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

特許第5785362号
(P5785362)

(45)発行日　平成27年9月30日(2015.9.30)　(24)登録日　平成27年7月31日(2015.7.31)

| (51)Int.Cl. | | F I | | |
|---|---|---|---|---|
| G06F 21/34 | (2013.01) | G06F | 21/34 | |
| G05B 9/02 | (2006.01) | G05B | 9/02 | Z |
| H04L 9/10 | (2006.01) | H04L | 9/00 | 621A |
| H04L 9/32 | (2006.01) | H04L | 9/00 | 673A |

請求項の数 15　(全 27 頁)

(21)出願番号　特願2010-10972(P2010-10972)
(22)出願日　平成22年1月21日(2010.1.21)
(65)公開番号　特開2010-170550(P2010-170550A)
(43)公開日　平成22年8月5日(2010.8.5)
審査請求日　平成25年1月21日(2013.1.21)
(31)優先権主張番号　12/356,863
(32)優先日　平成21年1月21日(2009.1.21)
(33)優先権主張国　米国(US)

前置審査

(73)特許権者　512132022
フィッシャー－ローズマウント　システムズ，インコーポレイテッド
アメリカ合衆国　テキサス州　７８６８１　ラウンド　ロック　ウェスト　ルイス　ヘナ　ブルバード　１１００　ビルディング　１
(74)代理人　100079049
弁理士　中島　淳
(72)発明者　リー　アレン　ネイゼル
アメリカ合衆国　７８７５９　テキサス州　オースティン　カッシア　ドライブ　１０７２７

最終頁に続く

(54)【発明の名称】取り外し可能なセキュリティモジュール、および関連する方法

(57)【特許請求の範囲】

【請求項１】

第１のプロセス制御装置及び第２のプロセス制御装置と共に使用するための取り外し可能セキュリティモジュールであって、

取り外し可能な状態で前記第１のプロセス制御装置又は前記第２のプロセス制御装置に連結されるように構成された本体と、

前記本体に配置された、共有秘密キーが格納されたメモリと、

前記本体に内蔵されると共に前記メモリに連結され、前記第１のプロセス制御装置から情報を読み取り、前記情報を前記共有秘密キーと比較してから該比較に基づいて前記第１のプロセス制御装置の作動を認証する処理ユニットと、

を備え、

前記メモリは前記第１のプロセス制御装置の作動に関連する作動情報を格納し、前記取り外し可能セキュリティモジュールは、前記第１のプロセス制御装置から取り外し可能であり、前記第２のプロセス制御装置の作動を認可する必要なく前記第２のプロセス制御装置に取り外し可能な状態で連結され、かつ前記第２のプロセス制御装置を前記作動情報に従って作動させるよう、前記第１のプロセス制御装置及び前記第２のプロセス制御装置に関連付けられている、

取り外し可能セキュリティモジュール。

【請求項２】

前記比較に基づいて前記第１のプロセス制御装置が認証されない場合に、前記処理ユニ

ットが前記第１のプロセス制御装置を作動可能な状態にすることを妨げる、請求項１に記載の取り外し可能セキュリティモジュール。

【請求項３】

前記作動情報が機器構成情報を含み、前記機器構成情報が、装置識別子または制御パラメータの少なくとも一つを含む、請求項１に記載の取り外し可能セキュリティモジュール。

【請求項４】

前記メモリがそれに格納された暗号化情報を含み、且つ前記処理ユニットが、前記第１のプロセス制御装置に関連した通信の安全を確保するために前記暗号化情報を使用する、請求項１～３のいずれか一項に記載の取り外し可能セキュリティモジュール。

【請求項５】

前記暗号化情報が暗号キーを含む、請求項４に記載の取り外し可能セキュリティモジュール。

【請求項６】

前記第１のプロセス制御装置から受け取った情報を提示するための表示ディスプレイを更に備える、請求項１～５のいずれか一項に記載の取り外し可能セキュリティモジュール。

【請求項７】

前記表示ディスプレイを介して提示された前記情報に応答してユーザ入力を受け取るための入力装置を更に備える、請求項６に記載の取り外し可能セキュリティモジュール。

【請求項８】

前記表示ディスプレイを介して提示された前記情報が、前記第１のプロセス制御装置に格納された前記共有秘密キーである、請求項６に記載の取り外し可能セキュリティモジュール。

【請求項９】

第１のプロセス制御装置及び第２のプロセス制御装置と共に使用するための複数の取り外し可能セキュリティモジュールであって、

前記取り外し可能セキュリティモジュールのそれぞれが、

取り外し可能な状態で前記第１のプロセス制御装置又は前記第２のプロセス制御装置に連結されるように構成された本体と、

前記本体に配置された、共有秘密キーが格納されたメモリと、

前記本体に配置され且つ前記メモリに連結されており、前記第１のプロセス制御装置から情報を読み取り該情報を前記共有秘密キーと比較してから該比較に基づいて前記第１のプロセス制御装置の作動を認証するように構成された処理ユニットと、

を備え、

前記メモリは前記第１のプロセス制御装置の作動に関連する作動情報を格納し、前記取り外し可能セキュリティモジュールは、前記第１のプロセス制御装置から取り外し可能であり、前記第２のプロセス制御装置の作動を認可する必要なく前記第２のプロセス制御装置に取り外し可能な状態で連結され、かつ前記第２のプロセス制御装置を前記作動情報に従って作動させるよう、前記第１のプロセス制御装置及び前記第２のプロセス制御装置に関連付けられている、

複数の取り外し可能セキュリティモジュール。

【請求項１０】

前記取り外し可能セキュリティモジュールのそれぞれが、前記第１のプロセス制御装置により異なるタイプの機能または異なるレベルの機能性が提供されることを可能にする、請求項９に記載の複数の取り外し可能セキュリティモジュール。

【請求項１１】

前記複数のセキュリティモジュールのうちの第１のモジュールが前記複数のセキュリティモジュールのうちの第２のモジュールの交換用として機能し、前記第２のモジュールを前記第１のモジュールに置き換える時に前記第１のプロセス制御装置は取り外す必要なく

作動可能である、請求項９又は１０に記載の複数の取り外し可能セキュリティモジュール。

【請求項１２】

取り外し可能セキュリティモジュールで第１のプロセス制御装置及び第２のプロセス制御装置の安全を確保する方法であって、

前記第１のプロセス制御装置を前記取り外し可能セキュリティモジュールに連結し、

前記取り外し可能セキュリティモジュールに備えられた処理ユニットにより、前記取り外し可能セキュリティモジュールを介して前記第１のプロセス制御装置における秘密情報及び作動情報を含む情報を読み取り、

前記処理ユニットにより、該秘密情報を、前記取り外し可能セキュリティモジュールのメモリに格納された共有秘密キーと比較し、

前記処理ユニットにより、前記取り外し可能セキュリティモジュールを介し前記比較に基づいて前記第１のプロセス制御装置の作動を認証し、

前記第１のプロセス制御装置から前記取り外し可能セキュリティモジュールを取り外し、前記取り外し可能セキュリティモジュールを前記第２のプロセス制御装置に連結し、前記第２のプロセス制御装置の作動を認可する必要なく前記第２のプロセス制御装置を前記作動情報に従って作動する、

方法。

【請求項１３】

該比較に基づいて前記第１のプロセス制御装置が認証されない場合に、前記第１のプロセス制御装置を作動可能な状態にすることを妨げる、請求項１２に記載の方法。

【請求項１４】

分散形プロセス制御システムであって、

一つ又は複数のプロセス制御装置と、

プロセス制御装置の一つに連結された取り外し可能セキュリティモジュールを介して前記プロセス制御装置の一つから秘密情報及び作動情報を含む情報を読み取るための手段と、

前記秘密情報を、前記取り外し可能セキュリティモジュールのメモリに格納された共有秘密キーと比較するための手段と、

前記比較に基づいて前記プロセス制御装置の一つを認証するための手段と、

前記プロセス制御装置の一つで使用するための一つ又は複数のアプリケーションを認可するための手段と、

前記プロセス制御装置の一つから前記取り外し可能セキュリティモジュールを取り外すための手段と、

前記取り外し可能セキュリティモジュールを前記プロセス制御装置の他の一つに連結するための手段と、

前記プロセス制御装置の他の一つの作動を認可する必要なく前記プロセス制御装置の他の一つを前記作動情報に従って作動するための手段と、を備え、

前記メモリは前記プロセス制御装置の作動に関連する作動情報を格納する、

分散形プロセス制御システム。

【請求項１５】

一つ又は複数のアプリケーションに関連する第１の個人による命令を第２の個人により認可する二人制認可を行うための手段を更に備える請求項１４に記載の分散形プロセス制御システム。

【発明の詳細な説明】

【技術分野】

【０００１】

本開示は、概してプロセス制御システムに関し、具体的にはプロセス制御装置と共に使用するための取り外し可能なセキュリティモジュールに関する。

【背景技術】

【０００２】
通常、化学薬品の処理、石油精製、製剤工程、紙・パルプ加工工程またはその他の製造工程に使用されるようなプロセス制御システムは、オペレーターワークステーションを少なくとも一つ含む少なくとも一つのホストへと、また、精油所や自動車製造施設などの物理的な工場において物理的な工程または製造に携わる個々の作業（例えば、バルブの開閉およびプロセスパラメータの測定または推測）を制御するための一つ又は複数のフィールド装置（例えば、装置コントローラ、バルブ、バルブアクチュエータ、バルブポジショナ、スイッチ、トランスミッタ、温度センサ、圧力センサ、流量センサおよび化学成分センサ、またはそれの組み合わせ）へと通信可能に連結されるコントローラおよび入・出力（Ｉ／Ｏ）サーバーのような一つ又は複数のプロセス制御装置を含む。プロセス制御装置は、フィールド装置により行われたプロセス計測且つ又はフィールド装置に関係するその他の情報を示す信号を受け取り、制御ルーチンを実施するべくこの情報を使用し、且つプロセス制御システムの動作を制御するべくバスまたはその他の通信回線を通じてフィールド装置へと送られる制御信号を生成する。

【発明の概要】
【発明が解決しようとする課題】
【０００３】
多くのプロセス制御システムには、アクセス権の無い人が制御パラメータを変更したり、装置に命令を出したり、プロセス制御情報を得たりするなどを行えないようにしてプロセス工場の安全且つ信頼できる動作を保証するためのセキュリティ機能特性が組み込まれている。

危険な化学薬品が関与する、或いはメインまたは一次プロセス制御システムが障害を起こしたり、そうでなければ作動中に何らかの問題が生じて信用性を失ったりした際に安全性リスクを伴うその他如何なる材料または工程が関与するような特定のプロセスの動作についてメインまたは一次プロセス制御システムを安全にシャットダウンするために必要とされうる安全計装システム（ＳＩＳ）を含むプロセス制御工場においては、かかるセキュリティ機能特性が特に重要になりえる。従来から、プロセス制御システムは、独立した個別の安全システムを使用することにより（通常、その使用は限られた数の要員により認可される）、安全計装システムのセキュリティを提供していた。但し、完全に別々のシステムを運用し維持するコストおよび手間が増大したため、プロセス制御システム内の安全システムの統合につながった。このように安全システムをプロセス制御システムへと統合することによりセキュリティ上の懸念を招き、プロセス制御システム自体のセキュリティが侵害された時でも安全計装システムへの変更が無許可で行われることを防ぐためにセキュリティ対策を追加することが要求されるようになった。

【課題を解決するための手段】
【０００４】
プロセス制御装置と共に使用するための例示的な取り外し可能セキュリティモジュール、および関連した方法が開示される。例示的な取り外し可能セキュリティモジュールは、プロセス制御装置に取り外し可能な状態で連結されるように構成された本体と、該本体の中に配置されたメモリとを含み、更に該メモリの中に格納された共有秘密キーを有する。また、例示的な取り外し可能セキュリティモジュールには、本体の中に配置され且つメモリに連結されており、プロセス制御装置から情報を読み出してその情報を共有秘密キーと比較してからその比較に基づいてプロセス制御装置を認証するように構成された処理ユニットも含まれている。

【０００５】
別の実施例では、プロセス制御装置と共に使用するための複数の取り外し可能セキュリティモジュールのそれぞれに、取り外し可能な状態でプロセス制御装置に連結されるように構成された本体と、該本体の中に配置されたメモリとが含まれており、更に該メモリの中に格納された共有秘密キーを備える。更に、複数のモジュールのそれぞれには、本体の中に配置され且つメモリに連結されており、プロセス制御装置から情報を読み出してその

