(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7050409号
(P7050409)

(45)発行日　令和4年4月8日(2022.4.8)

(24)登録日　令和4年3月31日(2022.3.31)

(51)国際特許分類

Ｈ０２Ｊ　13/00　(2006.01)	Ｈ０２Ｊ	13/00	３０１Ｂ	
Ｈ０２Ｊ　7/00　(2006.01)	Ｈ０２Ｊ	7/00	Ｙ	
Ｈ０２Ｊ　7/34　(2006.01)	Ｈ０２Ｊ	7/34	Ｂ	
Ｈ０４Ｑ　9/00　(2006.01)	Ｈ０４Ｑ	9/00	３０１Ａ	
Ｈ０１Ｍ　10/48　(2006.01)	Ｈ０１Ｍ	10/48	Ｐ	

ＦＩ

請求項の数　21　外国語出願　（全34頁）　最終頁に続く

(21)出願番号　特願2016-80207(P2016-80207)
(22)出願日　平成28年4月13日(2016.4.13)
(65)公開番号　特開2017-22968(P2017-22968A)
(43)公開日　平成29年1月26日(2017.1.26)
審査請求日　平成31年4月5日(2019.4.5)
(31)優先権主張番号　62/146,796
(32)優先日　平成27年4月13日(2015.4.13)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　15/096,701
(32)優先日　平成28年4月12日(2016.4.12)
(33)優先権主張国・地域又は機関
米国(US)
前置審査

(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　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９４０８７，サニーヴェール，ルビス・ドライブ ８２３

最終頁に続く

(54)【発明の名称】　産業用制御システムのための安全な電源

(57)【特許請求の範囲】
【請求項１】
電源であって、
バッテリ・セル、および前記バッテリ・セルと通信可能に結合され、前記バッテリ・セルを監視して、前記バッテリ・セルの動作情報および前記バッテリ・セルのステータス情報の少なくとも何れかを取得するように構成されるバッテリ・モニタを含む、バッテリ・モジュールと、
前記バッテリ・モジュールに動作可能に結合され、かつ、前記バッテリ・モニタとの双方向通信を行うように構成されたコントローラであって、前記バッテリ・セルの動作情報および前記バッテリ・セルのステータス情報の少なくとも何れかの情報を前記バッテリ・モニタから受け取り、前記情報に基づいてバッテリ・モジュールレベルでの前記バッテリ・セルの診断を行い、前記バッテリ・セルの動作情報、前記バッテリ・セルのステータス情報、および前記診断により得られた前記バッテリ・セルの診断情報の少なくとも何れかへのネットワーク・アクセスを提供するように構成される、コントローラと
を備え、
前記提供されるネットワーク・アクセスは、少なくとも前記診断情報を、ネットワークを介して外部の複数の電源にブロードキャストすることを含む、電源。
【請求項２】
前記バッテリ・セルがリチウム・イオン・バッテリ・セルを含む、請求項１記載の電源。
【請求項３】

複数のバッテリ・モジュールを備え、前記バッテリ・モジュールの各々がスタックされて前記バッテリ・モジュールの他の１つと接続するように構成される、請求項１記載の電源。
【請求項４】
前記バッテリ・モジュールの各々１つが物理的および電気的に保護されるように、それぞれのバッテリ・モジュール保護レイヤによってケース収容される、請求項３記載の電源。
【請求項５】
前記バッテリ・モジュール保護レイヤによってケース収容された前記複数のバッテリ・モジュールが物理的および電気的に保護されるように、前記複数のバッテリ・モジュールがさらにバッテリ・パック保護レイヤによってケース収容される、請求項４記載の電源。
【請求項６】
前記バッテリ・パック保護レイヤによってケース収容された前記複数のバッテリ・モジュールおよび前記コントローラが保護されるようにケース収容する電源保護レイヤを更に備え、前記電源保護レイヤが、１つ以上の方向に取り付け可能な剛性のケースを規定する、請求項５記載の電源。
【請求項７】
前記診断情報が前記バッテリ・セルの動作電圧、前記バッテリ・セルの動作電流、前記バッテリ・セルに関連づけられる電荷、または前記バッテリ・セルに関連づけられる経過年数の少なくとも１つを含む、請求項１記載の電源。
【請求項８】
電源ネットワークであって、
複数の分散電源を備え、前記複数の分散電源が相互に通信し、各電源が、
バッテリ・セル、および前記バッテリ・セルと通信可能に結合され、前記バッテリ・セルを監視して、前記バッテリ・セルの動作情報および前記バッテリ・セルのステータス情報の少なくとも何れかを取得するように構成されるバッテリ・モニタを含む、バッテリ・モジュールと、
前記バッテリ・モジュールに動作可能に結合され、かつ、前記バッテリ・モニタとの双方向通信を行うように構成されたコントローラであって、前記バッテリ・セルの動作情報および前記バッテリ・セルのステータス情報の少なくとも何れかの情報を前記バッテリ・モニタから受け取り、前記情報に基づいてバッテリ・モジュールレベルでの前記バッテリ・セルの診断を行い、前記バッテリ・セルの動作情報、前記バッテリ・セルのステータス情報、および前記診断により得られた前記バッテリ・セルの診断情報の少なくとも何れかへのネットワーク・アクセスを提供するように構成される、コントローラと
を備え、
前記提供されるネットワーク・アクセスは、少なくとも前記診断情報を、ネットワークを介して外部の複数の電源にブロードキャストすることを含む、電源ネットワーク。
【請求項９】
前記バッテリ・セルがリチウム・イオン・バッテリ・セルを含む請求項８記載の電源ネットワーク。
【請求項１０】
各電源が複数のバッテリ・モジュールを備え、前記バッテリ・モジュールの各々が、スタックされて前記バッテリ・モジュールの他の１つと接続するように構成される、請求項８記載の電源ネットワーク。
【請求項１１】
前記バッテリ・モジュールの各々１つが物理的および電気的に保護されるように、それぞれのバッテリ・モジュール保護レイヤによってケース収容される、請求項１０記載の電源ネットワーク。
【請求項１２】
前記バッテリ・モジュール保護レイヤによってケース収容された前記複数のバッテリ・モジュールが物理的および電気的に保護されるように、前記複数のバッテリ・モジュールがさらにバッテリ・パック保護レイヤによってケース収容される、請求項１１記載の電源ネ

ットワーク。
【請求項１３】
各電源が更に、前記バッテリ・パック保護レイヤによってケース収容された前記複数のバッテリ・モジュールおよび前記コントローラが保護されるようにケース収容する電源保護レイヤを備え、前記電源保護レイヤが１つ以上の方向に取り付け可能な剛性のケースを規定する、請求項１２記載の電源ネットワーク。
【請求項１４】
前記診断情報が前記バッテリ・セルの動作電圧、前記バッテリ・セルの動作電流、前記バッテリ・セルに関連づけられる電荷、または前記バッテリ・セルに関連づけられる経過年数の少なくとも１つを含む、請求項８記載の電源ネットワーク。
【請求項１５】
産業用制御システムであって、
制御モジュールと、
前記制御モジュールによって制御および監視される入力／出力モジュールであって、センサからの入力信号を受け取り、またはアクチュエータ若しくはモータに出力信号を供給するように構成される、入力／出力モジュールと、
前記制御モジュールおよび前記入力／出力モジュールの少なくとも１つに電力を供給する電力モジュールと、
前記電力モジュールに対し電力を分散させる電源であって、
バッテリ・セル、および前記バッテリ・セルと通信可能に結合され、前記バッテリ・セルを監視して、前記バッテリ・セルの動作情報および前記バッテリ・セルのステータス情報の少なくとも何れかを取得するように構成されるバッテリ・モニタを含む、バッテリ・モジュールと、
前記バッテリ・モジュールに動作可能に結合され、かつ、前記バッテリ・モニタとの双方向通信を行うように構成されたコントローラであって、前記バッテリ・セルの動作情報および前記バッテリ・セルのステータス情報の少なくとも何れかの情報を前記バッテリ・モニタから受け取り、前記情報に基づいてバッテリ・モジュールレベルでの前記バッテリ・セルの診断を行い、前記バッテリ・セルの動作情報、前記バッテリ・セルのステータス情報、および前記診断により得られた前記バッテリ・セルの診断情報の少なくとも何れかへのネットワーク・アクセスを提供するように構成される、コントローラと
を備え、
前記提供されるネットワーク・アクセスは、少なくとも前記診断情報を、ネットワークを介して外部の複数の電源にブロードキャストすることを含む、電源と
を備える、産業用制御システム。
【請求項１６】
前記バッテリ・セルがリチウム・イオン・バッテリ・セルを含む、請求項１５記載の産業用制御システム。
【請求項１７】
前記電源が複数のバッテリ・モジュールを備え、該バッテリ・モジュールの各々が、スタックされて前記バッテリ・モジュールの他の１つと接続するように構成される、請求項１５記載の産業用制御システム。
【請求項１８】
前記バッテリ・モジュールの各々１つが物理的および電気的に保護されるように、それぞれのバッテリ・モジュール保護レイヤによってケース収容される、請求項１７記載の産業用制御システム。
【請求項１９】
前記バッテリ・モジュール保護レイヤによってケース収容された前記複数のバッテリ・モジュールが物理的および電気的に保護されるように、前記複数のバッテリ・モジュールがさらにバッテリ・パック保護レイヤによってケース収容される、請求項１８記載の産業用制御システム。

【請求項２０】
前記バッテリ・パック保護レイヤによってケース収容された前記複数のバッテリ・モジュールおよび前記コントローラが保護されるようにケース収容する電源保護レイヤを更に備え、前記電源保護レイヤが１つ以上の方向に取り付け可能な剛性のケースを規定する、請求項１９記載の産業用制御システム。
【請求項２１】
前記診断情報が前記バッテリ・セルの動作電圧、前記バッテリ・セルの動作電流、前記バッテリ・セルに関連づけられる電荷、または前記バッテリ・セルに関連づけられる経過年数の少なくとも１つを含む、請求項１５記載の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] 本願は、２０１５年４月１３日に出願され "POWER SUPPLY SYSTEM"と題する米国仮特許出願第６２／１４６，７９６号に対して、35 U.S.C. § 119(e)に基づく優先権を主張するものである。また、本願は、２０１４年１０月２０日に出願され "SECURE POWER SUPPLY FOR AN INDUSTRIAL CONTROL SYSTEM"と題する米国特許出願第１４／５１９，０３２号の一部継続出願でもある。米国特許出願第１４／５１９，０３２号は、２０１４年２月１４日に出願され"BACKUP POWER SUPPLY"と題する米国仮特許出願第６１／９４０，００３号に対して、35 U.S.C. § 119(e)に基づく優先権を主張するものである。また、米国特許出願第１４／５１９，０３２号は、２０１３年８月６日に出願され "SECURE INDUSTRIAL CONTROL SYSTEM"と題する 国際出願第ＰＣＴ/ＵＳ２０１３/０５３７２１号の一部継続出願でもある。また、本願は、２０１４年８月２７日に出願され "SECURE INDUSTRIAL CONTROL SYSTEM"と題する米国特許出願第１４／４６９，９３１号の一部継続出願でもある。また、米国特許出願第１４／４６９，９３１号は、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号の一部継続出願でもあり、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ものである。以上で相互引用した仮特許出願および特許出願の各々は、ここで引用したことにより、その内容全体が本願に含まれるものとする。
【背景技術】
【０００２】
[0002] 標準的な産業用制御システム（ＩＣＳ）またはプログラム可能自動化コントローラ（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／またはオペレータ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。
【０００３】
[0003] 他の例では、ＳＣＡＤＡシステムは、地理的に広範囲にわたり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リモート端末ユニット（ＲＴ

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

【発明の概要】

【発明が解決しようとする課題】

【０００４】

[0004] 産業用制御システム、または分散電源ネットワークを含む如何なるシステムのための電源(power supply)が開示される。実施形態では、電源は、バッテリ・セルおよびバッテリ・セルを監視するように構成されるバッテリ・モニタを含むバッテリ・モジュールを含む。実施形態において、電源はまた、バッテリ・モジュールに動作可能に結合されたセルフ・ホスト・サーバを備える。セルフ・ホスト・サーバは、診断情報をバッテリ・モニタから受け取り、診断情報へのネットワーク・アクセスを提供するように構成される。実装態様では、セルフ・ホスト・サーバが格納した診断情報は、企業制御／監視システム、アプリケーション制御／監視システム、または安全なネットワーク（例えば安全なアクセス・クラウド・コンピューティング環境）を介して他のリモート・システムにブロードキャストされるか、またはリモートでアクセスされる。

