(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7010612号
(P7010612)

(45)発行日　令和4年1月26日(2022.1.26)

(24)登録日　令和4年1月17日(2022.1.17)

(51)国際特許分類

G06F 21/31 (2013.01)		G06F	21/31	
G05B 23/02 (2006.01)		G05B	23/02	Z
G06F 21/32 (2013.01)		G06F	21/32	
G06F 21/35 (2013.01)		G06F	21/35	

請求項の数　9　（全32頁）

(21)出願番号　特願2017-139311(P2017-139311)
(22)出願日　平成29年7月18日(2017.7.18)
(65)公開番号　特開2018-14099(P2018-14099A)
(43)公開日　平成30年1月25日(2018.1.25)
審査請求日　令和2年7月20日(2020.7.20)
(31)優先権主張番号　15/214,949
(32)優先日　平成28年7月20日(2016.7.20)
(33)優先権主張国・地域又は機関
米国(US)

(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　100096091
弁理士　井上 誠一
(72)発明者　トッド・エム・トープケ
アメリカ合衆国 ミネソタ州 ５５３４７ エデン プレーリー ポーチライト レーン １５８１５
(72)発明者　ジョセフ・ディー・フィッシャー

最終頁に続く

(54)【発明の名称】　プロセスプラントにおけるユーザインターフェイスデバイスに対する二要素認証

(57)【特許請求の範囲】

【請求項１】

プロセスプラント内のユーザインターフェイスデバイスにおいて二要素認証を提供する方法であって、

前記ユーザインターフェイスデバイスにおける１つ以上のプロセッサにおいて、ユーザの第１のタイプの識別情報を受信するステップであって、前記ユーザインターフェイスデバイスがプロセスプラント内のプラント資産に接続する一体型の入出力能力を含み、前記ユーザインターフェイスデバイスの電気的特性は本質的安全レベルに関する所定の電気的閾値以下となるように本質的に安全に動作するように構成されている、ステップと、

前記１つ以上のプロセッサにおいて、ユーザの第２のタイプの識別情報を受信するステップと、

前記１つ以上のプロセッサによって、前記ユーザの第１及び第２のタイプの識別情報それぞれを前記ユーザインターフェイスデバイスにアクセスする権限が与えられた複数のユーザの複数のタイプの識別情報と比較するステップと、

前記第１及び第２のタイプの識別情報それぞれが同じ権限が与えられたユーザに対応する場合に、前記１つ以上のプロセッサによって、前記ユーザに権限が与えられたアクセスを提供するステップと、を有し、

前記ユーザが前記ユーザインターフェイスデバイスに対して権限が与えられたアクセスを有し、前記ユーザインターフェイスデバイスがプラント資産に接続される場合、前記ユーザインターフェイスデバイスは前記プロセスプラント内の前記接続されたプラント資産と

通信するよう構成される、方法。
【請求項２】
前記第１のタイプの識別情報は、識別装置から提供される、または、前記ユーザの身体的特徴であり、前記第２のタイプの識別情報は前記ユーザによって提供される知識ベースの識別情報である、請求項１に記載の方法。
【請求項３】
前記第１のタイプの識別情報は、電子識別カードから短距離通信リンクを介して受信され、
前記第２のタイプの識別情報は、前記ユーザによって前記ユーザインターフェイスデバイスを介して入力されるユーザログイン情報である、請求項１又は請求項２に記載の方法。
【請求項４】
前記１つ以上のプロセッサによって、前記ユーザの権限レベルを決定するステップであって、前記権限レベルは、前記ユーザがアクセスする権限が与えられた１つ以上のプラント資産または前記ユーザが前記ユーザインターフェイスデバイスで実行する権限が与えられた１つ以上の機能を含む前記ユーザに割り当てられたアクセス権のセットを含む、ステップと、
前記１つ以上のプロセッサによって、前記ユーザの前記権限レベルに基づいて、前記接続されたプラント資産にアクセスする権限がユーザに与えられているかを決定するステップと、をさらに備える、請求項１乃至請求項３のいずれか１項に記載の方法。
【請求項５】
前記ユーザに対して権限レベルを決定するステップは、
前記１つ以上のプロセッサにおいて、前記ユーザインターフェイスデバイスにアクセスする権限が与えられた複数のユーザそれぞれに割り当てられたアクセス権のセットを取得し、
前記１つ以上のプロセッサによって、前記ユーザに割り当てられた前記アクセス権のセットを識別することを含む、請求項４に記載の方法。
【請求項６】
前記ユーザに対する前記権限レベルは、さらに、（ｉ）前記ユーザが前記１つ以上のプラント資産または前記ユーザインターフェイスデバイスでの１つ以上の機能にアクセスする権限が与えられた時間長、または（ｉｉ）前記ユーザが前記１つ以上のプラント資産にアクセスする権限が与えられたプラント領域、の少なくとも１つをさらに含む、請求項４又は請求項５に記載の方法。
【請求項７】
前記１つ以上のプロセッサによって、前記ユーザインターフェイスデバイスに割り当てられたアクセス権のセットを取得するステップと、
前記１つ以上のプロセッサによって、前記ユーザインターフェイスデバイスに割り当てられた前記アクセス権のセットに基づいて、前記接続されたプラント資産にアクセスする権限が前記ユーザインターフェイスデバイスに与えられたかを決定するステップと、をさらに備える、請求項１乃至請求項６のいずれか１項に記載の方法。
【請求項８】
前記接続されたプラント資産にアクセスする権限が前記ユーザ及び前記ユーザインターフェイスデバイスに与えられた場合、前記１つ以上のプロセッサによって、前記接続されたプラント資産に動作を実施する機能が実行される、請求項７に記載の方法。
【請求項９】
プロセスプラント内で二要素認証を提供するユーザインターフェイスデバイスであって、
１つ以上のプロセッサと、
前記プロセスプラント内のプラント資産に接続する一体型の入出力構成要素と、
前記１つ以上のプロセッサ及び前記一体型の入出力構成要素に接続され、指示を記憶する非一時的コンピュータ可読媒体と、を備え、前記指示は、前記１つ以上のプロセッサによって実行されると、前記ユーザインターフェイスデバイスが、請求項１乃至請求項８のいずれか１項に記載のステップを実行するよう構成される、ユーザインターフェイスデバイ

ス。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、概ねプロセス制御システムに関し、特に、プロセスプラントにおけるユーザを認証するために２タイプの識別（ＩＤ）を受信することに関わる。
【背景技術】
【０００２】
化学、石油、または他のプロセスで使用される、分散型プロセス制御システムは、一般的に、１つ以上のプロセスコントローラと、少なくとも１つのホストまたはオペレータワークステーションと１つ以上のフィールドデバイスに、アナログ、デジタル、またはアナログ／デジタル複合バス、または無線通信リンクまたはネットワークを介して通信可能に接続された入出力（Ｉ／Ｏ）装置を含む。フィールドデバイス、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、レベル及び流量センサ）は、プロセス環境の内部に位置し、一般的に例えばバルブを開閉したり、あるいは、測定プロセスパラメータなどの物理的またはプロセス制御機能を行って、プロセスプラントまたはシステム内で実行する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のようなスマートフィールドデバイスも、制御計算、アラーム機能、及び一般的にコントローラ内で共通に実行される他の制御機能を実行することもできる。プロセスコントローラは、一般的にプラント環境内に位置してもいるが、センサまたはフィールドデバイス及び／またはフィールドデバイスに関連する他の情報によって行われたプロセス測定を表す信号を受信し、例えばプロセス制御決定を下す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し、制御信号を受信した情報にもとづいて生成し、ＨＡＲＴ（登録商標）、無線ＨＡＲＴ（登録商標）、及びＦＯＵＮＤＡＴＩＯＮ（登録商標）フィールドバスフィールドデバイスなどのようなフィールドデバイスで実行中の制御モジュールまたはブロックと調和させる。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することによって、プロセスプラントまたはシステムの少なくとも一部の操作を制御する。
【０００３】
フィールドデバイスと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１つ以上の他のハードウェア装置、例えば、一般的に、ただし常にではないが、より過酷なプラント環境から離隔した制御室または他の位置に載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、または演算装置、データヒストリアン、レポートジェネレータ、中央データベース、または他の集中管理演算装置上で利用できるようになる。これらのハードウェア装置は、それぞれ、一般的に、ただし常にではないが、プロセスプラントまたはプロセスプラントの一部にわたって集中化されている。これらのハードウェア装置は、例えば、オペレータがプロセスの制御及び／またはプロセスプラントの操作に対する機能、例えば、プロセス制御ルーチンの設定を変更すること、コントローラまたはフィールドデバイス内の制御モジュールの操作を変更すること、プロセスの現在の状態を表示すること、フィールドデバイスやコントローラが生成したアラームを表示すること、人材育成またはプロセス制御ソフトウェアのテストを目的とするプロセスの操作をシミュレートすること、構成データベースなどを維持し、更新することなどを実行できるようにするアプリケーションを実行する。ハードウェア装置、コントローラ、及びフィールドデバイスが利用するデータハイウェイは、有線通信パス、無線通信パス、または有線及び無線複合通信パスを含んでいてもよい。
【０００４】
一例として、Ｅｍｅｒｓｏｎ　Ｐｒｏｃｅｓｓ　Ｍａｎａｇｅｍｅｎｔが販売するＤｅｌｔａＶ（商標）制御システムは、プロセスプラント内の様々な場所に位置する異なるデバイス内に保存され、それによって実行される複数のアプリケーションを含む。構成アプリケ

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演算装置内にあるもので、ユーザがプロセス制御モジュールを生成したり、変更したりできるとともにこれらのプロセス制御モジュールを専用の分散型コントローラにデータハイウェイを介してダウンロードすることができるようになる。一般的に、これらの制御モジュールは、入力に基づいて制御スキーム内で機能を実行し、制御スキーム内の他の機能ブロックへの出力を提供する、通信可能に相互接続した機能ブロックから構成される。また、構成アプリケーションにより、コンギギュレーションの設計者が表示アプリケーションで使用してデータをオペレータに対して表示するオペレータインターフェースを生成または変更することができるとともに、オペレータがプロセス制御ルーチン内で、設定点などのような設定を変更できるようになる。それぞれの専用コントローラと、場合によっては１つ以上のフィールドデバイスは、それに割り当てられ、ダウンロードされた制御モジュールを実行して実際のプロセス制御機能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保存し実行する。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とデータハイウェイと通信可能に接続された１つ以上のリモート演算装置）で実行可能な表示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介してデータを受信し、このデータをプロセス制御システムデザイナー、オペレータ、またはユーザにオペレータインターフェースを使って表示し、オペレータ用の表示、エンジニア用の表示、また技術者用の表示など、異なる多数の表示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、一般的に、データハイウェイに提供されたデータの一部またはすべてを収集または保存するデータヒストリアンデバイスによって保存及び実行される一方で、構成データベースアプリケーションをデータハイウェイに取り付けたさらに別のコンピュータで実行して、現在のプロセス制御ルーチン構成とそれに伴うデータを保存することができる。あるいは、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にあってもよい。

【０００５】

上述したように、オペレータ表示アプリケーションは、一般的に１つ以上のワークステーションでシステムベースで実行され、プラント内の制御システムまたはデバイスの運転状態に関して、オペレータまたは保守作業員にディスプレイを提供する。一般的に、これらの表示はプロセスプラント内のコントローラやデバイスによって生成されたアラームを受信するアラーム表示の形態をとり、プロセスプラント内のコントローラや他の装置の運転状態を示すディスプレイや、プロセスプラント内のデバイスの運転状態を示す保守ディスプレイなどを制御する。これらのディスプレイは一般的に周知の方法でプロセスプラント内のプロセス制御モジュールやデバイスから受取った情報やデータを表示するように構成されている。周知のシステムでは、ディスプレイは、物理的または論理的要素に通信可能に繋がった物理的または論理的要素に関連付けられたグラフィックを有し、物理的または論理的要素に関するデータを受信する。グラフィックは、受信したデータに基づいて表示画面上で変更され、例えば、タンク内が半分充填されていることをイラストで示したり、流量センサなどによって測定した流れをイラストで示すようにすることができる。

【０００６】

周知のシステムでは、オペレータは、携帯型または他の可搬式演算装置（例えば、ユーザインターフェース（ＵＩ）デバイス）を使って、プロセス制御装置（例えば、コントローラ、フィールドデバイスなど）、回転機器（例えば、モータ、ポンプ、圧縮機、駆動装置）、機械式容器（例えば、タンク、パイプなど）、電力配電装置（例えば、スイッチギヤ、モータ制御センタ）、あるいは、プロセスプラント内の他の設備などを含むことができる、プロセスプラント内のプラント資産に関する構成、トラブルシューティング、キャリブレーション、または実行することができる。例えば、オペレータは、ＵＩ装置をフィールドデバイスに物理的に取り付け、そのＵＩ装置を介してフィールドデバイスと通信してもよい。しかし、ＵＩ装置は、例えば、ログイン情報を入力するなどの認証要求は備えていない。結果として、プロセスプラント内の誰もがＵＩ装置を獲得でき、プラント資産を変更できる。これにより権限のない者がプロセスプラント内のいずれかのプラント資産に

