(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3958365号
(P3958365)
(45)発行日　平成19年8月15日(2007.8.15)　(24)登録日　平成19年5月18日(2007.5.18)

(51)Int.Cl.　F I
G06F 11/18 (2006.01)　G06F 11/18 310C

請求項の数 7 (全 7 頁)

(21)出願番号　特願平9-508049
(86)(22)出願日　平成8年6月20日(1996.6.20)
(65)公表番号　特表平11-510925
(43)公表日　平成11年9月21日(1999.9.21)
(86)国際出願番号　PCT/EP1996/002688
(87)国際公開番号　WO1997/006487
(87)国際公開日　平成9年2月20日(1997.2.20)
審査請求日　平成15年6月18日(2003.6.18)
(31)優先権主張番号　19529434.3
(32)優先日　平成7年8月10日(1995.8.10)
(33)優先権主張国　ドイツ(DE)

(73)特許権者
イーテーテー・アウトモティーフェ・オイローペ・ゲゼルシャフト・ミト・ベシュレンクテル・ハフツング
ドイツ連邦共和国、Ｄ－６０４８８　フランクフルト・アム・マイン、ゲーリケストラーセ、７
(74)代理人
弁理士　江崎　光史
(74)代理人
弁理士　三原　恒男
(74)代理人
弁理士　奥村　義道

最終頁に続く

(54)【発明の名称】安全上重要な制御装置のためのマイクロプロセッサ装置

(57)【特許請求の範囲】

【請求項１】

同じ入力情報を受けて同じプログラムを処理する、同期的に動作する２個の中央ユニットまたはＣＰＵと、読出し専用メモリ（ＲＯＭ）および随時書込み読出しメモリ（ＲＡＭ）と、前記中央ユニットまたはＣＰＵの出力データまたは出力信号をチェックし、不一致のときに切断信号を発生する比較器と、前記中央ユニット若しくはＣＰＵ又は前記比較器内に格納されているテストデータ発生器とを備えた、安全上重要な制御装置のためのマイクロプロセッサ装置において、

前記の一方の中央ユニットまたはＣＰＵ（１）は、第１バスシステム（３）を介して読出専用メモリ（５）および随時書込み読出しメモリ（６）並びに入力ユニット（７，８）および出力ユニット（９）に接続され、

前記の他方の中央ユニットまたはＣＰＵ（２）は、第２バスシステム（４）を介して少なくとも１つの随時書込み読出しメモリ（１１）及び前記第１バスシステム（３）の前記両メモリ（５，６）より小容量であるパリティ又はテストデータ用のパリティ読出専用メモリ（１０）並びに入力ユニット（１２，１３）および出力ユニット（１４）に接続され、

この場合、前記第１バスシステム（３）のデータのためのパリティ又はテストデータが、第２バスシステム（４）のパリティ読出専用メモリ（１０）に記憶されていて、

これらの中央ユニットまたはＣＰＵ（１，２）はそれぞれ、各バスシステム（３，４）を介して、各読出専用メモリ（５，１０）および各随時書込み読出しメモリ（６，１１）並びに各入力ユニット（７，８；１２，１３）および各出力ユニット（９，１４）に接続さ

