(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6678664号
(P6678664)
(45)発行日　令和2年4月8日(2020.4.8)　(24)登録日　令和2年3月19日(2020.3.19)

(51)Int.Cl.		F I		
G06F 21/86	(2013.01)	G06F	21/86	
G06F 21/60	(2013.01)	G06F	21/60	
G05B 19/05	(2006.01)	G05B	19/05	N

請求項の数 18　(全 17 頁)

(21)出願番号	特願2017-521497(P2017-521497)
(86)(22)出願日	平成27年10月20日(2015.10.20)
(65)公表番号	特表2017-537379(P2017-537379A)
(43)公表日	平成29年12月14日(2017.12.14)
(86)国際出願番号	PCT/US2015/056538
(87)国際公開番号	WO2016/064933
(87)国際公開日	平成28年4月28日(2016.4.28)
審査請求日	平成30年10月19日(2018.10.19)
(31)優先権主張番号	62/066,267
(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)

(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　100140109
弁理士　小野　新次郎
(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の改竄防止モジュール

(57)【特許請求の範囲】

【請求項１】

安全な産業用制御システム・モジュールであって、

電気回路を含む回路基板と、

前記回路基板を収容する封止エンケースメントであって、第１ハウジング面および第２ハウジング面を有するハウジングを含み、前記第１ハウジング面および前記第２ハウジング面が連結されると前記ハウジングが前記回路基板を収容するように構成される、封止エンケースメントと、

前記封止エンケースメントと一体化された第１センサ・コンポーネントであって、前記回路基板および電気回路に通信可能に結合され、権限のないアクセス・イベントの指示を供給するように構成される、第１センサ・コンポーネントと、

当該産業用制御システム・モジュールの物理的な権限のないアクセス・イベントについての代替の指示を供給することができる第２センサ・コンポーネントであって、前記電気回路に通信可能に結合され、権限のないアクセス・イベントについての前記指示を検証するように機能する、第２センサ・コンポーネントと、

を備える、安全な産業用制御システム・モジュール。

【請求項２】

請求項１記載の安全な産業用制御システム・モジュールにおいて、前記電気回路が、高電位コンデンサ、通信モジュール、バックプレーン、電力モジュール、物理相互接続デバイス、コントローラ、メモリ、およびプロセッサの内の少なくとも１つを含む、安全な産

業用制御システム・モジュール。
【請求項３】
請求項１記載の安全な産業用制御システム・モジュールにおいて、前記センサ・コンポーネントが、光学センサ、熱センサ、振動センサ、音センサ、加速度計、および物理センサの内の少なくとも１つを含む、安全な産業用制御システム・モジュール。
【請求項４】
請求項１記載の安全な産業用制御システム・モジュールにおいて、前記権限のないアクセス・イベントが、エンケースメント封止部を破壊することを含む、安全な産業用制御システム・モジュール。
【請求項５】
請求項１記載の安全な産業用制御システム・モジュールであって、更に、
前記権限のないアクセス・イベントの指示に基づいて、セキュリティ・アクションを実施するように構成されるセキュリティ・モジュールを備える、安全な産業用制御システム・モジュール。
【請求項６】
請求項５記載の安全な産業用制御システム・モジュールにおいて、前記セキュリティ・モジュールが、高電位コンデンサまたは電源の少なくとも一方に結合されるコントローラを含む、安全な産業用制御システム・モジュール。
【請求項７】
請求項５記載の安全な産業用制御システム・モジュールにおいて、前記セキュリティ・アクションが電気ショック・イベントを含む、安全な産業用制御システム・モジュール。
【請求項８】
請求項５記載の安全な産業用制御システム・モジュールにおいて、前記セキュリティ・アクションが情報消去イベントを含む、安全な産業用制御システム・モジュール。
【請求項９】
請求項１記載の産業用制御システム・モジュールであって、更に、
前記回路基板に配置されたコネクタを備え
前記ハウジングが、前記コネクタに外部アクセスを提供するように構成される少なくとも１つのポートを含み、
前記第１センサ・コンポーネントまたは前記第２センサ・コンポーネントが、前記第１ハウジング面と一体化された電子スイッチ・アセンブリであって、前記回路基板および電気回路に電気的に結合され、前記第２ハウジング面に配置されたスイッチ・トリガによってトリガされるように構成される、電子スイッチ・アセンブリを含む、
産業用制御システム・モジュール。
【請求項１０】
請求項９記載の産業用制御システム・モジュールにおいて、前記ハウジングが少なくとも１つのキャプティブ・ファスナを含む、産業用制御システム・モジュール。
【請求項１１】
請求項９記載の産業用制御システム・モジュールにおいて、前記電子スイッチ・アセンブリが高電位コンデンサを含む、産業用制御システム・モジュール。
【請求項１２】
封止エンケースメントに収容された産業用制御システム・モジュールにおける権限のないアクセスを検出する、コンピュータにより実装された方法であって、
前記コンピュータにより実装されたコントローラを使用して、前記産業用制御システム・モジュールにおける権限のないアクセス・イベントの指示を、第１センサ・コンポーネントから受け取るステップと、
前記産業用制御システム・モジュールにおける前記権限のないアクセス・イベントの追加の指示を、第２センサ・コンポーネントから受け取るステップであって、前記追加の指示が、前記権限のないアクセス・イベントを検証するように機能する、ステップと、
前記コンピュータにより実装されたセキュリティ・モジュールを使用して、前記産業用

制御システム・モジュールにおける前記権限のないアクセス・イベントの指示に基づいて、セキュリティ・アクションを実施するステップと、
を含む、方法。
【請求項１３】
前記エンケースメントに収容された前記産業用制御システム・モジュールにおける権限のないアクセスを検出する請求項１２記載の方法において、前記権限のないアクセス・イベントが、エンケースメント封止部を破壊することを含む、方法。
【請求項１４】
前記エンケースメントに収容された前記産業用制御システム・モジュールにおける権限のないアクセスを検出する請求項１２記載の方法において、前記センサ・コンポーネントが、光センサ、熱センサ、振動センサ、および動きセンサの内の少なくとも１つを含む、方法。
【請求項１５】
前記エンケースメントに収容された前記産業用制御システム・モジュールにおける権限のないアクセスを検出する請求項１２記載の方法において、前記セキュリティ・アクションを実施するステップが、電気サージ・イベントを発生させることを含む、方法。
【請求項１６】
前記エンケースメントに収容された前記産業用制御システム・モジュールにおける権限のないアクセスを検出する請求項１２記載の方法において、前記セキュリティ・アクションを実施するステップが、暗号化アルゴリズムを実装することを含む、方法。
【請求項１７】
前記エンケースメントに収容された前記産業用制御システム・モジュールにおける権限のないアクセスを検出する請求項１２記載の方法において、前記セキュリティ・アクションを実施するステップが、情報を消去することを含む、方法。
【請求項１８】
前記エンケースメントに収容された前記産業用制御システム・モジュールにおける権限のないアクセスを検出する請求項１２記載の方法において、前記セキュリティ・アクションを実施するステップが、前記産業用制御システム・モジュールを、破壊熱または破壊電磁場の内の少なくとも一方にさらすことを含む、方法。
【発明の詳細な説明】
【関連出願】
【０００１】
関連出願の相互参照
[0001] 本出願は、２０１４年１０月２０日付けで出願された「ＴＡＭＰＥＲ ＲＥＳＩＳＴＡＮＴ ＭＯＤＵＬＥ ＦＯＲ ＩＮＤＵＳＴＲＩＡＬＣＯＮＴＲＯＬＳＹＳＴＥＭ」と題された特許米国仮出願第６２／０６６，２６７号について３５Ｕ．Ｓ．Ｃ§１１９（ｅ）の利益を享受するものである。米国仮出願第６２／０６６２６７号は、参照により本明細書に完全に組み込まれるものである。
【背景技術】
【０００２】
[0002] コンピューティング・デバイスは、自動化されたプロセスを制御するのと同様に、大量の情報を格納し、処理し、位相するための手段(instrumental)である。産業用制御システム（ＩＣＳ）は、プロセス制御システム（ＰＣＳ）、分散型制御システム（ＤＣＳ）、プログム可能ロジック・コントローラ（ＰＬＣ）ベース・システム、管理(supervisory)制御およびデータ取得（ＳＣＡＤＡ）システム等を含むことができ、通信ネットワークを利用して、製品の生産および必須のサービスの提供を促進することができる。
【発明の概要】
【課題を解決するための手段】
【０００３】
[0003] 権限のない(unauthorized)のモジュール・アクセス・イベントの指示に応じた

