(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6960715号
(P6960715)

(45)発行日　令和3年11月5日(2021.11.5)　(24)登録日　令和3年10月14日(2021.10.14)

(51)Int.Cl.		F I		
H02J 7/00	(2006.01)	H02J	7/00	302A
G01R 31/36	(2020.01)	G01R	31/36	
G05B 23/02	(2006.01)	G05B	23/02	V
H01M 10/42	(2006.01)	H01M	10/42	P
H01M 10/48	(2006.01)	H01M	10/48	P

請求項の数 8　外国語出願　(全 30 頁)　最終頁に続く

(21)出願番号　特願2014-243827 (P2014-243827)
(22)出願日　平成26年12月2日 (2014.12.2)
(65)公開番号　特開2015-156786 (P2015-156786A)
(43)公開日　平成27年8月27日 (2015.8.27)
審査請求日　平成29年12月4日 (2017.12.4)
審判番号　不服2020-4176 (P2020-4176/J1)
審判請求日　令和2年3月30日 (2020.3.30)
(31)優先権主張番号　61/940,003
(32)優先日　平成26年2月14日 (2014.2.14)
(33)優先権主張国・地域又は機関
米国 (US)
(31)優先権主張番号　62/021,438
(32)優先日　平成26年7月7日 (2014.7.7)
(33)優先権主張国・地域又は機関
米国 (US)

(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　100120112
弁理士　中西　基晴
(74)代理人　100173565
弁理士　末松　亮太

最終頁に続く

(54)【発明の名称】産業用制御システムに関する安全な電源

(57)【特許請求の範囲】
【請求項１】
電源であって、
電池セルと、該電池セルをモニタして該電池セルに関連付けられる診断情報を生成するように構成されるバッテリモニタとを備える電池モジュールと、
前記電池モジュールに動作可能に結合されるコントローラであって、前記電池モジュールから前記診断情報を受け取るように構成されるコントローラと、
を備え、
前記電池セルのターミナルへの電気経路が短絡回路であるか、または、当該電源における前記電池モジュールへの別のデバイスの接続が認証モジュールによって認証することができないかの少なくとも一方のときに、前記バッテリモニタが、前記電池セルへの電気的アクセスを防止するように構成される、電源。
【請求項２】
前記電池セルが、リチウムイオン電池セルを有することを特徴とする請求項１に記載の電源。
【請求項３】
前記診断情報が前記電池セルの動作電圧、前記電池セルの動作電流、前記電池セルと関連した電荷、または、前記電池セルと関連した寿命の少なくとも１つを含む、請求項１に記載の電源。
【請求項４】

当該電源が複数の電池モジュールを備え、該複数の電池モジュールが、スタックされて電気的に相互に接続される、請求項１に記載の電源。
【請求項５】
前記バッテリモニタが、アナログスイッチにより直列に接続された複数の電界効果トランジスタを備えた電子信号切換デバイスを備え、
前記電子信号切換デバイスは、前記バッテリモニタからの認証なしで、エネルギが、前記電池セルに蓄電されること、または、前記電池セルから放電されることの少なくとも一方を防止するように構成される、請求項１に記載の電源。
【請求項６】
前記電池モジュールまたは前記コントローラの少なくとも１つが、前記認証モジュールによる前記認証に関し、ユニーク識別子またはユニークセキュリティ証明書の少なくとも１つを用いて構成される、請求項１に記載の電源。
【請求項７】
制御システムであって、
電源と、
該電源に電気的に結合された交流電源と、
前記交流電源により供給される電気エネルギを蓄電および放電するように前記交流電源に電気的に結合される無停電電源であって、電池セル、および該電池セルをモニタして該電池セルに関連付けられる診断情報を生成するように構成されたバッテリモニタを備える少なくとも１つの電池モジュールと、該電池モジュールに動作可能に結合され、前記電池モジュールから前記診断情報を受け取るように構成されるコントローラと、を備える、無停電電源と、
前記交流電源に電気的に接続される少なくとも１つの制御エレメントまたはサブシステムと、を備え、
前記無停電電源は、前記電源により供給される電気エネルギが中断されると、前記少なくとも１つの制御エレメントまたはサブシステムに電力を供給するように、前記交流電源に電気エネルギを放電するように構成され、
前記電池セルのターミナルへの電気経路が短絡回路であるか、または、前記電源における前記電池モジュールへの接続が認証モジュールによって認証することができないかの少なくとも一方のときに、前記バッテリモニタが、前記電池セルへの電気アクセスを防止するように構成される、制御システム。
【請求項８】
制御システムであって、
電源と、
該電源に電気的に結合された交流電源と、
前記交流電源により供給される電気エネルギを蓄電および放電するように前記交流電源に電気的に結合される無停電電源であって、電池セル、および該電池セルをモニタして該電池セルに関連付けられる診断情報を生成するように構成されたバッテリモニタを備える少なくとも１つの電池モジュールと、該電池モジュールに動作可能に結合され、前記電池モジュールから前記診断情報を受け取るように構成されるコントローラと、を備える、無停電電源と、
前記交流電源に電気的に接続される少なくとも１つの制御エレメントまたはサブシステムと、を備え、
前記無停電電源は、前記電源により供給される電気エネルギが中断されると、前記少なくとも１つの制御エレメントまたはサブシステムに電力を供給するように、前記交流電源に電気エネルギを放電するように構成され、
前記バッテリモニタは、アナログスイッチにより直列に接続される複数の電界効果トランジスタを備える電子信号切換装置を備え、
前記電子信号切換デバイスは、前記バッテリモニタからの認証なしで、エネルギが、前記電池セルに蓄電されること、または、前記電池セルから放電されることの少なくとも一

方を防止するように構成される、制御システム。
【発明の詳細な説明】
【技術分野】
【０００１】
関連出願についてのクロス・リファレンス
[0001] 米国特許法§１１９（ｅ）の下で米国の仮特許出願番号第６１／９４０，００３号の本出願は２０１４年2月１４日に「ＢＡＣＫＵＰ　ＰＯＷＥＲ　ＳＵＰＰＬＹ」というタイトルで出願され、本願明細書において、全体的にリファレンスによって、組み込まれ、優先権を有する。本出願は、２０１３年８月６日に出願された国際出願番号ＰＣＴ／ＵＳ２０１３／０５３７２１「ＳＥＣＵＲＥＩＮＤＵＳＴＲＩＡＬＣＯＮＴＲＯＬＳＹＳＴＥＭ」の一部継続出願でもある　本出願は、２０１４年８月２７日に出願された米国特許出願公開番号１４／４６９，９３１（「ＳＥＣＵＲＥ　ＩＮＤＵＳＴＲＩＡＬ　ＣＯＮＴＲＯＬ　ＳＹＳＴＥＭ」）の米国特許法第１２０条の一部継続でもある。本出願は、２０１４年7月３０日に出願された米国特許出願公開番号１４／４４６，４１２（「ＩＮＤＵＳＴＲＩＡＬ　ＣＯＮＴＲＯＬ　ＳＹＳＴＥＭ　ＣＡＢＬＥ」）の米国特許法第１２０条の一部継続でもあり、２０１４年7月７日に出願された米国仮特許出願番号６２／０２１，４３８（「ＩＮＤＵＳＴＲＩＡＬ　ＣＯＮＴＲＯＬ　ＳＹＳＴＥＭ　ＣＡＢＬＥ」）の米国特許法第１１９条（ｅ）の下で優先権を主張　し、米国仮特許出願番号６１／９４０,００３および６２／０２１，４３８、並びに、米国特許出願公開番号１４／４４６，４１２および１４／４６９，９３１、並びに、国際出願番号ＰＣＴ／ＵＳ２０１３／０５３７２１は、本願明細書において、全体としてリファレンスによって、組み込まれる。
【背景技術】
【０００２】
[0002] 例えば標準産業用制御システム（ＩＣＳ）またはプログラム可能なオートメーション・コントローラ（ＰＡＣ）は、工業生産、例えば安全基準（例えばＩＥＣ１５０８）に保証される管理制御およびデータ収集（ＳＣＡＤＡ）システム、分散制御システム（ＤＣＳ）、プログラマブル論理コントローラ（ＰＬＣ）および産業安全システムのような産業用制御システムにおいて、使用する様々な形の制御装置を備える。これらのシステムが、電気、水および廃水、油およびガス生産および精製、化学、食品、医薬およびロボット工学を含む産業において、使われる。プロセス変数を測定するために様々な形のセンサから集められる情報を使用して、産業用制御システムからのオートメーション化したおよび／またはオペレータ駆動管理命令は、さまざまなアクチュエーター装置（例えば制御弁、油圧アクチュエータ、磁気アクチュエータ、電気的スイッチ、モーター、ソレノイド、など）に発信されることがありえる。これらのアクチュエーター装置はセンサからデータを集める。そして、センサシステム（開閉弁およびブレーカ）は弁を制御する。そして、モーターは警報状態などに関し工業処理をモニタする。
【０００３】
[0003] 他の例示において、ＳＣＡＤＡシステムは、地理的に広く分離されることができるプロセス・サイトを有する開ループ制御を使用することがありえる。一つ以上のコントロール・センターに管理データを送るために、これらのシステムは、Ｒｅｍｏｔｅ　Ｔｅｒｍｉｎａｌ　Ｕｎｉｔｓ（ＲＴＵｓ）を使用する。ＲＴＵのものを配備するＳＣＡＤＡアプリケーションは、流体パイプライン、電気分布および大きい通信システムを備える。ＤＣＳシステムが、広帯域の、低レーテンシ・データ・ネットワークによって、リアルタイムデータ収集および連続制御に関し全般的に使われて、大きなキャンパス工業処理プラント（例えば油およびガス、精製、化学薬品、医薬、食品および飲料、水および廃水、パルプおよび紙、有用性パワーおよび鉱業および金属）において、使われる。ＰＬＣが、より典型的にブールのおよび経時的なロジック・オペレーションおよびタイマーを提供して、連続制御と同様に、しばしば独立型機械およびロボット工学において、使われる。更に、建物、空港、船、宇宙ステーション、など（例えば、モニタして、暖房・換気および空調（ＨＶＡＣ）装置およびエネルギー消費を制御するために）に関し、ＩＣＥおよびＰ

ＡＣシステムが、施設プロセスで使われることがありえる。産業用制御システムが進化するにつれて、新技術はこれらのさまざまなタイプの制御システムの態様を結合している。例えば、ＰＡＣｓは、ＳＣＡＤＡ、ＤＣＳおよびＰＬＣの態様を備えることがありえる。

【発明の概要】

【課題を解決するための手段】

【０００４】

[0004] 制御システムは、電源に電気的に結合される電源および交流（ＡＣ）電源を備える。ＡＣ電源により供給される格納および帰りの電気エネルギ源に関し、無停電電源は、ＡＣ電源に電気的に結合される。無停電電源は、複数の電池モジュールを備える。各電池モジュールは電池セルを備え、バッテリモニタはモニタに電池セルを構成した。各電池モジュールも、電池モジュールに有効に連結するコントローラを備える。コントローラは、電池モジュールから診断情報を受信するように構成される。制御システムも、ＡＣ電源に電気的に接続している制御要素またはサブシステムを備える。電源により供給される電気エネルギが中断されるとき、無停電電源は、制御エレメントまたはサブシステムに電力を供給するように、電気エネルギをＡＣ電源に戻すように構成される。二つ以上の電池モジュール、コントローラ、無停電電源に連結するデバイス、制御システムの動きオリジネータなどの間に認証シーケンスに参加するために、無停電電源は、一つ以上の認証モジュールを包含することもありえる。

【０００５】

[0005] 詳細な説明において、下に更に記載される単純化された様態の概念の選択を導くために、この要約は、提供される。この要約は請求された内容の鍵となる特徴または基本的特徴を確認することを目的としないし、請求された内容の範囲を決定する際の援助として使われることを、それは目的としない。

【０００６】

[0006] 詳細な説明は、添付の図に関して記載される。説明および図の異なる事例の同じ参照番号の使用は、類似または同一のアイテムを示す。

【図面の簡単な説明】

【０００７】

【図１】[0007] 図１は、現在の開示の例示の実施形態による一つ以上の認証モジュールを備える電源を例示しているブロック図である。

【図２】[0008] 図２は、現在の開示の例示の実施形態による産業用制御システムを例示しているブロック図である。

【図３】[0009] 産業用制御システムが複数のソース（例えばパワー格子および一つ以上のローカル・パワー・ジェネレータ）から電力を受信する所で、そして、一つ以上の予備電力供給が現在の開示の例示の実施形態に従って複数の電池モジュールを用いてストアおよび戻る電気エネルギ源に構成される所で、図３は産業用制御システム（例えば図２の産業用制御システム）を例示しているブロック図である。

【図４】[0010] 図４は通信でシステム（例えば図２の産業用制御システム）を有する結合に構成されて、電気エネルギ源（予備電力供給がコントローラおよび複数の電池モジュールを備える）を記憶して、戻すために電源（例えば、図２のパワー格子および／またはローカル・パワー・ジェネレータ）につながるために構成される予備電力供給を例示しているブロック図であり、各電池モジュールは現在の開示の例示の実施形態に従って通信でコントローラに連結するバッテリモニタを有する。

【図５】[0011] 図５は、予備電力供給（例えば図４に図示される予備電力供給）を例示しているブロック図であり、予備電力供給は、通信でシステム（例えば図２の産業用制御システム）を有する結合に構成され、予備電力供給は、現在の開示の例示の実施形態による予備電力供給によって、備えられる複数の電池モジュールの状態に関して情報を有するシステムを提供するために構成されるコントローラを備える。

【図６】[0012] 図６はデバイス（例えば図１および／または他のデバイスで例示される電源）を認証する安全な制御システムの略図であり、例えば、それを、現在の開示の例示

