(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 803 209**

(51) Int. CI.:

G06F 12/14 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.04.2016 E 16166334 (9)**

(97) Fecha y número de publicación de la concesión europea: **01.04.2020 EP 3086235**

(54) Título: **Procedimiento de control sistemático de direcciones de zonas de memoria en el marco de una transferencia por acceso directo**

(30) Prioridad:

22.04.2015 FR 1500854

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.01.2021

(73) Titular/es:

THALES (100.0%)
Tour Carpe Diem, Place des Corolles, Esplanade Nord
92400 Courbevoie, FR

(72) Inventor/es:

DUPREZ, ADRIEN;
GRISAL, OLIVIER;
SALIBA, ERIC y
DELOVE ALEXANDRE

(74) Agente/Representante:

SALVÀ FERRER, Joan

DESCRIPCIÓN

Procedimiento de control sistemático de direcciones de zonas de memoria en el marco de una transferencia por acceso directo

[0001] La presente invención se refiere a un procedimiento de control sistemático. La presente invención se refiere también a un dispositivo de control adaptado para la implementación del procedimiento de control. La presente invención se refiere igualmente a un producto de programa informático y a un soporte de información asociados.

[0002] Una transferencia por acceso directo (en inglés, *direct memory access*) es un procedimiento informático en el que se intercambian datos entre un elemento de emisión y de recepción de datos tal como un periférico de hardware externo conectado a una plataforma y una zona de memoria de la plataforma sin intervención de un procedimiento de terceros.

[0003] Dichas zonas de memoria son gestionadas clásicamente por una unidad de gestión de memoria (en inglés, *memory management unit* o *MMU*). Dicha unidad de gestión de memoria permite en particular controlar los accesos a las zonas de memoria de un procedimiento informático, tal como un programa informático que refiere direcciones de memoria virtuales. Para ello, la unidad de gestión de memoria traduce las direcciones de memoria virtuales referidas por el programa informático en direcciones físicas que corresponden a las zonas de memoria usadas.

[0004] Además, para asegurar una transferencia de datos por acceso directo entre una aplicación que se ejecuta en una plataforma y un periférico de hardware externo conectado a la plataforma, se sabe hacer transitar los datos por un controlador de interfaz que accede directamente a las zonas de memoria concernidas.

[0005] Sin embargo, dicho controlador de interfaz puede presentar debilidades en la gestión y el uso de las direcciones físicas referidas en los campos de los datos transferidos, lo que puede conllevar una transferencia de datos ilícitos hacia zonas de memoria prohibidas por medio de las zonas de memoria en acceso directo.

[0006] El documento US 2014/173236 A1 describe un procedimiento para proteger una porción de memoria del sistema a la que puede accederse mediante periféricos externos.

[0007] El documento US 2004/205203 A1 describe, por su parte, un vector de exclusión usado por un acceso DMA que define un conjunto de páginas a las que no pueden acceder los circuitos externos que acceden en directo a la memoria del sistema. El núcleo con seguridad garantiza así un aislamiento al permitir que ciertas páginas sean excluidas de los accesos DMA.

[0008] Existe así la necesidad de un procedimiento de control sistemático que permite detectar la transferencia de mensajes ilícitos hacia zonas de memoria prohibidas.

[0009] La presente invención se define mediante las reivindicaciones independientes adjuntas a las que conviene referirse. Se exponen características ventajosas en las reivindicaciones dependientes. Se considera que las realizaciones o ejemplos descritos en la presente descripción mostrada a continuación que no están cubiertos por las reivindicaciones no forman parte de la invención.

[0010] Otras características y ventajas de la invención se desprenderán de la lectura de la descripción que se ofrece a continuación de realizaciones de la invención, proporcionada a modo de ejemplo únicamente y en referencia a los dibujos que son:

- figura 1, una vista esquemática de un ejemplo de una transferencia de datos por acceso directo entre una aplicación que se ejecuta en una plataforma y un periférico de hardware externo conectado con la plataforma,
- figura 2, una vista esquemática de un ejemplo de una transferencia de datos por acceso directo entre una aplicación que se ejecuta en una plataforma y un periférico de hardware externo conectado con la plataforma según una primera realización, estando los datos transferidos controlados por un dispositivo de control,
- figura 3, una vista esquemática de un ejemplo de una transferencia de datos por acceso directo según una segunda realización, y
- figura 4, una vista esquemática de un ejemplo de una transferencia de datos por acceso directo según una tercera realización.

[0011] En lo que sigue de la descripción, los datos ilustrados en las figuras son líneas de código informático y/o direcciones denotadas de manera arbitraria.

[0012] En las figuras 2, 3 y 4 se representa un dispositivo de control 10.

[0013] El dispositivo de control 10 está adaptado para la implementación de un procedimiento de control

sistemático de al menos un mensaje de configuración de transferencia. El mensaje de configuración de transferencia es un mensaje de configuración de una transferencia por acceso directo desde una aplicación App que se ejecuta en una plataforma 12 hacia al menos una zona de memoria M1, M2 usada por al menos un periférico de hardware externo 16 conectada con la plataforma 12 por un controlador de interfaz 30.

[0014] El mensaje de configuración comprende al menos un campo y un cuerpo.

[0015] El campo del mensaje de configuración comprende informaciones relativas a la dirección física @P1, respectivamente @P2, de una primera zona de memoria M1, respectivamente de una segunda zona de memoria M2, destinada a al menos una transferencia de datos por acceso directo. Cada zona de memoria M1, M2 se caracteriza, de hecho, por una dirección física única.

[0016] El cuerpo del mensaje de configuración comprende informaciones relativas a acciones para efectuar en la primera zona de memoria M1, respectivamente en la segunda zona de memoria M2.

[0017] El mensaje de configuración es apto para ser memorizado en una estructura 24 de control de las transferencias. La estructura 24 es usada por el controlador de interfaz 30 para realizar transferencias de datos en la primera zona de memoria M1, respectivamente en la segunda zona de memoria M2, por acceso directo a la dirección física @P1 de la primera zona de memoria M1, respectivamente a la dirección física @P2 de la segunda zona de memoria M2, referidas en la estructura 24.

[0018] La estructura 24 es referida por la aplicación App por medio de un controlador de interfaz 19 (en inglés, *driver*).

