(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7029220号
(P7029220)

(45)発行日　令和4年3月3日(2022.3.3)

(24)登録日　令和4年2月22日(2022.2.22)

(51)国際特許分類
Ｇ０５Ｂ　19/05　(2006.01)

ＦＩ
Ｇ０５Ｂ　19/05　L

請求項の数　20　外国語出願　（全34頁）

(21)出願番号　特願2016-21763(P2016-21763)
(22)出願日　平成28年2月8日(2016.2.8)
(65)公開番号　特開2016-149128(P2016-149128A)
(43)公開日　平成28年8月18日(2016.8.18)
審査請求日　平成31年1月7日(2019.1.7)
審判番号　不服2020-16407(P2020-16407/J1)
審判請求日　令和2年11月30日(2020.11.30)
(31)優先権主張番号　62/114,030
(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)
最終頁に続く

(73)特許権者　514091080
ベドロック・オートメーション・プラットフォームズ・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
(74)代理人　100118902
弁理士　山本 修
(74)代理人　100106208
弁理士　宮前 徹
(74)代理人　100173565
弁理士　末松 亮太
(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
(72)発明者　アルバート・ルーヤッカーズ
最終頁に続く

(54)【発明の名称】　多チャネル切り替え能力を有する入力／出力モジュール

(57)【特許請求の範囲】
【請求項１】
制御システムであって、
支持フレームと係合するように構成される第１ケースを有する制御モジュールと、
前記支持フレームと係合するように構成される第２ケースを有する複数の入力／出力モジュールであって、該複数の入力／出力モジュールのそれぞれが、前記制御モジュールと通信可能に結合され、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・デバイスと接続するように構成され、前記複数の入力／出力モジュールのそれぞれが、更に、前記第２ケース内にスイッチ・ファブリックを含み、該スイッチ・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・デバイスとの間における接続性を選択的に促進するように構成される、入力／出力モジュールと、
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、前記複数の入力／出力モジュールのうちの入力／出力モジュールを、前記複数の入力／出力モジュールのうちの他の入力／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他の入力／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
を備え、前記入力／出力モジュールのそれぞれが、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成される、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、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力モジュールを含む、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、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。

【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・アドレサブル・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（ＯＰＣ ＵＡ）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（ＯＰＣ ＵＡ）クライアントまたはＯＰＣ ＵＡ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】
複数の入力／出力モジュールであって、
支持フレームと係合するように構成されるケースと、
前記ケース内の複数の通信チャネルであって、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る、複数の通信チャネルと、
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、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、
前記複数の入力／出力モジュールのうちの入力／出力モジュールを、前記外部制御モジュールに対し、前記複数の入力／出力モジュールのうちの他の入力／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外部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外部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外部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他の入力／出力モジュールとの間において情報を送信ように構成される、パラレル通信ポートと、
前記スイッチ・ファブリックに結合されたコントローラと、
を含み、前記コントローラが、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成される、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ネルが複数のイーサネット・チャネルを含む、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・チャネルのそれぞれのイーサネット・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、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、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・アドレサブル・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（ＯＰＣ ＵＡ）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】
請求項１３記載の入力／出力モジュールにおいて、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、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（ＯＰＣ ＵＡ）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。

【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１４／５９７，４９８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。

【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。

【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はブ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、宇宙ステーション等（例えば、過熱、換気、および空調（ＨＶＡＣ）機器およびエネルギ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。

【課題を解決するための手段】
【０００６】
[0006] 本開示は、多チャ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、複数の通信チャネルを含み、これらのチャネルの各々は、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。
【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。
【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／出力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）に応答して、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・アドレサブル・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（ＯＰＣ ＵＡ）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チャネルがＯＰＣ ＵＡプロトコルを起動し(run)、一方で第２チャネルがＰＲＯＦＩＢＵＳを実行している等であってもよい。
【００１２】
例示の実装態様
[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・チャネル等のような、複数の通信チャネル１０２を含むことができる。通信チャネル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ネルの内各チャネルは、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。
【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、ＯＰＣ ＵＡ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ＯＰＣ ＵＡ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。

【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ネル１０２が、コントローラ１０６によって、ＯＰＣ ＵＡ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ＯＰＣ ＵＡ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。

