

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7586674号
(P7586674)

(45)発行日 令和6年11月19日(2024.11.19)

(24)登録日 令和6年11月11日(2024.11.11)

(51)国際特許分類

F I

G 0 6 F 21/33 (2013.01)

G 0 6 F 21/31 (2013.01)

G 0 6 F 21/44 (2013.01)

G 0 6 F 21/33

G 0 6 F 21/31

G 0 6 F 21/44

請求項の数 9 外国語出願 (全24頁)

(21)出願番号	特願2020-156316(P2020-156316)	(73)特許権者	512132022
(22)出願日	令和2年9月17日(2020.9.17)		フィッシャー・ローズマウント システ
(65)公開番号	特開2021-51740(P2021-51740A)		ムズ, インコーポレイテッド
(43)公開日	令和3年4月1日(2021.4.1)		アメリカ合衆国 テキサス 7 8 6 8 1 -
審査請求日	令和5年5月30日(2023.5.30)		7 4 3 0 ラウンド ロック ウェスト ル
(31)優先権主張番号	62/904,352		イス ヘナ ブルバード 1 1 0 0 ビルデ
(32)優先日	令和1年9月23日(2019.9.23)		イング 1 エマーソン プロセス マネー
(33)優先権主張国・地域又は機関	米国(US)	(74)代理人	100096091
			弁理士 井上 誠一
		(72)発明者	フェデリコ・ホセ・ゲレロ・アラゴン
			フィリピン共和国 パラニャーケ 1 7 0
			0 メトロ・マニラ サン イシドロ エス
			エーヴィー12 サン ホセ ストリート
			3 0
			最終頁に続く

(54)【発明の名称】 モバイルデバイスによるプロセス制御データのセキュアなオフプレミスアクセス

(57)【特許請求の範囲】

【請求項1】

クラウドベースの認証方法であって、前記方法が、

(1) 製品を製造するためにプロセス制御環境内で動作する複数のプロセス制御フィールドデバイスを制御するプロセスコントローラを含むプロセス制御環境の制御を容易にする、モバイルデバイス上で実行しているプロセス制御アプリケーションと、(2) 前記プロセス制御環境に通信可能に結合されたモバイルサーバとの間でデータを転送するように構成されたリレー要素をクラウドベースのサーバ内でインスタンス化することと、

前記モバイルデバイス上で実行している前記プロセス制御アプリケーションから、第1の中間サービスによってキー保管庫から取り出され、前記プロセス制御アプリケーションに提供される第1のバリデーションキーを前記リレー要素で受信することと、

前記リレー要素において、前記第1のバリデーションキーをアプリケーションバリデーションキーと比較することであって、(i) 前記第1のバリデーションキーが前記アプリケーションバリデーションキーと一致する場合、前記モバイルデバイス上で実行している前記プロセス制御アプリケーションを認証し、(i i) 前記第1のバリデーションキーが前記アプリケーションバリデーションキーと一致しない場合、前記モバイルデバイス上で実行している前記プロセス制御アプリケーションに対する認証を拒否する、比較することと、

前記モバイルサーバから、第2の中間サービスによってキー保管庫から取り出され、前記モバイルサーバに提供される第2のバリデーションキーを前記リレー要素で受信するこ

とと、

前記第2のバリデーションキーが正当である場合、前記モバイルサーバを前記リレー要素で認証することと、

前記プロセス制御アプリケーションおよび前記モバイルサーバの両方が正当であると確認された場合、前記リレー要素を介して、前記モバイルデバイス上で実行している前記プロセス制御アプリケーションと前記モバイルサーバとの間の通信を許可することと、を含む、方法。

【請求項2】

前記第1の中間サービスは、リレーアクセスAPIを含む、請求項1に記載の方法。

【請求項3】

前記モバイルデバイス上で実行している前記プロセス制御アプリケーションのユーザに関連付けられたユーザ名およびパスワードをリレーアクセスAPIで受信することと、

前記リレー要素に関連付けられたURLを前記リレーアクセスAPIで受信することと、

前記ユーザ名およびパスワードに応じて、前記ユーザを前記リレーアクセスAPIで認証することと、

前記ユーザが認証された場合、前記モバイルデバイス上で実行している前記プロセス制御アプリケーションに前記第1のバリデーションキーを提供することと、をさらに含む、請求項1または請求項2に記載の方法。

【請求項4】

前記ユーザ名およびパスワードに応じて前記ユーザを認証することが、

リレーゲートウェイサービスを介して、前記ユーザ名およびパスワードを前記モバイルサーバに送信することと、

前記リレーゲートウェイサービスを介して、前記ユーザが認証されているという表示を前記モバイルサーバから受信することと、を含む、請求項3に記載の方法。

【請求項5】

前記リレー要素を介して、前記モバイルデバイス上で実行している前記プロセス制御アプリケーションと、前記モバイルサーバとの間の通信を許可することが、

前記モバイルデバイス上で実行している前記プロセス制御アプリケーションから1つ以上のプロセス制御コマンドを受信することと、

リレーゲートウェイサービスを介して、前記1つ以上のプロセス制御コマンドを前記モバイルサーバに転送することと、を含む、請求項1から請求項4のいずれかに記載の方法。

【請求項6】

前記リレー要素を介して、前記モバイルデバイス上で実行している前記プロセス制御アプリケーションと、前記モバイルサーバとの間の通信を許可することが、

前記モバイルサーバから、リレーゲートウェイサービスを介して、前記プロセス制御環境からのプロセスデータを受信することと、

前記プロセスデータを前記モバイルデバイス上で実行している前記プロセス制御アプリケーションに転送することと、を含む、請求項1から請求項5のいずれかに記載の方法。

【請求項7】

モバイルデバイス上で実行しているプロセス制御アプリケーションを認証する方法であって、

前記プロセス制御アプリケーションからリレーアクセスAPIに、前記プロセス制御アプリケーションのユーザのユーザ名およびパスワードを送信することと、

前記プロセス制御アプリケーションからリレーアクセスAPIに、クラウドベースのリレー要素に関連付けられたURLを送信することと、

前記ユーザ名およびパスワードに回答して、前記プロセス制御アプリケーションで前記リレーアクセスAPIから、第1のバリデーションキーを受信することと、

前記プロセス制御アプリケーションから前記クラウドベースのリレー要素に、前記第1のバリデーションキーを送信することと、

前記プロセス制御アプリケーションで、前記ユーザが認証されているという前記リレー

10

20

30

40

50

要素からの表示を受信することと、

前記プロセス制御アプリケーションから前記リレー要素に、(i) プロセス制御環境からのプロセス制御データをモバイルサーバから受信するためのリクエスト、および(ii) 前記プロセス制御環境内で制御動作を引き起こすためのプロセス制御コマンド、のうちの一方または両方を送信することと、を含む、方法。

【請求項 8】

前記モバイルサーバから、前記クラウドベースのリレー要素を介して、リアルタイムのプロセス制御データを前記プロセス制御アプリケーションで受信すること、をさらに含む、請求項 7 に記載の方法。

【請求項 9】

前記モバイルサーバから前記プロセス制御データを受信するための前記リクエストを送信することが、

前記モバイルサーバから、前記クラウドベースのリレー要素を介して、受信されるのに利用可能なプロセス制御データのリストを前記プロセス制御アプリケーションで受信することと、

前記プロセス制御データのうちの 1 つ以上の、前記ユーザによる選択を前記プロセス制御アプリケーションで受信することと、

前記プロセス制御アプリケーションから前記モバイルサーバに、前記クラウドベースのリレー要素を介して、前記 1 つ以上のプロセス制御データの前記選択を送信することと、

前記プロセス制御アプリケーションで、前記 1 つ以上のプロセス制御データを受信することと、を含む、請求項 7 または請求項 8 に記載の方法。

【発明の詳細な説明】

【技術分野】

【0001】

本開示は、概して、プロセス制御環境のモバイル監視に関し、特に、プロセスプラント環境の外部でモバイルデバイスをセキュアに認証して、モバイルデバイス上のプロセス制御システムのカスタマイズ可能でリアルタイムの認識を提供するためのシステムおよび方法に関する。

【背景技術】

【0002】

分散型制御システム(DCS)は、化学、石油化学、精製、製薬、食品および飲料、電力、セメント、上下水道、石油およびガス、バルブおよび紙、ならびに鉄鋼を含む様々なプロセス工業において使用され、単一の施設または遠隔地で動作するバッチ、供給バッチ、および連続プロセスを制御するために使用される。プロセスプラントは、通常、アナログバス、デジタルバス、もしくはアナログ/デジタルバスを介して、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含む。様々なデバイスが、集合的に監視、制御、およびデータ収集機能を実行して、プロセス、安全遮断システム、火災およびガス検出システム、機械の健康状態の監視システム、保守システム、意思決定支援、ならびに他のシステムを制御する。

【0003】

フィールドデバイスは、例えば、バルブ、バルブポジショナ、スイッチ、および送信機(例えば、温度、圧力、レベル、および流量センサ)であり得るが、これらは、プロセス環境内に配置され、一般に、バルブの開放または閉鎖、プロセスパラメータの測定などの物理的またはプロセス上の制御機能を実行して、プロセスプラント内またはシステム内で実行している 1 つ以上のプロセスを制御する。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また、制御計算、アラーム機能、およびコントローラ内で一般に実装される他の制御機能も実行し得る。プロセスコントローラも典型的にはプラント環境内に配置され、このプロセスコントローラは、フィールドデバイスによって行われるプロセス測定を示す信号および/またはフィールドデバ

10

20

30

40

50

スに関する他の情報を受信し、例えば、プロセス制御判断を行い、受信した情報に基づき制御信号を生成し、HART（登録商標）、Wireless HART（登録商標）、および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で行わ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実行するコントローラアプリケーションを実行する。コントローラ内の制御モジュールは、通信ラインまたはリンクを経由して、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分の動作を制御する。

【0004】

フィールドデバイスおよびコントローラからの情報は、制御室もしくはより厳しいプラント環境から離れた他の場所に典型的に配置される、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、集中データベース、または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対して、通常、データハイウェイを通じて利用可能になる。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分にわたって集中化される。これらのハードウェアデバイスは、例えば、オペレータが、プロセス制御ルーチンの設定の変更、コントローラもしくはフィールドデバイス内の制御モジュールの動作の修正、プロセスの現在の状態の閲覧、フィールドデバイスおよびコントローラによって生成されたアラームの閲覧、担当者の訓練もしくはプロセス制御ソフトウェアの試験を目的としたプロセスの動作のシミュレーション、構成データベースの保持および更新などの、プロセスの制御および／またはプロセスプラントの動作に関する機能を行うことを可能にし得るアプリケーションを実行する。ハードウェアデバイス、コントローラ、およびフィールドデバイスにより利用されるデータハイウェイは、有線通信パス、無線通信パス、または有線および無線通信パスの組み合わせを含むことができる。

