(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 603 329**

(51) Int. CI.:

G06K 7/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **18.11.2010 E 10191635 (1)**

(97) Fecha y número de publicación de la concesión europea: **24.08.2016 EP 2455887**

(54) Título: **Método y aparato para comunicar entre un módulo de seguridad y un dispositivo host**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.02.2017

(73) Titular/es:

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

(72) Inventor/es:

OSEN, KARL y
ODOOM, ERNEST

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Método y aparato para comunicar entre un módulo de seguridad y un dispositivo host

Introducción

[0001] La presente invención se refiere al dominio de interferencia electromagnética de radiofrecuencia y más específicamente a métodos y dispositivos para la reducción de tal interferencia en circuitos electrónicos.

Estado de la técnica

[0002] Con el uso creciente cada vez más alto y alto de frecuencias de señal en el funcionamiento de circuitos electrónicos, los problemas relacionados con interferencia electromagnética o EMI están volviéndose más graves. En el dominio de acceso condicional, es común el uso de un módulo de seguridad. Un módulo de seguridad se usa normalmente en cooperación con un dispositivo host que comprende al menos un lector de tarjetas para interconectar con el módulo de seguridad. El dispositivo host puede comprender además un módulo criptográfico y otro hardware relacionado de acceso condicional y software. El módulo de seguridad contiene información personalizada tal como llaves criptográficas y similares, que tienen que ser mantenidos en secreto.
El módulo de seguridad es generalmente un dispositivo portátil que es separable del dispositivo host.

[0003] Un ejemplo común de un módulo de seguridad es un chip electrónico alojado en una tarjeta, generalmente en forma de una tarjetas de crédito, una tarjeta SIM o una tarjeta microSIM u otro soporte similar.
La tarjeta es normalmente presentada al módulo host, o más particularmente al lector de tarjetas en el módulo host, vía una ranura en el módulo host. El contacto se hace entre el chip y el lector de tarjetas por un conjunto de contactos que vienen a reposar sobre un conjunto de almohadillas de contacto correspondientes sobre una superficie de la tarjeta, que conectan con el chip.

[0004] Con la tendencia de que las frecuencias en funcionamiento de los módulos de seguridad anteriormente mencionados sean más altas, es decir en gamas de más de varios cientos de megahercios, cualesquiera conexiones al módulo de seguridad que llevan señales con componentes de frecuencia en tales gamas, es decir conexiones a reloj y pin de datos por ejemplo, tenderán a emitir radiación electromagnética.
Tal radiación electromagnética se puede interceptar por una tercera parte y ser usada para romper la seguridad del módulo de seguridad. Por ejemplo supervisando la radiación electromagnética durante el tiempo que el módulo de seguridad transmite una clave secreta, puede ser posible para una tercera parte reconstruir la clave secreta para uso malicioso. De forma similar, un módulo de seguridad puede ser susceptible de interferencia por campos electromagnéticos suficientemente fuertes generados externamente al módulo de seguridad con el fin de influir en el funcionamiento del módulo de seguridad y/o lector de tarjetas durante el funcionamiento.
Tal interferencia, generada o bien externa o internamente por el módulo de seguridad o cualquier otro circuito en el host durante el funcionamiento, es conocida como interferencia electromagnética o EMI.

[0005] El fenómeno EMI es bien conocido en la industria electrónica. De hecho, hay límites que son estándares de industria colocados en circuitos electrónicos en relación a la cantidad de radiación electromagnética que se permite generar a tales circuitos. Estos límites se diseñan para minimizar la posibilidad de circuitos susceptibles de generar grandes cantidades de EMI en los circuitos vecinos de afectación y para evitar el riesgo de daño físico a seres humanos en la proximidad de tales circuitos.

[0006] Es usual, en el dominio de circuitos electrónicos que se diseñan para funcionar a frecuencias radiofónicas (RF), incluir tales circuitos dentro de una caja cuyas paredes son cubiertas totalmente por un material que tiene las propiedades de la provisión de protección contra la radiación electromagnética.
Esto proporciona generalmente protección suficiente contra la radiación producida por el circuito para que no escape hacia el exterior de la caja cerrada y para que la radiación generada en el exterior no penetre en la caja y no interfiera con el funcionamiento del circuito.

