

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2022-3543  
(P2022-3543A)

(43) 公開日 令和4年1月11日(2022.1.11)

(51) Int.Cl. F I テーマコード(参考)  
G05B 19/05 (2006.01) G05B 19/05 L 5H220

審査請求 有 請求項の数 20 O L 外国語出願 (全 38 頁)

(21) 出願番号	特願2021-148592 (P2021-148592)	(71) 出願人	514091080 ベドロック・オートメーション・プラットフォーム・インコーポレーテッド アメリカ合衆国カリフォルニア州95134, サンノゼ, リオ・ロブルズ 160
(22) 出願日	令和3年9月13日(2021.9.13)	(74) 代理人	100118902 弁理士 山本 修
(62) 分割の表示	特願2016-21763 (P2016-21763) の分割	(74) 代理人	100106208 弁理士 宮前 徹
原出願日	平成28年2月8日(2016.2.8)	(74) 代理人	100173565 弁理士 末松 亮太
(31) 優先権主張番号	62/114,030	(72) 発明者	クレイグ・マーコヴィック アメリカ合衆国カリフォルニア州95134, サンノゼ, リオ・ロブルズ 160
(32) 優先日	平成27年2月9日(2015.2.9)		
(33) 優先権主張国・地域又は機関	米国 (US)		
(31) 優先権主張番号	14/618,292		
(32) 優先日	平成27年2月10日(2015.2.10)		
(33) 優先権主張国・地域又は機関	米国 (US)		

最終頁に続く

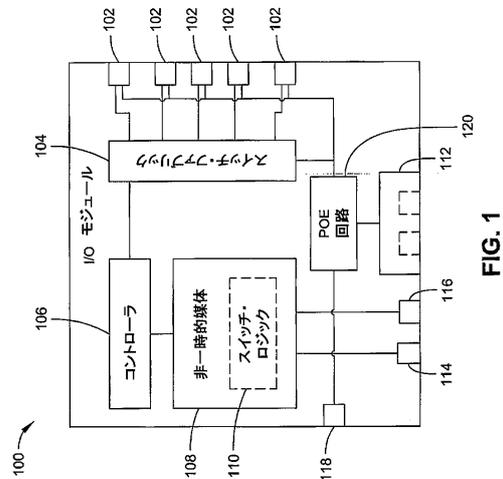
(54) 【発明の名称】 多チャンネル切り替え能力を有する入力/出力モジュール

(57) 【要約】 (修正有)

【課題】 ロバストで安全な入力/出力モジュールを備えた産業用通信および制御システムを提供する。

【解決手段】 入力/出力モジュールは、各チャンネルが1つ以上のフィールド・デバイスに接続するように構成される複数の通信チャンネルと、複数の通信チャンネルを通じて外部制御モジュールと1つ以上のフィールド・デバイスとの間における接続性を選択的に促進するように構成されたスイッチ・ファブリックと、入力/出力モジュールを制御モジュールに第2入力/出力モジュールと並列に接続するように構成されたシリアル通信ポートと、入力/出力モジュールを制御モジュールに別個に接続するように構成されたパラレル通信ポートであって、パラレル通信ポートが、入力/出力モジュールと制御モジュールとのあいだにおいて情報を送信し、入力/出力モジュールと第2入力/出力モジュールとの間において情報を送信するように構成される、パラレル通信ポートを含む。

【選択図】 図1



**【特許請求の範囲】****【請求項 1】**

制御システムであって、  
制御モジュールと、

該制御モジュールと結合された入力/出力モジュールであって、当該入力/出力モジュールが複数の通信チャネルを含み、該複数の通信チャネルの各チャネルが、1つ以上のフィールド・デバイスと接続するように構成され、前記入力/出力モジュールが、更に、前記複数の通信チャネルを通じて、前記制御モジュールと前記1つ以上のフィールド・デバイスとの間における接続性を選択的に促進するように構成されたスイッチ・ファブリックを含む、入力/出力モジュールと、

10

前記入力/出力モジュールを前記制御モジュールに接続するように構成されたシリアル通信インタフェースであって、前記シリアル通信インタフェースが、前記入力/出力モジュールを第2入力/出力モジュールと並列に接続し、前記シリアル通信インタフェースが、前記入力/出力モジュールと前記制御モジュールとの間において情報を送信するように構成される、シリアル通信インタフェースと、

前記入力/出力モジュールを前記制御モジュールに別個に接続するように構成されたパラレル通信インタフェースであって、当該パラレル通信インタフェースが、前記入力/出力モジュールと前記制御モジュールとの間において情報を送信し、前記入力/出力モジュールと前記第2入力/出力モジュールとの間において情報を送信するように構成される、パラレル通信インタフェースと

20

を備える、制御システム。

**【請求項 2】**

請求項1記載の制御システムにおいて、前記シリアル通信インタフェースがマルチドロップ・バスを含む、制御システム。

**【請求項 3】**

請求項1記載の制御システムにおいて、前記パラレル通信インタフェースがクロス・スイッチを備える、通信システム。

**【請求項 4】**

請求項1記載の制御システムにおいて、前記制御モジュールは、前記入力/出力モジュールが物理的に前記制御モジュールに接続される物理的位置に関連付けられた一意の識別子を、前記入力/出力モジュールに割り当てるように構成される、制御システム。

30

**【請求項 5】**

請求項1記載の制御システムにおいて、前記シリアル通信インタフェースが、前記入力/出力モジュールを冗長制御モジュールに並列に接続するように構成され、前記パラレル通信インタフェースが、前記入力/出力モジュールを前記冗長制御モジュールに別個に接続するように構成される、制御システム。

**【請求項 6】**

請求項1記載の制御システムであって、更に、電力を前記入力/出力モジュールに供給する電源モジュールを含む、制御システム。

**【請求項 7】**

請求項8記載の制御システムにおいて、前記入力/出力モジュールが、前記複数の通信チャネルのそれぞれのチャネルを通じて、電力を少なくとも1つのフィールド・デバイスに供給するように構成される、制御システム。

40

**【請求項 8】**

請求項1記載の制御システムにおいて、前記複数の通信チャネルが複数のイーサネット・チャネルを備える、制御システム。

**【請求項 9】**

請求項1記載の制御システムにおいて、前記入力/出力モジュールが、更に、前記スイッチ・ファブリックに結合されたコントローラを含み、該コントローラが、前記複数の通信チャネルのそれぞれのチャネル上で同時に起動する多数の通信規格に対応するように構

50

成され、前記通信規格が、イーサネット・バス、H1フィールド・バス、プロセス・フィールド・バス（PROFIBUS）、ハイウェイ・アドレスابل・リモート・トランスデューサ（HART）バス、Modbus、ならびにプロセス制御統一アーキテクチャ用オブジェクト連携および埋め込み（OPCUA）バスの内少なくとも2つを含む、制御システム。

【請求項10】

請求項1記載の制御システムにおいて、前記入力/出力モジュールが、プロセス制御統一アーキテクチャ用オブジェクト連携および埋め込み（OPCUA）クライアントまたはOPCUAサーバの内少なくとも1つとして動作可能である、制御システム。

【請求項11】

請求項1記載の制御システムにおいて、前記入力/出力モジュールが、IEEE1588タイミング・プロトコルにしたがって、1つ以上のフィールド・デバイスを同期させるように構成される、制御システム。

【請求項12】

請求項1記載の制御システムであって、更に、前記入力/出力モジュールと通信可能なデバイス寿命管理システムを含み、該デバイス寿命管理システムが前記1つ以上のフィールド・デバイスを認証するように構成される、制御システム。

【請求項13】

入力/出力モジュールであって、

複数の通信チャンネルであって、各チャンネルが1つ以上のフィールド・デバイスに接続するように構成される、複数の通信チャンネルと、

前記複数の通信チャンネルを通じて、外部制御モジュールと前記1つ以上のフィールド・デバイスとの間における接続性を選択的に促進するように構成されるスイッチ・ファブリックと、

前記入力/出力モジュールを前記制御モジュールに第2入力/出力モジュールと並列に接続するように構成されるシリアル通信ポートであって、前記入力/出力モジュールと前記制御モジュールとの間において情報を送信するように構成される、シリアル通信ポートと、

前記入力/出力モジュールを前記制御モジュールに別個に接続するように構成されたパラレル通信ポートであって、当該パラレル通信ポートが、前記入力/出力モジュールと前記制御モジュールとの間において情報を送信し、前記入力/出力モジュールと前記第2入力/出力モジュールとの間において情報を送信するように構成される、パラレル通信ポートを含む、入力/出力モジュール。

【請求項14】

請求項13記載の入力/出力モジュールにおいて、前記複数の通信チャンネルが複数のイーサネット・チャンネルを含む、入力/出力モジュール。

【請求項15】

請求項14記載の入力/出力モジュールにおいて、前記入力/出力モジュールが、前記複数のイーサネット・チャンネルのそれぞれのイーサネット・チャンネルを通じて、電力を少なくとも1つのフィールド・デバイスに供給するように構成される、入力/出力モジュール。

【請求項16】

請求項13記載の入力/出力モジュールであって、更に、前記スイッチ・ファブリックに結合されたコントローラを含み、前記コントローラが、前記複数の通信チャンネルのそれぞれのチャンネル上で同時に起動する多数の通信規格に対応するように構成され、前記通信規格が、イーサネット・バス、H1フィールド・バス、プロセス・フィールド・バス（PROFIBUS）、ハイウェイ・アドレスابل・リモート・トランスデューサ（HART）バス、Modbus、ならびにプロセス制御統一アーキテクチャ用オブジェクト連携および埋め込み（OPCUA）バスの内少なくとも2つを含む、入力/出力モジュール。

【請求項17】

10

20

30

40

50

請求項 13 記載の入力 / 出力モジュールにおいて、前記コントローラが、プロセス制御統一アーキテクチャ用オブジェクト連携および埋め込み (OPCUA) クライアント通信 / 制御プロトコル、または OPC UA サーバ通信 / 制御プロトコルの内少なくとも 1 つとして起動するように構成される、入力 / 出力モジュール。

【請求項 18】

請求項 13 記載の入力 / 出力モジュールにおいて、前記シリアル通信ポートまたは前記パラレル通信ポートの内少なくとも 1 つが、第 1 磁気回路部分を形成する電磁コネクタを備え、該電磁コネクタが、

第 1 コア部材と、

前記第 1 コア部材に配置された第 1 コイルと、

を含み、

前記電磁コネクタが第 2 電磁コネクタと嵌合するように構成され、前記第 2 電磁コネクタが第 2 磁気回路部分を形成するように構成され、第 2 コア部材と前記第 2 コア部材に配置された第 2 コイルとを備え、前記第 1 コア部材および前記第 2 コア部材が前記第 1 コイルを前記第 2 コイルに結合するように構成され、前記電磁コネクタが前記第 2 電磁コネクタと嵌合されたとき、前記第 1 磁気回路部分および前記第 2 磁気回路部分によって磁気回路が形成され、前記磁気回路が、前記第 2 コイルが付勢されたときに、前記第 1 コイル内に信号を誘導するように構成される、入力 / 出力モジュール。

【請求項 19】

請求項 18 記載の入力 / 出力モジュールにおいて、前記第 1 コイルが、印刷回路ボードに配置された平面巻線を備える、入力 / 出力モジュール。

【請求項 20】

請求項 18 記載の入力 / 出力モジュールにおいて、前記第 1 コア部材が E 字型コア部材を含む、入力 / 出力モジュール。

【請求項 21】

請求項 18 記載の入力 / 出力モジュールにおいて、前記第 1 コア部材および前記第 2 コア部材によって形成された前記磁気回路がエア・ギャップを含む、入力 / 出力モジュール。

【発明の詳細な説明】

【技術分野】

【0001】

関連出願に対する相互引用

[0001] 本願は、2015年2月9日に出願され“INPUT/OUTPUT MODULE WITH MULTI-CHANNEL SWITCHING CAPABILITY”と題する米国仮特許出願第62/114,030号に対して、35 U.S.C. § 119(e)に基づく優先権を主張する。また、本願は、2013年8月6日に出願され“SECURE INDUSTRIAL CONTROL SYSTEM”と題する国際出願PCT/US2013/053721号の一部継続出願である。また、本願は、2014年8月27日に出願され“SECURE INDUSTRIAL CONTROL SYSTEM”と題する米国特許第14/469,931号の35 U.S.C. § 120に基づく一部継続出願である。また、本願は、2014年7月30日に出願され“INDUSTRIAL CONTROL SYSTEM CABLE”と題する米国特許出願第14/446,412号の35 U.S.C. § 120に基づく一部継続出願であり、米国特許出願第14/446,412号は、2014年7月7日に出願され“INDUSTRIAL CONTROL SYSTEM CABLE”と題する米国仮特許出願第62/021,438号に対して、35 U.S.C. § 119(e)に基づく優先権を主張する。また、本願は、2014年10月20日に出願され“OPERATOR ACTION AUTHENTICATION IN AN INDUSTRIAL CONTROL SYSTEM”と題する米国特許出願第14/519,066号の35 U.S.C. § 120に基づく一部継続出願である。また、本願は、2014年10月20日に出願され“INDUSTRIAL CONTROL SYSTEM REDUNDANT COMMUNICATIONS/CONTROL MODULES AUTHENTICATION”と題する米国特許出願第14/519,047号の35 U.S.C. § 120に基づく一部継続出願である。また、本願は、2015年1月15日に出願され“ELECTROMAGNETIC CONNECTOR”と題する米国特許出願第14/597

10

20

30

40

50

、498号の35 U.S.C. §120に基づく一部継続出願であり、米国特許出願第14/597,498号は、2011年12月30日に出願され“ELECTROMAGNETIC CONNECTOR”と題する米国特許出願第13/341,143号の35 U.S.C. §120に基づく継続出願である。また、本願は、2012年12月28日に出願され(2011年12月30日の優先日を有する)“ELECTROMAGNETIC CONNECTOR AND COMMUNICATIONS/CONTROL SYSTEM/SWITCH FABRIC WITH SERIAL AND PARALLEL COMMUNICATIONS INTERFACES”と題する国際出願PCT/US2012/072056号の一部継続出願である。また、本願は、2014年9月30日に出願され“SWITCH FABRIC HAVING A SERIAL COMMUNICATIONS INTERFACE AND A PARALLEL COMMUNICATIONS INTERFACE”と題する米国特許出願第14/501,974号の35 U.S.C. §120に基づく一部継続出願であり、米国特許出願第14/501,974号は、2011年12月30日に出願され“SWITCH FABRIC HAVING A SERIAL COMMUNICATIONS INTERFACE AND A PARALLEL COMMUNICATIONS INTERFACE”と題する米国特許出願第13/341,161号の35 U.S.C. §120に基づく継続出願である。また、本願は、2014年9月30日に出願され“COMMUNICATIONS CONTROL SYSTEM WITH A SERIAL COMMUNICATIONS INTERFACE AND A PARALLEL COMMUNICATIONS INTERFACE”と題する米国特許出願第14/502,006号の35 U.S.C. §120に基づく一部継続出願であり、米国特許出願第14/502,006号は、2011年12月30日に出願され“COMMUNICATIONS CONTROL SYSTEM WITH A SERIAL COMMUNICATIONS INTERFACE AND A PARALLEL COMMUNICATIONS INTERFACE”と題する米国特許出願第13/341,176号の35 U.S.C. §120に基づく継続出願である。

10

20

#### 【0002】

[0002] 以上で相互引用した特許出願の各々は、ここで引用したことにより、その内容全体が本願にも含まれるものとする。

#### 【背景技術】

#### 【0003】

[0003] 標準的な産業用制御システム(ICS)またはプロム可能自動コントローラ(PAC)のような産業用制御システムは、監視制御およびデータ取得(SCADA)システム、分散型制御システム(DCS)、プログラム可能ロジック・コントローラ(PLC)、およびIEC1508のような安全規格に対して証明された産業用安全システムというように、工業生産において使用される種々のタイプの制御機器を含む。これらのシステムは、電気、給水および排水、石油およびガス生産ならびに精製、化学、食品、薬品、およびロボットを含む産業において使用される。プロセス変数を測定するために種々のタイプのセンサから収集された情報を使用することにより、自動化されたおよび/または操作員によって送り出される産業用制御システムからの監視コマンドを、制御弁、油圧アクチュエータ、磁気アクチュエータ、電気スイッチ、モータ、ソレノイド等のような、種々のアクチュエータ・デバイスに送信することができる。これらのアクチュエータ・デバイスは、センサおよびセンサ・システムからデータを収集し、弁および遮断器を開閉し、弁およびモータを規制し、産業用プロセスの警報条件を監視する等を行う。

