(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2016-105591
(P2016-105591A)
(43)公開日　平成28年6月9日(2016.6.9)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/66	(2006.01)	H04L	12/66	B	5H220
G05B 19/042	(2006.01)	G05B	19/042		5K030
H04L 12/28	(2006.01)	H04L	12/28	100F	5K033

審査請求 未請求　請求項の数 37　ＯＬ　（全 18 頁）

(21)出願番号　特願2015-227228 (P2015-227228)
(22)出願日　平成27年11月20日 (2015.11.20)
(31)優先権主張番号　14/549,909
(32)優先日　平成26年11月21日 (2014.11.21)
(33)優先権主張国　米国(US)

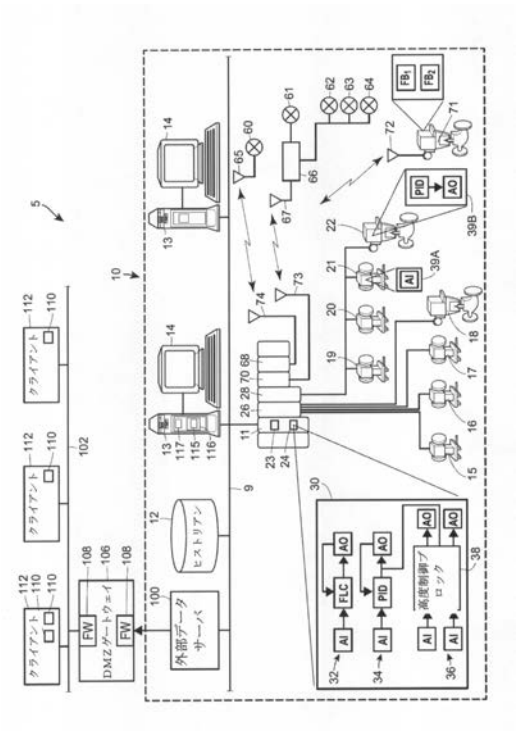
（特許庁注：以下のものは登録商標）
１．イーサネット

(71)出願人　512132022
フィッシャー－ローズマウント　システムズ，インコーポレイテッド
アメリカ合衆国　テキサス州　７８６８１　ラウンド　ロック　ウェスト　ルイス　ヘナ　ブルバード　１１００　ビルディング　１
(74)代理人　100079049
弁理士　中島　淳
(74)代理人　100084995
弁理士　加藤　和詳
(72)発明者　リー　エー．　ネイゼル
アメリカ合衆国　７８７５９　テキサス州　オースティン　カシア　ドライブ　１０７２７

最終頁に続く

(54)【発明の名称】安全な外部アクセスを有するプロセスプラントネットワーク

(57)【要約】　（修正有）
【課題】プロセス制御システムにおいて、外部データサーバがセキュリティ攻撃によって侵害される能力を減少または排除する費用効率の高いセキュリティ機構を提供する。
【解決手段】ファイアウォール１０８を介してプロセス制御データを外部ネットワーク１０２に提供する外部データサーバ１００を有し、事前に設定されたまたは事前に決められたデータビューをＤＭＺゲートウェイ１０６に公表するように外部データサーバを構成する。ＤＭＺゲートウェイは、外部データサーバに対して読み取り及び書き込み要求を実施することなく、データビューによって定義されたデータ／イベント／アラームを制御システムから自動的に受信し、外部ネットワーク上のデータビュー内のデータを再公表して、公表されたデータビュー内のプロセス制御データを外部ネットワークに接続された１つ以上のクライアントアプリケーション１１０に対して利用可能にする。
【選択図】図１



【特許請求の範囲】
【請求項１】
通信システムであって、
共に通信可能に接続された複数のプロセス制御デバイスを含むプロセス制御ネットワークと、
前記プロセス制御ネットワーク内に配置された外部データサーバと、
前記プロセス制御ネットワークの外側に配置された外部通信ネットワークと、
前記外部データサーバと前記外部通信ネットワークとの間に通信可能に連結されたゲートウェイデバイスと、
１つ以上のデータビューに従ってデータを前記外部通信ネットワークに公表するように前記外部データサーバを構成するために、前記プロセス制御ネットワーク内のデバイス内のプロセッサ上で実行する、前記プロセス制御ネットワーク内の前記デバイス内のコンピュータメモリに保存された構成アプリケーションであって、前記１つ以上のデータビューのそれぞれが、公表されるプロセス制御データのセットを定義する、構成アプリケーションと、を備える、前記通信システム。
【請求項２】
前記構成アプリケーションが、１つ以上のデータビュー内の前記データを指定するデータビューファイルを含み、かつ前記データビューファイルを前記外部通信ネットワークに接続された前記ゲートウェイデバイスに公表するように前記外部データサーバを構成するために、前記プロセス制御ネットワーク内の前記デバイス内の前記プロセッサ上でさらに実行する、請求項１に記載の前記通信システム。
【請求項３】
前記外部データサーバが、前記ゲートウェイデバイスからの読み取りコールに応答することができない、請求項１に記載の前記通信システム。
【請求項４】
前記外部データサーバが、前記ゲートウェイデバイスからの書き込みコールに応答することができない、請求項１に記載の前記通信システム。
【請求項５】
前記外部データサーバが、前記ゲートウェイデバイスからの構成コールに応答することができない、請求項１に記載の前記通信システム。
【請求項６】
前記１つ以上のデータビューのうちの１つが、前記プロセス制御ネットワーク内のもう１つのプロセスコントローラによって生成または収集されるプロセス制御データのセットを指定する、請求項１に記載の前記通信システム。
【請求項７】
前記１つ以上のデータビューのうちの１つが、前記プロセス制御ネットワーク内のもう１つのフィールドデバイスによって生成または収集されるプロセス制御データを指定する、請求項１に記載の前記通信システム。
【請求項８】
前記１つ以上のデータビューのうちの１つが、前記プロセス制御ネットワーク内のさらなるデバイスのメモリに保存されたプロセス制御構成データを指定する、請求項１に記載の前記通信システム。
【請求項９】
前記１つ以上のデータビューのうちの１つが、前記プロセス制御ネットワーク内の１つ以上のプロセス制御デバイスに関する保守データを指定する、請求項１に記載の前記通信システム。
【請求項１０】
前記構成アプリケーションが、前記１つ以上のデータビューに従ってデータを外部データサーバに定期的に公表するように構成するために実行する、請求項１に記載の前記通信システム。

【請求項１１】
前記外部データサーバが、ＯＰＣプロトコルに準拠する、請求項１に記載の前記通信システム。
【請求項１２】
前記外部データサーバが、前記プロセス制御ネットワーク内のデバイスからのみ構成コマンドを受信し、それに従って行動するように構成される、請求項１に記載の前記通信システム。
【請求項１３】
前記構成アプリケーションが、前記外部データサーバ内で保存及び実行される、請求項１に記載の前記通信システム。
【請求項１４】
前記プロセス制御ネットワーク内に配置されたデータまたはイベントヒストリアンをさらに含み、前記外部データサーバが、前記１つ以上のデータビューによって定義された前記プロセス制御データのうちの一部を、前記データまたはイベントヒストリアンから取得する、請求項１に記載の前記通信システム。
【請求項１５】
前記ゲートウェイデバイスがファイアウォールを含む、請求項１に記載の前記通信システム。
【請求項１６】
前記ゲートウェイデバイスが、前記外部データサーバから受信された前記１つ以上のデータビューに従ってデータを前記外部通信ネットワーク上の１つ以上のクライアントアプリケーションに再公表するように構成される、請求項１に記載の前記通信システム。
【請求項１７】
前記ゲートウェイデバイスが、前記外部データサーバに対して読み取りまたは書き込みまたは構成コールを実行することができない、請求項１に記載の前記通信システム。
【請求項１８】
通信システムであって、
共に通信可能に接続された複数のプロセス制御デバイスを含むプロセス制御ネットワークと、
前記プロセス制御ネットワーク内に配置された外部データサーバと、
前記プロセス制御ネットワークの外側に配置された外部通信ネットワークと、
前記外部データサーバと前記外部通信ネットワークとの間に通信可能に連結されたゲートウェイデバイスと、を備え、
前記外部データサーバが、１つ以上のデータビューファイルを保存し、１つ以上のデータビューファイルに従ってデータを前記ゲートウェイデバイスに公表するために実行し、前記１つ以上のデータビューファイルのそれぞれが、公表される前記プロセス制御ネットワーク内からのプロセス制御データのセットを定義し、前記ゲートウェイデバイスが、前記外部データサーバからの公表を介して前記外部データサーバから受信されるデータを定義するさらなるデータビューファイルのセットを保存し、前記ゲートウェイデバイスが、前記さらなるデータビューファイルのセットを使用して、データを前記外部通信ネットワークに接続される１つ以上のクライアントアプリケーションに再公表するように構成される、前記通信システム。
【請求項１９】
前記外部データサーバが、前記１つ以上のデータビューファイルに従ってデータを前記ゲートウェイデバイスに定期的に公表する、請求項１８に記載の前記通信システム。
【請求項２０】
前記１つ以上のデータビューファイルを保存するように前記外部データサーバを構成するために実行する前記プロセス制御ネットワーク内のデバイス内に保存される構成アプリケーションをさらに含む、請求項１８に記載の前記通信システム。
【請求項２１】

