(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 105373091 B
(45)授权公告日 2019.06.04

(21)申请号 201510490839.2

(22)申请日 2015.08.11

(65)同一申请的已公布的文献号
申请公布号 CN 105373091 A

(43)申请公布日 2016.03.02

(30)优先权数据
14/456,763 2014.08.11 US

(73)专利权人 费希尔-罗斯蒙特系统公司
地址 美国德克萨斯州

(72)发明人 M·J·尼克松 K·J·贝奥特尔
D·D·克里斯滕森 D·陈
J·H·莫尔

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

(51)Int.Cl.
G05B 19/418(2006.01)

(56)对比文件
CN 101047507 A,2007.10.03,
CN 102857363 A,2013.01.02,
US 2005213768 A1,2005.09.29,
US 2009070589 A1,2009.03.12,
CN 101398685 A,2009.04.01,
US 2013290706 A1,2013.10.31,

审查员 傅磊

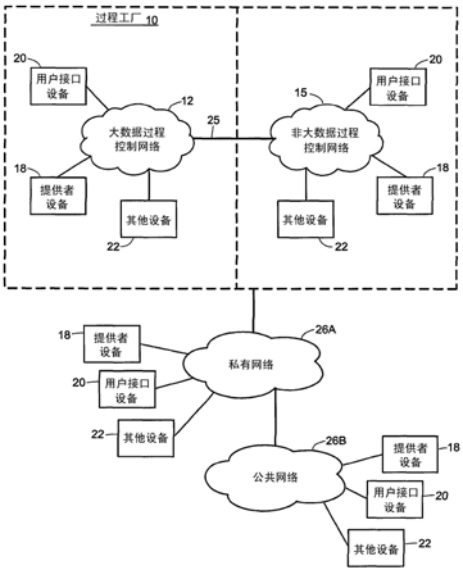
权利要求书2页 说明书32页 附图8页

(54)发明名称

用于在过程控制系统中使用的方法和装置

(57)摘要

用于确认用于在过程工厂中或与过程工厂一起使用的设备安全的技术包括为所述设备配备至少部分根据指示在允许所述设备访问所述过程工厂的网络之前必须满足的必需的条件和/或属性的数据生成的密钥。在初始化后,所述设备基于所述密钥来确定是否满足所述必需的条件,并且所述设备因此使其自身隔离或访问所述过程控制网络。密钥和其中指示的所述必需的条件/属性可以基于例如位置、时间、背景、客户、供应商、特定工厂、制造商、用户、数据类型、设备类型和/或其他标准。额外地,可以根据另一组必需的条件/属性来生成与密钥相关联的子密钥。子密钥可以由与密钥提供者实体不同的实体提供。



CN 105373091 B

1.一种用于在过程控制工厂中使用的过程控制设备,所述过程控制设备包括:

处理器;

非易失性存储器,其存储指示允许所述过程控制设备使用所述过程控制工厂的网络与另一设备进行通信所需要的一组必需的属性的数据,所述一组必需的属性描述允许所述过程控制设备与所述另一设备进行通信的环境;以及

计算机可执行指令,其存储在所述过程控制设备的所述非易失性存储器上或另一存储器上,所述计算机可执行指令在启动所述过程控制设备之后并且在所述过程控制设备与任何其他设备进行通信之前能够由所述处理器执行以进行以下中的至少一项:(i)对所述过程控制设备进行配置,或者(ii)对用于控制所述过程控制工厂中的过程的数据进行发送或接收中的至少一项,

其中,所述计算机可执行指令当由所述处理器执行时,使得所述过程控制设备:

确定所述过程控制设备在所述启动之后所处的当前环境的一组当前属性;

基于指示所述一组必需的属性的所述数据来确定所述过程控制设备所处的所述当前环境的所述一组当前属性是否遵从所述一组必需的属性;

当所述一组当前属性遵从所述一组必需的属性时,允许所述过程控制设备与所述另一设备进行通信以进行以下中的至少一项:(i)对所述过程控制设备进行配置,或者(ii)发送或接收实时数据以使得所述过程被控制中的至少一项;并且

当所述一组当前属性不遵从所述一组必需的属性时,阻止所述过程控制设备与所述另一设备进行通信以进行以下中的至少一项:(i)对所述过程控制设备进行配置,或者(ii)对所述实时数据进行发送或接收来使得所述过程被控制中的至少一项。

2.根据权利要求1所述的过程控制设备,还包括地理空间接收机,并且其中:

所述计算机可执行指令还能够由所述处理器执行以使得所述过程控制设备使用所述地理空间接收机来确定过程控制设备的当前地理空间位置,并且

对应于所述过程控制设备所处的环境的所述一组必需的属性包括特定地理空间区域。

3.根据权利要求2所述的过程控制设备,其中:

所述计算机可执行指令还能够执行以使得所述过程控制设备确定当前时间,并且

对应于所述过程控制设备所处的所述环境的所述一组必需的属性还包括对应于所述特定地理空间区域的特定时间间隔。

4.根据权利要求1所述的过程控制设备,其中,所述非易失性存储器被配备有用于在将所述过程控制设备与所述过程控制工厂的所述网络进行认证中使用的密钥,所述密钥基于种子来生成,所述种子包括密钥生成数据和随机生成的或伪随机生成的数字,并且所述密钥生成数据指示允许所述过程控制设备使用所述过程控制工厂的所述网络与所述另一设备进行通信所需要的所述一组必需的属性。

5.根据权利要求4所述的过程控制设备,其中:

被配备到所述过程控制设备的所述非易失性存储器中的所述密钥是已加密密钥,

通过对未加密密钥进行加密来生成所述已加密密钥,并且

所述种子用于生成所述未加密密钥。

6.根据权利要求4所述的过程控制设备,还包括额外的计算机可执行指令,所述额外的计算机可执行指令当由所述处理器执行时使得在已经确定所述一组当前属性遵从所述一

组必需的属性之后并且在所述过程控制设备与所述另一设备进行通信以进行以下中的至少一项之前，所述过程控制设备使用被配备到所述非易失性存储器中的所述密钥与所述另一设备或与证书授权机构进行认证：(i)对所述设备进行配置，或者(ii)对所述实时数据进行发送或接收来使得所述过程被控制中的至少一项。

7.根据权利要求4所述的过程控制设备，其中，所发送或所接收的实时数据的至少一部分被包含在消息的内容中，并且其中，包含在所述消息的消息完整性字段中以验证所述消息的所述内容的数据是基于所述密钥的或是基于根据所述密钥而生成的子密钥的。

8.根据权利要求1所述的过程控制设备，其中，所述一组必需的属性包括以下中的至少一项：由所述过程控制设备发送的用于控制所述过程的数据的类型、由所述过程控制设备接收的用于控制所述过程的数据的类型、所述过程控制设备的制造商、所述过程控制工厂的标识、所述过程控制工厂的区域的标识、操作所述过程控制工厂的组织实体的标识、或所述过程控制工厂所处的国家的标识。

9.根据权利要求8所述的过程控制设备，其中，所述一组必需的属性还包括用户的属性。

10.根据权利要求1所述的过程控制设备，其中，所述过程控制设备是以下中的一个：过程控制器、现场设备、或与所述过程控制器连接的输入/输出(I/O)卡。

11.根据权利要求1所述的过程控制设备，还包括将所述过程控制设备通信连接到集中式或分布式大数据装置的接口，并且其中，所述过程控制设备将所述实时数据提供到所述集中式或分布式大数据装置。

用于在过程控制系统中使用的方法和装置

技术领域

[0001] 本公开内容总体上涉及过程工厂和过程控制系统，并且更具体地涉及确认过程工厂和过程控制系统的设备和部件安全。

背景技术

[0002] 诸如那些在化学过程工厂、炼油过程工厂或其他过程工厂中使用的分布式过程控制系统通常包括经由模拟总线、数字总线或组合的模拟/数字总线或经由无线通信链接或网络通信耦合到一个或多个现场设备的一个或多个过程控制器。现场设备被定位在过程环境内并且通常执行诸如打开或关闭阀门、测量过程参数等的物理或过程控制功能以控制在过程工厂或系统内执行的一个或多个过程，该现场设备可以例如是阀门、阀门定位器、开关和发射机(例如，温度传感器、压力传感器、水平传感器和流速传感器)。诸如符合众所周知的Fieldbus协议的现场设备的智能现场设备还可以执行控制计算、报警功能和通常在控制器内实施的其他控制功能。通常还被定位在工厂环境内的过程控制器接收指示由现场设备进行的过程测量和/或与现场设备有关的其他信息的信号并执行例如运行不同控制模块的控制器应用程序，该不同控制模块做出过程控制决策、基于接收到的信息来生成控制信号并且与正在诸如HART®、无线HART®和FOUNDATIONN®Fieldbus现场设备的现场设备中执行的控制模块或控制块协作。控制器中的控制模块通过通信线路或链接将控制信号发送到现场设备以由此控制对过程工厂或系统的至少一部分的操作。

[0003] 来自现场设备和控制器的信息通常通过数据高速通路可用于诸如操作者工作站、个人计算机或计算设备、数据历史记录库(historian)、报告生成器、集中式数据库或可以被放置在控制室或远离较严酷的工厂环境的其他位置中的其他集中式管理计算设备的一个或多个其他硬件设备。在一些过程工厂中，这些硬件设备中的至少一些被集中在过程工厂上或过程工厂的一部分上。这些硬件设备运行可以例如使得操作者能够执行关于控制过程和/或操作过程工厂的功能的应用程序，所述功能例如改变过程控制例程的设置、修改控制器或现场设备内的控制模块的操作、查看过程的当前状态、查看由现场设备和控制器生成的警报、出于训练工作人员或测试过程控制软件的目的对过程的操作进行模拟、保持和更新配置数据库等。由硬件设备、控制器和现场设备利用的数据高速通路可以包括有线通信路径、无线通信路径或有线通信路径和无线通信路径的组合。在一些过程工厂中，数据高速通路的至少一部分包括支持大数据的过程控制网络。

[0004] 作为范例，由爱默生过程管理(Emerson Process Management)销售的DeltaV™控制系统包括存储在被定位在过程工厂内的多个位置处的不同设备内中并由定位在过程工厂内的多个位置处的不同设备执行的多个应用程序。驻存在一个或多个工作站或计算设备中的配置应用程序使得用户能够创建或改变过程控制模块并经由数据高速通路将这些过程控制模块下载到专用的分布式控制器。通常，这些控制模块由相互通信连接的功能块组成，所述功能块是基于对其的输入来执行控制方案内的功能并向控制方案内的其他功能块提供输出的面向对象编程协议中的对象。配置应用程序还可以允许配置设计者创建或改变

操作者接口，所述操作者接口由查看应用程序使用以向操作者显示数据并使得操作者改变过程控制例程内的诸如设定点的设定。每个专用控制器并且在一些情况下一个或多个现场设备存储并执行运行配备和下载到其的控制模块以实施实际的过程控制功能的相应的控制器或现场设备应用程序。可以在一个或多个操作者工作站上(或在与操作者工作站和数据高速通路通信连接的一个或多个远程计算设备上)执行的查看应用程序经由数据高速通路从控制器或现场设备应用程序接收数据并使用用户接口向过程控制系统设计者、操作者或用户显示该数据，并且可以提供多个不同视角中的任何视角，例如操作者的视角、工程师的视角、技术员的视角等。数据历史记录库应用程序通常被存储在数据历史记录库设备中并由数据历史记录库设备执行，所述数据历史设备收集并存储在数据高速通路上提供的数据中的一些或全部，而配置数据库应用程序可以运行与数据高速通路附接的另一计算机以存储当前过程控制例程配置和与其相关联的数据。备选地，配置数据库可以被定位在与配置应用程序相同的工作站中。

[0005] 在一些布置中，分布式过程控制系统包括提供用于支持对过程数据的大规模数据挖掘和数据分析的基础设施的大数据网络或系统(在本文中被可互换地称为“过程控制大数据网络”或“大数据过程控制网络”)。这样的过程控制系统大数据网络或系统的范例可以在前面提到的题目为“BIG DATA IN PROCESS CONTROL SYSTEMS”的美国专利申请No.13/784,041中并且在题目为“DISTRIBUTED BIG DATA IN A PROCESS CONTROL SYSTEM”的美国专利申请No.14/212,493中找到。大数据过程控制网络或系统包括用于收集并存储由包括在过程控制系统或工厂内并与过程控制系统或工厂相关联的设备生成、接收和/或观察到的所有(或几乎所有)数据的多个节点。节点可以经由诸如互联网协议主干网的大数据网络主干网、利用支持大数据的过程控制专用协议的主干网、或计算设备的其他网络组相互连接。在一些实施例中，大数据网络的主干网可以至少部分地与不支持大数据的过程控制系统的至少一部分相交。

[0006] 在支持大数据的一些过程工厂中，过程控制大数据网络的节点之一是大数据被集中地存储、管理和/或历史记录(historize)在其上的过程控制系统大数据装置。过程控制系统大数据装置包括例如统一逻辑数据存储区，所述统一逻辑数据存储区被配置为使用通用格式存储由过程控制系统、过程工厂和由过程工厂控制的一个或多个过程生成或与过程控制系统、过程工厂和由过程工厂控制的一个或多个过程相关的多种类型的数据。例如，统一逻辑数据存储区可以存储配置数据、连续数据、事件数据、工厂数据、指示用户动作的数据、网络管理数据和由或向过程控制系统或工厂外部的系统提供的数据。在其他过程控制节点处，数据(例如，大数据)被盖上时间戳、缓存和/或存储，并且之后可以被流传到大数据装置以用于整合和存储。

[0007] 大数据过程控制网络的其他节点可以包括例如诸如控制器、现场设备和/或将现场设备连接到控制器的I/O(输入/输出)卡的过程控制设备。可以被包括在过程控制大数据网络中的节点的额外范例是路由器、接入点、网关、适配器等。

[0008] 在支持大数据的一些过程工厂中，大数据中的至少一些被本地存储、管理和/或历史记录，例如，大数据被分布式地存储、管理和/或历史记录在大数据过程控制网络的多个节点上。例如，每个分布式大数据节点可以本地存储相应的配置数据、连续数据、事件数据、工厂数据、指示用户动作的数据、网络管理数据和由或向过程控制系统或工厂外部的系统

提供的数据。

[0009] 此外，无论是在大数据装置上和/或在分布式大数据节点上，大数据过程控制系统提供服务和/或数据分析以自动或手动地发现规定的和/或预测的知识，并基于所发现的知识来确定对过程控制系统和对服务和/或分析的组的改变和/或增加，以优化过程控制系统或工厂。

[0010] 然而，无论过程控制系统包括或不包括对大数据的支持，分布式控制系统的一个重要方面是将分布和连接设备和部件分布在整个工厂中或甚至在由单个公司或组织实体拥有或操作的各种工厂中的能力。这些设备和/或部件可以在功能上不同。例如，设备和/或部件中的一些可以直接涉及控制一过程(例如，控制器、现场设备等)和/或设备和/或部件中的一些可以涉及设置、管理、维护和/或诊断工厂的至少一部分(例如，配置设备、诊断设备、数据收集和分析设备等)。此外，设备和/或部件中的一些可以包括用户接口(例如，操作者工作站、移动计算设备、一件测试设备等)。设备和/或部件的至少一些可以是基本上固定的，例如控制器、泵、或传感器可以是基本上固定的。设备和/或部件的至少一些可以是移动的，例如笔记本电脑、平板计算设备或便携式诊断工具可以是移动的。

[0011] 与过程控制工厂的过程控制系统相关联的设备和/或部件的安全性成为关注的重要话题。必须确认连接到过程控制网络的设备和/部件(并且，具体而言，动态连接到过程控制网络和从过程控制网络断开连接的移动设备和/或部件)安全从而减轻潜在的数据盗窃和恶意攻击。如果没有这样做可能导致对过程及其输出的控制的损失。此外，在过程工厂的实时操作期间对不安全的设备和部件的使用可能导致对私人网络和数据的攻破并且在一些情况下可能导致诸如爆炸、火灾和/或设备和/或生命的损失的灾难事件的发生。更进一步的，可能需要确认或验证设备和/或部件在过程控制系统中使用安全以验证设备和/或部件的其相应的指定和预期用途，以及减轻对设备和/或部件的可能的非法再使用和/或恶意使用。

发明内容

[0012] 本文中公开的技术、方法、系统和设备的实施例允许确认设备或部件对过程控制网络或工厂安全，或者允许所述设备或部件能够安全地访问所述过程控制网络和工厂，使得如预期地所述设备或部件安全地被包括在过程控制系统或过程工厂中并且如预期地安全地被利用于过程控制系统或过程工厂中或与过程控制系统或过程工厂一起安全地使用。本文中公开的技术、方法、系统和设备可以适用于具有与过程控制系统或工厂相关联的不同功能的各种不同类型的设备或部件。例如，如之前所讨论的，要确认安全的设备或部件可以用于在控制过程控制系统或过程工厂(例如，控制器、现场设备、I/O卡等)中操作的过程或要由过程控制系统或过程工厂实时控制的过程。能确认安全的设备或部件可以用于设置、管理、维护和/或诊断过程控制系统或工厂的至少一部分(例如，配置设备、诊断工具、数据收集和分析设备等)。用于在过程工厂的实时操作期间使用的能确认安全的设备或部件可以包括用户接口(例如，操作者工作站、移动计算设备、测试设备、包括集成用户接口的过程控制设备等)。能确认安全的设备或部件可以是基本上固定的，或者能确认安全的设备或部件可以是移动的。能确认安全的设备可以是有线设备、无线设备或者可以包括有线接口和无线接口两者。在实施例中，能确认安全的设备或部件用作过程控制系统大数据网络中

的节点。

[0013] 总体上，能够使用本文中描述的技术中的至少一些来确认对过程工厂或过程控制系统安全的(和/或可以被授权安全地访问所述过程控制工厂或系统的过程控制网络的)设备或部件包括处理器和存储器(其可以是非易失性存储器或其他合适的存储器)。所述存储器被配置为存储能够由处理器执行以使得确认所述设备或部件对所述过程控制系统或工厂安全或确认所述设备或部件安全地访问所述过程控制系统或工厂的计算机可执行指令。在一些情况下，所述计算机可执行指令的至少一部分在递送到过程控制系统或工厂之前(例如，在制造厂、工厂、分级或航运站点等)、和/或在所述过程工厂操作以控制过程的同时对所述设备或部件进行配置或利用以进行实时操作之前被存储在所述设备或部件中。先验地存储在所述设备或部件的所述存储器中的指令一般在运输期间或在设备处于现场时是不可改变的。