【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。

【００１６】

[0030] 通信チャネル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、この回路は受電した電力を通信チャネル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、ＰＥＯ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ネル１０２のために、ＰＯＥ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、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ネル１０２のＰＯＥ機能を使用不可にするように構成することができる。

【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、Ｉ－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・ネットワーキング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が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。
【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、締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。締りばめは、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でもよい(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でもよい。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、破砕）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。
【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でもよい。磁気回路は、電力または通信バックプレーン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。
【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。

【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 would

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。

【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。

【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。

【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マム可能クロス・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)のでなくてもよく、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。

【００３０】

[0044] パラレル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２

００／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ろう。

【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、およびパラレル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およびパラレル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およびパラレル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。

【００３２】

[0046] スイッチ・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、金属および鉱業、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消費を監視および制御するため）。

【００３３】

[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・データをディジタル・データに変換するように（例えば、アナログ／ディジタル変換器（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、ディジタル・データをアナログ・データに変換するように（例えば、ディジタル／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、ＯＰＣ ＵＡ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。

【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。

【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。

【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。

【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・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）変換器を含むのでもよい。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。

【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、ルーカル発電(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・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。

【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。

【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を含むのでもよい。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、ＰＣＢ２２４の熱面(thermal plane)に接続されて、ＰＣＢ２２４のコンポーネントによって発生される熱をＰＣＢ２２４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２ＩＤ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。

【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２

０２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。

【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。

【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／ＵＳ２０１３／０５３７２１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。

【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、ディジタル証明書、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。

【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。

【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）。

【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「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。

【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。

【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。

【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、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。

【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、ディジタル署名によって）を可能にする(provide)。

【００５９】

[0073] 実装態様では、認証プロセスは、異なる製造元／販売朋／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。

【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（ウィルス）、データ・マイニング・アプリケーション等の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。

【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。

【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が一緒に携行できることである。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。

【００６４】

[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３０４は、安全が確保されたワークステーション３２６を含むことができる。ワークステーション３２６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３２６は、生物計量または多要素暗号デバイス３２８（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３２８は、スマート・カード３２４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。

【００６５】

[0079] Ｉ／Ｏモジュール１００、またはアクション発起元３０２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３０６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３０６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３３０（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１００または任意の他の産業用エレメント／コントローラ３０６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３３２（例えば、コントローラ１０６）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３０２および／またはアクション認証器３３２によって暗号化され、プロセッサ３３２によって解読も行われなければならず、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１００または任意の他の産業用エレメント／コントローラ３０６は、仮想鍵スイッチ３３４（例えば、プロセッサ３３２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３３４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３３２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。

【００６６】

[0080] 図１２は、本明細書において説明したアクション認証パス３００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４００の流れ図を示す。実装態様では、方法４００は、産業用制御システム２００および／また産業用制御システム２００の認証パス３００によって明示することができる。方法４００は、アクション要求を発するステップ（４０２）（例えば、発起元／設計インタフェース３０８／３１０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３１６／３２０）によって）と、アクション認証器３０４によってアクション要求に署名するステップ（４０４）と、任意にアクション認証器３０４によってアクション要求を暗号化するステップ（４１２）と、署名されたアクション要求を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に送るまたはダウンロードするステップ（４０６）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（４０８）と、任意に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によってアクション要求を解読するステップ（４１４）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、要求されたアクションを実行するステップ（４１０）とを含む。

【００６７】

[0081] セキュリティ強化のために、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「ハンドシェーク」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。
【００６９】
[0083] あるいは、アクション認証器３０４は、ハンドシェー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。
【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ー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ークは、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ークに適用可能性であることを、当業者は認めよう。
【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、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（ＳＤＤ）、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ー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。
【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１Ｉ／Ｏモジュール１００Ａおよび第２Ｉ／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１Ｉ／Ｏモジュール１００Ａは、要求データグラム５０２を第２Ｉ／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（

ＮｏｎｃｅＡ）、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１Ｉ／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（ＮｏｎｃｅＡ）を生成し、第１ノンス（ＮｏｎｃｅＡ）、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１Ｉ／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１Ｉ／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）に格納されるのでもよい。