30

#### 【0004】

[0004] 他の例では、SCADAシステムは、地理的に広く離れているかもしれないプロセス・サイトでオープン・ループ制御を使用することができる。これらのシステムは、監視データを1つ以上の制御センターに送るために遠隔端末ユニット(RTU)を使用する。RTUを展開するSCADAの用途には、流体パイプライン、配電、および大規模通信システムが含まれる。DCSシステムは、通常、高帯域幅低レイテンシ・データ・ネットワークとのリアル・タイム・データ収集および連続制御に使用され、石油およびガス、精製、化学、薬品、食品および飲料水、給水および排水、パルプおよび紙、外部電力、ならびに鉱業および金属のような、大規模な(large campus)産業用プロセス・プラントにおいて使用される。更に典型的には、PLCはプールおよびシーケンス・ロジック演算、タイマ、ならびに連続制御を可能とし、多くの場合単体の機械類およびロボットにおいて使用される。更に、ICEおよびPACシステムは、建物、空港、船舶、宇宙ステーション

40

50

等（例えば、過熱、換気、および空調（HVAC）機器およびエネルギー消費を監視し制御するため）のための設備プロセスにおいて使用することができる。産業用制御システムが発展するに連れて、新たな技術がこれら種々のタイプの制御システムの態様を結合させつつある。例えば、PACは、SCADA、DCS、およびPLCの態様を含むことができる。

【発明の概要】

【発明が解決しようとする課題】

【0005】

【0005】 産業用制御システム内部では、通信/制御モジュールがフィールド・デバイス（例えば、アクチュエータ、センサ等）と入力/出力モジュールを介して通信するのが通例である。技術的進歩によって、フィールド・デバイス間の接続性強化の要求、更に高いレベルの企業および産業用システムの要求が生じ、デバイス自体間の接続性が増々求められることとなった。これに関して、産業用システムは、「もののインターネット (internet of things)」と同様に発展しつつあるが、安全性、信頼性、およびスループットに対する要求は遙かに高い。産業用通信および制御システムにおいて生まれつつある要望に答えるためには、ロバストで安全な入力/出力モジュールが必要とされる。

10

【課題を解決するための手段】

【0006】

【0006】 本開示は、多チャンネル切り替え能力を有する入力/出力モジュールを対象とし、これは産業用制御システムの通信バックプレーン内部に安全に埋め込むことができる。ある実施形態では、この入力/出力モジュールは、複数の通信チャンネルを含み、これらのチャンネルの各々は、1つ以上のフィールド・デバイスに接続するように構成される。この入力/出力モジュール内にあるスイッチ・ファブリックが、選択的に、外部制御モジュールと1つ以上のフィールド・デバイスとの間の接続性を、通信チャンネルによって促進する。通信バックプレーンによって相互接続を容易にするために、入力/出力モジュールは、更に、シリアル通信ポートおよびパラレル通信ポートを含むことができる。シリアル通信ポートは、入力/出力モジュールを制御モジュールに、少なくとも1つの追加の（第2）入力/出力モジュールと並列に接続することができ、シリアル通信ポートは入力/出力モジュールと制御モジュールとの間で情報を送信する。パラレル通信ポートは、入力/出力モジュールを制御モジュールに別個に接続することができ、パラレル通信ポートは、入力/出力モジュールと制御モジュールとの間で情報を送信し、更に入力/出力モジュールと第2入力/出力モジュールとの間でも情報を送信する。

20

30

【0007】

【0007】 この摘要は、詳細な説明において以下で更に説明する概念から選択したものを、簡略化した形態で紹介するために設けられている。この摘要は、特許請求する主題の主要な特徴や必須の特徴を特定することを意図するのではなく、特許請求する主題の範囲を判断するときに補助として使用されることを意図するのでもない。

【0008】

【0008】 添付図面を参照しながら詳細な説明について記載する。説明および図における異なる実例において同じ参照番号を使用する場合、同様の項目または同一の項目を示すことができる。

40

【図面の簡単な説明】

【0009】

【図1】 図1は、本開示の実施形態による入力/出力モジュールを示すブロック図である。

【図2】 図2は、本開示の実施形態による産業用制御システムを示すブロック図である。

【図3】 図3は、本開示の実施形態によるスイッチ・ファブリックを示すブロック図である。

【図4】 図4は、本開示の実施形態による産業用制御システムを示す等幅図である。

【図5】 図5は、図4に示した産業用制御システムの支持フレームに結合された入力/出

50

カモジュールの等幅図である。

【図6】図6は、図4に示した入力/出力モジュールの等幅図である。

【図7】図7は、図4に示した入力/出力モジュールの側面図である。

【図8】図8は、図4に示した入力/出力モジュールおよび産業用制御システムの支持フレームの側断面図である。

【図9】図9は、図4に示した産業用制御システムのための付属回路ボードを有する支持フレームの等幅図である。

【図10】図10は、本開示の実施形態による産業用制御システムに対するアクション認証パスを示すブロック図である。

【図11】図11は、本開示の実施形態による、図10に示したアクション認証パスを更に示すブロック図である。

【図12】図12は、図10または図11において示したアクション認証パスのような、アクション認証パスによってアクション要求を認証するプロセスの一例を示す流れ図である。

【図13】図13は、本開示の実施形態にしたがって、第2入力/出力モジュールと認証シーケンスを実行する第1入力/出力モジュールを示すブロック図である。

【図14】図14は、第2入力/出力モジュールと認証する第1入力/出力モジュールによって実行される認証シーケンスの一例を示す流れ図である。

【図15】図15は、第1入力/出力モジュールによって実行される認証シーケンス（例えば、図14に示すような）に回答して、第2入力/出力モジュールによって実行される応答認証シーケンスの一例を示す流れ図である。

【発明を実施するための形態】

【0010】

#### 概要

[0024] 産業用制御システムにおいて通信/制御モジュールとフィールド・デバイス（例えば、アクチュエータ、センサ等）との間で通信を行うために、入力/出力（I/O）モジュールが使用される。技術的進歩によって、フィールド・デバイス間の接続性強化の要求、更に高いレベルの企業および産業用システムの要求が生じ、フィールド・デバイス自体間の接続性が増々求められることとなった。これに関して、産業用システムは、「もののインターネット」と同様に発展しつつあるが、安全性、信頼性、およびスループットに対する要求は遙かに高い。とりわけ、TCP/IP通信プロトコルを安全に促進するために、多ポート・スイッチを使用することができる。しかしながら、スイッチ（例えば、多ポート・イーサネット・スイッチ）は、通例、産業用制御システムの通信バックプレーンの外側に位置しており、その結果安全性の脅威を一層受け易くなる可能性があり、スイッチを介して産業用制御システムに通信可能に結合されたデバイスを危険に晒すおそれがあり、産業用制御システム全体を危険な状態に置く潜在性がある。

【0011】

[0025] 多チャンネル切り替え能力を有するI/Oモジュールについて開示する。このI/Oモジュールは、産業用制御システムの通信バックプレーン内に安全に埋め込まれるように構成される。ある実施形態では、入力/出力モジュールは、イーサネット・バス、H1フィールド・バス、プロセス・フィールド・バス（PROFIBUS）、ハイウェイ・アドレスابل・リモート・トランスデューサ（HART）バス、Modbus、ならびにプロセス制御統一アーキテクチャ（OPCUA）用オブジェクト連結および埋め込み通信規格というような、しかしこれらには限定されない、種々の通信プロトコルに対応する（accommodate）ように構成することができる複数の通信チャンネルを含む。ある実施形態では、2つ以上の全く異なる通信規格を同時に通信チャンネルのそれぞれにおいて実行することができる。例えば、第1チャンネルがOPCUAプロトコルを起動し（run）、一方で第2チャンネルがPROFIBUSを実行している等であってもよい。

【0012】

#### 例示の実装態様

10

20

30

40

50

[0026] 図1は、本開示の実施形態によるI/Oモジュール100を示す。I/Oモジュール100は、イーサネット・チャンネル等のような、複数の通信チャンネル102を含むことができる。通信チャンネル102は、図2に示し以下で更に詳しく説明する産業用制御システム200のような、分散型制御システム内にあるフィールド・デバイスに接続するために使用することができる。例えば、これら複数の通信チャンネルの内各チャンネルは、アクチュエータ・デバイス218およびセンサ・デバイス220のような、1つ以上のフィールド・デバイス217に接続するように構成することができる。限定するのではないが、アクチュエータ・デバイス218およびセンサ・デバイス220には、制御弁、油圧アクチュエータ、磁気アクチュエータ、モータ、ソレノイド、電気スイッチ、送信機、入力センサ/受信機(例えば、照明、放射線、ガス、温度、電気、磁気、および/または音響センサ)、通信サブバス等が含まれる。I/Oモジュール内にあるスイッチ・ファブリック104は、外部制御モジュール(例えば、通信/制御モジュール214)と1つ以上のフィールド・デバイス217との間における接続性(例えば、情報/データの転送)を、複数の通信チャンネル102によって選択的に促進するように構成することができる。

10

#### 【0013】

[0027] 実施形態では、I/Oモジュール100は、マイクロプロセッサ、マイクロコントローラ、ASIC、FPGA、あるいは他の単一または多重コア処理ユニットのような、スイッチ・ファブリック104を制御するように構成されたコントローラ106を含む。例えば、コントローラ106は、スイッチ・ファブリック等に対して調停規則または優先順位を設定するように構成することができる。コントローラ106は、コントローラ106に通信可能に結合された非一時的媒体108(例えば、フラッシュまたはソリッド・ステート・メモリ・デバイス)からスイッチ・ファブリック104を制御するためのスイッチ・ロジック110(例えば、プログラム命令)を起動する/実行する(run/execute)ように構成されてもよい。ある実施形態では、I/Oモジュール100は、OPCUAクライアントおよび/またはサーバとして動作可能である。例えば、コントローラ106は、コントローラ106にOPCUAクライアントまたはサーバ通信/制御プロトコルを実装させるスイッチ・ロジック110を走らせる/実行するように構成することができる。

20

#### 【0014】

[0028] ある実施形態では、コントローラ106はそれぞれのチャンネル102上において同時に実行する多数の通信規格に対応するように構成される。例えば、第1チャンネル102がコントローラ106によってPROFIBUSプロトコルを利用して情報を送信および受信するように構成されることが可能であり、第2の同時に動作可能なチャンネル102が、コントローラ106によって、OPCUAプロトコルを利用して情報を送信および受信するように構成されることが可能である。一般に、2つ以上の通信規格をそれぞれのチャンネル102によって同時に実施することができ、通信規格は、イーサネット・バス、H1フィールド・バス、PROFIBUS、HARTバス、Modbus、およびOPCUA通信規格を含むことができるが、これらに限定されるのではない。

30

#### 【0015】

[0029] 更に、I/Oモジュール100は、IEEE1588高精度時間プロトコル(PTP)のようなタイミング・プロトコルにしたがって、接続されたフィールド・デバイス217のタイミングを同期させるように構成することができる。これに関して、I/Oモジュール100は、時間分布システムを実装することができ、I/Oモジュール100が同期マスタ・デバイスまたは中間同期デバイスとなり、フィールド・デバイス217は、タイミング制御階層においてI/Oモジュール100よりも低くなる。

40

#### 【0016】

[0030] 通信チャンネル102を通じてフィールド・デバイス217への接続性(connectivity)を策定することに加えて、I/Oモジュール100は、更に、電力をフィールド・デバイス217に供給するように構成することができる。ある実施形態では、例えば、I/Oモジュール100はイーサネット経由給電(POE)回路120を含み、この回路は

50

受電した電力を通信チャンネル102の内1つ以上に配給するように構成される。電力は、電力バックプレーン接続ポート112（例えば、E-コア接続ポート）または入力ジャック118を介してI/Oモジュールに供給されてもよい。例えば、入力ジャック118が外部電源（例えば、ローカル発電機、バックアップ電源等）に結合されてもよい。実施形態では、コントローラ106は、通信チャンネル102を通じた電力転送を選択的に可能にするように構成することができる。例えば、P/E能力を有するフィールド・デバイス217（例えば、低電圧アクチュエータ218、センサ220、または通信デバイス）に結合された通信チャンネル102のために、P/E機能を使用可能にすることができる。デバイス217が他の電源（例えば、電力バックプレーン234、内部/外部バッテリー、または他の内部/外部電源への接続）によって給電されるように構成される場合、コントローラ106は、デバイス217と結合されたそれぞれの通信チャンネル102のP/E機能を使用不可にするように構成することができる。

10

20

30

40

50

**【0017】**

[0031] 更に、I/Oモジュール100は、通信バックプレーン（例えば、スイッチ・ファブリック202）を介した少なくとも1つの通信/制御モジュール214との相互接続性(interconnectivity)を促進する1つ以上の接続ポート（例えば、E-コア接続ポート）も含む。ある実施形態では、I/Oモジュール100は少なくとも1つのシリアル通信ポート114および少なくとも1つのパラレル通信ポート116を含む。シリアル通信ポート114は、I/Oモジュール100を通信/制御モジュール214に、少なくとも1つの追加の（第2）I/Oモジュール100と並列に接続することができる。例えば、第1および第2I/Oモジュール100を同時に通信/制御モジュール214に、それぞれのシリアル・インタフェース接続204を介して接続することができ、この場合各I/Oモジュール100は、それぞれのシリアル・インタフェース204を介して、情報を通信/制御モジュール214から受信し、情報を通信/制御モジュール214に送信することができる。パラレル通信ポート116は、別個にI/Oモジュール100を通信/制御モジュール214に、パラレル通信インタフェース206を介して接続することができ、この場合I/Oモジュール100は、パラレル通信インタフェース206を介して、情報を通信/制御モジュール214から受信し、情報を通信/制御モジュール214に送信することができる。また、I/Oモジュール100は、パラレル通信ポート116およびインタフェース206を介して、他のI/Oモジュール100と通信することもできる。

**【0018】**

[0032] 実施形態では、I/Oモジュールの1つ以上のポート（例えば、シリアル通信ポート114、パラレル通信ポート116、電力バックプレーン入力112、および/または入力ジャック118）は、米国特許出願第13/341,143号（公開US2013/0170258）および第14/597,498号、ならびに国際出願PCT/US2012/072056（国際公開WO/2013/102069）において記載されているような、コネクタ・アセンブリ208の電磁コネクタ207を含む、または電磁コネクタ207に結合される。これらの特許出願をここで引用したことにより、その内容全体が本願にも含まれるものとする。電磁コネクタ207は、電気信号および/または電力を回路間で送信しつつ、これらの回路間で絶縁を維持するために電気回路を互いに結合することが望ましい用途であればいずれにでも使用することができる。電磁コネクタ207は、以下を含む用途において使用することができるが、必ずしもこれらに限定されるのではない。産業用制御システム/プロセス制御システム（例えば、I/Oモジュール100を電力および/または通信信号送信回路に接続するため）、電気通信（例えば、オーディオ、高帯域、ビデオ、および/または音声送信のため）、情報/データ通信（例えば、イーサネット機器、モデム等のようなコンピュータ・ネットワーク機器を接続するため）、コンピュータ・ハードウェア相互接続（例えば、ジョイスティック、キーボード、マウス、モニタ等のような周辺機器を接続するため）、ゲーム・コンソール、検査/測定計器、電力コネクタ（例えば、AC主電力(mains)からの電力送信のため）等。

**【0019】**

[0033] 電磁コネクタ207のそれぞれのもの(each one)は、磁気回路部分を形成するように構成され、コア部材と、このコア部材に取り付けられた(例えば、周囲または内部に)コイルとを含む。本開示に限って言えば、「コア部材」は、磁気コアの不完全な部分を指すために使用され、電磁コネクタ207と一緒に結合されるときに、他のコア部材によって完成されることは注記してしかるべきである。各電磁コネクタ207は、電磁コネクタ207を介して接続されたコンポーネント間で電力および/または通信信号を送信するために、コネクタ・アセンブリ208の他の電磁コネクタ207と嵌合するように構成される。例えば、電磁コネクタ207の第1コア部材は、第1電磁コネクタ207が第2電磁コネクタ207と嵌合されるときに、他の電磁コネクタ207の第2コア部材と接触するように構成することができる。このように、第1電磁コネクタ207のコイルを第2電磁コネクタ207の他のコイルに緊密に結合することができ、第1電磁コネクタ207の磁気回路部分および第2電磁コネクタ207の磁気回路部分によって、磁気回路が形成される。この磁気回路は、これらのコイルの一方が付勢されると、他方のコイルに信号を誘導するように構成され、電磁コネクタ207を介して接続されたコンポーネント間において電力および/または通信信号を送信することを可能にする。実装態様では、コイルを緊密に結合すること(例えば、約1の結合係数を得るために鉄製コアを使用する)、厳密に(critically)結合すること(例えば、通過帯域におけるエネルギー転送が最適である)、または過剰結合すること(例えば、二次コイルが一次コイルに非常に近いために一次コイルの磁場を崩す)が可能である。

