



19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

11 Número de publicación: **2 270 903**

51 Int. Cl.:
G05B 19/042 (2006.01)
G05B 23/02 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Número de solicitud europea: **01100230 .0**
86 Fecha de presentación : **03.01.2001**
87 Número de publicación de la solicitud: **1128241**
87 Fecha de publicación de la solicitud: **29.08.2001**

54 Título: **Procedimiento y dispositivo para la supervisión de la seguridad de una instalación de seguridad.**

30 Prioridad: **23.02.2000 DE 100 08 434**

45 Fecha de publicación de la mención BOPI:
16.04.2007

45 Fecha de la publicación del folleto de la patente:
16.04.2007

73 Titular/es: **PHOENIX CONTACT GmbH & Co. KG.**
Flachmarktstrasse 8-28
32825 Blomberg, DE

72 Inventor/es: **Horn, Steffen**

74 Agente: **Lehmann Novo, María Isabel**

ES 2 270 903 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Procedimiento y dispositivo para la supervisión de la seguridad de una instalación de seguridad.

La invención se refiere a un procedimiento para la supervisión de la seguridad de una instalación de seguridad en una instalación de automatización de acuerdo con la reivindicación 1 y a un dispositivo para la supervisión de la seguridad de una instalación de seguridad en una instalación de automatización de acuerdo con la reivindicación 12.

Las instalaciones de control se emplean cada vez en mayor medida para controlar o regular especialmente procesos o ciclos técnicos industriales, por ejemplo en la fabricación industrial o en el montaje final. De la misma manera se utilizan para la supervisión de procesos de este tipo accionados de forma automática en la mayor medida posible como también para la representación del estado momentáneo del proceso.

Las instalaciones de automatización o instalaciones automáticas correspondientes han alcanzado, en virtud del alto grado de productividad posible de esta manera, una posición excelente no sólo en la fabricación industrial. Así, por ejemplo, las instalaciones de automatización han encontrado aceptación en los procesos de mecanización con una alta carga para la salud humana o incluso con un potencial de peligro grande. Además, ha resultado casi imposible la realización de procesos químicos industriales o el contacto con materiales reactivos sin automatización.

Por lo tanto, tales instalaciones de automatización presentan, en general, al menos secciones o componentes, en los que se plantean altos o máximos requerimientos con respecto a la seguridad. Por ejemplo, debe asegurarse que determinadas máquinas son accionadas dentro de determinados parámetros de funcionamiento o debe impedirse que una máquina funcione, aunque se encuentre una persona en su zona de trabajo. A este respecto, por ejemplo una máquina giratoria ni puede exceder un número de revoluciones predeterminado ni una persona puede mantenerse en el radio de acción del robot durante el funcionamiento del mismo.

Además, durante el funcionamiento de una instalación de automatización debe estar asegurado que la instalación en funcionamiento no debe pasar, en el caso de un fallo de un componente del sistema, a un estado indefinido, imprevisible o incluso incontrolable.

Un principio para la solución de estos problemas de acuerdo con el estado de la técnica consiste especialmente en construir especialmente los componentes relevantes para la seguridad del sistema con varios canales, es decir, de forma redundante. Por ejemplo, en una instalación de automatización puede estar previsto realizar de forma duplicada los componentes de seguridad, es decir, por ejemplo, los usuarios del bus, que están asociados a una máquina relevante para la seguridad. Al mismo tiempo también el control central y el bus pueden estar constituidos de varios canales o incluso puede estar previsto un control de seguridad separado del control del proceso y constituido de forma redundante en determinadas circunstancias para el control de los componentes relevantes para la seguridad. Este control de la seguridad lleva a cabo esencialmente los enlaces de las informaciones de entrada relacionados con la seguridad y transmite a continuación, por ejemplo a través de un bus de automati-

zación, datos de enlace relacionados con la seguridad a los componentes de salida. Los componentes de salida, por su parte, procesan las medidas de seguridad recibidas y las transmiten después de la verificación positiva a unidades o aparatos periféricos. Además, conmutan sus salidas a un estado seguro cuando terminan la existencia de un error o no han recibido ya datos válidos dentro de un periodo de tiempo predeterminado.

