(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 105278398 B
(45)授权公告日 2019.08.16

(21)申请号 201410799473.2

(22)申请日 2014.12.19

(65)同一申请的已公布的文献号
申请公布号 CN 105278398 A

(43)申请公布日 2016.01.27

(30)优先权数据
62/021,438 2014.07.07 US
14/446,412 2014.07.30 US
14/469,931 2014.08.27 US
14/519,066 2014.10.20 US

(73)专利权人 基岩自动化平台公司
地址 美国加利福尼亚州

(72)发明人 S·加尔潘 T·克力士
J·G·加尔文 A·鲁亚科斯

(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 邬少俊 王英

(51)Int.Cl.
G05B 19/042(2006.01)

(56)对比文件
US 2009204458 A1,2009.08.13,
WO 2006059195 A1,2006.06.08,
CN 103376766 A,2013.10.30,
CN 103701919 A,2014.04.02,
CN 102546707 A,2012.07.04,
US 2014068712 A1,2014.03.06,

审查员 贺春圆

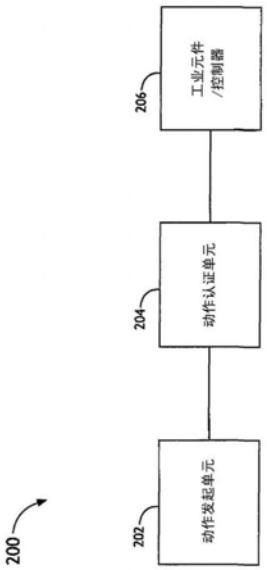
权利要求书3页 说明书11页 附图5页

(54)发明名称

工业控制系统中的操作员动作认证

(57)摘要

经由从动作发起单元到通信/控制模块或任何其它工业元件/控制器的认证路径来操作员动作和/或其它命令或请求的安全。在实施中，工业控制系统包括动作认证单元，其被配置为对由动作发起单元所生成的动作请求进行签名。目的通信/控制模块或任何其它工业元件/控制器被配置为接收被签名的动作请求，验证被签名的动作请求的真实性，并且当被签名的动作请求的真实性被验证时，执行所请求的动作。



CN 105278398 B

1.一种安全工业控制系统,包括:

动作发起单元,其被配置为传输在所述动作发起单元处接收的动作请求;

动作认证单元,其物理地位于远离所述动作发起单元处并且包括与存储介质通信的至少一个处理器,所述存储介质具有由密钥管理实体提供的存储在其上的私钥,其被配置为:

接收来自所述动作发起单元的所述动作请求,

确定所接收的动作请求是否是独立于所述动作发起单元的授权的动作请求,

使用所述私钥对所接收的动作请求进行签名,从而基于所述确定生成所述动作请求的被签名的版本,

传输所述动作请求;以及

与一个或多个工业元件通信的通信/控制模块,所述一个或多个工业元件包括至少一个输入/输出模块,其可操作用于接收工业传感器信息或将控制信息发送到工业驱动器或电机,所述通信/控制模块包括至少一个处理器和承载能够由所述至少一个处理器执行的指令组的非瞬时性介质,所述指令组包括用于执行以下操作的指令:

从所述动作认证单元接收所述动作请求,

基于确定所接收的动作是否是所述动作请求的被签名的版本来认证所接收的动作请求,以及

基于所接收的动作请求是否是经认证的动作请求来执行所述动作请求,其中,所述动作请求包括操作员控制动作,包括:读取或改变控制设定点,控制一个或多个驱动器,以及执行来自操作员接口或工程接口的控制命令。

2.根据权利要求1所述的工业控制系统,其中,所述动作发起单元包括以下中的至少一个:操作员接口、工程接口、本地应用接口、以及远程应用接口。

3.根据权利要求1所述的安全工业控制系统,其中,所述动作认证单元包括便携式加密装置,其包括与其上存储有所述私钥的所述存储介质通信的所述至少一个处理器。

4.根据权利要求3所述的安全工业控制系统,其中,所述处理器包括加密的微处理器。

5.根据权利要求3所述的安全工业控制系统,其中,所述便携式加密装置包括智能卡。

6.根据权利要求1所述的安全工业控制系统,其中,所述动作认证单元包括安全的工作站。

7.根据权利要求6所述的安全工业控制系统,其中,所述安全的工作站能够经由以下中的至少一个来访问:物理密钥、便携式加密装置、以及生物计量密码装置。

8.根据权利要求1所述的安全工业控制系统,其中,所述通信/控制模块和所述至少一个输入/输出模块被配置为在各个制造点处从所述密钥管理实体接收相应的第一唯一的安全凭证和第二唯一的安全凭证,所述第一唯一的安全凭证和所述第二唯一的安全凭证被存储在所述通信/控制模块和所述至少一个输入/输出模块的相应的存储器中,其中,所述第一唯一的安全凭证和所述第二唯一的安全凭证中的至少一个能够由所述密钥管理实体在不同于所述通信/控制模块和所述至少一个输入/输出模块中的相应的一个的相应制造点的地点处进行以下中的至少一个:修改、撤销、或认证。

9.根据权利要求1所述的安全工业控制系统,其中,所述动作认证单元被配置为在将所述动作请求传输到所述通信/控制模块之前对所述动作请求进行加密。

10.根据权利要求1所述的安全工业控制系统,其中,所述通信/控制模块进一步包括虚

拟按键开关，其使得所述至少一个处理器能够在将所述动作请求认证为所述动作请求的被签名的版本时，执行所述动作请求。

11.根据权利要求1所述的安全工业控制系统，其中，所述通信/控制模块和所述动作认证单元进一步被配置为执行认证序列。

12.根据权利要求1所述的安全工业控制系统，其中，所述一个或多个工业元件进一步包括以下中的至少一个：通信/控制模块、电源模块、现场装置、交换机、工作站、以及物理互连装置。

13.一种通信/控制模块，包括：

至少一个处理器；以及

非瞬时性介质，其承载有能够由所述至少一个处理器执行的指令组，所述指令组包括用于执行以下步骤的指令：

接收在动作发起单元处启动的动作请求，其中：

所述动作请求的未签名的版本被从所述动作发起单元传输到物理地位于远离所述动作发起单元处的动作认证单元，

所述动作认证单元确定所接收的动作请求是否是独立于所述动作发起单元的授权的动作请求，

所述动作认证单元基于所述确定生成所述动作请求的被签名的版本，以及

所述动作认证单元将所述动作请求传输到所述通信/控制模块；

基于所接收的动作请求是否是所述动作请求的被签名的版本来确定所接收的动作请求的真实性；以及

基于所述确定执行与所接收的动作请求相关联的动作，其中，所述动作请求包括在所述动作发起单元处提供的至少一个操作员控制动作，并且其中，所述动作发起单元包括以下中的至少一个：操作员接口、工程接口、本地应用接口、以及远程应用接口。

14.根据权利要求13所述的通信/控制模块，进一步包括：

虚拟按键开关，其使得所述至少一个处理器能够在确定所接收的动作请求是所述动作请求的被签名的版本时，执行所接收的动作请求。

15.根据权利要求13所述的通信/控制模块，其中，所接收的动作请求是所述动作请求的加密的版本，并且所述指令组进一步包括用于解密所述动作请求的加密的版本的指令。

16.根据权利要求13所述的通信/控制模块，其中，用于在确定所述动作请求是所述动作请求的被签名的版本时执行所述动作请求的所述指令包括：

用于控制通信地耦合的工业元件的指令，所述通信地耦合的工业元件包括以下中的至少一个：通信/控制模块、输入/输出模块、电源模块、现场装置、交换机、工作站、以及物理互连装置。

17.一种在安全工业控制系统中执行被请求的动作的方法，包括：

在动作发起单元处接收动作请求；

传输来自所述动作发起单元的所述动作请求；

在物理地位于远离所述动作发起单元处的动作认证单元处接收来自所述动作发起单元的所述动作请求；

确定所述动作请求是否是在所述动作认证单元处的独立于所述动作发起单元的授权

的动作请求；

基于所述确定在所述动作认证单元处对所述动作请求进行签名，所述动作认证单元包括与其上存储有私钥的存储介质通信的至少一个处理器，所述至少一个处理器被配置为使用所述私钥基于所述确定来对所述动作请求进行签名，从而生成所述动作请求的被签名的版本；