【0005】

例として、Emerson Process Managementによって販売されている、DeltaV（商標）制御システムは、プロセスプラント内の多様な場所に配置された異なるデバイス内に記憶され、異なるデバイスによって実行される複数のアプリケーションを含む。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内に備わる構成アプリケーションは、ユーザによる、プロセス制御モジュールの作成または変更、およびデータハイウェイを経由した、これらのプロセス制御モジュールの、専用分散型コントローラへのダウンロードを可能にする。典型的には、これらの制御モジュールは、通信可能に相互接続された機能ブロックで構成され、これらの機能ブロックは、それに対する入力に基づき制御スキーム内で機能を実行し、出力を制御スキーム内の他の機能ブロックに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。構成アプリケーションはまた、データをオペレータに表示し、かつオペレータがプロセス制御ルーチン内のセットポイントなどの設定値を変更できるようにするための閲覧アプリケーションが使用するオペレータインターフェースを、構成エンジニアが作成または変更することを可能にし得る。各専用コントローラ、および場合によっては、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、それらに割り当てられてダウンロードされた制御モジュールを実行するそれぞれのコントローラアプリケーションを記憶および実行する。閲覧アプリケーションは、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およびデータハイウェイと通信可能に接続された1つ以上のリモートコンピューティングデバイス）上で実行され得、この閲覧アプリケーションは、コントローラアプリケーションからデータハイウェイを経由してデータを受信し、ユーザインターフェースを使用してこのデータをプロセス制御システム設計者、オペレータ、またはユーザに表示して、オペレータのビュー、エンジニアのビュー、技師のビューなどのいくつかの異なるビューのうちのいずれかを提供し得る。データヒストリアンアプリケーションが、典型的には、データハイウェイにわたって提供されたデータの一部または全てを収集および記憶するデータヒストリアンデバイスに記憶され、それによって

10

20

30

40

50

実行される一方で、構成データベースアプリケーションが、現在のプロセス制御ルーチン構成およびそれと関連付けられたデータを記憶するために、データハイウェイに取り付けられたなおさらに離れたコンピュータで実行され得る。代替的に、構成データベースは、構成アプリケーションと同じワークステーション内に配置され得る。

【0006】

多くの分散型プロセス制御システムにおいて、プロセスプラント内の各フィールドデバイスは固有のデバイスタグを割り当てられる。固有のデバイスタグは、対応するフィールドデバイスを参照するための容易な手段を提供する。デバイスタグは、プロセス制御システムの構成中に使用されて、制御モジュール内の機能ブロックへの入力または出力の、それぞれソースまたは行先を特定することができる。各信号タイプには、特定のフォーマットまたは情報のセットが関連付けられており、特定のデバイスのデバイスタグには、特定の信号タイプが関連付けられている場合があり、それによりデバイスタグが機能ブロックの入力または出力と関連付けられている場合、機能ブロックには、その信号に関連付けられているフォーマットおよび情報がわかる。フィールドデバイスが、それと関連付けられた複数の信号を有する場合（例えば、バルブは、圧力および温度の両方を測定し、送信する場合がある）、デバイス信号タグは、そのフィールドデバイスの各信号と関連付けられ得る。

【0007】

様々な理由から、プロセス制御システムのデータへのアクセスは、従来、プロセスプラントプレミスにある間、かつ／またはオペレータワークステーション、コントローラ、データヒストリアン、および他の設備に結合するデータハイウェイに接続されたデバイスを使用する間のみ利用可能であった。セキュリティは、プロセス制御システムに関して特別な関心事であり、したがって、プロセス制御システムのオペレータは、一般に、プロセス制御システムを外部ネットワーク環境（例えば、インターネット）から物理的に分離して、外部の行為者がプロセス制御システムに損害を引き起こし、製品品質もしくは実行の可能性に影響を及ぼし、または知的財産情報にアクセスもしくは盗用する機会を制限または防止する。

【0008】

近年、プロセスプラントを構成するプロセスネットワークおよびデータハイウェイに直接結合していなくても、ユーザがスマートフォンなどのモバイルデバイスを介してプロセス制御システムから情報を閲覧するのを可能にするモバイルソリューションが登場した。このようなモバイルソリューションの1つに、Emerson Process Management社からのDelta V（商標）モバイルアプリケーションがある。このようなソリューションは、ユーザが、プロセスプラントの内部および外部の両方からリアルタイムでプロセスプラントから様々なデータにアクセスするのを可能にすることができるが、少なくともプロセス制御環境の複雑な状況下では適切な認証プロセスが実現されていないという理由から、実際には、プロセスプラントの外部からそのようなデータにアクセスすることは、厳格に制限されているか、かつ／またはプロセスプラントからモバイルデバイス（複数可）への情報の単一方向通信に限定され、その結果、プロセス制御環境への悪意のある攻撃および／またはコマンドの進入を防止してきた。すなわち、以前のシステムでは、公的に利用可能なアプリケーション層のエンドポイントにおいてリクエストを受信するモバイルサーバが必要であったが、上述したセキュリティに関連した理由から望ましくないことである。

【発明の概要】

【0009】

実施形態では、クラウドベースの認証方法は、モバイルデバイス上で実行しているプロセス制御アプリケーションと、プロセス制御環境に通信可能に結合されたモバイルサーバとの間でデータを転送するように構成されたリレー要素をクラウドベースのサーバ内でインスタンス化することを含む。このリレー要素は、インターネットを介して、例えば、モバイルデバイスおよびモバイルサーバに通信可能に結合される。この方法の認証方法は、

モバイルデバイス上で実行しているプロセス制御アプリケーションから第1のバリデーションキーをリレー要素で受信することと、リレー要素において第1のバリデーションキーをアプリケーションバリデーションキーと比較することと、を含む。第1のバリデーションキーがアプリケーションバリデーションキーと一致する場合、リレー要素は、プロセス制御アプリケーションを正当であると確認し、第1のバリデーションキーがアプリケーションバリデーションキーと一致しない場合、プロセス制御アプリケーションによるリレー要素へのアクセスは、拒否される。この方法はまた、モバイルサーバから、第2のバリデーションキーをリレー要素で受信することと、第2のバリデーションキーが正当である場合に、モバイルサーバをリレー要素で認証することと、をも含む。その後、この方法は、プロセス制御アプリケーションおよびモバイルサーバの両方が正当であると確認された場合に、リレー要素を介して、モバイルデバイス上で実行しているプロセス制御アプリケーションとモバイルサーバとの間の通信を許可することを含む。

【0010】

他の実施形態では、プロセス制御データを、モバイルデバイス上で動作しているプロセス制御アプリケーションに提供する方法は、プロセス制御環境に通信可能に結合されたモバイルサーバから、クラウドベースのサーバ上で動作するアプリケーションウェブサービスAPIに、プロセス制御アプリケーションとモバイルサーバとの間でデータを転送するように構成されたリレー要素をクラウドベースのサーバ内でインスタンス化するためのコマンドを送信することを含む。この方法は、リレーゲートウェイサービスを介して、モバイルサーバをリレー要素に対して認証するように動作可能であるバリデーションキーをリレー要素に送信することと、プロセス制御アプリケーションから、リレー要素およびリレーゲートウェイサービスを介して、プロセス制御アプリケーションのユーザに関連付けられたユーザ名およびパスワードを受信することと、を含む。この方法は、プロセス制御アプリケーションのユーザを認証することと、リレー要素およびリレーゲートウェイサービスを介して、利用可能なプロセス制御データのリストをプロセス制御アプリケーションに送信することと、をさらに含む。その後、この方法は、プロセス制御アプリケーションから、リレー要素およびリレーゲートウェイサービスを介して、送信するためのプロセス制御データの選択を受信することと、リレー要素およびリレーゲートウェイサービスを介して、選択されたプロセス制御データをプロセス制御アプリケーションに送信することと、を含む。

【0011】

実施形態では、プロセス制御アプリケーションにプロセス制御環境へのセキュアなオフプレミスアクセスを提供するためのシステムは、プロセス制御環境に通信可能に結合され、(i) プロセス制御環境からリアルタイムのプロセス制御データを受信し、(ii) プロセス制御環境内のコントローラに制御コマンドを送信する、ように構成されたモバイルサーバを含む。このシステムはまた、リレーゲートウェイサービスを介して、モバイルサーバに通信可能に結合されたクラウドベースのサーバ環境も含む。次に、このクラウドベースのサーバ環境は、モバイルデバイス上で実行しているプロセス制御アプリケーションとモバイルサーバとの間でデータを転送するように構成されたクラウドベースのリレー要素を含む。このクラウドベースのサーバ環境の第1のアプリケーションプログラミングインターフェース(API)は、モバイルサーバから、クラウドベースのリレー要素をインスタンス化および有効にするためのリクエストを受信するように構成される。このクラウドベースサーバ環境の第2のAPIは、プロセス制御アプリケーションから、クラウドベースのリレー要素にアクセスするためのリクエストを受信し、プロセス制御アプリケーションのユーザを認証し、クラウドベースのリレー要素にアクセスするための第1のバリデーションキーをプロセス制御アプリケーションに提供するように構成される。このクラウドベースサーバ環境のリレー管理データベースは、クラウドベースのリレー要素の構成情報を記憶している。このクラウドベースのサーバ環境のキー保管庫要素は、認証キーを記憶している。このシステムは、モバイルサーバをプロセス制御環境に結合する第1のネットワークと、モバイルサーバをクラウドベースのサーバ環境に結合する第2のネットワー

