(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106249706 A
(43)申请公布日 2016.12.21

(21)申请号 201610404083.X

(22)申请日 2016.06.08

(30)优先权数据
14/734,399 2015.06.09 US

(71)申请人 费希尔控制产品国际有限公司
地址 美国爱荷华州

(72)发明人 S·C·安德森

(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 曹雯

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

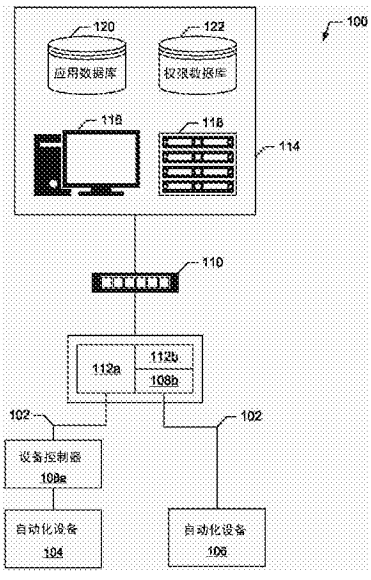
权利要求书3页 说明书11页 附图6页

(54)发明名称

过程控制设备中的定制应用环境

(57)摘要

公开了用于提供设备控制器中的定制应用空间的方法和装置。示例性公开的方法包括:将设备控制器通信地耦合到主机。示例性主机提供过程控制系统内的设备控制器和自动化设备。示例性公开的方法还包括:将过程控制应用安装到设备控制器的固件中的应用空间中。示例性过程控制应用由主机提供权限数据。示例性公开的方法还包括执行应用空间中的过程控制应用。示例性过程控制应用扩展设备控制器的功能。示例性公开的方法还包括缓和过程控制应用对设备控制器的物理资源的访问。示例性权限数据限定了过程控制应用具有对物理资源中的哪些物理资源的访问。



CN 106249706 A

1.一种用于管理的方法,包括:

将设备控制器通信地耦合到主机,所述主机提供过程控制系统内的所述设备控制器和自动化设备;

将过程控制应用安装到所述设备控制器的固件中的应用空间中,所述过程控制应用被提供有权限数据;

经由处理器执行所述应用空间中的所述过程控制应用,所述过程控制应用对所述设备控制器的功能进行扩展;以及

缓和所述过程控制应用对所述设备控制器的物理资源的访问,所述权限数据限定所述过程控制应用具有对所述物理资源中的哪些物理资源的访问。

2.根据权利要求1所述的方法,其中,缓和所述过程控制应用对所述设备控制器的所述物理资源的访问包括:保持与所述设备控制器内的固件存储空间分离的应用存储空间,其中,所述过程控制应用具有对所述应用存储空间的访问,但不具有对所述固件存储空间的访问。

3.根据权利要求1所述的方法,其中,缓和所述过程控制应用对所述设备控制器的所述物理资源的访问包括:向所述过程控制应用提供对所述设备控制器的网络通信的访问,所述权限数据指定所述过程控制应用能够与所述主机进行通信的频率。

4.根据权利要求1所述的方法,其中,缓和所述过程控制应用对所述设备控制器的所述物理资源的访问包括:向所述过程控制应用提供对所述设备控制器的自动化设备通信的访问,所述权限数据指定所述过程控制应用能够与所述自动化设备进行通信的频率。

5.根据权利要求4所述的方法,其中,所述权限数据指定对所述过程控制应用何时能够与所述自动化设备进行通信进行调节的逻辑条件。

6.根据权利要求1所述的方法,还包括:

对数据空间进行保持,所述过程控制应用将数据写入到所述数据空间以与所述设备控制器的所述固件共享;以及

基于所述权限数据来缓和所述过程控制应用对所述数据空间的访问。

7.根据权利要求6所述的方法,其中,所述过程控制应用是由以下情况下的至少一个来提供的:当安装所述过程控制应用时由所述主机提供;或者当制造所述设备控制器时由制造商提供。

8.一种设备控制器,所述设备控制器与将要安装在过程控制系统中的自动化设备相关联,所述设备控制器包括:

设备控制器管理器,所述设备控制器管理器将所述设备控制器通信地耦合到主机,所述主机提供所述过程控制系统内的所述设备控制器和所述自动化设备;

安装器,所述安装器将过程控制应用安装到所述设备控制器的固件中的应用空间中,所述过程控制应用由所述主机提供权限数据;

应用框架处理器,所述应用框架处理器用于:

执行所述应用空间中的所述过程控制应用,所述过程控制应用对所述设备控制器的功能进行扩展;以及

缓和所述过程控制应用对所述设备控制器的物理资源的访问,所述权限数据定义用于缓和所述过程控制应用对所述设备控制器的所述物理资源的所述访问的规则。

9.根据权利要求8所述的设备控制器，其中，为了缓和所述过程控制应用对所述设备控制器的所述物理资源的访问，所述应用框架处理器保持与所述设备控制器内的固件存储空间分离的应用存储空间，其中，所述过程控制应用具有对所述应用存储空间的访问，但不具有对所述固件存储空间的访问。

10.根据权利要求8所述的设备控制器，其中，为了缓和所述过程控制应用对所述设备控制器的所述物理资源的访问，所述应用框架处理器向所述过程控制应用提供对所述设备控制器的网络通信的访问，所述权限数据指定所述过程控制应用能够与所述主机进行通信的频率。

11.根据权利要求8所述设备控制器，其中，为了缓和所述过程控制应用对所述设备控制器的所述物理资源的访问，所述应用框架处理器向所述过程控制应用提供对所述设备控制器的自动化设备通信的访问，所述权限数据指定所述过程控制应用能够与所述自动化设备进行通信的频率。

12.根据权利要求11所述的设备控制器，其中，所述权限数据指定对所述过程控制应用何时能够与所述自动化设备进行通信进行调节的逻辑条件。

13.根据权利要求8所述的设备控制器，其中，为了缓和所述过程控制应用对所述设备控制器的所述物理资源的访问，所述应用框架处理器保持数据空间，所述过程控制应用将数据写入到所述数据空间以与所述设备控制器的所述固件共享。

14.根据权利要求13所述的设备控制器，其中，为了缓和所述过程控制应用对所述设备控制器的所述物理资源的访问，所述应用框架处理器基于所述权限数据来缓和所述过程控制应用对所述数据空间的访问。

15.一种制品，所述制品包括当被执行时使得设备控制器至少进行以下操作的指令：

将所述设备控制器通信地耦合到主机，所述主机提供过程控制系统内的所述设备控制器和自动化设备；

将过程控制应用安装到所述设备控制器的固件中的应用空间中，所述过程控制应用由所述主机提供权限数据；

执行所述应用空间中的所述过程控制应用，所述过程控制应用对所述设备控制器的功能进行扩展；以及

缓和所述过程控制应用对所述设备控制器的物理资源的访问，所述权限数据定义用于缓和所述过程控制应用对所述设备控制器的所述物理资源的所述访问的规则。

16.根据权利要求15所述的制品，其中，为了缓和所述过程控制应用对所述设备控制器的所述物理资源的访问，所述指令使得所述设备控制器保持与所述设备控制器内的固件存储空间分离的应用存储空间，其中，所述过程控制应用具有对所述应用存储空间的访问，但不具有对所述固件存储空间的访问。

17.根据权利要求15所述的制品，其中，为了缓和所述过程控制应用对所述设备控制器的所述物理资源的访问，所述指令使得所述设备控制器向所述过程控制应用提供对所述设备控制器的网络通信的访问，所述权限数据指定所述过程控制应用能够与所述主机进行通信的频率。

