(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 450 469**

(51) Int. CI.:

H04L 12/40 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **08.04.2011 E 11161630 (6)**

(97) Fecha y número de publicación de la concesión europea: **04.12.2013 EP 2509265**

(54) Título: **Dispositivo de protección de acceso para una red de automatización**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.03.2014

(73) Titular/es:

SIEMENS AKTIENGESELLSCHAFT (100.0%)
Wittelsbacherplatz 2
80333 München, DE

(72) Inventor/es:

GERLACH, HENDRIK y
SCHMID, WOLFGANG

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Dispositivo de protección de acceso para una red de automatización

La presente invención hace referencia a un dispositivo de protección de acceso para una red de automatización, en particular a un dispositivo de protección de acceso para una red de automatización que se encuentra conectada a una instalación de automatización.

Por la solicitud WO 2005/047991 A2 se conoce un método para el mantenimiento de dispositivos de campo, donde un ordenador de mantenimiento de un fabricante de dispositivos se encuentra dispuesto en una red de la empresa del fabricante de dispositivos de campo. El ordenador de mantenimiento se encuentra conectado a un dispositivo de campo mediante la red de la empresa, una red pública y una red del cliente. La red de la empresa y la red del cliente se encuentran aseguradas respectivamente por un ordenador Firewall con respecto a la red pública. En la red pública se proporciona un ordenador del servidor de directorio, donde se registran una unidad del cliente y el ordenador de mantenimiento. Además, el ordenador del servidor de directorio otorga un número de identificación de sesión en caso de una petición del cliente y selecciona una dirección de red de un servidor de retransmisión que se encuentra conectado a la red pública. Este número de identificación de sesión se reenvía a la unidad del cliente y al ordenador de mantenimiento. Mediante el servidor de retransmisión, a través del número de identificación de sesión, es posible una conexión par a par (peer-to-peer) para intercambiar información de los dispositivos de campo entre la unidad del cliente y el ordenador de mantenimiento.

En la solicitud EP 1 283 632 A2 se describe un método para transmitir datos, donde en base a una web del cliente se envía una petición de llamada para establecer un canal de transmisión en un servidor web. A partir de un sistema a ser operado u observado se envía una petición de llamada para establecer un primer canal de transmisión en el servidor web. Esta petición permanece abierta, de manera que entre el sistema y el servidor web se genera un túnel de transferencia de datos. Al tener lugar la petición de llamada del cliente web, entre el cliente web y el servidor web se crea al menos otro canal de transmisión. El cliente web, para enviar y recibir datos útiles de forma bidireccional mediante el túnel de transferencia de datos, establece contacto con el sistema a ser operado u observado.

En la actualidad, los dispositivos de automatización se encuentran interconectados cada vez más a través de ethernet. Con ello, también el tema relativo a la seguridad de la red cobra una mayor importancia. La protección de áreas delimitables a través de dispositivos de seguridad en los límites se encuentra actualmente en el estado del arte. En la tecnología de automatización esto se conoce como concepto celular. Los dispositivos de seguridad típicos son los firewalls (cortafuegos). Éstos realizan el seguimiento del desarrollo del protocolo y, junto a las direcciones fuente y de destino, así como junto a otros parámetros importantes del protocolo, verifican también el estado del protocolo. Los firewalls de esta clase se denominan también por eso Stateful Packet Inspection Firewalls (cortafuegos de inspección de paquetes).

A este respecto, es objeto de la presente invención crear un dispositivo de protección de acceso mejorado para una red de automatización, un método mejorado para operar un dispositivo de protección de acceso y un medio de almacenamiento digital mejorado para un dispositivo de protección de acceso.

El objeto de la invención se alcanzará a través de las reivindicaciones independientes. En las reivindicaciones dependientes se indican formas de ejecución de la presente invención.

La invención hace referencia a un dispositivo de protección de acceso para una red de automatización que se encuentra conectada a una instalación de automatización que está diseñada para un proceso de automatización. Como un proceso de automatización se entiende por ejemplo un proceso de fabricación o de producción automatizado. Éstos, así como otros procesos automatizados se denominan aquí como procesos de automatización.

Una red de automatización, por ejemplo, puede estar diseñada como una red industrial de automatización. Las redes industriales de automatización de esta clase, a modo de ejemplo, pueden estar diseñadas, configuradas y/o previstas para controlar y/o regular instalaciones industriales de automatización (por ejemplo instalaciones de producción, instalaciones de transporte, etc.). En particular, las redes de automatización, así como las redes industriales de automatización pueden presentar protocolos de comunicación en tiempo real (por ejemplo Profinet, Profibus, Real-Time-Ethernet) para la comunicación, al menos entre los componentes que participan en las tareas de control y/o de regulación (por ejemplo entre las unidades de control y las instalaciones y/o máquinas a ser controladas). Asimismo, a través de la red de automatización, los componentes para verificar y guiar el proceso de automatización pueden conectarse con los componentes de control y de regulación, así como conectarse unos con otros. Esto comprende también el manejo y observación directos de los componentes de control y de regulación. La transmisión segura de los datos se encuentra cubierta igualmente a través de medios de almacenamiento.

Asimismo, junto con un protocolo de comunicación en tiempo real, puede proporcionarse también al menos un protocolo de comunicación adicional (que no necesariamente debe operar en tiempo real) en la red de

automatización o en la red industrial de automatización, por ejemplo para controlar, configurar, reprogramar y/o reparametrizar una o varias unidades en la red de automatización. Debe tenerse en cuenta que en la red de automatización también puede tener lugar una comunicación que no se desarrolle en tiempo real. Una comunicación de esta clase tiene lugar mediante protocolos específicos de automatización.

Una red de automatización, por ejemplo, puede contener componentes de comunicación a través de conexiones y/o de componentes de conexión inalámbricos. Una red de automatización puede comprender además al menos un equipo de automatización.

Un equipo de automatización, a modo de ejemplo, puede consistir en un ordenador, PC y/o controlador (PLC) con tareas de control y/o de regulación, así como con capacidades de control y/o de regulación. En particular, un equipo de automatización puede consistir, a modo de ejemplo, en un equipo industrial de automatización que por ejemplo se encuentra especialmente diseñado, configurado y/o previsto para controlar y/o regular instalaciones industriales. En particular, los equipos de automatización de esta clase, así como los equipos industriales de automatización, pueden operar en tiempo real, es decir que posibilitan un control o una regulación en tiempo real. Para ello, el equipo de automatización o el equipo industrial de automatización puede comprender por ejemplo un sistema operativo en tiempo real y/o al menos, entre otros, ser respaldado por un protocolo de comunicación en tiempo real para la comunicación (por ejemplo Profinet, Profibus, Real-Time- Ethernet).