情報を共有秘密キーと比較してからその比較に基づいてプロセス制御装置を認証するように構成された処理ユニットが含まれている。

【０００６】

更に別の実施例で、取り外し可能セキュリティモジュールによりプロセス制御装置の安全を確保する方法には、セキュリティモジュールを介してプロセス制御装置における情報を読み取ることと、セキュリティモジュールのメモリの中に格納された共有秘密キーとその情報を比較することとが含まれる。また、例示的な方法にはセキュリティモジュールによる比較に基づいてプロセス制御装置を認証することも含まれる。

【０００７】

プロセス制御装置の安全を確保する別の例示的な方法には、プロセス制御装置で依頼または命令を受け取ることが含まれ、この場合、該依頼または命令は第１の個人と関連する。また、例示的な方法には、依頼または命令の受信に応答して秘密キーを得ることと、第２の個人に秘密キーを提供することと、第２の個人を介してプロセス制御装置に秘密キーを送信することと、秘密キーを受け取るプロセス制御装置に応答してプロセス制御装置の依頼または命令を認可することも含まれる。

【０００８】

更なる実施例では、分散形プロセス制御システムが、一つ又は複数のプロセス制御装置と、プロセス制御装置の少なくとも一つから情報を読み取るための手段と、その情報を共有秘密キーと比較するための手段とを含む。また、例示的なプロセス制御システムは、該比較に基づいてプロセス制御装置の少なくとも一つを認証するための手段と、プロセス制御装置の少なくとも一つで使用するための一つ又は複数のアプリケーションを認可するための手段も含む。

【図面の簡単な説明】

【０００９】

【図１】ここに記載される例示的な方法および機器を実施する例示的なプロセス制御システムを示すブロック図である。

【図２】図１の例示的なセキュリティモジュールの詳細ブロック図である。

【図３】図１の例示的なセキュリティモジュールの平面図を表す図である。

【図４】同側面図を表す図である。

【図５】セキュリティモジュールを制御装置からおよび通信バスから電気的に絶縁するべく図１の例示的なセキュリティモジュールと接続して実施されうるアイソレーション回路構成を表す図である。

【図６】制御装置に委託しアクションを認可するべく図１の例示的なセキュリティモジュールを実施するのに使用されうる例示的な方法のフローチャートを表す図である。

【図７】アクションの二人制認可を実施するべく図１の例示的なセキュリティモジュールを実施するのに使用されうる例示的な方法のフローチャートを表す図である。

【図８】ここに記載される例示的な方法および機器を実施するのに使用されうる例示的なプロセッサシステムのブロック図である。

【発明を実施するための形態】

【００１０】

以下、例示的な方法と装置が、その他数ある構成部分の中でも特にハードウェア上で実行されるソフトウェア且つ又はファームウェアを含むものとして説明されているが、かかるシステムは単なる例示に過ぎず本発明を限定するものと見なされるべきでないことをここに述べておく。例えば、これらのハードウェア、ソフトウェアおよびファームウェア部材のいずれかまたは全てを、ハードウェアにおいてのみ、ソフトウェアにおいてのみ、またはハードウェアとソフトウェアの如何なる組み合わせにおいて具現化することも可能であることを意図するものである。しかるべく、以下、例示的な装置およびシステムを説明するが、通常の技術を有する当業者であれば、提示されている実施例がかかる装置およびシステムを実施するための唯一の方法ではないことを容易に理解できるだろう。

【００１１】

例示的なプロセス制御システム（例えば図１のプロセスシステム１００）は、制御室（例えば図１の制御室１０２）、プロセス制御装置区域（例えば、図１のプロセス制御装置区域１０４）、一つ又は複数の成端区域（例えば図１の第１の成端区域１０６と第２の成端区域１０８）および一つ又は複数のプロセス区域（例えば図１のプロセス区域１１０、１１２、１１４および１１６）を含む。プロセス区域は、特定のプロセス（例えば、化学薬品の処理、石油精製、製剤工程、紙・パルプ加工工程、など）を行うことに関連する動作（例えば、ボイラの制御、モータの制御、バルブの制御、監視、パラメータの測定、など）を行う複数のフィールド装置を含む。幾つかのプロセス区域は、厳しい環境条件（例えば、比較的高い温、空気中に浮遊する毒素、危険な放射能レベル、など）により人間によるアクセスが不可能なものもある。制御室は、一般に人間が安全にアクセスできる環境内に備えられる一つ又は複数のワークステーションを含む。ワークステーションは、例えば変数値やプロセス制御機能の変更などによってプロセス制御システムの動作を制御するためにユーザ（例えばエンジニア、オペレータ、など）がアクセスできるユーザ・アプリケーションを含む。プロセスコントローラ区域は、制御室内のワークステーション（複数可）に通信可能に連結された一つ又は複数の制御装置を含む。制御装置は、ワークステーションを介して実施されたプロセス制御方式を実行することによりプロセス区域におけるフィールド装置の制御を自動化する。例示的なプロセス実施法には、圧力センサーフィールド装置を使用して圧力を測定することと、圧力測定に基づいてフローバルブを開・閉するべくバルブポジショナへと自動的に命令を送信することとが関与する。成端区域は、制御装置がプロセス区域におけるフィールド装置と通信することを可能にするマーシャリング・キャビネットを含む。具体的に、マーシャリング・キャビネットは、制御装置に通信可能に連結された一つ又は複数のＩ／Ｏカードとフィールド装置との間で信号をマーシャリングする、整理する、且つ又は経由するといった作業を行う。

【００１２】

プロセス制御システム内のフィールド装置は、フィールド装置のそれぞれと、制御装置（例えばプロセスコントローラ、プログラマブル論理制御装置、など）に通信可能に連結されためいめいのＩ／Ｏカードとの間にバス（例えばワイヤまたは複数のワイヤ、ケーブルまたは回路）を使用することにより制御装置に通信可能に連結される。Ｉ／Ｏカードは、制御装置およびフィールド装置の間で通信される情報を翻訳または変換することにより、異なるデータタイプ且つ又は信号タイプ（例えば、アナログ入力（ＡＩ）データタイプ、アナログ出力（ＡＯ）データタイプ、離散入力（ＤＩ）データタイプ、離散出力（ＤＯ）データタイプ、デジタル入力データタイプおよびデジタル出力データタイプ）且つ又は異なるフィールド装置通信プロトコルと関連する複数のフィールド装置へと制御装置を通信可能に連結することを可能にする。例えば、Ｉ／Ｏカードは、当該フィールド装置と関連するフィールド装置通信プロトコルを使用して該フィールド装置と情報を交換するように構成された一つ又は複数のフィールド装置インターフェースを備えうる。異なるフィールド装置インターフェースは、異なるチャネルタイプ（例えば、アナログ入力（ＡＩ）チャネルタイプ、アナログ出力（ＡＯ）チャネルタイプ、離散入力（ＤＩ）チャネルタイプ、離散出力（ＤＯ）チャネルタイプ、デジタル入力チャネルタイプおよびデジタル出力チャネルタイプ）を介して通信する。加えて、Ｉ／Ｏカードは、フィールド装置から受け取った情報（例えば電圧レベル、デジタル値など）をプロセス情報（例えば圧力測定値）に変換することができる。

【００１３】

特定の制御装置およびフィールド装置間の通信の安全が確保されないと、認可されていない命令（例えば命令を発行することを認可されていない個人且つ又は制御装置に応答して発行された命令）によってプロセス制御システムの安全な動作に深刻になセキュリティ侵害がもたらされうる。例えば、制御信号、或いは、更に概して言うと、フィールド装置にアクションを行わせる（例えば、バルブを閉じて、有毒の且つ又は極めて反応性に富む化学物質の流れを止めさせる）ようなフィールド装置への命令または依頼を通信する権限を特定の制御装置には与えないようにしうる。特定の制御装置且つ又は要員だけがかかる

危険性の高い制御装置且つ又はフィールド装置を動せるようにするためには、制御装置およびフィールド装置の高度なセキュリティが要求される。

【００１４】

セキュリティは、安全計装システムにとって最も重要なものであるが、一般にプロセス制御システムにおいて（特に、統合化安全装置または設備を含み、プロセス制御システム全体としてのセキュリティが侵害されているかどうかにかかわらず安全装置のセキュリティを要するプロセス制御システムにおいて）相当な重要性を持つ。周知のプロセス制御システムの幾つかにおいては、プロセス制御システムに組み込まれた如何なる制御装置の認証および認可を要求することにより制御装置の委託中にある程度のセキュリティが提供されている。装置が認証され認可された後でのみ、システムにおけるアイデンティティ（識別可能能特性）および役割がその装置に与えられ、その後、該装置がプロセス制御システムとの相互動作を行えるようになる。

【００１５】

制御装置の委託後、委託された制御装置へとデータを提供する（例えば、コードまたはソフトウェアをダウンロードする）ことにより、制御装置の役割が有効になる。制御装置の作動中に（即ち、それがそれの役割に準じてそれのダウンロード済みコードまたはソフトウェアを実行中に）、オペレータ、エンジニアまたはその他如何なる認定ユーザが、制御装置の動作を監視したり、制御装置へと命令を送信したり、制御装置からの情報を依頼したりなどすることが可能になりうる。

【００１６】

一般に、制御装置の認証によって、制御装置が意図される如く作動すべき制御システムで使用されていることが確認される。周知の認証工程の幾つかは、例えば、制御装置および制御装置が組み込まれているシステムにより認知される共有秘密キーを含む情報を使用しうる。かかる共有秘密キーは、製造時に制御装置に永久的に格納されうるし、プロセス制御システムは制御装置が認証されるとこの共有秘密キーを認識するように構成される。加えて、制御装置は、制御装置がプロセス制御システムと相互運用することができるかを判断するために使用されるプロセス制御システムについての情報を永久的に格納しうる、

【００１７】

一旦、制御装置が認証および認可されたなら、ワークステーション、コントローラ、認定されていない要員などによる制御装置の認定されていないアクションまたは使用を防止するべく、制御装置はそれの作動中に更なるセキュリティ対策を採用しうる。多くの場合かかる更なるセキュリティ対策には、制御装置およびプロセス制御システムと関連するその他如何なる構成体（例えばコントローラ、フィールド装置、ワークステーション、要員、アプリケーションなど）の間における如何なる通信に対して暗号化を使用することが含まれうる。これを達成するために、幾つかのプロセス制御装置には、それの製造時に制御装置の中に格納（もしくは製造）されうる一つの暗号キーまたは複数の暗号キーが含まれうる。

【００１８】

共有秘密キー、暗号キーなどをはじめとする上述のセキュリティ対策は効果的でありえるが、これらのセキュリティ対策が展開される現在の様態では、実施上の問題が幾つか伴う場合がある。例えば、製造時に制御装置の幾つかの中にハードコードされる共有秘密キーのセキュリティが万一侵害された（例えば、許可されていない構成体に知られてしまった）場合には、その装置のセキュリティを回復するために、制御装置の中の共有秘密キーを変更しなければならないことになる。但し、かかる共有秘密キーの変更には、プロセス制御システムから制御装置を取り外してからその制御装置をそれの製造メーカへ送り共有秘密キーを変更してもらう必要がありうる。更に、万一制御装置が障害を起し交換する必要が生じた場合、不具合を持つ装置に取って代わる装置が如何なるものでも、置換装置の委託（例えば、ソフトウェアまたはそれの役割を行うためのコードの認証、認可、ダウンロード、など）を必要とするが、このような作業には多大なる時間と高額な費用がかかることに加え、しばしば許容できないほど長い時間プロセス制御システムをオフライン状態