の実施形態に従って、受電デバイスは図１に図示される電源に接続した。
【図７】[0013] 図７は、現在の開示の例示の実施形態に従って産業用制御システム（例えば図６の安全な制御システム）に関しアクション認証経路を例示しているブロック図である。
【図８】[0014] 図８は、現在の開示の例示の実施形態による図７のアクション認証経路を更に例示しているブロック図である。
【図９】[0015]図９は、アクションを認証することに関する方法が現在の開示の実施形態を例示による要求することを示しているフロー図である。
【発明を実施するための形態】
【０００８】
[0016] 産業的な制御システムの設定において、パワーは、ローカル・パワー生成（例えば現場でのタービンおよび／またはディーゼル・パワー・ジェネレータを用いて）を用いてパワー格子（例えばＡＣ本線からの高電圧パワーを使用して）から、オートメーション装置（例えばコントローラ）、入出力（Ｉ／Ｏ）モジュール、などに典型的に供給される。しばしば、予備電力は、電池からこれらの設定のオートメーション装置にも供給される。例えば、例えば、大規模電池ストレージは、鉛酸蓄電池を用いて産業的な設定において、提供されることがありえる。大規模電池ストレージからのパワーは、集中化した、交流現在の（ＡＣ）パワー伝送技術を用いて供給されることがありえる。他の例において、より小さい、分散する直流（ＤＣ）電池電源が、用いられる。例えば、バックアップ・バッテリーパワーは、キャビネット、コントローラ、Ｉ／Ｏモジュールなどのレベルでより小さい鉛酸蓄電池により供給される。しかしながら、より新規な再充電可能電池技術（例えばリチウムイオン電池）と比較されるとき、鉛酸蓄電池は比較的低いエネルギー密度を有する。更に、これらの構成で、バックアップ・バッテリは制御ハードウェアと全般的に別であり、モニタ・バッテリの状態に各電池への別々の接続を必要とする。例えば、かかる電池の動作（例えば、オン／オフ動作の状況）をモニタするために、産業的なオートメーション設定のバックアップ・バッテリは、制御ハードウェアの予備のＩ／Ｏポートに、典型的に接続している。
【０００９】
[0017] モニタリングを容易にするシステムおよび技術は本願明細書において、記載される、および／または、電池の制御は産業用制御システムで設定（例えば無停電電源（ＵＰＳ）装置）を供給する。記載される技術およびシステムは、より高エネルギー密度再充電可能電池技術（例えばリチウムイオン再充電可能電池技術）を用いて実装されることがありえる。開示の実施形態において、産業用ＵＰＳは、通信および／またはセキュリティ機能（例えば双方向性システム通信、制御システム統合、サイバー・セキュリティ統合、など）に供給する。例えば、産業用ＵＰＳは、状態情報、診断情報、信頼性情報、双方向性通信、などを提供する。いくつかの実施形態では、産業用ＵＰＳは、鍵暗号化マイクロコントローラ技術を実装する。
【００１０】
[0018] いくつかの実施形態では、電源は、電源の認証を実行することがありえる回路（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）および／または電源に接続しているデバイスを備える。その特定の電源または電源（例えば、低い電圧供給が高電圧デバイスにプラグインされるという可能性を防止するかまたは最小化する）のタイプによって、用いられることを目的としないデバイスに電源をプラグインすることに関し、これは、可能性を防止することがありえるかまたは最小化することがありえる。例えば、電源が適切なおよび／または所望のデバイスに係合されることを確かめるために、電源は、被結合モジュールを有する「ハンドシェイク」オペレーションを実行する。いくつかの実施形態では、インジケータ（例えば発光ダイオード（ＬＥＤ）インジケータ・ライト）は、この認証の通知を提供するために用いる。例えば、認証（例えばソリッドグロー、グローでない、点滅する、１つの状態に関し１色および他の状態などに関し他の色を使用して）の状態を示すために、多色ＬＥＤまたは単一の色ＬＥＤは、診

断情報を提供する。

【００１１】

[0019] いくつかの実施形態では、他のデバイス（例えば電源からパワーを受信する機器）を認証するために、電源は、用いることがありえる。例えば、電源回路は、受電デバイス、一種の受電デバイス、受電デバイスの製造業者、などを認証するために用いることがありえる。このように、産業的なオートメーション設定の偽の装置の使用は、防止されることがありえるかまたは最小化されることがありえる。更に、電源は、装置（例えばコントローラ、入出力（Ｉ／Ｏ）モジュール、端デバイス、フィールド・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）など）にそれ自体を認証するために用いることがありえる。いくつかの実施形態では、電源に接続している電源とデバイスの間に、電源は、暗号の通信を促進する。例えば、電源は、電源と端デバイス、フィールド・デバイス、などの間に双方向性暗号の通信を提供することがありえる。更に、実施形態によっては、オペレータは、フィールド・デバイス（例えばセンサ、アクチュエータまたは他のいかなる機器も）に関する認証情報を得るためにネットワークに接続している電源を使用することがありえる。いくつかの実施形態では、予定の時間および／または他のあらかじめ定義されたイベントで、新規なデバイスが、スタートアップ／リセットで、周期的に取り付けられる認証シーケンス（例えば、「ハンドシェイク」）を実行するために、2以上の認証モジュール（例えば、第１の認証モジュールおよび２台目の認証モジュール）は、構成される。認証モジュールが他のデバイスおよび／または互いを認証することに失敗するべきであるならば、デバイス（例えば、証明されてないデバイス）の少なくとも１台は部分的に、または、完全に使用不能でありえておよび／または他のデバイスと通信するのを制限されることがありえる。

【００１２】

[0020] 産業用制御システムにおいて、さまざまな産業的なエレメント／サブシステム（例えば、入出力モジュール、パワー・モジュール、フィールド・デバイス、スイッチ、ワークステーションおよび／または物理的な相互接続デバイス）は、制御要素／サブシステム（例えば、一つ以上の通信／制御モジュール）により制御されるかまたは駆動される。オペレータインタフェース（例えば、ＳＣＡＤＡまたは人間の機械インタフェース（ＨＭＩ）、エンジニアリング・インタフェース、ローカル・アプリケーション、リモート・アプリケーションなど（必ずしもこれらに限られない）のようなアクションオリジネータから、例えば受信されるが、プログラミングおよびアクション要求（例えば、実行可能ソフトウェア・モジュール、制御コマンド、データ要求、など）に従って、制御要素／サブシステムは、機能する。複数のアクションオリジネータがいる所で、産業用制御システムはデータおよび／または規制への無許可の接近に弱くありえる。更に、破壊工作ソフト、スパイウェアまたは最新版、アプリケーション画像、制御コマンド、等の形で送信されることがありえる他の不正な／悪意のあるソフトウェアに、産業用制御システムは、弱くてもよい。有効なログインまたは表面上有効な（例えば、大幅に削られる）アプリケーションまたはオペレータ／エンジニアリング・インタフェースを介して、発明されることがありえる悪意のある行為者または意図せずに未許可のリクエスト／コマンドからさえシステムを得るのに、単にオペレータを認証することは、十分ではなくてもよい。

【００１３】

[0021] 本開示は、産業用制御システムにおいて許可されていないアクション要求が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。オペレーションの所与の選択、或いは、すべてのオペレータ・アクションおよび／または他のアクションもしくは要求は、アクション発起元(action originator)から産業エレメント／コントローラ（例えば、通信／制御モジュール、入出力（Ｉ／Ｏ）モジュール、パワー・モジュール、フィールド・デバイス、スイッチ、ワークステーション、物理相互接続デバイス等）までの認証経路を介してセキュア化することができる。実装態様において、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たアクション要求に署名することを、アクション認証器に求める。未署名のアクション要求は、自動的にエラーという結果

となり、産業エレメント／コントローラにより処理または実行されないことになる。産業エレメント／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確実性を検査し、署名されたアクション要求の確実性が検査されたときに、要求された動作を実行するように構成することができる。このようにいて、悪意のあるまたは許可されていないアクション要求は処理されず、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許可されていない変更、データに対する許可されていないアクセスなどから保護することができる。

例示の実装態様

[0022] 図１～図６を全般的に参照する。例示の電源１２０を本開示に従って説明する。いくつかの実施形態では、電源１２０は、電源１２０に接続されるデバイス（例えば、（例えば、図１に示される）Ｉ／Ｏモジュール１０２、制御モジュール１０４など）に対し、電源１２０および／または電源１２０の１つ以上の電池モジュール１２２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を備える。認証モジュール１３４はまた、電源１２０に接続される１つ以上のデバイスを認証するのに使用することができる。いくつかの実施形態では、認証モジュール１３４は、電源１２０に関連づけられるユニークの識別子１３６および／またはセキュリティ証明書１３８を記憶する（例えば、図５に示されるように、認証モジュールは、プロセッサ１４０と、１つ以上のユニーク識別子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、を備える。）。認証モジュール１３４は、認証に基づいて、電源１２０に接続されるデバイスに対する接続を確立および／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、オペレータに対し）認証を示すインジケータ（例えば、インジケータ・ライト１４４）を含むこともできる。

【００１４】

[0023] いくつかの実施形態では、電源１２０は、警報モジュール１４６を備える。開示の実施形態において、電源１２０に接続している電源１２０および／またはデバイスに関し条件の状態および／またはセットが満たされるとき、（例えば、オペレータに対する）警報を提供するために、警報モジュール１４６は構成される。例えば、電源１２０の認証または電源に接続しているデバイスが得られておよび／または故障するときに、警報は認証モジュール１３４により生成されて、警報モジュール１４６により提供される。例えば、電源１２０が適切なおよび／または所望のデバイスに係合されることを確かめるために、電源１２０は、被結合受電デバイス（例えば、Ｉ／Ｏモジュール１０２および／または制御モジュール１０４）を有する「ハンドシェイク」オペレーションを実行する。そうでない場合には、警報モジュール１４６は、オペレータ（例えば、ネットワークを介して）に警告するために用いることがありえる。いくつかの実施形態では、警報は、電子メールの形でオペレータに提供される。他の実施態様において、警報は、テキストメッセージの形でオペレータに提供される。しかしながら、これらの警報は、例証として提供されて、現在の開示を制限するはずでない。他の実施態様において、異なる警報は、オペレータに提供される。更に、条件が認証プロシージャ（例えば、電子メールおよびテキストメッセージなど）に関し満たされるときに、複数の警報はオペレータに提供されることがありえる。また、パワー電源故障、電池モジュール故障、接続される装置故障、電源および／または受電デバイスに関しさまざまなエラー条件などを包含する（しかし、必ずしもこれに限らない）警報が他の条件に関し認証モジュール１３４および／または警報モジュール１４６により提供されることがありえることは注意すべきである。

【００１５】

[0024] 電源１２０に接続している電源１２０と一つ以上のデバイスの間に通信を暗号化するために、認証モジュール１３４は、構成されることもありえる。図１に示すように、電源１２０は、暗号化モジュール１４８を備えることがありえる。例えば、一つ以上の暗号のプロトコルは、電源１２０と受電デバイスの間に情報を送信するために用いる。かかる暗号のプロトコルの例は、例えばトランスポート層セキュリティ（ＴＬＳ）プロトコル、安全なソケット層（ＳＳＬ）プロトコルなどを備えるが、それらに限定されない。例

えば、電源１２０と受電デバイス間の通信はＨＴＴＰ安全なプロトコル（ＨＴＴＰＳ）を使用することがありえ、ＨＴＴＰプロトコルはＳＳＬおよび／またはＴＬＳプロトコルに階層化される。

【００１６】

[0025] いくつかの実施形態では、電源１２０に接続している電源１２０とデバイスの間に、認証シーケンスが実行されることがありえる。例えば、コントローラ１２８の認証モジュール１３４を用いた認証シーケンスを実行することによって、電源１２０は、被結合入出力装置１０２、制御モジュール１０４などを認証する。他の実施態様において、電源１２０に接続しているデバイスは、電源１２０を認証することがありえる。例えば、コントローラ１２８の認証モジュール１３４を有する認証シーケンスを実行することによって、制御モジュール１０４は、被結合電源１２０を認証する。更なる実施形態において、１つの電源１２０は、他の電源１２０を認証することがありえる。例えば、第１の電源１２０のコントローラ１２８の第１の認証モジュール１３４と第２の電源１２０のコントローラ１２８の第２の認証モジュール１３４の間に認証シーケンスを実行することによって、第１の電源１２０は、第２の（例えば、冗長な）電動電源１２０を認証する。いくつかの実施形態では、第２の電源１２０は、第１の電源１２０を認証することもありえる。

【００１７】

[0026] プロセッサ１４０およびメモリ１４２がコントローラ１２８（例えば、図１に関して）の一部としていくつかの特性により記載されると共に、この構成が例証として提供されて、現在の開示を制限するはずでない点に留意する必要がある。かくして、電池モジュール１２２の一つ以上は、プロセッサ、メモリ、など（例えば、コントローラ１２８で備えられるプロセッサ１４０およびメモリ１４２に加えて、または、それの代わりに）を備えることもありえる。このような実施形態では、電池モジュール１２２の一つ以上は、一つ以上の認証モジュール１３４を備えることがありえ、例えば、一つ以上の他のデバイス（例えば、他の電池モジュール１２２、コントローラ１２８、制御要素またはサブシステム、など）に電池モジュール１２２を認証しておよび／または電源１２０に連結する他のデバイス（例えば、他の電池モジュール１２２、コントローラ１２８、制御要素またはサブシステム、など）を認証するために、認証モジュール１３４は、プロセッサおよびメモリ（おそらく格納一つ以上のキー、証明書、ユニーク識別子、セキュリティ証明書、など）を使用する。

【００１８】

[0027] いくつかの実施形態では、電池モジュール１２２は、電源１２０および／または接続される装置（例えば電源１２０に連結する受電デバイス）のコントローラ１２８を認証することがありえる。例えば、電池モジュール１２２の認証モジュール１３４を用いた認証シーケンスを実行することによって、電池モジュール１２２は、電源１２０および／または被結合入出力装置１０２、制御モジュール１０４、などのコントローラ１２８を認証する。他の実施態様において、電源１２０に接続している受電デバイスは、電池モジュール１２２の一つ以上を認証することがありえる。例えば、それぞれの電池モジュール１２２の認証モジュール１３４を有する認証シーケンスを実行することによって、制御モジュール１０４は、被接続電源１２０の一つ以上の（例えば、各々）電池モジュール１２２を認証する。

【００１９】

[0028] いくつかの実施形態では、コントローラ１２８は、電池モジュール１２２の一つ以上を認証することがありえる。例えば、コントローラ１２８の認証モジュール１３４とそれぞれの電池モジュール１２２の認証モジュール１３４の間に認証シーケンスを実行することによって、コントローラ１２８は、一つ以上の電池モジュール１２２を認証する。更なる実施形態において、ある電池モジュール１２２は、他の電池モジュール１２２を認証することがありえる。例えば、第１の電池モジュール１２２の第１の認証モジュール１３４と第２の電池モジュール１２２の第２の認証モジュール１３４の間に認証シーケンスを実行することによって、第１の電池モジュール１２２は、第２の電池モジュール１２

