

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **3 026 182**

51 Int. Cl.:

G06F 21/74 (2013.01)

G06F 21/76 (2013.01)

G05B 9/02 (2006.01)

G05B 19/05 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **13.08.2020** **E 20190930 (6)**

97 Fecha y número de publicación de la concesión europea: **05.03.2025** **EP 3792807**

54 Título: **Sistema de seguridad de un dispositivo**

30 Prioridad:

10.09.2019 FR 1909965

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

10.06.2025

73 Titular/es:

SCHNEIDER ELECTRIC INDUSTRIES SAS
(100.00%)

35 Rue Joseph Monier
92500 Rueil Malmaison, FR

72 Inventor/es:

EHLE, VALÉRIE;
EYRAUD, ANNICK;
BUCHET, YANNICK y
FABRON, DAVID

74 Agente/Representante:

GONZÁLEZ PECES, Gustavo Adolfo

ES 3 026 182 T3

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

DESCRIPCIÓN

Sistema de seguridad de un dispositivo

Campo técnico

La presente invención se refiere a un sistema de seguridad o de protección.

- 5 Se encuadra en el campo de las aplicaciones de automatización, en particular para la automatización industrial, la automatización de edificios o los sistemas de control y/o mando de redes de distribución de energía.

Técnica anterior

Se sabe que los autómatas programables se utilizan para la gestión de procedimientos domésticos o industriales, por ejemplo para la gestión de una red eléctrica.

- 10 Para garantizar la seguridad de estos procedimientos frente a cualquier riesgo de robo de datos o intentos de intrusión malintencionados, los autómatas suelen incluir uno o más sistemas de seguridad para garantizar el control y la integridad de los datos almacenados y la fiabilidad de las comunicaciones del PLC.

Estos sistemas de seguridad pueden, por ejemplo, adoptar la forma de software (herramienta antimalware, cortafuegos, escaneo de vulnerabilidades, etc.) o restricciones físicas de acceso (llaves, contraseñas cifradas, etc.).

- 15 A modo de ejemplo, para controlar el acceso local directo a determinados módulos de autómatas, éstos incluyen un sistema de seguridad en forma de interfaz hombre-máquina, que requiere que un operario introduzca una contraseña en un teclado si desea acceder al autómata.

Sin embargo, tales sistemas no son del todo satisfactorios.

- 20 De hecho, es necesario proporcionar una interfaz hombre-máquina por módulo del autómata. Además de que una interfaz hombre-máquina es cara, lleva mucho tiempo implementarla en cada módulo y consume mucha energía, puede ser vulnerable si la contraseña ha sido divulgada o robada.

Además, aunque algunas situaciones operativas requieren un estado de seguridad alto de los autómatas, un estado de seguridad más bajo también puede ser suficiente en otras situaciones operativas, por lo que no se requieren sistemas de seguridad relativamente complejos.

- 25 El documento del estado de la técnica WO2018038536 divulga un procedimiento para conceder a un usuario que opera un terminal en un modo de bloqueo y un modo de desbloqueo una primera y una segunda autoridad que permiten al usuario controlar el primer y el segundo conjunto de elementos respectivamente. El segundo conjunto contiene más elementos que el primero. El primer resultado se obtiene controlando el elemento del primer conjunto en modo de bloqueo. El modo de bloqueo se cambia a modo de desbloqueo mientras se borra parte de los primeros resultados después de obtener el primer resultado, lo que impide que los primeros resultados afecten a los elementos del segundo conjunto cuando el usuario utiliza el terminal en modo de desbloqueo.

Sumario

La invención mejora la situación.

- 35 La invención tiene por objeto más particularmente proporcionar un sistema de seguridad eficaz para un dispositivo, tal como un autómata, para una utilización particularmente simple y flexible, que permita en particular variar el estado de seguridad de manera simple y segura en función de las necesidades de funcionamiento.

Se propone un sistema de seguridad montado en un dispositivo, comprendiendo el sistema de seguridad un elemento de control operable por al menos un operario:

- 40
 - en una primera posición, en la que el dispositivo está configurado para estar en un estado de alta seguridad, y
 - en una segunda posición, en la que el dispositivo está configurado para estar en un estado de baja seguridad.

Gracias a estas disposiciones, la actuación de un elemento de control en el dispositivo permite determinar el estado de seguridad esperado. Para garantizar la seguridad del sistema se utilizan tanto el control de acceso físico como programas informáticos especialmente sencillos y eficaces.