とすることが要される。

【００１９】

更に、Ｉ／Ｏカードおよびフィールド装置が正確な制御装置に連結されている場合でも万一制御装置が不正に使用されると（例えば、誤った命令または依頼に応答してアクションを実行すると）、この場合も、プロセス制御システムにおいて深刻且つ危険な結果が生じうる。制御装置が少なくとも幾つかの動作について正しく使用されること（または、不当に修正変更されないようにすること）を保証するために、幾つかの制御システムまたは当該制御システムの諸部分は、特定の制御装置が依頼または命令に応答して適切なアクションを行うことを許されているかどうかを判断するべく当該制御装置の付加的なアクセス制御または認可を要求する。幾つかの状況（例えば極めて機密性の高い作業）における制御装置の認可には、制御室のオペレータまたはエンジニア、そして制御装置に配置されている別の個人が認可作業を行うことが要求されうる（即ち、二人制認可が要求される）。従来から、制御装置に配置されている人員は、制御室にいる人員からの指示に基づいて装置の所で鍵を回したりコードを入力したりすることが要求されるが、これには、これらの物理的な制約を付けて（例えば、キーロックや鍵などを備えた状態で）制御装置を製造する必要があるだけでなく、鍵の損失や無許可の複製または鍵の乱雑を防ぐために鍵の管理プロトコルを実施することも必要とされる。物理的な鍵を使用することによって、鍵のアクセスの管理、鍵の発行および保管場所の監視、実際に鍵を回す要員の記録管理、などが更に要求される。更に、鍵の切り替えは時間切れになったりしないが、その代わり、物理的に一個人により始動させる必要があるので、結果として実際の運用にて永久に鍵が掛かった状態になったり、または、無制限に有効になったりする。

【００２０】

ここに記載される例示的な機器および方法は、より柔軟且つ確実にプロセス制御システムの安全を確保するために使用されうる。特に、ここに記載される例示的な機器および方法は、制御装置（例えばフィールド装置、コントローラなど）に取り外し可能な状態で連結することができるセキュリティモジュールを使用する。セキュリティモジュールは、制御装置を認証し、委託し、それの安全を確保するため、および制御装置に関連したアクションまたはアプリケーションを認可するために必要な実質的に全てのセキュリティソフトおよび電子機器を提供する。これには、例えば、制御装置を認証するために使用される秘密キー（例えば共有秘密キー）を格納すること、制御装置のアクションを認可するために使用される暗号キーまたはその他の暗号情報を格納すること、認定されていない依頼または命令から保護すること、制御装置にアイデンティティを提供すること、プロセス制御システムにおける制御装置の役割を割り当てること、二人制認可方式を円滑に実施すること、および割り当てられた役割を行うべきデータで制御装置を構成することが含まれる。

【００２１】

セキュリティモジュールが制御装置に連結される場合、セキュリティモジュールは制御装置から制御装置情報を読み取る。この情報は、セキュリティ装置のメモリに格納された共有秘密キーと比較される。制御装置情報および共有秘密キーの間に相互関連性（例えば一致するもの）がある場合、制御装置の据え付けが認証される。よって、セキュリティモジュールは制御装置を認証し、プロセス制御システムへそれを組み込む。共有秘密キーおよび制御装置情報が相互に関連しない、または一致しない場合、制御装置は、セキュリティモジュールを使用することが認証されず、当該のプロセス制御システムまたはプロセス制御システムの当該の部分に据え付けられることが認可されない。その場合、制御装置は委託不可能となり、よって作動不能のままとなる。

【００２２】

制御装置が委託された後、制御装置は、認証中にそれに割り当てられた役割を行うために制御装置が必要とするデータで構成される。一旦制御装置が作動し始めると、該制御装置には普通一人又は複数人のオペレータまたはエンジニアが立ち合う。オペレータ且つ又はエンジニアは、システム（またはその部分）が目的通りに作動していることを保証するために例えば抄紙機、蒸留塔または生産セルを含む自分が担当する（例えば物理的な工場

などの）プロセス制御システムの部分を制御または監視するべく該制御装置（並びにその他の制御装置）と交信する。プロセス制御システムの作動中に、制御装置は多数の依頼、命令、修正変更、且つ又はその他の通信を受け取る。制御装置が認定されていない通信に応答してアクションを行うのを防ぐために、セキュリティモジュールは通信を監視し、アクションを認可、或いは妨害する。例えば、セキュリティモジュールは、通信に含まれる情報を抽出し、該情報の少なくとも幾つかを、セキュリティモジュールのメモリに格納された暗号キーと比較しうる。暗号キーと通信に含まれる情報との間に相互関連性がある場合、セキュリティモジュールは、通信に応答して適切なアクションを行うことを制御装置に認可しうる。暗号キーとの相互関連性がない場合、制御装置によるアクションは認可されず、よって、妨害される。

【００２３】

加えて、より詳しく後述される如く、ここに記載される例示的なセキュリティモジュールは制御装置に取り外し可能な状態で連結することができるので、制御装置を交換してから製造メーカに制御装置を送って再設定してもらったり、若しくはプロセス制御システムから制御装置を取り外したりする必要なく、セキュリティモジュールを取り外して所望の異なるセキュリティ機能特性を使用する別のセキュリティモジュールに交換することにより、制御装置により使用されるセキュリティ機能特性を変更することができる。加えて、第１の制御装置から取り外したセキュリティモジュールは、第２の制御装置を委託する必要なく第２の制御装置（例えば第１の制御装置の交換品）に取り外し可能な状態で連結しうる。

また、より詳しく後述される如く、改訂された（例えば、アップグレードされた）セキュリティソフトウェア且つ又は電子機器（例えば診断法を含む）が制御装置により使用される同じタイプのセキュリティ機能特性に向けて利用可能な場合、制御装置を交換して制御装置の再委託を行い、製造メーカに制御装置を送って再構成してもらったり、若しくはプロセス制御システムから制御装置を取り外したりする必要なく制御装置のセキュリティモジュールを取り外して、改訂されたセキュリティソフト且つ又は電子機器を有する異なるセキュリティモジュールと交換することができる。つまり、制御装置のセキュリティモジュールだけが、異なるセキュリティ機能特性を含む異なるセキュリティモジュールと交換されることになる。

【００２４】

ここに記載される例示的なセキュリティモジュールは、セキュリティソフトを含む自己完結型のカプセル化電子モジュールでありうる。更に、これらの例示的なセキュリティモジュールは、様々なタイプ、製造元（例えば、異なる製造メーカにより提供された）および機種の制御装置に取り外し可能な状態で挿入（若しくは連結）されうる。制御装置に対してセキュリティ機能特性を提供するべく、例示的なセキュリティモジュールを標準化して、異なるタイプの制御装置と接続して使用しうる。より具体的には、制御装置の実装、電気接続（例えばピン配列）などを含む機械的な構成およびインターフェースと、セキュリティモジュールは標準としうるので、異なるセキュリティ機能特性を提供する複数の獲得可能セキュリティモジュールの如何なるものを、如何なる数のメーカにより製造された様々な制御装置の如何なるものと使用することができる。同様に、セキュリティモジュールが制御装置内のその他の電子機器と通信する様態も標準化しうる。言い換えると、セキュリティモジュールの制御装置との互換性を更に円滑に実施するべく、制御装置とセキュリティモジュールの間で通信を可能にするために使用される通信方式を、制御装置の諸タイプ、諸製造元、諸機種などにわたり適合するしうるように標準化することも可能である。

【００２５】

ここに記載される例示的なセキュリティモジュールは、制御装置セキュリティの標準化を可能にする、よって、特定のセキュリティプログラム（即ち、一式のセキュリティ機能特性）にこだわることなくセキュリティモジュールを製造できるようになる。つまり、制御装置を製造後（例えば、制御装置がプロセス制御システムに据え付けられる時に、また

は委託中に）制御装置の中に適切なセキュリティモジュールを据え付けることにより、かかるセキュリティ機能特性を割り当てる、或いは構成することができる。これにより、必要予備部品（例えば予備の制御装置）の数を減らすことができ、制御装置をある一つのセキュリティプログラムから別のセキュリティプログラムに簡単に切り替えられるようになる。また、もはや相当な量の内部セキュリティ電子機器またはソフトウェアを制御装置に含む必要がなくなるので、ここに記載される例示的な方法および機器は、制御装置の製造を簡素化することもできる。従って、ここに記載される例示的な方法および機器によって、製造メーカが異なるセキュリティ機能特性を採用する同じような制御装置を以前のように数多く生産する必要がなくなる。

【００２６】

更に、例示的なセキュリティモジュールは、実質的に全ての制御装置用通信ソフトおよび電子機器を含みうる。よって、「Apparatus and Methods to Communicatively Couple Field Devices to Controllers in a Process Control System」（仮訳：「プロセス制御システムにおいてフィールド装置をコントローラに通信可能な状態で連結する機器および方法」）と題され且つ、ここに参照することによりその全体にわたりに援用される同時係属中の共同所有された米国出願書第１２／２３６，１６５号に記載される通信モジュールの機能特性の全てを、ここに記載されるセキュリティモジュールは含みうる。

【００２７】

なおさらに、セキュリティモジュールを、新しいまたは異なる機能特性を組み込んだソフトウェアを含む改訂またはアップグレード済みソフトウェアを備える別のセキュリティモジュールに交替することによりセキュリティソフト改訂またはアップグレードを簡単に加えうるのでシステムの保守コストを削減しうる。更にまた、制御装置の内部電子機器にアクセスすることなく、ここに記載される例示的なセキュリティモジュールを簡単に取り替える、または交換することができるので、セキュリティプログラムのアップグレード且つ又は変更をそのままの状態で（即ち、制御装置を取り外す必要なく）行うことができる。加えて、制御装置の診断をセキュリティモジュールに含みうるので、より新しい、またはより良い診断ソフトウェアを望む利用者は、制御装置の内部電子機器を変更する必要なく、セキュリティモジュールを所望の診断法を含む別のセキュリティモジュールと取り替えることができる。更に、幾つかの例示的なセキュリティモジュールは、例えば制御装置シリアル番号（複数可）且つ又はその他の制御装置情報のようなローカルタグ付け情報を含みうる。セキュリティソフト、診断情報且つ又はローカルタグ付け情報のいずれかまたは全てを例示的なセキュリティモジュールに含むことにより、制御装置の構成および制御装置の作動状態、履歴、保守保全の必要性などの評価を円滑に実施できるようになる。

【００２８】

加えて、幾つかの実施例では、セキュリティモジュールを、それに含まれるセキュリティ機能特性、アップグレード、更新、診断法などのタイプに応じてコード化（例えば、色分け）しうる。コード化方式によって、制御装置（複数可）に連結するのに適切なセキュリティモジュールの識別を円滑に実施できるようになる。

【００２９】

ここで図１を詳細にわたって参照するに、例示的なプロセス制御システム１００は、一般にアプリケーション制御ネットワーク（ＡＣＮ）と呼ばれるローカルエリアネットワーク（ＬＡＮ）１２４またはバスを介して第１の制御装置（例えばコントローラ）１２０および第２の制御装置（例えばコントローラ）１２２を含む一つ又は複数の制御装置に通信可能に連結されたワークステーション１１８を備える制御室１０２を含む。ＬＡＮ１２４は如何なる所望の通信媒体およびプロトコルを使用して実施されうる。例えば、ＬＡＮ１２４は配線接続式またはワイヤレスのイーサネット（登録商標）通信プロトコルに基づきうる。但し、その他如何なる適切な有線または無線の通信媒体およびプロトコルを使用することも可能である。一つ又は複数の情報技術アプリケーション、ユーザ対話型アプリケーション且つ又は通信アプリケーションと関連する動作を行うようにワークステーション１１８を構成しうる。例えば、プロセス制御関連アプリケーションおよび、ワークステー

ション１１８と制御装置１２０および１２２が如何なる所望の通信媒体（例えば無線通信、配線接続式など）およびプロトコル（例えばＨＴＴＰ、ＳＯＡＰなど）を用いてその他の装置またはシステムと通信することを可能にする通信アプリケーションと関連する動作を行うようにワークステーション１１８を構成しうる。例えばワークステーション１１８またはその他如何なるワークステーションを用いてシステムエンジニアまたはその他のシステム・オペレータにより生成され、そして制御装置１２０および１２２にダウンロードされてインスタンス化された一つ又は複数のプロセス制御ルーチンまたは機能を行うように制御装置１２０および１２２を構成しうる。図示される実施例において、ワークステーション１１８は制御室１０２に設置されており、制御装置１２０および１２２は、物理的に制御室１０２とは別の所にある制御装置区域１０４に設置されている。

