticado que no existe error y los datos de control = DESACTIVADOS significa que las condiciones de funcionamiento y control del dispositivo de entrada están DESACTIVADAS. Por el contrario, se establece que los datos de control = ACTIVADOS (“ALTOS”) y los datos de estado = ACTIVADOS (“ALTOS”) en la operación 706. Los datos de estado = ACTIVADOS (“ALTOS”) significa que se ha diagnosticado que no existe error y los datos de control = ACTIVADOS (“ALTOS”) significa que las condiciones de funcionamiento y control reales del dispositivo de entrada están ACTIVADAS. Las operaciones 704, 705, 706 son ejecutadas por la parte 103 de tratamiento central en caso del esclavo 1A de seguridad y por la parte 203 de tratamiento central en caso del controlador 2 de seguridad.

En el tratamiento de entrada antes descrito, cuando un resultado de diagnosis de error indica que no hay error, un valor lógico bruto (es decir, estado ACTIVADO y estado DESACTIVADO que son condición de operación real o condición de control) dado al terminal de entrada del esclavo 1A de seguridad o al controlador 2 de seguridad es reflejado sobre los datos de control cuando hay. Sin embargo, si el resultado de la diagnosis de error indica que existe un error, el valor lógico de los datos de control de un dispositivo correspondiente es establecido a "BAJO" de manera obligatoria independientemente del valor lógico bruto dado al terminal de entrada.

Adicionalmente, los datos de control individuales para el dispositivo de entrada obtenidos de este modo son siempre proporcionados con los datos de estado, que es un punto importante, y esos datos de control son finalmente emitidos a la par. Mientras tanto, la salida mencionada aquí significa que los datos son almacenados en una memoria tampón apropiada (no mostrado). Como resultado, es posible distinguir automáticamente qué terminal de entrada tiene un error mientras sus datos de control son DESACTIVADOS obligatoriamente y qué terminal de entrada no tiene error mientras sus datos de control son realmente DESACTIVADOS.

Volviendo al diagrama de flujo de la fig. 5, en el tratamiento principal (operación 503), un tratamiento inherente es ejecutado dependiendo de si el dispositivo del presente invento es un esclavo 1A de seguridad, un esclavo 1C de seguridad de I/O o un maestro 2 de seguridad como se ha descrito previamente.

Por ejemplo, si el dispositivo del invento es conseguido como el esclavo 1A de seguridad de entrada, en el tratamiento principal (operación 503), los datos de control obtenidos en el tratamiento de entrada (operación 502) y los datos de estado son transmitidos a un destino de transmisión predeterminado (por ejemplo, maestro 2 de seguridad) a la par. Si los datos de control y los datos de estado son transmitidos a la par, el maestro 2 de seguridad que recibe estos puede interpretar el significado de los datos de control basándose en el contenido de los datos de estado unidos a los datos de control.

Más específicamente, incluso si el valor lógico de los datos de control es DESACTIVADO ("BAJO)", puede determinarse si eso es un reflejo de una señal de entrada bruta o está causado por el tratamiento de establecimiento obligatorio ejecutado debido a que tiene lugar un error en el terminal de entrada, basándose en el valor lógico de los datos de estado, haciendo por ello posible adoptar una acción apropiada para restauración del sistema.

Mientras tanto, el tratamiento en caso de que el dispositivo del presente invento es un esclavo 1C de seguridad de I/O es igual al caso del esclavo 1A de seguridad de entrada descrito previamente si se habla de su entrada solamente y por ello su descripción es omitida. En el caso del esclavo 1C de seguridad de I/O y el esclavo 1B de seguridad de salida, sus terminales de salida pueden estar provistos con una estructura para diagnosticar un error en el dispositivo de salida o un error (cortocircuito, desconexión y similar) en el cableado conectado al terminal de salida. Los datos de control y los datos de estado de cada terminal de entrada pueden ser transmitidos a un destino de transmisión predeterminado a la par y al mismo tiempo, los datos de estado del terminal de salida pueden ser transmitidos por separado. Debido a que los datos de salida del terminal de salida son transmitidos desde el controlador de seguridad pero no transmitidos por el esclavo de seguridad, son transmitidos por separado sin acompañar a los datos de salida.

