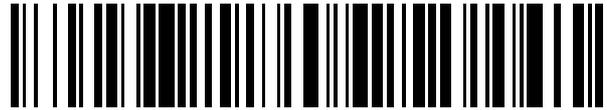


19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 434 874**

51 Int. Cl.:

**G05B 19/042** (2006.01)

**G05B 23/02** (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **20.11.2009 E 09804248 (4)**

97 Fecha y número de publicación de la concesión europea: **25.09.2013 EP 2356527**

54 Título: **Control de seguridad y procedimiento para el control de una instalación automática con una pluralidad de componentes de hardware de la instalación**

30 Prioridad:

**25.11.2008 DE 102008060005**

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

**17.12.2013**

73 Titular/es:

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

72 Inventor/es:

**ZONDLER, MARTIN;  
EHRHART, HELMUT y  
FOERSTER, HARALD**

74 Agente/Representante:

**UNGRÍA LÓPEZ, Javier**

**ES 2 434 874 T3**

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

## DESCRIPCIÓN

Control de seguridad y procedimiento para el control de una instalación automática con una pluralidad de componentes de hardware de la instalación

5 La invención se refiere a un control de seguridad para el control de una instalación automática con una pluralidad de componentes de hardware de la instalación, que comprende una pluralidad de sensores y una pluralidad de actuadores, con una unidad de control, a la que están asociadas una pluralidad de señales de entrada de control desde una pluralidad de sensores, en el que la unidad de control está configurada para generar una pluralidad de señales de salida de control en función de las señales de entrada de control de acuerdo con un programa de aplicación que se ejecuta en ella, en el que con una pluralidad de señales de salida de control se activan la pluralidad de actuadores, con una interfaz para una unidad de representación, en el que la unidad de representación está configurada para representar mensajes de diagnóstico, con una unidad de evaluación de diagnóstico de procesos, a la que se alimentan una pluralidad de señales de salida de diagnóstico de procesos, en el que la unidad de evaluación de diagnóstico de procesos está configurada para establecer en función de la pluralidad de señales de salida de diagnóstico de procesos, cuál de varios estados de procesos de la instalación a controlar está presente en un primer instante definido, en el que la unidad de evaluación de diagnóstico de procesos está configurada para generar una pluralidad de señales de estado de procesos, en el que la pluralidad de señales de estado de procesos representa una pluralidad de estados de procesos establecidos, en el que la pluralidad de estados de procesos establecidos están presentes en el primer instante definido, con una unidad de evaluación de diagnóstico del sistema, a la que se alimentan una pluralidad de señales de entrada de diagnóstico del sistema, en el que la unidad de evaluación de diagnóstico del sistema está configurada para establecer en función del número de señales de entrada de diagnóstico del sistema, cuál de varios estados del sistema del control de seguridad está presente en un segundo instante definido, en el que la unidad de evaluación de diagnóstico del sistema está configurada para generar una pluralidad de señales del estado del sistema, en el que la pluralidad de señales de estado del sistema representa una pluralidad de estados del sistema establecidos, en el que la pluralidad de estados del sistema establecidos están presentes en el segundo instante definido, y con una unidad de mensajes de diagnóstico, a la que se alimentan la pluralidad de señales de estado de proceso y la pluralidad de señales de estado del sistema, en el que la unidad de mensajes de diagnóstico está configurada para acondicionar una pluralidad de mensajes de diagnóstico para la pluralidad de estados de proceso establecidos y para la pluralidad de estados del sistema establecidos, en el que la unidad de mensajes de diagnóstico genera una pluralidad de señales de diagnóstico, que representan los mensajes de diagnóstico, en el que la pluralidad de señales de diagnóstico son conducidos a la unidad de representación para la representación de los mensajes de diagnóstico.

La invención se refiere, además, a un procedimiento para el control de una instalación automática con una pluralidad de componentes de hardware de las instalaciones, que comprenden una pluralidad de sensores y actuadores, con las etapas:

- 35 - establecer en función de una pluralidad de señales de entrada de diagnóstico del procesos, cuál de varios estados del proceso de la instalación a controlar está presente en un primer instante definido, y generar una pluralidad de señales de estado del proceso, en el que la pluralidad de señales de estado del procesos representa una pluralidad de estados del proceso establecidos, en el que la pluralidad de estados del proceso establecidos están presentes en un primer instante definido,
- 40 - establecer en función de una pluralidad de señales de entrada de diagnóstico del sistema, cuál de varios estados del sistema del control de seguridad está presente en un segundo instante definido, y generar una pluralidad de señales de estado del sistema, en el que la pluralidad de señales de estado del sistema representa una pluralidad de estados del sistema establecidos, en el que la pluralidad de estados del sistema establecidos están presentes en el segundo instante definido,
- 45 - alimentar la pluralidad de señales de estado del proceso y la pluralidad de señales de estado del sistema a una unidad de mensajes de diagnóstico,
- preparar una pluralidad de mensajes de diagnóstico para la pluralidad de estados del proceso establecidos y para la pluralidad de estados del sistema establecidos, y generar una pluralidad de señales de diagnóstico en la unidad de mensajes de diagnóstico, en el que la pluralidad de señales de diagnóstico representan la pluralidad de mensajes de diagnóstico,
- 50 - alimentar la pluralidad de señales de diagnóstico hacia una unidad de representación para la representación de la pluralidad de mensajes de diagnóstico,

Un control de seguridad de este tipo y un procedimiento de este tipo se publican esencialmente en el documento GB 2 398 395 A.

55 Un control del sistema en el sentido de la presente invención es un aparato y un dispositivo que reciben las señales de entrada suministradas por sensores y a partir de ellas se generan señales de salida a través de enlaces lógicos y,

en determinadas circunstancias, de otras etapas de procesamiento de señales o de procesamiento de datos. Las señales de salida pueden ser alimentadas entonces a actuadores, que provocan entonces acciones o reacciones en el medio ambiente, en función de las señales de entrada.

5 Un campo de aplicación preferido para tales controles de seguridad es en el campo de la seguridad de las máquinas para la supervisión de conmutadores de desconexión de emergencia, controles con las dos manos, puertas de protección o rejillas luminosas. Tales sensores se utilizan para asegurar, por ejemplo, una máquina, desde la que parte en el funcionamiento un peligro para el hombre o para productos materiales. Cuando se abre la puerta de protección o cuando se activa el conmutador de desconexión de emergencia se genera en cada caso una señal, que es alimentada al control de seguridad como señal de entrada. Como reacción a ello, el control de seguridad desconecta entonces, por ejemplo con la ayuda de un actuador, la pieza de la máquina que lleva el peligro.

10 En un control de seguridad, en oposición a un control "normal", es característico que el control de seguridad propiamente dicho garantiza siempre un estado seguro de la instalación o máquina que lleva el peligro, cuando aparece una función errónea en ella o en un aparato conectado con ella. Por lo tanto, en controles de seguridad se plantean requerimientos extremadamente altos a la seguridad propia contra fallos, lo que tiene como consecuencia un gasto considerable en el desarrollo y fabricación.

15 En general, los controles de seguridad necesitan antes de su utilización una autorización especial a través de las autoridades de inspección competente, como por ejemplo en Alemania a través de las Asociaciones Profesionales o el TÜV. El control de seguridad debe contener en este caso normas de seguridad predeterminadas, que están registradas, por ejemplo en la Norma europea EN 954-1 o en una Norma comparable, por ejemplo la Norma IEC 61508 o la Norma EN ISO 13849-1. Por lo tanto, a continuación por un control de seguridad se entiende un aparato o bien un dispositivo, que cumple al menos la categoría de seguridad de dicha Norma europea EN 954-1.

20 Un control de seguridad programable ofrece al usuario la posibilidad de establecer individualmente los enlaces lógicos u, dado el caso, otras etapas de procesamiento de señales o de datos con la ayuda de un software, el llamado programa de aplicación, de acuerdo con sus necesidades. De ello resulta una gran flexibilidad en comparación con soluciones anteriores, en las que los enlaces lógicos han sido generados a través de un cableado definido entre diferentes módulos de seguridad. Un programa de aplicación se puede cerrar, por ejemplo, con la ayuda de un ordenador personal (PC) de venta en el comercio y utilizando programas de software instalados de forma correspondiente.

25 El programa de aplicación que se ejecuta en el control de seguridad establece el proceso, que se ejecuta en la instalación controlada por el control de seguridad. Este proceso es supervisado por medio de una diagnosis del proceso. En el marco de la diagnosis del proceso se verifica cuál de varios estados del proceso de la instalación a controlar está presente en un instante definido. De esta manera se registran tanto estados admisibles como inadmisibles del proceso. Un objetivo es detectar estados inadmisibles del proceso, las llamadas averías, y representarlás en una unidad de representación, de manera que el personal de servicio de la instalación a controlar puede eliminar la avería. En general, en una unidad de representación de este tipo se trata de una unidad de representación integrada en el puesto de mando de la instalación a controlar.

30 En general, a través de la diagnosis del proceso y la representación implicada con ello de los estados del proceso detectados, es decir, establecidos, se representa una copia del proceso en la unidad de representación, que comprende tanto los estados admisibles como también los estados inadmisibles del proceso.

35 Los estados del proceso detectados por medio de la diagnosis de procesos son calculados, entre otras cosas, a través de consultas lógicas, por lo que estados inadmisibles establecidos del proceso son designados también como errores lógicos. En estas consultas lógicas se realizan, por ejemplo comparaciones de valores límites o comparaciones de intervalos para magnitudes detectadas con sensores, es decir, que el valor de medición presente en cada caso de la magnitud detectada se compara con uno o varios valores límites.

40 Un ejemplo a este respecto es la supervisión del estado de llenado de un envase. A tal fin, se asocia al envase un sensor del nivel de llenado. El sensor del nivel de llenado genera una señal de nivel de llenado, que representa el nivel de llenado detectado del envase. En general, en la señal del nivel de llenado se trata de una tensión, en la que el valor de la tensión es proporcional al nivel de llenado presente en el envase. En función de si el procesamiento siguiente se ejecuta de forma analógica o digital, se compara este valor de la tensión propiamente dicho o una magnitud derivada del mismo con un valor límite. Si se establece en esta comparación que se ha excedido el valor límite, entonces esto es interpretado como "envase lleno" y no se crea ningún mensaje de diagnosis. En cambio, si se establece en la comparación que no se ha alcanzado el valor límite, entonces esto es interpretado como "envase vacío". Se parte de que existe un estado inadmisibile del proceso, un estado de error. Sobre la unidad de representación se representa un mensaje de diagnosis, que representa este estado inadmisibile del proceso. De esta manera se representa un error lógico en la unidad de representación.

45 Sin embargo, ahora son concebibles dos constelaciones. En la primera constelación, el envase está realmente vacío. En este caso, el estado del proceso establecido, es decir el error lógico establecido corresponde a la realidad.

El mensaje de diagnóstico representado en la unidad de representación reproduce correctamente la realidad. El envase debe llenarse por el personal de servicio, por ejemplo un técnico de mantenimiento.

5 Pero también es concebible una segunda constelación, en la que el envase no está realmente vacío. En este caso el espado del proceso establecido, es decir, el error lógico establecido, no corresponde a la realidad y el mensaje de diagnóstico representado en la unidad de representación no reproduce correctamente la realidad. Éste puede ser el caso, por ejemplo, cuando el sensor del nivel de llenado está averiado o existe un error en el cableado que conecta el sensor el nivel de llenado al control de seguridad o existe un error en el propio control de seguridad. En todos estos casos se representa un mensaje de diagnóstico, que hace referencia a un envase vacío, aunque el envase está  
10 lleno. La representación de este mensaje de diagnóstico no sólo es errónea, sino que, además, el personal de servicio no recibe ninguna indicación sobre la causa realmente presente, que ha conducido a que se haya establecido a través de la diagnosis del proceso el estado del proceso que sirve de base para el mensaje de diagnóstico representado.

15 El documento GB 2 398 395 A mencionado al principio describe una instalación de proceso con un sistema de seguridad integrado, que utiliza junto con el control del proceso hardware común de comunicación, de diagnóstico y de representación y también software correspondiente. Una aplicación de diagnóstico puede representar informaciones de diagnóstico tanto para el sistema de control del proceso como también para el sistema de seguridad utilizando una interfaz común y realizar actividades de diagnóstico. En este caso, el documento GB 2 398 395 A da importancia a que se representen alarmas del control del proceso y alarmas del sistema de seguridad de tal manera que se  
20 distingan las alarmas del sistema de control de procesos y del sistema de seguridad unas de las otras. A través de mecanismos de filtro, que se pueden aplicar en todas las alarmas en la instalación, un usuario puede adaptar de manera correspondiente la representación de alarmas a sus necesidades. En el documento GB 2 398 395 A no se publica una asociación fijamente depositada en el sistema de alarmas de procesos y alarmas de seguridad.

25 El documento EP 0 482 523 A2 publica un sistema de representación para la diagnosis de errores en instalaciones industriales complejas. El sistema de representación identifica fuentes posibles de errores y utiliza estas informaciones de diagnóstico para representar las secciones interesantes en cada caso dentro de una jerarquía de procesos y dentro de una jerarquía de componentes. En una representación de dos partes se representan los componentes de hardware sobre un lado y las etapas del proceso en el otro lado, respectivamente, en una disposición jerárquica.

30 Las explicaciones anteriores muestran que las medidas de diagnóstico empleadas en los controles de seguridad y procedimientos conocidos no son todavía óptimas.

Por lo tanto, un cometido de la presente invención es desarrollar un control de seguridad y un procedimiento del tipo mencionado al principio para informar al personal de servicio de una instalación todavía mejor sobre averías que aparecen durante el funcionamiento de la instalación y apoyarle todavía mejor en la eliminación de estas averías.

35 Este cometido se soluciona por medio de un control de seguridad y un procedimiento del tipo mencionado al principio, en el que la unidad de mensajes de diagnóstico presenta una unidad de memoria de asociación, en la que están depositadas una pluralidad de magnitudes de asociación al menos para una pluralidad de los varios estados de proceso y al menos para una pluralidad de los varios estados del sistema, en el que las magnitudes de asociación depositadas representan cuál de los varios estados del sistema está asociado, respectivamente, a cuya  
40 de los varios estados de proceso en virtud de una asociación predefinida, en el que la unidad de mensajes de diagnóstico está configurada para seleccionar una pluralidad de magnitudes de asociación depositadas para una pluralidad de parejas de los estados del sistema establecidos y de los estados de proceso establecidos, en el que cada una de estas magnitudes de asociación seleccionadas representa al menos una de las parejas, en el que la unidad de mensajes de diagnóstico está configurada para calcular una pluralidad de estados del sistema asociados en función de las magnitudes de asociación, y en el que al menos para uno de los estados de proceso establecidos se prepara un mensaje de diagnóstico en función de este estado del proceso y del número de estados del sistema asociados, que están asociados a este estado del proceso.

45 El nuevo control de seguridad y el nuevo procedimiento se basan en la idea de enlazar la diagnosis de procesos con la diagnosis del sistema. A tal fin, está prevista una unidad de evaluación de la diagnosis de procesos, que está configurada para establecer, en función de una pluralidad de señales de entrada de diagnosis de procesos, que se alimentan a ella, cuál de varios estados de procesos de la instalación a controlar está presente en un primer instante definido. En general, pueden estar presentes una pluralidad de estados de procesos establecidos en el primer instante definido. Además, está prevista una unidad de evaluación de diagnosis del sistema, que está configurada para establecer en función de una pluralidad de señales de entrada de diagnosis del sistema, que son alimentadas a ella, cuál de varios estados del sistema del control de seguridad está presente en un segundo instante definido. En  
50 general, pueden existir una pluralidad de estados del sistema establecidos en el segundo instante definido.

Un estado del sistema de un control de seguridad es un estado, que puede adoptar, por una parte, el control de seguridad como tal, es decir, la unidad de construcción, en la que están alojados los componentes lógicos, por

ejemplo procesadores y memorias, que son necesarios para la realización de tareas de control y, por otra parte, que aquellos componentes, por ejemplo sensores y actuadores, que están conectados con la instalación a controlar, que están conectados eléctricamente con esta unidad de construcción y, además, los llamados aparatos de alarma, por ejemplo conmutadores selectores de tipos de funcionamiento, que están conectados de la misma manera con esta unidad constructiva. En esta consideración se comprende también al mismo tiempo todos los cableados. Con vistas a la diagnosis, son interesantes sobre todo aquellos estados del sistema, en los que en uno de los componentes enumerados anteriormente aparece un error. Estos errores se designan como errores físicos.

El enlace de diagnosis del proceso y diagnosis del sistema se realiza porque para aquel estado del proceso establecido, para el que en los estados del sistema establecidos están contenidos estados del sistema que están asociados a este estado del proceso, se prepara un mensaje de diagnosis en función de este estado del proceso propiamente dicho y en función de una pluralidad de estados del sistema asociados.

Además, la unidad de mensajes de diagnosis presenta una unidad de memoria de asociación (350), en la que están depositadas una pluralidad de magnitudes de asociación al menos para una pluralidad de los varios estados de proceso y al menos para una pluralidad de los varios estados del sistema, en el que las magnitudes de asociación depositadas representan cuál de los varios estados del sistema está asociado, respectivamente, a cual de los varios estados de proceso en virtud de una asociación predefinida, en el que la unidad de mensajes de diagnosis está configurada para ella. A través de esta medida es posible de una manera sencilla y, además, muy fiable calcular el número de estados del sistema asociados. Puesto que en la unidad de memoria de asociación están memorizadas fijamente las asociaciones predefinidas, que existen, respectivamente, entre los varios estados del sistema y los varios estados del proceso, se puede establecer de una manera unívoca cuál de los estados del sistema establecidos está asociado en cada caso a cual de los estados del proceso establecidos. De esta manera se garantiza una instrucción completa y fiable del personal de servicio de una instalación.

Con preferencia, estas magnitudes de asociación están configuradas como magnitudes lógicas, que indica para cuál de las combinaciones, que son concebibles entre los varios estados del sistema y los varios estados del proceso, existe en cada caso una asociación. Para las magnitudes de asociación son concebibles varias formas de realización. Así, por ejemplo, se puede tratar de una matriz, en la que en un campo de la matriz se registra un uno lógico, cuando entre el estado del proceso que pertenece a su campo de la matriz y el estado del sistema que pertenece a este campo de la matriz existe una asociación predefinida y en la que en un campo de la matriz se registra un cero lógico, cuando entre el estado del proceso que pertenece a este estado campo de la matriz y el estado del sistema que pertenece a este campo de la matriz no existe ninguna asociación predefinida. De manera alternativa, en las magnitudes de asociación se puede tratar de varios vectores. En este caso, cada uno de estos vectores representa uno de los varios estados del proceso e indica aquellos estados del sistema, que están asociados a este estado del proceso a través de asociaciones predefinidas. En otra alternativa, en las magnitudes de asociación se puede tratar de una pluralidad de duplicados. Cada uno de estos duplicados representa una combinación de uno de los varios estados del sistema y de uno de los varios estados del proceso, entre los que existe una asociación predefinida.