【００３０】

図１の例示的な実施形態において、第１の制御装置１２０は、バックプレーン通信または内部Ｉ／Ｏバス１４４を介してＩ／Ｏカード１４０ａ－ｂおよび１４２ａ－ｂに通信可能に連結される。ワークステーション１１８と通信するために、第１の制御装置１２０はＬＡＮ１２４を介してワークステーション１１８に通信可能に連結される。第２の制御装置１２２は、ＬＡＮ１２４を介してワークステーション１１８とＩ／Ｏカード１４０ｃ－ｄおよび１４２ｃ－ｄに通信可能に連結される。Ｉ／Ｏカード１４０ｃ－ｄおよび１４２ｃ－ｄは、ＬＡＮ１２４を介して第２の制御装置１２２およびワークステーション１１８と通信するように構成される。このように、Ｉ／Ｏカード１４０ｃ－ｄおよび１４２ｃ－ｄは、ワークステーション１１８と情報を直接取り交わすことができる。

【００３１】

図示される実施例において、例示的なプロセス制御システム１００は、フィールド装置１２６ａ－ｃを第１のプロセス区域１１０に、フィールド装置１２８ａ－ｃを第２のプロセス制御区域１１２に、フィールド装置１３０ａ－ｃを第３のプロセス制御区域１１４に、そしてフィールド装置１３２ａ－ｃを第４のプロセス制御区域１１６に含む。制御装置１２０および１２２と、フィールド装置１２６ａ－ｃ、１２８ａ－ｃ、１３０ａ－ｃおよび１３２ａ－ｃとの間で情報を通信するために、例示的なプロセス制御システム１００には、フィールド・ジャンクションボックス（ＦＪＢ）１３４ａ－ｄおよびマーシャリング・キャビネット１３６ａ－ｂが備えられている。フィールド・ジャンクションボックス１３４ａ－ｄのそれぞれは、めいめいの多重導体ケーブル１３８ａ－ｄ（例えばマルチバスケーブル）を介してフィールド装置１２６ａ－ｃ、１２８ａ－ｃ、１３０ａ－ｃおよび１３２ａ－ｃのめいめいのものからマーシャリング・キャビネット１３６ａ－ｂのうちの一つへと信号を経由させる。それに対してマーシャリング・キャビネット１３６ａ－ｂは、フィールド装置１２６ａ－ｃ、１２８ａ－ｃ、１３０ａ－ｃおよび１３２ａ－ｃから受け取った情報（例えば信号）をマーシャリングして（例えば、整理したり、グループに分類したり、などを行って）、フィールド装置情報を制御装置１２０と１２２のめいめいのＩ／Ｏカード（例えばＩ／Ｏカード１４０ａ－ｄ）へと経由させる。図示される実施例において、Ｉ／Ｏカード１４０ａ－ｄと制御装置１２０および１２２から受け取った情報をフィールド・ジャンクションボックス１３４ａ－ｄを介してフィールド装置１２６ａ－ｃ、１２８ａ－ｃ、１３０ａ－ｃおよび１３２ａ－ｃのめいめいのものに経由させるためにもマーシャリング・キャビネット１３６ａ－ｂを使用しうるように、制御装置１２０および１２２と、フィールド装置１２６ａ－ｃ、１２８ａ－ｃ、１３０ａ－ｃおよび１３２ａ－ｃとの間の通信は双方向に行われるようになっている。

【００３２】

図１の実施例では、フィールド装置１２６ａ－ｃ、１２８ａ－ｃ、１３０ａ－ｃおよび１３２ａ－ｃが、導電性（例えば配線接続式）且つ又はワイヤレス通信媒体、且つ又は光通信媒体を介してフィールド・ジャンクションボックス１３４ａ－ｄに通信可能に連結される。例えば、フィールド・ジャンクションボックス１３４－ａ－ｄには、フィールド装置１２６ａ－ｃ、１２８ａ－ｃ、１３０ａ－ｃおよび１３２ａ－ｃの有線、無線且つ又は光トランシーバと通信するために一つ又は複数の有線、無線、且つ又は光学データ・トラ

ンシーバを備えうる。図示される実施例において、フィールド・ジャンクションボックス１３４ｂおよび１３４ｄは、（ここに記載される順で）めいめいフィールド装置１２８ｃおよび１３２ｃへとワイヤレス方式で通信可能に連結される。代替的な例示的な実施形態では、マーシャリング・キャビネット１３６ａ－ｂを省略しても良く、介在する構造のない状態で（即ち、マーシャリング・キャビネット１３６ａ－ｂなしで）フィールド装置１２６ａ－ｃ、１２８ａ－ｃ、１３０ａ－ｃおよび１３２ａ－ｃからの信号を、フィールド・ジャンクションボックス１３４ａ－ｄから直接制御装置１２０および１２２のＩ／Ｏカード１４０ａ－ｄへと経由させることも可能である。更に別の例示的な実施形態では、フィールド・ジャンクションボックス１３４ａ－を省略しても良く、フィールド装置１２６ａ－ｃ、１２８ａ－ｃ、１３０ａ－ｃおよび１３２ａ－ｃを直接マーシャリング・キャビネット１３６ａ－ｂに連結することができる。

【００３３】

フィールド装置１２６ａ－ｃ、１２８ａ－ｃ、１３０ａ－ｃおよび１３２ａ－ｃはフィールドバス適合バルブ、作動装置、センサなどでありえ、その場合、フィールド装置１２６ａ－ｃ、１２８ａ－ｃ、１３０ａ－ｃおよび１３２ａ－ｃは、周知のＦＯＵＮＤＡＴＩＯＮフィールドバス通信プロトコルを使用しデジタルデータ・バスを介して通信する。もちろん、その他のタイプのフィールド装置および通信プロトコルをその代りに使用することも可能である。例えば、フィールド装置１２６ａ－ｃ、１２８ａ－ｃ、１３０ａ－ｃおよび１３２ａ－ｃは、その代わり周知のプロフィバスおよびＨＡＲＴ通信プロトコルを使用しデータバスを介して通信するプロフィバス（ＨＡＲＴ）またはＡＳ－ｉ適合装置でありえる。例示的な実施形態の幾つかにおいて、フィールド装置１２６ａ－ｃ、１２８ａ－ｃ、１３０ａ－ｃおよび１３２ａ－ｃは、デジタル通信の代わりに、アナログ通信または離散通信を使用して情報を通信することができる。加えて、通信プロトコルは異なるデータタイプに関連した情報を通信するのにも使用することができる。

【００３４】

フィールド装置１２６ａ－ｃ、１２８ａ－ｃ、１３０ａ－ｃおよび１３２ａ－ｃのそれぞれは、フィールド装置識別情報を格納するように構成される。フィールド装置識別情報は、フィールド装置１２６ａ－ｃ、１２８ａ－ｃ、１３０ａ－ｃおよび１３２ａ－ｃのそれぞれを一意的に同定する物理的装置タグ（ＰＤＴ）値、装置タグ名、電子シリアル番号などでありうる。図１に示される実施例では、フィールド装置１２６ａ－ｃ、１２８ａ－ｃ、１３０ａ－ｃおよび１３２ａ－ｃが、フィールド装置識別情報を物理的装置タグ数値「ＰＤＴ００－ＰＤＴ１１」の形式で格納する。フィールド装置識別情報は、フィールド装置の製造メーカにより、且つ又はフィールド装置１２６ａ－ｃ、１２８ａ－ｃ、１３０ａ－ｃおよび１３２ａ－ｃの据え付け且つ又は委託に関与するオペレータまたはエンジニアにより、フィールド装置１２６ａ－ｃ、１２８ａ－ｃ、１３０ａ－ｃおよび１３２ａ－ｃに格納またはプログラムされる。

【００３５】

制御装置１２０および１２２（且つ又はワークステーション１１８）と、フィールド装置１２６ａ－ｃ、１２８ａ－ｃ、１３０ａ－ｃおよび１３２ａ－ｃとの間のＩ／Ｏ通信を制御するために、制御装置区域１０４には複数のＩ／Ｏカード１４０ａ－ｄが備えられている。図示される実施例において、Ｉ／Ｏカード１４０ａ－ｂは、第１の制御装置１２０（且つ又はワークステーション１１８）と第１および第２のプロセス区域１１０および１１２におけるフィールド装置１２６ａ－ｃおよび１２８ａ－ｃとの間のＩ／Ｏ通信を制御するように構成され、そしてＩ／Ｏカード１４０ｃ－ｄは、第２の制御装置１２２（且つ又はワークステーション１１８）と第３および第４のプロセス区域１１４および１１６におけるフィールド装置１３０ａ－ｃおよび１３２ａ－ｃとの間のＩ／Ｏ通信を制御するように構成される。

【００３６】

図１に示される実施例では、Ｉ／Ｏカード１４０ａ－ｄが制御装置区域１０４に存在する。フィールド装置１２６ａ－ｃ、１２８ａ－ｃ、１３０ａ－ｃおよび１３２ａ－ｃから

ワークステーション１１８に情報を通信するために、Ｉ／Ｏカード１４０ａ－ｄは、制御装置１２０および１２２に情報を通信し、それに対して制御装置１２０および１２２はワークステーション１１８に情報を通信する。同様に、ワークステーション１１８からフィールド装置１２６ａ－ｃ、１２８ａ－ｃ、１３０ａ－ｃおよび１３２ａ－ｃへと情報を通信するために、ワークステーション１１８は制御装置１２０および１２２に情報を通信し、制御装置１２０および１２２はＩ／Ｏカード１４０ａ－ｄに情報を通信し、そしてＩ／Ｏカード１４０ａ－ｄはフィールド装置１２６ａ－ｃ、１２８ａ－ｃ、１３０ａ－ｃおよび１３２ａ－ｃに情報を通信する。代替的な例示的な実施形態において、Ｉ／Ｏカード１４０ａ－ｄがワークステーション１１８且つ又は制御装置１２０および１２２と直接通信することができるように、Ｉ／Ｏカード１４０ａ－ｄは制御装置１２０および１２２の内部にあるＬＡＮ１２４に通信可能に連結できるようになっている。

【００３７】

Ｉ／Ｏカード１４０ａ－ｄのいずれかが障害を起した際にフォールト・トレラントな（耐障害性を有する）動作を提供するべく、Ｉ／Ｏカード１４０ａ－ｄが冗長Ｉ／Ｏカードとして構成されている。即ち、Ｉ／Ｏカード１４０ａが障害を起した場合、冗長Ｉ／Ｏカード１４２ａが制御を引き継ぎ、Ｉ／Ｏカード１４０ａが障害の生じなかった場合に行うであろう動作と同じ動作を行う。同様に、Ｉ／Ｏカード１４０ｂが障害を起した場合、冗長Ｉ／Ｏカード１４２ｂが制御を引き継ぐ、などといった具合に以降同様に構成される。

【００３８】

制御装置区域１０４に示されるように、第１のセキュリティモジュール１５０は、第１の制御装置１２０に直接連結され、また第２のセキュリティモジュール１５２は第２の制御装置１２２に直接連結される。加えて、セキュリティモジュール１５４、１５６および１５８は、この実施例ではフィールド装置として示されるめいめいの制御装置１２６ａ、１２６ｂおよび１２６ｃに直接連結される。セキュリティモジュール１５０－１５８は、お守りのような形をした取り外し可能、プラグ接続可能または挿入可能な装置（例えば保護カバーまたは筐体を有する回路カードと、プラグ接続できる電気コネクタ）として構成されうる。代替的な例示的な実施形態では、セキュリティモジュール１５０－１５８が中間構造（複数可）または装置（複数可）を介して制御装置１２０および１２２且つ又は１２６ａ－ｃに通信可能に連結されうる。

【００３９】

制御装置１２０、１２２および１２６ａ－ｃを認証および委託するため、および受け取った依頼または命令に応答して制御装置により行われるアクションを認可するためにプロセス制御システム１００により使用される実質的に全てのセキュリティソフトおよび電子機器を、セキュリティモジュール１５０－１５８は提供する。更に概して言えば、セキュリティモジュール１５０－１５８は、適切な制御装置がプロセス制御システム１００に適切に連結され、これらの装置が適切な様態で使用されることを保証する。以下、例示的なセキュリティモジュール１５０－１５８およびそれらの関連動作をより詳しく説明する。

