(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 107976972 B
(45)授权公告日 2022.10.21

(21)申请号 201711003982.X

(22)申请日 2017.10.24

(65)同一申请的已公布的文献号
申请公布号 CN 107976972 A

(43)申请公布日 2018.05.01

(30)优先权数据
15/332,751 2016.10.24 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 E·罗特沃尔德 M·J·尼克松
M·J·布德罗

(74)专利代理机构 永新专利商标代理有限公司 72002
专利代理师 曹雯

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

(56)对比文件
JP 2011021977 A,2011.02.03
JP 2011021977 A,2011.02.03
US 2016147206 A1,2016.05.26
US 2002161927 A1,2002.10.31
US 2016205133 A1,2016.07.14
US 2015104017 A1,2015.04.16
US 2015195086 A1,2015.07.09
CN 104049575 A,2014.09.17
CN 105373091 A,2016.03.02
CN 104035392 A,2014.09.10

审查员 任爽

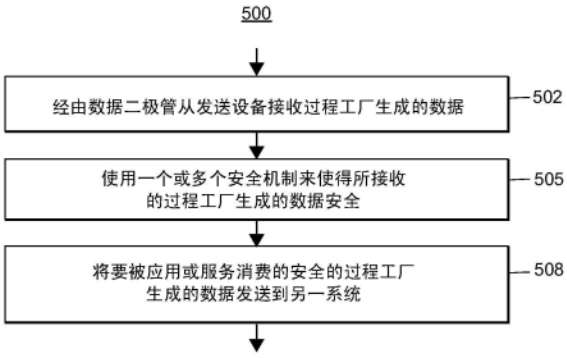
权利要求书5页 说明书26页 附图7页

(54)发明名称

安全的过程控制通信

(57)摘要

使从过程工厂到远程系统的通信安全包括设置在其间的数据二极管,其允许数据从工厂流出,但是防止数据进入工厂及其相关联的系统。通过将二极管的工厂端处的发送设备跨数据数据二极管安全地供应给远程系统端的接收设备使数据安全。发送和接收设备共享循环地更新的密钥材料。为了确保跨单向数据二极管的通信的保真度,发送设备会循环地提供描述工厂数据源的上下文信息。此外,可以使用相应的安全机制/技术来使从工厂数据源传送到数据二极管的发送设备的数据安全,并且可以使用相应的安全机制来使从数据二极管的接收设备传送到远程系统的数据安全。



CN 107976972 B

1.一种用于将通信从过程工厂安全地传输到另一系统的系统,安全的通信传输系统包括:

设置在所述过程工厂的网络与所述另一系统的网络之间的数据二极管,所述数据二极管被配置为防止过程工厂网络与所述另一系统的网络之间的双向通信;

边缘网关,所述边缘网关将所述数据二极管的一组输出与所述另一系统互连,所述边缘网关存储第一密钥的相应的副本;以及

现场网关,所述现场网关将所述过程工厂网络与所述数据二极管的一组输入互连,所述现场网关存储所述第一密钥的相应的副本,

所述现场网关被配置用于:

生成第二密钥,使用所述第一密钥加密所述第二密钥并且经由所述数据二极管将加密的第二密钥传输至所述边缘网关;以及

使用所述第二密钥加密过程工厂数据,所述过程工厂数据在所述过程工厂进行操作以控制工业过程时由所述过程工厂的设备所生成并且将加密的过程工厂数据跨所述数据二极管传输至所述边缘网关;并且

所述边缘网关被配置用于使用所述第二密钥解密经由所述数据二极管接收的加密的过程工厂数据、使得解密的过程工厂数据安全、并且将安全的解密的过程工厂数据传输到所述另一系统的网络。

2.根据权利要求1所述的系统,其中,所述数据二极管的硬件被配置为不包括用于将由所述另一系统的网络所流出的通信传送到所述过程工厂网络的物理通信路径。

3.根据权利要求2所述的系统,其中,所述数据二极管的硬件被配置为经由以下至少一个来防止由所述另一系统的网络所流出的通信进入所述过程工厂网络:排除、省略和/或禁用所述数据二极管的输入端口用于从所述边缘网关接收数据;或者排除、省略和/或禁用数据二极管的输出端口用于传输数据到所述现场网关。

4.根据权利要求1所述的系统,其中,所述数据二极管的软件被配置为防止由所述另一系统的网络所流出的通信进入所述过程工厂网络。

5.根据权利要求4所述的系统,其中,所述数据二极管的软件被配置为通过丢弃或阻止在所述数据二极管的输出端口处从所述边缘网关接收的任何消息或者通过丢弃或阻止寻址到所述现场网关的任何消息来防止由所述另一系统的网络所流出的通信进入所述过程工厂网络。

6.根据权利要求1所述的系统,其中,所述加密的过程工厂数据基于TCP(传输控制协议)、UDP(用户数据报协议)或串行通信跨所述数据二极管传输。

7.根据权利要求1所述的系统,其中,所述现场网关被设置在所述过程工厂处。

8.根据权利要求7所述的系统,其中所述数据二极管被设置在所述过程工厂处。

9.根据权利要求1所述的系统,还包括将所述过程工厂网络与所述现场网关互连的本地工厂网关,所述本地工厂网关使用TLS(传输层安全性)封装来使所述过程工厂数据安全。

10.根据权利要求9所述的系统,其中,包括以下情况中的至少一种:

由包括在所述过程工厂中的所述设备生成的数据的至少第一部分被流传输到所述本地工厂网关;或者

由包括在所述过程工厂中的所述设备生成的数据的至少第二部分响应于轮询而被发

送到所述本地工厂网关。

11.根据权利要求1所述的系统，其中，由所述现场网关使用所述第二密钥执行的加密是第一加密，并且其中，由所述设备生成的至少一些数据的第二加密在所述设备处被执行。

12.根据权利要求9所述的系统，其中，由所述设备生成和加密的所述数据中的至少一些数据经由所述过程工厂的无线网络或有线网络中的至少一个传送到所述本地工厂网关。

13.根据权利要求1所述的系统，其中，所述边缘网关设置在所述过程工厂处。

14.根据权利要求1所述的系统，其中，所述边缘网关使用令牌或证书来确保所述过程工厂数据传送到所述另一系统。

15.根据权利要求14所述的系统，其中：

所述令牌或证书由包括在所述另一系统中的安全服务管理；

所述令牌或证书对于有限的时间段是有效的；以及

所述有限的时间段有不超过一小时的持续时间。

16.根据权利要求1所述的系统，其中，所述安全的过程工厂数据使用以下各项中的至少一项来从所述边缘网关传送到所述另一系统的网络：互联网连接、蜂窝路由器或另一类型的回程互联网连接。

17.根据权利要求1所述的系统，其中，所述过程工厂数据储存在所述另一系统处，并且仅对所述另一系统的授权用户授予对在所述另一系统处储存的数据的访问。

18.根据权利要求1所述的系统，其中，所述第一密钥在所述现场网关与所述边缘网关之间共享。

19.根据权利要求16所述的系统，其中，所述边缘网关还被配置用于生成所述第一密钥并且将所述第一密钥与所述现场网关共享。

20.根据权利要求1所述的系统，其中，所述另一系统被包括在所述过程工厂中。

21.根据权利要求1所述的系统，其中，所述另一系统在一个或多个计算云中实现。

22.根据权利要求1所述的系统，其中，所述另一系统能够经由公共互联网访问。

23.根据权利要求1所述的系统，其中，所述另一系统不能经由公共互联网访问。

24.根据权利要求1所述的系统，其中，所述另一系统提供与所述过程工厂相对应的一个或多个服务，所述一个或多个服务包括以下各项中的至少一项：

监控在所述过程工厂处发生的状况和/或事件；

感测在所述过程工厂处发生的状况和/或事件；

监控由所述过程工厂控制的过程的至少一部分；

描述性分析；

规定性分析；或者

用于修改所述过程工厂的至少一部分的一个或多个规定性更改。

25.根据权利要求1所述的系统，其中：

所述设备中的至少一个设备经由包括在所述过程工厂中的通信网络与所述过程工厂内的另一设备进行通信，以控制所述过程工厂内的过程的至少一部分，

所述通信网络与所述过程工厂网络不同，并且

所述通信网络支持Wi-Fi协议、以太网协议和IEEE 802.11兼容协议、移动通信协议、短波无线电通信协议、4-20ma信令、HART® 协议、WirelessHART® 协议、

FOUNDATION®现场总线协议、PROFIBUS协议、DeviceNet协议或另一种工业通信协议中的至少一种。

26.根据权利要求25所述的系统，其中，包括在所述过程工厂中的所述通信网络是第一通信网络，并且其中，所述数据二极管经由所述过程工厂网络从一个或多个设备接收所生成的数据。

27.根据权利要求1所述的系统，其中，所述过程工厂网络支持至少一种工业通信协议。

28.一种使过程工厂与另一系统之间的通信安全的方法，所述方法包括：

在现场网关处从过程工厂网络接收数据，所述数据由所述过程工厂的一个或多个设备在所述过程工厂进行操作以控制工业过程时生成，由所述过程工厂的一个或者多个设备生成的数据是过程工厂数据，并且相应的过程工厂数据由所述一个或者多个设备中的每个设备确保经由第一安全机制安全，以从所述一个或多个设备中的每个设备传输到所述现场网关；

经由第二安全机制由所述现场网关使所接收的过程工厂数据安全，所述第二安全机制包括(i)供应在与所述另一系统通信连接的边缘网关或者所述现场网关之一中的第一密钥，所述第一密钥在所述边缘网关和所述现场网关之间共享；(ii)基于所述第一密钥进行加密的第二密钥；以及(iii)由所述现场网关使用所述第二密钥对所接收的过程工厂数据进行的加密；以及

跨数据二极管将所述安全的过程工厂数据传输到所述边缘网关，以传送到所述另一系统，由所述边缘网关和所述另一系统经由第三安全机制使所述边缘网关与所述另一系统之间的通信连接安全，并且所述数据二极管被配置为防止由所述边缘网关传送的任何数据进入所述现场网关。

29.根据权利要求28所述的方法，其中，所述数据二极管被配置为经由以下至少一个来防止由所述另一系统的网络所流出的通信进入所述过程工厂网络：排除、省略和/或禁用所述数据二极管的输入端口用于从所述边缘网关接收数据；或者排除、省略和/或禁用数据二极管的输出端口用于传输数据到所述现场网关；或者丢弃或阻止从所述边缘网关收到的任何消息；或者丢弃或阻止发往所述现场网关的任何消息。

30.根据权利要求28所述的方法，其中：

(i)所述方法还包括：

由所述现场网关生成第二密钥；

由所述现场网关基于第一密钥对所述第二密钥进行加密；以及

由所述现场网关经由所述数据二极管将加密的第二密钥传输至所述边缘网关；以及

(ii)所述数据二极管被配置为当在所述边缘网关处接收到加密的第二密钥时防止由所述另一系统的网络所流出的通信进入所述过程工厂网络。

31.根据权利要求28所述的方法，其中，所述第一安全机制，所述第二安全机制和所述第三安全机制是不同的安全机制。

32.根据权利要求28所述的方法，

还包括以所述第一密钥供应所述现场网关和所述边缘网关，包括在所述现场网关处接收由所述边缘网关生成第一密钥。

33.根据权利要求28所述的方法，其中，所述第一安全机制包括由所述一个或多个设备

中的每个设备对由所述一个或多个设备中的每个设备生成的过程工厂数据进行相应的加密。

34.根据权利要求33所述的方法，其中，所述第一安全机制还包括将经加密的过程工厂数据封装在所述过程工厂中实现的安全层中。

35.根据权利要求28所述的方法，其中，所述第三安全机制包括安全令牌或证书。

36.根据权利要求28所述的方法，其中，所述第三安全机制包括由所述边缘网关执行的加密。

37.一种使过程工厂与服务所述过程工厂的另一系统之间的通信安全的方法，所述方法包括：

(i)在边缘网关处经由通信地连接到所述过程工厂的现场网关的数据二极管接收数据，所述数据由所述过程工厂中的一个或多个设备在所述过程工厂进行操作以控制工业过程时生成，由所述过程工厂中的一个或多个设备生成的数据是过程工厂数据，其中：

所述过程工厂数据由所述一个或多个设备中的每个设备经由第一安全机制确保安全，用于从所述一个或多个设备中的每个设备传输到所述现场网关，并且进一步由所述现场网关经由第二安全机制确保安全，用于跨所述数据二极管从所述现场网关传输到所述边缘网关，所述第二安全机制包括(i)供应在所述边缘网关或所述现场网关中的第一密钥，所述第一密钥在所述边缘网关和所述现场网关之间共享；(ii)基于所述第一密钥进行加密的第二密钥；以及(iii)由所述现场网关使用所述第二密钥对所接收的过程工厂数据进行的加密，并且

所述数据二极管被配置为防止由所述边缘网关传送的任何数据进入所述现场网关；

(ii)由所述边缘网关使用所述第二密钥对由所述现场网关加密并且在所述边缘网关处经由所述数据二极管接收的所述过程工厂数据进行解密；

(iii)经由第三安全机制由所述边缘网关使所解密的过程工厂数据安全；以及

(iv)由所述边缘网关将由所述边缘网关确保安全的所述过程工厂数据传送到所述另一系统。

38.根据权利要求37所述的方法，其中，所述数据二极管被配置为经由以下至少一个来防止由所述另一系统的网络所流出的通信进入所述过程工厂网络：排除、省略和/或禁用所述数据二极管的输入端口用于从所述边缘网关接收数据；或者排除、省略和/或禁用数据二极管的输出端口用于传输数据到所述现场网关；或者丢弃或阻止从所述边缘网关收到的任何消息；或者丢弃或阻止发往所述现场网关的任何消息。

39.根据权利要求37所述的方法，其中，所述第二密钥由所述现场网关进行加密；并且所述方法还包括在所述边缘网关处经由所述数据二极管从所述现场网关接收经加密的第二密钥。

40.根据权利要求39所述的方法，其中，所述数据二极管被配置为当在所述边缘网关处接收到加密的第二密钥时防止由所述另一系统的网络所流出的通信进入所述过程工厂网络。

41.根据权利要求37所述的方法，其中，所述第一安全机制包括由所述一个或者多个设备中的每个设备对所述过程工厂数据的相应的加密。

42.根据权利要求37所述的方法，其中，所述第一安全机制包括由所述一个或者多个设

备中的每个设备对所述过程工厂数据在安全层中的相应的封装。

43.根据权利要求37所述的方法，还包括：使用所述第一密钥跨所述数据二极管在所述边缘网关与所述现场网关之间建立安全连接，所述第一密钥是秘密密钥，并且其中，所述第二安全机制包括在所述边缘网关与所述现场网关之间建立的所述安全连接。

44.根据权利要求37所述的方法，还包括：在所述边缘网关与所述另一系统之间建立安全连接，并且其中，所述第三安全机制包括在所述边缘网关与所述另一系统之间建立的所述安全连接。

45.根据权利要求44所述的方法，其中，在所述边缘网关与所述另一系统之间建立所述安全连接包括：

对由所述另一系统提供的安全服务进行认证；以及

响应于所述认证而接收安全令牌或证书。

46.根据权利要求45所述的方法，其中，将所述由所述边缘网关确保安全的过程工厂数据传送到所述另一系统包括：将所述安全令牌或证书结合所述过程工厂数据传送到所述另一系统。

47.根据权利要求45所述的方法，其中，所述安全令牌或者证书仅对于有限的时间周期有效。

48.根据权利要求37所述的方法，其中，由所述边缘网关通过由所述边缘网关加密所述解密的过程工厂数据来使所述解密的过程工厂数据安全。

49.根据权利要求37所述的方法，其中，将所述由所述边缘网关来确保安全的过程工厂数据传送到所述另一系统包括：将所述由所述边缘网关来确保安全的过程工厂数据传送到所述过程工厂中包括的系统。

50.根据权利要求37所述的方法，其中，由所述边缘网关将所述安全的过程工厂数据传送到所述另一系统包括：将所述安全的过程工厂数据传送到在一个或多个计算云中实现的系统。