【０００５】

[0005] 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。

【０００６】

[0006] 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】

【０００７】

【図１】図１は、本開示の例示の実施形態による１つ以上の認証モジュールを含む電源を示すブロック図である。

【図２】図２は、本開示の例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、本開示の例示の実施形態による図２の産業用制御システムのような産業用制御システムを示すブロック図である。産業用制御システムは、電力グリッドおよび１つ以上の局所発電機のような多数のソースから電力を受け取り、また、１つ以上のバックアップ電源が、多数のバッテリ・モジュールを使用して電気エネルギーを蓄積および返流するように構成される。

【図４】図４は、本開示の例示の実施形態による図２の産業用システムのようなシステムと通信可能に結合するように構成され、また、電気エネルギーを蓄積および返流ために電源（例えば、図２の電力グリッドおよび／または局所発電機）に接続するように構成されるバックアップ電源を示すブロック図である。バックアップ電源はコントローラおよび多

数のバッテリ・モジュールを含み、各バッテリ・モジュールはコントローラに通信可能に接続されるバッテリ・モニタを含む。
【図５】図５は、図４に示したバックアップ電源のようなバックアップ電源を示すブロック図である。バックアップ電源は、図２の産業用制御システムのようなシステムに通信可能に結合される。バックアップ装置はまた、本開示の例示の実施形態によるバックアップ電源と共に含まれる多数のバッテリ・モジュールのステータスに関する情報をシステムに提供するように構成されるコントローラも含む。
【図６】図６は、安全な制御システムのブロック図である。安全な制御システムは、本開示の例示の実施形態による図１に示した電源のようなデバイス、および／または図１に示した電源に接続された受電デバイスのような他のデバイスを認証する。
【図７】図７は、本開示の例示の実施形態による図６の安全な制御システムのような産業用制御システムについての行動認証パスを示すブロック図である。
【図８】図８は、本開示の例示の実施形態による図７の行動認証パスを更に示すブロック図である。
【図９】図９は、本開示の例示の実施形態によるアクション要求を認証する方法を示すフロー図である。
【図１０】図１０は、本開示の例示の実施形態によるバッテリ・モジュールを示すブロック図である。
【図１１】図１１は、本開示の例示の実施形態による電源および産業用制御システム・エレメントの間の接続性について示すブロック図である。
【図１２】図１２は、本開示の例示の実施形態による第１電源および１つ以上の冗長構成の電源の間の接続性について示すブロック図である。
【発明を実施するための形態】
【０００８】
概要
[0019] 産業用制御システムの設定(setting)では、電力は通例、局所発電(local power generation)（例えば、現場の(on-site)タービンまたはディーゼル局所発電機）等を用いた（例えば、ＡＣ主電源からの高電圧電力を使用する）電力グリッドから、コントローラや入力／出力（I／O）モジュール等のような自動化機器に供給される。しばしば、バックアップ電力はまた、バッテリから自動化機器(automation equipment)にこれら設定で供給される。例えば、大規模バッテリ・ストレージは、鉛酸蓄電池を使用する産業用の設定で設けることができる。大規模バッテリ・ストレージからの電力は、集中化した交流（ＡＣ）電力伝送技術を使用して供給することができる。他の例では、より小規模に分散した直流（ＤＣ）バッテリ供給が使用される。例えば、バックアップ電力は、キャビネット、コントローラやＩ／Ｏモジュール等のレベルで、より小規模の鉛酸蓄電池によって供給される。しかしながら、鉛酸蓄電池は、より新しい再充電可能なバッテリ技術（例えばリチウム・イオン電池）と比較すると、相対的に低エネルギー密度しか有さない。更に、これらの構成では、バックアップ・バッテリは通常、制御ハードウェアから分離され、バッテリのステータスを監視するために、各バッテリへの個別の接続を必要とする。例えば、産業用オートメーションでのバックアップ・バッテリは、通例、このようなバッテリの動作（例えば、オン／オフのステータス）を監視するために、制御ハードウェアの予備のＩ／Ｏポートに接続される。
【０００９】
[0020] 産業用制御システム、または分散電源ネットワークを含む如何なるシステムのための電源を開示する。電源は、バッテリ・セル、およびバッテリ・セルを監視するように構成されるバッテリ・モニタを含むバッテリ・モジュールを含む。実施形態では、電源はまた、バッテリ・モジュールに動作可能に結合されるセルフ・ホスト・サーバ(self-hosted server)を有する。セルフ・ホスト・サーバは、診断情報をバッテリ・モニタから受け取り、診断情報へのネットワーク・アクセスを提供するように構成される。実装態様では、セルフ・ホスト・サーバに格納された診断情報は、企業(enterprise)制御／監視システ

ム、アプリケーション制御／監視システム、または安全なネットワーク（例えば、セキュア・アクセス・クラウド・コンピューティング環境）を介して他のリモート・システムにブロードキャストすることができ、またはこれらによってリモートにアクセスすることができる。電源ネットワークは、分散された複数の電源を含むことができる。分散された電源は（例えば、それぞれのサーバ間のネットワークを介して）相互に通信してもよい。

【００１０】

[0021] 産業用制御システムは、少なくとも１つの入力／出力モジュールに結合される少なくとも１つの制御モジュールを含むことができる。入力／出力モジュールは、制御モジュールによって制御および監視される。ここでは、入力／出力モジュールは、センサから入力信号を受け取り、または、アクチュエータ若しくはモータに出力信号を供給するように構成される。制御モジュールおよび／または入力／出力モジュールは、当該制御モジュールおよび／または入力／出力モジュールに電力を供給する電力モジュールに結合することができる。実施形態の中には、第１電力モジュールは、制御モジュールおよび入力／出力モジュールの両方にサービス提供するものもある。他の実施形態では、第１電力モジュールが制御モジュールにサービス提供し、また、第２電力モジュールが入力／出力モジュールにサービス提供するものもある。更に、多数の制御モジュールおよび／または多数の入力／出力モジュールを実装できることが理解される。上述の例は、例示目的で提供され、システムを、単一の制御モジュール、入力／出力モジュール、または電力モジュールに限定するものと理解されてはならないものである。産業用制御システムは、電力モジュールに対し電力を配給するための１つ以上の電源（例えば、スタンドアロン電源または電源の分散ネットワーク）を含むことができる。

【００１１】

[0022] 本明細書において、無停電電源（ＵＰＳ）のような産業用制御システムにおいてバッテリの供給の監視および／または制御を強化するシステムおよび技術についても説明する。説明する技術およびシステムは、リチウム・イオン再充電可能バッテリ技術のような、より高エネルギー密度再充電可能バッテリ技術を使用して実装することができる。開示する実施形態では、産業用ＵＰＳは、通信および／またはセキュリティ機構（例えば双方向通信システム、制御システム・インテグレーション、サイバー・セキュリティ統合等）への供給を行う。例えば、産業用ＵＰＳは、ステータス情報、診断情報、信頼性情報および双方向通信等を提供する。実施形態の中には、産業用ＵＰＳが鍵暗号化マイクロコントローラ技術を実装するものもある。

【００１２】

[0023] 実施形態の中には、電源は電気回路（例えば、印刷回路基板（ＰＣＢ）、集積回路（ＩＣ）チップ、および／または他の回路）を含むものもある。電気回路は、電源および／または該電源に接続されたデバイスの認証を実行することができる。これにより、特定の電源または電源のタイプで使用することを意図しないデバイスに電源のプラグを繋ぐ可能性を防止または最小化することができる（例えば、低電圧電源のプラグを高電圧デバイスに繋ぐ可能性を防止または最小化する）。例えば、電源が適切なおよび／または所望のデバイスと組になる(mate)のを検証するために、電源は、結合されたモジュールとの「ハンドシェーク」動作を実行する。実施形態の中には、発光ダイオード（ＬＥＤ）のインジケータ・ライトのようなインジケータが、当該認証の通知を提供するのに使用されるものもある。例えば、多色ＬＥＤまたは単色ＬＥＤによって診断情報が提供されて、（例えば、同一調の明るさ(glow)、明るさがない、点滅、１ステータスに対し１色および他のステータスに対し他の色等を使用して）認証のステータスを示すことができる。

【００１３】

[0024] 実施形態の中には、電源を使用して、別のデバイス（例えば、電源から電力を受ける計器）を認証できるものもある。例えば、電源の電気回路を使用して、受電デバイス、受電デバイスのタイプ、および受電デバイスの製造業者等を認証することができる。このように、産業用オートメーション設定が偽造された機器の使用を防止または最小化することができる。更に、電源を使用して、コントローラ、入力／出力（Ｉ／Ｏ）モジュール

、エンド・デバイス、現場(field)デバイス（例えば、プロセス・センサおよび／またはアクチュエータ）等のような機器に対し、それ自体を認証することができる。実施形態の中には、電源は、電源と当該電源に接続されたデバイスとの間の暗号通信を促進するものもある。例えば、電源は、電源とエンド・デバイスや現場デバイス等との間の双方向の暗号通信を提供することができる。更に、実施形態の中には、オペレータは、現場デバイス（例えばセンサ、アクチュエータ、または如何なる他の計器も）に関する認証情報を取得するために、ネットワークに接続される電源を使用できるものもある。実施形態の中には、２つ以上の認証モジュール（例えば、第１認証モジュールおよび第２認証モジュール）は、新たなデバイスの設置の時、スタートアップ／リセット時に、周期的に、予定された時点に、および／または好ましいイベント時において、認証シーケンスを実行する（例えば、「ハンドシェーク」）ように構成されるものもある。認証モジュールが他のデバイスの認証、および／または相互の認証に失敗する場合に、デバイスの少なくとも１つ（例えば、認証されていないデバイス）は、他のデバイスと通信することに対し、部分的にまたは完全にディセーブルおよび／または制限することができる。

【００１４】

[0025] 産業用制御システムでは、制御エレメント／サブシステム（例えば、１つ以上の通信／制御モジュール）によって、様々な産業用エレメント（例えば、入力／出力モジュール、電力モジュール、現場デバイス、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）が制御され、または駆動される。制御エレメント／サブシステムは、アクション発起元(action originator)から受け取るプログラミングおよびアクション要求（例えば、実行可能なソフトウェア・モジュール、制御コマンド、およびデータ要求等）にしたがって動作する。アクション発起元は、これに限定されないが、例えば、オペレータ・インタフェース（例えば、ＳＣＡＤＡまたはヒューマン・マシン・インタフェース（ＨＭＩ））、設計インタフェース、ローカル・アプリケーションやリモート・アプリケーション等である。複数のアクション発起元が存在する場合に、産業用制御システムは、データおよび／または制御への認証されていないアクセスに対して脆弱となることがある。更に、産業用制御システムは、マルウェア、スパイウェア、または他の不正／悪意のあるソフトウェアに対して脆弱となる場合がある。当該ソフトウェアは、アップデート、アプリケーション・イメージや制御コマンド等の形態で送信されることがある。単純にオペレータを認証するだけでは、悪意のある行為や、更には意図しない要求／コマンドからもシステムを安全にするには不十分である。当該意図しない要求／コマンドは、有効なログインを介して生成されること、または見かけ上有効な（例えばハックされた）アプリケーション若しくはオペレータ／設計インタフェースを介して生成されることがある。

【００１５】

[0026] 本開示は、認証されていないアクション要求が産業用制御システムで処理されるのを防止するためのコントローラ、システムおよび技術に向けられる。好適な動作の選択若しくは全オペレータ・アクション、および／または他の制御アクション若しくは要求は、アクション発起元から産業用エレメント／コントローラ（例えば、通信／制御モジュール、入力／出力（Ｉ／Ｏ）モジュール、電力モジュール、現場デバイス、スイッチ、ワークステーションや物理相互接続デバイス等）までの認証パスを介して安全なものとすることができる。実装態様では、産業用制御システムは、アクション発起元によって生成されるアクション要求に署名するアクション認証器を必要とする。署名されていないアクション要求は結果として自動的にエラーとなり、産業用エレメント／コントローラによって処理または実行されることにはならない。産業用エレメント／コントローラは、署名されたアクション要求を受け取り、署名されたアクション要求の信頼性(authenticity)を検証し、そして、署名されたアクション要求の信頼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することができる。このようにして、悪意のある、または認証されていないアクション要求は処理されない。つまり、システムは、マルウェア、スパイウェア、制御パラメータについての認証されていない変更、およびデータに対する認証されていないアクセス等から保護することができる。