アクセスすることができる。
【発明の概要】
【０００７】
ＵＩ装置は、二要素認証を行って、ユーザがＵＩ装置にアクセスし、プロセス制御装置に関する、あるいは、そのＵＩ装置に接続されたプラント資産を行うことができるようにする。さらに具体的には、ＵＩ装置は、ユーザを一意的に識別するユーザに対する第１のタイプの識別情報を受取ることができる。第１のタイプの識別情報は、識別装置からのものでもよく、また、ユーザの身体的特徴であってもよい。例えば、ＵＩ装置は、近距離通信（ＮＦＣ）信号のような無線周波数識別（ＲＦＩＤ）タグをユーザに属する電子ＩＤカードから受取ってもよい。ＲＦＩＤタグは、ユーザを一意に識別する従業員ＩＤ番号を含んでいてもよい。ＵＩ装置は従業員ＩＤ番号を保存された従業員ＩＤ番号と比較してユーザを確認及び識別してもよい。
【０００８】
さらに、ＵＩ装置はユーザ用の第２のタイプの識別情報を受信してもよい。第２のタイプの識別情報は、ユーザが知っている情報である情報に基づいた知識であってもよい。例えば、第２のタイプの識別情報は、ユーザが提供したユーザ名及びパスワードのようなユーザログイン情報であってもよい。ユーザ名及びパスワードは、保存したユーザ名やパスワードの組み合わせと比較して、再度ユーザを確認し識別してもよい。ＵＩ装置がＲＦＩＤタグに基づいて同じユーザを識別する場合、ユーザは認証され、ＵＩ装置へのアクセスが許可される。結果、ユーザは、接続したｒ個のプラント資産に対する操作を行うことができる。また、別の例では、第２のタイプの識別情報は一意的にユーザを識別するパスコード／個人識別番号（ＰＩＮ）であってもよい。パスコードは、４桁の数字などの数値のパスワードでも、またはＵＩ装置のスワイプパターンでもよい。
【０００９】
反対に、ＲＦＩＤタグが保存した従業員ＩＤ番号のうちの１つに対応していない場合には、ユーザ名及び／またはパスワードは保存したユーザ名及びパスワードの組み合わせのうちの１つに対応しない、またはＲＦＩＤタグ及びユーザのログイン情報は、同じユーザに対応せず、ユーザは、ＵＩ装置へのアクセスが拒否される。よって、ユーザは、接続されたプラント資産に対する操作を行うことができない。
【００１０】
いくつかの実施形態では、ユーザ認証に加え、ＵＩ装置は、ユーザとＵＩ装置が接続されたプラント資産に関する操作を実行することに対して権限があるどうかを判断する。また、ＵＩ装置は、ユーザ及びＵＩ装置に対する権限の程度、例えば、権限を有する時間、ユーザとＵＩ装置が実行の権限を付与された機能、ＵＩ装置にライセンスを与えるソフトウェアなどを決定することができる。ユーザが、ユーザがアクセスを許可されていないプラント資産にアクセスしようとすると、ＵＩ装置は、ユーザにアクセスが拒否されたことを通知する表示をすることができる。また、ＵＩ装置は、権限のないユーザが特定のプラント資産にアクセスしようとしていることを示す通知をサーバに送信してもよい。システム管理者は、通知を表示し、アクションを起こすことができる。例えば、システム管理者は、権限のないユーザに、追加の権限を追加して、その権限のないユーザが特定のプラント資産へのアクセス権を持つようにすることができる。
【図面の簡単な説明】
【００１１】
【図１Ａ】図１Ａは、二要素認証を行うＵＩ装置を含むプロセスプラント内に配置された分散型プロセス制御ネットワークのブロック図である。
【００１２】
【図１Ｂ】図１Ｂは、図１Ａに示されているプロセスプラント内の電子識別カード、ＵＩ装置、及び１つまたは複数のプロセス制御装置との間の相互作用の例を示すブロック図である。
【００１３】

【図１Ｃ】図１Ｃは、図１Ａに略図で示すＵＩ装置の例のブロック図である。
【００１４】
【図２Ａ】図２Ａ～２Ｂは、二要素認証プロセスの間にＵＩ装置上に示された画面表示の例を示す。
【図２Ｂ】同上。
【００１５】
【図３Ａ】図３Ａ～３Ｃは、ユーザの権限レベルを決定するために、サーバによって生成され、ＵＩ装置に提供することができるデータテーブルの例を示す。
【図３Ｂ】同上。
【図３Ｃ】同上。
【００１６】
【図４】図４は、ＵＩ装置上で二要素認証を行うための方法の例示するフロー図である。
【００１７】
【図５】図５は、ユーザが特定のプラント資産にアクセスしなければならない権限レベルを決定するための方法を例示するフロー図である。
【００１８】
【図６】図６は、アクセス権のセットを生成し、ユーザとＵＩ装置にアクセス権を割り当てるための方法を例示するフロー図である。
【発明を実施するための形態】
【００１９】
図１Ａは、プロセス制御システムまたはプロセスプラント１０内で作動するプロセス制御ネットワーク１００を例示的するブロック図である。プロセス制御ネットワーク１００は、他の様々なデバイス間で直接または間接的接続を提供するネットワークバックボーン１０５を含んでいてもよい。ネットワークバックボーン１０５に接続されたデバイスは、様々な実施形態において、アクセスポイント７２、携帯型も含むＵＩ装置１１２、サーバ１５０、コントローラ１１、入力／出力（Ｉ／Ｏ）カード２６及び２８、有線フィールドデバイス１５～２２、無線ゲートウェイ３５、及び無線通信ネットワーク７０の組み合わせを含む。通信ネットワーク７０は、無線フィールドデバイス４０～４６、無線アダプタ５２ａ及び５２ｂ、アクセスポイント５５ａ及び５５ｂ、及びルータ５８を含む無線デバイス４０～５８を含んでいてもよい。無線アダプタ５２ａ及び５２ｂは、それぞれ、非無線フィールドデバイス４８及び５０に接続されてもよい。コントローラ１１は、プロセッサ３０、メモリ３２、及び１つまたは複数の制御ルーチン３８を含んでいてもよい。図１Ａは、ネットワークバックボーン１０５に接続された装置のいくつかの単一のもののみを示しているが、デバイスのそれぞれは、ネットワークバックボーン１０５上では、複数のインスタンスを持ちうるものであり、実際、プロセスプラント１０は複数のネットワークバックボーン１０５を含んでいてもよいことは理解できよう。
【００２０】
ＵＩ装置１１２は、ネットワークバックボーン１０５を介してコントローラ１１及び無線ゲートウェイ３５に通信可能に接続されてもよい。コントローラ１１は、入力／出力（Ｉ／Ｏ）カード２６及び２８を介して有線フィールドデバイス１５～２２に通信可能に接続されてもよいし、ネットワークバックボーン１０５と無線ゲートウェイ３５を介して無線フィールドデバイス４０～４６に通信可能に接続されてもよい。コントローラ１１は、フィールドデバイス１５～２２及び４０～５０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施するように動作することができる。一例として、Ｅｍｅｒｓｏｎ　Ｐｒｏｃｅｓｓ　Ｍａｎａｇｅｍｅｎｔによって販売されているＤｅｌｔａＶ（商標）コントローラなどのコントローラ１１は、プロセス制御ネットワークバックボーン１０５に通信可能に接続されている。コントローラ１１はまた、例えば、標準の４～２０ｍＡデバイス、Ｉ／Ｏカード２６、２８、及び／またはＦＯＵＮＤＡＴＩＯＮ（登録商標）フィールドバスプロトコル、ＨＡＲＴ（登録商標）プロトコル、無線ＨＡＲＴ（登録商標）プロトコルなどのようなスマート通信プロトコルに関連付けられた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フィールドデバイス１５～２２及び４０～５０に通信可能に接続してもよい。図１Ａに示す実施形態では、コントローラ１１、フィールドデバイス１５～２２及びＩ／Ｏカード２６、２８は、有線デバイスであり、フィールドデバイス４０～４６無線フィールドデバイスである。

【００２１】

いくつかの実施形態では、ＵＩ装置１１２は、プロセスプラント内のフィールドデバイス１５～２２、４０～５０のいずれかの箇所に搬入できる。ＵＩ装置１１２は、キャリブレーション、構成、トラブルシューティング、監視、制御、またはフィールドデバイス１５～２２、４０～５０の他のあらゆる適した操作を行うために一時的に有線及び／または無線接続７６を介してフィールドデバイス１５～２２、４０～５０に接続してもよい。さらに、ＵＩ装置１１２は、キャリブレーション、構成、トラブルシューティング、監視、制御、またはコントローラ１１の他のあらゆる適した操作を行うために一時的に有線及び／または無線接続を介してコントローラ１１に接続してもよい。また、ＵＩ装置１１２は、較正、構成、トラブルシューティング、監視、制御、またはプラント資産の他の適した操作のために、一時的に他のプラント資産（例えば、回転機器、機械式容器、電力配電装置など）に接続してもよい。

【００２２】

ＵＩ装置１１２の動作において、ＵＩ装置１１２は、いくつかの実施形態では、ＵＩ装置１１２が、入力インタフェースを介して入力を受け入れ、ディスプレイに出力を提供することができるように、ユーザインターフェース（ＵＩ）を実行してもよい。ＵＩ装置１１２は、サーバ１５０からデータ（例えば、プロセスパラメータ、アクセス権、ログデータ、センサーデータ及び／または他のキャプチャまたは保存可能なデータなどのようなプロセス関連のデータ）を受信することができる。他の実施形態では、ＵＩをサーバ１５０で全体的または部分的に実行して、サーバ１５０が表示データをＵＩ装置１１２に送信してもよい。ＵＩ装置１１２は、ＵＩデータ（表示データ及び許可データを含んでいてもよい）をコントローラ１１、無線ゲートウェイ３５、またはサーバ１５０のようなプロセス制御ネットワーク１００内の他のノードからバックボーン１０５を介して受信してもよい。

【００２３】

いくつかの実施形態では、アクセス権は、例えば、システム管理者がサーバ１５０で生成してもよい。各アクセス権は読み取り専用アクセス、読み取り／書き込みアクセス、キャリブレーション機能のためのアクセス、構成機能のためのアクセスなど、特定のプラント資産へのアクセスのレベルを指定することができる。また、システム管理者は、プロセスプラント内のユーザとＵＩ装置にアクセス権を割り当ててもよい。いくつかの実施形態では、サーバ１５０は、アクセス権、プロセスプラント内の権限を有するユーザ、プロセスプラント内のＵＩ装置の表示、及びアクセス権、ユーザ、及びＵＩ装置の間の関連付けを保存する１つ以上のデータベースに通信可能に接続してもよい。対応するユーザと各許可に割り当てられたＵＩ装置のアクセス権ならびに表示は、ＵＩ装置１１２に送信できる。

【００２４】

したがって、ＵＩ装置１１２は、ユーザ及び／またはＵＩ装置１１２に割り当てられたアクセス権を使用して、ＵＩ装置１１２に接続されたプラント資産に対してユーザが有する権限レベルルを決定することができる。本明細書では、ユーザの権限レベルは、プロセスプラント内のプラント資産に対してユーザが有するアクセスの複合レベルを指すこととする。アクセスの複合レベルは、ユーザ及び／またはＵＩ装置１１２に割り当てられたアクセス権のセットに基づき、各アクセス権は、特定のプラント資産へのアクセスレベルを指定するものでもよい。いくつかの実施形態では、ユーザの権限レベルは、特定のプラント資産に対してユーザが有するアクセスの複合レベルも指すこととする。アクセスの複合レベルは、ユーザ及び／またはＵＩ装置１１２に割り当てられたアクセス権それぞれに基づき、各アクセス権は、特定のプラント資産へのアクセスレベルを指定するものでもよい。

【００２５】

また、本明細書では、プラント資産は、プロセス制御装置（例えば、コントローラ、フィ

ールドデバイスなど）、回転機器（例えば、モータ、ポンプ、圧縮機、駆動装置）、機械式容器（例えば、タンク、パイプなど）、電力配電装置（例えば、スイッチギヤ、モータ制御センタ）、あるいは、プロセスプラント内の任意の他の設備などを含んでいてもよい。単に例示を容易にするために、明細書では、ＵＩ装置がプロセス制御装置に接続されているシナリオを記述する。しかし、ＵＩ装置１１２は、プロセスプラント内の任意のプラント資産に接続することもできる。

【００２６】

ＵＩ装置１１２で受信されたＵＩデータに基づいて、ＵＩ装置１１２は、ユーザが認証されているかどうか、そしてユーザは、特定のプロセス制御装置または他のプラント資産またはプロセス制御装置または他のプラント資産で実行される機能へのアクセスを許可されているかどうかを示す出力（すなわち、視覚的表現またはグラフィック）を提供する。例えば、ＵＩ装置１１２は、下記に図２Ａを参照して後にさらに詳しく説明するように、ユーザに電子ＩＤカードをスキャンするように要求するＩＤスキャン表示することができる。また、ＵＩ装置１１２は、図２Ｂを参照して後にさらに詳しく説明するように、ユーザにユーザ名とパスワードまたはパスコード／ＰＩＮ番号を入力するように要求するユーザログイン画面を表示することもできる。また、ユーザは、ＵＩ装置１１２に入力を提供することによって、プロセスの制御に影響を与えることができる。例示のため、ＵＩ装置１１２は、ＵＩ装置１１２に接続されているプロセス制御装置により測定されたプロセスパラメータを指示することができる。ユーザは、プロセス制御装置によって得られた測定値をキャリブレーションするためにＵＩ装置１１２とやりとりすることができる。

【００２７】

特定の実施形態では、ＵＩ装置１１２は、シンクライアント、ウェブクライアント、またはシッククライアントなど、どのタイプのクライアントでも実行可能である。例えばＵＩ装置１１２は、（例えば、ウェアラブルデバイスで）ＵＩ装置１１２のメモリやバッテリー電源に制限がある場合などに、ＵＩ装置１１２の動作に必要な処理の大部分を他のノード、コンピュータ、ＵＩ装置、またはサーバに依存し得る。そのような例では、ＵＩ装置１１２は、サーバ１５０またはその他のＵＩ装置と通信することができ、サーバ１５０または他のＵＩ装置１１２は、１つ以上の他のノード（例えば、サーバ）とプロセス制御ネットワーク１００上で通信することができ、表示データ、アクセス権データ、及び／またはプロセスデータを決定し、ＵＩ装置１１２に送信することができる。さらに、ＵＩ装置１１２は、サーバ１５０は、ユーザ入力に関連するデータを処理し、それに応じて動作することができるように、サーバ１５０に受信したユーザ入力に関連するデータを渡すことができる。換言すれば、ＵＩ装置１１２は、グラフィックスをレンダリングするより多くを行うことができ、１つの以上のノード、またはデータを保存し、ＵＩ装置１１２の動作に必要なルーチンを実行するサーバに対してポータルとして動作することができる。シンクライアントＵＩ装置は、ＵＩ装置１１２のための最低限のハードウェア要件の利点を提供する。

【００２８】

他の実施形態では、ＵＩ装置１１２は、ウェブクライアントである。そのような実施形態では、ＵＩ装置１１２のユーザは、ＵＩ装置１１２にブラウザを介してプロセス制御システムとやりとりすることができる。ブラウザにより、ユーザは、バックボーン１０５を介して別のノードまたは（サーバ１５０のような）サーバにおいてデータとリソースにアクセスできるようになる。例えば、ブラウザは、ブラウザが制御及び／または処理の一部または全部を監視するためのグラフィックを描写することができ、そのようなサーバ１５０から表示データ、アクセス権データ、またはプロセスパラメータデータなどのＵＩデータを受信することもできる。ブラウザはまた、ユーザ入力（例えば、グラフィック上でのマウスクリック）を受信することができる。ユーザが入力することにより、ブラウザがサーバ１５０に保存された情報リソースを取得する、または情報リソースにアクセスする。例えば、マウスクリックにより、ブラウザが（サーバ１５０から）クリックしたグラフィックが含む情報を取得して表示する。

