(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7383368号
(P7383368)

(45)発行日　令和5年11月20日(2023.11.20)

(24)登録日　令和5年11月10日(2023.11.10)

(51)国際特許分類
Ｇ０５Ｂ　23/02　(2006.01)

ＦＩ
Ｇ０５Ｂ　23/02　３０１Ｚ

請求項の数　28　外国語出願　（全39頁）

(21)出願番号　特願2017-205476(P2017-205476)
(22)出願日　平成29年10月24日(2017.10.24)
(65)公開番号　特開2018-106689(P2018-106689A)
(43)公開日　平成30年7月5日(2018.7.5)
審査請求日　令和2年10月20日(2020.10.20)
(31)優先権主張番号　15/332,622
(32)優先日　平成28年10月24日(2016.10.24)
(33)優先権主張国・地域又は機関
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 ７８６８１－７４３０ 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 エマーソン プロセス マネージメント
(74)代理人　110002860
弁理士法人秀和特許事務所
(72)発明者　エリック ロトヴォルド
アメリカ合衆国 ミネソタ ５５１１８ ウエスト セント ポール メンドータ ロード １５９
(72)発明者　マーク ジェイ． ニクソン

最終頁に続く

(54)【発明の名称】　プロセスプラントから別のシステムへの通信を安全に転送するための方法、システム

(57)【特許請求の範囲】

【請求項１】

プロセスプラントから別のシステムへの通信を安全に転送するための方法であって、

フィールドゲートウェイにおいて、プロセスプラントネットワークと、前記フィールドゲートウェイとエッジゲートウェイとの間の双方向通信を防止するように構成されたデータダイオードと、を相互接続し、前記データダイオードを経由して前記エッジゲートウェイに、前記プロセスプラントの１つ以上のデバイスの各々を記述するそれぞれのコンテキスト情報であって、前記１つ以上のデバイスの前記各々のデバイスの識別子の指標と、前記１つ以上のデバイスの前記各々のデバイスによって生成されたデータが、前記データダイオードを経由して前記エッジゲートウェイに、前記フィールドゲートウェイにより提供されるべきそれぞれの速度の指標と含む前記コンテキスト情報を、複数のコンテキスト設定フェーズの各コンテキスト設定フェーズ中において反復的に告知し、前記エッジゲートウェイが前記１つ以上のデバイスを検出することと、

前記各コンテキスト設定フェーズの後に発生するそれぞれのデータ配信フェーズにおいて、（ｉ）前記プロセスプラントがプロセスを制御するように動作している間に、前記１つ以上のデバイスの前記各々のデバイスによって生成されたデータを、前記プロセスプラントネットワークを介して前記フィールドゲートウェイで受信することと、（ｉｉ）前記フィールドゲートウェイによって、前記データダイオードを経由して前記エッジゲートウェイに、前記各コンテキスト設定フェーズ中に前記エッジゲートウェイに送信されるそれぞれのコンテキスト情報に従って、且つ前記データダイオードを介して前記プロセスプラ

ントで生成されたデータを送信するために使用される通信プロトコルのパブリッシングメカニズムを使用して、前記１つ以上のデバイスの前記各々のデバイスによって生成されたデータをパブリッシュすることと、を含む、方法。

【請求項２】

前記１つ以上のデバイスに含まれる特定のデバイスを記述する前記それぞれのコンテキスト情報を反復的に告知することが、前記特定のデバイスを記述する前記それぞれのコンテキスト情報を周期的に送信することを含み、周期性が、失われたデータのアプリケーションの許容差に基づいており、前記アプリケーションが、前記特定のデバイスによって生成される前記データのコンシューマであり、前記アプリケーションが、前記エッジゲートウェイに通信可能に接続される、請求項１に記載の方法。

【請求項３】

前記フィールドゲートウェイによって、前記１つ以上のデバイスに含まれる特定のデバイスにポーリングを送信することをさらに含み、

前記フィールドゲートウェイにおいて、前記１つ以上のデバイスの前記各々のデバイスによって生成されたデータを受信することが、前記フィールドゲートウェイにおいて、前記ポーリングに応答して前記特定のデバイスによって生成されたデータを受信することを含む、請求項１又は２に記載の方法。

【請求項４】

前記１つ以上のデバイスの前記各々のデバイスによって生成されたデータを受信することが、診断結果を示すデータを受信することを含む、請求項１から３のいずれか一項に記載の方法。

【請求項５】

前記１つ以上のデバイスの前記各々のデバイスの前記それぞれのコンテキスト情報を反復的に告知することが、コマンド０、コマンド２０、コマンド５０、コマンド７４、またはコマンド１０５を含むＨＡＲＴプロトコルコマンドの群からの少なくとも１つのＨＡＲＴプロトコルコマンドを使用して、前記１つ以上のデバイスの前記各々のデバイスについて前記それぞれのコンテキスト情報を反復的に送信することを含む、請求項１から４のいずれか一項に記載の方法。

【請求項６】

前記１つ以上のデバイスの前記各々のデバイスによって生成されたデータを前記データダイオードを経由してパブリッシュすることが、ＨＡＲＴ－ＩＰ（登録商標）プロトコルを使用して、前記データダイオードを経由して前記１つ以上のデバイスの前記各々のデバイスによって生成されたデータをパブリッシュすることを含む、請求項１から５のいずれか一項に記載の方法。

【請求項７】

前記１つ以上のデバイスの前記各々のデバイスによって生成されたデータを前記データダイオードを経由してパブリッシュすることが、ＪＳＯＮフォーマットを使用して前記データダイオードを経由して前記１つ以上のデバイスの前記各々のデバイスによって生成されたデータをパブリッシュすることを含む、請求項１から６のいずれか一項に記載の方法。

【請求項８】

前記フィールドゲートウェイにおいて、前記１つ以上のデバイスの前記各々のデバイスによって生成されたデータを受信することが、前記フィールドゲートウェイにおいて、ＨＡＲＴ－ＩＰ（登録商標）プロトコルを介して、前記１つ以上のデバイスの前記各々のデバイスによって生成されたデータのうちの少なくとも一部を受信することを含む、請求項１から７のいずれか一項に記載の方法。

【請求項９】

前記１つ以上のデバイスの前記各々のデバイスによって生成されたデータのうちの少なくとも一部を前記ＨＡＲＴ－ＩＰプロトコルを介して受信することが、前記１つ以上のデバイスの前記各々によって前記データダイオードを介して配信するために、前記フィールドゲートウェイにパブリッシュされたデータを受信することを含む、請求項８に記載の方

法。
【請求項１０】
プロセスプラントから別のシステムへの通信を安全に転送するためのシステムであって、
プロセスプラントネットワークに通信可能に結合されたフィールドゲートウェイと、
前記別のシステムに通信可能に結合されたエッジゲートウェイと、
前記フィールドゲートウェイと前記エッジゲートウェイとを相互接続するデータダイオードであって、前記エッジゲートウェイによって送信された通信が前記フィールドゲートウェイに進入することを防止するように構成される、データダイオードと、を備え、
各コンテキスト設定フェーズの後に発生するそれぞれのデータ配信フェーズにおいて、前記プロセスプラントが工業プロセスを制御するように動作している間に、前記プロセスプラントに含まれる１つ以上のデバイスによって生成されたデータが、前記プロセスプラントネットワークを介して前記フィールドゲートウェイにおいて受信され、前記フィールドゲートウェイによって、前記データダイオードを経由して前記エッジゲートウェイに、前記各コンテキスト設定フェーズ中にエッジゲートウェイに送信されるそれぞれのコンテキスト情報に従って、且つ前記データダイオードを介して前記プロセスプラントで生成されたデータを送信するために使用される通信プロトコルのパブリッシングメカニズムを介してパブリッシュされ、
前記各コンテキスト設定フェーズ中において、前記エッジゲートウェイが前記１つ以上のデバイスを検出するように、前記フィールドゲートウェイによって、前記データダイオードを経由して前記エッジゲートウェイに、前記１つ以上のデバイスの前記それぞれのコンテキスト情報が告知され、各デバイスのそれぞれのアイデンティティの指標と、前記各々のデバイスによって前記データが生成されるそれぞれの速度の指標とを含む、１つ以上のデバイスのそれぞれのコンテキスト情報が、前記フィールドゲートウェイによってパブリッシュされる、システム。
【請求項１１】
前記通信プロトコルは、ＨＡＲＴ－ＩＰ（登録商標）プロトコルである、請求項１０に記載のシステム。
【請求項１２】
前記通信プロトコルは、ＪＳＯＮフォーマットを使用する、請求項１０に記載のシステム。
【請求項１３】
前記データダイオードが、イーサネット接続される、請求項１０から１２のいずれか一項に記載のシステム。
【請求項１４】
前記データダイオードが、直列接続される、請求項１０から１２のいずれか一項に記載のシステム。
【請求項１５】
前記別のシステムが、
前記プロセスプラントで起こる状況及び／または事象を監視することと、
前記プロセスプラントで起こる状況及び／または事象を感知することと、
前記プロセスプラントによって制御されているプロセスの少なくとも一部分を監視することと、
前記生成されたデータを使用して記述的分析を遂行することと、
前記生成されたデータを使用して規範的分析を遂行すること、または、
前記生成されたデータに基づいて、前記プロセスプラントの少なくとも一部分を修正するための規範的機能を生成することと、のうちの少なくとも１つを行うように構成される、請求項１０から１４のいずれか一項に記載のシステム。
【請求項１６】
前記別のシステムが、少なくとも部分的に１つ以上のクラウドコンピューティングシステムで実装される、請求項１０から１５のいずれか一項に記載のシステム。

【請求項１７】
前記プロセスプラントが工業プロセスを制御するように動作している間に、前記１つ以上のデバイスによって生成された前記データが、前記１つ以上のデバイスによって生成された動的データ、または前記１つ以上のデバイスの診断もしくは試験の結果として生成された診断データのうちの少なくとも１つを含む、請求項１０から１６のいずれか一項に記載のシステム。
【請求項１８】
前記別のシステムで実行されるアプリケーションが、前記プロセスプラントに含まれる前記１つ以上のデバイスによって生成された前記データのうちの少なくとも一部のコンシューマである、請求項１０から１７のいずれか一項に記載のシステム。
【請求項１９】
前記エッジゲートウェイが、前記プロセスプラントに含まれる前記１つ以上のデバイスによって生成された前記データのうちの少なくとも一部をパブリッシュし、前記別のシステムで実行される前記アプリケーションが、前記エッジゲートウェイによってパブリッシュされた前記データのサブスクライバである、請求項１８に記載のシステム。
【請求項２０】
前記フィールドゲートウェイが、前記データダイオードを経由して前記エッジゲートウェイに、前記パブリッシングメカニズムを介して、前記１つ以上のデバイスの前記各々のデバイスを記述するそれぞれの情報をさらにパブリッシュする、請求項１０から１９のいずれか一項に記載のシステム。
【請求項２１】
前記１つ以上のデバイスの前記各々のデバイスを記述する前記それぞれの情報が、前記１つ以上のデバイスの前記各々のデバイスのそれぞれのアイデンティティの指標と、前記１つ以上のデバイスの前記各々のデバイスによって生成されたデータがパブリッシュされるべきそれぞれの速度と、を含む、請求項２０に記載のシステム。
【請求項２２】
前記１つ以上のデバイスの前記各々のデバイスを記述する前記それぞれの情報が、前記１つ以上のデバイスの前記各々のデバイスの状態の指標をさらに含む、請求項２１に記載のシステム。
【請求項２３】
前記１つ以上のデバイスによって生成された前記データが、受信され、前記フィールドゲートウェイに提供される無線ゲートウェイをさらに含む、請求項１０から２２のいずれか一項に記載のシステム。
【請求項２４】
前記無線ゲートウェイが、ＷｉｒｅｌｅｓｓＨＡＲＴ（登録商標）である、請求項２３に記載のシステム。
【請求項２５】
前記無線ゲートウェイが、前記１つ以上のデバイスによって生成された前記データを、ＨＡＲＴ－ＩＰプロトコルを使用して前記フィールドゲートウェイに提供する、請求項２３又は２４に記載のシステム。
【請求項２６】
前記１つ以上のデバイスのうちの少なくとも１つが、それぞれの生成されたデータを前記データダイオードを介して配信するために、前記無線ゲートウェイにパブリッシュする、請求項２３から２５のいずれか一項に記載のシステム。
【請求項２７】
前記それぞれの生成されたデータがパブリッシュされる前記無線ゲートウェイが、前記それぞれの生成されたデータのサブスクライバである、請求項２６に記載のシステム。
【請求項２８】
前記無線ゲートウェイが、前記１つ以上のデバイスのうちの少なくとも１つをポーリングして、それぞれの生成されたデータを取得する、請求項２３から２７のいずれか一項に

記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
相互参照
本開示は、２０１４年１０月６日に出願され、「Ｒｅｇｉｏｎａｌ Ｂｉｇ Ｄａｔａ ｉｎ Ｐｒｏｃｅｓｓ Ｃｏｎｔｒｏｌ Ｓｙｓｔｅｍｓ」と題する共同所有の米国特許出願第１４／５０７、１８８号、２０１６年９月２３日に出願され、「Ｄａｔａ Ａｎａｌｙｔｉｃｓ Ｓｅｒｖｉｃｅｓ ｆｏｒ Ｄｉｓｔｒｉｂｕｔｅｄ Ｉｎｄｕｓｔｒｉａｌ Ｐｅｒｆｏｒｍａｎｃｅ Ｍｏｎｉｔｏｒｉｎｇ」と題する共同所有の米国特許出願第１５／２７４、５１９号、２０１６年９月２３日に出願され、「Ｄｉｓｔｒｉｂｕｔｅｄ Ｉｎｄｕｓｔｒｉａｌ Ｐｅｒｆｏｒｍａｎｃｅ Ｍｏｎｉｔｏｒｉｎｇ ａｎｄ Ａｎａｌｙｔｉｃｓ」という名称の米国特許出願第１５／２７４、２３３号；及び２０１６年１０月２４日に出願された「Ｐｒｏｃｅｓｓ Ｄｅｖｉｃｅ Ｃｏｎｄｉｔｉｏｎ ａｎｄ Ｐｅｒｆｏｒｍａｎｃｅ Ｍｏｎｉｔｏｒｉｎｇ」と題する共同所有の米国特許出願第１５／３３２、５２１号に関連し、その全体の開示は参照により本明細書に組み込まれる。
【０００２】
本開示は、概して、プロセスプラント及びプロセス制御システムに関し、より具体的には、ローカルプロセスプラント／プロセス制御システムと、パーベイシブセンシングシステムなどのローカルプロセス制御プラント／システムにサービスを提供する遠隔システムとの間の通信をセキュリティ保護することに関する。
【背景技術】
【０００３】
化学、石油、または他のプロセスプラントで使用されるものなどの分散プロセス制御システムは、アナログ、デジタル、もしくはアナログ／デジタル結合バスを介して、または無線通信リンクもしくはネットワークを介して、１つ以上のフィールドデバイスに通信可能に結合された１つ以上のプロセスコントローラを典型的に含む。例えばバルブ、バルブ位置決め器、スイッチ、及びトランスミッタ（例えば、温度、圧力、レベル、及び流量センサ）であってもよいフィールドデバイスは、プロセス環境内に位置し、例えばバルブの開閉、プロセスプラントまたはシステム内で実行されている１つ以上のプロセスを制御するために、圧力、温度などのプロセスパラメータの測定などのような、一般に物理的またはプロセス制御機能を遂行する。周知のフィールドバスプロトコルに準拠するフィールドデバイスなどのスマートフィールドデバイスは、制御計算、アラーム機能、及びコントローラ内で通常実装される他の制御機能を遂行することもできる。典型的にプラント環境内に位置するプロセスコントローラは、フィールドデバイスによって作られたプロセス測定値及び／またはフィールドデバイスに関する他の情報を示す信号を受信し、例えば、プロセス制御決定を行い、受信した情報に基づいて制御信号を生成し、ＨＡＲＴ（登録商標）、ＷｉｒｅｌｅｓｓＨＡＲＴ（登録商標）、ＦＯＵＮＤＡＴＩＯＮ（登録商標）Ｆｉｅｌｄｂｕｓフィールドデバイスなどのフィールドデバイスで実施される制御モジュールまたはブロックと連携する、異なる制御モジュールを動作させるコントローラアプリケーションを遂行する。コントローラ内の制御モジュールは、通信ラインまたはリンクを介してフィールドデバイスに制御信号を送信し、それによってプロセスプラントまたはシステムの少なくとも一部の動作を制御する。
【０００４】
フィールドデバイス及びコントローラからの情報は、通常、データハイウェイを介して、オペレータワークステーション、パーソナルコンピュータもしくはコンピューティングデバイス、データヒストリアン、レポートジェネレータ、集中型データベース、または典型的にはより厳しいプラント環境から離れた制御室もしくは他の場所に配置される他の集中管理コンピューティングデバイスなどの１つ以上の他のハードウェアデバイスに利用可能になる。これらのハードウェアデバイスの各々は、典型的には、プロセスプラントにわ

たって、またはプロセスプラントの一部にわたって集中管理される。これらのハードウェアデバイスは、例えば、プロセス制御ルーチンの設定を変更すること、コントローラ及びフィールドデバイスプロセス内の制御モジュールの動作を修正すること、プロセスの現在の状態を視認すること、フィールドデバイス及びコントローラによって生成されたアラームを視認すること、人員の訓練またはプロセス制御ソフトウェアの試験の目的でプロセス動作をシミュレートすること、構成データベースを維持及び更新することなど、プロセスの制御及び／またはプロセスプラントの動作に関する機能を、オペレータが遂行することができるアプリケーションを実施することができる。ハードウェアデバイス、コントローラ、及びフィールドデバイスによって利用されるデータハイウェイは、有線通信経路、無線通信経路、または有線及び無線通信経路の組み合わせを含むことができる。

【０００５】

一例として、Ｅｍｅｒｓｏｎ　Ｐｒｏｃｅｓｓ　Ｍａｎａｇｅｍｅｎｔが販売するＤｅｌｔａＶＴＭ制御システムには、プロセスプラント内の多様な場所に位置する異なるデバイスに格納され、実行される複数のアプリケーションが含まれる。１つ以上のワークステーションまたはコンピューティングデバイスに存在する構成アプリケーションによって、ユーザが、プロセス制御モジュールを作成または変更し、これらのプロセス制御モジュールを、データハイウェイを介して専用の分散コントローラにダウンロードすることができる。典型的には、これらの制御モジュールは、そこへの入力に基づいて制御スキーム内の機能を遂行し、制御スキーム内の他の機能ブロックに出力を提供するオブジェクト指向プログラミングプロトコル内のオブジェクトである通信可能に相互接続された機能ブロックで構成される。構成アプリケーションはまた、構成設計者が、視認アプリケーションによってデータをオペレータに表示し、オペレータがプロセス制御ルーチン内の設定点などの設定を変更することができるようにするオペレータインターフェイスを作成または変更することを可能にすることができる。各々の専用コントローラ及び場合によっては１つ以上のフィールドデバイスは、実際のプロセス制御機能を実装するために割り当てられ、ダウンロードされた制御モジュールを実施するそれぞれのコントローラアプリケーションを格納及び実行する。１つ以上のオペレータワークステーション（またはオペレータワークステーション及びデータハイウェイと通信可能に接続された１つ以上の遠隔コンピューティングデバイス）上で実行される視認アプリケーションは、データハイウェイを介してコントローラアプリケーションからデータを受信し、ユーザインターフェースを使用してプロセス制御システムの設計者、オペレータ、またはユーザにこのデータを表示することができ、オペレータの視点、技術者の視点、技能者の視点など、多数の異なる視点のいずれかを提供することができる。データヒストリアンアプリケーションは、典型的には、データハイウェイにわたって提供されるデータの一部または全部を収集して保存するデータヒストリアンデバイスに格納されて実行され、一方、構成データアプリケーションを、データハイウェイに接続されたさらに別のコンピュータ内で実施し、現在のプロセス制御ルーチン構成及びそれに関連するデータを格納することができる。代替的に、構成データベースを構成アプリケーションと同一のワークステーションに位置させることもできる。