- 45 Más particularmente, una conexión remota al dispositivo no permite modificar su estado de seguridad, siendo necesario el acceso y accionamiento directo del sistema de seguridad.

Según otro aspecto, se propone un dispositivo que comprende dicho sistema de seguridad.

Según otro aspecto, se propone un procedimiento de funcionamiento de dicho sistema de seguridad, que comprende las siguientes etapas:

- si el elemento de control está en la primera posición :
- comprobar si ya se ha configurado la seguridad en el dispositivo, y
- 5 • si no, descargue los datos de configuración específicos del dispositivo y configure la seguridad en el dispositivo antes de utilizarlo.

Según otro aspecto, se propone un programa de ordenador que comprende instrucciones para implementar todo o parte de un procedimiento como se define en el presente documento cuando dicho programa es ejecutado por un procesador.

- 10 Según otro aspecto, se proporciona un medio de grabación no transitorio legible por ordenador en el que se graba dicho programa.

Por "ordenador" se entiende cualquier medio de procesamiento de información programable, por ejemplo un procesador incluido en un ordenador fijo, tableta, teléfono móvil o similar.

- 15 Las características expuestas en los párrafos siguientes pueden, opcionalmente, ser implementadas. Pueden utilizarse de forma independiente o combinadas entre sí:

El estado de alta seguridad incluye una configuración de funciones de protección de software.

El elemento de control puede ser accionado por un operario manualmente.

El elemento de control comprende una ranura para hacer pivotar un selector entre al menos la primera posición y la segunda posición.

- 20 El elemento de control es accionable por un operario mediante comunicación inalámbrica con el dispositivo realizada a corta distancia.

El elemento de control también es operable en una tercera posición, en la que el dispositivo se encuentra en un estado de restablecimiento.

El dispositivo es un autómatas programable o un módulo de autómatas programable industrial.

- 25 El dispositivo comprende una cara frontal y una cara posterior, estando montado el sistema de seguridad en la cara posterior, estando configurada la cara posterior para disponerse en contacto con un soporte.

El procedimiento comprende las siguientes etapas:

- si el elemento de control está en la tercera posición :
- desplazar el elemento de control a la primera o segunda posición.

- 30 El accionamiento del elemento de control entre la primera posición y la segunda posición requiere un paso intermedio en la tercera posición.

Breve descripción de los dibujos

Otras características, detalles y ventajas se pondrán de manifiesto a partir de la descripción detallada que figura a continuación, y del análisis de los dibujos adjuntos, en los que:

- 35 **Fig. 1**
La fig. 1 muestra una vista en perspectiva de la cara posterior de un dispositivo que comprende un sistema de seguridad según una realización.
- 40 **Fig. 2**
La fig. 2 muestra una vista en perspectiva de la cara frontal del dispositivo de la fig. 1 fijado sobre un soporte con otros dispositivos.
- 45 **Fig. 3**
La fig. 3 muestra una vista esquemática del dispositivo de la fig. 1.
- Fig. 4**
La fig. 4 muestra una vista parcial ampliada de la cara posterior del dispositivo de la fig. 1.
- Fig. 5**
La Fig. 5 muestra un diagrama que ilustra el procedimiento de funcionamiento del sistema de seguridad según una realización.

Descripción de realizaciones

Los dibujos y la descripción que figuran a continuación contienen, en su mayor parte, elementos de certeza. Por lo tanto, no sólo pueden servir para mejorar la comprensión de esta divulgación, sino también contribuir a su definición, cuando proceda.

- 5 Se hace referencia a la Fig. 1, que representa un dispositivo 1 que comprende un sistema de seguridad según la invención. El sistema de seguridad es más concretamente un dispositivo de protección informática, también conocido como sistema de ciberseguridad.

Según una realización, el dispositivo 1 está implementado en un autómata programable industrial (API; en inglés "Programmable Logic Controller", PLC). Un autómata de este tipo está configurado para controlar un procedimiento doméstico o industrial, en particular mediante el procesamiento secuencial de la información. Más concretamente, el autómata puede transmitir una orden a uno o más autómatas o sistemas de accionamiento basándose en datos de entrada, como mediciones de sensores, valores de consigna u otros datos.

A modo de ejemplo, el autómata se utiliza para controlar máquinas y sensores en una fábrica o edificio, o para accionar un sistema de gestión de energía.

- 15 Ventajosamente, el dispositivo 1 según la invención se refiere a un autómata seguro.