【００２９】
さらに他の実施形態では、ＵＩ装置１１２の処理の大部分は、ＵＩ装置１１２で行われてもよい。例えば、ＵＩ装置１１２は、ユーザの権限レベルを決定してもよい。ＵＩ装置１１２はまた、データをローカルに保存、アクセス、分析できる。
【００３０】
本明細書では、ユーザは、ＵＩ装置１１２とやりとりすることによって、フィールドデバイス１５～２２、４０～５０、コントローラ１１、回転機器（例えば、モータ、ポンプ、圧縮機、駆動装置）、機械式容器（例えば、タンク、パイプなど）、電力配電装置（例えば、スイッチギヤ、モータ制御センタ）、あるいは、プロセスプラント内の他の任意の設備などのいずれかのようなプロセス制御ネットワーク１００の１つ以上のプラント資産を監視、構成、トラブルシューティング、キャリブレーションまたは制御してもよい。また、ユーザはＵＩ装置１１２とやりとりして、例えば、コントローラ１１に保存された制御ルーチンに関連付けられたパラメータを変更または変化させてもよい。コントローラ１１のプロセッサ３０は、制御ループを含み得る１つ以上のプロセス制御ルーチン（メモリ３２内に保存）を実行または監視する。ロセッサ３０は、フィールドデバイス１５～２２及び４０～５０、及びバックボーン１０５に通信可能に接続された他のノードと通信することができる。本明細書に記載の任意の制御ルーチンまたはモジュール（品質予測及び不良検出モジュールまたは機能ブロックを含む）は、そのほうが好ましければ、その一部を別のコントローラまたは他のデバイスで実行または実施することができるものとする。同様に、本命最初に記載の制御ルーチンまたはモジュールは、プロセス制御システム内で実行されるべきものであり、ソフトウェア、ファームウェア、ハードウェアなどを含むいかなる形態でもよい。制御ルーチンは、オブジェクト指向プログラミング、ラダー論理、シーケンシャルファンクションチャート、機能ブロック図、電子デバイス記述言語（ＥＤＤＬ）、フィールドデバイスの統合（ＦＤＩ）を使用して、または任意の他のソフトウェアプログラミング言語またはデザインパラダイムを使用して、任意の所望のソフトウェア形式で実行することができる。特に、制御ルーチンは、ＵＩ装置１１２を介してユーザによって実行するものでもよい。制御ルーチンは、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、任意の所望の種類のメモリに保存されてもよい。同様に、制御ルーチンは、例えば、１つ以上のＥＰＲＯＭ、ＥＥＰＲＯＭ、特定用途向け集積回路（ＡＳＩＣ）、または任意の他のハードウェアまたはファームウェア要素をハードコードしてもよい。従って、コントローラ１１は、任意の所望の方法で制御戦略または制御ルーチンを実行するために（特定の実施形態においては、ユーザによって、ＵＩ装置１１２を用いて）構成することができる。制御ルーチンに加えて、ＵＩ装置１１２は、コントローラ１１とやりとりをして他の機能を実施したり、他のタイプのデータを送信／受信する。
【００３１】
図１Ａをさらに参照すると、無線フィールドデバイス４０～４６は、無線ＨＡＲＴプロトコルのような無線プロトコルを用いて無線ネットワーク７０で通信する。特定の実施形態では、ＵＩ装置１１２は、無線ネットワーク７０を使用して無線フィールドデバイス４０～４６と通信することができるように構成してもよい。このような無線フィールドデバイス４０～４６は、直接（例えば、無線プロトコルを使用して）無線で通信できるようにも構成されるプロセス制御ネットワーク１００の１つ以上の他のノードと通信することができる。無線で通信するように構成されていない１つ以上の他のノードと通信するため、無線フィールドデバイス４０～４６は、バックボーン１０５に接続された無線ゲートウェイ３５を利用することができる。もちろん、フィールドデバイス１５～２２及び４０～４６は、任意の他の所望の規格（単数または複数）または将来開発される任意の規格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などのプロトコルに準拠してもよい。
【００３２】
無線ゲートウェイ３５は、無線通信ネットワーク７０の様々な無線デバイス４０～５８へのアクセスを提供することができるプロバイダ装置１１０の一例である。特に、無線ゲー

トウェイ３５は、無線デバイス４０～５８と、（図１Ａのコントローラ１１を含む）プロセス制御ネットワーク１００の他のノードとの間の通信接続を提供する。無線ゲートウェイ３５は、有線及び無線プロトコルスタックの層（例えば、アドレス変換、ルーティング、パケットの分割、優先順位付け、等）を下げるために、場合によっては、共有の層または有線及び無線プロトコルスタックの層をトンネリングしながら、ルーティング、バッファリング、及びタイミングサービスによって、通信接続を提供する。他の場合には、無線ゲートウェイ３５は、任意のプロトコル層を共有しない有線及び無線プロトコル間でコマンドを変換することができる。

【００３３】

有線フィールドデバイス１５～２２と同様に、無線ネットワーク７０の無線フィールドデバイス４０～４６は、プロセスプラント１０内で物理的制御機能（例えば、バルブの開閉やプロセスパラメータの測定）を実行することができる。しかしながら、無線フィールドデバイス４０～４６は、ネットワーク７０の無線プロトコルを用いて通信するように構成されている。このように、無線フィールドデバイス４０～４６、無線ゲートウェイ、及び無線ネットワーク７０のその他の無線ノード５２～５８は、無線通信パケットの生産者と消費者である。

【００３４】

いくつかのシナリオでは、無線ネットワーク７０は、非無線デバイスを含んでいてもよい。例えば、図１Ａのフィールドデバイス４８は、従来の４～２０ｍＡデバイス及びフィールドデバイス５０は、従来の有線ＨＡＲＴデバイスであってもよい。ネットワーク７０内で通信するために、フィールドデバイス４８及び５０は、無線アダプタ（ＷＡ）５２ａ、または５２ｂを介して無線通信ネットワーク７０に接続されてもよい。また、無線アダプタ部５２ａ、５２ｂは、Ｆｏｕｎｄａｔｉｏｎ（登録商標）はフィールドバス、ＰＲＯＦＩＢＵＳ、ＤｅｖｉｃｅＮｅｔ等のような他の通信プロトコルをサポートすることができる。さらに、無線ネットワーク７０は、無線ゲートウェイ３５との有線通信における別個の物理デバイスであってもよいし、一体装置として無線ゲートウェイ３５が設けられていてもよいし、１つ以上のネットワークアクセスポイント５５ａ、５５ｂを含んでいてもよい。無線ネットワーク７０は、無線通信ネットワーク７０内の１つの無線デバイスから別の無線デバイスにパケットを転送するために、１つ以上のルータ５８を含むこともできる。無線デバイス３２～４６と５２～５８は、互いに、そして無線ゲートウェイ３５と無線通信ネットワーク７０の無線リンク６０上で通信することができる。

【００３５】

特定の実施形態では、プロセス制御ネットワーク１００は他の無線プロトコルを使って通信するネットワークバックボーン１０５に接続された他のノードを含んでいてもよい。例えば、プロセス制御ネットワーク１００は、ＷｉＦｉ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のような他の無線プロトコルを利用する１つ以上の無線アクセスポイント７２、ＷｉＭＡＸ（マイクロ波アクセスのための世界的相互運用性）、ＬＴＥ（ロングタームエボリューション）、または他のＩＴＵ－Ｒ（国際電気通信連合無線通信部門）互換プロトコルのようなモバイル通信プロトコル、ＮＦＣやＢｌｕｅｔｏｏｔｈ（登録商標）、または他の無線通信プロトコルのような短波長の無線通信などを含んでいてもよい。一般的には、このような無線アクセスポイント７２により、携帯型または他のポータブル演算装置（例えば、ＵＩ装置）が無線ネットワーク７０とは異なり、無線ネットワーク７０とは異なる無線プロトコルをサポートしているそれぞれの無線ネットワーク上で通信することができるようになる。例えば、ＵＩ装置は、ユーザがプロセスプラント内で使用す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もよい。いくつかの実施形態では、ＵＩ装置１１２は、無線アクセスポイント７２を使ってプロセス制御ネットワーク１００上で通信する。いくつかのシナリオでは、可搬式演算装置に加え、１つ以上のプロセス制御装置（例えば、コントローラ１１、フィールドデバイス１５～２２、または無線デバイス３５、４０～５８）もアクセスポイント７２によってサポートされた無線ネットワークを使って通信することができる。

【００３６】
図１Ａには、有限数のフィールドデバイス１５～２２、４０～５０を有する単一のコントローラ１１を示すが、これは例示に過ぎず、限定することのない実施形態である。プロセス制御ネットワーク１００のプロバイダ装置に含まれるコントローラ１１の数は、いくつでもよく、どのコントローラ１１も、何台の有線または無線フィールドデバイス１５～２２、４０～５０と通信してプラント１０のプロセスを制御してもよい。さらに、プロセスプラント１０は、何台の無線ゲートウェイ３５、ルータ５８、アクセスポイント５５、７２、及び／または無線通信ネットワーク７０を含んでいてもよい。
【００３７】
二要素認証を行うため、ＵＩ装置１１２は複数のタイプの識別をユーザから受取る。さらに具体的には、ＵＩ装置１１２は、物理的、または固有の識別情報を識別装置（例えば、電子ＩＤカード、社会保険カード、免許証など）、またはユーザデバイスの身体的特徴（例えば、指紋、網膜像など）から第１のタイプの識別情報として受取ってもよい。ＵＩ装置１１２はまた、第２のタイプの識別情報としてユーザが知る知識ベースの識別情報（例えば、ユーザ名とパスワード、電子メールアドレス、生年月日、セキュリティの質問に答え、パスコード／ＰＩＮ番号、など）を受信することができる。
【００３８】
図１Ｂは、ＵＩ装置１１２と、電子ＩＤカード１１０と１つまたは複数のプロセス制御装置１１、１５、４２、回転機器（例えば、モータ、ポンプ、圧縮機、駆動装置）、機械式容器（例えば、タンク、パイプなど）、電力配電装置（例えば、スイッチギヤ、モータ制御センタ）、あるいは、任意の他の設備（例えば、スイッチギヤ、モータ制御センタ、など）またはその他のプラント資産の間の例示の相互作用を示すブロック図である。上述したように、ユーザは、ＵＩ装置１１２を、プロセス制御装置１１、１５、４２の１つに接続して、接続したプロセス制御装置上で監視、制御、構成、トラブルシューティング、キャリブレーション、または任意の他の操作の実行を行うことができる。
【００３９】
いずれの場合も、ユーザが接続したプロセス制御装置で操作を行うことが出来るようになる前に、ＵＩ装置１１２は、二要素認証を使ってユーザを認証し、ユーザが接続したプロセス制御装置にアクセス権があるかどうかを判定する。接続したプロセス制御装置がコントローラ１１である場合、ＵＩ装置１１２はユーザが、コントローラ１１によって制御されたフィールドデバイスに対してアクセス権があるかどうかを判定することができる。いくつかの実施形態では、ユーザは、ユーザがコントローラ１１によって制御されたフィールドデバイスのそれぞれにアクセスできない限り、コントローラ１１にアクセスできない場合もある。
【００４０】
電子ＩＤカード１１０は、表面に識別情報、例えば従業員の写真、従業員の名前などのＩＤが印刷された従業員バッジでもよい。電子ＩＤカード１１０は、ＲＦＩＤまたはＮＦＣ信号のような電子信号を伝達するチップを埋め込んだものでもよい。埋め込みチップには、従業員の識別情報、例えば、プロセスプラントの中の従業員を一意的に識別する従業員ＩＤ番号、従業員のジョブ機能の識別、従業員の名前、または他の適した情報を有するタグ１１４を含んでいてもよい。
【００４１】
ＵＩ装置１１２は、電子データを送受信するための通信ユニットを含む。通信ユニットは、ＲＦＩＤまたはＮＦＣ信号を受信し、復号するＲＦＩＤリーダまたはＮＦＣリーダを含んでいてもよい。よって、ユーザはその電子ＩＤカード１１０をＵＩ装置１１２のＲＦＩＤまたはＮＦＣ通信範囲（例えば、１インチ、３インチ、６インチ、１フィート、３フィートなど）に載置することによって第１のタイプの識別情報をＵＩ装置１１２に提供してもよい。図２Ａは、電子ＩＤカード１１０をスキャンするためのＵＩ装置１１２上で提示できる例示のスクリーンディスプレイ２００を示す図である。例示のスクリーンディスプレイ２００は、ユーザに対して自分の電子ＩＤカード１１０をスキャンするようにとの要

求２１０と、ＵＩ装置１１２が電子ＩＤカード１１０からＲＦＩＤタグを受信したかどうかの識別を含んでいてもよい。例えば、識別は、ＲＦＩＤタグを受取ったときには緑色の背景色で、ＲＦＩＤタグを受取っていないときには赤い背景色でもよい。また別の例では、識別は、ＲＦＩＤタグを受取ったときＵＩ装置１１２からビーという音またはその他の音を発するものでもよい。これにより、ユーザが自分の電子ＩＤカード１１０をＵＩ装置１１２の通信範囲に載置すると、ＲＦＩＤタグ１１４がＵＩ装置１１２に伝達される。すると、ＵＩ装置１１２は、ＲＦＩＤタグが受取ったＩＤを表示する。別の実施形態では、ＵＩ装置１１２は、ＲＦＩＤタグ内の識別情報が認証された後にＲＦＩＤタグが受信したＩＤを表示する。

【００４２】

いくつかの実施形態では、ＵＩ装置１１２は権限を有するユーザのＩＤと、アクセス権を有するユーザのユーザ／従業員ＩＤ番号を保存してもよい。ＵＩ装置１１２は、受信した信号に含まれるユーザ／従業員ＩＤを、権限を有するユーザのＩＤと比較してユーザを認証してもよい。他の実施形態では、ＵＩ装置１１２はユーザ／従業員ＩＤをサーバ１５０に伝送して、サーバ１５０に比較を実行させてもよい。いずれの場合も、ユーザ／従業員ＩＤは権限を有するユーザのＩＤのユーザ／従業員ＩＤのうちの１つと一致し、ＵＩ装置１１２は第２のタイプの識別情報に対するユーザへの要求を表示してもよい。

【００４３】

例えば、ＵＩ装置１１２は、ユーザに対してユーザ名とパスワードなどのユーザログイン情報を入力するように要求してもよい。図２Ｂは、ユーザログイン情報を提供するための、別のスクリーンディスプレイ２５０の例を示す。スクリーンディスプレイ２５０は、ユーザ名を入力するためのテキストフィールド２６０と、パスワードを入力するためのテキストフィールド２７０と、ログインボタン２８０を含む。よって、ユーザは、ユーザ名とパスワードをＵＩ装置１１２上のソフトウェアキーボード表示またはＵＩ装置１１２に取り付けられたハードウェアキーボードを使ってテキストフィールド２６０，２７０に入力してもよい。他の実施形態では、スクリーンディスプレイ２５０は、パスコード／ＰＩＮ番号を入力するためのテキストフィールドを含む。いくつかの実施形態では、ＵＩ装置１１２は、ユーザの第１のタイプの識別情報を認証後にスクリーンディスプレイ２５０を提示してもよい。

【００４４】

第１のタイプの識別情報に類似して、ユーザがログインボタン２８０を選択すると、ＵＩ装置１１２はユーザ名とパスワードを比較してユーザのログイン情報を権限を有するユーザに対して保存する。別の実施形態では、ＵＩ装置１１２はユーザ名とパスワードをサーバ１５０に送って、サーバ１５０に比較を行わせてもよい。ユーザ名とパスワードがユーザ／従業員ＩＤと同じユーザに対してユーザログイン情報と一致すると、ＵＩ装置１１２はユーザを認証する。その結果、ユーザは、ＵＩ装置１１２のアクセスが許可され、それにより、接続したプロセス制御装置または他のプラント資産に対する操作を行うことができるようになる。

