

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号

特許第7085826号

(P7085826)

(45)発行日 令和4年6月17日(2022.6.17)

(24)登録日 令和4年6月9日(2022.6.9)

(51)国際特許分類

F I

H 0 4 L 9/08 (2006.01)

H 0 4 L 9/08

G 0 6 F 21/44 (2013.01)

G 0 6 F 21/44

請求項の数 18 外国語出願 (全29頁)

(21)出願番号	特願2017-237592(P2017-237592)	(73)特許権者	514091080
(22)出願日	平成29年12月12日(2017.12.12)		ベドロック・オートメーション・プラッ
(65)公開番号	特開2018-152841(P2018-152841 A)		トフォームズ・インコーポレーテッド
(43)公開日	平成30年9月27日(2018.9.27)		アメリカ合衆国カリフォルニア州951
審査請求日	令和2年12月2日(2020.12.2)	(74)代理人	34, サンノゼ, リオ・ロブルズ 160
(31)優先権主張番号	15/381,667		100140109
(32)優先日	平成28年12月16日(2016.12.16)		弁理士 小野 新次郎
(33)優先権主張国・地域又は機関	米国(US)	(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	100120112
			中西 基晴
		(74)代理人	100173565
			弁理士 末松 亮太

最終頁に続く

(54)【発明の名称】 安全な産業用制御システムのためのイメージ・キャプチャ・デバイス

(57)【特許請求の範囲】

【請求項1】

安全な産業用制御システムのためのイメージ・キャプチャ・デバイスであって、
イメージ・センサと、

前記イメージ・センサに結合される信号プロセッサと、

前記信号プロセッサを管理して、処理済みイメージ信号に関連付けられるデータを、通信
インタフェースを介して入力／出力モジュールまたは通信／制御モジュールの少なくとも
一方に送信するコントローラであって、

前記通信インタフェースが、前記入力／出力モジュールまたは前記通信／制御モジュール
の前記少なくとも一方に前記コントローラを結合し、

前記コントローラが、当該イメージ・キャプチャ・デバイスの一意のセキュリティ証明と
、前記入力／出力モジュールまたは前記通信／制御モジュールの前記少なくとも一方の
一意のセキュリティ証明とに基づいて、前記コントローラと前記入力／出力モジュールまた
は前記通信／制御モジュールの前記少なくとも一方との間に暗号化済みトンネルを確立す
るよう構成される、

コントローラと、を備え、

前記イメージ・キャプチャ・デバイスは、前記一意のセキュリティ証明が、鍵管理エン
ティティによって、前記イメージ・キャプチャ・デバイスの製造場所でプロビジョニング
され、

前記イメージ・キャプチャ・デバイスの前記一意のセキュリティ証明が、前記入力／出

力モジュールまたは前記通信／制御モジュールの前記少なくとも一方によって修正可能または無効化可能の内少なくとも1つである、イメージ・キャプチャ・デバイス。

【請求項2】

請求項1記載のイメージ・キャプチャ・デバイスにおいて、前記コントローラが、更に、当該イメージ・キャプチャ・デバイスの前記一意のセキュリティ証明と、前記入力／出力モジュールまたは前記通信／制御モジュールの前記少なくとも一方の前記一意のセキュリティ証明とを利用して、前記入力／出力モジュールまたは前記通信／制御モジュールの前記少なくとも一方と認証シーケンスを実行するように構成される、イメージ・キャプチャ・デバイス。

【請求項3】

請求項1記載のイメージ・キャプチャ・デバイスにおいて、前記イメージ・キャプチャ・デバイスの前記一意のセキュリティ証明が、前記イメージ・キャプチャ・デバイスの前記製造場所とは異なるサイトにおいて、前記鍵管理エンティティによって修正可能、無効化可能、または認証可能の内少なくとも1つである、イメージ・キャプチャ・デバイス。

【請求項4】

請求項1記載のイメージ・キャプチャ・デバイスにおいて、前記イメージ・キャプチャ・デバイスの前記一意のセキュリティ証明が、前記入力／出力モジュールまたは前記通信／制御モジュールの前記少なくとも一方によって認証可能である、イメージ・キャプチャ・デバイス。

【請求項5】

請求項1記載のイメージ・キャプチャ・デバイスにおいて、前記通信インタフェースが、前記入力／出力モジュールまたは前記通信／制御モジュールの前記少なくとも一方を介して、シリアル通信インタフェースおよびパラレル通信インタフェースを含む通信バックプレーンに前記コントローラを接続するように構成される、イメージ・キャプチャ・デバイス。

【請求項6】

請求項5記載のイメージ・キャプチャ・デバイスにおいて、前記通信インタフェースが、前記入力／出力モジュールまたは前記通信／制御モジュールの前記少なくとも一方によって供給される電力を受けるためのパワー・オーバ・イーサネット（POE）ポートを備える、イメージ・キャプチャ・デバイス。

【請求項7】

1つ以上の前記処理済み信号が、前記イメージ・センサによって検出されるスペクトル・データを含む、請求項1記載のイメージ・キャプチャ・デバイス。

【請求項8】

請求項7記載のイメージ・キャプチャ・デバイスにおいて、前記コントローラが、火、塵、煙、微粒子、熱、水分、高圧力、ガス、または放射線の1つ以上の環境上の存在を含む、1つ以上の産業用制御システムの環境条件を監視するために前記スペクトル・データを送信するように構成される、イメージ・キャプチャ・データ。

【請求項9】

安全な産業用制御システムであって、

第1の一意のセキュリティ証明がプロビジョニングされる通信／制御モジュールと、

第2の一意のセキュリティ証明がプロビジョニングされる入力／出力モジュールと、

前記入力／出力モジュールに前記通信／制御モジュールを物理的および通信可能に結合する通信バックプレーンと、

第3の一意のセキュリティ証明がプロビジョニングされるイメージ・キャプチャ・デバイスであって、

イメージ・センサと、

前記イメージ・センサに結合される信号プロセッサと、

前記信号プロセッサを管理して、処理済みイメージ信号に関連付けられるデータを、通信インタフェースを介して前記入力／出力モジュールまたは前記通信／制御モジュールの少

10

20

30

40

50

なくとも一方に送信するコントローラであって、
前記通信インタフェースが、前記入力／出力モジュールまたは前記通信／制御モジュールの前記少なくとも一方に前記コントローラを結合し、
前記コントローラが、前記イメージ・キャプチャ・デバイスの前記第3の一意のセキュリティ証明と、前記入力／出力モジュールまたは前記通信／制御モジュールの前記少なくとも一方に関連付けられる前記第1および第2の一意のセキュリティ証明の少なくとも1つとに基づいて、前記コントローラと前記入力／出力モジュールまたは前記通信／制御モジュールの前記少なくとも一方との間に暗号化済みトンネルを確立するように構成される、コントローラと、
を備える、イメージ・キャプチャ・デバイスと、
を備え、

10

前記イメージ・キャプチャ・デバイスは、前記第3の一意のセキュリティ証明が、鍵管理エンティティから、前記イメージ・キャプチャ・デバイスの製造場所でプロビジョニングされ、

前記イメージ・キャプチャ・デバイスの前記第3の一意のセキュリティ証明が、前記入力／出力モジュールまたは前記通信／制御モジュールの前記少なくとも一方によって修正可能または無効化可能の内少なくとも1つである、安全な産業用制御システム。

【請求項10】

請求項9記載の安全な産業用制御システムにおいて、前記コントローラが、更に、前記イメージ・キャプチャ・デバイスの前記第3の一意のセキュリティ証明と、前記入力／出力モジュールまたは前記通信／制御モジュールの前記少なくとも一方に関連付けられる前記第1および第2の一意のセキュリティ証明の前記少なくとも1つとに基づいて、前記入力／出力モジュールまたは前記通信／制御モジュールの前記少なくとも一方と認証シーケンスを実行するように構成される、安全な産業用制御システム。

20

【請求項11】

請求項9記載の安全な産業用制御システムにおいて、前記イメージ・キャプチャ・デバイスの前記第3の一意のセキュリティ証明が、前記製造場所とは異なるサイトにおいて、前記鍵管理エンティティによって修正可能、無効化可能、または認証可能の内少なくとも1つである、安全な産業用制御システム。

【請求項12】

30

請求項9記載の安全な産業用制御システムにおいて、前記イメージ・キャプチャ・デバイスの前記第3の一意のセキュリティ証明が、前記入力／出力モジュールまたは前記通信／制御モジュールの前記少なくとも一方によって認証可能である、安全な産業用制御システム。

【請求項13】

請求項9記載の安全な産業用制御システムにおいて、前記通信インタフェースが、前記入力／出力モジュールまたは前記通信／制御モジュールの前記少なくとも一方を介して、前記コントローラを前記通信バックプレーンに接続するように構成され、前記通信バックプレーンが、シリアル通信インタフェースおよびパラレル通信インタフェースを含む、安全な産業用制御システム。

40

【請求項14】

請求項13記載の安全な産業用制御システムにおいて、前記通信インタフェースが、前記入力／出力モジュールまたは前記通信／制御モジュールの前記少なくとも一方によって供給される電力を受けるためのパワー・オーバ・イーサネット（POE）ポートを備える、安全な産業用制御システム。