れることを特徴とするマイクロプロセッサ装置。
【請求項２】
比較器（１８，１９）が、両バスシステム（３，４）に達する、パリティ又はテストデータと命令を含む両中央ユニットまたはＣＰＵ（１，２）の入力データおよび出力データの一致をチェックすることを特徴とする請求項１に記載のマイクロプロセッサ装置。
【請求項３】
読出し専用メモリ（５）および随時書込み読出しメモリ（６）の記憶場所並びにパリティ読出専用メモリ（１０）及び随時書込み読出しメモリ（１１）の記憶場所は、両バスシステム（３，４）に接続されたこれらのメモリ（５，６，１０，１１）内に割り当てられていることを特徴とする請求項１または２に記載のマイクロプロセッサ装置。
【請求項４】
読出し専用メモリ（５）と随時書込み読出しメモリ（６）は、第１バスシステム（３）に接続され、パリティ読出専用メモリ（１０）及び随時書込み読出しメモリ（１１）は、第２バスシステム（４）に接続されていることを特徴とする請求項３に記載のマイクロプロセッサ装置。
【請求項５】
少なくとも２つの中央ユニットまたはＣＰＵ（１，２）、読出し専用メモリ（５）、随時書込み読出しメモリ（６）、パリティ読出専用メモリ（１０）及び随時書込み読出しメモリ（１１）、中央ユニットまたはＣＰＵから入力されるデータの一緒の読取りを可能にするドライバステージ（１５，１６，１７）及び比較器（１８，１９）は、１個のシングルチップに設けられていること、及び、両バスシステム（３，４）が、前記ドライバステージ（１５，１６，１７）に接続されていることを特徴とする請求項１～４のいずれか１項に記載のマイクロプロセッサ装置。
【請求項６】
両バスシステム（３，４）は、それぞれデータ情報、テスト情報バス（Ｄｐ）、アドレスバス（Ａ）及び制御バス（Ｃ）を備えていることを特徴とする請求項１～５のいずれか１項に記載のマイクロプロセッサ装置。
【請求項７】
両中央ユニットまたはＣＰＵ（１，２）の信号、すなわち両バスシステム（３，４）上の信号が、平行に接続された２個のハードウェア比較器（１８，１９）に供給され、このハードウェア比較器は、１個のチップ内で空間的に分離して配置されていることを特徴とする請求項１～６のいずれか１項に記載のマイクロプロセッサ装置。
【発明の詳細な説明】
本発明は、同じ入力情報を受けて同じプログラムを処理する、同期的に動作する２個の中央ユニットまたはＣＰＵと、読出し専用メモリ（ＲＯＭ）および随時書込み読出しメモリ（ＲＡＭ）と、テスト情報のための記憶場所と、テスト情報発生器と、中央ユニットまたはＣＰＵの出力情報をチェックし、不一致のときに切断信号を発生する比較器とを備えた、安全上重要な（安全臨界の）制御装置のために設けられるマイクロプロセッサ装置に関する。
安全上重要な制御装置には、例えばブレーキ機能に介入する自動車制御装置が所属する。この自動車制御装置のうち、特にホイールロックコントロールシステムまたはアンチロックコントロールシステム（ＡＢＳ）と、トラクションスリップコントロールシステム（ＡＳＲ、ＴＣＳ等）が多くの形で市場で入手可能であり、重要である。走行安定性コントロールシステム（ＤＳＣ、ＡＳＭＳ）とサスペンションコンロールシステム等は同様に安全上重要である。なぜなら、これらのシステムがブレーキ介入に基づいているかあるいはそれが機能しないとき車両の走行安定性を損なうことがあり得るからである。従って、このようなシステムの機能実施可能性を常に監視することが必ず必要である。それによって、エラーが発生したときに、コントロールを停止するかあるいは安全性にとってあまり危険でない状態に切り換えることができる。
例えばアンチロック車両ブレーキ装置の制御および監視のための回路装置またはマイクロ

プロセッサシステムの一例が、ドイツ連邦共和国特許第３２３４６３７号公報によって知られている。この文献では、入力データが同じようにプログラミングされた２個のマイクロコンピュータに平行に供給され、そこで同期処理される。両マイクロコンピュータの出力信号と中間信号は冗長的比較器によって一致しているかどうかチェックされる。信号が互いに異なっていると、同様に冗長的に設計された回路を介して、コントロールの切断が行われる。この公知の回路の場合には、両マイクロコンピュータの一方がブレーキ圧力制御信号を発生するために使用され、他方が検査信号を発生するために使用される。すなわち、この対称構造のマイクロプロセッサ装置の場合には、所属の読出しメモリと随時書込み読出しメモリを含む全部揃った２個のマイクロコンピュータが必要である。

