(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4941748号
(P4941748)
(45)発行日　平成24年5月30日(2012.5.30)　(24)登録日　平成24年3月9日(2012.3.9)

(51)Int.Cl.　　F I
G05B 9/02 (2006.01)　　G05B 9/02　E
G05B 23/02 (2006.01)　　G05B 23/02　V

請求項の数 3　(全 12 頁)

(21)出願番号　特願2007-188462(P2007-188462)
(22)出願日　平成19年7月19日(2007.7.19)
(65)公開番号　特開2009-26063(P2009-26063A)
(43)公開日　平成21年2月5日(2009.2.5)
審査請求日　平成22年4月20日(2010.4.20)

(73)特許権者　000006507
横河電機株式会社
東京都武蔵野市中町２丁目９番３２号
(72)発明者　大迫　悟
東京都武蔵野市中町２丁目９番３２号　横河電機株式会社内

審査官　川東　孝至

最終頁に続く

(54)【発明の名称】安全制御システム

(57)【特許請求の範囲】
【請求項１】
制御バスに接続された制御ステーション間のデータ共有のために実装されているリンク伝送通信手段を有する分散型制御システムの前記制御バスに複数台の安全制御ステーションが接続され、前記制御バスを介して互いに通信する安全制御システムにおいて、
前記安全制御ステーションは
自己ステーションの送信データに安全情報を付加して前記リンク伝送通信手段に定周期でブロードキャストして前記リンク伝送通信手段が保持する自己ステーションに対応するリンク伝送通信データを更新すると共に、
自己の起動するタイミングで前記リンク伝送通信手段にアクセスし、他ステーションの送信データを保持する前記リンク伝送通信データより自己処理に必要なデータを受信し、受信データの集合体に対して前記安全情報の診断を行うことを特徴とする安全制御システム。
【請求項２】
前記安全制御ステーションは、前記制御バスとのインターフェイスに前記安全情報の生成及び診断を実行するセーフティレイヤを備えることを特徴とする請求項１に記載の安全制御システム。
【請求項３】
前記安全情報は、ＣＲＣコードを含むことを特徴とする請求項１または２に記載の安全制御システム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、分散型制御システムと統合された安全制御システムにおいて、両システムで共通使用される制御バスに接続された安全制御ステーション間の通信の安全確保に関するものである。
【背景技術】
【０００２】
分散型制御システムに統合された安全制御システムについては、特許文献１に技術開示がある。図８は、特許文献１に開示されている、分散型制御システムと安全制御システムの統合環境を示す機能ブロック図である。
【０００３】
鎖線の領域Ａで示した分散型制御システムと、鎖線の領域Ｂで示した安全制御システムとは、共通の制御バス１に接続され、同じくこの制御バスに接続された両システムに共通の操作監視ステーション２と通信する。
【０００４】
分散型制御システムＡにおいて、制御ステーション３１，３２は、制御バス１を介して操作監視ステーション２と通信すると共に、プラント４の機器（図示せず）と通信して制御する。
【０００５】
安全制御システムＢにおいて、安全制御ステーション５１，５２は、制御バス１を介して操作監視ステーション２と通信すると共に、プラント４の機器と通信し、プラント４からのトリップ要求を受信してプラントの停止操作を実行する。
【０００６】
安全制御システムＢは、分散型制御システムＡと同一の制御バス１上で，SIL3レベルの認証を受けた安全通信を行うことにより、従来からの分散型制御システムの制御通信を混在させた統合システムの構築が可能となっている。
【０００７】
尚、安全制御ステーション間通信は、各安全制御ステーションで検知した異常を、いち早く他の安全制御ステーションに通知することで、プラントの異常にいち早く対応でき、危険防止や被害範囲の縮小に効果がある。
【０００８】
安全制御システムにおける安全通信とは、既存の非安全な通信システム上で、安全関連データが、間違いなく確実に通信相手に受け渡されたことをチェックできる仕組みを持った通信方式のことである。
【０００９】
安全通信では、通信のアプリケーションレイヤの部分に、非安全な外界と安全機能を分離するセーフティレイヤを設け、通信によって発生しうる危険事象（データの破壊，抜け，遅延等）をすべてチェックする。
【００１０】
図９は、２台の安全制御ステーション５１，５２間の安全通信の仕組みを説明する機能ブロック図である。ＢＯＯＬ型，整数型，実数型のデータ形式の通信データは、バインディング変数と呼ばれる独自のデータ形式に変換されて制御バス１上を流れる。
【００１１】
このバインディング変数には、データ値の他に、送信時刻のタイムスタンプ，シーケンス番号，通信データ全体のエラーチェックのためのＣＲＣ（Cyclic Redundancy Check）コードが格納されている。これらの安全情報を作成するのが、安全制御ステーション５１の送信側ファンクションブロック５１ａであり、変換されたバインディング変数５１ｂが制御バス１に送信される。
【００１２】

一方、受信した安全制御ステーション５２側では、受信したバインディング変数５２ｂを、受信側ファンクションブロック５２ａにより全ての通信異常をチェックする。異常を検知した際は，あらかじめ指定されたフェイルセーフ値をデータとして出力し、データステータスに異常を出力すると共に、エラー発生のシステムアラームを発報する。

【００１３】

送信側のファンクションブロック５１ａと受信側のファンクションブロック５２ａにより、２台の安全制御ステーション５１，５２間の安全通信のためのセーフティレイヤ６０を形成する。