２を認証する。いくつかの実施形態では、第２の電池モジュール１２２は、第１の電池モジュール１２２を認証することもありえる。

【００２０】

[0001] 電源１２０が、産業用制御システムで使われることがありえる。例えば、図２に関して、例示の産業用制御システム１００は、現在の開示に従って記載される。実施形態において、産業用制御システム１００は産業用制御システム（ＩＣＳ）、プログラム可能なオートメーション・コントローラ（ＰＡＣ）、管理制御およびデータ収集（ＳＣＡＤＡ）システムを含むことができる。そして、分散制御システム（ＤＣＳ）、プログラマブル論理コントローラ（ＰＬＣ）および産業安全システムが安全基準（例えばＩＥＣ１５０８等）に保証される。制御要素またはサブシステムを備える分散制御システムを実装するために、産業用制御システム１００は通信制御アーキテクチャを使用する。ここで、システムの全体にわたって割り当てられる一つ以上のコントローラによって、サブシステムは制御される。例えば、一つ以上のＩ／Ｏモジュール１０２は、一つ以上の制御モジュール１０４に接続している。産業用制御システム１００は、Ｉ／Ｏモジュール１０２へ／から伝達するデータに構成される。Ｉ／Ｏモジュール１０２は、入力モジュール、出力モジュールおよび／または入出力モジュールを含むことがありえる。例えば、入力モジュールはその過程で入力センサから情報を受信するために用いることがありえる。その一方で、出力モジュールが出力アクチュエータに伝達する命令に用いられることがありえる。例えば、Ｉ／Ｏモジュール１０４は、ガス工場、精練所、などに関し配管の圧力を測定することに関しプロセス・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）に接続していることがありえ、および／またはアクチュエータ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、モーター、ソレノイド、電気的スイッチ、送信機、等）をプロセスに接続した。

【００２１】

[0029] 実装において、システムを制御して、例えば、製造、パワー生成、製作および精製、インフラ・プロセス、処理および配布、廃水収集および処理に給水にかかるもの、油およびガスパイプライン、送電および配布（風力発電所および大きい通信システム）、建物、空港、船および宇宙ステーション（例えば、暖房・換気および空調（ＨＶＡＣ）装置およびエネルギー消費をモニタし、制御するために）に関し施設プロセス、大きなキャンパス工業処理プラント（例えば油およびガス、精製、化学薬品、医薬、食品および飲料、水および廃水、パルプおよび紙、有用性パワー、鉱業、金属）、および／または重要なインフラのような工業処理（しかし、これらに限定されない）を備えているアプリケーションのデータを集めるために、自我／Ｏモジュール１０２は、用いることがありえる。

【００２２】

[0030] 実装において、（例えばＡ／Ｄ変換器（ＡＤＣ）回路などを用いて）センサ１０６からデジタルデータまで受信されるアナログ・データを変換するために、Ｉ／Ｏモジュール１０２は、構成されることがありえる。Ｉ／Ｏモジュール１０２は、アクチュエータ１０８に接続していることもありえ、アクチュエータ１０８（例えば速度、トルクなど）の一つ以上の機能している特性を制御するために構成されることもありえる。更に、Ｉ／Ｏモジュール１０２は、アクチュエータ１０８（例えばＡ／Ｄ変換器（ＤＡＣ）回路などを用いて）に、アナログの送信のためのデータに共垂直線デジタルデータに構成されることがありえる。実装において、Ｉ／Ｏモジュール１０２の一つ以上は、通信下位バス（例えばイーサネット（登録商標）・バス、Ｈ１フィールド・バス、Ｐｒｏｃｅｓｓ Ｆｉｅｌｄ Ｂｕｓ（ＰＲＯＦＩＢＵＳ）、ハイウェーＡｄｄｒｅｓｓａｂｌｅ Ｒｅｍｏｔｅ Ｔｒａｎｓｄｕｃｅｒ（ＨＡＲＴ）バス、Ｍｏｄｂｕｓなど）を介して通信することに関し構成される通信モジュールから成ることがありえる。更に、2以上のＩ／Ｏモジュール１０２は、通信下位バスに関しフォールト・トレラントおよび冗長な接続を提供するために用いることがありえる。

【００２３】

[0031] あるＩ／Ｏモジュール１０２と他のＩ／Ｏモジュール１０２を区別することに

関し、各Ｉ／Ｏモジュール１０２は、ユニーク識別子（ＩＤ）により提供されることがありえる。実装において、それが産業用制御システム１００に接続するときに、Ｉ／Ｏモジュール１０２はそのＩＤにより確認される。複数のＩ／Ｏモジュール１０２は、産業用制御システム１００で冗長性を提供するために用いることがありえる。例えば、2以上のＩ／Ｏモジュール１０２は、センサ１０６および／またはアクチュエータ１０８に接続していることがありえる。各Ｉ／Ｏモジュール１０２は、Ｉ／Ｏモジュール１０２（例えば印刷回路基板（ＰＣＢ）など）で備えられるハードウェアおよび回路への物理的な接続に供給する一つ以上のポートを備えることがありえる。

【００２４】

[0032] ワイド領域セルラ電話ネットワーク（例えばモバイル通信（ＧＳＭ）ネットワークに関し３Ｇセルラー電話網、４Ｇのセルラー電話網またはＧｌｏｂａｌシステム）、無線コンピュータ通信ネットワーク（例えばＷｉ－Ｆｉネットワーク（例えば、ＩＥＥＥ８０２．１１ネットワーク標準を使用して機能する無線ＬＡＮ（ＷＬＡＮ、パーソナルエリアネットワーク（ＰＡＮ）（例えば、ＩＥＥＥ８０２．１５ネットワーク標準を使用して機能したＷｉｒｅｌｅｓｓＰＡＮ（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、インターネットなどを含むが必ずしもこれに限られない他のネットワークに接続することに関し、Ｉ／Ｏモジュール１０２の一つ以上は、インタフェースを備えることがありえる。更に、Ｉ／Ｏモジュール１０２をコンピュータバスなどに接続することに関し、Ｉ／Ｏモジュール１０２の一つ以上は、接続を備えることがありえる。

【００２５】

[0033] Ｉ／Ｏモジュール１０２をモニタして、制御して、一緒に2以上のＩ／Ｏモジュール１０２を接続するために、制御モジュール１０４は、用いることがありえる。開示の実施形態において、Ｉ／Ｏモジュール１０２に関し固有ＩＤに基づく産業用制御システム１００にＩ／Ｏモジュール１０２が接続するときに、制御モジュール１０４はルーティング・テーブルを更新することがありえる。更に、複数の冗長なＩ／Ｏモジュール１０２が用いられるときに、データがＩ／Ｏモジュール１０２から受信されておよび／またはそれに発信されるにつれて、各制御モジュール１０４はＩ／Ｏモジュール１０２に関して情報のデータベースのミラーリングを実装することがありえて、それらを更新することがありえる。いくつかの実装において、2以上の制御モジュール１０４は、冗長性を提供するために用いる。付加的なセキュリティに関して、スタートアップ、リセット、新規な制御モジュール１０４の取付け、制御モジュール１０４の置換、周期的に、予定の時間など（ただし、これらに限定されない）を包含しているあらかじめ定義されたイベントまたは時間に互いを認証するために認証シーケンスまたは握手を実行するために、制御モジュール１０４は、構成されることがありえる。更に、ランダムな（例えば、疑似乱数の）時間間隔で認証を実行するために、制御モジュール１０４は、構成されることがありえる。

【００２６】

[0034] 産業用制御システム１００により送信されるデータはパケット化でありえる、すなわち、データの別々の部分はネットワーク制御情報、などとともにピン部から成るデータパケットに変換されることがありえる。産業用制御システム１００はデータ伝送に関し一つ以上のプロトコルを使用することがありえる。そして、ビットを指向する同期データリンク層プロトコル、例えばＨｉｇｈ－Ｌｅｖｅｌデータリンク制御、ＨＤＬＣを包含する。いくつかの実施形態では、産業用制御システム１００は、標準の国際標準化機構（ＩＳＯ）１３２３９等に従ってＨＤＬＣを実装する。更に、2以上の制御モジュール１０４は、冗長なＨＤＬＣを実装するために用いることがありえる。しかしながら、ＨＤＬＣが例えば提供されて、現在の開示で拘束性のはずでない点に留意する必要がある。かくして、産業用制御システム１００は、現在の開示に従って他のさまざまな通信プロトコルを使用することがありえる。

【００２７】

[0035] モニタリングに関し情報を使用するコンポーネントと交換しておよび／または

Ｉ／Ｏモジュール１０２（例えば一つ以上の制御ループ・フィードバック機構／コントローラ）を介して産業用制御システム１００に接続している計装を制御することに関し、制御モジュール１０４の一つ以上は、構成されることがありえる。実装において、コントローラは、マイクロコントローラ／Ｐｒｏｇｒａｍｍａｂｌｅ Ｌｏｇｉｃ Ｃｏｎｔｒｏｌｌｅｒ（ＰＬＣ）、Ｐｒｏｐｏｒｔｉｏｎａｌ－Ｉｎｔｅｇｒａｌ－Ｄｅｒｉｖａｔｉｖｅ（ＰＩＤ）コントローラなどとして構成されることがありえる。開示の実施形態において、例えば、ネットワーク１１０を介して一つ以上のＩ／Ｏモジュール１０２を一つ以上のコントローラに接続するために、Ｉ／Ｏモジュール１０２および制御モジュール１０４は、ネットワーク・インターフェースを備える。実装において、Ｉ／Ｏモジュール１０２をローカル・エリア・ネットワーク（ＬＡＮ）に接続することに関しギガビットイーサネット（登録商標）・インタフェースとして、ネットワーク・インターフェースは、構成されることがありえる。更に、2以上の制御モジュール１０４は、冗長なギガビットイーサネット（登録商標）を実装するために用いることがありえる。

【００２８】

[0036] しかしながら、ギガビットイーサネット（登録商標）が例えば提供されて、現在の開示で拘束性のはずでない点に留意する必要がある。かくして、制御モジュール１０４をワイド領域セルラ電話ネットワーク（例えば３Ｇセルラー電話網、４Ｇのセルラー電話網またはＧＳＭネットワーク）、無線コンピュータ通信ネットワーク（例えばＷｉ－Ｆｉネットワーク（例えば、ＩＥＥＥ８０２．１１ネットワーク標準を使用して機能したＷＬＡＮ）、ＰＡＮ（例えば、ＩＥＥＥ８０２．１５ネットワーク標準を使用して機能したＷＰＡＮ）、ＷＡＮ、イントラネット、エクストラネット、インターネット、などの（ただし、これらに限定されない）さまざまなネットワークに接続することに関し、ネットワーク・インターフェースは、構成されることがありえる。加えて、ネットワーク・インターフェースは、コンピュータバスを使用して実装されることがありえる。例えば、ネットワーク・インターフェースは、Ｐｅｒｉｐｈｅｒａｌ Ｃｏｍｐｏｎｅｎｔ Ｉｎｔｅｒｃｏｎｎｅｃｔ（ＰＣＩ）カードインターフェース（例えばミニＰＣＩインターフェイスなど）を備えることがありえる。更に、異なるアクセス・ポイント全体の単一のネットワークまたは複数のネットワークを備えるために、ネットワーク１１０は、構成されることがありえる。

【００２９】

[0037] 図３を次に参照する。産業用制御システム１００は、複数のソースから電力を受信することができる。例えば、ＡＣ電力は、（例えば、ＡＣ本線からの高電圧電源を使用して）送電網(power grid)１１２から供給される。ＡＣ電力は、ローカル発電（例えば、現場でのタービンまたはディーゼル・ローカル発電機１１４）を使用して供給されることもできる。電源１１６は、送電網１１２から産業用制御システム１００のオートメーション装置（例えばコントローラ、Ｉ／Ｏモジュール、など）に向けて電力を配電するために使用される。他の電源１１８は、ローカル発電機１１４からオートメーション装置まで電力を配電するために使用される。産業用制御システム１００はまた、複数の電池モジュール１２２を用いてＤＣ電力を特電および放電するように構成される追加（バックアップ）電源１２０を含む。例えば、電源１２０は、ＵＰＳとして機能する。本開示の実施形態において、複数の電源１１６、１１８、および／または１２０は、産業用制御システム１００内で分散される（例えば、物理的に集中させない(decentralized)。）。

【００３０】

[0038] いくつかの実施形態では、一つ以上のパワーは１１６、１１８を供給する、および／または、１２０はキャビネットのレベルで提供される。例えば、１つの電源１２０は、制御モジュール１０４およびその付随するＩ／Ｏモジュール１０２に予備電力を提供するために用いる。他の実施態様において、１つの電源１２０は制御モジュール１０４に予備電力を提供するために用いる。そして、付随するＩ／Ｏモジュール１０２（例えば、Ｉ／Ｏモジュール１０２および制御モジュール１０４が施設の範囲内でいくつかの距離によって、物理的に分離されるところ、電気的絶縁がＩ／Ｏモジュール１０２と制御モジュ

ール１０４、などの間に維持されるところ）に予備電力を提供するために、他の電源１２０は用いる。

【００３１】

[0039] パワーは１１６、１１８を供給する、および／または、パワー・フィールド・デバイス（例えば図２に関して記載されるセンサ１０６および／またはアクチュエータ１０８）に、１２０は構成されることもありえる。例えば、アクチュエータ１０８（例えば、アクチュエータ１０８がＤＣモーターまたは他のＤＣアクチュエータである実装で）に伝送に関しＡＣ（例えば、ＡＣ本線により供給されるように）をＤＣに変換することに関し、電源１１６および１１８の一つ以上は、ＤＣに対するＡＣ（ＡＣ／ＤＣ）コンバータを備える。更に、冗長性を提供するために用いる2以上の電源１１６、１１８および／または１２０は、各電源１２０に関し別々の（冗長な）パワー・バックプレーンを用いた産業用制御システム１００のオートメーション装置に接続していることがありえる。

【００３２】

[0040] 図４を参照する。電源１２０は、複数の電池モジュール１２２を備える。開示の実施形態において、各電池モジュール１２２は、リチウムイオン電池セル１２４を含む。例えば、電池モジュール１２２は、１および１／２ボルト（１．５ Ｖ）のリチウムイオン電池セル、３ボルト（３ Ｖ）のリチウムイオン電池セル、などを用いて実装される。いくつかの実施形態では、電源１２０は、一緒に積み重なる８～１０の電池モジュール１２２を備える。しかしながら、多くの８～１０の電池モジュール１２２は、例えば提供されて、現在の開示を制限するはずでない。他の実施態様において、８足らずまたは１０以上の電池モジュール１２２は、一緒に積み重なる。

【００３３】

[0041] 更に、電池モジュール１２２がリチウムイオン電池セル１２４を備えるとして記載されるにもかかわらず、現在の開示のシステムおよび技術が、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、リチウム鉄のリン酸塩電池、リチウム―チタン酸塩電池、亜鉛臭化物電池、バナジウム・レドックス電池、ナトリウム―硫黄電池、熱した塩電池、銀―酸化物電池などを含むが必ずしもこれに限らず他の再充電可能電池、ストレージおよび／またはアキュムレータ技術を使用することがありえる点に留意する必要がある。

