(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2009-541636
(P2009-541636A)
(43)公表日　平成21年11月26日(2009.11.26)

(51)Int.Cl.		F I			テーマコード（参考）
F02D 45/00	(2006.01)	F02D	45/00	374C	3G384
		F02D	45/00	374Z	

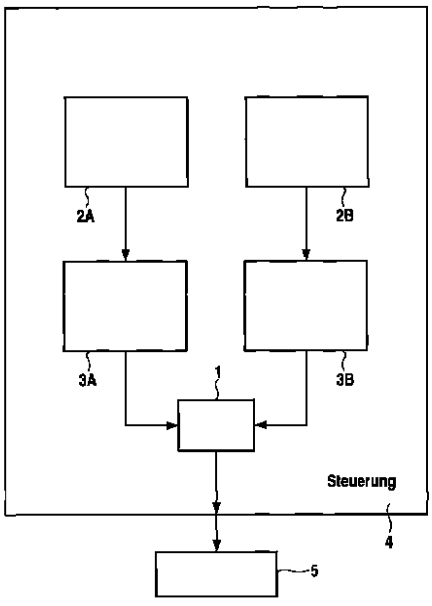
審査請求 有　予備審査請求 未請求　（全 18 頁）

(21)出願番号	特願2009-515899 (P2009-515899)
(86)(22)出願日	平成19年9月19日 (2007.9.19)
(85)翻訳文提出日	平成20年12月22日 (2008.12.22)
(86)国際出願番号	PCT/EP2007/059904
(87)国際公開番号	WO2008/043650
(87)国際公開日	平成20年4月17日 (2008.4.17)
(31)優先権主張番号	102006048169.0
(32)優先日	平成18年10月10日 (2006.10.10)
(33)優先権主張国	ドイツ(DE)

(71)出願人　501125231
ローベルト　ボッシュ　ゲゼルシャフト　ミット　ベシュレンクテル　ハフツング
ドイツ連邦共和国　７０４４２　シュトゥットガルト　ポストファッハ　３０　０２２０
(74)代理人　100095957
弁理士　亀谷　美明
(74)代理人　100096389
弁理士　金本　哲男
(74)代理人　100101557
弁理士　萩原　康司
(72)発明者　ミュラー、ベルント
ドイツ連邦共和国　７０８３９　ゲルリンゲン　シュターラーシュトラーセ　３８
最終頁に続く

(54)【発明の名称】内燃機関のエンジン制御部の機能を監視するための方法および装置

(57)【要約】
本発明は、複数の実行ユニット（２Ａ、２Ｂ）を有する、内燃機関のエンジン制御部の機能を監視する方法を創出する。その際、トルク監視プログラムが、比較駆動モード（ＶＭ）においてシステムの複数の実行ユニット（２）で実行され、監視プログラムの実行時に複数の実行ユニット（２）により出力された信号が、エラー検出のために互いに比較される。
【選択図】図３



4 Controller

【特許請求の範囲】
【請求項１】
複数の実行ユニット（２）を有するシステムで駆動する制御部の機能を監視する方法であって、
監視プログラムは、比較駆動モード（ＶＭ）において前記システムの前記複数の実行ユニット（２）で実行され、
前記監視プログラムの実行時にこれらの実行ユニット（２）により出力された信号がエラー検出のために互いに比較される、複数の実行ユニット（２）を有するシステムで駆動する制御部の機能を監視する方法。
【請求項２】
前記監視プログラムは、エンジンにより生成されたトルクを監視するトルク監視プログラムによって形成される、請求項１に記載の方法。
【請求項３】
前記制御部は、エンジン制御部によって形成される、請求項１に記載の方法。
【請求項４】
前記監視プログラムは、前記複数の実行ユニット（２）で同期して実行される、請求項１に記載の方法。
【請求項５】
前記監視プログラムは、前記複数の実行ユニット（２）で同期せずに実行される、請求項１に記載の方法。
【請求項６】
前記システムは、前記監視プログラムの実行後に、パフォーマンス駆動モード（ＰＭ）へと切り替えられ、
前記パフォーマンス駆動モード（ＰＭ）では、前記複数の実行ユニット（２）が異なるプログラムを実行する、請求項１に記載の方法。
【請求項７】
前記パフォーマンス駆動モード（ＰＭ）で実行されるプログラムは、制御を実行する、請求項６に記載の方法。
【請求項８】
前記監視プログラムは周期的に実行される、請求項１に記載の方法。
【請求項９】
前記監視プログラムの実行時に前記複数の実行ユニット（２）により出力される信号が互いに相違している場合に、エラーが前記監視プログラムの実行時に検出される、請求項１に記載の方法。
【請求項１０】
エラー検出の後で、前記監視プログラムの実行の際に、前記制御部（４）により制御されるユニット（５）が停止させられる、請求項９に記載の方法。
【請求項１１】
複数の実行部を有する制御部（４）であって、
監視プログラムが、比較駆動モード（ＶＭ）において複数の実行ユニット（２）で実行され、
前記監視プログラムの実行時に前記複数の実行ユニット（２）により出力された信号が、エラー検出のために互いに比較される、複数の実行部を有する制御部（４）。
【請求項１２】
前記監視プログラムは、エンジンにより生成されたトルクを監視するトルク監視プログラムに相当する、請求項１１に記載の制御部。
【請求項１３】
前記制御部（４）はエンジン制御部に相当する、請求項１１に記載の制御部。
【請求項１４】
前記複数の実行ユニット（２）は、ＣＰＵ、コプロセッサ、デジタル信号プロセッサＤ

