(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 626 982**

(51) Int. CI.:

G06F 21/53 (2013.01)
G06F 21/55 (2013.01)
G06F 21/85 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **21.12.2006 PCT/EP2006/070065**

(87) Fecha y número de publicación internacional: **28.06.2007 WO07071755**

(96) Fecha de presentación y número de la solicitud europea: **21.12.2006 E 06830778 (4)**

(97) Fecha y número de publicación de la concesión europea: **29.03.2017 EP 1964016**

(54) Título: **Sistema en chip seguro**

(30) Prioridad:

23.12.2005 EP 05112983

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.07.2017

(73) Titular/es:

NAGRAVISION S.A. (100.0%)
Route de Genève 22-24
1033 Cheseaux-sur-Lausanne, CH

(72) Inventor/es:

KUDELSKI, ANDRÉ

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Sistema en chip seguro

Introducción

[0001] La presente invención concierne al campo de la seguridad del entorno de procesamiento.

Estado de la técnica

[0002] Ya se han descrito entornos seguros para procesadores, en particular, respecto a la arquitectura de multi-procesamiento.
Por ejemplo, una solución para limitar el acceso a una memoria segura se describió en el documento WO04015553.
Según esta solución, el procesador tiene dos modos de operaciones; en el primer modo, llamado el modo seguro, se permite el acceso a la memoria segura; y en el modo inseguro, el acceso a la memoria segura está prohibido.
El modo no seguro se destina a fines de desarrollo, es decir prueba o depuración del circuito.
Durante la ejecución en el modo no seguro, el acceso a la memoria segura está bloqueado físicamente, es decir, se genera una señal "inhabilitada".
Esta señal "inhabilitada" prohíbe cualquier intento de acceder a la memoria segura.

[0003] Otra solución se describe en el documento PCT/EP2005/056145 donde un procesador de desaleatorización de chip único procesa los datos audio/video codificados para no permitir nunca el acceso a los datos claros.
Cuando se ha realizado la operación de desaleatorización, la unidad de desaleatorización comprende un motor de codificación para encriptar los datos desaleatorizados antes de que estos se almacenen temporalmente en una memoria externa.
Cuando el procesador finaliza la tarea de organización, los datos se descifran en el módulo de emisión y se envian al dispositivo de visualización.

[0004] El número de publicación de patente estadounidense US-A-5 533 123 divulga un sistema en chip seguro con un número de mecanismos de seguridad diferentes para proteger de cualquier intento detectado de ganar acceso no autorizado al sistema.
Los mecanismos descritos incluyen: el uso de un cortafuegos; el uso de un mecanismo de monitorización de bus por el cual se controla una copia de los datos escritos últimos para un bus en un tiempo determinado frente al valor del bus en un momento posterior para detectar si el bus ha sido manipulado; y un mecanismo de supervisión de ataque de software para detectar cuándo se genera un número excesivo de errores de comando, indicando así un posible ataque de software.

[0005] 1124330 divulga un método del uso de una clave secreta programada de máscara para configurar de forma segura una matriz de puertas programable de campo.

Breve descripción de la invención

[0006] El objetivo de la presente invención es proporcionar un sistema en chip seguro para el procesamiento de datos y un chip electrónico según las reivindicaciones independientes y las varias formas de realización de las reivindicaciones dependientes.

[0007] La característica principal de la invención es un módulo independiente, independiente desde la unidad central de procesamiento y que tiene su propio núcleo procesador y ejecuta la tarea de supervisión.

[0008] Estas tareas se definen por un conjunto de definiciones de condiciones de trabajo normales que definen el diagrama cronológico normal y circulación de datos en el sistema en chip.
Las condiciones de trabajo normales se comparan con las condiciones de trabajo en tiempo real cuando el sistema en chip recibe procesos y envía datos.

Breve descripción de los dibujos

[0009] La invención se entenderá mejor gracias a las figuras anexas donde:
- la figura 1 describe la sistema en chip y sus varios elementos en el modo de codificación/descodificación,
- las figuras 2A y 2B describen la fase de codificación usando dos unidades,
- la figura 3 describe la sistema en chip y su varios elementos en el modo de firma,

- la 4 muestra un ejemplo de un sistema en chip aumentado donde los módulos seguros y no seguros se sitúan en el mismo chip.