【００３４】

[0042] 電池モジュール１２０の各々はリアルタイム・バッテリモニタ１２６を備え、例えば、印刷回路基板（ＰＣＢ）を用いて実装されることがありえる。開示の実施形態において、バッテリモニタ１２６は、電池セル１２４を作動するコントローラ１２８（例えば、マイクロコントローラ）により用いられる。例えば、各バッテリモニタ１２６は、コントローラ１２８に各電池セル１２４に関し診断情報を提供する。診断情報は、電池セル１２４、電池セル１２４（例えば、アンペアの）の操作の流れ、電池セル１２４（例えば、クーロンの）への電荷のユニット、電池セル１２４（例えば、クーロンの）からの電荷のユニット、電池セル１２４（例えば、充電／放電サイクルなどの数において、時間を単位にする）ができてからの年数など（ただしこれらに限定されない）の操作の電圧を包含する。

【００３５】

[0043] いくつかの実施形態では、各バッテリモニタ１２６は、コントローラ１２８に別々接続している。他の実施態様において、複数のバッテリモニタ１２６は、コントローラ１２８に接続して、共有通信チャネル（例えば直列バス）に接続している。パワー調節装置１３０（例えば、トランスを備える）に、バッテリモニタ１２６も接続している。そして、それは外部電源（例えば電源１１６および／または電源１１８）から電力を受信する。パワー調節装置１３０から供給される電気エネルギ源を使用して、電池セル１２４は、荷電される。電気エネルギ源は他のパワー調節装置１３２を用いたバッテリ・セル１２

４から排出される。そして、電池セル１２４（例えば電圧）により供給される電気エネルギ源の一つ以上の出力特性を調整するために、それは用いることがありえる。

【００３６】

[0044] 開示の実施形態において、各電池モジュール１２２は、ホイルで包まれた電池セル１２４を有する支持フレームを備える。ここでは、複数の支持フレームは、電池セル１２４が封止を維持するように積み重ねることができる一方で、ホイル内で電池セル１２４の膨張および収縮を許容する。開示の実施形態において、また、バッテリモニタ１２６を備えるＰＣＢは、支持フレームにおいて電池セル１２４によってエンケースされる。更に、ＰＣＢは、電池セル１２４によって、電力が供給され、各電池セル１２４に向かう、および各電池セル１２４から出る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、電子信号切換デバイス（例えば、アナログスイッチにより直列に接続される２つの電界効果トランジスタ（ＦＥＴ）を備え、バッテリモニタ１２６からの許可なしで、エネルギが電池に蓄電され、および／または電池から放電されるのを防止する。このようにして、電池セル１２４のターミナルが予想外の（例えば、短絡された）電気径路に接続されるときに、電池セル１２４への電気接続は防止される。更に、バッテリモニタ１２６が非アクティブであるとき（例えば、電池セル１２４の充電がないときに）に、電池セル１２４への電気接続は防止される。この例では、電池モジュール１２２は、それらが電源１２０に挿入されるときに、少なくとも部分的に充電される。

【００３７】

[0045] 開示の実施形態において、電池モジュール１２２は、各支持フレームに配置されている電気的接触（例えば、電気コネクタ）を使用して積み重なって、接続される。電気コネクタは、電池セル１２４（例えば、バッテリモニタＰＣＢを経た）に電気的に接続していて、支持フレーム（さもなければ電池セル１２４へのはんだ付けされた接続を必要とする）から伸びているワイヤのない支持フレームに配置されていることがありえる。例えば、他の支持フレーム（例えば、他の支持フレームの底面に配置されている）上の対応するスナップフィット電気コネクタと嵌合する１つの支持フレーム（例えば、支持フレームの上面に配置されている）に、スナップフィット電気コネクタは、提供される。電気コネクタの間にコンタクトの表面積を増加させておよび／または電気コネクタ（例えば、他の電気コネクタへの挿入に関し一部の１つの電気コネクタを構成することによって、）の自動配列を提供するために、電気コネクタは、構成されることがありえる。

【００３８】

[0046] 開示の実施形態において、複数の電池モジュール１２２が予想外の方法で一緒に接続されるのを防止するように、電気コネクタは、幾何学的に調整される（例えば、大きさを設定されて配置した。）。例えば、１つの電気的接触は支持フレームに関して上方へ全般的に正しい位置に置かれることがありえる。その一方で、他の電気的接触は支持フレームに関して下方へ全般的に正しい位置に置かれることがありえる。他の実施態様において、２つの電池モジュール１２２（例えば、色分け、表示など）を整列配置することに関し、ビジュアル・キューは、提供される。

【００３９】

[0047] 更に、電池モジュール１２２に関し機械の登録を提供する（例えば一つの電池モジュール１２２の電気コネクタを他の電池モジュール１２２の嵌合用電気コネクタでおよび／または電源１２０に対する電気コネクタで合わせることに関しに）ために、電源１２０は、スロット、チャネル、トラックなどを備えることがありえる。例えば、電池モジュール１２２は、電源１２０のハウジングのそれぞれのトラックおよびハウジングに関する電池モジュール１２２の提供している配列への挿入に関し構成されるタブまたはポストを備える。更に、独自に特定の配列において、および／または電源１２０のハウジングに関する特定位置で被結合各電池モジュール１２２を確認するために、コントローラ１２８は、ユニークな物理的な身分証明（ＩＤ）を各電池モジュール１２２と関連させることがありえる。

【００４０】

[0048] 開示の実施形態において、電源１２０は、取付キャビネット、取付ラック、取付壁などに関し組み立てられる。電源１２０のハウジングは剛性、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）の中で組み立てられることがありえる。そして、さもなければ電池セル故障が生じた場合リリースされるエネルギーを含むために、それは用いることがありえる。更に、ハウジングは、（電池故障のため放出されることができる）リチウムのような化学電池セル・コンポーネントを含み、または少なくとも実質的含むようめに構成されることがありえる。加えて、電源１２０に含まれるコンポーネントは、互いから電気的に絶縁されることがありえる。例えば、コントローラ１２８に対する信号は、バッテリモニタ１２６および電池セル１２４から直流電気よって分離される。更に、コントローラ128及び電源レギュレータ130は、電気的および/またはバッテリモジュール122及び電力調整器132から絶縁された漏電である（例えば別々のトランス、光アイソレータ、などを用いて）。

【００４１】

[0049] 図５を次に参照すると、コントローラ１２８は、産業用制御システム１００（例えば、ネットワーク１１０を介して）に接続している。開示の実施形態において、コントローラ１２８は、コントローラ・レベルでおよび／または各電池モジュール１２２のレベルでセキュリティおよび／または診断法を実装する。コントローラ１２８は、そのコンポーネントの一部もしくは全部を備えて、計算機制御中で作動することがありえる。例えば、ソフトウェア、ファームウェア、ハードウェア（例えば、固定ロジック回路）、手動処理またはそれらの組み合わせを用いて本願明細書において、記載されるコントローラ１２８のコンポーネントおよび関数を制御するために、プロセッサ１４０は、コントローラ１２８で、または、それにおいて、備えられることがありえる。本明細書で用いられる用語「コントローラ」、「機能」、「サービス」および「ロジック」は、コントローラ１２８を制御することに関連して、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、ファームウェアまたはハードウェアの組合せを全般的に表す。ソフトウェア実装の場合、プロセッサ（例えば、中央演算処理装置（ＣＰＵ）またはＣＰＵ）に実行されるときに、指定された作業を遂行するプログラムコードを、モジュール、機能またはロジックは表す。プログラムコードは、一つ以上のコンピュータ読取可能メモリ・デバイス（例えば、内部メモリーおよび／または一つ以上の有形媒体）などに記憶されることがありえる。様々なプロセッサを有している様々な商業的な計算プラットフォームに、本願明細書において、記載される構造、関数、アプローチおよび技術は、実装されることがありえる。

【００４２】

[0050] プロセッサ１４０はコントローラ１２８に関し処理機能を提供して、いかなる数のプロセッサ、マイクロ・コントローラまたは他の演算処理システムを備えることがありえる。そして、格納データおよび他の情報に関しレジデントまたは外部メモリがコントローラ１２８によって、アクセスされるかまたは生成される。プロセッサ１４０は、本願明細書において、記載される技術を実装する一つ以上のソフトウェア・プログラムを実行することがありえる。プロセッサ１４０は、それが形成される材料または、そこにおいて、使用される処理機構により制限されなくて、このように、半導体および／またはトランジスタ（例えば電子集積回路（ＩＣ）コンポーネントを用いて）、などを介して実装されることがありえる。

【００４３】

[0051] コントローラ１２８も、メモリ１４２を備える。本願明細書において、記載される機能を実行するために、メモリ１４２は、コントローラ１２８（例えばソフトウェア・プログラムおよび／またはコード部分またはプロセッサ１４０およびおそらくコントローラ１２８の他のコンポーネントに指示する他のデータ）のオペレーションと関連したさまざまなデータを記憶するために、ストレージ機能を提供する、有形の、コンピュータ可読のストレージ媒体の例示である。かくして、メモリ１４２は、データ（例えばパワー電源１２０（そのコンポーネントを備える）を作動することに関し命令のプログラム、など

）を記憶することがありえる。開示の実施形態において、メモリ１４２は、電源１２０に関しユニーク識別子１３６および／またはセキュリティ証明書１３８を記憶することがありえる。単一のメモリ１４２が記載されると共に、メモリ（例えば、有形の、非一時的なメモリ）の多種多様なタイプおよび組合せが使用されることがありえる点に留意する必要がある。メモリ１４２は、プロセッサ１４０とともに要素を成すことがありえるか、独立型メモリから成ることがありえるか、または、両方の組合せでありえる。メモリ１４２は、着脱可能および取り外し不可能なメモリ・コンポーネント（例えばランダムアクセス・メモリ（ＲＡＭ）、読出し専用メモリ（ＲＯＭ）、フラッシュ・メモリ（例えば、安全なデジタル（ＳＤ）メモリ・カード、ミニＳＤメモリ・カードおよび／またはｍｉｃｒｏＳＤメモリ・カード）、磁気メモリ、光メモリー、汎用直列バス（ＵＳＢ）メモリ・デバイス、堅いディスクメモリ、外部メモリなど）（ただしこれらに限定されない）を包含することがありえる。実装において、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）メモリを備えることがありえる。そして、例えば、それをメモリは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）などにより提供される。

【００４４】

[0052] コントローラ１２８は、通信インタフェース１５０を備える。電源１２０のコンポーネントと通信するために、通信インタフェース１５０は、有効に構成される。例えば、通信インタフェース１５０はコントローラ１２８のストレージに関し伝達するデータに構成されることがありえる、コントローラ１２８、などのストレージからデータを検索する。電源１２０のコンポーネントとプロセッサ１４０間のデータ転送（例えば、通信でコントローラ１２８および／または通信出力に連結するデバイスから通信でコントローラ１２８（例えばバッテリモニタ１２６）に連結するデバイスまで受信されるプロセッサ１４０への通信入力に関し）を容易にするために、通信インタフェース１５０は、プロセッサ１４０にも通信で連結する。例えば、プロセッサを複数のバッテリモニタ１２６に接続するために、通信インタフェース１５０は、共有通信チャネル（例えば直列バス）を使用して実装される。

【００４５】

[0053] 開示の実施形態において、コントローラ１２８は、バッテリモニタ１２６を有する双方向通信に関し構成される。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、電池セル１２４に関する状態情報および／または信頼性情報）を集める。コントローラ１２８も、例えば、記憶する電池モジュール１２２および電源１１６、電源１１８、などから供給される戻る電気エネルギ源に指示している電池モジュール１２２を作動する。通信インタフェース１５０がコントローラ１２８のコンポーネントとして記載されると共に、有線のおよび／またはワイヤレス接続を介して通信でコントローラ１２８に連結する外部のコンポーネントとして、通信インタフェース１５０の一つ以上のコンポーネントが実装されることがありえる点に留意する必要がある。コントローラ１２８は、ディスプレイ、マウスなどを含むが必ずしもこれに限らずデバイス（例えば、通信インタフェース１５０を介して）から成ることもありえておよび／または一つ以上の入出力（Ｉ／Ｏ）に接続することもありえる。例えば、コントローラ１２８は表示装置（例えば多色（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）に接続していることがありえる。そして、それは電源１２０の状態を示すことがありえる。

【００４６】

[0054] ワイドな領域セルラ電話ネットワーク（例えば３Ｇセルラー電話網、４Ｇのセルラー電話網またはＧＳＭ（ＧＳＭ）ネットワーク）、無線コンピュータ通信ネットワーク（例えばＷｉＦｉネットワーク（例えば、ＩＥＥＥ８０２．１１ネットワーク標準を使用して機能した無線ＬＡＮ（ＷＬＡＮ、インターネット、ワイド・エリア・ネットワーク（ＷＡＮ）、ローカル・エリア・ネットワーク（ＬＡＮ）、個人領域ネットワーク（ＰＡＮ）（例えば、ＩＥＥＥ８０２．１５ネットワーク標準を使用して機能した無線個人領域

ネットワーク（ＷＰＡＮ）、公共電話網、エクストラネット、イントラネット、など。を含むが必ずしもこれに限らず、様々な異なるネットワーク１１０と通信するために、通信インタフェース１５０および／またはプロセッサ１４０は、構成されることがありえる。しかしながら、このリストは、例示だけであり、現在の開示を制限するものではない。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されることがありえる。例えば、通信インタフェース１５０は、ＰＣＩカードインターフェース（例えばミニＰＣＩインターフェイスなど）を備えることがありえる。更に、異なるアクセス・ポイント全体の単一のネットワーク１１０または複数のネットワークと通信するために、通信インタフェース１５０は構成されることがありえる。このように、コントローラ１２８は、通信で電源１２０を産業用制御システム１００に連結するために用いる。

【００４７】

[0055] 図６を次に参照すると、制御要素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、など）は、一つ以上のバックプレーンによって、一緒に接続される。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に接続していることがありえる。更に、電源１２０は、Ｉ／Ｏモジュール１０２におよび／またはパワー・バックプレーン１５４による制御モジュール１０４に接続していることがありえる。開示の実施形態において、物理的な相互接続デバイス（例えば、限定的ではないがアメリカ非仮特許出願の出願番号１４／４４６，４１２に記載されるそれらのようなスイッチ、コネクタまたはケーブル）は、Ｉ／Ｏモジュール１０２、制御モジュール１０４、電源１２０およびおそらく他の産業用制御システム装置に接続するために用いる。例えば、ケーブルは制御モジュール１０４をネットワーク１１０に接続するために用いる、他のケーブルは電源１１６をパワー格子１１２に接続するために用いる、他のケーブルは電源１１８をローカル・パワー・ジェネレータ１１４、などに接続するために用いる。

