(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5985516号
(P5985516)
(45)発行日　平成28年9月6日(2016.9.6)　(24)登録日　平成28年8月12日(2016.8.12)

(51)Int.Cl.　F I
G05B 9/03 (2006.01)　G05B 9/03

請求項の数 11 (全 13 頁)

(21)出願番号	特願2013-553791 (P2013-553791)
(86)(22)出願日	平成24年2月16日 (2012.2.16)
(65)公表番号	特表2014-507034 (P2014-507034A)
(43)公表日	平成26年3月20日 (2014.3.20)
(86)国際出願番号	PCT/DE2012/100037
(87)国際公開番号	WO2012/113385
(87)国際公開日	平成24年8月30日 (2012.8.30)
審査請求日	平成27年1月9日 (2015.1.9)
(31)優先権主張番号	102011011755.5
(32)優先日	平成23年2月18日 (2011.2.18)
(33)優先権主張国	ドイツ(DE)

(73)特許権者　503355292
コンティ　テミック　マイクロエレクトロニック　ゲゼルシャフト　ミット　ベシュレンクテル　ハフツング
Ｃｏｎｔｉ　Ｔｅｍｉｃ　ｍｉｃｒｏｅｌｅｃｔｒｏｎｉｃ　ＧｍｂＨ
ドイツ連邦共和国　ニュルンベルク　ジーボルトシュトラーセ　１９
Ｓｉｅｂｏｌｄｓｔｒａｓｓｅ　１９，Ｄ－９０４１１　Ｎｕｅｒｎｂｅｒｇ，Ｇｅｒｍａｎｙ
(74)代理人　100069556
弁理士　江崎　光史
(74)代理人　100111486
弁理士　鍛冶澤　實

最終頁に続く

(54)【発明の名称】車両内で使用するための安全コンセプト用の半導体回路と方法

(57)【特許請求の範囲】

【請求項１】

－一つの、ＥＧＡＳコンセプトの少なくともレベル１機能、並びに、レベル２機能を実施することにより車両の通常作動を制御している機能用コンピューター（ＦＲ）、

－少なくとも一つの、ＥＧＡＳコンセプトの少なくともレベル３機能を実施する監視ユニット（ＭＵ）、

－一つの、機能用コンピューター（ＦＲ）との少なくとも一種のＱ＆Ａプロシージャ（ＦＡＶ）を実施可能な監視用コンピューター（ＵＲ）、

を包含する車両内で用いる機械的には本質安全ではないシステムに用いる電子制御装置用の半導体回路であって、

－機能用コンピューター（ＦＲ）、監視ユニット（ＭＵ）、並びに、監視用コンピューター（ＵＲ）が、互いに物理的に独立しており、

－監視用コンピューター（ＵＲ）がダウンした場合は、半導体回路の全ての、或いは、制限された機能が、機能用コンピューター（ＦＲ）によって保障され、

－機能用コンピューター（ＦＲ）がダウンした場合は、半導体回路の全ての、或いは、制限された機能が、監視用コンピューター（ＵＲ）によって保障され、

－半導体回路が一つの監視ユニット（ＭＵ）を有している場合において、該監視ユニット（ＭＵ）が以下の：

ａ．監視ユニット（ＭＵ）と機能用コンピューター（ＦＲ）間のＱ＆Ａプロシージャ（ＦＡＶ）を初期化、

ｂ．機能用コンピューター（ＦＲ）と監視用コンピューター（ＵＲ）間のＱ＆Ａプロシージャ（ＦＡＶ）を初期化、
ｃ．機能用コンピューター（ＦＲ）と監視ユニット（ＭＵ）間のＱ＆Ａプロシージャ（ＦＡＶ）にはエラーは無いが、機能用コンピューター（ＦＲ）と監視用コンピューター（ＵＲ）間のＱ＆Ａプロシージャ（ＦＡＶ）にはエラーがあるケースにおいては、
該機能用コンピューター（ＦＲ）が、予め定められ、エラーに依存して実施される手順の後に、監視用コンピューター（ＵＲ）をリセットし、半導体回路の全ての、或いは、制限された機能を受け持つ、
ｄ．機能用コンピューター（ＦＲ）と監視ユニット（ＭＵ）間のＱ＆Ａプロシージャ（ＦＡＶ）にエラーがあるケースにおいて、監視ユニット（ＭＵ）が、予め定められ、エラーに依存して実施される手順の後に、先ず、監視シグナルをアクティブにし、続いて、機能用コンピューター（ＦＲ）をリセットする、
ｅ．監視用コンピューター（ＵＲ）が、監視シグナルと機能用コンピューター（ＦＲ）のリセットシグナルを読む、
ｆ．監視用コンピューター（ＵＲ）が、半導体回路の全ての、或いは、制限された機能を受け持つ、
ステップを実行するよう構成されている
ことを特徴とする車両内で用いる機械的には本質安全ではないシステムに用いる電子制御装置用の半導体回路。

