

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4388571号
(P4388571)

(45) 発行日 平成21年12月24日(2009.12.24)

(24) 登録日 平成21年10月9日(2009.10.9)

(51) Int.Cl. F I
H03K 5/19 (2006.01) H03K 5/19 T
G06F 1/04 (2006.01) G06F 1/04 302Z

請求項の数 3 (全 10 頁)

(21) 出願番号	特願2007-283196 (P2007-283196)	(73) 特許権者	308033711
(22) 出願日	平成19年10月31日(2007.10.31)		OKIセミコンダクタ株式会社
(65) 公開番号	特開2009-111824 (P2009-111824A)		東京都八王子市東浅川町550番地1
(43) 公開日	平成21年5月21日(2009.5.21)	(74) 代理人	100079119
審査請求日	平成21年3月16日(2009.3.16)		弁理士 藤村 元彦
		(74) 代理人	100109036
			弁理士 永岡 重幸
		(74) 代理人	100147728
			弁理士 高野 信司
		(72) 発明者	山田 健太
			東京都港区虎ノ門1丁目7番12号 沖電
			気工業株式会社内
		審査官	石田 勝

最終頁に続く

(54) 【発明の名称】 高速クロック検知回路

(57) 【特許請求の範囲】

【請求項1】

クロック信号に従って動作する機能回路から前記クロック信号を取り込んで、その異常高速状態を検知する高速クロック検知回路であって、

前記異常高速状態に対応するクロック周期以上の遅延時間が設定された遅延回路と、
 前記クロック信号に従ってディレイフリップフロップ動作し、自身の出力信号が反転帰還入力される第1フリップフロップ回路と、

前記クロック信号に従ってディレイフリップフロップ動作し、自身の出力信号が前記遅延回路を介して反転帰還入力される第2フリップフロップ回路と、

前記第1フリップフロップ回路の出力信号と前記第2フリップフロップ回路の出力信号との差分を検知し、前記差分の発生に応じて前記異常高速状態を表す高速クロック検知信号を前記機能回路に供給する検出結果出力回路と、

を含むことを特徴とする高速クロック検知回路。

【請求項2】

前記検出結果出力回路は、前記差分の発生をカウントし、そのカウント値が所定閾値に達した場合に前記高速クロック検知信号を出力することを特徴とする請求項1記載の高速クロック検知回路。

【請求項3】

前記検出結果出力回路は、前記所定閾値が設定されるカウント閾値設定レジスタを含み、前記カウント閾値設定レジスタの内容を前記機能回路から変更自在とする手段をさらに

10

20

含むことを特徴とする請求項 2 記載の高速クロック検知回路。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、クロック周波数に従って動作する L S I 等の回路装置に備えられ、クロック周波数が高速化する異常を検知する高速クロック検知回路に関する。

【背景技術】

【0002】

金融システムに使用される決済端末等の装置には高いセキュリティが要求される。かかる装置に使用される L S I は企業内部や外部からの攻撃によって、不正にデータを変えられたりデータを盗まれたりするハッキングの危険に晒されている。L S I に対する攻撃には様々の方法があるが、1つの方法としては、L S I の外部クロックを意図的に速くして当該 L S I に備えられる C P U を誤動作させる攻撃がある。そこで、このような攻撃に対して L S I が誤動作しないように、規定周波数以外のクロック周波数を検知するクロック検知回路が求められる。

【0003】

図 1 は、従来のクロック検知回路例の概要を示している。この例では、外部から攻撃され難くするためにリングオシレータによって基準クロックが生成されている。この基準クロックでカウント動作をするカウンタ A と C P U クロックでカウント動作をするカウンタ B でそれぞれカウントアップが行われ、カウンタのオーバーフロー信号やカウント値を用いて基準クロックとの比率が監視され、C P U クロックの周波数が高速クロックの高周波であるかどうかを検知される。

【0004】

しかしながら、図 1 に示される例では、高速クロックを検知する際にカウンタがオーバーフローを起こすまでの一定間隔で監視及び検知を行っていたため、一時的な高速クロック、例えば数パルス～数百パルス数の高速クロックによる攻撃を検知できなかった。

【0005】

特許文献 1 は、クロック信号の周期が制限値を超えたことを検出して誤動作を防止することのできる半導体試験装置を開示している。そこで、かかるクロック検知回路をハッキング防止のために L S I に組み込むことにより、一時的な高速クロックによる攻撃を検知することが考えられる。

