(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 629 499**

(51) Int. CI.:

G21D 3/00 (2006.01)
G05B 23/02 (2006.01)
G06F 21/56 (2013.01)
G06F 21/57 (2013.01)
G05B 19/05 (2006.01)
G06F 21/55 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **30.01.2014 PCT/EP2014/051837**

(87) Fecha y número de publicación internacional: **14.08.2014 WO14122063**

(96) Fecha de presentación y número de la solicitud europea: **30.01.2014 E 14705055 (3)**

(97) Fecha y número de publicación de la concesión europea: **29.03.2017 EP 2954534**

(54) Título: **Dispositivo y procedimiento para detectar manipulaciones no autorizadas del estado del sistema de una unidad de control y regulación de una instalación nuclear**

(30) Prioridad:

06.02.2013 DE 102013201937

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.08.2017

(73) Titular/es:

AREVA GMBH (100.0%)
Paul-Gossen-Strasse 100
91052 Erlangen, DE

(72) Inventor/es:

HALBIG, SIEGFRIED

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Dispositivo y procedimiento para detectar manipulaciones no autorizadas del estado del sistema de una unidad de control y regulación de una instalación nuclear

La invención se refiere a un dispositivo y a un procedimiento para detectar manipulaciones no autorizadas del estado del sistema de una unidad de control y regulación, en especial de un control programable por memoria de una instalación nuclear. Se refiere asimismo a un control programable por memoria, a una instalación de monitorización digital para una instalación nuclear y a una instalación nuclear correspondiente.

En las instalaciones nuclearse, como por ejemplo instalaciones para producir energía (centrales nucleares) se desarrollan en paralelo muchos procesos cooperativos, que comprenden habitualmente procesos de control y regulación. Para los procesos respectivos se usan con ello para la aplicación unas unidades de control y regulación optimizadas y configuradas.

Mediante la creciente integración técnica en red de los datos también de instalaciones nucleares, en especial de instalaciones para producir energía, y su conexión a redes externas hasta llegar a la Internet, estas instalaciones se vuelven propensas a los ataques con ayuda de virus u otras sustancias nocivas. Un caso conocido, en el que una instalación de este tipo fue atacada por un virus de software, fue STUXNET. Un ataque de este tipo puede conducir a pérdida de producción hasta llegar a una parada completa de las instalaciones, y causar unos daños personales y económicos elevados. Además de esto un software maligno infiltrado clandestinamente de este tipo puede emplearse para espionaje industrial. Asimismo existe el riesgo, en el caso de un primer ataque mediante un virus, de que se propague el virus, de tal manera que el mismo pueda atacar otros dispositivos de control de la misma instalación nuclear o también dispositivos de control de instalaciones integradas en red con ella. A causa de estos riesgos el uso de sistemas de control, cuya configuración de memoria puede modificarse en principio durante su evolución a causa de un software maligno, puede representar en entornos integrados en red un elevado riesgo para la seguridad. Los sistemas de control de este tipo son controles programables por memoria (SPS).

El documento WO 2009/128905 A1 da a conocer un dispositivo para detectar manipulaciones no autorizadas del estado del sistema de una unidad de control y regulación de una instalación nuclear y contiene la monitorización de controles programables por memoria.

Por ello la invención se ha impuesto la tarea de proporcionar un dispositivo con el que puedan detectarse de forma fiable las manipulaciones no autorizadas. Asimismo con una instalación de monitorización de este tipo se pretende proporcionar un control programable por memoria y una instalación de monitorización digital, así como una instalación nuclear.

Esta tarea es resuelta conforme a la invención mediante un dispositivo según la reivindicación 1.

Unas configuraciones ventajosas de la invención son objeto de las reivindicaciones dependientes. La invención se basa en la idea de que los ataques mediante virus o un software maligno similar tienen éxito si pueden influir en el estado de sistema de sistemas de control y/o regulación, de tal manera que su funcionalidad se modifica, amplía o destruye deforma indeseada. Esto puede realizarse por medio de que se carguen o lleven a cabo un programa maligno y/o unos daños malignos en una memoria en la que puede escribirse durante el funcionamiento. Por este motivo resulta ser problemático en primer lugar, emplear estos sistemas de control y/o regulación en las instalaciones críticas para la seguridad. En las instalaciones nucleares se exige el cumplimiento de los máximos estándares de seguridad, ya que las modificaciones de los sistemas de control puede conducir a espionaje, avería de componentes, malos funcionamientos y graves accidentes.

En el caso de un ataque de este tipo se intentaría, p.ej., infiltrar clandestinamente en la unidad de control y regulación un código de programa adicional, o sustituir un código de programa existentes por un código infiltrado. Asimismo podría intentarse modificar una configuración de tal manera que los datos de los sensores ya no puedan recibirse y/o los actuadores ya no puedan recibir respuesta o activarse.

Como se ha descubierto ahora, los elevados estándares de seguridad exigidos pueden cumplirse por medio de que se monitoricen y se comuniquen las modificaciones de los procesos internos del sistema de una unidad de control y regulación usada en una instalación de este tipo, en otras palabras, es decir el estado operacional y/o el estado de ampliación del hardware y/o el estado del programa.

Mediante la generación de un mensaje puede analizarse directamente de qué tipo es la modificación y si, dado el caso, se ha producido sin autorización. Además de esto se hace posible reaccionar directamente a esta modificación. En el marco de la solicitud recibe el nombre de unidad de control y regulación cada unidad electrónica que sólo puede llevar a cabo procesos de control o regulación, o bien ambas clases de procesos.

La unidad de control y regulación presenta de forma preferida al menos una memoria en la que puede escribirse con unos datos archivados en la misma, en donde el módulo de monitorización genera un mensaje si se producen modificaciones en los datos archivados en la memoria. El estado operacional, el estado de ampliación del hardware y el estado del programa de una unidad de control y regulación con una memoria en la que puede escribirse como

una memoria programable por memoria se determinan fundamentalmente mediante su contenido de memoria. El contenido de memoria comprende con ello habitualmente el código de programa, la configuración en cuanto a hardware y software y los campos de datos aplicados dinámicamente, variables, etc. Un ataque enemigo desde el exterior mediante software maligno se hará notar en las modificaciones de la memoria, de tal manera que las modificaciones del contenido de memoria pueden indicar unas manipulaciones no autorizadas.