【請求項15】

1つ以上の前記処理済み信号が、前記イメージ・センサによって検出されるスペクトル・データを含む、請求項9記載の安全な産業用制御システム。

【請求項16】

請求項15記載の安全な産業用制御システムにおいて、前記コントローラが、火、塵、煙

50

、微粒子、熱、水分、高圧力、ガス、または放射線の1つ以上の環境上の存在を含む、1つ以上の産業用制御システムの環境条件を監視するために前記スペクトル・データを送信するように構成される、安全な産業用制御システム。

【請求項17】

請求項9記載の安全な産業用制御システムにおいて、前記入力／出力モジュールまたは前記通信／制御モジュールの少なくとも一方が、当該安全な産業用制御システムの他の産業用エレメントまたはネットワーク接続デバイスにイメージ信号を送信する前に、前記イメージ・キャプチャ・デバイスから受け取った前記イメージ信号を、事前処理または事後処理するように構成される、安全な産業用制御システム。

【請求項18】

安全な産業用制御システムであって、

第1の一意のセキュリティ証明がプロビジョニングされる通信／制御モジュールと、

第2の一意のセキュリティ証明がプロビジョニングされる入力／出力モジュールと、

前記入力／出力モジュールに前記通信／制御モジュールを物理的および通信可能に結合する通信バックプレーンであって、

前記入力／出力モジュールを前記通信／制御モジュールに接続す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通信／制御モジュールに別個に接続するパラレル通信インタフェースと、

を含む、通信バックプレーンと、

第3の一意のセキュリティ証明がプロビジョニングされるイメージ・キャプチャ・デバイスであって、

イメージ・センサと、

前記イメージ・センサに結合される信号プロセッサと、

前記信号プロセッサを管理して、処理済みイメージ信号に関連付けられるデータを、通信インタフェースを介して前記入力／出力モジュールまたは前記通信／制御モジュールの少なくとも一方に送信するコントローラであって、前記通信インタフェースが、前記イメージ・キャプチャ・デバイスの前記第3の一意のセキュリティ証明と、前記入力／出力モジ

ュールまたは前記通信／制御モジュールの前記少なくとも一方に関連付けられる前記第1

および第2の一意のセキュリティ証明の少なくとも1つとに基づいて、前記入力／出力モ

ジュールまたは前記通信／制御モジュールの前記少なくとも一方に前記コントローラを結

合する、コントローラと、

を備える、イメージ・キャプチャ・デバイスと、

を備え、
前記イメージ・キャプチャ・デバイスは、前記第3の一意のセキュリティ証明が、鍵管

理エンティティから、前記イメージ・キャプチャ・デバイスの製造場所でプロビジョニン

グされ、
前記イメージ・キャプチャ・デバイスの前記第3の一意のセキュリティ証明が、前記入

力／出力モジュールまたは前記通信／制御モジュールの前記少なくとも一方によって修正

可能または無効化可能の内少なくとも1つである、安全な産業用制御システム。

【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] 本出願は、2015年11月16日に出願され"SECURE INDUSTRIAL CONTR

OL SYSTEM"と題する米国特許出願第14／942,304の一部継続出願である。当該

米国特許出願第14／942,304は、2014年8月27日に出願され"SECURE IN

DUSTRIAL CONTROL SYSTEM"と題する米国特許出願第14／469,931号（米国

特許第9,191,203号としての発行済み）の継続出願であり、当該米国特許出願第1

4／469,931号は、2013年8月6日に出願され"SECURE INDUSTRIAL CONTR

10

20

30

40

50

OL SYSTEM"と題する国際出願第PCT/US2013/053721の継続である。本出願は、2014年10月20日に提出され"OPERATOR ACTION AUTHENTICATION IN AN INDUSTRIAL CONTROL SYSTEM"と題する米国特許出願番号第14/519,066号の一部継続出願でもある。本出願は、2016年10月7日に提出され"INDUSTRIAL CONTROL SYSTEM REDUNDANT COMMUNICATIONS/CONTROL MODULES AUTHENTICATION"と題する米国特許出願第15/287,937号の一部継続出願でもある。当該米国特許出願第15/287,937号は、2014年10月20日に提出され"INDUSTRIAL CONTROL SYSTEM REDUNDANT COMMUNICATIONS/CONTROL MODULES AUTHENTICATION"と題する米国特許出願第14/519,047号（米国特許第9,467,297号として発行済み）の継続出願である。本出願は、2015年1月15日に提出され"ELECTROMAGNETIC CONNECTOR"と題する米国特許出願第14/597,498号の一部継続出願でもある。当該米国特許出願第14/597,498号は、2011年12月30日に提出され"ELECTROMAGNETIC CONNECTOR"と題する米国特許出願第13/341,143号の継続出願である。本出願は、2016年8月26日に提出され"SWITCH FABRIC HAVING A SERIAL COMMUNICATIONS INTERFACE AND A PARALLEL COMMUNICATIONS INTERFACE"と題する米国特許出願第15/247,998号の一部継続出願でもある。当該米国特許出願第15/247,998号は、2014年9月30日に提出され"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号の継続出願であり（米国特許第9,436,641号として発行済み）、当該米国特許出願第14/501,974号は、2011年12月30日に提出され"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号の継続出願である（米国特許第8,862,802号として発行済み）。本出願は、2016年10月10日に提出され"COMMUNICATIONS CONTROL SYSTEM WITH A SERIAL COMMUNICATIONS INTERFACE AND A PARALLEL COMMUNICATIONS INTERFACE"と題する米国特許出願第15/289,613号の一部継続出願でもある。当該米国特許出願第15/289,613号は、2014年9月30日に提出され"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号の継続出願であり（米国特許第9,465,762号として発行済み）、当該米国特許出願第14/502,006号は、2011年12月30日に提出され"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号の継続出願である（米国特許第8,868,813号として発行済み）。

【0002】

[0002] 上記に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。

【従来技術】

【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IEC61508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た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

10

20

30

40

50

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こともあるプロセス・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に送るためにリモート端末ユニット(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、また、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、並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、多くの場合は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ー消費を監視し制御する)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つれて、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組み合わせつつある。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] 産業用システムは、「モノのインターネット(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。全てのレベルにおいてセキュリティが必要とされる。これにはエッジ・デバイスが含まれる。エッジ・デバイスは、安全でないままとされると、悪意のある行為者のためのシステムになることができる。

【課題を解決するための手段】

【0006】

[0006] 安全な産業用制御システムのためのイメージ・キャプチャ・デバイス(例えばカメラ)の実装態様について本願明細書に開示する。イメージ・キャプチャ・デバイスは、イメージ・センサと、イメージ・センサに結合される信号プロセッサと、信号プロセッサを管理するコントローラとを含むことができる。コントローラはまた、処理済みイメージ信号に関連付けられるデータを、イメージ・キャプチャ・デバイスに結合される1つ以上のデバイスに送信するように構成することができる。例えば、コントローラは、処理済みイメージ信号に関連付けられるデータ(例えば、符号化済みイメージ・フレームやメタデータ等)を、通信インタフェースを介して、入力／出力モジュールおよび／または通信／制御モジュールに送信することができる。通信インタフェースは、入力／出力モジュールおよび／または通信／制御モジュールにコントローラを結合する。実施形態では、コントローラは、イメージ・キャプチャ・デバイスの少なくとも1つの各セキュリティ証明と、入力／出力モジュールおよび／または通信／制御モジュールの少なくとも1つの各セキュリティ証明とに基づいて、コントローラと入力／出力モジュールまたは通信／制御モジュールとの間に暗号化済みトンネルを確立するように構成される。コントローラはまた、イメージ・キャプチャ・デバイスの少なくとも1つの各セキュリティ証明と、入力／出力モジュールおよび／または通信／制御モジュールの少なくとも1つの各セキュリティ証明とを利用して、入力／出力モジュールおよび／または通信／制御モジュールと認証シーケンスを実行するように構成される。これにより、イメージ・キャプチャ・デバイスは、入力／出力モジュールおよび／若しくは通信／制御モジュール、並びに／または安全な産業用制御システムの他のコンポーネントから情報を送信および／または受信するために、パー

ミッションが認証されおよび／または付与されることができる。

【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安全な産業用制御システム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安全な産業用制御システムのためのイメージ・キャプチャ・デバイス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安全な産業用制御システムの通信バックプレーンためのスイッチ機構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安全な産業用制御システムのためのアクション認証経路を示すブロック図である。

【図5】図5は、本開示の実施形態による図4のアクション認証経路を更に示すブロック図である。

【図6】図6は、本開示の実施形態による安全な産業用制御システムが有するイメージ・キャプチャ・デバイスと、入力／出力モジュール（IOM）または通信／制御モジュール（CCM）との間の認証シーケンスを示すブロック図である。

