(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3748078号
(P3748078)
(45)発行日　平成18年2月22日(2006.2.22)　(24)登録日　平成17年12月9日(2005.12.9)

(51)Int.Cl.		F I		
H04L 12/403	(2006.01)	H04L	12/403	
G05B 9/02	(2006.01)	G05B	9/02	E
G05B 19/048	(2006.01)	G05B	19/048	
G05B 23/02	(2006.01)	G05B	23/02	V

請求項の数 7　(全 16 頁)

(21)出願番号　特願2003-508023(P2003-508023)
(86)(22)出願日　平成14年6月21日(2002.6.21)
(86)国際出願番号　PCT/JP2002/006242
(87)国際公開番号　WO2003/001749
(87)国際公開日　平成15年1月3日(2003.1.3)
審査請求日　平成16年1月5日(2004.1.5)
(31)優先権主張番号　特願2001-190418(P2001-190418)
(32)優先日　平成13年6月22日(2001.6.22)
(33)優先権主張国　日本国(JP)

(73)特許権者　000002945
オムロン株式会社
京都市下京区塩小路通堀川東入南不動堂町８０１番地
(74)代理人　100092598
弁理士　松井　伸一
(72)発明者　宗田　靖男
日本国京都府京都市下京区塩小路通堀川東入南不動堂町８０１番地　オムロン株式会社内
(72)発明者　中村　敏之
日本国京都府京都市下京区塩小路通堀川東入南不動堂町８０１番地　オムロン株式会社内

最終頁に続く

(54)【発明の名称】安全ネットワークシステム及び安全スレーブ

(57)【特許請求の範囲】

【請求項１】

安全ネットワークに接続可能な安全スレーブであって、

前記安全ネットワークを介して送られてきた安全コントローラからの要求に応じて、安全状態にあるか否かを特定する安全情報を送信する安全情報送信制御機能と、

前記安全スレーブについての非安全情報を記憶する非安全情報記憶手段と、

その非安全情報記憶手段に格納された前記非安全情報が、安全機器の寿命に関する経過条件を満たした際に、前記安全コントローラに向けて少なくともその経過条件を満たした非安全情報を送信する非安全情報送信制御機能と、を備えたことを特徴とする安全スレーブ。

【請求項２】

安全ネットワークに接続可能な安全スレーブであって、

前記安全ネットワークを介して送られてきた安全コントローラからの要求に応じて、安全状態にあるか否かを特定する安全情報を送信する安全情報送信制御機能と、

前記安全スレーブについての非安全情報を記憶する非安全情報記憶手段と、

前記非安全情報の送信のための条件を記憶する記憶手段と、

前記非安全情報に記憶された前記非安全情報が前記条件を満たすか否かを判断する監視手段と、

その監視手段の監視結果に基づいて送信タイミングを決定する決定手段とを備えたことを特徴とする安全スレーブ。

【請求項３】
前記非安全情報の送信は、前記要求に基づく１回の通信サイクル中において、他の安全スレーブの安全応答の終了後に行うようにしたことを特徴とする請求の範囲第１項または第２項に記載の安全スレーブ。
【請求項４】
安全コントローラと、請求の範囲第１項から第３項の何れか１項に記載の安全スレーブとが安全ネットワークを介して接続されて構築されるネットワークシステムであって、
前記スレーブから出力された前記機器の情報が、前記コントローラへ送信されることを特徴とするネットワークシステム。
【請求項５】
前記安全コントローラが管理する１回の通信サイクルは、前記各安全スレーブからの安全応答を受信後、非安全情報の受信期間を持つことを特徴とする請求の範囲第４項に記載の安全ネットワークシステム。
【請求項６】
安全ネットワークに接続可能な安全スレーブであって、
前記安全ネットワークを介して送られてきた他のノードからの要求に応じて、安全状態にあるか否かを特定する安全情報を送信する安全情報送信制御機能と、
前記安全スレーブについての非安全情報を記憶する非安全情報記憶手段と、
その非安全情報記憶手段に格納された前記非安全情報が、安全機器の寿命に関する経過条件を満たした際に、前記他のノードに向けて少なくともその経過条件を満たした非安全情報を送信する非安全情報送信制御機能と、を備えたことを特徴とする安全スレーブ。
【請求項７】
安全ネットワークに接続可能な安全スレーブであって、
送信条件を満たした場合に、安全状態にあるか否かを特定する安全情報を送信する安全情報送信制御機能と、
前記安全スレーブについての非安全情報を記憶する非安全情報記憶手段と、
その非安全情報記憶手段に格納された前記非安全情報が、安全機器の寿命に関する経過条件を満たした際に、前記安全ネットワークに接続された他のノードに向けて少なくともその経過条件を満たした非安全情報を送信する非安全情報送信制御機能と、を備えたことを特徴とする安全スレーブ。
【発明の詳細な説明】
技術分野
この発明は、安全ネットワークシステム及び安全スレーブに関するものである。
背景技術
ファクトリーオートメーション（以下、「ＦＡ」と称する）で用いられるプログラマブルコントローラ（以下、「ＰＬＣ」と称する）は、スイッチやセンサなどの入力機器からＯＮ／ＯＦＦ情報を入力し、ラダー言語などで書かれたシーケンスプログラム（ユーザプログラムとも称する）に沿って論理演算を実行し、求められた演算結果に従い、リレーやバルブ，アクチュエータなどの出力機器にＯＮ／ＯＦＦ情報の信号を出力することで制御が実行される。
ところで、ＰＬＣと、入力機器並びに出力機器との接続形態は、ＰＬＣに直接接続する場合もあれば、ネットワークを介して接続する場合もある。係るネットワークで接続されたネットワークシステムを構築した場合、上記ＯＮ／ＯＦＦ情報の送受をネットワークを経由して行うことになる。このとき、通常、ＰＬＣ側がマスタとなり、機器側がスレーブとなるマスタスレーブ方式で情報の伝送が行われる。
一方、最近ではＰＬＣによる制御においても、フェイルセーフ（安全）システムが導入されつつある。つまり、ＰＬＣや各機器自体はもちろんネットワークも安全機能を組み込まれたもので構成される。ここで安全機能とは、安全であることを確認し、出力を行う機能である。そして、安全システムは、緊急停止スイッチが押下されたり、ライトカーテンなどのセンサが人（身体の一部）の進入を検出した場合等のネットワークシステムが危険状

態になった場合に、フェイルセーフが働き、システムが安全側になって、動作が停止するようにするものである。換言すると、上記した安全機能により、安全であることが格納されたときのみ出力し、機械を動かすシステムである。よって、安全が確認できない場合には、機械が停止する。

上記した安全機能を備えたネットワークシステム（安全ネットワークシステム）の場合、異常，危険状態が発生した時から、安全動作（装置の停止等）を実行するまでに要する最大応答時間を一定にする必要がある。すなわち、良く知られているように、マスタースレーブ方式で情報伝送をする場合、図１（ａ）に示すように、マスタからの要求に従って各スレーブが順にマスタに安全応答を返すようになる。図１に示す例では、ネットワークシステムを構成するスレーブは３つ。なお、ここで扱うＯＮ／ＯＦＦ情報は、正常（安全）／異常（危険）という安全制御用の情報である。最大応答時間は、１回の通信サイクルにかかる時間が保証される。