【００１６】

例示の実装態様

[0027] 図１から図１２を包括的に参照して、本開示による例示の電源について説明する。実施形態の中には、（例えば図１に示されるように）電源１２０は、電源１２０を認証するように構成される１つ以上の認証モジュール１３４、および／または電源１２０に接続されたデバイス（例えば、Ｉ／Ｏモジュール１０２や制御モジュール１０４等）に対する、電源１２０の１つ以上のバッテリ・モジュール１２２を含むものがある。認証モジュール１３４はまた、電源１２０に接続された１つ以上のデバイスを認証するのに使用することもできる。実施形態の中には、認証モジュール１３４は、電源１２０に関連付けられる一意の識別子１３６および／またはセキュリティ証明書１３８を格納するものもある（例えば、図５に示すように、認証モジュールは、プロセッサ１４０と、1つ以上の一意識別子１３６および／またはセキュリティ証明書１３８を格納するメモリ１４２とを含んだコントローラ１２８を使用して実装される。）。認証モジュール１３４は、電源１２０に接続されたデバイスへの接続を、認証に基づいて確立および／または防止するように構成することができる。電源１２０はまた、（例えば、オペレータに対する）認証を示すために、インジケータ（例えばインジケータ・ライト１４４）を含むこともできる。

【００１７】

[0028] 実施形態の中には、電源１２０はアラート・モジュール１４６を含むものもある。開示する実施形態では、アラート・モジュール１４６は、電源１２０および／または電源１２０に接続されたデバイスに対して、条件および／または条件のセットが満たされるときに、アラートを与えるように構成される。例えば、電源１２０および電源１２０に接続されたデバイスの認証が得られたとき、並びに／または認証に失敗したときに、アラートは認証モジュール１３４によって発生され、アラート・モジュール１４６によって与えられる。例えば、電源１２０は、結合された受電デバイス（例えば、Ｉ／Ｏモジュール１０２および／または制御モジュール）との「ハンドシェーク」動作を実行して、その結果、電源１２０が適切および／または所望のデバイスと組になったことを検証することができる。そうでない場合は、アラート・モジュール１４６は、（例えば、ネットワークを介して）オペレータにアラートするように使用することができる。実施形態の中には、アラートは、電子メールの形態でオペレータに与えられるものもある。他の実施態様では、アラートは、テキスト・メッセージの形態でオペレータに与えられる。しかしながら、これらアラートは、例示として設けられ、本開示を制限するのを意図するのではない。他の実施態様では、異なるアラートがオペレータに与えられる。条件が、（例えば、電子メールやテキスト・メッセージ等の）認証手順を満たすときは更に、多数のアラートをオペレータに提供することもできる。なお、これに限定されないが次の他の条件について、認証モジュール１３４および／またはアラート・モジュール１４６によって認証を設けることもできることが留意されるべきである。即ち、電源故障、バッテリ・モジュール故障、接続したデバイス故障、並びに電源および／または受電デバイスの様々なエラーの条件等である。

【００１８】

[0029] 認証モジュール１３４はまた、電源１２０と電源１２０に接続された１つ以上のデバイスとの間の通信を暗号化するように構成することもできる。図１に示すように、電源１２０は、暗号化モジュール１４８を含むことができる。例えば、１つ以上の暗号プロトコルを使用して、電源１２０および受電デバイスの間で情報を送信することができる。このような暗号プロトコルの例には、必ずしもこれに限定されないが、トランスポート層セキュリティ（ＴＬＳ）プロトコルやセキュア・ソケット層（ＳＳＬ）プロトコル等を含む。例えば、電源１２０および受電デバイスの間の通信は、ＨＴＴＰセキュア（ＨＴＴＰＳ）プロトコルを使用することができる。ＨＴＴＰプロトコルはＳＳＬおよび／またはＴＬＳプロトコル上でレイヤ化される。

【００１９】

[0030] 実施形態の中には、電源１２０と該電源１２０に接続されたデバイスとの間で認

証シーケンスを実行することができるものもある。例えば、コントローラ１２８の認証モジュール１３４を使用して認証シーケンスを実行することにより、電源１２０は、結合されたＩ／Ｏデバイス１０２や制御モジュール１０４等を認証する。他の実施形態では、電源１２０に接続されたデバイスが電源１２０を認証することができる。例えば、コントローラ１２８の認証モジュール１３４を使用して認証シーケンスを実行することにより、制御モジュール１０４が、結合された電源１２０を認証する。更なる実施形態では、１つの電源１２０が他の電源１２０を認証することができる。例えば、第１電源１２０のコントローラ１２８が有する第１認証モジュール１３４と、第２電源１２０のコントローラ１２８が有する第２認証モジュール１３４との間で認証シーケンスを実行することにより、第１電源１２０が（例えば冗長構成の）第２電源１２０を認証する。実施形態の中には、第２電源１２０がまた第１電源を認証することができるものもある。

【００２０】

[0031] なお、プロセッサ１４０およびメモリ１４２が（例えば、図１を参照して）コントローラ１２８の一部として若干特定して説明される一方で、本構成は例示のものとして設けられ、本開示を限定することを意図するのではないことが留意されるべきである。つまり、バッテリ・モジュール１２２の１つ以上は、（例えば、コントローラ１２８と共に含まれるプロセッサ１４０およびメモリ１４２に加えて、或いはその代わりに）プロセッサやメモリ等をまた含むことができる。このような実施形態では、バッテリ・モジュール１２２の１つ以上は１つ以上の認証モジュール１３４を含むことができる。ここでは、例えば、認証モジュール１３４はプロセッサおよびメモリ（おそらくは１つ以上の鍵、証明書、一意識別子、セキュリティ証明書等）を採用して、１つ以上の他のデバイス（例えば、他のバッテリ・モジュール１２２、コントローラ１２８、サブシステムの制御エレメント等）に対し、バッテリ・モジュール１３４を認証することができ、並びに／または、電源１２０と結合された他のデバイス（例えば、他のバッテリ・モジュール１２２、コントローラ１２８、および制御エレメントまたはサブシステム等）を認証することができる。

【００２１】

[0032] 実施形態の中には、バッテリ・モジュール１３４は、電源１２０のコントローラ１２８および／または、接続されたデバイス（例えば、電源１２０と結合された受電デバイス）を認証することができるものもある。例えば、バッテリ・モジュール１２２は、該バッテリ・モジュール１２２が有する認証モジュール１３４を使用して認証シーケンスを実行することにより、電源１２０のコントローラ１２８、および／または結合されたＩ／Ｏデバイス１０２、並びに制御モジュール１０４等を認証する。他の実施態様では、電源１２０に接続された受電デバイスは、バッテリ・モジュール１２２の１つ以上を認証することができる。例えば、制御モジュール１０４は、各バッテリ・モジュール１３４が有する認証モジュール１３４を使用して認証シーケンスを実行することにより、接続された電源１２０の１つ以上の（例えば各）バッテリ・モジュール１２２を認証する。

【００２２】

[0033] 実施形態の中には、コントローラ１２８がバッテリ・モジュール１２２の１つ以上を認証することができるものもある。例えば、コントローラ１２８は、該コントローラ１２８が有する認証モジュールと各バッテリ・モジュール１２２の認証モジュール１３４との間で認証シーケンスを実行することにより、１つ以上のバッテリ・モジュール１２２を認証する。更なる実施形態では、１つのバッテリ・モジュール１２２が他のバッテリ・モジュール１２２を認証することができる。例えば、第１バッテリ・モジュール１２２は、該第１バッテリ・モジュール１２２が有する第１認証モジュール１３４と第２バッテリ・モジュール１２２が有する第２認証モジュール１３４との間で認証シーケンスを実行することにより、第２バッテリ・モジュール１２２を認証する。実施形態の中には、第２バッテリ・モジュール１２２がまた第１バッテリ・モジュール１２２を認証することができるものもある。

【００２３】

[0001] 電源１２０は、産業用制御システムと共に使用することができる。図２を参照し

て、例えば、本開示による例示の産業用制御システム１００について説明する。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化コントローラ（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。産業用制御システム１００は、制御エレメントおよびサブシステムを含む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。ここでは、サブシステムは、システムにわたって分散された１つ以上のコントローラによって制御される。例えば、１つ以上のＩ／Ｏモジュール１０２が１つ以上の制御モジュール１０４に接続される。産業用制御システム１００は、Ｉ／Ｏモジュール１０２に、そしてＩ／Ｏモジュール１０２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１０２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、プロセスにおいて入力センサから情報を受けるために使用することができ、一方で、出力モジュールは、命令を出力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１０２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１０６（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）に接続することができ、および／またはプロセス・アクチュエータ１０８（例えば、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、送信機等）に接続することができる。

【００２４】

[0034] 実装態様では、Ｉ／Ｏモジュール１０２は制御システムに使用することができ、また、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のに使用することができる。即ち、製造、生産、発電、製作、および精製のような産業用プロセス、水処理および給水、排水収集および処理、石油およびガス・パイプライン、送電および配電、集合型風力発電所、大規模通信システムのようなインフラストラクチャ・プロセス、建物、空港、船舶、宇宙ステーションのための設備プロセス（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）、石油およびガス、精製、化学、薬品、食品および飲料水、水および排水、パルプおよび紙、外部電力(utility power)、鉱業、金属というような大規模(large campus)工業プロセス・プラント、並びに／または重要なインフラストラクチャである。

【００２５】

[0035] 実装態様では、Ｉ／Ｏモジュール１０２は、センサ１０６から受けたアナログ・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）電気回路等を使用して）構成することができる。また、Ｉ／Ｏモジュール１０２は、アクチュエータ１０８に接続することができ、速度やトルク等のような、アクチュエータ１０８の１つ以上の動作特性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１０２は、アクチュエータ１０８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１０２の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・トランスデューサ（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る通信モジュールを備えることができる。更に、２つ以上のＩ／Ｏモジュール１０２を使用して、通信サブバス用にフォールト・トレラントおよび冗長接続を設けることができる。

【００２６】

[0036] 各Ｉ／Ｏモジュール１０２には、Ｉ／Ｏモジュール１０２間で区別するための一意識別子（ＩＤ）を供給することができる。実装態様では、産業用制御システム１００に接続されるときに、Ｉ／Ｏモジュール１０２はその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１０２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１０２をセンサ１０６および／またはアクチュエータ１０８に接続することができる。各Ｉ／Ｏモジュール１０２は、印刷回路基板（ＰＣＢ）等のような、Ｉ／Ｏモジュール１０２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つ以上のポートを含むことができる。

【００２７】

[0037] Ｉ／Ｏモジュール１０２の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。必ずしもこれに限定されないが、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（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動作するワイヤレス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動作するワイヤレス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)やインターネット(the internet)等が含まれる。更に、Ｉ／Ｏモジュール１０２の１つ以上は、Ｉ／Ｏモジュール１０２をコンピュータ・バス等に接続するためのコネクションも含むことができる。

【００２８】

[0038] 制御モジュール１０４は、Ｉ／Ｏモジュール１０２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１００を共に接続するために使用することができる。開示する実施形態では、制御モジュール１０４は、Ｉ／Ｏモジュール１０２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１０２の一意ＩＤに基づいて、ルーティング・テーブルをアップデートすることができる。更に、多数の冗長Ｉ／Ｏモジュール１０２が使用されるときに、各制御モジュール１０４はＩ／Ｏモジュール１０２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１０２から受信される毎および／またはＩ／Ｏモジュール１００に送信される毎にそれらをアップデートすることができる。実施形態の中には、冗長性を設けるために、２つ以上の制御モジュール１０４が使用されることもある。セキュリティ向上のために、制御モジュール１０４は、スタートアップ、リセット、新規の制御モジュール１０４の設置、制御モジュール１０４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、相互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。更に、制御モジュール１０４はランダムな（例えば擬似乱数の）時間間隔で認証を実行するように構成することができる。

【００２９】

[0039] 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、データの不連続な(discrete)部分は、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・パケットに変換されることができる。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。実施形態の中には、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を実装するものもある。更に、冗長ＨＤＬＣを実装するために、２つ以上の制御モジュール１０４を使用することもできる。しかしながら、ＨＤＬＣは一例として挙げたに過ぎず、本開示を限定するのを意味するのではないことが留意されるべきである。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。

【００３０】

[0040] 制御モジュール１０４の１つ以上は、１つ以上の制御ループ・フィードバック機構／コントローラのように、Ｉ／Ｏモジュール１０２を介して産業用制御システム１００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(proportional)－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。開示する実施形態では、Ｉ／Ｏモジュール１０２および制御モジュール１０４は、例えばＩ／Ｏモジュール１０２を１つ以上のコントローラにネットワーク１１０を通じて接続するネットワーク・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１０２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することができる。更に、冗長ギガビット・イーサネットを実装するために、２つ以上の制御モジュール１０４を使用することもできる。