【発明を実施するための形態】

【0010】

概要

[0015] 産業用システムは、「モノのインターネット」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ものである。全てのレベルにおいてセキュリティが必要とされる。これにはエッジ・デバイスが含まれる。エッジ・デバイスは、安全でないままとされると、悪意のある行為者のためのシステムになる可能性がある。例えば、監視カメラは、しばしば「セキュリティ・デバイス」としてみなされることがあるが、産業用制御システムへの脆弱なアクセス・ポイントとなる可能性がある。幾らかの例では、偽造されたか、またはハッキングされたカメラを使用して、産業用制御システムへの非認証のエントリを獲得する可能性があり、その結果、ビデオ映像または他の情報へのアクセスを獲得するか、或いは、（例えば、不正のアラームを妨害する目的等のために）架空のビデオ映像を差し込むことさえもある。幾らかの例では、カメラ・ネットワーク接続を利用して、例えば、リモート・アクセスを獲得し、制御システム情報を用いて盗み出すまたは改竄する等のために悪意のあるコードのエントリ・ポイントとして、非カメラ・ネットワーク・データベースにマルウェアをワームさせることがある。

【0011】

[0016] 安全な産業用制御システムのためのイメージ・キャプチャ・デバイス（例えば、カメラ）の実装態様が、本願明細書に開示される。実施形態では、安全な産業用制御システムのためのイメージ・キャプチャ・デバイスは、イメージ・センサと、イメージ・センサに結合される信号プロセッサと、信号プロセッサを管理するコントローラとを含むことができる。コントローラはまた、処理済みイメージ信号に関連付けられるデータを、イメージ・キャプチャ・デバイスに結合される1つ以上のデバイスに送信するように構成することができる。例えば、コントローラは、処理済みイメージ信号に関連付けられるデータ（例えば、符号化済みイメージ・フレームやメタデータ等）を、通信インタフェースを介

10

20

30

40

50

して、入力／出力モジュールおよび／または通信／制御モジュールに送信することができる。通信インタフェースは、入力／出力モジュールおよび／または通信／制御モジュールにコントローラを結合する。実施形態では、コントローラは、イメージ・キャプチャ・デバイスの少なくとも1つの各セキュリティ証明と、入力／出力モジュールおよび／または通信／制御モジュールの少なくとも1つの各セキュリティ証明とに基づいて、コントローラと入力／出力モジュールまたは通信／制御モジュールとの間に暗号化済みトンネルを確立するように構成される。コントローラはまた、イメージ・キャプチャ・デバイスの各セキュリティ証明と、入力／出力モジュールおよび／または通信／制御モジュールの各セキュリティ証明とを利用して、入力／出力モジュールおよび／または通信／制御モジュールと認証シーケンスを実行するように構成される。これにより、イメージ・キャプチャ・デバイスは、入力／出力モジュールおよび／若しくは通信／制御モジュール、並びに／または安全な産業用制御システムの他のコンポーネントから情報を送信および／または受信するために、パーミッションが認証されおよび／または付与されることができる。例えば、送信情報は、これに限定されないが、キャプチャ・イメージ、ビデオ映像、スペクトル情報（例えば、火、ガスおよび／または放射線の検出のため）、またはこれらの組み合わせを含むことができる。

10

【0012】

例示の実装態様

【0017】 図1は、本開示の例示の実施形態による産業用制御システム100を示す。実施形態では、産業用制御システム100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1に示すように、産業用制御システム100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102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（I/O）モジュール、電力モジュール、フィールド・デバイス、イメージ・キャプチャ・デバイス（例えば、監視カメラ、物理セキュリティ・カメラ、特定スペクトル検出・カメラ（例えば、火、ガスおよび／または放射線の検出用）等）、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）を含んで分散型制御システムを実装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104は、制御エレメント／サブシステム102を構成する1つ以上の通信／制御モジュール106（時折、（CCM）と略記する。）に接続されてもよい。

20

30

【0013】

【0018】 産業用制御システム100は、I/Oモジュール104にそしてI/Oモジュール104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104は、入力モジュール、出力モジュール、並びに／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、入力デバイス130（例えば、センサ）から情報を受信するために使用することができる一方、出力モジュールは、命令を出力デバイス（例えば、アクチュエータ）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104は、ガス・プラントや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状態若しくは多状態スイッチや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130は、直接に、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104と通信可能に結合される。これらデバイス130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）、並びに通信サブ・バス等を含むことができる。

40

【0014】

【0019】 I/Oモジュール104は、産業用制御システム100において、以下を含むが

50

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。即ち、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（例えば、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）、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ー消費を監視および制御するため）である。

【0015】

【0020】 幾らかの実装態様では、I/Oモジュール104はまた、イメージ・キャプチャ・デバイス200（例えば、監視カメラ、物理セキュリティ・カメラや特定スペクトル検出カメラ等のカメラ）を産業用制御システム100に接続するのに使用することができる。他の実装態様では、イメージ・キャプチャ・デバイス200は、通信／制御モジュール106または他の入力手段を介してバックプレーン116に接続することができる。バックプレーン116は、産業用制御システム・エレメントのオンサイトおよびオフサイトでの相互接続性（例えば、企業システム／アプリケーション、外部制御システム／アプリケーション、設計インタフェース制御システム／アプリケーション、外部監視システム／アプリケーション、およびオペレータ／管理者監視または制御システム／アプリケーション等のためのネットワーク120への接続性）を高める。

【0016】

【0021】 図2に示すように、イメージ・キャプチャ・デバイス200は、イメージ・センサ（例えば、CMOSイメージ・センサやCCDイメージ・センサ等）を含む。イメージ・センサは、イメージ・センサ204に結合される信号プロセッサ206を有する。実施形態では、イメージ・センサ204はレンズまたはレンズ・アセンブリ202を有することができる。レンズ・アセンブリ202は、イメージ・センサ204に向けて光をフォーカスするためにイメージ・センサ204を覆って配置される。信号処理器206は、イメージ・センサ204からイメージ信号を受信するように構成することができる。また、1つ以上のフィルタを使用し、利得レベルを調整し、そして、アナログ形式からデジタル形式にイメージ信号を変換する等のように構成することができる。イメージ・キャプチャ・デバイス200は、産業用制御システム100内のエンド・デバイスによって復号することができるデータ・フォーマットに、処理済みイメージ信号を符号化するためのコーデック210を更に含むことができる。幾らかの実施形態では、イメージ・キャプチャ・デバイス200は、例えば、信号処理の前、後またはその間において1つ以上の信号コンポーネントの（即ち、信号プロセッサ206での）利得を増進させる(boost)ことによって、画像属性（例えば、輝度やコントラスト等）を調整するためのビデオ・エンハンサ208を含む。イメージ・キャプチャ・デバイス200は、更に、信号プロセッサ206のコンポーネント、回路、および／またはイメージ・キャプチャ・デバイス200のモジュールを管理するためのコントローラ212（例えば、マイクロコントローラ、マイクロプロセッサ、ASICやプログラム可能ロジック・デバイス等）を含む。コントローラ212はまた、イメージ・キャプチャ・デバイス200に結合される1つ以上のデバイスに、処理済みイメージに関連付けられるデータを、送信するように構成することができる。例えば、コントローラ212は、通信インタフェース214（例えば、送信機、受信機、および／または送受信機）を介して、入力／出力モジュール104および／または通信／制御モジュール106に、処理済みイメージ信号に関連付けられるデータ（例えば、符号化済みイメージ・フレームやメタデータ等）を送信することができる。通信インタフェース214は、入力／出力モジュール104および／または通信／制御モジュール106にコントローラ212を結合する。幾らかの実施形態では、入力／出力モジュール104および／または通信／制御モジュール106は、安全な産業用制御システムの他の産業エレメントまたはネットワーク接続デバイスに対して処理済みイメージ信号を送信する前に、イメージ・キャプチャ・デバイス200から受信したイメージ信号を事前処理または事後処理するように構成される。例えば、入出力モジュール104および／または通信／制御モジュール106は、処理済みイメージ信号について、追加のフィルタリング、符号化、または

10

20

30

40

50

暗号化を実行するように構成することができる。幾らかの実施形態では、通信インタフェース 214 はポートを含み、イメージ・キャプチャ・デバイス 200 を外部デバイス（例えば、IOM104、CCM106、または他の産業用制御システム・エレメント）に結合するために有線接続を受けるように構成される。他の実施形態では、通信インタフェース 214 は、無線送信機、受信機、および／または送受信機を含むことができ、イメージ・キャプチャ・デバイス 200 および外部デバイスの間の無線接続性を高める。

【0017】

[0022] 通信インタフェース 214 は、外部デバイスによって供給される電力を受けるパワー・オーバ・イーサネット（登録商標）（POE; Power Over Ethernet）ポートを備えてもよい。例えば、イメージ・キャプチャ・デバイス 200 は、POE 性能を有するセキュア・イーサネット（登録商標）I/O モジュールに結合されてもよい。I/O モジュール 104 は、BEDROCKS I/O 4. E セキュア・イーサネット（登録商標）・モジュール等を含むことができる。幾らかの実施形態では、I/O モジュール 104（例えば、BEDROCKS I/O 4. E セキュア・イーサネット（登録商標）・モジュール）は、マルチ・チャネルの安全なソフトウェア構成可能イーサネット・モジュールを備える。当該モジュールは、各ポート上でソフトウェア設定可能なプロトコル、イーサネット（登録商標）I/P 用サポート、Modbus TCP および OPC UA クライアント、計画された Profinet および DNP3 を含む他のプロトコル、イーサネット（登録商標）給電デバイス用の 1 つ以上のポートで利用可能な POE、並びに／または、10/100 Mbps の半／全二重機能を有することができる。幾らかの実装態様では、イメージ・キャプチャ・デバイス 200 は、5~60 fps のフレーム・レートおよび 240~1080 p の解像度によって、約 9600 および 10 M の間の範囲のビット・レートで処理済みイメージに関連付けられるデータを送信するように構成される。例えば、イメージ・キャプチャ・デバイス 200 は、2 M ビット・レート未満で、15 fps、720 p で送信するように構成することができる。これらの範囲は、例示のために設けたに過ぎず、本開示に限定するものとみなしてはならないものである。