【００４０】

図示される実施例において、マーシャリング・キャビネット１３６ａ－ｂ、セキュリティモジュール１５０－１５８、Ｉ／Ｏカード１４０ａ－ｄおよび１４２ａ－ｄ、そして制御装置１２０、１２２および１２６ａ－ｃによって、既存のプロセス制御システムの据え付けを、図１の例示的なプロセス制御システム１００の構成に実質的に類似する構成へと切り替える作業が円滑に行えるようになる。例えば、如何なる適切なインターフェース・タイプを含むようにセキュリティモジュール１５０－１５８を構成することができるので、セキュリティモジュール１５０－１５８は如何なるタイプの制御装置に通信可能に連結されるように構成することができる。同様に、制御装置１２０および１２２は、既に据え付けられているワークステーションへとＬＡＮを介して通信するための周知のＬＡＮインターフェースを含むように構成することができる。例示的な実施形態の幾つかでは、プロセス制御システムに既に据え付けられている制御装置を交換する必要がないように、Ｉ／Ｏカード１４０ａ－ｄおよび１４２ａ－ｄを周知の制御装置の中に設置するか、またはそ

れに通信可能に連結することができる。

【００４１】

図５に描かれる代替的な実施例では、セキュリティモジュール１５０および１５２を使用してＬＡＮ１２４または内部Ｉ／Ｏバス１４４にめいめいの制御装置１２０および１２２を連結しうる。当該の実施例において、ワークステーション１１８からの通信は全てセキュリティモジュール１５０および１５２により処理され、また、適切な場合は以下詳述されるようにめいめいの制御装置１５０および１５２へと通信される。加えて、Ｉ／Ｏカード１４０ａ－ｄおよび１４２ａ－ｄからの通信も全てセキュリティモジュール１５０および１５２により処理され、適切な場合はめいめいの制御装置１５０および１５２へと通信される。

【００４２】

図２は、ここに記載される例示的なセキュリティモジュールの如何なるものを表しうるセキュリティモジュール２００の例示的な実施を示す。図２の例示的なセキュリティモジュール２００には、セキュリティモジュール２００がＬＡＮ１２４且つ又は内部Ｉ／Ｏバスに制御装置を連結するために使用される構成において例えばＩ／Ｏカード且つ又はワークステーションとセキュリティモジュール２００が通信することを可能にするための外部バスインターフェース２０２が含まれる。

【００４３】

セキュリティモジュール２００のアドレス且つ又は制御装置のアドレスを同定するために、セキュリティモジュール２００にはアドレス識別子２０４が与えられている。セキュリティモジュール２００が制御装置に差し込まれた時にセキュリティモジュール・アドレス（例えばネットワーク・アドレス）について制御装置に問い合わせ（クエリー）するようにアドレス識別子２０４を構成しうる。このように、セキュリティモジュール２００は、制御装置にまたは制御装置から情報を通信する際にセキュリティモジュール・アドレスをソース且つ又は宛先アドレスとして使用することができる。

【００４４】

また、例示的なセキュリティモジュール２００は、外部バスを介してその他のシステム構成部分と情報を取り交わすための外部バス通信プロセッサ２０６も備えている。図示される実施例において、外部バス通信プロセッサ２０６は、情報を別のシステム構成部分へと送信するためにパケット化し、その他のシステム構成部分から受け取った情報を非パケット化する。パケット化された情報は、外部バスを通じた送信に向けて外部バスインターフェース２０２へと通信される。図示される実施例において、外部バス通信プロセッサ２０６は、送信されるべき各パケット用にヘッダー情報を生成し、受信したパケットからヘッダー情報を読み取る。例示的なヘッダー情報としては、宛先アドレス（例えばＩ／Ｏカードのネットワーク・アドレス）、ソースアドレス（例えばセキュリティモジュール２００のネットワーク・アドレス）、パケットタイプまたはデータタイプ（例えばアナログ・フィールド装置情報、フィールド装置情報、コマンド情報、温度情報、実時間データ値など）、およびエラーチェック情報（例えば巡回冗長検査（ＣＲＣ）情報）が挙げられる。例示的な実施形態の幾つかにおいては、処理ユニット２０８と同じマイクロプロセッサまたはマイクロコントローラを使用して外部バス通信プロセッサ２０６を実施しうる。

【００４５】

セキュリティモジュール２００の様々な動作を制御するために、セキュリティモジュール２００には処理ユニット２０８が備えられている。例示的な実施形態においては上述の如く、マイクロプロセッサまたはマイクロコントローラを使用して処理ユニット２０８を実施することができる。処理ユニット２０８は、セキュリティモジュール２００のその他の部分へと、当該部分の動作を制御するべく指示または命令を通信する。

【００４６】

処理ユニット２０８は、例えば制御装置に格納される秘密キーのような認証情報を含む制御装置情報を制御装置から得るために使用される読み取り機構２１０を備える、または該読み取り機構２１０と通信可能に連結される。また、読み取り機構２１０は、セキュリ

ティモジュール２００のメモリ２１２からも情報を得る。該メモリは、如何なるタイプの構成可能なデータベースを含みうるし、また、例えば、制御装置の認証のための共有秘密キー情報、制御装置のアクションを認可するために使用される暗号キーを含む暗号化情報、制御装置と関連する委託情報、例えば装置識別子または制御パラメータのような構成情報およびその他如何なる情報などの情報を含みうる。

【００４７】

また、処理ユニット２０８はコンパレータ（比較機構）２１４を備えるか、またはコンパレータ２１４に通信可能に連結される。コンパレータ２１４は受信した且つ又はに格納された情報を評価するために使用されうる。例えば、コンパレータ２１４は、セキュリティモジュール２００がメモリ２１２に格納された第２の秘密キーに対して連結された制御装置から受け取った第１の秘密キーを含む情報を比較しうる。コンパレータ２１４は、第１と第２の秘密キーの間の相互関連性の度合いを評価して、それらが共有秘密キー（例えば、実質的に一致するかまたは同一の秘密キー情報）を構成するかどうか判断しうる。更に、コンパレータ２１４は、メモリ２１２に格納された依頼または命令または暗号キーとその他如何なる通信に含まれる情報を比較して、その通信が認可されるかどうか判断するために二者間の相互関連性の度合いを評価しうる。

【００４８】

また、処理ユニット２０８は、オーセンチケータ２１６を備えるか、またはオーセンチケータ２１６と通信可能に連結される。図中、オーセンチケータ２１６およびコンパレータ２１４が別々のブロックとして示されているが、幾つかの実施例では、ソフトウェア且つ又はその他の構造を使用してオーセンチケータ２１６とコンパレータ２１４を統合しうる。この実施例では、制御装置からの情報がセキュリティモジュール２００に格納された秘密キーと十分な相互関連性（例えば共有秘密キー）を有するとコンパレータ２１４が判断すると、セキュリティモジュール２００、オーセンチケータ２１６が制御装置の委託を行う。

【００４９】

セキュリティモジュール２００が連結された制御装置に供給される電力の量を制御するために、セキュリティモジュール２００には電力制御装置２１８が備えられている。図示される実施例では、例えばマーシャリング・キャビネット１３６ａ－ｂのうちの一つに存在しうるまたは制御装置と関連しうる電源（例えば図５の電源５０４）が、制御装置との通信を可能にするべく通信チャネルインターフェースに電力を供給するためにセキュリティモジュール２００に電力を供給する。図示される実施例において、電力制御装置２１８は、外部電源供給によりセキュリティモジュール２００に供給される電力を条件付けたり、調整したり、および昇圧したり且つ又は降圧したりするように構成される。例示的な実施形態の幾つかでは、可燃性または燃焼性の環境において発火の危険性を著しく減少またはゼロにするべく、制御装置と通信するのに使用される且つ又は制御装置に供給される電力の量を制限するように電力制御装置２１８を構成しうる。

【００５０】

電源から受けた電力をセキュリティモジュール２００用の電力に変換するために、セキュリティモジュール２００には電力変換装置２２０が備えられている。図示される実施例において、セキュリティモジュール２００を実施するために使用される回路構成は、セキュリティモジュール２００が連結されている制御装置により必要とされる電圧レベルとは異なる一種又は複数種の電圧レベル（例えば３．３Ｖ）を使用する。電力変換装置２２０は、セキュリティモジュール２００に対して電源から受けた電力を使用して制御装置と通信するために異なる電圧レベルを供給するように構成される。図示される実施例において、電力変換装置２２０により生成された電源出力は、セキュリティモジュール２００およびそれに連結された制御装置に電力を供給するため、およびセキュリティモジュール２００と制御装置との間で情報を通信するために使用される。幾つかの制御装置通信プロトコルは、その他の通信プロトコルよりも比較的高いまたは低い電圧レベル且つ又は電流レベルを必要とする。図示される実施例において、電力制御装置２１８は、制御装置に電力を

供給するため、および制御装置と通信するための電圧レベルを提供するように電力変換装置２２０を制御する。

【００５１】

制御装置から且つ又は、セキュリティモジュール２００が連結されているシステムのその他如何なる構成部分からセキュリティモジュール２００の回路構成を電気的に絶縁するために、セキュリティモジュール２００には一つ又は複数のアイソレーション（絶縁）装置（複数可）２２２が備えられている。アイソレーション装置（複数可）２２２は流電アイソレータ且つ又は光アイソレータを使用して実施されうる。例示的なアイソレーション構成を、図５を参照して以下に詳述する。

【００５２】

アナログおよびデジタル信号間で変換を行うために、セキュリティモジュール２００には、デジタル／アナログ変換器２２４およびアナログ／デジタル変換器２２６が備えられている。デジタル／アナログ変換器２２４は、受け取ったデジタル表現の値（例えば測定値）または情報を、システム（例えば図１のプロセス制御システム１００）における更なる通信に向けてアナログ値または情報変換するように構成される。同様に、アナログ／デジタル変換器２２６は、受け取ったアナログ値または情報を、システム（例えば図１のプロセス制御システム１００）における更なる通信に向けてデジタル表現の値または情報に変換するように構成される。システム内の通信が全てデジタル且つ又は全てアナログである代替的な例示的な実施形態では、デジタル／アナログ変換器２２４且つ又はアナログ／デジタル変換器２２６をセキュリティモジュール２００から省略しうる。

【００５３】

セキュリティモジュール２００が連結されている制御装置との通信を制御するために、セキュリティモジュール２００には制御装置通信プロセッサ２２８が備えられている。制御装置通信プロセッサ２２８は、情報が、セキュリティモジュール２００の連結されている制御装置に通信するのに正しい形式および電圧タイプ（例えばアナログまたはデジタル）であることを保証する。また、セキュリティモジュール２００の連結されている制御装置が、デジタルのパケット化された情報を使用して通信するように構成されている場合、制御装置通信プロセッサ２２８は、情報をパケット化または非パケット化するようにも構成される。加えて、制御装置通信プロセッサ２２８は、制御装置から受け取った情報を抽出して当該の情報をそれ以降の別のシステム構成部分への通信に向けてアナログ／デジタル変換器２２６に且つ又は外部バス通信プロセッサ２０６に通信するように構成される。

【００５４】

また、セキュリティモジュール２００をそれが物理的に連結される制御装置に通信可能に連結するように構成された制御装置インターフェース２３０が、例示的なセキュリティモジュール２００には備えられている。例えば、制御装置通信プロセッサ２２８によりパケット化された情報を、セキュリティモジュール２００の連結されている制御装置の内部バスを通じての送信に向けて制御装置インターフェース２３０へと通信しうる。

【００５５】

図示される実施例では、制御装置通信プロセッサ２２８が、受け取った情報にタイムスタンプを生成するようにも構成されうる。セキュリティモジュール２００でタイムスタンプを生成することによって、ミリセカンド未満の範囲のタイムスタンプ精度を用いてシークエンスオブイベンツ（ＳＯＥ）動作を円滑に実施することが可能になる。例えば、タイムスタンプおよびめいめいの情報をワークステーション１１８に通信することができる。その後、例えばワークステーション１１８（図１）（またはその他如何なるプロセッサシステム）により行われるシークエンスオブイベンツ動作は、動作の特定の状態（例えば、故障モード）が発生した原因を判定するために該動作の特定の状態の発生前、発生中、且つ又は発生後に何が起こったかを分析するために使用することができる。また、ミリセカンド未満の範囲でタイムスタンプを生成することによって、比較的高度な細分性で事象を捕らえることが可能になる。例示的な実施形態の幾つかにおいて、制御装置通信プロセッサ２２８および処理ユニット２０８は同じマイクロプロセッサまたはマイクロコントロー

