

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4920748号
(P4920748)

(45) 発行日 平成24年4月18日 (2012. 4. 18)

(24) 登録日 平成24年2月10日 (2012. 2. 10)

(51) Int. Cl.

F I

G 0 6 F 21/02 (2006.01)

G 0 6 F 21/02 1 7 5

請求項の数 10 (全 9 頁)

(21) 出願番号	特願2009-513662 (P2009-513662)	(73) 特許権者	501263810
(86) (22) 出願日	平成19年6月4日 (2007. 6. 4)		トムソン ライセンシング
(65) 公表番号	特表2009-540410 (P2009-540410A)		Thomson Licensing
(43) 公表日	平成21年11月19日 (2009. 11. 19)		フランス国, 92130 イッシー レ
(86) 国際出願番号	PCT/EP2007/055458		ムーリノー, ル ジャンヌ ダルク,
(87) 国際公開番号	W02007/141233		1-5
(87) 国際公開日	平成19年12月13日 (2007. 12. 13)		1-5, rue Jeanne d' A
審査請求日	平成22年5月7日 (2010. 5. 7)		rc, 92130 ISSY LES
(31) 優先権主張番号	0652064		MOULINEAUX, France
(32) 優先日	平成18年6月8日 (2006. 6. 8)	(74) 代理人	100070150
(33) 優先権主張国	フランス (FR)		弁理士 伊東 忠彦
		(74) 代理人	100091214
			弁理士 大貫 進介
		(74) 代理人	100107766
			弁理士 伊東 忠重

最終頁に続く

(54) 【発明の名称】 セキュリティ機能を備えた電子ボード、及び電子ボードのセキュリティを確実にする方法

(57) 【特許請求の範囲】

【請求項 1】

電子カードであって、制御回路を含む複数の第1の電子回路を備える保護ゾーンであって、前記第1の電子回路は互いに3ミリメートル以下だけ離れており、電気リンクが前記第1の回路に接続され、3ミリメートルを上回る距離だけ前記第1の回路と離れて保護信号を送信する保護ゾーンと、3ミリメートルを上回る距離だけ、前記第1の回路と離れているか、又は前記保護信号を送信するその電気リンクが3ミリメートルを上回る距離だけ離れている第2の電子回路を備える非保護ゾーンとを備え、前記保護ゾーンは、前記第1の回路と前記第2の回路との間の信号の伝送を可能にする通信回路を備え、前記通信回路内の電気信号の伝送は、前記制御回路によって送出される電気制御信号によって調節される電子カード。

【請求項 2】

請求項1記載の電子カードであって、前記通信回路内の電気信号の伝送を調節する前記電気制御信号は、前記制御回路において実行される命令の動作コードに依存する電子カード。

【請求項 3】

請求項1及び2の何れか一項に記載の電子カードであって、前記通信回路内の電気信号の伝送を調節する前記電気制御信号は、前記制御回路において実行される命令の動作コードのアドレスに依存する電子カード。

【請求項 4】

10

20

請求項 1 乃至 3 の何れか一項に記載の電子カードであって、前記通信回路内の電気信号の伝送を調節する前記電気制御信号は、前記制御回路の出力ポートによって送出される電子カード。

【請求項 5】

請求項 1 乃至 4 の何れか一項に記載の電子カードであって、前記電気制御信号は、前記制御回路の入力ポートに、その電気ステータスを読み出すことができるように接続され、前記制御回路によって課される論理ステータスに、ポート上に存在しているステータスが対応しない場合に前記制御回路が遮断される電子カード。

【請求項 6】

請求項 1 乃至 5 の何れか一項に記載の電子カードであって、前記通信回路は、前記電子制御信号がイネーブルされると、前記制御回路がデータをバックアップすることを可能にし、よって、保護部分への前記データの出力を阻止する電子カード。

【請求項 7】

電子カード内のデータへのアクセス制御方法であって、制御回路を含む複数の第 1 の電子回路を備える保護ゾーンであって、前記第 1 の電子回路は互いに 3 ミリメートル以下だけ離れており、電気リンクが前記第 1 の回路に接続され、最大、3 ミリメートルを上回る距離だけ前記第 1 の回路と離れて保護信号を伝送する保護ゾーンと、3 ミリメートルを上回る距離だけ、前記第 1 の回路と離れているか、又は、前記保護信号を伝送する電気リンクが 3 ミリメートルを上回る距離だけ離れている第 2 の電子回路を備える非保護ゾーンとを備える電子カード内のデータへのアクセス制御方法において、