在与一个或多个工业元件通信的通信/控制模块处接收所述动作请求，所述一个或多个工业元件包括至少一个输入/输出模块，其可操作用于接收工业传感器信息或将控制信息发送到工业驱动器或电机，所述通信/控制模块包括至少一个处理器和承载能够由所述至少一个处理器执行用于控制与所述一个或多个工业元件的通信的指令组的非瞬时性介质；

确定所述动作请求是否是在所述通信/控制模块处的所述动作请求的被签名的版本；

在所述通信/控制模块处基于所述确定来认证所述动作请求；以及

仅当所述动作请求被认证时，经由所述通信/控制模块执行所述动作请求，其中，所述动作请求包括操作员控制动作，包括：读取或改变控制设定点，控制一个或多个驱动器，以及执行来自操作员接口和工程接口的控制命令。

18.根据权利要求17所述的方法，其中，所述动作请求在传输到所述通信/控制模块之前被所述动作认证单元加密。

19.根据权利要求17所述的方法，其中，所述动作认证单元包括以下中的至少一个：便携式加密装置、安全的工作站、以及装置生命周期管理系统。

20.根据权利要求17所述的方法，其中，执行所述动作请求进一步包括：

根据所述动作请求来控制工业元件，所述工业元件包括以下中的至少一个：通信/控制模块、输入/输出模块、电源模块、现场装置、交换机、工作站、以及物理互连装置。

工业控制系统中的操作员动作认证

[0001] 相关申请的交叉引用

[0002] 本申请是于2013年8月6日递交的、题为“SECURE INDUSTRIAL CONTROL SYSTEM”的国际专利申请No.PCT/US2013/053721的部分延续。本申请在美国法典第120节第35款下还是于2014年8月27日递交的、题为“SECURE INDUSTRIAL CONTROL SYSTEM”的美国专利申请序列No.14/469,931的部分延续。本申请在美国法典第120节第35款下还是于2014年7月30日递交的、题为“INDUSTRIAL CONTROL SYSTEM CABLE”的美国专利申请序列No.14/446,412的部分延续，该专利申请在美国法典第119(e)节第35款下要求享有于2014年7月7日递交的、题为“INDUSTRIAL CONTROL SYSTEM CABLE”的美国临时专利申请序列No.62/021,438的优先权。美国临时专利申请序列No.62/021,438;美国专利申请序列No.14/446,412和14/469,931;以及国际专利申请No.PCT/US2013/053721以引用方式全部并入本文。

背景技术

[0003] 工业控制系统，例如标准工业控制系统(ICS)或可编程自动化控制器(PAC)，包括用于工业生产的各种类型的控制设备，例如监督控制和数据采集(SCADA)系统、分布式控制系统(DSC)、可编程逻辑控制器(PLC)、以及诸如IEC1508的安全标准认证的工业安全系统。这些系统用于以下行业，包括电、水和废水、石油和天然气生产和精炼、化学、食品、药品以及机器人。使用从各种类型的传感器采集到的信息来测量过程变量，来自工业控制系统的自动化和/或操作员驱使的监督命令可以被传输到各种驱动器装置，例如控制阀、液压驱动器、磁驱动器、电子开关、电机、电磁阀等。这些驱动器装置从传感器和传感器系统采集数据、打开和关闭阀门和断路器、调节阀门和电机、针对报警条件而监控工业过程等。

[0004] 在其它示例中，SCADA系统可以使用开环控制，其中处理地点可以在地理上相隔很远。这些系统使用远程终端单元(RTU)来向一个或多个控制中心发送监督数据。采用RTU的SCADA应用包括流体管道、配电和大型通信系统。DCS系统一般用于使用高带宽、低延迟数据网络的实时数据采集和连续控制，并且用于大型园区工业处理厂，例如石油和天然气、精炼、化学、药品、食品和饮品、水和废水、纸浆和造纸、公用电力、采矿和金属。PLC更典型地提供布尔和时序逻辑运算、和计时器、以及连续控制，并且经常用于独立的机械和机器人。此外，ICE和PAC系统可以用于针对建筑、机场、船舶、空间站等的设施过程(例如，用于监测和控制供热、通风、空调(HVAC)设备和能耗)。随着工业控制系统的演进，新的技术将这些各种类型的控制系统结合起来。例如，PAC可以包括SCADA、DCS、和PLC的各方面。

发明内容

[0005] 根据本公开的各个实施例，一种安全工业控制系统包括一个或多个通信/控制模块，其用于控制或驱动一个或多个工业元件(例如，输入/输出(I/O)模块、电源模块、现场装置、交换机、工作站、和/或物理互连装置)。可以经由从动作发起单元到通信/控制模块的认证路径来保护操作员动作和/或其它命令或请求。在实施中，工业控制系统要求动作认证单元对由动作发起单元所生成的动作请求进行签名。目的通信/控制模块被配置为接收被签

名的动作请求，验证被签名的动作请求的真实性，并且当被签名的动作请求的真实性被验证时，执行所请求的动作。通过这种方式，不处理恶意或其它未经授权的动作请求，并且因此保护系统以防止恶意软件、间谍软件、未经授权而改变控制参数、未经授权而访问数据等。

[0006] 在一些实施例中，通信/控制模块包括至少一个处理器和承载了可由所述处理器执行的指令组的非瞬时性介质。所述指令组至少包括用于执行以下步骤的指令：接收由动作发起单元所启动的并由动作认证单元签名的动作请求；验证被签名的动作请求的真实性；并且当被签名的动作请求的所述真实性被验证时，执行所请求的动作。

[0007] 此外，公开了一种认证所请求的动作的方法。所述方法包括：用动作认证单元对动作请求进行签名；将被签名的动作请求发送到通信/控制模块；验证被签名的动作请求的真实性；并且当被签名的动作请求的所述真实性被验证时，用通信/控制模块来执行所请求的动作。

[0008] 提供本发明内容的概要来以简化的形式介绍挑选出的概念，这些概念将在下文的具体实施方式中进一步描述。(本发明内容的概要既不是要识别所要求保护的主题的关键特征或本质特征，也不是要用于帮助确定所要求保护的主题的范围。)

附图说明

[0009] 参考附图描述了具体实施方式。在描述和图中的不同实例中使用相同的附图标记可以指示相似或相同的物品。

[0010] 图1为示出了根据本公开的示例实施例的工业控制系统的框图。

[0011] 图2为示出了根据本公开的示例实施例的用于工业控制系统的动作认证路径的框图。

[0012] 图3为进一步示出了根据本公开的示例实施例的动作认证路径的框图。

[0013] 图4为示出了根据本公开的示例实施例的认证动作请求的方法的流程图。

[0014] 图5为进一步示出了根据本公开的示例实施例的认证动作请求的方法的流程图。

具体实施方式

[0015] 概述

[0016] 在工业控制系统中，各种工业元件/子系统(例如，输入/输出(I/O)模块、电源模块、过程传感器和/或驱动器、交换机、工作站、和/或物理互连装置)被控制元件/子系统(例如，一个或多个通信/控制模块)来控制或驱动。控制元件/子系统根据程序和从动作发起单元接收到的动作请求(例如，可执行软件模块、控制命令、数据请求等)而运行，所述动作发起单元可以是例如(但不限于)：操作员接口(例如，SCADA或人机界面(HMI))、工程接口、本地应用、和/或远程应用。在存在多个动作发起单元的情况下，工业控制系统可能易受未经授权的数据访问和/或控制的侵害。此外，工业控制系统可能易受恶意软件、间谍软件、或能够以更新、应用程序映像、控制命令等的形式传输的其它破坏/恶意软件。仅认证操作员可能不足以保护系统以防止恶意行为者或甚至可能源自经由有效登陆或看似有效的(例如，非法侵入)应用或操作员/工程接口的无意间的未经授权请求/命令。