【００４５】

２つのタイプの識別情報がＲＦＩＤタグとユーザログイン情報として記述されているが、これらは識別情報の説明上のものにすぎない。第１のタイプの識別情報は、物理的または固有の識別情報のいかなる適したタイプでもよく、また、第２のタイプの識別情報はユーザが提供するいかなる適したタイプのナリッジベースの情報でもよい。さらに、あらゆる適したタイプの識別情報を二要素認証プロセスにおける第１と第２のタイプの識別情報に対して使用してもよい。

【００４６】

図１Ｃは、例示のＵＩ装置１１２のブロック図である。ＵＩ装置１１２は、携帯型デバイスであってもよい。ＵＩ装置１１２は、ディスプレイ８４、１つ以上のプロセッサまたはＣＰＵ８８，メモリ５２、ランダムアクセスメモリ（ＲＡＭ）９０，入力／出力（Ｉ／Ｏ）回路９２、及び通信ユニット８６を備え、ローカルエリアネットワーク、ワイドエリア

ネットワーク、またはその他の適したネットワークを介してデータを送受信する。通信ユニット８６はＮＦＣまたはＲＦＩＤリーダ９８を備え、ＮＦＣまたはＲＦＩＤ信号を受信及び復号してもよい。ＵＩ装置１１２は、コントローラ１１、サーバ１５０及び／または任意の他の適した演算装置と通信することができる。Ｉ／Ｏ回路９２は、ＵＩ装置１１２をコントローラ１１、フィールドデバイス１５～２２、４０～５０、または他のプラント資産を物理的に取り付けるための外部コネクタなどの一体通信コンポーネントを含んでいてもよい。外部コネクタは、特定のコントローラ１１、フィールドデバイス１５～２２、４０～５０、または他のプラント資産と通信することができる一体Ｉ／Ｏ機能を含んでいてもよい。このように、ＵＩ装置１１２は特定のコントローラ１１、フィールドデバイス１５～２２、４０～５０、またはＵＩ装置１１２に接続する他プラント資産と一体化されてもよい。

【００４７】

メモリ５２はオペレーティングシステム７８、ディスプレイ８８を制御してプロセス制御装置または他のプラント資産と通信するコントロールユニット９４、及びユーザを認証し、そのユーザの権限レベルを判定する認証／権限付与モジュール９６とを含んでいてもよい。いくつかの実施形態では、認証／権限付与モジュール９６はユーザが接続されたプラント資産へのアクセス権を有するかどうか、並びにユーザが接続されたプラント資産上で実行の権限を有する操作のタイプを判定する。一度ユーザが特定の機能を実行して接続されたプラント資産（例えば、構成機能）上で操作を行う権限を有すると判定されると、コントロールユニット９４はユーザから入力を受信すること、接続されたプラント資産からの出力を表示すること、そして接続されたプラント資産と通信して接続されたプラント資産の設定を調整することによって、接続されたプラント資産の構成を制御してもよい。

【００４８】

さらに、ＵＩ装置１１２は、ＵＩ装置１１２を、特定の設備資産の近くのような可燃性及び／または爆発性雰囲気を有する危険区域で、その危険区域から退避する必要なく使用できるように、本質的に安全とすることができる。好ましくは、ＵＩ装置１１２は、例えば、ファクトリー・ミューチュアル・リサーチ社、カナダ規格協会、国際電気標準会議、ＡＴＥＸディレクティブ及び／または同様の安全基準準拠することによって本質的安全に対する基準を満たす。ＵＩ装置１１２は、本質的に安全である、すなわち、例えば、ＡＮＳＩ／ＮＥＣ分類システムによるクラスＩ、ディビジョン１領域あるいは、可燃性または爆発性の雰囲気の類似した領域のような危険領域で使用しても安全であると認定することができる。

【００４９】

例えば、ＵＩ装置１１２は安全及び危険領域の両方で使用するのに適した保護筐体を含んでいてもよい。さらに、ＵＩ装置１１２で利用可能な総エネルギー量は、爆発性雰囲気に点火するのに十分な閾値以下でもよい。エネルギーは、電気（例えばスパークの形態）または熱（例えば暑い表面の形態）でもよい。例えば、ＵＩ装置１１２の内部の電圧は、閾値（例えば２９Ｖ）未満でよく、ＵＩ装置１１２を通って流れる電流は、閾値（例えば３００ｍＡ）未満でもよく、ＵＩ装置１１２のいずれかの回路または回路コンポーネントに関連付けられた電力は、閾値ワット数（例えば１．３Ｗ）以下でもよい。ＵＩ装置１１２は、コンポーネントの不具合によってこれらのエネルギーの限度を超えることが無いように保証するために、１つ以上の組み込み冗長性（例えば、自動遮断、冗長構成要素など）を含んでいてもよい。

【００５０】

ユーザとＵＩ装置にプロセス制御装置または他のプラント資産へのアクセス権を与えるために、サーバ１５０は、特定のプロセス制御装置または他のプラント資産へのアクセスのレベルを指定するアクセス権を生成する。例えば、第１のアクセス権により、デバイスからデータを読み取って、監視機能を実行するためのフィールドデバイスＡへのアクセスを許可してもよい。第２のアクセス権により、デバイスへのデータの読み書きを行ってキャリブレーションや構成機能を実行するためのフィールドデバイスＢへのアクセスを許可し

てもよい。さらに、第２のアクセス権は、時間（例えば１時間）と、ユーザがプロセス制御装置にアクセスできるプラント領域を指定してもよい。いくつかの実施形態では、システム管理者はサーバ１５０と相互作用してアクセス権を生成してもよい。

【００５１】

アクセス権を生成することに加え、サーバ１５０は、１人もしくは数人のユーザと、１つもしくは数台のＵＩ装置に各アクセス権を割り当ててもよい。例えば、システム管理者はプロセスプラントにおいて、第１のサブセットのユーザと第１のサブセットのＵＩ装置に第１のアクセス権を与えてもよい。いくつかのシナリオでは、同じアクセス権を付与された各ユーザは、プロセスプラントと同一または類似のジョブ機能を有していてもよい。例えば、プロセスプラントにおけるメンテナンス技術者の各々は、同一のアクセス権を割り当てることができる。いくつかの実施形態では、アクセス権の表示、プロセスプラント内のユーザ、プロセスプラント内のＵＩ装置、及び権限、ユーザ及びＵＩ装置の間の関連付けは、サーバ１５０に通信可能に接続された１つ以上のデータベースに保存してもよい。

【００５２】

図３Ａ～３Ｃは、サーバ１５０によって生成され、１つ以上のデータベースに保存されたデータテーブルの例を示す。例示的なデータテーブルは、例示の目的のみのために示されたものであり、関連する機能は、任意の適切な形式及び／または、生成、保存、及びアクセス許可、ユーザ、及びＵＩの間のアクセス権、ユーザ、ＵＩ装置、及び関連付けを検索するための設計を使用して実行することができる。したがって、権限、ユーザ、及びＵＩ装置間のアクセス権との関連付けは、生成され、保存され、そして任意の適切な方法で検索することができる。さらに、各データテーブルは、いくつかのエントリを含むが、これは単に説明を容易にするためである。各データテーブルは、数十、数百、数千、またはデータ項目の任意の適切な数を含んでいてもよい。

【００５３】

図３Ａは、いくつかのアクセス権の表示を含む例示の権限データテーブル３００を示す図である。各権限は、一意的にアクセス権を識別するアクセス権ＩＤ３０２を含んでいてもよい。各アクセス権は、アクセス権（例えば、フィールドデバイスＡ、フィールドデバイスＢ）及びアクセス権３０６に対するアクセスのタイプ（例えば読み取り専用、読み書きなど）を介してアクセス可能なプラント資産３０４に対する一意的な識別子を含んでいてもよい。さらに、アクセスの権利が与えられたプラントの領域３０８を含んでいてもよい（例えば、プラント領域Ａ、プラント領域Ｂ）。領域は、プロセスプラント内の特別な部屋であってもよく、特定のプラント資産の位置の周りの閾値半径を用いて決定してもよく、プロセスプラント内の建物でもよく、また任意の他の適した領域でもよい。このようにして、ユーザは、ユーザがプラント資産に近接している場合にのみ特別なプラント資産にアクセスしてもよい。いくつかのアクセス権は、すべての領域に対するアクセスが許可されたことを示してもよい。いくつかの実施形態では、アクセス権は、アクセス権を介してアクセス可能なプラント資産３０４に対する一意的な識別子を含んでいなくともよく、代わりにそのアクセス権はプラント領域３０８内のすべてのプラント資産に対するアクセスを提供してもよい。

【００５４】

さらに、アクセス権には、ユーザが実行して対応するプラント資産に対する操作を行うことができる機能３１０を含んでいてもよい（例えば、構成、キャリブレーション、トラブルシューティング、監視、制御）。いくつかの実施形態では、機能はアクセス権３０６に含まれるアクセスのタイプに基づくものでもよい。例えば、アクセス権を読み取り専用のアクセスとし、ユーザがプラント資産に対して書き込みを要求する構成機能を実行できないようにすることもできる。機能はユーザが制御するＵＩ装置１１２上のソフトウェアアプリケーションであっても、ソフトウェアアプリケーションの機能であってもよい。例えば、アクセス権は、ＵＩ装置１１２が特定のプラント資産に接続されたときにユーザがＵＩ装置１１２上でどのソフトウェアアプリケーションにアクセスできるかということを指定することができる。このアクセス権は、特定のソフトウェアアプリケーションを使って

どの機能がユーザからアクセス可能かを指定することもできる。いくつかのアクセス権は、すべての機能に対するアクセスが許可されたことを示してもよい。

【００５５】

さらに、各アクセス権は、対応するプラント資産にアクセスできる時間長３１２を含んでいてもよい。時間長は、無限でもよいし、またはアクセスに対する閾値時間を含んでいてもよい（例えば、３０分、１時間、３時間など）。このようにしてユーザはプラント資産へ閾値時間の間アクセスすることができ、時間切れとなった場合には、ユーザは、プラント資産と相互通信を続けることができなくなるようにしてもよい。

【００５６】

例示の権限データテーブル３００は、アクセス権ＩＤ３０２、デバイス３０４、アクセスタイプ３０６、プラント領域３０８、機能３１０、及び時間長３１２を含む一方、データフィールド、追加の、あるいはより少ない、あるいは別のデータフィールドがそれぞれのアクセス権に含まれていてもよい。いくつかの実施形態では、アクセス権は、システム管理者がサーバ１５０上のユーザインターフェースを介して生成してもよい。

【００５７】

アクセス権を生成することに加え、サーバ１５０は、プロセスプラントのユーザとＵＩ装置にアクセス権を割り当ててもよい。アクセス権を割り当てられたユーザはプラント資産あるいは、ＵＩ装置を使ったときにアクセス権内に含まれるプラント領域内のプラント資産のグループへのアクセスを許可されてもよい。いくつかの実施形態では、ＵＩ装置もＵＩ装置を使用するときにプラント資産にアクセスするユーザのためにプラント資産へのアクセスの提供を必要とする場合もある。他の実施形態では、ユーザとＵＩ装置のいずれか一方が、プラント資産へのアクセス権を得た場合には、ユーザは、ＵＩ装置を介してプラント資産にアクセスできる。

【００５８】

いずれの場合も、図３Ｂは、プロセスプラントで働く数人のユーザの指示を含むユーザデータテーブル３３０の例を示す。ユーザデータテーブル３００は、各ユーザに対するユーザプロファイルを生成するために使用することができる。各ユーザは、一意的にユーザ（例えば、０００１、０００２、０００３、ＸＸＹ、ＡＡＣなど）を識別するユーザＩＤ３３２を有することができる。各ユーザは、（例えば、構成エンジニア、メンテナンス技術者、等）、プロセスプラント内の関連するジョブ機能３３４を有していてもよい。

【００５９】

ユーザのグループを、セキュリティグループ３３６に割り当てることができ、そのセキュリティグループのメンバーの各々には、同じアクセス権を割り当てることができる。例えば、第１のセキュリティグループは、アクセス権１～４を含んでいてもよい。ユーザが第１のセキュリティグループに割り当てられている場合、そのユーザは、自動的にアクセス権１～４のそれぞれに割り当てられる。このようにして、システム管理者は個々に同じセットのアクセス権をいくつかのユーザに割り当てる必要がない。

【００６０】

このシステム管理者はアクセス権をサーバ１５０のユーザインターフェースを介してセキュリティグループに割り当ててもよい。たとえば、システム管理者は、以前にセキュリティグループに割り当てられたアクセス権の指示を見ることができ、また、セキュリティグループ（例えば、アクセス権ＩＤ）に割り当てられる新しいアクセス権の識別子を入力し、いくつかのアクセス権の許可をドロップダウンメニューから選択し、または他の任意の適切な方法で、セキュリティグループにアクセス権を割り当ててもよい。

【００６１】

いくつかの実施形態では、セキュリティグループのメンバーは、このようなプロセスプラント内の同じジョブ機能や役割などのプロセスプラント内の共通の属性を共有するユーザを含んでいてもよい。例えば、第１のセキュリティグループは構成エンジニアのためであり、第２のセキュリティグループは、メンテナンス技術者のためであり、第３のセキュリティグループは、プラントオペレータ、等のためであってもよい。さらに、ユーザは複数

のセキュリティグループに割り振られるか、様々なセキュリティグループへの一時的なアクセスを提供することができる。例えば、ユーザが一時的に自分の通常のジョブ機能以外の追加の職務を実行しなければならない時、ユーザは、自分の通常のジョブ機能のセキュリティグループに割り当てられている一方で、ユーザは、追加のジョブ機能のための別のセキュリティグループに割り振ることもできる。

【００６２】

いくつかの実施形態では、ユーザは自動的にユーザのジョブ機能に基づいてセキュリティグループに割り当てられる。他の実施形態では、システム管理者は、サーバ１５０上のユーザインターフェースを介してセキュリティグループにユーザを割り当てる。例えば、システム管理者は、ユーザのユーザプロファイルを表示することができ、セキュリティグループの識別子を入力し、ドロップダウンメニューでいくつかのセキュリティグループからセキュリティグループを選択し、または任意の他の適した方法でセキュリティグループにユーザを割り当ててもよい。

【００６３】

ユーザデータテーブル３３０は、各ユーザに割り当てられているアクセス権３３８の表示を含んでいてもよい。いくつかの実施形態では、ユーザに割り当てられたアクセス許可は、ユーザのセキュリティグループに割り当てられたアクセス権に対応していてもよい。ユーザがセキュリティグループに属していない場合、またはセキュリティグループに割り当てられたアクセス権に加えて、アクセス権の指示は、個々にユーザに割り当てられたアクセス権を含んでいてもよい。