産業用制御システム・モジュール内の機密(sensitive)データの自己破壊(self-destruction)若しくは破壊および／または消失について、産業用制御システム・モジュールおよび方法を説明する。実装態様では、安全な産業用制御システム・モジュールは、電気回路を含む回路基板と、回路基板を収容する封止エンケースメントであって、第１ハウジング面および第２ハウジング面を有するハウジングを含み、第１ハウジング面および第２ハウジング面が連結されるとハウジングが回路基板を収容するように構成される、封止エンケースメントと、封止エンケースメントと一体化された第１センサ・コンポーネントであって、回路基板および電気回路に通信可能に結合され、権限のないアクセス・イベントの指示を供給するように構成される、第１センサ・コンポーネントと、を含む。

【０００４】

[0004] 実装態様では、耐タンパ性の産業用制御システム・モジュールは、電気回路を含む回路基板と、回路基板に配置されたコネクタと、第１ハウジング面および第２ハウジング面を有するハウジングであって、第１ハウジング面および第２ハウジング面が連結されるとハウジングが回路基板を収容するように構成され、コネクタに外部アクセスを提供するように構成される少なくとも１つのポートを含む、ハウジングと、第１ハウジング面と一体化された電子スイッチ・アセンブリであって、回路基板および電気回路に電気的に結合され、第２ハウジング面に配置されたスイッチ・トリガによってトリガされるように構成される、電子スイッチ・アセンブリと、を含む。

【０００５】

[0005] 実装態様では、封止エンケースメントに収容された産業用制御システム・モジュールにおける権限のないアクセスを検出する方法は、コントローラを使用して、産業用制御システム・モジュールにおける権限のないアクセスの指示を、第１センサ・コンポーネントから受け取るステップと、セキュリティ・モジュールを使用して、産業用制御システム・モジュールにおける権限のないアクセスの指示に基づいて、セキュリティ・アクションを実施するステップと、を含む。

【０００６】

[0006] 開示される産業用制御システム・モジュールおよびセキュリティ・アクションは、産業用制御システムまたは他の電子デバイス内における権限のないモジュール・アクセス・イベントの発生時のデータおよび情報アクセスを防止するための耐タンパ性モジュールおよび／または自己破壊デバイスを提供することができる。

【０００７】

[0007] この摘要は、詳細な説明において以下で更に説明する概念から選択したものを、簡略化した形態で紹介するために設けられている。この摘要は、特許請求する主題の主要な特徴や必須の特徴を特定することを意図するのではなく、特許請求する主題の範囲を判断するときに補助として使用されることを意図するのでもない。

【０００８】

[0008] 添付図面を参照しながら詳細な説明について記載する。説明および図における異なる実例において同じ参照番号を使用する場合、同様の項目または同一の項目を示すことができる。

【図面の簡単な説明】

【０００９】

【図１】図１は、本開示の例示の実装態様による耐タンパ性の産業用制御システム・モジュールを示す組立分解等角図である。

【図２】図２は、本開示の例示の実施形態による少なくとも１つの耐タンパ性の産業用制御システム・モジュールを含む産業用制御システムを示すブロック図である。

【図３】図３は、本開示の例示の実施形態による耐タンパ性の産業用制御システム・モジュールで使用されるコントローラを示すブロック図である。

【図４】図４は産業用制御システム環境を示し、当該産業用制御システムは、本開示の例示の実施形態による耐タンパ性の産業用制御システム・モジュールを含む。

【図５】図５は、本開示の例示の実施形態による少なくとも１つのセンサ・コンポーネン

トを含む産業用制御システム・モジュールを示すブロック図である。
【図６】図６は、本開示の例示の実施形態による封止エンケースメントに収容される産業用制御システム・モジュールの権限のないアクセスを検出する方法を示すフロー図である。
【発明を実施するための形態】
【００１０】
概要
[0015] 産業制御システム（ＩＣＳ）は、当初、単離された信頼性のあるドメインで動作するように案出されていた。しかしながら、拡張された接続技術が生産性を押し上げ、工場作業場また世界の遠隔位置の両方からの情報をレバレッジするのを許容することにより、ＩＣＳを潜在的に大多数の人々にさらしたままにする。生憎、この拡張接続技術は、対応するサイバー・セキュリティ・ソリューションを上回っており、クリティカルなシステムを高度なサイバー脅威から安全に保つために、工学技術の理解およびセキュリティ・スキルを有する人々に負担を課す。
【００１１】
[0016] ＩＣＳにおいて使用されるデータ・ストレージ・デバイスは、秘密情報(confidential information)を含む大量の情報を記録および格納することができる。幾らかの電子データ・ストレージは、格納データを格納および抽出するのに電力を必要とすることができる。データ・ストレージ・デバイスは、オフラインまたはポータブルのストレージを含むように構成され、その結果、デバイスを複数のコンピューティング・デバイスでモバイル化(mobilize)および使用することができる。機密情報(sensitive information)を有することができる追加の電子デバイスは、プロセッサのようなコンピューティング・デバイス、メモリ・モジュール（例えば、ランダム・アクセス・メモリ（ＲＡＭ）、リード・オンリ・メモリ（ＲＯＭ））および通信デバイス等を含むことができる。機密データは、これら電子データ・ストレージ・デバイスに格納することができ、暗号化およびセキュリティ対策を必要とする。
【００１２】
[0017] １つのサイバー・セキュリティ規格は、米国政府コンピュータ・セキュリティ規格を含む１４０シリーズの連邦政府情報処理規格（ＦＩＰＳ１４０）を含む。これは、暗号化モジュールについての要件を規定し、クリティカルなシステム安全性を維持するように設計されるものである。ＦＩＰＳ１４０規格は、暗号化モジュールについての要件および規格を調整する。暗号化モジュールは、米国連邦政府の部(department)や機関(agency)によって使用するハードウェアおよびソフトウェアの両方を含む。他のサイバー・セキュリティ規格は、セキュリティ機構である安全なセッション開始プロトコル（ＳＩＰ）む。これは、トランスポート層セキュリティの暗号化チャネルを通じてＳＩＰメッセージを送るためにＳＩＰＲＰＣ３２６１によって規定される。
【００１３】
[0018] しかしながら、ＩＣＳは特に、例えばＦＩＰ１４０または安全なＳＩＰのような既存のセキュリティ規格に関してであっても、権限のないアクセスを受けやすくなる場合がある。これら産業用制御システムは、産業スパイおよび技術窃盗の文脈では、機密で価値のある情報を含む場合がある。全ての電子デバイスおよび／またはデータ・ストレージ・デバイスが、安全なデータおよび／または電子デバイスへの権限のないアクセスを防止するのに充分な必須の暗号化またはセキュリティ対策を含む訳ではない。
【００１４】
[0019] したがって、権限のないモジュール・アクセス・イベントの指示に応じた産業用制御システム・モジュール内の機密データの自己破壊若しくは破壊および／または消失について、産業用制御システム・モジュールおよび方法を説明する。実装態様では、耐タンパ性の産業用制御システム・モジュールは、電気回路を含む回路基板と、回路基板に配置されたコネクタと、第１ハウジング面および第２ハウジング面を有するハウジングであって、第１ハウジング面および第２ハウジング面が連結されるとハウジングが回路基板を