Según una realización, el dispositivo 1 es un módulo, tal como un módulo de comunicación, del PLC. De forma más general, el dispositivo 1 puede ser cualquier módulo o equipo industrial que permita configurar la seguridad a distancia.

Como se ilustra en la Fig. 2, el dispositivo 1 puede configurarse para ser montado sobre un soporte, por ejemplo un carril 2. El soporte 2 comprende generalmente otros dispositivos 3, 4, 5 dispuestos de forma modular entre sí. Por lo tanto, el dispositivo 1 puede almacenarse en un armario eléctrico (no representado).

El dispositivo 1 tiene generalmente una forma de paralelepípedo. Sin embargo, también son posibles otras formas.

El dispositivo 1 comprende así una cara frontal 1a, visible en la Fig. 2, accesible a un operario.

El dispositivo 1 comprende además una cara posterior 1b, visible en la Fig. 1, capaz de enfrentarse, en particular de entrar en contacto, con el soporte 2. Una vez fijado el dispositivo 1 al soporte 2, la cara posterior 1b ya no es directamente accesible al operario. El aparato 1 debe retirarse del soporte 2 para acceder al panel trasero 1b.

Como se ilustra en Fig. 2 y Fig. 3, el dispositivo 1 comprende interfaces de entrada 10 / salida 11 configuradas para recibir y enviar información desde / hacia el dispositivo 1 para la gestión de procedimientos.

El dispositivo 1 también comprende un procesador 12 (en inglés "Central Processing Unit", CPU) configurado para procesar instrucciones que constituyen el programa de ordenador para operar el dispositivo 1.

- 30 El dispositivo 1 también comprende una memoria 13 configurada para almacenar las instrucciones que componen el programa operativo de ordenador, así como información diversa.

El dispositivo 1 también comprende una interfaz de comunicación por cable o inalámbrica 14, en particular con un servidor remoto configurado para almacenar datos del dispositivo 1.

Finalmente, el dispositivo 1 puede comprender una fuente de energía, tal como una batería (no mostrada), o estar conectado directamente a una red eléctrica.

Según la invención, el dispositivo 1 comprende además al menos un sistema de seguridad. El sistema de seguridad comprende un elemento de control 20 montado en el dispositivo 1.

Como se ilustra en la Fig. 1, el elemento de control 20 está ventajosamente montado en la cara posterior 1b del dispositivo 1.

- 40 El elemento de control 20 puede ser operado por un operario.

Según una realización, el elemento de control 20 puede ser accionado manualmente por el operario.

A tal fin, el elemento de control 20 puede comprender una ranura que permita utilizar un elemento de tipo destornillador plano para hacer girar un selector 21. No obstante, son posibles otros tipos de accionamiento manual, mediante una llave, una manivela o cualquier otra herramienta conocida per se, específica o no. Además, son posibles otros tipos de elementos de control 20, como un pomo pivotante u otros.

Según otra realización, el elemento de control 20 puede ser accionado sin contacto por el operario. Ventajosamente, el accionamiento se realiza a corta distancia.

Por "corto alcance" se entiende en particular un accionamiento por comunicación inalámbrica con el dispositivo 1 realizado, por ejemplo, a una distancia inferior a 1 metro, o incluso ventajosamente a una distancia inferior a 10 centímetros. Esta comunicación de corto alcance puede utilizar, por ejemplo, la tecnología de comunicación en campo cercano (en inglés "Near Field Communication"; NFC).

- 5 Dicha comunicación de corto alcance es ventajosamente segura en términos de autenticación, integridad y confidencialidad de la información.

Así, el elemento de control 20 es operable entre al menos una primera posición y una segunda posición.

- 10 En la primera posición (ilustrada por la posición A en la Fig. 4), el dispositivo 1 se encuentra en un estado de alta seguridad. En particular, el dispositivo 1 requiere una configuración de seguridad antes de poder ser utilizado. Una configuración de este tipo permite implementar funciones de protección, en particular funciones de software, conocidas per se, como la encriptación de datos, un cortafuegos, el control de acceso, el diagnóstico de protección, las actualizaciones y otras.

A modo de ejemplo, el dispositivo 1 no puede establecer la comunicación hasta que se haya configurado el estado de seguridad. Una vez en estado seguro, las comunicaciones están autenticadas y protegidas.

- 15 En la segunda posición (ilustrada por la posición B en la Fig. 4), el dispositivo 1 se encuentra en un estado de seguridad baja.