[0088] 第２Ｉ／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２Ｉ／Ｏモジュール１００Ｂは、楕円曲線ディ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２Ｉ／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２Ｉ／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２Ｉ／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２Ｉ／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１Ｉ／Ｏモジュール１００Ａを使用不可にし、および／または第１Ｉ／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に応答して、第２Ｉ／Ｏモジュール１００Ｂは、応答データグラム５０４を第１Ｉ／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（ＮｏｎｃｅＢ）、第１および第２ノンスに関連付けられた第１署名（ＳｉｇＢ［ＮｏｎｃｅＡ｜｜ＮｏｎｃｅＢ］）、第２デバイス認証鍵（ＤＡＫＢ）を含む第２デバイス認証鍵証明書（ＣｅｒｔＤＡＫＢ）、および第２識別情報属性証明書（ＩＡＣＢ）を含む。ある実施形態では、第２Ｉ／Ｏモジュール１００Ｂは、ＴＲＮＧによって第２ノンス（ＮｏｎｃｅＢ）を生成し、第１ノンス（ＮｏｎｃｅＡ）および第２ノンス（ＮｏｎｃｅＢ）を連結し、または言い換えると組み合わせ、連結された／組み合わされたノンスに、第２Ｉ／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２Ｉ／Ｏモジュール１００Ｂは、更に、第２ノンス（ＮｏｎｃｅＢ）、第１および第２ノンスに関連付けられた第１署名（ＳｉｇＢ［ＮｏｎｃｅＡ｜｜ＮｏｎｃｅＢ］）、第２デバイス認証鍵証明書（ＣｅｒｔＤＡＫＢ）、および第２識別情報属性証明書（ＩＡＣＢ）を連結してまたは言い換えると組み合わせて、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（ＣｅｒｔＤＡＫＢ

）および第２識別情報属性証明書（ＩＡＣＢ）は、第２Ｉ／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２Ｉ／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）に格納されるのでもよい。

【００７５】

[0090] 第１Ｉ／Ｏモジュール１００Ａは、第２デバイス認証鍵証明書（ＣｅｒｔＤＡＫＢ）および第２識別情報属性証明書（ＩＡＣＢ）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１Ｉ／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１Ｉ／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でもよい。

【００７６】

[0091] 応答データグラムの有効性を判断するために、第１Ｉ／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（ＳｉｇＢ［ＮｏｎｃｅＡ｜｜ＮｏｎｃｅＢ］）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１Ｉ／Ｏモジュール１００Ａは、第１のローカルに格納されたノンス（ＮｏｎｃｅＡ）と、第２Ｉ／Ｏモジュール１００Ｂから受けた第２平文ノンス（ＮｏｎｃｅＢ）とを連結し、第１暗号署名（ＳｉｇＢ［ＮｏｎｃｅＡ｜｜ＮｏｎｃｅＢ］）を公開デバイス認証鍵によって検証し（例えば、ＣｅｒｔＤＡＫＢからのＤＡＫＢ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（ＳｉｇＢ［ＮｏｎｃｅＡ｜｜ＮｏｎｃｅＢ］）を検証するように構成される。第１Ｉ／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１Ｉ／Ｏモジュール１００Ａは、エラー・メッセージを生成し、部分的または完全に第２Ｉ／Ｏモジュール１００Ｂを使用不可にし、および／または第２Ｉ／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１Ｉ／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２Ｉ／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１Ｉ／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１Ｉ／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１Ｉ／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。

【００７８】

[0093] 認証データグラム５０６に応答して、第２Ｉ／Ｏモジュール１００Ｂは、更に、応答認証データグラム５０８を第１Ｉ／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２Ｉ／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２Ｉ／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２Ｉ／Ｏモジュール１００Ｂは、第１Ｉ／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２Ｉ／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２Ｉ／Ｏモジュール１００Ｂは、部分的または完全に第１Ｉ／Ｏモジュール１００Ａを使用不可にし、および／または第１Ｉ／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。

【００７９】

[0094] Ｉ／Ｏモジュール１００が「マスター－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１Ｉ／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１／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。

【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１Ｉ／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２Ｉ／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２Ｉ／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２Ｉ／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２Ｉ／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。

【００８２】

[0097] 図１５を参照すると、認証応答シーケンス７００（例えば、第２Ｉ／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１Ｉ／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１Ｉ／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１Ｉ／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１Ｉ／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。

【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ー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できることも考えられる。

【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、回路のエレメントは、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。

