(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 417 309**

(51) Int. CI.:

G06F 11/10 (2006.01)
G05B 19/042 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **20.04.2010 E 10720342 (4)**

(97) Fecha y número de publicación de la concesión europea: **19.06.2013 EP 2422271**

(54) Título: **Procedimiento y dispositivo para la creación de un programa de usuario para un control de seguridad**

(30) Prioridad:

20.04.2009 DE 102009019089

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.08.2013

(73) Titular/es:

PILZ GMBH & CO. KG (100.0%)
Felix-Wankel-Strasse 2
73760 Ostfildern, DT

(72) Inventor/es:

MOOSMANN, PETER y
REUSCH, MATTHIAS

(74) Agente/Representante:

UNGRÍA LÓPEZ, Javier

DESCRIPCIÓN

Procedimiento y dispositivo para la creación de un programa de usuario para un control de seguridad.

La presente invención se refiere a un procedimiento y a un dispositivo para la creación de un programa de usuario para un control de seguridad, que está configurado para controlar una instalación automatizada con una pluralidad de sensores y una pluralidad de accionadores, presentando el control de seguridad un primer procesador y un segundo procesador, creándose un código fuente para un programa de usuario, comprendiendo el código fuente una cantidad de instrucciones de control para el control de los accionadores y procesándose para el tratamiento de las instrucciones de control variables de programa relevantes para la seguridad con ayuda del primer y del segundo procesador en modo a prueba de errores, generándose además un código máquina dependiendo del código fuente y estableciéndose al menos una suma de comprobación para al menos una parte del código máquina.

Un procedimiento de este tipo y un dispositivo correspondiente son conocidos por el documento WO 02/067065 A2.

Un control de seguridad en el sentido de la presente invención es un aparato o un dispositivo que recoge señales de entrada suministradas por sensores y, a partir de esto, mediante combinaciones lógicas y eventualmente otras etapas de procesamiento de señal o datos, genera señales de salida. Las señales de salida pueden suministrarse entonces a accionadores que, dependiendo de las señales de entrada, dan lugar a acciones o reacciones en una instalación controlada.

Un campo de aplicación preferido para tales controles de seguridad es la supervisión de pulsadores de apagado de emergencia, controles bimanuales, puertas de protección o resguardos fotoeléctricos en el ámbito de la seguridad de las máquinas. Tales sensores se usan para asegurar, por ejemplo, una máquina de la cual parte durante el funcionamiento un peligro para seres humanos o productos materiales. Al abrir la puerta de protección o al activar el pulsador de apagado de emergencia se genera respectivamente una señal que se suministra como señal de entrada al control de seguridad. Como reacción a esto, el control de seguridad desconecta entonces, por ejemplo, con ayuda de un accionador, la parte de la máquina que genera peligro.

En un control de seguridad, a diferencia de un control "normal", es característico que el control de seguridad garantiza siempre un estado seguro de las instalaciones o máquinas que generan peligro, incluso cuando en el mismo o en un aparato unido con el mismo aparece un mal funcionamiento. Por tanto, en controles de seguridad se plantean requisitos extremadamente elevados a la propia seguridad contra errores, lo que tiene como consecuencia una considerable complejidad durante el desarrollo y la producción.

Por norma general, los controles de seguridad necesitan, antes de su uso, una autorización particular por las autoridades de inspección competentes, tales como, por ejemplo, en Alemania por las asociaciones profesionales o el servicio de inspección técnica (TÜV). A este respecto, el control de seguridad tiene que cumplir estándares de seguridad predefinidos que están consignados, por ejemplo, en la norma europea EN 954-1 o una norma comparable, por ejemplo, la norma IEC 61508 y o la norma EN ISO 13849-1. En lo sucesivo, por tanto, por un control de seguridad se entiende un aparato o un dispositivo que cumple al menos la categoría de seguridad 3 de la norma europea mencionada EN 954-1 o cuyo Nivel de Integridad de Seguridad (SIL) alcanza al menos el nivel 2 de acuerdo con la norma mencionada IEC 61508.

Un control de seguridad programable ofrece al usuario la posibilidad de fijar individualmente las combinaciones lógicas y, dado el caso, otras etapas de procesamiento de señal o datos con ayuda de un software, el denominado programa de usuario, de forma que se corresponda a sus necesidades. A partir de esto resulta una gran flexibilidad en comparación con soluciones anteriores, en las que las combinaciones lógicas se generaron mediante una conexión alámbrica definida entre distintos elementos de seguridad. Un programa de usuario se puede crear, por ejemplo, con ayuda de un ordenador personal (PC) disponible en el mercado y mediante el uso de programas de software organizados correspondientemente.

Como se ha mencionado anteriormente, los controles de seguridad antes de su uso necesitan una autorización particular por una autoridad de inspección competente. En una autorización de este tipo se verifica el contenido relevante para la seguridad del programa de usuario. En el caso del contenido relevante para seguridad del programa de usuario se trata de las instrucciones de seguridad que se requieren para las tareas de seguridad a realizar por el control de seguridad. Para el tratamiento de las instrucciones de seguridad se procesan en modo a prueba de errores las variables del programa relevantes para la seguridad. Después de la verificación realizada se establece para el contenido relevante para la seguridad del programa de usuario, particularmente para el contenido relevante para la seguridad del código máquina, una suma de comprobación y este contenido relevante para la seguridad se sella con la suma de comprobación. Mediante la suma de comprobación, la autoridad de inspección, después de la validación realizada puede reconocer cambios realizados en el contenido relevante para la seguridad del programa de usuario. De este modo se pueden comprobar, por ejemplo, manipulaciones inadmisibles en el contenido relevante para la seguridad de un programa de usuario.

Si después de la autorización realizada por la autoridad de inspección se llevan a cabo cambios en el contenido relevante para la seguridad de un programa de usuario existente, por ejemplo, para optimizar la aplicación que se está ejecutando en la instalación controlada, se requiere una nueva autorización por la autoridad de inspección del programa de usuario cambiado. Ya que el contenido relevante para la seguridad de un programa de usuario comprende también instrucciones de diagnóstico, también se requiere una nueva autorización cuando se llevan a cabo posteriormente solo cambios en tales instrucciones de diagnóstico. A este respecto, no es infrecuente llevar a cabo, después de la autorización realizada, cambios en las instrucciones de diagnóstico. Por ejemplo, solo con motivo de un funcionamiento de prueba de la instalación se obtienen conclusiones que requieren una adaptación de las instrucciones de diagnóstico. Ya que las instrucciones de diagnóstico en sí no son relevantes para la seguridad, a diferencia de las instrucciones de control de seguridad, es desventajoso que se requiera una nueva autorización por una autoridad de inspección incluso en el caso de que se posteriormente lleven a cabo, después de una autorización ya realizada, solo cambios en las instrucciones de diagnóstico. Esto está asociado a un consumo de tiempo aumentado y costes adicionales. Además, esto limita la flexibilidad al proyectar una instalación a controlar y, por tanto, durante la creación de un programa de usuario.