【００６４】

このシステム管理者はアクセス権をサーバ１５０のユーザインターフェースを介してユーザに割り当ててもよい。例えば、システム管理者は、ユーザのユーザプロファイルを表示することができ、アクセス権（例えば、アクセス権ＩＤ）に対する識別子を入力し、ドロップダウンメニューでいくつかのアクセス権からアクセス権を選択し、またはユーザにアクセス権を任意の他の適した方法で割り当ててもよい。

【００６５】

例示のユーザデータテーブル３３０には、ユーザＩＤ３３２、ジョブ機能３３４、セキュリティグループ３３６、及びアクセス権３３８を含む一方、データフィールド、追加の、あるいはより少ない、あるいは別のデータフィールドがそれぞれのユーザに含まれていてもよい。例えば、ユーザデータテーブル３３０も、出生データフィールド、自宅の住所データフィールド、作業開始日データフィールド、ユーザ名とパスワードデータフィールドなどを含むことができる。

【００６６】

図３Ｃは、プロセスプラント内のＵＩ装置の指示を含むＵＩ装置データテーブル３６０の例を示す。各ＵＩ装置は、一意的にＵＩ装置（例えばＵＩ０１，ＵＩ０２，ＵＩ０３，ＸＸＸ，ＢＢＺなど）を識別するＵＩ装置ＩＤ３６２を有していてもよい。ＵＩ装置データテーブル３６０は、各ＵＩ装置に割り当てられているアクセス権３６４の表示を含んでいてもよい。

【００６７】

このシステム管理者はアクセス権をサーバ１５０のユーザインターフェースを介してＵＩ装置に割り当ててもよい。例えば、システム管理者は、ＵＩ装置のプロファイルを表示することができ、アクセス権（例えば、アクセス権ＩＤ）に対する識別子を入力し、ドロップダウンメニューでいくつかのアクセス権からアクセス権を選択し、またはＵＩ装置にアクセス権を任意の適した方法で割り当ててもよい。

【００６８】

ＵＩ装置に割り当てられたアクセス権に加えて、各ＵＩ装置は、ライセンス機能３６６またはライセンスされたソフトウェアを有していてもよい。例えば、プロセスプラントは、他のＵＩ装置にライセンスを取得することなく、１つのＵＩ装置上のソフトウェアアプリケーション用ライセンスを取得してもよい。したがって、ＵＩ装置にある機能を実行する

アクセス権が、ＵＩ装置に割り当てられたアクセス権によってシステム管理者から与えられていても、ＵＩ装置に機能のライセンスが与えられていない場合は、ＵＩ装置はその機能を実行することができない。例えば、ＵＩ装置ＵＩ０１は、フィールドデバイスAにキャリブレーション機能を実行するためのアクセス権をUIデバイスＵＩ１０１に付与する、アクセス権１を割り当てられている。しかし、ＵＩ装置ＵＩ０１ためのライセンス機能３６６によると、ＵＩ装置ＵＩ０１は、キャリブレーション機能を実行するためのライセンスは付与されていない（例えば、キャリブレーションソフトウェアは、ＵＩ装置ＵＩ０１上ではライセンスされていない）。よって、ＵＩ装置ＵＩ０１は、フィールドデバイスＡをキャリブレートするキャリブレーションソフトウェアを動作させることはない。

【００６９】

例示のＵＩ装置データテーブル３６０には、ＵＩ装置ＩＤ３６２、アクセス権３６４、及びライセンスを与えられた機能３６６が含まれている一方、データフィールド、追加の、あるいはより少ない、あるいは別のデータフィールドがそれぞれのＵＩ装置に含まれていてもよい。例えば、ＵＩ装置データテーブル３６０は、使用されていない時にＵＩ装置が保存されているプロセスプラント内の位置を示す位置データフィールドも含むことができる。さらに、ＵＩ装置データテーブル３６０は、ＵＩ装置の製造元とモデル、ＵＩ装置用のシステム情報などを含んでいてもよい。さらに、ＵＩ装置データテーブル３６０は、ＵＩ装置は、ライセンスされた機能３６６の１つとして、特定の機能を実行するための適切なハードウェア／ソフトウェアを含むか否かを決定するため、ＵＩ装置上のハードウェア／ソフトウェアモジュールの表示を含んでいてもよい。

【００７０】

いくつかの実施形態では、サーバ１５０は、図３Ａ～３Ｃに示すようなデータテーブル３００、３３０、３６０のそれぞれからデータをプロセスプラントのＵＩ装置に送信してもよい。ユーザがＵＩ装置の１つにアクセスしようとしたとき、上述のように、ＵＩ装置は、ユーザの二要素認証を行う。ユーザが認証されると、ＵＩ装置は、送信されたデータを使用するユーザの権限レベルを決定することができる。また、いくつかの実施形態では、サーバ１５０は、ユーザの電子ＩＤカードにユーザデータテーブル３３０からユーザに対応するデータを送信してもよい。このように、電子ＩＤカード内のＲＦＩＤタグは、ユーザに割り当てられているアクセス権のセットを含んでいてもよい。

【００７１】

例えば、ＵＩ装置がプロセス制御装置または他のプラント資産に接続されている場合、ＵＩ装置は、プロセス制御装置または他のプラント資産を一意的に識別するデバイスＩＤとして、識別子を受信することができる（例えば、フィールドデバイスＡ、フィールドデバイスＢ、など）。いくつかの実施形態では、ＵＩ装置（例えば、ＲＦＩＤタグまたはユーザ名とパスワードを介して）二要素認証プロセス中にユーザのユーザＩＤを取得してもよい。ＵＩ装置は、メモリにそのＵＩデバイスＩＤを保存してもよい。次に、ＵＩ装置が取得したユーザＩＤとＵＩデバイスＩＤを使用して、それぞれ、ユーザデータテーブル３３０とＵＩ装置データテーブル３６０からユーザ及びＵＩ装置のためのアクセス権のセットを取り出すことができる。他の実施形態では、サーバ１５０は、ユーザ及び／またはＵＩ装置に割り当てられているアクセス権のセットをＵＩ装置からユーザＩＤ及びＵＩデバイスＩＤを受信し、送信することができる。さらに他の実施形態において、ＲＦＩＤタグは、ユーザのアクセス権のセットを含んでいてもよい。ＵＩ装置は、二要素認証プロセス中にＲＦＩＤタグを介してユーザのユーザＩＤを取得すると、ＲＦＩＤタグは、ユーザのアクセス権のセットを送信することができる。

【００７２】

いずれの場合も、ＵＩ装置は、ユーザ及び／またはＵＩ装置及びそのＵＩ装置に接続されたプロセス制御装置または他のプラント資産へのアクセスレベルを指定するために割り当てられているアクセス権を識別することができる。いずれのアクセス権が接続されたプラント資産へのアクセスレベルを指定しない場合、ＵＩ装置は、ユーザが接続されたプラント資産へのアクセスを有していないと判断する。したがって、ＵＩ装置は、ユーザが接続

されたプラント資産と通信することを許可しない。いくつかの実施形態では、ＵＩ装置は、ユーザが接続されたプラント資産へのアクセスを拒否されたことを示すユーザインターフェースを介してメッセージを表示することができる。メッセージは、ユーザが何故アクセスを拒否されたか（例えば、ユーザはプラント資産にアクセスするアクセス権限がない、ＵＩ装置は、プラント資産にアクセスするアクセス権を持っていない、またはユーザとＵＩ装置の両方がプラント資産にアクセスするアクセス権がない、など）の説明を提供することができる。また、メッセージはこのようなプラント資産へアクセスするアクセス権を持つＵＩ装置を取得するための命令、またはシステム管理者に連絡するための手順として、プラント資産へのアクセスを獲得するための指示を提供することができる。

【００７３】

一方、１つ以上のアクセス権が、接続されたプラント資産へのアクセスレベルを指定する場合、ＵＩ装置は、ユーザ及び／またはＵＩ装置が有するアクセスのタイプと、ユーザ及び／またはＵＩ装置が実行を許可されている機能を決定する。ＵＩ装置は、ユーザが接続されたプラント資産へのアクセスを有する領域を識別することができる。いくつかの実施形態では、ＵＩ装置は、全地球測位システム（ＧＰＳ）のように、位置決めセンサを介してその位置を決定してもよい。他の実施形態では、サーバ１５０は、各プラント資産の位置の表示を保存することができる。ＵＩ装置は、サーバ１５０から接続されたプラント資産の位置を取得することができるか、接続されたプラント資産の位置を決定するための各プラント資産の位置の指標を得ることができる。ＵＩ装置は、その位置を接続されたプラント資産の位置として決定してもよい。ＵＩ装置は、位置が、ユーザが接続されたプラント資産へのアクセスを有している領域内にあるかどうかを判断することができる。さらに、ＵＩ装置は、アクセスするための時間長を識別し、定期的に現在時刻とアクセス開始時間との差と時間長とを比較してもよい。

【００７４】

ユーザが、接続されたプラント資産に対する操作を実行するためにＵＩ装置上の特定の機能（例えば、ソフトウェアアプリケーションまたはソフトウェアアプリケーションの機能）を実行しようとすると、ＵＩ装置は、ユーザが機能にアクセスすることを許可されているか否かを判断する。さらに、ＵＩ装置は、機能がＵＩ装置上でライセンスされているかどうかを判定する。さらに加えて、ＵＩ装置はＵＩ装置が機能を実行するための適切なハードウェア／ソフトウェアを含むか否か、及び／または接続されたプラント資産が実行される機能に対応する動作を実行するための適切なハードウェア／ソフトウェアを含むか否かを判定する。例えば、ＵＩ装置は、プロセス制御装置に接続したとき、ＵＩ装置は、プロセス制御装置が特定の動作を実行するための適切なハードウェア／ソフトウェアを含むかどうかを決定するためのプロセス制御装置上のハードウェア／ソフトウェアモジュールの指示を受信することができる。

【００７５】

ユーザが機能にアクセスすることを許可されており、その機能は、ＵＩ装置上にライセンスされ、ＵＩ装置／接続されたプラント資産が、ＵＩ装置の機能を実行し、実行される機能に対応する動作を行うための適切なハードウェア／ソフトウェアを有する場合には、ＵＩ装置は、接続されたプラント資産に対する操作を行う機能を実行してもよい。一方、ユーザは、接続されたプラント資産とやりとりする際にその機能へのアクセスが許可されておらず、その機能がＵＩ装置上でライセンスされておらず、あるいは、ＵＩ装置／接続されたプラント資産が機能を実行し操作を行うための適切なハードウェア／ソフトウェアを有していない場合は、ＵＩ装置は、ユーザが機能にアクセスできないことを示すメッセージを表示してもよい。別の実施形態では、ユーザがＵＩ装置に特定の機能を実行しようとしたときに、ＵＩ装置がサーバ１５０に機能の指示を送信してもよい。サーバ１５０は、ユーザがユーザのユーザＩＤ、ユーザデバイスのＵＩ装置ＩＤ、及び／または接続されたプラント資産のためのデバイスＩＤに基づいてアクセス権を取得することにより、機能にアクセスできるかどうかを決定することができる。次に、ＵＩ装置は、アクセスが許可または拒否されたことを記述するサーバ１５０からの指示を受信することができる。

【００７６】
いくつかの実施形態では、ユーザは、接続されたプラント資産またはＵＩ装置上で実行される機能へのアクセスを拒否された場合、ＵＩ装置は、権限のないユーザが特定のプラント資産または機能にアクセスしようとしていることを示すサーバ１５０に通知を送信してもよい。通知は、システム管理者がレビューできるように、サーバ１５０のユーザインターフェース上に表示することができる。さらに、通知は、権限のないユーザのユーザＩＤ、ＵＩ装置のためのＵＩデバイスＩＤ、接続されたプラント資産のデバイスＩＤ、選択された機能の指標、ＵＩ装置の位置の指標などのような権限のない不正使用に関する情報を含んでいてもよい。通知はまた、アクセスを拒否した理由の表示（例えば、ユーザは、アクセスを許可されていないプラント資産にアクセスしようとした、ユーザが許可された領域の外でプラント資産にアクセスしようとした、ユーザが許可された時間長より長い時間プラント資産にアクセスしようとした、など）を含んでいてもよい。
【００７７】
システム管理者は、通知を確認し、例えば、複数のユーザが許可領域外で同じプロセス制御装置にアクセスしようとしたことを判断することができる。結果として、システム管理者は、許可された領域を調整する必要があるか、あるいはユーザがどの領域へのアクセスが許可されているか、そしてどの領域へのアクセスが拒否するかを通知する必要があるかどうかを判断してもよい。システム管理者は、プロセス制御装置とやりとりするとき、ユーザは、特定のプロセス制御装置または特定の機能にアクセスできるように、通知を確認し、ユーザに新しいアクセス権を割り当てることができる。許可が更新されている、またはユーザ及び／またはＵＩ装置が各アクセス権の変更に割り当てられている場合は、サーバ１５０は、ＵＩ装置への更新されたアクセス権のリストを送信してもよい。
【００７８】
図４は、プロセスプラントで二要素認証を行うための方法４００の例示するフロー図である。方法４００は、ＵＩ装置１１２上で実行されてもよい。いくつかの実施形態では、方法４００は、非一時的なコンピュータ可読メモリに保存された命令のセットで実行し、ＵＩ装置１１２の１個以上のプロセッサによって実施することができる。例えば、図１Ｃに示すように、方法４００は、認証／権限付与モジュール９６によって行われてもよい。
【００７９】
ブロック４０２において、ＵＩ装置１１２は、ユーザの第１のタイプの識別情報を受信する。第１のタイプの識別情報は、識別装置から提供されたものでもよく、また、ユーザの身体的特徴であってもよい。例えば、ＵＩ装置１１２は、図２Ａに示すように、ユーザに自分の電子ＩＤカードをスキャンさせる要求２１０を含む表示画面２００を提示することができる。次いで、ユーザは、自分の電子ＩＤカードをＵＩ装置１１２の通信範囲内に載置し、（例えば、１インチ、３インチ、６インチ、１フィート、３フィート、など）電子ＩＤカードとＵＩ装置１１２間の短距離通信リンクを確立することができる。電子ＩＤカードは、次いで、ユーザＩＤなどのユーザの識別情報を含むＵＩ装置１１２にＲＦＩＤタグを送信する。しかし、これは単にＵＩ装置１１２に提供することができる識別情報の１つの例示のタイプに過ぎない。識別情報の追加または代替のタイプ、例えば、社会保険カード、運転免許証、指紋または網膜画像などの生体情報を提供してもよい。
【００８０】
いずれの場合も、ＵＩ装置１１２はユーザのための第１のタイプの識別情報を認証してもよい（ブロック４０４）。例えば、ＵＩ装置１１２は、プロセスプラント内の各権限を有するユーザのユーザプロファイルを保存することができる。ユーザプロファイルは、ユーザＩＤ、ユーザ名、パスワード、パスコード／ＰＩＮ番号、許可されたユーザに関連する任意の他の適切な情報を含んでいてもよい。具体的には、ユーザプロファイルは、図３Ｂに示すようにユーザデータテーブル３３０からのデータに基づいて生成することができる。ＵＩ装置１１２は、ユーザに対する第１のタイプの識別情報（例えば、ＲＦＩＤタグ内のユーザＩＤ）をユーザプロファイルまたはユーザデータテーブル３３０と比較して、第１のタイプの識別情報がプロセスプラント内の権限を有するユーザに対応するかどうかを