ＳＰ、浮動小数点演算装置ＦＰＵ、または演算論理装置ＡＬＵにより形成される、請求項１１に記載の制御部。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、複数の実行ユニットを有するシステムで駆動する制御部の機能を監視するための方法に関する。
【背景技術】
【０００２】
組み込み型システム分野、特に自動車技術または自動化技術では、ハードウェアのエラーが結果的に安全性に関わりうる、複数のアプリケーションまたはアプリケーションプログラムが存在する。従って、このような安全性に関わる帰結を回避するために、または、このような安全性に関わる帰結による作用を低減するために、この種のエラーを検出するための監視措置が採られる。このような監視をほぼ恒久的に必要とするアプリケーションが存在する。他のアプリケーションでは、定期的に、例えば周期的に、または、特定の要求に応じて、他のハードウェア構成要素のデータ処理システムが正確に機能しているかどうかについて検証する監視機能、が使用される。
【０００３】
図１は、エンジン制御分野における従来の監視方法の構成を示している。エンジン制御の場合、燃料が噴射システムによって燃焼室へと噴射される。安全性の観点から、ここで例示されるエンジン制御分野でのアプリケーションは、３つのレベルＥ１、Ｅ２、Ｅ３に構造化される。
【０００４】
噴射制御部のアプリケーションプログラムは、本来行なうべき機能を含む基礎、または基礎レベルＥ１を形成する。噴射制御部は、どれだけの燃料が、厳密にどの時点において燃料室に噴射されるべきかについて決定する。噴射制御部の誤作動の際には、噴射制御部が、過剰にまたは常に、燃焼室に燃料を噴射し、結果的に、車両が極めて強く加速し事故に繋がるケースが発生する可能性がある。従って、従来のシステムでは、レベルＥ１の噴射制御部が正常に機能しているかどうかを監視する、監視レベルＥ２が設けられている。
【０００５】
監視レベルＥ２は、追加的なプログラム、または、場合により追加的なセンサにアクセスする追加的なソフトウェアコードによって形成される。従来のエンジン制御部の場合、監視レベルＥ２は、通常、連続トルク監視部（ｋｏｎｔｉｎｕｉｅｒｌｉｃｈｅ Ｍｏｍｅｎｔｅｎｕｅｂｅｒｗａｃｈｕｎｇ）によって形成される。連続トルク監視部では、エンジンにより目下生成されたトルクが、特定の閾値を超えていないかどうかが監視される。
【０００６】
従来のエンジン制御部の場合、噴射制御レベルＥ１および監視レベルＥ２のプログラムは、同じハードウェア、または同じ実行ユニットで駆動する。噴射制御部のアプリケーションプログラムは、同一実行ユニットまたはＣＰＵのレベルＥ１で駆動し、トルク監視部は、同一実行ユニットまたはＣＰＵのレベルＥ２で駆動するので、実行ユニットでのハードウェアエラーは、噴射制御部と、トルク監視部とが同時に故障することに繋がりうる。従って、安全性の理由から、従来のエンジン制御部では、監視レベルＥ２が正常に機能しているかどうかを検査する、更なる別の安全レベルＥ３が設けられている。
【０００７】
安全レベルＥ３は、実行ユニットと、ＡＳＩＣ等の外部ハードウェア構成要素との、問い合わせ・応答通信を実行する。その際、基本的に、実行ユニットまたはマイクロコントローラの機能、特に、アプリケーションプログラムの機能が、監視レベルＥ２で検査される。監視レベルＥ２のアプリケーションプログラムは、妥当性検査を実行する。