Una instalación de automatización conectada a la red de automatización comprende uno o varios sensores y actuadores. Los actuadores son controlados al menos por un dispositivo de control. Los valores de medición de los sensores pueden ser registrados y procesados por el dispositivo de control o por otros dispositivos de red. En particular, los valores de medición pueden ser registrados y procesados también a través de un dispositivo de protección de acceso según las formas de ejecución de la invención. Los actuadores, los sensores y al menos un dispositivo de control intercambian datos unos con otros. Para el intercambio de datos se utiliza un protocolo de automatización. Al menos un dispositivo de control controla los actuadores, los sensores y el intercambio de datos de manera que se desarrolla un proceso mediante maquinaria, en el cual por ejemplo se fabrica un producto.

Además, para la interconexión de sensores pueden utilizarse también conexiones que no emplean un protocolo de automatización. Por ejemplo, los valores de medición de un sensor pueden transmitirse también mediante líneas alámbricas en dispositivos de red y/o mediante un dispositivo de protección de acceso según las formas de ejecución de la invención.

Un dispositivo industrial de automatización, por ejemplo, puede contener un controlador programable de almacenamiento, un módulo o parte de un controlador programable de almacenamiento, un controlador programable de almacenamiento integrado a un ordenador o a un PC, así como dispositivos de campo apropiados, sensores y/o actuadores, dispositivos de entrada y/o de salida o similares para la conexión a un controlador programable de almacenamiento o similares. Un controlador programable de almacenamiento integrado a un ordenador o PC puede consistir particularmente en un controlador implementado por software. En ese caso no se presentan por tanto componentes del hardware, los cuales se encargan exclusivamente del funcionamiento del controlador programable de almacenamiento. Un controlador implementado por software, a modo de ejemplo, puede desarrollarse en un procesador del ordenador o del PC, el cual también se utiliza para otras funciones del ordenador o del PC.

Dentro del marco de la presente invención se entiende como protocolo de automatización cualquier clase de protocolo que se encuentra previsto, adaptado y/o configurado para la comunicación con equipos de automatización, conforme a la presente descripción. Los protocolos de automatización de esta clase, por ejemplo, pueden consistir en el protocolo de Profi-bus (por ejemplo conforme a IEC 61158/EN50170), un protocolo DP de Profi-bus, un protocolo PA de Profi-bus, un protocolo Profi-Net, un protocolo I0 Profi-Net, un protocolo conforme a la interfaz AS, un protocolo conforme a IOLink, un protocolo KNX, un protocolo conforme a una interfaz multipunto (Multipoint-Interface, MPI), un protocolo para un acoplamiento punto a punto (Point-to-Point, PtP), un protocolo conforme a las especificaciones de la comunicación S7 (la cual por ejemplo se encuentra prevista y configurada por la empresa Siemens para la comunicación de controladores programables de almacenamiento) o también un protocolo ethernet industrial o protocolo en tiempo real, así como otros protocolos específicos para la comunicación con equipos de automatización, como por ejemplo Modbus, FFB u otros. Dentro del marco de la presente descripción, como protocolo de automatización puede preverse también cualquier combinación deseada de los protocolos mencionados.

El proceso de automatización puede desarrollarse al menos en dos estados. A modo de ejemplo, el primer estado corresponde al estado normal de funcionamiento del proceso de automatización y el segundo estado corresponde a un estado que no es el estado normal de funcionamiento. Por ejemplo, esto puede depender de si uno o varios dispositivos de la instalación de automatización no están funcionando o determinados parámetros de medición no corresponden a los valores deseados. A modo de ejemplo, éste puede ser el caso, cuando el proceso es perturbado o interrumpido debido al defeco de un componente vinculado a la tecnología del procedimiento, el cual por ejemplo es controlado por la red de automatización, y ejecuta el proceso de producción o de fabricación.

Entre las redes de automatización figuran también dispositivos que se encuentran separados localmente de una parte principal de la red de automatización, pero que se encuentran conectados a la red de automatización mediante una conexión segura. Una conexión segura de esta clase puede ser por ejemplo un túnel VPN.

El dispositivo de protección de acceso comprende un medio de almacenamiento digital, medios del procesador y conexiones de red. El medio de almacenamiento digital se encuentra diseñado para almacenar al menos primeras y segundas reglas. Los medios del procesador, por ejemplo, pueden comprenden uno o varios procesadores que ejecutan instrucciones de programa. Los medios del procesador se encuentran diseñados para leer al menos primeras y segundas reglas, para procesar al menos primeras y segundas reglas y para recibir y reenviar datos mediante las conexiones de red. Por tanto, mediante las conexiones de red pueden recibirse datos de la red de automatización y/o de la instalación de automatización a través del dispositivo de protección de acceso y también pueden reenviarse datos desde el dispositivo de protección de acceso a la red de automatización. De este modo, el dispositivo de protección de acceso puede estar conectado sólo a la red de automatización o tanto a la red de automatización como también a la instalación de automatización, en particular a sus sensores.

Las primeras reglas, en un primer estado del proceso de automatización, definen qué datos recibidos se reenvían y qué datos recibidos no se reenvían. La decisión sobre el reenvío de los datos puede efectuarse por ejemplo con respecto al emisor y al receptor de los datos, o también con respecto a la clase de datos. Por consiguiente, las reglas definen los derechos de acceso de dispositivos dentro o fuera de la red de automatización y/o de la instalación de automatización a otros dispositivos de la red de automatización y/o de la instalación de automatización. El primer estado, por ejemplo, puede ser el estado normal de funcionamiento de la instalación de automatización. Esto significa que el proceso de automatización se desarrolla del modo previsto.

Además, los medios del procesador se encuentran diseñados para recibir al menos una señal. Al menos una señal puede comprender una indicación con respecto a la modificación del estado del proceso de automatización, Una modificación del estado puede presentarse por ejemplo cuando el proceso de automatización ya no se desarrolla del modo previsto. Puede tratarse también por ejemplo de estados de la instalación o del proceso que se presentan de forma recurrente, por ejemplo la puesta en funcionamiento, mantenimiento, diagnóstico, avería, en caso de emergencia o un estado crítico de un valor de medición, como por ejemplo la temperatura, presión, velocidad de flujo, el nivel de líquido o la detención de un dispositivo de la instalación de automatización.

Al menos una señal, por ejemplo, puede comprender directamente la indicación sobre la modificación del estado. De forma alternativa, la señal puede comprender también varios valores de medición que entonces pueden ser analizados por los medios del procesador, de manera que los propios medios del procesador determinan si se encuentra presente una modificación del estado del proceso de automatización. Después de recibir al menos una señal, las segundas reglas definen qué datos recibidos se reenvían y qué datos recibidos no se reenvían. Por tanto, las segundas reglas, del mismo modo que las primeras reglas, comprenden derechos de acceso, donde sin embargo las segundas reglas se diferencian de las primeras reglas.