【０００６】

一般的には、プロセスプラントのプロセス制御システムは、フィールドデバイス、コントローラ、ワークステーション、ならびに階層化ネットワーク及びバスのセットによって相互接続される他のデバイスを含む。プロセス制御システムは、例えば、製造及び運用コストを低減し、生産性及び効率を高め、プロセス制御及び／またはプロセスプラント情報などへのタイムリーなアクセスを提供するために、様々な事業体及び外部ネットワークと接続されてもよい。一方、プロセスプラント及び／またはプロセス制御システムを、企業及び／または外部のネットワーク及びシステムに相互接続することにより、企業及び／または外部ネットワークで使用されるもののような、商用システム及びアプリケーションにおいて予想される脆弱性から生じ得る、サイバー侵入及び／または悪意のあるサイバー攻撃のリスクが高まる。プロセスプラント、ネットワーク、ならびに／または制御システムのサイバー侵入及び悪意のあるサイバー攻撃は、一般的に言えば、汎用コンピューティン

グネットワークの脆弱性と同様の脆弱性である情報資産の機密性、完全性、及び／または可用性に悪影響を与える可能性がある。しかしながら、汎用コンピュータネットワークとは異なり、プロセスプラント、ネットワーク、及び／または制御システムのサイバー侵入は、プラント設備、製品、及び他の物理的資産の損傷、破壊、及び／または損失だけでなく、人命の喪失をもたらす可能性がある。例えば、サイバー侵入によってプロセスが制御不能になり、爆発、火災、洪水、危険物への曝露などが生成する可能性がある。したがって、プロセス制御プラント及びシステムに関連する通信を、セキュリティ保護することが特に重要である。

【０００７】

図１は、プロセス制御または工業プロセスシステムのセキュリティの例示的なレベルのブロックダイヤグラム１０を含む。ダイヤグラム１０は、プロセス制御システムの様々な構成要素、プロセス制御システムそれ自体、及びプロセス制御システムが、通信可能に接続することができる他のシステム及び／またはネットワーク間の相互接続、ならびに、プロセス制御システムと他のシステム／ネットワークの内部及び間の通信に対するセキュリティの階層またはレベルを示す。セキュリティレベルは、セグメント化または分離によるセキュリティへの階層的なアプローチを提供し、様々なレベルは、１つ以上のファイアウォール１２Ａ、１２Ｂ、１２Ｃによって保護され、異なるレベル間で許可されたトラフィックのみを許可する。図１では、低い番号のセキュリティレベルは、制御されているオンラインプロセスに近く、高い番号のセキュリティレベルは実行プロセスからより多く削除されている。したがって、信頼レベル（メッセージ、パケット、及び他の通信の安全性と妥当性の信頼度など）は、デバイスレベル（レベル０）で最も高く、信頼レベルは、事業体ネットワークレベル上、例えば、公衆インターネット及び／または他の公衆ネットワーク上で最も低レベル（レベル５）にある。ＩＳＡ（国際自動学会（Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｓｏｃｉｅｔｙ ｏｆ Ａｕｔｏｍａｔｉｏｎ））９５．０１－ＩＥＣ（国際電気標準会議（Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｅｌｅｃｔｒｏｔｅｃｈｎｉｃａｌ Ｃｏｍｍｉｓｓｉｏｎ））６２２６４－１で標準化されている制御階層（Ｐｕｒｄｕｅ Ｍｏｄｅｌ ｆｏｒ Ｃｏｎｔｒｏｌ Ｈｉｅｒａｒｃｈｙ）論理フレームワークのパーデュ（Ｐｕｒｄｕｅ）モデルを使用すると、プロセス制御システムは一般にセキュリティレベル０～２に分類され、製造、会社、及び企業システムは、一般にセキュリティレベル３～５に分類される。

【０００８】

異なるセキュリティレベルの各々における異なる機能性の例を、図１に示す。典型的には、レベル０には、プロセスプラント内に配設され、プロセス及び／またはプロセスフローと直接接触するフィールドデバイス及び他のデバイス、例えば、センサ、バルブ、バルブ位置決め器、スイッチ、トランスミッタ、及びバルブの開閉、圧力、温度などのプロセスパラメータの測定などの物理的及び／またはプロセス制御機能を遂行する他のデバイスを含む。例示を明確にするために、例示的なフィールドデバイスは、図１には示されていない。

【０００９】

レベル１は、例えば、フィールドデバイスからの入力を受信し、制御スキーム、モジュール、または他の論理を使用して入力を処理し、結果出力を他のデバイスに送信することによって、プロセスのリアルタイム動作の基本制御を提供するコントローラ及び他のプロセス制御デバイス１５Ａ～１５Ｄを含む。一般に、このようなプロセス制御デバイスは、それぞれの制御方式でプログラムされ、及び／または構成されている。例えば、レベル１のプロセス制御デバイスは、プロセスコントローラ、プログラマブルロジックコントローラ（ＰＬＣ）、遠隔ターミナルユニット（ＲＴＵ）などを含むことができる。図１に示すように、レベル１のプロセス制御デバイスは、バッチ制御１５Ａ、個別制御１５Ｂ、連続制御１５Ｃ、ハイブリッド制御１５Ｄ、及び／または他のタイプの制御を遂行するものを含むことができる。

【００１０】

レベル２は、プロセスプラントの生産領域監視制御を提供するデバイス及び設備１８Ａ～１８Ｄを含む。例えば、レベル２は、警告及び／または警報システム１８Ａ、オペレータワークステーション１８Ｃ、他のヒューマンマシンインターフェース（ＨＭＩ）１８Ｂ、１８Ｄなどを含むことができる。一般に、レベル２のデバイス及び設備は、レベル１のデバイス１５Ａ～１５Ｄならびにレベル３のデバイス及び設備と、例えば１つ以上のファイアウォール１２Ａ、１２Ｂを介して通信することができる。

【００１１】

レベル３は、プラントシステム及び／またはネットワーク、例えば、デバイス、設備及びサイト／プラントを管理し、所望の最終製品を生産または製造するための制御を管理するシステム２０Ａ～２０Ｄを収容する。例えば、レベル３は、生産管理、報告、スケジューリング等に使用される生産システム２０Ａ、品質、生産性、効率などを改善するために使用される最適化システム２０Ｂ、プロセスプラントによって生成された、及び／もしくは示すデータを履歴化するためのヒストリアン２０Ｃ、ならびに／または制御スキーム及びモジュール、オペレータワークステーション、及び／もしくはＨＭＩインターフェースなどの設計及び開発のために要員が使用するエンジニアリングワークステーションもしくはコンピューティングデバイス２０Ｄを含むことができる。

【００１２】

レベル５にスキップすると、レベル５には一般的に、事業体、会社、または企業のシステム及び／またはネットワークが収納される。典型的には、そのようなシステム及び／またはネットワークは、企業外のシステムとのインターフェースを管理する。例えば、企業のＶＰＮ（仮想プライベートネットワーク）、会社もしくは企業インターネットアクセスサービス、ならびに／または他のＩＴ（情報技術）インフラストラクチャシステム及びアプリケーションは、レベル５にある。

【００１３】

レベル５の内部拡張と見なすことができるレベル４は、一般的に企業の内部にある会社または企業システム、例えば、電子メール、イントラネット、サイトの事業計画とロジスティクス、在庫管理、スケジューリングをサポートする会社システム及び／または他の会社／企業システム及びネットワークを収納する。

【００１４】

図１に示すように、セキュリティレベル３及び４は、事業体もしくは企業システム及び／またはネットワークを、プラント／プロセスシステム及び／またはネットワークから分離する非武装地帯（ＤＭＺ）２２を介して相互にインターフェースし、それによってプロセスプラントが曝されるセキュリティリスクを最小にする。ＤＭＺ２２は、１つ以上のそれぞれのファイアウォール１２Ｃを含み、より低いセキュリティレベルでプラント関連デバイス、機器、及び／もしくはアプリケーションと通信し、ならびに／または企業関連デバイス、機器、アプリケーションと高度なセキュリティレベルで通信する、様々なデバイス、機器、サーバ、及び／またはアプリケーション２５Ａ～２５Ｆを収容してもよい。例えば、ＤＭＺ２２は、２、３の例を挙げると、ターミナルサービス２５Ａ、パッチ管理２５Ｂ、１つ以上のＡＶサーバ２５Ｃ、１つ以上のヒストリアン２５Ｄ（例えばミラーヒストリアンを含み得る）、Ｗｅｂサービスオペレーション２５Ｅ、及び／または１つ以上のアプリケーションサーバ２５Ｆを含む。典型的には、ＤＭＺ２２の上のセキュリティレベルのデバイス、機器、及び／またはアプリケーションについては、許可されたものだけがプロセスプラントに通信可能にアクセスすることが許可され、さらにデバイス、機器、サーバ及び／またはＤＭＺ２２のアプリケーション２５Ａ～２５Ｆを介して接続されることが要求される。ＤＭＺデバイス２５Ａ～２５Ｆは、下位レベルへの別個の接続を維持し、それにより、プロセスプラント及び制御システムを、企業（及び上位）システム及び／またはネットワークからの攻撃から保護する。

【００１５】

遠隔サービスの簡単な議論に移ると、遠隔サービスは、異なるユーザ及びシステムによって、ますます一般的に使用されるようになってきている。例えば、Ｍｉｃｒｏｓｏｆｔ

Ｗｉｎｄｏｗｓ（登録商標）オペレーティングシステムによって提供される遠隔デスクトップサービス製品を使用すると、ユーザは、会社ネットワーク及び／またはインターネットから、データセンター内のセッションベースのデスクトップ、仮想マシンベースのデスクトップ、及び／または他のアプリケーションにアクセスすることが可能になる。Ｉｎｔｕｉｔ（登録商標）が提供するＱｕｉｃｋＢｏｏｋｓ（登録商標）Ｏｎｌｉｎｅ製品は、ユーザがキャッシュフロー管理、請求書発行、インターネットを介してのオンライン支払いなどの会計機能を遂行することを可能にする。一般的に言えば、遠隔サービスは、遠隔サービスにアクセスするシステムまたはユーザから遠隔操作で実行する１つ以上のアプリケーションによって提供される。例えば、１つ以上のアプリケーションは、サーバの遠隔バンク、クラウドなどでデータを実行及び管理し、企業ネットワーク及び／または公衆インターネットのような１つ以上のプライベート及び／または公衆ネットワークを介してアクセスされる。

【発明の概要】

【００１６】

一実施形態では、プロセスプラントから別のシステムへ通信を安全に転送する方法は、フィールドゲートウェイにおいて、プロセスプラントのネットワークと、フィールドゲートウェイとエッジゲートウェイと、の間の双方向通信を防止するように構成されたデータダイオードとを相互接続することと、データダイオードを経由してエッジゲートウェイに対して、プロセス制御プラントの１つ以上のデバイスの各々を記述するそれぞれのコンテキスト情報を反復的に告知することと、プロセスプラントがプロセスを制御するように動作している間に、１つ以上のデバイスの各々によって生成されたデータを、プロセスプラントネットワークを介してフィールドゲートウェイで受信することと、フィールドゲートウェイによって、データダイオードを経由してエッジゲートウェイにプロセスプラントデータをパブリッシュすることと、を含む。

【００１７】

一実施形態では、プロセスプラントから別のシステムへ通信を安全に転送するシステムは、プロセスプラントのネットワークに通信可能に結合されたフィールドゲートウェイと、他のシステムに通信可能に結合されたエッジゲートウェイと、フィールドゲートウェイとエッジゲートウェイとを相互接続するデータダイオードと、を含む。データダイオードは、エッジゲートウェイによって送信された通信がフィールドゲートウェイに進入することを防止するように構成され、プロセスプラントが工業プロセスを制御するように動作している間に、プロセスプラントに含まれる１つ以上のデバイスによって生成されたデータが、プロセスプラントネットワークを介してゲートウェイ受信され、フィールドゲートウェイによって、データダイオードを経由してエッジゲートウェイにパブリッシュされる。

【図面の簡単な説明】

【００１８】

【図１】特に、プロセス制御システムの様々な例示的構成要素と、プロセス制御システム自体と、他の例示的なシステム及び／またはネットワークとの間の相互接続を含む、プロセス制御または工業プロセスシステムのセキュリティの例示的なレベルのブロック図を含む。

【図２】プロセス制御システムの様々な例示的構成要素と、プロセス制御システム自体と、他の例示的なシステム及び／またはネットワークとの間の相互接続を特に示すプロセスプラントまたはプロセス制御システムの例のブロック図である。

【図３】プロセスプラントまたはプロセス制御システムのための例示的なセキュリティアーキテクチャのブロック図である。

【図４】プロセスプラントまたはプロセス制御システムの安全な通信をプロビジョニングするために使用されるメッセージフローの例を示す。

【図５】データダイオードを経由してプロセスプラントデータを配信するために使用され得るメッセージフローの例を示す。

【図６】プロセスプラントまたはプロセス制御システムから通信を安全に転送するための

例示的な方法のフロー図である。
【図７】プロセスプラントまたはプロセス制御システムから通信を安全に輸送するための例示的な方法のフロー図である。
【発明を実施するための形態】
【００１９】
上述したように、サイバー侵入及び悪意のあるサイバー攻撃に対してプロセス制御プラント及びシステムを安全にすることは、典型的にファイアウォール及び他のセキュリティメカニズムを使用して安全にされた層またはレベルの少なくとも一部によって、層状またはレベル化されたセキュリティ階層を利用する。例えば、図１に関して上記に説明したように、セキュリティレベル０～３のプロセスプラントシステム、ネットワーク、及びデバイスは、セキュリティレベル４～５の企業ネットワークから、及び／または企業ネットワークを利用するレベル５より高い任意の外部ネットワークからの脅威から、例えば、ＤＭＺ２２及び１つ以上のファイアウォール１２Ａ～１２Ｃを使用することによって、保護され得る。しかしながら、プロセスプラントデータ上で動作するより多くのサービス及びアプリケーションが、（例えば、企業またはビジネス内のレベル４及び／または５の）例えば、プロセスプラントの外部ネットワーク及びシステム上で、ならびに／または企業もしくは事業体の外部にあるネットワーク及びシステム（例えば、レベル５以上、インターネットもしくは他の公衆ネットワークを介して）上であっても、遠隔操作で実行するために移動されるとき、プロセスプラントシステム、ネットワーク、及びデバイスが危険に曝されるのを防ぐためのより強力な技術が必要である。
【００２０】
本明細書で説明される新たなシステム、構成要素、装置、方法、及び技術は、プロセスプラント及びそのネットワークに関連するこれら及び他のセキュリティ問題に対処し、特に、プロセスプラント／ネットワークと他のネットワークまたはシステムとの間の通信をセキュリティ保護することに関する。
【００２１】
説明するために、図２は、オンライン動作中の工業プロセスを制御するように構成され、本明細書に記載された新たなセキュリティ技術のうちの任意の１つ以上を利用してセキュリティ保護され得る例示的なプロセスプラント１００のブロック図である。プロセスプラント１００（本明細書では、同義的に、プロセス制御システム１００またはプロセス制御環境１００とも称される）は、フィールドデバイスによって行われたプロセス測定値を示す信号を受信し、この情報を処理して制御ルーチンを実装し、有線または無線のプロセス制御通信リンクまたはネットワークを介して他のフィールドデバイスに送信される制御信号を生成して、プラント１００内のプロセスの動作を制御する１つ以上のプロセスコントローラを含む。典型的には、少なくとも１つのフィールドデバイスが、プロセスの動作を制御する物理的機能（例えば、バルブの開閉、温度の上昇または低下、測定の取得、状況の検出など）を遂行する。一部のタイプのフィールドデバイスは、Ｉ／Ｏデバイスを使用してコントローラと通信する。プロセスコントローラ、フィールドデバイス、及びＩ／Ｏデバイスは、有線または無線であってもよく、任意の数及び組み合わせの有線及び無線プロセスコントローラ、フィールドデバイス、及びＩ／Ｏデバイスが、プロセスプラント環境またはシステム１００に含まれてもよい。
【００２２】
例えば、図２は、入出力（Ｉ／Ｏ）カード１２６及び１２８を介して有線フィールドデバイス１１５～１２２に通信可能に接続され、無線ゲートウェイ１３５及びプロセス制御データハイウェイまたはバックボーン１１０を介して無線フィールドデバイス１４０～１４６に通信可能に接続されているプロセスコントローラ１１１を示す。プロセス制御データハイウェイ１１０は、１つ以上の有線及び／または無線通信リンクを含むことができ、例えば、イーサネットプロトコルのような任意の所望のまたは好適なまたは通信のプロトコルを使用して実装することができる。いくつかの構成（図示せず）では、コントローラ１１１は、バックボーン１１０以外の１つ以上の通信ネットワークを使用して、例えば、

Ｗｉ－Ｆｉまたは他のＩＥＥＥ８０２．１１準拠の無線ローカルエリアネットワークプロトコル、移動通信プロトコル（例えば、ＷｉＭＡＸ、ＬＴＥ、または他のＩＴＵ－Ｒ互換プロトコル）、Ｂｌｕｅｔｏｏｔｈ（登録商標）、ＨＡＲＴ（登録商標）、ＷｉｒｅｌｅｓｓＨＡＲＴ（登録商標）、Ｐｒｏｆｉｂｕｓ、ＦＯＵＮＤＡＴＩＯＮ（登録商標）Ｆｉｅｌｄｂｕｓなどをサポートする任意の数の他の有線または無線通信リンクを使用して、無線ゲートウェイ１３５に通信可能に接続されてもよい。

【００２３】

例えば、Ｅｍｅｒｓｏｎ　Ｐｒｏｃｅｓｓ　Ｍａｎａｇｅｍｅｎｔによって販売されているＤｅｌｔａＶＴＭコントローラであってもよいコントローラ１１１は、フィールドデバイス１１５～１２２及び１４０～１４６の少なくとも一部を使用してバッチプロセスまたは連続プロセスを実装するように動作することができる。一実施形態では、コントローラ１１１は、プロセス制御データハイウェイ１１０に通信可能に接続されることに加えて、フィールドデバイス１１５～１２２及び１４０～１４６のうちの少なくともいくつかに、４～２０ｍＡデバイス、Ｉ／Ｏカード１２６、１２８、及び／またはＦＯＵＮＤＡＴＩＯＮ（登録商標）Ｆｉｅｌｄｂｕｓプロトコル、ＨＡＲＴ（登録商標）プロトコル、ＷｉｒｅｌｅｓｓＨＡＲＴ（登録商標）プロトコルなどの任意のスマート通信プロトコルに関連する任意の所望のハードウェア及びソフトウェアを使用して通信可能に接続される。図２では、コントローラ１１１、フィールドデバイス１１５～１２２及びＩ／Ｏカード１２６、１２８は、有線デバイスであり、フィールドデバイス１４０～１４６は、無線フィールドデバイスである。当然のことながら、有線フィールドデバイス１１５～１２２及び無線フィールドデバイス１４０～１４６は、将来開発される任意の標準またはプロトコルを含む任意の有線または無線プロトコルのような任意の他の所望の標準またはプロトコルに準拠することができる。