18.根据权利要求15所述的制品，其中，为了缓和所述过程控制应用对所述设备控制器的所述物理资源的访问，所述指令使得所述设备控制器向所述过程控制应用提供对所述设

备控制器的自动化设备通信的访问，所述权限数据指定所述过程控制应用能够与所述自动化设备进行通信的频率。

19.根据权利要求18所述的制品，其中，所述权限数据指定对所述过程控制应用何时能够与所述自动化设备进行通信进行调节的逻辑条件。

20.根据权利要求15所述的制品，所述指令使得所述设备控制器保持数据空间，所述过程控制应用将数据写入到所述数据空间以与所述设备控制器的所述固件共享。

过程控制设备中的定制应用环境

技术领域

[0001] 概括地说，本公开内容涉及控制在过程控制系统中的自动化设备，更具体而言，涉及提供过程控制设备中的定制应用环境。

背景技术

[0002] 过程控制系统(如在化学、石油或其它过程中使用的那些过程控制系统)通常包括一个或多个系统控制器，这些系统控制器经由模拟、数字或组合的模拟/数字总线通信地耦合到至少一个主机或操作者工作站并通信地耦合到一个或多个自动化设备。自动化设备(其可以是例如阀、阀定位器、开关以及传送器(例如，温度传感器、压力传感器和流速传感器))在过程控制系统内执行诸如开启或关闭阀以及测量过程参数之类的功能。过程控制器接收指示由自动化设备进行的过程测量的信号和/或与自动化设备有关的其它信息，使用该信息来实现控制例程，并且然后生成控制信号，该控制信号通过总线或其它通信线路发送给自动化设备以控制过程控制系统的操作。

附图说明

[0003] 图1示出了示例性过程控制系统。

[0004] 图2示出了具有用于自动化设备的定制应用环境的示例性设备控制器。

[0005] 图3示出了图2的示例性应用管理器的实现方式。

[0006] 图4是表示可被执行以实现图2和图3的应用管理器的示例性方法的流程图。

[0007] 图5是表示可被执行以实现图2和图3的应用管理器的另一个示例性方法的流程图。

[0008] 图6是示例性处理器系统的框图，其中示例性处理器系统被构造为执行机器可读指令以执行由图4和/或图5所表示的方法，从而实现图2和图3的示例性应用管理器。

发明内容

[0009] 示例性公开的方法包括：将设备控制器通信地耦合到主机。示例性主机用于提供过程控制系统内的所述设备控制器和自动化设备。示例性公开的方法还包括：将过程控制应用安装到所述设备控制器的固件中的应用空间中。示例性过程控制应用由所述主机提供权限数据。示例性公开的方法还包括：执行所述应用空间中的所述过程控制应用。示例性过程控制应用扩展所述设备控制器的功能。示例性公开的方法还包括：缓和所述过程控制应用对所述设备控制器的物理资源的访问。示例性权限数据限定所述过程控制应用具有所述物理资源中的哪些物理资源的访问。

[0010] 一种示例性公开的设备控制器，所述设备控制器与安装在过程控制系统中的自动化设备相关联，所述设备控制器包括：设备控制器管理器，所述设备控制器管理器用于将所述设备控制器通信地耦合到主机。示例性主机提供所述过程控制系统内的所述设备控制器和所述自动化设备。示例性设备控制器还包括安装器(installer)，所述安装器用于将过程

控制应用安装到所述设备控制器的固件中的应用空间中。示例性过程控制应用由所述主机提供权限数据。示例性设备控制器还包括应用框架处理器(handler),所述应用框架处理器用于执行所述应用空间中的所述过程控制应用,所述过程控制应用用于扩展所述设备控制器的功能,以及缓和所述过程控制应用对所述设备控制器的物理资源的访问,所述权限数据定义用于缓和所述过程控制应用对所述设备控制器的所述物理资源的所述访问的规则。

[0011] 一种示例性制品,所述制品包括当被执行时使得设备控制器将所述设备控制器通信地耦合到主机的指令。示例性主机提供所述过程控制系统内的所述设备控制器和所述自动化设备。示例性制品还包括当被执行时使得设备控制器将过程控制应用安装到所述设备控制器的固件中的应用空间中的指令。示例性过程控制应用由所述主机提供权限数据。示例性制品还包括当被执行时使得设备控制器执行所述应用空间中的所述过程控制应用的指令。示例性过程控制应用扩展示例性设备控制器的功能。示例性制品还包括当被执行时使得设备控制器缓和所述过程控制应用对所述设备控制器的物理资源的访问的指令。示例性权限数据定义用于缓和示例性过程控制应用对示例性设备控制器的所述物理资源的所述访问的规则。

具体实施方式

[0012] 概括地说,本公开内容涉及过程控制系统中的自动化设备,更具体而言,涉及用于提供过程控制设备(例如,设备控制器)中的定制应用环境的方法、设备和制品。过程控制系统包括工作站和/或服务器,这些工作站和/或服务器与位于过程控制系统中的系统控制器、设备控制器和/或自动化设备进行交互。在本文所公开的示例中,除了由设备控制器的固件所执行的主要过程控制功能以外,设备控制器还执行过程控制应用。自动化设备可以是例如阀、阀定位器、开关和传送器,并且可以执行过程控制功能,例如开启或关闭阀以及测量过程控制参数。除了管理自动化设备以外,设备控制器还可以基于从自动化设备接收的信息来生成过程数据(例如,过程控制信息)。过程数据可以包括过程统计、警报、监视信息、过程趋势信息、诊断信息、自动化设备状态信息和/或来自自动化设备的消息。在一些示例中,设备控制器可以被集成到自动化设备中。替代地或另外,在一些示例中,设备控制器可以有线或无线地连接到自动化设备。

[0013] 设备控制器执行固件,以例如与主机(例如,工作站、服务器等)进行通信,与自动化设备进行通信和/或生成过程数据。通常,为了更新设备控制器的功能,使该设备控制器离线并对其固件进行更新。替代地,固件的镜像版本在后台进行更新并且切换到固件的活动版本。此外,为了提供定制功能,对固件或固件的模块进行改变和重新编译。这种方法限制了设备控制器的灵活性,并会需要大量的时间和资源。

[0014] 在本文所公开的示例中,设备控制器的固件包括应用空间。应用空间允许对过程控制器的功能进行扩展和/或更新而无需更新固件且无需中断过程控制器的操作。在下面所示的示例中,可以在应用空间中下载和执行过程控制应用而不改变固件或重置自动化设备。为了提供安全性和稳定性,应用空间与固件的其余部分隔离。

[0015] 应用管理器通过隔离存储器(例如,只读存储器(ROM)、随机存取存储器(RAM)、硬盘、固态存储器等)的一部分来限定应用空间,在存储器的该部分中可以存储应用空间中执行的过程控制应用,并且可以从存储器的该部分读取过程控制应用和/或可以向存储器的

该部分写入过程控制应用。此外，过程控制应用不能够读取和/或写入存储器中的未被定义用于应用空间的其它区域。在本文所公开的示例中，应用管理器缓和对设备控制器的物理资源(例如，网络通信，自动化设备通信，传感器，致动器等)的访问。在一些示例中，应用管理器通过控制对固件的功能的可访问性(例如，只读访问、读取-写入访问、向主机发送和/或接收的消息的能力等)来缓和过程控制应用。例如，应用管理器可以允许过程控制应用读取由自动化设备发送的消息和/或数据，但会阻止过程控制应用将消息(例如，命令信号)发送给自动化设备。应用管理器还可以控制访问物理资源的频率。例如，应用管理器可以限制过程控制应用可以将消息发送给主机的频率(例如，以阻止偶然的或恶意的拒绝服务式(denial-of-service)攻击等)。

[0016] 在本文所公开的示例中，过程控制应用与权限数据相关联。权限数据限定了过程控制应用对设备控制器的物理资源的访问。例如，权限数据可以指定过程控制应用可将消息发送给主机，但不发送给自动化设备。在这些示例中，如果过程控制应用包括用于将消息发送给自动化设备的指令，则应用管理器不向过程控制应用提供相对应的功能。在一些示例中，制造商可以针对为不同的客户制造的设备控制器(例如，在硬件中、在固件中等)设定不同的权限策略。例如，为了安全的目的，客户可以决定在某些过程控制系统中的设备控制器上执行的过程控制应用不将消息发送给自动化设备。

[0017] 利用过程控制应用将示例性的权限数据传送给设备控制器。在一些示例中，如果过程控制应用已安装但不与权限数据相关联，则应用管理器不执行过程控制应用。在一些示例中，在创建过程控制应用时创建权限数据。在这些示例中，当经由主机安装过程控制应用时，提示用户确认(例如，接受)权限数据。在一些示例中，与过程控制应用分离地生成权限数据。例如，可以在应用安装到设备控制器上时生成权限数据。在一些此类示例中，在安装过程控制应用时，提示用户为过程控制应用选择权限。