Por otro lado, en caso de que el dispositivo del presente invento es el controlador 2 de seguridad (maestro de seguridad), como el tratamiento principal (operación 503), una señal de entrada obtenida a través de la unidad de entrada 2A es convertida a datos de control mediante el tratamiento de entrada y a continuación transmitida a la unidad CPU del otro controlador 2 de seguridad (no mostrado) con los datos de estado. Después de eso, se comprenderá fácilmente por los expertos en la técnica que el tratamiento original de la unidad CPU de seguridad (por ejemplo, tratamiento de ejecución del programa de usuario) es ejecutado después de eso.

En caso de que el dispositivo del presente invento es el controlador 2 de seguridad, los datos de control y los datos de estado a la par pueden ser transmitidos no solamente a su propia unidad CPU sino también a otro controlador de seguridad. Dentro del propio controlador, los datos de control pueden ser utilizados para ejecución del programa de usuario después de que el contenido de los datos de control es certificado basándose en aquellos, mejorando por ello la fiabilidad de ejecución del programa de usuario. Desde luego, si los datos de control son transmitidos a otro controlador de seguridad también, pueden ser utilizados para ejecución del programa de usuario sobre el controlador de seguridad en ese destino de transmisión mejorando por ello la fiabilidad de ejecución del programa de usuario.

A continuación, la fig. 8 muestra un gráfico de tiempos que muestra la transición de estado cuando se ha diagnosticado que existe un error en la diagnosis en el instante del tratamiento inicial (caso de estado "ALTO" = normal). El diagrama de flujo nº 1 y el diagrama de flujo nº 2 en la misma figura indican números correspondientes del diagrama de flujo de la fig. 6.

Si se ha diagnosticado que existe un error en la diagnosis en el momento del tratamiento inicial como se ha indicado en la misma figura, el valor de los datos de control es mantenido obligatoriamente en "BAJO" que está en el lado de seguridad independientemente de cuál es el valor lógico de los datos de entrada brutos y el valor de los datos de estado es mantenido obligatoriamente en "ALTO" indicando que existe un error. Así, los datos de estado nunca son activados a "ALTO" indicando una condición normal justo después de que la alimentación sea ACTIVADA.

A continuación, un gráfico de tiempos (en el caso en el que el estado "BAJO" = normal) que indica la transición de estado en el caso en que se ha diagnosticado que existe un error en la diagnosis después de que la operación comience esta mostrado en la fig. 9. Mientras tanto, el diagrama de flujo nº 1, el diagrama de flujo nº 3, el diagrama de flujo nº 6, el diagrama de flujo nº 5 y el diagrama de flujo nº 4 en la misma figura indican la relación con las operaciones en las figs. 7, 8.

Si se ha diagnosticado que no existe error en la diagnosis después de que la operación comience como es evidente por la misma figura, el valor lógico de los datos de control cambia de manera correspondiente al valor lógico de los datos de entrada brutos. Por el contrario, el valor lógico de los datos de estado es mantenido en el estado "BAJO" solamente en un período en el que se ha determinado que no existe error. Así, después de que en el valor lógico de los datos de control es establecido "BAJO" obligatoriamente como resultado de la diagnosis de que existe un error en el instante t5, el valor lógico de los datos de estado es también "BAJO" y así, es posible confirmar que este BAJO no es producido por la operación real o control de los datos de entrada brutos sino que es establecido "BAJO" obligatoriamente como resultado de la diagnosis de que existe un error en el instante t5 basándose en esos dos datos. Adicionalmente, de acuerdo con este ejemplo, incluso si los datos de control son "BAJO" justo después de que sea activada la alimentación, es posible confirmar que el tratamiento de diagnóstico de error acerca de esos datos de control no ha sido terminado basándose en un hecho de que los datos de estado son también "BAJOS".

A continuación, un gráfico de tiempos que indica la transición de estado cuando se ha diagnosticado que existe un error después de que comience la operación (caso en que el estado "ALTO" = normal) está mostrado en la fig. 10.

Como se ha indicado en la misma figura, de acuerdo con este ejemplo, los datos de estados son mantenidos en "BAJO" independientemente de que sea alrededor del instante t2 cuando se ha diagnosticado que no existe error en el tratamiento inicial y así, si los datos de control "BAJO" justo después de que la alimentación haya sido activada han sufrido diagnosis para un error no pueden ser determinados. En este punto, la fiabilidad de los datos de control puede decirse que es baja.