[0019] Las zonas de memoria M1, M2 y la estructura 24 son gestionadas por una unidad de gestión de memoria 18 (en inglés, *memory management unit* o *MMU*). Las reglas de acceso (en inglés, *memory mapping*) de la aplicación App a la estructura 24 pueden configurarse por medio del dispositivo de control 10. La aplicación App no dispone de derechos de configuración de la unidad de gestión de memoria 18. La aplicación App accede en lectura y en escritura a la estructura 24 por medio del controlador de interfaz 19 y la unidad de gestión de memoria 18.

[0020] A modo de ilustración, la primera zona de memoria M1 es una zona de memoria autorizada para la aplicación App y la segunda zona de memoria M2 es una zona de memoria prohibida para la aplicación App.

[0021] La estructura 24 se subdivide asimismo en bloques de memoria gestionados por la unidad de gestión de memoria 18.

[0022] Las informaciones contenidas en el mensaje de configuración pueden conllevar acciones en zonas de memoria prohibidas. Dichas acciones se deben, por ejemplo, a una ausencia de control por la unidad de gestión de memoria 18 de las direcciones físicas de las zonas de memoria contenidas en el campo del mensaje y/o a transferencias de datos no gestionadas por la unidad de gestión de memoria 18. La realización de acciones en zonas de memoria prohibidas se ilustra, en particular, en la figura 1 en la que un mensaje que se dirige a la segunda zona de memoria M2 se transmite a la segunda zona de memoria M2 a la vez que la segunda zona de memoria M2 está prohibida para la aplicación App.

[0023] Una de las funciones del dispositivo de control 10 es impedir una o varias transferencias de datos ilícitos desde la aplicación App hacia el periférico externo 16 por medio de las zonas de memoria M1, M2 internas en la plataforma 12. Recíprocamente, el dispositivo de control 10 está configurado para impedir las transferencias de datos ilícitos desde el periférico externo 16 hacia la aplicación App.

[0024] Para impedir dichas transferencias de datos ilícitos entre la aplicación App y el periférico externo 16, el dispositivo de control 10 implementa al menos una de las funciones siguientes:

- una función de verificación, ilustrada por la referencia «CHECK» en las figuras 2 a 4, de los mensajes de configuración escritos, por la aplicación App por medio del controlador de interfaz 19, en la estructura 24 antes de la lectura y el tratamiento de dichos mensajes por el controlador de interfaz 30.
- una función de sincronización, ilustrada por la referencia «SYNCHRO» en las figuras 2 a 4, de los tratamientos en curso efectuados por el controlador de interfaz 30 sobre los datos de la estructura 24. La sincronización comprende, por ejemplo, un control del estado de progreso de los tratamientos efectuados por el controlador de interfaz 30 y/o de puesta en marcha o en parada de los tratamientos efectuados por el controlador de interfaz 30 en la estructura 24.
- una función de bloqueo, ilustrada por la referencia «FREEZE» en las figuras 2 a 4, de los mensajes controlados por el dispositivo de control 10 hasta al tratamiento de dichos mensajes por el controlador de interfaz 30, de forma que se garantiza la no modificación por la aplicación App o por el controlador de interfaz 19 de los mensajes de transferencias verificados por el dispositivo de control 10,
- una función de alerta, ilustrada por la referencia «ALERT» en las figuras 2 a 4, hacia un sistema operativo 17 (en inglés, *Operating System*) en caso de detección de anomalías en las direcciones de transferencia contenidas en los

mensajes de transferencia memorizados en la estructura 24 y verificados por el dispositivo de control 10.
- una función de configuración del dispositivo de control 10 con una política de seguridad.

[0025] La función de sincronización implementada por el dispositivo de control 10 permite controlar que la función de verificación de los mensajes de configuración sea invocada y realizada sistemáticamente antes del tratamiento de los mensajes por el controlador de interfaz 30.

[0026] La función de bloqueo es implementada por el dispositivo de control 10 por medio de dos mecanismos que pueden usarse de forma exclusiva o concurrente.

[0027] El primer mecanismo se basa en el uso por el dispositivo de control 10 de la configuración de la unidad de gestión de memoria 18. Así, el dispositivo 10 asegura un bloqueo que prohíbe el acceso de la aplicación App a un bloque de memoria de la estructura 24, de manera que dicho bloque de memoria contiene los mensajes de configuración ya verificados por el dispositivo 10. El bloqueo se mantiene hasta el tratamiento de dichos mensajes por el controlador de interfaz 30. Una vez tratados los mensajes, el dispositivo 10 configura de nuevo la unidad de gestión de memoria 18 para desbloquear el acceso a dicho bloque de memoria de la estructura 24 y bloquear un nuevo bloque de memoria de la estructura 24 que contiene nuevos mensajes de configuración de transferencias verificados por el dispositivo de control 10.

[0028] El procedimiento según el primer mecanismo se ilustra esquemáticamente en la figura 2.

[0029] El segundo mecanismo se basa en el cálculo y el almacenamiento por el dispositivo de control 10 de motivos de integridad para uno o varios mensajes de configuración de transferencia verificados por el dispositivo de control 10. Los motivos de integridad son memorizados en una zona de memoria específica 25 de la plataforma 12 de manera que solo el dispositivo de control 10 tenga acceso a dicha zona de memoria específica 25. Los motivos de integridad son controlados justo antes del tratamiento de los mensajes por el controlador de interfaz 30.

[0030] El procedimiento según el segundo mecanismo se ilustra esquemáticamente en la figura 3.

[0031] El dispositivo de control 10 es apto para detener y volver a arrancar el controlador de interfaz 30 de manera que el controlador de interfaz 30 trate solo los mensajes verificados por el dispositivo de control 10 después de la implementación del primer mecanismo y/o del segundo mecanismo descritos anteriormente.

[0032] La función de verificación del dispositivo de control 10 permite controlar que las direcciones referidas en la estructura 24 estén de acuerdo con una política de seguridad. En caso de detección de una anomalía, el dispositivo de control 10 realiza un tratamiento de neutralización y/o genera una excepción. La neutralización consiste, por ejemplo, en sustituir las direcciones prohibidas por direcciones que hacen referencia a una zona de memoria no válida o una zona de memoria controlada por el único dispositivo de control 10.

[0033] El dispositivo de control 10 pertenece a la plataforma 12.

[0034] Como variante, el dispositivo de control 10 pertenece al periférico de hardware externo 16.

[0035] El dispositivo de control 10 es, según el ejemplo de las figuras 2 a 4, un producto de programa informático. El producto de programa es, por ejemplo, un programa informático tal como un software, un software integrado o un microcódigo (en inglés, *firmware*).