【００２４】

図２のプロセスコントローラ１１１は、（例えば、メモリ１３２に格納された）１つ以上のプロセス制御ルーチン１３８を実装または監督するプロセッサ１３０を含む。プロセッサ１３０は、フィールドデバイス１１５～１２２及び１４０～１４６及びコントローラ１１１に通信可能に接続された他のノードと通信するように構成されている。本明細書に記載された任意の制御ルーチンまたはモジュールは、そのように所望される場合、異なるコントローラまたは他のデバイスによってその一部が実装または実行されてもよい。同様に、プロセス制御システム１００内で実装される本明細書に記載の制御ルーチンまたはモジュール１３８は、ソフトウェア、ファームウェア、ハードウェアなどを含む任意の形態を採ることができる。制御ルーチンは、オブジェクトラダーロジック、シーケンシャルファンクションチャート、ファンクションブロックダイアグラム、または他の任意のソフトウェアプログラミング言語もしくは設計パラダイムを使用して実装することができる。制御ルーチン１３８は、ランダムアクセスメモリ（ＲＡＭ）または読み出し専用メモリ（ＲＯＭ）のような任意の所望のタイプのメモリ１３２に格納することができる。同様に、制御ルーチン１３８は、例えば、１つ以上のＥＰＲＯＭ、ＥＥＰＲＯＭ、特定用途向け集積回路（ＡＳＩＣ）、または他の任意のハードウェアもしくはファームウェア要素にハードコード化されてもよい。したがって、コントローラ１１１は、任意の所望の方法で制御ストラテジまたは制御ルーチンを実装するように構成することができる。

【００２５】

コントローラ１１１は、一般的に機能ブロックと称されるものを使用して制御ストラテジを実装し、各々の機能ブロックは全体制御ルーチンのオブジェクトまたは他の部分（例えばサブルーチン）であり、他の機能ブロックと共に（リンクと称される通信を介して）動作して、プロセス制御システム１００内のプロセス制御ループを実装する。制御ベースの機能ブロックは、典型的には、送信機、センサまたは他のプロセスパラメータ測定デバイスに関連する入力機能の１つ、ＰＩＤ、ファジィ論理等の制御を遂行する制御ルーチンに関連するもののような制御機能；プロセス制御システム１００内のいくつかの物理的機能を実行するためのバルブなどのデバイスの動作を制御する出力機能の１つを遂行する。

当然のことながら、ハイブリッド及び他のタイプの機能ブロックが存在する。機能ブロックは、典型的には、これらの機能ブロックが標準４～２０ｍＡデバイス及びＨＡＲＴ（登録商標）デバイスのようないくつかのタイプのスマートフィールドデバイスに使用されるか、または関連する場合に、コントローラ１１１に格納され、コントローラ１１１によって実行されてもよく、ＦＯＵＮＤＡＴＩＯＮ（登録商標）フィールドバスデバイスの場合のようにフィールドデバイス自体に格納され、実装されてもよい。コントローラ１１１は、１つ以上の機能ブロックを実行することによって遂行される１つ以上の制御ループを実装することができる、１つ以上の制御ルーチン１３８を含むことができる。

【００２６】

有線フィールドデバイス１１５～１２２は、センサ、バルブ、送信機、位置決め器などのような任意のタイプのデバイスとすることができ、Ｉ／Ｏカード１２６及び１２８は、任意の所望の通信プロトコルまたはコントローラプロトコルに準拠する任意のタイプのＩ／Ｏデバイスであってもよい。図２に示すように、フィールドデバイス１１５～１１８は、アナログラインまたはアナログ及びデジタルの結合ラインを介してＩ／Ｏカード１２６と通信する、標準的な４～２０ｍＡデバイスまたはＨＡＲＴ（登録商標）デバイスであり、フィールドデバイス１１９～１２２は、ＦＯＵＮＤＡＴＩＯＮ（登録商標）フィールドバス通信プロトコルを使用してデジタルバスを介してＩ／Ｏカード１２８と通信するＦＯＵＮＤＡＴＩＯＮ（登録商標）Ｆｉｅｌｄｂｕｓフィールドデバイスなどのスマートデバイスである。しかし、いくつかの実施形態では、少なくとも一部の有線フィールドデバイス１１５、１１６、１１８～１２１及び／または少なくとも一部のＩ／Ｏカード１２６、１２８は、プロセス制御データハイウェイ１１０を使用して及び／または他の適切な制御システムプロトコル（例えば、Ｐｒｏｆｉｂｕｓ、ＤｅｖｉｃｅＮｅｔ、Ｆｏｕｎｄａｔｉｏｎ Ｆｉｅｌｄｂｕｓ、ＣｏｎｔｒｏｌＮｅｔ、Ｍｏｄｂｕｓ、ＨＡＲＴなど）を使用することによって、コントローラ１１１と付加的または代替的に通信する。

【００２７】

図２では、無線フィールド機器１４０～１４６は、ＷｉｒｅｌｅｓｓＨＡＲＴ（登録商標）プロトコルなどの無線プロトコルを使用して、無線プロセス制御通信ネットワーク１７０を介して通信する。そのような無線フィールド機器１４０～１４６は、（例えば、無線プロトコルまたは別の無線プロトコルを使用して）無線通信するようにも構成された無線ネットワーク１７０の１つ以上の他のデバイスまたはノードと直接通信することができる。無線通信するように構成されていない他のノードと通信するために、無線フィールド機器１４０～１４６は、プロセス制御データハイウェイ１１０または別のプロセス制御通信ネットワークに接続された無線ゲートウェイ１３５を利用することができる。無線ゲートウェイ１３５は、無線通信ネットワーク１７０の様々な無線デバイス１４０～１５８へのアクセスを提供する。特に、無線ゲートウェイ１３５は、無線デバイス１４０～１５８、有線デバイス１１５～１２８、及び／またはプロセス制御プラント１００の他のノードまたはデバイス間の通信結合を提供する。例えば、無線ゲートウェイ１３５は、プロセス制御データハイウェイ１１０を使用することによって、及び／またはプロセスプラント１００の１つ以上の他の通信ネットワークを使用することによって、通信結合を提供することができる。

【００２８】

有線フィールドデバイス１１５～１２２と同様に、無線ネットワーク１７０の無線フィールドデバイス１４０～１４６は、プロセスプラント１００内の物理的制御機能、例えば、バルブの開閉、またはプロセスパラメータの測定を遂行する。しかし、無線フィールドデバイス１４０～１４６は、ネットワーク１７０の無線プロトコルを使用して通信するように構成されている。このように、無線ネットワーク１７０の無線フィールドデバイス１４０～１４６、無線ゲートウェイ１３５、及び他の無線ノード１５２～１５８は、無線通信パケットのプロデューサ及びコンシューマである。

【００２９】

プロセスプラント１００のいくつかの構成では、無線ネットワーク１７０は、非無線デ

バイスを含む。例えば、図２では、図２のフィールドデバイス１４８、は従来の４～２０ｍＡデバイスであり、フィールドデバイス１５０は有線ＨＡＲＴ（登録商標）デバイスである。ネットワーク１７０内で通信するために、フィールドデバイス１４８、１５０は、それぞれの無線アダプタ１５２Ａ、１５２Ｂを介して無線通信ネットワーク１７０に接続される。無線アダプタ１５２Ａ、１５２Ｂは、ＷｉｒｅｌｅｓｓＨＡＲＴのような無線プロトコルをサポートし、Ｆｏｕｎｄａｔｉｏｎ（登録商標）Ｆｉｅｌｄｂｕｓ、ＰＲＯＦＩＢＵＳ、ＤｅｖｉｃｅＮｅｔなどの１つ以上の他の通信プロトコルもサポートすることができる。付加的に、いくつかの構成では、無線ネットワーク１７０は、無線ゲートウェイ１３５と有線通信する別個の物理デバイスであってもよいし、一体型デバイスとして無線ゲートウェイ１３５を備えてもよい１つ以上のネットワークアクセスポイント１５５Ａ、１５５Ｂを含む。無線ネットワーク１７０はまた、１つの無線デバイスから無線通信ネットワーク１７０内の別の無線デバイスにパケットを回送するための１つ以上のルータ１５８を含むことができる。図２では、無線デバイス１４０～１４６及び１５２～１５８は、無線通信ネットワーク１７０の無線リンク１６０を介して、及び／またはプロセス制御データハイウェイ１１０を介して、相互に及び無線ゲートウェイ１３５と通信する。

【００３０】

図２では、プロセス制御システム１００は、データハイウェイ１１０に通信可能に接続された１つ以上のオペレータワークステーション１７１を含む。オペレータワークステーション１７１を介して、オペレータは、プロセスプラント１００のランタイムオペレーションを閲覧し、監視し、ならびに、診断、是正、維持、及び／または必要とされる可能性のある他の措置を取ることができる。オペレータワークステーション１７１の少なくとも一部は、プラント１００内またはプラント１００の近くの様々な保護領域、例えばプラント１００のバックエンド環境、に位置させることができ、状況によっては、オペレータワークステーション１７１の少なくともいくつかが遠隔地に位置するが、それにもかかわらずプラント１００と通信可能に接続される。オペレータワークステーション１７１は、有線または無線のコンピューティングデバイスであってもよい。

【００３１】

例示的なプロセス制御システム１００は、構成アプリケーション１７２Ａ及び構成データベース１７２Ｂを含むものとしてさらに示されており、これらの各々はまた、データハイウェイ１１０にも通信可能に接続される。上述したように、構成アプリケーション１７２Ａの様々なインスタンスは、１つ以上のコンピューティングデバイス（図示せず）上で実行して、ユーザが、プロセス制御モジュールを作成または変更し、これらのモジュールをデータハイウェイ１１０を介してコントローラ１１１にダウンロードできるようにするとともに、オペレータがデータを表示し、プロセス制御ルーチン内のデータ設定を変更することができるオペレータインターフェイスを、ユーザが作成または変更することができるようにする。構成データベース１７２Ｂは、作成された（例えば、構成された）モジュール及び／またはオペレータインターフェイスを格納する。一般的に、構成アプリケーション１７２Ａ及び構成データベース１７２Ｂは集中しており、プロセス制御システム１００に対し単一の論理的な外観を有するが、構成アプリケーション１７２Ａの複数のインスタンスは、プロセス制御システム１００内に複数のインスタンスを同時に実行することができ、構成データベース１７２Ｂは、複数の物理的データ格納デバイスを経由して実装される。したがって、構成アプリケーション１７２Ａ、構成データベース１７２Ｂ、及びそれらに対するユーザインターフェイス（図示せず）は、制御及び／または表示モジュール用の構成または開発システム１７２を含む。典型的には、必須ではないが、構成システム１７２のユーザインターフェースは、プラント１００がリアルタイムで動作しているかどうかにかかわらず、構成エンジニア及び開発エンジニアによって利用されるので、オペレータワークステーション１７１は、プロセスプラント１００のリアルタイム動作中にオペレータによって利用されるが（ここでは、同義的に、プロセスプラント１００の「ランタイム」オペレーションと称される）、構成システム１７２のユーザインターフェースは、オペレータワークステーション１７１とは異なる。

【００３２】
例示的なプロセス制御システム１００は、データヒストリアンアプリケーション１７３Ａ及びデータヒストリアンデータベース１７３Ｂを含み、それらの各々はまた、データハイウェイ１１０に通信可能に接続される。データヒストリアンアプリケーション１７３Ａは、データハイウェイ１１０にわたって提供されたデータの一部または全部を収集し、長期格納のためにヒストリアンデータベース１７３Ｂにデータを履歴化または格納するように動作する。構成アプリケーション１７２Ａ及び構成データベース１７２Ｂと同様に、データヒストリアンアプリケーション１７３Ａ及びヒストリアンデータベース１７３Ｂは、集中化され、プロセス制御システム１００に対して単一の論理的外観を有するが、データヒストリアンアプリケーション１７３Ａの複数のインスタンスが、制御システム１００内で同時に実行してもよく、データヒストリアン１７３Ｂは、複数の物理データ格納デバイスにわたって実装されてもよい。
【００３３】
いくつかの構成では、プロセス制御システム１００は、Ｗｉ－Ｆｉまたは他のＩＥＥＥ８０２．１１準拠無線ローカルエリアネットワークプロトコルなどの他の無線プロトコル、ＷｉＭＡＸなどのモバイル通信プロトコル、ＬＴＥ（Ｌｏｎｇ Ｔｅｒｍ Ｅｖｏｌｕｔｉｏｎ）または他のＩＴＵ－Ｒ（Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｔｅｌｅｃｏｍｍｕｎｉｃａｔｉｏｎ Ｕｎｉｏｎ Ｒａｄｉｏｃｏｍｍｕｎｉｃａｔｉｏｎ Ｓｅｃｔｏｒ）互換プロトコル、近距離無線通信（ＮＦＣ）及びＢｌｕｅｔｏｏｔｈなどの短波長無線通信、または他の無線通信プロトコルを使用して他のデバイスと通信する１つ以上の他の無線アクセスポイント１７４を含む。典型的には、そのような無線アクセスポイント１７４は、ハンドヘルドまたは他のポータブルコンピューティングデバイス（例えば、ユーザインターフェースデバイス１７５）が、無線ネットワーク１７０とは異なり、無線ネットワーク１７０とは異なる無線プロトコルをサポートするそれぞれの無線プロセス制御通信ネットワークにわたって通信することを可能にする。例えば、無線またはポータブルユーザインターフェースデバイス１７５は、プロセスプラント１００内のオペレータ（例えば、オペレータワークステーション１７１の１つのインスタンス）によって利用されるモバイルワークステーションまたは診断テスト機器であってもよい。いくつかのシナリオでは、ポータブルコンピューティングデバイスに加えて、１つ以上のプロセス制御デバイス（例えば、コントローラ１１１、フィールドデバイス１１５～１２２、または無線デバイス１３５、１４０～１５８）も、アクセスポイント１７４によってサポートされる無線プロトコルを使用して通信する。
【００３４】
いくつかの構成では、プロセス制御システム１００は、即時プロセス制御システム１００の外部にあるシステムへの１つ以上のゲートウェイ１７６、１７８を含む。典型的には、そのようなシステムは、プロセス制御システム１００によって生成または操作されるカスタマーまたはサプライヤである。情報、例えば、プロセス制御プラント１００は、即時プロセスプラント１００を別のプロセスプラントと通信可能に接続するためのゲートウェイノード１７６を含むことができる。付加的または代替的に、プロセス制御プラント１００は、即時プロセスプラント１００を、実験室システム（例えば、実験室情報管理システムまたはＬＩＭＳ）、オペレータラウンド在庫管理システム、材料ハンドリングシステム、製品在庫管理システム、維持管理システム、生産スケジューリングシステム、気象データシステム、出荷及び処理システム、パッケージングシステム、インターネット、別のプロバイダのプロセス制御システム、または他の外部システムなどの公衆またはプライベートシステムに通信可能に接続することができるゲートウェイノード１７８を含むことができる。
【００３５】
なお、図２は、例示的なプロセスプラント１００に含まれる有限数のフィールドデバイス１１５～１２２及び１４０～１４６、無線ゲートウェイ１３５、無線アダプタ１５２、アクセスポイント１５５、ルータ１５８、及び無線プロセス制御通信ネットワーク１７０

を有する単一のコントローラ１１１のみを示しているが、これは、例示的かつ非限定的な実施形態に過ぎないことに留意されたい。任意の数のコントローラ１１１を、プロセス制御プラントまたはシステム１００に含めることができ、コントローラ１１１のいずれかは、任意の数の有線または無線デバイス及びネットワーク１１５～１２２、１４０～１４６、１３５、１５２、１５５、１５８、１７０と通信してプラント１００内のプロセスを制御することができる。

【００３６】

図３は、図１の例示プロセスプラント１００の例示的なセキュリティアーキテクチャ２００のブロック図を示す。参照として、セキュリティアーキテクチャ２００の様々な部分が含まれ得るセキュリティレベルを示すために、図１の様々なレベルのセキュリティ０～５が、図３の上部を経由して描かれているが、しかしながら、この参照は、図３に示されたものとは異なるセキュリティレベル内にセキュリティアーキテクチャ２００の様々な部分が収納され得るようなガイドラインに過ぎない。

【００３７】

図３に示すように、１つ以上のデバイス２０２は、例えば、図１の無線ゲートウェイ１３５のインスタンスであり得る１つ以上の無線ゲートウェイ２０５Ａ、２０５Ｂに通信可能に接続される。前述したように、無線ゲートウェイ２０５Ａ、２０５Ｂは、セキュリティレベル１及び／またはセキュリティレベル２、例えばプロセスプラント１００自体に位置してもよい。ゲートウェイ２０５Ａ、２０５Ｂとデバイス２０２との間の通信接続は、参照番号２０４Ａ、２０４Ｂで示されている。

【００３８】

デバイス２０２のセットは、プロセスプラント１００のセキュリティレベル０にあるものとして示されており、有限数の無線フィールドデバイスを含むものとして示されている。しかしながら、デバイス２０２に関する本明細書に記載された概念及び特徴は、プロセスプラント１００の任意の数のフィールドデバイスだけでなく、任意のタイプのフィールドデバイスにも容易に適用できることが理解される。例えば、フィールドデバイス２０２は、プロセスプラント１００の１つ以上の有線通信ネットワーク１１０を介して無線ゲートウェイ２０５Ａ、２０５Ｂに通信可能に接続された１つ以上の有線フィールドデバイス１１５～１２２を含むことができ、及び／またはフィールドデバイス２０２は、無線アダプタ１５２Ａ、１５２Ｂに結合され、それによって無線ゲートウェイ２０５Ａ、２０５Ｂに結合された有線フィールドデバイス１４８、１５０を含むことができる。

【００３９】

さらに、デバイス２０２のセットは、プロセスデータを生成するフィールドデバイスだけに限定されず、プロセスプラント１００がオンラインプロセスを制御する結果としてデータを生成するプロセスプラント１００内の任意のデバイスまたは構成要素を付加的または代替的に含み得ることが理解される。例えば、デバイス２０２のセットは、診断データを生成する診断デバイスまたは構成要素、プロセスプラント１００の様々な構成要素及び／またはデバイスの間で情報を送信するネットワークルーティングデバイスまたは構成要素などを含むことができる。実際には、図２に示す構成要素のうちの任意の１つ以上（例えば、構成要素１１１、１１５～１２２、１２６、１２８、１３５、１４０～１４６、１５２、１５５、１５８、１６０、１７０、１７１～１７６、１７８）及び図２には示されていない他の構成要素は、遠隔システム２１０に配信するためのデータを生成するデバイスまたは構成要素２０２であってもよい。このように、デバイス２０２のセットは、本明細書では「データソース２０２」または「データソースデバイス２０２」と同義的に称される。