- 20 Por "estados de seguridad alto / bajo" se entiende que los estados de seguridad se entienden relativos entre sí. Así, el estado de baja seguridad puede corresponder a un estado estándar, en el que el dispositivo 1 no requiere ninguna configuración de seguridad, o incluye funciones de protección relativamente menos importantes que las proporcionadas en el estado de alta seguridad.

Según una realización, el elemento de control 20 puede accionarse adicionalmente en otra u otras posiciones correspondientes a otros estados de seguridad del dispositivo 1, no descritos en lo que sigue.

De acuerdo con la realización ilustrada en la Fig. 4, el elemento de control 20 también puede accionarse en una tercera posición.

- 25 En la tercera posición (ilustrada por la posición C en la Fig. 4), el dispositivo 1 se encuentra en un estado de restablecimiento. Más concretamente, el aparato 1 vuelve a su estado inicial, en particular a su estado al salir de fábrica. La configuración de seguridad y algunas o todas las funciones de protección que puedan haber sido implementadas por el dispositivo 1 se eliminan, en particular se borran de la memoria 13 del dispositivo 1.

- 30 El dispositivo 1 comprende ventajosamente una salida dedicada que permite al operario conocer el estado de seguridad del dispositivo 1, por ejemplo mediante una torre de señalización o una columna luminosa montada en el armario eléctrico que comprende el dispositivo 1 o mediante una aplicación informática destinada al operario.

El dispositivo 1 puede comprender también un indicador que permita a un operario conocer en particular el estado de seguridad del dispositivo 1. El indicador está dispuesto en la cara frontal 1a del dispositivo 1, como se muestra en la Fig. 1.

- 35 Según una realización, el indicador comprende una o más luces indicadoras 15 para mostrar el estado de seguridad, diagnóstico y/o funcionamiento del dispositivo 1. En particular, la visualización del indicador o indicadores 15 puede ser comparada por el operario con la posición del sistema de seguridad para garantizar la integridad del dispositivo 1.

A continuación se describe un procedimiento de funcionamiento, y más particularmente de instalación, del sistema de seguridad del dispositivo 1, en relación con la Fig. 5.

- 40 Inicialmente, el elemento de control 20 está en una de las primeras, segundas o terceras posiciones A, B, C, correspondientes respectivamente al dispositivo 1 en el estado de alta seguridad, el estado de baja seguridad o el estado de restablecimiento.

Si el elemento de control 20 se encuentra inicialmente en la primera posición, una etapa del procedimiento consiste en comprobar si ya se ha configurado una seguridad en el dispositivo 1.

- 45 Si ya se ha implementado la configuración, se puede utilizar el dispositivo 1.

- 50 En el caso de que la seguridad aún no esté configurada en el dispositivo 1, el procedimiento comprende una o más etapas de configuración adicionales. Durante estas etapas de configuración, los datos de seguridad CS_conf pueden ser descargados por el dispositivo 1, en particular mediante la interfaz de comunicación 14. La descarga se realiza, por ejemplo, mediante comunicación Ethernet o USB desde una aplicación de configuración específica almacenada en un servidor remoto o un servidor web interno.

Alternativamente, los datos de seguridad CS_conf pueden estar ya almacenados en la memoria 13 del dispositivo 1.

La seguridad se configura mediante un programa informático ventajosamente ya presente en el dispositivo 1. Una vez finalizada la configuración, la seguridad está implementada y el dispositivo 1 puede utilizarse.

Si el elemento de control 20 se encuentra inicialmente en la segunda posición, el dispositivo 1 puede utilizarse sin requerir ninguna configuración de seguridad especial del dispositivo 1.

- 5 Si el elemento de control 20 está inicialmente en la tercera posición, el elemento de control 20 debe accionarse a una de las otras posiciones antes de cualquier uso para que el dispositivo 1 esté en el estado de seguridad alto o bajo. A continuación, pueden aplicarse las fases del procedimiento descritas anteriormente.

En uso, el dispositivo 1 se fija al soporte 2. La cara posterior 1b del dispositivo 1 ya no es directamente accesible para el operario.

- 10 Además, el accionamiento del elemento de control 20 está ventajosamente desactivado cuando el dispositivo 1 está en uso, en particular conectado a la fuente de alimentación.

De este modo se evita que el elemento de control 20 pueda ser accionado fácilmente para modificar el estado de seguridad del aparato 1 después de que éste haya sido conectado.

- 15 Así, si se desea pasar del estado de alta seguridad al estado de baja seguridad, o viceversa, es necesario desconectar primero el dispositivo 1 de la fuente de alimentación y/o separar el dispositivo 1 del soporte 2 de manera que la cara posterior 1b del dispositivo 1 sea de nuevo accesible.