一方、定期的或いは非定期的に、上記安全情報以外のスレーブの状態や通電時間や動作回数などのスレーブ或いはスレーブに接続された機器を監視するための補完的な情報（非安全情報）を収集したいという要求がある。係る非安全情報を取得することにより、例えば機器の寿命判定が行え、実際に故障を生じてシステムが停止する前に交換することができる。

しかし、上記のように、非安全情報を送る場合には、例えば図１（ａ）に示す例において通信サイクル１では全て非安全情報を送信し、次の通信サイクル２では全て安全情報を送信することが考えられる。しかし、係る方式によると、通信サイクル１の期間は安全情報を送ることができないので、結局最大応答時間は通信サイクルの２倍の長さとなる。

また、別の方式としては、図１（ｂ）に示すように、マスタからの要求に対し、安全情報を送信する安全応答に非安全情報を付加した情報を返すこともできる。

このように非安全情報を通信させると、上記した何れの方式をとってもトラフィックに影響を与え、安全情報の通信性能に影響を与えてしまう。つまり、当然のことながら非安全情報を通信しているときは安全情報を通信することはできないので、その分安全情報を送るのが遅れてしまう。

そして、係る非安全情報は、マスタ（安全ＰＬＣ）からの読み出し要求を受けて、安全スレーブが持つ非安全情報を返しているので、読み出す間隔を小さくするほどよりリニアな非安全情報をモニタすることができる反面、読み出し要求の発行間隔が短くなるほど、ネットワークトラフィックへの影響が大きくなる。

この発明は、ネットワークトラフィックへの影響を可及的に抑制しつつ、非安全情報を効率良く収集することのできる安全ネットワークシステム及び安全スレーブを提供することを目的とする。

発明の開示

この発明による安全スレーブは、安全ネットワークに接続可能な安全スレーブである。そして、前記安全ネットワークを介して送られてきた安全コントローラからの要求に応じて、安全状態にあるか否かを特定する安全情報を送信する安全情報送信機能と、前記安全スレーブについての非安全情報を記憶する非安全情報記憶手段と、その非安全情報記憶手段に格納された前記非安全情報が、安全機器の寿命に関する経過条件を満たした際に、前記安全コントローラに向けて少なくともその経過条件を満たした非安全情報を送信する非安全情報送信制御機能と、を備えて構成する。そして、前記非安全情報の送信は、前記要求に基づく１回の通信サイクル中において、他の安全スレーブの安全応答の終了後に行うようにすることができる。

また、安全ネットワークに接続可能な安全スレーブであって、前記安全ネットワークを介して送られてきた安全コントローラからの要求に応じて、安全状態にあるか否かを特定する安全情報を送信する安全情報送信制御機能と、前記安全スレーブについての非安全情報を記憶する非安全情報記憶手段と、前記非安全情報の送信のための条件を記憶する記憶手段と、前記非安全情報に記憶された前記非安全情報が前記条件を満たすか否かを判断する監視手段と、その監視手段の監視結果に基づいて送信タイミングを決定する決定手段とを

備えたものとしてもよい。
一方、本発明に係る安全ネットワークシステムは、安全コントローラと、請求項１または２に記載の安全スレーブとが安全ネットワークを介して接続されて構築されるネットワークシステムであり、前記スレーブから出力された前記機器の情報が、前記コントローラへ送信されるようにした。
そして、前記安全コントローラが管理する１回の通信サイクルは、前記各安全スレーブからの安全応答を受信後、非安全情報の受信期間を持つようにするとよい。
ここで、安全情報とは、少なくも安全スレーブ及びまたはそれに接続された安全機器の状態が安全状態か否かの情報を含むものである。もちろん、それ以外の情報を含むことはかまわない。これに対し、非安全情報は、上記安全情報を含まない各種の情報であり、例えば、リレーの寿命，調査結果，通電時間，動作回数，型情報等がある。ここで、「通電時間」や「動作回数」などは、例えば、それぞれタイマやカウンタで計時・計数して求め、求めた現時点の数値を非安全情報として送る。また、「リレーの寿命」とは寿命予知である。つまり、ここでいう非安全情報としてのリレーの寿命は、寿命が来て安全動作ができない旨の情報ではなく（この時は安全情報扱いとなる）、安全に動作するがメンテナンス（交換，調整手入れなど）をする時期が近づいてきている旨の予知的な情報である。「調査結果」は、たとえば統計的に予知或いは検出するような旨の情報である。なお、非安全情報としての検査結果の例としては、安全に動作するが、（１）もう少しで寿命が来そうだとか、（２）悪い環境で使用されているとか、（３）温度（４）振動状態（５）供給電圧（６）酷使状態かどうか…などの情報がある。係る情報を知ることで、早めにメンテナンス（交換，調整手入れなど）をすることができ、寿命が来て動かなくなり、異常の影響が大きくなることが防止できる。さらには、自己診断した結果も非安全情報の一種となる。
また、「安全機能」とは、いわゆるフェールセーフ機能のことであり、安全であることを条件に出力し、機械を動かすシステムである。従って、安全でなくなった場合には、出力が停止される。よって、コントローラなどの制御で異常が生じた場合や通信異常が生じた場合に制御停止させるとともに、コントローラの停止により出力対処の機器や制御機器が安全な状態を維持することができる。
この制御停止が必要な場合の例としては、コントローラのＣＰＵその他の各処理部等を二重化して両者の不一致を検知した場合、何らかの原因でネットワークに異常が生じた場合、機械システムの緊急停止スイッチが押下された場合、ライトカーテンなどの多光軸光電センサにより危険領域に人（身体の一部）の進入を検出したときなどの危険状態になった場合などがある。そして、上記の場合には、安全機能により、確実に制御対象の機械システムを安全な状態に動作させ、またはその動作に加えて安全な状態で停止させ、またはフェイルセーフが働いて機械システムが安全な状態で動作を強制的に停止させることができる。
また、安全機器は、安全スレーブに接続されている場合も有れば、安全機器自体が安全スレーブとなり、安全コントローラとデータの送受をすることもあり得る。この安全機器自体が安全スレーブともなる具体例としては、ライトカーテン（多光軸光電センサ）がある。つまり、危険域などに人が入ったことを検出する機能は安全機器（入力機器）であるし、検出結果の信号をネットワーク経由でマスタに通信する機能は安全スレーブとなる。
さらに、安全スレーブについての非安全情報とは、安全スレーブに接続された安全機器の非安全情報も含む概念であり、係る安全機器の非安全情報のみの場合もある。
この発明によれば、非安全情報を収集，記憶した安全スレーブ側で、非安全情報を送信するタイミングにあるか否かを判断し、送信タイミングに達したときに非安全情報を安全コントローラに向けて送信する。つまり、非安全情報は、さほど頻繁に送る必要がないものの、ある設定値に達したときは、メンテナンスや寿命の予知のために知りたいという要求がある。そして、係る設定値に達したか否かは、実際に非安全情報を収集している安全スレーブのみが知り得る。
従って、従来安全コントローラ側で行っていた送信するか否かの決定を安全スレーブ側に