【００４０】

図３は、プロセスプラント１００に関して利用され得る、及び／またはプロセスプラント１００が利用する遠隔アプリケーションまたはサービス２０８のセットをさらに示す。遠隔アプリケーションまたはサービス２０８のセットは、１つ以上の遠隔システム２１０で実行またはホストされ、遠隔アプリケーション／サービス２０８のセットは、一般的に

セキュリティレベル５以上であると見なされる。アプリケーションまたはサービス２０８の少なくとも一部は、リアルタイムデータがプロセスプラント１００によって生成され、アプリケーションまたはサービス２０８によって受信されると、リアルタイムデータ上でリアルタイムで動作する。他のアプリケーションまたはサービス２０８は、より厳しいタイミング要件を必要とすることなく、プロセスプラント生成データを操作または実行することができる。遠隔システム２１０で実行されるかまたはホストされ、プロセスプラント１００によって生成されるデータのコンシューマであるアプリケーション／サービス２０８の例は、プロセスプラント１００で生成する状況及び／または事象を監視及び／または検出するアプリケーション及びプロセスプラント１００で実行されているオンラインプロセス自体の少なくとも一部を監視するアプリケーションまたはサービスを含む。アプリケーション／サービス２０８の他の例は、プロセスプラント１００によって生成されたデータ上で動作し、場合によっては、プロセスプラント生成データならびに他のプロセスプラントから生成され受信されたデータを分析して収集または発見された知識に基づいて動作し得る記述的及び／または規範的解析を含む。アプリケーション／サービス２０８のさらに別の例は、規範的機能、構成及び／または他のデータの修正、及び／または、例えば、別のサービスまたはアプリケーションの結果として、プロセスプラント１００に再実装されるべき他の規範的変更を実装する１つ以上のルーチンを含む。アプリケーション及びサービス２０８のいくつかの例は、２０１６年９月２３日に出願され、「分散産業性能監視のためのデータ分析サービス（Ｄａｔａ Ａｎａｌｙｔｉｃｓ Ｓｅｒｖｉｃｅｓ ｆｏｒ Ｄｉｓｔｒｉｂｕｔｅｄ Ｉｎｄｕｓｔｒｉａｌ Ｐｅｒｆｏｒｍａｎｃｅ Ｍｏｎｉｔｏｒｉｎｇ）」という名称の米国特許出願第１５／２７４、５１９号、２０１６年９月２３日に出願され、「分散産業性能監視及び分析（Ｄｉｓｔｒｉｂｕｔｅｄ Ｉｎｄｕｓｔｒｉａｌ Ｐｅｒｆｏｒｍａｎｃｅ Ｍｏｎｉｔｏｒｉｎｇ ａｎｄ Ａｎａｌｙｔｉｃｓ）」という名称の米国特許出願第１５／２７４、２３３号、２０１６年１０月２４日に出願され、「プロセスデバイス条件及びパフォーマンス監視（Ｐｒｏｃｅｓｓ Ｄｅｖｉｃｅ Ｃｏｎｄｉｔｉｏｎ ａｎｄ Ｐｅｒｆｏｒｍａｎｃｅ Ｍｏｎｉｔｏｒｉｎｇ）」と題する米国特許出願第１５／３３２、５２１号に記載されており、その全体の開示内容は参照により本明細書に組み込まれる。

【００４１】

１つ以上の遠隔システム２１０は、ネットワークサーバの遠隔バンク、１つ以上のクラウドコンピューティングシステム、１つ以上のネットワークなど、任意の所望の方法で実装することができる。説明を容易にするために、本明細書では、１つ以上の遠隔システム２１０は、該用語が１つのシステム、２つ以上のシステム、または任意の数を指すことがあると理解されるが、単数時制、すなわち「遠隔システム２１０」を使用して参照される。

【００４２】

一般的に言えば、セキュリティアーキテクチャ２００は、デバイス２０２がインストールされ動作するプロセスプラント１００のフィールド環境から、プロセスプラント１００によって生成されたデータ上でコンシュームし、動作するアプリケーション及び／またはサービス２０８を提供する遠隔システム２１０にエンドツーエンドのセキュリティを提供する。このように、デバイス２０２及びプロセスプラント１００の他の構成要素によって生成されたデータは、遠隔アプリケーション／サービス２０８による使用のために遠隔システム２１０に安全に転送されることができ、一方、サイバー攻撃、侵入、及び／または他の悪意のあるイベントからプラント１００を保護する。特に、セキュリティアーキテクチャ２００は、プロセスプラント１００（例えば、プロセスプラント１００の無線ゲートウェイ２０５Ａ、２０５Ｂの間の）と遠隔システム２１０との間に配設されたフィールドゲートウェイ２１２、データダイオード２１５、及びエッジゲートウェイ２１８を含む。典型的には、必須ではないが、フィールドゲートウェイ２１２、データダイオード２１５、及びエッジゲートウェイ２１８は、セキュリティレベル２～５に含まれる。

【００４３】

セキュリティアーキテクチャ２００の重要な態様は、データダイオード２１５である。

データダイオード２１５は、ハードウェア、ファームウェア及び／またはソフトウェアで実装される構成要素であり、特に、プロセスプラント１００と遠隔システム２１０との間の双方向通信を防止するように構成されている。すなわち、データダイオード２１５は、データトラフィックがプロセス制御システム１００から遠隔システム２１０に出ることを可能にし、データトラフィック（例えば、遠隔システム２１０または他のシステムから送信または送られる）がプロセス制御システム１００に侵入することを防止する。

【００４４】

したがって、データダイオード２１５は、フィールドゲートウェイ２１２に通信可能に接続された少なくとも１つの入力ポート２２０と、エッジゲートウェイ２１８に通信可能に接続された少なくとも１つの出力ポート２２２とを含む。データダイオード２１５はまた、その入力ポート２２０をその出力ポート２２２に接続する他の好適な技術の光ファイバまたは通信リンクを含む。データトラフィックがプロセス制御システム１００に流れる（例えば、そこに進入する）のを防ぐために、例示的実装形態では、データダイオード２１５は、エッジゲートウェイ２１８（またはより高いセキュリティレベルの他の構成要素）からデータを受信する入力ポートを除外または省略し、及びまたはフィールドゲートウェイ２１２（またはより低いセキュリティレベルの他の構成要素）にデータを送信するために出力ポートを除外または省略する。付加的または代替的な実装形態では、データダイオード２１５は、データが出力ポート２２２から入力ポート２２０に流れることを可能にする送受信機を除外、省略、及び／または無効にし、及び／または出力ポート２２２から入力ポート２２０にデータが流れるための物理的な通信経路を除外する。さらに付加的または代替的に、データダイオード２１５は、ソフトウェアを介して、例えば、エッジゲートウェイ２１８（またはより高いセキュリティレベルの構成要素）から出力ポート２２２で受信された任意のメッセージをドロップまたはブロックすることによって、及び／またはフィールドゲートウェイ２１２（またはより低いセキュリティレベルの構成要素）宛ての任意のメッセージをドロップまたはブロックすることによって、入力ポート２２０から出力ポート２２２への単方向データフローのみをサポートすることができる。

【００４５】

プロセスプラント１００から出て、データダイオード２１５を経由して入力ポート２２０から出力ポート２２２に送信されたデータは、暗号化によってデータダイオード２１５を経由してさらにセキュリティ保護されてもよい。一例では、フィールドゲートウェイ２１２は、データを暗号化し、暗号化されたデータを入力ポート２２０に配信する。別の例では、データダイオード２１５は、フィールドゲートウェイ２１２からデータトラフィックを受信し、データダイオード２１５は、データを出力ポート２２２に送信する前に、受信したデータトラフィックを暗号化する。データダイオード２１５を経由して暗号化されて送信されるデータトラフィックは、一例ではＵＤＰ（Ｕｓｅｒ　Ｄａｔａｇｒａｍ　Ｐｒｏｔｏｃｏｌ）データトラフィックであり、別の例ではＪＳＯＮデータトラフィックまたは他の汎用通信フォーマットであってもよい。

【００４６】

フィールドゲートウェイ２１２は、データダイオード２１５の下位セキュリティ側をプロセス制御プラント１００に通信可能に接続する。図３に示すように、フィールドゲートウェイ２１２は、プロセスプラント１００のフィールド環境内に配設され、１つ以上のデバイスまたはデータソース２０２に通信可能に接続された無線ゲートウェイ２０５Ａ、２０５Ｂに通信可能に接続される。前述したように、デバイスまたはデータソース２０２及び無線ゲートウェイ２０５Ａ、２０５Ｂは、ＷｉｒｅｌｅｓｓＨＡＲＴ工業プロトコルまたは１つ以上のセキュリティ機構を介して安全な通信を提供するように構成された他の適切な無線プロトコルを使用して通信することができる。例えば、ＷｉｒｅｌｅｓｓＨＡＲＴ工業プロトコルは１２８ビットＡＥＳ暗号化を提供し、それに応じて通信経路２０４Ａ、２０４Ｂを保護することができる。

【００４７】

付加的に、無線ゲートウェイ２０５Ａ、２０５Ｂとフィールドゲートウェイ２１２との

間の通信接続２２５は、通信接続２０４Ａ、２０４Ｂに利用されるのと同じまたは異なるセキュリティ機構を使用してそれぞれセキュリティ保護される。一例では、通信接続２２５は、ＴＬＳ（Ｔｒａｎｓｐｏｒｔ Ｌａｙｅｒ Ｓｅｃｕｒｉｔｙ）ラッパーによってセキュリティ保護される。例えば、無線ゲートウェイ２０５Ａ、２０５Ｂは、ＨＡＲＴ－ＩＰフォーマットのパケットを生成し、フィールドゲートウェイ２１２への転送のためにＴＬＳラッパーによってセキュリティ保護される。

【００４８】

したがって、一実施形態では、前述したように、デバイス２０２によって生成されたデータまたはパケットは、第１のセキュリティ機構を使用して無線ゲートウェイ２０５Ａ、２０５Ｂへの転送２０４Ａ、２０４Ｂのためにセキュリティ保護され、その後、第２のセキュリティ機構を使用して無線ゲートウェイ２０５Ａ、２０５Ｂから、フィールドゲートウェイ２１２への転送２２５のためにセキュリティ保護され、第３のセキュリティ機構を使用してデータダイオード２１５を経由して転送するために引き続きセキュリティ保護され得る。

【００４９】

ここで、データダイオード２１５のより上位セキュリティ側に向けると、データダイオード２１５から出るデータトラフィックは、所望されれば、第４のセキュリティ機構を使用することによって、またはセキュリティ機構のうちの１つを使用することによって、上述したデータダイオード２１５のより下位セキュリティ側で使用されるセキュリティ機構のうちの１つを使用することによって、エッジゲートウェイ２１８への転送のためにセキュリティ保護され得る。付加的に、または代替的に、図３に示すように、エッジゲートウェイ２１８は、図１のファイアウォール１２Ｃまたは別のファイアウォールであってもよいファイアウォール２２８によって保護されてもよい。

【００５０】

エッジゲートウェイ２１８から遠隔システム２１０へのデータ転送は、プライベート企業ネットワーク、インターネット、セルラールータ、バックホールインターネットまたは他のタイプのバックホール接続などの１つ以上の公衆及び／またはプライベートネットワークを使用して配信することができる。注目すべきことに、エッジゲートウェイ２１８から遠隔システム２１０へ転送するデータは、第５のセキュリティ機構を使用することによって、または前述のセキュリティ機構の１つを使用することによってセキュリティ保護される。図３は、遠隔システム２１０に設けられたトークンサービス２３０を介して管理されることができるＳＡＳ（Ｓｈａｒｅｄ Ａｃｃｅｓｓ Ｓｉｇｎａｔｕｒｅ）トークンを介してセキュリティ保護されているとして、エッジゲートウェイ２１８から遠隔システム２１０に配信されるデータトラフィックを示す。エッジゲートウェイ２１８は、トークンサービス２３０を認証し、限られた時間期間、例えば２分、５分、３０分、１時間を超えて有効である可能性のあるＳＡＳトークンを要求する。エッジゲートウェイ２１８は、コンテンツデータがエッジゲートウェイ２１８から遠隔システム２１０に送信される遠隔システム２１０へのＡＭＱＰ（アドバンストメッセージキュープロトコル（Ａｄｖａｎｃｅｄ Ｍｅｓｓａｇｅ Ｑｕｅｕｉｎｇ Ｐｒｏｔｏｃｏｌ））接続をセキュリティ保護し、認証するためにＳＡＳトークンを受信し、使用する。当然のことながら、エッジゲートウェイ２１８と遠隔システム２１０との間のデータ転送をセキュリティ保護するためのＳＡＳトークン及びＡＭＱＰプロトコルの使用は、多くの可能性のあるセキュリティ機構のうちの１つに過ぎない。例えば、Ｘ．５０９証明書、他のタイプのトークン、ＭＱＴＴ（ＭＱ Ｔｅｌｅｍｅｔｒｙ Ｔｒａｎｓｐｏｒｔ）またはＸＭＰＰ（Ｅｘｔｅｎｓｉｂｌｅ Ｍｅｓｓａｇｉｎｇ ａｎｄ Ｐｒｅｓｅｎｃｅ Ｐｒｏｔｏｃｏｌ）などの他のＩＯＴプロトコルなどの任意の１つ以上の好適な、Ｉｎｔｅｒｎｅｔ－Ｏｆ－Ｔｈｉｎｇｓ（ＩＯＴ）セキュリティ機構が、エッジゲートウェイ２１８と遠隔システム２１０との間のデータ転送をセキュリティ保護するために利用することができる。これらの他の実施形態では、サービス２３０は、例えば、適切なセキュリティトークンまたは証明書を提供及び／または発行する。

【００５１】
遠隔システム２１０において、ユーザ認証及び／または許可は、任意の１つ以上の好適な認証及び／または許可セキュリティ機構２３２によって提供される。例えば、遠隔システム２１０への安全なアクセスは、ドメイン認証サービス、ＡＰＩユーザ認証サービス、及び／または任意の他の好適な認証及び／または許可サービス２３２によって提供されてもよい。したがって、認証及び／または許可サービス２３２を介して認証及び／または許可されたユーザ２３５のみが、遠隔システム２１０で利用可能な少なくとも一部のデータ、とりわけ、データデバイス２０２によって生成されたデータを含むデータにアクセスすることができる。
【００５２】
したがって、上述のように、セキュリティアーキテクチャ２００は、プロセスプラント１００内で動作して、例えばその送信を介してデータソース２０２によるデータの開始から遠隔システム２１０へ１つ以上の遠隔アプリケーションまたはサービス２０８によって操作されるプロセスを制御する間に、デバイスまたはデータソース２０２によって生成されたデータに対してエンドツーエンドのセキュリティを提供する。重要なことに、セキュリティアーキテクチャ２００は、このエンドツーエンドのセキュリティを提供し、プロセスプラント１００で悪意のある攻撃が発生するのを防止する。
【００５３】
なお、図３は、デバイスまたはデータソース２０２をフィールドゲートウェイ２１２に通信可能に接続する無線ゲートウェイ２０５Ａ、２０５Ｂを示しているが、いくつかの構成では、無線ゲートウェイ２０５Ａ、２０５Ｂのうちの１つ以上が省略され、ソースデータがデータソース２０２から直接フィールドゲートウェイ２１２に送信されることに留意されたい。例えば、データソース２０２は、プロセスプラント１００のビッグデータネットワークを介してフィールドゲートウェイ２１２にソースデータを直接送信することができる。一般的に、プロセスプラント１００のビッグデータネットワークは、バックボーンプラントネットワーク１１０ではなく、またはビッグデータネットワークは、工業用通信プロトコル（例えば、Ｐｒｏｆｉｂｕｓ、ＤｅｖｉｃｅＮｅｔ、Ｆｏｕｎｄａｔｉｏｎ Ｆｉｅｌｄｂｕｓ、ＣｏｎｔｒｏｌＮｅｔ、Ｍｏｄｂｕｓ、ＨＡＲＴなど）を使用してデバイス間で制御信号を送信するために使用される工業用プロトコルネットワークでもない。むしろ、プロセスプラント１００のビッグデータネットワークは、例えばデータ処理及び解析目的のためにノード間でデータを流すプロセスプラント１００用に実装されたオーバーレイネットワークであってもよい。ビッグデータネットワークのノードは、例えば、データソース２０２、無線ゲートウェイ２０５Ａ、２０５Ｂ、及びフィールドゲートウェイ２１２、ならびに図２に示す、構成要素１１１、１１５～１２２、１２６、１２８の任意の１つ以上、１３５、１４０、１４６、１５２、１５５、１５８、１６０、１７０、１７１～１７６、１７８及び他の構成要素を含むことができる。したがって、プロセスプラントデータネットワークの多くのノードには、典型的には、工業通信プロトコルを利用するプロセスプラントオペレーションのための指定インターフェースと、例えばストリーミングプロトコルを利用するデータ処理／分析オペレーションのための別の指定インターフェースが含まれる。プロセスプラント１００において利用され得るビッグデータネットワークの例は、「プロセス制御システムにおける地域的ビッグデータ（Ｒｅｇｉｏｎａｌ Ｂｉｇ Ｄａｔａ ｉｎ Ｐｒｏｃｅｓｓ Ｃｏｎｔｒｏｌ Ｓｙｓｔｅｍｓ）」と題する、２０１４年１０月６日に出願された、米国特許出願第１４／５０７、１８８号に記載され、参照により本明細書に組み込まれる。
【００５４】
いくつかの実施形態では、図３に関して、有線ゲートウェイ（図示せず）を無線ゲートウェイ２０５Ａ、２０５Ｂのうちの１つの代わりに利用することができることにさらに留意されたい。さらに、フィールドゲートウェイ２１２、データダイオード２１５、及びエッジゲートウェイ２１８は、図３に示すボックス２３６によって示されるように、物理的に同じ場所に位置してもよく、または構成要素２１２、２１５、２１８のうちの１つ以上

は、複数の場所を経由して物理的に位置してもよい。例えば、フィールドゲートウェイ２１２、データダイオード２１５、またはエッジゲートウェイ２１８のうちの１つ以上が、プロセスプラント１００に配設されてもよい。付加的に、または代替的に、フィールドゲートウェイ２１２、データダイオード２１５、またはエッジゲートウェイ２１８のうちの１つ以上が、プロセスプラント１００から遠隔地に配設されてもよい。

【００５５】

プロセスプラント１００は、所望されれば、複数のフィールドゲートウェイ２１２によってサービスされてもよく、任意の数のフィールドゲートウェイ２１２が単一のエッジゲートウェイ２１８によってサービスされてもよい。いくつかの実施形態では、遠隔システム２１０は、所望されれば、複数のエッジゲートウェイ２１８によってサービスされる。

【００５６】

前述したように、データダイオード２１５を経由して転送されるデータトラフィックはセキュリティ保護される。そのようなデータトラフィックは、例えば、シリアル通信またはＵＤＰ通信を使用することによって、データダイオード２１５を経由して通信され得る。しかしながら、双方向通信なしでこのような通信をセキュリティ保護することは困難かつ扱いにくく、一般的にＵＤＰ通信とシリアル通信の両方は、両方に双方向通信（データダイオード２１５を使用することは不可能である）するだけでなく、長いキーシーケンスを記憶し、入力する必要がある。したがって、従来の双方向通信を使用して単方向データダイオード２１５を経由してデータ転送をセキュリティ保護するのではなく、転送されたデータを、エッジゲートウェイ２１８とフィールドゲートウェイ２１２との間で利用されるセキュリティプロビジョニングプロセスを介してセキュリティ保護することができる。セキュリティプロビジョニングプロセスは、エッジゲートウェイ２１８とフィールドゲートウェイ２１２（例えば、対称キーまたは対称マテリアル）、例えば、結合キー、の間で共有化される固有の初期キーまたは機密マテリアルを確立する。結合キーを使用して、エッジゲートウェイ２１８及びフィールドゲートウェイ２１２は、データダイオード２１５を経由して安全にデータトラフィックを転送するために利用されるさらなるキーまたは機密マテリアルを交換するために使用される安全な接続を確立する。

