(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 752 203**

(51) Int. CI.:

G06F 21/60 (2013.01)
G06F 21/79 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **04.06.2014 PCT/EP2014/061540**

(87) Fecha y número de publicación internacional: **31.12.2014 WO14206695**

(96) Fecha de presentación y número de la solicitud europea: **04.06.2014 E 14728183 (6)**

(97) Fecha y número de publicación de la concesión europea: **24.07.2019 EP 2981926**

(54) Título: **Dispositivo de almacenamiento de datos para el intercambio de datos protegido entre distintas zonas de seguridad**

(30) Prioridad:

27.06.2013 DE 102013212525

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.04.2020

(73) Titular/es:

SIEMENS MOBILITY GMBH (100.0%)
Otto-Hahn-Ring 6
81739 München, DE

(72) Inventor/es:

FALK, RAINER

(74) Agente/Representante:

LOZANO GANDIA, José

DESCRIPCIÓN

Dispositivo de almacenamiento de datos para el intercambio de datos protegido entre distintas zonas de seguridad

La invención se refiere a un dispositivo de almacenamiento de datos para el intercambio de datos protegido entre distintas zonas de seguridad con al menos una unidad de almacenamiento, una unidad de validación de datos y una unidad de control de acceso.

En sectores especiales, como las comunicaciones con las autoridades, en los que son aplicables altos requisitos de seguridad y en los que existe una clasificación de seguridad de documentos e información, se conocen las llamadas soluciones de dominio cruzado, a través de las que se realiza un intercambio automático y seguro de documentos y mensajes, por ejemplo correos electrónicos, entre zonas de seguridad con diferentes grados de seguridad.

Para el acoplamiento de redes de control industrial con una red de oficina, Internet pública u otras redes de control se utilizan firewalls convencionales hasta el momento, que filtran la comunicación de datos. A este respecto, la comunicación de datos está permitida o bloqueada en función de la dirección del interlocutor de comunicación y el protocolo de comunicación utilizado. También es habitual establecer una conexión de red a través de un servidor proxy de aplicación que termina la conexión TCP.

En el documento WO 2012/170485 se realiza una solución de seguridad entre dominios cruzados basada en una solución de virtualización, en la que una máquina virtual controla la transferencia de información entre dos dominios de información con diferentes niveles de seguridad. Un sistema semejante comprende un dispositivo informático con una unidad de supervisión para máquinas virtuales (VMM) que controla una primera máquina virtual para un primer dominio de información, una segunda máquina virtual para un segundo dominio de información y una máquina virtual para una solución de dominio cruzado. La máquina virtual para la solución de dominio cruzado controla el intercambio de información entre el primer y el segundo dominio de información o las máquinas virtuales correspondientes.

En el documento WO 2012/045984 A1 se describe un dispositivo para la transferencia segura de datos entre dos sistemas informáticos. A este respecto se escribe un archivo por el primer sistema informático en un primer módulo de gestión de archivos del dispositivo de transferencia de datos, desde allí se transfiere a un módulo de verificación interno y se examina y desde allí se transfiere en función del resultado del examen a un segundo módulo de gestión de archivos para la lectura por parte del segundo sistema informático.

Para el intercambio de datos entre una red de oficina o un equipo de servicio con una red de control o un equipo de control, por ejemplo, para distribuir nuevos programas o instrucciones, las soluciones complejas con firewall intermedio o solución de virtualización no son factibles, en particular cuando a través de muchas interfaces distribuidas se deben intercambiar datos a través de diferentes zonas de seguridad.

Por lo tanto, el objetivo de la presente invención es proporcionar una solución fácilmente realizable y aplicable para el intercambio de datos, por ejemplo, con una red de control o un equipo de control, que no presente reacción y sea robusta frente a ataques. La solución debe ser integrable en particular en un equipo de control individual o implementable como un bloqueo de datos entre dos zonas de seguridad de un sistema de control.

El objetivo se consigue mediante las medidas descritas en la reivindicación independiente. En las reivindicaciones dependientes están representados perfeccionamientos ventajosos del dispositivo de almacenamiento de datos según la invención.

El dispositivo de almacenamiento de datos según la invención para el intercambio de datos protegido entre distintas zonas de seguridad comprende al menos una unidad de almacenamiento, una unidad de validación de datos y una unidad de control de acceso. La unidad de almacenamiento presenta una primera interfaz con una primera zona de seguridad, a través de la que los elementos de datos solo se pueden escribir en la unidad de almacenamiento. Además, la unidad de almacenamiento presenta una segunda interfaz con una segunda zona de seguridad, a través de la que los elementos de datos solo se pueden leer de la unidad de almacenamiento. La unidad de validación está configurada para verificar la concordancia de los elementos de datos escritos en la unidad de almacenamiento con un patrón predeterminado. La unidad de control de acceso está configurada para permitir una lectura de los elementos de datos desde la unidad de almacenamiento solo cuando los elementos de datos se consideran como concordantes y, por lo tanto, están validados como válidos.

Al realizar la validación de datos en un dispositivo de almacenamiento de datos, es decir, en un componente de hardware, se puede realizar una validación con alta fiabilidad contra la manipulación. Gracias a cada vez una interfaz separada para las diferentes zonas de seguridad, el dispositivo de almacenamiento de datos según la invención se puede intercalar de manera sencilla. El dispositivo de almacenamiento de datos está construido de manera sencilla y por lo tanto se puede implementar de forma relativamente económica, en particular en

comparación con las soluciones de dominio cruzado conocidas hasta ahora. El dispositivo de almacenamiento de datos según la invención se puede intercalar entre zonas de seguridad cualesquiera o las redes correspondientes y no está limitado a un entorno específico. A este respecto, cada zona de seguridad puede funcionar como una red cerrada, ya que no se realiza ninguna comunicación de red. Solo los elementos de datos proyectables seleccionados se proporcionan en el otro lado, en tanto que una validación de datos no haya producido anomalías. Asimismo, se garantiza la libertad de respuesta en el intercambio de datos de una red externa a una red cerrada. No se generan elementos de datos adicionales dado que solo se transmiten los elementos de datos introducidos en el dispositivo de almacenamiento de datos, de modo que no se transmiten elementos de datos adicionales de vuelta a la primera zona de seguridad.