[0007] Sin embargo, en el caso de un dispositivo host diseñado para recibir un módulo de seguridad vía una ranura o puerto, resulta difícil impedir que EMI escape puesto que el puerto presenta una discontinuidad en la caja y por lo tanto una discontinuidad en la protección exponiendo por tanto un área donde puede escapar la EMI. La patente estadounidense con número de publicación US 7,351,919 B1 describe una cubierta de puerto para limitar la transferencia de radiación electromagnética desde el puerto de un dispositivo host cuando el módulo de seguridad está funcionando dentro del puerto. Una cubierta de puerto se instala sobre la ranura para la tarjeta chip después de que es introducida la tarjeta chip. La cubierta del puerto se alinea con un material conductor, que contribuye a las propiedades de protección de la EMI de la cubierta del puerto y permite que se complete un circuito eléctrico cuando la cubierta del puerto está en la posición, permitiendo así la detección de si la cubierta del puerto está o no cerrada debidamente.

[0008] También existen dispositivos para suministrar una protección alrededor de componentes electrónicos susceptibles de emitir EMI tal como el dispositivo descrito en la patente estadounidense con número de publicación de US 5,436,803 que enseña un revestimiento flexible que rodea una tarjeta de circuito electrónico en el dispositivo host,

comprendiendo la tarjeta de circuito electrónico el componente perjudicial. El revestimiento flexible comprende una hoja de aislamiento tal como polietileno y una hoja de fibras conductoras tal como nilón metalizado que dan una resistividad en el orden de un décimo de un ohmio.
Otro ejemplo es descrito en la patente internacional con número de publicación WO 2005/106953 A1, que divulga una capa de selección, que comprende una capa de material magnético blando de alta permeabilidad relativa tal como hierro, níquel o cobalto o cualquiera de sus aleaciones, colocada en la superficie del componentes susceptible de emitir la EMI perjudicial. El documento además pasa a describir el uso de otra capa de material duro adicional, tal como carbono diamantado, en la superficie del componente para impedir el acceso al componente a través de medios mecánicos o químicos.

[0009] En la patente estadounidense con número de publicación 6,223,298, está descrita una interfaz de comunicaciones, permitiendo así que una unidad procesadora dialogue con una tarjeta IC a través de un bus en serie. Esta invención resuelve un problema donde la comunicación entre el procesador y la tarjeta IC solo es posible a índices de transmisión predeterminados, donde dichos índices son fijados por medios de serialización de la interfaz y toman solo un número muy limitado de valores. Incluso cuando el procesador trabaja a velocidad nominal (normalmente alta), los índices son típicamente pequeños. La invención por lo tanto se dirige a permitir que el número de índices posibles sea sustancialmente más alto y que los valores de los índices mismos sean cercanos a la frecuencia operativa máxima de la tarjeta IC, conduciendo así posiblemente a la generación de EMI.
Esto es útil por ejemplo en la prueba de las tarjetas IC, donde el (procesador) probador tiene que ser ejecutado a alta velocidad. Ninguna consideración se da a los inconvenientes posibles de EMI que se genera dentro de tal sistema.

Breve resumen de la invención

[0010] En vista del estado de la técnica, es un objetivo de la presente invención proporcionar medios para la reducción de la cantidad de interferencia electromagnética detectable desde el exterior de un dispositivo host mientras el dispositivo host está de comunicación con un módulo de seguridad, especialmente cuando el dispositivo host comprende una ranura o puerto a través del cual se inserta el módulo de seguridad.

[0011] Es otro objetivo de la presente invención proporcionar un medio para la reducción de la cantidad de interferencia electromagnética que escapa de un módulo de seguridad hacia componentes electrónicos comprendidos dentro de un dispositivo host mientras el módulo de seguridad está de comunicación con el dispositivo host.

[0012] Es otro objetivo de la presente invención proporcionar tal reducción en la interferencia electromagnética mientras se retiene la facilidad de acceso físico al dispositivo host por el módulo de seguridad, permitiendo así la facilidad del cambio de un módulo de seguridad a otro.
Este requisito por lo tanto excluye la posibilidad del uso de una cubierta de puerto o un revestimiento flexible como se describe en el estado de la técnica al igual que el uso de capas protectoras alrededor del módulo de seguridad.
Adicionalmente, un objetivo de la presente invención es reducir los costes de fabricación asociados a la producción de dispositivos host destinados a recibir módulos de seguridad que funcionan a frecuencias operativas suficientemenete altas como para generar la EMI no deseada y por lo tanto el uso de capas de protección costosas tales como aquellas descritas en el estado de la técnica no es una opción deseada.

[0013] Los objetivos de la presente invención se consiguen por lo tanto utilizando un método según la reivindicación 1 y un dispositivo según la reivindicación 2.

