(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 101840221 B
(45)授权公告日 2015.05.06

(21)申请号 200910215252.5
(22)申请日 2009.12.31
(30)优先权数据
12/356,863 2009.01.21 US
(73)专利权人 费舍－柔斯芒特系统股份有限公司
地址 美国德克萨斯州
(72)发明人 李·艾伦·奈策尔 加里·基思·劳戈弗雷·罗兰·谢里夫
(74)专利代理机构 北京德琦知识产权代理有限公司 11018
代理人 康泉 宋志强
(51)Int.Cl.
G05B 19/418(2006.01)
(56)对比文件
CN 101154103 A,2008.04.02, 全文.
US 2003/0145221 A1,2003.07.31, 全文.
US 2007/0261103 A1,2007.11.08, 全文.
US 2008/0027587 A1,2008.01.31, 说明书第102-145,149,155,175,192-193,224节.
DE 102006058330 A1,2008.06.12, 全文.
审查员 卜冬泉

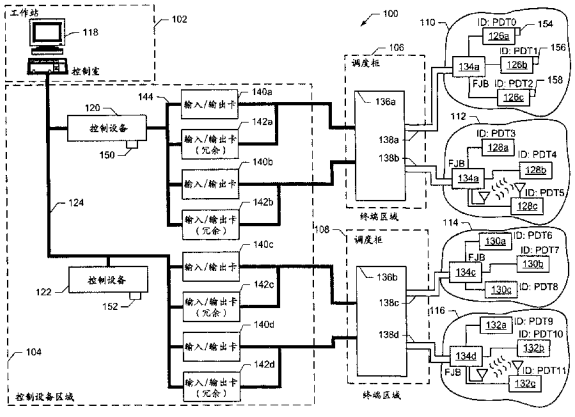
权利要求书3页 说明书17页 附图7页

(54)发明名称

可移动安全模块及相关方法

(57)摘要

本发明公开一种可移动安全模块及相关方法。一范例可移动安全模块包括一主体（所述主体配置成可移动地连接到所述过程控制设备）及布置在所述主体中的一存储器（所述存储器中存储一共享秘密）。所述范例可移动安全模块也包括一处理单元，所述处理单元布置在所述主体中，并连接到所述存储器，而且配置成读取来自所述过程控制设备的信息、对所述信息与所述共享秘密进行比较以及根据所述比较来鉴定所述过程控制设备。



CN 101840221 B

1. 一种用于过程控制系统中的第一过程控制设备和第二过程控制设备的可移动安全模块，所述可移动安全模块包括：

一主体，所述主体配置成可移动地连接到所述第一过程控制设备或所述第二过程控制设备；

一存储器，所述存储器布置在所述主体中，其中所述存储器上存储：

一共享秘密，和

与所述第一过程控制设备和所述第二过程控制设备相关的调用信息，使得所述可移动安全模块从所述第一过程控制设备可迁移，以在不需要调用所述第二过程控制设备的情况下可移动地连接到所述第二过程控制设备；以及

一处理单元，所述处理单元布置在所述主体中、连接到所述存储器，而且配置成：

读取来自所述第一过程控制设备的信息，

对所述信息与所述共享秘密进行比较，

根据所述比较，鉴定所述第一过程控制设备，以及

如果根据所述比较，所述第一过程控制设备未获得鉴定，则防止所述第一过程控制设备结合到所述过程控制系统中，其中防止所述第一过程控制设备结合致使所述第一过程控制设备在所述过程控制系统中不能操作。

2. 如权利要求 1 所述的可移动安全模块，其中所述存储器包括存储在其上的加密信息，及其中所述处理单元配置成使用所述加密信息来保护与所述第一过程控制设备相关的通信。

