(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2006-505798
(P2006-505798A)
(43)公表日　平成18年2月16日(2006.2.16)

(51)Int.Cl.		F I			テーマコード（参考）
G01R 31/28	(2006.01)	G01R	31/28	ZECG	2G132
G06F 11/22	(2006.01)	G06F	11/22	360P	5B048
G06F 21/22	(2006.01)	G06F	9/06	660L	5B076

審査請求 未請求　予備審査請求 未請求　（全 18 頁）

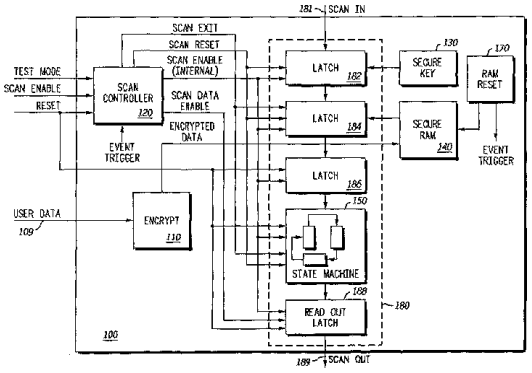
(21)出願番号　特願2004-557093 (P2004-557093)
(86)(22)出願日　平成15年4月14日 (2003.4.14)
(85)翻訳文提出日　平成16年11月29日 (2004.11.29)
(86)国際出願番号　PCT/US2003/011399
(87)国際公開番号　WO2004/051294
(87)国際公開日　平成16年6月17日 (2004.6.17)
(31)優先権主張番号　10/135,877
(32)優先日　平成14年4月30日 (2002.4.30)
(33)優先権主張国　米国 (US)

(71)出願人　504199127
フリースケール　セミコンダクター　インコーポレイテッド
アメリカ合衆国テキサス州７８７２９，オースティン，ウエスト・パーマー・レーン　７７００
(74)代理人　100116322
弁理士　桑垣　衛
(72)発明者　トカシク、トーマス
アメリカ合衆国　８５０４４　アリゾナ州　フェニックス　エス．サーティエイス　プレイス　１３４０６

最終頁に続く

(54)【発明の名称】機密保護走査試験のための方法および装置

(57)【要約】
電子的ハッキングから感知可能情報を保護するためのプロセッサ、走査コントローラおよび方法。プロセッサ内に存在する感知可能データのセキュリティを維持するために、走査コントローラは、プロセッサの走査観察可能部分からデータが除去されるまで、走査チェーンへのアクセスを拒否し、次に試験モードから抜け出す前に走査チェーンを再びクリアし、通常動作を再開する。試験モードへおよび／またはから遷移する場合に、プロセッサの走査観察可能部分内に記憶しているデータを除去または他の方法で修正すると、許可を受けていない人が、走査チェーンから機密保護データを簡単にシフトするのが防止され、感知可能状態情報を設定しようとする際に、通常動作の前に走査チェーン内にデータが予め負荷されるのが防止される。



【特許請求の範囲】
【請求項１】
構成信号を受信して試験のために走査チェーン（１８０）を準備するステップと、
前記構成信号に応じて、データ・プロセッサの走査観察可能部分の情報を修正するステップと、
前記修正ステップの後で、前記走査観察可能部分の走査試験をできるようにするステップと、を含む方法。
【請求項２】
前記修正ステップが、前記構成信号に応じて、前記走査観察可能部分をリセットすることを含み、
前記走査試験をできるようにするステップが、イネーブル走査信号を生成して前記走査観察可能部分内で走査ロジックを動作できるようにすること、を含む請求項１に記載の方法。
【請求項３】
前記走査試験をできるようにするステップの前に、前記走査観察可能な部分に情報が走査されるのを防止するステップと、
前記走査試験をできるようにするステップの前に、前記走査観察可能部分から情報が走査されるのを防止するステップと、をさらに含む請求項１に記載の方法。
【請求項４】
構成インジケータを受信して、通常動作のために走査チェーン（１８０）を準備するステップと、
前記構成インジケータに応じて、データ・プロセッサ（１００）の走査観察可能部分の情報を修正するステップと、
前記修正ステップの後で前記データ・プロセッサの通常動作を可能にするステップとを含む方法。
【請求項５】
前記修正ステップが、前記走査観察可能部分をリセットすること、を含む請求項４に記載の方法。
【請求項６】
前記走査試験をできるようにするステップの後で、前記走査観察可能部分内に情報が走査されるのを防止するステップと、
前記走査試験をできるようにするステップの後で、前記走査観察可能な部分から情報が走査されるのを防止するステップとをさらに含む、請求項４に記載の方法。
【請求項７】
走査試験の前に、走査リセット信号を供給するためのロジックを備え、前記走査リセット信号がデータ・プロセッサの走査観察可能な部分の情報を修正する走査コントローラ（１２０）。
【請求項８】
通常モード中に機密保護情報を処理するための機能部分であって、試験モード中に観察することができる機能部分と、
前記機能部分を試験する前に、前記機能部分の情報を修正することにより、前記機密保護情報へのアクセスを防止するための試験制御部分とを備えるプロセッサ。
【請求項９】
前記試験制御部分が、走査試験の前に走査リセット信号を供給するためのロジックを備え、前記走査リセット信号が前記プロセッサの前記機能部分の情報を修正する、請求項８に記載のプロセッサ。
【請求項１０】
前記試験制御部分が、走査試験の後で走査リセット信号を供給するためのロジックをさらに備える、請求項８に記載のプロセッサ。
【発明の詳細な説明】

【技術分野】
【０００１】
本発明は、概して、プロセッサ走査試験に関し、特に走査試験機密保護デバイスに関する。
【背景技術】
【０００２】
走査チェーンの最も基本的な形態の場合、走査チェーンは、１つの素子の出力が次の素子の入力に直列にリンクし、この素子の出力が次の素子の入力にリンクし、以後同様に前の素子の出力が次の素子の入力にリンクするように一緒にリンクしている一連の素子である。場合によっては、回路設計者は、そうでない場合にはアクセスすることができないプロセッサの内部素子に試験の目的でアクセスするために、走査チェーンを使用する。走査チェーンを使用することにより、試験エンジニアは、１つの入力ポートを通してデータをプロセッサ内に順次シフトすることができる。プロセッサは、データを処理して、次に、１つの出力ポートを通して、処理結果が順次読み出される。このようにして、最大量の内部回路を、複雑になるのを最小限度に留めながら試験することができる。
【０００３】
しかし、試験はこのように簡単になっても、データにアクセスする問題が起こる。この問題は、特に、ソフトウェア、電気通信、エンターテインメントおよび他の産業の暗号化および機密保護要件の観点から見て考慮に入れなければならない。例えば、電気通信産業は、携帯電話、ポケットベル（ｐａｇｅｒ）等で情報を処理するために使用する半導体チップの中のあるものに機密保護コードを記憶させる必要がある。これらの機密保護コードは、機密保護状態を指定する目的でハードウェアの識別および認証を行うための、または他のいくつかの目的のための専用のデータ処理方法の一部として使用することができる。しかし、これらのコードを取り扱うための回路が、走査チェーンを介してアクセスすることができる場合には、競合相手が、チップ内に記憶している機密保護コードにアクセスするために、または機密保護状態に侵入するために走査チェーンを利用できるかもしれない。
【０００４】
チップ内に記憶している機密保護情報にアクセスすべく走査チェーンを利用する、またはチップをだまして機密保護状態にあるように思い込ませて走査チェーンを利用する、という問題を解決するために、メーカーは、一般的に、機密保護情報を処理するために使用した回路を走査チェーンから除去しておく。走査チェーンからこの回路を除去することにより、許可を受けていないユーザが機密保護コードにアクセスするのがますます困難になる。しかし、この解決方法を使用した場合には、チップのかなりの部分を完全には試験できないという問題が残る。
【発明の開示】
【発明が解決しようとする課題】
【０００５】
上記説明から明らかなように、現在入手できる試験方法は、これらの試験方法を使用した場合、設計者は、データの機密保護を犠牲にして試験のためのアクセスをするか、またはデータ・プロセッサのかなりの部分に試験のためのアクセスをしないでデータの機密保護を守るか、のどちらかを選択しなければならないという点で理想的な方法であるとは言えない。現在必要なのは、機密保護情報を処理するプロセッサの一部に試験のためにアクセスすることはできるが、すべての機密保護情報の秘密をプロセッサ内に機密保持する何らかの方法である。
【課題を解決するための手段】
【０００６】
添付の図面を参照しながら、下記の説明および特許請求の範囲を読めば、本発明の種々の利点、機能および特徴、および構造の関連素子の方法、動作および機能、並びに製造部材および製造の経済性の組合せを理解することができるだろう。上記図面、説明および特

