(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6302283号
(P6302283)
(45)発行日　平成30年3月28日(2018.3.28)　(24)登録日　平成30年3月9日(2018.3.9)

(51)Int.Cl.　　F I
G06F 21/55 (2013.01)　　G06F 21/55 340
H04L 12/66 (2006.01)　　H04L 12/66 B

請求項の数 7　(全 12 頁)

(21)出願番号　特願2014-40025(P2014-40025)
(22)出願日　平成26年3月3日(2014.3.3)
(65)公開番号　特開2014-179074(P2014-179074A)
(43)公開日　平成26年9月25日(2014.9.25)
審査請求日　平成29年2月23日(2017.2.23)
(31)優先権主張番号　13/801,496
(32)優先日　平成25年3月13日(2013.3.13)
(33)優先権主張国　米国(US)

(73)特許権者　390041542
ゼネラル・エレクトリック・カンパニイ
アメリカ合衆国、ニューヨーク州　１２３４５、スケネクタデイ、リバーロード、１番
(74)代理人　100137545
弁理士　荒川　聡志
(74)代理人　100105588
弁理士　小倉　博
(74)代理人　100129779
弁理士　黒川　俊久
(74)代理人　100113974
弁理士　田中　拓人

最終頁に続く

(54)【発明の名称】産業用制御システムのためのインテリジェントサイバーフィジカル侵入検出および侵入防止システムならびに方法

(57)【特許請求の範囲】
【請求項１】
制御システム挙動を測定するように構成されているデバイス監視構成要素と、
前記デバイス監視構成要素および通信ネットワークに通信可能に結合された侵入防止システムとを備え、前記侵入防止システムは、
前記デバイス監視構成要素によって測定された前記制御システム挙動を、第１のルールセットと対照して分析するように構成されている制御システム分析構成要素と、
第２のルールセットに対して前記通信ネットワークから送信された複数の通信パケットの複数のネットワークパラメータを分析するネットワーク分析構成要素であって、前記分析が、第１及び第２のリストに含まれるデータと前記複数のネットワークパラメータとを比較し、前記比較の結果に基づいて、前記複数の通信パケットを少なくとも異常が存在するか、侵入が存在するかに分類することにより行われる、前記ネットワーク分析構成要素と、
前記制御システム分析構成要素の結果と前記ネットワーク分析構成要素の結果とを相関し、相関結果がいつ偽陽性または偽陰性に導かれたかを特定し、偽陽性または偽陰性に導かれたかを特定された場合、前記第１及び第２のルールセットを修正する機械学習及び相関構成要素と、
を含む、
システム。
【請求項２】

前記侵入防止システムがメンテナンスモードにあるときに前記第１及び第２のルールセットが修正される請求項１記載のシステム。
【請求項３】
前記制御システム挙動は、コントローラの挙動からなり、そのとき、前記デバイス監視構成要素は前記コントローラに通信可能に結合されている請求項１記載のシステム。
【請求項４】
前記コントローラ挙動は、前記コントローラ内の構成要素の電力使用、前記コントローラ内の前記構成要素の温度、前記コントローラの動作、入力／出力のタイミング、前記コントローラに結合されたデバイスのテレメトリデータ、またはそれらの任意の組合せを含む請求項３記載のシステム。
【請求項５】
前記コントローラ内の前記構成要素は、処理ユニット、メモリ、記憶デバイス、および通信装置を含み、
前記デバイス監視構成要素は、前記コントローラ内に設置される又は、前記コントローラとは別個のデバイスを備える請求項３記載のシステム。
【請求項６】
前記侵入防止システムは、別個のデバイスを備え、
ガスタービンシステム、ガス化システム、蒸気タービンシステム、風力タービンシステム、水力タービンシステム、発電システム、電力グリッド自動化システム、またはそれらの任意の組合せからなる産業用制御システムである請求項１記載のシステム。
【請求項７】
電子デバイスのプロセッサによって実行可能な複数の命令を記憶する有形で非一時的なコンピュータ可読媒体であって、前記命令は、実行されたときにプロセッサが、
産業制御システムをシュミレーションするモデルであって、侵入を含まないモデルを実行し、
前記モデルの実行時に送信された通信パケットの複数のネットワークパラメータを特定し、
前記複数のネットワークパラメータに少なくとも部分的に基づいてネットワークルールの組を生成し、
前記モデルの実行時に測定された制御システムパラメータを特定し、
前記制御システムパラメータに少なくとも部分的に基づいて、制御システムルールの組を生成するように実行し、
前記ネットワークルールの組と前記制御システムルールの組は、前記産業制御システムの稼働中に侵入が起こったか否かを検出するために使用され、
前記プロセッサはさらに、
第１及び第２のリストに含まれるデータと前記複数のネットワークパラメータとを比較し、
比較の結果に基づいて前記複数の通信パケットを侵入に分類することを実行する、
媒体。