決定する（ブロック４０６）。別の例では、ＵＩ装置１１２は、第１のタイプの識別情報をサーバ１５０に送信することができ、サーバ１５０は、第１のタイプの識別情報をユーザプロファイルまたはユーザデータテーブル３３０と比較することができる。

【００８１】

いずれの場合も、第１のタイプの識別情報が、プロセスプラント内の許可されたユーザに対応しない場合、ＵＩ装置１１２は、ユーザを認証せず、ユーザにいずれかのタイプの識別情報を提供するよう、あるいは、ＩＤカードを再度スキャンすることを求めることができる。第１のタイプの識別情報は、プロセスプラント内のユーザに対応する一方、ＵＩ装置１１２は、ユーザの第２のタイプの識別情報を受信する（ブロック４０８）。第２のタイプの識別情報は、ユーザによって提供された情報であってもよい。例えば、ＵＩ装置１１２は図２Ｂに示すような、ユーザにユーザ名とパスワードなどのユーザログイン情報を入力するユーザコントロール２６０、２７０を含む表示画面２５０を提示してもよい。しかし、これは単にＵＩ装置１１２に提供することができる識別情報の１つの例示のタイプに過ぎない。追加または代替のタイプの識別情報、例えばユーザＩＤ、メールアドレス、生年月日、パスコード／ＰＩＮ番号なども、ユーザによって提供されてもよい

【００８２】

いずれの場合も、ＵＩ装置１１２はユーザのための第２のタイプの識別情報を認証してもよい（ブロック４１０）。例えば、ＵＩ装置１１２は、ユーザに対する第２のタイプの識別情報（例えば、ユーザ名及びパスワード）をユーザプロファイルまたはユーザデータテーブル３３０と比較して、第２のタイプの識別情報がプロセスプラント内の権限を有するユーザに対応するかどうかを決定する（ブロック４１２）。別の例では、ＵＩ装置１１２は、第２のタイプの識別情報をサーバ１５０に送信することができ、サーバ１５０は、第２のタイプの識別情報をユーザプロファイルまたはユーザデータテーブル３３０と比較することができる。

【００８３】

第２のタイプの識別情報が、プロセスプラント内の権限を有するユーザに対応しない場合、ＵＩ装置１１２は、ユーザを認証せず、ユーザにいずれかのタイプの識別情報を提供するよう、あるいは、ユーザ名とパスワードを再び入力しようとすることを求めることができる。さらに、ＵＩ装置１１２は、第１及び第２のタイプの識別情報は、プロセスプラント内の同じ権限を有するユーザに対応するかどうかを判断する（ブロック４１４）。第１及び第２のタイプの識別情報が、同じ許可されたユーザに対応しない場合、ＵＩ装置１１２は、ユーザを認証せず、ユーザに第１及び第２のタイプの識別情報を再び提供することを求めることができる。一方、第１及び第２のタイプの識別情報が、同じ権限を有するユーザに対応する場合には、ユーザは、ＵＩ装置１１２へのアクセスを提供される（ブロック４１６）。従って、ユーザは、ＵＩ装置１１２上で機能を実行することができる。この機能は、プロセス制御装置または他のプラント資産において、接続したＵＩ装置１１２に、接続したプロセス制御装置または他のプラント資産を監視、制御、キャリブレーション、構成、またはトラブルシューティングなどの機能のような操作を実行することができる。

【００８４】

方法４００は、識別情報を受信すると、そのそれぞれのタイプを認証するステップを含むが、第１及び第２のタイプの識別情報の両者は、認証前に受信することもできる。例えば、ＵＩ装置１１２は、ＲＦＩＤタグとユーザからユーザ名及びパスワードを受信することができ、その後、プロセスプラント内の権限を有するユーザのユーザプロファイルにＲＦＩＤタグとユーザ名とパスワードからユーザＩＤを比較する。さらに、方法４００は、それぞれのユーザプロファイルを２度目に検索して第２のタイプの識別情報に適合する権限を有するユーザを探すことを回避するステップを含んでいてもよい。例えば、第１のタイプの識別情報と一致する認証されたユーザを識別した後に、ＵＩ装置１１２は、認証されたユーザのユーザデータを第２のタイプの識別情報と比較することができる。

【００８５】

上述したように、ユーザは、二要素認証プロセスを介して認証された後、ＵＩ装置１１２

は、ユーザがＵＩ装置１１２に接続されているプロセス制御装置または他のプラント資産に対して有する権限レベルを判定する。例えば、ユーザは、バルブにＵＩ装置１１２を接続して、監視、制御、構成、キャリブレーション、トラブルシューティング、またはバルブ上の任意の他の適切な動作を行ってもよい。

【００８６】

図５は、ユーザがプラント資産に接続しなければならない権限レベルを決定するための方法５００を例示するフロー図である。方法５００は、ＵＩ装置１１２上で実行されてもよい。いくつかの実施形態では、方法５００は、非一時的なコンピュータ可読メモリに保存された命令のセットで実施し、ＵＩ装置１１２の１台以上のプロセッサによって実行することができる。例えば、図１Ｃに示すように、方法５００は、認証／権限付与モジュール９６によって行われてもよい。

【００８７】

ブロック５０２及び５０４において、ＵＩ装置１１２はユーザとＵＩ装置１１２それぞれに対しアクセス権のセットを得ることができる。例えば、図３Ａ～Ｃに示すように、ＵＩ装置１１２はそれぞれ、サーバ１５０から、権限データテーブル３００、ユーザデータテーブル３３０と、ＵＩ装置データテーブル３６０を取得してもよい。ＵＩ装置１１２は、また、ＵＩ装置１１２に接続されているプロセス制御装置または他のプラント資産から識別子を取得してもよい（ブロック５０６）。例えば、プロセス制御装置または他のプラント資産がデバイスＩＤをＵＩ装置１１２に送信してもよい。ＵＩ装置１１２はまた、ユーザＩＤとして、二要素認証プロセスからのユーザの識別子を取得してもよく、そのようなＵＩ装置ＩＤなどのＵＩ装置１１２の識別子を取得してもよい。

【００８８】

そして、ＵＩ装置１１２は、ユーザＩＤとＵＩ装置ＩＤを使って、ユーザとＵＩ装置１１２に対しアクセス権のセットを取得することができる。例えば、アクセス権は、ユーザデータテーブル３３０とＵＩ装置データテーブル３６０から取得できる。ＵＩ装置１１２は、デバイスＩＤを使用して接続されたプラント資産へのアクセスレベルを指定するアクセス権を識別することができる。他の実施形態では、ＵＩ装置１１２は、サーバ１５０に接続されたプラント資産のユーザＩＤ、ＵＩ装置ＩＤ、デバイスＩＤを送信することができるとともに、サーバ１５０からユーザ及びＵＩ装置１１２に割り当てられたアクセス権のセットを受信することができる。さらに他の実施形態において、ＲＦＩＤタグは、ユーザのアクセス権のセットを含んでいてもよい。ＵＩ装置１１２は、二要素認証プロセス中にＲＦＩＤタグを介してユーザの識別子を取得すると、ＲＦＩＤタグは、ユーザのアクセス権のセットを送信することができる。

【００８９】

接続されたプラント資産へのアクセスレベルを指定する権限レベルに基づいて、ＵＩ装置１１２は、ユーザの権限レベルを識別することができる（ブロック５０８）。例えば、ユーザ及び／またはＵＩ装置１１２は、接続されたプラント資産へのアクセスレベルを指定するアクセス権のいずれへも割り当てられなくてもよい。よってＵＩ装置１１２は、接続されたプラント資産へのアクセスを拒否されたことを示すメッセージをユーザに表示することができる。またメッセージは、アクセス拒否の説明（例えば、利用者は接続されたプラント資産にアクセスする権限がない、ＵＩ装置１１２は、接続されたプラント資産にアクセスする権限を持っていない、またはユーザとＵＩ装置112のいずれも接続されたプラント資産にアクセスする権限がない、など）を含んでいてもよい。

【００９０】

ユーザの権限レベルは、ユーザが接続されたプラント資産（例えば、読み取り専用、読み取り／書き込みなど）、ユーザが接続されたプラント資産（例えば、構成、トラブルシューティング、キャリブレーション、監視、制御など）での操作を行うためにアクセスすることができる機能を有しているアクセスのタイプを含んでいてもよい。権限レベルは、ユーザが接続されたプラント資産へのアクセスを有するプロセスプラントの領域と、ユーザが接続されたプラント資産にアクセスするための時間長を含んでいてもよい。

【００９１】
ブロック５１０では、ユーザは、ＵＩ装置１１２に、接続されたプラント資産に対する操作を行うように指示することができる。ＵＩ装置１１２はユーザの権限レベルに基づいて、ユーザが接続されたプラント資産で要求された操作を行う機能にアクセスできるかどうかを判定する（ブロック５１２）。例えば、ＵＩ装置１１２は、ＧＰＳまたは任意の他の適切な位置決め装置を介してその位置を判定してもよい。別の例では、サーバ１５０は、各プラント資産の位置の表示を保存することができる。ＵＩ装置は、サーバ１５０から接続されたプラント資産の位置を取得することができるか、接続されたプラント資産の位置を決定するための各プラント資産の位置の指標を得ることができる。ＵＩ装置は、その位置を接続されたプラント資産の位置として決定してもよい。ＵＩ装置１１２は、位置が、ユーザが接続されたプラント資産へのアクセスを有している領域内にあるかどうかを判断することができる。さらに、アクセスのタイプと権限レベルに対する機能は、要求された操作を行う機能と比較してもよい。ＵＩ装置１１２は、また、権限の時間長が満了したか否かも判定してもよい。いくつかの実施形態では、ＵＩ装置１１２は、要求された操作を行う機能がＵＩ装置１１２にライセンスされているか否かを判定してもよい（ブロック５１２）。また、いくつかの実施形態では、ＵＩ装置１１２は、ＵＩ装置／接続されたプラント資産が機能を実行し、実行される機能に対応する動作を行うための適切なハードウェア／ソフトウェアを有するかどうかを判定することができる。

【００９２】
機能がユーザの権限レベルに基づいて許可されており、ＵＩ装置１１２が機能を行うためのライセンスを与えられており、ＵＩ装置／接続されたプラント資産が、ＵＩ装置の機能を実行し、実行される機能に対応する動作を実行するための適切なハードウェア／ソフトウェアを有する場合には、ＵＩ装置１１２は、対応する操作をプロセス制御装置または他のプラント資産上で行ってもよい（ブロック５１６）。例えば、ＵＩ装置１１２は、プロセス制御装置は、ＵＩ装置１１２に表示される測定値を取得して送信することを要求することができる。機能がユーザの権限レベル（例えば、ユーザが許可された領域外にいる、権限付与の時間長を超えている、ユーザが接続されたプラント資産と通信する際にその機能を実行することが許可されていない、など）に基づいて許可されておらず、ＵＩ装置１１２が機能を実行するためのライセンスを与えられておらず、ＵＩ装置／接続プラント資産が、ＵＩ装置の機能を実行し、実行される機能に対応する動作を行うための適切なハードウェア／ソフトウェアを有していない場合には、ＵＩ装置１１２は、機能を実行しない。さらに、接続されたプラント資産へのアクセスが拒否された旨を示すメッセージをユーザに表示してもよい（ブロック５１８）。メッセージは、アクセス拒否に関する説明を含んでいてもよい。

【００９３】
図６は、アクセス権のセットを生成し、プロセスプラント内でユーザとＵＩ装置にアクセス権を割り当てるための方法６００を例示するフロー図である。方法６００は、サーバ１５０上で実行されてもよい。いくつかの実施形態では、方法６００は、非一時的なコンピュータ可読メモリに保存された命令のセットで実施し、サーバ１５０の１台以上のプロセッサによって実行することができる。

【００９４】
ブロック６０２では、サーバ１５０は、いくつかのアクセス権を生成し、各アクセス権は、特定のプロセス制御装置または他のプラント資産または特定のプラント領域内のプロセス制御装置または他のプラント資産のグループへのアクセスレベルを指定する。例えば、アクセス権は、デバイスＩＤとして、プロセス制御装置のための識別子を含んでいてもよい。アクセス権はまた、プロセス制御装置または読み取り専用、読み取り／書き込み、などのような他のプラント資産へのアクセスのタイプを含んでいてもよい。また、アクセス権は、プロセス制御装置または他のプラント資産の操作を行う機能を含んでいてもよい。さらに、アクセス権は、プロセス制御装置または他のプラント資産へのアクセスが許可されているプラント領域、及びプロセス制御装置または他のプラント資産にアクセスするた

めの時間長を含んでいてもよい。いくつかの実施形態では、システム管理者はサーバ１５０と相互作用してアクセス権を生成してもよい。

【００９５】

アクセス権を生成することに加え、サーバ１５０は、プロセスプラント内の１人もしくは数人のユーザ（ブロック６０４）と、１つもしくは数台のＵＩ装置（ブロック６０６）に各アクセス権を割り当ててもよい。このシステム管理者はアクセス権をサーバ１５０のユーザインターフェースを介してユーザに割り当ててもよい。例えば、システム管理者は、ユーザのユーザプロファイルを表示することができ、アクセス権（例えば、アクセス権ＩＤ）に対する識別子を入力し、ドロップダウンメニューでいくつかのアクセス権からアクセス権を選択し、またはユーザにアクセス権を任意の他の適した方法で割り当てもよい。このシステム管理者はアクセス権をサーバ１５０のユーザインターフェースを介してＵＩ装置に割り当てもよい。例えば、システム管理者は、ＵＩ装置のプロファイルを表示することができ、アクセス権（例えば、アクセス権ＩＤ）に対する識別子を入力し、ドロップダウンメニューでいくつかのアクセス権からアクセス権を選択し、またはＵＩ装置にアクセス権を任意の他の適した方法で割り当てもよい。

【００９６】

いくつかの実施形態では、サーバ１５０は、複数のユーザを含むセキュリティグループへのアクセス権を割り当てることができる。アクセス権がセキュリティグループに割り当てられている場合には、セキュリティグループに属するユーザのそれぞれには、アクセス権が与えられる。このシステム管理者は、アクセス権をサーバ１５０のユーザインターフェースを介してセキュリティグループの表示を見ることによって、セキュリティグループに割り当ててもよい。システム管理者は、アクセス権（例えば、アクセス権ＩＤ）に対する識別子を入力し、ドロップダウンメニューでいくつかのアクセス権からアクセス権を選択し、またはセキュリティグループにアクセス権を任意の他の適した方法で割り振ってもよい。

