(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2022年11月17日(17.11.2022)

WIPO | PCT

(10) 国際公開番号
WO 2022/239116 A1

(51) 国際特許分類:
G05B 23/02 (2006.01) *H04L 12/70* (2013.01)
H04L 12/66 (2006.01) *G05B 19/048* (2006.01)

(21) 国際出願番号： PCT/JP2021/017904

(22) 国際出願日： 2021年5月11日(11.05.2021)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

(71) 出願人: 三菱電機株式会社(**MITSUBISHI ELECTRIC CORPORATION**) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目７番３号 Tokyo (JP).

(72) 発明者: 宮▲崎▼ 清人(**MIYAZAKI, Kiyohito**); 〒1008310 東京都千代田区丸の内二丁目７番３号 三菱電機株式会社内 Tokyo (JP).

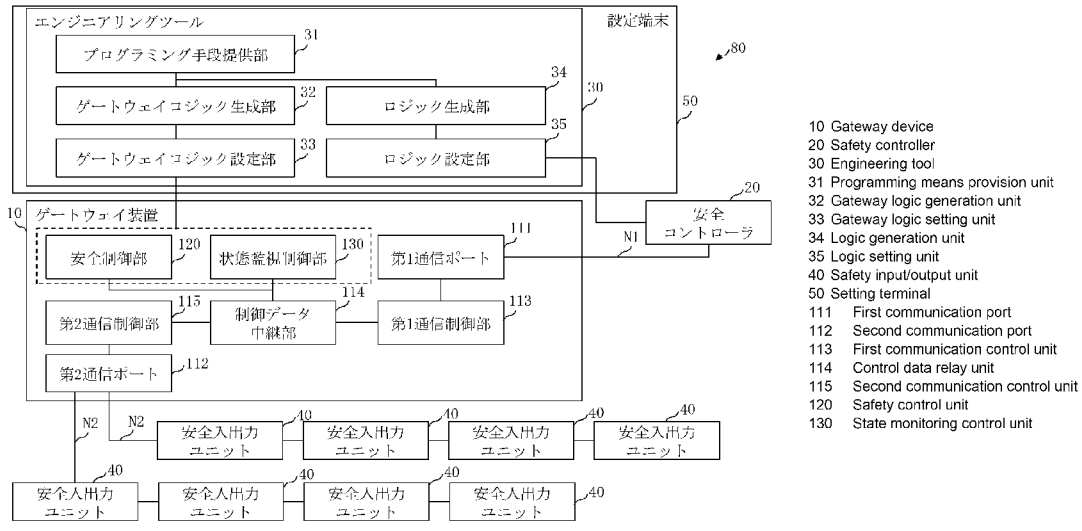
(74) 代理人: 弁理士法人クロスボーダー特許事務所(**CROSS-BORDER PATENT FIRM**); 〒2470056 神奈川県鎌倉市大船二丁目１７番１０号３階 Kanagawa (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ,

(54) **Title:** GATEWAY DEVICE, GATEWAY CONTROL METHOD, AND GATEWAY CONTROL PROGRAM

(54) 発明の名称： ゲートウェイ装置、ゲートウェイ制御方法、及び、ゲートウェイ制御プログラム

図5



(57) **Abstract:** A gateway device (10) according to the present invention relays safety data communication between a safety input/output unit (40) and a safety controller (20) that controls the safety input/output unit (40). The gateway device (10) comprises a state monitoring control unit (130) and a safety control unit (120). The state monitoring control unit (130) manages a control state that corresponds to the state of a safety control system (80) and that is a safe state or an unsafe state. The state monitoring control unit (130) applies safety data that the gateway device (10) has received from the safety input/output unit (40) to state transition information indicative of state transition of the control state, and thereby controls the state transition of the control state. When the control state is changed from the unsafe state to the safe state, the safety control unit (120) generates safety data that indicates the safe state and that is transmitted to the safety input/output

WO 2022/239116 A1

［続葉有］

NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

一 国際調査報告(条約第21条(3))

unit (40).

(57) 要約:ゲートウェイ装置(１０)は、安全入出力ユニット(４０)と安全入出力ユニット(４０)を制御する安全コントローラ(２０)との間における安全データの通信を中継し、状態監視制御部(１３０)と、安全制御部(１２０)とを備える。状態監視制御部(１３０)は、安全制御システム(８０)の状態に対応する状態であって、安全状態と非安全状態とのいずれかの状態である制御状態を管理し、かつ、ゲートウェイ装置(１０)が安全入出力ユニット(４０)から受信した安全データを、制御状態についての状態遷移を示す状態遷移情報に適用することにより制御状態の状態遷移を制御する。安全制御部(１２０)は、制御状態が非安全状態から安全状態に遷移した場合に、安全入出力ユニット(４０)に送信する安全データであって、安全状態を示す安全データを生成する。

明　細　書

発明の名称 ：

ゲートウェイ装置、ゲートウェイ制御方法、及び、ゲートウェイ制御プログラム

技術分野

[0001] 本開示は、ゲートウェイ装置、ゲートウェイ制御方法、及び、ゲートウェイ制御プログラムに関する。

背景技術

[0002] 安全制御は、作業者の保護、又は事故の防止等に関わる制御であり、フェールセーフな特性を保証するように実現される。作業者の保護は、具体例として、生産設備のインタロック制御により実現される。事故の防止は、具体例として、化学プラントの温度制御により実現される。安全制御を実現するシステムは安全関連系（ＳＲＳ）と呼ばれ、国際規格であるＩＥＣ（Ｉｎｔｅｒｎａｔｉｏｎａｌ　Ｅｌｅｃｔｒｏｔｅｃｈｎｉｃａｌ　Ｃｏｍｍｉｓｓｉｏｎ）　６１５０８シリーズ等において、安全関連系が満たすべき要求事項が規定されている。

安全制御に関する重要な性能の一つに安全応答時間がある。安全応答時間は、システムへの非定常データの入力に対して安全コントローラが反応し、安全コントローラが安全状態への遷移を示すデータを出力するための時間である。非定常データは、システムを安全状態に遷移させるべきことを示す情報である。安全状態は、具体例として、安全停止の制御を実行すべき状態である。安全応答時間が短いほど、生産設備の危険部への安全距離を小さく設計することができる。そのため、安全応答時間の短さは生産設備の小型化等に寄与する。

一方、ＦＡ（Ｆａｃｔｏｒｙ　Ａｕｔｏｍａｔｉｏｎ）又はＰＡ（Ｐｒｏｃｅｓｓ　Ａｕｔｏｍａｔｉｏｎ）における制御は、分散して配置されたコントローラと、入出力ユニット等の機器同士が通信することにより実現され

るため、機器間をフィールドバス又はフィールドネットワーク等により接続することによって実現される。また、安全制御に必要な入出力データの通信において、通信するデータに対して特別な通信エラー対策を施す安全通信技術が用いられる。安全通信においてエラー対策のための処理等が実行されるために、安全通信は安全応答時間を構成する一要素となる。

ＩＥＣ　６１７８４－３シリーズで標準化された複数種類の安全通信方式の各々に対応した製品が市場に流通しており、互いに異なる安全通信方式に対応する製品の間に相互接続性は基本的にない。なお、互いに異なる安全通信方式に対応する装置同士を接続して生産ラインを構築する場合に対応するため、安全通信方式を変換する製品が市場に存在する。

[0003] 特許文献１は、安全通信方式を採用する安全ネットワークシステムにおいて、安全応答時間を短縮する技術を開示している。特許文献１を適用しないシステムでは、安全スレーブに入力された安全情報全てを安全コントローラに送信するため、安全スレーブの台数が増加した場合に台数に応じて通信サイクル時間が増加し、安全応答時間が長くなるという課題があった。ここで、安全スレーブは安全入出力ユニットとも呼ばれる。

そこで、特許文献１に係る安全スレーブは、複数の入力安全情報に基づいて安全条件を満足するか否かを判断する安全判断手段を備える。安全判断手段は、具体例として、入力安全情報を用いた論理演算により簡単に安全条件を満足するか否かを判断することができる手段である。安全スレーブは、安全コントローラに対して入力安全情報そのものではなく、安全判断手段が判断した判断結果を送信する。そのため、特許文献１によれば、安全コントローラに送信すべきデータ量が少なくなるために１回のサイクルタイムを短縮することができ、その結果、安全応答時間を短縮することができる。

なお、特許文献１は、前述の技術の適用対象を安全スレーブに限定しておらず、具体例として、異種フィールドバスを接続するゲートウェイに対して前述の技術を適用する構成のほか、判断結果の送信元であるノード以外のデバイスを判断結果の送信先とする構成も開示している。

先行技術文献

特許文献

[0004] 特許文献1：国際公開第２００３／００１３０６号

発明の概要

発明が解決しようとする課題

[0005] 特許文献１が開示する技術によれば、送信データ量の削減を通して安全応答時間を短縮することができるが、安全入出力ユニットから安全コントローラに至る通信パスの伝送遅延が大きい場合に、安全応答時間を比較的安価なコストで短縮することができないという課題がある。当該技術には、通信周期を改善する効果はあるものの伝送遅延を改善する効果はないことがその一因である。

ここで、通信パスの伝送遅延が大きくなる場合は、具体例として、システム構成が下記に示す構成である場合である。なお、伝送遅延時間には一般的に幅があるが、伝送遅延の平均値又は中央値ではなく、ジッタを加味して受容可能な到達性を確率的に保証する時間を伝送遅延時間と呼ぶこととする。

構成１：定時性の低い拠点内ネットワークを介する構成。当該ネットワークは、具体例として、ソフトウェアレベルでの中継処理が経路に存在するネットワーク、タイムスロット管理若しくはＱｏＳ（Ｑｕａｌｉｔｙ　ｏｆ　Ｓｅｒｖｉｃｅ）制御等の遅延の抑制制御がなされていないネットワーク、又は、送信の衝突が起こりうる無線部分を含むネットワークである。

構成２：安全コントローラが公衆網を隔てた先にある構成。具体例として、安全コントローラが遠隔地のデータセンター又はクラウドにある構成。

[0006] 本開示は、安全入出力ユニットから安全コントローラに至る通信パスの伝送遅延が大きい場合であっても、安全応答時間を比較的安価なコストで短縮することを目的とする。

課題を解決するための手段

[0007] 本開示に係るゲートウェイ装置は、

安全制御システムが備える安全入出力ユニットと前記安全入出力ユニットを制御する安全コントローラとの間における安全データの通信を中継することにより前記安全入出力ユニットと前記安全コントローラとの安全コネクションを確立するゲートウェイ装置であって、

前記安全制御システムの状態に対応する状態であって、安全状態と非安全状態とのいずれかの状態である制御状態を管理し、かつ、前記ゲートウェイ装置が前記安全入出力ユニットから受信した安全データを、前記制御状態についての状態遷移を示す状態遷移情報に適用することにより前記制御状態の状態遷移を制御する状態監視制御部と、

前記制御状態が前記非安全状態から前記安全状態に遷移した場合に、前記安全入出力ユニットに送信する安全データであって、前記安全状態を示す安全データを生成する安全制御部と

を備える。

発明の効果

[0008] 本開示によれば、ゲートウェイ装置は安全入出力ユニットと安全コントローラとの間に位置しており、安全制御部は安全入出力ユニットに送信する安全データであって安全状態を示す安全データを生成する。そのため、本開示によれば、安全コントローラが当該安全データを安全入出力ユニットに送信する場合と比較して、当該安全データが安全入出力ユニットに到達するまでの時間を短縮することができる。また、状態監視制御部は制御状態が安全状態と非安全状態とのいずれであるかを判断する機能を有していれば十分である。従って、本開示によれば、安全入出力ユニットから安全コントローラに至る通信パスの伝送遅延が大きい場合であっても、安全応答時間を比較的安価なコストで短縮することができる。

図面の簡単な説明

[0009] [図1]実施の形態１に係る安全コントローラ２０のハードウェア構成例を示す図。

[図2]実施の形態１に係る安全入出力ユニット４０のハードウェア構成例を示

す図。

[図3]実施の形態１に係るゲートウェイ装置１０のハードウェア構成例を示す図。

[図4]実施の形態１に係る設定端末５０のハードウェア構成例を示す図。

[図5]実施の形態１に係る安全制御システム８０の構成例を示す図。

[図6]実施の形態１に係る安全制御部１２０と状態監視制御部１３０との構成例を示す図。

[図7]実施の形態１に係る通信パケットを説明する図。

[図8]実施の形態１に係る制御ロジックの具体例を示す図。

[図9]実施の形態１に係る安全制御システム８０の基本動作を示すフローチャート。

[図10]実施の形態１に係るゲートウェイ装置１０の基本動作を示すフローチャート。

[図11]実施の形態１に係る安全制御システム８０の動作を示すフローチャート。

[図12]実施の形態１に係るゲートウェイ装置１０の特徴的な動作を示すフローチャート。

[図13]実施の形態１に係る安全データマッピング表１９４の具体例を示す図。

[図14]実施の形態１に係る出力定義情報１９１の具体例を示す図。

[図15]実施の形態１に係る安全制御システム８０の動作を示すフローチャート。

[図16]実施の形態１に係るゲートウェイ装置１０の特徴的な動作を示すフローチャート。

[図17]実施の形態１に係る状態遷移表１９２の具体例を示す図。

[図18]実施の形態１に係るエンジニアリングツール３０の動作を示すフローチャート。

[図19]実施の形態１に係る全体状態遷移表の具体例を示す図。

[図20]実施の形態１に係るエンジニアリングツール３０の動作を説明する表。

[図21]実施の形態１に係るエンジニアリングツール３０の動作を説明する表。

[図22]実施の形態１に係る出力定義情報１９１の具体例を示す図。

[図23]実施の形態１の変形例に係るゲートウェイ装置１０のハードウェア構成例を示す図。

発明を実施するための形態

[0010] 実施の形態の説明及び図面において、同じ要素及び対応する要素には同じ符号を付している。同じ符号が付された要素の説明は、適宜に省略又は簡略化する。図中の矢印はデータの流れ又は処理の流れを主に示している。また、「部」を、「回路」、「工程」、「手順」、「処理」又は「サーキットリー」に適宜読み替えてもよい。

[0011] 実施の形態１．

以下、本実施の形態について、図面を参照しながら詳細に説明する。

[0012] ＊＊＊構成の説明＊＊＊

図１から図４は、安全制御システム８０が備える各構成要素のハードウェア構成例を示している。安全制御システム８０は、安全コントローラ２０と、安全入出力ユニット４０と、ゲートウェイ装置１０と、設定端末５０とを備える。安全制御システム８０は、ファクトリーオートメーション（ＦＡ）又はプロセスオートメーション（ＰＡ）の分野における、安全制御に関するシステムである。各構成要素は、安全関連系（ＳＲＳ）の要求事項に従って開発されたハードウェアであり、典型的にはコンピュータである。必要な安全度水準（ＳＩＬ）を満たすために、各構成要素の一部又は全体、あるいは構成要素である機器が二重化されていてもよい。

[0013] 安全コントローラ２０は、プロセッサ２１と、メモリ２２と、設定ポート２３と、第１ポート２４と、バス２５と、不揮発メモリ２６とを備える。

プロセッサ２１は、演算処理を行うＩＣ（Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒ

ｃｕｉｔ）であり、かつ、コンピュータが備えるハードウェアを制御する。プロセッサ１１は、具体例として、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）、ＤＳＰ（Ｄｉｇｉｔａｌ　Ｓｉｇｎａｌ　Ｐｒｏｃｅｓｓｏｒ）、又はＧＰＵ（Ｇｒａｐｈｉｃｓ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）である。安全コントローラ２０は、プロセッサ２１を代替する複数のプロセッサを備えてもよい。複数のプロセッサは、プロセッサ２１の役割を分担する。

メモリ２２は、典型的には、揮発性の記憶装置である。メモリ２２は、主記憶装置又はメインメモリとも呼ばれる。メモリ２２は、具体例として、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）である。メモリ２２に記憶されたデータは、必要に応じて不揮発メモリ２６に保存される。

設定ポート２３は、エンジニアリングツール３０による設定を行うためのポートである。設定ポート２３は、具体例として、ＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）端子である。

第１ポート２４は、通信方式１に対応したポートであり、レシーバ及びトランスミッタである。第１ポート２４は、具体例として、通信チップ又はＮＩＣ（Ｎｅｔｗｏｒｋ　Ｉｎｔｅｒｆａｃｅ　Ｃａｒｄ）である。

バス２５は、内部通信を実現するための信号線である。

不揮発メモリ２６は、典型的には、不揮発性の記憶装置である。不揮発メモリ２６は、具体例として、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）、ＨＤＤ（Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅ）、又はフラッシュメモリである。不揮発メモリ２６は、プログラム及びパラメータ等を格納する。不揮発メモリ２６に記憶されたデータは、必要に応じてメモリ２２にロードされる。メモリ２２及び不揮発メモリ２６は一体的に構成されていてもよい。

[0014] 安全入出力ユニット４０は、安全Ｉ／Ｏ（Ｉｎｐｕｔ／Ｏｕｔｐｕｔ）又は安全Ｉ／Ｏデバイスとも呼ばれる。Ｉ／ＯはＩＯとも表記される。安全入出力ユニット４０は、プロセッサ４１と、メモリ４２と、ＩＯポート４３と、第２ポート４４と、バス４５と、不揮発メモリ４６とを備える。

プロセッサ４１はプロセッサ２１と同様である。メモリ４２はメモリ２２と同様である。第２ポート４４は、通信方式１の代わりに通信方式２に対応したポートである点を除いて第１ポート２４と同様である。バス４５はバス２５と同様である。不揮発メモリ４６は不揮発メモリ２６と同様である。

ＩＯポート４３は、安全入出力ユニット４０は、接続機器からデータを受け付け、制御装置にデータを出力するためのポートである。ＩＯポート４３は、具体例として、ＵＳＢ端子である。接続機器は、具体例として、センサとスイッチとの少なくともいずれかである。制御装置は、具体例として、アクチュエータとリレーとの少なくともいずれかである。接続機器と制御装置とは一体的に構成されていてもよい。

[0015] ゲートウェイ装置１０は、プロセッサ１１と、メモリ１２と、第１ポート１３と、第２ポート１４と、バス１５と、不揮発メモリ１６と、設定ポート１７とを備える。ゲートウェイ装置１０は安全ゲートウェイとも呼ばれる。

プロセッサ１１はプロセッサ２１と同様である。メモリ１２はメモリ２２と同様である。第１ポート１３は第１ポート２４と同様である。第２ポート１４は第２ポート４４と同様である。バス１５はバス２５と同様である。不揮発メモリ１６は、不揮発メモリ２６と同様であり、ゲートウェイ制御プログラムを記憶している。設定ポート１７は設定ポート２３と同様である。

なお、本明細書に記載されているいずれのプログラムも、コンピュータが読み取り可能な不揮発性の記録媒体に記録されていてもよい。不揮発性の記録媒体は、具体例として、光ディスク又はフラッシュメモリである。本明細書に記載されているいずれのプログラムも、プログラムプロダクトとして提供されてもよい。

[0016] 設定端末５０は、ソフトウェアであるエンジニアリングツール３０を実行するための端末であり、具体例として、一般的なＰＣ（Ｐｅｒｓｏｎａｌ Ｃｏｍｐｕｔｅｒ）である。設定端末５０は、プロセッサ５１と、メモリ５２と、バス５５と、不揮発メモリ５６とに加え、設定ポート５３を備える。

プロセッサ５１はプロセッサ２１と同様である。メモリ５２はメモリ２２

と同様である。バス５５はバス２５と同様である。不揮発メモリ５６は不揮発メモリ２６と同様であり、エンジニアリングプログラムを記憶している。

設定ポート５３は、設定ポート２３と同様であり、安全コントローラ２０とゲートウェイ装置１０との各々に対してプログラム及びパラメータ等を設定するためのポートである。

[0017] 図５は、安全制御システム８０の構成例を示している。安全制御システム８０の構成する要素は適宜一体的に構成されていてもよい。安全制御システム８０が備える各構成要素の機能は、ソフトウェアにより実現される。

[0018] 安全コントローラ２０は、安全入出力ユニット４０からの入力を元に制御ロジックを実行し、制御ロジックを実行した結果に基づく出力を安全入出力ユニット４０に対し出力する機能を持つ。即ち、安全コントローラ２０は安全入出力ユニット４０を制御する。制御ロジックは安全入出力ユニット４０を制御するアルゴリズム等である。安全コントローラ２０は、安全入出力ユニット４０と直接的に通信せず、第１ポート２４を介してゲートウェイ装置１０と通信する。安全コントローラ２０とゲートウェイ装置１０との間の通信経路は、ネットワークＮ１で接続されている。ネットワークＮ１は通信方式１に対応するネットワークである。

