(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 104850091 B
(45)授权公告日 2020.12.08

(21)申请号 201410802889.5

(22)申请日 2014.12.19

(65)同一申请的已公布的文献号
申请公布号 CN 104850091 A

(43)申请公布日 2015.08.19

(30)优先权数据
61/940,003 2014.02.14 US
62/021,438 2014.07.07 US
14/446,412 2014.07.30 US
14/469,931 2014.08.27 US
14/519,032 2014.10.20 US

(73)专利权人 基岩自动化平台公司
地址 美国加利福尼亚州

(72)发明人 A·鲁亚科斯 J·G·加尔文 G·克兰肖

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

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

(56)对比文件
EP 2613421 A1,2013.07.10
EP 2557657 A2,2013.02.13
CN 102290612 A,2011.12.21
US 5422558 A,1995.06.06
CN 1988699 A,2007.06.27
CN 101322089 A,2008.12.10

审查员 贺春圆

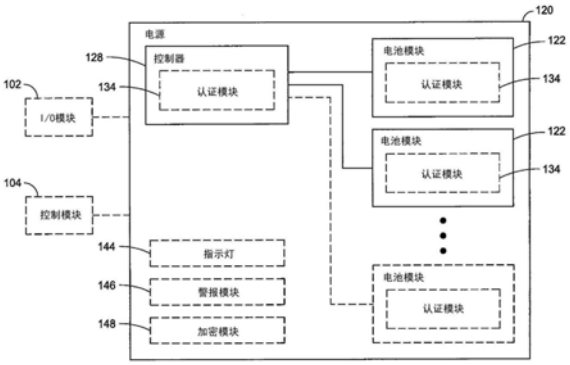
权利要求书2页 说明书19页 附图9页

(54)发明名称

用于工业控制系统的安全电源

(57)摘要

本发明描述了一种控制系统，其包括电功率源和与所述电功率源电耦合的交流(AC)电源。不间断电源与所述AC电源电耦合，用于存储并返回由所述AC电源供应的电能。不间断电源包括多个电池模块。每个电池模块包括电池单元和被配置为监测所述电池单元的电池监测器。每个电池模块还包括与所述电池模块操作地耦合的控制器。控制器被配置为从所述电池模块接收诊断信息。不间断电源还可以包括一个或多个认证模块，以参与电池模块、控制器、与不间断电源耦合的装置、控制系统中的动作发生器等中两个或更多装置之间的认证序列。



CN 104850091 B

1.一种电源,包括:

电池模块,所述电池模块包括电池单元和被配置为监测所述电池单元的电池监测器,所述电池模块被配置为执行认证操作以认证与所述电源耦合的其它装置;以及

控制器,其与所述电池模块操作地耦合,所述控制器被配置为从所述电池模块接收诊断信息,其中,所述电池监测器被配置为在通过由所述电池模块执行的认证操作没有建立与所述电池模块的连接的认证时防止电接入至所述电池单元。

2.根据权利要求1所述的电源,其中,所述电池单元包括锂离子电池单元。

3.根据权利要求1所述的电源,其中,所述诊断信息包括所述电池单元的操作电压、所述电池单元的操作电流、与所述电池单元相关联的电荷、或与所述电池单元相关联的寿命的至少其中之一。

4.根据权利要求1所述的电源,其中,所述电源包括多个电池模块,所述多个电池模块中的每个电池模块被配置为通过堆叠与所述多个电池模块中的另一个相应的电池模块连接。

5.根据权利要求1所述的电源,其中,所述电池监测器包括利用串联连接的多个场效应晶体管来实施的电子信号开关器件。

6.根据权利要求1所述的电源,其中,所述电池模块或所述控制器的至少其中之一被配置有唯一标识符或唯一安全性凭证的至少其中之一。

7.根据权利要求1所述的电源,其中,所述电池模块与所述控制器电气隔离。

8.一种电源,包括:

多个电池模块,所述多个电池模块中的每个电池模块都包括电池单元和被配置为监测所述电池单元的电池监测器,所述多个电池模块中的至少一个电池模块被配置为执行认证操作以认证与所述电源耦合的其它装置;

控制器,其与所述多个电池模块操作地耦合,所述控制器被配置为从所述多个电池模块接收诊断信息;以及

认证模块,所述认证模块被配置为参与所述多个电池模块的至少其中之一、所述控制器、要与所述电源耦合的装置、或动作发生器中的至少一对之间的认证序列,其中,所述多个电池模块中的所述至少一个电池模块的电池监测器被配置为在通过由所述至少一个电池模块执行的认证操作没有建立与所述至少一个电池模块的连接的认证时防止电接入至所述至少一个电池模块的电池单元。

9.根据权利要求8所述的电源,其中,所述认证模块包括在所述多个电池模块中的第一模块内,所述认证模块被配置为向所述控制器或要与所述电源耦合的所述装置中的至少其中之一认证所述多个电池模块中的所述第一模块。

10.根据权利要求8所述的电源,其中,所述认证模块包括在所述多个电池模块中的第一模块内中,所述认证模块被配置为认证所述控制器或要与所述电源耦合的所述装置的至少其中之一。

11.根据权利要求8所述的电源,其中,所述认证模块包括在所述控制器中,所述认证模块被配置为向所述多个电池模块中的第一模块或要与所述电源耦合的所述装置的至少其中之一认证所述控制器。

12.根据权利要求8所述的电源,其中,所述认证模块包括在所述控制器内,所述认证模

块被配置为认证所述多个电池模块中的第一模块或要与所述电源耦合的所述装置的至少其中之一。

13.根据权利要求8所述的电源，其中，所述认证模块还被配置为认证工业控制系统环境中所接收的动作请求。

14.一种控制系统，包括：

电功率源；

交流电源，所述交流电源与所述电功率源电耦合；

与所述交流电源电耦合的不间断电源，所述不间断电源用于存储并返回由所述交流电源供应的电能，所述不间断电源包括至少一个电池模块和控制器，其中，所述至少一个电池模块包括电池单元和被配置为监测所述电池单元的电池监测器，所述至少一个电池模块被配置为执行认证操作以认证与所述不间断电源耦合的其它装置，所述控制器与所述电池模块操作地耦合，所述控制器被配置为从所述电池模块接收诊断信息；以及

至少一个控制元件或子系统，所述至少一个控制元件或子系统电连接到所述交流电源，其中，所述不间断电源被配置为在由所述电功率源供应的电能中断时，向所述交流电源返回电能以为所述至少一个控制元件或子系统供电，并且所述电池监测器被配置为在通过由所述至少一个电池模块执行的认证操作没有建立与所述至少一个电池模块的连接的认证时防止电接入至所述电池单元。

15.根据权利要求14所述的控制系统，其中，所述电池监测器被配置为在建立至所述电池单元的端子的非期望电路径时防止电接入至所述电池单元。

16.根据权利要求14所述的控制系统，其中，所述诊断信息包括所述电池单元的操作电压、所述电池单元的操作电流、与所述电池单元相关联的电荷、或与所述电池单元相关联的寿命的至少其中之一。

17.根据权利要求14所述的控制系统，其中，所述电池监测器包括利用串联连接的多个场效应晶体管来实施的电子信号开关器件。

18.根据权利要求14所述的控制系统，其中，所述电池模块或所述控制器的至少其中之一被配置有唯一标识符或唯一安全性凭证的至少其中之一。

19.根据权利要求14所述的控制系统，其中，所述电池模块与所述控制器电气隔离。

20.根据权利要求19所述的控制系统，还包括用于将所述电池模块与所述控制器电气隔离的光隔离器。

用于工业控制系统的安全电源

[0001] 相关申请的交叉引用

[0002] 本申请根据35U.S.C.§119(e)要求2014年2月14日提交的标题为“BACKUP POWER SUPPLY”的美国临时申请No.61/940,003的优先权的权益，通过引用将该美国临时申请的全部内容并入本文中。本申请还是2013年8月6日提交的标题为“SECURE INDUSTRIAL CONTROL SYSTEM”的国际申请No.PCT/US2013/053721的部分延续。根据35U.S.C.§120，本申请还是2014年8月27日提交的标题为“SECURE INDUSTRIAL CONTROL SYSTEM”的美国专利申请No.14/469,931的部分延续。根据35U.S.C.§120，本申请还是2014年7月30日提交的标题为“INDUSTRIAL CONTROL SYSTEM CABLE”的美国专利申请No.14/446,412的部分延续，该美国专利申请根据35U.S.C.§119要求2014年7月7日提交的标题为“INDUSTRIAL CONTROL SYSTEM CABLE”的美国临时申请No.62/021,438的优先权的权益。通过引用将美国临时申请No.61/940,003和62/021,438；美国专利申请No.14/446,412和14/469,931；以及国际申请PCT/US 2013/053721的全部内容并入本文中。

背景技术

[0003] 诸如标准工业控制系统(ICS)或可编程自动化控制器(PAC)之类的工业控制系统包括工业生产中使用的各种类型的控制设备，例如监视控制和数据采集(SCADA)系统、分布式控制系统(DCS)、可编程逻辑控制器(PLC)和由诸如IEC 1508之类的安全标准认证的工业安全系统。这些系统用于包括电气、水和污水、油气生产和精炼、化工、食品、药品和机器人技术的产业中。利用从各种类型的传感器收集的信息来测量过程变量，可以将来自工业控制系统的自动的和/或操作员驱动的监视命令传送到各种致动器装置，例如控制阀、液压致动器、磁致动器、电子开关、电动机、螺线管等。这些致动器装置从传感器和传感器系统收集数据、打开以及关闭阀和断路器、调节阀和电动机、监测工业过程的报警条件，等等。

[0004] 在其它示例中，SCADA系统能够利用具有可以在地理上广泛分布的过程站点(process site)的开环控制。这些系统利用远程终端单元(RTU)向一个或多个控制中心发送监视数据。部署RTU的SCADA应用包括流体管道、配电和大型通信系统。DCS系统通常用于具有高带宽、低延迟数据网络的实时数据收集和连续控制，并且用于大场地工业加工厂，例如油气、精炼、化工、药品、食品和饮料、水和污水、纸浆和纸张、公用电源、以及采矿和金属。PLC更典型地提供布尔逻辑和顺序逻辑操作、和计时器、以及连续控制，并且PLC通常用于独立的机械和机器人技术中。此外，ICE和PAC系统可以用于楼宇、机场、船舶、空间站等的设施加工中(例如，用以监测并控制加热、通风和空调(HVAC)设备和能耗)。随着工业控制系统的发展，新技术与这些各种类型的控制系统的方面正在进行组合。例如，PAC能够包括SCADA、DCS和PLC的方面。

发明内容

[0005] 控制系统包括电功率源和与电功率源电耦合的交流(AC)电源。不间断电源与AC电源电耦合，用于存储并返回由AC电源供应的电能。不间断电源包括多个电池模块。每个电池

模块包括电池单元和被配置为监测电池单元的电池监测器。每个电池模块还包括与电池模块操作地耦合的控制器。控制器被配置为从电池模块接收诊断信息。控制系统还包括电连接到AC电源的控制元件或子系统。不间断电源被配置为返回电能到AC电源，以在由电功率源供应的电能中断时为控制元件或子系统供电。不间断电源还可以包括一个或多个认证模块，以参与电池模块、控制器、要与不间断电源耦合的装置、控制系统中的动作发生器等中的两个或更多装置之间的认证序列。

[0006] 提供本发明内容是为了以简化的形式引入概念的选择，以下在具体实施方式中进一步描述所述概念的选择。本发明内容并不是要确定所要求保护的主题内容的关键特征或必要特征，也不是要用于帮助确定所要求保护的主题内容的范围。

附图说明

[0007] 参考附图来描述具体实施方式。在说明和附图中的不同实例中的相同附图标记的使用可以指示相似的或相同的项目。

[0008] 图1是根据本公开内容的示例性实施例的示出包括一个或多个认证模块的电源的方框图。

[0009] 图2是根据本公开内容的示例性实施例的示出工业控制系统的方框图。

[0010] 图3是根据本公开内容的示例性实施例的示出诸如图2的工业控制系统之类的工业控制系统的方框图，其中工业控制系统从诸如电网和一个或多个本地发电机之类的多个源接收电功率，并且其中一个或多个备用电源被配置为利用多个电池模块来存储并返回电能。

[0011] 图4是根据本公开内容的示例性实施例的示出备用电源的方框图，所述备用电源被配置为与诸如图2的工业控制系统之类的系统通信地耦合，并且被配置为连接到电功率源(例如，图2的电网和/或本地发电机)以存储并返回电能，其中备用电源包括控制器和多个电池模块，并且每个电池模块具有与控制器通信地耦合的电池监测器。

[0012] 图5是根据本公开内容的示例性实施例的示出诸如图4中所示的备用电源之类的备用电源的方框图，其中备用电源被配置为与诸如图2的工业控制系统之类的系统通信地耦合，并且其中备用电源包括控制器，控制器被配置为向系统提供关于备用电源中包括的多个电池模块的状态的信息。

[0013] 图6是根据本公开内容的示例性实施例的安全控制系统的示意图，所述安全控制系统对诸如图1中所示的电源之类的装置、和/或诸如连接到图1中所示的电源的被供电装置之类的其它装置进行认证。

