

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6647310号
(P6647310)

(45) 発行日 令和2年2月14日 (2020.2.14)

(24) 登録日 令和2年1月16日 (2020.1.16)

(51) Int. Cl.	F I
G05B 23/02 (2006.01)	G05B 23/02 Z
G06F 13/00 (2006.01)	G06F 13/00 351Z
G06F 21/55 (2013.01)	G06F 21/55 340

請求項の数 8 (全 17 頁)

(21) 出願番号	特願2017-541606 (P2017-541606)	(73) 特許権者	500575824
(86) (22) 出願日	平成28年2月1日 (2016.2.1)		ハネウェル・インターナショナル・インコーポレーテッド
(65) 公表番号	特表2018-513443 (P2018-513443A)		Honeywell International Inc.
(43) 公表日	平成30年5月24日 (2018.5.24)		アメリカ合衆国ニュージャージー州07950, モリス・ブレインズ, テイバー・ロード 115
(86) 国際出願番号	PCT/US2016/015890		115 Tabor Road Morris Plains NJ 07950
(87) 国際公開番号	W02016/126573		United States of America
(87) 国際公開日	平成28年8月11日 (2016.8.11)	(74) 代理人	100140109
審査請求日	平成30年8月14日 (2018.8.14)		弁理士 小野 新次郎
(31) 優先権主張番号	62/113,186		
(32) 優先日	平成27年2月6日 (2015.2.6)		
(33) 優先権主張国・地域又は機関	米国 (US)		
(31) 優先権主張番号	14/871,732		
(32) 優先日	平成27年9月30日 (2015.9.30)		
(33) 優先権主張国・地域又は機関	米国 (US)		

最終頁に続く

(54) 【発明の名称】 工業プロセス制御および自動化システムのリスク・データを収集するためのインフラストラクチャ監視ツール

(57) 【特許請求の範囲】

【請求項 1】

リスク管理システムによって、コンピューティング・システムにおいて複数のデバイスを発見するステップと、

前記リスク管理システムによって前記複数のデバイスを複数のセキュリティ・ゾーンにグループ化するステップと、

セキュリティ・ゾーン毎に、当該セキュリティ・ゾーン内にある1つ以上のデバイスが、前記リスク管理システムによって前記1つ以上のデバイスへ送られたコンフィギュレーション・データにしたがって、前記1つ以上のデバイスに関連する警告およびイベントを識別する情報を前記リスク管理システムに提供するようにさせるステップであって、前記コンフィギュレーション・データは、前記1つ以上のデバイスによって提供されるべき前記警告およびイベントを定義し、前記コンフィギュレーション・データは、データの分類を定義し前記1つ以上のデバイスによって実行されて前記警告およびイベントを前記リスク管理システムに提供される情報に変換することが可能な管理パックを含み、前記管理パックは、カテゴリ毎に構成され、収集されるデータのタイプ毎に一意のコンフィギュレーション識別子を有する、ステップと、

前記リスク管理システムによって、一意の識別値と関連付けて前記情報を格納するステップであって、前記一意の識別値が異なるタイプの情報を識別する、ステップと、

を含む、方法。

【請求項 2】

請求項1記載の方法において、前記リスク管理システムが、MICROSOFT CORPORATIONからのシステム・センター・オペレーションズ・マネージャ（SCOM）インフラストラクチャ監視ソフトウェア・ツールを使用する、方法。

【請求項3】

請求項1記載の方法であって、更に、各セキュリティ・ゾーンにおいて、各デバイスによって供給される警告およびイベントを定めるコンフィギュレーション・データを前記1つ以上のデバイスに送るステップを含む、方法。

【請求項4】

請求項1記載の方法であって、更に、前記一意の識別値を使用してクエリーを実行することによって、前記格納された情報に基づいてリスクを計算するステップを含む、方法。

10

【請求項5】

リスク管理システムであって、
コントローラと、
ディスプレイと、
を含み、前記コントローラが、
コンピューティング・システムにおいて複数のデバイスを発見し、
前記複数のデバイスを複数のセキュリティ・ゾーンにグループ化し、
セキュリティ・ゾーン毎に、当該セキュリティ・ゾーン内にある1つ以上のデバイスが、
前記コントローラによって前記1つ以上のデバイスへ送られたコンフィギュレーション・データにしたがって、前記1つ以上のデバイスに関連する警告およびイベントを識別する情報を提供するようにさせ、

20

前記コンフィギュレーション・データは、前記1つ以上のデバイスによって提供されるべき前記警告およびイベントを定義し、前記コンフィギュレーション・データは、データの分類を定義し前記1つ以上のデバイスによって実行されて前記警告およびイベントを前記リスク管理システムに提供される情報に変換することが可能な管理パックを含み、前記管理パックは、カテゴリ毎に構成され、収集されるデータのタイプ毎に一意のコンフィギュレーション識別子を有し、

一意の識別値と関連付けて前記情報を格納し、前記一意の識別値が異なるタイプの情報を識別する、

ように構成される、リスク管理システム。

30

【請求項6】

請求項5記載のリスク管理システムにおいて、前記リスク管理システムが、MICROSOFT CORPORATIONからのシステム・センター・オペレーションズ・マネージャ（SCOM）インフラストラクチャ監視ソフトウェア・ツールを使用する、リスク管理システム。

【請求項7】

請求項5記載のリスク管理システムにおいて、前記リスク管理システムが、各セキュリティ・ゾーン内にある前記1つ以上のデバイスに、各デバイスによって供給される警告およびイベントを定めるコンフィギュレーション・データを送る、リスク管理システム。

【請求項8】

40

実行可能命令がエンコードされた非一時的機械読み取り可能媒体であって、前記実行可能命令は、実行されると、リスク管理システムの1つ以上のプロセッサに、

コンピューティング・システムにおいて複数のデバイスを発見するステップと、

前記複数のデバイスを複数のセキュリティ・ゾーンにグループ化するステップと、

セキュリティ・ゾーン毎に、当該セキュリティ・ゾーン内にある1つ以上のデバイスが、前記リスク管理システムによって前記1つ以上のデバイスへ送られたコンフィギュレーション・データにしたがって、前記1つ以上のデバイスに関連する警告およびイベントを識別する情報を提供するようにさせるステップであって、前記コンフィギュレーション・データは、前記1つ以上のデバイスによって提供されるべき前記警告およびイベントを定義し、前記コンフィギュレーション・データは、データの分類を定義し前記1つ以上のデ

50

バイスによって実行されて前記警告およびイベントを前記リスク管理システムに提供される情報に変換することが可能な管理パックを含み、前記管理パックは、カテゴリ毎に構成され、収集されるデータのタイプ毎に一意のコンフィギュレーション識別子を有する、ステップと、

一意の識別値と関連付けて前記情報を格納させるステップであって、前記一意の識別値が異なるタイプの情報を識別する、ステップと、

を行わせる、非一時的機械読み取り可能媒体。

【発明の詳細な説明】

【技術分野】

【0001】

[0001] 本願は、2015年2月6日に出願された米国仮特許出願第62/113,186号の出願日の権利を主張する。この仮特許出願をここで引用したことにより、その内容が本願にも含まれるものとする。

【0002】

[0002] 本開示は、一般には、ネットワーク・セキュリティに関する。更に特定すれば、本開示は、工業プロセス制御および自動化システムのリスク・データを収集するためのインフラストラクチャ監視ツールに関する。