El documento WO 02/067065 A2 mencionado al principio divulga un procedimiento para la programación de un control de seguridad, fijándose combinaciones lógicas entre señales de entrada de los controles de seguridad y asignándose productos de combinación a señales de salida del control de seguridad. La fijación de las combinaciones y la asignación se realizan mediante módulos de programa con especificidad de función predefinidos que se seleccionan de un conjunto de tales módulos de programa. Cada módulo de programa seleccionado se asigna inequívocamente a un grupo funcional definido. Cuando el programador ha seleccionado y parametrizado todos los módulos de programa necesarios, se almacena todo el programa de usuario en una memoria y se asegura allí adicionalmente con una suma de comprobación de CRC. Desde la memoria se puede transmitir entonces el programa de usuario al control de seguridad. Mediante la suma de comprobación de CRC se puede reconocer y, dado el caso, evitar una falsificación del programa de usuario durante la transmisión al control de seguridad.

El documento WO 88/09590 divulga un procedimiento para la comprobación de una señal que se transmite a través de una línea de transmisión con respecto a errores, aplicándose también en este caso una suma de comprobación de CRC.

Es un objetivo de la presente invención perfeccionar un procedimiento y un dispositivo del tipo mencionado al principio para continuar aumentando la flexibilidad durante la creación de un programa de usuario y, por tanto, la realización de un control de seguridad, para posibilitar, de este modo, una programación más rápida y económica de un control de seguridad.

Este objetivo se resuelve mediante un procedimiento y un dispositivo del tipo mencionado al principio, comprendiendo el código fuente además una cantidad de instrucciones de diagnóstico para la creación de mensajes de diagnóstico que se indican en una unidad de indicación de diagnóstico y quedando desatendidas las instrucciones de diagnóstico al establecer la suma de comprobación.

El nuevo procedimiento y el nuevo dispositivo se basan en la idea de que al establecer la suma de comprobación quedan desatendidas las instrucciones de diagnóstico. Por tanto, la suma de comprobación se establece solamente para las instrucciones de control de seguridad. Por tanto, las instrucciones de diagnóstico quedan desatendidas incluso en la suma de comprobación que se establece en el marco de la autorización por una autoridad de inspección. Por tanto, es posible poder llevar a cabo, después de la autorización realizada, cambios en las instrucciones de diagnóstico sin que esto tenga ninguna influencia sobre la suma de comprobación a crear con el fin de la verificación. Por tanto, después de la autorización o validación realizada se pueden llevar a cabo complementaciones en instrucciones de diagnóstico ya existentes antes de la autorización. Sin embargo, también es concebible crear, después de la autorización realizada, por primera vez instrucciones de diagnóstico. Esto aumenta la flexibilidad al crear un programa de usuario. Ya que los cambios en las instrucciones de diagnóstico no requieren ninguna nueva autorización del programa de usuario por una de las autoridades de inspección, por tanto, se reducen el consumo de tiempo y, como consecuencia, también los costes para la creación de un programa de usuario y, por tanto, la programación de un control de seguridad.

Por tanto, el objetivo que se ha mencionado anteriormente se resuelve por completo.

En otra configuración de la invención se marcan las instrucciones de diagnóstico.

Las instrucciones de diagnóstico marcadas se pueden reconocer inequívocamente. De este modo se asegura que las instrucciones de diagnóstico se reconozcan al establecer la suma de comprobación y, por tanto, queden definitivamente desatendidas. Esta medida da lugar a que el procedimiento de acuerdo con la invención y el dispositivo de acuerdo con la invención trabajen de forma fiable.

Preferentemente, las marcas de diagnóstico se marcan automáticamente al crear el código fuente por un programa informático usado para la creación del programa de usuario. Por tanto, el programador del programa de usuario no

tiene que realizar esto por sí mismo. Esta medida ahorra tiempo y, por tanto, costes. Además, garantiza una alta fiabilidad del procedimiento de acuerdo con la invención y del dispositivo de acuerdo con la invención.

Preferentemente, el marcaje de las instrucciones de diagnóstico se realiza mediante anteposición y posposición, respectivamente, de una marca de diagnóstico. Las instrucciones de diagnóstico, por tanto, están incluidas en dos marcas de diagnóstico o están enmarcadas por las mismas. Sin embargo, también son concebibles otras medidas para el marcaje de las instrucciones de diagnóstico. De este modo, cada instrucción de diagnóstico individual puede marcarse, por ejemplo, mediante inclusión de caracteres especiales previstos para esto.

En otra configuración de la invención, el código máquina comprende un primer código de seguridad y un segundo código de seguridad, estableciéndose para cada uno de los dos códigos de seguridad respectivamente una suma de comprobación.

Esta medida posibilita una flexibilidad particularmente alta con respecto a cambios que se llevan a cabo eventualmente después de la autorización realizada por una autoridad de inspección. Si se llevan a cabo, por ejemplo, cambios que tienen un efecto solo sobre uno de los dos canales de un control de seguridad, se requiere una nueva autorización solo para el contenido del programa de usuario que está asignado a este canal.

En otra configuración de la invención, el código máquina comprende un primer código de seguridad y un segundo código de seguridad, teniéndose en cuenta durante la generación del primer código de seguridad las instrucciones de diagnóstico y quedando desatendidas durante la generación del segundo código de seguridad.

Esta medida posee la ventaja de que uno de los dos canales del control de seguridad está completamente libre de instrucciones de diagnóstico. Por tanto, los cambios en las instrucciones de diagnóstico no tienen ningún tipo de efecto sobre este canal. Por tanto, se pueden añadir otras instrucciones de diagnóstico a instrucciones de diagnóstico ya existentes o se pueden crear en realidad por primera vez instrucciones de diagnóstico sin que esto tenga ninguna influencia sobre este canal.

Se entiende que las características que se han mencionado anteriormente y que aún se han de explicar posteriormente se pueden usar no solo en la combinación respectivamente indicada, sino también en otras combinaciones o en solitario sin apartarse del alcance de la presente invención.

Están representados ejemplos de realización de la invención en el dibujo y se explican con más detalle en la siguiente descripción. Muestran:

La Figura 1, una representación esquemática de una instalación a controlar;
La Figura 2, una representación esquemática para la explicación de la generación del código máquina y del establecimiento de sumas de comprobación.

En la Figura 1 está indicado un dispositivo de acuerdo con la invención en su totalidad con la referencia 10.