ラを使用して実施することができる。

【００５６】

制御装置またはセキュリティモジュール２００と関連した秘密キー、コード、指示、識別、状態またはその他の情報を表示するために、セキュリティモジュール２００には表示ディスプレイ２３２が備えられている。オーセンチケータ２１６が制御装置の委託を行わない場合、表示ディスプレイ２３２は、委託の試みが失敗したことを示す情報を提示しうる。セキュリティモジュール２００が二人制認可を必要とする場合、表示ディスプレイ２３２は、（例えば、制御装置且つ又はセキュリティモジュール２００から受け取った認可情報、指示、などを含む）情報を、認可に関与する人員のうちの１人へと提供しうる。加えて、表示ディスプレイ２３２は、制御装置活動情報（例えば操作・保守情報など）、データタイプ情報（例えばアナログ信号、デジタル信号など）、且つ又はその他如何なる制御装置情報を表示するために使用することができる。セキュリティモジュール２００が複数の制御装置に通信可能に連結されるように構成される場合、表示ディスプレイ２３２は、セキュリティモジュール２００に通信可能に連結された全ての制御装置に関連する制御装置情報を表示するために使用することができる。図示される実施例において、表示ディスプレイ２３２は液晶ディスプレイ（ＬＣＤ）を使用して実施される。但し、その他の例示的な実施形態では、その他如何なる適切なタイプの表示装置を使用して表示ディスプレイ２３２を実施することができる。

【００５７】

また、セキュリティモジュール２００には入力装置２３４も備えられている。入力装置２３４は、オペレータにより、例えば表示ディスプレイ２３２を介した少なくとも幾つか認可またはその他の情報の提示に応答してセキュリティモジュール２００へと情報を入力するために使用されうる。例えば、二人制認可中に、以下に詳述される如く、制御装置のオペレータは、制御装置に送られた依頼または命令から生成され且つ表示ディスプレイ２３２に示される秘密キーに応答してセキュリティモジュール２００へとコードまたは命令を入力しうる。入力装置２３４は、個人によるアクションを登録するために使用されうるキーパッド、タッチスクリーン、タッチパネル、ボタン、スイッチまたはその他如何なる適切な装置を含みうる。

【００５８】

また、セキュリティモジュール２００が制御装置用通信ソフトおよび電子機器を含む構成では、セキュリティモジュール２００に通信ユニット２３６が備えられている。例示的な通信ユニット２３６が米国出願書第１２／２３６，１６５号に記載されている。

【００５９】

図３は、例示的なセキュリティモジュール２００および例示的な制御装置４００（ここに記載された例示的なセキュリティモジュール且つ又は制御装置の如何なるものを表しうる）の例示的な機械的接続の平面図を表し、図４は同側面図を表す。図示される実施例において、例示的なセキュリティモジュール２００は、本体２０１と、セキュリティモジュール２００を制御装置４００へと通信可能に連結する（且つ又は電気的に連結する）一つ又は複数の接触子４０４（例えばピン、ツメ、配線など）を含む。この実施例において、セキュリティモジュール２００は、介在するベース４０２を介して制御装置４００に連結される。例えばＩ／Ｏバスからの導電性通信媒質（例えばワイヤエンド）をつなぎ止める、または終端処理する、或いは確保する装置インターフェース機構でありうる留め金具４０６（例えばネジ）がベース４０２には備えられている。セキュリティモジュール２００がベース４０２に取り外し可能な状態で連結される場合、セキュリティモジュール２００と制御装置４００の間で信号を送り情報を通信すること可能にするべく、留め金具４０６が接触子４０４の一つ又は複数に連通される。その他の例示的な実施形態では、留め金具４０６の代わりにその他如何なる適切なタイプのフィールド装置インターフェース機構（例えばソケット）をベース４０２に備えうる。

【００６０】

セキュリティモジュール２００を制御装置４００へ通信可能に連結するために、ベース

４０２には制御装置接触子またはコネクタ４０８が備えられている。ユーザが制御装置４００にベース４０２を差し込むと、制御装置コネクタ４０８が制御装置４００の内部バスを係合する。制御装置コネクタ４０８は、例えばパンチブロックのようなインターフェースを含む如何なる適切なインターフェースを使用して実施されうる。セキュリティモジュール２００と制御装置４００間における情報の通信を可能にするために、制御装置コネクタ４０８は、セキュリティモジュール２００の接触子４０４の一つ又は複数に接続されている。

【００６１】

図示される実施例において、セキュリティモジュール２００は、セキュリティモジュール２００且つ又はセキュリティモジュール２００と制御装置４００の接続　を周囲の環境から保護するために使用されうるカバー４１０（図３において取り除かれた）も備える。カバー４１０は、水分且つ又はその他の有害な（若しくは損傷をもたらしうる）環境条件が当該状態にさらされうるプロセス区域におけるセキュリティモジュール２００に悪影響をもたらすことを防ぐ。カバー４１０は、適切な如何なるプラスチックや金属または、通信モジュール４００を密閉若しくは保護するのに適切なその他の材料で作製しうる。

【００６２】

図４に示される如く、ベース４０２には、外部表示ディスプレイへとセキュリティモジュール２００を通信可能に連結するべくオプショナルの表示インターフェースコネクタ４１２を備えうる。

例えば、セキュリティモジュール２００が表示ディスプレイ２３２なしで実施される場合、セキュリティモジュール２００は、外部表示ディスプレイへ指令、警告、エラー、コード、数値またはその他如何なる情報を出力するために表示インターフェースコネクタ４１２を使用できる。

【００６３】

図５は、セキュリティモジュール１５０、そして例えばＬＡＮ１２４且つ又は内部Ｉ／Ｏバス１４４を制御装置１２０から電気的に絶縁するために図１の例示的なセキュリティモジュール１５０に接続して実施されうるアイソレーション回路の構成を描く。この実施例においてセキュリティモジュール１５０が図示されているが、その他如何なるセキュリティモジュールを同じまたは類似した様態でその他如何なる制御装置に連結しうる。図示される実施例において、セキュリティモジュール１５０はセキュリティモジュール回路構成５０２（例えば図２を参照して上述される一つ又は複数のブロック）を含む。また、セキュリティモジュール１５０は、内部Ｉ／Ｏバス１４４および電源５０４に接続されている。

【００６４】

セキュリティモジュール回路構成５０２を内部Ｉ／Ｏバス１４４から電気的に絶縁するために、セキュリティモジュール１５０にはアイソレーション回路５０６が備えられている。

このように、セキュリティモジュール回路構成５０２は、電力サージまたはその他の電力変動が制御装置１２０内で生じた場合、内部Ｉ／Ｏバス１４４の電圧への影響なく、およびＩ／Ｏカード１４０ａ（図１）を破損をもたらすことなく制御装置１２０の電圧レベルに追従（例えば浮動）するように構成することができる。セキュリティモジュール１５０において実施されるアイソレーション回路５０６およびその他如何なるアイソレーション回路は光学アイソレーション回路または流電アイソレーション回路を使用して実施されうる。

【００６５】

セキュリティモジュール回路構成５０２を電源５０４から絶縁するために、セキュリティモジュール１５０にはアイソレーション回路５０８が備えられている。電源５０４からセキュリティモジュール回路構成５０２を絶縁することにより、制御装置１２０に関連した如何なる電力変動（例えば電力サージ、電流の瞬時過渡現象、など）が電源５０４に破損をもたらすことがなくなる。また、セキュリティモジュール１５０における如何なる電

力変動が、例えばその他のセキュリティモジュール１５２を含むその他のシステム構成部分の動作に障害をもたらしたり、または悪影響を及ぼしたりしなくなる。

【００６６】

一般に、アイソレーション回路は制御装置の中に備えられており、よって、セキュリティーシステムが利用できる空き容量が減る。但し、図５の例示的な実施例に示される如くセキュリティモジュール１５０の中にアイソレーション回路５０６および５０８を備えることにより、選択的にアイソレーション（絶縁）を必要とするセキュリティモジュールだけでアイソレーション回路を使用することが可能になる。例えば、図１のセキュリティモジュール１５０－１５８のうち幾つかはアイソレーション回路なしで実施しうる。

【００６７】

図６および図７は、セキュリティモジュール（例えば図１および図２のセキュリティモジュール１５０－１５８および２００）を実施するために使用されうる例示的な方法のフローチャートである。例示的な実施形態の幾つかにおいて、図６および図７の例示的な方法は、プロセッサ（例えば図８の例示的なプロセッサシステム８１０に示されるプロセッサ８１２）による実行向けのプログラムを構成する機械可読指示を使用して実施されうる。周知の様態で、プロセッサと関連する且つ又はファームウェア且つ又は専用ハードウェアにおいて具現化されたＣＤ－ＲＯＭ、フロッピー（登録商標）ディスク、ハードドライブ、デジタル多用途ディスク（ＤＶＤ）またはメモリのような有形コンピュータまたはプロセッサ可読媒体に格納されたソフトウェアにおいて該プログラムを具現化しうる。更に、例示的な方法が図６および図７に示されるフローチャートを参照して説明されているが、通常の技術を有する当業者であれば、ここに記載される例示的なセキュリティモジュール１５０－１５８および２００を実施するその他多くの方法をその代わりに使用しうることが容易に理解できるだろう。例えば、ブロックの実行順序は変更しえるものであり、且つ又は、ここに記載されるブロックのうちの幾つかを変更、除外、または組み合わせることが可能である。

【００６８】

図１の例示的なセキュリティモジュール１５０に関連して図６および図７の例示的な方法を説明する。具体的に、図６および図７のフローチャートは、例示的なセキュリティモジュール１５０がどのように制御装置１２０を認証してそれに関連するアクションを認可するかを説明するのに用いられる。但し、図６および図７の例示的な方法は、更に概して言うとその他如何なるセキュリティモジュール（例えばモジュール１５２－１５８、２００など）を実施するのに使用されうる。

【００６９】

図６を詳細にわたって参照するに、初期段階において、セキュリティモジュール１５０は制御装置１２０に連結され、またセキュリティモジュール１５０は、それが制御装置１２０を検出したかどうか判断する（ブロック６０２）。例えば、セキュリティモジュール１５０が電気的接続を成す場合、セキュリティモジュール１５０は制御装置１２０を検出して割り込みまたは状態レジスタを受け取るか、またはさもなければ制御装置１２０を検知する。制御装置１２０が検出されないと、制御装置１２０（またはその他如何なる制御装置）が検出されるまで制御がブロック６０２に留まる。

【００７０】

一旦制御装置１２０が検出されると、セキュリティモジュール１５０は制御装置情報を得る（ブロック６０４）。例えば、読み取り機構２１０は、制御装置に格納された情報を読み出す。かかる情報には、シリアル番号、製造元且つ又は機種の指標および、制御装置のタイプおよび可能な用途を判断することに関連しうるその他如何なる情報などが含まれる。特に、制御装置情報は共有秘密キーまたは共有秘密キーの一部を含みうる。

【００７１】

それから、セキュリティモジュール１５０は、ブロック６０４で得られた情報（得られた秘密キー情報の如何なるもの）をセキュリティモジュール１５０に格納された秘密キーと比較する（ブロック６０５）。ブロック６０５で比較を行った後に、セキュリティモジ

ュール１５０は、得られた制御装置情報が共有秘密キーを含む（即ち、セキュリティモジュール１５０に格納された秘密キーが制御装置１２０から得られた如何なる秘密キー情報と実質的にまたは完全に一致する）かどうか判断する（ブロック６０６）。例えば、コンパレータ２１４は、制御装置情報を分析して、当該情報の如何なるものが、セキュリティモジュール１５０のメモリ２１２に格納されたその他の情報（例えば共有秘密キーを含む）に一致するかさもなければ相互に関連するかどうかを評価する。相互関連性が見つからない場合、セキュリティモジュール１５０はエラーメッセージを表示しうる（ブロック６０８）。制御装置情報および共有秘密キーの間に相互関連性がない場合、それは、プロセス制御システム１００の当該位置に設置されている制御装置が正しくないことを示しうる。それに加えて、又はその代わりとして、相互関連性がない場合、それは、当該特定の制御装置に正しいセキュリティモジュールが備えられていないことを示しうる。例えば、制御装置は、異なるまたはより制限の厳しいセキュリティ機能特性を備えたセキュリティモジュールを必要としうる。セキュリティに細心の注意を払う必要性の比較的低い制御装置用のセキュリティモジュールでは、この実施例におけるシステムを適切に保護してその安全を確保できないことになる。セキュリティモジュール１５０に格納されている秘密キーと制御装置情報との間に相互関連性がないと判断された場合、制御装置の委託が妨げられて（ブロック６１０）、その工程が終了する。この場合、制御装置１２０は作動不能のままになる。

