

(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)Int. Cl.

F I

H 0 2 J 13/00 (2006.01)
H 0 2 J 7/00 (2006.01)
H 0 2 J 7/34 (2006.01)
H 0 4 Q 9/00 (2006.01)
H 0 1 M 10/48 (2006.01)

H 0 2 J 13/00 3 0 1 B
H 0 2 J 7/00 Y
H 0 2 J 7/34 B
H 0 4 Q 9/00 3 0 1 A
H 0 1 M 10/48 P

請求項の数 21 外国語出願 (全 43 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9513
4, 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9408
7, 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、

バッテリー・セル、および前記バッテリー・セルと通信可能に結合され、前記バッテリー・セルを監視して、前記バッテリー・セルの動作情報および前記バッテリー・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ー・モジュールを含む、バッテリー・モジュールと、

前記バッテリー・モジュールに動作可能に結合され、かつ、前記バッテリー・モジュール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、前記バッテリー・セルの動作情報および前記バッテリー・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ー・モジュールから受け取り、前記情報に基づいてバッテリー・モジュールレベルでの前記バッテリー・セルの診断を行い、前記バッテリー・セルの動作情報、前記バッテリー・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ー・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】

前記バッテリー・セルがリチウム・イオン・バッテリー・セルを含む、請求項1記載の電源。

【請求項3】

10

20

複数のバッテリー・モジュールを備え、前記バッテリー・モジュールの各々がスタックされて前記バッテリー・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】

前記バッテリー・モジュールの各々1つが物理的および電氣的に保護されるように、それぞれのバッテリー・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】

前記バッテリー・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ー・モジュールが物理的および電氣的に保護されるように、前記複数のバッテリー・モジュールがさらにバッテリー・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。

10

【請求項6】

前記バッテリー・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ー・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ー・セルの動作電圧、前記バッテリー・セルの動作電流、前記バッテリー・セルに関連づけられる電荷、または前記バッテリー・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】

20

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、バッテリー・セル、および前記バッテリー・セルと通信可能に結合され、前記バッテリー・セルを監視して、前記バッテリー・セルの動作情報および前記バッテリー・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ー・モニタを含む、バッテリー・モジュールと、

前記バッテリー・モジュールに動作可能に結合され、かつ、前記バッテリー・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、前記バッテリー・セルの動作情報および前記バッテリー・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ー・モニタから受け取り、前記情報に基づいてバッテリー・モジュールレベルでの前記バッテリー・セルの診断を行い、前記バッテリー・セルの動作情報、前記バッテリー・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ー・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

30

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】

前記バッテリー・セルがリチウム・イオン・バッテリー・セルを含む請求項8記載の電源ネットワーク。

【請求項10】

40

各電源が複数のバッテリー・モジュールを備え、前記バッテリー・モジュールの各々が、スタックされて前記バッテリー・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】

前記バッテリー・モジュールの各々1つが物理的および電氣的に保護されるように、それぞれのバッテリー・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】

前記バッテリー・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ー・モジュールが物理的および電氣的に保護されるように、前記複数のバッテリー・モジュールが

50

さらにバッテリー・パック保護レイヤによってケース収容される、請求項 1 1 記載の電源ネットワーク。

【請求項 1 3】

各電源が更に、前記バッテリー・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ー・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 1 2 記載の電源ネットワーク。

【請求項 1 4】

前記診断情報が前記バッテリー・セルの動作電圧、前記バッテリー・セルの動作電流、前記バッテリー・セルに関連づけられる電荷、または前記バッテリー・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。

10

【請求項 1 5】

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、

20

バッテリー・セル、および前記バッテリー・セルと通信可能に結合され、前記バッテリー・セルを監視して、前記バッテリー・セルの動作情報および前記バッテリー・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ー・モニタを含む、バッテリー・モジュールと、

前記バッテリー・モジュールに動作可能に結合され、かつ、前記バッテリー・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、前記バッテリー・セルの動作情報および前記バッテリー・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ー・モニタから受け取り、前記情報に基づいてバッテリー・モジュールレベルでの前記バッテリー・セルの診断を行い、前記バッテリー・セルの動作情報、前記バッテリー・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ー・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

30

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 1 6】

前記バッテリー・セルがリチウム・イオン・バッテリー・セルを含む、請求項 1 5 記載の産業用制御システム。

【請求項 1 7】

前記電源が複数のバッテリー・モジュールを備え、該バッテリー・モジュールの各々が、スタックされて前記バッテリー・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 5 記載の産業用制御システム。

40

【請求項 1 8】

前記バッテリー・モジュールの各々 1 つが物理的および電氣的に保護されるように、それぞれのバッテリー・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 1 7 記載の産業用制御システム。

【請求項 1 9】

前記バッテリー・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ー・モジュールが物理的および電氣的に保護されるように、前記複数のバッテリー・モジュールがさらにバッテリー・パック保護レイヤによってケース収容される、請求項 1 8 記載の産業用

50

制御システム。

【請求項 20】

前記バッテリー・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ー・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ー・セルの動作電圧、前記バッテリー・セルの動作電流、前記バッテリー・セルに関連づけられる電荷、または前記バッテリー・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。

10

【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。

20

30

【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 IEC 1508 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。

40

【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 (RTU

50

）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。

10

【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、バッテリー・セルおよびバッテリー・セルを監視するように構成されるバッテリー・モニタを含むバッテリー・モジュールを含む。実施形態において、電源はまた、バッテリー・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ー・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。

20

【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。

30

【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。

40

【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、多数のバッテリー・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

50

数のバッテリー・モジュールを含み、各バッテリー・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ー・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ー・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。

10

【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ー・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。

20

【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、バッテリーから自動化機器(automation equipment)にこれら設定で供給される。例えば、大規模バッテリー・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。大規模バッテリー・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)バッテリー供給が使用される。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ー技術(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・バッテリーは通常、制御ハードウェアから分離され、バッテリーのステータスを監視するために、各バッテリー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・バッテリーは、通例、このようなバッテリーの動作(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。

30

40

【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、バッテリー・セル、およびバッテリー・セルを監視するように構成されるバッテリー・モニタを含むバッテリー・モジュールを含む。実施形態では、電源はまた、バッテリー・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ー・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

50

、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ー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ー技術のような、より高エネルギー密度再充電可能バッテリー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)、明るさが無い、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、

10

20

30

40

50

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、「ハンドシェイク」）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。

10

【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。

20

30

【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。

40

50

【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つ以上のバッテリー・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。

10

【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「ハンドシェイク」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、バッテリー・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。

20

30

【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。

40

【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

50

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。

10

【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、バッテリー・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、バッテリー・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、他のバッテリー・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、バッテリー・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、他のバッテリー・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。