La unidad de almacenamiento presenta una pluralidad de células de almacenamiento, en donde a cada célula de almacenamiento se le puede asociar un identificador de verificación y solo a una célula de almacenamiento con un elemento de datos validado como válido se le asocia un identificador de validación. La célula de almacenamiento está habilitada para un acceso de lectura solo con un identificador de validación asociado.

Esto tiene la ventaja de que solo se requiere una unidad de almacenamiento para el dispositivo de almacenamiento de datos y, por lo tanto, este se puede realizar de manera muy compacta y económica.

En una realización alternativa no según la invención, la unidad de almacenamiento presenta un primer componente de almacenamiento que permite un acceso de solo escritura con respecto a la primera interfaz y transmite los elementos de datos escritos a la unidad de validación. La unidad de almacenamiento comprende además un segundo componente de almacenamiento que lee los elementos de datos de la unidad de validación y permite un acceso de solo lectura con respecto a la segunda interfaz.

Esto tiene las ventajas de que el intercambio de datos se realiza mediante un procedimiento estándar sencillo, a saber, la copia sencilla de los elementos de datos. En el caso de una validación de datos no exitosa es posible de forma muy sencilla una limpieza de los elementos de datos.

Además, es ventajoso si el dispositivo de almacenamiento de datos comprende varias regiones de almacenamiento, una región de almacenamiento comprende al menos una unidad de almacenamiento y/o una unidad de validación y/o una unidad de acceso y cada región de almacenamiento transporta los elementos de datos en direcciones respectivamente diferentes. La al menos una unidad de validación verifica la concordancia de los elementos de datos para cada dirección con un patrón propio, independiente de la dirección opuesta u otras direcciones.

Por lo tanto es posible de forma independiente entre sí un intercambio de datos seguro protegido frente a manipulación en diferentes direcciones, en particular en la dirección de ida y vuelta.

En un ejemplo de realización ventajoso, las regiones de memoria presentan una capacidad de almacenamiento diferente. De este modo, el dispositivo de almacenamiento de datos se puede optimizar en términos de capacidad para un flujo de datos no simétrico en diferentes direcciones.

En una forma de realización, la unidad de control de acceso proporciona un valor de reemplazamiento o un valor inválido o una información adicional para un elemento de datos escrito cuyo valor ha sido validado como inválido. Esto presenta la ventaja de que se puede leer un conjunto de datos completo a pesar de un elemento de datos validado como inválido y un equipo de control puede continuar funcionando, por ejemplo, con el último valor válido antes de la transmisión de datos o un valor promedio de los últimos valores válidos como un valor de reemplazamiento.

En otra forma de realización, la unidad de control de acceso bloquea el acceso de lectura a un elemento de datos si ese elemento de datos se ha validado como inválido. Esto presenta la ventaja de que no se leen elementos de datos inválidos, por ejemplo corruptos, en la segunda zona de seguridad y, por lo tanto, allí tampoco pueden desarrollar efectos dañinos.

En una forma de realización, la unidad de control de acceso trata, en el caso de uno o un cierto número de elementos de datos validados como inválidos, todos o parte de los elementos de datos validados como válidos de la misma manera que el elemento de datos validado como inválido. Por lo tanto, a todos los elementos de datos que contienen los datos de un archivo se les puede asignar un valor predeterminado, si bien solo un único elemento de datos del archivo no es válido. De este modo se consigue que se proporcione un conjunto de datos global autoconsistente de una pluralidad de células de almacenamiento.

En una forma de realización ventajosa, la unidad de control de acceso desactiva todo el dispositivo de almacenamiento de datos cuando uno o varios elementos de datos escritos se han validado como inválidos.

En otra realización, la unidad de control de acceso bloquea el acceso de escritura al dispositivo de almacenamiento si uno o más elementos de datos se han validado como inválidos. Este bloqueo de acceso de escritura se puede aplicar a todos o ciertos accesos.

En otro ejemplo de realización, la unidad de control de acceso dispone, en el caso de uno o varios elementos de datos validados como inválidos, un reinicio de la célula de almacenamiento, en la que está almacenado el elemento de datos validado como inválido, o dispone un reinicio de una región parcial o dispone un reinicio de todas las células de almacenamiento de la unidad de almacenamiento. Por lo tanto, las células de almacenamiento ”infectadas” de la unidad de almacenamiento se limpian de inmediato, de modo que no se puedan producir daños a continuación.

En una forma de realización ventajosa, en el dispositivo de almacenamiento de datos está configurada una tercera interfaz, que es accesible desde la primera zona de seguridad y que duplica y lee los elementos de datos escritos a través de la primera interfaz desde la primera zona de seguridad en la unidad de almacenamiento. De este modo es posible interceptar valores de datos escritos dentro de una zona de seguridad, pero sin influir en la comunicación dentro de la zona de seguridad y entre las zonas de seguridad.

En una forma de realización ventajosa, un elemento de datos escrito está configurado como un valor de actuador. Este elemento de datos leído en un entorno de control se puede aplicar allí directamente como entrada. Esto tiene la ventaja de que, por ejemplo, mediante un servicio de internet se puede proporcionar un valor de datos pero sin requerir para ello una comunicación de red. De este modo, un entorno de control configurado como una zona de seguridad es una red cerrada.

En otra forma de realización, la unidad de validación está configurada para almacenar y/o cargar varios patrones diferentes. Esto permite una amplia validación adaptada a varios criterios.

En una forma de realización ventajosa, la unidad de validación valida los elementos de datos respecto a varios patrones, y la unidad de control de acceso solo permite entonces un acceso de lectura cuando al menos uno o un cierto número mínimo de patrones o una combinación lógica de patrones están validados como válidos.

En una forma de realización, un patrón es un formato o tipo de archivo o un rango de valores o una suma de verificación válida o una concordancia de dependencias de varios elementos de datos entre sí o una dependencia temporal de varios elementos de datos.