3. 如权利要求 2 所述的可移动安全模块，其中所述加密信息包括一加密密钥。

4. 如权利要求 3 所述的可移动安全模块，其中所述调用信息包括配置信息。

5. 如权利要求 4 所述的可移动安全模块，其中所述配置信息包括一设备标识符号或一控制参数的至少其中之一。

6. 如权利要求 1 所述的可移动安全模块，进一步包括一显示器，以用于呈现接收自所述第一过程控制设备的授权信息。

7. 如权利要求 6 所述的可移动安全模块，进一步包括一输入设备，以用于接收一用户输入以响应通过所述显示器呈现的所述授权信息中的至少一些授权信息。

8. 如权利要求 6 所述的可移动安全模块，其中所述授权信息是存储在所述第一过程控制设备中的一秘密。

9. 如权利要求 1 所述的可移动安全模块，其中所述可移动安全模块进一步包括一通信单元，以便为所述第一过程控制设备实质地提供全部通信软件及电子器件。

10. 用于过程控制系统中的第一过程控制设备和第二过程控制设备的多个可移动安全模块，其中所述模块中的每个模块包括：

一主体，所述主体配置成可移动地连接到所述第一过程控制设备或所述第二过程控制设备；

一存储器，所述存储器布置在所述主体中，其中所述存储器上存储：

一共享秘密，和

与所述第一过程控制设备和所述第二过程控制设备相关的调用信息，使得所述可移动安全模块从所述第一过程控制设备可迁移，以在不需要调用所述第二过程控制设备的情况

下可移动地连接到所述第二过程控制设备；以及

一处理单元，所述处理单元布置在所述主体中、连接到所述存储器，而且配置成：

读取来自所述第一过程控制设备的信息，

对所述信息与所述共享秘密进行比较，

根据所述比较，鉴定所述第一过程控制设备，以及

如果根据所述比较，所述第一过程控制设备未获得鉴定，则防止所述第一过程控制设备结合到所述过程控制系统中，其中防止所述第一过程控制设备结合致使所述第一过程控制设备在所述过程控制系统中不能操作。