Breve descripción de los dibujos

[0014] La presente invención será mejor entendida gracias a la descripción detallada que sigue y los dibujos anexos, que se dan como ejemplos no limitativos de formas de realización de la invención, donde:
Fig. 1 muestra un módulo de seguridad conectado a un dispositivo host como existe en el estado de la técnica.
Fig. 2 muestra módulo de seguridad conectado a un dispositivo host según una forma de realización de la presente invención.
Fig. 3 muestra un módulo convertidor como empleado en una forma de realización de la presente invención.
Fig. 4 ilustra como un módulo de conversión según una forma de realización de la presente invención convierte una pluralidad de señales de baja frecuencia para formar una señal de frecuencia alta.
Fig. 5 muestra una tarjeta chip con un módulo de seguridad insertado a través de una lengüeta en un alojamiento según una forma de realización de la presente invención.

Descripción detallada

[0015] Es bien conocido por quienes están familiarizados con el dominio de interferencia electromagnética (EMI) de radiofrecuencia (RF) que una variable que contribuye en la determinación de la cantidad de EMI que será emitida por un cable es proporcional a la longitud de este cable y que otra variable que contribuye es el contenido de frecuencia de una señal transportada por el cable.
En una forma de realización preferida de la presente invención se busca por lo tanto minimizar la longitud de cualesquiera cables que llevan tales señales con alto contenido de frecuencia en el conjunto de módulo del

dispositivo/seguridad host y para minimizar el número de tales cables.

[0016] Fig. 1 muestra un módulo de seguridad conectado a un dispositivo host.
El módulo de seguridad tiene forma de un chip electrónico (CH) alojado en una tarjeta chip (CC).
Esta configuración es generalmente conocida en el estado de la técnica. El módulo de seguridad o chip (CH) en su tarjeta chip (CC) se inserta en una ranura en el dispositivo host (HST) y las almohadillas de contacto del chip entran en contacto con un conjunto de contactos conectados al lector de tarjetas del dispositivo host (RDR).
Para simplicidad, la figura solo muestra la conexión a la entrada/salida del chip (IO) y almohadillas del reloj (CK).
En realidad el lector de tarjetas generalmente también entraría en contacto con las otras almohadillas del chip tales como restablecimiento, suministro de energía, suelo y almohadillas de programación de memoria por ejemplo. Como se verá más adelante, cuando se describe la invención, según una forma de realización de la presente invención, puesto que la almohadilla de entrada/salida (IO) y la almohadilla de reloj (CK) son aquellas que llevan señales de la frecuencia máxima, atención particular se dirige hacia el tratamiento de conexiones que van a estas almohadillas. Fig. 1 también muestra un módulo criptográfico (DCD) en el dispositivo host (HST).
El módulo criptográfico comunica con el lector por medio de varios buses y señales, representado por las líneas de EMI de bus ilustradas (B1 B2) y líneas de señal (L1, L2).
El módulo criptográfico produce salidas (Q; CO) para ser más procesadas o enviadas hacia fuera con el dispositivo host (HST) y también puede recibir varios buses y señales (I, CI) desde el exterior del dispositivo host (HST) o de otros componentes en el dispositivo host (HST). Cualquiera o todas las señales anteriormente descritas pueden comprender características de alta frecuencia conduciendo a la generación de EMI o conduciendo a sensibilidad de cara a incidente de EMI.

[0017] Fig. 2 muestra una forma de realización de la presente invención donde un módulo convertidor (CVT) ha sido introducido en la configuración mostrada en la Fig. 1.
El módulo convertidor (CVT) se usa como una interfaz entre el módulo de seguridad (CH) y el lector de tarjetas (RDR_SL) y su fin es atrasar las señales de frecuencia alta es decir la señal de entrada/salida (IO) y la señal de reloj (CK) de modo que lector de tarjetas (RDR_SL) y de hecho cualquiera de los otros circuitos comprendidos en el dispositivo host puedan operar a una frecuencia que es lo suficientemente baja como para no generar ninguna EMI o al menos reducir sustancialmente la cantidad de EMI que es generada.
Cabe observar que al igual que las señales entre el lector de tarjetas (RDR_SL) y el módulo convertidor (CVT) son ralentizadas, las otras señales que entran entre el lector de tarjetas (RDR_SL) y cualquiera de los otros módulos en el dispositivo host serán igualmente ralentizadas. Como se muestra en el ejemplo representado por la Fig. 2, el módulo convertidor (CVT) emite la señal de reloj (CK) al módulo de seguridad (CH), que es convertida a partir de dos señales subordinadas a reloj (CK1 CK0) separadas que vienen del lector de tarjetas (RDR_SL), que se modifica con respecto al lector de tarjetas (RDR) de Fig.1 para trabajar a una frecuencia inferior. De forma similar, la señal de entrada/salida (IO) para el módulo de seguridad (CH) es convertida a partir de dos entradas separadas (I1 I0) del lector de tarjetas (RDR_SL) y a dos salidas separadas (01,00) al lector de tarjetas (RDR_SL).
Fig. 2 también muestra el lector de tarjetas (RDR_SL) comunicando con un decodificador (DCD_SL), que en consecuencia también puede funcionar a una frecuencia reducida.
Para simplicidad, la Fig. 2 solo muestra al módulo convertidor (CVT) produciendo una conversión de uno a dos para cada línea. En realidad, para conseguir reducciones mucho más sustanciales en las frecuencias de señal, el módulo convertidor convertiría en una proporción de 8 a 1 o 16 a 1 o más alto por ejemplo.

