(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5645921号
(P5645921)
(45)発行日　平成26年12月24日(2014.12.24)　(24)登録日　平成26年11月14日(2014.11.14)

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

請求項の数 13　(全 18 頁)

(21)出願番号	特願2012-506392 (P2012-506392)
(86)(22)出願日	平成22年4月20日 (2010.4.20)
(65)公表番号	特表2012-524353 (P2012-524353A)
(43)公表日	平成24年10月11日 (2012.10.11)
(86)国際出願番号	PCT/EP2010/002436
(87)国際公開番号	WO2010/121796
(87)国際公開日	平成22年10月28日 (2010.10.28)
審査請求日	平成25年2月8日 (2013.2.8)
(31)優先権主張番号	102009019087.2
(32)優先日	平成21年4月20日 (2009.4.20)
(33)優先権主張国	ドイツ(DE)

前置審査

(73)特許権者　501493037
ピルツ　ゲーエムベーハー　アンド　コー．カーゲー
ドイツ連邦共和国，Ｄ－７３７６０　オストフィルデルン，フェーリクス－ヴァンケル－シュトラーセ　２番地
(74)代理人　100087701
弁理士　稲岡　耕作
(74)代理人　100101328
弁理士　川崎　実夫
(74)代理人　100149766
弁理士　京村　順二
(74)代理人　100110799
弁理士　丸山　温道

最終頁に続く

(54)【発明の名称】安全関連制御ユニットおよび自動化設備の制御方法

(57)【特許請求の範囲】
【請求項１】
安全関連制御ユニットの内部で実行するアプリケーションプログラム（３４）に従って自動化設備（１２）を制御するための前記安全関連制御ユニットにおいて、前記自動化設備（１２）が複数のセンサ（１６）および複数のアクチュエータ（１４）を備え、前記アプリケーションプログラム（３４）が前記アクチュエータ（１４）を制御するための複数の制御命令（４４，４６，４８）を含み、
複数の第１プログラム変数を処理することにより前記制御命令の少なくとも一部（４４）を実行するように設計されている第１プロセッサ（２０）であって、第１の規定タイミングに少なくとも１つの前記第１プログラム変数（ＦＳＶ１Ａ）に対して存在する瞬時値（ＦＳＶ１Ａ（ｎ））に応じて前記第１プログラム変数（ＦＳＶ１Ａ）の第１試験値（ＣＲＣＦＳＶ１Ａ（ｎ））を決定するように設計されている第１プロセッサ（２０）と、
複数の第２プログラム変数を処理することにより前記制御命令の少なくとも一部（４８）を実行するように設計されている第２プロセッサ（２２）であって、さらに前記第１試験値（ＣＲＣＦＳＶ１Ａ（ｎ））に対応する第２試験値（ＣＲＣＦＳＶ１Ｂ（ｎ））を決定するように設計されている第２プロセッサ（２２）と、
前記瞬時値（ＦＳＶ１Ａ（ｎ））、前記第１試験値（ＣＲＣＦＳＶ１Ａ（ｎ））、および前記第２試験値（ＣＲＣＦＳＶ１Ｂ（ｎ））を、ゼロ電圧保護データとして記憶するように設計されている１つの不揮発性データメモリ（９２）と、を備え、
再始動中に、前記第１プロセッサ（２０）により前記第１試験値（ＣＲＣＦＳＶ１Ａ（

ｎ））に対する前記瞬時値（ＦＳＶ１Ａ（ｎ））の妥当性を確認するとともに、前記第２プロセッサ（２２）により前記第２試験値（ＣＲＣＦＳＶ１Ｂ（ｎ））に対する前記瞬時値（ＦＳＶ１Ａ（ｎ））の妥当性を確認するように設計されていることを特徴とする安全関連制御ユニット。

【請求項２】

前記第２プロセッサ（２２）が、さらに前記第２プログラム変数（ＦＳＶ１Ｂ）の１つのうちの前記第１プログラム変数（ＦＳＶ１Ａ）に対応する前記第２プログラム変数（ＦＳＶ１Ｂ）の瞬時値（ＦＳＶ１Ｂ（ｎ））に応じて前記第２試験値（ＣＲＣＦＳＶ１Ｂ（ｎ））を決定するように設計されていることを特徴とする、請求項１に記載の安全関連制御ユニット。

【請求項３】

前記第１プログラム変数（ＦＳＶ１Ａ）の瞬時値（ＦＳＶ１Ａ（ｎ））および前記第２プログラム変数（ＦＳＶ１Ｂ）の瞬時値（ＦＳＶ１Ｂ（ｎ））が同じタスクサイクル（ｎ）に由来することを特徴とする、請求項２に記載の安全関連制御ユニット。

【請求項４】

前記２つの試験値（ＣＲＣＦＳＶ１Ａ（ｎ），ＣＲＣＦＳＶ１Ｂ（ｎ））を異なる方法で決定するように設計されていることを特徴とする、請求項１～請求項３のいずれか１項に記載の安全関連制御ユニット（１０）。

【請求項５】

前記２つの試験値（ＣＲＣＦＳＶ１Ａ（ｎ），ＣＲＣＦＳＶ１Ｂ（ｎ））を連続するタイミングに対して繰り返し決定するように設計されていることを特徴とする、請求項１～請求項４のいずれか１項に記載の安全関連制御ユニット（１０）。

【請求項６】

前記第１プロセッサ（２０）がさらに瞬時値比較を行うように設計されていることを特徴とする、請求項１～請求項５のいずれか１項に記載の安全関連制御ユニット。

【請求項７】

前記データメモリ（９２）が前記第１プログラム変数（１１６）に割り当てられた２つの記憶領域（１３０，１３２）を備えたことを特徴とする、請求項１～請求項６のいずれか１項に記載の安全関連制御ユニット。

【請求項８】

前記瞬時値（ＦＳＶ１Ａ（ｎ））および前記２つの試験値（ＣＲＣＦＳＶ１Ａ（ｎ），ＣＲＣＦＳＶ１Ｂ（ｎ））を前記２つの記憶領域（１３０，１３２）に交互に記憶させるように設計されていることを特徴とする、請求項７に記載の安全関連制御ユニット（１０）。

【請求項９】

前記２つのプロセッサ（２０，２２）の少なくとも一方が書き込みカウンタ（ＳＺＡ，ＳＺＢ）の値（ＳＺＡ（ｎ），ＳＺＢ（ｎ））を決定するように設計されていることを特徴とする、請求項１～請求項８のいずれか１項に記載の安全関連制御ユニット。

【請求項１０】

前記第１プロセッサ（２０）が前記瞬時値（ＦＳＶ１Ａ（ｎ））および前記書き込みカウンタ（ＳＺＡ）の値（ＳＺＡ（ｎ））に応じて前記第１試験値（ＣＲＣＦＳＶ１Ａ（ｎ））を決定するようにも設計されていることを特徴とする、請求項９に記載の安全関連制御ユニット。

【請求項１１】

前記第１および第２のプログラム変数がそれぞれ安全関連プログラム変数であることを特徴とする、請求項１～請求項１０のいずれか１項に記載の安全関連制御ユニット。

【請求項１２】

第１プロセッサ（２０）と第２プロセッサ（２２）とを含む安全関連制御ユニットを用いて、自動化設備（１２）を制御するための方法において、前記設備（１２）が複数のセンサ（１６）および複数のアクチュエータ（１４）を備え、

前記第１プロセッサ（２０）を用いて複数の第１プログラム変数を処理するステップと、

前記第１プロセッサ（２０）を用いて第１の規定タイミングに少なくとも１つの前記第１プログラム変数（ＦＳＶ１Ａ）に対して存在する瞬時値（ＦＳＶ１Ａ（ｎ））に応じて前記第１プログラム変数（ＦＳＶ１Ａ）の第１試験値（ＣＲＣＦＳＶ１Ａ（ｎ））を決定するステップと、