【００８５】

[0100] 以上、構造的特徴および／またはプロセス動作に特定的な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まるべきである。逆に、以上で説明した特定の特徴やアクトは、特許請求の範囲を実現する形態例として開示されたまでである。

【図面】

【図１】

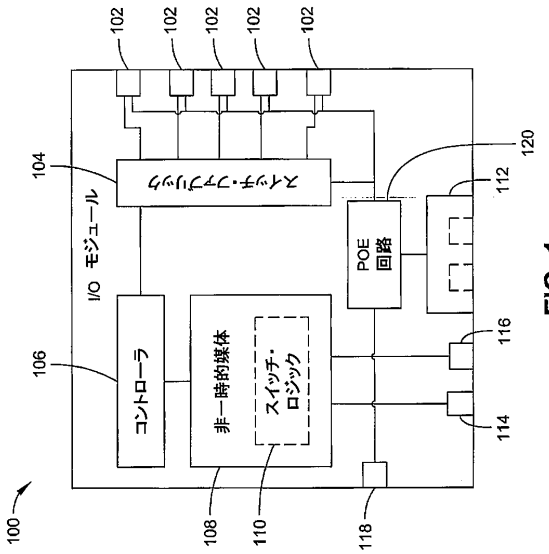

FIG. 1

【図２】

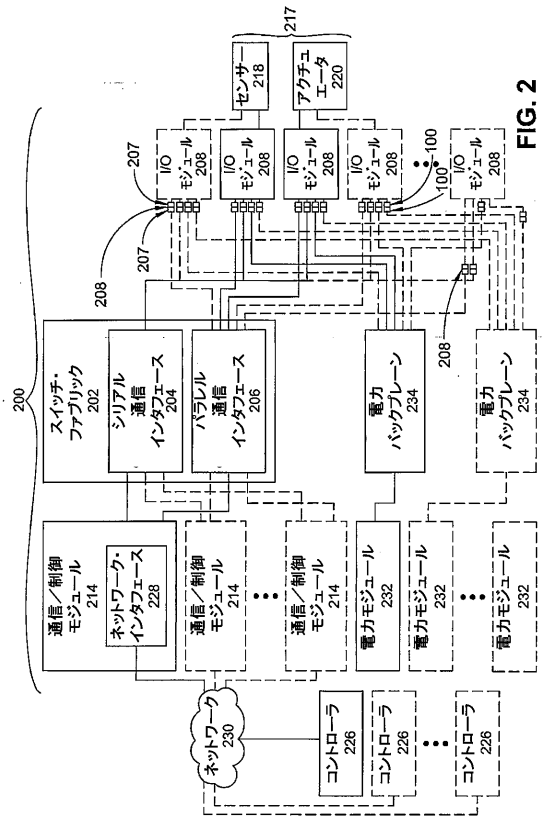

FIG. 2

【図３】

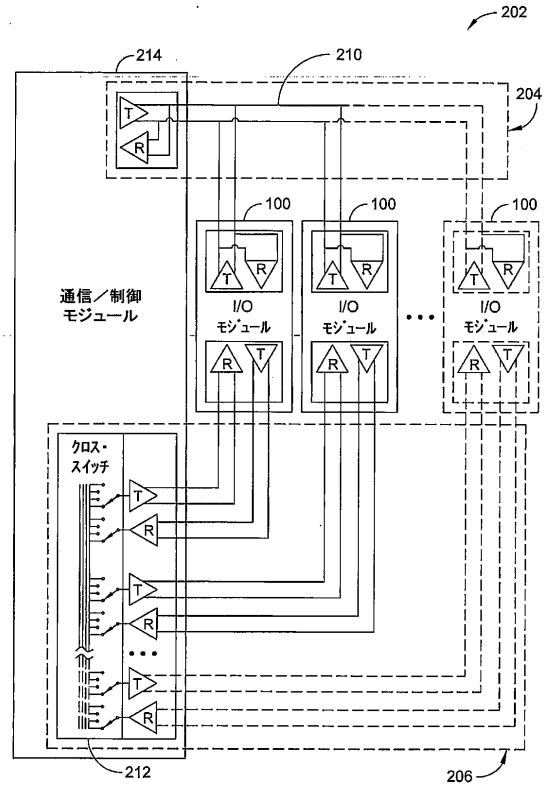

FIG. 3

【図４】

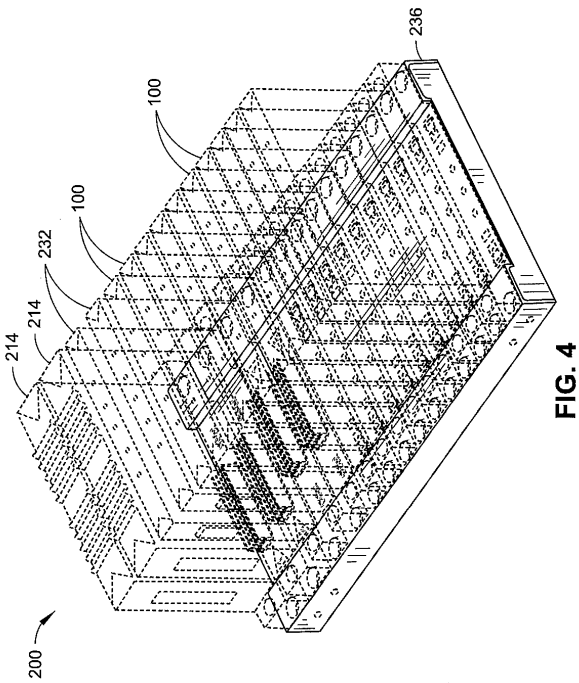