【0018】

[0023] 実施形態では、イメージ・キャプチャ・デバイスのコントローラ 212 は、コントローラ 212 および外部デバイス（例えば、入力／出力モジュール 104 または通信／制御モジュール 106）の間に暗号化済みトンネルを確立するように構成される。暗号化済みトンネルの確立は、イメージ・キャプチャ・デバイス 200 の少なくとも 1 つの各セキュリティ証明と、外部デバイスの少なくとも 1 つの各セキュリティ証明とに基づく。コントローラ 212 はまた、イメージ・キャプチャ・デバイス 200 の各セキュリティ証明と、外部デバイスの各セキュリティ証明とを利用して、外部デバイスと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。これにより、イメージ・キャプチャ・デバイス 200 は、入力／出力モジュール 104 および／若しくは通信／制御モジュール 106、並びに／または、安全な産業用制御システムの他のコンポーネントから情報を送信および／または受信するために、パーミッションを認証および／または付与することができる。

【0019】

[0024] 以下により詳細に検討するように、イメージ・キャプチャ・デバイス 200 の各セキュリティ証明は、鍵管理エンティティ 124 によってイメージ・キャプチャ・デバイス 200 にプロビジョニングされる一意のセキュリティ証明を含むことができる。例えば、一意のセキュリティ証明は、鍵管理エンティティ 124 から（イメージ・キャプチャ・デバイス 200 の）各製造場所 (point of manufacture) においてプロビジョニングされることができる。幾らかの実施形態では、各セキュリティ証明は、（例えば、イメージ・キャプチャ・デバイス 200 が産業用制御システム 100 に設置されるときに）各製造場所とは異なるサイトにおいて、鍵管理エンティティ 124 によって、修正可能、無効化可能、および／または認証可能である。これに加えてまたはこれに替えて、各セキュリティ証明は、外部デバイス（例えば、入力／出力モジュール 104 または通信／制御モジュール 106）によって、或いはイメージ・キャプチャ・デバイス 200 と通信する他の産業

用制御システム・エレメントによって、修正可能、無効化可能、および／または認証可能としてもよい。

【0020】

[0025] 幾らかの実施形態では、イメージ・キャプチャ・デバイス200は、専門(specialty)カメラを含んでもよい。例えば、1つ以上の処理済みイメージ信号は、イメージ・センサ204によって検出されるスペクトル・データを含む。コントローラ212は、1つ以上の産業用制御システムの環境条件を監視するために、スペクトル・データを送信するように構成することができる。例えば、イメージ・キャプチャ・デバイス200は、これに限定されないが、以下の1つ以上の環境上の存在を含む、1つ以上の産業用制御システムの環境条件を監視するように構成してもよい。即ち、火、塵、煙、微粒子、熱、水分、高圧力、ガスや放射線等である。幾らかの実施形態では、イメージ・センサ204は、熱イメージ・センサ、暗視イメージ・センサ、紫外線センサや赤外線光センサ等を備えることができる。実装態様では、イメージ・キャプチャ・デバイス200によって検出されるスペクトル・データは、(例えば、火やガス漏れ等を検出することに応答して)アラーム／アラートをトリガすることができる。

10

【0021】

[0026] 図1を再度参照する。I/Oモジュール104は、センサから受信したアナログ・データを、(例えば、アナログ／デジタル変換器(ADC)回路等を使用して)デジタル・データに変換するように構成することができる。I/Oモジュール104は、また、モータまたは調節弁、或いは電気リレー、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に接続されることができ、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、或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104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、(例えば、デジタル／アナログ(DAC)回路等を使用して)アナログ・データに変換するように構成することができる。実装態様では、I/Oモジュール104の内1つ以上は、イーサネット(登録商標)・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可能リモート変換器(HART)バスやModbus等のような通信サブ・バスを介して通信するように構成された通信モジュールを備えることができる。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130や通信サブ・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提供することができる。

20

30

【0022】

[0027] 各I/Oモジュール104には、I/Oモジュール104を他のI/Oモジュール104から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104は、産業用制御システム100に接続されるときに、そのIDによって識別される。冗長性を設けるために、多数のI/Oモジュール104を産業用制御システム100と共に使用することができる。例えば、2つ以上のI/Oモジュール104をプロセス・センサおよび／またはアクチュエータに接続することができる。各I/Oモジュール104は、印刷回路ボード(PCB)224等のような、I/Oモジュール104と共に含まれるハードウェアおよび回路への物理接続を設ける1つ以上のポート222を含むことができる。例えば、各I/Oモジュール104はケーブルの接続を含み、I/Oモジュール104内の印刷配線ボード(PWB)にケーブルを接続する。

40

【0023】

[0028] I/Oモジュール104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。他のネットワークには、これに限定されないが、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(登録商標))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、W

50

i-Fiネットワーク（例えば、IEEE 802.11ネットワーク規格を使用して運用されるワイヤレス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、IEEE 802.15ネットワーク規格を使用して運用されるワイヤレス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。更に、I/Oモジュール104の内1つ以上は、I/Oモジュール104をコンピュータ・バス等に接続するための接続を含むことができる。

【0024】

[0029] 通信／制御モジュール106は、I/Oモジュール104を監視および制御するため、並びに2つ以上のI/Oモジュール104と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106は、I/Oモジュール104が産業用制御システム100に接続されたときに、I/Oモジュール104の一意のIDに基づいて、ルーティング・テーブル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104が使用される場合は、各通信／制御モジュール106はI/Oモジュール104に関する情報データベースのミラーリングを実装し、データがI/Oモジュール104から受信される毎、および／またはI/Oモジュール104に送信される毎に、これらを更新することができる。幾らかの実施形態では、冗長性を設けるために、2つ以上の通信／制御モジュール106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106は、スタートアップ、リセット、新たな制御モジュール106の設置、通信／制御モジュール106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イクを実行するように構成することができる。

【0025】

[0030] 幾らかの実装形態では、産業用制御システム100によっ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、データの別個の部分、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100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。幾らかの実装形態では、産業用制御システム100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106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図するもので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100は、本開示にしたがって、他の様々な通信プロトコルを使用することもできる。

【0026】

[0031] 通信／制御モジュール106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／コントローラのような、I/Oモジュール104を介して産業用制御システム100に接続されたフィールド・デバイス130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）や比例－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。幾らかの実施形態では、通信／制御モジュール104および通信／制御モジュール106は、例えば、ネットワークを介して1つ以上のI/Oモジュール104を1つ以上にコントローラに接続するために、ネットワーク・インタフェースを含む。実装態様では、ネットワーク・インタフェースは、I/Oモジュール104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（登録商標）・インタフェースとして構成することができる。更に、冗長ギガビット・イーサネット（登録商標）を実装するために、2つ以上の通信／制御モジュール106を使用することができる。しか

10

20

30

40

50

しながら、ギガビット・イーサネット（登録商標）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。つまり、ネットワーク・インタフェースは、通信／制御モジュール106を他の様々なネットワークに接続するように構成することもできる。他の様々なネットワークには、これに限定されないが、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（登録商標））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用されるWLAN）のようなワイヤレス・コンピュータ通信ネットワーク、PAN（例えば、IEEE802.15ネットワーク規格を使用して運用されるWPAN）、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。加えて、ネットワーク・インタフェースは、コンピュータ・バスを使用して実装することができる。例えば、ネットワーク・インタフェースは、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、ネットワークは、異なるアクセス・ポイントにわたる単一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。

【0027】

[0032] 産業用制御システム100は、多数のソース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108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、オンサイトのタービンまたはディーゼル・ローカル発電機110）を使用して供給することもできる。電源112は、コントローラやI/Oモジュール等のような産業用制御システム100の自動機器に、電力グリッド108からの電力を配給するように使用される。また、電源112は、ローカル発電機110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100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る追加の（バックアップ）電源も含むことができる。例えば、電源112はUPSとして機能してもよい。本開示の実施形態では、多数の電源112を産業用制御システム100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。

【0028】

[0033] 幾らかの実施形態では、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、I/Oモジュール104、通信／制御モジュール106や電力モジュール232等）は、1つ以上のバックプレーン114によって互いに接続することができる。例えば、通信／制御モジュール106は、I/Oモジュール104に、通信バックプレーン116によって接続することができる。更に、電源112は、電力バックプレーン118によって、I/Oモジュール104に、および／または通信／制御モジュール106に接続することもできる。幾らかの実施形態では、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104、通信／制御モジュール106、電力モジュール112、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106をネットワーク120に接続するためにケーブルを使用することができ、電源112を電力グリッド108に接続するために他のケーブルを使用することができ、電源112をローカル発電機110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。