10

20

30

40

50

くと、プロセス制御アプリケーションをクラウドベースのサーバ環境に結合する第3のネットワークと、を含む。

【図面の簡単な説明】

【0012】

本明細書に記載の方法、装置、およびシステムの特徴および利点は、以下の詳細な説明および添付の図面を参照することによって最もよく理解されるであろう。

【図1】本記載による、例示的なプロセス制御環境のブロック図である。

【図2】本記載による、プロセス制御環境でのモバイル情報配信のためのシステムの全体的なアーキテクチャを例示するブロック図を描写する。

【図3】セキュアな認証システムおよび方法に伴う様々なコンポーネント、ならびにコンポーネント間の情報の流れを描写するブロック図である。

【図4】モバイルサーバがリレー要素を作成、有効化、無効化、または別の方法で修正するのを可能にするための方法を描写する通信フロー図である。

【図5】リレー要素に対してモバイルサーバを認証する方法を描写する通信フロー図である。

【図6】リレー要素に対してモバイルアプリケーションを認証する方法を描写する通信フロー図である。

【図7】リレー要素に対してモバイルサーバを認証するための、図6の方法の代替方法を描写する通信フロー図である。

【発明を実施するための形態】

【0013】

上述したように、既知の分散型プロセス制御システムは、オペレータ、保守担当者、およびプロセス制御システムに関連する他の人々がオペレータワークステーションから離れ、かつ／またはプロセスプラントの物理的な場所から離れている場合に、状況認識をセキュアに維持するための能力を欠いている。その結果、プラント担当者は、彼らが物理的に居ない限り、プロセス制御システムおよびプロセスプラントの動作を観察することができないか、または堅牢な認証プロトコルを欠いているために、プロセスプラントプレミスに居ないときには、プロセス制御システムに制御コマンドをセキュアに送信することができない。プロセスプラントは、通常、複数の交代勤務で稼働されるため、プロセスプラントの観察および操作は、多くの場合、毎日複数回、引き渡される。特定の交代勤務に係るプラント担当者は、次の交代勤務に係るそれらの人々に記録メモを残すことができるが、これらの交代勤務は、結果としてプロセスおよび設備の操作および管理における不連続性をもたらし、その不連続性は、製品品質、プラント効率、保守、環境安全、法規制の遵守、およびプロセスプラント管理の他の面に悪影響を及ぼす可能性がある。本明細書に記載されているモバイルデバイスのセキュアな認証のためのシステム、デバイス、および方法の実装は、情報へのセキュアなアクセス、ならびに制御コマンドのセキュアな送信、アラームまたはイベントの確認応答、および他のモバイルからプロセスへの通信を容易にすることができ、これらの利点は、以下の開示全体を通じて明らかになるであろう。

【0014】

図1は、複数のモバイルデバイス14をサポートするためのモバイルサービスインフラストラクチャ12を含む例示的なプロセスプラントネットワーク10を示し、必ずしもプロセスプラントプレミスに配置される必要はなく、プロセスプラントに関連付けられたデータにアクセスすることができる。本明細書に詳細に記載されているように、モバイルサービスインフラストラクチャ12は、モバイルデバイス14とプロセスプラントネットワーク10との間の、リアルタイムでセキュアな単方向または双方向通信を容易にし、その通信には、プロセス制御プラントネットワーク10内で利用可能なプロセスプラントデータのうちのいずれか、ならびにモバイルデバイス14からプロセス制御プラントネットワーク10へのコマンドおよび他のデータのいずれかの通信が含まれ、同時にプロセスプラントネットワーク10のセキュリティを維持する。モバイルデバイス14の各々は、他の要素の間で、モバイルデバイス14によって実行可能なアプリケーション16を含み、

ユーザがグラフィカルユーザインターフェース（GUI）18を介してプロセスプラントデータと相互にやり取りするのを可能にする。以下に説明されるように、モバイルサービスインフラストラクチャ12は、モバイルデバイスのセキュアな認証のためのアーキテクチャを含む。

【0015】

一般に、プラント担当者は、1つ以上のアプリケーション20を利用して、プロセスプラント10、およびプロセスプラント10内に実装された分散型制御システム22の動作を監督または制御する。閲覧または監視アプリケーション20は、一般に、ユーザインターフェースアプリケーションを含み、様々な異なるディスプレイを使用して、オペレータおよび保守技師、ならびに／またはワークステーション30および32などのワークステーションにおける他のユーザの各々に、プロセスグラフィックスをグラフで図示する。

【0016】

図1のプロセスプラント環境はまた、グラフィカル構成システム34も含む。グラフィカル構成システム34は、一般に、グラフィカルディスプレイを含む、プロセスプラントの制御のための制御および監視スキームの作成を容易にする。グラフィカル構成システム34は、例えば、モジュールを制御するとともにライブラリ内に記憶されたモジュールテンプレート、グラフィカルディスプレイおよびテンプレート、ならびに制御システムの他の面を制御するために使用され得、かつ、その後、制御モジュールのインスタンスをコントローラにダウンロードすることにより、またはプラント10の動作中に、例えば、オペレータおよび保守要員に提示されるユーザディスプレイのグラフィカルディスプレイのインスタンスを実行することにより、プロセスプラントの制御内で実際に実行されているインスタンスまたは使用法を作成するために使用され得る構成エディタ35を含み得る。当然ながら、グラフィックス構成システム34、構成エディタ35、ならびに様々な制御モジュール、テンプレート、およびグラフィカルディスプレイの各々は、有形のコンピュータ可読メモリまたは媒体内に記憶され、本明細書に説明される機能を実行するために1つ以上のプロセッサ上で実行することができる。

【0017】

一般的にそうであるように、図1に示す分散型プロセス制御システム22は、1つ以上のコントローラ40を有し、それらの各々は、例えば、Fieldbusインターフェース、Profibusインターフェース、HARTインターフェース、標準的な4-20mAインターフェースなどであってもよい入力／出力（I/O）デバイスまたはカード48を介して、1つ以上のフィールドデバイス44および46（これらは、スマートデバイスであってもよい）に接続される。コントローラ40はまた、例えば、イーサネットリンクであってもよいデータハイウェイ54を介して、1つ以上のホストまたはオペレータワークステーション30～32にも結合される。プロセスデータのデータベース58は、データハイウェイ54に接続され得、プロセス変数、プロセスパラメータ、ステータス、ならびにコントローラ、フィールドデバイス、およびプラント10内の任意の他のデバイスと関連付けられた他のデータを収集および記憶するように動作する。プロセスプラント10の動作中、プロセスデータのデータベース58は、コントローラ40から、および間接的にデータハイウェイ54を経由してフィールドデバイス44～46からプロセスデータを受信し得る。

【0018】

構成データベース60は、コントローラ40およびフィールドデバイス44、46内にダウンロードおよび記憶されたときに、プラント10内に分散型制御システム22の現在の構成を記憶する。この構成データベース60は、分散型制御システム22の1つまたはいくつかの制御手順、デバイス44、46の構成パラメータ、デバイス44、46の、プロセス制御機能への割り当て、およびプロセスプラント10に関連する他の構成データを定義するプロセス制御機能を記憶する。構成データベース60はさらに、グラフィカルオブジェクトまたはユーザディスプレイ、ならびに本明細書により詳細に説明されるこれらのオブジェクトまたはディスプレイと関連付けられた構成データを記憶して、プロセスプ

10

20

30

40

50

ラント 10 内の要素の様々なグラフィカル表現を提供し得る。記憶されたグラフィカルオブジェクトのうちのいくつかは、プロセス制御機能（例えば、特定の PID ループのために開発されたプロセスグラフィック）に対応し得、他のグラフィカルオブジェクトは、デバイス固有（例えば、圧力センサに対応するグラフィック）であり得る。

【0019】

データヒストリアン 62（別のデータベース）は、イベント、アラーム、コメント、およびオペレータが取った行動を記憶する。イベント、アラーム、およびコメントは、個々のデバイス（例えば、バルブ、送信機）、通信リンク（例えば、有線 Fieldbus セグメント、Wireless HART 通信リンク）、またはプロセス制御機能（例えば、所望される温度設定値を維持するための PID 制御ループ）に関係し得る。さらに、知識倉庫 64 は、参考資料、オペレータ記録簿記載事項、ヘルプトピック、またはこれらと、オペレータおよび保守技師がプロセスプラント 10 を監督するときに役立つと思われる他のマニュアル類とへのリンクを記憶する。なおさらに、ユーザデータベース 66 は、オペレータおよび保守技師などのユーザに関する情報を記憶する。各ユーザに対して、ユーザデータベース 66 は、例えば、ユーザの組織内での役割、ユーザの制御期間、ユーザに関連するプロセスプラント 10 内のエリア、作業チームの連携、セキュリティ情報、システム権限、交代勤務情報などを記憶することができる。

【0020】

データベース 58～66 の各々は、任意の所望されるタイプのメモリと、データを記憶するための任意の所望されるかまたは既知のソフトウェア、ハードウェアもしくはファームウェアと、を有する任意の所望されるタイプのデータ記憶装置または収集ユニットであり得る。当然ながら、データベース 58～66 は、別個の物理デバイスに存在する必要はない。したがって、いくつかの実施形態においては、データベース 58～66 のうちのいくつかは、共有のデータプロセッサおよびメモリ上に実装され得る。一般に、より少ないデータベースまたはより多いデータベースを利用して、図 1 のシステムの例におけるデータベース 58～66 によって集合的に記憶され、管理されたデータを記憶することも可能である。

【0021】

コントローラ 40、I/O カード 48、およびフィールドデバイス 44、46 は、典型的には、過酷な場合があるプラント環境内に配置され、その全体に分散されるが、オペレータワークステーション 30 および 32、ならびにデータベース 58～66 は、通常、コントローラ、保守、および他の様々なプラント担当者によって容易に評価可能である制御室または他のあまり過酷ではない環境に配置される。しかしながら、場合によって、データハイウェイ 54 に結合された手持ち式デバイスを使用してこれらの機能を実施することができ、これらの手持ち式デバイスは、通常、プラント内の様々な場所に持ち運ばれる。かかる手持ち式デバイス、ならびに場合によって、オペレータワークステーションおよび他のディスプレイデバイスは、無線通信接続を介して DCS 22 に接続され得る。手持ち式デバイスは、モバイルデバイスが必ずしもプロセスプラントプレミスに存在する必要はなく、データハイウェイ 54 に（有線または無線手段を介して）直接結合される必要はないという点で、モバイルデバイス 14 とは区別される。

【0022】

既知のように、例として、Emerson Process Management によって販売されている Delta V（商標）コントローラであり得るコントローラ 40 の各々は、任意の数の独立して実行される異なる制御モジュールまたはブロック 70 を使用して、制御手順を実装するコントローラアプリケーションを記憶し、実行する。制御モジュール 70 の各々は、一般に機能ブロックと称されるもので構成され得、各機能ブロックは、全体的な制御ルーチンの一部またはサブルーチンであり、（リンクと呼ばれる通信を介して）他の機能ブロックと共に動作して、プロセスプラント 10 内でプロセス制御ループを実施する。周知のように、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り得る機能ブロックは、典型的には、送信器、センサ、もしくは他のプロセスパラ