Los datos comprenden de forma ventajosa el código de programa o magnitudes de programa generadas a partir del mismo. El código de programa, en especial un programa de usuario cargable, se ejecuta durante el funcionamiento mientras dura su evolución y contiene las indicaciones que se llevan a cabo. Para detectar tales manipulaciones no es sin embargo imprescindible que se monitoricen directamente las modificaciones del código. Aquí es más efectivo y económico que se monitoricen modificaciones de magnitudes de programa derivadas del mismo o generadas con ayuda del código de programa (código de usuario, firmware, sistema operativo, etc.), es decir en cierto modo secundarias, siempre que en caso de modificaciones del código se produzcan también con una probabilidad suficientemente grande modificaciones de estas magnitudes. Este es por ejemplo el caso también con las sumas de comprobación o longitudes generadas a partir del código, respectivamente de segmentos de código o componentes de código. La CPU presenta con ello ventajosamente la “disyunción o exclusivo sobre las sumas de comprobación de los elementos de software o módulos” como funcionalidad interna. Los resultados (por ejemplo valores de 32 bits) son leídos después por el módulo de monitorización y se monitorizan sus modificaciones. Los controles programables por memoria como el SIMATIC S7-300 y el SIMATIC S7-400 generan por sí mismos automáticamente sumas de comprobación, en especial sumas transversales. Estas sólo tienen que ser leídas por el módulo de monitorización y monitorizarse sus modificaciones. Mediante una comparación de valores antiguos/nuevos puede detectarse de este modo cada modificación de programa.

Los datos comprenden ventajosamente los datos del sistema, en especial la configuración del hardware y/o magnitudes de sistema generadas a partir de los mismos. La configuración del hardware comprende con ello en sistemas modulares datos sobre los grupos constructivos usados. La planificación de la configuración de hardware se realiza, por ejemplo en el SIMATIC, a través de HWKonfig contenida en el software de programación STEP7/PCS7. Cada grupo constructivo, que se pretende insertar en un S7-300 o S7-400 modular, para poder funcionar tiene que parametrizarse en el HWKonfig y a continuación cargarse en la CPU de la estación de destino. En el HWKonfig se parametrizan todos los ajustes como dirección de grupo constructivo, ajustes de diagnóstico, ajustes de márgenes de medición, etc. del respectivo grupo constructivo. De este modo puede prescindirse de ajustes a través de p.ej. interruptores puente. En el caso de una sustitución de grupo constructivo ya no hace falta ningún ajuste adicional.

La citada planificación se archiva en los llamados datos de sistema. Una comprobación de las modificaciones de estos datos de sistema hace posible la detección de posibles ataques. Como se ha descrito anteriormente, la unidad de control y regulación proporciona también disyunciones o exclusivo a través de las sumas de comprobación, éstas son leídas por el módulo de monitorización y se monitorizan sus modificaciones mediante una comparación de valores antiguos/nuevos.

En una forma de realización preferida el módulo de monitorización monitoriza la posición de un conmutador de clases de funcionamiento de la CPU de la unidad de control y regulación. Un conmutador de clases de funcionamiento de este tipo puede presentar varios ajustes. Estos pueden ser por ejemplo:

- MRES (reposición de la memoria de variables)
- STOP (no es posible tratar el programa, sólo comunicación)
- RUN (tratamiento de programa con posibilidad de modificación de programa bloqueada
- RUN-P (tratamiento de programa con posibilidad de modificación de programa).

En muchas CPUs actuales sin interruptor de llave sólo existen ya las posiciones de conmutador “START” y “STOP”, en donde en la posición “STOP” no es posible un tratamiento de programa, de tal manera que en este caso una valoración técnica del programa en la CPU no produce una modificación.

Pude estar previsto asimismo que el módulo de monitorización monitorice modificaciones de una etapa de seguridad de la unidad de control y regulación. La etapa de seguridad puede presentar por ejemplo als posiciones “sólo lectura” o “lectura y escritura”, combinadas respectivamente con protección por contraseña.

En el caso de que durante la monitorización se establezcan modificaciones del estado operacional, del estado de ampliación del hardware y/o del estado del programa, se genera un mensaje, lo que puede realizarse de diferente modo. Para que el mensaje esté disponible en un momento posterior para las valoraciones, se escribe de forma ventajosa en una memoria, en especial en un regulador de diagnóstico de la CPU de la unidad de control y regulación y/o en un regulador de monitorización del módulo de monitorización. Un regulador de diagnóstico puede estar realizado por ejemplo como una zona de memoria integrada en una CPU, que como regulador anular puede recibir registros de diagnóstico. Estos registros reciben de forma preferida un marcador cronológico de fecha / hora. El módulo de monitorización presenta de forma preferida una memoria de monitorización, en la que puede escribirse el mensaje, de forma preferida con un marcador cronológico para fecha y hora. Esta memoria de monitorización puede estar realizada por ejemplo como regulador anular. Un registro del mensaje sólo puede escribirse en una de

las dos memorias o para obtener redundancia en ambas memorias, siempre que se disponga de ellas.

Alternativamente a esto o de forma preferida adicionalmente a esto el mensaje se proporciona a una salida en especial binaria del dispositivo, en especial del módulo de monitorización. De este modo está disponible para que el planificador realice una distribución del mensaje específica de la instalación. Con ello están disponibles ventajosamente varias salidas, que están asociadas a las diferentes clases de modificación detectada (memoria de programa, memoria de datos de sistema, etapa de seguridad, etc.). De forma preferida está previsto un módulo de seguridad, el cual conmuta una etapa de seguridad de la unidad de control y regulación en caso necesario, en especial si se acciona un interruptor de llave. La etapa de seguridad presenta con ello en especial las posiciones “lectura y escritura” y “solo lectura” y “protección contra escritura y lectura”, en donde estas posiciones pueden estar enlazadas alternativamente a una legitimización de contraseña. Un interruptor de llave, a través del cual puede realizarse esta conmutación, está instalado después por ejemplo en al armario de distribución. De este modo puede garantizarse que sólo las personas autorizadas realizan modificaciones del programa. Sin la conmutación o el accionamiento del interruptor de llave las modificaciones de programa están después en cierta medida bloqueadas y de este modo descartadas. El interruptor de llave se cablea hasta una entrada digital cualquiera. En el programa de control se conmuta esta señal en un módulo (SecLev_2), el cual ajusta después a través de una función de sistema el nivel de seguridad.

Conforme a la invención, está previsto un módulo de control que monitoriza el funcionamiento del módulo de monitorización, en donde también el módulo de monitorización monitoriza el funcionamiento del módulo de control. La idea en la que se basa esta conformación es la siguiente. Para que un intruso pueda llevar a cabo una modificación de programa no reconocida en la unidad de control y regulación, debe obtener primero un acceso de escritura mediante el posicionamiento de la etapa de seguridad en “lectura y escritura”. Además de esto debe impedirla actividad del módulo de monitorización, es decir, en el caso de una realización del módulo de monitorización mediante un módulo de software o un elemento de software, debe impedir su tratamiento o el tratamiento de sus indicaciones de programa por parte de la CPU. Para detectar o recoger esto último está previsto el módulo de control.