[0019] ゲートウェイ装置１０は、安全コントローラ２０と安全入出力ユニット４０との間の通信経路上に介在し、第１通信ポート１１１と、第２通信ポート１１２と、第１通信制御部１１３と、制御データ中継部１１４と、第２通信制御部１１５とを有する。また、ゲートウェイ装置１０は、本実施の形態が特徴とする部分として、制御データ中継部１１４と接続された、安全制御部１２０と状態監視制御部１３０とを有する。ゲートウェイ装置１０は、安全入出力ユニット４０と安全コントローラ２０との間における安全データの通信を中継することにより安全入出力ユニット４０と安全コントローラ２０との安全コネクションを確立する。安全制御部１２０は安全状態発動解除制御部とも呼ばれる。状態監視制御部１３０はステートマシン監視制御部とも呼ばれる。

第１通信ポート１１１と第１通信制御部１１３との各々は、通信方式１に対応しており、第１ポート１３により実現される。

第２通信ポート１１２と第２通信制御部１１５との各々は、通信方式２に対応しており、第２ポート１４により実現される。

[0020] 図６は、安全制御部１２０と状態監視制御部１３０との各々の構成例を示している。

[0021] 安全制御部１２０は、安全状態管理部１２１と安全データ制御部１２２とを備える。安全制御部１２０は、制御状態が非安全状態から安全状態に遷移した場合に、安全入出力ユニット４０に送信する安全データであって、安全状態を示す安全データを生成する。安全制御部１２０は、制御状態が非安全状態から安全状態に遷移した場合に、安全コネクションを切断する制御を実行してもよい。安全制御部１２０は、安全コネクションが切断されている場合において、制御状態が安全状態から非安全状態に遷移した場合に安全コネクションの切断を解除してもよい。安全制御部１２０は、安全コネクションを切断する制御として、安全状態を示す安全データとなるよう、ゲートウェイ装置１０が安全コントローラ２０から受信した安全データを書き換える制御を実行してもよい。安全コントローラ２０が出力した安全データをゲートウェイ装置１０が直接的に安全入出力ユニット４０に中継しないことにより、安全コネクションが切断されている。

ここで、安全状態は、受容できないリスクから免れている状態であり、具体例として、制御システムが制御する工作機械が停止している状態、又は、当該工作機械が安全な速度で動作している状態等の作業者が保護されている状態である。一方、非安全状態は、直面するリスクが許容できない状態であり、具体例として、作業者に危害を加えるリスクが十分に低減されていない状態である。安全状態及び非安全状態の各々は、安全入出力ユニット４０の下位に接続された接続機器に対する入出力値として表現される。

[0022] 状態監視制御部１３０は、状態遷移検出部１３１と安全データ監視部１３２とを備える。状態監視制御部１３０は、制御状態を管理し、かつ、ゲート

ウェイ装置１０が安全入出力ユニット４０から受信した安全データを、状態遷移情報に適用することにより制御状態の状態遷移を制御する。状態遷移情報は、制御状態についての状態遷移を示す情報である。状態監視制御部１３０は、ゲートウェイ装置１０が安全コントローラ２０から受信した安全データを状態遷移情報に適用することにより制御状態の状態遷移を制御してもよい。状態監視制御部１３０は、安全コネクションが切断されている場合において、安全コネクションを切断する契機となった安全データよりも古い安全データに基づいて制御を実施した結果を示す安全データであって、ゲートウェイ装置１０が安全コントローラ２０から受信した安全データを用いずに制御状態の状態遷移を制御してもよい。状態監視制御部１３０は、安全コントローラ２０が用いる制御ロジックの少なくとも一部である部分制御ロジックを用いてもよい。状態遷移情報は、部分制御ロジックの少なくとも一部を示す情報であってもよい。状態遷移情報は、エンジニアリングツール３０を用いて設定された情報であってもよい。

[0023] ゲートウェイ装置１０が実施する処理は、主に下記の処理１から処理３である。

処理１：通信方式１と通信方式２とを相互に変換する処理。

処理２：安全コントローラ２０が安全入出力ユニット４０からの非定常信号の入力に応答して安全入出力ユニット４０に対して行った非安全状態を示す出力を、安全状態を示す出力になるよう上書きし、上書きした出力を安全入出力ユニット４０に出力する処理。

処理３：安全状態への遷移後、安全コントローラ２０からの安全状態の解除出力が安全入出力ユニット４０に反映されるように、処理２における出力よりも安全コントローラ２０からの出力を優先するよう切り替える処理。

[0024] 安全入出力ユニット４０は、安全入出力ユニット４０の下位に接続された接続機器からの入力値に対応する安全データを安全コントローラ２０に送信し、また、安全コントローラ２０から受信した安全データに対応するデータを下位に接続された制御装置に出力する。安全データは、安全Ｉ／Ｏデータ

、Ｉ／Ｏデータ、又は安全情報とも呼ばれる。安全入出力ユニット４０は、安全コントローラ２０と直接的に通信せず、第２ポート４４を介してゲートウェイ装置１０と通信する。ゲートウェイ装置１０と安全入出力ユニット４０との間は、ネットワークＮ２で接続されている。ネットワークＮ２は通信方式２に対応するネットワークである。

[0025] エンジニアリングツール３０は、プログラミング手段提供部３１と、ロジック生成部３４と、ロジック設定部３５とを有し、さらに、本実施の形態が特徴とする部分として、ゲートウェイロジック生成部３２と、ゲートウェイロジック設定部３３とを有する。エンジニアリングツール３０はゲートウェイ装置１０と通信することができる。ユーザは安全制御システム８０の利用者である。制御アプリケーションは、安全制御システム８０の機能を実現するアプリケーションであり、安全制御アプリケーションとも呼ばれる。アプリケーションは、特に断りがない限りアプリケーションプログラムを指す。制御アプリケーションは、制御ロジックに基づいて制御状態を求め、求めた制御状態を管理する。制御状態は、制御アプリケーションが示す状態であり、安全制御システム８０の状態として想定される状態である。制御状態は内部状態とも呼ばれる。制御状態は、安全制御システム８０の状態に対応する状態であって、安全状態と非安全状態とのいずれかの状態である。

プログラミング手段提供部３１は、ユーザが実現したい制御アプリケーションに応じて制御プログラム及びパラメータを作成するための手段をユーザに提供する。

ロジック生成部３４は、プログラミング手段提供部３１の処理結果に応じて、安全コントローラ２０に設定すべき制御ロジック及びパラメータを生成する。

ロジック設定部３５は、ロジック生成部３４が生成した制御ロジック及びパラメータを安全コントローラ２０に設定する。

ゲートウェイロジック生成部３２は、プログラミング手段提供部３１の処理結果に応じて、ゲートウェイ装置１０の説明で述べた動作を実現するため

の制御ロジック及びパラメータを生成する。

ゲートウェイロジック設定部３３は、ゲートウェイロジック生成部３２が生成した制御ロジック及びパラメータをゲートウェイ装置１０に設定する。

なお、安全コントローラ２０と安全入出力ユニット４０との各々は既存のものであってよい。即ち、ゲートウェイ装置１０は、動作が透過的になるよう、安全コントローラ２０に対して通信方式１を採用する安全入出力ユニット４０のように振る舞い、かつ、安全入出力ユニット４０に対して通信方式２を採用する安全コントローラ２０のように振る舞ってもよい。

また、通信方式１と通信方式２とは基本的に互いに異なるが、通信方式１と通信方式２とは同じ通信方式であってもよい。通信方式１と通信方式２とが同じ通信方式である場合において、通信方式を変換する効果は得られないが、ゲートウェイ装置１０が安全入出力ユニット４０に対してキャッシュサーバのように代理応答することによって、安全応答時間を短縮する効果は得られる。安全応答時間は、安全入出力ユニット４０が安全データを送信してから、安全入出力ユニット４０が出力した安全データに対応する安全データを安全入出力ユニット４０が受信するまでの最悪時間である。安全応答時間は、安全状態への遷移においてアクチュエータが反応する時間等、機器の動作に関する時間を含んでもよい。

[0026] 補足として、安全制御とその他の一般制御とを同じシステム内又はネットワーク内に混在させることは広く行われており、本実施の形態においても安全制御システム８０内にこれらの制御が混在してよい。一般制御は、具体例として、一般ＩＯ制御、又は駆動制御である。これらの制御が混在する場合において、一般制御に係る機器が混在して第２通信ポート１１２に接続されていてもよく、安全コントローラ２０に加えて一般ＩＯコントローラと駆動制御コントローラとの少なくとも一方が第１通信ポート１１１に接続されていてもよく、一般制御に係る制御ロジックが安全コントローラ２０の制御ロジックに統合されていてもよい。また、この場合において、ゲートウェイ装置１０が一般制御の通信データに対しレイヤ２とレイヤ３との少なくともい

ずれか等の中継処理のみを行うことが考えられる。

[0027] 図７は、通信方式１と通信方式２との各々に対応する通信パケットを説明する図である。通信パケットの構造は、一般的な安全通信における構造と同じである。

一般通信パケット９０は、一般通信ヘッダ９１と、一般通信ペイロード９２と、一般通信ＦＣＳ（Ｆｒａｍｅ　Ｃｈｅｃｋ　Ｓｅｑｕｅｎｃｅ）９３とから構成される。一般通信ペイロード９２の少なくとも一部として安全通信パケット９２０が格納される。

安全通信パケット９２０は、一般通信パケット９０に格納され、安全通信ヘッダ９２１と、安全通信ペイロード９２２と、安全通信ＦＣＳ９２４とから構成される。安全通信パケット９２０は安全パケットとも呼ばれる。

安全通信ヘッダ９２１は、安全通信パケット９２０の伝送中の宛先誤り又は適時性に関するエラー等の通信エラーを検出するための情報等を含む。適時性に関するエラーは、具体例として、喪失又は受容できない遅延である。

安全通信ペイロード９２２は、安全データの本体であり、安全入出力データ９２３等を含む。

安全通信ＦＣＳ９２４は、安全通信パケット９２０の完全性を確認するものであり、ＣＲＣ（Ｃｙｃｌｉｃ　Ｒｅｄｕｎｄａｎｃｙ　Ｃｈｅｃｋ）等により生成されたチェックサム等が格納される。

通信パケットの構造が通信方式１と通信方式２との各々に対して定義され、通信方式１と通信方式２との各々の構造が互いに異なってもよい。ここで、通信方式１に従う安全通信パケット９２０を安全通信パケットＰ１と呼ぶ。通信方式２に従う安全通信パケット９２０を安全通信パケットＰ２と呼ぶ。

また、通信パケットの内部は前述の構造と異なってもよく、具体例として、通信パケットの構造は下記に示す構造であってもよい。

構造１：安全通信パケット９２０が一般通信パケット９０に格納されずに伝送路を伝送される構造。

構造２：安全通信ヘッダ９２１と安全通信ＦＣＳ９２４とが一体となって安全通信パケット９２０に格納された構造。

構造３：安全通信ヘッダ９２１と、安全通信ペイロード９２２と、安全通信ＦＣＳ９２４との少なくとも１つが、安全通信パケット９２０内に複製されて格納された構造、又は、安全通信パケット９２０内に分割されて格納された構造。

[0028] ＊＊＊動作の説明＊＊＊

ゲートウェイ装置１０の動作手順はゲートウェイ制御方法に相当する。ゲートウェイ装置１０の動作を実現するプログラムはゲートウェイ制御プログラムに相当する。エンジニアリングツール３０の動作手順はエンジニアリング方法に相当する。エンジニアリングツール３０の動作を実現するプログラムはエンジニアリングプログラムに相当する。

[0029] 安全制御システム８０の動作は、設定フェーズと制御フェーズとから成る。

設定フェーズでは、ユーザがエンジニアリングツール３０を用いて必要な制御ロジックをプログラミングし、エンジニアリングツール３０は、その結果生成されたプログラム及びパラメータを、安全コントローラ２０及びゲートウェイ装置１０に設定する。

制御フェーズでは、設定されたプログラム及びパラメータに基づいて、安全コントローラ２０及びゲートウェイ装置１０が安全入出力ユニット４０と連携して安全制御を行う。

[0030] ＜制御フェーズ＞

図８は、安全制御システム８０に設定される１つの制御ロジックの一例を示している。以下では、この制御ロジックに従うゲートウェイロジックを設定する場合における安全制御システム８０の動作を説明する。なお、安全制御システム８０において互いに異なる複数の制御ロジックが並列に設定されていてもよい。安全制御システム８０は、以下で説明する１つの制御ロジックに対する具体例を複数の制御ロジックの各々に適用することにより、複数

の制御ロジックが並列に設定されている場合に対応することができる。また、安全制御システム８０において複数の安全制御プログラムが連動する場合については、状態遷移の条件に他の安全制御プログラムによる出力が加わるのみであるため、安全制御システム８０は以下で説明する方法により当該場合に対応することができる。

図８に示す制御ロジックは、状態０から状態６までの７つの状態を持ち、１１の状態遷移を持つ。これらのうち、非安全状態は状態４及び状態５のみであり、それ以外の状態は安全状態である。非安全状態は、具体例として、接続機器の動作が許可されることを示す状態である。安全状態は、具体例として、接続機器を停止させることを示す状態である。安全状態において安全制御システム８０は安全制御を実施する。

安全制御システム８０が図８に示す制御を行うためには、安全制御システム８０は、下記の認識事項１及び認識事項２を認識することができなければならない。ここで、管理対象非安全状態は、非安全状態のうち、安全状態と見分けるために管理される状態である。管理対象非安全状態は後述の管理対象安全状態と同様である。

認識事項１：制御状態が管理対象非安全状態である状態４又は状態５であること。

認識事項２：非安全状態から安全状態への遷移条件である条件６－Ａ又は条件６－Ｂが満たされたこと。

認識事項２のみを考慮するよう安全制御システム８０を構成することも考えられるが、条件６－Ａ及び条件６－Ｂの少なくとも一方と他の遷移条件とに重複があると、既に安全状態であるにも関わらず不要な出力が行われる可能性がある。不要な出力が行われた場合、安全状態を示す出力がなされるため制御が意図せず安全状態を逸脱するリスクはないものの、不要な出力により制御アプリケーションの動作が不安定になり、その結果エラーが発生するリスクがある。このため、安全制御システム８０を運用するに当たり、安全制御システム８０において認識事項１と認識事項２との双方を認識すること

ができるか否かを確認する必要がある。

[0031] 図９は、安全制御システム８０の基本動作についての全体の流れの一例を示すフローチャートである。本図を参照して安全制御システム８０の基本動作を説明する。

ここで、制御アプリケーションの一連の処理を説明する。まず、安全入出力ユニット４０は、接続機器から得たデータを示す安全データを安全コントローラ２０に向けて出力する。次に、安全コントローラ２０は、ゲートウェイ装置１０を介して入力された安全データを用いて安全入出力ユニット４０の制御を決定し、決定した結果を示す安全データを安全入出力ユニット４０に向けて出力する。次に、安全入出力ユニット４０は、ゲートウェイ装置１０を介して入力された安全データに応じたデータを制御装置に向けて出力する。この一連の処理が繰り返されることにより、制御アプリケーションが実現される。

前段の説明として、入力から出力までの基本的な動作について、既存技術と本実施の形態との特徴的な差異に当たる部分を除いて説明する。なお、下記では安全入出力ユニット４０が接続機器からデータを取得してから制御装置にデータを出力まで１回の流れに着目して安全制御システム８０の動作を説明している。しかしながら、安全制御システム８０において、安全入出力ユニット４０と、ゲートウェイ装置１０と、安全コントローラ２０とが非同期的に動作し、その結果として安全入出力ユニット４０が取得したデータがバケツリレー式に処理されるという動作が実現されてもよい。また、安全入出力ユニット４０と、ゲートウェイ装置１０と、安全コントローラ２０との各々についても、安全通信パケットＰ２の生成若しくは検査、又は制御ロジックの実行等の各内部処理が、独立したタイミングで動作していてもよい。

[0032] （ステップＳ０１）

安全入出力ユニット４０は、安全入出力ユニット４０の配下に接続された接続機器から信号又は電位等を読み出すことにより、入力値を取得する。入力値は、ビット値又はアナログ値を模した多値であってもよい。入力値を取

得するタイミングは、どのようなタイミングであってもよく、具体例として、あらかじめ決めた周期に従うタイミング、又は、安全コントローラ２０若しくはゲートウェイ装置１０からの要求に応じたタイミングである。

[0033]（ステップＳ０２）

安全入出力ユニット４０は、入力値を示すデータを安全データとして安全通信パケットＰ２に格納し、当該安全通信パケットＰ２を、ネットワークＮ２を介してゲートウェイ装置１０に送出する。安全入出力ユニット４０が安全通信パケットＰ２を送出するタイミングは、ステップＳ０１におけるタイミングと同じタイミングであることが一般的であるが、ステップＳ０１におけるタイミングと異なるタイミングであってもよい。

本ステップを含め、以後の全てのステップにおいて、安全通信パケット９２０の生成、送出、又は検査に関わる処理は、安全層において実現される。安全層は、ＩＥＣ（Ｉｎｔｅｒｎａｔｉｏｎａｌ　Ｅｌｅｃｔｒｏｔｅｃｈｎｉｃａｌ　Ｃｏｍｍｉｓｓｉｏｎ）　６１５０８等の機能安全規格に基づいて実現されたソフトウェアである。

[0034]（ステップＳ０３）

ゲートウェイ装置１０は、安全通信パケットＰ２を受信し、受信した安全通信パケットＰ２を検査する。ゲートウェイ装置１０は、安全通信パケットＰ２に含まれている安全データを取り出して使用する前に、安全通信パケットＰ２に対する通信エラーが生じているか否かを検査により確認する。

図１０は、本ステップの詳細なフローの一例を示すフローチャートである。本図を参照して当該フローを説明する。

[0035]（ステップＳ０３－１）

ゲートウェイ装置１０は、第２通信ポート１１２を用いてネットワークＮ２から安全通信パケットＰ２を受信する。

[0036]（ステップＳ０３－２）

ゲートウェイ装置１０は、受信した安全通信パケットＰ２に通信エラーがあるか否かを、安全通信パケットＰ２が含む安全通信ヘッダ９２１と安全通

信ＦＣＳ９２４との各々の内容を確認することにより検査する。ゲートウェイ装置１０は、具体例として、安全通信ヘッダ９２１の個々のフィールドの値が正しい安全通信パケットＰ２として期待される範囲の値であること、又は、安全通信ＦＣＳ９２４を含む安全通信パケットＰ２全体のチェックサムを規定の初期値及び多項式を用いたＣＲＣ演算により計算し、計算した結果が正常を示す値であること等の確認方法を組み合わせることにより安全通信パケットＰ２を検査する。また、安全通信パケットＰ２を検査する方式は安全通信方式ごとに異なってもよい。

[0037] （ステップＳ０３－３）

受信した安全通信パケットＰ２に通信エラーがない場合、ゲートウェイ装置１０はステップＳ０３－４に進む。それ以外の場合、ゲートウェイ装置１０はステップＳ０３－５に進む。

[0038] （ステップＳ０３－４）

ゲートウェイ装置１０は、受信した安全通信パケットＰ２に含まれている安全データに異常がないものとして安全データを扱う。具体的には、ゲートウェイ装置１０は、次のステップにおいて、当該安全データを信頼し、安全データを制御ロジックへ入力する際と、制御ロジックによる出力を安全入出力ユニット４０へ出力する際とにエラー出力等を行わない。

[0039] （ステップＳ０３－５）

ゲートウェイ装置１０は、受信した安全通信パケットＰ２に含まれている安全データに異常があるものとして安全データを扱う。具体的には、ゲートウェイ装置１０は、当該安全データを、制御ロジックへ入力することと、制御ロジックによる出力を安全入出力ユニット４０へ出力することに用いない。本ステップの処理を実現するために、一般的には当該安全データを廃棄し以後のステップに渡さないこと、通信パケットに通信エラーを表すフラグを設定し当該安全データが制御に用いられないようにすること、あるいは通信エラーを契機として直後のネットワークにおいてコネクションを強制的に切断すること等の方法が取られる。

[0040] なお、安全通信パケットＰ２の受信と検査との各々は、ステップＳ０２における安全通信パケットＰ２の送出と同じ頻度で行われることが一般的であるが、当該頻度と異なる頻度で行われてもよい。

以後の安全通信パケット９２０の受信と検査とに関わるフローについても、動作の主体と扱う安全通信パケット９２０の通信方式との各々に差異があることがあるものの、ステップＳ０３－１からステップＳ０３－５のフローと同様である。ここで、以後の安全通信パケット９２０の受信と検査とに関わるフローを、以下で説明する。