[0018] Fig. 3 muestra una forma de realización del módulo convertidor (CVT) con mayor detalle. La señal de reloj (CK) para el módulo de seguridad se genera multiplexando dos señales subordinadas a reloj (CK0 CK1) separadas, adecuadamente sincronizadas. De forma similar, la señal de entrada/salida (IO) es multiplexada desde dos entradas (11, I0) y demultiplexada para producir dos salidas separadas (01,00). Nuevamente, la figura muestra un ejemplo simplificado de dos líneas que se multiplexan en una.
La forma de realización en general sin embargo permite que buses paralelos de por decir 8 bits de datos más un bit de paridad por ejemplo en el lector sean multiplexados en una línea por el módulo convertidor, permitiendo así que el módulo de seguridad trabaje a las frecuencias más altas necesarias mientras que el lector de tarjetas y otro circuito relacionado en el host puede ejecutarse a frecuencias significativamente más bajas.

[0019] Para reducir más la cantidad de EMI irradiada del dispositivo host, el cableado usado para los buses y señales entre el módulo convertidor (CVT) y el lector de tarjetas (RDR_SL) puede ser de tipo blindado.
De hecho, como una regla general, cualquier cableado de intermódulo en el dispositivo host es preferiblemente de un tipo blindado.

[0020] Fig. 4 muestra un ejemplo de como el módulo convertidor (CVT) puede producir una señal de reloj para el módulo de seguridad (CH) que usa ocho líneas subordinadas a reloj (CK7, CK6, ..., CK0). La señal de reloj (CK) tiene un periodo de reloj (t) y se genera por multiplexado de ocho relojes subordinados (CK7, CK6, ..., CK0) cada uno con un periodo subordinado a reloj (T), que es ocho veces el periodo de reloj (t=T/8). El periodo subordinado a reloj (T) se divide en ocho fases separadas (Ø7, Ø6, ..., Ø0). Cada uno de los ocho relojes subordinados tiene un pulso durante solo una fase del periodo subordinado a reloj (T). En el ejemplo dado para la forma de realización descrita de la presente invención, las ocho fases son consecutivas y sin superposición. Los impulsos de cada uno de los relojes subordinados consecutivos ocurren durante fases consecutivas.

De esta manera, cada reloj subordinado consecutivo contribuye a que cada pulso consecutivo del reloj produzca así la frecuencia de reloj necesaria de ocho veces mayor que las frecuencias subordinadas a reloj. Un método similar se usa para la parte de entrada de la línea de entrada/salida.
Ocho líneas diferentes diferentes subordinadas a entrada representan el estado de la línea subordinada a entrada/salida durante ocho fases consecutivas del reloj (CK) y las ocho líneas subordinadas a entrada se multiplexan sobre el pin de entrada/salida (IO). Por ejemplo, para cada línea subordinada a entrada, durante la fase donde está activa, esta dará un pulso para un primer estado lógico y ningún pulso para un segundo estado lógico. De forma similar, la parte de salida del pin de entrada/salida, es decir, conducido por el módulo de seguridad (CH cuando el módulo de seguridad está en el modo de salida, es multiplexada en tiempo por ocho líneas subordinadas a salida, donde cada línea consecutiva subordinada a salida representa el estado del pin de entrada/salida durante fases consecutivas del reloj (CK).

[0021] Para reducir más cualquier EMI generada de cualquiera de las entradas subordinadas, salidas subordinadas o relojes subordinadas, puede ser empleada cualquiera de las técnicas conocidas para reducir la velocidad de rotación de estas líneas. Por ejemplo para hacer las líneas resistivas, la constante RC relacionada resultante contribuirá a ralentizar las transitorias de las líneas.