許請求の範囲は、すべて本明細書の一部を形成している。
【発明を実施するための最良の形態】
【０００７】
下記の図面の詳細な説明においては、「アサート（ａｓｓｅｒｔ）する」および「否定する」（または「アサートを解除する」）という用語は、信号、状態ビットまたは類似の装置を、それぞれ論理的真または論理的偽の状態にする行為に言及する際に使用する。論理的真の状態が論理レベル１である場合には、論理的偽の状態は論理レベル０である。論理的真の状態が論理レベル０である場合には、論理的偽の状態は論理レベル１である。
【０００８】
それ故、本明細書で説明する各信号は、正または負のロジックとして設計することができる。この場合、負のロジックは、信号名の上のバーにより、または信号名の後のアステリスク（＊）で表すことができる。負の論理信号の場合には、信号はアクティブ・ロー・レベルにあり、論理的真の状態は論理レベル０に対応する。正の論理信号の場合には、信号はアクティブ・ハイ・レベルにあり、論理的真の状態は論理レベル１に対応する。
【０００９】
図１～図７は、プロセッサ試験モードにより感知可能情報へのアクセスを防止することにより、電子ハッキングに対する保護レベルを実現するために、情報プロセッサ内で走査コントローラをどのように使用できるかを示す。機密保護が維持されるこの方法を使用すれば、感知可能情報の機密保護を犠牲にしないで、構成要素試験の範囲を広げることができる。試験範囲が広くなると、製品の試験のコストが安くなり、市場へもっと短時間で出荷できるようになる。
【００１０】
感知可能データのセキュリティを維持するために、本明細書において説明する一実施形態は、走査チェーンにアクセスできるようにする前に、プロセッサの走査を観察することができる部分から読出感知可能セキュリティ・データを除去して試験モードから外し、通常動作を再開する前に書込感知可能セキュリティ・データを除外する。これらの時点で走査チェーンの感知可能部分を除去すれば、許可を受けていない人が機密保護データを簡単に走査したり、感知可能状態情報を設定するために通常動作の前に走査チェーン上に要素を予め負荷することが防止される。
【００１１】
図１について説明すると、この図は、本明細書に記載する教示による走査コントローラを使用するプロセッサである。参照番号１００はプロセッサ全体を示す。プロセッサ１００は、一連のラッチ１８２～１８８および走査チェーン１８０上に位置する状態機械１５０、機密保護キー１３０および機密保護ランダム・アクセス・メモリ（ＲＡＭ）１４０のような感知可能情報の種々のソース、および走査チェーン１８０へのアクセスを制御し、リセットおよび／またはモード構成信号を供給する走査コントローラ１２０を含む。プロセッサ１００は、またユーザのデータを暗号化するための暗号化ブロック１１０、および機密保護ＲＡＭ１４０から情報をクリアするためのＲＡＭリセット１７０を含む。走査チェーン１８０上にはいくつかの要素しか示していないが、例えば、暗号化ブロック１１０のような走査試験を必要とする任意の要素も走査チェーン１８０上に設置することができることに留意されたい。
【００１２】
アクセスから保護しなければならない情報は、配線識別キー（ｈａｒｄｗｉｒｅｄ　ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　ｋｅｙ）および専用ハードウェア／ファームウェアが実施したアルゴリズム、または製造後に記憶した感知可能情報のような、製造中にプロセッサ１００内に記憶した情報を含むことができる。例えば、機密保護キー１３０は、特定の移動体通信デバイスを識別するために使用するハードウェア識別キーであってもよいし、状態機械１５０は、プロセッサのモードが機密保護動作モードであるかどうかを判断するために、プロセッサ１００が使用する一連の論理要素であってもよい。これらそれぞれの場合において、プロセッサ１００内に組み込まれた情報は、偽造を防止するために、または

競合者によるリバース・エンジニアリングをさらに困難にするために、機密保護状態に維持しなければならない。

【００１３】

機密保護キー１３０は製造中に実施することができるが、機密保護ＲＡＭ１４０は、製造プロセスが終了した後でプロセッサ１００内で機密保護情報を記憶するための１つの方法である。例えば、プロセッサ１００が無線インターネット装置で使用するグラフィックス・プロセッサであると仮定しよう。特定のサービス・プロバイダが専用のグラフィックス圧縮アルゴリズムを有している場合には、プロバイダは、暗号化したアルゴリズムをユーザ・データ入力１０９を通して、プロセッサ１００内にロードすることができる。プロセッサ１００は、次に、暗号化ブロック１１０によりこのアルゴリズムを解読し、解読したデータを記憶するために機密保護ＲＡＭ１４０に転送する。当業者であれば、図１に示す方法の他に、または代わりに、プロセッサ１００に情報を記憶するための適当な方法を本明細書の教示から逸脱することなしに使用することができることを理解することができるだろう。

【００１４】

ラッチ１８２、１８４、１８６および１８８は、通常モードおよび試験モードの両方のモードで機能することができる。通常モードの場合には、ラッチ１８２および１８４および状態機械１５０は、プロセッサ１００の他の部分が使用できるように感知可能情報を保持する。例えば、ラッチ１８２は、機密保護キー１３０にアクセスするために使用する多数のラッチのうちの１つであってもよく、機密保護キー１３０をプロセッサ１００の認証部分（図示せず）に配信することができる。もう１つの例について説明すると、暗号化したソフトウェア・サブルーチンを、ラッチ１８４を通して機密保護ＲＡＭ１４０から中央処理装置に送ることができる。ラッチ１８２または１８４が、正式な許可なしでアクセスしてはならない情報を含んでいる場合には、ラッチは読出感知可能情報を含んでいると言われる。

【００１５】

状態機械１５０は、プロセッサ１００を非機密保護モードにするデータを保持することができる。状態機械１５０内の状態データを、走査モードから抜け出す直前に変更することができる場合には、プロセッサにモードが非機密保護モードであると思い込ませ、それにより機密保護動作が危険にさらされる恐れがある。走査モード動作の後で記憶から保護する必要があるデータを書込感知可能データと呼ぶことができる。他のラッチ（図示せず）は、読出または書込感知可能情報を含むことができる他の状態機械（図示せず）の出力を記憶するために使用することができる。これらの各例の場合、走査チェーンへのアクセスが保護されていない場合には、データのセキュリティが危険にさらされる恐れがある。

