(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6467123号
(P6467123)
(45)発行日　平成31年2月6日(2019.2.6)　(24)登録日　平成31年1月18日(2019.1.18)

(51)Int.Cl.　F I
G05B 19/05 (2006.01)　G05B 19/05 L

請求項の数 18　外国語出願　(全 13 頁)

(21)出願番号　特願2013-93295(P2013-93295)
(22)出願日　平成25年4月26日(2013.4.26)
(65)公開番号　特開2013-232190(P2013-232190A)
(43)公開日　平成25年11月14日(2013.11.14)
審査請求日　平成28年4月19日(2016.4.19)
(31)優先権主張番号　13/460,794
(32)優先日　平成24年4月30日(2012.4.30)
(33)優先権主張国　米国(US)

前置審査

(73)特許権者　390041542
ゼネラル・エレクトリック・カンパニイ
アメリカ合衆国、ニューヨーク州　１２３４５、スケネクタデイ、リバーロード、１番
(74)代理人　100137545
弁理士　荒川　聡志
(74)代理人　100105588
弁理士　小倉　博
(74)代理人　100113974
弁理士　田中　拓人
(72)発明者　ジャスティン・ブランドン・チョン
アメリカ合衆国、バージニア州・２４１５３、セーラム、ロアノーク・ブールバード、１５０１番

最終頁に続く

(54)【発明の名称】産業用コントローラのセキュアな動作のためのシステムおよび方法

(57)【特許請求の範囲】
【請求項１】
メモリおよびプロセッサを含む産業用コントローラであって、
前記プロセッサが、前記産業用コントローラをオープンモードで動作させるように構成され、前記オープンモードは、前記産業用コントローラの前記プロセッサが未認証ネットワーク接続またはローカル接続を介して命令を受信することができるように構成されており、
続いて、前記プロセッサが、前記未認証ネットワーク接続を証明書認証済ネットワーク接続に変更して、前記産業用コントローラを前記オープンモードの代わりにセキュアモードで動作させるように構成され、前記セキュアモードは、前記産業用コントローラの前記プロセッサが前記証明書認証済ネットワーク接続を介してのみ命令を受信することができるように構成され、
前記プロセッサが、前記産業用コントローラをネゴシエーションモードで動作させるように構成され、前記ネゴシエーションモードにより、前記産業用コントローラの前記プロセッサが証明機関（ＣＡ）から証明書を取得し、前記産業用コントローラへの未認証ネットワーク接続およびローカル接続をディセーブルにするように構成されている、
産業用コントローラ。
【請求項２】
前記産業用コントローラの前記メモリに記憶されたホワイトリストを含み、前記ホワイトリストが複数の値を含み、各値が、前記産業用コントローラの前記メモリに記憶されて

いる実行可能ファイルに関連付けられる、請求項１に記載の産業用コントローラ。
【請求項３】
前記オープンモードは、前記産業用コントローラが前記メモリに記憶されている複数の実行可能ファイルのうちのいずれかを実行することができるように構成されている、請求項２に記載の産業用コントローラ。
【請求項４】
前記セキュアモードは、前記産業用コントローラの前記プロセッサが前記ホワイトリストに関連する値がない前記メモリに記憶されている前記複数の実行可能ファイルのうちのいずれかを実行することをブロックするように構成されている、請求項２または３に記載の産業用コントローラ。
【請求項５】
前記プロセッサが、前記産業用コントローラを認証モードで動作させるように構成され、前記認証モードは、前記産業用コントローラの前記プロセッサが前記産業用コントローラと構成ツールとの間に前記証明書認証済ネットワーク接続を確立するために前記ＣＡから取得された前記証明書を使用するように構成されている、請求項１から４のいずれかに記載の産業用コントローラ。
【請求項６】
前記証明書認証済ネットワーク接続が、暗号化済認証済ネットワーク接続である、請求項５に記載の産業用コントローラ。
【請求項７】
前記産業用コントローラがセキュアモードの動作を開始した後に、前記プロセッサが、パワーサイクリング、ソフトウェア更新、アプリケーションダウンロード、またはそれらの組合せの間中、前記産業用コントローラを前記セキュアモードで動作させ続けるように構成されている、請求項１から６のいずれかに記載の産業用コントローラ。
【請求項８】
前記未認証ネットワーク接続が、テルネットまたはファイル転送プロトコル（ＦＴＰ）接続を含み、前記証明書認証済ネットワーク接続が、セキュアソケットレイヤ（ＳＳＬ）を含む、請求項１から７のいずれかに記載の産業用コントローラ。
【請求項９】
請求項１から８のいずれかに記載の産業用コントローラと、
前記産業用システムにより制御される、ガス化器、ガス処理ユニット、タービン、発電機、またはそれらの組合せと、
を含む、システム。
【請求項１０】
産業用コントローラをオープンモードで動作させるステップであって、前記産業用コントローラは、オープンモード、ネゴシエーションモード、認証モード、またはセキュアモードのうちの１つで互いに排他的に動作するように構成され、前記オープンモードは、前記産業用コントローラの前記プロセッサが未認証ネットワーク接続を使用して構成ツールと通信することを含む、ステップと、
前記構成ツールから前記産業用コントローラをセキュアモードで動作させる命令を受信するステップと、
前記産業用コントローラを前記ネゴシエーションモードで動作させるステップであって、前記ネゴシエーションモードは、前記プロセッサが証明機関からセキュリティ証明書を取得、未認証ネットワーク接続をディセーブルにすることを含む、ステップと、
前記産業用コントローラを前記認証モードで動作させるステップであって、前記認証モードは、前記プロセッサが前記構成ツールと証明書認証済ネットワーク接続を確立することを含む、ステップと、
前記産業用コントローラを前記セキュアモードで動作させるステップであって、前記セキュアモードは、前記プロセッサが前記証明書認証済ネットワーク接続を介して前記構成ツールと通信することを含む、ステップと、