Descripción detallada de la invención

[0010] Según un primer aspecto de la invención ilustrado en la figura 1, el sistema en chip SOC comprende un módulo de supervisión autónoma SM que puede controlar de forma determinista el sistema en chip SOC. Este módulo SM, comprende unas definiciones de condiciones de trabajo normales del sistema en chip SOC y medios de deshabilitación cuando las condiciones normales ya no se cumplen.
Este se consigue por medios diferentes.
Unos primeros medios incluyen la medición de la cantidad de datos emitidos, por ejemplo contar el número de conjuntos de datos emitidos.
Esta operación se describirá de aquí en adelante como recuento de datos.
Unos segundos medios incluyen la definición de periodos de tiempo durante los que se permiten las operaciones de entrada o salida.
Por lo tanto, un bloque de datos se permite si la longitud del mismo no excede el tiempo máximo definido para un bloque.
Unos terceros medios incluyen la detección del estado de la unidad central CPU y su duración respectiva, y la actuación por consiguiente como será ilustrada de aquí en adelante.
La unidad central CPU típicamente tiene estados posibles diferentes, tales como estado de adquisición, estado de tratamiento, estado de espera y estado de resultado de emisión.
Cuando un mensaje llega al sistema en chip, el mismo cambia del estado de espera al estado de adquisición.
Durante el estado de adquisición, el canal de entrada se habilita por el módulo de supervisión SM.
También durante el mismo estado de adquisición, el módulo de supervisión SM cuenta la llegada de datos y compara este número con un máximo predefinido.
Cualquier situación anormal lleva a un estado de advertencia donde la unidad central CPU puede decidir cómo reaccionar.
El módulo de supervisión SM tiene la capacidad, especialmente en caso de un estado de advertencia, de bloquear los canales entrada y de salida y/o el motor de codificación/descodificación CR-EN.

[0011] Cuando el mensaje externo se recibe, el módulo de supervisión SM provoca la unidad central CPU para ir al estado de tratamiento.
Durante este estado, los canales de entrada y de salida se deshabilitan.
El módulo de supervisión SM comprende un modelo temporal que corresponde con el tiempo de procesamiento mínimo por la unidad central CPU y deshabilita los canales durante este tiempo.
La unidad central CPU puede informar al módulo de supervisión SM de que no se emitirá ningún resultado.
Esto tiene la consecuencia de que el módulo de supervisión SM solo habilita el canal de entrada para la espera de un mensaje nuevo.
El canal de salida luego permanece deshabilitado.

[0012] En una caja donde la unidad central CPU desea enviar datos al mundo externo, luego informa por consiguiente al módulo de supervisión SM, que a su vez habilita el canal de salida.
El módulo de supervisión SM todavía continúa para controlar las actividades en el canal de salida contando los datos enviados y aplicando un periodo de tiempo durante el que se autoriza el envío.

[0013] En esta forma de realización de la invención, el módulo de supervisión SM es así capaz de trabajar con la información recibida de la unidad central CPU, al igual que con modelos de trabajo preprogramados.

[0014] Este módulo puede también controlar el motor de codificación/descodificación CR-EN contando los datos codificados o descodificados.
De la misma manera, el modelo de trabajo del motor de codificación/descodificación CR-EN se supervisa en términos de cantidad de datos procesados y tiempo.
El módulo de supervisión puede inhabilitar el motor de codificación/descodificación CR-EN si se detectan condiciones anormales.

[0015] Hay que señalar que el módulo de supervisión SM se puede implementar en un sistema en chip sin la codificación/descodificación en el canal de entrada/salida.
Los datos son procesados sin añadir un nivel de codificación adicional (o descodificación) y el canal de entrada/salida se observa por el módulo de supervisión SM.

[0016] Según un segundo aspecto de la invención, se propone un sistema en chip seguro para el procesamiento de datos, este sistema en chip comprende al menos una unidad central de procesamiento, un canal de entrada y de salida, un motor de codificación/descodificación y una memoria, caracterizado por el hecho de que dicho canal de entrada comprende un módulo de codificación de entrada para encriptar todos los datos de entrada, dicho canal de salida incluye un módulo de descodificación de salida para descodificar todos los datos de salida,

dicha unidad central de procesamiento recibe los datos codificados desde el módulo de codificación de entrada y almacena estos en la memoria, y durante el procesamiento de los datos almacenados, dicha unidad central de procesamiento lee los datos almacenados de la memoria, solicita la descodificación del mismo motor de codificación/descodificación, procesa los datos y solicita la codificación del resultado por el motor de codificación/descodificación y almacena el resultado codificado, emite el resultado al módulo de descodificación de salida para fines de descodificación y sale el resultado descodificado vía el canal de salida.

[0017] En esta forma de realización, la codificación se produce para datos aún en un medio ambiente considerado como seguro.
La descodificación se produce solo en la fase posterior cuando los datos se usan realmente por la unidad central, los datos claros que nunca son accesibles en un estado estático.
Cuando se procesan, los datos se pueden almacenar en claro si estos son para fines internos o recodificados si estos se destinan a ser emitidos del sistema en chip.

[0018] Una vez recodificados, los datos son temporalmente almacenados en un tampón antes de ser enviados al canal de emisión.