En caso de accionamiento no permitido del elemento de control 20, el sistema de seguridad puede comprender una alarma (no ilustrada), por ejemplo visual o audible, para advertir al operario.

- 20 Según una realización, para cambiar de un estado de alta seguridad a un estado de baja seguridad, o viceversa, es necesario previamente accionar el elemento de control 20 en la tercera posición.

Así, la configuración de seguridad se borra necesariamente antes de que el dispositivo 1 pueda entrar en el otro estado de seguridad. De este modo, se garantiza que ninguna información relativa a la configuración del dispositivo 1 pueda almacenarse en el estado de baja seguridad, que es potencialmente más vulnerable a los ciberataques.

- 25 Obviamente, la invención no se limita a las realizaciones descritas anteriormente y proporcionadas únicamente a modo de ejemplo. Abarca diversas modificaciones, formas alternativas y otras variantes que puede considerar el experto en la materia en el contexto de la presente invención, y en particular cualquier combinación de los diversos modos de funcionamiento descritos anteriormente, que pueden tomarse por separado o combinados.

REIVINDICACIONES

- 5 1. Sistema de seguridad montado en un dispositivo (1) que forma parte de un autómata industrial programable y que comprende una cara frontal (1a) y una cara posterior (1b), estando el sistema de seguridad montado en la cara posterior (1b), estando la cara posterior (1b) configurada para estar dispuesta en contacto con un soporte (2) cuando el dispositivo está en uso, comprendiendo el sistema de seguridad un elemento de control (20) que puede ser accionado por un operario al menos:
- en una primera posición, en la que el dispositivo (1) está configurado para estar en un estado de alta seguridad, y
 - en una segunda posición, en la que el dispositivo (1) está configurado para estar en un estado de baja seguridad,
- 10 en el que la cara posterior (1b) del dispositivo (1) no es directamente accesible al operario cuando la cara posterior (1b) está en contacto con el soporte (2).
2. Sistema de seguridad según la reivindicación 1, en el que el estado de alta seguridad comprende una configuración de funciones de protección de software del dispositivo (1).
- 15 3. Sistema de seguridad según la reivindicación 1 ó 2, en el que el elemento de control (20) puede ser accionado manualmente por un operario.
4. Sistema de seguridad según la reivindicación 3, en el que el elemento de control (20) comprende una ranura que permite hacer pivotar un selector (21) entre al menos la primera posición y la segunda posición.
5. Sistema de seguridad según la reivindicación 1 ó 2, en el que el elemento de control (20) es accionable por un operario mediante comunicación inalámbrica de corto alcance con el dispositivo (1).
- 20 6. Sistema de seguridad según una cualquiera de las reivindicaciones precedentes, en el que el elemento de control (20) también es accionable en una tercera posición, en la que el dispositivo (1) se encuentra en un estado de restablecimiento.
7. Dispositivo (1) que comprende el sistema de seguridad según una cualquiera de las reivindicaciones precedentes.
- 25 8. Procedimiento de funcionamiento del sistema de seguridad según una cualquiera de las reivindicaciones 1 a 6, que comprende las siguientes etapas:
- si el elemento de control (20) está en la primera posición :
 - comprobar si ya se ha configurado la seguridad del dispositivo (1), y
 - en caso contrario, descargar los datos de configuración específicos del dispositivo (1) y configurar el estado de alta seguridad del dispositivo (1) antes de su uso.
- 30 9. Procedimiento según la reivindicación 8 para hacer funcionar el sistema de seguridad según la reivindicación 6, que comprende las siguientes etapas:
- si el elemento de control (20) está en la tercera posición :
 - accionar el elemento de control (20) en la primera o en la segunda posición.
- 35 10. Procedimiento según la reivindicación 9, en el que el accionamiento del elemento de control (20) entre la primera posición y la segunda posición requiere un paso intermedio a la tercera posición.
11. Programa de ordenador que comprende instrucciones para implementar el procedimiento según una de las reivindicaciones 8 a 10 cuando este programa es ejecutado por un ordenador.
12. Medio de grabación no transitorio legible por ordenador en el que está grabado un programa para implementar el procedimiento según una de las reivindicaciones 8 a 10 cuando dicho programa es ejecutado por un ordenador.