【００５７】

図４は、セキュリティプロビジョニングプロセスに使用され得る例示的なメッセージフロー２５０を示す。図４では、フィールドゲートウェイ２１２及びエッジゲートウェイ２１８は、両方、フィールドゲートウェイ２１２をエッジゲートウェイ２１８にプロビジョニングするためにユーザによって操作されるプロビジョニングサーバまたはコンピューティングデバイス２５２と同様に、プロビジョニングネットワーク（例えば、同じサブネット、図示せず）上に含まれる。プロビジョニングネットワークを介して、一実施形態では、フィールドゲートウェイ２１２及びエッジゲートウェイ２１８は、例えばＴＣＰタイプの通信を使用して、プロビジョニングをセットアップするために相互に一時的に双方向に通信することができる。

【００５８】

例えば、参照番号２５５で、ユーザは、プロビジョニングデバイス２５２を介してエッジゲートウェイ２１８のユーザインターフェース（ＵＩ）にログインし、それに対して認証される。例えば、エッジゲートウェイ２１８のＵＩは、ウェブインターフェース、または他の何らかの好適なＵＩであってもよい。エッジゲートウェイ２１８のプロビジョニングページまたは表示ビューを介して、ユーザは、フィールドゲートウェイ２１２のアドレス（例ではＩＰアドレスであってもよい）を入力し（参照番号２５８）、エッジゲートウェイ２１８にフィールドゲートウェイ２１２のためのホワイトリストエントリーを作成させる（参照番号２６０）。その後、エッジゲートウェイ２１８は、データ移送に使用されるフィールドゲートウェイ２１２の資格情報をプロビジョニングデバイス２５２に要求する（参照番号２６２）。

【００５９】

エッジゲートウェイの要求に応答して、ユーザは、プロビジョニングデバイス２５２を

介して、フィールドゲートウェイ２１２の認可及びセキュリティ情報を提供する（参照番号２６５）。該認可情報及びセキュリティ情報は、典型的には（必ずしもそうではないが）、フィールドゲートウェイ２１２と共有化されるべき初期キーマテリアルを含む。一例では、初期キーマテリアルは、１２８ビット、１９２ビット、または２５６ビットの結合キーを含み、パケット暗号化／復号化のため、及び場合によってはパケットに対して遂行されたＭＩＣ（メッセージ整合性チェック（Ｍｅｓｓａｇｅ Ｉｎｔｅｇｒｉｔｙ Ｃｈｅｃｋ））計算のために、ノンスの一部として使用される３２ビットまたは６４ビットのパケットカウンタを含む。例えば、パケットカウンタの値は、ネットワーク再生攻撃に対する防御を助けるために、各々の送信のノンスで増加、変更、または更新される。いずれにしろ、エッジゲートウェイ２１８は、初期キーマテリアルのローカルコピーを暗号化して格納し、初期キーマテリアルならびにエッジゲートウェイ２１８の１つ以上のアドレス（例えば、ＩＰアドレス及び／またはエッジゲートウェイ２１８のＭＡＣアドレス）をフィールドゲートウェイ２１２に送信する（参照番号２６８）。フィールドゲートウェイ２１２で、フィールドゲートウェイ２１２が初期キーマテリアルのローカルコピーならびにエッジゲートウェイ２１８のアドレスを暗号化して格納し、エッジゲートウェイ２１８への受信を確認する（参照番号２７０）。

【００６０】

その後、フィールドゲートウェイ２１２は、例えばＵＤＰを使用することによって、データダイオード２１５を経由してエッジゲートウェイ２１８との単方向通信を開始する。具体的には、フィールドゲートウェイ２１２は、後続のメッセージの暗号化と整合性チェックに使用される新たにランダムに生成されたネットワークキー及びランダムに生成されたパケットカウンタ（例えば、ノンス及びＭＩＣ計算に使用される）を含む初期メッセージをエッジゲートウェイ２１８に送信する。新しいネットワークキー及びそれぞれのパケットカウンタは、初期キーマテリアル、例えば、結合キー及びそのそれぞれのパケットカウンタを使用して暗号化される（参照番号２７２）。エッジゲートウェイ２１８は、ローカルな場所に格納された初期キーマテリアルを使用して受信した初期メッセージを復号化し、新しいネットワークキー及びパケットカウンタを格納し（参照番号２７５）、パケットカウンタに格納されたネットワークキーを使用して、フィールドゲートウェイ２１２からその後受信したメッセージまたはパケットを復号化する。

【００６１】

図４に示すように、エッジゲートウェイ２１８が、新しいネットワークキーを使用して暗号化され、新しいパケットカウンタ（参照番号２７８、２８０）を含むフィールドゲートウェイ２１２からの第１のメッセージを受信すると、セキュリティ保護されたプロビジョニングプロセスは完了したと見なされ、プロビジョニングデバイス２５２は、メッセージフロー２５０には、もはや含まれなくてもよいことに留意されたい。結果として、一実施形態では、エッジゲートウェイ２１８からフィールドゲートウェイ２１２へ通信するために利用された一時的な通信チャネル（例えば、参照で利用された２６８）が削除されたり、無効にされたり、利用できなくなったりする。しかしながら、フィールドゲートウェイ２１２は、格納されたネットワークキー及びパケットカウンタ（参照番号２８２）を使用して、単方向データダイオード２１５を経由してエッジゲートウェイ２１８にデータを送信し続け、エッジゲートウェイ２１８は、受信したメッセージを、格納されたカウンタ及びパケットカウンタを使用して復号化し続ける（参照番号２８５）。

【００６２】

しかし、いくつかの実施形態では、フィールドゲートウェイ２１２及びエッジゲートウェイ２１８は、プロビジョニングデバイス２５２のネットワークからの切断時に、またはメッセージフロー２５０中の早期に、データダイオード２１５を経由して単方向通信に戻る。例えば、エッジゲートウェイ２１８は、初期の、結合キーマテリアルをフィールドゲートウェイ２１２に送信すると単方向通信に戻り（参照番号２６８）、フィールドゲートウェイ２１２は、初期キーマテリアルの受信の確認を送信すると単方向通信に戻ることができる（参照番号２７０）。

【００６３】
単方向データダイオード２１５を経由するデータ送信の堅牢性及び信頼性のために、フィールドゲートウェイ２１２は、エッジゲートウェイ２１８との新たなまたは更新されたネットワークキー材料を確立するために、別の初期化メッセージ及びそれぞれのランダムパケットカウンタを生成する。例えば、フィールドゲートウェイ２１２は、初期結合キーマテリアルを使用して暗号化され、新たまたは更新されたネットワークキーと、対応する新たなまたは更新されたパケットカウンタを含む別の初期化メッセージを送信する（参照番号２８８）。初期結合キーマテリアルは、フィールドゲートウェイ２１２及びエッジゲートウェイ２１８（例えば、参照番号２６５、２６８、２７０参照）に予め格納され、更新されたネットワークキー及びランダムパケットカウンタは、例えば、フィールドゲートウェイ２１２においてランダムに生成される。

【００６４】
参照番号２９０において、エッジゲートウェイ２１８は、例えば、ホワイトリスト及び／または新しい初期化メッセージが受信されたアドレスをチェックすることによって、受信した初期化メッセージを検証する。エッジゲートウェイ２１８は、受信した新しい初期化メッセージが有効であると判断した場合、エッジゲートウェイ２１８は、ローカルな場所に格納された初期結合キーマテリアルを用いて初期化メッセージを復号化し、フィールドゲートウェイ２１２から受信される将来のメッセージの処理に利用するため新たな／更新されたネットワークキーを保存する。例えば、フィールドゲートウェイ２１２は、新たな／更新されたネットワークキー及びランダムパケットカウンタを使用して暗号化される後続のメッセージを送信し（参照番号２９２、２９５）、エッジゲートウェイ２１８は、格納された新たな／更新されたネットワークキー及びランダムパケットカウンタを使用して、受信したメッセージを復号化する（参照番号２９８、３００）。

【００６５】
フィールドゲートウェイ２１２は、反復的に、周期的に、または所望される際、例えば、ユーザコマンド発生または別のイベントの発生の結果として、更新されたまたは新たなネットワークキー及びそれぞれのランダムパケットカウンタを確立するために、新たなまたは更新された初期化メッセージ（例えば、参照２７５、２８８など）を送信することを繰り返す。フィールドゲートウェイ２１２とエッジゲートウェイ２１８との間の通信はデータダイオード２１５を経由する単方向であるため、フィールドゲートウェイ２１２は、エッジゲートウェイ２１８が実際にフィールドゲートウェイ２１２によって送信されたデータを受信していることを明示的に確認することはない。したがって、フィールドゲートウェイ２１２は、新たな／更新されたネットワークキー及び対応するランダムパケットカウンタを含む新たな／更新された初期化メッセージを反復的に送信することによって、フィールドゲートウェイ２１２とエッジゲートウェイ２１８との間で共有化されるネットワークキーマテリアルを再同期させることができる。この再同期技術により、エッジゲートウェイに障害が発生して交換または再起動されたとき、及び／またはパケットが欠落したときなど、エラーまたは障害状況中の回復が可能になる。ネットワークキーマテリアル再同期化の期間の長さは、アプリケーション依存性であり得、例えば、失われたパケットまたはデータに対するアプリケーション（例えば、アプリケーションまたはサービス２０８のうちの１つ）の許容差によって管理され、構成可能であり得る。

【００６６】
したがって、上述したように、エッジゲートウェイ２１８（参照番号２６８）及びフィールドゲートウェイ２１２（参照番号２７０）に格納されている初期プロビジョニングされた結合キー及びランダムパケットカウンタまたはノンスマテリアルを利用して、初期ランダムネットワークキー及びランダムパケット開始カウンタ（２７５）を提供する初期の初期化メッセージを暗号化／復号化し、後続の通信は、初期化メッセージに含まれるランダムネットワークキー及びパケットカウンタを利用してそこで送信されるデータを暗号化／復号化する。反復的に、周期的に、または、所望されるときに、フィールドゲートウェイ２１２は、初期結合キーマテリアルを使用して暗号化／復号化され、新たな／更新され

たランダムネットワークキー及びランダムパケット開始カウンタを提供する新たなまたは更新された初期化メッセージを生成する（参照２８８）。新たな／更新された初期化メッセージの後に送信される通信は、その中で送信されるデータを暗号化／復号化するための新たな／更新されたランダムネットワークキー及びパケットカウンタの影響を受ける。したがって、エッジゲートウェイ２１８は、新しいネットワークキー情報に移行する際に故障により到着しない可能性のあるパケットをある時間の間に処理することができるように、以前に使用されたネットワークキー情報及び新しいネットワークキー情報を同時に格納することができる。

【００６７】

図４に示すように、メッセージフロー２５０は、プロビジョニングネットワーク及びプロビジョニングデバイス２５２を利用して、フィールドゲートウェイ２１２とエッジゲートウェイ２１８との間の安全なプロビジョニングプロセスを遂行する。しかしながら、これは多くの可能な実施形態のうちの１つに過ぎない。

【００６８】

例えば、別の実施形態では、フィールドゲートウェイ２１２及びエッジゲートウェイ２１８は、プロビジョニングネットワーク上になく、同じネットワーク上にいなくてもよい。この実施形態では、フィールドゲートウェイ２１２及びエッジゲートウェイ２１８を安全にプロビジョニングするために、ユーザはエッジゲートウェイ２１８に直接認証し、セキュリティ情報またはフィールドゲートウェイ２１２を記述するデータを提供する。例えば、ユーザは、エッジゲートウェイ２１８でそのホワイトリストエントリーのためにフィールドゲートウェイ２１２のＩＰアドレスを提供し、ユーザは、例えば、図４の参照２６５によって上で議論したのと同様の方法で、セキュリティ情報または初期キーマテリアルを提供する。セキュリティ情報は暗号化され、フィールドゲートウェイ２１２との通信に使用するためにエッジゲートウェイ２１８に格納される。付加的に、暗号化されたセキュリティ情報は、それぞれ暗号化され得る別々のファイルに保存される。別々のファイルは、例えば、ユーザによって、フィールドゲートウェイ２１２に転送される。ユーザはフィールドゲートウェイ２１２を直接認証し、フィールドゲートウェイ２１２で使用するために別個のファイルを提供する。フィールドゲートウェイ２１２は、別個のファイルを検証し（必要に応じてファイルを復号化する）、その中に格納されているセキュリティ情報（例えば、初期キーマテリアル）を取得し、取得したセキュリティ情報を暗号化し、データダイオード２１５を経由してエッジゲートウェイ２１８との将来の通信に使用するために暗号化されたセキュリティ情報をローカルな場所に格納する。

【００６９】

別の実施形態では、ＵＤＰの代わりに、シリアル通信を使用してデータダイオード２１５を経由してデータが転送される。この実施形態では、セキュリティ保護されたプロビジョニングプロセスは、フィールドゲートウェイ２１２及びエッジゲートウェイ２１８をプロビジョニングするために上述したものと同様であってもよく、ゲートウェイ２１２、２１８は、プロビジョニングネットワーク上に存在しないか、または別個のネットワーク上にある。

【００７０】

いくつかの実装形態では、セキュリティ保護されたＴＣＰ、ＵＤＰ、及び／またはデータダイオード２１５を経由するシリアル通信の下に、データダイオード２１５を経由してプロセスプラントで生成されたデータを送信するために利用される通信プロトコルは、修正ＨＡＲＴ－ＩＰプロトコルであってもよいし、例えばＦｉｅｌｄｂｕｓのような、任意の既知の工業通信プロトコルへの修正であってもよい。

【００７１】

ＨＡＲＴ－ＩＰプロトコルを例示的であるが非限定的な例として使用するために、ＨＡＲＴ－ＩＰプロトコルを活用して、プロセスプラント１００内で動作するデバイス１０２から遠隔システム２１０へのエンドツーエンド通信に対する付加的なセキュリティをさらに提供することができる。特に、ＨＡＲＴ－ＩＰ及びＨＡＲＴに含まれるパブリッシング

メカニズムは、データダイオード２１５を経由して単方向通信をサポートするために独特の方法で活用され、その結果、プロセスプラント１００で生成されたデータが、データダイオード２１５を経由してフィールドゲートウェイ２１２とエッジゲートウェイ２１８との間で送信されるメッセージまたはパケットを介して遠隔アプリケーション２０８に配信され得る（例えば、図４の参照番号２７８、２８２、２９２、２９５によって示されるように）。

【００７２】

修正されたＨＡＲＴ－ＩＰプロトコルパケットは、トークンパッシングデータリンク層フレームフォーマット（Ｔｏｋｅｎ－Ｐａｓｓｉｎｇ Ｄａｔａ－Ｌｉｎｋ Ｌａｙｅｒ Ｆｒａｍｅ Ｆｏｒｍａｔ）であってもよく、及び／または直接／無線パケットフォーマット（Ｄｉｒｅｃｔ／Ｗｉｒｅｌｅｓｓ Ｐａｃｋｅｔ Ｆｏｒｍａｔ）であってもよい。例えば、ＨＡＲＴ－ＩＰヘッダは、セキュリティタイプの指標（例えば、ヘッダのメッセージタイプ（Ｍｅｓｓａｇｅ Ｔｙｐｅ）フィールドの値として）などのセキュリティ情報を含むように修正されてもよく、Ｈａｒｔ－ＩＰセッション初期化メッセージは、初期セキュリティキーマテリアル情報及び／または他のＨＡＲＴメッセージタイプ（例えば、リクエスト（Ｒｅｑｕｅｓｔ）、リスポンス（Ｒｅｓｐｏｎｓｅ）など）は、ネットワークセキュリティキーフィールド及びネットワークセキュリティカウンタフィールドを含むようにされてもよい。

【００７３】

データダイオード２１５を経由する通信をセキュリティ保護するための修正されたＨＡＲＴ－ＩＰプロトコルの使用例を、図５に示す。図５は、１つ以上の送信デバイス４０２によって生成されたプロセスプラントデータを、データダイオード２１５を経由して１つ以上の受信デバイス４０５に配信するために使用され得る例示的なメッセージフロー４００を示す。一般的に言えば、送信デバイス４０２は、最初に受信デバイス４０５にディスカバリ情報を提供して、データダイオード２１５を経由して送信されるコンテンツまたはペイロードデータのコンテキストを設定する。ディスカバリ情報は、受信デバイス４０５が、どのデータ生成構成要素またはデバイスが、データダイオード２１５のプロセスプラント側にあるか、プロセスプラント側構成要素によって生成されるデータのタイプ及び／またはアイデンティティ、生成されたデータが受信デバイス４０５に到着すると予想される速度、様々なデータ生成構成要素またはデバイスの状態などを知ることを可能にする。重要なことに、ディスカバリ情報により、受信デバイス４０５が、データダイオード２１５の単方向性のために行うことができない受信デバイス４０５がデータダイオード２１５のプロセスプラント側の構成要素デバイスを問い合わせるまたは質問することを必要とせずに、受信デバイス４０５がこの知識を得ることができる。

【００７４】

ディスカバリ情報が送信デバイス４０２によって受信デバイス４０５に供給された後、送信デバイス４０２は、例えば、送信デバイス４０２がソースデータを生成するとき、及び／または送信デバイス４０２がプロセスプラント１００内の１つ以上の他の構成要素からソースデータを受信するときに、リアルタイムでディスカバー情報を提供されたコンテキストに従って、変更されたＨＡＲＴ－ＩＰプロトコルを使用して、データダイオード２１５を経由してコンテンツまたはペイロードデータをパブリッシュする。したがって、受信デバイス４０５は、送信デバイス４０２によってパブリッシュされるデータのサブスクライバであってもよい。

【００７５】

付加的に、データダイオード２１５の単方向性のために、送信デバイス４０２は、受信デバイス４０５の状態を識別することができず（例えば、受信デバイス４０５が動作しているか、パワーサイクルされているか、切断されているかなど）、受信デバイス４０５が送信されたデータを受信したかどうかを明示的に判定することはできない。したがって、送信デバイス４０２は、受信デバイス４０５に反復的に（例えば、周期的に、及び／または所望されるときに）、ディスカバリ情報を提供、送信、または告知するので、受信デバ

イス４０５が使用不能になった場合、送信デバイス４０２によって送信されるコンテンツまたはペイロードデータのコンテキストを迅速に（再）理解することができる。ディスカバリ情報を送信する間の時間期間の長さは、失われたパケットまたはデータについてのデータダイオード２１５の受信デバイス側のクライアントアプリケーション（例えば、遠隔アプリケーションまたはサービス２０８のうちの１つ）の許容差に依存し得、かつ構成可能であり得る。ディスカバリ情報はまた、データソース２０２及び／または無線ゲートウェイ２０５がプロセスプラント１００に追加またはプロセスプラント１００から除去される場合など、送信デバイス４０２側の変更が生じたときに送信されてもよい。