[0019] La clave para codificar y descodificar los datos en una forma de realización preferida es única para este sistema en chip.
Esta clave se puede preprogramar en la etapa de fabricación o se puede generar de forma aleatoria en la fase de inicialización y nunca ser conocida por nadie.
Esta clave se usa solo internamente.
El algoritmo usado se puede mantener en secreto al igual que los parámetros de dicho algoritmo.
Por ejemplo, el algoritmo IdeaNxt se usa como motor de codificación y los valores de la caja de sustitución se generan de forma aleatoria en el sistema en chip.

[0020] Según una forma de realización particular, el algoritmo de codificación/descodificación es asimétrico, de modo que un par de claves (públicas/privadas) se utilizan respectivamente para encriptar y desencriptar los datos.

[0021] Según una forma de realización alternativa, el módulo de codificación de entrada se puede sustituir por un módulo de firma, los datos se firman mientras se introducen en el sistema en chip y la firma almacenada con los datos.
Cuando la unidad central desea usar estos datos, el motor de codificación/descodificación que es ahora un motor de verificación de firma, verifica la firma y autoriza el uso de los datos si la firma es correcta.

[0022] Por datos se hace referencia a un byte único o un conjunto de bytes por ejemplo para formar un mensaje o un mensaje de derecho en el sistema en chip.

[0023] El sistema en chip seguro SOC se basa en una unidad de procesamiento central CPU.
El objetivo de esta unidad es ejecutar el código y para realizar las tareas solicitadas.
La sistema en chip SOC comprende dos canales conectados al mundo externo, es decir los canales de entrada y salida.
El canal de entrada RCV comprende un módulo de codificación de entrada RCV-E que encripta todos los datos que vienen del mundo externo.
De la misma manera, el canal de emisión SND comprende un módulo de descodificación de emisión SND-D para descodificar los datos recibidos de la unidad central CPU antes de enviarlos al mundo externo.

[0024] La unidad central CPU tiene acceso al motor de codificación/descodificación CR-EN.
Este motor tiene la misma función que el módulo de codificación de entrada y el módulo de descodificación de salida.
La clave K cargada en el módulo de codificación de entrada es la misma en la parte de codificación del motor de codificación/descodificación.
Lo mismo se aplica al módulo de descodificación de salida y la parte de descodificación del motor de codificación/descodificación, para las operaciones de descodificación.
Cuando la unidad central CPU necesita algunos datos, que bien directamente vienen del módulo de codificación de entrada o llegan desde la memoria MEM, estos datos primero pasan por el motor de descodificación para descodificarlos antes de que se usen en la unidad central CPU.

[0025] De la misma manera, cuando la unidad central CPU ha completado una tarea y produce un resultado, la etapa siguiente es depositar el resultado (o emitir el resultado al canal de salida).
Este resultado previamente pasa a través del motor de codificación CR-EN para la codificación antes de ser almacenado.
Este resultado codificado puede después ser almacenado en una memoria o enviado al canal de salida.

[0026] La unidad central de procesamiento CPU puede decidir si el resultado debe ser recodificado o quedarse en claro.
En vez de dejar el procesador decidir, la ubicación objeto puede seleccionar comportamientos diferentes como se muestra en la figura 2A.
Si el resultado debe ser almacenado en una memoria volátil V-MEM, puede tener lugar una codificación doble.
En el contrario, si el almacenamiento está en una (EEPROM) memoria no volátil NV-MEM, solo se usa una unidad de codificación, esta con una clave permanente.
De la misma manera, cuando se leen los datos de la memoria volátil, la descodificación doble se aplica aunque se lean los datos desde la memoria no volátil, solo se aplica una unidad de descodificación.

[0027] Según una forma de realización alternativa que se muestra en la figura 3, el proceso de codificación se sustituye por un proceso de firma.
Los datos no se codifican pero se genera una firma y se asocia a los datos.
Para todos los datos que vienen del mundo exterior, se calcula una firma en el módulo de firma de entrada RCV-S.
Los datos luego se almacenan con sus firmas.
Cuando la unidad central necesita acceder a estos datos, el motor de verificación de firma S-VER primero verifica la firma antes de que la unidad central tenga derecho a usar los datos.
Antes de que los datos se emitan por el canal de salida, la firma se verifica en el módulo de firma de salida SDN-V.
La firma luego se retira de los datos que se envían al canal de salida SND.

[0028] Según una forma de realización alternativa, el motor de codificación/descodificación está directamente situado en la unidad central CPU.
Cuando unos datos se leen desde la memoria, por ejemplo cargando una variable en el acumulador de la CPU (por ejemplo LDAA #1200h para Motorola 68HC11), los datos leídos en esa ubicación pasan automáticamente al motor de descodificación antes de ser transferidos al acumulador.
De la misma manera, la instrucción para depositar el contenido del acumulador a la memoria (por ejemplo STAA #1200h) no se ejecuta directamente pero los datos en el acumulador pasan previamente a través del motor de codificación antes de ser almacenados en la ubicación 1200h.

