(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 606 006**

(51) Int. CI.:

G06F 11/10 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **07.07.2011 PCT/EP2011/061457**

(87) Fecha y número de publicación internacional: **09.02.2012 WO12016781**

(96) Fecha de presentación y número de la solicitud europea: **07.07.2011 E 11733633 (9)**

(97) Fecha y número de publicación de la concesión europea: **31.08.2016 EP 2601581**

(54) Título: **Elemento de control de memoria y procedimiento de configuración asociado**

(30) Prioridad:

05.08.2010 AT 13262010

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.03.2017

(73) Titular/es:

SIEMENS AG ÖSTERREICH (100.0%)
Siemensstrasse 90
1210 Wien, AT

(72) Inventor/es:

EPPENSTEINER, FRIEDRICH;
GHAMESHLU, MAJID y
TAUCHER, HERBERT

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Elemento de control de memoria y procedimiento de configuración asociado

Campo técnico

La presente invención se refiere en general al campo de la tecnología informática y sus componentes electrónicos y módulos. La presente invención se refiere a un elemento de control de memoria que se puede emplear en un sistema de ordenador y que en un primer lado comprende al menos una interfaz de usuario con un circuito controlador asociado y en un segundo lado una interfaz con manejo de protocolo para la conexión de al menos un elemento de memoria del sistema informático. En el elemento de control de memoria está previsto para un control de acceso también un circuito digital para una asignación de recursos de acceso - un llamado árbitro. Además, la invención se refiere a un procedimiento correspondiente para la configuración del elemento de control de memoria según la invención.

Estado de la técnica

El campo de la tecnología informática que incluye por ejemplo ámbitos como la tecnología digital y la microelectrónica, se dedican a la concepción y la construcción de instalaciones o sistemas que procesan información o datos - los llamados ordenadores o sistemas informáticos. En un sistema informático, por una unidad de procesamiento central (CPU / Central Processing Unit) son ejecutados programas, comandos (por ejemplo, partes de código) y/o datos útiles asociados a programas, que forman la base de aplicaciones puestas a disposición por el sistema informático, o por otras unidades periféricas (por ejemplo, tarjetas de red, tarjetas de sonido, etc.), por vía de un llamado controlador de acceso directo a memoria (controlador DMA), se accede a programas y/o a datos útiles que han de ser procesados.

Estos programas así como los datos útiles que han de ser procesados se depositan como datos en un elemento de memoria - la llamada memoria central - para poder ser llamados en un momento posterior. A diferencia de un elemento de memoria permanente, no volátil (por ejemplo, EPROM, EEPROM, etc.), a la memoria central puede producirse un acceso mucho más rápido por ejemplo por la CPU o el controlador DMA, pero la memoria central no tiene la capacidad de que se mantengan datos en caso de un corte de corriente. Como memoria central se usan en la actualidad por ejemplo elementos de memoria como por ejemplo SDRAM DDR2 o DDR3 o elementos de memoria DDR móviles que permiten un procesamiento rápido de datos. La abreviatura DDR corresponde a Double Data Rate y la de SDRAM corresponde a Synchronous Dynamic Random Access Memory.

Para una regulación de un flujo de datos entre un elemento de memoria como una memoria central y una o varias unidades como por ejemplo CPU, unidades periféricas vía DMA, en un sistema informático se usa habitualmente un elemento de control de memoria que también se denomina controlador de memoria. El elemento de control de memoria constituye un módulo propio e incluye funciones para leer y escribir la memoria central (por ejemplo, DRAM, SDRAM DDR, etc.). El elemento de control de memoria garantiza también una actualización permanente de la memoria central, el llamado refrescamiento, ya que, en caso contrario, se perderían los datos en la memoria central volátil.

Para la regulación de los accesos a la memoria central, el elemento de control de memoria presenta un circuito digital propio para una asignación de recursos de acceso - el llamado árbitro o la llamada lógica de arbitración. Por el árbitro se solucionan y se priorizan conflictos o colisiones de acceso. Esto es necesario por ejemplo cuando, a través del elemento de control de memoria, varias unidades tales como CPU, controladores DMA, etc., pueden acceder como llamados maestros - es decir, activamente - a un elemento de memoria como la memoria central.