【００７６】

送信デバイス４０２は、フィールドゲートウェイ２１２、無線ゲートウェイ２０５、データソースデバイス２０２、及び／またはプロセスプラント１００内で動作する１つ以上の構成要素もしくはデバイスによって生成されたデータを提供する任意の他の構成要素であってもよい。受信デバイス４０５は、エッジゲートウェイ２１８、遠隔システム２１０を含む１つ以上のデバイス、及び／またはソースデータのコンシューマであるクライアントアプリケーション（例えば、遠隔アプリケーションまたはサービス２０８のうちの１つ）であってもよい。しかしながら、図５では、説明を簡単にするために、メッセージフロー４００は、送信デバイス４０２が図３のフィールドゲートウェイ２１２であり、受信デバイス４０５は、図３のエッジゲートウェイ２１８であるかのように説明されるが、これは多数の可能な実施形態のうちの１つに過ぎないことが理解される。

【００７７】

コンテキスト設定フェーズ４０８中、送信デバイス４０２は、データがデータダイオード２１５を経由して送信されるべきプロセスプラント１００の各々のデータソースを記述するそれぞれの情報を送信する。記述データソース情報は、例えば、データソースのアイデンティティ（例えば、一意の識別子、デバイスタグなど）、データのアイデンティティ（例えば、プライマリ変数（ＰＶ）、セカンダリ変数（ＳＶ）、第３変数（ＴＶ）、第４変数（ＱＶ）などの１つ以上のそのダイナミック変数へのマッピング情報を含むことができる）、識別されたデータが到着すると予想される速度の指標（例えば、バースト構成情報）、及び／または、例えばデータソースが通信可能に接続された特定のゲートウェイを示すデータ、データソースの状態、そのゲートウェイの状態などのデータ及び／またはデータソースを記述する他の情報を含む。図５に示すように、一実施形態では、送信デバイス４０２は、コンテキスト設定フェーズ４０８中に、データソースデバイス２０２ごと、無線ゲートウェイ２０５ベースごとに反復する。例えば、送信デバイス４０２は、例えば無線ゲートウェイ２０５Ａ、２０５Ｂのうちの１つであってもよい無線ゲートウェイ０（参照番号４１０）の記述情報を送信する。送信デバイス４０２は、例えば、修正されたＨＡＲＴ－ＩＰコマンド０、２０、または７４を使用することによって、無線ゲートウェイ０の記述情報を送信することができる。続いて、送信デバイス置４０２は、例えば修正されたＨＡＲＴ－ＩＰコマンド０、２０、５０、１０５、及び任意選択で、サブデバイスバーストマッピングのためのコマンド７４及び１０１を使用して、ゲートウェイ０に通信可能に接続されたＮ個のデバイスの各々についてのそれぞれの記述情報を送信する（参照番号４１２）。このシーケンスは、Ｍ個のゲートウェイの各々について繰り返され、コンテキスト設定フェーズ４０８は、ゲートウェイＭ及びそのそれぞれのＮ個のデバイスに関する記述情報が受信デバイス４０５（参照４１５、４１８）に送信された後に終了する。

【００７８】

パブリッシュフェーズ４２０中に、送信デバイス４０２は、コンテキスト設定フェーズ４０８中にコンテキストが設定されたデータソースデバイス２０２のいずれかのデータダイオード２１５を経由してソースデータをパブリッシュする。一例では、送信デバイス４０２は、修正されたＨＡＲＴ－ＩＰコマンド４８または他の好適なＨａｒｔ－ＩＰコマンドを使用することによって、データダイオード２１５を経由してソースデータをパブリッシュする。特定のソースデータは、ソースデータが送信デバイス４０２で、例えばデバイス２０２からそのそれぞれの無線ゲートウェイ２０５を介して受信される速度でパブリッ

シュされる。すなわち、プロセスプラント１００のオンライン動作中、プロセスプラント１００によって生成されたソースデータは、送信デバイス４０２によって受信されるとリアルタイムでデータダイオード２１５を経由してパブリッシュされる。プロセスプラント１００のいくつかのデータ生成構成要素（例えば、データソースデバイス２０２のいくつか及び／または無線ゲートウェイ２０５の一部）は、データダイオード２１５を経由する配信のためにフィールドゲートウェイ２１２に直接データをパブリッシュしてもよいことに留意されたい。プロセスプラント１００の他のデータ生成構成要素（例えば、データソースデバイス２０２及び／または無線ゲートウェイ２０５の他のもの）は、パブリッシュをサポートしていなくてもよく、フィールドゲートウェイ２１２は、これらのタイプのデバイス／ゲートウェイをポーリングして、これらのそれぞれのソースデータを受信してもよい。例えば、フィールドゲートウェイ２１２は、例えばＨＡＲＴ－ＩＰコマンド３または９を使用することによって、パブリッシュをサポートしないデバイス／ゲートウェイのバースト構成に基づいてポーリングすることができる。

【００７９】

前述したように、所定の時間が経過した後、または所望されるときに、コンテキスト情報４１０～４１８の少なくとも一部が、送信デバイス４０２によって受信デバイス４０５に再送信または更新される。一実施形態では、ゲートウェイ０～Ｍ及びそれぞれのデバイス１～Ｎのコンテキストデータ４１０～４１８の全体が再送信または更新される。別の実施形態では、特定のデバイスに対する特定のコンテキストデータは、例えば、失われたデータまたはパケットに対する特定のコンシューマの許容差に基づいて、データの特定のコンシューマに必要とされる様々な異なる時間に再送信または更新される。これらの実施形態では、異なるデバイスは、これらのそれぞれのコンテキストデータが再送信または更新される異なる周期性または間隔を有することができる。

【００８０】

付加的に、上記のメッセージフロー４００は、データダイオード２１５がイーサネット接続されたデータダイオードである実施形態で説明されていることに留意されたい。しかしながら、所望されれば、直列接続されたデータダイオードにも同様の技術を容易に適用することができる。さらに、上記のメッセージフロー４００は、ＨＡＲＴ－ＩＰプロトコルを使用して説明されたが、メッセージフロー４００のコンテキストフェーズ４０８及びデータ配信フェーズ４２０中において、他の通信プロトコルを利用することもできる。いくつかの構成例では、ＨＡＲＴ－ＩＰ以外の工業通信プロトコル（例えば、Ｐｒｏｆｉｂｕｓ、ＤｅｖｉｃｅＮｅｔ、Ｆｏｕｎｄａｔｉｏｎ Ｆｉｅｌｄｂｕｓ、ＣｏｎｔｒｏｌＮｅｔ、Ｍｏｄｂｕｓ、ＨＡＲＴなど）を利用することができる。他の例示的な構成では、工業通信用に特に設計されていない他のプロトコルが、メッセージフロー４００のコンテキストフェーズ４０８及びデータ配信フェーズ４２０中に利用されてもよい。

【００８１】

例えば、一実施形態では、ＨＡＲＴ－ＩＰを使用する代わりに、ＪＳＯＮ（ＪａｖａＳｃｒｉｐｔ Ｏｂｊｅｃｔ Ｎｏｔａｔｉｏｎ）フォーマットを使用してデータダイオード２１５を経由してパケットを送信することができる。この実施形態では、フィールドゲートウェイ２１２は、プロセスプラント１００内の様々なデバイス及び構成要素から受信したデータを、データダイオード２１５を経由して配信するためのＪＳＯＮフォーマットに変換する。所望されれば、追加の意味を持つラベル（例えば、「ＰＶ」ではなく「ＰＲＥＳＳＵＲＥ」、様々なデータ値に対するデバイス固有のラベルなど）を提供するなど、ＪＳＯＮパケットデータの拡張を追加できる。

【００８２】

さらに、上記の図５の説明は、送信ゲートウェイ４０２がフィールドゲートウェイ２１２であり、受信デバイス４０５がエッジゲートウェイ２１８であるかのように生成するメッセージフロー４００を説明しているが、これは多くの実施形態のうちの１つに過ぎない。例えば、メッセージフロー４００の他の実施形態では、送信デバイス４０２は、フィールドゲートウェイ２１２、無線ゲートウェイ２０５、データソースデバイス２０２、及び

／またはプロセスプラント１００内で動作する１つ以上の構成要素またはデバイスによって生成されたデータを提供する任意の他の構成要素、及び受信デバイス４０５は、エッジゲートウェイ２１８、遠隔システム２１０を含む１つ以上のデバイス、及び／またはソースデータのコンシューマであるクライアントアプリケーション（例えば、遠隔アプリケーションまたはサービス２０８のうちの１つ）であってもよい。例えば、クライアントアプリケーション２０８の第１のものは、データダイオード２１５を経由してパブリッシュされた特定のデバイス２０２によって生成されたデータにサブスクライブすることができ、クライアントアプリケーション２８の第２のものは、別の特定のデバイス２０２によって生成されたデータにサブスクライブすることができる。この例では、エッジゲートウェイ２１８は、受信データをそれぞれのデータサブスクライバに配信するためのルータとして機能することができる。別の例では、エッジゲートウェイ２１８は、受信した全てのデータをデータダイオード２１５を経由してパブリッシュし、様々なアプリケーション２０８は、エッジゲートウェイ２１８によってパブリッシュされた特定のデータにサブスクライブする。他のパブリッシャ／サブスクライバ関係も可能であり、本明細書で説明するセキュリティ保護された通信技術のいずれか１つ以上によってサポートされてもよい。

【００８３】

さらに、セキュリティ保護された通信技術のうちの任意の１つ以上を、プロセスプラント１００にローカルなシステム及び／またはデバイスに送信されるセキュリティ保護されたデータに容易に適用することができる。例えば、セキュリティアーキテクチャ２００のそれぞれのデータダイオード２１５及び／またはインスタンスを使用して、プロセスプラント１００のＤＭＺ２２を経由して選択された（または全ての）データをパブリッシュし、プロセスプラント１００のセキュリティレベル０～３で生成されたデータＤＭＺ２２を介してレベル４～５の企業システムに、それぞれのデータダイオードを介して安全に配信される。別の例では、それぞれのデータダイオード２１５及び／またはセキュリティアーキテクチャ２００のインスタンスは、プロセスプラント１００に配設された１つ以上のデータソース２０２から選択された（または全ての）データをプロセスプラント１００内またはローカルな場所に配設され、ローカルサービス及びアプリケーションをホストまたは提供する１つ以上のローカルサーバにパブリッシュするために利用することができる。このような構成は、例えば、ローカルなサービス及びアプリケーションが、ダウンロードされるか、または他の方法でオンラインプロセスプラント１００に実装されるローカルな規範的変更を生成する場合に有益であるが、一般的に、規範的機能、構成及び／またはデータの修正、及び／または他の変更を、遠隔地に位置するアプリケーション及びサービス２０８によってプロセスプラント１００に実装することができる。

【００８４】

しかし、アプリケーション／サービス２０８によって決定される任意の規範的変更は、データダイオード２１５が、プロセスプラント１００に関して出力方向において単方向であるため、データダイオード２１５以外の何らかの他の通信機構を介してプロセスプラント１００に一般的に実装されることに留意されたい。例えば、プロセスプラント１００への規範的変更を実施するために、遠隔アプリケーション／サービス２０８は、データダイオード２１５を介する以外の、オペレータワークステーション１７１、構成アプリケーション１７２Ａ、構成データベース１７２Ｂなどのプロセスプラント１００の１つ以上の管理またはバックエンド構成要素への接続を確立することができ、規範的変更はプロセスプラント１００にダウンロードされるか、さもなければ配信される。実際、一実施形態では、データダイオード２１５及び／またはセキュリティアーキテクチャ２００の別のインスタンスを、進入方向に確立して、遠隔アプリケーション／サービス２０８からプロセスプラント１００への規範的変更を安全に配信することができる。

【００８５】

さらに、一般的に言えば、遠隔システム２１０からプロセスプラント１００への進入通信は、典型的には、出力データダイオード２１５及び／または出力セキュリティアーキテクチャ２００以外の通信機構を利用する。例えば、遠隔システム２１０は、進入方向に適

用されたデータダイオード２１５及び／またはセキュリティアーキテクチャ２００の別のインスタンス、または他の何らかの好適なセキュリティ保護された接続または通信経路を利用することができる。

【００８６】

ここで、プロセスプラント１００からのセキュリティ保護された出力通信に戻ると、図６は、図２のプロセスプラント１００などのプロセスプラントから通信を安全に転送するための例示的な方法４５０のフロー図を示す。いくつかの実施形態では、方法４５０の少なくとも一部分は、１つ以上の固定コンピュータ読み取り可能メモリに格納されたコンピュータ実行可能命令またはコンピュータ読み取り可能命令のセットを実行することによって実装され、例えば、システム２００の１つ以上のプロセッサによって実行される。例えば、方法４５０の少なくとも一部分は、フィールドゲートウェイ２１２または送信デバイス４０２のような、図１～５に示されるシステム２００の１つ以上の構成要素によって遂行されてもよい。したがって、方法４５０は、図１～５を同時に参照して以下に説明されるが、しかしながら、これは説明を簡単にするためのものであって、限定目的のものではない。

【００８７】

ブロック４５２において、方法４５０は、プロセスプラントの送信デバイスを受信デバイスでプロビジョニングすることを含む。送信デバイスは、（例えば、１つ以上の好適なネットワークを介して）プロセスプラントに通信可能に接続され、受信デバイスは、例えば、１つ以上の好適なネットワークを介して別のシステムに通信可能に接続される。他のシステムは、実行時、オペレーション中にプロセスプラントによって生成されたデータ、及び任意選択でプロセスプラントによって生成される他のデータ上で動作するように構成された１つ以上のアプリケーションまたはサービスをホストする。送信デバイスは、例えば、送信デバイス４０２であってもよく、受信デバイスは、例えば、図５に示す受信デバイス４０５であってもよい。このように、送信デバイス４０２は、フィールドゲートウェイ２１２、データソースデバイス２０２、無線ゲートウェイ２０５、またはプロセスプラント１００の別の構成要素であってもよく、受信デバイスは、エッジゲートウェイ２１８、遠隔システム２１０、または遠隔システム２１０に含まれるコンピューティングデバイス、または遠隔システム２１０で実行されるアプリケーションまたはサービス２０８であってもよい。当然のことながら、送信デバイス及び／または受信デバイスの他の実施形態、例えば上述したもののいずれかが可能である。

【００８８】

送信デバイス及び受信デバイスは、図３のデータダイオード２１５などのデータダイオードを介して相互接続される。データダイオードは、送信デバイスから受信デバイスに単方向通信を送信できるように構成され、受信デバイスから送信デバイスに通信が送信されないように構成されている（一実施形態では、初期プロビジョニングメッセージの他に）。

【００８９】

受信デバイスへの送信デバイスのプロビジョニング（ブロック４５２）は、結合キーとも称される第１のキーを使用して遂行される。結合キーは、機密キーまたは共有化機密であってもよく、例えば、送信デバイス及び／または受信デバイスに通信可能に接続されたプロビジョニングデバイスを介して、または手動データ転送を介して、ユーザによって提供されてもよい。いくつかの構成では、第１のパケットカウンタ（結合パケットカウンタとも称される）または他のそれぞれのノンスマテリアルが、結合キーと共に提供される。結合キー及び／または結合パケットカウンタは、所望されれば、ランダムに生成されてもよい。

【００９０】

いくつかの実施形態では、送信デバイスをプロビジョニングすること（ブロック４５２）は、受信デバイスから送信デバイスへの通信が結合キーを送信及び／または検証できるように一時的通信チャネルを確立することを含む。一時的通信チャネルは、データダイオードを介して確立されてもよいし、外部有線または無線接続、可搬型格納デバイスを介す

る手動転送などの他の何らかの通信接続を介して確立されてもよい。これらの実施形態では、受信デバイスによる結合キーの送信及び／または送信デバイスでの結合キーの受信時に、一時的通信チャネルは、失効、削除、または無効化される可能性がある。一般的に言えば、一時的通信チャネルは、送信デバイスと受信デバイスとの間で第１または結合キーを共有化する役割しか果たしない。初期キーマテリアル（例えば、結合キー及びそのそれぞれのパケットカウンタまたは他のノンスマテリアル）が共有化された後、初期キーマテリアルは、ローカルな場所に暗号化され、送信デバイス及び受信デバイスの両方にそれぞれ格納される。

【００９１】

方法４５０は、例えば、送信デバイスによって、第１または結合キーを使用して初期化メッセージを暗号化すること（ブロック４５５）、及び暗号化された初期化メッセージをデータダイオードを経由して受信デバイスに提供することを含む（ブロック４５８）。初期化メッセージは、データダイオードを経由して送信デバイスから受信デバイスに送信される後続のメッセージまたはパケットを処理するために、送信デバイス及び受信デバイスによって利用される、本明細書ではネットワークキーとも称される第２のキーを内部に含む。第２のキーは、例えば、別の機密キーまたは共有化機密キーであってもよい。第２またはネットワークキーを使用して処理される後続のメッセージまたはパケットの少なくとも一部は、生成されたプロセスデータ、診断データ及び他のタイプのデータなどのプロセスを制御するためにリアルタイムで動作している間に、プロセスプラントによって生成されたデータを含むコンテンツまたはペイロードを含む。いくつかの構成では、第２のパケットカウンタ（ネットワークパケットカウンタとも称される）または他のそれぞれのノンスマテリアルが暗号化され、後続のメッセージ／パケットを処理する際に使用されるネットワークキーと共に提供される。ネットワークキー及び／またはネットワークパケットカウンタは、所望されれば、ランダムに生成されてもよい。

【００９２】

したがって、方法４５０は、プロセスを制御するためにリアルタイムで動作している間に、プロセスプラントによって生成されたデータを送信デバイスで受信すること（ブロック４６０）、送信デバイスによって、また、ネットワークキー及び任意選択でネットワークパケットカウンタを使用して、ペイロードとしてプロセスプラント生成データを含む後続のメッセージ／パケットを暗号化すること（ブロック４６２）、そして暗号化された後続メッセージ／パケットをデータダイオードを経由して受信デバイスに提供すること（ブロック４６５）をさらに含む。このように、ブロック４６２、４６５において、少なくとも一部がプロセスプラントによって生成されたデータを含む後続のメッセージ／パケットは、共有化機密ネットワークキーを使用してデータダイオードを経由する転送のためにセキュリティ保護される。いくつかの実施形態では、所望されれば（図示せず）追加の暗号化によって、データダイオードを経由する転送のために、後続のメッセージ／パケットがさらにセキュリティ保護される。

【００９３】

プロセスを制御するためにリアルタイムまたはオンライン動作中にプロセスプラントによって生成されたデータを受信すること（ブロック４６０）は、データ生成ソース（例えば、デバイスまたは構成要素２０２）からデータを直接受信すること、及び／またはデータ生成ソース（例えば、デバイスまたは構成要素２０２）からゲートウェイに送信されたデータをゲートウェイ（例えば、無線ゲートウェイ２０５）から受信することを含むことができる。送信デバイスで受信されるプロセスプラント生成データは、データ生成ソース（例えば、デバイスまたは構成要素２０２）によって、及び／またはゲートウェイ（例えば、無線ゲートウェイ２０５）によって、例えば、前述のような形態で、暗号化され、ラップされ、さもなければセキュリティ保護されることができる。