[0022] Según un ejemplo más que líneas multiplexadas como se muestra anteriormente, se usa una técnica de multiplicación de modo que se pueden usar frecuencias inferiores en todo el host hasta que sean necesarias frecuencias más altas en el módulo de seguridad. Por ejemplo, mientras que un módulo de seguridad tiene que funcionar a 100MHz, los circuitos en el dispositivo host pueden funcionar a una frecuencia más modesta basada en un reloj de referencia de más o menos 1 MHz, produciendo así cantidades sustancialmente bajas de EMI.
El módulo convertidor (CVT) en este caso comprende un multiplicador de frecuencia basado en un bucle bloqueado de fase por ejemplo, que se utiliza para multiplicar la frecuencia de referencia por 100 por ejemplo para generar la frecuencia más alta justo donde se requiere para el módulo de seguridad.

[0023] Según una forma de realización de la presente invención, otras técnicas se emplean por proporcionar medios para minimizar la cantidad de EMI que penetra desde el interior del dispositivo host al exterior. Como se ha descrito anteriormente, para un host que comunica con un módulo de seguridad de alta velocidad, al menos el reloj del módulo de seguridad (CK) y las conexiones de entrada/salida (IO) pueden ser susceptibles de producir cantidades significativas de EMI. Las conexiones de alta velocidad son mantenidas tan cortas como posible puesto que es conocido que la longitud sobre la que está presente una señal de alta frecuencia es una variable significativa que contribuye a la cantidad de EMI emitida. Adicionalmente, estas líneas son preferiblemente hechas de cableado blindado.

[0024] Según otra forma de realización de la presente invención, un protector se construye para reducir sustancialmente que cualquier EMI generada dentro del dispositivo host penetre al exterior del host. En esta forma de realización, el protector tiene forma de una lengüeta que cubre el puerto o ranura del dispositivo host a través del cual se inserta la tarjeta chip que comprende el módulo de seguridad.
La lengüeta está hecha de un material epoxi electroconductor o una resina electroconductora y está posicionada y dimensionada adecuadamente para incluir adecuadamente la tarjeta chip cuando se inserta en la ranura.
De esta manera, puesto que el epoxi o resina muestra propiedades elásticas, se forma un sello alrededor de la tarjeta chip cuando se inserta en la ranura.
Puesto que el epoxi o resina son electroconductores, la lengüeta proporciona protección contra EMI de manera que cualquier EMI generada en el dispositivo host no se propaga al exterior del dispositivo host o es al menos atenuada sustancialmente de forma que no sea considerada un problema.
Según variantes de esta forma de realización de la invención, la lengüeta se puede formar por una hoja de epoxi o resina, fijada a la parte superior o al fondo de la ranura o la lengüeta puede hacerse a partir de una hoja mayor de epoxi o resina con un corte de ranura cerca del medio de la hoja para recibir la tarjeta chip o la lengüeta se puede realizar por dos hojas de material de resina o epoxi, siendo la dos hojas fijadas adecuadamente a la ranura de manera que los bordes de las dos hojas concurren formando así la lengüeta cerca del medio de la ranura.

[0025] Cabe observar que el efecto técnico en la EMI alcanzada por cualquiera de las formas de realización de la presente invención sirve no solo para reducir la cantidad de EMI que penetra desde el interior del dispositivo host hacia el exterior, sino que sirve además para reducir la cantidad de EMI que penetra en el host desde el exterior, reduciendo así la posibilidad de que los componentes en el alojamiento sean afectados por interferencia desde el exterior.

[0026] Según otra forma de realización de la presente invención, una reducción en la cantidad de EMI que escapa desde el interior del dispositivo host hacia el exterior se consigue por la fabricación de un alojamiento para el dispositivo host, o al menos para los componentes del dispositivo host que son susceptibles de producir EMI, de un material plástico conductor.
Estos materiales proporcionan protección para la EMI debido a sus propiedades conductoras y no requieren los pasos adicionales de adición de capas conductoras o pintura conductora y por lo tanto contribuyen a minimizar el coste de fabricación de un alojamiento que proporcione protección de EMI.