El módulo de monitorización y el módulo de control monitorización monitorizan mutuamente su funcionamiento. Por lo tanto no se presenta aquí una simple monitorización redundante de la unidad de control y regulación. Conforme a la invención el módulo de monitorización y el módulo de control están diseñados como elementos de software, en donde ambos módulos monitorizan más bien mutuamente su procesamiento. Esto se realiza ventajosamente por medio de que se comprueba si durante un periodo de tiempo prefijado, p.ej. un segundo, se presenta un procesamiento correcto del módulo monitorizado respectivamente. Si no éste el caso se comunica la falta de procesamiento, lo que puede indicar el intento de una intrusión o una ya realizada. Un borrado de elementos de software desde fuera a causa de un ataque sólo es posible consecutivamente. Es decir el intruso, siempre que haya podido realmente tener conocimiento de la existencia de ambos módulos y sus funciones, tendrá que borrar o desactivar los mismos consecutivamente. En el caso de un borrado o una desactivación de uno de los dos módulos, esto lo detectará sin embargo el otro módulo respectivo y se generará un mensaje correspondiente, de tal manera que puede detectarse con fiabilidad una avería de uno de los dos módulos.

En el caso de que el módulo de control determine irregularidades en el funcionamiento del módulo de monitorización, indica a una salida binaria el funcionamiento defectuoso o el procesamiento defectuoso del módulo de monitorización. El módulo de monitorización muestra irregularidades del funcionamiento del módulo de control en al menos una de las vías descritas anteriormente: un mensaje se escribe en una memoria o un regulador de la CPU o módulo de monitorización, de forma preferida junto con un marcador cronológico de fecha/hora, respectivamente se pone a disposición en una salida (binaria) para una emisión de mensajes adicional específica de la instalación. De forma preferida se siguen las tres vías.

Con relación al control programable por memoria, la tarea citada anteriormente es resuelta conforme a la invención mediante un dispositivo descrito anteriormente e integrado mediante módulos de software. Es decir, los módulos antes citados (módulo de monitorización, módulo de control, módulo de seguridad) están realizados respectivamente como módulos de software o elementos de software y están situados en el estado operacional de la unidad de control y regulación en su memoria.

Con relación a la instalación de monitorización digital para una instalación nuclear, la tarea antes citada es resuelta conforme a la invención con un control programable por memoria representada anteriormente.

Con relación a la instalación nuclear, la tarea antes citada es resuelta conforme a la invención con una instalación de monitorización digital de este tipo.

Las ventajas de la invención consisten en especial en que mediante la monitorización del estado operacional, del estado de ampliación del hardware y del estado del programa de la unidad de control y regulación se impide en gran medida una manipulación detectada y puede comunicarse de forma fiable, de tal manera que puedan aplicarse unas medidas para evitar daños a la instalación directa y específicamente. El uso de controles programables por memoria es posible por primera vez de este modo en entornos integrados en red, críticos para la seguridad. Mediante la monitorización mutua del módulo de monitorización y del módulo de control se consigue que las manipulaciones no

sean posibles mediante la desconexión de la monitorización.

Se explica con más detalle un ejemplo de realización de la invención basado en un dibujo. En el mismo muestran en una exposición muy esquematizada:

la fig. 1 una instalación nuclear con una unidad de monitorización digital con una unidad de control y regulación con un dispositivo integrado con un módulo de monitorización, un módulo de seguridad y un módulo de control en una forma de realización preferida,

la fig. 2 un diagrama de desarrollo de la funcionalidad del módulo de seguridad del dispositivo conforme a la fig. 1,

la fig. 3 un diagrama de desarrollo de la funcionalidad del módulo de monitorización del dispositivo conforme a la fig. 1,

la fig. 4 un diagrama de desarrollo de la funcionalidad del módulo de control del dispositivo conforme a la fig. 1.

Las piezas iguales poseen en todas las figuras los mismos símbolos de referencia.

Una instalación nuclear 2 representada en la fig. 1 comprende una instalación de monitorización digital 4 con unidad de control y regulación 8, que está realizada como control programable por memoria (SPS) modular 10. Con ello puede tratarse por ejemplo de un SIMATIC S7-300 o S7-400 de la empresa Siemens. El mismo comprende una CPU 20 y una memoria 26, que comprende varias zonas de memoria. En una zona de memoria de programa 32 están archivados el o los programas, que se procesan durante el funcionamiento del SPS 10. Además de esto están archivadas sumas de comprobación del código y sus longitudes, en donde las mismas las calcula la CPU 20 para la transmisión de los programas a la CPU y, en el caso de existir modificaciones, se actualizan de inmediato. Del mismo modo se calculan a través de estas sumas de comprobación las disyunciones o exclusivo, se archivan en la memoria de datos de sistema 38 y se actualizan en el caso de existir modificaciones. También puede estar previsto que estas magnitudes derivadas del código de programa se archiven en una zona de memoria propia.

En la zona de memoria de datos de sistema 38 la CPU 20 archiva además datos de configuración, en especial los datos de configuración del hardware. Para que en un SPS 10 con estructura modular, como en el caso presente, un grupo constructivo pueda ejecutarse, éste tiene que parametrizarse en la configuración de hardware y a continuación cargarse en la CPU 20. En la configuración de hardware se parametrizan todos los ajustes como dirección de grupo constructivo, ajustes de diagnóstico, ajustes de margen de medición, etc. del respectivo grupo constructivo. En el caso de una sustitución de grupo constructivo ya no es necesario realizar ningún ajuste adicional. La memoria 26 comprende además también otras zonas de memoria 40.

El SPS 10 está unido en el lado de entrada a unos grupos se sensores 44, que comprenden varios sensores, y en el lado de salida a unos grupos constructivos de actuadores 50, que por su parte comprenden varios actuadores. Una línea de datos 56 conduce desde fuera hasta la instalación nuclear y une, a través de una interfaz 62, el SPS 10 a una Red de Área Local (LAN) o incluso a la Internet. A causa de este enlace existe la posibilidad de que intrusos potenciales intenten infiltrar clandestinamente un virus o instalar otras clases de software maligno para, o bien obtener información sobre los datos archivados en la CPU 20 (espionaje industrial) o modificar, impedir o destruir la funcionalidad del SPS 10. Un ataque de este tipo que tenga éxito puede conducir a graves daños personales y también a daños económicos, si el SPS 10 con el control se ocupa de procesos críticos para la seguridad.

Para impedir estos daños y poder detectar de forma fiable y rápida ataques y con ello manipulaciones no autorizadas del estado operacional, del estado de ampliación del hardware y/o el estado del programa del SPS 10, está previsto conforme a la invención un dispositivo 70 que, en el caso presente, está integrado en el SPS 10. El dispositivo 70 comprende tres módulos 76, 82, 116, que se describen a continuación. Estos módulos están realizados como elementos de software y archivados en la zona de memoria de programa.