【００１６】

試験モードの場合には、ラッチ１８２、１８４、１８６および状態機械１５０に関連するラッチは、走査チェーン１８０を介して、プロセッサ１００の外部から観察することができる。走査チェーン１８０へのアクセスは、スキャンイン・ポート１８１およびスキャンアウト・ポート１８９を通して行われる。データは、スキャンイン・ポート１８１を介して、ラッチ１８２、すなわち走査チェーン１８０上の第１の走査観察可能なラッチにクロック制御の下で送られる。データが、ラッチ１８２内にクロック制御の下で送られる度に、ラッチ１８２のところの出力データは、ラッチ１８４の入力に送られる。ラッチ１８２の出力データがラッチ１８４の入力に送られる度に、出力データ・ラッチ１８４がラッチ１８６の入力に送られ、データがチェーンを通してスキャンアウト・ポート１８９に送られるまで、同じ動作が反復して行われる。例えば、図の走査チェーン１８０において、論理１が第１のクロック・サイクル中にラッチ１８２内にクロック制御の下で送られたと仮定しよう。第２のクロック・サイクル中、ラッチ１８２内に記憶された論理１は、ラッチ１８４に配信される。第３のクロック・サイクル中、同じ論理１がラッチ１８６に送られる。このプロセスは、最後に、論理１が読出しラッチ１８８に転送され、第４のクロック・サイクル中に、スキャンアウト・ポート１８９上での読出しのために使用できるよう

になるまで継続して行われる。当業者であれば、この簡単な例は単に例示としてのものに過ぎないこと、特定のラッチにシフトしたデータを走査チェーン１８０の残りの部分を通して送る前に、種々の方法で操作することができることを理解することができるだろう。

【００１７】

図の実施形態の場合には、読出しラッチ１８８は、ラッチ１８２、１８４および状態機械１５０とは対照的に、通常モード中、感知可能データを保持しない。代わりに、読出しラッチ１８８は、走査コントローラ１２０の制御の下で、ある所定の条件の場合を除いて、走査チェーンからのデータの読出しを阻止する。図示していないが、読出しラッチ１８８に類似の方法で制御されているラッチを、任意のデータが走査されるのを阻止するために、走査チェーン１８０への入力のところで使用できることを理解することができるだろう。また、以下に説明する種々の実施形態のような他の実施形態の場合には、読出しラッチ１８８を使用しないことも理解することができるだろう。

【００１８】

走査コントローラ１２０は、走査チェーン１８０へのアクセスを制御し、それによりラッチ１８２、１８４および状態機械１５０に記憶することができるすべての感知可能情報へのアクセスを制御する。少なくとも１つの実施形態の場合には、走査コントローラ１２０は、入力としてＴＥＳＴ　ＭＯＤＥ信号、ＳＣＡＮ　ＥＮＡＢＬＥ信号、ＲＥＳＥＴ信号、およびＥＶＥＮＴ　ＴＲＩＧＧＥＲ信号を受信する。これらの入力信号を使用して、走査コントローラ１２０は、ＳＣＡＮ　ＥＮＡＢＬＥ（ＩＮＴＥＲＮＡＬ）信号およびＳＣＡＮ　ＤＡＴＡ　ＥＮＡＢＬＥ信号を生成し、これらの信号は走査試験を行うことができるように、ラッチ１８２～１８８および状態機械１５０を構成するために使用される。例えば、アサートしたＳＣＡＮ　ＥＮＡＢＬＥ（ＩＮＴＥＲＮＡＬ）は、各走査ラッチを走査モードにするが、アサートした走査データ・イネーブルは、データをスキャンアウト・ポート１８９に走査できるようにする。走査コントローラ１２０は、また必要に応じて走査チェーン１８０上の素子をリセットするために使用されるＳＣＡＮ　ＥＸＩＴおよびＳＣＡＮ　ＲＥＳＥＴ信号を生成する。

【００１９】

図の実施形態の場合には、走査コントローラ１２０は、走査チェーン１８０に関連する大部分のリセット・シーケンスを制御し、各ラッチ１８２～１８８および状態機械１５０が、確実に必要に応じて正しくリセットされるようにする。図の実施形態の場合には、感知可能情報を記憶するのに使用しないラッチ１８６および１８８は、感知可能情報を保護するためにリセットする必要がないことに留意されたい。しかし、「ハード」リセット中または他の時点でラッチ１８６および１８８をリセットすることが望ましい場合もあるので、走査コントローラ１２０へのＲＥＳＥＴ入力が、ラッチ１８６、１８８をリセットするために供給される。他の実施形態の場合には、ＲＥＳＥＴ信号をＳＣＡＮ　ＲＥＳＥＴ信号の他に、例えば、状態機械１５０のような機密保護走査チェーン素子に供給することができる。多くの状況の下で、走査チェーン上の各素子をリセットするのが望ましい場合があるが、非感知性要素は、本明細書の教示から逸脱することなしに、走査コントローラ１２０の出力によりリセットしない状態に保持することができる。

【００２０】

一実施形態の場合には、ＲＡＭリセット１７０は、あるイベントに応じて機密保護ＲＡＭ１４０から情報をクリアするために使用される。ＲＡＭリセット１７０は、別のリセット状態機械（図示せず）により、走査コントローラ１２０により直接、または他の方法により制御することができる。ＲＡＭリセット１７０は、また、機密保護ＲＡＭ１４０内に記憶しているデータのクリアに成功したことを示すＥＶＥＮＴ　ＴＲＩＧＧＥＲ信号を供給することができる。この出力信号は、走査コントローラ１２０に対するＥＶＥＮＴ　ＴＲＩＧＧＥＲ入力として使用することができる。機密保護ＲＡＭ１４０をリセットするのに必要な時間がはっきりしない場合には、ＥＶＥＮＴ　ＴＲＩＧＧＥＲ信号を使用すると特に有利である。図の実施形態ではＲＡＭリセット１７０が使用されているが、すべての実施形態にとって必要なものではないことを理解することができるだろう。少なくとも一

実施形態の場合には、ＳＣＡＮ　ＤＡＴＡ　ＥＮＡＢＬＥ信号、ＳＣＡＮ　ＥＮＡＢＬＥ（ＩＮＴＥＲＮＡＬ）信号、およびＥＶＥＮＴ　ＴＲＩＧＧＥＲ信号または他の類似の信号の生成が、少なくとも部分的には、走査チェーン１８０の素子内に含まれているデータが、リセットまたは他の方法により機密保護されているかどうかを示す信号（図１に図示せず）により制御される。このような信号の一実施形態としてはＵＮＳＥＣＵＲＥ＊信号があるが、これについては後で図５のところで説明する。

【００２１】

図２を参照しながら、本発明のある実施形態によるプロセッサ１００（図１）のようなプロセッサを走査試験するための方法について説明する。この方法はステップ２１０からスタートする。この場合、プロセッサ１００は、通常モード、すなわち非試験モードで動作している。通常モードの場合には、走査チェーン１８０上の素子は、通常の処理タスクを実行するために使用される。走査チェーン１８０の素子が通常モードである場合には、これらの素子には、スキャンイン・ポート１８１またはスキャンアウト・ポート１８９を介してアクセスすることができない。何故なら、ラッチ１８２～１８８および状態機械１５０は、その走査チェーン・ポートを介して情報を送受信するように構成されていないからである。通常モードの場合、ラッチ１８２、１８４および状態機械１５０は、感知可能データまたは状態情報を含むことができる。そのため、走査チェーン１８０上の素子が、通常動作中に走査チェーン・アクセスのために動作できるようにすることができる場合には、走査チェーンの素子内に含まれている任意の情報をスキャンアウト・ポート１８９から読み出すことができ、情報のセキュリティが危険にさらされる恐れがある。

【００２２】

この方法はステップ２２０に進む。このステップにおいては、リセットによる試験のために、または所望の入力または入力の組合せに応じて、走査チェーン・ラッチ１８２、１８４および状態機械１５０内の感知可能データを他の方法で修正するために走査チェーンの準備が行われる。例えば、一実施形態の場合には、アサートされたＴＥＳＴ　ＭＯＤＥ信号およびアサートされたＳＣＡＮ　ＥＮＡＢＬＥ信号を受信すると、走査コントローラ１２０は、ラッチ１８２、１８４および状態機械１５０のリセット・ピンに直接供給することができるアサートされたＳＣＡＮ　ＲＥＳＥＴ信号を生成する。別の方法としては、適当なハードウェア、ソフトウェアまたはファームウェア・コントローラは、機密保護データがラッチから決して検索されないように、ランダムにまたは他の方法でラッチ１８２、１８４および状態機械１５０内のデータを修正することができる。