[Fig. 1]

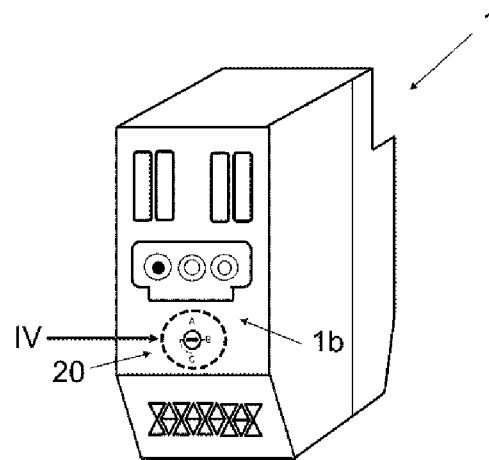


FIG. 1

[Fig. 2]

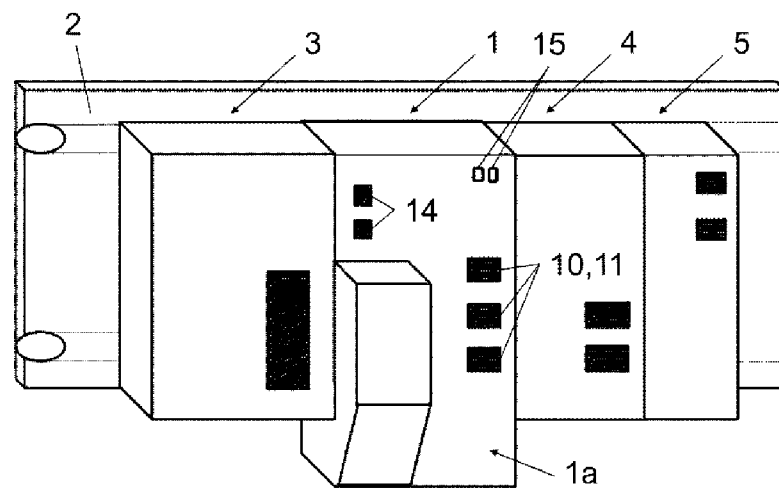


FIG. 2

[Fig. 3]

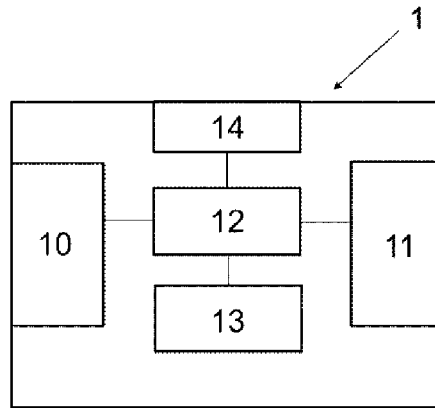


FIG. 3

[Fig. 4]

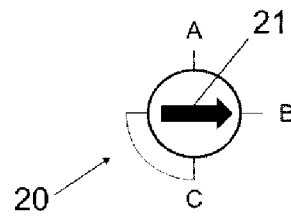


FIG. 4

[Fig. 5]

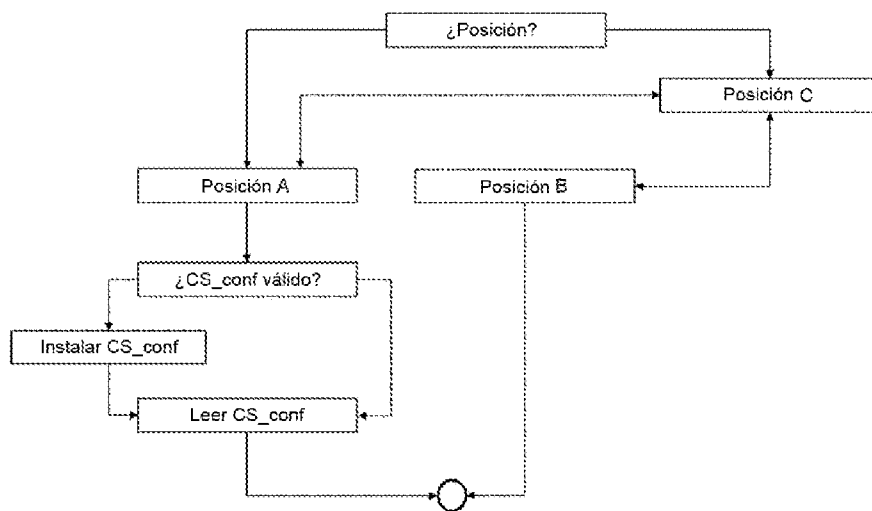


FIG. 5