[0017] 本公开指向用于防止未经授权的动作请求在工业控制系统中被处理的工业控制

系统通信/控制模块、子系统和技术。在实施例中，经由从动作发起单元到通信/控制模块的认证路径来保护预先定义的操作的选集或所有的操作员动作和/或其它控制动作或请求。在实施中，工业控制系统要求动作认证单元对由动作发起单元所生成的动作请求进行签名。未签名的动作请求可以自动导致错误并且将不会由通信/控制模块来处理或执行。通信/控制模块被配置为接收被签名的动作请求，验证被签名的动作请求的真实性，并且当被签名的动作请求的真实性被验证时，执行所请求的动作。通过这种方式，不处理恶意或其它未经授权的动作请求，并且因此保护系统以防止恶意软件、间谍软件、未经授权而改变控制参数、未经授权而访问数据等。

[0018] 示例实施

[0019] 图1示出了根据本公开的示例实施例的工业控制系统100。在实施例中，工业控制系统100可以包括工业控制系统(ICS)、可编程自动化控制器(PAC)、监督控制和数据采集(SCADA)系统、分布式控制系统(DSC)、可编程逻辑控制器(PLC)、以及诸如IEC1508的安全标准认证的工业安全系统等。如图1中所示，工业控制系统100使用通信控制架构来实现分布式控制系统，该分布式控制系统包括由分布在整个系统中的一个或多个控制元件或子系统102来控制或驱动的一个或多个工业元件(例如，输入/输出模块、电源模块、现场装置、交换机、工作站、和/或物理互连装置)。例如，一个或多个I/O模块104可以连接到组成控制元件/子系统102的一个或多个通信/控制模块106。工业控制系统100被配置为向I/O模块104传输数据、或从I/O模块104传输数据。I/O模块104可以包括输入模块、输出模块、和/或输入和输出模块。例如，在过程中，输入模块可以用于从输入装置130(例如，传感器)接收信息，而输出模块可以用于向输出装置(例如，驱动器)传输指令。例如，I/O模块104可以连接到过程传感器以用于测量天然气厂、精炼厂等的管道中的压力，和/或可以连接到过程驱动器以用于控制阀门、二或多状态开关、发射器等。现场装置130直接或经由网络连接而与I/O模块104通信地耦合。这些装置130可以包括控制阀、液压驱动器、磁驱动器、电机、电磁阀、电子开关、发射器、输入传感器/接收器(例如，照度、辐射、气体、温度、电、磁、和/或声传感器)通信子总线等。

[0020] 在实施中，I/O模块104可以被使用，工业控制系统100在以下应用中采集数据，这些应用包括但不限于关键基础设施和/或工业过程，例如产品制造和加工、公用事业发电、石油、天然气、和化学精炼；药品、食品和饮品、纸浆和造纸、金属和采矿以及针对建筑、机场、船舶、空间站等的设施和大型园区工业过程(例如，用于监测和控制供热、通风、空调(HVAC)设备和能耗)。

[0021] 在实施中，I/O模块104可以被配置为将从传感器接收到的模拟数据转换为数字数据(例如，使用模数转换器(ADC)电路等)。I/O模块104还可以连接到诸如电机或调节阀或电气继电器和其他形式的驱动器这样的一个或多个过程驱动器，并且可以被配置为控制电机的一个或多个运行特性，例如电机转速、电机扭矩、或调节阀的位置或电气继电器的状态等。此外，I/O模块104可以被配置为将数字数据转换为模拟数据以用于传输到驱动器(例如，使用数模转换器(DAC)电路等)。在实施例中，I/O模块104中的一个或多个可以包括通信模块，其被配置为用于经由通信子总线进行通信，所述通信子总线可以是例如，以太网总线、H1现场总线、过程现场总线(PROFIBUS)、可寻址远程传感器高速通道(HART)总线、Modbus等。此外，可以使用两个或更多I/O模块104来提供针对现场装置130的容错和冗余连

接，所述现场装置130可以是例如，控制阀、磁驱动器、电机、电磁阀、电子开关、发射器、输入传感器/接收器(例如，照度、辐射、气体、温度、电、磁、和/或声传感器)通信子总线等。

[0022] 每个I/O模块104可以被提供有唯一的标识符(ID)以用于将一个I/O模块104与另一个I/O模块104区别开。在实施中，当I/O模块104连接到工业控制系统100时，该I/O模块104由其ID进行标识。多个I/O模块104由工业控制系统100使用以提供冗余。例如，两个或多个I/O模块104可以连接到过程传感器和/或驱动器。每个I/O模块104可以包括提供了到该I/O模块104所包含的硬件和电路(例如，印刷电路板(PCB))的物理连接的一个或多个端口。例如，每个I/O模块104包括用于电缆的连接，该电缆将其自身连接到I/O模块104中的印刷线路板(PWB)。

[0023] I/O模块104中的一个或多个可以包括用于连接到其它网络的接口，所述其它网络包括但不限于：广域蜂窝电话网络，例如3G蜂窝网络、4G蜂窝网络、全球移动通信系统(GSM)网络；无线计算机通信网络，例如Wi-Fi网络(例如，使用IEEE 802.11网络标准运行的无线LAN(WLAN))；个域网(PAN)(例如，使用IEEE 802.15网络标准运行的无线PAN(WPAN))；广域网(WAN)；内联网；外联网；互联网；因特网等。此外，I/O模块104中的一个或多个可以包括用于将I/O模块104连接到计算机总线等的连接。

[0024] 通信/控制模块106可以用于监测和控制I/O模块104，并且可以用于将两个I/O模块104连接起来。在本公开的实施例中，当I/O模块104基于针对I/O模块104的唯一ID而连接到工业控制系统100时，通信/控制模块106可以更新路由表。此外，当使用了多个冗余的I/O模块104时，每个通信/控制模块106可以实现对关于I/O模块104的信息数据库的镜像，并且在从I/O模块104接收到数据和/或将数据传输到I/O模块104时更新这些镜像。在一些实施例中，使用两个或更多通信/控制模块106以提供冗余。对于增加的安全性，通信/控制模块106可以被配置为执行认证序列或握手以在预先定义的事件或时间互相认证，所述预先定义的事件或时间可以是例如，新控制模块的启动、重置、安装，通信/控制模块106的周期性替换，排定的时间等。

[0025] 如图2和图3中所示，通信/控制模块106或任何其它工业元件/控制器206(例如，I/O模块104、现场装置130，例如驱动器或传感器、网络互连装置、交换机、电源模块112等)可以至少部分地基于来自动作发起单元202的请求/命令而运行。在实施中，动作发起单元202包括操作员接口208(例如，SCADA或HMI)、包括编辑器212和编译器214的工程接口210、本地应用220、远程应用216(例如，经由本地应用220通过网络218进行通信)等。在图2和图3中所示的认证路径200中，工业元件/控制器206(例如，通信/控制模块106、I/O模块104、诸如驱动器或传感器、网络互连装置、交换机、电源模块112的现场装置130等)仅在由动作认证单元204已对动作请求(例如，请求数据、控制命令、固件/软件更新、设定点控制、应用程序映像下载等)进行签名和/或已对动作请求加密时处理该动作请求。这防止来自有效用户简档的未经授权的动作请求并且进一步保护系统以防止来自无效(例如，非法侵入)简档的未经授权的动作请求。

[0026] 动作认证单元204可以与动作发起单元202同在一处(例如，之间连接的装置生命周期管理系统(“DLM”)222或安全工作站226)或位于远程(例如，经由网络218连接的DLM 222)。一般来说，动作认证单元204包括具有存储于其上的私钥的存储介质以及被配置为用该私钥来对由动作发起单元202所生成的动作请求进行签名和/或加密的处理器。该私钥被

存储在不能通过标准操作员登陆而访问的存储器中。例如，安全工作站226可以要求物理密钥、便携式加密装置(例如，智能卡、RFID标签等)、和/或用于访问的生物计量输入。