【0029】

[0034] 通信バックプレーン116は、スイッチ・ファブリック300を含み、通信バックプレーン116を介して結合される産業用制御システム・エレメントの相互接続性を高める。例えば、通信バックプレーン116は、通信／制御モジュール106をI/Oモジュール104に物理的に且つ通信により結合することができる。更に、これら産業用制御

10

20

30

40

50

システム・エレメントをネットワーク１２０に結合することができる（例えば、企業デバイスや設計制御インタフェース／アプリケーション等にアクセスを提供する）。イメージ・キャプチャ・デバイス２００（および他のデバイス１３０）は、直接に或いは通信制御モジュール１０６またはＩ／Ｏモジュール１０４を介して、通信バックプレーン１１６に結合することができ、その結果、スイッチ・ファブリック３００を通じて高速セキュア通信へとアクセスを高めることができる。

【００３０】

[0035] 実施形態では、スイッチ・ファブリック３００は、多数の通信／制御モジュール１０６、Ｉ／Ｏモジュール１０４、イメージ・キャプチャ・デバイス２００、フィールド・デバイス１３０、および／または産業用制御システム１００の他のエレメントの間の通信を設けるために、シリアル通信インタフェース３０２およびパラレル通信インタフェース３０４を含む。様々なエレメントは、１つ以上の電磁コネクタを使用して、産業用制御システム１００に接続することができる。例えば、各Ｉ／Ｏモジュール１０４は、１つ以上の電磁コネクタまたはコネクタ・アセンブリを含むことができ、またはこれらに結合されることができ、コア部材がコイルを通じて延伸する。幾らかの実施形態では、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１０４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、また、電磁コネクタ・アセンブリの両半分の一定の嵌合を確実にする。

【００３１】

[0036] 幾らかの実施形態では、三面において固有の締結および支持を与える「溝形」("tongue and groove")構成を使用することができる。例えば、Ｉ／Ｏモジュール１０４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・セグメントに沿うように、また、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、一次コイルおよび二次コイルの双方が巻線コイルを含んでもよい。

【００３２】

[0037] スイッチ・ファブリック３００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３００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い。ここでは、サブシステムが、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３００は、多数のスレーブ・デバイスとの通信を設けるために、シリアル通信インタフェース３０２およびパラレル通信インタフェース３０４を含む。

【００３３】

[0038] シリアル通信インタフェース３０２は、互いに並列に接続されたコネクタのグループを使用して実装されてもよい。ある実施形態では、（例えば、前述したような）コネクタは、電磁コネクタ／コネクタ・アセンブリ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３０２は、マルチドロップ・バス(multidrop bus)３０６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３０６は、Ｉ／Ｏモジュール１０４／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304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304は、クロス・スイッチ308等を使用して実装されてもよい。

【0034】

[0039] 図3に示す実施形態では、パラレル通信インタフェース304が、各I/Oモジュール104／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308を使用して実装されてもよい。実装態様では、各接続は、（例えば、前述のような）1つ以上の電磁コネクタ／コネクタ・アセンブリを使用して設けられてもよい。クロス・スイッチ308は、ポイント・ツー・ポイント・バスを接続し、I/Oモジュール104／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308は、通信／制御モジュール106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106／マスタ・デバイスは、クロス・スイッチ308内に含まれる一組以上のレジスタを、I/Oモジュール104／スレーブ・デバイス間の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106／マスタ・デバイスは、どのようにI/Oモジュール104／スレーブ・デバイスを相互接続するかを指令するルール・セットを含んでもよい。例えば、通信／制御モジュール106／マスタ・デバイスが一組のレジスタを備え、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）規定してもよい。つまり、クロス・スイッチ308は、必ずしも自動構成設定(auto-configure)する必要がなく、その替わり、通信／制御モジュール106／マスタ・デバイスによって与えられる構成を実施してもよい。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308が自動構成設定してもよい。

【0035】

[0040] パラレル通信インタフェース304は、I/Oモジュール104／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104／スレーブ・デバイスは通信／制御モジュール106／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104／スレーブ・デバイスは、同時に通信／制御モジュール106と通信することができる。つまり、産業用制御システム100（即ち、スイッチ・ファブリック300）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104／スレーブ・デバイスのそれに制限されることになるであろう。

【0036】

[0041] 実装態様では、スイッチ・ファブリック300、シリアル通信インタフェース302、およびパラレル通信インタフェース304は、単一のモノリシック回路ボードに実装することができ、例えば、電磁コネクタの多数のE字型コア部材が回路ボードを通じて延伸する。実装態様では、コア部材は回路ボードから機械的に分離されてもよい（例えば、回路ボードに接触することなく）。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302およびパラレル通信インタフェース304は、シリアル通信インタフェース302およびパラレル通信インタフェース304を別個に実装するための多数の別個の半導体デバイス等のような、多数のコンポーネントにおける異なる配置(arrangement)を使用して実装されてもよい。

【0037】

[0042] スwitch・ファブリック300は、1つ以上のI/Oモジュール104を（例えば、スレーブ・デバイスとして）接続し、I/Oモジュール104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してもよい。I/Oモジュール104は、入力モジュール、出力モジュール、並びに／または入力および出力モジュールを含んでもよい。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104を、イメージ信号やスペクトル信号等を検出するためにイメージ・キャプチャ・デバイス200に接続することができ、或いは、ガス・プラントや精製所等の配管における圧力を測定するためのセンサのようなプロセス・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104は、産業用制御システム100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。即ち、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クリティカル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、並びに、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）である。

【0038】

[0043] スイッチ・ファブリック300を使用して送信されるデータは、パケット化されてもよい。即ち、データの別個の部分、データ部分をネットワーク制御情報等と共に含んだデータ・パケットに変換してもよい。産業用制御システム100／スイッチ・ファブリック300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100／スイッチ・ファブリック300は、国際標準化機構（ISO）13239規格等によるHDLCを実装してもよい。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106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100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。

【0039】

[0044] 産業用制御システム100は、米国特許出願第14／469,931号（米国特許第9,191,203として発行済）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装し、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100は、セキュリティ証明ソース（例えば、工場122）、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124）を含む。実施形態では、デバイス・ライフタイム管理システムは、セキュリティ証明インタプリメンタおよび鍵管理エンティティを備えることができる。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130、I/Oモジュール103、通信／制御モジュール106、および電力モジュール112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。

【0040】

[0045] 産業用制御システム100における多数の（例えば、各）デバイス130、I/Oモジュール104、通信／制御モジュール106、電源112や物理相互接続デバイス等には、産業用制御システム100の多数の（例えば、全ての）レベルにおいてセキュリティを提供するために、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んだ制御エレメント／サブシステムおよび／または産業用エレメントには、製造の間に（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100のセキュリティを高めるために、産業用制御システム100の鍵管理エンティティ

124によって生産時から管理することができる。例えば、鍵管理エンティティ124は、各製造サイトにおけるコンポーネントのために（例えば、イメージ・キャプチャ・デバイス200および他の産業用制御システム・エレメントに）一意の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。また、鍵管理エンティティ124は、更に、複数のコンポーネントが各コンポーネントの各製造サイトとは異なるサイトにおいて実装されるときに（例えば、コンポーネントが産業用制御システム100内に設置／使用されるときに）、セキュリティ証明を認証、無効化、または修正するように構成することができる。

【0041】

[0046] 幾らかの実施形態では、産業用制御システム100において、センサおよび／またはアクチュエータ等を含んだ制御エレメント／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。認証プロセスは、産業用制御システム100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んだ制御エレメント／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、認証プロセスは、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、そのエレメントおよび／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。

【0042】

[0047] 実装態様では、産業用制御システム100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100の各エレメントには、それ自体の一意の組（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、個々の組の鍵および証明書が規定される）。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、強固な暗号を提供／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装することができる。

【0043】

[0048] 認証プロセスの結果に基づいて、認証済みである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100内においてエレメントの部分的機能をイネーブルまたはディセーブルにすることができ、産業用制御システム100内において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100内におけるこのエレメントの機能を完全にディセーブルすることができる（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を促進しない）。この点に関し、各エレメント（例えば、通信／制御モジュール102やI/Oモジュール104等）は、他の産業用制御システム・エレメント（例えば、デバイス130やイメージ・キャプチャ・デバイス200等）のセキュリティ証明を、産業用制御システム・エレメントの各セキュリティ証明を利用して、認証シーケンスの成功または失敗に基づいて、認証、無効化、または修正するように構成してもよい。

【0044】

[0049] 実施形態では、産業用制御システム・エレメントは、該エレメントの各セキュリティ証明に基づいて、情報をセキュアに送信するための安全な通信経路、即ち「トンネル」を確立することができる。例えば、通信は、各セキュリティ証明に基づいて、第1の（送信）エレメントによって署名または暗号化されることができると共に、第2の（受信）エレメントによって認証される（例えば、検証または複合化される）ことができる。実施形態では、イメージ・キャプチャ・デバイス200は、安全なトンネルを介して、通信／制御モジュール106またはI/Oモジュール104（または産業用制御システム100の他のコンポーネント）に対し、処理済みイメージ信号（例えば、イメージ・フレーム、

10

20

30

40

50

スペクトル・データやメタデータ等）に関連付けられるデータを通信するように構成することができる。幾らかの実施形態では、イメージ・キャプチャ・デバイス 200 は、受信デバイスによって成功裡に認証した後または認証された後に、通信／制御モジュール 106 または I/O モジュール 104（または産業用制御システム 100 の他のコンポーネント）に情報を伝達するに過ぎない。