を含む、方法。
【請求項１１】
前記セキュアモードは、前記産業用コントローラの前記プロセッサがホワイトリストに対応するエントリがないバイナリファイルを実行するのをブロックすることを含む、請求項１０に記載の方法。
【請求項１２】
証明書認証済接続を確立することが、前記産業用コントローラの前記プロセッサが前記構成ツールと証明書認証済、暗号化済接続を確立することを含む、請求項１１に記載の方法。
【請求項１３】
前記セキュアモードが、ローカル接続を介しての前記産業用コントローラの前記プロセッサへのアクセスをディセーブルにすることを含む、請求項１０から１２のいずれかに記載の方法。
【請求項１４】
産業用コントローラのプロセッサによって実行可能な命令を記憶するように構成された有形の非一時的コンピュータ可読媒体であって、前記命令が、
オープンモードでの動作を中止して、前記プロセッサが、未認証ネットワーク接続を介してのまたはローカル接続を介して命令を受信することをブロックする命令を含む、セキュアモードでの動作を開始する命令と、
前記未認証ネットワーク接続を証明書認証済ネットワーク接続に変更して、前記証明書認証済ネットワーク接続を介して前記プロセッサが命令を受信することを可能にする命令と、
前記コンピュータ可読媒体上に記憶されている実行可能ファイルを実行する前に、前記実行可能ファイルが変更されなかったことを前記プロセッサが検証する命令と、
を含み、
オープンモードでの動作を中止してセキュアモードでの動作を開始する前記命令が、
証明機関にコンタクトし、証明書を取得する命令と、
前記証明書を使用して、認証済ネットワーク接続、暗号化済ネットワーク接続、または認証済、暗号化済ネットワーク接続を介して構成ツールと通信する命令と、
を含む、
媒体。
【請求項１５】
構成ツールから前記産業用コントローラを動作のオープンモードから動作のセキュアモードに変更する命令を受信する命令を含む、請求項１４に記載の媒体。
【請求項１６】
前記産業用コントローラがパワーサイクリング、ソフトウェア更新、アプリケーションダウンロード、またはそれらの任意の組合せの間中、前記セキュアモードで動作させ続けるようにする命令を含む、請求項１５に記載の媒体。
【請求項１７】
前記実行可能ファイルが変更されなかったことを検証する前記命令が、
前記実行可能ファイルのためのハッシュ鍵値を判定する命令と、
前記ハッシュ鍵値がホワイトリストファイルに存在するときに前記実行可能ファイルが変更されなかったことを判定する命令と、
を含む、請求項１４から１６のいずれかに記載の媒体。
【請求項１８】
前記産業用コントローラが、ガス化器コントローラ、ガス処理コントローラ、タービンコントローラ、発電機コントローラ、またはそれらの任意の組合せを含む、請求項１４から１７のいずれかに記載の媒体。
【発明の詳細な説明】
【技術分野】

【０００１】
本明細書で開示される主題は、産業用制御システムに関し、より詳細には、産業用制御システムの動作をセキュリティ保護することに関する。
【背景技術】
【０００２】
自動発電システム（例えば、風力タービンシステム、水力タービンシステム、およびガスタービンシステム）や自動製造システム（例えば、精油所、化学製造プラントなど）など産業用制御システムは、現代産業の一般的な特色である。そのような産業用制御システムでは、一般に、産業用コントローラがシステムの動作を制御することができる。例えば、産業用制御システムにおけるいくつかのデバイス（例えば、センサ、ポンプ、弁、アクチュエータなど）が、産業用コントローラによって制御されることがあり、産業用コントローラにデータを報告することができる。さらに、産業用コントローラは、一般に命令（例えば、ファームウェアおよび／またはアプリケーション）を実行することができ、それにより産業用コントローラは、産業用制御システム（例えば、ガスタービンシステム）の動作を制御することができる。これらの命令は、産業用コントローラの製造業者によって提供されてもよい。例えば、これらの命令は、産業用コントローラが産業用制御システムにインストールされる前に、産業用コントローラ上にロードされてもよい。さらに、産業用コントローラは、ネットワーク接続又はローカルポートを介してなど、産業用コントローラにアクセスする、および／または産業用コントローラに命令を提供するいくつかの異なる方法を提供することができる。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】米国特許出願公開第１３／４６０，７２１号明細書
【発明の概要】
【０００４】
本願発明と同等の範囲を有するいくつかの実施形態を以下で要約する。これらの実施形態は、本願発明の範囲を限定することを意図するものではなく、これらの実施形態は、本発明の可能な形態の概要を提供することのみを意図するものである。実際、本発明は、以下で説明される諸実施形態と同様であるまたは異なることもある様々な形態を包含してもよい。
【０００５】
一実施形態では、システムは、メモリおよび産業用コントローラをオープンモードで動作させるように構成されたプロセッサを有する産業用コントローラを含み、オープンモードは、産業用コントローラが未認証ネットワーク接続またはローカル接続を介して命令を受信することができるように構成される。産業用コントローラのプロセッサは、産業用コントローラをセキュアモードで動作させるようにさらに構成され、セキュアモードは、産業用コントローラが認証済ネットワーク接続を介してのみ命令を受信することができるように構成される。
【０００６】
他の実施形態では、方法は、産業用コントローラをオープンモードで動作させるステップを含み、オープンモードは、産業用コントローラに未認証ネットワークプロトコルを使用して構成ツールと通信することを可能にすることを含む。本方法はまた、構成ツールから産業用コントローラをセキュアモードで動作させる命令を受信するステップを含み、セキュアモードは、産業用コントローラが認証済ネットワークプロトコルのみを使用して構成ツールと通信するように制限することを含む。本方法はまた、産業用コントローラをネゴシエーションモードで動作させるステップを含み、ネゴシエーションモードは、証明機関からセキュリティ証明書を取得し、未認証ネットワークプロトコルをディセーブルにすることを含む。本方法はまた、産業用コントローラを認証モードで動作させるステップを含み、認証モードは、産業用コントローラと構成ツールとの間に証明書認証済接続を確立