10

20

30

40

50

メータ測定デバイスと関連付けられるものなどの入力機能、PID、ファジー論理などの制御を実行する制御ルーチンと関連付けられるものなどの制御機能、またはバルブなどの何らかのデバイスの動作を制御して、プロセスプラント10内で何らかの物理的機能を行う出力機能のうちの1つを行う。当然ながら、ハイブリッドおよび他のタイプの複雑な機能ブロック、例えば、モデル予測コントローラ(MPC)、オブティマイザなどが存在する。FieldbusプロトコルおよびDeltaVシステムプロトコルが、オブジェクト指向プログラミングプロトコル内で設計され、実装された制御モジュールおよび機能ブロックを使用するが、一方で制御モジュールは、例えば、逐次機能ブロック、ラダーロジックなどを含む任意の所望の制御プログラミングスキームを使用して設計され得、機能ブロックまたは任意の他の特定のプログラミング技法を使用する設計および実装に限定されない。コントローラ40の各々はまた、Emerson Process Managementによって販売されるアプリケーションのAMS(登録商標)スイートをサポートし得、予測知能を使用して、機械設備、電気システム、プロセス設備、器具、非スマートおよびスマートフィールドデバイス44、46などを含む、生産資産の利用可能性および性能を改善し得る。

【0023】

説明されたように、DCS22は、制御室内のワークステーション(複数可)30、32に通信可能に連結されたコントローラ40のうちの1つ以上を含む。コントローラ40は、ワークステーション30、32を介して実装されるプロセス制御手順を実行することによって、プロセスエリア内のフィールドデバイス44、46の制御を自動化する。プロセス手順の一例としては、圧力センサフィールドデバイスを使用して圧力を測定し、圧力測定に基づいてフローバルブを開閉するためにバルブポジションにコマンドを自動的に送ることが挙げられる。I/Oカード48は、フィールドデバイス44、46から受信した情報をコントローラ40と互換性のあるフォーマットに変換し、コントローラ40からの情報をフィールドデバイス44、46と互換性のあるフォーマットに変換する。

【0024】

I/Oカード48を介して、コントローラ40は、コントローラ40にダウンロードされている制御モジュール70に応じてフィールドデバイス44、46と通信し得る。制御モジュール70は、構成システム34を使用してプログラムされる。構成システム34において、エンジニアは、例えば、1つ以上の機能ブロックをインスタンス化することによって制御モジュール70を作成し得る。一例として、構成エンジニアは、フィールドデバイス44、46のうち的一方からアナログ入力を受信するためにAI機能ブロックをインスタンス化し得、AI機能ブロックは、フィールドデバイス44、46のアナログ出力と関連付けられた様々な値(例えば、信号値、アラーム上限および下限、信号状態など)を受信し得る。AI機能ブロックは、対応する信号を別の機能ブロック(例えば、比例積分微分(PID)制御機能ブロック、カスタム機能ブロック、ディスプレイモジュールなど)に出力することができる。一旦AI機能ブロックがインスタンス化されると、機能ブロックを、フィールドデバイス44、46に関連付けられた固有のデバイスタグに関連付けることにより、以前にコントローラ40にダウンロードされた機能ブロックを、適切なI/Oカード48と協働させて、正しいフィールドデバイス44、46からの情報を処理させる。

【0025】

図1に示されたプラントネットワーク10において、コントローラ40に接続されたフィールドデバイス44、46は、標準的な4~20mAデバイスであってもよく、プロセスおよびメモリを含むHART(登録商標)、Profibus、またはFOUNDATION(登録商標)Fieldbus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であってもよく、または任意の他の所望のタイプのデバイスであってもよい。これらのデバイスのうちのいくつか、例えばFieldbusフィールドデバイス(図1に参照番号46で符号付けされる)は、コントローラ40内に実装された制御手順と関連付けられるか、またはプロセスプラント内でデータ収集、動向、アラーム、較正などの他のア

10

20

30

40

50

クションを行う、機能ブロックなどのモジュールまたはサブモジュールを記憶し、実行し得る。Fieldbusフィールドデバイス46内の2つの異なるフィールドデバイスに配設されるように図1に示される機能ブロック72は、周知であるように、コントローラ40内で制御モジュール70の実行と共に実行されて、プロセス制御を実施し得る。当然ながら、フィールドデバイス44、46は、センサ、バルブ、送信機、ポジショナなどの任意のタイプのデバイスであってもよく、I/Oデバイス48は、HART、Fieldbus、Profibusなどの任意の所望される通信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。

【0026】

続けて図1を参照すると、ワークステーション30および32は、プラント10内で担当者によって実行される様々な異なる機能のために使用される様々なアプリケーションを含むことができる。ワークステーション30および32の各々は、様々なアプリケーション、プログラム、データ構造などを記憶するメモリ80、およびメモリ80内に記憶されたアプリケーションのいずれかを実行するために使用され得るプロセッサ82を含む。図1に示した例では、ワークステーション30はまた、ディスプレイおよび閲覧アプリケーション20に加えて、1つ以上のプロセスコントローラ構成アプリケーション84も含み、これは、例えば、制御モジュール作成アプリケーション、オペレータインターフェースアプリケーション、ならびに任意の認証された構成エンジニアがアクセスして制御モジュール70および72などの制御ルーチンまたはモジュールを作成し、それらをプラント10の様々なコントローラ40およびデバイス46にダウンロードすることができる他のデータ構造を含み得る。構成アプリケーション84はまた、制御モジュール70を作成するために使用され得る構成エディタ35を有するディスプレイまたはグラフィカル構成システム34も含む。

【0027】

大雑把に言えば、閲覧アプリケーション20は、オペレータがプロセスプラント10の特定のエリアの動作に関する特定の情報を提供し、ディスプレイモジュール上の情報に応じてプロセスプラント10の動作を制御するように構成されたディスプレイモジュールを閲覧するのを可能にする。ディスプレイモジュールは、ワークステーション30、32上で描画され、そしてコントローラ40およびフィールドデバイス44、46から受信したリアルタイムプロセスデータを組み込む。本明細書に使用される際、データの「リアルタイム」通信は、追加の大幅な遅延の意図的な導入なしで、処理、ルーティング、および送信に通常の遅延を有する電子通信ネットワークを介したデータの電子通信を指す。いくつかの実施形態において、5秒未満（好ましくは、2秒未満）の些細な遅延が、リアルタイムでデータを通信するときのネットワーク輻輳を低減するために導入され得る。ディスプレイモジュールは、例えば、オペレータまたは他の使用がデータ値を操作して（例えば、読み出しまたは書き込みを実行して）、フィールドデバイス44、46、制御モジュール70、および機能ブロック72、ならびにDCS22およびプロセスプラント10全体としての動作を監視または変更することを可能にする任意のタイプのインターフェースであってもよい。ディスプレイモジュールは、ワークステーション30、32のメモリ80内に記憶され得、また構成データベース60内にも記憶され得る。

【0028】

制御モジュール70および、いくつかの実施形態では、ディスプレイモジュールは、構成データベース60内の構成ファイル74の一部であってもよい。つまり、制御モジュール70は、ディスプレイモジュールと共に、またはディスプレイモジュールとは別個に、構成ファイル74内に記憶され得る。いずれにしても、構成ファイル74は、一般に、デバイス、デバイスタグ、フレンドリ名、変数が各制御ループに関連付けられているデータフォーマット情報（例えば、スケーリング情報、ユニットタイプなど）、定義されている制御手順などを含む、DCS22の全体的な構成を記憶する。以前に示したように、構成ファイル74はまた、コントローラ40にダウンロードされて、構成ファイル74内に定義された制御手順を実装してもよい。

10

20

30

40

50

【0029】

理解されるように、プロセスプラント10は、数百、数千、さらには数万の信号、数百もしくは数千のフィールドデバイス44、46上の送信機（すなわち、センサ）からの出力、および／またはそれらのフィールドデバイス44、46への入力を含み得、制御モジュール70にプログラムされた制御手順に応じて、フィールドデバイス44、46に制御機能を実行させる。プラント10は、様々なエリアに分割され得、それらのエリアのうちの複数は、単一のコントローラ40によって制御され得、それらのエリアの各々は、単一のコントローラもしくは複数のコントローラ40、または何らかの組み合わせによって制御されてもよい。いずれにしても、プロセスプラント10を構成するフィールドデバイス44、46は、プロセスプラント10内で何回も別々に複製化されやすい（例えば、多くの任意のタイプのバルブ、多くのポンプ、多くのヒータ、多くのタンクなどが存在してもよい）。フィールドデバイス44、46はまた、物理的エリア（「プロセスエリア」）内の機能グループに組み合わされてもよく、そこでは、そのプロセスエリア内のフィールドデバイス44、46は、プロセス全体のうちの特定の部分を実行する。例えば、特定のプロセスエリアは、プロセスの他の部分に蒸気を発生させるための設備を有してもよい。プロセスエリア内には、同様の構造および機能を共有する設備の複製された部分またはグループ（「プロセスユニット」）があってもよい。一例として、蒸気発生プロセスエリア内のプロセスユニットは、ボイラーおよびターボ発電機を含んでもよく、プロセスエリアは、このプロセスユニットの複数のインスタンスを含んでもよい。

【0030】

システムアーキテクチャ

ここで図2に目を向けると、本明細書に記載されているように、ブロック図は、モバイルデバイス14を認証するための認証サービスアーキテクチャ、ならびにアーキテクチャ152全体の他のコンポーネントを含むプロセス制御環境内におけるモバイル情報配信のためのシステムのアーキテクチャ152全体を示す。アーキテクチャ152は、本明細書に記載されている認証サービスアーキテクチャの状況を説明する目的のために記載されている。アーキテクチャ152は、概して、3つのレベル、すなわち、プラント／プロセスレベル154、データサービスレベル156、およびモバイルサービスレベル158に分けられ、これらは、集合的に4～6つの異なるネットワークを含む。プラント／プロセスレベル154は、コントローラ40をフィールドデバイス44、46に結合するフィールドネットワーク（図2には示さず）、ならびにコントローラ40を、ワークステーション30、32、データベース58～66、およびプロセス制御プラント10内にある他のコンポーネントに結合する制御ネットワーク（図1に、データハイウェイ54として図示する）を含む。プラント／プロセスレベル154は、制御ネットワーク54を他のビジネスレベルアプリケーションに結合することができる中間ネットワーク160を任意選択的に含むことができる。プラント／プロセスレベル154は、ネットワーク162によって、データサービスレベル156に結合されている。データサービスレベル156は、ネットワーク164によって、モバイルサービスレベル158に結合されている。モバイルサービスレベル158は、インターネットおよび／またはモバイル電話／データネットワークなどの1つ以上の他のネットワークを含む。層154、156、158の各々、および実際のネットワークの各々は、他のセキュリティ対策に加えて、ハードウェアおよび／またはソフトウェアのファイアウォールによって他のものから分離され得る。階層化アーキテクチャにより、様々なネットワーク54、160、162、164などの間の分離を可能にしている。

