(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 318 192**

(51) Int. Cl.:
G05B 9/02 (2006.01)
G05B 15/02 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **03794897 .3**
(96) Fecha de presentación : **20.08.2003**
(97) Número de publicación de la solicitud: **1532494**
(97) Fecha de publicación de la solicitud: **25.05.2005**

(54) Título: **Dispositivo de seguridad para realizar un control a prueba de fallos de procesos críticos en cuanto a seguridad y método para implementar un nuevo programa de explotación en dicho dispositivo.**

(30) Prioridad: **28.08.2002 DE 102 40 584**

(45) Fecha de publicación de la mención BOPI:
01.05.2009

(45) Fecha de la publicación del folleto de la patente:
01.05.2009

(73) Titular/es: **Pilz GmbH & Co. KG.**
Felix-Wankel-Strasse 2
73760 Ostfildern, DE

(72) Inventor/es: **Klopfer, Johannes y**
Wohnhaas, Klaus

(74) Agente: **Isern Jara, Jorge**

DESCRIPCIÓN

Dispositivo de seguridad para realizar un control a prueba de fallos de procesos críticos en cuanto a seguridad y método para implementar un nuevo programa de explotación en dicho dispositivo.

El presente invento hace referencia a un dispositivo de seguridad para realizar un control a prueba de fallos de procesos críticos en cuanto a seguridad, especialmente la parada a prueba de fallos de una máquina o de maquinaria que cuenta con un módulo de entrada que lee automáticamente las señales del proceso, un módulo de tratamiento de señales a prueba de fallos para tratar automáticamente las señales del proceso y un módulo de salida a prueba de fallos que, dependiendo del módulo de tratamiento de señales, genera señales de control; además, el módulo de tratamiento de señales incorpora, al menos, un procesador programable y una primera memoria de sólo lectura en la que se almacena permanentemente un programa de control actual para el procesador.

Además, el invento hace referencia a un método para implementar un nuevo programa de explotación en un dispositivo de seguridad de este tipo, así como al correspondiente programa de explotación.

Un dispositivo de seguridad de este tipo puede encontrarse, por ejemplo, en la patente WO-98/44399.

En el sentido del presente invento, un dispositivo de seguridad es un instrumento -o una combinación de instrumentos interconectados- que recibe señales de proceso desde sensores y que, a partir de ellas y mediante operaciones lógicas -incluyendo etapas de tratamiento de datos o señales, eventualmente-, genera señales de salida. Las señales de salida se introducen en actuadores, que ejercen las acciones o reacciones deseadas en el entorno. Un ámbito de aplicación preferente de los dispositivos de seguridad es, en cuanto a seguridad de las máquinas se refiere, el control de los pulsadores de parada de emergencia, mandos a dos manos, puertas de protección, protecciones fotoeléctricas, detectores de parada y análogos. Dichos sensores se emplean para asegurar una máquina que, en funcionamiento, puede suponer un riesgo para los trabajadores que la están utilizando. Al abrir la puerta de protección o al accionar el pulsador de parada de emergencia se genera una señal de proceso que se introduce en el dispositivo de seguridad como señal de entrada. El dispositivo de seguridad reacciona a dicha señal de entrada y desconecta, de modo seguro (a prueba de fallos) y con ayuda del actuador, la parte de la máquina que pudiera suponer un peligro.

Al contrario de lo que sucede con los dispositivos de control “normales”, resulta característico de los dispositivos de seguridad que deben garantizar continuamente un estado seguro del proceso controlado, por ejemplo de la máquina que implica algún peligro. Esto debe ser así incluso aunque se produzca un fallo en el dispositivo de seguridad o en alguno de los aparatos conectados al mismo. Por esta razón, se fijan exigencias extraordinariamente elevadas en cuanto a la seguridad ante los propios fallos del dispositivo, lo que provoca un considerable aumento de los costes durante el desarrollo y la fabricación de dichos dispositivos. Por regla general, los dispositivos de seguridad necesitan recibir una autorización especial por parte de las autoridades pertinentes antes de su utilización, tarea realizada por las asociaciones profesionales o la TÜV (la ITV alemana). El dispositivo de seguridad debe cumplir con las normas de seguridad definidas, por ejemplo, en la norma europea EN 954-1. El presente invento considera todas estas características. Por tanto, el término “dispositivo de seguridad” se refiere exclusivamente a un instrumento -o a una combinación de instrumentos interconectados- que estén acreditados, como mínimo según la categoría 3 de la norma europea mencionada, para controlar máquinas, maquinaria y similares.

Un dispositivo de seguridad programable ofrece al usuario la posibilidad de ajustar las operaciones lógicas de las señales de entrada a sus necesidades individuales mediante un software denominado software de usuario. Así pues, el dispositivo de seguridad programable permite sustituir el cableado de los sensores individuales -anteriormente muy habitual- por los elementos de conexión lógicos.

Para poder desempeñar dicha función, el dispositivo de seguridad programable cuenta con un programa de explotación -independiente del programa de usuario- que determina el ámbito de funcionamiento principal del dispositivo. En especial, el programa de explotación incluye códigos fuente mediante los cuales los componentes de hardware del dispositivo de seguridad responden directamente y, con ello, pueden ser “resucitados”.

Además, en el programa de explotación también se han implementado reglas de control de seguridad que el usuario puede llamar con su programa de usuario como módulos funcionales preparados y que puede parametrizar con señales de entrada y salida actuales. Por ejemplo, en el programa de explotación existen módulos funcionales preparados para valorar a prueba de fallos un pulsador de parada de emergencia de dos canales o una puerta de protección de dos canales. En el programa de usuario, el usuario sólo puede determinar el modo en que los módulos preparados -se incluyen aquí el pulsador de parada de emergencia y la puerta de protección- se unen entre sí mediante operaciones lógicas.

El usuario no tiene acceso al programa de explotación por razones de seguridad, es decir, no puede intercambiarlo o modificarlo. En la terminología del sector a menudo se denomina el programa de explotación como *firmware*.

En la patente WO-98/44399 mencionada al comienzo del documento, se describe un método para programar un dispositivo de seguridad en el que las reglas de control de seguridad se implementan en el dispositivo en forma de módulos funcionales. El usuario puede seleccionar, parametrizar e interconectar mediante operaciones lógicas los módulos funcionales con su programa de usuario. Para ello, se emplea un aparato de programación con el que se

transfieren los comandos para seleccionar, parametrizar e interconectar mediante operaciones lógicas. Como ya se mencionó anteriormente, el usuario no tiene la posibilidad de acceder a las reglas de control de seguridad, es decir, no puede sustituirlas ni modificarlas.