[0027] 在一些实施例中，动作认证单元204包括诸如智能卡224的便携式加密装置(其包括安全微处理器)。使用便携式加密装置的优势在于具有对动作发起单元202的接口的授权访问的操作员或用户可以携带整个装置(包括私密地存储的密钥和与其通信的处理器)。无论动作认证节点204经由安全还是不安全工作站来访问认证路径200，来自动作发起单元202的动作请求可以在便携式加密装置的架构(而非可能不太安全的工作站或基于云的架构)内被安全地签名和/或加密。这保护了工业控制系统100以防止未经授权的动作。例如，在智能卡224能够认证经由动作发起单元202所发出的任何动作请求之前，未经授权的个人将不得不物理地拥有智能卡224。

[0028] 此外，可以采用多层的安全性。例如，动作认证单元204可以包括只可经由智能卡访问等来访问以签名和/或加密动作请求的安全工作站226。另外，安全工作站226可以经由生物计量或多因素密码装置228来访问(例如，指纹扫描器、虹膜扫描器、和/或面部识别装置)。在一些实施例中，在使能智能卡224或其它便携式加密装置来对动作请求进行签名之前，多因素密码装置228要求有效的生物计量输入。

[0029] 通信/控制模块106或由动作发起单元202驱动的其它工业元件/控制器206被配置为接收被签名的动作请求，验证被签名的动作请求的真实性，并且当被签名的动作请求的真实性被验证时，执行所请求的动作。在一些实施例中，工业元件/控制器206包括被配置为存储动作请求(例如，应用程序映像、控制命令、和/或由动作发起单元发送的任何其它数据)的存储介质230(例如，SD/微型SD卡、HDD、SDD、或任何其它非瞬时性存储装置)。通信/控制模块106或任何其它工业元件/控制器206进一步包括在验证签名后进行/执行动作请求(即，执行所请求的动作)的处理器232。在一些实施例中，由动作发起单元202和/或动作认证单元232来加密动作请求，并且在能够执行所请求的动作之前，必须由处理器232进行解密。在实施中，通信/控制模块106或其它工业元件/控制器206包括虚拟按键开关234(例如，运行在处理器232上的软件模块)，该虚拟按键开关234使得处理器121能够仅在验证了动作请求签名之后和/或解密动作请求之后执行来执行所请求的动作。在一些实施例中，在能够在通信/控制模块106或任何其它工业元件/控制器206上运行之前，每个动作或关键动作的选集中的每个必须清空认证路径。

[0030] 图4和图5示出了根据本公开的示例性实施例的认证动作请求的方法300。在实施中，可以由工业控制系统100和/或工业控制系统100的认证路径200来体现方法300。方法300包括：(302)发起动作请求(例如，经由操作员/工程接口208、210或远程/本地应用即216、220)；(304)用动作认证单元204对动作请求进行签名；(312)可选地用动作认证单元204加密动作请求；(306)将被签名的动作请求发送或下载到通信/控制模块106或任何其它工业元件/控制器206；(308)验证被签名的动作请求的真实性；(314)可选地用通信/控制模块106或任何其它工业元件/控制器206解密动作请求；以及(310)当被签名的动作请求的真实性被验证时，用通信/控制模块106或任何其它工业元件/控制器206来执行所请求的动作。

[0031] 对于增强的安全性，通信/控制模块106或任何其它工业元件/控制器206可以进一步被配置为在由通信/控制模块106或任何其它工业元件/控制器206运行所请求的动作之

前，用动作认证单元204(例如，智能卡224等)来执行认证序列。例如，可以在步骤310甚至在步骤306之前执行所谓的“握手”。在一些实施例中，可以用更复杂的认证序列来替换签名和验证步骤304和308。或者，认证序列可以被执行为额外的安全措施以扩充较简单的签名验证和/或解密措施。

[0032] 在一些实施例中，由通信/控制模块106或任何其它工业元件/控制器206实现的认证序列可以包括：向动作认证单元204发送请求数据报，该请求数据报包括第一随机数、第一装置认证密钥证书(例如，包含装置认证密钥的第一认证证书)、以及第一身份属性证书；从动作认证单元204接收响应数据报，该响应数据报包括第二随机数、与第一随机数和第二随机数相关联的第一签名、第二装置认证密钥证书(例如，包含装置认证密钥的第二认证证书)、以及第二身份属性证书；通过验证与第一随机数和第二随机数相关联的第一签名、第二装置认证密钥证书、以及第二身份属性证书来证实该响应数据报；并且当该响应数据报有效时，向动作认证单元204发送认证数据报，该认证数据报包括与第一随机数和第二随机数相关联的第二签名。

[0033] 替代地，动作认证单元204可以启动握手，在这种情况下，由通信/控制模块106或任何其它工业元件/控制器206实现的认证序列可以包括：从动作认证单元204接收请求数据报，该请求数据报包括第一随机数、第一装置认证密钥证书、以及第一身份属性证书；通过验证第一装置认证密钥证书和第一身份属性证书来证实该请求数据报；当该请求数据报有效时，向动作认证单元204发送响应数据报，该响应数据报包括第二随机数、与第一随机数和第二随机数相关联的第一签名、第二装置认证密钥证书、以及第二身份属性证书；从动作认证单元204接收认证数据报，该认证数据报包括与第一随机数和第二随机数相关联的第二签名；并且通过验证与第一随机数和第二随机数相关联的第二签名来证实该认证数据报。

[0034] 在于2014年10月20日递交的、题为“INDSUTRIAL CONTROL SYSTEM REDEUNDANT COMMUNICATIONS/CONTROL MODULES AUTHENTICATION”的、发明人为Timothy Clish等的共同未决美国临时专利申请序列No.(还未分配)中进一步描述了可由通信/控制模块106或任何其它工业元件/控制器206以及动作认证单元204实现的握手或认证序列，该专利申请以引用方式全部并入本文。本领域技术人员将理解冗余通信/控制模块106之间的握手对本文中所描述的通信/控制模块106或任何其它工业元件/控制器206与动作认证单元204之间的握手的适用性。

[0035] 动作发起单元202、动作认证单元204、以及通信/控制模块106或任何其它工业元件/控制器206中的每个可以包括被使能以执行本文中所描述的功能或操作(例如，方法300的块和认证序列)的电路和/或逻辑。例如，动作发起单元202、动作认证单元204、以及通信/控制模块106或任何其它工业元件/控制器206中的每个可以包括执行程序指令的一个或多个处理器，该程序指令由非瞬时性机器可读介质永久地、半永久地、或临时地存储，该非瞬时性机器可读介质可以包括但不限于：硬盘驱动器(HDD)、固态盘(SDD)、光学盘、磁存储装置、闪速驱动器、或SD/微型SD卡。

[0036] 再次参考图1，由工业控制系统100所传输的数据可以被分组，即数据的离散部分可以被转换为数据分组，该数据分组包括数据部分以及网络控制信息等。工业控制系统100可以使用用于数据传输的一个或多个协议，包括诸如高级数据链路控制(HDLC)这样的面向

比特的同步数据链路层协议。在一些实施例中，工业控制系统100根据国际标准化组织(ISO)13239标准等来实现HDLC。此外，两个或更多通信/控制模块106可以用于实现冗余HDLC。然而，应当注意HDLC仅通过示例的方式提供，并且并不意味着对本公开的限制。因此，根据本公开的工业控制系统100可以使用其它各种通信协议。

[0037] 通信/控制模块106中的一个或多个可以被配置为用于与用于监测和/或控制现场装置130(例如，传感器和/或驱动仪器)的组件交换信息，该现场装置130经由I/O模块104(例如，一个或多个控制回路反馈机制/控制器)而连接到工业控制系统100。在实施中，控制器可以被配置为微控制器/可编程逻辑控制器(PLC)、比例-积分-微分(PID)控制器等。在一些实施例中，I/O模块104和通信/控制模块106包括网络接口，例如用于经由网络将一个或多个I/O模块104连接到一个或多个控制器。在实施中，网络接口可以被配置为用于将I/O模块104连接到局域网(LAN)的千兆以太网接口。此外，两个或更多通信/控制模块106可以用于实现冗余的千兆以太网。然而，应当注意千兆以太网仅通过示例的方式提供，并且并不意味着对本公开的限制。因此，网络接口可以被配置为用于将通信/控制模块106连接到其它各种网络，其包括但不限于：广域蜂窝电话网络，例如3G蜂窝网络、4G蜂窝网络、GSM网络；无线计算机通信网络，例如Wi-Fi网络(例如，使用IEEE 802.11网络标准运行的WLAN)；PAN(例如，使用IEEE 802.15网络标准运行的WPAN)；WAN；内联网；外联网；互联网；因特网等。另外，可以使用计算机总线来实现网络接口。例如，网络接口可以包括外设部件互连(PCI)卡接口，例如Mini PCI接口等。此外，网络可以被配置为包括单个网络或跨不同接入点的多个网络。