ドイツ連邦共和国特許出願公開第４１３７１２４号公報に記載された回路を構成する他の公知装置では、入力データが同様に２個のマイクロコンピュータに平行に供給され、このマイクロコンピュータの１個だけが面倒である完全な信号処理を行う。第２のマイクロコンピュータは特に監視のために役立つ。従って、入力信号は調整および時間的な変化率を求めた後で、簡略化された制御アルゴリズムと簡略化された制御フィロソフィによって更に処理することができる。簡略化されたデータ処理は、高価なマイクロコンピュータ内で処理される信号と比較することによって装置の規定通りの運転を推定することを可能にする信号を発生させるために充分である。小さな出力の検査マイクロコンピュータの使用により、全部揃った同じ出力の高価な２個のマイクロコンピュータを備えた装置と比較して、製作コストを低減することができる。

冒頭に述べた種類のマイクロプロセッサ装置はドイツ連邦共和国特許公開第４３４１０８２号公報によって既に知られている。このマイクロプロセッサ装置は特にアンチロックブレーキ装置の制御システムに適用される。シングルチップに収納可能なこの公知の装置は、２個の中央ユニットまたはＣＰＵを含んでいる。この中央ユニットまたはＣＰＵでは入力データが平行に処理される。両中央ユニットまたはＣＰＵに接続された読出し専用メモリと随時書込み読出しメモリは、テスト情報のための付加的な記憶場所を有し、それぞれテスト情報を発生するための発生器を含んでいる。両中央ユニットまたはＣＰＵの一方の出力信号は制御信号を発生するために更に処理され、他方の“受動式の”中央ユニットまたはＣＰＵは“能動式の”中央ユニットまたはＣＰＵを監視するためにのみ役立つ。テスト情報を収容するためにメモリを比較的に少しだけ拡張し、この装置のメモリを２倍にすることをやめることにより、エラー識別に悪影響を与えないで製作コストの大幅な低減が達成される。

本発明の根底をなす課題は、安全上重要な用途に必要である、きわめて高い確率と信頼性で、装置の誤動作を認識し、信号化するようなマイクロプロセッサ装置を開発することである。同時に、このようなマイクロプロセッサ装置のための製作コストを低減すべきである。

この課題が請求項１に記載した装置によって解決されることが判った。この装置の特徴は、中央ユニットまたはＣＰＵが別個のバスシステムを介して読出し専用メモリおよび随時書込み読出しメモリと入力ユニットと出力ユニットに接続され、バスシステムがドライバステージによって互いに接続され、このドライバステージにより、両中央ユニットまたはＣＰＵが、懸案のデータ、すなわちテストデータと命令を含む、両バスシステムに供されるデータを一緒に読出しおよび処理することができることにある。両バスシステムに達する両中央ユニットまたはＣＰＵの入力データおよび出力データは、テストデータおよび命令を含めて、本発明による装置の比較器によって一致するかどうかチェックされる。

従属請求項には本発明の有利な若干の実施形が記載されている。

本発明によるマイクロプロセッサ装置は完全に冗長的に動作する同一の２個のプロセッサコアまたは中央ユニットの使用に基づいている。このプロセッサコアまたは中央ユニットまたはＣＰＵは別個のバスシステムから供給されるデータを一緒に冗長的に処理する。安全上の理由から第２の比較器が平行に接続配置されている簡単なハードウェア比較器によって、両中央ユニットまたはＣＰＵの入力信号と出力信号が一致しているかどうかチェックされる。本発明による装置のメモリは１回だけ存在する。例えばパリティビットの形を

