(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 781 853**

(51) Int. CI.:

G05B 9/03 (2006.01)
F23D 14/00 (2006.01)
F23N 5/24 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **23.03.2015 E 15160378 (4)**

(97) Fecha y número de publicación de la concesión europea: **22.01.2020 EP 3073333**

(54) Título: **Instalación de quemador con un dispositivo de seguridad**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.09.2020

(73) Titular/es:

SIEMENS AKTIENGESELLSCHAFT (100.0%)
Werner-von-Siemens-Straße 1
80333 München, DE

(72) Inventor/es:

OBRECHT, KLAUS

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Instalación de quemador con un dispositivo de seguridad

La presente revelación se refiere a instalaciones de quemadores con dispositivos de seguridad. En el centro de la arquitectura de seguridad, según la presente divulgación, se encuentra la seguridad en caso de fallo.

Las arquitecturas de seguridad se tratan, entre otros, en el estándar IEC 61508. Este estándar se publicó como 2ª edición en 2010. Se ocupa de la seguridad funcional de los sistemas eléctricos / electrónicos / programables en relación con la seguridad.

Además, la norma EN13611 - Dispositivos de seguridad, regulación y control para quemadores y aparatos de gas – del año 2011, así como EN60730 – aparatos de regulación y control eléctricos automáticos para uso doméstico y aplicaciones similares - también de 2011, describen los requisitos mínimos para sistemas de seguridad.

Los sistemas de control relacionados con la seguridad se conocen de las áreas de los sistemas de quemadores, de la tecnología de automatización, de la tecnología médica y de la tecnología automotriz, entre otros.

Del estado de la técnica se sabe que en los sistemas con tareas críticas para la seguridad se deben de tomar medidas para proteger contra fallos de funcionamiento. Esto incluye, por ejemplo, la supervisión de los bloques de función de un dispositivo de seguridad utilizando señales de prueba. También se conoce la implementación multicanal de una arquitectura de seguridad con comparación de resultados.

Sobre la base de estas medidas, se deben de identificar los fallos aleatorios (y opcionalmente también los fallos sistemáticos). Por medio de una unidad de supervisión se puede conseguir que un sistema (quemador) o un proceso se encuentre en un estado seguro.

En relación con las arquitecturas de seguridad y los circuitos de seguridad correspondientes, se distingue entre las arquitecturas tolerantes a fallos y a prueba de fallos. Las arquitecturas tolerantes a fallos se caracterizan por el hecho de que las tareas de control y supervisión pueden continuar realizándose incluso después de la aparición de uno o más fallos. Para lograr tal tolerancia frente a los fallos aleatorios, las arquitecturas deben construirse de forma redundante en múltiples canales.

A diferencia de una arquitectura tolerante a fallos, un sistema a prueba de fallos debe lograr un estado de sistema seguro como resultado de la ocurrencia de un primer fallo. Lo mismo se aplica a otros errores que se produzcan. Incluso en tales casos, el sistema debe alcanzar un estado de sistema seguro. Por lo tanto, el primer y segundo error en el dispositivo de seguridad deben conducir a un estado del sistema seguro.

En particular, el requisito del control de múltiples errores a menudo conduce a redundancias múltiples y, por lo tanto, aumenta la complejidad de la arquitectura. Además, la estructura multicanal aumenta los costos de dichos sistemas. Finalmente, el esfuerzo considerable en software y hardware asociado a la estructura multicanal a menudo no contribuye al cumplimiento real de la tarea de control y/o a la tarea de regulación de un sistema.

La solicitud de patente alemana DE102005030770A1 se presentó el 1 de julio de 2005 y se publicó el 23 de marzo de 2006. DE102005030770A1 describe una disposición de circuito y un procedimiento para controlar un dispositivo de seguridad para un vehículo.

La solicitud de patente estadounidense US2013/245794A1 se presentó el 6 de octubre de 2011 y se publicó el 19 de septiembre de 2013. US2013/245794A1 enseña un dispositivo de seguridad y un método de cálculo para un dispositivo de seguridad.

El objeto de la presente divulgación es un dispositivo de seguridad mejorado y/o una arquitectura de seguridad que supera, al menos en parte, las desventajas mencionadas anteriormente de los sistemas existentes.

Tareas técnicas y ventajas

La presente revelación tiene como objeto crear una instalación de quemador con una arquitectura de seguridad y/o un circuito de seguridad, que proporcione una estructura eficiente y de costo optimizado para un dispositivo de seguridad. La arquitectura de seguridad y/o el circuito de seguridad, en particular, deberían ser más rentables que un diseño redundante múltiple. Al mismo tiempo, los primeros y segundos errores aleatorios en el dispositivo de seguridad deberían conducir a un estado seguro del sistema. Por lo tanto, el dispositivo de seguridad y/o el circuito de seguridad según la presente divulgación deberían iniciar una desconexión (del sistema) tan pronto como ocurra un primer fallo.

No se requiere ninguna otra operación. Un error independiente adicional no debe conducir a una condición insegura del sistema. Por lo tanto, la arquitectura de seguridad debe ser a prueba de errores.

El objeto mencionado se logra, según la invención, mediante una instalación de quemador con un dispositivo de seguridad según la reivindicación 1. Realizaciones preferentes se dan en las reivindicaciones dependientes.

La presente revelación se basa además en el objeto de proporcionar una arquitectura de seguridad y/o un circuito de seguridad y/o un dispositivo de seguridad que (entre otros) produce un estado de la instalación seguro al interrumpir el suministro de energía, en particular, al interrumpir el suministro de corriente eléctrica.

La presente revelación también tiene como objeto proporcionar una arquitectura de seguridad y/o un circuito de seguridad y/o un dispositivo de seguridad que permita el bloqueo (de seguridad).

La presente revelación también tiene como objeto proporcionar una arquitectura de seguridad y/o un circuito de seguridad y/o un dispositivo de seguridad que pueda supervisar una multiplicidad de señales de entrada (de diseño diferente).

La presente revelación además tiene como objeto proporcionar una arquitectura de seguridad y/o un circuito de seguridad y/o un dispositivo de seguridad que se implementa (al menos parcialmente) en un procesador (multinúcleo) con redundancia.

La presente revelación además tiene como objeto proporcionar una arquitectura de seguridad y/o un circuito de seguridad y/o un dispositivo de seguridad que está diseñado para procesar señales analógicas o digitales relevantes para la seguridad.

La presente revelación además tiene como objeto proporcionar una arquitectura de seguridad y/o un circuito de seguridad y/o un dispositivo de seguridad que está configurado para procesar (inicialmente) señales estáticas.