【００３１】

[0041] 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、本開示を限定するのを意味するのではないことが留意されるべきである。つまり、ネットワーク・インタフェースは、制御モジュール１０４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ができる。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動作される（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動作される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１１０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ができる。

【００３２】

[0042] これより図３を参照する。産業用制御システム１００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、局所発電（例えば、現場タービンまたはディーゼル局所発電機１１４）を使用して供給することもできる。電源１１６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の自動化機器に、電力グリッドからの電力を配給するために使用される。他の電源１１８が、局所発電機１１４から自動化機器に電力を配給するために使用される。また、産業用制御システム１００は、多数のバッテリ・モジュール１２２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１２０も含む。例えば、電源１２０はＵＰＳとして機能してもよい。開示する実施形態では、多数の電源１１６、１１８および／または１２０を産業用制御システム１００内に分散させる（例えば、物理的に散在させる）ことができる。

【００３３】

[0043] 実施形態の中には、１つ以上の電源１１６、１１８および／または１２０がキャビネットのレベルで設けられるものもある。例えば、１つの電源１２０は、制御モジュール１０４およびそれに付随するＩ／Ｏモジュール１０２にバックアップ電力を供給するように使用される。他の実施態様では、１つの電源１２０は、制御モジュール１０４にバックアップ電力を供給するように使用される。また、他の電源１２０は、付随するＩ／Ｏモジュール１０２にバックアップ電力を供給するように使用される（例えば、ここでは、Ｉ／Ｏモジュール１０２および制御モジュール１０４は、設備(facility)内で幾らかの距離だけ物理的に分離され、Ｉ／Ｏモジュール１０２および制御モジュール１０４等との間の電気的絶縁が維持される。）。

【００３４】
[0044] 電源１１６、１１８および／または１２０はまた、図２を参照して説明したように、センサ１０６および／またはアクチュエータ１０８のような現場デバイスに給電するように構成することができる。例えば、電力１１６および１１８の１つ以上は、（例えば、アクチュエータ１０８がＤＣモータまたは他のＤＣアクチュエータである実施態様では、）アクチュエータ１０８への伝送のために、ＡＣ（例えばＡＣ主電源によって供給される）をＤＣに変換するＡＣからＤＣへの（ＡＣ／ＤＣ）変換器を含む。更に、冗長構成を設けるために使用される２つ以上の電源１１６、１１８および／または１２０が、電源１２０毎に別個の（冗長構成の）電力バックプレーンを使用して、産業用制御システム１００の自動化機器に接続することができる。

【００３５】
[0045] 図４を参照する。電源１２０は、多数のバッテリ・モジュール１２２を含む。開示する実施形態では、各バッテリ・モジュール１２２は、リチウムイオン・バッテリ・セル１２４を含む。例えば、１つのバッテリ・モジュール１２２は、１．５ボルト（１．５Ｖ）のリチウム・イオン電池セル、および３ボルト（３Ｖ）のリチウム・イオン電池セル等を使用して実装される。実施形態の中には、電源１２０は、共にスタックされる８から１０個の間のバッテリ・モジュール１２２を含むものもある。しかしながら、８から１０個の間のバッテリ・モジュール１２２のスタックは、例示で設けられるに過ぎず、本開示を限定することを意図するのではない。他の実施形態では、８個未満または１０個より大きいバッテリ・モジュール１２２が共にスタックされる。

【００３６】
[0046] 電源１２０の他の実施形態について図１０に示す。電源１２０は、（それぞれ１つ以上のバッテリ・セルを含む）バッテリ・モジュール１２２のスタックを含むバッテリ・パックを含むことができる。実施形態の中には、各バッテリ・モジュール１２２は、バッテリ・モジュール保護レイヤ４０４（例えば、ガルバニック絶縁層）でケース収容される。そして、バッテリ・モジュール１２２は共にスタックされて、バッテリ・パックを形成する。スタックされたバッテリ・モジュール１２２（即ち、バッテリ・パック）はまた、バッテリ・パック保護層４０２（例えば、他のガルバニック絶縁層または遮蔽バリア）によってケース収容することもできる。電源１２０は、１つ以上のバッテリ・パックを含むことができ、更に、電源保護層４００（例えば、電源１２０を構成するバッテリ・モジュール（１または複数）の周囲でケース収容する産業用グレード（例えば、アルミニウム））を有することができる。実施形態の中には、電源保護層／ケース４００は、水不浸透性コネクタを有するマルチ・トーン・プレスで組み立てられるものもある。電源保護層／ケース４００は、１つ以上の方向（例えば、現場配備のために見込まれる複数の方向）に取り付け可能とすることができる。

【００３７】
[0047] なお、バッテリ・モジュール１２２は、リチウムイオン・バッテリ・セル１２４を含むものとして説明されるものの、本開示のシステムおよび技術は、必ずしもこれに限定されないが以下を含む、他の再充電可能バッテリ、ストレージ、および／または蓄電池技術を使用することができる点が留意されるべきである。即ち、鉛酸蓄電池、アルカリ電池、ニッケル・カドミウム電池、ニッケル水素電池、リチウムイオン・ポリマー電池、リチウム硫黄電池、薄膜リチウム電池、カリウム・イオンバッテリ、ナトリウム・イオン電池、ニッケル鉄電池、ニッケル水素電池、ニッケル亜鉛電池、リチウム空気電池、リン酸鉄リチウム電池、チタン酸リチウム電池、亜鉛臭素電池、バナジウム・レドックス電池、ナトリウム硫黄電池、溶融塩電池および酸化銀電池等である。

【００３８】
[0048] バッテリ・モジュール１２２の各々は、リアルタイム・バッテリ・モニタ１２６を含み、例えば、印刷回路基板（ＰＣＢ）を使用して実装することができる。開示する実施形態では、バッテリ・モニタ１２６は、バッテリ・セル１２４を動作させるコントローラ１２８（例えば、マイクロコントローラ）によって使用される。例えば、各バッテリ・

モニタ１２６は、コントローラ１２８に対し、バッテリ・セル毎の診断情報を供給する。診断情報は、必ずしもこれに限定されないが以下のものを含む。即ち、バッテリ・セル１２４の動作電圧、バッテリ・セル１２４の動作電流（例えば、アンペアで）、電荷のバッテリ・セル１２４へのユニット（例えば、クーロンで）、電荷のバッテリ・セル１２４からの電荷のユニット（例えば、クーロンで）、バッテリ・セル１２４の年数（例えば、時間のユニット、充電／放電のサイクル数等）等である。

【００３９】

[0049] 実施形態では、コントローラ１２８は、セルフ・ホスト・サーバとして構成され、および／または、電源１２０に対してセルフ・ホスト・サーバと通信可能に結合される。セルフ・ホスト・サーバは、例えば、ローカル・メモリ（例えば、内蔵型のハード・ディスク、ソリッド・ステート・ディスク・ドライブ、フラッシュ・メモリ等）にデータを維持するサーバを備えることができる。セルフ・ホスト・サーバは、電源が有する各バッテリ・モニタ１２６から、診断情報を受信および格納することができる。セルフ・ホスト・サーバは、診断情報へのネットワーク・アクセスを提供するように構成される。例えば、セルフ・ホスト・サーバは、診断情報をブロードキャストすることができ、または、サーバへのインターネット接続若しくはイントラネット接続を通じて、データベース、ファイル・ディレクトリまたはログへのアクセスを提供することができる。実施形態では、セルフ・ホスト・サーバは、ＩＥＥＥ６２５４１のＯＰＣ統合アーキテクチャの通信スタックに準拠する。セルフ・ホスト・サーバは、様々な電力変数および／または診断へのアクセスを提供することができ、産業用制御システム・アプリケーション、企業、および／または、電力供給ネットワークを監視するパーミッションを有する安全なネットワーク（例えば、クラウド）のコンピューティング・アプリケーションによって、制御され、監視され、傾向を示され(trended)、警告され、および／または履歴化される(historicized)ことができる。

【００４０】

[0050] 実施形態の中には、各バッテリ・モニタ１２６は、コントローラ１２８に個別に接続されるものもある。他の実施態様では、多数のバッテリ・モニタ１２６が、例えばシリアル・バスのように、コントローラ１２８に接続される共有通信チャネルに接続される。バッテリ・モニタ１２６はまた、（例えば、トランスを含む）電源レギュレータ１３０に接続される。電源レギュレータ１３０は、電源１１６および／または電源１１８のような外部電源から電力を受け取る。バッテリ・セル１２４は、電源レギュレータ１３０から供給される電気エネルギーを使用して充電される。電気エネルギーは、他の電源レギュレータ１３２を使用して、バッテリ・セル１２４から放電される。他の電源レギュレータ１３２は、バッテリ・セル１２４によって供給される電気エネルギーが有する１つ以上の出力特性（例えば、電圧）を調整するように使用することができる。実施形態では、電源レギュレータ１３０はインターリーブ力率改善（ＰＦＣ; Power Factor Correction）を実装することができ、その結果、ほぼ力率１(near-unity power factor)およびゼロ・スイッチ・トポロジを実現して、ＭＯＳＦＥＴ移行損失をゼロにして駆動させることができる。

【００４１】

[0051] 開示する実施形態では、各バッテリ・モジュール１２２は、支持フレームを、ホイルで包まれた(foil-wrapped)バッテリ・セル１２４と共に備える。ここでは、バッテリ・セル１２４はシールされたままとなるように多数の支持フレームがスタックでき、加えてホイル内でバッテリ・セル１２４の伸び縮みを許容する。開示する実施形態では、バッテリ・モニタを備えるＰＣＢはまた、支持フレームにおいてバッテリ・セル１２４と共にケース収容される。更に、ＰＣＢは、電池セル１２４によって給電され、また、各電池セル１２４への、および各電池セル１２４からの電流を制限するように構成される。例えば、バッテリ・モニタ１２６は、電子信号のスイッチング・デバイス（例えば、アナログ・スイッチの手法で直列に接続された２つの電界効果トランジスタ（ＦＥＴ））を含み、バッテリ・モニタ１２６から認証を行うことなく、エネルギーがバッテリに蓄電されるのを防止し、また、エネルギーがバッテリから返流されるのを防止する。このようにして、バ

ッテリ・セル１２４の端子が、意図しない（例えば短絡された）電気パスに接続されるときに、バッテリ・セル１２４への電気的接続が防止される。更に、バッテリ・モニタ１２６がアクティブではないとき（例えば、バッテリ・セル１２４が何ら充電されていないとき）に、バッテリ・セル１２４への電気的接続が防止される。この例では、バッテリ・モジュール１２２が電源１２０に挿入されるときに、バッテリ・モジュール１２２は少なくとも部分的に充電される。

【００４２】

[0052] 開示する実施形態では、バッテリ・モジュール１２２は、各支持フレームに配置される電気的コンタクト（例えば、電気コネクタ）を使用してスタックおよび接続される。電気コネクタは、（例えば、バッテリ・モニタＰＣＢを介して）バッテリ・セル１２４に電気的に接続され、（さもなければバッテリ・セル１２４への半田付け接続を要することになる）支持フレームから延伸するワイヤがなくても支持フレームに配置することができる。例えば、スナップ・フィット電気コネクタが１つの支持フレーム上に設けられ（例えば、支持フレームの上面に配置され）、他の支持フレーム上の対応する（例えば、他の支持フレームの底面に配置される）スナップ・フィット電気コネクタと組になる。電気コネクタ間のコンタクトの表面領域を増加させるように、および／または（例えば、１つの電気コネクタの一部を他の電気コネクタに挿入するために構成することによる）電気コネクタの自己整合(self-alignment)を提供するように、電気コネクタを構成することができる。

【００４３】

[0053] 開示する実施形態では、多数のバッテリ・モジュール１２２が意図しない手法で共に接続されるのを防止するために、電気コネクタが幾何学的に配置される（例えば、適切な位置を定められ、サイズ設定される等）。例えば、１つの電気的コンタクトは、支持フレームに対して全般的に上方へ指向することができる一方で、他の電気的コンタクトは支持フレームに対して全般的に下方に指向することができる。他の実施態様では、２つのバッテリ・モジュール１２２を整列させるために視覚的なキュー（例えば、カラー・コーディングや色分け等）が設けられる。