A través del principio de acuerdo con la invención se consigue que durante la preparación de un mensaje de diagnosis se tengan en cuenta al mismo tiempo el estado del proceso propiamente dicho y estados del sistema asociados a este estado del proceso. Es decir, que en la preparación del mensaje de diagnosis no sólo entra el estado del proceso establecido propiamente dicho, sino también entran los estados del sistema que lo provocan. Con otras palabras: durante la preparación del mensaje de diagnosis no sólo se tienen en cuenta errores físicos, sino también los errores físicos que los provocan.

La consideración simultánea de un estado del proceso y de los estados del sistema que lo provoca forma la base para una instrucción amplia del personal de servicio sobre averías que aparecen durante el funcionamiento de una instalación. Se puede comunicar al personal de servicio el error físico en el que se basa el error lógico. De esta manera, el personal de servicio puede tomar medidas amplias para la eliminación del error físico y, por lo tanto, de la avería.

Al mismo tiempo, a través del principio de acuerdo con la invención, se eleva la fiabilidad con respecto a un mensaje de diagnosis, que representa un estado del proceso establecido. Si se representa en una unidad de representación un mensaje de diagnosis, que contiene solamente informaciones sobre un estado del proceso establecido, es decir, sobre un error físico, y no contiene ninguna referencia a un estado del sistema que sirve de base y, por lo tanto, a un error físico que provoca el error lógico, esto significa en virtud del principio de acuerdo con la invención que el estado del proceso establecido reproduce correctamente la realidad y no existe ninguna causa de error físico para el mensaje de diagnosis. Puesto que un control de seguridad debe estar realizado de tal forma que para la consecución de un control a prueba de fallos, se detectan todos los errores físicos concebibles.

A través del principio de acuerdo con la invención se consigue de esta manera una instrucción mejorada del personal de servicio sobre averías que aparecen durante el funcionamiento de una instalación y se consigue un

apoyo mejorado durante la eliminación de estas averías.

5 Cuando con relación al control de seguridad de acuerdo con la invención y al procedimiento de acuerdo con la invención se habla de personal de servicio, entonces por ello debe entenderse no sólo el usuario clásico de una instalación, sino también el técnico de mantenimiento, el creador de un programa de aplicación o el fabricante de la instalación de control.

De esta manera se soluciona totalmente el cometido mencionado.

Antes de representar a continuación las configuraciones preferida de la invención, se presentan algunas consideraciones.

10 De acuerdo con las explicaciones anteriores, la unidad de evaluación de diagnóstico de procesos está configurada para establecer cuál de varios estados de procesos de la instalación a controlar está presente en un primer instante definido, en cambio la unidad de evaluación de diagnóstico del sistema está configurada para establecer cuál de varios estados del sistema del control de seguridad está presente en un segundo instante definido. La distinción en un primer instante definido y en un segundo instante definido tiene en cuenta el siguiente hecho: un control de seguridad programable es un sistema basado en un microprocesador, que trabaja de forma discreta en el tiempo con un pulso de reloj definido. Por este motivo, las señales presentes de forma continua en el tiempo, es decir, las señales analógicas, que son acondicionadas por ejemplo por sensores, son convertidas en señales digitales, para que sea posible, en general, su procesamiento en el control de seguridad. La conversión se realiza en instantes predeterminados por el pulso de reloj. De esta manera, puede suceder que para un estado del proceso y un estado del sistema asociado, las consultas, con las que se puede establecer la presencia del estado respectivo, se realizan en instantes insignificamente diferentes. Éste es el caso, por ejemplo, cuando en el control de seguridad ha sido acondicionada una magnitud a evaluar para el estado del proceso antes que una magnitud a evaluar para el estado del sistema. Por consiguiente, en el control de seguridad se establecen el estado del proceso y el estado del sistema en instantes diferentes. En general, estos dos instantes se encuentran dentro de un intervalo de tiempo pequeño definido, cuya longitud corresponde a un múltiplo de la duración periódica predeterminada por el pulso de reloj. En este caso, el primer instante definido y el segundo instante definido se encuentran muy estrechamente adyacentes entre sí, el estado del sistema y el estado del proceso se establecen casi al mismo tiempo. La consideración de un primer instante definido y de un segundo instante definido debe comprender también el hecho, en el que entre la fijación de un estado del proceso y la fijación de un estado del sistema transcurren varios segundos o incluso minutos.

30 La división condicionada funcionalmente representada anteriormente en una unidad de evaluación de diagnóstico de procesos, una unidad de evaluación de diagnóstico del sistema y una unidad de mensajes de diagnóstico no debe tener ninguna especificación para la configuración estructural realizada en concreto dentro de un control de seguridad. De esta manera, es concebible realizar la idea de estas tres unidades de forma estructural autónoma o realizar la unidad de evaluación de diagnóstico de procesos y la unidad de evaluación de diagnóstico del sistema como una unidad estructural común o incluso realizar todas las tres unidades como una unidad estructural común.

40 En una configuración preferida de la invención, la unidad de mensajes de diagnóstico está configurada para calcular una pluralidad de magnitudes de asociación, en la que las magnitudes de asociación indican cuál de la pluralidad de estados del sistema establecidos está asociado a cuál de la pluralidad de estados del proceso establecidos, respectivamente, estando configurada la unidad de mensajes de diagnóstico para calcular el número de estados asociados del sistema en función del número de magnitudes de asociación.

Esta medida representa un modo de proceder sencillo para la asociación de un estado del sistema a un estado del proceso. De esta manera, la pluralidad de estados del sistema establecidos, que provocan un estado del proceso establecido, está asociada a este estado del proceso.

45 En una configuración preferida de la invención, la unidad de mensajes de diagnóstico está configurada para acondicionar, en presencia de un estado del proceso establecido y de una pluralidad de estados del sistema asociados, como mensaje de diagnóstico para este estado del proceso una pluralidad de mensajes de diagnóstico del sistema, de manera que la pluralidad de mensajes de diagnóstico del sistema se presentan la pluralidad de estados del sistema asociados.

50 Como ya se ha indicado, un estado del proceso, es decir, un error lógico, tiene como causa un estado del sistema, es decir, un error físico. A través de esta medida se consigue que para un estado del proceso establecido no se represente el mensaje de diagnóstico del proceso que lo representa, sino inmediatamente los mensajes de diagnóstico del sistema, que representan la pluralidad de estados del sistema asociados, sobre la unidad de representación. De esta manera, se indica al personal de servicio de una instalación qué errores físicos existen. El personal de servicio puede comenzar de esta manera inmediatamente con la solución de la avería. Esta medida posibilita de este modo una eliminación óptima de la avería en el tiempo.

En una configuración preferida de la invención, la unidad de mensajes de diagnóstico está configurada para

5 acondicionar un mensaje de diagnóstico combinado, como mensaje de diagnóstico para este estado del proceso en el caso de presencia de un estado del proceso establecido y de una pluralidad de estados del sistema asociados, de manera que el mensaje de diagnóstico combinado contiene tanto un mensaje de diagnóstico del proceso como también una pluralidad de mensajes de diagnóstico del sistema, de manera que el mensaje de diagnóstico del proceso representa el estado del proceso establecido y la pluralidad de mensajes de diagnóstico del sistema representan la pluralidad de estados del sistema asociados.

10 La medida tiene la ventaja de que el personal de servicio de una instalación es informado ampliamente tanto sobre un estado del proceso establecido como también sobre aquellos estados del sistema establecidos, que están asociados a este estado del proceso. De esta manera, el personal de servicio es informado sobre un error lógico presentes y sobre los errores físicos que provocan este error lógico. No sólo se garantiza una instrucción amplia del personal de servicio, sino que sobre la base de la instrucción amplia es posible una eliminación inmediata de un estado de avería.

En otra configuración de la medida mencionada anteriormente, la unidad de representación está configurada para

15 - representar en primer lugar el mensaje de diagnóstico del proceso y en el caso de presencia de una solicitud de diagnóstico del sistema, sustituir el mensaje de diagnóstico del proceso por al menos uno de la pluralidad de mensajes de diagnóstico del sistema o de forma complementaria al mensaje de diagnóstico del proceso, representar al menos uno de la pluralidad de mensajes de diagnóstico del sistema, o

- representar el mensaje de diagnóstico del proceso y al menos uno de la pluralidad de mensajes de diagnóstico del sistema, o

20 - representar solamente al menos uno de la pluralidad de mensajes de diagnóstico del sistema.

Si se prepara como mensaje de diagnóstico un mensaje de diagnóstico combinado, entonces son concebibles, en principio, diferentes modos de proceder, en lo que se refiere a la representación de la información contenida en el mensaje de diagnóstico combinado.

25 Tanto la primera alternativa, en la que se representa el mensaje de diagnóstico del proceso y en el caso de presencia de una solicitud de diagnóstico del sistema de forma sustitutiva o complementaria al menos un de los mensajes de diagnóstico del sistema, como también la segunda alternativa, en la que se representan desde el principio al mismo tiempo el mensaje de diagnóstico del proceso y al menos tiempo uno de los mensajes de diagnóstico del sistema, tienen la ventaja de la instrucción amplia del personal de servicio. Frente a la segunda alternativa, la primera alternativa tiene la ventaja de que la representación en la unidad de representación es en primer lugar clara y sencilla y, en caso necesario, se puede representar cuando por ejemplo una persona lee la unidad de representación, que dispone de una autorización de acceso correspondiente, y posibilita una intervención en la instalación para la eliminación de una avería, de uno o varios errores físicos y, por lo tanto, de los defectos presentes en la instalación. La tercera alternativa, según la cual desde el principio solamente se representa al menos uno de los mensajes de diagnóstico del sistema, el personal de servicio de la instalación se desplaza a la instalación para comenzar inmediatamente con la eliminación de la avería. Además, tiene la ventaja de una representación clara y sencilla.

35 En una configuración preferida de la invención, la unidad de mensajes de diagnóstico está configurada para preparar como un primer mensaje de diagnóstico al menos un mensaje de diagnóstico del proceso, en el caso de presencia de un estado del proceso establecido y de una pluralidad de estados del sistema establecidos, y preparar como un segundo mensaje de diagnóstico adicionalmente una pluralidad de mensajes de diagnóstico del sistema en el caso de presencia de una solicitud de diagnóstico del sistema, en el que el mensaje de diagnóstico del proceso representa el estado del proceso establecido y la pluralidad de mensajes de diagnóstico del sistema representan la pluralidad de estados del sistema asociados.

45 Esta medida prevé acondicionar los mensajes de diagnóstico en dos etapas. En una primera etapa solamente se acondiciona el mensaje de diagnóstico del proceso. Si existe un requerimiento de diagnóstico del sistema, entonces se acondicionan en una segunda etapa una pluralidad de mensajes de diagnóstico del sistema. De esta manera se asegura que a través de la preparación de mensajes de diagnóstico no vaya unida innecesariamente potencia de cálculo. De acuerdo con este principio, para la preparación de los mensajes de diagnóstico del sistema solamente debe aplicarse potencia de cálculo cuando exista una demanda de diagnóstico del sistema.

50 En otra configuración de la medida mencionada anteriormente, la unidad de representación está configurada para sustituir el mensaje de diagnóstico del sistema por al menos uno de la pluralidad de mensajes de diagnóstico del sistema o al menos representar uno de la pluralidad de los mensajes de diagnóstico del sistema como complemento del mensaje de diagnóstico del proceso.

Esta medida posibilita una instrucción amplia y, además, clara y sencilla del personal de servicio de una instalación.

En otra configuración de la medida mencionada anteriormente, a la unidad de representación está asociada una

unidad de solicitud de diagnóstico del sistema, en la que la unidad de solicitud de diagnóstico del sistema está configurada para registrar una solicitud de diagnóstico del sistema.

5 Esta medida posibilita a una persona, que lee la unidad de representación, depositar de una manera sencilla una solicitud de diagnóstico del sistema, para recibir representados, en caso necesario, mensajes de diagnóstico del sistema. De manera más ventajosa, la unidad de representación y la unidad de solicitud de diagnóstico del sistema forman una unidad de construcción.

10 En una configuración preferida de la invención, la unidad de evaluación de diagnóstico de procesos está configurada para establecer continuamente cuál de varios estados del proceso está presente en un instante definido, respectivamente, y/o la unidad de evaluación de diagnóstico del sistema está configurada para establecer continuamente cuál de varios estados del sistema está presente en un instante definido, respectivamente.

15 A través de esta medida se asegura que no sólo se creen mensajes de diagnóstico en un intervalo de tiempo pequeño, sino continuamente y, por lo tanto, sobre un periodo de tiempo más largo, por ejemplo durante todo el funcionamiento de la instalación. De esta manera se asegura que el personal de servicio de la instalación sea informado también con relación al tiempo ampliamente sobre averías producidas. Los instantes definidos, en los que se establece cuál de varios estados de procesos está presente en cada caso, están establecidos a través del primer instante definido y, por ejemplo, el pulso de reloj, con el que trabaja el control de seguridad. Lo mismo se aplica de manera correspondiente para los estados del sistema, pero con relación al segundo instante definido.

20 En otra configuración de la medida mencionada anteriormente, la unidad de mensajes de diagnóstico presenta una unidad de memoria de estados, que está configurada para memorizar continuamente estados de procesos establecidos y estados del sistema establecidos, estando configurada la unidad de mensajes de diagnóstico para tener en cuenta estados del sistema establecidos ya memorizados y/o estados del proceso establecidos ya memorizados en el caso de que se determine si en el estado del sistema a memorizar se trata de un estado del sistema asociado y/o en el caso de que se determine si para un estado del proceso a memorizar están presentes estados del sistema asociados.

25 Esta medida posibilita hacer confluír estados de procesos y estados del sistema, que han sido establecidos en un intervalo de tiempo grande, es decir, calcular aquellos estados del sistema, que están asociados a un estado del proceso y preparar mensajes de diagnóstico correspondiente. Entonces es concebible la siguiente constelación: en un instante temprano se establece ya un estado del sistema y, por lo tanto, un error físico, porque, por ejemplo, un sensor está defectuoso. Pero en este instante, no se establece todavía ningún estado del proceso, es decir, ningún error lógico, porque en este instante no se ha llamado todavía, por ejemplo, una rutina contenida en el programa de aplicación, en la que se procesa la señal acondicionada por el sensor. En este caso, se puede realizar una confluencia del estado del proceso y del estado del sistema. En general, esta medida posibilita una instrucción amplia del personal de servicio de una instalación.

35 De manera más ventajosa, la consideración de estados del sistema establecidos ya memorizados y/o de estados de procesos establecidos ya memorizados se realiza porque el cálculo de una magnitud de asociación para un estado del sistema a memorizar y/o para un estado del proceso a memorizar se tienen en cuenta estado del sistema establecidos ya memorizados y/o estados del proceso establecidos ya memorizado. Por una parte, se seleccionan aquellas magnitudes de asociación, que representan las asociaciones predefinidas, que indican a qué estados del proceso está asociado el estado del sistema de memorizar, y, por otra parte, se seleccionan aquellas magnitudes de asociación, que representan aquellas asociaciones predefinidas, que indican qué estados del sistema están asociados al estado del proceso a memorizar. En este caso se tiene en cuenta de manera más ventajosa cuál de las magnitudes de asociación ya han sido seleccionadas en un instante anterior. De esta manera, se evita una nueva representación de mensajes de diagnóstico.

45 De manera más ventajosa, adicionalmente a los estados de procesos establecidos, se memorizan también aquellos mensajes de diagnóstico de procesos, que representan estos estados de procesos. De la misma manera, para los estados del sistema establecidos se memorizan también aquellos mensajes de diagnóstico del sistema que representan estos estados del sistema.

50 La memorización progresiva de los estados de procesos establecidos y de los estados del sistema establecidos en la unidad de memoria de estados tiene otras ventajas. Así, por ejemplo, es posible preparar un mensaje sobre el estado actual de la instalación a controlar. En este caso, además de los estados de procesos establecidos actualmente y los estados del sistema establecidos actualmente también se tiene en cuenta estados de procesos ya establecidos y estados del sistema ya establecidos, que están memorizados en la unidad de memoria de estados. Además, es posible preparar un mensaje, que representa una modificación del estado. Adicionalmente, se puede realizar una evaluación y, por lo tanto, diagnóstico con el propósito de conocer qué mensajes de diagnóstico están presentes actualmente. Además, se puede crear un informe de acontecimientos que contiene datos sobre el instante en el que aparece un mensaje de diagnóstico, es decir, el instante en el que ha sido preparado y el instante en el que ha desaparecido de nuevo un mensaje de diagnóstico, es decir, que ha desaparecido aquella avería, que se

representa en el mensaje de diagnóstico.

En otra configuración preferida de la invención, la unidad de control presenta una unidad de entrada y salida con varias entradas y con varias salidas, en el que la unidad de entrada y salida está configurada para recibir a través de una pluralidad de varias entradas, respectivamente, al menos una de una pluralidad de señales de entrada de control, y para emitir a través de una pluralidad de las varias salidas, respectivamente, al menos una de la pluralidad de señales de salida de control, en el que el programa de aplicación comprende varias variables del programa, en el que las varias variables del programa comprenden una pluralidad de variables de entrada y una pluralidad de variables de salida, en el que de acuerdo con una regla de asociación definida durante la creación del programa de aplicación, por una parte, se asocian las variables de entrada, respectivamente, a una de las entradas y a una señal de entrada de control recibida a través de esta entrada y, por otra parte, se asocian las variables de salida, respectivamente, a una de las salidas y a una señal de salida de control emitida a través de esta salida, en el que las magnitudes de asociación depositadas se crean en función de la regla de asociación.

Esta medida posibilita calcular de una manera sencilla y sin mucho gasto las magnitudes de asociación depositadas, dicho con mayor precisión, las asociaciones predefinidas. Una etapa parcial en la creación de un programa de usuario es en cualquier caso la asociación de las variables de entrada a las señales de entrada de control y, por lo tanto, a los terminales de entrada del control de seguridad y la asociación de las variables de salida a las señales de salida de control y, por lo tanto, a los terminales de salida del control de seguridad, puesto que sin estas asociaciones no es posible un control de la instalación a través del programa de aplicación. Esta asociación se designa habitualmente como mapeo de E/S. A través de esta asociación se conoce el enlace entre, por una parte, el proceso, que se representa a través de las variables de entrada y las variables de salida y, por otra parte, el sistema, que se representa a través de las señales de entrada de control y las señales de salida de control o bien los terminales de entrada y los terminales de salida del control de seguridad. De esta manera, se puede utilizar esta asociación como base para el enlace de los estados del proceso y de los estados del sistema, dicho con mayor precisión la asociación de estados del sistema a estados de procesos. La secuencia, es decir, si una variable está asociada a una señal y, por lo tanto, a un terminal o si una variable está asociada a un terminal y, por lo tanto, a una señal, no tiene importancia en este caso. Solamente es importante que estos tres datos sean combinados.