前記構成アプリケーションが、前記外部データサーバ内に保存される、請求項２０に記載の前記通信システム。
【請求項２２】
前記ゲートウェイデバイスが、前記１つ以上のさらなるデータビューファイルを保存する、請求項１８に記載の前記通信システム。
【請求項２３】
前記外部データサーバが、前記ゲートウェイデバイスからの読み取りまたは書き込みコールに応答することができないように構成される、請求項１８に記載の前記通信システム。
【請求項２４】
前記ゲートウェイデバイスが、前記外部データサーバと前記外部通信ネットワークとの間に配置されたファイアウォールを含む、請求項１８に記載の前記通信システム。
【請求項２５】
前記ゲートウェイデバイスが、前記外部データサーバに読み取りまたは書き込みコールを送信することができないように構成される、請求項１８に記載の前記通信システム。
【請求項２６】
前記外部データサーバが、前記プロセス制御ネットワーク内のソースからの構成コマンドにのみ応答するように構成される、請求項１８に記載の前記通信システム。
【請求項２７】
前記外部データサーバが、前記プロセス制御ネットワークを介して、前記１つ以上のデータビューによって定義されたデータを取得するように構成される、請求項１８に記載の前記通信システム。
【請求項２８】
プロセス制御ネットワークからの情報を、前記プロセス制御ネットワーク内に連結された外部データサーバを有し、かつ外部通信ネットワークに接続されたゲートウェイデバイスに通信可能に接続されたシステムにおいて、前記外部通信ネットワークに安全に提供する方法であって、
１つ以上のデータビューファイルを前記外部データサーバ内に保存することであって、各データビューファイルが、前記外部通信ネットワークに定期的に公表されるプロセス制御データのセットを指定する、保存することと、
データ公表信号を使用して前記ゲートウェイデバイスと通信するように前記外部データサーバを構成することと、
前記外部データサーバに、前記１つ以上のデータビューファイルによって指定されたプロセス制御データを前記ゲートウェイデバイスに自動的に公表させることと、
前記外部データサーバが、前記ゲートウェイデバイスからの読み取り、書き込み、及び構成コマンドに応答することを防ぐことと、を含む、前記方法。
【請求項２９】
前記ゲートウェイデバイスに、前記外部データサーバによって前記ゲートウェイデバイスに送信された前記プロセス制御データを前記外部通信ネットワーク上の１つ以上のクライアントアプリケーションに再公表させることをさらに含む、請求項２８に記載の前記方法。
【請求項３０】
データ公表信号を介して前記外部データサーバから受信され、かつ前記１つ以上のクライアントアプリケーションに再公表される前記プロセス制御データを定義する前記ゲートウェイデバイスにさらなるデータビューファイルを保存することをさらに含む、請求項２９に記載の前記方法。
【請求項３１】
前記１つまたは前記クライアントデバイスに、前記ゲートウェイデバイスによって再公表された前記プロセス制御データにサブスクライブさせることをさらに含む、請求項２９に記載の前記方法。

【請求項３２】
前記プロセス制御ネットワーク内のデバイス内に構成アプリケーションを保存することと、前記構成アプリケーションを使用して、前記１つ以上のデータビューファイルによって指定された前記プロセス制御データを公表するように前記外部データサーバを構成することと、をさらに含む、請求項２８に記載の前記方法。
【請求項３３】
前記プロセス制御データを１つ以上のクライアントアプリケーションに再公表するように前記ゲートウェイデバイスを構成することをさらに含む、請求項３２に記載の前記方法。
【請求項３４】
前記構成アプリケーションを保存することが、前記構成アプリケーションを、前記外部データサーバとは異なる前記プロセス制御ネットワーク上のデバイス内に保存することを含む、請求項３２に記載の前記方法。
【請求項３５】
前記外部データサーバに、前記１つ以上のデータビューファイルによって指定されたプロセス制御データを前記ゲートウェイデバイスに自動的に公表させることが、前記外部データサーバに、前記１つ以上のデータビューファイルによって指定された前記プロセス制御データを前記プロセス制御ネットワークから取得させ、かつ前記取得されたプロセス制御データを前記ゲートウェイデバイスに定期的に送信させることを含む、請求項２８に記載の前記方法。
【請求項３６】
前記プロセス制御ネットワーク内のデバイスから受信された構成コマンドを実施することしかできないように前記外部データサーバを構成することをさらに含む、請求項２８に記載の前記方法。
【請求項３７】
前記外部通信ネットワーク上の１つ以上のクライアントアプリケーションから受信されたコマンドに応答して、前記外部データサーバに対して読み取り及び書き込みコールを実施することができないように前記ゲートウェイデバイスを構成することをさらに含む、請求項２８に記載の前記方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本出願は、概して、プロセスプラント通信システムに関し、より具体的には、プロセスプラント制御及び保守システムの安全を確保しながら、これらのシステムからのデータへの外部アクセスを可能にすることに関する。
【背景技術】
【０００２】
関連分野の説明
発電、化学、石油、または他の製造工程において使用されるもののような、分散型または拡張可能なプロセス制御システムなどのプロセス制御システムは、典型的には、互いに、プロセス制御ネットワークを介して少なくとも１つのホストまたはオペレータに、及びアナログ、デジタル、またはアナログ／デジタル複合型バスを介して１つ以上のフィールドデバイスに、通信可能に連結された１つ以上のコントローラを含む。例えば、バルブ、バルブポジショナ、スイッチ、及びトランスミッタ（例えば、温度、圧力、及び流量センサ）であり得るフィールドデバイスは、バルブを開閉すること、デバイスのスイッチをオン及びオフにすること、ならびにプロセスパラメータを測定することなど、プロセスまたはプラント内で機能を実行する。コントローラは、フィールドデバイスによってなされたプロセスもしくはプラント測定を示す信号、及び／またはフィールドデバイスに付属する他の情報を受信し、この情報を使用して１つ以上の制御ルーチンを実施し、次いでプラントネットワークのバスまたは通信チャネルを介してフィールドデバイスに送信される制御

信号を生成してプロセスもしくはプラントの操作を制御する。オペレータまたは保守員が、プラントの現状を見ること、プラントの操作を修正すること、デバイスを較正することなど、プロセスまたはプラントに関して任意の所望の機能を実行ことができるように、フィールドデバイス及びコントローラからの情報は、典型的には、オペレータワークステーションによって実行される１つ以上のアプリケーションに利用可能になる。

【０００３】

操作中、典型的にはプロセス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りなされた、もしくはそれに関連するプロセス測定もしくはプロセス変数を示す信号、及び／またはフィールドデバイスに付属する他の情報を受信し、この情報を使用してコントローラアプリケーションを実行する。コントローラアプリケーションは、例えば、プロセス制御決定を行う様々な制御モジュールを実施し、受信した情報に基づいて制御信号を生成し、ＨＡＲＴ（登録商標）及び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内の制御モジュールまたはブロックと連携する。プロセスコントローラ内の制御モジュールは、通信ラインまたは他の信号経路を介して制御信号をフィールドデバイスに送信し、それによってプロセスの操作を制御する。