[0027] En otra forma de realización de la presente invención, se hace provisión para proteger la EMI generada por vías que llevan señales de alta frecuencia de contaminar otros circuitos electrónicos en el dispositivo host y de escapar al exterior del dispositivo host. Preferiblemente, si las medidas han sido tomadas para minimizar el número de vías

afectadas y para reducir las longitudes de tales vías a un mínimo, entonces es fácilmente realizable la provisión anteriormente mencionada. En esta forma de realización, además de que se hace uso de la lengüeta de protección como se ha descrito anteriormente para impedir que EMI escape desde el host, se hace uso de una caja de protección que aísle aquellas vías que llevan señales de de alta frecuencia.

Por ejemplo, tal y como se menciona en los ejemplos precedentes, las dos vías de entrada/salida (10) y el reloj (CK) tienen que ser aislados. Las vías perjudiciales se aíslan geográficamente y físicamente se posicionan en una región cerca de la ranura del host, donde entrarán en contacto con el módulo de seguridad. La lengüeta (FLP) se utiliza para aislar la EMI generada por las vías desde el exterior del host. Este aislamiento se completa por el hecho de que el host se aloja en bien una caja metálica o una caja hecha de plástico conductor como se ha descrito anteriormente. Esta caja se designa como un alojamiento.

Además, para aislar la EMI del resto de los componentes electrónicos del host, se hace una pared en el alojamiento (HSE) bien de metal o de plástico conductor para aislar electromagnéticamente las vías perjudiciales del resto del circuito en el dispositivo host. Según otra forma de realización, en vez de formar sencillamente una pared, el metal o plástico conductor se puede formar para incluir las vías perjudiciales y conectar a la lengüeta, creando así una caja impermeable a la EMI en el dispositivo host. Las juntas entre el metal o plástico conductor están preferiblemente selladas con resina epoxi electroconductora puesto que hay espacios entre el metal o plástico conductor y la lengüeta asegurando así un aislamiento máximo.

[0028] Por lo contrario, o en combinación, como en otra forma de realización de la presente invención, en vez de encerrar las vías perjudiciales es una caja de protección contra la EMI, el resto de los circuitos en el dispositivo host, que pueden ser susceptibles a EMI que viene de las vías de alta frecuencia mencionadas anteriormente, se pueden aislar de la EMI generada externamente revistiéndolos con epoxi conductora que proteja contra la EMI o envolviéndolos con cinta conductora que proteja contra EMI.

Como con todas las técnicas que impliquen cintas, resinas, epoxis o adhesivos electroconductores, tal tratamiento puede ser parte de un tratamiento multicapa donde son aplicadas capas alternantes de cintas, resinas, epoxis o adhesivos no conductores y conductores.

[0029] Si cualquiera de las vías de alta velocidad mencionadas tienen que cubrir más que la distancia mínima posible, resulta preferible convertir tales señales en una señal diferencial sobre dos vías situadas muy próxima una de la otra - preferiblemente adyacentes entre sí a separación mínima o, si tales vías existen como cables, entonces como un par trenzado. Las señales deberían ser preferiblemente de un modo corriente, de nivel de voltaje mínimo de modo común y tener un giro de voltaje mínimo entre estados lógicos. Un protocolo diferencial de bajo voltaje tal como el protocolo de comunicación conocido como LVDS es adecuado para este tipo de vías. Según otra forma de realización de la presente invención, los conductores LVDS se utilizan para convertir la señal de reloj de un cable monoterminado a un bus diferencial de modo corriente de dos terminaciones con un resistor de cien ohmios y según el protocolo de comunicación LVDS. Un extremo del bus de dos terminaciones se utiliza para conducir el relleno de reloj del módulo de seguridad. Conductores Similares se utilizan para convertir la señal de entrada/salida para ser compatible con el protocolo LVDS .

REIVINDICACIONES

1. Método para la comunicación entre un módulo de seguridad (CH), estando dicho módulo de seguridad (CH) alojado en una tarjeta chip (CC), y un dispositivo host (HST), donde dicho dispositivo host (HST) comprende un lector de tarjetas (RDR_SL) para la conexión al módulo de seguridad (CH) por medio de al menos una línea de comunicación que funciona a una primera frecuencia, comprendiendo dicho método :
puesta en servicio del dispositivo host (HST) a una segunda frecuencia, siendo dicha segunda frecuencia inferior a la primera frecuencia, generando dicho funcionamiento una pluralidad de señales hacia el lector de tarjetas (RDR_SL), teniendo al menos una de las cuales una tercera frecuencia, siendo dicha tercera frecuencia igual o inferior a la segunda frecuencia, recibiendo el lector de tarjetas (RDR_SL) dicha pluralidad de señales; y
Conversión, por el lector de tarjetas (RDR_SL), de al menos una de las señales recibidas, donde dicha conversión produce al menos la línea de comunicación que funciona a la primera frecuencia,
caracterizado por el hecho de que:
Dichas señales recibidas comprenden dos señales subordinadas a reloj (CK0 CK1) separadas, adecuadamente sincronizadas y al menos dos entradas para dicho módulo de seguridad (I0, I1);
Dicha conversión siendo:
la generación de una señal de reloj (CK) para el módulo de seguridad por multiplexado de dichas dos señales subordinadas a reloj (CK0 CK1) separadas, adecuadamente sincronizadas;
Multiplexado a partir de dichas al menos dos entradas (10; I1) de una señal de entrada (I) para entrada en el módulo de seguridad; y
Demultiplexado de una señal de salida (O) de dicho módulo de seguridad para producir al menos dos salidas separadas (00, O1).