【００１４】

図１０は，複数の送受信データがある場合の安全通信のイメージ図である。送信側の安全制御ステーションの送信装置は、複数の送信用バインディング変数を一旦集めて、相手ステーションに通信する。相手ステーション受信装置は、対応する受信用のバインディング変数に分配する。

【００１５】

図１１は、ユーザが作成する安全通信のアプリケーションの機能ブロック図である。基本は、バインディング変数を仲介した１対１の安全通信である。ユーザは、このバインディング変数と入出力用のファンクションブロックを作成し、アプリケーションロジックに接続する。

【００１６】

【特許文献１】特開２００６－１６４１４３号公報

【発明の開示】

【発明が解決しようとする課題】

【００１７】

従来の安全制御ステーション間の安全通信は、データひとつひとつに安全通信を保証するための情報を付加し、受信側のファンクションブロックに設けたセーフティレイヤで受信データの診断を行うことで、分散型制御システムの通信データも流れる同一制御バス１上で，安全通信を保証することができた。

【００１８】

しかしながら、従来の安全制御ステーション間の安全通信では、以下の問題点がある。

（１）バインディング変数とファンクションブロックの両方のアプリケーションをユーザが作成しなくてはならず、エンジニアリングが面倒。→エンジニアリング工数の増加

【００１９】

（２）データ個別の送受信であるので、通信及びＣＰＵパフォーマンスを消費するため、多くのステーション間でデータ共有ができない。→通信パフォーマンスの制限

【００２０】

（３）データ１点１点で診断を行うため、送信側の安全制御ステーションの停止で、データ数分のアラームが通知される。→アラームの洪水が発生

【００２１】

本発明は上述した問題点を解決するためになされたものであり、簡単なエンジニアリングで、通信及びＣＰＵパフォーマンスを消費せずに多数のステーション間での情報共有を可能にする安全制御システムの実現を目的としている。

【課題を解決するための手段】

【００２２】

このような課題を達成するために、本発明の構成は次の通りである。

（１）制御バスに接続された制御ステーション間のデータ共有のために実装されているリンク伝送通信手段を有する分散型制御システムの前記制御バスに複数台の安全制御ステーションが接続され、前記制御バスを介して互いに通信する安全制御システムにおいて、

前記安全制御ステーションは

自己ステーションの送信データに安全情報を付加して前記リンク伝送通信手段に定周期でブロードキャストして前記リンク伝送通信手段が保持する自己ステーションに対応するリ

ンク伝送通信データを更新すると共に、
自己の起動するタイミングで前記リンク伝送通信手段にアクセスし、他ステーションの送信データを保持する前記リンク伝送通信データより自己処理に必要なデータを受信し、受信データの集合体に対して前記安全情報の診断を行うことを特徴とする安全制御システム。

【００２４】
（２）前記安全制御ステーションは、前記制御バスとのインターフェイスに前記安全情報の生成及び診断を実行するセーフティレイヤを備えることを特徴とする（１）に記載の安全制御システム。

【００２５】
（３）前記安全情報は、ＣＲＣコードを含むことを特徴とする（１）または（２）に記載の安全制御システム。

【発明の効果】

【００２７】
本発明によれば、次のような効果を期待することができる。
（１）制御バスを利用するリンク伝送通信手段を使って安全通信データを送信できるため、多数のステーション間での情報共有が簡単に、かつ高速にできる。受信側の安全制御ステーションは、自由に好きなタイミングでデータを受信できるので、アプリケーションの追加が簡単に行える。

【００２８】
（２）リンク伝送の決まったデータ領域を使って安全通信データをやり取りするので、その領域とのデータのアクセスを行うためのファンクションブロックと、割付け定義のデータベースだけがあればよいので、エンジニアリングが容易である。

【００２９】
（３）受信側の安全制御ステーションは、受信データの集合体に対して安全情報の診断を行うので、ＣＰＵ負荷が小さく、万一送信側の制御ステーションが停止しても、アラームは該当ステーションに対するものだけを出力すればよく、アラームの洪水が発生しない。

【発明を実施するための最良の形態】

【００３０】
以下、本発明を図面により詳細に説明する。図１は、本発明を適用した安全制御システムの一実施形態を示す機能ブロック図である。図６で説明した従来システムと同一要素には同一符号を付して説明を省略する。

【００３１】
本発明は、分散型制御システムでの制御ステーション間でデータ共有するために実装されているリンク伝送通信手段を利用し、安全制御ステーション間の安全通信をより簡単にデータ共有を可能とした安全制御システムである。

【００３２】
図１において、リンク伝送通信手段が実装された制御バス１００に、本発明が適用された安全制御ステーション５０１（タグ名SCS0101），５０２（タグ名SCS0102），…５０ｎ（タグ名SCS010n）が、インターフェイス６０１，６０２，…６０ｎを介して接続されている。これらインターフェイスの中に安全通信のためのセーフティレイヤが形成される。

【００３３】
各安全制御ステーションの機能構成を、安全制御ステーション５０２で代表して示せば、ユーザアプリケーションから他の安全制御ステーションに通信したい自己の送信データは、インターフェイス６０２を介して定周期で制御バス１００に送信（矢印Ｓで示す）される。