Dicha prohibición del acceso al programa de explotación se corresponde con la práctica habitual en dispositivos de seguridad, ya que dicho programa de explotación -junto con el hardware del dispositivo- está sujeto a autorización por parte de las autoridades pertinentes. Si el usuario pudiera acceder al hardware y al programa de explotación, el fabricante del dispositivo de seguridad no podría garantizar con convencimiento que su aparato es a prueba de fallos.

No obstante, dicha práctica habitual tiene una consecuencia negativa: sólo el fabricante del dispositivo de seguridad puede modificar funciones del programa de explotación. Cuando se desee realizar una modificación de este tipo o cualquier otro acceso al programa de explotación, el usuario debe o bien enviar el dispositivo de seguridad al fabricante, o bien solicitar al mismo personal de servicio experto y autorizado. Esto se traduce en un esfuerzo caro y engorroso y que, además, puede afectar negativamente a los tiempos de parada de la maquinaria donde esté instalado el dispositivo.

En otros ámbitos fuera de la técnica de seguridad, por ejemplo en ordenadores personales corrientes, es práctica común que el usuario pueda realizar actualizaciones de software bajo su propia responsabilidad; para ello, no tiene más que adquirir un software nuevo del fabricante y lo implementa en su ordenador, en su caso siguiendo unas guía de instrucciones. Esto es asimismo válido en los denominados sistemas operativos, que representan un programa de explotación en el sentido otorgado en el presente invento. No obstante, existe el convencimiento general de que un procedimiento similar es impensable para aplicaciones de técnica de seguridad, ya que se le arrebataría al fabricante su control exclusivo sobre la combinación de hardware y programa de explotación. En lugar de eso, sería posible configurar combinaciones de hardware y programa de explotación no controladas, lo que supone un riesgo para la seguridad.

A partir de la patente EP-1.193.576-A2 se conoce un control de procesos con unidades de campo triplemente redundantes, el cual permite descargar un programa actualizado en cada una de dichas unidades sin que el proceso controlado se vea influido de manera permanente. Sin embargo, obviamente no se trata de un dispositivo de seguridad como el mencionado al comienzo del documento.

El objeto del presente invento es proporcionar un dispositivo de seguridad como el mencionado al comienzo del presente documento que permite una adaptación a los deseos del usuario más flexible y económica.

Dicho objeto se alcanza mediante un dispositivo de seguridad (del tipo mencionado al comienzo del documento) que cuenta con un dispositivo de descarga para aplicar un nuevo programa de explotación y una segunda memoria de sólo lectura en la cual se ha almacenado una primera información de hardware -que resulta característica al menos para el módulo de tratamiento de señales-, de tal forma que el nuevo programa de explotación contiene una segunda información de hardware que resulta característica, y de tal forma que el dispositivo de descarga habilita o impide a prueba de fallos la transferencia del nuevo programa de explotación dependiendo de la información de habilitación que contiene la primera y la segunda información del hardware.

El objeto también se cumple mediante un método para implementar un nuevo programa de explotación en un dispositivo de seguridad del tipo mencionado al principio del documento, que consta de los pasos que se describirán a continuación.

Preparar el dispositivo de seguridad con una primera memoria sólo de lectura en la que se ha almacenado un programa de explotación actual.

Preparar una primera información de hardware -característica para el dispositivo de seguridad- en una segunda memoria sólo de lectura del dispositivo de seguridad.

Preparar un nuevo programa de explotación.

Preparar una segunda información de hardware en el nuevo programa de explotación, de tal modo que la segunda información de hardware, bajo unos requisitos mínimos de hardware, sea característica para el nuevo programa de explotación.

Transferir el nuevo programa de explotación a la primera memoria de sólo lectura dependiendo de la información de habilitación que contiene la primera y la segunda información de hardware.

Con el dispositivo de seguridad descrito y el correspondiente método es posible, por vez primera, que un usuario de un nuevo programa de explotación, es decir, de un firmware nuevo, implemente o transfiera sobre un dispositivo de seguridad disponible. El presente invento se libera así del hasta ahora inquebrantable axioma de que únicamente el fabricante -que es responsable frente a las autoridades competentes- podía llevar a cabo acciones que afectaran a las reglas de control de seguridad.

El distanciamiento de la práctica empleada hasta ahora se basa en el sorprendente conocimiento de que el control ejercido por el fabricante sobre el dispositivo de seguridad -con ayuda de una información de habilitación especial o

adicional- puede mantenerse ininterrumpidamente. La elección y la definición de la información adicional queda en manos del fabricante. El hecho de que la implementación de un nuevo programa de explotación se pueda interrumpir a prueba de fallos -y, por tanto, "automática" o "mecánicamente"- dependiendo de la información de habilitación, permite al fabricante del dispositivo de seguridad limitar la cantidad de posibles combinaciones de hardware y programa de explotación del usuario. Basta con configurar el dispositivo de descarga de tal modo que la transferencia del nuevo programa de explotación sólo acontezca cuando, a través de la información de habilitación requerida, el dispositivo reconozca que la transferencia sobre la plataforma de hardware ha sido autorizada por el fabricante. La comprobación de la información de habilitación que, por ejemplo, contiene una lista de plataformas de hardware permitidas, puede realizarse a prueba de fallos mediante medidas informáticas o eléctricas -conocidas y corrientes en el ámbito de la seguridad en máquinas-, en particular mediante comprobación de doble canal -y, preferentemente, comprobación diversificada- de la información de habilitación y/o el bloqueo de doble canal -preferentemente, bloqueo diversificado- de la transferencia.

En otras palabras, el dispositivo de seguridad impide que el dispositivo de habilitación almacene el nuevo programa de explotación en función de la comparación establecida entre la primera y la segunda información de hardware. De este modo, el fabricante del dispositivo de seguridad puede controlar que el nuevo programa de explotación sólo se ponga en funcionamiento en una plataforma de hardware que cumpla con una serie de requisitos mínimos impuestos y probados por él. Así, el fabricante del dispositivo de seguridad puede restringir la variedad de combinaciones posibles de plataformas de hardware y programas de explotación.