【背景技術】

【0003】

[0003] 処理設備は、工業プロセス制御および自動化システムを使用して管理されることが多い。従来の制御および自動化システムは、サーバ、ワークステーション、スイッチ、ルータ、ファイアウォール、セーフティ・システム、企業固有のリアル・タイム・コントローラ、および工業用現場デバイスのような、種々のネットワーク接続(networked)デバイスを含むのが通常である。多くの場合、機器は多数の異なるベンダーから来る。工業環境では、サイバー・セキュリティの関心が高まりつつあり、これらのコンポーネントの内いづれかにおいてセキュリティ脆弱性の取り組みがなされていないと、攻撃者によって、工業設備における運営を混乱させるために不当に利用され、危険な状態を生ずるおそれがある。

【発明の概要】

【0004】

[0004] 本開示は、工業プロセス制御および自動化システムのリスク・データを収集するためのインフラストラクチャ監視ツールを提供する。方法は、リスク管理システムによって、コンピューティング・システムにおける複数のデバイスを発見するステップを含む。この方法は、リスク管理システムによって、複数のデバイスを複数のセキュリティ・ゾーンにグループ化するステップを含む。この方法は、セキュリティ・ゾーン毎に、そのセキュリティ・ゾーンにおける1つ以上のデバイスに、この1つ以上のデバイスに関連する警告およびイベントを識別する情報をリスク管理システムに提供させるステップを含む。この方法は、リスク管理システムによって、一意の識別値(identifier value)と関連付けて情報を格納するステップを含み、一意の識別値は異なるタイプの情報を識別する。

【0005】

[0005] ある実施形態では、リスク管理システムは、MICROSOFT CORPORATIONからのシステム・センター・オペレーションズ・マネージャ(SCOM)インフラストラクチャ監視ソフトウェア・ツールを使用する。ある実施形態では、リスク管理システムは、各セキュリティ・ゾーン内の1つ以上のデバイスに、各デバイスによって供給されるべき警告およびイベントを定めるコンフィギュレーション・データを送る。ある実施形態では、そのセキュリティ・ゾーンにおける1つ以上のデバイスが、発見時に、そして追加のイベントが後に検出されたときにも、情報をリスク管理システムに提供する。ある実施形態では、そのセキュリティ・ゾーンにおける1つ以上のデバイスが、予め設定された(preconfigured)間隔で情報をリスク管理システムに提供する。ある実施形態では、リスク管理システムは、一意の識別値を使用してクエリーを実行することによって、

10

20

30

40

50

格納された情報に基づいてリスクを計算する。ある実施形態では、リスク管理システムは、更に、リスク値を計算するために、各セキュリティ・ゾーン内の1つ以上のデバイスから収集した情報を分類する。

【0006】

[0006] 他の技術的特徴は、以下の図、説明、および特許請求の範囲から、当業者には容易に明白になるであろう。

【図面の簡単な説明】

【0007】

[0007] 本開示の理解を更に深めるために、これより、添付図面と関連付けて以下の説明を参照する。図面において、

【図1】図1は、本開示による工業プロセス制御および自動化システムの一例を示す。

【図2】図2は、本開示にしたがって、工業プロセス制御および自動化システムのリスク・データを収集するためのインフラストラクチャ監視アーキテクチャの一例を示す。

【図3】図3は、開示する実施形態によるプロセスのフローチャートを示す。

【発明を実施するための形態】

【0008】

[0011] 以下で論ずる図、および本特許文書において本発明の原理を説明するために使用される種々の実施形態は、例示に過ぎず、決して発明の範囲を限定するように解釈してはならない。相応しく構成されたデバイスまたはシステムであればいずれにおいても、本発明の原理を実現できることが当業者には理解されよう。

【0009】

[0012] 図1は、本開示による工業プロセス制御および自動化システム100の一例を示す。図1に示すように、システム100は、少なくとも1つの製品または他の素材(material)の生産または処理を容易にする種々のコンポーネントを含む。例えば、ここでは、システム100は、1つまたは複数のプラント101a~101nにおけるコンポーネントの制御を容易にするために使用される。各プラント101a~101nは、少なくとも1つの製品または他の素材を生産するための1つ以上の製造設備のような、1つ以上の処理設備（またはその1つ以上の部分）を表す。一般に、各プラント101a~101nは、1つ以上のプロセスを実施すればよく、個々にまたは纏めてプロセス・システムと呼ぶことができる。プロセス・システムとは、一般に、何らかの方法で1つ以上の製品または他の素材を処理するように構成された任意のシステムまたはその一部を表す。

【0010】

[0013] 図1において、システム100は、プロセス制御のパデュー・モデル(Purdue model)を使用して実装される。パデュー・モデルでは、「レベル0」は1つ以上のセンサ102aと1つ以上のアクチュエータ102bとを含むことができる。センサ102aおよびアクチュエータ102bは、プロセス・システムにおいて、多種多様な機能の内任意のものを実行することができるコンポーネントを表す。例えば、センサ102aは、温度、圧力、または流量のような、プロセス・システムにおける多種多様な特性を測定することができる。また、アクチュエータ102bは、プロセス・システムにおける多種多様な特性を変化させることができる。センサ102aおよびアクチュエータ102bは任意の適したプロセス・システムにおける任意の他のまたは追加のコンポーネントを表すこともできる。センサ102aの各々は、プロセス・システムにおける1つ以上の特性を測定するのに適した任意の構造を含む。アクチュエータ102bの各々は、プロセス・システムにおける1つ以上の条件に対して効果を現す、または1つ以上の条件に作用する任意の適した構造を含む。

【0011】

[0014] 少なくとも1つのネットワーク104がセンサ102aおよびアクチュエータ102bに結合されている。ネットワーク104は、センサ102aおよびアクチュエータ102bとの相互作用を容易にする。例えば、ネットワーク104は測定データをセンサ102aから移送し、制御信号をアクチュエータ102bに供給することができる。ネ

ットワーク104は、任意の適したネットワークまたはネットワークの組み合わせを表すことができる。特定例として、ネットワーク104はイーサネット（登録商標）・ネットワーク、電子信号ネットワーク（HARTまたはFOUNDATION FIELDBUSネットワーク等）、空気制御信号ネットワーク、または任意の他のまたは追加のタイプ（1つまたは複数）のネットワーク（1つまたは複数）を表すことができる。

【0012】

[0015] パデュー・モデルでは、「レベル1」は、ネットワーク104に結合される1つ以上のコントローラ106を含むことができる。とりわけ、各コントローラ106は、1つ以上のセンサ102aからの測定値を使用して、1つ以上のアクチュエータ102bの動作を制御することができる。例えば、コントローラ106は測定データを1つ以上のセンサ102aから受信し、この測定データを使用して、1つ以上のアクチュエータ102bのために制御信号を生成することができる。各コントローラ106は、1つ以上のセンサ102aと相互作用し、1つ以上のアクチュエータ102bを制御するのに適した任意の構造を含む。各コントローラ106は、例えば、ロバスト多変数予測制御技術（RMPCT: Robust Multivariable Predictive Control Technology）コントローラ、あるいはモデル予測制御（MPC: model predictive control）または他の高度予測制御（APC: advanced predictive control）を実現する他のタイプのコントローラのような、比例-積分-微分（PID）コントローラまたは多変数コントローラを表すことができる。特定例として、各コントローラ106はリアル・タイム・オペレーティング・システムを実行するコンピューティング・デバイスを表すことができる。