[0014] 额外地或备选地，包括在所述设备或部件中的所述存储器或不同的存储器被配置为存储必须在允许所述设备或部件通信连接到所述过程控制网络或系统之前满足的一组必需的条件、特性和/或属性(例如，“必需的”条件和/或属性)的一个或多个指示。在一些情况下，所述一组必需的条件的所述一个或多个指示的至少一部分在递送到所述过程控制系统或工厂之前(例如，在制造厂、工厂、分级或航运站点等)、和/或在所述过程工厂操作以控制过程的同时对所述设备或部件进行配置或利用以进行实时操作之前被存储在或被配备到所述设备或部件中。通常，先验地存储的所述指示在运输期间或在设备处于现场时是不可改变的。

[0015] 在一些情况下，所述一组必需的条件、特性和/或属性描述或指示所述设备其自身，例如设备的类型、模型、制造商、序列号等。额外地或备选地，所述一组必需的条件和/或属性描述或指示所述设备在操作在所述过程工厂中或与所述过程工厂联合操作的同时可以发送和/或接收的数据的类型、值和/或状态。更进一步地，额外地或备选地，所述一组必需的条件、特性和/或属性是描述或指示所述设备(在初始化或启动以用于在过程工厂中进行实时操作后)可以处于的环境。在一些情况下，所述一组必需的条件与所述设备的特性用户或用户组相关联。通常，但并不是必需地，只要所述设备是固定的，则所述一组必需的条件、特性和/或属性是相对静态的条件、特性和/或属性。例如，所述一组必需的条件可以包括所述设备的特定地理空间位置，但是将不包括由所述设备观察到的无线信号的信号强度并且将不包括所述设备其自身的动态操作状态(例如，节能模式、睡眠模式等)。

[0016] 此外，能够使用本文描述的技术的实施例来确认对过程控制工厂、系统或网络安全的所述设备或部件还包括到所述过程控制工厂、系统或网络的至少一个相应的通信链接的至少一个接口。所述通信链接可以是有线的或无线的。所述通信链接可以支持过程控制专用协议(例如，Fieldbus、HART、无线HART、过程控制专用大数据协议等)，和/或可以支持诸如以太网或IP协议的通用通信协议。在一些实施例中，为了访问通信链接，第一设备或部件与第二设备或部件通过接口连接，并且所述第二设备代表所述第一设备或部件(例如，连接至I/O卡的现场设备)经由所述通信链接通信信息。

[0017] 在实施例中，设备或部件自我确认安全。例如，为了确认所述设备安全，所述设备或部件被配备或被配置有必须满足的一组相应的必需的条件、特性和/或属性的一个或多个指示。因此，在出于在所述过程工厂内实时操作的目的初始化/启动所述设备或部件之后

或后，并且在与任何其他设备通信以对所述设备进行配置以在所述过程工厂内进行实时操作和/或在所述过程工厂的实时操作期间操作所述设备之前，所述设备或部件检测或确定对应于其自身的和/或对应于其当前所处的环境的一组当前条件或特性。通常，所述设备在不与所述过程工厂的任何其他设备进行通信的情况下执行所述检测或确定。额外地，所述设备确定检测到的一组当前条件是否符合或遵从所述一组必需的条件。如果满足所述必需的条件，则所述设备出于配置和/或实时操作的目的继续与所述过程控制系统或工厂的其他网络设备或部件通信。如果不满足所述必需的条件，则所述设备或部件不允许其自身与所述过程控制工厂或网络中的另一网络设备或部件通信，例如，所述设备或部件阻止其自身与任何其他设备通信和/或通过任何过程控制网络进行通信。以这种方式，所述设备或部件自我检查并在不满足所述必需的条件时使其自身与所述过程控制系统或工厂自我隔离，因此为所述过程控制系统或工厂提供了一定程度的安全性，并且提供了所述设备或部件仅仅如预期(例如，仅仅在指定的位置和/或时间、和/或仅仅当满足特定其他标准时)进行操作的保证。然而，要注意的是，尽管特定的设备或部件与过程控制网络隔离，但是所述特定的设备或部件不需要与其他类型的网络(例如，公共可用通信网络、公司私有网络等)隔离。

[0018] 在实施例中，使用认证过程，例如通过使用密码密钥来确认设备或部件对过程控制网络安全。在通用计算和通信网络中，出于安全性目的，密码密钥通常生成自随机数或伪随机数。然而，在利用本文中公开的技术的实施例的过程控制系统网络和工厂中，增加了额外的安全级别。在范例中，为了确认设备或部件特别对于过程工厂安全，所述设备或部件与根据种子生成的密钥相关联，所述种子包括数字和密钥生成数据两者。所述密钥生成数据指示在主机设备或部件(例如，被配备有所述密钥的设备或部件)被授权访问过程控制网络之前必须满足的一组必需的条件(例如，环境条件、位置、数据状态或值等)。即，所述种子(其包括数字和密钥生成数据两者)可以用于生成密钥，并且所述密钥可以被配备或配置到目标设备或部件中使得所配备的目标设备或部件是主机设备或部件。

[0019] 在实施例中，增加备选或额外的安全级别以确认用于与过程控制系统或工厂中使用的设备或部件安全。在该实施例中，根据指示必须满足以授权所述设备/部件访问过程控制网络的第一必需的条件(例如，环境条件、位置、数据状态或值等)的种子来生成用于设备/部件的密钥。额外地，根据所述密钥来生成子密钥，其中，所述子密钥对应于必须满足以授权所述设备/部件访问过程控制网络的第二组必需的条件(例如，环境条件、位置、数据状态或值等)。在一些情况下，第一组条件和第二组条件可以由不同方限定。

[0020] 下面更详细地描述用于确认设备和部件安全地与过程控制系统或过程工厂网络进行通信的这些和其他技术。要注意的是，本文中描述的技术的实施例可以被单独利用，或与一种或多种其他技术结合使用以确认用于与过程控制系统或过程工厂一起使用的设备或部件安全。

附图说明

[0021] 图1是包括设备或部件可以通信连接到其的一个或多个网络的范例过程控制系统或过程工厂的框图；

[0022] 图2是未被配置为支持过程控制大数据并且设备或部件可以通信连接到其的图1的过程控制系统的一部分的示意图；

[0023] 图3是被配置为支持过程控制大数据并且设备或部件可以通信连接到其的图1的过程控制系统的一部分的框图；

[0024] 图4提供了被连接到过程控制大数据网络主干网的各种提供者节点的范例配置；

[0025] 图5A是用于确认过程控制系统或工厂中的设备的安全的范例方法的流程图；

[0026] 图5B是用于将设备与过程工厂进行认证的另一设备或网络的范例方法的流程图；

[0027] 图6是用于确认过程控制系统或工厂中的设备安全的范例方法的流程图；以及

[0028] 图7是可以在过程控制系统或工厂中或与过程控制系统或工厂联合利用的范例设备的框图。

具体实施方式

[0029] 图1是被配置为控制一个或多个过程的范例过程工厂10(在本文中也可互换地被称为“过程控制系统”、“分布式过程控制系统”、或“自动化工业系统”)的框图。过程工厂10可以例如是具有工业应用程序的化学过程工厂、炼油过程工厂、制造过程工厂或其他过程工厂。分布式过程控制系统或工厂10可以包括设备或部件可以连接或访问以通信信息的一个或多个网络12、15。出于说明的目的，图1的过程工厂10被示出为包括被配置为支持过程控制大数据的一个或多个网络12的组，并且过程工厂10被示出为包括未被配置为支持过程控制大数据的一个或多个网络15(例如，支持用于传统的过程控制环境的诸如以太网、EthernetIP,DeviceNet、CompNet、ControlNet、Modbus、Fieldbus、HART®、无线HART®、Wi-Fi等的一个或多个协议的网络15、和/或有线网络或无线网络)的组。然而，在一些实施例中，过程控制系统或工厂10可以仅仅包括大数据过程控制网络12，或可以仅仅包括非大数据过程控制网络15。在其中过程控制系统或工厂10包括两种类型的网络12、15的实施例中，该两种类型的网络12、15可以例如经由网关或网络接口25通信连接。

[0030] 各种类型的设备和部件被通信连接到网络组12、15中的一个或两者。如在本文中所使用的，“设备”或“部件”可互换地被称为网络12、15的“节点”。通常，网络节点被配置为经由其通信连接的一个或多个网络12、15发送和/或接收通信。同样，通常，但不是必需的，可以通过相应的网络地址来引用网络节点。在一些情况下，网络节点生成其发送的数据或信息。在一些情况下，网络节点接收数据或信息并且使用接收到的数据或信息来执行例如控制过程工厂内执行的过程的功能和/或存储接收到的数据或信息。在一些情况下，网络节点可以在一个或多个网络12、15中路由数据或信息。注意的是在图1中，尽管设备18、20、22被示出为被通信连接到大数据网络12或非大数据网络15，但是该配置仅仅是为了观看的方便而并非限制。例如，设备18、20、22中的一个或多个可以被通信连接到大数据网络12和非大数据网络15两者，例如，设备18、20、22中的一个或多个可以是大数据网络12的节点和非大数据网络15的节点两者。

[0031] 额外地，过程工厂10的网络12、15可以是能够经由外部(相对于过程工厂10)私有网络26a和/或公共网络26b接入的。在一些配置中，过程工厂10的网络12、15被包括在由拥有和/或操作过程工厂10的企业提供的私有网络26a中或与由拥有和/或操作过程工厂10的企业提供的私有网络26a通信连接。例如，过程工厂10的网络12、15被包括在私有企业网络26a中，该私有公司网络26a包括企业的支持该企业的各种功能的其他网络，例如用于人员管理、库存、商情预测、会计等的网络。在另一范例中，企业操作多个过程工厂，过程工厂中

的每个具有其自己的网络12、15，并且多个过程工厂的多个网络12、15被包括在企业的私有公司网络26a(该私有网络可以转而通信连接到一个或多个企业支持网络)中或与企业的私有公司网络26a通信连接。在一些配置中，过程工厂10的网络12、15被通信连接到一个或多个公共网络26b，例如互联网、数据网络和/或电信网络。过程工厂10的网络12、15可以经由图1所示的私有网络26a被通信连接到公共网络26b，或者可以例如在不使用中介私有网络26a的情况下经由直接连接被通信连接到例如公共网络26b。

[0032] 通常，私有网络26a和/或公共网络26b可以利用任何已知的一种或多种网络技术。例如，私有网络26a和/或公共网络26b可以利用有线连接或链接和/或无线连接或链接、分组网络、同步网络、异步网络、ad-hoc网络、云网络、客户机/服务器网络、和/或利用任何已知的其他网络技术的网络或链接。

[0033] 过程控制系统10的多个节点可以包括若干不同组或类型的节点18-22。在过程工厂10中，一个或多个节点18-22可以被通信连接到大数据过程控制网络12，并且一个或多个节点18-22可以被通信连接到非大数据网络15。在一些实施例中，与过程工厂10相关联的一个或多个节点18-22经由一个或多个私有网络26a和/或经由一个或多个公共网络26b被通信连接到过程工厂10的网络12、15中的至少一个。

[0034] 在本文中被称为“提供者节点”、“提供者部件”、或“提供者设备”的第一组节点18包括生成、发送、路由和/或接收实时过程控制数据以使得一个或多个过程能够被在过程工厂环境10中被实时控制的节点、部件或设备。提供者设备或节点18的范例包括其主要功能旨在生成过程控制数据和/或对过程控制数据进行操作以控制过程的设备，例如诸如有线现场设备和无线现场设备、控制器或输入/输出(I/O)设备的过程控制设备。提供者设备18的其他范例包括其主要功能是提供对过程控制设备10的一个或多个通信网络12、15的访问或通过过程控制设备10的一个或多个通信设备网络12、15的路由的设备，例如诸如接入点、路由器、到有线控制总线的接口、到无线通信网络的网关、到外部网络或系统的网关和其他设备的网络设备。提供者设备18的其他范例还包括其主要功能是存储在整个过程控制系统10中累积的实时过程数据和其他相关数据并且任选地使得所存储的数据被发送以用于聚集、整合和/或历史记录的设备。

[0035] 在本文中被称为“用户接口节点”、“用户接口部件”、或“用户接口设备”的第二组或类型的节点20包括节点或设备，节点或设备中的每个具有集成用户接口，经由所述集成用户接口用户或操作者可与过程控制系统或过程工厂10交互以执行与过程工厂10相关的活动(例如，配置、查看、监视、测试、分析、诊断、命令、计划、调度、注释和/或其他活动)。这些用户接口节点或设备20的范例包括移动或固定的计算设备、工作站、手持设备、平板电脑、表面计算设备、诊断设备、工具、以及具有处理器、存储器和集成用户接口的任何其他计算设备。集成用户接口可以包括屏幕、键盘、小键盘、鼠标、按钮、触摸屏、生物计量接口、扬声器和麦克风、相机、和/或任何其他用户接口技术，并且每个用户接口节点20包括一个或多个集成用户接口。用户接口节点20可以包括到过程控制网络12、15的直接连接或者可以包括例如经由互联网26b或经由通过接入点或网关的其他网络26a、26b到过程控制网络12、15的间接连接。用户接口节点20可以以有线方式和/或无线方式通信连接到过程控制系统网络12、15。在一些实施例中，用户接口节点20以ad-hoc方式连接到过程控制系统网络12、15。通常使用无线通信协议来建立这样的ad-hoc连接，该无线通信协议例如符合IEE

802.11的无线局域网协议、诸如WiMAX、LTE或其他兼容ITU-R的移动通信协议、诸如近场通信(NFC)或蓝牙的短波无线通信协议、诸如无线HART或无线大数据过程控制协议的过程控制无线协议、或一些其他合适的无线通信协议。

[0036] 在一些实施例中，设备是提供者设备18和用户接口设备20两者，例如当提供者设备18包括集成用户接口时。

[0037] 当然，被通信连接到过程控制系统或工厂10的网络12、15的多个节点并不仅限于提供者节点18和用户节点20。一个或多个其他类型的节点22还可以被包括在多个节点中。这样的节点22的范例包括在过程工厂10外部(例如，在实验室系统处或材料处理系统的计算机)并且被通信连接到系统10的网络12、15的设备、以及远程控制的移动诊断设备。此外，节点或设备22可以经由直接或间接连接、和或经由有线连接或无线连接被通信连接到系统10的网络12、15。在一些实施例中，从过程控制系统10中省略该组其他节点22。

[0038] 图2是图1的网络15的部分28的范例的示意图。如之前提到的，网络15不支持在过程工厂10中的过程控制大数据，并且一个或多个设备或部件18至22可以被通信连接到网络15。通常，非大数据网络15的部分28包括一个或多个有线网络和/或无线网络，所述一个或多个有线网络和/或无线网络中的至少一个使用过程控制协议来将数据承载到和来自诸如控制器、I/O设备、和现场设备的过程控制设备的数据，该过程控制设备对数据进行操作并执行控制过程工厂10中的过程的物理功能。在一个范例中，部分28是利用非大数据协议的传统过程控制网络，该非大数据协议例如以太网、EthernetIP、DeviceNet、CompNet、ControlNet、Modbus、Fieldbus、HART®、无线HART®、Wi-Fi等。如图2中所示，过程控制系统10的部分28包括连接到数据历史记录库32和每个具有显示屏34的一个或多个主机工作站或计算机33(其可以是任何类型的个人计算机、工作站等)的至少一个过程控制器31。过程控制器31还经由输入/输出(I/O)卡46和48连接到现场设备35至42。数据历史记录库32可以是具有用于存储数据的任何期望类型的存储器和任何期望的或已知的软件、硬件或固件的任何期望类型的数据收集单元，并且尽管数据历史记录库32被图示为单独的设备，但是其可以代替地或额外地是工作站33或诸如服务器的另一计算机设备中的一个的部分。可以为例如由爱默生过程管理销售的DeltaV™控制器的控制器31被通信连接到主机计算机33并且经由通信网络49被通信连接到数据历史记录库32，通信网络49可以例如是有线以太网连接或无线以太网连接。

[0039] 控制器31被图示为使用硬接线通信方案被通信连接到现场设备35-42，所述硬接线通信方案可以包括对任何期望的硬件、软件和/或固件的使用以实施包括例如标准4-20mA通信的硬接线通信和或使用诸如FOUNDATION®、Fieldbus通信协议、HART®通信协议等的任何智能通信协议的任何通信，。现场设备35-42可以是诸如传感器、阀门、发射机、定位器等的任何类型的设备，而I/O卡46和48可以是符合任何期望的通信或控制器协议的任何类型的I/O设备。在图2中所示的实施例中，现场设备35-38是通过模拟线路与I/O卡46通信的标准4-20mA设备，而现场设备39-42则是诸如使用Fieldbus协议通信通过数字总线与I/O卡48通信的Fieldbus现场设备的智能设备。当然，现场设备35-42可以符合(一个或多个)任何其他期望的标准或协议，包括在未来发展的任何标准或协议。

[0040] 此外，过程控制系统10的部分28包括设置在要控制的工厂中的多个无线现场设备60-64和71，以由此控制过程。现场设备60-64在图2中被描绘为发射机(例如，过程变量传感

器)，并且现场设备71被描绘为阀门。然而，这些现场设备可以是设置在过程内以实施物理控制活动或测量过程内的物理参数来控制工厂10内的过程的任何其他期望类型的设备。可以使用包括现在已知的或稍后发展的硬件、软件、固件或其任何组合的任何期望的无线通信设备来在控制器31与现场设备60-64和71之间建立无线通信。在图2中示出的范例情况下，天线65被耦合到现场设备60并且专门用于执行现场设备60的无线通信，而具有天线67的无线路由器或其他模块66被耦合以统一地处理现场设备61-64的无线通信。同样地，天线72被耦合至阀门71以执行阀门71的无线通信。现场设备或相关联的硬件60-64、66和71可以实施由合适的无线通信协议(在范例中，无线HART®协议、WiFi或其他符合IEEE 802.11的无线局域网协议、诸如WiMAX(全球互通微波存取)的移动通信协议、LTE(长期演进)或其他可兼容ITU-R(国际电信联盟无线电通信组)的协议、诸如近场通信(NFC)和蓝牙的短波无线通信、或其他无线通信协议)使用的协议堆栈操作以经由天线65、67和72接收、解码、路由、编码和发送无线信号来实施控制器31与发射机60-64和阀门71之间的无线通信。

[0041] 如果期望，现场设备或发射机60-64可以组成各种过程设备与控制器31之间的单一链接，并且因此被依赖以将正确的信号发送至控制器31，从而确保产品质量和流量不受损。额外地，阀门或其他现场设备71可以向控制器31提供由阀门71内的传感器进行的测量或由阀门71生成或计算的其他数据作为阀门71操作的一部分，所述数据包括由在阀门71内执行的功能块FB1和FB2收集、计算、或以其他方式生成的数据。当然，阀门71还可以从控制器31接收控制信号来影响物理参数，例如，工厂内的流量。