[0038] 工业控制系统100可以从多个源接收电力。例如，从电网108提供交流电力(例如，使用来自交流电源的高压电源)。还可以使用本地发电来提供交流电力(例如，现场涡轮或柴油本地发电机)。电源112用于将来自电网108的电力分配到工业控制系统100的自动化设备，例如控制器、I/O模块等。电源112还可以用于将来自本地发电机110的电力分配到工业控制系统设备。工业控制系统100还可以包括额外的(候补)电源，其被配置为使用多个电池模块来存储并返回直流电力。例如，电源112作为不断电系统(UPS)。在本公开的实施例中，多个电源112可以分布(例如，物理地分散)在工业控制系统100内。

[0039] 在一些实施例中，控制元件/子系统和/或工业元件(例如，I/O模块104、通信/控制模块106、电源112等)由一个或多个背板114连接在一起。例如，可以由通信背板116将通信/控制模块106连接到I/O模块104。此外，可以由电力背板118将电源112连接到I/O模块104和/或通信/控制模块106。在一些实施例中，物理互联装置(例如，开关、连接器、或电缆，例如但不限于美国临时专利申请序列No.14/446,412中所描述的那些)用于连接到I/O模块104、通信/控制模块106、电源112、以及可能其它的工业控制系统设备。例如，电缆可以用于将通信/控制模块106连接到网络120，另一个电缆可以用于将电源112连接到电网108，另一个电缆可以用于将电源112连接到本地发电机110等。

[0040] 在一些实施例中，工业控制系统100实现安全控制系统。例如，工业控制系统100包括安全凭证源(例如，工厂122)和安全凭证实现单元(例如，密钥管理实体124)。安全凭证源被配置为生成唯一的安全凭证(例如，密钥、证书等，例如唯一的标识符、和/或安全凭证)。安全凭证实现单元被配置为向控制元件/子系统和/或工业元件(例如，电缆、装置130、I/O模块104、通信/控制模块106、电源112等)提供由安全凭证源生成的唯一的安全凭证。

[0041] 工业控制系统100的多个(例如,每个)装置130、/O模块104、通信/控制模块106、物理互连装置等可以被提供有安全凭证以用于在工业控制系统100的多个(例如,所有)层级处提供安全性。更进一步地,包括传感器和/或驱动器等的控制元件/子系统和/或工业元件可以在制造(例如,产生)期间被提供有唯一的安全凭证(例如,密钥、证书等),并且可以从产生开始由工业控制系统100的密钥管理实体124来管理以用于提升工业控制系统100的安全性。

[0042] 在一些实施例中,工业控制系统100的包括传感器和/或驱动器等的控制元件/子系统和/或工业元件之间的通信包括认证过程。可以执行认证过程以用于对工业控制系统100中所实现的包括传感器和/或驱动器等的控制元件/子系统和/或工业元件进行认证。此外,认证过程可以利用与元件和/或物理互连装置相关联的安全凭证以用于对该元件和/或物理互连装置进行认证。例如,安全凭证可以包括加密密钥、证书(例如,公钥证书、数字证书、身份证书、安全证书、不对称证书、标准证书、非标准证书)和/或标识号。

[0043] 在实现中,工业控制系统100的多个控制元件/子系统和/或工业元件可以被提供有它们自身唯一的安全凭证。例如,在制造工业控制系统100的元件时,每个元件可以被提供有其自身唯一的证书集合、加密密钥集合和/或标识号集合(例如,在产生该元件时定义了密钥和证书的各个集合)。证书、加密密钥和/或标识号的集合可以被配置为用于提供/支持强加密。可以用标准(例如,商用现货(COTS))加密算法(例如,美国国家安全局(NSA)算法、美国国家标准技术研究所(NIST)算法等)来实现加密密钥。

[0044] 基于认证过程的结果,被认证的元件可以被激活、可以在工业控制系统100内启用或禁用该元件的部分功能、可以在工业控制系统100内启用该元件的完整功能、和/或可以在工业控制系统100内完全禁用该元件的功能(例如,不促成该元件与工业控制系统100的其它元件之间的通信)。

[0045] 在实施例中,与工业控制系统100的元件相关联的密钥、证书和/或标识号可以指明该元件的原始设备制造商(OEM)。如在本文中所使用的,术语“原始设备制造商”或“OEM”可以被定义为物理地制造该装置(例如,元件)的实体和/或该装置的供应商(例如,从物理制造商处购买并销售该装置的实体)。因此,在实施例中,可以由既是物理制造商也是装置供应商的OEM来制造和分销(销售)该装置。然而,在其它实施例中,可以由作为供应商(而不是物理制造商)的OEM来分销装置。在这样的实施例中,OEM可以使得该设备由物理制造商来制造(例如,OEM可以从物理制造商处购买、订约、订购等该装置)。

[0046] 另外,在OEM包含供应商(该供应商不是装置的物理制造商)的情况下,装置可以承载供应商的品牌而不是物理制造商的品牌。例如,在元件(例如,通信/控制模块106)与特定OEM(其是供应商而不是物理制造商)相关联的实施例中,元件的密钥、证书和/或标识号可以指明该来源。在认证工业控制系统100的元件期间,当确定了被认证的元件是由不同于工业控制系统100中的一个或多个其它元件的OEM的实体所制造或供应的时,则可以在工业控制系统100内至少部分地禁用该元件的功能。例如,可以在该元件和工业控制系统100的其它元件之间的通信(例如,数据传送)上施加限制,从而使得工业控制系统100内的元件不能工作/起作用。当工业控制系统100的元件中的一个需要替换时,该特征可以防止工业控制系统100的用户不知情地用非同类元件(例如,具有与工业控制系统100的其余元件不同的来源(不同的OEM)的元件)来替换所述元件,并且在工业控制系统100中实现该非同类元件。

以这种方式，本文中所描述的几乎可以防止将其它OEM的元件替入到安全的工业控制系统100。在一个示例中，可以防止这样的替代：用提供类似功能的元件来代替由原始OEM所提供的元件，这是因为用于替代的元件不能在原始OEM的系统中认证并运行。在另一个示例中，第一经销商可以被提供有具有原始OEM的第一组物理和密码标签的元件，并且该第一经销商的元件可以安装在工业控制系统100中。在该示例中，第二经销商可以被提供有具有同一原始OEM的第二(例如，不同)组物理和密码标签的元件。在该示例中，可以防止该第二经销商的元件在工业控制系统100中运行，这是因为它们不能进行认证并且不能与第一经销商的元件一起运行。然而，应当注意第一经销商和第二经销商可以进入双方协议，其中第一元件和第二元件可以被配置为在工业控制系统100内进行认证和运行。此外，在一些实施例中，还可以实现经销商之间的用于允许互操作的协议，使得该协议仅适用于特定的顾客、一组顾客、设施等。

[0047] 在另一个实例中，用户可以尝试在工业控制系统100中实现被错误地指定的(例如，被误标注的)元件。例如，误标注的元件可以具有标注于其上的物理标记，该物理标记错误地指示出该元件与工业控制系统100中的其它元件的OEM相同的OEM相关联。在这样的实例中，由工业控制系统100所实现的认证过程可以使得用户被警告该元件是伪造的。该过程还可以提高针对工业控制系统100的改进的安全性，这是因为伪造的元件经常是恶意软件通过其而被引入到工业控制系统100中的载体。在实施例中，认证过程为工业控制系统100提供安全的空气间隔，以确保该安全控制系统与不安全网络物理地隔离。