En una forma de realización, la primera y/o la segunda interfaz está configurada como una interfaz según un estándar I2C (Inter-Integrated Circuit), SPI (Serial Peripheral Interface), RS232 (Electronical Industries Alliance-232-F), RS485 (Electronical Industries Alliance-485), USB (Universal Serial Bus), de tarjeta SD (Secure Digital Memory Card) o un estándar de Internet, Profinet IO (Input-Output), IP (Internet Protocoll), FTP (File Transfer Protocoll), scp (Secure Copy), HTTP (hypertext transfer protocoll), HTTPS (hypertext transfer protocoll secure), CoAP (Constrained Application Protocoll), OPC (OLE for Process Control) o OPC UA (OLE for Process Control Unified Architecture).

En una forma de realización ventajosa, el dispositivo de almacenamiento de datos está configurado en forma de un módulo de almacenamiento como disposición de puerta lógica programable en campo o como circuito integrado específico de la aplicación o como sistema en un circuito integrado. Mediante una realización en hardware se produce una alta protección contra la manipulación. Además, una solución semejante se puede implementar de forma relativamente económica. Un intercambio de datos se puede realizar de forma sencilla, ya que los elementos de datos se proporcionan con valores de datos a un archivo, por ejemplo, como el contenido de un módulo de almacenamiento, en particular una tarjeta SD o una memoria USB.

Ejemplos de realización del dispositivo de almacenamiento de datos según la invención están representados a modo de ejemplo en los dibujos y se explican más en detalle mediante la descripción siguiente.

Muestran:

La Figura 1 una primera forma de realización de un dispositivo de almacenamiento de datos según la invención con una unidad de almacenamiento y una primera y una segunda interfaz en una representación esquemática;

La Figura 2 una segunda forma de realización de un dispositivo de almacenamiento de datos según la invención con una unidad de almacenamiento, que está formada por dos componentes de almacenamiento separados, en una representación esquemática; y

La Figura 3 un tercer ejemplo de realización de un dispositivo de almacenamiento de datos según la invención con dos regiones de almacenamiento para un intercambio de datos en las direcciones de ida y vuelta en una representación esquemática.

Las partes correspondientes entre sí están provistas en todas la figuras con las mismas referencias.

La figura 1 muestra un ejemplo de realización de un dispositivo de almacenamiento de datos que valida los datos con dos interfaces 14, 15 para intercambiar datos de forma segura entre dos zonas de seguridad 16, 17. El intercambio de datos se realiza mediante una sincronización de datos con una validación de datos, en la que los elementos de datos 18 registrados a través de una primera interfaz 14 se introducen en una primera unidad de almacenamiento 11 y solo son visibles para la segunda interfaz 15 después de una validación y, por lo tanto, se pueden leer. Esto es posible un intercambio de datos controlado entre una zona externa, aquí la zona de seguridad 16, y una zona con una alta necesidad de protección, aquí la zona de seguridad 17, en la que, por ejemplo, tiene lugar una comunicación de control entre los equipos de control o incluso una comunicación en tiempo real. A este respecto, una zona de seguridad se puede hacer funcionar como una red cerrada dado que no se realiza ninguna comunicación de red con otra zona de seguridad. Solo los elementos de datos proyectables seleccionados 18 se proporcionan para la segunda zona de seguridad 17, en tanto que una validación de datos no haya producido anomalías. De este modo se garantiza igualmente una libertad de respuesta de una red externa, aquí por ejemplo en la zona de seguridad 16, a una red cerrada, aquí la zona de seguridad 17. No se transmiten elementos de datos que no se correspondan con un patrón que sirve de base en la validación.

La unidad de almacenamiento 11 está conectada además a una unidad de validación 12 y una unidad de control de acceso 13. La unidad de validación 12 está conectada igualmente a la unidad de control de acceso. En particular, los elementos de datos leídos 18 se envían directamente o en copia de la unidad de almacenamiento 11 a la unidad de validación 12 y allí se examinan frente a al menos un patrón y, por lo tanto, se validan. De la unidad de validación 12 se transmite los elementos de datos validados 18 y/o información sobre un resultado de validación, es decir, si un elemento de datos se validado como válido o inválido, a la unidad de validación 11. La unidad de validación 11 reenvía estos elementos de datos y/o información a la unidad de almacenamiento 11.

El dispositivo de almacenamiento de datos 10 representado en la figura 1 comprende una primera interfaz 14 a través de la que los elementos de datos 18 se introducen desde una zona de seguridad 16 a una célula de almacenamiento 19 de la unidad de almacenamiento 11 bajo indicación de una dirección de almacenamiento 21 que identifica una célula de almacenamiento 19. A este respecto, la unidad de almacenamiento 11 está configurada de modo que solo es posible un acceso de lectura a la unidad de almacenamiento 11 desde la primera interfaz 14. La unidad de almacenamiento 11 está configurada además de modo que solo por una segunda interfaz 15, que está en contacto con la segunda zona de seguridad 17, se otorga un acceso de lectura.

La unidad de almacenamiento 11 está configurada, por ejemplo, como una memoria DPRAM (Dual Port RAM), que permite tanto el acceso de lectura como de escritura desde ambas interfaces 14, 15. En este caso, se puede determinar a nivel de célula de almacenamiento, desde qué lado se permite un acceso de lectura o de escritura.

En una variante adicional se puede acceder a una célula de almacenamiento 19 en forma de lectura y de escritura tanto desde la primera interfaz 14 como también desde la segunda interfaz 15. Aquí también es posible un acceso de lectura al contenido de la célula de almacenamiento solo después de una validación exitosa. Eventualmente, la validación de los elementos de datos, es decir, cuál o cuáles patrones se utilizan para examinar los elementos de datos, puede depender de si el acceso de escritura se realiza desde la primera interfaz 14 o desde la segunda interfaz 15.

La unidad de validación 12 está configurada para almacenar al menos un patrón 22. Se pueden cargar otros patrones 22', 22" en la unidad de validación 12 a través de una interfaz no representada o bien a través de la primera interfaz 14 y almacenarse allí. Para una pluralidad de células de almacenamiento 19 o también para cada célula de almacenamiento individual 19, se puede definir una configuración de validación. Una configuración de validación comprende uno o varios patrones 22, 22', 22" con los que uno o varios elementos de datos 19 se examinan y aceptan como válidos solo en caso de concordancia.