【特許文献 1】特開平 7 - 1 5 1 8 3 9 号公報

【発明の開示】

【発明が解決しようとする課題】

【0006】

しかしながら、特許文献 1 に開示されている技術では、検知したいクロック信号の周期に制約が課せられるという問題がある。特許文献 1 に開示されている技術は、基準となる所定のパルス幅を有するとともにクロック信号のパルス幅だけ遅延した遅延信号の波形と、クロック信号の波形との論理積を直接とることにより検出信号を発生する構成であり、クロック信号のパルス幅を固定的なものとして扱っている。すなわち、クロック信号の周期が変動すると共にパルス幅が変動するような場合、例えばデューティ比が固定であってクロックの高速化につれてパルス幅が小さくなるような場合が想定されていない。例えば、パルス幅が 1 5 n s e c に設定されると 1 5 n s e c 以下のパルス周期は全て異常と検知されてしまうことになる。

【0007】

本発明は以上の問題に鑑みて考案されたものであり、その目的は、任意の周期を閾値として高速クロック信号を検知することができる高速クロック検知回路を提供することである。

【課題を解決するための手段】

【0008】

10

20

30

40

50

本発明による高速クロック検知回路は、クロック信号に従って動作する機能回路から該クロック信号を取り込んで、その異常高速状態を検知する高速クロック検知回路であって、該異常高速状態に対応する周期以上の遅延時間が設定された遅延回路と、該クロック信号に従ってディレイフリップフロップ動作し、自身の出力信号が反転帰還入力される第1フリップフロップ回路と、該クロック信号に従ってディレイフリップフロップ動作し、自身の出力信号が該遅延回路を介して反転帰還入力される第2フリップフロップ回路と、該第1フリップフロップ回路の出力信号と該第2フリップフロップ回路の出力信号との差分を検知し、該差分の発生に応じて該異常高速状態を表す高速クロック検知信号を該機能回路に供給する検出結果出力回路と、を含むことを特徴とする。

【発明の効果】

10

【0009】

本発明による高速クロック検知回路によれば、パルス幅如何に関わらず、任意の周期を閾値として高速クロックを検知することができる。

【発明を実施するための最良の形態】

【0010】

本発明の実施例について添付の図面を参照しつつ詳細に説明する。

<第1の実施例>

図2は、本発明の第1の実施例を示し、高速クロック検知回路の構成を示している。高速クロック検知回路100は、大きく3つの回路部に分かれ、通常ループバック回路部20と、遅延ループバック回路部30と、検出結果出力回路部10とから構成される。

20

【0011】

通常ループバック回路部20は、D(ディレイ)型のフリップフロップ回路21と反転回路22とを含み、フリップフロップ回路21の出力信号(F/F-1値)を反転回路22により反転し、得られる反転信号を単純にループバックさせて通常ループバック信号としてフリップフロップ回路21へ帰還入力している。また、フリップフロップ回路21のクロック端子には外部から入力されるCPUクロック信号が供給される。

【0012】

遅延ループバック回路部30は、D型のフリップフロップ回路31と反転回路32と遅延回路33とを含み、フリップフロップ回路31の出力信号(F/F-2値)を反転回路32により反転し、得られる反転信号を遅延回路33により遅延させた上でループバックさせて遅延ループバック信号としてフリップフロップ回路31へ帰還入力している。また、フリップフロップ回路31のクロック端子には外部から入力されるCPUクロック信号が供給される。

30

【0013】

遅延回路33はバッファ等のディレイ素子により実現される。遅延回路33の遅延量 T_D はディレイ素子の構成如何により任意に設定可能であり、高速とみなされる異常動作周波数の閾値を与える。遅延量 T_D は、通常、CPUの最大動作周波数に相当する周期 T_C よりやや大きめの遅延量に設定される。例えば、CPUの最大動作周波数50MHzとすると、これに相当する周期 T_C は20nsである。そこで、最大動作周波数に対するマージンを確保して異常動作周波数を48MHzとすると、遅延回路33の遅延量 T_D は21nsの遅延量に設定される。もちろん、異常動作周波数を最大動作周波数と同じか、もしくは最大動作周波数より少し速い周波数まで許容する場合も考えられることから、遅延量 T_D は、最大動作周波数の周期 T_C よりも低く設定しても、同じに設定しても、高く設定しても良い。さらには、異常動作周波数がCPUの最大動作周波数とは直接関係のない任意の基準により決定されて遅延量 T_D が設定されてもよい。