La presente revelación también tiene como objeto proporcionar una arquitectura de seguridad y/o un circuito de seguridad y/o un dispositivo de seguridad que está configurado para comprobarse periódicamente para detectar si hay errores.

Breve descripción de las figuras

A partir de la siguiente descripción detallada serán evidentes para los expertos en la materia diversos detalles. Las realizaciones individuales no son restrictivas. Los dibujos que acompañan a la descripción se pueden describir de la siguiente manera:

La figura 1 muestra un diagrama de bloques de un sistema simple con una unidad de supervisión que puede realizar una función de seguridad entre la entrada y la salida.

La figura 2 muestra un diagrama de bloques de un sistema simple con un canal de supervisión y diagnóstico adicional.

La figura 3 muestra un diagrama de bloques de un sistema redundante múltiple.

La figura 4 ilustra, por medio de un diagrama de bloques, la dinamización de las señales.

La figura 5 ilustra, por medio de un diagrama de bloques, el control de las señales de salida por retroalimentación.

La figura 6 describe, por medio de un diagrama de bloques, medidas tales como la redundancia y los mecanismos de control para evitar la distorsión de las señales de datos digitales.

La figura 7 describe, por medio de un diagrama de bloques, las diferentes formas de alimentar señales relevantes para la seguridad en la arquitectura de seguridad.

La figura 8 trata, por medio de un diagrama de bloques, de las medidas para reconocer otros errores secundarios que ocurren aleatoriamente.

La figura 9 ilustra como un diagrama de bloques la implementación práctica de una arquitectura de un solo canal con diagnóstico por un procesador redundante (multinúcleo).

La figura 10 ilustra, por medio de un diagrama de bloques, el suministro de señales analógicas relevantes para la seguridad en un procesador redundante (multinúcleo).

Descripción detallada

La figura 1 muestra una arquitectura simple 1oo1 (inglés one out of one) con una entrada 1 y una salida 2 y una unidad de supervisión 3. Una avería o un error en la unidad de supervisión 3 de esta arquitectura simple 1oo1 puede hacer que el sistema no realice ninguna función de seguridad en la instalación. De esto se deduce que se requieren medidas adicionales para controlar los errores accidentales (y opcionalmente también sistemáticos) para la seguridad de la planta.

La Figura 2 muestra la llamada arquitectura 1oo1D (es decir, un canal con diagnóstico y seguridad inherente). La arquitectura que se muestra en la figura 2 proporciona una unidad de supervisión 5, que inicialmente puede realizar una función de seguridad entre la entrada 1 y la salida 2. Sin embargo, un fallo en la unidad de supervisión 5 también puede conducir a un fallo de la función de seguridad. Un canal de supervisión y diagnóstico adicional 6 asegura que un fallo en la unidad de supervisión 5 conduce a un estado seguro del sistema. Por un lado, el canal de supervisión y diagnóstico 6 tiene la tarea de detectar los errores que se producen en la unidad de supervisión 5. Por otro lado, el canal de supervisión y diagnóstico 6 tiene la tarea de lograr una desconexión segura por medio de una medida adicional. La eficacia de la medida depende de la capacidad de diagnóstico del canal de supervisión y diagnóstico 6.

La figura 3 muestra una arquitectura redundante múltiple 1oo3 (one out of three) con una salida 2. La avería de uno o dos canales 7, 8, 9 de la supervisión conduce a una desconexión de seguridad por parte del tercer canal funcional. Pueden ocurrir hasta dos fallos independientes en las unidades de supervisión. Entonces todavía puede realizarse una desconexión de seguridad del proceso. Sin embargo, esto requiere al menos tres unidades de supervisión independientes 7, 8, 9. En el caso más simple, las unidades de supervisión están diseñadas de forma redundante. Se ha previsto otras variantes, tales como funciones inversamente redundantes o aquellas que cuentan con dispositivos de diagnóstico, que también se pueden usar.

De lo anterior se deduce que el esfuerzo en la arquitectura aumenta si, a pesar de varios fallos, se debe alcanzar una instalación o un estado de funcionamiento seguro.

Uno de los objetos de la presente revelación es proporcionar una arquitectura de seguridad que garantice la seguridad frente a fallos para dos fallos independientes. No es necesario ningún otro funcionamiento después de que se haya producido el primer fallo. Por lo tanto, la arquitectura no tiene que ser necesariamente tolerante a los fallos. Un fallo independiente adicional no debe conducir a una condición insegura del sistema. La arquitectura también debe tener una estructura eficiente y rentable.

Para poder reducir las unidades funcionales, no todas las unidades de supervisión deben ejecutarse repetidas veces. Por ejemplo, la comparación de resultados en la estructura de seguridad se puede llevar a cabo poco antes de que se emitan las señales de resultados. En este caso, se requiere un desembolso correspondientemente alto en las unidades de supervisión (véase la figura 3) en todos los canales.

El resultado de un cálculo complejo, por ejemplo, solo puede representar una señal de validación. En tal caso, el procesamiento posterior de la señal puede reducirse a la consideración a prueba de fallos de las señales de autorización. La tramitación correcta del procesamiento de la señal puede, por lo tanto, ser supervisada en forma reducida.

La arquitectura según la presente divulgación además tiene en cuenta que el sistema solo debe ejecutarse a prueba de fallos. La tolerancia a los fallos no es obligatoria. En consecuencia, se puede realizar una desconexión de seguridad y, si es necesario, un bloqueo después de que se haya producido un primer error.

Un requisito previo para una arquitectura de seguridad que sea económica es la reducción de los bloques de funciones a las unidades mínimas requeridas. La arquitectura 1oo1D de la figura 2 proporciona una base para esto. Los errores iniciales de la unidad de supervisión 5 son detectados por el canal de supervisión y diagnóstico 6. Son controlados mediante una desconexión de seguridad a través del canal de supervisión y diagnóstico 6. La capacidad de diagnóstico debe ser de tan alta calidad (confiable) que los errores que se produzcan sean detectados de manera segura.

En otras palabras, la capacidad de diagnóstico debe evitar y/o preferiblemente excluir los errores del primer tipo, es decir, la no detección de los errores que se producen. Al mismo tiempo, la capacidad de diagnóstico debe evitar y/o preferiblemente excluir los errores del segundo tipo, es decir la detección de no errores como errores. Según una forma de realización especial, se proporciona el reconocer errores en el canal de supervisión y diagnóstico 6 mediante la comprobación de los resultados del diagnóstico.