Los patrones 22, 22', 22" comprenden, por ejemplo, un formato o un tipo de archivo del elemento de datos o un rango de valores con el que se deben corresponder los elementos de datos. Asimismo, un patrón 22, 22', 22" puede comprender sumas de verificación predeterminadas para uno o varios elementos de datos o dependencias de varios elementos de datos entre sí o una dependencia temporal de varios elementos de datos. En una verificación respecto un patrón 22, 22', 22" con sumas de verificación, las sumas de verificación se pueden haber determinado según un examen de redundancia cíclica CRC o también mediante un algoritmo Hash, como el SHA1, o mediante códigos de integridad de mensajes criptográficos como AES-CBC-MAC, HMAC-SHA1 o mediante firmas digitales.

En el caso de un patrón con dependencias de varios elementos de datos se realiza, por ejemplo, un análisis en serie sobre varios elementos de datos 18 o se realiza una comparación cruzada con otras células de almacenamiento 19 o sus elementos de datos 18. En un patrón con dependencias temporales se verifica, por ejemplo, el período desde el último acceso de escritura respecto a un valor de consigna.

Si la unidad de validación 12 verifica como válido un elemento de datos 18, se le notifica un mensaje de validación 23 a la unidad de control de acceso 13, especificando la dirección de almacenamiento 21 de la célula de almacenamiento 19 en la que está depositado el elemento de datos verificado 18. Esta reenvía la información de dirección 21 y el mensaje de validación 23 a la unidad de almacenamiento 11. Solo después de una validación válida se provee la célula de almacenamiento 19 de un identificador de validación 20. Solo las células de almacenamiento 19 con el identificador de validación 20 están habilitadas para la lectura a través de la interfaz 15.

Si un elemento de datos escrito 18 ha sido validado como inválido, la unidad de control de acceso 13 proporciona un valor de reemplazamiento o un valor inválido o una información adicional y lo transfiere a la unidad de almacenamiento 11 que, por lo tanto, se puede leer a través de la segunda interfaz 15 por un usuario de la segunda zona de seguridad 17. Con uno o un cierto número de elementos de datos validados como inválidos, la unidad de control de acceso 13 también puede tratar todos o una parte de los elementos de datos validados como válidos de la misma manera que el elemento de datos validado como inválido.

Adicional o alternativamente, la unidad de control de acceso 13 puede bloquear el acceso de escritura a la célula de almacenamiento 19 cuando uno o varios elementos de datos 19 se han validado como inválidos. Esto se le comunica a la unidad de almacenamiento 11, 111 mediante el mensaje de validación 23 o 123 en el ejemplo de realización 100, 200 del dispositivo de almacenamiento de datos. El mensaje de validación 123 en la realización 100, 200 del dispositivo de almacenamiento de datos se transmite desde la unidad de control de acceso 113 a través de la unidad de validación 112 o también directamente desde la unidad de control de acceso 113, no representada, al primer componente de almacenamiento 111.

Como otra opción, la unidad de control de acceso 13, en el caso de uno o varios elementos de datos validados como inválidos, dispone un reinicio de la célula de almacenamiento 19 que contiene el elemento de datos validado como inválido. Alternativamente, una región parcial de la unidad de almacenamiento 11 se puede reiniciar en el caso de un elemento de datos validado como inválido o también puede disponer un reinicio de todas las células de almacenamiento 19 de la unidad de almacenamiento 11.

Alternativamente, la unidad de control de acceso 13 desactiva todo el dispositivo de almacenamiento de datos 10.

Para leer una célula de almacenamiento 19, la segunda interfaz 15 transmite la dirección de memoria 21 de la célula de almacenamiento deseada 19 y, a cambio, recibe el elemento de datos solicitado 18. Las células de almacenamiento 19 sin el identificador de validación 20 están bloqueadas para el acceso de lectura. Esto asegura que las células de almacenamiento 19 no se puedan leer durante la validación. De este modo, las células de almacenamiento que se han validado como inválidas también pueden permanecer bloqueadas dado que no reciben un identificador de validación 20. Al reescribir una célula de almacenamiento a través de la primera interfaz 14 se borra el indicador de validación 20.

En la fig. 2 está representada otra forma de realización de un dispositivo de almacenamiento de datos 100. El dispositivo de almacenamiento de datos 100 comprende una primera interfaz 14 con una primera zona de seguridad 16 y una segunda interfaz 15 con una segunda zona de seguridad 17. Las interfaces 14, 15 están conectadas a una unidad de almacenamiento 111, la unidad de almacenamiento 111 a su vez está conectada a una unidad de validación 112 y una unidad de control de acceso 113, que están realizadas aquí, por ejemplo, como una unidad integrada.

La unidad de almacenamiento 111 comprende un primer componente de almacenamiento 101, que solo presenta una interfaz con la primera interfaz 14. Un acceso de solo escritura al componente de almacenamiento 101 es posible a través de esta primera interfaz. Además, la unidad de almacenamiento 111 comprende un segundo componente de almacenamiento 102, que presenta un acceso de solo lectura con respecto a la segunda interfaz 15. Los elementos de datos 118 introducidos a través de la primera interfaz 14 se depositan en la célula de almacenamiento 119, que se determina a través de la información de dirección 121. Aquí se realiza un intercambio de datos entre la primera interfaz 14 y la segunda interfaz 15 mediante una copia de los elementos de datos 118 desde el primer componente de almacenamiento 101 en la unidad de validación 112.

En la unidad de validación 112, según se describe en el ejemplo de realización anterior 10, tiene lugar una verificación de los elementos de datos 118 en base a información de validación que comprende uno o más patrones 122. Si un elemento de datos 118 se valida como válido, este elemento de datos 118 se transfiere a través de la unidad de control de acceso 113 al segundo componente de almacenamiento 102, indicando la dirección 121' de la célula de almacenamiento 103 en la que se escribe el elemento de datos. A través de la segunda interfaz 15, el elemento de datos 118 se puede leer indicando la dirección de almacenamiento 121' de la célula de almacenamiento 103.