したテストデータのための付加的な記憶場所だけが設けられている。
本発明の好ましい実施形によれば、中央ユニットまたはＣＰＵと読出し専用メモリと随時書込み読出しメモリと入力ステージと出力ステージからなる全部揃った１個のマイクロプロセッサが、両バスシステムの一方に接続され、第１のバスシステムは読出し専用メモリと随時書込み読出しメモリの代わりに、テストデータのための記憶場所にのみ直接接続されている。しかし、両バスシステムを接続するドライバステージにより、両中央ユニットまたはＣＰＵは、有効データメモリとテストデータメモリと入力ステージから供給される必要なすべてのデータを読出すことができる。これにより、本発明によるマイクロプロセッサ装置の構造が非常に簡単になり、このマイクロプロセッサ装置はすべての構成要素が１個のシングルチップに収納されるという利点がある。
本発明の他の特徴、効果および用途は、添付の図に基づく実施の形態の次の説明から明らかになる。図は本発明によるマイクロプロセッサ装置の重要な構成部品を概略的に示している。
本発明によるマイクロプロセッサ装置の原理的な構造と作用を説明するために添付の図が役立つ。この実施の形態では、マイクロプロセッサ装置はシングルチップマイクロコンピュータ装置である。このシングルチップマイクロコンピュータは、コンピュータコアまたはプロセッサコアあるいはＣＰＵと呼ばれる、同期作動する２個の中央ユニットまたはＣＰＵ１，２と、別個のバスシステム３，４（バス１，ス２）を備えている。両中央ユニットまたはＣＰＵ１，２にとって共通のクロックは、接続部ｃ１（共通クロック）から供給される。中央ユニットまたはＣＰＵ１は、読出し専用メモリ５（ＲＯＭ）と、随時書込み読出しメモリ６（ＲＡＭ）と、入力ステージ７，８（周辺装置１、ポート１）と、出力ステージ９とによって補足されて完全なマイクロコンピュータＭＣ１が形成される。これに対して、第２のバスシステム４（バス２）には、中央ユニットまたはＣＰＵ２のほかに、テストデータメモリ１０，１１と入力ステージ１２，１３と出力ステージ１４だけが接続されている。読出し専用メモリ５内のデータのためのテストデータ記憶場所はメモリ１０内に収納され、随時書込み読出しメモリ６のためのテストデータはメモリ１１内に収納されている。全体が“リーン”マイクロコンピュータＭＣ２を形成している。
更に、両バスシステム３，４（バス１，バス２）はドライバステージ１５，１６，１７を通じて接続されている。これは本発明によって重要である。これらのドライバステージは、入力されるデータを両中央ユニットまたはＣＰＵ１，２から一緒に読み取ることを可能にする。ステージ１５～１７はドライバ（またはイネーブル機能を有する“バッファ”）である。ドライバ１５～１７の伝送方向は矢印によって示してある。ドライバ１５はバスシステム３（バス１）内にあるデータを中央ユニットまたはＣＰＵ２に伝送する働きをし、ドライバ１６はテストデータメモリ１０，１１からテスト情報またはテストデータを中央ユニットまたはＣＰＵ１に伝送する働きをし、ドライバ１７は第２のバスシステム（バス２）の入力ステージ１２，１３からデータを中央ユニットまたはＣＰＵ１に伝送する働きをする。
バスシステム３，４はそれぞれコントロールバス“Ｃ”とデータバス“Ｄ”とアドレスバス“Ａ”を備えている。データバスはテストデータ“ｐ”も含んでいる。従って、ハードウェア比較器１８と、同じチップに場所的に分離して配置された同じような比較器１９において一致（相関関係）を検査される中央ユニットまたはＣＰＵの入力データと出力データは、“ＣＤｐＡ”で示してある。
公知の装置と異なり、本発明によるマイクロプロセッサ装置の場合には、アクティブプロセッサとパッシブプロセッサを区別することができない。両プロセッサコアまたは中央ユニットまたはＣＰＵ１，２は同じ権限がある。両プロセッサコアまたは中央ユニットまたはＣＰＵは一緒に読み出されるデータを完全に冗長的に処理する。このデータには、テスト情報または冗長情報と制御命令が属する。プロセッサ１，２の入力信号と出力信号は相関関係が検査され、所属のバスシステム３，４と出力ユニット９，１４を経て、象徴的に示した弁操作制御装置２０に供給される。この弁操作制御装置は次のように機能する。
両中央ユニットまたはＣＰＵ１，２はバスシステム３，４を経て同一の出力信号を出力ユ

ニット９，１４に供給する。両出力ユニットの一方に至る経路、ここでは出力ユニット１４に至る経路に、インバータ２２が挿入されている。弁操作制御装置２０は直列バス２１によって接続されている。この実施の形態では、２個の出力シフトレジスタ２２，２３が設けられている。この場合、プロセッサの間の短絡を防止するために、第２のシフトレジスタ２２にはデータが反転されて供給される。シフトレジスタ２２，２３に含まれるデータは、反転する入力部を有するアンドゲート（論理積ゲート）２４によって相関関係（一致）が比較される。ゲート２４が監視するアンド条件が満たされないと、動かされる弁またはアクチュエータ２５のための給電部にあるスイッチ２６が開放し、それによってアクチュエータ操作が停止される。なぜなら、エラーが存在するからである。