【0045】

[0050] 実施形態では、産業用制御システム 100 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(physically)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該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、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、注文する等を行うことができる）。

【0046】

[0051] 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に替えて、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 106）が、供給元であるが実際の製造元ではない特定の OEM に関連付けられる実施形態では、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 100 のエレメントの認証中に、認証されているエレメントが、産業用制御システム 100 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がなされたときに、エレメントの機能は、産業用制御システム 100 内部では少なくとも部分的にディセーブル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 100 の他エレメントとの間の通信（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 100 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 100 のエレメントの内 1 つが交換を必要とするとき、この機構(feature)は、産業用制御システム 100 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 100 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、および、そのエレメントを産業用制御システム 100 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術は、安全な産業用制御システム 100 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ものである。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ことを防止することができる。何故ならば、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 の販売代理人(reseller)には、元となる OEM によって第 1 セット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 100 内に設置することができる。この例では、第 2 の販売代理人には、同一の元となる OEM によって第 2 セットの（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 の販売代理人のエレメントは、産業用制御システム 100 内では動作することが妨げられることがある。何故ならば、これらは認証することができず、また、第 1 の販売代理人のエレメントと共に動作することができないからである。しかしながら、第 1 の販売代理人および第 2 の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、同一の産業用制御システム 100 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

10

20

30

40

50

も注記して然るべきである。更に、幾らかの実施形態では、相互動作を許容する販売代理店の間の契約(agreement)は、この契約が特定の顧客、顧客のグループや工場等のみに適用されるように実施することもできる。

【0047】

[0052] 他の例では、ユーザが産業用制御システム100内において誤って指定された(例えば、誤ってマーク付けされた)エレメントを実装しようとする可能性がある。例えば、誤ってマーク付けされたエレメントは、産業用制御システム100の他のエレメントのOEMと同一のOEMに当該エレメントが関連づけられたことを誤って示す物理指標が、そのエレメントにマーク付けされたという可能性もある。このような例では、産業用制御システム100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アラートすることができる。また、このプロセスは、産業用制御システム100ひえのセキュリティ向上を促進することもできる。何故なら、模造エレメントは、悪意のあるソフトウェアを産業用制御システム100内に混入させる可能性がある伝達手段(vehicle)となる場合がしばしばあるからである。実施形態では、認証プロセスは、産業用制御システム100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安全でないネットワークから物理的に分離されることを確認する。

【0048】

[0053] 実装態様では、安全産業用制御システム100は、鍵管理エンティティ124を含む。鍵管理エンティティ124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124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100のエレメント用に生成する。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のいずれか)における鍵に関係する。

【0049】

[0054] 実施形態では、鍵管理エンティティ124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124は、I/Oモジュール104、通信／制御モジュール106、およびネットワーク120とはリモートに位置することができる。例えば、ファイアウォール126が鍵管理エンティティ124を、制御エレメントまたはサブシステム102およびネットワーク120(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126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・パケットを分析することによって、また、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を判断することによって、入来および発出するネットワーク・トラフィックを制御する。つまり、ファイアウォール126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120)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128(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(barrier)を構築する。実施形態では、ファイアウォール126は、鍵管理エンティティ124と、制御エレメント若しくはサブシステム102の1つ以上、および／またはネットワーク120との間で選択的な(例えば、安全な)通信を可能にする。例えば、1つ以上のファイアウォールを産業用制御システム100内の様々な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120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。

【0050】

[0055] 更に、安全産業用制御システム100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100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124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100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124はこれら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された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124は、製造場所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。

【0051】

[0056] 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124は、（例えば、暗号化された通信パイプラインによって）、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、特定のコードの使用を確認して署名し、また、任意の特定のコードの使用を無効化し（例えば、除去し）、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124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100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124によって維持することができる。鍵管理エンティティ124は、そのエレメントとの通信を通じて鍵を無効化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機構の能力を高める。

【0052】

[0057] 実装態様では、鍵管理エンティティ124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120に、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124は中央システムまたは分散型システムとすることができる。更に、実施形態では、鍵管理エンティティ124をローカルまたはリモートで管理することができる。幾らかの実装態様では、鍵管理エンティティ124をネットワーク120および／または制御エレメント若しくはサブシステム102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124は、管理を提供することができ、および／または様々な方法で管理されることができる。例えば、鍵管理エンティティ124は、中央位置における顧客によって、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100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、レイヤに応じて実装／管理することができる。

【0053】

[0058] 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、スケーラブルで、ユーザ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106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、セキュリティを実装することができる。実装態様では、コードの暗号化がエレメントにおいて実装される一方で、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100全体に分散させること（例えば、フローさせること）ができる。例えば、セキュリティは、産業用制御システム100全てを、エンド・ユーザまでフローさせることができ、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）を提供する。

【0054】

[0059] 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、OE

10

20

30

40

50

M) によって製造および／若しくは供給されたエレメントの安全な産業用制御システム 100 内における相互運用性を提供し、並びに／または可能にするために実装することができる。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な（例えば、一部の）相互運用性を可能にすることができる。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）は、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 100 の異なるエレメントによって実行するのを可能にする。

【0055】

[0060] 更に、産業用制御システム 100 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置し（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）やデータ・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、アクション発起元(action originator) 204 と、通信／制御モジュール 106 または他の如何なる産業用エレメント／コントローラ 206 との間で送信されるデータ・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。

【0056】

[0061] 図 4 および図 5 に示すように、I/O モジュール 104、通信／制御モジュール 106、または他の産業用エレメント／コントローラ 406 は、少なくとも部分的に、アクション発起元(action originator) 402 からの要求／コマンドにしたがって動作することができる。例えば、アクション発起元 402 は、IOM 104 または CCM 106 からのデータにアクセスすることができ、および／または、これらに結合されたイメージ・キャプチャ・デバイス 200 若しくはフィールド・デバイス 130 のための 1 つ以上の変数のセッティングまたは調整に関連付けられる命令／要求を送信することができる。実装態様では、アクション発起元 402 は、オペレータ・インタフェース 408（例えば、SCADA または HMI）、エディタ 412 およびコンパイラ 414 を含む設計インタフェース 410、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 416（例えば、ネットワーク 418 を通じてローカル・アプリケーション 420 を介して通信する）等を含む。図 4 および図 5 に示す認証経路 400 では、産業用エレメント／コントローラ 406（例えば、IOM 104 または CCM 106）は、オペレータ・アクションがアクション認証器 404 によって署名および／または暗号化されたときにのみ、或いは、オペレータ・アクションに付随する通信（例えば、認証メッセージ）が署名および／または暗号化されたときにのみ、オペレータ・アクション（例えば、データ、1 つ以上のシステム変数を変更／調整する命令、設計インタフェース・コマンド、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オペレータ・アクションを防止し、更に、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装される。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。

【0057】

[0062] アクション認証器 344 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 402 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、標準的なオペレータ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、セキュアなワークステーション 426 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／または生体入力を要求することができる。

実施形態では、秘密鍵（例えば、セキュリティ証明）は、オンサイトまたはオフサイトの鍵管理エンティティ（例えば、オンサイトのデバイス寿命管理システム（「DLM」）422または、ネットワーク418を通じて接続されたリモートに配置されたDLM422）によってプロビジョニングすることができる。

【0058】

[0063] 幾らかの実施形態では、アクション認証器404は、（セキュアなマイクロプロセッサを含むことができる）スマート・カード424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、（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）デバイス全体を、アクション発起元402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オペレータまたはユーザと一緒に携行できるということである。アクション認証ノード404が認証経路400に、セキュアなワークステーションまたはセキュアで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402からのアクション要求は、あまりセキュアでな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100をセキュアにする。例えば、許可されていない人は、スマート・カード424を物理的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402を介して送られる如何なるアクション要求をも認証することはできない。

【0059】

[0064] 更にまた、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404は、セキュアなワークステーション426を含むことができる。セキュアな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することができない。加えて、セキュアなワークステーション426は、生体または多要素暗号デバイス428（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。幾らかの実施形態では、多要素暗号デバイス428は、スマート・カード424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、有効な生体入力を必要とする。

【0060】

[0065] アクション発起元402によって駆動される産業用エレメント／コントローラ406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。幾らかの実施形態では、産業用エレメント／コントローラ406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430（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。産業用エレメント／コントローラ406は、更に、オペレータ・アクションまたはそれに付随する通信を認証した後に、オペレータ・アクションに関連付けられるコードを実行／実施する（即ち、要求されたアクションを行う）プロセッサ432（例えば、マイクロコントローラ、マイクロプロセッサやASIC等）を含む。幾らかの実施形態では、オペレータ・アクションはアクション発起元402および／またはアクション認証器432によって暗号化され、また、プロセッサ432によって復号化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、産業用エレメント／コントローラ406は、仮想鍵スイッチ434（例えば、プロセッサ432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434は、オペレータ・アクションまたはそれに付随する通信が検証された後でのみ、プロセッサ432によってオペレータ・アクションを実施することを可能にする。例えば、仮想鍵スイッチ434は、プロセッサ432の1つ以上の動作モード（例えば、セーフ・モード、標準動作モードや安全動作モード等）を選択的にイネーブル／デ

