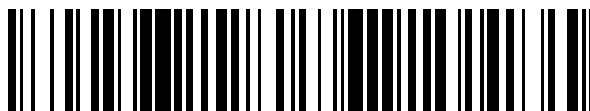


19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 774 418**

51 Int. Cl.:

**G05B 9/03**

(2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **22.11.2016** **E 16200066 (5)**

97 Fecha y número de publicación de la concesión europea: **01.01.2020** **EP 3176654**

54 Título: **Sistema de seguridad automatizado de una instalación industrial**

30 Prioridad:

**01.12.2015 FR 1561680**

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

**21.07.2020**

73 Titular/es:

**SCHNEIDER ELECTRIC INDUSTRIES SAS**  
**(100.0%)**

**35, rue Joseph Monier**  
**92500 Rueil-Malmaison, FR**

72 Inventor/es:

**PRUNIER, MICHEL**

74 Agente/Representante:

**GONZÁLEZ PECES, Gustavo Adolfo**

ES 2 774 418 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

Sistema de seguridad automatizado de una instalación industrial

### Campo Técnico

5 La invención se sitúa en el campo de la seguridad de las instalaciones industriales y se refiere más específicamente a un sistema de seguridad automatizado de una instalación industrial que comprende una pluralidad de sensores destinados a tomar medidas de un proceso industrial, una pluralidad de accionadores destinados a ejecutar acciones de seguridad que dependen de señales de medida suministradas por dichos sensores, al menos dos cadenas de tratamiento distintas que conectan los sensores y los accionadores, y al menos un módulo de prueba independiente de dichas cadenas de tratamiento destinado a detectar un fallo de una de dichas cadenas de tratamiento.

### 10 Estado de la técnica anterior

Para mejorar la fiabilidad y la seguridad de las instalaciones industriales, en particular de las instalaciones nucleares, los sistemas de seguridad comprenden generalmente dos tipos de arquitectura, o bien un sistema redundante en el que las funciones aplicativas, de las cuales se encarga un autómata programable por ejemplo, son duplicadas para mejorar la disponibilidad de las funciones críticas de seguridad, de manera que si un módulo de entrada/salida o un procesador falla, la parte redundante compensa este fallo. A tal efecto, estos sistemas comprenden generalmente dos  
15 autómatas programables que aseguran estas funciones críticas y un módulo de votación utilizado para seleccionar un solo comando de entre los comandos emitidos por los autómatas programables y para aplicar el comando seleccionado a un accionador.

20 Un inconveniente de los sistemas de seguridad de la técnica anterior proviene del hecho de que no protegen las instalaciones bajo vigilancia contra los fallos denominados de modos comunes. Estos fallos afectan simultáneamente a dos cadenas de tratamiento distintas que comprenden al menos dos módulos de seguridad de hardware y/o de software que utilizan tecnologías redundantes de la misma naturaleza.

25 El documento US5984504 describe un sistema de seguridad que comprende subsistemas redundantes que forman una primera y una segunda cadenas de tratamiento destinadas a asegurar una protección de una instalación nuclear contra fallos.

Un objetivo de la invención es compensar los inconvenientes de la técnica anterior descritos anteriormente.

### Descripción de la invención

Este objetivo se alcanza por medio de un sistema compacto, poco complejo y poco costoso que permite asegurar una redundancia parcial para ciertas funciones clave de un sistema automatizado.

30 Este sistema comprende una pluralidad de sensores destinados a tomar medidas de un proceso industrial, una pluralidad de accionadores destinados a ejecutar operaciones que dependen de señales de medidas suministradas por dichos sensores, al menos una primera cadena de tratamiento y al menos una segunda cadena de tratamiento que conecta los sensores y los accionadores, la primera cadena de tratamiento comprende al menos una primera unidad de tratamiento que implementa una primera tecnología mientras que la segunda cadena de tratamiento comprende al  
35 menos una segunda unidad de tratamiento que implementa una segunda tecnología diferente de la primera tecnología de manera que se asegura una redundancia parcial de al menos una función crítica de seguridad de la instalación industrial.

40 Según la invención, el sistema comprende además al menos un módulo de prueba independiente de las cadenas de tratamiento adaptado para sustituir las señales de prueba por las señales de medida de los sensores y para comparar las respuestas a dicha señales de prueba a la salida de cada unidad de tratamiento con señales tipo pregrabadas.

De forma preferente, la primera unidad de tratamiento es un circuito de relés y/o un circuito analógico mientras que la segunda unidad de tratamiento es un autómata industrial programable, siendo un circuito analógico un circuito electrónico a base de componentes analógicos, tales como amplificadores operacionales, transistores, etc....