Por ejemplo, las segundas reglas pueden definir derechos de acceso de una clase determinada, de manera que la eliminación de una falla, una puesta en funcionamiento, un mantenimiento, un diagnóstico o el análisis de un problema pueden ser efectuados por un usuario mediante un dispositivo de la red de automatización, lo cual no es posible según los derechos de acceso de las primeras reglas.

De forma alternativa, las segundas reglas pueden definir derechos de acceso de manera que se impida un acceso a una instalación de automatización desde un dispositivo de la red de automatización para que un proceso químico o de otra clase pueda continuar sin problemas dentro de la instalación de automatización.

De acuerdo con las formas de ejecución de la invención, los medios del procesador se encuentran diseñados para recibir al menos una señal mediante al menos una de las conexiones de red. Expresado de otro modo, la señal puede ser recibida por ejemplo directamente por la instalación de automatización, por ejemplo por un sensor, o por un dispositivo de la red de automatización.

De acuerdo con las formas de ejecución de la invención, el dispositivo de protección de acceso comprende una conexión para recibir al menos una señal. Al menos una señal comprende al menos un parámetro de medición del proceso de automatización, donde dicho parámetro fue medido por un sensor de la instalación de automatización.

De acuerdo con las formas de ejecución de la invención, los medios del procesador se encuentran diseñados para comparar al menos un parámetro de medición con un valor umbral. El parámetro de medición puede haber sido medido por ejemplo por un sensor de la instalación de automatización, y referirse al nivel de un líquido, a una velocidad de flujo, a presión o a temperatura. Los medios del procesador comparan al menos un parámetro de medición con al menos un valor umbral. En el caso de una pluralidad de parámetros de medición, la pluralidad de parámetros de medición es comparada también con una pluralidad de valores umbral. Un valor de medición siempre es comparado con el valor umbral correspondiente. Por ejemplo, esto significa que un valor de presión siempre es

comparado con el valor umbral para ese valor de presión. También es posible la comparación de una pluralidad de valores de medición de la misma clase con una pluralidad de valores umbral de la misma clase. Por ejemplo, una pluralidad de valores de temperatura puede ser comparada con una pluralidad de valores umbral para esos valores de temperatura. De este modo, el valor de temperatura A se compararía con el valor umbral A, el valor de temperatura B con el valor umbral B, etc.

La comparación es realizada por los medios del procesador a través de una operación de cálculo. Las operaciones de cálculo pueden comprender por ejemplo una conversión a escala o una linealización. Los medios del procesador detectan la modificación del estado del proceso de automatización cuando al menos un parámetro de medición sobrepasa al menos un valor umbral o se ubica por debajo del mismo. De este modo, una modificación del estado del proceso de automatización es detectado por los medios del procesador. Conforme a esa modificación del estado, las primeras reglas ya no son aplicadas por los medios del procesador, sino las segundas reglas. El segundo estado puede consistir por ejemplo en un estado de emergencia o en un estado de mantenimiento.

De acuerdo con las formas de ejecución de la invención, los medios del procesador se encuentran diseñados para recibir una pluralidad de señales y/o al menos una señal comprende una pluralidad de parámetros de medición. Los medios del procesador se encuentran diseñados para detectar una modificación del estado del proceso de automatización empleando operaciones de cálculo sobre la pluralidad de parámetros de medición. Estas operaciones de cálculo pueden comprender por ejemplo una conversión a escala o una linealización. También es posible que, durante la recepción de la pluralidad de parámetros de medición, sólo una parte de estos parámetros de medición deban sobrepasar o ubicarse por debajo de los respectivos valores umbral. A modo de ejemplo, los medios del procesador pueden encontrarse diseñados de manera que una modificación del estado del proceso de automatización sea detectada cuando dos de tres parámetros de medición sobrepasen o se ubiquen por debajo de los respectivos valores umbral.

De acuerdo con las formas de ejecución de la invención, las primeras y las segundas reglas definen derechos de acceso en función de un emisor y de un receptor de los datos. De forma adicional puede considerarse también la clase de datos.

De acuerdo con las formas de ejecución de la invención, las primeras reglas se encuentran reunidas al menos en un primer grupo de reglas y las segundas reglas en al menos un segundo grupo de reglas. El hecho de reunir las reglas en grupos de reglas mejora la visibilidad para el usuario. Por ejemplo, puede estar presente un grupo de reglas, conforme al cual se bloqueen todos los accesos a los dispositivos de red de la red de automatización. Por ejemplo, éste podría ser el primer grupo de reglas. El segundo grupo de reglas, en el caso de una falla, podría admitir el acceso de una estación de control de emergencia de la red de automatización a un servidor de la red de automatización.

De acuerdo con las formas de ejecución de la invención, el primer estado de automatización es un estado de funcionamiento y el segundo estado un estado de emergencia. Las segundas reglas permiten un acceso a todos los dispositivos de red de la red de automatización desde un dispositivo de red de control de emergencia. En el caso de un estado de emergencia, esto permite al usuario tomar medidas rápidamente para poner fin al estado de emergencia. Esto sucede de forma automática debido a que los medios del procesador reciben la primera señal. De este modo, el usuario no debe permitir manualmente el acceso a través del dispositivo de red de control de emergencia. Esto posibilita una intervención rápida en el caso de un estado de emergencia del proceso de automatización.

De acuerdo con las formas de ejecución de la invención, el primer estado de automatización es un estado de funcionamiento y el segundo estado un estado de emergencia. Las segundas reglas permiten un acceso a todos los dispositivos de red de la red de automatización desde cualquier dispositivo de red de la red de automatización. En este caso, un usuario de cualquier dispositivo de red de la red de automatización puede remediar el estado de emergencia sin que los derechos de acceso deban ser modificados de forma manual.

La utilización de las segundas reglas en lugar de las primeras reglas puede denominarse también como una modificación de la red de automatización. Las primeras reglas definen un primer estado de la red de automatización y las segundas reglas definen un segundo estado de la red de automatización. Debido a que una conmutación del estado de la red de automatización se activa de forma automática a través de la modificación del estado del proceso de automatización, el estado de la red de automatización sigue siempre al estado del proceso de automatización, sin que deba modificarse manualmente el estado de protocolo de la red de automatización. Esto se considera ventajoso para poder reaccionar de forma rápida frente a estados del proceso cambiantes del proceso de automatización.