Como se ha descrito previamente, el sistema de control de seguridad de esta realización está constituido combinando el controlador 2 de seguridad que funciona como el maestro de seguridad y la unidad (1A, 1C) de seguridad remota que funciona como el esclavo de seguridad a través de la red 3.

La unidad (1A, 1C) de seguridad remota comprende una parte 101 de terminal de entrada que tiene uno o dos o más terminales de entrada (terminal 1, terminal 2,... terminal m) alimentado con una señal de entrada procedente del dispositivo de entrada 4 basado en la especificación de seguridad, una parte 102 de diagnóstico de error de terminal utilizado para diagnosticar la presencia o ausencia de un error en cada terminal de entrada (terminal 1, terminal 2,... terminal m) de la parte 101 de terminal de entrada, un dispositivo de diagnóstico de error (operaciones 602, 701) para diagnosticar la presencia o ausencia de un error en cada terminal de entrada de la parte de terminal de entrada que utiliza la parte 102 de diagnóstico de error de terminal, un dispositivo de entrada (operaciones 701-706) que tiene una función de convertir una señal de entrada que tiene un valor lógico bruto proporcionada a cada terminal de entrada de la parte de terminal de entrada a datos de control que tienen un valor lógico cuya seguridad está garantizada con referencia a un resultado de diagnosis de error por el dispositivo de diagnóstico de error y emitir los datos de control obtenidos por esa conversión a la par con los datos de estado que indican el resultado de la diagnosis de error mencionado al producirse la conversión y un dispositivo de transmisión (parte 104 de transmisión de datos) que tiene una función de transmitir los datos de control obtenidos desde el dispositivo de entrada y los datos de estado formando un par con ellos a la red.

Por otro lado, el controlador 2 de seguridad incluye un dispositivo receptor (parte 204 de transmisión/recepción de datos) para recibir los datos de control y los datos de estado formando un par con ellos desde la red 3 y un dispositivo reproductor de datos de entrada (operación 503) para reproducir los datos de entrada basándose en los datos de estado que forman un par con los datos de control y tratándolos.

Con tal estructura, la unidad (1A, 1C) de seguridad remota está provista con un dispositivo de transmisión que tiene una función de transmitir los datos de control obtenidos desde el dispositivo de entrada y los datos de estado que

forman un par con ellos y el controlador 2 de seguridad está provisto con un dispositivo receptor para recibir los datos de control y los datos de estado que forman par con ellos desde la red 3 y un dispositivo reproductor de datos de entrada para reproducir los datos de entrada basados en los datos de control y en los datos de estado que forman un par con ellos. Así, el controlador 2 de seguridad puede hacer un uso efectivo de un resultado de diagnosis en la unidad 1 de seguridad remota consiguiendo por ello un control de seguridad más fiable.

El presente invento permite que un resultado de diagnosis de error mencionado por las unidades de seguridad tal como esta clase de maestro de seguridad y esclavo de seguridad en un proceso de tratamiento de entrada de generar los datos de control a partir de la señal de entrada bruta que se ha mencionado por el lado que utiliza los datos de control también, de modo que pueda conseguirse una variedad de los controles de seguridad basándose en los datos de control.

REIVINDICACIONES

1.- Una unidad (1A) esclava de seguridad adaptada para ser conectada a una pluralidad de dispositivos de entrada (4), para recibir, procedentes de los dispositivos de entrada cuando está conectada a ellos, señales de entrada y para ser conectada a un controlador (2) de seguridad a través de una red (3) de manera que transmita las señales de entrada a un maestro de comunicación del controlador (2) de seguridad, comprendiendo la unidad (1A) esclava de seguridad:

una parte (101) de terminal de entrada que tiene una pluralidad de terminales de entrada adaptado cada uno para recibir una señal de entrada que tiene un valor lógico bruto procedente de un dispositivo de entrada (4) conectado de manera correspondiente que es activado cuando existe un peligro, en que el valor lógico bruto indica la presencia o ausencia de activación del dispositivo de entrada (4) conectado de manera correspondiente; y

una parte (102) de diagnóstico de error que diagnostica un error de corte o de cortocircuito de cableados entre cada terminal de entrada y el dispositivo de entrada (4) conectado de manera correspondiente, y genera, para cada terminal de entrada, datos de estado de diagnosis que tienen un valor lógico "Alto" durante la ausencia del error y un valor lógico "Bajo" durante la presencia del error; y