10

20

**【0020】**

[0034] 第1コア部材は、第1電磁コネクタ207が第2電磁コネクタ207と嵌合するとき、必ずしも第2コア部材に接触するように構成されなくてもよい。つまり、電磁コネクタ・アセンブリ208は、例えば、絞りばめ構成を使用して電磁コネクタ207を介して接続されたコンポーネント間において、電力および/または通信信号を送信するように構成することができる。この場合、一方のコイルが第1コイル部材の周囲に配され、他方のコイルが第2コア部材の内部に配される。絞りばめは、円錐形、同心状、偏心状、幾何学的外形、摺り合わせのための傾斜付き等を含むがこれらに限定されない外形を有するコネクタを使用して固めるのもよい(establish)。

**【0021】**

[0035] 実装態様では、コア部材および/またはコイルの一方または両方を、保護層内に少なくとも部分的に(例えば、完全にまたは部分的に)機械的に包み込むことができる。保護層は、薄膜プラスチック材のコーティングのような、非導電性/絶縁材で製作されるとよい。保護層(例えば、非導電性/絶縁材)は、被覆、塗装、堆積等を含むがこれらに限定されない技法を使用して被着することができる。例えば、I/Oモジュール100内部に含まれる第1電磁コネクタ207のコア部材およびコイルを部分的にカバーで包囲することができ、一方電力または通信バックプレーン202/234内部に含まれる第2電磁コネクタ207は、このカバーと嵌合するように構成されたシャフトを含むのもよい。このように、カバーおよびシャフトは、第1電磁コネクタ207のコア部材および/またはコイルを腐食、機械的損傷(例えば、破碎)などから保護しつつ、第1電磁コネクタ207の第2電磁コネクタ207との適正な整列(alignment)を確保するように構成することができる。外装(encasement)は、コア部材が脆弱な材料で作られるときに特に有用であると考えられる。例えば、プラスチック材で形成された保護層内に、コア部材を緊密に包み込むことができる。このように、コア部材に損傷が発生したとき(例えば、コア部材におけるひびまたは破断)、外装の内部に材料の破片を実質的に互いに接触した状態で維持することができ、したがってコア材料に対する損傷が動作性能(performance)を著しく低下させないで済む。

30

40

**【0022】**

[0036] 電磁コネクタ207同士が嵌合されるとき、電力または通信バックプレーン202/234のコア部材、およびI/Oモジュール100のコア部材が磁気回路によってコイルを結合するように構成されるのもよい。磁気回路は、電力または通信バックプレ

50

ーン202/234のそれぞれのコイルが付勢されたときに（例えば、DC/AC変換器からのAC信号によって）、I/Oモジュール100のコイルに信号を誘導することができる。I/Oモジュール100のコイル内に誘導される信号は、モジュール100の回路に給電するため、および/またはモジュール100の回路との通信を行うために使用することもできる。尚、電力または通信バックプレーン202/234は、I/Oモジュール100内に信号を誘導すると説明したが、この実装態様は一例として挙げたに過ぎず、本開示を限定することを意味するのではないことは注記してしかるべきである。また、磁気回路は、I/Oモジュール100のコイルが付勢されたときに、電力または通信バックプレーン202/234のコイル内に信号を誘導して、電力または通信バックプレーン202/234に給電するため、および/または電力または通信バックプレーン202/234との通信を行うために使用することもできる（例えば、スイッチ・ファブリック202を介した通信/制御モジュール214への通信の送信）。更に、嵌合する電磁コネクタ207と共に含まれるコイルは、双方向通信等を行うために、交互シーケンス（例えば、次から次に）で付勢されてもよい。

10

20

30

40

50

#### 【0023】

[0037] 図2から図9は、本開示の種々の実施形態による産業用制御システム200を示す。実施形態では、産業用制御システム200は、産業用制御システム（ICS）、プログラム可能自動コントローラ（PAC）、監視制御およびデータ取得（SCADA）システム、分散型制御システム（DCS）、プログラム可能ロジック・コントローラ（PLC）、およびIEC1508のような安全規格に対して証明された産業用安全システム等を含むことができる。図2に示すように、産業用制御システム200は、システムにわたって分散された1つ以上の制御エレメントまたはサブシステムによって制御または駆動される1つ以上の産業用エレメント（例えば、入力/出力モジュール、電力モジュール、フィールド・デバイス、スイッチ、ワークステーション、および/または物理相互接続デバイス）を含む分散型制御システムを実現するために通信制御アーキテクチャを使用する。例えば、1つ以上のI/Oモジュール100が、1つ以上の通信/制御モジュール214に接続されてもよい。

#### 【0024】

[0038] 産業用制御システム200は、I/Oモジュール100にそしてI/Oモジュール100からデータを送信するように構成される。I/Oモジュール100は、入力モジュール、出力モジュール、および/または入力および出力モジュールを含むことができる。例えば、入力モジュールは、入力フィールド・デバイス217（例えば、センサ218）から情報を受信するために使用することができ、一方出力モジュールは、命令を出力フィールド・デバイス217（例えば、アクチュエータ220）に送信するために使用することができる。例えば、I/Oモジュール100は、ガス・プラント、精製所等の配管における圧力を測定するためのプロセス・センサに接続することができ、および/または弁、2状態または多状態スイッチ、送信機等を制御するためにプロセス・アクチュエータに接続することができる。フィールド・デバイス217は、直接またはネットワーク接続を介してのいずれかで、I/Oモジュール100と通信可能に結合されている。例えば、フィールド・デバイス217は、1つ以上のTCP/IP規格に対応する通信チャネル102を通じて接続することができる。これらのデバイス217は、制御弁、油圧アクチュエータ、磁気アクチュエータ、モータ、ソレノイド、電気スイッチ、送信機、入力センサ/受信機（例えば、照明、放射線、ガス、温度、電気、磁気、および/または音響センサ）、通信サブバス等を含むことができる。

#### 【0025】

[0039] 産業用制御システム200は、通信バックプレーンの相互接続性を促進するスイッチ・ファブリック202を含む。実施形態では、スイッチ・ファブリック202は、多数のI/Oモジュール100との通信を行うために、シリアル通信インタフェース204およびパラレル通信インタフェース206を含む。図2～図9に示すように、I/Oモジュール100は、1つ以上の電磁コネクタ207を使用して、産業用制御システム200

0に接続することができる。例えば、各I/Oモジュール100は、1つ以上の電磁コネクタ207またはコネクタ・アセンブリ208を含むこと、または結合されることが可能であり、コア部材がコイルを貫通する。ある実施形態では、コイルを回路ボード上の平面巻線として実装することができる。I/Oモジュール100に含まれるとき、回路ボードは部分的なばね負荷に対抗して「浮遊する」ことができ、例えば、回路ボードにわたる公差を補償するために、コア部材の平面に対して回路ボードの垂直な動きを可能にする。例えば、電磁接続の嵌合を容易にするために一定の下方圧力を加えるために、自己保持用ばね装荷メカニズムをモジュール内に設けることができ、モジュール、PCB、およびベースプレート/支持フレームの累積公差(stacked tolerance)を補償し、電磁コネクタ・アセンブリの両半分の一定の嵌合を確保する。

10

#### 【0026】

[0040] ある実施形態では、三面において固有の締結および支持を与える「溝形」構成を使用することができる。例えば、I/Oモジュール100内部に含まれる印刷回路ボードを、コア部材の平面に対して垂直な方向に、2つのトラック・セグメントに沿って、そしてこれらの間を摺動するように構成することができる。更に、コア部材を機械的に回路ボードから分離する(例えば、接触しない)こともできる。尚、平面一次および二次巻線による実装態様は、一例として挙げたに過ぎず、本開示を限定することを必ずしも意味しないことは注記してしかるべきである。つまり、他の実装態様は、巻線コイル(wire wound coil)等のような他のコイル構成を使用することができる。例えば、一次コイルが平面巻線を含んでもよく、二次コイルが巻線コイルを含んでもよい。更に、一次コイルが巻線コイルを含んでもよく、二次コイルが平面巻線を含んでもよい。他の実装態様では、一次および二次コイルの双方が巻線コイルを含んでもよい。

20

#### 【0027】

[0041] 図3は、スイッチ・ファブリック202の実施形態を示す。スイッチ・ファブリック202は、電気通信ネットワーク技術、コンピュータ・ネットワーク技術、プロセス制御システム技術等のような、任意のシステム技術と共に使用する構成にすることができる。例えば、スイッチ・ファブリック202は、コントローラ・エレメントおよびサブシステムで構成される分散型制御システムと共に使用されてもよく、サブシステムは、システム全域に分散された1つ以上のコントローラによって制御される。スイッチ・ファブリック202は、多数のスレーブ・デバイスとの通信を行うために、シリアル通信インタフェース204およびパラレル通信インタフェース206を含む。

30

#### 【0028】

[0042] シリアル通信インタフェース204は、互いに並列に接続された1群のコネクタを使用して実装されてもよい。ある実施形態では、コネクタは、電磁コネクタ207/コネクタ・アセンブリ208(例えば、前述したような)として構成されてもよい。例えば、シリアル通信インタフェース204は、マルチドロップ・バス(multidrop bus)210等を使用して実装されてもよい。実装態様では、マルチドロップ・バス210は、I/Oモジュール100/スレーブ・デバイスの構成および診断機能のために使用されてもよい。パラレル通信インタフェース206は、多数の信号を同時に多数の専用高速パラレル通信チャンネル上で送信することを可能にする。例えば、パラレル通信インタフェース206は、クロス・スイッチ212等を使用して実装されてもよい。

40

#### 【0029】

[0043] 図3に示す実施形態では、パラレル通信インタフェース206が、各I/Oモジュール100/スレーブ・デバイスに対して専用接続を有する、四(4)線全二重クロス・スイッチ212を使用して実装されてもよい。実装態様では、各接続が、1つ以上の電磁コネクタ207/コネクタ・アセンブリ208(例えば、前述のような)を使用して設けられてもよい。クロス・スイッチ212は、ポイント・ツー・ポイント・バスを接続し、I/Oモジュール100/スレーブ・デバイス間におけるトラフィックを可能にするプログラム可能クロス・スイッチとして実装することができる。クロス・スイッチ212は、通信/制御モジュール214のような、マスタ・デバイスによって構成されてもよ

50

い。例えば、通信/制御モジュール214/マスタ・デバイスは、クロス・スイッチ212内に含まれる1組以上のレジスタを、I/Oモジュール100/スレーブ・デバイス間におけるトラフィックを制御するように構成することができる。実装態様では、通信/制御モジュール214/マスタ・デバイスが、どのようにI/Oモジュール100/スレーブ・デバイスを相互接続するか指令するルール・セットを含むのでもよい。例えば、通信/制御モジュール214/マスタ・デバイスが1組のレジスタを含み、各レジスタが特定のスイッチの動作を(例えば、パケットがどのように転送されるか等に関して)定めるのでもよい。つまり、クロス・スイッチ212は、必ずしも自動構成設定する(auto-configure)のでもなく、代わりに、通信/制御モジュール214/マスタ・デバイスによって与えられる構成を実施するのでもよい。しかしながら、この構成は、一例として挙げられたに過ぎず、本開示を限定することを意味するのではない。したがって、他の実装態様では、クロス・スイッチ212が自動構成設定するのでもよい。

10

#### 【0030】

[0044] 並列通信インタフェース206は、I/Oモジュール100/スレーブ・デバイスからのデータ収集のために使用されてもよい。更に、各I/Oモジュール100/スレーブ・デバイスは通信/制御モジュール214/マスタ・デバイスへのそれ自体のプライベート・バスを有するので、各I/Oモジュール100/スレーブ・デバイスは同時に通信/制御モジュール214と通信することができる。つまり、産業用制御システム200/スイッチ・ファブリック202の総応答時間は、典型的なマルチドロップ・バスにおけるように全てのスレーブ・デバイスの合計ではなく、最も遅いI/Oモジュール100/スレーブ・デバイスのそれに制限されることになる。

20

#### 【0031】

[0045] 実装態様では、スイッチ・ファブリック202、シリアル通信インタフェース204、および並列通信インタフェース206は、1つのモノリシック回路ボード216内に実装することができ、例えば、電磁コネクタ207の多数のE字型コア部材が、図9に示すように、回路ボード216を貫通する。実装態様では、コア部材が回路ボード216から機械的に分離されるとよい(例えば、回路ボード216に接触しない)。しかしながら、この構成は一例として挙げられたに過ぎず、本開示を限定することを意味するのではない。つまり、シリアル通信インタフェース204および並列通信インタフェース206は、シリアル通信インタフェース204および並列通信インタフェース206を別個に実装するための多数のディスクリート半導体デバイス等のような、多数のコンポーネントの異なる配置(arrangement)を使用して実装されてもよい。

30

#### 【0032】

[0046] スwitch・ファブリック202は、1つ以上のI/Oモジュール100(例えば、スレーブ・デバイスとして)を接続し、I/Oモジュール100にそしてI/Oモジュール100からデータを送信するように構成することもできる。I/Oモジュール100は、入力モジュール、出力モジュール、および/または入力および出力モジュールを含むことができる。例えば、入力モジュールは、プロセスまたは現場において入力計器から情報を受信するために使用することができ、一方出力モジュールは現場における出力計器に命令を送信するために使用することができる。例えば、I/Oモジュール100を、ガス・プラント、精製所等の配管における圧力を測定するためのセンサ218のような、プロセス・センサに接続することができる。実装態様では、I/Oモジュール100は、産業用制御システム200において、以下を含むが必ずしもそれらに限定されない用途においてデータを収集するために使用することができる。製品製造および製作、外部発電(utility power generation)、石油、ガス、および化学精製のような重要なインフラストラクチャおよび/または工業プロセス、薬品、食品および飲料水、パルプおよび紙、金属および鋳業、ならびに建物、空港、船舶、宇宙ステーション用の設備および大規模な工業プロセス(例えば、加熱、換気、および空調(HVAC)機器ならびにエネルギー消費を監視および制御するため)。

40

#### 【0033】

50

[0047] 実装態様では、I/Oモジュール100は、センサから受信したアナログ・データをデジタル・データに変換するように（例えば、アナログ/デジタル変換器（ADC）回路等を使用して）構成することができる。また、I/Oモジュール100は、モータまたは調節弁、あるいは電気リレー、およびその他の形態のアクチュエータというような1つ以上のプロセス・アクチュエータ220に接続され、モータ速度、モータ・トルクのようなモータの1つ以上の動作特性、あるいは調節弁の位置または電気リレーの状態等を制御するように構成することができる。更に、I/Oモジュール100は、アクチュエータ220への送信のために、デジタル・データをアナログ・データに変換するように（例えば、デジタル/アナログ（DAC）回路等を使用して）構成することもできる。実装態様では、I/Oモジュール100の内1つ以上が、イーサネット・バス、H1フィールド・バス、PROFIBUS、HARTバス、Modbus、OPCUAバス等のような通信サブバスを通じて通信するように構成された通信モジュールを含むことができる。更に、制御弁、油圧アクチュエータ、磁気アクチュエータ、モータ、ソレノイド、電気スイッチ、送信機、入力センサ/受信機（例えば、照明、放射線、ガス、温度、電気、磁気、および/または音響センサ）のような種々のフィールド・デバイス217、通信サブバス等のために、2つ以上のI/Oモジュール100を使用してフォールト・トレラントおよび冗長接続を設けることができる。

10

#### 【0034】

[0048] 各I/Oモジュール100には、I/Oモジュール100間で区別するための一意の識別子（ID）を与えることができる。実装態様では、I/Oモジュール100は、産業用制御システム200に接続されるときに、そのIDによって識別されるのでもよい。冗長性を設けるために、多数のI/Oモジュール100を産業用制御システム200と共に使用することができる。例えば、図2に示すように、2つ以上のI/Oモジュール100をセンサ218、アクチュエータ220、または任意の他のフィールド・デバイス217に接続することができる。各I/Oモジュール100は、印刷回路ボード（PCB）224等のような、I/Oモジュール100と共に含まれるハードウェアおよび回路への物理的接続を設ける1つ以上のポート222を含むことができる。

20

#### 【0035】

[0049] I/Oモジュール100の内1つ以上は、他のネットワークに接続するためのインタフェースを含むことができる。必ずしも限定するのではないが、他のネットワークには、3Gセルラ・ネットワーク、4Gセルラ・ネットワーク、または全地球移動体通信システム（GSM）ネットワークのようなワイド・エリア・セルラ電話ネットワーク、Wi-Fiネットワーク（例えば、IEEE802.11ネットワーク規格を使用して運営されるワイヤレスLAN（WLAN））のようなワイヤレス・コンピュータ通信ネットワーク、パーソナル・エリア・ネットワーク（PAN）（例えば、IEEE802.15ネットワーク規格を使用して運営されるワイヤレスPAN（WPAN））、ワイド・エリア・ネットワーク（WAN）、イントラネット、エクストラネット、内部ネット（an internet）、インターネット（the internet）等が含まれる。更に、I/Oモジュール100の内1つ以上は、I/Oモジュール100をコンピュータ・バス等に接続するための接続も含むことができる。