[0029] En una forma de realización particular, el motor de codificación/descodificación se comparte con el canal de entrada y de salida.
Por lo tanto, el módulo de codificación de entrada es un módulo virtual y las operaciones de codificación en el canal de entrada se consiguen por el motor de codificación a través de unos datos multiplexor.
La introducción de datos en el sistema en chip SOC, en particular, a través del canal de entrada se pasan a través del motor de codificación antes de otra manipulación por ejemplo para depositar los datos en un tampón de entrada. El módulo de codificación de entrada es por lo tanto un módulo virtual que utiliza el recurso del motor de codificación/descodificación en el modo de codificación.
Lo mismo se aplica al módulo de descodificación de salida que usa el motor de codificación/descodificación en el modo de descodificación.

[0030] El módulo de codificación de entrada RCV-E puede comprender más de una unidad de codificación.
Según una forma de realización particular que se muestra en la figura 2A, dos unidades de codificación (o más) se conectan en series, cada una con una clave diferente.
La primera unidad de codificación se carga con una clave K1 que pertenece al de sistema en chip, es decir, es única y constante para un dispositivo específico.
Esta clave se carga durante la etapa de instalación o se genera internamente.
La segunda unidad ENC2 se carga con una clave K2 que se genera dinámicamente al activar el dispositivo.
Cuando el sistema en chip se reinicializa, esta clave se pierde y se genera una clave nueva.
Los datos que tienen que ser permanentemente almacenados, una vez procesados por el procesador CPU son solo reencriptados con la primera unidad con la clave permanente K1.

[0031] El módulo de descodificación de salida al igual que el motor de codificación/descodificación comprenden de la misma manera también dos o más unidades.

[0032] Alternativamente, si el procesador CPU reconoce que los datos recibidos, almacenados en un tampón de entrada no necesitan ser procesados, pero solo se deben almacenar en una memoria permanente NV-MEM, el procesador puede solicitar desde el motor de codificación/descodificación la descodificación por solo una unidad de descodificación, es decir, la unidad con la clave volátil.
Los datos almacenados todavía permanecen codificados por la clave permanente para un uso posterior.

[0033] Este sistema en chip SOC se usa como módulo de control de acceso seguro encargado de recibir los mensajes de gestión incluyendo derechos o claves.

Este módulo puede también comprender una unidad de desaleatorización de marcha rápida para recibir un flujo de datos de vídeo codificado.

[0034] La figura 4 muestra un sistema en chip aumentado SOC con dos núcleos, un núcleo no seguro llamado USC y el otro núcleo seguro llamado SC.
La descripción mencionada anteriormente del sistema en chip es ahora solo una parte del SOC aumentado y corresponde con el núcleo seguro SC.
La parte no segura USC comprende medios procesadores CPU1 y memoria interna MEM1.
Sin embargo, en vistas de los programas grandes y datos procesados por este procesador, la memoria externa MEM es necesaria.
A través de la memoria externa o a través de la interfaz al mundo exterior, el núcleo no seguro puede recibir un programa troyano para captar la recepción de datos y envío a través de la interfaz interna I2.
Por lo tanto, los datos recibidos o solicitados por el núcleo inseguro USC a través de la interfaz insegura INT se consideran como el mismo nivel de seguridad que los datos externos.
El núcleo seguro SC sigue observando las actividades del código no seguro tal como detección de fallo, análisis de potencia, iluminación ligera, cambio de temperatura.
Estas funciones se sitúan en el módulo detector DTC.
Este módulo informa el núcleo seguro de cualquier condición anormal, conduciendo así al cambio del estado del módulo de supervisión SM.
Cabe destacar que el módulo detector se puede situar directamente en el módulo seguro SC.

[0035] Según una variante de la invención, el módulo detector DTC ejecuta operaciones de vigilancia del estado del sistema en chip SOC. Este recibe por ejemplo el suministro positivo Vdd (generalmente 5V) y observa el comportamiento de riesgos tal como cambios repentinos de voltaje, alta o anormalmente baja tensión.
Según el criterio definido, este puede informar al módulo seguro SC por ejemplo generando un mensaje de error y así desactivando ciertas funciones del módulo anteriormente mencionado.
La interfaz de comunicaciones I2 se observa por el módulo detector.
Por comunicación, entendemos todas las vías por las que la información entra o sale del módulo seguro.
El módulo detector puede también controlar el funcionamiento del módulo inseguro USC y sus vías de comunicación.
Esta supervisión abarca el suministro de energía, el reloj y el restablecimiento.
En la reacción a condiciones anormales detectada por el módulo detector DTC, el módulo seguro SC puede reducir el acceso a datos sensibles desde la memoria interna MEM2.
El módulo seguro SC puede también iniciar un restablecimiento del módulo inseguro USC, reanudando así una revisión completa del programa y ambiente de datos.