シフトレジスタ２２，２３は出力ステージ９または１４の構成部品であると見なされる。すなわち、比較器１８，１９と関係なく、出力信号の相関関係がもう一度、この場合外部で監視される。従って、エラーがある場合、中央ユニットまたはＣＰＵ１，２の機能とは関係なく、弁２５の動作が中断される。

すなわち、本発明では、演算ユニット全部とシーケンス制御部を含む中央ユニットまたはＣＰＵは、演算結果を保護し、プログラムを正しく実行するために、二重に形成されている。データバスはそれぞれ、例えばパリティビットのためのテストデータまたは冗長情報のための発生器だけ拡張されている。両中央ユニットまたはＣＰＵの出力信号はチェックのためにハードウェア比較器（１８，１９）に導かれる。この比較器はテスト信号を含む信号の同一性をチェックし、プログラムの同期実行が冗長性中央ユニットまたはＣＰＵによって互いに異なる結果を生じるときには、システムを切断する。

両中央ユニットまたはＣＰＵの出力信号は同じような権限がある。すなわち、メモリユニット（ＲＡＭ，ＲＯＭ）または“周辺装置”の操作は両中央ユニットまたはＣＰＵの一方によって行うことができる。

自動車制御装置の場合、出力信号が制御装置の重要な入力量である例えば車輪センサは、図において周辺装置１と周辺装置２と呼ばれる入力ユニット７，１２を介して接続可能である。その際、図に示すように、センサ信号供給部を両バスシステム３，４に分配することができる。信号供給は勿論、冗長的に行うことができる。すなわち、すべてのセンサ信号を両バスシステム３，４に接続することによって行うことができる。

同じことが入力ステージ８，１３（ポート１、ポート２）を経て供給される情報についても言える。制御されるブレーキシステムの場合には、例えば制動灯スイッチと他のセンサがこの入力ステージを介して接続される。

本発明の重要な特徴は、データ処理操作の充分な冗長性および“保護”にもかかわらず、メモリのコストが比較的に少なくて済むことにある。すなわち、読出し専用メモリと随時書込み読出しメモリは前述のように、両マイクロコンピュータの一方（ＭＣ１）のためだけに設けられ、第２のマイクロコンピュータ（ＭＣ２）にはテストデータのための記憶場所（１０，１１）だけが組み込まれている。両バスシステムを接続するドライバステージ１５，１６，１７により、それにもかかわらず、データ処理操作時に、記憶された有効データとテストデータが両中央ユニットまたはＣＰＵに供される。

図示した実施の形態と異なり、メモリ５，６，１０，１１の記憶場所は両バスシステム３，４またはマイクロコンピュータＭＣ１，ＭＣ２に完全に異なるように分配することできる。それによって、全体として必要な記憶場所が増大することはない。

記憶されたデータおよび記憶すべきデータの読出しおよび書込みの際のエラーの識別のために、テストデータまたはパリティデータが用いられる。読出し専用メモリと随時書込み読出しメモリの各々の記憶セルには、テストデータのための記憶場所だけを有する第２のマイクロプロセッサＭＣ２のメモリ１０，１１内で同じアドレスで、冗長信号が格納されている。読出し専用メモリのためのテスト情報または冗長情報はプログラミング中に既に定められている。随時書込み読出しメモリの場合、このテスト情報または冗長情報は書込みの際に発生させられる。データや命令の読出しと同様に、テスト情報または冗長情報は両バスシステム３，４を接続するドライバステージ１６を経て伝達される。書込みアクセスの際に、書込むべきデータは冗長情報だけ拡張される。この冗長情報はデータと共に記