【００４４】

[0054] 更に、バッテリ・モジュール１２２に機械的組み合わせ(mechanical registration)を設けるために（例えば、１つのバッテリ・モジュール１２２の電気コネクタを、他のバッテリ・モジュール１２２の電気コネクタと組にして整列させ、および／または電源１２０への電気コネクタと共に整列させるために）、電源１２０は、スロット、チャネルおよびトラック等を含むことができる。例えば、電源１２０のハウジングの各トラックへの挿入のために、およびハウジングに対してバッテリ・モジュール１２２の整列を設けるために、バッテリ・モジュール１２２はタブまたはポストを含む。更に、コントローラ１２８は、一意の物理識別情報（ＩＤ）を各バッテリ・モジュール１２２と関連付けることができ、その結果、電源１２０のハウジングに対して特定の順序および／または特定の位置で結合された各バッテリ・モジュール１２０を一意に特定することができる。

【００４５】

[0055] 開示する実施形態では、電源１２０は、キャビネット取付け、ラック取付け、壁取付け等の用途で組み立てられる。電源１２０のハウジングは、剛性の絶縁材料（例えばアクリロニトリル・ブタジエン・スチレン（ＡＢＳ）または他のプラスチック材料）、または、さもなければバッテリ・セルに故障が生じた場合にリリースされることになるエネルギーを含めるのに使用することができる他のプラスチック材料で作ることができる。更に、ハウジングは、例えばリチウムのような、バッテリ故障に因りリリースされることがある化学バッテリ・セル・コンポーネントを含める、または少なくとも実質的にこれを含めるように構成することができる。加えて、電源１２０に含まれるコンポーネントは相互に電気的に絶縁することができる。例えば、コントローラ１２８への信号は、バッテリ・モニタ１２６およびバッテリ・セル１２４から直流的に(galvanically)絶縁される。更に、コントローラ１２８および電源レギュレータ１３０は、（例えば、別個のトランスや光

アイソレータ等を使用して）バッテリ・モジュール１２２および電源レギュレータ１３２から電気的に分離および／または故障分離される。

【００４６】

[0056] これより図５を参照する。コントローラ１２８は（例えば、ネットワーク１１０を介して）産業用制御システム１００に接続される。開示する実施形態では、コントローラ１２８は、コントローラ・レベルで、および／または各バッテリ・モジュール１２２のレベルで、セキュリティおよび診断を実施する。コントローラ１２８は、そのコンポーネントの一部または全部を含み、コンピュータ制御下で動作することができる。例えば、プロセッサ１４０はコントローラ１２８と共にまたはコントローラ１２８の中に含めることができ、その結果、ソフトウェア、ファームウェア、ハードウェア（例えば、固定ロジック電気回路）、手動処理、またはそれらの組み合わせを使用して、本明細書に説明されるコントローラ１２８のコンポーネントおよび機能を制御することができる。本明細書で用いる「コントローラ」、「機能」、「サービス」および「ロジック」という用語は、全般的に、コントローラ１２８を制御することに関連し、ソフトウェア、ファームウェア、ハードウェア、または、ソフトウェア、ファームウェア若しくはハードウェアの組み合わせを表すものである。ソフトウェアによる実装の場合、モジュール、機能またはロジックは、プロセッサ（例えば、１または複数の中央処理装置（ＣＰＵ））で実施されると特定のタスクを実行するプログラム・コードを表す。プログラム・コードは、１つ以上のコンピュータ可読メモリ・デバイス（例えば、内部メモリおよび／または１つ以上の有形媒体）等に格納することができる。本明細書に説明される構造、機能、手法および技術は、様々なプロセッサを有する様々な商用コンピューティング・プラットフォーム上で実装することができる。

【００４７】

[0057] プロセッサ１４０は、処理機能をコントローラ１２８に提供する。プロセッサ１４０は、如何なる数のプロセッサ、マイクロコントローラ、または他の処理システムも含むことができる。また、コントローラ１２８によってアクセスされ若しくは生成されるデータおよび他の情報を格納する常駐(resident)メモリまたは外部メモリを含むことができる。プロセッサ１４０は、本明細書に説明される技術を実装する１つ以上のソフトウェア・プログラムを実行することができる。プロセッサ１４０は、プロセッサが形成される材料または、そこに採用される処理機構によって限定されることはなく、つまり、半導体（１または複数）および／またはトランジスタ等を通じて（例えば、電子集積回路（ＩＣ）コンポーネントを使用して）実装することができる。

【００４８】

[0058] コントローラ１２８はまた、メモリ１４２を含む。メモリ１４２は、有形コンピュータ可読ストレージ媒体の例示であり、コントローラ１２８の動作に関連付けられる様々なデータ（例えばソフトウェア・プログラムおよび／若しくはコード部分、またはプロセッサ１４０およびおそらくはコントローラ１２８の他のコンポーネントに指示する他のデータ）を格納するストレージ機能を提供して、本明細書に説明される機能を実行する。つまり、メモリ１４２は、データ（例えば、電源１２０（そのコンポーネントを含む）を動作させるための命令を有するプログラム等）を格納することができる。開示する実施形態では、メモリ１４２は、電源１２０のための一意識別子１３６および／またはセキュリティ証明書１３８を格納することができる。なお、単一のメモリ１４２について記載する一方で、様々なタイプおよび組み合わせのメモリ（例えば、有形非一時的メモリ）を採用できることが留意されるべきである。メモリ１４２は、プロセッサ１４０と一体であっても、また、スタンドアロンのメモリを備えても、または、両方の組み合わせともすることができる。メモリ１４２は、これらに限定されないが、例えば、ランダム・アクセス・メモリ（ＲＡＭ）、リード・オンリ・メモリ（ＲＯＭ）、フラッシュ・メモリ（例えば、セキュア・デジタル（ＳＤ）メモリ・カード、ミニＳＤカード、および／またはマイクロＳＤカード）、磁気メモリ、光メモリ、ユニバーサル・シリアル・バス（ＵＳＢ）メモリ・デバイス、ハード・ディスク・メモリ、外部メモリ等のような、着脱可能および着脱不可

能メモリ・コンポーネントを含むことができる。実施態様では、電源１２０および／またはメモリ１４２は、着脱可能な集積回路カード（ＩＣＣ）メモリ（例えば、加入者識別モジュール（ＳＩＭ）カード、汎用加入者識別モジュール（ＵＳＩＭ）カード、汎用集積回路カード（ＵＩＣＣ）等により提供されるメモリ）を含むことができる。

【００４９】

[0059] コントローラ１２８は、通信インタフェース１５０を含む。通信インタフェース１５０は、電源１２０のコンポーネントと通信するように動作可能に構成される。例えば、通信インタフェース１５０は、コントローラ１２８におけるストレージのためにデータを送信し、コントローラ１２８におけるストレージからデータを抽出等をするように構成することができる。通信インタフェース１２０はまた、プロセッサ１４０とも通信可能に結合される。その結果、例えば、コントローラ１２８と通信可能に結合されたデバイスから受信される入力をプロセッサ１４０に伝達し、および／または、バッテリ・モジュール１２６のようにコントローラ１２８と通信可能に結合されたデバイスに出力を伝達するように、電源１２０のコンポーネントとプロセッサ１４０の間のデータ移送を促進することができる。例えば、通信インタフェース１５０は、プロセッサを多数のバッテリ・モニタ１２６に接続する共有通信チャネル（例えば、シリアル・バス）を使用して実装される。

【００５０】

[0060] 開示する実施形態では、コントローラ１２８は、バッテリ・モニタ１２６と双方向通信を行うように構成される。例えば、コントローラ１２８は、バッテリ・モニタ１２６から診断情報（例えば、バッテリ・セル１２４に関するステータス情報および／または信頼性情報）を収集する。コントローラ１２８はまた、バッテリ・モジュール１２２を動作させる。例えば、電源１１６や電源１１８等から供給される電気エネルギーを蓄積および返流させるようにバッテリ・モジュール１２２に命令する。なお、通信インタフェース１５０はコントローラ１２８のコンポーネントとして説明される一方で、通信インタフェース１５０の１つ以上のコンポーネントを、有線接続および／または無線接続を介してコントローラ１２８に通信可能に結合される外部コンポーネントとして実装できることが留意されるべきである。コントローラ１２８はまた、（例えば通信インタフェース１５０を介して）１つ以上の入力／出力（Ｉ／Ｏ）デバイスを備え、および／または接続することができる。１つ以上の入力／出力（Ｉ／Ｏ）デバイスは、これに限定されないが、ディスプレイやマウス等を含む。例えば、コントローラ１２８は、ディスプレイ・デバイス（例えば、マルチ・カラー（例えば、三色）の発光ダイオード（ＬＥＤ）（例えば、インジケータ・ライト１４４））に接続することができ、電源１２０のステータスを示すことができる。

【００５１】

[0061] 通信インタフェース１５０および／またはプロセッサ１４０は様々な異なるネットワーク１１０と通信するように構成することができる。様々な異なるネットワークは、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）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、ＷｉＦｉネットワーク（例えば、ＩＥＥＥ８０２．１１ネットワーク規格を使用して動作されるワイヤレス・ローカル・エリア・ネットワーク（ＷＬＡＮ））のようなワイヤレス・コンピュータ通信ネットワーク、インターネット(an internet)、インターネット(the internet)、ワード・エリア・ネットワーク（ＷＡＮ）、ローカル・エリア・ネットワーク（ＬＡＮ）、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動作するワイヤレスＰＡＮ（ＷＰＡＮ））、公衆電話網、エクストラネット、イントラネット等を含む。しかしながら、このリストは、例示のみで提供され、本開示を限定するのを意図するものではない。加えて、通信インタフェース１５０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、通信インタフェース１５０は、ＰＣＩカード・インタフェース（例えば、ミニＰＣＩインタフェース等）を含むことができる。更に、通信インタフェース１５０は、単一のネットワーク１１０および異なるアクセス・ポイントにわたる多数のネットワークと通信する

ように構成することができる。このようにして、コントローラ１２８は、電源１２０を産業用制御システム１００に通信可能に結合するのに使用される。

【００５２】

[0062] これより図６を参照する。制御エレメントまたはサブシステム（例えば、Ｉ／Ｏモジュール１０２、制御モジュール１０４、電源１２０等）は１つ以上のバックプレーンによって共に接続される。例えば、制御モジュール１０４は、通信バックプレーン１５２によってＩ／Ｏモジュール１０２に接続することができる。更に、電源１１６、１１８および／または１２０は、電力バックプレーン１５４によって、Ｉ／Ｏモジュール１０４に、および／または制御モジュール１０６に接続することができる。実装態様の中には、各制御モジュール１０４またはＩ／Ｏモジュール１０２は、バックプレーン１５４上に少なくとも１つの独立トレースを有することができ、他の制御モジュール１０４および／またはＩ／Ｏモジュール１０２を結合する他のチャネル（即ち、トレース）からのガルバニック絶縁および独立制御を有する電力チャネルを規定する。開示する実施形態では、物理相互接続デバイス（例えば、スイッチ、コネクタまたはケーブルであり、これに限定するのではないが、米国特許出願番号第１４／４４６,４１２に記載されているもの）は、I／Ｏモジュール１０２、制御モジュール１０４、電源１２０、およびおそらくは他の産業用制御システム機器に接続するのに使用される。例えば、ケーブルは制御モジュール１０４をネットワーク１１０に接続するために使用され、他のケーブルは電源１２０を電力グリッド１１２に接続するために使用され、他のケーブルは電源１２０をローカル発電機１１４に接続するために使用される等である。

【００５３】

[0063] 電力配給アーキテクチャの他の実施形態が図１１に示される。電力配給ネットワーク５００は電源５０２（例えば、現場取り付け型(field-mounted)ＵＰＳ）を含むことができ、制御モジュール５０６、入力／出力モジュール５０６、５０８、５１０、５１２等に電力を供給するためのバックプレーン１５４に取り付けられた１つ以上の電力モジュール５０４に結合される。図１２に示すように、電力配給ネットワークは、追加の（補足的な）安全な電源５１４を含んでもよい。安全な電源５１４は、電源５０２が受電するのとは異なるデバイスに補足的な電力を供給するために、または電力を供給するために、電源５０２（例えば安全なＵＰＳ）に電気的に接続することができる。実施形態では、電源５０２および安全な電源５１４は、ネットワーク要件に基づいて相互に双方向に電力を送り、および／または電源の間で閾値充電レベルを維持するように構成することができる。