[0036] El sistema de la invención es escalable, es decir, cada sistema en chip comprende su propio módulo de supervisión como se ha descrito anteriormente.
Cuando diferentes sistemas en chip se enlazan para crear un chip mayor como se muestra en la figura 4, un SSM de módulo de supervisión superior adicional se añade para sincronizar el módulo de supervisión SM.
Un canal dedicado permite la comunicación entre los módulos de supervisión SM de la entidad única y el módulo de supervisión superior SSM del chip.
Cada módulo de supervisión comprende una máquina de estado que describe las operaciones permitidas durante ese estado.
El módulo de supervisión superior compara los estados de las varias entidades e informa el módulo de supervisión de entidad y el estado de la otra entidad.
Una máquina de estado general manejada por el módulo de supervisión superior controla que el estado de las entidades sea conforme con el escenario de trabajo.
Por ejemplo, si una entidad está en el estado de la recepción de los datos de la otra entidad, el módulo de supervisión superior comprueba que la otra entidad esté en el estado del envío de datos.

[0037] En una forma de realización alternativa, el módulo de supervisión superior se localiza directamente en la entidad más segura, en nuestro ejemplo en el sistema en chip seguro SC.

[0038] La comunicación entre cada entidad a través del canal dedicado está preferiblemente codificada con una clave cargada durante la inicialización del chip.

[0039] Esta clave puede utilizarse para codificar y descodificar los datos cambiados entre dos módulos de supervisión o con el módulo de supervisión superior.
Al iniciar el chip, esta clave puede utilizarse para generar una clave temporal, por ejemplo usando el algoritmo Diffie-Hellmann.

REIVINDICACIONES

1. Sistema en chip seguro (SOC) para el tratamiento de datos, este sistema en chip comprende al menos una unidad de procesamiento central, un canal de entrada y de salida, un motor de codificación/descodificación y una memoria, dicho sistema en chip comprende además un módulo de supervisión autónomo (SM) que se preprograma con definiciones de condiciones de trabajo normales, dicho módulo de supervisión (SM) comprende medios de deshabilitación para la deshabilitación de los canales de entrada/salida cuando las condiciones de trabajo normales ya no se cumplen, dicho módulo de supervisión (SM) comprende además primeros medios para medir una cantidad de datos emitida, segundos medios para definir el periodo de tiempo durante el que se permiten las operaciones de entrada y salida, terceros medios para la detección del estado de la unidad central de procesamiento (CPU) y sus duraciones respectivas, dicho módulo de supervisión está configurado para determinar que las condiciones normales ya no se cumplen y se basan en la comparación de las definiciones preprogramadas de condiciones de trabajo normales con datos y el estado obtenido por los primeros, segundos y terceros medios.

2. Sistema en chip seguro (SOC), según la reivindicación 1, donde dicho módulo de supervisión (SM) comprende además medios para inhabilitar un motor de codificación/descodificación (CR-EN) dependiendo de la comparación.

3. Sistema en chip seguro, según la reivindicación 1 o 2, **caracterizado por el hecho de que** las definiciones de condiciones de trabajo normales comprenden una duración donde el módulo de supervisión deshabilita los canales de entrada y/o de salida después de la recepción de un bloque de datos.

4. Sistema en chip seguro, según las reivindicaciones 1 a 3, **caracterizado por el hecho de que** dicho canal de entrada comprende un módulo de codificación de entrada para la codificación de todos los datos de entrada, dicho canal de salida comprende un módulo de descodificación de salida para la descodificación de todos los datos de salida, dicho tratamiento central está configurado para recibir los datos codificados del módulo de descodificación de entrada y almacenarlos en la memoria, y mientras se procesan los datos almacenados, dicha unidad central de procesamiento está configurada para leer los datos almacenados de la memoria, solicitar descodificación de los mismos en el motor de codificación/descodificación, procesar los datos y solicitar la codificación del resultado por el motor de codificación/descodificación y almacenar el resultado codificado, emitir el resultado a la salida del módulo de descodificación para fines de descodificación y emitir el resultado descodificado vía el canal de salida.

5. Sistema en chip seguro, según la reivindicación 4, **caracterizado por el hecho de que** el módulo de codificación de entrada es un módulo virtual que pasa los datos que se van a codificar al motor de codificación/descodificación en el modo de codificación.

6. Sistema en chip seguro, según la reivindicación 4, **caracterizado por el hecho de que** el módulo de codificación de entrada es un módulo virtual que pasa los datos que se van a descodificar al motor de codificación/descodificación en el modo de descodificación.