El dispositivo 10 contiene un ordenador 12 convencional con una unidad de indicación 14. En el ordenador 12 se ejecuta un programa informático 16. El programa informático 16 posibilita la creación de un programa de usuario para un control de seguridad. El programa informático 16 se denomina en la terminología técnica, por tanto, frecuentemente también herramienta de programación. El ordenador 12 puede estar realizado como PC y la unidad de indicación 14, como monitor.

En la Figura 1 está representado un circuito de seguridad indicado en su totalidad con la referencia 18, que presenta un control de seguridad 20 que está configurado para controlar una instalación automatizada indicada en su totalidad con la referencia 22. La instalación 22 automatizada comprende una pluralidad de accionadores 24 y una pluralidad de sensores 26. De forma ilustrativa está representado un consumidor 28 contenido en la instalación 22, en cuyo caso puede tratarse, por ejemplo, de un robot.

El control de seguridad 20 está estructurado de forma redundante con dos canales para conseguir la seguridad contra fallos requerida para el control de procesos o aplicaciones críticos para la seguridad. En la Figura 1, en representación de la estructura de dos canales, están representados dos procesadores separados entre sí, concretamente un primer procesador 30 y un segundo procesador 32. Los dos procesadores 30, 32 están unidos entre sí a través de una interfaz de comunicación 34 bidireccional para controlarse mutuamente y poder intercambiar datos. Preferentemente, los dos canales del control de seguridad 20 y los dos procesadores 30, 32 están estructurados de forma diversa, es decir, distinta entre sí para excluir esencialmente errores sistemáticos.

Con la referencia 36 está indicada una unidad de entrada/salida que está unida con cada uno de los dos procesadores 30, 32. La unidad de entrada/salida 36 recibe una pluralidad de señales de entrada de control 38 de la pluralidad de sensores 26 y transmite las mismas en un formato de datos adaptado a cada uno de los dos procesadores 30, 32. Además, la unidad de entrada/salida 36, dependiendo de los procesadores 30, 32, genera una pluralidad de señales de salida de control 40 con las que se controla la pluralidad de accionadores 24.

Con la referencia 42 está indicada una memoria de programa en la que se almacena el programa de usuario en forma de código máquina. El código máquina se crea con ayuda del dispositivo 10. Si la memoria de programa 42 está configurada como tarjeta electrónica, esto posibilita un intercambio sencillo del código máquina y, por tanto, del programa de usuario incluso sin conexión directa al ordenador 12. Como alternativa, la memoria de programa 42 puede estar configurada también como una memoria montada de forma fija en el control de seguridad 20, por ejemplo, una EEPROM.

El programa informático 16 facilita una superficie de usuario 44 en la unidad de indicación 14. La superficie de usuario 44 posibilita a un programador la creación de un programa de usuario. El programador crea el programa de usuario suministrando al ordenador 12 entradas a través de una unidad de entrada conectada al mismo. En el caso de la unidad de entrada puede tratarse, por ejemplo, de un teclado o un ratón. Dependiendo del lenguaje de programación que se usa para la creación del programa de usuario se diferencian los conceptos de entrada. Si se usa como lenguaje de programación, por ejemplo, Structured Text o Instruction List, se crea el programa de usuario mediante entradas textuales. Si por el contrario se usa Function Block Diagram como lenguaje de programación, entonces el programador crea el programa de usuario seleccionando, mediante el uso de un ratón, módulos de programa predefinidos que se representan, por ejemplo, mediante símbolos gráficos sobre la superficie de usuario 44.

El programa informático 16 comprende un módulo de indicación 46. Con el módulo de indicación 46 se registran y evalúan las entradas realizadas por el programador a través de la unidad de entrada. Por un lado, el módulo de indicación 46 genera un contenido de código fuente 48 que representa la respectiva entrada, que se almacena en una memoria de código fuente 50. Por otro lado, el módulo de indicación 46 da lugar a la indicación de símbolos gráficos sobre la superficie de usuario 44. Estos símbolos gráficos representan las entradas realizadas por el programador y, por tanto, el contenido de código fuente 48 generado por el módulo de indicación 46.

Cuando el programador ha llevado a cabo todas las entradas necesarias para el programa de usuario, en la memoria de código fuente 50 existe un código fuente 52. El código fuente 52 comprende una primera parte de código fuente 54 y una segunda parte de código fuente 56. La primera parte de código fuente 54 representa instrucciones de seguridad que se requieren para las tareas de seguridad a realizar por el control de seguridad 20. En el caso de las instrucciones de seguridad se trata de primeras instrucciones de control 58 para el control de accionadores. Para el tratamiento de las primeras instrucciones de control 58 se procesan en modo a prueba de errores variables de programa relevantes para la seguridad. Las primeras instrucciones de control pueden denominarse también instrucciones de control de seguridad. Además, en el caso de las instrucciones de seguridad se trata de primeras instrucciones de diagnóstico 60 para la generación de mensajes de diagnóstico. Las primeras instrucciones de diagnóstico se pueden denominar también instrucciones de diagnóstico de seguridad. La segunda parte de código fuente 56 representa instrucciones estándar que se requieren para las tareas estándar a realizar por el control de seguridad 20. En el caso de las instrucciones estándar se trata de segundas instrucciones de control 62 para el control de accionadores. Para el tratamiento de las segundas instrucciones de control 62 se procesan variables de programa no relevantes para la seguridad, no requiriéndose para las variables de programa no relevantes para la seguridad un procesamiento en modo a prueba de errores. Las segundas instrucciones de control se pueden denominar también instrucciones de control estándar. Además, en el caso de las instrucciones estándar se trata de segundas instrucciones de diagnóstico 64 para la generación de mensajes de diagnóstico. Las segundas instrucciones de diagnóstico pueden denominarse también instrucciones de diagnóstico estándar.

A partir del código fuente 52 contenido en la memoria de código fuente 50, mediante dos compiladores 66, 68 se genera un código máquina 70. El código máquina 70 se transmite a través de una pasarela 72 al control de seguridad 20 y se almacena allí en la memoria de programa 42. El código máquina 70 se genera del siguiente modo:

El código fuente 52 se suministra a un primer compilador 66. El primer compilador 66 comprende una primera unidad de generación de código máquina 74 y una primera unidad de establecimiento de suma de comprobación 76. Con la primera unidad de generación de código máquina 74 se genera una primera parte de código máquina 78. La primera parte de código máquina 78 comprende un primer código de seguridad 80 y un código estándar 82. El primer código de seguridad 80 se genera dependiendo de la primera parte de código fuente 54. El primer código de seguridad 80 comprende terceras instrucciones de control 84, las denominadas instrucciones de control de seguridad, y terceras instrucciones de diagnóstico 86, las denominadas instrucciones de diagnóstico de seguridad. Durante la generación del primer código de seguridad 80, por tanto, la primera parte de código fuente 54 se convierte por completo en código máquina, es decir, tanto las primeras instrucciones de control 58 como las primeras instrucciones de diagnóstico 60 se convierten en código máquina. Se cumple la siguiente asociación: las primeras instrucciones de control 58 existentes en el lado del código fuente se corresponden con las terceras instrucciones de control 84 existentes en el lado del código máquina. Las primeras instrucciones de diagnóstico 60 existentes en el lado del código fuente se corresponden con las terceras instrucciones de diagnóstico 86 existentes en el lado del código máquina.