20

【0021】

[0032]実施形態の中には、バッテリー・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、バッテリー・モジュール 122 は、該バッテリー・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。他の実施形態では、電源 120 に接続された受電デバイスは、バッテリー・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、各バッテリー・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）バッテリー・モジュール 122 を認証する。

30

【0022】

[0033]実施形態の中には、コントローラ 128 がバッテリー・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ー・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 つ以上のバッテリー・モジュール 122 を認証する。更なる実施形態では、1 つのバッテリー・モジュール 122 が他のバッテリー・モジュール 122 を認証することができる。例えば、第 1 バッテリー・モジュール 122 は、該第 1 バッテリー・モジュール 122 が有する第 1 認証モジュール 134 と第 2 バッテリー・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 バッテリー・モジュール 122 を認証する。実施形態の中には、第 2 バッテリー・モジュール 122 がまた第 1 バッテリー・モジュール 122 を認証することができるものもある。

40

【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

50

、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。

10

20

【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。

30

【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・データをデジタル・データに変換するように（例えば、アナログ／デジタル変換器（ADC）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、デジタル・データをアナログ・データに変換するように（例えば、デジタル／アナログ（DAC）回路等を使用して）構成することもできる。実装態様では、I/Oモジュール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。

40

【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

50

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。

10

【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と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イ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。

20

30

【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。

40

【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

50

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。

10

【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。

20

【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、多数のバッテリー・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。

30

40

【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。）。

50

【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。

10

【0035】

[0045]図4を参照する。電源120は、多数のバッテリー・モジュール122を含む。開示する実施形態では、各バッテリー・モジュール122は、リチウムイオン・バッテリー・セル124を含む。例えば、1つのバッテリー・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個の間のバッテリー・モジュール122を含むものもある。しかしながら、8から10個の間のバッテリー・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ー・モジュール122が共にスタックされる。

20

【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つ以上のバッテリー・セルを含む）バッテリー・モジュール122のスタックを含むバッテリー・パックを含むことができる。実施形態の中には、各バッテリー・モジュール122は、バッテリー・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、バッテリー・モジュール122は共にスタックされて、バッテリー・パックを形成する。スタックされたバッテリー・モジュール122（即ち、バッテリー・パック）はまた、バッテリー・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つ以上のバッテリー・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ー・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。

30

【0037】

[0047]なお、バッテリー・モジュール122は、リチウムイオン・バッテリー・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ー、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・イオンバッテリー、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、熔融塩電池および酸化銀電池等である。

40

【0038】

[0048]バッテリー・モジュール122の各々は、リアルタイム・バッテリー・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、バッテリー・モニタ126は、バッテリー・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、各バッテリー・モ

50

ニタ126は、コントローラ128に対し、バッテリー・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、バッテリー・セル124の動作電圧、バッテリー・セル124の動作電流（例えば、アンペアで）、電荷のバッテリー・セル124へのユニット（例えば、クーロンで）、電荷のバッテリー・セル124からの電荷のユニット（例えば、クーロンで）、バッテリー・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ー・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、各バッテリー・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。他の実施形態では、多数のバッテリー・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。バッテリー・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。バッテリー・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、バッテリー・セル124から放電される。他の電源レギュレータ132は、バッテリー・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、各バッテリー・モジュール122は、支持フレームを、ホイルで包まれた(foil-wrapped)バッテリー・セル124と共に備える。ここでは、バッテリー・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ー・セル124の伸び縮みを許容する。開示する実施形態では、バッテリー・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ー・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、バッテリー・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、バッテリー・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ーに蓄電されるのを防止し、また、エネルギーがバッテリー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、バッテリー・セル124への電氣的接続が防止される。更に、バッテリー・モニタ126がアクティブではないとき（例えば、バッテリー・セル124が何ら充電されていないとき）に、バッテリー・セル124への電氣的接続が防止される。この例では、バッテリー・モジュール122が電源120に挿入されるときに、バッテリー・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、バッテリー・モジュール122は、各支持フレームに配置される電氣的コンタクト（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、バッテリー・モニタPCBを介して）バッテリー・セル124に電氣的に接続され、（さもなければバッテリー・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、多数のバッテリー・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つの電氣的コンタクトは、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、他の電氣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つのバッテリー・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、バッテリー・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つのバッテリー・モジュール122の電気コネクタを、他のバッテリー・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ー・モジュール122の整列を設けるために、バッテリー・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)を各バッテリー・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ー・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ー・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、バッテリー故障に困りリリースされることがある化学バッテリー・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氣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、バッテリー・モニタ126およびバッテリー・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

10

20

30

40

50

イソレータ等を使用して) バッテリ・モジュール 1 2 2 および電源レギュレータ 1 3 2 から電氣的に分離および／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 1 2 8 は(例えば、ネットワーク 1 1 0 を介して)産業用制御システム 1 0 0 に接続される。開示する実施形態では、コントローラ 1 2 8 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 1 2 2 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 1 2 8 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 1 4 0 はコントローラ 1 2 8 と共にまたはコントローラ 1 2 8 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 1 2 8 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 1 2 8 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。

10

20

【0047】

[0057]プロセッサ 1 4 0 は、処理機能をコントローラ 1 2 8 に提供する。プロセッサ 1 4 0 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 1 2 8 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 1 4 0 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 1 4 0 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。

30

【0048】

[0058]コントローラ 1 2 8 はまた、メモリ 1 4 2 を含む。メモリ 1 4 2 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 1 2 8 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 1 4 0 およびおそらくはコントローラ 1 2 8 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 1 4 2 は、データ(例えば、電源 1 2 0 (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 1 4 2 は、電源 1 2 0 のための一意識別子 1 3 6 および／またはセキュリティ証明書 1 3 8 を格納することができる。なお、単一のメモリ 1 4 2 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 1 4 2 は、プロセッサ 1 4 0 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することもできる。メモリ 1 4 2 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

40

50

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、バッテリー・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ー・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、バッテリー・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、バッテリー・モニタ 126 から診断情報（例えば、バッテリー・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、バッテリー・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ー・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、3 G セルラ・ネットワーク、4 G 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、IEEE 802.11 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、IEEE 802.15 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

10

20

30

40

50

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）からのガバナニ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。

10

20

【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）に電氣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。

30

【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。

40

【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

50

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

10

20

30

40

50

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

10

20

30

40

50

、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認する。

10

【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。

20

【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。

30

40

【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、

50

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

10

20

30

40

50

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（ウイルス）、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 のバッテリー・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 のバッテリー・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（Nonce A）、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（Nonce A）を生成し、第 1 ノンス（Nonce A）、第 1 デバイス認証鍵証明書（CertDAKA）、および第 1 識別情報属性証明書（IACA）を連結して、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