収容するように構成され、コネクタに外部アクセスを提供するように構成される少なくとも１つのポートを含む、ハウジングと、第１ハウジング面と一体化された電子スイッチ・アセンブリであって、回路基板および電気回路に電気的に結合され、第２ハウジング面に配置されたスイッチ・トリガによってトリガされるように構成される、電子スイッチ・アセンブリと、を含む。

【００１５】

[0020] 実装態様では、封止エンケースメントに収容された産業用制御システム・モジュールにおける権限のないアクセスを検出する方法は、コントローラを使用して、産業用制御システム・モジュールにおける権限のないアクセスの指示を、第１センサ・コンポーネントから受け取るステップと、セキュリティ・モジュールを使用して、産業用制御システム・モジュールにおける権限のないアクセスの指示に基づいて、セキュリティ・アクションを実施するステップと、を含む。

【００１６】

[0021] 開示される産業用制御システム・モジュールおよびセキュリティ・アクションは、産業用制御システムまたは他の電子デバイス内における権限のないモジュール・アクセス・イベントの発生時のデータおよび情報アクセスを防止するための耐タンパ性モジュールおよび／または自己破壊デバイスを提供することができる。

【００１７】

例示の産業用制御システム・モジュール

[0022] 図１は、本開示の例示の実装態様による産業用制御システム・モジュール１００を示す。図示するように、産業用制御システム・モジュール１００は、セキュリティをデバイスに提供し、（例えば、物理的および通信による等の）権限のないアクセスに応じて産業用制御システム・モジュール１００および内部の電気回路１２０に電気サージを印加するように構成される電子スイッチ・アセンブリ１１４を含むことができる。

【００１８】

[0023] 図１から図５に図示するように、産業用制御システム（ＩＣＳ）１０１は、本開示の例示の実装態様によって説明される少なくとも１つの産業用制御システム・モジュール１００を含むことができる。本明細書で用いられる「産業用制御システム」という用語は、プロセス制御システム（ＰＣＳ）、管理制御およびデータ収集（ＳＣＡＤＡ）システム、分散型制御システム（ＤＣＳ）、および他のより小規模の制御システム構成（例えば産業界やクリティカルなインフラストラクチャでしばしばみられるプログラム可能論理コントローラ（ＰＬＣ））を含む、工業生産において使用される幾らかの種別の制御システムを包含する産業用制御システム１００は、様々な産業（例えば電気、水、油、ガス、データ等）において実装される。

【００１９】

[0024] ＳＣＡＤＡシステムは、製造(manufacturing)、生産(production)、発電、製作(fabrication)、および精油(refining)を含む産業プロセスで用いることができる。ＳＣＡＤＡシステムはまた、水処置および給水、廃水収集および処置、油およびガス・パイプライン、送電および給電、風力発電所、大規模通信システム等を含むインフラストラクチャ・プロセスで用いることができる。更に、ＳＣＡＤＡシステムは、（例えば、ヒーティング、ベンチレーション、およびエア・コンディショニング（ＨＶＡＣ）装置およびエネルギー消費を監視および制御するために）建物、空港、船、宇宙ステーション等のための施設プロセスで用いることができる。ＤＣＳシステムは、通常、大規模キャンパス産業プロセス・プラント（例えば油およびガス、精油、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、外部電力、鉱業、金属等）において用いられる。ＰＬＣは、通例、産業界において、また、クリティカルなインフラストラクチャで用いられる。

【００２０】

[0025] 実施形態では、産業用制御システム・モジュール１００は、電気回路１２０を有する回路基板１０２を含むことができる。幾らかの実装態様では、回路基板１０２は、印刷回路基板を含むことができる。他の実装態様では、回路基板１０２は、他の回路基板

を含むことができる。当該回路基板は、配線、パッド、並びに／または回路基板１０２にエッチングされ或いは回路基盤１０２内におよび／若しくは回路基盤１０２上に配置される導電性トラックを用いて、複数の電子コンポーネントを支持および電気接続するように構成される。回路基板１０２は、片面とすることができ（例えば、電子コンポーネントおよび／または電気接続が回路基板の一面上に配置される。）、或いは両面にすることができる（例えば、電子コンポーネントを回路基板の両面上に配置することができる。）。特定の実装態様では、回路基板１０２は電源バックプレーンおよび通信バックプレーンを有する印刷回路基板を含む。

【００２１】

[0026] 実装態様では、電気回路１２０は少なくとも１つの電子コンポーネントを含むことができる。電子コンポーネントは、回路基盤１０２を通じて他のコンポーネントに結合することができる。電気回路１２０の幾らかの例では、受動コンポーネント（例えば、レジスタ、トランジスタ、コンデンサ、インダクタおよびダイオード等）、ＩＣチップ、通信モジュール（例えば、通信インタフェース１４０、アンテナおよびトランシーバ等）、Ｉ／Ｏモジュール１５２、メモリ・モジュール（例えば、メモリ１３８）、プロセッサ１３６、コネクタ１０４、並びに／またはスイッチを含むことができる。また、回路基板１０２は、アナログ回路、デジタル回路、および／または混合信号回路を含むことができる。

【００２２】

[0027] 図１の例示の実施形態に示すように、回路基板１０２は、コネクタ１０４を備え、および／または、コネクタ１０４に結合されることができる。コネクタ１０４は、機械式アセンブリを用いて電気回路を結合する電気機械式デバイスを含むことができる。幾らかの実装態様では、コネクタ１０４は、プラグおよび／またはジャッキを含むことができる。一実施形態では、ハウジング１０５（例えば、または封止エンケースメント１２２）内でポート１１８を介してコネクタ１０４が外部電気デバイスに通信によりアクセス可能となるように、コネクタ１０４を配置することができる。コネクタ１０４の幾らかの特定の例は、ビデオ・グラフィックス・アレイ（ＶＧＡ）コネクタ、シリアル・ポート・コネクタ、ユニバーサル・シリアル・バス（ＵＳＢ）コネクタ、同軸コネクタ、電源用ＤＣプラグ・コネクタ、イーサネット（登録商標）コネクタ、ＲＪ４５コネクタ、および／またはＳ―ビデオ・ケーブル・コネクタを含むことができる。