[0018] 在一些示例中，为了阻止恶意应用获得对过程控制器固件的功能的访问，权限数据可以存储在与相对应的过程控制应用分离的权限数据储存库中并在安装相对应的过程控制应用时取回。在一些此类示例中，基于过程控制应用来预先计算认证值。例如，可以使用过程控制应用来计算散列值。在这些示例中，当要经由主机来安装过程控制应用时，基于过程控制应用来计算新的认证值。在这些示例中，如果新计算的认证值和预先计算的认证值匹配，则权限文件被取回并传送给过程控制器。在这些示例中，该匹配表示，自创建权限数据以后过程控制应用未被改变。替代地或另外地，在一些示例中，权限数据包含数字签名。在这些示例中，除非验证数字签名(例如，经由相对应的公钥)，否则主机和/或设备控制器不安装权限数据。

[0019] 应用管理器还包括应用框架处理器，应用框架处理器提供应用空间与固件之间的接口。在一些示例中，过程控制应用可以是经编译的指令集。在这些示例中，应用框架处理器向应用空间中的过程控制应用提供了对包含在固件内的函数库(例如，网络通信函数，自动化设备通信函数等)的访问。在一些示例中，过程控制应用可以是脚本。在这些示例中，应用框架解释脚本并提供对包含在固件内的函数(例如，脚本挂钩)的访问。在这些示例中，过程控制应用向应用管理器请求(例如，经由库函数调用、经由挂钩等)访问过程控制器的物理资源，并且应用管理器基于与过程控制应用相关联的权限数据来许可或拒绝该请求。如果应用管理器许可该请求，则应用管理器允许对固件的库函数调用。例如，如果过程控制应

用请求读取阀致动器上的位置传感器的位置值，则应用管理器将取回该值(例如，向固件请求该值)，并将其传递给过程控制应用。

[0020] 图1示出了示例性过程控制系统100，该示例性过程控制系统100可以结合本文所描述的设备控制器中的定制应用环境来使用。示例性过程控制系统100采用集成了一个或多个智能工厂能力(包括现场总线102(如HART®和/或FOUNDATION™现场总线)、高速离散总线、嵌入式高级控制、以及高级单元和批量管理)的工厂过程控制架构。过程控制系统100内的现场总线102网络自动化设备104、106和/或设备控制器108提供用于各种应用(包括装置管理、配置、监视和诊断等)的基础设施。

[0021] 在示出的示例中，过程控制系统100包括示例性自动化设备104、106、示例性设备控制器108a、108b、示例性系统控制器110、示例性I/O装置112a、112b以及示例性主机114。示例性I/O设备112a、112b促进示例性系统控制器110与示例性自动化设备106和/或示例性设备控制器108a之间的通信。示例性I/O装置112a、112b支持各个模块，以便与各个自动化设备106和/或示例性设备控制器108a进行通信(例如，经由数字和/或模拟通信)。例如，I/O设备112b可以具有模拟模块，以便与自动化设备106(例如，三线式温度探针等)对接，以及数字模块，以便与设备控制器108a对接。示例性I/O装置112a、112b从示例性自动化设备106和/或示例性设备控制器108a接收数据，并将该数据转换成能够由示例性系统控制器110处理的通信。另外，示例性I/O装置112a、112b将来自示例性系统控制器110的数据和/或通信转换为能够由示例性自动化设备106和/或示例性设备控制器108a处理的格式。在一些示例中，I/O装置112a、112b和设备控制器108组合成一个单元。

[0022] 示例性自动化设备104、106可以例如包括控制和监视过程控制系统100中的流体(例如，流体、气体、半流体等)的一个或多个仪表。自动化设备104、106可以例如包括阀、致动器、传感器、探针、邻近开关、电机起动器、驱动器等。示例性设备控制器108a、108b控制和/或监视示例性自动化设备104、106。在示出的示例中，设备控制器108a、108b从示例性自动化设备104、106读取(例如，来自传感器的数据等)和/或产生至示例性自动化设备104、106的控制信号(例如，以控制阀的位置，以控制电机的速度等)。例如，设备控制器108a、108b可接收来自位置传感器和/或其它传感器的数据，并且可以传送控制信号以控制阀和/或其它装置。

[0023] 示例性自动化设备104通信地耦合到设备控制器108a。在一些此类示例中，设备控制器108a可集成到自动化设备104中。例如，用于控制阀上的致动器的硬件可以与设备控制器108a在相同的外壳中。替代地，设备控制器108a可与自动化设备104分离。在一些示例中，设备控制器108b可与I/O设备112b集成在一起。

[0024] 在示出的示例中，设备控制器108a、108b执行固件，以对从示例性自动化设备104、106和/或系统控制器110接收到的数据进行处理。示例性固件的范围可从提供基本功能(例如，报告数据，对自动化设备104、106的控制等)的固件到提供高级功能(例如，计算处理数据，生成警告数据等)的固件。固件包括应用空间，在该应用空间中执行例如从主机114下载的过程控制应用。过程控制应用通过例如执行不包括在固件中的功能来扩展设备控制器108a、108b的固件的功能。例如，过程控制应用可以计算过程数据，控制自动化设备104、106，生成警告等。在一些示例中，固件可以执行应用空间中的多个过程控制应用和/或提供多个应用空间。在一些示例中，设备控制器108a、108b的固件可具有基本功能(例如，读取/

报告传感器数据，生成控制信号等)，并且应用空间中的过程控制应用可以用于定制设备控制器108a、108b的功能。以此方式，降低了对固件更新的需求并且增大了定制设备控制器108a、108b的功能的能力。

[0025] 示例性系统控制器110经由有线或无线网络(例如，LAN、WAN、互联网等等)耦合到示例性主机114。示例性系统控制器110控制例程，以便基于来自自动化设备104、106和/或设备控制器108a、108b的输出来计算过程数据以用于过程控制应用，包括例如监视应用、报警管理应用、过程趋势和/或历史应用、诊断应用、批处理和/或广告管理应用、统计应用、流式传输视频应用、高级控制应用、安全仪表应用、事件应用等。系统控制器110以周期性间隔和/或在处理或生成过程数据时将过程数据转发给主机114。由系统控制器110发送的过程数据可以包括过程控制值、数据值、报警信息、文本、块模式元素状态信息、诊断信息、误差消息、参数，事件和/或设备标识符。

[0026] 在图1中所示的示例中，主机114可包括一个或多个工作站116和/或服务器118，以执行系统控制应用。系统控制应用与示例性控制器110进行通信，以监视、控制和/或诊断过程控制系统100中的示例性设备控制器108a、108b和/或示例性自动化设备104、106。例如，过程控制应用可以包括控制自动化、过程控制系统100的图形表示、变更管理、过程控制编辑、数据采集、数据分析等。在一些示例中，工作站116经由用户界面显示系统控制应用，以便以图形格式呈现过程数据，以使得工作站116的用户能够以图形方式查看(经由应用)由示例性设备控制器108a、108b和/或示例性自动化设备104、106生成的过程数据。在一些示例中，当过程控制应用在服务器118上执行时，操作者可以建立从工作站(例如，工作站116)到服务器118的远程连接，以访问过程控制应用。

[0027] 示例性主机114包括示例性应用数据库120。示例性应用数据库120存储可以安装在过程控制系统100中的一个或多个设备控制器108a、108b的固件的应用空间中的过程控制应用。在一些示例中，工作站116可用于管理设备控制器108a、108b中的过程控制应用的安装和卸载。为了安装过程控制应用，工作站116经由系统控制器110和I/O设备112a、112b将过程控制应用从应用数据库120(例如，经由块传输)发送给设备控制器108a、108b。

[0028] 在图1的示出的示例中，示例性主机114包括示例性权限数据库122。权限数据限定了过程控制应用对设备控制器108a、108b的物理资源的访问和/或对过程控制应用何时能够访问设备控制器108a、108b的物理资源进行调节的逻辑条件。例如，权限数据可以指定过程控制应用可将消息发送给主机114，但不能将控制信号发送给自动化设备104、106。举另一个例子，当从主机114接收到许可该访问的消息时，权限数据可以指定过程控制应用可以与自动化设备104、106进行通信。当过程控制应用被发送给设备控制器108a、108b时，权限数据被发送给设备控制器108a，108b。在一些示例中，如果过程控制应用安装在设备控制器108a、108b上但不与权限数据相关联，则设备控制器108a、108b的固件将不执行过程控制应用。