2. Dispositivo host (HST) que comprende un lector de tarjetas (RDR_SL) para la conexión de un módulo de seguridad (CH) al dispositivo host (HST), dicho módulo de seguridad (CH) siendo alojado en una tarjeta chip (CC), donde dicha conexión es hecha por medio de al menos una línea de comunicación, donde dicha línea de comunicación funciona a una primera frecuencia, donde dicho lector de tarjetas (RDR_SL) es adaptado para recibir una pluralidad de señales, dicho dispositivo host (HST) **caracterizado por el hecho de que**:

El lector de tarjetas (RDR_SL) se adapta para procesar la pluralidad de señales a una segunda frecuencia, siendo dicha segunda frecuencia inferior a la primera frecuencia, teniendo dicha pluralidad de señales una frecuencia menor o igual a la segunda frecuencia; y
El lector de tarjetas (RDR_SL) comprende un módulo convertidor para la conversión (CVT) de al menos una de la pluralidad de señales para producir al menos la línea de comunicación que funciona a la primera frecuencia,
caracterizado por el hecho de que:
Dichas señales recibidas comprenden dos señales reloj (CK0 CK1) separadas, adecuadamente sincronizadas y al menos dos entradas para dicho módulo de seguridad (10, I1),
Y dicho convertidor se adapta para generar una señal de reloj (CK) para el módulo de seguridad por multiplexado de dichas dos señales subordinadas a reloj (CK0 CK1) separadas, adecuadamente sincronizadas y se adapta para el multiplexado de dichas al menos dos entradas (10; I1) una señal de entrada (I) para la entrada en el módulo de seguridad y
se adapta para demultiplexar una señal de salida (O) de dicho módulo de seguridad para producir al menos dos salidas separadas (O0, O1).

3. Dispositivo host (HST) según la reivindicación 2, donde dicha línea de comunicación está hecha de cable que se adapta para proporcionar protección electromagnética.

4. Dispositivo host (HST) según la reivindicación 2, donde un protector es construido alrededor del dispositivo host, dicho protector es adaptado para reducir la interferencia electromagnética que entra al exterior del host.

5. Dispositivo host (HST) según la reivindicación 2, donde el dispositivo host (HST) comprende un alojamiento, comprendiendo dicho alojamiento material plástico conductor.

6. Dispositivo host (HST) según la reivindicación 2, donde dicha línea de comunicación se encierra dentro de una caja que está hecha de metal o de plástico conductor.

7. Dispositivo host (HST) según la reivindicación 2, donde todos los componentes que comprende el dispositivo host (HST), aparte de la línea de comunicación, están encerrados dentro de una caja que está hecha de metal o de plástico conductor.

8. Dispositivo host (HST) según la reivindicación 2, donde dicha línea de comunicación comprende un par diferencial.

9. Dispositivo host (HST) según la reivindicación 2, donde el par diferencial se adapta para funcionar en un modo corriente.

10. Dispositivo host (HST) según la reivindicación 2, donde el par diferencial se adapta para funcionar según un protocolo diferencial LVDS de bajo voltaje.