Como se muestra en la figura 4, todas las señales estáticas 10 se hacen dinámicas mediante señales de prueba adicionales 11. El objetivo es la capacidad de prueba continua. Por lo tanto, la arquitectura de seguridad puede realizar comprobaciones de valores discretos y de tiempo discretos en los bloques de función.

En la figura 5 se ilustran las medidas de la unidad de supervisión en el caso de las señales de salida 13. Las señales de salida 13 se realimentan, para fines de control, como señales de entrada 12 de la unidad de supervisión 4b. Reciben la dinamización correspondiente por medio de las señales de prueba 14. Esto significa que la unidad de supervisión también puede controlar inicialmente las señales estáticas.

La figura 4 y 5 se refieren así a la dinamización por medio de señales de prueba. El dispositivo de supervisión 30 del dispositivo de seguridad que se describe en detalle a continuación está diseñado preferentemente para dinamizar al menos una señal de salida 31, 37 del dispositivo de supervisión con fines de control por medio de señales de prueba. El bloque de prueba 34 del dispositivo de seguridad que se describe en detalle a continuación está diseñado preferentemente para dinamizar al menos una señal de salida 35 del bloque de prueba 34 con fines de control por medio de señales de prueba. La etapa de salida 38 del dispositivo de seguridad que se describe en detalle a continuación está diseñada preferentemente para dinamizar al menos una señal de salida 39 de la etapa de salida 38 con fines de control por medio de señales de prueba.

La retroalimentación de la señal en la figura 5 tiene lugar después de un controlador de salida y/o contacto de relé 19 disponible opcionalmente. De esta manera, el valor en el terminal de salida puede ser supervisado.

Según la figura 6, las señales de datos digitales entre las unidades funcionales individuales 17, 18 están protegidas contra la distorsión mediante medidas de seguridad adicionales. Los datos de prueba adicionales 16 se agregan a los datos de usuario 15. Esto crea una redundancia adicional y un mecanismo de control efectivo. Las unidades de transmisión y recepción pueden realizar el mismo procedimiento de cálculo o un cálculo redundante inverso.

Según la figura 7, las señales analógicas 28 relevantes para la seguridad pueden ser suministradas a la arquitectura de seguridad mediante convertidores analógicos/digitales redundantes y/o de un solo canal, a través de un multiplexor de señales. Según una forma de realización particular, una señal de referencia definida 27a, 27b está conectada a la entrada analógica del convertidor A/D de la unidad de supervisión para las señales analógicas 29 a través de una referencia de voltaje variable con el fin de probar la funcionalidad. A continuación, se realiza una prueba.

Con la ayuda de esta dinamización de las señales de la interfaz, todas las señales de entrada de un solo canal tienen una opción de control adicional. Las señales de salida se pueden controlar por medio de la retroalimentación a las entradas.

Para poder reconocer otros segundos fallos que se producen aleatoriamente, la arquitectura 1oo1D 30 de la figura 8 genera otras dos señales de control 32, 33 para la señal de salida real 31. Las señales de control 32, 33 indican por lo tanto que no hay fallos. Al menos una señal de control es una señal que cambia dinámicamente. Al menos una señal que cambia dinámicamente puede verificarse mediante otro bloque de prueba 34.

Según la figura 8, el bloque de prueba 34 comprende un canal de supervisión y diagnóstico 53. Preferentemente el bloque de prueba 34 tiene un canal de supervisión y diagnóstico 53 con al menos una entrada, en el que al menos una entrada del canal de supervisión y diagnóstico 53 del bloque de prueba 34 se configura para recibir al menos una 32 de las señales de salida de la unidad de supervisión 30.

Las señales de control 32 contienen valores de datos que se determinan según un método de cálculo y un mecanismo de control temporal. El mecanismo de control temporal permite un control temporal y lógico. La señal de control cambia su valor de datos según un algoritmo definido. Esto asegura una alta protección (dinámica) contra la falsificación.

Según una forma de realización preferente, la señal de control 32 se realiza mediante una supervisión de preguntas y respuestas. Al mismo tiempo el otro bloque de prueba 34 genera un valor binario de 4 bits. El valor binario de 4 bits se transmite a la arquitectura 30 1oo1D a petición. El valor binario de 4 bits cambia después de cada prueba exitosa de acuerdo con el esquema:

XOR de los valores de bit X3, X4. Está integrado en X1 usando un comando de desplazamiento. Esto le da a la arquitectura 1oo1D 30 una tarea cambiante con una circulación de 16 valores. Como respuesta a cada tarea (valor de 4 bits), la arquitectura 1oo1D 30 debe enviar tres respuestas consecutivas (valores de 8 bits) al bloque de prueba 34 dentro de una ventana Watchdog y a continuación una respuesta fuera de la ventana Watchdog. Las respuestas son valores fijos y se comprueban mediante el bloque de verificación 34. Después de cuatro ciclos exitosos, se libera la señal de salida 35.

Según la figura 8, la unidad de supervisión 30 comprende un canal de supervisión y diagnóstico 6. Por lo tanto, la unidad de supervisión 30 tiene preferentemente un canal de supervisión y diagnóstico 6 con al menos una salida, en el que la salida del canal de supervisión y diagnóstico 6 de la unidad de supervisión 30 está diseñada para proporcionar al bloque de prueba 34 al menos una señal de control 33. La arquitectura de la unidad de supervisión 30 corresponde, en particular, preferentemente a una arquitectura 1oo1D.

Para demostrar la efectividad del bloque de prueba 34, las señales de control 32 y 33 se cambian cíclicamente en una señal de fallo por la arquitectura 1oo1D 30. Esto da como resultado una señal de salida 35. Esto es verificado por otro comparador 36 con una señal 37 generada de forma diversa.

En otras palabras, la presente revelación se refiere a un dispositivo de seguridad que comprende una unidad de supervisión 30, un bloque de prueba 34 y una etapa de salida 38 con al menos un elemento de contacto &41, en la que la unidad de supervisión 30 tiene al menos dos, preferiblemente al menos tres, salidas y está configurada para proporcionar al menos dos 32, 37 , preferiblemente al menos tres 31, 32, 37, señales de salida diferentes para comprobar que están libres de fallos.

Si las señales son correctas, la señal de resultado conduce a la validación a través de una etapa de salida 38 construida de forma redundante.

En otras palabras, la etapa de salida 38 proporciona una función de desconexión, teniendo en cuenta el resultado del enlace hecho por el elemento de contacto & 41 y el control de señal de los bloques 30 y 34.

En consecuencia, el bloque de prueba 34 está preferentemente configurada para proporcionar al menos una señal de retroalimentación 35 para la unidad de supervisión 30.