7. Sistema en chip seguro, según las reivindicaciones 4 a 6, **caracterizado por el hecho de que** el algoritmo para codificar y descodificar los datos es un algoritmo simétrico.

8. Sistema en chip seguro, según la reivindicación 7, **caracterizado por el hecho de que** el algoritmo de codificación/descodificación usa un conjunto de constantes de inicialización y todas o parte de las constantes de inicialización se generan de forma aleatoria en el sistema en chip.

9. Sistema en chip seguro, según las reivindicaciones 4 a 6, **caracterizado por el hecho de que** el algoritmo para codificar y descodificar los datos es un algoritmo asimétrico.

10. Sistema en chip seguro, según las reivindicaciones 4 o 9, **caracterizado por el hecho de que** este comprende medios para generar de forma aleatoria la clave o par de claves usadas por el motor de codificación/descodificación.

11. Sistema en chip seguro, según cualquiera de las reivindicaciones 1 a 10, **caracterizado por el hecho de que** las operaciones de codificación/descodificación se pueden ejecutar en unos datos únicos o un conjunto de datos a la vez.

12. Chip electrónico que comprende el sistema en chip seguro, según cualquiera de las reivindicaciones 1 a 11, el chip electrónico comprende además otro sistema en chip, el otro sistema en chip comprende otra unidad central de procesamiento, un primer enlace de datos con el mundo externo, un segundo enlace de datos a la entrada/salida del sistema en chip seguro y otro módulo de supervisión que se preprograma con definiciones de condiciones de trabajo normales de al menos el primer enlace de datos y el segundo enlace de datos, el chip

electrónico comprende medios para inhabilitar el primer y segundo enlace de datos si las condiciones actuales exceden las definiciones de condiciones normales.

13. Chip electrónico, según la reivindicación 12, que comprende además un módulo de supervisión superior SSM que se comunica con el módulo de supervisión y el otro módulo de supervisión, y controla si las condiciones de trabajo del módulo de supervisión son compatibles con las condiciones de trabajo del otro módulo de supervisión.