【００２３】

ステップ２３０において、走査コントローラは、任意の感知可能データがクリアされたか、または他の方法で修正されたかをチェックする。ステップ２３０において、走査コントローラ１２０の入力のところにアサートされたＥＶＥＮＴ　ＴＲＩＧＧＥＲ信号が存在しているかどうかをチェックすることができ、ＥＶＥＮＴ　ＴＲＩＧＧＥＲ信号がアサートされない場合には、ＳＣＡＮ　ＥＮＡＢＬＥ（ＩＮＴＥＲＮＡＬ）信号もアサートされない。例えば、走査チェーン１８０にアクセスできるようになる前に、機密保護ＲＡＭ１４０をリセットしたい場合には、走査コントローラ１２０は、機密保護ＲＡＭ１４０のリセットがすでに完了したことを示すＲＡＭリセット１７０からの信号を受信するために待機することができる。他の実施形態の場合には、ＥＶＥＮＴ　ＴＲＩＧＧＥＲ信号は必要ない。何故なら、走査チェーン素子内のデータの修正のためのタイミングが決定性であり、ステップ２３０が、ラッチ１８２～１８４をリセットすることをできるようにするには十分な、多数のクロック・サイクルを単に待機するだけで行われるからである。

【００２４】

ステップ２３０において感知可能データが修正されると、走査コントローラ１２０は、ステップ２４０において走査チェーン１８０へのアクセスを許可する。ステップ２４０中に、当業者にとって周知の通常の走査試験手順を、走査チェーン１８０の走査観察可能素子の中の任意の素子内にすでに記憶されていた感知可能情報のセキュリティを犠牲にしないで使用することができる。データをスキャンイン・ポート１８１内まで走査することが

でき、プロセッサ１００の種々の内部の部分の機能を試験するために、スキャンアウト・ポート１８９から読出すことができる。

【００２５】

走査試験が終了すると、図２の方法はステップ２４０からステップ２５０に進む。ステップ２５０において、走査試験モードから抜け出し、通常モードに再度入るための準備が行われる。一実施形態の場合には、ステップ２５０中は、走査チェーン１８０へのアクセスが阻止され、ラッチ１８２、１８４および状態機械１５０内の任意のデータが修正またはリセットされる。走査チェーン１８０は、ＴＥＳＴ　ＭＯＤＥ信号のアサートを解除することにより、通常モードに入ることを走査コントローラ１２０（図１）に通知することにより阻止することができる。ＴＥＳＴ　ＭＯＤＥ信号のアサートを解除するとそれに応じて、ラッチ１８２、１８４および状態機械１５０（図１）、および感知可能情報の読出しまたは書込みを含むことができる走査チェーン１８０の任意の他の素子をリセットするためにＳＣＡＮ　ＲＥＳＥＴ信号をアサートすることができる。さらに、走査チェーンの観察可能部分上の素子を、データが走査により読み出されるのを防止するために再構成することができる。通常動作の目的で走査チェーンを準備するために使用した信号については、図７のところでさらに詳細に説明する。

【００２６】

非試験状態に抜け出る前にプロセッサ１００の走査観察可能な部分から情報をクリアすることにより、何者かが走査試験中に「シード」情報を走査するのを防止し、次に、シード情報に対してどんな動作が行われたのかを判断するために、プロセッサ１００の出力を監視するのが防止される。また、この時点で情報をクリアすれば、何者かが、事実はそうでなくても、例えば、プロセッサに機密保護モードで動作していると「信じ込ませる」ことができる特定の状態に、例えば、状態機械１５０のような状態機械を設定するのが防止される。少なくとも１つの実施形態の場合には、ステップ２５０中に生成したＳＣＡＮ　ＥＸＩＴ信号を、すでに説明したように、データの修正／リセットの代わりにまたはこれに加えて、現在の状態が正確でないのかもしれないことを示すために、種々の状態機械への入力として使用することができる。状態機械は、次に、状態ビットが走査出口でクリアされてなくても、それ自身の上の既知の状態に遷移することができる。

【００２７】

ステップ２６０において、走査コントローラ１２０は、ステップ２３０のところで説明したのと同じかまたは類似の技術により、プロセッサ１００の任意の必要な走査観察可能な部分からデータがクリアされていることを確認するためにチェックを行う。例えば、一実施形態の場合には、走査コントローラ１２０は、データが走査チェーン１８０内にまたはからシフトするのを許可し、または防止するために使用することができるＳＣＡＮ　ＤＡＴＡ　ＥＮＡＢＬＥ信号がアサートされる前に、リセットが終了したことを示すために、ＥＶＥＮＴ　ＴＲＩＧＧＥＲ信号のアサートを待機することができる。図５のところでさらに詳細に説明する他の実施形態の場合には、ＵＮＳＥＣＵＲＥ＊信号のアサートの解除を、ＥＶＥＮＴ　ＴＲＩＧＧＥＲ信号がアサートされた場合に記述することができる。

【００２８】

図５のところで説明するＵＮＳＥＣＵＲＥ＊信号は、通常動作のための走査チェーン１８０上の種々の素子の構成を禁止または許可するために、走査チェーン１８０上の１つまたはそれ以上の素子を制御するために使用される。例えば、ＵＮＳＥＣＵＲＥ＊は、データが出力されるのを防止するために、図１のＳＣＡＮ　ＤＡＴＡ　ＥＮＡＢＬＥ信号のような制御信号の代わりに使用することができる。別の方法としては、ＵＮＳＥＣＵＲＥ＊を、例えば、ＳＣＡＮ　ＤＡＴＡ　ＥＮＡＢＬＥまたはＳＣＡＮ　ＥＮＡＢＬＥ（ＩＮＴＥＲＮＡＬ）のような１つまたはそれ以上の信号を生成するために使用する論理回路への１つの入力として使用することができる。少なくとも１つの実施形態の場合には、ＵＮＳＥＣＵＲＥ＊信号（図５）は、ＳＣＡＮ　ＲＥＳＥＴおよびＳＣＡＮ　ＥＸＩＴ信号（図３～図４）両方の機能を結合する。データおよび／または状態情報がクリアされると、走査コントローラ１２０または他の適当なハードウェア、ソフトウェアまたはファームウェ

ア素子は、プロセッサ１００を通常モードに戻すことができる。

【００２９】

図２の方法の種々のステップは、本発明の教示から逸脱することなしに、同時にまたは異なる順序で実施することができることを理解することができるだろう。例えば、ステップ２３０の場合のように、感知可能データが、走査観察可能素子からクリアされたかどうかを確認するためのチェックは、ステップ２３０の後でも実行することができるし、通常モード２１０でも実行することができる。別の方法としては、感知可能データがクリアされたかどうかのチェックは、継続的に行うこともできる。また、種々の設計、マーケティング、コスト、セキュリティまたは他の要因により、図２の方法のある部分を、他の部分を除いて実施することもできる。例えば、ステップ２２０の場合のように、試験モードに入る時に、いくつかのラッチ内のデータだけをクリアすることもできるし、ステップ２５０および２６０を、通常モードへ抜け出す前に、機密保護状態機械から状態情報をクリアするためだけに使用することができる。