[0041]（ステップＳ０５）

安全コントローラ２０は、ゲートウェイ装置１０から受信した安全通信パケットＰ１に対し、ステップＳ０３－１からステップＳ０３－５のフローと同様のことを行う。

[0042]（ステップＳ０８）

ゲートウェイ装置１０は、安全コントローラ２０から受信した安全通信パケットＰ１に対し、ステップＳ０３－１からステップＳ０３－５のフローと同様のことを行う。

[0043]（ステップＳ１０）

安全入出力ユニット４０は、ゲートウェイ装置１０から受信した安全通信パケットＰ２に対し、ステップＳ０３－１からステップＳ０３－５のフローと同様のことを行う。

[0044]（ステップＳ０４）

ゲートウェイ装置１０は、安全データを安全通信パケットＰ１に格納し、ネットワークＮ１に当該安全通信パケットＰ１を送出する。ここで、格納される安全データは、ステップＳ０３を実行した結果得られた安全データである。

なお、ステップＳ０３において通信エラーが検出された場合、ゲートウェイ装置１０は、具体例として、送出する安全通信パケットＰ１に非定常状態を表す安全データを格納すること、安全通信パケットＰ１に通信エラーを表

すフラグを設定すること、あるいは安全コネクションを切断すること等を実行することにより、安全コントローラ２０に通信エラーの発生を伝達することができるようにする。

[0045]（ステップＳ０５）

安全コントローラ２０は、ネットワークＮ１を介してゲートウェイ装置１０から安全通信パケットＰ１を受信し、受信した安全通信パケットＰ１を検査する。この際、安全コントローラ２０は、ステップＳ０３におけるゲートウェイ装置１０の処理と同様の処理を実行する。

安全コントローラ２０が通信エラーを検出した場合、安全コントローラ２０は、受信した安全通信パケットＰ１に含まれている安全データを正常な安全データとして制御ロジックに使わないこととする。

[0046]（ステップＳ０６）

安全コントローラ２０は、受信した安全通信パケットＰ１に含まれている安全データを入力として制御ロジックを実行する。当該制御ロジックは、安全入出力ユニット４０が生成した安全データを入力として安全入出力ユニット４０を制御するためのプログラムを実行し、プログラムを実行した結果を安全入出力ユニット４０に向けて安全データとして出力するよう構成されている。なお、当該制御ロジックは、入力された安全データが非定常状態を表すこと、安全通信パケットＰ１に通信エラーを表すフラグが設定されていること、又は、安全コネクションの切断が発生したこと等を検出したことによって通信エラーを検出した場合等に、安全制御システム８０の状態が安全状態となるよう安全制御システム８０を制御する処理を含む。

[0047]（ステップＳ０７）

安全コントローラ２０は、制御ロジックを実行した結果を示す安全データを安全通信パケットＰ１に格納し、当該安全通信パケットＰ１をネットワークＮ１に送出する。

[0048]（ステップＳ０８）

ゲートウェイ装置１０は、安全コントローラ２０から安全通信パケットＰ

１を受信し、受信した安全通信パケットＰ１を検査する。この際、ゲートウェイ装置１０は、ステップＳ０３におけるゲートウェイ装置１０の処理と同様の処理を実行する。ゲートウェイ装置１０が通信エラーを検出した場合、ゲートウェイ装置１０は、安全通信パケットＰ１に含まれている安全データを正常な安全データとして制御ロジックに使わないこととする。

[0049]（ステップＳ０９）

ゲートウェイ装置１０は、安全通信パケットＰ１に含まれている安全データを安全通信パケットＰ２に格納し、当該安全通信パケットＰ２をネットワークＮ２に送出する。

[0050]（ステップＳ１０）

安全入出力ユニット４０は、安全通信パケットＰ２を受信し、受信した安全通信パケットＰ２を検査する。この際、安全入出力ユニット４０は、ステップＳ０３におけるゲートウェイ装置１０の処理と同様の処理を実行する。

[0051]（ステップＳ１１）

安全入出力ユニット４０は、ステップＳ１０で受信した安全通信パケットＰ２に含まれている安全データに対応する出力値の出力を、安全入出力ユニット４０の配下に接続された制御装置に対して実行する。安全入出力ユニット４０は、安全入出力ユニット４０が備える接続端子を介して出力を実行してもよい。出力の方法は、一般的な安全入出力ユニットが採用する出力の方法と同様であってもよい。安全入出力ユニット４０は、具体例として、ＰＮＰトランジスタ出力等により出力を実行する。

なお、ステップＳ１０で安全入出力ユニット４０が通信エラーを検出した場合において、具体例として、安全入出力ユニット４０は、当該通信エラーに関するパラメータ等があらかじめ設定された許容範囲内ではない場合、出力をあらかじめ定めた値であって安全状態に対応する値とし、制御状態を安全状態に遷移させる。許容範囲は、具体例として、回数と時間との少なくともいずれかについての範囲である。なお、あらかじめ設定されたウォッチドッグ時間内に、安全入出力ユニットが規定の数以上の正常な安全通信パケッ

トを受信したか否かによって通信エラーに関するパラメータ等が許容範囲内であるか否かを判断する手法が採用されることが一般的には多い。しかしながら、安全入出力ユニット４０は他の手法により通信エラーの発生が許容範囲内であるか否かを判断してもよい。

[0052] 以上が、本実施の形態の特徴を除いた、ゲートウェイ装置１０を含む安全制御システム８０の入力から出力までの基本的な動作である。以下では、前述の基本的な動作と、本実施の形態に係る特徴的な動作との差分を説明する。

本実施の形態では、ステップＳ０４を変更してステップＳ０４’とし、ステップＳ０４’においてゲートウェイ装置１０が安全入出力ユニット４０から受信した安全データに対応する制御を行うことにより、高い応答性能を実現することができるようにする。

[0053] 図１１は、安全制御システム８０の動作についての全体の流れの一例を示すフローチャートである。本図を参照して、安全制御システム８０の特徴的な動作を説明する。

[0054]（ステップＳ０４’）

図１２は、ステップＳ０４’の詳細なフローの一例を示すフローチャートである。本図を参照して当該フローを説明する。

[0055]（ステップＳ０４’－１）

安全データ監視部１３２は、制御データ中継部１１４が中継する安全データを、監視安全データとして監視する。ステップＳ０４’における監視安全データは、ゲートウェイ装置１０が安全入出力ユニット４０から安全コントローラ２０に向けて中継する安全データである。監視安全データは、制御データ中継部１１４が管理するメモリ領域の一部に格納されており、状態監視制御部１３０は、監視安全データへアクセスする方法を示す情報がなければ当該方法が分からない。そこで、監視安全データの識別情報と、監視安全データにアクセスするためのメモリアドレス等の情報を対応づけて示す安全データマッピング表１９４が用意される。メモリアドレスをアドレスと表記す

ることもある。

図１３は、安全データマッピング表１９４の具体例を表形式で示している。シンボルは、データを識別する情報であり、データの名称等である。安全データマッピング表１９４が本例に示すものである場合、安全データ監視部１３２は、具体例として、Ｓ＿Ｅｓｔｏｐ１という安全データを監視安全データとして監視する必要がある場合、安全データマッピング表１９４を参照して当該監視安全データがメモリアドレス０ｘ１００１Ｃ番地のビット０に示されているという情報を得て、当該メモリアドレスにアクセスすることによりＳ＿Ｅｓｔｏｐ１の値を得る。

[0056]（ステップＳ０４’－２）

状態遷移検出部１３１は、監視安全データに基づき、制御状態が、状態遷移表１９２が示すいずれの状態であるかを検出する。状態遷移検出部１３１は状態比較検出部とも呼ばれる。少なくとも制御状態が非安全状態であるか否かを制御アプリケーションが把握することができるよう、かつ、制御アプリケーションが互いに異なる複数の非安全状態のいずれかを制御状態として示し得る場合に、制御状態が複数の非安全状態のいずれの状態であるかを制御アプリケーションが識別することができるよう、状態遷移表１９２は構成される。また、管理対象安全状態であるか否かを制御アプリケーションが把握することができるよう、かつ、制御アプリケーションが互いに異なる複数の管理対象安全状態を示し得る場合、互いに異なる複数の管理対象安全状態のいずれの状態であるかを制御アプリケーションが識別することができるよう、状態検出表１０２は構成される。ここで、管理対象安全状態は、安全状態のうち、非安全状態と見分けるために管理される状態である。ここで、非安全状態と管理対象安全状態とを総称して管理対象状態と呼ぶ。

ここで、図８を用いて管理対象安全状態の具体例を説明する。まず、状態遷移検出部１３１が制御データ中継部１１４のデータを静的に確認するのみでは状態２と状態４とを区別することができないものとする。このとき、現状態が状態４であれば条件６－Ａが満たされたことをもって状態６に遷移す

るが、現状態が状態２であれば条件６－Ａが満たされても状態遷移は起こらない。そのため、状態遷移検出部１３１は、状態２と状態４とを区別する必要があり、状態２と状態４とを区別するために、状態２を管理対象安全状態として監視しなければならない。また、状態２を監視するために、状態１と状態２とを区別することができないものとすると、状態遷移検出部１３１は状態１も管理対象安全状態として監視する必要がある。一方、状態３は非安全状態に遷移しうる状態であるが、状態遷移検出部１３１は、状態４及び状態３と、状態５及び状態３との各々を制御データ中継部１１４のデータを静的に確認するのみで区別することができるものとすると、状態３を監視する必要がない。従って、このとき状態３は管理対象安全状態に含まれない。

状態遷移表１９２は、少なくとも、ある時刻における制御状態を示す現状態と、現状態における出力値と、現状態においてとり得る次状態と、現状態から次状態への遷移条件との各々を示す。次状態は現状態の次の状態である。出力値は、安全コントローラ２０が安全入出力ユニット４０に向けて出力する安全データの値であり、具体例として、０若しくは１を取るバイナリ値、又は、連続値を離散値で表現したアナログ値ある。遷移条件は、次状態への遷移を起こすために安全データが取るべき条件であり、具体例として、出力値が特定の値であることと、出力値の立ち上がり又は立ち下がりが特定の値であることと、出力値が閾値を上回っていること又は下回っていることと、今回の出力値と前回の出力値との差が閾値を超えていること等、出力値の変化が特定の基準を満たすこととの少なくとも１つを組み合わせた条件である。また、遷移条件は、１つの安全データに対する条件に限らず、複数の安全データの各々に対する条件を組み合わせた条件であってもよく、複数の条件の論理和又は論理積等により表現されてもよい。状態遷移表１９２は、状態遷移情報に当たり、部分制御ロジックの少なくとも一部を示す情報に当たる。

状態遷移検出部１３１は、状態記憶部１９３に制御状態の現状態を記録する。状態記憶部１９３は、少なくとも、現状態が管理対象状態のいずれかに

あたるか否かを区別して記憶することができる。状態記憶部１９３は、制御状態の現状態を表す情報に加えて、現状態が直前の制御状態から変化したか否かを表す状態変化ビットを有していてもよい。

[0057]（ステップＳ０４’－３）

状態遷移検出部１３１は、状態遷移表１９２を参照して現状態に対応する遷移条件のいずれかが満たされているか否かを、監視安全データに基づいて、少なくとも、監視安全データに変化が発生する全てのタイミングにおいて、繰り返し判定する。

遷移条件のいずれかが満たされている場合、ゲートウェイ装置１０はステップＳ０４’－４に進む。それ以外の場合、ゲートウェイ装置１０はステップＳ０４’－８に進む。

[0058]（ステップＳ０４’－４）

状態遷移検出部１３１は、状態記憶部１９３が示す現状態を、満たされた遷移条件に対応する次状態が示す状態に書き換える。

安全制御部１２０は、状態遷移検出部１３１の動作によって状態記憶部１９３が記憶している制御状態が変化した場合、安全入出力ユニット４０の状態を安全状態に遷移させる制御、又は、安全入出力ユニット４０の状態を安全状態から非安全状態に解除する制御を適切に行うために、安全データの値と安全データの出力経路とを変更する制御を行う。安全制御部１２０は、具体的には下記の処理を実行する。

[0059]（ステップＳ０４’－５）

安全状態管理部１２１は、状態記憶部１９３を参照し、制御状態が前回確認したときの状態から変化しているか否かを確認する。安全状態管理部１２１は安全状態発動管理部とも呼ばれる。安全状態管理部１２１は、制御状態の変化を確認するために状態記憶部１９３の状態変化ビットを利用してもよい。安全状態管理部１２１は、制御状態が変化している場合、状態記憶部１９３から変化後の制御状態を読み出し、読み出した制御状態に対応する状態遷移表１９２のエントリを参照する。

制御状態が非安全状態から安全状態に遷移していた場合、ゲートウェイ装置１０はステップＳ０４’－６に進む。それ以外の場合、ゲートウェイ装置１０はステップＳ０５に進む。

[0060]（ステップＳ０４’－６）

安全制御システム８０において比較的高速に安全制御を実施することができるよう、ゲートウェイ装置１０は、対象安全データを非定常な値に書き換え、値を書き換えた対象安全データを安全入出力ユニット４０に出力する。対象安全データは、制御データ中継部１１４が管理する安全データであり、ゲートウェイ装置１０によって書き換えられた上で安全入出力ユニット４０に出力される安全データである。対象安全データは、安全コントローラ２０が出力した安全データであってもよく、安全コントローラ２０から安全データを受信していない場合においてデフォルト値を示すデータであってもよい。当該デフォルト値は、非定常状態を示し、安全入出力ユニット４０に入力されても安全入出力ユニット４０に問題が生じない値である。安全入出力ユニット４０は、受信した対象安全データを、安全コントローラ２０が出力した安全データと同等に扱うことができる。ここで、書き換えられた対象安全データを単に対象安全データと表記することもある。具体例として、ゲートウェイ装置１０は、安全コントローラ２０から安全入出力ユニット４０に向けて対象安全データを中継しているように見せかけて、安全入出力ユニット４０に対象安全データを出力する。

安全状態管理部１２１は、非安全状態から安全状態へ制御状態が変化した場合に、どのように対象安全データを変更すればよいか、出力定義情報１９１を参照して判断する。出力定義情報１９１は安全状態出力定義情報とも呼ばれる。出力定義情報１９１は、少なくとも前状態と現状態と出力定義との３つを組にした情報であり、前状態から現状態に制御状態が変化したときに出力すべき値を表す情報である。前状態は現状態の１つ前の状態である。ゲートウェイ装置１０が出力定義に従って安全データを生成すると生成した安全データが安全状態を示すよう、出力定義は定義される。図１４は、出力定

義情報１９１の具体例を示している。「制御アプリケーション」欄には、制御アプリケーションの名称が入力されている。

安全状態管理部１２１は、対象安全データを出力定義に従う安全データに変更するよう、安全データ制御部１２２に対して指示する。

なお、安全制御部１２０は、ステップＳ０９’における解除が実行されるまで、本ステップ及びステップＳ０４’－７の処理を継続して実行する。

[0061]（ステップＳ０４’－７）

安全データ制御部１２２は、安全データ監視部１３２が実行した処理と同様に、安全データマッピング表１９４を参照して、対象安全データのアドレスを特定する。

その後、安全データ制御部１２２は、特定したアドレスに対応する対象安全データを出力定義に従い書き換える。ゲートウェイ装置１０は、書き換えられた対象安全データを安全入出力ユニット４０に出力される。その結果、安全制御システム８０において必要な安全制御が比較的高速に行われる。

なお、制御データ中継部１１４による対象安全データの書き換えについては、対象安全データが安全状態を示すよう書き換える契機となった監視安全データ、又は、当該監視安全データよりも新しい安全データに基づく安全コントローラ２０の出力によって制御状態が安全状態から非安全状態に遷移するまで、対象安全データが非安全状態を示すよう書き換えられることがないように管理する必要がある。具体例として、安全データ制御部１２２がある監視安全データに基づいて安全状態を表す安全データとなるよう対象安全データを上書きした後で、安全コントローラ２０が当該ある監視安全データよりも古い安全データに基づいた制御結果として非安全状態を示す安全データを出力した場合を考える。この場合において、ゲートウェイ装置１０は、安全コントローラ２０から受信した安全データではなく対象安全データを優先的に安全入出力ユニット４０に出力しなければならない。このための手段の具体例として、対象安全データに安全データ制御部１２２による上書きが行われていることにより対象安全データがロックされていることを示すフラグ

を設け、フラグの値が特定の値である場合に安全コントローラ２０が出力する安全データにより対象安全データを更新しないように制御する手段が挙げられる。別の手段として、安全コントローラ２０による出力が対象安全データに反映されないように対象安全データを別のバッファ領域に待避させる等、対象安全データを保護する手段が挙げられる。

本ステップの処理によって、ゲートウェイ装置１０が安全入出力ユニット４０に出力する対象安全データに安全入出力ユニット４０から受信した安全データに対する制御結果が反映される。また、ゲートウェイ装置１０は、制御結果が反映された対象安全データを安全通信パケットＰ２に含めて安全入出力ユニット４０に送出する。このため、本ステップの処理の終了後、ステップＳ０９から処理が継続される。

[0062]（ステップＳ０４’－８）

状態遷移検出部１３１は、状態記憶部１９３が示す現状態を書き換えない。

また、安全制御部１２０は何も実施せず、ゲートウェイ装置１０はステップＳ０５に遷移する。

[0063] 一方、制御状態が安全状態から非安全状態に遷移した場合、前述の手段と類似の手段によって、安全コントローラ２０から受信した安全データを優先的に安全入出力ユニット４０に出力するよう切り替える制御が必要である。

そのため、安全状態管理部１２１は、制御状態が変化した場合に、安全データをどのように変更すればよいか、出力定義情報１９１を参照して判断する。出力定義情報１９１の構造は前述の通りであるが、出力定義に格納する内容が異なる。

そこで、本実施の形態ではステップＳ０９を変更してステップＳ０９’とし、ステップＳ０９’において安全コントローラ２０の出力に基づいて安全状態の解除を検出し、ステップＳ０４’で行った安全状態へ遷移するための処理を解除する。

図１５は、安全制御システム８０の動作についての全体の流れの一例を示

すフローチャートである。本図を参照して、安全制御システム８０の特徴的な動作を説明する。

[0064]（ステップＳ０９’）

図１６は、ステップＳ０９’の詳細なフローの一例を示すフローチャートである。本図を参照して当該フローを説明する。

[0065]（ステップＳ０９’－１）

本ステップはステップＳ０４’－１と同様である。ただし、本ステップにおける監視安全データは、ゲートウェイ装置１０が安全コントローラ２０から安全入出力ユニット４０に向けて中継する安全データである。

[0066] ステップＳ０９’－２は、ステップＳ０４’－２と同様である。

ステップＳ０９’－３は、ステップＳ０４’－３と同様である。

ステップＳ０９’－４は、ステップＳ０４’－４と同様である。

ステップＳ０９’－５は、ステップＳ０４’－５と同様である。なお、制御状態が安全状態のまま変化していない場合、安全状態管理部１２１は何も行なわず、ステップＳ１０に遷移する。

[0067]（ステップＳ０９’－６）

安全状態管理部１２１は、対象安全データの書き換え解除を、安全データ制御部１２２に要求する。即ち、本ステップでは、ステップＳ０４’－６で安全状態管理部１２１が安全データ制御部１２２に対して行った対象安全データの書き換えの逆に当たる処理を行うことにより、対象安全データの代わりに安全コントローラ２０が出力した安全データが、安全入出力ユニット４０に出力されるようにする。

安全状態管理部１２１は、制御状態が安全状態から非安全状態へ変化した場合に、対象安全データをどのように変更すればよいかを、出力定義情報１９１を参照して判断する。出力定義情報１９１は、出力定義として、制御状態が安全状態から非安全状態に遷移していた場合において、操作すべき安全データと安全データを操作する方法を示す情報とを含む。この方法には、具体例として、ステップＳ０４’－６で安全状態管理部１２１が行った対象安

全データの書き換えを終了させる操作が含まれる。

安全状態管理部１２１は、出力定義に応じた出力を対象安全データに反映させるため、安全データ制御部１２２に対して指示する。

ただし、安全制御部１２０は、本ステップで対象安全データの書き換え解除を行う前に、制御状態に非安全状態から安全状態への遷移が起きていないことを追加的に確認し、当該遷移が発生していない場合にのみ、安全データの書き換え解除を行うことが考えられる。なぜならば、安全入出力ユニット４０が安全データを出力してから安全コントローラ２０が当該安全データに基づく制御ロジックの実行結果を出力するまでの時間には通信パスが長いこと等による遅延がある。そのため、安全コントローラ２０が非安全状態への遷移を示す安全データを出力した時点において、安全入出力ユニット４０が出力したより新しい安全データが、安全状態への遷移を起こすべき内容に変わっている場合があり得るためである。ここで、当該場合に安全制御部１２０が対象安全データの書き換え解除を行うと、非安全状態への遷移が優先されて安全状態への遷移が行われず、安全応答時間が延びるリスクがある。

[0068] （ステップＳ０９’－７）

安全データ制御部１２２は、制御データ中継部１１４による安全データ書き換え操作を変更する。安全データ制御部１２２は、ステップＳ０４’－７で安全データ監視部１３２が実行した方法と同様に、安全データマッピング表１９４を参照して、対象の安全データのアドレスを特定する。