El empleo de dos controles en el sistema es decir, un control de procesos así como el control de seguridad descrito tiene, sin embargo, como consecuencia algunos inconvenientes. Precisamente en virtud de los requerimientos crecientes planteados al tiempo de reacción de las instalaciones de automatización, un sistema de este tipo debe estar distribuido con frecuencia en islas de seguridad. Además, especialmente en los sistemas de control de varios canales se plantean problemas de sincronización que, a pesar de una instalación en principio intacta, pueden conducir a fallos o incluso a destrucciones de partes de las máquinas o de todas las máquinas. Además, la estructura de canales múltiples implica una elevación de los costes del sistema como también de los costes de mantenimiento debido al incremento del gasto del hardware.

Se conoce a partir del documento DE 198 15 150 A1 una disposición de sensores para la supervisión de un aparato de trabajo, que comprende una unidad de evaluación conectada en un bus, que espía de una manera continua las señales transmitidas a través del sistema de bus. El aparato de trabajo solamente se pone en funcionamiento cuando está presente una identificación libre de errores de codificaciones que se transmiten a través del sistema de bus. A tal fin, se evalúan los datos de entrada emitidos a través del usuario del bus a un maestro y que hacen conectar o desconectar el aparato de trabajo como reacción a la evaluación. Un principio de este tipo no es, en efecto, tan intensivo de costes, pero es muy poco flexible con respecto a una ampliación del sistema o a una adaptación de la instalación a otros componentes del bus.

También la publicación DE 35 02 387 describe un procedimiento para la supervisión de sistemas de microprocesador y de controles programables con memoria, en el que una unidad de control está conectada directamente en el bus del sistema de microprocesador o en el control programable con memoria. Este procedimiento se basa en una comparación de los datos transmitidos a través del bus del sistema con datos que están memorizados en los llamados puntos de control. Una comparación entre el valor teórico y el valor real que tiene lugar en este caso en la unidad de control posibilita el reconocimiento de funciones erróneas y genera una señal de error, que provoca una detención de un sistema que está conectado con el sistema de microprocesador o con el control programable con memoria. En este procedimiento existe, en efecto, una separación del proceso de control con respecto al proceso de supervisión. Sin embargo, es un inconveniente que el control se basa esencialmente en información memorizada.

El documento US-A-5 696 495 describe una instalación para la supervisión y control de una construcción de instalación compleja desde un punto local o remoto. Cada uno de los componentes funcionales de la instalación presenta un procesador subordinado conectado con el mismo, que están acoplados con una

unidad maestra y con una unidad de procesador adicional.

Por lo tanto, la invención tiene el cometido de configurar un procedimiento y un dispositivo para la supervisión de la seguridad de una instalación de seguridad en una instalación de automatización, de tal forma que el control y también la función de seguridad se aseguran, de una manera independiente de una separación de las dos funciones, a través de una verificación descentralizada redundante y se puede iniciar de forma directa una función de seguridad en función del resultado de la verificación.

Para la solución de este cometido sirven las características de las reivindicaciones 1 y 12.

La invención implica como ventaja una alta cota de seguridad. Es especialmente ventajosa la evitación de funciones de seguridad activadas de forma errónea a través de un mecanismo de control interno dentro de la supervisión de la seguridad.

Otras características ventajosas se deduce a partir de las reivindicaciones dependientes.