【請求項２】

－一つの、ＥＧＡＳコンセプトの少なくともレベル１機能、並びに、レベル２機能を実施することにより車両の通常作動を制御している機能用コンピューター（ＦＲ）、
－少なくとも一つの、ＥＧＡＳコンセプトの少なくともレベル３機能を実施する監視ユニット（ＭＵ）、
－一つの、機能用コンピューター（ＦＲ）との少なくとも一種のＱ＆Ａプロシージャ（ＦＡＶ）を実施可能な監視用コンピューター（ＵＲ）、
を包含する車両内で用いる機械的には本質安全ではないシステムに用いる電子制御装置用の半導体回路であって、
－機能用コンピューター（ＦＲ）、監視ユニット（ＭＵ）、並びに、監視用コンピューター（ＵＲ）が、互いに物理的に独立しており、
－監視用コンピューター（ＵＲ）がダウンした場合は、半導体回路の全ての、或いは、制限された機能が、機能用コンピューター（ＦＲ）によって保障され、
－機能用コンピューター（ＦＲ）がダウンした場合は、半導体回路の全ての、或いは、制限された機能が、監視用コンピューター（ＵＲ）によって保障され、
－監視ユニット（ＭＵ）が第一監視ユニット（ＭＵ１）及び第二監視ユニット（ＭＵ２）で構成されている場合において、該第一監視ユニット（ＭＵ１）及び第二監視ユニット（ＭＵ２）が以下の：
ａ．第一監視ユニット（ＭＵ１）と機能用コンピューター（ＦＲ）間のＱ＆Ａプロシージャ（ＦＡＶ）を初期化、
ｂ．第二監視ユニット（ＭＵ２）と監視用コンピューター（ＵＲ）間のＱ＆Ａプロシージャ（ＦＡＶ）を初期化、
ｃ．機能用コンピューター（ＦＲ）と監視用コンピューター（ＵＲ）間のＱ＆Ａプロシージャ（ＦＡＶ）を初期化、
ｄ．機能用コンピューター（ＦＲ）と第一監視ユニット（ＭＵ１）間のＱ＆Ａプロシージャ（ＦＡＶ）にエラーがあるケースにおいては、
第一監視ユニット（ＭＵ１）が、予め定められ、エラーに依存して実施される手順の後に、先ず、監視シグナルをアクティブにし、続いて、機能用コンピューター（ＦＲ）をリセットする、
ｅ．監視用コンピューター（ＵＲ）が、監視シグナルと機能用コンピューター（ＦＲ）のリセットシグナルを読む、

ｆ．監視用コンピューター（ＵＲ）が、半導体回路の全ての、或いは、制限された機能を受け持つ、
ｇ．監視用コンピューター（ＵＲ）と第二監視ユニット（ＭＵ２）間のＱ＆Ａプロシージャ（ＦＡＶ）にエラーがあるケースにおいては、第二監視ユニット（ＭＵ２）が、予め定められ、エラーに依存して実施される手順の後に、先ず、監視シグナルをアクティブにし、続いて、監視用コンピューター（ＵＲ）をリセットする、
ｈ．機能用コンピューター（ＦＲ）が、監視シグナルと監視用コンピューター（ＵＲ）のリセットシグナルを読む、
ｉ．機能用コンピューター（ＦＲ）が、半導体回路の全ての、或いは、制限された機能を受け持つ、
ｊ．機能用コンピューター（ＦＲ）と監視用コンピューター（ＵＲ）間のＱ＆Ａプロシージャ（ＦＡＶ）にエラーがあるケースにおいては、機能用コンピューター（ＦＲ）が、予め定められ、エラーに依存して実施される手順の後に、監視用コンピューター（ＵＲ）をリセットする、
ｋ．機能用コンピューター（ＦＲ）が、半導体回路の全ての、或いは、制限された機能を受け持つ、
ステップを実行するよう構成されていることを特徴とする車両内で用いる機械的には本質安全ではないシステムに用いる電子制御装置用の半導体回路。

【請求項３】

機能用コンピューター（ＦＲ）と監視用コンピューター（ＵＲ）が、それぞれ独立した電源（ＳＶ１，ＳＶ２）を有していることを特徴とする請求項１或いは２に記載の半導体回路。

【請求項４】

監視用コンピューター（ＵＲ）の電源（ＳＶ２）が、監視用コンピューター（ＵＲ）を付加的に監視するウォッチドッグ（ＷＤ）を有していることを特徴とする請求項１～３の何れか一項に記載の半導体回路。

【請求項５】

コンピューター（ＦＲ，ＵＲ）の電源（ＳＶ１，ＳＶ２）が、コンピューター（ＦＲ，ＵＲ）を監視するウォッチドッグ（ＷＤ）を有していることを特徴とする請求項１～３の何れか一項に記載の半導体回路。

【請求項６】

その後に、監視シグナルがアクティブにされ、続いて、コンピューター（ＦＲ，ＵＲ）がリセットされるための、予め定められ、エラーに依存して実施される手順が、以下の：
ａ．ｍ回、誤った回答があると、監視する／質問するユニット（ＭＵ，ＦＲ，ＵＲ）が、先ず、クリティカルなアクチュエーター・パワーアンプの電源をカットするための監視シグナルを作動させる、
ｂ．監視する／質問するユニット（ＭＵ，ＦＲ，ＵＲ）と監視されている／回答するユニット（ＦＲ，ＵＲ）間のＱ＆Ａプロシージャ（ＦＡＶ）において、更にｎ回、誤った回答があると、監視する／質問するユニット（ＭＵ，ＦＲ，ＵＲ）は、監視されている／回答するユニット（ＦＲ，ＵＲ）をリセットする
ステップを包含していることを特徴とする請求項１或いは２に記載の半導体回路を監視するための方法。

【請求項７】

コンピューター（ＦＲ，ＵＲ）のブート中、適宜な時間制御、ロジック、或いは、ソフトウェアによって、エラー発生時には、それぞれの安全機能が作動することが保障されていることを特徴とする請求項６に記載の方法。

【請求項８】

半導体回路の制御されたラン・アウト（「シャットダウン」）を、双方のコンピューター（ＦＲ，ＵＲ）のラン・アウト・フェーズにおいて、シーケンス「制御下に監視を非活性化する」から、シーケンス「電源（ＳＶ１，ＳＶ２）をカットする」までを実施するこ

