(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5068436号
(P5068436)
(45)発行日　平成24年11月7日(2012.11.7)　(24)登録日　平成24年8月24日(2012.8.24)

(51)Int.Cl.　F I
G06F 13/00 (2006.01)　G06F 13/00 301P
G06F 13/00 301V

請求項の数 16　(全 15 頁)

(21)出願番号　特願2005-235667(P2005-235667)
(22)出願日　平成17年8月16日(2005.8.16)
(65)公開番号　特開2006-59356(P2006-59356A)
(43)公開日　平成18年3月2日(2006.3.2)
審査請求日　平成19年2月9日(2007.2.9)
審判番号　不服2010-24270(P2010-24270/J1)
審判請求日　平成22年10月28日(2010.10.28)
(31)優先権主張番号　102004039932.8
(32)優先日　平成16年8月17日(2004.8.17)
(33)優先権主張国　ドイツ(DE)

(73)特許権者　504019733
フェニックス　コンタクト　ゲーエムベーハー　ウント　コムパニー　カーゲー
ドイツ国．３２８２５　ブロムベルク，フラクスマルクトシュトラーセ　８
(74)代理人　100094112
弁理士　岡部　讓
(74)代理人　100064447
弁理士　岡部　正夫
(74)代理人　100085176
弁理士　加藤　伸晃
(74)代理人　100104352
弁理士　朝日　伸光
(74)代理人　100128657
弁理士　三山　勝巳

最終頁に続く

(54)【発明の名称】安全性関連処理のバス結合のための方法と装置

(57)【特許請求の範囲】
【請求項１】
少なくとも２つの冗長処理チャネル（１、２）を、安全性関連処理のための１チャネルのバスに結合するための方法であって、
少なくとも２つの冗長処理チャネル（１、２）上の前記安全性関連処理に関連するデータ記録は、特定のプロトコル、すなわち、同じ法則に従って、各々の安全プロトコル（１４、２４）を形成するように処理され、
冗長性の前記安全プロトコル（１４、２４）は、冗長処理チャネル（１、２）の各々により共通のバッファ・レジスタ（３０）が交互にアクセスされることによって、１チャネルのバスに結合するための共通かつ単一の安全プロトコルへと組み立てられ、ここにおいて、レジスタ場所の各々に対する書き込み権限は前記安全プロトコル（１４、２４）のどちらか一方に対し一回だけ割り当てられ、前記安全プロトコル（１４、２４）に共通の構成要素、すなわち共通のデータの一方のみが当該場所に書き込まれることによって、前記共通かつ単一の安全プロトコルが組み立てられる、
方法。
【請求項２】
さらに、前記バッファ・レジスタ（３０）から１チャネルのバス（４０）へと前記共通かつ単一の安全プロトコルを移送する前に、共通かつ単一の安全プロトコルが形成されていることを確認するため、前記バッファ・レジスタ（３０）内の各々のレジスタ場所の内容が、前記冗長処理チャネル（１、２）の各々によって読み取られる、請求項１に記載の

方法。
【請求項３】
さらに、前記共通かつ単一の安全プロトコルの書き込み前に、前記処理チャネル（１、２）を介して冗長的に形成された前記安全プロトコル（１４、２４）が互いに同じであることがチェックされる、請求項１または２のいずれか１項に記載の方法。
【請求項４】
さらに、書き込み権限の割り当てに重複のないことを確認するための検査手順が実行される、請求項１乃至３のいずれか１項に記載の方法。
【請求項５】
さらに、それぞれ異なった特定の初期設定値を前記バッファ・レジスタ（３０）内の前記レジスタ場所のすべてに書き込むように前記検査手順中に前記処理チャネル（１、２）の各々を介して試みがなされ、その後、前記バッファ・レジスタ（３０）内の前記レジスタ場所のすべてが前記処理チャネル（１、２）の各々を介して読み取られ、前記レジスタ場所の内容が重複なくインターリーブされているか確認される、請求項４に記載の方法。
【請求項６】
さらに、前記検査手順が一回よりも多く実行され、かつ／または前記レジスタの場所が、異なる前記処理チャネル（１、２）を介して交互に書き込みおよび読み取りをされる、請求項４乃至５のいずれか１項に記載の方法。
【請求項７】
さらに、標準的なＲＡＭまたは標準的なＤＰＭが前記バッファ・レジスタ（３０）として使用される、請求項１乃至６のいずれか１項に記載の方法。
【請求項８】
さらに、前記共通かつ単一の安全プロトコルが１つのチャネル上で前記バッファ・レジスタ（３０）から、特定の用途に基づいて設計されるバス連結装置（３５）へと移送される、請求項１乃至７のいずれか１項に記載の方法。
【請求項９】
少なくとも２つの冗長処理チャネル（１、２）を、安全性関連処理のための１チャネルのバスに結合するための装置であって、
同一の入力データを、特定のプロトコル、すなわち、同じ法則を使用して各々の安全プロトコル（１４、２４）へと組み立てる少なくとも２つの冗長コンピュータ（１１、２１）と、
前記安全プロトコル（１４、２４）の各々の共通部分を一体とすることで共通かつ単一の安全プロトコルを形成するように、前記コンピュータ（１１、２１）のうちの一方だけが共通のバッファ・レジスタ（３０）内の各々のレジスタ場所に関して書き込みアクセス能力を有するような方式で、各々のコンピュータ（１１、２１）を交互に前記バッファ・レジスタ（３０）へと接続するための回路配列と、
を有する装置。
【請求項１０】
さらに、前記コンピュータ（１１、２１）の各々が、前記バッファ・レジスタ（３０）内の各々のレジスタ場所に関して読み取りアクセス能力を有するように前記回路配列が設計される、請求項９に記載の装置。
【請求項１１】
さらに、前記コンピュータ（１１、２１）が通信インターフェース（１０１）を介して互いに接続される、請求項９または１０のいずれか１項に記載の装置。
【請求項１２】
さらに、前記コンピュータ（１１、２１）各々が集積型プロトコル・チップを有するかまたは出力側でプロトコル・チップ（１３、２３）へと接続されるか、あるいは前記プロトコル・チップの機能を提供するソフトウェアを有する、請求項９乃至１１のいずれか１項に記載の装置。
【請求項１３】