【００４８】

[0056] 開示の実施形態において、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。例えば、産業用制御システム１００は、セキュリティ証明書ソース（例えば、工場１５６）およびセキュリティ証明書メーカー（例えば、キー管理実体１５８）を備える。固有のセキュリティ証明書（例えば、キー、証明書など（例えばユニーク識別子１３６および／またはセキュリティ証明書１３８）を生成するために、工場１５６は、構成される。供給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（例えば、複数の電池モジュール１２２および／またはコントローラ１２８の一つ以上を備える）に、キー管理実体１５８は、工場１５６によって、固有のセキュリティ証明書を生成して構成される。例えば、Ｉ／Ｏモジュール１０２および合同電源１２０は、ユニークなセキュリティ証明書によって、各々配給されることがありえる。

【００４９】

[0057] それから、産業用制御システム１００で実装される制御要素またはサブシステムを認証することに関し認証プロセスは、ユニークな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、ユニークなセキュリティ証明書（例えば、認証プロセスに基づく）に基づいて二方向に互いと通信するように、制御モジュール１０４および電源１２０は、操作可能である。更に、本願明細書において、開示される安全な産業用制御システム１００で、産業用制御システム１００の複数の（例えば、全て）レベルでセキュリティを提供することに関し、産業用制御システム１００の複数の（例えば、あらゆる）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、電源、物理的な相互接続デバイスなど）は、セキュリティ証明書により配給される。またさらに、エレメントは、製造（例えば、出生時）の間、ユニークなセキュリティ証明書（例えば、キー、証明書など）により配給されることがありえて、産業用制御システム１００の安全を進めることに関し、産業用制御システム１００のキー管理実体によって、出生から管理されることがありえる。

【００５０】
[0058] いくつかの実施形態では、コンポーネント（例えば、電源１２０）と物理的な相互接続の間に認証の実装に関しデバイス（例えば、ケーブル組立体）がそのコンポーネントに接続していることができる物理的な相互接続デバイス（例えば、１－ワイヤ暗号化チップ）に接続しているかまたはそれにおいて、備えられるコントローラを用いて、制御要素またはサブシステムは、接続される。例えば、安全な暗号化された技術がそうであることがありえるマイクロプロセッサは、ケーブルにアセンブリを構築して、産業用制御システム１００の特定の成分にキーを操作した。そのケーブル組立体と関係があるために構成されないコンポーネントにユーザがケーブル組立体を設置する（例えば、プラグインする）ときに、この構成は産業用制御システム１００に関しセキュリティを提供する。実施形態において、１－ワイヤ・シリアル・キー（例えば、１－ワイヤ組込形キー）は、一つ以上において、実装する（例えば、各々の）物理的な相互接続デバイス。
【００５１】
[0059] 開示の実施形態において、産業用制御システム１００のエレメントおよび／または物理的な相互接続デバイス（例えば、ケーブル組立体）間の通信は、認証プロセスを備える。産業用制御システム１００で実装されるエレメントおよび／または物理的な相互接続デバイスを認証することに関し、認証プロセスは、実行されることがありえる。実装において、そのエレメントおよび／または物理的な相互接続デバイスを認証することに関し、認証プロセスは、エレメントおよび／または物理的な相互接続デバイスと関連したセキュリティ証明書を利用することがありえる。例えば、セキュリティ証明書は、暗号化キー、証明書（例えば、公開鍵証明書、デジタル証明書、アイデンティティ証明書、セキュリティ証明書、非対称の証明書、標準証明書、非標準証明書）および／または識別番号を備えることがありえる。実施形態において、産業用制御システム１００のコンポーネントおよび／または物理的な相互接続デバイスで備えられておよび／またはそれに接続しているコントローラ（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ことに関し構成されることがありえる。
【００５２】
[0060] 実装において、システム１００がそうである産業的な制御の複数の制御要素またはサブシステム（例えば、エレメントおよび／または物理的な相互接続デバイス）は、それらの自分のものによって、ユニークなセキュリティ証明書に配給した。例えば、エレメントが製造される（例えば、個々のものはキーの中でセット、そして、証明書はエレメントの出生で定められる）ときに、産業用制御システム１００の各エレメントは証明書、暗号化キーおよび／または識別番号のそれ自身のユニークなセットにより配給される。証明書、暗号化キーおよび／または識別番号のセットは、強い暗号化を提供して／サポートすることに関し構成される。暗号化キーは、標準（例えば、在庫品の（ＣＯＴＳ）コマーシャル）暗号化アルゴリズム（例えば国家安全保障局（ＮＳＡ）アルゴリズム、国立標準技術研究所（ＮＩＳＴ）アルゴリズム、等）により実装されることがありえる。
【００５３】
[0061] いくつかの実施形態では、例えば、認証モジュールのＳＲＡＭで、暗号鍵および証明書は、オンチップ・メモリ（ＯＣＭ）に記憶されることがありえる。加えて、感受性が高い作業（例えば、秘密情報を有する。そして、時々広報を有するさえ作業）は、それがＯＣＭにおいて、実行するスタックを有することができる。例えば、暗号の作業は、地元にＯＣＭに記憶されるスタックから、カーネル空間またはアプリケーション空間において、遂行されることができる。
【００５４】
[0062] 認証プロセスの結果に基づいて、認証されているエレメントは活性化されることがありえる、エレメントの部分的な機能は産業用制御システム１００の範囲内で使用可能または使用不可にされることがありえる、エレメントの完全な機能は産業用制御システム１００の範囲内で許可されることがありえる、および／または、産業用制御システム１００の範囲内のエレメントの機能は完全に使用不能でありえる（例えば、産業用制御シス

テム１００のそのエレメントと他のエレメントの間に促進される通信でない）。

【００５５】

[0063] 実施形態において、産業用制御システム１００のエレメントと関連したキー、証明書および／または識別番号は、そのエレメントのオリジナルの装置製造業者（ＯＥＭ）を特定することがありえる。本明細書において、デバイス（例えば、エレメント）および／またはデバイス（例えばデバイスを物理的な製造業者から購入して、デバイスを販売する実体）の供給元を物理的に製造する実体として、用語「相手先商標製造会社」または「ＯＥＭ」は、定義されることがありえる。かくして、実施形態で、物理的な製造業者およびデバイスの供給元であるＯＥＭによって、デバイスは、製造および供給されることがありえる（販売される）。しかしながら、他の実施形態では、デバイスは、供給元であるＯＥＭによって、割り当てられることがありえるが、物理的な製造業者でない。このような実施形態では、ＯＥＭは、デバイスに物理的な製造業者によって、製造させられることがありえる（例えばＯＥＭ缶購入、契約、オーダーなどで、ある物理的な製造業者からデバイス）。

【００５６】

[0064] 加えて、ＯＥＭがデバイスの物理的な製造者でない供給元から成る所で、デバイスは物理的な製造業者のブランドの代わりに供給元のブランドを支持することがありえる。例えば、エレメント（例えば、電源１２０）が物理的な製造業者でなく供給元である特定のＯＥＭを伴う実施形態で、エレメントのキー、証明書および／または識別番号は、その起源を特定することがありえる。産業用制御システム１００のエレメントの認証の間、判定がそれをされるときに、産業用制御システム１００の一つ以上の他のエレメントのＯＥＭとは異なる実体によって、認証されているエレメントは製造されたかまたは出力された、そして、そのエレメントの機能は産業用制御システム１００の範囲内で少なくとも部分的に使用不能でありえる。例えば、限定は産業用制御システム１００のそのエレメントと他のエレメントの間に通信（例えば、データ転送）に置かれることがありえる。そうすると、エレメントは働くことができなくて／産業用制御システム１００の範囲内で機能することができない。産業用制御システム１００のエレメントの１つが置換を必要とするときに、知らずに非同種のエレメント（例えば、産業用制御システム１００の残りのエレメントより異なる起源（異なるＯＥＭ）を有しているエレメント）にエレメントを置き換えて、産業用制御システム１００のエレメントを実装するのを、この特徴は産業用制御システム１００のユーザが防止することがありえる。このように、本願明細書において、記載される技術は、安全な産業用制御システム１００に、他のＯＥＭのエレメントの置換を防止することがありえる。ある例では、始まっているＯＥＭにより提供されるエレメントの代わりに、同程度の機能性に供給するエレメントの置換は防止されることがありえる。これは、次のことの故である。置換されたエレメントは始まっているＯＥＭのシステムを認証することができなくて、それの範囲内で機能した。他の例では、エレメントが始まっているＯＥＭによって、物理的および暗号ラベルの中でセット第１を有して、第１の再販業者は提供されることがありえる。そして、第１の再販業者のエレメントは産業用制御システム１００に取り付けられることがありえる。この例では、エレメントがＯＥＭを発明している同じことによって、物理的および暗号ラベルの中でセット１秒（例えば、異なる）を有して、２人目の再販業者は、提供されることがありえる。この例では、第2の再販業者のエレメントは産業用制御システム１００の範囲内で機能するのを防止されることができる。これは、次のことの故である。それらは第１の再販業者のエレメントを認証することができなくて、それによって、機能した。しかしながら、また、第１の再販業者および第2の再販業者が双方の合意を結ぶことができることは注意すべきである。ここで、同じ産業用制御システム１００を認証して、それの範囲内で作動するために、第１および第２のエレメントは構成されることがありえる。更に、実施形態によっては、合意が特定の顧客、顧客のグループ、施設などに適用するだけであるように、相互運用を許容する再販業者間の合意は実装されることもありえる

[0065] 他の事例において、ユーザは、産業用制御システム１００の範囲内で誤って指

定された（例えば、ミスマーク）エレメントを実装することを試みることがありえる。例えば、エレメントが産業用制御システム１００の他のエレメントのＯＥＭと同じＯＥＭを伴うことを、不正に示すそれにマークされる物理的な表示を、ミス著しいエレメントは、有することがありえる。かかる事例において、産業的な制御システム１００により実装される認証プロセスは、エレメントが偽であるという警報を出されるユーザを生じさせる。このプロセスは産業用制御システム１００に関し改良された保安を促進することもありえる。これは、次のことの故である。偽のエレメントはしばしば、悪意のあるソフトウェアが産業用制御システム１００にもたらされることがありえる車両である。実施形態において、認証プロセスは産業用制御システム１００に関し安全なエアギャップを提供する。そして、安全な産業用制御システムが不安定なネットワークから物理的に分離されることを確実にする。

【００５７】

[0066] 暗号法の暗号鍵（例えば、暗号化キー）を管理することに関し、キー管理実体１５８は、構成されることがありえる。この暗号鍵（例えば、キー管理）を管理することは、キーの生成、交換、ストレージ、使用および／または置換を備えることがありえる。例えば、キー管理実体１５８はセキュリティ証明書ソースとして役立つために構成される。そして、産業用制御システム１００のエレメントに関しユニークなセキュリティ証明書（例えば、治安証明書、秘密のセキュリティ証明書）を生成する。キー管理は、ユーザおよび／またはシステム・レベル（例えば、ユーザまたはシステム間のどちらか）でキーに関係する。

【００５８】

[0067] 実施形態において、キー管理実体１５８は、安全な実体（例えば安全な施設に位置決めされる実体）から成る。キー管理実体１５８は、Ｉ／Ｏモジュール１０２、制御モジュール１０４およびネットワーク１１０から遠隔で位置決めされることがありえる。例えば、ファイアウォール１６０は、キー管理実体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、コーポレート・ネットワーク）から分離することがありえる。実装において、ルールセットに基づいて、ファイアウォール１６０は、データパケットを分析して、データパケットが許されるべきかどうか決定することによって、徹底的なおよび出て行くネットワーク・トラフィックを制御するソフトウェア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でありえる。ファイアウォール１６０は、固定されているとみなされなくて、信頼される（例えば、雲および／またはインターネット）信頼された、安全な内部ネットワーク（例えば、ネットワーク１１０）と他のネットワーク１６２の間の障壁をかくしてもたらす。実施形態において、ファイアウォール１６０は、キー管理実体１５８と制御要素またはサブシステムまたはネットワークの一つ以上の間に選択的な（例えば、安全な）通信に関し、１１０を許容する。例示のにおいて、一つ以上のファイアウォールは、産業用制御システム１００の範囲内でさまざまな位置で実装されることがありえる。例えば、ファイアウォールは、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集積されることがありえる。

【００５９】

[0068] 記載されるように、安全な産業用制御システム１００は一つ以上の製造存在物（例えば、工場１５６）を更に備えることがありえる。工場１５６は、産業用制御システム１００のエレメントに関し、オリジナルの装置製造業者（ＯＥＭ）と関係していることがありえる。キー管理実体１５８は、ネットワーク（例えば、クラウド）を介して、製造実体に通信で連結することがありえる。実装において、産業用制御システム１００のエレメントが一つ以上の工場１５６で製造されるときに、（例えば、暗号化された通信パイプラインを有することがありえる）エレメントに、キー管理実体１５８は通信で連結することがありえる。製造の際にセキュリティ証明書（例えば、キー、証明書および／または識別番号をエレメントに挿入する）を有するエレメントに配給することに関し、キー管理実体１５８は、通信パイプラインを利用することがありえる。

【００６０】

[0069] 更に、エレメントが使用（例えば、活性化される）に入れられるときに、キー管理実体１５８は世界的に個々のエレメントに通信で連結することがありえて（例えば、暗号化された通信パイプラインを介して）、特定のコードの使用を確認することがありえて、署名することがありえて、いかなる特定のコードの使用も無効にすることがありえて（例えば、取り除く）、および／または、いかなる特定のコードの使用も可能にすることがありえる。かくして、エレメントが最初は製造される（例えば、生まれる）工場で、キー管理実体１５８は各エレメントと通信することがありえる。そうすると、エレメントは管理されたキーで支えられる。産業用制御システム１００の各エレメントに関しすべての暗号化キー、証明書および／または識別番号を備えているマスタデータベースおよび／またはテーブルは、キー管理実体１５８により維持されることがありえる。キー管理実体１５８は、エレメントとのその通信によって、キーを無効にすることに関し構成される。それによって、コンポーネントの窃盗および再利用に対処する認証メカニズムの能力を進める。

【００６１】

[0070] 実装において、キー管理実体１５８は、他のネットワーク（例えば、雲および／またはインターネット）およびファイアウォールで制御要素およびサブシステムの一つ以上および／またはネットワーク１１０に通信で連結することがありえる。例えば、実施形態で、キー管理実体１５８は、集中化したシステムまたは分散処理システムでありえる。そのうえ、実施形態で、キー管理実体１５８は、局所的に、または、遠隔で管理されることがありえる。いくつかの実装において、（例えば、統合された）ネットワーク１１０または制御要素またはサブシステムの範囲内で、キー管理実体１５８は、位置決めされることがありえる。キー管理実体１５８は、管理を提供することがありえておよび／またはさまざまな方法で管理されることがありえる。例えば、キー管理実体１５８は、実装されることがありえて／管理されることがありえる：中央位置の顧客によって、個々の工場位置の顧客によって、外部の第三者管理会社によって、および／または産業的なものの異なる層の顧客によって、そして、層によって、異なる位置で、システム１００を制御する。