前記第２プロセッサ（２２）を用いて複数の第２プログラム変数を処理するステップと、

前記第２プロセッサ（２２）を用いて前記第１試験値（ＣＲＣＦＳＶ１Ａ（ｎ））に対応する第２試験値（ＣＲＣＦＳＶ１Ｂ（ｎ））を決定するステップと、

前記瞬時値（ＦＳＶ１Ａ（ｎ））、前記第１試験値（ＣＲＣＦＳＶ１Ａ（ｎ））、および前記第２試験値（ＣＲＣＦＳＶ１Ｂ（ｎ））をゼロ電圧保護データとして、１つの不揮発性データメモリ（９２）に記憶させるステップと、

再始動中に、前記安全関連制御ユニットを用いて、前記第１プロセッサ（２０）により前記第１試験値（ＣＲＣＦＳＶ１Ａ（ｎ））に対する前記瞬時値（ＦＳＶ１Ａ（ｎ））の妥当性を確認するとともに、前記第２プロセッサ（２２）により前記第２試験値（ＣＲＣＦＳＶ１Ｂ（ｎ））に対する前記瞬時値（ＦＳＶ１Ａ（ｎ））の妥当性を確認するステップと、を含むことを特徴とする方法。

【請求項１３】

請求項１～請求項１１のいずれか１項に記載の安全関連制御ユニット（１０）上でのプログラムコード実行時に請求項１２に記載の方法を実行するように設計されている前記プログラムコードを有するデータ媒体を備えたコンピュータプログラム製品。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、内部で実行するアプリケーションプログラムに従って自動化設備を制御するための安全関連制御ユニットであって、前記設備が複数のセンサおよび複数のアクチュエータを備え、前記アプリケーションプログラムが前記アクチュエータを制御するための複数の制御命令を含むことを特徴とする安全関連制御ユニットに関する。

また、本発明は、複数のセンサおよび複数のアクチュエータを備えた自動化設備を制御するための方法に関する。

【０００２】

本発明における安全関連制御ユニットは、センサからの入力信号を受信し、論理の組み合わせおよび場合によっては他の信号処理ステップまたはデータ処理ステップによって、これら入力信号から出力信号を生成する装置またはデバイスである。出力信号はアクチュエータに供給可能であり、入力信号に基づいて制御される設備中で動作または反応を起こすことができる。

【背景技術】

【０００３】

このような安全関連制御ユニットの好適な応用分野としては、機械の安全性の分野における緊急停止押しボタン、両手コントローラ、防護ドア、またはライトグリッドのモニタリングが挙げられる。そのようなセンサは、作動中に人間または有形財に対する危険を伴う機械の保護等に使用する。防護ドアが開かれたり、または緊急停止押しボタンが操作されたりすると、個別の信号が生成され、入力信号として安全関連制御ユニットに供給される。安全関連制御ユニットは、これに応答して、アクチュエータ等により危険を生じている機械の部分を停止させる。

【０００４】

安全関連制御ユニットは、「一般的な」制御ユニットとは対照的に、内部または接続された装置に異常が発生した場合でも、危険を生じている設備または機械の安全状態を常に確保する点が特徴である。このため、安全関連制御ユニットの場合には、それ自体のフェ

イルセーフ性の観点から極めて高い要求が課せられており、開発および製造にかかるコストが大幅に高くなってしまう。

【０００５】

安全関連制御ユニットは通例、専門職協会またはいわゆるドイツの

TÜV

【０００６】

等に相当する監督機関からの特別な承認を得る必要がある。この場合、安全関連制御ユニットは、たとえば欧州規格ＥＮ９５４－１、ＩＥＣ６１５０８もしくはＥＮ　ＩＳＯ１３８４９－１、またはこれらに相当する規格に規定された所定の安全基準を満たす必要がある。以下では、安全関連制御ユニットが少なくとも前記欧州規格ＥＮ９５４－１の安全カテゴリ３またはＩＥＣ６１５０８にかかる安全度水準（ＳＩＬ）２を満たす装置またはデバイスであるものとする。

【０００７】

プログラム可能な安全関連制御ユニットであれば、ユーザは、アプリケーションプログラムと呼ばれるソフトウェアを用いることにより、必要に応じて論理の組み合わせおよび場合によっては別の信号処理ステップまたはデータ処理ステップを個別に定義することができる。この結果、様々な安全関連モジュール間の規定のハードワイヤ結線により論理の組み合わせが生成された初期のソリューションに比べて、柔軟性は大幅に高くなる。たとえば、アプリケーションプログラムは、市販のパソコン（ＰＣ）およびしかるべきソフトウェアプログラムを用いて生成可能である。

【発明の概要】

【発明が解決しようとする課題】

【０００８】

前述した通り、安全関連制御ユニットには、フェイルセーフ性の観点から極めて高い要求が課せられる。たとえば、そのアプローチとして、少なくともプロセッサ等のデータ処理コンポーネントでは安全関連制御ユニットを冗長設計とすることが考えられる。これにより、発生する故障を考慮して、安全関連制御ユニットを最大限に利用することが可能となる。同様に、安全関連制御ユニットの外部で発生する可能性がある故障についても考慮して、安全関連制御ユニットの可用性を高くすることが望ましい。たとえば、電圧故障の後、安全関連制御ユニットは、電圧故障発生前に想定された状態で問題なく再作動しなければならない。しかし、とくに安全関連制御ユニットの外部で故障が発生した場合の可用性に関して、安全関連制御ユニットは未だ最適化されていない。

【０００９】

そこで、本発明は、安全関連制御ユニットの外部で発生した故障に対する適用性を高めると同時にコストを低減するための、安全関連制御ユニットおよび方法を提供することを目的とする。

【課題を解決するための手段】

【００１０】

本発明の目的は、複数の第１プログラム変数を処理することにより制御命令の少なくとも一部を実行するように設計されている第１プロセッサであって、第１の規定タイミングに少なくとも１つの前記第１プログラム変数に対して存在する瞬時値に応じて前記第１プログラム変数の第１試験値を決定するように設計されている第１プロセッサと、複数の第２プログラム変数を処理することにより前記制御命令の少なくとも一部を実行するように設計されている第２プロセッサであって、前記第１試験値に対応する第２試験値を決定するように設計されている第２プロセッサと、前記瞬時値、前記第１試験値、および前記第２試験値を記憶するように設計されているデータメモリと、を備えたことを特徴とする冒頭に記載した種類の安全関連制御ユニットによって達成される。

【００１１】

また、本目的は、複数の第１プログラム変数を処理するステップと、第１の規定タイミ

ングに少なくとも１つの前記第１プログラム変数に対して存在する瞬時値に応じて前記第１プログラム変数の第１試験値を決定するステップと、複数の第２プログラム変数を処理するステップと、前記第１試験値に対応する第２試験値を決定するステップと、前記瞬時値、前記第１試験値、および前記第２試験値をデータメモリに記憶させるステップと、を含むことを特徴とする冒頭に記載した種類の方法によって達成される。

【００１２】

前記の本発明の安全関連制御ユニットおよび本発明の方法は、プログラム変数の瞬時値と、第１プロセッサにより安全関連制御ユニットの第１チャンネルに対して決定された第１試験値および第２プロセッサにより第２チャンネルに対して決定された第２試験値の両者とをデータメモリに記憶させるという着想に基づいている。したがって、記憶された瞬時値の有効性は、たとえば動作シーケンスの予期せぬ中断後に再始動する場合、両チャンネルで重複して確認可能となる。これにより、安全関連制御ユニットの可用性は高くなる。両試験値が１つのデータメモリに記憶されるため、２つのチャンネルの一方にのみデータメモリを設ければ十分である。２つのチャンネルのそれぞれに対して個別のデータメモリを設ける必要はない。これにより、安全関連制御ユニットの実装コストが低減される。

【００１３】

以上のようにして、上述の目的は完遂される。

本発明の一改良形態においては、前記第２プロセッサが、前記第２プログラム変数のうちの前記第１プログラム変数に対応する第２プログラム変数のうちの１つの瞬時値に応じて前記第２試験値を決定するようにも設計される。

この改良形態の一部の変形例においては、前記第１および第２プログラム変数が、制御される設備の共通の瞬時値を表す相互に冗長なプログラム変数である。この改良形態には複数の利点がある。まず、２つの試験値が個別に独立して決定される。この結果、記憶された瞬時値が有効か否かの確認の信頼性がより高くなる。また、２つのチャンネルのそれぞれに対して個別の試験値が使用可能である。したがって、記憶された瞬時値の個別の有効性試験および妥当性確認を両チャンネルに対して行うことができる。この冗長性により、安全関連制御ユニットひいては制御される設備の可用性が高くなる。