[0036] La interacción del programa informático con la plataforma 12 permite implementar el procedimiento de control.

[0037] El producto de programa informático es memorizado en un soporte de informaciones. El soporte de informaciones es un soporte legible en una unidad de tratamiento de datos.

[0038] La aplicación App es un conjunto de programas informáticos aptos para ser ejecutados en la plataforma 12. La plataforma 12 es capaz de intercambiar informaciones con un periférico 16 por medio del controlador de interfaz 19. El controlador de interfaz 19 es un programa informático que permite que otro programa interaccione con un periférico por medio de un controlador de interfaz.

[0039] La plataforma 12 comprende una o varias interfaces físicas que conectan el o los periféricos 16 con la plataforma 12.

[0040] La plataforma 12 es, por ejemplo, una plataforma de hardware tal como un ordenador, un equipo de hardware, un sistema sobre chip (en inglés, *System on Chip o SoC*) o un componente electrónico dedicado (en inglés, *Application Specific Integrated Circuit* o ASIC) o una plataforma de software tal *como* un hipervisor, con las capas de abstracción del hipervisor asociadas con una plataforma de hardware y/o máquinas virtuales.

[0041] En el caso de una plataforma 12 de hardware, el dispositivo de control 10 está integrado en un microcódigo, configurable o no, en el sistema operativo, por ejemplo, en controladores de interfaz, o directamente en la implementación de hardware.

[0042] En el caso de una plataforma de software, el dispositivo de control 10 está integrado en el hipervisor o en las capas de abstracción del hipervisor asociadas a una plataforma de hardware, o en el sistema operativo.

[0043] En las realizaciones ilustradas en las figuras 1 a 4, la plataforma 12 comprende un módulo de conversión 20.d

[0044] El módulo de conversión 20 es apto para asociar a cada dirección virtual una dirección física que corresponde a una zona de memoria M1, M2. Una dirección virtual es una dirección de la memoria virtual que un sistema operativo pone a disposición de sus procedimientos para que se ejecuten dichos procedimientos. Una dirección física es un número binario que representa un emplazamiento en una memoria central 22 de la plataforma 12.

[0045] El periférico externo 16 comprende, por ejemplo, un soporte de almacenamiento de informaciones que permiten memorizar datos numéricos, por ejemplo, una clave USB, o un soporte de transferencia de informaciones que permiten intercambiar informaciones con la plataforma 12, por ejemplo, un enlace Ethernet.

[0046] El periférico 16 está conectado, por ejemplo, con la plataforma 12 por medio de un protocolo USB (del inglés *Universal Serial Bus*, traducido al español por *Bus Universal en Serie*) o por medio de un protocolo Ethernet.

[0047] El periférico 16 usa una pluralidad de zonas de memoria M1, M2.

[0048] Las zonas de memoria M1, M2, la estructura 24 y la zona de memoria específica 25 son capaces de memorizar datos.

[0049] El controlador de interfaz 30 puede conectar la plataforma 12 al periférico de hardware externo 16. El controlador de interfaz 30 puede igualmente conectar la plataforma 12 a otros periféricos de hardware externos como se presenta en la figura 4.

[0050] El controlador de interfaz 30 pertenece a la plataforma 12.

[0051] Como variante, el controlador de interfaz 30 está integrado en una aplicación App que se ejecuta en la plataforma 12.

[0052] A continuación, se describe el funcionamiento del dispositivo de control 10.

[0053] Inicialmente, el procedimiento de control comprende una etapa de suministro al dispositivo de control 10 de una política de seguridad que define los accesos autorizados o prohibidos a las zonas de memoria M1, M2 para la aplicación App.

[0054] Como complemento, el dispositivo de control 10 interroga a la unidad de gestión de memoria 18 para determinar si un acceso a una zona de memoria M1, M2 está autorizado o prohibido.

[0055] El procedimiento comprende asimismo una etapa de suministro al dispositivo de control 10 de una correspondencia entre el valor de un campo del mensaje y una dirección física @P1, @P2 de una zona de memoria M1, M2.

[0056] El procedimiento comprende a continuación la recepción del mensaje por el dispositivo de control 10.

[0057] A continuación, el dispositivo de control 10 convierte el cuerpo del mensaje en una o varias acciones para efectuar en una zona de memoria M1, M2.

[0058] Después, el dispositivo de control 10 comprueba la conformidad de cada acción con la política de seguridad tal como se describe a continuación.

[0059] El dispositivo de control 10 implementa la función de verificación de los mensajes de configuración de las transferencias, ilustrada por la referencia «CHECK» en las figuras 2 a 4.

[0060] La política de seguridad define, según un conjunto de reglas, la o las acciones autorizadas o prohibidas, de transferencia de datos hacia o desde un periférico externo 16 en cada zona de memoria M1, M2 para la aplicación App. Las acciones son, por ejemplo, la lectura de una zona de memoria M1, M2 o la escritura en una zona de memoria

M1, M2 por el controlador de interfaz 30.

[0061] La política de seguridad comprende al menos una de las reglas siguientes entre:

- una autorización o una prohibición, para la aplicación App, de escritura o de lectura en zonas de memoria M1, M2 usadas por el periférico 16, y
- una autorización o una prohibición, para el controlador de interfaz 30, de escritura o de lectura en zonas de memoria M1, M2 usadas por el periférico 16.

[0062] Dichas reglas se acoplan en su caso a un parámetro que conecta cada una de las reglas a un identificador del periférico de hardware externo 16 o a una dirección de una interfaz física de la plataforma 12.

[0063] Así, el dispositivo de control 10 adapta las reglas de control en función de la interfaz física en la que está conectado el periférico externo 16.

[0064] Ventajosamente, el dispositivo 10 trata simultáneamente varios periféricos externos 16, varias interfaces externas gestionadas por diferentes controladores de interfaz 30 o aprovecha varias estructuras de transferencia 24 o controla las autorizaciones de acceso para varias aplicaciones App. La figura 4 es un ejemplo de dicho modo de uso del dispositivo 10.

[0065] En los ejemplos de las figuras 1 a 4, la primera zona de memoria M1 está autorizada en lectura y en escritura por el controlador de interfaz 30 para transferencia hacia el periférico 16 y la segunda zona de memoria M2 no está autorizada ni en escritura ni en lectura por el controlador de interfaz 30 para transferencia hacia el periférico 16.

[0066] El procedimiento comprende, ventajosamente, una etapa de suministro al dispositivo de control 10 de la estructura 24.