El circuito digital para una asignación de los controles de acceso, es decir, el árbitro, decide entonces a qué maestro se concede acceso. Por arbitración se entiende por tanto una asignación de recursos de acceso (por ejemplo, canales de comunicación, bus de datos, sistemas de bus, etc.) a las diferentes unidades maestras. Por lo tanto, el árbitro es una instancia dentro del elemento de control de memoria, por el que se regula qué hardware es el siguiente en poder utilizar un canal de datos (el llamado bus).

Las unidades maestras - es decir, CPU y/o controladores DMA de unidades periféricas están conectadas - en un primer lado a través de interfaces de usuario con circuitos controladores asociados - los llamados puertos de usuario - al elemento de control de memoria. En un segundo lado, el elemento de control de memoria presenta una conexión a través de una interfaz con manejo de protocolo a uno o varios elementos de memoria o a la memoria central.

Por una parte, una creciente integración de funcionalidades en estructuras semiconductoras o componentes cada vez más pequeños, por los que quedan formadas unidades como por ejemplo la CPU, el controlador de memoria, la memoria central, etc. de un sistema informático, puede aumentar por ejemplo una probabilidad de errores. Esto puede conducir sobre todo a falsificaciones de datos transientes especialmente dentro de elementos de memoria

como por ejemplo memorias centrales. Estas falsificaciones de datos pueden ser provocadas por ejemplo por radiación cósmica y/o por electromigración. Las falsificaciones de datos pueden conducir a errores como por ejemplo los llamados errores de un solo bit, errores de bit múltiple etc. en datos depositados en memorias centrales y/o en datos /por ejemplo partes de código) durante la transferencia a la memoria central.

Por otra parte, especialmente en cuanto a los sistemas informáticos y aplicaciones relevantes para la seguridad, como por ejemplo en la industria automovilística, en la aeronáutica, etc., existen requerimientos cada vez más severas en cuanto a la seguridad de datos. Sobre todo los datos relevantes para la seguridad deben transferirse y almacenarse con una alta fiabilidad o con la menor tasa de errores posible. Para ello, por ejemplo en la normalización internacional según IEC61508 se definen llamados niveles de requerimientos de seguridad o niveles de integridad de seguridad (SIL). De los niveles de integridad de seguridad a los que se aspira respectivamente resultan principios orientados a la seguridad que han de cumplirse para minimizar un riesgo de fallos de funcionamiento. La IEC61508 es una norma internacional para el desarrollo de sistemas eléctricos, electrónicos y electrónicos programables, por los que es realizada una función de seguridad, y se emite por la Comisión Electrotécnica Internacional (IEC). En sistemas o aplicaciones relevantes para la seguridad, por ejemplo se aspira al cumplimiento de los requerimientos de la llamada SIL3 o SIL4 de la IEC61508.

Para la detección o la corrección de errores de datos como un error de un solo bit que se detectan independientemente entre sí se emplean por ejemplo procedimientos como el procedimiento de código de corrección de errores (procedimiento ECC). El procedimiento ECC es un algoritmo de corrección de errores que se emplea en elementos de memoria para el aseguramiento contra la falsificación de datos. De esta manera, se detectan habitualmente errores de un solo bit durante la lectura de los datos y se corrigen durante la entrega a un maestro que accede. Adicionalmente, con este procedimiento también se pueden detectar errores múltiples. Sin embargo, la detección de errores múltiples en los datos en un momento en el que estos ya son precisados por una aplicación no corresponde a los elevados requerimientos de seguridad para sistemas o aplicaciones relevantes para la seguridad, porque ya no se puede reaccionar con la rapidez suficiente a los estados de error producidos. Por ejemplo, ya no se puede realizar con la rapidez adecuada un cambio de sistema a un estado seguro.

Una problemática similar resulta durante un arranque de un sistema informático o de una aplicación. Durante ello, partes de código o de programa se copian de una memoria permanente (por ejemplo, EEPROM, etc.) a una memoria volátil (por ejemplo, DRAM, SDRAM DDR, etc.). En sistemas relevantes para la seguridad o conformes con la seguridad, para la comprobación de errores de las partes de código transferidas se emplean por ejemplo rutinas de software. Estas rutinas de software leen periódicamente partes de código por templo durante el arranque y las comprueban mediante una comprobación cíclica de redundancia - el llamado Cyclic Redundancy Check (CRC) - en cuanto a errores de un solo bit y errores de bit múltiple. La CRC está concebida de tal forma que se descubran con una alta probabilidad errores durante la transferencia de datos. La rutina de software por ejemplo forma un llamado bloque CRC y lo compara con un valor CRC teórico predefinido. Sin embargo, este procedimiento conduce a una reducción del rendimiento del sistema informático, especialmente de la CPU, y a una considerable carga de los canales de comunicación del sistema - especialmente en los llamados sistemas de un solo chip en los que todas o una gran parte de las funciones del sistema están integradas en una plataforma o en un chip.