un medio de tratamiento (103) adaptado para convertir, para cada terminal de entrada, la señal de entrada dada al terminal de entrada correspondiente en datos de mando que tiene un valor lógico que refleja el valor lógico bruto, caracterizado porque

el valor lógico de los datos de control es cambiado obligatoriamente, independientemente del valor lógico bruto de la señal de entrada dada al terminal de entrada correspondiente, al valor lógico correspondiente a la presencia de activación del dispositivo de entrada (4) conectado de manera correspondiente cuando los datos de estado de diagnóstico del terminal de entrada son un "Bajo" lógico, y el valor lógico de los datos de control no es cambiado cuando los datos de estado de diagnosis del terminal de entrada son un "Alto" lógico; y

una parte (104) de transmisión de datos adaptada para transmitir, a dicho maestro de comunicación de dicho controlador (2) de seguridad cuando está conectado, un par del valor lógico de los datos de control y del valor lógico de los datos de estado de diagnosis correspondientes; en el que

el esclavo (1A) de seguridad está adaptado para ejecutar un tratamiento inicial después de que la alimentación del esclavo (1A) de seguridad sea activada, en el que para cada terminal, el valor lógico de los datos de estado de diagnosis es establecido inicialmente a "Bajo" de manera que el valor lógico de los datos de control sea obligatoriamente establecido al valor lógico correspondiente a la presencia de activación del dispositivo de entrada (4) conectado de manera correspondiente.

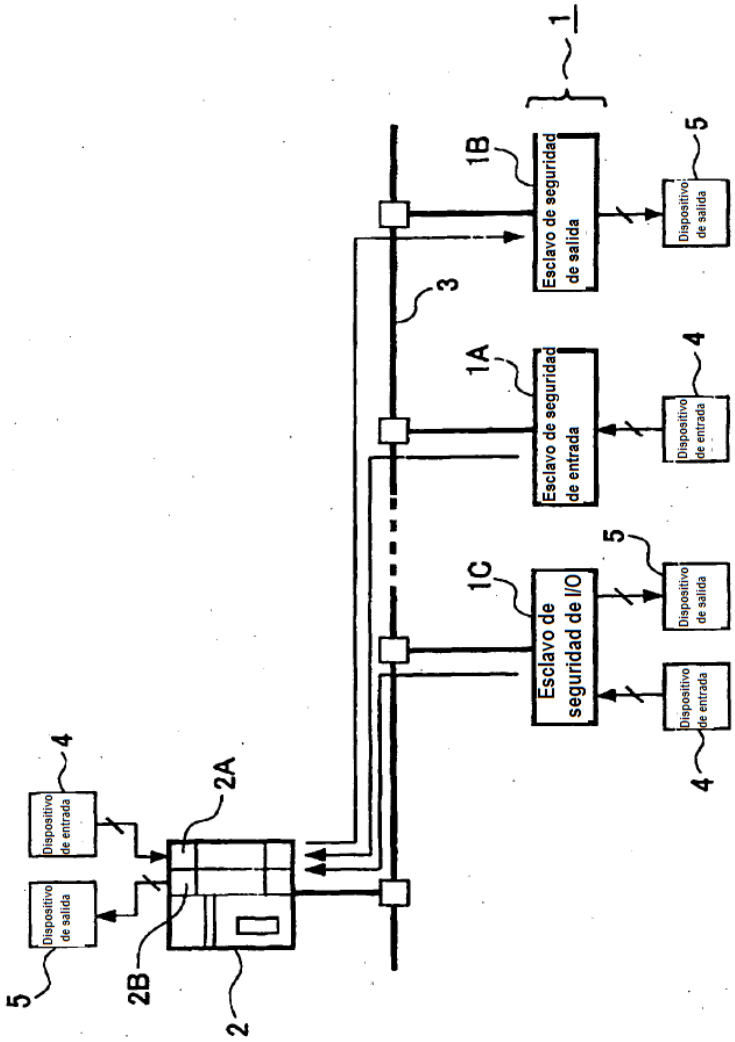


Diagrama de Configuración de Sistema de Control de Seguridad
1
1B
Esclavo de seguridad de salida
5
Dispositivo de salida
3
1A
Esclavo de seguridad de entrada
4
Dispositivo de entrada
1C
Esclavo de seguridad de I/O
5
Dispositivo de salida
Dispositivo de entrada
4
4
Dispositivo de entrada
2A
Dispositivo de salida
5
2B
2

