(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4599013号
(P4599013)
(45)発行日　平成22年12月15日(2010.12.15)　(24)登録日　平成22年10月1日(2010.10.1)

(51)Int.Cl.　F I
H04L 12/40 (2006.01)　H04L 12/40　A

請求項の数 10　(全 15 頁)

(21)出願番号	特願2001-518987(P2001-518987)
(86)(22)出願日	平成12年8月18日(2000.8.18)
(65)公表番号	特表2003-507965(P2003-507965A)
(43)公表日	平成15年2月25日(2003.2.25)
(86)国際出願番号	PCT/EP2000/008062
(87)国際公開番号	WO2001/015385
(87)国際公開日	平成13年3月1日(2001.3.1)
審査請求日	平成19年5月2日(2007.5.2)
(31)優先権主張番号	199 39 919.0
(32)優先日	平成11年8月23日(1999.8.23)
(33)優先権主張国	ドイツ(DE)
(31)優先権主張番号	199 40 874.2
(32)優先日	平成11年8月27日(1999.8.27)
(33)優先権主張国	ドイツ(DE)

(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
(72)発明者　ルップ，ローランド
ドイツ連邦共和国，Ｄ－７３１１０　ハッテンホーヘン，ウーラントシュトラーセ　６３番地

最終頁に続く

(54)【発明の名称】安全ステーションを設定する方法およびそれを利用した安全制御システム

(57)【特許請求の範囲】
【請求項１】
安全制御システム（１０）において、安全バスユーザー（１２、１４、１８～２４）をフィールドバス（１６）に接続する際に安全バスユーザーを設定する方法であって、定義されたユーザーアドレス（９０）が安全バスユーザー（１２、１４、１８～２４）に割り当てられており、
フィールドバス（１６）に接続された管理ユニット（７０）が所定の保守メッセージ（１１０）をフィールドバス（１６）に送出する工程と、
前記保守メッセージ（１１０）を受け取った前記安全バスユーザー（１２、１４、１８～２４）が、所定の広域アドレス（９２）を有する第一の登録メッセージ（１１４）を送出する工程と、
前記管理ユニット（７０）が前記安全バスユーザー（１２、１４、１８～２４）に定義されたユーザーアドレス（９０）を有するアドレス割り当てメッセージ（１１８）を送出する工程と、
前記安全バスユーザー（１２、１４、１８～２４）は、受け取ったユーザーアドレス（９０）を安全バスユーザーのメモリー（５８；１２０）に保存する工程とを含み、
アドレス割り当てメッセージ（１１８）を受け取った後、安全バスユーザー（１２、１４、１８～２４）が定義されたユーザーアドレス（９０）を含む第二の登録メッセージ（１１２）を管理ユニット（７０）に送出することを特徴とする方法。
【請求項２】

安全バスユーザー（１２、１４、１８～２４）は、定義された保守メッセージ（１１０）を初めて受け取った後でのみ、第一の登録メッセージ（１１４）を管理ユニット（７０）に送出し、また定義された保守メッセージ（１１０）を繰り返し受け取った場合は、第二の登録メッセージ（１１２）を管理ユニット（７０）に送出する、請求項１に記載の方法。

【請求項３】

管理ユニット（７０）の特別保守モード（１０６）が起動（１０６）された後でのみ、定義された保守メッセージ（１１０）が送出されることを特徴とする、請求項１または２に記載の方法。

【請求項４】

第二の登録メッセージ（１１２）を受け取った後に、管理ユニット（７０）が特別保守モードを自動的に終了させる（１２２）ことを特徴とする、請求項３に記載の方法。

【請求項５】

特別保守モードの最初に、定義されたユーザーアドレス（９０）が管理ユニット（７０）に送信（１０８）されることを特徴とする、請求項３または４に記載の方法。

【請求項６】

送信されたユーザーアドレス（９０）が、フィールドバス（１６）に接続されたバスユーザー（１２、１４、１８～２４）に既に割り当てられていた場合、管理ユニット（７０）は故障信号（１２８）を発生することを特徴とする、請求項１に記載の方法。

【請求項７】

管理ユニット（７０）は、定義された時間間隔で、フィールドバス（１６）に接続された全てのバスユーザー（１２、１４、１８～２４）に保守メッセージ（１１０）を送出することを特徴とする、請求項１ないし６のいずれかに記載の方法。

【請求項８】

少なくとも第一の登録メッセージ（１１４）とアドレス割り当てメッセージ（１１８）が、それぞれ受領メッセージ（１１６）で応答されることを特徴とする、請求項１ないし７のいずれかに記載の方法。

【請求項９】

フィールドバス（１６）に接続された少なくとも１つの安全バスユーザー（１２、１４、１８～２４）を有する安全性が不可欠なプロセス（２８～３２）を安全に制御する制御システムであって、

安全バスユーザー（１２、１４、１８～２４）はフィールドバス（１６）に接続された管理ユニット（７０）から所定の保守メッセージ（１１０）を受け取りまた評価するための第一の手段（４０）と、当該安全バスユーザー（１２、１４、１８～２４）に割り当てられるユーザーアドレス（９０）を保存するためのメモリー（５８；１２０）とを有し、

安全バスユーザー（１２、１４、１８～２４）は、前記保守メッセージ（１１０）を受け取った後、第一の登録メッセージ（１１４）を前記管理ユニット（７０）に送信することにより、当該安全バスユーザーを所定の広域アドレス（９２）で前記管理ユニット（７０）に登録するための第二の手段（４０、１２０；４０、５８）と、前記管理ユニット（７０）からユーザーアドレス（９０）を有するアドレス割り当てメッセージ（１１８）を受け取りまた評価するための第三の手段（４２、５４）とを含み、

安全バスユーザー（１２、１４、１８～２４）は、前記管理ユニット（７０）からアドレス割り当てメッセージ（１１８）を受け取った後、第二の登録メッセージ（１１２）を管理ユニット（７０）に送出するように構成されており、第二の登録メッセージ（１１２）は定義されたユーザーアドレス（９０）を含むことを特徴とする制御システム。

【請求項１０】

安全バスユーザー（１２、１４、１８～２４）は、定義された保守メッセージ（１１０）を初めて受け取った後でのみ、第一の登録メッセージ（１１４）を管理ユニット（７０）に送出し、また定義された保守メッセージ（１１０）を繰り返し受け取った場合は、第二の登録メッセージ（１１２）を管理ユニット（７０）に送出するように構成されている