移管することにより、適切なタイミングで非安全情報を送信することができる。安全コントローラ側にとっては、受信した非安全情報は全て有意義なものとなり、効率良く情報の収集が行える。

換言すると、安全コントローラ側からの要求に基づいて非安全情報を送るようにすると、不必要或いはあまり有益でない非安全情報を送る可能性があり、トラフィックに悪影響を生じるおそれがあるが、本発明によれば、予め設定した必要な送信タイミングに達したときに送信するので、ネットワークトラフィックへの影響が可及的に抑制される。

さらに、この発明によれば、各通信サイクル毎に非安全情報の送信のための時間を確保する必要があるが、通常、送信タイミングに達することが頻繁に無い場合には、１回の通信サイクルに設定する非全情報の送信のための時間は、例えば、１または少数分の安全スレーブからの送信ができる時間で有れば十分であり、トータル的に見ると通信時間が短縮される。また、仮に１個分の送信時間しかとっておらず、一度に送信タイミングに達した安全スレーブが複数存在したとしても、非安全情報の場合にはさほど緊急性がないので、送信できなかった安全スレーブの非安全情報は、次回以降の通信サイクルの時に送れば足りる。

また、上記した各発明は、安全コントローラからの要求に従って安全スレーブが安全情報や非安全情報を送信するものであるが、本発明はこれに限ることはなく、送信相手は任意である。

つまり、安全ネットワークに接続可能な安全スレーブであって、前記安全ネットワークを介して送られてきた他のノードからの要求に応じて、安全状態にあるか否かを特定する安全情報を送信する安全情報送信機能と、前記安全スレーブについての非安全情報を記憶する非安全情報記憶手段と、その非安全情報記憶手段に格納された前記非安全情報が、安全機器の寿命に関する経過条件を満たした際に、前記他のノードに向けて少なくともその経過条件を満たした非安全情報を送信する非安全情報送信制御機能と、を備えて構成することができる。

ここで他のノードとは、コンフィグレータ（コンフィグレーションツール）やモニタ装置や他のスレーブ等の安全ネットワークに接続されたノードである。

また、上記した各発明は、いずれも送信相手からの要求と言った外部トリガに基づいて安全情報や非安全情報を送信するものであるが、本発明はこれに限ることはなく、内部トリガに基づいて自発的に安全情報や非安全情報を送信するものも含む。

すなわち、安全ネットワークに接続可能な安全スレーブであって、送信条件を満たした場合に、安全状態にあるか否かを特定する安全情報を送信する安全情報送信機能と、前記安全スレーブについての非安全情報を記憶する非安全情報記憶手段と、その非安全情報記憶手段に格納された前記非安全情報が、安全機器の寿命に関する経過条件を満たした際に、前記安全ネットワークに接続された他のノードに向けて少なくともその経過条件を満たした非安全情報を送信する非安全情報送信制御機能と、を備えて構成することができる。

発明を実施するための最良の形態

本発明をより詳細に説明するにあたり、添付の図面に従ってこれを説明する。

図２は、本発明が適用される安全ネットワークシステムの一例を示している。同図に示すように、安全ＰＬＣ１（マスタ）と複数の安全スレーブ２が安全ネットワーク３を介して接続されている。安全ＰＬＣ１と安全スレーブ２とは、マスタースレーブ方式により情報の送受が行われる。更に、各安全スレーブ２には、安全ドアスイッチ，安全リミットスイッチや非常停止スイッチなどの他、各種の入力機器や出力機器等の安全機器４が接続されている。なお、安全ＰＬＣ１は、例えばＣＰＵユニット，マスタユニット（通信ユニット），Ｉ／Ｏユニットなどの複数のユニットを連結して構成するものが用いられる。この場合に、安全ネットワーク３に対しては、マスタユニットが接続される。

更に、モニタリングツール（パソコンなど）５が、安全ＰＬＣ１のＣＰＵユニットやマスタユニットに接続可能となっている。このモニタリングツール５は、後述するように安全ＰＬＣ１を介して安全スレーブ２、ひいてはそれに接続された安全機器４についての情報を収集し、管理する。

この安全ネットワークシステムを構成する各種装置は、全て安全機能（フェイルセーフ）が組み込まれたものを用いている。この安全機能は、安全であることを確認し、出力（制御）を行う機能である。そして危険状態になった場合にフェイルセーフが働いて、システムが安全側になって動作を停止させる。つまり、安全システムは、緊急停止スイッチが押下されたり、ライトカーテンなどのセンサが人（身体の一部）の進入を検出した場合等のネットワークシステムが危険状態になった場合に、フェイルセーフが働き、システムが安全側になって、動作が停止するようにするものである。換言すると、上記した安全機能により、安全であることが格納されたときのみ出力し、機械を動かすシステムである。よって、安全が確認できない場合には、機械が停止する。

次に、このような安全機能のうち、本発明の要部となる情報の送受について説明する。まず、安全ＰＬＣ１には、通信機能も組み込まれており、安全スレーブ２との間でマスタ・スレーブ方式で情報の送受を行うようになっている。基本的には従来と同様で、安全ＰＬＣ１は、安全ネットワーク３を介して各安全スレーブ２に対して順次要求を発し、その要求を受けた安全スレーブ２が、安全応答として安全情報を返すようになっている。

ここで本発明では、図３に示すように、安全ＰＬＣ１から各安全スレーブ２に対して一斉同報により要求を発行する。そして、全ての安全スレーブ２から要求に対する安全応答を受信したならば、直ぐに次の通信サイクルに移行するのではなく、一定期間の受信待機状態を設ける。この一定期間は、少なくとも１つの安全スレーブ２からの送信フレームを受信するために十分な時間を取る。

すなわち、この一定期間が、非安全情報の送受のための期間に設定される。そして、後述するごとく、非安全情報を送信するか否かの決定は、安全スレーブ２側で行い、非安全情報を送信することを決定した安全スレーブ２は、上記した一定期間の受信待機状態のときに非安全情報を安全ＰＬＣ１に向けて送信する。

つまり、非安全情報は、さほど頻繁に送信しなくても良いが、ある状況のときには確実に送りたいというタイミングがある。しかし、従来の安全ＰＬＣ１（マスタ）からの要求に対するレスポンスとして非安全情報を返す方式では、安全ＰＬＣ１は安全スレーブ２の状態が不知であるので、必ずしも上記した非安全情報を送りたいタイミングの時に要求を発するとは限らない。従って、タイミング良く非安全情報を取得するためには比較的頻繁に全ての安全スレーブに対して要求を発する必要がある。これに対し、本発明では、安全スレーブ２側で非安全情報の送信タイミングにあるか否かは簡単にわかるので、必要なときに確実に送信し、不必要なときは非安全情報を送信しないように制御できる。そして、上記した処理を実行するための安全ＰＬＣ１のＭＰＵにおける具体的な処理機能は、図４に示すフローチャートを実施するものである。