【０００８】
例えば、監視レベルＥ２の監視プログラムは、アクセルペダルの傾斜度αを読み込む。噴射制御レベルＥ１のアプリケーションプログラムにより設定された燃料の量が、感覚的に監視されるアクセルペダルの位置に依存する特定の閾値を超える場合に、レベルＥ２で駆動する監視プログラムが、噴射制御部でエラーが発生していることを検知し、通常では、安全面の理由からエンジンの停止を促す。
【０００９】
監視レベルＥ２は、エンジンで生成されたトルクを監視し閾値を超えた際にはエンジンを停止させるトルク監視プログラム等を、追加的に含んでいる。監視機能を実装するために、監視プログラムのコードは、複写されてＥ２’として格納される。その際、Ｅ２’のアルゴリズムまたはプログラムは、デフォルトデータまたはテストデータによって計算される。例えばＡＳＩＣ、すなわち、特定用途向け集積回路において駆動する安全レベルＥ３のプログラムは、実行ユニットまたはＣＰＵへの問い合わせとして、特定のビットマスタを割り当てる。実行ユニットまたはＣＰＵは、レベルＥ２’に基づいてデフォルト値によって、複写に含まれる監視プログラムを計算し、特定用途向け集積回路ＡＳＩＣ内のレベルＥ３の安全プログラムに対して、応答ビットマスタを出力する。安全プログラムは、ＣＰＵ内の監視プログラムが正常に機能しているかどうかを確認するために、応答ビットマスタと基準ビットマスタとを比較する。特定用途向け集積回路内の安全プログラムは、実行ユニットまたはＣＰＵで駆動する監視プログラムとは異なるハードウェア、すなわちＡＳＩＣにおいて駆動する。従って、この従来の処理手順は、ＣＰＵ内でのハードウェアエラーに対して、ある程度の安全を確保する。
【００１０】
いずれにせよ、図１で示すような従来の安全コンセプトの短所として、デフォルト値またはテスト値によって計算する命令テストのための監視プログラムが、複写に存在する必要がある、ということが挙げられる。従って、複写されたプログラム命令を格納するための記憶位置が、監視レベルＥ２’で必要である。
【００１１】
デフォルトデータまたはテストデータが、複写された監視プログラムＥ２’のための入力データとして役目を果たす、従来の命令テストの更なる別の短所は、オペランドに依存する（Ｏｐｅｒａｎｄｅｎ－ａｂｈａｅｎｇｉｇ）エラーが検出されないことにある。
【発明の開示】
【発明が解決しようとする課題】
【００１２】
従って、本発明の課題は、オペランドに依存するエラーも検出する、制御部の機能を監視する方法を創出することにある。
【課題を解決するための手段】
【００１３】
本発明は、複数の実行ユニットを有するシステムで駆動する制御部の機能を監視する方法であって、監視プログラムは、比較駆動モードＶＭにおいてシステムの複数の実行ユニットで実行され、監視プログラムの実行時にこれらの実行ユニットにより出力された信号が、エラー検出のために互いに比較される、複数の実行ユニットを有するシステムで駆動する制御部の機能を監視する方法を創出する。
【００１４】
本発明に基づく方法の利点は、監視プログラムの複写されたプログラム命令のために、記憶位置を無駄に使用しないことにある。
【００１５】
本発明に基づく方法の実施形態において、監視プログラムは、エンジンにより生成されたトルクを監視するトルク監視プログラムによって形成される。
【００１６】
本発明に基づく方法の実施形態において、制御部は、エンジン制御部によって形成され

る。
【００１７】
本発明に基づく方法の実施形態において、監視プログラムは、複数の実行ユニットで同期して実行される。
【００１８】
本発明に基づく方法の代替的な実施形態において、複数の実行ユニットで同期せずに実行される。
【００１９】
本発明に基づく方法の実施形態において、システムは、監視プログラムの実行後に、パフォーマンス駆動モードへと切り替えられ、パフォーマンス駆動モードでは、複数の実行ユニットが異なるプログラムを実行する。
【００２０】
本発明に基づく方法の実施形態において、パフォーマンス駆動モードで実行されるプログラムは、制御を実行する。
【００２１】
本発明に基づく方法の実施形態において、監視プログラムは周期的に実行される。
【００２２】
本発明に基づく方法の実施形態において、監視プログラムの実行時に複数の実行ユニットにより出力される信号が互いに相違している場合に、エラーが監視プログラムの実行時に検出される。
【００２３】
本発明に基づく方法の実施形態において、エラー検出の後で、監視プログラムの実行の際に、制御部により制御されるユニットが停止させられる。
【００２４】
さらに、本発明は、複数の実行部を有する制御部であって、監視プログラムが、比較駆動モードＶＭにおいて複数の実行ユニットで実行され、監視プログラムの実行時に複数の実行ユニットにより出力された信号が、エラー検出のために互いに比較される、複数の実行部を有する制御部を創出する。
【００２５】
本発明に基づく制御部の実施形態において、監視プログラムは、エンジンにより生成されたトルクを監視するトルク監視プログラムに相当する。
【００２６】
本発明に基づく制御部の実施形態において、制御部はエンジン制御部に相当する。
【００２７】
本発明に基づく制御部の実施形態において、複数の実行ユニットは、マイクロプロセッサ、コプロセッサ、デジタル信号プロセッサＤＳＰ、浮動小数点演算装置ＦＰＵ、または、演算論理装置ＡＬＵにより形成される。
【発明を実施するための最良の形態】
【００２８】
以下では、本発明の一実施形態に基づく方法、および、本発明の一実施形態に基づく制御部の好適な実施形態が、添付された図を参照しながら、本発明の本質的な特徴を解説するために記載される。
【００２９】
図２から分かるように、切り替えおよび比較回路１は、入力側で、Ｎ＋１個の実行ユニット２に接続されており、実行ユニット２－ｉから論理入力信号E_0、E_1、E_2、E_3・・・E_Nを獲得する。切り替えおよび比較ユニット１は、比較ロジック部１Ａと、切り替えロジック部１Ｂとを含んでいる。
【００３０】
図２に示すシステムは、少なくとも２つの駆動モードで駆動可能である。パフォーマンス駆動モードとも呼ばれる性能向上のための第１駆動モードにおいて、実行ユニット２－