【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、制御システムの物理的挙動を監視することによって、制御システムにおけるセキュリティ侵害を検出する侵入防止システム（intrusion prevention system）（ＩＰＳ）に関する。
【背景技術】
【０００２】
一般に、ＩＰＳは、制御システム内でネットワーク通信を監視することによって、産業用制御システムなどの制御システム内へのデジタル侵入を検出および／または防止するよ

うに構成することができる。具体的には、ネットワークＩＰＳは、ネットワークパラメータに基づいて侵入および／または異常の指標を探すことができる。たとえば、ネットワークＩＰＳは、ネットワークトラフィック、ファイルシステムアクセス／修正、またはオペレーティングシステム／ライブラリコールなどのパラメータを監視することができる。その後、監視されるパラメータをルールセットと比較して、制御システムに侵入および／または異常が存在するかどうかを判定することができる。

【０００３】

侵入と呼ばれるセキュリティ侵害は、権限のないパーティが、産業用制御システムなどの制御システムにアクセスすることを可能にし、システム内で予期しない挙動を引き起すおそれがある。たとえば、侵入は、システムに、要求されていなかったプロセスを実施させる場合がある。産業用制御システムは、タービン、発電機、圧縮機、または燃焼器などのデバイスを含むことができるため、ネットワークパラメータの範囲を超えて産業用制御システム内のセキュリティを改善することは有利であるであろう。

【先行技術文献】

【特許文献】

【０００４】

【特許文献１】米国特許出願公開第２０１３／００８６６８０号公報

【発明の概要】

【課題を解決するための手段】

【０００５】

最初に特許請求される本発明と範囲が一致するいくつかの実施形態が以下で要約される。これらの実施形態は、特許請求される本発明の範囲を制限するように意図されるのではなく、むしろ、これらの実施形態は、本発明の考えられる形態の簡潔な要約を提供するように意図されるにすぎない。実際には、本発明は、以下で述べる実施形態と類似していても、または異なっていてもよい種々の形態を包含することができる。

【０００６】

第１の実施形態は、システムを提供し、システムは、制御システム挙動を測定するように構成されているデバイス監視構成要素と、デバイス監視構成要素および通信ネットワークに通信可能に結合された侵入防止システムとを含む。侵入防止システムは、制御システム分析構成要素を備え、制御システム分析構成要素は、デバイス監視構成要素によって測定された制御システム挙動を、第１のルールセットと対照して分析して、異常が存在するか、侵入が存在するか、または両方が存在するかを判定するように構成されている。

【０００７】

第２の実施形態は、電子デバイスのプロセッサによって実行可能な複数の命令を記憶する有形で非一時的なコンピュータ可読媒体を提供する。命令は、通信パケットを受信する命令と、通信パケットがネットワークルールセットと対照して試験される第１の試験を実施する命令と、制御システム測定値を受信する命令であって、制御システム測定値が産業用制御システムの制御システム挙動を示す、命令と、制御システム測定値が制御システムルールと対照して試験される第２の試験を実施する命令と、第１の試験からの結果と第２の試験からの結果を相関させる命令と、相関データに基づいて産業用制御システムに異常が存在するか、侵入が存在するか、または両方が存在するかを判定する命令からなる。

【０００８】

第３の実施形態は、コントローラおよび監視ステーションに通信可能に結合された侵入防止システムを含むシステムを提供する。侵入防止システムは、監視ステーションとコントローラとの間で送信されるネットワーク通信を受信し、コントローラの状態、産業用制御システムの状態、コントローラに接続されたデバイス、またはそれらの任意の組合せに少なくとも部分的に基づいて、異常が存在するか、侵入が存在するか、または両方が存在するかを判定するように構成されている。