【００２３】

[0028] 産業用制御システム・モジュール１００は、第１ハウジング面１０６および第２ハウジング面１０８を有するハウジング１０５（即ち、エンケースメント１２２）を含むことができる。図１に示される実装態様では、第１ハウジング面１０６および第２ハウジング面１０８が相互に連結され、回路基板１０２と産業制御システム・モジュール１００の他のコンポーネントとを収容するように構成された筐体を形成するように構成される。第１ハウジング面１０６および／または第２ハウジング面１０８は、様々な材料（例えば、丈夫な(sturdy)ポリマまたはプラスチック材料）を含むことができ、産業用制御システム・モジュール１００および内部コンポーネント（例えば、回路基板１０２）の支持に供することができる。

【００２４】

[0029] 実施形態では、第１ハウジング面１０６および／または第２ハウジング面１０８は、それぞれの面を他方に連結するための手段を含むことができる。例えば、第１ハウジング面１０６は、第２ハウジング面１０８上に配置および／またはその一部となる受け部(receiver)１１２に接続および確実に結合するように構成されるクリップ機構１１０を含むことができる。この例では、クリップ機構１１０は、受け部１１２に永続的または半永続的に結合され、第１ハウジング面１０６および／または第２ハウジング面１０８を共に固定して、産業用制御システム・モジュール１００への権限のないアクセスを防止できるように構成することができる。

【００２５】

[0030] 幾らかの特定の実施形態では、第１ハウジング面１０６および第２ハウジング面１０８は、少なくとも１つのキャプティブ・ファスナを使用して連結されるように構成することができる。キャプティブ・ファスナは、産業用制御システム・モジュール１００のハウジング（例えば、第１ハウジング面１０６および第２ハウジング面１０８）内で永続的に保持するように設計されるファスナを含むことができる。実装態様では、キャプティブ・ファスナは、ねじ固定(thread locking)、プレス嵌め、および／または産業用制御システム・モジュール１００のハウジング内や第１ハウジング面１０６と第２ハウジング面１０８間でアンカー効き(anchor hold)を得るためのブローチを含むことができる。追加の実装態様では、キャプティブ・ファスナは、第１ハウジング面１０６および／または第２ハウジング面１０８の部材によって（例えば、冷間成形または溶接を通じて）併合(meld)されてもよい。１つの特定の実施形態では、第１ハウジング面１０６および第２ハウジング面１０８は、複数のキャプティブ・スクリューを用いて永続的に連結することができる。キャプティブ・スクリューは、第１ハウジング面１０６および第２ハウジング面１０８の間に永続的な嵌め合い(fit)を作成する。また、ハウジング１０５は、エンケースメント封止部１２６を含むことができる。エンケースメント封止部１２６は、産業制御システム・モジュール１００の内部コンポーネントを環境状態から封止するように供する。エンケースメント封止部１２６は、第１ハウジング面１０６および／若しくは第２ハウジング面１０８に、並びに／またはそれらの間に配置することができる。幾らかの特定の実装態様では、エンケースメント封止部１２６は、権限のないアクセス・イベントを示すための手段を含んでもよい。例えば、エンケースメント封止部１２６は電気回路（例えば、ワイヤ）を含み、破壊され或いは危惧化される(compromise)と、権限のないアクセス・イベントが発生したことをコントローラ１３４に示すことができる。産業用制御システム・モジュール１００は他の構成でも安全性を確保できるものと考察される。例えば、ハウジング１０５は１つのユニットとして形成されてもよく、その結果、アクセスがハウジング１０５の少なくとも一部の構造を損傷または取り外すことを要することになる。

【００２６】

[0031] 産業用制御システム・モジュール１００は、少なくとも１つのセンサ・コンポーネント（例えば、第１センサ・コンポーネント１２４、第２センサ・コンポーネント１３２および追加のセンサ・コンポーネント等）を含むことができ、権限のないアクセス・イベントを示すように機能する。例えば、第１センサ・コンポーネント１２４は、権限のないアクセスおよび／または権限のないアクセスでの試行を検出し、更に、権限のないアクセス・イベントの指示をコントローラ（例えば、コントローラ１３４等）に伝達するように構成することができる。そして、今度は後述するセキュリティ・アクションを実施することができる。産業用制御システム・モジュール１００内で利用されてもよいセンサの幾らかの例は、光学センサ（例えば、光学センサ１５４）、熱センサ（例えば、熱センサ１５６）、振動センサ（例えば、振動センサ１５８）、および／または加速度計（例えば、加速度計１６０）を含むことができる。

【００２７】

[0032] １つの特定の実装態様では、産業用制御システム・モジュール１００は、光学センサ１５４（例えば、フォトダイオード）を含むことができ、環境照明を検出するように構成される。この実装態様では、光学センサ１５４は、ハウジング１０５が権限のないアクセス試行イベントにおいて破壊されたときに、環境照明を検出することができる。また、権限のないアクセス試行イベントの指示をコントローラ１３４に供給することができる。他の特定の実装態様では、産業用制御システム・モジュール１００は、熱センサ１５６（例えば、熱電対列）を含むことができる。例えば、人が産業用制御システム・モジュール１００にアクセスし、それを改竄することを試行するときに、その人からの所定の熱量または放射線量を検出することができる。他の特定の実装態様では、産業用制御システム・モジュール１００は、振動センサ（例えば、圧電性フィルムの振動センサ）を含むことができ、産業用制御システム・モジュール１００の改竄を示す所定のレベルの振動を検出するように構成される。更なる他の特定の実装態様では、産業用制御システム・モジュ

ール１００は加速度計を含むことができ、産業用制御システム・モジュール１００の動きまたは位置移動を検出するように構成される。他のセンサ・コンポーネントまたはセンサ・コンポーネントの組み合わせが産業用制御システム・モジュール１００において利用されてもよいものと考察される。

【００２８】

[0033] 幾らかの実装態様では、産業用制御システム・モジュール１００は、複数のセンサ・コンポーネントを含んでもよい。例えば、産業用制御システム・モジュール１００は、第１センサ・コンポーネント１２４および第２センサ・コンポーネント１３２を含むことができる。これら実装態様では、追加のセンサ・コンポーネント（１または複数）が、権限のないモジュール・アクセスを検証、確証または更に示すように機能してもよい。１つの特定の実施形態では（図２および図５に示すように）、産業用制御システム・モジュール１００は、光学センサ１５４および加速度計１６０を含むことができる。この実施形態では加速度計１６０は、産業用制御システム・モジュール１００の変位を検出し、権限のないアクセスの指示をコントローラ１３４に供給することができる。また、光学センサ１５４は、環境照明を検出し、権限のないアクセスの指示およびハウジング１０５の破壊をコントローラ１３４に供給することができる。コントローラ１３４が加速度計１６０からの指示と光学センサ１５４からの指示とを受け取ると、コントローラ１３４は、セキュリティ・アクション（例えば、電気サージ、破壊熱、電磁場）を実施するために、セキュリティ・モジュール１２８を使用する。セキュリティ・アクションは、産業用制御システム・モジュール１００の少なくとも一部を破壊する（例えば、電気回路１２０を破壊する、電気回路１２０を融解させる、秘密情報１４４をメモリ１３８から消去する、および暗号鍵１４２を消去する等）ように構成される。