El procedimiento de acuerdo con la invención para la supervisión de la seguridad de una instalación de control en una instalación de automatización comprende las etapas indicadas a continuación. Se inscriben datos de entrada en una instalación de supervisión central y a partir de éstos se calculan primeros datos de salida en la instalación de supervisión central. Los primeros datos de salida y los datos de entrada son transmitidos a una instalación de supervisión descentralizada. En la instalación de supervisión descentralizada se calculan a partir de los datos de entradas unos segundos datos de salida. De acuerdo con la invención, se comparan los primeros con los segundos datos de salida en la instalación de supervisión descentralizada. En el caso de que exista al menos una coincidencia parcial de los primeros y los segundos datos de salida, se emiten como resultado de la comparación los primeros datos de salida al menos a una instalación asociada a la instalación de supervisión descentralizada.

El dispositivo de acuerdo con la invención para la supervisión de la seguridad de una instalación de control en una instalación de automatización comprende una instalación de supervisión central, configurada para la inscripción de datos de entrada y para el cálculo de primeros datos de salida a partir de los datos de entrada, y al menos una instalación de supervisión descentralizada que está configurada para la inscripción de los datos de entrada y/o de los primeros datos de salida. En este caso, al menos una instalación de supervisión descentralizada presenta un elemento de cálculo para el cálculo de segundos datos de salida a partir de los datos de entrada. De acuerdo con la invención, al menos una instalación de supervisión descentralizada está asociada al menos a una instalación. Además, en la instalación de supervisión descentralizada está prevista una unidad de comparación para la comparación de los primeros con los segundos datos de salida. El dispositivo de acuerdo con la invención contiene de la misma manera una instalación de emisión que está acoplada con la unidad de comparación, que emite los primeros datos de salida o bien los segundos datos de salida, en el caso de una coincidencia, como resultado de la comparación de los primeros y de los segundos datos de salida al menos a una instalación. Por otro lado, está prevista también una instalación de activación que, en el caso de una falta

de coincidencia de los primeros y los segundos datos de salida como resultado de la comparación, se activa con el fin de provocar una función relacionada con la seguridad.

El grado y la exactitud de la coincidencia parcial o bien de la no coincidencia parcial de los primeros y de los segundos datos de salida pueden ser influenciados de acuerdo con la invención a través de una preparación de un código de error reducido. De esta manera, se puede conseguir una seguridad casi absoluta. La reducción del error en los datos de entrada se puede conseguir a través del empleo de rutinas de control o de algoritmos de filtro.

La función relacionada con la seguridad puede ser una repetición de etapas individuales del procedimiento y/o de todas las etapas del procedimiento indicadas anteriormente. En este caso, los datos de entrada y/o los primeros datos de salida se pueden transmitir de nuevo. De la misma manera, en el marco de la invención está previsto repetir el cálculo de los primeros y/o de los segundos datos de salida a partir de los datos de entrada. En este caso, se conecta de nuevo el proceso de la comparación. En función del resultado de la comparación, deben repetirse de nuevo algunas o todas las etapas.

Pero en una forma de realización preferida de la invención está previsto también que la función relacionada con la seguridad comprenda una transferencia de una instalación individual a un estado ordenado, es decir, un estado de espera o bien limitado en el tiempo o que se mantiene hasta la siguiente activación así como una desconexión completa de la instalación. También la desconexión se puede acoplar con un tiempo de desconexión predeterminado. Pero la función relacionada con la seguridad puede comprender una terminación de un proceso de automatización, en el que se accionan de forma automática varias instalaciones.

Desde la instalación de supervisión descentralizada se transmiten datos de salida de una manera ventajosa a través del sistema de bus hacia una instalación que está conectada en el sistema de bus, como por ejemplo un robot. Así activan una acción determinada, como por ejemplo la repetición de un proceso de automatización. Como proceso de automatización se entiende, por ejemplo, el movimiento de un brazo de un robot o la terminación de un movimiento del robot.

De acuerdo con la invención, tales funciones relacionadas con la seguridad se adaptan al tipo y forma de realización de la instalación así como al potencial de peligro implicado con su funcionamiento.