[0042] 控制器31被耦合到一个或多个I/O设备73和74，一个或多个I/O设备73和74中的每个被连接到相应的天线75和76，并且这些I/O设备和天线73-76用作发射机/接收机以执行经由一个或多个无线通信网络与无线现场设备61-64和71的无线通信。可以使用例如上面讨论的诸如无线HART®协议、Ember协议、WiFi协议、IEEE无线标准等的一个或多个已知的无线通信协议来执行现场设备(例如，在发射机60-64与阀门71)之间的无线通信。更进一步地，I/O设备73和74可以实施由这些通信协议使用的协议堆栈操作以经由天线75和76来接收、解码、路由、编码和发送无线信号以实施控制器31与发射机60-64和阀门71之间的无线通信。

[0043] 如图2所示，控制器31包括实施或监督存储在存储器78中的一个或多个过程控制例程(或任何模块、块、或其子例程)的处理器77。存储在存储器78中的过程控制例程包括被实施在过程工厂内以控制过程的至少一部分的控制循环或与被实施在过程工厂内以控制过程的至少一部分的控制循环相关联。通常，控制器31执行一个或多个控制例程并与现场设备35-42、60-64和71(以及任选地主机计算机33和数据历史记录库32)通信来以(一个或多个)任何期望的方式控制过程。然而，应当注意的是，本文中描述的任何控制例程或模块可以具有以分布式方式被实施或执行在多个设备上的其部分。因此，如果期望，控制例程或模块可以具有由不同控制器、现场设备(例如，智能现场设备)或其他设备或其他控制元件实施的部分。

[0044] 同样，要在过程控制系统10内实施的本文中描述的控制例程或模块可以采取任何形式，包括软件、固件、硬件等。涉及提供这样的功能的任何设备或元件可以总体上在本文中可互换地被称为“控制元件”、“过程控制元件”、或“过程控制设备”，无论与其相关联的软件、固件、或硬件是否被设置在过程控制系统10内的控制器、现场设备、或任何其他设备(或

设备的集合)中。当然,控制模块可以是过程控制系统的包括例如存储在任何计算机可读介质上的例程、块或其任何元件的任何一部分或部分。这样的控制模块、控制例程或其任何部分可以由在本文中被统称为控制元件的过程控制系统10的任何元件或设备实施或执行。此外,可以是诸如子例程、子例程的部分(例如代码行)等的控制流程的模块或任何部分的控制例程可以以诸如面向对象编程、梯形逻辑、顺序功能图、功能框图的任何期望的软件格式或使用任何其他软件编程语言或设计范式实施。同样地,控制例程可以是被硬编码到例如一个或多个EPROM、EEPROM、专用集成电路(ASIC)或任何其他的硬件或固件元件中。更进一步地,可以使用包括图形设计工具或任何其他类型的软件/硬件/固件编程或设计工具的任何设计工具来设计控制例程。因此,控制器31可以被配置为以任何期望的方式实现控制策略或控制例程。

[0045] 在一些实施例中,控制器31使用通常被称为功能块的部件来实现控制策略或方案,其中,每个功能块是与其他功能块(经由被称为链接的通信)联合操作以实施过程控制系统10内的过程控制循环的整体控制例程的对象或其他部分(例如,子例程)。功能块通常执行诸如与发射机、传感器或其他过程参数测量设备相关联的的输入功能、诸如与执行PID、模糊逻辑、模型预测控制等的控制例程相关联的控制功能、或控制诸如阀门的特定设备的操作来执行过程控制系统10内的特定物理功能的输出功能中的一个。当然,本文中存在并且可以利用混合类型或其他类型的功能块。功能块可以被存储在控制器31中并由控制器31执行,这通常是当功能块被用于标准4-20mA设备和诸如HART®设备的一些类型的智能现场设备或与标准4-20mA设备和诸如HART®设备的一些类型的智能现场设备相关联时的情况。备选地或额外地,功能块可以被存储在现场设备其自身、I/O设备或过程控制系统10的其他控制元件中并由现场设备其自身、I/O设备或过程控制系统10的其他控制元件实施,这可以是系统利用Fieldbus设备的情况。尽管本文中使用功能块控制策略总体上提供了对控制系统10的描述,但是所公开的技术和系统还可以使用其他常规手段或编程范式来实施或设计。

[0046] 图3是被配置为支持过程控制数据(例如,网络12)并且设备和/或部件可以通信连接到其的过程控制系统10的范例部分30。具体地,图3示出了用于过程工厂或过程控制系统10的范例过程处理系统大数据网络100。范例过程控制系统大数据网络100包括过程控制系统大数据网络主干网105和通信连接到主干网105的多个节点108。在一些实施例中,节点108中的至少一个是集中式大数据装置102;然而,并不要求过程控制网络10的大数据网络部分12包括单个的集中式大数据装置102。例如,多个分布式大数据装置102可以被分布在工厂内,和/或单个的大数据节点每个可以执行分布式大数据功能。

[0047] 在范例过程控制系统大数据网络100中,过程相关的数据、工厂相关的数据、以及其他类型的数据在多个节点108处被收集、被缓冲和/或被存储作为大数据。在网络12的一些配置中,所收集、所缓冲和/或所存储的数据中的至少一些经由网络主干网105被递送到集中式和/或分布式过程控制系统大数据装置或装置102以用于长期存储(例如,“历史记录”)和处理。在网络12的一些配置中,所收集、所缓冲和/或所存储的数据中的至少一些被维持在节点108处,在节点108处收集数据以用于历史记录和处理,在实施例中,可以在网络100的节点108之间递送数据中的至少一些以例如实时控制过程。

[0048] 在实施例中,与过程控制系统10相关的任何类型的数据被历史记录在大数据装置

102处和/或在各个其他节点108处。在实施例中，收集由通信连接到网络主干网105的节点108中的至少一个子集生成、接收或观察到的所有数据并使所述数据被存储在过程控制系统大数据装置102中(例如，“集中式大数据”)。额外地或备选地，在特定节点108处收集并存储由特定节点108生成、接收或观察到的与过程控制系统10相关的所有数据(例如，“分布式大数据”)。

[0049] 在实施例中，收集并存储过程数据。例如，收集并存储实时过程数据，例如由于在过程工厂10中控制的过程而生成的(并且，在一些情况下指示过程的实时执行的效果的)连续数据、批处理数据、测量数据和事件数据。收集并存储过程定义数据、过程布置数据和过程启动数据，例如配置数据和/或批处理配方数据，和/或对应于配置、执行和过程诊断的结果的数据。还可以收集并存储其他类型的过程数据。

[0050] 在实施例中，收集并存储过程工厂10的主干网105的和各种其他通信网络的数据高速通路流量和网络管理数据。在实施例中，收集并存储用户相关数据，例如与用户流量、登陆尝试、查询和指令相关的数据。可以收集并存储文本数据(例如，日志、操作流程、手册等)、空间数据(例如，基于位置的数据)和多媒体数据(例如，闭路电视、视频剪辑等)。

[0051] 在实施例中，收集并存储与过程工厂10(例如，与包括在过程工厂10中的诸如机器和设备的物理设备)相关但可以不是由直接对过程进行配置、控制或诊断的应用程序生成的数据。例如，可以收集并存储振动数据和疏水阀数据，和/或可以收集并存储工厂安全数据。例如，存储指示对应于工厂安全的参数的值的数据(例如，腐蚀数据、气体检测数据等)，和/或存储指示对应于工厂安全的事件的数据。可以收集并存储对应于机器、工厂设备和/或设备的健康的数据。例如，收集并存储设备数据(例如，基于振动数据和其他数据确定的泵健康数据)和/或对应于对设备、机器和/或设备诊断的配置、执行和结果的数据。在一些实施例中，收集并存储由过程工厂10外部的实体生成或向所述实体发送的数据，例如与原材料的成本、零件或设备的预期到达时间、天气数据和其他外部数据相关的数据。

[0052] 如之前参考图1讨论的，过程控制大数据网络100可以包括多个节点18、20、22，这些节点在图3中统一由附图标记108指代。在图3中，第一组大数据节点110是例如以直接或间接的方式与过程控制大数据网络主干网105通信连接的提供者节点18。大数据提供者节点110可以是有线设备或无线设备。通常，大数据提供者设备110不具有集成用户接口，尽管提供者设备100中的一些可以具有与用户计算设备或用户接口通信连接的能力，例如，通过经由有线通信链接或无线通信链接进行通信或通过将用户接口设备插入到提供者设备110的端口中。

[0053] 额外地，在图3中，第二组大数据节点112是例如以直接或间接的方式和/或以有线的方式和/或以无线的方式通信连接到过程控制大数据网络主干网105的用户接口节点20。在一些实施例中，用户接口节点112以ad-hoc的方式连接至网络主干网105。此外，在过程工厂10的一些配置中，一个或多个其他类型的数据节点115被包括在多个节点108中。例如，在过程工厂10外部的系统(例如，实验室系统或材料处理系统)的节点可以被通信连接到系统100的网络主干网105。与提供者节点110类似，大数据用户接口节点112或其他大数据节点115可以经由直接连接或间接连接和/或经由有线连接或无线连接被通信连接到主干网105。

[0054] 任何数量的大数据节点108(例如，零个节点、一个节点或多于一个节点)每个包括

用于实时存储(和/或,在一些情况下,缓存)任务数据、测量数据、事件数据和其他数据的相应的存储装置(图3中由图符M_x指代)。在实施例中,存储装置M_x包括高密度存储装置技术,例如,固态驱动存储器、半导体存储器、光学存储器、分子存储器、生物存储器或任何其他合适的高密度存储器技术。在一些实施例中,存储装置M_x还包括闪速存储器。存储装置M_x(并且,在一些情况下,闪速存储器)被配置为存储和/或缓存由其相应的节点108生成、在其相应的节点108处接收或由其相应的节点108以其他方式观察到的数据。节点108中的至少一些的闪速存储器M_x还可以存储节点配置、批处理配方和/或其他数据的快照。在过程控制系统大数据网络100的实施例中,所有的节点110、112和任何数量的节点115包括高密度存储装置M_x。应理解,可以在节点108的集合上或在节点108的集合中包括的节点的子集上利用不同类型或技术的高密度存储装置M_x。

[0055] 在实施例中,任何数量的节点108(例如,零个节点、一个节点或多于一个节点)每个包括相应的多核硬件(例如,多核处理器或另一类型的并行处理器),如在图3中由图符P_{MCX}指代的。节点108中的至少一些可以指定其相应的处理器P_{MCX}的内核中的一个用于在节点处存储实时数据。额外地或备选地,节点108中的至少一些可以指定其相应的多核处理器P_{MCX}的多个内核中的多于一个的内核用于缓存实时数据(并且,在一些情况下,用于使所缓存的实时数据被存储在大数据装置102处)。在一些实施例中,一个或多个指定的用于存储实时数据的内核和一个或多个指定的用于缓存实时数据的内核被这样专有地指定(例如,一个或多个指定的内核除了执行与存储和处理大数据相关的处理之外不执行其他处理)。在实施例中,节点108中的至少一些每个指定其内核中的一个来执行控制过程工厂10中的过程的操作。在实施例中,一个或多个内核被专有地指定用于执行控制过程的操作,而不用于处理大数据。应理解,可以在节点108的集合上或在节点108的集合的节点的子集上利用不同类型或技术的多核处理器P_{MCX}。在过程控制系统大数据网络100的实施例中,所有的节点110、112和任何数量的节点115包括特定类型的多核处理器P_{MCX}。

[0056] 然而,要注意的是尽管图3将节点108示出为每个包括多核处理器P_{MCX}和高密度存储器M_x两者,但是并不要求节点108中的每个包括多核处理器P_{MCX}和高密度存储器M_x两者。例如,节点108中的一些可以仅包括多核处理器P_{MCX}而不包括高密度存储器M_x,节点108中的一些则可以仅包括高密度存储器M_x而不包括处理器P_{MCX},节点108中的一些可以包括多核处理器P_{MCX}和高密度存储器M_x两者,和/或节点108中的一些可以既不包括多核处理器P_{MCX}也不包括高密度存储器M_x。

[0057] 可以由提供者节点或设备110收集、缓存、和/或存储的实时数据的范例包括测量数据、配置数据、批处理数据、事件数据、和/或连续数据。例如,可以收集对应于对其配置、批处理配方、设定点、输出、速率、控制动作、诊断、警报、事件和/或改变的实时数据。实时数据的其他范例包括过程模型、统计、状态数据、以及网络和工厂管理数据。可以由用户接口节点或设备112收集、缓存、和/或存储的实时数据的范例包括例如用户登录、用户查询、由用户(例如,通过相机、音频或视频记录设备)捕获的数据、用户命令、文件的创建、修改或删除、用户接口节点或设备的物理或空间位置、由用户接口设备12执行的诊断或测试的结果、以及由与用户接口节点12交互的用户发起的或与和用户接口节点12交互的用户相关的其他动作或活动。

[0058] 所收集、所缓存和/或所存储的数据可以是动态数据或静态数据。例如,所收集、所

缓存和/或所存储的数据可以包括例如数据库数据、流传输数据、和/或交易数据。一般地，可以利用对应的时间戳或对收集/缓冲的时间的指示来收集、缓存和/或存储节点108生成、接收或观察到的任何数据。在优选实施例中，利用对每个数据的收集/缓冲的时间的相应的指示(例如，时间戳)来在节点108的存储装置(例如，高密度存储装置M_x)中收集、缓存和/或存储节点108生成、接收或观察到的所有数据。

[0059] 因此，在大数据过程控制网络100中，在节点或设备108处和/或在大数据装置102处收集、缓存和/或存储的数据的标识无需先验地被配置到设备108中。此外，也无需配置、选择或定义在节点108处收集的和从节点108递送的数据的速率。代替地，过程控制大数据系统100的节点110、112(和，备选地，其他节点115中的至少一个)自动地以生成、接收、获得数据的速率收集由节点生成的、在所述节点处接收的或由所述节点获得的所有数据，并且自动地使所收集的数据被本地存储在节点110、112处和/或大数据装置102处。

[0060] 图4图示了连接到过程控制大数据网络主干网105的各种提供者节点110的范例配置。如之前所讨论的，提供者节点110包括其主要功能是自动生成和/或接收用于在诸如过程控制器、现场设备和I/O设备的过程工厂环境10中执行对过程进行实时控制的功能的过程控制数据的设备。在过程工厂环境10中，过程控制器接收指示由现场设备进行的过程测量的信号、处理该信息以实施控制例程、并且生成通过有线通信链接或无线通信链接被发送到其他现场设备以控制对工厂10中的过程的操作的控制信号。通常，至少一个现场设备执行控制过程的操作(例如，打开或关闭阀门、增大或减小温度等)的物理功能，而一些类型的现场设备可以使用I/O设备与控制器通信。过程控制器、现场设备和I/O设备可以是有线的或无线的，并且任何数量的有线过程控制器和无线过程控制器、现场设备和I/O设备及其组合可以是过程控制大数据网络100的提供者节点110。

[0061] 例如，图4包括过程控制器131，过程控制器131经由输入/输出(I/O)卡146和148被通信连接到有线现场设备135-142，并且经由无线网关165和网络主干网105被通信连接到现场设备150-156(现场设备150-156中的一些是无线的150至154，而现场设备150-156中的一些不是无线的155、156)。(然而，在另一实施例中，控制器131使用除了主干网105之外的通信网络，例如通过使用另一有线通信链接或无线通信链接被通信连接到无线网关165)。在图4中，控制器131和I/O卡146、148被示出为是过程控制系统大数据网络100的节点110，而控制器131被直接连接到过程控制大数据网络主干网105。

[0062] 可以为例如由爱默生过程管理销售的DeltaV™控制器的控制器131可以用于使用现场设备135-142和150-156中的至少一些来实施批处理过程或连续过程。控制器131可以使用任何期望的硬件和软件被通信连接到现场设备135-142和150-156，所述任何期望的硬件和软件与例如标准4-20mA设备、I/O卡146、148和/或诸如FOUNDATION®Fieldbus协议、HART®协议、无线HART®协议等的任何智能通信协议相关联。在一些情况下，控制器131额外地或备选地使用大数据网络主干网105与现场设备135-142和150-156中的至少一些通信连接。在图4中图示的实施例中，控制器131、现场设备135-142、155、156和I/O卡146、148是有线设备，而现场设备150-154是无线现场设备。当然，有线现场设备135-142、155、156和无线现场设备150-154能够符合(一个或多个)任何其他期望的标准或协议，例如任何有线协议或无线协议，包括未来发展的任何标准或协议。

[0063] 图4的控制器131包括实施或监督(存储在存储器172中的)可以包括控制循环的一

个或多个过程控制例程的处理器170。处理器170可以与现场设备135-142和150-156以及通信连接到主干网105的其他节点(例如,节点110、112、115)通信。应当注意,如果期望,本文中描述的任何控制例程或模块(包括质量预测和故障检测模块或功能块)可以使其部分由不同的控制器或其他设备实施或执行。同样地,本文中描述的要在过程控制系统10内部实施的控制例程或模块可以采取任何形式,包括软件、固件、硬件等。可以以任何期望的软件格式实施控制例程,例如使用面向对象的编程、梯形逻辑、顺序功能图、功能框图或使用任何其他的软件编程语言或设计范式实施控制例程。控制例程可以被存储在诸如随机存取存储器(RAM)或只读存储器(ROM)的任何期望类型的存储器中。同样地,控制例程可以被硬编码到例如一个或多个EPROM、EEPROM、专用集成电路(ASIC)或其他硬件或固件元件中。因此,控制器31可以被配置为以任何期望的方式实施控制策略或控制例程。

[0064] 在一些实施例中,控制器131使用通常被称为功能块的部件来实施控制策略,其中,每个功能块是与其他功能块(经由被称为链接的通信)联合操作以实施过程控制系统10内的过程控制循环的整体控制例程的对象或其他部分(例如,子例程)。基于控制的功能块通常执行诸如与发射机、传感器或其他过程参数测量设备相关联的输入功能、诸如与执行PID、模糊逻辑、模型预测控制等的控制例程相关联的控制功能、或控制诸如阀门的特定设备的操作来执行过程控制系统10内的特定物理功能的输出功能中的一个。当然,存在混合类型或其他类型的功能块。功能块可以被存储在控制器31中并由控制器31执行,这通常是当这些功能块被用于标准4-20mA设备和诸如HART设备的一些类型的智能现场设备或与标准4-20mA设备和诸如HART设备的一些类型的智能现场设备相关联时的情况,或者功能块可以被存储在现场设备其自身中并由现场设备其自身执行,这能够是利用Fieldbus设备的情况。控制器131可以包括可以实施一个或多个控制循环的一个或多个控制例程178。每个控制循环通常被称为控制模块,并且可以通过执行功能块种的一个或多个来执行。

[0065] 有线现场设备135-142、155、156可以是诸如传感器、阀门、发射机、定位器等的任何类型的设备,而I/O卡146和148可以是符合任何期望的通信协议或控制器协议的任何类型的I/O设备。在图4中图示的实施例中,现场设备135-138是通过模拟线路或组合的模拟和数字线路与I/O卡146进行通信的标准4-20mA设备或HART设备,而现场设备139-142是使用Fieldbus通信协议通过数字总线与I/O卡148通信的智能设备,例如FOUNDATION® Fieldbus现场设备。然而,在一些实施例中,有线现场设备135-142中的至少一些和/或I/O卡146、148中的至少一些使用大数据网络主干网105与控制器131通信。在一些实施例中,有线现场设备135-142中的至少一些和/或I/O卡146、148中的至少一些是过程控制系统大数据网络100的节点110。