La unidad de supervisión 30 está preferentemente configurada para cambiar cíclicamente al menos una 32 de las señales de salida de la unidad de supervisión 30 en una señal de fallo con el fin de probar la efectividad del bloque de prueba 34.

La unidad de supervisión 30 también está preferentemente configurada para modificar cíclicamente la señal de control 33, en al menos una salida del canal de supervisión y diagnóstico 6 de la unidad de supervisión 30, en una señal de fallo con el fin de probar la eficacia del bloque de prueba 34.

Se puede lograr un estado de sistema seguro en aplicaciones, como, por ejemplo, la tecnología de combustión, al interrumpir la alimentación de corriente y/o el abastecimiento de energía y/o el suministro eléctrico de los actuadores conectados. La alimentación de corriente y/o el abastecimiento de energía y/o el suministro eléctrico se desconectan mediante elementos de contacto dispuestos en serie. El desbloqueo ocurre preferentemente solo cuando todos los elementos de contacto están cerrados.

Los valores de salida de todas las etapas de salida 38 se suministran a la arquitectura 1oo1D 30 como señales (dinámicas) 39. Esto crea un circuito de supervisión de seguridad (dinámico). Las señales 39 pueden retroalimentarse individualmente o como una señal común.

Un fallo que se produce conduce a una desconexión de seguridad (del sistema).

Preferentemente, el al menos un elemento de contacto &41 de la etapa de salida 38 está así en un estado ABIERTO o CERRADO, y la etapa de salida 38 tiene al menos una salida y está configurada para proporcionar el estado del al menos un elemento de contacto &41 como señal de retroalimentación 39 para la unidad de supervisión 30.

Preferentemente, la unidad de supervisión 30 tiene al menos una entrada y la al menos una entrada de la unidad de supervisión 30 está configurada para recibir una señal de retroalimentación 39 de la etapa de salida 38.

La validación del elemento de contacto 40 tiene lugar directamente desde la arquitectura 1oo1D 30. El elemento de contacto &41 está controlado por dos señales de validación (dinámicas) del bloque de prueba 34 y desde la arquitectura 1oo1D 30. La señal de validación para el elemento de contacto &42 requiere la dinámica del bloque de prueba 34 y de la arquitectura 1oo1D 30.

En otras palabras, la presente descripción se refiere a un dispositivo de seguridad, en el que la unidad de supervisión 30 está configurada para proporcionar al menos una señal de validación 37 para una función de desconexión, y en el que el bloque de prueba 34 está configurado para proporcionar al menos una señal de validación para una función de desconexión y en el que el bloque de prueba 34 tiene al menos una entrada y está diseñado para supervisar al menos una 32 de las señales de salida de la unidad de supervisión 30.

Con otras palabras, el bloque de prueba 34 tiene al menos una salida y está configurado para proporcionar al menos una señal de validación 35 para una función de desconexión.

Con otras palabras, el al menos un elemento de contacto &41 de la etapa de salida 38 tiene al menos dos entradas y está configurado para combinar al menos una 37 de las señales de salida de la unidad de supervisión 30 con la al menos una señal de validación del bloque de prueba 34 para producir un resultado.

Preferentemente, la etapa de salida 38 tiene al menos otro elemento de contacto 40 con una entrada, por lo que el al menos otro elemento de contacto 40 de la etapa de salida 38 está diseñado para ser validado directamente por una 31 de las señales de salida de la unidad de supervisión 30.

La etapa de salida (38) particularmente cumple su función de desconexión, teniendo en cuenta la validación del elemento de contacto 40.

Las extensiones son posibles y/o están previstas en forma paralela de elementos de contacto a elementos de contacto &42. Para este propósito, se requieren varios controles de la arquitectura 1oo1D 30. La señal de validación 35 se puede usar varias veces.

Por lo tanto, el principio de supervisión es que solo un sistema general sin fallos puede conducir a la validación del sistema. Incluso los fallos iniciales conducen a una función de desconexión por diferentes circuitos de supervisión de seguridad.

Con la ayuda de esta arquitectura construida se pueden manejar varias funciones relevantes para la seguridad en un sistema. Esto hace posible supervisar un gran número de señales de entrada realizadas de manera diferente. Así pues, un fallo en el sistema de supervisión y/o la aparición de un evento relevante para la seguridad conduce a una reacción del sistema relacionada con la seguridad.

La complejidad de las unidades de supervisión se reduce a una simple función de desconexión redundante. Esto permite ahorrar en comparación con las arquitecturas de seguridad completamente redundantes.

En la realización práctica según la figura 9, la arquitectura 1oo1D 30 se realiza mediante una arquitectura lockstep integrada (un procesador redundante (multinúcleo) 44). El procesador redundante (multinúcleo) comprende aquí, además de las tres unidades de supervisión 45, 46, 47, un procesador principal 48 y un procesador de prueba 49. También está presente un elemento de comparación 50.

El procesador redundante (multinúcleo) 44 se caracteriza porque el procesamiento de señales relevantes para la seguridad se lleva a cabo en un canal de función supervisado. La supervisión y el diagnóstico son de tan alta calidad que los fallos pueden detectarse de manera segura.

Se pueden instalar procesadores 44 redundantes adecuados (múltiples núcleos) de Texas Instruments (serie Hercules TMS570, RM4x), Freescale (serie MPC564x, SPC5744x) o STM (serie SPC56EL54). Esta lista no pretende ser completa.

Se generan varias señales diferentes 32, 33 desde el procesador 44 redundante (multi-núcleo). Estos son verificados por un bloque de prueba 34. El bloque de prueba 34 puede implementarse en la práctica mediante un circuito integrado. El circuito integrado realiza, por ejemplo, un control discreto del tiempo y valor de la señal de control (dinámica) 32. Como resultado, se genera la señal de validación 35. La señal de validación 35 tiene una dinámica definida.

Los bloques de supervisión adecuados 34 están disponibles, por ejemplo, en Texas Instruments (TPS65381) o Freescale (MC33908). Esta lista no pretende ser completa.

Esta dinámica es necesaria para la validación y/o control de los elementos de contacto &41 y &42 en la etapa de salida 38. Esto da como resultado la dependencia según la cual el resultado de la primera unidad 30 se verifica cíclicamente por la segunda unidad 34. Se requiere un resultado de prueba (generado dinámicamente) para validar los elementos de contacto &41 y &42 en la etapa de salida 38 junto con al menos una señal de control (dinámica) de la arquitectura 1oo1D 30.