Con la ayuda del ejemplo siguiente debe ilustrarse el modo de actuación. Si, por ejemplo, existe un error en un terminal de entrada, un llamado error físico, entonces se establece un estado del sistema correspondiente. En virtud del error en el terminal de entrada, también la variable de entrada correspondiente es forzosamente errónea. Si se realiza ahora utilizando esta variable de entrada una consideración del valor límite, que es la base para la fijación de un estado del proceso, entonces en virtud de la variable de entrada errónea se reconoce un error lógico y de esta manera se establece un estado del proceso. En virtud de la información de asociación utilizada para el mapeo de E/S se establece ahora que el estado del sistema establecido está asociado al estado del proceso establecido.

Se reserva desarrollar el principio, que sirve de base para la medida determinante precedente, también en una solicitud autónoma.

En una configuración preferida de la invención, el programa de aplicación es creado a través de la preparación de una pluralidad de componentes de software, en el que la pluralidad de componentes de software corresponden a la pluralidad de componentes de hardware de las instalaciones, en el que al menos a una pluralidad de los componentes de software están asociadas, respectivamente, una pluralidad de los varios estados del proceso así como una pluralidad de mensajes de diagnóstico de proceso, en el que la pluralidad de mensajes de diagnóstico del proceso representan la pluralidad de los varios estados del proceso.

Esta medida posibilita crear de una manera sencilla un programa de aplicación. La asociación de estados de procesos y de mensajes de diagnóstico de procesos, que representan los estados de procesos, a componentes individuales del software tiene varias ventajas. A través de la utilización de componentes de software, a los que están asociados estados de procesos y mensajes de diagnóstico de procesos que representan estos estados de procesos, se garantiza dentro de un programa de aplicación una uniformidad de tal forma que para componentes de hardware de las instalaciones idénticos contenidos en la instalación a controlar, con una selección correspondiente, se pueden preparar componentes de software idénticos entre sí con respecto a la diagnosis de procesos. Esto contribuye en último término también a una elevación de la seguridad contra fallos.

En una configuración preferida de la invención, el programa de aplicación presenta una formación estructurada con varios planos de jerarquía, en el que durante la creación del programa de aplicación se calcula una magnitud de la estructura de las instalaciones, que representa la formación estructurada jerárquicamente del programa de aplicación, en el que la unidad de mensajes de diagnóstico está configurada para preparar la pluralidad de mensajes de diagnóstico en función de la magnitud de la estructura de las instalaciones.

En planos jerárquicos individuales están asociados, respectivamente, una pluralidad de componentes de software, de manera que cada uno de estos componentes de software corresponde a un componente de hardware de la instalación. Si en el componente de hardware de la instalación se trata de un componente sencillo, entonces el

5 componente de software correspondiente está realizado como componente elemental, que no contiene otros componentes de software. En cambio, si en el componente de hardware de la instalación se trata de un componente complejo, entonces el componente de software correspondiente aquí está configurado como componente de grupos, y él mismo contiene de nuevo componentes de software. Los componentes de grupos conducen a la formación estructurada jerárquicamente del programa de aplicación, que corresponde de nuevo a la estructura de la instalación a controlar.

10 La preparación de la pluralidad de mensajes de diagnóstico en función del tamaño de la estructura de la instalación tiene la siguiente ventaja: un estado de proceso establecido está asociado de una manera unívoca a un componente de software. Por consiguiente, para el estado del proceso establecido se puede preparar un mensaje de diagnóstico, que está depositado en el componente de software, al que está asociado. En virtud del tamaño de la estructura de la instalación se conoce de nuevo a qué componente de software del plano jerárquico siguiente superior o a un plano jerárquico colocado todavía más alto está asociado el componente de software condicionado por la estructura, al que está asociado más bien el estado del proceso establecido. Esta asociación condicionada por la estructura se puede utilizar ahora para preparar en lugar de un mensaje de diagnóstico, que está depositado en el componente de software, al que está asociado un estado del proceso establecido, un mensaje de diagnóstico, que está depositado en un componente de software, que está colocado en el plano jerárquico siguiente superior o en un plano jerárquico todavía más alto, y al que está asociado el componente de software condicionado por la estructura, al que está asociado el estado del proceso establecido. Este principio posibilita, por ejemplo, la preparación de un llamado mensaje de diagnóstico colectivo. La preparación de un mensaje de diagnóstico colectivo se ofrece de manera más ventajosa en la siguiente constelación: se establecen varios estados del proceso. Estos estados del proceso no sólo están asociados a un componente de software, sino a varios componentes de software. Estos componentes de software desembocan en la estructura jerárquica del programa de aplicación en un componente de software, que está contenido en un plano jerárquico colocado más alto. En lugar de preparar ahora un mensaje de diagnóstico para cada estado del proceso establecido, se puede preparar un mensaje de diagnóstico que está contenido en el componente de software, en el que desembocan los otros componentes de software. En general, de esta manera se eleva la claridad durante la representación de mensajes de diagnóstico.

Se reserva desarrollar el principio que sirve de base para la medida descrita anteriormente, también en una solicitud autónoma.

30 En otra configuración de la invención, la unidad de evaluación de diagnóstico de procesos presenta una unidad de memoria de diagnóstico de procesos, en la que en la unidad de memoria de diagnóstico de procesos están depositados los varios estados de procesos así como una pluralidad de mensajes de diagnóstico de procesos, en la que los mensajes de diagnóstico de procesos representan, respectivamente, uno de los varios estados de procesos, en la que los varios estados de procesos y/o los mensajes de diagnóstico de procesos son creados durante la creación del programa de aplicación. Además, en la unidad de memoria de diagnóstico de procesos está depositada una magnitud de la estructura de la instalación.

En virtud de esta medida, todas las indicaciones necesarias para una diagnosis de procesos amplia están depositadas de forma coherente en un lugar central. Esto posibilita un establecimiento rápido de estados de procesos. Además, se pueden excluir posibles fuentes de errores, que pueden aparecer durante una deposición de los datos mencionados en varios lugares.

40 En una configuración preferida de la invención, la unidad de evaluación de diagnóstico del sistema presenta una unidad de memoria de diagnóstico del sistema, en la que en la unidad de memoria de diagnóstico del sistema están depositados los varios estados del sistema así como una pluralidad de mensajes de diagnóstico del sistema, en la que los mensajes de diagnóstico del sistema representan, respectivamente, uno de los varios estados del sistema.

45 Esta medida tiene la ventaja de que todas las indicaciones necesarias para una diagnosis del sistema están depositadas de forma centralizada. De esta manera, también es posible en este caso una determinación rápida de estados del sistema. También se excluyen posibles fuentes de errores, que pueden aparecer en el caso de una deposición de los datos mencionados anteriormente en varios lugares de la memoria.

50 De manera más ventajosa, los varios estados del sistema así como la pluralidad de mensajes de diagnóstico del sistema son definidos por el fabricante del control del sistema. Esta medida contribuye a un incremento de la seguridad contra fallos. Además, es ventajoso que tanto los varios estados del sistema como también la pluralidad de mensajes de diagnóstico del sistema estén depositados en la unidad de memoria de diagnóstico del sistema y, por lo tanto, no pueden ser modificados ni por el operador de la instalación ni por el creador del programa de aplicación que se ejecuta en el control del sistema. También esta medida contribuye a una elevación de la seguridad contra fallos.

55 En una configuración preferida de la invención, el control de seguridad está constituido por varios componentes de hardware de control, en el que a una pluralidad de los componentes de hardware de control está asociados, respectivamente, una pluralidad de los varios estados del sistema así como una pluralidad de mensajes de diagnóstico

del sistema, en el que la pluralidad de mensajes de diagnóstico del sistema representan la pluralidad de los varios estados del sistema.

Esta medida asegura que se asocien a un componente de hardware de control, respectivamente, los estados relevantes del sistema así como los mensajes de diagnóstico del sistema asociados a los estados del sistema. Teniendo en cuenta las reglas de asociación definidas es posible de esta manera una asociación unívoca de un estado del sistema a un estado del proceso.

En una configuración preferida de la invención, el control de seguridad presenta una formación estructurada jerárquicamente, en el que en la unidad de memoria de diagnóstico del sistema está depositada una magnitud de la estructura de control, que representa la formación estructurada jerárquicamente del control de seguridad, en el que la unidad de mensajes de diagnóstico está configurada para preparar el número de mensajes de diagnóstico en función de la magnitud de la estructura de control.

Esta medida posibilita también para la diagnóstico del sistema la preparación de mensajes de diagnóstico colectivos ya descrita más arriba en conexión con la diagnóstico de procesos. Por consiguiente, aquí se aplican de manera correspondiente las ventajas indicadas en conexión con la diagnóstico de procesos.

Se reserva desarrollar el principio, que sirve de base para la medida descrita anteriormente también en una solicitud autónoma.

En otra configuración de la invención, el programa de aplicación presenta al menos un módulo de control de seguridad, en el que se procesa a prueba de fallos señales de entrada de control relevantes para la seguridad, y al menos un módulo de control estándar, en el que se procesan de manera predominante señales de entrada de control relevantes para el proceso.

En esta configuración, la pluralidad de sensores comprende de manera más ventajosa una primera pluralidad de sensores, que están configurados para la detección de magnitudes relevantes para la seguridad, de manera que estas magnitudes relevantes para la seguridad son alimentadas por medio de señales de entrada de control relevantes para la seguridad al módulo de control de seguridad, y una segunda pluralidad de sensores, que están configurados para la detección de magnitudes relevantes para el proceso, de manera que estas magnitudes relevantes para el proceso son alimentadas por medio de señales de entrada de control relevantes para el proceso al módulo de normalización. Por lo demás, en esta configuración está previsto de manera más ventajosa que la pluralidad de señales de salida de control comprenda una pluralidad de señales de salida de control, que son calculadas en el módulo de control de seguridad, y que están destinadas para el control de una pluralidad de actuadores, que están configurados para la realización de acciones relevantes para la seguridad, y comprende una segunda pluralidad de señales de salida de control, que son calculadas en el módulo de control normalizado, y que están destinadas para el control de una segunda pluralidad de actuadores, que están configurados para la realización de acciones relevantes del proceso. Esta estructura del programa de aplicación, según la cual el programa de aplicación comprende al menos un módulo de control de seguridad y al menos un módulo de control normalizado, posibilita que con uno y el mismo programa de aplicación se puedan procesar tanto tareas de control, que están asociadas al aspecto de control de seguridad, como también tareas de control, que están asociadas al aspecto de control normalizado. De esta manera, con un control de seguridad configurado de acuerdo con este aspecto se pueden realizar tanto tareas de control, que están asociadas al aspecto de control de seguridad como también tareas de control, que están asociadas al aspecto de control normalizado. Esto tiene la ventaja de que para un control amplio de una instalación, es decir, para un control, que comprende tanto el aspecto de control de seguridad como también el aspecto de control normalizado, solamente es necesario un aparato de control, y no dos aparatos de control, uno de los cuales procesa las tareas de control, que están asociadas al aspecto de control de seguridad, y uno procesa las tareas de control, que están asociadas al aspecto de control normalizado. De esta manera se reduce también el gasto necesario para el cableado. En general, esta medida representa una posibilidad económica para realizar un control amplio para una instalación. En este lugar se hace referencia a que con la formulación de que en el módulo de control normalizado se procesan de manera predominante señales de entrada de control relevantes para el proceso, se entiende que en el módulo de control normalizado se pueden procesar también señales de entrada de control relevantes para la seguridad.

De manera más ventajosa, en la unidad de representación se trata de una unidad de representación integrada en el puesto de mando de la instalación a controlar. Pero se puede tratar también de otra unidad de representación, que está presente adicionalmente a la unidad de representación integrada en el puesto de mando en la instalación a controlar. La unidad de representación puede estar realizada, por ejemplo, como pantalla LCD, como pantalla basada en rayo catódico o como campo de texto alfanumérico.

Para completar, en este lugar se hace la siguiente referencia: si se ha establecido un estado de proceso y no se establecen estados del sistema asociados a este estado del proceso, entonces se prepara como mensaje de diagnóstico aquel mensaje de diagnóstico de procesos que representa el estado de proceso establecido.

Se entiende que las características mencionadas anteriores y explicadas todavía a continuación no sólo se pueden

aplicar en la combinación indicada en cada caso sino también en otras combinaciones o en posición exclusiva, sin abandonar el marco de la presente invención.

Los ejemplos de realización de la invención se representan en el dibujo y se explican en detalle en la descripción siguiente. En este caso:

5 La figura 1 muestra una representación esquemática de una instalación a controlar.

La figura 2 muestra una representación esquemática de un componente parcial de la instalación a controlar.

La figura 3 muestra una representación esquemática de un subcomponente contenido en el componente parcial y sus componentes individuales.

10 La figura 4 muestra una representación simplificada de una superficie gráfica para la creación de un programa de aplicación.

La figura 5 muestra una representación esquemática de los componentes de software para la instalación a controlar acondicionados en un plano jerárquico más alto del programa de aplicación.

La figura 6 muestra una representación esquemática de los componentes de software acondicionados para el componente parcial y los bloques de aspectos.

15 La figura 7 muestra una representación esquemática de los componentes de software acondicionados para el subcomponente y bloques de aspectos.

La figura 8 muestra una representación esquemática de los bloques de aspectos acondicionados para un componente individual contenido en el subcomponente.

La figura 9 muestra en una representación de conjunto la estructura jerárquica de un programa de aplicación creado.

20 La figura 10 muestra en una representación de conjunto la estructura jerárquica de un control de seguridad.

La figura 11 muestra una representación esquemática de un control de seguridad de acuerdo con la invención.

25 En la figura 1 se designa una instalación a controlar en su generalidad con el número de referencia 10. La instalación 10 comprende tres componentes parciales, a saber, una estación de manipulación 12, una estación de proceso 14 y una estación de ensayo 16, así como dos relés 18, 20. Con la estación de manipulación 12 se llena la estación de procesos 14 con piezas de trabajo. Estas piezas de trabajo son procesadas en la estación de procesos 14. A continuación, se transfieren las piezas de trabajo procesadas desde la estación de manipulación 12 hasta la estación de ensayo 16, en la que se verifica si la pieza de trabajo procesada cumple los criterios de ensayo correspondientes. Si se superan estos ensayos, se puede llenar la estación de procesos 14 de nuevo con una nueva pieza de trabajo a procesar. A través de los dos relés 18, 20 se conectan los consumidores 22 de la instalación 10 con una alimentación de corriente no representada. A la instalación está asociado un primer conmutador de desconexión de emergencia 24, con el que se desconecta la instalación 10 en caso de peligro y en este caso se puede transferir a un estado seguro. A tal fin, se activan los dos relés 18, 20, de tal manera que los consumidores 22 son separados de la alimentación de corriente. La instalación 10 se controla a través de un control de seguridad 26, de manera que el control de seguridad 26 está constituido por varios componentes de hardware de control 28, 30, 35, 32. Los componentes de hardware de control individuales pueden estar asociados a componentes parciales individuales, pero esto no tiene que ser forzosamente así. En el presente ejemplo de realización, el componente de hardware de control 28 debe estar asociado al componente parcial 12, el componente de hardware de control 30 debe estar asociado al componente parcial 14 y el componente de hardware de control 32 debe estar asociado al componente parcial 16. Puesto que se trata de una representación esquemática, se ha prescindido de la consideración de cableados.

40 En la figura 2 se designa el componente parcial estación de procesos en su totalidad con el número de referencia 14. Aunque a continuación solamente se consideran la estación de procesos y los componentes de hardware contenidos en ella, esto no debe tener ningún efecto de limitación. Las explicaciones siguientes se aplican de manera correspondiente también para la estación de manipulación 12 y la estación de ensayo 16.

45 La estación de procesos 14 comprende una mesa redonda 40, un módulo de ensayo 42, un módulo de perforación 44 y un módulo de expulsión 46. Con la mesa redonda 40 se pueden transportar todas las piezas de trabajo en la estación de procesos 14 entre los módulos 42, 44, 46 individuales. Con el módulo de ensayo 42 se verifican las piezas de trabajo a procesar con respecto a la presencia de predeterminadas propiedades. Con el módulo de perforación 44 se procesan las piezas de trabajo que se encuentran en la estación de procesos 14. Con el módulo de expulsión 46 se extraen las piezas de trabajo procesadas y se transfieren a la estación de ensayo 16. A la estación de procesos 14 está asociado un segundo conmutador de desconexión de emergencia 48, con el que se

desconecta la estación de procesos 14 en caso necesario y se puede transferir en este caso a un estado seguro.

En la figura 3 se designa el módulo de perforación en su totalidad con el número de referencia 44.

5 El módulo de perforación 44 presenta como componentes individuales con una función mecánica o eléctrica o electromecánica un motor 60, un cilindro de transferencia 64. Con los dos cilindros 62, 64 se puede mover el motor 60 a lo largo de una unidad de guía con relación a la pieza de trabajo a procesar y, en concreto, con el cilindro de perforación 64 en dirección vertical y con el cilindro de transferencia 62 en dirección horizontal. Al módulo de perforación 44 está asociado un tercer conmutador de desconexión de emergencia 66, con el que se puede desconectar en el caso de peligro el módulo de perforación 44 y en este caso se puede transferir a un estado seguro. Con el número de referencia 68 se designan aquellos componentes de hardware del control, que están contenidos en el componente de hardware de control 30, y que están asociados al módulo de perforación 44.

10 Como se puede deducir a partir de las representaciones en las figuras 1 a 3, la instalación 10 a controlar está constituida por una pluralidad de componentes de hardware de la instalación, a saber, al menos por los componentes parciales 12, 14, 16 representados en la figura 1, la mesa redonda 40 representada en la figura 2, el módulo de ensayo 47, el modulo de perforación 44 y el módulo de expulsión 46 así como los componentes representados en la figura 3, es decir, el motor 60, el cilindro de transferencia 62 y el cilindro de perforación 64. A ellos se añaden otros componentes, a saber, aquellos que están contenidos en la estación de manipulación 12 y en la estación de ensayo 16, los que no se ha hecho referencia, sin embargo, explícitamente con anterioridad.