前記保護ゾーンは、前記第 1 の回路と前記第 2 の回路との間の信号の伝送を可能にする通信回路を備え、前記通信回路内の電気信号の伝送は、前記制御回路によって送出される電気制御信号によって調節され、前記方法は、その電気ステータスを読み出すことができるように前記制御回路によって前記電気制御信号を読み出す読み出し工程と、検出された電気ステータスが、前記制御回路によって課されるステータスに対応しない場合、前記制御回路を遮断する遮断工程とを含む、データへのアクセス制御方法。

【請求項 8】

請求項 7 記載の、データへのアクセス制御方法であって、前記電気制御信号のステータスは、前記制御回路において実行される命令の動作コードに依存する、データへのアクセス制御方法。

【請求項 9】

請求項 7 記載の、データへのアクセス制御方法であって、前記電気制御信号のステータスは、前記制御回路において実行される命令の動作コードのアドレスに依存する、データへのアクセス制御方法。

【請求項 10】

請求項 7 乃至 9 の何れか一項に記載の、データへのアクセス制御方法であって、前記電子制御信号がイネーブルされると、前記通信回路において記憶を行い、よって、非保護部分に対する前記データの出力を阻止するデータ記憶工程を含む、データへのアクセス制御方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、保護機能の特徴とする電子カード、及び電子カードを保護する方法に関する。

【背景技術】

【0002】

電子装置は、電子部品が装着される 1 つ又は複数のプリント回路を含む。回路の密度を増加させ、多くのピンを有する回路の使用を可能にするように、プリント回路には、数層の銅片を装備し、よって、電気接続を行う。銅片の幅は通常、0.3 ミリメートルである。数レベル間の電気接続を実現するために、最も一般的な手法は、スルーホール手法であ

10

20

30

40

50

る。プリント回路は、穴があけられており、穴の中でメタラゼーションを行って穴が交差する銅片全てを電気接続する。

【 0 0 0 3 】

装置には、セキュリティ機能を有するものもある。とりわけ、以下のもの（すなわち、銀行の装置、構内又はコンピュータに対するアクセス制御装置、危険な機器（放射線機器、兵器検査、軍用機等）の制御装置、暗号計算によって生成される対象の鍵又は署名をイネーブルするセキュリティ・モジュールを備える装置、テレビのデコーダ等）がある。前述の装置は一般に、セキュリティ・コードが正しく提示されると、データへのアクセスが可能になる。前述のセキュリティ・コードの検証は、部品のメモリに記録された鍵を使用して行われる。システムのセキュリティの大部分は、保護領域の外で前述の鍵を読み出すことが可能でないことによって生じる。機密データを含むメモリへのアクセスを保護するために、第1の方法は、樹脂又はポリマー接着剤に部品及びプリント回路全てを埋め込む工程を含む。樹脂ブロックに取り付けられたコネクタにより、通信（特に、アクセス・コードの導入）が可能になる。悪意を持った個人は、メモリ部品にアクセスしたい場合、プリント回路及び電子部品を劣化させることなく樹脂を分解しなければならない。難しいが、この作業は、有効な手段を使用することによって実現可能である。次に、悪意を持った個人は、回路をオンにし、非常に薄い先端部を有する金属製スタイラスを使用して、別々の部品間でやりとりされる信号をひそかに探ることが可能である。樹脂又はポリマー接着剤は、製造工程を複雑にし、プリント回路の価格を増加させる。スタイラスの挿入を妨げるための別の手段は、間隔が3ミリメートル以下になるように部品を近付けて保護する手段を含む。前述の距離を下回ると、スタイラスを滑り込ませることは可能でない。

【 0 0 0 4 】

一般に、部品の一部ののみがセキュリティに直接関係する。前述の部品には通常、中央処理装置、リードオンリ・メモリ、及び暗号プロセッサが挙げられる。保護する対象のデータは一般に、通信バスでやりとりされる。多数の回路がデータをこのバス上で送受信し、必ずしも、保護機能を有しない。しかし、前述の回路は、バスにより、同じ保護対象データを受信し、よって、互いの離間距離は最大3ミリメートルでなければならない。部品が5個を超える場合、この3ミリメートルの規則に従って前述の部品を配置することはほぼ不可能である。