安全データ制御部１２２は、さらに、特定した対象安全データのアドレスを用いて対象安全データを操作する。この操作は、出力定義の内容によるが、ステップＳ０４’－７で実施した対象安全データの書き換えを終了し、安全コントローラ２０が出力する安全データが優先的に出力されるようにする操作である。この操作を実現する方法はどのような方法であってもよい。当該方法は、具体例として、ステップＳ０４’－７で対象安全データがロックされていることを示すフラグを設けることにより安全データ制御部１２２による安全データの上書きを実現していた場合、当該フラグの値を元の値に復

元する方法である。あるいは、ステップＳ０４’－７で安全コントローラ２０による出力が対象安全データに反映されないように対象安全データを別のバッファ領域に退避させる手段を実行していた場合、バッファ領域の状態を元の状態に復元する方法が考えられる。

[0069]（ステップＳ０９’－８）

安全制御部１２０は、状態遷移検出部１３１の動作によって状態記憶部１９３が記憶している制御状態が変化していない場合、何も実施せず、ステップＳ１０に遷移する。

[0070] 安全制御システム８０の動作は前述の通りである。本実施の形態の特徴であるステップＳ０４’とステップＳ０９’とがあることにより、安全データの入力から応答までの流れは下記の通りとなる。

[0071] ケース１：ゲートウェイ装置１０に入力された安全データの値が、定常状態又は非定常状態を引き続き示しているケース

入力値の取得から出力までの流れは基本動作と変わらない。従って、本実施の形態に係る安全応答時間は基本動作に係る安全応答時間と変わらない。ここで、定常状態は安全データの値が安全状態を示す値であることであり、非定常状態は安全データの値が非安全状態を示す値であることである。

[0072] ケース２：ゲートウェイ装置１０に入力された安全データの値が、定常状態から非定常状態に変化したケース

安全制御システム８０は、変更されたステップＳ０４’により、ステップＳ０５からステップＳ０８までのステップをスキップし、安全状態への遷移を引き起こすための安全データの安全入出力ユニット４０への出力をステップＳ０９から開始する。従って、本実施の形態に係る安全応答時間は、基本動作に係る安全応答時間と比較して改善される。

[0073] ケース３：ゲートウェイ装置１０に入力された安全データの値が、非定常状態から定常状態に変化したケース

変更されたステップＳ０９’により安全状態の解除が行われる。しかしながら、ステップの長さは基本動作におけるステップの長さと変わらないため

、本実施の形態に係る安全応答時間は基本動作に係る安全応答時間と変わらない。

[0074] 前述の３つのケースのうち、安全の確保のために重要であり、かつ、機能安全規格において性能の保証が求められる安全応答時間は、ケース２における最悪時間である。一方、ケース１及びケース３の安全応答時間については、生産性の向上につながることはあり得るものの、安全の確保にはつながらない。本実施の形態では、安全を確保するための安全応答時間を、ゲートウェイ装置１０による比較的簡易な処理によって短縮することができる。

[0075] 以下では、制御フェーズを実現するためのエンジニアリングツール３０による設定について説明する。

本実施の形態では、出力定義情報１９１と、状態遷移表１９２と、状態記憶部１９３と、安全データマッピング表１９４とをゲートウェイ装置１０に設定する必要がある。これらの具体的なデータは、実現すべき制御アプリケーションによって異なる。ユーザの手作業によってこれらを設定することも考えられるが、設定作業の工数削減のためエンジニアリングツールによってこれらをゲートウェイ装置１０に設定することが現実的である。

[0076] エンジニアリングツール３０を用いた設定作業であって、ユーザによるプログラミングに連動した設定作業の具体例を述べる。ここで、エンジニアリングツール３０の構成要素のうち、一般的なエンジニアリングツールに対する本実施の形態の特徴的な部分は、ゲートウェイロジック生成部３２と、ゲートウェイロジック設定部３３とである。

[0077] プログラミング手段提供部３１は、ユーザに対して、安全コントローラ２０が実行すべきプログラムを作成する手段と、必要なパラメータを設定する手段とを提供する。

具体例として、プログラミング手段提供部３１はあらかじめ汎用的に利用されるプログラムの構成要素をファンクションブロックとして提供し、ユーザは、提供されたファンクションブロックと、論理和（ＯＲ）と、積（ＡＮＤ）と、否定（ＮＯＴ）と、排他的論理和（ＸＯＲ）等の基本演算と、その

他独自に作成したファンクションブロック等とを組み合わせることによって、必要な制御ロジックを構成するプログラムを作成してよい。また、プログラムは、手続き型プログラミング又はラダーロジックによるもの等、ファクトリーオートメーションの分野で利用されるプログラミングの方式及び言語に従うプログラムであってもよい。また、プログラミング手段提供部３１は、安全プログラムを扱う構成要素であるため、典型的には機能安全のＩＥＣ６１５０８シリーズ等の安全規格に従って実現される必要がある。

[0078] ロジック生成部３４は、プログラミング手段提供部３１の結果に従って、安全コントローラ２０に割り付けるべきロジック及びパラメータを生成する。ロジックは、プログラミングされた制御ロジックを実行するためのファイルである。ロジック及びパラメータは、安全制御システム８０の誤動作につながるデータ破損を防ぐため、ＣＲＣ等を用いて保護される。

[0079] ロジック設定部３５は、ロジック生成部３４が生成したロジック及びパラメータを、安全コントローラ２０に送信する。安全コントローラ２０は、受信したロジック及びパラメータを書き込む。送信の手段として、ＵＳＢ、ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）等による手段が挙げられるが、ロジック設定部３５がロジック及びパラメータを安全コントローラ２０に送信し、安全コントローラ２０が受信したロジック及びパラメータを書き込む目的を達成することができれば、どのような手段であってもよい。

[0080] ゲートウェイロジック生成部３２は、プログラミング手段提供部３１によってエンジニアリングツール３０に入力されたプログラム及びパラメータに基づき、下記のことを行う。ここでは、プログラムが汎用のファンクションブロックを組み合わせて実現されていることを想定して説明する。

[0081] ＜状態遷移表１９２の生成＞

ゲートウェイロジック生成部３２は、プログラミング手段提供部３１において設定されたプログラムに基づいて状態遷移表１９２を作成する。図１７は、図１９に示す全体状態遷移表に対応する状態遷移表１９２の具体例を示している。ここで、「Ｓ＿Ｅｓｔｏｐ」１から「デバイスＣ」の各欄は安全

データの各項目を示している。状態遷移表１９２は、一般的なソフトウェア設計又はシステム設計等において用いられるプログラムの状態遷移表に相当する情報から、少なくとも下記の条件１及び条件２を状態遷移検出部１３１が判定することができるように情報を抜粋して構成したものである。

条件１：制御状態が管理対象非安全状態であること、及び、安全状態への遷移条件が満たされたこと

条件２：制御状態が安全状態から非安全状態に遷移したこと

[0082] 図１８は、状態遷移表１９２のうち条件１の判定を行うための部分を得るための処理の一例を示すフローチャートである。本図を参照して当該処理を説明する。

[0083]（ステップＳ１０１）

ゲートウェイロジック生成部３２は、制御ロジックの全体状態遷移表を得る。全体状態遷移表は、状態遷移表１９２にとって不要な情報を削減していない状態遷移表であって、制御ロジック全体についての状態遷移表である。

図１９は、図８に対応する全体状態遷移表の構成例を示している。ゲートウェイロジック生成部３２が全体状態遷移表を得るための方法として、エンジニアリングツール３０があらかじめ用意したファンクションブロックに対する状態遷移表であって設計段階において状態遷移表を作成し、作成した状態遷移表をエンジニアリングツール３０の一部として提供する方法が考えられる。状態遷移表１９２は、少なくとも、現状態を表す識別情報と、現状態に対応する状態遷移が発生するために満たされるべき条件と、次状態との各々を示す情報を含む。当該条件は、満たされるべきデバイスの値と値の変化等を識別することができるように定義したものである。値の変化は、具体例として、立ち上がりにおける値の変化、立ち下がりにおける値の変化、又は、値の変化が閾値を上回ること若しくは下回ることである。また、本実施の形態に係る全体状態遷移表は、各現状態が安全状態に当たるか否かを示す安全状態フラグを含んでいなければならない。

なお、ゲートウェイロジック生成部３２が全体状態遷移表を得る方法は、

前述の方法に限定されない。具体例として、ゲートウェイロジック生成部３２は、ユーザが生成したプログラムを解析することによって全体状態遷移表を得てもよく、プログラミング手段提供部３１と各種の設計ツールと連動してプログラムの設計情報に基づいて全体状態遷移表を得てもよい。

[0084]（ステップＳ１０２）

ゲートウェイロジック生成部３２は、非安全状態に当たる全ての行を全体状態遷移表から抽出する。ゲートウェイロジック生成部３２は、「安全状態フラグ」の値を参照することにより非安全状態に当たる状態を抽出することができる。ゲートウェイロジック生成部３２は、本ステップで抽出した行を保持する。

図２０は、図１９に示す例に対して本ステップの処理を実行した結果を示している。

[0085]（ステップＳ１０３）

ゲートウェイロジック生成部３２は、ステップＳ１０２で抽出した行のうち、全体状態遷移表の他の少なくともいずれかの行に対応する重複行を抽出する。重複行は、行の「条件」のうち安全データの各値が他の行の「条件」のうち安全データの各値と重複する行である。ここで、ゲートウェイロジック生成部３２は、２つの行の「条件」が完全に一致する場合に「条件」が重複するものと判断する。ゲートウェイロジック生成部３２は、本ステップで抽出した行を一次リストとして保持する。

図２０に示す例において、通番７の「条件」のうち安全データの各値であるＳ＿Ｅｓｔｏｐ１からデバイスＣまでの各値と、通番４及び５の各々の「条件」のうち安全データの各値とが重複する。よって、通番７に対応する行は重複行であるため、ゲートウェイロジック生成部３２は通番７に対応する行を一次リストとして保持する。

[0086]（ステップＳ１０４）

ゲートウェイロジック生成部３２がステップＳ１０３で重複行を抽出した場合、ゲートウェイロジック生成部３２はステップＳ１０５に遷移する。そ

れ以外の場合、ゲートウェイロジック生成部３２はステップＳ１０８に遷移する。

[0087]（ステップＳ１０５）

ゲートウェイロジック生成部３２は、一次リストに含まれている各行を一次リストから削除し、削除した各行が示す現状態を次状態とする行を全体状態遷移表から抽出する。ゲートウェイロジック生成部３２は、本ステップで抽出した行を一次リストに加えて保持する。

ここで、前述のように一次リストに通番７に対応する行が含まれている場合を考える。このとき、通番７の現状態は状態４であり、状態４を次状態とする行は通番５及び６の各々に対応する行である。そのため、ゲートウェイロジック生成部３２は通番５及び６の各々に対応する行を一次リストに加える。

[0088]（ステップＳ１０６）

ゲートウェイロジック生成部３２は、ステップＳ１０５を実行した結果である一次リストに含まれている行のうち、「条件」のうち安全データの各値が、ステップＳ１０２で抽出した行の「条件」のうち安全データの各値とも、本フローチャートの処理を開始してからこれまでに一度でも一次リストに加えられた行の「条件」のうち安全データの各値とも重複しない行を一次リストから削除する。一次リストに残った行がある場合、ゲートウェイロジック生成部３２はステップＳ１０５に戻る。ゲートウェイロジック生成部３２は、一次リストに含まれている行が尽きるまで、ステップＳ１０５を繰り返す。

ここで、前述のように一次リストに通番５及び６の各々に対応する行が含まれている場合を考える。通番５に対応する行は、通番４に対応する行と「条件」のうち安全データの各値が重複するため、一次リストから取り除かれず、ステップＳ１０５の処理対象とされる。ここで、通番５の現状態は状態２であり、状態２を次状態とする行は通番３に対応する行のみである。よって、次にゲートウェイロジック生成部３２がステップＳ１０５を実行した際

に、通番３に対応する行が一次リストに加えられる。通番６に対応する行は、本ステップにおける比較対象である行のいずれとも「条件」のうち安全データの各値が重複しないので、一次リストから取り除かれる。

[0089]（ステップＳ１０７）

ゲートウェイロジック生成部３２は、ステップＳ１０２で抽出した行と、ステップＳ１０３とステップＳ１０５とステップＳ１０６との少なくともいずれかで一度でも一次リストに加えられた行とを重複なく結合した状態遷移表を作成する。

図２１は、図１９に対応する状態遷移表であって、本ステップにおいて生成される状態遷移表の具体例を示している。

[0090]（ステップＳ１０８）

ゲートウェイロジック生成部３２は、ステップＳ１０７で作成した状態遷移表から、他の行との差別化において不要な要素を削除する。なお、本ステップは必須ではないが、状態遷移表１９２のサイズを削減するためにゲートウェイロジック生成部３２は本ステップを実施してもよい。

[0091] 以上の処理により、ゲートウェイロジック生成部３２は、状態遷移表１９２のうち条件１の判定を行うための部分を生成することができる。

同様に、状態遷移表１９２のうち条件２の判定を行うための部分は、ステップＳ１０１からステップＳ１０８までを下記の通り変更することにより生成することができる。

ステップＳ１０１では、制御ロジックの全体状態遷移表を、安全コントローラ２０が出力する安全データの値に対して生成する。

ステップＳ１０２では、ゲートウェイロジック生成部３２は、安全状態から非安全状態への遷移に当たる全ての行を全体状態遷移表から抽出する。

ステップＳ１０３からステップＳ１０８までについては、ゲートウェイロジック生成部３２は、上記と同様のことを行って状態遷移表を得る。

[0092]＜出力定義情報１９１の作成＞

ゲートウェイロジック生成部３２は、状態遷移表１９２と全体状態遷移表

とに基づいて、出力定義情報１９１を生成する。

具体例として、まず、ゲートウェイロジック生成部３２は、状態遷移表１９２が示す遷移のうち、安全状態への遷移が生じる遷移を抽出し、抽出した遷移に対応する状態遷移表１９２の「現状態」と「次状態」とを、それぞれ、出力定義情報１９１の「前状態」と「現状態」とする。なお、抽出した遷移が複数ある場合において、出力定義情報１９１の１行は１つの遷移に対応する。次に、ゲートウェイロジック生成部３２は、全体状態遷移表を参照して抽出した遷移に対応する「出力値」の変化を求め、求めた変化を示す情報を出力定義情報１９１の「出力定義」に入力する。図１４における「０－＞１」は、「前状態」における出力値が０であり、「現状態」における出力値が１であることを示している。なお、ゲートウェイ装置１０が複数の制御アプリケーションを並列に実行する場合、いずれの制御アプリケーションに対応する出力定義情報１９１であるかを示す情報を出力定義情報１９１に設けてもよい。

[0093] ＜状態記憶部１９３の作成＞

ゲートウェイロジック生成部３２は、状態記憶部１９３を作成し、作成した状態記憶部１９３を初期化する。

ゲートウェイ装置１０が複数の制御アプリケーションを並列に実行する場合において、ゲートウェイロジック生成部３２は、各制御アプリケーションの状態を記憶する記憶領域である状態記憶部１９３を作成し、各制御アプリケーションの状態が各制御アプリケーションの開始直後の状態であるものとして状態記憶部１９３を初期化する。

[0094] ＜安全データマッピング表１９４の作成＞

ゲートウェイロジック生成部３２は、安全データの名称とメモリの特定情報とを対応づけることにより安全データマッピング表１９４を作成する。当該名称はラベルであってもよい。当該特定情報は、具体例としてアドレスである。当該名称と当該特定情報との対応付けは、プログラミング手段提供部３１によってユーザによって設定され又は自動設定により生成され、ゲート

ウェイロジック生成部３２は、当該対応付けを示す情報に基づいて安全データマッピング表１９４を生成する。なお、安全データマッピング表１９４の要素は、状態監視制御部１３０及び安全制御部１２０が安全データの所在を特定することができる要素であればよい。前述の安全データの名称の代わりにシンボル名を用い、また、特定情報としてデバイス番号を用いる等、安全データマッピング表１９４の要素は適宜変更されてもよい。

[0095] なお、前述の状態遷移表１９２と、出力定義情報１９１と、状態記憶部１９３と、安全データマッピング表１９４との４つの情報の説明では、非安全状態から安全状態への遷移の場合を中心に述べたが、安全状態から非安全状態への遷移についても、同様に４つへの情報を作成する必要がある。情報の生成方法は非安全状態から安全状態への遷移の場合と類似するが、下記が異なる。

ゲートウェイロジック生成部３２は、状態遷移表１９２に、安全状態から非安全状態への遷移を表す全体状態遷移表の行を漏れなくかつ重複無く追加する。この際、ゲートウェイロジック生成部３２は、安全コントローラ２０から安全入出力ユニット４０に向けた安全データに着目して条件を追加する。一意に識別することができない条件が含まれる場合、ゲートウェイロジック生成部３２は、ステップＳ１０５と同じ考え方に基づき、当該条件を含む前状態の行を状態遷移表に追加し、新たに追加した前状態が他の行と区別することができるようになるまで前状態の追加を繰り返す。

ゲートウェイロジック生成部３２は、安全状態から非安全状態への遷移に対応する出力定義情報１９１を追加する。「出力定義」は、ステップＳ０９’－７で述べた安全データ書き換え操作の変更の方法を示すように作成する。図２２は、安全状態から非安全状態への遷移についての出力定義情報１９１の具体例を示している。当該出力定義情報１９１の出力定義は、安全データの書き換えを終了することを指示する情報、即ち、安全コントローラ２０の出力を優先するように切り替えることを指示する情報である。

[0096] ＊＊＊実施の形態１の効果の説明＊＊＊

以上のように、本実施の形態によれば、安全入出力ユニット４０と安全コントローラ２０との間の通信を中継するゲートウェイ装置１０であって、必要な処理量を削減したゲートウェイ装置１０を用いることにより、安全応答時間を短縮した安全制御システム８０を比較的安価に実現することができる。背景技術には内部状態を持つ制御ロジックを実行するゲートウェイ装置を実現することができないという課題があるが、本実施の形態によれば、内部状態を持つ制御ロジックを実行するゲートウェイ装置を少ない処理量で実現することができる。

安全応答時間の短縮は、安全状態への遷移をゲートウェイ装置１０の判断により実施できることによって実現される。そのため、先行技術における安全応答時間には、安全入出力ユニット４０から安全コントローラ２０までの往復に関する伝送遅延と伝送乗り遅れ時間とが含まれるが、本実施の形態によれば、安全入出力ユニット４０から安全コントローラ２０までの途中に位置するゲートウェイ装置１０から安全コントローラ２０までの往復に関する伝送遅延と伝送乗り遅れ時間とが安全応答時間に含まれないように構成することができる。安全応答時間は安全状態への遷移に要する最悪時間であるので、本実施の形態によれば安全応答時間を短縮することができる。また、本実施の形態によれば、あたかも通信方式の変換によるオーバヘッドがないように振る舞うゲートウェイ装置１０を構成することができる。

また、安全状態への遷移に関わる処理以外の処理をゲートウェイ装置１０が実行せず、安全コントローラ２０が判断するようにゲートウェイ装置１０が安全状態への遷移を判断することにより、ゲートウェイ装置１０の処理を削減することができる。そのため、安価なマイクロコンピュータ等のコンポーネントによって安全制御システム８０を実現することができるほか、限られた計算リソースでより多くの安全コネクションを変換するゲートウェイ装置１０を構成することができるため、安価に安全制御システム８０を構成することができる。加えて、ゲートウェイ装置１０を安全コントローラ２０と安全入出力ユニット４０との双方に対して透過的に振る舞うように構成する

ことができるため、既存の安全コントローラ２０と、安全入出力ユニット４０とをそのまま利用することができることも、安全制御システム８０を安価に実現できることに貢献する。

[0097] また、本実施の形態は、通信方式の変換を必要としない場合においても、同様の効果を有する。具体例として、安全制御システム８０の構成が安全入出力ユニット４０と安全コントローラ２０との間の伝送遅延が大きい構成である場合において、安全入出力ユニット４０から近い箇所等の伝送遅延が小さい箇所にゲートウェイ装置１０を設置することにより、安全応答時間を短縮することができる。安全入出力ユニット４０と安全コントローラ２０との間の伝送遅延が大きいシステム構成は、具体例として、ルータ又はＬ３（Ｌａｙｅｒ　３）スイッチ等で異なるネットワークセグメントを跨いだ通信が生じる構成、安全コントローラ２０がクラウド等伝送遅延の大きい箇所に設置されている構成、又は、安全コントローラ２０の処理の定時性が低いために最悪時間が大きい構成である。安全制御システム８０の構成がこのような構成である場合において、ゲートウェイ装置１０は、安全入出力ユニット４０とも安全コントローラ２０とも同じ通信方式で通信するように構成されればよい。