、請求項９に記載の制御システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、安全制御システム内において安全バスユーザーをフィールドバスに接続する際に、定義されたユーザーのアドレスを安全バスユーザーに割り当てた状態で、安全バスユーザーを設定する方法に関する。
本発明はまた、安全性が不可欠なプロセスを安全に制御するための制御システムに関し、フィールドバスに接続された少なくとも１つの安全バスユーザーを有し、前記安全バスユーザーはバスメッセージを受信および評価するための第一の手段と、バスユーザーに割り当てられたユーザーアドレスを保存するメモリーとを有する。
【０００２】
【従来の技術】
かかる方法およびかかる制御システムは、それぞれ安全性が不可欠なプロセスの制御における利用が知られている。
フィールドバスはデータ通信のためのシステムであり、その中では接続された各バスユーザーはバスを介して互いに結合されている。そのため、フィールドバスに接続された２つのバスユーザーは互いに個別にケーブルで直接接続されていなくても、互いに通信を行うことができる。公知のフィールドバスの例としては、いわゆるＣＡＮバス、プロフィバスおよびインターバスがある。
制御および自動化技術の分野では、フィールドバスの利用は比較的長い間十分に知られている。しかしごく最近まで、制御に関与する各ユニットが事実上互いに個別にケーブルで接続されている安全性が不可欠なプロセスの制御には、これは適用されなかった。その理由は、公知のフィールドバスでは、安全性が不可欠なプロセスの制御に求められる故障許容度（故障確率が10^{-11}未満）を保証できなかったからである。公知のフィールドバスは全てデータ通信中の故障に対する保護のための手段を含んでいるが、これらの手段は求められる故障許容度を保証するには十分ではない。しかもフィールドバスはオープンシステムであり、原則としていかなるユニットもそれに接続することができる。そのため、制御すべき安全性が不可欠なプロセスに全く何の関係もないユニットが、安全性が不可欠なプロセスに思わぬ影響を及ぼす危険がある。
【０００３】
安全性が不可欠なプロセスとは、故障が発生した場合に人体および財産に許容できない危険が生じるプロセスという意味に理解される。従って安全性が不可欠なプロセスの場合、理想的には、故障が発生した際にプロセスが安全な状態に移行することが１００％保証されなければならない。機械設備の場合には、これは設備の電源を切ることを意味する。しかし化学製造プロセスの場合は、状況によっては電源を切ると反応を暴走させる可能性があるので、この様な場合はプロセスを危険でない範囲のパラメータで実行するのが好ましい。
【０００４】
安全性が不可欠なプロセスはまた、より大きく高レベルの全体プロセスの部分的プロセスである可能性がある。例えば油圧プレスの場合、材料の供給は安全性が不可欠ではない部分プロセスである可能性があるが、プレス装置の起動は安全性が不可欠な部分プロセスとなりうる。安全性が不可欠な（部分）プロセスの他の例としては、安全柵、保護ドア、あるいは光バリアの監視、両手操作スイッチの制御あるいは非常停止スイッチの監視と評価がある。
【０００５】
安全性が不可欠なプロセスの制御に関与するユニットを、安全性が不可欠な作業に使用することが関係する監督機関に認可されるためには、このユニットはその実際の機能を超えた安全性に関連する機器を持たなければならない。これらの機器は、主に故障および機能の監視に使用される。故障が発生しても安全な運転を保証するために、これらの関係する

ユニットは原則として冗長な構成とされる。以下の説明において、この様な安全性に関連する機器を持つユニットは「通常の」ユニットと区別して安全であると定義する。

【０００６】

フィールドバスに接続されたユニットを、以下の説明では一般にバスユーザーと称する。安全性が不可欠なプロセスを安全に制御するための制御システムの場合、バスユーザーとは通常、制御ユニットまたは信号ユニットである。制御ユニットとは、あるプロセスを制御するための何らかのインテリジェント機能(intelligence)を持つバスユーザーである。技術用語としては、かかるバスユーザーは通常、クライアントと呼ばれる。これらは制御されるプロセスの状態変数を表すデータおよび／または信号を受け取り、この情報に依存して、制御されるプロセスに影響を与えるアクチュエータを起動する。インテリジェント機能は通常、制御ユニットのメモリーに可変のユーザープログラムの形で保存される。原則として、いわゆるＰＬＣ（プログラマブル・ロジック・コントローラー）が制御ユニットとして使用される。

【０００７】

それに対して信号ユニットは、本質的に入力および出力チャンネル（Ｉ／Ｏチャンネル）を提供するバスユーザーであり、これには一方ではプロセス変数を受け取るセンサーと、他方ではアクチュエータを接続できる。原則として信号ユニットは、可変のユーザープログラムの形でのいかなるインテリジェント機能も持っていない。これらは通常、技術用語ではサーバーと呼ばれる。

例えばＣＡＮバスのような多くのフィールドバスにおいて、個々のバスユーザーに個別のユーザーアドレスを割り当てることが知られている。ユーザーアドレスは、送信側のバスユーザーから受信側のバスユーザーに送られる情報とともにバスメッセージを選択的に送るために使用される。安全性が不可欠なプロセスを制御するための制御システムを構成する際に、バスユーザーにユーザーアドレスを割り当てることは、安全上重要な手順である。その理由は例えば、２つの別々の信号ユニットが２つの別の保護スクリーンの状態信号を捉えて制御ユニットに転送したとすると、２つの信号ユニットのアドレスの割り当てが間違っていれば、対応する保護スクリーンが開けられているにもかかわらず、保護すべき機械の動作を制御ユニットが切らないという事態が生じる可能性があるからである。

【０００８】

これまでに知られている一般的な制御システム、あるいは安全バスユーザーを設定するための対応する方法においては、ユーザーアドレスは直接バスユーザーに対して設定されていた。この目的のために、各バスユーザーは機械的な符号化スイッチ、特にロータリースイッチ、あるいはシリアルのプログラミングインターフェースを有している。この解決手段の欠点は、ユーザーアドレスを個々のバスユーザーの位置に直接設定しなければならないことである。しかし、工業分野での複雑なプロセス制御の場合、フィールドバスに接続された個々のバスユーザーは数百メートルも離れている可能性がある。従ってこの場合、安全制御システムの設定のために長い距離を歩く必要があり、設定が厄介となる。