ｉまたはコアは、異なるプログラムまたはタスクを並列処理する。実行ユニット２－ｉにおいては、計算命令を実行するための任意の実行ユニット２－ｉ、すなわち、例えば、プロセッサ、浮動小数点演算装置ＦＰＵ、デジタル信号プロセッサＤＳＰ、コプロセッサ、または、演算論理装置ＡＬＵが関わっている。

【００３１】

パフォーマンスモードＰＭにおける、異なる実行ユニット２－ｉによるプログラムの実行は、同期して、または同期せずに、行なわれることが可能である。パフォーマンスモードでは、冗長な処理は行なわれず、実行ユニット２－ｉは、異なる計算またはプログラムを並行して実行する。純粋なパフォーマンス駆動モードＰＭにおいて、全入力信号$Ｅ_{i}$が対応する出力信号$Ａ_{i}$へと切り替えられるか、または導かれる。

【００３２】

スーパースケーラ型（ｓｕｐｅｒｓｋａｌａｒ）演算システムの使用に並ぶ、マルチコア・アーキテクチャの第２の根拠は、複数の実行ユニット２－ｉが同一のプログラムを冗長に実行することによって、信号処理の安全性を高めることにある。安全モードもしくはセーフティモード、または比較モードＶＭとも呼ばれるこの第２の駆動モードでは、実行ユニットの演算結果または論理出力信号が、切り替えおよび比較回路１によって互いに比較される。従って、発生したエラー、または信号の相違が、一致を確かめる比較によって検出可能である。従って、純粋な比較駆動モードＶＭにおいては、全入力信号$Ｅ_{i}$が、厳密に１つの出力信号$Ａ_{i}$へと導かれるか、またはマッピングされる（ａｂｂｉｌｄｅｎ）。混合形態も可能である。

【００３３】

構成可能な切り替えロジック部１Ｂでは、いくつの出力端子または出力信号$Ａ_{i}$が設けられているのかについて示される。さらに、切り替えロジック部１Ａには、どの入力信号$Ｅ_{i}$がどの出力信号$Ａ_{i}$に作用するのかについて格納される。従って、切り替えロジック部１Ｂには、異なる出力信号$Ａ_{i}$に入力信号$Ｅ_{i}$を割り当てるマッピング関数（Ａｂｂｉｌｄｕｎｇｓｆｕｎｋｔｉｏｎ）が格納されている。

【００３４】

処理ロジック部１Ａは、各出力信号$Ａ_{i}$について、どのような形態で入力信号が各出力信号に作用するのかについて定める。例えば、出力信号$Ａ_{0}$は、入力信号$Ｅ_{1}$、・・・、$Ｅ_{n}$によって生成される。これは、ｍ＝１ならば、単純に、入力信号のインターコネクション（Ｄｕｒｃｈｓｃｈａｌｔｕｎｇ）に相当する。Ｍ＝２ならば、２つの入力信号$Ｅ_{1}$、$Ｅ_{2}$が互いに比較される。この比較は、同期して、または同期せずに、回路１によって実行される。その際、比較はビットごとに行なわれるか、または代替的に、有意なビットのみ互いに比較される。

【００３５】

Ｍ≧３ならば、様々な可能性がある。第１の可能性としては、全信号が互いに比較され、少なくとも２つの異なる値が存在する場合に、エラーが検出される。エラーは、任意選択で、切り替えおよび比較回路１により信号で知らされる。

【００３６】

更なる別の可能性は、Ｋ＞Ｍ／２ならば、ｍ個からＫ個を選択することにある。これは、実施形態において、比較器を設けることによって実現される。その際、複数の入力信号のうちの１つが、他の入力信号とは相違しているとして検知された場合に、任意選択で第１エラー信号が生成される。第１エラー信号とは別の、第２エラー信号が発生した場合には、全３つの入力信号が互いに相違している可能性がある。

【００３７】

更なる別の実施形態において、入力信号値は、更なる別の演算ユニットへと供給される。演算ユニットは、例えば、平均値もしくは中央値を計算する、または、フォールトトレラントなアルゴリズムＦＴＡを実行する。フォールトトレラントなアルゴリズムの場合、入力信号の極値が排除されるか、または無視され、残りの信号値の平均化が行なわれる。実施形態において、残りの信号の集合全体の平均化が行なわれるか、代替的な実施形態に

おいては、残りの信号値の、ハードウェア内で容易に形成される部分集合の平均化が行なわれる。平均値形成の際には、加算または除算が行なわれる必要がある一方、ＦＴＭ、ＦＴＡまたは中央値形成の際には、入力信号値の選別が部分的に必要である。実施形態において、信号の相違、または極値が十分に大きい場合には、任意選択でエラー信号が出力されるか、または示される。１つの信号へと信号処理するための上述の様々な可能性は、比較動作に相当する。

【００３８】

処理ロジック部１Ａは、各出力信号A_iおよび入力信号E_iについて、行なわれるべき比較演算の厳密な形態を定める。切り替えロジック部１Ｂ内での情報の組み合わせ、すなわち、出力信号または関数値ごとに処理ロジック部１Ａで定められる比較演算の割り当て関数は、駆動モード情報に相当し、駆動モードを設定する。この情報は、通常多価であり、１より多い論理ビットにより示される。ただ２つの実行ユニットが設けられており、従ってただ１つ比較モードが存在する場合には、駆動モードの全情報を、１つの論理ビットで補償ことが可能である。