Un módulo de seguridad 76 tiene acceso a la etapa de seguridad de la CPU 20, representado mediante una flecha 78. Se ha diseñado para conmutar la etapa de seguridad entre “lectura y escritura”, “sólo lectura” y “protección contra escritura y lectura” o a la inversa. Esta funcionalidad está acoplada a un interruptor de llave 80, que está instalado en un armario de distribución (no representado). Es decir en una primera posición del interruptor de llave el módulo de seguridad 76 activa la etapa de seguridad “lectura y escritura” y, en una segunda posición del interruptor de llave el módulo de seguridad 76 activa la etapa de seguridad “sólo lectura” o alternativamente “protección contra escritura y lectura”. Durante el funcionamiento esta segunda posición es la posición normal, de tal manera que las personas no autorizadas no pueden llevar a cabo ninguna modificación de programa y ninguna otra modificación en la memoria 26. Solamente si el interruptor de llave está en la primera posición son posibles las modificaciones. El intruso tendría que obtener de este modo, o bien acceso al interruptor de llave, es decir conseguir acceder a la instalación, lo que puede impedirse en gran medida mediante las medidas de seguridad usuales. Dado el caso también podría, si el interruptor de llave está en la primera posición, borrar mediante la infiltración clandestina de software maligno o después también modificar, mediante técnica de programa, directamente la etapa de seguridad en la CPU.

Para detectar de forma fiable la infiltración de software maligno en cualquier forma o modificaciones no autorizadas

del estado operacional, del estado de ampliación del hardware y del estado del programa del SPS 10, está previsto un módulo de monitorización 82. Como se ha indicado mediante una flecha 90, el módulo de monitorización 82 monitoriza modificaciones en la zona de memoria de programa de la memoria 32. Esto se produce de la forma siguiente: la CPU 20 genera, a partir del código de programa archivado en la zona de memoria de programa 32, por cada elemento unas sumas de comprobación y unas longitudes de programa. Mediante disyunciones o exclusivo sobre estas sumas de comprobación y longitudes de programa individuales se forma una suma de comprobación total (número de 32 bits) y se archiva en la memoria de datos de sistema 38. Los resultados (la suma de comprobación total) de estas disyunciones se monitorizan por si se producen modificaciones. Para ello se realiza en intervalos de tiempo prefijados una comparación entre valores antiguos/nuevos.

Como se ha simbolizado mediante una flecha 90, el módulo de monitorización 82 monitoriza también la zona de memoria de sistema 38 por si se producen modificaciones. Esto se realiza de nuevo a través de la comprobación de modificaciones en las disyunciones o exclusivo, generadas y proporcionadas por la CPU 20, sobre las longitudes y sumas de comprobación de los datos de sistema. El módulo de monitorización 82 monitoriza además modificaciones de la etapa de seguridad de la CPU 20, que también está archivada en la memoria de datos de sistema.

En el caso de producirse modificaciones en los resultados monitorizados, el módulo de monitorización 82 genera unos mensajes de tres formas diferentes. Por un lado se escribe el mensaje en el regulador de diagnóstico 88 del SPS 10. El mismo es una zona de memoria integrada realizada en la CPU20 como regulador anular, que puede recoger hasta 500 registros de diagnóstico. Incluso después del “borrado inicial” (el borrado inicial es una función en la que se borra toda la memoria de la CPU con excepción del regulador de diagnóstico 88, es decir, una CPU borrada inicialmente (ya) no funciona) o de una avería simultánea de batería y red, todavía puede seguir leyéndose esta memoria. Al escribir el mensaje en el regulador de diagnóstico 88 se garantiza de este modo que el mensaje no se pierda, incluso tras caídas de corriente. El contenido de este regulador de diagnóstico puede leerse y visualizarse por un lado a través del software de programación STEP7/PCS7. Por otro lado determinados aparatos HNI/sistemas de software, como por ejemplo WinCC o PCS7 OS pueden visualizar estos registros de regulador de diagnóstico también en texto en claro con marcador cronológico de fecha/hora.

El módulo de monitorización 82 escribe un mensaje también en un regulador de monitorización 94 construido como regulador anular, realizado en el módulo de monitorización 82 y que en el caso presente puede recoger 50 registros. Cada registro se compone de un marcador cronológico de fecha/hora y un bit por cada modificación producida. El regulador de monitorización 94 puede leerse y valorarse mediante STEP7/PCS7.

El mensaje se proporciona y visualiza asimismo respectivamente a/en una salida binaria 100, 102, 104 en el módulo de monitorización y, de este modo, se pone a disposición para un tratamiento ulterior. Tras la emisión de la alarma, el usuario puede en caso necesario leer unas informaciones más profundas a través del regulador de diagnóstico o el regulador de monitorización. A cada una de las tres monitorizaciones descritas anteriormente (código de programa, datos de sistema, etapa de seguridad) está asociada respectivamente su propia salida binaria 100, 102, 104, de tal manera que la fijación de un bit es suficiente para enviar un mensaje. Mediante la respectiva fijación de un bit se envían los mensajes en el caso de modificaciones del código de programa a la salida binaria 100, los mensajes en el caso de modificaciones de los datos de sistema a la salida binaria 102 y los mensajes en el caso de modificaciones de la etapa de seguridad a la salida binaria 104.

Mediante el módulo de monitorización 82 descrito pueden detectarse intentos basándose en los mensajes generados, de llevar a cabo modificaciones en los datos de sistema y/o el código de programa, lo que por ejemplo pueden ser los efectos de un ataque viral con el que se limita la funcionalidad del SPS 10. La generación de los mensajes podría también impedirse por medio de que el intruso borre o desactive parcial o totalmente el módulo de monitorización 82, antes de que el módulo de monitorización 82 advierta la intrusión y pueda generar un mensaje. Para impedir este tipo de escenarios está previsto un módulo de control 116. Como se ha representado mediante una flecha doble 112, el módulo de monitorización 82 y el módulo de control se monitorizan mutuamente. Esto se realiza de forma visible de tal manera, que se monitoriza respectivamente el procesamiento de las indicaciones de programa. Para ello se comprueba respectivamente si en un intervalo de tiempo prefijado, aquí 1 segundo (habitualmente los programas con técnica de guiado se procesan en márgenes de tiempo de 10 a 100 milisegundos), se ha proseguido con el procesamiento de las indicaciones del código de programa. Si uno de los dos módulos 82, 106 detecta que en el otro módulo 82, 106 respectivo no se prosigue con el tratamiento, genera un mensaje correspondiente, de tal manera que puede reaccionarse ante un posible ataque.

El módulo de control 116 muestra el procesamiento defectuoso o nulo del módulo de monitorización 82 en una salida binaria 110. El procesamiento defectuoso o nulo del módulo de monitorización 82 se escribe, como se ha descrito antes con relación a las monitorizaciones de la memoria 26, respectivamente con un marcador cronológico de fecha/hora en el regulador de diagnóstico 88 y en el regulador de monitorización 94, y se pone a disposición en la salida binaria 110 para una emisión de mensaje adicional específica de la instalación.