Preferentemente, la unidad de supervisión 30 tiene por lo tanto al menos una entrada y la al menos una entrada de la unidad de supervisión 30 está configurada para recibir la señal de retroalimentación 35 del bloque de prueba 34 y la unidad de supervisión 30 está configurada para utilizar la señal de retroalimentación 35 del bloque de prueba 34, que sigue a una señal 32, 33 de la unidad de supervisión 30 que se ha modificado en una señal de fallo, con el fin de probar la eficacia del bloque de prueba 34.

Preferentemente, en este caso, la etapa de salida 38 está configurada para vincular la señal de retroalimentación 35 del bloque de prueba con una señal de salida de la unidad de supervisión por medio de un elemento de contacto &42 para desconectar y/o bloquear por medio del elemento de contacto &42 de la etapa de salida si se comprueba que el bloque de prueba 34 es ineficaz.

Preferentemente, la unidad de supervisión 30 está diseñada también para proporcionar una señal de salida 31, 37 en el caso de que el bloque de prueba 34 sea ineficaz, de tal manera que la recepción de la señal de salida 31, 37 por un elemento de contacto &41 de la etapa de salida 38 active la función de desconexión de la etapa de salida 38.

Según una forma de realización preferente, la etapa de salida 38 se bloquea en caso de que se produzca un fallo en la unidad de diagnóstico y supervisión. De esta manera, antes de que se produzca un fallo múltiple, se almacena un indicador de fallo en el área de memoria del procesador (multinúcleo) 44 y/o en una memoria externa (preferentemente no volátil). El contenido de esta área de memoria está integrado en la generación de la señal de control 32. En consecuencia, en el caso de un fallo múltiple en la arquitectura 1oo1D 30, se puede producir un bloqueo de seguridad en el bloque de prueba 34 y la etapa de salida 38.

Preferentemente, el dispositivo de supervisión 30 está, por lo tanto, configurado para almacenar una señal de salida 31, 37, que es adecuada para activar la función de desconexión de la etapa de salida 38, interna o externa y volátil o no volátil. Además, el dispositivo de supervisión 30 está diseñado preferentemente para leer dicha señal de una memoria interna o externa y volátil o no volátil. El dispositivo de supervisión 30 también está diseñado preferentemente para evaluar una señal leída de esta manera desde una memoria. El dispositivo de supervisión está especialmente configurado para establecer al menos una señal de salida 31, 37 como resultado de la evaluación de la señal de lectura de modo que la función de desconexión de la etapa de salida 38 se active y/o permanezca activada. Por lo tanto, la etapa de salida está bloqueada o permanece bloqueada.

Lo mismo se aplica independientemente de esto, también a la etapa de salida 38 y su señal o sus señales de salida 39. La etapa de salida 38 también está diseñada preferentemente para el almacenamiento, la lectura y la evaluación de una señal con respecto al bloqueo.

Según la figura 10, las señales analógicas relevantes para la seguridad pueden ser suministradas a la arquitectura de seguridad, ya sea mediante convertidores analógico/ digitales redundantes 51, 52 y/o mediante un solo canal a través de un multiplexor de señales. Para probar la funcionalidad, una señal de referencia definida 27 se conecta a la entrada analógica del convertidor A/D a través del bloque de prueba 34 y/o a través de una referencia de voltaje variable. El resultado de la prueba se puede vincular a la generación de la señal de validación 32 de la misma manera que antes. Las señales de referencia pueden conectarse directamente a las variables de entrada analógica y/o mediante multiplexores de señal. Se mantienen los principios de las pruebas dinámicas.

Preferentemente, la unidad de supervisión 30 tiene por lo tanto al menos una entrada para recibir señales relevantes para la seguridad. Preferentemente, la unidad de supervisión 30 comprende al menos un convertidor analógico/digital 51, 52 para suministrar al menos una señal analógica relevante para la seguridad.

Se prevé utilizar una arquitectura de seguridad según la presente divulgación también para el control y/o la regulación, así como la supervisión de pilas de combustible. Ese uso puede referirse tanto a las celdas de combustible de óxido sólido como también a las celdas de combustible de electrolitos de polímero. También se contempla el uso de la arquitectura de seguridad según la presente divulgación para el control y/o la regulación, así como para la supervisión de baterías. Esto implica en particular el control y/o la regulación, así como la supervisión de las baterías de flujo redox como, por ejemplo, los acumuladores redox de vanadio, los acumuladores redox de bromuro de sodio y/o los acumuladores de zinc-bromo. También se proporciona el control y/o regulación, así como la supervisión de las baterías de flujo redox basadas en quinonas orgánicas.

Las partes de una arquitectura de seguridad o de un procedimiento según la presente revelación pueden implementarse como hardware, como un módulo de software ejecutado por una unidad informática, o por medio de un ordenador en la nube o por medio de una combinación de las opciones antes mencionadas. El software puede incluir un firmware, un controlador de hardware que se ejecuta dentro de un sistema operativo o un programa de aplicación. Por lo tanto, la presente revelación se refiere también a un producto de programa informático que contiene las características de esta revelación o realiza los pasos necesarios. Cuando se implementa como software, las funciones descritas se pueden almacenar como uno o más comandos en un medio legible por ordenador. Algunos ejemplos de medios legibles por ordenador son la memoria de acceso aleatorio (RAM), la memoria magnética de acceso aleatorio (MRAM), la memoria de solo lectura (ROM), la memoria flash, la ROM programable electrónicamente (EPROM), la ROM programable y borrable eléctricamente (EEPROM), los registros de una unidad informática, un disco duro, un dispositivo de almacenamiento extraíble, una memoria óptica o cualquier otro medio adecuado al que pueda accederse por medio de un ordenador u otros dispositivos y aplicaciones de TI.

Lo anterior se refiere a formas de realización individuales de la revelación. Se pueden hacer varios cambios a las formas de realización sin apartarse de la idea subyacente y sin apartarse del alcance de esta revelación. El objeto de la presente revelación está definido por sus reivindicaciones. Se pueden hacer varios cambios sin salir del alcance de protección de las siguientes reivindicaciones.