【００９４】

受信されたプロセスプラント生成データ（ブロック４６０）は、いくつかのデータ生成ソースデバイスが、例えば無線ゲートウェイ２０５及び／または送信デバイス４０２にそ

れぞれの生成されたデータをパブリッシュするときに、パブリッシュデータを含むことができる。他のデータ生成ソースデバイスは、それらのそれぞれの生成されたデータが送信デバイスで受信されるように（例えば、無線ゲートウェイ２０５及び／または送信デバイス４０２によって）ポーリングすることができる（ブロック４６０）。さらに、パブリッシュされ、ポーリングされ、またはそうでなければ受信される（ブロック４６０）かどうかにかかわらず、プロセスプラント生成データは、ＨＡＲＴ互換フォーマット、ＪＳＯＮ互換フォーマット、または任意の好適な工業通信プロトコル汎用通信プロトコルに従う、他の好適なフォーマットであってもよい。

【００９５】

前述したように、プロセスプラント生成データをペイロードとして含むメッセージ／パケットを暗号化すること（ブロック４６２）は、ネットワークキー及び任意選択でネットワークパケットカウンタを使用して、該メッセージ／パケットを例えばノンスマテリアルとして、暗号化することを含み、データダイオードを経由するメッセージ／パケットの転送は、データダイオードの単方向通信構成によってさらにセキュリティ保護される。

【００９６】

付加的に、データダイオードを経由して暗号化された後続メッセージを受信デバイスに供給または送信すること（ブロック４６５）は、例えば、プロセスプラントの１つ以上のデータ生成デバイスの各々を記述するそれぞれのコンテキスト情報を、データダイオードを経由して受信デバイスに反復的に告知または送信することを含むことができる。それぞれのコンテキスト情報は、対象データ生成デバイスの識別子と、対象デバイスによって生成されたデータが送信またはパブリッシュされるそれぞれの速度と、対象データ生成デバイスの現在の状態の指標、及び／または図５に関して上述したような、対象データ生成デバイスを記述する他の情報と、を含む。

【００９７】

コンテキスト情報を反復的に告知することは、一例では、データダイオードを経由して受信デバイスにコンテキスト情報を周期的に送信することを含むことができる。周期性の持続時間は、異なるタイプのコンテンツデータ、プロセスプラントのソースを生成する異なるデータ、及び／またはコンテンツデータの異なるコンシューマ（例えば、遠隔アプリケーション２０８）に対して異なることがある。例えば、特定のタイプのコンテンツデータの周期性の持続時間は、失われたパケット及び／または遅延のためのデータのコンシューマの許容誤差に基づくことができる。当然のことながら、送信デバイスが再起動した後、新しいデータ生成デバイスがプロセスプラントに追加されたとき、ユーザが指示したときなど、または所望されるときに、データダイオードを経由して受信デバイスにコンテキスト情報を告知することができる。

【００９８】

さらに、コンテキスト情報を告知することは、一実施形態では、工業通信プロトコルの１つ以上のメッセージタイプを利用することを含むことができる。例えば、何らかのタイプのＨＡＲＴ通信プロトコルがデータダイオードを経由して利用される場合、コンテキスト情報を告知することは、ＨＡＲＴコマンド０、２０、５０、７４、１０５、及び任意選択でコマンド７４及び１０１を使用することを含むことができる。別の実施形態では、コンテキスト情報を告知することは、ＪＳＯＮまたは他の何らかの好適な汎用通信プロトコルのような汎用通信プロトコルを使用して実装することができる。種々の工業通信プロトコルの様々なメッセージタイプは、一例では、告知に対応するように修正することができる。

【００９９】

データダイオードを経由して暗号化された後続メッセージを受信デバイスに提供すること（ブロック４６５）は、以前に送信されたコンテキスト情報に従って、データダイオードを経由してコンテンツデータを送信または転送することも含む。前述したように、コンテンツデータは、プロセスデータ、診断データなどのプロセスを制御するためにオンラインで動作している間に、プロセスプラントによって生成された動的データを含む。一実施

形態では、データダイオードを経由して暗号化された後続メッセージを提供することは、例えば、上述したような形態で、データダイオードを経由してコンテンツデータをパブリッシュすることを含む。

【０１００】

方法４５０は、第１のまたは結合キーを使用して第２の（例えば、後続の）初期化メッセージを暗号化することと（ブロック４６８）、暗号化された第２の初期化メッセージをデータダイオードを経由して受信デバイスに供給する（ブロック４７０）ことと、を含む。第２の初期化メッセージは、送信デバイスから受信デバイスへデータダイオードを経由して送信される後続のメッセージまたはパケットを処理するために、送信デバイス及び受信デバイスによって利用される更新されたまたは新たなネットワークキーを含む。更新されたまたは新たなネットワークキーは、ブロック４５２に関して論じた結合キーとは異なる別の共有化キーまたは共有化機密であってもよく、ブロック４５５、４５８に関して説明したネットワークキーとは異なる。後続のメッセージ／パケットを処理するためにも使用される、更新されたまたは新たなネットワークパケットカウンタは、更新されたまたは新たなネットワークキーと共にデータダイオードを経由して生成され、転送されてもよい。所望されれば、新たなまたは更新されたネットワークキー及び／またはパケットカウンタをランダムに生成することができる。

【０１０１】

したがって、ブロック４６８、４７０では、送信デバイス及び受信デバイスによって使用されてメッセージ／パケットを処理するネットワークキーが再同期される。この再同期化は、少なくともデータダイオードが単方向であり、したがって受信デバイスがその動作状態、メッセージの成功または不成功受信などに関するフィードバックを送信デバイスに供給することができないため重要である。しかしながら、ブロック４６８、４７０を介して、方法４５０は、ネットワークキーマテリアルを再同期させることによって、送信デバイスと受信デバイスとの間の通信切断をアドレス指定することができる。実際に、いくつかの実施形態では、ブロック４６８、４７０は、反復的に、周期的に、及び／または特定のイベントの生成に基づいて繰り返される（例えば、送信デバイスの再起動、ユーザが所望されるときに指示した際など）。周期性の持続時間は、例えば、失われたパケット及び／または遅延に対するコンテンツデータの１つ以上のコンシューマの許容誤差に基づくことができる。

【０１０２】

ブロック４６８、４７０に関して、受信デバイスは、例えば、送信された順序とは異なる順序でデータダイオードを介して到着するパケット処理のために、有限の期間、第１のネットワークキー／パケットカウンタ及び第２のネットワークキー／パケットカウンタの両方を維持する必要があり得ることに留意されたい。

【０１０３】

図７は、図２のプロセスプラント１００などのプロセスプラントから通信を安全に転送するための例示的な方法５００のフロー図を示す。いくつかの実施形態では、方法５００の少なくとも一部分は、１つ以上の固定可読メモリに格納されたコンピュータ実行可能命令またはコンピュータ可読命令のセットを実行することによって実装され、例えば、システム２００の１つ以上のプロセッサによって実行される。例えば、方法５００の少なくとも一部は、図１～５に示されるエッジゲートウェイ２１８または受信デバイス４０５のような、システム２００の１つ以上の構成要素によって遂行されてもよい。したがって、方法５００は、図１～図５を同時に参照して以下に説明されるが、これは説明を簡単にするためのものであり、限定的なものではない。

【０１０４】

ブロック５０２において、方法５００は、プロセスを制御するためにリアルタイムで動作している間に、プロセスプラントによって生成されたデータをデータダイオードを介して受信することを含む。データダイオードは、単方向通信が送信デバイスから受信デバイスに送信される一方で、受信デバイスから送信デバイスへの通信が防止されるように構成

されている。データダイオードを介して受信されるプロセスプラント生成データ（ブロック５０２）は、生成されたプロセスデータ、診断データ、及び他のタイプのデータを含むことができ、エッジゲートウェイ２１８または受信デバイス４０５などの受信デバイスで受信することができる。受信されたプロセスプラント生成データは、例えば、上述の暗号化技術によって、または他の何らかのセキュリティ機構によってセキュリティ保護されたセキュリティ保護されたデータであってもよい。

【０１０５】

ブロック５０５において、方法５００は、データダイオードを経由して利用されたものと同じセキュリティ機構を含むことができる１つ以上のセキュリティ機構を使用して、受信したプロセスプラント生成データをセキュリティ保護することを含むか、または１つ以上の異なるセキュリティ機構を含むことができる。ブロック５０８において、方法５００は、ブロック５０５でセキュリティ保護されたプロセスプラント生成データを、受信デバイスに通信可能に接続された別のシステムに送信することを含む。例えば、セキュリティ保護されたプロセスプラント生成データは、プロセスプラント生成データの１つ以上のアプリケーション、サービス、または他のコンシューマ２０８が常駐し実行する１つ以上の遠隔システム２１０に送信される。アプリケーション、サービスまたは他のコンシューマは、プロセスプラント生成データの少なくとも一部で動作してもよい。

【０１０６】

一実施形態では、受信したプロセスプラント生成データのセキュリティ保護すること（ブロック５０５）及びセキュリティ保護されたプロセスプラント生成データを他のシステムに送信する（ブロック５０８）ことは、受信デバイスと他のシステムとの間にセキュリティ保護された接続を確立することを含む。セキュリティ保護されたプロセスプラント生成データを他のシステムに送信すること（ブロック５０８）は、公衆インターネット、民間企業ネットワークなどの１つ以上の公衆／またはプライベートネットワークを介してデータを送信することを含むことができる。このように、受信デバイスと他のシステムとの間にセキュリティ保護された接続を確立することは、１つ以上の公衆及び／またはプライベートネットワークを介してセキュリティ保護された接続を確立することを含む。異なるタイプのコンテンツデータ、プロセスプラントのソースを生成する異なるデータ、及び／または所望されれば、コンテンツデータの異なるコンシューマに対して異なるセキュリティ保護された接続を確立することができる。

【０１０７】

一例では、受信デバイスと他のシステムとの間の接続は、トークンサービスを使用してセキュリティ保護される。受信デバイスは、他のシステムによって提供されるトークンサービスに対して認証し、認証に応答して、受信デバイスは、他のシステムからＳｈａｒｅｄ Ａｃｃｅｓｓ Ｓｉｇｎａｔｕｒｅ（共有アクセス署名）（ＳＡＳ）トークンを受信する。次いで、受信デバイスは、コンテンツデータ（例えば、プロセスプラント生成データ）を他のシステムに送信しながら、ＳＡＳトークンを使用する。例えば、受信デバイスは、ＳＡＳトークンを使用して、例えばＡＭＱＰ（Ａｄｖａｎｃｅｄ Ｍｅｓｓａｇｅ Ｑｕｅｕｉｎｇ Ｐｒｏｔｏｃｏｌ）接続を介して、他のシステムへの接続をセキュリティ保護し、認証する。付加的に、所望されれば、コンテンツデータ及びＳＡＳトークンは、他のシステムに送信する前に暗号化されてもよい。

【０１０８】

方法５００はまた、受信デバイスと他のシステムとの間の接続を再セキュリティ保護することを含むことができる（ブロック５１０）。受信デバイスと他のシステム５１０との間の接続を再セキュリティ保護することは、例えば、他のシステムから（例えば、他のシステムのトークンサービスから）更新されたＳＡＳトークンまたは異なるＳＡＳトークンを受信して、後続のコンテンツデータを送信するために使用することを含む。特定のＳＡＳトークンは、予め定義された満了期間（例えば、５分、１０分、１時間未満、または他の満了期間、設定可能であり得る）を有することができる。トークンの満了時に、受信デバイスは、後続のメッセージに使用する新しいＳＡＳトークンを要求または取得すること

ができる。代替的に、他のシステムは、前のトークンの満了時に使用する受信デバイス用の更新されたまたは新たなＳＡＳトークンを自動的に送信することができる。

【０１０９】

当然のことながら、受信デバイスと他のシステム（例えば、ブロック５０５、５０８、及び５１０）との間の接続のセキュリティ保護すること及び再セキュリティ保護することは、ＳＡＳトークン及びＡＭＱＰプロトコルを利用するものとして説明したが、これは、方法５００の様々な可能な実施形態の１つに過ぎない。任意の１つ以上の好適なＩＯＴセキュリティ機構、例えば、Ｘ．５０９証明書、他のタイプのトークン、ＭＱＴＴまたはＸＭＰＰなどの他のＩＯＴプロトコルなどが、方法５００によって利用されてもよい。

【０１１０】

本開示に記載された技術の実施形態は、以下の態様のうちの任意の数を単独でまたは組み合わせて含むことができる。

【０１１１】

１．プロセスプラントから別のシステムへの通信を安全に転送するための方法であって、フィールドゲートウェイにおいて、プロセスプラントのネットワークと、フィールドゲートウェイとエッジゲートウェイとの間の双方向通信を防止するように構成されたデータダイオードと、を相互接続し、データダイオードを経由してエッジゲートウェイに、プロセス制御プラントの１つ以上のデバイスの各々を記述するそれぞれのコンテキスト情報を反復的に告知することと，プロセスプラントがプロセスを制御するように動作している間に、１つ以上のデバイスの各々によって生成されたデータを、プロセスプラントネットワークにわたってフィールドゲートウェイで受信することと、フィールドゲートウェイによってデータダイオードを経由してエッジゲートウェイにプロセスプラントデータをパブリッシュすることと、を含む、方法。

【０１１２】

２．特定のデバイスを記述するそれぞれのコンテキスト情報を反復的に告知することが、特定のデバイスを記述するそれぞれのコンテキスト情報を周期的に送信することを含み、周期性が、失われたデータのアプリケーションの許容差に基づいており、アプリケーションが、特定のデバイスによって生成するデータのコンシューマであり、アプリケーションが、エッジゲートウェイに通信可能に接続される、先の態様に記載の方法。

【０１１３】

３．フィールドゲートウェイにおいて、１つ以上のデバイスの各々によって生成されたデータを受信することが、フィールドゲートウェイにおいて、ＨＡＲＴ－ＩＰ（登録商標）プロトコルを介して、１つ以上のデバイスの各々によって生成されたデータのうちの少なくとも一部を受信することを含む、先の態様１または２のいずれか１つに記載の方法。

【０１１４】

４．１つ以上のデバイスの各々によって生成されたデータのうちの少なくとも一部をＨＡＲＴ－ＩＰプロトコルを介して受信することが、１つ以上のデバイスの各々によってパブリッシュされたデータを受信することを含む、先の態様１～３のいずれか１つに記載の方法。

【０１１５】

５．フィールドゲートウェイによって、特定のデバイスにポーリングを送信することをさらに含み、フィールドゲートウェイにおいて、１つ以上の各々によって生成されたデータを受信することが、フィールドゲートウェイにおいて、ポーリングに応答して特定のデバイスによって生成されたデータを受信することを含む、先の態様１～４のいずれか１つに記載の方法。

【０１１６】

６．１つ以上のデバイスの各々によって生成されたデータを受信することが、診断結果を示すデータを受信することを含む、先の態様１～５のいずれか１つに記載の方法。

【０１１７】

７．１つ以上のデバイスの各々のそれぞれのコンテキスト情報を反復的に告知すること

が、コマンド０、コマンド２０、コマンド５０、コマンド７４、またはコマンド１０５を含むＨＡＲＴプロトコルコマンドの群からの少なくとも１つのＨＡＲＴプロトコルコマンドを使用して、１つ以上のデバイスの各々についてそれぞれのコンテキスト情報を反復的に送信することを含む、先の態様１～６のいずれか１つに記載の方法。

【０１１８】

８．１つ以上のデバイスの各々のそれぞれのコンテキスト情報を反復的に告知することが、１つ以上のデバイスの各々の識別子の指標と、１つ以上のデバイスの各々によって生成されたデータが提供されるべきそれぞれの速度の指標と、を反復的に送信することを含む、先の態様１～７のいずれか１つに記載の方法。

【０１１９】

９．プロセスプラントデータをデータダイオードを経由してパブリッシュすることが、ＨＡＲＴ－ＩＰ（登録商標）プロトコルを使用してデータダイオードを経由してプロセスプラントデータをパブリッシュすることを含む、先の態様１～８のいずれか１つに記載の方法。

【０１２０】

１０．プロセスプラントデータをデータダイオードを経由してパブリッシュすることが、ＪＳＯＮフォーマットを使用して、データダイオードを経由してプロセスプラントデータをパブリッシュすることを含む、先の態様１～９のいずれか１つに記載の方法。

【０１２１】

１１．プロセスプラントから別のシステムへの通信を安全に転送するためのシステムであって、プロセスプラントのネットワークに通信可能に結合されたフィールドゲートウェイと、別のシステムに通信可能に結合されたエッジゲートウェイと、フィールドゲートウェイとエッジゲートウェイとを相互接続するデータダイオードであって、エッジゲートウェイによって送信された通信がフィールドゲートウェイに進入することを防止するように構成される、データダイオードと、を備え、プロセスプラントが、工業プロセスを制御するように動作している間に、プロセスプラントに含まれる１つ以上のデバイスによって生成されたデータが、プロセスプラントネットワークを介してフィールドゲートウェイにおいて受信され、フィールドゲートウェイによって、データダイオードを経由してエッジゲートウェイにパブリッシュされる、システム。

【０１２２】

１２．態様１～１０のいずれかに記載の方法の少なくとも一部を遂行するようにさらに構成された、態様１１に記載のシステム。

【０１２３】

１３．１つ以上のデバイスによって生成されたデータが、ＨＡＲＴ－ＩＰ（登録商標）プロトコルを使用してデータダイオードを経由してパブリッシュされる、態様１１～１２に記載のシステム。

【０１２４】

１４．１つ以上のデバイスによって生成されたデータが、ＪＳＯＮフォーマットを使用してデータダイオードを経由してパブリッシュされる、態様１１～１３に記載のシステム。

【０１２５】

１５．１つ以上のデバイスによって生成されたデータが、受信され、フィールドゲートウェイに提供される無線ゲートウェイをさらに含む、態様１１～１４に記載のシステム。

【０１２６】

１６．無線ゲートウェイが、ＷｉｒｅｌｅｓｓＨＡＲＴ（登録商標）である、態様１１～１５に記載のシステム。

【０１２７】

１７．無線ゲートウェイが、１つ以上のデバイスによって生成されたデータを、ＨＡＲＴ－ＩＰプロトコルを使用してフィールドゲートウェイに提供する、態様１１～１６に記載のシステム。

【０１２８】

１８．１つ以上のデバイスのうちの少なくとも１つが、それぞれのデータを前記無線ゲートウェイにパブリッシュする、態様１１～１７に記載のシステム。

【０１２９】

１９．それぞれの生成されたデータがパブリッシュされる無線ゲートウェイが、それぞれの生成されたデータのサブスクライバである、態様１１～１８に記載のシステム。

【０１３０】

２０．無線ゲートウェイが、１つ以上のデバイスのうちの少なくとも１つをポーリングして、それぞれの生成されたデータを取得する、態様１１～１９に記載のシステム。

【０１３１】

２１．別のシステムで実行されるアプリケーションが、プロセスプラントに含まれる１つ以上のデバイスによって生成されたデータのうちの少なくとも一部のコンシューマである、態様１１～２０に記載のシステム。

【０１３２】

２２．エッジゲートウェイが、プロセスプラントに含まれる１つ以上のデバイスによって生成されたデータのうちの少なくとも一部をパブリッシュし、別のシステムで実行されるアプリケーションが、エッジゲートウェイによってパブリッシュされたデータのサブスクライバである、態様１１～２１に記載のシステム。