10

20

30

40

50

・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／組み合わせられたノンスに、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、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

10

20

30

40

50

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(s i g A [N o n c e A | | N o n c e B])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、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(s i g A [N o n c e A | | E r r o r])とを含む「失敗」認証データグラムと置き換えることができる。

10

【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(s i g B [N o n c e A | | E r r o r])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(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(N o n c e A)および第2のローカルに格納されているノンス(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(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。

20

30

【0079】

[0089]認証モジュールが「マスタスレーブ」構成にしたがって配置される実装態様では、マスタ(例えば、第1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。

40

【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、S C A D AまたはH M I)、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

50

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 (「DL M」) 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 D L M 222) 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、RF I D 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 のインター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と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か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、HDD

10

20

30

40

50

、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「ハンドシェイク」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

10

20

30

40

50

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取ることができる。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取ることができる。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（SSD）、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】

[0100]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、回路の要素は、多数の集積回路にわたって実装することもできる。このような集積回路は、モノリシック集積回路、フリップ・フロップ集積回路、マルチチップ・モジュール集積回路、および／または混合信号集積回路を含む種々の集積回路を含むことができるが、必ずしもこれらに限定されるのではない。ソフトウェア実装態様の例では、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まるべきである。逆に、以上で説明した特定の主題は、特許請求の範囲を実現する形態例として開示されたまでである。