[0048] 在实施中，安全工业控制系统100包括密钥管理实体124。密钥管理实体124可以被配置为用于管理密码系统中的密码密钥(例如，加密密钥)。该对密码密钥的管理(例如，密钥管理)可以包括生成、交换、存储、使用和/或替换密钥。例如，密钥管理实体124被配置为作为安全凭证源，以为工业控制系统100的元件生成唯一的安全凭证(例如，公开安全凭证、秘密安全凭证)。密钥管理关于用户和/或系统层级处(例如，在用户之间或系统之间)的密钥。

[0049] 在实施例中，密钥管理实体124包括安全实体，例如位于安全实施中的实体。密钥管理实体124可以位于远离I/O模块104、通信/控制模块106、和网络120处。例如，防火墙126可以将密钥管理实体124与控制元件或子系统102和网络120(例如，企业网)分离。在实施中，防火墙126可以是基于软件和/或硬件的网络安全系统，该网络安全系统通过分析数据分组并确定是否应当允许数据分组通过而基于规则集来控制输入和输出的网络流量。因此，防火墙126在可信、安全内部网络(例如，网络120)与另一个不被认为安全和可信的网络128(例如，云和/或因特网)之间建立屏障。在实施例中，防火墙126允许密钥管理实体124与控制元件或子系统102和/或网络120中的一个或多个之间的有选择的(例如，安全的)通信。在示例中，可以在工业控制系统100中的各个位置实现一个或多个防火墙。例如，防火墙可以被集成在网络120的交换机和/或工作站中。

[0050] 安全工业控制系统100可以进一步包括一个或多个制造实体(例如，工厂122)。制造实体可以与工业控制系统100的元件的原始设备制造商(OEM)相关联。密钥管理实体124可以经由网络(例如，云)与制造实体通信地耦合。在实施中，当工业控制系统100的元件在一个或多个制造实体处被制造时，密钥管理实体124可以与该元件通信地耦合(例如，可以具有到该元件的加密的通信管道)。密钥管理实体124可以利用该通信管道以在制造时为该

元件提供安全凭证(例如,将密钥、证书和/或标识号插入到元件中)。

[0051] 此外,当将元件投入使用(例如,激活)时,密钥管理实体124可以被通信地耦合(例如,经由加密的通信管道)到全世界的每个元件并且可以确认并签名具体代码的使用、撤销(例如,移除)任意特定代码的使用、和/或使能任意特定代码的使用。因此,密钥管理实体124可以在元件起初被制造(例如,产生)的工厂处与每个元件通信,从而使得该元件生来便具有管理的密钥。包括工业控制系统100的每个元件的所有加密密钥、证书和/或标识号的主数据库和/或表可以由密钥管理实体124来维持。密钥管理实体124(通过其与元件的通信)被配置为用于撤销密钥,从而提升认证机制反盗窃和反组件的重新使用的能力。

[0052] 在实施中,密钥管理实体124可以经由另一个网络(例如,云和/或因特网)和防火墙与控制元件/子系统、工业元件、和/或网络120通信地耦合。例如,在实施例中,密钥管理实体124可以是集中式系统或分布式系统。另外,在实施中,可以在本地或远程地管理密钥管理实体124。在一些实施中,密钥管理实体124可以位于(例如,集成到)网络120和/或网络元件或子系统102中。密钥管理实体124可以以多种方式提供管理和/或以多种方式被管理。例如,可以由中央位置处的顾客、由个体工厂位置处的顾客、由外部的第三方管理公司和/或由工业控制系统100的不同层(并且根据该层,在不同位置)处的顾客来实现/管理密钥管理实体124。

[0053] 可以由认证过程来提供变化的安全性级别(例如,可放缩的、用户配置的安全性的量)。例如,可以提供安全性的基础级别,其认证元件并保护元件内的代码。也可以添加其它的安全性的层级。例如,安全性可以被实现到这样的程度:使得诸如通信/控制模块106的组件在没有发生合适的认证的情况下不能通电。在实施中,在元件中实现在代码中加密,而在元件上实现安全凭证(例如,密钥和证书)。安全性可以通过工业控制系统100分布(例如,流动(flow))。例如,安全性可以通过工业控制系统一路流向最终用户,最终用户知道什么模块被指定以在该实例中进行控制。在实现中,认证过程提供对装置的加密、标识以用于系统硬件或软件组件的安全通信和认证(例如,提供数字签名)。

[0054] 在实施中,可以实现认证过程以支持和/或使能安全工业控制系统100中的由不同制造商/零售商/供应商(例如,OEM)所制造和/或供应的元件的互操作性。例如,可以启用由不同制造商/零售商/供应商所制造和/或供应的元件之间的有选择的(例如,一些)互操作性。在实施例中,在认证期间所实现的唯一的安全凭证(例如,密钥)可以形成分级结构,从而允许由工业控制系统100的不同元件执行不同功能。

[0055] 连接工业控制系统100的组件的通信链路可以进一步采用置于(例如,注入和/或填入)其中的数据分组(例如,短分组(例如,小于六十四(64)字节的分组)),以提供增加的安全性级别。短分组的使用增加了外部信息(例如,诸如虚假消息、恶意软件(病毒)、数据挖掘应用程序等这样的恶意内容)能够被注入到通信链路上的难度。例如,可以在动作发起单元204与通信/控制模块106或任何其它工业元件/控制器206之间传输的数据分组之间的间隙中将短分组注入到通信链路上,以阻碍外部实体将恶意内容注入到通信链路上的能力。

[0056] 总体上,可以使用硬件(例如,诸如集成电路的固定逻辑电路)、软件、固件、手动处理、或其组合来实现本文中所描述的任何功能。因此,本公开以上内容中所讨论的块总体上表示硬件(例如,诸如集成电路的固定逻辑电路)、软件、固件、或其组合。在硬件配置的实例中,本公开以上内容中所讨论的各个块可以被实现为其它集成电路以及其它功能性。这样

的集成电路可以包括给定的块、系统、或电路的所有功能，或包括块、系统、或电路对的一部分功能。此外，可以跨多个集成电路来实现块、系统、或电路的元件。这样的集成电路可以包括但不一定限于以下各种集成电路，包括：单片集成电路、倒装芯片集成电路、多芯片模块集成电路、和/或混合信号集成电路。在软件实施的实例中，本公开以上内容中所讨论的各个块表示可执行指令(例如，程序代码)，当在处理器上执行这些可执行指令时，执行特定的任务。这些可执行指令可以存储在一个或多个有形计算机可读介质中。在一些这样的实例中，可以使用系统、块、或电路的软件或固件等同物来实现整个系统、块、或电路。在其它实例中，可以在软件或固件中实现给定的系统、块、或电路的一部分，而在硬件中实现其它部分。

[0057] 尽管以针对结构性特征和/或处理操作的语言描述了主题，但是应当理解在所附权利要求中所定义的主题并不一定限于上文所述的具体特征或行为。相反，上文所述的具体特征或行为被公开为实现权利要求的示例形式。