FIG. 4

【図５】

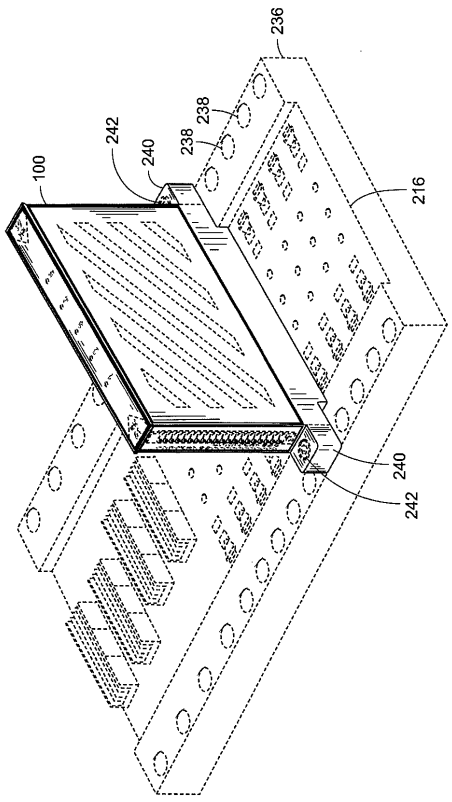

FIG. 5

【図６】

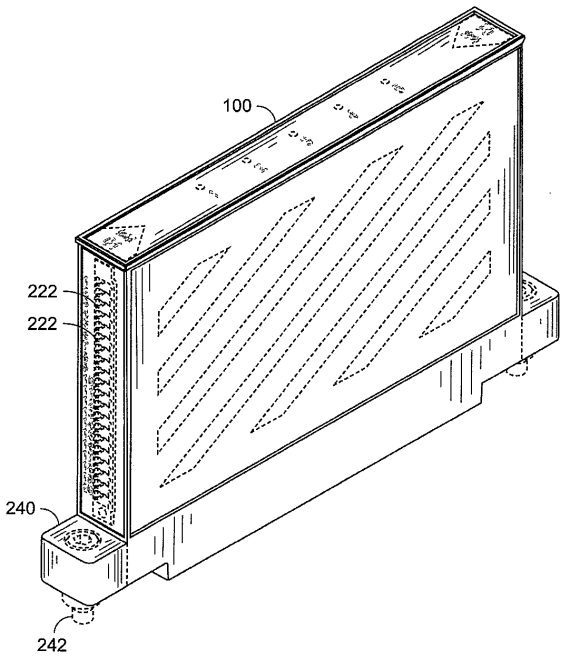

FIG. 6

【図７】

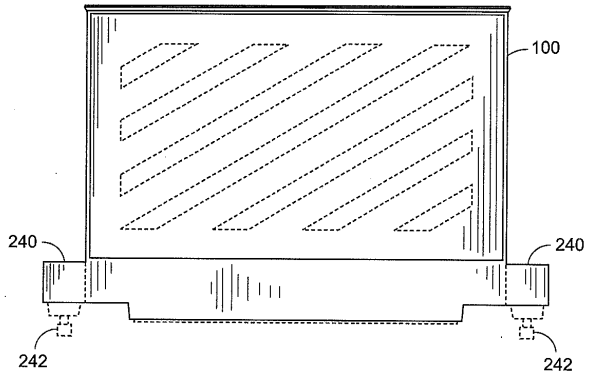

FIG. 7

【図８】

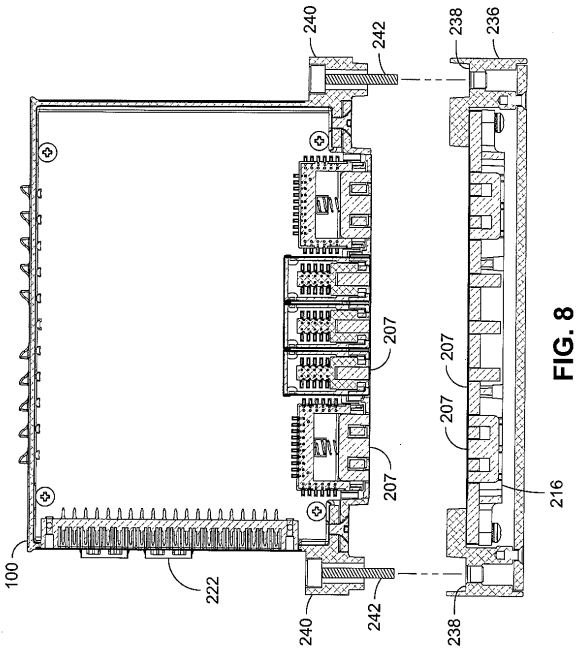

FIG. 8

【図９】

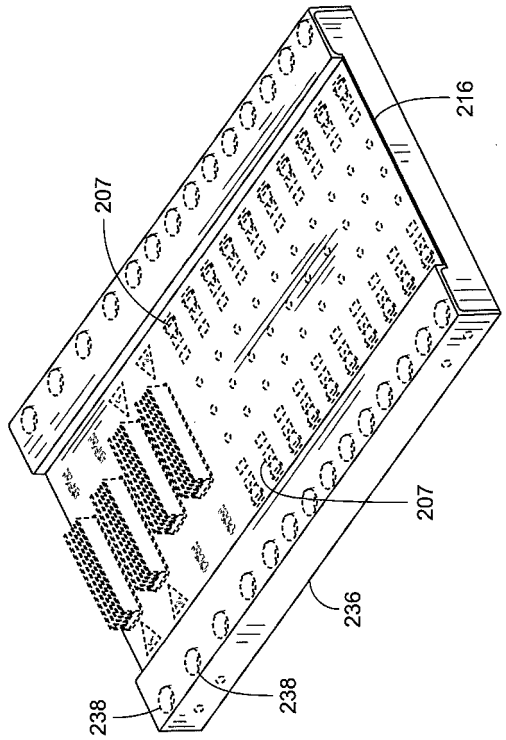

FIG. 9

【図１０】

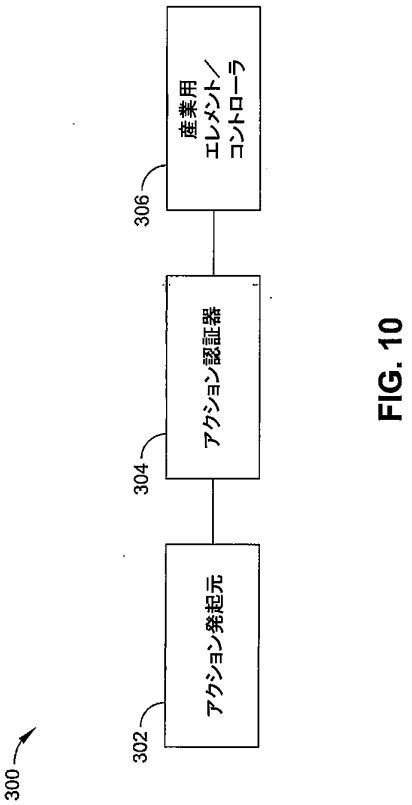

FIG. 10

【図１１】