51.根据权利要求37所述的方法，其中，由所述边缘网关将所述过程工厂数据传送到所述另一系统包括：经由公共互联网上的安全连接将所述过程工厂数据传送到所述另一系统。

52.根据权利要求37所述的方法，其中，由所述边缘网关将所述过程工厂数据传送到所述另一系统包括：将所述过程工厂数据传送到提供以下至少一个的系统：

监控在所述过程工厂处发生的状况和/或事件；

感测在所述过程工厂处发生的状况和/或事件；

监控由所述过程工厂执行的过程的至少一部分；

描述性分析；

规定性分析；或者

用于修改所述过程工厂的至少一部分的规定性更改。

安全的过程控制通信

[0001] 相关参考文献

[0002] 本公开内容涉及以下专利申请:于2014年10月6日提交的题为“Regional Big Data in Process Control Systems”的共同拥有的美国专利申请No.14/507,188;于2016年9月23日提交的题为“Data Analytics Services for Distributed Industrial Performance Monitoring”的共同拥有的美国专利申请No.15/274,519;于2016年9月23日提交的题为“Distributed Industrial Performance Monitoring and Analytics”的美国专利申请No.15/274,233;以及于2016年10月24日提交的标题为“Process Device Condition and Performance Monitoring”的共同拥有的美国专利申请No.15/332,521,上述申请的全部公开内容通过引用并入本文。

技术领域

[0003] 本公开内容总体上涉及过程工厂和过程控制系统,更具体而言,涉及本地过程工厂/过程控制系统与服务本地过程控制工厂/系统的远程系统(例如普适的感测系统)之间的安全通信。

背景技术

[0004] 分布式过程控制系统(如在化学、石油或其它过程工厂中使用的分布式过程控制系统)通常包括一个或多个过程控制器,其经由模拟、数字或组合的模拟/数字总线或者经由无线通信链路或网络通信地耦合到一个或多个现场设备。可以是例如阀、阀定位器、开关和变送器(例如,温度、压力、液位和流量传感器)的现场设备位于过程环境内,并且通常执行物理或过程控制功能,例如打开或关闭阀、测量诸如压力、温度等的过程参数等,以控制在过程工厂或系统内执行的一个或多个过程。智能现场设备(例如遵循公知的现场总线协议的现场设备)还可以执行通常在控制器内实现的控制计算、报警功能和其它控制功能。通常也位于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它信息的信号,并执行运行例如不同控制模块的控制器应用,该不同的控制模块进行过程控制决策,基于接收到的信息生成控制信号,并与在现场设备(诸如HART®、WirelessHART®和FOUNDATION®现场总线现场设备等)中执行的控制模块或块进行协调。控制器中的控制模块通过通信线路或现场设备的链路发送控制信号,从而控制过程工厂或系统的至少一部分的操作。

[0005] 来自现场设备和控制器的信息通常可以通过数据高速通道而可用于一个或多个其它硬件设备,诸如操作员工作站、个人计算机或计算设备、数据历史库、报告生成器、集中式数据库或其它集中式管理计算设备等,这些硬件设备通常放置在控制室或其它远离更苛刻的工厂环境的位置。这些硬件设备中的每一个通常跨过程工厂或过程工厂的一部分而集中。这些硬件设备运行应用,其例如可以使得操作员能够执行关于控制过程和/或操作过程工厂的功能,诸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、查看现场设备和控制器生成的报警、仿真过程的操作以便培训人员

或测试过程控制软件、保持和更新配置数据库等。由硬件设备、控制器和现场设备使用的数据高速通道可以包括有线通信路径、无线通信路径或有线和无线通信路径的组合。

[0006] 作为示例，由艾默生过程管理公司出售的DeltaV™控制系统包括储存在位于过程工厂内的不同位置处的不同设备内并由其执行的多个应用。驻留在一个或多个工作站或计算设备中的配置应用使得用户能够创建或更改过程控制模块，并经由数据高速通道将这些过程控制模块下载到专用分布式控制器。通常，这些控制模块由通信互连的功能块组成，这些功能块是面向对象的编程协议中的对象，这些对象基于对其的输入执行控制方案内的功能，并且向控制方案内的其它功能块提供输出。配置应用还可以允许配置设计者创建或改变由查看应用使用操作员界面，以向操作员显示数据并且使得操作员能够在过程控制例程内改变设置(诸如设定点)。每个专用控制器，并且在某些情况下，一个或多个现场设备，储存和执行相应的控制器应用，其运行分配并下载到其中的控制模块以实现实际的过程控制功能。可以在一个或多个操作员工作站上(或在与操作员工作站和数据高速通道通信连接的一个或多个远程计算设备上)执行的查看应用经由数据高速通道从控制器应用接收数据并使用用户界面向过程控制系统设计人员、操作员或用户显示该数据，并且可以提供诸如操作员视图、工程师视图、技术人员视图等的许多不同视图中的任何视图。数据历史库应用通常储存数据历史库设备中并由其执行，该数据历史库设备收集并储存跨数据高速通道提供的一些或全部数据，而配置数据库应用可以在附接到数据高速通道的另外的计算机中运行以储存当前过程控制例程配置和与其相关联的数据。替代地，配置数据库可以位于与配置应用相同的工作站中。

[0007] 一般而言，过程工厂的过程控制系统包括通过一组分层网络和总线互连的现场设备、控制器、工作站和其它设备。过程控制系统可以转而与各种商业和外部网络连接，例如，以降低制造和运营成本、提高生产力和效率、及时提供对过程控制和/或过程工厂信息的访问等。另一方面，过程工厂和/或过程控制系统与企业和/或外部网络和系统的互连增加了可能由商业系统和应用(例如企业和/或外部网络中使用的商业系统和应用)中的预期隐患引起的网络入侵和/或恶意网络攻击的风险。过程工厂、网络和/或控制系统的网络入侵和恶意网络攻击可能会对信息资产的机密性、完整性和/或可用性产生负面影响，一般而言，这是与通用计算网络相似的隐患。然而，与通用计算机网络不同，过程工厂、网络和/或控制系统的网络入侵还可能导致不仅工厂装备、产品和其它物理资产的损害、毁坏和/或损失，而且还会导致人命丧失。例如，网络入侵可能使得过程变得不受控制，从而产生爆炸、火灾、洪水、暴露于危险材料等。因此，保护与过程控制工厂和系统相关的通信是至关重要的。

[0008] 图1包括用于过程控制或工业过程系统的示例性安全级别的框图10。图10描绘了在过程控制系统的各个部件、过程控制系统本身以及过程控制系统可以通信地连接到的另一系统和/或网络之间的互连，以及与在过程控制系统和另一系统/网络中及过程控制系统与另一系统/网络之间的通信有关的层或级别。安全级别经由分段或分离提供分层安全的方法，并且各个级别受一个或多个防火墙12A、12B、12C保护，以允许只有不同级别之间的授权业务。在图1中，较低编号的安全级别更接近正被控制的在线过程，而较高编号的安全级别从执行过程中被更多地移除。因此，信任级别(例如，消息、分组和其它通信的安全性和有效性的相对信任程度)在设备级别上是最高的(级别0)，以及信任级别是商业网络级别以上的最低级别(级别5)，例如，在公共互联网和/或其它公共网络上。使用由ISA(国际自动化学

会)95.01-IEC(国际电工委员会)62264-1标准化的控制层级逻辑框架的Purdue模型,过程控制系统通常落在安全级别0-2,并且制造、公司和企业系统一般落在安全级别3-5。

[0009] 在图1中示出了不同安全级别中的每一个处的不同功能的示例。通常,级别0包括现场设备和设置在过程工厂内并且与过程和/或过程流直接接触的其它设备,例如,传感器、阀、阀定位器、开关、变送器和执行物理和/或过程控制功能(诸如打开或关闭阀、测量诸如压力、温度等过程参数,等等)的其它设备。为了说明清楚,示例性现场设备在图1中未示出。

[0010] 级别1包括控制器和其它过程控制设备15A-15D,其例如通过从现场设备接收输入、使用控制方案、模块或其它逻辑来处理输入、并将所得输出发送到其它设备来提供对过程的实时操作的基本控制。通常,这些过程控制设备被编程和/或配置有相应的控制方案。例如,级别1处的过程控制设备可以包括过程控制器、可编程逻辑控制器(PLC)、远程终端单元(RTU)等。如图1所示,级别1处的过程控制设备可以包括执行批量控制15A、离散控制15B、连续控制15C、混合控制15D和/或其它类型控制的过程控制设备。

[0011] 级别2包括为过程工厂提供生产区域监督控制的设备和装备18A-18D。例如,级别2可以包括报警和/或告警系统18A、操作员工作站18C、其它人机接口(HMI)18B、18D等。通常,级别2设备和装备可以经由一个或多个防火墙12A、12B与级别1设备15A-15D以及级别3设备和装备进行通信。

[0012] 级别3容纳工厂系统和/或网络,例如管理现场/工厂操作和控制的设备、装备和系统20A-20D,以生产或制造期望的最终产品。例如,级别3可以包括用于生产控制、报告、调度等的生产系统20A;用于提高质量、生产率、效率等的优化系统20B;用于历史化由过程工厂生成的数据和/或指示过程工厂的数据的历史库20C;和/或由人员用于设计和开发控制方案和模块、操作员工作站和/或HMI接口等的工程工作站或计算设备20D。

[0013] 跳到级别5,级别5通常容纳商业、公司或企业系统和/或网络。通常,这样的系统和/或网络管理与企业外的系统的接口连接。例如,可以在级别5找到企业的VPN(虚拟专用网络)、公司或企业互联网接入服务和/或其它IT(信息技术)基础设施系统和应用。

[0014] 可以被视为级别5的向内扩展的级别4通常容纳企业内部的公司或企业系统,例如支持电子邮件、内联网、现场业务规划和物流、库存、调度的公司系统和/或其它公司/企业系统和网络。

[0015] 如图1所示,安全级别3和4跨隔离区(DMZ)22之间彼此相连,该隔离区(DMZ)22将商业或企业系统和/或网络与工厂/过程系统和/或网络分离,从而最小化过程工厂暴露的安全风险的级别。DMZ 22可以包括一个或多个相应的防火墙12C,并且可以容纳与在较低安全级别的工厂相关的设备、装备和应用通信、和/或与在较高安全级别的企业相关的设备、装备和应用通信的各种设备、装备、服务器、和/或应用25A-25F。例如,DMZ 22可以容纳终端服务25A、补丁管理25B、一个或多个AV服务器25C、一个或多个历史库25D(其可以包括例如镜像历史库)、Web服务操作25E和/或一个或多个应用服务器25F,仅举几例。通常,对于在DMZ 22以上的安全级别的设备、装备和/或应用,仅授权的设备被允许通信地访问过程工厂,并且还需要经由DMZ 22的设备、装备、服务器和/或应用来进行连接。DMZ设备25A-25F转而保持与较低级别的分离连接,从而保护过程工厂和控制系统免受来自企业(及更高)系统和/或网络的攻击。

[0016] 现在转向对远程服务的简要讨论，远程服务越来越普遍地被不同的用户和系统使用。例如，微软(Microsoft) Windows®操作系统提供的远程桌面服务产品使得用户能够从公司网络和/或互联网访问基于会话的桌面、基于虚拟机的桌面或数据中心中的其它应用。Intuit®提供的QuickBooks®在线产品使得用户能够经由互联网执行会计功能(诸如现金流管理、开发票和在线付款等)。一般而言，远程服务由一个或多个应用提供，该一个或多个应用远离访问远程服务的系统或用户而执行。例如，该一个或多个应用在云等中执行和管理远程服务器组处的数据，并且经由一个或多个专用和/或公共网络(例如企业网络和/或公共网络)来访问。

发明内容

[0017] 在一实施例中，一种用于将通信从过程工厂安全地传送到另一系统的系统包括设置在所述过程工厂的网络与所述另一系统的网络之间的数据二极管。所述数据二极管被配置为防止所述过程工厂网络与所述另一系统的网络之间的双向通信，使得在所述过程工厂进行操作以控制工业过程时由所述过程工厂的设备所生成的数据被加密并且跨数据二极管或经由数据二极管从所述过程工厂网络安全地传输到所述另一系统的网络。

[0018] 在一实施例中，一种使过程工厂与另一系统之间的通信安全的方法包括：在现场网关处从过程工厂网络接收数据，所述数据由所述过程工厂的一个或多个设备在所述过程工厂进行操作以控制工业过程时生成，其中，所述过程工厂数据被确保经由第一安全机制从所述一个或多个设备传输到所述现场网关。所述方法还包括经由第二安全机制由所述现场网关使所述过程工厂数据安全，以及跨数据二极管传输所述安全的过程工厂数据以经由边缘网关传送到所述另一系统。所述边缘网关通信地连接到所述另一系统，经由第三安全机制使所述边缘网关与所述另一系统之间的通信连接安全。所述数据二极管被配置为防止由所述边缘网关传送的任何数据进入所述现场网关。

[0019] 在一实施例中，一种使过程工厂与服务于所述过程工厂的另一系统之间的通信的方法包括：在边缘网关处经由通信地连接到所述过程工厂的现场网关的数据二极管接收数据，所述数据由所述过程工厂中的一个或多个设备在所述过程工厂进行操作以控制工业过程时生成。所述过程工厂数据被确保用于经由第一安全机制从所述一个或多个设备传输到所述现场网关，并且进一步被确保用于经由第二安全机制跨所述数据二极管从所述现场网关传输到所述边缘网关。此外，所述数据二极管被配置为防止由所述边缘网关传送的任何数据进入所述现场网关。所述方法还包括经由第三安全机制由所述边缘网关使所述过程工厂数据安全，并由所述边缘网关将所述安全的过程工厂数据传送到所述另一系统。

附图说明

[0020] 图1包括用于过程控制或工业过程系统的示例性安全级别的框图，其尤其包括过程控制系统的各个示例性部件、过程控制系统本身和其它示例性系统和/或网络之间的互连；

[0021] 图2是示例性过程工厂或过程控制系统的框图，其尤其例示了过程控制系统的各个示例性部件、过程控制系统本身和其它示例性系统和/或网络之间的互连；

[0022] 图3是用于过程工厂或过程控制系统的示例性安全架构的框图；

[0023] 图4描绘了可以用于为过程工厂或过程控制系统供应(provisioning)安全通信的示例性消息流；

[0024] 图5描绘了可以用于在数据二极管上传送过程工厂数据的示例消息流；

[0025] 图6是用于从过程工厂或过程控制系统安全地传送通信的示例性方法的流程图；以及

[0026] 图7是用于从过程工厂或过程控制系统安全地传送通信的示例性方法的流程图。

具体实施方式

[0027] 如上所述，保护过程控制工厂和系统免受网络入侵和恶意网络攻击通常利用分层或分级的安全层级，其中，至少一些层或级别通过使用防火墙和其它安全机制来保护。例如，如先前关于图1所讨论的，处于安全级别0-3的过程工厂系统、网络和设备可以被保护免受来自处于安全级别4-5的企业网络和/或来自利用企业网络的高于级别5的任何外部网络的威胁，例如，通过使用DMZ 22和一个或多个防火墙12A-12C。然而，随着越来越多的对过程工厂数据进行操作的服务和应用被移动以远程地执行，例如在过程工厂之外的网络和系统上(例如，处于企业或商业内的级别4和/或级别5)，和/或甚至在企业或商业外部的网络和系统(例如，级别5以上，经由互联网或其它公共网络)上，需要用于防止过程工厂系统、网络和设备遭到破坏的更强大的技术。

[0028] 本文描述的新颖系统、部件、装置、方法和技术解决与过程工厂及其网络相关的这些和其它安全问题，并且特别地涉及使得过程工厂/网络与其它网络或系统之间的通信安全。

[0029] 为了说明，图2是示例性过程工厂100的框图，其被配置为在在线操作期间控制工业过程，并且可以利用本文所描述的新颖安全技术中的任何一种或多种来保护。过程工厂100(其在文中也可以互换地称为过程控制系统100或过程控制环境100)包括一个或多个过程控制器，其接收指示由现场设备进行的过程测量的信号，处理该信息以实现控制例程，并生成通过有线或无线过程控制通信链路或网络发送到其它现场设备的控制信号以控制工厂100中的过程的操作。通常，至少一个现场设备执行物理功能(例如，打开或关闭阀、提高或降低温度、进行测量、感测条件等)以控制过程的操作。某些类型的现场设备通过使用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，并且有线和无线过程控制器、现场设备和I/O设备的任意数量和组合可以包括在过程工厂环境或系统100中。

[0030] 例如，图2例示了过程控制器111，其经由输入/输出(I/O)卡126和128通信地连接到有线现场设备115-122，并且经由无线网关135和过程控制数据高速通道或主干110通信地连接到无线现场设备140-146。过程控制数据高速通道110可以包括一个或多个有线和/或无线通信链路，并且可以使用任何期望的或适当的或通信协议(例如，以太网协议)来实现。在一些配置(未示出)中，控制器111可以使用除了主干110之外的一个或多个通信网络来通信地连接到无线网关135，例如通过使用支持一个或多个通信协议(例如Wi-Fi或其它遵循IEEE 802.11的无线局域网协议、移动通信协议(例如，WiMAX、LTE或其它ITU-R兼容协议)、Bluetooth®、HART、WirelessHART、Profibus、FOUNDATION®现场总线等)的任意数量的其它有线或无线通信链路。