40

【0014】

検出結果出力回路部10は、D型のフリップフロップ回路11と、排他的論理和回路12と、論理和回路13とを含む。排他的論理和回路12は、通常ループバック回路部20からの反転信号と、遅延ループバック回路30からの反転信号との排他的論理和(EX-OR値)を論理和回路13の一方に入力する。論理和回路13の出力信号はフリップフロ

50

ップ回路 11 に入力される。フリップフロップ回路 11 の出力信号は高速クロック検知信号として出力されると共に論理和回路 13 の他方に入力される。フリップフロップ回路 11 のクロック端子には、外部から入力される CPU クロック信号が供給されてもよいし、制御回路から供給される別の制御クロック信号であってもよい。

【 0015 】

図 3 は、本発明による高速クロック検知回路がコンピュータシステムに適用された場合の例を示している。ここで、コンピュータシステムは、所望の機能を奏する機能回路として、CPU 200 と、メモリ 500 と、機能モジュールや入出力モジュール等の周辺回路 600 と、制御回路 300 とから構成され、これら各部がバス 400 を介して相互に接続される。制御回路 300 は、例えば内部のリングオシレータクロックなどにより CPU クロック信号とは異なるクロックで動作し、外部入力クロックを基にして CPU クロック信号を生成し、CPU 200 に対して該 CPU クロック信号を供給すると共に電源 ON/OFF の制御を行う。高速クロック検知回路 100 は、該 CPU クロック信号を取り込むと共に、高速クロックの検知に応じて、高速クロック検知信号を制御回路 300 に供給する。CPU クロック信号は、外部入力されるクロックを基にして生成されるために、外部の不正動作または異常動作により正常な周波数範囲から逸脱して異常な高周波になる可能性がある。

【 0016 】

図 4 は、第 1 の実施例における高速クロック検知回路の動作タイミングを示している。本図を参照すると、CPU クロック信号と、通常ループバック信号と、通常ループバック回路における $F/F - 1$ 値と、遅延ループバック信号と、遅延ループバック回路における $F/F - 2$ 値と、排他的論理和回路における EX-OR 値と、高速クロック検知信号 ($F/F - 3$ 値) の各々が横軸を時間軸として示されている。この横軸において、CPU クロック信号の周期が T_C で示され、且つそのクロックタイミングが $t_1 \sim t_n$ (n は正数) で示されている。

【 0017 】

タイミング $t_1 \sim t_3$ の期間において、通常ループバック信号と $F/F - 1$ 値とは、CPU クロック信号のクロックに応じて、互いに交互に反転するパルス波形を呈する。例えば、タイミング t_2 において、遅延ループバック信号の値は “0” から “1” に変化するのに反して、 $F/F - 1$ 値は “1” から “0” に変化する。

【 0018 】

一方、遅延ループバック信号は、通常ループバック信号に比べて、遅延回路による遅延時間 T_D 分だけ遅れたパルス波形を呈する。しかし、遅延時間 T_D が CPU クロック信号の周期 T_C がよりも短い限り、遅延ループバック信号の立ち下がり、CPU クロック信号の次のクロックパルスの立ち上がりより前に発生する。例えば、タイミング t_2 において、遅延ループバック信号の値は既に “0” である。よって、タイミング t_2 におけるクロックパルスの立ち上がりに応じて、遅延ループバック回路におけるフリップフロップ回路の出力信号の $F/F - 2$ 値は “1” から “0” に変化する。

【 0019 】

この時点では、 $F/F - 1$ 値及び $F/F - 2$ 値が共に “0” であり、それらの反転信号の値は共に “1” となり差分が無いことから、排他的論理和回路の出力信号の EX-OR 値は “0” となる。タイミング t_3 において、CPU クロック信号のクロックパルスに応じて、EX-OR 値 “0” が検知結果出力回路部におけるフリップフロップ回路により保持されて、高速クロック検知信号 ($F/F - 3$ 値) “0” が出力される。これは CPU クロック信号が正常であることを表している。

【 0020 】

タイミング t_4 の冒頭において外部からの攻撃が発生し、CPU クロック信号の周期 T_C が以前よりも短くなり、遅延時間 T_D 未満になったとする。この場合、通常ループバック信号と $F/F - 1$ 値とは、周期が短くなった CPU クロック信号のクロックに応じて、以前と同様に互いに交互に反転するパルス波形を呈する。例えば、タイミング t_5 において