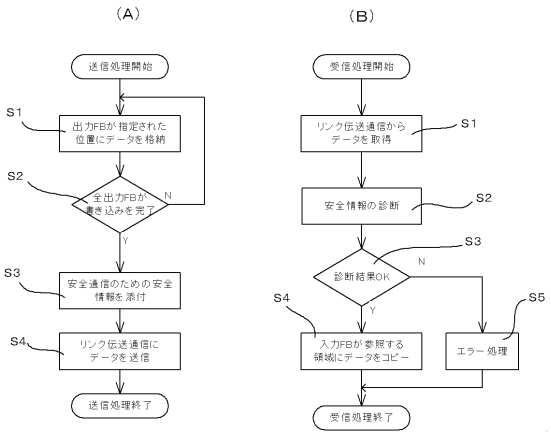
【００３４】
安全制御ステーション５０２は、同時に他の安全ステーションの送信データを制御バス１００より受信（矢印Ｒで示す）して、インターフェイス６０２を介してアプリケーションが取得することができる。

【００３５】
その他の安全制御ステーションについても同一機能を備えている。リンク伝送通信手段は、各安全制御ステーションのデータが定周期の送信により更新されるまで、送信データを保持する。
【００３６】
リンク伝送データは、安全制御ステーション毎に例えば３２バイトデータを１００ミリ秒周期で、各安全制御ステーションに通知するブロードキャスト通信である。各安全制御ステーションは、ロジックの処理に必要なデータを他の安全制御ステーションから受信し、自己の演算結果を送信する。
【００３７】
送信側の安全制御ステーションは、自己の送信データがどの安全制御ステーションで受信されているかの意識はない。そのデータを必要とする安全制御ステーションが、自分の起動するタイミングでデータ受信する、パッシブ形の通信である。
【００３８】
図２は、各安全制御ステーションが持っている安全通信のデータ領域とその通信内容を示すデータ構成図である。タグ名は、図１と共通である。各安全制御ステーションは、関連する制御ステーション数のデータ領域を持ち、自己の領域だけを送信バッファとして書き込みが可能である。
【００３９】
各データ領域は３２バイトのサイズであるが、この実施形態ではリンク伝送通信手段を利用して安全通信を行うために、前半１６バイトをデータ領域に、後半１６バイトを安全情報としている。安全情報は、１６バイトのデータに対して、シーケンス番号や送信時刻を表すタイムスタンプ及びＣＲＣコードを付加している。
【００４０】
図３は、本発明を適用した安全制御ステーション５０１と５０２間の、安全通信の仕組みを説明する機能ブロック図である。本発明の特徴部は、制御バス１００とのインターフェイス６０１及び６０２に新規に追加したセーフティレイヤ７００である。
【００４１】
送信側安全制御ステーション５０１では、アプリケーションロジックの結果を安全通信データとして送信するための出力ファンクションブロック８０１の送信データ対して、このセーフティレイヤ７００の機能により、安全情報を付加して制御バス１００上にリンク伝送データとして送信する。
【００４２】
受信側安全制御ステーション５０２では、制御バス１００を介して安全制御ステーション５０１から受信したリンク伝送データに付加されている安全情報をセーフティレイヤ７００の機能により診断し、異常を検知するとシステムアラームを送信する。異常診断後に入力ファンクションブロック８０２を経由してアプリケーションロジックに渡される。
【００４３】
図４は、リンク伝送データを扱うためのアプリケーションとユーザ定義のデータベースを説明する機能ブロック図であり、安全制御ステーション５０２（タグ名SCS0102）を代表として示している。
【００４４】
アプリケーションロジック上は、入力ファンクションブロック８０２ａ及び出力ファンクションブロック８０２ｂを置くだけのシンプルな構造である。実際の入出力ファンクションブロックと送受信データのどれが結びついているかが、データベース８０２ｃに保持される送信定義と受信定義である。
【００４５】
ユーザは、このデータベースの送信定義と受信定義を、自由に割付けて設定することができる。入出力ファンクションブロック８０２ａ，８０２ｂは，このデータベースの定義を参照して、自分がどのデータにアクセスするのかを知ることができる。