【０００４】

フィールドデバイス及びプロセスコントローラからの情報は、典型的には、プラント内もしくはプラント外部の１つ以上の他のハードウェアデバイス、例えば、オペレータワークステーション、保守ワークステーション、サーバ、パーソナルコンピュータ、携帯デバイス、データもしくはイベントヒストリアン、レポートジェネレータ、集中データベースなどに、１つ以上の安全なプロセス制御ネットワークを介して利用可能になる。プロセス制御ネットワークを介して通信される情報は、オペレータもしくは保守員が、プロセスに関して所望の機能を実行すること、及び／またはプラントの稼働を見ることを可能にする。例えば、制御情報は、オペレータが、プロセス制御ルーチンの設定を変更すること、プロセスコントローラまたはスマートフィールドデバイス内の制御モジュールの動作を修正すること、プロセスの現状またはプロセスプラント内の特定のデバイスの状態を見ること、フィールドデバイス及びプロセスコントローラによって生成されるアラーム及びまたはアラートを見ること、作業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のためにプロセスの動作をシミュレーションすること、プロセスプラント内の問題またはハードウェア障害を診断すること、などを可能にする。

【０００５】

フィールドデバイス及びコントローラは、通常、例えば、イーサネット構成のＬＡＮとして実装され得る１つ以上の安全なプロセス制御ネットワークを介して、他のハードウェアデバイスと通信する。プロセス制御ネットワークは、プロセスパラメータ、ネットワーク情報、及び他のプロセス制御データを、様々なネットワークデバイスを介して、プロセス制御システム内の様々なエンティティに送信する。典型的なネットワークデバイスとしては、ネットワークインターフェースカード、ネットワークスイッチ、ルータ、サーバ、ファイアウォール、コントローラ、及びオペレータワークステーションが挙げられる。ネットワークデバイスは、典型的には、ネットワークを介したデータのフローを、そのルーティング、フレームレート、タイムアウト、及び他のネットワークパラメータを制御することによって促進するが、プロセスデータ自体は変更しない。プロセス制御ネットワークのサイズ及び複雑性が大きくなると、それ相応にネットワークデバイスの数及び種類が増加する。システム及びネットワーク増大の結果として、これらの複合システム内のセキュリティ及びそれらの管理は、ますます困難になっている。しかしながら、手始めに、これらのネットワークは、一般的に他の外部ネットワークから孤立され、１つ以上のファイアウォールによって外部攻撃から守られる。

【０００６】

実際、典型的な産業用制御システムにおいて、プラント制御システムワークステーション／サーバは、プラントに関連する様々な機能を実行する外部プラントネットワークと、

制御システム内で制御及びデータ取得機能を実行する埋込型制御デバイス（例えば、コントローラ、ＰＬＣ、ＲＴＵ）との間に戦略的に置かれる。結果として、制御ワークステーション／サーバにとっての主要なセキュリティ目標は、マルウェアが制御システムに入り、埋込型デバイスに悪影響を与えることを防ぐこと、ならびに、マルウェアがプラントプロセス制御データベース内に保存された構成及び過去データを変更することを防ぐことである。依然としてさらに、これらのワークステーション／サーバは、プラント構成の権限のない変更、プラントデータへの権限のないアクセスなどを防ぐために、制御システムへの権限のないアクセスを防ぐ。ファイアウォール、「アンチウイルス」ソフトウェア、及び「ホワイトリスティング」などのいくつかのセキュリティ機能を使用して、これらのセキュリティ目標に対処することができるが、これらのセキュリティ機能は、典型的には、十分ではない。例えば、アンチウイルスソフトウェアは、「ゼロデイ」ウイルスから守ることができず、ホワイトリスティングは、権限のないアプリケーションの実行を防ぐだけである。加えて、これらのセキュリティ機能はプラントオペレータの活動を妨げる可能性を有するため、これらの機能のいくつかは、介入的すぎてプロセス制御システムにおいて実用的ではない。

【０００７】

一般的には、ゼロデイ攻撃の中心にあるようなマルウェアは、典型的に、プロセス制御ネットワーク内のメモリデバイス、ネットワークポート、もしくはダイレクトデータリンクにアクセスする特権または承認を有するアプリケーションまたはサービスの操作によって、外部ネットワークへの承認された通信接続を介して安全な制御システムネットワークに持ち込まれる。その後、マルウェアは、他のデバイス（例えば、通信を介して）に伝播され、及び／または、マルウェアに感染したアプリケーションもしくはサービスのセキュリティ特権を使用してプロセス制御ネットワーク内のデバイス内で実行されることができる。加えて、マルウェアは、それ自体が局所的に生き残り、ネットワーク化されたデバイスの再起動後に再び実行されることを可能にし得る。場合によっては、マルウェアは、ホスト、例えば感染したアプリケーションまたはサービス、の特権を、アプリケーションまたはサービスが実行されているアカウントの特権を使用して拡大し得、そうすることで、マルウェアは、より高位の特権を要するプロセス制御デバイスまたはネットワーク内で行動または操作を実行することができ得、それ故に、典型的には、制御システム操作にとってより有害である。これらの攻撃がプラント制御システムの継続する動作を妨害するとき、これらの攻撃は、深刻かつ潜在的に破壊的な影響または致命的でさえある影響をプロセスプラント内に与え得る。

【０００８】

したがって、プロセス制御ネットワークを他のプラントネットワークから孤立させてプロセス制御ネットワークの脆弱性を制限することが望ましいが、人員がプロセス制御ネットワークの外部のポイントから（すなわち、プロセス制御ネットワークを保護するファイアウォールの外側から）プロセスプラントデータまたはプロセス制御ネットワークデータにアクセスすることを可能にすることも望ましい、及び時に必要である。そのようなアクセスを可能にするために、プロセス制御システムは時に、プロセス制御システムデータなどを読み取り、そのデータを外部ネットワーク内のクライアントデバイスに送信するように、制御システムネットワーク内のプロセス制御デバイスにコールを出し得るプロセス制御ネットワークのファイアウォール内に配置された外部データアクセスサーバを有する。この外部データサーバは、プロセス制御ネットワークから所望の情報を取得するために、ファイアウォールを介して外部ネットワークからの外部データサーバとインターフェース接続する１つ以上のクライアントアプリケーションを介してアクセス可能であり得る。例として、ＯＰＣ　Ｆｏｕｎｄａｔｉｏｎは、安全なプロセス制御ネットワーク内に位置し、かつそれに接続されるＯＰＣサーバにアクセスするために、プロセス制御ネットワークファイアウォールの外側に位置するクライアントアプリケーションによって使用され得るプログラムインターフェースを定義する一連のＯＰＣ仕様を公表している。これらのインターフェースは、呼び出され得る方法、及びＯＰＣクライアントとＯＰＣサーバとの間で

渡されるパラメータに関して定義される。これらのインターフェースは、典型的には、プラントのプロセス制御ネットワークのファイアウォール内のプロセス制御及び製造自動化システム内のランタイムならびに過去データ及びイベントに対する構成、閲覧、読み取り、書き込み、ならびにコールバックアクセスを提供する。

【０００９】

プロセス制御または製造自動化システムと他の外部（または内部）プラントネットワークとの間の接続を安全にする必要性が高まっているのに伴い、プラント構造は、プラント制御ネットワークと他のプラントシステムとの間にＤＭＺと称されるバッファゾーンをますます提供するようになっている。ＤＭＺは、典型的には、安全な様式で、プロセスプラントネットワーク内で、サーバ、例えばＯＰＣサーバのような外部データサーバとインターフェース接続する任務を負う１つ以上のサーバまたはゲートウェイデバイスを含む。具体的には、これらのシステムにおいて、ＤＭＺの外側に位置するクライアントアプリケーションは、ユーザ認証などに基づいてＯＰＣサーバへのアクセスを提供するＤＭＺゲートウェイデバイスを介して、プロセス制御システムファイアウォール内に位置するＯＰＣサーバにアクセスする。クライアントアプリケーションは、次いで、構成、閲覧、読み取り、書き込み、コールバックなどの要求を、ＤＭＺゲートウェイを介してＯＰＣサーバに送信し、ＯＰＣサーバが、プラントネットワークまたは制御ネットワーク内のデータにアクセスし、そのデータまたは情報を、ＤＭＺゲートウェイを介してクライアントアプリケーションに送信するようにさせる。ＤＭＺの使用は、他のプラントまたは外部ワークステーションと制御システムデバイスとの間の直接接続を防ぐが、ＤＭＺがマルウェアに感染した場合、外部ネットワークからの制御システムへの直接的な接続性を提供することになり得、制御システムが侵害されるのを簡単にすることが経験から示されている。したがって、ＤＭＺは、マルウェア攻撃またはウイルスにさらされるとき、承認された接続を通じて、ＯＰＣサーバを、直接的にクライアントアプリケーションに、または他の外部デバイスに露出するように操作し得、それによってＤＭＺゲートウェイデバイスにより提供されるファイアウォール保護を破り、プロセス制御ネットワークを攻撃または侵害にさらす。