10

20

30

40

50

F / F - 1 値は “ 1 ” から “ 0 ” に変化する。

【 0 0 2 1 】

しかし、遅延ループバック信号について見ると、遅延時間 T_D が CPU クロック信号の周期 T_C よりも長いことから、遅延ループバック信号の立ち下がり、CPU クロック信号の次のクロックパルスの立ち上がりよりも後ろに遅れる。例えば、タイミング t_5 において、遅延ループバック信号の値は未だに “ 1 ” である。よって、タイミング t_5 におけるクロックパルスの立ち上がりに応じて、遅延ループバック回路におけるフリップフロップ回路の出力信号の F / F - 2 値は “ 1 ” のままである。

【 0 0 2 2 】

この時点で、F / F - 1 値が “ 0 ” であるのに反して F / F - 2 値は “ 1 ” であり、それらの反転信号の値は互いに異なり差分が発生したことから、排他的論理和回路の出力信号の EX - OR 値は “ 1 ” となる。タイミング t_6 において、CPU クロック信号のクロックパルスに応じて、EX - OR 値 “ 1 ” が検知結果出力回路部におけるフリップフロップ回路により保持されて、高速クロック検知信号 (F / F - 3 値) “ 1 ” が出力される。これは CPU クロック信号が異常であることを表している。

【 0 0 2 3 】

タイミング t_{11} 以降において、外部からの攻撃が止み、CPU クロック信号の周期 T_C が旧に復したとしても、その後は高速クロック検知信号 (F / F - 3 値) は “ 1 ” を出力する。異常を表す高速クロック検知信号に応じて、制御回路が CPU のクロックや電源を停止する等の処置を行うことができる。

【 0 0 2 4 】

以上の第 1 の実施例において、高速クロック検知回路 1 0 0 は、高速クロックが入力された場合、クロックをカウントすることなく即座に高速クロックが入力されたことを検知することができる。そのため、少パルスの高速クロックによる攻撃に対しても、これを検知することができる。また、リングオシレータやカウンタ回路を必要とせずに 3 つのフリップフロップ回路と数個の論理ゲートのみで構成しているため、LSI のチップ面積を大きくすることもなく且つ LSI のチップコストを下げるることができる。

【 0 0 2 5 】

高速クロックであると判定する閾値は、遅延回路における遅延量によって設定することができる。該遅延量は高速クロック周波数に対応する周期を与えればよく、当該高速クロックのパルス幅を特に顧慮する必要がない。また、該遅延量によって精確に正常と異常との境が判定されるために、検知誤差のためのマージンを過大に考慮する必要がない。

< 第 2 の実施例 >

図 5 は、本発明の第 2 の実施例を示し、高速クロック検知回路の構成を示している。高速クロック検知回路 1 0 0 は、通常ループバック回路部 2 0 と、遅延ループバック回路部 3 0 と、検知結果出力回路部 1 0 とから構成される。第 2 の実施例における通常ループバック回路部 2 0 及び遅延ループバック回路部 3 0 は、第 1 の実施例における同一の構成を備える。

【 0 0 2 6 】

第 2 の実施例では、検知結果出力回路部 1 0 の構成が第 1 の実施例の場合とは異なる。検知結果出力回路部 1 0 は、排他的論理和回路 1 2 と、複数のフリップフロップ回路により実現され得るカウンタ 1 4 とを含む。排他的論理和回路 1 2 は、通常ループバック回路部 2 0 からの反転信号と、遅延ループバック回路 3 0 からの反転信号との排他的論理和 (EX - OR 値) をカウンタ 1 4 に入力する。カウンタ 1 4 は、CPU クロック信号に同期して排他的論理和 (EX - OR 値) が “ 1 ” となる状態をカウントし、そのカウント値がカウント閾値を超えた時に初めて高速クロック検知信号を出力する。該カウント閾値は予め適切な値に調整される。これによりノイズ等による高速クロック誤検知が回避される。

【 0 0 2 7 】

図 6 は、第 2 の実施例における高速クロック検知回路の動作タイミングを示している。前提として上記したカウント閾値を 3 とする。タイミング $t_1 \sim t_5$ に至る動作は第 1 の

10

20

30

40

50

実施例と同様である。すなわち、タイミング t 5 以前においては、排他的論理和回路の EX - OR 値が “ 0 ” を維持していることから、カウンタ値は “ 0 ” のままである。