11. 如权利要求 10 所述的多个可移动安全模块，其中所述模块中的每个模块使得能够由所述第一过程控制设备提供一不同类别的功能或功能水平。

12. 如权利要求 10 所述的多个可移动安全模块，其中所述模块的至少其中之一提供相对于所述模块的另外其中之一的升级功能。

13. 如权利要求 10 所述的多个可移动安全模块，其中所述多个模块的一第一模块被实施为所述多个模块中的一第二模块的代替物。

14. 如权利要求 13 所述的多个可移动安全模块，其中所述第一过程控制设备在所述第一模块代替所述第二模块时保持运作。

15. 一种以一可移动安全模块来保护第一过程控制设备和第二过程控制设备的方法，所述方法包括：

将所述第一过程控制设备连接到所述可移动安全模块；

通过所述可移动安全模块，读取所述第一过程控制设备中的信息；

对所述信息与存储在所述可移动安全模块的一存储器中的一共享秘密进行比较；

通过所述可移动安全模块，根据所述比较，鉴定所述第一过程控制设备；

从所述第一过程控制设备迁移所述可移动安全模块；

将所述可移动安全模块连接到所述第二过程控制设备，其中所述存储器在其上存储与所述第一过程控制设备和所述第二过程控制设备相关的调用信息；以及

在不需要调用所述第二过程控制设备的情况下操作所述第二过程控制设备。

16. 如权利要求 15 所述的方法，进一步包括防止所述第一过程控制设备的调用 - 如果根据所述比较，所述第一过程控制设备未获得鉴定。

17. 如权利要求 15 所述的方法，进一步包括使用存储在所述存储器中的加密信息来保护与所述第一过程控制设备相关的通信。

18. 如权利要求 17 所述的方法，其中所述加密信息包括一加密密钥。

19. 如权利要求 15 所述的方法，进一步包括在所述存储器中存储调用信息，以响应所述第一过程控制设备被鉴定。

20. 如权利要求 19 所述的方法，其中所述调用信息包括配置信息。

21. 如权利要求 20 所述的方法，其中所述配置信息包括一设备标识符号或一控制参数的至少其中之一。

22. 一种分布式过程控制系统，包括：

一个或多个过程控制设备；

用于通过连接到所述过程控制设备中的一个的可移动安全模块读取来自所述过程控

制设备中的所述一个的信息的工具；

用于对所述信息与存储在所述可移动安全模块的一存储器中的一共享秘密进行比较的工具；

用于根据所述比较来鉴定所述过程控制设备中的所述一个的工具；

用于授权一个或多个应用程序以用于所述过程控制设备中的所述一个的工具；

用于从所述过程控制设备中的所述一个迁移所述可移动安全模块的工具；

用于将所述可移动安全模块连接到所述过程控制设备中的另一个的工具，其中所述存储器在其上存储与所述过程控制设备相关的调用信息；以及

用于在不需要调用所述过程控制设备中的所述另一个的情况下操作所述过程控制设备中的所述另一个的工具。

23. 如权利要求 22 所述的分布式过程控制系统，进一步包括用于进行一个或多个应用程序的两人授权的工具。

可移动安全模块及相关方法

技术领域

[0001] 本发明总体上涉及过程控制系统，尤其涉及用于过程控制设备的可移动安全模块。

背景技术

[0002] 过程控制系统－如那些用于化学、石油、药物、制浆及造纸或其他制造过程的过程控制系统－典型地包括一个或多个过程控制设备（比如控制器及输入／输出服务器），所述过程控制设备与至少一个主机（包括至少一个操作员工作站）或与一个或多个现场设备（例如设备控制器、阀、阀启动器、阀定位器、开关、传送器、温度传感器、压力传感器、流率传感器及化学成分传感器或这些设备的组合）通信连接，以控制一物理工厂（炼油厂及汽车制造设施）中的物理过程或离散制造操作（例如开启或关闭阀及测量或推断过程参数）。过程控制设备接收所述现场设备所进行的过程测量的信号及／或关于所述现场设备的其他信息，并使用这些信息来实施控制例程，然后产生控制信号并通过总线或其他通信线传送至所述现场设备，以控制所述过程控制系统的操作。

[0003] 许多过程控制系统结合安全特征，以防止未经授权的人员改变控制参数、命令设备、获取过程控制信息等等，从而确保一过程工厂的安全及可靠操作。这些安全特征在包括一安全仪表系统 (SIS) 的过程控制工厂中特别重要，过程控制工厂可能需要为涉及危险化学物或可能在一主要或首要过程控制系统在操作期间发生故障或受危及时造成安全风险的任何其他材料或过程执行所述主要或首要过程控制系统的安全停机。传统上，过程控制系统通过使用一独立及个别安全系统为安全仪表系统提供安全，所述独立及分离的安全系统的使用典型地授权予数目有限的人员。然而，由于操作及维护完全分离的系统所需的成本及工夫增加，促使在过程控制系统中结合安全系统。这样的安全系统与过程控制系统的结合引致安全关注及需要额外的安全措施来防止未经授权的、对安全仪表系统的改变（即使所述过程控制系统本身已经被危及）。

发明内容

[0004] 本发明公开用于过程控制设备的范例可移动安全模块及相关方法。一范例可移动安全模块包括一主体（所述主体配置成可移动地连接到所述过程控制设备）及布置在所述主体中的一存储器（所述存储器中存储一共享秘密）。所述范例可移动安全模块也包括一处理单元，所述处理单元布置在所述主体中，并连接到所述存储器，而且配置成读取来自所述过程控制设备的信息、对所述信息与所述共享秘密进行比较以及根据所述比较来鉴定所述过程控制设备。

[0005] 在另一范例中，用于一过程控制设备的所述多个可移动安全模块中的每个可移动安全模块包括一主体（所述主体配置成可移动地连接到所述过程控制设备）及布置在所述主体中的一存储器（所述存储器中存储一共享秘密）。此外，所述模块中的每个模块包括一处理单元，所述处理单元布置在所述主体中，并连接到所述存储器，而且配置成读取来自所

述过程控制设备的信息、对所述信息与所述共享秘密进行比较以及根据所述比较来鉴定所述过程控制设备。

[0006] 在又另一范例中，以一可移动安全模块保护一过程控制设备的一方法包括通过所述安全模块读取所述过程控制设备中的信息及对所述信息与存储在所述安全模块的一存储器中的一共享秘密进行比较。所述范例方法也包括通过所述安全模块、根据所述比较来鉴定所述过程控制设备。

[0007] 另一用于保护一过程控制设备的范例方法包括在所述过程控制设备接收一要求或命令，其中所述要求或命令与一第一人员相关。所述范例方法也包括取得一秘密以响应所述要求或命令的接收、提供所述秘密予一第二人员、通过所述第二人员发送所述秘密到所述过程控制设备以及为所述过程控制设备授权所述要求或命令以响应所述过程控制设备接收所述秘密。