En una forma de realización de la presente invención, la transmisión de los primeros datos de salida y de los datos de entrada hacia una instalación de supervisión descentralizada se lleva a cabo a través de un sistema de bus. Pero también es posible llevar a cabo directamente la transmisión.

El cálculo de los primeros datos de salida se puede realizar de acuerdo con la invención de una manera similar al proceso de cálculo para los segundos datos de salida. No obstante, es concebible también una variación de los procesos de cálculo respectivos en las diferentes instalaciones de supervisión. La instalación de supervisión central y la instalación de supervisión descentralizada pueden estar conectadas fijamente por cable de acuerdo con la invención.

También está previsto en el marco de la invención, realizar las instalaciones de supervisión a través

de componentes electrónicos o elementos de conmutación. No obstante, también los componentes esenciales de las instalaciones de supervisión o todas las instalaciones de supervisión pueden estar configurados como microprocesadores o procesadores de señales especialmente programables. En este caso, resulta ventajoso realizar de una manera relativamente sencilla una modificación de la instalación de supervisión a través de una intervención en el algoritmo programado.

También está incluida en la idea de la invención una forma de realización diferente de la instalación de supervisión central y de la instalación de supervisión descentralizada. Así, por ejemplo, de una manera opcional una de las dos instalaciones de supervisión puede estar constituida totalmente por microprocesadores o procesadores de señales programables o puede estar configurada como realización unitaria en forma de componentes electrónicos en lugar de estar controlada por hardware. Pero es concebible también una combinación de ellos. Así, por ejemplo, las dos instalaciones de supervisión pueden estar realizadas del mismo tipo de acuerdo con las variantes indicadas.

En el marco de la invención está incluido que las instalaciones están realizadas como instalaciones de control para procesos de fabricación, robots industriales y/o procesos de clasificación o de separación, como por ejemplo aparecen de forma automática a escala industrial.

La invención comprende como forma de realización preferida una instalación de supervisión descentralizada, que se incorpora como módulo posteriormente en una instalación de automatización y que se puede utilizar de acuerdo con las etapas indicadas anteriormente.

La invención se explica en detalle a continuación en combinación con los dibujos adjuntos en un ejemplo de realización. En éstos:

La figura 1 muestra el diagrama de bloques de un sistema de automatización accionado aplicando el procedimiento de acuerdo con la invención o bien utilizando el dispositivo de acuerdo con la invención.

La figura 2 muestra el flujo de datos esquemático de una instalación de supervisión central.

La figura 3 muestra una representación esquemática del protocolo de transmisión de una instalación de supervisión descentralizada.

De acuerdo con la figura 1, la instalación de automatización 1 presenta un control 2 y una instalación de supervisión central 3. La instalación de automatización 1 contiene unidades de entrada y salida directas (Unidades de E/S) así como una conexión de bus en serie. Todos los datos que son necesarios para el control y/o verificación del proceso de automatización se pueden transmitir de acuerdo con la invención directamente a través de las unidades de entrada y salida 4 o a través de la conexión del bus de serie 5 hacia la instalación de automatización o bien se puede emitir desde ésta. A través de la conexión de bus en serie 5, la instalación de automatización 1 está conectada con un sistema de bus 6. En el sistema de bus 6 están previstas unidades de entrada 7, 8 o interfaces de entrada para la entrada de datos. Por otro lado, el sistema de bus 6 está diseñado de tal forma que a través de una instalación de supervisión central, que está realizada de una manera preferida como instalación de supervisión de salida 9, activa una instalación periférica no

mostrada en la figura 1. El sistema de bus 6 posee de acuerdo con la figura 1 otra unidad 10, con la que se pueden emitir datos.

El procedimiento de acuerdo con la invención o bien el modo de funcionamiento del dispositivo de acuerdo con la invención se llevan a cabo esencialmente como se indica a continuación y se explican con la ayuda de las siguientes figuras 2 y 3.