【0013】

[0016] 2つのネットワーク108がコントローラ106に結合されている。ネットワーク108は、データをコントローラ106に移送する、そしてデータをコントローラ106から移送することによってというようにして、コントローラ106との相互作用を容易にする。ネットワーク108は、任意の適したネットワークまたはネットワークの組み合わせを表すことができる。特定例として、ネットワーク108は、HONEYWELL INTERNATIONAL INCからのフォールト・トレラント・イーサネット（登録商標）（FTE）ネットワークのような、イーサネット（登録商標）・ネットワークの冗長対を表すことができる。

【0014】

[0017] 少なくとも1つのスイッチ／ファイアウォール110が、ネットワーク108を2つのネットワーク112に結合する。スイッチ／ファイアウォール110は、トラフィックを1つのネットワークから他方に移送することができる。また、スイッチ／ファイアウォール110は、1つのネットワーク上におけるトラフィックが他方のネットワークに達するのを阻止することもできる。スイッチ／ファイアウォール110は、HONEYWELL CONTROL FIREWALL（CF9）デバイスのような、ネットワーク間に通信を提供するのに適した任意の構造を含む。ネットワーク112は、FTEネットワークのような、任意の適したネットワークを表すことができる。

【0015】

[0018] パデュー・モデルでは、「レベル2」は、ネットワーク112に結合された1つ以上の機械レベル・コントローラ114を含むことができる。機械レベル・コントローラ114は、コントローラ106、センサ102a、およびアクチュエータ102bの動作や制御をサポートするために種々の機能を実行し、特定の工業機器（ボイラまたは他の機械等）と関連付けることができる。例えば、機械レベル・コントローラ114は、センサ102aからの測定データ、またはアクチュエータ102bのための制御信号のような、コントローラ106によって収集または生成された情報を記録することができる。また、機械レベル・コントローラ114は、コントローラ106の動作を制御することによって、アクチュエータ102bの動作を制御するアプリケーションを実行することもできる。加えて、機械レベル・コントローラ114は、コントローラ106へのセキュア・アクセスを付与することもできる。機械レベル・コントローラ114の各々は、機械(machine

)または他の個々の機器(equipment)へのアクセスを付与する、機械または他の個々の機器の制御を行う、あるいは機械または他の個々の機器に係る動作を行うのに適した任意の構造を含む。機械レベル・コントローラ114の各々は、例えば、MICROSOFT WINDOWS(登録商標)オペレーティング・システムを実行するサーバ・コンピューティング・デバイスを表すことができる。図示されていないが、プロセス・システムにおける異なる機器を制御するために、異なる機械レベル・コントローラ114を使用することができる(ここで、各機器は、1つ以上のコントローラ106、センサ102a、およびアクチュエータ102bと関連付けられる)。

【0016】

[0019] 1つ以上のオペレータ・ステーション(operator station)116がネットワーク112に結合されている。オペレータ・ステーション116は、機械レベル・コントローラ114にユーザ・アクセスを付与するコンピューティング・デバイスまたは通信デバイスを表し、次いでコントローラ106(そしておそらくはセンサ102aおよびアクチュエータ102b)へのユーザ・アクセスを付与することができる。特定例として、オペレータ・ステーション116は、ユーザが、コントローラ106および/または機械レベル・コントローラ114によって収集された情報を使用して、センサ102aおよびアクチュエータ102bの動作履歴を見直すことを可能にすることができる。また、オペレータ・ステーション116は、ユーザが、センサ102a、アクチュエータ102b、コントローラ106、または機械レベル・コントローラ114の動作を調節することも可能にすることができる。加えて、オペレータ・ステーション116は、コントローラ106または機械レベル・コントローラ114によって生成される警告、警報、あるいは他のメッセージまたは表示を受信し表示することもできる。オペレータ・ステーション116の各々は、システム100における1つ以上のコンポーネントのユーザ・アクセスおよび制御をサポートするのに適した任意の構造を含む。オペレータ・ステーション116の各々は、例えば、MICROSOFT WINDOWS(登録商標)オペレーティング・システムを実行するコンピューティング・デバイスを表すことができる。

【0017】

[0020] 少なくとも1つのルータ/ファイアウォール118が、ネットワーク112を2つのネットワーク120に結合する。ルータ/ファイアウォール118は、セキュア・ルータまたはルータ/ファイアウォールの組み合わせのような、ネットワーク間に通信を提供するのに適した任意の構造を含む。ネットワーク120は、FTEネットワークのような、任意の適したネットワークを表すことができる。

【0018】

[0021] パデュー・モデルでは、「レベル3」は、ネットワーク120に結合された1つ以上のユニット・レベル・コントローラ122を含むことができる。各ユニット・レベル・コントローラ122は、通例、プロセス・システムにおける1つのユニットと関連付けられ、このユニットは、プロセスの少なくとも一部を実現するために一緒に動作する異なる機械の集合体を表す。ユニット・レベル・コントローラ122は、下位レベルにおけるコンポーネントの動作および制御をサポートするために種々の機能を実行する。例えば、ユニット・レベル・コントローラ122は、下位レベルにおけるコンポーネントによって収集または生成された情報を記録し、下位レベルにおけるコンポーネントを制御するアプリケーションを実行し、下位レベルにおけるコンポーネントへのセキュア・アクセスを付与することができる。ユニット・レベル・コントローラ122の各々は、プロセス・ユニットにおける1つ以上の機械または他の機器へのアクセスを付与する、1つ以上の機械または他の機器の制御を行う、あるいは1つ以上の機械または他の機器に係る動作を行うのに適した任意の構造を含む。ユニット・レベル・コントローラ122の各々は、例えば、MICROSOFT WINDOWS(登録商標)オペレーティング・システムを実行するサーバ・コンピューティング・デバイスを表すことができる。図示されていないが、プロセス・システムにおける異なるユニットを制御するためには、異なるユニット・レベル・コントローラ122を使用することができる(各ユニットは、1つ以上の機械レ

ベル・コントローラ 114、コントローラ 106、センサ 102a、およびアクチュエータ 102b と関連付けられる)。

【0019】

[0022] ユニット・レベル・コントローラ 122 へのアクセスは、1つ以上のオペレータ・ステーション 124 によって付与することもできる。オペレータ・ステーション 124 の各々は、システム 100 における 1つ以上のコンポーネントのユーザ・アクセスおよび制御をサポートするのに適した任意の構造を含む。オペレータ・ステーション 124 の各々は、例えば、MICROSOFT WINDOWS (登録商標) オペレーティング・システムを実行するコンピューティング・デバイスを表すことができる。

【0020】

[0023] 少なくとも 1つのルータ／ファイアウォール 126 が、ネットワーク 120 を 2つのネットワーク 128 に結合する。ルータ／ファイアウォール 126 は、セキュア・ルータまたはルータ／ファイアウォールの組み合わせのような、ネットワーク間に通信を提供するのに適した任意の構造を含む。ネットワーク 128 は、FTE ネットワークのような、任意の適したネットワークを表すことができる。