El nuevo dispositivo de seguridad es mucho más flexible en su asistencia logística gracias a que el usuario tiene la posibilidad de actualizar el software del programa de explotación. Los costes de producción y servicio del fabricante se reducen. Por otro lado, los tiempos de parada de una maquinaria también pueden acortarse modificando el dispositivo de seguridad a nivel del programa de explotación, ya que no debe esperarse a que acuda un técnico del fabricante.

Además, el usuario posee un abanico más amplio de aplicaciones para un mismo dispositivo de seguridad, ya que éste puede reequiparse sin más que implementar un nuevo programa de explotación con más funciones. Y, por encima de todo, debe señalarse que las ventajas mencionadas no acarrean pérdidas en la seguridad, ya que el usuario, tal y como sucedía anteriormente, sigue sin tener acceso a las reglas de control de seguridad internas.

Por lo tanto, el objeto mencionado se cumple completamente.

En una configuración del invento, la información de habilitación se ha integrado -al menos parcialmente- en el nuevo programa de explotación de modo que pueda ser leída automáticamente.

Dicha configuración es una posibilidad especialmente sencilla -a la par que cómoda para el usuario- de evaluar la información de habilitación a prueba de fallos y, por tanto, de ejecutar o cancelar la transferencia del nuevo programa de explotación. Además, las manipulaciones con una función de habilitación -al menos parcialmente integrada- se pueden impedir incluso de manera más eficiente. Todo esto conduce a un mayor nivel de seguridad.

En otra configuración, la información de habilitación contiene una primera y una segunda información de versión secuencial, de tal modo que la primera información de versión secuencial se asigna al programa de explotación actual y la segunda información de versión secuencial se asigna al nuevo programa de explotación.

Una información de versión secuencial, es decir, una información de versión dispuesta según un orden inequívoco, constituye una posibilidad especialmente sencilla para realizar un bloqueo o una activación a prueba de fallos. Básicamente, los dispositivos de seguridad del fabricante se suministran con un programa de explotación implementado. La combinación de plataforma de hardware y programa de explotación actual sigue estando sujeta al control total del fabricante. Éste, con ayuda de una información de versión secuencial, puede garantizar fácilmente que el usuario sólo podrá implementar un programa de explotación más nuevo, es decir, con una información de versión secuencial superior. De este modo, el usuario nunca podrá dotar al dispositivo de seguridad suministrado de un programa de explotación más "antiguo". Así, la mayoría de las combinaciones no verificadas -y, por tanto, no autorizadas- de plataforma de hardware y programa de explotación quedan eficazmente excluidas de un modo sencillo.

Para el fabricante es suficiente que pueda demostrar, ante las autoridades correspondientes, que la nueva versión del programa de explotación con una información de versión superior puede funcionar a prueba de fallos en las plataformas de hardware empleadas hasta el momento. El coste que esto implica es relativamente pequeño, ya que las nuevas versiones de los programas de explotación se basan en las versiones anteriores y, por tanto, sólo incluyen un número limitado de modificaciones.

La posibilidad teórica de que el usuario implemente un programa de explotación antiguo y no verificado sobre un dispositivo de seguridad antiguo, queda excluida gracias a la comprobación a prueba de fallos de la información de versión secuencial.

En otra configuración del invento, el dispositivo de descarga incluye un comparador -para comparar la primera y la segunda información de versión- y un dispositivo de habilitación, de modo que éste impide o no la implementación del nuevo programa de explotación en función del resultado de la comparación: cuando la segunda información de versión secuencial es inferior a la primera, la implementación se impide.

Esta configuración es una posibilidad especialmente ventajosa para valorar automática o mecánicamente las informaciones de versiones secuenciales, con el fin ulterior de autorizar o bloquear la transferencia. Debe entenderse que el comparador o el dispositivo de habilitación pueden ser indistintamente módulos de hardware o de software -es decir, estar incluidos en el propio programa de explotación-.

En otra configuración, el dispositivo de habilitación sólo autoriza la implementación del nuevo programa de explotación cuando la segunda información de versión secuencial es superior a la primera.

En otras palabras: el almacenamiento del nuevo programa de explotación también se impide cuando la segunda información de versión secundaria secuencial coincide con la primera.

En esta configuración, la novedad respecto a los enfoques ya analizados es que se impide implementar de nuevo un programa de explotación idéntico al existente. Esto puede resultar útil en el siguiente ejemplo: el usuario, que ha detectado ciertos errores en el funcionamiento de ciertas funciones, determina que implementando de nuevo el programa de explotación podrá solventarlos. Sin embargo, este tipo de "autoayuda" suele resultar engañosa. Por tanto, desde el punto de vista de la seguridad, resulta ventajoso que el usuario sólo pueda implementar por sí mismo un programa de explotación con una información de versión superior en su dispositivo de seguridad.

En otra configuración, las informaciones de versión primera y segunda se protegen a prueba de fallos en el correspondiente programa de explotación.

La protección a prueba de fallos de la información de versión se consigue mediante un almacenamiento redundante y/o una formación de firma -ya conocida-, por ejemplo en forma de una suma de verificación CRC (cyclic redundancy check). En esta configuración es aún más fiable implementar un nuevo programa de explotación, ya que es imposible implementarlo por error, incluso aunque tenga lugar un fallo o la información de versión esté manipulada. El control del fabricante del dispositivo de seguridad se ha vuelto a reforzar.

En otra configuración, el nuevo programa de explotación incluye un código fuente que implementa reglas de control de seguridad en el dispositivo de seguridad cuando el nuevo programa de explotación se introduce en el dispositivo de seguridad.

Esta medida permite modificar el conjunto de funciones del dispositivo de seguridad de manera especialmente favorable sin que el fabricante pierda el control sobre la seguridad. Mediante esta configuración, las ventajas del invento resaltan especialmente. El usuario tiene la posibilidad de modificar las reglas de control de seguridad mediante la implementación del programa de explotación. No obstante, el usuario está obligado a intercambiar el "paquete completo" -controlado por el fabricante- de todas las reglas de control de seguridad implementadas. El usuario, por tanto, no puede modificar ni manipular por sí mismo las reglas de control, lo que supondría un riesgo para la seguridad.

En otra configuración, la primera y la segunda información de hardware contienen informaciones de versión secuenciales.