このような安全制御システム８０を構成する場合に、ゲートウェイ装置１０に対して制御ロジックに応じたゲートウェイロジックを設定することに関する手間が生じることが考えられる。しかしながら、エンジニアリングツール３０の支援によって半自動的にゲートウェイロジックを生成すること及び設定することができるため、当該場合に係る手間を軽減することができる。

[0098] ここで、特許文献１に係る課題が生じる理由を述べる。特許文献１では判断結果の送信先を変えた変形例を認めていることから、安全コントローラの制御出力を待つことなく安全制御を行うことにより伝送遅延が生じることを回避することができるゲートウェイ装置を実現することが考えられる。しかし、特許文献１の開示範囲では、安全判断を簡易に行うことができる場合が限られるため、幅広い安全制御に対応するためには安全コントローラと同等

の制御ロジックをもつゲートウェイが必要である。そのため、特許文献１の技術によってはゲートウェイ装置を安価に実現することができない。具体的には下記の通りである。

特許文献１では、安全判断手段は安全条件を満足するか否かを入力安全情報を用いた論理演算により簡単に判断することができると説明しているものの、詳細な判断手法を開示していない。しかし、多くの安全制御アプリケーションでは内部状態を伴って制御を行うため、入力安全情報を用いた演算のみでは安全判断を実行することができない。具体例として、入力安全情報が同じであったとしても、入力安全情報が生成されるまでにある手順を経ているか否かによって安全状態が異なることがある。非常停止ボタンと、両手操作系と、ミューティング等の制御が本例に該当する。

同様に、判断結果を安全状態から非安全状態に見直す場合についても、所定のリセット等の手順を経ているか否かを確認する必要があるものの、特許文献１が開示する技術では手順の確認等に対応することができない。

従って、先行技術を利用するだけではゲートウェイ装置での安全判断を適切に行うことができないため、安全コントローラと同程度の複雑度をもつ安全判断部をゲートウェイ装置に実現する手法と、ゲートウェイ装置の安全判断部を、安全判断部の複雑度を下げる代わりに本来不要な安全状態への遷移を引き起こし得るものとする手法とのいずれか等を追加的に採用せざるを得ない。ここで、ゲートウェイ装置を安全コントローラに比べて安価で実現することが一般的に期待される。さらに、ゲートウェイ装置は安全コントローラと安全入出力ユニットとの両方との通信を行わなければならない。そのため、前者を採用する場合、ゲートウェイ装置の処理に十分な余裕がなくなるリスクがある。後者を採用する場合、常に通常よりも安全な状態が保たれるために機能安全の観点において課題はないものの、安全制御システム８０の可用性が低下するため実用的ではないという課題がある。しかしながら、本実施の形態によればこれらの課題が生じない。

[0099] ＊＊＊他の構成＊＊＊

＜変形例１＞

図２３は、本変形例に係るゲートウェイ装置１０のハードウェア構成例を示している。

ゲートウェイ装置１０は、プロセッサ１１、プロセッサ１１とメモリ１２、プロセッサ１１と不揮発メモリ１６、あるいはプロセッサ１１とメモリ１２と不揮発メモリ１６とに代えて、処理回路１８を備える。

処理回路１８は、ゲートウェイ装置１０が備える各部の少なくとも一部を実現するハードウェアである。

処理回路１８は、専用のハードウェアであってもよく、また、メモリ１２に格納されるプログラムを実行するプロセッサであってもよい。

[0100] 処理回路１８が専用のハードウェアである場合、処理回路１８は、具体例として、単一回路、複合回路、プログラム化したプロセッサ、並列プログラム化したプロセッサ、ＡＳＩＣ（ＡＳＩＣはＡｐｐｌｉｃａｔｉｏｎ Ｓｐｅｃｉｆｉｃ Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ）、ＦＰＧＡ（Ｆｉｅｌｄ Ｐｒｏｇｒａｍｍａｂｌｅ Ｇａｔｅ Ａｒｒａｙ）又はこれらの組み合わせである。

ゲートウェイ装置１０は、処理回路１８を代替する複数の処理回路を備えてもよい。複数の処理回路は、処理回路１８の役割を分担する。

[0101] ゲートウェイ装置１０において、一部の機能が専用のハードウェアによって実現されて、残りの機能がソフトウェア又はファームウェアによって実現されてもよい。

[0102] 処理回路１８は、具体例として、ハードウェア、ソフトウェア、ファームウェア、又はこれらの組み合わせにより実現される。

プロセッサ１１とメモリ１２と不揮発メモリ１６と処理回路１８とを、総称して「プロセッシングサーキットリー」という。つまり、ゲートウェイ装置１０の各機能構成要素の機能は、プロセッシングサーキットリーにより実現される。

本明細書に記載されている他の装置についても本変形例と同様の構成であ

ってもよい。

[0103] ＊＊＊他の実施の形態＊＊＊

実施の形態１について説明したが、本実施の形態のうち、複数の部分を組み合わせて実施しても構わない。あるいは、本実施の形態を部分的に実施しても構わない。その他、本実施の形態は、必要に応じて種々の変更がなされても構わず、全体としてあるいは部分的に、どのように組み合わせて実施されても構わない。

なお、前述した実施の形態は、本質的に好ましい例示であって、本開示と、その適用物と、用途の範囲とを制限することを意図するものではない。フローチャート等を用いて説明した手順は、適宜変更されてもよい。

符号の説明

[0104] １０　ゲートウェイ装置、１１　プロセッサ、１２　メモリ、１３　第１ポート、１４　第２ポート、１５　バス、１６　不揮発メモリ、１７　設定ポート、１８　処理回路、１１１　第１通信ポート、１１２　第２通信ポート、１１３　第１通信制御部、１１４　制御データ中継部、１１５　第２通信制御部、１２０　安全制御部、１２１　安全状態管理部、１２２　安全データ制御部、１３０　状態監視制御部、１３１　状態遷移検出部、１３２　安全データ監視部、１９１　出力定義情報、１９２　状態遷移表、１９３　状態記憶部、１９４　安全データマッピング表、２０　安全コントローラ、２１　プロセッサ、２２　メモリ、２３　設定ポート、２４　第１ポート、２５　バス、２６　不揮発メモリ、３０　エンジニアリングツール、３１　プログラミング手段提供部、３２　ゲートウェイロジック生成部、３３　ゲートウェイロジック設定部、３４　ロジック生成部、３５　ロジック設定部、４０　安全入出力ユニット、４１　プロセッサ、４２　メモリ、４３　ＩＯポート、４４　第２ポート、４５　バス、４６　不揮発メモリ、５０　設定端末、５１　プロセッサ、５２　メモリ、５３　設定ポート、５５　バス、５６　不揮発メモリ、８０　安全制御システム、９０　一般通信パケット、９１　一般通信ヘッダ、９２　一般通信ペイロード、９３　一般通信ＦＣ

Ｓ、９２０　安全通信パケット、９２１　安全通信ヘッダ、９２２　安全通信ペイロード、９２３　安全入出力データ、９２４　安全通信ＦＣＳ、Ｎ１，Ｎ２　ネットワーク、Ｐ１，Ｐ２　安全通信パケット。

請求の範囲

[請求項1] 安全制御システムが備える安全入出力ユニットと前記安全入出力ユニットを制御する安全コントローラとの間における安全データの通信を中継することにより前記安全入出力ユニットと前記安全コントローラとの安全コネクションを確立するゲートウェイ装置であって、

前記安全制御システムの状態に対応する状態であって、安全状態と非安全状態とのいずれかの状態である制御状態を管理し、かつ、前記ゲートウェイ装置が前記安全入出力ユニットから受信した安全データを、前記制御状態についての状態遷移を示す状態遷移情報に適用することにより前記制御状態の状態遷移を制御する状態監視制御部と、

前記制御状態が前記非安全状態から前記安全状態に遷移した場合に、前記安全入出力ユニットに送信する安全データであって、前記安全状態を示す安全データを生成する安全制御部と

を備えるゲートウェイ装置。

[請求項2] 前記安全制御部は、前記制御状態が前記非安全状態から前記安全状態に遷移した場合に、前記安全コネクションを切断する制御を実行する請求項１に記載のゲートウェイ装置。

[請求項3] 前記状態監視制御部は、前記ゲートウェイ装置が前記安全コントローラから受信した安全データを前記状態遷移情報に適用することにより前記制御状態の状態遷移を制御し、

前記安全制御部は、前記安全コネクションが切断されている場合において、前記制御状態が前記安全状態から前記非安全状態に遷移した場合に前記安全コネクションの切断を解除する請求項２に記載のゲートウェイ装置。

[請求項4] 前記安全制御部は、前記安全コネクションを切断する制御として、前記安全状態を示す安全データとなるよう、前記ゲートウェイ装置が前記安全コントローラから受信した安全データを書き換える制御を実行する請求項２又は３に記載のゲートウェイ装置。

[請求項5] 前記状態監視制御部は、前記安全コネクションが切断されている場合において、前記安全コネクションを切断する契機となった安全データよりも古い安全データに基づいて制御を実施した結果を示す安全データであって、前記ゲートウェイ装置が前記安全コントローラから受信した安全データを用いずに前記制御状態の状態遷移を制御する請求項２から４のいずれか１項に記載のゲートウェイ装置。

[請求項6] 前記状態監視制御部は、前記安全コントローラが用いる制御ロジックの少なくとも一部である部分制御ロジックを用い、

前記状態遷移情報は、前記部分制御ロジックの少なくとも一部を示す情報である請求項１から５のいずれか１項に記載のゲートウェイ装置。

[請求項7] 前記状態遷移情報は、前記ゲートウェイ装置と通信することができるエンジニアリングツールを用いて設定された情報である請求項１から６のいずれか１項に記載のゲートウェイ装置。

[請求項8] 前記安全入出力ユニットが採用する通信方式は、前記安全コントローラが採用する通信方式と異なる請求項１から７のいずれか１項に記載のゲートウェイ装置。

[請求項9] 安全制御システムが備える安全入出力ユニットと前記安全入出力ユニットを制御する安全コントローラとの間における安全データの通信を中継することにより前記安全入出力ユニットと前記安全コントローラとの安全コネクションを確立するゲートウェイ装置を制御するゲートウェイ制御方法であって、

前記安全制御システムの状態に対応する状態であって、安全状態と非安全状態とのいずれかの状態である制御状態を管理し、かつ、前記ゲートウェイ装置が前記安全入出力ユニットから受信した安全データを、前記制御状態についての状態遷移を示す状態遷移情報に適用することにより前記制御状態の状態遷移を制御し、

前記制御状態が前記非安全状態から前記安全状態に遷移した場合に

、前記安全入出力ユニットに送信する安全データであって、前記安全状態を示す安全データを生成するゲートウェイ制御方法。

[請求項10] 安全制御システムが備える安全入出力ユニットと前記安全入出力ユニットを制御する安全コントローラとの間における安全データの通信を中継することにより前記安全入出力ユニットと前記安全コントローラとの安全コネクションを確立するコンピュータであるゲートウェイ装置を制御するゲートウェイ制御プログラムであって、

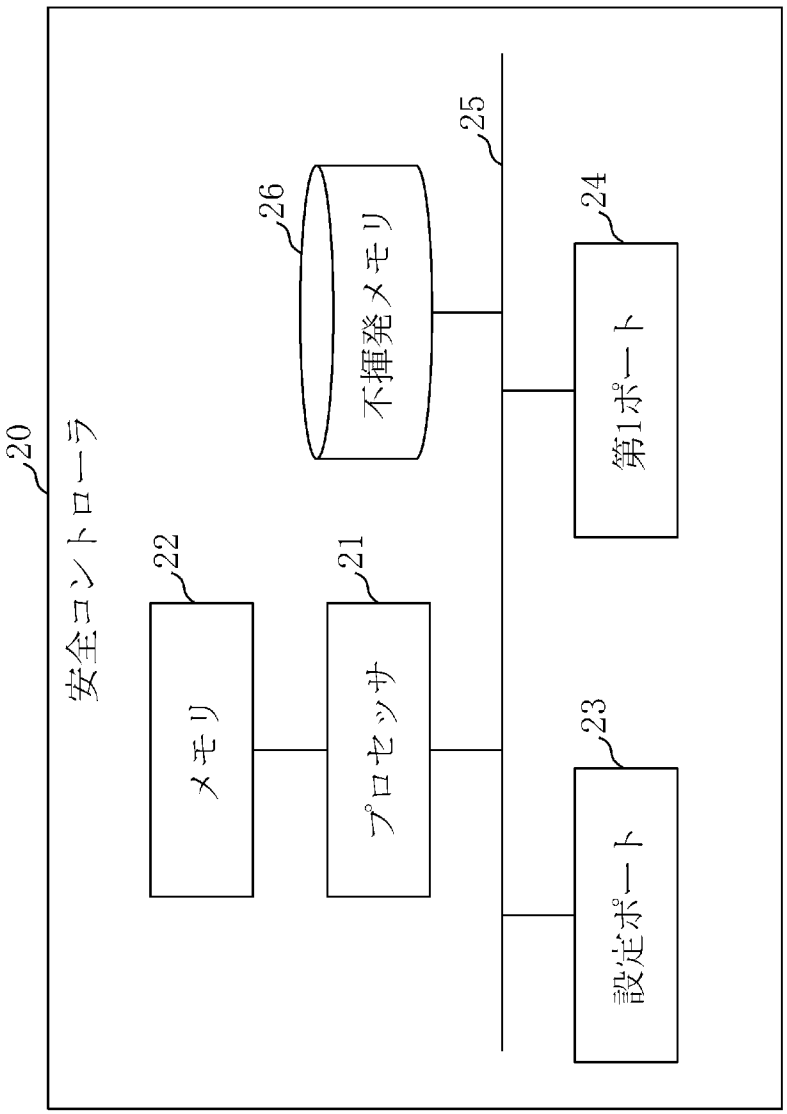
前記安全制御システムの状態に対応する状態であって、安全状態と非安全状態とのいずれかの状態である制御状態を管理し、かつ、前記ゲートウェイ装置が前記安全入出力ユニットから受信した安全データを、前記制御状態についての状態遷移を示す状態遷移情報に適用することにより前記制御状態の状態遷移を制御する状態監視制御処理と、

前記制御状態が前記非安全状態から前記安全状態に遷移した場合に、前記安全入出力ユニットに送信する安全データであって、前記安全状態を示す安全データを生成する安全制御処理と

を前記ゲートウェイ装置に実行させるゲートウェイ制御プログラム。

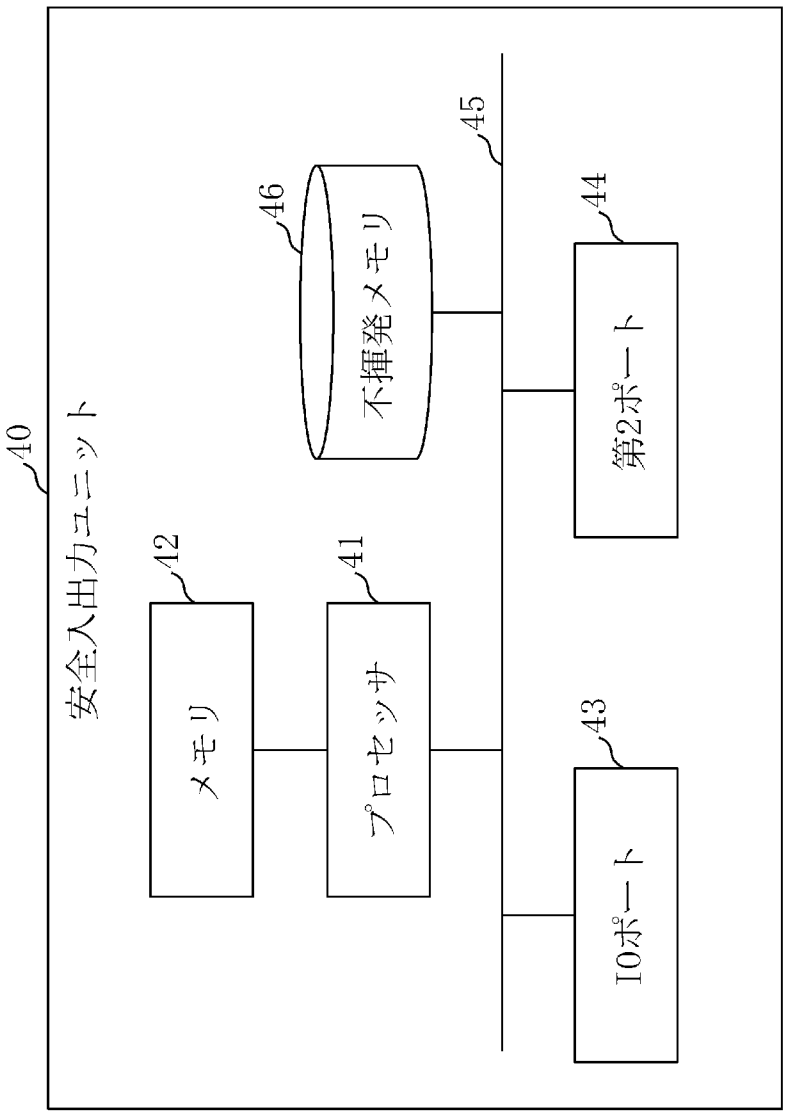
[図1]

図1



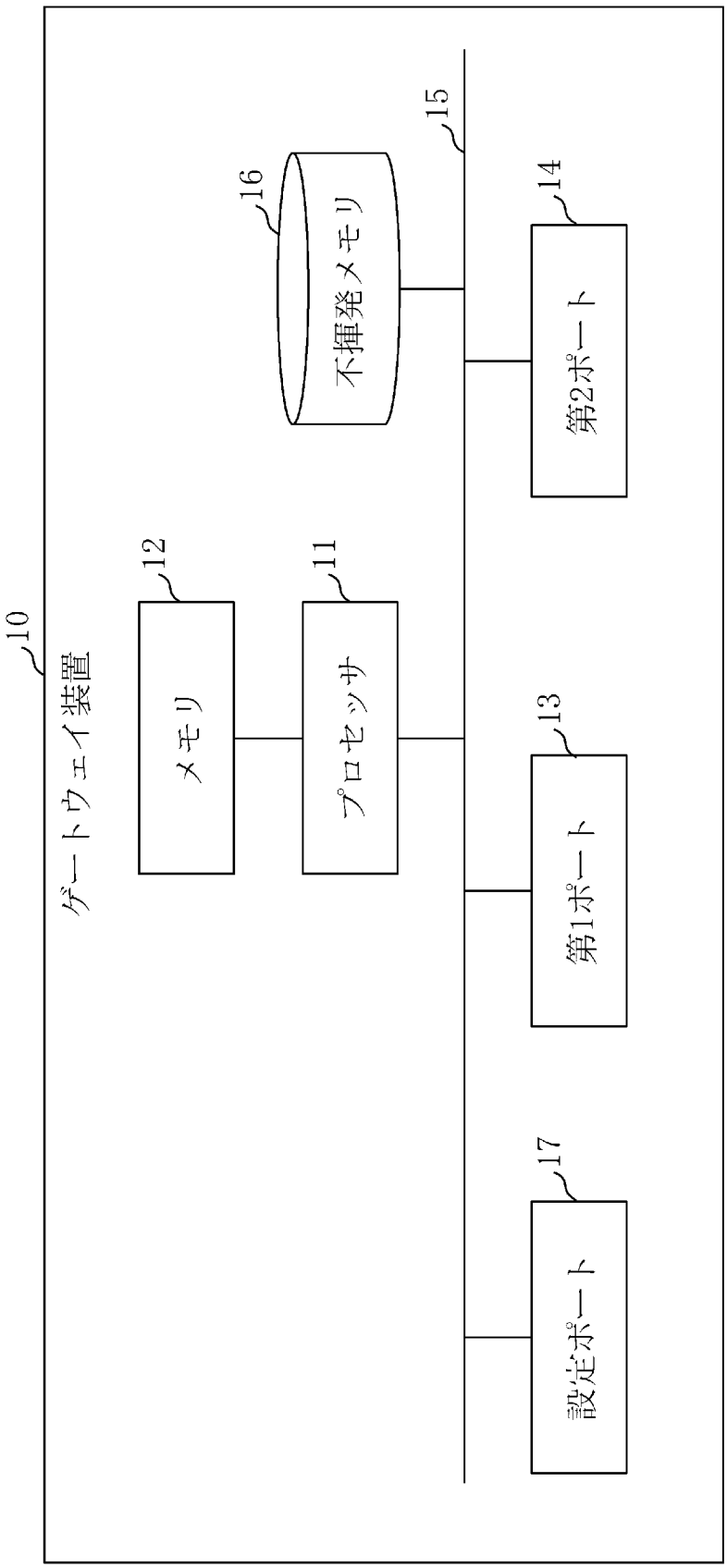
[図2]