15 De la misma manera, a partir de las representaciones de las figuras 1 a 3 se puede deducir que el control de seguridad está constituido por varios componentes de hardware de control y presenta, en general, una constitución estructurada de forma jerárquica.

20 En la figura 4 se designa una superficie gráfica en su totalidad con el número de referencia 80. Esta superficie gráfica posibilita a un programador la creación de un programa de aplicación.

25 La superficie de usuario gráfica 80 contiene un campo de componentes de software 82, que contiene una cantidad 84 de componentes de software predefinidos en forma de símbolos gráficos. Los componentes de software predefinidos han sido creados por el proveedor del programa de ordenador, con el que se realiza el procedimiento para la creación de un programa de aplicación, y están depositados en una base de datos contenida en este programa de ordenador. El campo de componentes de software 82 contiene, además, una cantidad 86 de componentes de software creados nuevos en forma de símbolos gráficos. En los componentes de software creados nuevos se trata de aquellos componentes de software que son creados por el programador durante la creación del programa de aplicación para componentes de hardware de la instalación contenidos en la instalación 10 a controlar, para los que no están contenidos componentes de software predefinidos correspondientes en la base de datos mencionada anteriormente. La base de datos contenida en el programa de ordenador se amplía con estos componentes de software.

30 Aquellos componentes de software, que no contienen ellos mismos otros componentes de software, se representan con un bloque pequeño. Estos componentes de software se designan como componentes elementales. En cambio, aquellos componentes de software que contienen ellos mismos otros componentes de software, se representan con un bloque grande. Estos componentes de software se designan como componentes de grupos.

35 El programa de aplicación se crea a través de la preparación de una pluralidad de componentes de software. Con esta finalidad, la superficie de usuario gráfica 80 contiene un campo de componentes 88. Los componentes de software a preparar son seleccionados y son transferidos al campo de componentes 88, como se indica por medio de dos flechas 90, 92. La selección y transferencia se pueden realizar, por ejemplo, por medio de una llamada función Drag & Drop.

40 El campo de componentes 88 contiene, por consiguiente, una pluralidad 94 de componentes de software, que han sido preparados. En este caso se trata de los componentes de software del plano jerárquico más alto del programa de usuario. A través de enlace lógico de la pluralidad 94 de componentes de software se crea un programa parcial de componentes. A tal fin, se conectan entre sí al menos una parte de las salidas lógicas de los componentes de software, lo que se representa a través de una pluralidad 96 de conexiones. En virtud de los enlaces lógicos internos contenidos, respectivamente, en los componentes de software, si están contenidos en estos componentes de software componentes elementales y/o componentes de grupos, estos componentes de software contenidos se enlazan de esta manera entre sí de forma automática. Por consiguiente, durante la creación del programa parcial de componentes, es suficiente enlazar lógicamente entre si los componentes de software contenidos en el plano jerárquico más alto.

45 El programa de aplicación está estructurado jerárquicamente. A través de la pluralidad 94 preparada de componentes de software se establece un plano jerárquico más alto. Si esta pluralidad 94 de componentes de software contiene un componente de software, que está configurado como componente de grupo, entonces a través de la pluralidad de componentes de software, que están contenidos en este componente de software, se establece

otro plano jerárquico que se encuentra por debajo del plano jerárquico más alto.

Antes de describir otros campos contenidos en la superficie gráfica 80, se representa en primer lugar la estructura de principio de un componente de software. Esto debe realizarse previamente con la ayuda de la figura 8 que se describirá a continuación.

5 A partir de la figura 8 se puede deducir una estructura de principio de un componente de software configurado como componente elemental. Un componente elemental contiene varios bloques de aspectos. A cada uno de estos bloques de aspectos está asociado uno de varios aspectos de control diferentes entre sí, de manera que cada uno de estos aspectos de control representa un aspecto parcial autónomo del control de seguridad. El componente de software contiene en este caso todos aquellos bloques de aspectos, que son importantes para aquel componente de hardware de la instalación, que representa el componente de software. De esta manera se describe el componente de hardware de la instalación con visión sobre los aspectos parciales del control de seguridad a través del componente de software que lo representa. En comparación con un componente elemental, un componente de grupos contiene, además de los aspectos de bloques, adicionalmente componentes de software, que pueden ser realizados como componente elemental o componente de grupos.

10 De manera más ventajosa, en los aspectos de control diferentes entre sí se puede tratar de los siguientes aspectos de control: aspecto de control normalizado, que representa el aspecto parcial de control normalizado; aspecto de control de seguridad, que representa el aspecto parcial del control de seguridad; aspecto de diagnóstico, que representa el aspecto parcial de diagnóstico; aspecto de visualización, que representa el aspecto parcial de visualización; aspecto de regulación del accionamiento, que representa el aspecto parcial de regulación del accionamiento; aspecto de refrigeración, que representa el aspecto parcial de refrigeración; aspecto de autorización de acceso, que representa el aspecto parcial de la autorización de acceso; aspecto de bloqueo, que representa el aspecto parcial de bloqueo; aspecto de accionamiento manual, que representa el aspecto parcial de accionamiento manual; aspecto de procesamiento de datos, que representa el aspecto parcial de procesamiento de datos.

15 Para cada bloque de aspectos contenido en un componente de software se establecen en primer lugar según el motivo al menos aquellas magnitudes lógicas y/o aquellos parámetros y/o aquellas señales de los sensores, que se necesitan para el procesamiento, y que se pueden alimentar a través de entradas correspondientes al bloque de aspectos, y aquellas magnitudes lógicas y/o aquellos parámetros y/o aquellas señales de salida, que se calculan, respectivamente, en la pluralidad de bloques de aspectos, y que son emitidas a través de salidas correspondientes desde el bloque de aspectos. La determinación de los sensores y/o actuadores concretos, que deben conectarse con el bloque de aspectos respectivo, se realiza en último término ya durante la creación del programa de aplicación.

20 Además, al menos en una parte de los bloques de aspectos contenidos en un componente de software está depositado en cada caso un programa de función, que establece propiedades del aspecto del componente de hardware para aquel aspecto, al que está asociado en bloque de aspectos respectivo.

25 La superficie gráfica 80 contiene, además, un campo de aspectos 98. En este campo de aspectos 98 están dispuestos una pluralidad 100 de bloques de aspectos. Cada uno de estos bloques de aspectos está asociado al mismo aspecto de control. En el ejemplo de realización se trata del aspecto de control normalizado, que representa el aspecto parcial de control normalizado. La pluralidad 100 de bloques de aspectos comprende los bloques de aspectos contenidos en todos los planos de la jerarquía del programa de aplicación, que están asociados al aspecto de control normalizado y, en concreto, independientemente de si están contenidos de forma autónoma en uno de los planos de la jerarquía o están contenidos como parte de un componente de software. El campo del aspecto contiene también los bloques de aspectos, que están contenidos en el plano más alto de la jerarquía del programa de aplicación.

30 La superficie gráfica 80 contiene, además, un campo de sensores 102. En este campo de sensores 102 están dispuestos una pluralidad 104 de símbolos de sensores gráficos. Para cada sensor, que está contenido en la instalación 10 a controlar, el campo de sensores 102 contiene un símbolo de sensor gráfico correspondiente. La pluralidad 104 de símbolos de sensores gráficos representan tanto los sensores relacionados con el aspecto de control de seguridad como también los sensores relacionados con el aspecto de control normalizado, que están contenidos en la instalación 10 a controlar. Como otro campo, la superficie gráfica 80 contiene un campo de actuadores 106. En este campo de actuadores 106 están dispuestos una pluralidad de símbolos de actuadores gráficos. Para cada actuador, que está contenido en la instalación 10 a controlar, el campo de actuadores 106 contiene un símbolo de actuadores gráfico correspondiente. La pluralidad 108 de símbolos de actuadores gráficos comprenden tanto los actuadores contenidos en la instalación de control relacionados con el aspecto de control de seguridad como también los relacionados con el aspecto de control normalizado.

35 Para la pluralidad 100 de bloques de aspectos contenidos en el campo de aspectos 98 se crea un programa parcial de aspectos. A tal fin se realiza al menos para una parte de los bloques de aspectos contenidos en el campo de aspectos 98 tanto para sus entradas como también para sus salidas un llamado mapeo de E/S. Es decir, que al menos a una parte de las entradas de señales se asocian aquellos medios sensores, cuyas señales de sensor son

procesadas en el bloque de aspectos respectivo. Esto se representa a modo de ejemplo por medio de una flecha 110. Además, se asocian al menos a una parte de las salidas de señales unos actuadores, que son activados con las señales de salida calculadas en el bloque de aspectos respectivo. Esto se representa a modo de ejemplo por medio de una flecha 112. De manera alternativa. El mapeo de E/S se puede realizar también a través de entradas textuales en un campo de entrada 114.

En el procedimiento descrito anteriormente para la creación de un programa de aplicación, todas las variables del programa están contenidas en los bloques de aspectos. Por consiguiente, a las entradas de señales de los bloques de aspectos se asocian variables de entrada contenidas en el programa de aplicación y a las salidas de las señales de los bloques de aspectos se asocian variables de salida contenidas en el programa de aplicación. A través de la asociación de los sensores a las entradas de señales se define de esta manera la asociación entre sensores y variables de entrada, dicho con mayor precisión entre señales de entrada de control y variables de entrada. Puesto que se conoce qué sensor está conectado en qué entrada de una unidad de entrada/salida contenida en el control de seguridad, de esta manera se define, en general, la asociación entre entradas, señales de entrada de control y variables de entrada. A través de la asociación de los actuadores a las salidas de señales se define, además, la asociación entre actuadores y variables de salida, dicho con mayor precisión entre variables de salida de control y variables de salida, Puesto que se conoce qué actuador está conectado en qué salida de la unidad de entrada y salida, de esta manera se define la asociación entre salidas, variables de salida de control y variables de salida.

Si se han creado los programas parciales de aspectos para todos los aspectos de control, entonces está totalmente definida la regla de asociación y se pueden crear las magnitudes de asociación a depositar.

En general, para cada aspecto de control está creado un programa parcial de aspectos. Si están creados todos los programas parciales de aspectos, se combinan el programa parcial de componentes y los programas parciales de aspectos para formar el programa de aplicación.

En la figura 5 se representan aquellos componentes de software y bloques de aspectos para la instalación 10 a controlar, que están contenidos en el plano jerárquico más alto.

En particular, se trata de los siguientes componentes de software: un primer componente de software 120, que corresponde a un conmutador de desconexión de emergencia 24 y que está configurado como componente individual. Un segundo componente de software 122, que corresponde a la estación de manipulación 12. Un tercer componente de software 124, que corresponde a la estación de procesos 14. Un cuarto componente de software 126, que corresponde a la estación de ensayo 16. En el que los componentes de software 122, 124, 126 están configurados, respectivamente, como componente de grupos. Cada uno de los componentes de software 122, 124, 126 representa un componente de hardware de la instalación mecánica real presente en la instalación a controlar. Los componentes de software están conectados entre sí para la realización de un primer control del ciclo con una primera pluralidad 128 de conexiones lógicas.

Además, se trata de los siguientes bloques de aspectos: un primer bloque de aspectos 130, que está asociado a un aspecto de control normalizado, un segunda bloque de aspectos 132, que está asociado a un aspecto de control de seguridad, un tercer bloque de aspectos 134, que está asociado a un aspecto de diagnóstico, un cuarto bloque aspectos 136, que está asociado a un primer aspecto de visualización, un quinto bloque de aspectos 138, que está asociado a un aspecto de regulación del accionamiento y un sexto bloque de aspectos 140, que está asociado a un aspecto de bloqueo.

En cada uno de estos bloques de aspectos está depositado un programa de funciones, que está configurado para el procesamiento de aquellas tareas de control, que pertenecen al aspecto de control, al que está asociado el bloque de aspectos respectivo. En el tercer bloque de aspectos 134 están depositados aquellas condiciones de ensayo y mensajes de diagnóstico de procesos, que son necesarias para la realización de una diagnosis de procesos para la instalación 10 a controlar como tal. La instalación 10 a controlar como tal está definida a través de la conexión de la estación de manipulación 12, de la estación de procesos 14 y de la estación de ensayo 16 y, por lo tanto, a través de la conexión de los componentes de software 122, 124, 126 del plano jerárquico más alto del programa de aplicación. Se ha prescindido a la representación de conexiones lógicas entre bloques de aspectos individuales entre sí o bien con un componente de software por razones de claridad.

En la figura 6 se representan los componentes de software y los bloques de aspectos contenidos en el tercer componente de software.

Con el signo de referencia 150 se designa un quinto componente de software, que corresponde al segundo conmutador de desconexión de emergencia 48 y que está configurado como componente elemental. Con el signo de referencia 152 se designa un sexto componente de software, que corresponde a la mesa redonda 40. Con el número de referencia 154 se designa un séptimo componente de software, que corresponde al módulo de ensayo 42. Con el número de referencia 156 se designa un octavo componente de software, que corresponde al módulo de perforación 44. Con el número de referencia 158 se designa un noveno componente de software, que corresponde al módulo de expulsión 46. Los componentes de software 152, 154, 156, 158 están configurados como componentes de grupos.

Los componentes de software están conectados para la realización de un control de ciclo entre sí con una segunda pluralidad 160 de conexiones lógicas. También los componentes de software 152, 154, 156, 158 representan, respectivamente, un componente de hardware de la instalación mecánico real presente en la instalación 10 a controlar.

5 Adicionalmente, el tercer componente de software 124 presenta varios bloques de aspectos. Un séptimo bloque de aspectos 162, que está asociado al aspecto de control normalizado, un octavo bloque de aspectos 164, que está asociado al aspecto de control de seguridad, un noveno bloque de aspectos 166, que está asociado al aspecto de diagnóstico, un décimo bloque de aspectos 168, que está asociado al aspecto de visualización, un undécimo bloque de aspectos 170, que está asociado al aspecto de regulación de accionamiento y un duodécimo bloque de aspectos 172, que está asociado a un programa de funciones. En el noveno bloque de aspectos 166 están depositadas aquellas condiciones de ensayo y aquellos mensajes de diagnóstico de procesos, que son necesarios para la realización de una diagnosis de procesos para la estación de procesos 14 como tal. Se prescinde de la representación de conexiones lógicas entre bloques de aspectos individuales entre sí o bien con un componente de software por razones de claridad.

10 En la figura 7 se representan los componentes de software contenidos en el octavo componente de software 156 y los bloques de aspectos. En este caso se trata de un décimo componente de software 180, que corresponde al tercer conmutador de desconexión de emergencia 66. De trata de un undécimo componente de software 184, que corresponde al cilindro de perforación 64, de un duodécimo componente de software 184, que corresponde al cilindro de transferencia y de un décimo tercer componente de software 186, que corresponde al motor 60. Estos componentes de software están configurados como componentes elementales.

Además, el octavo componente de software 156 contiene un décimo tercero bloque de aspectos 188, que está asociado al aspecto de control normalizado, un décimo quinto bloque de aspectos 192, que está asociado a aspecto de diagnóstico, un décimo sexto bloque de aspectos 194, que está asociado al aspecto de visualización, un décimo séptimo bloque de aspectos 196, que está asociado al aspecto de regulación del accionamiento, y un décimo octavo bloque de aspectos 198, que está asociado al aspecto de bloqueo. En el décimo quinto bloque de aspectos 192 están depositadas aquellas condiciones de ensayo y mensajes de diagnóstico de procesos, que son necesarios para la realización de una diagnosis de procesos para el módulo de perforación 44 como tal.

Los componentes de software y una parte de los bloques de aspectos están conectados entre sí para la realización de un control del ciclo a través de una pluralidad de conexiones lógicas. Se prescinde de la representación completa de las conexiones lógicas por razones de claridad.

En la figura 8 se representan aquellos bloques de aspectos, que están contenidos en un componente de software, que corresponde a un cilindro contenido en la instalación 10 a controlar. En el presente ejemplo de realización, éste es por ejemplo el undécimo componente de software 182. Sin embargo, esto no debe tener ningún efecto de limitación; las explicaciones siguientes se aplican de la misma manera al duodécimo componente de software 184.

35 El undécimo componente de software 182 contiene un décimo noveno bloque de aspectos 210, que está asociado al aspecto de control normalizado y un vigésimo bloque de aspectos 212, que está asociado al aspecto de diagnóstico. Puesto que el modo de trabajo de un bloque de aspectos asociado al aspecto de diagnóstico debe explicarse con la ayuda del aspecto de control normalizado, no se representan otros bloques de aspectos en la figura 8.

40 Al décimo noveno bloque de aspectos 210 se alimentan a través de cuartas conexiones lógicas 214 unas señales, que son generadas por dos sensores de posición final, y que indican en cada caso que el cilindro de perforación 64 adopta una de las dos posiciones finales extremas. Estas dos señales son alimentadas de la misma manera al vigésimo bloque de aspectos 212 a través de las cuartas conexiones lógicas 214. En el décimo noveno bloque de aspectos 210 se generan de acuerdo con el programa de funciones depositado en él unas señales de salida de control, con las que se controla el cilindro de perforación 64. Estas señales de salida de control son alimentadas al vigésimo bloque de aspectos 212 a través de quintas conexiones lógicas 216. El vigésimo bloque de aspectos 212 realiza una diagnosis de procesos en función de las señales alimentadas al mismo. Con la ayuda de esta diagnosis de procesos se puede establecer los siguientes estados del proceso: "El cilindro no está introducido", "El cilindro no está extendido"; "Ambos conmutadores finales están activados". El mensaje de diagnóstico de procesos, que representa el estado del proceso establecido, se emite a través de una sexta conexión lógica 218.

50 En la figura 9 se designa una primera estructura jerárquica en su totalidad con el número de referencia 220.

Esta primera estructura jerárquica representa tanto aquella estructura jerárquica, que sirve de base para la instalación 10 a controlar, como también aquella estructura jerárquica, que sirve de base para el programa de aplicación para el control de seguridad. En la representación seleccionada para la figura 9, cada bloque tiene dos significados. Con el número de referencia que está delante del trazo inclinado se indica qué componente de hardware de la instalación 10 a controlar representa el bloque respectivo. Con el número de referencia que está detrás del trazo inclinado se indica qué componente de software representa el bloque respectivo en el programa de

aplicación.