En cuanto a otro aspecto, la presente invención hace referencia a un sistema de automatización con una instalación de automatización y una red de automatización. En cuanto a otro aspecto adicional, la invención hace referencia a un método para operar un dispositivo de protección de acceso en una red de automatización que se encuentra conectada a una instalación de automatización, la cual está diseñada para ejecutar un proceso de automatización. El método comprende los siguientes pasos.

En primer lugar, el proceso de automatización se ejecuta en un primer estado. En este caso, las primeras reglas son leídas desde un medio de almacenamiento del dispositivo de protección de acceso a través de medios del procesador del dispositivo de protección de acceso. Las primeras reglas definen derechos de acceso para un acceso desde una primera subred de la red de automatización hacia una segunda subred de la red de automatización. Al aplicar las primeras reglas a través de los medios del procesador, las primeras reglas definen qué datos se reenvían y que datos no se reenvían. Esto puede depender de la clase de datos, del emisor de los datos y del receptor de los datos.

En el caso de que se modifique el estado del proceso de automatización, los medios del procesador del dispositivo de protección de acceso reciben al menos una señal que comprende una indicación sobre la modificación del estado del proceso de automatización. En este caso, los medios del procesador leen las segundas reglas desde el medio de almacenamiento y las aplican. Las segundas reglas definen qué datos recibidos se reenvían y qué datos recibidos no se reenvían. Por consiguiente, las segundas reglas también definen derechos de acceso, pero que son diferentes con respecto a las primeras reglas.

De acuerdo con las formas de ejecución de la invención, al menos una señal comprende al menos un parámetro de medición del proceso de automatización, donde dicho parámetro fue medido por un sensor de la instalación de automatización Al recibir la señal, los medios del procesador comparan al menos un parámetro de medición con al menos un valor umbral correspondiente. Los medios del procesador detectan una modificación del estado del proceso de automatización cuando el parámetro de medición sobrepasa al menos un valor umbral o se ubica por debajo del mismo.

De acuerdo con las formas de ejecución de la invención, las primeras y las segundas reglas definen derechos de acceso en función de un emisor y de un receptor de los datos. También la clase de datos puede definir derechos de acceso. Como clase de datos se entienden aquí en particular por ejemplo datos de automatización o también datos de diferentes subprotocolos de automatización, datos de Internet, datos de video o datos de control.

De acuerdo con las formas de ejecución de la invención, las primeras reglas se encuentran reunidas al menos en un primer grupo de reglas y las segundas reglas en al menos un segundo grupo de reglas. Esto aumenta la visibilidad para el usuario.

En cuanto a otro aspecto adicional, la invención hace referencia a un medio de almacenamiento digital para un dispositivo de protección de acceso en una red de automatización que se encuentra conectada a una instalación de automatización, la cual está diseñada para ejecutar un proceso de automatización. El medio de almacenamiento digital comprende instrucciones de programa que inducen a que el dispositivo de protección de acceso ejecute un método acorde a los formas de ejecución de la invención.

A continuación se explican en detalle formas de ejecución de la invención mediante los dibujos. Las figuras muestran:

Figura 1: un dispositivo de protección de acceso para una red de automatización que se encuentra conectada a una red de automatización;

Figura 2: un diagrama de flujo de un método acorde a las formas de ejecución de la invención; y

Figura 3: una representación esquemática de dos estados de la red de automatización.

Los elementos de las siguientes figuras que se corresponden se encuentran indicados con los mismos símbolos de referencia.

La figura 1 consiste en un diagrama de bloques de un dispositivo de protección de acceso 104, donde se muestra una primera parte 100 de una red de automatización y de una instalación de automatización 102, en donde se encuentra una segunda parte 103 de la red de automatización. La primera subred de automatización 100 se encuentra conectada a la segunda subred de automatización 103 mediante el dispositivo de protección de acceso 104. Los datos que son enviados desde la primera subred de automatización 100 en los dispositivos de red hacia la segunda subred de automatización 103 son enviados a través del dispositivo de protección de acceso 104 que aplicando las reglas reenvía los datos o bloquea su reenvío. Los datos que son enviados desde la segunda subred de automatización 103 hacia la primera subred de automatización 100 son enviados a través del dispositivo de protección de acceso 104. El dispositivo de protección de acceso 104 aquí también aplica reglas para verificar derechos de acceso de diferentes dispositivos de la subred de automatización 103 sobre diferentes aparatos de la primera subred de automatización 100. También otras instalaciones de automatización 102 pueden estar conectadas a otras segundas subredes de automatización en la primera subred de automatización (lo cual aquí no se encuentra representado). Por ejemplo, en el estado de funcionamiento, los dispositivos de la primera subred de automatización 100 no pueden acceder o sólo pueden acceder de forma restringida a los dispositivos de la segunda subred de

automatización 103. Un acceso se encuentra prohibido o restringido a través del dispositivo de protección de acceso 104. Del mismo modo, en un estado normal de funcionamiento, a través del dispositivo de protección de acceso 104, puede prohibirse o restringirse un acceso de un dispositivo de la subred de automatización 103 a un dispositivo de la red de automatización 100.

El dispositivo de protección de acceso 104 comprende un procesador 106 y un medio de almacenamiento digital 108. El procesador 106 está diseñado para ejecutar instrucciones de programa que se encuentran almacenadas en el medio de almacenamiento digital 108. Debe tenerse en cuenta que las instrucciones de programa también pueden ser ejecutadas a través de varios procesadores del dispositivo de protección de acceso. El dispositivo de protección de acceso 104, mediante una conexión de red 110, recibe paquetes de datos a ser filtrados 112 que son procesados a través del procesador 106. A través de la ejecución de las instrucciones de programa en el medio de almacenamiento digital 108, se induce al procesador 106 a aplicar reglas que igualmente se encuentran almacenadas en el medio de almacenamiento digital 108. Las reglas pueden almacenarse también en otros medios de almacenamiento que no se encuentran representados aquí.

Según la decisión basada en el procesamiento de las reglas, el paquete de datos 112 a ser filtrado es enviado o no del lado de salida mediante la conexión de red 113. Por tanto, las reglas definen si una señal es reenviada o bloqueada. En el sentido opuesto, los paquetes de datos 112 a ser filtrados son recibidos mediante la conexión de red 113 y eventualmente enviados mediante la conexión de red 110. También aquí las reglas definen si una señal es reenviada o bloqueada.

Las reglas a ser aplicadas se orientan según el estado de proceso del proceso de automatización que se desarrolla en la instalación de automatización 102. En un primer estado del proceso, el procesador 106 aplica primeras reglas y en un segundo estado el procesador aplica segundas reglas.