【0031】

プラント／プロセスレベル154において、コミュニケーターインターフェース170は、コントローラ40とプロセスプラント10との間のインターフェースを一方の側で提供し、データサービスレベル156を他方の側で提供する。図1Lには、単一のコミュニケーターインターフェース170が、単一のコントローラ40（したがって、単一のプロセスプラント10）と通信するように図示されているが、コミュニケーターインターフェース1

70は、単一のプロセスプラントを制御する多様なコントローラ40と通信することができ、そこでは、プロセスプラント10の様々なエリアが、別個のコントローラ40によって制御される。また、実施形態では、複数のプロセス制御システム10が、複数のコミュニケーションインターフェース170によって、データサービスレベル156およびモバイルサービスレベル158に結合され得ることも考えられる。特定の実施形態では、コミュニケーションインターフェース170は、各プロセス制御システム10に結合され、コミュニケーションインターフェース170のグループは、データサービスレベル156に結合される。また、複数の制御システムが、異なる施設に（例えば、異なる化学プラントに）物理的に配置され得ることも想定される。

【0032】

コミュニケーションインターフェース170は、インターフェース全体をデータサービスおよびモバイルサービスレベル、それぞれ156および158に提供するさらに大きなポータル171の一部であってもよい。ポータル171は、ユーザ情報、デバイスおよびシステム情報、ならびにソフトウェア／ハードウェアライセンスの構成を容易にするなどの機能性を含むことができる。

【0033】

また、プラント／プロセスレベル154では、ファイルインターフェース172が、構成ファイル74をデータサービスレベル156に転送する機能を果たす。いくつかの実施形態では、ファイルインターフェース172は、プロセスプラント10を構成するために使用されるワークステーション30、32のうちの専用ワークステーションの一部であり、グラフィカル構成システム34、構成エディタ35などを含む。他の実施形態では、ファイルインターフェース172は、コミュニケーションインターフェース170の一部であってもよい。いずれにしても、ファイルインターフェース172は、データサービスレベル156に結合され、プロセスプラントの構成データをデータサービスレベル156に転送する。

【0034】

データサービスレベル156において、データサーバ174は、多くの異なるデータサービス176を含み、そのデータサービスは、集散的に、通信インターフェース170およびファイルインターフェース172からデータを受信し、その受信したデータをモバイルサービスレベル158に伝達する。プラント／プロセスレベル154から受信され、そしてモバイルサービスレベル158に伝達されるデータの中には、アラーム、プロセスパラメータ、診断、履歴データ、および構成データがある。様々なデータサービス176はまた、ファイルインターフェース172から受信した構成ファイル74に索引付けする役割も果たすことができる。索引付け動作は、詳細なサーチ能力をサポートするために、モジュールパラメータおよびモジュールヒエラルキーなどの特定の情報に対して索引付けすることを含み得、これにより、ユーザがプロセスプラント10のパラメータ名、デバイスタグ、アラーム、または他のデータをサーチするのを可能にすることができる。

【0035】

モバイルサーバ178は、モバイルサービスレベル158の心臓部である。このモバイルサーバ178は、モバイルデバイス14への接続をサポートし、モバイルデバイス14が登録される様々なリスト（例えば、アラームリスト、監視項目リストなど）の構成をサポートし、サーチ能力を提供し、モバイル通知を管理する。モバイルサーバ178はまた、データサービス176からの様々なデータへの登録を作成および維持する責任も担う。モバイルサーバ178は、多様な無線データ技術のうちのいずれかを介してモバイルデバイス14に結合され、その無線データ技術には、Wi-Fi（すなわち、IEEE 802.11プロトコル群のプロトコル）、および／またはLTEサービス、インターネット180を利用し得るサービスのうちの一部もしくはすべてを含むがこれらに限定されない、現在もしくは将来利用可能な様々なデータサービスのいずれかを使用するモバイル（「セルラー」）インフラストラクチャが含まれ得る。

【0036】

モバイルサービスレベル158はまた、以下でさらに詳細に説明されることになる認証サービスコンポーネント183も含む。モバイルサービスコンポーネント183は、モバイルサーバ178と通信して様々な認証サービスを実行するサブアーキテクチャを含み、その認証サービスには、モバイルデバイス14、モバイルサーバ178、および実施形態によっては他のコンポーネントの上でも実行しているアプリケーションの認証が含まれる。
【0037】

モバイルデバイス14は、Google社が開発したAndroidモバイルオペレーティングシステムを実行するモバイルデバイス、Apple社が開発したiOSもしくはiPad（登録商標）OSモバイルオペレーティングシステムを実行するモバイルデバイス、または現在既知のもしくは将来開発される任意の他のオペレーティングシステムを含み得る。Android、iOS、および／またはiPad（登録商標）OSモバイルオペレーティングシステムを実行するモバイルデバイス14の場合、通知は、AppleまたはGoogleの通知サービス182を介してモバイルデバイス14に配信され得、そのようなサービスの使用に慣れている人々には、容易に理解されるであろう。モバイルサーバ178は、システムレベルおよび／またはユーザレベルでの通知サービスの構成を容易にする。

【0038】

モバイル情報配信の構成に関して、モバイルサーバ178は、モバイルデバイス14に備わっているモバイルデバイスインターフェースを介していくつかの構成サービスを提供する。モバイルサーバ178はまた、ウェブページを介して（すなわち、ウェブブラウザを使用して）構成オプションも提供する。理解されるように（例えば、参照によりその全体が本明細書に組み込まれる米国特許出願公開第2018/0109651号を見ると）、様々なアラームリストおよび監視項目リストは、サーチ（すなわち、構成ファイル74の索引付けされたデータをサーチすること）および／もしくはフィルタを使用するか、またはシステムヒエラルキー情報、機能分類、アラーム優先度、アラームカテゴリなどを利用するウェブインターフェースを介して構成されてもよい。

【0039】

モバイルサービスレベル158での構成データの利用可能性は、エンドユーザにとって特に豊かなモバイル環境を提供する役割を果たし得、その理由は、システムが、データだけではなく、データ間の関係性にもアクセスすることができるからである。さらに、セキュアな認証プロトコルを実装する本記載の実施形態では、プロセス制御システム10は、監視されることに加えて、制御されるか、または別の方法で互いにやり取りされ得る。例として、アラームのステータス（例えば、有効）またはパラメータ値のステータス（例えば、正常、高い、低いなど）のみを有するのではなく、モバイルサーバ178は、構成ファイル74からの構成データを介して、データとデータタイプとの間の連携関係にアクセスすることができる。したがって、システムは、特定の有効アラームが「高い」状態であるパラメータステータスの結果であり、ひいては、パラメータデータ値が特定の制限を超えたことからパラメータステータスが「高い」状態であると判断することができる。このような豊富な連携情報がモバイルサーバ178に利用可能である結果として、ユーザインターフェースは、例えば、アラームがリアルタイムのデータおよび履歴と一緒に描写され得るか、またはプロセス変数が現在および過去の設定値、ならびに任意選択的に、関連するモジュール関係と一緒に描写され得るという状況でデータを提示するように動作可能であり、これにより、ユーザが、プロセス制御デバイス間、機能ブロック間などの関係に基づいて、1つのデータから他の関連データに移動するのを可能にすることができる。

【0040】

さらに、セキュアに認証される環境では、モバイルサーバ178は、モバイルデバイス（複数可）14からデータおよび／またはコマンドを受信することができ、データをプラントレベル154に戻す送信が禁止された先行技術システムとは対照的に、コマンドおよび／またはデータをデータサービスレベル156および／またはプラントレベル154に戻すことができ、プロセスプラント環境10のセキュリティを確実にすることができる。

すなわち、プラントレベル 154 からデータサービスレベル 156 および／またはモバイルサービス 158 への通信が単一方向でなければならないという要件は、そのような通信が受信され得るモバイルデバイス 14 がセキュアに認証されるため、緩和され得る。その結果、モバイルデバイス 14 のユーザは、制御プラント 10 がそのような通信を許可するように構成されている場合、アラーム確認応答および制御コマンドをプラントレベル 154 に送り返すことができる。

【0041】

認証サービス

図 2 に描写された認証サービスコンポーネント 183 は、モバイルサービスレベル 158 におけるプロセス制御プラント 10 の近くにあるコンポーネント 183A と、プロセス制御プラント 10 から遠く離れ、かつインターネットを介してアクセス可能なコンポーネント 183B とを伴うサブアーキテクチャを含む。コンポーネント 183B は、モバイルデバイス（複数可）14 上で実行するグラフィカルユーザインターフェース（GUI）アプリケーション（本明細書ではまた、プロセス制御アプリケーションとも呼ばれる）200、および Microsoft Azure クラウドコンピューティングプラットフォームなどのクラウドコンピューティングプラットフォーム上のホストとして働き、かつ本明細書では「ホストとして働くコンポーネント」と呼ばれ得る様々なコンポーネントを含む。このホストとして働くコンポーネントは、以下にさらに詳細に説明されることになるが、リレーハイブリッド接続（RHC）（本明細書ではまた、リレー要素とも呼ばれる）202、代表的状態転送（REST）アプリケーションプログラミングインターフェース（API）204、リレー管理 API 206、リレーアクセス API 208、リレー管理データベース 210、キー保管庫 212、およびアプリケーションサービスウェブ API 214 を含む。

【0042】

コンポーネント 183A は、モバイルサーバ 178 に通信可能に結合されたリレーゲートウェイサービス（RGS）218 を含む。この RGS 218 は、モバイルサーバ 178 上で実行しているソフトウェアコンポーネントであってもよい。

【0043】

RHC 202 は、インターネット（有線、無線、および／またはセルラー通信インフラストラクチャを介することを含む）を使用して、モバイルアプリケーション 200 とモバイルサーバ 178 との間のセキュアな通信チャネルを介して、セキュアな通信を容易にする責任を担う。特に、RHC 202 は、RGS 218 と協働して、モバイルアプリケーション 200 とモバイルサーバ 178 との間でデータ（認証データおよびプロセスデータを含む）を渡すことができる。以下に説明されているように、RHC 202 は、モバイルサーバ 178、およびモバイルアプリケーション 200 の各ユーザが適切に認証されることを確実にする様々な認証プロセスを使用してセキュアな通信チャネルを作成して、プロセス制御システム 10 への不正アクセスを防止する。