【００３９】

パフォーマンスモードＰＭから比較モードＶＭへの切り替えは、パフォーマンスモードＰＭでは、様々な信号出力部へとマッピングされるか、または、インターコネクトされている（ｄｕｒｃｈｓｃｈａｌｔｅｎ）実行ユニット２－ｉが、比較モードＶＭでは、同じ信号出力部へとマッピングされるか、もしくはスルー接続されることによって、一般的に行なわれる。このことは、特に、実行ユニット２－ｉの部分集合が設けられることによって、実現される。その際、パフォーマンス駆動モードＰＭでは、部分集合として考えるべき全入力信号E_iが、対応する出力信号A_iへと直接的に切り替えられる。一方、比較モードＶＭでは、全入力信号が１つの信号出力部へとマッピングされるか、または１つの信号出力部へとインターコネクトされる。代替的に、切り替えは、組み合わせが変更されることによって実現可能である。

【００４０】

駆動モードは、ソフトウェアを介して制御されて、駆動中に動的に切り替えられることが可能である。実施形態において、切り替えは、特別な切り替え命令、特別な命令シーケンス、および、明示的にラベル付けされた命令、の実行を介して、または、システムの少なくとも１つの実行ユニット２－ｉによる特定のアドレスに対するアクセスによって、引き起こされる。

【００４１】

冗長的な実行および検査が行なわれるセーフティモードＶＭと、異なるプログラム駆動により性能向上を達成するパフォーマンスモードＰＭとの間での切り替えは、切り替え装置１によって行なわれる。実施形態において、切り替えのために、プログラム、アプリケーションプログラム、プログラム部分、またはプログラム命令への、識別子によるラベル付けが行なわれる。識別子によって、これらのプログラム命令が安全性に関わるかどうかが検知可能である。すなわち、安全駆動モードもしくは比較駆動モードＶＭで実行される必要があるかどうか、または、パフォーマンス駆動モードＰＭが利用できるかどうか、について検知することが可能である。ラベル付けは、１ビットによってプログラム命令内で行なわれうる。代替的に、特別なプログラム命令によって、後続のシーケンスをラベル付けすることが可能である。

【００４２】

安全駆動モードまたはセーフティモードＶＭでは、異なる実行ユニット２－ｉで同期して実行する際に、実行ユニット２－ｉの演算結果または出力信号の計算に同じ時間が掛かる。演算結果は、安全駆動モードＶＭでは、同期実行において切り替え装置１に同時に提供される。演算結果が一致する場合には、対応するデータが利用可能になる。信号が不一致の際には、所定のエラー対応が行なわれる。

【００４３】

システムがパフォーマンス駆動モードＰＭにある場合には、プログラムが並行して実行

され、切り替えおよび比較回路１内の比較器は駆動されない。

【００４４】

複数の実行ユニット２を有するシステムで駆動する制御部の機能を監視するための、本発明の一実施形態に基づく方法において、少なくとも１つの監視プログラムが、比較駆動モードＶＭにおいて、システムの複数の実行ユニットまたは全実行ユニットで実行される。監視プログラムの実行時にこれらの実行ユニット２により出力される信号は、エラー検出のために、互いに比較される。本発明の一実施形態に基づく制御部の好適な実施形態において、制御部は、少なくとも３つの実行ユニット２を有する。残りの信号とは最も大きく相違している信号が、例えば多数決によって、誤りがあるとして検知される。実施形態において、信号は、デジタル論理信号、特に二値信号が関わっている。本発明の一実施形態に基づく制御部４において、好適な実施形態において、内燃機関を制御するためのエンジン制御部が関わっている。代替的な実施形態において、制御部４は、電動機を駆動するための制御部に相当する。監視プログラムは、例えば、内燃機関または電動機により生成されるトルクを監視する、トルク監視プログラムによって形成される。その際、監視プログラムは、同期して、または同期せずに、複数の実行ユニット２で実行可能である。

【００４５】

本発明に基づく方法において、エンジン制御のための通常のアプリケーションプログラムが、パフォーマンス駆動モードＰＭにおいて実行される。すなわち、システムの各実行ユニット２は、性能向上のために、制御のためのプログラムを実行する。一方、他の実行ユニット２は、それ（制御のためのプログラム）とは異なるアプリケーションプログラムを実行する。レベルＥ２で駆動する監視プログラムは、本発明の一実施形態に基づく方法の可能な実施形態において、周期的に呼び出される。本発明の一実施形態に基づく方法において、監視プログラムは、比較駆動モードＶＭにおいて、システムの複数の実行ユニット２で実行される。比較駆動モードＶＭでは、システムの複数の実行ユニット２、または全実行ユニット２は、同じ監視プログラムを実行する。その際生成される出力信号は、エラー検出のために互いに比較される。可能な実施形態において、例えば、すべて周期的に呼び出される複数の監視プログラムが、レベルＥ２で実行される。呼び出された全監視プログラムは、比較駆動モードＶＭで実行される。代替的な実施形態において、監視プログラムは、特定の要請または要請命令に応じて呼び出され、引き続いて比較駆動モードＶＭにおいて、システムの複数の実行ユニット２または少なくとも２つの実行ユニットによって実行される。監視プログラムを実行するためのこの種の要請命令は、例えば割込みによって起動される。