[0014] 图7是根据本公开内容的示例性实施例的示出用于诸如图6的安全控制系统之类的工业控制系统的动作认证路径的方框图。

[0015] 图8是根据本公开内容的示例性实施例的进一步示出图7的动作认证路径的方框图。

[0016] 图9是根据本公开内容的示例性实施例的示出用于认证动作请求的方法的流程图。

具体实施方式

[0017] 概要

[0018] 在工业控制系统环境中，通常利用本地发电(例如，利用现场涡轮机和/或柴油发电机)等将功率从电网(例如，利用来自AC输电干线的高压功率)供应到诸如控制器、输入/输出(I/O)模块等的自动化设备。通常还将备用功率从电池供应到这些环境中的自动化设备。例如，可以利用例如铅酸电池在工业环境中提供大规模蓄电池。可以利用集中式交流(AC)功率传输技术来供应来自大规模蓄电池的功率。在其它示例中，利用较小的分散式直流(DC)电池电源。例如，在机柜、控制器、I/O模块等的级别上，由较小的铅酸电池来供应备用电池功率。然而，在与诸如锂离子电池之类的较新的可充电电池技术相比时，铅酸电池的能量密度相对较低。此外，在这些配置中，备用电池通常与控制硬件分开，需要与每个电池进行单独连接，以监测电池状态。例如，工业自动化环境中的备用电池通常连接到控制硬件的空闲I/O端口，以监测这种电池的活动(例如，开/关状态)。

[0019] 本文中描述了帮助监测和/或控制工业控制系统环境中的诸如不间断电源(UPS)设备之类的电池电源的系统和技术。可以利用较高能量密度的可充电电池技术，例如锂离子可充电电池技术来实现所描述的技术和系统。在本公开内容的实施例中，工业UPS提供通信和/或安全特征，例如双向系统通信、控制系统集成、网络安全集成等。例如，工业UPS提供状态信息、诊断信息、可靠性信息、双向通信等。在一些实施例中，工业UPS实施密钥加密微控制器技术。

[0020] 在一些实施例中，电源包括能够执行电源和/或连接到电源的装置的认证的电路(例如，印刷电路板(PCB)、集成电路(IC)芯片和/或其它电路)。这能够防止或最小化将电源插入到并非要使用该特定电源或电源的类型的装置中的可能性(例如，防止或最小化将低压电源插入到高压装置中的可能性)。例如，电源与耦合的模块执行“握手”操作，以验证电源与适当的和/或期望的装置配对。在一些实施例中，利用诸如发光二极管(LED)指示器灯之类的指示器来提供这种认证的通知。例如，多色LED和/或单色LED提供诊断信息，以指示认证的状态(例如，利用连续发光、不发光、闪烁、用于一种状态的一种颜色和用于另一种状态的另一种颜色，等等)。

[0021] 在一些实施例中，电源可以用于认证另一个装置，例如从电源接收功率的仪器。例如，电源电路可以用于认证被供电的装置、被供电的装置的类型、被供电的装置的制造商等。通过这种方式，可以防止或最小化工业自动化环境中的伪造设备的使用。此外，电源可以用于向诸如控制器、输入/输出(I/O)模块、末端装置、现场装置(例如，过程传感器和/或致动器)等的设备认证自身。在一些实施例中，电源促进了电源与连接到电源的装置之间的密码通信。例如，电源能够提供电源与末端装置、现场装置等之间的双向密码通信。此外，在一些实施例中，操作员能够利用连接到网络的电源来获得关于诸如传感器、致动器或任何其它仪器之类的现场装置的认证信息。在一些实施例中，两个或更多认证模块(例如，第一认证模块和第二认证模块)被配置为在安装新装置时、在启动/重置时、周期性地、在预定时间处，和/或发生其它预先定义的事件时执行认证序列(例如，“握手”)。如果认证模块未能认证另一个装置和/或认证彼此，则可以部分地或完全禁用装置的至少其中之一(例如，未认证的装置)，和/或限制其与其它装置进行通信。

[0022] 在工业控制系统中，由控制元件/子系统(例如一个或多个通信/控制模块)来控制

或驱动各种工业元件/子系统(例如,输入/输出模块、电源模块、现场装置、开关、工作站和/或物理互连装置)。控制元件/子系统根据从动作发生器接收的编程和动作请求(例如,可执行软件模块、控制命令、数据请求等)来进行操作,所述动作发生器例如但不必限于操作员接口(例如,SCADA或人机接口(HMI))、工程接口、本地应用、远程应用等。在存在多个动作发生器时,工业控制系统可能容易遭受对数据和/或控制的未授权访问的攻击。此外,工业控制系统可能容易遭受能够以更新、应用图像、控制命令等形式传送的恶意软件、间谍软件或其它破坏/恶意软件的攻击。简单地认证操作员可能不足以保护系统使其不受恶意行动者、或者甚至可以经由有效登录或看似有效的(例如黑客)应用或操作员/工程接口而发起的未授权请求/命令的攻击。

[0023] 本公开内容针对用于防止未授权的动作请求在工业控制系统中进行处理的控制器、系统和技术。可以经由从动作发生器到工业元件/控制器(例如,通信/控制模块、输入/输出(I/O)模块、电源模块、现场装置、开关、工作站、物理互连装置等)的认证路径来保护操作的预先定义的选择或所有操作员动作和/或其它控制动作或请求。在实施方式中,工业控制系统要求动作认证器签署由动作发生器产生的动作请求。未签署的动作请求可以自动产生错误并且将不会被工业元件/控制器处理或执行。工业元件/控制器可以被配置为接收已签署的动作请求、验证已签署的动作请求的真实性、并且在已签署的动作请求的真实性得到验证时执行所请求的动作。通过这种方式,恶意的或其它未授权的动作请求不被处理,并且因此可以保护系统使其不受恶意软件、间谍软件、对控制参数的未授权的改变、对数据的未授权访问等的影响。

[0024] 示例性实施方式

[0025] 总体参考图1到6,根据本公开内容描述了示例性电源120。在一些实施例中,电源120包括一个或多个认证模块134,其被配置为向诸如I/O模块102、控制模块104等(例如,如图1中所示)的连接到电源120的装置认证电源120和/或电源120的一个或多个电池模块122。认证模块134还可以用于认证连接到电源120的一个或多个装置。在一些实施例中,认证模块134存储与电源120相关联的唯一标识符136和/或安全性凭证138(例如,如图5中所示,其中利用包括处理器140和存储一个或多个唯一标识符136和/或安全性凭证138的存储器142的控制器128来实施认证模块)。认证模块134可以被配置为基于认证来建立和/或阻止与连接到电源120的装置的连接。电源120还可以包括指示器(例如指示灯144)以(例如,向操作员)指示认证。

[0026] 在一些实施例中,电源120包括警报模块146。在本公开内容的实施例中,警报模块146被配置为在电源120和/或连接到电源120的装置满足条件和/或一组条件时(例如向操作员)提供警报。例如,在获得电源120和/或连接到电源的装置的认证和/或认证失败时,由认证模块134产生并由警报模块146提供警报。例如,电源120与耦合的被供电的装置(例如,I/O模块102和/或控制模块104)执行“握手”操作,以验证电源120与适当的和/或期望的装置配对。如果不是与适当的和/或期望的装置配对,则警报模块146可以用于(例如,经由网络)向操作员发出警报。在一些实施例中,以电子邮件的形式向操作员提供警报。在其它实施例中,以文本消息的形式向操作员提供警报。然而,这些警报通过示例的方式提供,并且不表示对本公开内容进行限制。在其它实施例中,向操作员提供不同的警报。此外,在认证程序满足条件时,可以向操作员提供多个警报(例如,电子邮件和文本消息等)。还应该注

意，可以由认证模块134和/或警报模块146为其它条件提供警报，所述其它条件包括但不必限于电源故障、电池模块故障、连接的装置故障、电源和/或被供电的装置的各种错误条件等。

[0027] 认证模块134还可以被配置为对电源120与连接到电源120的一个或多个装置之间的通信进行加密。如图1中所示，电源120可以包括加密模块148。例如，一种或多种密码协议用于在电源120与被供电的装置之间传送信息。这种密码协议的示例包括但不必限于传输层安全(TLS)协议、安全套接层(SSL)协议等。例如，电源120与被供电的装置之间的通信可以使用HTTP安全(HTTPS)协议，其中HTTP协议层叠在SSL和/或TLS协议上。

[0028] 在一些实施例中，可以在电源120与连接到电源120的装置之间执行认证序列。例如，电源120通过利用控制器128的认证模块134执行认证序列来认证耦合的I/O装置102、控制模块104等。在其它实施例中，连接到电源120的装置能够认证电源120。例如，控制模块104通过利用控制器128的认证模块134执行认证序列来认证耦合的电源120。在其它实施例中，一个电源120能够认证另一个电源120。例如，第一电源120通过执行第一电源120的控制器128的第一认证模块134与第二电源120的控制器128的第二认证模块134之间的认证序列来认证第二(例如，冗余)电源120。在一些实施例中，第二电源120也可以认证第一电源120。

[0029] 应该注意，尽管利用一些特殊性描述了作为控制器128的一部分的处理器140和存储器142(例如，参考图1)，但是这种配置通过示例的方式提供，并且不是要对本公开内容进行限制。因此，电池模块122中的一个或多个电池模块还可以包括处理器、存储器等(例如，除了控制器128所包括的处理器140和存储器142以外或代替控制器128所包括的处理器140和存储器142)。在这这种实施例中，电池模块122中的一个或多个可以包括一个或多个认证模块134，例如，其中认证模块134采用处理器和存储器(可能存储一个或多个密钥、证书、唯一标识符、安全性凭证等)来向一个或多个其它装置(例如，其它电池模块122、控制器128、控制元件或子系统等)认证电池模块122和/或认证与电源120耦合的其它装置(例如，其它电池模块122、控制器128、控制元件或子系统等)。

[0030] 在一些实施例中，电池模块122能够认证电源120的控制器128和/或诸如与电源120耦合的被供电的装置之类的连接的装置。例如，电池模块122通过利用电池模块122的认证模块134执行认证序列来认证电源120的控制器128和/或耦合的I/O装置102、控制模块104等。在其它实施例中，连接到电源120的被供电的装置能够认证电池模块122中的一个或多个电池模块。例如，控制模块104通过利用相应的电池模块122的认证模块134执行认证序列来认证连接的电源120的一个或多个(例如，每个)电池模块122。

[0031] 在一些实施例中，控制器128能够认证电池模块122中的一个或多个电池模块。例如，控制器128通过执行控制器128的认证模块134与相应的电池模块122的认证模块134之间的认证序列来认证一个或多个电池模块122。在其它实施例中，一个电池模块122能够认证另一个电池模块122。例如，第一电池模块122通过执行第一电池模块122的第一认证模块134与第二电池模块122的第二认证模块134之间的认证序列来认证第二电池模块122。在一些实施例中，第二电池模块122还可以认证第一电池模块122。

[0032] 电源120可以用于工业控制系统。例如，参考图2，根据本公开内容描述了示例性工业控制系统100。在实施例中，工业控制系统100可以包括工业控制系统(ICS)、可编程自动化控制器(PAC)、监视控制和数据采集(SCADA)系统、分布式控制系统(DCS)、可编程逻辑控

制器(PLC)、以及由诸如IEC1508之类的安全标准认证的工业安全系统，等等。工业控制系统100利用通信控制架构来实施包括控制元件或子系统的分布式控制系统，其中子系统由分布在整个系统内的一个或多个控制器控制。例如，一个或多个I/O模块102连接到一个或多个控制模块104。工业控制系统100被配置为传送到和来自I/O模块102的数据。I/O模块102可以包括输入模块、输出模块和/或输入和输出模块。例如，输入模块可以用于在过程中接收来自输入传感器的信息，而输出模块可以用于向输出致动器传送指令。例如，I/O模块104可以连接到用于测量天然气加工厂、精炼厂等的管道中压力的过程传感器106(例如，照明、辐射、气体、温度、电、磁、和/或声传感器)和/或连接到过程致动器108(例如，控制阀、液压致动器、磁致动器、电动机、螺线管、电子开关、发射器等)。

[0033] 在实施方式中，I/O模块102可以用于在应用中控制系统并且收集数据，所述应用包括但不必限于：工业加工，例如制造、生产、发电、制作和精炼；基础设施加工，例如水处理和分配、污水收集和处理、油气管道、电功率输送和分配、风电场、以及大型通信系统；用于楼宇、机场、船舶和空间站的设施加工(例如，以监测并控制加热、通风和空调(HVAC)装置和能耗)；大场地工业加工厂，例如油气、精炼、化工、药品、食品和饮料、水和污水、纸浆和纸张、公用电源、采矿、金属；和/或关键基础设施。

[0034] 在实施方式中，I/O模块102可以被配置为将从传感器106接收的模拟数据转换成数字数据(例如，利用模数转换器(ADC)电路等)。I/O模块102还可以连接到致动器108并且被配置为控制致动器108的一个或多个操作特性，例如速度、转矩等。此外，I/O模块102可以被配置为将数字数据转换成模拟数据，用以传送到致动器108(例如，利用数模(DAC)电路等)。在实施方式中，I/O模块102中的一个或多个I/O模块可以包括通信模块，其被配置用于经由诸如以太网总线、H1现场总线、过程现场总线(PROFIBUS)、可寻址远程传感器数据公路(HART)总线、Modbus等的通信子总线进行通信。此外，两个或更多I/O模块102可以用于为通信子总线提供容错和冗余连接。