10

20

30

40

50

【図1】

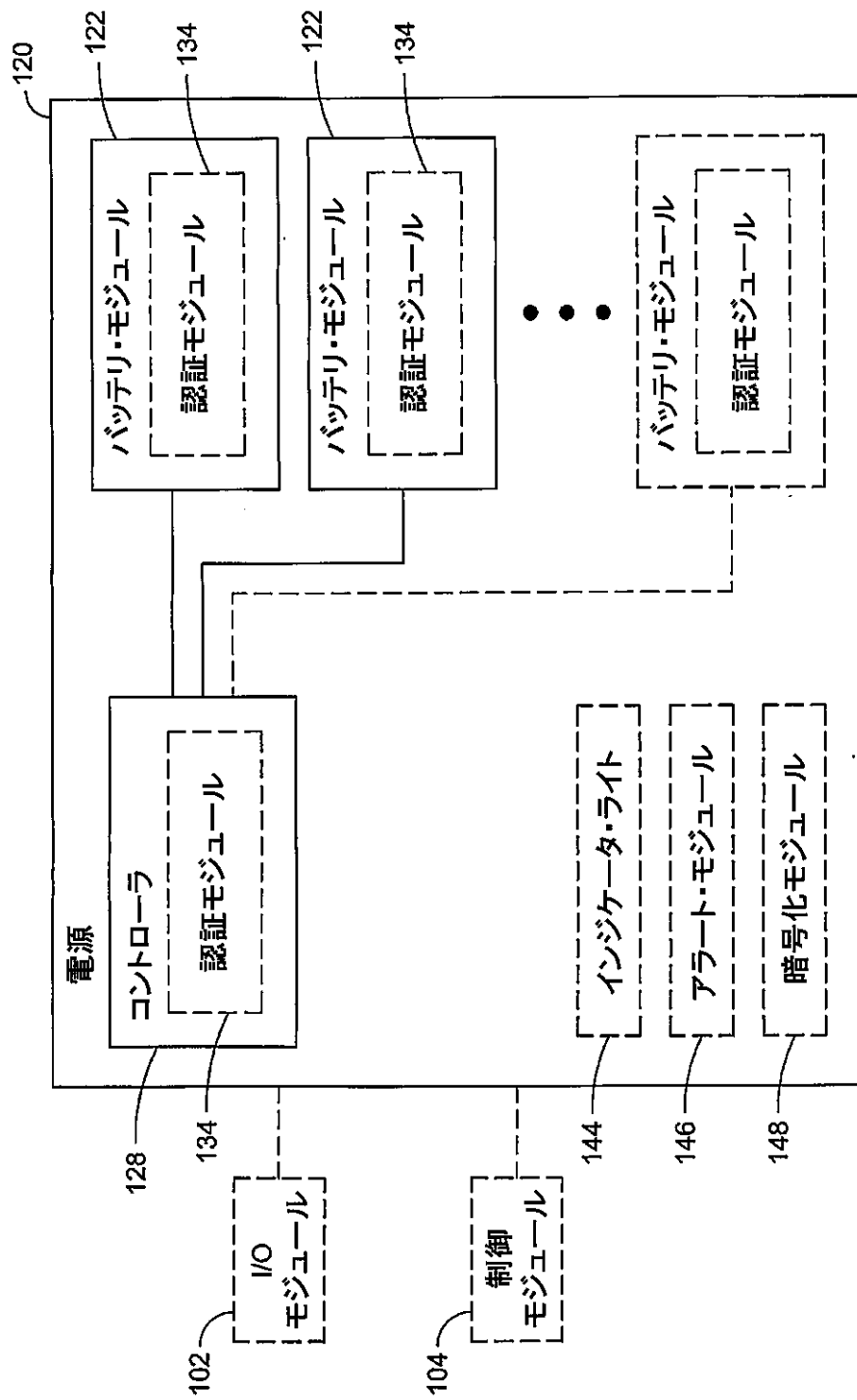


FIG. 1

10

20

30

40

50

【図2】

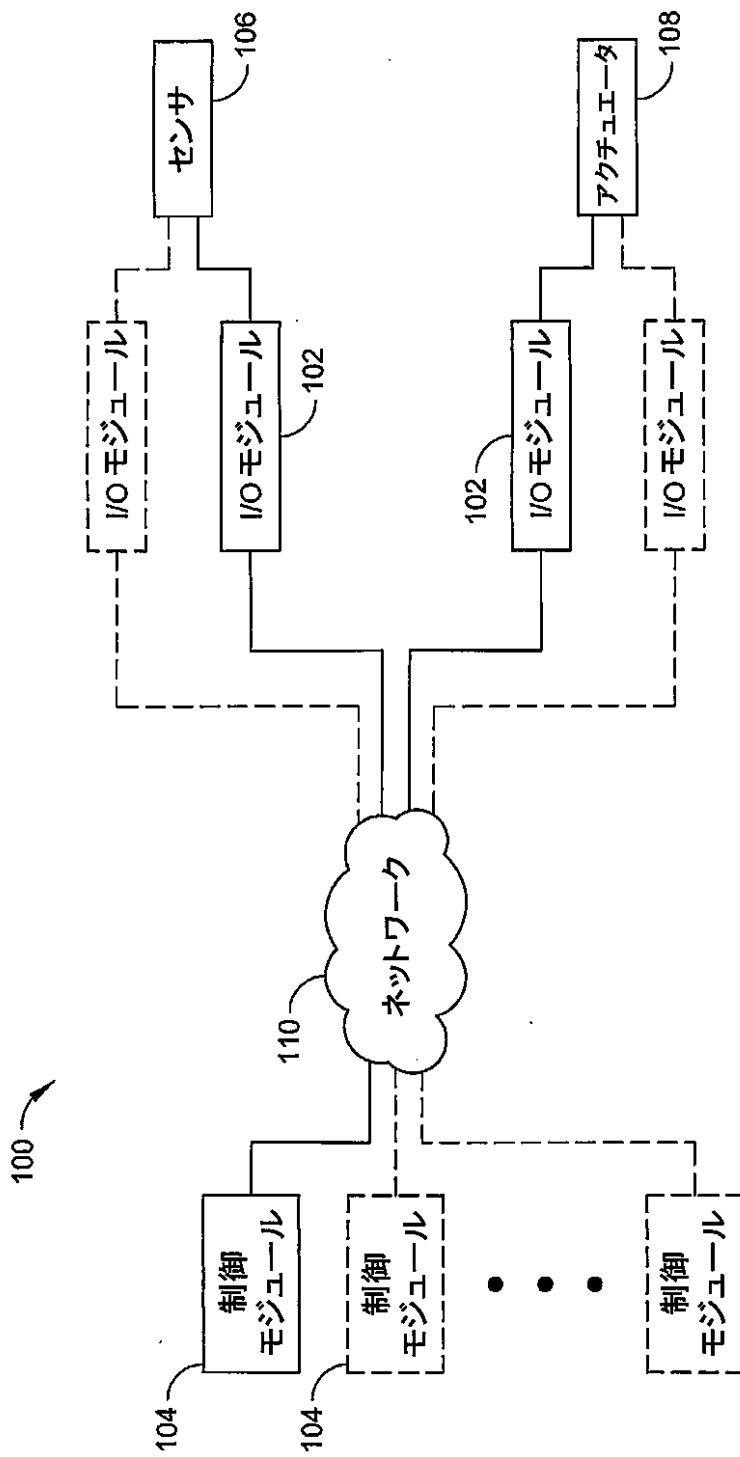


FIG. 2

10

20

30

40

50

【図3】

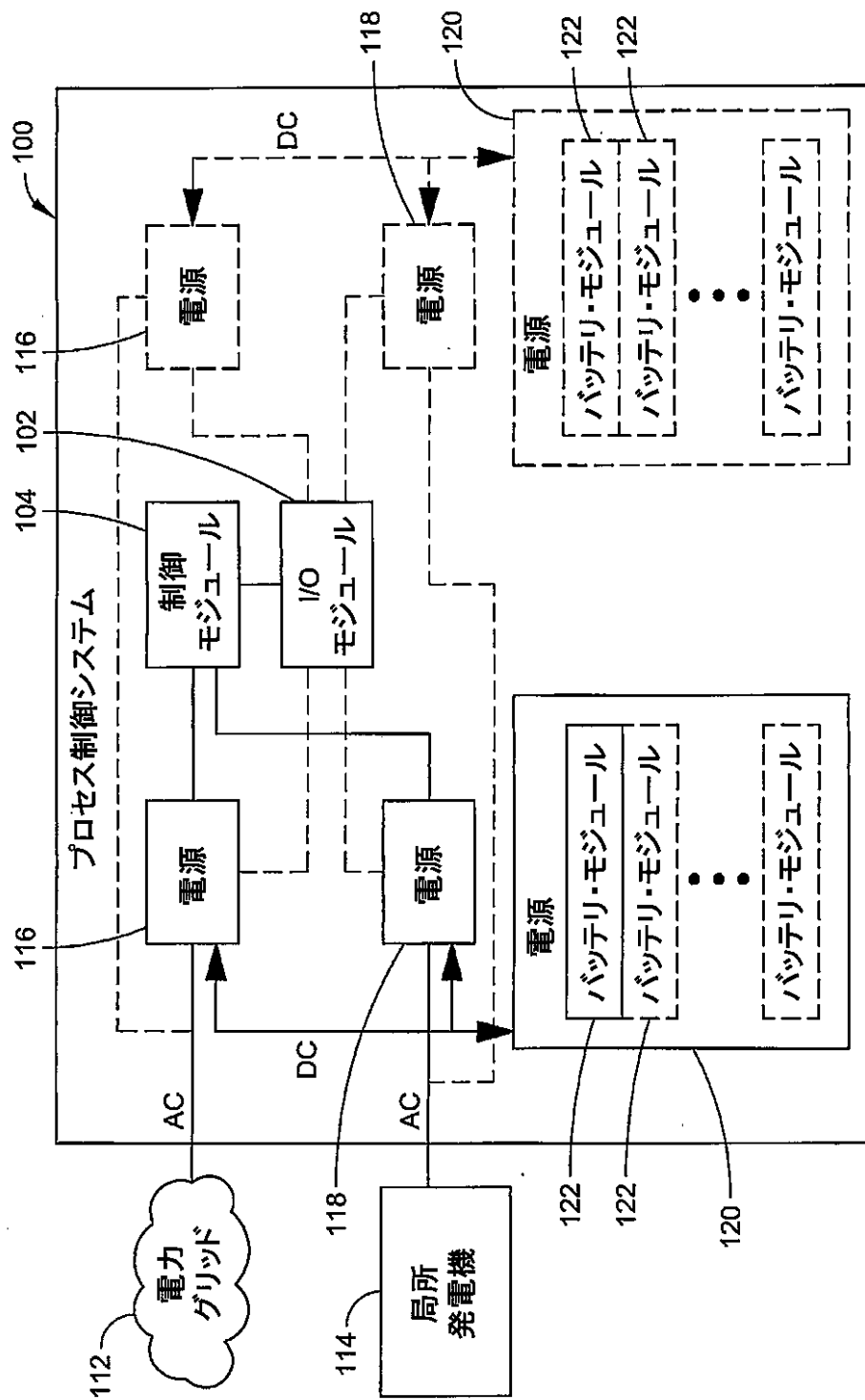