とによって行っていることを特徴とする請求項６或いは７に記載の方法。
【請求項９】
全てのアクティブなＱ＆Ａプロシージャを、機能用コンピューター（ＦＲ）が全ての電源（ＳＶ１，ＳＶ２）の自己保持の解除直前に至るまで、実施し続けることを特徴とする請求項８に記載の方法。
【請求項１０】
監視用コンピューター（ＵＲ）の電源（ＳＶ２）内に内蔵されているウォッチドッグ（ＷＤ）が、監視用コンピューター（ＵＲ）を、該監視用コンピューターが、機能用コンピューターによってまだ監視されていないフェーズに監視することを特徴とする請求項６，７、８或いは９に記載の方法。
【請求項１１】
コンピューター（ＦＲ，ＵＲ）の電源（ＳＶ１，ＳＶ２）内に内蔵されているウォッチドッグ（ＷＤ）が、コンピューター（ＦＲ，ＵＲ）を、監視ユニット（ＭＵ１，ＭＵ２）によってこれらが監視されていない、或いは、まだ監視されていないフェーズにおいて、付加的に監視することを特徴とする請求項６、７、８、９或いは１０に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、独立請求項のプレアンブルに定義されている車両内で使用するための安全コンセプト用の半導体回路と方法に関する。
【０００２】
車両内で使用される機能ユニット、例えば、半導体回路を備えた制御装置などを故障フリーあるいは本質安全に構成する様々なコンセプトが既に存在している。制御装置の本質安全を達成する例としては、３レベル・コンセプトにおける監視が挙げられる。
【０００３】
特許文献１からは、車両の駆動ユニットの制御用の方法および装置が既知である。ここでは、出力を制御するための制御装置は、唯一のマイクロコントローラーのみしか有していない。即ち、該マイクロコントローラーは、制御と監視の双方を受け持っている。作動信頼性および稼働率は、制御の実施と監視を実施する少なくとも二つの互いに独立したレベルが、該唯一のマイクロコントローラーに設けられることによって確保されているが、詳しくは、第一レベルでは、出力制御の機能が決定され、第二レベルでは、特に、監視モジュールとの組み合わせにおいて、この機能、要するに、該マイクロコントローラーの作動を、自ら監視している。
【０００４】
また、特許文献１には、第二レベルのプログレス・コントロールを実施する第三レベルが開示されている。第三レベルによる監視により、制御装置の信頼性と稼働率は、有意に向上する。特に、第二レベルのプログレス・コントロールは、監視モジュールにおいてＱ＆Ａコミュニケーションとして実施されている。
【０００５】
このような３レベル監視コンセプト（ＥＧＡＳコンセプト）は、電子エンジン制御システムを監視するための車両のエンジン制御装置において、一般的に採用されている。ここでは、エンジン制御装置は、所謂、機能用コンピューターと監視用コンピューターから構成されている。尚、該機能用コンピューターと該監視用コンピューターは、Ｑ＆Ａコミュニケーションによって互いにコミュニケーションしている。更にこれらは、独立した停止パスを有している。
【０００６】
レベル１には、車両の駆動ユニットの機能を制御するための機能モジュールそのものが、包含されている。よって、これは、機能レベルとも呼ばれる。これは、エンジン制御機能、例えば、要求されるエンジン・モーメント、コンポーネント監視、入力値や出力値の診断、並びに、エラーが認識された際のシステム・リアクションの制御なども包含してい

る。そして、このレベル１は、機能用コンピューターにおいて実施される。

【０００７】

レベル２は、機能監視レベルとも呼ばれ、安全用モジュールを包含し、これも、機能用コンピューターにおいて実施される。これは、レベル１の機能モジュールの監視されなければならない範囲、例えば、計算されたモーメントや車両の加速の誤った動作を検出する。エラーがある場合、システム・リアクションの作動が、実施される。レベル２は、レベル３によって安全が確保された機能用コンピューターのハードウェア範囲において実施される。

【０００８】

該レベル３は、コンピューター監視レベルとも呼ばれ、命令系テスト、プログラム・プログレス・コントロール、Ａ／Ｄ変換器テスト及び周期的かつ総合的なレベル２のメモリーテストを実施する独立した監視ユニット（ＡＳＩＣ或いはμＣ）上の監視モジュールを包含している。機能用コンピューターから独立した監視ユニットは、Ｑ＆Ａプロシージャに従って機能用コンピューターのプログラム命令の正常なプログレスをテストする。エラーがある場合、システム・リアクションの作動は、機能用コンピューターから独立して実施される。

【０００９】

従来の電子エンジン制御システムでは、全ての機能用ソフトウェアと監視用ソフトウェアが、一つの制御装置上にある。また、このような監視コンセプトは、他の車両制御装置、特に、トランスミッション制御装置内においても実施可能である。

【００１０】

このような安全コンセプトでは略必ず、第二レベルでエラーがあった場合は、制御装置内のパワーを設定するためのパワーアンプによって、アクチュエーターは、電源カット状態にされる。エラーが第三レベルで発生した場合は、第一ステップにおいて、制御装置内のパワーを設定するためのパワーアンプによって、アクチュエーターは、電源カット状態とされ、第二ステップにおいて、監視ユニット（第三レベル）によって、機能用コンピューターが、リセットされる。このような電源カット状態は、略常に、被制御システム全体、特に、オートマチック・トランスミッションが安全な状態にあると言える。

【００１１】

即ち、圧力がかかっていない状態においてバネの力で開かれるクラッチを有するトランスミッションの具体例で説明すると、緊急時、パワーを設定するためのパワーアンプが、オフになった場合、クラッチを作動させる油圧システムも使用できないが、クラッチが、機械的なバネの力によって開いている状態に保持され、よって、エンジンのモーメントが、駆動輪に伝達されない、即ち、意図されている緊急状態には移行することができる。

【００１２】

しかしながら、電流が流れていない、或いは、圧力がかかっていない状態で機械的バネ力に対して閉じるクラッチ、所謂「ｎｏｒｍａｌｌｙ　ｃｌｏｓｅｄ（ノーマリー・クローズド）」クラッチもあり、このようなクラッチには、上記のような形態の監視コンセプトは、採用できない。