Del mismo modo, el dispositivo de protección de acceso 104 se encuentra diseñado para recibir una primera señal 114 mediante una conexión 111. La primera señal 114 comprende una indicación sobre el estado del proceso de automatización que se desarrolla en la instalación de automatización 102. La conexión 111 puede consistir en una conexión de red adicional o en una conexión para otro enlace entre el dispositivo de protección de acceso y la instalación de automatización. Ésta puede consistir por ejemplo en un circuito de dos hilos o también en una conexión inalámbrica, como por ejemplo Funk o WLAN. Sin embargo, la conexión 111 puede también coincidir con la conexión 110, cuando la conexión 111 se encuentra diseñada también como una conexión de red o la señal 114 es transmitida mediante un protocolo de red. Asimismo, la señal 114 puede ser recibida a través de la conexión 113, mediante la cual el dispositivo de protección de acceso 104 se encuentra conectado a la segunda subred de automatización 103.

A modo de ejemplo, la señal 114 puede comprender uno o varios valores de medición que son registrados a través de un módulo de registro 116 por el dispositivo de protección de acceso 104. El registro puede tener lugar de forma alternativa también a través del procesador 106. Los valores de medición recibidos pueden entonces ser vinculados a través de un módulo de enlace 118. El enlace puede tener lugar de forma alternativa también a través del procesador 106. A través de la vinculación de los valores de medición, el procesador 106 puede ejecutar operaciones de cálculo, a través de las cuales puede detectar una modificación del proceso de automatización. Estas operaciones de cálculo pueden comprender por ejemplo una conversión a escala o una linealización. Como operación de cálculo puede entenderse también que los valores de medición son comparados con valores umbral correspondientes y que una modificación del estado se detecta en caso de que se sobrepasen los valores umbral o en caso de que los valores de medición se ubiquen por debajo de los mismos.

De manera alternativa, la señal 114 puede ser emitida también por otro dispositivo de la subred de automatización 103 en el dispositivo de protección de acceso 104 y, en ese caso, no comprender valores de medición sino directamente una indicación sobre una modificación de estado del estado del proceso.

Las reglas que definen los derechos de acceso pueden figurar de forma individual o estar reunidas en grupos.

Las reglas que figuran de forma individual pueden representarse en pseudocódigos, por ejemplo del siguiente modo:

pass inet proto tcp from <EmergencyConsole> to

<Server> **when PlantState equal Hardfault**

Esto significa que se permiten los accesos hacia el servidor mediante todos los protocolos TCP desde el dispositivo de red de control de emergencia cuando el proceso de automatización presenta fallos.

Otra regla posible en pseudocódigo podría representarse del siguiente modo:

drop inet proto tcp from <EmergencyConsole> to

<Server> **when PlantState not equal HardFault**

Esto significa que se permiten los accesos hacia el servidor mediante todos los protocolos TCP desde el dispositivo de red de control de emergencia cuando el proceso de automatización no presenta fallos.

La siguiente regla en pseudocódigo significa que se permite el acceso desde una consola sobre una unidad de control para una caldera, cuando la caldera ha alcanzado una temperatura crítica:

pass inet proto tcp from <Console> to <BoilerPLC>

when BoilerTemperature > CriticalLimit

Por ejemplo, los grupos de reglas pueden representarse del siguiente modo:

También puede diferenciarse entre diferentes clases de acceso. Por ejemplo, puede permitirse la lectura pero prohibirse la escritura. Otra clase de acceso consiste en la ejecución de instrucciones ejecutables de programa que puede permitirse o prohibirse de forma individual.

El dispositivo de protección de acceso 104 puede utilizarse también para controlar el acceso a la primera subred de automatización 100 ó a una subred en una instalación de automatización 102 desde otra subred (por ejemplo una red de oficina o la Internet). En este caso, el dispositivo de protección de acceso 104, mediante la conexión de red 110, y la primera subred de automatización 100, se encuentran conectadas a la otra red. Aquí el dispositivo de protección de acceso puede utilizarse también para controlar accesos desde otra subred a dispositivos de la subred de automatización 103. Los accesos de esta clase pueden tener lugar mediante el dispositivo de protección de acceso 104, a través de la subred de automatización 100, hacia la subred de automatización 103.

También pueden utilizarse dos o varios dispositivos de protección de acceso 104 cuando la subred de automatización se compone por ejemplo de dos o más subredes que se encuentran conectadas unas a otras vía Internet. A modo de ejemplo, en una subred puede localizarse una sala de control que accede a una segunda subred - por ejemplo a una o a varias estaciones de bombeo - mediante Internet, y que puede controlarlas. Los accesos a la primera subred y a la segunda subred, así como los accesos desde la primera y la segunda subred pueden controlarse de este modo mediante los respectivos dispositivos de protección de acceso.

La figura 2 muestra un diagrama de flujo de un método para operar un dispositivo de protección de acceso en una red de automatización, el cual puede ser ejecutado por un procesador del dispositivo de protección de acceso a través de la ejecución de instrucciones de programa en un medio de almacenamiento digital del dispositivo de protección de acceso. La red de automatización se representa como en la figura 1, conectada a una instalación de automatización que está diseñada para ejecutar un proceso de automatización.

El proceso de automatización puede encontrarse en un primer o en un segundo estado.

En un primer paso S1, el proceso de automatización se encuentra en un primer estado. El primer estado, por ejemplo, puede ser el estado normal de funcionamiento del proceso de automatización. En el caso de un proceso de fabricación o de producción, éste puede ser el funcionamiento normal de la instalación de automatización. En un segundo paso S2, primeras reglas son leídas por el procesador del dispositivo de protección de acceso desde el medio de almacenamiento del dispositivo de protección de acceso. Los datos se reenvían aplicando las primeras reglas en el paso S3 a través del dispositivo de protección de acceso. Las primeras reglas definen qué datos se reenvían y qué datos no se reenvían. Esto puede tener lugar por ejemplo en función del emisor, del receptor y de la clase de datos. Expresado de otro modo, las primeras reglas definen primeros derechos de acceso.

En el caso de que se modifique el estado del proceso de automatización, en el paso S4 se emite una señal en el dispositivo de protección de acceso. La señal comprende una indicación sobre una modificación de estado. Preferentemente, la señal es recibida y procesada por el procesador del dispositivo de protección de acceso. La señal puede comprender directamente la indicación sobre la modificación de estado o también valores de medición que son procesados a través del procesador. En este último caso, el propio procesador detecta la modificación de estado del proceso de automatización. Esto puede efectuarse por ejemplo mediante operaciones de cálculo como una linealización o una conversión a escala y/o a través de una simple comparación de los valores de medición con valores umbral correspondientes.