[0066] 在图4中示出的实施例中,无线现场设备150-154使用诸如无线HART协议的无线协议在无线网络180中通信。这样的无线现场设备150-154可以直接与还被配置为(例如,使用相同或不同的无线协议)无线通信的过程控制大数据网络100中的一个或多个其他节点108通信。为了与未被配置为无线通信的一个或多个其他节点进行通信,无线现场设备150-154可以利用连接至主干网105或另一过程控制通信网络的无线网关165。在一些实施例中,无线现场设备150-154中的至少一些和无线网关165是过程控制系统大数据网络100的节点110。

[0067] 无线网关165是可以提供对包括在过程工厂10中的无线通信网络180的各种无线

设备的访问的提供者设备110的范例。具体地，无线网关165提供无线设备150-154、157-159、无线设备135-142、155、156和/或过程控制大数据网络100中的其他节点(包括图4的控制器131)之间的通信耦合。例如，无线网关165可以通过使用大数据网络主干网105和/或通过使用过程工厂10的一个或多个其他通信网络来提供通信耦合。

[0068] 在一些情况下，无线网关165在隧穿(tunnelling)有线和无线协议堆栈的一个或多个共享层的同时，通过对有线和无线协议堆栈的下层的路由服务、缓冲服务、定时服务(例如，地址转换、路由、数据包分割、优先化等)来提供通信耦合。在其他情况下，无线网关165可以在不共享任何协议层的有线协议与无线协议之间转化命令。除了协议和命令转换，无线网关165可以提供由与在无线网络180中实施的无线协议相关联的调度方案的时隙和超帧(在时间上等间隔的通信时隙组)使用的同步时钟。此外，无线网关165可以为无线网络180提供网络管理和监管功能，例如资源管理、性能调节、网络故障缓解、监测流量、安全确认等。无线网关165可以是过程控制系统大数据网络100的节点110。

[0069] 与有线现场设备135-142类似，无线网络180的无线现场设备150-154可以执行过程工厂10内部的物理控制功能，例如，打开或关闭阀门或对过程参数进行测量。然而，无线现场设备150-154被配置为使用网络180的无线协议进行通信。因此，无线网络180中的无线现场设备150-154、无线网关165和其他无线节点157-159是无线通信数据包的生产者和消费者。

[0070] 在一些情形中，无线网络180可以包括非无线设备。例如，图4中的现场设备155可以是传统的4-20mA设备，而现场设备156可以是传统的有线HART设备。为了在网路180内进行通信，现场设备155和156可以分别经由无线适配器(WA)157a或157b被连接到无线通信网络180。此外，无线适配器157a、157b可以支持诸如FOUNDATION®Fieldbus、PROFIBUS、DeviceNet等的其他通信协议。此外，无线网络180可以包括一个或多个网络接入点158a、158b，一个或多个网络接入点158a、158b可以是与无线网关165有线通信的单独的物理设备或者可以被配备有无线网关165作为集成设备。无线网络180还可以包括用于在无线通信网络180内将数据包从一个无线设备转发到另一无线设备的一个或多个路由器159。无线设备150-154和157-159可以通过无线通信网络180的无线链接175相互通信并与无线网关165通信。

[0071] 因此，图4包括主要用于向过程控制系统的各个网络提供网络路由功能和监管的提供者设备110的若干范例。例如，无线网关165、接入点158a、158b和路由器159包括用于在无线通信网络180中对无线数据包进行路由的功能。无线网关165执行无线网络180的流量管理和监管功能，以及将流量路由到与无线网络180通信连接的有线网络和从与无线网络180通信连接的有线网络路由流量。无线网络180可以利用专门支持过程控制消息和功能的无线过程控制协议，例如无线HART。

[0072] 然而，过程控制大数据网络100中的提供者节点110还可以包括使用其他无线协议通信的其他节点。例如，提供者节点110可以包括利用其他无线协议的一个或多个无线接入点192，所述其他无线协议可以与过程控制无线网络180中利的无线协议不同或相同。例如，无线接入点192可以使用Wi-Fi或其他符合IEEE 802.11的无线局域网协议、诸如WiMAX(全球互通微波存取)的移动通信协议、LTE(长期演进)或其他可兼容ITU-R(国际电信联盟无线电通信组)的协议、诸如近场通信(NFC)和蓝牙的短波无线电通信、或其他无线通信协议。通

常，这样的无线接入点192允许手持设备或其他便携式计算设备(例如，用户接口设备112)通过不同于无线网络180并支持与无线网络180不同的无线协议的的相应的无线网络进行通信。在一些情形中，除了便携式计算设备，一个或多个过程控制设备(例如，控制器31、现场设备135-142或无线设备150-154)还可以使用由接入点192支持的无线装置进行通信。

[0073] 额外地或备选地，提供者节点110可以包括到在当前过程控制系统或工厂10的外部但又与拥有和/或操作工厂10的企业相关联的系统的一个或多个网关195、198。通常，这样的系统是由过程控制系统或工厂10生成或操作的信息的用户或供应者，并且可以经由诸如图1中示出的私有网络25a的私有企业网络相互连接。例如，工厂网关节点195可以将(具有它自己的相应的过程控制大数据网络主干网105的)当前过程工厂10与具有它自己的相应的过程控制大数据网络主干网的另一过程工厂通信连接。在实施例中，单个过程控制大数据网络主干网105可以服务多个过程工厂或过程控制环境。

[0074] 在另一实施例中，工厂网关节点195可以将当前过程工厂10通信连接到不包括过程控制大数据网络100或主干网105的传统或现有技术的过程工厂。在该范例中，工厂网关节点195可以在由工厂10的过程控制大数据主干网105利用的协议与由传统系统(例如，以太网、Profibus、Fieldbus、DeviceNet等)利用的不同协议之间转换或转化消息。

[0075] 提供者节点110可以包括将过程控制大数据网络100与外部公共或私有系统的网络通信连接的一个或多个外部系统网关节点198，所述外部公共或私有系统例如实验室系统(例如，实验室信息管理系统或LIMS)、运营商轮数据库、材料处理系统、维护管理系统、产品库存控制系统、生产调度系统、天气数据系统、航运和处理系统、封装系统、互联网、另一提供者的过程控制系统、或其他外部系统。例如，可以经由私有网络访问(例如，图1中的私有网络26a)来访问一个或多个外部系统，和/或经由公共网络(例如，图1中的公共网络26b)来访问一个或多个外部系统。

[0076] 额外地，尽管图4仅示出了具有有限数量的现场设备135-142和150-156的单个控制器131，但是这仅仅是说明性的而非限制性的实施例。可以在过程控制大数据网络100的提供者节点110中包括任何数量的控制器131，并且控制器131中的任何可以与任何数量的有线或无线现场设备135-142、150-156通信以控制工厂10中的过程。此外，过程工厂10还可以包括任何数量的无线网关165、路由器159、接入点158、无线过程控制通信网络180、接入点192和/或网关195、198。

[0077] 如之前讨论的，一个或多个提供者节点110可以包括相应的多核处理器P_{MCX}、相应的高密度存储装置M_X、或相应的多核处理器P_{MCX}和相应的高密度存储装置M_X两者(在图4中由图符BD指代)。每个提供者节点100可以利用其存储装置M_X(和，在一些实施例中，其闪速存储器)来收集、存储和/或缓冲数据。如之前讨论的，在一些过程工厂10中，提供者节点110中的至少一些将所存储和/或所缓存的大数据发送到大数据装置102以用于历史记录、聚集和/或整合，和/或提供者节点100中的至少一些将大数据维持在本地以用于历史记录、聚集和/或整合。

[0078] 进一步参考图4，过程控制系统大数据网络主干网105包括多个联网计算设备或交换机，所述多个联网计算设备或交换机被配置为将数据包路由到过程控制系统大数据网络100的各个节点/从过程控制系统大数据网络100的各个节点路由数据包，并且在网络100中包括过程控制大数据装置102的情况下将数据包路由到过程控制大数据装置102/从过程控

制大数据装置102路由数据包。主干网105的多个联网的计算设备可以通过任何数量的无线链接和/或有线链接相互连接。在实施例中，过程控制系统大数据网络主干网105包括一个或多个防火墙设备。

[0079] 大数据网络主干网105支持一个或多个合适的路由协议，例如，在互联网协议(IP)族中包括的协议(例如，UPD(用户数据报协议)、TCP(传输控制协议)、以太网等)、或其他合适的路由协议。在实施例中，节点中的至少一些利用诸如流控制传输协议(SCTP)的流传输协议来经由网络主干网105从节点将所缓存的数据流传输到过程控制传大数据装置102。在实施例中，由大数据网络主干网105支持的路由协议是用于过程控制大数据的过程控制专用路由协议。通常，在过程控制大数据网络100中包括的每个节点108可以至少支持由主干网105支持的(一个或多个)路由协议的应用层(和，对于一些节点，附加层)。在实施例中，每个节点108在过程控制系统大数据网络100内例如由唯一的网络地址唯一地标识。

[0080] 在实施例中，过程控制系统大数据网络100的至少一部分是ad-hoc网络。因此，节点108中的至少一些可以以ad-hoc的方式连接到网络主干网105(或连接到网络100中的另一节点)。在实施例中，请求加入网络100的每个节点必须是被认证的。将在稍后的章节更详细地讨论认证。

[0081] 返回图3，在其处存储大数据的每个节点108(例如，大数据装置102和/或一个或多个其他节点108)包括具有支持过程控制系统相关的数据的所有类型的存储的结构的统一逻辑数据存储区(例如，M_X)。例如，在逻辑数据存储区(例如，M_X)处存储的每个条目、数据点、或观察结果可以包括对数据的标识的指示(例如，源、设备、标签、位置等)、数据的内容(例如，测量结果、值等)、以及指示收集、生成、接收或观察到的时间的数据时间戳。因此，这些条目、数据点或观察结果在本文中被称为“时间序列数据”。可以使用通用格式将数据存储在节点108的数据存储区中，所述通用格式包括例如支持可扩展存储、流传输数据和低延时查询的架构(schema)。

[0082] 在实施例中，所述架构可以包括在每行中存储多个观察结果，以及使用具有定制哈希的行密钥来对所述行中的数据进行过滤。在实施例中，所述哈希是基于时间戳和标签的。例如，所述哈希可以是时间戳的取整值，并且所述标签可以对应于过程控制系统的事件或实体或与过程控制系统相关的事件或实体。在实施例中，对应于每行或一组行的元数据还可以与时间序列数据一起整体地或与时间序列数据分离地被存储在数据存储区M_X中。例如，可以以无架构的形式与时间序列数据分离地存储元数据。

[0083] 在实施例中，用于在装置数据存储装置M_X处存储数据的架构在大数据存储装置102和节点108的至少一个上是通用的。因此，在该实施例中，当将数据从节点的本地存储区M_X通过主干网105传送到过程控制系统大数据装置数据存储装置120时维持该架构。

[0084] 再次参照图1，并且如以上所讨论的，本文中公开的技术、方法、系统和设备允许确认设备或部件18、20、22对过程工厂10安全，和/或允许确认设备或部件18、20、22安全地访问工厂10的过程控制网络(例如，网络12、15中的至少一个)，使得设备或部件18、20、22如预期或指定的被安全地包括在过程控制系统或过程工厂10中或与过程控制系统或过程工厂10一起利用。为了说明，图5A描绘了确认诸如过程控制工厂10的过程控制工厂的设备安全的范例方法200。方法200可以用于例如确认设备(例如，“目标”设备)安全并安全地与过程工厂10中的另一设备通信。额外地或备选地，方法200可以用于确认目标设备无危险地和安

全地与过程工厂网络12、15进行通信，例如与网络12、15中包括的一个或多个设备进行通信。目标设备可以是例如设备18、20、22中的一个。在一些情况下，方法200的至少一部分由设备18、20、22中的一个或另一设备执行。在实施例中，设备18、20、22中的一个的处理器执行存储在设备18、20、22的存储器上的计算机可执行指令组，并且对所述指令的执行使得设备18、20、22执行方法200的至少一部分。为了便于讨论，下面同时参考图1至4来讨论方法200，然而该讨论并不是限制性的。

[0085] 方法200包括确定目标设备18、20、22所处的环境、区域或场所的一组当前条件、特性和/或属性、和/或确定目标设备其自身的一组当前条件、特性和/或属性(框202)。例如，在出于在过程工厂10中进行实时操作的目的而初始化或启动目标设备18、20、22后，并且在目标设备18、20、22出于在过程工厂10中进行实时操作的目的而与任何其他设备进行通信之前(例如，在与其他任何设备通信以对设备18、20、22进行配置和/或对数据进行发送或接收以使得过程被控制之前)，目标设备18、20、22检测或确定其自身的一组当前条件、特性、或属性、和/或目标设备18、20、22在初始化或启动之后发现其自身所处的环境的一组当前条件、特性、或属性。即，在初始化或启动之后并且在目标设备18、20、22执行目标设备18、20、22的所要求的任何动作使得目标设备18、20、22可以在过程在过程工厂10中被控制的同时操作之前，目标设备18、20、22检测或确定其自身的一组当前条件或属性、和/或目标设备18、20、22当前所处的环境的一组当前条件或属性。一般地，目标设备18、20、22在没有与过程工厂10中的任何其他设备进行通信的情况下执行所述检测和/或确定，然而，在一些情况下，目标设备18、20、22可以与不知道或没有意识到过程工厂10的另一设备进行通信。例如，目标设备18、20、22可与GPS卫星通信以确定其地理空间位置。然而，一些目标设备18、20、22可以完全不与任何其他设备进行通信以执行对当前条件、特性和/或属性的检测和/或确定。

[0086] 如之前所讨论的，所述一组当前条件、特性和/或属性通常描述或指示目标设备18、20、22其自身和/或目标设备18、20、22所处的环境。例如，目标设备18、20、22和/或其当前环境的当前条件或属性可以是目标设备18、20、22的地理空间位置(其可以例如通过在目标设备18、20、22上包括的GPS收发机来确定)。当前条件或属性的其他范例包括时间和/或日期(例如，为了在过程工厂10中进行实时操作对设备10的初始化/启动的时间和/或日期)和设备18、20、22在初始化/启动后所处的过程工厂10的具体区域。当前条件/属性的进一步的其他范例包括设备的用户的标识、利用其操作设备的过程工厂10的标识、操作过程工厂10的组织实体(通常，已经获得了目标设备18、20、22和/或打算将设备用在过程工厂10中或用于过程工厂10的组织实体)的标识、和/或诸如过程工厂10所处于的县、州、省或国家的管辖区域的标识。当前条件/属性的进一步范例包括设备的类型(例如，控制器、I/O卡、智能现场设备、路由器、网关、接入点、平板电脑、笔记本电脑、诊断监视器等)、设备的制造商、设备的模型、以及在目标设备18、20、22在过程工厂10中操作的同时要由设备18、20、22传送的实时数据的类型。通常，目标设备18、20、22通过操作目标设备18、20、22的部件(例如，GPS收发机、高度计、陀螺仪、用户登录机制等)和/或通过读取存储在目标设备18、20、22的存储器中的数据来确定其自身和/或其当前环境的一组当前条件/属性。

[0087] 方法200包括确定对应于目标设备18、20、22和/或其当前位置的一组当前条件或属性是否遵从或符合为了目标设备18、20、22能够访问过程控制网络12、15或访问其他设备

必需要满足或要呈现的一组条件或属性(框205)。暂时忽略(如由虚线指示的)任选框212和215,如果在框205处一组当前条件或属性遵从所述一组必需的条件或属性,则目标设备18、20、22被认为是安全的并且被允许访问过程控制网络或网络12、15或其他设备(框208)。因此,确认安全的设备18、20、22可以继续在工厂10操作以控制过程的同时在过程工厂10内实时操作。例如,确认安全的设备18、20、22可以与过程工厂10中的另一设备通信;确认安全的设备18、20、22可以使用或通过网络12、15中的至少一个进行通信;确认安全的设备18、20、22可以从与过程工厂10相关联的另一设备接收并实例化规定其实时操作行为的配置;确认安全的设备18、20、22可以对实时数据进行发送或接收以使过程被控制;等等。在实施例中,对由确认安全的设备18、20、22向其他设备或经由网络12、15中的一个或多个发送的通信中的一些或全部进行加密(框218)。例如,对过程数据进行加密和/或对其他数据进行加密。

[0088] 在框205处,如果一组当前条件或属性不遵从或不符合所述一组必需的条件或属性,则不允许(例如,拒绝或阻止)目标设备18、20、22访问过程控制网络或网络12、15或其他设备(框210)。即,设备18、20、22被确定为不安全的或未处于其想要被使用的环境中。因此,设备18、20、22通过不经由过程控制网络12、15中的任何网络或向其他设备发送任何通信、并且具体地通过避免与网络12、15中的任何节点或与其他设备进行通信,来将其自身与过程工厂10隔离。如果设备18、20、22包括集成用户接口、则设备18、20、22可以在其上指示其非遵从性。额外地或备选地,设备18、20、22可以经由不是诸如蜂窝通信网络或其他私有或公共计算网络的过程控制网络12、15中的一个的网络来指示其非遵从性。

[0089] 在实施例中,一组必需的条件和/或属性的指示被配备到或被存储在目标设备18、20、22的存储器(例如,非易失性存储器)中。例如,所述一组必需的条件或属性可以被配备在工厂、在制造站点、在分级站点、或在目标设备18、20、22被初始化或被启动以用于在过程工厂10的实时操作期间使用之前的任何位置或时间。可以使用任何已知和/或合适的技术来执行对所述一组条件和/或属性的配备,例如通过在制造期间配备所述一组条件和/或属性、使用外部工具配备、和/或使用证书配备。

[0090] 在一些情况下,在被配备到目标设备18、20、22中的密钥中包括所述一组条件和/或属性,所述密钥例如被利用于将设备18、20、22与过程工厂10的一个或多个网络和/或包括在过程工厂10中的设备进行认证的密钥。在实施例中,根据种子和密钥生成数据的组合来生成被配备到设备18、20、22中的密钥,其中,所述密钥生成数据指示为了允许设备18、20、22访问过程工厂的一个或多个网络而必需的对应于目标设备18、20、22和/或目标设备18、20、22可以处于的环境的一组条件、特性和/或属性。例如,种子是随机或伪随机生成数,和/或种子是基于设备标识符(例如,HART或无线HART设备ID)的;并且密钥生成数据是位映像、数组、一组值、代码、到其他数据的一个或多个指针、或指示一组必需的条件、特性和/或属性的任何其他合适的数据排列。