【０００９】

更に、長い歩行距離のために全体像を見失いやすく、間違ったアドレスを割り当てる可能性がある。従来知られている解決手段の別の大きな欠点は、欠陥のあるバスユーザーを交換するときに、そのユーザーアドレスが分かっていて、その後で代わりのバスユーザーにそのアドレスを割り当てられるようにしなければならないことである。このことは、２４時間運転が行われることの多い工業的設備の場合、故障したバスユーザーを交換するために必要な知識を持つ人員を常駐させなければならないことを意味する。プログラミング装置を利用して、シリアルインターフェースを通してバスユーザーにユーザーアドレスが割り当てられる場合、そのプログラミング装置も常に必要となる。

【００１０】

プログラミングインターフェースを通してユーザーアドレスを割り当てる場合、バスユーザーに割り当てられたユーザーアドレスが外部から認識できないという、別の欠点がある。その結果、前に別のユーザーアドレスで使用されていたバスユーザーが、新しい環境で

使われるときに間違って古いユーザーアドレスで動作させられてしまうという危険がある。既に使用されたバスユーザーが、保守作業中に別の制御システムに組み込まれるという場合、この危険性は特に高くなる。

【００１１】

【発明が解決しようとする課題】

そこで本発明の目的は、最初に述べたタイプの方法を特定して、それを使って単純かつ故障が生じない方法で中央から安全バスユーザーにユーザーアドレスを割り当てられるようにすることである。さらに、本発明の目的は、対応する制御システムを特定することである。

【００１２】

【課題を解決するための手段】

上記の目的は、下記の各工程からなる最初に述べたタイプの方法によって達成される。すなわち、フィールドバス（１６）に接続された管理ユニット（７０）が所定の保守メッセージ（１１０）をフィールドバス（１６）に送出する工程と、前記保守メッセージ（１１０）を受け取った前記安全バスユーザー（１２、１４、１８～２４）が、所定の広域アドレス（９２）を有する第一の登録メッセージ（１１４）を送出する工程と、前記管理ユニット（７０）が前記安全バスユーザー（１２、１４、１８～２４）に定義されたユーザーアドレス（９０）を有するアドレス割り当てメッセージ（１１８）を送出する工程と、前記安全バスユーザー（１２、１４、１８～２４）は、受け取ったユーザーアドレス（９０）を安全バスユーザーのメモリー（５８；１２０）に保存する工程とを含み、アドレス割り当てメッセージ（１１８）を受け取った後、安全バスユーザー（１２、１４、１８～２４）が定義されたユーザーアドレス（９０）を含む第二の登録メッセージ（１１２）を管理ユニット（７０）に送出する。

【００１３】

上記の目的は更に、最初に述べたタイプの制御システムによって達成されるが、その中でバスユーザーは、第一の登録メッセージにより、フィールドバスに接続された管理ユニットにおいて所定 の広域アドレスで登録するための第二の手段と、ユーザーアドレスを含むアドレス割り当てメッセージを受け取り、また評価するための第三の手段を有する。

前記の方法を使用すれば、個々のユーザーアドレスを最初に割り当てずに、設定すべきバスユーザーをフィールドバスに接続することが可能になる。このバス ユーザーは次ぎに、所定の広域アドレスに基づいて前記の管理ユニットに登録することができる。この管理ユニットは、好ましくは全制御システムに対する中央 の管理ユニットである。次の工程では、管理ユニットは設定すべきバスユーザーに個別のユーザーアドレスを送る。これは、管理ユニットから設定すべきバス ユーザーに送られる特別のアドレス割り当てメッセージを使って行われる。アドレス指定されたバスユーザーは、送られたユーザーアドレスを取り出してそれを メモリーに保存することにより、受け取ったアドレス割り当てメッセージを評価する。好ましくは、例えばＥＥＰＲＯＭのような不揮発性メモリーにユーザーア ドレスを保存する。

【００１４】

この方法を使うことにより、中央すなわち管理ユニットから安全バスユーザーに定義されたユーザーアドレスを割り当てることが可能になる。制御システムが空間的に広く配置されている場合でも、従来必要とされていた長い距離の歩行がこれにより不要となる。更に、中央から全てのバスユーザーを設定できることにより全体像が得られ、間違ったアドレスを割り当てる危険が軽減される。更に安全バスユーザーと管理ユニットの両方とも安全性に関連した設備からなるので、バスシステムに欠陥が存在する可能性にもかかわらず、定義されたユーザーアドレスを故障に耐える方法で送ることが可能となる。