【００４６】

監視プログラムの実行後に、システムは、パフォーマンス駆動モードＰＭへと戻して切り替えられる。パフォーマンス駆動モードＰＭでは、実行ユニット２が、特に第１レベルＥ１の異なるプログラム、例えば制御プログラムを実行する。

【００４７】

本発明の一実施形態に基づく方法の実施形態において、監視プログラムの実行時に比較駆動モードＶＭで実行ユニット２により出力された信号が互いに相違している場合に、監視プログラムの実行時に、エラーがレベルＥ２で検出される。その際、特に、エラーが検出された後で、監視プログラムの実行の際に、制御部４により制御されるユニット５、例えばエンジンが停止させられる。

【００４８】

図３は、本発明の一実施形態に基づく制御システムの可能な実施形態の構成図を示している。図３で示される実施形態において、本発明の一実施形態に基づく制御部４は、２つの実行ユニット２Ａ、２Ｂを有する。実行ユニット２Ａ、２Ｂにおいては、完全なマイクロプロセッサまたはＣＰＵ、コプロセッサ、デジタル信号プロセッサＤＳＰ、浮動小数点演算装置ＦＰＵ、または演算論理装置ＡＬＵが関わっている。本発明の一実施形態に基づく制御部４の更なる別の実施形態において、２より多い実行ユニット２が設けられている。図３に示す簡単な実施形態において、実行ユニット２Ａ、２Ｂにより生成される信号は

それぞれ、一時記憶装置３Ａ、３Ｂに一時格納される。各実行ユニット２は、特に、出力側に自身の一時格納装置３を有している。一時格納された、実行ユニット２の演算結果または出力信号は、比較ユニット１に供給される。比較ユニット１は、例えば、図２に示すように、切り替えおよび比較回路１によって形成可能である。一時格納された出力信号の比較は、対応する比較プログラムまたは比較ソフトウェアの動作によって実行されるか、または、ハードウェアに組み込まれて実行される。

【００４９】

図４は、本発明の一実施形態に基づく、制御部の機能を監視する方法の可能な実施形態のフローチャートを示している。

【００５０】

第２レベルＥ２で監視プログラムが呼び出された後で、工程Ｓ１では、パフォーマンスモードＰＭから比較駆動モードＶＭへのシステムの切り替えが行なわれる。引き続いて、図３に示すように、両実行ユニット２Ａ、２Ｂは、同一の監視プログラムを実行するために工程Ｓ２、Ｓ３で作動され、トルク監視プログラム等の同一の監視プログラムを実行する。図４に示される実施形態の場合、両実行ユニット２Ａ、２Ｂは、工程Ｓ２、Ｓ３において、同期せずに、対応する演算結果信号を計算する。演算結果信号は、工程Ｓ４、Ｓ５において、各一時記憶装置３Ａ、３Ｂに一時格納される。代替的な実施形態において、両実行ユニット２Ａ、２Ｂは、工程Ｓ２、Ｓ３において、各出力信号または演算結果値を互いに同期して計算する。２つの演算結果値または出力信号が提示された後に、工程Ｓ６において、特に切り替えおよび比較回路１によって、両出力信号の間での比較が実行される。両信号が互いに相違している場合にはエラーが検出され、引き続いて対応するエラー処理が行なわれる。安全性に関わるアプリケーションの場合、制御部４により駆動されるユニット５、例えばエンジンが、停止させられる。工程Ｓ６における比較は、引き続いて一時記憶装置３Ａ、３Ｂを読み出した後に、ソフトウェアごとの対応する比較演算によって実行される。または、代替的な実施形態において、組み込まれた回路による比較が行なわれる。

【００５１】

図５は、本発明の一実施形態に基づく方法の可能な実施形態を解説するための時間フローチャートを示している。本実施形態において、監視プログラムがレベルＥ２で周期的に呼び出され、比較駆動モードＶＭにおいて複数の実行ユニット２により同時に実行される。監視プログラムの実行後に、システムは、パフォーマンス駆動モードＰＭに戻り、レベルＥ１で本来の制御プログラムを実行する。

【００５２】

本発明の一実施形態に基づく制御部４の代替的な実施形態において、制御部４は、常にパフォーマンス駆動モードＰＭで稼動する。その際、監視プログラムは、少なくとも２つの実行ユニット２により、同期せずに計算される。実行ユニットによりその際出力される演算結果または出力信号は、その際、エラー検出のために互いに比較される。いずれにせよ、本実施形態では、演算結果がそれぞれ一時格納される必要があり、演算結果は、引き続いて２回互いに比較される。すなわち、両実行ユニット２の可能なハードウェアエラーに考慮するために、第１実行ユニット２Ａで一回、さらに、第２実行ユニット２Ｂで一回比較される。従って、この実施形態は、比較駆動モードＶＭで監視プログラムを実行する実施形態よりもコストが掛かる。

【００５３】

本発明の一実施形態に基づく方法は、オペランドに依存するエラーの検出も許容する。さらに、本発明の一実施形態に基づく方法によって、図１に示す従来の安全コンセプトに比較して、記憶位置が明らかに節約される。