さらに、前記装置がバス加入者ユニットであり、かつ複数の処理データ入力ユニットの連結のために前記コンピュータが入力側で少なくとも入力チャネルへと接続されるか、あるいは前記装置がバス制御ユニットである、請求項９乃至１２のいずれか１項に記載の装置。

【請求項１４】

前記回路配列が単純な論理を使用して設計されるか、またはＦＰＧＡの形式である、請求項９乃至１３のいずれか１項に記載の装置。

【請求項１５】

さらに、前記バッファ・レジスタ（３０）が標準的なＲＡＭまたは標準的なＤＰＭである、請求項９乃至１４のいずれか１項に記載の装置。

【請求項１６】

さらに、前記バッファ・レジスタ（３０）が直接的な１チャネルのバス結合のため、または特定の用途に基づいて設計されるバス連結装置（３５）への１チャネルの連結のためのインターフェースを有する、請求項９乃至１５のいずれか１項に記載の装置。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、安全性関連処理の１チャネル・バスの結合のための方法およびその方法を実行するように構成される装置に関する。

【背景技術】

【０００２】

以下の文章で、「安全性関連処理」という表現は故障が生じても人々および／または有形財に対する無視し得る以上の危険性に結びつかない処理を意味する。したがって安全性関連処理では、理想的なケースで、故障が存在するときにこの処理、この処理につながるその後の処理、および／またはこの処理を含む全体的なシステムが安全な状態にされることを１００％の信頼性で確実化することが必要である。したがってこのような安全性関連処理はまた、さらに大きくさらに高いレベルの全体的システムのうちの処理要素であることが可能である。安全性関連処理の範例は厳密な処理が予め決められた範囲内に保たれることが必須である化学的処理、および例えば液圧プレスまたは生産ライン用の複雑な機械制御システムであり、このケースでは、例えば、プレス／切断工具の起動は安全性関連処理要素を代表することが可能である。安全性関連処理（処理要素）のさらなる範例は防護ガード、防護ドアまたは照明領域のモニタリング、両手操作スイッチの制御、あるいはそのほかに非常時切断スイッチへの反応である。

【０００３】

したがって、すべての安全性関連処理に関して、作成、記録、もしくは測定されるそれぞれに付随の安全性関連データがどのような間違いも伴わずにリアルタイムで搬送されることは完全に必須であり、なぜならばどのような間違いも間違った操作および／または反応に結びつく可能性があり、それが最終的に人々の生命および健康を危険にさらす可能性があるからである。

【０００４】

安全性の規制を満たすために、数多くの取り決めが近年達成されており、それらはバス・システムを使用するときに事実上誤りの無いデータ搬送を必要とする。これらは特に、データ搬送自体に関連し、かつそれぞれの用途および／またはそれぞれの処理の関数としての許容し得る残留誤差の確率（残差確率）に関連する。このケースで引用されることが可能な関連規格は特に、ＥＮ６１５０８およびＥＮ　９５４－１、ならびにＧｅｒｍａｎ　Ｉｎｄｕｓｔｒｉａｌ　Ｐｒｏｆｅｓｓｉｏｎａｌ　ＳｏｃｉｅｔｉｅｓのＴｅｓｔ　ａｎｄ　Ｃｅｒｔｉｆｉｃａｔｉｏｎ　Ｃｅｎｔｅｒによって作成された「ｂｕｓ　ｓｙｓｔｅｍｓ　ｆｏｒ　ｔｈｅ　ｔｒａｎｓｍｉｓｓｉｏｎ　ｏｆ　ｓａｆｅｔｙ－ｒｅｌｅｖａｎｔ　ｍｅｓｓａｇｅｓ」の検査と認証の原則を含む。

【０００５】

これらの取り決めおよび規格に従って安全性ベースのバス・システムが開発されており、それは高い冗長度を備えたデータを送信する。生じ得る故障または誤りは都合の良い時間に発見され、どのような危険性も回避されることが可能である。この範例は、とりわけ、Ｓａｆｅｔｙ　Ｂｕｓ　Ｐ、Ｐｒｏｆｉｂｕｓ　Ｆ、Ｉｎｔｅｒｂｕｓ　Ｓａｆｅｔｙなどを含む。

【０００６】

しかしながら、このケースの１つの欠点は、既にインストールされているバス・システムが安全性ベースのバス・システムの使用のために差し替えられなければならないことであり、加入者の数、データ搬送速度、またはデータ・プロトコルに制限を受けることを頻繁に必要とする。

【０００７】

その結果、既に存在するバス・システムのさらに単純かつさらに低コストの改造を可能にする安全性ベースの方法および／または構成要素が開発されてきた。処理に含まれる個々のユニット間で既に使用されている（フィールド）バス・システムは、このケースでは特にセンサ、アクチュエータ、および／または制御装置間の安全性関連データの送信用のデータ通信に、特に制御および自動化技術に使用される電子式安全方法のケースで使用される。

【０００８】

例を挙げると、ＥＰ　１１８８０９６Ｂ１号は、安全性関連処理を制御するための制御ユニットおよびＩ／Ｏチャネルを介して安全性関連処理へと連結される信号ユニットが経由して接続されるフィールド・バスを備えた安全性関連処理のための制御システムを開示している。フェイルセーフを備えた相互の通信を保証するために、これらのユニットは安全性関連装置を有し、その目的は安全ではないユニットを安全にすることである。詳細に述べると、各々のケースで少なくとも２つの冗長処理チャネルが、一方の処理チャネルでの誤りもしくは故障が他方の余剰処理チャネルのそれとは異なる結果に基づいて識別され、可能であれば修正されるような方式で設けられる。この多重チャネル構造は特に２つの冗長コンピュータによって供給され、安全性分析が２つの冗長コンピュータの後段で終了され、その分析結果は、どのようなさらなる命令文も伴わずにこの時点から安全性データ・プロトコルのために使用される。

【０００９】

以下の文章では、一般的言葉のコンピュータは本質的にマイクロコンピュータ、マイクロプロセッサ、マイクロコントローラ、あるいはその他のＰＣといったどのようなタイプのデータ処理装置も意味する。