【００２９】

[0034] 実装態様では、セキュリティ・モジュール１２８は、コントローラ１３４からの信号および／または命令を受信してセキュリティ・アクションを実施するように構成されるコンポーネントおよび／またはデバイスを含むことができる（当該デバイスは更に、プロセッサ、メモリおよび／または通信インタフェースを有する別個のセキュリティ・コンのローラ１３０を含んでもよい。）。例えば、コントローラ１３４が（例えば、少なくとも１つのセンサ・コンポーネントからの指示を受け取って）権限のないモジュール・アクセス・イベントが発生したと判断すると、コントローラ１３４は、セキュリティ・アクションをセキュリティ・モジュール１２８に実施させることができる。セキュリティ・アクションの幾らかの例は、（例えば、産業用制御システム・モジュール１００内の電気回路１２０、メモリ１３８および／または他のコンポーネントに向けられる）電気パルスおよび／若しくはサージ、電気回路１２０および／若しくは産業用制御システム・モジュール１００を融解或いは損傷させるように構成される（例えば、電気回路１２０等に向けられる）過剰な熱量、データをメモリ１３８から消去するのに十分な電磁場への露出、並びに／または、産業用制御システム・モジュール１００の少なくとも一部の構造を損傷させる能力を有する物理ショックを含むことができる。これら実装態様では、セキュリティ・アクションは、権限のないモジュール・アクセス・イベントの指示に応じて、情報を破壊または産業用制御システム・モジュール１００を使用不能にすることによって、暗号鍵１４２、秘密情報１４４、または他の機密情報を権限のないアクセスから保護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１２８の幾らかの例は、高電位コンデンサ、熱を発生させるように構成される抵抗電気回路（または他の発熱デバイス）、電磁場を発生させるように構成される磁気コイル、並びに／または、電気回路１２０に物理的損傷を生じさせるのに十分な電源モジュールおよび／若しくは電力供給１４６から電圧を導くのに適したスイッチを含むことができる。

【００３０】

[0035] 図１に示すように、第１センサ・コンポーネント１２４および／または第２センサ・コンポーネント１３２の他の例は、電子スイッチ・アセンブリ１１４およびスイッチ・トリガ１１６を含むことができる。電子スイッチ・アセンブリ１１４は、第１ハウジ

ング面１０６上に配置することができる。電子スイッチ・アセンブリ１１４は、更に、（例えば、スプリング付勢ボタン、一組の電気コンタクトおよびタッチ・スイッチ等の）機構を含むことができる。当該機構は、妨害および／またはトリガされると（例えば、電気的に閉じられるまたは開かれると）、産業用制御システム・モジュール１００およびコントローラ１３４によってそれぞれ格納される機密データを消去および／または破壊するように構成される電気パルスおよび／またはサージを伝送することができる。１つの特定の実施形態では、電子スイッチ・アセンブリ１１４は高電位コンデンサを含む。高電位コンデンサは、複数の電気導体の間でエネルギー量を保存するように構成されるコンデンサを含むことができる。ここでは、エネルギー量は、産業用制御システム・モジュール１００および／またはメモリ１３８内に格納されたデータを消去および／または削除するのに少なくとも十分である。実施形態では、電子スイッチ・アセンブリ１１４に保存されるエネルギー量は、回路基板１０２に含まれる電気回路１２０の少なくとも幾らかを破壊し、使用不能にし、および／または無能力にするのに十分なものとすることができる。特定の実施形態では、電子スイッチ・アセンブリ１１４は、トリガされたときに、回路基板１０２上に配置される付随した電気回路１２０を電気的に使用不能にし、また、産業用制御システム・モジュール１００に格納される機密データを消去するように構成されるエネルギー量を伝送するように構成することができる。

【００３１】

[0036] 図１に示される実施形態では、電子スイッチ・アセンブリ１１４が配置され、その結果、第１ハウジング面１０６および第２ハウジング面１０８が連結されると、スイッチ・トリガ１１６が電子スイッチ・アセンブリ１１４に結合するように、および／または電子スイッチ・アセンブリ１１４と嵌め合うように構成される。スイッチ・トリガ１１６は、第２ハウジング面１０８の一部として配置および／または含めることができる。一例では、スイッチ・トリガ１１６は、第２ハウジング面１０８上のタブまたは突起を含むことができ、第２ハウジング面１０８が第１ハウジング面に連結されるときに、スイッチが「オフ」、即ちトリガされない位置を維持するように、タブまたは突起が電子スイッチ・アセンブリ１１４に嵌入する。この例では、産業用制御システム・モジュール１００への権限のないアクセス（例えば、連結された第１ハウジング面１０６および第２ハウジング面１０８を分離させる試行）が示されると、スイッチ・トリガ１１６（例えば、第２ハウジング面１０８上に配置されるタブまたは突起）が、電子スイッチ・アセンブリ１１４から分離および／または取り外される。電子スイッチ・アセンブリ１１４からのスイッチ・トリガ１１６のこの分離または取り外しは、回路基板１０２および／または電気回路１２０に対し、（例えば高電位コンデンサをトリガすることによって）電子スイッチ・アセンブリ１１４に保存されるエネルギーの放出を開始することができる。放出されるエネルギー、並びに回路基板１０２および／または電気回路１２０に伝送されるエネルギーは、データ・ストレージ・コンポーネント（例えば、メモリ１３８）を含む電気回路１２０に過負荷をかけることができる。また、データを消去し、および／または電気回路１２０の電気コンポーネントを破壊することができる。

【００３２】

[0037] 産業用制御システム・モジュール１００は、そのコンポーネントの一部または全部を含み、コンピュータ制御下で動作することができる。例えば、プロセッサは、ソフトウェア、ファームウェア、ハードウェア（例えば、固定論理回路）、手動処理、またはこれらの組み合わせを用いることにより、産業用制御システム・モジュール１００が有するコンポーネントおよび機能を制御する産業用制御システム・モジュール１００と共に、またはその中に含めることができる。本明細書で用いる「コントローラ」、「機能」、「サービス」、および「論理」という用語は、全般的に、産業用制御システム・モジュール１００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、ファームウェア若しくはハードウェアの組み合わせを表す。ソフトウェア実装の場合、モジュール、機能、または論理は、プロセッサ（例えば、中央演算処理装置（ＣＰＵ）または複数のＣＰＵ）上で実行されると、特定のタスクを実行するプログラ

ム・コードを表す。プログラム・コードは、１つ以上のコンピュータ可読メモリ・デバイス（例えば、内部メモリおよび／または１つ以上の有形媒体）等に格納することができる。本明細書において説明する構造、機能、手法、および技術は、様々なプロセッサを有する様々な商用コンピューティング・プラットフォーム上で実装することができる。