[0031] 可以是例如由艾默生过程管理公司出售的DeltaV™控制器的控制器111可以进行操作以使用至少一些现场设备115-122和140-146来实现批量过程或连续过程。在实施例中，除了通信地连接到过程控制数据高速通道110之外，控制器111还使用任何期望的硬件和软件(其与例如标准的4-20mA设备、I/O卡126、128和/或任何智能通信协议(诸如现场总线协议、HART协议、WirelessHART®协议等)相关联)来通信地连接到现场设备115-122和140-146中的至少一些。在图2中，控制器111、现场设备115-122和I/O卡126、128是有线设备，并且现场设备140-146是无线现场设备。当然，有线现场设备115-122和无线现场设备140-146可以符合任何其它期望的标准或协议(例如任何有线或无线协议)，包括将来开发的任何标准或协议。

[0032] 图2的过程控制器111包括实现或监视一个或多个过程控制例程138(例如，储存在存储器132中)的处理器130。处理器130被配置为与现场设备115-122和140-146通信以及与通信地连接到控制器111的其它节点通信。应当注意，本文描述的任何控制例程或模块可以具有由不同的控制器或其它设备实现或执行的部分，如果需要的话。同样地，将在过程控制系统100内实现的本文描述的控制例程或模块138可以采取任何形式(包括软件、固件、硬件等)。控制例程可以以任何期望的软件格式来实现(例如使用面向对象的编程、梯形逻辑、顺序功能图、功能框图，或使用任何其它软件编程语言或设计范例)。控制例程138可以储存在任何期望类型的存储器132(诸如随机存取存储器(RAM)或只读存储器(ROM)等)中。同样地，控制例程138可以被硬编码到例如一个或多个EPROM、EEPROM、专用集成电路(ASIC)或任何其它硬件或固件元件。因此，控制器111可以被配置为以任何期望的方式来实现控制策略或控制例程。

[0033] 控制器111使用通常所称的功能块来实现控制策略，其中，每个功能块是整个控制例程的对象或其它部分(例如，子例程)，并且与其它功能块结合操作(经由称为链路的通信)以实现过程控制系统100内的过程控制回路。基于控制的功能块通常执行以下功能中的一个以在过程控制系统100内执行某些物理功能：诸如与变送器、传感器或其它过程参数测量设备等相关联的输入功能；诸如与执行PID、模糊逻辑等的控制例程相关联的控制功能；或控制诸如阀等的某些设备的操作的输出功能。当然，存在混合和其它类型的功能块。功能块可以储存在控制器111中并由控制器111执行，这通常是这些功能块用于标准4-20mA设备和某些类型的智能现场设备(例如HART®设备)或与标准4-20mA设备和某些类型的智能现场设备(例如HART®设备)相关联的情况，或可以储存在现场设备本身中并由现场设备本身实现，这可以是FOUNDATION®现场总线设备的情况。控制器111可以包括可以实现通过执行一个或多个功能块来执行的一个或多个控制回路的一个或多个控制例程138。

[0034] 有线现场设备115-122可以是任何类型的设备(诸如传感器、阀、变送器、定位器等)，而I/O卡126和128可以是符合任何期望的通信或控制器协议的I/O设备。在图2中，现场设备115-118是标准的4-20mA设备或HART®设备，其通过模拟线路或组合的模拟和数字线路与I/O卡126进行通信，而现场设备119-122是例如FOUNDATION®现场总线现场设备之类的智能设备，其使用FOUNDATION®现场总线通信协议在数字总线上与I/O卡128进行通信。然而，在一些实施例中，尽管有线现场设备115、116和118-121中的至少一些和/或I/O卡126、128中的至少一些另外地或替代地使用过程控制数据高速通道110，和/或

通过使用其它适当的控制系统协议(例如,Profibus、DeviceNet、Foundation Fieldbus、ControlNet、Modbus、HART等),来与控制器111进行通信。

[0035] 在图2中,无线现场设备140-146使用诸如WirelessHART®协议之类的无线协议经由无线过程控制通信网络170进行通信。这样的无线现场设备140-146可以直接与无线网络170的一个或多个其它设备或节点通信,这些设备或节点也被配置为进行无线通信(例如,使用无线协议或另一无线协议)。为了与未配置为进行无线通信的其它节点进行通信,无线现场设备140-146可以利用连接到过程控制数据高速通道110或另一个过程控制通信网络的无线网关135。无线网关135提供对无线通信网络170的各种无线设备140-158的访问。具体地,无线网关135提供无线设备140-158、有线设备115-128和/或过程控制工厂100的其它节点或设备之间的通信耦合。例如,无线网关135可以通过使用过程控制数据高速通道110和/或通过使用过程工厂100的一个或多个其它通信网络来提供通信耦合。

[0036] 与有线现场设备115-122类似,无线网络170的无线现场设备140-146执行过程工厂100内的物理控制功能(例如,打开或关闭阀、或进行过程参数的测量)。然而,无线现场设备140-146被配置为使用网络170的无线协议进行通信。因此,无线网络170的无线现场设备140-146、无线网关135和其它无线节点152-158是无线通信分组的生产者和消费者。

[0037] 在过程工厂100的一些配置中,无线网络170包括非无线设备。例如,在图2中,图2的现场设备148是传统的4-20mA设备,现场设备150是有线HART®设备。为了在网络170内通信,现场设备148和150经由相应的无线适配器152A、152B连接到无线通信网络170。无线适配器152A、152B支持例如WirelessHART的无线协议,并且还可以支持一个或多个其它通信协议(诸如Foundation®现场总线、PROFIBUS、DeviceNet等)。另外,在一些配置中,无线网络170包括一个或多个网络接入点155A、155B,其可以是与无线网关135进行有线通信的单独的物理设备,或者可以被提供有无线网关135作为整体设备。无线网络170还可以包括一个或多个路由器158,以将分组从一个无线设备转发到无线通信网络170内的另一个无线设备。在图2中,无线设备140-146和152-158在无线通信网络170的无线链路160上、和/或经由过程控制数据高速通道110彼此通信并且与无线网关135通信。

[0038] 在图2中,过程控制系统100包括通信地连接到数据高速通道110的一个或多个操作员工作站171。经由操作员工作站171,操作员可以查看和监控过程工厂100的运行时间操作,以及采取任何可能需要的诊断、纠正、维护和/或其它措施。至少一些操作员工作站171可以位于工厂100中或附近的各种保护区域(例如,在工厂100的后端环境中),并且在一些情况下,至少一些操作员工作站171可以远程地定位,但与设备100通信连接。操作员工作站171可以是有线或无线计算设备。

[0039] 示例性过程控制系统100被进一步例示为包括配置应用172A和配置数据库172B,配置应用172A和配置数据库172B中的每一个还通信地连接到数据高速通道110。如上所述,配置应用172A的各种实例可以在一个或多个计算设备(未示出)上执行,以使得用户能够创建或改变过程控制模块,并且经由数据高速通道110将这些模块下载到控制器111,以及使用户能够创建或改变操作员接口,经由该操作员接口,操作员能够在过程控制例程内查看数据和改变数据设置。配置数据库172B储存所创建的(例如,经配置的)模块和/或操作员接口。通常,尽管配置应用172A的多个实例可以在过程控制系统100内同时执行,但是配置应用172A和配置数据库172B是集中式的并且具有到过程控制系统100的统一的逻辑外观,并

且配置数据库172B可以是跨多个物理数据储存设备来实现。因此，配置应用172A、配置数据库172B及其用户接口(未示出)包括用于控制和/或显示模块的配置或开发系统172。通常，但不一定，用于配置系统172的用户接口不同于操作员工作站171，因为配置和开发工程师使用配置系统172的用户接口，而不管工厂100是否在实时操作，而操作员工作站171由操作者在过程工厂100的实时操作(本文也被互换地称为过程工厂100的“运行时间”操作)期间使用。

[0040] 示例性过程控制系统100包括数据历史库应用173A和数据历史库数据库173B，数据历史库应用173A和数据历史库数据库173B中的每一个还通信地连接到数据高速通道110。数据历史库应用173A操作以收集跨数据高速通道110提供的数据的部分或全部，并且将数据历史化或储存在历史数据库173B中用于长期储存。与配置应用172A和配置数据库172B类似，尽管数据历史库应用173A的多个实例可以在该过程控制系统100内同时执行，但是数据历史库应用173A和历史库数据库173B是集中式的，并且对于过程控制系统100具有统一的逻辑外观，并且数据历史库173B可以跨多个物理数据储存设备来实现。

[0041] 在一些配置中，过程控制系统100包括一个或多个其它无线接入点174，其使用其它无线协议(比如Wi-Fi或其它遵循IEEE 802.11的无线局域网协议、诸如WiMAX(全球微波接入互操作性)、LTE(长期演进)或其它ITU-R(国际电信联盟无线电通信部门)兼容协议等的移动通信协议、诸如近场通信(NFC)和蓝牙等的短波无线电通信或其它无线通信协议等)与其它设备通信。通常，这样的无线接入点174允许手持式或其它便携式计算设备(例如，用户接口设备175)通过与无线网络170不同的并支持与无线网络170不同的无线协议的相应无线过程控制通信网络进行通信。例如，无线或便携式用户接口设备175可以是由过程设备100内的操作员使用的移动工作站或诊断测试装备(例如，操作员工作站171中的一个的实例)。在一些情况下，除了便携式计算设备之外，一个或多个过程控制设备(例如，控制器111、现场设备115-122或无线设备135、140-158)还使用由接入点174支持的无线协议进行通信。

[0042] 在一些配置中，过程控制系统100包括通往在即时过程控制系统100外部的系统的一个或多个网关176、178。通常，这样的系统是由过程控制系统100生成或操作的信息的客户或供应商。例如，过程控制工厂100可以包括网关节点176，以将过程过程工厂100与另一过程工厂通信连接。另外或替代地，过程控制工厂100可以包括网关节点178，以将即时过程工厂100与外部公共或私人系统(诸如实验室系统(例如，实验室信息管理系统或LIMS)、操作员循环数据库、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、运输和处理系统、封装系统、互联网、另一供应商的过程控制系统或其它外部系统等)通信连接。

[0043] 注意，虽然图2仅例示了单个控制器111以及包括在示例性过程工厂100中的具有有限数量的现场设备115-122和140-146、无线网关35、无线适配器152、接入点155、路由器1158和无线过程控制通信网络170，这仅仅是说明性和非限制性的实施例。任意数量的控制器111可以包括在过程控制工厂或系统100中，并且任何控制器111可以与任意数量的有线或无线设备和网络115-122、140-146、135、152、155、158和170进行通信，以控制工厂100中的过程。

[0044] 图3例示了图1的示例性过程工厂100的示例性安全架构200的框图。为了参考，跨

图3的顶部描绘了来自图1的各个安全级别0-5，以指示在安全架构200的各个部分中可以包括的安全级别，然而，该参考仅仅是指导原则，因为安全架构200的各个部分可以以与图3所描绘的不同的安全级别来容纳。

[0045] 如图3所示，一个或多个设备202通信地连接到一个或多个无线网关205A、205B，无线网关205A、205B例如可以是图1的无线网关135的实例。如前所讨论的，无线网关205A、205B可以位于安全级别1和/或安全级别2(例如，在过程工厂100本身内)。网关205A、205B与设备202之间的通信连接由附图标记204A、204B表示。

[0046] 该组设备202被例示为处于过程工厂100的安全级别0，并且被描绘为包括有限数量的无线现场设备。然而，应当理解，本文关于设备202描述的概念和特征可以容易地应用于过程工厂100的任意数量的现场设备以及应用于任何类型的现场设备。例如，现场设备202可以包括有线现场设备115-122中的一个或多个，其经由过程工厂100的一个或多个有线通信网络110通信地连接到无线网关205A、205B，和/或设备202可以包括有线现场设备148、150，其耦合到无线适配器152A、152B，从而耦合到无线网关205A、205B。

[0047] 此外，应当理解，该组设备202并不仅限于生成过程数据的现场设备，而是可以附加地或替代地包括作为过程工厂100控制在线过程的结果而生成数据的过程工厂100内的任何设备或部件。例如，该组设备202可以包括生成诊断数据的诊断设备或部件、在过程工厂100的各个部件和/或设备之间传送信息的网络路由设备或部件等。实际上，图2所示部件中的任何一个或多个部件(例如，部件111、115-122、126、128、135、140-146、152、155、158、160、170、171-176、178)和图中未示出的其它部件可以是生成用于传送到远程系统210的数据的设备或部件202。因此，该组设备202在本文中可互换地被称为“数据源202”或“数据源设备202”。

[0048] 图3还例示了可以结合过程工厂100和/或由过程工厂100利用的一组远程应用或服务208。该组远程应用或服务208可以在一个或多个远程系统210处被执行或托管，并且一般而言，该组远程应用/服务208被认为处于安全级别5或更高级别。当实时数据由过程工厂100生成并由应用或服务208接收时，应用或服务208中的至少一些实时地操作实时数据。其它应用或服务208可以对过程工厂生成的数据进行不太严格的时序要求地操作或执行。示例性的应用/服务208可以在远程系统210处执行或被托管，并且可以是由过程工厂100生成的数据的消费者，应用/服务208的示例包括监控和/或感测在过程工厂100发生的状况和/或事件的应用，以及在过程工厂100正在执行时监控在线过程本身的至少一部分的应用程序或服务。应用/服务208的其它示例包括描述性和/或规范性分析，其可以对由过程工厂100生成的数据进行操作，并且在某些情况下，可以对通过分析过程工厂生成的数据而收集或发现的知识以及从其它过程工厂生成和接收的数据进行操作。应用/服务208的其它示例包括的一个或多个例程，其实现规范性功能、配置和/或其它数据的修改、和/或将被实施回到过程工厂100中的其它规定性改变(例如，作为另一服务或应用的结果)。应用和服务208的一些示例在2016年9月23日提交的题为“用于分布式工业性能监控的数据分析服务”的美国专利申请No.15/274,519中描述，并且在2016年9月23日提交的题为“分布式工业性能监控和分析”的美国专利申请No.15/274,233中描述，以及在2016年10月24日提交的题为“过程设备状况和性能监控”的美国专利申请No.15/332,521中描述，这些专利的全部公开内容通过引用并入本文。

[0049] 一个或多个远程系统210可以以任何期望的方式实现，例通过由远程联网服务器组(bank)、一个或多个云计算系统、一个或多个网络等。为了便于讨论，尽管可以理解为所述术语可以指一个系统、一个以上的系统或任意数量的系统，但是一个或多个远程系统210在本文中使用单数时态，即“远程系统210”来引用。

[0050] 一般而言，安全架构200提供从设备202安装和操作的过程工厂100的现场环境到远程系统210的端到端的安全性，远程系统210提供消费由过程工厂100生成的数据并且对由过程工厂100生成的数据进行操作的应用和/或服务208。因此，由设备202和过程工厂100的其它组件生成的数据能够被安全地传送到远程系统210以供远程应用/服务208使用，同时保护工厂100免受网络攻击、入侵和/或其它恶意事件。具体地，安全架构200包括设置在过程工厂100(例如，过程工厂100的无线网关205A、205B之间)与远程系统210之间的现场网关212、数据二极管215和边缘网关218。通常但不一定，现场网关212、数据二极管215和边缘网关218被包括在安全级别2-5中。

[0051] 安全架构200的关键方面是数据二极管215。数据二极管215是以硬件、固件和/或软件实现的部件，并且特别地被配置为防止过程工厂100与远程系统210之间的双向通信。换而言之，数据二极管215允许数据业务从过程控制系统100传输到远程系统210，并且防止数据业务(例如，从远程系统210或另一系统传送或传送的数据业务)进入过程控制系统100。

[0052] 因此，数据二极管215包括通信地连接到现场网关212的至少一个输入端口220和通信地连接到边缘网关218的至少一个输出端口222。数据二极管215还包括将其输入端口222连接到其输出端口222的任何其它适当技术的光纤或通信链路。为了防止数据业务流向(例如，进入)过程控制系统100，在示例性实现中，数据二极管215不包括或者省略从边缘网关218(或更高安全级别的其它部件)接收数据的输入端口，和/或排除或省略将数据传送到现场网关212(或较低安全级别的其它部件)的输出端口。在附加或替代实现中，数据二极管215不包括、省略和/或禁用将允许数据从输出端口222流向输入端口220的收发器，和/或不包括数据从输出端口222流向输入端口220的物理通信路径。另外或替代地，数据二极管215可以仅支持经由软件从输入端口220到输出端口222的单向数据流动，例如通过丢弃或阻止在输出端口222处从边缘网关218(或更高安全级别部件)接收的消息，和/或通过丢弃或阻止寻址到现场网关212(或较低安全级别部件)的任何消息。