【０００９】

本発明のこれらのまた他の特徴、態様、および利点は、以下の詳細な説明が添付図面を

参照して読まれるとよりよく理解されるであろう。添付図面では、同じ符号は、図面全体を通して同じ部品を示す。

【図面の簡単な説明】

【００１０】

【図１】産業用制御システム内の侵入防止システム（ＩＰＳ）のブロック図である。

【図２】図１からの侵入防止システム（ＩＰＳ）の実施形態のブロック図である。

【図３】産業用制御システム内で異常が起こったかどうかを判定するのに適した方法の実施形態のフローチャートである。

【図４】侵入防止システム（ＩＰＳ）内でルールセットを生成および／または修正するのに適した方法の実施形態のフローチャートである。

【発明を実施するための形態】

【００１１】

本発明の１つまたは複数の特定の実施形態が以下で述べられる。これらの実施形態の簡潔な説明を提供しようとして、実際の実装形態の全ての特徴が本明細書で述べられない可能性がある。任意のこうした実際の実装形態の開発において、任意の工学および設計プロジェクトの場合と同様に、実装形態ごとに変動する場合がある、システム関連制約およびビジネス関連制約の遵守などの開発者の固有の目的を達成するために、多数の実装形態固有の決定が行われなければならないことが認識されるべきである。さらに、こうした開発努力は複雑でかつ時間がかかる可能性があるが、それでも、本開示の利益を受ける当業者にとって、設計、作製、および製造の日常的な仕事であることになることが認識されるべきである。

【００１２】

本発明の種々の実施形態の要素を導入するとき、冠詞「ある（ａ）」、「ある（ａｎ）」、「その（ｔｈｅ）」、または「前記（ｓａｉｄ）」は、要素の１つまたは複数が存在することを意味することが意図される。用語「備える（ｃｏｍｐｒｉｓｉｎｇ）」、「含む（ｉｎｃｌｕｄｉｎｇ）」、または「有する（ｈａｖｉｎｇ）」は、包含的であり、挙げた要素以外のさらなる要素が存在する可能性があることを意味することが意図される。

【００１３】

本開示は、一般に、侵入が産業用制御システムに入る可能性を低減するように構成することができる、産業用制御システムなどの制御システム内に配設された侵入防止システム（ＩＰＳ）を対象とする。本明細書で使用されるように、侵入は、産業用制御システムに入る可能性があるデジタルセキュリティ侵害を指す。侵入は、産業用制御システムに入ると、産業用制御システム内で異常を引き起す場合がある。換言すれば。侵入は、産業用制御システム内で予期しない挙動を引き起す場合がある。たとえば、侵入は、産業用制御システムに、要求されなかったデータを、ネットワーク接続を通して送信させる場合がある。そのため、侵入を低減するように設計されたシステムは、ネットワークトラフィック、ファイルシステムアクセス／修正、またはオペレーティングシステム／ライブラリコールなどの、産業用制御システム内のネットワークパラメータを監視するように構成することができる。しかし、産業用制御システム内のさらなるパラメータを、産業用制御システムのセキュリティを改善するために監視することができる。

【００１４】

したがって、本開示は、システムを提供し、システムは、制御システム挙動を測定するように構成されているデバイス監視構成要素と、デバイス監視構成要素および通信ネットワークに通信可能に結合された侵入防止システムとを含む。侵入防止システムは、制御システム分析構成要素を備え、制御システム分析構成要素は、デバイス監視構成要素によって測定された制御システム挙動を、ルールセットと対照して分析して、異常が起こったかどうかを判定するように構成されている。換言すれば、ネットワークパラメータを監視することに加えて、開示される技法はまた、フィジカルパラメータを監視して、産業用制御システムをよりよく理解し、産業用制御システム内に異常および／または侵入が存在するかどうかをよりよく判定する。