することを含む。本方法は、産業用コントローラをセキュアモードで動作させるステップをさらに含む。

【０００７】

他の実施形態では、有形の非一時的コンピュータ可読媒体は、産業用コントローラのプロセッサによって実行可能な命令を記憶するように構成される。命令は、未認証ネットワーク接続を介してのまたはローカルポートを介しての産業用コントローラへの通信をディセーブルにする命令を含む。命令は、認証済ネットワーク接続を介しての産業用コントローラへの通信をイネーブルにする命令をさらに含む。命令は、実行可能ファイルが実行できるようにする前にコンピュータ可読媒体上に記憶されている実行可能ファイルが変更されなかったことを検証する命令をさらに含む。

【０００８】

本発明のこれらのおよび他の特徴、態様、および利点は、以下の詳細な説明を、全図面にわたって同様の符号は同様の部分を表す添付の図面と併せ読めば、より良く理解されるであろう。

【図面の簡単な説明】

【０００９】

【図１】本開示の諸態様による、産業用コントローラによって作動される産業用制御システムの一実施形態の概略図である。

【図２】本開示の諸態様による、産業用コントローラが動作のオープンモードからセキュリティモードへそれによって移動することができるプロセスの一実施形態のための流れ図である。

【図３】本開示の諸態様による、産業用コントローラがネゴシエーションモードで動作することができるプロセスの一実施形態の流れ図である。

【図４】本開示の諸態様による、産業用コントローラが認証モードで動作することができるプロセスの一実施形態の流れ図である。

【発明を実施するための形態】

【００１０】

本発明の１つまたは複数の特定の実施形態が以下で説明される。これらの実施形態を簡明に説明するために、必ずしも実際の実施形態のすべての特徴が本明細書に記載されていないことがある。いずれのエンジニアリングまたは設計プロジェクトにおいてもと同様に、いずれのそのような実際の実施形態の開発においても、実施形態ごとに異なる可能性があるシステム関連の制約およびビジネス関連の制約の順守など、開発者の特定の目的を達成するために多数の実施形態特有の決定がなされなければならないことを理解されたい。さらに、そのような開発努力は、複雑で時間のかかるものである可能性があるが、それにもかかわらず、本開示の利益を受ける当業者にとっては、設計、製作、および製造の日常的な仕事であろうことを理解されたい。

【００１１】

本発明の様々な実施形態の要素を紹介する場合、冠詞「ａ」、「ａｎ」、「ｔｈｅ」、および「ｓａｉｄ」は、１つまたは複数の要素が存在することを意味するものとする。用語「ｃｏｍｐｒｉｓｉｎｇ（備える）」、「ｉｎｃｌｕｄｉｎｇ（含む）」、および「ｈａｖｉｎｇ（有する）」は包括的であるものとし、列挙された要素以外の追加の要素が存在してもよいことを意味するものとする。さらに、本明細書で使用される場合は、用語「実行可能ファイル」および「バイナリファイル」は、両方とも一般的に、プロセッサ（例えば、産業用コントローラのプロセッサ）によって実行されてもよい命令（例えば、バイナリ命令）を含むコンピュータ可読ファイルを指してもよい。さらに、本明細書で使用される場合は、用語「ソフトウェア開発者」は、一般に、産業用コントローラの動作を制御するためのソースコードの形での命令および／または実行可能ファイルを開発、維持、および／または提供する団体を指してもよい。さらに、本明細書で使用される場合は、用語「ホワイトリスト」は、産業用コントローラ上で動作することを認可された実行可能ファイルを識別するリストを含むファイルを指してもよい。さらに、用語「認可された」は、

本明細書では、信頼できるソース（すなわち、ソフトウェア開発者）からのものであることが検証され、そのコンテンツが信頼できるソースによって提供された場合と同じものであると検証された実行可能ファイルを指すために使用されてもよい。