【発明の概要】

【００１０】

１つ以上のファイアウォールを介して、プロセス制御データを外部ネットワークに提供する外部データサーバを有するプロセス制御システムは、外部データサーバが、外部ネットワークに起因するウイルスもしくは他のセキュリティ攻撃によって侵害される能力を減少させるか、または排除する、費用効率の高い安全な機構を実現する。一般的に言うと、プロセス制御ネットワークセキュリティシステムは、プロセス制御ネットワークの外側に配置され、かつ外部ネットワークに接続されるＤＭＺゲートウェイデバイスに通信可能に接続された外部データサーバ（プロセス制御ネットワーク内に位置する）を含む。外部データサーバを構成するために使用される構成エンジンは、プロセスプラントネットワークファイアウォール内に位置し、そのためプロセス制御ネットワークの内側から動作する。構成エンジンは、外部データサーバによってプロセス制御ネットワークから自動的に取得され、かつ外部データサーバによって様々な時点でＤＭＺゲートウェイデバイスに公表されることとなるデータを定義する１つ以上のデータシート、データフォーム、またはデータビューを生成するように外部データサーバを構成する。構成エンジンはまた、公表されたデータビューを受信し、かつこれらのデータビューを、外部ネットワークを介してＤＭＺゲートウェイデバイスに接続された１つ以上のクライアントまたはクライアントアプリケーションに再公表するようにＤＭＺゲートウェイデバイスを構成する。

【００１１】

構成された後、外部データサーバは、データシートまたはデータビューによって指定されたようにプラント内のデータにアクセスし、データシートまたはデータビュー内のデータをＤＭＺゲートウェイデバイスに提供する。ＤＭＺゲートウェイデバイスは次いで、外部ネットワーク上の様々なクライアントアプリケーションと通信し、このクライアントアプリケーションは、ＤＭＺゲートウェイデバイスでデータシートまたはデータビューの様

々なものにサブスクライブする。そうすることで、クライアントアプリケーションは、外部データサーバによってＤＭＺゲートウェイデバイスに提供されるデータシートまたはデータビュー内のデータを自動的に受信するように動作する。クライアントアプリケーションは、ＤＭＺゲートウェイデバイス内の１つ以上のデータシートまたはデータビューをサブスクライブすることができるが、ＤＭＺゲートウェイデバイスは、クライアントアプリケーションからの閲覧、読み取り、書き込み、及び構成コールを無視するか、サポートしないように構成または実装される。さらには、外部データサーバもまた、ＤＭＺゲートウェイデバイスからの閲覧、読み取り、書き込み、及び構成コールを無視するか、サポートしないように構成または実装される。１つの事例では、外部データサーバのファイアウォール側での外部データサーバの読み取り、書き込み、及び構成ポートは、これらのポートを介した外部アクセスを防ぐために、ブロックまたはシャットダウンされる。このようにして、ＤＭＺゲートウェイデバイスは、プラント制御ネットワーク内から構成されるデータシートまたはデータビューに従って外部データサーバによって提供されるデータ以外は、外部データサーバを介してデータにアクセスすることはできない。結果として、たとえＤＭＺゲートウェイデバイスがウイルス攻撃にさらされたり、または権限のない者によってアクセスされたとしても、ＤＭＺゲートウェイデバイスは、外部データサーバを介して制御システムに要求を出す直接的な能力を有しないので、ウイルスまたは権限のない者は、ＤＭＺゲートウェイデバイスを使用して外部データサーバを介して制御システムまたはプロセス制御ネットワークへのアクセスを得ることはできない。

【００１２】

これらのセキュリティ機構の使用は、これらのセキュリティ機構が、感染したまたは侵害されたＤＭＺゲートウェイデバイスが、外部データサーバを介してプロセス制御システムへのアクセスを得ること、及び感染したまたは侵害された外部クライアントアプリケーションがＤＭＺゲートウェイデバイスへのアクセスを得ることを、不可能でないにしても、困難にするので、ゼロデイウイルス攻撃などのウイルス攻撃及び他のマルウェアの影響を受けにくいプロセス制御システムまたはプロセスプラント内のソフトウェア及び通信環境をもたらす。

【図面の簡単な説明】

【００１３】

【図１】１つ以上のオペレータ及び保守ワークステーション、サーバ、コントローラ、フィールドデバイスを含み、かつ外部ネットワークから制御システムへの安全な外部アクセスを提供するように構成された外部データサーバを含む、分散型プロセス制御システム及びプロセス自動化ネットワークを有するプロセスプラントの例示的な図である。

【図２】図１のものなどのプロセス制御ネットワーク内の外部データサーバと、ＤＭＺゲートウェイデバイスと、本明細書に記載される安全な構成を使用してＤＭＺゲートウェイを介して外部データサーバからのデータにアクセスする１つ以上のクライアントデバイスとの間の通信接続の例示的なブロック図である。

【発明を実施するための形態】

【００１４】

図１は、プロセス制御ネットワーク１０（図１の点線内側に示される）及び１つ以上の他のプラントネットワーク（図１の点線外側に示される）を含む、プロセスプラント５の略図である。プロセス制御ネットワーク１０は、例えば、本明細書に記載されるセキュリティ機能を実施してプロセス制御ネットワーク１０内のプロセス制御システム情報への安全な外部アクセスを促進するために様々なコンピュータデバイスが使用され得る、プロセスプラント内に配置され得る。図１に例証されるように、プロセス制御ネットワーク１０は、プロセス制御データバス９を介して、データまたはイベントヒストリアン１２、及びそれぞれがディスプレイ画面１４を有する１つ以上のホストワークステーションまたはコンピュータ１３（パーソナルコンピュータ、ワークステーションなどの任意の種類であり得る）に接続されたプロセスコントローラ１１を含む。データまたはイベントヒストリアン１２は、データ保存のために、任意の所望の種類のメモリ、及び任意の所望もしくは既

知のソフトウェア、ハードウェア、またはファームウェアを有する、任意の所望の種類のデータ収集ユニットであり得る。例えば、データバス９は、例えばイーサネット通信リンクとして実装されるローカルエリアネットワークなどの安全な通信ネットワークであり得る。コントローラ１１もまた、入力／出力（Ｉ／Ｏ）カード２６及び２８、ならびにプロセス制御フィールドデバイスネットワーク、またはラインを介して、フィールドデバイス１５～２２に接続される。コントローラ１１は、図１内において、ハードワイヤード通信ネットワーク及び通信スキームを使用して、フィールドデバイス１５～２２に通信可能に接続される。