Este mecanismo es extremadamente fiable, ya que un atacante tendría en realidad que obtener primero conocimiento desde el exterior de la presencia de dos módulos 82, 116 que se controlan o monitorizan mutuamente. Además de esto no le será posible borrar al mismo tiempo los dos módulos 82 y 116, de tal manera que al menos uno de los dos módulos 82 ó 116 genera un mensaje y de este modo puede detectarse el ataque. Sin embargo,

también sin un ataque pueden detectarse la avería o perturbaciones funcionales de uno de los dos módulos 82, 116.

En la fig. 2 se ha representado un diagrama de desarrollo de los pasos de procedimiento que se producen en el estado operacional del módulo de seguridad 76. El procedimiento implementado en el módulo de seguridad 76 en cuanto a software comienza en Inicio 120. En una decisión 126 se comprueba si el interruptor de llave 80 entrega una señal válida, que hace posible el acceso a escritura/lectura, y si al mismo tiempo el estatus de esta señal es válido o se trata de una simulación. Si se han cumplido todas estas condiciones, el procedimiento se deriva al bloque 132, en el que se conmuta el nivel de seguridad de la CPU 20 a acceso a escritura/lectura, lo que se corresponde con una etapa de seguridad 1.

En caso contrario el procedimiento se deriva a una decisión 134, en la que se comprueba si sin legitimización de contraseña debe impedirse un acceso a escritura y lectura. Si se produce esto, el procedimiento se deriva al bloque 136, en el que el nivel de seguridad o la etapa de seguridad de la CPU 20 se conmuta a acceso a escritura7lectura sin legitimización de contraseña. En el bloque 138 se conmuta el nivel de seguridad a protección contra escritura con legitimización de contraseña, si las dos decisiones anteriores 126, 134 han resultado ser negativas, lo que se corresponde con una etapa de seguridad 2. En el bloque 140 se lee y visualiza el nivel de seguridad actual. El procedimiento finaliza en Fin 142.

Un procedimiento implementado en cuanto a software en el módulo de monitorización 82 se ha representado en la fig. 3 mediante un diagrama de desarrollo y comienza en Inicio 150. En el bloqueo 152 se leen las sumas de comprobación, aquí sumas transversales, para la configuración de hardware HWKonfig y el código de programa así como el nivel de seguridad. En la decisión 154 se comprueba mediante una comparación de valores antiguos/nuevos, si el valor de la suma de comprobación del HWKonfig coincide con el valor de la última consulta. Si no es éste el caso, el procedimiento se deriva al bloque 145. Allí se registra o escribe el registro de mensaje “modificación de HWKonfig” en el regulador de monitorización 94 y en el regulador de diagnóstico 88, respectivamente con marcador cronológico de fecha/hora, y la salida binaria 102 se establece para el tratamiento ulterior específico de la instalación, es decir, al bit se asigna el valor que se corresponde con un mensaje (p.ej. 1 para mensaje, 0 para ningún mensaje). En el caso de que no se haya determinado ninguna modificación de la suma transversal mediante la comparación de valores antiguos/nuevos, en el bloque 158 se repone la salida 102, con lo que se garantiza que no se visualice un mensaje de forma errónea.

En una decisión 160 se comprueba si el valor de la suma transversal leída del código de programa ha variado respecto a su valor anterior procedente de la última consulta. Si ha sucedido esto el procedimiento se deriva al bloque 162. Allí se escribe un registro de mensaje “modificación de programa” en el regulador de monitorización 94 y en el regulador de diagnóstico 88, incluyendo un marcador cronológico de fecha/hora, y se establece la salida 100. En caso contrario se repone la salida 100 en el bloque 164.

En una decisión 166 se comprueba si la etapa de seguridad de la CPU 20 se ha modificado desde la última consulta. Si es éste el caso, se escribe en el bloque 168 un registro de mensaje “modificación de la etapa de seguridad” junto con un marcador cronológico en el regulador de monitorización 94 y en el regulador de diagnóstico 88. Asimismo se establece la salida 104. En caso contrario se repone esta salida en el bloque 170.

En una decisión 172 se comprueba si la recuperación de los pasos de procedimiento descritos es anterior a 1 segundo. Si es éste el caso en el bloque se emite un error de parámetro (los tres módulos descritos 76, 82, 116 junto con otros módulos se ponen a disposición en una biblioteca para una aplicación. El usuario puede elegir/ajustar diferentes comportamientos mediante parametrización de los módulos durante la programación o durante la puesta en funcionamiento. Si el usuario parametriza/elige un comportamiento inadmisible recibe una visualización de error de parametrización y puede corregir su parametrización). En caso contrario el procedimiento se deriva al bloque 176, en el que se repone el error de parametrización.

La monitorización mutua del módulo de monitorización 82 y del módulo de control 116 se consigue en el presente ejemplo de realización por medio de que cada módulo presenta respectivamente un contador, en el él mismo suma y un contador, en el que suma respectivamente el otro módulo. Si ambos módulos 82 y 116 funcionan adecuadamente, los contadores tienen respectivamente los mismos valores. Si se avería un módulo, el contador en el que él mismo suma ya no suma en el otro módulo, de tal manera que puede detectarse la avería del módulo.

El procedimiento pasa a continuación a una decisión 178, en la que se compara el valor de un contador de monitorización en el que suma el módulo de monitorización 82 con el valor de un contador de control en el que suma el módulo de control 116. Si coinciden estos valores, en el bloque 180 se suma en el contador de monitorización. Si no coinciden los dos valores, en una decisión 182 se comprueba si la última suma de contador del contador de control es anterior a 1 s y todavía no se ha producido registro en el regulador de monitorización 94 y en el regulador de diagnóstico 88. Si es éste el caso, esto demuestra que el módulo de control 106 no funciona adecuadamente. Por ello se registra después en el bloque 184 un registro de mensaje “error de monitorización de borrado” o “error de módulo de control” en el regulador de monitorización 94 y en regulador de diagnóstico 88, respectivamente con marcador cronológico, y en una salida binaria 108, en la que se visualizan errores del módulo de control 116, se establece un bit. En caso contrario se comprueba en la decisión 188, si en el regulador de diagnóstico 88 de la CPU ya existe el registro “módulo de monitorización funciona de nuevo”, que se ha registrado en el bloque 184. Si es éste

el caso en el bloque 192 se repone la salida 108. En caso contrario se lleva a cabo en el bloque 192, en el regulador de monitorización 94 y en el regulador de diagnóstico con marcador cronológico, un registro de mensaje “módulo de control funciona ok” o “monitorización de borrado ok”.