【００５４】

[0064] 図６を再度参照する。産業用制御システム１００は、安全な制御システムを実装することができる。例えば、産業用制御システム１００は、セキュリティ証明書供給元（例えば、工場１５６）およびセキュリティ証明書実装元（例えば、鍵管理エンティティ１５８）を含む。工場１５６は、一意のセキュリティ証明書（例えば、鍵、証明書など（例えば一意識別子１３６および／またはセキュリティ証明書１３８））を生成するように構成される。鍵管理エンティティ１５８は、Ｉ／Ｏモジュール１０２、制御モジュール１０４、電源１１６、電源１１８、および／または電源１２０に対して、工場１５６が生成した一意セキュリティ証明書を供給するように構成される。例えば、Ｉ／Ｏモジュール１０２および関連付けられる電源１２０は、それぞれが一意のセキュリティ証明書の供給を受けることができる。

【００５５】

[0065] 次いで、産業用制御システム１００で実装される制御エレメントまたはサブシステムを認証するための認証プロセスが、一意のセキュリティ証明書に基づいて実行される。例えば、実施形態では、制御モジュール１０４および電源１２０は、（例えば、認証プロセスに基づいて）一意のセキュリティ証明書に基づき相互に双方向に通信するように動作可能である。更に、本明細書に説明される安全な産業用制御システム１００では、産業用制御システム１００が有する多数の（例えば全ての）制御エレメントおよびサブシステム（例えば、Ｉ／Ｏモジュール、電力供給源、物理相互接続デバイス等）は、産業用制御

システム１００の多数の（例えば全ての）レベルでセキュリティを提供するセキュリティ証明書が供給される。更にまた、エレメントは、製造の間（生産された時(at birth)）に、一意のセキュリティ証明（例えば、鍵や証明書等）の供給を受けることができ、また、生産されてからは、産業用制御システム１００のセキュリティを強化するために産業用制御システム１００の鍵管理エンティティによって管理することができる。

【００５６】

[0066] 実施形態の中には、制御エレメントまたはサブシステムは、物理相互接続デバイス（例えば、１ワイヤ暗号化チップ）に接続されるか、またはこれに含まれるコントローラを使用して接続されるものもある。コントローラは、コンポーネントと、コンポーネントに接続された物理相互接続デバイス（例えば、ケーブル・アセンブリ）との間の認証を実施することを許容する。例えば、マイクロプロセッサのセキュア暗号化技術はケーブル・アセンブリに組み込むことができ、産業用制御システム１００の特定コンポーネントに対し鍵を掛けることができる。当該構成は、ユーザがケーブル・アセンブリを、該ケーブル・アセンブリと接続されるようには構成されないコンポーネントに設置するときに、セキュリティを産業用制御システム１００に提供する。実施形態では、１ワイヤのシリアル・キー（例えば、１ワイヤ組込鍵）は、１つ以上の（例えば、各々の）物理相互接続デバイスに実装される。

【００５７】

[0067] 開示する実施形態では、産業用制御システム１００が有するエレメントおよび／または物理相互接続デバイス（例えば、ケーブル・アセンブリ）間の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に実装されたエレメントおよび／または物理相互接続デバイスを認証するために実行することができる。実装態様では、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。実施形態では、産業用制御システム１００のコンポーネントおよび／または物理相互接続デバイスに含まれ、および／またはそれに接続されるコントローラ（例えば、安全なマイクロコントローラ）は、認証プロセスを実行するように構成することができる。

【００５８】

[0068] 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またはサブシステム（例えば、エレメントおよび／または物理相互接続デバイス）は、それら自体の一意のセキュリティ証明の供給を受ける。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提供を受けるのでもよい（例えば、エレメントが生産される時に、個々の１組の鍵および証明書が定められる）。複数組の証明書、暗号化鍵、および／または識別番号は、強力な暗号を提供／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。

【００５９】

[0069] 実施形態の中には、暗号鍵および証明書はオン・チップ・メモリ（ＯＣＭ）、例えば認証モジュールのＳＲＡＭに格納することができるものもある。また、機密を扱う(sensitive)タスク（例えば、秘密情報を有し、時には好適な女医右方でさえも有するタスク）は、ＯＣＭで実施するスタックを有することができる。例えば、暗号タスクは、カーネル・スペースまたはアプリケーション・スペースで、ＯＣＭにローカルに格納されたスタックから実行することができる。

【００６０】

[0070] 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アクティブ化すること

ができ、産業用制御システム１００内においてこの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することができ、産業用制御システム１００内においてこのエレメントの完全な機能をイネーブルすることができ、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、産業用制御システム１００の当該エレメントと他のエレメントとの間で通信が促進されない）。

【００６１】

[0071] 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」という用語は、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）。

【００６２】

[0072] 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１２０）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、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、産業用制御システム１００の当該エレメントと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、この特徴は、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、そのエレメントを産業用制御システム１００内に実装するのを防止することができる。このようにして、本明細書に説明される技術は、安全な産業用制御システム１００内に、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販売代理人は、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の提供を受けることができ、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販売代理人は、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の提供を受けることができる。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１００内では動作することが妨げられることがあり得る。何故ならば、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にも留意されるべきである。更に、実施形態の中には、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。

【００６３】

[0073] 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１００の他のエレメントのＯＥＭと同一の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１００によって実装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に対するセキュリティの向上を強化することもできる。何故ならば、模造エレメントが、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はないネットワークから物理的に分離されるのを確証する。

【００６４】

[0074] 鍵管理エンティティ１５８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１５８は、セキュリティ証明ソースとしてサービス提供するように構成され、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。

【００６５】

[0075] 実施形態では、鍵管理エンティティ１５８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備える。鍵管理エンティティは、Ｉ／Ｏモジュール１０２、通信／制御モジュール１０４、およびネットワーク１１０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１６０が鍵管理エンティティ１５８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１１０（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１６０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、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１６０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１１０）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１６２（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１６０は、鍵管理エンティティ１５８、および制御エレメントまたはサブシステムの１つ以上、並びに／またはネットワーク１１０間で選択的な（例えば、安全な）通信を許容する。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１００内の種々の位置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１１０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。

【００６６】

[0076] 上述したように、安全産業用制御システム１００は更に、１つ以上の製造エンティティ（例えば、工場１５６）を含むことができる。製造エンティティ１５６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１５８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つ以上の工場１５６において製造されているとき、鍵管理エンティティ１５８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１５８は、製造の時点においてエレメントにセキュリティ証明を供給する（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。

【００６７】

[0077] 更に、エレメントが使用に移される（例えば、アクティブ化される）とき、鍵管理エンティティ１５８は、各個々のエレメントにワールドワイドに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および署名し、任意の特定のコードの使用を無効にし（例えば、除去する）、並びに／または任意の特定のコードの使用をイネーブルすることができる。つまり、鍵管理エンティティ１５８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／若しくは識別番号を含むマスタ・データベース並びに／またはテーブルを、鍵管理エンティティ１５８によって維持することができる。鍵管理エンティティ１５８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。

【００６８】

[0078] 実装態様では、鍵管理エンティティ１５８は、制御エレメント／サブシステム、および／またはネットワーク１１０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）並びに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１５８は集中システムまたは分散型システムとしてもよい。更に、実施形態では、鍵管理エンティティ１５８をローカルでまたはリモートで管理することができる。実装態様の中には、鍵管理エンティティ１５８をネットワーク１１０および／または制御エレメント若しくはサブシステム内に配置する（例えば、統合する）ことができる。鍵管理エンティティ１５８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可能である。例えば、鍵管理エンティティ１５８は、中央位置においてカスタマによって、個々の工場位置におけるカスタマによって、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カスタマによって、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。

【００６９】

[0079] 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、電源１２０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装され、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１００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１００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）を提供する。

【００７０】

[0080] 実装態様では、認証プロセスは、異なる製造元／販売元／供給元（例えば、ＯＥＭ）によって製造および／または供給されたエレメントの安全な産業用制御システム１００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(enable)ように実装するこ

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（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）が階層構造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ことを許容する。

【００７１】

[0081] 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、制御モジュール１０４および電源１２０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。

【００７２】

[0082] 開示する実施形態では、認証シーケンスを開始するために、第１認証モジュール（例えば、電源１２０、電源１２０のコントローラ１２８、電源１２０のバッテリ・モジュール１２２、Ｉ／Ｏデバイス１０２のような制御エレメントまたはサブシステム、制御モジュール１０４等に含まれる）は、要求データグラムを第２認証モジュール（例えば、電源１２０、電源１２０のコントローラ１２８、電源１２０のバッテリ・モジュール１２２、Ｉ／Ｏデバイス１０２のような制御エレメントまたはサブシステム、制御モジュール１０４等に含まれる）に送信するように構成される。実装態様では、要求データグラムは、第１平文ノンス（ＮｏｎｃｅＡ）、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）、および第１識別情報属性証明書（ＩＡＣＡ）を含む。実施形態の中は、第１認証モジュールは、真正乱数生成器（以後、「ＴＲＮＧ」という。）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、言い換えると組み合わせて、要求データグラムを生成するように構成されるものもある。実施形態の中には、第１デバイス認証鍵証明書（ＣｅｒｔＤＡＫＡ）および第１識別情報属性証明書（ＩＡＣＡ）は、第１認証モジュールによってローカルに格納される。例えば、これらの証明書が第１認証モジュールのローカル・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ストレージ媒体）に格納されてもよいものもある。

【００７３】

[0083] 第２認証モジュールは、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・ライフ委来る管理システム（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、認証モジュールのＳＲＡＭまたは他のローカル・メモリに格納され、認証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に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。実施形態の中には、第２認証モジュールは、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）または他の検証動作によって証明書を検証できるものもある。実施形態の中には、第２認証モジュールが、更に、次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できるものもある。即ち、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」という。）または識別情報属性証明書（以後「ＩＡＣ」という。）であること、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「ＭＰＳＮ」という。）が互いに一致することである。実施形態の中には、第２認証モジュールは更に、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）にはないことを検証するように構成できるものもある。第２認証モジュールが要求データグラムの有効性を判断できなかったとき、第２認証モジュールはエラー・メッセージを生成し、部分的にまたは完全に第１認証モジュールをディセーブルし、および／または第１認証モジュールへ／からの通信を切断または制限することができる。

【００７４】

[0084] 有効な要求データグラムに応答して、第２認証モジュールは、応答データグラムを第１認証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。実施形態の中には、第２認証モジュールは、ＴＲＮＧを用いて第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２認証モジュールによってローカルに格納されている秘密鍵（例えば、ＤＡＫ）を用いて署名するように構成されるものもある。第２認証モジュールは更に、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）、並びに第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、応答データグラムを生成するように構成される。実施形態の中には、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２認証モジュールによってローカルに格納されるものもある。例えば、証明書は、第２認証モジュールのローカル・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ストレージ媒体）に格納されてもよい。

【００７５】

[0085] 第１認証モジュールは、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抽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。実施形態の中には、第１認証モジュールは更に、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るものもある。即ち、ＩＡＣおよびＤＡＫ証明書が一致するＭＰＳＮを有すること、ＩＡＣ名称が一致すること、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こと、正しいソース名称が両方の証明書上にあること、ＤＡＫモジュール・タイプが正しいタイプである（例えば、通信／制御モジュール）。実施形態の中には、第１認証モジュールは更に、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ものもある。

【００７６】

[0086] 応答データグラムの有効性を判断するために、第１認証モジュールは更に、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る。実施形態の中には、第１認証モジュールは、第１のローカルに格納されたノンス（ＮｏｎｃｅＡ）と、第２認証モジュールから受けた第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ものもある。第

１認証モジュールが応答データグラムの有効性を判断できなかったとき、第１認証モジュールは、エラー・メッセージを生成し、部分的若しくは完全に第２認証モジュールをディセーブルにし、および／または第２認証モジュールへ／からの通信を切断または制限することができる。

【００７７】

[0087] 更に、第１認証モジュールは、応答データグラムが有効であるとき、認証データグラムを第２認証モジュール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。実施形態の中には、第１認証モジュールは、ローカルに生成された第１および第２ノンスの連結に、第１認証モジュール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、認証データグラムを、第２ノンスに関連付けられた署名と、第１認証モジュール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」認証データグラムと置き換えることができる。

【００７８】

[0088] 認証データグラムに応答して、第２認証モジュールは更に、応答認証データグラムを第１認証モジュール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は、第１ノンスに関連付けられた署名と、第２認証モジュール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。実施形態の中には、第２認証モジュールは、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、認証データグラムの有効性を確認するように構成されるものもある。実施形態の中には、第２認証モジュールは、第１認証モジュールから受けた第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ものもある。エラー報告メッセージに加えて、第２認証モジュールが認証データグラムの有効性を判断できなかったとき、第２認証モジュールは、部分的若しくは完全に第１認証モジュールをディセーブルにし、および／または第１認証モジュールへ／からの通信を切断または制限することができる。