【００１０】

ＷＯ　０１／２４３８５Ａ２号もやはり（フィールド）バス・システムを使用する安全性関連処理の制御に関し、安全性関連処理の制御に含まれるユニットが今度もやはり冗長処理チャネルを概して有する。冗長チャネルの各々はコンピュータを有し、それらのコンピュータが相互にモニタし合う。この多重チャネル構造は、フィールド・バスへと接続されるさらなるコンピュータによって１チャネル構造へと変えられる（図３）。そのドキュメントはさらに広範囲の命令文を含むことはなく、多重チャネル構造形式から１チャネル構造形式への変更を含む。

【００１１】

ＷＯ　０１／２４３９１Ａ１号および公開特許明細書のＤＥ　１９９３９５６７Ａ１号は安全プロトコル作成のために相互にモニタし合う冗長処理チャネル、および／またはコンピュータを備えた安全バス加入者のさらなる範例であり、後に、バスに連結され、かつプロトコル・チップに接続されるかもしくはそれに一体化されるさらなるコンピュータを介して２チャネル形式から１チャネル形式へと変わる。このケースでも同様に、２つの冗長コンピュータに基づいて、さらなる技術対策の開示を伴うことなく安全分析が終了し、安全データ・プロトコルのための分析がこの時点から役割を果たすようになる。

【００１２】

２つの冗長コンピュータによって形成されたデータの１チャネル送信のための装置に関連する特許明細書ＤＥ　１９５３２６３９Ｃ２号は、回路の複雑さを軽減するために２つの冗長コンピュータのうちの一方にバス結合の機能を一体化させる。その結果、バス結合の機能を有するそのコンピュータだけが出力チャネルを有し、そこにこのコンピュータから由来する有用データおよび他方のコンピュータから由来する試験データ、またはその逆が供給され、あるいは両方のコンピュータからの有用データと試験データが供給され、互いに交互配置される（図４）。しかしながら、バスを制御しているコンピュータが、他方のコンピュータが影響を与えることの不可能なメッセージを作成し得ないことを確実化するために、安全分析の実施は増大した複雑さを含む。なぜならば安全プロトコルの作成に関して一方では反応からの解放、他方ではコンピュータの独立性が検証されなければならないからである。この背景で、この特許明細書は適切な接続だけを提案しており、それぞれのコンピュータ出力の接続が無い。

【００１３】

さらに、ＤＥ　１００６５９０７Ａ１号は２チャネル形式から１チャネル形式への変更のために、２つの論理的に同一のデータ領域を備えたバッファ・レジスタを使用し、並列もしくは直列のネットワークまたはバス・システム上でデータを送信するために安全データ搬送に関する「交差比較を伴う冗長度」の原則に基づいた方法を述べている。バス・システムを介して１つのチャネル上で送信される完全な安全性ベースのメッセージはバッファ・レジスタの両方のデータ領域のデータ内容を含む。ここでもやはり２つの冗長コンピュータが用途の性質に応じて送信器端部のバッファ・レジスタの上流に接続され、各々のケースで安全データを形成するために（１チャネルまたは２チャネル上で利用可能にされる）安全性関連データを冗長情報で前処理し、それを相互に交換してチェックする。もしも両方が同じ結果に至れば、各々のコンピュータはその安全データをバッファ・レジスタへと移し、各々のデータ領域は各々のケースで１つのコンピュータから入る安全データで満たされ、そのデータ自体が既に誤りもしくは故障識別のための冗長情報を含んでいる。別の代替選択肢の実施形態で、もしもバッファ・レジスタが２つのコンピュータのうちの一方に含まれ、それにより、結果としてこの一方のコンピュータが第２のコンピュータとの合意の後にバッファ・レジスタの両方のデータ領域を満たす場合、この第２のコンピュータはモニタリングのためにバッファ・レジスタを２つのデータ領域で再度読み取る。用途に応じて、バッファ・レジスタの２つのデータ領域のうちの一方のデータ内容は、例えば系統的な故障を送信器、受信器、および／またはデータを通過させる他のユニット内で識別するために反転データ、または他の追加的なインタリービングを有することもやはり可能である。したがって、これは安全ベースのメッセージの全体のデータ長が実際の有用データに関して極端に大きくなり、その結果、実際の有用データのためのデータ伝送速度が低くなるという特定の欠点を有するが、なぜならば、２つの同じ有用データ記録、ならびに同じ有用データ記録の各々に関する情報のそれぞれの冗長項目が送信されなければならないためである。例えばＩｎｔｅｒｂｕｓを伴うケースのようにもしもデータ・パケット当たりの送信される有用データ項目の数が減少すると、全体的データ長に対する有用データ長の比は大幅に減少する。

【特許文献１】ＥＰ　１１８８０９６Ｂ１号
【特許文献２】ＷＯ　０１／２４３８５Ａ２号
【特許文献３】ＷＯ　０１／２４３９１Ａ１号
【特許文献４】ＤＥ　１９９３９５６７Ａ１号
【特許文献５】ＤＥ　１９５３２６３９Ｃ２号
【特許文献６】ＤＥ　１００６５９０７Ａ１号

【発明の開示】

【発明が解決しようとする課題】

【００１４】

したがって本発明の１つの目的は、安全性関連処理の安全なバス結合のために多チャネル形式から１チャネル形式へと変更するためのさらなる、新規性があり、かつ改善された

手法を提供すること、および容易に導入されることが可能な方式で、特に付け加えると容易に検査されることが可能な方式で、バスを介して安全性メッセージとして送信されるように意図される安全性ベースのプロトコルの作成に際して反応からの解放および独立性を保証することである。