El código estándar 82 se genera dependiendo de la segunda parte de código fuente 56. El código estándar 82 comprende cuartas instrucciones de control 88, las denominadas instrucciones de control estándar, y cuartas

instrucciones de diagnóstico 90, las denominadas instrucciones de diagnóstico estándar. Durante la generación del código estándar 82, por tanto, la segunda parte de código fuente 56 se convierte por completo en código máquina, es decir, tanto las segundas instrucciones de control 62 como las segundas instrucciones de diagnóstico 64 se convierten en código máquina. Se cumple la siguiente asociación: las segundas instrucciones de control 62 existentes en el lado del código fuente se corresponden con las cuartas instrucciones de control 88 existentes en el lado del código máquina. Las segundas instrucciones de diagnóstico 64 existentes en el lado del código fuente se corresponden con las cuartas instrucciones de diagnóstico 90 existentes en el lado del código máquina.

Además se suministra el código fuente 52 a un segundo compilador 68. El segundo compilador 68 comprende una segunda unidad de generación de código máquina 92 y una segunda unidad de establecimiento de suma de comprobación 94. Con la segunda unidad de generación de código máquina 92 se genera una segunda parte de código máquina 96. La segunda parte de código máquina 96 comprende un segundo código de seguridad 98. El segundo código de seguridad 98 se genera dependiendo de la primera parte de código fuente 54. La segunda parte de código fuente 56 queda desatendida. El segundo código de seguridad 98 comprende solamente quintas instrucciones de control 100, las denominadas instrucciones de control de seguridad. El segundo código de seguridad 98 no comprende ninguna instrucción de diagnóstico. Durante la generación del segundo código de seguridad 98, por tanto, no se convierte toda la primera parte de código fuente 54 en código máquina. Se convierten solamente las primeras instrucciones de seguridad 58 en código máquina. Las primeras instrucciones de diagnóstico 60 quedan desatendidas.

Con la primera unidad de establecimiento de suma de comprobación 76 se establece una primera suma de comprobación 102 para el primer código de seguridad 80. La primera suma de comprobación 102, sin embargo, se establece solamente para las terceras instrucciones de control 84 contenidas en el primer código de seguridad 80. Las terceras instrucciones de diagnóstico 86 contenidas en el primer código de seguridad 80 a este respecto quedan desatendidas. La primera suma de comprobación 102 se transmite también a través de la pasarela 72 al control de seguridad 20 y se almacena en la memoria de programa 42. Con la segunda unidad de establecimiento de suma de comprobación 94 se establece una segunda suma de comprobación 104 para el segundo código de seguridad 98. Ya que el segundo código de seguridad 98 no contiene ninguna instrucción de diagnóstico, durante el establecimiento de la segunda suma de comprobación 104 se tienen en cuenta solamente las instrucciones de control, en concreto las quintas instrucciones de control 100. La segunda suma de comprobación 104 se transmite también a través de la pasarela 72 al control de seguridad 20 y se almacena en la memoria de programa 42. Mediante las dos sumas de comprobación 102, 104 almacenadas en el control de seguridad 20 y, por tanto, introducidas, se puede comprobar en cualquier momento si el contenido relevante para seguridad del programa de usuario ejecutado por el control de seguridad 20 es idéntico al contenido relevante para la seguridad que se verificó durante la autorización por una de las autoridades de inspección y que se selló por una suma de comprobación establecida en su momento. Preferentemente también están almacenadas las sumas de comprobación establecidas en el marco de la autorización en el control de seguridad 20.

Ventajosamente, las dos unidades de generación de código máquina 74, 92 y las dos unidades de establecimiento de suma de comprobación 76, 94 están configuradas de forma diversa. Sin embargo, también es concebible que las dos unidades de establecimiento de suma de comprobación 76, 94 estén configuradas de modo idéntico. Además es concebible que esté prevista solo una única unidad de establecimiento de suma de comprobación. Con la misma se establece respectivamente una suma de comprobación tanto para el primer código de seguridad 80 generado con la unidad de generación de código máquina 74 como para el segundo código de seguridad 98 generado con la unidad de generación de código máquina 92.

En total, el código máquina 70 está compuesto del primer código de seguridad 80, el código estándar 82 y el segundo código de seguridad 98, estando asignados el primer código de seguridad 80 y el código estándar 82 al primer procesador 30. El segundo código de seguridad 98 está asignado al segundo procesador 32. El programa de usuario creado por el programador se representa en total por el código fuente 52 y el código máquina 70.

Dependiendo del avance del tratamiento del programa de usuario, en el primer procesador 30 por un lado se ejecuta una primera instrucción de seguridad 106 actual y, por otro lado, una instrucción estándar 108 actual. Esencialmente al mismo tiempo, en el segundo procesador 32 se ejecuta una segunda instrucción de seguridad 110 actual. En el caso de la primera instrucción de seguridad 106 actual puede tratarse de una instrucción de control de seguridad contenida en las terceras instrucciones de control 84 o de una instrucción de diagnóstico de seguridad contenida en las terceras instrucciones de diagnóstico 86. En el caso de la instrucción estándar 108 actual puede tratarse de una instrucción de control estándar contenida en las cuartas instrucciones de control 88 o de una instrucción de diagnóstico estándar contenida en las cuartas instrucciones de diagnóstico 90. En el caso de la segunda instrucción de seguridad 110 actual se trata de una instrucción de control de seguridad contenida en las quintas instrucciones de control 100. Las instrucciones de control de seguridad se denominan también instrucciones de control relevantes para la seguridad. Las instrucciones de control estándar se denominan también instrucciones de control no relevantes para la seguridad.