【0044】

REST API 204 は、RHC 202 を管理する複数の API からなり、モバイルアプリケーション 200 とモバイルサーバ 178 の両方を RHC 202 に対して認証するキーを生成および記憶する責任を担う。具体的には、REST API 204 は、RHC 202 に対してモバイルアプリケーション 200 を認証する送信キー、および RHC 202 に対してモバイルサーバ 178 を認証するリスンキーを生成して記憶する。

【0045】

リレー管理 API 206 は、様々な顧客サイトの RHC 202 を作成、有効化、および無効化する責任を担う。すなわち、リレー管理 API 206 は、特定のプロセスプラントオペレータのアーキテクチャに固有ではないクラウドコンピューティングプラットフォーム上で動作するグローバルコンポーネントであり得るが、代替的に様々な異なるプロセスプラントのための RHC 202 を作成することができる。リレー管理 API 206 は、REST API 204 と協働して RHC 202 を管理することができる。リレー管理 AP

I 2 0 6 はまた、R H C 情報を提供し、リレー管理データベース 2 1 0 と通信して R H C 情報を記憶する責任も担う。

【 0 0 4 6 】

リレーアクセス A P I 2 0 8 は、同様に、クラウドコンピューティングプラットフォーム上でホストとして働く。リレーアクセス A P I 2 0 8 は、モバイルアプリケーション 2 0 0 による、R H C 2 0 2 への初期アクセス、およびモバイルアプリケーション 2 0 0 とモバイルサーバ 1 7 8 との間の通信接続のセットアップを容易にする。特に、リレーアクセス A P I 2 0 8 は、モバイルアプリケーション 2 0 0 から、認証トークン（「送信キー」に関しては、後述する）のためのリクエストを、モバイルアプリケーション 2 0 0 を使用する個人のユーザ名およびパスワードと一緒に受信する。リレーアクセス A P I 2 0 8 は、モバイルアプリケーション 2 0 0 が正当であることを確認するためのリクエストを容易にする。

10

【 0 0 4 7 】

リレー管理データベース 2 1 0 はまた、クラウドコンピューティングプラットフォーム上でもホストとして働く。リレー管理データベース 2 1 0 は、セキュアなオフプレミスマーキテクチャを使用して、様々な顧客サイトの R H C 情報（アドレス、接続状態など）を記憶する共通のコンポーネントである。

【 0 0 4 8 】

キー保管庫 2 1 2 は、様々なアクセストークンおよび資格情報を記憶する。これらには、リレー管理データベース 2 1 0 に対してアプリケーションサービスウェブ A P I 2 1 4 を認証するための資格情報、R E S T A P I 2 0 4 に対してアプリケーションサービスウェブ A P I 2 1 4 を認証するための資格情報、リレー管理 A P I 2 0 6 に対してリレーアクセス A P I 2 0 8 を認証するための資格情報、R E S T A P I 2 0 4 に対してリレー管理 A P I 2 0 6 を認証するための資格情報などが含まれ得る。

20

【 0 0 4 9 】

アプリケーションサービスウェブ A P I 2 1 4 は、同様に、クラウドコンピューティングプラットフォーム上でホストとして働く。アプリケーションサービスウェブ A P I 2 1 4 は、モバイルサーバ 1 7 8 と、残りのコンポーネント 1 8 3 B との間のバックエンド通信を容易にし、特に、R H C 2 0 2 のセットアップ、およびモバイルサーバ 1 7 8 による、R H C 2 0 2 へのアクセスを容易にする。アプリケーションサービスウェブ A P I 2 1 4 は、モバイルサーバ 1 7 8 から、認証トークンのリクエストを受信し（「リスンキー」に関しては、後述する）、それと共に、モバイルサーバ 1 7 8 に、例えば、R H C 2 0 2 を有効にする、R H C 2 0 2 を無効にする、R H C 2 0 2 のアドレスを変更するなどによって R H C 2 0 2 の動作を変更するためにアクセスを提供する。

30

【 0 0 5 0 】

図 4 は、モバイルサーバ 1 7 8 の認証、および R H C 2 0 2 のセットアップのための方法 2 5 0 の中で、システム内の様々な要素間の通信を描写する通信フロー図である。R H C 2 0 2 の動作を作成、有効化、無効化、または別の方法で修正するための動作中に、モバイルサーバ 1 7 8 は、R H C 2 0 2 の修正をアプリケーションサービスウェブ A P I 2 1 4 に送信する（メッセージ 2 5 2）。アプリケーションサービスウェブ A P I 2 1 4 は、認証するためのリクエスト（メッセージ 2 5 4）を使ってモバイルサーバ 1 7 8 に応答することができ、それに応答して、モバイルサーバ 1 7 8 は、システムキー 2 5 6 を送信することができる（メッセージ 2 5 6）。実施形態では、システムキーは、モバイルサーバ 1 7 8 に提供されるライセンスキーもしくはその一部であってもよく、またはモバイルサーバ 1 7 8 上で実行しているソフトウェアの一部、もしくはルーチンに関連付けられていてもよい。図 4 および他の図に描写されている通信フローは、いくつかのメッセージが組み合わされるようにわずかに修正され得ることを理解されたい。例えば、モバイルサーバ 1 7 8 がアプリケーションサービスウェブ A P I 2 1 4 へのアクセスをリクエストするメッセージ 2 5 2 はまた、システムキーを含み得、その結果、メッセージ 2 5 4 および 2 5 6 は、削除される。これらのタイプの調整は、当技術分野においてよく理解されてお

40

50

り、さらなる効率をもたらし得る。

【0051】

システムキーを受信すると、アプリケーションサービスウェブAPI 214は、アプリケーションサービスウェブAPI 214による、リレー管理データベース210へのアクセスを与える資格情報をキー保管庫212からリクエストすることができる（メッセージ258）。キー保管庫212は、既にアプリケーションサービスウェブAPI 214を認証している場合があり、または実施形態では、キー保管庫212は、アクティブディレクトリ管理された識別情報を使用してアプリケーションサービスウェブAPI 214を認証する。例えば、管理された識別情報は、クラウドベースのプラットフォームでインスタンス化されると、アプリケーションサービスウェブAPI 214に対して有効化および作成され得、キー保管庫212は、管理された識別情報に依拠して、アプリケーションサービスウェブAPI 214がキー保管庫212にセキュアにアクセスし得ることを確実にすることができる。資格情報のリクエストに回答して（メッセージ258）、キー保管庫212は、リレー管理データベース210にアクセスするための資格情報をアプリケーションサービスウェブAPI 214に送信することができる（メッセージ260）。

【0052】

キー保管庫212から、リレー管理データベース210にアクセスするための資格情報を受信すると（メッセージ260）、アプリケーションサービスウェブAPI 214は、資格情報をリレー管理データベース210に送信することができる（メッセージ262）、それに応じて、正常な認証を確認するメッセージを受信することができる（メッセージ264）。次いで、アプリケーションサービスウェブAPI 214は、モバイルサーバ178から受信したシステムキーをリレー管理データベース210に送信することができる（メッセージ266）、それに応じて、リレー管理データベース210から、システムキーが認証されたという確認を受信することができる（メッセージ268）。次いで、アプリケーションサービスウェブAPI 214は、RHC 202に関連する任意の動作に対して1つ以上のリクエスト（複数可）を送信することができる、その動作には、RHC 202（既にリレー管理データベース210内に用意されている）を作成すること、RHC 202を有効化すること、RHC 202を無効化すること、および／またはRHC 202の動作を修正することが含まれる（メッセージ270）。それに応じて、リレー管理データベース210は、リクエストを確認応答する、かつ／またはリクエストされた修正の正常な完了を確認応答するメッセージをアプリケーションサービスウェブAPI 214に送信することができる（メッセージ272）。アプリケーションサービスウェブAPI 214は、リクエストされた修正の正常な完了の確認応答を転送することができる（メッセージ274）。

【0053】

RHC 202が作成され、クラウドベースプラットフォーム上で実行していると、モバイルサーバ178は、RHC 202に対してそれ自体を認証することができる必要がある。図5は、RHC 202に対してモバイルサーバ178を認証するための方法300の中で、システム内の様々な要素間の通信を描写する通信フロー図である。実施形態では、この図は、リレーゲートウェイサービス218からモバイルサーバ178への、リスンキーのリクエストによって開始される（メッセージ302）。上記で暗に触れたように、リスンキーは、RHC 202に対してモバイルサーバ178を認証する認証資格情報であり、そのモバイルサーバ178が認証されてモバイルアプリケーション200へのセキュアなチャンネルにアクセスすることを確実にする。このリクエストに回答して、モバイルサーバ178は、リスンキーのリクエストをアプリケーションサービスウェブAPI 214に送信する（メッセージ304）。アプリケーションサービスウェブAPI 214は、リスンキーのリクエストに回答して（メッセージ304）、REST API 204にアクセスするための資格情報のリクエストをキー保管庫212に送信する（メッセージ306）。上述したように、キー保管庫212は、既にアプリケーションサービスウェブAPI 214を認証している場合があり、または実施形態では、キー保管庫212は、アクティブ

ディレクトリ管理された識別情報を使用してアプリケーションサービスウェブAPI 214を認証する。例えば、管理された識別情報は、クラウドベースのプラットフォームでインスタンス化されると、アプリケーションサービスウェブAPI 214に対して有効化および作成され得、キー保管庫212は、管理された識別情報に依拠して、アプリケーションサービスウェブAPI 214がキー保管庫212にセキュアにアクセスし得ることを確実にすることができる。資格情報のリクエストに応答して（メッセージ306）、キー保管庫212は、REST API 204にアクセスするための資格情報をアプリケーションサービスウェブAPI 214に送信することができる（メッセージ308）。

【0054】

アプリケーションサービスウェブAPI 214は、REST API 204にアクセスするための資格情報を受信すると、REST API 資格情報をREST API 204に送信することができ（メッセージ310）、そのREST APIは、正常な認証を確認応答するメッセージを使ってアプリケーションサービスウェブAPI 214に応答することができる（メッセージ312）。次いで、アプリケーションサービスウェブAPI 214は、リスンキーのリクエストをREST API 204に送信することができ（メッセージ314）、それに応答して、REST API 204は、リスンキーをアプリケーションサービスウェブAPI 214に送信することができる（メッセージ316）。当然ながら、特定のメッセージを組み合わせることができる。例えば、アプリケーションサービスウェブAPI 214は、それがREST API 資格情報を送信すると同時にリスンキーをリクエストすることができ、例えば、REST API 214は、リスンキーと同時に認証確認応答を送信することができる。アプリケーションサービスウェブAPI 214は、リスンキーをモバイルサーバ178に返信することができ（メッセージ318）、次に、リスンキーをリレーゲートウェイサービス218に送信することができる（メッセージ320）。リレーゲートウェイサービス218は、リスンキーをRHC 202に送信することができる（メッセージ322）。RHC 202は、インスタンス化／作成されたときに、そのリスンキーと一緒にプログラムされる。したがって、RHC 202がリレーゲートウェイサービス218を介してモバイルサーバ178から正しいリスンキーを受信すると、RHC 202は、モバイルサーバを認証し、その後、モバイルサーバ178は、リレーゲートウェイサービス218およびRHC 202を介して、モバイルアプリケーション200と通信することができる（メッセージ324）。