[0067] La estructura 24 comprende, por ejemplo, el número de zonas de memoria M1, M2, el volumen de datos memorizables en cada zona de memoria M1, M2 o el volumen de datos memorizados en cada zona de memoria M1, M2 o la asociación de cada memoria M1, M2 a una interfaz física gestionada por el controlador de interfaz 30 o el identificador del periférico externo 16.

[0068] La etapa de suministro al dispositivo de control 10 de la estructura 24 puede referirse a varias estructuras 24 como se representa en la figura 4.

[0069] Además, el procedimiento de control comprende una etapa de verificación por el dispositivo de control 10 del mensaje y de realización de una o varias acciones de control en una zona de memoria M1, M2 para el periférico 16.

[0070] La verificación se efectúa por medio de una tabla de reglas memorizada en una memoria del dispositivo de control 10. La etapa de verificación permite determinar las acciones no conformes con la política de seguridad, por ejemplo, las acciones relativas a la escritura y/o a la lectura de una zona de memoria prohibida.

[0071] A continuación, el procedimiento de control comprende una etapa de bloqueo de los mensajes de configuración controlados en la estructura 24 por el dispositivo de control 10.

[0072] Por ejemplo, la etapa de bloqueo es implementada por una configuración de la unidad de gestión de memoria 18 que prohíbe cualquier modificación en la zona de memoria M1, M2 en la que se memoriza el o los mensajes controlados. Como variante, la etapa de bloqueo es realizada por cálculo del motivo de integridad del o de los mensajes controlados. El motivo de integridad es opcionalmente un motivo criptográfico y se memoriza en una zona de memoria específica 25 accesible solo por el dispositivo 10.

[0073] Además, el procedimiento comprende, cuando se realiza la acción de bloqueo, una etapa de desbloqueo. Según la elección de implementación de la etapa de bloqueo, el desbloqueo se implementa por

- una reconfiguración de la unidad de gestión de memoria 18 después de que el controlador de interfaz 30 haya realizado la transferencia del mensaje en la primera zona de memoria M1, y
- un control del motivo de integridad antes de la transferencia del mensaje en la primera zona de memoria M1 por el controlador de interfaz 30.

[0074] Para que las etapas de verificación y de bloqueo estén sincronizadas, el dispositivo 10 controla de manera permanente el progreso de los tratamientos del controlador de interfaz 30 y, llegado el caso, suspende y relanza los tratamientos del controlador de interfaz 30.

[0075] Cuando la acción de verificación detecta una no conformidad con respecto a la política de seguridad, el dispositivo de control 10 interrumpe la transferencia. El mensaje no es tratado así por el controlador de interfaz 30 y la transferencia no se efectúa.

[0076] Opcionalmente, el dispositivo de control 10 hace activarse una alerta o una notificación que permite que el sistema operativo sea informado de la no conformidad de una acción. Dicha alerta o notificación permite, por ejemplo, detectar ataques informáticos o disfuncionamientos y refuerza así la seguridad de la transferencia de datos.

[0077] Así, el dispositivo de control 10 asegura una protección suplementaria durante las transferencias de mensajes por acceso directo entre una aplicación App que se ejecuta en una plataforma 12 y zonas de memoria M1, M2 usadas para transferencias hacia periféricos de hardware externos 16.

[0078] En una realización ventajosa, el dispositivo de control 10 implementa las etapas siguientes.

[0079] Cuando se define la estructura 24 y el controlador de interfaz 30 es instado por el controlador de interfaz 19 para iniciar la transferencia, el controlador de interfaz 19 comunica al controlador de interfaz 30, por medio de registros del controlador de interfaz 30, la dirección del primer mensaje de configuración. Dicha dirección es, por ejemplo, denotada como «@ controler_init».

[0080] El dispositivo 10 controla de forma permanente el controlador de interfaz 30. El dispositivo 10 detecta así la activación del controlador de interfaz 30 con la dirección @ controler_init.

[0081] El dispositivo 10 realiza entonces las operaciones de inicialización siguientes:

- ○ detención del controlador 30 que no trata así la solicitud del controlador de interfaz 19,
- ○ análisis de la estructura 24 y en particular reglas de acceso a la estructura 24,
- ○ verificación de que la dirección @ controler_init está definida en las reglas de acceso de la estructura 24,
- ○ verificación del mensaje de configuración situado en la dirección @ controler_init,
- ○ realización opcional de una verificación de los mensajes de configuración situados en otras direcciones, y
- ○ si no se detecta ninguna alerta, rearranque del controlador de interfaz 30.

[0082] Como continuación a las operaciones de inicialización en la dirección @ controler_init, el dispositivo 10 asegura las operaciones de control de la verificación de los mensajes de configuración en al menos una dirección de la estructura 24. La dirección de la estructura 24 se denota, por ejemplo, por «@ verify». Para ello, el dispositivo de control 10 controla:

- ○ que la dirección actual, denotada por «@ verify_current», del mensaje de configuración para verificar es estrictamente superior a la dirección actual, denotada por «@ controler_current» del mensaje de configuración para tratar por el controlador de interfaz 30. Si esta propiedad no se verifica, el dispositivo 10 detiene el controlador de interfaz 30 y realiza las operaciones de verificación de los mensajes de configuración hasta que la dirección actual «@ verify_current» del mensaje de configuración para verificar sea estrictamente superior a la dirección actual «@ controler_current» del mensaje de configuración para tratar por el controlador de interfaz 30.
- ○ que la dirección actual @ verify_current del mensaje de configuración para verificar por el dispositivo 10 está contenida estrictamente en las reglas de acceso a la estructura 24. Si esta propiedad no se cumple, el dispositivo 10 genera una alerta.
- ○ que la desviación entre la dirección actual @ controler_current del mensaje de configuración para tratar por el controlador de interfaz 30 y la dirección de configuración del mensaje de configuración que el controlador de interfaz 30 ha tratado anteriormente, denotada por «@ controler_previous» es estrictamente igual a una unidad de dirección en las reglas de acceso de la estructura 24. Si esta propiedad no se cumple, el dispositivo 10 reinicia las operaciones de inicialización en la dirección @ controler_init descrita anteriormente considerando que la dirección @ controler_init es igual a la dirección actual @ controler_current.

[0083] La implementación del procedimiento es sencilla de realizar en la práctica ya que no se efectuará ninguna modificación en los procesadores, los periféricos de hardware y el software de aplicación existente.

[0084] Así, el procedimiento puede estar integrado en numerosos tipos de arquitecturas que se apoyan tanto en hardware como en software sin tener que modificarlos.