[0029] 在一些示例中，在创建过程控制应用时创建权限数据。在一些示例中，在将过程控制应用经由主机114发送给设备控制器108a、108b之前，提示用户接受权限数据。例如，工作站116可显示与过程控制应用相关联的权限数据，并且可以提供按钮以供用户按下以指示接受权限数据。在一些示例中，如果用户不接受权限数据，则主机114不会将过程控制应用发送给设备控制器108a、108b。在一些示例中，经由主机114与过程控制应用分离地生成权

限数据。例如，在将过程控制应用发送给设备控制器108a、108b时，可以提示用户选择权限数据。例如，工作站116可显示可以包括在权限数据中的可能权限（例如，从自动化设备104、106读取，向自动化设备104、106写入等等），并允许用户选择要在权限数据中包括哪些权限。

[0030] 在一些示例中，当制造设备控制器108a、108b时，设备控制器108a、108b的制造商使设备控制器108a、108b具有权限数据。在一些此类示例中，制造商所设定的权限数据由在设备控制器108a、108b上执行的过程控制应用所使用。例如，可以包括用于设备控制器108a、108b的权限数据，其阻止安装在设备控制器108a、108b上的过程控制应用从相对应的自动化设备104、106读取和/或向相对应的自动化设备104、106写入。在这些示例中，过程控制应用不能够访问相对应的自动化设备104，而不管与特定的过程控制应用相关联的权限数据所设置的权限如何。

[0031] 在一些示例中，为了阻止恶意的过程控制应用获得对固件的功能的访问，当将过程控制应用发送给设备控制器108a、108b时，单独地发送存储在权限数据库122中的权限数据。在一些示例中，预先计算预期的认证值（例如，散列值等）并存储在权限数据库122中。例如，在写入过程控制应用之后，可以对过程控制应用使用散列函数，以产生预期的认证值。在这些示例中，当要经由主机114安装过程控制应用时，基于过程控制应用来计算新的认证值。在这些示例中，如果新计算的认证值和预期的认证值匹配，则权限数据被取回并传送给过程控制器108a、108b。替代地或另外地，在一些示例中，存储在权限数据库122中的权限数据包括根据数字签名标准（DSS）使用私钥生成的数字签名。在这些示例中，当从主机114接收到权限数据时，设备控制器108a、108b使用与私钥相对应的公钥来验证数字签名。在这些示例中，如果数字签名经验证，则设备控制器108a、108b安装权限数据。否则，在这些示例中，如果数字签名未经验证，则设备控制器108a、108b丢弃权限数据。

[0032] 图2示出了具有固件202的设备控制器108的示例性实现方式，其中固件202包括用于执行过程控制应用206的示例性定制应用空间204。在示出的示例中，设备控制器108包括示例性固件202和示例性物理资源208。在示出的示例中，物理资源208包括示例性处理器210、示例性存储器212、示例性非易失性储存设备214（例如，闪存，硬盘等）、示例性传感器216、示例性总线I/O 218、以及示例性自动化设备I/O 220。示例性固件202包括示例性应用空间204、示例性应用管理器222、以及示例性设备控制器管理器224。

[0033] 示例性设备控制器管理器224包含使用物理资源208的功能。例如，设备控制器管理器224可以经由总线102（图1）发送和接收至主机114（图1）的消息。在一些示例中，设备控制器管理器224还可以包含管理自动化设备104、106（图1）的功能。例如，设备控制器管理器224可以从自动化设备104、106的传感器（例如，压力传感器，位置传感器等）读取，计算误差，并将控制信号发送给自动化设备104、106，以保持期望的设定点。在示出的示例中，设备控制器管理器224还管理示例性处理器210与应用管理器222的共享，以允许设备控制器管理器224运行过程控制功能以及允许应用管理器222执行过程控制应用206。

[0034] 在图2中所示的示例中，应用管理器222管理在示例性应用空间204中执行的示例性过程控制应用206。为了将应用空间204与设备控制器管理器224隔离，示例性应用管理器222在应用空间204与设备控制器管理器224之间划分示例性存储器212和/或示例性储存器214。保持该隔离，以阻止过程控制应用206偶然地或恶意地覆写设备控制器管理器224所使

用的存储器值。示例性过程控制应用206存储在示例性存储器212和/或示例性储存设备214中的被指定用于应用空间204的部分中。另外，示例性过程控制应用206仅可以从示例性存储器212和/或示例性储存器214中的被指定用于应用空间204的部分读取和向该部分写入。当过程控制应用206请求向存储器212和/或储存设备214写入时，示例应用管理器222管理该请求，并向示例性存储器212和/或示例性储存设备214的所指定的部分写入。当过程控制应用206请求从存储器212和/或储存设备214读取时，示例性应用管理器222管理该请求，并从示例性存储器212和/或示例性储存设备214的所指定的部分读取。

[0035] 在示出的示例中，应用管理器222提供应用框架处理器，以缓和过程控制应用206对设备控制器108的物理资源208的访问。过程控制应用206可以是经编译的指令集或脚本。当过程控制应用206是编译的指令集时，应用管理器222向过程控制应用206提供对函数库的访问，以访问设备控制器108的物理资源208。当过程控制应用206是脚本时，应用管理器222解释脚本，并提供对函数的访问(访问设备控制器108的物理资源208)。示例性过程控制应用206向应用管理器222请求(例如，经由库调用，经由挂钩等)访问设备控制器108的物理资源208。

[0036] 在一些示例中，应用管理器222和设备控制器管理器224限定了存储器212和/或储存设备214中的数据空间225。在这些示例中，数据空间225是过程控制应用206和过程控制器管理器224的过程可以读取和写入的空间。以此方式，示例性过程控制应用206能够计算可以由设备控制器管理器224的过程所使用的过程数据。例如，过程控制应用206可以计算控制值，以用于对装置控制管理器224将要使用的阀进行控制。在一些此类示例中，可以由应用管理器222通过权限数据来缓和对数据空间225的访问。在一些示例中，为了阻止读取/写入冲突，对数据空间225的访问是由信号量(semaphore)来控制的。在一些此类示例中，信号量阻止过程控制应用206在设备控制管理器224正在向数据空间225写入时从数据空间225读取和/或阻止设备控制管理器224在过程控制应用206正在向数据空间225写入时从数据空间225读取。

[0037] 示例性应用管理器222基于与做出请求的过程控制应用206相关联的权限数据来许可或拒绝对访问物理资源208的请求。在示出的示例中，为了阻止过程控制应用206改变权限数据，将权限数据存储在存储器212和/或储存器214的中的与应用空间204隔离的部分中。例如，如果过程控制应用206将向主机114发送消息，则应用管理器222检查与过程控制应用206相关联的权限数据，以确定过程控制应用206是否具有访问总线的I/0218的权限。如果应用管理器222许可该请求，则应用管理器222利用过程控制应用206所指定的参数(例如，消息、控制信号的值等)来进行相对应的函数调用。例如，如果过程控制应用206确实有权限将消息发送给主机114，则应用管理器222进行适当的函数调用。举另一个例子，如果过程控制应用206请求读取自动化设备104、106的阀上的位置传感器的值，则应用管理器222取回值(例如，向固件请求该值)，并将该值传递给过程控制应用206。

[0038] 图3示出了图2中的用于对在应用空间204(图2)中执行的过程控制应用206(图2)进行管理的示例性应用管理器222的实现方式。示例性应用管理器222包括示例性权限管理器300、示例性安装器302、以及示例性应用框架处理器304。在示出的示例中，当过程控制应用206请求访问(例如，经由库函数调用、经由挂钩等)时，权限管理器300确定在应用空间204中执行的进程控制应用206是否有权限访问特定的物理资源208(图2)。为了做出该确

定，示例性权限管理器300从存储器212(图2)和/或储存设备214(图2)中取回权限数据。

[0039] 当过程控制应用206请求访问时，示例性权限管理器300将所请求的访问与权限数据进行比较。例如，如果过程控制应用206进行函数调用以经由自动化设备I/O 220(图2)将控制信号发送给自动化设备104、106，则权限管理器300确定相关联的权限数据是否指示过程控制应用206能够访问自动化设备I/O 220。如果权限数据指示过程控制应用206具有权限访问所请求的物理资源208，则示例性权限管理器300允许相对应的函数调用继续进行。

[0040] 在一些示例中，权限管理器300控制过程控制应用206能够访问特定的物理资源208的频率。例如，权限管理器300可以允许过程控制应用206仅每秒一次地将消息发送给主机114(图1)，以阻止过程控制应用206偶然地或恶意地执行对系统控制器110(图1)和/或主机114的拒绝服务式攻击。