30

40

#### 【0036】

[0050] 通信/制御モジュール214は、I/Oモジュール100を監視および制御するため、ならびに2つ以上のI/Oモジュール100を一緒に接続するために使用することができる。本開示の実施形態では、通信/制御モジュール214は、I/Oモジュール100が産業用制御システム200に接続されたときに、I/Oモジュール100の一意のIDに基づいて、ルーティング・テーブル（routing table）を更新することができる。更に、多数の冗長I/Oモジュール100が使用されるとき、各通信/制御モジュール214はI/Oモジュール100に関する情報データベースのミラーリングを実施し、データがI/Oモジュール100から受信される毎および/またはI/Oモジュール100に送信される毎にこれらを更新することができる。ある実施形態では、冗長性を設けるため

50

に、2つ以上の通信/制御モジュール214が使用される。セキュリティ向上のために、通信/制御モジュール214は、始動、リセット、新たな制御モジュール214の設置、通信/制御モジュール214の交換、周期的、予定された時刻等のような、規定のイベントまたは時点において、互いに認証するために認証シーケンスまたはハンドシェークを実行するように構成することができる。また、I/Oモジュール100も、図10～図15に示し以下で更に説明するように、認証シーケンスまたは「ハンドシェーク」を実行するように構成することができる。

【0037】

[0051] スイッチ・ファブリック202を使用して送信されるデータは、パケット化することもできる。即ち、データの離散部分を、データ部分をネットワーク制御情報等と共に含むデータ・パケットに変換することができる。産業用制御システム200/スイッチ・ファブリック202は、データ送信のために1つ以上のプロトコルを使用することができる。これらのプロトコルには、上位データ・リンク制御(HDLC)のようなビット指向同期データ・リンク・レイヤ・プロトコル(bit-oriented synchronous data link layer protocol)が含まれる。具体的な一例では、産業用制御システム200/スイッチ・ファブリック202は、国際標準化機構(ISO)13239規格等によるHDLCを実装することもできる。更に、冗長HDLCを実装するために、2つ以上の通信/制御モジュール214を使用することもできる。しかしながら、HDLCは一例として挙げられたに過ぎず、本開示を限定することを意味するのではないことは注記してしかるべきである。つまり、産業用制御システム200は、本開示にしたがって、他の種々の通信プロトコルを使用することもできる。

10

20

【0038】

[0052] 通信/制御モジュール214の内1つ以上は、1つ以上の制御ループ・フィードバック・メカニズム/コントローラ226のような、I/Oモジュール100を介してスイッチ・ファブリック202に接続された計装機器(instrumentation)を監視および/または制御するために使用されるコンポーネントと情報を交換するように構成することもできる。実装態様では、コントローラ226は、マイクロコントローラ/プログラム可能ロジック・コントローラ(PLC)、比例・積分・微分(PID)コントローラ等として構成することができる。通信/制御モジュール214の内1つ以上は、産業用制御システム200をコントローラ226にネットワーク230を通じて接続するためのネットワーク・インタフェース228を含むこともできる。実装態様では、ネットワーク・インタフェース228は、スイッチ・ファブリック202をローカル・エリア・ネットワーク(LAN)に接続するためのギガビット・イーサネット・インタフェースとして構成されてもよい。更に、冗長ギガビット・イーサネットを実施するために、2つ以上の通信/制御モジュール214を使用することもできる。しかしながら、ギガビット・イーサネットは一例として挙げられたに過ぎず、本開示を限定することを意味するのではないことは注記してしかるべきである。つまり、ネットワーク・インタフェース228は、産業用制御システム200を他の種々のネットワークに接続するように構成することもできる。他の種々のネットワークには、3Gセルラ・ネットワーク、4Gセルラ・ネットワーク、または全地球移動体通信システム(GSM)ネットワークのようなワイド・エリア・セルラ電話ネットワーク、Wi-Fiネットワーク(例えば、IEEE802.11ネットワーク規格を使用して運営されるワイヤレスLAN(WLAN))のようなワイヤレス・コンピュータ通信ネットワーク、パーソナル・エリア・ネットワーク(PAN)(例えば、IEEE802.15ネットワーク規格を使用して運営されるワイヤレスPAN(WPAN))、ワイド・エリア・ネットワーク(WAN)、イントラネット、エクストラネット、インターネット(an internet)、インターネット(the internet)等が含まれるが、必ずしもこれらに限定されるのではない。加えて、ネットワーク・インタフェース228は、コンピュータ・バスを使用して実装されてもよい。例えば、ネットワーク・インタフェース228は、ミニPCIインタフェース等のような、周辺コンポーネント相互接続(PCI)カード・インタフェースを含むことができる。更に、ネットワーク230は、異なるアクセス

30

40

50

・ポイントにわたる1つのネットワークまたは多数のネットワークを含むように構成することもできる。

#### 【0039】

[0053] 産業用制御システム200は、電力をフィールド・デバイスにI/Oモジュール100を介して供給するために1つ以上の電力モジュール232を含むことができる。電力モジュール232の内1つ以上は、モータ220のような(例えば、モータ220がDCモータを含む実装態様において)フィールド・デバイスへの送信のために交流(AC)(例えば、AC主電源等によって供給されるような)を直流(DC)に変換するためのAC-DC(AC/DC)変換器を含むのもよい。冗長性を設けるために、2つ以上の電力モジュール232を使用することができる。例えば、図2に示すように、電力モジュール232毎に別個の(冗長な)電力バックプレーン234を使用して、2つの電力モジュール232をI/Oモジュール100の各々に接続することができる。実装態様では、電力バックプレーン234は、電磁コネクタ207/コネクタ・アセンブリ208を使用して、I/Oモジュール100の内1つ以上に接続されてもよい(例えば、前述したように)。実装態様では、電力バックプレーン234には、シリアル通信インタフェース204およびパラレル通信インタフェース206と共に、回路ボード216が含まれてもよい。

10

#### 【0040】

[0054] 産業用制御システム200は、多数の電源から電力を受けることができる。例えば、AC電力は電力グリッドから供給されてもよい(例えば、AC主電源からの高電圧電力を使用する)。また、AC電力は、ローカル発電(local power generation)(例えば、現場のタービンまたはディーゼル居所発電機)を使用して供給することもできる。電源は、コントローラ、I/Oモジュール等のような産業用制御システム200の自動機器に、電力グリッドからの電力を配給するのでもよい。また、電源は、ローカル発電機からの電力を産業用制御システムの機器に配給するために使用することもできる。また、産業用制御システム200は、多数のバッテリー・モジュールを使用してDC電力を蓄積および返流するように構成された追加の(バックアップ)電源も含むことができる。例えば、電源がUPSとして機能してもよい。ある実施形態では、多数の電源を産業用制御システム200内部に分散させる(例えば、物理的に散在させる)ことができる。

20

#### 【0041】

[0055] 産業用制御システム200は、支持フレーム236を使用して実装されてもよい。支持フレーム236は、通信/制御モジュール(1つまたは複数)214、電力モジュール(1つまたは複数)232、スイッチ・ファブリック202、電力バックプレーン(1つまたは複数)234、および/またはI/Oモジュール100を支持および/または相互接続するために使用することができる。例えば、スイッチ・ファブリック202は回路ボード216を含む場合もある。回路ボード216は、例えば、両面テープ、接着材、または機械的締結具(例えば、ねじ、ボルト等)のような締結具を使用して支持フレーム236に取り付けられてもよい。加えて、電磁コネクタ207のコア部材は、例えば、両面テープ、接着材、または機械的締結具(例えば、ねじ、ボルト等)のような締結具を使用して支持フレーム236に取り付けられてもよい。ある実装態様では、コア部材を支持フレーム236のチャンネル内に位置付けるために、テンプレートが使用されてもよい。実装態様では、コア部材の上面が、回路ボード216の上面と実質的に面一になるのでもよい。他の実装態様では、コア部材の上面が、回路ボード216の上面よりも下にある距離だけ下がっていてもよく(例えば、約1ミリメートル(1mm)だけ)、および/または回路ボード216の上面よりも上に突出してもよい。

30

40

#### 【0042】

[0056] 支持フレーム236は、I/Oモジュール100のコネクタ(例えば、電磁コネクタ207)を、回路ボード216に含まれるコネクタ(例えば、電磁コネクタ207)と、および/または電力バックプレーン234のコネクタ(例えば、電磁コネクタ207)と整列させるためというように、I/Oモジュール100のための位置合わせを行う

50

ためのスロット 238 を含むことができる。例えば、I/Oモジュール 100 は、スロット 238 に挿入し、回路ボード 216 に対する I/Oモジュール 100 の整列を行うためのタブ/ポスト 242 を有するコネクタ 240 を含むのもよい。実装態様では、コネクタ 240 の内 1 つ以上が、熱伝導性材料（例えば、金属）で作られると、PCB 224 の熱面 (thermal plane) に接続されて、PCB 224 のコンポーネントによって発生される熱を PCB 224 から遠ざけて支持フレーム 236 に導くことができる。支持フレーム 236 は、それ自体が熱伝導性材料（例えば、金属）で作られてもよい。更に、産業用制御システム 200 は、特定のスロット 238 と結合された各 I/Oモジュール 100 を一意に識別するために、一意の物理 ID を各物理スロット 238 と関連付けることができる。例えば、特定のスロット 238 の ID は、スロット 238 と結合された I/Oモジュール 100 と関連付けることができ、および/または第 2 ID を I/Oモジュール 100 と一意に関連付けることができる。更に、特定の I/Oモジュール 100 の ID は、その I/Oモジュール 100 がスロット 238 と結合されるときに、スロット 238 に対する ID として使用することもできる。支持フレーム 236 は、キャビネット取り付け、ラック取り付け、壁取り付け等に合わせて組み立てることができる。

10

#### 【0043】

[0057] 尚、添付図面において、産業用制御システム 200 は 1 つのスイッチ・ファブリック 202 を含むと説明したが、1 つよりも多いスイッチ・ファブリック 202 が産業用制御システム 200 に設けられてもよい。例えば、2 つ以上のスイッチ・ファブリック 202 が産業用制御システム 200 と共に使用されてもよい（例えば、冗長スイッチ・ファブリック 202 間に物理的な分離を設けるため等）。スイッチ・ファブリック 202 の各々には、それ自体の支持フレーム 236 が設けられてもよい。更に、シリアル通信インタフェース 204 およびパラレル通信インタフェース 206 の双方が 1 つのスイッチ・ファブリック 202 内に含まれると説明したが、物理的に別個のスイッチ・ファブリックが設けられてもよく、1 つのスイッチ・ファブリックがシリアル通信インタフェース 204 を含み、他のスイッチ・ファブリックがパラレル通信インタフェース 206 を含んでもよいことは認められよう。

20

#### 【0044】

[0058] 制御エレメント/サブシステムおよび/または産業用エレメント（例えば、I/Oモジュール 100、通信/制御モジュール 214、電力モジュール 232 等）は、1 つ以上のバックプレーンによって互いに接続することができる。例えば、前述のように、通信/制御モジュール 214 は I/Oモジュール 100 に、通信バックプレーン（例えば、スイッチ・ファブリック 202）によって接続することができる。更に、電力モジュール 232 は、電力バックプレーン 234 によって、I/Oモジュール 100 および/または通信/制御モジュール 214 に接続することもできる。ある実施形態では、物理相互接続デバイス（例えば、米国特許出願第 14/446,412 号に記載されているようなスイッチ、コネクタ、またはケーブルであるが、これらに限定されるのではない。この特許出願をここで引用したことによりその内容全体が本願にも含まれるものとする）が、I/Oモジュール 100、通信/制御モジュール 214、電力モジュール 232、および恐らくは他の産業用制御システム機器に接続するために使用される。例えば、通信/制御モジュール 214 をネットワーク 230 に接続するためにケーブルを使用することができ、電力モジュール 232 を電力グリッドに接続するために他のケーブルを使用することができ、電力モジュール 232 をローカル発電機に接続するために他のケーブルを使用することができる等である。

30

40

#### 【0045】

[0059] ある実施形態では、産業用制御システム 200 は、米国特許出願第 14/469,931 号および国際出願 PCT/US 2013/053721 に記載されているような、安全制御システムを実現する。この特許出願をここで引用したことによりその内容全体が本願にも含まれるものとする。例えば、産業用制御システム 200 は、セキュリティ証明ソース（例えば、工場）、およびセキュリティ証明インプリメンタ（例えば、鍵管理

50

エンティティ)を含む。セキュリティ証明ソースは、一意のセキュリティ証明(例えば、鍵、一意の識別子のような証明書等、および/またはセキュリティ証明)を生成するように構成される。セキュリティ証明インプリメンタは、制御エレメント/サブシステムおよび/または産業用エレメント(例えば、ケーブル、デバイス217、I/Oモジュール100、通信/制御モジュール214、電力モジュール232等)に、セキュリティ証明ソースによって生成された一意のセキュリティ証明をプロビジョニングするように構成される。

#### 【0046】

[0060] 産業用制御システム200の多数の(例えば、各)デバイス217、I/Oモジュール100、通信/制御モジュール214、電力モジュール232、物理相互接続デバイス等には、産業用制御システム200の多数の(例えば、全ての)レベルにおいてセキュリティが得られるために、セキュリティ証明をプロビジョニングすることができる。更にまた、センサおよび/またはアクチュエータ等を含む制御エレメント/サブシステムおよび/または産業用エレメントには、製造中に(例えば、生産時に)一意のセキュリティ証明(例えば、鍵、証明書等)をプロビジョニングすることができ、産業用制御システム200のセキュリティを高めるために、産業用制御システム200の鍵管理エンティティによって生産時から管理することができる。

10

#### 【0047】

[0061] ある実施形態では、産業用制御システム200のセンサおよび/またはアクチュエータ等を含む制御エレメント/サブシステムおよび/または産業用エレメント間における通信は、認証プロセスを含む。この認証プロセスは、産業用制御システム200内に実装されたセンサおよび/またはアクチュエータ等を含む制御エレメント/サブシステムおよび/または産業用エレメントを認証するために実行することができる。更に、この認証プロセスは、そのエレメントおよび/または物理相互接続デバイスを認証するために、エレメントおよび/または物理相互接続デバイスに関連付けられたセキュリティ証明を利用することができる。例えば、セキュリティ証明は、暗号化鍵、証明書(例えば、公開鍵証明書、デジタル証明書、識別証明書、セキュリティ証明書、非対称証明書、標準証明書、非標準証明書)および/または識別番号を含むことができる。

20

#### 【0048】

[0062] 実装態様では、産業用制御システム200の多数の制御エレメント/サブシステムおよび/または産業用エレメントには、それら自体の一意のセキュリティ証明がプロビジョニングされる。例えば、産業用制御システム200の各エレメントには、それら自体の一意の1組(複数組)の証明書、暗号化鍵、および/または識別番号が、そのエレメントが製造されるときにプロビジョニングされるのでもよい(例えば、エレメントの生産時に、個々の1組の鍵および証明書が定められる)。これら複数組の証明書、暗号化鍵、および/または識別番号は、強い暗号を提供/サポートするように構成される。暗号化鍵は、アメリカ国家安全保障局(NSA)アルゴリズム、アメリカ国立標準技術研究所(NIST)アルゴリズム等のような、標準的な(例えば、商用オフザシェルフ(COTS))暗号アルゴリズムによって実施することができる。

30

#### 【0049】

[0063] 認証プロセスの結果に基づいて、認証されたエレメントを作動させることができ、産業用制御システム200内においてこのエレメントの部分的機能を使用可能または使用不可にすることができ、産業用制御システム200内においてこのエレメントの完全な機能を使用可能にすることができ、および/または産業用制御システム200内におけるこのエレメントの機能を完全に使用不可にすることができる(例えば、そのエレメントと産業用制御システム200の他のエレメントとの間で通信が促進されない)。

40

#### 【0050】

[0064] 実施形態では、産業用制御システム200のエレメントに関連付けられた鍵、証明書、および/または識別番号は、そのエレメントの相手先ブランド製造(OEM)を指定することができる。本明細書において使用する場合、「相手先ブランド製造」または

50

「OEM」は、デバイス（例えば、エレメント）を実際に製造するエンティティ、および/または実際の製造元からデバイスを購入しそのデバイスを販売するエンティティというような、デバイスの供給元として定義することができる。つまり、実施形態では、デバイスは、当該デバイスの実際の製造元および供給元の双方であるOEMによって製造および流通（販売）することができる。しかしながら、他の実施形態では、供給元であるが実際の製造元ではないOEMによって、デバイスを流通することもできる。このような実施形態では、OEMは、実際の製造元によってデバイスを製造させることができる（例えば、OEMは、デバイスを実際の製造元から購入する、契約する、注文する等が可能である）。