【００１５】

これにより、上記の目的は完全に達成される。

この方法のある実施形態においては、安全バスユーザーはアドレス割り当てメッセージを受け取ると、管理ユニットに第二の登録メッセージを送り、第二の登録メッセージは定義

されたユーザーアドレスを含んでいる。
この手段には、安全バスユーザーが、割り当てられたユーザーアドレスをエラー無しに受け取ったかどうかだけでなく、それをエラー無しに処理したかどうかを、管理ユニットがチェックできるという利点がある。これは更にアドレス割り当ての信頼性を高める。例えばこの手段は、安全バスユーザーがそれに割り当てられたユーザーアドレスを受け取った後で、管理ユニットに再度登録を行うことを意味する。更にこの手段は、管理ユニットの観点から見ると、広域アドレスがあいまいさ無しに再度発行されるという利点も有する。従ってこれは、影響されるバスユーザーに関して多義性（あいまいさ）が生じる可能性無しに、他のバスユーザーが利用することができる。
【００１６】
本発明の別の実施形態では、定義された保守メッセージを受け取った後にのみ、安全バスユーザーが第一の登録メッセージを管理ユニットに送る。
この手段には、管理ユニットが常にフィールドバス上での交信に対して制御を維持するという利点がある。したがって新しいバスユーザーが先ず最初に管理ユニットによってその目的のために解放されることなく、フィールドバス上での交信に入るように設定されることはあり得ない。このことも、中央での制御が保証されることで制御システムの安全性が向上する。
【００１７】
この手段の好適な実施形態では、定義された保守メッセージを最初に受け取った後にのみ、安全バスユーザーが第一の登録メッセージを管理ユニットに送り、定義された保守メッセージを繰り返し受け取ると第二の登録メッセージを送る。
この手段には、フィールドバスに接続された全てのバスユーザーに、保守メッセージをいわゆるブロードキャストメッセージとして同時に共同で送ることができるという利点がある。これにより、設定すべき新しいバスユーザーの登録が、既に登録および設定されたバスユーザーによって妨害されたり遅らされたりすることがないので、本発明の方法が更に単純化される。これはまた、はるかに少ない方法の工程数で本発明の方法を実行することを可能とする。本発明の方法の実際の実施によっては、最初の受信は、制御システムの各スイッチをＯＮにした後の最初の受信に関連させることができる。しかし、バスユーザーがフィールドバスに接続された後の最初の受信に関連させることが好ましい。
【００１８】
上記の手段の更に別の実施形態においては、定義された保守メッセージは、管理ユニットの特別保守モードが起動された後にのみ送られる。
特別保守モードは、好適には、管理ユニットに接続されたキースイッチまたはコードロックを操作することにより起動される。管理ユニットの特別保守モードは、定義された保守メッセージが送出されるのはこの保守モードにおいてのみであるという点で、管理ユニットの他のどの動作モードとも異なる。この手段には、安全制御システムに対する意図的な介入の後でのみユーザーアドレスを割り当てることができるという利点がある。これにより、間違ってユーザーアドレスを送ってしまうことが防止できる。ユーザーアドレスを間違って割り当てる危険がこれによって大幅に軽減される。
【００１９】
上記の手段の更に別の実施形態においては、管理ユニットは第二の登録メッセージを受け取った後に、特別保守モードを自動的に終了させる。
この場合は、それぞれのケースでの１回のアドレス割り当てに対してだけ、特殊保守モードが起動されるので、この手段も間違ったアドレス割り当ての危険を大幅に軽減する。従って、ユーザーアドレスの割り当てをするたびに安全制御システムへの意図的な介入が新たに必要となる。このこともシステムの安全性を大幅に向上させる。
【００２０】
上記の手段の更に別の実施形態においては、定義されたユーザーアドレスは特別保守モードの始めに管理ユニットに送信される。
この手段の代わりとして、管理ユニットがメモリーから定義されたユーザーアドレスを自

動的に読み出し、それによりユーザーアドレスのリストから個々のバスユーザーに続けてユーザーアドレスを割り当てるという方法が可能である。それと比較すると上記の手段では、個々のユーザーアドレスを割り当てるために、バスユーザーの設定を行いたい側の意図的な動作が再度要求されるという利点がある。このこともアドレス割り当ての安全性を大幅に高める。

【００２１】

上記の手段の更に別の実施形態においては、送信されるユーザーアドレスが、フィールドバスに接続されたバスユーザーに既に割り当てられている場合は、管理ユニットは故障信号を発生する。

この手段も、別々のバスユーザーにユーザーアドレスを重複して割り当てることを確実に防止するので、間違ったアドレス割り当ての防止に貢献する。

本発明の別の実施形態では、管理ユニットはフィールドバスに接続された全てのバスユーザーに、定められた時間間隔で保守メッセージを送る。

【００２２】

この手段は、各ケースで特殊保守モードの個別の起動後にのみ保守メッセージを送ることができるのと異なる。比較すると前記の手段は、制御システムが動作中に、非常に単純かつ楽に新しいバスユーザーを接続できるという利点を有している。この構成では、ユーザーアドレスは可能性のあるユーザーアドレスのリストから管理ユニットによって自動的に選択されるか、または新しいバスユーザーが接続される前に管理ユニットに送信することができる。

【００２３】

本発明による方法の更に別の実施形態は、下記の工程によって特徴づけられる。すなわち、フィールドバスにアクティブに接続されている全てのバスユーザーが存在するかどうかを、各バスユーザーの公称設定によって、またバスユーザーの応答メッセージによってチェックする工程と、もはやアクティブでないと判断されたバスユーザーのユーザーアドレスを定義されたユーザーアドレスとして送出する工程とを更に含む。

【００２４】

本発明のこの実施形態は、既に設定されている安全制御システムに対する保守作業に関して、特に有利である。それは、新しいバスユーザーに意図的にユーザーアドレスを割り当てる必要なく、故障したバスユーザーを新しいバスユーザーに交換することが、公知の手段を利用して単純な方法で可能になるからである。この実施形態では、管理ユニットはそこに登録された全てのバスユーザーがフィールドバスにアクティブに接続されているかどうかを常にチェックする。もしも不明のバスユーザーがあれば、それは故障しているか、またはこのバスユーザーが既にフィールドバスから切り離されていることを示す。管理ユニットは公知の公称設定に基づいて、不明のバスユーザーのユーザーアドレスを特定できる。新しいバスユーザーが所定の広域アドレスの下で管理ユニットに登録するとすぐに、不明のバスユーザーのユーザーアドレスがそれに割り当てられる。これにより、古いユーザーアドレスを新しいバスユーザーに手動で割り当てることなく、故障したバスユーザーを交換することが可能になる。本発明のこの実施形態は好適には、管理ユニットの特別保守モードを起動した後だけに送出される、定義された保守メッセージと組み合わされる。これは、一方ではユーザーアドレスの割り当てに関する非常に高い信頼性が得られ、また他方では故障したバスユーザーが非常に単純な方法で、また技術的知識なしに交換できるからである。このことは、２４時間運転が行われる生産設備の場合に特に有利である。