【００１２】

一般に、産業用制御システムの産業用コントローラをセキュアモードで動作させることが望ましいことがある。すなわち、一般に、産業用制御システムのセキュリティ全体を改善するために産業用コントローラの典型的な挙動または動作にいくつかの制限を課すことが望ましいことがある。例えば、以下で詳細に説明されるように、産業用コントローラをセキュアモードで動作させることは、一般に、未認証実行可能ファイルの実行をブロックし、かつ／または未認証の人またはシステムによる産業用コントローラへのアクセスをブロックすることができる。したがって、本開示のシステムおよび方法は、セキュアモードでの産業用コントローラの動作をイネーブルにし、この場合、セキュアモードは、一般に、産業用コントローラへの未認証アクセスをブロックする。さらに、本開示の諸実施形態は、産業用コントローラにいくつかのセキュリティ制限を徐々に適用することにより産業用コントローラが(例えば、制限なしの)オープンモードから（例えば、追加のセキュリティ制限のある）セキュアモードへ移動することができるようにする。産業用コントローラが産業用コントローラの様々な動作（例えば、パワーサイクルおよびソフトウェア更新）にまたがって存続するセキュアモードで動作することができるようにすることにより、本開示の諸実施形態は、一般に、未認証アクセスおよび／または未認証命令の実行のリスクが低減された産業用制御システムを提供する。

【００１３】

上記を考慮して、図１は、産業用制御システム１０を例示する概略図である。例示された産業用制御システム１０は、本開示の諸態様による、少なくともオープンモードおよびセキュアモードで動作するように構成することができる産業用コントローラ１２（例えば、Ｍａｒｋ（登録商標）Ｖｉｅ、または米国ニューヨーク州スケネクタディ市のゼネラルエレクトリック社から入手可能な任意の他のＭａｒｋ（登録商標）産業用コントローラ）を含む。さらに、産業用コントローラ１２は、いくつかのフィールドデバイス１６、１８および２０の動作を制御するためにネットワーク１４に結合されてもよい。例えば、例示された産業用コントローラ１２は、ガスタービンシステム２２の動作を監視および制御するためにネットワーク１４を介していくつかのフィールドデバイス１６、１８、および２０（温度センサ、圧力センサ、電圧センサ、制御弁、アクチュエータ、または産業用制御システムのための同様のフィールドデバイス）からセンサデータを受信する。他の実施形態では、ガスタービンシステム２２ではなく、産業用制御システム１０によって監視および制御されるシステムは、例えば、任意の自動製造システム（例えば、精油所システム、化学生産システム、ガス化システム、もしくは同様の自動製造システム）または自動発電システム（例えば、発電所、蒸気タービンシステム、風力タービンシステム、および同様の自動発電システム）を含むことができる。例えば、一実施形態では、ガス化システムは、合成ガスを生成するために炭素質供給原料をガス化するように構成されたガス化器、望ましくない要素（例えば、酸性ガス）を除去するために合成ガスを処理するように構成されたガス処理ユニット、タービンを駆動するために合成ガスを燃焼させるように構成された燃焼器、および電力を生産するように構成されたタービンに結合された発電機を含むことができる。そのような実施形態では、産業用コントローラ１２は、少なくともフィールドデバイス１６、１８、および２０を使用してガス化システムの様々な構成要素（例えば、ガス化器、ガス処理ユニット、燃焼器、およびタービン）を監視および制御することができる。

【００１４】

例示された産業用制御システム１０では、フィールドデバイス１６、１８、および２０は、産業用コントローラ１２に（例えば、ネットワーク１４を介して）通信可能に結合され、ガスタービンシステム２２の動作の様々な態様およびパラメータを監視および制御する（例えば、ガスタービンシステムの燃焼器内の温度を監視し、ガスタービンシステムの

シャフトに結合された発電機の電圧出力を制御し、燃焼器に入る流体の流れを調整し、熱回収蒸気発生器（ＨＲＳＧ）の蒸気入力を制御するなど）。例示された産業用制御システム１０は、簡略化された産業用制御システムを表し、他の産業用制御システムは、任意の自動システム２２の一部分を監視および制御するために任意の適切な数の産業用コントローラ１２、ネットワーク１４、ネットワークデバイス、フィールドデバイスなどを含むことができることを理解されたい。

【００１５】

図示された実施形態では、産業用コントローラ１２は、フィールドデバイス１６、１８、または２０のうちの任意の１つと通信し、それを制御するためにネットワーク１４を使用することができる。例えば、産業用コントローラ１２は、産業プラントに常駐してもよく、デバイス１６、１８、２０に関する１つまたは複数のプロセス条件を調整するように構成されてもよい。ネットワーク１４は、通信をイネーブルにするのに適した任意の電子および／または無線ネットワークとすることができ、ファイバ媒体、ツイストペアケーブル媒体、無線通信ハードウェア、イーサネット(商標）ケーブル媒体（例えば、Ｃａｔ－５、Ｃａｔ－７）などを含むことができる。さらに、ネットワーク１４は、毎秒１００ＭＢ以上の通信速度で産業用制御システム１０の構成要素を接続するのに適した高速イーサネット(商標）サブバスなど、いくつかのサブバスを含むことができる。さらに、ネットワーク１４は、米国電気電子技術者協会(ＩＥＥＥ)８０２．３標準規格に準拠したＩ／Ｏネットワークなどの入力／出力（Ｉ／Ｏ）ネットワークを含むことができる。ネットワーク１４はまた、毎秒約３１．２５Ｋｂの通信速度で産業用制御システム１０の構成要素を接続するのに適したＨ１ネットワークサブバスを含むことができる。サブバスは、例えば、リンキングデバイス、またはドイツ、ハールのＳｏｆｔｉｎｇ　ＡＧ社によって提供される名称ＦＧ－１００の下で入手可能なゲートウェイ、および／または米国ニューヨーク州スケネクタディ市のゼネラルエレクトリック社から入手可能なＩ／Ｏパックなどのゲートウェイを使用することにより、相互に通信することができる。実際、ネットワーク１４のいくつかの相互接続されたサブバスが産業用制御システム１０の構成要素の間で通信するために使用されてもよい。