【０１３３】

２３．プロセスプラントが工業プロセスを制御するように動作している間に、１つ以上のデバイスによって生成されたデータが、１つ以上のデバイスによって生成された少なくとも１つの動的データまたは１つ以上のデバイスの診断もしくは試験の結果として生成された診断データのうちの少なくとも１つを含む、態様１１～２２に記載のシステム。

【０１３４】

２４．データダイオードが、イーサネット接続される、態様１１～２３に記載のシステム。

【０１３５】

２５．データダイオードが、直列接続される、態様１１～２４に記載のシステム。

【０１３６】

２６．フィールドゲートウェイが、データダイオードを経由してエッジゲートウェイに、１つ以上のデバイスの各々を記述するそれぞれの情報を、さらにパブリッシュする、態様１１～２５に記載のシステム。

【０１３７】

２７．１つ以上のデバイスの各々を記述するそれぞれの情報が、１つ以上のデバイスの各々のそれぞれのアイデンティティの指標と、１つ以上のデバイスの各々によって生成されたデータがパブリッシュされるべきそれぞれの速度と、を含む、態様１１～２６に記載のシステム。

【０１３８】

２８．１つ以上のデバイスの各々を記述するそれぞれの情報が、１つ以上のデバイスの各々の状態の指標をさらに含む、態様１１～２７に記載のシステム。

【０１３９】

２９．別のシステムが、
プロセスプラントで起こる状態及び／または事象を監視することと、

【０１４０】

プロセスプラントで起こる状況及び／または事象を感知することと、プロセスプラントによって制御されているプロセスの少なくとも一部分を監視することと、生成されたデータを使用して記述的分析を遂行することと、生成されたデータを使用して規範的分析を遂行すること、または、生成されたデータに基づいて、プロセスプラントの少なくとも一部を修正するための規範的機能を生成することと、のうちの少なくとも１つのことを行うように構成される、態様１１～２８に記載のシステム。

【０１４１】

３０．別のシステムが、少なくとも部分的に１つ以上のクラウドコンピューティングシステムで実装される、態様１１～２９に記載のシステム。

【０１４２】

３１．先の態様のいずれかの他の１つと組み合わせる、先の態様のいずれか１つ。

【０１４３】

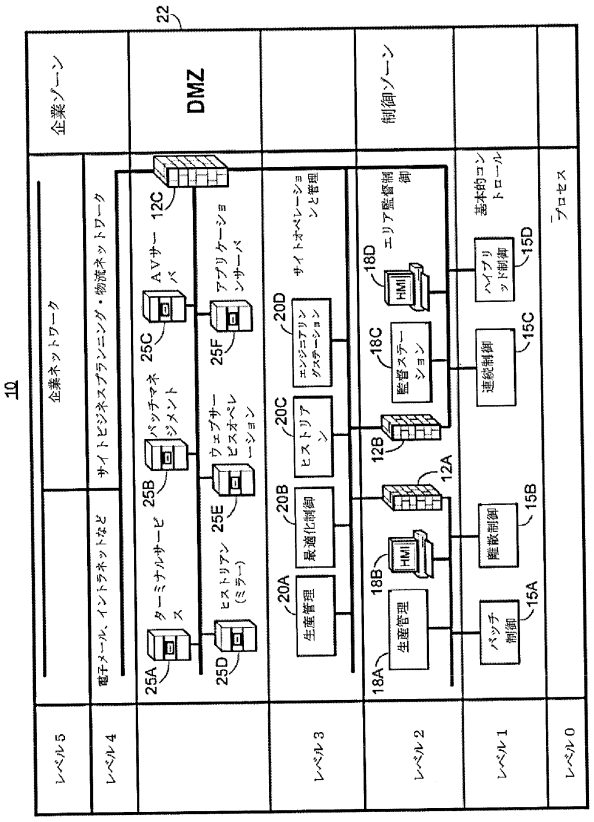
ソフトウェアとして実行される場合、本明細書において記載されるアプリケーション、サービス、及びエンジンのいずれも、磁気ディスク、レーザディスク、固体メモリデバイス、分子メモリ格納デバイス、または他の格納媒体のような任意の有形の固定のコンピュータ可読メモリに格納することができ、コンピュータまたはプロセッサのＲＡＭまたはＲＯＭなどに格納することができる。本明細書において開示される例示的なシステムは、構成要素の中でもとりわけ、ハードウェア上で実行されるソフトウェア及び／またはファームウェアを含むものとして開示されているが、このようなシステムは、単なる例示に過ぎず、限定的に考えられてはならないことに留意されたい。例えば、これらのハードウェア構成要素、ソフトウェア構成要素、及びファームウェア構成要素のいずれか、または全てが、ハードウェアとして排他的に搭載される、ソフトウェアとして排他的に搭載される、またはハードウェア及びソフトウェアの任意の組み合わせとして搭載されるような構成が想到される。したがって、当該技術分野の当業者であれば、提供されるこれらの例が、このようなシステムを実現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であろう。

【０１４４】

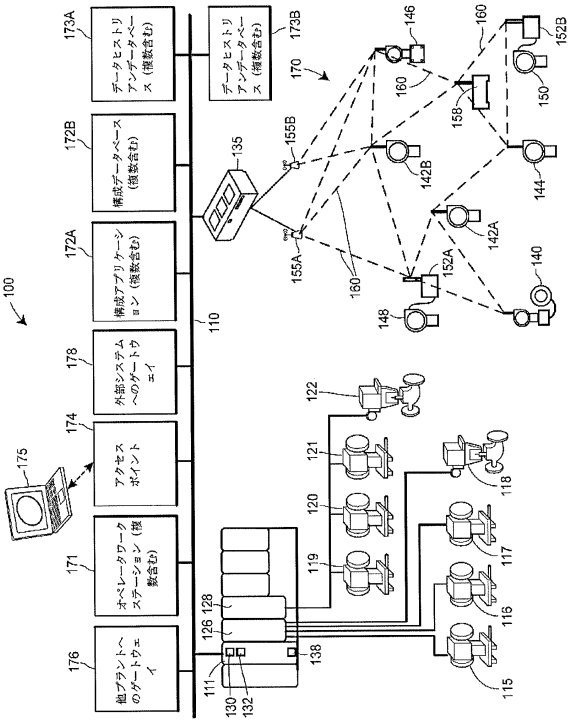
以上、本発明を例示のみを意図したものであって発明の限定を意図したものではない特定の例を参照して説明したが、発明の趣旨及び範囲を逸脱することなく、開示された実施形態に変更、追加、または削除を行ってよいことは、当該技術分野における当業者には明らかであろう。

【図面】

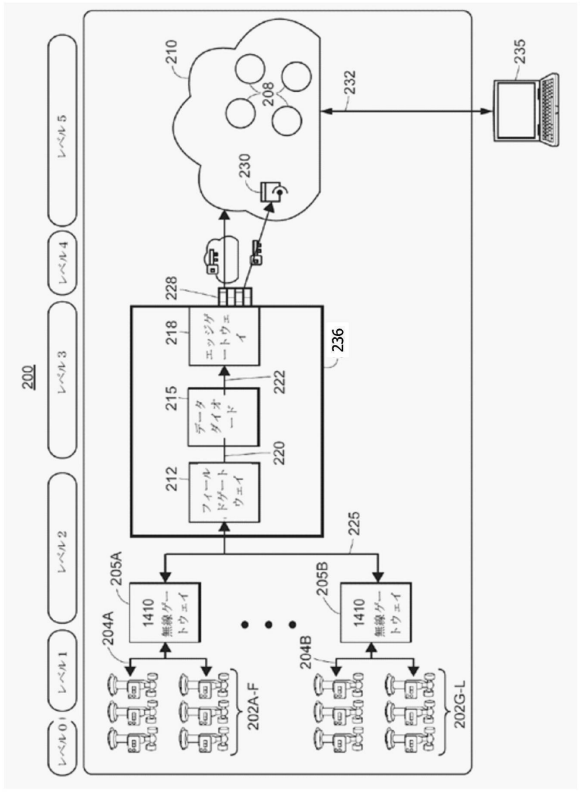
【図１】


10
22
企業ゾーン
企業ネットワーク
サイトビジネスプランニング・物流ネットワーク
電子メール、イントラネットなど
DMZ
制御ゾーン
基本的コントロール
プロセス
レベル5
レベル4
レベル3
レベル2
レベル1
レベル0
ターミナルサービス
AVサーバ
パッチマネジメント
ウェブサービスオペレーション
アプリケーションサーバ
ヒストリアン（ミラー）
ヒストリアン
最適化制御
生産管理
エンジニアリングステーション
サイトオペレーションと管理
監督ステーション
エリア監督制御
HMI
生産管理
連続制御
離散制御
バッチ制御
ハイブリッド制御
12A
12B
12C
15A
15B
15C
15D
18A
18B
18C
18D
20A
20B
20C
20D
25A
25B
25C
25D
25E
25F

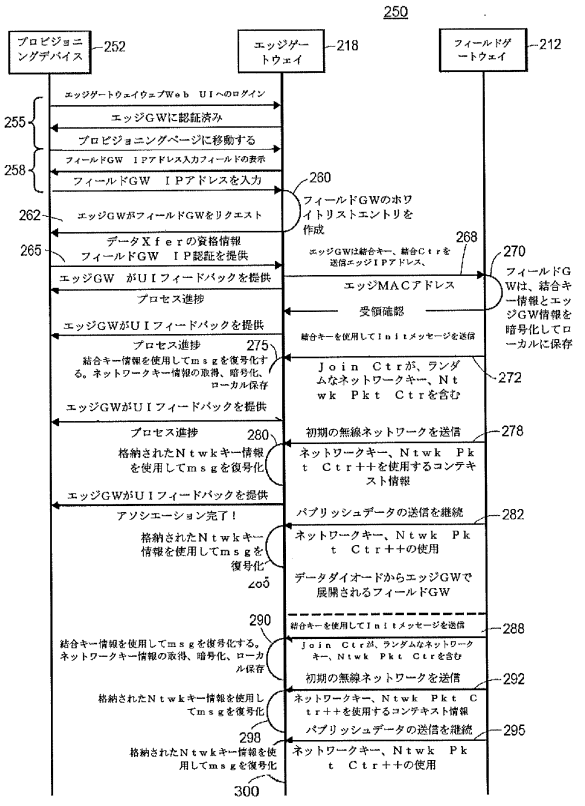
【図２】


100
110
データヒストリアンデータベース（複数含む）
構成データベース（複数含む）
構成アプリケーション（複数含む）
外部システムへのゲートウェイ
アクセスポイント
オペレータワークステーション（複数含む）
他プラントへのゲートウェイ
135
138
142A
142B
144
146
148
150
152A
152B
155A
155B
158
160
170
173A
173B
174
175
176
178
111
115
116
117
118
119
120
121
122
126
128
130
132
140

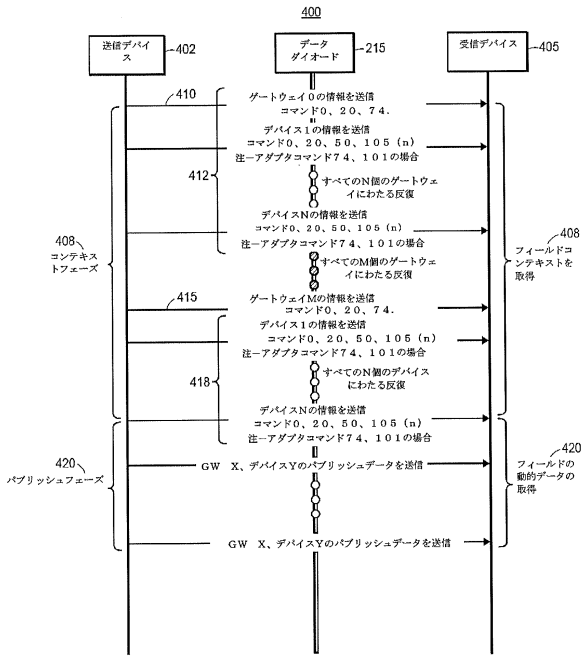
【図３】


200
210
208
230
232
235
228
218
エッジゲートウェイ
236
215
データダイオード
222
220
212
フィールドゲートウェイ
225
205A
205B
1410
無線ゲートウェイ
204A
204B
202A-F
202G-L
レベル5
レベル4
レベル3
レベル2
レベル1
レベル0

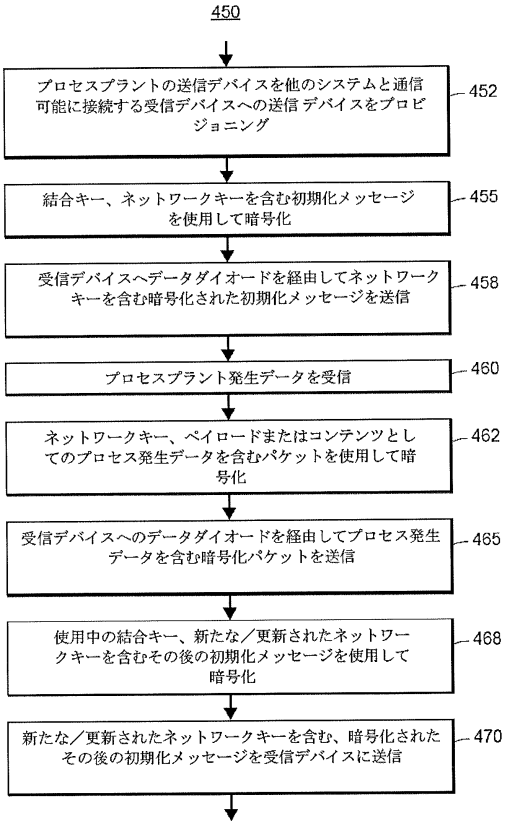
【図４】


250
プロビジョニングデバイス 252
エッジゲートウェイ 218
フィールドゲートウェイ 212
エッジゲートウェイウェブWeb UIへのログイン
255
エッジGWに認証済み
プロビジョニングページに移動する
フィールドGW IPアドレス入力フィールドの表示
258
フィールドGW IPアドレスを入力
260
フィールドGWのホワイトリストエントリを作成
262
エッジGWがフィールドGWをリクエスト
データXferの資格情報
フィールドGW IP認証を提供
265
エッジGWは結合キー、結合Ctrを送信エッジIPアドレス、
268
270
フィールドGWは、結合キー情報とエッジGW情報を暗号化してローカルに保存
エッジMACアドレス
受領確認
エッジGW がUIフィードバックを提供
プロセス進捗
エッジGWがUIフィードバックを提供
プロセス進捗
結合キー情報を使用してmsgを復号化する。ネットワークキー情報の取得、暗号化、ローカル保存
275
結合キーを使用してInitメッセージを送信
Join Ctrが、ランダムなネットワークキー、Ntwk Pkt Ctrを含む
272
エッジGWがUIフィードバックを提供
プロセス進捗
格納されたNtwkキー情報を使用してmsgを復号化
280
初期の無線ネットワークを送信
278
ネットワークキー、Ntwk Pkt Ctr++を使用するコンテキスト情報
エッジGWがUIフィードバックを提供
アソシエーション完了！
パブリッシュデータの送信を継続
282
格納されたNtwkキー情報を使用してmsgを復号化
ネットワークキー、Ntwk Pkt Ctr++の使用
データダイオードからエッジGWで展開されるフィールドGW
290
結合キーを使用してInitメッセージを送信
288
結合キー情報を使用してmsgを復号化する。ネットワークキー情報の取得、暗号化、ローカル保存
Join Ctrが、ランダムなネットワークキー、Ntwk Pkt Ctrを含む
初期の無線ネットワークを送信
292
格納されたNtwkキー情報を使用してmsgを復号化
ネットワークキー、Ntwk Pkt Ctr++を使用するコンテキスト情報
パブリッシュデータの送信を継続
295
298
格納されたNtwkキー情報を使用してmsgを復号化
ネットワークキー、Ntwk Pkt Ctr++の使用
300

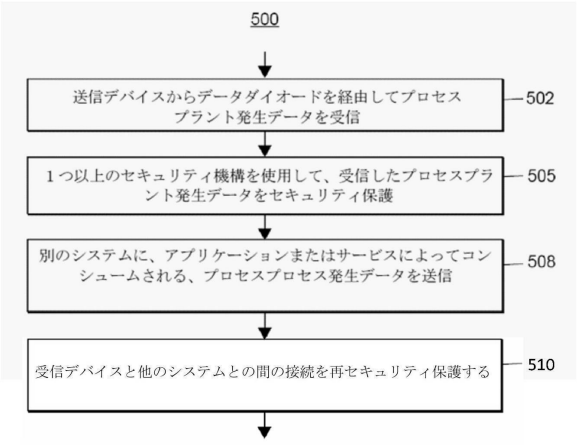
【図５】


400
送信デバイス
402
データダイオード
215
受信デバイス
405
410
ゲートウェイ０の情報を送信
コマンド０、２０、７４．
デバイス１の情報を送信
コマンド０、２０、５０、１０５（ｎ）
注－アダプタコマンド７４、１０１の場合
412
すべてのＮ個のゲートウェイにわたる反復
デバイスＮの情報を送信
コマンド０、２０、５０、１０５（ｎ）
注－アダプタコマンド７４、１０１の場合
すべてのＭ個のゲートウェイにわたる反復
408
コンテキストフェーズ
408
フィールドコンテキストを取得
415
ゲートウェイＭの情報を送信
コマンド０、２０、７４．
デバイス１の情報を送信
コマンド０、２０、５０、１０５（ｎ）
注－アダプタコマンド７４、１０１の場合
418
すべてのＮ個のデバイスにわたる反復
デバイスＮの情報を送信
コマンド０、２０、５０、１０５（ｎ）
注－アダプタコマンド７４、１０１の場合
420
パブリッシュフェーズ
GW X、デバイスYのパブリッシュデータを送信
420
フィールドの動的データの取得
GW X、デバイスYのパブリッシュデータを送信

【図６】


450
プロセスプラントの送信デバイスを他のシステムと通信可能に接続する受信デバイスへの送信デバイスをプロビジョニング
452
結合キー、ネットワークキーを含む初期化メッセージを使用して暗号化
455
受信デバイスへデータダイオードを経由してネットワークキーを含む暗号化された初期化メッセージを送信
458
プロセスプラント発生データを受信
460
ネットワークキー、ペイロードまたはコンテンツとしてのプロセス発生データを含むパケットを使用して暗号化
462
受信デバイスへのデータダイオードを経由してプロセス発生データを含む暗号化パケットを送信
465
使用中の結合キー、新たな／更新されたネットワークキーを含むその後の初期化メッセージを使用して暗号化
468
新たな／更新されたネットワークキーを含む、暗号化されたその後の初期化メッセージを受信デバイスに送信
470

【図７】


500
送信デバイスからデータダイオードを経由してプロセスプラント発生データを受信
502
１つ以上のセキュリティ機構を使用して、受信したプロセスプラント発生データをセキュリティ保護
505
別のシステムに、アプリケーションまたはサービスによってコンシュームされる、プロセスプロセス発生データを送信
508
受信デバイスと他のシステムとの間の接続を再セキュリティ保護する
510

フロントページの続き

アメリカ合衆国 テキサス ７８６８１ ラウンド ロック ブラックジャック ドライブ １５０３

審査官 稲垣 浩司

(56)参考文献 特開２０１３－１９５３９８（ＪＰ，Ａ）
特開２０１４－２１９９９１（ＪＰ，Ａ）
特開２０１６－１０５５９１（ＪＰ，Ａ）

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０５Ｂ ２３／０２