Una información de versión secuencial, como ya se ha comentado, es una clasificación unívoca y ordenada. La licitud de las configuraciones de plataforma de hardware y programa de explotación creadas por el usuario se controla así de un modo especialmente seguro y sencillo.

En otra configuración, la primera y la segunda información de hardware incluyen una información tipo.

De este modo puede comprobarse de forma más sencilla y fiable si una determinada combinación de plataforma de hardware y programa de explotación está autorizada. Una información tipo permite diferenciar entre sí series y plataformas de hardware de tal modo que se impide la implementación de un programa de explotación de tipo desconocido independientemente de la información de versión. En combinación con una información de versión secuencial se obtiene la posibilidad de realizar una comprobación doble, lo cual supone un aumento en la seguridad.

Debe entenderse que las características mentadas y las que se mencionarán de ahora en adelante pueden aplicarse no sólo en la combinación concreta descrita, sino también en otras combinaciones o por separado, sin abandonar el marco del presente invento.

En los dibujos se representan ejemplos de realización, que se describirán con más detalle de ahora en adelante. Los dibujos muestran lo siguiente:

En la figura 1 se muestra una representación esquemática de un dispositivo de seguridad según el invento;

En la figura 2 se muestra un diagrama de flujo para ilustrar el método según el invento.

En la figura 1 se designa la totalidad del dispositivo de seguridad según el invento con la cifra 10.

La función del dispositivo de seguridad 10 -configurado según una forma de realización preferente del invento- es realizar una parada segura de una maquinaria, especialmente de una maquinaria situada en un entorno de producción.

En este ejemplo, la maquinaria son tres accionamientos eléctricos 12 que pueden ser apagados por el dispositivo de seguridad 10 conjunta o individualmente. En este ejemplo de aplicación, el dispositivo de seguridad 10 evalúa como señales de entrada dos pulsadores de parada de emergencia 14 y la puerta de protección 16. Se conoce el modo en que los pulsadores de parada de emergencia 14 y la puerta de protección 16 están situados en la maquinaria, para poder así garantizar que quedan protegidos y son seguros durante la explotación de ésta.

El dispositivo de seguridad 10 de la presente forma de realización es, como aparato propietario, el único responsable de la protección de la maquinaria, es decir, de la parada de los accionamientos 12 cuando exista una señal de entrada procedente de los pulsadores de parada de emergencia 14 o de la puerta de protección 16. El control del funcionamiento de la máquina, por ejemplo la aceleración y frenado de los accionamientos 12 durante los ciclos de trabajo, no es cometido del dispositivo de seguridad 10. Para ello se prevé un control de funcionamiento ya conocido que, por razones de claridad, no se representa en la figura. No obstante, también existe la posibilidad de que en otras formas de realización el dispositivo de seguridad 10 también se encargue de controlar el funcionamiento de la maquinaria. Debe entenderse que, en este caso, el dispositivo de seguridad 10 presenta una mayor complejidad por lo que, además de las señales de entrada y salida mencionadas, recibe y transmite otras señales de control habituales en las máquinas.

También debe tenerse en cuenta que, además de los emisores de la señal de entrada mostrados -es decir, los pulsadores de parada de emergencia 14 y la puerta de protección 16-, pueden estar conectados a la entrada del dispositivo de seguridad 10 cualesquiera otros generadores de señal, como mandos de dos manos, detectores de parada, armarios eléctricos o conmutadores de posición. La valoración a prueba de fallos de dichos generadores de señal tiene lugar en el dispositivo de seguridad 10 de un modo conocido con ayuda del programa de explotación y del programa de usuario.

De igual modo, a la salida del dispositivo de seguridad 10 pueden estar conectadas otras partes receptoras accionadas eléctricamente, las cuales pueden desconectarse a prueba de fallos en función de las señales de entrada que reciba el dispositivo de seguridad 10.

Por último, debe señalarse que el usuario puede programar el dispositivo de seguridad 10 de un modo conocido empleando el software de usuario. Por ejemplo, puede consultarse la patente WO 98/44399 mencionada al comienzo del documento. Las ventajas del invento, no obstante, también se dan en aquellos dispositivos de seguridad que el usuario no puede programar por sí mismo mediante un software de usuario, siempre y cuando se disponga de un programa de explotación en el sentido conferido durante todo el documento. Los dispositivos de seguridad de este tipo son comercializados por la empresa solicitante del presente invento bajo la familia de productos PNOZelog™; todavía no es posible que el usuario cambie el programa de explotación de un aparato de esta familia.

Para recibir las variables del proceso de los generadores de señal -en este caso los pulsadores de parada de emergencia 14 y la puerta protectora 16-, el dispositivo de seguridad 10 posee un módulo de entrada 18. Debido a la seguridad a prueba de fallos exigida, dicho módulo de entrada 18 está diseñado con doble canal redundante, lo que se representa en la figura 1 con la línea discontinua.

No obstante, en ciertos casos particulares puede bastar configurar el módulo de entrada 18 -o al menos ciertas partes- con un solo canal. Además, para mantener la claridad del dibujo se ha representado el módulo de entrada como un bloque de funciones propio en el diagrama de bloques de la figura 1. No obstante, puede realizarse parcialmente mediante software e incorporarse al programa de explotación.

La cifra 20 designa un módulo de tratamiento de la señal del dispositivo de seguridad 10. Dicho módulo une -de un modo conocido- las señales de proceso recogidas por el módulo de entrada 18, generando a partir de ellas señales de control que son emitidas a través del módulo de salida 22. A menudo, el módulo de salida 22 incluye relés, contactores o conmutadores electrónicos con los que se interrumpe a prueba de fallos la alimentación eléctrica de los accionamientos 12 y de la maquinaria en general. La seguridad a prueba de fallos se simboliza de nuevo mediante una línea diagonal que remite a un diseño redundante del módulo de salida 20. El flujo de la señal desde el módulo de entrada 18 hasta el módulo de salida 22 -pasando a través del módulo de tratamiento de la señal 20- se refleja en la figura 1 con las correspondientes flechas de bloque.