[0085] Así, el procedimiento permite cubrir los riesgos de fugas de datos durante los intercambios con periféricos externos.

[0086] El dispositivo de control 10 es independiente de la plataforma 12 y del periférico de hardware 16.

[0087] Además, el dispositivo de control 10 puede realizarse en forma de hardware o de software. El dispositivo

de control 10 puede configurarse además de manera que permita tener en cuenta fácilmente nuevos ataques y/o amenazas.

[0088] El experto en la materia comprenderá que la invención no se limita a la realización descrita en la figura 1, ni a los ejemplos concretos de la descripción. Otra variante consiste, por ejemplo, en combinar uno o varios ejemplos descritos anteriormente.

REIVINDICACIONES

1. Procedimiento de control sistemático por un dispositivo de control (10) de al menos un mensaje de configuración de transferencia, siendo el mensaje de configuración de transferencia un mensaje de configuración de una transferencia por acceso directo desde una aplicación (App) que se ejecuta en una plataforma (12) hacia una zona de memoria (M1, M2) usada por al menos un periférico de hardware externo (16), comprendiendo la plataforma (12) una o varias interfaces físicas, de manera que el periférico (16) está conectado con la plataforma (12) por medio de una o varias interfaces físicas de la plataforma (12), el periférico (16) usa una pluralidad de zonas de memoria (M1, M2), cada zona de memoria (M1, M2) está **caracterizada por** una dirección física única (@P1, @P2), el mensaje de configuración de una transferencia comprende al menos un campo y un cuerpo, el campo refiere una dirección física de una zona de memoria (M1, M2), el dispositivo de control (10) pertenece a la plataforma (12) e implementa al menos una de las funciones siguientes:

- una función de verificación (CHECK),
- una función de sincronización (SYNCHRO),
- una función de bloqueo (FREEZE),
- una función de alerta (ALERT), y
- una función de configuración del dispositivo de control (10) con una política de seguridad,

de manera que el procedimiento es implementado por el dispositivo de control (10) y comprende al menos las etapas siguientes:

- suministro al dispositivo de control (10) de una política de seguridad que define las direcciones de las zonas de memoria (M1, M2) autorizadas para la aplicación (App),
- suministro al dispositivo de control (10) de una correspondencia entre el valor de un campo del mensaje y una dirección física (@P1, @P2) de una zona de memoria (M1, M2),
- suministro de una estructura (24) de control de las transferencias en la que el mensaje de configuración es apto para ser memorizado, usándose la estructura (24) para realizar transferencias de datos en una primera zona de memoria (M1), respectivamente en una segunda zona de memoria (M2), por acceso directo a una dirección física (@P1) de la primera zona de memoria (M1), respectivamente a una dirección física (@P2) de la segunda zona de memoria (M2), referidas en la estructura (24),
- recepción del mensaje por el dispositivo de control (10),
- conversión por el dispositivo de control (10) del cuerpo del mensaje en una o varias acciones para efectuar en una zona de memoria (M1, M2), y
- prueba por el dispositivo de control (10) de la conformidad de cada acción con la política de seguridad y emisión de una notificación cuando una acción no está de acuerdo con la política de seguridad.

2. Procedimiento según la reivindicación 1, en el que la plataforma (12) comprende un hipervisor, de manera que el dispositivo de control (10) forma parte del hipervisor.

3. Procedimiento según la reivindicación 1 o 2, en el que la estructura (24) se usa igualmente durante la implementación de la prueba de conformidad.

4. Procedimiento según cualquiera de las reivindicaciones 1 a 3, en el que la política de seguridad comprende al menos una de las reglas siguientes:

- autorización de escritura en zonas de memoria (M1, M2) usadas por el periférico (16),
- prohibición de escritura en zonas de memoria (M1, M2) usadas por el periférico (16),
- autorización de lectura de zonas de memoria (M1, M2) usadas por el periférico (16), y - prohibición de lectura de zonas de memoria (M1, M2) usadas por el periférico (16).

5. Procedimiento según cualquiera de las reivindicaciones 1 a 4, en el que el periférico (16) está conectado con la plataforma (12) por medio de un protocolo USB o un protocolo Ethernet.

6. Procedimiento según cualquiera de las reivindicaciones 1 a 5, comprendiendo la plataforma (12) un controlador de interfaz (30) corriente arriba del dispositivo de control (10) y capaz de efectuar la o las acciones, comprendiendo el procedimiento igualmente al menos una de las etapas siguientes:

- si la acción sometida a prueba está de acuerdo con la política de seguridad, el mensaje se comunica al controlador de interfaz (30) y la acción se efectúa, y
- si la acción sometida a prueba no está de acuerdo con la política de seguridad, el mensaje no se comunica al controlador de interfaz (30) y la acción no se efectúa.

7. Procedimiento según la reivindicación 6, en el que el controlador de interfaz (30) pertenece a la plataforma (12) o está integrado en una aplicación (App) que se ejecuta en la plataforma (12).

8. Dispositivo de control (10) adaptado para la implementación de un procedimiento de control sistemático por un dispositivo de control (10) de al menos un mensaje de configuración de transferencia, siendo el mensaje de configuración de transferencia un mensaje de configuración de una transferencia por acceso directo desde una aplicación (App) que se ejecuta en una plataforma (12) hacia una zona de memoria (M1, M2) usada por al menos un periférico de hardware externo (16), comprendiendo la plataforma (12) una o varias interfaces físicas, de manera que el periférico (16) está conectado con la plataforma (12) por medio de una o varias interfaces físicas de la plataforma (12), el periférico (16) usa una pluralidad de zonas de memoria (M1, M2), cada zona de memoria (M1, M2) está **caracterizada por** una dirección física única (@P1, @P2), el mensaje de configuración de una transferencia comprende al menos un campo y un cuerpo, el campo refiere una dirección física de una zona de memoria (M1, M2), el dispositivo de control (10) pertenece a la plataforma (12) e implementa al menos una de las funciones siguientes:

- una función de verificación (CHECK),
- una función de sincronización (SYNCHRO),
- una función de bloqueo (FREEZE),
- una función de alerta (ALERT), y
- una función de configuración del dispositivo de control (10) con una política de seguridad,

siendo el dispositivo de control (10) capaz de implementar al menos las etapas siguientes:

- recepción de una política de seguridad que define las direcciones de las zonas de memoria (M1, M2) autorizadas para la aplicación (App),
- recepción de una correspondencia entre el valor de un campo del mensaje y una dirección física (@P1, @P2) de una zona de memoria (M1, M2),
- recepción de una estructura (24) de control de las transferencias en la que el mensaje de configuración es apto para ser memorizado, de manera que la estructura (24) se usa para realizar transferencias de datos en una primera zona de memoria (M1), respectivamente en una segunda zona de memoria (M2), por acceso directo a una dirección física (@P1) de la primera zona de memoria (M1), respectivamente a una dirección física (@P2) de la segunda zona de memoria (M2), referidas en la estructura (24),
- recepción del mensaje,
- conversión del cuerpo del mensaje en una o varias acciones para efectuar en una zona de memoria (M1, M2), y
- prueba de la conformidad de cada acción con la política de seguridad y emisión de una notificación cuando una acción no está de acuerdo con la política de seguridad.