Si en el caso de la instrucción estándar 108 actual se trata de una instrucción de control estándar, entonces se intercambian primeros datos 112 no relevantes para la seguridad entre el primer procesador 30 y la unidad de

entrada/salida 36. En este caso, al primer procesador 30 se suministran datos usando variables de entrada de programa, representando sus valores momentáneos valores de señales de entrada de control 114 no relevantes para la seguridad que se generan por sensores 116 no relevantes para la seguridad. En el caso de los sensores 116 no relevantes para la seguridad se trata de sensores que registran, por ejemplo, parámetros de entrada necesarios para una regulación de accionamiento. En este caso puede tratarse, por ejemplo, de revoluciones, ángulos o velocidades. Los sensores 116 no relevantes para la seguridad no están configurados a prueba de errores. A la unidad de entrada/salida 36 se suministran datos usando variables de salida de programa, representando sus valores momentáneos valores de señales de salida de control 118 no relevantes para la seguridad, que se suministran a accionadores 120 no relevantes para la seguridad para su control. En el caso de los accionadores 120 no relevantes para la seguridad se puede tratar, por ejemplo, de motores o de cilindros de ajuste. Los valores momentáneos de las variables de salida de programa no relevantes para la seguridad se establecen dependiendo de las variables de entrada de programa no relevantes para la seguridad de acuerdo con instrucciones de control estándar.

Si en el caso de la instrucción estándar 108 actual se trata de una instrucción de diagnóstico estándar, entonces se intercambian segundos datos 122 no relevantes para la seguridad entre el primer procesador 30 y la unidad de entrada/salida 36. Por ejemplo, al primer procesador 30 se suministran también los valores momentáneos de las señales de entrada de control 114 no relevantes para la seguridad y/o los valores momentáneos de las señales de salida de control 118 no relevantes para la seguridad. Entonces, dependiendo de los valores momentáneos suministrados se puede comprobar qué estado de proceso de la instalación 22 a controlar existe. Se indica un mensaje de diagnóstico correspondiente mediante la unidad de indicación de diagnóstico 124.

Si en el caso de la primera instrucción de seguridad 106 actual se trata de una instrucción de control de seguridad, entonces se intercambian primeros datos 126 relevantes para la seguridad entre el primer procesador 30 y la unidad de entrada/salida 36. En este caso, al primer procesador 30 se suministran datos usando variables de entrada de programa relevantes para la seguridad, representando sus valores momentáneos valores de señales de entrada de control 128 relevantes para la seguridad que se generan por sensores 130 relevantes para la seguridad. En el caso de los sensores 130 relevantes para la seguridad se trata, por ejemplo, de pulsadores de apagado de emergencia, controles bimanuales, puertas de protección, aparatos de supervisión de revoluciones u otros sensores para la captación de parámetros relevantes para la seguridad. A la unidad de entrada/salida 36 se suministran datos mediante el uso de variables de salida de programa relevantes para la seguridad, representando sus valores momentáneos valores de señales de salida de control 132 relevantes para la seguridad que se suministran a accionadores 134 relevantes para la seguridad para su control. En el caso de los accionadores 134 relevantes para la seguridad se trata, por ejemplo, de denominados contactores, cuyos contactos de trabajo están dispuestos en la conexión entre una alimentación de corriente 136 y el consumidor 28. A través de los accionadores 134 relevantes para la seguridad se puede desconectar la alimentación de corriente 136 del consumidor 28, por lo que es posible, con incidencia de un mal funcionamiento correspondiente, pasar al menos el consumidor 28 a un estado seguro. Los valores momentáneos de las variables de salida de programa relevantes para la seguridad se establecen dependiendo de las variables de entrada de programa relevantes para la seguridad de acuerdo con las instrucciones de control de seguridad.

Si en el caso de la primera instrucción de seguridad 106 actual se trata de una instrucción de diagnóstico de seguridad, entonces se intercambian segundos datos 138 relevantes para la seguridad entre el primer procesador 30 y la unidad de entrada/salida 36. Por ejemplo, al primer procesador 30 se suministra también los valores momentáneos de las señales de entrada de control 128 relevantes para la seguridad y/o los valores momentáneos de las señales de salida de control 132 relevantes para la seguridad. Dependiendo de los valores momentáneos suministrados se puede comprobar entonces qué estado de proceso de la instalación 22 a controlar existe. Se indica un mensaje de diagnóstico correspondiente mediante una unidad de indicación de diagnóstico 124.

En el caso de la segunda instrucción de seguridad 110 actual se trata de una instrucción de control de seguridad, en la que se procede de forma correspondiente a la primera instrucción de seguridad 106 actual ejecutada en el primer procesador 30. Con respecto a la segunda instrucción de seguridad 110 actual se usan terceros datos 140 relevantes para la seguridad que se corresponden con los primeros datos 126 relevantes para la seguridad.

Las anteriores explicaciones, de acuerdo con las cuales tanto por el primer procesador 30 como por el segundo procesador 32 se generan valores para las señales de salida de control 132 relevantes para la seguridad, no significan que los valores generados por estos dos procesadores 30, 32 se emitan al mismo tiempo como señales de salida de control 132. Las explicaciones anteriores han de reproducir solamente la estructura redundante con respecto a las tareas de seguridad a realizar del control de seguridad 20. Ambos procesadores 30, 32 están configurados para establecer valores para las señales de salida de control 132. Durante el funcionamiento a prueba de errores del control de seguridad 20 se emiten solamente los valores establecidos por un procesador, por ejemplo, el primer procesador 30, como señales de salida de control 132.

A través de la unidad de entrada/salida 36 se intercambian entre el control de seguridad 20 y los sensores 130 relevantes para la seguridad, los accionadores 134 relevantes para la seguridad y la unidad de indicación de diagnóstico 124 señales de prueba 142. Con ayuda de las señales de prueba 142 se puede comprobar en el control

de seguridad 20 si los componentes conectados a los mismos trabajan a prueba de errores, lo que es necesario, ya que tiene que estar garantizado un estado seguro de la instalación 22 a controlar en cuanto en un aparato conectado al control de seguridad 20 aparezca un mal funcionamiento.

En la Figura 2 está representada la forma de proceder para la generación de un código máquina dependiendo de un código fuente, considerándose solamente la primera parte de código fuente 54 y, por tanto, el contenido relevante para la seguridad del código fuente y, por tanto, del programa de usuario.

La primera parte de código fuente 54 comprende una primera instrucción de control de seguridad FSSA1QC indicada con la referencia 160. La nomenclatura usada tiene, a este respecto, el siguiente significado: FS se refiere a "fail-safe" (a prueba de errores) y, por tanto, indica que se trata de una instrucción de control relevante para la seguridad. SA se refiere, en general, a "instrucción de control". Mediante posposición de la cifra 1 se obtiene el identificador de la instrucción de control de seguridad, mediante el cual se puede identificar la misma en una pluralidad de instrucciones de control de seguridad. QC indica que se trata de una instrucción de control de seguridad del lado del código fuente. Esta nomenclatura se usa de forma unitaria en la Figura 2.