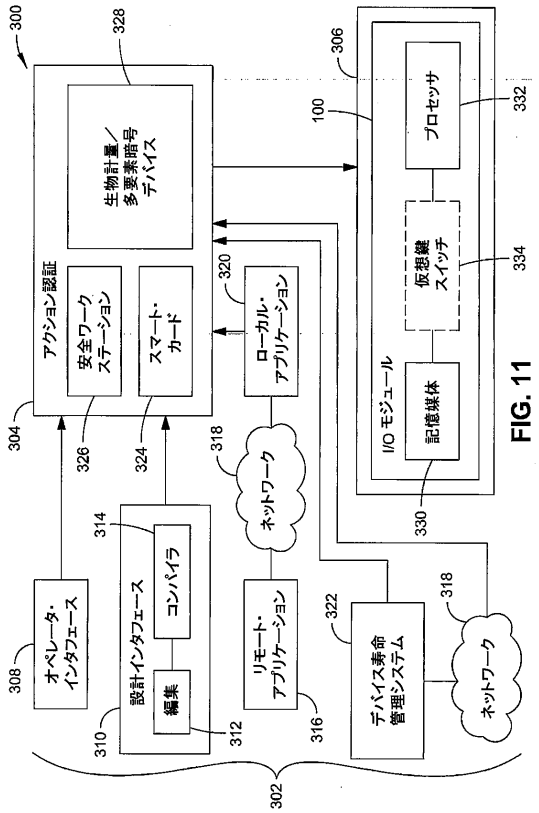

FIG. 11

【図１２】

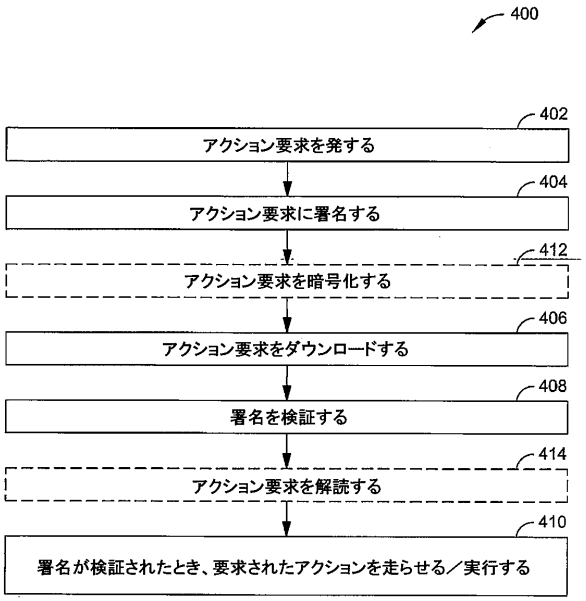

FIG. 12

【図１３】

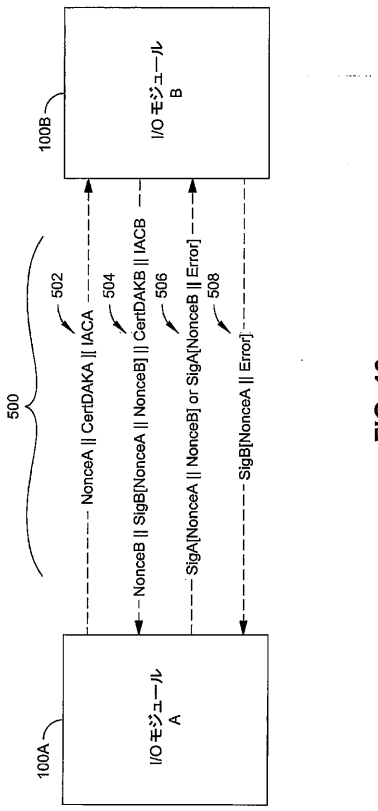

FIG. 13

【図１４】

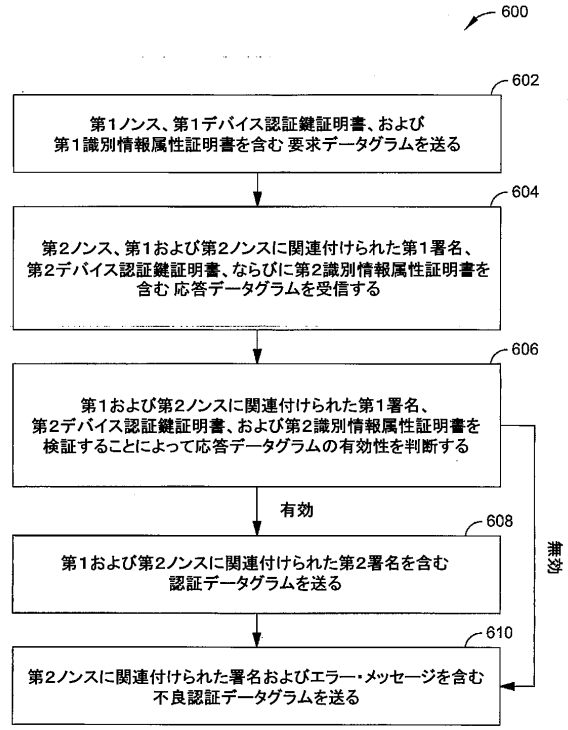

FIG. 14

【図１５】

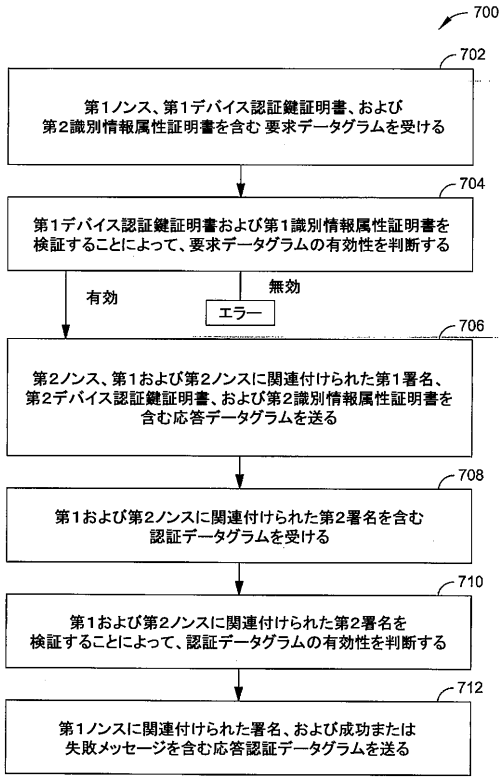
700
702
第1ノンス、第1デバイス認証鍵証明書、および
第2識別情報属性証明書を含む 要求データグラムを受ける
704
第1デバイス認証鍵証明書および第1識別情報属性証明書を
検証することによって、要求データグラムの有効性を判断する