【００２５】

本発明の更に別の実施形態では、１つ以上のバスユーザーが第一の登録メッセージを送出すると、管理ユニットは故障信号を発する。

この手段も、多くのバスユーザーにユーザーアドレスを同時に割り当てることが防止されるので、信頼性が向上するという利点を有している。

本発明の更に別の実施形態では、少なくとも第一の登録メッセージとアドレス割り当てメッセージに対して、受領メッセージが返される。

【００２６】
この手段では、実際の処理とは関係なく、前記のメッセージの受信側が発生側に受領メッセージを送り返すようにする。これにより発信側は、受信側がそれぞれのメッセージをエラー無しに受け取ったかどうかをチェックできるので、これもアドレス割り当ての信頼性を大幅に高める。
上記の特徴および以下に説明する特徴は、各ケースで述べた組み合わせだけでなく、本発明の範囲から逸脱することなく別の組み合わせで、またそれら単独でも使用できる。
【００２７】
【発明の実施の形態】
以下、本発明の実施形態を図面を参照してより詳しく説明する。
図１において、安全性が不可欠なプロセスを安全に制御するための制御システムの全体を参照番号１０で表している。
制御システム１０は、フィールドバス１６を介して全部で４つの安全信号ユニット１８、２０、２２、２４に接続されている２つの安全制御ユニット１２、１４を有する。制御ユニット１２、１４および信号ユニット１８～２４は、本発明におけるバスユーザーである。
【００２８】
安全信号ユニット１８～２４の各々は多くのＩ／Ｏチャンネルからなり、これを介して各々が安全性が不可欠なプロセス２８、３０、３２に接続されている。この場合は、安全信号ユニット１８、２０はプロセス２８に接続され、信号ユニット２２はプロセス３０に接続され、そして信号ユニット２４はプロセス３２に接続されている。安全性が不可欠なプロセス２８は、例えば、図示しない機械軸の回転速度が監視されている機械設備の両手操作制御機器である。安全性が不可欠なプロセス３０は例えば非常停止スイッチの監視であり、安全性が不可欠なプロセス３２は保護スクリーン（図示せず）の監視である。
【００２９】
信号ユニット１８～２４は、それらのＩ／Ｏチャンネル２６を介して安全性が不可欠なプロセス２８～３２の信号および／またはデータの値を読む。かかる信号またはデータの値は、例えば、機械軸の現在の回転速度および非常停止スイッチの切替位置である。他方、信号ユニット１８～２４はＩ／Ｏチャンネル２６を介して図示しないアクチュエータに作用して、それにより安全性が不可欠なプロセス２８～３２に影響を与える。従って、例えばその非常停止スイッチの切替位置が監視されている安全性が不可欠なプロセス３０には、制御されまた監視されている機械設備の電源を切ることのできるアクチュエータが含まれる。
【００３０】
安全制御ユニット１２、１４はＰＬＣ制御機器である。原則として、これらは同一の構造を有しているが、異なるアプリケーションプログラムがそれらの中で実行されるという点で基本的に異なる。
制御ユニット１２、１４および信号ユニット１８～２４の以下の説明において、図１に示した参照符号は分かりやすくするためにそれぞれ１度だけ引用する。
制御ユニット１２、１４はそれぞれ、図１で一点鎖線３６の上に示された安全処理部３４を含んでいる。線３６の下には非安全部３８があり、これは基本的にバスコントローラーと呼ばれるチップ４０を含む。バスコントローラー４０は、使用されるフィールドバス１６の標準的プロトコルが組み込まれている標準チップである。バスコントローラー４０はメッセージをフレームの形で送出および受信することを独立して処理することができる。送出されるメッセージは、安全処理部３４からバスコントローラー４０によって受け取られる。バスコントローラー４０は、受け取ったメッセージを逆に安全処理部３４に供給する。
【００３１】
本発明の好適な実施形態によれば、フィールドバス１６はこの場合ＣＡＮバスである。このバスにおいて送出されるメッセージは、フィールドバス１６を通って送るためにつけ加

えられた制御情報によって補足されたユーザーデータフィールド内で送信される。制御情報とユーザーデータフィールドの完全なパッケージがバスメッセージを形成する。バスコントローラー４０は、安全処理部３４から受け取った情報を、プロトコルに対応した形式で送出されるべきバスメッセージ内に独立して埋め込むことができる。逆にこれは、受け取ったバスメッセージ内のユーザーデータフィールドに含まれる情報を取り出すことができる。

【００３２】

各制御ユニット１２、１４の安全処理部３４は、２チャンネルの冗長を持って構成されている。２チャンネルの各々は基本的にプロセッサー４２ａ、４２ｂを含み、それはこの場合アプリケーションプログラム４４ａ、４４ｂを実行するための関連周辺機器を有している。アプリケーションプログラム４４ａ、４４ｂは機械設備の制御、従って制御ユニット１２、１４のインテリジェント機能を有している。

【００３３】

２つのプロセッサー４２ａ、４２ｂは、互いに関して冗長に安全性に関するタスクを実行する。このプロセスにおいて、これらは図１において矢印４６で示されたように互いをチェックする。安全性に関するタスクには、例えば送信または送出されたメッセージのエラー保護手段が含まれる。これらの手段は、標準的な手段としてバスコントローラー４０によって既に実行されているエラー保護手段に加えて、またそれを補完するものとして実行される。これにより、それ自体安全でないフィールドバス１６と比較して、故障確率を大幅に高めることができる。

【００３４】

信号ユニット１８～２４は、安全制御ユニット１２、１４と同じバスコントローラー４０を介してフィールドバス１６に接続されている。これに対応して、図１で線５０の上の部分４８もまた、本発明において安全でない。線５０の下の安全処理部において、信号ユニット１８～２４の各々もまた、２チャンネルの冗長度を持たせて構成されている。２つの冗長処理チャンネルもまた相互のエラー監視を行うことができる。

【００３５】

信号ユニット１８～２４の各処理チャンネルは、プロセッサー５４ａ、５４ｂとスイッチ手段５６ａ、５６ｂを有している。参照番号５８ａ、５８ｂはそれぞれの場合メモリーを示すが、これは一方では所定の広域アドレスがこのメモリーに保存され、また他方ではプロセッサー５４ａ、５４ｂが割り当てられたユーザーアドレスをこのメモリーに保存できる。従って、バスコントローラー４０との関連で、信号ユニット１８～２４の各々は所定の広域アドレスでフィールドバスに接続された管理ユニットに登録し、また逆に関連するユーザーアドレスとともにアドレス割り当てメッセージを受け取りかつ評価することができる。図１ではこれは明示的に図示されていないが、安全制御ユニット１２、１４もまた同じ能力を有する。

【００３６】

スイッチ手段５６ａ、５６ｂは、信号ユニット１８～２４が図示されてないアクチュエータを起動して、安全性が不可欠なプロセス２８～３２に影響を与えることを可能にする。従って、安全信号ユニット１８～２４は、安全性が不可欠なプロセス２８～３２を、例えば非常停止スイッチが作動したときに機械設備の電源を切るように、安全な状態にすることができる。