【００１３】

該第三レベルは、機能用コンピューターの監視を主に実施する、ＡＳＩＣ、或いは、独立したマイクロコントローラーであってもよい。その際、Ｑ＆Ａプロシージャのためのデータ交換は、通常、コンピューターでは一般的なインターフェース、例えば、ＳＰＩ（Ｓｅｒｉａｌ　Ｐｅｒｉｐｈｅｒａｌ　Ｉｎｔｅｒｆａｃｅ）を介して実施される。

【００１４】

しかし、第三レベルが、ＡＳＩＣの「モニタリング・ユニット」の機能の一部として実施されているケースでは、Ｑ＆Ａプロシージャのエラー時においては、アクチュエーターは、唯一の状態、即ち、そのパワーを設定するためのパワーアンプが、電源カット状態とされる、言い換えれば、スイッチング・シーケンスや制御されたアクション・フローなどは実施できない状態に、略必ず、されてしまう。但し、アクション・フローには、アクチ

ュエーターの位置を適切なセンサーシグナルによって割出、必要に応じて、変更、或いは、制御することも含まれる。これは、ＡＳＩＣには、エレクトロニクスに影響を与えられるスイッチング・シグナルは、一つしか出力できないこと、更に、ＡＳＩＣには、センサー・シグナルが処理できないため、制御シグナルを出力することができないためである。

【００１５】

第三レベルが、付加的なコンピューター（μＣ）によって実施されているケースでは、Ｑ＆Ａプロシージャにおいてエラーがあった場合に、「質問側」或いは「回答側」である双方のコンピューターのいずれが、本当にエラー無しに作動しているか否かを絶対的に疑い無くは、特定できない。そのため、エラー発生時、双方のコンピューターは、安全なシステム状態（パワーアンプ電源カット）とし、リセットされなければならない。即ち、例え二つ目のコンピューターを第三レベルに使用したとしても、エラー発生時には、スイッチング・シーケンスや制御されたアクション・フローを実施できない。

【００１６】

双方のケースにおいて、車両は、直ちに駆動しない状態（エンジンが切られ、駆動系がオープン　＝　「立ち往生車両」）となり、且つ、いかなる制御機能もないため緊急運転（エンジンがかかっており、制限されたモーメント伝達が可能　＝　「ｌｉｍｐ　ｈｏｍｅ　ｍｏｄｅ　（びっこをひいたような状態のモード）」）すらできないと言う更なる欠点がある。

【先行技術文献】

【特許文献】

【００１７】

【特許文献１】独国特許出願公開第４４３８７１４号明細書

【発明の概要】

【発明が解決しようとする課題】

【００１８】

よって本発明の課題は、車両内で用いる機械的には本質安全ではないシステムに用いる、エラー発生時に、制御された安全な緊急作動、或いは、少なくとも、安全な状態、特に、「駆動系オープン」状態を保障できる電子制御装置用の半導体回路を提供することである。

【課題を解決するための手段】

【００１９】

この課題は、本発明の独立請求項１記載の特徴を持つ半導体回路によって達成される。

【００２０】

半導体回路上には、ＩＳＯ　２６２６２に準拠して、機能用コンピューター、監視ユニット、監視用コンピューターが、それぞれ独立したモジュールとして互いに独立して、好ましくは、一つの共通の回路担体に配置されている。仮に、監視用コンピューターが、安全に関わるエラーによって使えなくなった場合には、機能用コンピューターが、半導体回路の全ての、或いは、制限された機能を請け負うことができる。逆に、機能用コンピューターが、使えなくなった場合には、監視用コンピューターが、半導体回路の全ての、或いは、制限された機能を請け負うことができるようになっている。尚、「制限された機能」とは、駆動系がオープンである、或いは、制限されたモーメントの伝達を保障する緊急作動のことである。

【００２１】

これは、基本的には、一つ、乃至、二つのコンピューターよって、この機能を実施できるようになっていることを意味する。即ち、これにより、完全な、或いは、部分的な冗長性が確保されている。エラー発生時、一つのコンピューターに機能的な異常が確信をもって認識され、リセット状態に保たれている間、他のコンピューターは、機能的に正常であると見なされる。

【００２２】

これにより、作動中いかなる時点においても、駆動系の状態が、双方のコンピューター

の内の少なくとも一つによって認識され、システム内のこの情報が、ハードウェア、及び、ソフトウェアによって、安全な状態、即ち、駆動系がオープン、或いは、緊急作動状態を、常に確保できることが保障されている。

【００２３】

このコンセプトの更なる長所としては、機能用コンピューターのアプリケーションに依存する特定の機能を、監視用コンピューターへ移行させることができることが、挙げられる。

【００２４】

更に、半導体回路内でリソース問題がある場合、機能用コンピューターと監視用コンピューター間の機能ブロックを、ＣＰＵの最大負荷を超えないように、移行させることも可能である。

【００２５】

また、完全な冗長性を達成するため、アプリケーションに依存する機能を機能用コンピューターと監視用コンピューターの双方に持たせることも可能である。

【００２６】

更なる安全アスペクトとしては、特に、機能用コンピューターと監視用コンピューター（ＵＲ）が、それぞれ独立した電源を有していることが挙げられる。

【００２７】

特に、双方のコンピューターのブート中は、システム内で安全に関わるエラーが起こった場合でも、適切なタイム制御とロジックによって、それぞれの安全機能が作動するように保障されていることが好ましい。監視用コンピューターが、機能用コンピューターによって監視されていない、或いは、まだ監視されていないフェーズにおいては、監視用コンピューターの電源に内蔵された「ウォッチドッグ（番犬）」が、付加的にこれを監視することもできる。

【００２８】

本発明の更なる課題は、車両内で用いる機械的には本質安全ではないシステムに用いる、エラー発生時に、制御された安全な緊急作動、或いは、少なくとも、安全な状態、特に、「駆動系オープン」状態を保障できる電子制御装置用の方法を提供することである。