#### 【0051】

[0065] 加えて、OEMがデバイスの実際の製造元ではない供給元を含む場合、デバイスは、実際の製造元のブランドの代わりに、供給元のブランドを表示する(bear)ことができる。例えば、エレメント（例えば、通信/制御モジュール214またはI/Oモジュール100）が、供給元であるが実際の製造元ではない特定のOEMに関連がある実施形態では、このエレメントの鍵、証明書、および/または識別番号がその出所(origin)を特定することができる。産業用制御システム200のエレメントの認証中に、認証されるエレメントが、産業用制御システム200の1つ以上の他のエレメントのOEMとは異なるエンティティによって製造または供給されたと判定されたとき、このエレメントの機能は、産業用制御システム200内部では少なくとも部分的に使用不可にすることができる。例えば、そのエレメントと産業用制御システム200の他エレメントとの間における通信（例えば、データ転送）に対して制限を設けて、このエレメントが産業用制御システム200内において動作/機能できないようにすることができる。産業用制御システム200のエレメントの内1つが交換を必要とするとき、この特徴は、産業用制御システム200のユーザが、そのエレメントを異質のエレメント（例えば、産業用制御システム200の残りのエレメントとは異なる出所（異なるOEM）を有するエレメント）と知らずに交換し、そのエレメントを産業用制御システム200内に実装することを防止することができる。このように、本明細書において説明する技法は、安全が確保された産業用制御システム200内において、他のOEMのエレメントを置換するのを防止することができる。一例では、元となるOEM(originating OEM)によって提供されるエレメントの代わりに同様の機能を設けるエレメントに置換するのを防止することができる。何故なら、置換されるエレメントは元のOEMシステム内部では認証および動作することができないからである。他の例では、第1販売代理人には、元となるOEMによって第1組の物理および暗号ラベルを有するエレメントを提供することができ、この第1販売代理人のエレメントを産業用制御システム200内に設置することができる。この例では、第2販売代理人には、同じ元となるOEMによって第2組の（例えば、異なる）物理および暗号ラベルを有するエレメントを提供することができる。この例では、第2販売代理人のエレメントは、産業用制御システム200内では動作することが妨げられることがあり得る。何故なら、これらは認証できず、第1販売代理人のエレメントと一緒に動作できないからである。しかしながら、第1販売代理人および第2販売代理人が相互契約を結ぶこともあり、この場合第1および第2エレメントは、同じ産業用制御システム200内で認証および動作するように構成することができることも注記してしかるべきである。更に、ある実施形態では、相互動作を許容する販売代理店間の契約は、この契約が特定の顧客、顧客のグループ、工場等のみに適用されるように実施することもできる。

#### 【0052】

[0066] 他の例では、ユーザが産業用制御システム200内において誤って指定された（例えば、誤ったマークが付けられた）エレメントを実装しようとする可能性がある。例えば、誤ったマークが付けられたエレメントは、産業用制御システム200の他のエレメントのOEMと同じOEMに関連することを誤って示す物理指標が、そのエレメントに付けられたということもあり得る。このような場合、産業用制御システム200によって実施される認証プロセスは、そのエレメントが模造品であることをユーザに警告することが

10

20

30

40

50

できる。また、このプロセスは、産業用制御システム200に対するセキュリティ向上を促進することもできる。何故なら、模造エレメントが、悪意のソフトウェアを産業用制御システム200内に混入させる可能性がある媒介物となる場合が多いからである。実施形態では、認証プロセスは、産業用制御システム200のために安全なエア・ギャップを提供し、安全な産業用制御システムが危険なネットワークから物理的に分離されることを確保する。

#### 【0053】

[0067] 実装態様では、安全産業用制御システム200は、鍵管理エンティティを含む。鍵管理エンティティは、暗号システムにおいて暗号鍵（例えば、暗号化鍵）を管理するように構成することができる。この暗号鍵の管理（例えば、鍵管理）は、鍵の生成、交換、格納、使用、および/または交換を含むことができる。例えば、鍵管理エンティティは、セキュリティ証明ソースとして役割を果たすように構成され、一意のセキュリティ証明（例えば、公開セキュリティ証明、秘密セキュリティ証明）を産業用制御システム200のエレメントに生成する。鍵管理は、ユーザおよび/またはシステム・レベル（例えば、ユーザまたはシステム間）における鍵に関係する。

10

#### 【0054】

[0068] 実施形態では、鍵管理エンティティは、安全な設備内に位置するエンティティのような、安全なエンティティを含む。鍵管理エンティティは、I/Oモジュール100、通信/制御モジュール214、およびネットワーク230とは離れて位置することができる。例えば、ファイアウォールが鍵管理エンティティを制御エレメントまたはサブシステムおよびネットワーク230（例えば、企業ネットワーク）から分離することができる。実装態様では、このファイアウォールは、ソフトウェアおよび/またはハードウェアベースのネットワーク・セキュリティ・システムとすることができ、データ・パケットを分析し、ルール・セットに基づいて、データ・パケットの通過を許可すべきか否か判断することによって、着信および発信するネットワーク・トラフィックを制御する。つまり、ファイアウォールは、信頼が得られた安全な内部ネットワーク（例えば、ネットワーク230）と、安全であり信頼が得られたとは想定されない他のネットワーク（例えば、クラウドおよび/またはインターネット）との間に障壁を構築する。実施形態では、ファイアウォールは、鍵管理エンティティ、および制御エレメントまたはサブシステムの1つ以上、および/またはネットワーク230間で選択的な（例えば、安全な）通信を可能にする。例では、1つ以上のファイアウォールを産業用制御システム200内の種々の場所に実装することができる。例えば、ファイアウォールをネットワーク230のスイッチおよび/またはワークステーションに統合することができる。

20

30

#### 【0055】

[0069] 更に、安全産業用制御システム200は、1つ以上の製造エンティティ（例えば、工場）を含むことができる。製造エンティティには、産業用制御システム200のエレメントについて、相手先ブランド製造元（OEM）を関連付けることができる。鍵管理エンティティは、ネットワーク（例えば、クラウド）を通じて製造エンティティと通信可能に結合することができる。実装態様では、産業用制御システム200のエレメントが1つ以上の製造エンティティにおいて製造されているとき、鍵管理エンティティはこれらのエレメントと通信可能に結合することができる（例えば、エレメントへの暗号化通信パイプラインを有することができる）。鍵管理エンティティは、製造時点においてエレメントにセキュリティ証明をプロビジョニングする（例えば、鍵、証明書、および/または識別番号をエレメントに挿入する）ために通信パイプラインを利用することができる。

40

#### 【0056】

[0070] 更に、エレメントが使用に移される（例えば、作動される）とき、鍵管理エンティティは、各個々のエレメントに世界中で通信可能に結合することができ（例えば、暗号化された通信パイプラインによって）、特定のコードの使用を確認し署名し、任意の特定のコードの使用を無効にし（例えば、除去する）、および/または任意の特定のコードの使用を可能にすることができる。つまり、鍵管理エンティティは、エレメントに被管理

50

鍵が付けられるように、そのエレメントが元々製造された（例えば、生産された）工場において各エレメントと通信することができる。産業用制御システム 200 のエレメント毎に全ての暗号化鍵、証明書、および/または識別番号を含むマスタ・データベースおよび/またはテーブルを、鍵管理エンティティによって維持することができる。鍵管理エンティティは、そのエレメントとの通信によって、鍵を無効にするように構成され、これによってコンポーネントの窃盗および再使用に反撃する認証メカニズムの能力を高める。

【0057】

[0071] 実装態様では、鍵管理エンティティは、制御エレメント/サブシステム、産業用エレメント、および/またはネットワーク 230 の内 1 つ以上と他のネットワーク（例えば、クラウドおよび/またはインターネット）およびファイアウォールを介して通信可能に結合することができる。例えば、実施形態では、鍵管理エンティティは集中システムまたは分散型システムであることも可能である。更に、実施形態では、鍵管理エンティティをローカルでまたはリモートで管理することができる。ある実装態様では、鍵管理エンティティをネットワーク 230 および/または制御エレメントまたはサブシステム内部に配置する（例えば、統合する）ことができる。鍵管理エンティティは、管理を提供することができる、および/または種々の方法で管理されることが可能である。例えば、鍵管理エンティティは、中央位置において顧客によって、個々の工場位置における顧客によって、外部の第三者管理会社によって、および/または産業用制御システム 200 の異なるレイヤにおける顧客によって、そして異なる場所で、レイヤに応じて実施/管理することができる。

10

20

【0058】

[0072] 認証プロセスによって、様々なレベルのセキュリティ（例えば、スケーラブルな、ユーザが設定可能なセキュリティ量）を提供することができる。例えば、エレメントを認証しエレメント内のコードを保護する基準レベルのセキュリティを提供することができる。他のレイヤのセキュリティも同様に追加することができる。例えば、通信/制御モジュール 214 または I/O モジュール 100 のようなコンポーネントが、適正な認証が行われなければ、起動 (power up) することができないというような度合いで、セキュリティを実施することができる。実装態様では、コードにおける暗号化がエレメントにおいて実施され、一方セキュリティ証明（例えば、鍵および証明書）はエレメント上に実装される。セキュリティは、産業用制御システム 200 全体に分散させること（例えば、流れること）ができる。例えば、セキュリティは、産業用制御システム 200 全てを通過してエンド・ユーザまで流れることができ、エンド・ユーザは、その時点で、モジュールが何を制御するように設計されたのか把握する。実施形態では、認証プロセスは、暗号化、安全な通信のためのデバイスの識別、およびシステム・ハードウェアまたはソフトウェア・コンポーネントの認証（例えば、デジタル署名によって）を可能にする (provide)。

30

【0059】

[0073] 実装態様では、認証プロセスは、異なる製造元/販売元/供給元（例えば、OEM）によって製造および/または供給されたエレメントの安全な産業用制御システム 200 内における相互運用性に備える、および/または可能にするために実施することができる。例えば、異なる製造元/販売元/供給元によって製造および/または供給されたエレメント間における選択的（例えば、一部の）相互運用性を可能にする (enable) ことができる。実施形態では、認証の間に実装される一意のセキュリティ証明（例えば、鍵）が階層を形成することができ、これによって異なる機能を産業用制御システム 200 の異なるエレメントによって実行することを可能にする。

40

【0060】

[0074] 更に、産業用制御システム 200 のコンポーネントを接続する通信リンクは、ラント・パケット（例えば、64 バイトよりも小さいパケット）のような、データ・パケットを採用して内部に配し（例えば、注入および/または詰め込み）、セキュリティのレベル向上に資することができる。ラント・パケットの使用により、外部情報（例えば、偽りのメッセージ、マルウェア（ウイルス）、データ・マイニング・アプリケーション等の

50

ような悪意のあるコンテンツ)を通信リンクに注入できる難度を高める。例えば、外部エンティティが悪意のあるコンテンツを通信リンクに注入する能力を阻害するために、通信チャンネル102の1つ以上を通じてI/Oモジュール100から1つ以上のフィールド・デバイス217に送信されるデータ・パケット間のギャップ内において、ラント・パケットを通信リンクに注入することができる。

#### 【0061】

[0075] 図10および図11に示すように、I/Oモジュール100または他の産業用エレメント/コントローラ306(例えば、通信/制御モジュール214、フィールド・デバイス217、物理的相互接続デバイス、スイッチ、電力モジュール232等)は、少なくとも部分的に、アクション発起元(action originator)302からの要求/コマンドにしたがって動作させることができる。実装態様では、アクション発起元302は、オペレータ・インタフェース308(例えば、SCADAまたはHMI)、エディタ312およびコンパイラ314を含む設計インタフェース310、ローカル・アプリケーション320、リモート・アプリケーション316(例えば、ネットワーク318を通じてローカル・アプリケーション320を介して通信する)等を含む。図10および図11に示す認証パス300では、産業用エレメント/コントローラ306(例えば、I/Oモジュール100)は、アクション要求がアクション認証器304によって署名および/または暗号化されたときにのみ、アクション要求(例えば、データ、制御コマンド、ファームウェア/ソフトウェアの更新、設定点制御、アプリケーション・イメージのダウンロード等の要求)を処理する。これによって、有効なユーザ・プロファイルからの不正なアクション要求を防止し、無効な(例えば、ハッキングされた)プロファイルから来る不正なアクション要求から、システムの安全性を更に確保する。実施形態では、アクション認証プロセスは、米国特許出願第14/519,066号に記載されたように実施される。この特許出願をここで引用したことにより、その内容全体が本願にも含まれるものとする。

10

20

#### 【0062】

[0076] アクション認証器304は、アクション発起元302と同じ場所(例えば、直接接続されたデバイス・ライフサイクル管理システム(「DLM」)322または安全性が確保されたワークステーション326)にあること、または離れて位置すること(例えば、ネットワーク318を通じて接続されたDLM322)ができる。一般に、アクション認証器304は、秘密鍵が格納された記憶媒体と、秘密鍵を使用してアクション発起元302によって生成されたアクション要求に署名するおよび/または暗号化するように構成されたプロセッサとを含む。秘密鍵は、標準的な操作者のログインによってアクセスすることができないメモリに格納される。例えば、安全性が確保されたワークステーション326は、アクセスのために、物理鍵、携帯用暗号化デバイス(例えば、スマート・カード、RFIDタグ等)、および/または生物計量入力を要求することができる。

30

#### 【0063】

[0077] ある実施形態では、アクション認証器304は、スマート・カード324(安全性が確保されたマイクロプロセッサを含むことができる)のような携帯用暗号化デバイスを含む。携帯用暗号化デバイスを使用する利点は、デバイス全体(秘密に格納された鍵、およびそれと通信するプロセッサを含む)を、アクション発起元302のインタフェースに対して許可されたアクセスを有する操作者またはユーザと一緒に携行することである。アクション認証ノード304が認証パス300に、安全性が確保されたワークステーションまたは安全性が確保されていないワークステーションのいずれを介してアクセスしても、アクション発起元302からのアクション要求は、安全性が低い可能性があるワークステーションまたはクラウド・ベースのアーキテクチャの代わりに、携帯用暗号化デバイスのアーキテクチャ内部において安全に署名および/または暗号化することができる。これにより、不正アクションから産業用制御システム200の安全性を確保する。例えば、許可されていない人は、スマート・カード324を実際に所持しなければならず、その後でなければ、アクション発起元302を介して送られるいずれのアクション要求も認証することができない。

40

50

## 【 0 0 6 4 】

[0078] 更に、多数のレイヤのセキュリティを採用することもできる。例えば、アクション認証器 3 0 4 は、安全が確保されたワークステーション 3 2 6 を含むことができる。ワークステーション 3 2 6 は、スマート・カード・アクセス等を介して、アクション要求に署名するためおよび/または暗号化するためだけにしかアクセスできない。加えて、安全が確保されたワークステーション 3 2 6 は、生物計量または多要素暗号デバイス 3 2 8 (例えば、指紋スキャナ、虹彩スキャナ、および/または顔認識デバイス)によってアクセス可能にすることもできる。ある実施形態では、多要素暗号デバイス 3 2 8 は、スマート・カード 3 2 4 または他の携帯用暗号化デバイスがアクション要求に署名することを可能にする前に、有効な生物計量入力を要求する。

10

## 【 0 0 6 5 】

[0079] I/Oモジュール 1 0 0、またはアクション発起元 3 0 2 によって駆動される任意の他の産業用エレメント/コントローラ 3 0 6 は、署名付きアクション要求を受け、この署名付きアクション要求の真正性を検証し、この署名付きアクション要求の真正性が検証されたときに、要求されたアクションを実行するように構成される。ある実施形態では、産業用エレメント/コントローラ 3 0 6 は、アクション要求(例えば、アプリケーション・イメージ、制御コマンド、および/またはアクション発起元によって送られる任意の他のデータ)を格納するように構成された記憶媒体 3 3 0 (例えば、SD/マイクロSDカード、HDD、SSD、または任意の他の非一時的記憶デバイス)を含む。I/Oモジュール 1 0 0 または任意の他の産業用エレメント/コントローラ 3 0 6 は、更に、署名が検証された後にアクション要求を行う/実行する(即ち、要求されたアクションを行う)プロセッサ 3 3 2 (例えば、コントローラ 1 0 6)を含む。ある実施形態では、アクション要求はアクション発起元 3 0 2 および/またはアクション認証器 3 3 2 によって暗号化され、プロセッサ 3 3 2 によって解読も行われなければならない。その後でなければ、要求されたアクションを実行することができない。実装態様では、I/Oモジュール 1 0 0 または任意の他の産業用エレメント/コントローラ 3 0 6 は、仮想鍵スイッチ 3 3 4 (例えば、プロセッサ 3 3 2 上で実行するソフトウェア・モジュール)を含む。仮想鍵スイッチ 3 3 4 は、アクション要求の署名が検証された後および/またはアクション要求が解読された後でのみ、プロセッサ 3 3 2 が要求されたアクションを実行することを可能にする。ある実施形態では、あらゆるアクションまたは重要なアクションの選択の各々は、I/Oモジュール 1 0 0 または任意の他の産業用エレメント/コントローラ 3 0 6 において実行される前に、認証パスを通過しなければならない。