[0041] 示例性安装器302管理过程控制应用206的安装和卸载。示例性安装器302经由总线I/O 218(图2)从主机114接收示例性过程控制应用206和相对应的权限数据。示例性安装器302将过程控制应用206复制到存储器212和/或储存设备214中的被提供用于应用空间204的部分。在一些示例中，安装器302将权限数据复制到存储器212和/或储存器214中的被提供用于权限数据的部分。示例性安装器302然后向应用框架处理器304通知有关安装的过程控制应用206的开始位置，并向权限管理器300通知有关权限数据的位置。

[0042] 在图3的示出的示例中，应用框架处理器304控制所安装的过程控制应用206的执行。在一些示例中，应用框架处理器304基本上连续地执行所安装的过程控制应用206。另外地或替代地，在一些示例中，应用框架处理器304响应于事件和/或触发而多次执行过程控制应用206。例如，当阀关闭时或当检测到故障状况时，应用框架处理器304可以执行过程控制应用206。应用框架处理器304为过程控制应用206调度对处理器(例如，图2的处理器210)的访问。在一些示例中，应用框架处理器304解释过程控制应用206(例如，当过程控制应用206是脚本时)。此外，应用框架处理器304提供了允许过程控制应用206访问设备控制器108的物理资源208的库和/或挂钩。例如，如果过程控制应用206要将控制信号发送给自动化设备104、106，则过程控制应用206包括对包括在应用框架处理器304中的自动化设备I/O函数的调用。应用框架处理器304结合权限管理器300要么允许函数调用继续进行(例如，过程控制应用206与相对应的权限相关联)要么忽略函数调用(例如，过程控制应用206不与相对应的权限相关联)。以此方式，应用管理器222缓和对物理资源208的访问。

[0043] 尽管在图3中示出了实现图2的示例性应用管理器222的示例性方式，但图3中示出的元件、过程和/或设备中的一个或多个可以被组合、划分、重新布置、省略、取消和/或以任何其它方式来实现。此外，示例性权限管理器300、示例性安装器302、示例性应用框架处理器304和/或更一般的图2的示例性应用管理器222可以由硬件、软件、固件和/或硬件、软件、固件的任何组合来实现。因此，例如示例性权限管理器300、示例性安装器302、示例性应用框架处理器304和/或更一般的示例性应用管理器222中的任何一个可以由一个或多个模拟或数字电路、逻辑电路、可编程处理器、专用集成电路(ASIC)、可编程逻辑器件(PLD)和/或现场可编程逻辑器件(FPLD)来实现。当阅读本专利中的用以涵盖纯软件和/或固件实现方式的装置或系统权利要求中的任何一个时，示例性权限管理器300、示例性安装器302和/或示例性应用框架处理器304中的至少一个故此被明确地定义为包括存储软件和/或固件的有形计算机可读储存设备或储存盘，例如存储器、数字多功能盘(DVD)、压缩盘(CD)、蓝光盘

等。此外，除了图3中示出的那些元件、过程和/或设备之外或者作为其替代，图2的示例性应用管理器222可以包括一个或多个元件、过程和/或设备，和/或可以包括所示出的元件、过程和设备中的任意或全部元件、过程和设备中的一个以上。

[0044] 在图4和/或图5中示出了表示用于实现图2和图3的示例性应用管理器222的示例性方法的流程图。在这些示例中，可以使用由处理器(例如，以下结合图6所讨论的示例性处理器平台600中示出的处理器210)执行的程序来实现所述方法。程序可以包含在存储在有形计算机可读储存介质(例如，CD-ROM、软盘、硬盘驱动器、数字多功能盘(DVD)、蓝光盘、或者与处理器210相关联的存储器)上的软件中，但是整个程序和/或其部分可以替代地由除了处理器210之外的设备来执行和/或包含在固件或专用硬件中。此外，尽管参照在图4和/或图5中示出的流程图描述了示例性程序，但可以替代地使用实现示例性应用管理器222的许多其它方法。例如，可以改变框的执行顺序，和/或可以改变、取消或组合所描述的框中的一些框。

[0045] 如上面所提到的，图4和/或图5的示例性方法可以使用存储在有形计算机可读储存介质(例如硬盘驱动器、闪存、只读存储器(ROM)、压缩盘(CD)、数字多功能盘(DVD)、高速缓存、随机存取存储器(RAM)和/或信息在其中存储任何持续时间(例如，扩展的时间段、永久地、短暂地、临时缓冲、和/或对信息的高速缓存)的任何其它储存设备或储存盘)上的经编码的指令(例如，计算机和/或机器可读指令)来实现。如本文所使用的，术语有形计算机可读储存介质被明确地定义为包括任何类型的计算机可读储存设备和/或储存盘，并且不包括传播信号以及不包括传输介质。如本文所使用的，“有形计算机可读储存介质”和“有形机器可读储存介质”可互换使用。另外地或替代地，图4和/或图5的示例性方法可以使用存储在非暂时性计算机和/或机器可读介质(例如，硬盘驱动器、闪存、只读存储器、压缩盘、数字多功能盘、高速缓存、随机存取存储器和/或信息在其中存储任何持续时间(例如，扩展的时间段、永久地、短暂地、临时缓冲、和/或对信息的高速缓存)的任何其它储存设备或储存盘)上的经编码的指令(例如，计算机和/或机器可读指令)来实现。如本文所使用的，术语非暂时性计算机可读储存介质被明确地定义为包括任何类型的计算机可读储存设备和/或储存盘，并且不包括传播信号以及不包括传输介质。如本文所使用的，当短语“至少”用作权利要求的前序中的过渡术语时，其是开放式的，与术语“包括”是开放式的方式相同。

[0046] 图4是表示可以被执行以实现图2和图3的应用管理器222以执行设备控制器108(图1和图2)上的示例性过程控制应用206(图2)的示例性方法400的流程图。设备控制器管理器224与系统控制器110(图1)和/或主机114(图1)进行通信，以在过程控制系统100(图1)中提供设备控制器108(框402)。在一些示例中，为了提供设备控制器108，设备控制器管理器224提供设备控制器108和/或相对应的自动化设备104、106(图1)的配置信息(例如，设备描述文件、设备控制器标识符、自动化设备标识符、通用设备信息、范围设置信息、传感器/致动器参数和/或容差等)。

[0047] 应用管理器222将从主机114接收到的过程控制应用206安装到设备控制器108的应用空间204中(框404)。例如，应用管理器222可以将过程控制应用206置于存储器202和/或储存设备214中的被指定用于应用空间204的部分中。权限管理器300将从主机114接收到的与过程控制应用206相关联的权限数据安装到存储器212和/或储存设备214中的被指定用于权限数据的部分(例如，权限存储器)中(框406)。应用管理器222然后管理过程控制应

用206的执行(框408)。在一些示例中,应用管理器222解释过程控制应用206。

[0048] 应用管理器222还缓和过程控制应用206对设备控制器108的物理资源208的访问(框410)。例如,如果过程控制应用206请求访问(例如,经由库函数调用、经由脚本挂钩等),则应用管理器222使用与过程控制应用206相关联的权限数据来确定过程控制应用206是否可以访问特定的物理资源208。另外,为了缓和访问,应用管理器222阻止过程控制应用206向未被定义用于应用空间204的存储器212和/或储存设备214进行读取或写入。

[0049] 图5是表示可以被执行以实现图2和图3的应用管理器222以缓和示例性过程控制应用206(图2)对设备控制器108(图1和图2)的物理资源208(图2)的访问的示例性方法500的流程图。应用框架处理器304(图3)管理过程控制应用206的执行(框502)。例如,应用框架处理器304解释过程控制应用206和/或将存储器212(图2)中的开始位置加载到处理器210(图2)的程序计数器中。应用框架处理器304确定过程控制应用206是否请求对物理资源208的访问(例如,经由库函数调用、经由脚本挂钩等)(框504)。

[0050] 如果过程控制应用206请求对物理资源208的访问,则权限管理器300(图3)确定过程控制应用206是否具有权限访问特定的物理资源208(框506)。为了做出该确定,权限管理器300检查与特定的过程控制应用206相关联的权限数据。如果过程控制应用206的确具有权限访问特定的物理资源208,则应用框架处理器304将该请求(例如,经由库函数等)传递至特定的物理资源208(框508)。如果过程控制应用206不具有权限访问特定的物理资源208,则应用框架处理器304忽略该请求(框510)。在一些示例中,应用框架处理器304设定标志和/或向主机114发送消息以指示过程控制应用206尝试访问其没有权限访问的物理资源208。