Un procedimiento realizado conforme a software en el módulo de control 116 se ha representado como diagrama de desarrollo en la fig. 4 y comienza en Inicio 194. En una decisión 196 se comprueba si la conexión al módulo de monitorización 82 es adecuada o correcta. En el ejemplo de realización presente el usuario tiene precisamente que establecer, durante la planificación/programación, una conexión/línea en un editor CFC (Continuous Function Chart) haciendo clic con el ratón entre los dos módulos. Mediante esta conexión el módulo de control 16 puede leer y escribir en el módulo de datos de trámite del módulo de monitorización 82. El propio módulo de control no tiene su propia memoria de datos. Si no es éste el caso, en un bloque 198 se emite un error de parametrizacion. En caso contrario se comprueba en una decisión 200, si la última recuperación de esta función es anterior a 1 s. En caso negativo en el bloque 202 se emite un error de parametrización. En caso positivo el procedimiento pasa al bloque 204, en el que el error de parametrización se repone.

En el módulo de control 116 se suma en el contador de control si el contador, en el suma el módulo de monitorización 82, es mayor que el contador del módulo de control 116. En una decisión 206 se comparan entre sí el contador de monitorización y el contador de control. Si el contador de monitorización es mayor que el contador de control, el contador de control se aumenta en el bloque 208. Después de esto se comprueba en una decisión si se ha registrado en el regulador de diagnóstico 88 un registro “el módulo de monitorizacion trabaja de nuevo”. En caso negativo, esto se recupera en el bloque 212. En el bloque 214 se repone después la salida binaria correspondiente.

Si existe una coincidencia, en una decisión 216 se comprueba si el último aumento de contador del contador de monitorización es anterior a 1 s y todavía no se ha producido un registro en el regulador de diagnóstico 88. Si todavía no se producido ningún registro, en el bloque 218 se lleva a cabo un registro “módulo de monitorización ya no funciona” en el regulador de diagnóstico 88. En el bloque 220 se establece después la salida 110.

Si el último aumento de contador era anterior a 1 s y no existía ningún registro, el procedimiento se deriva desde la decisión 216 directamente al bloque 220. El procedimiento finaliza en Fin 222.

En los tres módulos la secuencia de los pasos de procedimiento puede discurrir también en otra secuencia o en paralelo, siempre que se garantice la funcionalidad ilustrada. La sucesión de los pasos de procedimiento ilustrados respectivamente entre Inicio y Fin se repite en intervalos de tiempo regulares. Respectivamente entre Inicio y Fin el módulo respectivo suma un uno en el contador actualizado por el mismo.

Lista de símbolos de referencia

2	Instalación nuclear
4	Instalación de monitorización digital
8	Unidad de control y regulación
10	Control programable por memoria
20	CPU
26	Memoria
32	Zona de memoria de programa
38	Zona de memoria de datos de sistema
40	Zonas de memoria adicionales
44	Grupos constructivos de sensores
50	Grupos constructivos de actuadores
56	Línea de datos
62	Interfaz
70	Dispositivo
76	Módulo de seguridad
78	Flecha

80	Interruptor de llave
82	Módulo de monitorización
84	Flecha
88	Regulador de diagnóstico
90	Flecha
92	Flecha
94	Regulador de diagnóstico de monitorización
100	Salida binaria
102	Salida binaria
104	Salida binaria
108	Salida binaria
110	Salida binaria
112	Flecha doble
116	Módulo de control
120	Inicio
126	Decisión
132	Bloque
134	Decisión
136	Bloque
138	Bloque
140	Bloque
142	Fin
150	Inicio
152	Bloque
154	Decisión
156	Bloque
158	Bloque
160	Decisión
162	Decisión
164	Bloque
166	Decisión
168	Bloque
170	Bloque
172	Decisión
174	Bloque
176	Bloque

178 Decisión

180 Bloque

182 Decisión

184 Bloque

186 Bloque

188 Decisión

188 Decisión

190 Bloque

192 Bloque

194 Inicio

196 Decisión

198 Bloque

200 Decisión

202 Bloque

204 Bloque

206 Decisión

208 Bloque

210 Decisión

212 Bloque

214 Bloque

216 Decisión

218 Bloque

220 Bloque

222 Fin

REIVINDICACIONES

1.- Dispositivo (70) para detectar manipulaciones no autorizadas del estado del sistema de una unidad de control y regulación (9), en donde

- está previsto un módulo de monitorización (82), el cual monitoriza el estado operacional y/o el estado de ampliación del hardware y/o el estado del programa de la unidad de control y regulación (8) y, en caso de existir modificaciones de este estado, genera un mensaje,
- está previsto un módulo de control (116), el cual monitoriza el funcionamiento del módulo de monitorización (82), y
- el módulo de monitorización (82) monitoriza el funcionamiento del módulo de control (116),

caracterizado porque la unidad de control y regulación (8) presenta un control (10) programable por memoria y el módulo de monitorización (82) y el módulo de control (116) son elementos de software del control programable por memoria (10), que comprueban mutuamente si el otro módulo respectivo procesa según lo previsto indicaciones de programa dentro de un intervalo de tiempo prefijado.

2.- Dispositivo (70) según la reivindicación 1, en donde la unidad de control y regulación (8) presenta al menos una memoria en la que puede escribirse (26) con unos datos archivados en la misma, y en donde el módulo de monitorización (82) genera un mensaje si se producen modificaciones en los datos archivados en la memoria (26).

3.- Dispositivo (70) según la reivindicación 2, en donde los datos comprenden el código de programa y/o las magnitudes de programa generadas a partir del mismo.

4.- Dispositivo (70) según las reivindicaciones 2 o 3, en donde los datos comprenden los datos de sistema, en especial la configuración de hardware y/o las magnitudes de sistema generadas a partir de los mismos.

5.- Dispositivo (70) según una de las reivindicaciones 1 a 4, en donde el módulo de monitorización (82) monitoriza la posición de un interruptor de clases de funcionamiento de la CPU de la unidad de control y regulación (8).

6.- Dispositivo (70) según una de las reivindicaciones 1 a 5, en donde el módulo de monitorización (82) monitoriza modificaciones de una etapa de seguridad de la unidad de control y regulación (8).