9. Producto de programa informático que incluye instrucciones de software, de manera que las instrucciones de software implementan un procedimiento según cualquiera de las reivindicaciones 1 a 7, cuando las instrucciones de software son ejecutadas por una plataforma.

10. Soporte de informaciones en el que se memoriza un producto de programa informático según la reivindicación 9.

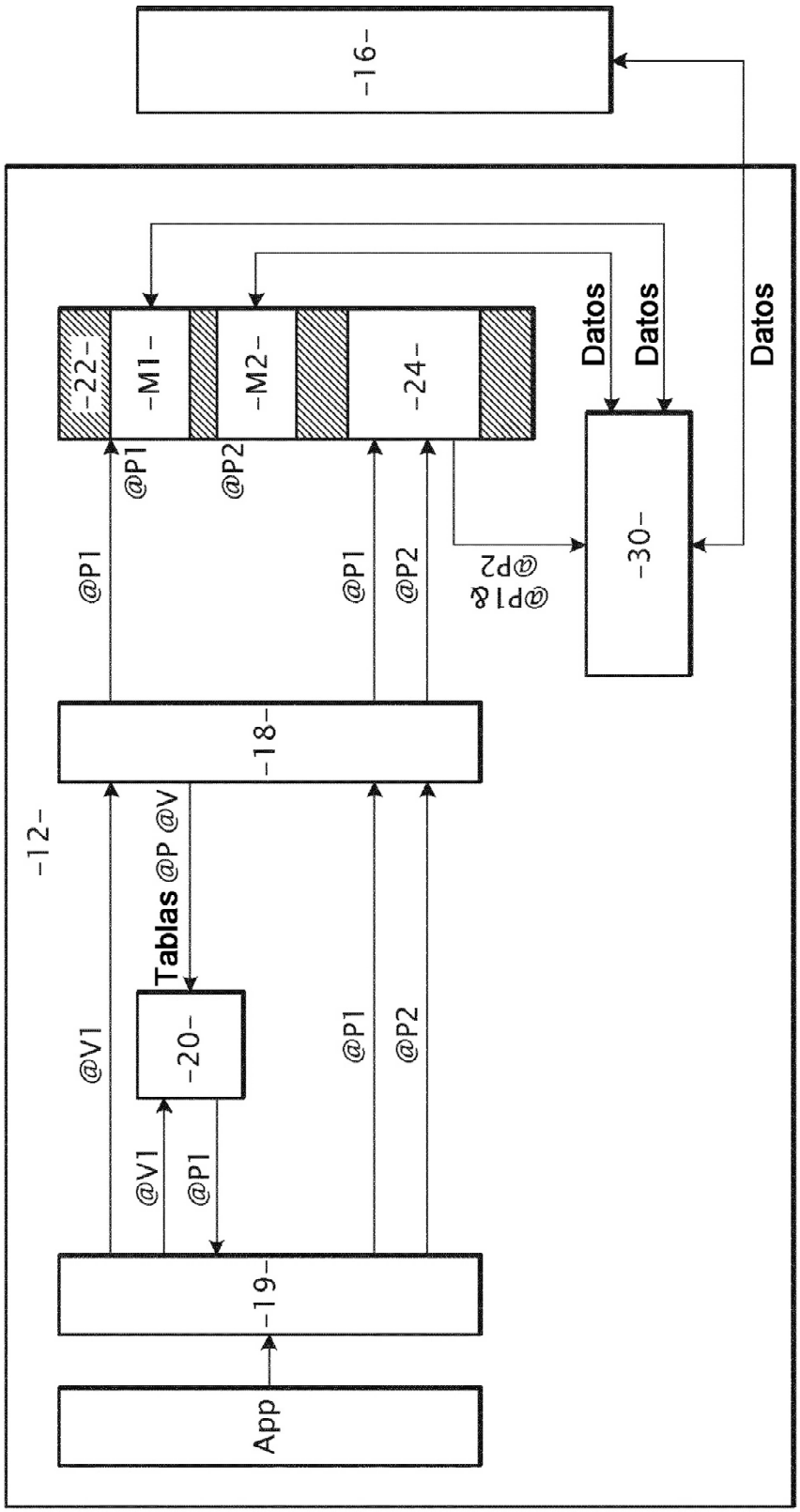

-16-
-12-
-22-
-M1-
-M2-
-24-
Datos
Datos
Datos
@P1
@P2
@P1
@P2
@P1&
@P2
-30-
-18-
Tablas @P @V
-20-
@V1
@P1
@V1
@P1
@P1
@P2
-19-
App