【００１６】

メモリ３４およびプロセッサ３６を含む産業用コントローラ１２は、一般に、産業用制御システム１０の動作を制御するために、命令（例えば、実行可能ファイル内のバイナリ命令）を実行することができる。例えば、産業用コントローラ１２のメモリ３４は、ガスタービンシステム２２の一部分の中に配置されたフィールドデバイス１６、１８、および２０を制御および監視するためにプロセッサ３６によって実行することができるバイナリ命令を含む１つまたは複数のファイルを含むことができる。これらの実行可能ファイルは、例えば、産業用コントローラ１２が産業用制御システム１０にインストールされる前に、産業用コントローラ１２の製造業者によって産業用コントローラ１２のメモリ３４に最初にインストールされてもよい。さらに、産業用コントローラ１２のメモリ３４に記憶されている実行可能ファイルは、例えば、前のソフトウェアの特徴を増大し、ならびに性能を改善するために、ときどき更新されてもよい。

【００１７】

さらに、ヒューマンマシンインターフェース（ＨＭＩ）システム２７、製造実行システム（ＭＥＳ）２８、監視制御およびデータ取得（ＳＣＡＤＡ）システム２９、分散制御システム（ＤＣＳ）３０、または同様のインターフェースシステムをホストすることができるメモリ２５およびプロセッサ２６を含むデバイス２４は、産業用コントローラ１２に（例えば、ネットワーク１４または別の適切なネットワークを介して）通信可能に結合される。とりわけ、いくつかの実施形態では、デバイス２４は、米国ニューヨーク州スケネクタディ市のゼネラルエレクトリック社から入手可能な（要素３２によって表されている）ＴｏｏｌｂｏｘＳＴ（登録商標）などの構成アプリケーションまたはツールをホストすることができる。一般に、前述のシステムは、ユーザが産業用コントローラ１２の動作をそれによって監視および制御することができる１つまたは複数のインターフェースを提供す

ることができる。例えば、ＨＭＩ２７および／またはＴｏｏｌｂｏｘＳＴ３２は、産業用制御システム１０の様々なパラメータ（例えば、産業用コントローラ１２のメモリ３４に記憶されている）を強制または設定することができるユーザインターフェースを提供することができる。他の例では、ＨＭＩ２７および／またはＴｏｏｌｂｏｘＳＴ３２は、コントローラ１２のメモリ３４に記憶されている様々な実行可能ファイルが新しいバージョンにそれを介して更新されるインターフェースを含むことができる。いくつかの実施形態では、前述のシステムは、単一のデバイス２４上でホストされてもよく、一方、他の実施形態では、それぞれ、産業用制御システム１０内の１つまたは複数のデバイス上にインストールされてもよい。

【００１８】

さらに、メモリ４０およびプロセッサ４２を有するセキュリティサーバ３８は、（例えば、ネットワーク１４または別の適切なネットワークを介して）産業用コントローラ１２およびデバイス２４に通信可能に結合されてもよく、証明機関（ＣＡ）４４をホストすることができる。セキュリティサーバ３８によってホストされた証明機関４４は、一般に、例えば、産業用コントローラ１２とデバイス２４との間のセキュアな通信をイネーブルにするために、産業用制御システム１０の中で証明書を発行し、取り消すことができる。図１には単一のセキュリティサーバ３８および証明機関４４しか例示されていないが、いくつかの実施形態では、産業用制御システム１０は、１つ、２つ、３つ、４つ、またはそれ以上のセキュリティサーバ３８および／または証明機関４４を有してもよいことを理解されたい。

【００１９】

一般的に言って、証明書は、証明書ホルダの識別を検証するためにディジタル署名を使用することができる電子文書である。例えば、制御システム１０の様々な構成要素が相互認証または他のセキュリティ技法（例えば、二要素認証）を使用して相互の識別を検証することが望ましい。一般に、相互認証は、第１の証明書ホルダ（例えば、デバイス２４）が第２の証明書ホルダ（例えば、産業用コントローラ１２）の識別を検証し、相互に、第２の証明書ホルダが引き続き（例えば、ネットワーク１４を介して）第１の証明書ホルダの識別を検証することを指してもよい。したがって、相互認証は、産業用制御システム１０の未認証使用の可能性を低減することができる。