【００７２】

制御装置情報および共有秘密キーの間に相互関連性があると判断された場合（ブロック６０６）、セキュリティモジュール１５０は制御装置の認証を始める（ブロック６１２）。認証は、制御装置１２０がプロセス制御システムにおける当該の位置に適切な装置であること、且つ又はセキュリティモジュール１５０が制御装置１２０に適切なセキュリティモジュールである（例えば、適切なセキュリティ機能特性を含んでいる）ことを示す指標である。認証指標を提供するために、処理ユニット２０８のオーセンチケータ２１６は例えば制御装置１２０が認証されていることを示す信号を生成しうる、且つ又は制御装置１２０が作動することを可能にするべく、オーセンチケータが通信且つ又は電気的な限定または停止を出しうる。よって、認証により、安全な通信状態が制御装置１２０のために確立される。加えて、オーセンチケータ２１６は、例えば制御システム１００内の通信の宛先を指定する目的でシステムにおいて制御装置１２０を同定するために使用される例えば英数字の文字列などのアイデンティティを制御装置１２０に提供しうる。（ブロック６１４）。また、オーセンチケータ２１６は、制御装置１２０に役割を割り当てる（ブロック６１６）。該役割は、例えば制御装置１２０が通信、監視且つ又は制御しうるフィールド装置を含みうるシステムにおいて制御装置１２０が行いうるアクション、制御装置１２０が与えることができる命令、および制御装置１２０が行えるその他のアクションの指標を提示しうる。加えて、オーセンチケータ２１６は、制御装置１２０の構成を円滑に実施しうる（ブロック６１８）。制御装置１２０の構成には、システムにおいて制御装置１２０がそれの役割を行うのに必要なデータまたはその他如何なる情報またはツール且つ又は制御パラメータへのアクセスを提供することが含まれる。

【００７３】

制御装置１２０が委託された（例えばブロック６１２－６１８）後、制御装置１２０はシステム１００の作動中に依頼および命令を受け取る。セキュリティモジュール１５０は、制御装置１２０の通信を監視し、依頼または命令が制御装置１２０で受け取られるかどうか判断する（ブロック６２０）。依頼または命令が制御装置で受け取られない場合、制御がブロック６２０に留まる。依頼または命令が受け取られた場合、セキュリティモジュール１５０は、制御装置１２０が依頼または命令に応答して適切に使用されるかを判断する。依頼または命令に応答して制御装置１２０がアクションを行う認証を得られるかどうか判断するために、セキュリティモジュール１５０は、依頼または命令に含まれる暗号化情報の如何なるものをメモリ２１２に格納された一つ又は複数の暗号キーと比較する（ブロック６２２）。アクションが認可されたことをセキュリティモジュール１５０の暗号キ

ーが示す場合（ブロック６２４）、セキュリティモジュール１５０は、制御装置１２０が依頼または命令を処理することを可能にし（ブロック６２６）、それ以降の通信（複数可）に向けて制御がブロック６２０に戻る。

【００７４】

それに加えて、又はその代わりとして、暗号化ベースの認可は、検証技法、カギ管理技法および対妨信技法を含むその他の承認技法に取り替え（または置き換え）ても良い。更に、幾つかの実施例では、セキュリティモジュールが、制御装置１２０と通信することを許された装置の、または制御装置１２０が行えるアクションの、ホワイトリストを維持管理しうる。セキュリティモジュール１２０がホワイトリストまたはその他の事前承認リストを維持管理する場合、図６の介在する動作中に実行される比較およびその他のアクションなしで、装置から前承認済みの依頼または命令を受け取る工程、且つ又は前承認済みの装置から通信を受ける工程（ブロック６２０）から、通信（複数可）に含まれる依頼または命令を認可および処理する工程（ブロック６２６）へと処理が進む。

【００７５】

但し、アクションが認可されていないと判断されると（ブロック６２４）、セキュリティモジュール１５０は、例えば制御装置１２０が依頼または命令を含む通信に応答してアクションを行うのを妨げる（ブロック６２８）ことにより、認可れていないアクションに対して制御装置１２０（および全システム１００）を保護する。その後、次回通信に向けて制御がブロック６２０に戻る。

【００７６】

図７は、アクション（例えば制御装置による制御動作）の二人制認可を実施するべく図１および図２のセキュリティモジュールを実施するのに使用されうる例示的な方法のフローチャートを表す。プロセス制御システムにおける幾つかの動作は、十分セキュリティに細心の注意を払うべきものであり、よって例えば制御室にオペレータまたはエンジニアを、そして装置の所に別の人員を配置することが要求される、即ち、当該動作を行うには、制御装置１２０のアクションの二人制認可が要求される。

【００７７】

例示的な方法は、第１の個人（例えば制御室１０２における人員）に関連した依頼または命令が制御装置１５０で受け取られたかどうかの判断から始まる（ブロック７０２）。かかる依頼または命令を含んだ通信が受け取られない場合、かかる通信が受け取られるまで、制御はブロック７０２に留まる。但し、かかる依頼または命令が受け取られた場合、セキュリティモジュール１５０または、動かないように制御装置に連結された（例えば、内部統合化された）その他のセキュリティ構成部分が、第１の個人により送られた依頼または命令と関連する秘密キーを取得する（ブロック７０４）。幾つかの実施例では、セキュリティモジュール１５０または、動かないように制御装置に連結された（例えば、内部統合化された）その他のセキュリティ構成部分により取得されるべき秘密キーが生成される。秘密キーは、如何なるタイプのキーワードおよびコード、暗号、パルス、光帯、音、またはその他如何なるタイプの個人的な通信または鍵でありうる。

【００７８】

その後、秘密キーは、受け取った依頼または命令に応答したアクションについて認可を（必要に応じて）与える第２の個人（例えば、制御装置１２０が実際に設置されている現場にいる人員）に提供される（ブロック７０６）。幾つかの実施例では、第２の個人が閲覧できるように秘密キーが表示ディスプレイ２３２上に表示される。その他の実施例における秘密キーは、その他如何なる表示ディスプレイ（例えばワークステーション１１８に）に送られるか、またはさもなければ、セキュリティモジュール１５０を介して第２の個人に提示されうる。

【００７９】

その後、第２の個人は、例えばセキュリティモジュール１５０、第１の個人且つ又は制御装置１２０に秘密キーを送り返すことを含むアクションを実行する。幾つかの実施例では、第２の個人が、セキュリティモジュールの入力装置２３４を介して秘密キーを送り返

すアクションを入力する。（これには、第１の個人へと秘密キーを転送するという指示をタイプ入力するという作業を含みうる。）幾つかの実施例では、秘密キーが、第２の個人から依頼のソース（例えば制御室１０２におけるワークステーション１１８）に送られ、その後制御装置１２０に送り返される。秘密キーが送り返されると、若しくは第２の個人が制御装置のアクションを認可するためのアクションを実行したと判断されると（ブロック７０８）、セキュリティモジュール１５０は、依頼または命令に応答してアクションが認可されたことを認識し、またセキュリティモジュール１５０は、依頼または命令を処理することを制御装置に認可する（ブロック７１０）。その後、別の通信が受け取られるまで、制御がブロック７０２に戻る。例えば、所定の時間が経過した後になっても第２の個人が秘密キーを送り返していない場合（ブロック７０８）、別の通信が受け取られるまで、制御がブロック７０２に戻る。よって、ブロック７０８は、あらかじめ定められた時間間隔が経過した後にタイムアウトすることを含む動作を含みうる。

【００８０】

図８は、ここに記載される機器および方法を実施するのに使用されうる例示的なプロセッサシステム８１０のブロック図である。例えば、例示的なプロセッサシステム８１０に類似するまたはそれと同一であるプロセッサシステムは、図１のワークステーション１１８、制御装置１２０、１２２および１２６ａ－ｃ、Ｉ／Ｏカード１４０ａ－ｄおよび１４２ａ－ｄ、且つ又はセキュリティモジュール１５０－１５８を実施するために使用されうる。以下、例示的なプロセッサシステム８１０が複数の周辺機器、インターフェース、チップ、メモリなどを含んだ状態で説明されているが、一つ又は複数のワークステーション１１８、制御装置１２０、１２２および１２６ａ－ｃ、Ｉ／Ｏカード１４０ａ－ｄおよび１４２ａ－ｄ、且つ又はセキュリティモジュール１５０－１５８を実施するために使用されるその他の例示的なプロセッサシステムから当該素子の一つ又は複数を省略しても良い。

【００８１】

図８に示される如く、プロセッサシステム８１０は、相互接続バス８１４に連結されるプロセッサ８１２を含む。プロセッサ８１２は、レジスタセットまたはレジスタ領域８１６を含む。図８では、該レジスタセットまたはレジスタ領域８１６が全てチップ上に形成された状態で描かれているが、その代わりとして、全体的にまたは部分的にチップの外部に配置し、専用の電気配線を介して且つ又は相互接続バス８１４を介してプロセッサ８１２に直接連結するようにしても良い。図８には示されていないが、システム８１０は、マルチプロセッサ・システムでありえ、よって、プロセッサ８１２と同一であるか類似しているものであり且つ相互接続バス８１４に通信可能に連結される一つ又は複数の付加的なプロセッサを含みうる。

【００８２】

図８のプロセッサ８１２は、メモリーコントローラ８２０および周辺入出力（Ｉ／Ｏ）コントローラ８２２を含むチップセット８１８に連結される。周知の如く、一般にチップセットは、チップセット８１８に連結される一つ又は複数のプロセッサによりアクセス可能なまたはそれにより使用される複数の汎用且つ又は専用レジスタやタイマーなどに加え、入出力および記憶管理機能を備えている。メモリ制御器８２０は、プロセッサ８１２（または、複数のプロセッサが備えられている場合は複数のプロセッサ）がシステムメモリ８２４および大容量記憶メモリ８２５にアクセスできるようにする機能を果たす。

【００８３】

システムメモリ８２４は、例えば静的ランダムアクセス記憶装置（ＳＲＡＭ）、動的ランダムアクセス記憶装置（ＤＲＡＭ）、フラッシュメモリ、読み取り専用メモリ（ＲＯＭ）など所望するあらゆるタイプの揮発性且つ又は不揮発性メモリを含みうる。大容量記憶メモリ８２５は、所望するあらゆるタイプの大容量記憶装置を含みうる。例えば、例示的なプロセッサシステム８１０がワークステーション１１８（図１）を実施するために使用される場合、大容量記憶メモリ８２５としては、ハードディスクドライブ、光ドライブ、テープ記憶装置などが挙げられる。或いは、例示的なプロセッサシステム８１０が制御装

置１２０、１２２および１２６ａ－ｃ、Ｉ／Ｏカード１４０ａ－ｄおよび１４２ａ－ｄ、且つ又はセキュリティモジュール１５０－１５８を実施するために使用される場合、大容量記憶メモリ８２５としては、ソリッドステートメモリ（例えばフラッシュメモリ、ＲＡＭメモリ、など）、磁性記憶装置（例えばハードドライブ）、または制御装置１２０、１２２および１２６ａ－ｃ、Ｉ／Ｏカード１４０ａ－ｄおよび１４２ａ－ｄ、且つ又はセキュリティモジュール１５０－１５８における大容量記憶に適しているその他如何なるメモリなどが挙げられる。

【００８４】

周辺Ｉ／Ｏコントローラ８２２は、プロセッサ８１２が周辺機器Ｉ／Ｏバス８３２を介して周辺機器入・出力（Ｉ／Ｏ）装置８２６，８２８およびネットワーク・インターフェース８３０と通信することを可能にする機能を行う。Ｉ／Ｏ装置８２６および８２８は、例えばキーボード、表示ディスプレイ（例えば液晶ディスプレイ（ＬＣＤ）、ブラウン管（ＣＲＴ）ディスプレイ、など）、ナビゲーション装置（例えばマウス、トラックボール、容量性タッチパッド、ジョイスティック、など）などのような所望する如何なるタイプのＩ／Ｏ装置でありうる。ネットワーク・インターフェース８３０は、プロセッサシステム８１０が別のプロセッサシステムと通信することを可能にする例えばイーサネット（登録商標）装置、非同期転送モード（ＡＴＭ）装置、８０２．１１装置、ＤＳＬモデム、ケーブルモデム、セルラーモデムなどでありうる。