【００３３】

[0038] 産業用制御システム・モジュール１００は、認証動作、暗号化および暗号通信等を制御するためのコントローラ１３４を含むことができるコントローラ１３４は、プロセッサ１３６、メモリ１３８、および通信インタフェース１４０を含むことができる。プロセッサ１３６は、コントローラ１３４のために処理機能を提供する。プロセッサ１３６は、如何なる数のプロセッサ、マイクロ・コントローラ、または他の処理システム、および、コントローラ１３４によってアクセスまたは生成されるデータおよび他の情報を格納するレジデンシャル若しくは外部メモリをも含むことができる。プロセッサ１３６は、本明細書において説明する技術を実装する１つ以上のソフトウェア・プログラムを実行することができる。プロセッサ１３６は、それらが形成され材料、または採用される処理機構によって限定されず、このように、半導体（１または複数）および／またはトランジスタ（例えば、電子集積回路（ＩＣ）コンポーネントを使用する）等を通じて実装することができる。

【００３４】

[0039] メモリ１３８の例は、有形のコンピュータ可読ストレージ媒体である。当該媒体は、コントローラ１３４の動作に関連付けられる様々なデータ（例えば、ソフトウェア・プログラムおよび／若しくはコード・セグメント）、または、プロセッサ１３６およびコントローラ１３４の他の見込まれるコンポーネントに、本明細書に説明する機能を実行させるように指示するための他のデータを格納するストレージ機能を提供する。つまり、メモリ１３８は、（そのコンポーネントを含む）産業用制御システム・モジュール１００を動作させる指示のプログラムのようなデータ等を格納することができる。本開示の実施形態では、メモリ１３８は、産業用制御システム・モジュール１００の暗号鍵１４２および／または秘密情報１４４を格納することができる。なお、単一メモリ１３８について説明する一方で、メモリ（例えば、有形の非一時的メモリ）の多種多様な種別および組み合わせを採用することができる点に留意すべきである。メモリ１３８は、プロセッサ１３６と一体化することができ、スタンド・アロンのメモリを備えることができ、または、その両方の組み合わせとすることができる。

【００３５】

[0040] メモリ１３８は、必ずしも限定される訳ではないが、以下のものを含むことができる。即ち、着脱可能および着脱不可能なメモリ・コンポーネント（例えば、ランダム・アクセス・メモリ（ＲＡＭ）、リード・オンリ・メモリ（ＲＯＭ）、フラッシュ・メモリ（例えば、セキュア・デジタル（ＳＤ）メモリ・カード、ミニＳＤメモリ・カード、および／またはマイクロＳＤメモリ・カード）、磁気メモリ、光学メモリ、ユニバーサル・シリアル・バス（ＵＳＢ）メモリ・デバイス、ハードディスク・メモリ、外部メモリ等）である。実装態様では、産業用制御システム・モジュール１００および／またはメモリ１３８は、着脱可能統合回路カード（ＩＣＣ）メモリ（例えば、加入者識別モジュール（ＳＩＭ）カードにより提供されるメモリ、ユニバーサル加入者識別モジュール（ＵＳＩＭ）カード、ユニバーサル統合回路カード（ＵＩＣＣ）等）を含むことができる。

【００３６】

[0041] 通信インタフェース１４０は、各産業用制御システム・モジュール１００のコンポーネントと通信するように動作可能に構成される。例えば、通信インタフェース１４０は、産業用制御システム・モジュール１００のストレージのためのデータを送信し、産業用制御システム１００のストレージからデータを抽出する等のように構成することができる。通信インタフェース１４０はまた、（例えば、コントローラ１３４と通信可能に結合されるデバイスから受け取る入力をプロセッサ１３６に伝達するために）産業用制御システム・モジュール１００のコンポーネントとプロセッサ１３６との間のデータ転送を容

易にするようにプロセッサ１３６と通信可能に結合される。なお、通信インタフェース１４０はコントローラ１３４のコンポーネントとして説明する一方で、通信インタフェース１４０の１つ以上のコンポーネントは、有線および／または無線接続を介して、産業用制御システム・モジュール１００に通信可能に接続される外部エレメントとして実装することができる。産業用制御システム・モジュール１００はまた、（例えば、通信インタフェース１４０を介して）１つ以上の入力／出力（Ｉ／Ｏ）デバイス（例えば、I／0モジュール１５２）を備え、および／または接続することができる。１つ以上の入力／出力（Ｉ／Ｏ）デバイスは、必ずしもこれに限定されないが、ディスプレイ、マウス、タッチパッド、キーボード等を含む。

【００３７】

[0042] 通信インタフェース１４０および／またはプロセッサ１３６は、様々な異なるネットワーク（例えば、ネットワーク１４８）と通信するように構成することができる。様々な異なるネットワークは、必ずしもこれに限定されないが、ワイド・エリア・セルラ電話ネットワーク（例えば、３Ｇセルラ・ネットワーク、４Ｇセルラ・ネットワーク、またはモバイル通信用グローバル・システム（ＧＳＭ）ネットワーク用グローバル・システム、ワイヤレス・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ネットワーク規格を使用して動作するワイヤレス・ローカル・エリア・ネットワーク（ＷＬＡＮ））、インターネット(internet)、インターネット(the Internet)、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）、パーソナル・エリア・ネットワーク（ＰＡＮ）（例えば、ＩＥＥＥ８０２．１５ネットワーク規格を使用して動作するワイヤレス・パーソナル・エリア・ネットワーク（ＷＰＡＮ））、公共電話ネットワーク、エクストラネット、イントラネット等を含む。しかしながら、このリストは、例示のために提供したに過ぎず、本開示を限定するのを意味するものではない。更に、通信インタフェースは、異なるアクセス・ポイントにわたり単一のネットワークまたは複数のネットワークと通信するように構成することができる。

【００３８】

[0043] 実施形態では、産業用制御システム・モジュール１００またはサブシステム（例えば、コントローラ１３４、第１センサ・コンポーネント１２４、第２センサ・コンポーネント１３２、セキュリティ・モジュール１２８、および電力供給１４６等）の制御要素は、１つ以上のバックプレーン１５０によって共に接続することができる。例えば、図２に図示するように、回路基板１０２、コントローラ１３４、第１センサ・コンポーネント１２４、第２センサ・コンポーネント１３２、および／またはセキュリティ・モジュール１２８は、通信バックプレーン１５０によって接続することができる。また、電力供給１４６は、電源バックプレーン１５０によって、コントローラ１３４、第１センサ・コンポーネント１２４、第２センサ・コンポーネント１３２、および／またはセキュリティ・モジュール１２８に接続することができる。

【００３９】

[0044] また、産業用制御システム・モジュール１００は、産業用制御システム１０１内で電源モジュール１４６（例えば、電力供給１４６）に結合される。幾らかの実装態様では、電源モジュール１４６は、（例えば、ＡＣ本線(main)等によって供給される）交流（ＡＣ）を直流（ＤＣ）に変換するためのＡＣからＤＣへの（ＡＣ／ＤＣ）変換器を含む。更に、２つ以上の電源モジュール１４６を用いて、冗長性を提供することができる。例えば、２つの電源モジュール１４６は、電源モジュール１４６ごとに別個の（例えば、冗長な）電源バックプレーンを用いて、入力／出力モジュール１５２の各々に接続することができる。実施形態では、電源バックプレーン（１または複数）は、コネクタ／コネクタ・アッセンブリを使用して、入力／出力モジュールの１つ以上に接続される。