Con la referencia 162 se indica una segunda instrucción de control de seguridad FSSA2QC. Las dos instrucciones de control de seguridad FSSA1QC y FSSA2QC están contenidas en las primeras instrucciones de control 58. Con las referencias 164, 166 están indicadas una primera instrucción de diagnóstico de seguridad FSDA1QC y una segunda instrucción de diagnóstico de seguridad FSDA2QC. DA, a este respecto, se refiere en general a "instrucción de diagnóstico". Mediante posposición, por ejemplo, de la cifra 1 se obtiene un identificador mediante el cual se puede identificar una instrucción de diagnóstico de seguridad en una pluralidad de instrucciones de diagnóstico de seguridad.

Las dos instrucciones de diagnóstico de seguridad FSDA1QC y FSDA2QC están rodeadas o enmarcadas por una primera marca de diagnóstico FSDM1QC indicada con la referencia 168 y una segunda marca de diagnóstico FSDM2QC indicada con la referencia 170 o están rodeadas por las mismas. DM, a este respecto, se refiere en general a "marca de diagnóstico". Mediante posposición, por ejemplo, de la cifra 1 se obtiene un identificador mediante el cual se puede identificar una marca de diagnóstico. Mediante las dos marcas de diagnóstico FSDM1QC y FSDM2QC, durante el proceso de la compilación se pueden reconocer instrucciones de diagnóstico de seguridad que están contenidas en la primera parte de código fuente 54. Las dos instrucciones de diagnóstico de seguridad FSDA1QC y FSDA2QC así como las dos marcas de diagnóstico FSDM1QC y FSDM2QC están contenidas en las primeras instrucciones de diagnóstico 60.

La primera parte de código fuente 54 se suministra al primer compilador 66, lo que está indicado mediante una flecha 172. Con el primer compilador 66 se generan primeros datos de canal 174. Los primeros datos de canal 174 están asignados al canal en el que está contenido el primer procesador 30. Con la primera unidad de generación de código máquina 74 se genera un primer código de seguridad 80 que comprende terceras instrucciones de control 84. En el caso de las terceras instrucciones de control 84 se trata de una tercera instrucción de control de seguridad FSSA1MCA indicada con la referencia 176 y una cuarta instrucción de control de seguridad FSSA2MCA indicada con la referencia 178. MC indica que se trata de una instrucción de control de seguridad en el lado del código máquina. La letra A indica que estas instrucciones de control de seguridad están asignadas al primer procesador 30 y, por tanto, al canal A. Entre las instrucciones de control de seguridad del lado del código fuente y las instrucciones de control de seguridad del lado del código máquina se cumple la siguiente asociación: la tercera instrucción de control de seguridad del lado del código máquina FSSA1MCA está asignada a la primera instrucción de control de seguridad del lado del código fuente FSSA1QC. La cuarta instrucción de control de seguridad del lado del código máquina FSSA2MCA está asignada a la segunda instrucción de control de seguridad del lado del código fuente FSSA2QC.

Además, el primer código de seguridad 80 comprende terceras instrucciones de diagnóstico 86. En el caso de las terceras instrucciones de diagnóstico 86 se trata de una tercera instrucción de diagnóstico de seguridad FSDA1MCA indicada con la referencia 180 y de una cuarta instrucción de diagnóstico de seguridad FSDA2MCA indicada con la referencia 182. Entre las instrucciones de diagnóstico de seguridad del lado de código fuente y las instrucciones de diagnóstico de seguridad del lado de código máquina se cumple la siguiente asociación: la tercera instrucción de diagnóstico de seguridad del lado del código máquina FSDA1MCA está asignada a la primera instrucción de diagnóstico de seguridad del lado del código fuente FSDA1QC. La cuarta instrucción de diagnóstico de seguridad del lado del código máquina FSDA2MCA está asignada a la segunda instrucción de diagnóstico de seguridad del lado del código fuente FSDA2QC.

Con la primera unidad de establecimiento de suma de comprobación 76 se establece una primera suma de comprobación CRCFSA indicada con la referencia 102 para el primer código de seguridad 80. Las letras CRC (cyclic reduncancy check) (comprobación de redundancia cíclica) indican que se realiza dicho establecimiento de suma de comprobación según un procedimiento de CRC. Durante la creación de la primera suma de comprobación CRCFSA se tienen en cuenta solamente las instrucciones de control de seguridad contenidas en el primer código de seguridad 80, de hecho, las dos instrucciones de control de seguridad FSSA1MCA y FSSA2MCA. Las instrucciones de diagnóstico de seguridad contenidas en el primer código de seguridad 80, de hecho, las dos instrucciones de diagnóstico de seguridad FSDA1MCA y FSDA2MCA quedan desatendidas.

La primera unidad de establecimiento de suma de comprobación 76, por tanto, está configurada de tal manera que quedan desatendidas las instrucciones de diagnóstico de seguridad contenidas en la primera parte de código fuente 54 durante el establecimiento de la primera suma de comprobación CRCFSA. Para esto, la primera unidad de establecimiento de suma de comprobación 76 reconoce las marcas de diagnóstico contenidas en la primera parte de código fuente 54. Mediante las dos marcas de diagnóstico FSDM1QC y FSDM2QC está fijado para la primera unidad de establecimiento de suma de comprobación 76 que no se han de atender las instrucciones de seguridad dispuestas entre estas dos marcas de diagnóstico durante la creación de la primera suma de comprobación CRCFSA.

Además, la primera parte de código fuente 54 se suministra al segundo compilador 68, lo que está indicado mediante una flecha 184. Con el segundo compilador 68 se generan segundos datos de canal 168. Los segundos datos de canal 168 están destinados al canal en el que está contenido el segundo procesador 32. Con la segunda unidad de generación de código máquina 92 se genera un segundo código de seguridad 98. El segundo código de seguridad 98 comprende quintas instrucciones de control 100. En el caso de las quintas instrucciones de control 100 se trata de una quinta instrucción de control de seguridad FSSA1MCB indicada con la referencia 188 y una sexta instrucción de control se seguridad FSSA2MCB indicada con la referencia 190. La letra B indica que estas instrucciones de control de seguridad están asignadas al segundo procesador 32, y por tanto, al canal B. A este respecto se cumple la siguiente asociación entre las instrucciones de control de seguridad del lado del código fuente y las instrucciones de control de seguridad del lado del código máquina: la quinta instrucción de control de seguridad del lado del código máquina FSSA1MCB está asignada a la primera instrucción de control de seguridad del lado del código fuente FSSA1QC. La sexta instrucción de control de seguridad del lado del código máquina FSSA2MCB está asignada a la segunda instrucción de control de seguridad del lado del código fuente FSSA2QC.