【００３０】

図３を参照しながら、走査コントローラ１２０の一部の特定の実施形態について説明する。この図の実施形態の場合には、走査コントローラ１２０の一部は、３つの入力、すなわち、ＴＥＳＴ　ＭＯＤＥ、ＲＥＳＥＴおよびＳＣＡＮ　ＥＮＡＢＬＥを有する。これら３つの入力は、３つの出力、すなわち、ＳＣＡＮ　ＥＮＡＢＬＥ（ＩＮＴＥＲＮＡＬ）、ＳＣＡＮ　ＲＥＳＥＴおよびＳＣＡＮ　ＥＸＩＴを生成するために組合わせて使用される。ＴＥＳＴ　ＭＯＤＥは、もっと簡単に試験できるように回路を機能的に修正するために使用する信号である。この信号は走査試験がスタートする前にアサートされる。ＳＣＡＮ　ＥＮＡＢＬＥは、データを走査チェーン内にシフトするために使用する信号であり、ＲＥＳＥＴは、内部データをクリアし、既知の状態に設定し、および／または他の方法で修正すべきであることを示す信号である。ＳＣＡＮ　ＥＮＡＢＬＥ（ＩＮＴＥＲＮＡＬ）は、走査チェーンを通してデータをシフトするために、ＳＣＡＮ　ＥＮＡＢＬＥの代わりに、内部回路が使用するＳＣＡＮ　ＥＮＡＢＬＥをゲート制御したものである。ＳＣＡＮ　ＲＥＳＥＴは、アサートされた場合、走査チェーンの走査観察可能素子から感知可能データをクリアするために使用することができる。ＳＣＡＮ　ＥＸＩＴは、アサートされた場合、ＴＥＳＴ　ＭＯＤＥ信号が示すように、試験モードのアサートがすでに解除されていて、既知の状態に強制的に状態遷移するために、状態機械への入力として使用することができることを示す信号である。

【００３１】

走査コントローラ１２０の一部は、感知可能回路内の情報がクリアされるまで、データを決して走査チェーン内にシフトすることができないようにする。例えば、制御中の回路が試験モードであることを示すＴＥＳＴ　ＭＯＤＥ信号がアサートされるまで、データは走査チェーン内にシフトすることはできない。さらに、走査コントローラ１２０の一部は、ＴＥＳＴ　ＭＯＤＥ信号がアサートされてから２つのクロック・サイクルまで、情報が走査チェーン内にシフトするのを遅延する。これにより、確実に、走査コントローラ１２０は、ＴＥＳＴ　ＭＯＤＥ信号がアサートされた場合に自動的に生成されるＳＣＡＮ　ＲＥＳＥＴパルスを生成するための時間を有する。試験モードから抜け出した場合には、ＴＥＳＴ　ＭＯＤＥ信号のアサートの解除が示すように、ＳＣＡＮ　ＥＸＩＴ信号がアサートされる。信号のタイミングについては、図６および図７のところでさらに詳細に説明する。

【００３２】

図４について説明すると、この図は走査コントローラ１２０の一部のもう１つの実施形態である。図の実施形態のロジックは、ＳＣＡＮ　ＥＮＡＢＬＥ（ＩＮＴＥＲＮＡＬ）のアサートが、この場合、ＥＶＥＮＴ　ＴＲＩＧＧＥＲ信号のアサートの際に記述される点を除けば、図３のところで説明したロジックと本質的に同じものである。図３の走査コントローラは、必要な場合には、図４の走査コントローラが供給する機能を含むように修正することができることを理解することができるだろう。ＥＶＥＮＴ　ＴＲＩＧＧＥＲ信号

は、図１のところで説明したように、制御下の回路内の情報が必ず修正、リセット、クリア等されているようにするために、また走査チェーンのすべての素子または特定の素子がクリアされ、設定され、または他の方法で試験モードに入る準備ができているようにするための追加制御として使用される。ＥＶＥＮＴ　ＴＲＩＧＧＥＲ信号を受信した場合だけ、出力信号、ＳＣＡＮ　ＥＮＡＢＬＥ（ＩＮＴＥＲＮＡＬ）が生成される。ＳＣＡＮ　ＥＮＡＢＬＥ（ＩＮＴＥＲＮＡＬ）信号は、データが走査チェーン内にまたはからシフトするのを防止する目的で、入力または出力ゲート、フリップフロップ等の制御を含んでいて、図３のところで説明したように使用することができる。

【００３３】

図５を参照しながら、非同期フリップフロップを使用する走査コントローラ１２０の一部からなるある実施形態について考察する。図５の実施形態は、図３および図４の実施形態と本質的に同じ効果を達成するために動作するが、若干異なるロジック構成を使用する。さらに、図５は、修正した走査コントローラまたは図１の他の回路の一部とすることができるゲート５１０および５２０を含むロジックも示す。

【００３４】

図５について説明すると、ＴＥＳＴ　ＭＯＤＥ信号は、ＴＥＳＴ　ＭＯＤＥ信号の立上がり縁部が、フリップフロップ５４０の出力を高レベルにし、ＴＥＳＴ　ＭＯＤＥ信号の立下がり縁部がフリップフロップ５５０の出力を高レベルにするように、フリップフロップ５４０のクロック入力およびフリップフロップ５５０の倒置クロック入力に送られる。

【００３５】

それ故、ＴＥＳＴ　ＭＯＤＥの任意の遷移は、フロップへのＲＥＳＥＴ入力のアサートが解除されると仮定した場合、ＵＮＳＥＣＵＲＥ＊をアサートさせる。ＵＮＳＥＣＵＲＥ＊がアサートされると、ＳＣＡＮ　ＥＮＡＢＬＥ　ＩＮＴＥＲＮＡＬのアサートが解除され、走査チェーンの動作を防止する。非同期状態にあるフリップフロップ５４０および５５０のリセット入力は、フリップフロップ５６０の倒置出力に接続され、そのためフリップフロップ５４０および５５０は、ＳＥＣＵＲＥ　ＲＥＳＥＴ信号に応じてリセットされる。ＳＥＣＵＲＥ　ＲＥＳＥＴは、ユーザの動作に応じて、または他の方法で、システム・リセットの一部として生成することができる。少なくとも１つの実施形態の場合には、ＳＥＣＵＲＥ　ＲＥＳＥＴは、図１のＲＥＳＥＴ信号の特別な例である。フリップフロップ５４０および５５０の信号入力は、高い基準電圧に接続しているので、ＳＥＣＵＲＥ　ＲＥＳＥＴ信号が少なくとも２つのクロック・サイクルの間アサートされると、アクティブ・ローの論理信号、ＵＮＳＥＣＵＲＥ＊のアサートが解除され（すなわち、論理ハイ値になり）、感知可能データが機密保護されていることを示す。

【００３６】

図の実施形態の場合には、ＳＥＣＵＲＥ　ＲＥＳＥＴ信号がアサートされる前に、ＴＥＳＴ　ＭＯＤＥがアサートされると、アサートされたＳＥＣＵＲＥ　ＲＥＳＥＴ信号を受信した後で、ＵＮＳＥＣＵＲＥ＊信号のアサートが解除され、感知可能データが機密保護されていることを示し、ＳＥＣＵＲＥ　ＲＥＳＥＴ信号のアサートが解除された後でも、ＵＮＳＥＣＵＲＥ＊はアサートされないままになる。しかし、ＴＥＳＴ　ＭＯＤＥ信号が、ＳＥＣＵＲＥ　ＲＥＳＥＴ信号のアサートが解除された後で状態を変えると、ＵＮＳＥＣＵＲＥ＊信号がアサートされ、走査チェーン内のデータは機密保護されないことを示す。ＵＮＳＥＣＵＲＥ＊信号の機能の理解を容易にするために、以下の節においてその例について考察する。

【００３７】

下記の例について考察する場合、ＳＣＡＮ　ＩＮ（ＩＮＴＥＲＮＡＬ）５０７、ＳＣＡＮ　ＯＵＴ（ＩＮＴＥＲＮＡＬ）５１７、およびＳＣＡＮ　ＥＮＡＢＬＥ（ＩＮＴＥＲＮＡＬ）は、ＳＣＡＮ　ＩＮ１８１、ＳＣＡＮ　ＯＵＴ１８９およびＳＣＡＮ　ＥＮＡＢＬＥ（図１）をゲート制御したものであり、これらすべては走査チェーン１８０の外部アクセスを制限するために使用することができることに留意されたい。ＳＣＡＮ　ＩＮ（ＩＮＴＥＲＮＡＬ）およびＳＣＡＮ　ＯＵＴ（ＩＮＴＥＲＮＡＬ）は、図１にははっきりと示