【００２９】

本発明では、上記課題は、独立請求項４及び５に記載の特徴を有する方法によって解決される。

【００３０】

エレクトロニクス制御装置内の半導体回路を監視するための方法は、一つの監視ユニットを有する半導体回路、並びに、一つ以上の監視ユニットを有する半導体回路に分類できる。但し、後者では、各々の監視ユニットは、一つのエレクトロニクス・モジュール、或いは、複数の独立したモジュールに配置されることができる。

【００３１】

このような方法では、先ず、コンピューター間、或いは、該当する監視ユニット間のそれぞれのＱ＆Ａプロシージャが、初期化される。

【００３２】

Ｑ＆Ａプロシージャのどこでエラーが起こったのかに依存して、監視用コンピューターがリセットされる、或いは、機能用コンピューターが、緊急作動において、半導体回路の機能を請け負う、或いは、その逆が、実施される。このような機能は、通常、安全な状態とする、或いは、緊急作動（「Ｌｉｍｐ　ｈｏｍｅ」）を実施するためにある。その際、エラーを起こしているコンピューターは、例えば、半導体回路のパワー・アップ・リセットが終了するまで、リセット状態に維持される。一つ以上の監視ユニットを用いることにより、コストは上がるが、システムの安全性は、向上する。

【００３３】

特に、機能用コンピューターと監視用コンピューターのブート中、例えば、タイム・アウトなどの適切な時間制御、ロジックやソフトウェアによって、このフェーズにおいて発

生し得るエラーが実際起こった場合に該当する安全機能が作動することを保証することが好ましい。これが、機能用コンピューターによって監視されていない、或いは、まだ監視されていないフェーズにおいては、監視用コンピューターの電源に内蔵された「ウォッチドッグ（番犬）」が、付加的にこれを監視することもできる。

【００３４】

半導体回路の制御されたラン・アウト（「シャットダウン」）は、双方のコンピューターのラン・アウト・フェーズにおいて、半導体回路の監視の制御された非活性化シーケンスから双方のコンピューターのそれぞれの電源の停止まで実施されることが好ましい。これにより、例えば、全てのアクティブなＱ＆Ａプロシージャを、機能用コンピューターが、全ての電源が自らオフになる寸前に停止するまで、実施し続けることができる。

【００３５】

ハードウェアとソフトウェアから構成される適宜なシステム・アーキテクチャにより、このコンセプトによって、いかなる作動時点においても、特に、半導体回路の初期化フェーズにおいて、駆動系の安全に関わる状態が、双方のコンピューターのうち少なくとも一つによって、確実に認識され、且つ、その情報は、システム内のハードウェア及びソフトウェアによって、エラー発生時に、車両の安全な状態、即ち、駆動系がオープン、或いは、緊急作動状態になることが常に保障できるように、処理される。

【００３６】

以下の発明の詳細な説明において、本発明の特徴および詳細を、図面に基づいた実施例を挙げながら詳しく説明する。なお、各バリエーションにおいて記載されている特徴および関連事項は、基本的に全ての実施例において採用可能である。

【図面の簡単な説明】

【００３７】

【図１】監視ユニットを備えた半導体回路のブロック図である。

【図２】二つの監視ユニットを備えた半導体回路のブロック図である。

【図３】監視ユニットを備えた方法用のフローチャートである。

【図４】二つの監視ユニットを備えた方法用のフローチャートである。

【図５】コンピューターがリセットされた後の動作を示すフローチャートである。

【発明を実施するための形態】

【００３８】

図１は、物理的にはそれぞれ独立している機能用コンピューター（ＦＲ）、監視用コンピューター（ＵＲ）、並びに、監視ユニット（ＭＵ）を備えた半導体回路のブロック図である。該機能用コンピューター（ＦＲ）は、特に、車両の通常作動を、既に説明したＥＧＡＳコンセプトの少なくともレベル１機能、並びに、レベル２機能を実施することにより制御している。また、該監視ユニット（ＭＵ）は、ＥＧＡＳコンセプトのレベル３機能を実施している。尚、監視ユニット（ＭＵ）は、監視用コンピューター（ＵＲ）とシグナル的につながっている。機能用コンピューター（ＦＲ）と監視用コンピューター（ＵＲ）間だけでなく、機能用コンピューター（ＦＲ）と監視ユニット（ＭＵ）間においても、それぞれの正しい機能を監視するために、Ｑ＆Ａプロシージャ（ＦＡＶ）が実施されている。これは、図１において、機能用コンピューター（ＦＲ）と監視用コンピューター（ＵＲ）間、並びに、機能用コンピューター（ＦＲ）と監視ユニット（ＭＵ）間の二本矢印で示されている。

【００３９】

特に、監視用コンピューター（ＵＲ）がダウンした場合、半導体回路の全ての、或いは、制限された機能は、機能用コンピューター（ＦＲ）によって保障される。また、機能用コンピューター（ＦＲ）がダウンした場合、半導体回路の全ての、或いは、制限された機能は、機能している監視用コンピューター（ＵＲ）によって保障可能であることが好ましい。

【００４０】

機能用コンピューター（ＦＲ）と監視用コンピューター（ＵＲ）が、独立した電源を有

していることは、安全に関する更なる長所である。

【００４１】

特に、監視用コンピューター（ＵＲ）の電源（ＳＶ２）内に内蔵されている付加的なウォッチドッグ（ＷＤ）は、監視用コンピューター（ＵＲ）を、双方のコンピューター（ＦＲ，ＵＲ）のブート・フェーズ中であって、該監視用コンピューター（ＵＲ）が、機能用コンピューター（ＦＲ）によって監視されていない、或いは、まだ監視されていない場合に、監視することができる。特に、このフェーズ中は、システム内で安全に関わるエラーが起こった場合でも、適切なタイム制御とロジックによって、それぞれの安全機能が作動するように保障されていることが好ましい。