La publicación US-A-2010/0185897 corresponde al preámbulo de la reivindicación 1.

Exposición de la invención

Por lo tanto, la invención tiene el objetivo de proporcionar un elemento de control de memoria según la reivindicación 1 que se pueda emplear en un sistema informático, así como un procedimiento asociado para la configuración del elemento de control de memoria, mediante los que de manera sencilla sean posibles una comprobación a tiempo de datos o de áreas de datos predefinidas, en cuanto a falsificaciones del contenido de memoria, cumpliendo altos requisitos de seguridad y sin reducción del rendimiento.

Este objetivo se consigue mediante un elemento de control de memoria del tipo indicado al principio, estando prevista una interfaz de seguridad adicional hacia un circuito de comprobación que está preparado para comprobar datos (por ejemplo, datos almacenados, partes de código almacenadas, etc.) en cuanto a falsificaciones, especialmente en cuanto a llamadas falsificaciones y errores transientes (por ejemplo, errores múltiples, errores de bloque CRC, etc.) que pueden producirse respectivamente dentro de módulos de memoria, para corregir errores detectados y/o para provocar en caso de excederse umbrales de error ajustables un cambio del sistema a un estado seguro.

El aspecto principal de la solución propuesta consiste en que contenidos de memoria como por ejemplo datos, partes de código, etc., se comprueban de forma precoz en cuanto a su consistencia. Falsificaciones producidas por ejemplo por electromigración, radiaciones cósmicas etc. y que pueden conducir a errores de contenidos de memoria (por ejemplo, errores de un solo bit, errores de bit múltiple, errores de bloque CRC, etc.) son detectados ya por el hardware y por tanto se identifica de manera precoz un posible fallo de comportamiento de aplicaciones o del sistema. De esta manera, mediante el uso del elemento de control de memoria según la invención puede

mantenerse estable o incluso incrementarse el rendimiento del sistema. Adicionalmente, se cumplen mejor también elevados requisitos de seguridad como por ejemplo el nivel de integridad de seguridad (SIL) 2, 3 o 4 según la normalización internacional según IEC61508, ya que se pueden corregir errores individuales como por ejemplo un error de un solo bit y el sistema conmuta más rápidamente a un estado seguro en caso de errores como por ejemplo numerosos errores de un solo bit, errores múltiples, errores de bloque CRC.

Resulta ventajoso si está prevista una ventana de dirección de memoria ajustable, dentro de la que estén ajustados como comprobables datos o partes de código para la interfaz de seguridad y el circuito de comprobación. De esta manera, para la interfaz de seguridad y el circuito de comprobación asociado se predefine un área de memoria, dentro de la que datos y/o partes de código que por ejemplo durante el arranque de un sistema se copian de un elemento de memoria permanente (por ejemplo, EEPROM, etc.) a un elemento de memoria volátil (por ejemplo, DRAM, SRAM DDR, etc.), se comprueban en cuanto a falsificaciones y/o errores como por ejemplo errores de un solo bit, errores de bit múltiple, errores de bloque CRC, etc. De esta manera, la comprobación se puede limitar de manera sencilla en cuanto a los datos y/o las partes de código relevantes para la seguridad.

También resulta ventajoso si al exceder uno de los umbrales de error ajustables se puede disparar una alarma. De esta manera, al emplear el elemento de control de memoria según la invención en un sistema se pueden conseguir mejor y de manera sencilla diferentes requisitos de seguridad como por ejemplo niveles de integridad de seguridad (por ejemplo, SIL2, SIL3, etc.).

En una forma de realización preferible del elemento de control de memoria según la invención está previsto que se puede ajustar una duración de tiempo para la comprobación de la ventana de dirección de memoria en la interfaz de seguridad y el circuito de comprobación asociado. Mediante un ajuste de la duración de tiempo dentro de la que debe concluir habitualmente periódicamente la comprobación del área de memoria predefinida, se pueden conseguir mejor también diferentes requisitos de seguridad como por ejemplo niveles de integridad de seguridad (por ejemplo, SIL2, SIL3, etc.) importantes por ejemplo en sistemas relevantes para la seguridad en ámbitos como por ejemplo la industria automovilística, la industria o la aeronáutica. Adicionalmente, de esta manera se detectan de manera precoz falsificaciones y errores en datos y/o partes de códigos relevantes para la seguridad. Por lo tanto, el sistema puede reaccionar rápidamente y conmutar a un estado seguro.