【００１５】
導入として、図１は、産業用制御システム１２内の侵入防止システム（ＩＰＳ）１０の実施形態を示す。自動化発電システム（たとえば、ガス、蒸気、風力、または水力タービン、熱回収蒸気発生器（heat recovery steam generator）（ＨＲＳＧ）、ガス化システム、燃焼システム、電気発電機、電力グリッド自動化システム、または同様の自動化発電システム）、または自動化製造システム（たとえば、化学プラント、製油所、または同様な製造システム）などの産業用制御システム１２は、監視ステーション１４、サイバーセキュリティ監視／応答システム１５、コントローラ１６、デバイス、および通信ネットワーク１８を含むことができる。
【００１６】
監視ステーション１４およびコントローラ１６は、通信ネットワーク１８を通して通信パケットを送信するように構成することができる。具体的には、通信パケットは、制御コマンドおよび／またはデータを含むことができる。Ｍｏｄｂｕｓリモート端末ユニット（remote terminal unit）（ＲＴＵ）、Ｐｒｏｆｉｂｕｓ、Ｃｏｎｉｔｅｌ、国際電気標準会議（international Electrotechnical Commission）（ＩＥＣ）６０８７０－５－１０１、ＩＥＣ６０８７０－５－１０４、ＩＥＣ６１８５０、分散ネットワークプロトコル（Distributed Network Protocol）（ＤＮＰ）３、または同様なものの種々のプロトコルが、通信ネットワーク１８によって使用され得る。プロトコルの一部は、産業用制御システムがインターネットを通じてアクセス可能であることを可能にすることができる伝送制御プロトコルおよびインターネットプロトコル（ＴＣＰ／ＩＰ）拡張版を含むことができる。したがって、産業用制御システム１２内への侵入のための１つのエントリポイントは、通信ネットワーク１８にある場合がある。
【００１７】
さらに、コントローラ１６は、タービン２０、センサ２２、アクチュエータ２４、ポンプ２６などの種々のデバイスを制御するように構成することができる。さらに、サブステーション構成では、コントローラ１６は、変圧器、ブレーカ、スイッチ、モータ、または発電機などの電力機器のための保護、制御、および調量（metering）機能を提供するように構成されているインテリジェント電子デバイスとすることができる。したがって、コントローラ１６は、処理ユニット２８、メモリ３０、記憶デバイス３２、およびデバイスと通信するように構成されている通信装置３４を含むことができる。そのため、侵入用の別のエントリポイントは、デバイスに直接入ることであるとすることができる。侵入用の他のエントリポイントは、コントローラ１６または監視ステーション１４に直接入ることであるとすることができる。
【００１８】
示す産業用制御システム１２はまた、ＩＰＳ１０を含む。ＩＰＳ１０は、コンピューティングデバイス（たとえば、コンピュータ、サーバ、ラップトップ、タブレット、携帯電話、モバイルデバイス、または同様の処理もしくはコンピューティングデバイス）で、あるいはコントローラ１６のメモリ３０、監視ステーション１４、コントローラ１６の記憶デバイス３２、またはその組合せなどの機械可読媒体に記憶される実行可能で非一時的なコンピュータ命令もしくはコードで実装することができる。ネットワークパラメータを監視することに加えて、ＩＰＳ１０は、異常および／または侵入が存在するかどうかを判定するために制御システム（すなわち、物理的）パラメータを監視するように構成することができる。ＩＰＳ１０は、デバイスとの通信、熱発生、または電力使用などの制御システムパラメータを監視するように構成することができ、その理由は、それらのパラメータが、産業用制御システム１２内で起こっているプロセスの正確な表現である場合があるからである。換言すれば、制御システムパラメータは、概して、回避するのがより難しい場合がある物理的法則に基づいている。たとえば、プロセッサの温度が、プロセッサが実施しているプロセスに関連する場合があるため、温度を監視することは、侵入によって引き起されるようなさらなるプロセスをプロセッサが実施しているかどうかを、ＩＰＳ１０が知ることを可能にする。したがって、ＩＰＳは、ネットワーク分析構成要素３６および制御

システム分析構成要素３８を含む。

【００１９】

ネットワーク分析構成要素３６は、ネットワークトラフィック、ファイルシステムアクセス／修正、またはオペレーティングシステム／ライブラリコールなどの、通信ネットワーク３０を通じて送信される通信パケットのネットワークパラメータを分析して、異常および／または侵入が存在するかどうかを判定するように構成することができる。したがって、ネットワーク分析構成要素３６は、通信ネットワーク１８に結合し、通信ネットワーク１８を通して送信される通信パケットを受信するように構成することができる。

【００２０】

同様に、制御システム分析構成要素３８は、デバイスとの通信、熱発生、または電力使用などの制御システムパラメータを分析して、異常および／または侵入が起こったかどうかを判定するように構成することができる。そのため、ＩＰＳ１０は、コントローラ１６およびコントローラ１６によって制御されるデバイス（たとえば、タービン２０、センサ２２、アクチュエータ２４、ポンプ２６、または電気的アシスト２７）の制御システム（すなわち、物理的）パラメータを監視し測定するように構成されているデバイス監視構成要素４０をさらに含むことができる。したがって、デバイス監視構成要素４０は、コントローラ１６に通信可能に結合することができる。示す実施形態では、デバイス監視構成要素４０は、コントローラ１６内に配置され、処理ユニット２８、メモリ３０、記憶デバイス３２、および通信装置３４に直接結合する。代替的に、デバイス監視構成要素４０は、別個のコンピューティングデバイスで、またはコントローラ１６のメモリ３０、監視ステーション１４、コントローラ１６の記憶デバイス３２、もしくはその組合せなどの機械可読媒体に記憶される実行可能で非一時的なコンピュータ命令で実装することができる。