技術用語では管理装置とも呼ばれる上記管理ユニットは、図１では参照番号７０で示される。管理ユニット７０はまた、バスコントローラー４０を介してフィールドバス１６に接続されている。従って、これはフィールドバス１６に接続された残りのユニットと通信することができる。しかしこれは、安全性が不可欠なプロセス２８～３２の制御には直接関与していない。

【００３７】

その安全処理部に、管理ユニット７０は基本的に２つの互いに冗長なメモリー７２ａ、７２ｂを有しており、これらメモリーには、制御システム１０の全構成と、特にバスユーザ

ー１２、１４およびバスユーザー１８～２４に対する定義されたユーザーアドレスの割り当てなどが記憶されている。管理ユニット７０は、プロセス２８～３２の制御とは独立に行われる中央の管理および監視機能を有する。例えば管理ユニット７０は、制御ユニット１２、１４および信号ユニット１８～２４の間の接続チェックを、決まった時間間隔で開始する。このプロセスの間、管理ユニット７０は制御ユニット１２、１４に接続チェックメッセージを送ることにより、これらの制御ユニットへの接続がエラー無しに動作しているかどうかをチェックする。このチェックメッセージに対する応答として、制御ユニット１２、１４はそれに関連する信号ユニット１８～２４にチェックメッセージを送出する。このプロセスの間、管理ユニット７０は全データ交信を監視し、またその結果として、それが把握している全てのバスユーザーがまだフィールドバス１６にアクティブに接続されているかどうかに関する情報を決まった時間間隔で受け取る。予想されたチェックメッセージが無い場合、あるいは予想された応答メッセージが無い場合は、管理ユニットはエラーメッセージを出し、これに基づいて安全性が不可欠なプロセス２８～３２は安全な状態に移行させられる。

【００３８】

ここに示した例示的実施形態の代わりに、管理ユニット７０を制御ユニット１２、１４の一方に組み込むこともできる。この場合、管理ユニット７０は制御ユニット１２、１４内の機能ブロックを表す。ここに図示しない別の実施形態では、制御システム１０は１つの制御ユニット１２だけを有する。

参照番号８０は、例えば、フィールドバス１６を介して２つのバスユーザーの間で送信されるバスメッセージを示す。バスメッセージ８０は使用される標準プロトコルに応じて、アドレスフィールド８２とユーザーデータフィールド８４を有する。それに加えて、ここに図示しない他の制御情報もバスメッセージ８０に含めることができる。

【００３９】

図１の構成において、フィールドバス１６に接続されたユニットの各々には個別に定義されたユーザーアドレス９０が割り当てられており、それは制御ユニット１４においては例えば“２”である。従って、例えば、管理ユニット７０は定義されたユーザーアドレス“０”を有し、信号ユニット１８はユーザーアドレス“３”を有する。更に図１で“ｘｙ”という記号で表されている所定の広域アドレス９２が各ユニットに保存される。当然それぞれの場合において、ユーザーアドレス９０と広域アドレス９２の両方とも、個々のユニットのメモリーにデータ値として記憶される。

【００４０】

図２に信号ユニット１８の設定中の通信の流れを、管理ユニット７０、安全制御ユニット１２および安全信号ユニット１８の例と共に図示する。この例では、時間軸が矢印１００の向きに延びている。様々なユニット間で送られる個々のメッセージを矢印で表し、その始点には発信点の丸を付し、終点はそれぞれの場合の受信側を表す。

図２の最初の時間区分では、安全信号ユニット１８はまだフィールドバス１６に接続されていない。そのためこの時間区分では破線で示されているだけである。管理ユニット７０は決まった時間間隔で制御ユニット１２に接続チェックメッセージ１０２を送出する。これは次ぎに応答メッセージ１０４で応答する。応答メッセージ１０４の所定の期間内の受信が、管理ユニット７０によって監視される。その結果管理ユニット７０は、フィールドバス１６にアクティブに接続されているユニットの実際の数を、公称設定に基づく公称数と比較することができる。所定の時間が経過すると、このプロセスが繰り返される。つまり管理ユニット７０は再度接続チェックメッセージ１０２を送出し、応答メッセージ１０４を受け取る。

【００４１】

ここで信号ユニット１８がフィールドバス１６に新たに接続されると仮定する。従って信号ユニット１８を設定しなければならず、これに定義されたユーザーアドレス９０が割り当てられる。ここで説明した本発明の実施形態によれば、管理ユニット７０は先ず特別保守モードにされる。好適な実施形態では、これは管理ユニット７０に装備されたキースイ