【００６２】

[0071] セキュリティ（例えば、計測可能な、ユーザを構成された量のセキュリティ）の様々なレベルは、認証プロセスにより提供されることがありえる。例えば、エレメントを認証して、エレメントの範囲内でコードを保護するベースは、セキュリティで水平に提供されることがありえる。セキュリティの他の層は、同様に加えられることがありえる。例えば、コンポーネント（例えば電源１２０）が適当な認証が発生しなくて強化することができないかかる程度に、セキュリティは、実装されることがありえる。実装において、エレメント（証明書（例えば、キーおよび証明書）がエレメントに実装されるという保証）で、コードの暗号化は、実装される。セキュリティは、産業用制御システム１００によって、割り当てられることがありえる（例えば、フロー）。例えば、セキュリティはエンドユーザにずっと産業用制御システム１００の中を流れることがありえる。そして、モジュールがその事例において、何を制御するように設計されているかについて、その人は知っている。実施形態において、認証プロセスは、暗号化（安全な通信に関し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構成要素（例えば、デジタル署名を介して）の認証）を提供する。

【００６３】

[0072] 実装において、異なる製造業者／ベンダー／供給元（例えば、ＯＥＭ）により製造されておよび／または供給されるエレメントの安全な産業用制御システム１００の範囲内でインターオペラビリティを提供しておよび／または可能にするために、認証プロセスは、実装されることがありえる。例えば、異なる製造業者／ベンダー／供給元により製造されておよび／または供給されるエレメント間の選択的な（例えば、少し）インターオペラビリティは、許可されることがありえる。実施形態において、認証の間、実装されるユニークなセキュリティ証明書（例えば、キー）は階層を形成することがありえる。それによって、異なる関数が産業用制御システム１００の異なるエレメントにより実行される

のを許す。

【００６４】

[0073] そこにおいて、配置されて（例えば、射出しておよび／または押し込んだ）、産業用制御システム１００のコンポーネントを接続している通信リンクはデータパケット（例えばラントパケット（例えば、６４バイトより小さいパケット）を更に使用することがありえる。そして、セキュリティの加算レベルを提供する。外側の情報（例えば、悪意のあるコンテンツ（例えば虚偽のメッセージ、破壊工作ソフト（ウイルス）、データマイニング・アプリケーションなど）が通信リンク上に射出されることがありえる問題点のレベルを、runt packet（ラントパケット）の使用は、上昇させる。例えば、通信リンク上に悪意のあるコンテンツを射出する外部の実体の能力を妨げるために制御モジュール１０４と電源１２０の間に送信されるデータパケット間のギャップの範囲内で、ラントパケットは、通信リンク上に射出されることがありえる。

【００６５】

[0074] 開示の実施形態において、認証シーケンスを開始するために、第２の認証モジュール（例えば、電源１２０、電源１２０のコントローラ１２８、電源１２０の電池モジュール１２２、制御要素またはサブシステム（例えば入出力装置１０２、制御モジュール１０４、など）において、備えられる）に、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の電池モジュール１２２、制御要素またはサブシステム（例えば入出力装置１０２、制御モジュール１０４、など）において、備えられる）がそうである第１の認証は、伝送するためにリクエスト・データグラムを構成した。実装において、リクエスト・データグラムは第１のプレーンテキスト目下（ＮｏｎｃｅＡ）を備える。そして、第一装置認証キー証明書（ＣｅｒｔＤＡＫＡ）が第一装置認証キー（ＤＡＫＡ）および第１のアイデンティティ属性証明書（ＩＡＣＡ）を含む。いくつかの実施形態では、本当の乱数発生器（以下「ＴＲＮＧ」）を有する第１の目下（ＮｏｎｃｅＡ）を生成して、リクエスト・データグラムを生成するために第１の目下（ＮｏｎｃｅＡ）、第一装置認証キー証明書（ＣｅｒｔＤＡＫＡ）および第１のアイデンティティ属性証明書（ＩＡＣＡ）を連結するかまたは結合するために、第１の認証モジュールは、構成される。いくつかの実施形態では、第一装置認証キー証明書（ＣｅｒｔＤＡＫＡ）および第１のアイデンティティ属性証明書（ＩＡＣＡ）は、第１の認証モジュールによって、地元に記憶される。例えば、証明書は、第１の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なストレージ媒体）に記憶されることができる。

【００６６】

[0075] 第一装置認証キー証明書（ＣｅｒｔＤＡＫＡ）およびデバイス・ライフサイクルｍａｎａｇｅｍｅｎｔｓシステム（ＤＬＭ）により生成されるかまたは暗号のライブラリ関数を利用して得られる公開鍵を有する第１のアイデンティティ属性証明書（ＩＡＣＡ）を検査することによって、リクエスト・データグラムを確認するために、第２の認証モジュールは、構成される。この点に関しては、公開鍵が、ＳＲＡＭまたは認証モジュールの他のローカルメモリに記憶されることができて、検査する暗号のライブラリ関数によって、用いられることが可能であるかまたは暗号によって、交換されたデータ（例えば認証モジュールの間で交換されるｎｏｎｃｅｓ）に署名されることができる。いくつかの実施形態では、第２の認証モジュールは、楕円カーブ・デジタル署名アルゴリズム（以下「ＥＣＤＳＡ」）または他の確認オペレーションを有する証明書を検査できる。いくつかの実施形態では、以下を検査することによって、プレーンテキスト値から証明書値を確認するために、第２の認証モジュールは、更に構成されることができ、証明書タイプは、各証明書、ＩＡＣ名マッチ、ＤＡＫ証明書モジュール・タイプ・マッチ・モジュール・タイプ引数、および／または、ペイロードが各々に適合させるというメッセージの各証明書のマイクロプロセッサ直列数（以下「ＭＰＳＮ」）に関しデバイス認証キー（以下「ＤＡＫ」）またはアイデンティティ属性証明書（以下「ＩＡＣ」）である。いくつかの実施形態では、第２の認証モジュールはＤＡＫを検査するために更に構成されることができ、そして、

ローカル取り消しリスト（例えば、無効にされたおよび／または無効な証明書を備えているリストまたはデータベース）において、ＩＡＣ証明書はない。第２の認証モジュールがリクエスト・データグラムを確認することに失敗するときに、第２の認証モジュールがエラー・メッセージを生成できるか、部分的にまたは完全に第１の認証モジュールを無効にして、および／または、第１の認証モジュールに出入りする通信を中断するかまたは制限する。

【００６７】

[0076] 有効なリクエスト・データグラムに応答して、反応データグラムを第１の認証モジュールに発信するために、第2の認証モジュールは、構成される。実装において、反応データグラムが第２のプレーンテキスト目下（ＮｏｎｃｅＢ）を備えること、第１および第２のｎｏｎｃｅｓと関係している第一のシグニチャー（ＳｉｇＢ［ＮｏｎｃｅＡ｜｜ＮｏｎｃｅＢ］）、第２のデバイス認証キー（ＤＡＫＢ）を含んでいる第２のデバイス認証キー証明書（ｃｅｒｔＤＡＫＢ）および第２のアイデンティティ属性証明書（ＩＡＣＢ）。いくつかの実施形態では、ＴＲＮＧを有する第２の目下（ＮｏｎｃｅＢ）を生成して、第１の目下（ＮｏｎｃｅＡ）および第２の目下（ＮｏｎｃｅＢ）を連結するかまたは結合して、２台目の認証モジュールによって、地元に記憶されるプライベートな鍵（例えば、ＤＡＫ）を有する連結された／複合ｎｏｎｃｅｓに署名するために、第２の認証モジュールは、構成される。第２の目下（ＮｏｎｃｅＢ）を連結するかまたは結合するために構成されて、モジュールが更にある第２の認証、第１および第２のｎｏｎｃｅｓと関係している第一のシグニチャー（ＳｉｇＢ［ＮｏｎｃｅＡ｜｜ＮｏｎｃｅＢ］）、第２のデバイス認証キー証明書（ｃｅｒｔＤＡＫＢ）および反応データグラムを生成する第２のアイデンティティ属性証明書（ＩＡＣＢ）。いくつかの実施形態では、第２のデバイス認証キー証明書（ＣｅｒｔＤＡＫＢ）および第２のアイデンティティ属性証明書（ＩＡＣＢ）は、第２の認証モジュールによって、地元に記憶される。例えば、証明書は、第２の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なストレージ媒体）に記憶されることができる。

【００６８】

[0077] 第２のデバイス認証キー証明書（ＣｅｒｔＤＡＫＢ）および地元に記憶されるかまたはＥＣＤＳＡまたは他の確認オペレーションを利用している暗号のライブラリから取り出される公開鍵を有する第２のアイデンティティ属性証明書（ＩＡＣＢ）を検査することによって、反応データグラムを確認するために、第１の認証モジュールは、構成される。いくつかの実施形態では、以下を検査することによって、プレーンテキスト値から証明書値を確認するために、第１の認証モジュールは、更に構成されることができる：すなわち、証明書がＭＰＳＮｓに適合させて有するＩＡＣ及びＤＡＫ、ＩＡＣはマッチを挙げる、タイプが両方とも正しい証明書は認定する（ＩＡＣ及びＤＡＫ）、正しい発行人名は両方の証明書にある、ＤＡＫモジュール・タイプは正しいタイプ（例えば、通信／制御モジュール）である。いくつかの実施形態では、第１の認証モジュールはＤＡＫを検査するために更に構成されることができる。そして、ＩＡＣ証明書はローカル取り消しリストにおいて、ない。

【００６９】

[0078] 反応データグラムを確認する、第１および第２のｎｏｎｃｅｓを伴う第１のシグニチャーを検査するために、第１の認証モジュールは、更に構成される（ｓｉｇＢ［ＮｏｎｃｅＡ｜｜ＮｏｎｃｅＢ］）。いくつかの実施形態では、第１の認証モジュールは、第１のシグニチャーを検査するために構成される（ｓｉｇＢ［ＮｏｎｃｅＡ｜｜ＮｏｎｃｅＢ］）第２の認証モジュールから受信される第１のローカルに格納される目下（ＮｏｎｃｅＡ）および第２の元の文目下（ＮｏｎｃｅＢ）を連結することによって、第１の暗号化署名を検査する（ｓｉｇＢ［ＮｏｎｃｅＡ｜｜ＮｏｎｃｅＢ］）一般のデバイス認証キー（例えばｃｅｒｔＤＡＫＢからＤＡＫＢを用いて）および第１の目下および第２の目下の局所的に生成された連結を第１の目下および第２の目下の暗号により検査された連結と比較するを有する。第１の認証モジュールが反応データグラムを確認することに失敗する

ときに、第１の認証モジュールがエラー・メッセージを生成できるか、部分的にまたは完全に第２の認証モジュールを無効にして、および／または、第２の認証モジュールに出入りする通信を中断するかまたは制限する。

【００７０】

[0079] 反応データグラムが有効であるときに、認証データグラムを第2の認証モジュールに発信するために、第１の認証モジュールは更に構成される。実装において、認証データグラムは、第１および第２のｎｏｎｃｅｓを伴う第２のシグニチャーを備える（ｓｉｇＡ［ＮｏｎｃｅＡ｜｜ＮｏｎｃｅＢ］）。実施形態によっては、第１および第２ ｎｏｎｃｅｓめの局所的に生成された第１の認証モジュールによって、地元に記憶されるプライベートな鍵（例えば、ＤＡＫ）と署名するために、第１の認証モジュールは、構成される。反応データグラムが無効であるときに、第２の目下およびエラーを報告しているメッセージ（例えば、「失敗」）と関連したシグニチャーを備えている「失敗した」認証データグラムと、認証データグラムは、置き換えられることが可能である（ｓｉｇＡ［ＮｏｎｃｅＢ｜｜Ｅｒｒｏｒ］）第１の認証モジュールによって、生成する。

【００７１】

[0080] 認証データグラムに応答して、応答する認証データグラムを第１の認証モジュールに発信するために、第2の認証モジュールは、更に構成されることができる。実装において、応答する認証データグラムは、第１の目下およびエラーを報告しているメッセージ（例えば、「成功」または「失敗」）と関連したシグニチャーを備える（ｓｉｇＢ［ＮｏｎｃｅＡ｜｜Ｅｒｒｏｒ］）第２の認証モジュールによって、生成する。いくつかの実施形態では、第１および第２のｎｏｎｃｅｓを伴う第２のシグニチャーを検査することによって、認証データグラムを確認するために、第２の認証モジュールは、構成される（ｓｉｇＡ［ＮｏｎｃｅＡ｜｜ＮｏｎｃｅＢ］）。いくつかの実施形態では、第２の認証モジュールは、第２のシグニチャーを検査するために構成される（ｓｉｇＡ［ＮｏｎｃｅＡ｜｜ＮｏｎｃｅＢ］）第１の認証モジュールおよび第２のローカルに格納される目下（ＮｏｎｃｅＢ）から受信される第１の元の文目下（ＮｏｎｃｅＡ）を連結することによって、第２の暗号化署名を検査する（ｓｉｇＡ［ＮｏｎｃｅＡ｜｜ＮｏｎｃｅＢ］）一般のデバイス認証キー（例えばｃｅｒｔＤＡＫＡからＤＡＫＡを用いて）および第１の目下および第２の目下の局所的に生成された連結を第１の目下および第２の目下の暗号により検査された連結と比較するを有する。メッセージを報告しているエラーに加えて、第2の認証モジュールが認証データグラムを確認することに失敗するときに、第2の認証モジュールは部分的に、または、完全に第１の認証モジュールを無効にすることができて、および／または第１の認証モジュールに出入りする通信を中断できるかまたは制限できる。

【００７２】

[0081] 認証モジュールを使用しているデバイスが「マスター・スレーブ」構成に従って配置される実装において、マスター（例えば、第１の認証モジュール）は、各スレーブを認証するために構成されることができる。失敗した認証が生じた場合、マスターは、証明されてないスレーブに出入りする通信を少なくとも部分的に抑制できるかまたは制限できる。別の実施形態として、マスターなしで平行に機能している2以上のスレイブモジュールは互いを認証できる。ここで、部分的に、または、完全に使用不能になっている両方のデバイスに、失敗した認証は結果としてなる。例えば、2以上の冗長な電源１２０は、使用不能でありえるそれらが、正常に起動時に認証シーケンスまたは他のあらかじめ定義された時間／イベントを完了することを失敗するべきである。

【００７３】

[0082] 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エレメント／コントローラ２０６は、アクション発起元２０２からの要求／命令に従って少なくとも部分的に動作することができる。実装態様において、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および／またはＨＭＩ）、エディタ２１２およびコンパイラ２１４を含むエンジニアリング・インタフェース２１０、ローカル・アプリケーション２２０、並びに、リモート・アプリケーション２１６（例えば