【００２０】

したがって、本開示の諸実施形態は、証明書を使用した相互認証（例えば、双方向認証）を使用して産業用コントローラ１２への通信をセキュリティ保護するのに適したシステムおよび方法を含む。例えば、以下で詳細に論じられるように、デバイス２４（例えば、デバイス２４上で動作するＨＭＩ２７またはＴｏｏｌｂｏｘＳＴ３２）および産業用コントローラ１２は、証明機関４４からそれぞれの証明書を取得することができる。次いで、例えば、ＴｏｏｌｂｏｘＳＴ３２が産業用コントローラ１２への認証済通信チャネルを確立することを必要とする場合は、これらの２つのデバイスは、それぞれの識別を検証することの一部分としてそれぞれの証明書を交換することができる。この認証は、一般に、デバイス２４および／または産業用コントローラ１２の未認証使用の可能性を低減または除去することができる。さらに、デバイス２４は、産業用制御システム１０のセキュリティをさらに改善するために産業用コントローラ１２の識別を相互に検証することができる。さらに、この認証に加えて、いくつかの実施形態はまた、暗号化の使用が認証済通信チャネルをさらにセキュリティ保護することができるようにすることができる。すなわち、いくつかの実施形態では、産業用コントローラ１２およびデバイス２４は、通信内容が産業用制御システム１０内の他のデバイスによって一般的に読み出し不可能であるように、これらの内容を暗号化するために他方のデバイスの証明書に含まれているデータの一部分（例えば、公開鍵）をそれぞれ使用することができる。

【００２１】

通信をセキュリティ保護することに加えて、本開示の諸実施形態は、実行の前に、産業用コントローラ１２のメモリ３４に記憶されている各実行可能ファイルを検証するために

ホワイトリスティング方法を利用することができる。例えば、このホワイトリストファイルは、特定のソフトウェアリリースにおける認可済実行可能ファイルのために決められたハッシュ鍵値の集まりを含むことができる。すなわち、各実行可能ファイルが構築された（例えば、コンパイルされた）後に、実行可能ファイルがハッシュ関数（例えば、巡回冗長検査（ＣＲＣ）ハッシュ関数、メッセージダイジェストアルゴリズム（ＭＤ）ハッシュ関数、セキュアハッシュアルゴリズム（ＳＨＡ）ハッシュ関数、または他の適切なハッシュ関数）への入力として提供されてもよく、その実行可能ファイルに関連付けられたハッシュ鍵値出力は、ホワイトリストファイル（例えば、拡張可能マークアップ言語（ＸＭＬ）ファイル）に記憶されてもよい。さらに、ホワイトリストファイルは、産業用コントローラにセキュアに提供されることが可能である（例えば、パッケージングおよび／またはトランスポートの前に暗号化され、産業用コントローラによって復号される）。産業用コントローラはまた、特定の実行可能ファイルを実行する前に、その特定の実行可能ファイルを同じハッシュ関数（例えば、ＣＲＣ、ＭＤ５、ＳＨＡ－１、または他の適切なハッシュ関数）に提供することができ、ハッシュ関数から出力されたハッシュ鍵値がホワイトリストファイルに含まれているかどうかを引き続き判定することができる。ハッシュ鍵値がホワイトリストファイルにある場合は、産業用コントローラは、特定の実行可能ファイルが（例えば、信頼できるソースから）認可されており、構築されて以来変更されていないと結論を下してもよく、続けて実行可能ファイルを実行することができる。しかし、ハッシュ鍵値がホワイトリストファイルにない場合は、産業用コントローラは、特定の実行可能ファイルの実行をブロックすることができ、未認証実行の試みをログすることができる。このようなやり方でホワイトリスティング方法を使用することにより、産業用コントローラ１２は、実行の前に各実行可能ファイルの識別および内容を効率よく同時に検証することができる。

【００２２】

したがって、本開示の諸実施形態は、産業用コントローラ１２を動作のオープンモードから動作のセキュアモードへ移動するために（例えば、順次）いくつかのセキュリティ制限を課すことができる。図２は、本開示の諸態様による、産業用コントローラ１２が動作のオープンモードから動作のセキュアモードへそれによって移動することができるプロセス５０の一実施形態のための流れ図である。プロセス５０は、産業用コントローラ１２がオープンモードで動作すること（ブロック５２）から開始する。一般的に言って、産業用コントローラ１２の動作のオープンモードは、産業用コントローラとの通信を制限せず、産業用コントローラによる実行可能ファイルの実行も制限しない。このオープンモードで動作している間に、産業用コントローラ１２は、産業用コントローラの動作のモードをオープンモードからセキュアモードに変更する命令を構成ツール（例えば、デバイス２４上のＴｏｏｌｂｏｘＳＴ３２）から受信することができる（ブロック５４）。

【００２３】

産業用コントローラ１２をセキュアモードで動作させる命令を構成ツール（例えば、デバイス２４上のＴｏｏｌｂｏｘＳＴ３２）から受信することに応答して、産業用コントローラは、ネゴシエーションモードで動作すること（ブロック５６）に切り換えることができる。一般的に言って、ネゴシエーションモード中に、産業用コントローラ１２は、一般に、セキュアモード動作の準備をすることができる。例えば、図３を参照すると、本開示の諸態様による、産業用コントローラ１２がネゴシエーションモードで実行することができるプロセス７０の一実施形態のための流れ図が例示されている。ネゴシエーションモードプロセス７０は、産業用コントローラ１２が証明機関（例えば、ネットワーク１４を介してセキュリティサーバ３８上の証明機関４４）からセキュリティ証明書を取得すること（ブロック７２）から開始することができる。図４に関して以下で論じられるように、この証明書は、例えばＴｏｏｌｂｏｘＳＴ３２へのセキュアな（例えば、認証済および／または暗号化済）接続を確立するために産業用コントローラ１２によって後ほど使用されてもよい。次に、産業用コントローラ１２は、産業用コントローラ１２のための未認証および／または未暗号化ネットワーク接続をディセーブルにすることができる（ブロック７４