【００８５】

メモリーコントローラ８２０とＩ／Ｏコントローラ８２２がチップセット８１８内の別々の機能的ブロックとして図８に表されているが、これらのブロックにより行われる機能は、単一の半導体回路内に統合しても良いし、または別々の集積回路を二つ以上使用して実施しても良い。

【００８６】

ここに記載される例示的な方法およびシステムでは、プロセス制御システムのオペレータが複数の制御装置に交換可能な状態で連結できる複数のセキュリティモジュールを採用できるという利点を提供する。また、これによって、プロセス制御システムのオペレータは、制御装置のセキュリティプログラムを素早く簡単に変更することができるようになる。例えば、プロセス制御システムにおける特定の制御装置にとってより有利であろう特定の性能特性またはその他の利点および保護性能を有する一式のセキュリティ機能、レベルまたは特徴が別に存在する場合、オペレータは、制御装置のセキュリティプログラムを、ある一式のセキュリティ機能、レベルまたは機能特性から、該他方の一式のセキュリティ機能、レベルまたは機能特性に変更することを希望しうる。加えて、オペレータは、当初装置が製造された時には存在しなかった改訂またはアップグレードされたセキュリティプログラムまたは特定の機能特性を含むように制御装置を更新することを希望しうる。

【００８７】

加えて、業界標準を正式に採用する前にシステムに組み込まれた一般公開前の最先端装置およびセキュリティ機能特性を含むプロセス制御システムのオペレータは、適切な業界標準に適合するように装置を更新するべく一般公開前の制御装置の一つに業界標準を組み込んだここに記載される例示的なセキュリティモジュールの一つを連結することができる。

【００８８】

ここに記載される例示的なセキュリティモジュールにより具現化される別の利点は、セキュリティ機能特性や委託情報など全てを変更せずに、セキュリティモジュールに連結された制御装置を変更しうるということである。加えて、該セキュリティモジュールの幾つかの実施例には、制御装置から情報を収集するために使用されうる診断ソフトウェアを含みうる。オペレータは、セキュリティモジュールを所望の診断ソフトウェアを有する別のセキュリティモジュールに変更することにより、より新しい、より良い、より装置に適した診断法を利用しうる。例えば、制御装置の特定の状態をより良く評価するために新しい診断テストが開発されうる。ここに記載される例示的なセキュリティモジュールでは、既

存制御装置の制御装置自体または電子回路基板を変えることなく確立済みの制御装置で新しい診断テストを実施しうる。

【００８９】

更に、制御装置の製造メーカは、セキュリティ電子機器およびソフトウェア且つ又は診断電子機器およびソフトウェアを制御装置のそれ以外の電子機器から離すことができるので、制御装置用に開発したり、製造したり、在庫保管したりなどする必要のある回路基板の種類が少なくて済む。例えば、製造メーカが、二つの異なるセキュリティプログラムをそれぞれ備える制御装置を５台の提供する場合、１０枚の回路基板（装置とプログラムの各組み合わせにつき一枚）を生産する必要がある。ここに記載される例示的なセキュリティモジュールを使用すれば、５枚の回路基板（各装置につき一枚）だけで済むので、２種類ののセキュリティモジュール（各プログラムにつき１種類）を生産すればよくなる。よって、製造メーカの開発および保管コストが大幅に削減される。加えて、セキュリティモジュールはその他の制御装置と共に使用することができる。

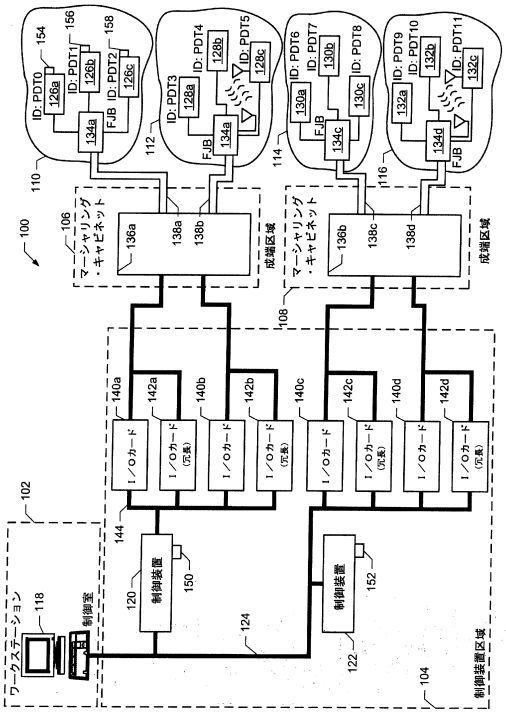
【００９０】

更にまた、図５を参照して上述されるアイソレーション回路構成は、例示的なセキュリティモジュールに連結された電源および制御装置を保護する。電気的なスパイク（瞬時過渡現象）または電気工による不注意な配線引き回しにより許容できないほど高い電圧または電流負荷が生じた際には、アイソレーション回路がセキュリティモジュールに過大荷重を吸収させる。従って、セキュリティモジュールだけを交換する必要がありえ、制御装置の回路基板は正常に機能し続ける。よって、上記の如く、保全および修理のコストが大幅に減る。

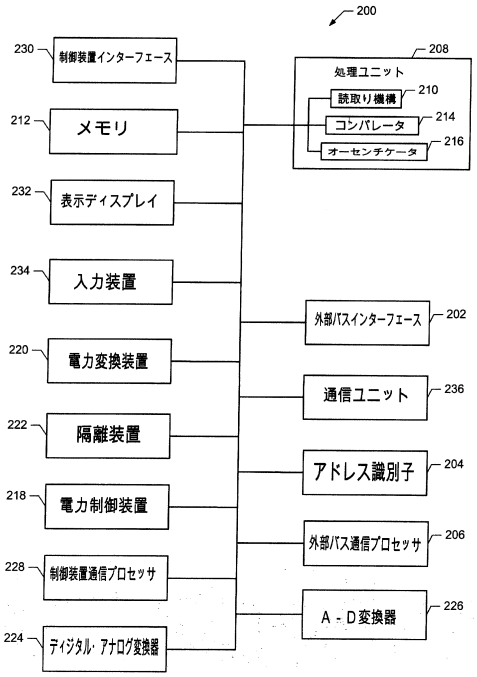
【００９１】

ここに実施例として挙げられる特定の方法、機器および製造品が記載されているが、この特許の適用領域の範囲はそれに限定されるものではない。それとは反対に、この特許は、字義的に若しくは均等論に基づいて添付の特許請求の範囲内に公正に含まれる方法、機器および製造品の全てを網羅するものである。

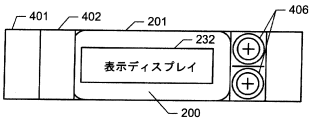
【図１】



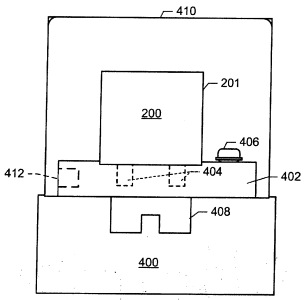

【図２】



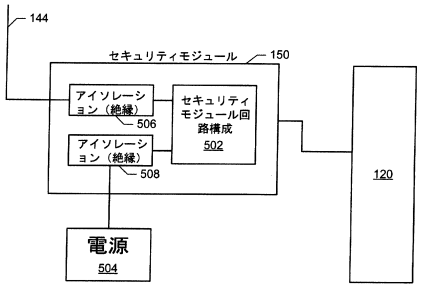

【図３】



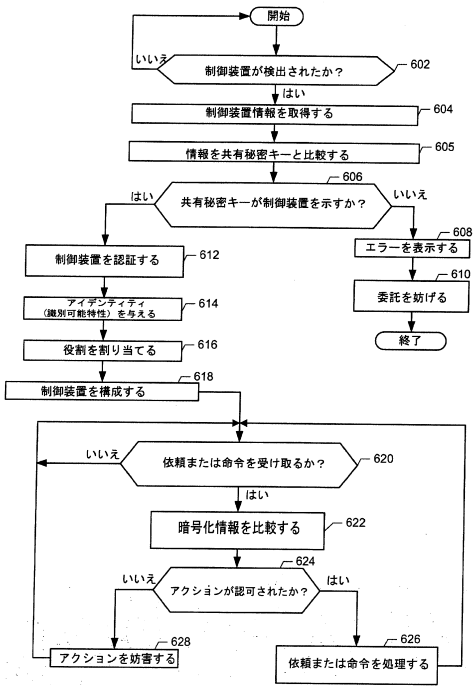

【図４】



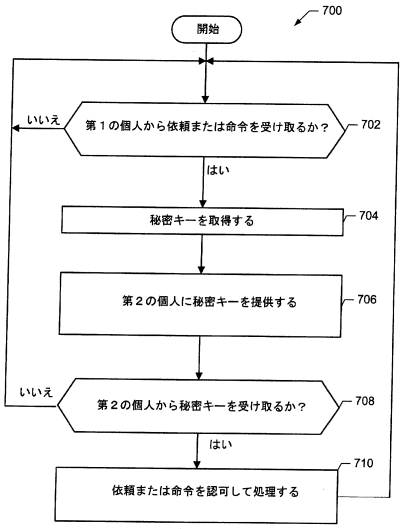

【図５】



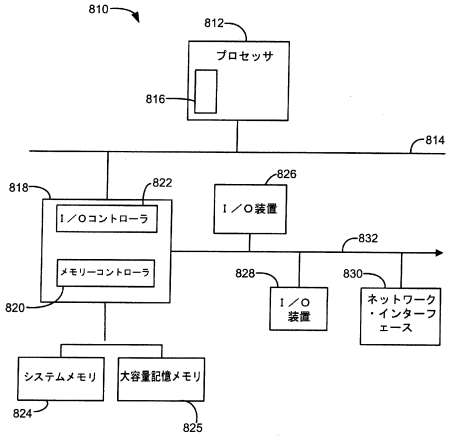

【図６】



【図７】


700
開始
第１の個人から依頼または命令を受け取るか？
いいえ
702
はい
秘密キーを取得する
704
第２の個人に秘密キーを提供する
706
第２の個人から秘密キーを受け取るか？
いいえ
708
はい
依頼または命令を認可して処理する
710

【図８】


810
812
プロセッサ
816
814
818
822
826
Ｉ／Ｏコントローラ
Ｉ／Ｏ装置
メモリーコントローラ
832
828
830
820
Ｉ／Ｏ
装置
ネットワーク
・インターフ
ェース
システムメモリ
大容量記憶メモリ
824
825

フロントページの続き

(72)発明者 ギャリー キース ロウ
アメリカ合衆国 ７８６２８ テキサス州 ジョージタウン ミッシェル コート １１０
(72)発明者 ゴドフリー ローランド シェリフ
アメリカ合衆国 ７８７１７ テキサス州 オースティン ウェスト ドーマン ドライブ １６４１０

審査官 脇岡 剛

(56)参考文献 特表２００３－５３３８１４（ＪＰ，Ａ）
特開２００７－０１３４３９（ＪＰ，Ａ）
特開２００３－０２２４０８（ＪＰ，Ａ）
特開平０８－２２１４８２（ＪＰ，Ａ）
特開平０９－１１４９４６（ＪＰ，Ａ）
特開昭６４－０７３４８５（ＪＰ，Ａ）
米国特許出願公開第２００７／０２６１１０３（ＵＳ，Ａ１）
特開２００２－２７８６０８（ＪＰ，Ａ）
国際公開第２００８／０１８７６２（ＷＯ，Ａ１）
特開２００２－２４５４２２（ＪＰ，Ａ）
特開２００４－０５４９５１（ＪＰ，Ａ）
米国特許出願公開第２００８／００２７５８７（ＵＳ，Ａ１）
米国特許出願公開第２００４／００６４６９９（ＵＳ，Ａ１）
独国特許発明第１０２００６０５８３３０（ＤＥ，Ｂ３）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／３４
Ｇ０５Ｂ ９／０２
Ｈ０４Ｌ ９／１０
Ｈ０４Ｌ ９／３２