Signos de referencia

1 Entrada

2 Salida

3 Unidad de supervisión

4a Unidad de supervisión

4b Unidad de supervisión

5 Unidad de supervisión

6 Canal de supervisión y diagnóstico

7 Canal de supervisión

8 Canal de supervisión

9 Canal de supervisión

10 Señal estática, señales estáticas

11 Señal de prueba adicional, señales de prueba adicionales

12 Señal o señales de entrada

13 Señal o señales de salida

14 Señal o señales de prueba

15 Datos de usuario

16 Datos de prueba

17 Unidad funcional

18 Unidad funcional

19 Controlador de salida y/o contacto de relé

27, 27a, 27b Señal o señales de referencia

28 Señal o señales analógicas relevantes para la seguridad

29 Unidad de supervisión de señales analógicas

30 Arquitectura (1oo1D)

31 Señal de salida

32 Señal de control adicional

33 Señal de control adicional

34 Bloque de prueba

35 Señal de salida

36 Comparador adicional

37 Señal generada de forma diversa

38 Etapa de salida

39 Señal de retroalimentación (dinámica)

40 Elemento de contacto

&41 Elemento de contacto

&42 Elemento de contacto

44 Procesador (multinúcleo)

45 Unidad de supervisión

46 Unidad de supervisión

47 Unidad de supervisión

48 Procesador principal

49 Procesador de prueba

50 Elemento de comparación

51 Convertidor A/D

52 Convertidor A/D

53 Canal de supervisión y diagnóstico

REIVINDICACIONES

1. Instalación de quemador, en particular sistema de quemador de gas o sistema de quemador de fuel, con un dispositivo de seguridad, dicho dispositivo de seguridad comprende una unidad de supervisión (30), un bloque de prueba (34) y una etapa de salida (38) que tiene al menos un elemento de contacto (&41), en el que la unidad de supervisión (30) tiene al menos dos, preferentemente al menos tres salidas, y está configurada para proporcionar al menos dos (32, 37), preferentemente al menos tres (31, 32, 37) señales de salida diferentes para comprobar que no tienen fallos, en el que la unidad de supervisión (30) está configurada para proporcionar al menos una señal de salida como señal de validación (37) para una función de desconexión, en el que el bloque de prueba (34) tiene al menos una entrada y está configurada para supervisar al menos una (32) de las señales de salida de la unidad de supervisión (30), en el que el bloque de prueba (34) tiene al menos una salida y está configurada para proporcionar al menos otra señal de validación para la función de desconexión, caracterizada porque, el al menos un elemento de contacto (&41) de la etapa de salida (38) tiene al menos dos entradas y está configurado para vincular al menos una (37) de las señales de salida de la unidad de supervisión (30) con al menos una señal de validación adicional del bloque de prueba (34) para obtener un resultado y que la etapa de salida (38) comprende la función de desconexión y la función de desconexión está diseñada para ser activada teniendo en cuenta el resultado del enlace realizado por el elemento de contacto (&41).

2. Instalación de quemador según la reivindicación 1, en el que el bloque de prueba (34) tiene un canal de supervisión y diagnóstico (53) con al menos una entrada, y en el que al menos una entrada del canal de supervisión y diagnóstico (53) del bloque de prueba (34) está configurada para recibir al menos una (32) de las señales de salida de la unidad de supervisión (30).

3. Instalación de quemador según una de las reivindicaciones 1 o 2, en el que la unidad de supervisión (30) tiene un canal de supervisión y diagnóstico (6) con al menos una salida, y en el que la al menos una salida del canal de supervisión y diagnóstico (6) de la unidad de supervisión (30) está configurada para proporcionar al menos una señal de control (33) para el bloque de prueba (34).

4. Instalación de quemador según una de las reivindicaciones 1 a 3, en el que la etapa de salida (38) tiene al menos un elemento de contacto adicional (40) con una entrada, en el que el al menos un elemento de contacto adicional (40) de la etapa de salida (38) está configurado para ser validado directamente por una (31) de las señales de salida de la unidad de supervisión (30).

5. Instalación de quemador según la reivindicación 4, en el que la etapa de salida (38) está configurada para activar su función de desconexión teniendo en cuenta la validación del elemento de contacto (40).

6. Instalación de quemador según una de las reivindicaciones 1 a 5, en el que el bloque de prueba (34) está configurado para proporcionar una señal de retroalimentación (35) a la unidad de supervisión (30).

7. Instalación de quemador según una de las reivindicaciones 1 a 6, en el que la unidad de supervisión (30) está configurada para cambiar cíclicamente al menos una (32) de las señales de salida de la unidad de supervisión (30) en una señal de fallo con el fin de probar la efectividad del bloque de prueba (34).

8. Instalación de quemador según la reivindicación 3, en el que la unidad de supervisión (30) está configurada para cambiar cíclicamente la señal de control (33) en al menos una salida del canal de supervisión y diagnóstico (6) de la unidad de supervisión (30), en una señal de fallo con el fin de probar la eficacia del bloque de prueba (34).

9. Instalación de quemador según la reivindicación 6 y según una de las reivindicaciones 7 u 8,

en el que la unidad de supervisión (30) tiene al menos una entrada y en el que la al menos una entrada de la unidad de supervisión (30) está configurada para recibir la señal de retroalimentación (35) del bloque de prueba (34) y en el que la unidad de supervisión (30) está configurada para utilizar la señal de retroalimentación (35) del bloque de prueba (34), que sigue a una señal (32, 33) de la unidad de supervisión (30) que se ha modificado en una señal de fallo, con el fin de probar la eficacia del bloque de prueba (34).

10. Instalación de quemadores según la reivindicación 9, en el que la unidad de supervisión (30) está configurada para proporcionar una señal de salida (31, 37), en caso de ineficacia probada del bloque de prueba (34), de modo que la recepción de la señal de salida (31, 37) por el elemento de contacto (&41) de la etapa de salida (38) activa la función de desconexión de la etapa de salida (38).

11. Instalación de quemador según una de las reivindicaciones anteriores, en el que el al menos un elemento de contacto (&41) de la etapa de salida (38) se encuentra en un estado ABIERTO o CERRADO, y en el que la etapa de salida (38) tiene al menos una salida y está configurada para proporcionar el estado del al menos un elemento de contacto (&41) como señal de retroalimentación (39) para la unidad de supervisión (30).

12. Instalación de quemador según la reivindicación 11, en el que la unidad de supervisión (30) tiene al menos una entrada y en el que la al menos una entrada de la unidad de supervisión (30) está configurada para recibir la señal de retroalimentación (39) desde la etapa de salida (38).

13. Instalación de quemador según una de las reivindicaciones anteriores, en el que la unidad de supervisión (30) está configurada para dinamizar al menos una señal de salida (31, 37) de la unidad de supervisión (30) con fines de control mediante señales de prueba.

14. Instalación de quemador según una de las reivindicaciones anteriores, en el que la unidad de supervisión (30) tiene al menos una entrada para recibir señales relevantes para la seguridad y en el que, preferiblemente, la unidad de supervisión (30) tiene al menos un convertidor analógico/digital (51, 52) para suministrar al menos una señal analógica relevante para la seguridad.