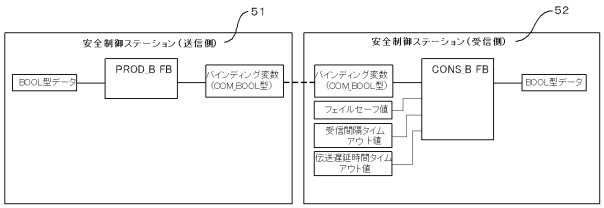
【００４６】
このように、入出力ファンクションブロックとリンク伝送通信手段間で、データ位置の取り決めをあらかじめ行い、安全通信の送受信データを１６バイトのデータの集合体としたことで、安全情報を一つにまとめることができる。
【００４７】
図５は、本発明を適用した安全制御システムの安全通信の送信処理及び受信処理の手順を示すフローチャートである。図５（Ａ）は送信処理のフローチャート、図５（Ｂ）は受信処理のフローチャート示す。
【００４８】
図５（Ａ）の送信処理では、ステップＳ１及びステップＳ２により、出力ファンクションブロックが指定位置に全データを書き込みが終了すると、ステップＳ３で安全通信のための情報が付加され、ステップＳ４でリンクデータ通信にデータ送信する。
【００４９】
図５（Ｂ）の受信処理では、ステップＳ１でリンク伝送通信から必要データを取得し、ステップＳ２で安全情報の診断を行う。ステップＳ３での診断がＯＫであれば、データはステップＳ４で集合体のままコピーされ、入力ファンクションブロックが必要なデータを取り出す。ステップＳ３での診断がパスしなければステップＳ５でエラー処理する。
【００５０】
本来、リンク伝送通信手段は、分散型制御システムの制御ステーション（ＦＣＳ）では、グローバルスイッチとしてＦＣＳ間のデータ通信のために使用されてきた。安全制御ステーション（ＳＣＳ）でも、このリンク伝送通信手段を用いることにより、通信相手がＦＣＳなのか、ＳＣＳなのかを認識さえすれば、ＦＣＳ－ＳＣＳ間のデータ共有にもこの通信手段を使用することができる。
【００５１】
図６は、分散型制御システムの制御ステーションと安全制御ステーション間のデータ共有を説明する機能ブロック図である。図は、分散型制御システムの制御ステーションFCS0101のリンク伝送データを、安全制御ステーションSCS0103が受信し、入力ファンクションブロックを介してロジックに入力しているイメージである。
【００５２】
図７は、安全制御ステーションが受信する、制御ステーションデータと安全制御ステーションデータの相違を示すデータ構成図である。図７（Ａ）は、安全制御ステーション（ＳＣＳ）のデータ構成、図７（Ｂ）は制御ステーション（ＦＣＳ）のデータ構成である。
【００５３】
ＦＣＳデータは３２バイト全てデータであるのに対して、ＳＣＳデータは前半１６バイトのみがデータになる。ＦＣＳにとっては、ＳＣＳからの送信データの１６バイトについては、グローバルスイッチとして参照が可能である。
【図面の簡単な説明】
【００５４】
【図１】本発明を適用した安全制御システムの一実施形態を示す機能ブロック図である。
【図２】安全制御ステーションが持っている安全通信のデータ領域とその通信内容を示すデータ構成図である。
【図３】本発明を適用した安全制御ステーション間の安全通信の仕組みを説明する機能ブロック図である。
【図４】リンク伝送データを扱うためのアプリケーションとユーザ定義のデータベースを説明する機能ブロック図である。
【図５】本発明を適用した安全制御システムの安全通信の送信処理及び受信処理の手順を示すフローチャートである。
【図６】分散型制御システムの制御ステーションと安全制御ステーション間のデータ共有を説明する機能ブロック図である。
【図７】安全制御ステーションが受信する、制御ステーションデータと安全制御ステーシ

ョンデータの相違を示すデータ構成図である。
【図８】分散型制御システムと安全制御システムの統合環境を示す機能ブロック図である。
【図９】安全制御ステーション間の安全通信の仕組みを説明する機能ブロック図である。
【図１０】複数送受信データがある場合の安全通信のイメージ図である。
【図１１】ユーザが作成する安全通信のアプリケーションの機能ブロッ図である。
【符号の説明】
【００５５】
２　操作監視ステーション
３　制御ステーション
１００　制御バス
５０１，５０２，…５０ｎ　安全制御ステーション
５０１，５０２，…５０ｎ　インターフェイス