【課題を解決するための手段】

【００１５】

本発明による解決策は添付の独立請求項のうちの１つの特徴を伴う主題事項によって極めて驚異的な方式で達成される。

【００１６】

利点および／または好ましい実施形態および展開はそれぞれの従属請求項の主題事項である。

【００１７】

したがって本発明によれば、安全性臨界処理の１チャネルのバス結合のための方法が提案され、そこでは安全性臨界処理に関連するデータ記録が、特にプロトコル特異性の基礎で、各々のケースで１つの安全性ベースのプロトコルに関して同一の法則に従って少なくとも２つの冗長処理チャネルを介して処理され、１チャネルのバス結合のための冗長的な安全ベースのプロトコルが一体に連結されることで共通の安全性ベースのプロトコルを形成し、正確に述べると、共通の安全性ベースのプロトコルすなわち送信される安全性メッセージが各々のケースでそれぞれの安全性ベースのプロトコルの異なる構成要素に書き込むことによって構成要素内で連結されるような方式で、処理チャネルの各々が一回だけ割り当てられる各レジスタの場所に関する書き込み権限を備えて共通のバッファ・レジスタにアクセスする。

【００１８】

その結果、このケースの１つの主要な利点は、一方では両方の処理チャネルが、必要とされるメッセージ長に肯定的な影響を有するような方式で完全な安全性ベースのプロトコルを見積もることが可能であることであり、なぜならば、データ・ビットのすべては様々な安全性メカニズムを備えて冗長処理チャネル内で既に知られており、受信器端部での正確な見積もりの推論を可能にするために追加的なデータ・ビットが送信される必要がないからである。

【００１９】

さらに、これは一方の処理チャネルがそれ自体で、容易に導入されることが可能であり、かつ使用されるバス（システム）とは無関係に低コストで大幅に優れた安全性を保証するために高度に効率的である性能を表わす登録場所のデータに関して一回だけ各々のケースで割り当てられることが可能な書き込み権限による制御を伴って安全性メッセージを送信することが不可能となることを確実化する。

【００２０】

したがって、本発明による方法を実行するための知能的ユニットの提供は少なくとも２つの冗長コンピュータを有する装置の使用によって保証されることが可能であり、同一の入力データ記録を処理するためのそれらのコンピュータは各々のケースで１つの安全性ベースのプロトコルに関して同一の法則を使用して設計され、それらは、バッファ・レジスタ内の各々のレジスタ場所に関して各々のケースでコンピュータのうちの一方だけに書き込みアクセスが与えられるような方式で回路配列を介して共通のバッファ・レジスタへと接続される。まさに標準的構成要素の使用により、かつそれぞれのバス・システムとは無関係に、こうして本発明はそれぞれの安全性ベースのプロトコルの反応から解放されてかつ独立した形成のために、導入することが単純であり、高度に動的で高効率の解決策を可能にする。

【００２１】

安全性メッセージの形成のための特定の処理法則は、このケースでは、それぞれの安全正の必要条件、特にＳＩＬ　３　ＩＥＣ　６１５０８に従った単一送信のための安全性必要条件を満たすためにさらに好都合に適している。

【００２２】
このような装置を使用するとき、コンピュータの各々がバッファ・レジスタ内の各々のレジスタ場所に対する読み取りアクセスを行なうことが可能となるように回路配列が便宜的に設計される。
【００２３】
これはまた、単純で低コストの方式で標準的な構成要素を使用することを確実化することも可能にし、１つの好ましい展開では、各々の冗長処理チャネルの送信に関して連結された安全性ベースのプロトコルをバッファ・レジスタからバスへと移す前に、連結して形成された安全性ベースのプロトコルを確認するために各々のレジスタ場所に戻って読み取りアクセスが為されることが可能である。これが可能にする、連結して形成された安全性ベースのプロトコルと別々もしくは個々に形成されるそれぞれの安全性ベースのプロトコルとの、処理チャネルを介した追加的な比較は達成される安全性をさらに大幅に高める。その結果、コンピュータの不具合もしくは故障の事態に完全な安全性メッセージを作り出すことが不可能になり、それにより、不具合もやはり必然的に識別され、安全性ベースの機能が起動させられることが可能となる。
【００２４】
これを上回る安全性のさらなる増大もまた、１つの特に好ましい実施形態で、もしも連結された安全性ベースのプロトコルの書き込みの前に冗長的に形成された安全性ベースのプロトコルが最初に、それらが互いに同じであることを確実化するために処理チャネルによってチェックされ、それにより、同一の入力データ記録から互いに別々に処理される同一の安全性ベースのプロトコルに応答したときにのみ連結された安全性ベースのプロトコルが形成されるならば確実化される。もしも冗長処理自体に不具合もしくは誤りが発生すれば、これが初期の段階でさえこうして識別され、その処理は初期でさえ安全な状態へと変えられることが可能である。
【００２５】
本質的に互いに切り離されたコンピュータは通信インターフェースを介してこうして互いに接続されることが好ましい。
【００２６】
それぞれの書き込み権限をチェックすることもやはり好都合であり、それは各々のケースで確認のために検査手順によって規定の方式で処理チャネルへと割り当てられる。各々のレジスタ場所に関する完全な読み取りアクセスもやはりこの目的のために好都合である。
【００２７】
１つの好ましい検査手順によると、このケースではそれぞれ異なって特定的に付随した初期設定値をバッファ・レジスタ内のすべてのレジスタ場所に書き込むために処理チャネルの各々を介して試みが為される。その後、処理チャネルの各々がバッファ・レジスタ内のすべてのレジスタ場所を読み出し、明確なインタリービングに関してレジスタ場所の内容を確認する。
【００２８】
このような検査手順は一回よりも多く実行され、かつ／または異なる処理チャネルを介してレジスタ場所への書き込みと読み取りを交互に行なうことによって実行されることが好ましい。
【００２９】
本質的に、中に含まれ、連結された安全性ベースのプロトコル内もしくはバッファ・レジスタ内の特定の位置もしくはアドレスでバッファ・レジスタに移されるデータの結合によって選択されるすべての安全性移送／移譲規則は結論的に容易に検査されることが可能であり、したがって、コンピュータの不具合から結果的に生じるそれらを含めた、送信される安全性メッセージの形成時の不具合もしくは誤りすべてが確実に識別されることが可能である。
【００３０】