すなわち、電源が投入されると、所定のタイミングで全ての安全スレーブ２に対して一斉同報送信要求をする（ＳＴ１，ＳＴ２）。その後、受信タイムアウトするまで安全スレーブ２からの応答を待つ（ＳＴ３，ＳＴ４）。ここで受信タイムアウトは、送信要求をした後、一回の通信サイクルタイムとして設定した時間が経過した場合にタイムアウトとなる。具体的には、全ての安全スレーブ２からの安全応答を受信するための時間に、少なくとも１つの安全スレーブからの非安全情報を受信できる時間を加算した時間である。

そして、安全スレーブからの応答があった場合（ステップ４の分岐判断でＹｅｓ）には、ステップ５に進み、安全応答か否かを判断する。そして、安全応答の場合には、さらにその安全応答（受信した安全情報）の内容が安全か否かを判断する（ＳＴ６）。その判断結果が、異常（危険）の場合には、ステップ９に進み、フェイルセーフが働き、通信処理を停止し、出力遮断処理を実行する（ＳＴ７，ＳＴ８）。また、受信した内容が安全の場合には、ステップ３に戻り次の受信を待つ。

一方、ステップ５の分岐判断でＮｏ、つまり、非安全情報を受信した場合には、ステップ８に進み、所定の非安全情報の受信処理をする。つまり、受信した非安全情報をメモリに記憶したり、モニタに出力表示などをする。その後、ステップ３に戻り次の受信を待つ。

そして、受信タイムアウトしたならば（ステップ３の分岐判断でＹｅｓ）、今回の通信サイクルの処理は終了するので、次の通信サイクルの処理に移行する（ＳＴ７）。以後、上

記処理を繰り返し実行する。
なお、フローチャートでの表記は省略したが、実際には、受信タイムアウトした際に、安全ネットワーク３に接続された全ての安全スレーブ２からの応答を受信したか否かを判断する。もちろん、係る判断をするためには、安全応答を受信した安全スレーブの番号等を記憶する処理を行う。そして、受信していない安全スレーブが存在する場合には、ネットワーク上で異常があったと推定できるので、ステップ９における通信停止処理をする。また、このように１回でも受信できない安全スレーブがあった場合に、即停止するのではなく、Ｎ回連続して通信できない場合に通信停止処理をするようにすることもできる。これらの処理は、従来から行われるものである。
一方、安全スレーブ２は、安全ＰＬＣ１からの要求に従い、安全応答を返す機能と、非安全情報を収集するとともに記憶する機能と、記憶した非安全情報を所定のタイミングで安全ＰＬＣ１に対して送信する機能などを有する。係る機能を実現するための具体的な内部構造は、図５に示すようになっている。同図に示すように、安全ネットワーク３に接続し、安全ＰＬＣ１（マスタ）との間でデータの送受を行うネットワークインタフェース２１と、安全スレーブ２に接続された安全機器（図示省略）との間でデータの送受を行うための安全機器インタフェース２２と、システムＲＯＭ２４に格納されたプログラムを読み出し、システムＲＡＭ２５のメモリ領域を適宜使用して所定の処理を実行するＭＰＵ２３を備えている。ＭＰＵ２３は、ネットワークインタフェース２１を介して受信したマスタからの要求に従い、安全機器インタフェース２２を介して安全機器から取得した安全情報（安全／危険）を、ネットワークインタフェース２１，安全ネットワーク３を経由して安全ＰＬＣ１に返す処理を行う。
なお、安全スレーブ２自体が安全機器となることもでき、その場合に、安全機器インタフェース２２ではなく安全の有無などを検出する安全機器部となる。なおまた、安全スレーブ２における上記した各構成並びに動作原理は、従来のものと同様であるのでその詳細な説明を省略する。
さらに、ＭＰＵ２３は、安全機器４の動作状態（通電時間，ＯＮ／ＯＦＦ回数など）監視機能を備え、その監視機能を稼働させて得られた動作状態などの機器情報を非安全情報記憶部２６に格納する処理も実行する。そして、この非安全情報記憶部２６に格納された非安全情報（機器情報）を、後述するルールに従い安全ＰＬＣ１に送信する。
そして、非安全情報記憶部２６のデータ構造としては、例えば図６に示すようになる。ここで、入力１，２，３，…とは、安全スレーブ２の接点（端子台）の番号である。そして、図に示す登録する各項目のうち、機種種別，メーカー名，型式，寿命設定は、予め登録する。具体的には、例えば安全ＰＬＣ１や安全ネットワーク３に接続したツールを用い、安全ネットワーク３を介して安全スレーブ２に必要な情報を送ったり、安全スレーブ２に直接接続されたツールから情報を送り、安全スレーブ２のＭＰＵ２３が、ネットワークインタフェース２１を介して係る情報を取得するとともに、接点番号と関連付けて非安全情報記憶部２６に登録する。ここで寿命設定は、例えば寿命となる通電時間や、動作回数や、それらの値から所定の演算式により求められる値などである。なお、寿命が来た場合には、その安全機器４は交換時期にきたので、寿命結果が異常となり、安全情報（異常）を通知することになる。
また、状態，動作回数，通電時間，通知フラグなどは、実際のシステム稼働中にＭＰＵ２３が収集し、記録する。ここで、状態は、安全機器４が動作している（ＯＮ状態）か否か（ＯＦＦ情報）を識別する情報であり、動作回数は、安全機器４の接点のＯＮ／ＯＦＦ回数を示す情報であり、通電時間は、安全機器４に通電していた積算時間である。更に、寿命結果は、寿命がきたか否か（正常）を格納する。更に安全スレーブ２には、表示部を設け、非安全情報記憶部２６に格納された機器の情報を表示可能とするとよい。
そして、上記した通電時間並びにリレーＯＮ／ＯＦＦ回数等の収集アルゴリズムは、図７に示すフローチャートのようになっている。すなわち、ＭＰＵ２３は、自己診断並びに安全入力監視を行う（ＳＴ１１）。すなわち、自己診断は、接続された安全機器４に異常が発生していないかの検査を行うもので、この処理自体は従来公知のものである。また、安