En otra forma de realización del elemento de control de memoria según la invención también resulta ventajoso si la comprobación de la ventana de dirección de memoria puede ser realizada periódicamente por la interfaz de seguridad y el circuito controlador asociado.

El objetivo mencionado se consigue también mediante un procedimiento según la reivindicación 4, mediante el que el elemento de control de memoria según la invención se puede configurar de manera sencilla, siendo ajustada en la interfaz de seguridad y en el circuito de comprobación asociado la duración de tiempo de la comprobación de la ventana de dirección de memoria como valor teórico que se deduce por ejemplo de los requisitos de seguridad predeterminados para un sistema. El valor teórico se usa por ejemplo durante el funcionamiento para determinar una prioridad adecuada para la asignación de recursos de acceso - una llamada prioridad de árbitro - para la interfaz de seguridad y el circuito de comprobación asociado.

El aspecto principal del procedimiento para la configuración del elemento de control de memoria según la invención consiste en que en caso de un comportamiento no íntegramente conocido de aplicaciones en un sistema se predefine un valor teórico para la duración de tiempo de la comprobación. Este valor teórico se deduce por ejemplo de especificaciones y requisitos de seguridad para el sistema y debe perjudicar lo menos posible o solo ligeramente el rendimiento del sistema. La interfaz de seguridad y el circuito de comprobación asociado intentan alcanzar en un primer paso con la menor prioridad de árbitro el valor teórico de la duración de tiempo para la comprobación. Si no se alcanza el valor teórico de la duración de tiempo con esta prioridad de árbitro, la prioridad de árbitro es adaptada automáticamente por la interfaz o el circuito de comprobación asociado hasta que se cumpla el valor teórico.

En otra forma de realización, para la configuración del elemento de control de memoria también puede ser ventajoso que una duración de tiempo máxima para la comprobación de la ventana de dirección de memoria se deduzca de condiciones marco, especialmente de especificaciones de seguridad. Entonces, sobre la base de test o análisis empíricos se estiman secuencias de aplicaciones y características de arbitración de la interfaz de seguridad y del circuito de comprobación asociado y a partir de ello se determina la prioridad adecuada para la asignación de recursos de acceso, es decir, una prioridad de árbitro correspondiente, para la interfaz de seguridad y el circuito de comprobación asociado. Dicha prioridad de árbitro se parametriza entonces en el elemento de control de memoria según la invención.

De esta manera, la duración de tiempo para la comprobación se puede adaptar de manera ideal a las condiciones marco para el sistema correspondiente como por ejemplo especificaciones de seguridad, el comportamiento de aplicaciones en el sistema, características de arbitración de la interfaz de seguridad y del circuito de comprobación asociado etc. A partir de las condiciones marco y las características se puede determinar entonces de manera sencilla una prioridad de árbitro para la interfaz de seguridad y el circuito de comprobación asignado, en la que se

cumpla de forma segura la duración de tiempo máxima determinada para la comprobación. Dicha prioridad de árbitro se parametriza entonces fijamente en el elemento de memoria según la invención. De esta manera, la duración de tiempo de la comprobación se ajusta de forma indirecta a través de la prioridad de árbitro de la interfaz de seguridad y del circuito controlador asociado. De esta manera, se pueden conseguir mejor por una parte las especificaciones de seguridad y por otra parte se consigue mantener lo más reducida posible la influencia del rendimiento del sistema por el elemento de control de memoria según la invención. También existe la posibilidad de realizar en este procedimiento de configuración de forma separada entre sí los requisitos y los ajustes para la comprobación de datos y de códigos.

Breve descripción del dibujo

A continuación, la invención se describe a título de ejemplo con la ayuda de la figura 1 adjunta que muestra a título de ejemplo y esquemáticamente una estructura del primer elemento de control de memoria según la invención.

Realización de la invención

En la figura 1 está representado esquemáticamente y a título de ejemplo un elemento de control de memoria MC que comprende un circuito digital y elementos para controlar un flujo de datos de y a un elemento de memoria S. El elemento de control de memoria MC puede estar realizado como circuito integrado o chip o estar integrado en otro circuito integrado o chip.