【００７９】

[0089] 認証モジュールが「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１認証モジュール）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、マスタなしで並列に動作する２つ以上のスレーブ・モジュールが、互いに認証するのでもよい。ここでは認証失敗の結果、両方のデバイスを部分的にまたは完全にディセーブルにするのでもよい。例えば、２つ以上の冗長構成の電源１２０が、スタートアップ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、これらをディセーブルにすることができる。

【００８０】

[0090] これより図７および図８を参照する。各電源１２０または他の任意の産業用エレメント／コントローラ２０６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２０２は、オペレータ・インタフェース２０８（例えば、ＳＣＡＤＡまたはＨＭＩ）、エディタ２１２およびコンパイラ２１４を含む設計インタフェース２１０、ローカル・アプリケーション２２０、リモート・アプリケーション２１６（例えば、ネ

ットワーク２１８を通じてローカル・アプリケーション２２０を介して通信する）等を含む。図７および図８に示す認証パス２００では、産業用エレメント／コントローラ２０６（例えば、電源１２０）は、アクション要求がアクション認証器２０４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／ソフトウェアのアップデート、セット・ポイント制御、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）プロファイルから入来す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。

【００８１】

[0091] 開示する実施形態では、アクション認証器２０４は、アクション発起元２０２と同じ場所(on-site)（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」）２２２または安全なワークステーション２２６）にあること、またはリモートに位置すること（例えば、ネットワーク２１８を通じて接続されたＤＬＭ２２２）ができる。一般に、アクション認証器２０４は、秘密鍵が格納されたストレージ媒体と、秘密鍵を使用してアクション発起元２０２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・ログインを介してはアクセスできないメモリに格納される。例えば、安全なワークステーション２２６は、アクセスのために、物理鍵、携帯型暗号化デバイス（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。

【００８２】

[0092] 実施形態の中には、アクション認証器２０４は、スマート・カード２２４（安全なマイクロプロセッサを含むことができる）のような携帯型暗号化デバイスを含むものもある。このようにして、デバイス全体（プライベートに格納された鍵、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２０２のインタフェースに対して認可されたアクセスを有するオペレータまたはユーザが一緒に携行することができる。アクション認証ノード２０４が認証パス２００に、安全なワークステーションまたは安全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２０２からのアクション要求は、（例えば、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とは対照的に）携帯型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。例えば、許可されていない人は、スマート・カード２２４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２０２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。

【００８３】

[0093] 実施形態の中には、多数のレイヤのセキュリティを採用できるものもある。例えば、アクション認証器２０４は、安全なワークステーション２２６を含むことができる。ワークステーション２２６は、スマート・カード・アクセス２２４のアクセス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、安全なワークステーション２２６は、生体または多要素暗号デバイス２２８（例えば、指紋スキャナ、虹彩スキャナ、および顔認識デバイス等の内１つ以上）によってアクセス可能にすることもできる。実施形態の中には、多要素暗号デバイス２２８は、スマート・カード２２４または他の携帯型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、有効な生体入力を要求することができる。

【００８４】

[0094] 電源１２０、またはアクション発起元２０２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２０６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。実施形態の中には、産業用エレメント／コントローラ２０６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ストレージ媒体（例えば、ＳＤ／マイクロＳＤカード、ＨＤ

Ｄ、ＳＳＤ、または任意の他の非一時的ストレージ・デバイス）を含むものもある。産業用エレメント／コントローラ２０６は更に、署名が検証された後にアクション要求を実行する／実施する（即ち、要求されたアクションを実行する）プロセッサ（例えば、電源１２０のプロセッサ１４０）を含む。実施形態の中には、アクション要求はアクション発起元２０２および／またはアクション認証器２０４によって暗号化され、また、プロセッサ１４０によって復号化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ものもある。実装態様では、産業用エレメント／コントローラ２０６は、仮想鍵スイッチ２３４（例えば、プロセッサ１４０上で起動するソフトウェア・モジュール）を含む。仮想鍵スイッチ２３４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復号化された後でのみ、プロセッサ１４０により、要求されたアクションを実行することを可能にする。実施形態の中には、重要な(critical)アクションの選択の各々または全ては、産業用エレメント／コントローラ２０６において起動される前に、認証パスを通過(clear)しなければならない。

【００８５】

[0095] 図９は、例示の実施形態により、産業用制御システムでアクション要求を認証するためのプロセス３００を示す。実装態様では、プロセス３００は、（例えば、図１から図６を参照して説明した）産業用制御システム１００、および／または（例えば、図７および図８を参照して説明した）産業用制御システム１００における認容パスによって明示することができる。アクション要求が発生される（ブロック３１０）。例えば、アクション要求を生成するのに、オペレータ／設計インタフェース２０８／２１０、および／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２１６／２２０）が使用される。次いで、アクション認証器によってアクション要求が署名される（ブロック３２０）。例えば、アクション要求に署名するのにアクション認証器２０４が使用される。実施形態の中には、アクション認証器によってアクション要求を暗号化できるものもある（ブロック３２２）。次いで、署名されたアクション要求が産業用エレメント／コントローラに送られる（ブロック３３０）。例えば、アクション要求は参照用エレメント／コントローラ２０６に（例えば、電源１２に）供給される。次に、署名付きアクション要求の真正性が検証される（ブロック３４０）。実施形態の中には、産業用エレメント／コントローラによってアクション要求を復号化できるものもある（ブロック３４２）。例えば、産業用エレメント／コントローラ２０６がアクション要求を復号化することができる。次いで、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ことができる（ブロック３５０）。例えば、電源１２０は、オペレータ／設計インタフェース２０８，２１０および／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２１６，２２０によって要求されたアクションを実行する。

【００８６】

[0096] セキュリティ強化のために、産業用エレメント／コントローラ２０６（例えば電源１２０）は更に、要求されたアクションが産業用エレメント／コントローラ２０６によって実行される前に、アクション認証器２０４によって（例えば、スマート・カード２２４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、ブロック３５０の前、またはブロック３３０の前でさえも実行することができる。実施形態の中には、署名および検証ブロック３２０および３４０を、一層複雑な認証シーケンスを使用して実行できるものもある。加えて、実施形態の中には、認証シーケンスは、もっと簡単な署名検証および／または復号化手段(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。

【００８７】

[0097] 実施形態の中には、産業用エレメント／コントローラ２０６によって実装される認証シーケンスは、要求データグラムをアクション認証器２０４に送ることを含むものもある。ここでは、要求データグラムは、第１暗号ノンス、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）、および第１識別情報属性証明書を含む。次いで、アクション認証器２０４から応答データグラムを受ける。例えば、ここでは、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（例えば、デバイス認証鍵を含む第２認証証明書）、並びに第２識別情報属性証明書を含む。次に、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、並びに第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ことができる。次に、（例えば、応答データグラムが有効であると判断されたときに）認証データグラムはアクション認証器２０４に送ることができる。ここでは、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。

【００８８】

[0098] あるいは、アクション認証器２０４は、ハンドシェークを開始することができ、その場合、産業用エレメント／コントローラ２０６によって実装される認証シーケンスは、アクション認証器２０４から要求データグラムを受けることができる。例えば、ここでは、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。次いで、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ことができる。次いで、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に送ることができる。例えば、ここでは、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、第２識別情報属性証明書を含む。次に、アクション認証器２０４から認証データグラムを受けることができる。例えば、ここでは、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。次いで、例えば第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ことができる。

【００８９】

[0099] 産業用エレメント／コントローラ２０６およびアクション認証器２０４によって実装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は、（例えば、認証モジュールによって実行される認証を参照して）上述した技術の１つ以上を使用することによって遂行することができる。アクション発起元２０２、アクション認証器２０４、および産業用エレメント／コントローラ２０６の各々は、本明細書に説明される機能または動作（例えば、方法３００のステップ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２０２、アクション認証器２０４、および産業用エレメント／コントローラ２０６の各々は、これに限定されないが、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、磁気ストレージ・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。

【００９０】

[00100] 全般的に、本明細書に説明される機能はそのいずれもが、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装することができる。つまり、以上の開示において検討したブロックは、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ものである。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。