【００１４】

別の改良形態においては、前記第１プログラム変数の瞬時値および前記第２プログラム変数の瞬時値が同じタスクサイクルに由来する。

各プロセッサは通例、それぞれのプログラム変数を周期的に読み出して各制御プログラムを周期的に実行する。この実施形態では、第１および第２プログラム変数が共通のサイクルに由来するため、概ね同じタイミングに存在する２つの瞬時値を表す。この改良形態では、２つの瞬時値が時間の経過とともに合致するようになって類似性がより高くなるため、有効性試験に対しては一方の瞬時値のみを記憶させれば十分である。これにより、データメモリを費用対効果に優れたサイズとすることができる。タスクサイクルは、第１の規定タイミングにより定義すると都合が良い。

【００１５】

別の改良形態においては、安全関連制御ユニットが前記２つの試験値を異なる方法で決定するように設計される。

この改良形態によれば、有効性試験の信頼性が向上する。安全関連制御ユニットの２つのチャンネルに対しては、異なるアルゴリズムを用いて各試験値を決定するのが好ましい。

【００１６】

別の改良形態においては、前記データメモリが不揮発性データメモリとして設計される。

この改良形態では、とくに予期せぬ中断後に安全関連制御ユニットを再始動する際、記憶された瞬時値および２つの試験値が直ちに利用可能である。したがって、設備の再作動をより迅速に行うことができる。前記データメモリは、いわゆる磁気抵抗メモリ(MRAM: Magneto-resistive Random Access Memory)あるいは強誘電体メモリ(FRAM（登録商標）: F

erroelectric Random Access Memory)として設計するのが好ましい。

【００１７】

別の改良形態においては、安全関連制御ユニットが前記２つの試験値を連続するタイミングに対して繰り返し決定するように設計される。

この改良形態では、記憶された瞬時値が繰り返し更新される。この更新は、一定の時間間隔で発生するのが好ましい。この改良形態は、最新の値で設備を再始動できるため都合が良い。これにより、設備の再始動がより簡単かつ高速になる。

【００１８】

別の改良形態においては、前記第１プロセッサがさらに瞬時値比較を行うように設計される。

この改良形態では、第１プロセッサが異なるタイミングの瞬時値を比較する。この改良形態は、現在の瞬時値および２つの試験値の記憶を最適化する。瞬時値比較は、記憶済みの先行瞬時値と比較して変化があるか否かを調べるために行われる。変化がない場合、現在の瞬時値および２つの現在の試験値が再度記憶されることはない。すなわち、好ましくは、これら値の記憶は、実際に変化があった場合にのみ発生する。この結果、より小さなサイズのデータメモリを使用でき、コスト削減につながる。安全関連制御ユニットの動作に関して、この改良形態により、費用の最適化が図れる。これは、タスクサイクルごとに瞬時値および関連する試験値を記憶させる必要がないためである。

【００１９】

別の改良形態においては、安全関連制御ユニットが、再始動中に前記瞬時値の有効性確認を行うように設計され、前記第１プロセッサにより前記第１試験値に対する前記瞬時値の妥当性を確認するとともに、前記第２プロセッサにより前記第２試験値に対する前記瞬時値の妥当性を確認するように設計される。

この改良形態にはさらに、安全関連制御ユニットの２つのチャンネルの一方のみに対して決定された瞬時値を１つだけ用いて２つのチャンネルに対する有効性試験を実行可能であるという利点がある。この結果、たとえば瞬時値の記憶に要する費用を低減可能である。したがって、データメモリは１つだけ設ければ十分である。このデータメモリは、安全関連プログラム変数および非安全関連プログラム変数の両者が処理される安全関連制御ユニットのチャンネルに割り当てるのが好ましい。

【００２０】

別の改良形態においては、前記データメモリが前記第１プログラム変数に割り当てられた２つの記憶領域を備える。

この改良形態によれば、２つの異なるタイミングひいては２つの異なるタスクサイクルに対して、最近の瞬時値および２つの各々関連する試験値を記憶させることができる。このように、少なくとも２つの異なるタスクサイクルにわたる瞬時値の履歴を前記記憶領域に記憶させるのが好ましい。これにより、再始動の場合の制御される設備の可用性はさらに高くなる。最後に記憶された最新の瞬時値が有効ではないために安全関連制御ユニットの初期化に利用できないことが有効性試験中に分かった場合は、以前に記憶されたより古い瞬時値が依然として可用であり、再始動に利用できて都合が良い。

【００２１】

別の改良形態においては、安全関連制御ユニットが前記瞬時値および前記２つの試験値を前記２つの記憶領域に交互に記憶させるように設計される。

この改良形態では、２つの記憶領域を用いて瞬時値の履歴を交互に更新する。この改良形態では、任意のタイミングにおいて、最新の瞬時値（現在のタスクサイクルＺから）を一方の記憶領域に用意し、より古い瞬時値（先行するタスクサイクルＺ－１から）を他方の記憶領域に用意する。そして、この改良形態では、現在の瞬時値が次のタスクサイクルＺ＋１で読み込まれた場合は、その都度、最も古い瞬時値を書き換える。この改良形態では、安全関連制御ユニットの動作にあたって、最小限のメモリ所要量で２つの最新世代の瞬時値が常に記憶されるため、中断後の安全関連制御ユニットの初期化に利用可能である。

【００２２】
別の改良形態においては、前記２つのプロセッサの少なくとも一方が書き込みカウンタの値を決定するように設計される。
書き込みカウンタは、前記２つの記憶領域のいずれに最新の瞬時値が含まれるかをその都度表すため都合が良い。この改良形態によれば、異なるタイミングに存在する多数の瞬時値が前記データメモリに記憶されている場合、これら瞬時値のいずれが最も新しく、最初に有効性確認の対象となるかをより容易に決定することができる。２つの各プロセッサは、それぞれの書き込みカウンタを決定するのが好ましい。これにより、安全関連制御ユニットの可用性はさらに高くなる。
【００２３】
別の改良形態においては、前記第１プロセッサが前記瞬時値および前記書き込みカウンタの値に応じて前記第１試験値を決定するようにも設計される。
この改良形態では、チェックサムの決定において、第１プロセッサが瞬時値のみならず書き込みカウンタの値も考慮に入れる。第１試験値は、以下のように決定するのが好ましい。すなわち、記憶領域の２つの記憶セルに瞬時値および書き込みカウンタの値を記憶させる。そして、この２つの記憶セルの値により第１試験値を決定する。この実施形態には、試験値が瞬時値およびその伝搬の双方を保証するため、設備再始動時の情報の信頼性がさらに向上するという利点がある。
【００２４】
別の改良形態においては、前記第１および第２のプログラム変数がそれぞれ安全関連プログラム変数である。
この改良形態では、再始動および関連する初期化の場合、安全制御命令の処理のために安全関連制御ユニットで必要なプログラム変数の値が利用可能である。これにより、再始動から、設備の動作信頼性が保証される。ただし、前記データメモリには、非安全関連プログラム変数の瞬時値も記憶させることができる。
【００２５】
安全関連制御ユニットの再始動時に利用できるようにデータメモリに記憶させなければならないデータは一般的に、ゼロ電圧保護データと呼ばれる。前述の通り、ゼロ電圧保護データは本質的に安全関連データであり、安全関連プログラム入力変数の瞬時値、安全関連プログラム出力変数の瞬時値、または安全関連中間プログラム変数の瞬時値であってもよい。簡単には、安全関連制御命令の実行中に発生するデータであってもよい。ただし、非安全関連制御命令の実行中に発生する非安全関連データ、すなわち、非安全関連プログラム入力変数の瞬時値、非安全関連プログラム出力変数の瞬時値、または非安全関連中間プログラム変数の瞬時値であってもよい。また、非安全関連データは、設備の始動にも重要と考えられる。一例として、非安全関連カウンタ変数について言及する。この変数の瞬時値は、たとえば、すでにリフトケーブル上にはなくて保管所に収容されているチェアリフトの椅子の数を表す。
【００２６】
前記第１プロセッサは、任意の数の第１プログラム変数に対して、その都度、第１試験値を決定するように設計されていても好ましい。これに対して、前記第２プロセッサは、各第１試験値に対応する第２試験値を決定するように設計されていてもよい。
当然のことながら、上述の特徴および以下に説明する特徴は、本発明の要旨を逸脱しない範囲で、個別に示した組み合わせだけでなく、それ以外の組み合わせまたはそれら自体で使用可能である。
【００２７】
本発明の実施形態を図面に示すとともに、以下に詳細に説明する。
【図面の簡単な説明】
【００２８】
【図１】制御される設備の概略図である。
【図２】データメモリの概略図であって、第１の実施形態にかかるデータ記憶を説明する