図2



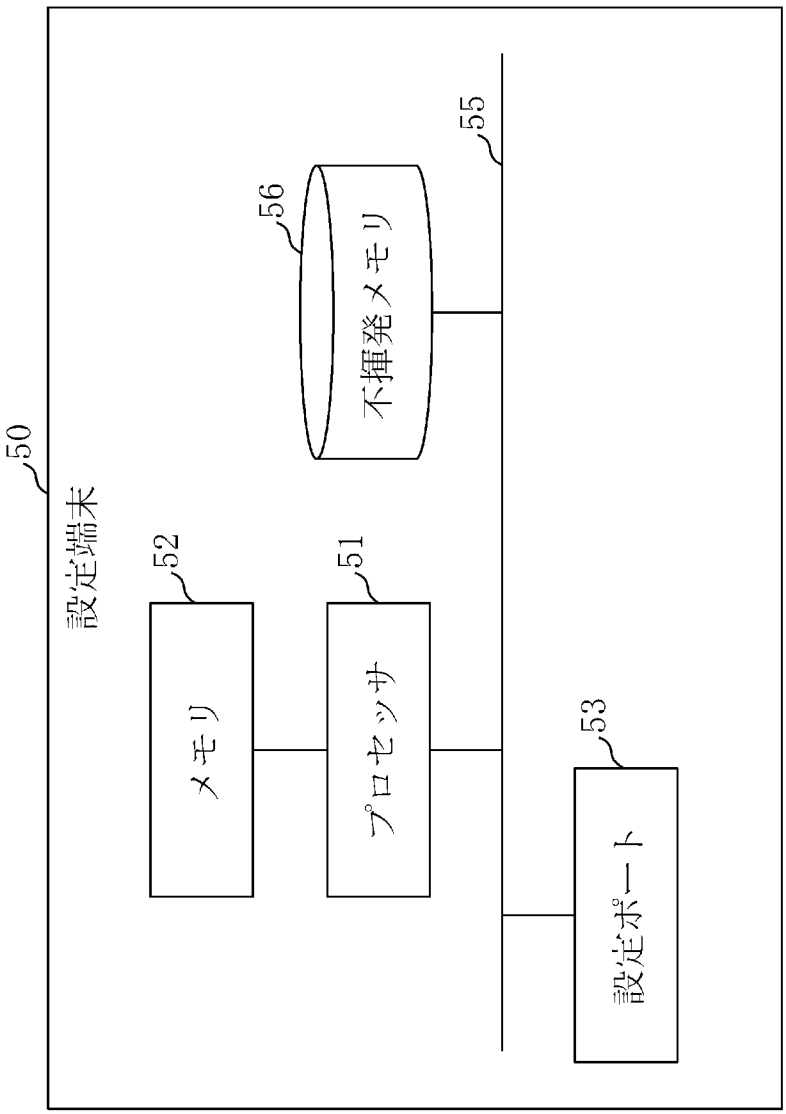
[図3]

図3


10
ゲートウェイ装置
12
メモリ
11
プロセッサ
16
不揮発メモリ
15
14
第2ポート
13
第1ポート
17
設定ポート

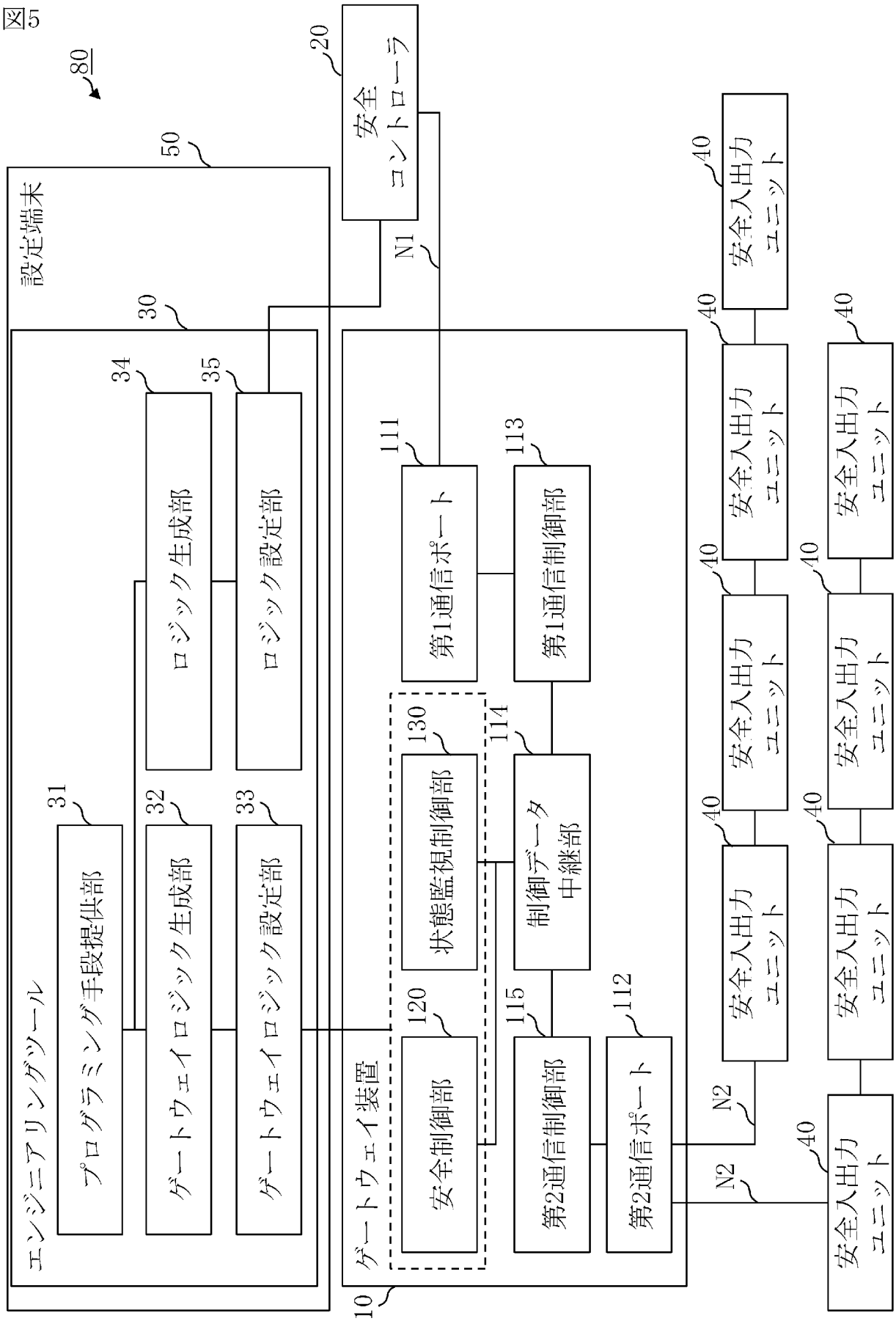
[図4]

図4



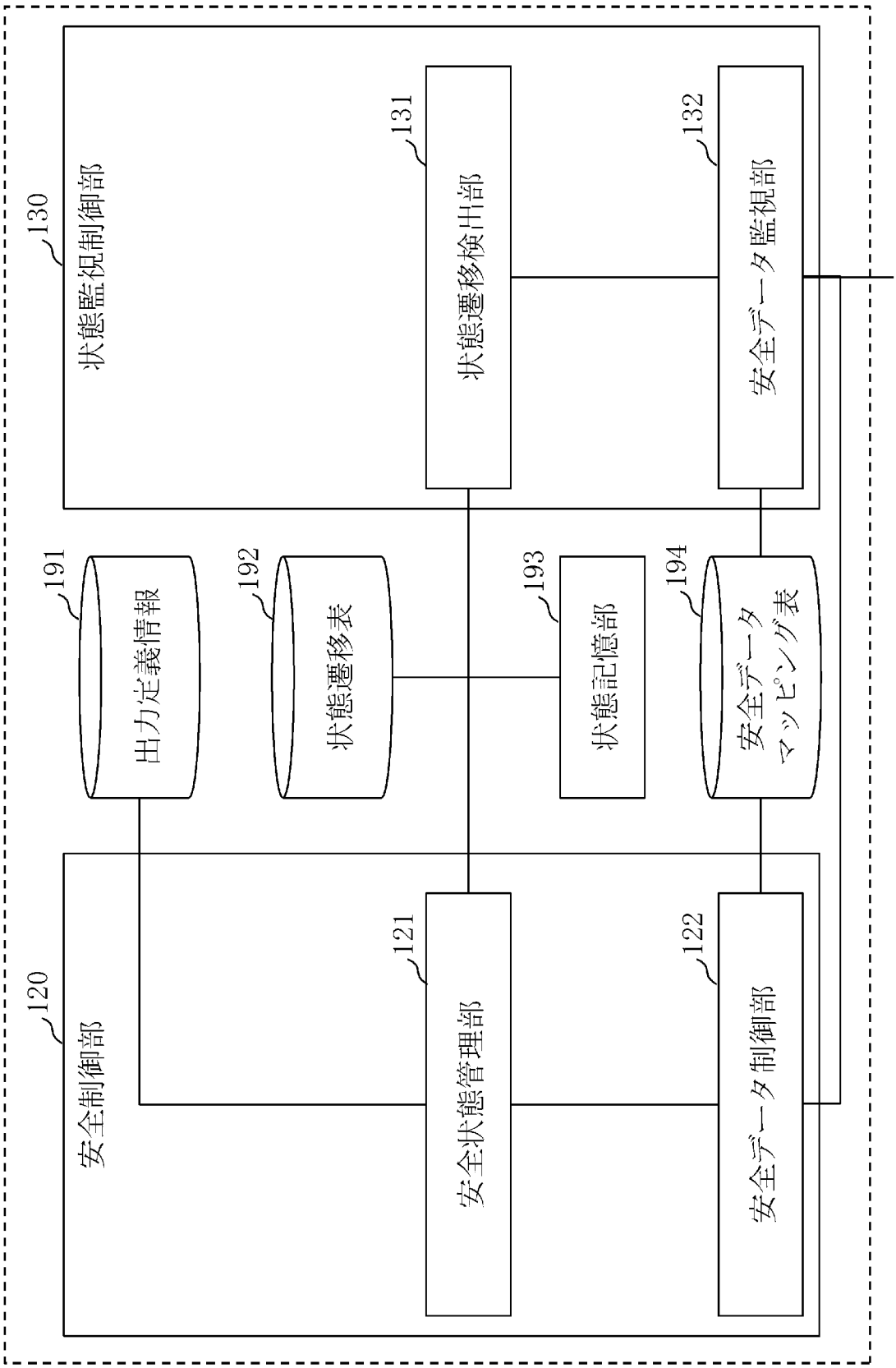
[図5]

図5


80
20
安全
コントローラ
50
設定端末
30
34
ロジック生成部
35
ロジック設定部
エンジニアリングツール
31
プログラミング手段提供部
32
ゲートウェイロジック生成部
33
ゲートウェイロジック設定部
N1
111
第1通信ポート
113
第1通信制御部
ゲートウェイ装置
130
状態監視制御部
114
制御データ
中継部
120
安全制御部
115
第2通信制御部
112
第2通信ポート
N2
N2
40
安全入出力
ユニット
40
安全入出力
ユニット
40
安全入出力
ユニット
40
安全入出力
ユニット
40
安全入出力
ユニット
40
安全入出力
ユニット
10

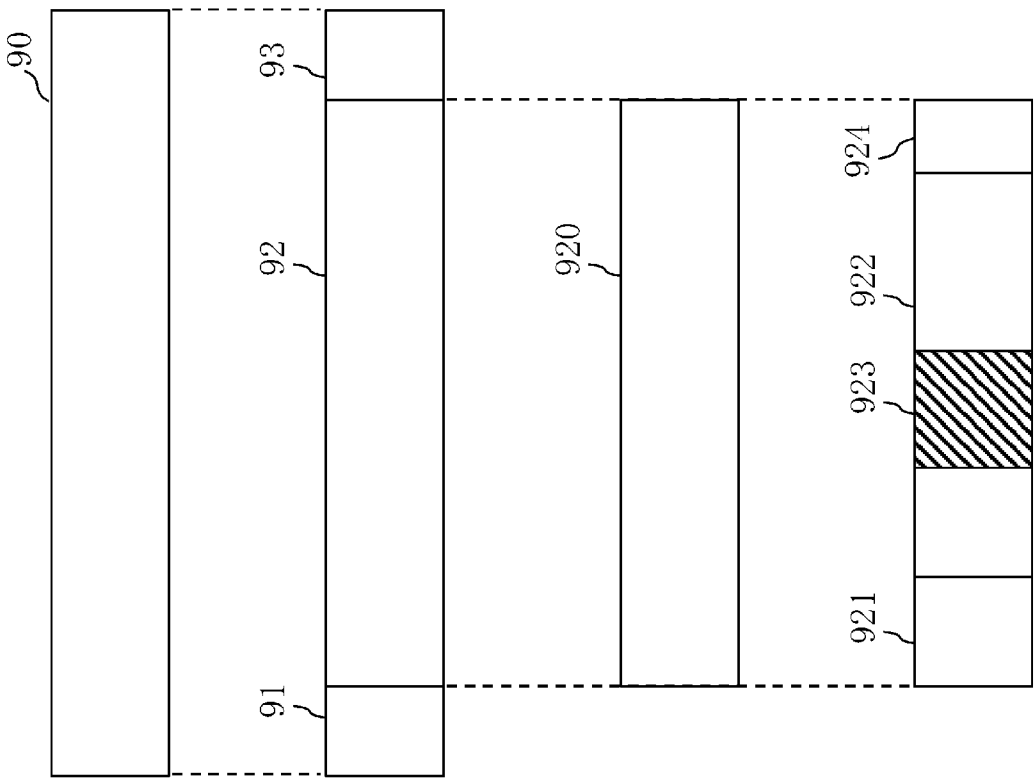
[図6]

図6


130
状態監視制御部
131
状態遷移検出部
132
安全データ監視部
191
出力定義情報
192
状態遷移表
193
状態記憶部
194
安全データ
マッピング表
120
安全制御部
121
安全状態管理部
122
安全データ制御部

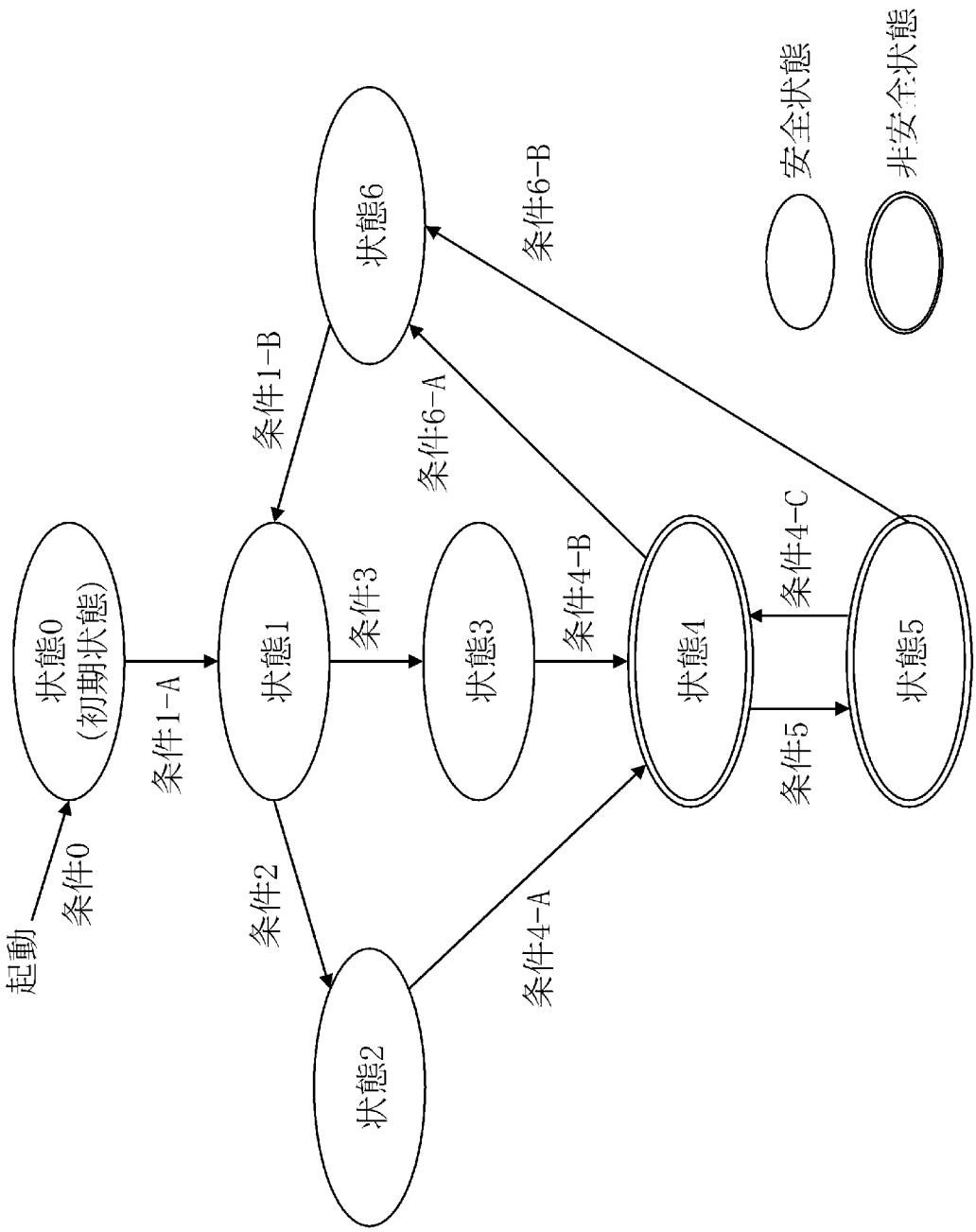
[図7]

図7



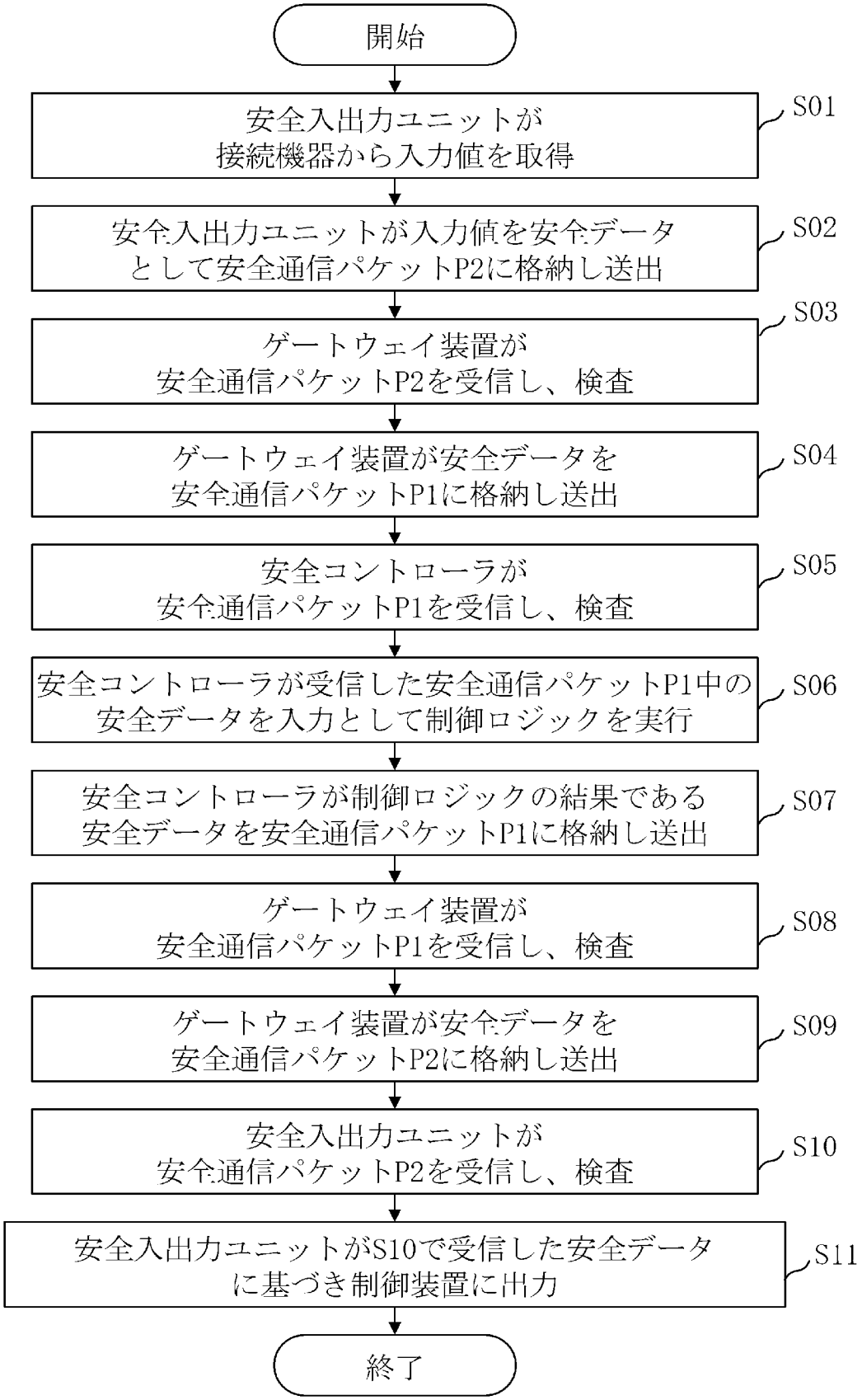
[図8]