入力データの各々のプロトコル特異性の処理を行なって安全性ベースのプロトコルを形成した後、特にこのプロトコルが保存され、プロトコル特異性に基づいてバスへと移され、安全なプロトコル・データ記録のために安全性ベースのプロトコルがそれぞれの用途に基づく必要条件を、特にバスおよび／または処理の機能として満たすことを確実化するために、各々のケースで一実施形態によるコンピュータは集積型プロトコル・チップを有する。別の代替選択肢の実施形態では、プロトコル・チップはコンピュータへの出力側で接続されることもやはり可能である。そのような集積型または下流のプロトコル・チップを回避し、結果的に部品の数およびコストも削減するために、さらなる特に都合の良い実施形態はコンピュータが、データの処理およびプロトコル特異性の移送のために適切に設計されるソフトウェアを設けられることを提案する。

【００３１】

本発明による装置はバス加入者ユニットであることが可能であり、この目的のためのコンピュータは入力側で少なくとも、処理データ入力ユニットの１チャネルもしくは多チャネルの連結、および特に対応する方式で、処理される安全性関連入力データの１チャネルもしくは多チャネルの記録のための入力チャネルへと接続されることが好都合であり、あるいは、例えば処理される安全性関連入力データを発生するバス制御ユニットの形式であることが好都合である。したがってコンピュータは、特に、マイクロコントローラまたは中央処理装置（ＣＰＵ）である。

【００３２】

本発明に従ってコンピュータを連結するための回路配列、またはもしも適切であれば、コンピュータの下流のプロトコル・チップは１つの好ましい実施形態では単純な論理回路であり、そのケースでは例えばＦＰＧＡ（書替え可能ゲートアレイ）の形で、付け加えるとまた特定用途向けでもあることが可能であると有利である大規模集積回路を使用することもやはり可能である。

【００３３】

バッファ・レジスタはインターフェースを有し、保存されている連結された安全性ベースのプロトコルがそれを介して１つのチャネル上でバス、例えばＩｎｔｅｒｂｕｓへと直接連結されることが可能であり、あるいは用途特異性に基づいて設計され、かつバスの上流に接続されるさらなるバス連結装置へと１つのチャネル上で移送されることが可能であり、そのケースでは、特に、さらなるプロトコル・チップ、さらなるマイクロコントローラまたはいくつかの他の知能的ユニットが用途特異性に基づいてバス連結装置として使用されることが可能である。

【００３４】

したがって、実に標準のＲＡＭがこのバッファ・レジスタ用に十分である。しかしながら、１つの好ましい展開は、特に、デュアル・ポート・メモリ（ＤＰＭ）の形のバッファ・レジスタもしくはバッファ貯蔵器を提供し、それにより、コンピュータは２つのインターフェース・ポートのうちの一方を介して極めて単純かつ低コストの方式で接続されることが可能となり、第２のインターフェース・ポートはバスへの１チャネル結合のために使用されることが可能となる。

【００３５】

本発明のさらなる特徴および利点は、単なる範例の方式に過ぎないが以下の本発明の好ましい実施形態の詳細な説明および添付の図面を参照すると明らかになるであろう。

【発明を実施するための最良の形態】

【００３６】

図１は、これ以上詳細には例示されないが、バス４０、例えばＩｎｔｅｒｂｕｓへの安全性臨界処理を連結するためのバス加入者ユニットもしくはバス制御ユニットの２つの冗長処理チャネル１および２を具体的に示している。バス加入者ユニットのケースでは、処理チャネルの各々が入出力ユニット、例えばセンサおよび／またはアクチュエータへと接続され、それらが安全性臨界処理に付随するが、しかし同様に例示されない。

【００３７】

したがって、特定のリンクの性質に応じて、安全性臨界処理に関連する同じ入力データが、センサ端部での用途を伴うバス加入者ユニットへの処理チャネル１および２のうちの１つのチャネルまたは２つのチャネルで利用可能にされ、このデータが、さらなる処理のために最初に便宜的にそれぞれのメモリ１２および２２の中に保存される。特に、バス制御ユニットのケースでは、安全なデータに関連するバス伝送の前に前処理される安全性関連の入力データがメモリ１２および２２の中に配置される。

【００３８】

最初に、バス４０を介して安全性メッセージの送信の前に各々のケースで安全性ベースのプロトコル１４および２４を形成するために同じ法則を使用して入力データが冗長処理される。この目的のための処理チャネルはメモリ１２または２２内に配置された安全性関連入力データのそれぞれの前処理／処理のためのそれぞれのマイクロコントローラ１１または２１を有し、それにより、安全性ベースのそれぞれのプロトコル１４または２４、および図１に示された実施形態ではそれぞれのプロトコル・チップ１３または２３を形成し、これがそれぞれのマイクロコントローラ１１または２１の下流に接続され、バス４０へのさらなる移送のためにそれぞれのマイクロコントローラ１１または２１によって見積もられた安全性ベースのそれぞれのプロトコル１４または２４を受け取る。それぞれの例示されたプロトコル・チップ１３および２３の別の代替選択肢の実施形態では、マイクロコントローラ１１および２１は適切に構成されたソフトウェアもやはり有することが可能であり、それにより、以下の文章で述べられるであろうが、マイクロコントローラ１１および２１はバス４０への見積もられたプロトコル１４および２４のさらなる移送を提供する。

【００３９】

その結果、見積もり中に誤り、過失、または不具合が生じなかったことを前提として、見積もられた安全もしくは安全性ベースのプロトコル１４および２４は同一である。もちろんこのケースでは安全プロトコルが安全性ベースの送信に関する規格の要求条件に準拠するように構成されることに留意すべきである。

【００４０】

本発明によると、安全性をさらに高めるために、バス４０を介した安全メッセージの送信の前にさらなる同一で共通の安全性ベースのプロトコルが供給され、その後、これが送信のために１つのチャネル上でバス４０へと移送される。

【００４１】

この連結された安全性ベースのプロトコルは、処理チャネル１および２各々によってアクセスされることが可能なバッファ貯蔵器もしくはバッファ・レジスタ３０内の安全プロトコル１４のデータおよび安全プロトコル２４のデータの構成要素１つ１つを単位とした構成によって形成される。