全入力監視は、接続された安全機器４からの入力を監視するものである。そして、異常或いは入力があった場合には、どの安全機器４についての情報かも特定する。
次いで、ステップ１１による自己診断・安全入力監視を行った結果が、異常検出や安全入力がＯＦＦ（安全でない・危険）であったか否かを判断する（ＳＴ１２）。そして、異常等が検出された場合には、異常処理をする（ＳＴ１３）。つまり、異常状態等を図示省略の安全情報記憶部の該当する接点番号における自己診断結果やオンオフ情報の欄に格納する。なお、この診断結果等は、安全ＰＬＣ１からの安全情報の要求に対応し、安全応答として送信する。
一方、ステップ１２の分岐判断でＮｏ、つまり安全状態の場合には、通電時間を更新する（ＳＴ１４）。この更新処理は、例えば、前回の更新処理から現在までの時間をタイマで計測し（安全機器４が停止中（通電なし）は計時せずに一時停止する）、前回の更新処理した際の通電時間に上記計測した更新処理から現在までの通電時間を加算した値を新たな通電時間とし、その通電時間を、非安全情報記憶部２６に格納する。
次いで、安全機器４の入力状態がＯＦＦ（前回）からＯＮ（今回）に変わったか否かを判断する（ＳＴ１５）。つまり、前回ＯＦＦの場合には、ステップ１３の処理を経て非安全情報記憶部２６のＯＮ／ＯＦＦ情報の欄はＯＦＦになっている。従って、係る該当する接点番号のＯＮ／ＯＦＦ情報がＯＦＦの場合には、この分岐判断はＹｅｓとなる。そこで、ステップ１６に進み、動作カウントを１インクリメントする（ＳＴ１６）。この動作カウントが、非安全情報記憶部２６の動作回数の欄に登録されるとともに、非安全情報記憶部２６の状態の欄をＯＮにする。これにより、１回動作カウントがインクリメントされると、状態はＯＮとなるので、その次のサイクルでステップ１５の分岐判断を実行した場合（途中で安全入力ＯＦＦにならない場合）には、Ｎｏとなり、動作カウントはされない。また、既にＯＮ状態と登録されているので、再度ＯＮ状態と書き込まなくても問題はない。以後、上記処理を繰り返し実行することにより、安全機器４の状態を収集，記憶することができる。
なお、通電時間や動作回数の計時／計数は、上記したように、安全スレーブ２側でタイマ・カウンタを持って行っても良いし、安全スレーブ２に接続した安全機器４側で通電時間や動作回数を計時・計数するとともに、安全機器４側で常時記憶しておき、安全スレーブ２が所定タイミングで安全機器４に記憶された記憶情報を読み出すようにしてもよい。
さらに、本形態では、非安全情報記憶部２６に格納された非安全情報を送信するタイミングを決定する非安全情報送信制御部２７を設けている。この非安全情報送信制御部２７は、本形態では、非安全情報を通知する送信タイミングのしきい値を記憶するメモリである。
つまり、非安全情報送信制御部２７のデータ構造は、図８に示すように、通電時間，リレーＯＮ／ＯＦＦ回数並びに通信のリトライ回数において、１または複数の送信するタイミングを格納している。通電時間でいうと、通電時間が２００ｈ，４００ｈ，６００ｈ，８００ｈを超えた時に安全ＰＬＣ（マスタ）１へ現在値を通知することを意味する。また、リレーのＯＮ／ＯＦＦ回数の場合、３０００回，５０００回，８０００回，１００００回を超えた時に安全ＰＬＣ１へ現在値を通知することを意味する。さらに、リトライ回数の場合、通信サイクルが５００回，１０００回，１５００回，２０００回時にその時点でのリトライ回数を安全ＰＬＣ１に通知することを意味する。
要は、寿命なら途中経過のどこかの区切りになったことを知らせればよい。例えばリレーのＯＮ／ＯＦＦ回数の場合には、図示のように５０００，８０００などの区切り数値としてもよいし、割合で決めてもよい。例えば、図６中の入力１のドアスイッチのように８００００（回或いは時間）が寿命設定なら、３分の１の２６６６７回や、８０％の６４０００回と設定してもよい。つまり、安全に動作するとみなせる範囲で、寿命経過（消耗途中経過）のどの辺りかを表す情報を得るようにすればよい。
このように、ネットワーク情報（通信エラー時のリトライ回数、入出力応答時間など）の通知により、ネットワーク環境の改善ポイントの明確化や応答時間（安全対応システムでは安全停止時間）の最適化を図ることができる。つまり、異常・故障を頻繁に生じる安全

機器がある場合には、何か問題があると予測できるので、使用する機器自体を変更するなどシステムの変更を図ることができる。
なお、上記した通電時間やリレーＯＮ／ＯＦＦ回数は、非安全情報記憶部２６にアクセスして取得することができる。また、通信サイクルやリトライ回数の情報は、通信を制御・実行するチップ自体が記憶保持しているので、係る情報を収集することにより、送信タイミングに来たか否かを判別できる。すなわち、本形態では、非安全情報の送信タイミングに来たか否かの実際の判断は、ＭＰＵ２３が非安全情報送信制御部２７をアクセスして各非安全情報の送信タイミングを取得するとともに、非安全情報記憶部２６をアクセスして送信タイミングになったものがあるか否かを判断する。そして、送信タイミングになった非安全情報を検出すると、該当する情報を送信するようになる。
さらにまた、送信する非安全情報としては、上記したものに限られないのは言うまでもなく、例えば自己診断結果を非安全情報として送信するようにしても良い。つまり、自己診断で異常となった場合に、その異常の要因を示す情報を送信することもできる。一例としては、ライトカーテン機能内蔵デバイスの自己診断異常要因情報としては、インターロック配線異常，外部リレーモニタ異常，干渉光異常，制御出力異常並びにセンサ破壊などがある。
そして、ＭＰＵ２３における安全情報並びに非安全情報の送信の制御アルゴリズムは、図９に示すフローチャートのようになっている。すなわち、電源投入後、安全ＰＬＣ（マスタ）から送られてくる要求を待ち（ＳＴ２１，ＳＴ２２）、要求を受けると、安全応答をする（ＳＴ２３）。つまり、安全状態（安全／異常）を通知する。
次いで、非安全情報の送信タイミングに来ているか否かを判断する（ＳＴ２４）。つまり、非安全情報記憶部２６に格納された所定の情報や通信回数が、非安全情報送信制御部２７に格納された設定値に達しているか否かや、通知すべき自己診断結果の有無等を判断する。そして、非安全情報の送信タイミングに来ている場合には、該当する非安全情報を送信する（ＳＴ２５）。また、係る送信タイミングでない場合には、今回の通信サイクルでは非安全情報を送信しない旨を決定し、処理をしない（ＳＴ２６）。以後、上記処理を繰り返し実行することにより、安全ＰＬＣ（マスタ）１からの要求に応じて安全応答をするとともに、非安全情報の送信タイミングに達した場合には、安全スレーブ２側が主体となって積極的に非安全情報を送信する。なお、非安全情報の送信は、上記要求を受信後に安全ネットワーク３上を流れるデータを監視し、送信フレームが伝送されなくなったことを確認後送信するようになる。
一方、本形態におけるネットワークインタフェース２１による安全ネットワーク３上のデータの送受，通信プロトコルは、ＣＡＮ（Controller Area Network）を用いている。すなわち、良く知られているように、ＣＡＮにおいては、データリンク層で優先順位の管理を行い、通信回線上のデータがワーヤードＯＲされ、データ「１」とデータ「０」が重なった場合、回線上では、データ「０」が現れる。このとき、各安全スレーブ２は、それぞれ自己が送信しようとする送信フレーム（安全情報）を送出するとともに、回線上のデータを監視し、回線上を流れるデータと自己が送出したデータが一致するか否かを判断し、一致しない場合には今回の送信をする権限がないと判断し、それ以降のデータの送信を停止する。
これにより、送信フレームは、通常、ヘッダ情報，送信先・送信元アドレス，送信するデータの順に配列されているので、送信元アドレスつまり各安全スレーブ２のノード番号の小さいものから順に送信することができる。よって、図３に示したように、安全ＰＬＣ１からの一斉同報による要求に対し、安全スレーブ２は、▲１▼→▲２▼→▲３▼の順に安全応答を返すようになる。
上記した実施の形態によると、図１０に示すように、非安全情報の送信タイミングにない場合には、各安全スレーブ２が安全応答を返した後は、各安全スレーブ２はそのまま次の要求の受信を待つ。なお、図では、安全スレーブ▲１▼をＳ１で示し、安全スレーブ▲２▼をＳ２で示し、安全スレーブ▲３▼をＳ３で示している。つまり、Ｎ回目の通信サイクルでは、安全応答のみ実行されて処理を終了する。