してないが、実施した場合、図１のＳＣＡＮ　ＩＮおよびＳＣＡＮ　ＯＵＴ信号をゲート制御することに留意されたい。例えば、走査チェーン１８０（図１）のモードが、現在走査試験モードになっていて、ＴＥＳＴ　ＭＯＤＥ信号はアサートされ、ＵＮＳＥＣＵＲＥ＊信号はアサート解除されていると仮定しよう。走査試験モードから抜け出すために、ＴＥＳＴ　ＭＯＤＥ信号のアサートが解除される。フリップフロップ５５０は、ＴＥＳＴ　ＭＯＤＥ信号の立下がり縁部によりトリガされ、それによりＵＮＳＥＣＵＲＥ＊がアサートされる。アサートされたＵＮＳＥＣＵＲＥ＊信号は、走査試験モードから抜け出していることを示し、また走査チェーン１８０（図１）内のデータをクリアする必要があることを示す。図の実施形態の場合には、ＵＮＳＥＣＵＲＥ＊は、データＳＣＡＮ　ＩＮ５８１が、ＡＮＤゲート５１０を通過し、走査チェーン１８０（図１）内に走査することができるＳＣＡＮ　ＩＮ（ＩＮＴＥＲＮＡＬ）データ５０７になるのを阻止するための、またデータＳＣＡＮ　ＯＵＴ（ＩＮＴＥＲＮＡＬ）５１７が走査チェーン１８０（図１）から読み出されるのを阻止するための論理ゲート５１０への入力として使用される。さらに、ＵＮＳＥＣＵＲＥ＊は、ＳＣＡＮ　ＥＮＡＢＬＥ（ＩＮＴＥＲＮＡＬ）が、データが機密保護されていない場合、ＳＣＡＮ　ＥＮＡＢＬＥに応じてアサートされるのを阻止するための論理ゲート５１２への入力として使用される。これらの方法の中の任意のものを、データがデバイス１００から走査されるのを防止するために使用することができることを理解することができるだろう。

【００３８】

論理ゲート５１０、５１２および５２０への入力として使用されるほかに、ＵＮＳＥＣＵＲＥ＊信号は、例えば、ＳＥＣＵＲＥ　ＲＥＳＥＴ信号をアサートするために、または他の方法で走査チェーン内のデータをクリアする目的で、中央プロセッサに通知するために使用することができる。ＵＮＳＥＣＵＲＥ＊信号は、また、種々のファームウェアまたはソフトウェアが走査チェーンの状態を判断するために参照することができる機密保護／非機密保護レジスタ（図示せず）を設定するためにも使用することができる。別の方法としては、ＵＮＳＥＣＵＲＥ＊信号を、図１の１つまたはそれ以上のラッチまたは状態機械の構成を制御するための直接入力として使用することができる。

【００３９】

最後に、図５の実施形態は、走査チェーンの走査観察可能素子内に記憶されているデータを修正する目的で、アサートされたＣＬＥＡＲ／ＲＥＳＥＴ信号を生成するために、ＳＥＣＵＲＥ　ＲＥＳＥＴ信号を使用する。ＣＬＥＡＲ／ＲＥＳＥＴは、図１のＳＣＡＮ　ＲＥＳＥＴに類似しているものでもよいことに留意されたい。ＳＥＣＵＲＥ　ＲＥＳＥＴ信号は、走査コントローラ１２０を使用するプロセッサ内の他の回路により自動的に生成することができるか、またはシステムを、オペレータがリセットを物理的にスタートした後でだけ、ＳＥＣＵＲＥ　ＲＥＳＥＴ信号を生成するように構成することができる。

【００４０】

図３および図６を参照しながら、走査コントローラの一実施形態で使用する信号間のタイミングの関係について説明する。図６は、試験モードに入った場合のタイミングの関係である。以下の説明のすべてのタイミングは、クロック６１０を基準にしていて、特にクロック・サイクルＣ１の第１の立上がり縁部を基準にしている。クロック・サイクルＣ１がスタートする前に、すべての信号のアサートが解除され、動作モードが通常モード、すなわち、非試験モードであることを示す。クロック・サイクルＣ１の前の半分の間に、ユーザはＳＣＡＮ　ＥＮＡＢＬＥ６３０をアサートすることにより走査ができるようにしようとする。走査コントローラ１２０を使用しているプロセッサは、依然として通常モードで動作しているので、ＳＣＡＮ　ＥＮＡＢＬＥ６３０をアサートしても、ＳＣＡＮ　ＥＮＡＢＬＥ（ＩＮＴＥＲＮＡＬ）６４０は高レベルにならない。

【００４１】

しかし、第２のクロック・サイクルＣ２の第１の立上がり縁部のところで、ＴＥＳＴ　ＭＯＤＥ６２０がアサートされる。ＳＣＡＮ　ＲＥＳＥＴ６６０は、ＴＥＳＴ　ＭＯＤＥ６２０がアサートされると高レベルになる。ＳＣＡＮ　ＲＥＳＥＴ６６０は、走査チェー

ン上の走査観察可能素子の修正、リセットまたはクリアをトリガするパルスである（図１参照）。クロック・サイクルＣ４の第１の立上がり縁部のところで、ＴＥＳＴ　ＭＯＤＥ６２０の後の２つの立ち上がりクロック縁部がアサートされ、ＳＣＡＮ　ＥＮＡＢＬＥ６３０およびＴＥＳＴ　ＭＯＤＥ６２０の両方が高レベルになっているので、ＳＣＡＮ　ＥＮＡＢＬＥ（ＩＮＴＥＲＮＡＬ）６４０が高レベルになる。２つのクロック・サイクル中、ＳＣＡＮ　ＥＮＡＢＬＥ（ＩＮＴＥＲＮＡＬ）６４０のアサートを遅らせることにより、走査チェーンへのアクセスが許可される前にリセットを行うことができる。それにより、試験モードになった場合、感知可能情報を保護する。ＲＥＳＥＴ６５０およびＳＣＡＮ　ＥＸＩＴ６７０は、試験モード中にはアサートされないことに留意されたい。サイクルＣ４のところでＳＣＡＮ　ＥＮＡＢＬＥ（ＩＮＴＥＲＮＡＬ）がアサートされてから後しばらく経過した後で、サイクルＣ１のところでアサートされているＴＥＳＴ　ＭＯＤＥ６２０に応じて、内部プロセッサの構成要素の試験を容易にするために、走査チェーン内におよびからデータをシフトすることができるが、この時点ですべての機密保護情報はクリアされる。