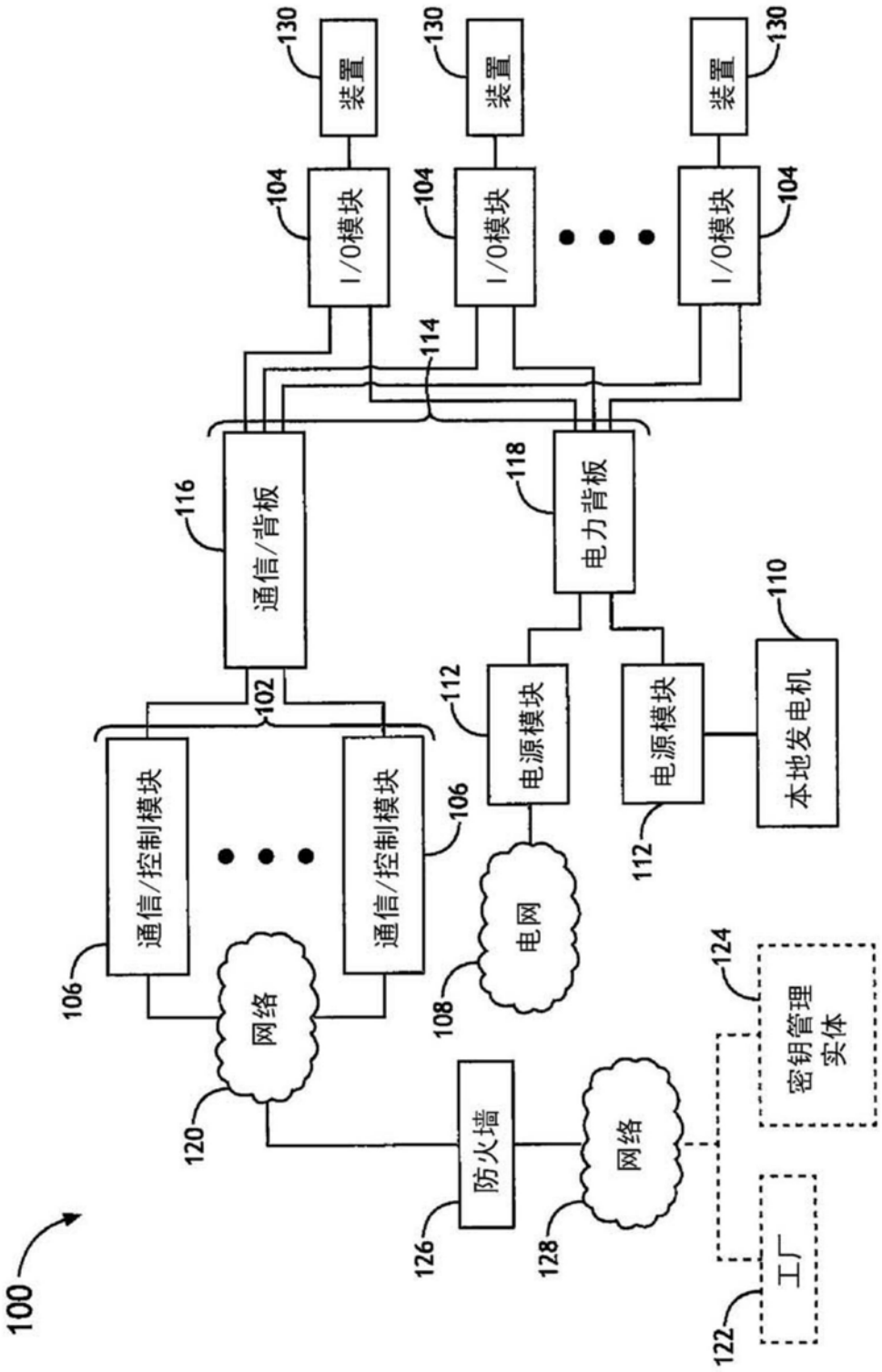

100
106
通信/控制模块
网络
120
102
通信/控制模块
106
116
通信/背板
114
104
I/O模块
130
装置
104
I/O模块
130
装置
104
I/O模块
130
装置
118
电力背板
112
电源模块
108
电网
112
电源模块
110
本地发电机
124
密钥管理实体
122
工厂
126
防火墙
128
网络