Fig. 1

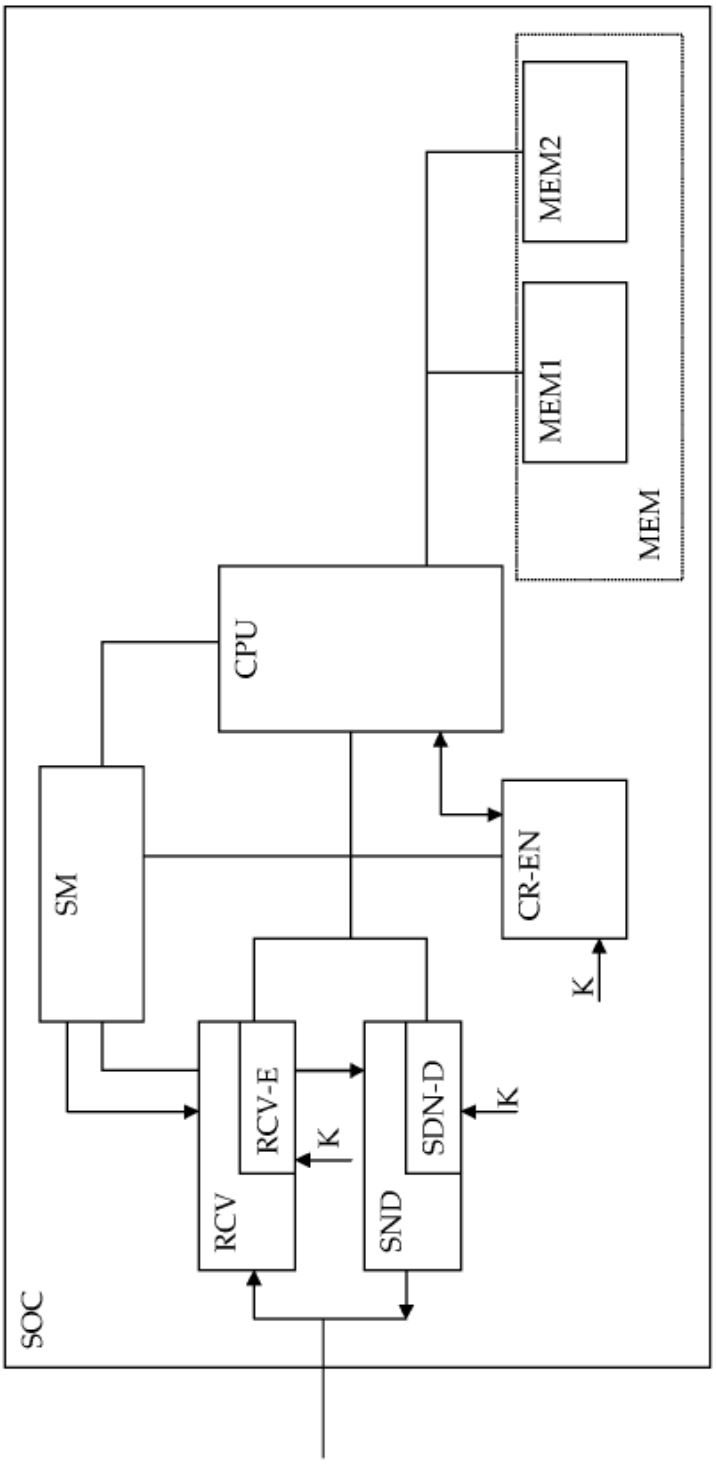


Fig. 2A

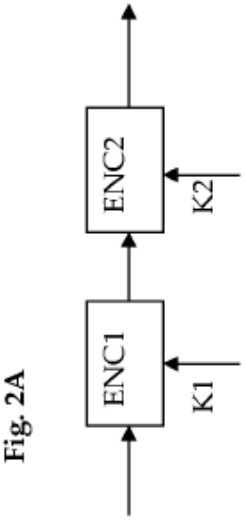
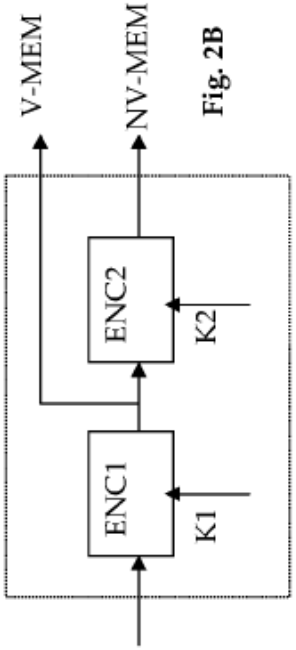