FIG. 3

10

20

30

40

50

【図4】

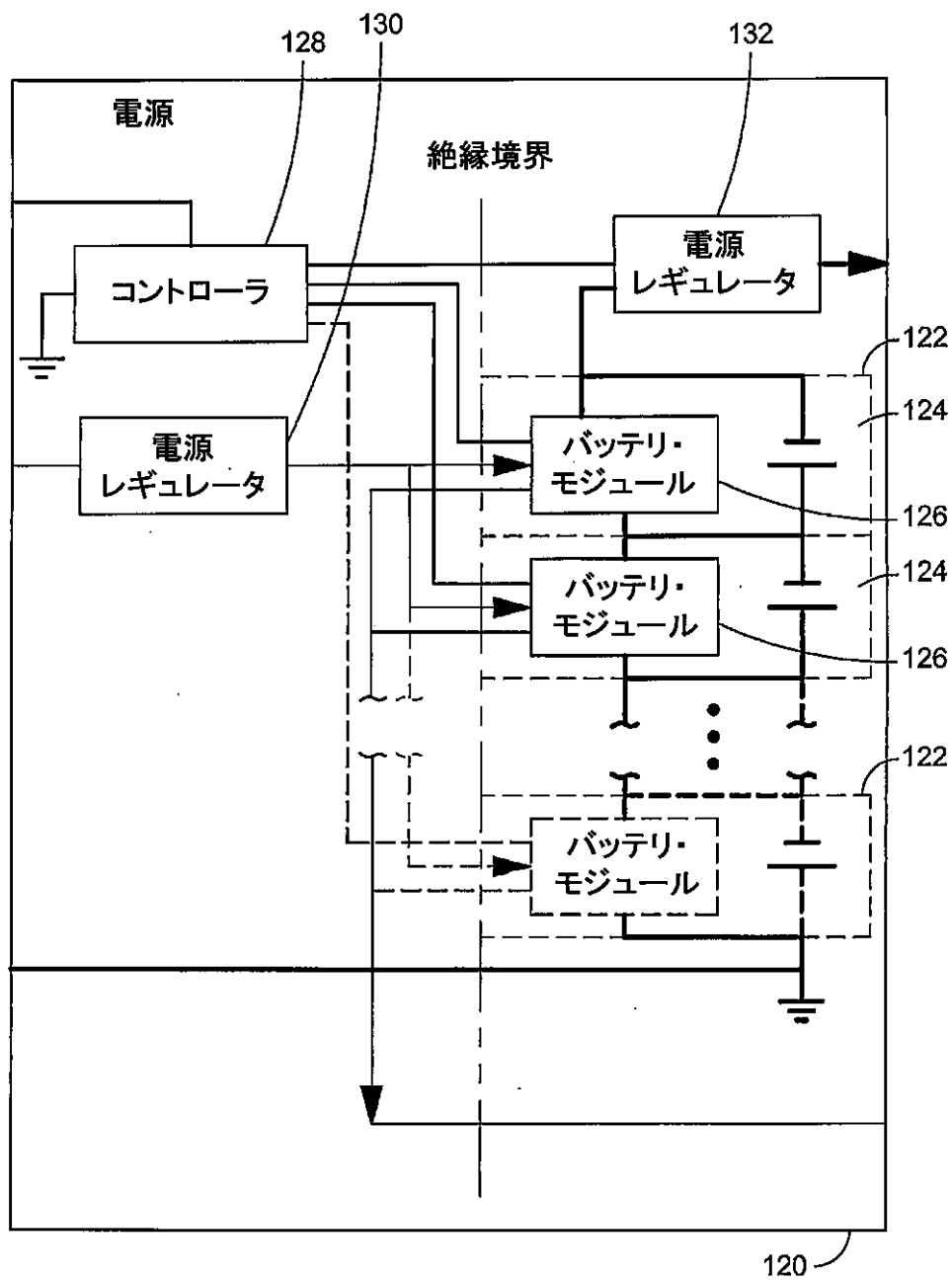


FIG. 4

【図5】

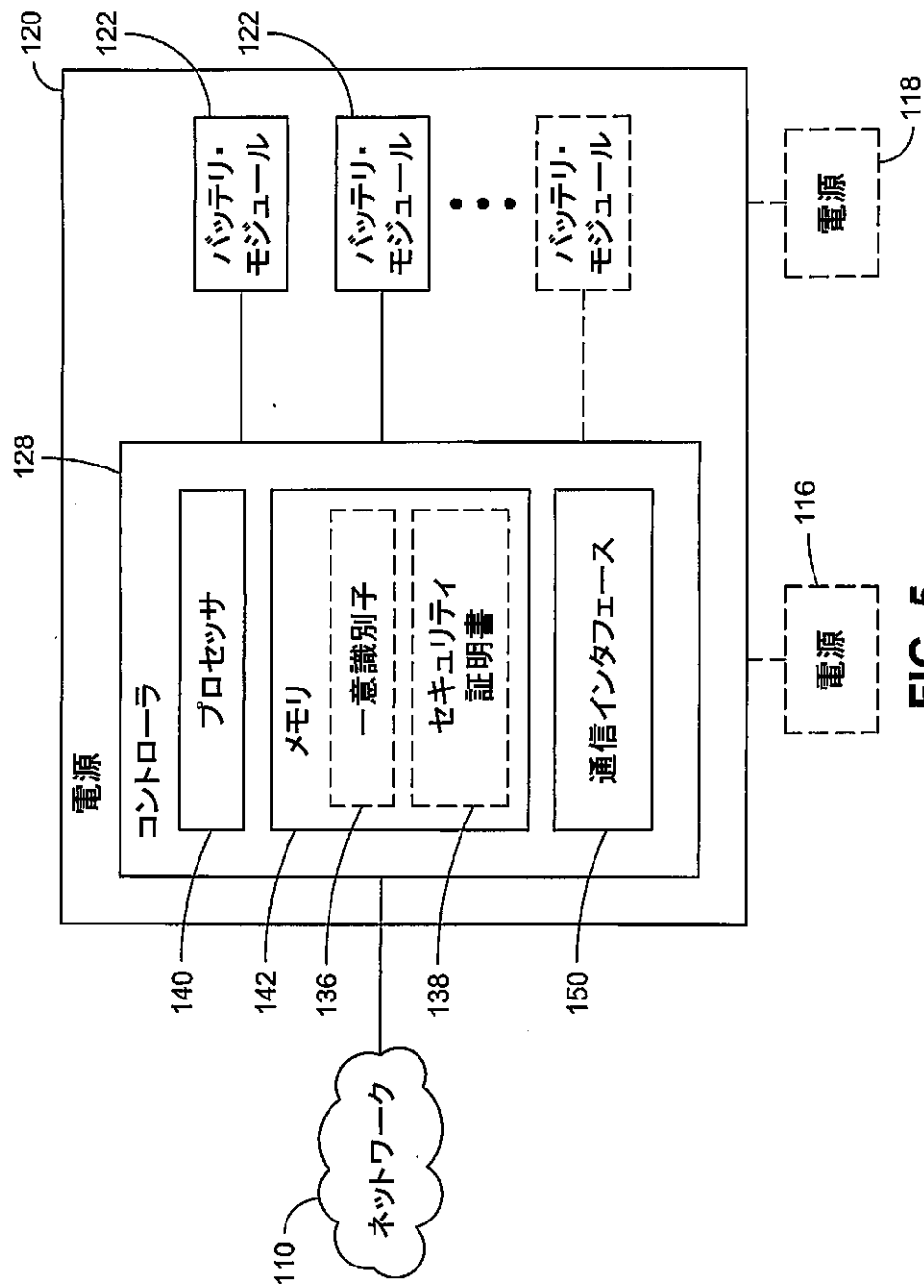


FIG. 5

【図 7】

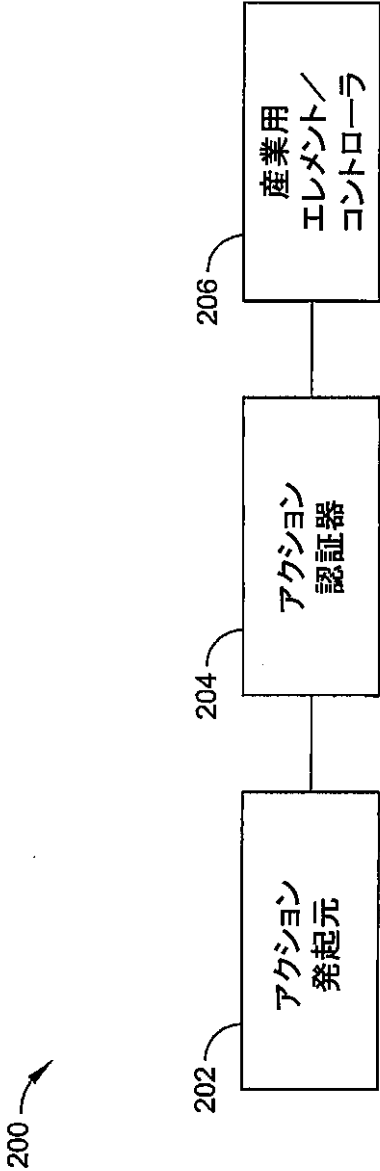


FIG. 7

10

20