En el paso S5, después de la recepción de la señal, segundas reglas son leídas por el procesador desde el medio de almacenamiento, donde dichas reglas se aplican en el paso S6. Las segundas reglas definen qué datos recibidos se reenvían y qué datos recibidos no deben reenviarse. Las segundas reglas definen por tanto derechos de acceso

para el segundo estado del proceso de automatización. El segundo estado del proceso de automatización, por ejemplo, puede tratarse de un caso de avería o de emergencia, donde se permite el acceso a todos los dispositivos de la instalación de automatización y de la red de automatización por un dispositivo de red de control de emergencia.

De este modo es posible para el usuario eliminar rápidamente los estados de emergencia, mantenimiento o fallos del proceso de automatización sin una conversión de los derechos de acceso.

Debido a que el estado del protocolo de la red de automatización siempre se adapta al estado de proceso del proceso de automatización puede prescindirse de una conversión manual. El estado del protocolo de la red de automatización es definido a través de las primeras y las segundas reglas. Al aplicar las primeras reglas, la red de automatización se encuentra por ejemplo en un primer estado del protocolo, y al aplicar las segundas reglas, en un segundo estado del protocolo.

La figura 3 muestra una representación esquemática de dos estados 300 y 302. En el primer estado 300, al recibir un paquete de datos mediante la conexión 110 (véase la figura 1) del dispositivo de protección de acceso, las primeras reglas son leídas y aplicadas al paquete de datos. Los datos son reenviados o bloqueados de acuerdo con las reglas.

En el caso de que a través de la conexión 111 (véase la figura 1) se reciba una señal que comprende una indicación sobre una modificación de estado del proceso de automatización, el estado de la red de automatización se modifica en el segundo estado 302. En el segundo estado 302, los paquetes de datos que se reciben mediante la conexión 110 son reenviados o bloqueados de acuerdo con las segundas reglas.

En el caso de que se reciba otra señal mientras la red de automatización se encuentra en el segundo estado 302, donde dicha señal comprende una indicación sobre una modificación de estado del proceso de automatización, el estado de la red de automatización se modifica en el primer estado 300.

Lista de símbolos de referencia

100 subred de automatización

102 instalación de automatización

103 subred de automatización

104 dispositivo de protección de acceso

106 procesador

108 medio de almacenamiento digital

110 conexión de red

111 conexión

112 paquete de datos

113 conexión de red

114 señal

116 módulo de registro

118 módulo de enlace

300 estado 1

302 estado 2

REIVINDICACIONES

1. Dispositivo de protección de acceso (104) para una red de automatización (100) que se encuentra conectada a una instalación de automatización (102), la cual se encuentra diseñada para ejecutar un proceso de automatización, donde el proceso de automatización puede desarrollarse al menos en dos estados y el dispositivo de protección de acceso comprende

- un medio de almacenamiento digital (108),

- medios del procesador (106), y

- conexiones de red (110)

donde el medio de almacenamiento digital se encuentra diseñado para almacenar al menos primeras y segundas reglas, donde las segundas reglas se diferencian de las primeras reglas, donde los medios del procesador se encuentran diseñados para leer al menos las primeras y las segundas reglas, para procesar las reglas y para recibir y reenviar datos mediante las conexiones de red,

donde las primeras reglas, en un primer estado del proceso de automatización, definen qué datos recibidos se reenvían y qué datos recibidos no se reenvían,

donde los medios del procesador se encuentran diseñados para recibir al menos una señal (114) mediante una de las conexiones de red de la instalación de automatización,

donde al menos una señal comprende una indicación con respecto a la modificación del estado del proceso de automatización,

donde los medios del procesador se encuentran diseñados para detectar una modificación del estado a través de la evaluación de la señal, y

donde después de recibir al menos una señal, las segundas reglas definen qué datos recibidos se reenvían y qué datos recibidos no se reenvían.

2. Dispositivo de protección de acceso conforme a la reivindicación 1, donde el procesador se encuentra diseñado para recibir al menos una señal mediante al menos una de las conexiones de red.

3. Dispositivo de protección de acceso conforme a la reivindicación 1, donde el dispositivo de protección de acceso comprende una conexión para recibir al menos una señal, y donde al menos una señal comprende al menos un parámetro de medición del proceso de automatización que fue medido por un sensor de la instalación de automatización.

4. Dispositivo de protección de acceso conforme a la reivindicación 3, donde el procesador se encuentra diseñado para comparar al menos un parámetro de medición con un valor umbral, y donde el procesador se encuentra diseñado para detectar la modificación del estado cuando al menos un parámetro de medición sobrepasa al menos un valor umbral o se ubica por debajo del mismo.

5. Dispositivo de protección de acceso conforme a una de las reivindicaciones precedentes, donde el procesador se encuentra diseñado para recibir una pluralidad de señales, y/o donde al menos una señal comprende una pluralidad de parámetros de medición, y donde el procesador se encuentra diseñado para detectar una modificación del estado del proceso de automatización empleando operaciones de cálculo sobre la pluralidad de parámetros de medición.

6. Dispositivo de protección de acceso conforme a una de las reivindicaciones precedentes, donde las primeras y las segundas reglas definen derechos de acceso en función de un emisor y de un receptor de los datos.

7. Dispositivo de protección de acceso conforme a una de las reivindicaciones precedentes, donde las primeras reglas se encuentran reunidas al menos en un primer grupo de reglas y las segundas reglas en al menos un segundo grupo de reglas.

8. Dispositivo de protección de acceso conforme a una de las reivindicaciones precedentes, donde el primer estado del proceso de automatización consiste en un estado de funcionamiento y el segundo estado en un estado de emergencia, y donde las segundas reglas permiten un acceso a todos los dispositivos de red de la red de automatización desde un dispositivo de red de control de emergencia.

9. Dispositivo de protección de acceso conforme a una de las reivindicaciones 1-7, donde el primer estado del proceso de automatización consiste en un estado de funcionamiento y el segundo estado en un estado de emergencia, y donde las segundas reglas permiten un acceso a todos los dispositivos de red de la red de automatización desde cualquier dispositivo de red de la red de automatización.

10. Método para operar un dispositivo de protección de acceso en una red de automatización que se encuentra conectada a una instalación de automatización, la cual está diseñada para ejecutar un proceso de automatización, donde el método comprende los siguientes pasos:

- ejecución (S1) del proceso de automatización en un primer estado,

- lectura (S2) de primeras reglas desde un medio de almacenamiento del dispositivo de protección de acceso a través de un procesador del dispositivo de protección de acceso,

- reenvío (S3) de datos empleando las primeras reglas, donde las primeras reglas definen qué datos recibidos por el dispositivo de protección de acceso (104) se reenvían y qué datos

recibidos por el dispositivo de protección de acceso (104) no se reenvían,

- recepción (S4) de al menos una señal, donde al menos una señal comprende una indicación al respecto de una modificación del estado del proceso de automatización, donde el procesador detecta esa modificación del estado a través de la evaluación de la señal,

- lectura (S5) de segundas reglas desde el medio de almacenamiento, donde las segundas reglas se diferencian de las primeras reglas, y

- reenvío (S6) de datos empleando las segundas reglas, donde las segundas reglas definen qué datos recibidos por el dispositivo de protección de acceso (104) se reenvían y qué datos recibidos por el dispositivo de protección de acceso (104) no se reenvían.