[0035] 每个I/O模块102可以设置有用于区分一个I/O模块102和另一个I/O模块102的唯一标识符(ID)。在实施方式中，I/O模块102在连接到工业控制系统100时由其ID来识别。可以将多个I/O模块102用于工业控制系统100来提供冗余。例如，两个或更多I/O模块102可以连接到传感器106和/或致动器108。每个I/O模块102可以包括一个或多个端口，其提供与I/O模块102包括的诸如印刷电路板(PCB)等的硬件和电路的物理连接。

[0036] I/O模块102中的一个或多个I/O模块可以包括用于连接到其它网络的接口，所述其它网络包括但不必限于：广域蜂窝电话网络，例如3G蜂窝网络、4G蜂窝网络、或全球移动通信系统(GSM)网络；无线计算机通信网络，例如Wi-Fi网络(例如，利用IEEE 802.11网络标准操作的无线LAN(WLAN))；个人局域网(PAN)(例如，利用IEEE 802.15网络标准操作的无线PAN(WPAN))；广域网(WAN)；内联网；外联网；互联网；因特网；等等。此外，I/O模块102中的一个或多个I/O模块可以包括用于将I/O模块102连接到计算机总线等的连接。

[0037] 控制模块104可以用于监测并控制I/O模块102，并且用于将两个或更多I/O模块102连接在一起。在本公开内容的实施例中，控制模块104可以基于I/O模块102的唯一ID来在I/O模块102连接到工业控制系统100时更新路由表。此外，在使用多个冗余I/O模块102时，每个控制模块104可以实施关于I/O模块102的信息数据库的镜像，并且在从I/O模块102接收数据和/或向I/O模块102发送数据时更新它们。在一些实施方式中，利用两个或更多控

制模块104来提供冗余。为了增加安全性，控制模块104可以被配置为执行认证序列或握手，以在预先定义的事件或时间处认证彼此，所述预先定义的事件或时间包括但不必限于启动、重置、新控制模块104的安装、控制模块104的更换、周期性地、预定的时间等。此外，控制模块104可以被配置为以随机(例如，伪随机)时间间隔执行认证。

[0038] 可以将由工业控制系统100传送的数据分组化，即，可以将数据的分立的部分转换成包括数据部分以及网络控制信息等的数据包。工业控制系统100可以使用用于数据传输的一种或多种协议，包括面向比特的同步数据链路层协议，例如高级数据链路控制(HDLC)。在一些实施例中，工业控制系统100根据国际标准化组织(ISO)13239标准等实施HDLC。此外，两个或更多控制模块104可以用于实施冗余的HDLC。然而，应该注意，HDLC仅通过示例的方式提供，并且并不是要对本公开内容进行限制。因此，根据本公开内容，工业控制系统100可以使用其它各种通信协议。

[0039] 控制模块104中的一个或多个控制模块可以被配置为与诸如一个或多个控制回路反馈机制/控制器之类的用于监测和/或控制经由I/O模块102连接到工业控制系统100的仪器的部件交换信息。在实施方式中，控制器可以被配置作为微控制器/可编程逻辑控制器(PLC)、比例-积分-微分(PID)控制器等。在本公开内容的实施例中，I/O模块102和控制模块104包括网络接口，例如，用于经由网络110将一个或多个I/O模块102连接到一个或多个控制器。在实施方式中，网络接口可以被配置作为千兆以太网接口，用于将I/O模块102连接到局域网(LAN)。此外，两个或更多控制模块104可以用于实施冗余的千兆以太网。

[0040] 然而，应该注意，千兆以太网仅通过示例的方式提供，并且并不是要对本公开内容进行限制。因此，网络接口可以被配置用于将控制模块104连接到其它各种网络，包括但不必限于：广域蜂窝电话网络，例如3G蜂窝网络、4G蜂窝网络、或GSM网络；无线计算机通信网络，例如Wi-Fi网络(例如，利用IEEE 802.11标准操作的WLAN)；PAN(例如，利用IEEE802.15网络标准操作的WPAN)；WAN；内联网；外联网；互联网；因特网；等等。此外，可以利用计算机总线来实施网络接口。例如，网络接口可以包括外围部件互连(PCI)卡接口，例如Mini PCI接口等。此外，网络110可以被配置为包括单个网络或跨越不同接入点的多个网络。

[0041] 现在参考图3，工业控制系统100可以从多个源接收电功率。例如，从电网112(例如，利用来自AC输电干线的高电压功率)供应AC功率。还可以利用本地发电(例如，现场涡轮机或柴油本地发电机114)供应AC功率。电源116用于将来自电网112的电功率分配到工业控制系统100的自动化设备，例如控制器、I/O模块等。另一个电源118用于将来自本地发电机114的电功率分配到自动化设备。工业控制系统100还包括附加(备用)电源120，其被配置为利用多个电池模块122存储并返回DC功率。例如，电源120用作UPS。在本公开内容的实施例中，多个电源116、118和/或120(例如，物理上分散地)分布在工业控制系统100内。

[0042] 在一些实施例中，在机柜的级别上提供一个或多个电源116、118和/或120。例如，一个电源120用于向控制模块104以及其相关联的I/O模块102提供备用功率。在其它实施例中，一个电源120用于向控制模块104提供备用功率，并且另一个电源120用于向相关联的I/O模块102提供备用功率(例如，其中I/O模块102和控制模块104在设施内物理上分开一些距离，其中I/O模块102与控制模块104之间保持电隔离，等等)。

[0043] 电源116、118和/或120还可以被配置用于为诸如参考图2所描述的传感器106和/或致动器108之类的现场装置供电。例如，电源116和118中的一个或多个电源包括AC到DC

(AC/DC)变换器，其用于将AC(例如，由AC输电干线供应)转换成DC，用以传输到致动器108(例如，在致动器108是DC电动机或其它DC致动器的实施方式中)。此外，用于提供冗余的两个或更多电源116、118和/或120可以利用用于每个电源120的单独的(冗余的)电源背板连接到工业控制系统100的自动化设备。

[0044] 参考图4，电源120包括多个电池模块122。在本公开内容的实施例中，每个电池模块122包括锂离子电池单元124。例如，利用一点五伏(1.5V)锂离子电池单元、三伏(3V)锂离子电池单元等来实施电池模块122。在一些实施例中，电源120包括堆叠在一起的八(8)到十(10)个电池模块122。然而，八(8)到十(10)个电池模块122的堆叠体仅通过示例的方式提供，并且并不是要对本公开内容进行限制。在其它实施例中，将少于八(8)个或多于十(10)个电池模块122堆叠在一起。

[0045] 此外，应该注意，尽管电池模块122被描述为包括锂离子电池单元124，但是本公开内容的系统和技术可以使用其它可充电电池、存储和/或蓄电池技术，包括但不必限于铅酸电池、碱性电池、镍镉电池、镍金属氢化物电池、锂离子聚合物电池、锂硫电池、薄膜锂电池、钾离子电池、钠离子电池、镍铁电池、镍氢电池、镍锌电池、锂空气电池、磷酸锂铁电池、钛酸锂电池、溴化锌电池、钒氧化还原电池、钠硫电池、熔盐电池、银氧化物电池等。

[0046] 电池模块120中的每个电池模块包括实时电池监测器126，其可以利用例如印刷电路板(PCB)来实施。在本公开内容的实施例中，电池监测器126由操作电池单元124的控制器128(例如，微控制器)使用。例如，每个电池监测器126向控制器128提供每个相应的电池单元124的诊断信息。诊断信息包括但不必限于电池单元124的操作电压、电池单元124的操作电流(例如，以安培为单位)、进入电池单元124中的电荷单位(例如，以库伦为单位)、从电池单元124释放的电荷单位(例如，以库伦为单位)、电池单元124的寿命(例如，以时间为单位、以充电/放电循环的数量为单位等)，等等。

[0047] 在一些实施例中，每个电池监测器126单独连接到控制器128。在其它实施例中，多个电池监测器126连接到与控制器128连接的共享的通信信道，例如串行总线。电池监测器126还连接到功率调节器130(例如，包括变压器)，其从诸如电源116和/或电源118的外部电源接收功率。利用由功率调节器130供应的电能为电池单元124充电。利用另一个功率调节器132从电池单元124中释放电能，这可以用于调整由电池单元124供应的电能的一个或多个输出特性，例如电压。

[0048] 在本公开内容的实施例中，每个电池模块122包括具有箔包裹的电池单元124的支撑架，其中多个支撑架可以堆叠在一起，以使电池单元124保持密封，同时允许电池单元124在箔内的膨胀和收缩。在本公开内容的实施例中，支撑架中的电池单元124还包围包括电池监测器126的PCB。此外，PCB由电池单元124供电并且被配置为限制流入和流出每个电池单元124的电流。例如，电池监测器126包括电子信号开关器件(例如，以模拟开关方式串联连接的两个(2)场效应晶体管(FET))，其防止能量在未经电池监测器126授权的情况下存储在电池中和/或从电池返回。通过这种方式，在电池单元124的端子连接到非预期的电路径时(例如，短路)，阻止电池单元124的电连接。此外，在电池监测器126不活动时(例如，在电池单元124中没有电荷时)，阻止电池单元124的电连接。在本示例中，在电池模块122插入电源120中时至少部分地为电池模块122充电。

[0049] 在本公开内容的实施例中，电池模块122是堆叠的并且利用设置在每个支撑架上

的电接触部(例如,电连接器)来连接。电连接器(例如,经由电池监测器PCB)电连接到电池单元124并且可以设置在支撑架上,而不需要从支撑架延伸出来的电线(其需要与电池单元124进行焊接连接)。例如,在一个支撑架上提供卡扣电连接器(例如,设置在支撑架的顶表面上),该电连接器与另一个支撑架上的相对应的卡扣电连接器(例如,设置在另一个支撑架的底表面上)配对。电连接器可以被配置为增大电连接器之间的接触部对表面面积和/或提供电连接器的自对准(例如,通过将一个电连接器的一部分配置用于插入到另一个电连接器中)。

[0050] 在本公开内容的实施例中,电连接器被几何布置为(例如,定位、改变大小等)防止多个电池模块122以非期望方式连接在一起。例如,一个电接触部可以总体上关于支撑架面向上方,而另一个电接触部可以总体上关于支撑架面向下方。在其它实施例中,视觉提示被提供用于对准两个电池模块122(例如,颜色编码、记号等)。

[0051] 此外,电源120可以包括槽、沟、轨道等,用于为电池模块122提供机械对准,例如用于将一个电池模块122的电连接器与另一个电池模块122的配对的电连接器和/或与至电源120的电连接器对准。例如,电池模块122包括接头或柱,其被配置用于插入到电源120的外壳的相应轨道中,并且提供电池模块122关于外壳的对准。此外,控制器128可以将唯一的物理标识(ID)与每个电池模块122相关联,以唯一地识别耦合在特定序列中和/或耦合在关于电源120的外壳的特定位置处的每个电池模块122。

[0052] 在本公开内容的实施例中,电源120被构建用于机柜安装、机架安装、壁板安装等。电源120的外壳可以由诸如丁二烯苯乙烯(ABS)或另一种塑料材料之类的刚性绝缘材料构建,所述材料可以用于容纳在电池单元发生故障时所释放的能量。此外,外壳可以被配置为容纳或至少大体上容纳可能由于电池故障而被释放的化学电池单元部件,例如锂。此外,电源120中容纳的部件可以彼此电隔离。例如,至控制器128的信号与电池监测器126和电池单元124电气隔离。此外,控制器128和功率调节器130与电池模块122和功率调节器132(例如,利用单独的变压器、光隔离器等)电气和/或故障隔离。

[0053] 现在参考图5,控制器128(例如,经由网络110)连接到工业控制系统100。在本公开内容的实施例中,控制器128在控制器级别和/或在每个电池模块122级别上实施安全和/或诊断。控制器128,包括其部件中的一些或全部,可以在计算机控制下进行操作。例如,处理器140可以包括在控制器128中,以利用软件、固件、硬件(例如,固定逻辑电路)、手动处理或它们的组合来控制本文中所描述的控制器128的部件和功能。本文中所使用的术语“控制器”、“功能”、“服务”和“逻辑”通常表示与对控制器128的控制相结合的软件、固件、硬件或软件、固件或硬件的组合。在软件实施方式的情况下,模块、功能或逻辑表示在处理器(例如,中央处理单元(CPU)或CPU)上执行时完成指定任务的程序代码。程序代码可以存储在一个或多个计算机可读存储装置(例如,内部存储器和/或一个或多个有形介质)等中。可以在具有多种处理器的多种商用计算平台上实施本文中所描述的结构、功能、方式和技术。

[0054] 处理器140为控制器128提供处理功能,并且可以包括任何数量的处理器、微控制器或其它处理系统、以及用于存储由控制器128访问或产生的数据和其它信息的常驻或外部存储器。处理器140可以执行实施本文中所描述的技术的一个或多个软件程序。处理器140不由形成处理器的材料或处理器中所采用的处理机制限制,并且像这样,处理器140可以经由(多个)半导体和/或晶体管(例如,利用电子集成电路(IC)部件)等实施。