En este ejemplo de realización, la unidad de validación 112 y la unidad de control de acceso 113 están configuradas integradas como un componente. También es posible una configuración separada según está representado en la figura 1 o la figura 3. Las funciones de la unidad de validación 112 o la unidad de control de acceso 113 se corresponden con las funciones de la unidad de validación 12 o de la unidad de control de acceso 13 del ejemplo

de realización 10. En el ejemplo de realización 100, los mismos elementos de datos 118 se copian desde la unidad de validación 112 a la unidad de control de acceso 113 y desde allí se le transfieren al segundo componente de almacenamiento en lugar de simplemente enviar un mensaje de validación 23 a la unidad de almacenamiento 11 y acto seguido asignar un identificador de validación 20 a la célula de almacenamiento correspondiente.

Para permitir un intercambio de datos en ambas direcciones, la estructura interna del dispositivo de almacenamiento de datos 10, 100 se puede disponer de forma duplicada o en espejo. Una disposición semejante está representada en la figura 3. En el ejemplo de realización 200 de un dispositivo de almacenamiento de datos que permite un intercambio de datos en ambas direcciones está configurada una primera interfaz 214 con una primera zona de seguridad 16 y una segunda interfaz 215 con una segunda zona de seguridad 17. Una primera región de almacenamiento 201 permite el intercambio de datos desde la primera zona de seguridad 16 a una segunda zona de seguridad 17, la segunda región de almacenamiento 202 permite un intercambio de datos validados desde la segunda zona de seguridad 17 a través de la segunda interfaz 215 hacia la primera interfaz 214 y la primera zona de seguridad 16 posterior.

En el dispositivo de almacenamiento de datos representado 200, la primera y segunda región de almacenamiento 201, 202 se corresponden con una unidad de almacenamiento 111 del aparato de almacenamiento de datos 100 junto con respectivamente una unidad de validación 112 y una unidad de control de acceso 113. A este respecto, aquí la unidad de validación 112 y la unidad de control de acceso 113 están configuradas como componentes separados. Ambas regiones de almacenamiento 201, 202 trabajan independientemente una de la otra. Así se pueden definir y validar diferentes patrones 122, 122’ y, por lo tanto, diferente información de validación para examinar los elementos de datos 118 para las diferentes direcciones. En lugar de respectivamente una unidad de validación 112 y respectivamente una unidad de control de acceso 113 por región de almacenamiento 201, 202 y, por tanto, dirección de transmisión, también puede estar configurada una unidad de validación y/o unidad de control de acceso común, no mostrada. Si solo están configuradas una unidad de control de acceso y una unidad de validación para ambas direcciones, entonces están contenidos patrones o información de validación separados respectivamente para las distintas direcciones, y el examen de las funciones de control de acceso se aplica según las regulaciones para la dirección de transmisión respectiva.

Los elementos de datos que se intercambian a través del dispositivo de almacenamiento de datos 10, 100, 200 pueden ser en particular datos de estado, datos de diagnóstico o datos de control de un sistema de control. En particular, estos pueden ser datos a escribir o proporcionar de forma cíclica, de modo que los datos pueden ser escritos o leídos en un marco de tiempo predeterminado. Los datos también pueden ser valores de actuador que se pueden aplicar directamente como entrada para un equipo de control en un entorno de control.

La primera interfaz 14, 214 y/o la segunda interfaz 15, 215 se corresponden, por ejemplo, con la interfaz I2C, SPI, RS232, RS435, USB, de tarjeta de memoria o interfaces de comunicación según el estándar Ethernet, Profinet IO, IP, FTP, scp, HTTP, HTTPS, CoAP, OPC, OPC UA.

En una variante no representada, el dispositivo de almacenamiento de datos 10, 100, 200 comprende una tercera interfaz, que es accesible desde la primera zona de seguridad 16. A través de esta tercera interfaz se pueden copiar y leer los elementos de datos 18, 118, los elementos de datos escritos a través de la primera interfaz 14, 214, 215 en la unidad de almacenamiento 11 o en el primer componente de almacenamiento de solo escritura 101 de la unidad de almacenamiento 111. Por consiguiente se puede supervisar una ”escucha” o supervisión de la primera interfaz de escritura 14, 214, 215. De este modo se garantiza una libertad de respuesta en la transmisión de datos a la segunda zona de seguridad 17 o al leer los datos a través de la segunda interfaz 15, 214, 215. Solo se interceptan los valores escritos dentro de una zona de seguridad, no obstante, sin influir en la comunicación dentro de la zona de seguridad.

El dispositivo de almacenamiento de datos 10, 100, 200 puede estar configurado, por ejemplo, como módulo de hardware, en particular como disposición de puerta lógica programable en campo FPGA o como circuito integrado específico a la aplicación ASIC o como sistema en un circuito integrado. Pero los dispositivos de almacenamiento de datos 10, 100, 200 descritos también se pueden usar como una unidad de acceso de almacenamiento que valida los datos, que bloquea un acceso de lectura a una región de almacenamiento de un módulo de almacenamiento separado después de un acceso de escritura y lo habilita después de la validación exitosa.

Todas las características descritas y/o dibujadas se pueden combinar ventajosamente entre sí en el marco de la invención.