【００４０】

産業用制御システム（複数可）において権限のないアクセスを検出する例示のプロセス

[0045] 図６は、封止エンケースメントに収容される産業用制御システム・モジュール

において権限のないアクセスを検出する例示の実施形態によるプロセス２００を表す。実装態様では、プロセス２００は、（例えば図１から図５を参照して説明した）産業用制御システム・モジュール１００によって明示することができる。産業用制御システム・モジュールにおける権限のないアクセス・イベントの指示を、第１センサ・コンポーネントから受け取る（ブロック２１０）。例えば、コントローラ１３４を利用して、少なくとも１つのセンサ・コンポーネント（例えば、第１センサ・コンポーネント１２４および第２センサ・コンポーネント１３２等）から指示を受け取ることができる。各センサ・コンポーネントは、コントローラ１３４に通信可能に結合することができる。少なくとも１つのセンサ・コンポーネントがトリガされると、センサ・コンポーネント（１または複数）は、権限のないモジュール・アクセス・イベントの指示（例えば、信号）をコントローラ１３４に供給することができる。

【００４１】

[0046] 次いで、セキュリティ・アクションが、産業用制御システム・モジュールにおける権限のないアクセス・イベントの指示に基づいて実施される（ブロック２２０）。例えば、コントローラ１３４は、少なくとも１つのセンサ・コンポーネントからの、権限のないモジュール・アクセス・イベントについての少なくとも１つの指示から、権限のないモジュール・アクセス・イベントが発生したことを判断することができる。また、コントローラ１３４は、セキュリティ・モジュール１２８に、セキュリティ・アクションを実施するよう伝達し、および／またはそれを実施させることができる。幾らかの例では、権限のないモジュール・アクセス・イベントは、エンケースメント封止部１２６の破壊を含んでもよい。

【００４２】

[0047] 特定の実施形態では、コントローラは、センサ・コンポーネントによって供給される指示に基づいて権限のないモジュール・アクセス・イベントが発生したことを判断することができ、電気パルスを含むセキュリティ・アクションを実施させるために、セキュリティ・モジュールに伝達することができる（ブロック２３０）。この実施形態では、コントローラ１３４は、例えば振動センサ１５８から指示を受け取ることができ、（例えば、高電位コンデンサを含む）セキュリティ・モジュール１２８に、産業用制御システム・モジュール１００の電気回路１２０に対する電圧サージを命令させることができる。つまり、電気回路１２０（例えば、メモリ１３８）内のデータおよび情報へのアクセスを破壊する。センサ・コンポーネント（例えば、第１センサ・コンポーネント１２４および第２センサ・コンポーネント等）は、様々なセンサ（例えば、光学センサ、熱センサ、振動センサ、加速度計、湿度センサ、ガス・センサ、マイクロホン、化学センサ、電気センサ、変位量センサ、熱電対列、トランスデューサおよび運動センサ等）を含むことができる。

【００４３】

[0048] 特定の実施形態では、コントローラは、光学センサにより提供される指示に基づいて権限のないモジュール・アクセス・イベントが発生したことを判断することができ、暗号化アルゴリズムを開始することを含むセキュリティ・アクションを実施させるために、セキュリティ・モジュールに伝達することができる（ブロック２４０）。この実施形態では、コントローラ１３４は、例えば熱センサ１５６から指示を受け取ることができ、（例えば、プロセッサを含む）セキュリティ・モジュール１２８に、産業用制御システム・モジュール１００のコントローラ１３４内の暗号化アルゴリズムを開始させることができる、つまり、電気回路１２０（例えば、メモリ１３８）内のデータおよび情報を暗号化する。

【００４４】

[0049] 特定の実施形態では、コントローラは、光学センサによって供給される指示に基づいて権限のないモジュール・アクセス・イベントが発生したことを判断することができ、メモリを消去することを含むセキュリティ・アクションを実施させるために、セキュリティ・モジュールに伝達することができる（ブロック２５０）。この実施形態では、コ

ントローラ１３４は、例えば加速度計１６０から、権限のないモジュール・アクセス・イベントの指示を受け取ることができ、（例えば、プロセッサを含む）セキュリティ・モジュール１２８に、産業用制御システム・モジュール１００のコントローラ１３４内のデータおよび／または情報（例えば、暗号鍵１４２および信頼情報１４４等）をメモリ１３８から削除および／または消去させることができる。つまり、データおよび／または情報へのアクセスを防止する。

【００４５】

[0050] 特定の実施形態では、コントローラは、光学センサによって供給される指示に基づいて権限のないモジュール・アクセス・イベントが発生したことを判断することができ、産業用制御システム・モジュールを破壊熱または破壊電磁場の少なくとも一方にさらすことを含むセキュリティ・アクションを実施させるために、セキュリティ・モジュールに伝達することができる（ブロック２６０）。この実施形態では、コントローラ１３４は、例えば光学センサ１５４および振動センサ１５８から権限のないモジュール・アクセス・イベントの指示を受け取ることができ、（例えば、プロセッサを含む）セキュリティ・モジュール１２８に、（例えば、コントローラ１３４、メモリ１３８、および／または産業用制御システム・モジュール１００の少なくとも一部を融解および／または損傷させるのに十分な）破壊的な熱量を発生させ、また、産業用制御システム・モジュール１００（例えば、メモリ１３８）の一部（複数可）を収容するデータおよび／または情報に対してその熱を向けることができる。つまり、データおよび／または情報へのアクセスを防止する。加えて、セキュリティ・モジュール１２８は、他の破壊的な力（例えば、電磁デバイスを含むセキュリティ・モジュール１２８によって発生される電磁場）を発生させてもよい。この力は、メモリ１３８、コントローラ１３４および／または産業用制御システム・モジュール１００の少なくとも一部を破壊するように構成される。

【００４６】

[0051] 実施形態では、権限のないアクセス・イベントの追加の指示を、第２センサ・コンポーネントから受け取ってもよい（ブロック２７０）。この実施形態では、第２センサ・コンポーネント１２６は、第１センサ・コンポーネント１２４からの指示に加えて、第１センサ・コンポーネント１２４から指示をコントローラ１３４に供給することができる。第２センサ・コンポーネント１２６（または、第３センサ・コンポーネントおよび第４センサ・コンポーネント等）から権限のないアクセスの追加の指示を供給することにより、権限のないモジュール・アクセス検出の精度を改善するのに供することができ、誤ったイベント・トリガおよび指示を最小化するのに供することができる。

【００４７】

結論

[0052] 主題について構造上の特徴および／またはプロセス動作に特有の言語で説明してきたが、添付の特許請求の範囲に定める主題が、上記の特定の特徴や行為には必ずしも限定されないことが理解されるべきである。そうではなく寧ろ、上記の特定の特徴および行為は、特許請求の範囲を実施する例示の形態として開示されるものである。