Para una gestión de accesos de lectura y de escritura a un elemento de memoria S, el elemento de control de memoria MC presenta un circuito digital AR para una asignación de recursos de acceso (por ejemplo, canales de comunicación, bus de datos, sistema de bus, etc.). Este circuito digital AR se denomina por ejemplo también como llamado árbitro o lógica de arbitración, por el que se resuelven o se priorizan conflictos de acceso o colisiones de acceso al elemento de memoria S. Para ello, el árbitro AR da por ejemplo llamadas prioridades de árbitro para unidades maestras M1 a Mn que acceden al elemento de memoria S, como por ejemplo CPU, controladores DMA de unidades periféricas etc. El circuito digital AR o el árbitro AR es por tanto una instancia dentro del elemento de control de memoria MC, que regula cuál es la siguiente unidad de hardware o maestra M1 a Mn en poder utilizar un canal para transferencias de datos del/al elemento de memoria S.

Las unidades maestras M1 a Mn como por ejemplo CPU, controladores DMA, pueden conectarse en un primer lado 1 del elemento de control de memoria MC a través de interfaces de usuario UP1 a UPn con circuitos controladores UA1 a UAn asociados. Por las interfaces de usuario UP1 a UPn con circuitos controladores UA1 a UAn asociados, las unidades maestras M1 a Mn son conectadas al árbitro AR del elemento de control de memoria MC. Las interfaces de usuario UP1 a UPn con circuitos controladores UA1 a UAn asociados también se denominan como llamados puertos de usuario del elemento de control de memoria MC, que constituyen interfaces de hardware que son excitadas por vía de canales de comunicación (por ejemplo, sistema de bus, etc.) a través de llamadas direcciones de puerto. Para el control de acceso a la memoria, las interfaces de usuario UP1 a UPn con circuitos controladores UA1 a UAn asociados son arbitradas por el árbitro AR según diferentes procedimientos (por ejemplo prioridades, Round Robin, etc.).

En un segundo lado 2, el elemento de control de memoria MC presenta una conexión a través de una interfaz MPH con manejo de protocolo a al menos un elemento de memoria S. Dicho elemento de memoria S habitualmente es una llamada memoria volátil como por ejemplo DRAM, SDRAM DDR, etc., que se usan por ejemplo como llamadas memorias centrales en sistema informáticos.

Adicionalmente, el elemento de control de memoria MC presenta una interfaz de seguridad SP con un circuito de comprobación SA asociado. La interfaz de seguridad SP con el circuito de comprobación SA asociado que está conectado al circuito digital AR para una asignación de recursos de acceso, participa en la arbitración por el elemento de memoria S. La interfaz de seguridad SP así como el circuito de comprobación SA asociado están preparados para comprobar datos y/o partes de código por ejemplo en cuanta o a falsificaciones y errores transientes (por ejemplo, errores de un solo bit, errores de bit múltiple, errores de bloque CRC).

Puede estar predefinida una ventana de dirección de memoria ajustable, dentro de la que datos y/o partes de código son comprobados habitualmente periódicamente por la interfaz de seguridad SP con circuito de comprobación SA asociado. Es decir que puede estar definida un área de dirección - la ventana de dirección de memoria - del elemento de memoria S, en la que por ejemplo están almacenados datos y/o partes de código relevantes para la seguridad. Estos datos son examinados entonces en cuanto a errores por la interfaz de seguridad SP o el circuito de comprobación SA asociado. En el caso de datos, por ejemplo durante la comprobación por la interfaz de seguridad SP con circuito de comprobación SA asociado se pueden corregir errores de un solo bit encontrados. De esta manera, se evita que estos conduzcan posteriormente a errores múltiples. Una gran cantidad de errores de un solo bit o errores múltiples detectados ya no son corregidos por la interfaz de seguridad SP con circuito de comprobación SA asociado, sino que al excederse puntos de error ajustables se produce un cambio del sistema a un estado

seguro. Igualmente, los errores de bloque CRC durante la comprobación de partes de código por la interfaz de seguridad SP con circuito de comprobación SA asociado conducen a un cambio del sistema a un estado seguro. Adicionalmente, al excederse uno de los umbrales de error ajustables en el elemento de control de memoria MC también puede estar previsto que por ello se dispare una alarma.