Fig. 1

Fig. 2

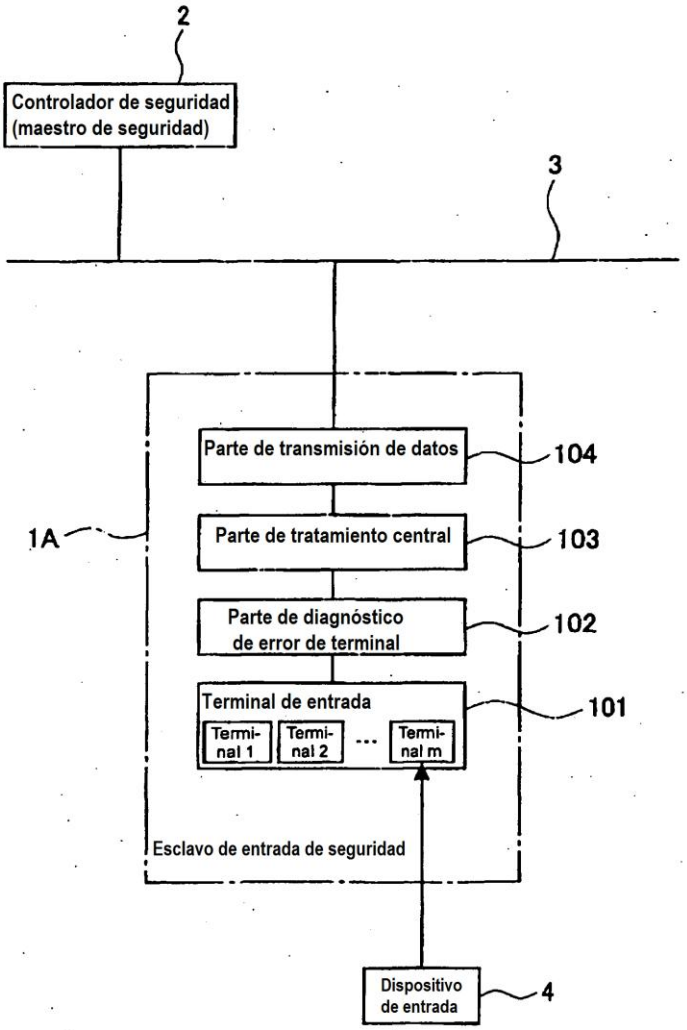


Diagrama de bloques que muestra la configuración de hardware interna del esclavo de seguridad de entrada