【００５４】

本発明の一実施形態に基づく制御部４の可能な実施形態において、制御部４は、少なくとも３つの実行ユニット２を有する。その際、信号が不一致である場合に、多数決によって、どの実行ユニット２が誤って駆動している可能性があるのか、確認可能である。引き

続いて、この誤って駆動している可能性がある実行ユニット２は、この誤って駆動している可能性がある実行ユニットが実際に故障しているのかどうかを確認するために、特に、セルフテストを実行する。実施形態において、実行ユニット２が実際に故障していることがセルフテストによって判明した場合に、実行ユニット２は停止させられる。従って、本実施形態において、システムはフォールトトレラントである。

【００５５】

両コアまたは実行ユニット２において、例えば製造欠陥により生じる恒常的なエラーに対して防護するために、本発明の一実施形態に基づく方法の可能な実施形態において、実行ユニット２のセルフテストがそれぞれ行なわれる。

【００５６】

本発明の一実施形態に基づく方法の可能な実施形態において、比較駆動モードＶＭでは、監視プログラムがレベルＥ２で実行される。その際、更なる別の防護のために、安全レベルＥ３が追加的に設けられている。レベルＥ３は、さらに、監視プログラムの機能を監視するための命令テストを実行する。この種の実施形態は、特に安全性に関わるアプリケーションにおいて可能である。

【図面の簡単な説明】

【００５７】

【図１】３つのレベルを有する従来の安全コンセプトを記載するための図を示す。

【図２】本発明の一実施形態に基づく方法において使用される、切り替えおよび比較ユニットの構成図を示す。

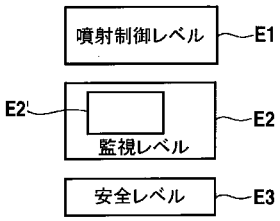
【図３】本発明の一実施形態に基づく制御部の可能な実施形態を記載するための構成図を示す。

【図４】本発明の一実施形態に基づく方法を解説するためのフローチャートを示す。

【図５】本発明の一実施形態に基づく方法の可能な実施形態を解説するための時間フローチャートを示す。

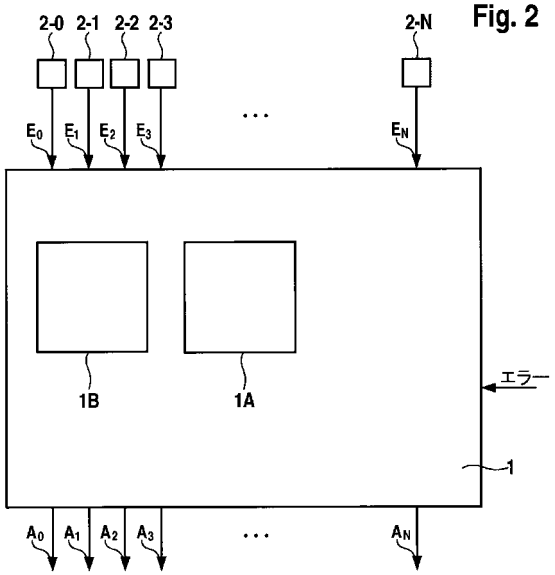
【図１】

Fig. 1



【図２】

Fig. 2



【図３】

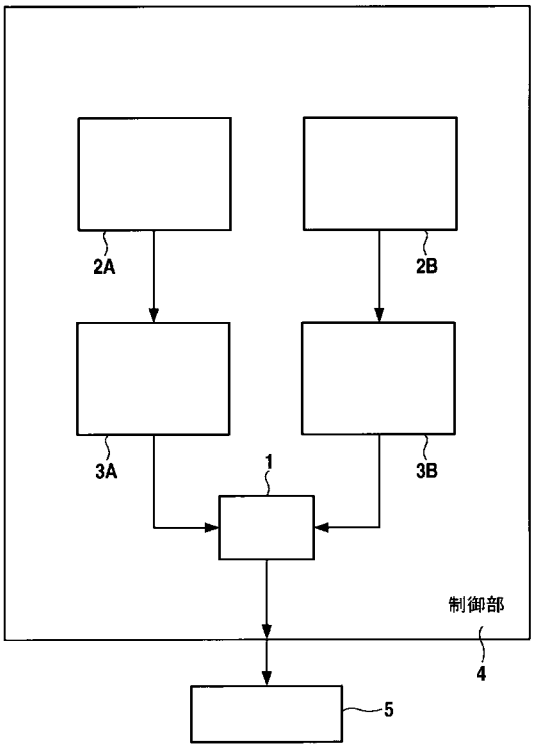
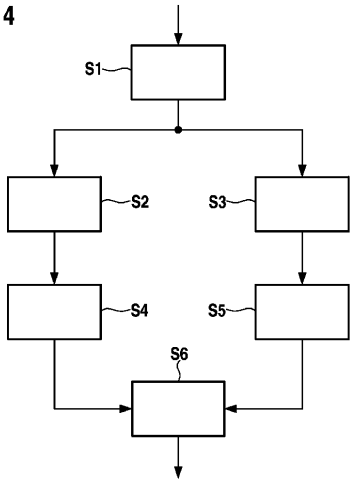