REIVINDICACIONES

1. Dispositivo de almacenamiento de datos para el intercambio de datos protegido entre diferentes zonas de seguridad (16, 17) con una unidad de almacenamiento (11, 111), una unidad de validación (12, 112) y una unidad de control de acceso (13, 113), en donde la unidad de almacenamiento (11, 111) presenta una primera interfaz (14 , 214) con una primera zona de seguridad (16), a través de la que los elementos de datos (18, 118, 118') solo se pueden escribir en la unidad de almacenamiento (11, 111), y la unidad de almacenamiento (11, 111) presenta una segunda interfaz (15, 215) con una segunda zona de seguridad (17), a través de la que los elementos de datos (18, 118, 118') solo se pueden leer de la unidad de almacenamiento (11, 111), la unidad de validación (12, 112) está configurada para verificar la concordancia de los elementos de datos (18, 118, 118') escritos en la unidad de almacenamiento (11, 111) con un patrón predeterminado (22, 22', 22", 122, 122') y

la unidad de control de acceso (13, 113) está configurada para permitir una lectura de los elementos de datos (18, 118, 118') desde la unidad de almacenamiento (11, 111) solo cuando los elementos de datos (18, 118, 118') se consideran como concordantes y por consiguiente están validados como válidos, en donde la unidad de almacenamiento (11) presenta una pluralidad de células de almacenamiento (19) y a cada célula de almacenamiento (19) está asociado un identificador de validación (20), en donde solo a una célula de almacenamiento (19) con un elemento de datos validado como válido está asociado un identificador de validación (20) y la célula de almacenamiento (19) está habilitada para un acceso de lectura solo con un identificador de validación asociado (20).

2. Dispositivo de almacenamiento de datos según la reivindicación 1, en donde el dispositivo de almacenamiento de datos (200) comprende varias regiones de almacenamiento (201, 202), una región de almacenamiento (201), una unidad de almacenamiento (11, 111) y/o una unidad de validación (12, 112) y/o una unidad de acceso (13, 113), y cada región de almacenamiento (201, 202) transporta los elementos de datos (18, 118, 118') en una dirección respectivamente diferente, y la al menos una unidad de validación (13, 113) examina la concordancia de los elementos de datos (18, 118, 118') para cada dirección con un patrón propio (22, 22', 22", 122, 122') independiente de la dirección opuesta o las otras direcciones.

3. Dispositivo de almacenamiento de datos según la reivindicación 2, en donde las regiones de almacenamiento (201, 202) presentan una capacidad de almacenamiento diferente.

4. Dispositivo de almacenamiento de datos según cualquiera de las reivindicaciones 1 a 3, en donde para un elemento de datos escrito (18, 118, 118') cuyo valor se ha sido validado como inválido, la unidad de control de acceso (13, 113) proporciona un valor de reemplazamiento o un valor inválido o información adicional.

5. Dispositivo de almacenamiento de datos según cualquiera de las reivindicaciones 1 a 3, en donde la unidad de control de acceso (13, 113) bloquea el acceso de lectura a un elemento de datos (18, 118, 118') si este elemento de datos (18, 118, 118') se ha sido validado como inválido.

6. Dispositivo de almacenamiento de datos según la reivindicación 4 o 5, en donde la unidad de control de acceso (13, 113), en el caso de uno o un cierto número de elementos de datos validados como inválidos, trata todos o una parte de los elementos de datos validados como válidos de la misma manera que el elemento de datos validado como inválido.

7. Dispositivo de almacenamiento de datos según cualquiera de las reivindicaciones 1 a 6, en donde la unidad de control de acceso (13, 113) desactiva todo el dispositivo de almacenamiento de datos (10, 100, 200) si uno o varios elementos de datos escritos (18, 118, 118') se han validado como inválidos.

8. Dispositivo de almacenamiento de datos según cualquiera de las reivindicaciones 1 a 7, en donde la unidad de control de acceso (13, 113) bloquea el acceso de escritura a la unidad de almacenamiento (11, 101) si uno o varios elementos de datos (18, 118, 118') se han validado como inválidos.

9. Dispositivo de almacenamiento de datos según cualquiera de las reivindicaciones 1 a 8, en donde la unidad de control de acceso (13, 113) dispone el reinicio de estas células de almacenamiento (19, 119) en el caso de uno o varios elementos de datos validados como inválidos, o dispone un reinicio de una región parcial en la que está almacenado el elemento de datos validado como inválido, o dispone un reinicio de todas las células de almacenamiento de la unidad de almacenamiento (11, 111).

10. Dispositivo de almacenamiento de datos según cualquiera de las reivindicaciones 1 a 9, en donde está configurada al menos una tercera interfaz, que es accesible desde la primera zona de seguridad (16) y que duplica y lee los elementos de datos (18, 118, 118') escritos a través de la primera interfaz (14, 214) desde la primera zona de seguridad (16) en la unidad de almacenamiento (11, 111).

11. Dispositivo de almacenamiento de datos según cualquiera de las reivindicaciones 1 a 10, en donde un elemento de datos escrito (18, 118, 118') está configurado como valor de actuador y el elemento de datos (18, 118, 118') leído en un entorno de control se puede usar directamente como entrada.

12. Dispositivo de almacenamiento de datos según cualquiera de las reivindicaciones 1 a 11, en donde la unidad de validación (12, 112) está configurada para almacenar y/o cargar varios patrones diferentes (22, 22', 22", 122, 122').

13. Dispositivo de almacenamiento de datos según cualquiera de las reivindicaciones 1 a 12, en donde la unidad de validación (12, 112) valida los elementos de datos (18, 118, 118') respecto a varios patrones (22, 22', 22", 122, 122') y la unidad de control de acceso (13, 113) solo permite entonces el acceso de lectura cuando al menos uno o un cierto número mínimo de patrones (22, 22', 22", 122, 122') o una combinación lógica de patrones (22, 22', 22", 122, 122') están validados como válidos.

14. Dispositivo de almacenamiento de datos según cualquiera de las reivindicaciones 1, 12 o 13, en donde un patrón (22, 22', 22", 122, 122') es un formato o un tipo de archivo o un rango de valores o una suma de verificación válida o una concordancia de dependencias de varios elementos de datos entre sí o uno dependencia temporal de varios elementos de datos.

15. Dispositivo de almacenamiento de datos según cualquiera de las reivindicaciones 1 a 14, en donde la primera y/o la segunda interfaz (14, 114, 214, 15, 115, 215) está configurada como una interfaz según el estándar I2C, SPI, RS232, RS435, USB , de tarjeta SD o un estándar Ethernet, Profinet IO, IP, FTP, scp, HTTP, HTTPS, CoAP, OPC u OPC UA estándar.

16. Dispositivo de almacenamiento de datos según cualquiera de las reivindicaciones 1 a 15, en donde el dispositivo de almacenamiento de datos (10, 100, 200) está configurado en la forma de un módulo de hardware como disposición de puerta lógica programable en campo o como circuito integrado específico de la aplicación o como sistema en un circuito integrado.