45 La utilización de dos tecnologías distintas en al menos dos cadenas de tratamiento distintas permite al sistema según la invención asegurar una protección de la instalación contra fallos denominados de modo común relacionados con las diferentes tecnologías utilizadas.

Además, debido a que la redundancia es parcial y se refiere únicamente a ciertas funciones críticas de seguridad de la instalación industrial, es posible concebir un sistema simple, robusto, poco costoso y más compacto que un sistema que comprenda dos autómatas industriales programables redundantes.

50 Dichas señales de prueba son una representación de la dinámica de variación de señales suministradas por los sensores.

En un modo preferido de realización, el sistema según la invención comprende un módulo de decisión que comprende un módulo de votación y un módulo de detección de incoherencia entre las respuestas de las unidades de tratamiento y, estando adaptado dicho módulo (16) de votación para seleccionar, en función del resultado del modo de detección de incoherencia, o bien señales de medida suministradas a la salida de la primera unidad de tratamiento, o bien señales de medida suministradas a la salida de la segunda unidad de tratamiento.

En el modo preferido de realización del sistema según la invención, la primera cadena de tratamiento comprende un panel de diagnóstico no digital y la segunda cadena de tratamiento comprende un panel de diagnóstico digital.

### Breve descripción de los dibujos

Otras características y ventajas de la invención se desprenderán de la descripción siguiente, tomada a título de ejemplo no limitativo, con referencia la figura 1 que ilustra esquemáticamente un modo preferido de realización del sistema de seguridad automatizado según la invención.

### Descripción detallada de modos de realización particulares

La figura 1 representa una arquitectura que permite tener una diversidad tecnológica entre un tratamiento programado por software y un tratamiento no programado por software. Esta diversidad es particularmente requerida para asegurar la seguridad de las instalaciones nucleares con el fin de liberarse de los fallos denominados de modo común entre dos tecnologías.

La arquitectura ilustrada en la figura 1 comprende una pluralidad de sensores 2 distintos destinados a tomar informaciones todo o nada o medidas de magnitudes físicas tales como por ejemplo una temperatura, una presión o cualquier otra magnitud medida en un proceso industrial. Con el fin de evitar los fallos de causa común, los diferentes sensores están constituidos de tecnologías diferentes o de constructores diferentes e implementan principios de medidas diferentes. Por ejemplo, ciertos sensores pueden medir impulsos representativos de variaciones de la magnitud física mientras que otros miden valores analógico representativos de las variaciones de esta magnitud física.

De forma preferible, el sistema de la figura 1 presenta una diversidad tecnológica a lo largo de toda la cadena de medida. Esta diversidad tecnológica se refiere a los sensores, las alimentaciones eléctricas de las unidades de tratamientos y los programas aplicativos implementados para asegurar la seguridad de instalación.

Como se ilustra por la figura 1, el sistema comprende dos cadenas de tratamiento paralelas. Una primera cadena de tratamiento que comprende una primera unidad 4 de tratamiento, y una segunda cadena de tratamiento que comprende una segunda unidad 6 de tratamiento. La primera unidad 4 de tratamiento es un circuito de relés y/o un circuito analógico mientras que la segunda unidad 6 es un autómata programable.

Cada una de las unidades 4 y 6 de tratamiento está conectada a uno o a varios sensores 2 a través de un miembro 8 de conmutación. Las salidas 10, 12 respectivamente de las unidades 4, 6 de tratamiento están conectadas a un módulo 14 de decisión que comprende un módulo 16 de votación y un módulo 18 de detección de incoherencia entre las respuestas de las unidades 4, 6 de tratamiento. La salida del módulo 14 de votación está conectada a un accionador 20.

En un modo preferido de realización de la invención, el sistema comprende además un módulo 22 de prueba independiente de las cadenas 4 y 6 de tratamiento, adaptado para reemplazar periódicamente, a las entradas de cada unidad de tratamiento, la señales de medidas suministradas por los sensores 2 por señales de prueba, y para comparar las respuestas suministradas en las salidas 10 y 12, respectivamente de las unidades 4 y 6 de tratamiento con señales tipo pregrabadas. Además, la primera cadena 4 de tratamiento comprende un panel 24 de diagnóstico no digital y la segunda cadena 6 de tratamiento comprende un panel 26 de diagnóstico digital. El módulo 22 de prueba realiza periódicamente la prueba de coherencia sin que el sistema esté informado del hecho de que está bajo prueba.

Las unidades 4, 6 de tratamiento están alimentadas respectivamente por una primera fuente 28 de alimentación, y por una segunda fuente 30 de alimentación. Con el fin de evitar fallos de causa común, las fuentes 28 y 30 de alimentación están igualmente constituidas de tecnologías diferentes o de constructores diferentes.