イセーブルするように構成することができる。幾らかの実施形態では、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、産業用エレメント／コントローラ４０６によって実行(run on)されるよりも前に、認証経路をクリアしなければならない。例えば、パラメータ／プロセス変数の如何なる変更、またはイメージ・キャプチャ・デバイス２００またはフィールド・デバイス１３０に送られるデータ要求を含むことができる。

【００６１】

[0066] 上述したように、更なるセキュリティのために、イメージ・キャプチャ・デバイス２００が接続されている外部デバイス（例えば、ＩＯＭ１０４またはＣＣＭ１０６）と認証するために、イメージ・キャプチャ・デバイス２００は、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。始動、リセット、イメージ・キャプチャ・デバイス２００の設置、イメージ・キャプチャ・デバイス２００の交換、周期的や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、認証を生じさせることができる。イメージ・キャプチャ・デバイス２００が結合される外部デバイスと認証するのをイメージ・キャプチャ・デバイス２００に生じさせることによって、イメージ・キャプチャ・デバイス２００が偽造または悪意をもって混入されるのを回避することができる。実装態様では、外部デバイスは、少なくとも部分的に、イメージ・キャプチャ・デバイス２００の機構をディセーブルすることができ、或いは、認証が失敗したときにイメージ・キャプチャ・デバイス２００との通信を阻止することができる。

【００６２】

[0067] 図８は、認証シーケンスの実行において、イメージ・キャプチャ・デバイス２００および外部デバイス（例えば、ＩＯＭ１０４またはＣＣＭ１０６）との間に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、外部デバイスは、要求データグラム５０２をイメージ・キャプチャ・デバイス２００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）と、第１デバイス認証鍵（DAKA）を収容する第１デバイス認証鍵証明書（CertDAKA）と、第１識別情報属性証明書（IACA）とを含む。幾らかの実施形態では、外部デバイスは、真正乱数生成器（以後、「TRNG」と称する。）によって第１ノンス（Nonce A）を生成し、また、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、言い換えると結合して、要求データグラム５０２を生成するように構成される。幾らかの実施形態では、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、外部デバイスによってローカルに格納される。例えば、証明書がＩ／Ｏモジュール１０４または通信／制御モジュール１０６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）に格納されてもよい。

【００６３】

[0068] イメージ・キャプチャ・デバイス２００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。公開鍵は、デバイス寿命管理システム（DLM）によって生成され、または暗号ライブラリ機能を利用して導き出される、この点に関して、公開鍵は、イメージ・キャプチャ・デバイス２００のＳＲＡＭまたは他のローカル・メモリに格納され、また、外部デバイスとイメージ・キャプチャ・デバイス２００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されてもよい。幾らかの実施形態では、イメージ・キャプチャ・デバイス２００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と称する。）または他の検証処理によって証明書を検証してもよい。幾らかの実施形態では、イメージ・キャプチャ・デバイス２００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。即ち、証明書タイプが、各証明書に対してデバイス認証鍵（以後「DAK」と称する。）または識別情報属性証明書（以後「IAC」と称する。）であること、IAC名称が一致しDAK証明書

10

20

30

40

50

モジュール・タイプがモジュール・タイプ引数と一致すること、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・シリアル番号（以後「MP SN」と称する。）が互いに一致すること、である。幾らかの実施形態では、イメージ・キャプチャ・デバイス 200 は、更に、DAK および IAC 証明書がローカル無効化リスト (local revocation list)（例えば、無効化されたおよび／または有効でない証明書を含んだリストまたはデータベース）にないことを検証するように構成されてもよい。イメージ・キャプチャ・デバイス 200 が要求データグラムの有効性を判断できないときは、イメージ・キャプチャ・デバイス 200 はエラー・メッセージを生成し、部分的にまたは完全に外部デバイスをディセーブルし、および／または外部デバイスへ／からの通信を遮断若しくは制限してもよい。

【0064】

[0069] 有効な要求データグラム 502 に応答して、イメージ・キャプチャ・デバイス 200 は、応答データグラム 504 を外部デバイス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) と、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]) と、第 2 デバイス認証鍵 (DAK B) を商用する第 2 デバイス認証鍵証明書 (Cert DAK B) と、第 2 識別情報属性証明書 (IAC B) とを含む。幾らかの実施形態では、イメージ・キャプチャ・デバイス 200 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、言い換えると結合し、そして、連結された／結合されたノンスに、イメージ・キャプチャ・デバイス 200 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。イメージ・キャプチャ・デバイス 200 は、更に、第 2 ノンス (Nonce B) と、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]) と、第 2 デバイス認証鍵証明書 (Cert DAK B) と、第 2 識別情報属性証明書 (IAC B) とを連結、言い換えると結合して、応答データグラム 504 を生成するように構成される。幾らかの実施形態では、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、イメージ・キャプチャ・デバイス 200 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、イメージ・キャプチャ・デバイス 200 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）に格納されてもよい。

【0065】

[0070] 外部デバイスは、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導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。幾らかの実施形態では、外部デバイスは、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の有効性を判断するように構成されてもよい。即ち、IAC および DAK 証明書が一致する MP SN を有すること、IAC 名称が一致すること、(IAC および DAK の) 両方の証明書について証明書タイプが正しいこと、正しい発行者名称が両方の証明書にあること、DAK モジュール・タイプが正しいタイプであること（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）である。幾らかの実施形態では、外部デバイスは、更に、DAK および IAC 証明書がローカル無効化リストにはないことを検証するように構成されてもよい。

【0066】

[0071] 応答データグラムの有効性を判断するために、外部デバイスは、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、外部デバイスは、ローカルに格納された第 1 ノンス (Nonce A) と、イメージ・キャプチャ・デバイス 200 から受け取った第 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 D

A K BからのD A K 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 ノンスにおける暗号的に検証済みの連結と比較することによって、第1 署名 (S i g B [N o n c e A | | N o n c e B]) を検証するように構成される。外部デバイスが応答データグラムの有効性を判断できなかったときは、外部デバイスはエラー・メッセージを生成して、部分的または完全にイメージ・キャプチャ・デバイス200をディセーブルし、および／または、イメージ・キャプチャ・デバイス200へ／からの通信を遮断または制限してもよい。

【0067】

[0072] 更に、外部デバイスは、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をイメージ・キャプチャ・デバイス200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 (s i g A [N o n c e A | | N o n c e B]) を含む。幾らかの実施形態では、外部デバイスは、ローカルに生成された第1および第2 ノンスの連結に、外部デバイスによってローカルに格納されている秘密鍵 (例えば、D A K) 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有効ではない場合、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、外部デバイス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 (s i g A [N o n c e A | | E r r o r]) とを含む「失敗」認証データグラム506と置き換えてもよい。

【0068】

[0073] 認証データグラム506に回答して、イメージ・キャプチャ・デバイス200は、更に、応答認証データグラム508を外部デバイスに送信するように構成してもよい。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、イメージ・キャプチャ・デバイス200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 (S i g B [N o n c e A | | E r r o r]) とを含む。幾らかの実施形態では、イメージ・キャプチャ・デバイス200は、第1および第2 ノンスに関連付けられた第2 署名 (s i g A [N o n c e A | | N o n c e B]) 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。幾らかの実施形態では、イメージ・キャプチャ・デバイス200は、外部デバイスから受け取った第1 平文ノンス (N o n c e A) およびローカルに格納されている第2 ノンス (N o n c e B) を連結し、第2 暗号署名 (s i g A [N o n c e A | | N o n c e B]) を公開デバイス認証鍵によって検証し (例えば、C e r t D A K AからのD A K Aを使用して)、第1 ノンスおよび第2 ノンスについて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済みの連結と比較することによって、第2 署名 (s i g A [N o n c e A | | N o n c e B]) 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、イメージ・キャプチャ・デバイス200が認証データグラムの有効性を判断できなかったときに、イメージ・キャプチャ・デバイス200は、部分的または完全に外部デバイスをディセーブルし、および／または、外部デバイスへ／からの通信を遮断または制限してもよい。

【0069】

[0074] 実装態様では、上述したように、イメージ・キャプチャ・デバイス200および外部デバイスのロールは予約することができる。幾らかの実装態様では、外部デバイスおよびイメージ・キャプチャ・デバイスは、「マスタースレーブ」構成にしたがって配置される。ここでは、マスタ (例えば、外部デバイス) は、スレーブ (例えば、イメージ・キャプチャ・デバイス200) を認証するように構成してもよい。認証失敗の場合、マスタは、非認証のスレーブへ／からの通信を少なくとも部分的にディセーブルまたは制限してもよい。代替として、認証失敗の結果、デバイスまたは擬似副デバイスの双方を部分的にまたは完全にディセーブルにしてもよい。例えば、セキュリティを高めるために、外部デバイス (例えば、I O M 104またはC C M 106) およびイメージ・キャプチャ・デバイス200が認証シーケンスを成功して完了した場合に、これらをディセーブルすることができる。