[0051] 应用框架处理器304确定是否继续执行过程控制应用206(框512)。如果应用框架处理器304要继续执行过程控制应用206,则过程500返回至框502。否则,过程500结束。

[0052] 图6是被构造为执行图4和图5的方法以实现图1和图2的示例性设备控制器108和/或图2和图3的示例性应用管理器222的示例性处理器平台600的框图。处理器平台600包括设备控制器108的在图2中的物理资源208。

[0053] 所示出的示例中的处理器平台600包括处理器210。所示出的示例中的处理器210是硬件。例如,处理器210可以由来自任何期望的家族或制造商的一个或多个集成电路、逻辑电路、微处理器或控制器来实现。

[0054] 所示出的示例中的处理器210包括本地存储器602(例如,高速缓存)。所示出的示例中的处理器210经由总线604与包括易失性存储器212a和非易失性存储器212b的主存储器进行通信。易失性存储器212a可以由同步动态随机存取存储器(SDRAM)、动态随机存取存储器(DRAM)、RAMBUS动态随机存取存储器(RDRAM)和/或任何其它类型的随机存取存储器设备来实现。非易失性存储器212b可以由闪存和/或任何其它期望类型的存储器设备来实现。对主存储器212a、212b的访问由存储器控制器来控制。可以为易失性存储器212a和/或大容量储存设备214的区段限定应用空间204。

[0055] 所示出的示例的处理器平台600还包括总线I/O 218和自动化设备220。总线I/O 218和自动化设备I/O 220可以由任何类型的接口标准(例如,Foundation Fieldbus、Profibus、Hart总线、以太网接口、通用串行总线(USB)、和/或PCI高速接口)来实现。

[0056] 在一些示例中,处理器平台600包括接口电路606,接口电路606可以包括通信设

备，例如发射机、接收机、收发机、调制解调器和/或网络接口卡，以促进经由网络608(例如，以太网连接、数字用户线(DSL)、电话线、同轴电缆、蜂窝电话系统等)与外部机器(例如，任何类型的计算设备)的数据交换。

[0057] 所示出的示例中的处理器平台600还包括用于存储软件和/或数据的一个或多个大容量储存设备214。这种大容量储存设备214的示例包括软盘驱动器、硬盘驱动器、或者任何其它适合的储存介质。

[0058] 用于实现图4和图5的方法的经编码的指令610可以存储在储存设备214中、易失性存储器212a中、非易失性存储器212b中、和/或诸如CD或DVD之类的可移动有形计算机可读储存介质上。

[0059] 在一些示例中，处理器平台600包括可以与自动化设备104、106的传感器分离的传感器216(例如，温度传感器、湿度传感器、加速计等)。在一些此类示例中，传感器216可以用于监视设备控制器108周围的状况和/或检测异常行为(例如，故障检测、盗窃检测等)。

[0060] 尽管本文已经公开了某些示例性方法、装置和制品，但是本专利的涵盖范围不限于此。相反，本专利涵盖完全落入本专利的权利要求的范围内的所有方法、装置和制品。

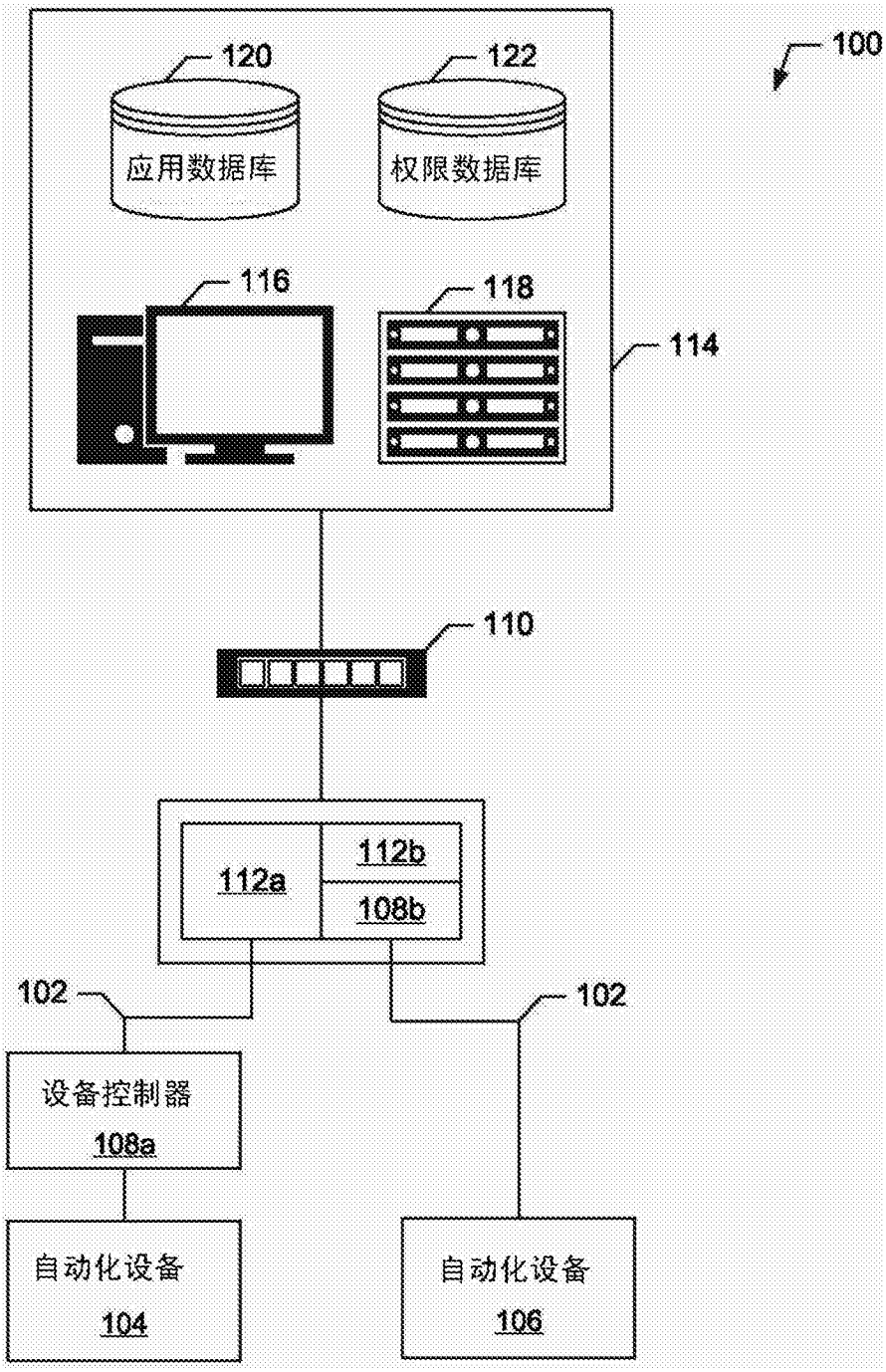

100
120
应用数据库
122
权限数据库
116
118
114
110
112a
112b
108b
102
102
设备控制器
108a
自动化设备
104
自动化设备
106