20

30

## 【 0 0 6 6 】

[0080] 図 1 2 は、本明細書において説明したアクション認証パス 3 0 0 のような、アクション認証パスによってアクション要求を認証するプロセス例 4 0 0 の流れ図を示す。実装態様では、方法 4 0 0 は、産業用制御システム 2 0 0 および/また産業用制御システム 2 0 0 の認証パス 3 0 0 によって明示することができる。方法 4 0 0 は、アクション要求を発するステップ(4 0 2)(例えば、発起元/設計インタフェース 3 0 8 / 3 1 0 またはリモート/ローカル・アプリケーション・インタフェース 3 1 6 / 3 2 0)によって)と、アクション認証器 3 0 4 によってアクション要求に署名するステップ(4 0 4)と、任意にアクション認証器 3 0 4 によってアクション要求を暗号化するステップ(4 1 2)と、署名されたアクション要求をI/Oモジュール 1 0 0 または任意の他の産業用エレメント/コントローラ 3 0 6 に送るまたはダウンロードするステップ(4 0 6)と、署名付きアクション要求の真正性を検証するステップ(4 0 8)と、任意にI/Oモジュール 1 0 0 または任意の他の産業用エレメント/コントローラ 3 0 6 によってアクション要求を解読するステップ(4 1 4)と、署名付きアクション要求の真正性が検証されたとき、I/Oモジュール 1 0 0 または任意の他の産業用エレメント/コントローラ 3 0 6 によって、要求されたアクションを実行するステップ(4 1 0)とを含む。

40

## 【 0 0 6 7 】

[0081] セキュリティ強化のために、I/Oモジュール 1 0 0 または任意の他の産業用

50

エレメント/コントローラ306は、更に、要求されたアクションがI/Oモジュール100または任意の他の産業用エレメント/コントローラ306によって実行される前に、アクション認証器304によって(例えば、スマート・カード324等によって)認証シーケンスを実行するように構成することもできる。例えば、いわゆる「ハンドシェイク」を、ステップ410の前またはステップ406の前に実行することもできる。ある実施形態では、署名および検証ステップ404および408を、一層複雑な認証シーケンスと完全に置き換えることができる。あるいは、もっと簡単な署名検証および/または解読手段(measure)を増やすために、認証シーケンスを追加のセキュリティ手段として実行することもできる。

**【0068】**

[0082] ある実施形態では、I/Oモジュール100または任意の他の産業用エレメント/コントローラ306によって実施される認証シーケンスは、以下のステップを含むことができる。要求データグラムをアクション認証器304に送るステップ。要求データグラムは、第1ノンス(nonce)と、第1デバイス認証鍵証明書(例えば、デバイス認証鍵を含む第1認証証明書)と、第1識別情報属性証明書とを含む。アクション認証器304から応答データグラムを受け取るステップ。応答データグラムは、第2ノンスと、第1および第2ノンスに関連付けられた第1署名と、第2デバイス認証鍵証明書(例えば、デバイス認証鍵を含む第2認証証明書)と、第2識別情報属性証明書とを含む。第1および第2ノンスに関連付けられた第1署名と、第2デバイス認証鍵証明書と、第2識別情報属性証明書とを検証することによって、応答データグラムの有効性を判断するステップ。応答データグラムが有効であるときに、認証データグラムをアクション認証器304に送るステップ。認証データグラムは、第1および第2ノンスに関連付けられた第2署名を含む。

10

20

**【0069】**

[0083] あるいは、アクション認証器304は、ハンドシェイクを開始することができ、その場合、I/Oモジュール100または任意の他の産業用エレメント/コントローラ306によって実施される認証シーケンスは次のステップを含むことができる。アクション認証器304から要求データグラムを受け取るステップ。要求データグラムは、第1ノンスと、第1デバイス認証鍵証明書と、第1識別情報属性証明書とを含む。第1デバイス認証鍵証明書および第1識別情報属性証明書を検証することによって、要求データグラムの有効性を判断するステップ。要求データグラムが有効であるとき、応答データグラムをアクション認証器304に送るステップ。応答データグラムは、第2ノンスと、第1および第2ノンスに関連付けられた第1署名と、第2デバイス認証鍵証明書と、第2識別情報属性証明書とを含む。アクション認証器304から認証データグラムを受け取るステップ。認証データグラムは、第1および第2ノンスに関連付けられた第2署名を含む。第1および第2ノンスに関連付けられた第2署名を検証することによって、認証データグラムの有効性を判断するステップ。

30

**【0070】**

[0084] I/Oモジュール100または任意の他の産業用エレメント/コントローラ306およびアクション認証器304によって実施することができるハンドシェイクまたは認証シーケンスについては、米国特許出願第14/519,047号に更に記載されている。この特許出願をここで引用したことにより、その内容が全体的に本願にも含まれるものとする。尚、冗長通信/制御モジュール106間におけるハンドシェイクは、本明細書において説明したI/Oモジュール100または任意の他の産業用エレメント/コントローラ306とアクション認証器304との間におけるハンドシェイクに適用可能性であることを、当業者は認めよう。

40

**【0071】**

[0085] アクション発起元302、アクション認証器304、およびI/Oモジュール100または任意の他の産業用エレメント/コントローラ306の各々は、本明細書において説明した機能または動作(例えば、方法400のブロックおよび認証シーケンス)を実行することを可能にされた回路および/またはロジックを含むことができる。例えば、

50

アクション発起元 302、アクション認証器 304、および I/O モジュール 100 または任意の他の産業用エレメント/コントローラ 306 の各々は、限定ではないが、ハード・ディスク・ドライブ (HDD)、ソリッド・ステート・ディスク (SSD)、光ディスク、磁気記憶デバイス、フラッシュ・ドライブ、または SD/マイクロ SD カードのような、非一時的機械読み取り可能媒体によって永続的、半永続的、または一時的に格納されたプログラム命令を実行する 1 つ以上のプロセッサを含むことができる。

#### 【0072】

[0086] 以上で論じたように、2 つ以上の I/O モジュール 100 が互いに並列に接続されてもよく、そして互いに通信することが可能であるとよい。ある実施形態では、更にセキュリティ強化のために、I/O モジュール 100 は、始動、リセット、新たな I/O モジュール 100 の設置、I/O モジュール 100 の交換、周期的、予定された時点等のように、予め定められたイベントまたは時点において、互いに認証し合うために認証シーケンスまたはハンドシェイクを実行するように構成される。I/O モジュール 100 に互いに認証させることによって、I/O モジュール 100 によって悪意をもって混入される偽造を回避することができる。

10

#### 【0073】

[0087] 図 13 は、認証シーケンスの実行において 2 つの I/O モジュール 100 (例えば、第 1 I/O モジュール 100A および第 2 I/O モジュール 100B) との間において送信されるデータグラム例 500 を示す。認証シーケンスを開始するために、第 1 I/O モジュール 100A は、要求データグラム 502 を第 2 I/O モジュール 100B に送信するように構成される。実装態様では、要求データグラム 502 は、第 1 平文ノンス (Nonce A)、第 1 デバイス認証鍵 (DAKA) を含む第 1 デバイス認証鍵証明書 (CertDAKA)、および第 1 識別情報属性証明書 (IACA) を含む。ある実施形態では、第 1 I/O モジュール 100A は、真正乱数生成器 (以後「TRNG」) によって第 1 ノンス (Nonce A) を生成し、第 1 ノンス (Nonce A)、第 1 デバイス認証鍵証明書 (CertDAKA)、および第 1 識別情報属性証明書 (IACA) を連結して、または言い換えると組み合わせて、要求データグラム 502 を生成するように構成される。ある実施形態では、第 1 デバイス認証鍵証明書 (CertDAKA) および第 1 識別情報属性証明書 (IACA) は、第 1 I/O モジュール 100A によってローカルに格納される。例えば、これらの証明書が第 1 I/O モジュール 100A のローカル・メモリ (例えば、ROM、RAM、フラッシュ・メモリ、または他の非一時的記憶媒体) に格納されるのもよい。

20

30

[0088] 第 2 I/O モジュール 100B は、第 1 デバイス認証鍵証明書 (CertDAKA) および第 1 識別情報属性証明書 (IACA) を、デバイス寿命管理システム (DLM) によって生成されるまたは暗号ライブラリ機能を利用して導き出される公開鍵によって検証することにより、要求データグラムの有効性を判断するように構成される。これに関して、公開鍵は、I/O モジュール 100 の SRAM または他のローカル・メモリに格納され、I/O モジュール 100 間で交換されるノンスのように、交換されるデータを検証するためまたは暗号で署名するために暗号ライブラリ機能と共に使用することができる。ある実施形態では、第 2 I/O モジュール 100B は、楕円曲線デジタル署名アルゴリズム (以後「ECDSA」: elliptic curve digital signing algorithm) または他の検証処理によって証明書を検証することもできる。ある実施形態では、第 2 I/O モジュール 100B が、更に、以下のことを検証することによって、平文値からの証明書値 (certificate value) の有効性を判断するように構成されてもよい。証明書のタイプが、各証明書に対してデバイス認証鍵 (以後「DAK」) または識別情報属性証明書 (以後「IAC」) である。IAC 名称が一致し、DAK 証明書モジュール・タイプがモジュール・タイプ引数と一致する。および/またはメッセージ・ペイロード内における各証明書のマイクロプロセッサ連番 (以後「MPSN」) が互いに一致する。ある実施形態では、第 2 I/O モジュール 100B が、更に、DAK および IAC 証明書がローカル失効リスト (local revocation list) (例えば、失効された証明書および/または無効の証明書を含むデー

40

50

データベースのリスト)にないことを検証するように構成されてもよい。第2 I/Oモジュール100Bが要求データグラムの有効性を判断できなかったとき、第2 I/Oモジュール100Bはエラー・メッセージを生成し、部分的にまたは完全に第1 I/Oモジュール100Aを使用不可にし、および/または第1 I/Oモジュール100Aへ/からの通信を切断または制限することができる。

#### 【0074】

[0089] 有効な要求データグラム502に回答して、第2 I/Oモジュール100Bは、応答データグラム504を第1 I/Oモジュール100Aに送信するように構成される。実装態様では、応答データグラム504は、第2 平文ノンス(Nonce B)、第1および第2 ノンスに関連付けられた第1署名(Sig B[Nonce A || Nonce B])、第2 デバイス認証鍵(DAK B)を含む第2 デバイス認証鍵証明書(Cert DAK B)、および第2 識別情報属性証明書(IAC B)を含む。ある実施形態では、第2 I/Oモジュール100Bは、TRNGによって第2 ノンス(Nonce B)を生成し、第1 ノンス(Nonce A)および第2 ノンス(Nonce B)を連結し、または言い換えると組み合わせ、連結された/組み合わせられたノンスに、第2 I/Oモジュール100Bによってローカルに格納されている秘密鍵(例えば、DAK)によって署名するように構成される。第2 I/Oモジュール100Bは、更に、第2 ノンス(Nonce B)、第1および第2 ノンスに関連付けられた第1署名(Sig B[Nonce A || Nonce B])、第2 デバイス認証鍵証明書(Cert DAK B)、および第2 識別情報属性証明書(IAC B)を連結してまたは言い換えると組み合わせ、応答データグラム504を生成するように構成される。ある実施形態では、第2 デバイス認証鍵証明書(Cert DAK B)および第2 識別情報属性証明書(IAC B)は、第2 I/Oモジュール100Bによってローカルに格納される。例えば、これらの証明書は、第2 I/Oモジュール100Bのローカル・メモリ(例えば、ROM、RAM、フラッシュ・メモリ、または他の非一時的記憶媒体)に格納されるのもよい。

10

20

#### 【0075】

[0090] 第1 I/Oモジュール100Aは、第2 デバイス認証鍵証明書(Cert DAK B)および第2 識別情報属性証明書(IAC B)を、ローカルに格納されている公開鍵または暗号ライブラリから引き出された公開鍵によって、ECDSAまたは他の検証処理を利用して検証することによって、応答データグラムの有効性を判断するように構成される。ある実施形態では、第1 I/Oモジュール100Aは、更に、以下のことを検証することによって、平文値からの証明書値(certificate value)の有効性を判断するように構成されてもよい。IACおよびDAK証明書が一致するMPSNを有する。IAC名称が一致する。両方の証明書(IACおよびDAK)について、証明書タイプが正しい。正しいソース名称が両方の証明書上にある。DAKモジュール・タイプが正しいタイプである(例えば、モジュール・タイプ=通信/制御モジュールであるか否か確認するためのチェック)。ある実施形態では、第1 I/Oモジュール100Aが、更に、DAKおよびIAC証明書がローカル失効リストにないことを検証するように構成されるのもよい。

30

#### 【0076】

[0091] 応答データグラムの有効性を判断するために、第1 I/Oモジュール100Aは、更に、第1および第2 ノンスに関連付けられた第1署名(Sig B[Nonce A || Nonce B])を検証するように構成されてもよい。ある実施形態では、第1 I/Oモジュール100Aは、第1のローカルに格納されたノンス(Nonce A)と、第2 I/Oモジュール100Bから受けた第2 平文ノンス(Nonce B)とを連結し、第1暗号署名(Sig B[Nonce A || Nonce B])を公開デバイス認証鍵によって検証し(例えば、Cert DAK BからのDAK Bを使用して)、ローカルに生成された第1 ノンスおよび第2 ノンスの連結を、第1 ノンスおよび第2 ノンスの暗号的に検証された連結と比較することによって、第1署名(Sig B[Nonce A || Nonce B])を検証するように構成される。第1 I/Oモジュール100Aが応答データグラムの有効性を判断できなかったとき、第1 I/Oモジュール100Aは、エラー・メッセージを生

40

50

成し、部分的または完全に第2 I/Oモジュール100Bを使用不可にし、および/または第2 I/Oモジュール100Bへ/からの通信を切断または制限することができる。

【0077】

[0092] 更に、第1 I/Oモジュール100Aは、応答データグラム504が有効であるとき、認証データグラム506を第2 I/Oモジュール100Bに送信するように構成される。実装態様では、認証データグラム506は、第1および第2ノンスに関連付けられた第2署名(`sigA[NonceA||NonceB]`)を含む。ある実施形態では、第1 I/Oモジュール100Aは、ローカルに生成された第1および第2ノンスの連結に、第1 I/Oモジュール100Aによってローカルに格納されている秘密鍵(例えば、`DAK`)によって署名するように構成される。応答データグラムが無効である場合、認証データグラム506を、第2ノンスに関連付けられた署名と、第1 I/Oモジュール100Aによって生成されたエラー報告(例えば、「失敗」(`failure`))メッセージ(`sigA[NonceA||Error]`)とを含む「失敗」認証データグラム506と置き換えることができる。

10

【0078】

[0093] 認証データグラム506に回答して、第2 I/Oモジュール100Bは、更に、応答認証データグラム508を第1 I/Oモジュール100Aに送信するように構成することができる。実装態様では、応答認証データグラム508は、第1ノンスに関連付けられた署名と、第2 I/Oモジュール100Bによって生成されたエラー報告(例えば、「成功」または「失敗」)メッセージ(`SigB[NonceA||Error]`)を含む。ある実施形態では、第2 I/Oモジュール100Bは、第1および第2ノンスに関連付けられた第2署名(`sigA[NonceA||NonceB]`)を検証することによって、認証データグラム506の有効性を確認するように構成される。ある実施形態では、第2 I/Oモジュール100Bは、第1 I/Oモジュール100Aから受けた第1平文ノンス(`NonceA`)および第2のローカルに格納されているノンス(`NonceB`)を連結し、第2暗号署名(`sigA[NonceA||NonceB]`)を公開デバイス認証鍵によって検証し(例えば、`CertDAKA`からの`DAKA`を使用して)、第1ノンスおよび第2ノンスのローカルに生成された連結を、第1ノンスおよび第2ノンスの暗号的に検証された連結と比較することによって、第2署名(`sigA[NonceA||NonceB]`)を検証するように構成される。エラー報告メッセージに加えて、第2 I/Oモジュール100Bが認証データグラムの有効性を判断できなかったとき、第2 I/Oモジュール100Bは、部分的または完全に第1 I/Oモジュール100Aを使用不可にし、および/または第1 I/Oモジュール100Aへ/からの通信を切断または制限することができる。

20

30

【0079】

[0094] I/Oモジュール100が「マスタ-スレーブ」構成にしたがって配置される実装態様では、マスタ(例えば、第1 I/Oモジュール100A)が各スレーブを認証するように構成することができる。認証失敗の場合、マスタは、認証されなかったスレーブへ/からの通信を少なくとも部分的に使用不可にまたは制限することができる。あるいは、2つ以上のスレーブI/Oモジュール100および/またはマスタなしで並列に動作する2つ以上のI/Oモジュール100が、互いに認証するのでもよい。認証失敗の結果、デバイスまたは擬似副デバイス(例えば、始動元でないI/Oモジュール)の双方を部分的にまたは完全に使用不可にするのでもよい。例えば、2つ以上の冗長なI/Oモジュール100が、始動時または他の予め定められた時点/イベントにおいて認証シーケンスを完了することに成功しなかった場合、これらを使用不可にすることができる。