A este respecto, la segunda unidad de generación de código máquina 92 está configurada de tal manera que quedan desatendidas las instrucciones de diagnóstico de seguridad contenidas en la primera parte de código fuente 54, de hecho, las dos instrucciones de diagnóstico de seguridad FSDA1QC y FSDA2QC. Para esto, la segunda unidad de generación de código máquina 92 reconoce las marcas de diagnóstico contenidas en la primera parte de código fuente, de hecho las dos marcas de diagnóstico FSDM1QC y FSDM2GC. Mediante las dos marcas de diagnóstico FSDM1QC y FSDM2GC está fijado para la segunda unidad de generación de código máquina 92 que no se han de atender las instrucciones de seguridad dispuestas entre estas dos marcas de diagnóstico durante la creación del primer código de seguridad 98. Las dos marcas de diagnóstico identifican las instrucciones de seguridad dispuestas entre las mismas como instrucciones de diagnóstico de seguridad.

Con la segunda unidad de establecimiento de suma de comprobación 94 se establece una segunda suma de comprobación CRCFSB indicada con la referencia 104 para el segundo código de seguridad 98. Ya que el segundo código de seguridad 98 contiene solamente instrucciones de control de seguridad, durante el establecimiento de la segunda suma de comprobación CRCFSB no se atiende ninguna instrucción de diagnóstico de seguridad.

Debido a que las dos instrucciones de diagnóstico de seguridad del lado del código máquina FSDA1MCA y FSDA2MCA quedan desatendidas durante el establecimiento de la primera suma de comprobación CRCFSA, por tanto, en este caso también quedan desatendidas las dos instrucciones de diagnóstico de seguridad del lado del código fuente FSDA1QC y FSDA2QC.

REIVINDICACIONES

1. Procedimiento para la creación de un programa de usuario para un control de seguridad (20), que está configurado para controlar una instalación (22) automatizada con una pluralidad de sensores (26) y una pluralidad de accionadores (24), presentando el control de seguridad (20) un primer procesador (30) y un segundo procesador (32), con las siguientes etapas:

- creación de un código fuente (52) para un programa de usuario, comprendiendo el código fuente (52) una cantidad de instrucciones de control (160, 162) para el control de los accionadores (24) y procesándose para el tratamiento de las instrucciones de control (160, 162) variables de programa relevantes para la seguridad con ayuda del primer y del segundo procesador (30, 32),
- generación de un código máquina (70) dependiendo del código fuente (52) y
- establecimiento de al menos una suma de comprobación (102, 104) para al menos una parte del código máquina (80, 98),

caracterizado por que el código fuente (52) comprende además una cantidad de instrucciones de diagnóstico (164, 166) para la generación de mensajes de diagnóstico que se indican en una unidad de indicación de diagnóstico (124), quedando desatendidas durante el establecimiento de la suma de comprobación (102, 104) las instrucciones de diagnóstico (164, 166).

2. Procedimiento de acuerdo con la reivindicación 1, **caracterizado por que** las instrucciones de diagnóstico (164, 166) se enmarcan en el código fuente (52).

3. Procedimiento de acuerdo con una de las reivindicaciones precedentes, **caracterizado por que** el código máquina (70) comprende un primer código de seguridad (80) y un segundo código de seguridad (98), estableciéndose para cada uno de los dos códigos de seguridad (80, 98) respectivamente una suma de comprobación (102, 104).

4. Procedimiento de acuerdo con una de las reivindicaciones precedentes, **caracterizado por que** el código máquina (70) comprende un primer código de seguridad (80) y un segundo código de seguridad (98), teniéndose en cuenta durante la generación del primer código de seguridad (80) las instrucciones de diagnóstico (164, 166) y quedando desatendidas durante la generación del segundo código de seguridad (98).

5. Dispositivo para la creación de un programa de usuario para un control de seguridad (20), que está configurado para controlar una instalación (22) automatizada con una pluralidad de sensores (26) y una pluralidad de accionadores (24), presentando el control de seguridad (20) un primer procesador (30) y un segundo procesador (32), con unidades (12, 14, 16) para la creación de un código fuente (52) para un programa de usuario, comprendiendo el código fuente (52) una cantidad de instrucciones de control (160, 162) para el control de los accionadores (24) y procesándose para el tratamiento de las instrucciones de control (160, 162) variables de programa relevantes para la seguridad en modo a prueba de errores con ayuda del primer y segundo procesador (30, 32), con unidades (74, 92) para la generación de un código máquina (70) dependiendo del código fuente (52) y con unidades (76, 94) para el establecimiento de al menos una suma de comprobación (102, 104) para al menos una parte del código máquina (80, 98), **caracterizado por que** el código fuente (52) comprende además una cantidad de instrucciones de diagnóstico (164, 166) para la generación de mensajes de diagnóstico que se indican en una unidad de indicación de diagnóstico (124), quedando desatendidas las instrucciones de diagnóstico (164, 166) durante el establecimiento de la suma de comprobación (102, 104).

6. Programa informático con medios de código de programa para llevar a cabo un procedimiento de acuerdo con una de las reivindicaciones 1 a 4 cuando se ejecuta el programa informático (16) en un ordenador (12).