、ローカル・アプリケーション２２０を介してネットワーク２１８を通じて通信する。）などである。図７および８に示される認証経路２００において、産業エレメント／コントローラ２０６（例えば、電源１２０）は、アクション要求（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・アップデート、設定されるポイントの制御やアプリケーション画像ダウンロード等を求める要求）がアクション認証器２０４により署名および／または暗号化されているときにだけ、当該アクション要求を処理する。このことは、有効なユーザ・プロファイルからの許可されていないアクション要求を防止し、更に、無効な（例えば、ハッキングされた）プロフィルから入来する許可されていないアクション要求からシステムをセキュア化する。

【００７４】

[0083] 開示の実施形態において、アクション証人２０４は、現場でアクション・オリジネータ２０２（例えば、直接被接続デバイス・ライフサイクル管理システム（ＤＬＭ）２２２または固定されたワークステーション２２６）といることがありえるかまたは遠隔で位置決めすることがありえる（例えば、ネットワーク２１８を介して接続されるＤＬＭ２２２）。一般に、その上に記憶されるプライベートなキーおよび署名しておよび／またはリクエストがプライベートなキーのアクション・オリジネータ２０２によって、生成したアクションを暗号化するために構成されるプロセッサを有するストレージ媒体を、アクション認証メッセージ２０４は、備える。標準オペレータ・ログインを経てアクセスされることができないメモリに、プライベートな鍵は、記憶される。例えば、固定されたワークステーション２２６は、アクセスに関し物理的なキー、携帯用の暗号化デバイス（例えば、スマートなカード、ＲＦＩＤタグ等）および／または生物測定入力を必要とすることがありえる。

【００７５】

[0084] いくつかの実施形態では、アクション認証メッセージ２０４は、携帯用の暗号化デバイス、例えばスマートなカード２２４、固定されたマイクロプロセッサを備えることがありえるを備える。このように、アクションオリジネータ２０２のインタフェースへの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、全デバイス（それとともに通信の個人的に格納されたキーおよびプロセッサを包含する）は、担持されることがありえる。アクション認証ノード２０４が固定されたか締められてないワークステーションを介して認証経路２００に接近するかどうか、携帯用の暗号化デバイス（例えば、潜在的により安全でないワークステーションまたはクラウド・ベースの建築を使用することと、は対照的に）の構造の範囲内で、アクションオリジネータ２０２からのアクションリクエストは確実に署名されることがありえておよび／または暗号化されることがありえる。例示のとして、アクションオリジネータ２０２を経て送られるいかなるアクション要求も認証することが可能である前に、未許可の人は、スマートなカード２２４の所有を物理的にとらなければならない。

【００７６】

[0085] いくつかの実施形態では、セキュリティの多層は、使用されることがありえる。例えば、アクション認証メッセージ２０４は、サインだけにアクセス可能でもよい固定されたワークステーション２２６を備えることがありえておよび／または２２４がアクセスするスマートなカードを介して、アクション要求を暗号化することがありえる。加えて、固定されたワークステーション２２６は、生物測定であるか多元的な暗号デバイス２２８（例えば、一つ以上の指紋スキャナ、虹彩スキャナ、顔認識デバイス、など）を介してアクセス可能でもよい。実施形態によっては、スマートなカード２２４または他の携帯用の暗号化デバイスがアクションリクエストに署名することを可能にする前に、多元的な暗号デバイス２２８は、有効な生物測定入力を必要とすることがありえる。

【００７７】

[0086] 署名されたアクションリクエストの確実性が検査されるときに、署名されたアクションリクエストを受信して、署名されたアクションリクエストの確実性を検査して、要請された動作を実行するために、アクションオリジネータ２０２により駆動されている

電源１２０または他のいかなる産業エレメント／コントローラ２０６も構成される。実施形態によっては、産業エレメント／コントローラ２０６（例えば、電源１２０）は、アクションリクエスト（例えば、アクションオリジネータによって、送られるアプリケーション画像、制御コマンドまたは他のいかなるデータも）を記憶するために構成されるストレージ媒体（例えば、ＳＤ／ｍｉｃｒｏＳＤカード、ＨＤＤ、ＳＳＤまたは他のいかなる非一時的なストレージ・デバイスも）（例えば、電源１２０のメモリ１４２）を備える。シグニチャーが検査されたあと、アクションリクエスト（すなわち、要請された動作を実行する）を実行して／実行するプロセッサ（例えば、電源１２０のプロセッサ１４０）を、産業エレメント／コントローラ２０６は、更に備える。実施形態によっては、要請された動作が実行されることがありえる前に、アクションリクエストはアクション・オリジネータ２０２またはアクション認証メッセージ２０４によって、暗号化されて、プロセッサ１４０によっても解読されなければならない。実装において、アクションリクエスト・シグニチャーが検査されたあとだけ、プロセッサ１４０が要請された動作を実行することを可能にする仮想キースイッチ２３４（例えば、プロセッサ１４０で動いているソフトウェア・モジュール）を、産業エレメント／コントローラ２０６は備える、および／または、アクションの後、リクエストは解読される。いくつかの実施形態では、産業エレメント／コントローラ２０６に動く前に、重要なアクションの選択のどの作用もまたは各一つは、認証経路を掃除しなければならない。

【００７８】

[0087] 産業用制御システムのアクションリクエストを認証することに関し、例示の実施形態に従って、図９は、プロセス３００を表す。実装において、産業用制御システム１００（例えば、図１～６に関して記載されるように）および／または産業用制御システム１００の認証経路２００（例えば、図７および８に関して記載されるように）によって、プロセス３００は、明らかにされることがありえる。アクションリクエストは、始められる（ブロック３１０）。例えば、オペレータ／エンジニアリング・インタフェース２０８／２１０および／または遠隔／ローカル・アプリケーション・インタフェース２１６／２２０が生成するためおよびアクションリクエストに用いられる。それから、アクションリクエストは、アクション認証メッセージ（ブロック３２０）により署名される。例えば、アクション証人２０４は、アクションリクエストに署名するために用いる。実施形態によっては、アクションリクエストは、アクション認証メッセージ（ブロック３２２）によって、暗号化されることがありえる。それから、署名されたアクションリクエストは、産業エレメント／コントローラ（ブロック３３０）に送信される（例えば、ダウンロードされる）。例えば、アクションリクエストは、産業エレメント／コントローラ２０６（例えば、電源１２０に）に供給される。次に、署名されたアクションリクエストの確実性は、検査される（ブロック３４０）。実施形態によっては、アクションリクエストは、産業エレメント／コントローラ（ブロック３４２）で解読されることがありえる。例えば、産業エレメント／コントローラ２０６は、アクションリクエストを解読することがありえる。それから、署名されたアクションリクエストの確実性が検査される（ブロック３５０）ときに、要請された動作は実行されることがありえる。例えば、電源１２０は、オペレータ／エンジニアリング・インタフェース２０８、２１０および／または遠隔／ローカル・アプリケーション・インタフェース２１６、２２０により要求される動作を実行する。

【００７９】

[0088] 強化されたセキュリティに関して、要請されたアクションが産業エレメント／コントローラ２０６に通される前に、アクション認証メッセージ２０４（例えば、スマートなカード２２４を有する）を有する認証シーケンスを実行するために、産業エレメント／コントローラ２０６（例えば、電源１２０）は更に構成されることがありえる。例えば、いわゆる「握手」は、ブロック３５０の前に、または、ブロック３３０の前にさえ実行されることがありえる。いくつかの実施形態では、シグニチャーおよび確認ブロック３２０および３４０は、より複雑な認証シーケンスを用いて実行されることがありえる。加えて、実施形態によっては、より単純なシグニチャー確認または解読が測定する接頭母音に

対する追加的な保安手段として、認証シーケンスは、実行されることがありえる。

【００８０】

[0089] いくつかの実施形態では、産業エレメント／コントローラ２０６により実装される認証シーケンスは、例えば、アクション認証メッセージ２０４にリクエスト・データグラムを送ることを備えることがありえる。ここで、リクエスト・データグラムは第１の暗号の目下、第一装置認証キー証明書（例えば、デバイス認証キーを含む第１の認証証明書）および第１のアイデンティティ属性証明書を備える。それから、例えば、反応データグラムはアクション認証メッセージ２０４から受信される。ここで、反応データグラムは第２の目下、第１および第２　のｎｏｎｃｅｓめを伴う第１のシグニチャー、第２のデバイス認証キー証明書（例えば、デバイス認証キーを含む第２の認証証明書）および第２のアイデンティティ属性証明書を備える。次に、第１および第２のｎｏｎｃｅｓめ、第２のデバイス認証キー証明書および第２のアイデンティティ属性証明書と関連した第１のシグニチャーを検査することによって、反応データグラムは、確認されることがありえる。次に、アクション認証メッセージ２０４（例えば、反応データグラムが有効であると決定されるときに）に、認証データグラムは送られることがありえる。ここで、認証データグラムは第１および第２　のｎｏｎｃｅｓめを伴う第２のシグニチャーを備える。

【００８１】

[0090] 別の実施形態として、アクション認証メッセージ２０４はハンドシェイクを開始することがありえる。その場合には、リクエスト・データグラムが第１の目下、第一装置認証キー証明書および第１のアイデンティティ属性証明書を備える所で、産業エレメント／コントローラ２０６により実装される認証シーケンスは、例えば、アクション認証メッセージ２０４からリクエスト・データグラムを受信することを備えることがありえる。次に、第一装置認証キー証明書および第１のアイデンティティ属性証明書を検査することによって、リクエスト・データグラムは、確認されることがありえる。それから、反応データグラムが第２の目下、第１および第２　のｎｏｎｃｅｓめを伴う第１のシグニチャー、第２のデバイス認証キー証明書および第２のアイデンティティ属性証明書を備える所で、例えば、リクエスト・データグラムが有効であるときに、反応データグラムはアクション動証メッセージに送られることがありえる。次に、例えば、アクション認証メッセージ２０４からの認証データグラムは受信されることがありえる。ここで、認証データグラムは第１および第２　のｎｏｎｃｅｓめを伴う第２のシグニチャーを備える。それから、第１および第２のｎｏｎｃｅｓめを伴う第２のシグニチャーを検査することによって、認証データグラムは、例えば、確認されることがありえる。

【００８２】

[0091] 上で（例えば、認証モジュールにより実行される認証に関して）記載される技術の一つ以上を使用して、産業エレメント／コントローラ２０６およびアクション認証メッセージ２０４により実装されることがありえるハンドシェイクまたは認証シーケンスは、達成されることがありえる。更に、アクションオリジネータ２０２、アクション認証メッセージ２０４および産業エレメント／コントローラ２０６の各々は、本願明細書において、記載される関数またはオペレーション（例えば、方法３００および認証シーケンスにおけるステップ）を実行する力を与えられる回路および／またはロジックを備えることがありえる。例えば、アクション・オリジネータ２０２、アクション認証メッセージ２０４および産業エレメント／コントローラ２０６の各々は、永久に、半永久に記憶されるプログラム命令または、一時的に非一時的な機械読み取り可読媒体、例えばハードディスク装置、ＨＤＤによって、固体物理ディスク（ＳＤＤ）を実行する一つ以上のプロセッサ、光ディスク、磁気記憶デバイス、フラッシュドライブまたはＳＤ／ｍｉｃｒｏＳＤカードを包含することがありえる。

【００８３】

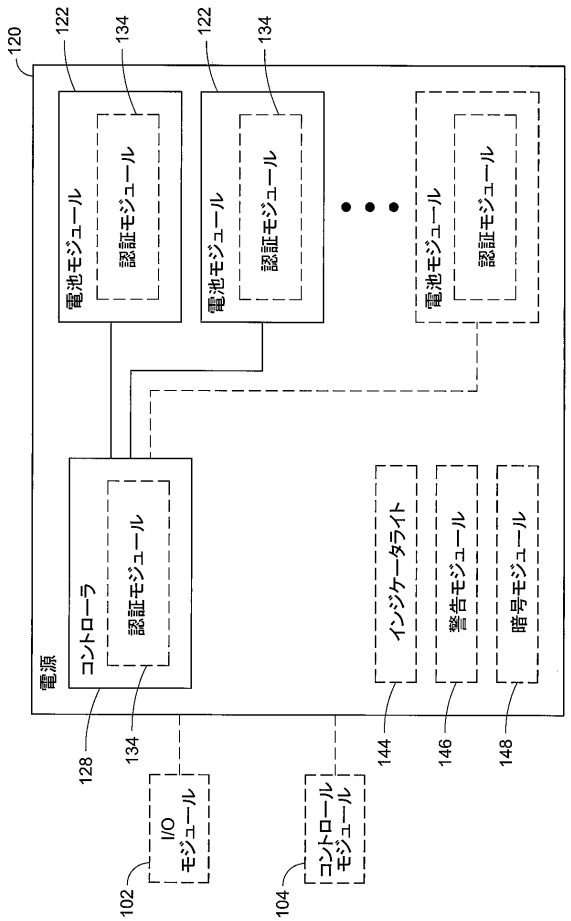
[0092] 全般的に、本願明細書において、記載される関数のいずれか、ハードウェア（例えば、固定ロジック回路（例えば集積回路）、ソフトウェア、ファームウェア、手動処理またはそれらの組み合わせを用いて実装されることがありえる。かくして、全般的に上

記の開示において、述べられるブロックは、ハードウェア（例えば、固定ロジック回路（例えば集積回路）、ソフトウェア、ファームウェアまたはそれらの組み合わせを表す。ハードウェアの構成の事例において、上記の開示において、述べられるさまざまなブロックは、他の機能と一緒の集積回路として実装されることができる。かかる集積回路は、された遮断（システムまたは回路）の関数またはブロック（システム）の一部の関数または回路の全てを備えることができる。更に、ブロック、システムまたは回路のエレメントは、複数の集積回路全体に実装されることができる。かかる集積回路は、モノリシック集積回路、フリップチップ集積回路、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包含するさまざまな集積回路から成ることができる。ソフトウェア実装の事例において、上記の開示において、述べられるさまざまなブロックは、プロセッサに実行されるときに、指定された作業を遂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、一つ以上の有形のコンピューター読み取り可能な媒体に記憶されることがありえる。いくつかにおいて、かかる事例、全システム、ブロックまたは回路は、そのソフトウェアまたはファームウェア等価物を用いて実装されることができる。他の例において、１部の所与のシステム、ブロックまたは回路はソフトウェアまたはファームウェアで実装されることができる。その一方で、他の部分はハードウェアにおいて、実装される。