5 Con el número de referencia 222 se designa un bloque, que representa la instalación 10 a controlar en su totalidad o el programa de aplicación en su totalidad. Con el número de referencia 224 se designa un plano jerárquico superior de la instalación, cuyos componentes de hardware de la instalación se designan como componentes parciales. Con el número de referencia 226 se designa un primer plano jerárquico de la instalación, que se encuentra directamente debajo del plano jerárquico más alto de la instalación y cuyos componentes de hardware de la instalación se designan como subcomponentes. Con el número de referencia 228 se designa un segundo plano jerárquico de la instalación, que se encuentra directamente debajo del primer plano jerárquico de la instalación y cuyos componentes de hardware de la instalación se designan como componentes individuales. En la figura 9 no se representa para cada componente parcial representado el plano jerárquico de la instalación y tampoco se representa para cada subcomponente representado el segundo plano jerárquico de la instalación. Esto no tiene que tener ningún efecto de limitación.

15 A los bloques individuales contenidos en la estructura están asociados estados de procesos y mensajes de diagnóstico de procesos, que representan los estados de procesos. Así, por ejemplo, al bloque 60/180 está asociado el estado de procesos "sobrecarga del motor" y el mensaje de diagnóstico del proceso correspondiente "sobrecarga del motor". A los bloques 62/184 y 64/182 están asociados varios estados de procesos. Un primer estado de procesos "posición del cilindro" con los dos mensajes de diagnóstico del proceso "El cilindro no está insertado" y "El cilindro no está extendido". Un segundo estado del proceso "conmutador de posición extrema" con el mensaje de diagnóstico de procesos "ambos conmutadores de posiciones extremas están activados". Un tercer estado del proceso "Estado de la señal" con el mensaje de diagnóstico "Señal de entrada/salida no válida". Un cuarto estado del proceso "Condición temporal" con los dos mensajes de diagnóstico de procesos "Tiempo de entrada excedido" y "Tiempo de salida excedido". A los bloques 2/120, 48/150 y 66/180 están asociados dos estados del proceso. Un primer estado del proceso "Estado" con el mensaje de diagnóstico de procesos "Presionado" y un segundo estado de procesos "Activación" con el mensaje de diagnóstico de procesos "Ninguna activación".

25 En virtud de la estructura jerárquica se pueden transferir estados de procesos, que aparecen, por ejemplo, en un bloque del segundo plano jerárquico de la instalación, al bloque asociado en el primer plano jerárquico de la instalación o incluso del plano jerárquico más alto de la instalación.

30 En la figura 10 se designa una segunda estructura jerárquica en su totalidad con el número de referencia 240. Esta segunda estructura jerárquica reproduce la estructura de los componentes de hardware de control 68 contenidos en el control de seguridad teniendo en cuenta el tercer conmutador de desconexión de emergencia 66. Por lo tanto, de aquellos componentes de hardware de control, que están asociados al módulo de perforación 44. La limitación al módulo de perforación 44 no tiene que tener ningún efecto de limitación. Evidentemente, para todo el control de seguridad, con el que se controla la instalación 10, se puede indicar una estructura jerárquica correspondiente.

35 Con el número de referencia 242 se designa una unidad lógica, en la que se ejecuta aquella parte del programa de aplicación, con la que se controla el módulo de perforación 44. La unidad lógica 242 define un plano jerárquico más alto del control, que se encuentra directamente debajo del plano jerárquico más alto. Con el número de referencia 246 se designa un segundo plano jerárquico de control, que se encuentra directamente debajo del primer plano jerárquico de control. Con el número de referencia 248 se designa un tercer plano jerárquico de control, que se encuentra directamente debajo del segundo plano jerárquico de control.

40 En el primer plano jerárquico de control 244 están contenidas una unidad de bus normalizado 250, que está asociada al aspecto de control normalizado, y una unidad de bus de seguridad 252, que está asociada al aspecto de control de seguridad. A través de estas dos unidades de bus se lleva a cabo la transmisión de datos, separados de acuerdo con datos relevantes para la seguridad y datos relevantes del proceso.

45 En el segundo plano de la jerarquía de control 246 está dispuesta una primera pluralidad 254 de módulos de entrada y salida, que están conectados con la unidad de bus normalizado 250. Estos módulos de entrada y salida ponen a disposición una pluralidad 256 de salidas normalizadas, a través de las cuales se pueden emitir señales de salida de control para la activación de actuadores. Además, estos módulos de entrada y salida proporcionan una pluralidad 258 de entradas normalizadas, a través de las cuales se pueden recibir señales de entrada de control.

50 En el segundo plano jerárquico de control 246 está dispuesta una segunda pluralidad 260 de módulos de entrada y salida, que están conectados con la unidad de bus de seguridad 252. Estos módulos de entrada y salida proporcionan una pluralidad 262 de entradas de seguridad y una pluralidad no representada de salidas de seguridad.

55 Al tercer plano jerárquico de control 248 pueden estar asociados, por ejemplo, los siguientes mensajes de diagnóstico del sistema: "Defecto del hardware", "Cortocircuito hacia 0V", "Cortocircuito hacia 24V". Al segundo plano jerárquico de control 246 pueden estar asociados, por ejemplo, los siguientes mensajes de diagnóstico: "Módulo defectuoso", "Error de Internet", "Error de la tensión de alimentación". Tanto al primer plano jerárquico de control 244 como también al plano jerárquico de control más alto pueden estar asociados, por ejemplo, los siguientes mensajes de

diagnosis del sistema: "Error de Internet", "Error de la tensión de almacenamiento". Evidentemente, los mensajes de diagnosis del sistema pueden estar asociados a los módulos o unidades individuales.

5 En la figura 11 se representa un circuito de seguridad designado en su generalidad con el número de referencia 270, que presenta un control de seguridad 26, que está configurado para controlar una instalación designada en su generalidad con el número de referencia 10. La instalación 10 comprende una pluralidad 272 de actuadores y una pluralidad 274 de sensores. Los consumidores contenidos en la instalación 10 están designados con el número de referencia 22.

10 El control de seguridad 26 comprende una unidad de control 276. La unidad de control 276 está constituido redundante de dos canales para conseguir la seguridad contra fallos necesario para el control de procesos críticos de seguridad. Como representación de la estructura de dos canales se representan en la figura 11 dos procesadores 78, 280 separados uno del otro, que están en conexión entre sí a través de una interfaz de comunicación bidireccional 282, para poder controlarse mutuamente y poder intercambiar datos. Con preferencia, los dos canales de la unidad de control 276 y los dos procesadores 278, 280, están constituidos diferentes, es decir, distintos uno del otro, para excluir en gran medida errores sistemáticos.

15 Con el número de referencia 284 se designa una unidad de entrada y salida, que está en conexión don cada uno de los dos procesadores 278, 280. La unidad de entrada y salida 284 recibe una pluralidad 286 de señales de entrada de control desde una pluralidad 274 de sensores y las transmite en un formato de datos adaptado a cada uno de los dos procesadores 278, 280. Además, la unidad de entrada y salida 284 genera, en función de los procesadores 278, 280 una pluralidad 288 de señales de salida de control, con las que se activan la pluralidad 272 de actuadores.

20 Con el número de referencia 290 se designa una tarjeta de chip, sobre la que se memoriza un programa de aplicación 292. El programa de aplicación 292 se crea con la ayuda de una herramienta de programación. En la herramienta de programación se trata, por ejemplo de un programa de ordenador 294, que se puede ejecutar en un PC 296 convencional. La utilización de una tarjeta de chip 290 como medio posibilita en este caso una sustitución sencilla del programa de aplicación 292 también sin conexión directa en el PC 296, en el que se ejecuta la herramienta de programación. De manera alternativa a ello, el programa de aplicación 292 puede estar memorizado también en una memoria incorporada fijamente en la unidad de control 276, por ejemplo una EEPROM. La reproducción del programa de aplicación en la tarjeta de chip 290 se indica por medio de una línea 297.

30 El programa de aplicación 292 establece las tareas de control a realizar por el control de seguridad 26. A tal fin, el programa de aplicación 292 recibe un módulo de control de seguridad 298, en el que se ejecutan aquellas tareas de control, que están asociadas al aspecto de control de seguridad. En el módulo de control de seguridad 298 se procesas a prueba de fallos señales de entrada de control 300 relevantes para la seguridad, que son generadas por sensores de seguridad 302 asociados al aspecto de control de seguridad. En los sensores de seguridad 302 se trata, por ejemplo, de conmutadores de desconexión de emergencia, controles de dos manso, puertas de protección, aparatos de supervisión del número de revoluciones u otros sensores para la recepción de parámetros relevantes para la seguridad. De acuerdo con las tareas de control asociadas en el aspecto de control de seguridad se activan, en función de las señales de entrada de control 300 relevantes para la seguridad las señales de salida de control 304 relevantes para la seguridad, con las que se activan relés 18, 20, los llamados actuadores de seguridad, es decir, actuadores que están asociados al aspecto de control de seguridad. Los contactos de trabajo de los relés 18,20 están dispuestos en la conexión entre una alimentación de corriente 306 y los consumidores 22. A través de los relés 18,20 se puede desconectar la alimentación de corriente de los consumidores 22, con lo que es posible, en el caso de que aparezca una función errónea correspondiente, transferir los consumidores 22 a un estado seguro.

35 Además, el programa de aplicación 292 presenta un módulo de control estándar 308, con el que se realizan aquellas tareas de control, que están asociadas al aspecto de control estándar. A tal fin se generan en el módulo de control estándar 308 señale de entrada de control 310 relevantes del proceso, que son generadas por sensores estándar 312. En los sensores estándar 312 se trata de aquellos sensores, que detectan, por ejemplo, magnitudes de entrada necesarias para una regulación del accionamiento. En este caso se puede tratar, por ejemplo, de números de revoluciones, ángulos o velocidades. En función de las señales de entrada de procesos 310 relevantes de procesos se generan, de acuerdo con las tareas de control asociadas al aspecto de control normalizado, unas señales de entrada de control 314 relevantes de procesos, que son alimentadas a actuadores normalizados 316. En los actuadores normalizados 316 se puede tratar, por ejemplo, de motores o servo cilindros.

50 La estructura seleccionada en el ejemplo de realización del programa de aplicación 292, de acuerdo con el cual éste contiene un módulo de control de seguridad 298 y un módulo de control normalizado 308, por lo que por la unidad de control 276 se realizan tanto tareas de control, que están asociadas al aspecto de control de seguridad, como también tareas de control, que están asociadas al aspecto e control normalizado, no debe tener ningún efecto de limitación. Evidentemente también es concebible que la unidad de control 276 solamente realice tareas de control que están asociadas al aspecto de control de seguridad. En este caso, el programa de aplicación 292 no contiene ningún módulo de control normalizado 308.

La unidad de entrada y salida 284 sirve también para la conexión de otros componentes contenidos en el control de seguridad 26 en los dos procesadores 278, 280. De esta manera, se alimentan a una unidad de evaluación de diagnóstico de procesos 318, partiendo desde la unidad de entrada y salida 294, una pluralidad 320 de señales de entrada de diagnóstico de procesos, La unidad de evaluación de diagnóstico de procesos 318 está configurada para establecer, en función de la pluralidad 320 de señales de entrada de diagnóstico de proceso, cuál de varios estados de procesos de la instalación 10 a controlar está presente en un primer instante definido. La unidad de evaluación de diagnóstico de procesos 318 genera una pluralidad 322 de señales de estados de procesos, de manera que la pluralidad 322 de señales de estados de procesos representa una pluralidad de estados de procesos establecidos, de manera que la pluralidad de estados de procesos establecidos están presentes en el primer instante definido. La pluralidad 322 de señales de estados de procesos son alimentados a la unidad de entrada y salida 284. De esta manera, la unidad de control 276 puede tomar medidas adecuadas de acuerdo con los estados de procesos establecidos.

Además, se alimentan a una unidad de evaluación de diagnóstico del sistema 324, partiendo desde la unidad de entrada y salida 284 una pluralidad 326 de señales de entrada de diagnóstico del sistema. La unidad de evaluación de diagnóstico del sistema 324 está configurada para establecer, en función de la pluralidad 326 de señales de entrada de diagnóstico del sistema, cuál de varios estados del sistema del control de seguridad 26 está presente en un segundo instante definido, estando configurada la unidad de evaluación de diagnóstico del sistema 324 para generar una pluralidad 328 de señales de estado del sistema, de manera que la pluralidad 328 de señales de estado del sistema representa una pluralidad de estados del sistema establecidos, de manera que la pluralidad de estados del sistema establecidos están presentes en un segundo instante definido. La pluralidad 328 de señales de estado del sistema son alimentadas a la unidad de entrada y salida 284. De esta manera, la unidad de control puede tomar medidas adecuadas de acuerdo con los estados del proceso establecidos.

Un estado del sistema debe detectar en este caso no sólo las unidades y componentes contenidos en el control de seguridad 26, sino también todas las unidades conectadas eléctricamente con el control de seguridad. En este caso, se trata de los sensores de seguridad 302, los relés 18, 20, formulado de forma general los actuadores de seguridad, los sensores normalizados 312, los actuadores normalizados 316 así como una unidad de representación que se describirá más adelante y una unidad de solicitud de diagnóstico del sistema que se describirá más adelante. De la misma manera, el estado del sistema debe comprender todos los cableados presentes entre el control de seguridad 26 y las unidades enumeradas anteriormente.

El control de seguridad 26 comprende una interfaz 330 para una unidad de representación 332. La unidad de representación 332 está configurada para representar mensajes de diagnóstico. Además, el control de seguridad 26 comprende una interfaz 334 para una unidad de solicitud de diagnóstico del sistema, que está configurada para detectar una solicitud de diagnóstico del sistema 337. La unidad de representación 332 y la unidad de solicitud de diagnóstico del sistema 336 pueden formar una unidad constructiva 338.

Además, el control de seguridad 26 presenta una unidad de mensajes de diagnóstico 340. A la unidad de mensajes de diagnóstico 340 se alimentan la pluralidad 322 de señales de estados de procesos y la pluralidad 328 de señales de estados del sistema. Además, se alimentan a la unidad de mensajes de diagnóstico 340, por una parte, una pluralidad 342 de mensajes de diagnóstico de procesos, en la que los mensajes de diagnóstico de procesos representan los estados de procesos establecidos. Por otra parte, a la unidad de mensajes de diagnóstico 340 se alimentan una pluralidad 344 de mensajes de diagnóstico del sistema. En la que los mensajes de diagnóstico del sistema representan estados del sistema establecidos.

La unidad de mensajes de diagnóstico acondiciona una pluralidad de mensajes de diagnóstico para la pluralidad de estados de procesos establecidos y para la pluralidad de estados del sistema establecidos. En este caso al menos para uno de los estados de procesos establecidos se acondiciona un mensaje de diagnóstico en función de este estado del proceso y de una pluralidad de estados del sistema asociados, que están contenidos en la pluralidad de estados del sistema establecidos y están asociados a este estado del proceso. La unidad de mensajes de diagnóstico 340 genera una pluralidad 346 de señales de diagnóstico, en la que la pluralidad de señales de diagnóstico representa la pluralidad de mensajes de diagnóstico. La pluralidad 346 de señales de diagnóstico son alimentadas a la unidad de representación 332 a través de una unidad de entrada y salida 284 para la representación de la pluralidad de mensajes de diagnóstico.

La unidad de evaluación de diagnóstico del proceso 318, la unidad de evaluación de diagnóstico del sistema 324 y la unidad de mensajes de diagnóstico 340 son agrupados en una unidad de diagnóstico 348.

La unidad de mensajes de diagnóstico 340 presenta una unidad de memoria de asociación 350, en la que al menos para una pluralidad de varios estados de proceso y al menos para una pluralidad de varios estados del sistema están depositadas una pluralidad de magnitudes de asociación. Las magnitudes de asociación depositadas indican cuál de los varios estados de procesos está asociado, respectivamente, a cuál de los varios estados del proceso en virtud de una asociación predefinida. Para una pluralidad de parejas de la pluralidad de estados establecidos del sistema y de la pluralidad de estados del proceso establecidos, se seleccionan una pluralidad de magnitudes de

asociación depositadas. Cada una de estas magnitudes de asociación seleccionada representa al menos una de las parejas. La pluralidad de estados del sistema asociados se calcula en función de la pluralidad de magnitudes de asociación.

5 La unidad de mensajes de diagnóstico 340 presenta una unidad de memoria de estado 352, que está configurada para memorizar de manera progresiva estados de procesos establecidos y estados del sistema establecidos. La unidad de mensajes de diagnóstico 340 está configurada para tener en cuenta estados del proceso establecidos ya memorizados y/o estados del sistema establecidos ya memorizados en el caso de que se determine si en el estado del sistema a memorizar se trata de un estado del sistema asociado y/o en el caso de que se determine si para un estado del proceso a memorizar están presentes estados del sistema asociados.

10 La unidad de evaluación de diagnóstico de procesos 318 presenta una unidad de memoria de diagnóstico de procesos 354, en la que están depositados los varios estados de procesos, los mensajes de diagnóstico de procesos que los representan y una magnitud de la estructura de la instalación. En general, estos son preparados durante la creación del programa de aplicación 292 y son transmitidos a la unidad de memoria de diagnóstico de procesos 354, lo que se indica por medio de una línea 356. De manera alternativa, estas informaciones pueden ser transmitidas también a través de una línea 297 sobre la tarjeta de chip 290 y desde ésta hasta la unidad de memoria de diagnóstico de procesos 354. La magnitud de la instalación es proporcionada a la unidad de mensajes de diagnóstico 340, lo que se indica por medio de una línea 358.

15 Las magnitudes de asociación depositadas en la unidad de memoria de asociación 350 son creadas de la misma manera del programa de aplicación 292 y son alimentadas a la unidad de memoria de asociación 350, lo que se indica a través de una línea 350.

20 La unidad de evaluación de diagnóstico normalizada 324 presenta una unidad de memoria de diagnóstico del sistema 362, en la que están depositados los varios estados del sistema así como una pluralidad de mensajes de diagnóstico del sistema, de manera que los mensajes de diagnóstico del sistema representan, respectivamente, uno de los varios estados del sistema. Estas informaciones están depositadas fijamente y proceden del fabricante del control de seguridad 26. Además, en la unidad de memoria de diagnóstico del sistema 362 deposita una magnitud de la estructura de control, que se proporciona a la unidad de mensajes de diagnóstico 340, lo que se indica a través de una línea 364.

25 A través de la unidad de entrada y salida 284 se intercambian señales de ensayo 364 entre el control de seguridad 26 y los sensores de seguridad 302, los relés 18, 20, la unidad de representación 332, la unidad de solicitud de diagnóstico del sistema 336. Con la ayuda de las señales de ensayo 364 se puede establecer en el control de seguridad 26 si las unidades y componentes conectados, lo que es necesario, puesto que debe garantizarse un estado seguro de la instalación 10 a controlar, tan pronto como aparece una función errónea en un aparato conectado con el control de seguridad 26.