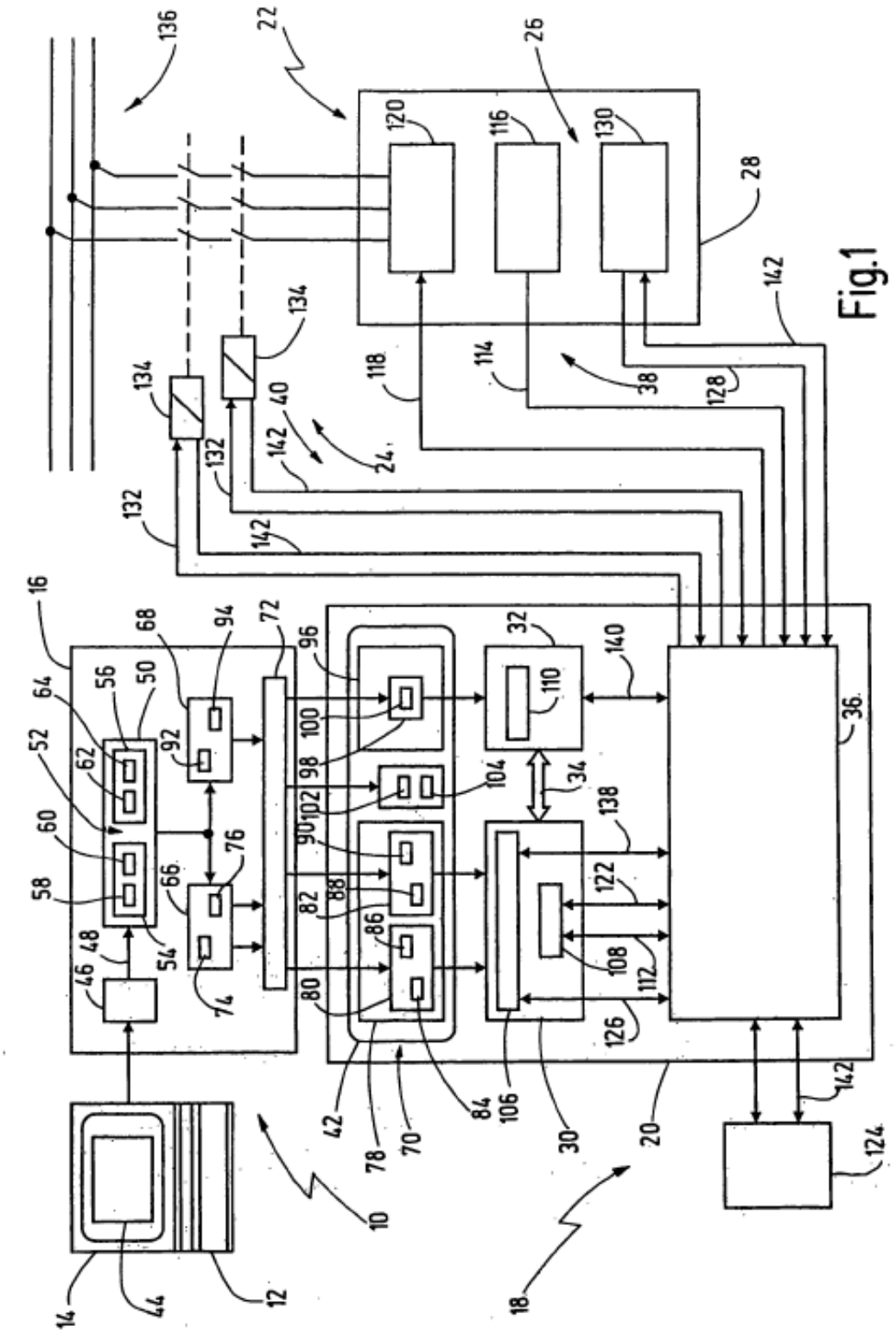
136
22
26
120
116
130
28
142
134
134
118
114
40
38
128
142
24
132
132
142
16
68
94
72
96
32
140
64
56
50
110
36
52
62
92
100
98
104
34
60
102
90
138
76
58
66
82
88
122
86
48
108
46
54
74
80
112
126
42
78
70
84
106
30
20
142
124
10
18
14
44
12

Fig.1

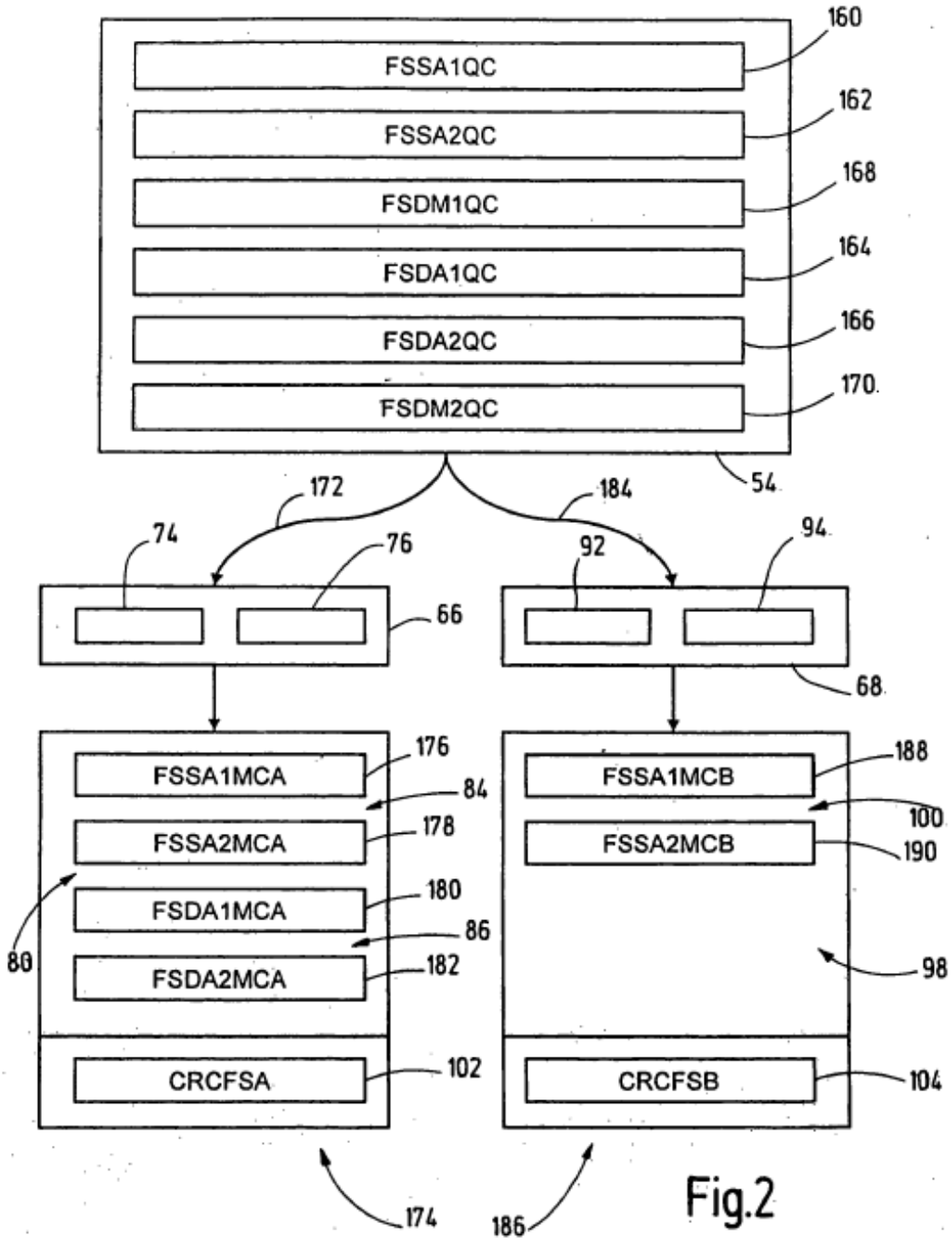
FSSA1QC
FSSA2QC
FSDM1QC
FSDA1QC
FSDA2QC
FSDM2QC
160
162
168
164
166
170
54
172
184
74
76
92
94
66
68
FSSA1MCA
FSSA2MCA
FSDA1MCA
FSDA2MCA
176
84
178
180
86
182
80
FSSA1MCB
FSSA2MCB
188
100
190
98
CRCFSA
CRCFSB
102
104
174
186

Fig.2