[0091] 此外,可以通过将种子和密钥生成数据以任何合适的方式组合来产生种子和密钥生成数据的组合。例如,种子和密钥生成数据可以被串联、使用函数被组合、和/或使其相应的位和/或字节的至少一部分相互交织以形成组合。对种子和密钥生成数据的组合(例如,作为一个整体或整体地)进行操作以生成被配备到设备18、20、22中的密钥。使用对种子和密钥生成数据的组合进行操作的任何合适或已知的密钥生成算法或函数来执行密钥生成。例如,公共密钥生成算法、对称密钥生成算法、密码哈希函数、分布式密钥生成算法和/或其

他合适或已知的密钥生成算法可以被应用到组合的种子和密钥生成数据。如果期望，方法200包括对由密钥生成算法生成的密钥进行加密来形成已加密密钥。可以使用任何合适或已知的加密技术、算法或函数来进行加密，例如公钥加密算法、对称密钥加密算法、PGP(良好隐私)加密算法、和/或任何其他合适或已知的加密算法、功能或技术。在一些情况下，密钥生成技术和加密技术是被应用到种子和密钥生成数据的组合的整体技术。

[0092] 此外，可以与本文中描述的技术一起利用的一些加密技术或算法可以基于密钥或消息的内容来生成消息完整性代码(MIC)、校验和、或可以被附加到或被包含到密钥或消息中的其他类型的验证码。这样的加密技术的范例是用于在无线HART协议中使用的加密算法。这样的MIC、校验和、或其他类型的验证码可以用于验证或确定消息/密钥的内容是否在传输期间被修改过。例如，已加密密钥的接收机可以应用由发送机使用的相同的方法或算法来生成MIC码，而接收机可以将其生成的MIC码与消息/密钥中嵌入的MIC码进行比较。当使用这样的加密算法其自身或附加其他加密算法时，可以在已加密密钥的主机设备与过程工厂10中的对等设备之间交换的消息中包含得到的MIC码以提供额外的安全性。

[0093] 在一些情形中，一个或多个子密钥还被配备到设备18、20、22中。众所周知，子密钥基于密钥、源自于密钥、绑定于密钥、取决于密钥、和/或以其他方式与密钥相关联。可以以与以上描述的密钥生成技术类似的方式基于子密钥生成数据来生成与密钥相关联的子密钥。例如，可以基于种子和子密钥生成数据的组合来生成子密钥。关于本文中描述的技术，通常子密钥生成数据和密钥生成数据是指示相应的不同的必需的条件/属性的不同的数据。在一些情形中，子密钥表示与密钥相关联的一个或多个条件中的另一限制条件或属性(例如，子条件或子属性)。例如，针对特定密钥的密钥生成数据可以指示设备由过程工厂操作公司XYZ使用的必需的条件，而针对与该特定密钥相关联的子密钥的子密钥生成数据可以指示设备在由操作公司XYZ操作的过程工厂#123中使用的必需的条件。此外，不同方或组织实体可以单独地定义密钥生成数据和子密钥生成数据。例如，设备18、20、22的提供者或供应商可以定义“过程工厂操作公司XYZ”作为密钥生成数据，而过程工厂操作公司XYZ则可以定义“过程工厂#123”作为子密钥生成数据。与密钥类似，可以例如通过使用与相关的密钥利用的加密算法相同或不同的加密算法对子密钥进行加密或不加密。在一些情形中，子密钥的提供者允许另一方访问一些子密钥而同时拒绝其他方访问其他子密钥。例如，操作公司XYZ可以启用或禁用设备18、20、22的制造商访问选定的子密钥的能力，即使制造商提供了根据其定义该选定的子密钥的密钥。

[0094] 因此，在方法200的框205的一些实施例中，确定对应于目标设备18、20、22和/或其当前位置的一组当前条件/属性是否遵从或符合所述一组必需的条件/数据包括使用已经被配备到设备18、20、22中的密钥和任何子密钥来做出所述确定。在实施例中，所配备的密钥和一个或多个子密钥(如果存在的话)被“逆向加工”或以其他方式被解构以确定根据其生成所配备的密钥的密钥生成数据并且如果适用的话确定根据其生成所配备的子密钥的子密钥生成数据。例如，为了恢复密钥生成数据，首先对所配备的密钥执行对密钥生成算法的逆向，并且之后解构所述结果(例如，使用用于组合种子和密钥生成数据的函数的逆向来解组合所述结果)以恢复种子和密钥生成数据。在另一范例中，可以对配备的密钥或子密钥应用函数或其他算法来确定、提取或恢复密钥或子密钥生成数据。因为所恢复的密钥生成数据和(如果适用的话)子密钥生成数据指示设备18、20、22访问过程控制网络12、15的必需

的条件/属性，所以通过将由所恢复的密钥和子密钥生成数据指示的必需的条件/属性与当前的条件/属性进行比较来确定是否允许设备18、20、22访问过程控制网络12、15(框205)。

[0095] 本文中描述的技术、方法和装置不仅能够允许确认设备对过程工厂及其网络安全，而且额外地或备选地允许确认设备仅在特定情形或条件期间对特定过程工厂安全以减轻盗窃、滥用、恶意使用、工厂攻破、失去对过程的控制、诸如爆炸、火灾的灾难事件的发生、和/或设备和/或人身生命的损失。下面提供若干范例情形来说明所述技术的用途和优点。

[0096] 在第一范例中，第一组现场设备由其制造商或供应商配备有指示设备将仅用于供应商的特定客户，例如石油公司A的密钥。同样，其他组的现场设备被配备有对其相应的客户，例如，纸质产品制造商B、粘合剂制造商C等的指示。因此，通过使用本文中描述的技术中的至少一部分，仅允许每个现场设备与其相应的公司的过程控制网络进行通信，例如，为石油公司A配备的现场设备将被禁止访问纸质产品制造商B的过程控制网络并被禁止在纸质产品制造商B的过程工厂中使用，即使该现场设备是期望的构造或模型。因此，设备制造商能够控制不期望或非法的再销售或在实体之间对设备的转移。更重要的是，如果被配备用于在合法客户的网络中使用的设备被对设备的使用具有恶意意图的实体或一方所偷窃，或所述配备的设备是非法销售给恶意方的，则所述设备被禁止在恶意方的过程网络中操作。例如，出于邪恶的目的期望制造爆炸材料的非法组织将不能够使用已经被配备用于仅在粘合剂制造商C的网络中使用的设备。

[0097] 在本技术的另一范例中，过程控制系统提供者，例如石油公司A为诊断工具配备子密钥生成数据，该子密钥生成数据指示允许使用诊断工具的时间和地点。例如，子密钥生成数据可以指示仅允许诊断设备在周末的凌晨2点到5点的几个小时期间访问网络以对过程工厂的特定区域执行诊断，并且可以指示在过程工厂的其他区域中允许诊断设备在任何时间访问网络。

[0098] 在又一范例中，石油公司A将特定过程控制设备配备为仅在特定的位置中使用。因此，如果过程控制设备被无意中运输到对于安装来说不正确的位置，则过程控制设备被禁止在不正确的位置访问网络并且因此防止了对设备的潜在滥用。

[0099] 在又一范例中，石油公司A提供并配备笔记本电脑或计算设备以供操作者使用。使用子密钥生成数据，石油公司A指定不同的子密钥以自动地定义和确认所述笔记本电脑可以在何时、何地、由何人用于访问石油公司A的各个过程控制网络和工厂。例如，石油公司A可以使用子密钥生成数据来指定当用户1144登录到笔记本电脑以连接到油井设备N的网络时，允许笔记本电脑允许无线连接到油井设备N的网络。然而，如果用户1144转而尝试连接另一油井设备的网络，则访问可以被拒绝。

[0100] 如之前所讨论的，除了被用于指示允许设备18、20、22访问过程工厂的一个或多个网络和/或与特定设备进行通信必需的一个或多个条件和/或属性之外，配备到设备18、20、22中的密钥和/或子密钥可以用于将设备18、20、22与一个或多个过程控制网络或包括在过程控制工厂中的特定设备进行认证。例如，对于其中使用证书来完成对设备的配备的实施例，证书授权机构或代理(CA)管理公共/私有密钥对和可用于验证指示访问过程控制网络的期望的各个设备的标识的证书。在一些情况下，设备的供应商或提供者(例如，爱默生过程管理)作为其设备的CA，并且制造商、过程控制系统操作实体和设备供应商的其他下游客户可以根据需要从设备供应商请求许多公共/私有密钥对。如上所述，基于密钥生成数据，

密钥对可以与单个设备18、20、22相关联或者可以与一组设备或商品(例如,特定类型的设备、特定的一群人(例如,通过角色、权限、工作组等进行划分)、特定的工厂位置或站点、特定位置或站点的特定区域、特定的制造商或客户等)相关联。因此,设备供应商能够利用适当的密钥对来对开箱即用的设备进行预配置,该密钥对通常被包含在由设备供应商(或由指定的CA)发布的证书中。密钥对被呈现以用于确认设备在设备的配备阶段期间,例如在设备已经离开供应商之后并且在设备被初始化以用于与接收所述设备的客户(例如,过程工厂操作实体)的过程工厂一起实时使用之前的特定时间点上安全。此外,以类似的方式,设备供应商的下游客户(例如制造商、操作实体或设备供应商的其他下游客户的过程控制系统等)可以作为与设备供应商密钥相关联的子密钥和与其对应的证书的本地CA。本地CA定义并提供与由设备供应商提供的密钥相关联的子密钥来如期望地管理在其过程工厂和场所中的安全确认、资产跟踪、风险等。然而,可以禁止本地CA修改或访问由设备供应商提供的任何密钥或信息。

[0101] 因此,现在返回到方法200和任选的框212、215,在一些实施例中,在确定目标设备18、20、22遵从访问必需的条件和/或属性之后(例如,框205的“是”分支),则方法200包括尝试将目标设备18、20、22与过程控制网络12、15或其他设备进行认证(框212)。例如,设备18、20、22通过利用对应于设备18、20、22的相应的密钥的证书来尝试与网络12、15中的至少一个或其他设备进行认证以例如用于证书交换。在一些情况下,设备18、20、22尝试通过利用对应于设备18、20、22的相应的子密钥的证书进行认证。

[0102] 对目标设备18、20、22进行认证(图5A的框212)的范例实施例被示出在图5B中。图5B包括将目标设备与另一设备或网络(例如,将目标设备与期望与其无危险和安全地通信的另一过程工厂设备或网络进行认证)进行认证的范例方法220的流程图。在图5B中,将目标设备与其他设备或网络进行认证包括请求对应于其他设备或网络的证书222和接收所请求的证书。一般地,接收到的证书证明目标设备18、20、22期望与其进行认证的其他设备或网络的有效性。例如,接收到的证书可以通过提供密钥的数字签名和任选的其他信息来证明其他设备或网络与用于加密和/或解密数据的密钥(例如,公共密钥)的绑定。在一些情况下,公共密钥被包含在证书中。证书可以已经由证书或证明机构(CA)发布到其他设备或网络。CA可以由过程工厂10提供、可以由过程工厂所属的企业提供、和/或可以是公共CA。

[0103] 在框225处,方法220包括初始化或发起会话,经由该会话目标设备和其他设备或网络用于确认安全地进行通信,例如,安全或确认安全的会话。在范例中,在目标设备与其他设备或网络之间的套接字层或其他合适的传输层或低级通信层来执行对会话的初始化225,然而,在一些情况下,在套接字或传输层以上或以下的通信层执行对双方(例如,目标设备18、20、22与网络12、15的其他设备或节点)之间的会话的初始化225。

[0104] 在实施例中,对双方之间的会话225初始化包括生成用于特定会话的私有密钥228。通常,私有密钥是对于该特定会话唯一的,并且在目标设备与其他设备或网络之间共享。在范例中,由目标设备例如以之前所讨论的方式基于对应于专用于目标设备其自身的数据的种子来生成私有密钥228。在一些情形中,对会话225初始化包括例如以之前所讨论的方式生成一个或多个私有子密钥。每个私有子密钥可以是对特定会话唯一的,并且可以在目标设备与其他设备或网络节点之间共享子密钥中的一个或多个。

[0105] 额外地或备选地,在一些情形中,对双方之间的会话225初始化包括确定或建立要

在会话期间使用的一种或多种加密技术或方法230。例如，目标设备基于由接收到的证书指示的公共密钥、基于所生成的私有密钥、和/或基于所生成的子密钥来确定或建立一种或多种加密技术或方法230。在一些情形中，特定技术用于加密，而不同的技术用于解密。

[0106] 要注意的是，尽管在图5B中，发起会话225包括生成私有密钥和/或子密钥228和确定(一种或多种)加密技术230两者，但是在一些实施例中，框228、230中的一个或两者被省略。例如，如果在目标设备与其他设备或网络之间利用对称密钥交换，则省略框228，因为仅交换与证书相关联的公共密钥。

[0107] 在框232处，方法200包括例如基于所生成的密钥和/或所确定的加密技术来在目标设备与其他设备之间或目标设备与过程工厂的网络12、15之间建立初始化的会话。会话可以是安全或确认安全的会话，经由该会话数据和通信可以在目标设备与其他设备或网络12、15之间安全地发送和接收。在一些情形中，可以利用该安全会话来管理服务质量(QoS)。例如，如果通过该安全会话通信多个不同类型的数据(例如，过程控制大数据、过程控制非大数据、移动控制室功能、网络管理数据等)，该会话管理不同类型的数据中的每个的QoS。

[0108] 在范例中，例如当特定用户使用用户接口设备20(例如，利用登录或其他访问证书)时，会话对于目标设备的用户是特定的。其中可以确认用户对会话安全的范例情形被提供在前面提到的题目为“METHOD FOR INITIATING OR RESUMING A MOBILE CONTROL SESSION IN A PROCESS PLANT”的美国专利申请No.14/028,913和题目为“METHOD FOR INITIATING OR RESUMING A MOBILE CONTROL SESSION IN A PROCESS PLANT”的美国专利申请No.14/028,921中。在这些情形中，经由用户接口设备20，将用户与过程控制网络12、15进行认证使得例如当(例如，由图2中的工作站34所支持的)传统的用户控制应用程序和功能代替地被支持在移动计算设备20上时，建立针对用户的安全会话以用于移动控制室应用程序。例如，用户使用移动用户接口设备20(例如，通过在移动用户接口设备20上登录或认证)来建立与过程控制网络12、15的安全会话。随着用户来回移动(例如，随着用户从过程工厂的一个区域移动到过程工厂的另一区域使得移动设备20在网络节点之间切换，或随着用户在远程位置来回移动)，对应于用户的安全会话被维持使得用户可以连续地且无缝地执行移动控制室任务。例如当用户在物理控制室中的静态工作站处初始地建立特定安全会话时，用户甚至可以在多个设备上维持所建立的安全会话并且之后将他或她的所建立的特定安全会话传递到平板电脑使得用户可以进入过程工厂现场并且经由所述平板电脑随着用户在工厂10周围移动来继续他或她的工作。

[0109] 在另一范例情形中，确认会话对特定设备而非过程控制网络安全，例如如在前面提到的题目为“METHOD AND APPARATUS FOR CONTROLLING A PROCESS PLANT WITH LOCATION AWARE MOBILE CONTROL DEVICES”的美国专利申请No.13/028,897、题目为“METHOD AND APPARATUS FOR CONTROLLING A PROCESS PLANT WITH LOCATION AWARE MOBILE CONTROL DEVICES”的美国专利申请No.14/028,785、题目为“MOBILE CONTROL ROOM WITH REAL-TIME ENVIRONMENT AWARENESS”的美国专利申请No.14/028,964和题目为“METHOD AND APPARATUS FOR DETERMINING THE POSITION OF A MOBILE CONTROL DEVICE IN A PROCESS PLANT”的美国专利申请No.14/028,923中所描述的。例如，移动诊断设备(其可以是用户接口设备20或其他设备22)移动到与现场设备接近的区域，并且基于所述设备的接近度来建立与现场设备的安全会话以从现场设备接收数据以用于例如经由用户接口

应用程序或经由无监督式应用程序在诊断中使用。在数据已经被传递之后，安全会话可以被安全地和确认安全地终止，并且移动诊断设备可以被移动到与不同的现场设备接近以从所述不同的现场设备收集数据。在另一范例中，将现场设备与过程工厂的集中式和/或分布式大数据装置或过程工厂的企业的大数据装置进行认证使得该现场设备可以安全地流传输大数据以用于历史记录。

[0110] 返回图5A的框212并尝试设备认证，当然，使用如以上针对方法220所描述的证书和密钥仅仅是可以用于将设备18、20、22与另一设备或与过程控制网络12、15中的至少一个进行认证的许多技术之一。额外地或备选地，可以使用用于设备认证(框212)的其他合适的技术。

[0111] 继续到框215，如果对设备18、20、22的认证是成功的，则设备18、20、22被认为是确认对过程工厂10安全的和被认证的，并且因此，设备18、20、22可以在工厂10操作以控制过程(208)的同时继续在过程工厂10内部实时操作。在确认安全的设备18、20、22被确认对过程工厂网络12、15安全的实施例中，确认安全的设备18、20、22维持其确认安全的状态，同时在网络12、15的不同节点上和在网络12、15的不同节点之间进行通信。例如，如果确认安全的设备18、20、22是移动设备，则确认安全的设备可以在过程工厂内部移动并且使用相同的确认安全的会话来切换从网络12、15的一个节点到网络12、15的另一节点的通信。

[0112] 在实施例中，成功认证的设备18、20、22对到其他设备或到设备18、20、22已成功地与其进行认证的工厂10的网络12、15的一些或所有通信进行加密(框218)。例如，已认证的设备18、20、22使用在图5B的框230处确定的一种或多种加密技术或方法来对过程控制数据进行加密(并且在一些情况下，还对非过程控制数据或所有发送的数据进行加密)。

[0113] 此外，对于利用验证或证实与其通信的消息内容的通信协议的已认证的设备18、20、22，方法200提供额外的安全层或安全程度。为了说明，考虑使用包括用于证实或验证每个消息或一组消息的内容的校验码和或其他消息内容完整性代码的协议与另一设备或网络12、15的节点进行通信的范例设备18、20、22。例如，范例设备18、20、22可以(至少部分)使用无线HART协议进行通信，这允许消息包括消息完整性代码(MIC)字段，通过该消息完整性码字段，消息内容被验证、被证实或被确认安全。因此，对于这样的设备18、20、22，不仅仅是设备18、20、22其自身(例如经由方法200和/或方法220)被确认对其他设备或网络12、15安全，而且由确认安全的设备18、20、22发送的消息也可以自身确认安全。在范例中，对到/来自确认安全的设备18、20、22的通信的加密(框218)导致对包含在所述通信中的校验码或消息完整性码的加密。即，设备其自身和由设备发送的消息两者均基于相同的密钥(例如，在框228处生成的私有密钥)被加密。在另一范例中，设备其自身和由该设备发送的消息基于不同的密钥被加密。例如，可以通过公钥或私有密钥来确认设备其自身安全，而可以通过私有子密钥来确认由该设备发送的消息内容安全，例如包括校验码和或消息完整性代码的消息可以基于私有子密钥而被特别地编码。在任何情况下，对于利用被构造为证实或验证消息内容的通信协议的已认证设备18、20、22，方法200可以提供多个安全层或安全级别，例如，对设备18、20、22其自身的安全确认、证实或验证以及对由设备18、20、22发送的消息的内容的安全确认、证实或验证。