En primer lugar se inscriben datos de entrada relevantes para la seguridad. Se trata de datos que garantizan el funcionamiento seguro de instalaciones, que son activadas o bien que funcionan a través de la instalación de automatización. Esto se lleva a cabo de acuerdo con la invención de una manera preferida a través de las unidades 7 y/u 8. Los datos de entrada (I1, I2, I3) relevantes para la seguridad se pueden transmitir también directamente, como se muestra en la figura 1, a la instalación de automatización 1. La instalación de supervisión central 3, que está prevista de una manera preferida directamente en la instalación de automatización 1, contiene ahora los datos de entrada I1 - I3 relevantes para la seguridad.

La instalación de supervisión central 3 calcula a partir de los datos de entrada ahora los primeros datos de salida Q_z que son relevantes para la seguridad de todo el proceso de automatización. Los datos de entrada I1 - I3 inscritos son transmitidos ahora junto con los datos de salida calculados Q_z hacia la instalación de supervisión de salida descentralizada 9. De acuerdo con la figura 2, los datos introducidos localmente (I1) o a través de la conexión de bus en serie (I2, I3) en la instalación de supervisión central 3 son combinados entre sí con la ayuda de operadores lógicos I1, I2 para formar los datos de salida Q_z , que se transmiten en un protocolo de salida predeterminado de la misma manera a la instalación de supervisión de salida descentralizada 9.

De acuerdo con la figura 3, la instalación de supervisión de salida descentralizada 9 calcula entonces a partir de los datos de entrada I1 - I3 transmitidos a esta instalación un dato de salida local Q_D , siendo empleados ahora operadores 13, 14 y/o unidades lógicas dentro de esta instalación de supervisión de salida descentralizada 9. De acuerdo con la invención, la instalación de supervisión de salida descentralizada 9 comprende un operador de comparación, que compara los datos de salida Q_z transmitidos desde la instalación de supervisión central 3 con los segundos datos de salida Q_D .

Si los datos de salida, calculados por la instalación de supervisión central 3, coinciden con los datos de salida Q^D calculados localmente, entonces estos datos son transferidos a una instalación periférica para el control, por ejemplo para la desconexión de la instalación periférica. En el caso de no coincidencia de los datos de salida Q_z y Q_D calculados en las dos instalaciones de supervisión diferentes, está presente un error en la transmisión de los datos y/o en uno de los algoritmos de cálculo o de supervisión. La instalación de supervisión de salida descentralizada 9 inicializa ahora otras repeticiones del proceso de cálculo o de comparación o también una repetición del proceso de transmisión de datos.

Así, por ejemplo, a diferencia de la figura 1, la instalación de supervisión de salida descentralizada 9 puede activar otras instalaciones periféricas. En una forma de realización de este tipo, está previsto adaptar el cálculo y la salida de los datos de salida Q_D a

las instalaciones periféricas conectadas. Pero también es concebible conectar cada instalación periférica con una instalación de supervisión de salida descentralizada, siendo calculados y transmitidos entonces solamente los datos necesarios para el cálculo o bien la supervisión de la instalación periférica.

La invención prevé, además, que la instalación de supervisión de salida descentralizada 9 contenga todas las informaciones necesarias para la supervisión redundante descentralizada de una función de segu-

5

10

15

20

25

30

35

40

45

50

55

60

65

ridad. De esta manera se asegura que en el caso de un fallo de la instalación de supervisión central 3 se garantice todavía una verificación de la supervisión redundante a través de la instalación de supervisión de salida descentralizada 9. De la misma manera, en una forma de realización preferida de la invención, también la instalación de supervisión central 3 recibe las informaciones redundantes, con el fin de poder eliminar errores, dado el caso, inherentes a los datos, durante el proceso de entrada.