[0008] 在又再一范例中，一分布式过程控制系统包括一个或多个过程控制设备、用于读取来自至少一个过程控制设备的信息的设备，以及对所述信息与一共享秘密进行比较的设备。所述范例过程控制系统也包括用于根据所述比较来鉴定所述过程控制设备的至少其中之一的设备，以及授权用于所述过程控制设备的至少其中之一的一个或多个应用程序的设备。

附图说明

[0009] 图 1 为一框图，其显示一范例过程控制系统，所述范例过程控制系统实施在此描述的范例方法及设备。

[0010] 图 2 为一详细框图，其显示图 1 的范例安全模块。

[0011] 图 3 描绘一顶视图，而图 4 描绘图 1 的范例安全模块的一侧面图。

[0012] 图 5 描绘一隔离电路配置，所述隔离电路配置可以连同图 1 的范例安全模块实施，以便使所述安全模块与控制设备及与通信总线电气隔离。

[0013] 图 6 描绘一范例方法的一流程图，所述范例方法可以用于实施图 1 的范例安全模块，以便调用一控制设备及授权一动作。

[0014] 图 7 描绘一范例方法的一流程图，所述范例方法可以用于实施图 1 的范例安全模块，以便实施一动作的两人授权。

[0015] 图 8 为一框图，其显示一范例处理器系统，所述范例处理器系统可以用于实施在此描述的范例方法及设备。

具体实施方式

[0016] 虽然以下描述范例方法及设备，其中除了其他构件以外，还包括在硬件上实施的软件及 / 或固件，但应该注意的是，这些系统只是在于阐明、而不应被当成是限制本发明包括的范围。例如，预期任何或所有这些硬件、软件及固件构件可以单独地实施在硬件、单独地实施在软件或实施在任何硬件及软件组合。因此，虽然以下描述一些范例设备及系统，但本领域的普通工程技术人员将能理解，在此提供的范例并不是实施这些设备及系统的仅有途径。

[0017] 一范例过程控制系统（例如图 1 的过程控制系统 100）包括一控制室（例如图 1

的控制室 102)、一过程控制设备区域（例如图 1 的过程控制设备区域 104)、一个或多个终端区域（例如图 1 的一第一终端区域 106 及一第二终端区域 108) 以及一个或多个过程区域（例如图 1 的过程区域 110、112、114 及 116)。一过程区域包括多个现场设备，这些现场设备执行与执行一特定过程（例如一化学过程、一石油过程、一药物过程、一制浆及造纸过程等等）相关的操作（例如控制阀、控制发动机、控制锅炉、监测参数及测量参数等等)。有些过程区域由于苛刻的环境条件（例如相对高的温度、气载毒素、不安全辐射水平等等）而不能由人类接近。所述控制室典型地包括在一可由人类安全地接近的环境中的一个或多个工作站。所述工作站包括用户应用程序，用户（例如工程师、操作员、过程控制人员等等）可以存取这些用户应用程序，以便通过（例如）改变可变值、过程控制功能等等来控制所述过程控制系统的操作。所述过程控制器区域包括一个或多个过程控制器，这些过程控制器通信连接到所述控制室中的工作站。所述过程控制器通过执行通过所述工作站实施的过程控制策略，使所述现场设备的控制自动化。一范例过程控制策略涉及使用一压力传感器现场设备来测量一压力，以及自动地发送一命令到一阀定位器，以便根据所述压力测量来开启或关闭一流量阀。所述终端区域包括一调度柜，所述调度柜使所述控制设备能够与所述过程区域中的现场设备通信。明确地说，所述调度柜调度、整理及 / 或路由所述现场设备与通信连接到所述控制设备的一个或多个输入 / 输出卡之间的信号。