图1

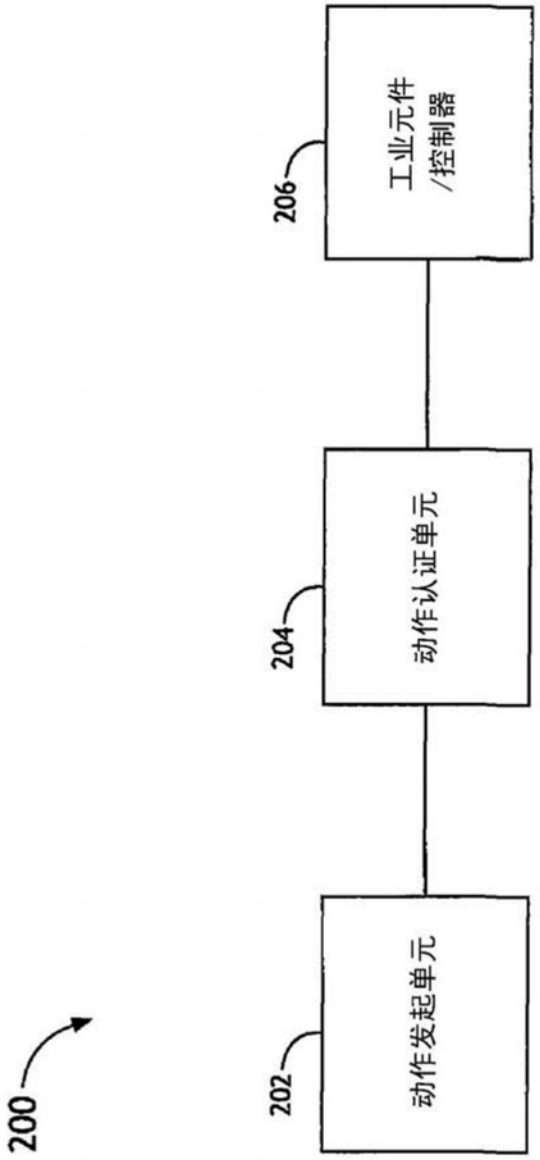


图2

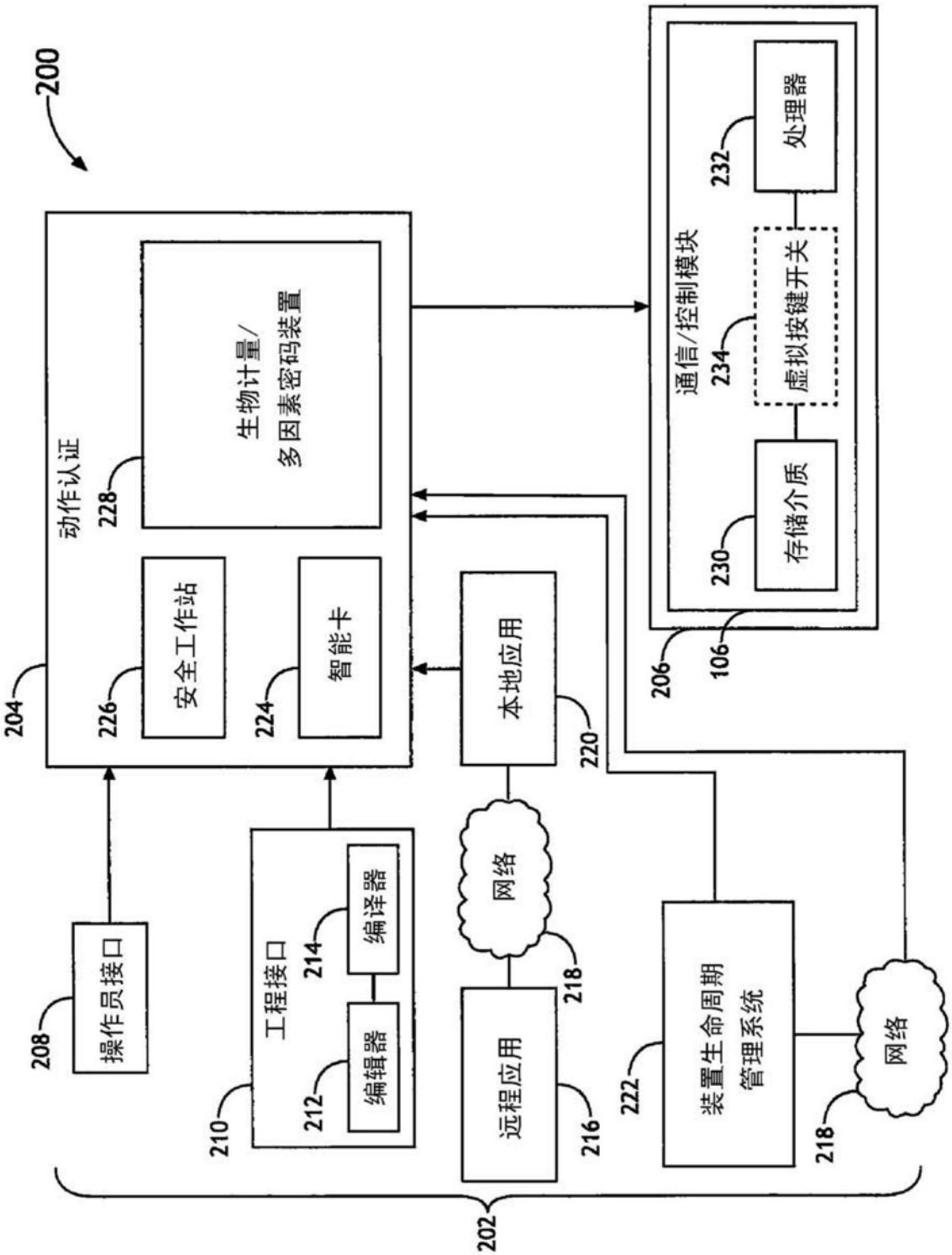

200
动作认证
204
生物计量/
多因素密码装置
228
安全工作站
226
智能卡
224
操作员接口
208
工程接口
210
编译器
214
编辑器
212
网络
218
本地应用
220
远程应用
216
装置生命周期
管理系统
222
网络
218
通信/控制模块
206
处理器
232
虚拟按键开关
234
存储介质
230
106
202

图3

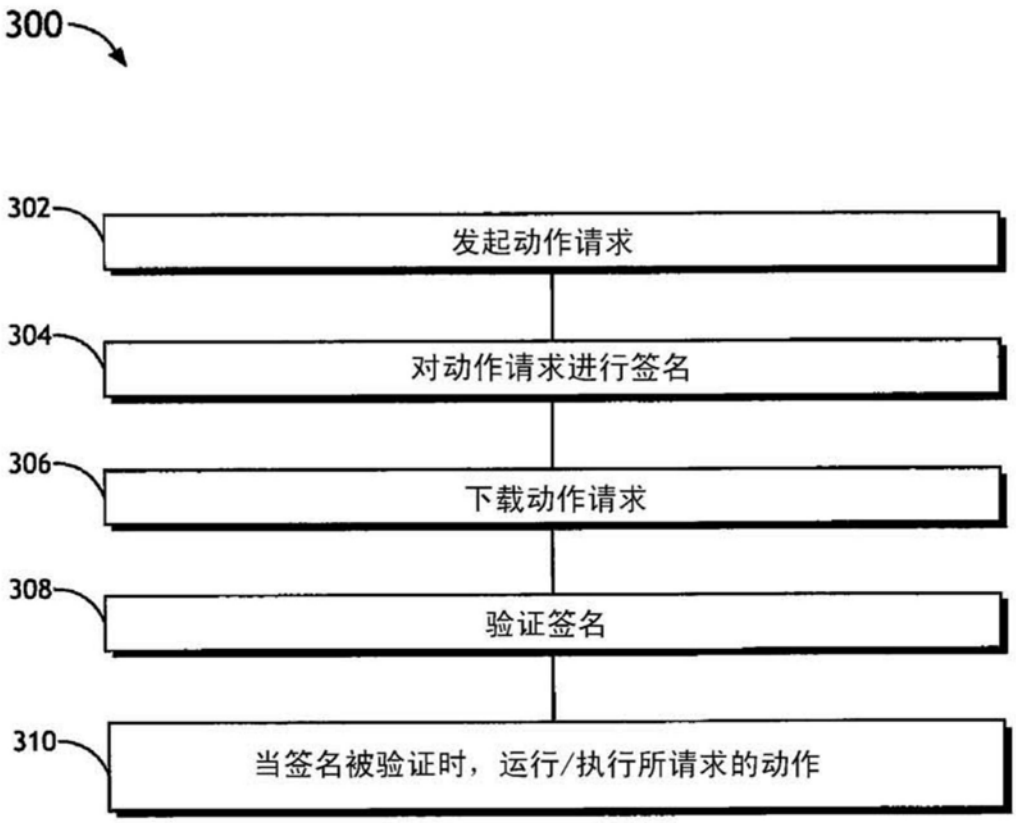

300
302
发起动作请求
304
对动作请求进行签名
306
下载动作请求
308
验证签名
310
当签名被验证时，运行/执行所请求的动作

图4

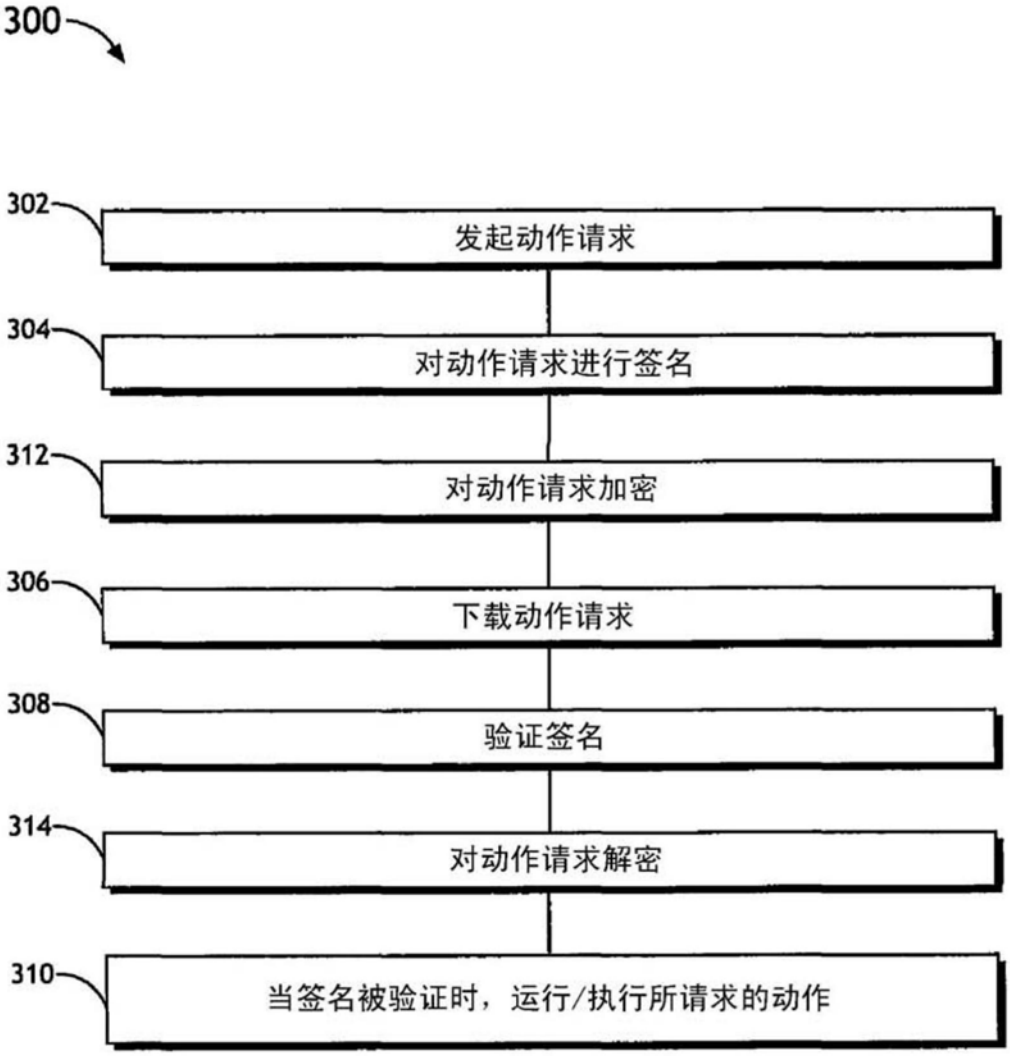

300
302
发起动作请求
304
对动作请求进行签名
312
对动作请求加密
306
下载动作请求
308
验证签名
314
对动作请求解密
310
当签名被验证时，运行/执行所请求的动作

图5