[0053] 从过程工厂100发出并通过数据二极管215从输入端口220传送到输出端口222的数据可以通过跨数据二极管215进行加密以进一步保护。在一示例中，现场网关212加密数据并将经加密的数据传送到输入端口220。在另一示例中，数据二极管215从现场网关212接收数据业务，并且数据二极管215在将数据传送到输出端口222之前加密接收到的数据业务。在一示例中，跨数据二极管215加密和传输的数据业务可以是UDP(用户数据报协议)数据业务，并且在另一示例中，可以是JSON数据业务或一些其它通用通信格式。

[0054] 现场网关212将数据二极管215的较低安全侧通信连接到过程控制工厂100。如图3所示，现场网关212通信地连接到无线网关205A、205B，其设置在过程工厂100的现场环境内，并且通信地连接到一个或多个设备或数据源202。如前所述，设备或数据源202和无线网关205A、205B可以使用构造成经由一个或多个安全机制提供安全通信WirelessHART工业协议或其它适当的无线协议进行通信。例如，WirelessHART工业协议提供128位AES加密，并且

可以相应地保护通信路径204A、204B。

[0055] 另外，无线网关205A、205B与现场网关212之间的通信连接225分别使用与通信连接204A、204B所使用的相同或不同的安全机制来保护。在一示例中，通信连接225由TLS(传输层安全)封装(wrapper)来保护。例如，无线网关205A、205B生成HART-IP格式的分组，这些分组由TLS封装器保护，用于传送到现场网关212。

[0056] 因此，如上所述，在一实施例中，可以使用第一安全机制来保护由设备202生成的数据或分组，以便将204A、204B传送到无线网关205A、205B，并且随后使用第二安全机制保护，以便将225从无线网关205A、205B传送到现场网关212，并且仍然随后使用第三安全机制保护，以便跨数据二极管215传送。

[0057] 现在转向数据二极管215的较高安全侧，如果需要，可以通过使用第四安全机制、或者通过使用上述讨论的数据二级管215的较低安全侧上所采用的安全机制中的一种来保护从数据二极管215运出的数据业务，以运送到边缘网关218。附加地或替代地，并且如图3所示，边缘网关218可以由防火墙228保护，防火墙228可以是图1的防火墙12C或另一防火墙。

[0058] 可以使用一个或多个公共和/或专用网络(诸如专用企业网络、互联网、蜂窝路由器、回程互联网或其它类型回程连接)来传送从边缘网关218向远程系统210运送的数据。重要的是，通过使用第五安全机制或通过使用先前讨论的安全机制中的一种来保护从边缘网关218向远程系统210运送的数据。图3描绘了经由SAS(共享访问签名)令牌进行保护的从边缘网关218向远程系统210传送的数据流量，该SAS(共享访问签名)令牌可通过在远程系统210处提供的令牌服务230来管理。边缘网关218认证到令牌服务230并请求SAS令牌，其可以仅在有限的时间段(例如，两分钟、五分钟、三十分钟、不超过一个小时等内有效。边缘网关218接收并使用SAS令牌来保护和认证到远程系统210的AMQP(高级消息队列协议)连接，内容数据经由远程系统210从边缘网关218传送到远程系统210。当然，使用SAS令牌和AMQP协议来保护在边缘网关218与远程系统210之间的运送的数据只是许多可能的安全机制中的一种。例如，可以利用任何一种或多种适当的物联网(IOT)安全机制来保护在边缘网关218与远程系统210之间的运送的数据(例如，X.509证书、其它类型的令牌、诸如MQTT(MQ遥测传输)或XMPP(可扩展消息传送和存在协议)之类的其它IOT协议，等等)。在这些其它实施例中，服务230例如提供和/或发出适当的安全令牌或证书。

[0059] 在远程系统210处，用户认证和/或授权由任何一个或多个适当的认证和/或授权安全机制232提供。例如，对远程系统210的安全访问可以由域认证服务、API用户认证服务和/或任何其它适当的认证和/或授权服务232提供。因此，仅经由认证和/或授权服务232认证和/或授权的用户235能够访问在远程系统210处可用的至少一些数据，该数据特别包括由设备202生成的数据。

[0060] 因此，如上所述，安全架构200在过程工厂100中操作时为在设备或数据源202生成的数据提供端到端的安全性，以控制过程，例如根据由数据源202通过其传输到远程系统210以由一个或多个远程应用或服务208进行操作的数据的初始化。重要的是，安全架构200在防止在过程工厂100上发生恶意攻击的同时提供这种端到端安全性。

[0061] 注意，尽管图3描绘了将设备或数据源202通信地连接到现场网关212的无线网关205A、205B，但是在一些布置中，省略了无线网关205A、205B中的一个或多个，并且源数据被

从数据源202直接传送到现场网关212。例如，数据源202可以经由过程工厂100的大数据网络将源数据直接传送到现场网关212。一般而言，过程工厂100的大数据网络不是主干工厂网络110，也不是用于使用工业通信协议(例如，Profibus、DeviceNet、Foundation Fieldbus、ControlNet、Modbus、HART等)在设备之间传送控制信号的工业协议网络。相反，过程工厂100的大数据网络可以是为过程工厂100实现的重叠网络，其例如为了数据处理和分析目的的节点之间串流数据。大数据网络的节点可以包括例如数据源202、无线网关205A、205B和现场网关212，以及图2所示的部件111、115-122、126、128、135、140-146、152、155、158、160、170、171-176、178中的任何一个或多个，以及其它部件。因此，对于过程工厂数据网络的许多节点，分别包括通常利用工业通信协议的用于过程工厂操作的指定接口，以及例如可以利用流传输协议的用于数据处理/分析操作的另一指定接口。可以在过程工厂100中使用的大数据网络的示例在2014年10月6日提交的题为“过程控制系统的区域大数据”的美国专利申请No.14/507,188中描述，该专利申请的全部公开内容通过引用并入本文。

[0062] 关于图3进一步注意到，在一些实施例中，有线网关(未示出)可以用于代替无线网关205A、205B中的一个。此外，现场网关212、数据二极管215和边缘网关218可以在物理上位于同一位置，例如由图3所示的框235所示，或者部件212、215、218中的一个或多个可以跨多个位置物理定位。例如，现场网关212、数据二极管215或边缘网关218中的一个或多个可以设置在过程工厂100处。附加地或替代地，现场网关212、数据二极管215或边缘网关218可以远离过程厂100设置。

[0063] 如果需要，过程工厂100可以由多于一个现场网关212服务，并且任意数量的现场网关210可以由单个边缘网关218服务。在一些实施例中，如果需要，远程系统210由多于一个边缘网关218服务。

[0064] 如前所述，跨数据二极管215传输的数据业务得到了保护。这样的数据业务可以例如通过使用串行通信或UDP通信进行通信。然而，保护这种没有双向通信的通信是困难和麻烦的，因为通常UDP和串行通信都要求双方不仅双向通信(这使用数据二极管215是不可能的)，而且还要记住并且进入长键序列。因此，可以经由在边缘网关218与现场网关212之间使用的安全提供过程来保护所传输的数据，而不是使用传统的双向通信来保护跨单向数据二极管215的数据传输。安全提供过程建立在边缘网关218与现场网关212之间共享的独特的初始密钥或秘密材料(例如，对称密钥或对称材料)，例如连接密钥。使用连接密钥，边缘网关218和现场网关212建立用于交换进一步的密钥或秘密材料的安全连接，这转而用于跨数据二极管215安全地传输数据流量。

[0065] 图4描绘了可以用于安全供应过程的示例性消息流250。在图4中，现场网关212和边缘网关218都包括在供应网络(例如，相同的子网，未示出)上，供应服务器或计算设备252也包括在供应网络上，供应服务器或计算设备252由用户操作以向边缘网关218供应现场网关212。在一个实施例中，经由供应网络，现场网关212和边缘网关218能够彼此临时地双向通信以例如使用TCP类型通信建立供应。

[0066] 例如，在附图标记255处，用户经由供应设备252登录到边缘网关218的用户界面(UI)，并且向其进行认证。例如，边缘网关218的UI可以是web界面或一些其它适当的UI。经由边缘网关218的供应页面或显示视图，用户输入现场网关212(附图标记258)的地址(在示

例中可以是IP地址)，从而使得边缘网关218创建网关212的白名单条目(附图标价260)。随后，边缘网关218向供应设备252请求将用于数据传输的现场网关212的凭证(附图标记262)。

[0067] 响应于边缘网关的请求，用户经由供应设备252提供现场网关212的授权和安全信息(附图标记265)。所述授权和安全信息通常(但不一定)包括将与现场网关212共享的初始密钥材料。在一示例中，初始密钥材料包括128位、192位或256位连接密钥，并且包括32位或64位分组计数器，其可以用作用于分组加密/解密并且在一些情况下用于对分组执行的MIC(消息完整性校验)计算的随机数的一部分。例如，分组计数器的值在每个传输的随机数中递增、改变或更新，以帮助抵御网络重放攻击。无论如何，边缘网关218加密并储存初始密钥材料的本地副本，并将初始密钥材料以及边缘网关218的一个或多个地址(例如，边缘网关218的IP地址和/或MAC地址)发送到现场网关212(附图标记268)。在现场网关212处，现场网关212加密并储存初始密钥材料的本地副本以及边缘网关218的地址，并确认接收到边缘网关218(附图标记270)。

[0068] 随后，现场网关212例如通过使用UDP发起跨数据二极管215的与边缘网关218的单向通信。具体地，现场网关212向边缘网关218传送初始消息，其包括将被用于加密和完整性校验后续消息的新的随机生成的网络密钥和随机生成的分组计数器(例如，将用于随机数和MIC计算)。新的网络密钥和相应的分组计数器(例如连接密钥及其相应的分组计数器(附图标记272))使用初始密钥材料来加密。边缘网关218使用其本地储存的初始密钥材料来解密所接收的初始消息，储存新的网络密钥和分组计数器(附图标记275)，并且使用分组计数器中所储存的网络密钥来解密随后从现场网关212接收的消息或分组。

[0069] 注意，如图4所示，在边缘网关218从现场网关212接收已经使用新的网络密钥加密并包括新的分组计数器(附图标记278、280)的第一消息时，所保护的供应过程可以被认为是完整的，并且供应设备252可能不再被包括在消息流250中。结果，在一实施例中，用于从边缘网关218到现场网关212的通信的临时通信信道(例如，在附图标记268处所使用的)被拆除、禁用或以其它方式不可用。然而，现场网关212使用所储存的网络密钥和分组计数器继续跨单向数据二极管215发送数据到边缘网关218(附图标记282)，并且边缘网关218使用其储存的网络密钥和分组计数器继续解密所接收的消息(附图标记285)。

[0070] 然而，在一些实施例中，在供应设备252与网络断开连接时，或者在消息流250期间早期，现场网关212和边缘网关218恢复为跨数据二极管215的单向通信。例如，在将初始连接密钥材料传送到现场网关212(附图标记268)时，边缘网关218可以恢复为单向通信，并且在传送接收到初始密钥材料的确认(附图标记270)时，现场网关212可以恢复为单向通信)。

[0071] 为了跨单向数据二极管215的数据传输的鲁棒性和可靠性，现场网关212生成另一初始化消息和相应的随机分组计数器，以与边缘网关218建立新的或更新的网络密钥材料。例如，网关212传送使用初始连接密钥材料加密并且包括新的或更新的网络密钥以及相应的新的或更新的分组计数器的另一个初始化消息(附图标记288)。初始连接密钥材料预先储存在现场网关212和边缘网关218处(参见例如附图标记265、268、270)，并且例如更新的网络密钥和随机分组计数器在现场网关212处被随机生成。

[0072] 在附图标记290处，边缘网关218例如通过检查接收到新的初始化消息的白名单和/或地址来验证接收到的初始化消息。如果边缘网关218确定接收到的新的初始化消息有

效，则边缘网关218使用其本地储存的初始连接密钥材料解密初始化消息，并且保存新的/更新的网络密钥和其中包含的随机分组计数器以用于处理从现场网关212接收的未来消息。例如，现场网关212可以发送使用新的/更新的网络密钥和随机分组计数器加密的后续消息(附图标记292、295)，并且边缘网关218使用所储存的新的/更新的网络密钥和随机分组计数器来解密所接收的消息(附图标记298、300)。

[0073] 现场网关212重复发送新的或更新的初始化消息(例如，附图标记275、288等)以循环地或周期性地或者在需要时建立更新的或新的网络密钥和相应的随机分组计数器，例如，作为用户命令或另一事件的发生的结果。由于现场网关212与边缘网关218之间的通信是跨数据二极管215单向的，所以现场网关212没有明确确认边缘网关218确实正在接收由现场网关212传送的数据。因此，现场网关212循环地发送包括新的/更新的网络密钥和相应的随机分组计数器的新的/更新的初始化消息，能够重新同步现场网关212与边缘网关218之间共享的网络密钥材料。这种重新同步技术允许在错误或故障状况下(例如当边缘网关发生故障并被替换或重启时，和/或当丢失分组时)进行恢复。网络密钥材料重新同步的时间段长度可以依赖于应用，例如，可以由应用(例如，应用或服务208中的一个)的容限来限定丢失的分组或数据，并且可以是可配置的。

[0074] 因此，如上所述，储存在边缘网关218(附图标记268)和现场网关212(附图标记270)处的初始供应的连接密钥和随机分组计数器或随机数材料被用于加密/解密提供初始随机网络密钥和随机分组起始计数器的初始化消息(附图标记275)，随后的通信利用包含在初始化消息中的随机网络密钥和分组计数器来对其中传送的数据进行加密/解密。循环地、周期性地和/或根据需要，现场网关212生成使用初始连接密钥材料来加密/解密的新的或更新的初始化消息，并且提供新的/更新的随机网络密钥和随机分组开始计数器(附图标记288)。在新的/更新的初始化消息之后发送的通信受新的/更新的随机网络密钥和分组计数器的支配以加密/解密在其中传送的数据。因此，边缘网关218可以在有限的时间内同时储存先前使用的网络密钥信息和新的网络密钥信息，以便能够处理在转换到新的网络密钥信息时可能混乱到达的分组。

[0075] 如图4所示，消息流250利用供应网络和供应设备252来执行现场网关212与边缘网关218之间的安全供应过程。然而，这仅是许多可能的实施例中的一个。

[0076] 例如，在另一实施例中，现场网关212和边缘网关218不在供应网络上，并且甚至可能不在同一网络上。在本实施例中，为了安全地供应现场网关212和边缘网关218，用户直接向边缘网关218进行认证，并提供描述现场网关212的安全信息或数据。例如，用户提供用于其在边缘网关218处的白名单条目的现场网关212的IP地址，并且用户提供安全信息或初始密钥材料，例如，以与上文中讨论的图4中的附图标记265类似的方式。安全信息被加密并储存在边缘网关218处以用于与现场网关212的通信。另外，加密的安全信息被保存到分离的文件，其也可以分别被加密。分离的文件例如由用户传输到现场网关212。用户直接对现场网关212进行认证，并提供分离的文件以供在现场网关212处使用。现场网关212验证分离的文件(如果需要，则对文件进行解密)，获得其中储存的安全信息(例如，初始密钥材料)，加密所获得的安全信息，并且本地储存加密安全信息以供跨数据二极管215与边缘网关218的将来通信中使用。

[0077] 在另一实施例中，代替UDP，使用串行通信跨数据二极管215传输数据。在该实施例

中，安全的供应过程可以类似于上述用于供应现场网关212和边缘网关218的安全供应过程，而网关212、218不在供应网络上或者在分离的网络上。

[0078] 在一些实现中，跨数据二极管215的安全的TCP、UDP和/或串行通信之下，用于跨数据二极管215传送过程工厂生成的数据的通信协议可以是经修改的HART-IP协议，或者可以是例如对任何已知的工业通信协议(例如现场总线)的修改。

[0079] 为了使用HART-IP协议作为说明性但非限制性的示例，可以利用HART-IP协议可以被利用来进一步向从在过程工厂100中操作的设备102到远程系统210的端到端通信提供附加安全性。具体地，包括在HART-IP和HART中的发布机制以独特的方式被利用以支持跨数据二极管215的单向通信，使得在过程工厂100处生成的数据可以经由跨数据二极管215在现场网关212与边缘网关218之间传送的消息或分组(例如，如图4中的附图标记278、282、292、295所示)而被传送到远程应用208。