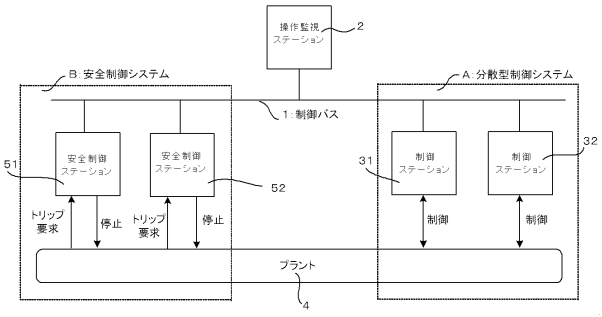
【図５】



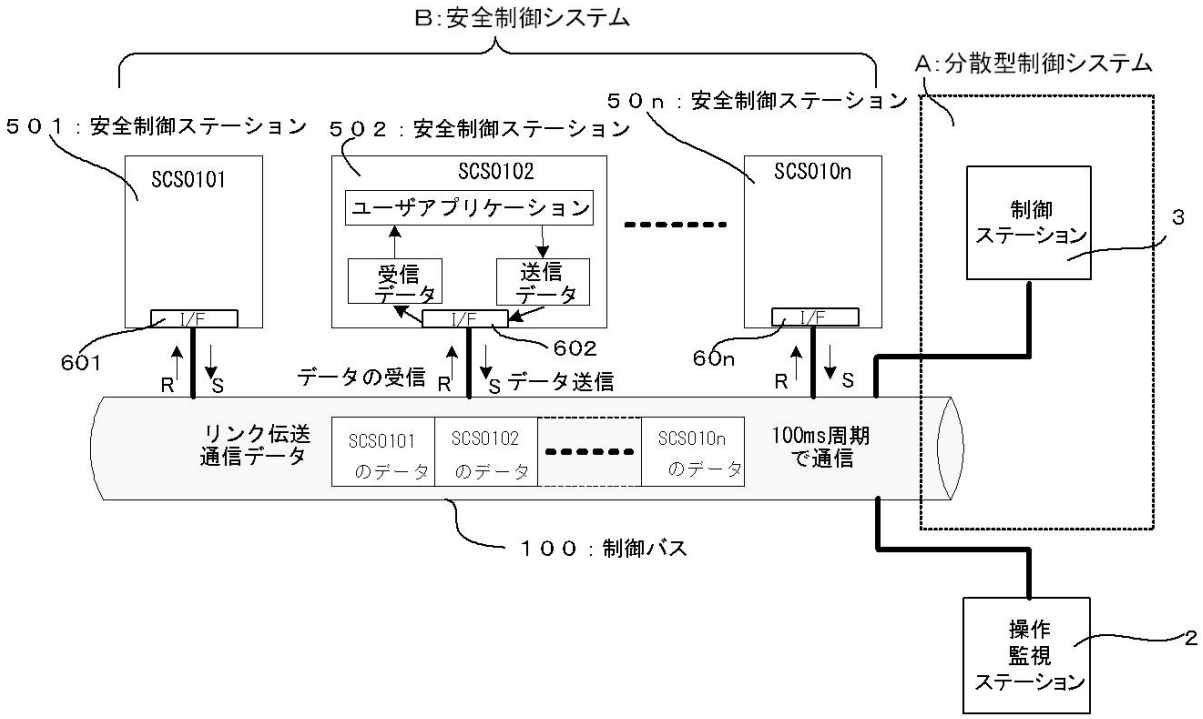
【図１１】



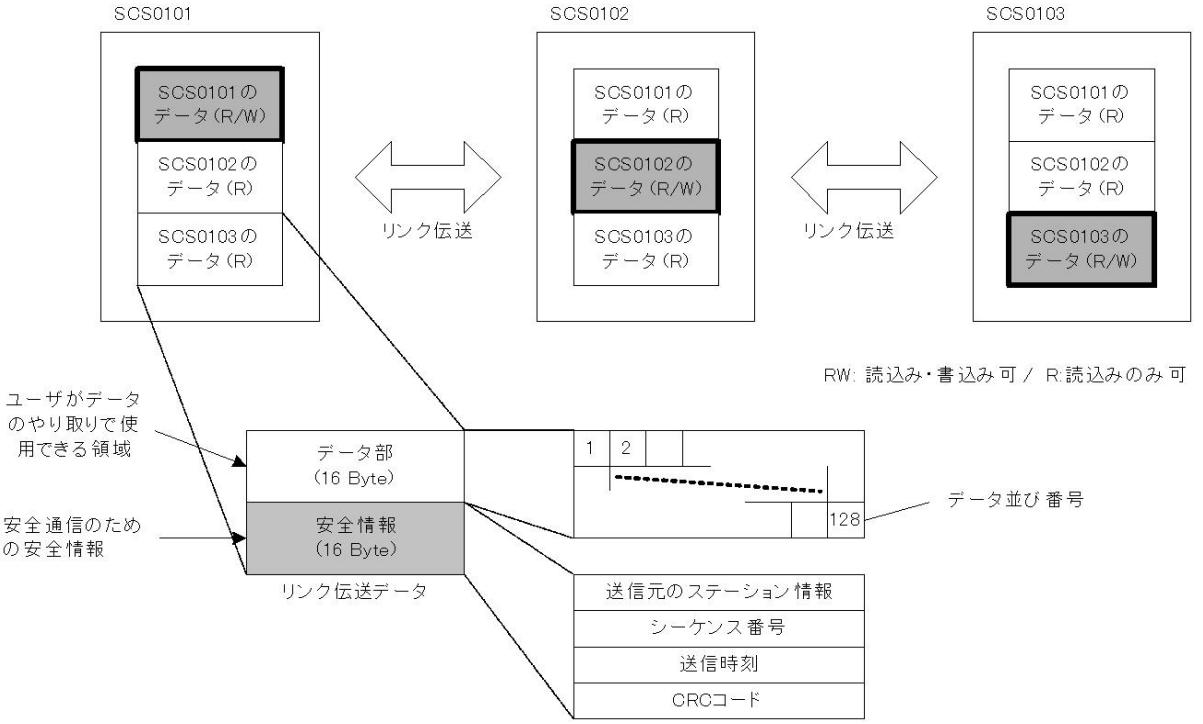
【図８】



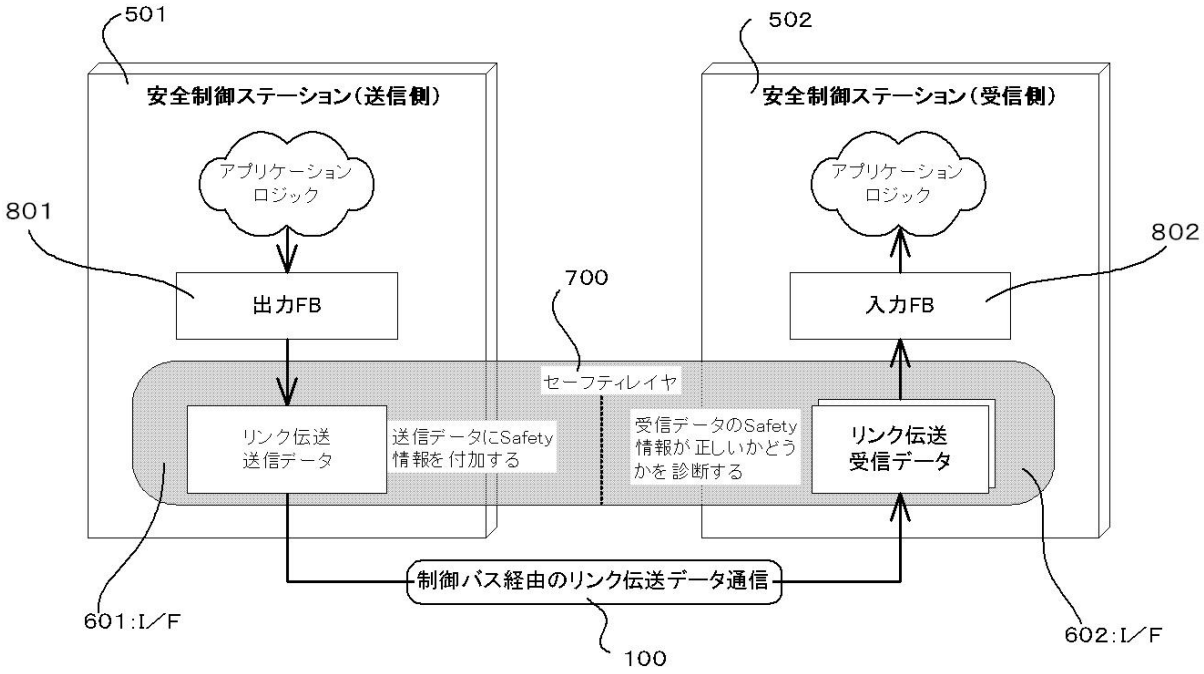
【図１】


B:安全制御システム
A:分散型制御システム
５０１：安全制御ステーション
５０２：安全制御ステーション
５０ｎ：安全制御ステーション
SCS0101
SCS0102
SCS010n
ユーザアプリケーション
受信データ
送信データ
I/F
601
602
60n
R
S
データの受信
データ送信
制御ステーション
3
リンク伝送通信データ
SCS0101のデータ
SCS0102のデータ
SCS010nのデータ
100ms周期で通信
１００：制御バス
操作監視ステーション
2