【 0 0 0 5 】

I N N O V A C A R D によって出願された仏国特許出願公開第2857534号明細書には、保護リンクにより、互いに接続された普通モジュール及び保護モジュールを含む集積回路が開示されている。保護モジュールに送信された要求は、通常のバス上を非符号化状態で流れ、保護バス上で暗号化される。モジュールは、マスタ・エレメント及びスレーブ・エレメントを含む。マスタ・エレメントから来る要求はそのスクランプリング・モジュールにより、スレーブ・エレメントに送信される前に送信される。これは次いで、保護モジュールによって復号される。保護モジュールはそれをスレーブ・エレメントにルーティングする。上記文献には、プリント回路に付着させた導電体によって、信号を探ることが制限されることを可能にする解決策は開示されていない。

【 発明の開示 】

【 発明が解決しようとする課題 】

【 0 0 0 6 】

本発明はとりわけ、プリント回路の特定のゾーンにおける高レベルのセキュリティを確実にする一方で、集積回路を実現するうえでの制約を制限することを可能にする。

【 課題を解決するための手段 】

【 0 0 0 7 】

本発明は、制御回路を含む複数の第1の電子回路を備える保護ゾーンであって、上記第1の電子回路は互いに最大、所定の距離だけ離れており、電気リンクが第1の回路に接続され、最大、上記所定の距離だけ第1の回路と離れて保護信号を伝送する保護ゾーンと、上記所定の距離を上回る距離だけ、第1の回路と離れているか、又は保護信号を伝送する

その電気リンクが上記所定の距離を上回る距離だけ離れている第2の電子回路を備える非保護ゾーンとを備える電子カードにおいて、保護ゾーンは、第1の回路と第2の回路との間の信号の伝送を可能にする通信回路を備え、通信回路内の電気信号の伝送は、制御回路によって送出される電気制御信号によって調節される電子カードに関する。

【0008】

このようにして、セキュリティ制約を受ける信号は、制御回路が認可した場合にのみ、保護ゾーンを離れる。

【0009】

改良例によれば、いくつかの通信回路が、制御回路によって送出される同じ電気制御信号を受け取る。このようにして、比較的一般的な回路を電子カード上に使用し、配置して、信号全ての保護に必要な数を得ることが可能である。改良例によれば、第1の回路と第2の回路との間でやりとりされる信号の一部は通信回路を通過し、この回路を通過しない信号は、保護する対象としないといみなされる。このようにして、通信回路の数及び容量が最適化される。

10

【0010】

改良例によれば、通信回路内の電気信号の伝送を調節する電気制御信号は、制御回路において実行される命令の動作コードに依存する。このようにして、データの保護は、命令毎に行われる。変形例によれば、電気制御信号は、制御回路において実行される命令の動作コードのアドレスに依存する。このようにして、プログラム・コード・バンクは、区画に分け、セキュリティ基準を割り当てることが可能である。変形例によれば、電気制御信号は、制御回路の出力ポートによって送出される。よって、非常に一般的な回路を使用し、ポートを使用して、次いで実行されることになる命令の保護ステータス又は非保護ステータスを電気レベルでセットすることが可能である。

20

【0011】

改良例によれば、電気制御信号は、電子カード上に存在しているその電子ステータスを読み出すことができるように制御回路の入力ポートに接続される。制御回路は、入力ポートのレベルにおいて物理的に検出されたステータスが、制御回路によって課される論理ステータスに対応しない場合に遮断する。このようにして、電気制御信号をイナクティブなステータスに陥らせることが試行された場合、これを検出し、必要な場合、制御回路の動作を阻止することが可能である。改良例によれば、通信回路は、制御回路がデータをバックアップすることを可能にするメモリを含む。このようにして、通信回路及びメモリは単一の回路を構成するに過ぎない。したがって、保護ゾーンに集積させる対象の回路は1つ少なくなる。

30

【0012】

本発明は、制御回路を含む複数の第1の電子回路を備える保護ゾーンであって、上記第1の電子回路は互いに少なくとも所定の距離だけ離れており、電気リンクが第1の回路に接続され、最大、上記所定の距離だけ第1の回路と離れて保護信号を伝送する保護ゾーンと、上記所定の距離を上回る距離だけ、第1の回路と離れているか、又は、保護信号を伝送するその電気リンクが上記所定の距離を上回る距離だけ離れている第2の回路を備える非保護ゾーンとを備える電子カード内のデータに対するアクセス制御方法であって、