【００２１】

上述したように、デバイス監視構成要素４０は、制御システム（すなわち、物理的）パラメータを測定するように構成することができる。測定された制御システム（すなわち、物理的）パラメータは、産業用制御システム１２の動作の物理的結果である。したがって、それらのパラメータは、産業用制御システム１２内で起こるプロセスの指標を提供することができる。たとえば、デバイス監視構成要素４０は、処理ユニット２８の電力使用または温度を測定することができる、通信装置３４とデバイス（たとえば、タービン２０、センサ２２、アクチュエータ２４、ポンプ２６、または電気的アシスト２７）との間の通信活動を測定することができる、またはコントローラ１６によって実施されるプロセスのタイミングを測定することができる。測定された制御システムパラメータは、その後、制御システム分析構成要素３８に送信され、制御システムルールセットと対照して分析されて、異常および／または侵入が存在するかどうかを判定することができる。

【００２２】

上述したように、産業用制御システム１２内への侵入は、産業用制御システム１２内で予期しない挙動または異常を引き起す場合がある。異常が検出されると、ＩＰＳ１０は、アラームを通して監視ステーション１４および／またはサイバーセキュリティ監視／応答システム１５に異常を通信することができる。監視ステーション１４および／またはサイバーセキュリティ監視／応答システム１５は、報告された異常を相関させる中央システムとして働くように構成することができる。さらに、両者は、オペレータが異常をさらに調査することを可能にするヒューマンマシンインタフェース（human-machine interface）（ＨＭＩ）を含むことができる。サイバーセキュリティ監視／応答システム１５上のオペレータは、異常が実際には偽陽性であると判定し、ネットワークルールセットを相応して変更することができる。さらに、オペレータは、検出された異常に対する応答を決定することができる。換言すれば、オペレータは、異常を回復させる対応策をとるよう産業用制御システム１２に指示することができる。いくつかの実施形態では、応答は、自動的に決定され、産業用制御システム１２に通信され得る。

【００２３】

図２は、図１に示す侵入防止システム（ＩＰＳ）１０の一実施形態を示す。示す実施形

態では、ネットワーク分析構成要素３６は、ネットワーク監視構成要素４２、およびネットワークルールセット４６を含むネットワークルールセット処理構成要素４４を含む。同様に、制御システム分析構成要素３８は、制御システム監視構成要素４８、および制御システムルールセット５２を含む制御システムルールセット処理構成要素５０を含む。

【００２４】

上述したように、ＩＰＳ１０は、通信ネットワーク１８から通信パケットを、また、デバイス監視構成要素４０から制御システム測定値を受信するように構成されている。通信パケットは、最初に、ネットワーク監視構成要素４２を通してＩＰＳ１０に入ることができる。ネットワーク監視構成要素４２は、ＩＰＳ１０に対するゲートウェイとして働くように構成することができる。通信パケットは、その後、ネットワークルールセット処理構成要素４４に渡される。ネットワークルールセット処理構成要素４４は、ネットワークルールセット４６と対照して通信パケットを分析して、ネットワーク異常および／または侵入が存在するかどうかを判定するように構成することができる。同様に、制御システム測定値は、最初に、制御システム監視構成要素４８を通してＩＰＳ１０に入り、その後、制御システムルールセット処理構成要素５０に渡される。制御システムルールセット処理構成要素５０は、制御システムルールセット５２と対照して制御システム測定値を分析して、制御システム異常および／または侵入が存在するかどうかを判定するように構成することができる。

【００２５】

図３は、異常および／または侵入が存在するかどうかを判定するために、ＩＰＳ１０によって使用される方法５４の一実施形態を示す。方法５４は、ネットワーク監視構成要素４２が通信ネットワーク１８から通信パケットを受信する（ブロック５６）ことで始まることができる。上述したように、通信パケットは、監視ステーション１４とコントローラ１６との間の制御コマンドおよび／またはデータを含むことができる。制御コマンドは、ファイルシステムアクセス／修正、アプリケーション／プロセスコール、オペレーティングシステムコール、ライブラリコール、またはそれらの任意の組合せを含むことができる。データは、コントローラ１６に結合されたセンサ２２などのデバイスによって得られる測定値を含むことができる。

【００２６】

次に、ネットワークルールセット処理構成要素４４は、ネットワークルールセット４６と対照して、受信されたパケットを試験して（ブロック５８）、ネットワーク異常および／または侵入が存在するとネットワークルールセット処理構成要素４４が考えるかどうかを判定することができる。ネットワークルールセット４６は、ホワイトリストおよびブラックリストを含むように構成することができる。ホワイトリストは、侵入に関連しないとＩＰＳ１０が考える通信パケットのリストとすることができ、ブラックリストは、侵入に関連するとＩＰＳ１０が考える通信パケットのリストとすることができる。通信パケットがホワイトリストにもブラックリストにも入らない事例では、侵入が存在するかどうかＩＰＳ１０が不確かであるため、通信パケットをネットワーク異常として分類することができる。