）。すなわち、産業用コントローラ１２のプロセッサ３６は、産業用コントローラへの未認証および／または未暗号化通信に関連する接続、ポート、および／またはプロトコルをディセーブルにする１つまたは複数の命令を実行することができる。例えば、いくつかの実施形態では、産業用コントローラ１２は、ファイル転送プロトコル（ＦＴＰ）、テルネット、および／または（例えば、ネットワーク１４を介しての）産業用コントローラ１２へのいずれの他の未認証接続または平文接続をもディセーブルにすることができる。さらに、産業用コントローラ１２は、産業用コントローラ１２のためのローカルポートアクセス（例えば、ローカルシリアルポートを介して産業用コントローラ１２をログインおよび／または制御する能力）をディセーブルにすることができる（ブロック７６）。

【００２４】

さらに、ネゴシエーションモードプロセス７０の一部分として、産業用コントローラ１２はまた、ホワイトリストファイルへの対応するエントリがないファイルの実行をブロックすることができる（ブロック７８）。すなわち、上記で説明されたように、これらの産業用コントローラ１２の実施形態は、特定のソフトウェアリリースのための実行可能ファイルと共に暗号化済ホワイトリストファイルを受信することができる。さらに、実行可能ファイルのうちの１つ（例えば、起動実行可能ファイル）は、ホワイトリストファイルを復号するために使用され得る秘密鍵値を含むことができる。次いで、特定の実行可能ファイルが実行を試みた場合、産業用コントローラ１２は、実行を試みるためにハッシュ鍵値を復号済ホワイトリストファイルに記載されているハッシュ鍵値と比較することができる。実行可能ファイルのためのハッシュ鍵値がホワイトリストファイルにない場合は、実行可能ファイルの実行はブロックされてもよい。ネゴシエーションプロセス中に、産業用コントローラ１２はまた、産業用コントローラ１２がネゴシエーションモードに入る前に実行を開始したいずれの実行可能ファイルも認可されることを検証することができることも理解されたい。すなわち、産業用コントローラ１２は、産業用コントローラ１２がネゴシエーションモードに入ったときに産業用コントローラ１２上で現在実行しているすべての実行可能ファイルのために実行可能ファイルの検証を実行することができる。

【００２５】

図２に戻ると、産業用コントローラ１２がネゴシエーションモードを完了した後は（ブロック５６）、産業用コントローラ１２は、認証モードで動作し始めることができる（ブロック５８）。一般的に言って、認証モードは、産業用コントローラ１２と構成ツール（例えば、デバイス２４上のＴｏｏｌｂｏｘＳＴ３２）との間にセキュアな（例えば、認証済および／または暗号化済）通信を確立する。例えば、図４を参照すると、本開示の諸態様による、産業用コントローラ１２が認証モードで実行することができるプロセス９０の一実施形態のための流れ図が例示されている。例示されているプロセス９０は、産業用コントローラ１２が産業用コントローラ１２への認証済および／または暗号化済接続（例えば、セキュアソケットレイヤ（ＳＳＬ）接続）を確立する要求を構成ツール（例えば、ＴｏｏｌｂｏｘＳＴ３２）から受信するステップ（ブロック９２）から開始する。プロセス９０は、産業用コントローラ１２が構成ツール（例えば、ＴｏｏｌｂｏｘＳＴ３２）と産業用コントローラ１２との間に認証済および／または暗号化済接続を確立するステップ（ブロック９４）を続行する。

【００２６】

再度図２を参照すると、産業用コントローラ１２が認証モードを完了した後に（ブロック５８）、産業用コントローラ１２は、セキュアモードで動作し始めてもよい（ブロック６０）。（例えば、図３および４で説明されたように）ネゴシエーションモードおよび認証モード中に産業用コントローラに課されたセキュリティ制限は、セキュアモードで適用され続けてもよいことを理解されたい。すなわち、産業用コントローラ１２がセキュアモードで動作している場合は、産業用コントローラへの未認証および／または未暗号化通信（例えば、ＦＴＰ、テルネット、ローカルポート通信）は、禁止されてもよく、すべての実行可能ファイルは、それらが実行の前に認可されていることを保証するために、ホワイトリストファイルと比較して検証されてもよい。セキュアモードは、パワーサイクリング

および／またはソフトウェア更新の間中、産業用コントローラ１２に存続してもよいことも理解されたい。例えば、いくつかの実施形態では、産業用コントローラ１２が再起動しているとき、産業用コントローラ１２は、産業用コントローラ１２がパワーサイクリングの前にセキュアモードで作動されていたことを示すメモリ内の変数に遭遇することがある。したがって、再起動プロセス中に、産業用コントローラ１２は、一般に、（例えば、産業用コントローラ１２が産業用制御システム１０を制御し始める前に）所望のセキュリティ制限を適用するためにネゴシエーションモードの動作を実行することができる（例えば、図３のプロセス７０）。したがって、産業用コントローラ１２は、セキュアモードでの（例えば、ＴｏｏｌｂｏｘＳＴ３２からの暗号化済接続しか受容せず、認可済実行可能ファイルしか実行しない）動作を開始することができる。