Fig. 3

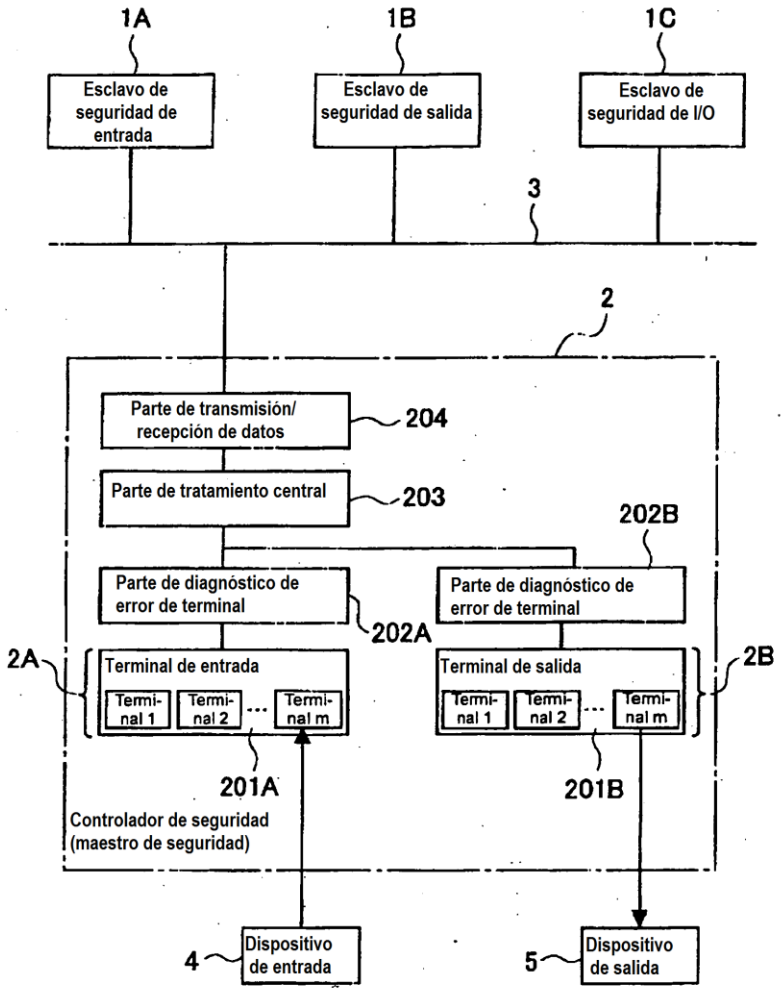


Diagrama de bloques que muestra la configuración del hardware interno de controlador de seguridad (maestro de seguridad)

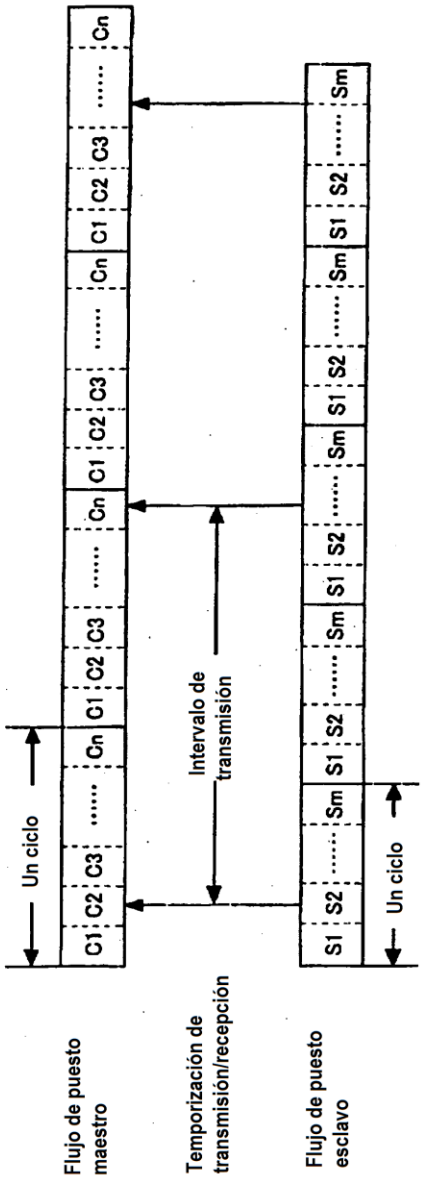


Fig. 4

Diagrama explicativo de temporización de comunicación entre puesto maestro y puesto esclavo

Fig. 5

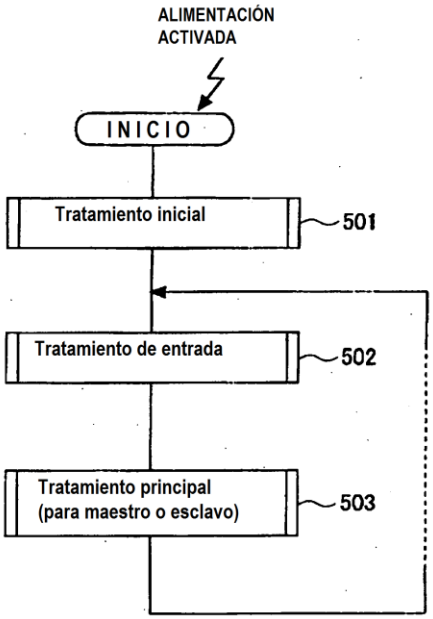


Diagrama de flujo general que muestra el contenido de tratamiento del dispositivo del presente invento