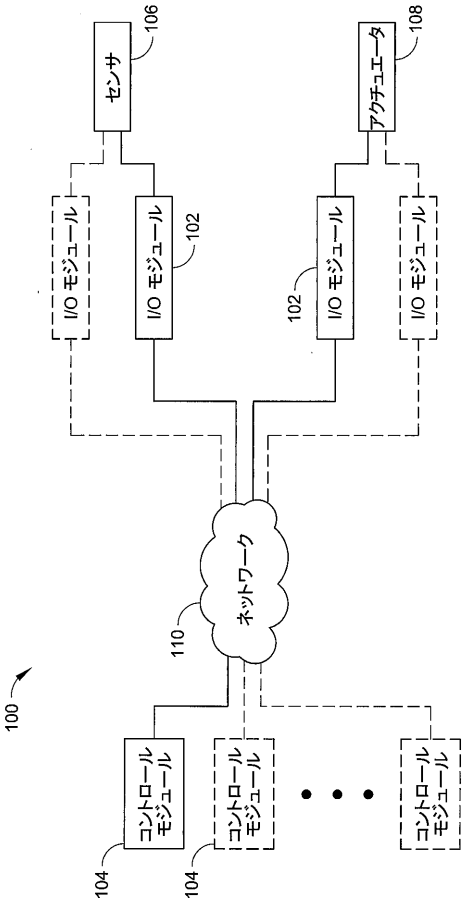
結論

[0093] 内容が構造特徴および／またはプロセス・オペレーションに特有の言語で記載されたにもかかわらず、添付の特許請求の範囲において、定められる内容が上で記載される特定の特徴または行為に必ずしも限られているというわけではないことを理解すべきである。むしろ、上で記載される特定の特徴および行為は、特許請求の範囲を実装することの例示の様態として開示される。

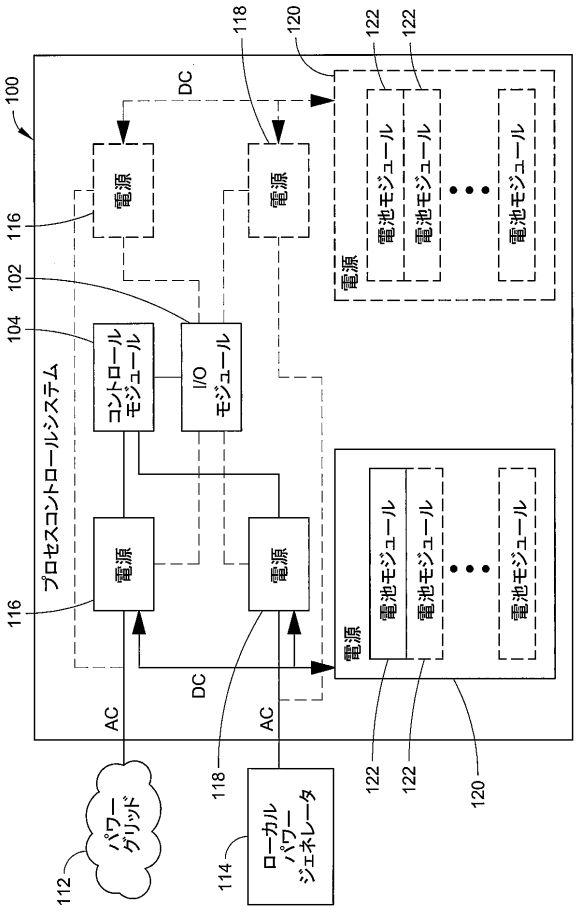
【図１】



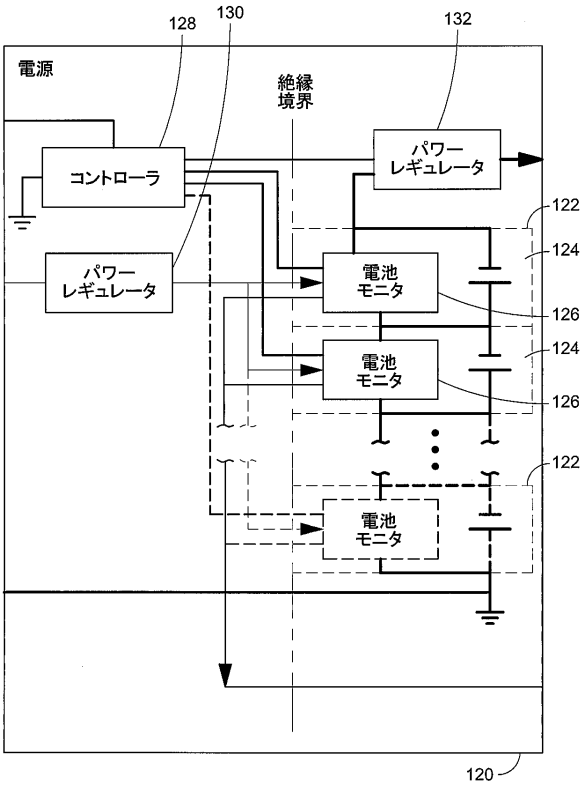
【図２】



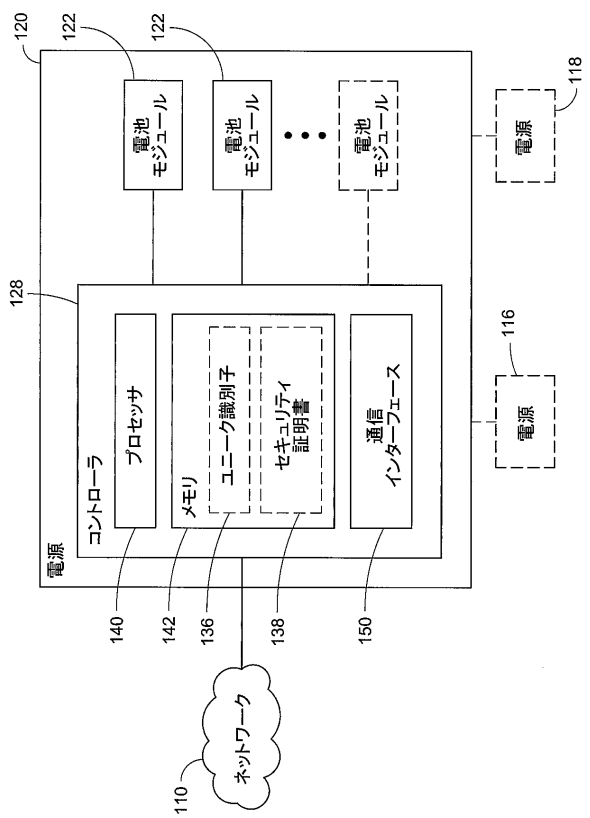
【図３】


100
プロセスコントロールシステム
DC
AC
電源
コントロール モジュール
I/O モジュール
電池モジュール
パワー グリッド
ローカル パワー ジェネレータ
102
104
112
114
116
118
120
122

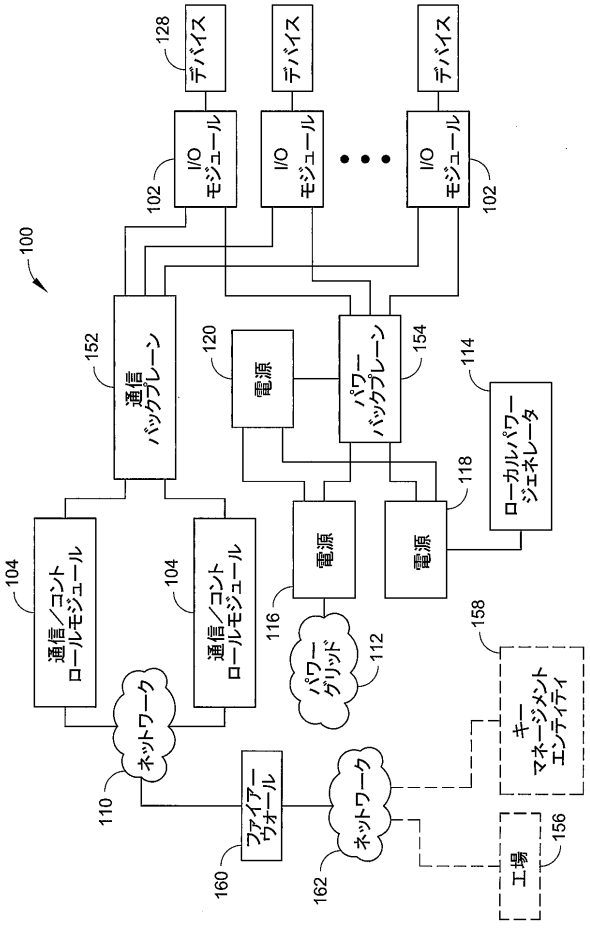
【図４】


電源
絶縁境界
コントローラ
パワー レギュレータ
電池 モニタ
120
122
124
126
128
130
132

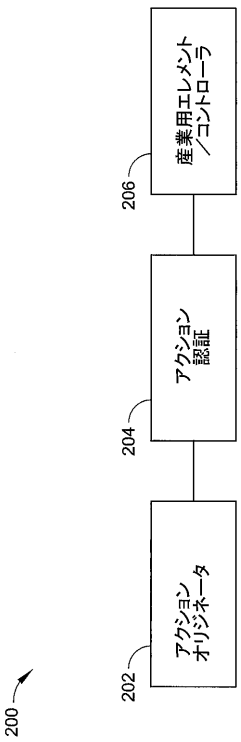
【図５】


電源
コントローラ
プロセッサ
メモリ
ユニーク識別子
セキュリティ 証明書
通信 インターフェース
電池 モジュール
ネットワーク
110
116
118
120
122
128
136
138
140
142
150

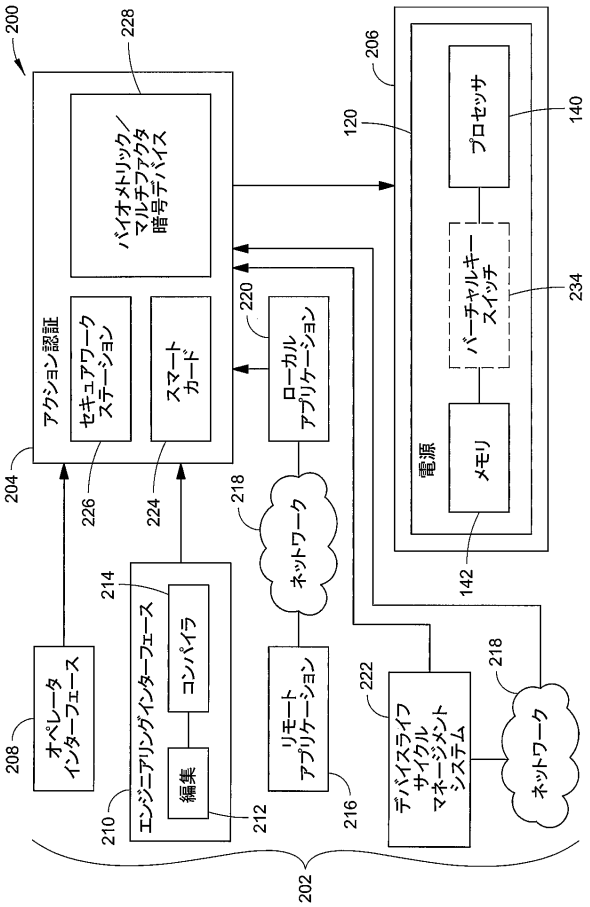
【図６】


100
デバイス
I/O モジュール
通信 バックプレーン
パワー バックプレーン
電源
ローカルパワー ジェネレータ
通信／コントロールモジュール
パワー グリッド
ネットワーク
ファイアーウォール
キー マネージメント エンティティ
工場
102
104
110
112
114
116
118
120
128
152
154
156
158
160
162

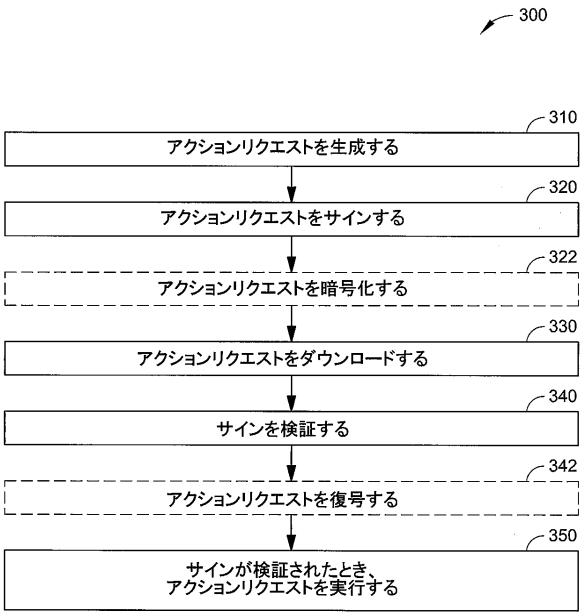
【図７】


200
202
アクション
オリジネータ
204
アクション
認証
206
産業用エレメント
／コントローラ

【図８】


200
202
204
206
208
210
212
214
216
218
220
222
224
226
228
120
140
142
234
アクション認証
セキュアワーク
ステーション
スマート
カード
バイオメトリック／
マルチファクタ
暗号デバイス
オペレータ
インターフェース
エンジニアリングインターフェース
コンパイラ
編集
ネットワーク
ローカル
アプリケーション
リモート
アプリケーション
デバイスライフ
サイクル
マネージメント
システム
ネットワーク
電源
メモリ
バーチャルキー
スイッチ
プロセッサ

【図９】


300
310
アクションリクエストを生成する
320
アクションリクエストをサインする
322
アクションリクエストを暗号化する
330
アクションリクエストをダウンロードする
340
サインを検証する
342
アクションリクエストを復号する
350
サインが検証されたとき、
アクションリクエストを実行する

フロントページの続き

(51)Int.Cl. F I
H02J 9/06 (2006.01) H02J 9/06 120

(31)優先権主張番号 14/446,412
(32)優先日 平成26年7月30日(2014.7.30)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号 14/469,931
(32)優先日 平成26年8月27日(2014.8.27)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号 14/519,032
(32)優先日 平成26年10月20日(2014.10.20)
(33)優先権主張国・地域又は機関
米国(US)

(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
(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
(72)発明者 ジョージ・クランショー
アメリカ合衆国カリフォルニア州９５１３４，サンノゼ，リオ・ローブルズ １６０

合議体
審判長 千葉 輝久
審判官 樫本 剛
審判官 木方 庸輔

(56)参考文献 特開２０１３－１９２３８９（ＪＰ，Ａ）
特表２００９－５３８１１２（ＪＰ，Ａ）
特開２００６－２５４６５０（ＪＰ，Ａ）
特開２０１１－２３３４７０（ＪＰ，Ａ）
欧州特許出願公開第２６１３４２１（ＥＰ，Ａ１）
欧州特許出願公開第２５５７６５７（ＥＰ，Ａ１）
特開２０１３－８３８１０（ＪＰ，Ａ）
特開２０１１－９６５２７（ＪＰ，Ａ）
特開２０１１－８６４６９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H02J 7/00 - 7/12
H02J 7/34 - 7/36
H02J 9/00 - 11/00
H01M 10/42 - 10/48