[0018] 一过程控制系统中的现场设备使用每个现场设备与通信连接到一控制设备（例如一过程控制器、一可编程逻辑控制器等等）的一相应输入 / 输出卡之间的一总线（例如一电线、一电缆或一电路)，通信连接到控制设备。一输入 / 输出卡使得能够通过转变或转换在所述控制设备与所述现场设备之间传送的信息，将一控制设备通信连接到与不同数据类别或信号类别（例如模拟输入 (AI) 数据类别、模拟输出 (AO) 数据类别、离散输入 (DI) 数据类别、离散输出 (DO) 数据类别、数字输入数据类别及数字输出数据类别）及不同现场设备通信协议关联的多个现场设备。例如，一输入 / 输出卡可以带有一个或多个现场设备界面，所述现场设备界面配置成使用与一现场设备相关的现场设备通信协议、与该现场设备交换信息。不同的现场设备界面通过不同的频道类别（例如模拟输入 (AI) 频道类别、模拟输出 (AO) 频道类别、离散输入 (DI) 频道类别、离散输出 (DO) 频道类别、数字输入频道类别及数字输出频道类别）进行通信。此外，所述输入 / 输出卡可以将接收自所述现场设备的信息（例如电压水平、数字值等等）转换成所述控制设备能够使用来执行与控制所述现场设备相关的操作的过程信息（例如压力测量值)。

[0019] 如果某些控制设备与现场设备之间的通信未受保护，未经授权的命令（例如为响应未经授权发出命令的人员及 / 或控制设备而发出的命令）可能严重地危及所述过程控制系统的安全操作。例如，一特定控制设备可能未获得授权传送控制信号（或更概括地 - 传送命令或要求）到一现场设备以促使所述现场设备执行一动作（例如关闭一阀及停止一有毒物质及 / 或高度反应性的化学物的流动)。为了确保只是某些控制设备及 / 或人员可以操作这样的关键性控制设备及 / 或现场设备，所述控制设备及所述现场设备需要高度安全性。

[0020] 在安全对安全仪表系统极为重要的同时，安全一般上已经在过程控制系统中显得相当重要，尤其是在包括集成安全设备或装置、而且需要所述安全设备的安全性的过程控制系统（不论所述过程控制系统整体的安全性是否已经被危及)，更是如此。在有些已知过

程控制系统中，在控制设备的调用期间，通过要求鉴定及授权合并入所述过程控制系统的任何控制设备，提供某个水平的安全性。一设备只是在被鉴定及授权之后方能被给予一身份及其在所述系统中的角色，以及在被给予身份及角色之后被允许与所述过程控制系统进行相互操作。

[0021] 在其调用之后，通过提供数据（例如下载编码或软件）到所述已调用控制设备，允许一控制设备的角色。在所述控制设备的操作期间（即在所述控制设备正在根据其角色执行其下载编码或软件时），操作员、工程师或任何其他获授权用户能够监测所述控制设备的操作、发送命令到所述控制设备、向所述控制设备要求信息等等。

[0022] 对一控制设备的鉴定典型地确保所述控制设备是在预定的、它在其中操作的一控制系统中被使用。有些已知鉴定过程可能使用所述控制设备及所述控制设备正在被并入的系统已知的、包括（例如）共享秘密的信息。这一共享秘密可以在制造时永存地存储在所述控制设备，而所述过程控制系统配置成在所述控制设备被鉴定时辨认这个共享秘密。此外，所述控制设备可以永久地存储有关所述过程控制系统的、用于确定所述控制设备是否能够与所述过程控制系统相互操作的信息。

[0023] 一旦一控制设备已经被鉴定及授权，所述控制设备可以在其操作期间使用进一步的安全措施，以防止工作站、控制器、未经授权的人员等等进行未经授权的动作或使用所述控制设备。这些进一步的安全措施经常包括所述控制设备与任何其他与所述过程控制系统相关的实体（例如控制器、现场设备、工作站、人员、应用程序等等）之间的任何通信的加密的使用。为了这个目的，有些过程控制设备包括一加密密钥或多个加密密钥，所述加密密钥可以在所述控制设备制造时存储在其中或以其他方式制造到其中。

[0024] 虽然前述包括共享秘密、加密密钥等等的安全措施可能有效，但当前这些安全措施被使用的方式可能带来一些实践问题。例如，如果一共享秘密（其在制造时硬编码到有些控制设备中）为危及（例如被未经授权的实体知晓），所述控制设备中的所述共享秘密将必须改变，以便为该设备恢复安全性。然而，要改变这一共享秘密可能需要将所述控制设备从所述过程控制系统迁移，并将所述控制设备送到其制造商以改变所述共享秘密。此外，如果一控制设备发生故障及需要置换，替换所述失效设备的任何设备将需要所述替换设备的调用（例如鉴定、授权、下载软件或编码以执行其角色等等），而所述替换设备的调用费时而昂贵，而且经常需要所述过程控制系统脱机一不可接受的时间长度。