35

40

45

## REIVINDICACIONES

- 1.- Control de seguridad para el control de una instalación automática (10) con una pluralidad de componentes de hardware de la instalación (12, 14, 16), que comprende una pluralidad de sensores y una pluralidad de actuadores,
- 5 con una unidad de control (276), a la que están asociadas una pluralidad de señales de entrada de control desde una pluralidad de sensores, en el que la unidad de control está configurada para generar una pluralidad de señales de salida de control en función de las señales de entrada de control de acuerdo con un programa de aplicación (292) que se ejecuta en ella, en el que con una pluralidad de señales de salida de control se activan la pluralidad de actuadores,
- 10 con una interfaz (330) para una unidad de representación (332), en el que la unidad de representación está configurada para representar mensajes de diagnóstico,
- 15 con una unidad de evaluación de diagnóstico de procesos (318), a la que se alimentan una pluralidad de señales de salida de diagnóstico de procesos, en el que la unidad de evaluación de diagnóstico de procesos está configurada para establecer en función de la pluralidad de señales de salida de diagnóstico de procesos, cuál de varios estados de procesos de la instalación a controlar está presente en un primer instante definido, en el que la unidad de evaluación de diagnóstico de procesos está configurada para generar una pluralidad de señales de estado de procesos, en el que la pluralidad de señales de estado de procesos representa una pluralidad de estados de procesos establecidos, en el que la pluralidad de estados de procesos establecidos están presentes en el primer instante definido,
- 20 con una unidad de evaluación de diagnóstico del sistema (324), a la que se alimentan una pluralidad de señales de entrada de diagnóstico del sistema, en el que la unidad de evaluación de diagnóstico del sistema está configurada para establecer en función del número de señales de entrada de diagnóstico del sistema, cuál de varios estados del sistema del control de seguridad está presente en un segundo instante definido, en el que la unidad de evaluación de diagnóstico del sistema está configurada para generar una pluralidad de señales del estado del sistema, en el que la pluralidad de señales de estado del sistema representa una pluralidad de estados del sistema establecidos, en el que la pluralidad de estados del sistema establecidos están presentes en el segundo instante definido, y
- 25 con una unidad de mensajes de diagnóstico (340), a la que se alimentan la pluralidad de señales de estado de proceso y la pluralidad de señales de estado del sistema, en el que la unidad de mensajes de diagnóstico está configurada para acondicionar una pluralidad de mensajes de diagnóstico para la pluralidad de estados de proceso establecidos y para la pluralidad de estados del sistema establecidos, en el que la unidad de mensajes de diagnóstico genera una pluralidad de señales de diagnóstico, que representan los mensajes de diagnóstico, en el que la pluralidad de señales de diagnóstico son conducidos a la unidad de representación para la representación de los mensajes de diagnóstico.
- 30 **caracterizado** porque la unidad de mensajes de diagnóstico presenta una unidad de memoria de asociación (350), en la que están depositadas una pluralidad de magnitudes de asociación al menos para una pluralidad de los varios estados de proceso y al menos para una pluralidad de los varios estados del sistema, en el que las magnitudes de asociación depositadas representan cuál de los varios estados del sistema está asociado, respectivamente, a cual de los varios estados de proceso en virtud de una asociación predefinida, en el que la unidad de mensajes de diagnóstico está configurada para seleccionar una pluralidad de magnitudes de asociación depositadas para una pluralidad de parejas de los estados del sistema establecidos y de los estados de proceso establecidos, en el que cada una de estas magnitudes de asociación seleccionadas representa al menos una de las parejas, en el que la
- 35 unidad de mensajes de diagnóstico está configurada para calcular una pluralidad de estados del sistema asociados en función de las magnitudes de asociación, y en el que al menos para uno de los estados de proceso establecidos se prepara un mensaje de diagnóstico en función de este estado del proceso y del número de estados del sistema asociados, que están asociados a este estado del proceso.
- 40
- 45 2.- Control de seguridad de acuerdo con la reivindicación 1, **caracterizado** porque la unidad de mensajes de diagnóstico está configurada para representar una pluralidad de magnitudes de asociación, en el que las magnitudes de asociación representan cuál de los estados del sistema establecidos está asociado a cuál de la pluralidad de estados de proceso establecidos, en el que la unidad de mensajes de diagnóstico está configurada para calcular el número de estados del sistema asociados en función del número de magnitudes de asociación.
- 50 3.- Sistema de seguridad de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque la unidad de mensajes de diagnóstico está configurada para preparar, en el caso de presencia de un estado del proceso establecido y de una pluralidad de estados del sistema asociados, como mensaje de diagnóstico para este estado del proceso, una pluralidad de mensajes de diagnóstico del sistema, en el que la pluralidad de mensajes de diagnóstico del sistema representan la pluralidad de estados del sistema asociados.
- 55 4.- Sistema de seguridad de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque la unidad de mensajes de diagnóstico está configurada para preparar un mensaje de diagnóstico combinado en el caso de presencia de un estado del proceso establecido y de una pluralidad de estados del sistema asociados, como mensaje de

diagnos para este estado del proceso, en el que el mensaje de diagnos combinado contiene tanto un mensaje de diagnos de proceso como también una pluralidad de mensajes de diagnos del sistema, en el que el mensaje de diagnos del proceso representa el estado del proceso establecido y la pluralidad de mensajes de diagnos representan la pluralidad de estados del sistema asociados.

5 5.- Sistema de seguridad de acuerdo con la reivindicación 4, **caracterizado** porque la unidad de representación está configurada para

- representar en primer lugar el mensaje de diagnos del proceso y en el caso de presencia de una solicitud de diagnos del sistema, sustituir el mensaje de diagnos del proceso por al menos uno de la pluralidad de mensajes de diagnos del sistema o de forma complementaria al mensaje de diagnos del proceso, representar al menos uno de la pluralidad de mensajes de diagnos del sistema, o

10 - representar el mensaje de diagnos del proceso y al menos uno de la pluralidad de mensajes de diagnos del sistema, o

- representar solamente al menos uno de la pluralidad de mensajes de diagnos del sistema.

15 6.- Sistema de seguridad de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque la unidad de mensajes de diagnos está configurada para preparar como un primer mensaje de diagnos al menos un mensaje de diagnos del proceso, en el caso de presencia de un estado del proceso establecido y de una pluralidad de estados del sistema establecidos, y preparar como un segundo mensaje de diagnos adicionalmente una pluralidad de mensajes de diagnos del sistema en el caso de presencia de una solicitud de diagnos del sistema, en el que el mensaje de diagnos del proceso representa el estado del proceso establecido y la pluralidad de mensajes de diagnos del sistema representan la pluralidad de estados del sistema asociados.

20 7.- Sistema de seguridad de acuerdo con la reivindicación 6, **caracterizado** porque la unidad de representación está configurada para sustituir el mensaje de diagnos del proceso por al menos uno de la pluralidad de mensajes de diagnos del sistema o para representar al menos uno de la pluralidad de mensajes de diagnos del sistema como complemento del mensaje de diagnos del proceso.

25 8.- Sistema de seguridad de acuerdo con la reivindicación 5 ó 6, **caracterizado** porque a la unidad de representación está asociada una unidad de solicitud de diagnos del sistema, en el que la unidad de solicitud de diagnos del sistema está configurada para detectar una solicitud de diagnos del sistema.

30 9.- Sistema de seguridad de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque la unidad de evaluación de diagnos del proceso está configurada para establecer progresivamente cuán de varios estados del procesos está presente en cada caso en un instante definido, y/o porque la unidad de evaluación de diagnos del sistema está configurado para establecer de forma progresiva cuál de varios estados del sistema está presente en cada caso en un instante definido.

35 10.- Sistema de seguridad de acuerdo con la reivindicación 9, **caracterizado** porque la unidad de mensajes de diagnos presenta una unidad de memoria de estados, que está configurada para memorizar progresivamente estados de proceso establecidos y estados del sistema establecidos, en el que la unidad de mensajes de diagnos está configurada para tener en cuenta estados del proceso establecidos ya memorizados y/o estados del sistema establecidos ya memorizados en el caso de que se determine si en el estado del sistema a memorizar se trata de un estado del sistema asociado y/o en el caso de que se determine si para un estado del proceso a memorizar están presentes estados del sistema asociados.

40 11.- Sistema de seguridad de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque la unidad de control presenta una unidad de entrada y salida con varias entradas y con varias salidas, en el que la unidad de entrada y salida está configurada para recibir a través de una pluralidad de varias entradas, respectivamente, al menos una pluralidad de señales de entrada de control, y para emitir a través de una de la pluralidad de las varias salidas, respectivamente, al menos una de la pluralidad de señales de salida de control, en el que el programa de aplicación comprende varias variables del programa, en el que las varias variables del programa comprenden una pluralidad de variables de entrada y una pluralidad de variables de salida, en el que de acuerdo con una regla de asociación definida durante la creación del programa de aplicación, por una parte, se asocian las variables de entrada, respectivamente, a una de las entradas y a una señal de entrada de control recibida a través de esta entrada y, por otra parte, se asocian las variables de salida, respectivamente, a una de las salidas y a una señal de salida de control emitida a través de esta salida, en el que las magnitudes de asociación depositadas se crean en función de la regla de asociación.

45 50 55 12.- Sistema de seguridad de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque el programa de aplicación es creado a través de la preparación de una pluralidad de componentes de software, en el que la pluralidad de componentes de software corresponden a la pluralidad de componentes de hardware de las instalaciones, en el que al menos a una pluralidad de los componentes de software están asociadas,

respectivamente, una pluralidad de los varios estados del proceso así como una pluralidad de mensajes de diagnóstico de proceso, en el que la pluralidad de mensajes de diagnóstico del proceso representan la pluralidad de los varios estados del proceso.

- 5 13.- Sistema de seguridad de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque el programa de aplicación presenta una formación estructurada con varios planos de jerarquía, en el que durante la creación del programa de aplicación se calcula una magnitud de la estructura de las instalaciones, que representa la formación estructurada jerárquicamente del programa de aplicación, en el que la unidad de mensajes de diagnóstico está configurada para preparar la pluralidad de mensajes de diagnóstico en función de la magnitud de la estructura de las instalaciones.
- 10 14.- Sistema de seguridad de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque la unidad de evaluación de diagnóstico del sistema presenta una unidad de memoria de diagnóstico del sistema, en el que en la unidad de memoria de diagnóstico del sistema están depositados los varios estados del sistema así como una pluralidad de mensajes de diagnóstico del sistema, en el que los mensajes de diagnóstico del sistema representan, respectivamente, uno de los varios estados del sistema.
- 15 15.- Sistema de seguridad de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque el control de seguridad está constituido por varios componentes de hardware de control, en el que al menos a una pluralidad de los componentes de hardware de control están asociados, respectivamente, una pluralidad de varios estados del sistema así como una pluralidad de mensajes de diagnóstico del sistema, en el que la pluralidad de mensajes de diagnóstico del sistema representan la pluralidad de los varios estados del sistema.
- 20 16.- Sistema de seguridad de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque el control de seguridad presenta una formación estructurada jerárquicamente, en el que en la unidad de memoria de diagnóstico del sistema está depositada una magnitud de la estructura de control, que representa la formación estructurada jerárquicamente del control de seguridad, en el que la unidad de mensajes de diagnóstico está configurada para preparar el número de mensajes de diagnóstico en función de la magnitud de la estructura de control.
- 25 17.- Procedimiento para el control de una instalación automática (10) con una pluralidad de componentes de hardware de la instalación (12, 14, 16), que comprenden una pluralidad de sensores y actuadores, con las etapas:
- 30 - establecer en función de una pluralidad de señales de entrada de diagnóstico del procesos, cuál de varios estados del proceso de la instalación a controlar está presente en un primer instante definido, y generar una pluralidad de señales de estado del proceso, en el que la pluralidad de señales de estado del procesos representa una pluralidad de estados del proceso establecidos, en el que la pluralidad de estados del proceso establecidos están presentes en un primer instante definido,
- 35 - establecer en función de una pluralidad de señales de entrada de diagnóstico del sistema, cuál de varios estados del sistema del control de seguridad está presente en un segundo instante definido, y
- 40 - generar una pluralidad de señales de estado del sistema, en el que la pluralidad de señales de estado del sistema representa una pluralidad de estados del sistema establecidos, en el que la pluralidad de estados del sistema establecidos están presentes en el segundo instante definido,
- 45 - alimentar la pluralidad de señales de estado del proceso y la pluralidad de señale de estado del sistema a una unidad de mensajes de diagnóstico (340),
- 50 - preparar una pluralidad de mensajes de diagnóstico para la pluralidad de estados del proceso establecidos y para la pluralidad de estados del sistema establecidos, y generar una pluralidad de señales de diagnóstico en la unidad de mensajes de diagnóstico, en el que la pluralidad de señales de diagnóstico representan la pluralidad de mensajes de diagnóstico,
- alimentar la pluralidad de señales de diagnóstico hacia una unidad de representación para la representación de la pluralidad de mensajes de diagnóstico,
- caracterizado** porque la unidad de mensajes de diagnóstico presenta una unidad de memoria de asociación (350), en la que al menos para una pluralidad de los varios estados del proceso y al menos para una pluralidad de los varios estados del sistema están depositadas una pluralidad de magnitudes de asociación, en el que las magnitudes de asociación establecidas representan cuál de los varios estados del sistema está asociado, respectivamente, a cuál de los varios estados del proceso en virtud de una asociación predefinida, en el que la unidad de mensajes de diagnóstico está configurada para seleccionar para una pluralidad de parejas de los estados del sistema establecidos y de los estados del proceso establecidos, una pluralidad de magnitudes de asociación depositadas, en el que cada una de estas magnitudes de asociación seleccionadas representa al menos una de las parejas, en el que la unidad de mensajes de diagnóstico está configurada para calcular una pluralidad de estados del sistema asociados en función de las magnitudes de asociación, en el que al menos para uno de los estados del proceso establecidos se

prepara un mensaje de diagnosis en función de este estado del proceso y de la pluralidad de estados del sistema asociados, que están asociados a este estado del proceso.

- 5 18.- Programa de ordenador con un soporte de datos con código de programa, que está configurado para realizar un procedimiento de acuerdo con la reivindicación 17, cuando el código del programa se ejecuta en un control de seguridad de acuerdo con una de las reivindicaciones 1 a 16.