[0080] 经修改的HART-IP协议分组可以是令牌传递数据链路层帧格式，和/或可以是直接/无线分组格式。例如，可以修改HART-IP报头以包括例如安全类型的指示的安全信息(例如，作为报头的消息类型字段中的值)，Hart-IP会话初始化消息可以被修改为包括初始安全密钥材料信息和/或其它HART消息类型(例如，请求、响应等)可以被修改为包括网络安全密钥字段和网络安全计数器字段。

[0081] 图5中示出了用于保护跨数据二极管215的通信的经修改的HART-IP协议的示例性使用。图5描绘了示例性消息流400，其可用于将由一个或多个发送设备402跨数据二极管215生成的过程工厂数据传送到一个或多个接收设备405。一般而言，发送设备402首先向接收设备405提供发现信息，以设置将被跨数据二极管215传送的内容或有效载荷数据的上下文。发现信息允许接收设备405了解哪些数据生成部件或设备处于数据二极管215的过程工厂侧上、将由过程工厂侧部件生成的数据的类型和/或标识、预期到达接收设备405的速率、各种数据生成部件或设备的状态等。重要的是，发现信息允许接收设备405获得这种知识，而不需要接收设备405询问或查询数据二极管215的过程工厂侧上的部件设备，这些是接收设备405由于数据二极管215的单向性而不能做。

[0082] 在发送设备402已经将发现信息提供给接收设备405之后，例如当发送设备402生成源数据时和/或当发送设备402从过程工厂100内的一个或多个其它部件接收源数据时，传送设备402根据发现消息中实时提供的上下文使用经修改的HART-IP协议公布跨数据二极管215的内容或有效载荷数据。同样地，接收设备405可以是由发送设备402发布的数据的订户。

[0083] 另外，还由于数据二极管215的单向特性，发送设备402不能识别接收设备405的状态(例如，接收设备405是否可操作的、电源循环的、断开连接的等)，并且不能明确地确定接收设备405是否已经接收到发送的数据。因此，发送设备402循环地(例如，周期性地和/或根据需要)向接收装置405提供、发送或宣布发现信息，使得如果接收设备405恰好不可用，则在恢复时接收设备405能够快速(重新)理解由发送设备402发送的内容或有效载荷数据的上下文。发送发现信息之间的时间段长度可以取决于针对丢失的分组或数据的数据二极管215的接收设备侧的客户端应用的容限(例如，远程应用或服务208中的一个)，并且可以是可配置的。当发送设备402侧发生变化时，例如当将数据源202和/或无线网关205被添加到过程工厂100或从过程工厂100移除时，也可以传送发现信息。

[0084] 发送设备402可以是现场网关212、无线网关205、数据源设备202和/或提供由过程工厂100内操作的一个或多个部件或设备生成的数据的任何其它部件。接收设备405可以是边缘网关218、包括远程系统210的一个或多个设备和/或作为源数据(例如,远程应用或服务208中的一个)的消费者的客户端应用。然而,在图5中,为了便于讨论,讨论了消息流400,就好像发送设备402是图3的现场网关212,并且接收设备405是图3的边缘网关218,尽管它被理解为这仅是许多可能的实施例中的一个。

[0085] 在上下文设置阶段408期间,发送设备402传送描述过程工厂100的每个数据源的相应信息,每个数据源的数据将被跨数据二极管215传送。描述性数据源信息包括例如数据源的标识(例如,唯一标识符、设备标签等);数据的标识(其可以包括例如将信息映射到其动态变量(诸如主变量(PV)、次级变量(SV)、第三变量(TV)、第四变量(QV)等等)中的一个或多个);对所识别的数据预期到达的速率的指示(例如,突发配置信息);和/或描述数据和/或数据源的其它信息(诸如指示数据源通信连接到的特定网关的数据、数据源的状态、其网关的状态等)。如图5所例示,在一实施例中,发送设备402在上下文设置阶段408期间基于每个数据源设备202在每个无线网关205上进行迭代。例如,发送设备402发送无线网关0(附图标记410)的描述信息,无线网关0可以是例如无线网关205A、205B中的一个。发送设备402可以例如通过使用经修改的HART-IP命令0、20或74来发送无线网关0的描述信息。随后,发送设备402例如通过使用经修改的HART-IP命令0、20、50、105发送通信地连接到网关0(附图标记412)的N个设备中的每一个的相应的描述信息,以及可选地用于子设备突发映射的命令74和101。为M个网关中的每一个重复该序列,并且上下文设置阶段408在网关M及其相应的N个设备的描述信息已被传送到接收设备405之后结束(附图标记415、418)。

[0086] 在发布阶段420期间,发送设备402在上下文设置阶段408期间针对上下文被设置的任何数据源设备202跨数据二极管215发布源数据。在一示例中,发送设备402通过使用经修改的HART-IP命令48或其它适当的Hart-IP命令来跨数据二极管215发布源数据。特定的源数据以在发送设备402处接收(例如,经由其相应的无线网关205从设备202接收)的源数据的速率发布。换言之,在过程工厂100的在线操作期间,由过程工厂100生成的源数据在其被发送设备402接收时跨数据二极管215实时地发布。注意,过程工厂100的一些数据生成部件(例如,一些数据源设备202和/或一些无线网关205)可以将数据直接发布到现场网关212以供跨数据二极管215传送。过程工厂100的其它数据生成部件(例如,其它数据源设备202和/或无线网关205)可能不支持发布,并且现场网关212可以轮询这些类型的设备/网关以便接收它们相应的源数据。例如,现场网关212可以基于不支持发布的设备/网关的突发配置进行轮询(例如通过使用HART-IP命令3或9)。

[0087] 如先前所讨论的那样,在经过预定义的时间段之后或者根据期望,上下文信息410-418中的至少一些由发送设备402重新发送或更新到接收设备405。在一个实施例中,网关0-M和相应的设备1-N的上下文数据410-418的整体重新发送或更新。在另一个实施例中,针对特定设备的特定上下文数据例如基于特定消费者对丢失数据或分组的容限,按照数据的特定消费者所需要的不同时间重新发送或更新。在这些实施例中,不同的设备可以具有它们相应的上下文数据被重新发送或更新的不同的周期性或间隔。

[0088] 另外,注意,在其中数据二极管215是以太网连接的数据二极管的实施例中描述了上述消息流400。然而,如果需要,类似的技术可能容易地应用于串行地进行连接的数据二

极管。此外，尽管使用HART-IP协议描述了上述消息流400，但是可以在消息流400的上下文阶段408和数据传送阶段420期间使用其它通信协议。在一些示例性配置中，可以使用除了HART-IP之外的工业通信协议(例如Profibus、DeviceNet、Foundation现场总线、ControlNet、Modbus、HART等)。在其它示例性配置中，可以在消息流400的上下文阶段408和数据传送阶段420期间利用未专门为工业通信设计的其它协议。

[0089] 例如，在一个实施例中，可以使用JSON(JavaScript对象符号)格式而不是使用HART-IP来跨数据二极管215传送分组。在该实施例中，现场网关212将从过程工厂100内的各种设备和部件接收的数据转换为JSON格式以供跨数据二极管215传送。如果需要，可以添加对JSON分组数据的增强，诸如提供具有附加含义的标签(例如“压力”代替“PV”，各种数据值的设备特定标签等)。

[0090] 此外，虽然上述图5的讨论描述了消息流400的发生，就好像发送网关402是现场网关212而接收设备405是边缘网关218一样，但这仅仅是许多实施例中的一个实施例。例如，在消息流400的其它实施例中，发送设备402可以是现场网关212、无线网关205、数据源设备202和/或提供在过程工厂100内操作的一个或多个部件生成的数据的任何其它部件，并且接收设备405可以是边缘网关218、包括远程系统210的一个或多个设备和/或作为源数据的消费者的客户端应用(例如远程应用或服务208中的一个)。例如，客户端应用208中的第一客户端应用可以订阅由跨数据二极管215发布的特定设备202生成的数据，并且客户端应用28中的第二客户端应用可以订阅由另一个特定设备202生成的数据。在该示例中，边缘网关218可以用作路由器，以将接收到的数据分发到相应的数据订户的。在另一示例中，边缘网关218经由数据二极管215发布其接收的所有数据，并且各种应用程序208订阅由边缘网关218发布的特定数据。其它发布者/订户关系是可能的，并且可以由本文描述的安全通信技术中的任何一种或多种支持。

[0091] 另外，安全通信技术中的任何一种或多种可以容易地应用于使得被传送到过程工厂100本地的系统和/或设备的数据安全。例如，相应的数据二极管215和/或安全架构200的实例可用于跨过程工厂100的DMZ 22发布所选择(或甚至全部)数据，使得在过程工厂100的安全级别0-3处生成的数据经由相应的数据二极管跨DMZ 22被安全地传送到处于4-5级的企业级系统。在另一示例中，相应的数据二极管215和/或安全架构200的实例可用于将选定(或甚至全部)数据从设置在过程工厂100中的一个或多个数据源202发布到也被设置在过程工厂100中或本地并且托管或提供本地服务和应用的一个或多个本地服务器。这样的配置是有益的，例如，当本地服务和应用生成将被下载或以其他方式实现到在线过程工厂100中的本地规定性改变时，尽管通常，规定性功能、对配置和/或其它数据的修改、和/或其它改变可以通过远程定位的应用和服务208被实现到过程工厂100中。

[0092] 应注意，由应用/服务208确定的任何规定性改变通常经由数据二极管215以外的其它通信机制实现到过程工厂100中，因为数据二极管215相对于过程工厂100的出口方向是单向的。例如，为了实现对过程工厂100的规定性改变，远程应用/服务208可以建立除经由数据二极管215之外与过程工厂100的一个或多个管理或后端部件(例如操作员工作站171、配置应用172A、配置数据库173B等)的安全通信连接，并且规定性改变可以被下载或以其他方式传送到过程工厂100。事实上，在一个实施例中，数据二极管215和/或安全架构200的另一实例可以在入口方向上建立，以安全地传送从远程应用/服务208到过程工厂100的

任何规定性改变。

[0093] 此外，一般而言，从远程系统210到过程工厂210的任何入口通信通常利用除出口数据二极管215和/或出口安全架构200之外的通信机制。例如，远程系统210可以利用在入口方向上应用的数据二极管215和/或安全架构200的另一实例或一些其它适当的安全连接或通信路径。

[0094] 现在返回到来自过程工厂100的安全的出口通信，图6描绘了用于从过程工厂(例如图2的过程工厂100的)安全地传输通信的示例性方法450的流程图。在一些实施例中，方法450的至少一部分通过执行储存在一个或多个非暂时性计算机可读存储器上并由一个或多个处理器(例如系统200的)执行的一组计算机可执行或计算机可读指令集合来实现。例如，方法450的至少一部分可以由图1-5中描绘的系统200的一个或多个部件(例如现场网关212或发送设备402)来执行。因此，下面同时参考图1-5来描述方法450；然而，这仅仅是为了便于解释，而不是为了限制的目的。

[0095] 在方框452处，方法450包括向接收设备供应过程工厂的发送设备。发送设备通信地连接到过程工厂(例如经由一个或多个适当的网络)，并且接收设备例如通信地连接到另一个系统(例如经由一个或多个适当的网络)。另一个系统托管一个或多个应用或服务，这些应用或服务被配置为对由过程工厂在其运行时间操作期间生成的数据进行操作以及可选地对由过程工厂生成的其它数据进行操作。发送设备可以是例如发送设备402，并且接收设备可以是例如图5所例示的接收设备405。因此，发送设备402可以是现场网关212、数据源设备202、无线网关205或过程工厂100的另一部件，并且接收设备可以是边缘网关218、包括在远程系统210中的计算设备、或在远程系统210处执行的应用或服务208。当然，发送设备和/或接收设备的其它实施例(例如诸如任何先前讨论的那些)是可能的。

[0096] 发送设备和接收设备经由诸如图3的数据二极管215的数据二极管互连。数据二极管被配置为允许从发送设备向接收设备传送单向通信，并且将防止任何通信从接收设备传送到发送设备(在实施例中，除了初始供应消息之外)。

[0097] 向接收设备供应发送设备(框452)使用也被称为连接密钥的第一密钥来执行。连接密钥可以是秘密密钥或共享密钥，并且可以由用户例如经由通信地连接到发送设备和/或接收设备的供应设备或者经由手动数据传输来提供。在一些布置中，与连接密钥一起提供第一分组计数器(也称为连接分组计数器)或其它相应的随机数材料。如果需要，可以随机生成连接密钥和/或连接分组计数器。

[0098] 在一些实施例中，向发送设备供应接收设备(框452)包括建立临时通信信道，以允许从接收设备到发送设备的通信来传送和/或验证连接密钥。临时通信信道可以经由数据二极管建立，或者可以经由诸如外部有线或无线连接的某些其它通信连接、经由便携式储存设备的手动传送等建立。在这些实施例中，在接收设备传送连接密钥和/或在发送设备处接收连接密钥时，临时通信信道可能被废除、拆除或以其他方式被禁用。一般而言，临时通信信道只用作共享发送设备与接收设备之间的第一或连接密钥。在初始密钥材料(例如连接密钥及其相应的分组计数器或其它随机数材料)已被共享之后，初始密钥资料被本地加密并分别储存在发送设备和接收设备两者之上。

[0099] 方法450包括例如由发送设备使用第一或连接密钥加密初始化消息(框455)，并且将经加密的跨数据二极管的初始化消息提供给接收设备(框458)。该初始化消息中包括在

其中的第二密钥，本文中也称为网络密钥，该密钥将由发送和接收设备用于处理跨数据二极管从发送设备传送到接收设备的后续消息或分组。例如，第二密钥可能是另一个秘密密钥或共享密钥。使用第二或网络密钥处理的后续消息或分组中的至少一些包括内容或有效载荷，其包括由过程工厂在实时操作以控制过程时生成的数据(例如生成的过程数据、诊断数据、和其它类型的数据)。在一些布置中，第二分组计数器(也称为网络分组计数器)或其它相应的随机数材料被加密并结合将被用于处理后续消息/分组的网络密钥提供。如果需要，可以随机生成网络密钥和/或网络分组计数器。

[0100] 因此，方法450还包括在发送设备处接收由过程工厂在实时操作以控制过程时生成的数据(框460)；通过发送设备并且使用网络密钥以及可选的网络分组计数器来加密包括过程工厂生成数据的后续消息/分组作为有效载荷(框462)；以及将经加密的跨数据二极管的后续消息/分组提供给接收设备(框465)。因此，在框462、465处，至少其中一些包括由过程工厂生成的数据的后续消息/分组确保用于使用共享秘密网络密钥跨数据二极管传输。在一些实施例中，如果需要(未示出)，进一步使得后续消息/分组确保通过附加加密跨数据二极管传输。

[0101] 接收由过程工厂在实时或在线操作期间以控制过程而生成的数据(框460)可以包括直接从数据生成源(例如设备或部件202)接收数据，和/或可以包括从网关(例如无线网关205)接收从数据生成源(例如设备或部件202)传送到网关的数据。在发送设备处接收到的过程工厂生成的数据可能已经被数据生成源(例如设备或部件202)和/或被网关(例如无线网关205)以例如先前描述的方式加密、封装、和/或另外使其安全。

[0102] 接收到的过程工厂生成的数据(框460)可以包括已发布的数据，当一些数据生成源设备可以将其相应生成的数据发布到例如无线网关205和/或发送设备402时。其它数据生成源设备可以被轮询(例如由无线网关205和/或由发送设备402)，使得它们相应生成的数据可以在发送设备处被接收(框460)。此外，根据任何适当的工业通信协议或通用的通信协议，过程工厂生成的数据(无论是发布的、轮询的还是以其他方式接收的)(框460)可以是HART兼容格式、JSON兼容格式或其他适当的格式。

[0103] 如前所述，将包括过程工厂生成数据的消息/分组加密作为有效负载(框462)包括使用网络密钥和可选地使用网络分组计数器来加密所述消息/分组，例如，作为随机数材料，并且跨数据二极管的消息/分组的传输通过数据二级管的单向通信配置来进一步得以确保。

[0104] 另外，向接收设备提供或发送经加密的跨数据二极管的后续消息(框465)可以包括例如跨数据二极管向接收设备循环地通知或发送描述过程工厂的一个或多个数据生成设备中的每一个的相应的上下文信息。该相应的上下文信息可以包括目标数据生成设备的标识符、由目标设备生成的数据将被发送或发布的相应速率、目标数据生成设备的当前状态的指示和/或描述目标数据生成装置的其他信息，例如上面参照图5所讨论的。