図8


起動
条件0
状態0
(初期状態)
条件1-A
状態1
条件1-B
状態6
条件6-B
条件6-A
条件2
状態2
条件3
状態3
条件4-A
条件4-B
状態4
条件4-C
条件5
状態5
安全状態
非安全状態

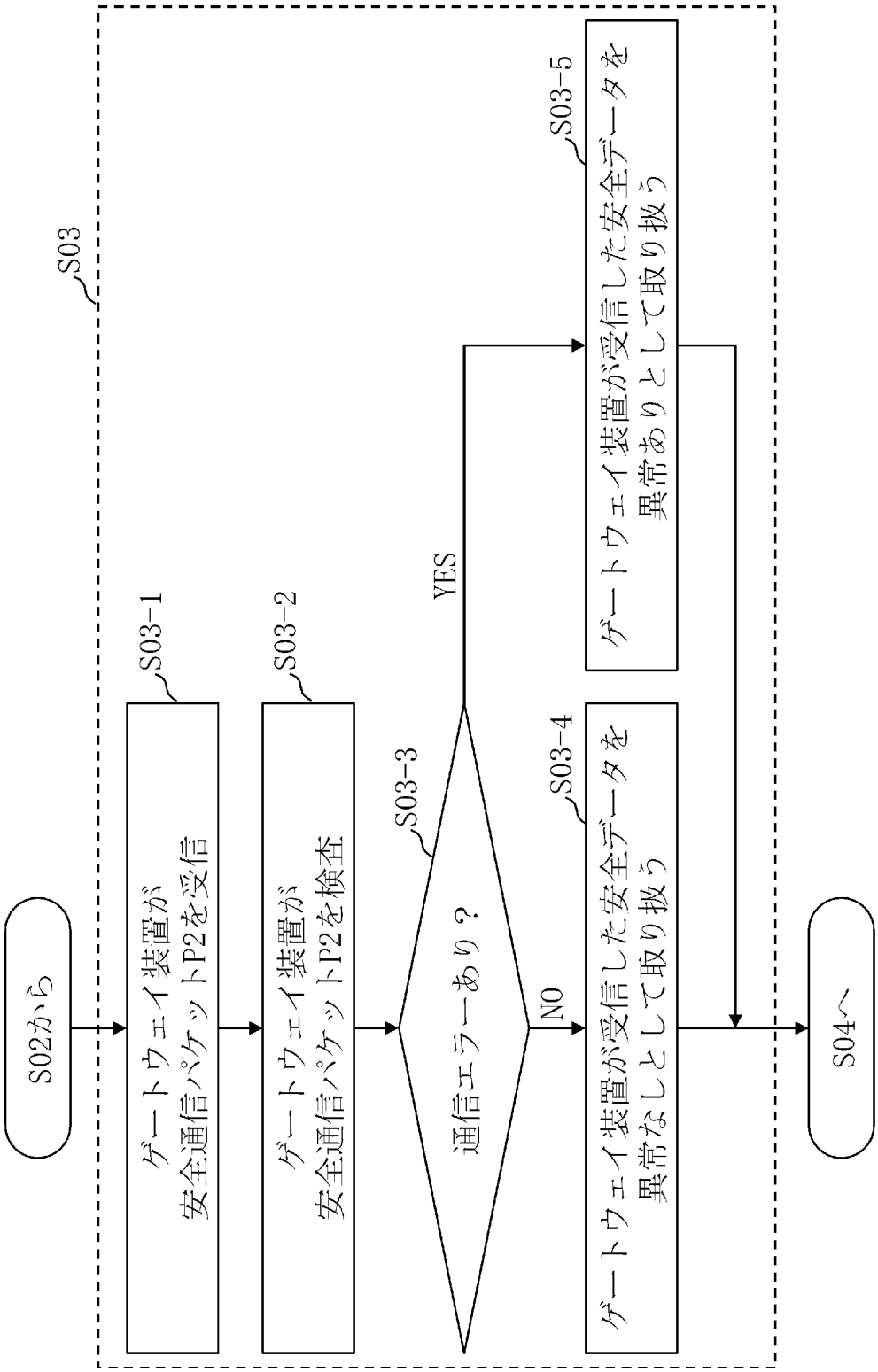
[図9]

図9


開始
安全入出力ユニットが
接続機器から入力値を取得
S01
安全入出力ユニットが入力値を安全データ
として安全通信パケットP2に格納し送出
S02
ゲートウェイ装置が
安全通信パケットP2を受信し、検査
S03
ゲートウェイ装置が安全データを
安全通信パケットP1に格納し送出
S04
安全コントローラが
安全通信パケットP1を受信し、検査
S05
安全コントローラが受信した安全通信パケットP1中の
安全データを入力として制御ロジックを実行
S06
安全コントローラが制御ロジックの結果である
安全データを安全通信パケットP1に格納し送出
S07
ゲートウェイ装置が
安全通信パケットP1を受信し、検査
S08
ゲートウェイ装置が安全データを
安全通信パケットP2に格納し送出
S09
安全入出力ユニットが
安全通信パケットP2を受信し、検査
S10
安全入出力ユニットがS10で受信した安全データ
に基づき制御装置に出力
S11
終了

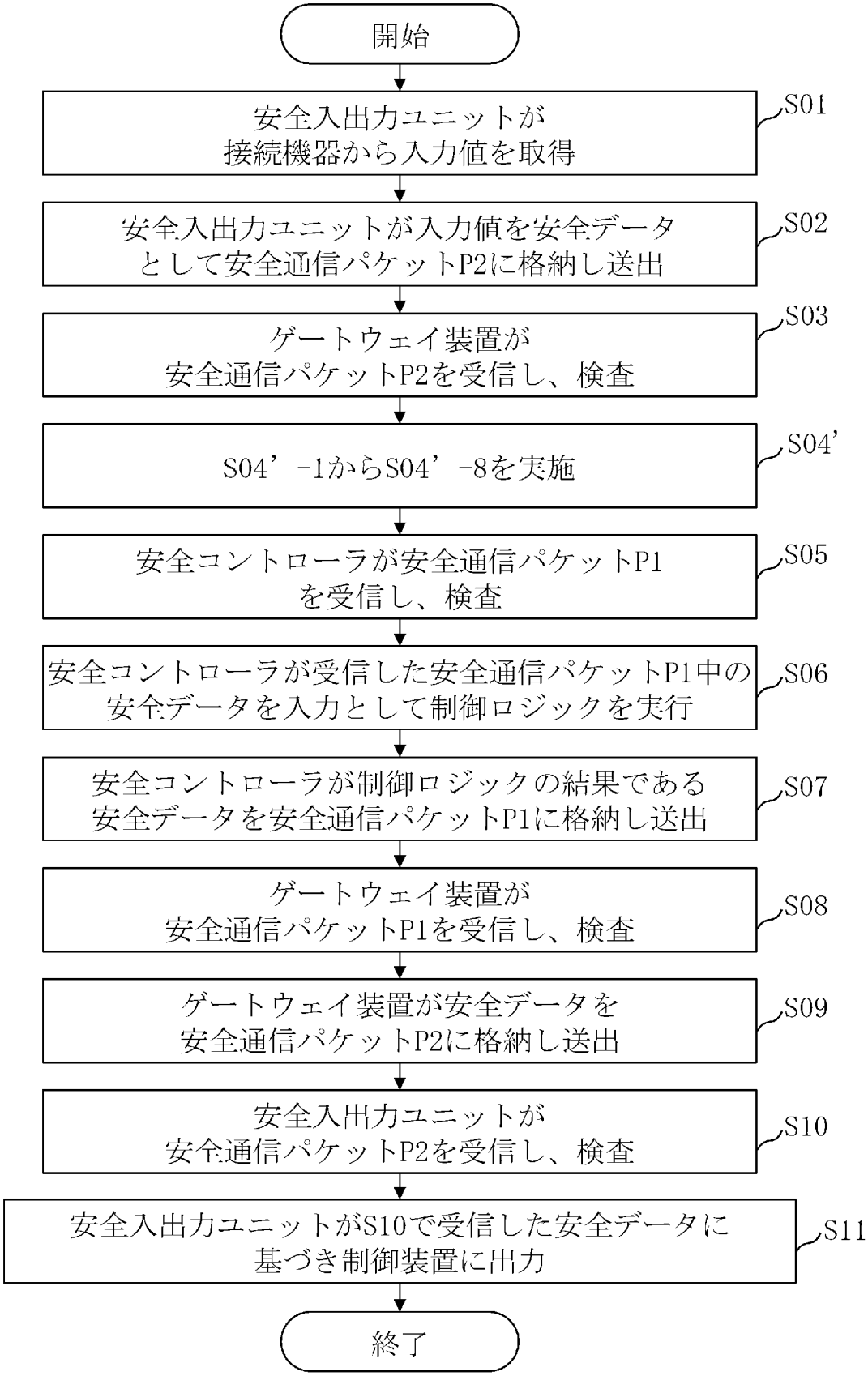
[図10]

図10


S03
S02から
S03-1
ゲートウェイ装置が
安全通信パケットP2を受信
S03-2
ゲートウェイ装置が
安全通信パケットP2を検査
S03-3
通信エラーあり？
YES
NO
S03-4
ゲートウェイ装置が受信した安全データを
異常なしとして取り扱う
S03-5
ゲートウェイ装置が受信した安全データを
異常ありとして取り扱う
S04へ

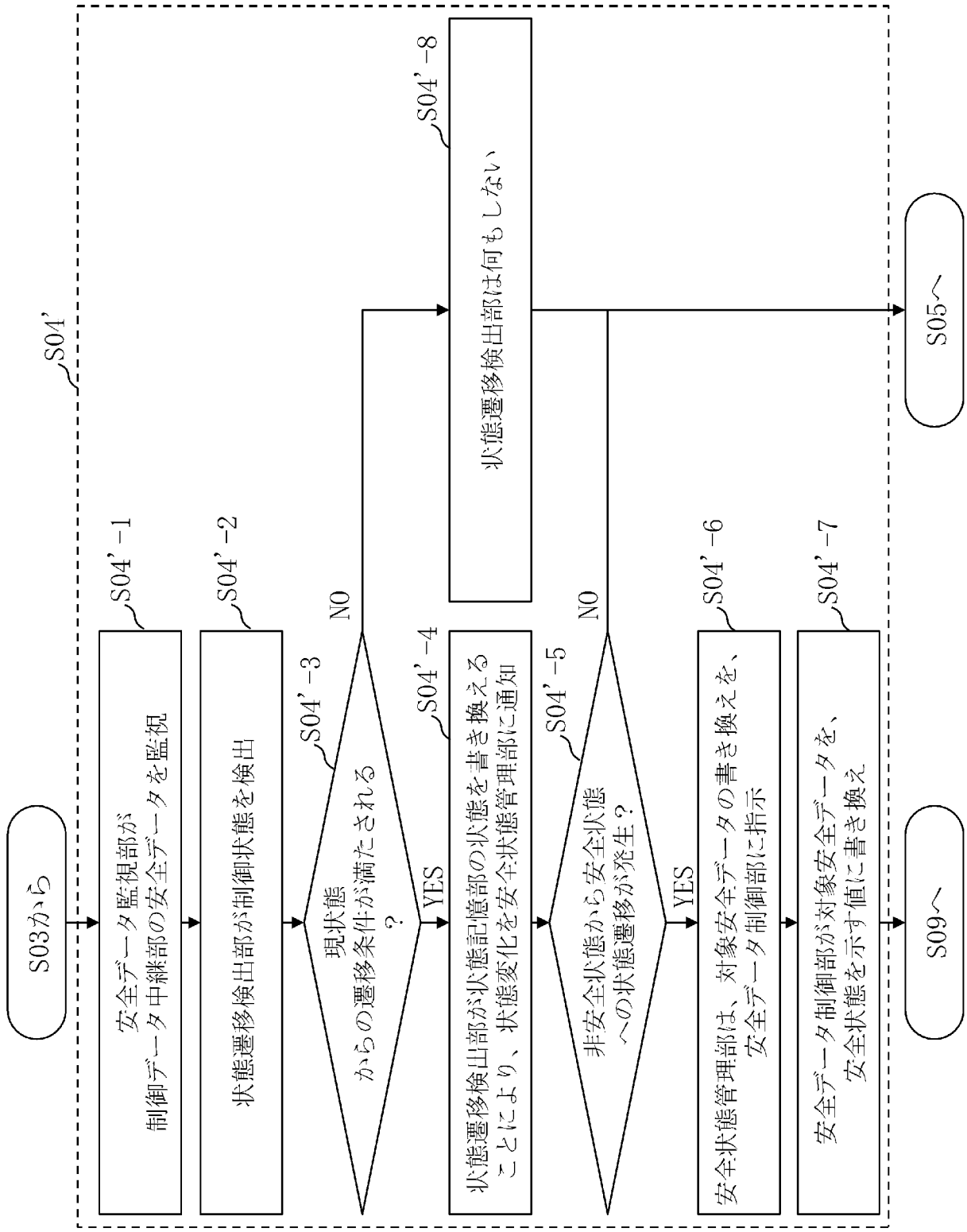
[図11]

図11


開始
安全入出力ユニットが
接続機器から入力値を取得
S01
安全入出力ユニットが入力値を安全データ
として安全通信パケットP2に格納し送出
S02
ゲートウェイ装置が
安全通信パケットP2を受信し、検査
S03
S04’-1からS04’-8を実施
S04’
安全コントローラが安全通信パケットP1
を受信し、検査
S05
安全コントローラが受信した安全通信パケットP1中の
安全データを入力として制御ロジックを実行
S06
安全コントローラが制御ロジックの結果である
安全データを安全通信パケットP1に格納し送出
S07
ゲートウェイ装置が
安全通信パケットP1を受信し、検査
S08
ゲートウェイ装置が安全データを
安全通信パケットP2に格納し送出
S09
安全入出力ユニットが
安全通信パケットP2を受信し、検査
S10
安全入出力ユニットがS10で受信した安全データに
基づき制御装置に出力
S11
終了

[図12]

図12


S04'
S03から
安全データ監視部が
制御データ中継部の安全データを監視
S04'-1
状態遷移検出部が制御状態を検出
S04'-2
現状態
からの遷移条件が満たされる
?
S04'-3
NO
YES
状態遷移検出部が状態記憶部の状態を書き換える
ことにより、状態変化を安全状態管理部に通知
S04'-4
状態遷移検出部は何もしない
S04'-8
非安全状態から安全状態
への状態遷移が発生?
S04'-5
NO
YES
安全状態管理部は、対象安全データの書き換えを、
安全データ制御部に指示
S04'-6
安全データ制御部が対象安全データを、
安全状態を示す値に書き換え
S04'-7
S05へ
S09へ

[図13]

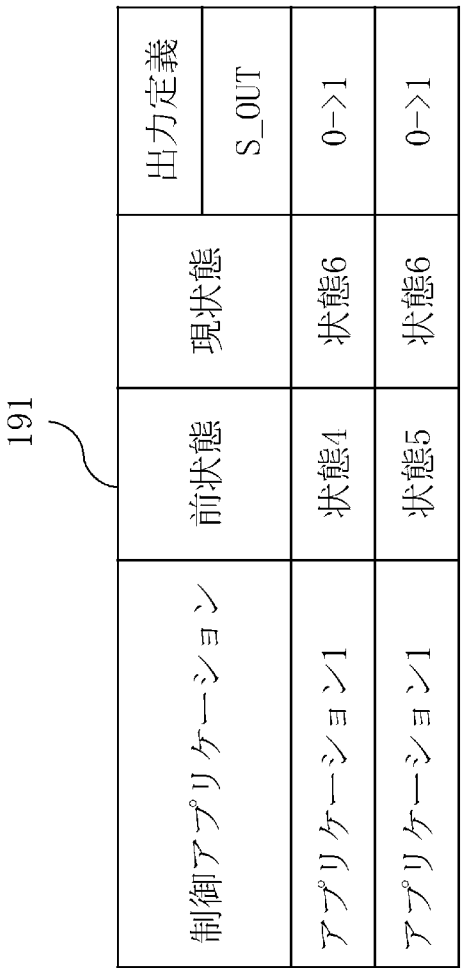
図13

194

シンボル	メモリアドレス
S_OUT	0x10000.bit0
S_Estop1	0x1001C.bit0
S_Estop2	0x1001C.bit1
デバイスA	0x10008.bit0
デバイスB	0x10008.bit1
デバイスC	0x10008.bit2

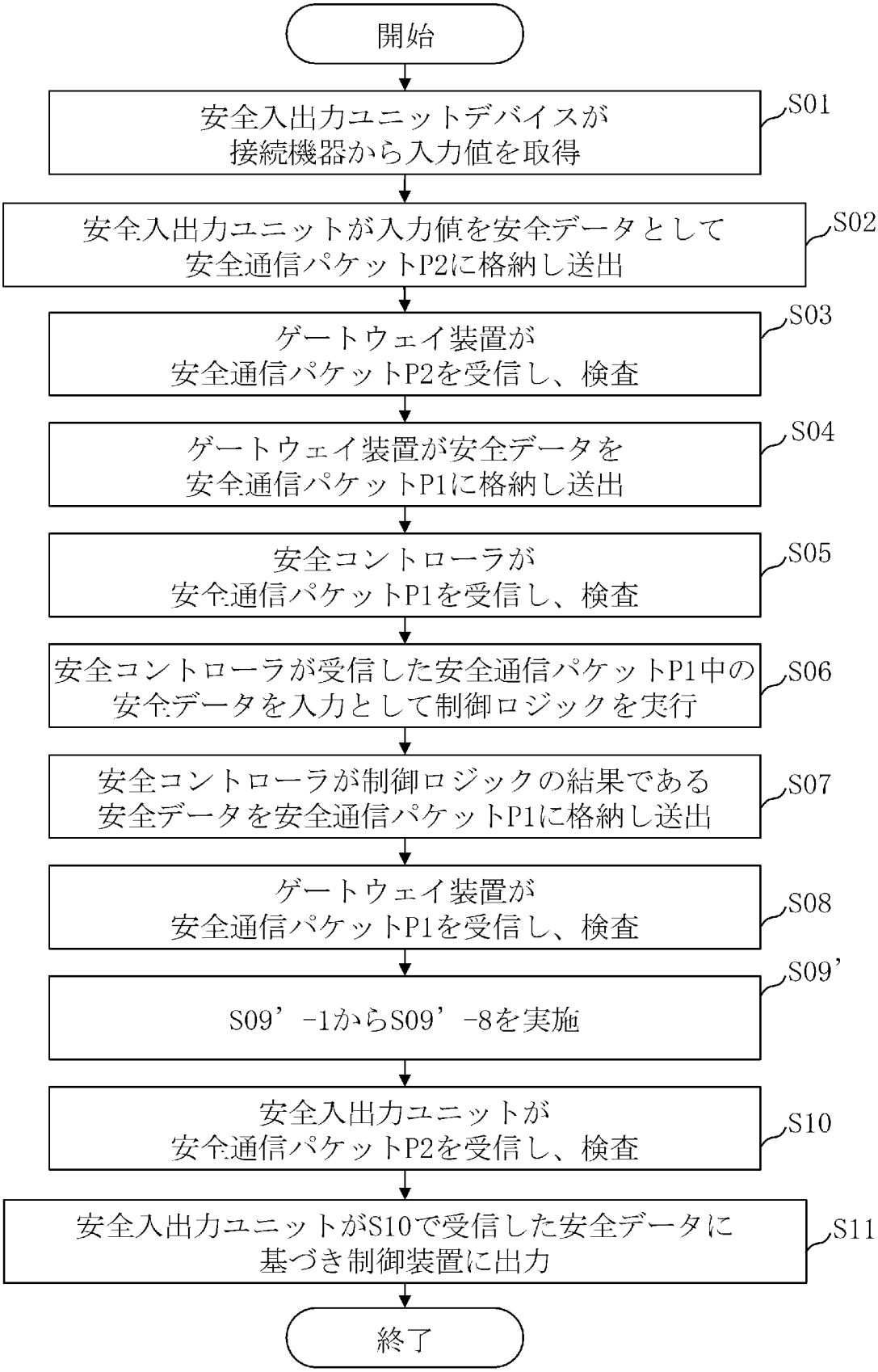
[図14]