有効
無効
エラー
706
第2ノンス、第1および第2ノンスに関連付けられた第1署名、
第2デバイス認証鍵証明書、および第2識別情報属性証明書を
含む応答データグラムを送る
708
第1および第2ノンスに関連付けられた第2署名を含む
認証データグラムを受ける
710
第1および第2ノンスに関連付けられた第2署名を
検証することによって、認証データグラムの有効性を判断する
712
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応答認証データグラムを送る

FIG. 15

フロントページの続き

(33)優先権主張国・地域又は機関
米国(US)
アメリカ合衆国カリフォルニア州９４０８７，サニーヴェール，ルビス・ドライブ ８２３
(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０２７０３，アトルボロ，ヘイゼルウッド・コート １

合議体
審判長 見目 省二
審判官 田々井 正吾
大山 健

(56)参考文献 米国特許出願公開第２０１３／０１７３８３２（ＵＳ，Ａ１）
特開平０５－３４６８０９（ＪＰ，Ａ）
米国特許出願公開第２０１４／０３４１２２０（ＵＳ，Ａ１）
米国特許出願公開第２０１４／０１４２７２５（ＵＳ，Ａ１）
特開２００３－２１６２３７（ＪＰ，Ａ）
米国特許出願公開第２０１４／０３３５７０３（ＵＳ，Ａ１）
特開平０４－１５３７０５（ＪＰ，Ａ）
特開２０１０－２０５１６３（ＪＰ，Ａ）
特開平１１－０９８２１５（ＪＰ，Ａ）
特開２００１－１００８０９（ＪＰ，Ａ）

(58)調査した分野 (Int.Cl.，ＤＢ名)
G05B 19/00 - 19/46