【００１５】

一般的に、フィールドデバイス１５～２２は、センサ、バルブ、トランスミッタ、ポジショナなどの任意の種類の制御デバイスであり得、Ｉ／Ｏカード２６及び２８は、例えば、４－２０ｍａプロトコル、ＨＡＲＴ（登録商標）プロトコル、ＦＯＵＮＤＡＴＩＯＮ（登録商標）フィールドバスプロトコルなどを含む、任意の所望の通信またはコントローラプロトコルに準拠する任意の種類のＩ／Ｏデバイスであり得る。コントローラ１１は、メモリ２４に保存される１つ以上のプロセス制御ルーチン（または、任意のモジュール、ブロック、もしくはそれらのサブルーチン）を実施または監督するプロセッサ２３を含み、かつコントローラ１１は、デバイス１５～２２、ホストコンピュータ１３、及びデータまたはイベントヒストリアン１２と通信して、任意の所望の様式でプロセスを制御する。さらには、一例において、コントローラ１１は、機能ブロックと一般に称されるものを使用して１つ以上の制御戦略またはスキームを実施し得、各機能ブロックは、プロセス制御ネットワーク１０内にプロセス制御ループを実施するために他の機能ブロックと共に操作する（リンクと呼ばれる通信を介して）総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）である。機能ブロックは、典型的には、トランスミッタ、センサ、もしくは他のプロセスパラメータ測定デバイスと関連するものなどの入力機能、ＰＩＤ、ＭＰＣ、ファジーロジックなどを実行する制御ルーチンと関連するものなどの制御機能、制御技術、またはバルブなどのいくつかのデバイスの操作を制御する出力機能、のうちの１つを実行して、プロセス制御ネットワーク１０を使用して実施されるプロセスプラントまたはプロセス制御システム内のいくつかの物理的機能を実行する。当然ながら、ハイブリッド及び他の種類の機能ブロックが存在し、図１のプロセスプラント例内で利用され得る。機能ブロックは、任意の所望または既知の様式で、コントローラ１１または他のデバイス内に保存され得、かつそれらによって実行され得る。

【００１６】

図１の分解図ブロック３０によって例証されるように、コントローラ１１は、制御ルーチン３２及び３４として例証されるいくつかの単一ループ制御ルーチンを含んでもよく、所望の場合、制御ループ３６として例証される１つ以上の高度制御ループを実施してもよい。そのような制御ループはそれぞれ、典型的には、制御モジュールと称される。単一ループ制御ルーチン３２及び３４は、バルブなどのプロセス制御デバイス、温度及び圧力トランスミッタなどの測定デバイス、またはプロセス制御システム１０内の任意の他のデバイスと関連し得る、適切なアナログ入力（ＡＩ）及びアナログ出力（ＡＯ）機能ブロックに接続された単一入力／単一出力ファジーロジック制御ブロック、及び単一入力／単一出力ＰＩＤ制御ブロックをそれぞれ使用して、単一ループ制御を実行するとして例証される。高度制御ループ３６は、１つ以上のＡＩ機能ブロックに通信可能に接続された入力、及び１つ以上のＡＯ機能ブロックに通信可能に接続された出力を有する高度制御ブロック３８を含むとして例証されるが、高度制御ブロック３８の入力及び出力を任意の他の所望の機能ブロックまたは制御要素に接続して、他の種類の入力を受信、及び他の種類の制御出力を提供してもよい。高度制御ブロック３８は、任意の種類の多重入力、多重出力制御スキームを実施してもよく、及び／または、プロセスモデルベースの制御ルーチンを実施してもよく、したがって、モデル予測制御（ＭＰＣ）ブロック、ニューラルネットワークモデリングまたは制御ブロック、多変数ファジーロジック制御ブロック、リアルタイムオプティマイザブロックなどを構成し得るか、または含み得る。

【００１７】
高度制御ブロック３８を含む、図１に例証される機能ブロックは、スタンドアローンのコントローラ１１によって実行され得ること、または代替的に、ワークステーション１３のうちの１つ、もしくはフィールドデバイス１９～２２のうちの１つなど、任意の他のプロセッシングデバイスもしくはプロセス制御システム１０の制御要素内に位置し、それによって実行され得ることが理解されよう。例として、それぞれトランスミッタ及びバルブであり得るフィールドデバイス２１及び２２は、制御ルーチンを実施するための制御要素を実行し得、したがって、１つ以上の機能ブロックなど、制御ルーチンの部分を実行するためのプロセッシング、及び他の構成要素を含み得る。より具体的には、フィールドデバイス２１は、図１に例証されるように、アナログ入力ブロックに関連するロジック及びデータを保存するためのメモリ３９Ａを有し得、フィールドデバイス２２は、ＰＩＤ、ＭＰＣ、またはアナログ出力（ＡＯ）ブロックと通信している他の制御ブロックに関連するロジック及びデータを保存するためのメモリ３９Ｂを有するアクチュエータを含み得る。

【００１８】
さらには、図１に例証される制御システム１０は、コントローラ１１に、及び可能性として互いに、無線で通信可能に連結された、いくつかのフィールドデバイス６０～６４及び７１を含む。図１に例証されるように、無線で接続されたフィールドデバイス６０は、アンテナ６５に通信可能に接続され、アンテナ７４と無線で通信するように協同して、次いでアンテナ７４は、コントローラ１１に接続された無線Ｉ／Ｏデバイス６８に連結される。さらには、フィールドデバイス６１～６４は、有線‐無線変換ユニット６６に接続され、有線‐無線変換ユニット６６は次いで、アンテナ６７に通信可能に接続される。フィールドデバイス６１～６４は、さらなる無線Ｉ／Ｏデバイス７０に接続されたアンテナ７３と、アンテナ６７を通じて無線で通信し、さらなる無線Ｉ／Ｏデバイス７０はコントローラ１１にも接続される。図１にさらに例証されるように、フィールドデバイス７１は、アンテナ７３及び７４のうちの１つまたは両方と通信するアンテナ７２を含み、それによってＩ／Ｏデバイス６８及び／または７０と通信する。Ｉ／Ｏデバイス６８及び７０は、次いで、有線バックプレーン接続（図１に示されない）を介して、コントローラ１１に通信可能に接続される。この場合、フィールドデバイス１５～２２は、Ｉ／Ｏデバイス２６及び２８を介して、コントローラ１１にハードワイヤードされたままである。

【００１９】
図１のプロセス制御システム１０は、追加として、任意の所望の様式で、トランスミッタ６０～６４、またはフィールドデバイス７１などの他の制御要素によって、測定、感知、または計算されたデータの無線伝送を使用または組み込み得る。図１の制御システム１０において、新しいプロセス変数測定値または他の信号値は、予定に従ってもしくは定期的に、または特定の条件が満たされたときなど、非定期的もしくは間欠的に、デバイス６０～６４及び７１によってコントローラ１１に伝送され得る。例えば、新しいプロセス変数測定値は、プロセス変数値が、デバイスによりコントローラ１１に送信された最後のプロセス変数測定値に対して所定量だけ変化するとき、または典型的にはコントローラ１１のスキャン速度よりもだいぶ遅い予め定義された更新レートあたり少なくとも１回、コントローラ１１に送信され得る。当然ながら、プロセス変数測定値を非定期的様式でいつ送信するかを決定する他の様式が、同様に、または代わりに実施され得る。

【００２０】
理解されるように、図１のトランスミッタ６０～６４のそれぞれは、それぞれのプロセス変数（例えば、フロー、圧力、温度、またはレベル信号）を示す信号も、１つ以上の制御ループもしくはルーチンにおける使用のため、または監視ルーチンにおける使用のためにコントローラ１１に伝送し得る。フィールドデバイス７１などの他の無線デバイスは、プロセス制御信号を無線で受信し得、かつ／または、任意の他のプロセスパラメータを示す他の信号を伝送するように構成され得る。図１の無線デバイスは、入力／出力デバイス６８及び７０を介してコントローラ１１に接続されているとして例証されるが、それらは、代わりに、データバス９に接続されたゲートウェイを介して、または任意の他の様式で

、コントローラ１１または任意の他のコントローラに接続され得る。さらには、理解されるように、コントローラ１１によって収集されたか、またはそれが利用可能になったデータのうちのいずれも、プロセス制御ネットワーク１０に関連するデータバス９を介して、ワークステーション１３及び／またはデータもしくはイベントヒストリアン１２に利用可能になり得るか、それらに保存され得るか、それらによって使用され得る。

【００２１】

図１に例証されるように、プロセス制御ネットワーク１０は、データバス９に通信可能に接続され、かつそれ故にプロセス制御ネットワーク１０内に配置された外部データサーバ１００を含む。周知のＯＰＣプロトコルまたは標準に準拠するＯＰＣサーバであり得る外部データサーバ１００は、１つ以上のＤＭＺゲートウェイデバイス１０６を有するＤＭＺを介して第２の通信ネットワーク１０２に接続される。第２の通信ネットワーク１０２は、例えば、ＴＣＰ通信を実装するイーサネット通信接続などのさらなるプラントネットワークであり得るか、例えば、公衆またはオープンネットワークへのインターネット接続であり得るか、またはプロセス制御ネットワーク１０から分離した任意の他の種類の外部通信もしくはコンピュータネットワークであり得る。