図14


191
制御アプリケーション
前状態
現状態
出力定義
S_OUT
アプリケーション1
状態4
状態6
0->1
アプリケーション1
状態5
状態6
0->1

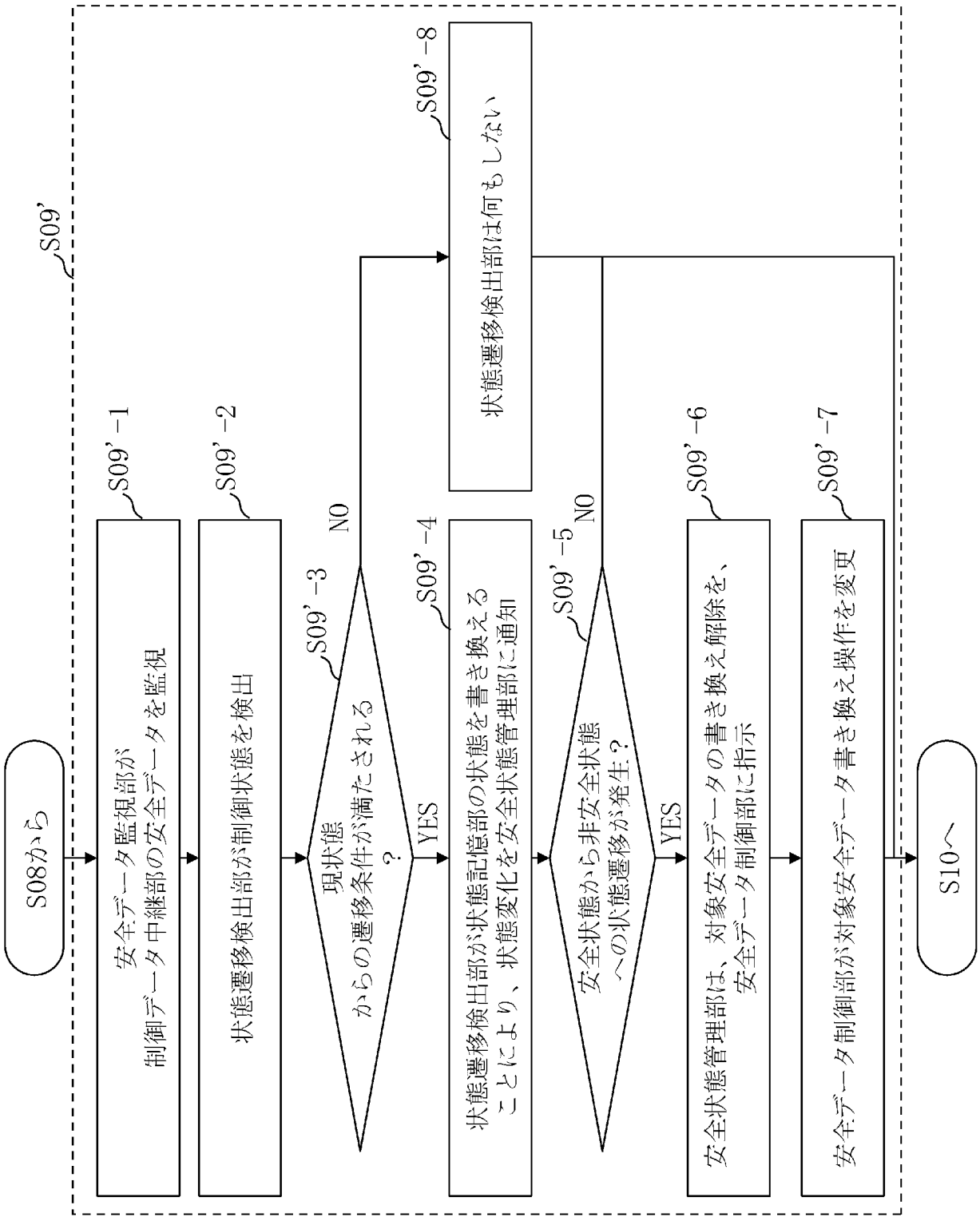
[図15]

図15


開始
安全入出力ユニットデバイスが
接続機器から入力値を取得
S01
安全入出力ユニットが入力値を安全データとして
安全通信パケットP2に格納し送出
S02
ゲートウェイ装置が
安全通信パケットP2を受信し、検査
S03
ゲートウェイ装置が安全データを
安全通信パケットP1に格納し送出
S04
安全コントローラが
安全通信パケットP1を受信し、検査
S05
安全コントローラが受信した安全通信パケットP1中の
安全データを入力として制御ロジックを実行
S06
安全コントローラが制御ロジックの結果である
安全データを安全通信パケットP1に格納し送出
S07
ゲートウェイ装置が
安全通信パケットP1を受信し、検査
S08
S09’-1からS09’-8を実施
S09’
安全入出力ユニットが
安全通信パケットP2を受信し、検査
S10
安全入出力ユニットがS10で受信した安全データに
基づき制御装置に出力
S11
終了

[図16]

図16


S09'
S08から
安全データ監視部が
制御データ中継部の安全データを監視
S09'-1
状態遷移検出部が制御状態を検出
S09'-2
現状態
からの遷移条件が満たされる
?
S09'-3
NO
YES
状態遷移検出部が状態記憶部の状態を書き換える
ことにより、状態変化を安全状態管理部に通知
S09'-4
安全状態から非安全状態
への状態遷移が発生?
S09'-5
NO
YES
状態遷移検出部は何もしない
S09'-8
安全状態管理部は、対象安全データの書き換え解除を、
安全データ制御部に指示
S09'-6
安全データ制御部が対象安全データ書き換え操作を変更
S09'-7
S10へ

[図17]

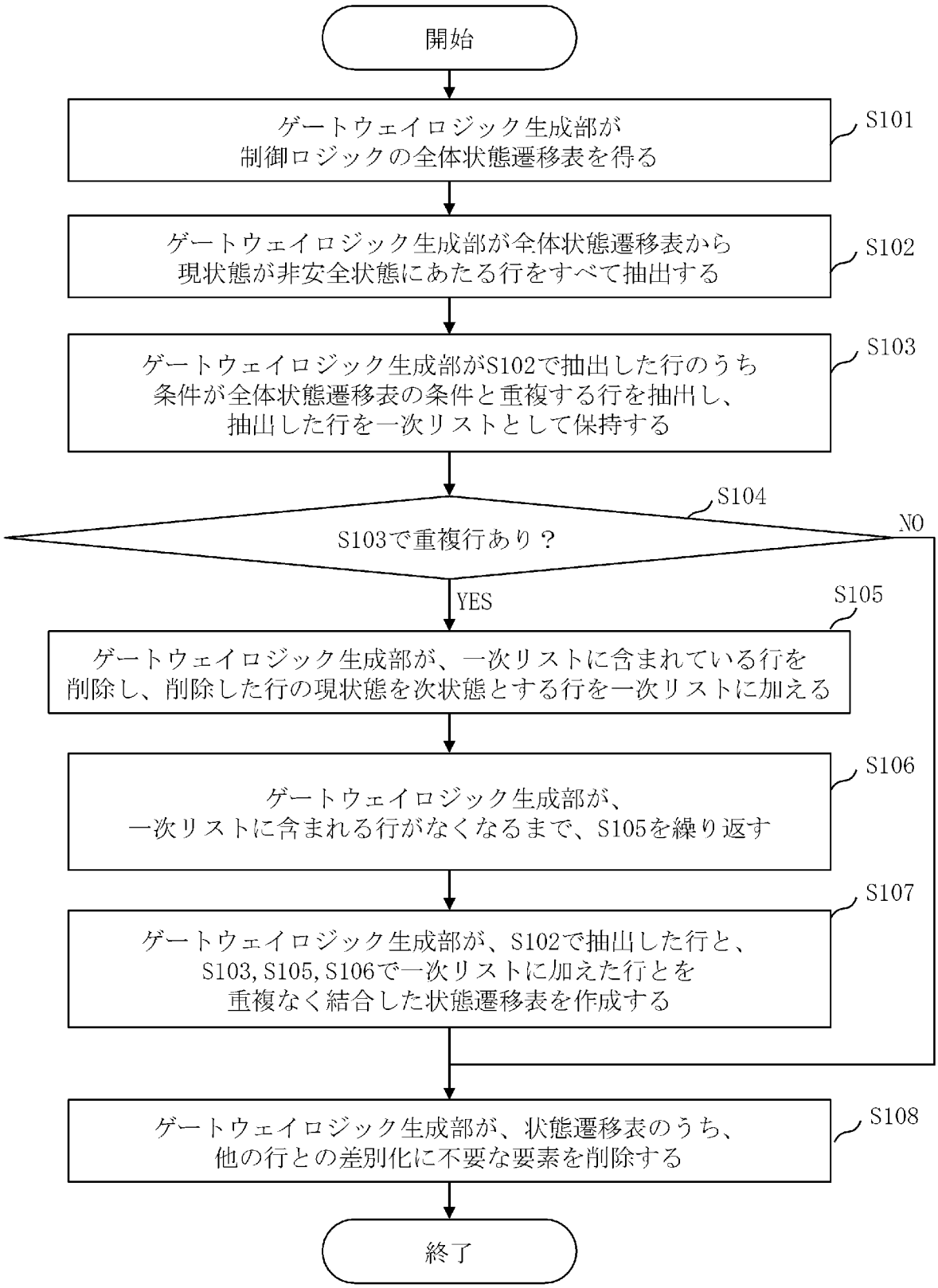
図17

192

通番	現状態	安全状態フラグ	出力値	条件				次状態
			S_OUT	状態	S_Estop1	S_Estop2	デバイスB	デバイスC	
7	状態4	非安全	1	条件5	−	−	1	−	状態5
8	状態4	非安全	1	条件6-A	1	−	−	−	状態6
9	状態5	非安全	1	条件4-C	−	−	−	1	状態4
10	状態5	非安全	1	条件6-B	−	1	−	−	状態6

[図18]

図18


開始
ゲートウェイロジック生成部が
制御ロジックの全体状態遷移表を得る
S101
ゲートウェイロジック生成部が全体状態遷移表から
現状態が非安全状態にあたる行をすべて抽出する
S102
ゲートウェイロジック生成部がS102で抽出した行のうち
条件が全体状態遷移表の条件と重複する行を抽出し、
抽出した行を一次リストとして保持する
S103
S104
S103で重複行あり？
NO
YES
S105
ゲートウェイロジック生成部が、一次リストに含まれている行を
削除し、削除した行の現状態を次状態とする行を一次リストに加える
S106
ゲートウェイロジック生成部が、
一次リストに含まれる行がなくなるまで、S105を繰り返す
S107
ゲートウェイロジック生成部が、S102で抽出した行と、
S103, S105, S106で一次リストに加えた行とを
重複なく結合した状態遷移表を作成する
S108
ゲートウェイロジック生成部が、状態遷移表のうち、
他の行との差別化に不要な要素を削除する
終了

[図19]

図19

通番	現状態	安全状態フラグ	出力値	条件					次状態
			S_OUT	状態	S_Estop1	S_Estop2	デバイスA	デバイスB	デバイスC	
1	(起動)	安全	0	条件0	–	–	–	–	–	状態0
2	状態0	安全	0	条件1-A	–	–	1	–	–	状態1
3	状態1	安全	0	条件2	–	–	–	0	1	状態2
4	状態1	安全	0	条件3	–	–	–	1	–	状態3
5	状態2	安全	0	条件4-A	–	–	–	1	–	状態4
6	状態3	安全	0	条件4-B	–	–	–	–	0	状態4
7	状態4	非安全	1	条件5	–	–	–	1	–	状態5
8	状態4	非安全	1	条件6-A	1	–	–	–	–	状態6
9	状態5	非安全	1	条件4-C	–	–	–	–	1	状態4
10	状態5	非安全	1	条件6-B	–	1	–	–	–	状態6
11	状態6	安全	0	条件1-B	–	–	–	–	–	状態1

[図20]

図20

通番	現状態	安全状態フラグ	出力値	条件					次状態
			S_OUT	状態	S_Estop1	S_Estop2	デバイスA	デバイスB	デバイスC	
7	状態4	非安全	1	条件5	−	−	−	1	−	状態5
8	状態4	非安全	1	条件6-A	1	−	−	−	−	状態6
9	状態5	非安全	1	条件4-C	−	−	−	−	1	状態4
10	状態5	非安全	1	条件6-B	−	1	−	−	−	状態6

[図21]

図21

通番	現状態	安全状態フラグ	出力値	条件					次状態
			S_OUT	状態	S_Estop1	S_Estop2	デバイスA	デバイスB	デバイスC	
3	状態1	安全	0	条件2	−	−	−	0	1	状態2
5	状態2	安全	0	条件4-A	−	−	−	1	−	状態4
6	状態3	安全	0	条件4-B	−	−	−	−	0	状態4
7	状態4	非安全	1	条件5	−	−	−	1	−	状態5
8	状態4	非安全	1	条件6-A	1	−	−	−	−	状態6
9	状態5	非安全	1	条件4-C	−	−	−	−	1	状態4
10	状態5	非安全	1	条件6-B	−	1	−	−	−	状態6

[図22]

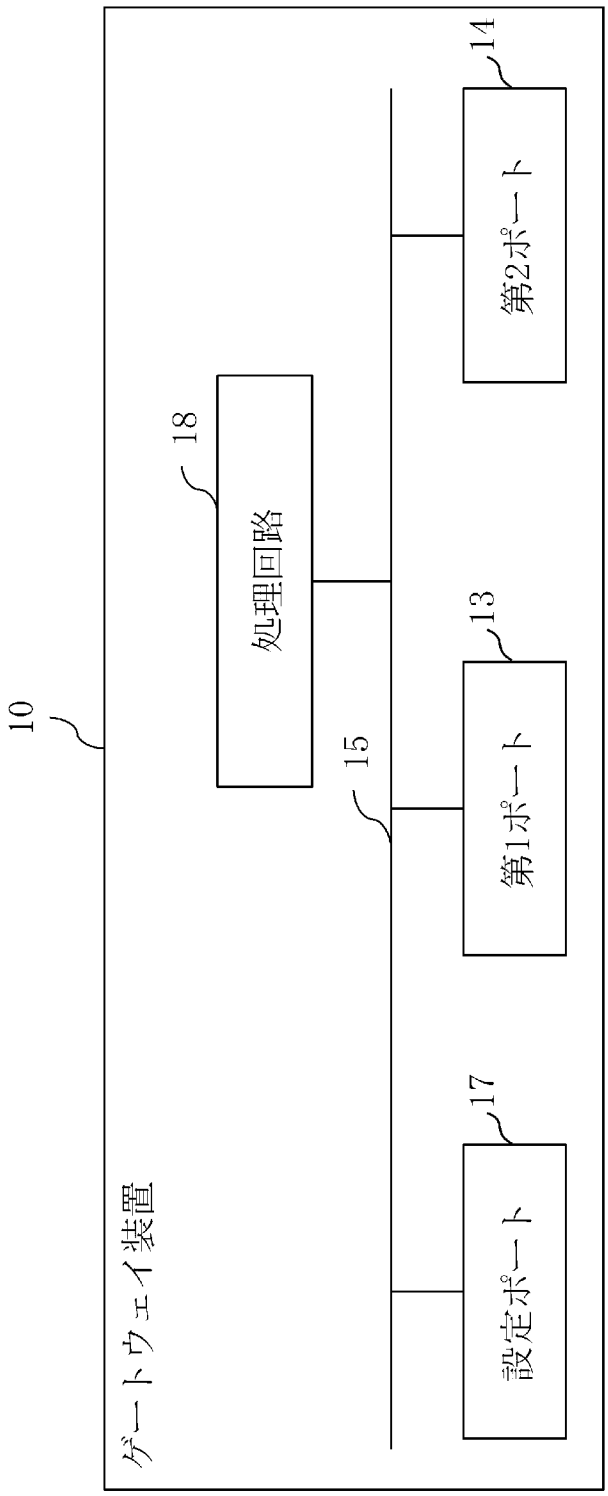
図22

191

制御アプリケーション	前状態	現状態	出力定義
			S_OUT
アプリケーション1	状態2	状態4	(書き換えを終了)
アプリケーション1	状態3	状態4	(書き換えを終了)

[図23]

図23



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2021/017904

A. CLASSIFICATION OF SUBJECT MATTER

G05B 23/02(2006.01)i; H04L 12/66(2006.01)i; H04L 12/70(2013.01)n; G05B 19/048(2006.01)i

FI: G05B19/048; H04L12/66 E; G05B23/02 302R; H04L12/70 100Z

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G05B23/02; H04L12/66; H04L12/70; G05B19/048

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2021
Registered utility model specifications of Japan	1996-2021
Published registered utility model applications of Japan	1994-2021

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2003/001306 A1 (OMRON CORPORATION) 03 January 2003 (2003-01-03) all pages	1-10
A	WO 2014/041829 A1 (MITSUBISHI ELECTRIC CORPORATION) 20 March 2014 (2014-03-20) all pages	1-10
A	JP 2015-100356 A (GROWTHMENT TECHNOLOGY CO LTD) 04 June 2015 (2015-06-04) all pages	1-10
A	CN 106911673 A (GLOBAL ENERGY INERCONNECTION RESEARCH INSTITUTE) 30 June 2017 (2017-06-30) all pages	1-10
A	JP 2008-507929 A (CITRIX SYSTEMS INC) 13 March 2008 (2008-03-13) all pages	1-10

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
07 July 2021 (07.07.2021)	20 July 2021 (20.07.2021)

Name and mailing address of the ISA/	Authorized officer
Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2021/017904

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
WO 2003/001306 A1	03 Jan. 2003	JP 3912378 B2	
		EP 1406134 A1	
WO 2014/041829 A1	20 Mar. 2014	US 2015/0220378 A1	
		CN 104641307 A	
JP 2015-100356 A	04 Jun. 2015	US 2015/0149617 A1	
		EP 2876893 A1	
		TW 201520947 A	
		CN 104656602 A	
CN 106911673 A	30 Jun. 2017	(Family: none)	
JP 2008-507929 A	13 Mar. 2008	US 2006/0029062 A1	
		WO 2006/012612 A1	
		EP 1853013 A1	
		KR 10-2007-0037648 A	

国際調査報告

国際出願番号
PCT/JP2021/017904

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

G05B 23/02(2006.01)i; H04L 12/66(2006.01)i; H04L 12/70(2013.01)n; G05B 19/048(2006.01)i
FI: G05B19/048; H04L12/66 E; G05B23/02 302R; H04L12/70 100Z

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

G05B23/02; H04L12/66; H04L12/70; G05B19/048

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０２１年
日本国実用新案登録公報	１９９６－２０２１年
日本国登録実用新案公報	１９９４－２０２１年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー*	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	WO 2003/001306 A1 (OMRON CORPORATION) 03.01.2003 (2003-01-03) 全ページ	1-10
A	WO 2014/041829 A1 (三菱電機株式会社) 20.03.2014 (2014-03-20) 全ページ	1-10
A	JP 2015-100356 A (生禾禾科技實業有限公司) 04.06.2015 (2015-06-04) 全ページ	1-10
A	CN 106911673 A (GLOBAL ENERGY INERCONNECTION RESEARCH INSTITUTE) 30.06.2017 (2017-06-30) 全ページ	1-10
A	JP 2008-507929 A (サイトリックス システムズ, インコーポレイテッド) 13.03.2008 (2008-03-13) 全ページ	1-10

☐ C欄の続きにも文献が列挙されている。

☑ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー
"A" 特に関連のある文献ではなく、一般的技術水準を示すもの
"E" 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
"L" 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
"O" 口頭による開示、使用、展示等に言及する文献
"P" 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
"T" 国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、発明の原理又は理論の理解のために引用するもの
"X" 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
"Y" 特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
"&" 同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
07.07.2021	20.07.2021

名称及びあて先
日本国特許庁(ISA/JP)
〒100-8915
日本国
東京都千代田区霞が関三丁目４番３号

権限のある職員（特許庁審査官）
松本　泰典 3U 3328
電話番号 03-3581-1101 内線 3364

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2021/017904

引用文献	公表日	パテントファミリー文献	公表日
WO 2003/001306 A1	03.01.2003	JP 3912378 B2	
		EP 1406134 A1	
WO 2014/041829 A1	20.03.2014	US 2015/0220378 A1	
		CN 104641307 A	
JP 2015-100356 A	04.06.2015	US 2015/0149617 A1	
		EP 2876893 A1	
		TW 201520947 A	
		CN 104656602 A	
CN 106911673 A	30.06.2017	（ファミリーなし）	
JP 2008-507929 A	13.03.2008	US 2006/0029062 A1	
		WO 2006/012612 A1	
		EP 1853013 A1	
		KR 10-2007-0037648 A	