[0114] 现在返回图5A的框215，当对设备18、20、22的认证不成功时，例如，如之前所讨论的，设备18、20、22保持与过程控制网络12、15和/或与其他设备隔离(框210)。如果设备18、

20、22包括集成用户接口，则设备18、20、22可以在其上指示其认证不成功。额外地或备选地，设备18、20、22可以经由未与过程控制网络12、15通信连接的诸如蜂窝通信网络的网络来指示其认证不成功。

[0115] 在确认设备对过程工厂安全的方法200的一些实施例中，在不对设备进行认证的情况下利用消息内容级别的安全确认，例如，省略框212、215。在这样的实施例中，设备18、20、22不对其他设备或网络12、15进行认证(例如，不在套接字层建立安全会话)，而是利用存储在设备18、20、22处的必需的条件的指示来对由设备18、20、22发送的消息、通信或其部分进行加密。例如，密钥(在一些情况下，一个或多个子密钥)被配备到设备18、20、22中，其中，例如以诸如之前所讨论的方式，密钥/子密钥基于指示为了设备18、20、22与过程工厂10进行通信必需的一组必需的条件和/或属性的数据。所配备的密钥或子密钥由设备18、20、22利用作为对由设备18、20、22发送到过程工厂10的一些或所有消息进行加密的基础。因此，使用基于所配备的密钥或子密钥的加密技术对(例如，包含在由设备18、20、22发送的消息中和用于验证由设备18、20、22发送的特定消息的内容的)校验码和或其他合适的消息内容完整性代码进行加密。因此，在不提供设备级别的认证的情况下提供消息级别的安全确认。这样的消息级别的安全确认技术特别适于确认低层设备，例如智能现场设备和其他类型的硬件提供者设备18。

[0116] 进一步参考图5A的方法200和图5B的方法220，用于确认设备对另一设备或对过程控制网络安全的技术中的一些或所有容易被应用以安全地和友好地终止在先前确认安全的设备与其他设备或与过程控制网络之间的通信。例如，当设备需要暂时下线以用于维护或转移以在另一位置使用时，或当确认安全的设备将要永久地退出服务时，确认安全的设备可以安全地并友好地从其他设备或从已经确认设备对其安全的过程控制网络脱离。对安全设备的这样的安全终止可以是主动的或被动的。例如，为了主动地终止确认安全的设备的访问，用于对设备进行认证的证书可以例如由CA撤回。为了被动地终止确认安全的设备的访问，确认安全的设备可以在(例如，如在图5A的框202处确定的)当前条件和/或属性不再满足必需的条件和/或属性时将其自身隔离(框210)。例如，设备可以被配置有将密钥管控为仅在预定的时间段内有效的属性。

[0117] 现在转到图6，图6描绘了用于确认用于与过程工厂一起使用的设备安全的方法250，例如用于确认图1的设备18、20、22中的一个安全的方法250。例如，范例方法250可以用于确认旨在用于与过程工厂一起使用并且因此可以访问过程工厂的一个或多个网络的过程控制设备或用户接口设备安全。在实施例中，计算设备包括在其上存储指令的存储器，该指令当由处理器执行时，使得计算设备执行方法250中的至少一些部分。此外，在一些情况下，可以联合图5A的方法200和/或图5B的方法220来执行方法250。为了便于讨论，下面同时参考图1-5A和5B来讨论方法250，然而该讨论不是限制性的。

[0118] 在框252处，方法250包括确定用于生成用于由期望被确认安全的诸如设备18、20、22中的一个的目标设备的设备所使用的密钥的种子。种子包括数字，所述数字可以是任何期望长度的随机生成数或伪随机生成数。额外地或备选地，种子可以包括指示对诸如HART或无线HART设备类型和/或设备ID编号的设备的标识的数字。

[0119] 在框255处，方法250包括确定密钥生成数据。如之前所讨论的，密钥生成数据指示必须在允许设备访问过程控制网络之前，例如，在确认设备对过程控制网络安全之前必须

满足的一组必需的条件。即，所述一组必需的条件必须在允许设备被配置用于其在过程工厂中的具体用途之前、在允许设备在过程工厂实时操作以控制过程的同时联合过程工厂进行操作之前、和/或在允许设备与包括在过程工厂中的过程控制网络的任何节点进行通信之前被满足。所述一组必需的条件可以指示设备出于联合过程工厂操作的目的而所处的环境的属性或特性。额外地或备选地，所述一组必需的条件可以指示设备其自身的与设备的位置或环境无关的属性。

[0120] 方法250还包括根据种子和密钥生成数据来生成密钥(框258)。例如，如之前所讨论的，种子和密钥生成数据可以被组合到整体单元或字符串中，并且密钥生成算法被应用到该整体单元或字符串以生成该密钥。在一些实施例中，方法250包括对初始未加密的生成的密钥进行加密以形成已加密密钥(框260)。框258和260可以单独执行或可以如期望地整体执行。在一些情况下，框260被省略，并且在这些情况下，初始生成(框258)的密钥保持未加密。

[0121] 在框262处，方法250包括使得设备被配备有密钥(其可以是加密的或未加密的)，例如使得该密钥被存储在设备的非易失性存储器中。可以在设备被配置用于其在过程工厂中的特定用途之前、在允许设备在过程工厂实时操作以控制过程(例如，通过发送和/或接收使过程被控制的实时数据)的同时联合过程工厂进行操作之前、和/或在允许设备与包含在过程工厂中的过程控制网络的任何节点进行通信之前的任何时间为设备配备所生成的密钥(框262)。例如，设备可以由设备供应商、设备制造商、或由过程控制系统提供者配备在例如设备要在其中进行操作的过程工厂中的分级区域。此外，可以使用任何期望或已知的配备技术来执行为设备配备所生成的密钥(框262)，例如在制造时将密钥存储到设备存储器中、使用工具将密钥存储到设备存储器中、或者在证书交换之后存储密钥。

[0122] 在任选框252处，方法250包括生成与密钥相关联的子密钥。在实施例中，生成与密钥相关联的子密钥(框265)包括确定用于生成子密钥的种子(其可以是或可以不是与用于生成与该子密钥相关联的密钥相同的种子)，并且包括确定子密钥生成数据(其通常，但不必需，与密钥生成数据不同)。子密钥种子和子密钥生成数据可以被组合，并且可以例如通过使用任何期望的密钥生成技术根据所述一组合来生成子密钥。如果期望，可以对初始生成的子密钥进行加密。

[0123] 在另一任选框268处，使得所生成的子密钥(无论加密或不加密)被配备到设备中。以与所讨论的为设备配备密钥(框260)类似的方式为设备配备子密钥(框268)。

[0124] 图7示出了可以被包括在图1的设备18、20、22中或可以联合过程工厂10使用的计算设备302的简化框图。尽管设备302被示出为计算设备，但是关于设备302所讨论的原理可以等同地应用到可以支持本公开内容中的技术、方法和系统的其他设备，包括但不限于，过程控制器、I/O卡、智能现场设备、路由器、接入点、网关、过程工厂大数据节点、蜂窝电话、智能电话和平板电脑等。在范例中，设备302执行方法200中的至少一部分。在范例中，设备302执行方法250的至少一部分。

[0125] 计算设备302可以包括用于执行计算机可执行指令的处理器305(在一些实施例中，可以被称为微控制器或微处理器)和用于永久地存储与计算机可执行指令相关的数据的程序或非易失性存储器308。例如，如果该设备302是设备18、20、22中的一个，则非易失性存储器308存储密钥，并且非易失性存储器308可以存储零个或多个密钥。

[0126] 设备302额外地包括用于暂时存储与计算机可执行指令相关的数据的随机存取存储器(RAM)310和输入/输出(I/O)电路312,其全部可以经由地址/数据总线315相互连接。

[0127] 应当认识到,尽管仅仅示出了一个处理器305,但是计算设备302可以包括多个处理器305。类似地,计算设备302的存储器可以包括多个RAM310和多个程序或非易失性存储器308。(一个或多个)RAM 310和程序存储器308可以被实施为例如一个或多个半导体存储器、磁性可读存储器、光学可读存储器、生物存储器和/或有形的非暂态计算机可读存储介质。额外地,尽管I/O电路312被示出为单个框,但是应当认识到I/O电路312可以包括多个不同类型的I/O电路。例如,第一I/O电路可以对应于显示设备318,并且第一I/O电路或第二I/O电路可以对应于用户接口320。用户接口320可以是例如键盘、鼠标、触摸屏、语音激活设备和/或任何其他已知的用户设备。在一些实施例中,显示设备318和用户接口320可以联合地被并入到单个物理设备中。在一些实施例中,例如,当计算设备302被实施在特定类型的过程控制设备中时,计算设备302不包括显示设备318和/或不包括用户接口320。在一些实施例中,计算设备302包括对通用计算设备通用的其他元件。

[0128] 计算设备302包括到一个或多个链接325的一个或多个网络或通信接口324,经由一个或多个链接325设备302可以连接到一个或多个网络322(例如,图1的过程控制网络12、15中的一个或多个)。在一些实施例中,不同的通信接口324利用不同的通信协议。链接325可以简单地是存储器接入功能或网络连接,和/或链接325可以是有线连接、无线连接、或多级连接。许多类型的链接在联网技术中是已知的并且可以联合计算设备302一起使用。在一些实施例中,显示设备318或用户接口320中的至少一个可以使用网络322和链接325被远程连接到计算设备302。

[0129] 此外,计算设备302可以经由一个或多个网络322与多个其他设备335a-335n通信连接。其他设备335a-335n可以包括例如图1的设备18、20、22中的一个或多个。尽管未示出,但是其他设备335a-335n分别还可以包括通常在通用计算设备中找到的并且与计算设备302类似的元件,例如存储器、处理器、RAM、总线、显示器、用户接口、网络接口和其他元件。

[0130] 更进一步地,计算设备302可以包括存储在其上的一组或多组计算机可执行指令340。如本文所使用的,术语“计算机可执行指令”、“计算机可运行指令”和“指令”可以互换使用。指令340可以被存储在存储器308上并且能够由处理器305执行以执行本文中描述的方法的任何部分,例如图5A的方法200、图5B的方法220和/或图6的方法250。

[0131] 本公开内容中描述的技术的实施例可以单独或组合地包括任何数量的以下方面:

[0132] 1、一种用于在过程控制工厂中使用的过程控制设备,所述过程控制设备包括:处理器;非易失性存储器,其存储指示允许所述过程控制设备使用所述过程控制工厂的网络与另一设备进行通信所需要的一组必需的属性的数据,其中,所述一组必需的属性描述允许所述过程控制设备与所述另一设备进行通信的环境;以及计算机可执行指令,其存储在所述过程控制设备的所述非易失性存储器上或另一存储器上。所述计算机可执行指令可以在启动所述过程控制设备之后并且在所述过程控制设备与任何其他设备进行通信之前能够由所述处理器执行以进行以下中的至少一项:(i)对所述过程控制设备进行配置,或者(ii)对用于控制所述过程控制工厂中的过程的数据进行发送或接收中的至少一项。具体地,所述计算机可执行指令当由所述处理器执行时,可以使得所述过程控制设备:确定所述过程控制设备在所述启动之后所处的当前环境的一组当前属性;基于指示所述一组必需的

属性的所述数据来确定所述过程控制设备所处的当前环境的一组当前属性是否遵从所述一组必需的属性;当所述一组当前属性遵从所述一组必需的属性时,允许所述过程控制设备与所述另一设备进行通信以进行以下中的至少一项:(i)对所述过程控制设备进行配置,或者(ii)发送或接收实时数据以使得所述过程被控制中的至少一项;并且当所述一组当前属性不遵从所述一组必需的属性时,阻止所述过程控制设备与所述另一设备进行通信以进行以下中的至少一项:(i)对所述过程控制设备进行配置,或者(ii)对所述实时数据进行发送或接收来使得所述过程被控制中的至少一项。

[0133] 2、根据方面1所述的过程控制设备,还包括地理空间接收机,其中,所述计算机可执行指令还能够由所述处理器执行以使得所述过程控制设备使用所述地理空间接收机来确定过程控制设备的当前地理空间位置,并且其中,对应于所述过程控制设备所处的环境的所述一组必需的属性包括特定地理空间区域。

[0134] 3、根据方面1或方面2所述的过程控制设备,其中,所述计算机可执行指令还能够执行以使得所述过程控制设备确定当前时间,并且对应于所述过程控制设备所处的所述环境的所述一组必需的属性还包括对应于所述特定地理空间区域的特定时间间隔。

[0135] 4、根据方面1至3中的任一方面所述的过程控制设备,其中,所述非易失性存储器被配备有用于在将所述过程控制设备与所述过程控制工厂的所述网络进行认证中使用的密钥,所述密钥基于种子来生成,所述种子包括密钥生成数据和随机生成的或伪随机生成的数字,并且所述密钥生成数据指示允许所述过程控制设备使用所述过程控制工厂的所述网络与所述另一设备进行通信所需要的所述一组必需的属性。

[0136] 5、根据方面4所述的过程控制设备,其中,被配备到所述过程控制设备的所述非易失性存储器中的所述密钥是已加密密钥,通过对未加密密钥进行加密来生成所述已加密密钥,并且所述种子用于生成所述未加密密钥。

[0137] 6、根据方面4或方面5所述的过程控制设备,还包括额外的计算机可执行指令,所述额外的计算机可执行指令当由所述处理器执行时使得在已经确定所述一组当前属性遵从所述一组必需的属性之后并且在所述过程控制设备与所述另一设备进行通信以进行以下中的至少一项之前,所述过程控制设备使用被配备到所述非易失性存储器中的所述密钥与所述另一设备或与证书授权机构进行认证:(i)对所述设备进行配置,或者(ii)对所述实时数据进行发送或接收来使得所述过程被控制中的至少一项。

[0138] 7、根据前面的方面中的任一方面所述的过程控制设备,其中,所发送或所接收的实时数据的至少一部分被包含在消息的内容中,并且其中,包含在所述消息的消息完整性字段中以验证所述消息的所述内容的数据是基于所述密钥的或是基于根据所述密钥而生成的子密钥的。

[0139] 8、根据前面的方面中的任一方面所述的过程控制设备,其中,所述一组必需的属性包括以下中的至少一项:由所述过程控制设备发送的用于控制所述过程的数据的类型、由所述过程控制设备接收的用于控制所述过程的数据的类型、所述过程控制设备的制造商、所述过程控制工厂的标识、所述过程控制工厂的区域的标识、操作所述过程控制工厂的组织实体的标识、或所述过程控制工厂所处的国家的标识。

[0140] 9、根据方面8所述的过程控制设备,其中,所述一组必需的属性还包括用户的属性。

[0141] 10、根据前面的方面中的任一方面所述的过程控制设备，其中，所述过程控制设备是以下中的一个：过程控制器、现场设备、或与所述过程控制器连接的输入/输出(I/O)卡。

[0142] 11、根据前面的方面中的任一方面所述的过程控制设备，还包括将所述过程控制设备通信连接到集中式或分布式大数据装置的接口，并且其中，所述过程控制设备将所述实时数据提供到所述集中式或分布式大数据装置。

[0143] 12、一种用于确认过程控制工厂中的设备的安全的方法，所述方法包括：在计算设备处确定用于生成密钥的种子，其中，所述种子至少部分基于随机生成的或伪随机生成的数字；在所述计算设备处确定密钥生成数据，其中：所述密钥生成数据指示被配备有所述密钥的主机设备使用所述过程控制工厂的网络进行通信以进行以下中的至少一项所需要的一组必需的条件：(i)对所述主机设备进行配置，(ii)发送实时数据来使得过程在所述过程控制工厂中被控制，或者(iii)接收实时数据来使得所述过程被控制，并且所述一组必需的条件对应于所述主机设备能够处于的环境；在所述计算设备处根据所述种子和所述密钥生成数据来生成所述密钥；并且通过所述计算设备来使得过程控制设备被配备有所生成的密钥使得所配备的过程控制设备是所述主机设备，并且使得所配备的过程控制设备使用所生成的密钥并基于所述一组必需的条件与对应于所配备的过程控制设备在启动后所处的当前环境的一组当前条件的比较来与所述网络进行认证。

[0144] 13、根据方面12所述的方法，其中，确定用于生成所述密钥的所述种子包括还基于所述过程控制设备的标识来确定所述种子。

[0145] 14、根据方面12或方面13所述的方法，其中，使得所述过程控制设备被配备有所生成的密钥包括在所述过程控制设备与任何其他设备进行通信以进行以下中的任一项之前，使得所生成的密钥被存储在所述过程控制设备的非易失性存储器中：(i)对所述主机设备进行配置，(ii)发送实时数据以使得所述过程被控制，或者(iii)接收实时数据以使得所述过程被控制。

[0146] 15、根据方面12至14中的任一方面所述的方法，其中，所述一组必需的条件包括以下中的至少一个：所述主机设备的地理空间位置、所述过程控制工厂的特定时间、特定时间间隔、特定日期或日期范围、或特定区域。

[0147] 16、根据方面12至15中的任一方面所述的方法，其中，所述一组必需的条件包括以下中的至少一个：由所述主机设备发送的实时数据的类型、由所述主机设备接收的实时数据的类型、或所述主机设备的制造商。

[0148] 17、根据方面12至16中的任一方面所述的方法，其中，所述一组必需的条件包括以下中的至少一个：所述过程控制工厂的标识、操作所述过程控制工厂的组织实体的标识、或所述过程控制工厂所处的国家的标识。

[0149] 18、根据方面12至17中的任一方面所述的方法，其中：所述计算设备是第一计算设备，所述密钥是第一密钥，所述种子是第一种子，所述密钥生成数据是第一密钥生成数据，所述一组条件是第一组必需的条件，所述主机设备是第一主机设备，并且所述过程控制设备是第一过程控制设备；并且其中，所述方法还包括：确定用于生成第二密钥的第二种子，所述第二种子基于第二密钥生成数据，所述第二密钥生成数据指示第二主机设备经由所述过程控制工厂的所述网络进行通信所需要的第二组必需的条件；根据所述第二种子来生成所述第二密钥；并且使得第二设备被配备有所述第二密钥使得所述第二设备是所述第二主

机设备，并使得所配备的第二设备使用所生成的第二密钥并基于所述第二组必需的条件与对应于所配备的第二设备在启动后所处的当前环境的一组当前条件的比较来与所述网络进行认证；并且所配备的第二设备是第二过程控制设备或第二计算设备。