【0021】

[0024] パデュー・モデルでは、「レベル 4」はネットワーク 128 に結合された 1つ以上のプラント・レベル・コントローラ 130 を含むことができる。各プラント・レベル・コントローラ 130 は、通例、プラント 101a~101n の内の 1つと関連付けられ、同じ、同様の、または異なるプロセスを実現する 1つ以上のプロセス・ユニットを含むことができる。プラント・レベル・コントローラ 130 は、下位レベルにおけるコンポーネントの動作および制御をサポートするために種々の機能を実行する。特定例として、プラント・レベル・コントローラ 130 は、1つ以上の製造実行システム (MES) アプリケーション、スケジューリング・アプリケーション、あるいは他のまたは追加のプラントまたはプロセス制御アプリケーションを実行することができる。プラント・レベル・コントローラ 130 の各々は、プロセス・プラントにおける 1つ以上のプロセス・ユニットへのアクセスを付与する、1つ以上のプロセス・ユニットの制御を行う、または 1つ以上のプロセス・ユニットに関係する動作を行うのに適した任意の構造を含む。プラント・レベル・コントローラ 130 の各々は、例えば、MICROSOFT WINDOWS (登録商標) オペレーティング・システムを実行するサーバ・コンピューティング・デバイスを表すことができる。

【0022】

[0025] プラント・レベル・コントローラ 130 へのアクセスは、1つ以上のオペレータ・ステーション 132 によって付与することもできる。オペレータ・ステーション 132 の各々は、システム 100 における 1つ以上のコンポーネントへのユーザ・アクセス、および 1つ以上のコンポーネントの制御をサポートするのに適した任意の構造を含む。オペレータ・ステーション 132 の各々は、例えば、MICROSOFT WINDOWS (登録商標) オペレーティング・システムを実行するコンピューティング・デバイスを表すことができる。

【0023】

[0026] 少なくとも 1つのルータ／ファイアウォール 134 が、ネットワーク 128 を 1つ以上のネットワーク 136 に結合する。ルータ／ファイアウォール 134 は、セキュア・ルータまたはルータ／ファイアウォールの組み合わせのような、ネットワーク間に通信を提供するのに適した任意の構造を含む。ネットワーク 136 は、企業規模のイーサネット (登録商標) または他のネットワーク、あるいは更に大きなネットワーク (インターネット等) の全部または一部のような、任意の適したネットワークを表すことができる。

【0024】

[0027] パデュー・モデルでは、「レベル 5」はネットワーク 136 に結合された 1つ以上の企業レベル・コントローラ 138 を含むことができる。各企業レベル・コントローラ 138 は、通例、複数のプラント 101a~101n に対する計画動作を実行し、プラ

ント101a~101nの種々の側面を制御することができる。また、企業レベル・コントローラ138は、プラント101a~101nにおけるコンポーネントの動作および制御をサポートするために種々の機能を実行することもできる。特定例として、企業レベル・コントローラ138は、1つ以上の命令処理アプリケーション、企業リソース計画（ERP）アプリケーション、高度計画およびスケジューリング（APS）アプリケーション、あるいは任意の他のまたは追加の企業制御アプリケーションを実行することができる。企業レベル・コントローラ138の各々は、1つ以上のプラントへのアクセスを付与する、1つ以上のプラントの制御を行う、または1つ以上のプラントの制御に関係する動作を行うのに適した任意の構造を含む。企業レベル・コントローラ138の各々は、例えば、MICROSOFT WINDOWS（登録商標）オペレーティング・システムを実行するサーバ・コンピューティング・デバイスを表すことができる。この文書では、「企業」という用語は、管理すべき1つ以上のプラントまたは他の処理設備を有する組織を指す。尚、1つのプラント101aを管理すればよい場合、企業レベル・コントローラ138の機能をプラント・レベル・コントローラ130に組み込むことができることを注記しておく。

10

【0025】

[0028] 企業レベル・コントローラ138へのアクセスは、1つ以上のオペレータ・ステーション140によって付与することもできる。オペレータ・ステーション140の各々は、システム100における1つ以上のコンポーネントのユーザ・アクセスおよび制御をサポートするのに適した任意の構造を含む。オペレータ・ステーション140の各々は、例えば、MICROSOFT WINDOWオペレーティング・システムを実行するコンピューティング・デバイスを表すことができる。

20

【0026】

[0029] パデュー・モデルの種々のレベルは、1つ以上のデータベースのような、他のコンポーネントを含むことができる。各レベルと関連付けられたデータベース（1つまたは複数）は、そのレベル、またはシステム100の1つ以上の他のレベルに関連する任意の適した情報を格納することができる。例えば、ヒストリアン(historian)141をネットワーク136に結合することができる。ヒストリアン141は、システム100についての種々の情報を格納するコンポーネントを表すことができる。ヒストリアン141は、例えば、生産スケジューリングおよび最適化の間に使用される情報を格納することができる。ヒストリアン141は、情報を格納し、情報の検索を容易にするのに適した任意の構造を表す。ネットワーク136に結合された1つの集中コンポーネントとして示すが、ヒストリアン141は、システム100におけるいずれの場所に位置することもでき、あるいは複数のヒストリアンをシステム100における異なる場所に分散することもできる。

30

【0027】

[0030] 特定の実施形態では、図1における種々のコントローラおよびオペレータ・ステーションは、コンピューティング・デバイスを表すことができる。例えば、コントローラ106、114、122、130、138の各々は、1つ以上の処理デバイス142と、処理デバイス（1つまたは複数）142によって使用される、生成された、または収集された命令およびデータを格納する1つ以上のメモリ144とを含むことができる。また、コントローラ106、114、122、130、138の各々は、1つ以上のイーサネット（登録商標）・インターフェースまたはワイヤレス・トランシーバのような、少なくとも1つのネットワーク・インターフェース146も含むことができる。また、オペレータ・ステーション116、124、132、140の各々は、1つ以上の処理デバイス148と、処理デバイス（1つまたは複数）148によって使用される、生成された、または収集された命令およびデータを格納する1つ以上のメモリ150とを含むことができる。また、オペレータ・ステーション116、124、132、140の各々は、1つ以上のイーサネット（登録商標）・インターフェースまたはワイヤレス・トランシーバのような、少なくとも1つのネットワーク・インターフェース152も含むことができる。

40

【0028】

50

[0031] 先に注記したように、サイバー・セキュリティは、工業プロセス制御および自動化システムに関して、増々関心が高まりつつある。システム100におけるコンポーネントのいずれかにおいて、セキュリティ脆弱性に対する取り組みがなされていないと、攻撃者によって工業設備における運営を混乱させるために利用され、危険な状態を生ずるおそれがある。例えば、プロセス制御および自動化システムは、発熱性である工業プロセス、あるいは毒性化学薬品または原子力をも伴う工業プロセスを制御するために使用される可能性がある。これらのプロセスに対する混乱は、大きな経済的問題または安全性の問題の原因となるおそれがある。しかしながら、多くの場合、操作員(operator)は、特定の工業用地(industrial site)において稼働する全ての機器を完全に理解しているのではなく、それらの一覧表を有しているのでもない。その結果、制御および自動化システムに対する潜在的な危険の発生源を素早く判断することは、多くの場合困難である。