【 0 0 2 8 】

タイミング t 5 において、高速クロックを検知したことから排他的論理和回路の出力信号の EX - OR 値は “ 1 ” となる。そして、タイミング t 6 において、CPU クロック信号のクロックパルスに応じて、カウンタがこの EX - OR 値 “ 1 ” を取り込み、カウント値を 1 とする。次いで、タイミング t 7 において、カウンタは、引き続き維持されている EX - OR 値 “ 1 ” を取り込み、カウント値を 2 とする。

【 0 0 2 9 】

タイミング t 1 0 において、カウント値がカウント閾値 “ 3 ” に達したことから、高速クロック検知信号が “ 1 ” となり、以後カウンタによって保持される。

【 0 0 3 0 】

以上の第 2 の実施例において、ノイズを原因とする高速クロック誤検出が回避されている。第 1 の実施例では、外部入力クロックにノイズ等により瞬間的に高速クロックが入力された状態になってしまうと誤検知してしまう可能性があった。しかし、第 2 の実施例では、検知結果出力回路部で一定回数カウントアップした場合にのみ高速クロック検知信号を出力するため、外部入力クロックに瞬間的にノイズが乗った場合等においても、誤りのない高速クロック検知ができる。

< 第 3 の実施例 >

図 7 は、本発明の第 3 実施例を示し、高速クロック検知回路の構成を示している。高速クロック検知回路 1 0 0 は、通常ループバック回路部 2 0 と、遅延ループバック回路部 3 0 と、検知結果出力回路部 1 0 とから構成されと共に、カウント閾値設定レジスタ 4 1 及びバスインタフェース 4 2 をさらに含む。第 3 の実施例における通常ループバック回路部 2 0 及び遅延ループバック回路部 3 0 は、第 1 及び第 2 の実施例における同一の構成を備える。

【 0 0 3 1 】

第 3 の実施例における検知結果出力回路部 1 0 は、第 2 の実施例における構成に加えて、カウント閾値設定レジスタ 4 1 を参照してカウント閾値を変更する機能を備える。カウント閾値設定レジスタ 4 1 の内容は、バスインタフェース 4 2 を介して制御回路（図 2 参照）におけるソフトウェアの実行より設定される。カウンタ 1 4 は、カウント閾値設定レジスタ 4 1 に設定されたカウント閾値に従って、第 2 の実施例の場合と同様にして高速クロック検知信号を出力する。

【 0 0 3 2 】

以上の第 3 の実施例において、カウント閾値がソフトウェアから変更可能にされている。第 2 の実施例ではノイズ等によって誤検知しないようにカウンタを設けていたが、ノイズの影響度合いとセキュリティ確保を両立するのに最適なカウント閾値に調整することは容易ではない。しかし、第 3 の実施例においては、カウント閾値がソフトウェアから変更可能にされたことで、最適なカウント閾値の調整を柔軟に行うことが可能である。

【 産業上の利用可能性 】

【 0 0 3 3 】

本発明による高速クロック検知回路は、決済端末の如くセキュリティが要求される装置に使用される L S I のみならず、外部からのハッキング行為が想定される多様な L S I に搭載することができる。

【 図面の簡単な説明 】

【 0 0 3 4 】

【 図 1 】 従来的高速クロック検知回路の概要を示す概要図である。

【 図 2 】 本発明の第 1 の実施例を示し、高速クロック検知回路の構成を示すブロック図である。

【 図 3 】 本発明による高速クロック検知回路がコンピュータシステムに適用された場合の例を示すブロック図である。

10

20

30

40

50

【図4】第1の実施例における高速クロック検知回路の動作タイミングを示すタイムチャートである。

【図5】本発明の第2の実施例を示し、高速クロック検知回路の構成を示すブロック図である。

【図6】第2の実施例における高速クロック検知回路の動作タイミングを示すタイムチャートである。

【図7】本発明の第3の実施例を示し、高速クロック検知回路の構成を示すブロック図である。

【符号の説明】

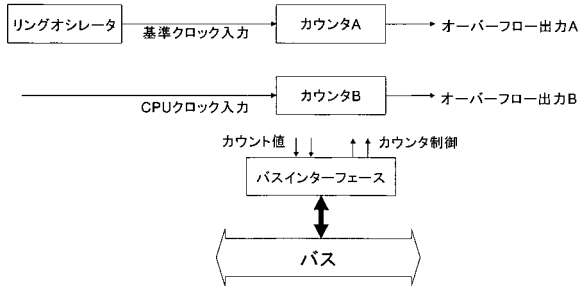
【0035】

- 10 検知結果出力回路部
- 11、21、31 フリップフロップ回路
- 12 排他的論理和回路
- 13 論理和回路
- 20 通常ループバック回路部
- 22、32 反転回路
- 30 遅延ループバック回路部
- 33 遅延回路
- 41 カウント閾値設定レジスタ
- 42 バスインタフェース
- 100 高速クロック検知回路
- 200 CPU
- 300 制御回路
- 400 バス
- 500 メモリ
- 600 周辺回路