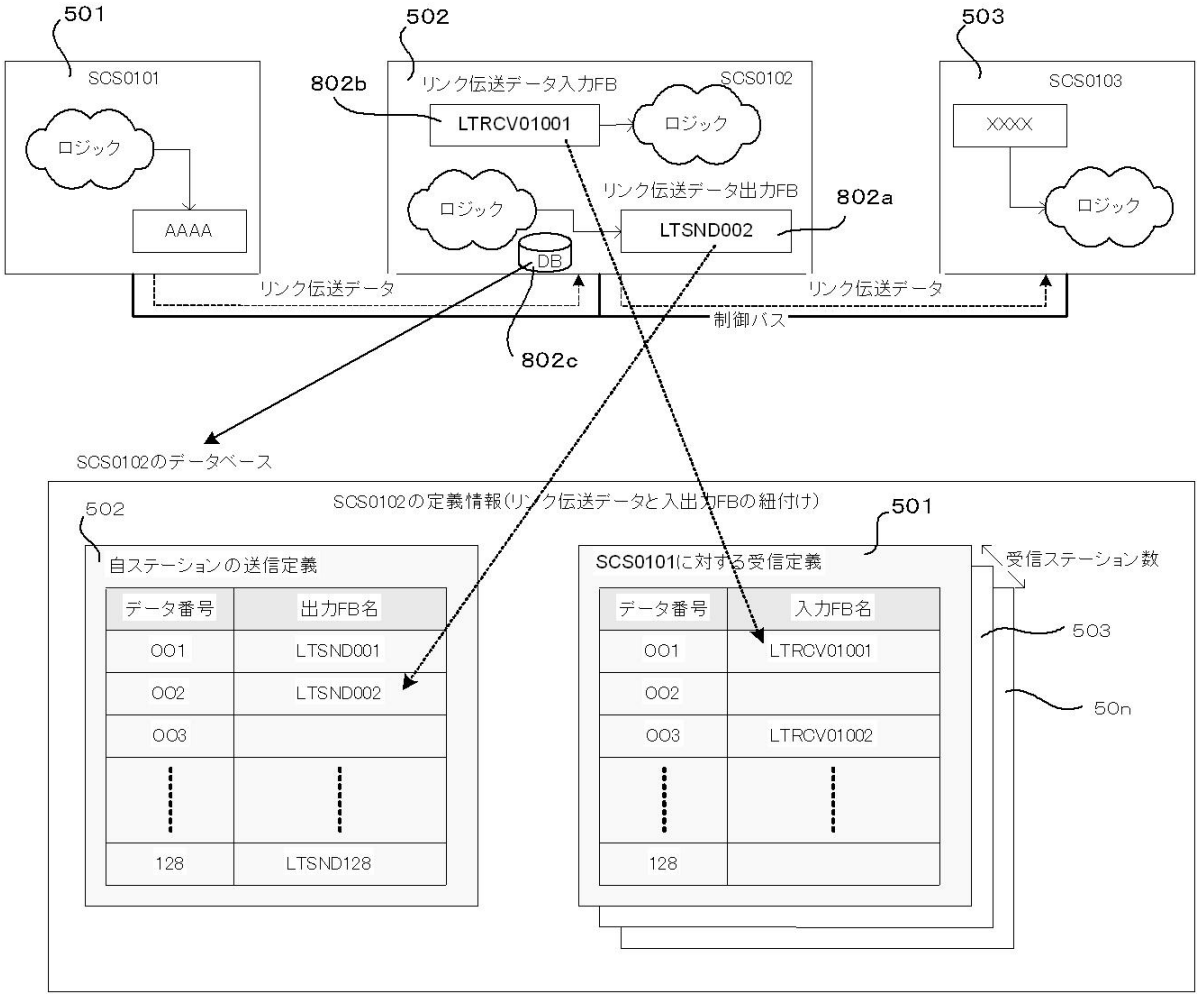
【図２】


SCS0101
SCS0102
SCS0103
SCS0101のデータ(R/W)
SCS0102のデータ(R)
SCS0103のデータ(R)
SCS0101のデータ(R)
SCS0102のデータ(R/W)
SCS0103のデータ(R)
SCS0101のデータ(R)
SCS0102のデータ(R)
SCS0103のデータ(R/W)
リンク伝送
リンク伝送
RW: 読込み・書込み可 / R:読込みのみ可
ユーザがデータのやり取りで使用できる領域
安全通信のための安全情報
データ部(16 Byte)
安全情報(16 Byte)
リンク伝送データ
1
2
128
データ並び番号
送信元のステーション情報
シーケンス番号
送信時刻
CRCコード

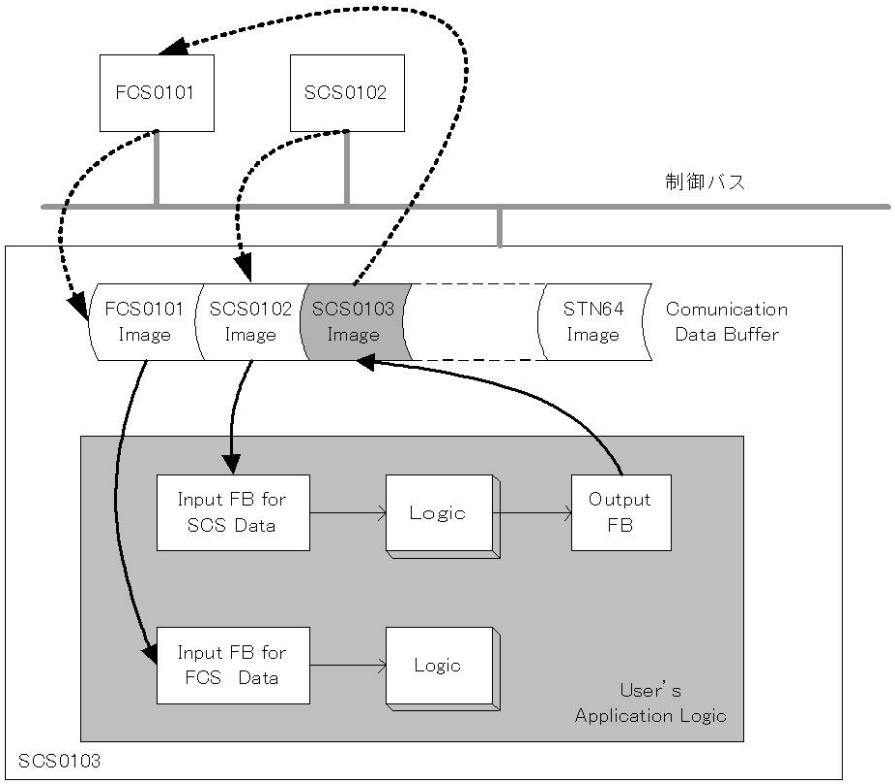
【図３】


501
安全制御ステーション(送信側)
アプリケーション
ロジック
801
出力FB
700
セーフティレイヤ
リンク伝送
送信データ
送信データにSafety
情報を付加する
受信データのSafety
情報が正しいかどう
かを診断する
リンク伝送
受信データ
502
安全制御ステーション(受信側)
アプリケーション
ロジック
802
入力FB
制御バス経由のリンク伝送データ通信
100
601:I/F
602:I/F

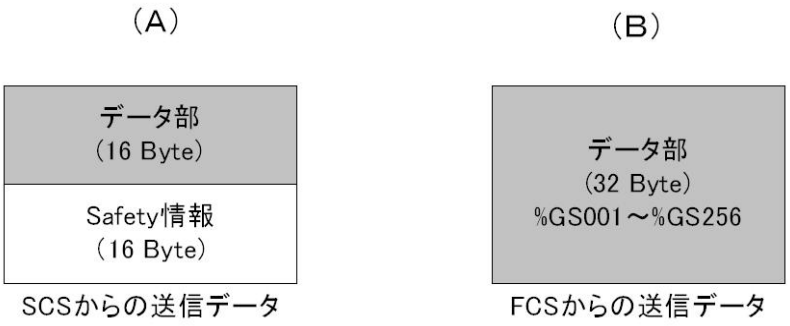
【図４】


501
SCS0101
ロジック
AAAA
502
802b
リンク伝送データ入力FB
SCS0102
LTRCV01001
ロジック
ロジック
リンク伝送データ出力FB
802a
LTSND002
DB
503
SCS0103
XXXX
ロジック
リンク伝送データ
リンク伝送データ
制御バス
802c
SCS0102のデータベース
SCS0102の定義情報(リンク伝送データと入出力FBの紐付け)
502
自ステーションの送信定義
データ番号
出力FB名
001
LTSND001
002
LTSND002
003
128
LTSND128
501
SCS0101に対する受信定義
受信ステーション数
データ番号
入力FB名
001
LTRCV01001
002
003
LTRCV01002
128
503
50n