图1

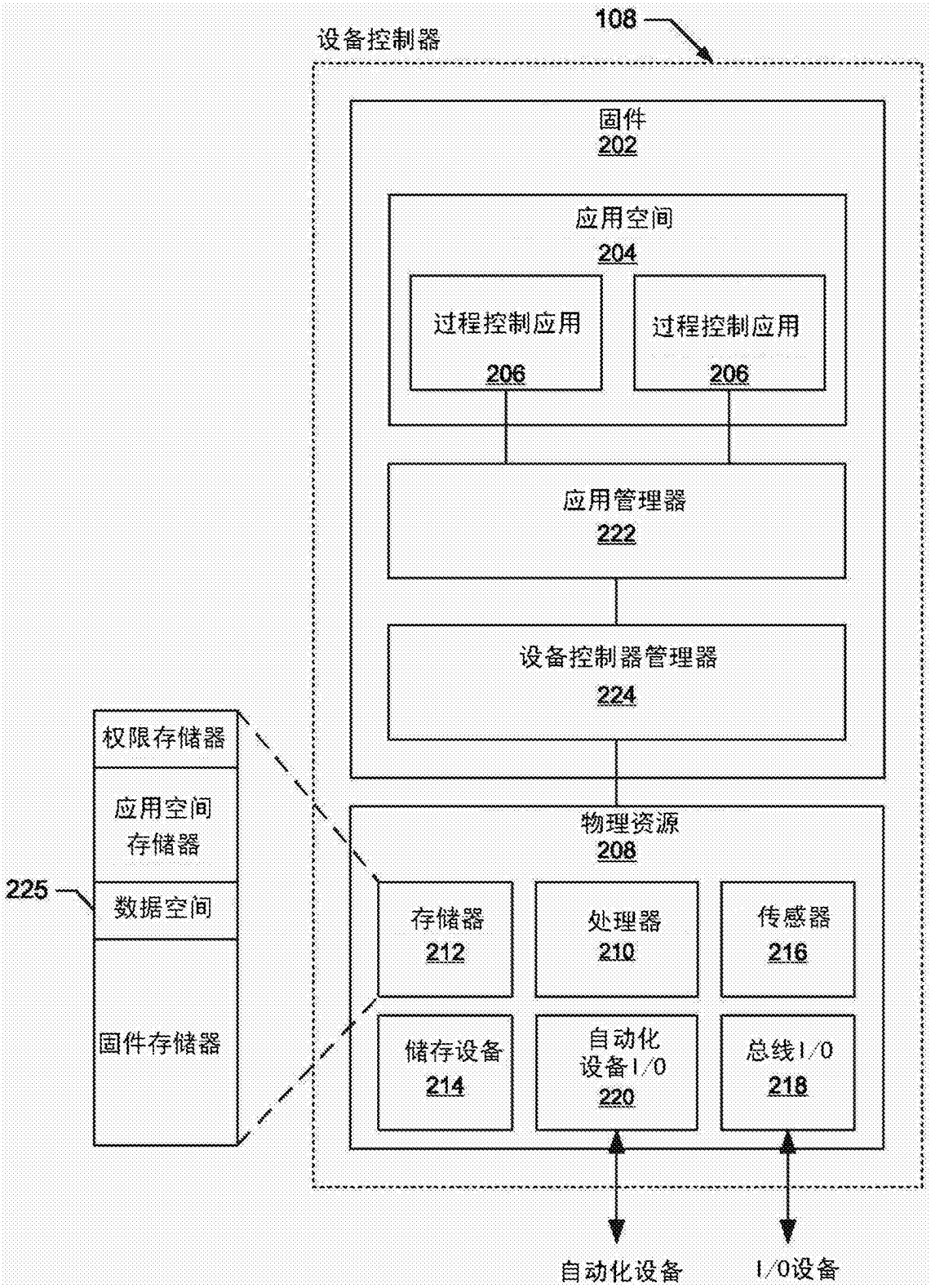

108
设备控制器
固件
202
应用空间
204
过程控制应用
206
过程控制应用
206
应用管理器
222
设备控制器管理器
224
物理资源
208
存储器
212
处理器
210
传感器
216
储存设备
214
自动化
设备I/O
220
总线I/O
218
权限存储器
应用空间
存储器
数据空间
固件存储器
225
自动化设备
I/O设备

图2

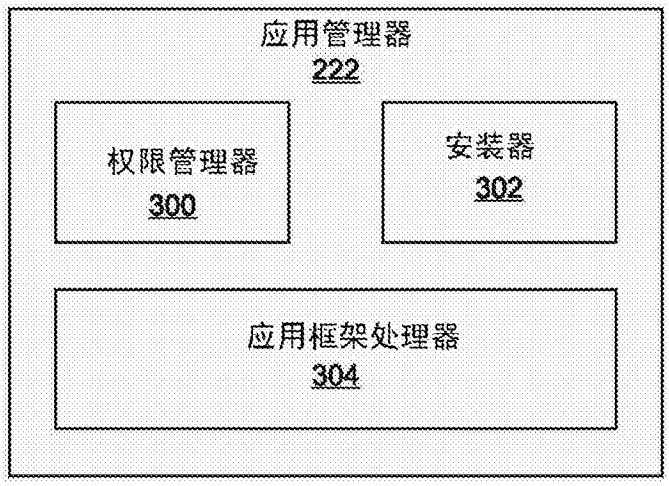


图3

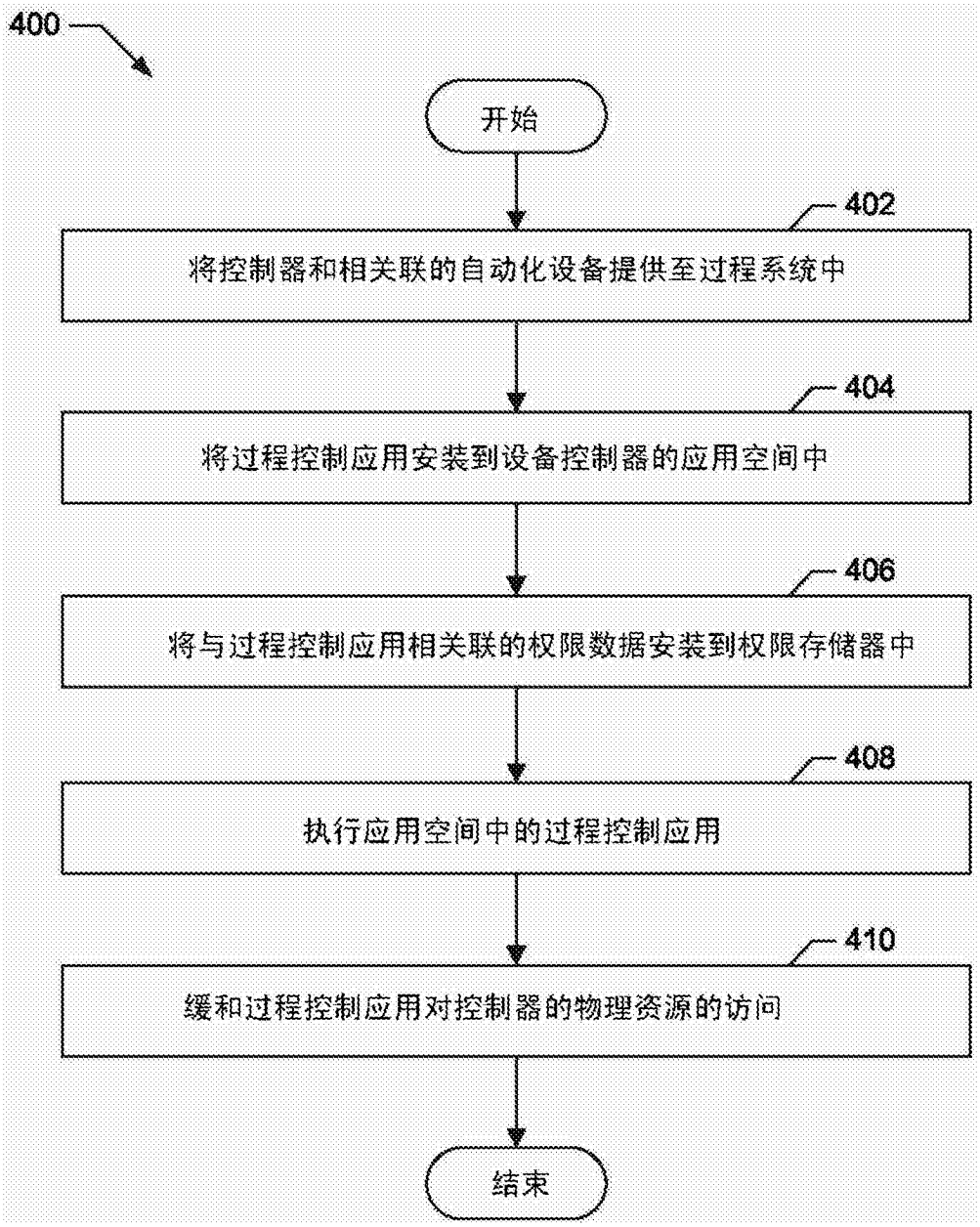

400
开始
402
将控制器和相关联的自动化设备提供至过程系统中
404
将过程控制应用安装到设备控制器的应用空间中
406
将与过程控制应用相关联的权限数据安装到权限存储器中
408
执行应用空间中的过程控制应用
410
缓和过程控制应用对控制器的物理资源的访问
结束