次いで、１回の通信サイクルに設定された時間が経過して受信タイムアウトすると、安全ＰＬＣ（マスタ）１が次の要求を発するので、それを受けて各安全スレーブが順に安全応答をする。そして、このＮ＋１回目の通信サイクルでは、ある安全スレーブ２が非安全情報の送信タイミングに来た（所定の非安全情報が設定されたしきい値を越える）ので、安全応答の終了後に、非安全情報を送信する。このとき送る非安全情報は、設定を超えた非安全情報のみとしている。これにより、送信するデータ量を抑え、短時間で送信できるようにしている。もちろん、しきい値を越えた非安全情報以外の情報を併せて送るようにしても良い。

なお、上記した実施の形態では、安全ＰＬＣ１から各安全スレーブに対して発行する要求を一斉同報により行ったが、本発明はこれに限ることはなく、例えば、図１１に示すように、各安全スレーブ２に対し、▲１▼→▲２▼→▲３▼といように順番に要求を発し、要求を受けた安全スレーブ２が順次安全要求を返すようにしたものにおいても同様に適用できる。この場合でも、図示するように、設定されたしきい値を越え、非安全情報の送信タイミングになった非安全スレーブが存在する場合には非安全情報を送信するが、係るタイミングにない場合には非安全情報は送信されない。

なお、上記した実施の形態では、非安全情報送信制御部２７と非安全情報記憶部２６とを別に記載したが、１つのテーブルとして格納するようにしてももちろん良い。また、上記した実施の形態では、非安全情報送信制御部２７は、送信タイミングに達したか否かの判断基準となるしきい値を記憶するメモリとし、実際の判断はＭＰＵ２３が行うようにしたが、非安全情報送信制御部２７が非安全情報記憶部２６を監視し、送信タイミングに来た場合にＭＰＵ２３に対してトリガをかけるようにしてももちろん良い。

また、上記した実施の形態では、１回の通信サイクルの中で、安全情報を送信する安全応答のための期間の後に非安全情報を送信する期間を設けたが、本発明はこれに限ることはなく、特別に非安全情報を送信する時間を設けないようにすることもできる。すなわち、一例を示すと、非安全情報の送信タイミングにきた場合には、安全情報に替えて非安全情報を送信することである。

つまり、安全ＰＬＣから安全要求が来た場合に、通常は安全応答をするが、非安全情報の送信タイミングの場合には非安全情報を送信する。このとき、前記安全スレーブが安全状態であることを条件に非安全情報を送信するようにする。すると、非安全情報が送信されるということは、安全スレーブの安全が保障されることを意味する。従って、安全スレーブが安全状態である場合には、安全ＰＬＣは、安全情報（安全）を受信することにより直接、或いは、非安全情報を受信することにより間接的に安全スレーブが安全状態にあることを確認できる。また、仮に非安全状態を送信するタイミングにある場合に安全状態でなくなると、安全でないと言う安全情報（危険・異常）を送信するので、安全状態でなくなった場合にフェイルセーフが起動するまでの応答時間は、延ばさずに済む。換言すると、安全ネットワークのトラフィックに影響を与えず、非安全情報をスレーブ（安全スレーブ）からマスタ（安全コントローラ）に通知できる。

なお、この場合に、安全ＰＬＣ側は受信したフレームが、安全情報なのか非安全情報なのかがわからなくなるので、例えば、それらを区別するフラグを送信フレームに付加すると良い。

一方、上記した実施の形態で説明したスレーブは、マスタユニットとの間でＩ／Ｏ情報を送受し、そのマスタユニットを経由してコントローラ（ＰＬＣ）と係るＩ／Ｏ情報の送受を行ってシステムの制御を行う例を示し、マスタユニットとスレーブとの間は、マスタからの要求に対して所望のスレーブがレスポンスを返すといったマスタースレーブ方式を説明した。しかし、本発明で言うスレーブは、マスタースレーブ間通信を行うものに限られない。つまり、スレーブとは称するものの、通信方式は任意のものを利用できる。その点では、厳密に言うと一般的に定義されているスレーブとは異なる概念を含むものであると言える。