10

【0029】

[0032] 本開示は、種々のシステムにおける潜在的な脆弱性を理解し、システム全体に対するリスクに基づいて脆弱性に優先順位を付け、自動的／論理的にこのデータを収集し分類する解決策の必要性を認識した。これは、(方法の中でもとりわけ) リスク・マネージャ154を使用することによって遂行される。リスク・マネージャ154は、工業プロセス制御および自動化システムのリスク・データの収集をサポートするのに適した任意の構造を含む。ここでは、リスク・マネージャ154は、1つ以上の処理デバイス156と、処理デバイス(1つまたは複数)156によって使用される、生成された、または収集された命令およびデータを格納する1つ以上のメモリ158と、少なくとも1つのネットワーク・インターフェース160とを含む。各処理デバイス156は、マイクロプロセッサ、マイクロコントローラ、ディジタル信号プロセス、フィールド・プログラマブル・ゲート・アレイ、特定用途集積回路、またはディスクリット・ロジックを表すことができる。各メモリ158は、ランダム・アクセス・メモリまたはフラッシュ・メモリのような、揮発性または不揮発性記憶および検索デバイスを表すことができる。各ネットワーク・インターフェース160は、イーサネット(登録商標)・インターフェース、ワイヤレス・トランシーバ、または外部通信を容易にする他のデバイスを表すことができる。リスク・マネージャ154の機能は、任意の適したハードウェア、またはハードウェアおよびソフトウェア／ファームウェア命令の組み合わせを使用して実現することができる。

20

【0030】

[0033] 図2は、本開示にしたがって、工業プロセス制御および自動化システムのリスク・データを収集するインフラストラクチャ監視アーキテクチャ200の一例を示す。アーキテクチャ200は、リスク・マネージャ154を使用して支援または実装することができる。このアーキテクチャ200は、工業プロセス制御および自動化システムに関連するリスク・データを収集および分析し、解決すべき潜在的なセキュリティ問題を識別する。

30

【0031】

[0034] アーキテクチャ200は、この例では、サーバ210、ネットワーク・ノード220、ルール・エンジン230、監視ノード240、およびユーザ・システム250を含む。サーバ210は、リスク・マネージャ154として、または処理デバイス(1つまたは複数)、メモリ、およびネットワーク・インターフェースのようなハードウェア・コンポーネントを有する他のサーバ・データ処理システムとして実装することができる。同様に、ユーザ・システム250は、本明細書において説明するようにサーバ210と通信するように構成された、そして具体的には、本明細書において説明するプロセスを構成する(configure)ための任意のデータ処理システムであることが可能であり、リスク・マネージャ154として実装することもできる。尚、ユーザ・システム250は、実施形態によっては、サーバ210と同じ物理システム上に実装できることを注記しておく。

40

【0032】

[0035] サーバ210は、例えば、リスク・マネージャ154によって実行されると、ウィルス対策ツールまたはアプリケーション・ホワイトリスト・ツール(application whi

50

telisting tool)からのデータ、Windows（登録商標）セキュリティ・イベント、ネットワーク・セキュリティ・データ（スイッチ、ルータ、ファイアウォール、および侵入検出／防止システムの状態を含む）、バックアップ・ステータス、パッチング・ステータス、およびアセット・ポリシーのような、種々のデータを監視ノード240から収集する。他の例は、監視ノード240として示され、ワークステーション、ホワイトリスト・サーバ、ウィルス対策システム、バックアップ・サーバ、および他のセキュリティ・ソフトウェアを含む。同様に、ネットワーク・ノード220を監視することもできる。ネットワーク・ノード220は、スイッチ、ルータ、ファイアウォールを含む侵入防止システム（IPSec）、および他のネットワーク・デバイスを含むことができ、ハードウェアで実現されるかまたはソフトウェアで実現されるかを問わない。

10

【0033】

[0036] 監視ノード240を監視し始めるためには、コンフィギュレーションをユーザ・システム250から受け取る、ストレージからそれをロードする、他のデバイスまたはプロセスからそれを受け取る、あるいはそれ以外の方法によってというようにして、サーバ210にコンフィギュレーションをロードし、サーバ210が受け取ることができる。このコンフィギュレーションは、サーバ210によって監視ノード240またはネットワーク・ノード220にプッシュすることができる。監視ノード240、ネットワーク・ノード220、およびサーバ210は、コンフィギュレーション・カテゴリについて知り、データ収集の各タイプおよびサブタイプはそれ自体のカテゴリ識別子を有することができる。各ノードはデバイスをスキャンして、各デバイスまたはソフトウェア・アプリケーション（古いWindows（登録商標）のパッチ等）上において知られている脆弱性を調べ、継続的にデバイスを監視して、セキュリティ関与があるイベント（ウィルス検出またはWindows（登録商標）認証失敗等）を発見するソフトウェアまたはハードウェアを含むことができる。監視のエリアは、ウィルス対策、アプリケーション・ホワイトリスト、Windows（登録商標）セキュリティ・イベント、ネットワーク・セキュリティ（スイッチ、ルータ、ファイアウォール、および侵入検出／防止システムの状態を含む）、バックアップ・ステータス、パッチング・ステータス、およびアセット・ポリシーを含むことができるが、これらに限定されるのではない。各ノードは、そのデバイス上で生成されたイベントを警告(alert)に変換し、そのコンフィギュレーション識別子を割り当てることができる。

20

30

【0034】

[0037] ある実施形態では、コンフィギュレーション情報は、一意のセキュリティ／リスク項目データ収集をレイアウトするために使用される管理パックと、リスク・マネージャ154によって分析されるデータの分類とを含むことができる。管理パックは、カテゴリ毎に構成され、収集されるデータのタイプ毎に一意のコンフィギュレーション識別子を有することができる。このコンフィギュレーションは拡張可能にすることができる。管理パック・コンフィギュレーションは、ノードの各々に送信して実行することができ、ノードまたは他の被監視デバイスによって生成されたイベントを、警告／イベントに変換し、これらを安全にサーバ210に送る。

【0035】

40

[0038] サーバ210は、この情報を収集または受信し、この情報を分析し、この情報および分析結果を操作者（アドミニストレータ等）に提示し、情報および結果を格納し、あるいはこれらをユーザ・システム250に送信することができる。種々の実施形態では、警告／イベントは分類され一意の識別子が割り当てられる。この一意の識別子は、リスク・マネージャ154がルール・エンジン・ロジック用のデータについてポーリングおよび問い合わせを行うために使用することができ、リスク・マネージャ・データベースに送られるリスク項目を計算ために、このデータを使用することができる。

【0036】

[0039] 種々の実施形態では、ルール・エンジン230は、データ・アダプタ232を使用して、しかるべきデータを各ノードに送ることができるように、そして各ノードから

50

受信したデータを、サーバ210による使用のために、一貫したフォーマットに変換することができるように、必要に応じて、ノードの各々へのデータおよびノードの各々からのデータを変換する。データを一貫性のあるフォーマットに変換することによって、ルール・エンジン154は、「ダッシュボード」ユーザ・インターフェースを提示することができ、これによって、被監視ノードの各々からの相対的なリスクを容易に比較することができる。