[0055] 控制器128还包括存储器142。存储器142是有形计算机可读存储介质的示例，其提供存储功能以存储与控制器128的操作相关联的各种数据，例如软件程序和/或代码段、或指导处理器140和控制器128的其它可能部件来执行本文中所描述的功能的其它数据。因此，存储器142可以存储数据，例如用于操作电源120(包括其部件)等的指令程序。在本公开内容的实施例中，存储器142可以存储用于电源120的唯一标识符136和/或安全性凭证138。应该注意，尽管描述了单个存储器142，但是可以采用多种类型的存储器(例如，有形非暂态存储器)和存储器的组合。存储器142可以与处理器140成为一体，可以包括独立的存储器，或者可以是二者的组合。存储器142可以包括但不必限于可移除和不可移除存储器部件，例如随机存取存储器(RAM)、只读存储器(ROM)、闪存存储器(例如，安全数字(SD)存储器卡、迷你SD存储器卡和/或微型SD存储器卡)、磁存储器、光存储器、通用串行总线(USB)存储器装置、硬盘存储器、外部储存器等。在实施方式中，电源120和/或存储器142可以包括可移除集成电路卡(ICC)存储器，例如由用户身份模块(SIM)卡、通用用户身份模块(USIM)卡、通用集成电路卡(UICC)等提供的存储器。

[0056] 控制器128包括通信接口150。通信接口150被操作地配置为与电源120的部件通信。例如，通信接口150可以被配置为传送用于存储在控制器128中的数据、从控制器128的存储中取回数据等。通信接口150还与处理器140通信地耦合，以有助于电源120和处理器140的部件之间的数据传递，例如，用于将从与控制器128通信地耦合的装置接收的输入发送到处理器140和/或将输出发送到诸如电池监测器126之类的与控制器128通信地耦合的装置。例如，利用诸如串行总线之类的共享通信信道来实施通信接口150，以将处理器连接到多个电池监测器126。

[0057] 在本公开内容的实施例中，控制器128被配置用于与电池监测器126进行双向通信。例如，控制器128从电池监测器126收集诊断信息(例如，关于电池单元124的状态信息和/或可靠性信息)。控制器128还操作电池模块122，例如，指导电池模块122来存储并返回由电源116、电源118等供应的电能。应该注意，尽管通信接口150被描述为控制器128的部件，但是可以将通信接口150的一个或多个部件实施为经由有线和/或无线连接与控制器128通信地耦合的外部部件。控制器128还可以包括和/或(例如，经由通信接口150)连接到一个或多个输入/输出(I/O)装置，包括但不必限于显示器、鼠标等。例如，控制器128可以连接到显示装置，例如能够指示电源120的状态的多色(例如，三色)发光二极管(LED)(例如，指示器灯144)。

[0058] 通信接口150和/或处理器140可以被配置为与多种不同网络110通信，所述多种不同网络110包括但不必限于：广域蜂窝电话网络，例如3G蜂窝网络、4G蜂窝网络、或全球移动通信系统(GSM)网络；无线计算机通信网络，例如Wi-Fi网络(例如，利用IEEE 802.11网络标准操作的无线局域网(WLAN))；互联网；因特网；广域网(WAN)；局域网(LAN)；个人局域网(PAN)(例如，利用IEEE 802.15网络标准操作的无线个人局域网(WPAN))；公共电话网络；外联网；内联网；等等。然而，该列表仅通过示例的方式提供，并且并不是要对本公开内容进行限制。此外，可以利用计算机总线来实施通信接口150。例如，通信接口150可以包括PCI卡接口，例如迷你PCI接口等。此外，通信接口150可以被配置为与单个网络或跨越不同接入点的多个网络通信。通过这种方式，控制器128用于将电源120通信地耦合到工业控制系统100。

[0059] 现在参考图6，控制元件或子系统(例如，I/O模块102、控制模块104、电源120等)由

一个或多个背板连接在一起。例如，控制模块104可以由通信背板152连接到I/O模块102。此外，电源120可以由电源背板154连接到I/O模块102和/或连接到控制模块104。在本公开内容的实施例中，物理互连装置(例如开关、连接器或电缆，例如但不限于美国非临时申请No.14/446,412中所描述的那些)用于连接到I/O模块102、控制模块104、电源120、以及其它可能的工业控制系统设备。例如，电缆用于将控制模块104连接到网络110，另一根电缆用于将电源116连接到电网112，另一根电缆用于将电源118连接到本地发电机114，等等。

[0060] 在本公开内容的实施例中，工业控制系统100实施安全控制系统。例如，工业控制系统100包括安全性凭证源(例如，工厂156)和安全性凭证实施者(例如，密钥管理实体158)。工厂156被配置为产生唯一安全性凭证(例如，诸如唯一标识符136和/或安全性凭证138之类的密钥、证书等)。密钥管理实体158被配置为向I/O模块102、控制模块104、电源116、电源118和/或电源120(例如，包括多个电池模块122中的一个或多个电池模块和/或控制器128)提供由工厂156产生的唯一安全性凭证。例如，可以向I/O模块102和相关联的电源120均提供唯一安全性凭证。

[0061] 然后，基于唯一安全性凭证执行用于认证工业控制系统100中实施的控制元件或子系统的认证过程。例如，在实施例中，控制模块104和电源120可以操作用于基于唯一安全性凭证(例如，基于认证过程)与彼此进行双向通信。此外，在本文中所公开的安全工业控制系统100中，向工业控制系统100的多个(例如，每个)控制元件和子系统(例如，I/O模块、电源、物理互连装置等)提供安全性凭证，用于在工业控制系统100的多个(例如所有)级别上提供安全性。此外，可以在制造期间(例如，在制成时)为元件提供唯一安全性凭证(例如，密钥、证书等)，并且可以从制成开始由工业控制系统100的密钥管理实体来管理，用以提升工业控制系统100的安全性。

[0062] 在一些实施例中，利用连接到物理互连装置(例如，单线加密芯片)或包括在物理互连装置中的控制器来连接控制元件或子系统，控制器允许实施部件(例如，电源120)与连接到该部件的物理互连装置(例如电缆组件)之间的认证。例如，微处理器安全加密技术可以被内置在电缆组件中并且对工业控制系统100的特定部件进行键控。这种配置在用户将电缆组件安装(例如，插入)到未配置为与该电缆组件连接的部件中时为工业控制系统100提供安全性。在实施例中，在物理互连装置中的一个或多个(例如，每个)物理互连装置中实施单线串行键(例如，单线嵌入键)。

[0063] 在本公开内容的实施例中，工业控制系统100的元件和/或物理互连装置(例如，电缆组件)之间的通信包括认证过程。可以执行认证过程，用以认证工业控制系统100中实施的元件和/或物理互连装置。在实施方式中，认证过程可以利用与元件和/或物理互连装置相关联的安全性凭证来认证该元件和/或物理互连装置。例如，安全性凭证可以包括密钥、证书(例如，公钥证书、数字证书、身份证书、安全性证书、不对称证书、标准证书、非标准证书)和/或标识号码。在实施例中，包括在工业控制系统100的部件和/或物理互连装置中和/或连接到工业控制系统100的部件和/或物理互连装置的控制器(例如，安全微控制器)可以被配置为执行认证过程。

[0064] 在实施方式中，为工业控制系统100的多个控制元件或子系统(例如，元件和/或物理互连装置)提供它们自身的唯一安全性凭证。例如，在制造工业控制系统100的每个元件时，为元件提供其自身唯一的(多个)证书组、加密密钥和/或标识号码(例如，在元件制成时

限定各自的加密密钥和证书组)。证书、加密密钥和/或标识号码组被配置用于提供/支持强加密。可以利用诸如国家安全局(NSA)算法、国家标准与技术研究院(NIST)算法等的标准(例如,商用现成品或技术(COTS))加密算法来实施加密密钥。

[0065] 在一些实施例中,密钥和证书可以存储在片上存储器(OCM)中,例如,存储在认证模块的SRAM中。此外,敏感任务(例如,具有秘密信息、有时甚至具有公共信息的任务)可以具有在OCM中执行的堆栈。例如,可以在来自OCM中本地存储的堆栈的内核空间或应用空间中执行加密任务。

[0066] 基于认证过程的结果,可以激活被认证的元件,可以在工业控制系统100内启用或禁用元件的部分功能,可以在工业控制系统100内启用元件的完整功能,和/或可以完全禁用工业控制系统100内的元件的功能(例如,在该元件与工业控制系统100的其它元件之间不促成任何通信)。

[0067] 在实施例中,与工业控制系统100的元件相关联的密钥、证书和/或标识号码可以指定该元件的原始设备制造商(OEM)。如本文中所使用的,可以将术语“原始设备制造商”或“OEM”限定为在物理上制造装置(例如,元件)的实体和/或装置的供应商,例如从物理制造商购买装置并且销售装置的实体。因此,在实施例中,可以由既是物理制造商又是装置供应商的OEM来制造并分配(销售)装置。然而,在其它实施例中,可以由仅作为供应商而不是物理制造商的OEM来分配装置。在这种实施例中,OEM可以使装置由物理制造商来制造(例如,OEM可以从物理制造商购买、合同购买、订购装置)。

[0068] 此外,在OEM包括非装置物理制造商的供应商的情况下,装置可以带有供应商的商标而不是物理制造商的商标。例如,在元件(例如,电源120)与作为供应商而不是物理制造商的特定OEM相关联的实施例中,元件的密钥、证书和/或标识号码可以指定该原产地。在工业控制系统100的元件的认证期间,在确定经认证的元件是由与工业控制系统100的一个或多个其它元件的OEM不同的实体来制造或供应时,则可以在工业控制系统100内至少部分地禁用该元件的功能。例如,可以限制该元件与工业控制系统100的其它元件之间的通信(例如,数据传输),以使元件不能在工业控制系统100内工作/发挥作用。当工业控制系统100的元件的其中之一需要更换时,该特征能够防止工业控制系统100的用户无意中利用不同类的元件(例如,具有与工业控制系统100的其它元件不同到原产地(不同OEM)的元件)来替代元件,并且在工业控制系统100中实施元件。通过这种方式,本文中所描述的技术能够防止将其它OEM的元件替换到安全工业控制系统100中。在一个示例中,可以防止利用提供类似功能的元件替换由原始OEM提供的元件,因为替换的元件不能在原始OEM的系统内进行认证和操作。在另一个示例中,可以由原始OEM为第一经销商提供具有第一组物理和密码标签的元件,并且可以在工业控制系统100中安装第一经销商的元件。在本示例中,可以由同一原始OEM为第二经销商提供具有第二(例如,不同的)组物理和密码标签的元件。在本示例中,可以防止第二经销商的元件在工业控制系统100内进行操作,因为它们不能认证第一经销商的元件并且与其一起进行操作。然而,还应该注意,第一经销商和第二经销商可以订立双方协定,其中第一元件和第二元件可以被配置为在同一工业控制系统100内进行认证和操作。此外,在一些实施例中,还可以实施允许交互操作的经销商之间的协定,以使得该协定仅应用于特定客户、客户组、设施等。

[0069] 在另一个实例中,用户可以尝试在工业控制系统100内实施错误指定(例如,错误

标记)的元件。例如,错误标记的元件可以具有标记在其上的物理记号,该物理记号错误地指示该元件与和工业控制系统100的其它元件的OEM相同的OEM相关联。在这种实例中,由工业控制系统100实施的认证过程可以使用户被警报该元件是伪造品。该过程还可以促进工业控制系统100的改进的安全性,因为伪造元件通常是可以将恶意软件引入工业控制系统100中的载体。在实施例中,认证过程为工业控制系统100提供了安全空隙,确保安全工业控制系统与不安全网络物理隔离。

[0070] 密钥管理实体158可以被配置用于管理密码系统中的密钥(例如,加密密钥)。密钥的这种管理(例如,密钥管理)可以包括密钥的产生、交换、存储、使用和/或更换。例如,密钥管理实体158被配置为用作安全性凭证源,其为工业控制系统100的元件产生唯一安全性凭证(例如,公共安全性凭证、秘密安全性凭证)。密钥管理涉及用户和/或系统级别上的密钥(例如,在用户或系统之间)。

[0071] 在实施例中,密钥管理实体158包括安全实体,例如位于安全设施中的安全实体。密钥管理实体158可以位于与I/O模块102、控制模块104和网络110距离远的位置。例如,防火墙160能够将密钥管理实体158与控制元件或子系统和网络110(例如,企业网络)分开。在实施方式中,防火墙160可以是基于软件或硬件的网络安全系统,其通过分析数据包并且基于规则组判断是否应该允许数据包通过来控制流入和流出的网络流量。防火墙160因此在受信任的安全内部网络(例如,网络110)与未被认定为安全可信任的另一个网络162(例如,云和/或因特网)之间建立屏障。在实施例中,防火墙160允许在密钥管理实体158与控制元件或子系统中的一个或多个部件和/或网络110之间进行选择性(例如,安全)通信。在示例中,可以在工业控制系统100内的各个位置处实施一个或多个防火墙。例如,可以将防火墙集成到网络110的交换机和/或工作站中。

[0072] 如所描述的,安全工业控制系统100还可以包括一个或多个制造实体(例如,工厂156)。工厂156可以与工业控制系统100的元件的原始设备制造商(OEM)相关联。密钥管理实体158可以经由网络(例如,云)与制造实体通信地耦合。在实施方式中,当在一个或多个工厂156处制造工业控制系统100的元件时,密钥管理实体158可以与元件通信地耦合(例如,可以具有至元件的加密通信管道)。密钥管理实体158可以利用通信管道来在制造时为元件提供安全性凭证(例如,向元件中插入密钥、证书和/或标识号码)。

[0073] 此外,当元件投入使用(例如,激活)时,可以将密钥管理实体158(例如,经由加密通信管道)通信地耦合到全世界的每个个体元件,并且能够确认并签署特定代码的使用、撤销(例如,去除)任何特定代码的使用和/或启用任何特定代码的使用。因此,密钥管理实体158能够与原始制造(例如,生产)元件的工厂处的每个元件通信,以使得元件生而具有受管理的密钥。可以由密钥管理实体158来维护包括用于工业控制系统100的每个元件的所有加密密钥、证书和/或标识号码的主数据库和/或表。密钥管理实体158通过与元件通信而被配置用于撤销密钥,由此促进认证机制抵抗盗窃和重新使用部件的能力。