ッチにより行われる。特別保守モードの起動は図２において線１０６で表されている。
【００４２】
特別保守モードが起動されると、信号ユニット１８に割り当てられるべき定義されたユーザーアドレス９０が、入力装置１０８を利用して管理ユニット７０に送信される。その後管理ユニット７０は、管理ユニット７０の通常の動作モードにおける接続チェックメッセージ１０２とは異なる定義された保守メッセージ１１０を送出する。既にフィールドバス１６に接続されていた制御ユニット１２は、保守メッセージ１１０の受信に対して、制御ユニット１２の定義されたユーザーアドレスを含む登録メッセージ１１２で応答するが、これは例えばユーザーアドレス“１”である。登録メッセージ１１２は、本発明における第二の登録メッセージである。本発明の好適な実施形態によれば、制御ユニット１２の登録メッセージ１１２は、上で述べた応答メッセージ１０４と同一である。しかしこのことは本方法を実施する上で必須ではない。
【００４３】
保守メッセージ１１０の送出と第二の登録メッセージ１１２の受信は、周期的に繰り返される。この期間中に、安全信号ユニット１８をフィールドバス１６に接続できる。これを行った後で、信号ユニット１８と制御ユニット１２は保守メッセージ１１０を受け取る。制御ユニット１２はこの保守メッセージ１１０に対して、上で述べたように第二の登録メッセージ１１２で応答するが、信号ユニット１８は保守メッセージ１１０の最初の受信に対して所定の広域アドレス“ｘｙ”を含む第一の登録メッセージ１１４を送出する。管理ユニット７０は第一の登録メッセージ１１４を受け取って、受領メッセージ１１６を信号ユニット１８に送出する。これに続いて、管理ユニット７０はアドレス割り当てメッセージ１１８を送出するが、そのユーザーデータフィールドは定義されたユーザーアドレス“３”を含む。信号ユニット１８は受領メッセージ１１６でアドレス割り当てメッセージ１１８の受信を知らせる。その後、信号ユニット１８は定義されたユーザーアドレス“３”をメモリー１２０に保存する。
【００４４】
管理ユニット７０は信号ユニット１８から受領メッセージ１１６を受け取ると、再度保守メッセージ１１０を送出する。これに続いて、制御ユニット１２は通常通り第二の登録メッセージ１１２で管理ユニット７０に登録する。ただしそれに加えて、今回は信号ユニット１８は第二の登録メッセージ１１２で管理ユニット７０に登録を行う。この場合、第二の登録メッセージ１１２は、信号ユニット１８に割り当てられていたユーザーアドレス“３”を含む。管理ユニット７０は、第二の登録メッセージ１１２の受け取りを知らせる受領メッセージ１１６を送る。
【００４５】
上に述べたメッセージのやり取りが完了すると、信号ユニット１８は本発明において設定されたことになる。従って本発明の好適な実施形態によれば、管理ユニット７０は線１２２で示される特別保守モードを自動的に終了する。その後管理ユニット７０と、フィールドバス１６に接続されたユニット１２、１８の間における通常のデータのやり取りが、上で述べたように再開される。このプロセスの間、管理ユニット７０は周期的な間隔で接続テストメッセージ１０２を送出し、応答メッセージ１０４を受け取る。
【００４６】
本発明の別の実施形態では、管理ユニット７０はここで述べた手順とは違い、割り当てられたアドレスが信号ユニット１８に保存された後、特殊保守モードをすでに終了している。この場合信号ユニット１８は、前記ユニットの通常の動作モードでの第二の登録メッセージ１１２によって、再度管理ユニット７０に登録するだけである。
分かりやすくするために、受領メッセージ１１６の送出については設定すべき信号ユニット１８に関してしか述べなかった。しかしこれと異なり、制御システム１０の好適な実施形態では、送出される各メッセージに対して受領メッセージ１１６の応答がある。受領メッセージ１１６が無ければ自動的にエラーメッセージが発生される。
【００４７】

図３は、信号ユニット１８の交換中の、本発明の方法の流れを示す。この場合も管理ユニット７０は、最初はその通常の動作モードであり、フィールドバス１６に接続された全てのユニットに周期的な間隔で接続チェックメッセージ１０２を送出する。接続された各ユニット、この場合は制御ユニット１２と信号ユニット１８は、対応する応答メッセージ１０４で応答する。これらの応答メッセージは、フィールドバス１６にアクティブに接続されているユニット１２、１８の数について、管理ユニット７０に知らせる。

【００４８】

信号ユニット１８を交換するためには、管理ユニット７０は先ず特別保守モードにされる。これは線１０６で示される。その前に、交換すべき信号ユニット１８はフィールドバス１６から切り離されている。

特殊保守モードでは、管理ユニット７０は前に説明したように定義された保守メッセージ１１０を送出するが、これはもはや信号ユニット１８には到達しない。これは図３において破線矢印１２３で示される。保守メッセージ１１０の受信に対して、制御ユニット１２は通常通りに第二の登録メッセージ１１２で応答する。他方、信号ユニット１８の第二の登録メッセージは、破線の矢印１２４で示されるように送信されない。そのため管理ユニット７０は、信号ユニット１８はもはやアクティブにフィールドバス１６に接続されていないことを認識することができる。そこで信号ユニット１８に割り当てられていた定義されたユーザーアドレス“３”をメモリー１２６に保存する。その後これは再度保守メッセージ１１０を周期的な間隔で送出する。既に説明したように、制御ユニット１２はこれに対して第二の登録メッセージ１１２で応答する。

【００４９】

信号ユニット１８またはそれと交換で装備される装置は、これでフィールドバス１６に接続できる。

新たに接続された信号ユニット１８が保守メッセージ１１０を受け取るとすぐに、所定の広域アドレス“ｘｙ”を含む第一の登録メッセージ１１４を送出する。新しい信号ユニット１８はこの手段によって、所定の広域アドレス“ｘｙ”で管理ユニット７０に登録する。既に説明したように、管理ユニット７０は第一の登録メッセージ１１４を受け取ったことを受領メッセージ１１６で知らせ、次ぎにアドレス割り当てメッセージ１１８を送出する。これは管理ユニット７０が前にメモリー１２６に保存した、定義されたユーザーアドレス“３”を含んでいる。信号ユニット１８は、アドレス割り当てメッセージ１１８を受け取ったことを受領メッセージ１１６で知らせて、割り当てられたユーザーアドレス“３”をそのメモリー１２０に保存する。その後、管理ユニット７０は再度保守メッセージ１１０を送出し、制御ユニット１２と信号ユニット１８の両方から第二の登録メッセージ１１２を受け取る。そしてこれらの登録メッセージを受け取ったことを受領メッセージ１１６で知らせて、再び線１２２で示されている特別保守モードを終了する。

【００５０】

上で説明した方法によれば、フィールドバス１６に接続されたバスユーザーの交換を、その定義されたユーザーアドレスを知らなくても行える。

図３に示す次の時間区分では、多くのバスユーザーが所定の広域アドレス“ｘｙ”で管理ユニット７０に登録する場合に生じる方法の手順が示されている。上で述べたように、管理ユニット７０は、先ず最初に特別保守モードになっている。次ぎにこれは保守メッセージ１１０を送出する。もしも制御ユニット１２と信号ユニット１８の両方が第一の登録メッセージ１１４で応答すれば、管理ユニット７０は故障信号１２８を起動して特別保守モードを終了する。

【００５１】

次の時間区分では、別のエラー源が示されている。ここでは、特別保守モードが起動された後、フィールドバス１６に接続されたバスユーザーに既に割り当てられているユーザーアドレスが、入力装置１０８を通して管理ユニット７０に送られると仮定する。管理ユニット７０は、それが把握しているアクティブなバスユーザーの公称設定状況から、アドレスが二度割り当てられたことを認識し、エラー信号１２８を起動する。そして再度特別保