【００４２】

処理チャネル１もしくは２の一方だけから入るデータだけに基づいて連結形成され、その結果、例えば２つのマイクロコントローラのうちの一方で生じた不具合に基づくような、２つのマイクロコントローラ１１もしくは２１の一方だけによる安全性メッセージの送信と同等になるであろうこの安全性ベースのプロトコルを防止するため、規定の、もしくは規定することの可能なアクセス規則がバッファ貯蔵器３０への書き込み権限を制御する。このケースでのアクセス規則は、各々の処理チャネル１および２から入るそれぞれの見積もられた安全性ベースのプロトコルの一部だけを記載し、それは連結の安全性ベースのプロトコルの形成のためにバッファ貯蔵器３０内の適切なメモリ場所に書き込まれることが可能であり、それぞれのマイクロコントローラ１１または２１がそれぞれの書き込み権限を有するものである。したがって、本発明によると、各々のケースで一方の書き込み権限だけが各々のメモリもしくはレジスタ場所に関して規定される。

【００４３】

安全プロトコル１４および２４が同一であるという仮定に基づくと、プロトコルの各々はしたがってやはり同じ数のバイトを有し、図１でバイトＸからバイトＸ＋５で注記され

ている。図１に示されたこの範例では、バイトＸ、バイトＸ＋２、およびバイトＸ＋４に関するバッファ貯蔵器３０のメモリ・アドレスの書き込み権限は処理チャネル２用のマイクロコントローラ２１に永続的に割り当てられ、バイトＸ＋１、バイトＸ＋３、およびバイトＸ＋５に入る書き込み権限は処理チャネル１用のマイクロコントローラ１１に割り当てられる。その結果、バッファ貯蔵器３０内のすべての交互になったバイトに関する一方の書き込み権限だけがマイクロコントローラ１１および２１の各々に割り当てられる。

【００４４】

例を挙げると、もしもＸ＝０であり、かつ冗長性の安全性ベースのプロトコル１４および２４、ならびに連結形成される同じ安全性ベースのプロトコル、すなわち送信されるべき次の安全性メッセージが合計６バイトを有するならば、冗長性安全プロトコルの中のデータ、したがって送信される安全性メッセージの中のデータもやはり、例えば２ビットのヘッダ、それに続く１４ビットの有用データ、８ビットのアドレス、および２４ビットのＣＲＣチェックサムで構成される。規定の方式で割り当てられる上記の書き込みアクセス権限は、２ビットを有するヘッダ、および図１を参照すると処理チャネル２を介して見積もられた安全プロトコル２４から移される有用データの最初の６ビット、処理チャネル１を介して見積もられた安全プロトコル１４から移される有用データの次の８ビット、入れ替わってプロトコル・データ記録２４から移される８ビットを有するアドレス、および見積もられたプロトコル１４、２４および１４から構成要素１つ１つ連続して移される２４ビットを有するＣＲＣチェックサムに結果的につながる。

【００４５】

したがって、標準的なＲＡＭでさえ、または、以下の文章から理解されるように好ましくはおよび、ＤＰＭがバッファ貯蔵器として使用されることが可能である。

【００４６】

もしもさらに好都合な方式で両方の処理チャネル１と２のマイクロコントローラ１１と２１がバッファ貯蔵器３０への完全な読み取りアクセスを割り当てられれば、二重の冗長性だけでさえこれを上回るさらに向上した安全性に結びつく。

【００４７】

これはすべてのデータの単純な比較を可能にするが、なぜならば、一方では、安全性メッセージとして送信され、例えばＳＩＬ　３　ＩＥＣ　６１５０８に従った単一送信のための安全性の要求条件を満たす連結形成された安全プロトコルが不具合もしくは誤りを有していないかどうかを単純な方式で、正確に述べると、既に別々に形成されているであろう独自の安全性ベースのプロトコル１４または２４に対するそれぞれの確認によってチェックすることが可能であるからである。さらに、処理チャネル１および２の各々に関する完全な読み取りアクセスは、アクセス規則がどのような誤りもしくは不具合も伴わずに概して実行されるかどうかのチェックのような、安全性臨界処理を制御／モニタ／調節する周囲状況で都合良く既に実行され得るものをチェックすることを可能にする。この背景では、特に一方または他方の処理チャネルのそれぞれのマイクロコントローラの見積もられたデータがバッファ貯蔵器３０内のそれぞれ割り当てられたメモリ・アドレスだけに排他的に（これは保証されるが）書き込まれるかどうかを判定するためにチェックが実行される。

【００４８】

もしもこの「自己確認」および／または「交差確認」が、同じではないという結果につながれば、誤りもしくは不具合が必然的に識別され、安全性ベースの機能が起動させられる。

【００４９】

プロトコル・チップではなく上述したようなソフトウェアを使用することによる範例を挙げると、図２は図１にスケッチした書き込み権限、ならびに完全な読み取り権限をこれらの確認処理用の基盤として実行するための１つの考え得る機能回路図を例示している。

【００５０】

図２に例示されるように、左に例示され、Ｍで注記される領域は安全性分析を伴った本

発明による多チャネルのアーキテクチャを有し、図２でＥで注記される右手の領域は、安全性メッセージとして送信される連結形成された安全性ベースのプロトコルを伴った１チャネルのアーキテクチャを有する。

【００５１】

したがって、本質的に図１に基づくと、２つのマイクロプロセッサ１１および２１はそれ自体知られている方式で切り離され、図２の参照番号１００によって識別され、さらに、それぞれ別々に見積もられた安全性ベースのプロトコル１４および２４の追加的な相互チェックのために通信インターフェース１０１を介して互いに接続される。

【００５２】

ｘが０とＮの間である場合のアドレスＡｘに関するアドレス・バス１０２、ｘが０とＮの間である場合のデータＤｘに関するデータ・バス１０３、ならびに／ＣＳ（チップ選択）信号、／ＲＤ（読み取り）信号は基準として標準的ＤＰＭに直接加えられ、これは図２で、／ＣＳＬ信号および／ＲＤＬ信号それぞれのための適切なピンで例示されている。アドレス・ラインＡ０は、マイクロコントローラ１１だけが偶数番号のアドレスに関する書き込み権限を有し、マイクロコントローラ２１だけが奇数番号のアドレスに関する書き込み権限を有するようにマイクロコントローラ１１および２１の書き込み信号／ＷＲ＿μＣ１および／ＷＲ＿μＣ２へと連結される。これらは書き込み信号／ＷＲが適切なピンを介して標準ＤＰＭのＲＡＭで「低活性」信号／ＷＬに関して起動させられ得る２つの状況だけである。しかしながら、両方のマイクロコントローラ１１と２１が読み取り目的で全体のメモリ３０にアクセスすることが可能である。