【0055】

リスンキー、ならびにモバイルアプリケーション200とリレーゲートウェイサービス218との間で送信される任意の他のデータは、通常、HTTPSプロトコルを使用して送信され、識別情報サーバ認証トークン、およびクラウドプラットフォームトークンを包含するリクエストヘッダを含むことができる。HTTPリクエストおよび応答本体は、JavaScript Object Notation (JSON) 形式のデータを含むことができる。

【0056】

図6は、RHC 202に対してモバイルアプリケーション200を認証するための方法350の中で、システムにおける様々な要素間の通信を描写する通信フロー図である。RHC 202への接続を確立するために、モバイルアプリケーション202は、アクセスリクエストをリレーアクセスAPI 208に送信する（メッセージ352）。リレーアクセスAPI 208は、モバイルアプリケーション200から認証情報をリクエストすることができ（メッセージ354）、それに応答して、モバイルアプリケーション200は、モバイルアプリケーション200のユーザに関連付けられたユーザ名およびパスワード、ならびにRHC 202のURLをリレーアクセスAPI 208に送信することができる（メッセージ356）。一実施形態では、RHC 202のURLは、https:// {リレー名前空間} . {クラウドコンピューティングプラットフォーム名前空間} / {ハイブリッド接続名} の形式を取ることができる。一例として、特定のRHC 202を指すURLは、https:// Relay-65.servicebus.windows.ne

10

20

30

40

50

て／HC100とすることができる。リレーアクセスAPI208は、モバイルアプリケーション200から受信したURLをリレー管理API206に送信することができ（メッセージ358）、それに応じて、リレー管理API206からRHC202への情報を受信することができる（メッセージ360）。

【0057】

リレーアクセスAPI208は、RHC202の情報を備えると、モバイルアプリケーション200から受信したユーザ名およびパスワード情報をRHC202に送信することができる（メッセージ362）。RHC202は、ユーザ名およびパスワード情報をリレーゲートウェイサービス218に送信することができ（メッセージ364）、次に、リレーゲートウェイサービスはユーザ名およびパスワード情報をモバイルサーバ178に送信することができる（メッセージ366）。モバイルサーバ178は、ユーザ名およびパスワードを認証し、ユーザ名およびパスワードが正当であること（実際、それが正当である場合）を確認する認証メッセージをリレーゲートウェイサービス218に送信する（メッセージ368）。リレーゲートウェイサービス218は、メッセージをRHC202に転送し（メッセージ370）、次に、RHC202は、メッセージをリレーアクセスAPI208に転送する（メッセージ372）。

【0058】

モバイルアプリケーション200のユーザの識別情報を確認すると、リレーアクセスAPI208は、今度は、モバイルアプリケーション200の送信キーをリクエストすることができる。上述したように、送信キーは、アプリケーション200がモバイルサーバ178と通信するためのセキュアなチャンネルにアクセスすることを認証されていることを、RHC202に証明する認証資格情報である。図7を参照すると、リレーアクセスAPI208は、送信キーのリクエストをリレー管理API206に送信することができる（メッセージ374）。リレー管理API206は、リレーアクセスAPI208から認証情報をリクエストすることができる（メッセージ376）。リレーアクセスAPI208は、対応する資格情報のリクエストをキー保管庫212に送信することができる（メッセージ378）。キー保管庫212は、既にリレーアクセスAPI208を認証している場合があり、または実施形態では、キー保管庫212は、アクティブディレクトリ管理された識別情報を使用してリレーアクセスAPI208を認証する。例えば、管理された識別情報は、クラウドベースのプラットフォームでインスタンス化されると、リレーアクセスAPI208に対して有効化および作成され得、キー保管庫212は、管理された識別情報に依拠して、リレーアクセスAPI208がキー保管庫212にセキュアにアクセスし得ることを確実にすることができる。資格情報のリクエストに回答して（メッセージ378）、キー保管庫212は、リクエストされた資格情報をリレーアクセスAPI208に送信することができる（メッセージ380）。

【0059】

リクエストされた資格情報を受信すると、リレーアクセスAPI208は、資格情報をリレー管理API206に送信することができ（メッセージ382）、そのリレー管理API206は、その認証を確認応答することができる（メッセージ384）。次いで、リレーアクセスAPI208は、それが送信キーをリクエストしているRHC202のURLをリレー管理API206に送信することができる（メッセージ386）。

【0060】

REST API204を使って認証するために、リレー管理API206は、REST API204に対してリレー管理API206を認証するための資格情報のリクエストをキー保管庫212に送信することができる（メッセージ388）。キー保管庫212は、既にリレー管理API206を認証している場合があり、または実施形態では、キー保管庫212は、アクティブディレクトリ管理された識別情報を使用してリレー管理API206を認証する。例えば、管理された識別情報は、クラウドベースのプラットフォームでインスタンス化されると、リレー管理API206に対して有効化および作成され得、キー保管庫212は、管理された識別情報に依拠して、リレー管理API206がキー保管

10

20

30

40

50

庫 2 1 2 にセキュアにアクセスし得ることを確実にすることができる。資格情報のリクエストに応答して（メッセージ 3 8 8）、キー保管庫 2 1 2 は、リクエストされた資格情報をリレー管理 API 2 0 6 に送信することができる（メッセージ 3 9 0）。

【 0 0 6 1 】

リレー管理 API 2 0 6 は、リクエストされた資格情報を所有している場合、R E S T A P I 2 0 4 に資格情報を送信することができ（メッセージ 3 9 2）、それに応じて、R E S T A P I 2 0 4 から認証確認応答メッセージを受信することができる（メッセージ 3 9 4）。認証の確認応答を受信すると、リレー管理 API 2 0 6 は、送信キーのリクエストを R E S T A P I 2 0 4 に送信することができ（メッセージ 3 9 6）、それに応答して、R E S T A P I 2 0 4 は、リクエストされた送信キーをリレー管理 API 2 0 6 に送信することができる（メッセージ 3 9 8）。次いで、リレー管理 API 2 0 6 は、送信キーをリレーアクセス API 2 0 8 に転送することができる（メッセージ 4 0 0）。

10

【 0 0 6 2 】

再度図 6 を参照すると、リレーアクセス API 2 0 8 は、送信キーを受信すると（メッセージ 4 0 0）、送信キーをモバイルアプリケーション 2 0 0 に送信することができる（メッセージ 4 0 2）。その後、モバイルアプリケーション 2 0 0 は、送信キーを R H C 2 0 2 に送信することができる（メッセージ 4 0 4）。R H C 2 0 2 は、クラウドベースのプラットフォームでインスタンス化／作成されると、その対応する送信キーと一緒にプログラムされ、モバイルアプリケーション 2 0 0 から受信した送信キーが R H C 2 0 2 にプログラムされた送信キーと一致すると、R H C 2 0 2 は、モバイルアプリケーション 2 0 0 を認証し、その後、R H C 2 0 2 およびリレーゲートウェイサービス 2 1 8 を介してモバイルアプリケーション 2 0 0 とモバイルサーバ 1 7 8 との間の通信を許可することができる（メッセージ 4 0 6）。

20

【 0 0 6 3 】

送信キー、ならびにモバイルアプリケーション 2 0 0 から R H C 2 0 2 に送信された任意の他のデータは、通常、H T T P S プロトコルを使用して送信され、識別情報サーバ認証トークンおよびクラウドプラットフォームトークンを包含するリクエストヘッダを含むことができる。H T T P リクエストおよび応答本体は、J a v a S c r i p t O b j e c t N o t a t i o n (J S O N) 形式のデータを含むことができる。

【 0 0 6 4 】

モバイルアプリケーション 2 0 0 に関連付けられた特定のユーザは、結果として、特定のメッセージがモバイルサーバ 1 7 8 によって許可または禁止され、確認応答または無視されることになり得る。実施形態では、R H C 2 0 2 は、ユーザについての情報をモバイルサーバ 1 7 8 に提供してもよい（例えば、送信キーをユーザに関連付けることによって）。例えば、モバイルサーバ 1 7 8 は、モバイルアプリケーション 1 7 8 を特定のユーザに関連付けることができ、その結果、ユーザに関連付けられたデータ（すなわち、ユーザが以前にリクエストし、かつ／またはモバイルサーバ 1 7 8 を構成してモバイルアプリケーション 2 0 2 を介してユーザに送信したデータストリーム）をアプリケーション 2 0 0 に送信すること、ユーザからプロセス制御コマンドを受信すること、ユーザから受信したものとして受信したコマンドの記録を取ること、特定のユーザに応答して送信されたデータおよび／または実装されたコマンドを制限することなどのユーザ固有の動作を有効化または無効化することができる。

30

40

【 0 0 6 5 】

本説明の観点から理解されるべきであるように、リレー要素 2 0 2 の単一のインスタンスは、モバイルサーバ 1 7 8 と、複数の、または多様なモバイルプロセス制御アプリケーション 2 0 0 との間の通信を容易にすることができる。実施形態では、リレー要素 2 0 2 の単一のインスタンスは、プロセス制御設備全体にサービスする 1 つ以上のモバイルサーバ 1 7 8 と、プロセス制御設備の維持および／または監視に関連付けられた担当者に対応するモバイルプロセス制御アプリケーション 2 0 0 の任意の数のインスタンスとの間の通信を提供することができる。他の実施形態では、リレー要素 2 0 2 の単一のインスタンス