El módulo de tratamiento de señales 20 incluye, al menos, un procesador programable 24, una memoria de sólo lectura 26 y una memoria principal 28. En la memoria de sólo lectura 26 se almacena -de modo conocido y permanente- el programa de explotación 30 para el procesador 24. En este caso se trata de una suma de comandos de programación -legibles por ordenador- que permiten desarrollar la funcionalidad principal del dispositivo de seguridad 10. En particular, el programa de explotación 30 incluye en este ejemplo de realización aquellos comandos de programación que permiten al procesador 24 leer y emitir señales. Los comandos permiten que el hardware del dispositivo de seguridad 10 “resucite”.

Además, el programa de explotación 30 incluye un conjunto de reglas de control de seguridad preparadas con las que, por ejemplo, puede llevarse a cabo la valoración a prueba de fallos de un pulsador de parada de emergencia de doble canal. Asimismo, se dispone de algoritmos de valoración a prueba de fallos para cualquier otro generador de señales autorizado y para todos los actuadores autorizados situados a la salida del dispositivo de seguridad 10.

En el caso de que el dispositivo de seguridad 10 sea un aparato propietario, el programa de explotación 30 incluirá además la asignación de las reglas de control de la seguridad a las claves de entrada y salida. Así, el usuario no tiene ninguna influencia -y si la tiene, muy reducida- sobre el abanico de funciones y su alcance. Como ya se ha comentado, también existe la alternativa de diseñar el dispositivo de seguridad de tal forma que el usuario, con ayuda de un programa de usuario diseñado por él, pueda seleccionar y parametrizar reglas de control de seguridad.

La memoria principal 28 sirve para almacenar temporalmente las variables intermedias y, en su caso, para registrar el programa de usuario, el cual se incorpora al programa de explotación 30.

El módulo de tratamiento de señales 20 del dispositivo de seguridad 10 está diseñado a prueba de fallos continuamente, lo que puede conseguirse, por ejemplo, mediante un diseño redundante con pruebas y controles mutuos. El procesador 24, la memoria de sólo lectura 26 y la memoria principal 28 se han representado dobles por este motivo.

En el diagrama de bloques se señala con la cifra 32 un dispositivo de descarga para implementar un nuevo programa de explotación 34. "Implementar" significa que el nuevo programa de explotación 34 se almacena en la memoria de sólo lectura 26 de tal modo que completa el abanico de funciones del dispositivo de seguridad 10 ofrecido por el programa de explotación 30, o bien lo sustituye. La implementación del nuevo programa de explotación 34 puede incluso tener como consecuencia la sustitución completa del programa de explotación 30 disponible. De ese modo, se tiene la posibilidad -entre otras- de sustituir las reglas de control de seguridad preparadas por otras modificadas.

El dispositivo de descarga 32 según el invento incluye un comparador 36 y un dispositivo de habilitación 38. Además, se prevé una información de versión secuencial tanto en el programa de explotación disponible 30 como en el nuevo programa 34 -señaladas en el diagrama de bloques con las cifras 40 y 42, respectivamente-. El comparador 36 lee la información de versión 40 del programa de explotación disponible 30 y la información de versión 42 del programa de explotación nuevo 34, comparándolas.

En función del resultado de dicha comparación, el dispositivo de habilitación 38 impide o permite la implementación del nuevo programa de explotación 34. Concretamente, el dispositivo de habilitación 38 sólo permite implementar el nuevo programa de explotación 34 cuando la información de versión del nuevo programa de explotación 34 es superior a la información de versión del programa de explotación disponible 30. En otras palabras, el dispositivo de seguridad 10 sólo permite implementar un nuevo programa de explotación 34 cuando éste es efectivamente más nuevo que el ya disponible 30, lo que se determina por comparación.

Debe entenderse que la representación de la figura 1 -con el comparador 36 y el dispositivo de habilitación 38 en primera línea- se ha escogido por motivos ilustrativos. En la práctica, la comparación de las informaciones de versión y la autorización o denegación de la implementación tiene lugar con ayuda de herramientas informáticas, es decir, mediante comandos de programación, los cuales se almacenan en la memoria de sólo lectura 26 -como parte del programa de explotación disponible 30- y son tratados por el procesador 24. En lo que se refiere al hardware, el dispositivo de descarga 32 cuenta además con una interfaz ya conocida -por ejemplo una interfaz RS232- mediante la cual pueda leerse el nuevo programa de explotación 34 en caso de que se reciba la autorización necesaria.

Según una forma de realización preferente del invento, las informaciones de versión 40 y 42 de los programas de explotación 30 y 34 están incluidas de manera múltiplemente redundantes en dichos programas y/o protegidas por medidas de seguridad a prueba de fallos, como una suma de verificación CRC o una creación de firma. El nuevo programa de explotación 34 sólo podrá ser habilitado por el dispositivo 38 si la comparación a prueba de fallos entre las dos informaciones de versión 40, 42 proporciona como resultado inequívoco que la información de versión del nuevo programa de explotación 34 es superior a la información de versión del programa de explotación 30.

Según una forma de realización preferente, en el dispositivo de seguridad 10 se almacena asimismo una información de hardware 44 que resulta característica (al menos para el módulo de tratamiento de señales 20). En otras palabras, la información de hardware 44 indica el grado de desarrollo de la plataforma de hardware del dispositivo de seguridad 10. Según una forma de realización preferente, la información de hardware también incluye una información tipo 46, mediante la cual pueden identificarse distintas plataformas de hardware con mayor precisión. Además, en el nuevo programa de explotación 34 se prevé una segunda información de hardware 48 que sirve para identificar los requisitos mínimos de hardware exigidos. Preferentemente, las informaciones de hardware 44, 48 son informaciones de versión secuenciales que permiten obtener una clasificación inequívoca de las plataformas de hardware (o de los requisitos mínimos exigibles) en un orden según el desarrollo.

En las formas de realización preferentes, durante la comprobación no sólo se tiene en cuenta si se autoriza o no la implementación del nuevo programa de explotación 34, sino también las informaciones de hardware 44, 46 y 48. En concreto, la implementación del nuevo programa de explotación 34 sólo se autoriza cuando los requisitos mínimos codificados en el programa de explotación 34 existen sin ningún género de dudas en la plataforma de hardware del dispositivo de seguridad 10 debido a las informaciones de hardware 44, 46 almacenadas.