【００２７】

さらに、通信パケットをよりよく特徴付けるため、ネットワークルールセット処理構成要素４４は、ネットワーク通信をコンテキスト的に観察するように構成することができる。換言すれば、ネットワークルールセット処理構成要素４４は、コントローラの状態、産業用制御システムの状態、コントローラに接続されたデバイス、またはそれらの任意の組合せを少なくとも部分的に観察するように構成することができる。たとえば、デバイス（たとえば、タービン２０、センサ２２、アクチュエータ２４、ポンプ２６、または電気的アシスト２７）が権限移譲状態（commissioned state）にあるとき、デバイスは、動作可能状態であり、構成に対する変更がほとんど行われるべきでない。したがって、通信パケットが、電気保護設定などの構成を変更しようとしているとネットワークルールセット処理構成要素４４が判定するとき、通信パケットをネットワーク異常として特定することが

できる。比較してみると、デバイスが構成状態にあるとき、デバイスが構成されることを可能にする、構成に対するより多くの変更が許容されるべきである。他の状態は、メンテナンス状態、緊急状態、またはセキュリティ応答状態を含むことができる。同様に、通信パケットがタービン２０などのデバイスのために意図されるが、タービン２０が産業用制御システム１２内に存在しない場合、ネットワークルールセット処理構成要素４４は、通信パケットをネットワーク異常として特定することができる。

【００２８】

方法５４は、引き続き、制御システム監視構成要素４８がデバイス監視構成要素４０から制御システム測定値を受信する（ブロック６０）ことを行うことができる。上述したように、デバイス監視構成要素４０は、コントローラ内の構成要素の電力使用、コントローラ内の構成要素の温度、コントローラの動作、入力／出力のタイミング、コントローラに結合したデバイスのテレメトリデータ、またはそれらの任意の組合せなどの、制御システム（すなわち、物理的）測定を産業用制御システム１２上で行うように構成することができる。たとえば、デバイス監視構成要素４０は、処理ユニット２８の電力使用または温度を測定することができる、通信装置３４とデバイス（たとえば、タービン２０、センサ２２、アクチュエータ２４、ポンプ２６、または電気的アシスト２７）との間の通信活動を測定することができる、またはコントローラ１６によって実施されるプロセスのタイミングを測定することができる。さらに、デバイス監視構成要素４０は、タービン２０が回転する速度などのデバイスのテレメトリデータを測定することができる。測定されたパラメータが、プロセスが産業用制御システム内で起こっていることを示すことが認識されるべきである。

【００２９】

次に、制御システムルールセット処理構成要素５０は、制御システムルールセット５２と対照して、受信された測定値を試験して（ブロック６２）、制御システム異常および／または侵入が存在すると制御システムルールセット処理構成要素５０が考えるかどうかを判定することができる。やはり、制御システムルールセット５２は、ホワイトリストおよびブラックリストを含むように構成することができる。ホワイトリストは、制御システム異常が存在しないときの、測定されたパラメータについての適切な測定範囲を含むことができる。ブラックリストは、満たされると、侵入を表明することができる閾値を含むことができる。測定値が、ホワイトリスト範囲内に入らないかまたはブラックリスト閾値を超えるとき、測定値は制御システム異常として分類され得ることが認識されるべきである。

【００３０】

ブロック５８およびブロック６２からの結果は、その後、ＩＰＳ１０内の機械学習および相関分析構成要素６８で相関されて（ブロック６４）、侵入および／または異常が存在するかどうかを判定する（ブロック６６）ことができる。認識されるはずであるが、ルールセット（たとえば、４６および５２）は、完全ではなく、偽陽性を返すかまたは異常を完全に見逃す場合（すなわち、偽陰性）がある。したがって、産業用制御システム１２のより正確な表現を達成するために、機械学習および相関分析構成要素６８は、ネットワーク異常、制御システム異常、および侵入を相関させて、異常または侵入が存在すると構成要素６８が考えるかどうかを判定することができる。２つのルールセット（たとえば、４６および５２）を使用することが、偽陽性ならびに異常および／または侵入の見逃しの可能性を低くする場合があるため、産業用制御システム１２の侵入および／または異常のより正確な検出が達成される。したがって、ルールセット（たとえば、４６および５２）に厳密に従う代わりに、異常および／または侵入を検出するときに、より大きな余裕を持つことができる。

【００３１】

図２に戻ると、異常が検出されると、監視ステーション１４および／またはサイバーセキュリティ監視／応答システム１５による応答に加えて、ＩＰＳ１０自体が、さらなる対応策をとることができる。ネットワークルールセット処理構成要素４４および制御システムルールセット処理構成要素５０によってとられる次の対応策は、ＩＰＳ１０がどんなモ