En funcionamiento, la primera unidad 4 de tratamiento realiza tratamientos aplicativos a base de tecnologías convencionales, no digitales, es decir no comprende software y la segunda unidad 6 de tratamiento realiza los tratamientos aplicativos programables. Los tratamientos aplicativos comprenden:

- tareas de vigilancia de buen funcionamiento de los miembros de tratamiento digital de la autómata programable, tal como la memoria,
- tareas de perro guardián que, en caso de solicitación de las tareas de vigilancia, sitúan las salidas de la autómata programable en una posición predeterminada y conocida con anterioridad. Esta posición predeterminada es por ejemplo una posición segura de todas o parte de las salidas.
- una tarea de señalización del paso de la prueba o no. Esta información es transmitida por autómata programable a partir de una entrada todo o nada que es una imagen de la posición del miembro de conmutación. Por tanto,

“posición prueba” corresponde a una “información activada”, “posición no prueba” corresponde a una “información desactivada”. El reflejo de esta información se transmite al panel 24 de diagnóstico convencional y al panel 26 de diagnóstico digital.

- 5 - una tarea de cumplimiento del tiempo de ciclo realizado por un software para controlar la no superación del tiempo de ciclo de tratamiento digital de la automática programable.

El módulo 16 de decisión es alimentado por una alimentación de alta disponibilidad que es realizada a partir de dos alimentaciones, por ejemplo. Este módulo 16 de decisión realiza la votación entre las salidas de unidades de tratamiento convencional 4 y digital 6 en función de la comparación de las respuestas suministradas en la salida 10 y 12, en las señales tipo pregrabadas.

- 10 Las unidades 4 y 6 de tratamiento entregan una información de buen funcionamiento al módulo 22 de prueba y respectivamente a los paneles 24 y 26 de diagnóstico si las diferentes tareas de vigilancia, de prueba y de seguridad no detectan un mal funcionamiento.

- 15 El módulo 22 de prueba realiza las pruebas de la arquitectura para garantizar que sea operacional y que no se detecte ningún fallo a través de los resultados de prueba medidos a la salida de las unidades de tratamiento convencional 4 y digital 6. Por esto, el módulo 22 de prueba introduce las señales de prueba en las entradas 40 y 42 respectivamente de las unidades de tratamiento convencional 4 y digital 6 a través del miembro 8 de conmutación, y las compara con las señales suministradas por el módulo 16 de votación al accionador 20.

- 20 El sistema según la invención, permite obtener una resistencia a los fallos de modo común por medio de una arquitectura compacta en la cual las funciones críticas que son normalmente realizadas por el automático programable son realizadas con una doble tecnología, una de tratamiento programado y otra de relés. Por tanto, se mejora el volumen y la fiabilidad global de los equipos. Además, se puede activar una alarma en caso de incoherencia, entre las señales suministradas al accionador por las unidades 4 y 6 de tratamiento.

## REIVINDICACIONES

1. Sistema de seguridad automatizado de una instalación industrial que comprende una pluralidad de sensores (2) destinados a tomar medidas de un proceso industrial, una pluralidad (20) de accionadores destinados a ejecutar operaciones que dependen de las señales de medida suministradas por dicho sensores (2), al menos una primera cadena de tratamiento y al menos una segunda cadena de tratamiento que conectan los sensores (2) y los accionadores (20), la primera cadena (4) de tratamiento comprende al menos una primera unidad (4) de tratamiento que implementa una primera tecnología mientras que la segunda cadena de tratamiento comprende al menos una segunda unidad (6) de tratamiento que implementa una segunda tecnología diferente de la primera tecnología de manera que asegura una redundancia parcial de al menos una función crítica de seguridad de la instalación industrial,  
5 **caracterizado porque** comprende al menos un módulo (22) de prueba independiente de dichas primera y segunda cadenas de tratamiento adaptado para sustituir las señales de prueba por las señales de medida suministradas por los sensores (2), y para comparar las respuestas suministradas en las salidas (10) y (12), respectivamente de las primera y segunda unidades (4) y (6) de tratamiento, con señales tipo pregrabadas.  
10
2. Sistema según la reivindicación 1, en el cual la primera unidad (4) de tratamiento es un circuito de relés (4) mientras que la segunda unidad de tratamiento es un autómata (6) industrial programable.  
15
3. Sistema según la reivindicación 1, en el cual la primera unidad (4) de tratamiento es un circuito analógico mientras que la segunda unidad de tratamiento es un autómata (6) industrial programable.
4. Sistema según la reivindicación 3, que comprende además un módulo (14) de decisión que comprende un módulo (16) de votación y un módulo (18) de detección de incoherencia entre las respuestas de las unidades (4) y (6) de tratamiento, estando adaptado dicho módulo (16) de votación para seleccionar, en función del resultado del módulo (18) de detección de incoherencia, o bien señales de medida suministradas a la salida de la primera unidad (4) de tratamiento, o bien señales de medida suministradas a la salida de la segunda unidad (6) de tratamiento.  
20
5. Sistema según la reivindicación 4, en el cual la primera cadena de tratamiento comprende un panel (24) de diagnóstico no digital y la segunda cadena de tratamiento comprende un panel (26) de diagnóstico digital.  
25