【００４２】

図２は、図１の半導体回路のブロック図であるが、ここでは、二つの監視ユニット（ＭＵ１，ＭＵ２）を備えている。この際、第一監視ユニット（ＭＵ１）は、Ｑ＆Ａプロシージャ（ＦＡＶ）により、機能用コンピューター（ＦＲ）の正しい機能を、同様に、第二監視ユニット（ＭＵ２）は、監視用コンピューター（ＵＲ）の正しい機能を監視することが特に好ましい。機能用コンピューター（ＦＲ）と監視用コンピューター（ＵＲ）も、例えば、Ｑ＆Ａプロシージャ（ＦＡＶ）を実施できるように、シグナル的につながっている。

【００４３】

図３は、機能用コンピューター（ＦＲ）の正しい機能を監視し、監視用コンピューター（ＵＲ）ともシグナル的につながっている監視ユニット（ＭＵ）を備えた半導体回路を監視するための方法用のフローチャートを示している。

【００４４】

先ず、機能用コンピューター（ＦＲ）と監視ユニット（ＭＵ）間、並びに、機能用コンピューター（ＦＲ）と監視用コンピューター（ＵＲ）間の対応するＱ＆Ａプロシージャ（ＦＡＶ）が、初期化されるが、この際、双方のＱ＆Ａプロシージャ（ＦＡＶ）は、同一である必要はない。

【００４５】

仮に、機能用コンピューター（ＦＲ）と監視ユニット（ＭＵ）間のＱ＆Ａプロシージャ（ＦＡＶ）にはエラーが無く、機能用コンピューター（ＦＲ）と監視用コンピューター（ＵＲ）間のＱ＆Ａプロシージャ（ＦＡＶ）にエラーがあった場合は、該監視用コンピューターは、予め定められ、エラーに依存して実施される手順に従って停止され、機能用コンピューターによって、リセット状態に維持される。そして、機能用コンピューター（ＦＲ）が、半導体回路の全ての、或いは、制限された機能を請け負う。その際、監視用コンピューター（ＵＲ）は、例えば、半導体回路のパワー・アップ・リセットが終了するまで、リセット状態に維持される。

【００４６】

仮に、機能用コンピューター（ＦＲ）と監視ユニット（ＭＵ）間のＱ＆Ａプロシージャ（ＦＡＶ）にエラーがある場合は、該機能用コンピューターは、予め定められ、エラーに依存して実施される手順に従って停止され、監視用コンピューターによって、リセット状態に維持される。そして、監視用コンピューター（ＵＲ）が、半導体回路の全ての、或いは、制限された機能を請け負う。その際、機能用コンピューター（ＦＲ）は、例えば、半導体回路のパワー・アップ・リセットが終了するまで、リセット状態に維持される。

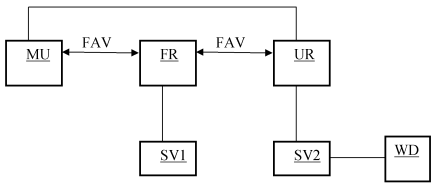
【００４７】

図４は、二つの監視ユニット（ＭＵ１，ＭＵ２）を備えた半導体回路を監視するための方法用のフローチャートであるが、ここでは、第一監視ユニット（ＭＵ１）は、機能用コンピューター（ＦＲ）を、第二監視ユニット（ＭＵ２）は、監視用コンピューター（ＵＲ）を監視している。先ず、機能用コンピューター（ＦＲ）と第一監視ユニット（ＭＵ１）間、監視用コンピューター（ＵＲ）と第二監視ユニット（ＭＵ２）間、並びに、機能用コンピューター（ＦＲ）と監視用コンピューター（ＵＲ）間の対応するＱ＆Ａプロシージャ（ＦＡＶ）が、初期化されるが、この際、それぞれのＱ＆Ａプロシージャ（ＦＡＶ）は、異なっていてもよい。