40

保護ゾーンは、第1の回路と第2の回路との間の信号の伝送を可能にする通信回路を備え、通信回路内の電気信号の伝送は、制御回路によって送出される電気制御信号によって調節され、上記方法は、その電気ステータスを読み出すことができるように制御回路によって電気制御信号を読み出す読み出し工程と、検出された電気ステータスが、制御回路によって課されるステータスに対応しない場合、制御回路を遮断する遮断工程とを含むアクセス制御方法に関する。

【発明を実施するための最良の形態】

【0013】

本発明の他の特性及び利点は、本出願記載の図を使用して説明する本発明の非限定的な実施例の説明から分かるであろう。

50

【実施例】

【0014】

好ましい実施例によれば、電子カードは、図1に示すような受信器（通常、表示装置2に接続されたデコーダ）において実現される。受信器は、番組メモリ6に接続された中央処理装置3と、リモコンの信号を受信するための赤外信号受信器7と、例えば前面パネル上にデータを表示するためのインタフェース回路5と、テレビ画面2に送出されるオーディオ/ビデオ信号を生成するためのオーディオ/ビデオ・デコード・ロジック9とを備える。受信器1は、OSD回路（画面上ディスプレイ（On Screen Display）の略）として表すことが多い、画面上にデータを表示する回路8も含む。OSD回路8は、メニュー、絵文字や他のグラフィックスの画面上の表示を可能にするテキスト及びグラフィックス生成器である。受信器は、特に、放送ネットワークのオーディオ及び/又はビデオ・データを、復調器4に接続された受信アンテナによって受信することを可能にするコネクタを有し、前述のネットワークは、無線、ケーブル又は衛星のタイプのものであり得る。コネクタにより、オーディオ・コンテンツの放送上で情報を受信することを可能にする局所の高ビットレートのデジタル・バスによる通信が提供される。インタフェース5は、他のコネクタにより、他の装置（例えば、USB、CVBS（コンポジット・ビデオ入力）又は4:2:2（CCIR656 - デジタル・ビデオ）のタイプの接続を装備した装置）を接続することも可能である。

10

【0015】

言うまでもなく、電子カードを装備し、保護機能を有する装置は何れも、本発明の範囲内に収まる。例えば、電子カードは、銀行の装置、構内又はコンピュータへのアクセス制御装置、危険な機器の制御装置、暗号計算によって鍵又は署名を生成することを可能にするセキュリティ・モジュールを備える装置、テレビのデコーダ等の中に配置することが可能である。

20

【0016】

図2は、保護する対象の回路、及び保護しなくてよい回路を略示した、印刷回路2.1の構成図を示す。保護する対象の回路を1つのプリント回路ゾーンにグループ化し、よって、保護ゾーンを規定する。前述の回路は、3ミリメートル（すなわち、互いの離間距離は3ミリメートル以内であり、保護ゾーンの回路間で保護するための信号を搬送するトラックは前述の距離よりも大きくなる）の規則に従う。前述の回路の中でも、場合によっては、実行可能なコード及び秘密データを格納するためのリードオンリ・メモリ2.3及び受信器1を大局的に制御する中央処理装置3であり得る制御装置2.2を見つけることが一般的である。他の回路2.4は、保護信号を受信しないように、それほど至近に設けなくてよい。保護信号を受信することを避けるために、保護ゾーンには、「アイソレーション出力を備えた論理バス用送信器回路」2.5、又は「バッファ」が装備される。バッファ2.5は、カードの保護ゾーンと電気回路の残りの部分との間で信号をやりとりすることができるポータル機能を実現する。実施例では、このドアは、双方向増幅器（又は「バッファ」）（例えば、74LVCR2245APWで表す回路）である。この回路は2つの制御入力を有する。DIR入力（図示せず）は、データの方法を規定し、バスのデータの伝送方向をどの時点でも規定する制御回路2.2に接続される。OE（出力イネーブル）入力は、バッファ2.5の出力をイネーブルするか、又はイネーブルしない。すなわち、前述の入力がイネーブルされない場合、出力は、トリステートロジックであり、その場合、入力に存在するデータを読み出すことは可能でない。OE入力がイネーブルされた場合、出力は、バッファ2.5の別々の入力線上に存在する信号を厳密に再生する。OE入力は配線2.6によって制御装置2.2に接続される。回路2.2、2.3及び2.5は全て、3ミリメートルの規則に従わなければならない。