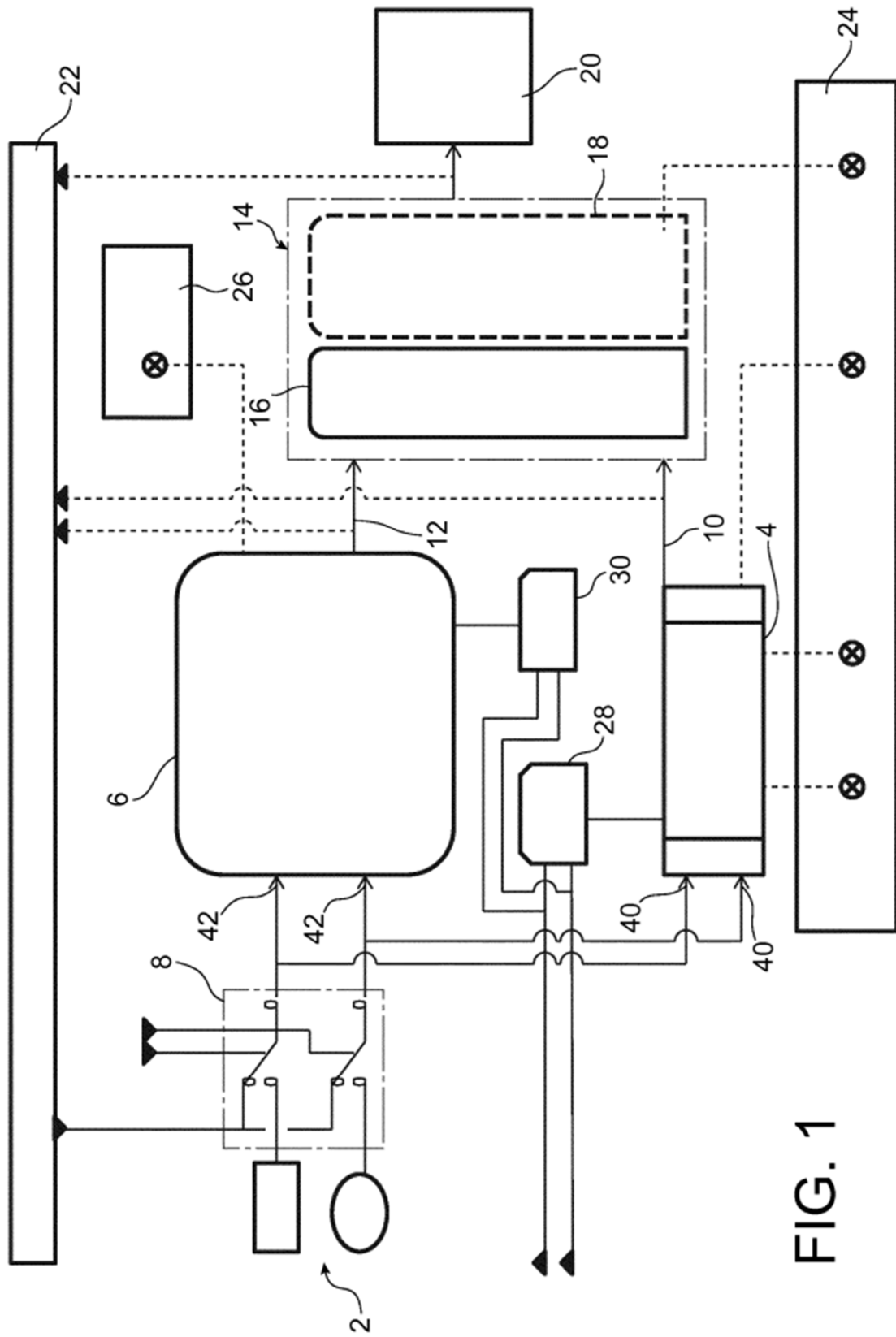


FIG. 1