Según otra forma de realización preferente, en el dispositivo de seguridad 10 se almacena permanentemente otra información de versión 50 que define la versión mínima autorizada para un nuevo programa de explotación 34. Así, la autorización para implementar un nuevo programa de explotación 34 sólo depende de si la información de versión 42 es superior a la información de versión mínima 50. Este nuevo criterio de comparación tiene como consecuencia

que la implementación del nuevo programa de explotación 34 dependa de otro control. No obstante, dicho control puede suprimirse si el fabricante del dispositivo de seguridad 10 garantiza que éste se suministra continuamente con un programa de explotación 30 en el que está contenida una información de versión 40.

El requisito mínimo para el nuevo programa de explotación 34 puede entonces definirse así: el nuevo programa de explotación 34 sólo podrá implementarse si posee una información de versión superior a la del programa existente.

En la figura 2 se representa esquemáticamente -mediante un diagrama de flujo- el modo en que puede tener lugar la implementación del programa de explotación 34. Es fácil deducir que una opción óptima es que el método se diseñe como un código fuente adecuado para el procesador 24.

En el paso 60 se activa, en primer lugar, un modo de descarga. Para impedir un servicio defectuoso y una activación involuntaria esto puede realizarse, preferentemente, de modo que se accione un interruptor de llave (no representado) -añadido únicamente para esto- en el dispositivo de seguridad 10. No obstante, también es posible activar el modo de descarga mediante un ordenador, por ejemplo introduciendo una contraseña.

Según el paso 62 tiene lugar la lectura de la información de versión actual 40 del programa de explotación 30. Finalmente, en el paso 64 se lee la información de versión 42 el nuevo programa de explotación 34. El paso 66 indica que se realiza una comparación entre ambas informaciones de versión 40, 42. Si la información de versión 40 del programa de explotación disponible 30 es superior o mayor a la información de versión 42 del nuevo programa de explotación 34, tiene lugar, según el paso 68, una interrupción del método y, preferentemente, finaliza el modo de descarga. Así, se impide la implementación del nuevo programa de explotación 34.

Si la comparación de ambas informaciones de versión 40, 43 indica que el nuevo programa de explotación 34 puede completar o sustituir al antiguo 30, el paso 70 indica que la información de hardware 44, 46 del dispositivo de seguridad 10 se lee. En el paso 72, finalmente, se lee la información de hardware 48, la cual define si el nuevo programa de explotación 34 puede arrancarse y está autorizado.

Según el paso 74 tiene lugar una forma de realización (representada) en la que tiene lugar una comparación de los tipos, es decir, se comprueba si el programa de explotación 34 está permitido para trabajar con el dispositivo de seguridad 10. Si éste no es el caso, el paso 76 indica que el modo de descarga se interrumpe indefectiblemente.

Si la comparación entre tipos es positiva, en el paso 78 se vuelve a comprobar un nuevo criterio, que consiste en verificar si la información de hardware 44 del dispositivo de seguridad 10 es mayor o al menos igual a la información de hardware 48 contenida en el programa de explotación 34. Si la comparación establece que el dispositivo de seguridad 10 no cumple con los requisitos mínimos de hardware, entonces se interrumpe el modo de descarga según el paso 80.

Sin embargo, si la comprobación de los requisitos da un resultado positivo según las informaciones de hardware, entonces el programa de explotación 34 se implementa según el paso 82. En otras palabras, el programa de explotación 34 se almacena en la memoria sólo de lectura 26. Tras finalizar la descarga, el nuevo programa de explotación sustituye o completa el anterior 30 durante el uso seguro del dispositivo de seguridad 10.

La transferencia del programa de explotación 34 al dispositivo de seguridad 10 puede suceder de diversos modos. Como se mencionó más arriba, el programa de explotación 34 puede transferirse al dispositivo de seguridad 10 gracias a la interfaz en serie si recibe la autorización. También es posible realizar la transferencia mediante un bus de campo o un medio de almacenamiento intercambiable. De hecho, la transferencia del nuevo programa de explotación 34 puede realizarse también por Internet.

Para aumentar aún más la seguridad resulta recomendable que el programa de explotación 34 y, especialmente, las informaciones de versión 42 y 48 estén protegidas frente a manipulaciones y falsificaciones mediante un algoritmo de clave. En ese caso, el dispositivo de seguridad 10 cuenta con un programa de clave (no representado).

En las formas de realización preferentes descritas hasta ahora las informaciones de versión incluyen, por ejemplo, combinaciones de números y/o letras que permiten establecer una clasificación inequívoca en un orden determinado. No obstante, también es posible preparar las informaciones de versión de manera que estén “no finalizadas”, es decir, en forma de un algoritmo que proporcione un resultado unívoco y, así, permita determinar la información de versión secuencial. En este caso, la información de versión secuencial lo es en el sentido dado a lo largo del documento.

REIVINDICACIONES

1. El presente invento hace referencia a un dispositivo de seguridad para realizar un control a prueba de fallos de procesos críticos en cuanto a seguridad, especialmente el paro a prueba de fallos de una máquina (12) o de maquinaria, que cuenta con un módulo de entrada (18) que lee automáticamente las señales del proceso, un módulo de tratamiento de señales (20) a prueba de fallos para tratar automáticamente las señales del proceso y un módulo de salida (22) a prueba de fallos que, dependiendo del módulo de tratamiento de señales (20), genera señales de control; además, el módulo de tratamiento de señales (20) incorpora, al menos, un procesador (24) programable y una primera memoria de sólo lectura (26) en la que se ha almacenado permanentemente un programa de control actual (30) para el procesador (24), **caracterizado** por un dispositivo de descarga (32) para transferir un nuevo programa de explotación (34) que cuenta con un dispositivo de descarga para aplicar un nuevo programa de explotación y una segunda memoria de sólo lectura (26) en la cual se ha almacenado una primera información de hardware (44) -que resulta característica al menos para el módulo de tratamiento de señales (20)-, de tal forma que el nuevo programa de explotación (34) contiene una segunda información de hardware (48) que resulta característica, y de tal forma que el dispositivo de descarga (32) habilita o impide a prueba de fallos la transferencia del nuevo programa de explotación (34) dependiendo de la información de habilitación (40, 42, 44, 48) que contiene la primera y la segunda información del hardware y la autoriza o rechaza a prueba de fallos.

2. Dispositivo de seguridad según la reivindicación 1, **caracterizado** por el hecho de que la información de habilitación (40, 42, 44, 48) está integrada, al menos en parte, en el nuevo programa de explotación (34) de forma que pueda leerse mecánicamente.