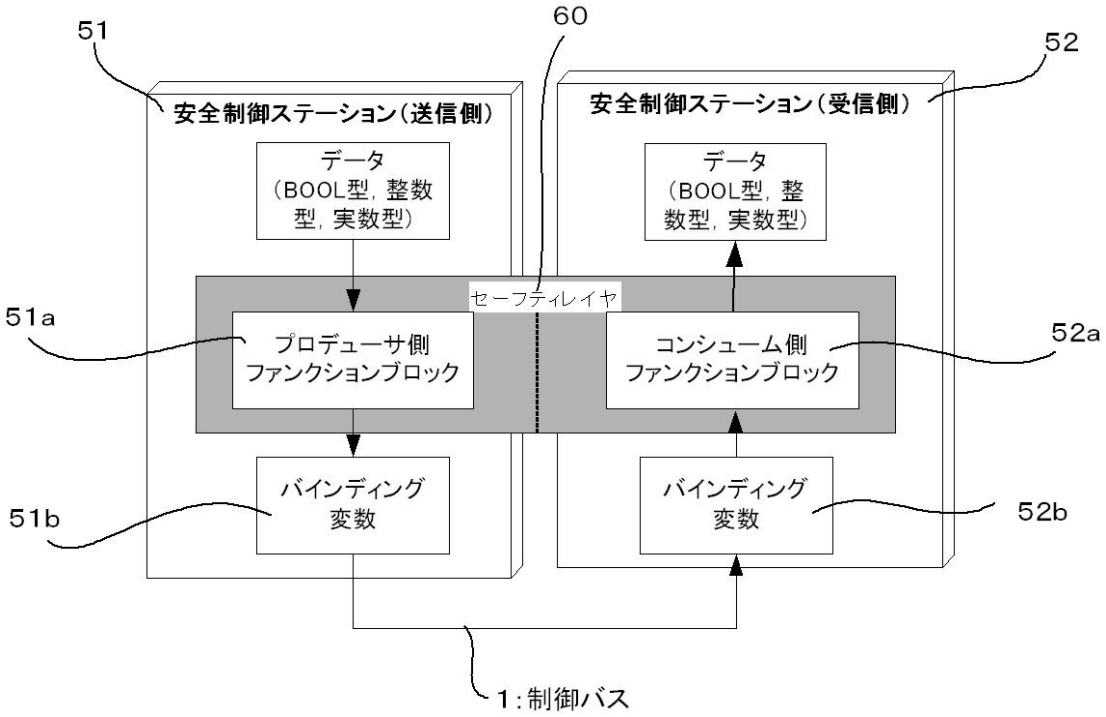
【図６】


FCS0101
SCS0102
制御バス
FCS0101 Image
SCS0102 Image
SCS0103 Image
STN64 Image
Comunication Data Buffer
Input FB for SCS Data
Logic
Output FB
Input FB for FCS Data
Logic
User's Application Logic
SCS0103

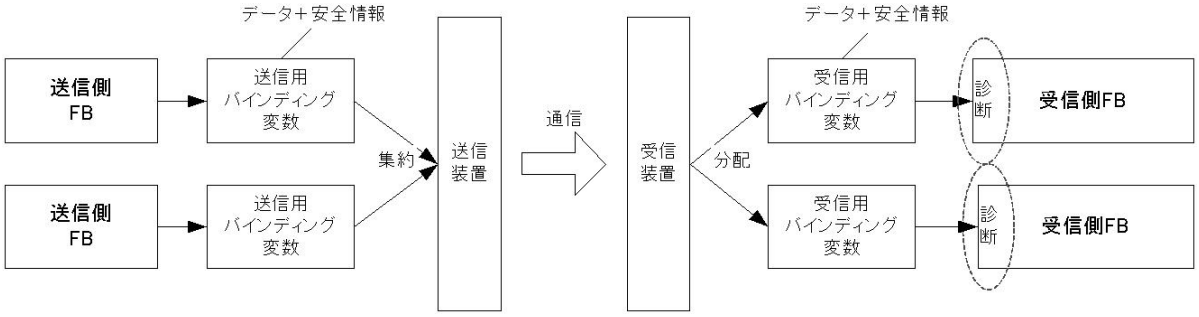
【図７】


(A)
(B)
データ部
(16 Byte)
Safety情報
(16 Byte)
SCSからの送信データ
データ部
(32 Byte)
%GS001～%GS256
FCSからの送信データ

【図９】


51
60
52
安全制御ステーション（送信側）
安全制御ステーション（受信側）
データ
（BOOL型，整数型，実数型）
データ
（BOOL型，整数型，実数型）
セーフティレイヤ
51a
プロデューサ側
ファンクションブロック
コンシューム側
ファンクションブロック
52a
バインディング
変数
バインディング
変数
51b
52b
1：制御バス

【図１０】


データ＋安全情報
送信側
FB
送信用
バインディング
変数
集約
送信
装置
通信
受信
装置
分配
データ＋安全情報
受信用
バインディング
変数
診断
受信側FB
送信側
FB
送信用
バインディング
変数
受信用
バインディング
変数
診断
受信側FB

フロントページの続き

(56)参考文献 特開２００６－２７６９５７（ＪＰ，Ａ）
特開２０００－２５９２１５（ＪＰ，Ａ）
特開２００７－０２６０１０（ＪＰ，Ａ）
特開２００６－１６４１４３（ＪＰ，Ａ）
特開平０５－０５３６１９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０５Ｂ　　９／００－　９／０５
Ｇ０５Ｂ　２３／００－２３／０２