[0025] 此外，即使在所述输入／输出卡及现场设备连接到正确的控制设备时，如果所述控制设备被不正确地使用（例如为响应一错误的命令或要求而执行一动作），所述过程控制系统中再次可能有严重而危险的后果。为了确保所述控制设备被正确地使用或不被不适当地修改，至少对于一些操作而言，这些控制系统的有些控制系统或部分需要对某些控制设备进行附加的存取控制或授权，以确定是否允许这些控制设备为响应一要求或命令而采取适当动作。在有些情况下（例如高度敏感的操作），一控制设备的授权可能需要所述控制室中的一操作员或工程师及在所述控制设备处的另一人执行授权任务（即需要两人授权）。传统上，在所述控制设备处的所述人员将需要根据来自所述控制室中的所述人员的一命令，在所述设备处转动一钥匙或输入一编码。然而，这不只需要所述控制设备制造时带有这些物理约束（例如具有一钥匙锁、键等等），还需要实施一钥匙锁管理制度，以避免钥匙锁的损失、未经授权的复制或混乱。实物钥匙的使用进一步需要管理钥匙取用、监测钥匙发

放及位置、保持真正转动钥匙的人员的记录等等。此外，钥匙开关不不按时间暂停而却需要由一人物理地开动，因此在实践中，所述钥匙可能被永久地上锁或无限期地激活。

[0026] 在此描述的范例设备及方法可以更灵活及可靠地保护一过程控制系统。明确地说，在此描述的范例设备及方法使用一安全模块，所述安全模块可以移动地连接到一控制设备（例如一现场设备、一控制器等等）。所述安全模块充分地提供鉴定、调用及保护一控制设备以及授权与所述控制设备相关的动作或应用程序所需要的全部安全软件及电子器件。这包括（例如）存储用于鉴定所述控制设备的秘密（例如共享秘密）、存储用于授权所述控制设备的动作的加密键或其他加密信息、提供防止未经授权的要求或命令的保护、提供一身份予所述控制设备、为所述过程控制系统中的所述控制设备分配一任务、推动两人授权方案以及以数据配置所述控制设备，以执行所分配的任务。

[0027] 在一安全模块连接到一控制设备时，所述安全模块读取来自所述控制设备的控制设备信息。这个信息与存储在所述安全设备的一存储器中的一共享秘密进行比较。如果所述控制设备信息与所述共享秘密之间存在相互关系（例如一匹配），则所述控制设备被授权安装。因此，所述安全模块鉴定所述控制设备，并将其结合到所述过程控制系统中。如果所述共享秘密与所述控制设备信息不互相关或匹配，所述控制设备不被授权使用所述安全模块，而且不被授权安装在该过程控制系统中或不被授权安装在所述过程控制系统的该部分中。在这种情况下，所述控制设备不能调用，因此保持不能操作。

[0028] 在所述控制设备被调用之后，所述控制设备被配置以所述控制设备为执行其在鉴定期间获分配的任务而需要的数据。一旦所述控制设备开始操作，所述控制设备一般由一个或多个操作员或工程师看顾。所述操作员及／或工程师与所述控制设备（以及其他控制设备）互动，以控制或监测他们负责的所述过程控制系统（例如物理工厂）的所述部分（包括（例如）一纸机、一蒸馏塔或一制造单元），以确保所述系统或其部分按预定计划操作。在所述过程控制系统的操作期间，所述控制设备接收许多要求、命令、修改及／或其他通信。为了防止所述控制设备为响应未经授权的通信而采取动作，所述安全模块监测所述通信及授权或防止动作。例如，所述安全模块可以摘录所述通信中的信息，并对所述信息中的至少一些信息与存储在所述安全模块的所述存储器中的加密键进行比较。如果所述加密键与所述通信中的所述信息存在相互关系，所述安全模块可以授权所述控制设备采取适当动作以响应所述通信。在不存在与所述加密键的相互关系时，所述控制设备的动作不被授权，而且因此被防止。