[0074] 在实施方式中,密钥管理实体158可以经由另一个网络(例如,云和/或因特网)和防火墙与控制元件和子系统中的一个或多个部件和/或网络110通信地耦合。例如,在实施例中,密钥管理实体158可以是集中式系统或分布式系统。此外,在实施例中,可以对密钥管理实体158进行本地管理或远程管理。在一些实施方式中,密钥管理实体158可以位于网络110和/或控制元件或子系统之内(例如,集成到其中)。密钥管理实体158可以通过多种方式

来提供管理和/或可以被管理。例如，取决于层级，可以由位于中央位置的客户、由位于个体工厂位置的客户、由外部第三方管理公司和/或由处于工业控制系统100的不同层级的客户、以及位于不同位置的客户来实施/管理密钥管理实体158。

[0075] 可以由认证过程提供不同级别的安全性(例如，可缩放、安全性的用户配置量)。例如，可以提供基础级别的安全性，其认证元件并保护元件内的代码。也可以增加其它层级的安全性。例如，可以将安全性实施到使诸如电源120之类的部件在未进行适当认证的情况下不能加电的程度。在实施方式中，在元件中实施代码中的加密，在元件上实施安全性凭证(例如，密钥和证书)。安全性可以分布于(例如，流动于)整个工业控制系统100。例如，安全性可以流过工业控制系统100一直到末端用户，末端用户知道模块在该实例中被设计为控制什么部件。在实施例中，认证过程提供装置的加密、识别，用于系统硬件和软件部件的安全通信和认证(例如，经由数字签名)。

[0076] 在实施方式中，可以实施认证过程以提供和/或启用由不同制造商/卖主/供应商(例如，OEM)制造和/或供应的元件在安全工业控制系统100内的交互操作性。例如，可以启用由不同制造商/卖主/供应商制造和/或供应的元件之间的选择性的(例如，一些)交互操作性。在实施例中，在认证期间实施的唯一安全性凭证(例如，密钥)可以形成层次结构，由此允许由工业控制系统100的不同元件执行不同功能。

[0077] 连接工业控制系统100的部件的通信链路还可以采用设置(例如注入和/或填充)于部件中的诸如短包(例如，小于六十四(64)字节的包)之类的数据包，以提供增加的安全级别。使用短包增大了可以向通信链路上注入外部信息(例如，诸如虚假消息之类的恶意内容、恶意软件(病毒)、数据挖掘应用等)的难度级别。例如，可以将短包注入到控制模块104与电源120之间传送的数据包之间的间隙内的通信链路上，以阻止外部实体向通信链路上注入恶意内容的能力。

[0078] 在本公开内容的实施例中，为了发起认证序列，第一认证模块(例如，包括在电源120、电源120的控制器128、电源120的电池模块122、诸如I/O装置102之类的控制元件或子系统、控制模块104等中)被配置为向第二认证模块(例如，包括在电源120、电源120的控制器128、电源120的电池模块122、诸如I/O装置102之类的控制元件或子系统、控制模块104等中)传送请求数据报。在实施方式中，请求数据报包括第一明文随机数(随机数A)、包含第一装置认证密钥(DAKA)的第一装置认证密钥证书(CertDAKA)、以及第一身份属性证书(IACA)。在一些实施例中，第一认证模块被配置为利用真正的随机数发生器(在下文中为“TRNG”)产生第一随机数(随机数A)，并且将第一随机数(随机数A)、第一装置认证密钥证书(CertDAKA)、和第一身份属性证书(IACA)连结或组合，以产生请求数据报。在一些实施例中，第一装置认证密钥证书(CertDAKA)和第一身份属性证书(IACA)由第一认证模块进行本地存储。例如，证书可以存储在第一认证模块的本地存储器(例如，ROM、RAM、闪存存储器或其它非暂态存储介质)中。

[0079] 第二认证模块被配置为通过利用由装置生命周期管理系统(DLM)产生或利用密码库函数获取的公钥对第一装置认证密钥证书(CertDAKA)和第一身份属性证书(IACA)进行验证来证实请求数据报。就这点而言，公钥可以存储在认证模块的SRAM或另一个本地存储器中并且与密码库函数一起使用来验证或以密码方式签署交换的数据，例如在认证模块之间交换的随机数。在一些实施例中，第二认证模块可以利用椭圆曲线数字签名算法(在下文

中为“ECDSA”)或其它验证操作来验证证书。在一些实施例中,第二认证模块还可以被配置为通过验证以下内容来证实来自明文值的证书值:证书类型是每个证书的装置认证密钥(在下文中为“DAK”)或身份属性证书(在下文中为“IAC”);IAC名称匹配,DAK证书模块类型匹配模块类型论据;和/或消息有效负载中的每个证书的微处理器序列号(在下文中为“MPSN”)彼此匹配。在一些实施例中,第二认证模块还可以被配置为验证DAK和IAC证书不在本地撤销列表(例如,包括撤销的和/或无效的证书的列表或数据库)中。在第二认证模块未能证实请求数据报时,第二认证模块可以产生错误消息,以部分地或完全禁用第一认证模块和/或断开或限制到/来自第一认证模块的通信。

[0080] 响应于有效请求数据报,第二认证模块被配置为向第一认证模块传送响应数据报。在实施方式中,响应数据报包括第二明文随机数(随机数B)、与第一随机数和第二随机数相关联的第一签名(SigB[NonceA‖NonceB])、包含第二装置认证密钥(DAKB)的第二装置认证密钥证书(certDAKB)、以及第二身份属性证书(IACB)。在一些实施例中,第二认证模块被配置为利用TRNG产生第二随机数(NonceB)、将第一随机数(NonceA)和第二随机数(NonceB)连结或组合、并且利用由第二认证模块本地存储的私钥(例如,DAK)来签署连结/组合的随机数。第二认证模块还被配置为将第二随机数(NonceB)、与第一随机数和第二随机数相关联的第一签名(SigB[NonceA‖NonceB])、第二装置认证密钥证书(certDAKB)和第二身份属性证书(IACB)连结或组合以产生响应数据报。在一些实施例中,第二装置认证密钥证书(CertDAKB)和第二身份属性证书(IACB)由第二认证模块进行本地存储。例如,证书可以存储在第二认证模块的本地存储器(例如,ROM、RAM、闪存存储器或其它非暂态存储介质)中。

[0081] 第一认证模块被配置为通过利用本地存储的或使用ECDSA或另一种验证操作从密码库中获取的公钥来对第二装置认证密钥证书(CertDAKB)和第二身份属性证书(IACB)进行验证,以证实响应数据报。在一些实施例中,第一认证模块还可以被配置为通过验证以下内容来证实来自明文值的证书值:IAC&DAK证书具有匹配的MPSN,IAC名称匹配,两个证书(IAC&DAK)上的证书类型均正确,两个证书上的颁发者名称正确,DAK模块类型是正确类型(例如,通信/控制模块)。在一些实施例中,第一认证模块还可以被配置为验证DAK和IAC证书不在本地撤销列表中。

[0082] 为证实响应数据报,第一认证模块还被配置为验证与第一随机数和第二随机数相关联的第一签名(sigB[NonceA‖NonceB])。在一些实施例中,第一认证模块被配置为通过如下方式验证第一签名(sigB[NonceA‖NonceB]):连结第一本地存储的随机数(NonceA)和从第二认证模块接收的第二明文随机数(NonceB),利用公共装置认证密钥(例如,利用来自certDAKB的DAKB)验证第一密码签名(sigB[NonceA‖NonceB]),并且对第一随机数和第二随机数的本地产生的连结与第一随机数和第二随机数的密码验证的连结进行比较。在第一认证模块未能证实响应数据报时,第一认证模块可以产生错误消息,以部分地或完全禁用第二认证模块和/或断开或限制到/来自第二认证模块的通信。

[0083] 第一认证模块还被配置为在响应数据报有效时向第二认证模块传送认证数据报。在实施方式中,认证数据报包括与第一随机数和第二随机数相关联的第二签名(sigA[NonceA‖NonceB])。在一些实施例中,第一认证模块被配置为签署第一随机数和第二随机数、由第一认证模块本地存储的私钥(例如,DAK)的本地产生的级联。在响应数据报无效时,

可以利用“失败的”认证数据报替代认证数据报，“失败的”认证数据报包括与第二随机数和由第一认证模块产生的错误报告(例如，“失败”)消息相关联的签名(sigA[NonceB‖Error])。

[0084] 响应于认证数据报，第二认证模块还可以被配置为向第一认证模块传送响应认证数据报。在实施方式中，响应认证数据报包括与第一随机数和由第二认证模块产生的错误报告(例如，“成功”或“失败”)消息相关联的签名(sigB[NonceA‖Error])。在一些实施例中，第二认证模块被配置为通过验证与第一随机数和第二随机数相关联的第二签名(sigA[NonceA‖NonceB])来证实认证数据报。在一些实施例中，第二认证模块被配置为通过如下方式来验证第二签名(sigA[NonceA‖NonceB])：将从第一认证模块接收的第一明文随机数(NonceA)和第二本地存储的随机数(NonceB)连结，利用公共装置认证密钥(例如，利用来自certDAKA的DAKA)来验证第二密码签名(sigA[NonceA‖NonceB])，并且对第一随机数和第二随机数的本地产生的连结与第一随机数和第二随机数的密码验证的连结进行比较。除了错误报告消息，在第二认证模块未能证实认证数据报时，第二认证模块可以部分地或完全禁用第一认证模块和/或断开或限制到/来自第一认证模块的通信。

[0085] 在采用认证模块的装置根据“主-从”配置进行布置的实施方式中，主装置(例如，第一认证模块)可以被配置为认证每个从装置。如果认证失败，主装置可以至少部分地禁用或限制到/来自未认证的从装置的通信。替代地，在没有主装置的情况下并行操作的两个或更多从装置可以认证彼此，其中失败的认证导致两个装置都被部分或完全禁用。例如，如果两个或更多冗余电源120在启动或另一个预定义时间/事件时未成功完成认证序列，则可以禁用它们。

[0086] 现在参考图7和8，每个电源120或任何其它工业元件/控制器206可以至少部分地根据来自动作发生器202的请求/命令进行操作。在实施方式中，动作发生器202是操作员接口208(例如，SCADA和/或HMI)、包括编辑器212和编译器214的工程接口210、本地应用220、远程应用216(例如，经由本地应用220通过网络218进行通信)等。在图7和8所示的认证路径200中，仅在动作请求已经被动作认证器204签署和/或加密时，工业元件/控制器206(例如，电源120)才处理动作请求(例如，对数据、控制命令、固件/软件更新、设定点控制、应用图像下载等的请求)。这防止了来自有效用户配置文件的未授权的动作请求，并且进一步保护系统不受来自无效(例如，黑客)配置文件的未授权的动作请求的影响。

[0087] 在本公开内容的实施例中，动作认证器204可以位于动作发生器202的现场位置(例如，直接连接的装置生命周期管理系统(DLM)222或安全工作站226)或二者设置得较远(例如，经由网络218连接的DLM 222)。通常，动作认证器204包括存储有私钥的存储介质和处理器，处理器被配置为签署和/或加密由动作发生器202利用私钥产生的动作请求。私钥存储在不能经由标准操作员登录访问的存储器中。例如，安全工作站226可能需要物理密钥、便携式加密装置(例如，智能卡、RFID标签等)和/或生物特征输入来进行访问。

[0088] 在一些实施例中，动作认证器204包括便携式加密装置，例如智能卡224(其可以包括安全微处理器)。通过这种方式，整个装置(包括私人存储的密钥和与它们通信的处理器)可以由已经被授权访问动作发生器202的接口的操作员或用户携带。无论动作认证节点204经由安全还是非安全工作站访问认证路径200，可以在便携式加密装置的架构内安全地签署和/或加密来自动作发生器202的动作请求(例如，与使用可能较不安全的工作站或基于

云的架构相反)。通过示例,未被授权的人在能够认证经由动作发生器202发送的任何动作请求之前将只能物理地占有智能卡224。

[0089] 在一些实施例中,可以采用安全性的多个层级。例如,动作认证器204可以包括安全工作站226,其仅可以经由智能卡224访问以签署和/或加密动作请求。此外,可以经由生物特征或多因素密码装置228(例如,指纹扫描仪、虹膜扫描仪、面部识别装置等中的一种或多种)访问安全工作站226。在一些实施例中,多因素密码装置228可能在使智能卡224或其它便携式加密装置能够签署动作请求之前需要有效的生物特征输入。

[0090] 由动作发生器202驱动的电源120或任何其它工业元件/控制器206被配置为接收已签署的动作请求、验证所签署的动作请求的真实性、以及在所签署的动作请求的真实性得到验证时执行所请求的动作。在一些实施例中,工业元件/控制器206(例如,电源120)包括存储介质(例如,SD/微型SD卡、HDD、SSD或任何其它非暂态存储装置)(例如,电源120的存储器142),其被配置为存储动作请求(例如,应用图像、控制命令和/或由动作发生器发送的任何其它数据)。工业元件/控制器206还包括处理器(例如,电源120的处理器140),其在验证签名之后完成/执行动作请求(即,完成所请求的动作)。在一些实施例中,由动作发生器202和/或动作认证器204对动作请求进行加密,并且还必须在能够执行所请求的动作之前由处理器140进行解密。在实施方式中,工业元件/控制器206包括虚拟键开关234(例如,在处理器140上运行的软件模块),其使处理器140能够仅在动作请求签名得到验证之后和/或在对动作请求进行解密之后完成所请求的动作。在一些实施例中,每个以及每一个动作或关键动作的选择中的每个关键动作在运行在工业元件/控制器206上之前必须清空认证路径。