FIG.1

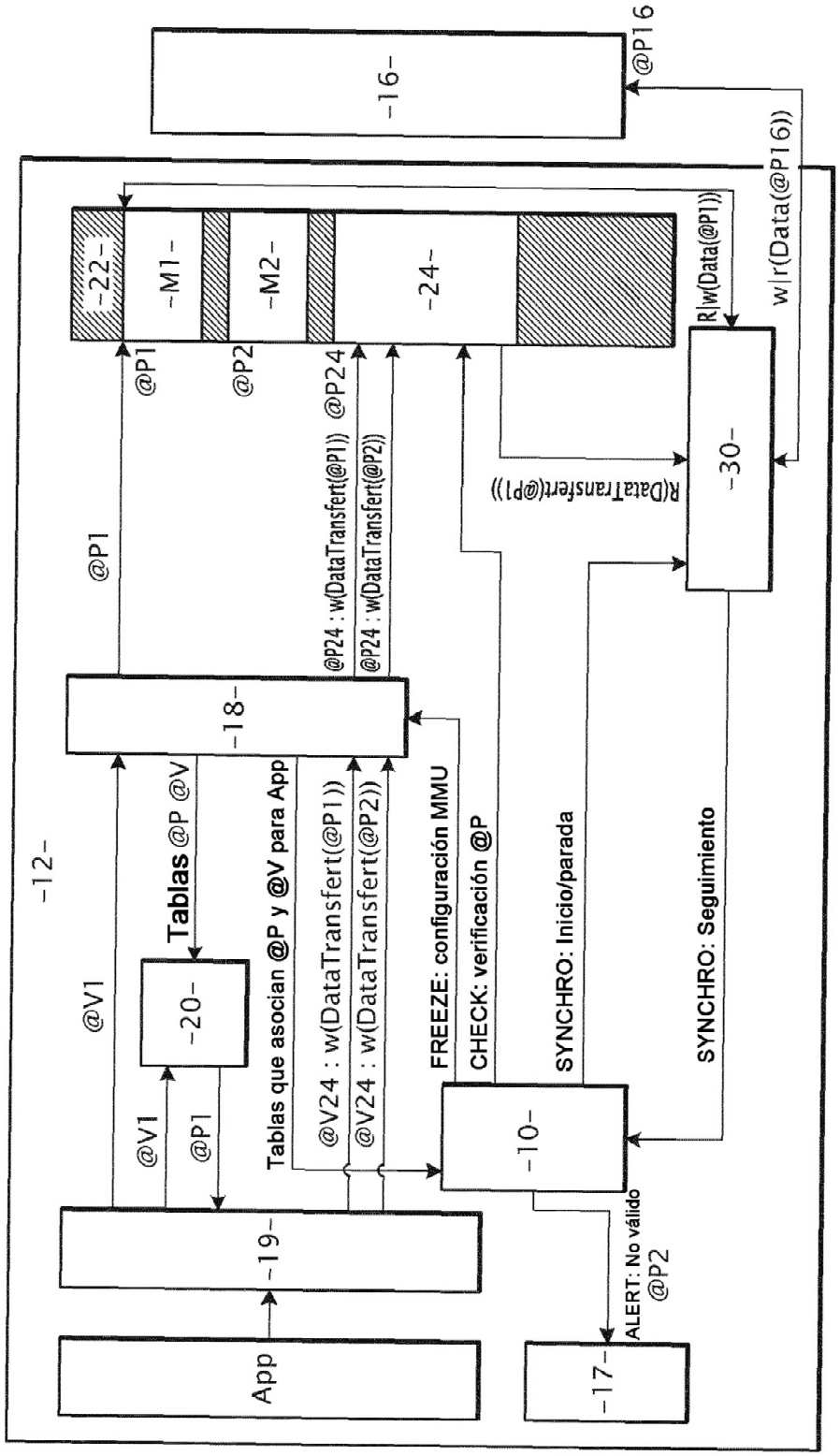

-16-
@P16
w|r(Data(@P16))
-22-
-M1-
-M2-
-24-
R|w(Data(@P1))
@P1
@P2
@P24
@P24 : w(DataTransfert(@P1))
@P24 : w(DataTransfert(@P2))
R(DataTransfert(@P1))
-30-
@P1
-18-
-12-
Tablas @P @V
@V1
-20-
Tablas que asocian @P y @V para App
@V24 : w(DataTransfert(@P1))
@V24 : w(DataTransfert(@P2))
FREEZE: configuración MMU
CHECK: verificación @P
SYNCHRO: Inicio/parada
SYNCHRO: Seguimiento
@V1
@P1
-10-
-19-
App
ALERT: No válido
@P2
-17-