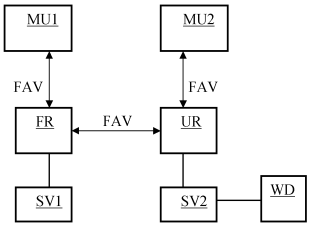
【００４８】
仮に、機能用コンピューター（ＦＲ）と第一監視ユニット（ＭＵ１）間のＱ＆Ａプロシージャ（ＦＡＶ）にエラーがある場合、第一監視ユニット（ＭＵ１）が、予め定められ、エラーに依存して実施される手順の後に、機能用コンピューター（ＦＲ）をリセットすることが特に好ましい。この機能用コンピューター（ＦＲ）のリセット・シグナルは、監視用コンピューター（ＵＲ）によって読まれ、該監視用コンピューター（ＵＲ）が、半導体回路の全ての、或いは、制限された機能を請け負う。
【００４９】
仮に、監視用コンピューター（ＵＲ）と第二監視ユニット（ＭＵ２）間のＱ＆Ａプロシージャ（ＦＡＶ）にエラーがある場合、第二監視ユニット（ＭＵ２）が、予め定められ、エラーに依存して実施される手順の後に、監視用コンピューター（ＵＲ）をリセットすることが特に好ましい。このリセット・シグナルは機能用コンピューター（ＦＲ）によって読まれ、該機能用コンピューター（ＦＲ）が、半導体回路の全ての、或いは、制限された機能を請け負う。
【００５０】
仮に、機能用コンピューター（ＦＲ）と監視用コンピューター（ＵＲ）間のＱ＆Ａプロシージャ（ＦＡＶ）にエラーがある場合、機能用コンピューター（ＦＲ）が、予め定められ、エラーに依存して実施される手順の後に、監視用コンピューター（ＵＲ）をリセットすることが特に好ましい。そして、機能用コンピューター（ＦＲ）が、半導体回路の全ての、或いは、制限された機能を請け負うことが好ましい。また、監視用コンピューター（ＵＲ）が、機能用コンピューター（ＦＲ）をリセットしてから、半導体回路の全ての、或いは、制限された機能を請け負うことも考え得る。
【００５１】
以下の説明は、一つの監視ユニットを備えた、並びに、二つの監視ユニット（ＭＵ１，ＭＵ２）を備えた半導体回路を監視するための方法に関する。
【００５２】
その実施後に、コンピューター（ＦＲ，ＵＲ）がリセットされる、予め定められ、エラーに依存して実施される手順の例は、図５に示されている。特に、その手順では、監視する／質問するユニット（ＭＵ，ＦＲ，ＵＲ）は、ｍ回、誤った回答があると、先ずは、監視シグナルを作動させ、クリティカルなアクチュエーター・パワーアンプの電源をカットすることができる。また、監視する／質問するユニット（ＭＵ，ＦＲ，ＵＲ）と監視されている／回答するユニット（ＦＲ，ＵＲ）間のＱ＆Ａプロシージャ（ＦＡＶ）において、更にｎ回、誤った回答があると、監視する／質問するユニット（ＭＵ，ＦＲ，ＵＲ）は、監視されている／回答するユニット（ＦＲ，ＵＲ）をリセットする。この際、ｍとｎの値は、４から１０の間であることが好ましい。
【００５３】
監視シグナルとリセットシグナルの状態は、まだ機能しているユニット（ＦＲ，ＵＲ）によって読まれ、該まだ機能しているユニット（ＦＲ，ＵＲ）が、機能していないユニット（ＦＲ，ＵＲ）をリセット状態に保ち、対応する必要な対策、例えば、半導体回路の、例えば、安全なシステム状態を得るなどと言った、全ての、或いは、制限された機能を受け持つことができるように、評価される。
【００５４】
その際、それぞれのエラーを起こしているコンピューター（ＦＲ，ＵＲ）は、例えば、半導体回路のパワー・アップ・リセットが終了するまで、リセット状態に維持される。一つ以上の監視ユニットを採用することにより、システムの安全性は、向上する。
【００５５】
適宜な初期化シーケンスと、各々のコンピューター（ＦＲ，ＵＲ）用で必ず独立した電源を用いることによって、コンピューター（ＦＲ，ＵＲ）が互いにブロックすることや、監視されていない時間を避けることができる、或いは、電源内の単純なエラーが、システム全体の機能を阻害することを避けることができる。

【００５６】
特に、機能用コンピューター（ＦＲ）と監視用コンピューター（ＵＲ）のブート中、例えば、タイム・アウトなどの適切な時間制御、ロジックやソフトウェアによって、このフェーズにおいて発生し得るエラーが実際起こった場合に該当する安全機能が作動することを保証することが好ましい。電源（ＳＶ１，ＳＶ２）に内蔵されたウォッチドッグ（ＷＤ）は、コンピューター（ＦＲ，ＵＲ）を、これが、監視ユニット（ＭＵ１，ＭＵ２）によって監視されていない、或いは、まだ監視されていないフェーズにおいて監視することができる。
【００５７】
半導体回路の制御されたラン・アウト（「シャットダウン」）は、双方のコンピューター（ＦＲ，ＵＲ）のラン・アウト・フェーズにおいて、半導体回路の監視の制御された非活性化シーケンスから双方のコンピューター（ＦＲ，ＵＲ）のそれぞれの電源（ＳＶ１，ＳＶ２）の停止まで実施されることが好ましい。これにより、例えば、全てのこの時点でアクティブなＱ＆Ａプロシージャ（ＦＡＶ）を、機能用コンピューター（ＦＲ）が、全ての電源（ＳＶ１，ＳＶ２）が自らオフになる寸前に停止するまで、実施し続けることができる。
【００５８】
制御されるシステムが、特に、少なくとも一つのノーマリー・クローズド・クラッチを備えたデュアルクラッチ・トランスミッションなど、緊急作動状態、或いは、安全な状態を得るために、スイッチング・シーケンスや制御された手順、アクティブな介入が必要とされ、この手順や制御がコンピューターによって行われなければならない機械的には本質安全ではないシステムである場合は、該当するコンピューターの完全な機能が確保されていなければならない。このような手順や介入の例としては、クラッチバルブへの制御された油圧注入や電気・油圧的なギヤ抜きが挙げられる。
【００５９】
即ち、基本的に、一つの、或いは、双方のコンピューターによって、（完全な、或いは、部分的な冗長性により）機能を遂行できる、且つ、エラー発生時、一つのコンピューターに、確信をもって、機能的な異常が認識され、これが、停止状態に保持されている間、もう一方のコンピューターは、正常に機能していなければならないことを意味する。
【００６０】
ハードウェアとソフトウェアから構成される適宜なシステム・アーキテクチャにより、このコンセプトによって、いかなる作動時点においても、特に、半導体回路の初期化フェーズにおいて、駆動系の安全に関わる状態が、双方のコンピューターのうち少なくとも一つによって、確実に認識され、且つ、その情報は、システム内のハードウェア及びソフトウェアによって、エラー発生時に、車両の安全な状態、即ち、駆動系がオープン、或いは、緊急作動状態になることが常に保障できるように、処理される。
【００６１】
このコンセプトの更なる長所は、機能用コンピューターのアプリケーションに依存する特定の機能を、監視用コンピューターへ移行させることができる、特に、エラー発生時に、これを監視用コンピューターによって、請け負わせることができることである。
【００６２】
更に、リソース問題がある場合、機能用コンピューターと監視用コンピューター間の機能ブロックを、ＣＰＵの最大負荷を超えないように、移行させることも可能である。
【００６３】
また、完全な冗長性を達成するため、アプリケーションに依存する機能を機能用コンピューターと監視用コンピューターの双方に持たせることも可能である。
【００６４】
本発明は、上記説明においては、該発明の原理と実用が可能な限りわかり易いように説明された。しかしながら、本発明は、適宜な変更によって、数多くの実施形態、並びに、組み合わせで実施可能なことは言うまでもない。