ードにあるかに依存する場合がある。具体的には、ＩＰＳ１０がパッシブモードにあるとき、ＩＰＳ１０は、産業用制御システム１２の動作においてできる限り最小限に干渉するように構成されている。したがって、ネットワークルールセット処理構成要素４４は、ネットワーク監視構成要素４２を通してサイバーセキュリティ監視／応答システム１５にアラームを送信するように構成することができる。同様に、制御システムルールセット処理構成要素５０は、制御システム監視構成要素４８を通して監視ステーション１４にアラームを送信するように構成することができる。ＩＰＳ１０がアクティブモードにあるとき、ＩＰＳ１０は、産業用制御システム１２を積極的に保護するように構成されている。したがって、ネットワークルールセット処理構成要素４４は、異常である通信パケットをフィルタリングするように構成することができ、制御システムルールセット処理構成要素５０は、制御信号を送信するように構成することができる。たとえば、制御システムルールセット処理構成要素５０は、検出された異常が、デバイスに予想外に動作させることになると判定する場合、デバイスの動作を中止する制御信号を送信することができる。

【００３２】

上述したように、ＩＰＳ１０は、機械学習および相関分析構成要素６８をさらに含むことができる。機械学習および相関分析構成要素６８は、ルールセット（たとえば、４６および５２）を生成することおよび修正することを容易にするように構成することができる。示す実施形態では、サイバーセキュリティ監視／応答システム１５および監視ステーション１４は、ＩＰＳ１０に偽陽性および偽陰性を通信するように構成することができる。機械学習および相関分析構成要素６８は、ルールセット（たとえば、４６および５２）を相応して修正するように構成することができる。具体的には、示す実施形態では、サイバーセキュリティ監視／応答システム１５は、ネットワークルールセット処理構成要素４４にネットワーク偽陽性および偽陰性を通信し、監視ステーション１４は、制御システムルールセット処理構成要素５０に制御システム偽陽性および偽陰性を通信する。偽陽性および偽陰性は、その後、機械学習および相関分析構成要素６８に通信される。

【００３３】

図４は、ルールセット（たとえば、４６および５２）を生成するかつ／または維持するように構成されている方法７０の一実施形態を示す。ＩＰＳ１０が構成／訓練モードにあるとき、ルールセット（たとえば、４６および５２）を、モデルに基づいて生成することができる。したがって、ＩＰＳ１０が構成／訓練モードにあるとき、方法７０は、モデルを実行する（ブロック７２）ことによって始まることができる。モデルは、侵入が存在しない状態での既知の動作のセットとすることができる。次に、ＩＰＳ１０は、ネットワークパラメータを読み取る（ブロック７４）。上述したように、ネットワークパラメータは、コントローラ１６と監視ステーション１４との間で通信される通信パケットを含むことができる。同様に、ＩＰＳ１０は、制御システムパラメータを読み取る（ブロック７６）。上述したように、制御システムパラメータは、電力使用、温度、タイミング、またはデバイス（たとえば、２０、２２、２４、２６、または２７）テレメトリデータなどの、デバイス監視構成要素４０からの測定値を含むことができる。読み取られたネットワークパラメータおよび制御システムパラメータは、その後、ルールセット（たとえば、４６および５２）を生成する（ブロック７８）ために使用することができる。その理由は、それらのパラメータが、侵入および／または異常が存在しない状態での予測されるパラメータを示すからである。ルールセット（たとえば、４６および５２）が生成されると、ＩＰＳ１０は、産業用制御システム１２の動作を監視し、ルールセット（たとえば、４６および５２）に基づいて異常および／または侵入が存在するかどうかを判定することができる。

【００３４】

上述したように、ルールセット（たとえば、４６および５２）は完全でない場合がある。したがって、ルールセット（たとえば、４６および５２）は、その後、異常および／または侵入をよりよく検出するように維持／修正することができる。ルールセット（たとえば、４６および５２）は、ＩＰＳ１０がメンテナンスモードにあるときに修正することができる（判定ブロック８２）。ＩＰＳ１０がメンテナンスモードにあるとき、方法７０は

、サイバーセキュリティ監視／応答システム１５および監視ステーション１４からの偽陽性および／または偽陰性があるかチェックすることができる。その後、ＩＰＳ１０は、再び、ネットワークパラメータを読み取り（ブロック７４）、制御システムパラメータを読み取る（ブロック７６）。したがって、ルールセット（たとえば、４６および５２）は、偽陽性、偽陰性、読み取られたネットワークパラメータ、および読み取られた制御システムパラメータに基づいて修正することができる。産業用制御システム１２が何らかの侵入および／または異常を含む場合があるため、ＩＰＳ１０は、ベイズ分類器、サポートベクトルマシン、人工ニューラルネットワーク、または進化的／遺伝的アルゴリズムなどのアルゴリズムを使用することができる。