【００９７】

ブロック６０８において、サーバ１５０は、アクセス権に割り当てられた各ユーザとＵＩ装置の指示と共に、プロセスプラント内の１台以上のＵＩ装置にアクセス権を与えることができる。いくつかの実施形態では、サーバ１５０は、プロセスプラントにおけるＵＩ装置それぞれにアクセス権を提供してもよい。また、いくつかの実施形態では、サーバ１５０は、特定のユーザに属する電子ＩＤカードに、（例えば、ユーザデータテーブルを介して）特定のユーザに対応するアクセス権を提供することができる。他の実施形態では、サーバ１５０は、ユーザがＵＩ装置にアクセスしようとした時、あるいは、ＵＩ装置がプロセス制御装置または他のプラント資産に接続された時に、アクセス権を与えることができる。例えば、ユーザがＵＩ装置にアクセスしようと試みて、ＵＩ装置をプロセス制御装置に接続したときに、ＵＩ装置が、ユーザのためのユーザＩＤ、ＵＩ装置のためのＵＩ装置ＩＤ及び／または接続したプロセス制御装置のデバイスＩＤをサーバ１５０に送信するようにしてもよい。サーバ１５０は、ユーザに対応するアクセス権のセット、ＵＩ装置、及び／または接続したプロセス制御装置を取得してＵＩ装置にアクセス権のセットを送信することができる。

【００９８】

ブロック６１０では、サーバ１５０及び／またはアクセス権に割り当てられたユーザとＵＩ装置へのアクセス権への更新があったか否かを判定する。例えば、サーバ１５０は、システム管理者がさらにアクセス権を追加したか、アクセス権を削除したか、別のアクセス権をユーザまたはＵＩ装置に割り当てたか、ユーザの割り当てられたアクセス権を削除したか、新しいユーザまたはＵＩ装置にアクセス権を割り当てたかどうか、などを判定することができる。

【００９９】

アクセス権または割り当てが更新されている場合は、サーバ１５０は、更新されたアクセス権リストをプロセスプラント内の１つ以上のＵＩ装置に提供してもよい（ブロック６１

２）。いくつかの実施形態では、サーバ１５０は、プロセスプラントにおけるＵＩ装置それぞれに更新したアクセス権リストを提供してもよい。他の実施形態では、サーバ１５０は、ユーザがＵＩ装置にアクセスしようとした時、あるいは、ＵＩ装置がプロセス制御装置または他のプラント資産に接続された時に、更新したアクセス権リストを提供することができる。

【０１００】

いくつかの実施形態では、ユーザは、接続されたプラント資産またはＵＩ装置上で実行される機能へのアクセスを拒否された場合、サーバ１５０は、権限のないユーザが特定のプラント資産または機能にアクセスしようとしていることを示す通知をＵＩ装置から受信してもよい。通知は、システム管理者がレビューできるように、サーバ１５０のユーザインターフェース上に表示することができる。さらに、通知は、権限のないユーザのユーザＩＤ、ＵＩ装置のためのＵＩ装置ＩＤ、接続されたプラント資産のデバイスＩＤ、選択された機能の指標、ＵＩ装置の位置の指標などのような権限のない不正使用に関する情報を含んでいてもよい。通知はまた、アクセスを拒否する理由（例えば、ユーザが、自分がアクセス権を持たないプロセス制御装置にアクセスしようとしたなど）の指示を含むことができる。

【０１０１】

システム管理者は、通知を確認し、例えば、複数のユーザが許可領域外で同じプロセス制御装置にアクセスしようとしたことを判断することができる。結果として、システム管理者は、許可された領域を調整する必要があるか、あるいはユーザがどの領域へのアクセスが許可されているか、そしてどの領域へのアクセスが拒否されるかを通知する必要があるかどうかを判断してもよい。システム管理者は、プラント資産とやりとりするとき、ユーザは、特定のプラント資産または特定の機能にアクセスできるように、通知を確認し、ユーザにアクセス権を割り当てることができる。

【０１０２】

本開示に記載の技術の実施形態は、任意の数の以下の態様を、単独でまたは組み合わせて含んでもよい。

【０１０３】

１．プロセスプラント内のユーザインターフェイスデバイスにおいて二要素認証を提供する方法であって、ユーザインターフェイスデバイスにおける１つ以上のプロセッサにおいて、ユーザに対する第１のタイプの識別情報を受信するステップであって、ユーザインターフェイスデバイスがプロセスプラント内のプラント資産に接続する一体型の入出力能力を含む、ステップと、１つ以上のプロセッサにおいて、ユーザに対する第２のタイプの識別情報を受信するステップと、１つ以上のプロセッサによって、ユーザに対する第１及び第２のタイプの識別情報それぞれをユーザインターフェイスデバイスにアクセスする権限が与えられた複数のユーザに対する複数のタイプの識別情報と比較するステップと、第１及び第２のタイプの識別情報それぞれが同じ権限が与えられたユーザに対応する場合に、１つ以上のプロセッサによって、ユーザに権限が与えられたアクセスを提供するステップとを有し、ユーザがユーザインターフェイスデバイスに対して権限が与えられたアクセスを有し、ユーザインターフェイスデバイスがプラント資産に接続される場合、ユーザインターフェイスデバイスはプロセスプラント内の接続されたプラント資産と通信するよう構成される、方法。

【０１０４】

２．第１のタイプの識別情報は、識別装置から提供される、または、ユーザの身体的特徴であり、第２のタイプの識別情報はユーザによって提供される知識ベースの識別情報である、態様１に記載の方法。

【０１０５】

３．第１のタイプの識別情報は、電子識別カードから短距離通信リンクを介して受信され、第２のタイプの識別情報は、ユーザによってユーザインターフェイスデバイスを介して入力されるユーザログイン情報である、態様１または２に記載の方法。

【０１０６】
４．１つ以上のプロセッサによって、ユーザログイン情報を入力する１つ以上のユーザコントロールを含むユーザログインスクリーンを表示するステップをさらに含む、態様１～３のうちいずれか１つに記載の方法。
【０１０７】
５．１つ以上のプロセッサによって、ユーザに対して権限のレベルを決定するステップであって、権限のレベルはユーザがアクセスする権限が与えられた１つ以上のプラント資産またはユーザがユーザインターフェイスデバイスで実行する権限が与えられた１つ以上の機能を含むユーザに割り当てられたアクセス権のセットを含む、ステップと、１つ以上のプロセッサによって、ユーザの権限レベルに基づいて、接続されたプラント資産にアクセスする権限がユーザに与えられているかを決定するステップとをさらに有する、態様１～４のうちいずれか１つに記載の方法。
【０１０８】
６．ユーザに対して
権限レベルを決定するステップは、１つ以上のプロセッサにおいて、ユーザインターフェイスデバイスにアクセスする権限が与えられた複数のユーザそれぞれに割り当てられたアクセス権のセットを取得し、１つ以上のプロセッサによって、ユーザに割り当てられたアクセス権のセットを識別することを含む、態様１～５のうちいずれか１つに記載の方法。
【０１０９】
７．ユーザの権限レベルは、さらに、ユーザが１つ以上のプラント資産またはユーザインターフェイスデバイスでの１つ以上の機能にアクセスする権限が与えられた時間長を含む、態様１～６のうちいずれか１つに記載の方法。
【０１１０】
８．１つ以上のプロセッサによって、ユーザインターフェイスデバイスに割り当てられたアクセス権のセットを取得するステップと、１つ以上のプロセッサによって、ユーザインターフェイスデバイスに割り当てられたアクセス権のセットに基づいて、接続されたプラント資産にアクセスする権限がユーザインターフェイスデバイスに与えられたかを決定するステップと、をさらに有する態様１～７のうちいずれか１つに記載の方法。
【０１１１】
９．接続されたプラント資産にアクセスする権限がユーザ及びユーザインターフェイスデバイスに与えられた場合、１つ以上のプロセッサによって、接続されたプラント資産に動作を実施する機能が実行される、態様１～８のうちいずれか１つに記載の方法。
【０１１２】
１０．１つ以上のプロセッサによって、ユーザインターフェイスデバイスが機能を実行するためのライセンスが与えられているかを決定するステップをさらに有する、態様１～９のうちいずれか１つに記載の方法。
【０１１３】
１１．プロセスプラント内で二要素認証を提供するユーザインターフェイスデバイスであって、１つ以上のプロセッサと、プロセスプラント内のプラント資産に接続する一体型の入出力構成要素と、１つ以上のプロセッサ及び一体型の入出力構成要素に接続され、指示を記憶する非一時的コンピュータ可読媒体とを備え、指示は、１つ以上のプロセッサによって実行されると、ユーザインターフェイスデバイスに、ユーザに対する第１のタイプの識別情報を受信させ、ユーザに対する第２のタイプの識別情報を受信させ、ユーザに対する第１及び第２のタイプの識別情報それぞれをユーザインターフェイスデバイスにアクセスする権限が与えられた複数のユーザに対する複数のタイプの識別情報と比較させ、第１及び第２のタイプの識別情報それぞれが同じ権限が与えられたユーザに対応する場合に、ユーザに権限が与えられたアクセスを提供させ、ユーザがユーザインターフェイスデバイスに対して権限が与えられたアクセスを有し、ユーザインターフェイスデバイスがプラント資産に接続された場合、ユーザインターフェイスデバイスはプロセスプラント内の接続されたプラント資産と一体型の入出力構成要素を介して通信するよう構成される、ユーザ

インターフェイスデバイス。
【０１１４】
１２．第１のタイプの識別情報は、識別装置から提供される、または、ユーザの身体的特徴であり、第２のタイプの識別情報はユーザによって提供される知識ベースの識別情報である、態様１１記載のユーザインターフェイスデバイス。
【０１１５】
１３．無線ラジオをさらに備え、第１のタイプの識別情報は、電子識別カードから無線ラジオにおいて短距離通信リンクを介して受信され、第２のタイプの識別情報は、ユーザによってユーザインターフェイスデバイスを介して入力されるユーザログイン情報である、態様１１または１２記載のユーザインターフェイスデバイス。
【０１１６】
１４．ユーザインターフェイスをさらに備え、指示は、さらに、ユーザインターフェイスデバイスに、ユーザログイン情報を入力する１つ以上のユーザコントロールを含むユーザログインスクリーンをユーザインターフェイス上に表示させる、態様１１～１３のうちいずれか１つに記載のユーザインターフェイスデバイス。
【０１１７】
１５．指示は、さらに、ユーザインターフェイスデバイスに、ユーザに対して権限レベルを決定させ、権限レベルはユーザがアクセスする権限が与えられた１つ以上のプラント資産またはユーザがユーザインターフェイスデバイスで実行する権限が与えられた１つ以上の機能を含むユーザに割り当てられたアクセス権のセットを含み、ユーザの権限レベルに基づいて、接続されたプラント資産にアクセスする権限がユーザに与えられているかを決定させる、態様１１～１４のうちいずれか１つに記載のユーザインターフェイスデバイス。
【０１１８】
１６．ユーザに対して権限レベルを決定するために、指示は、ユーザインターフェイスデバイスに、ユーザインターフェイスデバイスにアクセスする権限が与えられた複数のユーザそれぞれに割り当てられたアクセス権のセットを取得させ、ユーザに割り当てられたアクセス権のセットを識別させる、態様１１～１５のうちいずれか１つに記載のユーザインターフェイスデバイス。
【０１１９】
１７．ユーザの権限レベルは、さらに、ユーザが１つ以上の装置またはユーザインターフェイスデバイスでの１つ以上の機能にアクセスする権限が与えられた時間長を含む、態様１１～１６のうちいずれか１つに記載のユーザインターフェイスデバイス。
【０１２０】
１８．指示は、さらに、ユーザインターフェイスデバイスに、ユーザインターフェイスデバイスに割り当てられたアクセス権のセットを取得させ、ユーザインターフェイスデバイスに割り当てられたアクセス権のセットに基づいて、接続されたプラント資産にアクセスする権限がユーザインターフェイスデバイスに与えられたかを決定させる、態様１１～１７のうちいずれか１つに記載のユーザインターフェイスデバイス。
【０１２１】
１９．接続されたプラント資産にアクセスする権限がユーザ及びユーザインターフェイスデバイスが与えられた場合、指示は、ユーザインターフェイスデバイスに、接続されたプラント資産に動作を実施する機能を実行させる、態様１１～１８のうちいずれか１つに記載のユーザインターフェイスデバイス。
【０１２２】
２０．指示は、さらに、ユーザインターフェイスデバイスに、ユーザインターフェイスデバイスが機能を実行する認可が与えられているかを決定させる、態様１１～１９のうちいずれか１つに記載のユーザインターフェイスデバイス。
【０１２３】
さらに、本開示の諸態様は、例示に過ぎず、本開示の範囲を限定することを意図するものではない。

【０１２４】
下記の追加の考察は、前述の議論に適用される。本明細書を通して、任意のデバイスまたはルーチンによって行われるとして説明したアクションは、一般に、機械可読命令に応じてデータを操作または変換プロセッサのアクションまたはプロセスを意味する。機械可読命令は、通信プロセッサに結合された記憶装置に保存され、そこから取り出すことができる。すなわち、本明細書に記載される方法は、図１Ｃに示すようなコンピュータ可読媒体上（すなわち、メモリデバイス上）に保存された機械実行可能な命令のセットによって具現化することができる。命令は、対応するデバイス（例えば、サーバ、UI、など）の１つ以上のプロセッサによって実行されたとき、プロセッサに本方法を実行させる。命令、ルーチン、モジュール、プロセス、サービス、プログラム、及び／またはアプリケーションがコンピュータ可読メモリ上またはコンピュータ可読媒体に保存され、記憶されているものとしている場合、「保存」「記憶」という用語は、一時信号を含まないものであると解釈することを意図している。
【０１２５】
さらに、用語「オペレータ」、「人員」、「人」、「ユーザ」、「技師」、及び他の同様の用語を、使用したり、システム、装置と相互作用することができるプロセスプラント環境内の人を記述するために使用されているが、これらの用語は、限定を目的とするものではない。特定の用語を説明で使用する場合、その用語は、部分的には、プラント人員が関わる従来の活動のために使用されるが、その特定の活動に関わることができる人員に限定することを意図したものではない。
【０１２６】
また、本明細書を通して、複数のインスタンスは、単一のインスタンスとして説明した構成要素、動作、または構造を実行することができる。１つ以上の方法の個々の操作を操作として図示し説明しているが、個々のオペレーションの１つ以上を同時に行ってもよく、操作が図示の順序で実行されなければならないわけではない。例示の構成において別の構成要素として提示された構造と機能は、統合された構造または構成要素として実行することができる。同様に、単一の構成要素として提示された構造と機能は、別個の構成要素として実行することができる。これら及び他の変形、修正、追加、及び改良は、本明細書の主題の範囲内に含まれる。
【０１２７】
特に明記しない限り、本明細書の説明で使用する「処理」、「演算」、「計算」、「決定」、「識別」、「提示」、「提示させる」、「表示させる」、「表示する」、などの単語は、すなわち、１つ以上のメモリ（例えば、揮発性メモリ、不揮発性メモリ、またはそれらの組み合わせ）レジスタ、または情報を受信し、保存し、送信し、表示する他の機械構成要素内の物理的（例えば、電子的、磁気的、生物学的、または光学的）量として表されるデータを操作または変換する機械（例えば、コンピュータ）の動作または処理を意味する。
【０１２８】
ソフトウェアで実行される場合、本明細書に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かは、磁気ディスク上のような任意の有形の、非一時的なコンピュータ可読メモリ、レーザディスク、固体メモリ装置、分子メモリ記憶装置、またはコンピュータまたはプロセッサ等のＲＡＭまたはＲＯＭの他の記憶媒体に保存することができる。本明細書に開示された例示的なシステムは、ハードウェア上で実行されるなど、他の成分のうち、ソフトウェア及び／またはファームウェアとして開示されているが、そのようなシステムは単なる例示であり、限定するものとしてみなされるべきではないことは留意すべきことである。例えば、いずれかまたはこれらのハードウェア、ソフトウェア、及びファームウェアコンポーネントのすべてが排他的にソフトウェア、排他的にハードウェア、またはハードウェアとソフトウェアの任意の組み合わせで具現化できると考えられる。したがって、当業者は提供されている例は、このようなシステムを実行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。