ためのものである。
【図３】データメモリの概略図であって、第２の実施形態にかかるデータ記憶を説明するためのものである。
【発明を実施するための形態】
【００２９】
図１においては、安全関連制御ユニットを参照番号１０で示している。安全関連制御ユニット１０は、全体を参照番号１２で示した自動化設備を制御するように設計されている。設備１２は、複数のアクチュエータ１４と複数のセンサ１６とを備えている。一例としては、ロボット等の負荷１８が設備１２に含まれた場合を図示している。
安全関連制御ユニット１０は、セーフティクリティカルなアプリケーションまたはプロセスの制御に必要なフェイルセーフ性を確保するため、２チャンネルの冗長構成となっている。図１には、２チャンネル構成の代表例として、２つの個別プロセッサ、すなわち、第１プロセッサ２０および第２プロセッサ２２を図示している。これら２つのプロセッサ２０，２２は、相互モニタリングおよびデータ交換が可能なように、双方向通信インターフェース２４を介して互いに接続されている。安全関連制御ユニット１０の２つのチャンネルおよび２つのプロセッサ２０，２２は、システマティックエラーを大幅に削減するため、多様な構成、すなわち、互いに異なる構成とするのが好ましい。
【００３０】
２つの各プロセッサ２０，２２に接続された入出力ユニットを参照番号２６で示す。入出力ユニット２６は、センサ１６から制御入力信号２８を受け取り、しかるべきデータフォーマットで２つの各プロセッサ２０，２２に転送する。さらに、入出力ユニット２６は、各プロセッサ２０，２２に応じて、アクチュエータ１４の駆動に用いられる制御出力信号３０を生成する。
【００３１】
参照番号３２は、アプリケーションプログラム３４をマシンコードの形式で記憶させたプログラムメモリを示している。アプリケーションプログラム３４は、安全関連制御ユニット１０によって実行される。また、アプリケーションプログラム３４の全体は、プログラミングツールを活用して作成されるが、まず初めにソースコードが作成され、その後、マシンコードに変換される。このプログラミングツールは、たとえば従来のＰＣ３８上で実行可能なコンピュータプログラム３６である。また、プログラムメモリ３２は、ＳＤカードまたはＣＦカードとして構成するのが好ましい。これにより、ＰＣ３８に直接接続しなくても、アプリケーションプログラム３４を簡単に交換可能である。あるいは、安全関連制御ユニット１０に常設のＥＥＰＲＯＭ等のメモリにアプリケーションプログラム３４を記憶させてもよい。いずれの場合も、プログラムメモリ３２は、ゼロ電圧保護となるように構成される。
【００３２】
安全関連プログラム変数のフェイルセーフ処理を提供するため、プログラムメモリ３２には、第１マシンコード４０および第２マシンコード４２が記憶されている。第１マシンコード４０は第１プロセッサ２０を対象としており、第２マシンコード４２は第２プロセッサ２２を対象としている。また、第１マシンコード４０には、第１安全コード４４および標準コード４６が含まれる。この第１安全コード４４には、安全関連制御ユニット１０の処理対象である安全タスクの一部として第１プロセッサ２０により実行される安全制御命令が含まれる。また、標準コード４６には、安全関連制御ユニット１０の処理対象である標準タスクの一部として第１プロセッサ２０により実行される標準制御命令が含まれる。第２マシンコード４２には、第２プロセッサ２２により実行される安全制御命令を含む第２安全コード４８が含まれる。これら安全制御命令および標準制御命令は、本明細書中では「制御命令」と総称する。
【００３３】
処理の進展に応じて、一方では第１現行安全制御命令５０が、他方では現行標準制御命令５２が第１プロセッサ２０で実行される。本質的にはこれと同時に、第２プロセッサ２

２では第２現行安全制御命令５４が実行される。
非安全関連制御命令である現行標準制御命令５２の処理の一部として、第１プロセッサ２０と入出力ユニット２６との間では第１非安全関連データ５６が交換される。このプロセスでは、非安全関連プログラム入力変数によって、非安全関連センサ６０で生成された非安全関連制御入力信号５８の瞬時値が第１プロセッサ２０に供給される。非安全関連センサ６０は、設備の動作シーケンスにはその信号がとくに重要であるが、故障が起きても生命および四肢への即時危険を示すことのないセンサである。たとえば、非安全関連センサは、ワークピースを機械加工するツールの位置を検出する。非安全関連センサ６０は通例、非フェイルセーフ的に構成される。入出力ユニット２６には、非安全関連プログラム出力変数によって、駆動信号として非安全関連アクチュエータ６４に供給された非安全関連制御出力信号６２の瞬時値が供給される。非安全関連アクチュエータ６４は、たとえばモータまたは位置決めシリンダであってもよい。非安全関連制御出力信号６２の瞬時値は、非安全関連制御入力信号５８に応じて、標準制御命令に基づいて決定される。この際、瞬時値が非安全関連中間プログラム変数に割り当てられる中間量の決定が必要となる場合がある。非安全関連中間プログラム変数の瞬時値は、第２非安全関連データ６６によって、メインメモリ６８に供給されて一時的に記憶される。

【００３４】
安全関連制御命令である第１現行安全制御命令５０の処理の一部として、第１プロセッサ２０と入出力ユニット２６との間では第１安全関連データ７０が交換される。このプロセスでは、安全関連プログラム入力変数によって、安全関連センサ７４で生成された安全関連制御入力信号７２の瞬時値が第１プロセッサ２０に供給される。安全関連センサ７４は、たとえば緊急停止押しボタン、防護ドアスイッチ、ライトグリッド、回転速度モニタリング装置、または安全関連パラメータを記録するその他のセンサである。

【００３５】
入出力ユニット２６には、安全関連プログラム出力変数によって、駆動信号として安全関連アクチュエータ７８に供給された安全関連制御出力信号７６の瞬時値が供給される。安全関連アクチュエータ７８は、たとえば、常時開接点が電源８０と負荷１８との間に接続配置された回路遮断器であって、危険な駆動を確実に停止可能な安全関連電磁バルブ等のアクチュエータである。したがって、負荷１８の電源８０は遮断可能であり、その結果、対応する異常の発生時には少なくとも負荷１８を安全状態に移行させることができる。安全関連制御出力信号７６の瞬時値は、安全関連制御入力信号７２に応じて、安全制御命令に基づいて決定される。この際、瞬時値が安全関連中間プログラム変数に割り当てられる安全関連中間量の決定が必要となる場合がある。安全関連中間プログラム変数の瞬時値は、第２安全関連データ８２によって、メインメモリ６８に供給されて一時的に記憶される。

【００３６】
安全関連制御命令である第２現行安全制御命令５４の処理の一部として、その手順は第１現行安全制御命令５０に従う。この第２現行安全制御命令５４に関しては、第１安全関連データ７０に対応する第３安全関連データ８４および第２安全関連データ８２に対応する第４安全関連データ８６が対応するものとして用いられる。
したがって、第１プロセッサ２０は、複数の第１プログラム変数を論理的に組み合わせて、アプリケーションプログラムの制御命令の少なくとも一部を実行するように設計されている。この第１プロセッサ２０は、チャンネルＡと表される第１チャンネル８８の一部である。また、第２プロセッサ２２は、複数の第２プログラム変数を処理して、アプリケーションプログラムの制御命令の少なくとも一部を実行するように設計されている。この第２プロセッサ２２は、チャンネルＢと表される第２チャンネル９０の一部である。