[0091] 图9描绘了根据示例性实施例的用于认证工业控制系统中的动作请求的过程300。在实施方式中,过程300可以由工业控制系统100(例如,如参考图1到6所描述的)和/或工业控制系统100的认证路径200(例如,如参考图7和8所描述的)证明。发生动作请求(方框310)。例如,利用操作员/工程接口208/210和/或远程/本地应用接口216/220来产生动作请求。然后,利用动作认证器来签署动作请求(方框320)。例如,动作认证器204用于签署动作请求。在一些实施例中,可以利用动作认证器对动作请求进行加密(方框322)。然后,将所签署的动作请求发送(例如,下载)到工业元件/控制器(方框330)。例如,向工业元件/控制器206(例如,向电源120)提供动作请求。接下来,验证所签署的动作请求的真实性(方框340)。在一些实施例中,可以利用工业元件/控制器对动作请求进行解密(方框342)。例如,工业元件/控制器206能够对动作请求进行解密。然后,可以在所签署的动作请求的真实性得到验证时执行请求的动作(方框350)。例如,电源120执行由操作员/工程接口208、210和/或远程/本地应用接口216、220所请求的动作。

[0092] 为了增强安全性,工业元件/控制器206(例如,电源120)还可以被配置为在由工业元件/控制器206运行所请求的动作之前利用动作认证器204(例如,利用智能卡224)执行认证序列。例如,可以在方框350之前、或者甚至在方框330之前执行所谓的“握手”。在一些实施例中,可以利用更复杂的认证序列来执行签名和验证方框320和340。此外,在一些实施例中,可以执行认证序列作为附加的安全措施,以加强较简单的签名验证和/或解密措施。

[0093] 在一些实施例中,由工业元件/控制器206实施的认证序列可以包括向动作认证器204发送请求数据报,例如,其中请求数据报包括第一密码随机数、第一装置认证密钥证书

(例如,包含装置认证密钥的第一认证证书)和第一身份属性证书。然后,从动作认证器204接收响应数据报,例如,其中响应数据报包括第二随机数、与第一随机数和第二随机数相关联的第一签名、第二装置认证密钥证书(例如,包含装置认证密钥的第二认证证书)和第二身份属性证书。接下来,可以通过验证与第一随机数和第二随机数相关联的第一签名、第二装置认证密钥证书和第二身份属性证书来证实响应数据报。接下来,可以将认证数据报发送到动作认证器204(例如,在确定响应数据报为有效时),其中认证数据报包括与第一随机数和第二随机数相关联的第二签名。

[0094] 替代地,动作认证器204可以发起握手,在这种情况下,由工业元件/控制器206实施的认证序列可以包括从动作认证器204接收请求数据报,例如,其中请求数据报包括第一随机数、第一装置认证密钥证书和第一身份属性证书。接下来,可以通过验证第一装置认证密钥证书和第一身份属性证书来证实请求数据报。然后,可以在请求数据报有效时将响应数据报发送到动作认证器,例如,其中响应数据报包括第二随机数、与第一随机数和第二随机数相关联的第一签名、第二装置认证密钥证书和第二身份属性证书。接下来,可以接收来自动作认证器204的认证数据报,例如,其中认证数据报包括与第一随机数和第二随机数相关联的第二签名。然后,例如可以通过验证与第一和第二随机数相关联的第二签名来证实认证数据报。

[0095] 可以利用上述技术中的一种或多种技术(例如,参考由认证模块执行的认证)来实现可以由工业元件/控制器206和动作认证器204实施的握手或认证序列。此外,动作发生器202、动作认证器204和工业元件/控制器206中的每个部件可以包括能够执行本文中所描述的功能或操作(例如,方法300和认证序列的步骤)的电路和/或逻辑。例如,动作发生器202、动作认证器204和工业元件/控制器206中的每个部件可以包括一个或多个处理器,其执行由非暂态机器可读介质永久、半永久或暂时存储的程序指令,所述非暂态机器可读介质例如但不必限于硬盘驱动器(HDD)、固态磁盘(SDD)、光盘、磁存储装置、闪存驱动器或SD/微型SD卡。

[0096] 通常,可以利用硬件(例如,诸如集成电路之类的固定逻辑电路)、软件、固件、手动处理或它们的组合来实施本文中所描述的功能中的任何功能。因此,上述公开内容中论述的方框通常表示硬件(例如,诸如集成电路之类的固定逻辑电路)、软件、固件或它们的组合。在硬件配置的实例中,上述公开内容中论述的各个方框可以被实施为集成电路与其它功能。这种集成电路可以包括给定方框、系统或电路的所有功能、或方框、系统或电路的功能的一部分。此外,可以在多个集成电路上实施方框、系统或电路的元件。这种集成电路可以包括各种集成电路,包括但不必限于单片集成电路、倒装芯片集成电路、多芯片模块集成电路和/或混合信号集成电路。在软件实施方式的实例中,上述公开内容中论述的各个方框表示可执行指令(例如,程序代码),其在处理器上被执行时完成指定的任务。这些可执行指令可以存储在一种或多种有形计算机可读介质中。在一些这种实例中,整个系统、方框或电路可以利用其软件或固件等价物来实施。在其它实例中,可以在软件或固件中实施给定系统、方框或电路的一部分,而在硬件中实施其它部分。

[0097] 结论

[0098] 尽管已经以具体到结构特征和/或过程操作的语言来描述了主题内容,但是要理解,在所附权利要求中所限定的主题内容不必限于上述具体特征或动作。相反,上述具体特

征和动作被公开作为实施权利要求的示例形式。

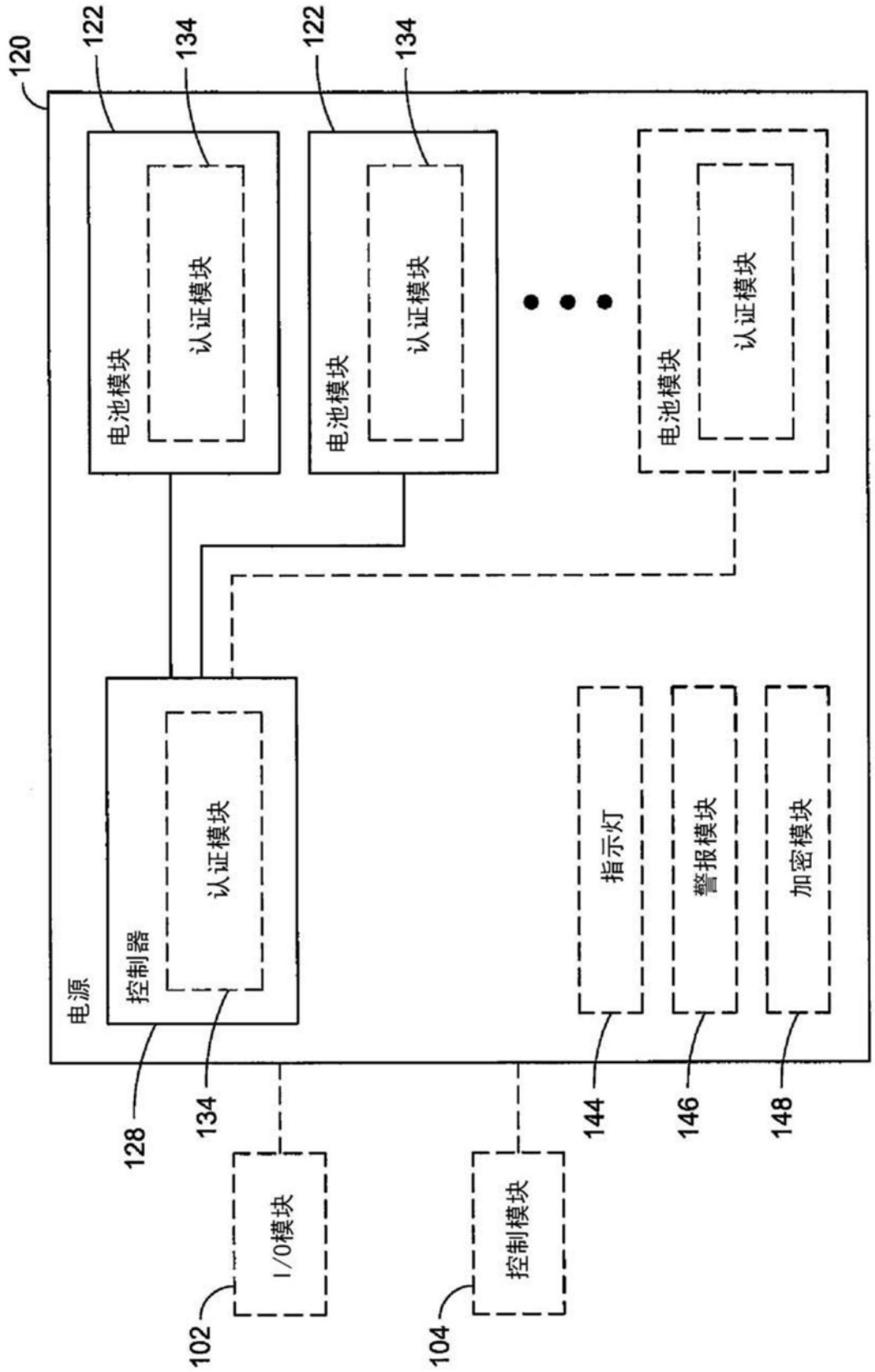

120
122
134
122
134
电池模块
认证模块
电池模块
认证模块
电池模块
认证模块
电源
控制器
认证模块
128
134
102
I/O模块
104
控制模块
144
指示灯
146
警报模块
148
加密模块

图1

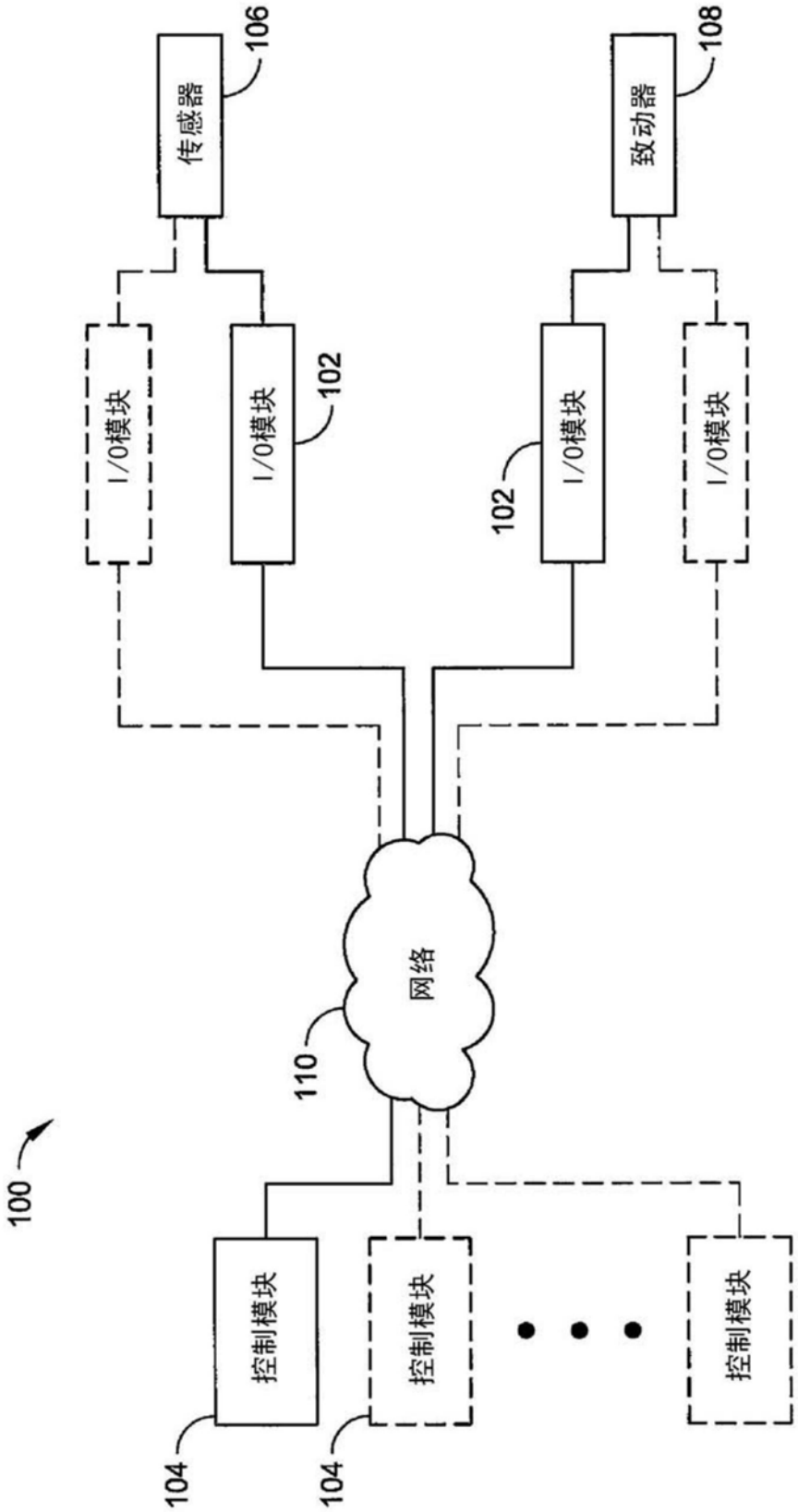

100
网络
110
传感器
106
致动器
108
I/O模块
102
I/O模块
102
I/O模块
I/O模块
控制模块
104
控制模块
104
控制模块