【０１２９】
本発明について、特定の例を挙げて説明してきたが、これらは例示に過ぎず、本発明を限定することを意図するものではないが、開示された実施形態は、本発明の趣旨と範囲から逸脱することなく、変更、追加、削除などを行えることは当業者にとって明らかであろう。
【０１３０】
本特許において、本明細書で使用される用語『_____』は、「。。。」を示すものとする、もしくはそれに類似した文で明らかに定義していない限り、その用語の意味を明示または暗示によってその平易または通常の意味を超えて限定する意図はなく、それらの用語は、この特許のいかなる部分においても（ただし特許請求の範囲の文言は除く）、その範囲を点綴して理解されるべきではないということは理解できよう。本特許の最後に添付の特許請求の範囲に記載の任意の用語は、専ら読者を混乱させないように明確化のために行われる単一の意味と一致する形で本特許で言及され、そしてそれはその請求項がその単一の意味に、明示的または暗示的に、限定することを意図するものではない。最後に、請求項の要素が、いかなる構造の詳説することなく単語「手段」及び機能を記載することによって定義されていない限り、いかなる請求項の要素の範囲も、３５Ｕ.Ｓ.Ｃ.§１１２（ｆ）及び／またはプレＡＩＡ３５Ｕ.Ｓ.Ｃ.§１１２、第６段落の適用に基づいて解釈されることを意図するものではない。
【０１３１】
さらに、上記のテキストは、記載多数の異なる実施形態の詳細な説明を設定しているが、特許の範囲は、本特許の最後に記載され、特許請求の範囲の文言によって定義されることは理解できよう。詳細な説明は単なる例示として解釈されるべきであり、すべての可能な実施形態を説明しているわけではない。なぜならすべての可能な実施形態を説明することは、不意可能でないまでも、非現実的であるからである。多数の代替実施形態は、やはり特許請求の範囲の範囲内に入る本特許の出願日後に開発された現在の技術または技術のいずれかを使用して、実施することができる。

【図面】

【図１Ａ】

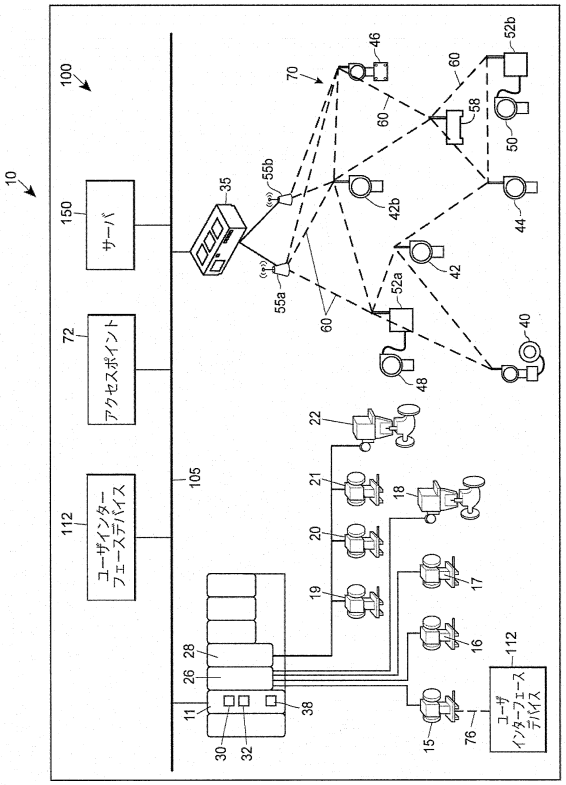

図１Ａ

【図１Ｂ】

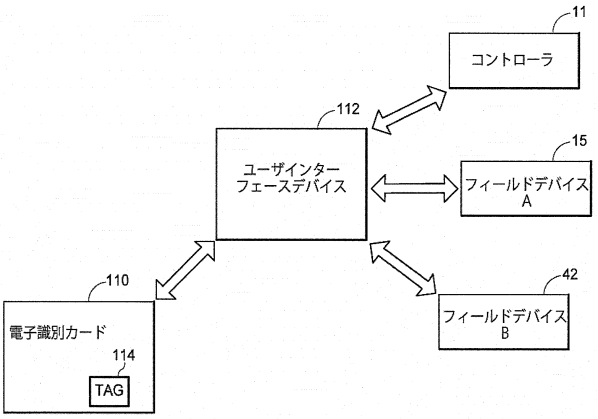

図１Ｂ

【図１Ｃ】

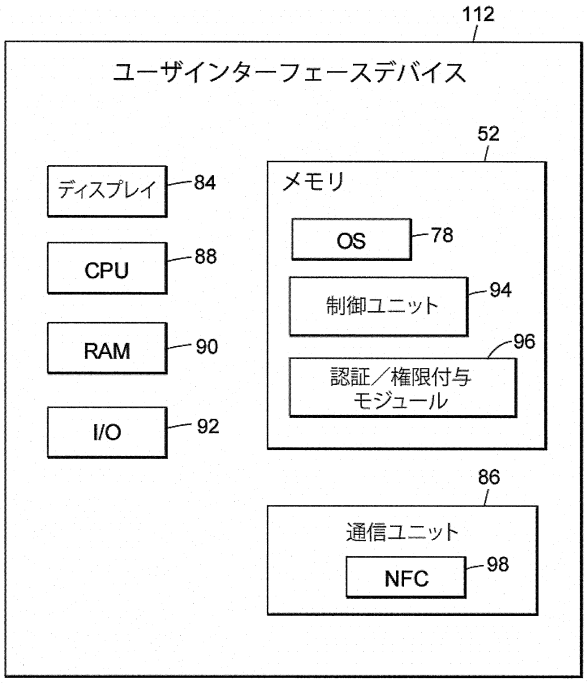

図１Ｃ

【図２Ａ】

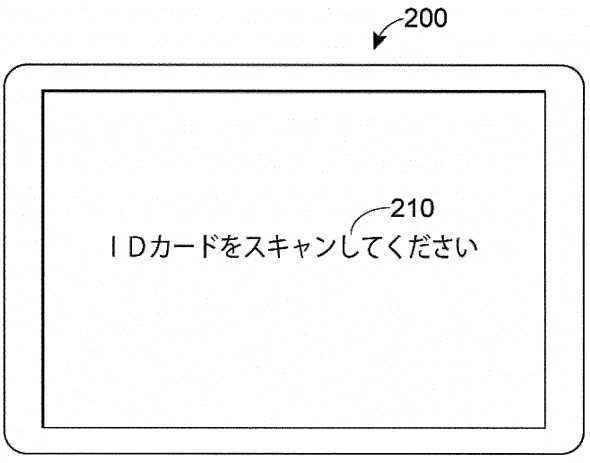

図２Ａ

【図２Ｂ】

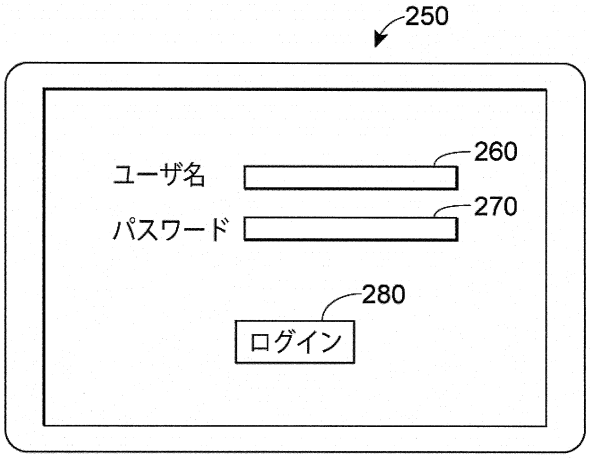

図２Ｂ

【図３Ａ】

アクセス権
300

アクセス権ＩＤ (302)	デバイス (304)	アクセスタイプ (306)	プラント領域 (308)	機能 (310)	時間長 (312)
1	フィールドデバイスＡ	R, R/W	A	構成、トラブルシューティング、キャリブレーション	8
2	フィールドデバイスＢ	R	B	監視	３０分

図３Ａ

【図３Ｂ】

330

ユーザＩＤ (332)	ジョブ機能 (334)	セキュリティグループ (336)	アクセス権 (338)
0001	構成エンジニア	1, 2	1, 2, 3, 4
0002	メンテナンス技術者	3	3, 5, 6, 8

図３Ｂ

【図３Ｃ】

ユーザインターフェースデバイス
360

ユーザインターフェースデバイスＩＤ (362)	アクセス権 (364)	ライセンス機能 (366)
UI01	1, 2, 3, 4	構成
UI02	10, 11, 12	構成、トラブルシューティング、キャリブレーション

図３Ｃ

【図４】

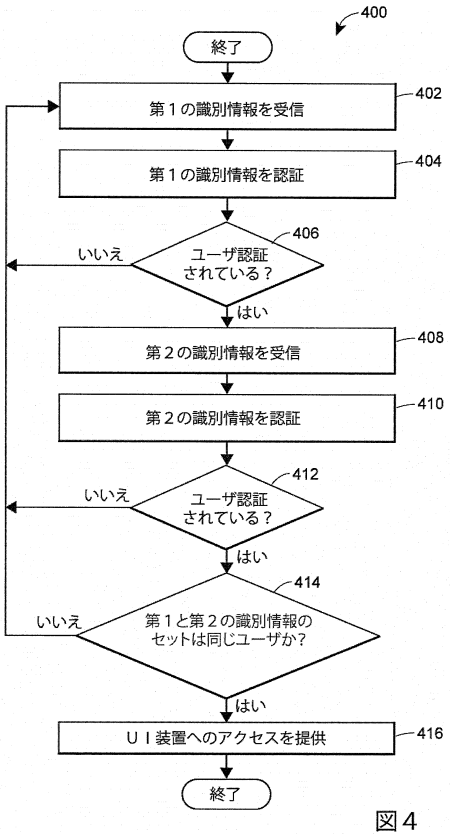

図４

【図５】

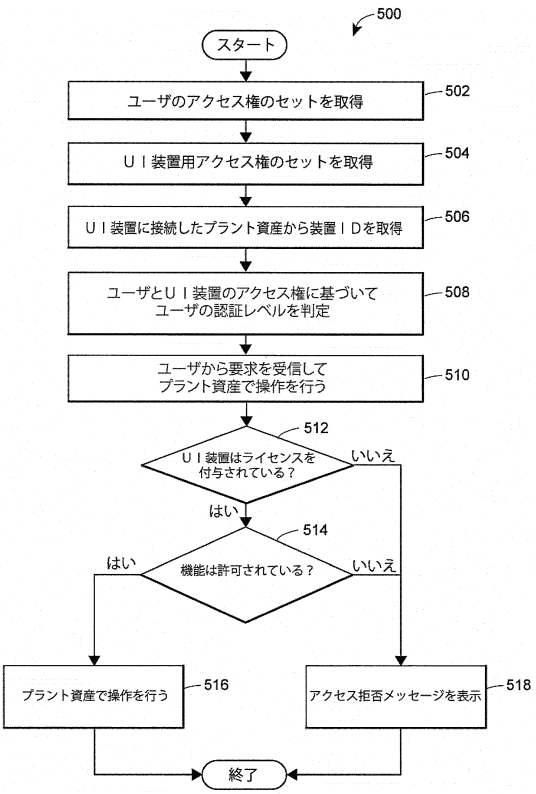

図５

【図６】

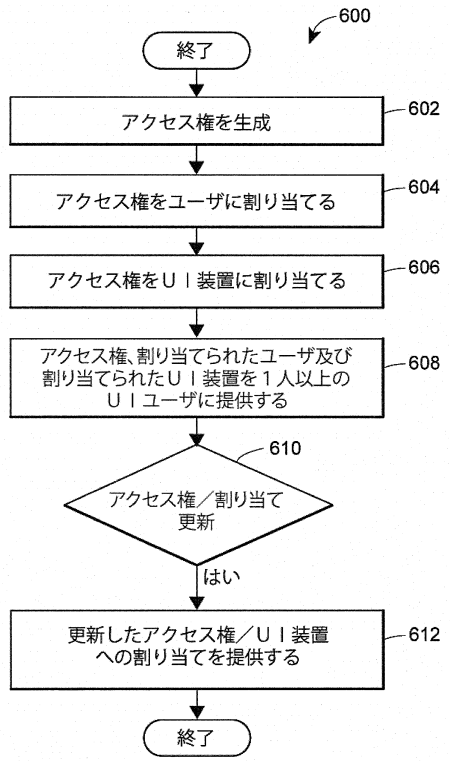

図６

フロントページの続き

アメリカ合衆国 ミネソタ州 ５５３０５ ミネトンカ アーバー レーン ３５０１
(72)発明者 クリストファー・ピー・カンツェス
アメリカ合衆国 ミネソタ州 ５５４１９ ミネアポリス ニュートン アベニュー サウス ４９２１
(72)発明者 ニール・ジェー・ピーターソン
アメリカ合衆国 テキサス州 ７８７５９ オースティン サマーヒル コーヴ ９２０３

審査官 宮司 卓佳
(56)参考文献 特開２０１０－２３１４７３（ＪＰ，Ａ）
特開２０１１－０８６０１２（ＪＰ，Ａ）
特開２０１４－０３２６３３（ＪＰ，Ａ）
特開２０１４－２２５２４０（ＪＰ，Ａ）
国際公開第２００５／０９３５４９（WO，Ａ１）
特表２０１４－５２６０９５（ＪＰ，Ａ）
(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／３１－２１／４６
Ｇ０５Ｂ ２３／０２