11. Método conforme a la reivindicación 10, donde las primeras y las segundas reglas definen derechos de acceso en función de un emisor y de un receptor de los datos.

12. Método conforme a la reivindicación 10, donde las primeras reglas se encuentran reunidas al menos en un primer grupo de reglas y las segundas reglas en al menos un segundo grupo de reglas.

13. Programa de ordenador que proporciona instrucciones de programa que pueden ser ejecutadas por un ordenador, las cuales, al ser ejecutadas en un ordenador, provocan que el ordenador ejecute un método conforme a una de las reivindicaciones 10-12.

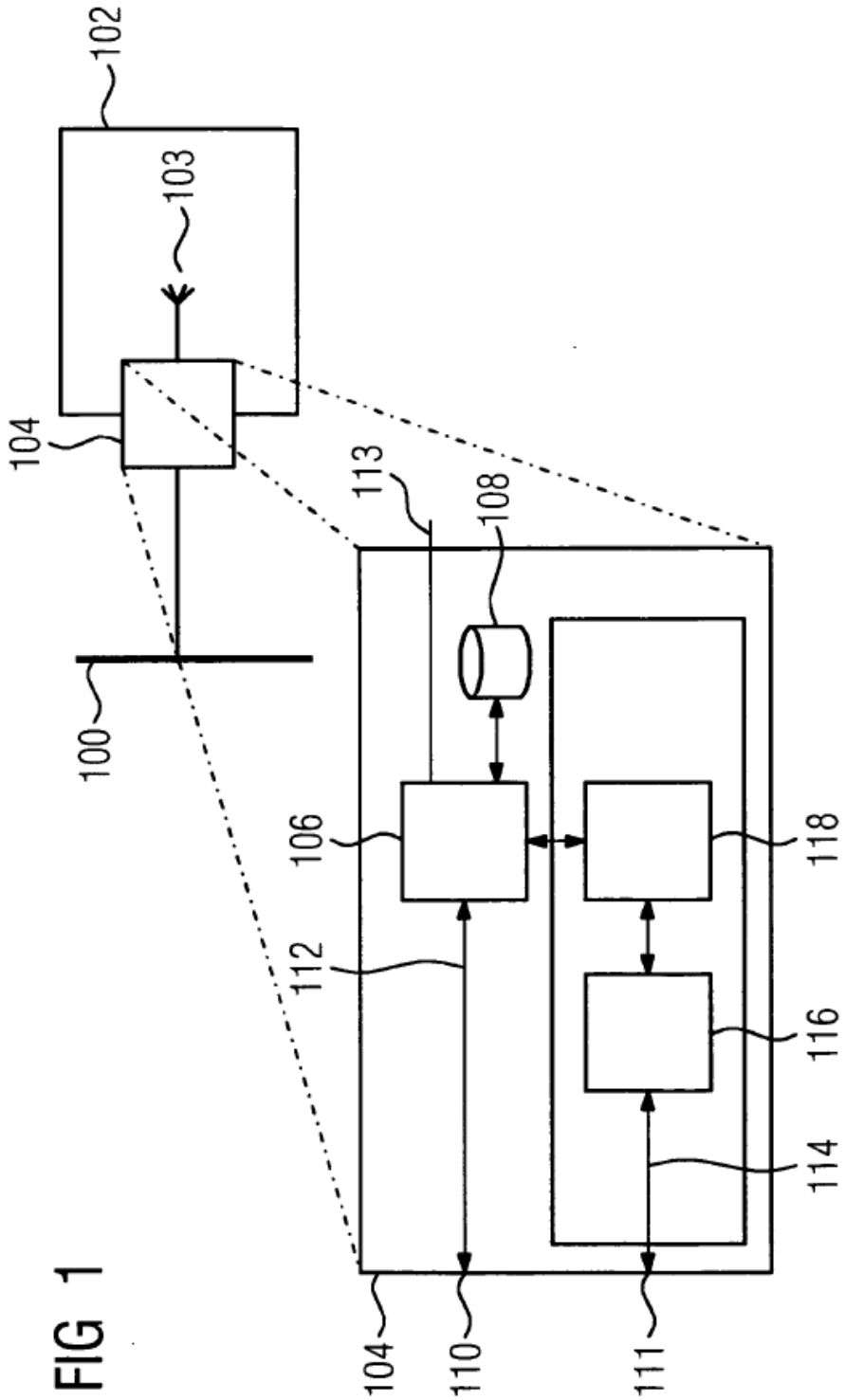


FIG 1

FIG 2

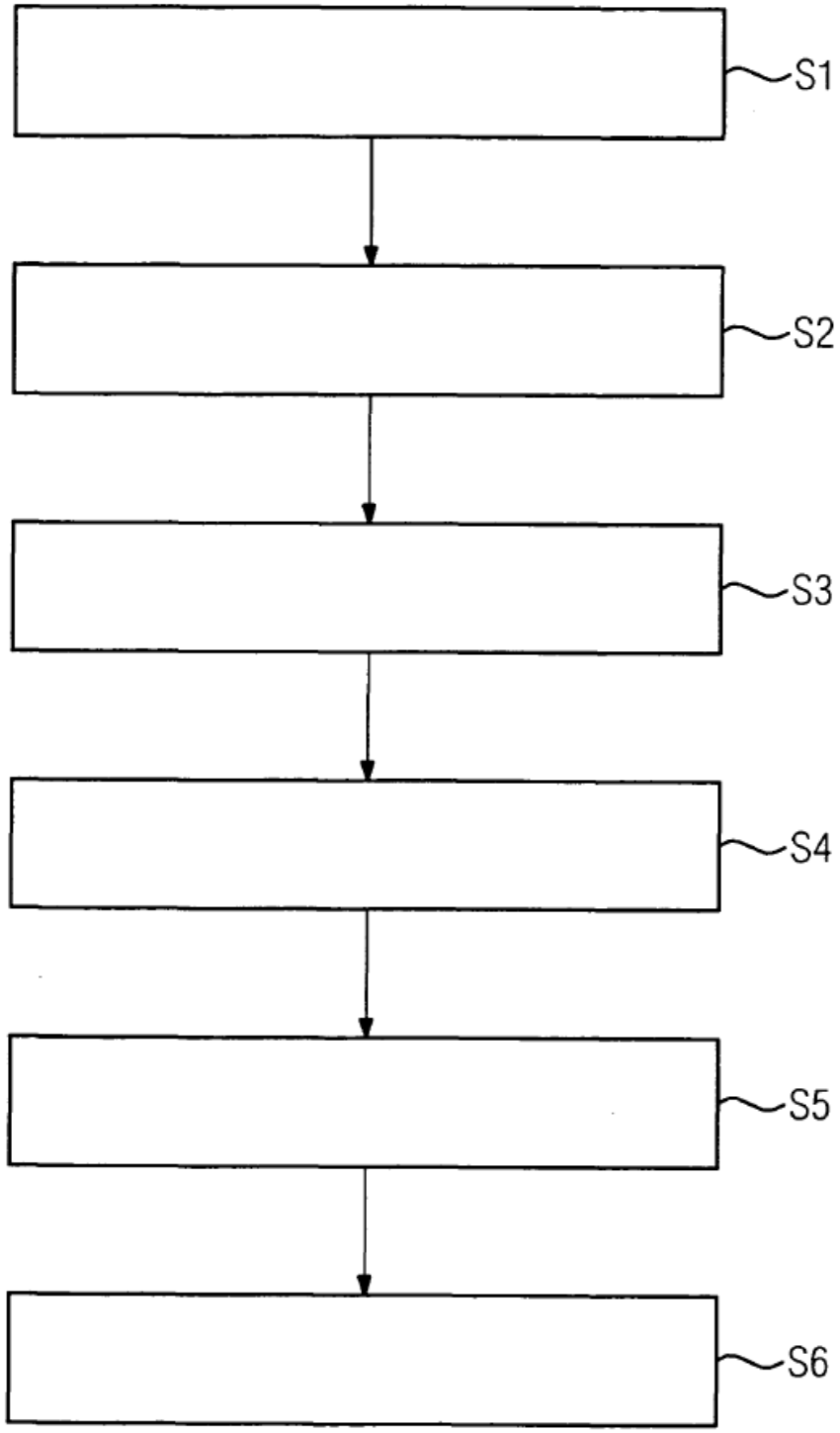