[0150] 19、一种用于在过程控制工厂中使用的设备，所述设备包括：处理器；以及非易失性存储器，其存储密钥和根据所述密钥导出的子密钥，其中，所述密钥是至少部分基于密钥生成数据来生成的，所述密钥生成数据指示被配备有所述密钥的主机设备与所述过程控制工厂的网络进行通信所需要的第一组必需的条件，其中，所述第一组必需的条件对应于所述主机设备能够处于的环境，所述子密钥是至少部分基于子密钥生成数据来生成的，所述子密钥生成数据指示被配备有所述子密钥的所述主机设备与所述过程控制工厂的所述网络进行通信所需要的第二组必需的条件，并且所述第二组必需的条件对应于所述主机设备能够处于的所述环境。所述设备还包括存储在所述设备的所述非易失性存储器或另一存储器上的计算机可执行指令，所述计算机可执行指令能够由处理器执行以使得所述设备：基于所述密钥或所述子密钥来确定所述设备所处的当前环境的一组当前条件是否遵从相应的一组必需的条件；当所述一组当前条件遵从相应的一组必需的条件时，允许所述设备与所述过程控制工厂的另一设备进行通信以进行以下中的至少一项：(i)对所述设备进行配置，或者(ii)对通过控制过程生成的实时数据进行发送或接收中的至少一项；并且当所述一组当前条件不遵从相应的一组必需的条件时，阻止所述过程控制设备与所述过程控制工厂的所述另一设备进行通信以进行以下中的至少一项：(i)对所述设备进行配置，或者(ii)对通过控制所述过程生成的所述实时数据进行发送或接收中的至少一项。

[0151] 20、根据方面19所述的设备，其中，所述另一设备是包括在所述过程控制工厂中的至少一个网络中的节点。

[0152] 21、根据方面19或方面20所述的设备，还包括额外的计算机可执行指令，所述额外的计算机可执行指令当由所述处理器执行时，使得所述设备确定所述设备所处的所述当前环境的所述一组当前条件。

[0153] 22、根据方面19至21中的任一方面所述的设备，还包括额外的计算机可执行指令，所述额外的计算机可执行指令当由所述处理器执行时，使得在所述设备与所述过程控制工厂的所述另一设备进行通信以进行以下中的至少一项之前，所述设备使用所述密钥或所述子密钥与所述另一设备或与证书授权机构进行认证：(i)对所述设备进行配置，或者(ii)对通过控制所述过程生成的所述实时数据进行发送或接收中的至少一项。

[0154] 23、根据方面19至22中的任一方面所述的设备，还包括额外的计算机可执行指令，所述额外的计算机可执行指令当由所述处理器执行时，使得所述设备建立用于在所述设备与所述另一设备之间进行通信的会话以进行以下中的至少一项：(i)对所述设备进行配置，或者(ii)对通过控制所述过程生成的所述实时数据进行发送或接收中的至少一项，并且其中，所述密钥或所述子密钥中的至少一个对于所述会话是唯一的。

[0155] 24、根据方面23所述的设备，其中，所述会话对应于所述另一设备或对应于所述另一设备是其中的节点的网络。

[0156] 25、根据方面19至24中的任一方面所述的设备，其中，所述第一组必需的条件或所述第二组必需的条件中的至少一个包括以下中的至少一个：所述过程控制工厂的地理空间位置、特定时间、特定时间间隔、日期、或区域。

[0157] 26、根据方面19至25中的任一方面所述的设备，其中，所述第一组必需的条件或所述第二组必需的条件中的至少一个包括以下中的至少一个：由所述设备发送的用于控制所述过程的数据的类型、由所述设备接收的用于控制所述过程的数据的类型、或所述设备的制造商。

[0158] 27、根据方面19至26中的任一方面所述的设备，其中，所述第一组必需的条件或所述第二组必需的条件中的至少一个包括以下中的至少一个：所述过程控制工厂的标识、所述过程控制工厂的区域的标识、操作所述过程控制工厂的组织实体的标识、或所述过程控制工厂所处的国家的标识。

[0159] 28、根据方面19至27中的任一方面所述的设备，其中，所述第一组必需的条件或所述第二组必需的条件中的至少一个包括所述设备的用户的属性。

[0160] 29、根据方面19至28中的任一方面所述的设备，其中，所述设备是以下中的一个：过程控制器、现场设备、或与所述过程控制器连接的输入/输出(I/O)卡。

[0161] 30、根据方面19至28中的任一方面所述的设备，其中，所述设备是计算设备，所述计算设备被配置为对对应于以下中的至少一个的数据进行发送或接收中的至少一项：过程控制器、现场设备、或与所述过程控制器连接的输入/输出(I/O)卡。

[0162] 31、根据方面19至28中的任一方面所述的设备，其中，所述设备是包括用户接口的移动计算设备，并且其中，移动控制室应用程序在所述移动计算设备上执行。

[0163] 32、根据方面19至31中的任一方面所述的设备，其中，由所述设备的提供者定义所述第一组必需的条件中的至少一个成员，并且其中，由所述设备的用户定义所述第二组必需的条件中的至少一个成员。

[0164] 33、根据方面19至32中的任一方面所述的设备，其中，通过控制所述过程生成并由所述设备发送或接收的所述实时数据被加密。

[0165] 34、根据方面19至33中的任一方面所述的设备，其中，由所述设备发送的所有数据被加密。

[0166] 35、根据方面33或34所述的设备，其中，所述数据至少部分基于所述密钥或所述子密钥中的一个来进行加密。

[0167] 36、前面的方面中的任一方面与前面的方面中的任何其他一个方面结合。

[0168] 额外地，本公开内容的前面的方面仅仅是示范性的而不旨在限制本公开内容的范围。

[0169] 以下额外的考虑适用于前述讨论。在本说明书中，所描述的如由任何设备或例程所执行的动作(例如，包括在方法200、220和/或250中的动作)一般指根据机器可读指令操纵或变换数据的处理器的动作或过程。机器可读指令可以被存储在通信耦合到处理器的存储器设备上或从通信耦合到处理器的存储器设备中检索。即，本文中描述的方法可以由存储在计算机可读介质上(即，存储器设备上)的一组机器可读指令实现，如图7所示。所述指令当由对应的设备(例如，服务器、移动设备等)的一个或多个处理器执行时，使得处理器执行所述方法。在指令、例程、模块、过程、服务、程序和/或应用程序在本文中被称为存储或保存在计算机可读存储器上或计算机可读介质上的情况下，词语“存储”和“保存”旨在不包括暂态信号。

[0170] 此外，当术语“操作者”、“人员”、“个人”、“用户”、“技术员”和类似其他术语用于描

述过程工厂环境中的可以与本文中描述的系统、装置和方法一起使用或交互的人时，这些术语不旨在为限制性的。在特定术语用于说明书中的情况下，使用所述术语至少部分是由于工厂人员所参与的传统活动，但是不旨在限制能够参与该特定活动的人员。

[0171] 此外，在本说明书中，多个实例可以实施作为单个实例进行描述的部件、操作或结构。尽管一个或多个方法的单个操作被示出并被描述为单独的操作，但是一个或多个单个操作可以同时执行，并且未要求所述操作按所示出的顺序执行。在范例配置中作为单独的部件呈现的结构和功能可以被实施为组合的结构或功能。类似地，作为单个部件呈现的结构和功能可以被实施为单独的部件。这些和其他变型、修改、增加和改进落入本文中的主题的范围内。

[0172] 除非特别另行指出，否则本文中使用诸如“处理”、“计算”、“运算”、“确定”、“识别”、“呈现”、“使得……被呈现”、“使得……被显示”、“显示”等的词语的讨论可以指操纵或变换数据的机器(例如，计算机)的动作或过程，所述数据在一个或多个存储器(例如，易失性存储器、非易失性存储器、或其组合)、寄存器、或接收、存储、发送或显示信息的其他机器部件内被表示为物理(例如，电子、磁性、生物或光学)量。

[0173] 当以软件实施时，本文中描述的应用程序、服务和引擎中的任何可以被存储在任何有形的非暂态计算机可读介质中，例如被存储在磁盘、激光盘、固态存储设备、分子存储装置设备、或其他存储介质上，被存储在计算机或处理器的RAM或ROM中等等。尽管本文中公开的范例系统被公开为除了其他部件，还包括在硬件上执行的软件和/或固件，但是应当注意这样的系统仅仅是示范性的而并不应当认为是限制性的。例如，预见到这些硬件、软件和固件部件中的任何或所有能够完全以硬件实现、完全以软件实现、或以软件和硬件的组合实现。因此，本领域技术人员将容易认识到，所提供的范例并不是实施这样的系统的唯一方式。

[0174] 因此，尽管参考具体范例来描述本发明，但是所述具体返利仅仅旨在是说明性的而不旨在为对本发明的限制，对于本领域技术人员显而易见的是，在不脱离本发明的精神和范围的情况下，可以对所公开的实施例进行改变、增加或删除。

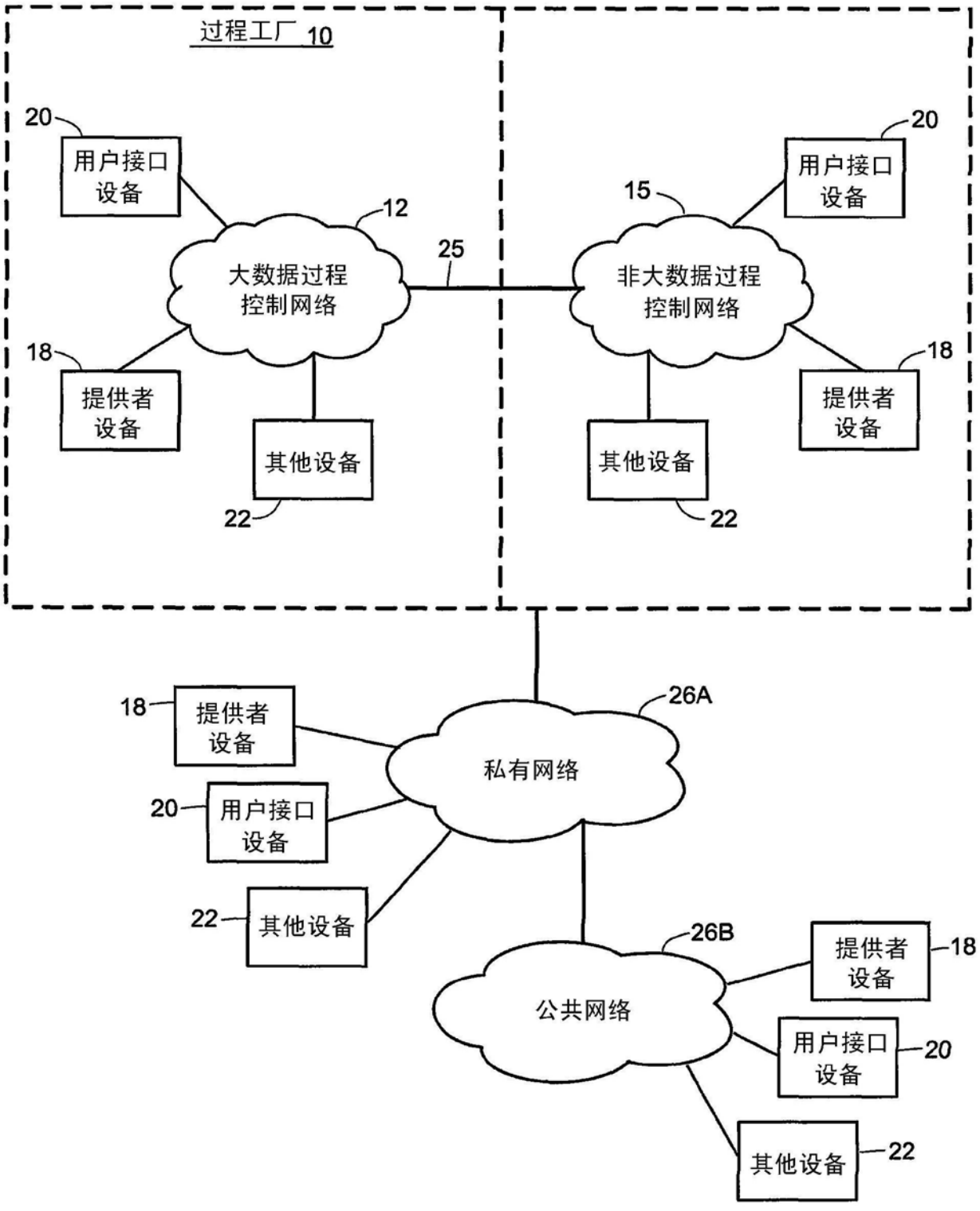

过程工厂 10
20
用户接口设备
12
大数据过程控制网络
25
15
非大数据过程控制网络
20
用户接口设备
18
提供者设备
其他设备
22
其他设备
22
18
提供者设备
18
提供者设备
26A
私有网络
20
用户接口设备
22
其他设备
26B
公共网络
提供者设备
18
用户接口设备
20
其他设备
22

图1

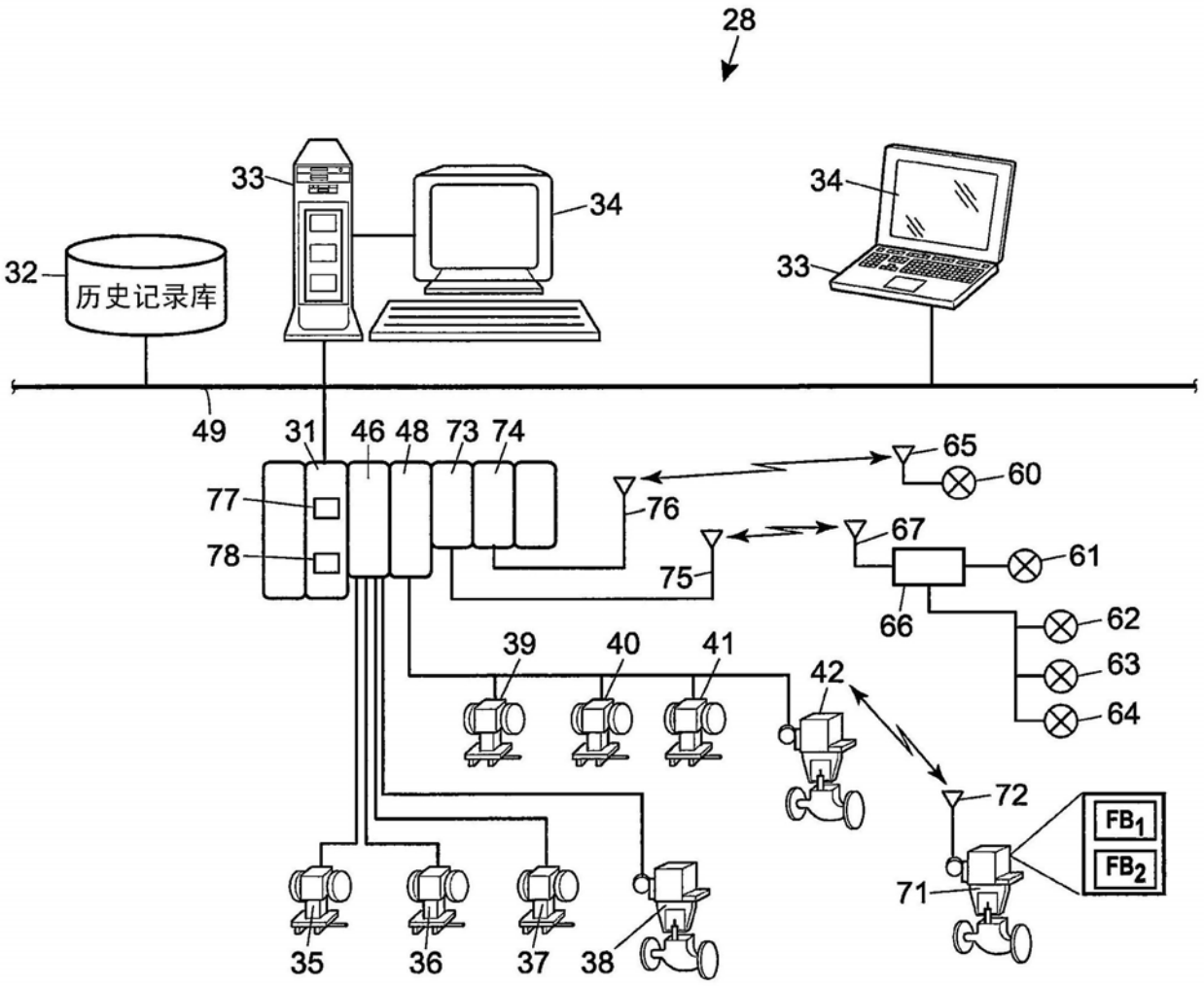

28
33
34
32
历史记录库
34
33
49
31
46
48
73
74
65
60
77
76
78
67
61
75
66
62
39
40
41
42
63
64
72
FB1
FB2
71
35
36
37
38