40

【0080】

[0095] 各I/Oモジュール100は、本明細書において説明した機能を実行するために使用可能にされる回路および/またはロジックを含むこともできる。例えば、コントローラ106は、ハード・ディスク・ドライブ(HDD)、ソリッド・ステート・ディスク(SDD)、光ディスク、磁気記憶デバイス、フラッシュ・ドライブ等のような、非一時

50

的機械読み取り可能媒体 108 によって永続的、半永続的、または一時的に格納されたプログラムを実行するように構成されるのでもよい。したがって、コントローラ 106 は、図 14 および図 15 にそれぞれ示される認証開始シーケンス 600 および / または認証応答シーケンス 700 を実行するように構成することができる。

#### 【0081】

[0096] 図 14 を参照すると、第 1 I/O モジュール 100A (即ち、開始側) によって実施される認証開始シーケンス 600 は、次のステップを含むことができる。要求データグラムを第 2 I/O モジュール 100B (即ち、応答側) に送るステップ (602)。要求データグラムは、第 1 ノンス、第 1 デバイス認証鍵証明書、および第 1 識別情報属性証明書を含む。第 2 I/O モジュール 100B から応答データグラムを受信するステップ (604)。応答データグラムは、第 2 ノンス、第 1 および第 2 ノンスに関連付けられた第 1 署名、第 2 デバイス認証鍵証明書、ならびに第 2 識別情報属性証明書を含む。第 1 および第 2 ノンスに関連付けられた第 1 署名、第 2 デバイス認証鍵証明書、および第 2 識別情報属性証明書を検証することによって応答データグラムの有効性を判断するステップ (606)。応答データグラムが有効であるとき、認証データグラムを第 2 I/O モジュール 100B に送るステップ (610)。認証データグラムは、第 1 および第 2 ノンスに関連付けられた第 2 署名を含む。または、応答データグラムが無効であるときに、不良認証データグラムを第 2 I/O モジュール 100B に送るステップ (608)。不良認証データグラムは、第 2 ノンスに関連付けられた署名およびエラー・メッセージを含む。

10

#### 【0082】

[0097] 図 15 を参照すると、認証応答シーケンス 700 (例えば、第 2 I/O モジュール 100B によって実施される) は、次のステップを含むことができる。第 1 I/O モジュール 100A から要求データグラムを受けるステップ (702)。要求データグラムは、第 1 ノンス、第 1 デバイス認証鍵証明書、および第 1 識別情報属性証明書を含む。第 1 デバイス認証鍵証明書および第 1 識別情報属性証明書を検証することによって、要求データグラムの有効性を判断するステップ (704)。要求データグラムが有効であるとき、第 1 I/O モジュール 100A に応答データグラムを送るステップ (706)。応答データグラムは、第 2 ノンス、第 1 および第 2 ノンスに関連付けられた第 1 署名、第 2 デバイス認証鍵証明書、および第 2 識別情報属性証明書を含む。第 1 I/O モジュール 100A から認証データグラムを受けるステップ (708)。認証データグラムは、第 1 および第 2 ノンスに関連付けられた第 2 署名を含む。第 1 および第 2 ノンスに関連付けられた第 2 署名を検証することによって、認証データグラムの有効性を判断するステップ (710)。第 1 I/O モジュール 100A に応答認証データグラムを送るステップ (712)。応答認証データグラムは、第 1 ノンスに関連付けられた署名、および成功または失敗メッセージを含む。

20

30

#### 【0083】

[0098] ある実施形態では、I/O モジュール 100 は、更に、通信/制御モジュール 214、フィールド・デバイス 217 (例えば、センサ 218 またはアクチュエータ 220)、電力モジュール 232、物理相互接続デバイス、スイッチ等のような、産業用制御システム 200 の他のエレメントと認証する、および / または他のエレメントによって認証されるように構成することもできる。産業用コントローラ/エレメントは、前述した認証シーケンス (冗長 I/O モジュール 100 間) のようなシーケンスまたはハンドシェイクを実行することによって、互いにまたは他のデバイスを認証するように構成することができる。例えば、I/O モジュール 100 は、通信/制御モジュール 214 またはフィールド・デバイス 217 と認証シーケンスを実行するように構成することができる (例えば、前述のように)。更に、通信可能に結合されたフィールド・デバイス 217 (例えば、センサ 218 またはアクチュエータ 220) は、以上で説明した認証プロセスと同様なやり方で互いに認証するように構成することも考えられる。

40

#### 【0084】

[0099] 尚、本明細書において説明した機能はいずれも、ハードウェア (例えば、集積

50

回路のような固定ロジック回路)、ソフトウェア、ファームウェア、手動処理、またはその組み合わせによって実現できることは理解されてしかるべきである。つまり、以上の開示において論じたブロック、動作、機能、またはステップは、総合的に、ハードウェア(例えば、集積回路のような固定ロジック回路)、ソフトウェア、ファームウェア、またはその組み合わせを表す。ハードウェア構成の実例では、以上の開示において論じた種々のブロックは、他の機能と共に集積回路として実現することもできる。このような集積回路は、所与のブロック、システム、または回路の機能の全て、あるいはこれらのブロック、システム、または回路の機能の一部を含むのでもよい。更に、ブロック、システム、回路の要素は、多数の集積回路にわたって実装することもできる。このような集積回路は、モノリシック集積回路、フリップ・フロップ集積回路、マルチチップ・モジュール集積回路、および/または混合信号集積回路を含む種々の集積回路を含むことができるが、必ずしもこれらに限定されるのではない。ソフトウェア実装態様の実例では、以上の開示において論じた種々のブロックは、プロセッサ上で実行されると、指定されたタスクを実行する実行可能命令(例えば、プログラム・コード)を表す。これらの実行可能命令は、1つ以上の有形コンピュータ読み取り可能媒体に格納することができる。このような実例の一部では、システム、ブロック、または回路全体が、そのソフトウェアまたはファームウェアの同等物を使用して実現されることも可能である。他の実例では、所与のシステム、ブロック、または回路の一部がソフトウェアまたはファームウェアで実現され、他の部分がハードウェアで実現されてもよい。

10

20

【0085】

[0100] 以上、構造的特徴および/またはプロセス動作に特定の文言で主題について説明したが、添付した特許請求の範囲において定められる主題は、以上で説明した特定の特徴やアクトに必ずしも限定されないことは理解されてしかるべきである。逆に、以上で説明した特定の主題は、特許請求の範囲を実現する形態例として開示されたものである。