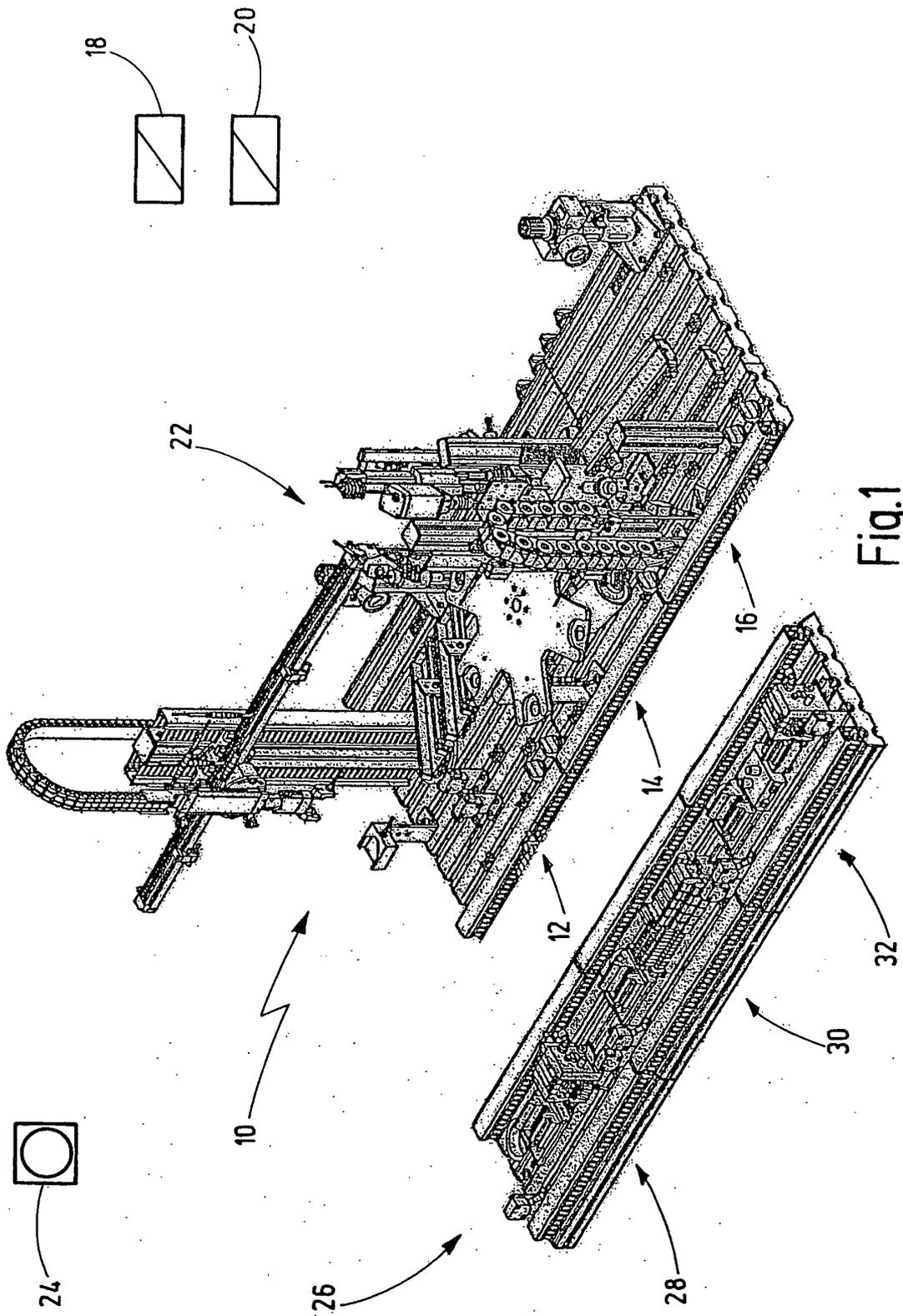


Fig.1

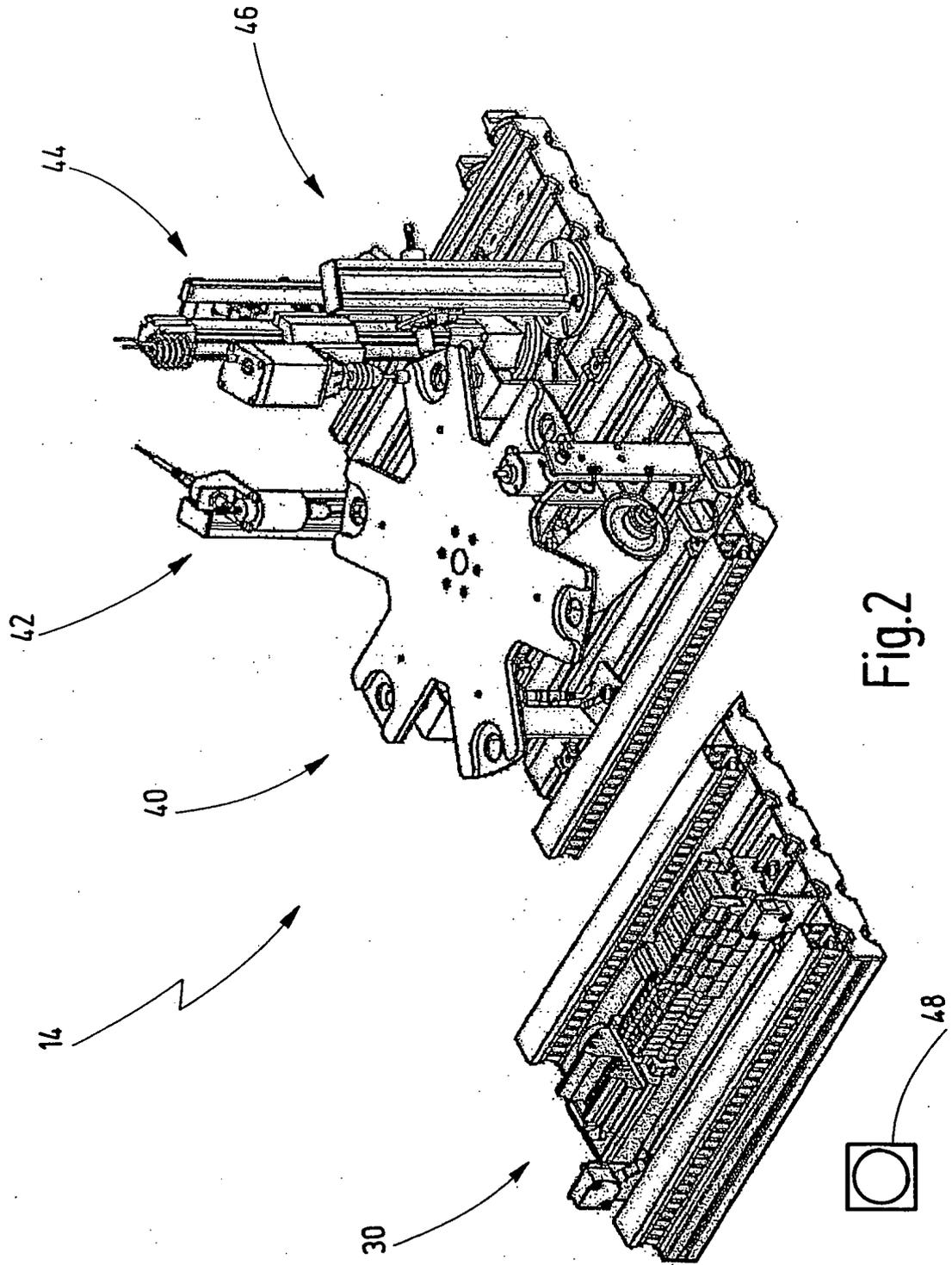


Fig. 2

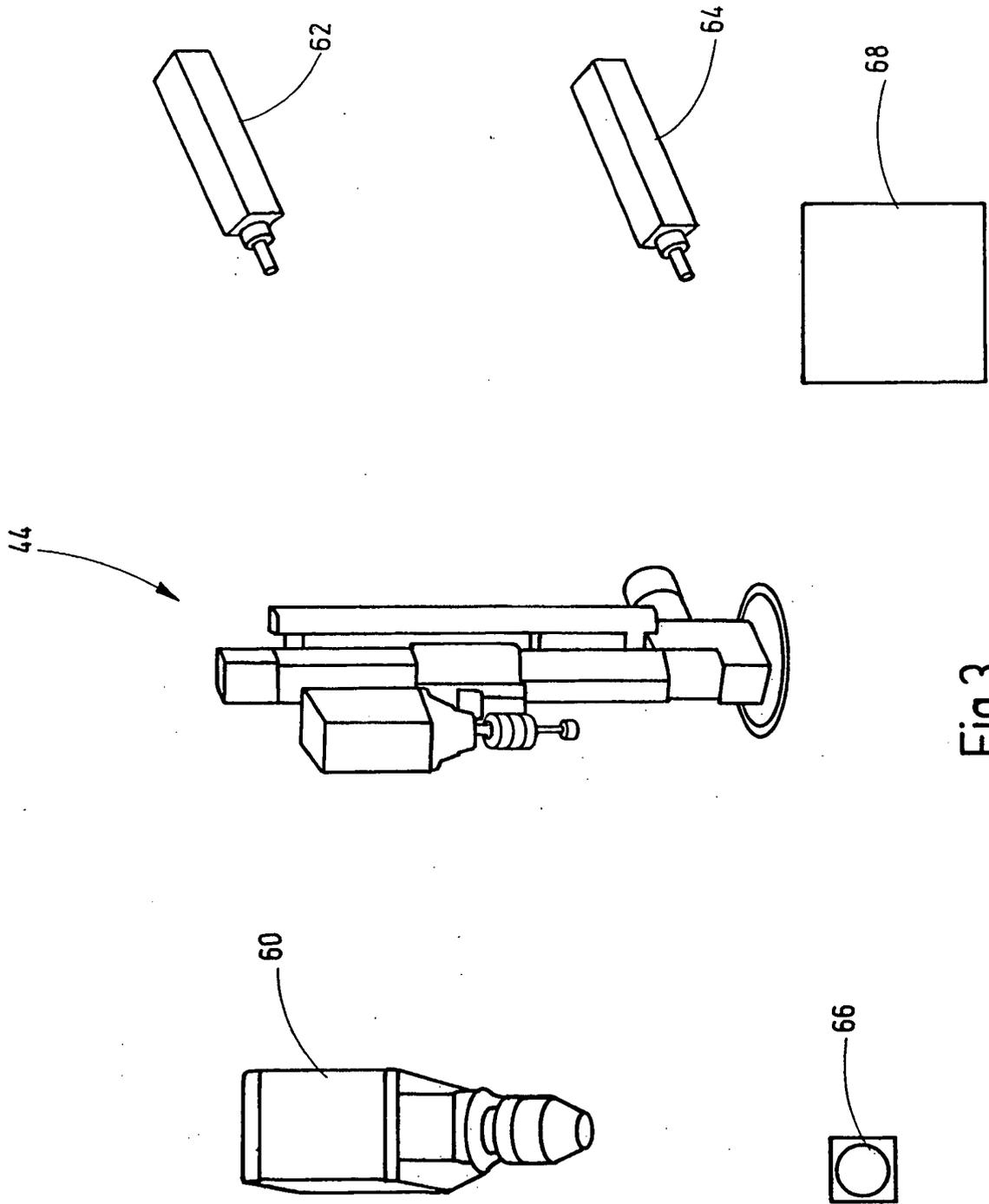


Fig.3

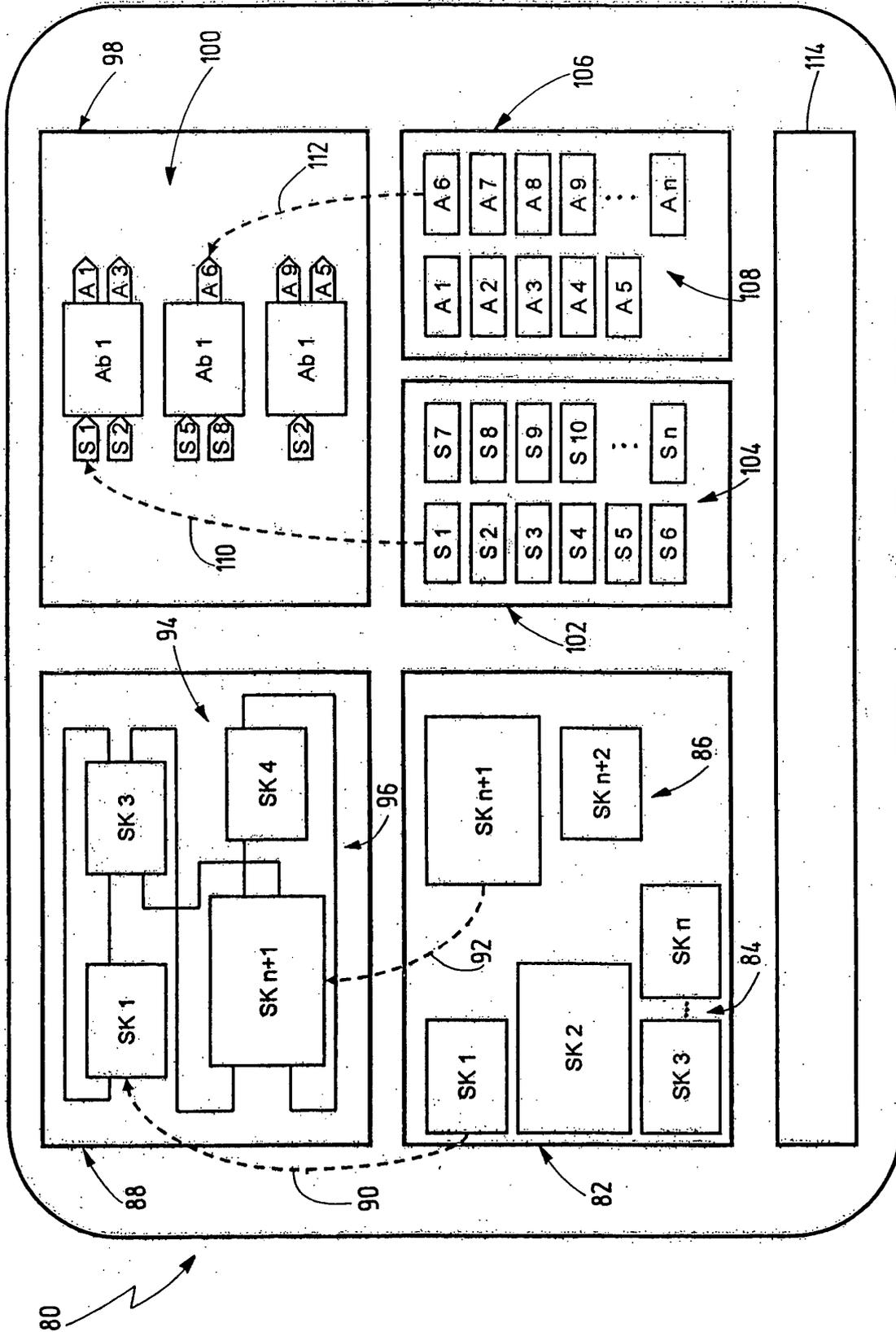


FIG. 4

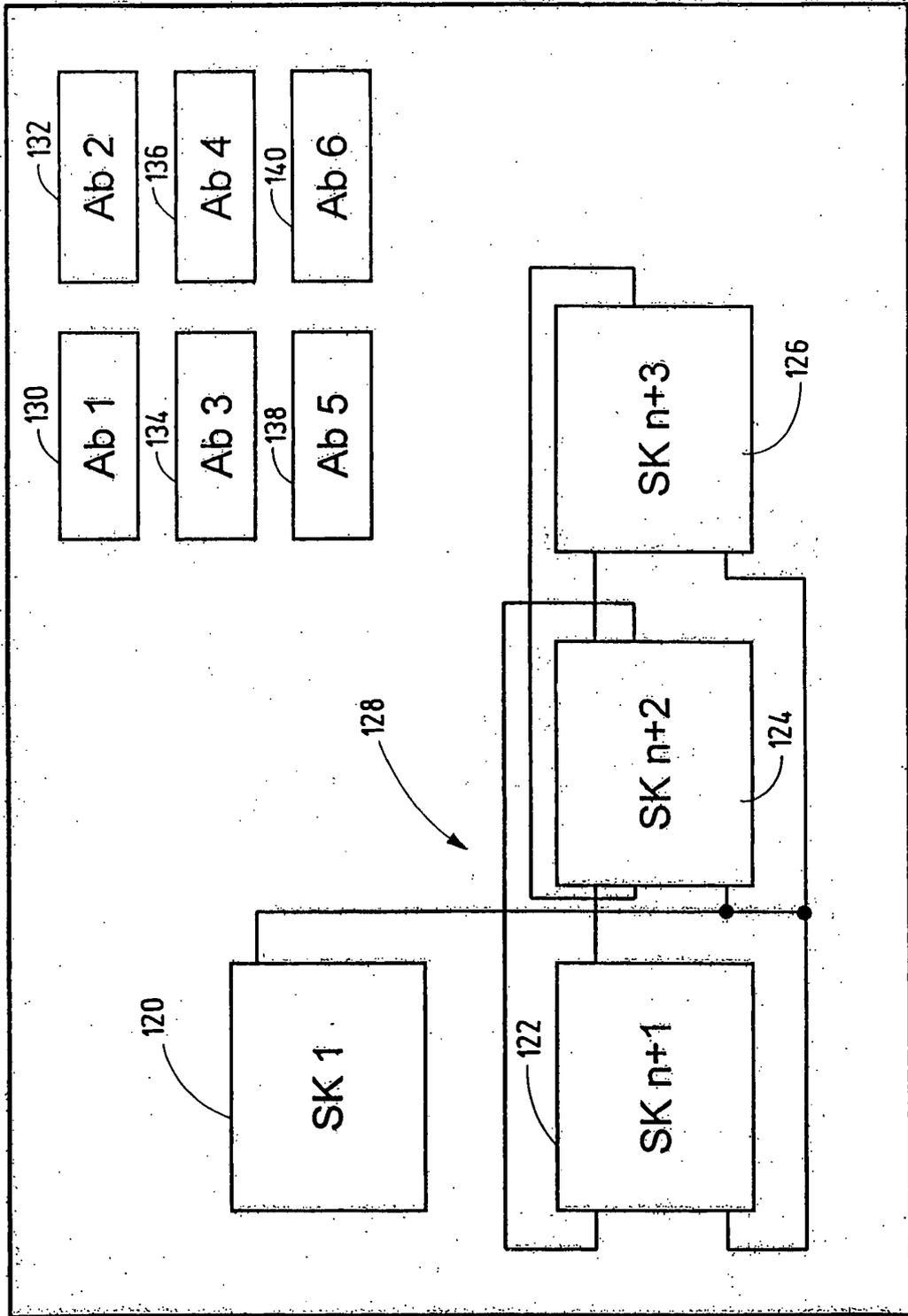


Fig.5

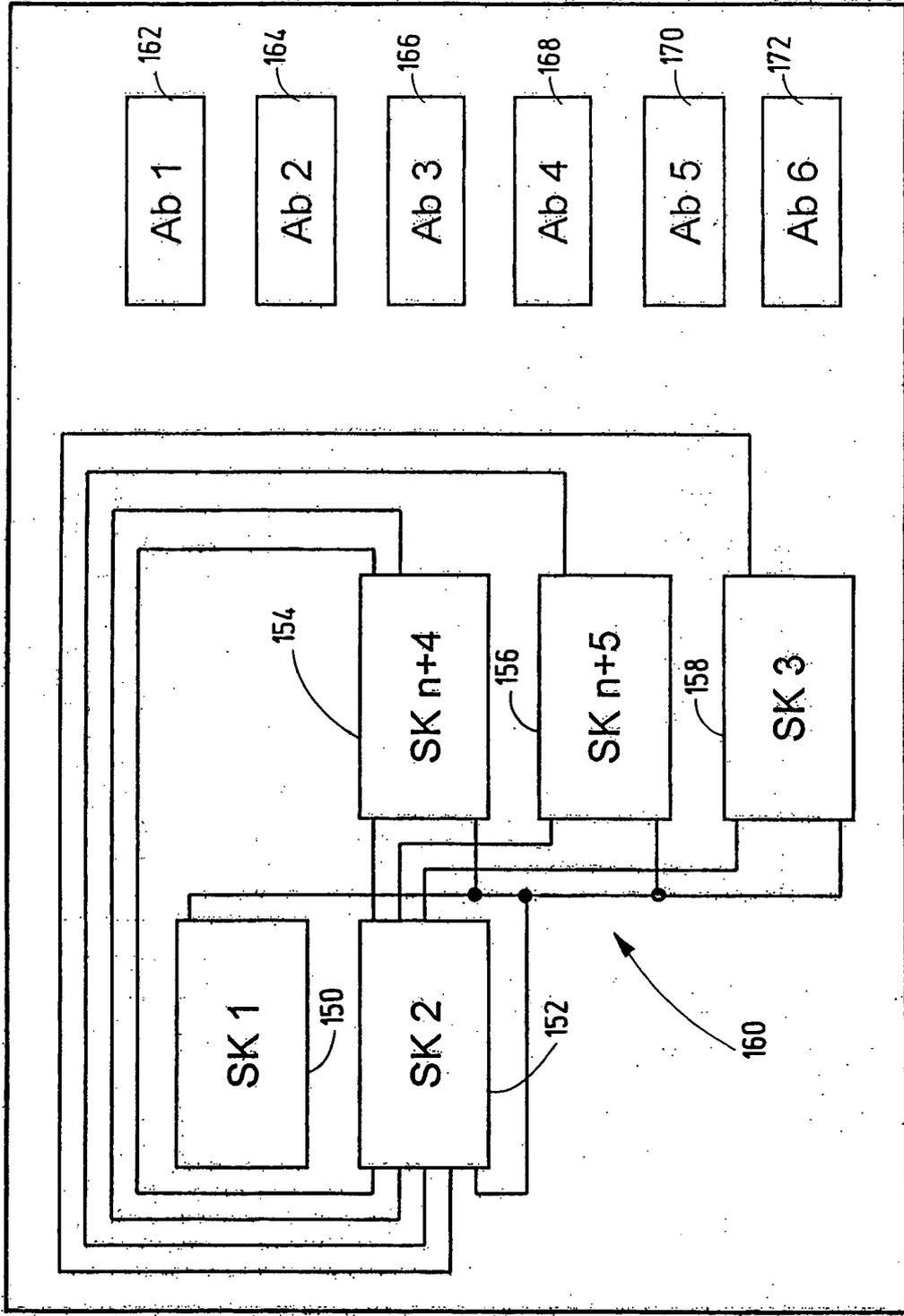