FIG 1

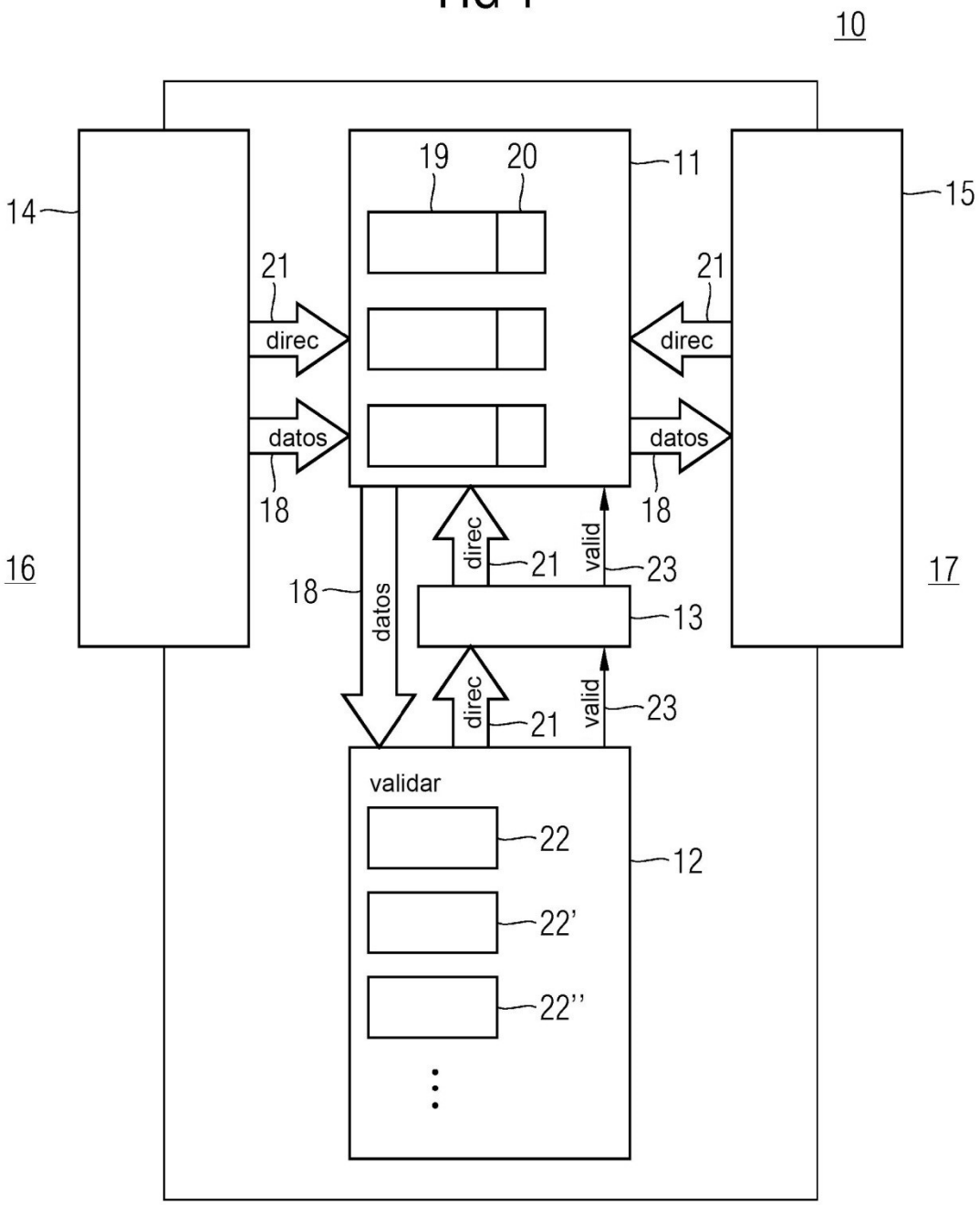

10
14
15
16
17
11
19
20
21
direc
datos
18
21
direc
datos
18
direc
21
valid
23
18
datos
13
direc
21
valid
23
validar
22
22'
22''
12