30

40

50

【図8】

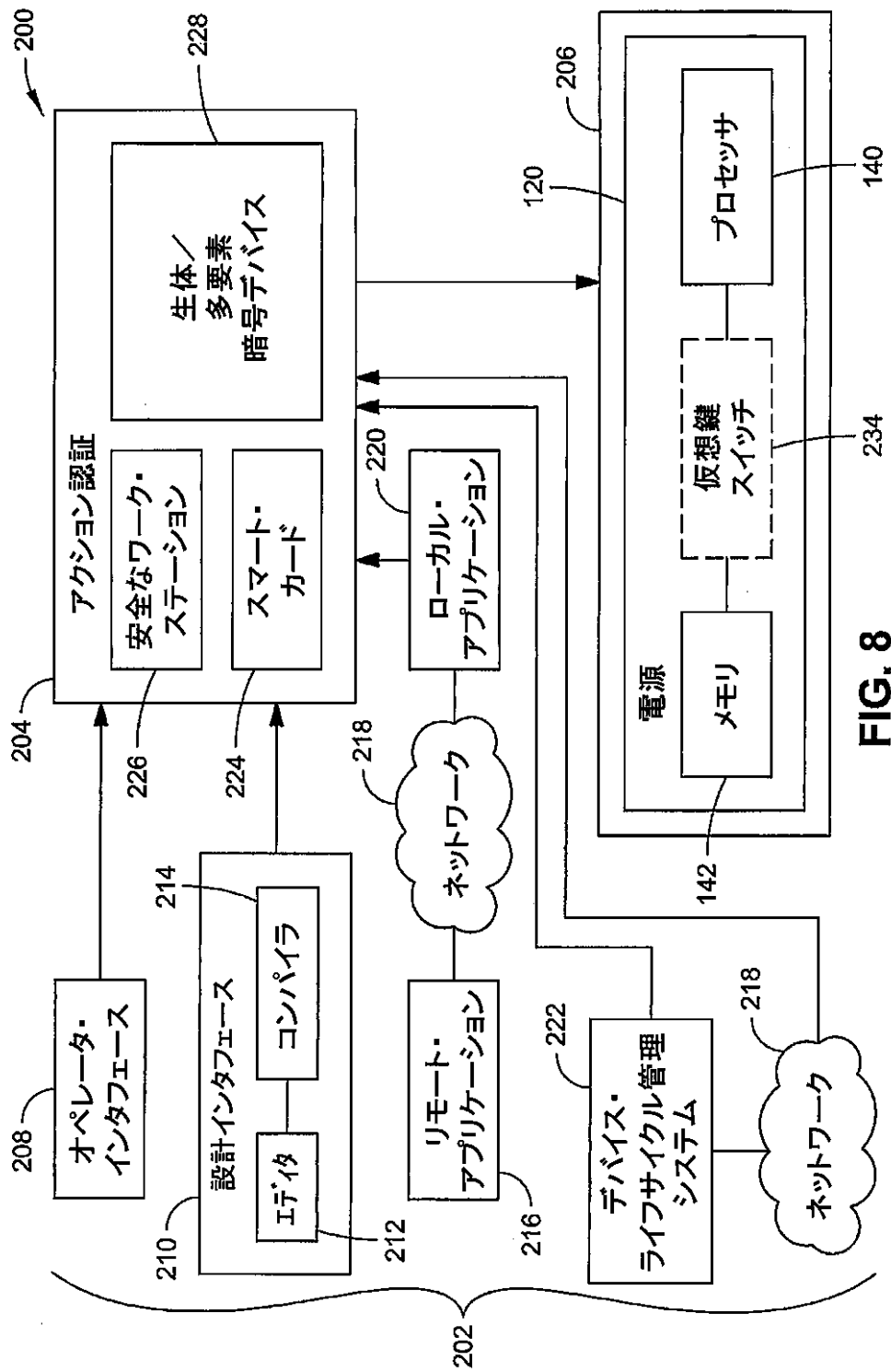


FIG. 8

10

20

30

40

50

【図9】

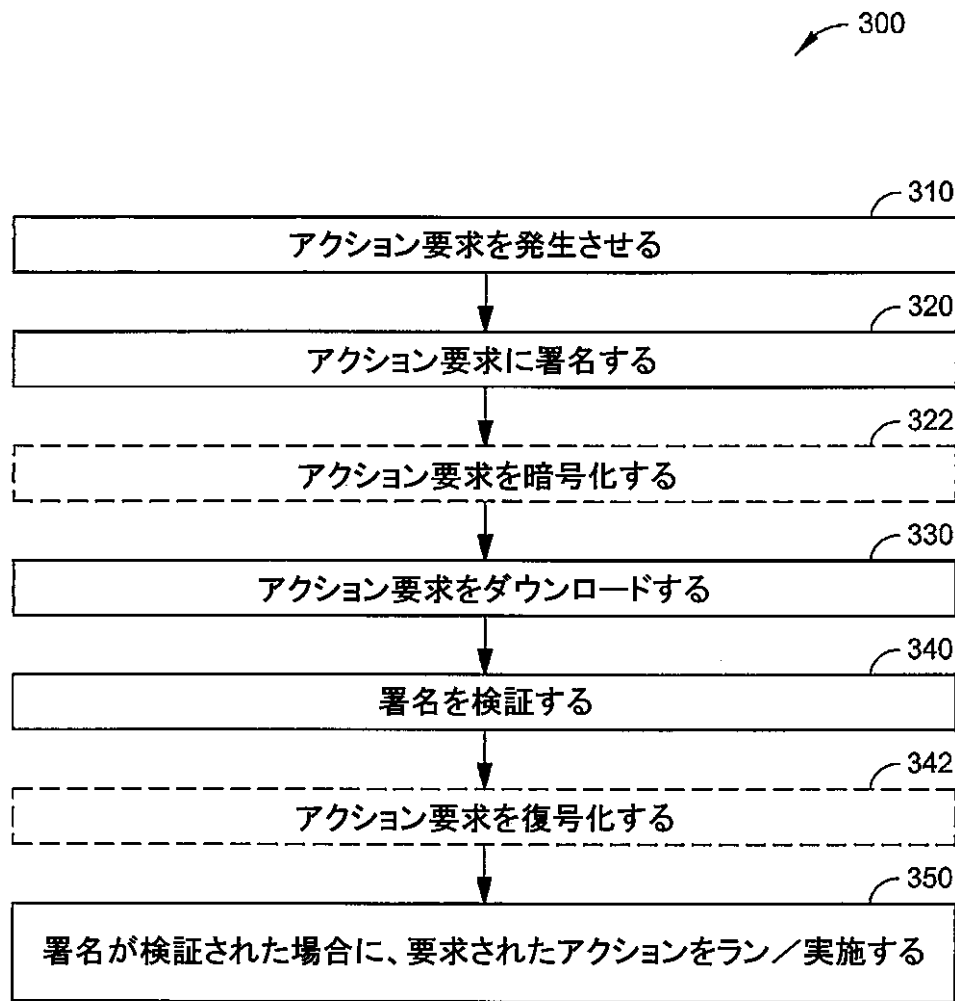


FIG. 9

【図10】

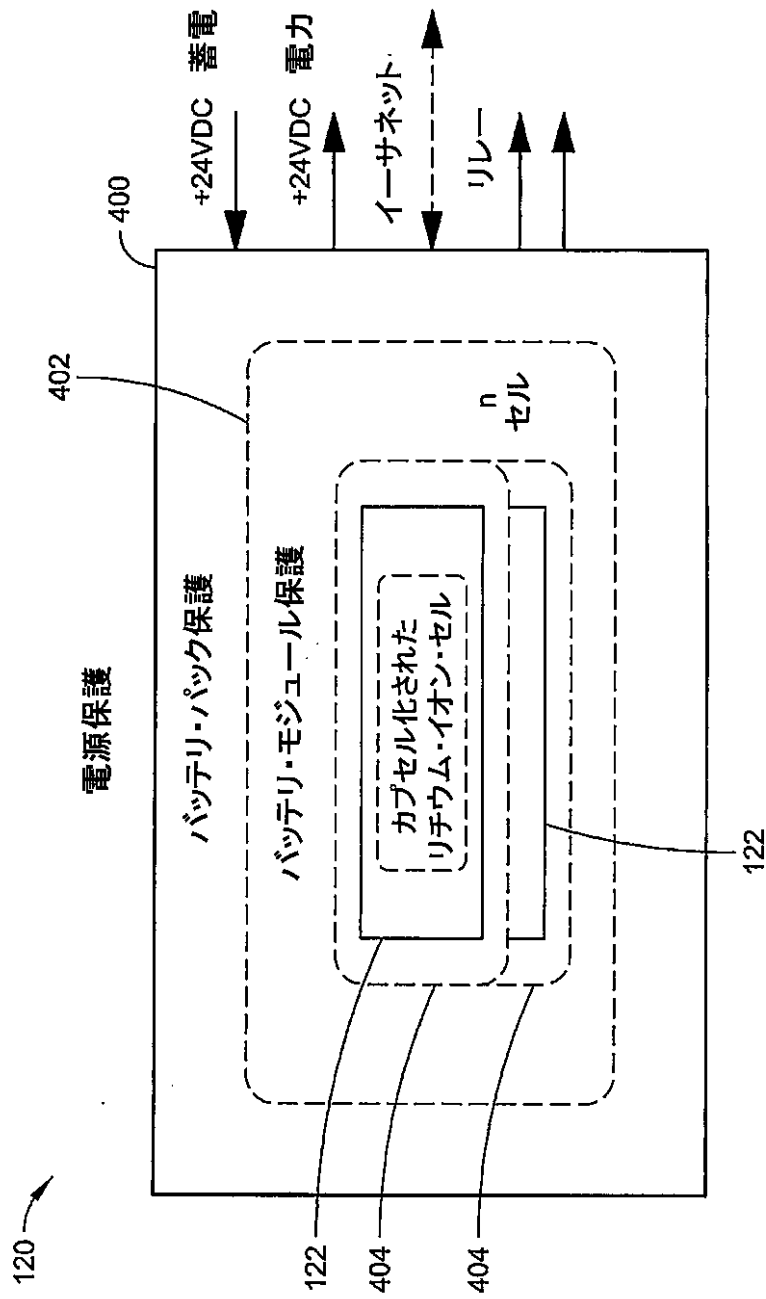


FIG. 10

10

20