图4

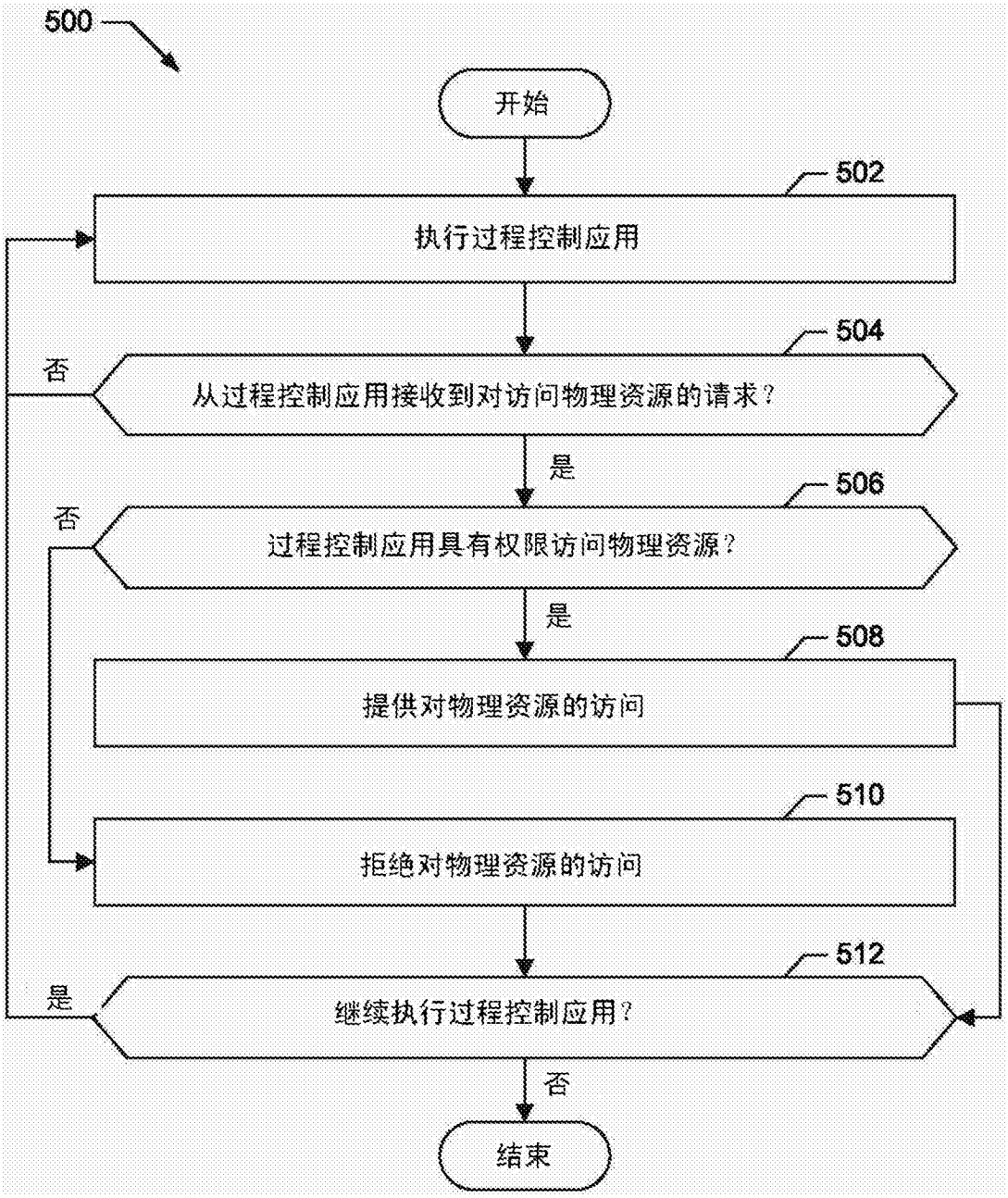

500
开始
502
执行过程控制应用
504
从过程控制应用接收到对访问物理资源的请求？
否
是
506
过程控制应用具有权限访问物理资源？
否
是
508
提供对物理资源的访问
510
拒绝对物理资源的访问
512
继续执行过程控制应用？
是
否
结束

图5

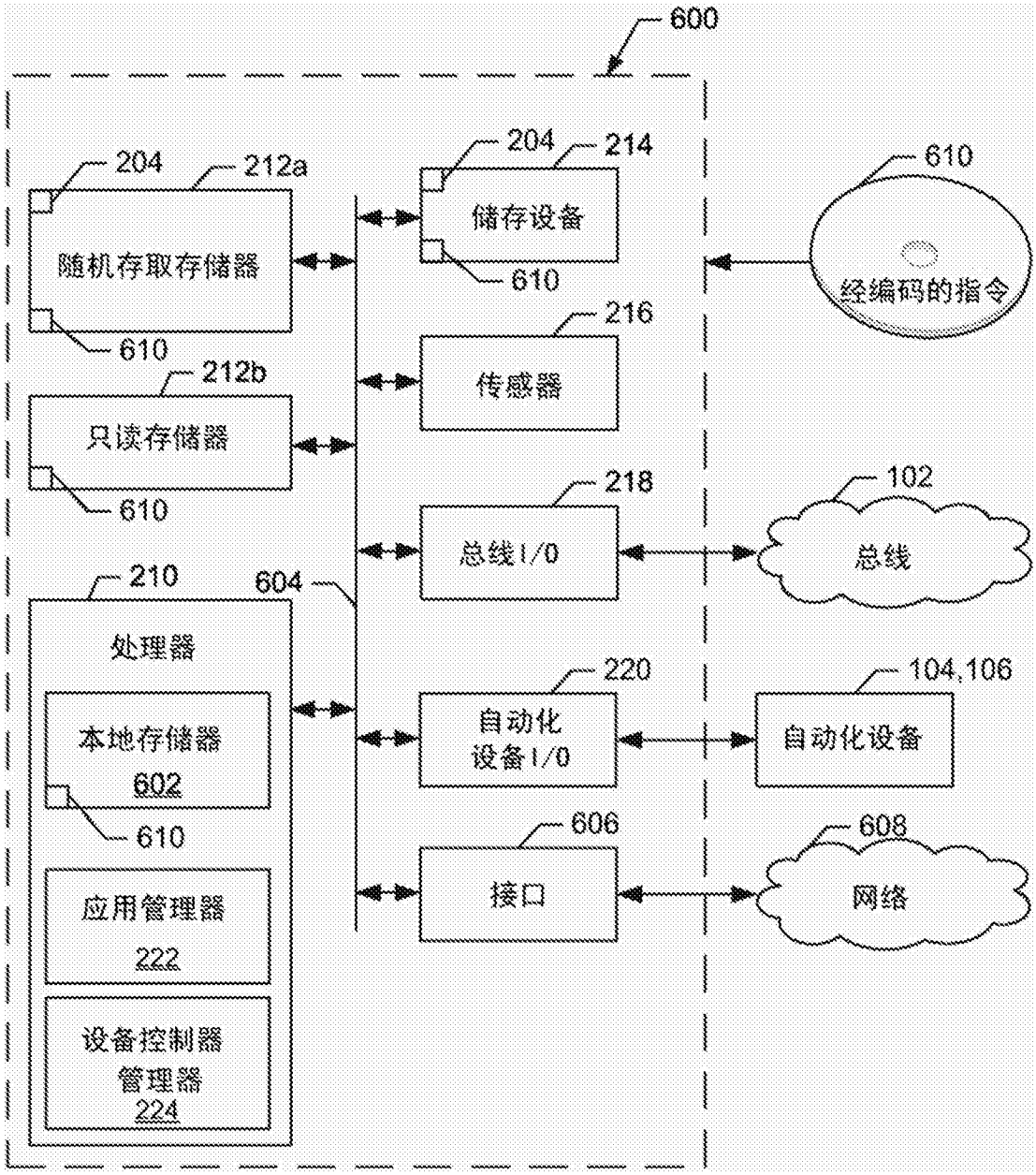

600
204
212a
随机存取存储器
610
212b
只读存储器
610
210
处理器
本地存储器
602
610
应用管理器
222
设备控制器
管理器
224
604
204
214
储存设备
610
216
传感器
218
总线I/O
220
自动化
设备I/O
606
接口
610
经编码的指令
102
总线
104,106
自动化设备
608
网络

图6