[0105] 在一个示例中，循环通知上下文信息可以包括跨数据二极管周期性地向接收设备发送上下文信息。对于不同类型的内容数据、对于过程工厂的不同数据生成源和/或内容数据的不同消费者(例如远程应用程序208)，周期的持续时间可能不同。例如，某些类型的内容数据的周期的持续时间可以基于消费者对丢失分组的数据的容限和/或延迟。当然，当如用户所指示的，新的数据产生装置被添加到处理工厂时，上下文信息可以跨数据二极管公

布，例如在发送装置重启之后。

[0106] 此外，在一个实施例中，通知上下文信息可以包括利用工业通信协议的一个或多个消息类型。例如，当某种类型的HART通信协议跨数据二极管上利用时，通知上下文信息可以包括使用HART命令0、20、50、74、105以及可选择的命令74和101。在另一个实施例中，通知上下文信息可以使用通用通信协议(例如JSON或某些其他合适的通用通信协议)来实现。在一个示例中，可以修改各种工业通信协议的各种消息类型以适应通知。

[0107] 向接收设备提供经加密的跨数据二极管的后续消息(框465)还包括根据先前发送的上下文信息发送或传输跨数据二极管的内容数据。如前所述，内容数据包括在线工作时由处理工厂生成的动态数据，以控制过程，例如过程数据、诊断数据等。在一个实施例中，跨数据二极管提供经加密的后续消息包括例如以上述方式跨数据二极管公布内容数据。

[0108] 方法450还包括使用第一或连接密钥加密第二(即后续的)初始化消息(方框468)，并且向接收设备提供经加密的跨数据二极管的第二初始化消息(框470)。第二初始化消息包括更新的或新的网络密钥，该网络密钥被后续消息或分组的发送设备和接收设备利用，该后续消息或分组的跨数据二极管从发送设备传输到接收设备。更新的或新的网络密钥可以是与关于块452所讨论的连接密钥不同的另一个共享密钥或共享密钥，并且不同于关于块455、458所讨论的网络密钥。更新的或新的也可用于处理后续消息/分组的网络分组计数器可以与更新的或新的网络密钥一起跨数据二极管来生成和传输。如果需要，可以随机生成新的或更新的网络密钥和/或分组包计数器。

[0109] 因此，在框468、470处，由发送设备和接收设备用于处理消息/分组的网络密钥被重新同步。这种重新同步至关重要，因为数据二极管是单向的，因此接收设备不能向发送设备提供关于其操作状态、成功或不成功接收消息的任何反馈。然而，通过块468、470，方法450能够通过重新同步网络密钥材料来解决发送设备和接收设备之间的通信断开。实际上，在一些实施例中，块468、470被循环地、周期性地和/或基于某些事件的发生(例如当用户根据需要而指示以重新启动发送设备等等)重复。例如，周期性的持续时间可以基于丢失分组的内容数据的一个或多个消费者的容限和/或延迟。

[0110] 注意，对于块468、470，接收设备可能需要在有限的时间段内维护第一网络密钥/分组计数器和第二网络密钥/分组计数器，例如用于处理以不同顺序跨数据二极管发送的分组。

[0111] 图7描绘了用于从过程工厂(诸如图2的过程工厂100)安全地传送通信的示例性方法500的流程图。在一些实施例中，方法500的至少一部分通过执行存储在一个或多个非暂时计算机可读存储器上并由例如系统200的一个或多个处理器执行的计算机可执行或计算机可读的指令的集合。例如，方法500的至少一部分可以由图1-5所示的系统200的一个或多个组件来执行，例如边缘网关218或接收设备405。因此，下面描述方法500同时参考图1-5，然而，这仅是为了便于说明而不是为了限制的目的。

[0112] 在框502处，方法500包括经由数据二极管接收由过程工厂生成的数据，同时实时操作以控制过程。数据二极管被配置为允许从发送设备向接收设备发送单向通信，同时防止从接收设备向发送设备发送任何通信。通过数据二极管接收的过程工厂产生的数据(框502)可以包括生成的过程数据、诊断数据和其他类型的数据，并且可以在接收设备处(譬如在边缘网关218或接收设备405处)接收。接收到的过程工厂生成的数据可以是安全数据，例

如,通过上述加密技术或通过某些其他安全机制使数据安全。

[0113] 在框505处,方法500包括使用一个或多个安全机制来使所接收的过程工厂生成的数据安全,安全机制可以包括跨数据二极管使用的相同的安全机制,或者可以包括一个或多个不同的安全性机制。在框508处,方法500包括将在块505处安全的过程工厂生成的数据发送到通信地连接到接收设备的另一系统。例如,该安全的、由过程工厂生成的数据被发送到一个或多个远程系统210,在该远程系统210,由过程工厂生成的数据208的一个或多个应用、服务或其他消费者驻留并执行。该应用程序、服务或其他消费者可以对至少一些过程工厂生成的数据进行操作。

[0114] 在一个实施例中,使所接收的过程工厂生成的数据安全(框505)并且将安全的过程工厂生成的数据传送到另一系统(框508)包括:在接收设备和另一系统之间建立安全连接。将安全的过程工厂生成的数据传送到另一系统(框508)可以包括经由诸如公共互联网、专用企业网络等的一个或多个公共和/或专用网络来传送数据。因此,建立接收设备与另一系统之间的安全连接包括通过一个或多个公共和/或专用网络建立安全连接。如果需要,可以为不同类型的内容数据、过程工厂的不同数据生成源和/或内容数据的不同消费者建立不同的安全连接。

[0115] 在一个示例中,使用令牌服务来使得接收设备与另一系统之间的连接安全。接收设备对由另一系统提供的令牌服务进行认证,并且响应于认证,接收设备从另一系统接收共享访问签名(SAS)令牌。然后,接收设备在将内容数据(例如过程工厂生成的数据)传送到另一系统时使用SAS令牌。例如,接收设备例如经由AMQP(高级消息队列协议)连接使用SAS令牌来使与另一系统的连接安全和认证与另一系统的连接。另外,如果需要,内容数据和SAS令牌可以在传输到另一系统之前被加密。

[0116] 方法500还可以包括使得接收设备与另一系统之间的连接重新安全(框510)。使得接收设备与另一系统之间的连接510重新安全包括例如从另一系统(例如从另一系统处的令牌服务)接收更新的或不同的SAS令牌,以用于传送后续内容数据。特定的SAS令牌可以具有预定义的有效期(例如五分钟、十分钟、小于一个小时、或其它有效期,其可以是可配置的)。在令牌过期时,接收设备可以请求或获取用于后续消息的新的SAS令牌。替代地,另一系统可以自动地发送用于接收设备的更新的或新的SAS令牌,以便在先前的令牌过期时使用。

[0117] 当然,尽管使得接收设备与另一系统之间的连接(例如,框505、508和510)安全或重新安全被描述为使用SAS令牌和AMQP协议,但这仅仅是方法500的许多可能实施例中的一个实施例。方法500可以利用任意一个或多个适当的IOT安全机制(诸如,举例来说,X.509证书、其它类型的令牌、例如MQTT或XMPP的其它IOT协议,等等)。

[0118] 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意数量的以下方面:

[0119] 1、一种用于将通信从过程工厂安全地传输到另一系统的系统,安全的通信传输系统包括:设置在所述过程工厂的网络与所述另一系统的网络之间的数据二极管,所述数据二极管被配置为防止所述过程工厂网络与所述另一系统的网络之间的双向通信,其中,在所述过程工厂进行操作以控制工业过程时由所述过程工厂的设备所生成的数据被加密并且跨所述数据二极管从所述过程工厂网络传输到所述另一系统的网络。

[0120] 2、根据前述方面的系统,其中,所述数据二极管的硬件被配置为不包括用于将由

所述另一系统的网络所流出的通信传送到所述过程工厂网络的物理通信路径。

[0121] 3、根据前述方面中任一方面所述的系统，其中，所述数据二极管的软件被配置为防止由所述另一系统的网络所流出的通信进入所述过程工厂网络。

[0122] 4、根据前述方面中任一方面所述的系统，其中，所述加密的过程工厂数据基于TCP(传输控制协议)、UDP(用户数据报协议)或串行通信跨数据二极管传输。

[0123] 5、根据前述方面中任一方面所述的系统，还包括将将所述过程工厂网络与所述数据二极管互连的现场网关，其中，所述现场网关加密所述过程工厂数据以跨所述数据二极管进行传输。

[0124] 6、根据前述方面中任一方面所述的系统，其中，所述现场网关被设置在所述过程工厂处。

[0125] 7、根据前述方面中任一方面所述的系统，其中，所述数据二极管被设置在所述过程工厂处。

[0126] 8、根据前述方面中任一方面所述的系统，还包括将所述过程工厂网络与所述现场网关互连的本地工厂网关，所述本地工厂网关使用TLS(传输层安全性)封装来使所述过程工厂数据安全。

[0127] 9、根据前述方面中任一方面所述的系统，包括以下情况中的至少一种：包括在所述过程工厂中的设备生成的数据的至少第一部分被流传输到所述本地工厂网关；或者由包括在所述过程工厂中的所述设备生成的数据的至少第二部分响应于轮询而被发送到所述本地工厂网关。

[0128] 10、根据前述方面中任一方面所述的系统，其中，由所述现场网关执行的加密是第一加密，并且其中，由所述设备生成的至少一些数据的第二加密在所述设备处被执行。

[0129] 11、根据前述方面中任一方面所述的系统，其中，由所述设备生成和加密的所述数据中的所述至少一些数据经由所述过程工厂的无线网络或有线网络中的至少一个传送到所述本地工厂网关。

[0130] 12、根据前述方面中任一方面所述的系统，还包括所述数据二极管与所述另一系统的网络互连的边缘网关，其中，所述边缘网关确保所述过程工厂数据用于传输到所述另一系统的网络。

[0131] 13、根据前述方面中任一方面所述的系统，其中，所述边缘网关设置在所述过程工厂处。

[0132] 14、根据前述方面中任一方面所述的系统，其中，所述边缘网关使用令牌或证书来确保所述过程工厂数据传送到所述另一系统。

[0133] 15、根据前述方面中任一项所述的系统，其中：所述令牌或证书由包括在所述另一系统中的安全服务管理；所述令牌或证书对于有限的时间段是有效的；所述有限的时间段有不超过一小时的持续时间。

[0134] 16、根据前述方面中任一方面所述的系统，其中，所述安全的过程工厂数据使用以下中的至少一个来从所述边缘网关传送到所述另一系统的网络：互联网连接、蜂窝路由器或另一类型的回程互联网连接。

[0135] 17、根据前述方面中任一方面所述的系统，其中，所述过程工厂数据储存在所述另一系统处，并且仅对所述另一系统的授权用户授予对在所述另一系统处储存的数据的访

问。

[0136] 18、根据前述方面中任一方面所述的系统，还包括：将所述过程工厂网络与所述数据二极管互连的现场网关；以及将所述数据二极管与所述另一系统的网络互连的边缘网关，其中，跨所述数据二极管传输的所述过程工厂数据使用在所述现场网关与所述边缘网关之间共享的密钥材料进行加密。

[0137] 19、根据前述方面中任一方面所述的系统，其中，所述现场网关被包括在所述过程工厂中。

[0138] 20、根据前述方面中任一方面所述的系统，其中，所述边缘网关被包括在所述过程工厂中。

[0139] 21、根据前述方面中任一方面所述的系统，其中，所述另一系统被包括在所述过程工厂中。

[0140] 22、根据前述方面中任一方面所述的系统，其中，所述另一系统在一个或多个计算云中实现。

[0141] 23、根据前述方面中任一方面所述的系统，其中，所述另一系统能够经由公共互联网访问。

[0142] 24、根据前述方面中任一方面所述的系统，其中，所述另一系统不能经由公共互联网访问。

[0143] 25、根据前述方面中任一方面所述的系统，其中，所述另一系统提供与所述过程工厂相对应的一个或多个服务，所述一个或多个服务包括以下至少一个：监控在所述过程工厂处发生的状况和/或事件；感测在所述过程工厂处发生的状况和/或事件；监控由所述过程工厂控制的过程的至少一部分；描述性分析；规定性分析；或者用于修改所述过程工厂的至少一部分的一个或多个规定性更改。

[0144] 26、根据前述方面中任一方面的系统，其中：所述设备中的至少一个设备经由包括在所述过程工厂中的通信网络与所述过程工厂内的另一设备进行通信，以控制所述过程工厂内的过程的至少一部分，所述通信网络与所述过程工厂网络不同，并且所述通信网络支持Wi-Fi协议、以太网协议和IEEE 802.11兼容协议、移动通信协议、短波无线电通信协议、4-20ma信令、HART®协议、WirelessHART®协议、FOUNDATION®现场总线协议、PROFIBUS协议、或DeviceNet协议中的至少一种。

[0145] 27、根据前述方面中任一方面所述的系统，其中，包括在所述过程工厂中的所述通信网络是第一通信网络，并且其中，所述数据二极管经由所述过程工厂网络从所述一个或多个设备接收所生成的数据。

[0146] 28、根据前述方面中任一方面所述的系统，其中，所述过程工厂网络支持HART-IP®协议。

[0147] 29、一种使过程工厂和其他系统之间的通信安全的方法，所述方法包括：在现场网关处从过程工厂网络接收数据，所述数据由所述过程工厂的一个或多个设备在所述过程工厂进行操作以控制工业过程时生成，所述过程工厂数据被确保经由第一安全机制从所述一个或多个设备传输到所述现场网关；经由第二安全机制由所述现场网关使所述过程工厂数据安全；以及跨数据二极管传输所述安全的过程工厂数据以经由边缘网关传送到所述另一系统，所述边缘网关通信地连接到所述另一系统，经由第三安全机制使所述边缘网关与所

述另一系统之间的通信连接安全，并且所述数据二极管被配置为防止由所述边缘网关传送的任何数据进入所述现场网关。

[0148] 30、根据前述方面的方法，其至少一部分由方面1-28中任一方面的系统执行。

[0149] 31、根据方面29-30中任一方面所述的方法，其中，所述第一安全机制，所述第二安全机制和所述第三安全机制是不同的安全机制。

[0150] 32、根据方面29-31中任一方面所述的方法，还包括供应所述现场网关和所述边缘网关，包括生成在所述现场网关与所述边缘网关之间共享的密钥；并且其中，经由所述第二安全机制由所述现场网关使所述过程工厂数据安全包括：由所述现场网关使用所述共享密钥来使所述过程工厂数据安全。

[0151] 33、根据方面29-32中任一方面所述的方法，其中，经由所述第二安全机制由所述现场网关使所述过程工厂数据安全还包括：由所述现场网关加密所述过程工厂数据。

[0152] 34、根据方面29-33中任一方面所述的方法，其中，所述第一安全机制包括由所述一个或多个设备对所述一个或多个设备生成的数据进行加密。

[0153] 35、根据方面29-34中任一方面所述的方法，其中，所述第一安全机制还包括将所述加密的过程工厂数据封装在所述过程工厂中实现的安全层中。

[0154] 36、根据方面29-35中任一方面所述的方法，其中，所述第三安全机制包括安全令牌或证书。

[0155] 37、根据方面29-36中任一方面所述的方法，其中，所述第三安全机制包括由所述边缘网关执行的加密。

[0156] 38、一种使过程工厂与服务所述过程工厂的另一系统之间的通信安全的方法，所述方法包括：在边缘网关处经由通信地连接到所述过程工厂的现场网关的数据二极管接收数据，所述数据由所述过程工厂中的一个或多个设备在所述过程工厂进行操作以控制工业过程时生成，其中：所述过程工厂数据被确保用于经由第一安全机制从所述一个或多个设备传输到所述现场网关，并且进一步被确保用于经由第二安全机制跨所述数据二极管从所述现场网关传输到所述边缘网关，并且所述数据二极管被配置为防止由所述边缘网关传送的任何数据进入所述现场网关。所述方法还包括：经由第三安全机制由所述边缘网关使所述过程工厂数据安全；以及由所述边缘网关将所述安全的过程工厂数据传送到所述另一系统。

[0157] 39、根据结合方面29-37中任一方面的前述方面所述的方法。

[0158] 40、根据方面38或方面39所述的方法，其至少一部分由方面1-28中任一方面的系统执行。

[0159] 41、根据方面38-40中任一方面所述的方法，其中，所述第一安全机制、所述第二安全机制和所述第三安全机制是不同的安全机制。

[0160] 42、根据方面38-41中任一方面所述的方法，其中，所述第一安全机制或所述第二安全机制中的至少一个包括所述过程工厂数据的相应加密。

[0161] 43、根据方面38-42中任一方面所述的方法，其中，所述第一安全机制包括所述过程工厂数据在安全层中的封装。

[0162] 44、根据方面38-43中任一方面所述的方法，还包括使用秘密密钥跨所述数据二极管在所述边缘网关与所述现场网关之间建立安全连接，并且其中，所述第二安全机制包括