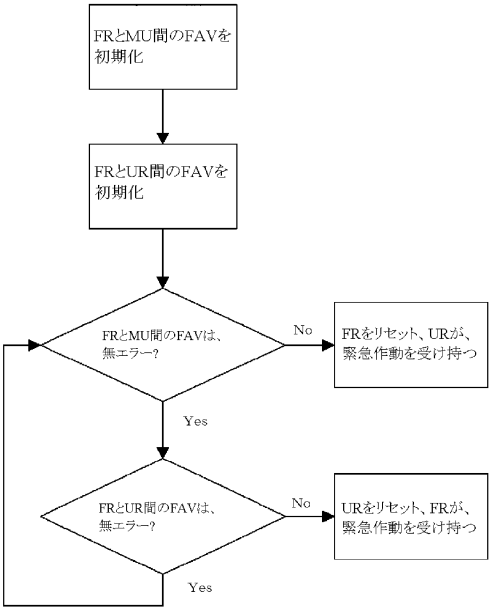
【図１】


MU
FAV
FR
FAV
UR
SV1
SV2
WD

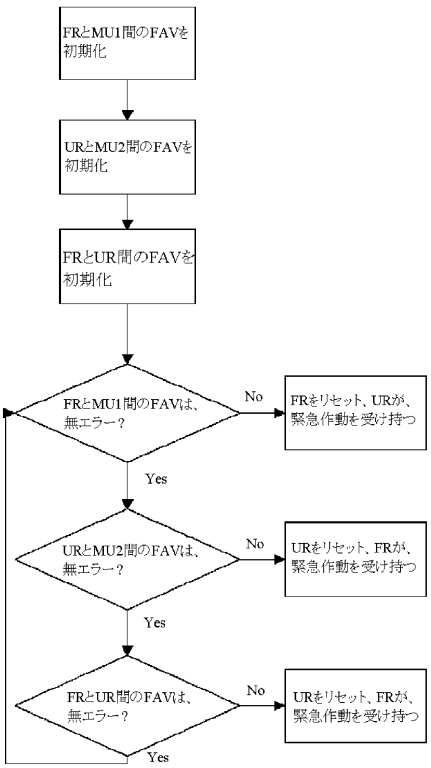
【図２】


MU1
MU2
FAV
FAV
FR
FAV
UR
SV1
SV2
WD

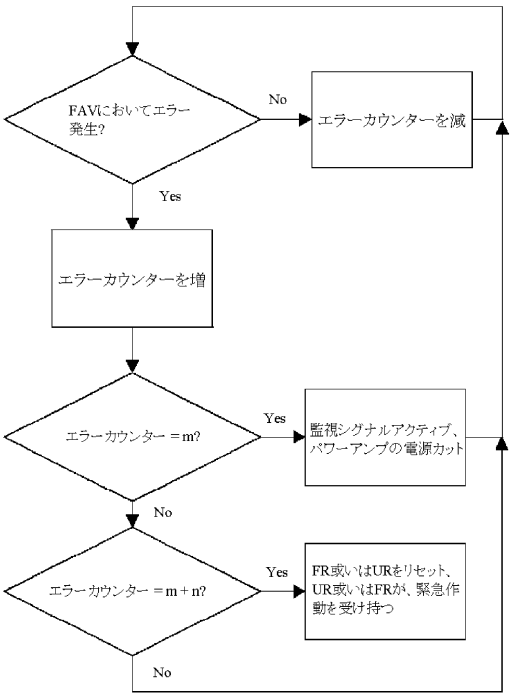
【図３】


FRとMU間のFAVを初期化
FRとUR間のFAVを初期化
FRとMU間のFAVは、無エラー?
No
FRをリセット、URが、緊急作動を受け持つ
Yes
FRとUR間のFAVは、無エラー?
No
URをリセット、FRが、緊急作動を受け持つ
Yes

【図４】


FRとMU1間のFAVを初期化
URとMU2間のFAVを初期化
FRとUR間のFAVを初期化
FRとMU1間のFAVは、無エラー?
No
FRをリセット、URが、緊急作動を受け持つ
Yes
URとMU2間のFAVは、無エラー?
No
URをリセット、FRが、緊急作動を受け持つ
Yes
FRとUR間のFAVは、無エラー?
No
URをリセット、FRが、緊急作動を受け持つ
Yes

【図５】


FAVにおいてエラー発生?
No
エラーカウンターを減
Yes
エラーカウンターを増
エラーカウンター＝m?
Yes
監視シグナルアクティブ、パワーアンプの電源カット
No
エラーカウンター＝m＋n?
Yes
FR或いはURをリセット、UR或いはFRが、緊急作動を受け持つ
No

フロントページの続き

(74)代理人 100157440
弁理士 今村 良太
(74)代理人 100173521
弁理士 篠原 淳司
(74)代理人 100153419
弁理士 清田 栄章
(72)発明者 ネーゲレ・フォルカー
ドイツ連邦共和国、７８１４１ シェーンヴァルト、ブールーアハルトーストラーセ、４
(72)発明者 ペヒトルト・ミヒャエル
ドイツ連邦共和国、９０７６５ フュルト、カールーハウプトマンーストラーセ、７８

審査官 稲垣 浩司

(56)参考文献 米国特許出願公開第２００５／００４４２１４（ＵＳ，Ａ１）
特開平０５－２７４１６６（ＪＰ，Ａ）
特開２０００－１０４５６７（ＪＰ，Ａ）
特開２００２－３５１７００（ＪＰ，Ａ）
米国特許出願公開第２００５／００３３５５８（ＵＳ，Ａ１）
特開２００９－１４９２０８（ＪＰ，Ａ）
特開２００８－３０５３１７（ＪＰ，Ａ）
特開平０５－０８８９２４（ＪＰ，Ａ）
独国特許出願公開第０４４３８７１４（ＤＥ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０５Ｂ ９／０３