FIG 1

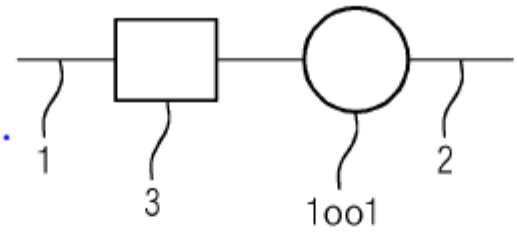


FIG 2

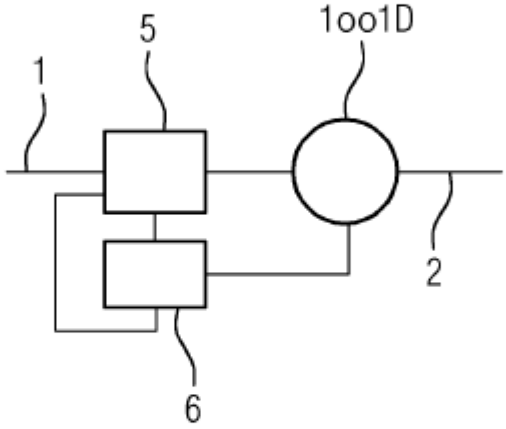


FIG 3

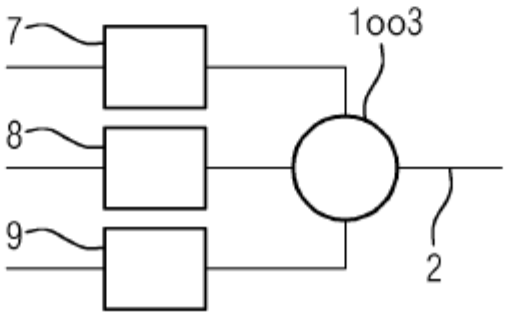


FIG 4

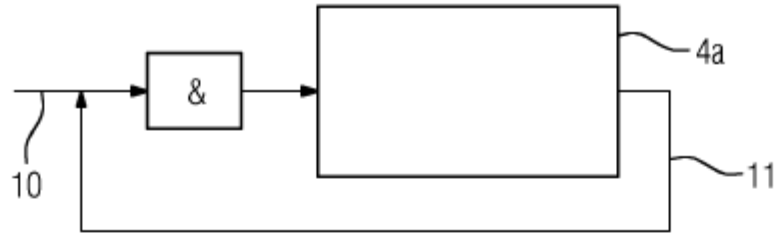


FIG 5

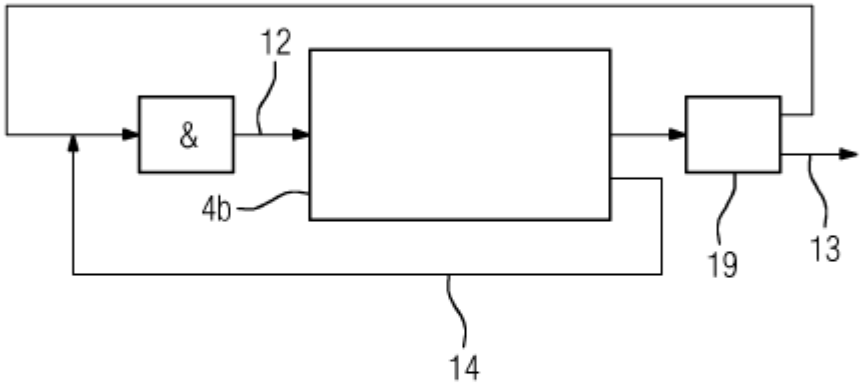


FIG 6

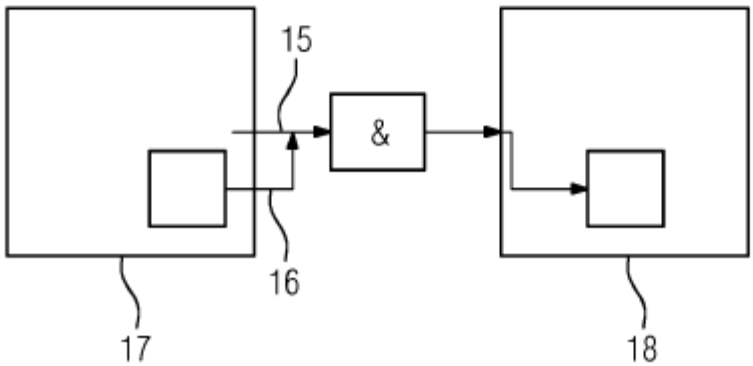


FIG 7