【００３７】
安全関連制御ユニット１０には、ゼロ電圧保護データを記憶させるためのデータメモリ９２が存在する。ゼロ電圧保護データは、たとえば電圧故障後に安全関連制御ユニット１０を作動させた場合の制御される設備１２の始動時になくてはならないデータである。こ

のデータメモリ９２は、不揮発性データメモリとして設計され、第１プロセッサ２０、すなわち、安全制御命令および標準制御命令の両者を処理するプロセッサに割り当てられている。このことには、第１プロセッサ２０が処理する安全関連データおよび非安全関連データを簡単な方法でデータメモリ９２に記憶させることができるという利点がある。第２プロセッサ２２で処理されてデータメモリ９２に記憶される安全関連データは、双方向通信インターフェース２４を介して第１プロセッサ２０に供給されて、データメモリ９２に書き込まれる。これに対応する逆の手順で、データメモリ９２に記憶されたデータが第２プロセッサ２２に戻される。データメモリ９２を第１プロセッサ２０に割り当てることは、限定的な効果を意図したものではない。データメモリ９２を第２プロセッサ２２に割り当てることも考えられる。同様に、両プロセッサ２０，２２から直接データメモリ９２にアクセス可能とすることも考えられる。

【００３８】

データのデータメモリ９２への書き込みおよびデータのデータメモリ９２からの読み出しは、それぞれ矢印９４および９６で表される。実際にどのデータをデータメモリ９２に書き込んで記憶させるかについては、図２および図３を参照して説明する。

試験信号９８は、入出力ユニット２６を介して、安全関連制御ユニット１０、安全関連センサ７４、および安全関連アクチュエータ７８の間で交換される。安全関連制御ユニット１０では、試験信号９８を用いて、接続されたコンポーネントが故障なく動作しているか否かを判定することができる。この判定が必要なのは、安全関連制御ユニット１０に接続された装置に異常が発生した場合に、制御される設備１２の安全状態を直ちに保証しなければならないためである。

【００３９】

安全関連制御出力信号７６の瞬時値は、上述の内容に従って、第１プロセッサ２０および第２プロセッサ２２の両者により生成されるが、これら２つのプロセッサ２０，２２で生成された瞬時値が制御出力信号７６として同時に出力されることを意味するものではない。上述の内容は、処理対象の安全タスクに関して冗長な安全関連制御ユニット１０の構成を再現することのみを意図したものである。

【００４０】

両プロセッサ２０，２２は、安全関連制御出力信号７６の瞬時値を決定するように設計されている。安全関連制御ユニット１０が故障なく動作している間は、第１プロセッサ２０等のプロセッサにより決定された値のみが出力される。非安全関連制御命令および安全関連制御命令の両者は、図２で選択した構成に従って、安全関連制御ユニット１０で処理されるが、この構成は限定的な効果を意図したものではない。安全関連制御ユニット１０は、安全関連制御命令を排他的に処理するように設計することも可能である。

【００４１】

図２は、第１の実施形態にかかる様々な値が記憶されるデータメモリ９２を示したものである。データメモリ９２は、安全関連プログラム変数を記憶するための第１下位記憶領域１１０を備える。さらに、データメモリ９２は、非安全関連プログラム変数を記憶するための第２下位記憶領域１１２を備える。このデータメモリ９２の構成は、限定的な効果を意図したものではない。それぞれ安全関連プログラム変数用および非安全関連プログラム変数用に２つの独立構成のデータメモリを設けることも可能である。

【００４２】

図１を参照して前述した通り、安全関連制御ユニット１０は、２チャンネルの冗長構成となっている。参照番号１１４は、第１チャンネル８８における複数の第１安全関連プログラム変数の処理を示している。第１チャンネル８８で処理される第１安全関連プログラム変数の１つとして、安全関連プログラム変数ＦＳＶ１Ａを参照番号１１６で示す。この場合、命名した名称には以下の意味がある。すなわち、ＦＳは「フェイルセーフ(Fail-safe)」を表し、この変数が安全関連プログラム変数であることを示している。Ｖ１は、考慮する安全関連プログラム変数の実際の名称であって、この名称により、第１プロセッサ２０で処理される複数の第１安全関連プログラム変数の中で識別可能である。文字Ａは、

この変数が第１チャンネル８８で処理されるプログラム変数であることを示している。この命名法は、図２および図３において一律に使用されている。

【００４３】

参照番号１１８は、第１チャンネル８８で使用される書き込みカウンタＳＺＡを示している。この場合、書き込みカウンタＳＺＡの値は、安全関連プログラム変数ＦＳＶ１Ａの瞬時値を第１下位記憶領域１１０に書き込む書き込みプロセスの数を規定する。参照番号１２０は、安全関連プログラム変数ＦＳＶ１Ａに対して第１チャンネル８８で行われる試験値決定ＣＲＣＦＳＶ１Ａを示している。文字列ＣＲＣ（Cyclic Redundancy Check：巡回冗長検査）は、この試験値決定がＣＲＣプロセスに従って発生することを示している。

【００４４】

参照番号１２２は、第２チャンネル９０における複数の第２安全関連プログラム変数の処理を示している。第２チャンネル９０で処理される第２安全関連プログラム変数の１つとして、安全関連プログラム変数ＦＳＶ１Ｂを参照番号１２４で示す。文字Ｂは、このプログラム変数が第２チャンネル９０で処理されるプログラム変数であることを示している。参照番号１２６は、第２チャンネル９０で使用される書き込みカウンタＳＺＢを示している。この場合、書き込みカウンタＳＺＢの値は、書き込みカウンタＳＺＡの値に対応する。参照番号１２８は、安全関連プログラム変数ＦＳＶ１Ｂに対して第２チャンネル９０で行われる試験値決定ＣＲＣＦＳＶ１Ｂを示している。

【００４５】

この場合、安全関連プログラム変数ＦＳＶ１Ｂは、安全関連プログラム変数ＦＳＶ１Ａに対応する。これは、以下のことを意味している。

すなわち、図１を参照して前述した通り、プログラムメモリ３２には、第１チャンネル８８用の第１マシンコード４０および第２チャンネル９０用の第２マシンコード４２が記憶され、安全関連制御ユニット１０にフェイルセーフ動作を提供している。両マシンコード４０，４２には、独立した安全コード４４，４８がそれぞれ含まれている。これら２つの各安全コード４４，４８を用いて、安全関連センサ７４の同じ安全関連制御入力信号７２が処理され、同じ安全関連アクチュエータ７８に対して安全関連制御出力信号７６が決定される。

【００４６】

この目的のため、これら２つの各安全コード４４，４８には、それぞれのプログラム変数が含まれ、第１安全コード４４には第１安全関連プログラム変数が、第２安全コード４８には第２安全関連プログラム変数が含まれる。第１プログラム変数および第２プログラム変数がそれぞれのメモリの独立した記憶領域を占有するという意味においては互いに独立しているものの、これら２つの安全コード４４，４８には、対ごとに対応するプログラム変数が含まれる。したがって、第１安全コード４４および第２安全コード４８にはそれぞれ、たとえば同じ緊急停止押しボタンによって生成されたセンサ信号の瞬時値を読み込み可能な安全関連プログラム入力変数が含まれる。このことは、安全関連プログラム出力変数および場合によって必要となる安全関連中間プログラム変数にも同じように当てはまる。

【００４７】

そして、第１下位記憶領域１１０には、安全関連プログラム変数ＦＳＶ１Ａの瞬時値、書き込みカウンタＳＺＡの値、ならびに２つの試験値決定ＣＲＣＦＳＶ１ＡおよびＣＲＣＦＳＶ１Ｂによって決定された試験値が以下のように記憶される。この第１下位記憶領域には、２つの記憶領域１３０，１３２が存在する。第１の規定タイミングに存在する第１プログラム変数ＦＳＶ１Ａの瞬時値ＦＳＶ１Ａ（ｎ）は、矢印１３６で示すように、第１記憶領域１３０の第１記憶セル１３４に記憶される。この場合、命名した名称には以下の意味がある。すなわち、追加表記（ｎ）は、これが瞬時値であることを示している。この瞬時値は、タスクサイクルｎ内の第１の規定タイミングに存在する。この場合、タスクサイクルとは、入力画像の更新に始まって、個別の制御命令を実行し、出力画像の提供に至るアプリケーションプログラムを安全関連制御ユニット１０がひと通り実行するのに必要