【００５３】

連結形成される安全性メッセージの書き込みの前に都合良く実行されることが可能であるアクセス・インターロック試験は、例えば、以下の手順に基づいて形成される。

【００５４】

マイクロコントローラ１１がＤＰＭ３０内のすべてのメモリ場所に初期設定値、例えばＦＦｈを書き込むことを試みる。

【００５５】

その後、マイクロコントローラ２１がＤＰＭ３０内のすべてのメモリ場所にさらなる初期設定値、例えば００ｈを書き込むことを試みる。

【００５６】

その後、マイクロコントローラ１１がＤＰＭ３０内のすべてのメモリ場所を読み取り、マイクロコントローラ２１に割り当てられるそれらのメモリ場所だけに値００ｈが記入されたかどうか、および可能であればマイクロコントローラ１１に割り当てられるメモリ場所に値ＦＦｈが記入されたかどうかをチェックする。その後、マイクロコントローラ１１は再度値ＦＦｈをすべてのメモリ場所に書き込むことを試みる。

【００５７】

その後、マイクロコントローラ２１がＤＰＭ３０内のすべてのメモリ場所を読み取り、マイクロコントローラ１１に割り当てられるそれらのメモリ場所だけに値ＦＦｈが記入されたかどうか、および可能であればマイクロコントローラ２１に割り当てられるメモリ場所に値００ｈが記入されたかどうかをチェックする。

【００５８】

もしもこの予期される挙動に誤りもしくは不具合が発生すれば、その誤りもしくは不具合が識別され、安全性ベースのプロトコルが起動させられ、例えば処理が安全な状態へと変化する。そうでなければ、アクセス・インターロックが正しく動作していると想定されることが可能である。したがって本発明による実施の１つの主な特徴は、それぞれのマイクロコントローラ１１または２１から出る実際の書き込み信号が直接使用されることはないが、その代わりにアドレスとの接続処理が実行されることである。したがって、それぞれのマイクロコントローラに割り当てられるアドレスだけに書き込むことが可能である。

【００５９】

その結果、ＤＰＭ３０内のＲＡＭに保存されるデータは極めて高度に安全なプロトコル

によって保護される。送信チャネル自体と同様の方式で、ＤＰＭ３０は安全であるとは見なされない。したがって、とりわけ図２のＭで注記される領域内のデータの構成および内容に関する予期される挙動に基づいて安全性が確立される。その結果、ＤＰＭ３０内に一時的に保存されたデータのさらなる処理もしくは分配が、例えば１つのチャネル上でＤＰＭ３０からデータを移送するさらなるマイクロコントローラ３５を介して行なわれることが可能であり、その後、そのデータは例えばフィールド・バス４０の中に入力されることによってバス・システムへと移送される。

【００６０】

自己確認処理を実行することによって、２つのマイクロコントローラ１１および２１はこのようにして自動的にそれぞれのアクセス規則を効果的にモニタし、その一方で安全性メッセージがバッファ貯蔵器３０に書き込まれ、メモリ内に保存されたデータが移送のためのバッファ貯蔵器３０のインターフェースを介して１つのチャネル上でプロトコル・チップ、さらなるマイクロコントローラ、またはいくつかの他の知能ユニットへと移送されることが可能となる。マイクロコントローラ１１または２１内に不具合もしくは故障がある場合にはもはや完全な安全性メッセージを作り出すことが不可能であるので、故障は必然的に識別され、安全性ベースの機能が起動させられる。冗長性アーキテクチャＭの安全性分析はこのようにしてメモリ３０内のデータの保存で終了する。この後、この時点から起こり得る誤りもしくは故障は送信に関してどのようなケースでも従来通り考慮に入れられ、かつ即応されなければならないので、プロトコルの安全性メカニズムが役割を果たすことになる。この目的のために考慮中の誤りもしくは故障は基本的に、「安全性関連メッセージの送信のためのバス・システム」の検査と確認に関するメッセージの破損である。

【００６１】

連結形成される安全プロトコル内の書き込まれる位置と書き込み権限の上述の無条件の結びつき、および両方のマイクロコントローラの無制限の読み取り権限はこのようにして、バス４０を介した実際の送信の前にまさに標準部品の使用により、送信される安全性メッセージの比較および確認を保証する。その結果、マイクロコントローラ１１または２１は勝手に安全性メッセージを送ることが不可能である。

【００６２】

図２に例示された機能回路図はこのようにしてまさに単純な論理回路によって作り出されることが可能であるが、しかし例えばＦＰＧＡによって形成されることもやはり可能である。さらに、もちろんであるが図２に例示されたようなＤＰＭ３０ではなく、単純な標準ＲＡＭを使用することもやはり可能である。しかしながら、ＤＰＭの使用はバッファ貯蔵器から安全性メッセージを読み取る処理に関して回路を単純化する。当業者にとって、図２に例示された回路配列が明白な書き込みアクセス権限のための考え得る技術的実行例の１つに過ぎないことは明らかである。例を挙げると、一方のコンピュータがバッファ貯蔵器の上側データ・ライン上でのみ書き込みアクセスを行なうことが可能となり、冗長コンピュータが下側データ・ライン上でのみ書き込みアクセスを行なうことが可能となるようにデータ・ラインが分割されることもやはり可能である。さらに、本発明による書き込みアクセス規則は２つよりも多くの冗長コンピュータ／処理チャネルに関して使用されることが可能である。