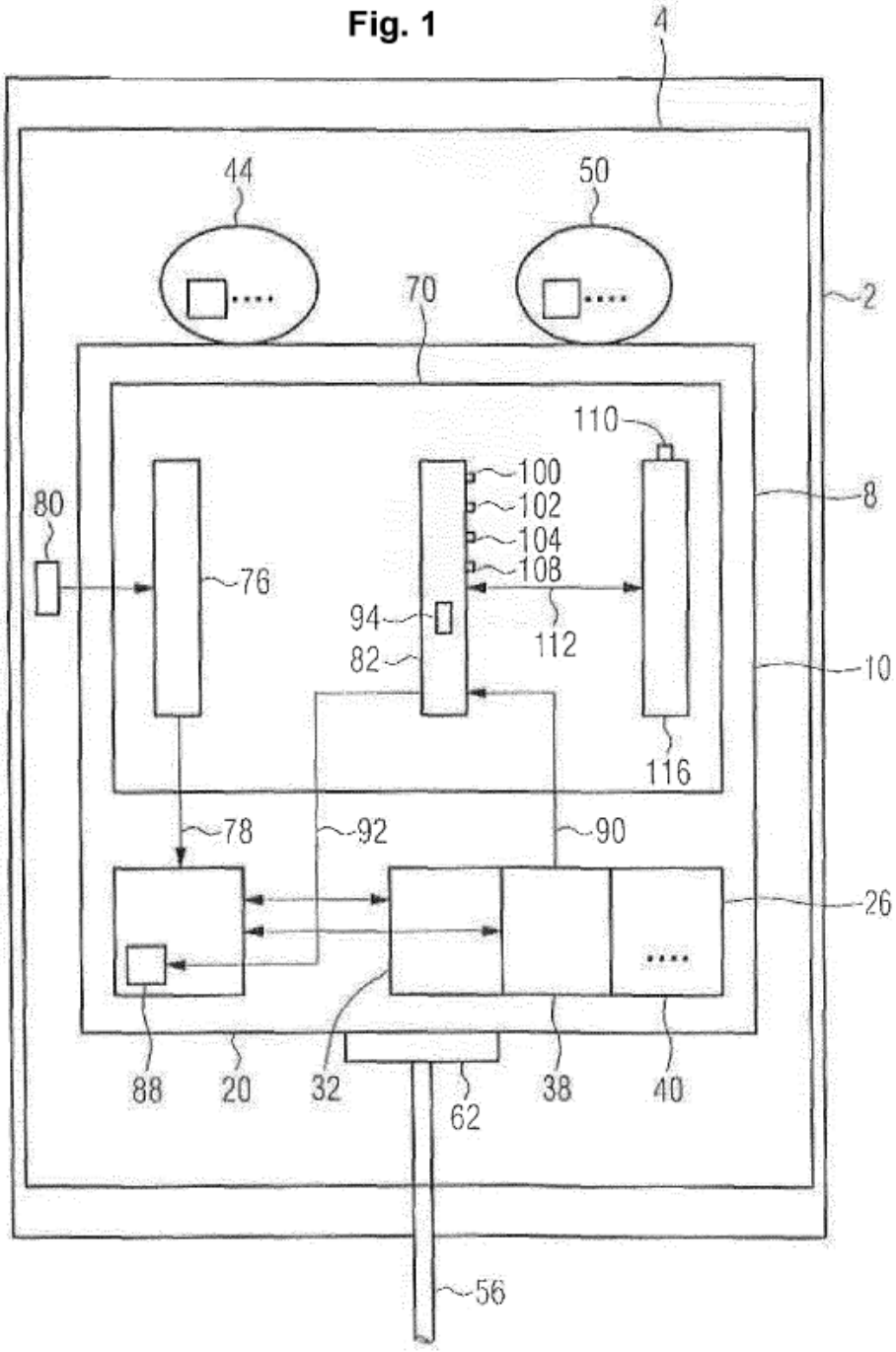
7.- Dispositivo (70) según una de las reivindicaciones 1 a 6, en donde el mensaje se escribe en una memoria, en especial en un regulador de diagnóstico (88) de la CPU de la unidad de control y regulación y/o en un regulador (94) del módulo de monitorización.

8.- Dispositivo (70) según una de las reivindicaciones 1 a 7, en donde el mensaje se proporciona a una salida (100, 102, 104, 108) del dispositivo (70), en especial del módulo de monitorización (82).

9.- Dispositivo (70) según una de las reivindicaciones 1 a 8, en donde está previsto un módulo de seguridad (76), el cual conmuta en caso necesario una etapa de seguridad de la unidad de control y regulación (8), en especial al accionar un interruptor de llave (80).

10. Instalación nuclear (2) con una instalación de monitorización digital según una de las reivindicaciones 1 a 9.

Fig. 1


4
44
50
70
2
110
80
100
102
104
108
8
76
94
82
112
10
116
78
92
90
26
88
20
32
62
38
40
56