图2

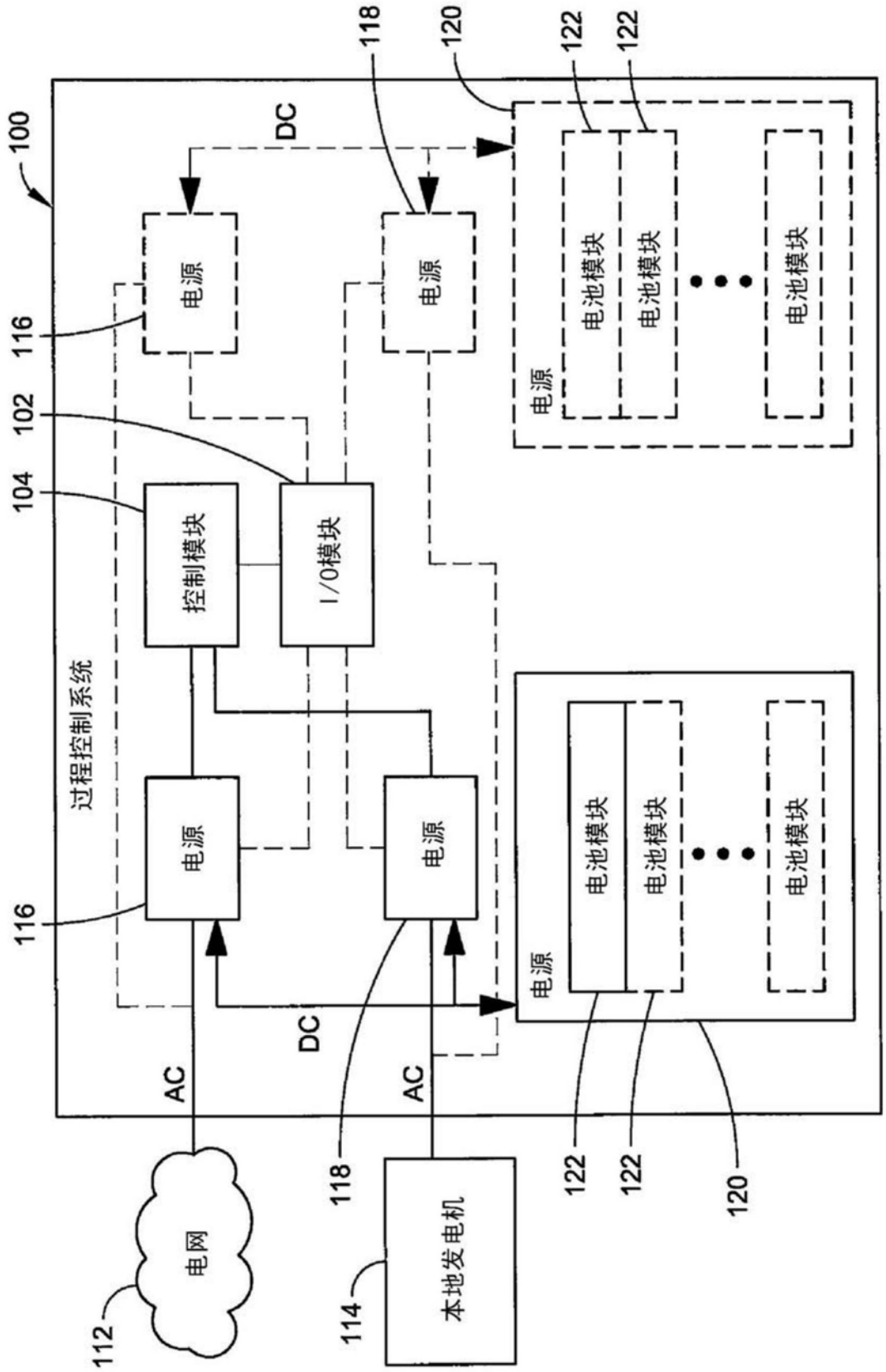

100
过程控制系统
DC
AC
电源
控制模块
I/O模块
电池模块
电网
本地发电机
112
114
116
118
120
122
102
104

图3

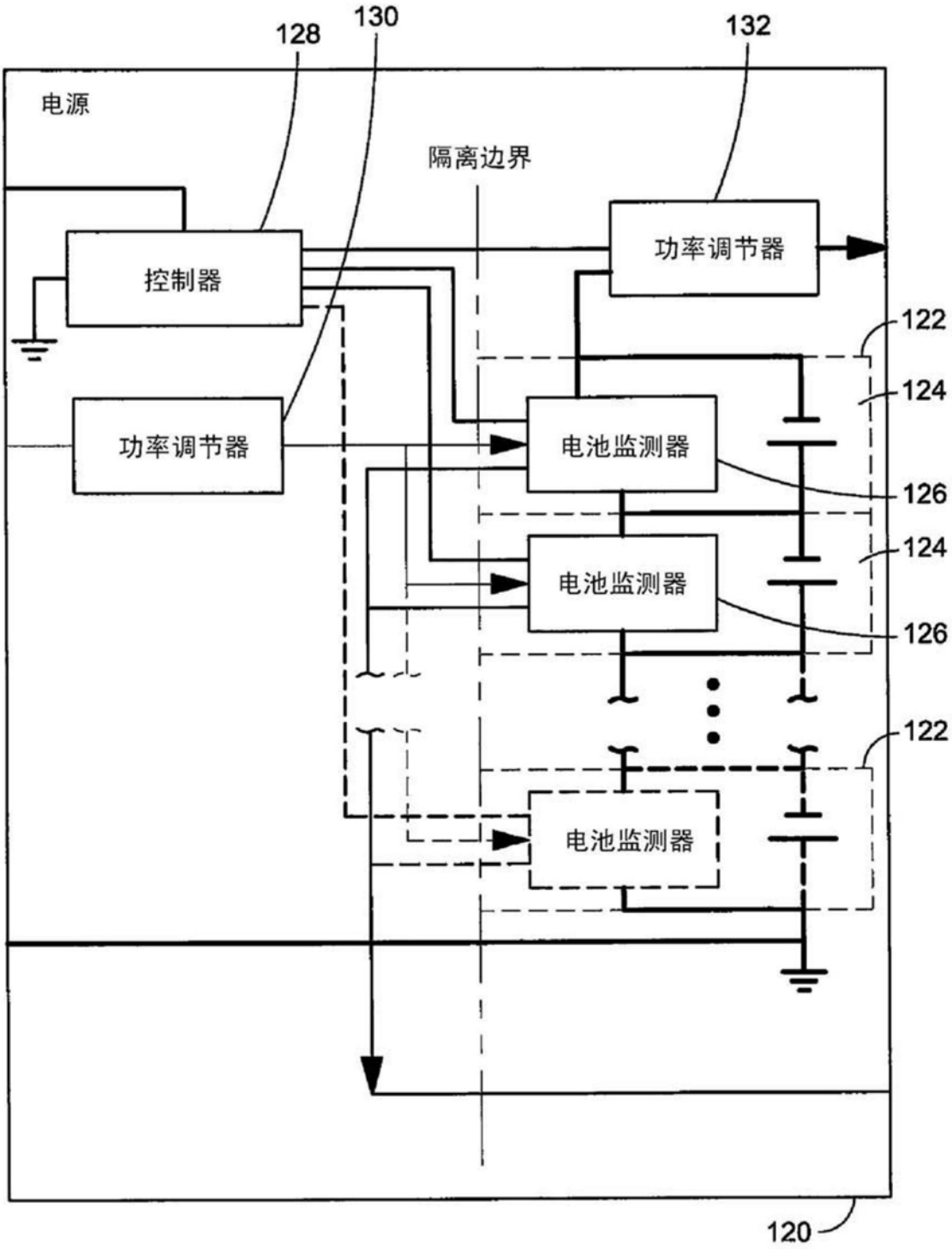

128
130
132
电源
隔离边界
控制器
功率调节器
功率调节器
122
124
电池监测器
126
124
电池监测器
126
122
电池监测器
120

图4

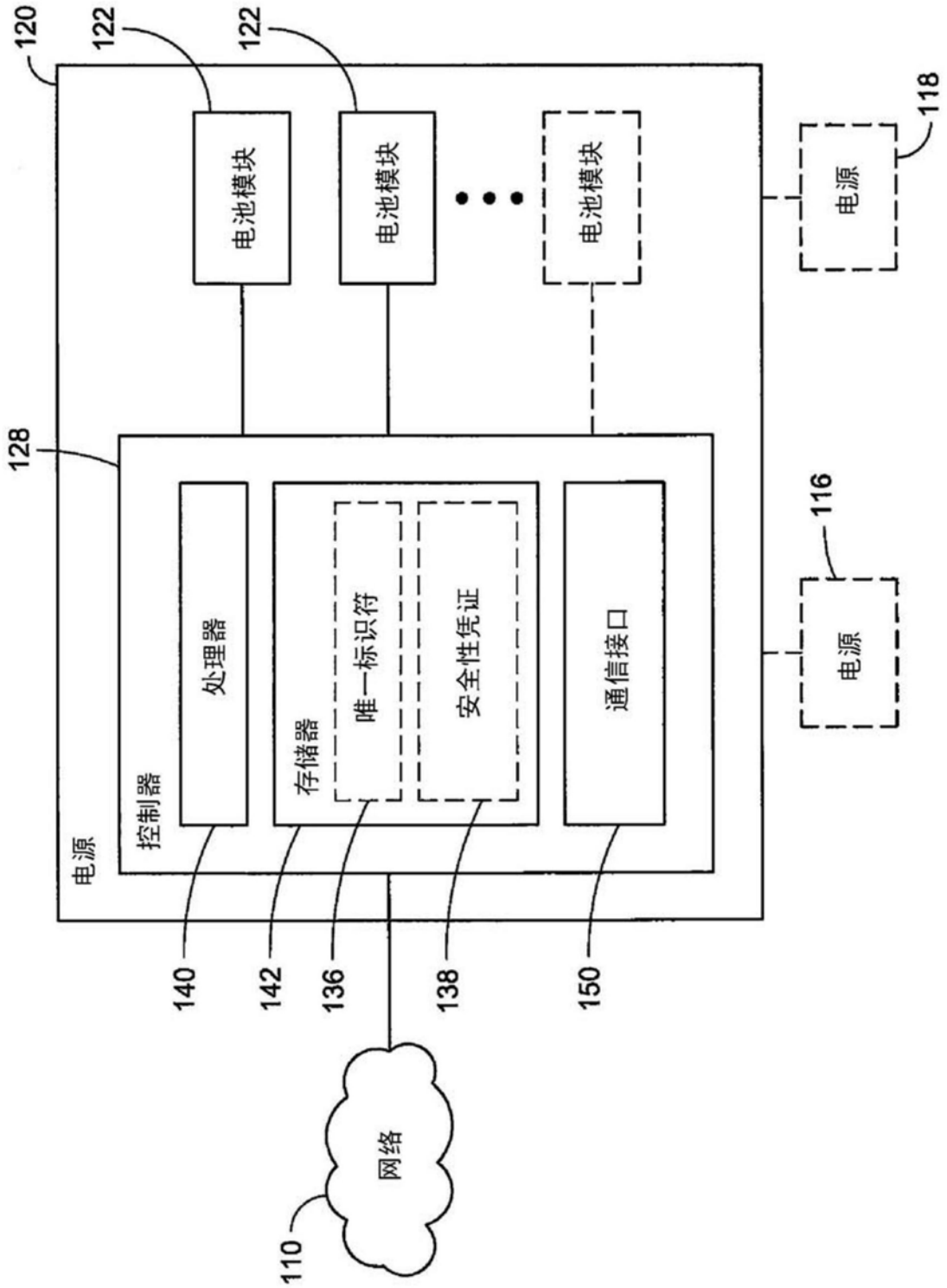

120
122
122
电池模块
电池模块
电池模块
118
电源
128
处理器
存储器
唯一标识符
安全性凭证
通信接口
116
电源
控制器
电源
140
142
136
138
150
网络
110