30

40

【0017】

保護は以下のように提供される。制御回路2.2は、保護ゾーン外でデータを捕捉してはならない旨の命令を実行すると、配線2.6上でコマンドを伝送することにより、バッファ2.5をディセーブルする。信号はその場合、保護ゾーン内で、局所化された状態に

50

留まる。制御回路 2 . 2 によって実行される命令を保護しなくてよい場合、バッファ 2 . 5 をディセーブルして、保護ゾーン外の回路 2 . 4 にデータを一方又は他方の方向に転送することを可能にする。セキュリティを向上させるモードでは、保護ゾーンとその他の電子回路との間でやりとりされる信号は全て、バッファ 2 . 5 を通過する。参照記号 7 4 L V C R 2 2 4 5 A P W は、テスト・ポイントにおいてピンがアクセス可能でなく、8 本の線上でデータの転送を可能にする回路に関する。よって、5 本の制御線、1 6 データ・ビット、及び 2 4 アドレス・ビットのバスの場合、6 つのバッファ 2 . 5 が必要である。本発明の改良例によれば、交換されるデータ信号の一部はバッファ 2 . 5 を通過し、最も機密性の高いものが優先度を有する。バッファ 2 . 5 を通過する線の本数を 2 本乃至 3 本だけ、目に見えるほどセキュリティを低減させることなく削減することができることが経験上、明らかになっている。このようにして、実現する対象のバッファの数は制限することが可能である。バッファ 2 . 5 が、保護ゾーンにあり、よって、3 ミリメートルの規則に従わなければならないので、この利点は、なおさら重要である。実現されたプロトタイプでは、バッファ 2 . 5 を通過する信号は、以下の信号である。

【 0 0 1 8 】

データ・バスの 1 6 本の線のうちの 6 本。線の選択は、絵文字機能に応じて行われる。

【 0 0 1 9 】

アドレス・バスの 8 本の最上位の配線。変動を解析することによって、動作コード・ブロックの変動を検出することが可能であるので、前述の配線は、機密性がより高いように思われる。

【 0 0 2 0 】

入出力をイネーブルする O E (出力イネーブル) 制御信号、及び入出力の方向をイネーブルする R D / W R 。

【 0 0 2 1 】

図 3 は、保護ゾーンの主回路をその主リンクとともに示す図である。「周辺 T S O P 」とマーキングされたインタフェース回路は、保護ゾーンに属さない。直線により、かつ、バッファ 7 4 L V C R 2 2 4 5 A P W を通過する線により、「B G A C P U 」とマーキングされた制御回路に接続される。前述の直線は保護されない。

【 0 0 2 2 】

図 4 は、実現されるプロトタイプの実現形態例による、保護ゾーンの主回路を示す実施図である。特に、3 ミリメートルの規則の適用が分かる。

【 0 0 2 3 】

好ましい実施例によれば、バッファ 2 . 5 の制御配線 2 . 6 の論理ステータスは、制御回路 2 . 2 によって現在実行されている命令の保護特性又は非保護特性に依存する。この回路は、動作コードによって識別される 2 つの命令の組を有し、保護命令の組の何れの命令も、バッファ 2 . 5 のイネーブルを配線 2 . 6 を介してトリガする。非保護の組の命令の実行は、バッファ 2 . 5 のイネーブルをトリガしない。変形例は、制御回路 2 . 2 が、実行する対象の命令のメモリ・アドレスに応じて制御配線 2 . 6 の論理ステータスを更新する。単純な方法は、バンク・プログラム・メモリを共用する工程、及び各バンクに、保護特性を規定する表示子を割り当てる工程を含む。バンクが、「保護する」としてマーキングされている場合、このバンク内の命令実行記録は何れも、バッファ 2 . 5 への制御配線 2 . 6 をイネーブルする。効果的には、表示子は、制御回路 2 . 2 に一体化された E E P R O M メモリ内にあり、その初期化は部品のカスタム化ノードにおいて、かつ、アクセス・コードの提示後に行われる。第 3 の変形例は、バッファ 2 . 5 の制御配線 2 . 6 が制御回路 2 . 2 の I / O ポートの出力ピンに接続されなければならないというものである。実行可能なコード・ルーチンを実行する前に、制御回路 2 . 2 は、配線 2 . 6 をイネーブルすることを可能にするビットの値を命令によって初期化する。ルーチンの最後では、別の命令により、制御回路 2 . 2 は配線をディセーブルする。