【００２２】

外部データサーバ１００に接続されたＤＭＺゲートウェイデバイス１０６は、承認されたデータフローのみを許可する任意の種類のファイアウォールであり得、かつ介入セキュリティ機能などの他のセキュリティ機能も実行し得る１つ以上の内部または外部ファイアウォール１０８によって保護される。図１の例において、外部データサーバ１００に接続されたＤＭＺゲートウェイデバイス１０６は、外部データサーバ１００に接続されたゲートウェイデバイス１０６の入力にバックエンドファイアウォール１０８、及びデータバス（または他の通信接続）１０２に接続されたゲートウェイデバイス１０６の入力にフロントエンドファイアウォール１０８を含む。当然ながら、バスまたは通信接続９及び１０２は、有線接続として例証されるが、これらの通信接続は、代わりに、または追加で、無線接続及び無線通信デバイス（例えば、無線イーサネット、ＷｉＦｉインターネット接続など）、または有線及び無線両方の通信及びデバイスの組み合わせを使用して実現され得ることが理解されよう。依然としてさらに、図１に例証されるように、様々なクライアントデバイス１１２内で実行される複数のクライアントアプリケーション１１０は、ＤＭＺゲートウェイデバイス１０６に接続され得、かつＤＭＺゲートウェイデバイス１０６と通信して安全な様式でプロセス制御ネットワーク１０から情報を取得し得る。

【００２３】

依然としてさらに、図１に例証されるように、構成アプリケーション（リソースマネージャとも呼ばれる）１１５は、プロセス制御ネットワーク１０内のプロセッシングデバイスのうちの１つ、例えば、ワークステーション１３のうちの１つ内に配置される。構成アプリケーション１１５は、コンピュータまたは持続性コンピュータ可読メモリ１１６に保存され、下により詳細に記載されるように、外部データサーバ１００、及びある程度まではＤＭＺゲートウェイデバイス１０６を構成するため、ワークステーション１３のプロセッサ１１７上で実行される。

【００２４】

一般的に言うと、動作中、外部データサーバ１００は、プロセス制御ネットワーク１０内のデバイスから（例えば、データまたはイベントヒストリアン１２、コントローラ１１、ワークステーション１３、フィールドデバイス１５～２２、６０～６４、及び７１などから）データバス９を介して情報を取得するように、プロセス制御ネットワーク１０内から構成され、たとえＤＭＺゲートウェイデバイス１０６が、ファイアウォール１０８を破るまたは侵害するマルウェアに攻撃されたとしても、この情報を外部ネットワーク１０２上のクライアントデバイス１１２内の１つ以上のクライアントアプリケーション１１０に安全な様式で提供する。一般的に言うと、外部データサーバ１００とクライアントデバイス１１２内の１つ以上のクライアントアプリケーション１１０との間に安全な通信接続を実現するために、外部データサーバ１００は、ＤＭＺゲートウェイデバイス１０６に事前

設定された種類または量のプロセス制御データ（「データビュー」またはデータフォームとも呼ばれる）をプロセス制御ネットワーク１０から、またはその中で取得されたデータと共に公表するように設定または構成される。この場合、データビュー内のデータは次いで、ＤＭＺゲートウェイデバイス１０６に保存され、ＤＭＺゲートウェイデバイス１０６によって、データビューのうちのいずれかまたは全てをサブスクライブし得るクライアントデバイス１１２内のクライアントアプリケーション１１０に提供される。さらには、この構成の一部として、外部データサーバ１００は、事前に設定されたまたは事前に決められたデータビューに従って（によって定義されるように）データをＤＭＺゲートウェイデバイス１０６に公表することのみでき、かつゲートウェイデバイス１０６から受信された読み取りもしくは書き込み要求（コマンド）を受容または実行すること、またはＤＭＺゲートウェイデバイス１０６から構成されることができないように構成される。したがって、１つの事例では、外部データサーバ１００の読み取り、書き込み、及び構成エンドポイントまたはポート（サーバ１００のＤＭＺゲートウェイ側）は、外部データサーバ１００がＤＭＺゲートウェイデバイス１０６によって提供される読み取り、書き込み、もしくは構成要求を受容する、またはそれに応答することができないように、無効にされる。重要なことには、外部データサーバ１００のための構成アプリケーションまたは構成エンジン１１５は、外部データサーバ１００自体、ワークステーション１３のうちの１つ、またはプロセスプラントネットワーク１０内に接続されている他のコンピュータもしくはサーバ内など、プロセス制御ネットワーク１０内に位置する。したがって、外部データサーバ構成アプリケーション１１５は、プロセス制御ネットワーク１０内のワークステーション１３のうちの１つ内に位置しているとして図１に例証されるが、それは、代わりに、データバス９またはプロセス制御ネットワーク１０内の他の接続を介して外部データサーバ１００に接続された任意の他のプロセッシングデバイス内に位置し得る。このようにして、外部データサーバ１００は、プロセス制御ネットワーク１０内からのみ構成されることができる。

【００２５】

さらなる例として、図２は、プロセス制御ネットワーク内に配置された構成アプリケーション２１５、外部データサーバ２００（この場合はＯＰＣ．ＮＥＴデータサーバであるとして例証される）、プロセス制御ネットワークの外側に配置された１つ以上のＤＭＺゲートウェイデバイス２０６、及びこれもまたプロセス制御ネットワークの外側に配置されるが、外部通信ネットワークを介してＤＭＺゲートウェイデバイス２０６に接続された１つ以上のクライアントデバイス内の１つ以上のクライアントアプリケーション２１０を使用して実現され得る通信フロー図を例証する。具体的には、図２のシステム例において例証されるように、図１の構成エンジン１１５であり得る構成エンジン２１５は、標準ＯＰＣ．ＮＥＴリソースマネージャまたは構成エンジンとして実装され、ＯＰＣ．ＮＥＴサーバとして例証される外部データサーバ２００と共に、プロセッサ及びメモリを有するサーバデバイスなどの、プロセス制御ネットワーク内の同じコンピューティングまたはプロセッシングデバイス内に配置される。ＯＰＣ．ＮＥＴサーバ２００は、クライアントデバイス内に実装されたＯＰＣ．ＮＥＴクライアント２１０へのアクセスを提供する既製の標準ＯＰＣ．ＮＥＴサーバであり得る。そのようなサーバは、サーバ２００へのＴＣＰ通信及びサーバ２００からのＴＣＰ通信を制御するＷＣＦエンドポイントとして本質的に実装されている、読み取りエンドポイント、書き込みエンドポイント、構成エンドポイント、及び公表エンドポイントを含む４つのポートまたは論理エンドポイントを有し得る。既知のように、読み取りエンドポイントは、読み取り要求を受容してプロセス制御ネットワーク１０内で読み取りを実行し、書き込みエンドポイントは、書き込み要求を（例えばＤＭＺゲートウェイデバイスから）受容してプロセス制御ネットワーク１０内で書き込みを実行し、構成エンドポイントは、閲覧要求をサポートし、かつ外部データサーバ２００がＯＰＣ．ＮＥＴリソースマネージャ２１５などの構成エンジンによって構成されることも可能にし、公表エンドポイントは、外部データサーバ２００が規則的または定期的または他の事前に構成された様式でデータを公表することを可能にする。当然ながら、読み取り、書

き込み、構成、及び公表エンドポイントを、任意の所望の様式で、データサーバ２００内で設定または確立することができ、例えば、要求、ポート、論理的または物理的エンドポイントなどとして実装することができる。しかしながら、図２のサーバ２００では、読み取り及び書き込みエンドポイントは、サーバ２００のオンサイト初期化（構成）を通じて（例えば、構成エンジン２１５によって）無効にされるが、構成エンドポイントは、構成エンジン２１５によってプロセス制御ネットワーク１０内でのみアクセス可能である。