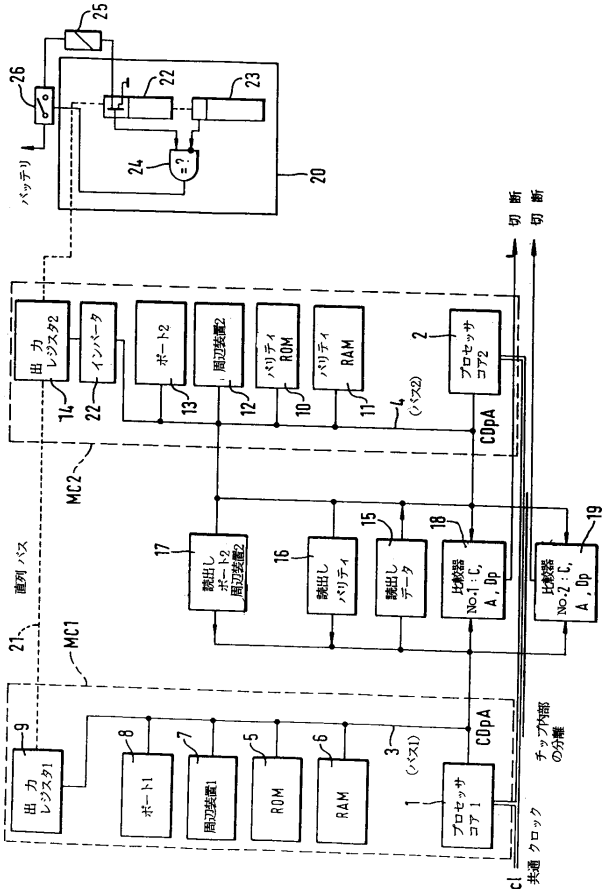
憶される。読出しアクセスの場合には、このデータと逆読みされる冗長情報は比較器１８，１９によって正当性がチェックされる。安全上の理由から入力データを冗長的に検出および処理すべきときには、入力ステージ（７，８，１２，１３）が二重に設計されている。このステージはそれぞれ一部を一方の中央ユニットまたはＣＰＵおよび他方の中央ユニットまたはＣＰＵのアドレス空間内に配置可能である。従って、対称マイクロプロセッサシステムの場合のように周辺要素が連結解除される。

出力信号、特に二重に設計された出力ステージを含む弁操作制御装置２０のための制御信号は同様に、それぞれ一部を一方または他方の中央ユニットまたはＣＰＵのアドレス空間内に配置可能である。従って、完全対称概念の場合のように、出力周辺要素が連結解除される。

バスシステムを経て情報を伝送する際のエラーを識別するために、このバスシステムはバスシステム３，４（バス１、バス４）の形に冗長的に設計されている。両中央ユニットまたはＣＰＵ１，２から出力されバスシステムに供給される信号は比較器１８，１９によって相互関係が監視される。

テストデータまたは冗長データを発生するためにパリティ発生器が使用されるとき、本発明によるシステムの場合には、２個の発生器が必要である。この発生器は例えば中央ユニットまたはＣＰＵ１，２または比較器１８，１９に収納することができる。随時書込み読出しメモリのために供される付加的な記憶場所（メモリ１１）に書込みアクセスする際に、冗長発生器によって中央ユニットまたはＣＰＵ２内で発生する情報が記憶される。読出し専用メモリまたは随時書込み読出しメモリ内のテストデータのための付加的な記憶場所に読出しアクセスする際に、冗長発生器によって発生した情報は、読出された冗長情報と相互関係が比較される。

適当な冗長発生器は例えば公知のごとく、排他的オアゲート（排他的論理和ゲート）によって実現可能である。



フロントページの続き

(72)発明者　ギールス・ベルンハルト
ドイツ連邦共和国、Ｄ－６０３２０　フランクフルト・アム・マイン、カイザーージークムントーストラーセ、６０

審査官　久保　正典

(56)参考文献　特開平０２－３０１８３６（ＪＰ，Ａ）
特開平０１－１５４２４１（ＪＰ，Ａ）
特開平０２－２０２６３６（ＪＰ，Ａ）
特開昭５９－１３０７６８（ＪＰ，Ａ）
特開平０７－１６０５２１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 11/16 - 20
G06F 15/16 - 15/177