【 0 0 2 4 】

改良例によれば、制御回路 2 . 2 は、配線 2 . 6 の電気ステータスを読み出すことを可

10

20

30

40

50

能にする入力回路を有する。この改良例は、前述の配線上でイナクティブ・ステータスを課すことを、悪意を持った個人が首尾良く行うケースにおいて特に有用である。それにより、バッファ 2 . 5 によって構成されるポータルが開状態のままにされ、その場合、保護信号を確かめることが可能になる。よって、実行可能なプログラムは、配線 2 . 6 の論理ステータスのコマンドが実際に、その電気レベルに対応するか否かを検査することが可能である。プログラムが、ディセーブル動作に対応する電気レベルを、そのコマンドがそれをイネーブルする一方で、検出した場合、遮断され、保護機能全ての実行を禁止する。遮断は、制御回路内のヒューズの溶断を含み得る。その後の電源オン動作中、制御装置 2 . 2 は、ヒューズのステータスを検査し、ヒューズが飛んだ場合、その動作を中断する。別の方法は、制御装置 2 . 2 内又は制御装置 2 . 2 外のメモリ内の E E P R O M セルにヒューズのステータスに対応する情報を書き込む工程を含む。

10

【 0 0 2 5 】

本発明の別の実施例によれば、メモリ 2 . 3 の少なくとも 1 つの部分がバッファ 2 . 5 に一体化される。図 5 は、保護する対象の回路、及び保護しなくてよい回路を略示した、印刷回路 2 . 1 の構成図を示す。よって、メモリ 3 . 1 は、制御信号、アドレス・バス、及びデータ・バスに対する直接アクセス・ポート、並びに、印刷回路の非保護部分に対する信号の入力及び出力のための 2 次ポートを有する。この実施例では、2 次ポートは、所定数のメモリ・ワードを備えた、メモリの一部としての制御回路 2 . 2 によってみられ、メモリ・ワードは特定数のデータ・ビットを有する。例えば、2 次ポートは、データの方向、及びアドレス信号の構成が 2 次ポート上で有効であることを表す、「R / w」及び「V W A」などの制御信号及び 8 本のデータ線、8 本のアドレス線を備える。この例では、2 次ポートは、2 5 6 バイトのメモリとして制御回路 2 . 2 によってみられる。通信回路 (2 . 5) は、データをバックアップし、電気制御信号 (2 . 6) がイネーブルされると、保護部分における前述のデータの伝送は認可されない。このようにして、情報は、機密の場合、保護部分のメモリ内に留まり、非保護部分の電子回路によって読み出すことが可能でない。

20

【 0 0 2 6 】

図 6 は、その他の実施例による、保護ゾーンの主回路をその主リンクとともに示す図である。リードオンリ・メモリは、「フラッシュ B G A」タイプのメモリ、及び少なくとも 1 つのバッファ 7 4 L V C R 2 2 4 5 A P W を備える。リンクの本数が削減されていることが、図 3 と比較すれば分かる。バッファ及びメモリを単一の回路に一体化したことにより、保護ゾーンの容量が削減される。

30

【 0 0 2 7 】

図 7 は、図 4 によって表すその他の実施例による、保護ゾーンの主回路の実施図を示す。図 4 と比較すれば、3 回路から 2 回路になると、プリント回路上の保護環境によって占有される空間が削減される。

【 0 0 2 8 】

この実施例は、その目的が例証的であるとみなされなければならないが、特許請求の範囲記載の範囲によって規定される範囲において修正することが可能である。特に、本発明は、上記デコーダに限定されず、セキュリティ制約を有する回路を装備した何れの装置にも適用される。