Fig. 6

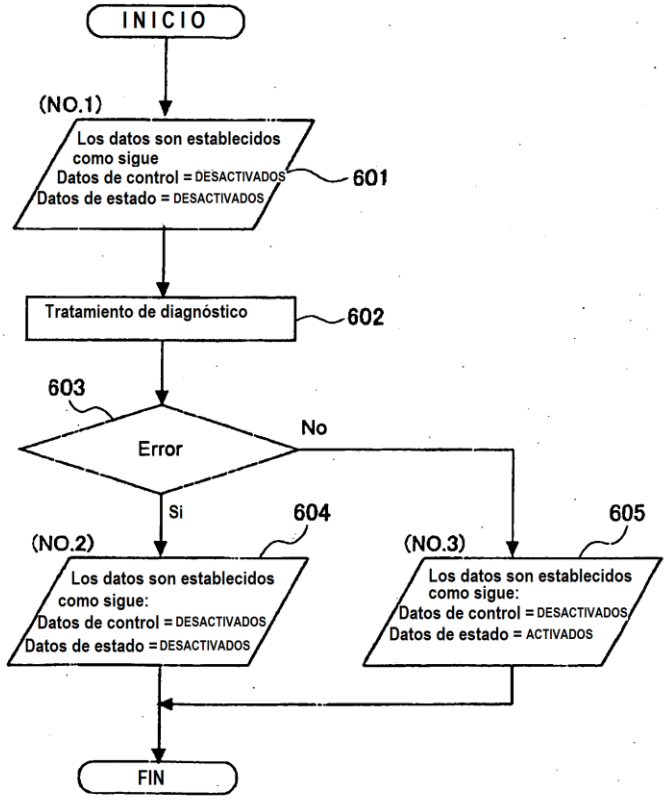


Diagrama de flujo que muestra el detalle del tratamiento inicial

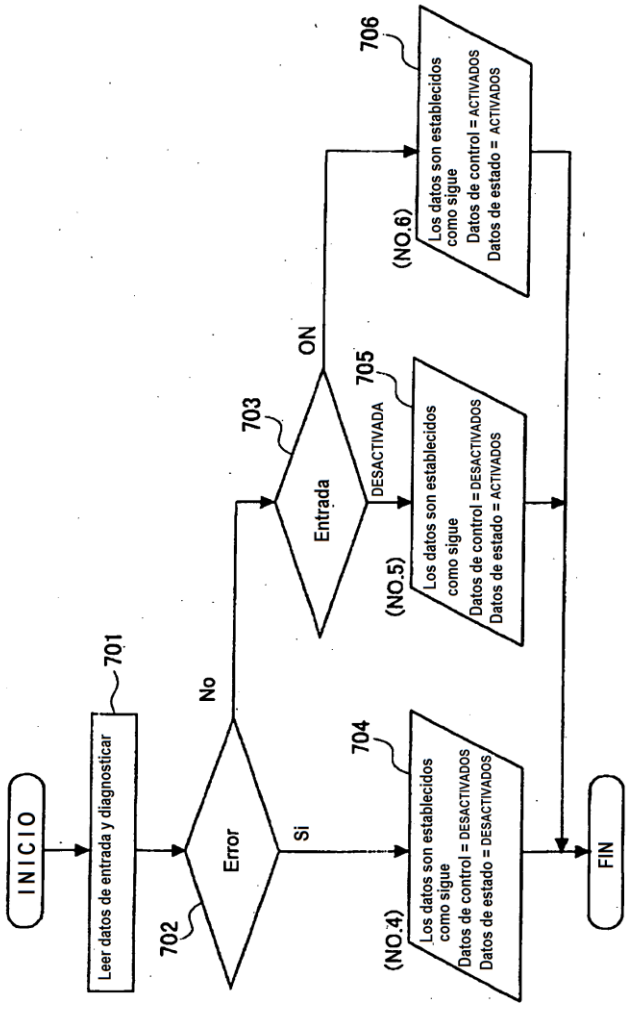


Fig. 7

Diagrama de flujo que muestra el detalle del tratamiento de entrada

Fig. 8

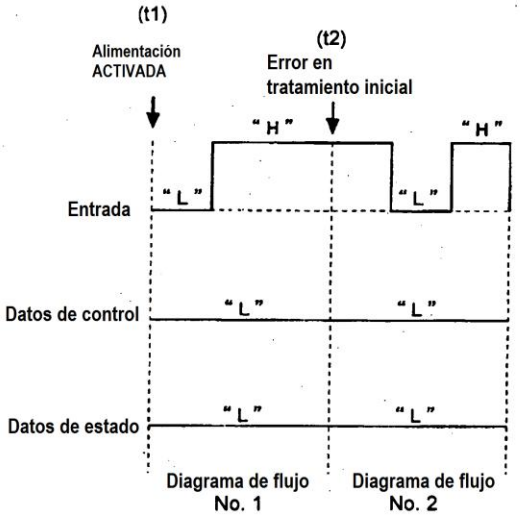


Gráfico de tiempos que muestra la transición de estado cuando se ha diagnosticado que existe un error en la diagnosis en el instante de tratamiento inicial (estado "H" = normal)