【図1】

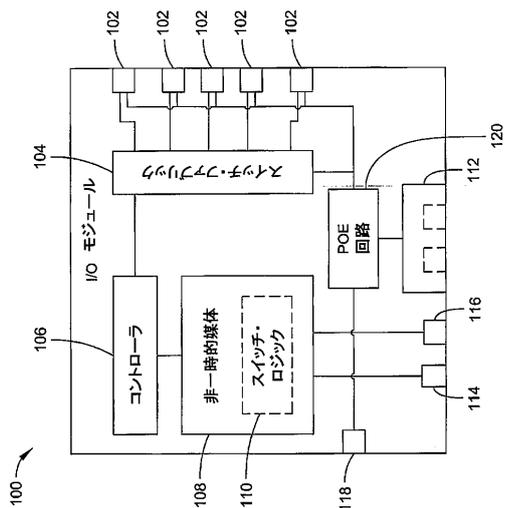


FIG. 1

【図2】

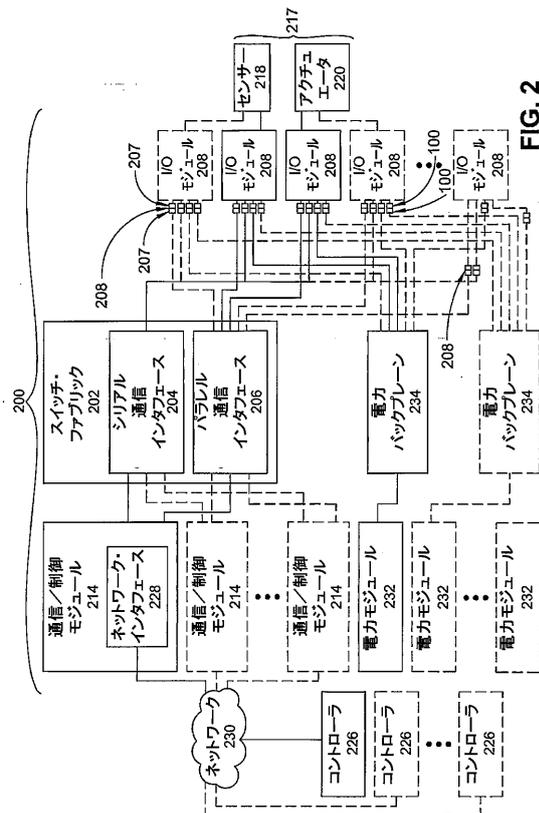


FIG. 2

【 図 3 】

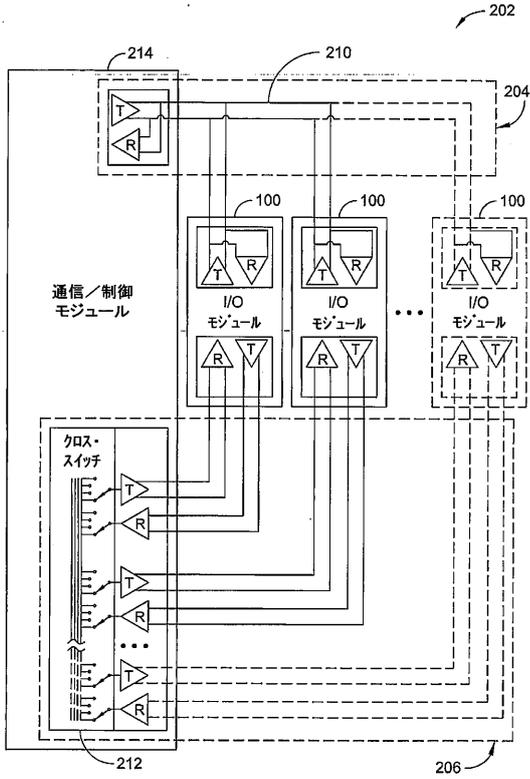


FIG. 3

【 図 4 】

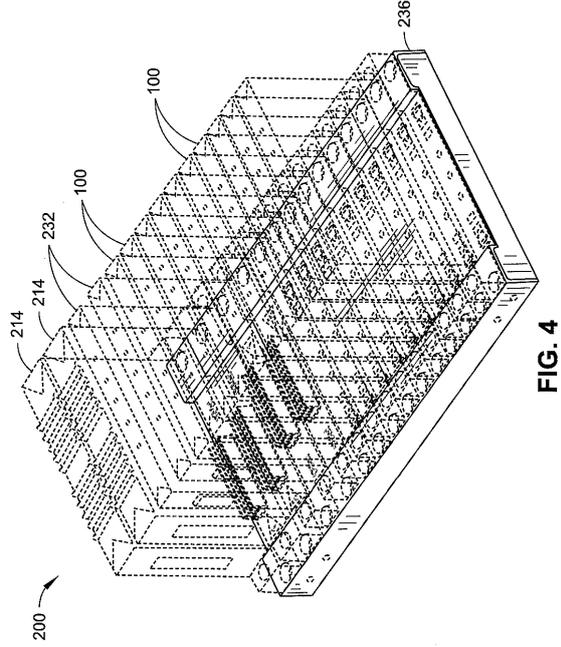


FIG. 4

【 図 5 】

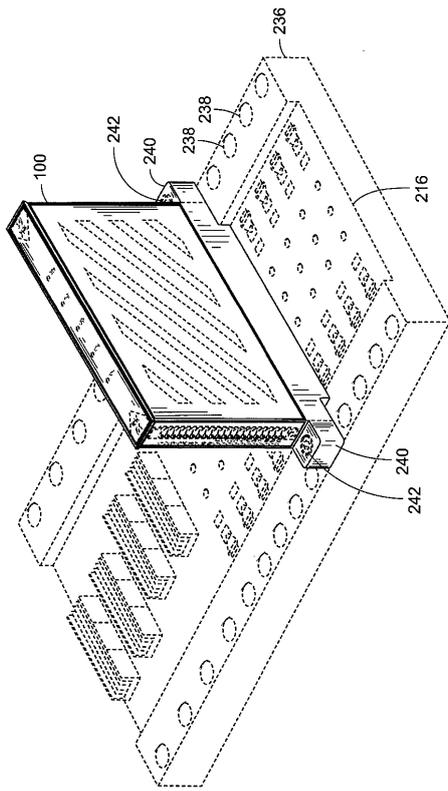


FIG. 5

【 図 6 】

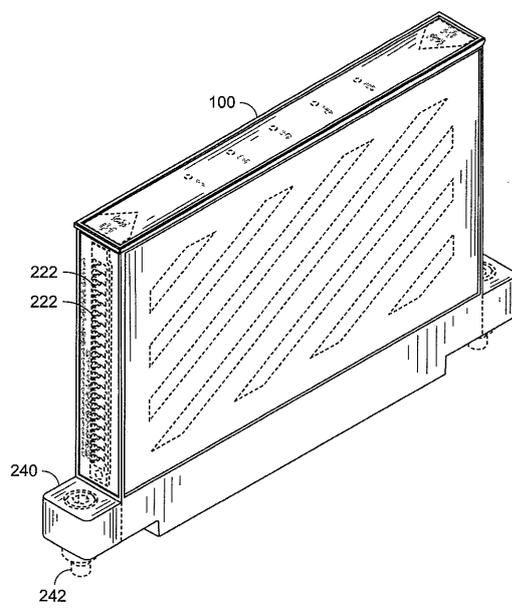


FIG. 6

【 図 7 】

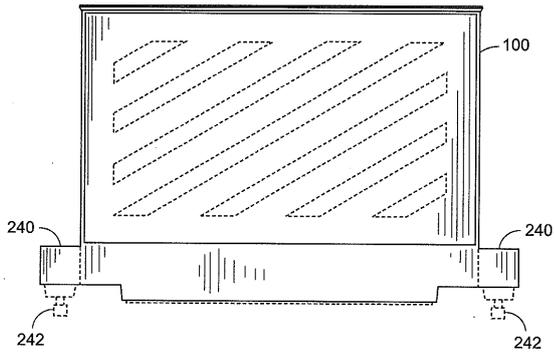


FIG. 7

【 図 8 】

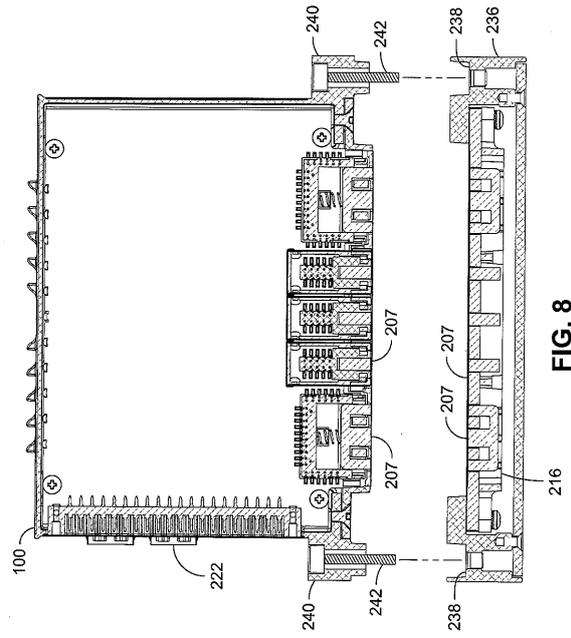


FIG. 8

【 図 9 】

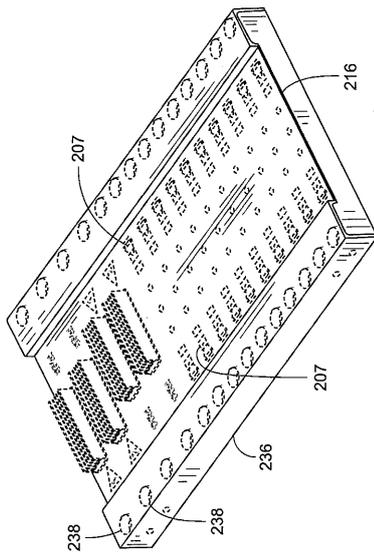


FIG. 9

【 図 10 】

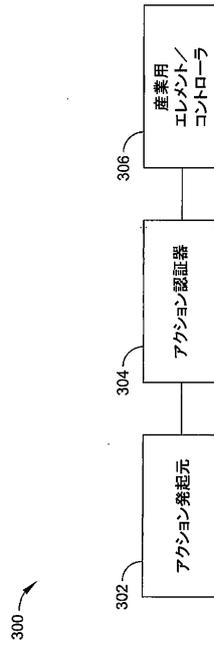


FIG. 10

【図 1 1】

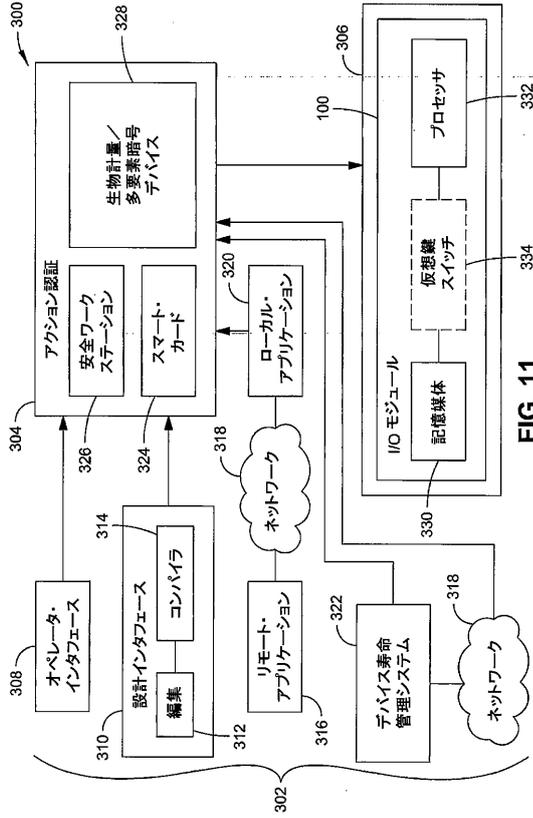


FIG. 11

【図 1 2】

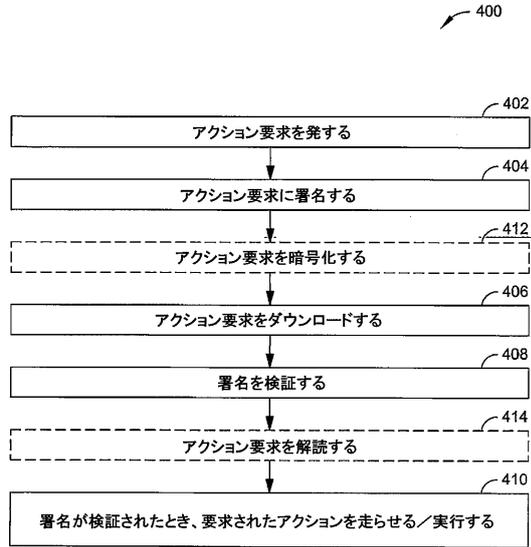


FIG. 12

【図 1 3】

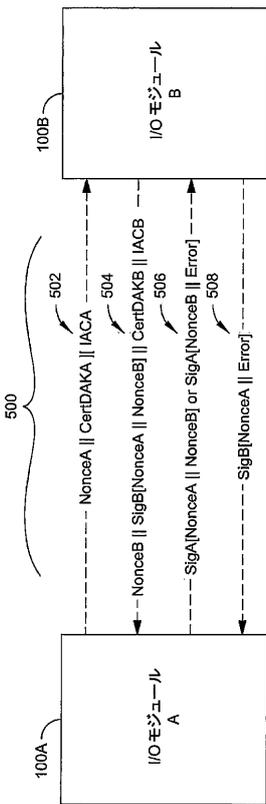


FIG. 13

【図 1 4】

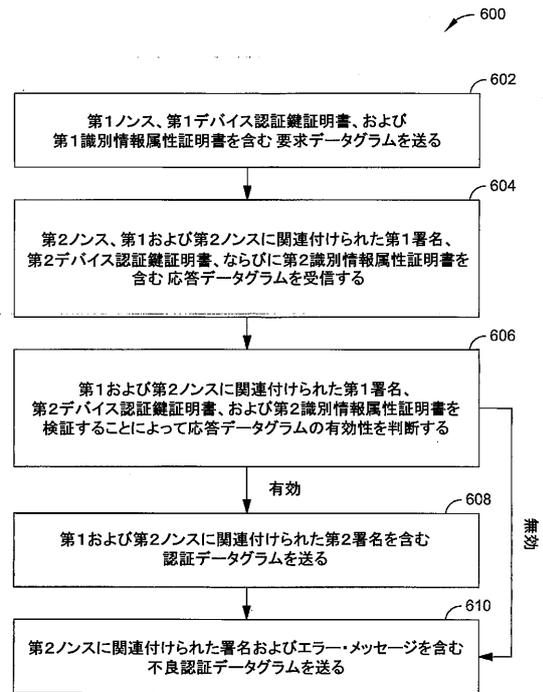


FIG. 14

【 図 1 5 】

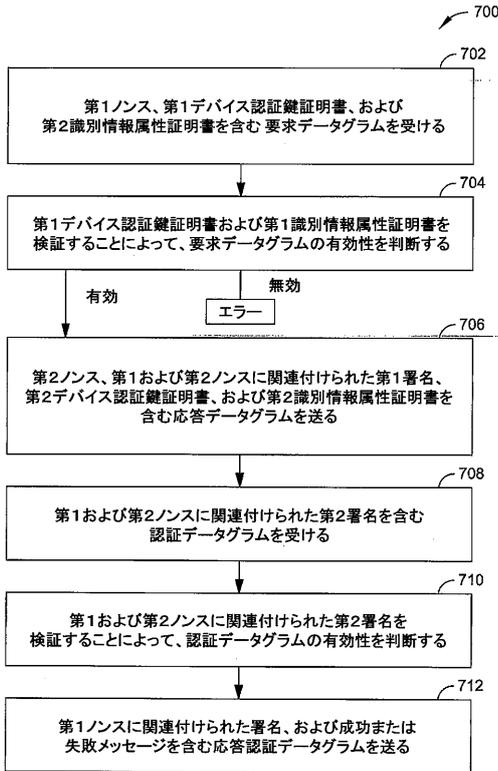


FIG. 15

## 【 手続 補正 書 】

【 提出 日 】 令和3年10月13日 (2021.10.13)

## 【 手続 補正 1 】

【 補正 対象 書類 名 】 特許 請求 の 範囲

【 補正 対象 項目 名 】 全文

【 補正 方法 】 変更

【 補正 の 内容 】

【 特許 請求 の 範囲 】

【 請 求 項 1 】

制御システムであって、

支持フレームと、

制御モジュールであって、前記支持フレームと嵌合し、前記制御モジュールと前記支持フレームとの間に通信可能な結合を提供するように構成された第1ケースを有する制御モジュールと、

入力/出力モジュールであって、前記支持フレームと嵌合し、前記入力/出力モジュールと前記支持フレームとの間に通信可能な結合を提供することにより、前記支持フレームを通じて、前記制御モジュールと前記入力/出力モジュールとの間に通信可能な結合を提供するように構成された第2ケースを有する、入力/出力モジュールと、を備え、

前記入力/出力モジュールが、前記第2ケース内に複数の通信チャネルを含み、該複数の通信チャネルの各チャネルが、1つ以上のフィールド・デバイスに接続するように構成され、

前記入力/出力モジュールが、更に、前記第2ケース内にスイッチ・ファブリックを含み、前記スイッチ・ファブリックが、前記複数の通信チャネルを通じて、前記制御モジュールと前記1つ以上のフィールド・デバイスとの間に接続性を選択的に促進するように構成され、

前記入力/出力モジュールが、更に、前記スイッチ・ファブリックに結合されたコントローラを含み、該コントローラが、前記複数の通信チャンネルを通じて同時に通信するように構成され、前記複数の通信チャンネルが、前記複数の通信チャンネルのそれぞれのチャンネル上で同時に起動する多数の通信規格を使用し、該多数の通信規格が少なくとも2つの異なる通信規格を含み、該少なくとも2つの異なる通信規格が、イーサネット・バス、H1フィールド・バス、プロセス・フィールド・バス（PROFIBUS）、ハイウェイ・アドレスابل・リモート・トランスデューサ（HART）バス、Modbus、並びに、プロセス制御統一アーキテクチャ用オブジェクト連携および埋め込み（OPCUA）バスの内少なくとも1つを含む、制御システム。

【請求項2】

請求項1記載の制御システムにおいて、前記制御モジュールは、前記入力/出力モジュールが物理的に前記制御モジュールに接続される物理的位置に関連付けられた一意の識別子を、前記入力/出力モジュールに割り当てるように構成される、制御システム。

【請求項3】

請求項1記載の制御システムであって、更に、電力を前記入力/出力モジュールに供給する電源モジュールを含む、制御システム。

【請求項4】

請求項1記載の制御システムにおいて、前記入力/出力モジュールが、前記複数の通信チャンネルのそれぞれのチャンネルを通じて、電力を少なくとも1つのフィールド・デバイスに供給するように構成される、制御システム。

【請求項5】

請求項1記載の制御システムにおいて、前記複数の通信チャンネルが複数のイーサネット・チャンネルを備える、制御システム。

【請求項6】

請求項1記載の制御システムにおいて、前記複数の通信チャンネルが、イーサネット・バス、H1フィールド・バス、プロセス・フィールド・バス（PROFIBUS）、ハイウェイ・アドレスابل・リモート・トランスデューサ（HART）バス、Modbus、または、プロセス制御統一アーキテクチャ用オブジェクト連携および埋め込み（OPCUA）バスの内少なくとも2つを含む、制御システム。

【請求項7】

請求項1記載の制御システムにおいて、前記入力/出力モジュールが、プロセス制御統一アーキテクチャ用オブジェクト連携および埋め込み（OPCUA）クライアントまたはOPCUAサーバの内少なくとも1つとして動作可能である、制御システム。

【請求項8】

請求項1記載の制御システムにおいて、前記入力/出力モジュールが、IEEE1588タイミング・プロトコルにしたがって、前記1つ以上のフィールド・デバイスを同期させるように構成される、制御システム。

【請求項9】

請求項1記載の制御システムであって、更に、前記入力/出力モジュールと通信可能なデバイス寿命管理システムを含み、該デバイス寿命管理システムが前記1つ以上のフィールド・デバイスを認証するように構成される、制御システム。

【請求項10】

請求項1記載の制御システムであって、更に、前記入力/出力モジュールを前記制御モジュールに接続するように構成されたシリアル通信インタフェースであって、前記入力/出力モジュールを第2入力/出力モジュールと並列に接続し、前記シリアル通信インタフェースが、前記入力/出力モジュールと前記制御モジュールとの間で情報を送信するように構成される、シリアル通信インタフェースと、

前記入力/出力モジュールを前記制御モジュールに別個に接続するように構成されたパラレル通信インタフェースであって、前記入力/出力モジュールと前記制御モジュールとの間で情報を送信し、前記入力/出力モジュールと前記第2入力/出力モジュールとの間

で情報を送信するように構成される、パラレル通信インタフェースと、を備える、制御システム。

【請求項 1 1】

入力/出力モジュールであって、

支持フレームと嵌合する第 1 ケースであって、前記支持フレームが、外部制御モジュールの第 2 ケースと嵌合することにより、前記入力/出力モジュールと前記外部制御モジュールとの間に通信可能な結合を提供するように構成される、第 1 ケースと、

前記第 1 ケース内の複数の通信チャンネルであって、該複数の通信チャンネルの各チャンネルが、1 つ以上のフィールド・デバイスに接続するように構成される、複数の通信チャンネルと、

前記ケース内のスイッチ・ファブリックであって、前記複数の通信チャンネルを通じて、前記外部制御モジュールと前記 1 つ以上のフィールド・デバイスとの間に接続性を選択的に促進するように構成される、スイッチ・ファブリックと、

前記スイッチ・ファブリックに結合されたコントローラであって、前記複数の通信チャンネルを通じて同時に通信するように構成されるコントローラと、を備え、

前記複数の通信チャンネルが、前記複数の通信チャンネルのそれぞれのチャンネル上で同時に起動する多数の通信規格を使用し、前記多数の通信規格が少なくとも 2 つの異なる通信規格を含み、前記少なくとも 2 つの異なる通信規格が、イーサネット・バス、H 1 フィールド・バス、プロセス・フィールド・バス ( P R O F I B U S )、ハイウェイ・アドレスブル・リモート・トランスデューサ ( H A R T ) バス、M o d b u s、並びに、プロセス制御統一アーキテクチャ用オブジェクト連携および埋め込み ( O P C U A ) バスの内少なくとも 1 つを含む、入力/出力モジュール。

【請求項 1 2】

請求項 1 1 記載の入力/出力モジュールにおいて、前記複数の通信チャンネルが複数のイーサネット・チャンネルを含む、入力/出力モジュール。

【請求項 1 3】

請求項 1 2 記載の入力/出力モジュールにおいて、前記入力/出力モジュールが、前記複数のイーサネット・チャンネルのそれぞれのイーサネット・チャンネルを通じて、電力を少なくとも 1 つのフィールド・デバイスに供給するように構成される、入力/出力モジュール。

【請求項 1 4】

請求項 1 1 記載の入力/出力モジュールであって、前記複数の通信チャンネルが、イーサネット・バス、H 1 フィールド・バス、プロセス・フィールド・バス ( P R O F I B U S )、ハイウェイ・アドレスブル・リモート・トランスデューサ ( H A R T ) バス、M o d b u s、またはプロセス制御統一アーキテクチャ用オブジェクト連携および埋め込み ( O P C U A ) バスの内少なくとも 2 つを含む、入力/出力モジュール。

【請求項 1 5】

請求項 1 1 記載の入力/出力モジュールにおいて、前記コントローラが、プロセス制御統一アーキテクチャ用オブジェクト連携および埋め込み ( O P C U A ) クライアント通信/制御プロトコル、または O P C U A サーバ通信/制御プロトコルの内少なくとも 1 つとして起動するように構成される、入力/出力モジュール。

【請求項 1 6】

入力/出力モジュールであって、

支持フレームと嵌合するように構成される第 1 ケースであって、前記支持フレームが、外部制御モジュールの第 2 ケースと嵌合することにより、前記入力/出力モジュールと前記外部制御モジュールとの間に通信可能な結合を提供するように構成される、第 1 ケースと、

前記第 1 ケース内の複数の通信チャンネルであって、該複数の通信チャンネルの各チャンネルが、1 つ以上のフィールド・デバイスに接続するように構成される、複数の通信チャンネルと、

前記ケース内のスイッチ・ファブリックであって、前記複数の通信チャネルを通じて、前記外部制御モジュールと前記1つ以上のフィールド・デバイスとの間に接続性を選択的に促進するように構成される、スイッチ・ファブリックと、

前記スイッチ・ファブリックに結合されたコントローラであって、前記複数の通信チャネルのそれぞれのチャネル上で同時に起動する多数の通信規格に対応するように構成される、コントローラと、

前記入力/出力モジュールを前記制御モジュールに第2入力/出力モジュールと並列に接続するように構成されるシリアル通信ポートであって、前記入力/出力モジュールと前記制御モジュールとの間で情報を送信するように構成される、シリアル通信ポートと、

前記入力/出力モジュールを前記制御モジュールに別個に接続するように構成されたパラレル通信ポートであって、前記入力/出力モジュールと前記制御モジュールとの間で情報を送信し、前記入力/出力モジュールと前記第2入力/出力モジュールとの間で情報を送信するように構成される、パラレル通信ポートとを含む、入力/出力モジュール。

【請求項17】

請求項16記載の入力/出力モジュールにおいて、前記シリアル通信ポートまたは前記パラレル通信ポートの内少なくとも1つが、第1磁気回路部分を形成する電磁コネクタを備え、該電磁コネクタが、

第1コア部材と、

前記第1コア部材に配置された第1コイルと、  
を含み、

前記電磁コネクタが第2電磁コネクタと嵌合するように構成され、前記第2電磁コネクタが第2磁気回路部分を形成するように構成され、第2コア部材と該第2コア部材に配置された第2コイルとを備え、前記第1コア部材および前記第2コア部材が、前記第1コイルを前記第2コイルに結合するように構成され、前記電磁コネクタが前記第2電磁コネクタと嵌合されたとき、前記第1磁気回路部分および前記第2磁気回路部分によって磁気回路が形成され、前記磁気回路が、前記第2コイルが付勢されたときに、前記第1コイル内に信号を誘導するように構成される、入力/出力モジュール。

【請求項18】

請求項17記載の入力/出力モジュールにおいて、前記第1コイルが、印刷回路ボードに配置された平面巻線を備える、入力/出力モジュール。

【請求項19】

請求項17記載の入力/出力モジュールにおいて、前記第1コア部材がE字型コア部材を含む、入力/出力モジュール。

【請求項20】

請求項17記載の入力/出力モジュールにおいて、前記第1コア部材および前記第2コア部材によって形成された前記磁気回路がエア・ギャップを含む、入力/出力モジュール。

---

フロントページの続き

- (72)発明者 アルバート・ルーヤッカーズ  
アメリカ合衆国カリフォルニア州 9 4 0 8 7 , サニーヴェール, ルピス・ドライブ 8 2 3
- (72)発明者 ジェームズ・ジー・カルヴァン  
アメリカ合衆国マサチューセッツ州 0 2 7 0 3 , アトルボロ, ヘイゼルウッド・コート 1
- Fターム(参考) 5H220 AA01 AA08 AA09 BB09 CC03 CC10 CX05 JJ07 JJ12 JJ17

【外国語明細書】

2022003543000001.pdf