图5

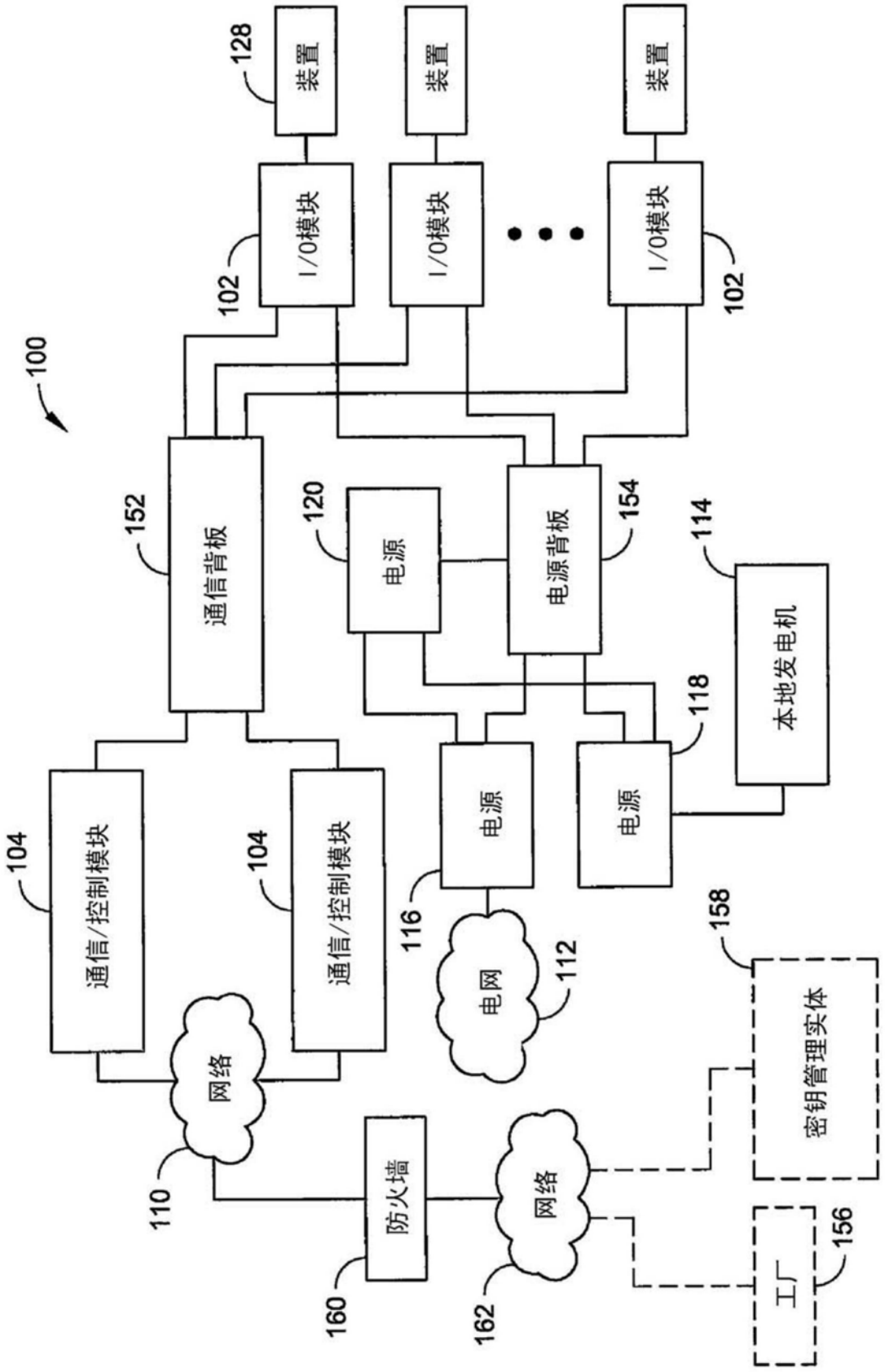

100
128
装置
装置
装置
102
I/O模块
I/O模块
I/O模块
102
152
通信背板
120
电源
电源背板
154
114
本地发电机
104
通信/控制模块
104
通信/控制模块
116
电源
电源
118
158
密钥管理实体
电网
112
网络
网络
110
防火墙
160
162
工厂
156

图6

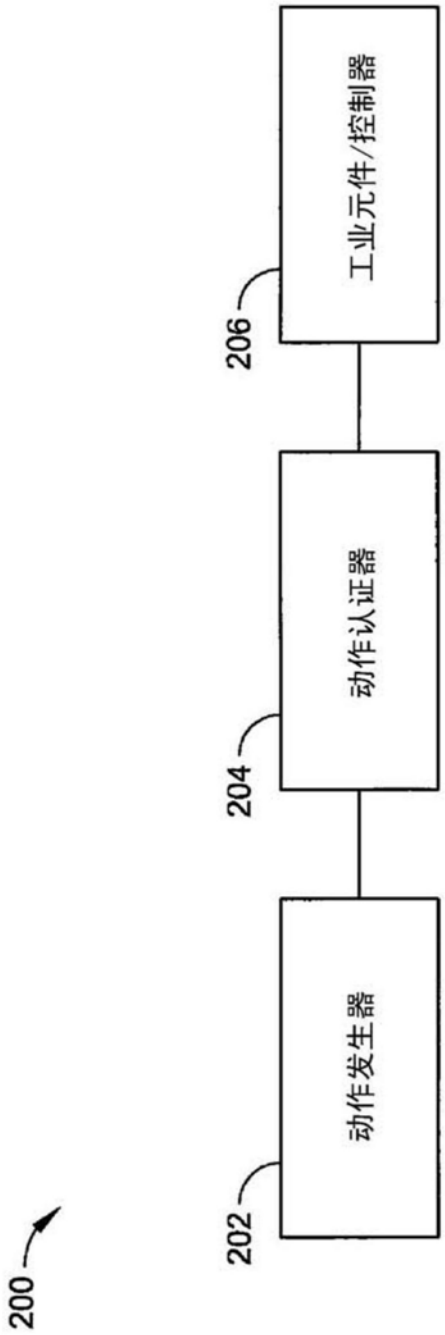


图7

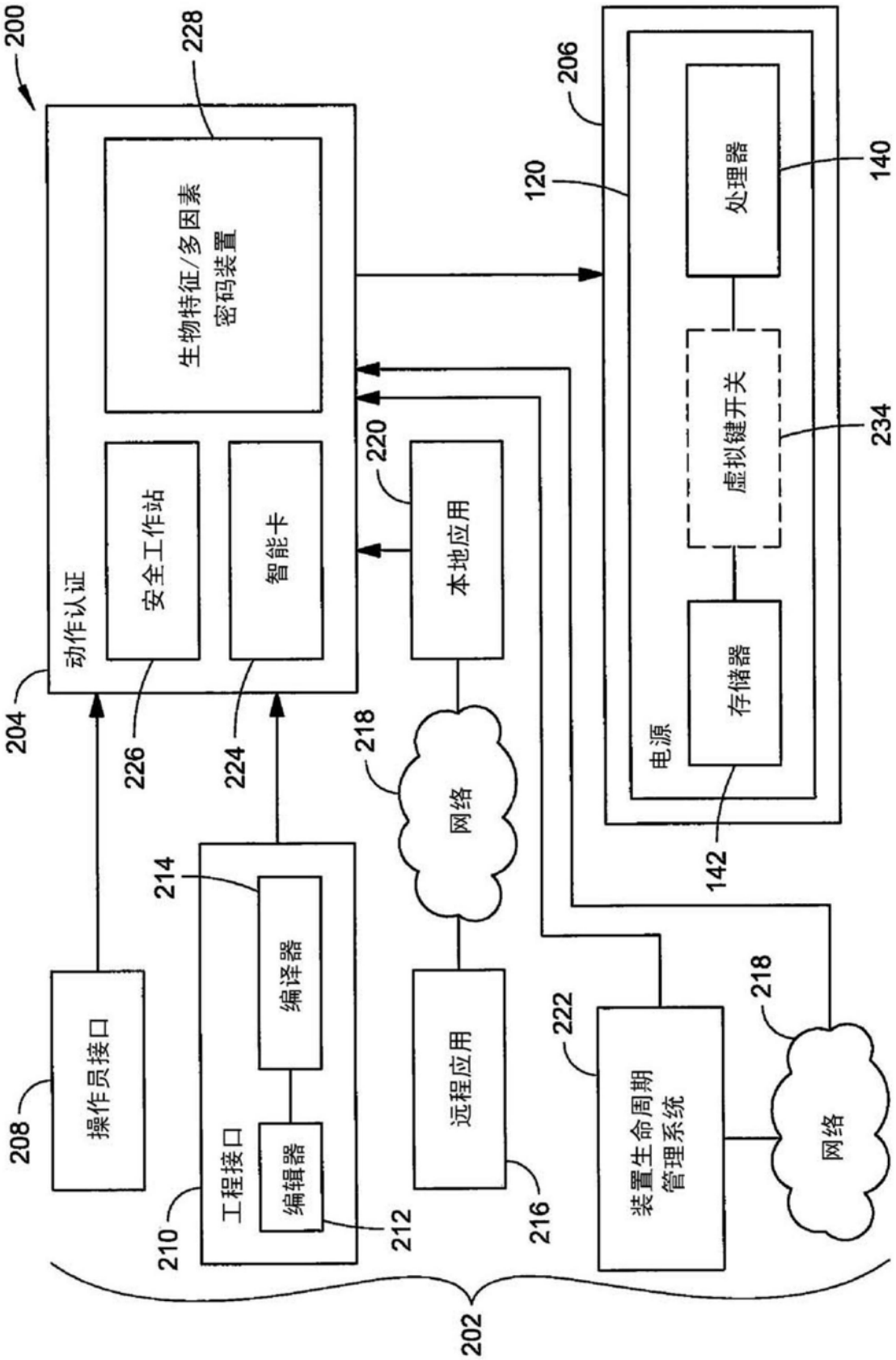

200
228
生物特征/多因素
密码装置
206
120
处理器
140
安全工作站
智能卡
220
本地应用
虚拟键开关
234
动作认证
204
226
224
218
网络
电源
存储器
142
214
编译器
操作员接口
208
工程接口
编辑器
210
212
远程应用
216
222
装置生命周期
管理系统
218
网络
202

图8

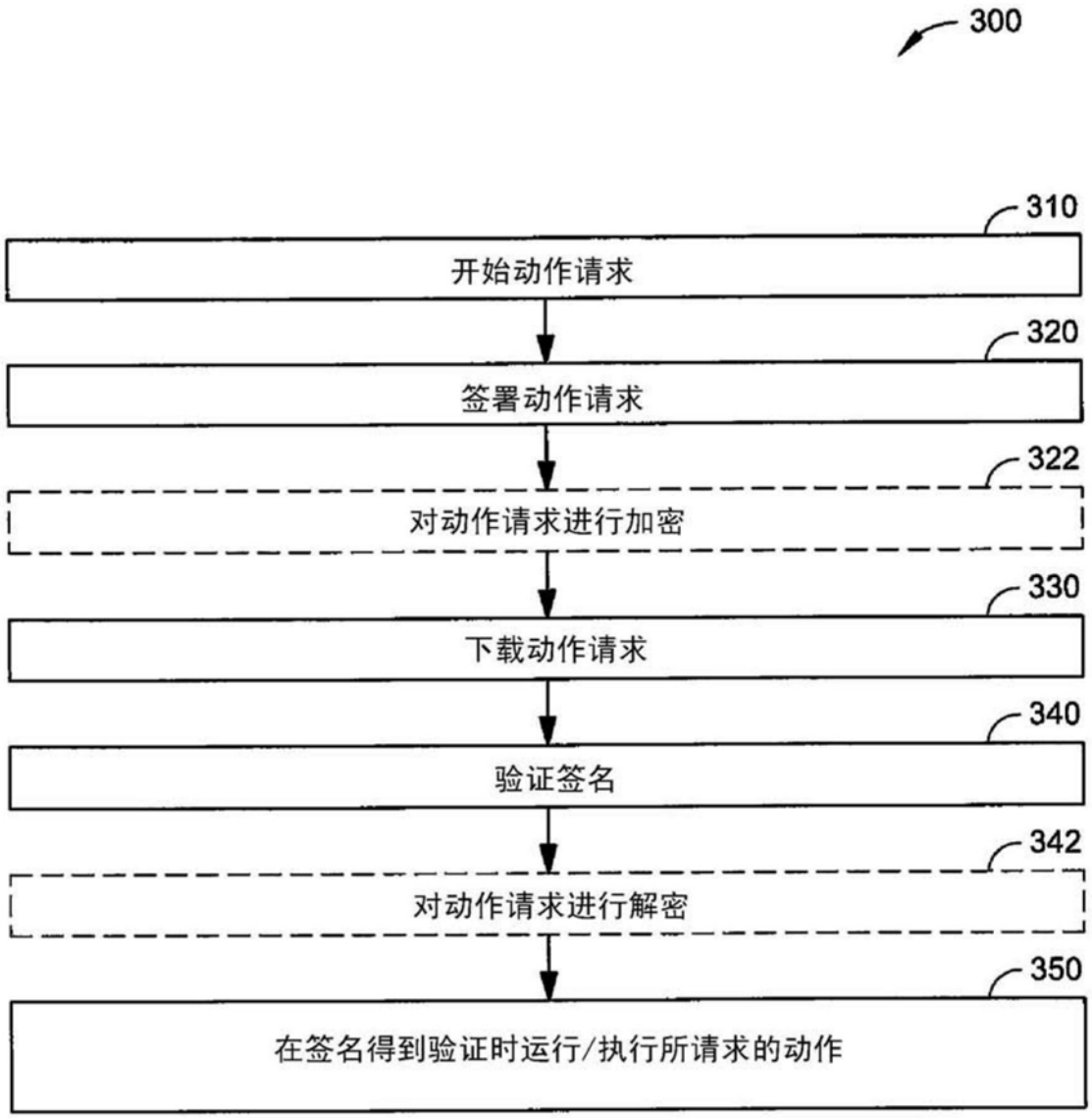

300
310
开始动作请求
320
签署动作请求
322
对动作请求进行加密
330
下载动作请求
340
验证签名
342
对动作请求进行解密
350
在签名得到验证时运行/执行所请求的动作

图9