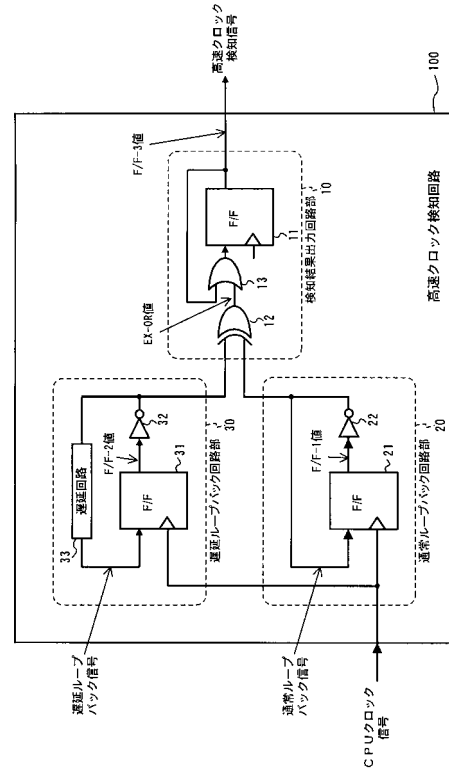
10

20

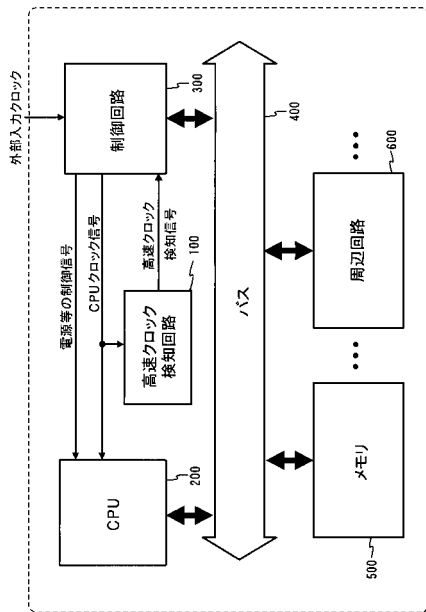
【図1】



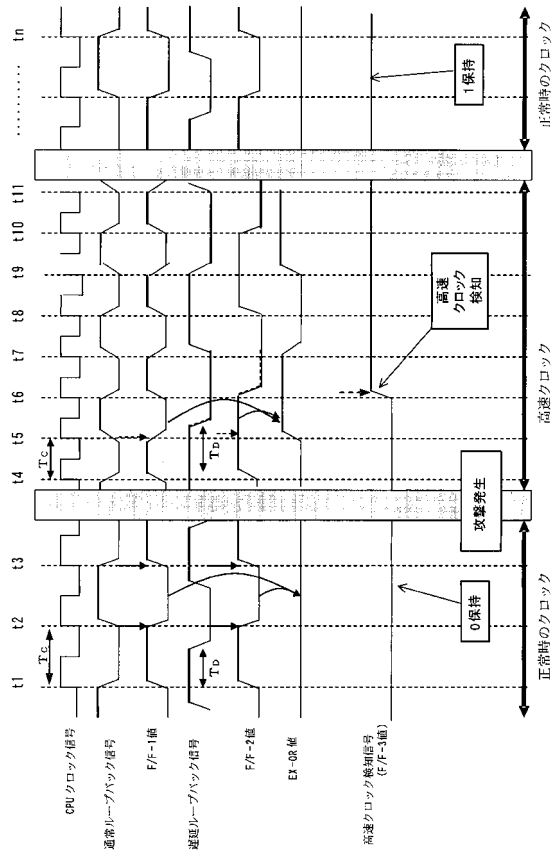
【図2】



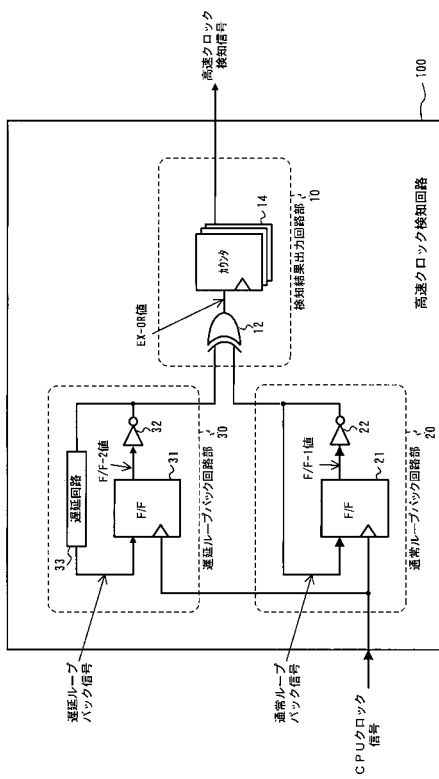
【図3】



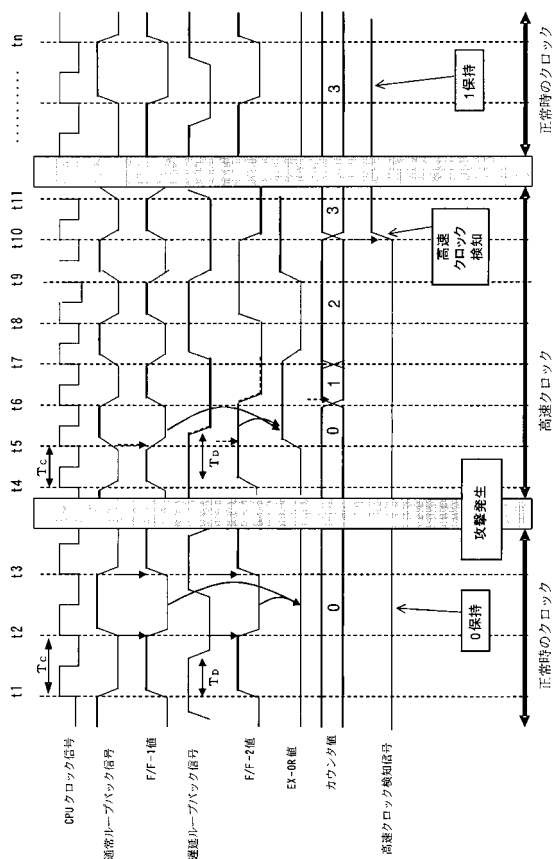
【図4】