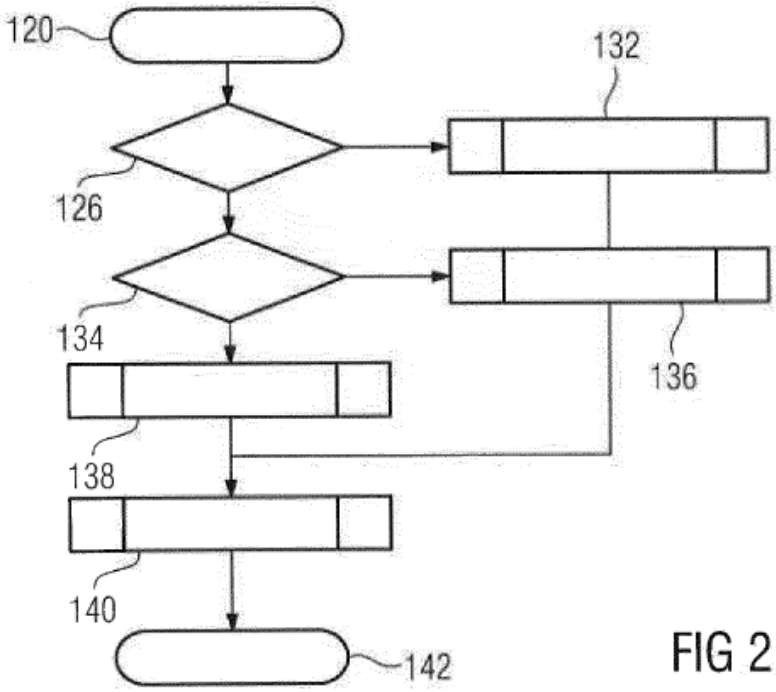


FIG 2

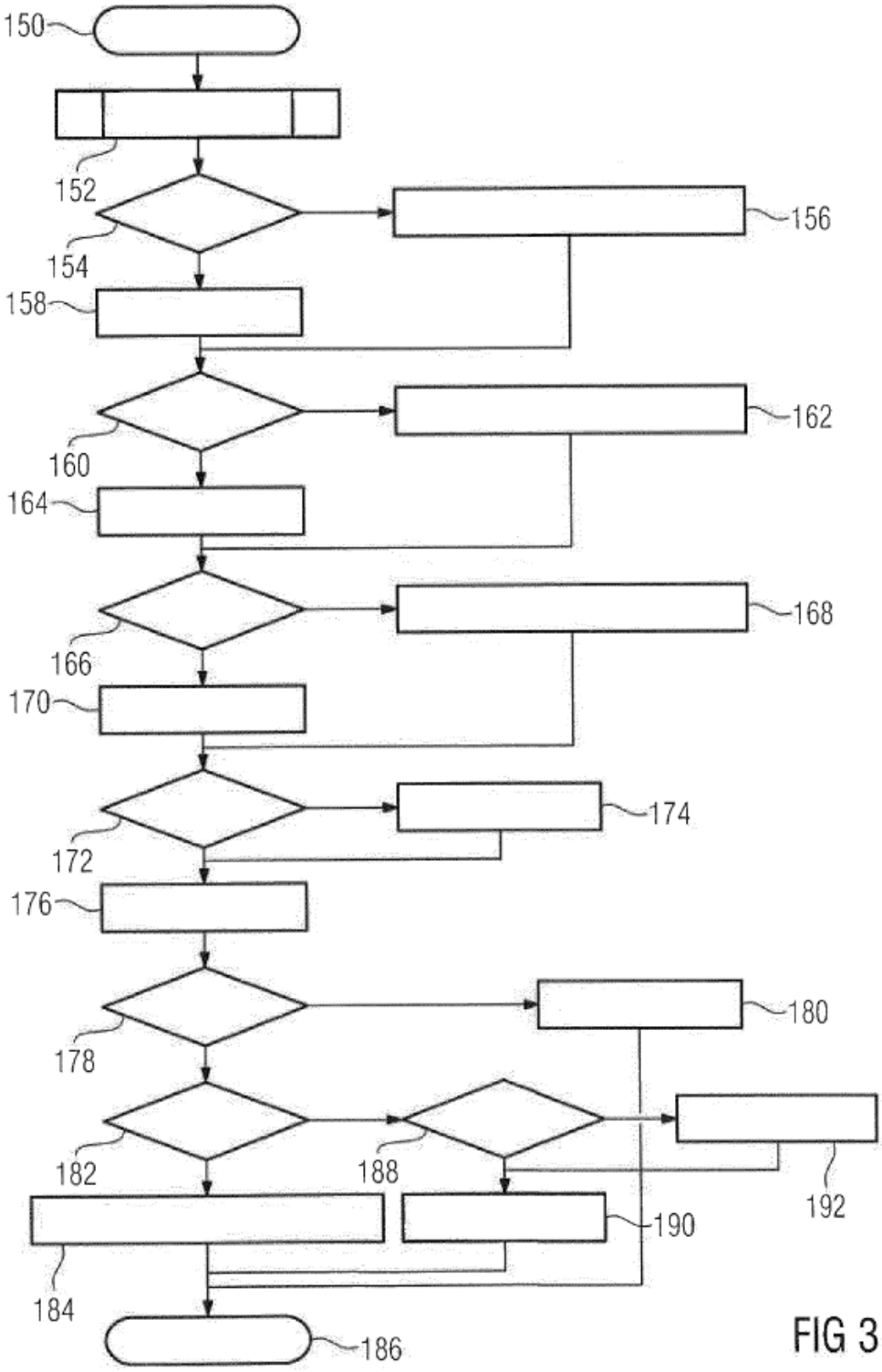

150
152
154
156
158
160
162
164
166
168
170
172
174
176
178
180
182
188
190
192
184
186

FIG 3

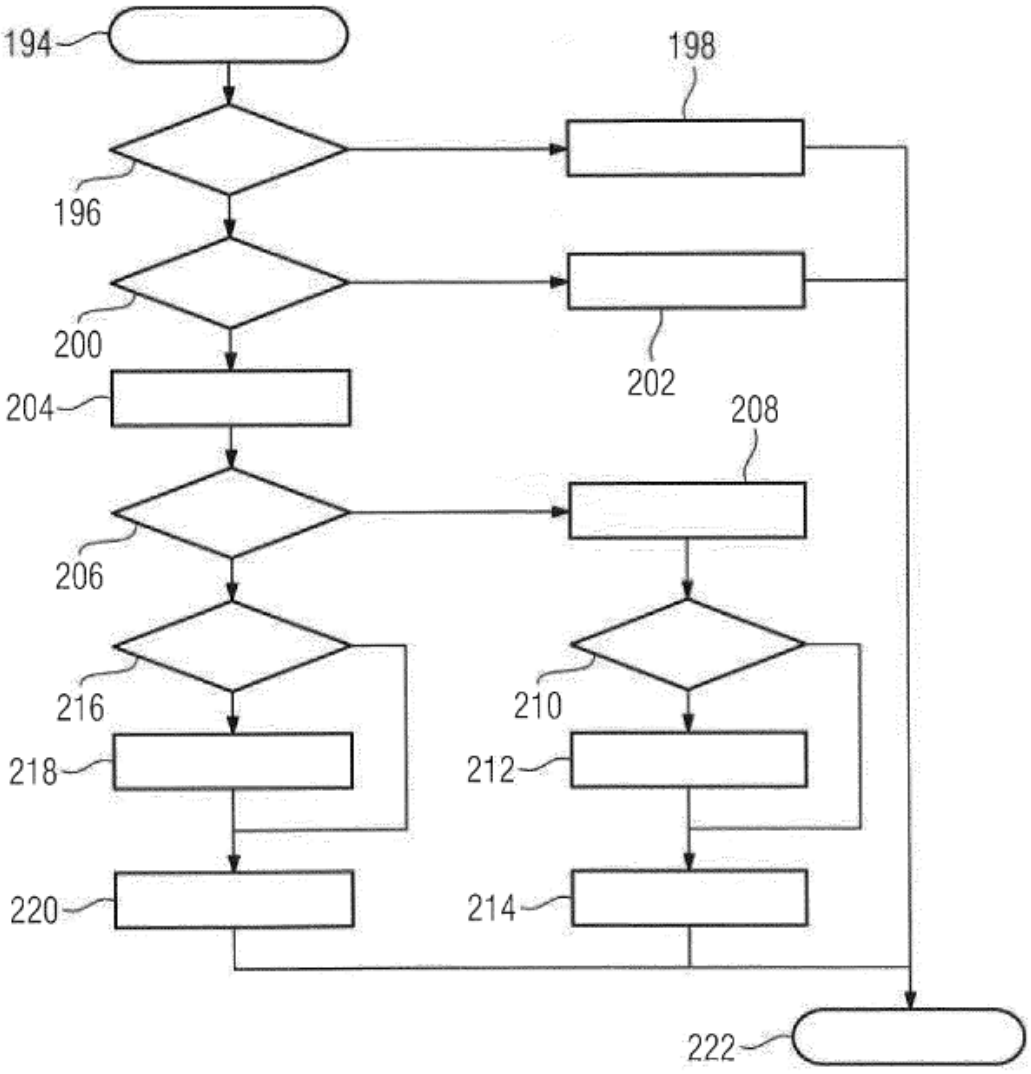


FIG 4