REIVINDICACIONES

1. Procedimiento para la supervisión de la seguridad de una instalación de control en una instalación de automatización (1), que comprende:

- la inscripción de datos de entrada en una instalación de supervisión central (3),
- el cálculo de los primeros datos de salida en la instalación de supervisión central (3) a partir de los datos de entrada

caracterizado por

- la transmisión de los primeros datos de salida y de los datos de entrada hacia al menos una instalación de supervisión descentralizada (9),
- el cálculo de segundos datos de salida en al menos una instalación de supervisión descentralizada (9) a partir de los datos de entrada,
- la comparación de los primeros con los segundos datos de salida en la instalación de supervisión descentralizada (9),
- la emisión de los primeros datos de salida como resultado de una coincidencia al menos parcial de los primeros y los segundos datos de salida al menos a una instalación asociada a la instalación de supervisión descentralizada (9).

2. Procedimiento de acuerdo con la reivindicación 1, **caracterizado** porque en el caso de no coincidencia al menos parcial de los primeros y segundos datos de salida, se activa una función relacionada con la seguridad.

3. Procedimiento de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque la función relacionada con la seguridad comprende una repetición de las etapas de la transmisión y/o del cálculo y/o de la comparación y/o de la emisión.

4. Procedimiento de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque la función relacionada con la seguridad comprende una transferencia de una instalación a un estado ordenado.

5. Procedimiento de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque la función relacionada con la seguridad comprende una desconexión de la instalación.

6. Procedimiento de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque la función relacionada con la seguridad comprende una terminación de un proceso de automatización.

7. Procedimiento de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque la transmisión de los primeros datos de salida y de los datos de entrada hacia una instalación de supervisión descentralizada (9) se lleva a cabo a través de un sistema de bus (6) y/o directamente.

8. Procedimiento de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque el cálculo de los primeros datos de salida corresponde al cálculo de los segundos datos de salida.

9. Procedimiento de acuerdo con una de las reivin-

dicaciones anteriores, **caracterizado** porque la instalación de supervisión central y la instalación de supervisión descentralizada (3, 9) están conectadas fijamente por cable.

10. Procedimiento de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque las instalaciones de supervisión (3, 9) están controladas por software.

11. Procedimiento de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque la instalación está realizada como instalación de control para procesos de fabricación, procesos de clasificación y/o procesos de separación.

12. Dispositivo para la supervisión de la seguridad de una instalación de control en una instalación de automatización (1)

- con una instalación de supervisión central (3), que está configurada para la inscripción de datos de entrada y para el cálculo de primeros datos de salida a partir de los datos de entrada,

caracterizado

- con al menos una instalación de supervisión descentralizada (9), que está configurada para la inscripción de los datos de entrada y/o de los primeros datos de salida, en la que al menos una instalación de supervisión descentralizada (9) presenta un elemento de cálculo para el cálculo de segundos datos de salida a partir de los datos de entrada, y al menos a una instalación de supervisión descentralizada (9) está asociada una instalación,
- con una unidad de comparación para la comparación de los primeros con los segundos datos de salida en al menos una instalación de supervisión descentralizada (9),
- con una instalación de salida acoplada con la unidad de comparación, que emite los primeros datos de salida como resultado de una coincidencia al menos parcial de los primeros y segundos datos de salida.

13. Dispositivo de acuerdo con la reivindicación 12, en el que una instalación de activación activa una función relacionada con la seguridad en el caso de una no coincidencia al menos parcial de los primeros y de los segundos datos de salida.

14. Dispositivo de acuerdo con la reivindicación 12 ó 13, en el que la instalación de supervisión central (3) y la instalación de supervisión descentralizada (9) están conectadas a través de un sistema de bus (6) y/o directamente.

15. Dispositivo de acuerdo con una de las reivindicaciones 12 a 14, en el que la instalación de supervisión descentralizada (3) está conectada con al menos una instalación a través de un bus (6) y/o directamente.

16. Dispositivo de acuerdo con una de las reivindicaciones 12 a 15, **caracterizado** porque las instalaciones de supervisión (3, 9) comprende microprocesadores y/o procesadores de señales programables.