【００２６】

より具体的には、この例ではＯＰＣ．ＮＥＴ　ＤＭＺリソースマネージャである構成エンジン２１５は、データまたはイベント／アラームまたは他のプロセスプラントデータを含む１つ以上の「データビュー」を公表するようにＯＰＣ．ＮＥＴサーバ２００を構成する。そのようなデータビューは、外部データサーバ２００に保存されたビュー２２０として図２に例証される。各データビュー２２０の定義は、設置の必要性に合わせてカスタマイズされ得、それは多くの場合、フェイスプレートまたはアラームリストなどの、ワークステーションディスプレイ上に示されるデータ／イベント／アラームを反映する。当然ながら、データビュー２２０を、図１のプロセス制御ネットワーク１０内のデータもしくはイベントヒストリアン１２（図１）、コントローラ１１、フィールドデバイス、または他のデバイス１５～２２及び６０～７２、ワークステーション１３などからの任意のプロセス制御情報などの、プロセス制御ネットワーク１０内からの任意の所望のプロセス制御情報を提供するように構成または設定することができる。そのようなプロセス制御情報は、制御情報、デバイス情報、保守情報、構成情報などを含み得るが、それらに限定されない。より具体的には、制御情報は、フロー、圧力、レベル、温度などの、測定された、シミュレーションされた、または別途決定されたプロセス変数情報を含み得る。そのような情報は、制御信号、コントローラ構成及びチューニング変数、制御設定、アラーム及びアラートなども含み得る。依然としてさらに、デバイス情報は、デバイス名、製造業者、シリアル番号、タグ、較正情報、またはデバイスに関する任意の他の情報を含み得る。保守情報は、デバイスまたは制御ルーチン較正情報、修理情報、デバイスアラームまたはアラート、ユーザまたは保守ログなどを含み得る。同様に、構成情報は、制御及びプラント階層、フロー図、配管計装図（ＰＩ＆Ｄｓ）などの項目のためのデバイス及び／または制御構成情報を含み得る。当然ながら、プロセス制御情報は、図１のプロセス制御ネットワーク１０に関して例証または記載された制御ルーチン、機能ブロック、デバイス、通信などに関する任意の情報であり得る。

【００２７】

いずれにせよ、一旦データビュー２２０が外部データサーバ２００内で構成されると、ＯＰＣ．ＮＥＴサーバ２００は、これらのデータビュー２２０に従って、またはそれらによって定義されるように、データを１つ以上のＯＰＣ．ＮＥＴ　ＤＭＺゲートウェイ２０６に公表する。この場合、サーバ２００は、データビュー２２０によって記載または定義されたデータをプロセス制御ネットワーク１０からアクセスまたは取得し、このデータを、データビュー２２０によって指定された、またはそれに関連するフォーマットを使用してゲートウェイデバイス（複数可）２０６に公表する。加えて、サーバ２００上のプロパティは、ＯＰＣ．ＮＥＴ　ＤＭＺゲートウェイ（複数可）２０６をデータビュー２２０によって定義された公表されたデータを受信することになる唯一の承認されたリモートアプリケーション（複数可）として（プロセス制御ネットワーク１０の外側で）識別するように、サーバ初期化中に構成エンジン２１５によって設定され得る。

【００２８】

依然としてさらに、ＯＰＣ．ＮＥＴ　ＤＭＺゲートウェイ２０６がＯＰＣ．ＮＥＴ要求を使用して公表されたデータを受信することを許可するために、ＯＰＣ．ＮＥＴ　ＤＭＺリソースマネージャ（すなわち、構成エンジン２１５）は、データビュー２２０のセット（１つ以上）のための構成識別子を含み、各データビュー及びそのデータ項目／イベント／アラームを記述もするファイルをエクスポートする。そのようなファイルは、ファイル２２２として図２に例証される。１つを超えるデータビューのセットが要求される場合、

ＯＰＣ．ＮＥＴ　ＤＭＺリソースマネージャ２１５は、追加の構成を作成し得、それもまたＤＭＺゲートウェイデバイス（複数可）２０６内のファイルにエクスポートする。ゲートウェイデバイス２０６のうちの異なるものが、データビュー２２０のうちの同じまたは異なるものを受信またはサブスクライブするように構成され得、したがって各ゲートウェイデバイス２０６が、データビュー２２０の総セットのサブセットに対応するファイル２２２のその独自のセットを有し得ることが理解されよう。

【００２９】

当然ながら、エクスポートされたデータビューファイル２２２は、安全な機構を通じてＯＰＣ．ＮＥＴ　ＤＭＺゲートウェイデバイス２０６に利用可能になり、その機構は、ＯＰＣ．ＮＥＴサーバ２００によって公表されたデータを受信及び解釈するためにＯＰＣ．ＮＥＴ　ＤＭＺゲートウェイ２０６が使用する。１つを超えるＯＰＣ．ＮＥＴ　ＤＭＺゲートウェイ２０６が存在する場合、各エクスポートされた構成ファイルを、任意に、特定のＯＰＣ．ＮＥＴ　ＤＭＺゲートウェイ２０６のみに安全に配布することができ、それ故に制御システムデータ／イベント／アラームへのアクセスをさらに制限する。いずれにせよ、理解されるように、構成エンジン２１５、すなわち、ＯＰＣ．ＮＥＴ　ＤＭＺリソースマネージャは、１つ以上の事前に設定されたまたは事前に決められたデータビューを特定のＤＭＺゲートウェイデバイス２０６に公表することのみできるようにＯＰＣサーバ２００を構成し、また、プロセス制御ネットワーク１０から取得された事前に設定されたまたは事前に決められたデータを含むようにデータビュー２２０を構成する。リソースマネージャまたは構成エンジン２１５はまた、データビュー２２０内のデータの概要を含むエクスポートされたデータビューファイル２２２をゲートウェイデバイス２０６に提供し、最終のクライアントデバイスまたはクライアントデバイス内のクライアントアプリケーション２１０がデータビュー２２０内のプロセス制御データを表示または使用することを可能にする。

【００３０】

構成または設定中、各ＯＰＣ．ＮＥＴゲートウェイデバイス２０６は、そのデータビューファイル２２２を再公表し、データビュー２２２内の公表されたデータ／イベント／アラームを受信及び解釈するために様々なＯＰＣ．ＮＥＴ　ＤＭＺサブスクライバ（すなわち、クライアントアプリケーション２１０）によって使用されることとなる同様のエクスポートファイルを作成する。このようにして、ＯＰＣ．ＮＥＴ　ＤＭＺサブスクライバ２１０は、ＯＰＣ．ＮＥＴ　ＤＭＺゲートウェイデバイス２０６に感染する限られた能力を有する。同様に、たとえ感染したとしても、ゲートウェイデバイス２０６は、サーバ２００に対する読み取り及び書き込みなどの要求（コマンド）を発行することができないので、及びサーバ２００に関する任意の構成動作を実行することができないので、ＯＰＣ．ＮＥＴ　ＤＭＺゲートウェイデバイス２０６が、ＯＰＣ．ＮＥＴサーバ２００に感染する見込みはほとんどない。

【００３１】

したがって、構成されたとおり、外部データサーバ２００は、構成エンジン（プロセス制御ネットワーク１０内）にローカルで応答すること、及びデータを外部デバイス（すなわち、プロセス制御ネットワークの外側のデバイスまたは外部ネットワーク１０２上のデバイス）のみに公表することだけができる。したがって、外部データサーバ２００は、外部で生成された読み取り及び書き込みコマンドを受信する能力を有さず、したがってこれらのコマンドを使用したＤＭＺゲートウェイデバイス２０６内でのマルウェアによる攻撃または他のプロセスにさらされることはない。さらには、従来のＯＰＣ．ＮＥＴクライアントは、プロセス制御ネットワーク１０内に実装されるＤＭＺリソースマネージャまたは構成エンジン２１５、及びプロセス制御ネットワーク１０の外側に実装されるＯＰＣ．ＮＥＴ　ＤＭＺゲートウェイ２０６を含む２つの別個のエンティティに分離されるため、外部データサーバ２００は、保護されるか、またはより安全である。依然としてさらに、この構成設定は、ＯＰＣ．ＮＥＴ　ＤＭＺゲートウェイデバイス２０６がＯＰＣ．ＮＥＴリソース管理（構成）、読み取り、及び書き込み要求をＯＰＣ．ＮＥＴサーバ２００に送信