Fig. 9

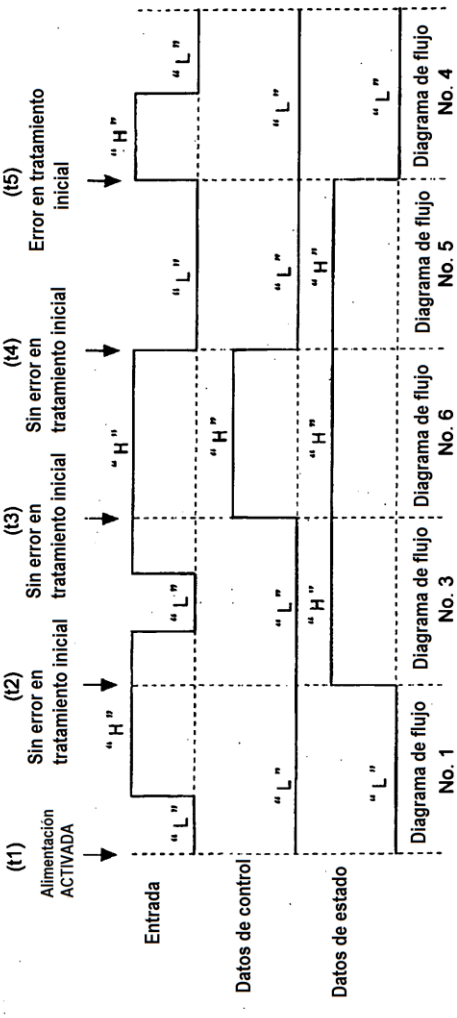


Gráfico de tiempos que muestra la transición de estado cuando se ha diagnosticado que existe un error en la diagnosis después de que la operación comience (estado "H" = normal)

Fig. 10

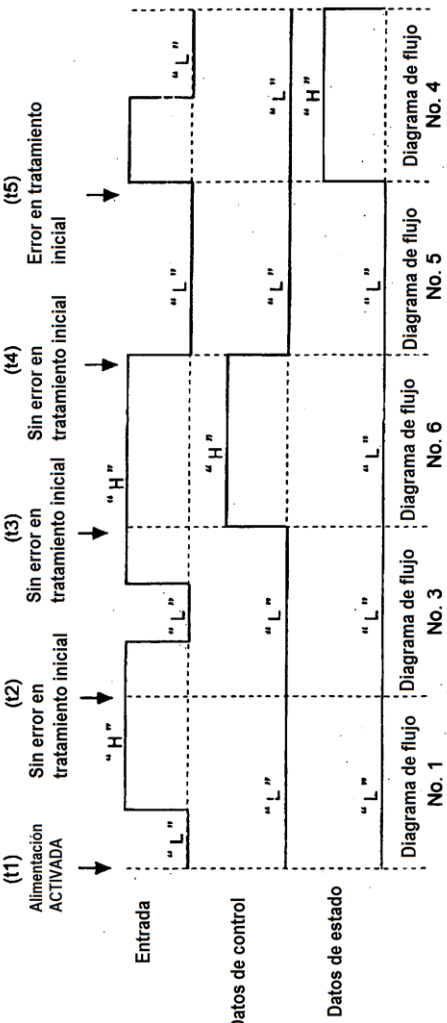
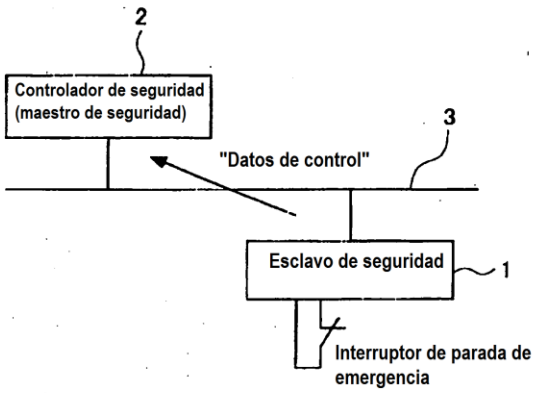


Gráfico de tiempo que muestra la transición de estado cuando se ha diagnosticado que existe un error después de que la operación comienza (estado "L" = normal)

Fig. 11



Tipos maestro/esclavo
Diagrama para explicar problemas en el sistema de control de seguridad