【0070】

[0075] 本明細書で説明した産業用制御モジュール・エレメントのそれぞれは、本明細書において説明した機能を実行するためにイネーブルされる回路および／またはロジックを含んでもよい。例えば、各産業用制御システム・エレメント（例えば、IOM104、CCM106やイメージ・キャプチャ・デバイス200等）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（SSD）、光ディスク、磁気記憶デバイスやフラッシュ・ドライブ等のような、非一時的マシン読み取り可能媒体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命令を実行するように構成されるプロセッサを含んでもよい。更にまた、上述したように、本明細書で説明した産業制御システム・エレメントは、鍵管理エンティティ124（全ての産業用制御システム・エレメント用の同一の鍵管理エンティティでもよい）による使用時または出生時に（例えば、製造のサイトで）配置されるときに、一意のセキュリティ証明書によってプロビジョニングされることができる。これらのセキュリティ証明は、各デバイス内（例えば、暗号化されたメモリ内）に格納することができる。更にまた、如何なるオペレータ・アクション、要求やデータグラム等についての認証は、各産業用制御システム・エレメントの境界（confine）内で（例えば、外部の認証器を介するのではなく、組み込まれたセキュリティ証明（複数可）および各エレメントのプロセッサを使用して）生じさせることができる。この点に関し、固有（intrinsic）のセキュリティが産業用制御システム100の各レベル／レイヤで実装することができる。

10

【0071】

[0076] 尚、本明細書において説明した機能の如何なるものも、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、マニュアル処理、またはその組み合わせによって実装することができることが理解されてしかるべきである。つまり、上述した開示において検討したブロック、動作、機能、またはステップは、全般的に、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例では、上述した開示において検討した様々なブロックは、他の機能性と一緒に集積回路として実装されてもよい。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、或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されてもよい。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例では、上述した開示において検討した様々なブロックは、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。このような実例の幾らかでは、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均等物を使用して実装されてもよい。他の例では、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装される一方で、他の部分はハードウェアで実現されてもよい。

20

30

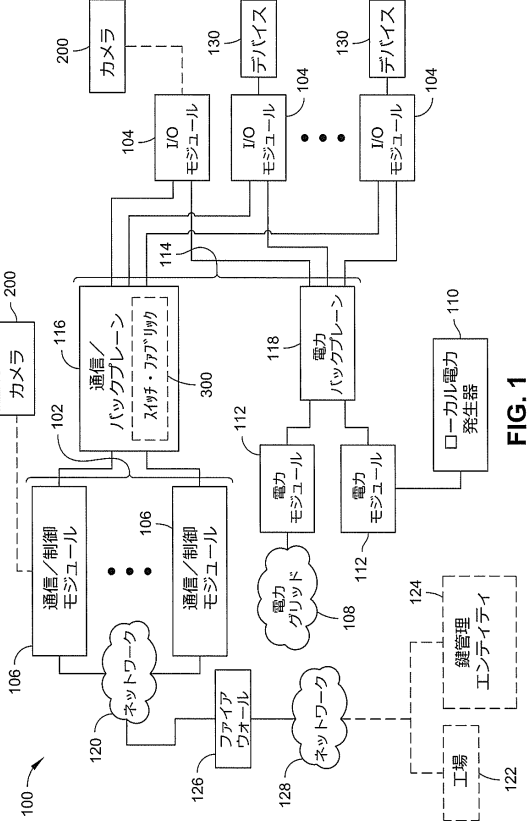
40

【0072】

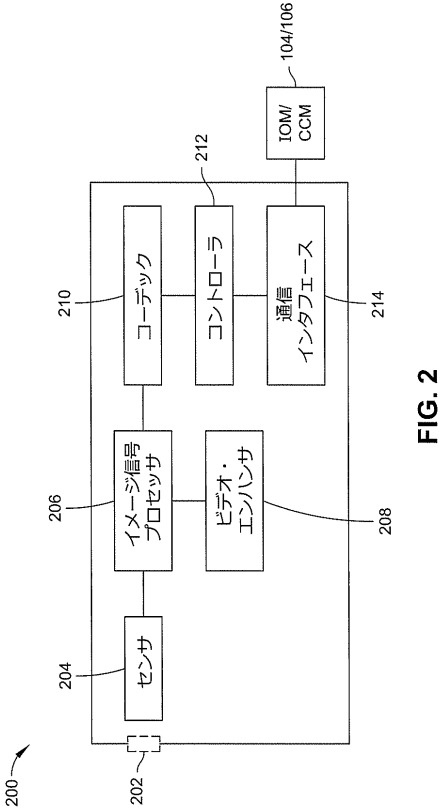
[0077] 以上、構造的特徴および／またはプロセス動作に特定の文言で主題について説明したが、添付した特許請求の範囲において定められる主題は、以上で説明した特定の特徴やアクトに必ずしも限定されないことは理解されてしかるべきである。逆に、以上で説明した特定の特徴やアクトは、特許請求の範囲を実現する形態例として開示されたまでである。

50

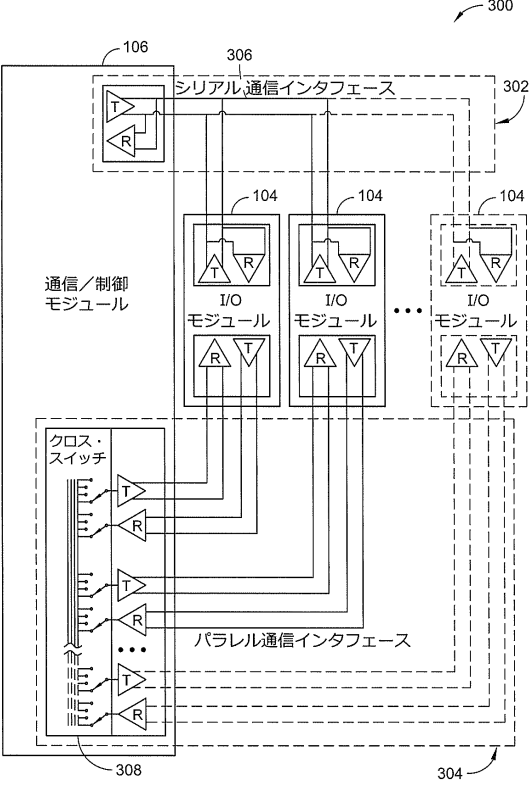
【図面】
【図 1】



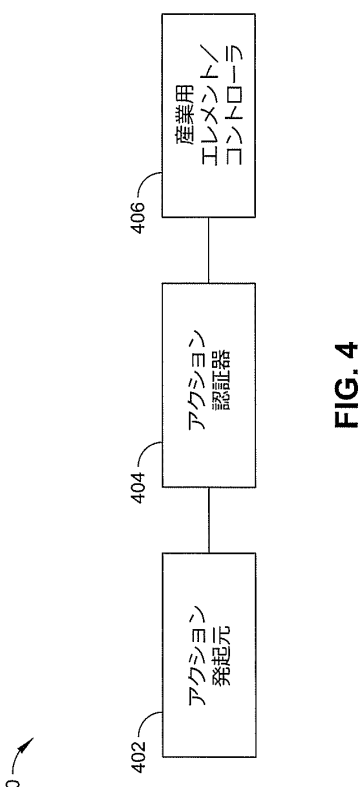
【図 2】



【図 3】



【図 4】



10

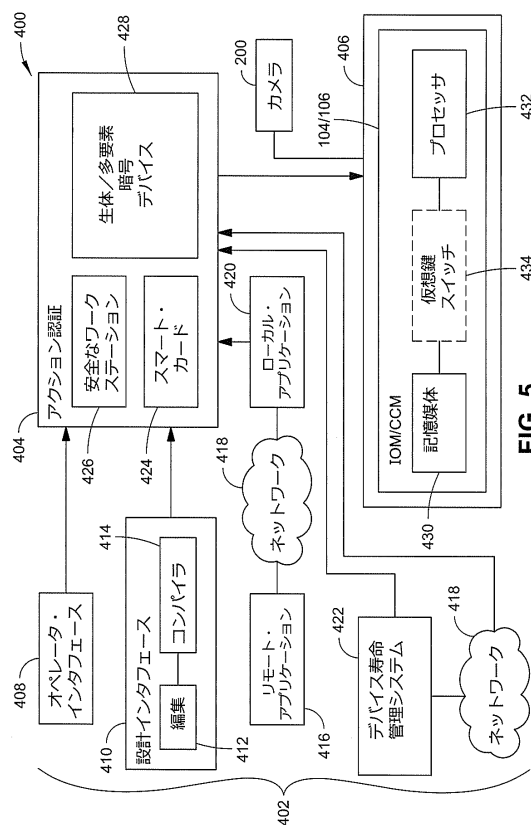
20

30

40

50

【図 5】



【図 6】



FIG. 6

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, ルビス・ドライブ 8 2 3

審査官 中里 裕正

(56)参考文献 特開 2 0 1 0 - 2 3 3 1 6 7 (J P, A)

特表 2 0 1 6 - 5 2 7 8 4 4 (J P, A)

特開 2 0 1 6 - 1 4 9 1 2 8 (J P, A)

国際公開第 2 0 1 4 / 0 6 1 3 0 7 (W O, A 1)

米国特許出願公開第 2 0 1 6 / 0 3 0 1 6 9 5 (U S, A 1)

(58)調査した分野 (Int.Cl., D B 名)

H 0 4 L 9 / 3 2

G 0 6 F 2 1 / 4 4