FIG 2

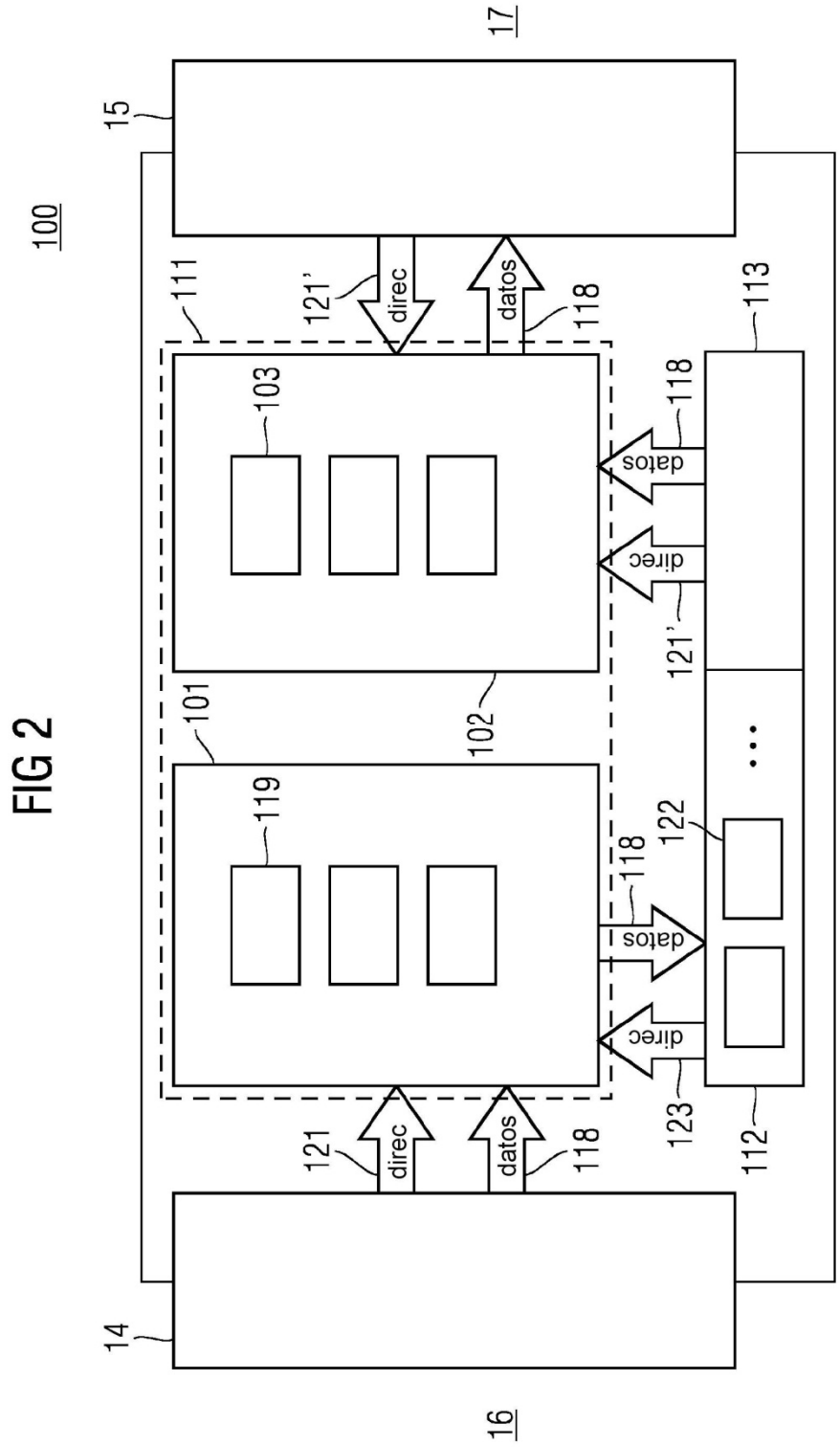
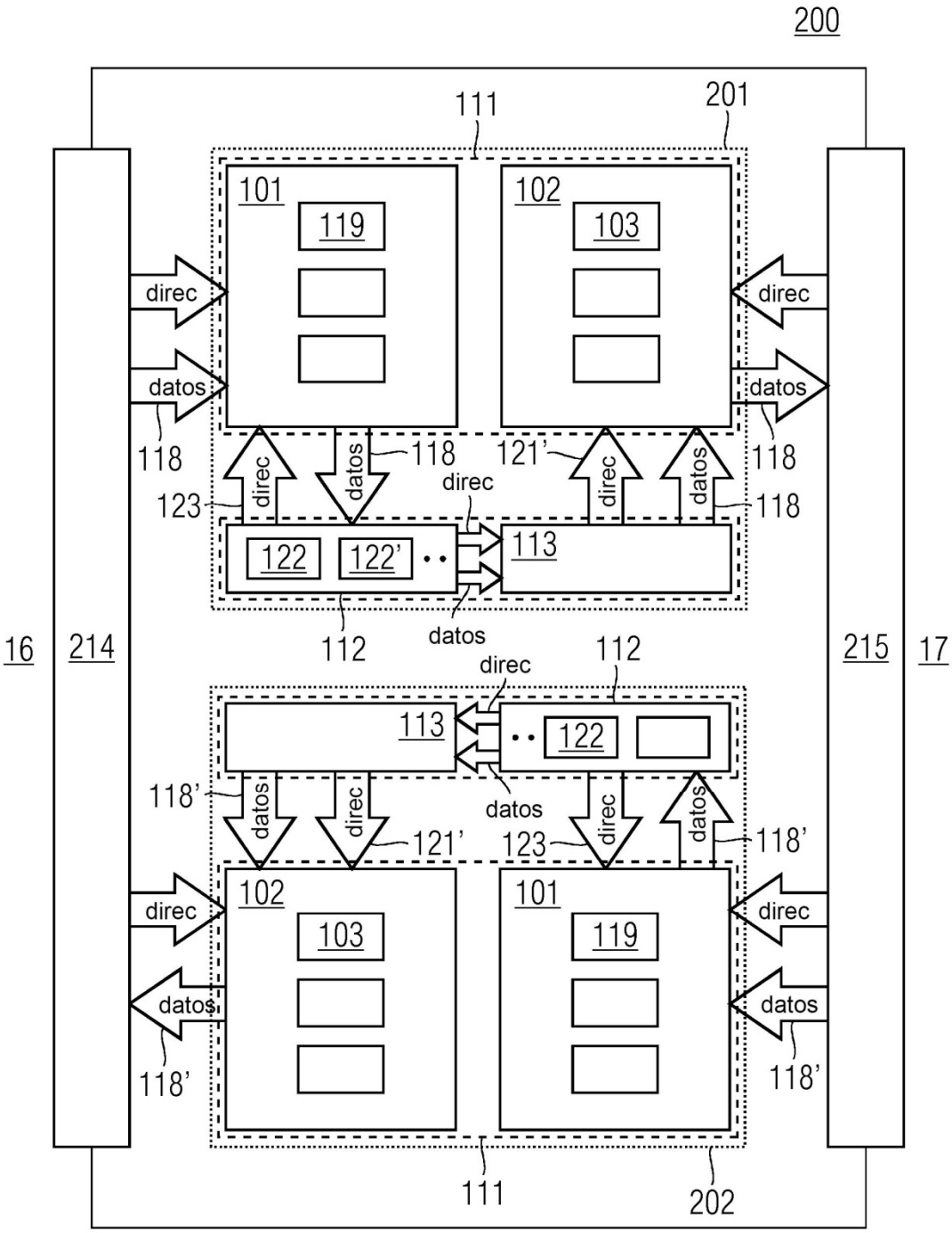

100
17
15
111
121'
direc
datos
118
113
103
118
datos
direc
121'
101
102
119
122
118
datos
direc
123
112
121
direc
datos
118
14
16

FIG 3


200
111
201
101
119
102
103
direc
datos
118
121'
123
122
122'
113
112
16
214
215
17
118'
202