[0029] 此外，如以下更详细描述的那样，由于在此描述的范例安全模块能够可移动地连接到一控制设备，所述控制设备使用的所述安全特征可以在不需要替换所述控制设备、将所述控制设备送回制造商供进行重新配置、或以其他方式将所述控制设备从所述过程控制系统迁移的情况下，通过迁移所述安全模块并以使用期望的不同的安全特征的另一安全模块替代所述安全模块来改变。此外，从一第一控制设备迁移的一安全模块可以在不需要调用一第二控制设备（例如所述第一控制设备的一替代控制设备）的情况下，可移动地连接到所述第二控制设备。此外，如以下更详细的描述那样，如果一控制设备使用的相同类别的安全特征有已修改的（例如更新的）安全软件及／或电子器件（包括诊断器件）可用，所述控制设备的所述安全模块可以在不需要替换所述控制设备、重新调用所述控制设备、将所述控制设备送回制造商供进行重新配置、或以其他方式将所述控制设备从所述过程控制

系统迁移的情况下迁移，而且可以以一不同的、具有所述已修改的安全软件及/或电子器件的安全模块替换。相反地，只是在所述控制设备处的所述安全模块调换为包括不同安全特征的一不同的安全模块。

[0030] 在此描述的范例安全模块可以是设备齐全、密封的电子模块，其包括安全软件。此外，这些范例安全模块可以移动地插入或以其他方式连接到不同类别、牌子（例如由不同制造商提供者）及样式的控制设备。所述范例安全模块可以标准化及用于不同类别的控制设备，以便为所述控制设备提供所述安全特征。更明确地说，所述机械配置及界面（包括所述控制设备的包装、电气连接（例如插脚引线）等等）以及所述安全模块可以标准化，使得提供不同安全特征的许多可用安全模块中的任何安全模块可以用于可能由任何数目的制造商制造的多种控制设备中的任何控制设备。同样地，所述安全模块与所述控制设备中的其他电子器件通信的方式也可以标准化。换句话说，用于使所述控制设备与所述安全模块之间能够进行通信的通信方案也可以跨越控制设备的类别、牌子、及样式等等标准化，以便进一步促进安全模块与控制设备之间的可交换性。

[0031] 在此描述的范例安全模块可以使控制设备安全能够标准化，从而使得能够在不需要任何一个安全编程（即安全特征集合）的特殊性的情况下制造所述安全模块。可以在制造一控制设备之后（例如在所述控制设备被安装在一过程控制系统时或在调用期间）、通过在所述控制设备中安装一适当的安全模块来分配或配置这样的安全特征。这样可减少所需要的零部件（例如备用的控制设备）的数目及便于容易将控制设备从一个安全编程转换到另一个安全编程。在此描述的范例方法及设备也简化控制设备的制造，这是由于所述控制设备可以不再需要包括可观数量的内部安全电子器件或软件。因此，在此描述的范例方法及设备为制造商消除了生产那么多使用不同安全特征的相似控制设备的需要。

[0032] 此外，所述范例安全模块可以实质地包括用于所述控制设备的所有通信软件及电子器件。因此，在此描述的安全模块可以包括在同时另案待审及共同拥有的、标题为“用于将现场设备通信连接到过程控制系统中的控制器的设备及方法”(Apparatus and Methods to Communicatively Couple FieldDevices to Controllers in a Process Control System)的美国12/236,165号专利申请(U.S.Application Serial Number 12/236,165)中描述的通信模块的所有特征；所述专利申请在此通过引用全部并入本专利。

[0033] 此外，系统维护成本可以减少，这是由于可以通过以具有经修改或升级的软件（包括结合新的或不同的特征的软件）置换一安全模块，轻易地添加安全软件修改或升级。此外，由于在此描述的范例安全模块可以在不需要存取一控制设备的内部电子器件的情况下轻易地调换或置换，一安全编程的升级及/或变更可以现场执行（即在不需要迁移所述控制设备的情况下执行）。此外，一控制设备的诊断器件可以包括在一安全模块中，因此需要更新或更好的诊断软件的客户可以在不需要改变所述控制设备的内部电子器件的情况下将一安全模块调换为包含所期望的诊断器件的另一安全模块。此外，有些范例安全模块可以包括本地标记信息，例如控制设备需要及/或其他控制设备信息。在所述范例安全模块中包括任何或所有的所述安全软件、诊断信息及/或本地标记信息便于控制设备的配置及控制设备的操作条件、历史、维护需要等等的评估。