つまり、本発明で言う所のスレーブは、制御に必要なＩ／Ｏ情報をコントローラと送受する機能が有れば、安全情報や非安全情報を送受信する際の通信プロトコルは任意である。

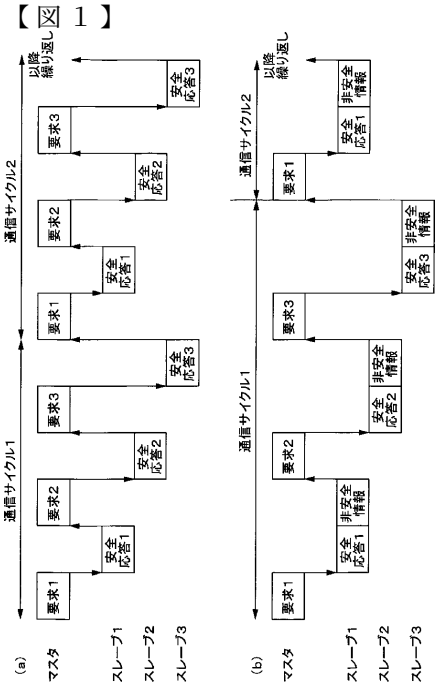
さらに本発明で送信対象とする安全情報，非安全情報の送信先は、マスタユニットやコントローラに限ることはなく、ネットワークに接続されたモニタ装置やコンフィグレーションツールや他のスレーブその他の装置等の自ノード以外のデバイス、つまり他ノードとすることができる。
そして、通信方式も、送信相手に応じて適宜選択できる。もちろん、送信するためのトリガも、上記したマスタからのリクエストのように外部からの要求（例えば、モニタ装置やコンフィグレーションツール等からの要求）に応じて行うものに限ることはなく、内部トリガ（内部のタイマ，一定の条件に合致したときに発生するイベントなど）に基づいて送信してもよい。
ここで、「内部トリガ」とは、スレーブ自身の所定の処理実行の結果に基づくもので、スレーブ内部で生成されるものである。そして、内部トリガの一例を示すと、以下のものがある。すなわち、異常状態が発生した時や、スレーブで取得した入出力機器の状態情報がしきい値に達したり、しきい値を越えたかどうかを判断すると、その判断結果が生じる。その判断結果をトリガ信号として利用するものがある。さらに、スレーブ内で時計を持たせておき、その時計により所定時間経過のたびに周期的にトリガ信号を生成したり、所定時刻でトリガ信号を生成するものもある。
上記した内部トリガをさらに詳細に説明すると、安全スレーブが情報を送信するタイミングを決定するためのものと、その情報を送信する際に非安全情報を送信するための条件を満たした場合に発するものがある。そして、前者の情報を送信するタイミングを決定するものとしては、内部タイマで一定時間結果した場合や、条件イベントが発生した場合などがある。後者の非安全情報の通知条件としての内部トリガは、非安全情報として収集している値がしきい知を超えた場合や、自己診断結果の結果通知が必要となった場合などがある。もちろん、この非安全情報の通知条件として、内部タイマを設け、通常の送信間隔よりも長い所定期間が経過した場合に非安全情報を通知するトリガを発生させるようにしても良い。
なお、各安全スレーブは、自己の内部タイマに基づいて情報を送信する場合、既に他の安全スレーブが送信中の場合には、送信を停止し、同時に送信しようとしてネットワーク上で衝突した場合には、優先順位の高い安全スレーブ（ノード番号の小さいもの）がそのまま通信を継続する。これにより、１回の通信サイクルで、所定の順で各安全スレーブから順次情報を送信することができる。そして、送信タイマを適宜に設定することにより、以後は、その順でスムーズに繰り返し情報の送信が行える。
そして、内部トリガに基づいてスレーブ側から自発的に情報を発信する場合、マスタからの要求に対する応答ではなく、例えば図１２に示すように、各安全スレーブが、それぞれ適宜のタイミングで安全情報を送信し、必要に応じて非安全情報を送信するように構成できる。この場合の送信先は、上記した実施の形態のようにマスタとすることもできるし、コンフィグレーションツールその他のデバイスとすることもできる。
そして、係る処理を実行するための安全スレーブの機能としては、図１３に示すフローチャートを実行するようにすれば良い。すなわち、電源投入後、送信条件になること、つまり、情報送信のための内部トリガが発生するのを待つ（ＳＴ３１，ＳＴ３２）。そして、情報送信のための内部トリガが発生すると、現在の安全状態（安全／異常）を安全情報として所定の相手に送信する（ＳＴ３３）。
次いで、非安全情報の送信タイミングに来ているか否かを判断する（ＳＴ３４）。つまり、非安全情報記憶部２６に格納された所定の情報や通信回数が、非安全情報送信制御部２７に格納された設定値に達しているか否かや、送信すべき自己診断結果があるか等を判断する。そして、条件を具備する場合には、該当する非安全情報を送信する（ＳＴ３５）。また、条件を具備しない場合には、今回の通信サイクルでは非安全情報を送信することなくステップ３１に戻り、次の内部トリガが発生するのを待つ。以後、上記処理を繰り返し実行することにより、安全スレーブは、適宜のタイミングで自発的に安全情報を発するとともに、非安全情報の送信タイミングに達した場合には、安全スレーブ側が主体となって積極的に非安全情報を送信する。

なお、非安全情報の送信は、安全情報を送信した後に安全ネットワーク３上を流れるデータを監視し、送信フレームが伝送されなくなったことを確認後送信するようになる。
また、この例でも、非安全情報の送信条件に来た場合に、安全スレーブが安全状態であることを条件に安全情報を送ることなく非安全情報のみを送信するようにすることもできる。つまり、安全スレーブが安全状態である場合には、安全ＰＬＣ等は、安全情報（安全）を受信することにより直接、或いは、非安全情報を受信することにより間接的に安全スレーブが安全状態にあることを確認できる。また、仮に非安全状態を送信するタイミングにある場合に安全状態でなくなると、安全でないと言う安全情報（危険・異常）を送信するので、安全状態でなくなった場合にフェイルセーフが起動するまでの応答時間は、延ばさずに済む。
なお、この場合に、安全ＰＬＣ側は受信したフレームが、安全情報なのか非安全情報なのかがわからなくなるので、例えば、それらを区別するフラグを送信フレームに付加すると良い。

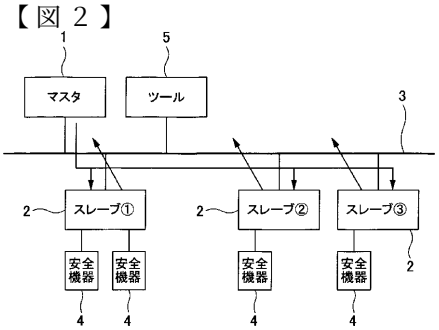
産業上の利用可能性

この発明では、機器情報記憶手段をスレーブに設け、スレーブに接続された機器の情報を記憶保持したため、その記憶保持したスレーブに接続された各機器についての情報をネットワークを介してコントローラやツールが収集することができる。そして、この発明では、システム全体で常時収集する必要がなくなるので、非安全情報の送受信がネットワークトラフィックに与える時間を軽減できる。しかも、非安全情報を収集している安全スレーブが、所望のタイミングで非安全情報を送信するので、安全コントローラその他の装置では非安全情報を効率良く収集することができる。