【００９１】

結び

[00101] 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】

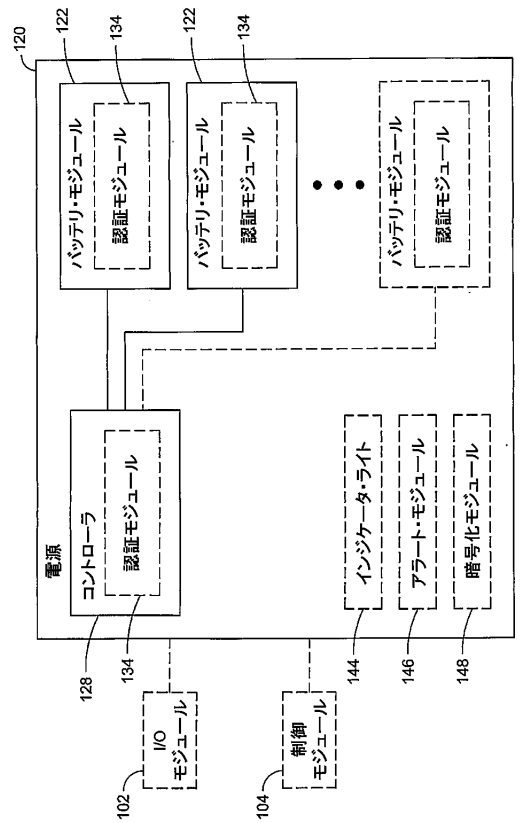

FIG. 1

【図２】

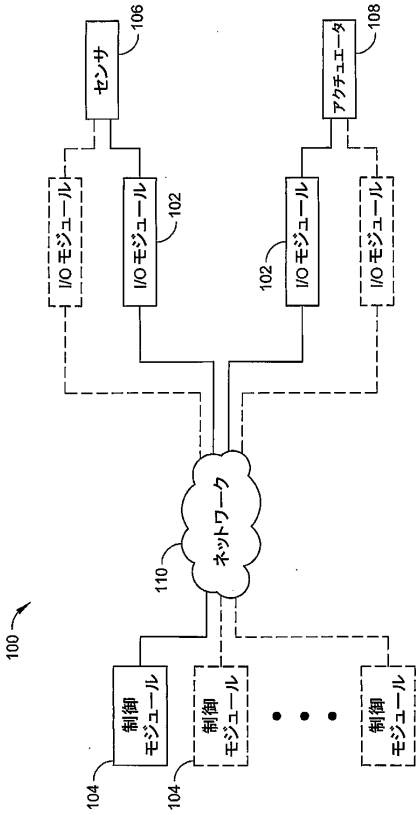

FIG. 2

【図３】

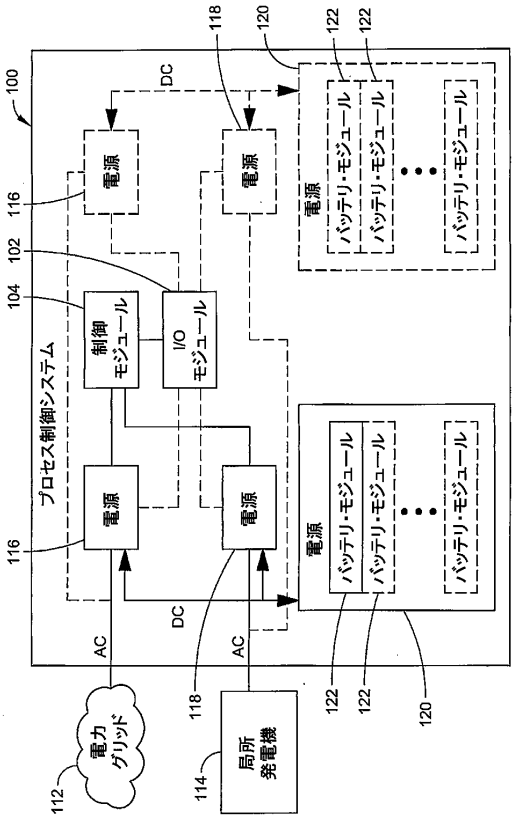

FIG. 3

【図４】

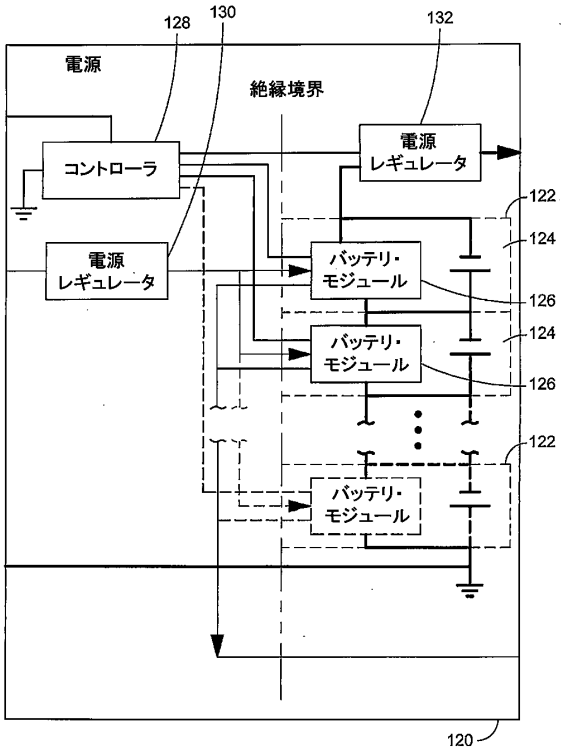

FIG. 4

【図５】

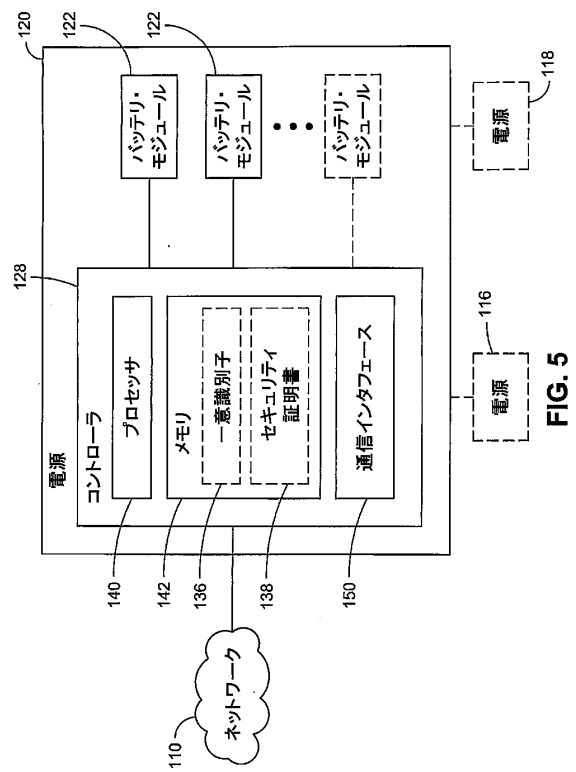

FIG. 5

【図６】

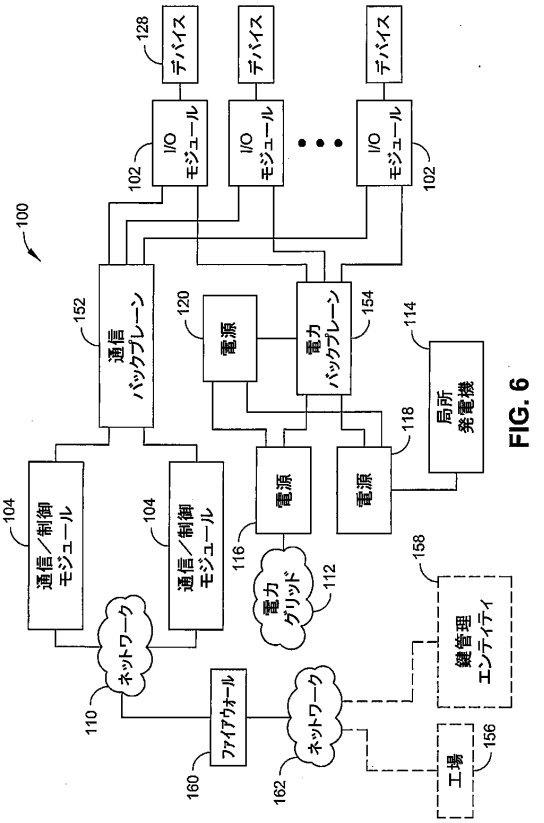

FIG. 6

【図７】

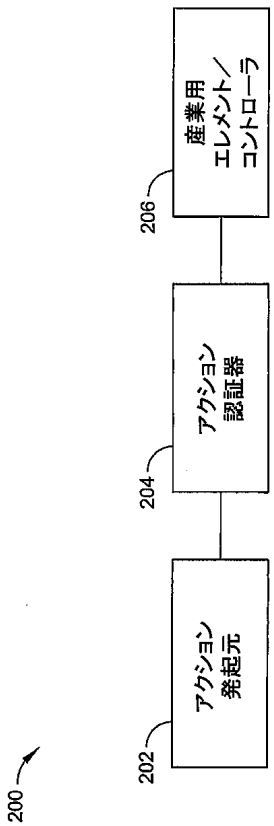

FIG. 7

【図８】

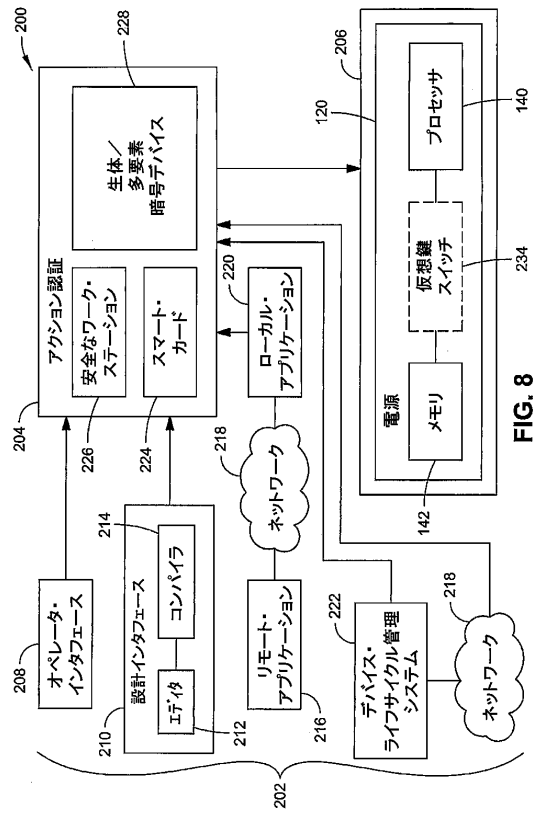

FIG. 8

【図９】

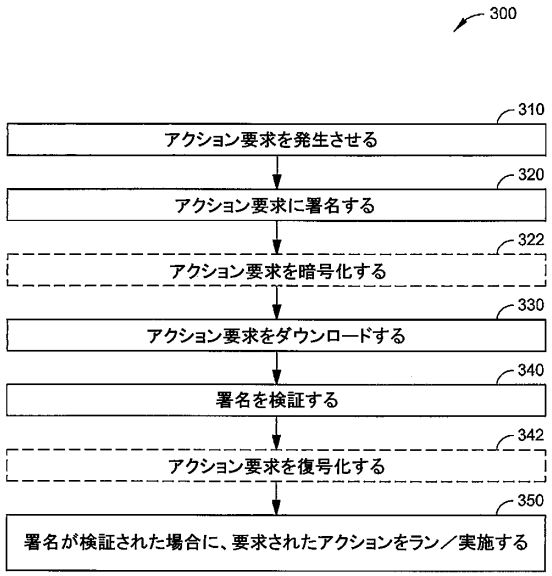

FIG. 9

【図１０】

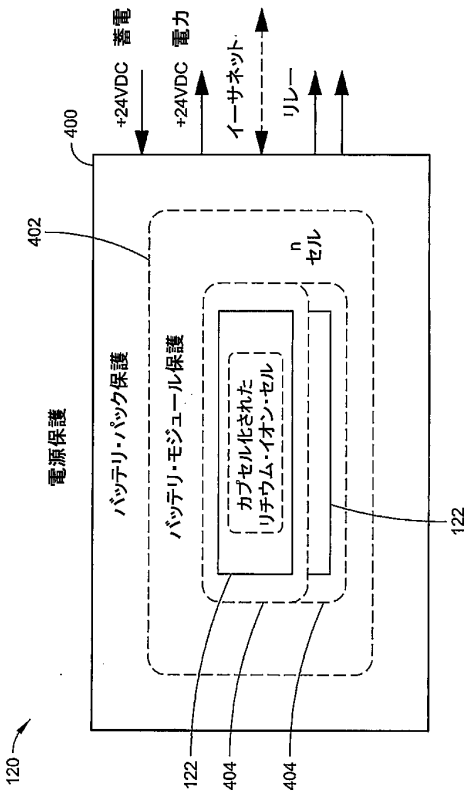

FIG. 10

【図１１】

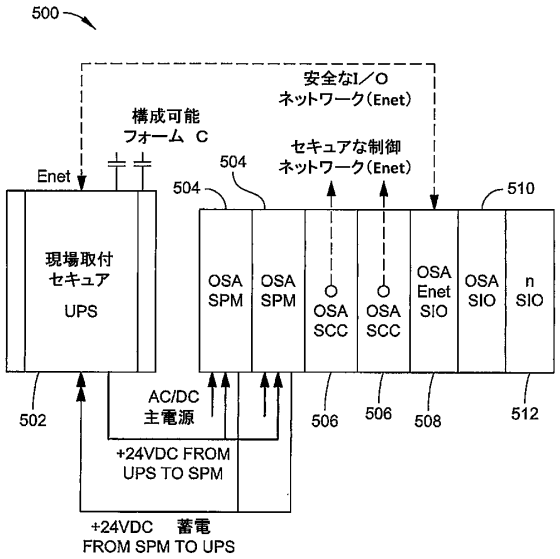

FIG. 11

【図１２】

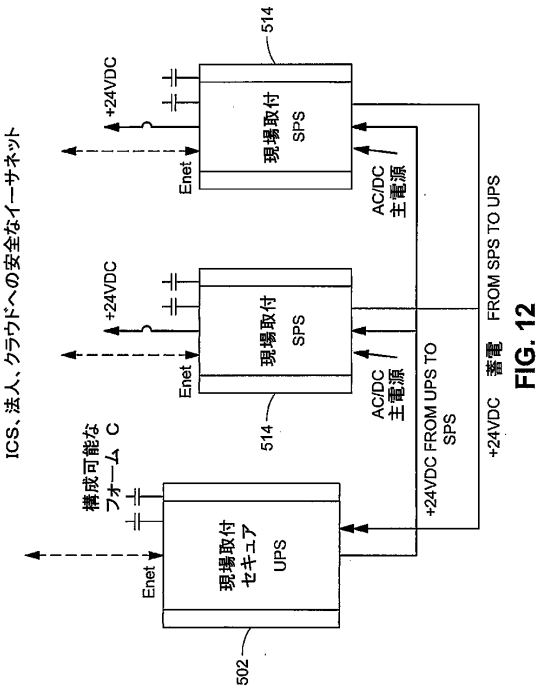

FIG. 12

フロントページの続き

(51)国際特許分類　　FI

H01M 10/44 (2006.01)		H01M	10/44	101
H01M 10/42 (2006.01)		H01M	10/42	P

(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

審査官　坂東 博司

(56)参考文献　米国特許出願公開第２０１３／００３１３８２（ＵＳ，Ａ１）
米国特許出願公開第２０１１／００８２６２１（ＵＳ，Ａ１）
特開２００５－１５１７２０（ＪＰ，Ａ）
特開２０１１－０７８２４９（ＪＰ，Ａ）
特開２０１２－１９５２５９（ＪＰ，Ａ）
特開２００９－１６３９０９（ＪＰ，Ａ）
特開２００２－１３４０７１（ＪＰ，Ａ）
米国特許出願公開第２００３／０１３７２７７（ＵＳ，Ａ１）
特開２０１３－０３１３５８（ＪＰ，Ａ）
特開２００１－２４２９７１（ＪＰ，Ａ）
特表２００４－５３２５９６（ＪＰ，Ａ）
国際公開第２０１４／１０３００８（WO，Ａ１）

(58)調査した分野　(Int.Cl.，ＤＢ名)

Ｈ０２Ｊ　１３／００
Ｈ０２Ｊ　７／００
Ｈ０２Ｊ　７／３４
Ｈ０４Ｑ　９／００
Ｈ０１Ｍ　１０／４８
Ｈ０１Ｍ　１０／４４
Ｈ０１Ｍ　１０／４２