图2

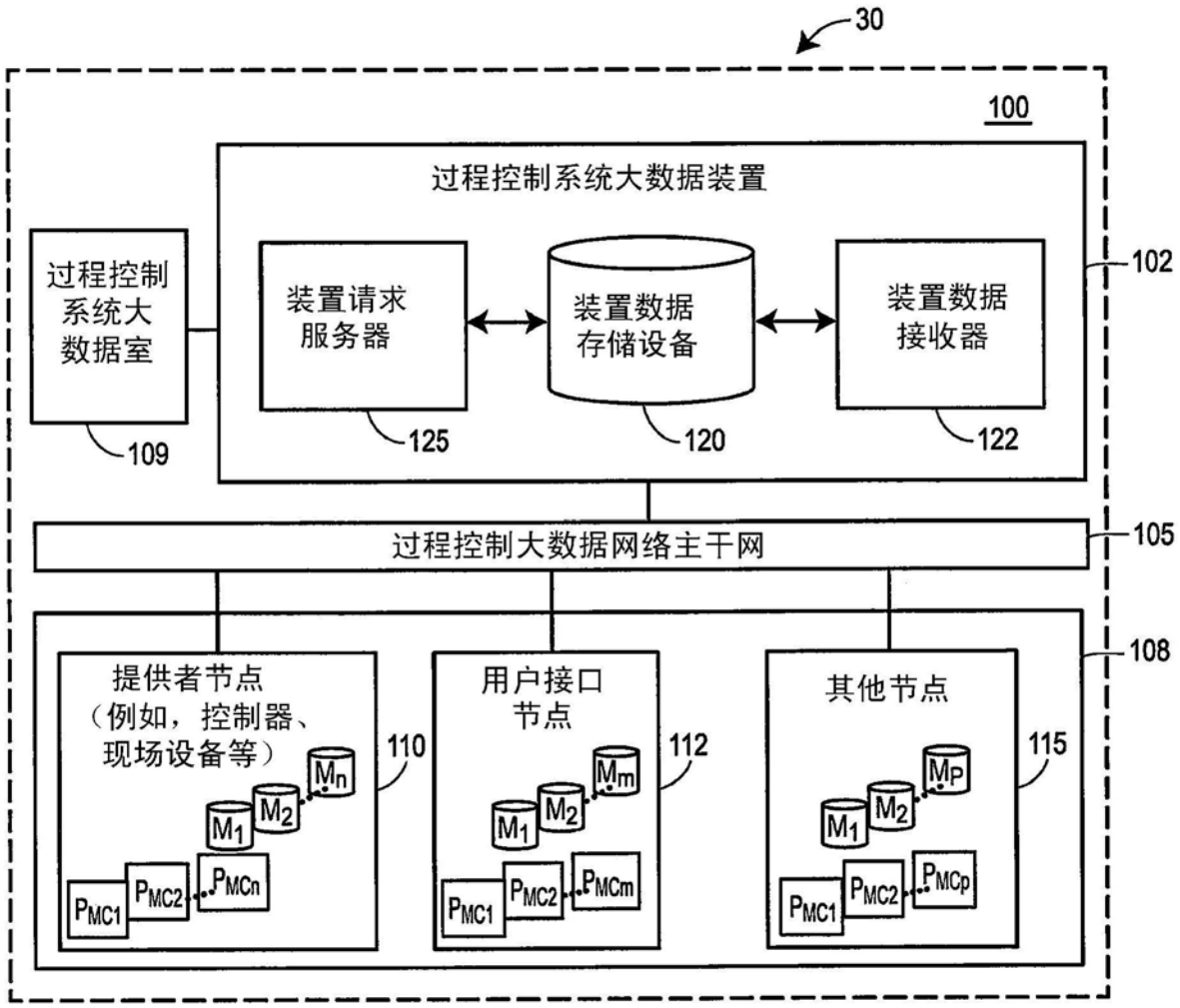

30
100
过程控制系统大数据装置
过程控制系统大数据室
装置请求服务器
装置数据存储设备
装置数据接收器
102
109
125
120
122
过程控制大数据网络主干网
105
108
提供者节点（例如，控制器、现场设备等）
110
用户接口节点
112
其他节点
115
Mn
M1
M2
Mm
MP
PMC1
PMC2
PMCn
PMCm
PMCp

图3

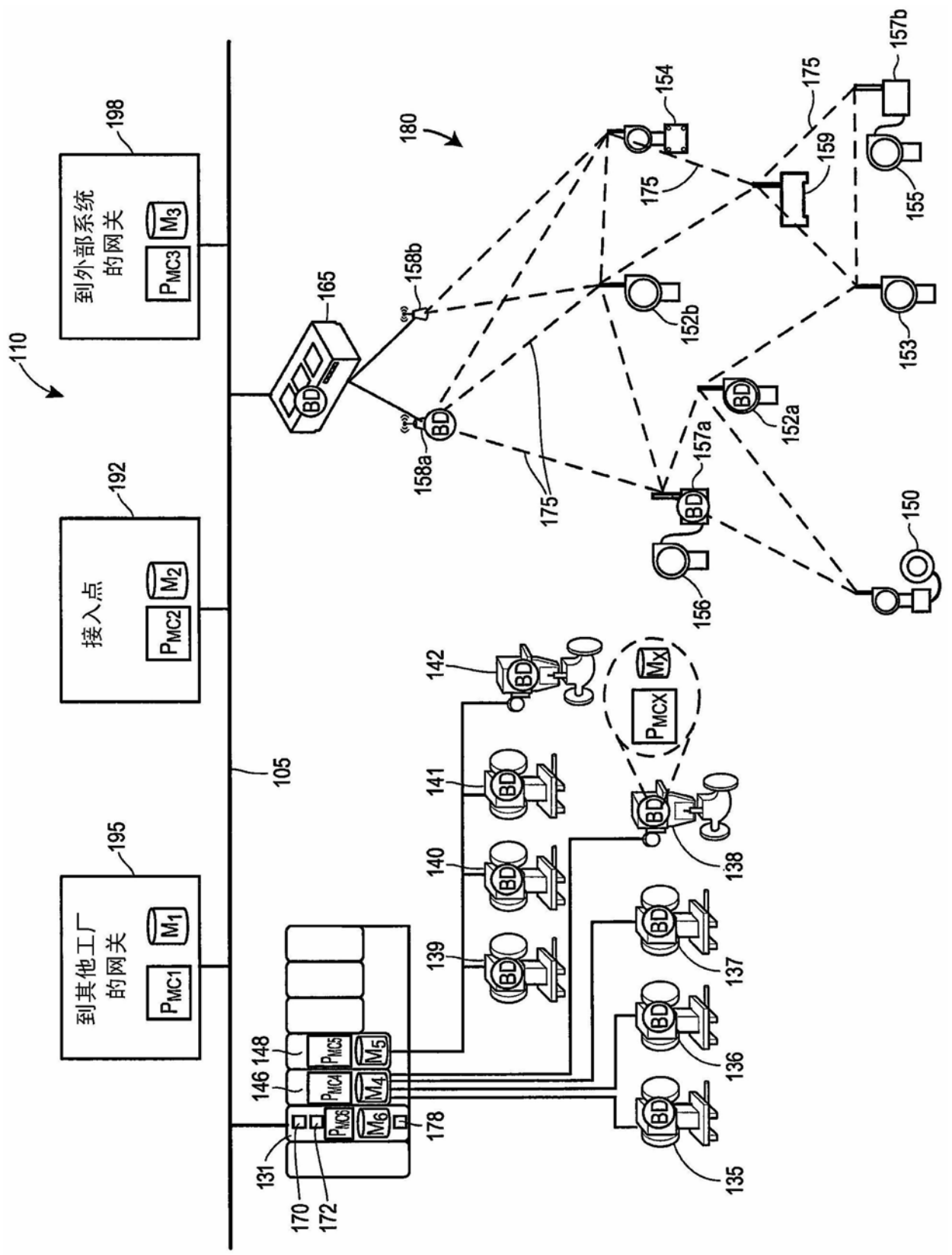

110
198
到外部系统的网关
PMC3
M3
192
接入点
PMC2
M2
195
到其他工厂的网关
PMC1
M1
105
165
BD
158b
158a
180
154
175
159
157b
155
152b
153
152a
157a
150
156
142
141
140
139
PMCX
MX
138
137
136
135
148
146
PMC5
M5
PMC4
M4
PMC6
M6
178
131
170
172

图4

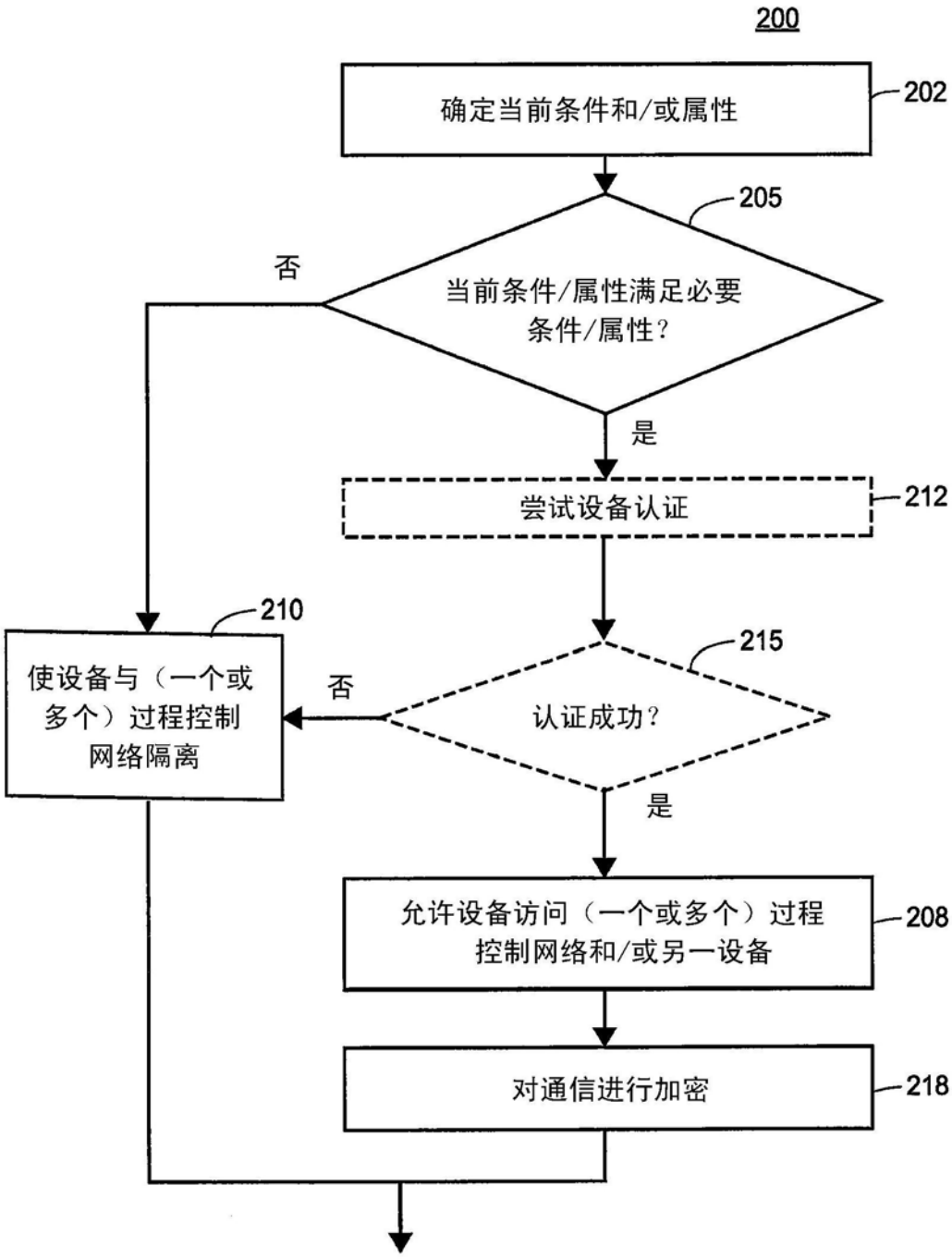

200
确定当前条件和/或属性
202
205
当前条件/属性满足必要条件/属性?
否
是
尝试设备认证
212
210
使设备与（一个或多个）过程控制网络隔离
215
否
认证成功?
是
允许设备访问（一个或多个）过程控制网络和/或另一设备
208
对通信进行加密
218

图5A

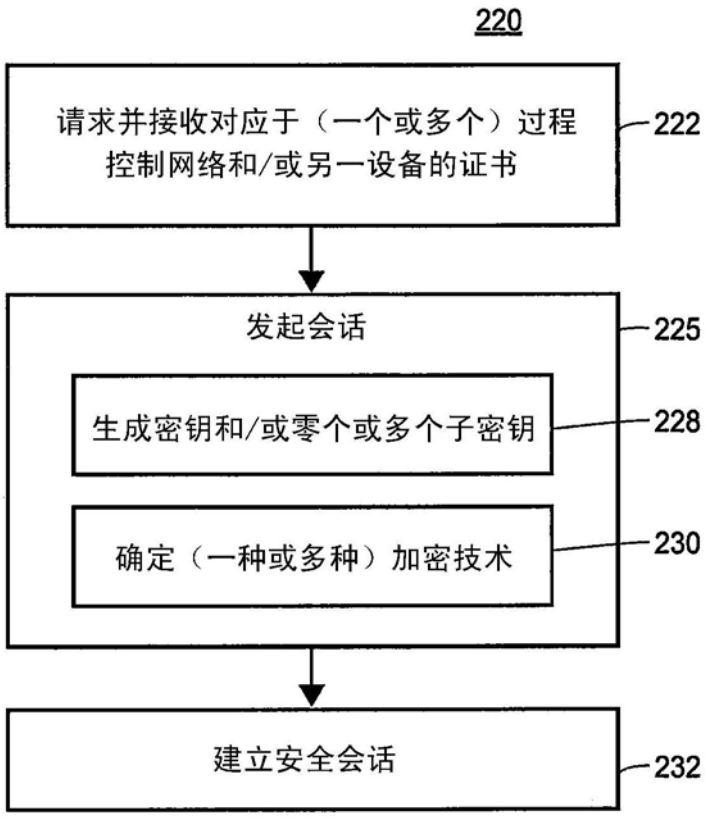

220
请求并接收对应于（一个或多个）过程控制网络和/或另一设备的证书
222
发起会话
225
生成密钥和/或零个或多个子密钥
228
确定（一种或多种）加密技术
230
建立安全会话
232

图5B

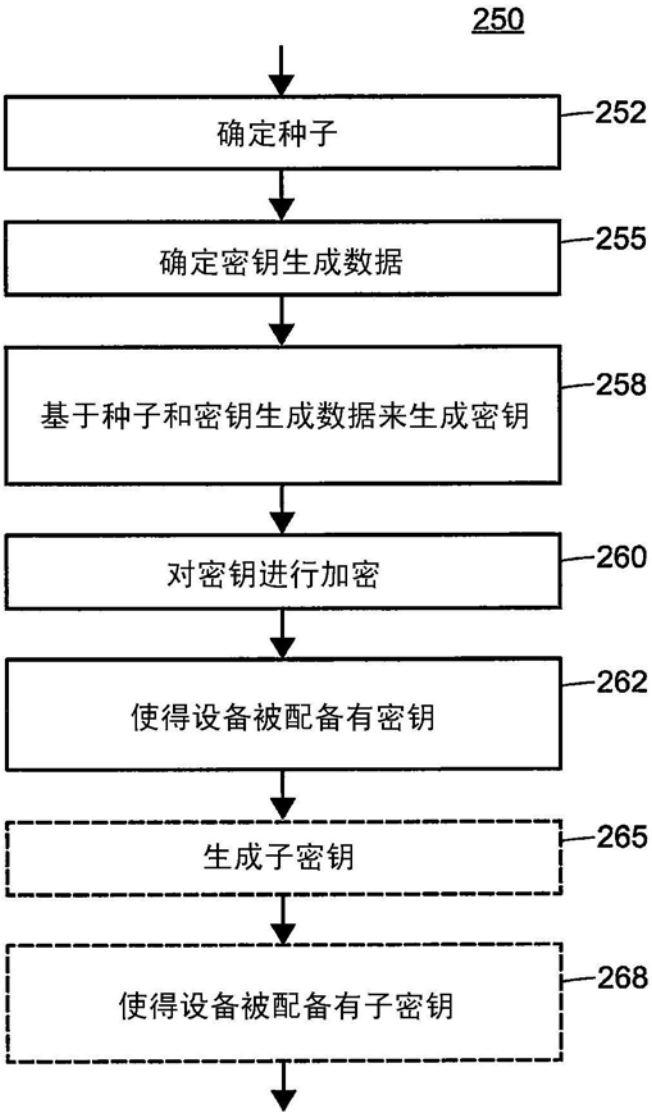

250
确定种子
252
确定密钥生成数据
255
基于种子和密钥生成数据来生成密钥
258
对密钥进行加密
260
使得设备被配备有密钥
262
生成子密钥
265
使得设备被配备有子密钥
268

图6

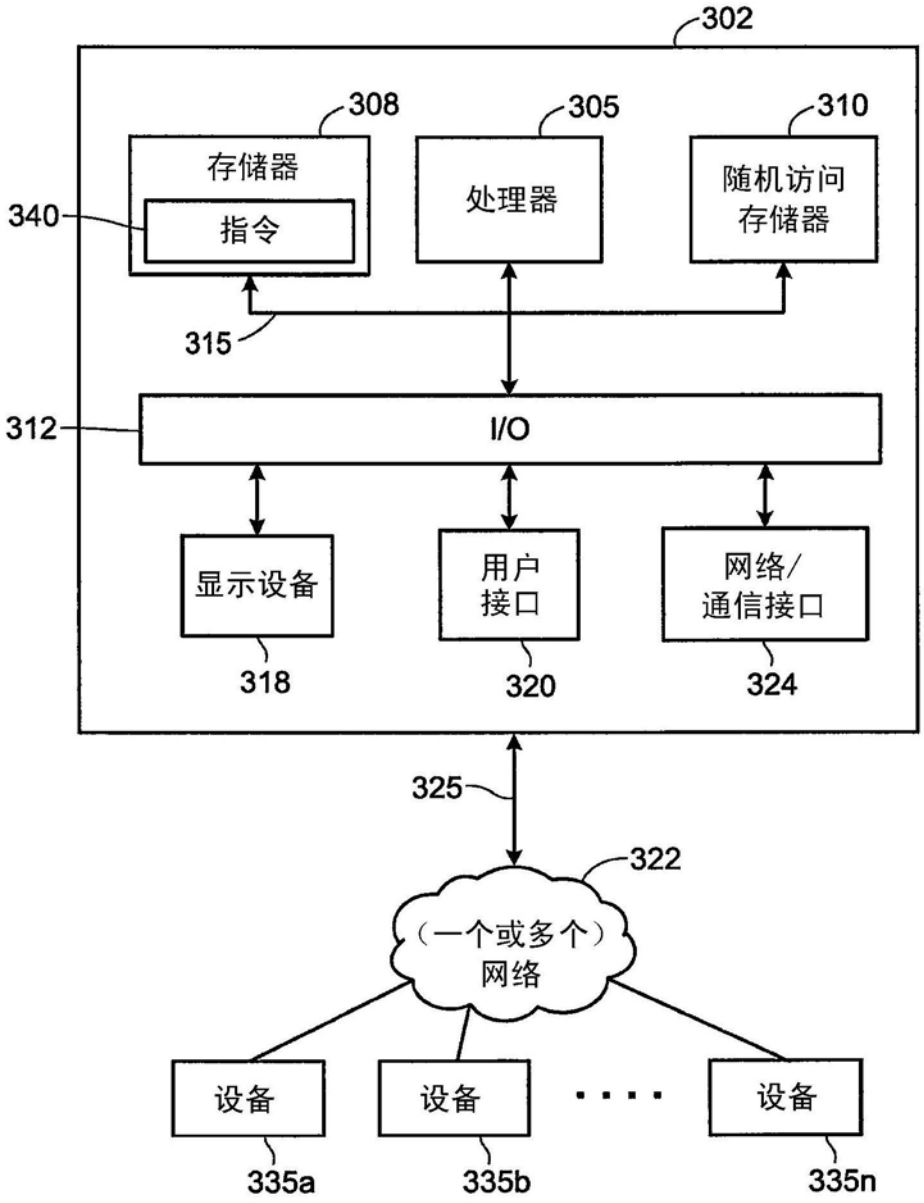

302
308
305
310
存储器
指令
处理器
随机访问
存储器
340
315
312
I/O
显示设备
用户
接口
网络/
通信接口
318
320
324
325
322
（一个或多个）
网络
设备
设备
设备
335a
335b
335n

图7