な期間である。その結果、たとえば安全関連プログラム入力変数および安全関連プログラム出力変数を用いる場合、これらプログラム変数のタスクサイクルあたりの変更は１回のみであるため、最小時間単位としてタスクサイクルに適応させれば十分である。この意味で、ｎは第１の規定タイミングひいてはそのタイミングが含まれるタスクサイクルを示している。（ｎ－１）という表記は、より古いタイミングひいては先行するタスクサイクルの１つを示し、（ｎ＋１）という表記は、より新しいタイミングひいては後続のタスクサイクルの１つを示す。

【００４８】

第１の規定タイミングに存在する書き込みカウンタＳＺＡの値ＳＺＡ（ｎ）についても、矢印１４０で示すように、第１記憶領域１３０、具体的には第２記憶セル１３８に記憶される。さらに、瞬時値ＦＳＶ１Ａ（ｎ）に応じて試験値決定ＣＲＣＦＳＶ１Ａにより決定された第１試験値ＣＲＣＦＳＶ１Ａ（ｎ）および第２試験値ＣＲＣＦＳＶ１Ｂ（ｎ）は、矢印１４６，１４８で示すように、第１記憶領域１３０の第３記憶セル１４２および第４記憶セル１４４に記憶される。

【００４９】

そして、第２試験値決定ＣＲＣＦＳＶ１Ｂにより決定された第２試験値ＣＲＣＦＳＶ１Ｂ（ｎ）は、第１試験値ＣＲＣＦＳＶ１Ａ（ｎ）に対応する。一方、第２試験値ＣＲＣＦＳＶ１Ｂ（ｎ）は、第１プログラム変数ＦＳＶ１Ａに対応する第２プログラム変数ＦＳＶ１Ｂの瞬時値に応じて決定される。さらに、第２プログラム変数ＦＳＶ１Ｂの瞬時値は、第１プログラム変数ＦＳＶ１Ａの瞬時値ＦＳＶ１Ａ（ｎ）と同じタスクサイクルに存在する。これら２つの試験値ＣＲＣＦＳＶ１Ａ（ｎ）およびＣＲＣＦＳＶ１Ｂ（ｎ）は、多様に決定されるのが好ましい。この目的のため、２つの試験値決定ＣＲＣＦＳＶ１ＡおよびＣＲＣＦＳＶ１Ｂは、ハードウェア技術および／またはソフトウェアにより多様に実行される。

【００５０】

第２記憶領域１３２では、矢印１５８，１６０，１６２，１６４で示すように、より古いタイミングひいては先行するタスクサイクルに対して、第１プログラム変数ＦＳＶ１Ａの瞬時値ＦＳＶ１Ａ（ｎ－１）、書き込みカウンタＳＺＡの値ＳＺＡ（ｎ－１）、第１試験値ＣＲＣＦＳＶ１Ａ（ｎ－１）、および第２試験値ＣＲＣＦＳＶ１Ｂ（ｎ－１）が第５記憶セル１５０、第６記憶セル１５２、第７記憶セル１５４、および第８記憶セル１５６に記憶される。記憶領域１３２に記憶された個々の値は、記憶領域１３０に記憶された対応する値に関して前述した通り、これらに対応して決定されたものである。

【００５１】

記憶セル１３４，１３８，１４２，１５０，１５２，１５４に記憶された値は、第１プロセッサ２０により決定されたものである。記憶セル１４４，１５６に記憶された値は、第２プロセッサ２２により決定されたものである。

第１プログラム変数ＦＳＶ１Ａの瞬時値ならびに試験値決定ＣＲＣＦＳＶ１ＡおよびＣＲＣＦＳＶ１Ｂによって決定された２つの試験値はいずれも、２つの記憶領域１３０，１３２に交互に記憶される。これにより、２つの試験値は、連続するタイミングに対して繰り返し決定されて記憶される。そして、より新しいタイミングひいては次のタスクサイクルについては、このタイミングに存在する瞬時値ＦＳＶ１Ａ（ｎ＋１）ならびに２つの試験値ＣＲＣＦＳＶ１Ａ（ｎ＋１）およびＣＲＣＦＳＶ１Ｂ（ｎ＋１）が記憶領域１３２の対応する記憶セル１５０，１５２，１５４，１５６に記憶される。

【００５２】

データメモリ９２は、安全関連プログラム変数ＦＳＶ１Ａに割り当てられた２つの記憶領域１３０，１３２を有する。上述の手順に従って、さらなる安全関連プログラム変数をデータメモリ９２に記憶させる場合は、これら各プログラム変数に対して２つの記憶領域を備える。

第１プロセッサ２０は、瞬時値比較を行うように設計されていてもよい。この瞬時値比較により、異なるタイミングに存在する安全関連プログラム変数ＦＳＶ１Ａの瞬時値が相

互に比較される。瞬時値比較によって、２つの直接連続するタイミングの瞬時値が同じであることが分かった場合は、より新しい瞬時値およびより新しい２つの試験値の記憶を省略することができる。すなわち、より新しい瞬時値およびより新しい２つの試験値は、このより新しい瞬時値が直前のタイミングに対して存在する瞬時値と異なる場合にのみ記憶される。

【００５３】

前述の通り、たとえば第１試験値ＣＲＣＦＳＶ１Ａ（ｎ）は、瞬時値ＦＳＶ１Ａ（ｎ）に応じて試験値決定ＣＲＣＦＳＶ１Ａにより決定される。これに対して、たとえば第２試験値ＣＲＣＦＳＶ１Ｂ（ｎ）は、瞬時値ＦＳＶ１Ｂ（ｎ）に応じて試験値決定ＣＲＣＦＳＶ１Ｂにより決定される。これは、各試験値が、関連する安全関連プログラム変数の瞬時値に対してのみ決定されることを意味するものと理解できる。あるいは、瞬時値ＦＳＶ１Ａ（ｎ）および書き込みカウンタＳＺＡの値ＳＺＡ（ｎ）から得られる組み合わせに対して第１試験値ＣＲＣＦＳＶ１Ａ（ｎ）が決定されてもよい。第２試験値ＣＲＣＦＳＶ１Ｂ（ｎ）についても同じことが言える。

【００５４】

前記瞬時値、書き込みカウンタの値、および試験値の第１下位記憶領域への記憶は、以下の考察に基づいている。たとえば電圧故障がない限り、すなわち、安全関連制御ユニット１０が故障なく動作している限り、２つの安全関連プログラム変数ＦＳＶ１ＡおよびＦＳＶ１Ｂには、個々のタスクサイクルにおいて同一の瞬時値が含まれる。その結果、データメモリ９２には、安全関連プログラム変数ＦＳＶ１Ａの瞬時値のみを記憶させれば十分である。また、１つのタスクサイクル内では、２つの書き込みカウンタＳＺＡおよびＳＺＢにも同一の値が含まれる。

【００５５】

このように、２つのチャンネル８８，９０に対して個別に決定された２つの試験値によって、データメモリ９２に最後に記憶された瞬時値ＦＳＶ１Ａ（ｎ）が有効であるか否かを確認することができる。このため、たとえば電圧故障後に必要となる再始動の場合、第１プロセッサ２０には、瞬時値ＦＳＶ１Ａ（ｎ）および第１試験値ＣＲＣＦＳＶ１Ａ（ｎ）が供給される。