Fig.6

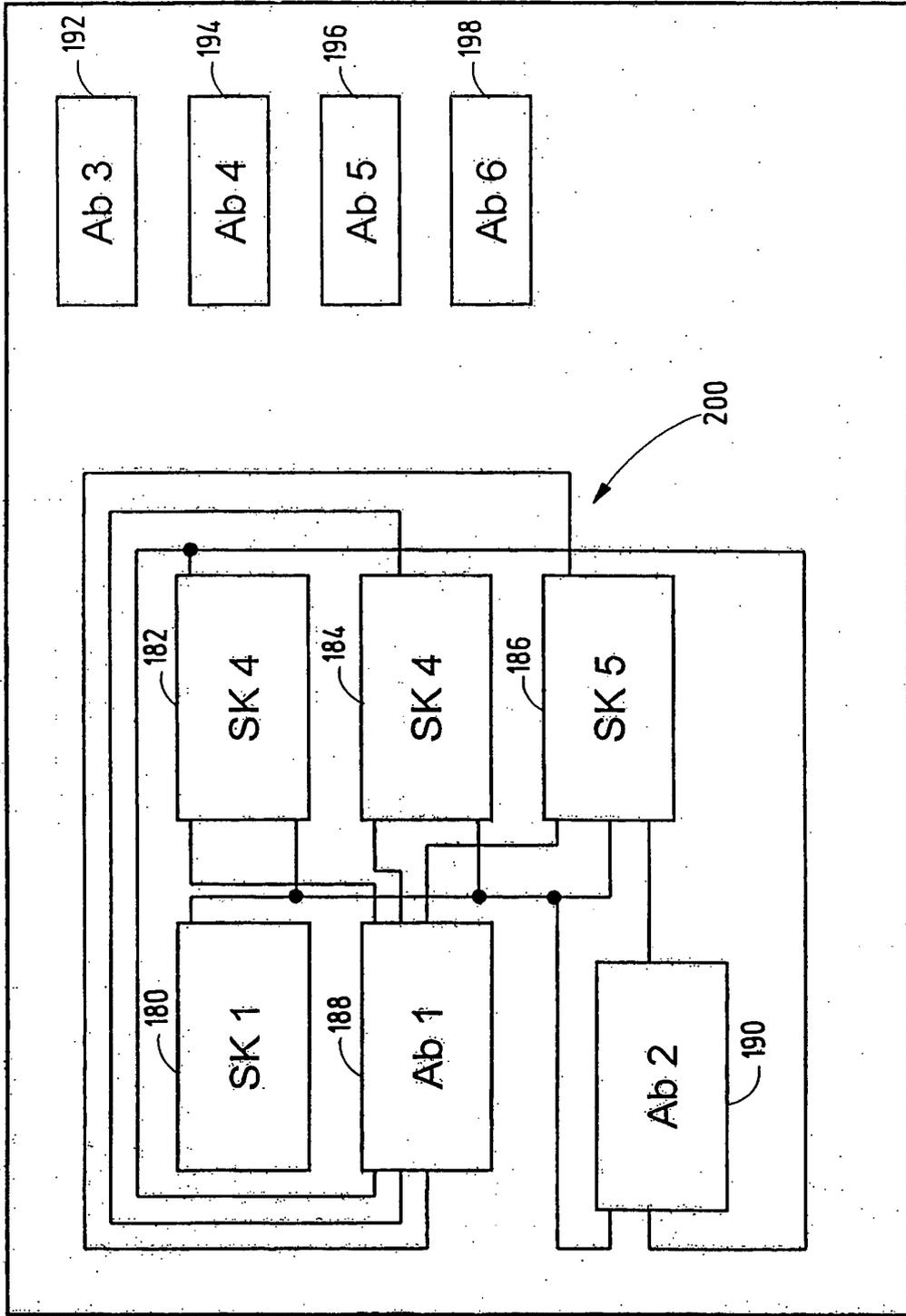


Fig.7

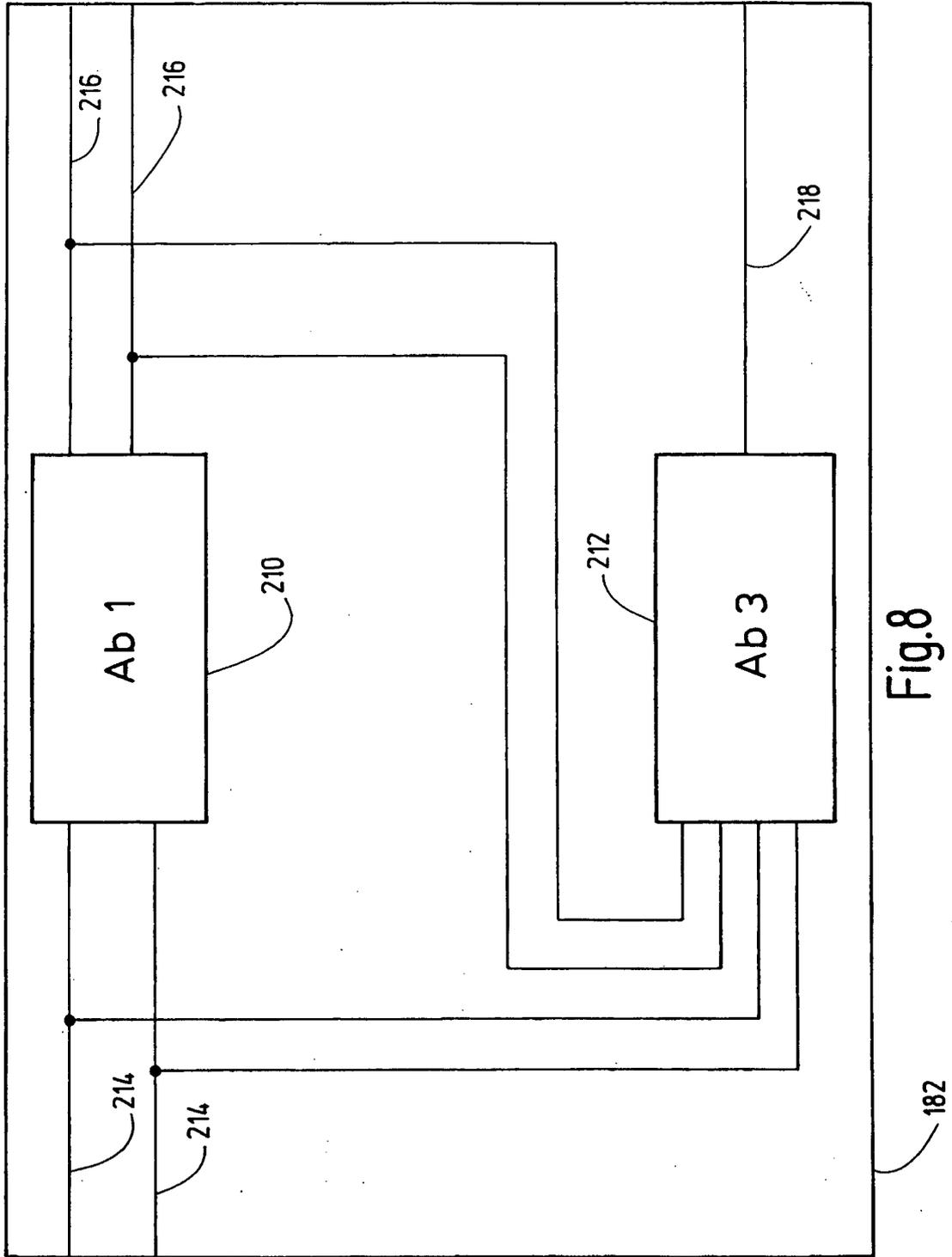


Fig.8

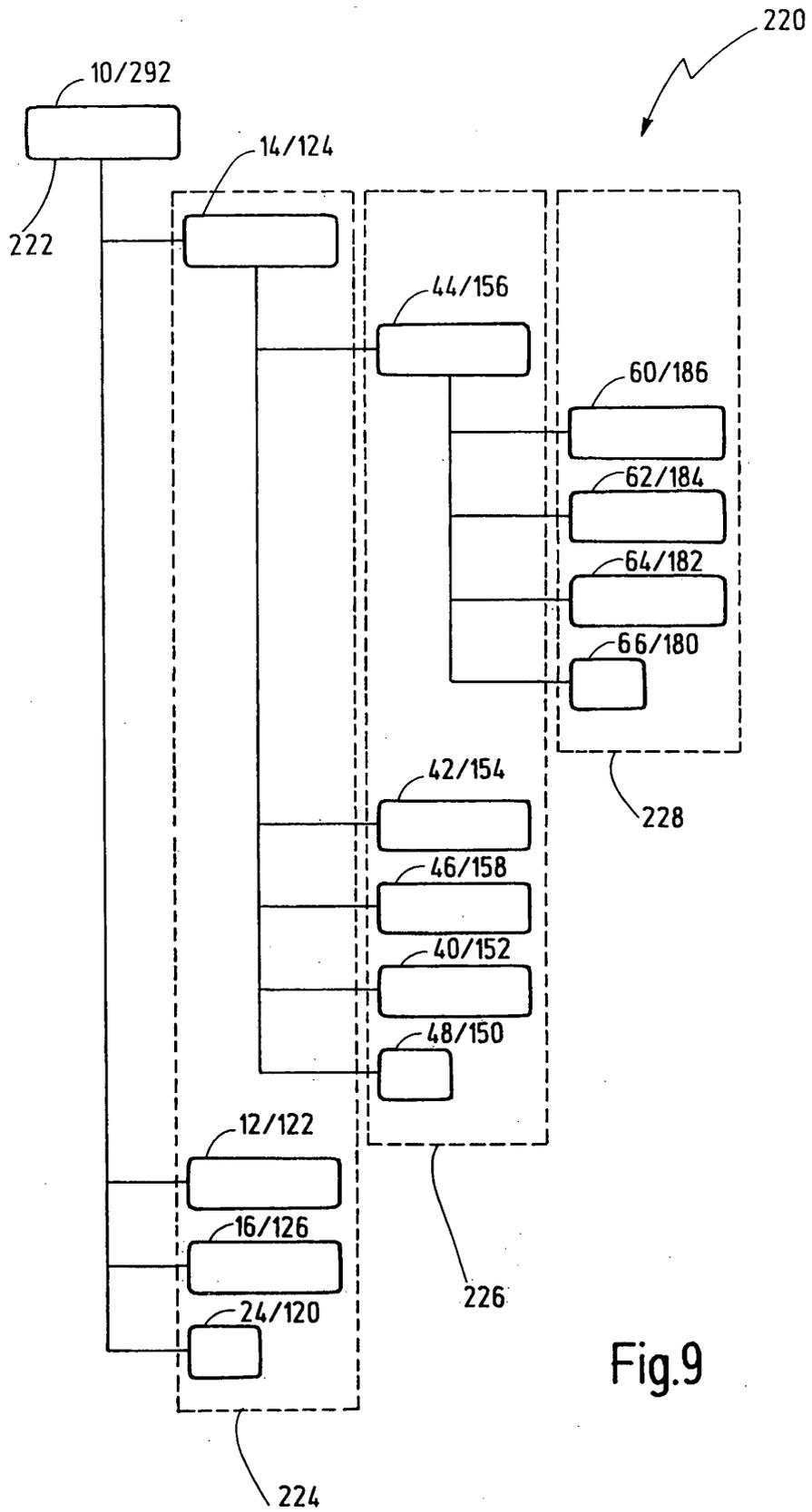


Fig.9

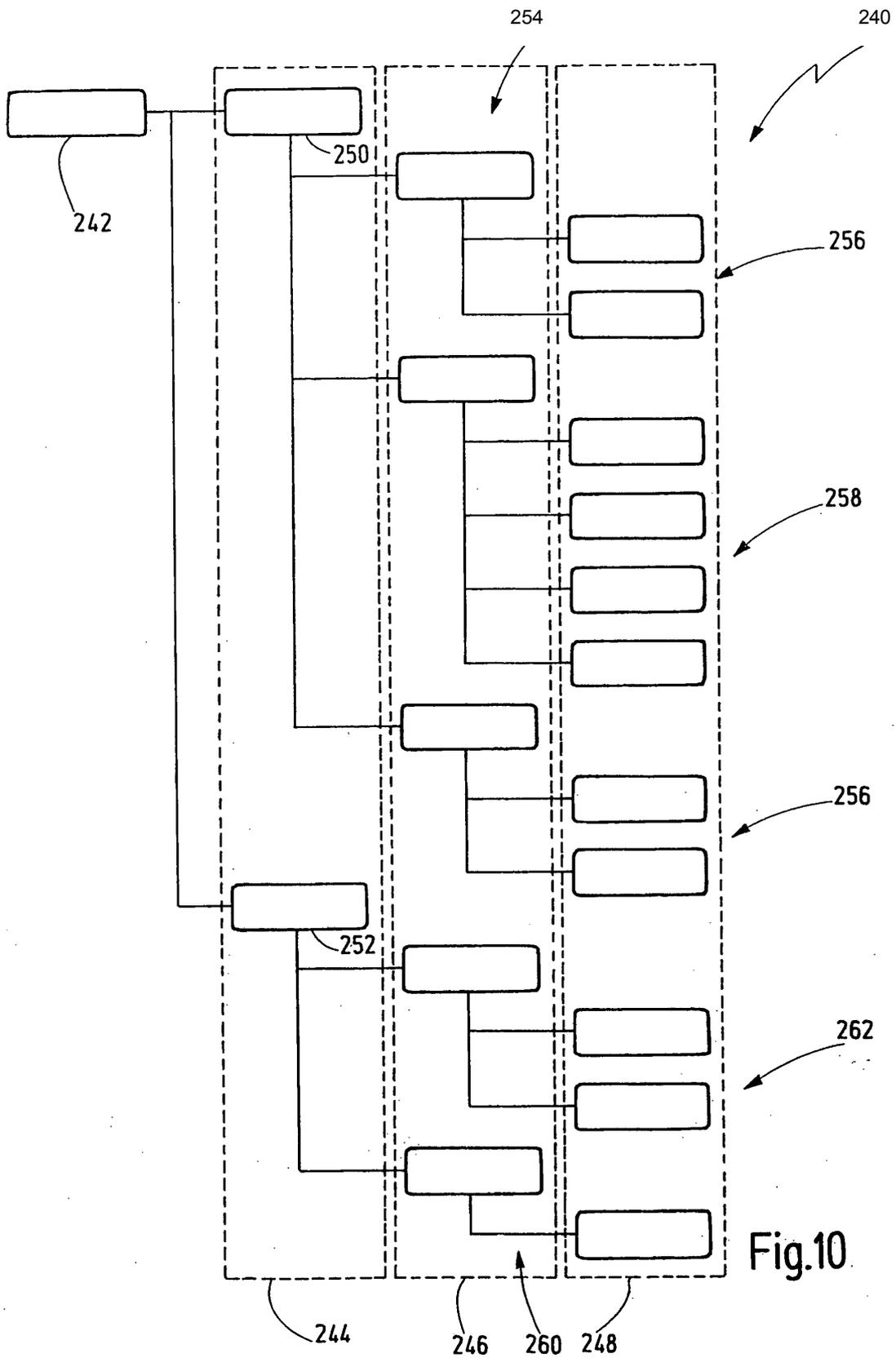


Fig.10

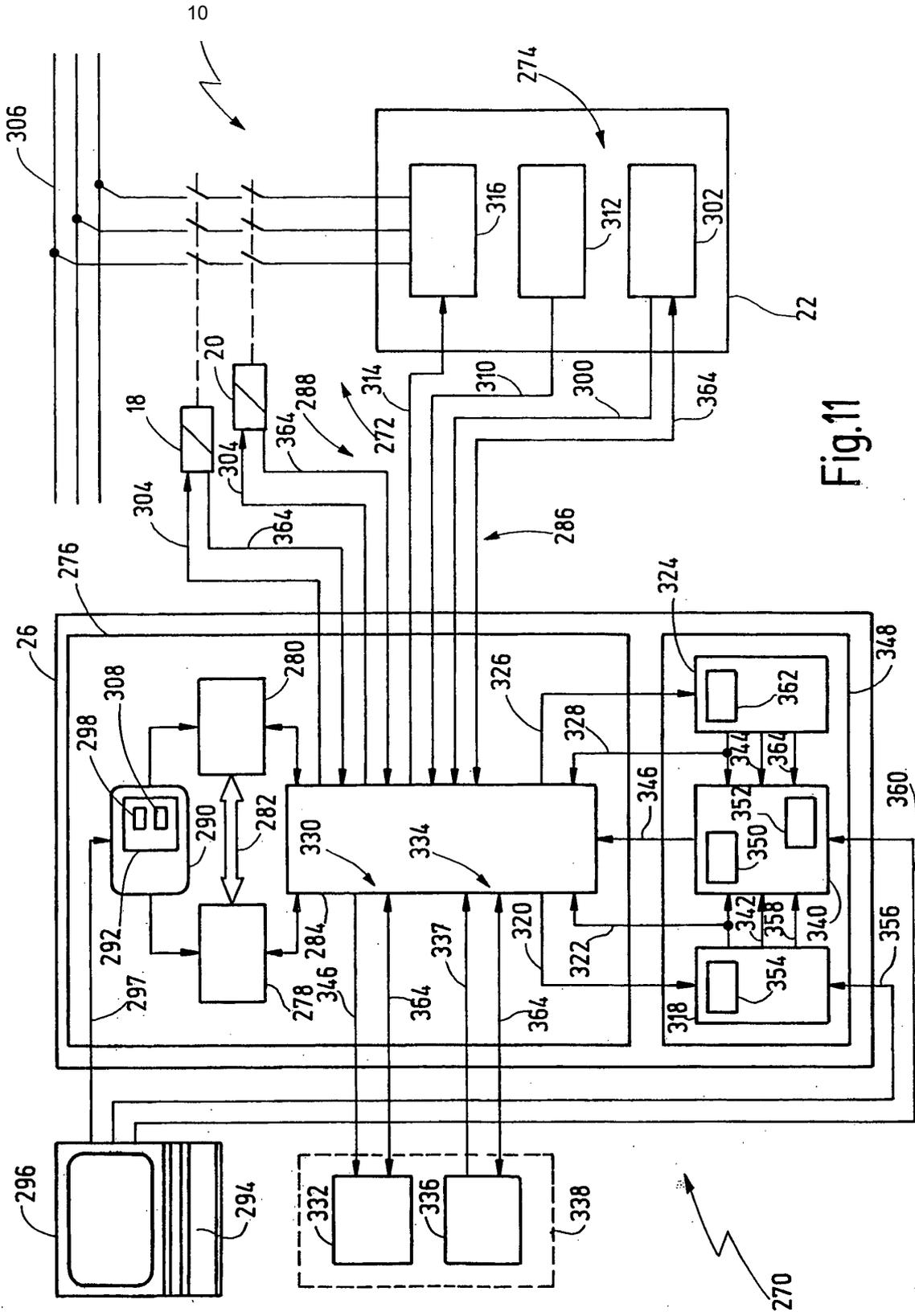


Fig.11