【0037】

[0040] ある実施形態では、アーキテクチャ200は、MICROSOFT CORPORATIONからのシステム・センター・オペレーションズ・マネージャ (SCOM) インフラストラクチャ監視ソフトウェア・ツールを使用して実装される。SCOMツールは、通常、ITサポート要員が、収集され報告された問題を監視し解決するための情報を提供するために使用される。リスク・マネージャ154は、セキュリティ関連データおよびプロセス制御関連データを収集し、ある実施形態では、SCOMツールは、この一意で特定のデータ集合のために使用される。これらの実施形態では、リスク・マネージャ154は、SCOMツールをITサポート・システムとして使用せず、代わりに、リスク・マネージャのデータ編成要件をサポートするための、非常に特定のセキュリティおよびリスク・データ収集システムとして使用する。勿論、特定の特許請求されなければ、特許請求する実施形態はSCOMの実施態様には限定されず、SCOMツールの実施態様に関係するとして本明細書において説明される特定の機能または動作は、SCOMツールに特に限定されるのではなく、アーキテクチャ200またはリスク・マネージャ154の他の実施態様にも適用されることは、当業者には認められよう。

【0038】

[0041] プロセス制御および自動化システム100では、SCOMツール（または他のツール）は、システム100においてデバイスを発見するため、そしてこれらのデバイスのデータベースを作成するために使用され、更に分析するために、デバイスをセキュリティ・ゾーンにグループ化する。一旦この発見が完了したなら、特定のセキュリティ／リスク項目データ収集のために、管理パックをターゲット・デバイスにプッシュするまたは送ることができる。管理パックがターゲット・デバイス上の監視サービスにおいてセキュリティ／リスクのために起動されると、特定の1組のデータを作成する。このデータは、SCOMデータ・パケット内に組み込まれた既定の一意の識別値に基づいて、SCOMツールに送られる。このプロセスは、本システムにおける複数のターゲット・デバイスのために繰り返すことができる。SCOMツールによって収集されたデータは、データ収集地点からのデータに組み込まれた一意の識別子に基づいて、リスク・マネージャ154によって利用される。種々の実施形態では、設計、管理パックは、SCOM製品コネクタ(SCOM product connector)に特化することができる。

【0039】

[0042] リスク・マネージャ154によって種々のデータ収集方法を使用することができる。例えば、SCOMツールによってデータ・アダプタ232を登録することができ、特定のデータ収集に基づいて、業務データベース・クエリー(operational database queries)を作ることができる。各データ・アダプタ232は、既定の間隔で、その特定のセキュリティ／リスク項目値についての情報をポーリングすることができる。各業務データベース・クエリーは、既定の間隔で、その特定のセキュリティ／リスク項目値についてのポーリング情報を収集することができる。SCOMツールにおいてデータを収集し、編成し、利用する手法が、分類されており更にモジュール状であることが、SCOMツールを含むシステムまたはリスク管理ツールの使用を非常に異なる独特のものにする1つの要素となる。一旦このデータがリスク・マネージャ154によって消費されたなら、そのデータは分離および編成され、ルール・エンジン230は、収集されたデータを使用して、一層効率的にリスク値を計算することができる。データ・アダプタ232は、それぞれのデータ・カテゴリに対して使用することができ、SCOMツール、リスク・マネージャ154、またはサーバ210に登録することができる。これによって、モジュール状設計におけ

る使用のために、データ項目の自動化が可能になり、システムのデータ収集効率を高めるまたは最大化するのに役立つ。

【0040】

[0043] 図3は、開示する実施形態によるプロセス300のフローチャートを示す。プロセス300は、例えば、リスク・マネージャ154、アーキテクチャ200、または説明した通りに実行するように構成された他のデバイスによって実行することができる。他のデバイスは、何らかのバージョンのSCOMを実装し、説明した通りに実行するように変更されたシステムを含み、これらの全てを以下では包括的に「リスク管理システム」と呼ぶ。

【0041】

[0044] リスク管理システムは、コンピューティング・システムにおいて複数のデバイスを発見する(305)。これらのデバイスは、アーキテクチャ200またはシステム100に関係するとして先に説明したデバイスの内任意のものを含むことができ、具体的には、監視ノード240またはネットワーク・ノード220に関係するデバイスの内任意のものを含む。

【0042】

[0045] リスク管理システムは、複数のデバイスを複数のセキュリティ・ゾーンにグループ化する(310)。例えば、デバイスのタイプ、デバイスによって引き起こされるリスクのタイプ、デバイスによって引き起こされるリスクの厳しさ、または他の類似項目にしたがって、デバイスをセキュリティ・ゾーンにグループ化することができる。具体的には、セキュリティ・ゾーンは、監視ノード240に対応するセキュリティ・ゾーン、およびネットワーク・ノード220に対応するセキュリティ・ゾーンを含むことができる。

【0043】

[0046] セキュリティ・ゾーン毎に、リスク管理システムは、そのセキュリティ・ゾーン内にある1つ以上のデバイスに、1つ以上のデバイスに関連する警告およびイベントを識別する情報を提供させ、この情報を受け取る(315)。これは、例えば、管理パックまたは他のコンフィギュレーション・データをデバイスの各々に送ることによって、デバイスによって提供されるべき警告およびイベントを定めるステップを含むことができる。この情報は、工業プロセス制御および自動化システムのリスク・データを含むことができる。ある場合には、特化された管理パックまたはコンフィギュレーションが、システム・ソフトウェア・パッチに対する変更があるときに、リスク管理システムに警告することができる。リスク管理システムは、関連システム・イベントを収集してリスク警告に変換することができ、更に発見時に各デバイスのリスク・データの初期情報を得て、追加のイベントを検出し、後にこれらのイベントが検出されるに連れて、そして検出されたときにシステムに警告することができる。

【0044】

[0047] 種々の実施形態では、データ・アダプタによってこの情報および他の警告データを収集し、ルール・エンジンによって情報のそれぞれの項目を計算することができるように、設定された間隔で、サーバまたはルール・エンジンによってポーリングすることができる。

【0045】

[0048] リスク管理システムは、一意の識別値と関連付けてこの情報を格納し(320)、一意の識別値は異なるタイプの情報を識別する。この情報、あるいは他のイベント・データまたは警告データは、収集された情報に基づいてルール・エンジンがリスクを計算できるように、一意の識別子を使用して、リスク管理システムによって問い合わせることができる。

【0046】

[0049] ある実施形態では、デバイスを監視してセキュリティまたはリスク情報を得るために、被監視デバイスの一部または全部に監視エージェントをインストールすることができる。エージェントをインストールすることができないデバイスについては、例えば、

10

20

30

40

50

ネットワーク・デバイスのコンフィギュレーションを読み取ることによって、サーバまたは他の専用エージェントをリスク管理システムによって監視することができる。

【0047】

[0050] 図1は、工業プロセス制御および自動化システム100の一例を示すが、図1に対して種々の変更を行うこともできる。例えば、制御および自動化システムは、任意の数のセンサ、アクチュエータ、コントローラ、サーバ、オペレータ・ステーション、ネットワーク、リスク・マネージャ、および他のコンポーネントを含むことができる。また、図1におけるシステム100の構成および配置も例示のために過ぎない。個々の必要性にしたがって、コンポーネントを追加する、削除する、組み合わせる、または任意の他の適した構成(configuration)に配することができる。更に、特定の機能がシステム100の特定のコンポーネントによって実行されることを説明した。これは例示のために過ぎない。一般に、制御および自動化システムは、多様に構成変更可能であり、個々の必要性にしたがっていずれの適した方法でも構成することができる。加えて、図1は、リスク・マネージャ154の機能を使用することができる環境例を示す。この機能は、他の適したデバイスまたはシステムのいずれでも使用することができる。