40

【図面の簡単な説明】

【 0 0 2 9 】

【図 1】電子カードの実施例を含むテレビ番組受信器の構成図である。

【図 2】実施例による、保護ゾーンを示す電子カードを示す構成図である。

【図 3】本発明の実現形態例による保護ゾーンの主回路を略示した図である。

【図 4】実現形態例による、保護ゾーンの主回路を示す実施図である。

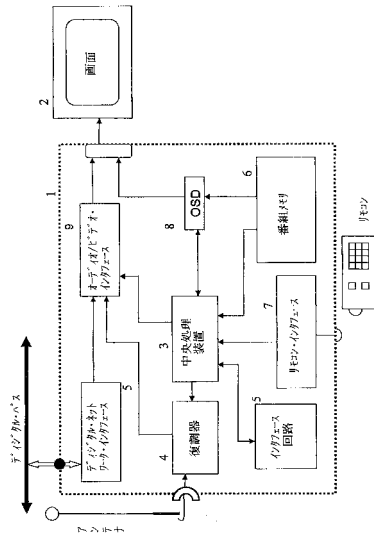
【図 5】改良例による、保護ゾーンを示す電子カードを示す構成図である。

【図 6】図 5 で示す改良例による、保護ゾーンの主回路を示す図である。

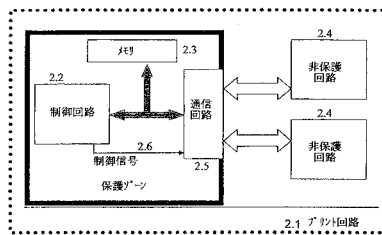
【図 7】実現形態例による、保護ゾーンの主回路を示す実施図である。

50

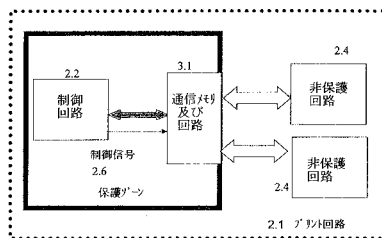
【図 1】



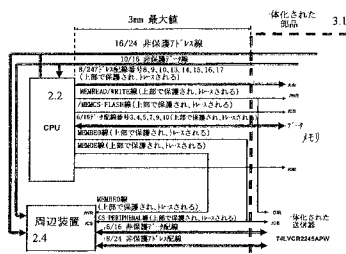
【図 2】



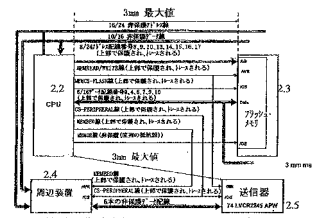
【図 5】



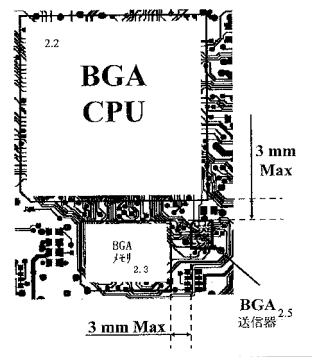
【図 6】



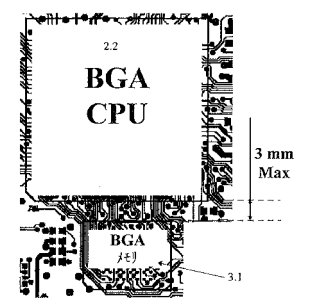
【図 3】



【図 4】



【図 7】



フロントページの続き

- (72)発明者 ギロ, フィリップ
フランス国, 3 5 1 7 0 ブリュズ, リュ・デ・ロシニョル 2 0
- (72)発明者 ヴィネロン, パトリック
フランス国, 3 5 0 0 0 レンヌ, リュ・ラオール・ボンション 6
- (72)発明者 ロネイ, フィリップ
フランス国, 3 5 2 0 0 レンヌ, リュ・テオフィル・ビュネル 6

審査官 和田 財太

- (56)参考文献 特開昭 6 3 - 1 2 4 1 5 5 (J P , A)
特開平 1 0 - 2 9 4 3 2 5 (J P , A)
特開平 1 1 - 2 5 8 2 9 3 (J P , A)
特開 2 0 0 5 - 2 5 0 5 3 8 (J P , A)
特開 2 0 0 5 - 2 7 8 1 8 9 (J P , A)
国際公開第 2 0 0 5 / 0 0 6 1 5 6 (W O , A 2)
欧州特許出願公開第 1 3 8 7 2 3 8 (E P , A 1)
米国特許第 6 4 1 8 5 5 2 (U S , B 1)
米国特許出願公開第 2 0 0 5 / 0 2 5 7 1 8 2 (U S , A 1)

- (58)調査した分野(Int.Cl. , D B 名)
- G06F 21/02
H05K 1/00- 3/00