【００５６】

第２プロセッサ２２にも瞬時値ＦＳＶ１Ａ（ｎ）は供給されるが、第２試験値ＣＲＣＦＳＶ１Ｂ（ｎ）は供給されない。安全関連制御ユニット１０が、２つの試験値ＣＲＣＦＳＶ１Ａ（ｎ）およびＣＲＣＦＳＶ１Ｂ（ｎ）が決定され瞬時値ＦＳＶ１Ａ（ｎ）およびこれら２つの試験値のいずれもがデータメモリ９２に記憶された時間窓において故障なく動作していた場合は、現在の第１試験値ＣＲＣＦＳＶ１Ａ（ｎ＋１）および現在の第２試験値ＣＲＣＦＳＶ１Ｂ（ｎ＋１）を繰り返し決定することによって、記憶された第１試験値ＣＲＣＦＳＶ１Ａ（ｎ）と現在の第１試験値ＣＲＣＦＳＶ１Ａ（ｎ＋１）とが同一であるとともに、記憶された第２試験値ＣＲＣＦＳＶ１Ｂ（ｎ）と現在の第２試験値ＣＲＣＦＳＶ１Ｂ（ｎ＋１）とが同一であることが示される。この場合、記憶された瞬時値ＦＳＶ１Ａ（ｎ）は有効で、安全関連制御ユニット１０の初期化に利用可能である。そして、両チャンネル８８，９０では処理が発生することになる。

【００５７】

これに対して、記憶された第１試験値ＣＲＣＦＳＶ１Ａ（ｎ）と現在の第１試験値ＣＲＣＦＳＶ１Ａ（ｎ＋１）とが同一でないか、または記憶された第２試験値ＣＲＣＦＳＶ１Ｂ（ｎ）と現在の第２試験値ＣＲＣＦＳＶ１Ｂ（ｎ＋１）とが同一でないことが判明した場合は、記憶された瞬時値ＦＳＶ１Ａ（ｎ）が無効で、安全関連制御ユニット１０の初期化に利用できない。この場合は、以前に記憶された瞬時値ＦＳＶ１Ａ（ｎ－１）が初期化に代用される。この瞬時値は、初期化に使用する前に、まず有効性試験を行うのが好ましい。これにより、安全関連制御ユニット１０および設備１２は、第１安全関連プログラム変数ＦＳＶ１Ａに対してデフォルト値を使用することなく、また、この目的ために必要な基準動作を実行することなく再始動が可能である。

【００５８】
前記有効性試験においては、書き込みカウンタＳＺＡの値ＳＺＡ（ｎ）およびＳＺＡ（ｎ－１）によって、第１記憶セル１３４および第５記憶セル１５０に記憶された２つの瞬時値のいずれがより新しいかの判定がまず行われる。そして、有効性確認においては、より新しい方の瞬時値の確認がまず行われる。
データメモリ９２は、第１チャンネル８８で処理される非安全関連プログラム変数を記憶するための第２下位記憶領域１１２を有する。
【００５９】
参照番号１６６は、第１チャンネル８８における複数の非安全関連プログラム変数の処理を示している。第１チャンネル８８で処理される第１非安全関連プログラム変数の１つとして、非安全関連プログラム変数ＳＴＶ１Ａを参照番号１６８で示す。この場合、ＳＴは「標準（Ｓｔａｎｄａｒｄ）」を表し、この変数が非安全関連プログラム変数であることを示している。符号Ｖ１および文字Ａの意味については、参照番号１１４を付した処理に関連する記述を参照することができる。参照番号１７０は、非安全関連プログラム変数ＳＴＶ１Ａに対して第１チャンネル８８で行われる試験値決定ＣＲＣＳＴＶ１Ａを示している。
【００６０】
以上から、第２下位記憶領域１１２には、非安全関連プログラム変数ＳＴＶ１Ａの瞬時値、書き込みカウンタＳＺＡの値、および試験値決定ＣＲＣＳＴＶ１Ａによって決定された試験値が以下のように記憶される。すなわち、この第２下位記憶領域１１２には、２つの記憶領域１７２，１７４が存在する。第１の規定タイミングに存在する第１非安全関連プログラム変数ＳＴＶ１Ａの瞬時値ＳＴＶ１Ａ（ｎ）は、矢印１７８で示すように、第３記憶領域１７２の第９記憶セル１７６に記憶される。第１の規定タイミングに存在する書き込みカウンタＳＺＡの値ＳＺＡ（ｎ）についても、矢印１８２で示すように、第１０記憶セル１８０に記憶される。さらに、瞬時値ＳＴＶ１Ａ（ｎ）に応じて試験値決定ＣＲＣＳＴＶ１Ａにより決定された試験値ＣＲＣＳＴＶ１Ａ（ｎ）は、矢印１８６で示すように、第１１記憶セル１８４に記憶される。
【００６１】
第４記憶領域１７４では、矢印１９４，１９６，１９８で示すように、より古いタイミングひいては先行するタスクサイクルに対して、非安全関連プログラム変数ＳＴＶ１Ａの瞬時値ＳＴＶ１Ａ（ｎ－１）、書き込みカウンタＳＺＡの値ＳＺＡ（ｎ－１）、および試験値ＣＲＣＳＴＶ１Ａ（ｎ－１）が第１２記憶セル１８８、第１３記憶セル１９０、および第１４記憶セル１９２に記憶される。第４記憶領域１７４に記憶された個々の値は、第３記憶領域１７２に記憶された対応する値に関して前述した通り、これらに対応して決定されたものである。また、記憶セル１７６，１８０，１８４，１８８，１９０，１９２に記憶された値は、第１プロセッサ２０により決定されたものである。
【００６２】
非安全関連プログラム変数ＳＴＶ１Ａの瞬時値および試験値決定ＣＲＣＳＴＶ１Ａによって決定された試験値はいずれも、２つの記憶領域１７２，１７４に交互に記憶される。そして、より新しいタイミングひいては次のタスクサイクルについては、このタイミングに存在する瞬時値ＳＴＶ１Ａ（ｎ＋１）および試験値ＣＲＣＳＴＶ１Ａ（ｎ＋１）が第４記憶領域１７４の対応する記憶セル１８８，１９０，１９２に記憶される。
【００６３】
データメモリ９２は、非安全関連プログラム変数ＳＴＶ１Ａに割り当てられた２つの記憶領域１７２，１７４を有する。上述の手順に従って、さらなる非安全関連プログラム変数をデータメモリ９２に記憶させる場合は、これら各プログラム変数に対して２つの記憶領域を備える。
非安全関連プログラム変数の記憶は、瞬時値比較を考慮して行うことができる。同様に、試験値の決定においては、書き込みカウンタＳＺＡの値を考慮することができる。最後に記憶された瞬時値ＳＴＶ１Ａ（ｎ）の有効性試験は、安全関連プログラム変数に関して

前述した通り、これに対応して行われる。

【００６４】

上述の内容に対応して、データメモリ９２に最後に記憶された非安全関連プログラム変数ＳＴＶ１Ａの瞬時値ＳＴＶ１Ａ（ｎ）が有効であるか否かを確認することができる。

この目的のため、第１プロセッサ２０には、たとえば安全関連制御ユニット１０の再始動時に瞬時値ＳＴＶ１Ａ（ｎ）および試験値ＣＲＣＳＴＶ１Ａ（ｎ）が供給される。安全関連制御ユニット１０が、試験値ＣＲＣＳＴＶ１Ａ（ｎ）が決定され瞬時値ＳＴＶ１Ａ（ｎ）および試験値ＣＲＣＳＴＶ１Ａ（ｎ）の両者がデータメモリ９２に記憶された時間窓において故障なく動作していた場合は、現在の試験値ＣＲＣＳＴＶ１Ａ（ｎ＋１）を繰り返し決定することによって、記憶された試験値ＣＲＣＳＴＶ１Ａ（ｎ）と現在の試験値ＣＲＣＳＴＶ１Ａ（ｎ＋１）とが同一であることが示される。この場合、記憶された瞬時値ＳＴＶ１Ａ（ｎ）は有効で、安全関連制御ユニット１０の初期化に利用可能である。そして、第１チャンネル８８で処理されることになる。

【００６５】

これに対して、記憶された試験値ＣＲＣＳＴＶ１Ａ（ｎ）と現在の試験値ＣＲＣＳＴＶ１Ａ（ｎ＋１）とが同一でないことが判明した場合は、記憶された瞬時値ＳＴＶ１Ａ（ｎ）が無効で、安全関連制御ユニット１０の初期化に利用できない。この場合は、以前に記憶された瞬時値ＳＴＶ１Ａ（ｎ－１）が初期化に代用される。この瞬時値は、初期化に使用する前に、まず有効性確認を行うのが好ましい。これにより、安全関連制御ユニット１０および設備１２は、非安全関連プログラム変数ＳＴＶ１Ａに対してデフォルト値を使用することなく、また、この目的のために必要な基準動作を実行することなく再始動が可能である。