【００３５】

開示される実施形態の技術的効果は、産業用制御システム１２におけるセキュリティを改善することを含む。具体的には、開示される技法は、産業用制御システム１２内で起こるプロセスをよりよく理解するように構成されている侵入防止システム（ＩＰＳ）１０を述べる。たとえば、ＩＰＳ１０は、電力使用、温度、タイミング、またはテレメトリデータなどの、ネットワークパラメータと制御システムパラメータの両方を監視するように構成されている。さらに、ＩＰＳ１０は、産業用制御システム１２のより大きなコンテキスト内でネットワークパラメータを監視するように構成することができる。最後に、ＩＰＳ１０は、ネットワークパラメータと制御システムパラメータの両方に基づいてルールセット（たとえば、４６および５２）を生成／修正するように構成することができる。

【００３６】

本明細書は、最良モードを含む本発明を開示するために、また同様に、任意のデバイスまたはシステムを作り使用すること、および組み込まれる任意の方法を実施することを含む、本発明を当業者が実施することを可能にするために例を使用する。本発明の特許可能な範囲は、特許請求の範囲によって規定され、当業者が思い付く他の例を含むことができる。こうした他の例は、特許請求の範囲の逐語的言語と異ならない構造的要素を有する場合、または特許請求の範囲の逐語的言語と非実質的相違を有する等価な構造的要素を含む場合、特許請求の範囲内にあることを意図される。

【符号の説明】

【００３７】

１０　サイバーフィジカル侵入防止システム（ＩＰＳ）
１４　監視ステーション
１５　サイバーセキュリティ監視／応答システム
１６　コントローラ
１８　通信ネットワークインフラストラクチャ
２０　タービン
２２　センサ
２４　アクチュエータ
２６　ポンプ
２７　電気的アシスト
２８　ＣＰＵ
３０　メモリ
３２　ストレージ
３４　通信
３６　ネットワーク分析構成要素
３８　制御システム分析構成要素
４０　デバイス監視構成要素
４２　ネットワーク監視構成要素
４４　ネットワークルールセット処理構成要素
４８　制御システム監視構成要素
５０　制御システムルールセット処理構成要素

６８　機械学習および相関分析構成要素

【図１】

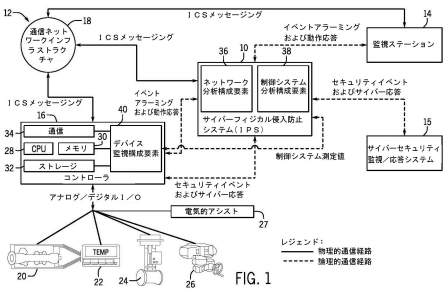

FIG. 1

【図２】

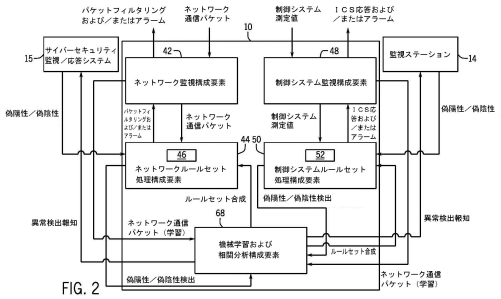

FIG. 2

【図３】

FIG. 3

【図４】

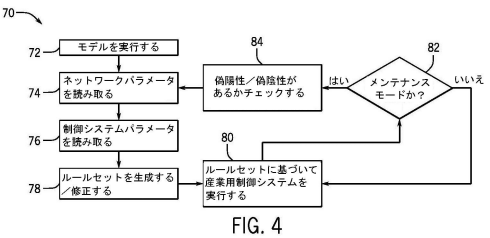

FIG. 4

フロントページの続き

(72)発明者　パリトッシュ・ディシット
インド、アンドラ・プラデッシュ、ミヤピュール、ハイテク・シティ、ブロック・１・サイバー・パール、ユニット・ナンバー０２－０１・セカンド・フロア
(72)発明者　ダニエル・サノス
カナダ、オンタリオ州・エル６シー０エム１、マークハム、マークランド、ストリート、６５０番

審査官　大桃　由紀雄

(56)参考文献　米国特許出願公開第２０１１／０２８８６９２（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／５５
Ｈ０４Ｌ　１２／６６