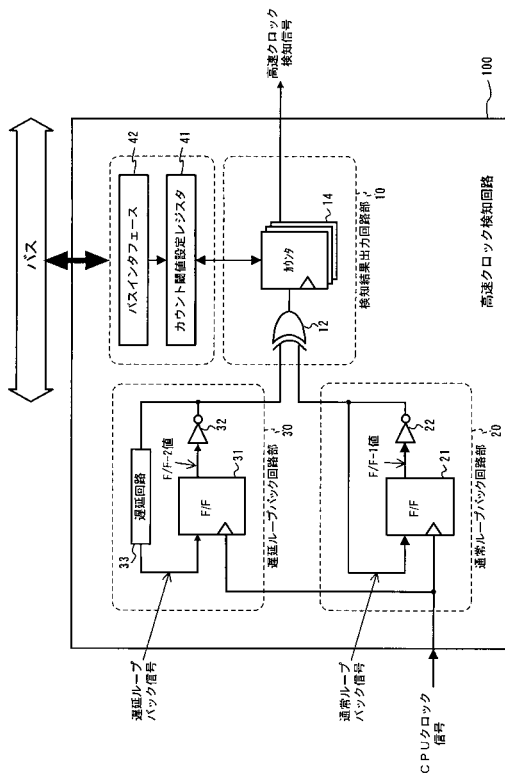
【図5】



【図6】



【図7】



フロントページの続き

- (56)参考文献 特開2005-182349(JP,A)
特開2002-43907(JP,A)
特開平11-15552(JP,A)
特開平10-240374(JP,A)
特開平6-204993(JP,A)
特開平4-371019(JP,A)
特開平1-205237(JP,A)

(58)調査した分野(Int.Cl., DB名)

H03K	5/19
G06F	1/04