3. Dispositivo de seguridad según la reivindicación 1 ó 2, **caracterizado** por el hecho de que la información de habilitación (40, 42, 44, 48) contiene una primera (40) y una segunda (42) información de versión secuencial, de modo que la primera información de versión secuencial (40) está asignada al programa de explotación actual (30) y la segunda (42) al nuevo programa de explotación (34).

4. Dispositivo de seguridad según la reivindicación 3, **caracterizado** por el hecho de que el dispositivo de descarga (32) incluye un comparador (36) -para comparar la primera y la segunda información de versión (40, 42)- y un dispositivo de habilitación (38), de modo que éste impide o no la implementación del nuevo programa de explotación (34) en función del resultado de la comparación: cuando la segunda información de versión secuencial (42) es inferior a la primera (40), la implementación se impide.

5. Dispositivo de seguridad según la reivindicación 4, **caracterizado** por el hecho de que el dispositivo de habilitación (38) sólo autoriza la implementación del nuevo programa de explotación (34) cuando la segunda información de versión (42) secuencial es superior a la primera (40).

6. Dispositivo de seguridad según una de las reivindicaciones de la 3 a la 5, **caracterizado** por el hecho de que las informaciones de versión primera y segunda (40, 42, 44, 48) se protegen a prueba de fallos en el correspondiente programa de explotación (30, 34).

7. Dispositivo de seguridad según una de las reivindicaciones de la 1 a la 6, **caracterizado** por el hecho de que el nuevo programa de explotación (42) incluye un código fuente que implementa reglas de control de seguridad en el dispositivo de seguridad (10) cuando el nuevo programa de explotación (42) se introduce en el dispositivo de seguridad (10).

8. Dispositivo de seguridad según una de las reivindicaciones de la 1 a la 7, **caracterizado** por el hecho de que la primera y la segunda información de hardware (44, 48) contienen informaciones de versión secuenciales.

9. Dispositivo de seguridad según una de las reivindicaciones de la 1 a la 8, **caracterizado** por el hecho de que la primera y la segunda información de hardware (44, 48) contienen información tipo de hardware (46).

10. Método para implementar un nuevo programa de explotación en un dispositivo de seguridad según una de las reivindicaciones de la 1 a la 9, que consta de los siguientes pasos: preparar el dispositivo de seguridad (10) con una primera memoria sólo de lectura (26) en la que se ha almacenado un programa de explotación actual (30); preparar una primera información de hardware (44) -característica para el dispositivo de seguridad (10)- en una segunda memoria sólo de lectura del dispositivo de seguridad (10); preparar un nuevo programa de explotación (34); preparar una segunda información de hardware (48) en el nuevo programa de explotación (34), de tal modo que la segunda información de hardware (48), bajo unos requisitos mínimos de hardware- sea característica para el nuevo programa de explotación (34); transferir el nuevo programa de explotación (34) a la primera memoria de sólo lectura (26) dependiendo de la información de habilitación (40, 42, 44, 48) que contiene la primera y la segunda información de hardware.

11. Método según la reivindicación 10, **caracterizado** por el hecho de que la información de habilitación (40, 42, 44, 48) contiene una primera (40) y una segunda (42) información de versión secuencial, de tal modo que la primera información de versión secuencial (40) se asigna al programa de explotación actual y la segunda información de versión secuencial (42) se asigna al nuevo programa de explotación (34).

12. Método según la reivindicación 11, **caracterizado** por el hecho de que la transferencia se impide cuando la segunda información de versión secuencial (42) es inferior a la primera (40).

13. Programa de explotación (34) para implementar en un dispositivo de seguridad (10) según el método descrito en una de las reivindicaciones de la 10 a la 12, **caracterizado** por el hecho de que la información de habilitación integrada (42, 48), la cual contiene al menos la segunda información de hardware (48) -característica de la configuración de hardware mínimamente exigible para el dispositivo de seguridad (10), en donde la segunda información de hardware (48) está prevista para poder autorizar o denegar la implementación del programa de explotación en el dispositivo de seguridad (10), dependiendo de la comparación que se establezca con la primera información de hardware (44) almacenada en el dispositivo de seguridad (10).

14. Programa de explotación según la reivindicación 13, **caracterizado** por un código fuente que implementa reglas de control de seguridad en el dispositivo de seguridad (10) cuando el programa de explotación (34) se desarrolla en un módulo de tratamiento de señales (20) del dispositivo de seguridad (10).

15. Programa de explotación según la reivindicación 13 ó 14, **caracterizado** por el hecho de que la información de habilitación (42, 48) se ha almacenado a prueba de fallos en el programa de explotación (34).