在所述边缘网关与所述现场网关之间建立的所述安全连接。

[0163] 45、根据方面38-44中任一方面所述的方法，其中，所述第二安全机制还包括由所述现场网关对所述过程工厂数据进行加密。

[0164] 46、根据方面38-45中任一方面所述的方法，还包括在所述边缘网关与所述另一系统之间建立安全连接，并且其中，所述第三安全机制包括在所述边缘网关与所述另一系统之间建立的所述安全连接。

[0165] 47、根据方面38-46中任一方面所述的方法，其中，在所述边缘网关与所述另一系统之间建立所述安全连接包括：对由所述另一系统提供的安全服务进行认证；以及响应于所述认证而接收安全令牌或证书。

[0166] 48、根据方面38-47中任一方面所述的方法，其中，将所述安全的过程工厂数据传送到所述另一系统包括：将所述安全令牌或证书结合所述过程工厂数据传送到所述另一系统。

[0167] 49、根据方面38-48中任一方面所述的方法，其中，所述安全令牌或证书是第一安全令牌或证书，并且所述方法还包括：接收不同的安全令牌或证书以在将由所述一个或多个设备生成的后续数据传送到所述另一个系统时利用。

[0168] 50、根据方面38-49中任一方面所述的方法，其中，由所述边缘网关经由所述第三机制来使所述过程工厂数据安全包括：由所述边缘网关加密所述过程工厂数据。

[0169] 51、根据方面38-50中任一方面所述的方法，其中，将所述安全的过程工厂数据传送到所述另一系统包括：将所述安全的过程工厂数据传送到所述过程工厂中包括的系统。

[0170] 52、根据方面38-51中任一方面所述的方法，其中，将所述安全的过程工厂数据传送到所述另一系统包括：将所述安全的过程工厂数据传送到在一个或多个计算云中实现的系统。

[0171] 53、根据方面38-52中任一方面所述的方法，其中，将所述过程工厂数据传送到所述另一系统包括：经由公共互联网上的安全连接将所述过程工厂数据传送到所述另一系统。

[0172] 54、根据方面38-53中任一方面所述的方法，其中，将所述过程工厂数据传送到所述另一系统包括：将所述过程工厂数据传送到提供以下至少一个的系统：监控在所述过程工厂处发生的状况和/或事件；感测在所述过程工厂处发生的状况和/或事件；监控由所述过程工厂执行的过程的至少一部分；描述性分析；规定性分析；或者用于修改所述过程工厂的至少一部分的规定性更改。

[0173] 55、结合前述方面中的任何其它方面的先前方面中的任何一个。

[0174] 当以软件实现时，本文描述的任何应用、服务和引擎可以储存在任何有形的、非暂时性的计算机可读存储器中，诸如在磁盘、激光盘、固态存储器件、分子存储器储存设备或其它储存介质中、在计算机或处理器的RAM或ROM中等。虽然本文公开的示例性系统被公开为包括在硬件上执行的软件和/或固件以及其它部件，但是应当注意，这样的系统仅仅是说明性的，不应被认为是限制性的。例如，可以想到，这些硬件、软件和固件部件中的任何一个或多个或全部可以专门以硬件、专门以软件或以硬件和软件的任何组合来体现。因此，虽然本文描述的示例性系统被描述为在一个或多个计算机设备的处理器上执行的软件中实现，但是本领域普通技术人员将容易地理解，所提供的示例不是实现这样的系统的唯一方式。

[0175] 因此，虽然已经参考具体实施例描述了本发明，这些具体实施例仅仅是说明性的而不是对本发明的限制，但是本领域普通技术人员将显而易见的是，可以在不脱离本发明的精神和范围的情况下对所公开的实施例进行更改、添加或者删除。

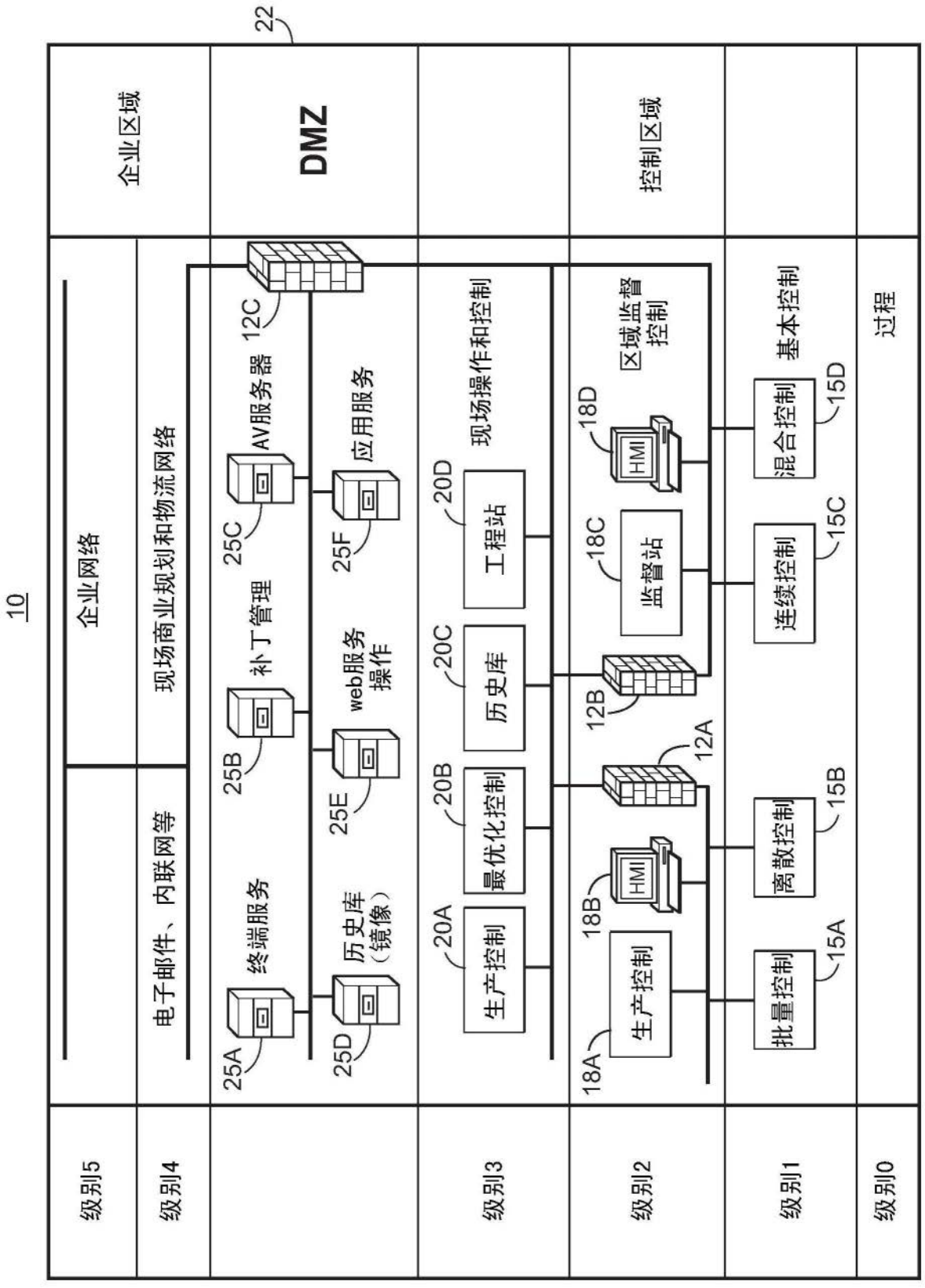

10
企业区域
企业网络
现场商业规划和物流网络
电子邮件、内联网等
DMZ
22
级别5
级别4
级别3
级别2
级别1
级别0
25A
终端服务
25B
补丁管理
25C
AV服务器
12C
25D
历史库（镜像）
25E
web服务操作
25F
应用服务
20A
生产控制
20B
最优化控制
20C
历史库
20D
工程站
现场操作和控制
18A
生产控制
18B
HMI
12A
12B
18C
监督站
18D
HMI
区域监督控制
15A
批量控制
15B
离散控制
15C
连续控制
15D
混合控制
基本控制
过程

图1

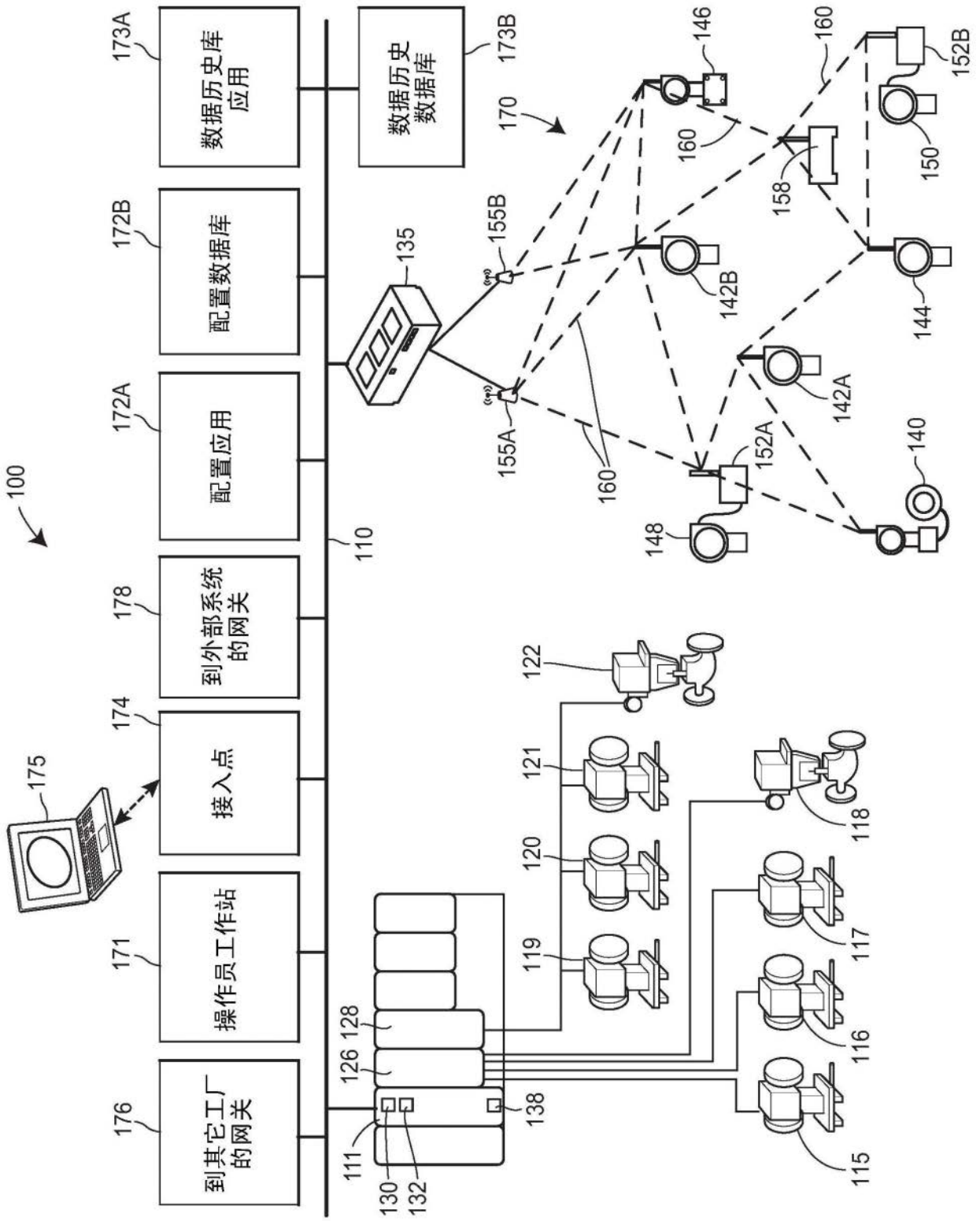

100
110
173A
数据历史库应用
173B
数据历史数据库
172B
配置数据库
172A
配置应用
178
到外部系统的网关
174
接入点
175
171
操作员工作站
176
到其它工厂的网关
170
135
155A
155B
160
142A
142B
144
146
148
150
152A
152B
158
140
111
130
132
126
128
138
119
120
121
122
115
116
117
118

图2

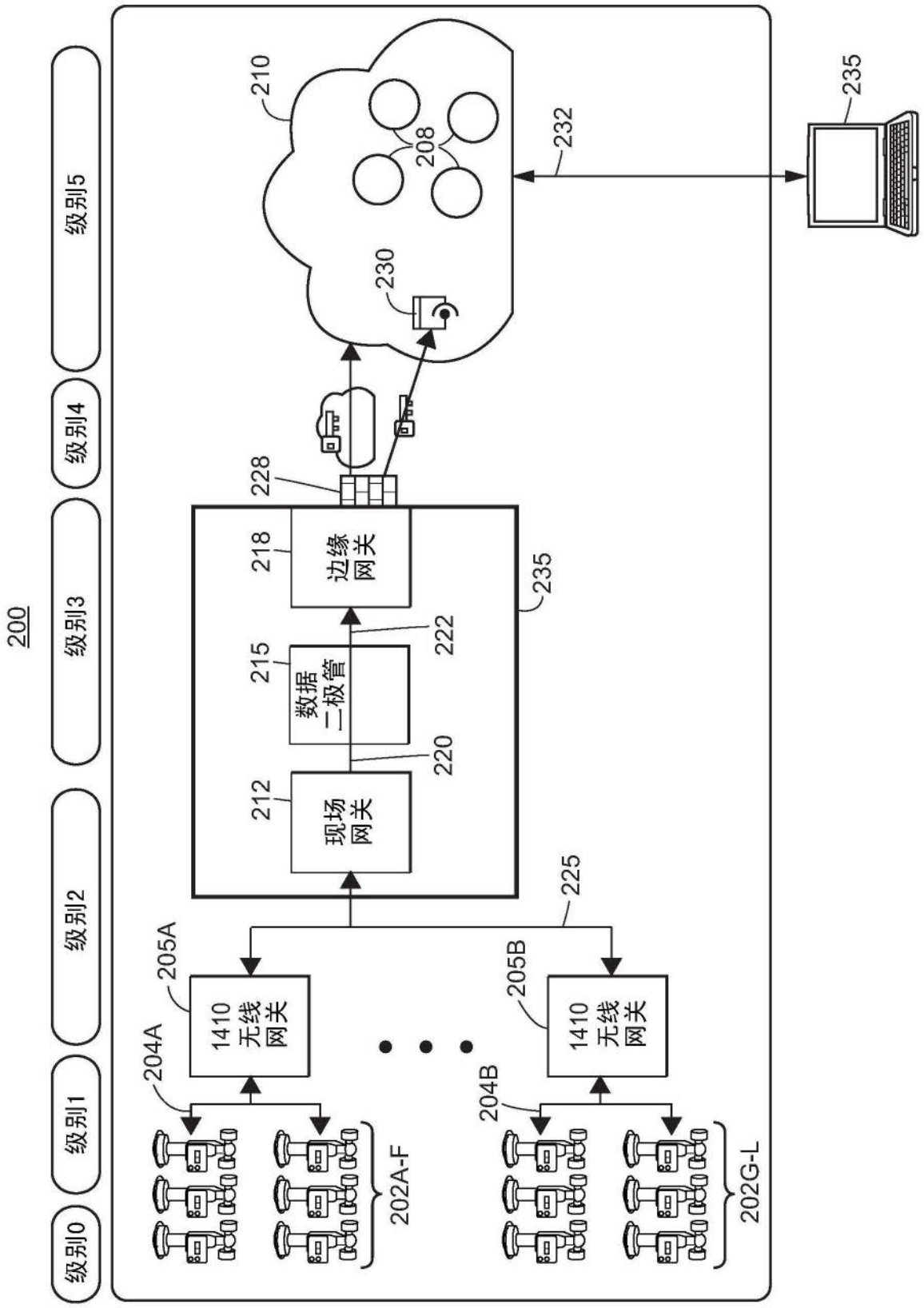

200
级别0
级别1
级别2
级别3
级别4
级别5
210
208
232
235
230
228
218
边缘网关
235
222
215
数据二极管
220
212
现场网关
225
205A
1410无线网关
204A
202A-F
205B
1410无线网关
204B
202G-L