【００２７】

本開示の技術的効果は、産業用制御システム１０のセキュリティ全体に対する改善を含む。すなわち、本開示の諸実施形態は、一般に、未認証実行可能ファイルの実行をブロックし、かつ／または未認証の人またはシステムによる産業用コントローラへのアクセスをブロックすることができるセキュアモードで産業用コントローラ１２を動作させることをできるようにする。さらに、本開示の諸実施形態は、いくつかのセキュリティ制限を産業用コントローラ１２に徐々に適用することにより産業用コントローラ１２が（例えば、制限のない）オープンモードから（例えば、追加のセキュリティ制限のある）セキュアモードへ移動することができるようにする。産業用コントローラ１２が産業用コントローラ１２の様々な動作（例えば、パワーサイクル、ソフトウェアダウンロード、および／またはソフトウェアアップロード）にまたがって存続するセキュアモードで動作することができるようにすることにより、本開示の諸実施形態は、一般に、未認証アクセスおよび／または未認証命令の実行のリスクが低減された産業用制御システム１０を提供する。

【００２８】

本書は、最良の形態を含めて、本発明を開示するために、さらに、当業者なら誰でも任意のデバイスまたはシステムを作成し使用すること、および任意の組み込まれた方法を実施することを含めて本発明を実施することができるようにするために、例を使用する。本発明の特許性のある範囲は、特許請求の範囲によって定義され、当業者に思い付く他の例を含むことができる。そのような他の例は、特許請求の範囲の文言と異ならない構造要素を有する場合、または特許請求の範囲の文言と事実上異ならない同等の構造要素を含む場合、特許請求の範囲内にあるものとする。

【符号の説明】

【００２９】

１０　産業用制御システム
１２　産業用コントローラ
１４　ネットワーク
１６　フィールドデバイス
１８　フィールドデバイス
２０　フィールドデバイス
２２　ガスタービンシステム
２４　デバイス
２５　メモリ
２６　プロセッサ
２７　ヒューマンマシンインターフェース（ＨＭＩ）システム
２８　製造実行システム（ＭＥＳ）
２９　監視制御およびデータ取得（ＳＣＡＤＡ）システム
３０　分散制御システム（ＤＣＳ）
３２　ＴｏｏｌｂｏｘＳＴ
３４　メモリ
３６　プロセッサ

３８　セキュリティサーバ
４０　メモリ
４２　プロセッサ
４４　証明機関（ＣＡ）

【図１】

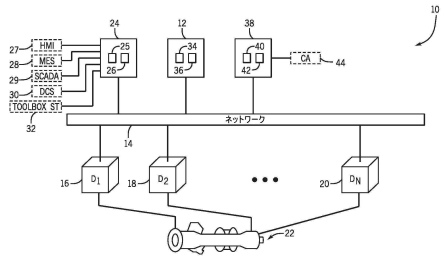

FIG. 1

【図２】

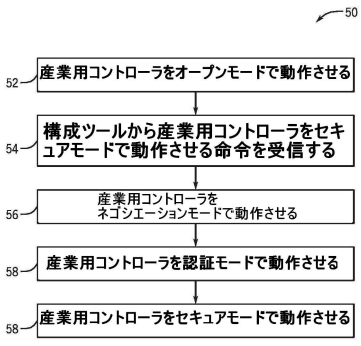

FIG. 2

【図３】

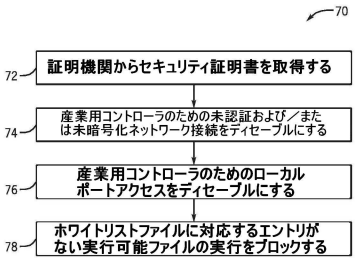

FIG. 3

【図４】

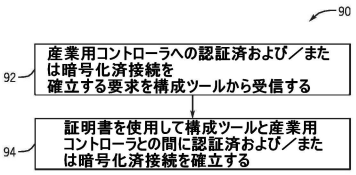

FIG. 4

フロントページの続き

(72)発明者　デイビッド・リチャード・ソッキー
アメリカ合衆国、バージニア州・２４０１８－５４０２、セーラム、ロアノーク・ブールバード、１５０１番
(72)発明者　パヴァン・クマール・シン・サクール
インドアンドラ・プラデッシュ・５００００１、ハイデラバッド・ハイテック・シティ、サイバー・パール・ブロック・１、セカンド・フロアー、ユニット・ナンバー０２－０１、ジーイー・ハイデラバッド・テクノロジー・センター
(72)発明者　ウィリアム・ロバート・ペッティグルー
アメリカ合衆国、バージニア州・２４１５３、セーラム、ロアノーク・ブールバード、１５０１番
(72)発明者　ロバート・ジェームズ・ボーリング
アメリカ合衆国、サウスカロライナ州・２９６１５、グリーンヴィル、ガーリングトン・ロード、３００番

審査官　山村　秀政

(56)参考文献　国際公開第２０１１／１２８９９３（WO，Ａ１）
特開平０３－２６８００５（ＪＰ，Ａ）
特開２００１－２４９８９９（ＪＰ，Ａ）
特開平１１－１６１３２１（ＪＰ，Ａ）
特開２０１１－０７６４６２（ＪＰ，Ａ）
特開２００９－０８６９０５（ＪＰ，Ａ）
特開２００９－１００００６２（ＪＰ，Ａ）
特開２００１－２９２１７６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０５Ｂ　　１９／０５