16. Portador de datos en el que se codifique un programa de explotación (34) según una reivindicación de la 13 a la 15.

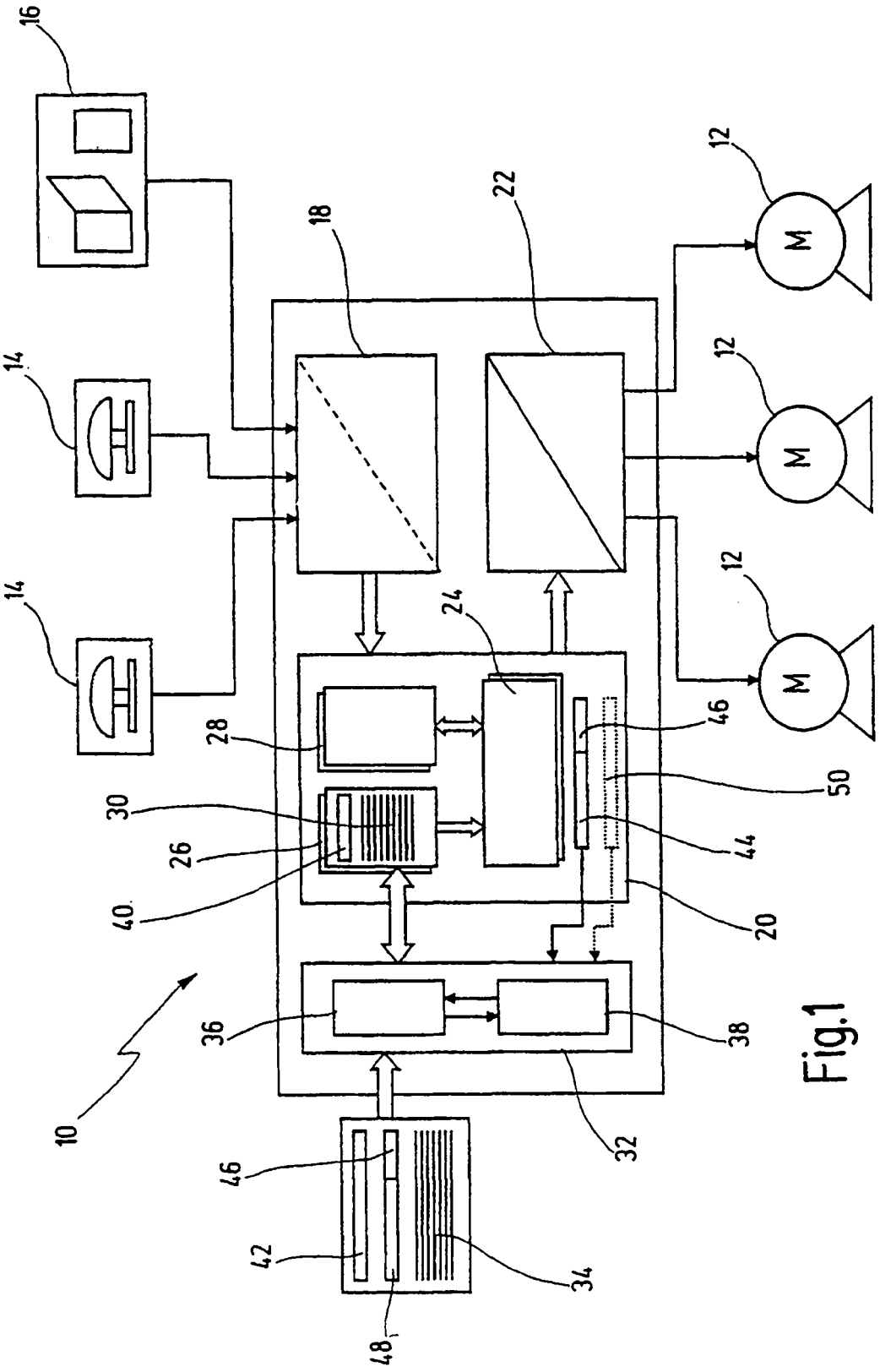
16
14
14
18
22
12
12
12
M
M
M
24
28
30
26
40
46
50
44
20
36
38
32
10
46
42
34
48

Fig.1

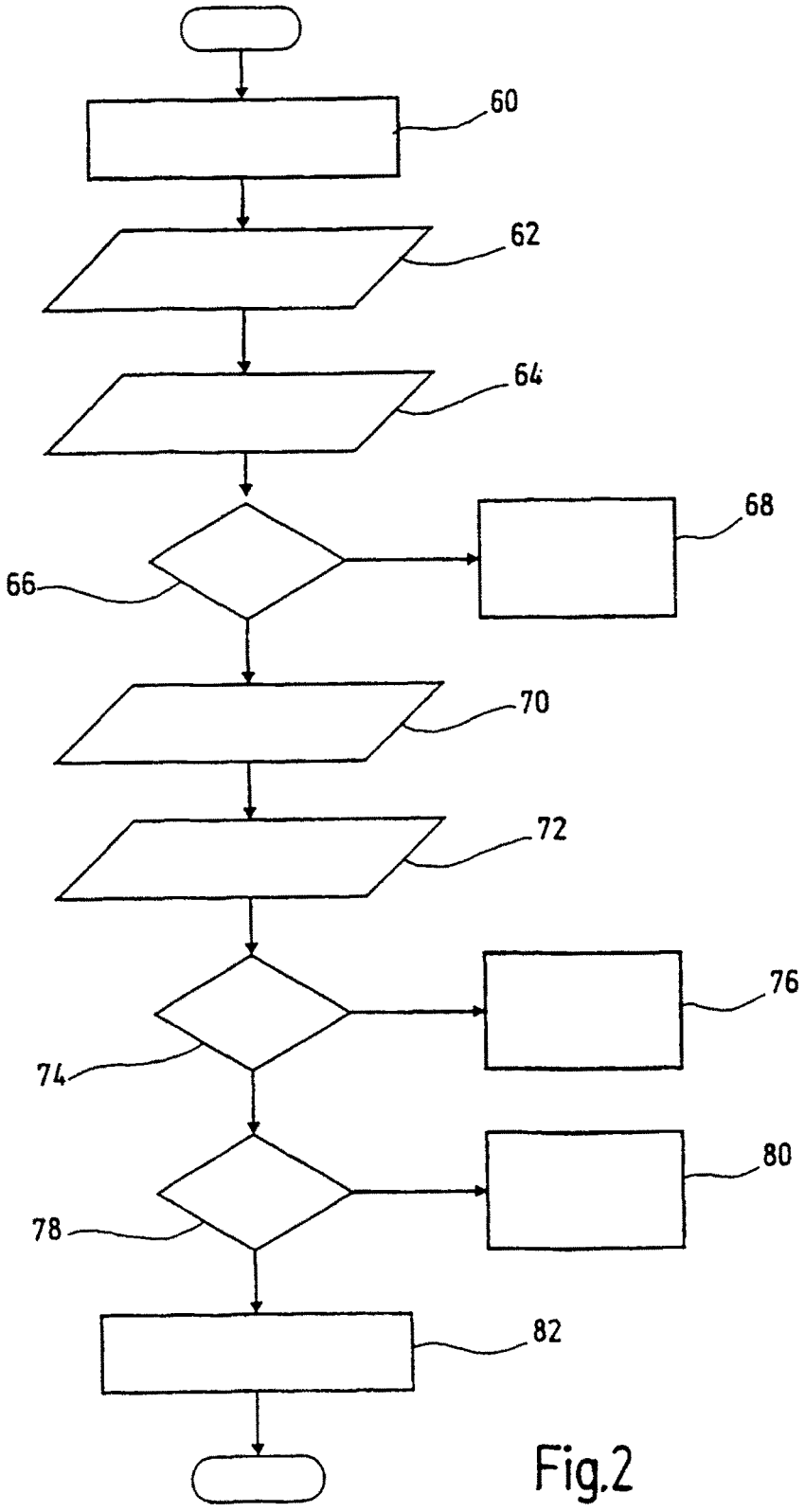

Fig.2