10

【0048】

[0051] 図2は、工業プロセス制御および自動化システムのリスク・データを収集するためのインフラストラクチャ監視アーキテクチャ200の一例を示すが、図2に対して種々の変更を行うことができる。例えば、図2におけるコンポーネントおよびサブコンポーネントの機能的分割は、例示のために過ぎない。種々のコンポーネントまたはサブコンポーネントを組み合わせること、更に細分化すること、再構成すること、または削除することができ、更に個々の必要性にしたがって追加のコンポーネントまたはサブコンポーネントを追加することもできる。

20

【0049】

[0052] 尚、本明細書において示したリスク・マネージャ154および／またはインフラストラクチャ監視アーキテクチャ200は、以下の以前に出願された特許出願および同時に提出された特許出願（ここで引用したことにより、これらの特許出願の全てはその内容が本願にも含まれるものとする）において記載されている種々の特徴の任意の組み合わせまたは全てと合わせて使用すること、または動作することができることを注記しておく。

30

・ "DYNAMIC QUANTIFICATION OF CYBER-SECURITY RISKS IN A CONTROL SYSTEM"（制御システムにおけるサイバー・セキュリティ・リスクの動的定量化）と題する米国特許出願第14/482, 888号。

・ "ANALYZING CYBER-SECURITY RISKS IN AN INDUSTRIAL CONTROL ENVIRONMENT"（工業制御環境におけるサイバー・セキュリティ・リスクの分析）と題する米国仮特許出願第62/036, 920号。

・ "RULES ENGINE FOR CONVERTING SYSTEM-RELATED CHARACTERISTICS AND EVENTS INTO CYBER-SECURITY RISK ASSESSMENT VALUES"（システム関連特性およびイベントをサイバー・セキュリティ・リスク評価値に変換するルール・エンジン）と題する米国仮特許出願第62/113, 075号、およびこれと同時に提出された同様の名称の対応する通常米国特許出願第14/871, 695号（整理番号H0048932-0115）。

40

・ "NOTIFICATION SUBSYSTEM FOR GENERATING CONSOLIDATED, FILTERED, AND RELEVANT SECURITY RISK-BASED NOTIFICATIONS"（統合、選別、および関連セキュリティ・リスク・ベース通知を生成する通知サブシステム）と題する米国仮特許出願第62/113, 221号、およびこれと同時に提出された同様の名称の対応する通常米国特許出願第14/871, 521号（整理番号H0048937-0115）。

・ "TECHNIQUE FOR USING INFRASTRUCTURE MONITORING SOFTWARE TO COLLECT CYBER-SECURITY RISK DATA"（インフラストラクチャ監視ソフトウェアを使用してサイバー・セキュリティ・リスク・データを収集する技法）と題する米国仮特許出願第62/113, 100号、およびこれと同時に提出された同様の名称の対応する通常米国特許出願第14/87

50

1, 855号(整理番号H0048943-0115)。

・"PATCH MONITORING AND ANALYSTS"(パッチ監視および分析)と題する米国仮特許出願第62/113, 165号、およびこれと同時に出願された同様の名称の対応する通常米国特許出願第14/871, 921号(整理番号H0048973-0115)。

・"APPARATUS AND METHOD FOR AUTOMATIC HANDLING OF CYBER-SECURITY RISK EVENTS"(サイバー・セキュリティ・リスク・イベントの自動処理装置および方法)と題する米国仮特許出願第62/113, 152号、およびこれと同時に出願された同様の名称の対応する通常米国特許出願第14/871, 503号(整理番号H0049067-0115)。

・"APPARATUS AND METHOD FOR DYNAMIC CUSTOMIZATION OF CYBER-SECURITY RISK RULES"(サイバー・セキュリティ・リスク項目規則の動的カスタム化装置および方法)と題する米国仮特許出願第62/114, 928号、およびこれと同時に出願された同様の名称の対応する通常米国特許出願第14/871, 605号(整理番号H0049099-0115)。

・"APPARATUS AND METHOD FOR PROVIDING POSSIBLE CAUSES, RECOMMENDED ACTIONS, AND POTENTIAL IMPACTS RELATED TO IDENTIFIED CYBER-SECURITY RISK ITEMS"(識別されたサイバー・セキュリティ・リスク項目に関係付けて、可能な原因、推奨されるアクション、および潜在的な影響を提示する装置および方法)と題する米国仮特許出願第62/114, 865号、およびこれと同時に出願された同様の名称の対応する通常米国特許出願第14/871, 814号(整理番号H0049103-0115)。

・"APPARATUS AND METHOD FOR TYING CYBER-SECURITY RISK ANALYSIS TO COMMON RISK METHODOLOGIES AND RISK LEVELS"(サイバー・セキュリティ・リスク分析を共通のリスク方法およびリスク・レベルに結び付ける装置および方法)と題する米国仮特許出願第62/114, 937号、およびこれと同時に出願された同様の名称の対応する通常米国特許出願第14/871, 136号(整理番号H0049104-0115)。

・"RISK MANAGEMENT IN AN AIR-GAPPED ENVIRONMENT"(気中環境におけるリスク管理)と題する米国仮特許出願第62/116, 245号、およびこれと同時に出願された同様の名称の対応する通常米国特許出願第14/871, 547号(整理番号H0049081-0115)。

【0050】

[0053] ある実施形態では、本特許文書において記載した種々の機能は、コンピュータ・プログラムによって実現されるか、またはサポートされる。コンピュータ・プログラムは、コンピュータ読み取り可能プログラム・コードによって形成され、コンピュータ読み取り可能媒体に具体化される。「コンピュータ読み取り可能プログラム・コード」という句は、ソース・コード、オブジェクト・コード、および実行可能コードを含む、あらゆるタイプのコンピュータ・コードを含む。「コンピュータ読み取り可能媒体」という句は、リード・オンリ・メモリ(ROM)、ランダム・アクセス・メモリ(RAM)、ハード・ディスク・ドライブ、コンパクト・ディスク(CD)、デジタル・ビデオ・ディスク(DVD)、または任意の他のタイプのメモリのような、コンピュータによってアクセス可能な任意のタイプの媒体を含む。「非一時的」コンピュータ読み取り可能媒体は、一時的な電子または他の信号を移送する有線、ワイヤレス、光、または他の通信リンクを除外する。非一時的コンピュータ読み取り可能媒体は、データを永続的に格納することができる媒体、および再書き込み可能光ディスクまたは消去可能メモリ・デバイスのような、データを格納し後に上書きすることができる媒体を含む。

【0051】

[0054] 本特許文書全体において使用されたある種の単語および句の定義を明記することは都合がよいと考えられる。「アプリケーション」および「プログラム」という用語は、1つ以上のコンピュータ・プログラム、ソフトウェア・コンポーネント、1組の命令、手順、関数、オブジェクト、クラス、インスタンス、関連データ、または適したコンピュータ・コード(ソース・コード、オブジェクト・コード、または実行可能コードを含む)