【００６６】

前記有効性確認においては、書き込みカウンタＳＺＡの値ＳＺＡ（ｎ）およびＳＺＡ（ｎ－１）によって、第９記憶セル１７６および第１２記憶セル１８８に記憶された２つの瞬時値のいずれがより新しいかの判定がまず行われる。そして、有効性確認においては、より新しい方の瞬時値の試験がまず行われる。

第１プロセッサ２０で処理されるプログラム変数は第１プログラム変数と総称し、第２プロセッサ２２で処理されるプログラム変数は第２プログラム変数と総称する。

【００６７】

図３は、データメモリ９２を示しており、第２の実施形態にかかる様々な値が記憶されている。

参照番号１１４’は、第１チャンネル８８における複数の第１安全関連プログラム変数の処理を示しているが、書き込みカウンタＳＺＡを一切考慮に入れていない点が処理１１４とは異なる。これに対応して、参照番号１２２’は、第２チャンネル９０における第２安全関連プログラム変数の処理を示している。また、参照番号１６６’は、第１チャンネル８８における非安全関連プログラム変数の処理を示している。

【００６８】

第５記憶領域２００では、矢印２０８，２１０，２１２で示すように、第１プログラム変数ＦＳＶ１Ａの瞬時値ＦＳＶ１Ａ（ｎ）、第１試験値ＣＲＣＦＳＶ１Ａ（ｎ）、および第２試験値ＣＲＣＦＳＶ１Ｂ（ｎ）が第１５記憶セル２０２、第１６記憶セル２０４、および第１７記憶セル２０６に記憶される。また、第６記憶領域２１４では、矢印２２０，２２２で示すように、非安全関連プログラム変数ＳＴＶ１Ａの瞬時値ＳＴＶ１Ａ（ｎ）および試験値ＣＲＣＳＴＶ１Ａ（ｎ）が第１８記憶セル２１６および第１９記憶セル２１８に記憶される。

【００６９】

記憶セル２０２，２０４，２１６，２１８に記憶された値は、第１プロセッサ２０により決定されたものである。記憶セル２０６に記憶された値は、第２プロセッサ２２により決定されたものである。記憶された個々の値は、図２に関連する記述に従って決定されたものである。

さらなる安全関連プログラム変数をデータメモリ９２に記憶させる場合は、後になるほど、これに対応するより多くの第５記憶領域２００を備える。このことは、非安全関連プログラム変数および第６記憶領域２１４についても当てはまる。同様に、非安全関連プログラム変数および安全関連プログラム変数の記憶は、瞬時値比較を考慮して行うことができる。

【００７０】

記憶された瞬時値ＦＳＶ１Ａ（ｎ）およびＳＴＶ１Ａ（ｎ）の有効性確認は、図２を参照して前述した通りに行われるが、以下のような違いがある。すなわち、たとえば瞬時値ＦＳＶ１Ａ（ｎ）が有効でないことが判明した場合は、瞬時値ＦＳＶ１Ａ（ｎ）と代用可能な第１安全関連プログラム変数ＦＳＶ１Ａの瞬時値がそれ以上データメモリ９２に記憶されることはない。この場合、安全関連制御ユニット１０は、第１安全関連プログラム変数ＦＳＶ１Ａのデフォルト値によって初期化するか、または設備１２の基準動作を実行して初期化しなければならない。このことは、非安全関連プログラム変数ＳＴＶ１Ａにも当てはまる。

【００７１】

ただし、図２を参照して説明した記憶の概念に対して、図３を参照して説明した記憶の概念には、データメモリ９２のサイズを小さくして費用対効果を高めることができるという利点がある。

本願において、非安全関連データの記憶に適用された記憶の概念は、明確な保護の対象とはなっていない。これについては、このような記憶の概念を対象とした発明を達成することが今後の課題である。

【図１】

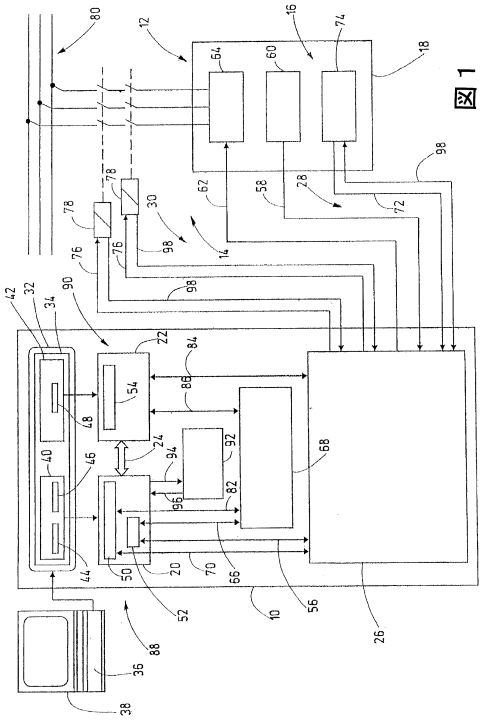

図１

【図２】

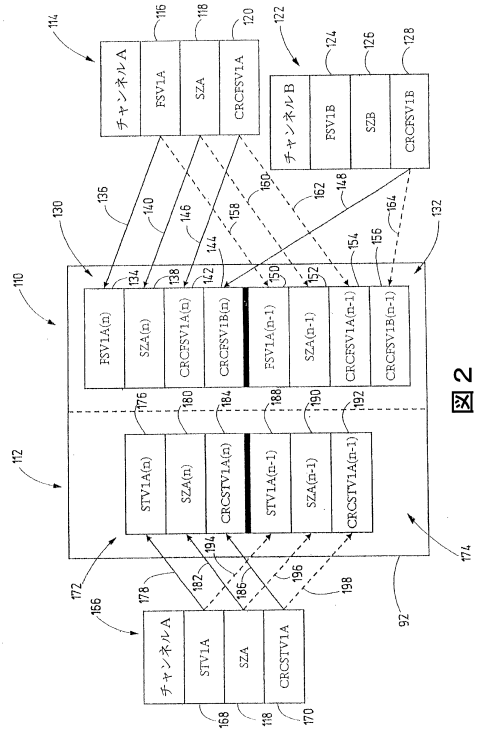

図２

【図３】

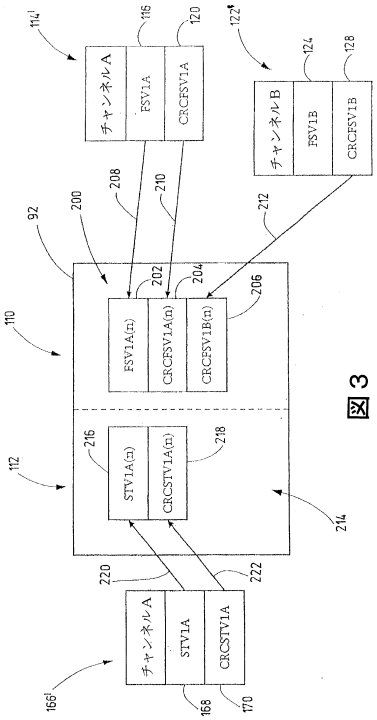
114
116
120
チャンネルA
FSV1A
CRCFSV1A
122
124
128
チャンネルB
FSV1B
CRCFSV1B
208
210
212
92
200
202
204
206
110
FSV1A(n)
CRCFSV1A(n)
CRCFSV1B(n)
216
218
112
STV1A(n)
CRCSTV1A(n)
214
220
222
チャンネルA
STV1A
CRCSTV1A
166
168
170

図３

フロントページの続き

(72)発明者　モースマン，ペーター
ドイツ連邦共和国，７３７６０　オストフィルデルン，フェーリクスーヴァンケルーシュトラーセ
２番地，ピルツ　ゲーエムベーハー　アンド　コー．カーゲー内

審査官　青山　純

(56)参考文献　特開平０９－３１９４０１（ＪＰ，Ａ）
特開平５－２７８８０（ＪＰ，Ａ）
特開平０７－２９５６０２（ＪＰ，Ａ）
特開平２－１１４８２７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０５Ｂ　　９／０３