【００４２】

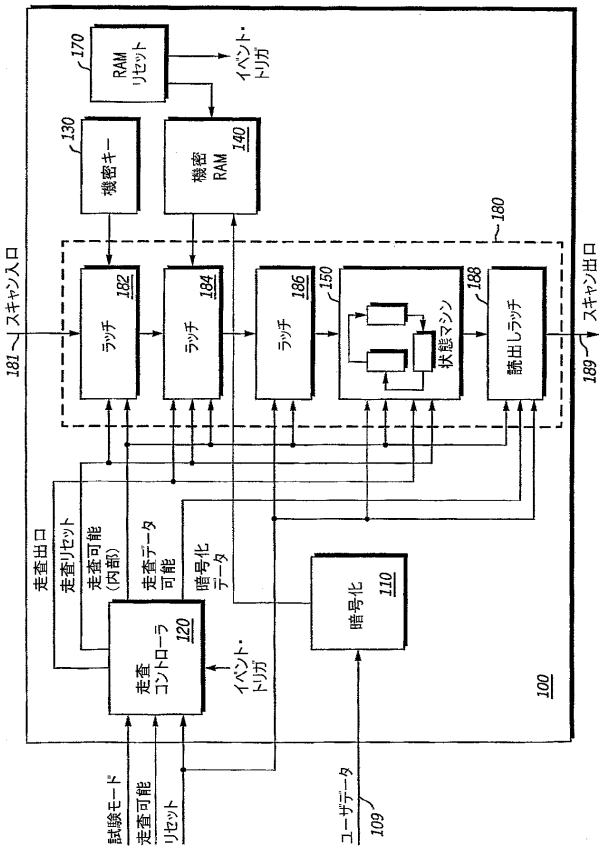
図３および図７を参照しながら、走査コントローラの一実施形態の信号間のタイミングの関係、特に試験モードから抜け出した場合のタイミングの関係についてさらに詳細に説明する。図７の信号のタイミングの関係について、クロック・サイクルＣ１の第１の立上がり縁部を参照しながら説明する。クロック・サイクルＣ１のスタートのところで、ＴＥＳＴ　ＭＯＤＥ７２０、ＳＣＡＮ　ＥＮＡＢＬＥ７３０およびＳＣＡＮ　ＥＮＡＢＬＥ（ＩＮＴＥＲＮＡＬ）７４０がアサートされ、一方、すべての他の信号が取り消される。このことは、感知可能データの漏洩を心配しないで、走査チェーン内におよびからデータを自由にシフトすることができる試験モードに対応する。クロック・サイクルＣ１の立下がり縁部のところで、ＴＥＳＴ　ＭＯＤＥ７２０が取り消され、試験サイクルの終了および通常モードへの移行が通知される。ＴＥＳＴ　ＭＯＤＥ７２０が取り消されるのと同時に、最後にＲＥＳＥＴ７５０がアサートされて以来試験モードに入っていて、そのモードから抜け出したことを通知するためにＳＣＡＮ　ＥＸＩＴ７７０がアサートされる。ＳＣＡＮ　ＥＸＩＴ７７０は、既知の状態に強制的に状態遷移するための状態機械への入力として使用することができ、ラッチの動作状態を制御するためのラッチへの入力として使用することができ、走査チェーン内のデータを通常動作で使用することができる前にリセットする必要があることを表示するためにプロセッサに結合することができ、または走査試験モードから抜け出したことを表示するために種々の他の類似の方法で使用することができる。

【００４３】

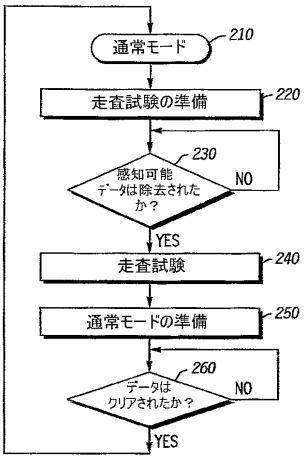
第２のクロック・サイクルＣ２の立下がり縁部のところで、ＲＥＳＥＴ７５０がアサートされ、それによりＳＣＡＮ　ＲＥＳＥＴ７６０がアサートされる。ＳＣＡＮ　ＲＥＳＥＴ７６０は、少なくとも１つの実施形態の場合には、走査チェーンを形成しているデータ・ラッチおよび状態機械へのリセット入力として使用される。このように使用された場合には、ＳＣＡＮ　ＲＥＳＥＴ７６０は、走査試験モードから抜け出した場合に、走査チェーンから感知可能データをクリアする。ＳＣＡＮ　ＥＮＡＢＬＥ（ＩＮＴＥＲＮＡＬ）７４０は、ＳＣＡＮ　ＥＸＩＴ７７０が取り消されるのと同時に低レベルになり、それにより、走査試験モードから抜け出した後で、走査チェーンからデータが走査されるのを防止する。最後に、ＳＣＡＮ　ＥＮＡＢＬＥ７３０のアサートが解除され、そのため追加のデータを走査チェーン内に走査することができない。現在タイミングを考察している走査コントローラ１２０の実施形態の場合には、ＳＣＡＮ　ＲＥＳＥＴ７６０は、ＴＥＳＴ　ＭＯＤＥ７２０が取り消された場合、自動的にはアサートされないことに留意されたい。その代わりに、ＲＥＳＥＴ７５０を、ユーザの動作または他の方法に応じてアサートしなければならないし、それにより、通常モードに入る前に走査チェーンをクリアするためにＳＣＡＮ　ＲＥＳＥＴ７６０がアサートされる。他の実施形態は、試験モードから抜け出した場合に、ＲＥＳＥＴ７５０に類似のリセット・パルスを自動的に生成することができる

。
【００４４】
要するに、上記説明をよく読めば、走査チェーンへのアクセスの許可の前および後で、プロセッサの走査観察可能部分内に記憶している情報を修正することにより、本明細書の教示により組立てた走査コントローラを使用するプロセッサは、試験性能を犠牲にしないでデータのセキュリティを強化することができることは明らかである。データのセキュリティが強化されると、自称模倣者がデータにアクセスするのを制限することにより感知可能データを簡単に利用できないようにすることができる。同時に、試験性能の向上により、製造コストを安くし、市場への製品の導入をスピードアップすることができる。
【００４５】
図面の上記詳細な説明において、本明細書の一部を構成していて、本発明を実行することができる例示としての特定の実施形態を示す添付の図面を参照した。これらの実施形態については、当業者が本発明を実行できるようにするために十分詳細に説明してあるが、他の実施形態も使用できること、また本発明の精神および範囲から逸脱することなしに、論理的、機械的、化学的、および電気的変更を行うことができることを理解されたい。
【００４６】
当業者が本発明を実行できるようにするために必要ではない詳細な説明を避けるために、当業者であれば周知のいくつかの情報を省略することができる。さらに、当業者であれば、本発明の教示を含む多くの他の変形した実施形態を容易に組立てることができるだろう。それ故、本発明の説明は、本明細書に記載した特定の形状に限定されるものではなく、それどころかこのような代替物、変形したものおよび等価物を、当然本発明の精神および範囲内に含まれるものとしてカバーする。それ故、上記の詳細な説明は、本発明を制限するものではなく、本発明の開示の範囲は添付の特許請求の範囲によってだけ定義される。
【図面の簡単な説明】
【００４７】
【図１】本発明のある実施形態による走査コントローラを使用するプロセッサのブロック図。
【図２】本発明のある実施形態によるプロセッサの走査観察可能部分にアクセスできるようになる前に、感知可能データをクリアすることを含む走査試験方法を示すフローチャート。
【図３】本発明の種々の実施形態による走査チェーンへのアクセスを制御するための走査コントローラを示す論理図。
【図４】本発明の種々の実施形態による走査チェーンへのアクセスを制御するための走査コントローラを示す論理図。
【図５】本発明の種々の実施形態による走査チェーンへのアクセスを制御するための走査コントローラを示す論理図。
【図６】試験モードへ入る行動に関連する、図３に示す論理図のタイミングを示す例示としてのタイミング図。
【図７】試験モードから抜け出す行動に関連する、図３の論理図のタイミングを示す例示としてのタイミング図。

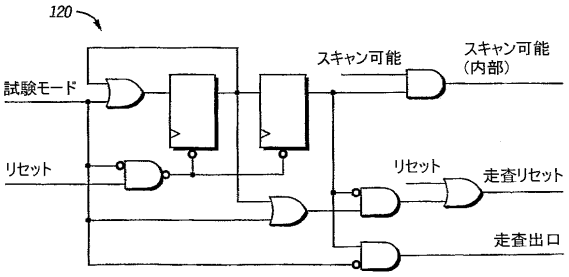
【図１】


RAM リセット
170
イベント・トリガ
機密キー
130
機密 RAM
140
180
スキャン入口
181
ラッチ
182
ラッチ
184
ラッチ
186
150
状態マシン
188
読出しラッチ
スキャン出口
189
走査出口
走査リセット
走査可能（内部）
走査データ可能
暗号化データ
暗号化
110
走査コントローラ
120
イベント・トリガ
100
試験モード
走査可能
リセット
ユーザデータ
109