FIG.2

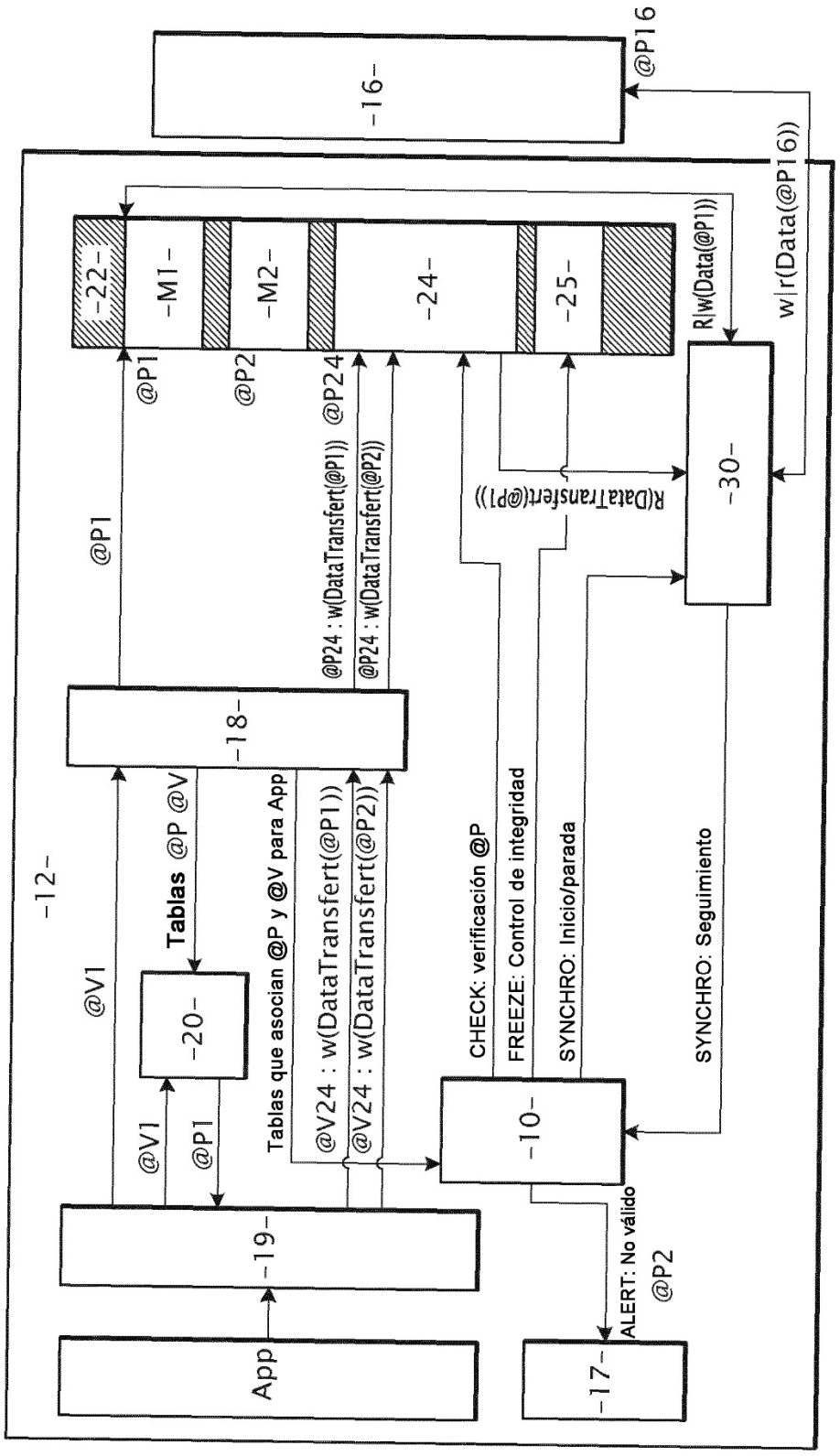
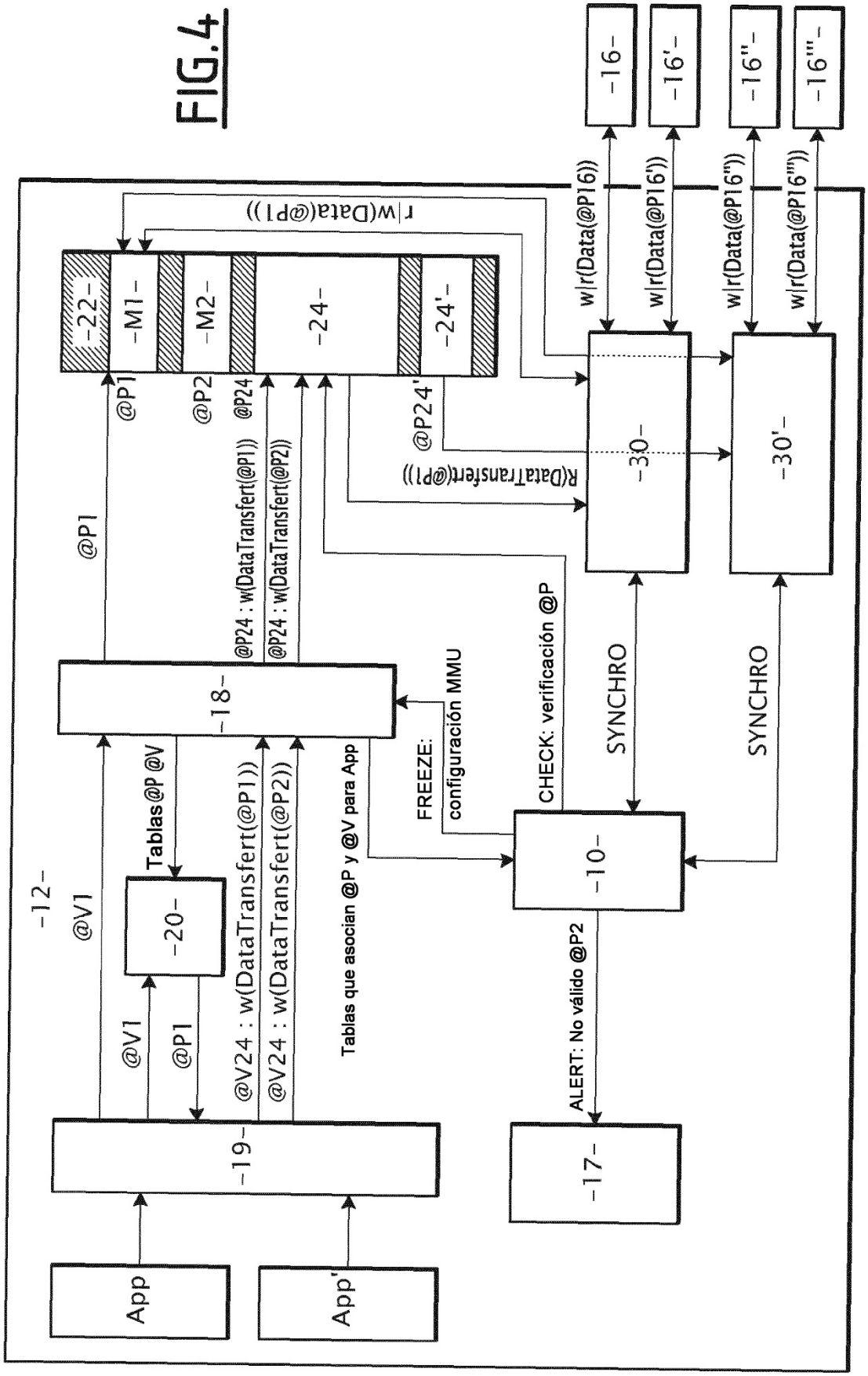

-16-
@P16
w|r(Data(@P16))
-22-
-M1-
-M2-
-24-
-25-
R|w(Data(@P1))
@P1
@P2
@P24
@P24 : w(DataTransfert(@P1))
@P24 : w(DataTransfert(@P2))
R(DataTransfert(@P1))
-30-
-18-
-12-
@V1
Tablas @P @V
Tablas que asocian @P y @V para App
@V24 : w(DataTransfert(@P1))
@V24 : w(DataTransfert(@P2))
CHECK: verificación @P
FREEZE: Control de integridad
SYNCHRO: Inicio/parada
SYNCHRO: Seguimiento
-20-
@V1
@P1
-10-
-19-
App
ALERT: No válido
@P2
-17-

FIG.3

FIG.4


-12-
@V1
-20-
Tablas @P @V
-18-
-19-
App
App'
-10-
-17-
-30-
-30'-
-16-
-16'-
-16''-
-16'''-
-22-
-M1-
-M2-
-24-
-24'-
@P1
@P2
@P24
@P24'
@V1
@P1
@V24 : w(DataTransfert(@P1))
@V24 : w(DataTransfert(@P2))
@P24 : w(DataTransfert(@P1))
@P24 : w(DataTransfert(@P2))
Tablas que asocian @P y @V para App
FREEZE:
configuración MMU
CHECK: verificación @P
SYNCHRO
SYNCHRO
ALERT: No válido @P2
r|w(Data(@P1))
R(DataTransfert(@P1))
w|r(Data(@P16))
w|r(Data(@P16'))
w|r(Data(@P16''))
w|r(Data(@P16'''))