Fig. 2B



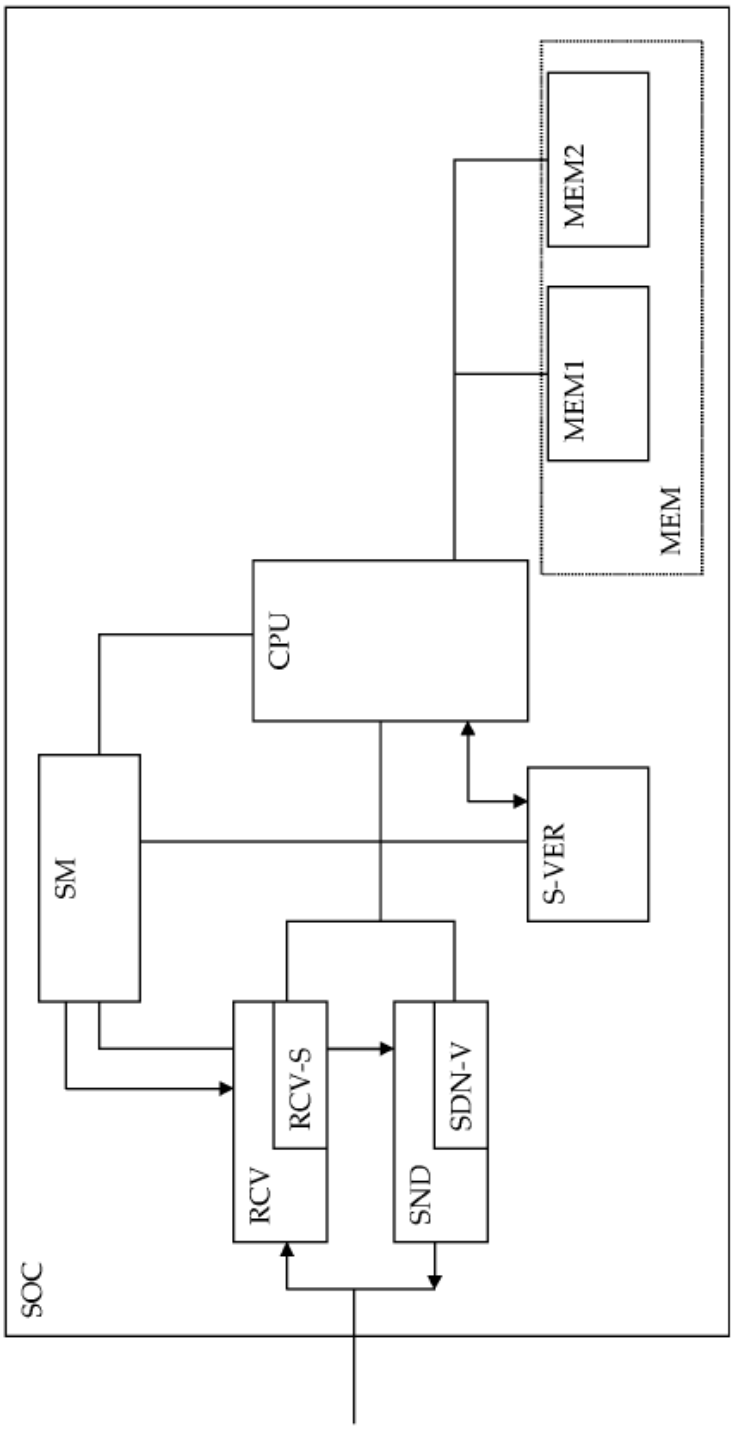


Fig. 3

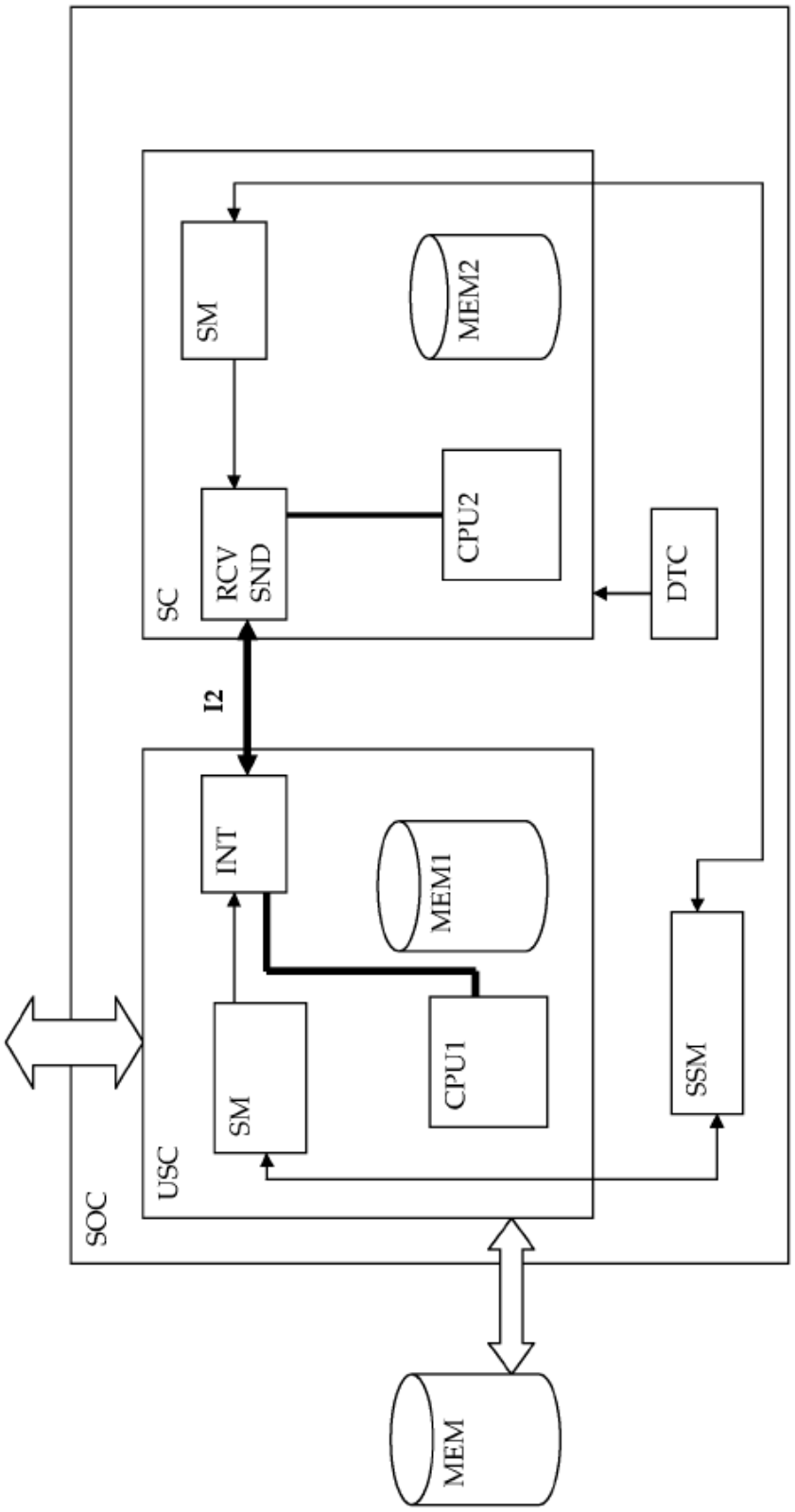


Fig. 4