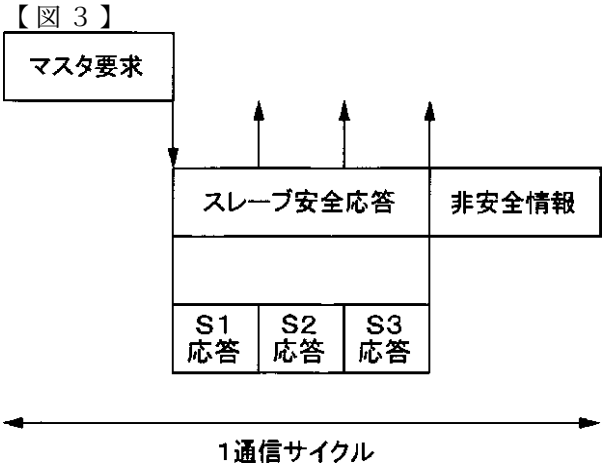
【図１】



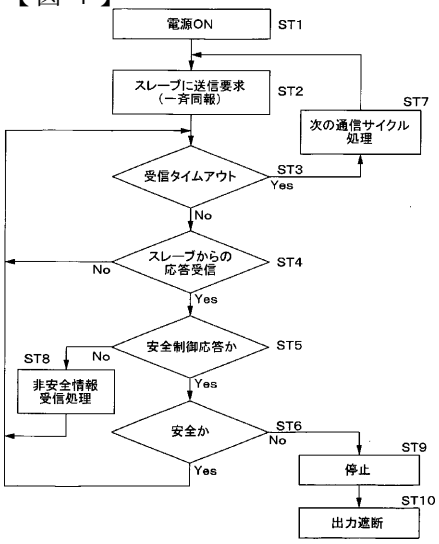
【図２】



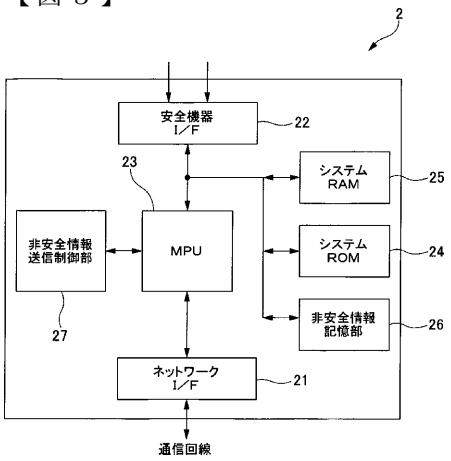
【図３】



【図４】



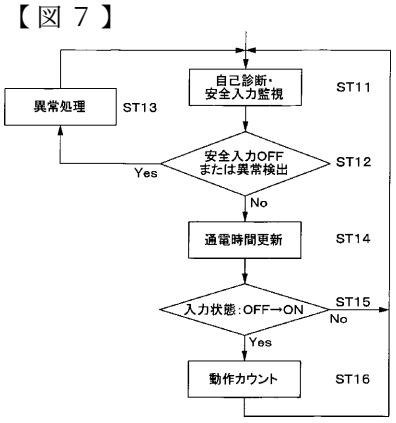
【図５】



【図６】

…	…		…	…		
通電時間	2877h		2897h	2899h		
寿命設定	80000		80000	50000		
動作回数	151		50	2		
状態	ON		ON	ON		
型式	XXXXX		YYYYY	ZZZZZ		
メーカー	A社		B社	A社		
機器種別	ドアSW		リミットSW	非常停止SW		
	入力1	入力2	入力3	入力4	…	

【図７】



【図８】

(a)

通電時間送信	
200h	送信
400h	送信
600h	送信
800h	送信

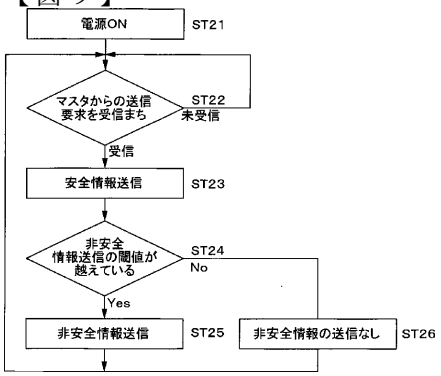
(b)

リレーON／OFF回数送信	
3000回	送信
5000回	送信
8000回	送信
10000回	送信

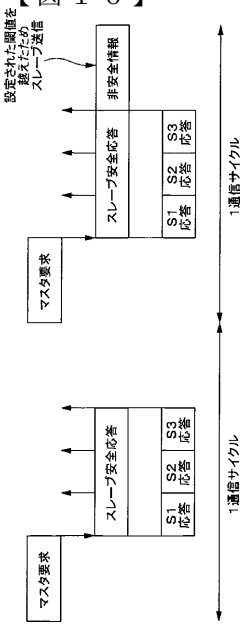
(c)

リトライ回数情報	
通信サイクル　500回	送信
通信サイクル　1000回	送信
通信サイクル　1500回	送信
通信サイクル　2000回	送信

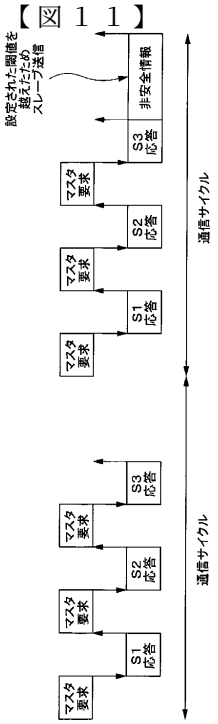
【図９】



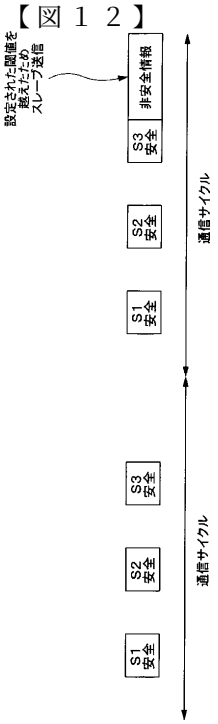
【図１０】



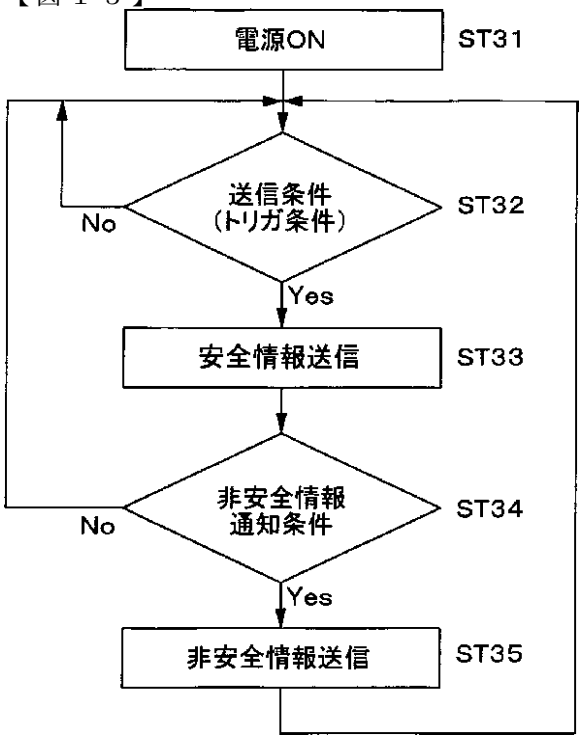
【図１１】



【図１２】



【図１３】


電源ON
ST31
送信条件
(トリガ条件)
ST32
No
Yes
安全情報送信
ST33
非安全情報
通知条件
ST34
No
Yes
非安全情報送信
ST35

フロントページの続き

審査官　中木　努

(56)参考文献　国際公開第０２／０９８０６５（WO，Ａ１）
国際公開第０２／０９７５４２（WO，Ａ１）
国際公開第０２／０９７５４３（WO，Ａ１）
国際公開第０３／００１３０６（WO，Ａ１）
国際公開第０３／００１３０７（WO，Ａ１）
特開平６－２３０８０６（ＪＰ，Ａ）
特開平５－７３８３（ＪＰ，Ａ）
特開平３－１１６３９５（ＪＰ，Ａ）
特開平４－４５６９７（ＪＰ，Ａ）
特開平８－２１１７９２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 12/28-46
G05B 9/02
G05B 19/048
G05B 23/02