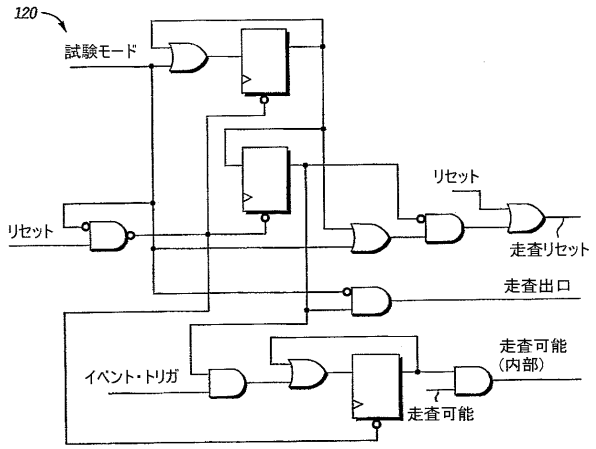
【図２】


通常モード
210
走査試験の準備
220
感知可能データは除去されたか？
230
NO
YES
走査試験
240
通常モードの準備
250
データはクリアされたか？
260
NO
YES

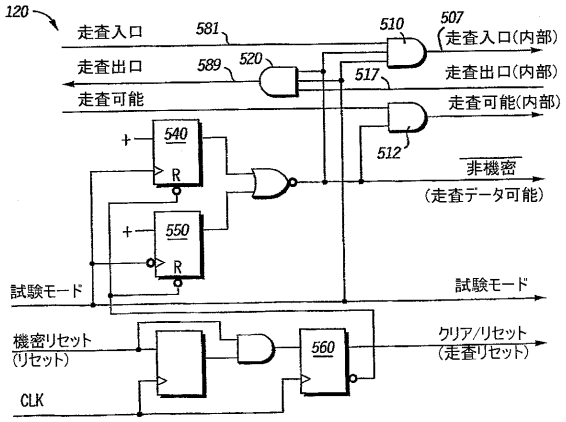
【図３】


120
試験モード
スキャン可能
スキャン可能（内部）
リセット
リセット
走査リセット
走査出口

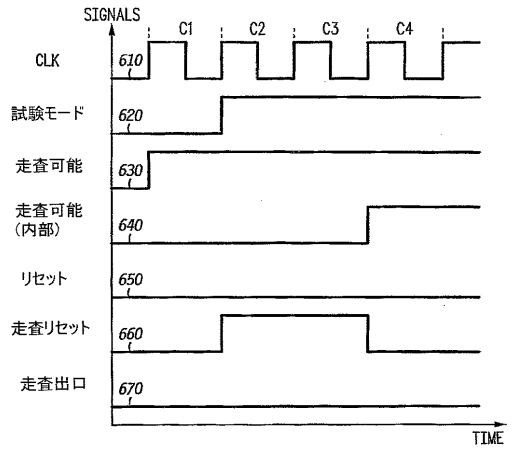
【図４】


120
試験モード
リセット
リセット
走査リセット
走査出口
イベント・トリガ
走査可能（内部）
走査可能

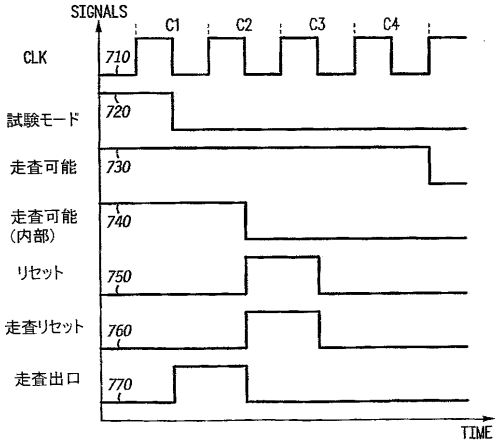
【図５】


120
走査入口
581
510
507
走査入口（内部）
走査出口
589
520
517
走査出口（内部）
走査可能
走査可能（内部）
512
540
非機密
（走査データ可能）
550
試験モード
試験モード
機密リセット（リセット）
560
クリア/リセット（走査リセット）
CLK

【図６】


SIGNALS
C1
C2
C3
C4
CLK
610
試験モード
620
走査可能
630
走査可能
(内部)
640
リセット
650
走査リセット
660
走査出口
670
TIME

【図７】


SIGNALS
C1
C2
C3
C4
CLK
710
試験モード
720
走査可能
730
走査可能
(内部)
740
リセット
750
走査リセット
760
走査出口
770
TIME

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Inter pplication No
PCT/US 03/11399

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G01R31/3185 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G01R G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, IBM-TDB, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 898 776 A (CHAN ANDREW K ET AL) 27 April 1999 (1999-04-27) abstract; figures 3,5 column 5, line 35 -column 7, line 51 column 1, line 12 -column 2, line 41	1-10
A	US 5 530 749 A (ZAJAC MYRON W ET AL) 25 June 1996 (1996-06-25) abstract; figure 3 column 2, line 11 - line 38	1-10

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 August 2003	01/09/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Böhm-Pélissier, A

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interr plication No
PCT/US 03/11399

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5898776 A	27-04-1999	NONE	
US 5530749 A	25-06-1996	US 5530753 A	25-06-1996

Form PCT/ISA/210 (patent family annex) (July 1992)

フロントページの続き

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IT,LU,MC,NL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NI,NO,NZ,OM,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,TJ,TM,TN,TR,TT,TZ,UA,UG,UZ,VC,VN,YU,ZA,ZM,ZW

(72)発明者 スピッタル、ジョン イー．ジュニア
アメリカ合衆国 ８５３５５ アリゾナ州 ウォデル エヌ．ワンハンドレッドセブンティセブンス アベニュー ７６０１
(72)発明者 ラッツ、ジョナサン
カナダ国 Ｎ２Ｍ ５Ｅ７ オンタリオ州 キッチナー ベルモント アベニュー ５６５ ナンバー２４
(72)発明者 ケース、ローレンス
アメリカ合衆国 ８５２６８ アリゾナ州 ファウンテン ヒルズ ノース スカイリッジ レーン １６４３３
(72)発明者 ハーディ、ダグラス
アメリカ合衆国 ８５２５９ アリゾナ州 スコッツデール イー．ローレル レーン １０７０５
(72)発明者 レッドマン、マーク
アメリカ合衆国 ８５２９６ アリゾナ州 ギルバート イー．アベニダ シエラ マドレ ７３４
(72)発明者 シュミット、グレゴリー
アメリカ合衆国 ８５２２６ アリゾナ州 チャンドラー ダブリュ．シカゴ ストリート ５３５０
(72)発明者 トゥーゲンバーグ、スティーブン
アメリカ合衆国 ８５２５８ アリゾナ州 スコッツデール エヌ．セブンティセブンス ストリート １０２１０
(72)発明者 フィッツシモンズ、マイケル ディ．
アメリカ合衆国 ７８７３１ テキサス州 オースティン エヌ．キャピタル オブ テキサス ハイウェイ ７７００ ナンバー７２３
(72)発明者 カーダー、ダレル エル．
アメリカ合衆国 ７８６２０ テキサス州 ドリッピング スプリングス ロッキー クリーク ３０１

Ｆターム(参考) 2G132 AA03 AB01 AC14 AK14 AK15 AK23 AL11
5B048 AA11 CC18 FF01
5B076 FA00 FA05 FC08 FD02 FD03