图3

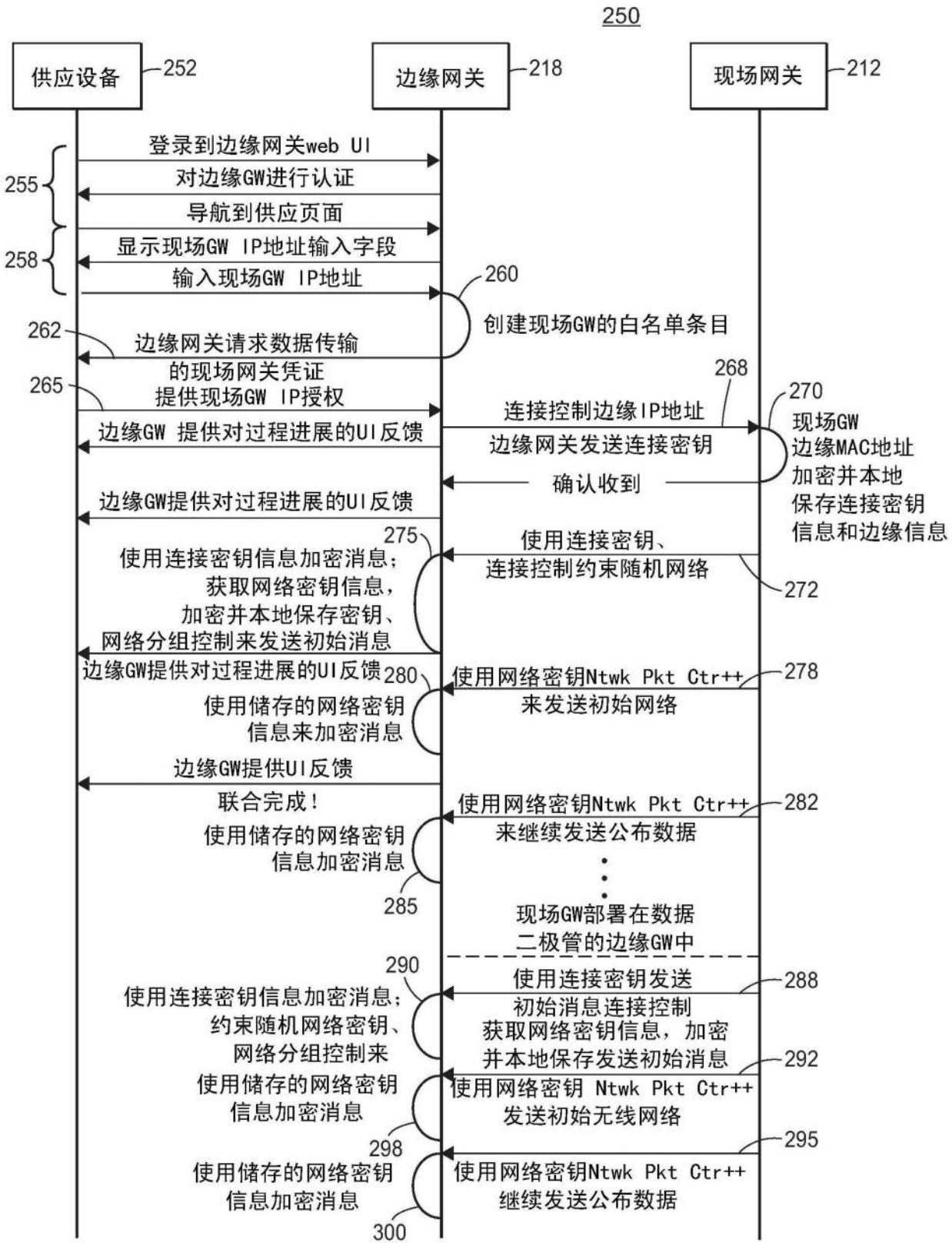

250
供应设备
252
边缘网关
218
现场网关
212
登录到边缘网关web UI
对边缘GW进行认证
255
导航到供应页面
显示现场GW IP地址输入字段
258
输入现场GW IP地址
260
创建现场GW的白名单条目
262
边缘网关请求数据传输
的现场网关凭证
265
提供现场GW IP授权
边缘GW 提供对过程进展的UI反馈
连接控制边缘IP地址
268
边缘网关发送连接密钥
270
现场GW
边缘MAC地址
加密并本地
保存连接密钥
信息和边缘信息
确认收到
边缘GW提供对过程进展的UI反馈
使用连接密钥、
连接控制约束随机网络
272
275
使用连接密钥信息加密消息；
获取网络密钥信息，
加密并本地保存密钥、
网络分组控制来发送初始消息
边缘GW提供对过程进展的UI反馈
280
使用网络密钥Ntwk Pkt Ctr++
278
来发送初始网络
使用储存的网络密钥
信息来加密消息
边缘GW提供UI反馈
联合完成！
使用网络密钥Ntwk Pkt Ctr++
282
来继续发送公布数据
使用储存的网络密钥
信息加密消息
285
现场GW部署在数据
二极管的边缘GW中
290
使用连接密钥发送
288
初始消息连接控制
使用连接密钥信息加密消息；
约束随机网络密钥、
网络分组控制来
获取网络密钥信息，加密
并本地保存发送初始消息
292
使用储存的网络密钥
信息加密消息
使用网络密钥 Ntwk Pkt Ctr++
发送初始无线网络
298
295
使用储存的网络密钥
信息加密消息
使用网络密钥Ntwk Pkt Ctr++
继续发送公布数据
300

图4

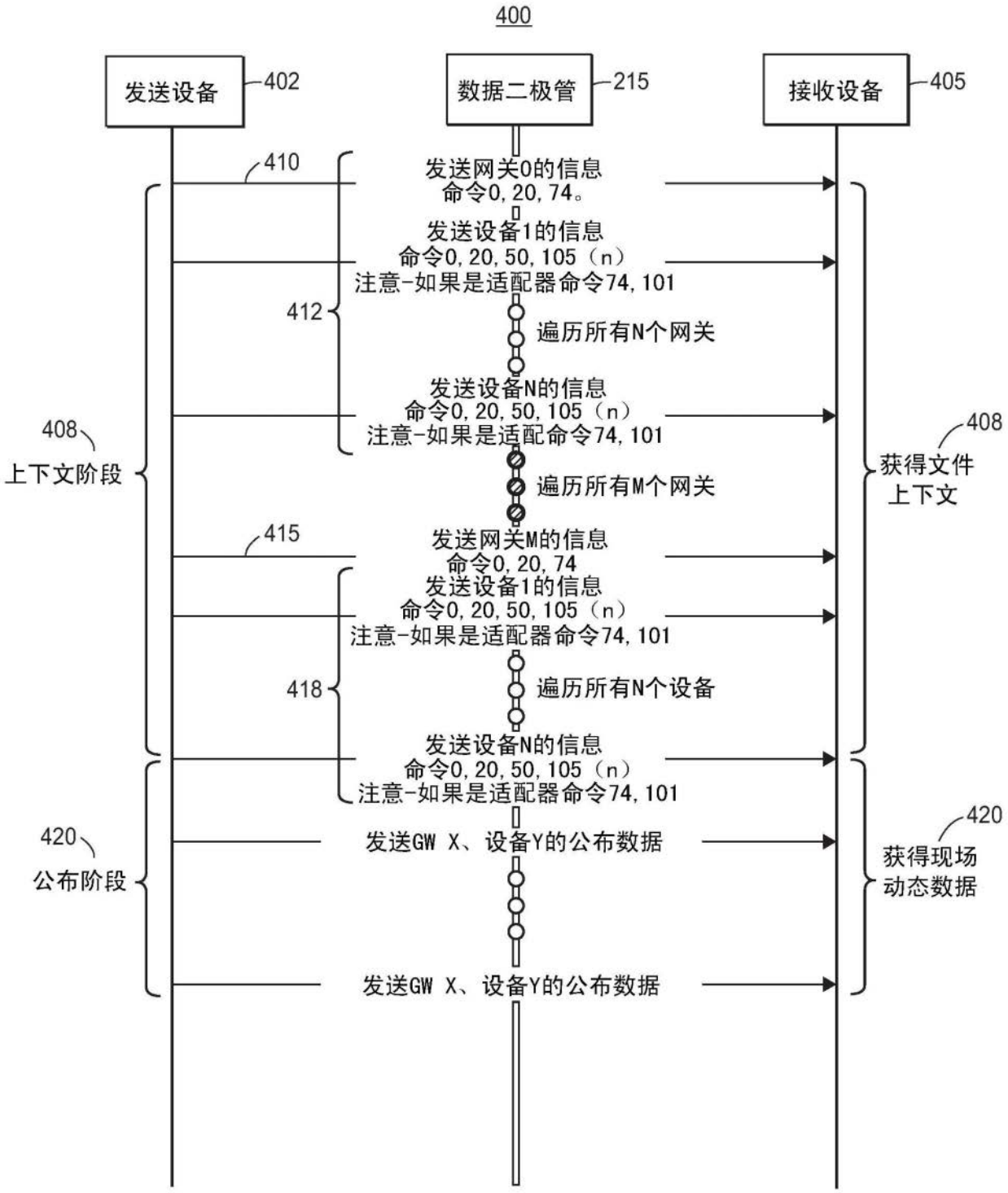

400
发送设备
402
数据二极管
215
接收设备
405
410
发送网关0的信息
命令0, 20, 74。
发送设备1的信息
命令0, 20, 50, 105（n）
注意-如果是适配器命令74, 101
412
遍历所有N个网关
发送设备N的信息
命令0, 20, 50, 105（n）
注意-如果是适配命令74, 101
408
上下文阶段
遍历所有M个网关
408
获得文件
上下文
415
发送网关M的信息
命令0, 20, 74
发送设备1的信息
命令0, 20, 50, 105（n）
注意-如果是适配器命令74, 101
418
遍历所有N个设备
发送设备N的信息
命令0, 20, 50, 105（n）
注意-如果是适配器命令74, 101
420
公布阶段
发送GW X、设备Y的公布数据
420
获得现场
动态数据
发送GW X、设备Y的公布数据

图5

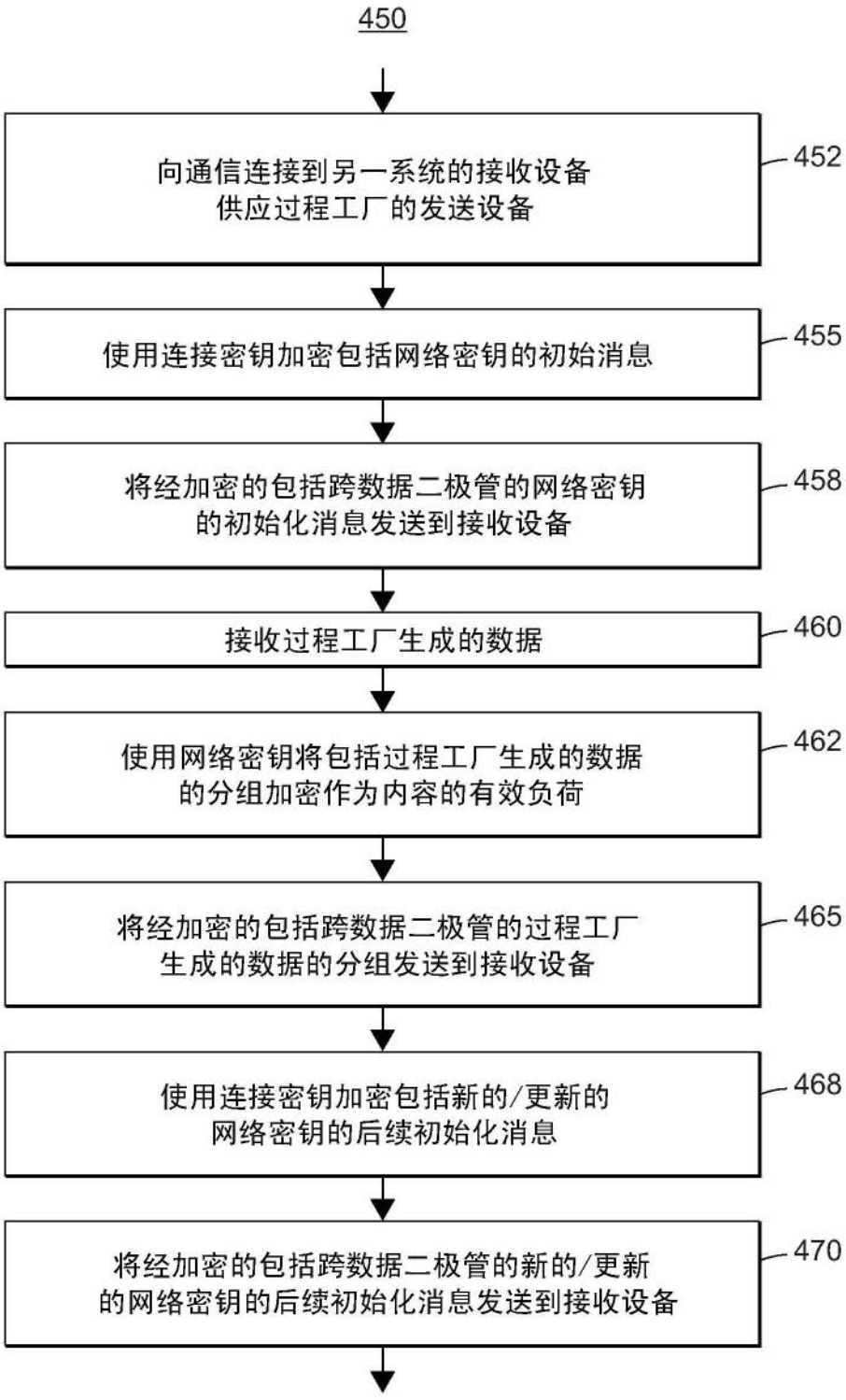

450
向通信连接到另一系统的接收设备
供应过程工厂的发送设备
452
使用连接密钥加密包括网络密钥的初始消息
455
将经加密的包括跨数据二极管的网络密钥
的初始化消息发送到接收设备
458
接收过程工厂生成的数据
460
使用网络密钥将包括过程工厂生成的数据
的分组加密作为内容的有效负荷
462
将经加密的包括跨数据二极管的过程工厂
生成的数据的分组发送到接收设备
465
使用连接密钥加密包括新的/更新的
网络密钥的后续初始化消息
468
将经加密的包括跨数据二极管的新的/更新
的网络密钥的后续初始化消息发送到接收设备
470

图6

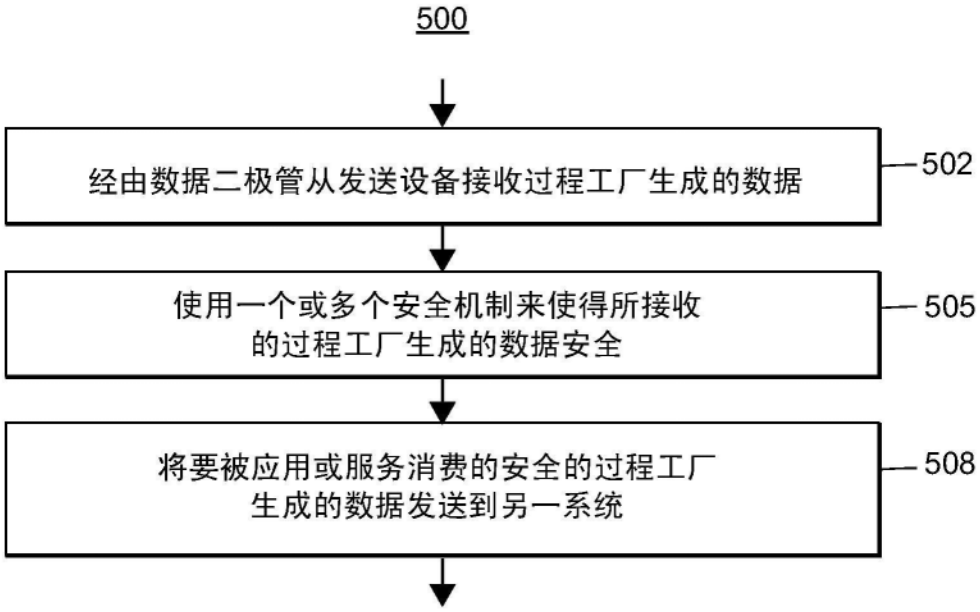

500
经由数据二极管从发送设备接收过程工厂生成的数据
502
使用一个或多个安全机制来使得所接收的过程工厂生成的数据安全
505
将要被应用或服务消费的安全的过程工厂生成的数据发送到另一系统
508

图7