Fig. 3

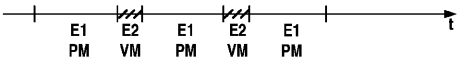
【図４】

Fig. 4



【図５】

Fig. 5



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2007/059904

A. CLASSIFICATION OF SUBJECT MATTER
INV. F02D41/22

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)
F02D

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 705 286 B1 (LIGHT DENNIS A [US] ET AL) 16 March 2004 (2004-03-16) paragraph [0005]	1-14
X	DE 199 28 477 A1 (BOSCH GMBH ROBERT [DE]) 28 December 2000 (2000-12-28) column 1, line 48 - line 63	1-14
X	DE 199 00 740 A1 (BOSCH GMBH ROBERT [DE]) 13 July 2000 (2000-07-13) column 2, line 25 - line 43	1-14
X	US 5 601 063 A (OHASHI HIDEYUKI [JP] ET AL) 11 February 1997 (1997-02-11) column 1, line 36 - line 43	1-14

-/--

[X] Further documents are listed in the continuation of Box C. [X] See patent family 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
18 Januar 2008	06/02/2008

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	Jackson, Stephen

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2007/059904

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 10 2006 003425 A1 (DENSO CORP [JP]; NIPPON SOKEN [JP]) 31 August 2006 (2006-08-31) paragraphs [0018], [0019]	1-14
A	US 6 305 347 B1 (RUSSELL JOHN DAVID [US]) 23 October 2001 (2001-10-23) the whole document	1-14

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2007/059904

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6705286 B1	16-03-2004	US 2004055568 A1	25-03-2004
DE 19928477 A1	28-12-2000	IT MI20001319 A1	13-12-2001
		JP 2001020803 A	23-01-2001
		US 6368248 B1	09-04-2002
DE 19900740 A1	13-07-2000	WO 0042307 A1	20-07-2000
		EP 1062417 A1	27-12-2000
		JP 2002535533 T	22-10-2002
		RU 2239078 C2	27-10-2004
		US 6386180 B1	14-05-2002
US 5601063 A	11-02-1997	JP 8270488 A	15-10-1996
DE 102006003425 A1	31-08-2006	KR 20060086874 A	01-08-2006
		US 2006192533 A1	31-08-2006
US 6305347 B1	23-10-2001	DE 10105507 A1	25-10-2001

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2007/059904

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. F02D41/22

Nach der internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
F02D

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 6 705 286 B1 (LIGHT DENNIS A [US] ET AL) 16. März 2004 (2004-03-16) Absatz [0005]	1-14
X	DE 199 28 477 A1 (BOSCH GMBH ROBERT [DE]) 28. Dezember 2000 (2000-12-28) Spalte 1, Zeile 48 - Zeile 63	1-14
X	DE 199 00 740 A1 (BOSCH GMBH ROBERT [DE]) 13. Juli 2000 (2000-07-13) Spalte 2, Zeile 25 - Zeile 43	1-14
X	US 5 601 063 A (OHASHI HIDEYUKI [JP] ET AL) 11. Februar 1997 (1997-02-11) Spalte 1, Zeile 36 - Zeile 43	1-14

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen [X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
18. Januar 2008	06/02/2008

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Jackson, Stephen

Formblatt PCT/ISA/210 (Blatt 2) (April 2005)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2007/059904

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	DE 10 2006 003425 A1 (DENSO CORP [JP]; NIPPON SOKEN [JP]) 31. August 2006 (2006-08-31) Absätze [0018], [0019] ---	1-14
A	US 6 305 347 B1 (RUSSELL JOHN DAVID [US]) 23. Oktober 2001 (2001-10-23) das ganze Dokument ---	1-14

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2007/059904

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 6705286 B1	16-03-2004	US 2004055568 A1	25-03-2004
DE 19928477 A1	28-12-2000	IT MI20001319 A1	13-12-2001
		JP 2001020803 A	23-01-2001
		US 6368248 B1	09-04-2002
DE 19900740 A1	13-07-2000	WO 0042307 A1	20-07-2000
		EP 1062417 A1	27-12-2000
		JP 2002535533 T	22-10-2002
		RU 2239078 C2	27-10-2004
		US 6386180 B1	14-05-2002
US 5601063 A	11-02-1997	JP 8270488 A	15-10-1996
DE 102006003425 A1	31-08-2006	KR 20060086874 A	01-08-2006
		US 2006192533 A1	31-08-2006
US 6305347 B1	23-10-2001	DE 10105507 A1	25-10-2001

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,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,IS,IT,LT,LU,LV,MC,MT,NL,PL,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,BH,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,SV,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

(72)発明者 ピツァール、フォルカー
ドイツ連邦共和国 ７３５５０ ヴァルトシュテッテン／ヴィスゴルディンゲン ウーラントシュトラーセ ２１
(72)発明者 グメーリヒ、ライナー
ドイツ連邦共和国 ７１２５４ ディッチンゲン ヘーエンヴェーク ２

Ｆターム(参考) 3G384 BA11 CA25 DA42 DA47 EB08 EC05 ED07 EE02 EE03