する能力を除去し、それによってＯＰＣ．ＮＥＴサーバ２００の攻撃表面を減少させる。さらには、この構成は、ＯＰＣ．ＮＥＴ　ＤＭＺゲートウェイデバイス２０６が、ＯＰＣ．ＮＥＴサーバ２００への典型的なＯＰＣクライアント／サーバ接続を確立することなく、ＯＰＣ．ＮＥＴデータ／イベント／アラームをＯＰＣ．ＮＥＴサーバ２００から受信することを可能にする。代わりに、ＯＰＣ．ＮＥＴ　ＤＭＺゲートウェイデバイス２０６は、リソースマネージャ２１５によってまたはそれを使用して作成されたデータビューによって予め定義されている公表されたデータを受信することだけができる。同様の様式で、クライアントアプリケーション２１０もまた、ＯＰＣ．ＮＥＴゲートウェイデバイス２０６によって公表されたデータビューのみを受信することに制限されるため、この構成は、ＯＰＣ．ＮＥＴ　ＤＭＺサブスクライバまたはクライアント２１０が、ＯＰＣ．ＮＥＴリソース管理（構成）、読み取り、及び書き込み要求をＯＰＣ．ＮＥＴ　ＤＭＺゲートウェイ２０６に送信する能力を除去する。実際、この構成において、ＯＰＣ　ＮＥＴ　ＤＭＺサブスクライバまたはクライアント２１０は、ゲートウェイ２０６によるデータビューの公表を介して、及びＯＰＣ．ＮＥＴ　ＤＭＺゲートウェイデバイス２０６への典型的なＯＰＣクライアント／サーバ接続を確立することなく、ＯＰＣ．ＮＥＴ　ＤＭＺゲートウェイデバイス２０６からＯＰＣ．ＮＥＴデータ／イベント／アラームを受信することだけができる。結果として、この構成では、３つの協調した、しかし別個の層のアクセス保護が実現されて制御システムデータ／イベント／アラームを保護する。

【００３２】

所望の場合、構成エンジン２１５（またはリソースマネージャ）は、データビューの多重構成を提供することによって、及び多重ＤＭＺゲートウェイ２０６の使用を通じて、アクセスの粒度を可能にさせる、またはそれをデータビューに提供してもよい。この場合、各ゲートウェイデバイス２０６は、１つ以上の特定のデータビューを受信し（サブスクライブし）、かつ再公表するように構成され得る。クライアントデバイス内のクライアントアプリケーション２１０は、次いで、特定のゲートウェイデバイス２０６によって公表されるような再公表されたデータビューの全てをサブスクライブし得（受信するように構成され得）、または特定のゲートウェイ２０６の特定のデータビューを受信する。この機能は、各クライアントアプリケーション２１０が、クライアントアプリケーション２１０が受信または使用を望む（例えば、ユーザに対するディスプレイ、何らかの様式におけるプロセスなど）特定のプロセス制御データ（利用可能なデータビューによって定義される）を選択することを可能にする。

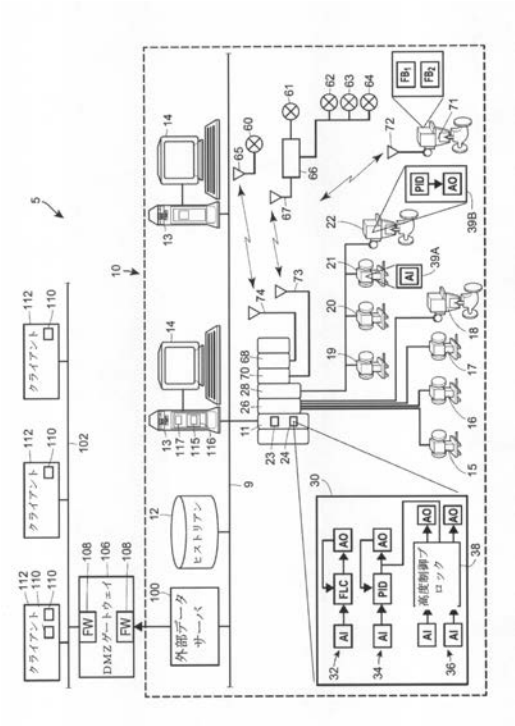
【００３３】

本明細書に記載されるセキュリティ技術は、イーサネット、ならびにフィールドバス、ＨＡＲＴ、及び標準４－２０ｍａプロトコルなどの様々な既知のプロセス制御プロトコルを使用して、ネットワーク化されたプロセス制御デバイス及びシステムと共に使用されると記載されているが、本明細書に記載されるセキュリティ技術を、当然ながら、任意の他のプロセス制御通信プロトコル、またはプログラミング環境を使用して任意の種類の制御デバイス内に実現することができ、かつ任意の他の種類のデバイス、機能ブロック、またはコントローラと共に使用してもよい。本明細書に記載されるセキュリティ機能は、好ましくは、ソフトウェアで実現されるが、それらを、ハードウェア、ファームウェア内などで実現してもよく、かつコンピュータデバイスに関連する任意の他のプロセッサによって実行してもよい。したがって、所望の場合は、本明細書に記載される方法を、標準多目的ＣＰＵ内に、または特別に設計されたハードウェアまたはファームウェア上、例えば、ＡＳＩＣなどで、実施してもよい。ソフトウェアで実施されるとき、ソフトウェアは、磁気ディスク、レーザディスク、光学ディスク、または他の保存媒体上、コンピュータもしくはプロセッサなどのＲＡＭもしくはＲＯＭ内等、任意のコンピュータ可読メモリに保存され得る。同様に、このソフトウェアは、例えば、コンピュータ可読ディスク、または他の可搬コンピュータストレージ機構上を含む、任意の既知または所望の送達方法を介して、ユーザまたはプロセス制御システムに送達され得るか、電話線、インターネットなどの通信チャネルを介して変調され得る。

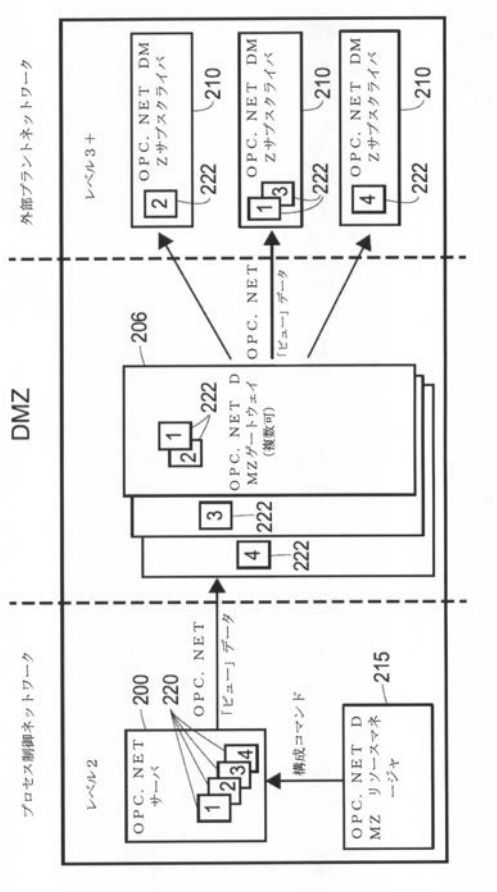
【００３４】

したがって、本発明は特定の実施例を参照して記載したが、それらは例証のみを目的とし、本発明を制限するものではなく、当業者にとっては、本発明の趣旨及び範囲から逸脱することなく開示された実施形態に変更、追加、削除が加えられ得ることは明らかであろう。

【図１】



【図２】



フロントページの続き

(72)発明者　ダン　エイチ.　ウジン
アメリカ合衆国　７８６２６　テキサス州　ジョージタウン　クレスティド　ビュート　ウェイ　１５０２

Ｆターム(参考) 5H220 AA01 BB09 CC07 CC09 CX05 JJ12 JJ17
5K030 GA15 HD03 LC13 LD20
5K033 AA08 AA09 BA08 DB18