【図１】

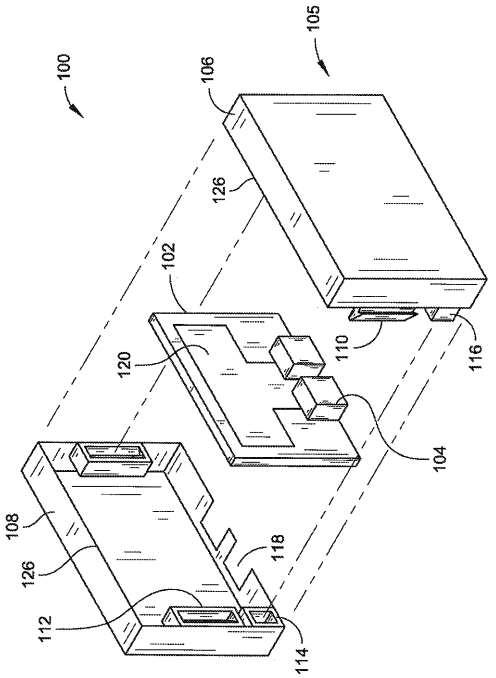


FIG. 1

【図２】

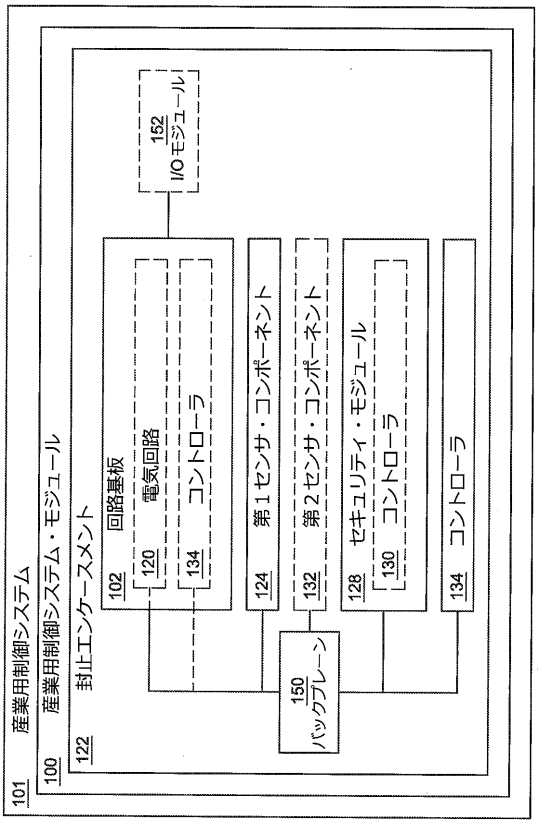


FIG. 2

【図３】

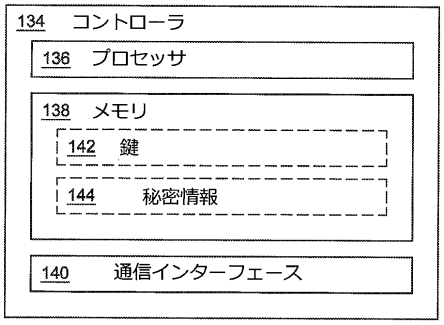


FIG. 3

【図４】

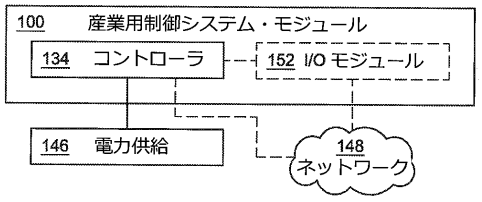


FIG. 4

【図５】

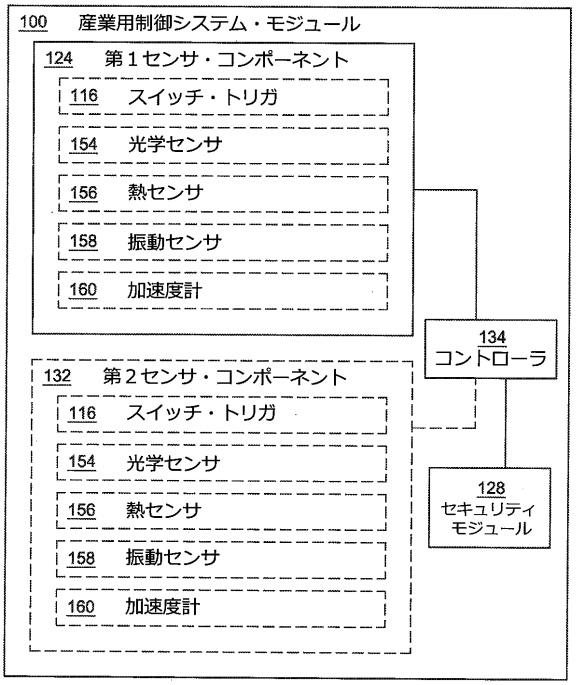


FIG. 5

【図６】

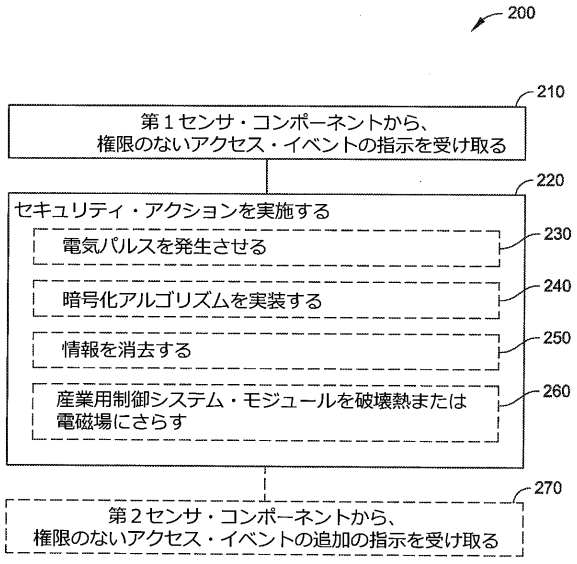

200
210
第１センサ・コンポーネントから、
権限のないアクセス・イベントの指示を受け取る
220
セキュリティ・アクションを実施する
230
電気パルスを発生させる
240
暗号化アルゴリズムを実装する
250
情報を消去する
260
産業用制御システム・モジュールを破壊熱または
電磁場にさらす
270
第２センサ・コンポーネントから、
権限のないアクセス・イベントの追加の指示を受け取る

FIG. 6

フロントページの続き

(72)発明者　ルーヤッカーズ，アルバート
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　ドーセット，ケン
アメリカ合衆国マサチューセッツ州０２７６６，ノートン，バーチ・ブルック・レーン　２０

審査官　岸野　徹

(56)参考文献　米国特許第０７４９５５５４（ＵＳ，Ｂ１）
特開平０７－２１９８５３（ＪＰ，Ａ）
米国特許出願公開第２０１４／０１２３３２２（ＵＳ，Ａ１）
米国特許出願公開第２０１２／０２９８１１９（ＵＳ，Ａ１）
特開平１１－１７５４０６（ＪＰ，Ａ）
特表２００４－５３２４９０（ＪＰ，Ａ）
特開平０５－１５８８００（ＪＰ，Ａ）
特開２００６－３４３８４４（ＪＰ，Ａ）
米国特許出願公開第２００６／００４９９４１（ＵＳ，Ａ１）
米国特許出願公開第２００１／００５６５４３（ＵＳ，Ａ１）
米国特許出願公開第２００８／０１２９５０１（ＵＳ，Ａ１）
特開２００１－１９５３０７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／８６
Ｇ０５Ｂ　１９／０５
Ｇ０６Ｆ　２１／６０