Adicionalmente, en la interfaz de seguridad SP con circuito de comprobación SA asociado del elemento de control de memoria MC según la invención puede estar previsto que se pueda ajustar una duración de tiempo - un llamado período de chequeo - para la comprobación - habitualmente periódica - de la ventana de dirección de memoria. Esta duración de tiempo se puede determinar mediante un procedimiento para la configuración del elemento de control de memoria MC a partir de una estimación del comportamiento de aplicaciones y a partir de condiciones marco (por ejemplo, especificaciones de seguridad) para el sistema informático en el que se emplea el elemento de control de memoria MC.

Por ejemplo, si el comportamiento de las aplicaciones que se ejecutan en el sistema informático no es completamente conocido o evaluable, la duración de tiempo o el período de chequeo necesario para la comprobación se ajusta como valor teórico en la interfaz de seguridad SP con circuito de comprobación SA asociado, siendo deducido dicho valor teórico a partir de las especificaciones y los requisitos de seguridad para el sistema informático. A continuación, sobre la base del valor teórico se determina una prioridad de árbitro adecuada para la interfaz de seguridad SP con circuito de comprobación asociado SA. Durante la comprobación de datos y/o de partes de código, la interfaz de seguridad SP con circuito de comprobación SA asociado intenta en primer lugar alcanzar con la menor prioridad de árbitro el valor teórico del período de chequeo. Si no se cumple el valor teórico, la interfaz de seguridad SP con circuito de comprobación SA asociado incrementa la prioridad de árbitro automáticamente hasta que se alcance el valor teórico para la duración de tiempo o el período de chequeo. La menor prioridad de árbitro como prioridad de inicio o un incremento sucesivo de la prioridad de árbitro de la interfaz de seguridad SP con circuito de comprobación SA asociado se elige para que se influya lo menos posible en el rendimiento del sistema informático.

Si el comportamiento de aplicación en el funcionamiento real del sistema informático con el elemento de control de memoria MC según la invención se puede predecir o evaluar bien o si este se determinó por ejemplo con la ayuda de test y/o análisis empíricos, a partir de ello se puede deducir por ejemplo una duración de tiempo máxima para la comprobación de la ventana de dirección de memoria a partir de condiciones marco como por ejemplo especificaciones de seguridad. Durante ello, se tienen en consideración secuencias de aplicaciones cumpliendo todos los llamados "corner cases" así como diferentes características de arbitración de la interfaz de seguridad SP y del circuito de comprobación SA asociado. A partir de ello se determina entonces la prioridad de árbitro adecuada para la interfaz de seguridad SP y el circuito de comprobación SA asociado, con la que se pueda cumplir de manera segura la duración de tiempo máxima determinada para la comprobación (período de chequeo). Dicha prioridad de árbitro se parametriza entonces fijamente para un funcionamiento real en el elemento de control de memoria MC o en la interfaz de seguridad SP con circuito de comprobación SA asociado. Para el caso de que con la prioridad de árbitro ajustada se exceda una vez la duración de tiempo máxima para la comprobación, puede estar previsto por ejemplo en el elemento de control de memoria MC que se dispare una alarma.

De esta manera, con un comportamiento de aplicación evaluable, la duración de tiempo de la comprobación o el período de chequeo pueden optimizarse de forma indirecta a través de la prioridad de árbitro para la interfaz de seguridad SP con circuito de comprobación SA asociado y se puede optimizar la influencia del elemento de control de memoria MC en el rendimiento del sistema informático. Adicionalmente, se pueden cumplir también requisitos de seguridad exigidos o predefinidos, y ajustes para una comprobación de datos pueden realizarse por separado de una comprobación de partes de código.