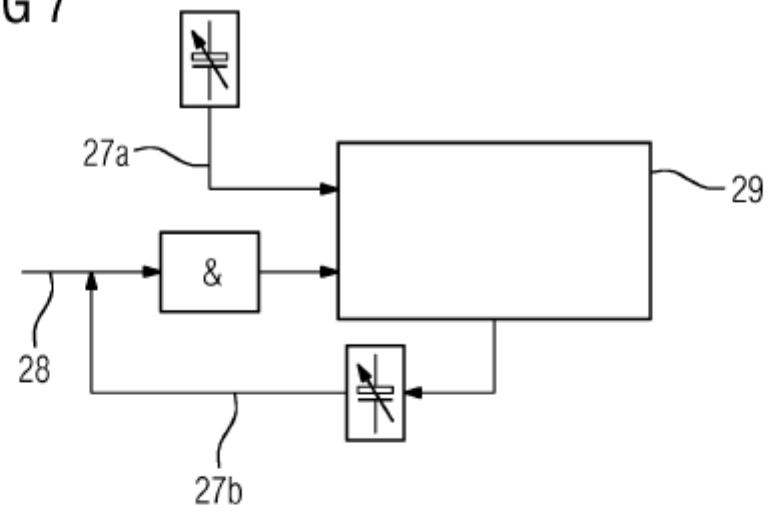


FIG 8

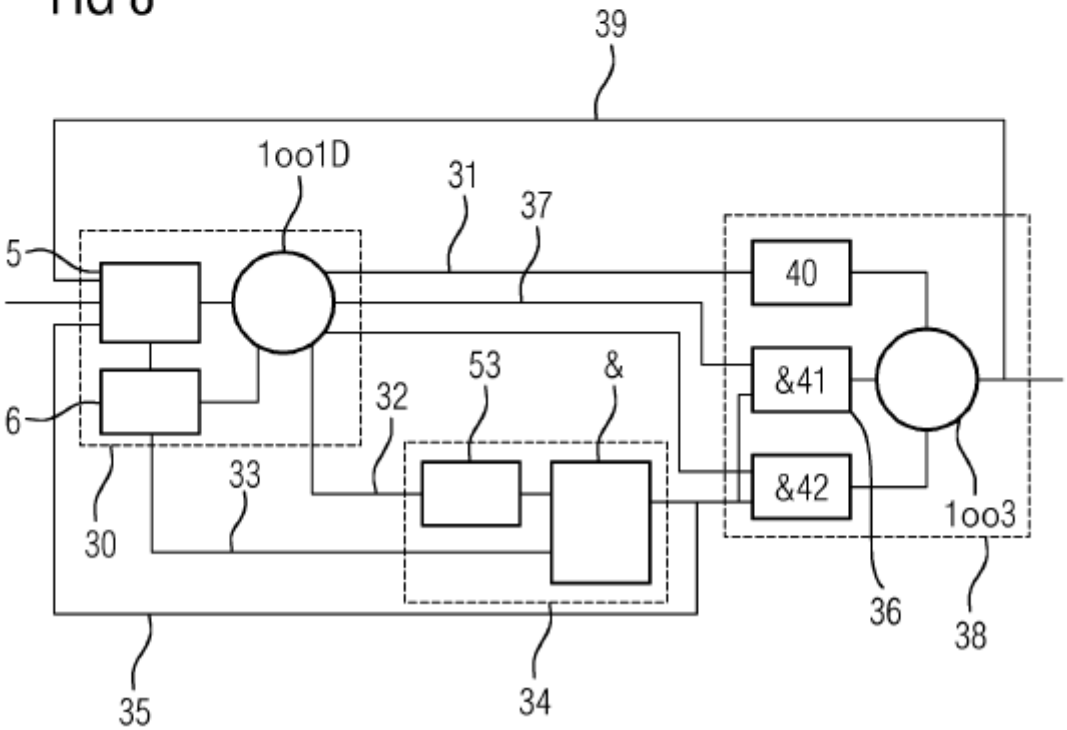


FIG 9

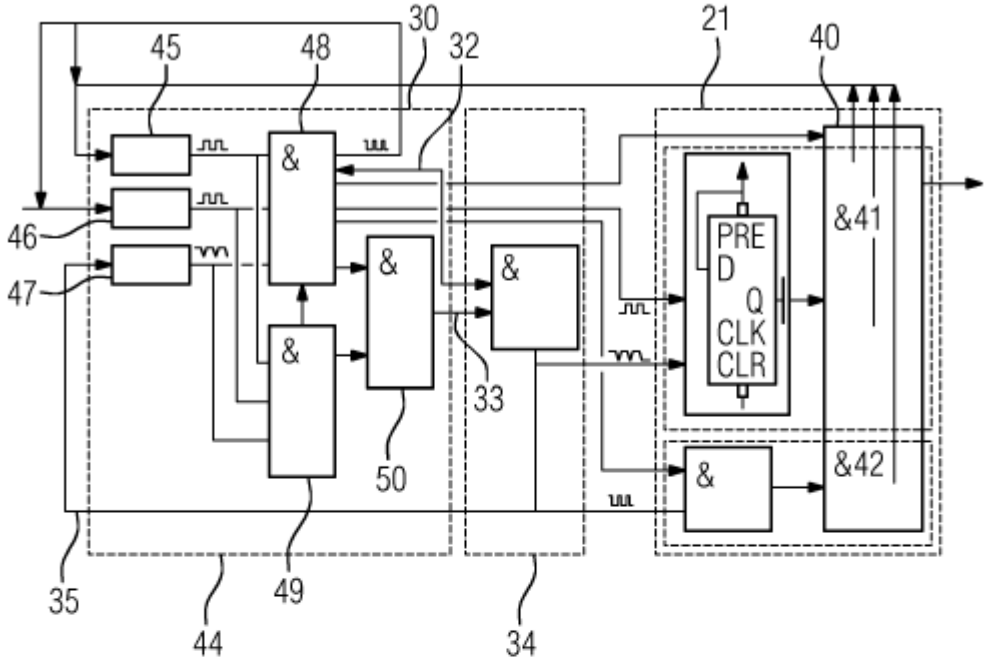
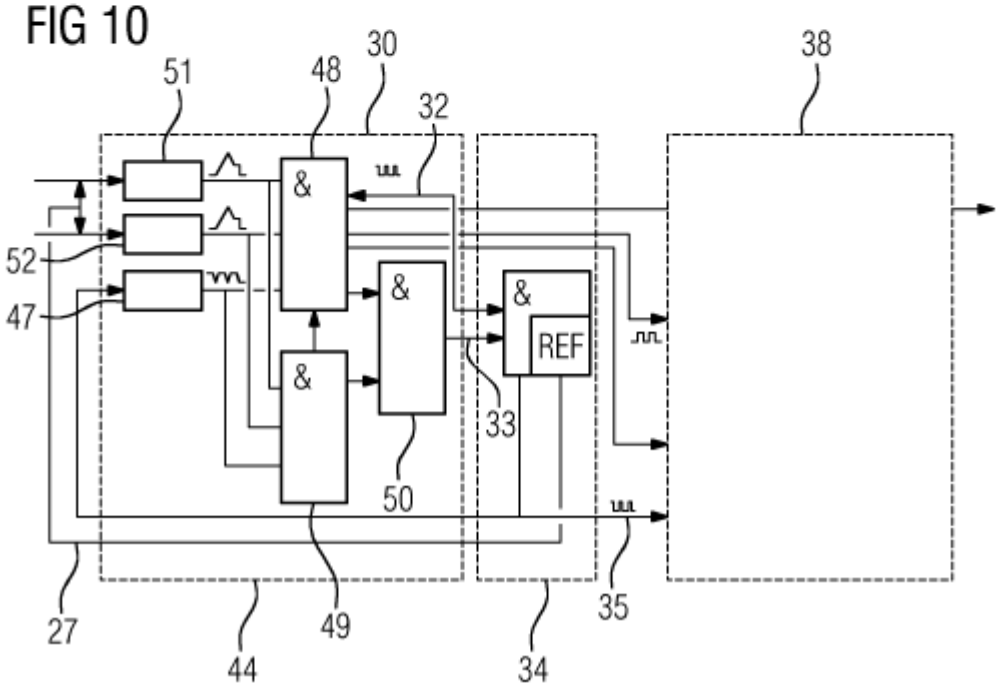

30
21
45
48
32
40
&
46
47
&
&
&
PRE
D
Q
CLK
CLR
&41
33
50
&
&42
35
49
44
34

FIG 10


30
38
51
48
32
&
52
&
&
47
&
REF
33
50
35
27
49
44
34