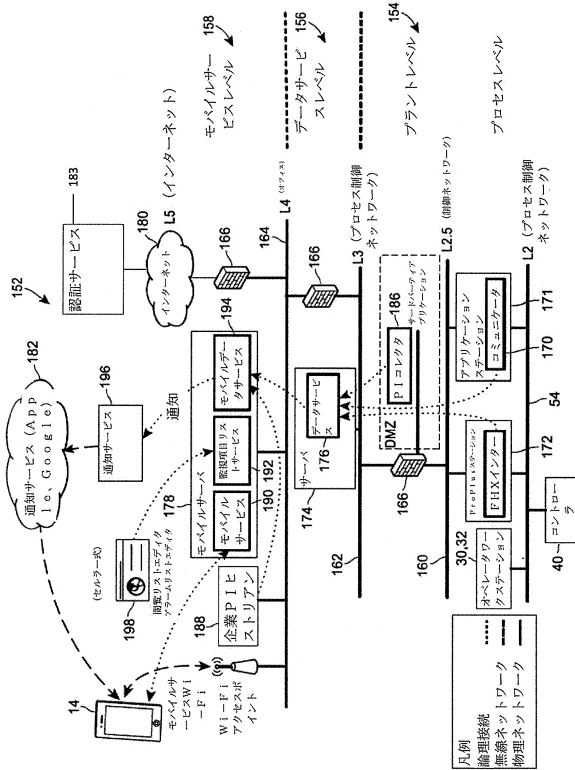
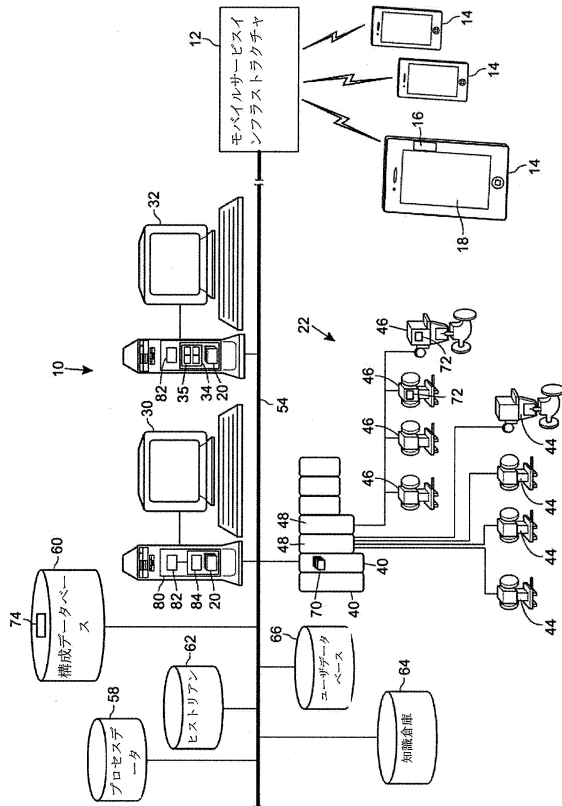
50

は、プロセス制御設備の一部にサービスする1つ以上のモバイルサーバ178と、プロセス制御設備の維持および／または監視に関連付けられた担当者に対応するモバイルプロセス制御アプリケーション200の任意の数のインスタンスとの間の通信を提供することができる。したがって、リレー要素202は、様々な実施形態において、2つ以上のモバイルプロセス制御アプリケーション200を認証することができ、かつ／または2つ以上のモバイルサーバ318を認証することができる。

【図面】

【図 1】

【図 2】



10

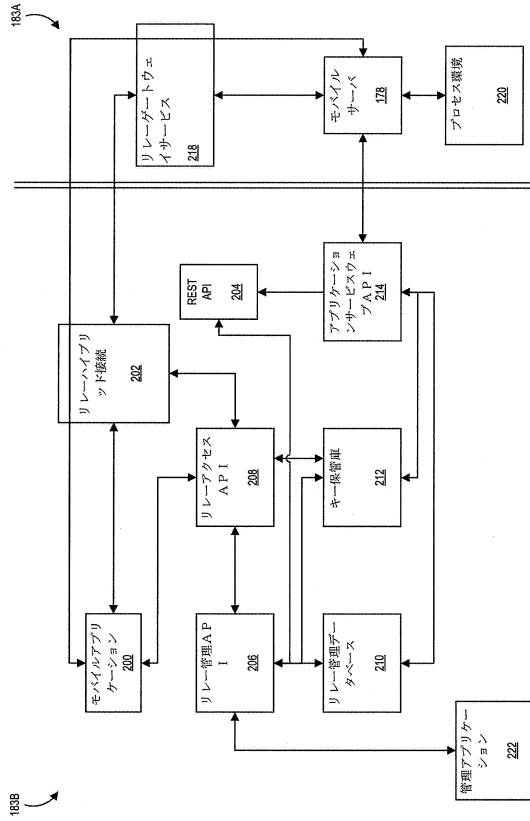
20

30

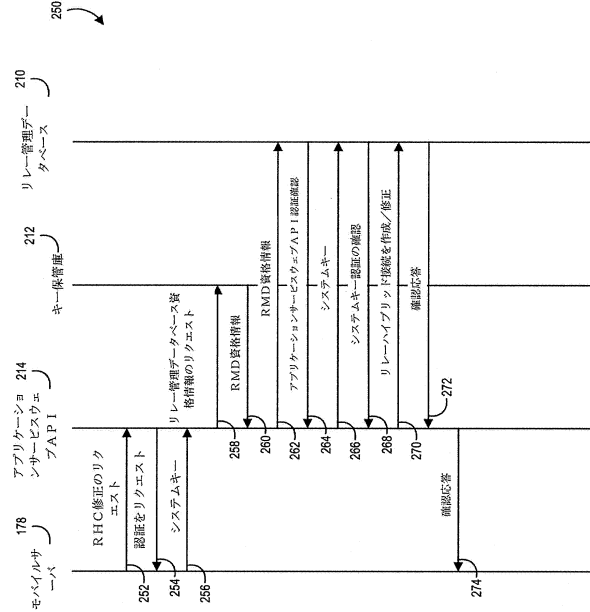
40

50

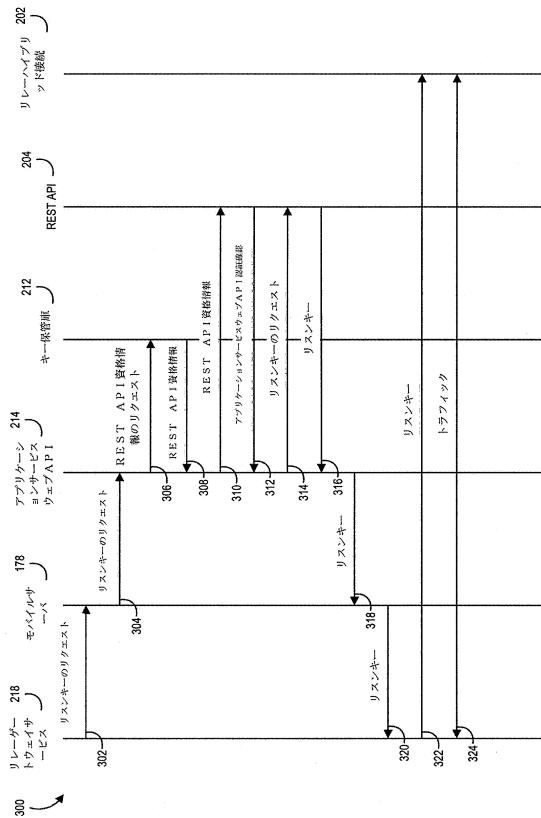
【図 3】



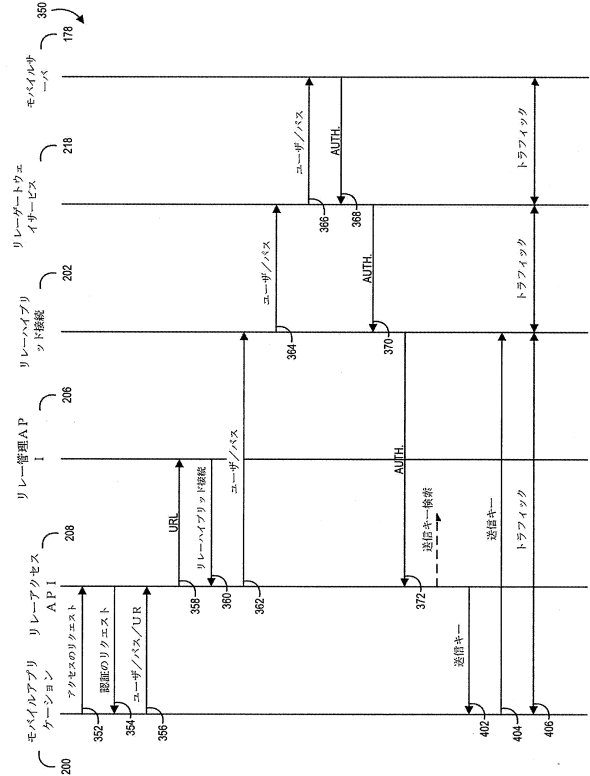
【図 4】



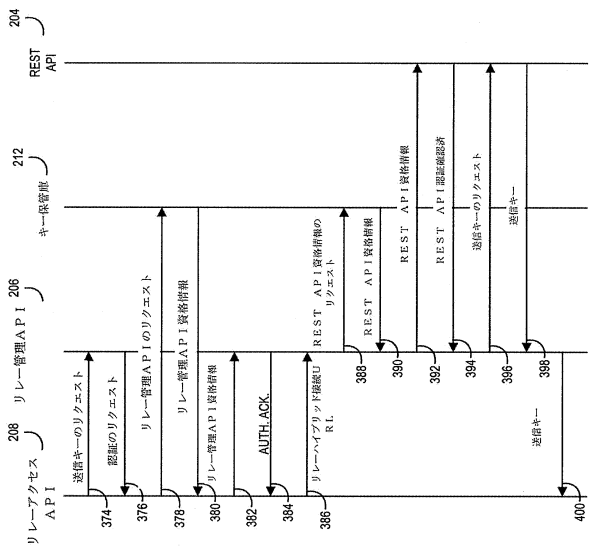
【図 5】



【図 6】



【図 7】



10

20

30

40

50

フロントページの続き

- (72)発明者 リチャード・クラランス・ダヨ・ファブロス
 フィリピン共和国 ラグーナ 4000 セント サン パブロ デルピラー ストリート 4 エムエイチ
- (72)発明者 アーウィン・パギオ
 フィリピン共和国 マンダルヨン・シティ ハイウェイ ヒルズ カルバヨグ ストリート アールエ
 スジー1 D10
- (72)発明者 ジョージ・シトン
 フィリピン共和国 キャビテ バコール・シティ モリノ アヴィタ セッティングス ビーエル12
 エルティ－23 ビーエイチ2
- (72)発明者 クリストファー・イアン・サルミエント・ユーワイ
 フィリピン共和国 メトロ・マニラ 1441 ヴァレンズレア・シティ カルハタン エー・パブロ
 ストリート 60-A号
- 審査官 石坂 知樹
- (56)参考文献 特表2013-546261 (JP, A)
 特開2018-055582 (JP, A)
- (58)調査した分野 (Int.Cl., DB名)
 G06F 21/33
 G06F 21/31
 G06F 21/44