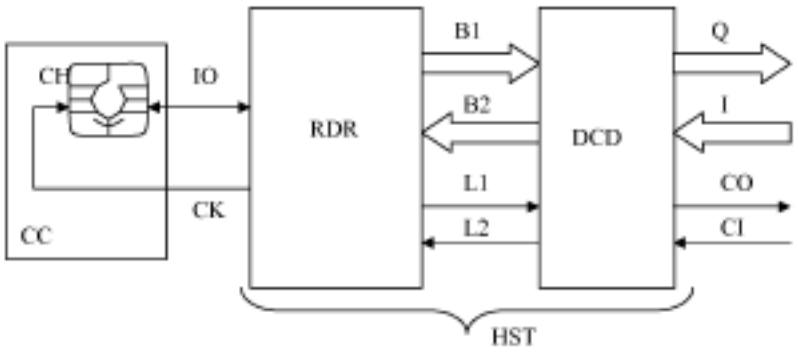

Fig. 1

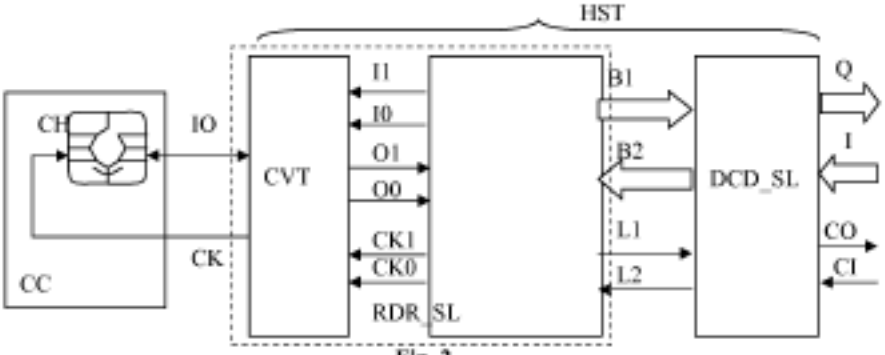

Fig. 2

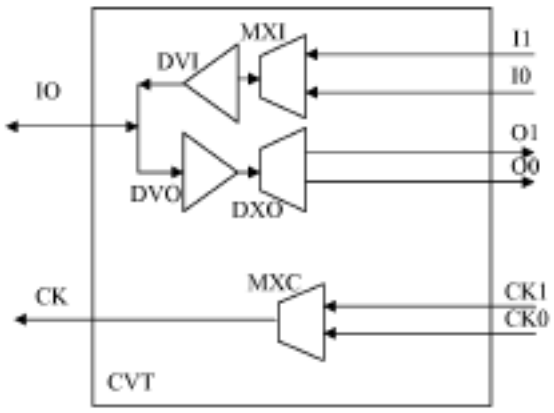

Fig. 3

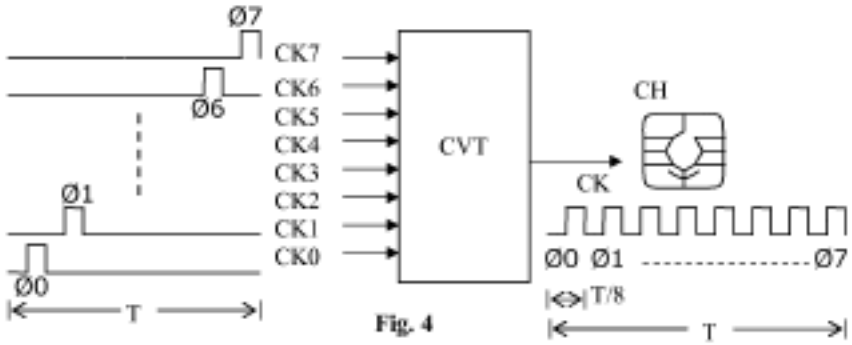
Ø7
CK7
CK6
Ø6
CK5
CK4
CK3
CK2
CK1
CK0
Ø1
Ø0
T
CVT
CH
CK
Ø0 Ø1
Ø7
T/8
T

Fig. 4

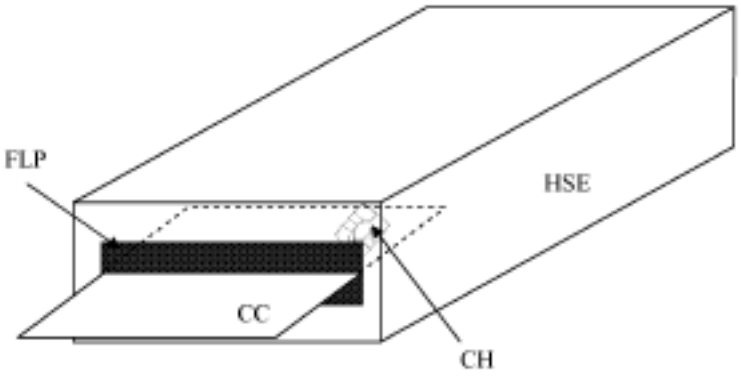
FLP
HSE
CC
CH

Fig. 5