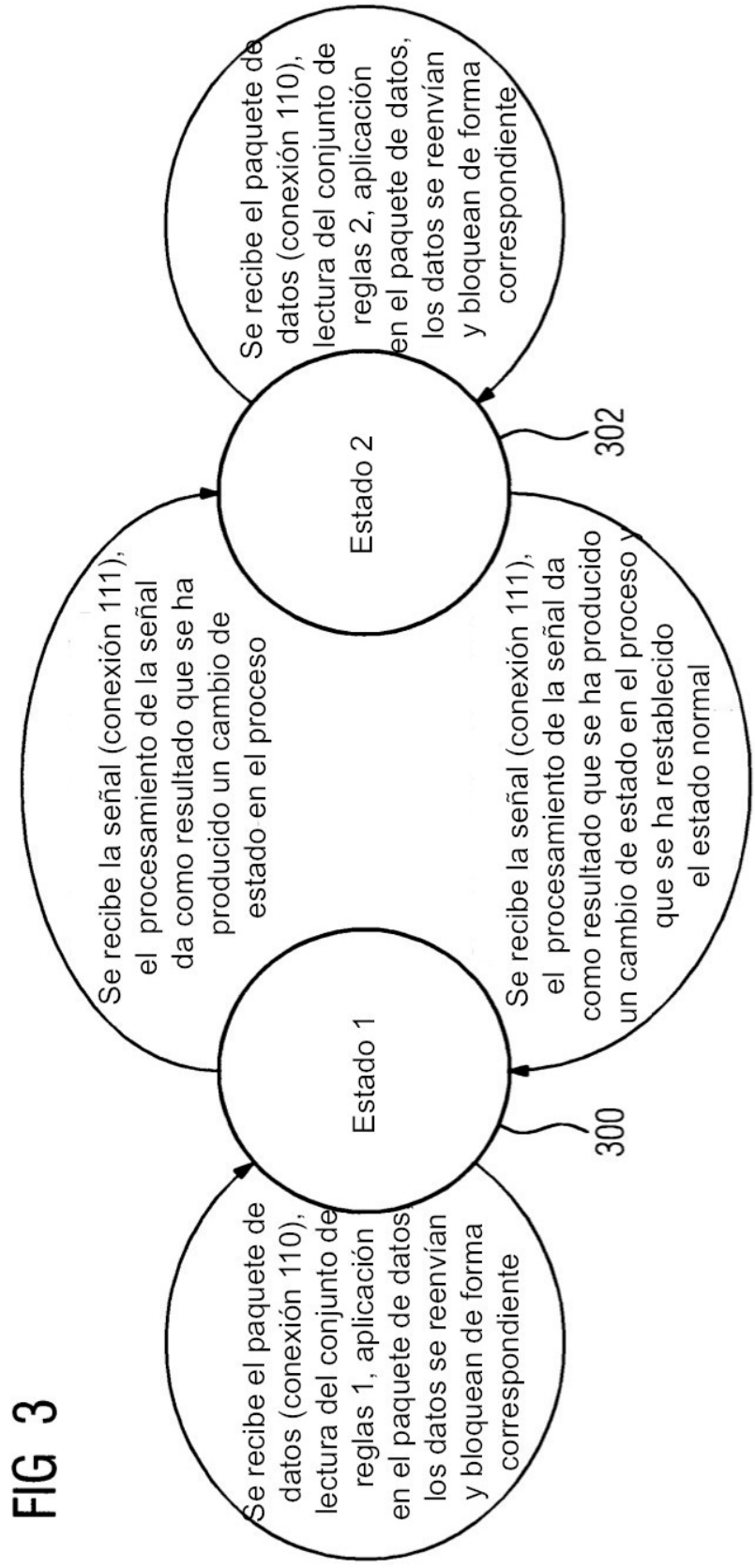


FIG 3


Estado 1
Estado 2
300
302
Se recibe el paquete de datos (conexión 110), lectura del conjunto de reglas 1, aplicación en el paquete de datos, los datos se reenvían y bloquean de forma correspondiente
Se recibe la señal (conexión 111), el procesamiento de la señal da como resultado que se ha producido un cambio de estado en el proceso
Se recibe el paquete de datos (conexión 110), lectura del conjunto de reglas 2, aplicación en el paquete de datos, los datos se reenvían y bloquean de forma correspondiente
Se recibe la señal (conexión 111), el procesamiento de la señal da como resultado que se ha producido un cambio de estado en el proceso y que se ha restablecido el estado normal