守モードを終了する。

【００５２】

本発明の別の好適な実施形態によれば、定義されたユーザーアドレス９０はこの場合、ＰＬＣ制御ユニット１２、１４のプロセスマップにおいて、各信号ユニット１８～２４に割り当てられた機能的プロセスのアドレスに更に関連づけられており、アプリケーションプログラム４４ａ、４４ｂはＰＬＣ制御の場合に知られている方法で、これらのプロセスマップにアクセスを行う。機能的プロセスのアドレスは、信号ユニット１８～２４に接続されたセンサーまたはアクチュエータ、例えば光バリヤーの機能をあいまいさ無しに指定する。これにより、定義されたユーザーアドレス９０に２つの機能が与えられる。それは、フィールドバス１６上での通信のために、信号ユニット１８～２４を指定することを可能にする一方で、アプリケーションプログラム４４ａ、４４ｂに常に変らないプロセスデータにアクセスする能力を与えるからである。

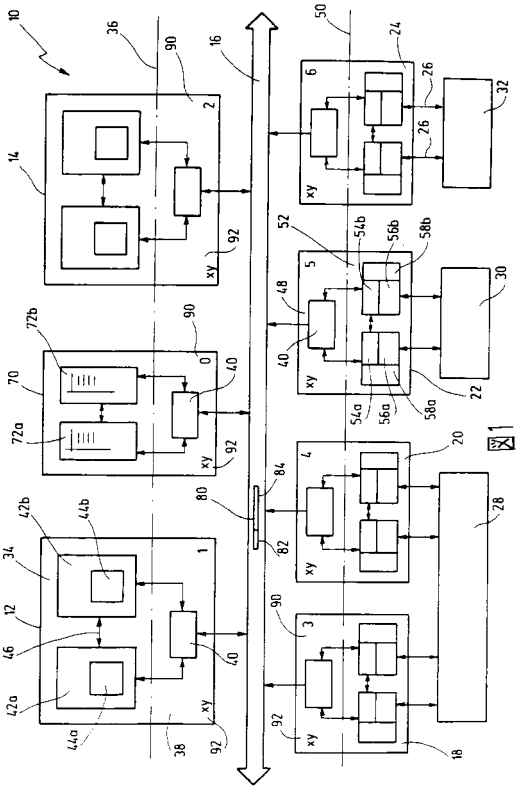
【図面の簡単な説明】

【図１】　安全性が不可欠なプロセスを安全に制御するための制御システムの模式図である。

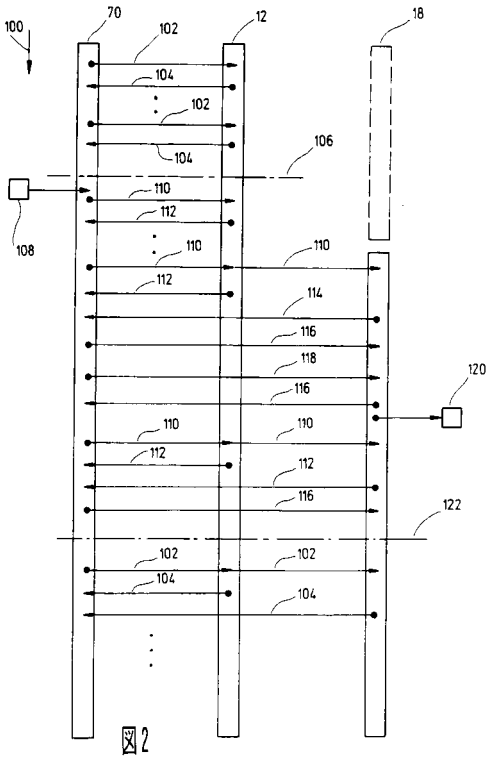
【図２】　本発明の第一の実施形態における管理ユニットと２つのバスユーザーの間の通信の流れを示す。

【図３】　本発明の別の実施形態における管理ユニットと２つのバスユーザーの間の通信の流れを示す。

【図１】



【図２】



【図３】

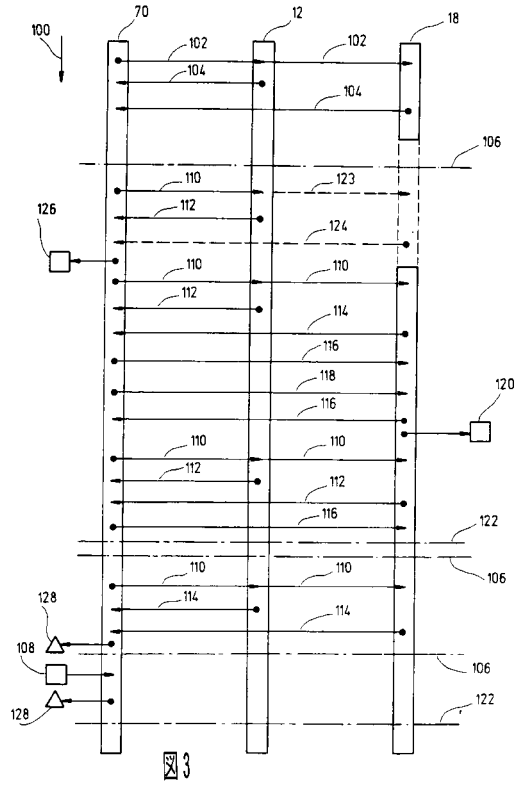

100
70
12
18
102
102
104
104
106
110
123
126
112
124
110
110
112
114
116
118
120
116
110
110
112
112
116
122
106
110
110
114
114
128
108
106
128
122

図３

フロントページの続き

(72)発明者　ヴォーンハース，クラオス
ドイツ連邦共和国，Ｄ－７０７３６　フェルバハ，マイスナー　シュトラッセ　１２番地
(72)発明者　シュヴェンケル，ハンス
ドイツ連邦共和国，Ｄ－７０１９２　シュトゥットガルト，ザオムヴェーク　１５番地

審査官　大石　博見

(56)参考文献　欧州特許出願公開第００１７３９０５（ＥＰ，Ａ１）
特開平１０－０１３４４３（ＪＰ，Ａ）
特開平０８－０３２６０７（ＪＰ，Ａ）
特開平０９－１３０３９７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 12/40