【図面の簡単な説明】

【００６３】

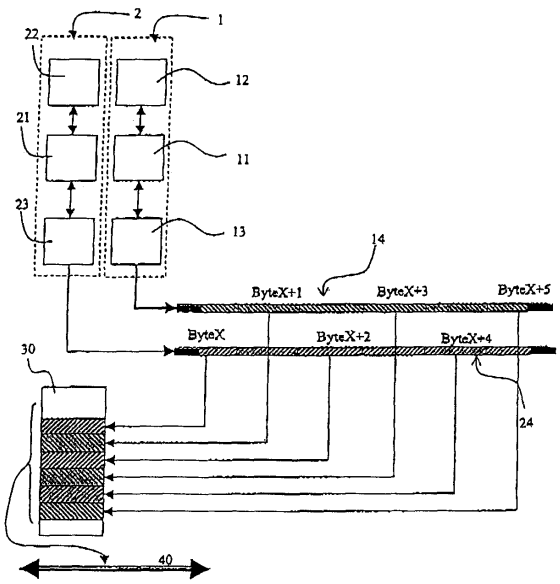
【図１】冗長処理チャネルによって送信される安全性メッセージのための安全性ベースのプロトコルの冗長的形成、およびそれに続く、各々のケースで安全性ベースのプロトコルから移譲／移送される構成要素に関する、移送／移譲規則の制御下での同一の安全性ベースのプロトコルの連結形成に関して概要を示す概略図である。

【図２】各々が完全な安全性ベースのプロトコルを冗長的に見積もる２つのマイクロコントローラに基づき、本発明の導入に関して考え得る１つの機能回路を示す図である。

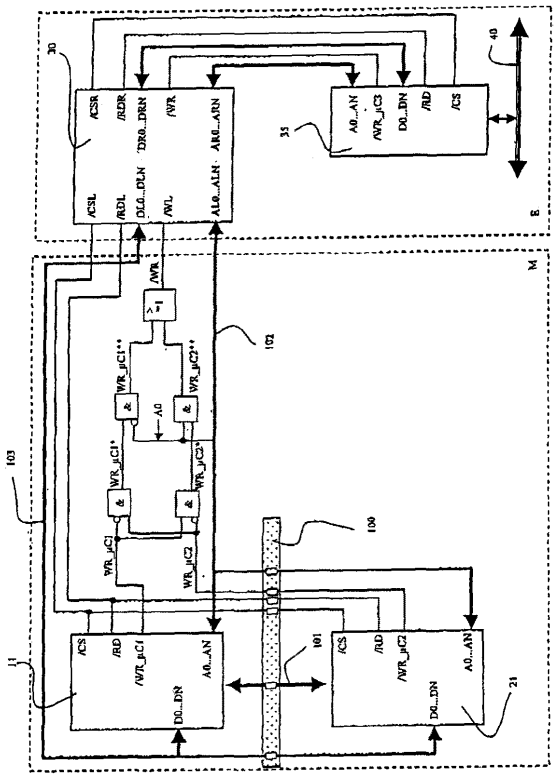
【図３】２チャネル形式から１チャネル形式への変更のための知られている実行例を示す図である。

【図４】２チャネル形式から１チャネル形式への変更のための知られている実行例を示す図である。

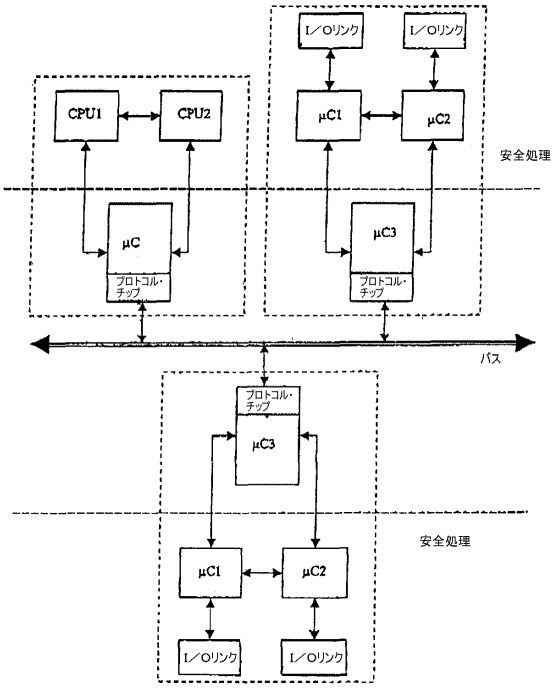
【図１】



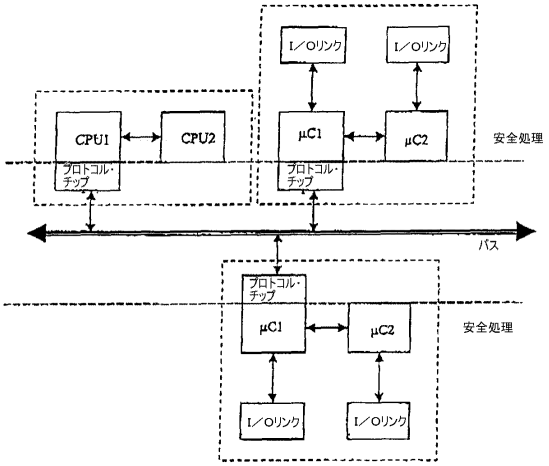
【図２】



【図３】


L／Oリンク
L／Oリンク
CPU1
CPU2
μC1
μC2
安全処理
μC
プロトコル・チップ
μC3
プロトコル・チップ
バス
プロトコル・チップ
μC3
安全処理
μC1
μC2
L／Oリンク
L／Oリンク

【図４】


L／Oリンク
L／Oリンク
CPU1
CPU2
μC1
μC2
安全処理
プロトコル・チップ
プロトコル・チップ
バス
プロトコル・チップ
μC1
μC2
安全処理
L／Oリンク
L／Oリンク

フロントページの続き

(72)発明者　ハインツーカルステン　ランドヴェール
ドイツ国，３２６５７　レムゴ，ホルンシェア　ヴェグ　６ツェー
(72)発明者　ヴィクトル　オステル
ドイツ国，３２８２５　ブロムベルク，ブナーベルクヴェグ　９
(72)発明者　ライナー　エシュ
ドイツ国，３２８２５　ブロムベルク，フリーダーヴェグ　９

合議体
審判長　清水　稔
審判官　甲斐　哲雄
審判官　和田　志郎

(56)参考文献　特開平４－１０３２４１（ＪＰ，Ａ）
特開２００４－１４５７４６（ＪＰ，Ａ）
特開平１０－３０７６０３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 13/00