における実装に合わせて構成されたその一部を指す。「通信する」という用語およびその派生語は、直接および間接双方の通信を含む。「含む」(include)および「備える」(comprise)、ならびにその派生語は、限定のない包含を意味する。「または」という用語は、包含的であり、および/またはを意味する。「と関連付けられた」という句およびその派生語は、含む、内部に含まれる、相互接続する、収容する(contain)、内部に収容される、～にまたは～と接続する、～にまたは～と結合する、～と通信可能である、～と協働する、交互配置する(interleave)、並置する、近接する、～にまたは～と結び付けられる(bound)、有する、の特性を有する、～にまたは～と関係を有する等を意味することができる。「少なくとも1つの」という句は、項目のリストと共に使用されるとき、掲示された項目の内1つ以上の異なる組み合わせが使用されてもよく、更にリストにおける1つの項目のみが必要とされてもよいことを意味する。例えば、「A、B、およびCの少なくとも1つ」は、A、B、C、AおよびB、AおよびC、BおよびC、ならびにAおよびBおよびCの組み合わせのいずれも含む。

【0052】

[0055] 本開示はある種の実施形態、および総合的に関連する方法について説明したが、これらの実施形態および方法の改変ならびに置換(permutation)は当業者には明白であろう。したがって、以上の実施形態例の説明は、本開示を定めるのでも、制約するのでもない。また、以下の特許請求の範囲によって定められる本開示の主旨および範囲から逸脱することなく、他の変更、置換、および改変も可能である。

【図 1】

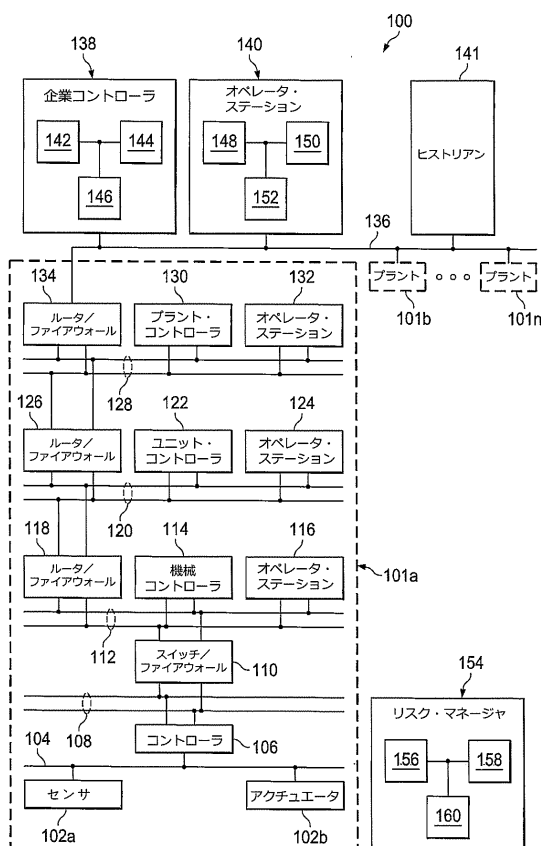


FIG. 1

【図 2】

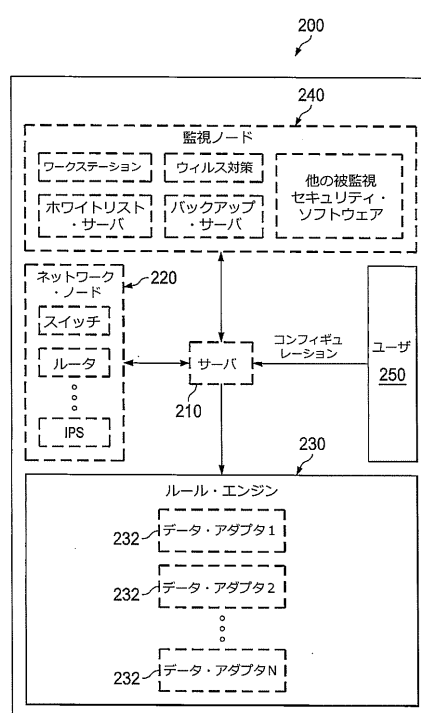


FIG. 2

【図 3】

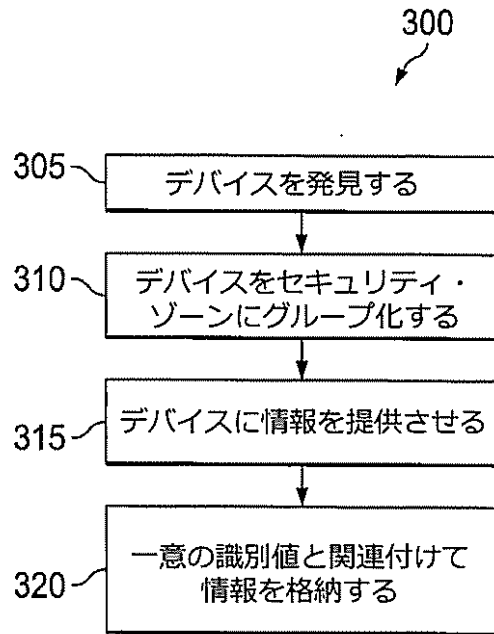


FIG. 3

フロントページの続き

- (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 100138759
弁理士 大房 直樹
- (72)発明者 タラマンチ, ベンカータ・スリニバサル・レディー
アメリカ合衆国ニュージャージー州07950, モリス・ブレインズ, テイバー・ロード 115
, エム/エス 4ディー3 ピー・オー・ボックス 377, ハネウェル・インターナショナル・
インコーポレーテッド, インテレクチュアル・プロパティーパテント・サーヴィシズ
- (72)発明者 ダイエットリッチ, ケネス・ダブリュー.
アメリカ合衆国ニュージャージー州07950, モリス・ブレインズ, テイバー・ロード 115
, エム/エス 4ディー3 ピー・オー・ボックス 377, ハネウェル・インターナショナル・
インコーポレーテッド, インテレクチュアル・プロパティーパテント・サーヴィシズ
- (72)発明者 ボイス, エリック・ティー.
アメリカ合衆国ニュージャージー州07950, モリス・ブレインズ, テイバー・ロード 115
, エム/エス 4ディー3 ピー・オー・ボックス 377, ハネウェル・インターナショナル・
インコーポレーテッド, インテレクチュアル・プロパティーパテント・サーヴィシズ
- (72)発明者 コワルチック, アンドリュー・ダブリュー.
アメリカ合衆国ニュージャージー州07950, モリス・ブレインズ, テイバー・ロード 115
, エム/エス 4ディー3 ピー・オー・ボックス 377, ハネウェル・インターナショナル・
インコーポレーテッド, インテレクチュアル・プロパティーパテント・サーヴィシズ
- (72)発明者 ガデ, ガネシュ・ピー.
アメリカ合衆国ニュージャージー州07950, モリス・ブレインズ, テイバー・ロード 115
, エム/エス 4ディー3 ピー・オー・ボックス 377, ハネウェル・インターナショナル・
インコーポレーテッド, インテレクチュアル・プロパティーパテント・サーヴィシズ

審査官 牧 初

- (56)参考文献 米国特許出願公開第2008/0235801 (US, A1)
特開2010-152878 (JP, A)
米国特許出願公開第2013/0326476 (US, A1)
米国特許出願公開第2016/0217160 (US, A1)
米国特許出願公開第2016/0212165 (US, A1)

(58)調査した分野(Int.Cl., DB名)

G05B 23/00-23/02
G05B 19/00-19/05
G05B 9/00-9/05