REIVINDICACIONES

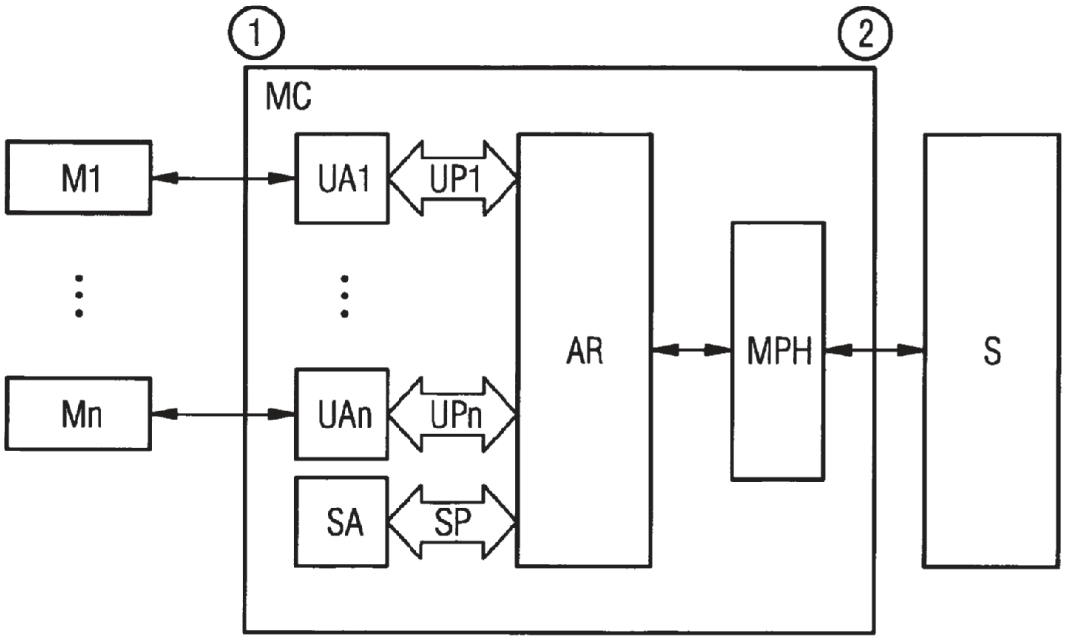
1. Elemento de control de memoria (MC) que se puede emplear en un sistema informático y que en un primer lado (1) en el que se pueden conectar unidades maestras (M1, …, Mn) del sistema informático comprende al menos una interfaz de usuario (UP1, …, UPn) con un circuito controlador (UA1, …, UAn) asociado y en un segundo lado (2) en el que se puede conectar al menos un elemento de memoria (S) del sistema informático comprende una interfaz (MPH) con manejo de protocolo hacia el elemento de memoria (S), y en el que para un control de acceso al elemento de memoria (S) está previsto un circuito digital (AR) para una asignación de recursos de acceso, **caracterizado porque** está prevista una interfaz de seguridad (SP) adicional hacia un circuito de comprobación (SA) que está preparado para comprobar datos en cuanto a falsificaciones y errores, corregir errores detectados y disparar una alarma en caso de excederse un umbral de error ajustable, y por que está prevista una ventana de dirección de memoria ajustable, dentro de la que datos para la interfaz de seguridad (SP) y el circuito de comprobación (SA) están ajustados como comprobables.

2. Elemento de control de memoria (MC) según la reivindicación 1, **caracterizado porque** se puede ajustar una duración de tiempo para la comprobación de la ventana de dirección de memoria en la interfaz de seguridad (SP) y en el circuito de comprobación (SA) asociado.

3. Elemento de control de memoria (MC) según una de las reivindicaciones 1 o 2, **caracterizado porque** la comprobación de la ventana de dirección de memoria puede ser realizada periódicamente por la interfaz de seguridad (SP) y el circuito de comprobación (SA) asociado.

4. Procedimiento para la configuración de un elemento de control de memoria (MC) según las reivindicaciones 1 a 3, **caracterizado porque** se ajusta una duración de tiempo de una comprobación de la ventana de dirección de memoria como valor teórico en la interfaz de seguridad (SP) y en el circuito de comprobación (SA) asociado, y a partir de ello se determina una prioridad adecuada para la asignación de recursos de acceso, una llamada prioridad de árbitro, para la interfaz de seguridad (SP) y el circuito de comprobación (SA) asociado.

5. Procedimiento para la configuración de un elemento de control de memoria (MC) según las reivindicaciones 1 a 4, **caracterizado porque** una duración de tiempo máxima para la comprobación de la ventana de dirección de memoria se deduce de condiciones marco, y por que entonces, sobre la base de test se determinan secuencias de aplicaciones teniendo en consideración características de arbitración de la interfaz de seguridad (SP) y del circuito de comprobación (SA) asociado, por que después, sobre la base de las secuencias de aplicación se determina la prioridad de árbitro adecuada para la interfaz de seguridad (SP) y el circuito de comprobación (SA) asociado, y por que entonces esta prioridad de árbitro determinada se parametriza fijamente.


1
2
MC
M1
Mn
UA1
UAn
SA
UP1
UPn
SP
AR
MPH
S