30

40

50

【図 11】

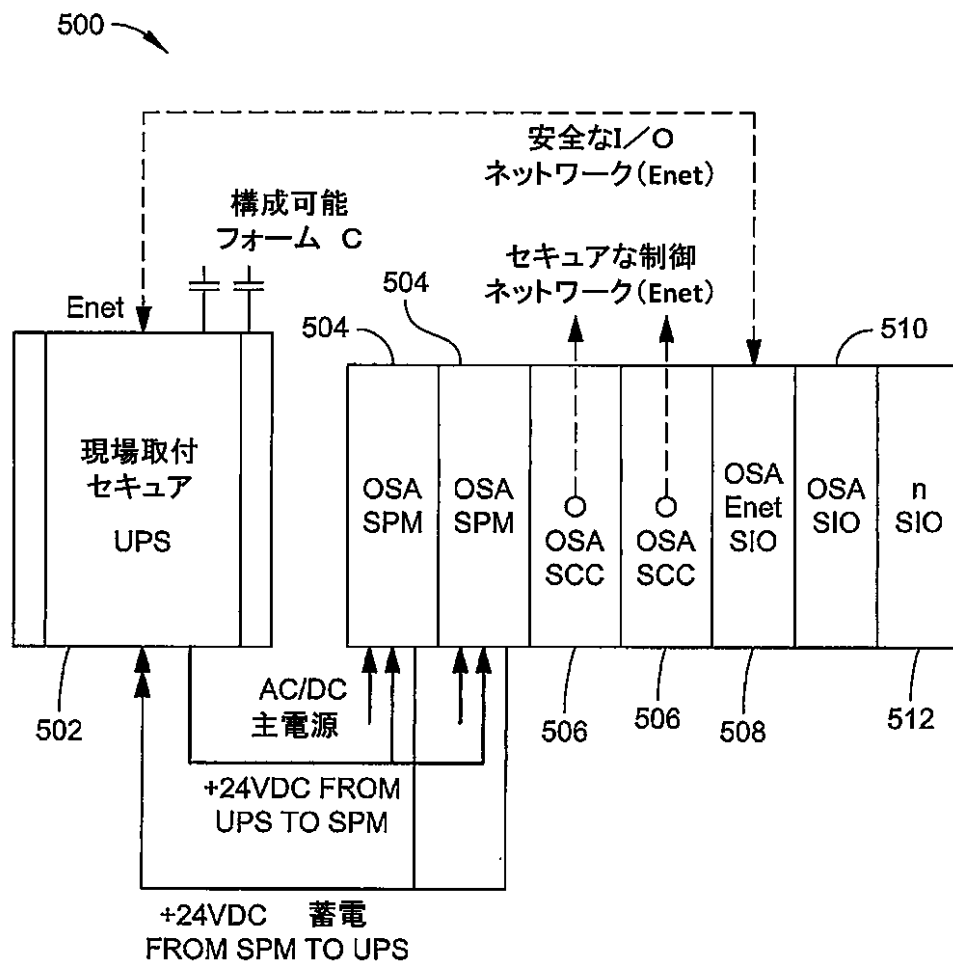


FIG. 11

【図12】

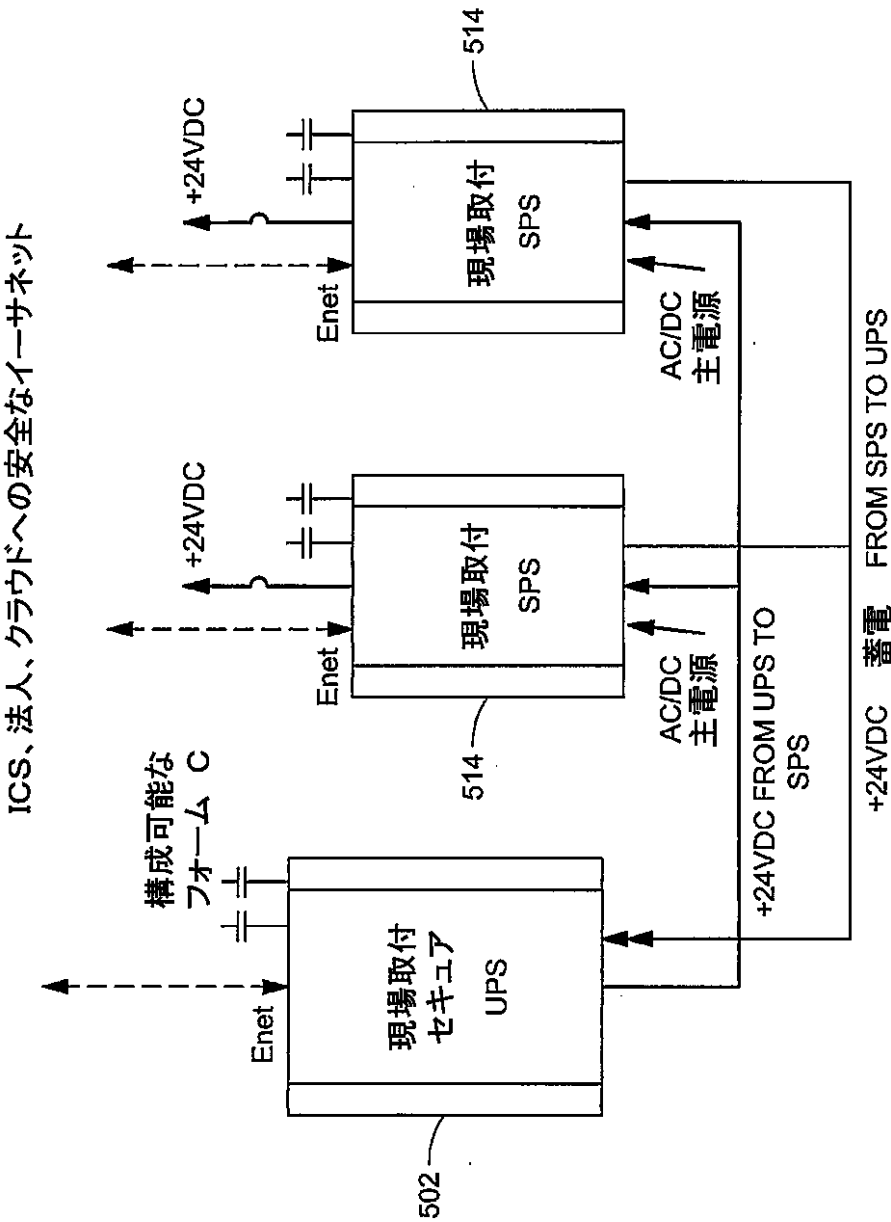


FIG. 12

10

20

30

40

50

フロントページの続き

(51)Int.Cl. F I
H 0 1 M 10/44 (2006.01) H 0 1 M 10/44 1 0 1
H 0 1 M 10/42 (2006.01) H 0 1 M 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)
H 0 2 J 1 3 / 0 0
H 0 2 J 7 / 0 0
H 0 2 J 7 / 3 4
H 0 4 Q 9 / 0 0
H 0 1 M 1 0 / 4 8
H 0 1 M 1 0 / 4 4
H 0 1 M 1 0 / 4 2