[0034] 此外，在有些范例中，所述安全模块可以根据其中包括的安全特征、升级、更新、诊断器件等等的类别编码（例如颜色编码）。所述编码方案便于识别用于连接到所述控制设

备的适当安全模块。

[0035] 现在详细参看图 1，一范例过程控制系统 100 包括所述控制室 102，控制室 102 带有一工作站 118，工作站 118 通过一般称为应用程序控制网络 (ACN) 的一总线或局域网 (LAN)124 通信连接到一个或多个控制设备，包括一第一控制设备（例如一控制器）120 及一第二控制设备（例如一控制器）122。局域网 (LAN)124 可以使用任何期望的通信媒介及协议来实施。例如，局域网 (LAN)124 可以基于有线或无线以太网通信协议。然而，可以采用任何其他适合的有线或无线通信媒介及协议。工作站 118 可以配置成执行与一个或多个信息技术应用程序、用户互动应用程序及 / 或通信应用程序相关的操作。例如，工作站 118 可以配置成执行与过程控制相关应用程序及通信应用程序相关的操作，以使工作站 118 及控制设备 120 及 122 能够使用任何期望的通信媒介（例如无线通信媒介、固定通信媒介等等）及协议（例如 HTTP，SOAP 等等），与其他设备或系统进行通信。控制设备 120 及 122 可以配置成执行一个或多个过程控制例程或功能，这些过程控制例程或功能已经由系统工程师或其他系统操作员使用（例如）工作站 118 或使用任何其他已经下载到控制设备 120 及 122 以及已经在控制设备 120 及 122 中初始化的工作站产生。在所述图解范例中，工作站 118 位于控制室 102 中，而过程控制设备 120 及 122 则位于与控制室 102 分开的控制设备区域 104 中。

[0036] 在图 1 的实施例中，第一控制设备 120 通过一背板通信或内部输入 / 输出总线 144 通信连接到输入 / 输出卡 140a-b 及 142a-b。为了与工作站 118 通信，第一控制设备 120 通过局域网 (LAN)124 通信连接到工作站 118。第二控制设备 122 通过局域网 (LAN)124 通信连接到工作站 118 及输入 / 输出卡 140c-d 及 142c-d。输入 / 输出卡 140c-d 及 142c-d 配置成通过局域网 (LAN)124，与第二控制设备 122 及工作站 118 通信。照这样，输入 / 输出卡 140c-d 及 142c-d 可以直接与工作站 118 交换信息。

[0037] 在所述图解范例中，范例过程控制系统 100 包括第一过程控制区域 110 中的现场设备 126a-c、第二过程控制区域 112 中的现场设备 128a-c、第三过程控制区域 114 中的现场设备 130a-c 及第四过程控制区域 116 中的现场设备 132a-c。为了在控制设备 120 及 122 与现场设备 126a-c、128a-c、130a-c 及 132a-c 之间传送信息，范例过程控制系统 100 带有现场接线盒 (FJB)134a-d 及调度柜 136a-b。现场接线盒 (FJB)134a-d 中的每个现场接线盒 (FJB) 通过相应的多导线电缆 138a-d（或一多总线电缆），将来自现场设备 126a-c、128a-c、130a-c 及 132a-c 中的相应现场设备的信号路由到调度柜 136a-b 的其中之一。调度柜 136a-b 依次地调度（例如整理、聚合等等）接收自现场设备 126a-c、128a-c、130a-c 及 132a-c 的信息，并将所述现场设备信息路由到控制设备 120 及 122 的相应输入 / 输出卡（例如输入 / 输出卡 140a-b）。在所述图解范例中，控制设备 120 及 122 与现场设备 126a-c、128a-c、130a-c 及 132a-c 之间的通信为双向，所以调度柜 136a-b 也用于通过现场接线盒 (FJB)134a-d、将接收自控制设备 120 及 122 的输入 / 输出卡 140a-b 的信息路由到现场设备 126a-c、128a-c、130a-c 及 132a-c 中的相应现场设备。

[0038] 在图 1 的所述范例中，现场设备 126a-c、128a-c、130a-c 及 132a-c 通过电导（例如有线）、无线及 / 或光纤通信媒介，通信连接到现场接线盒 (FJB)134a-d。例如，现场接线盒 (FJB)134a-d 可以带有一个或多个有线、无线及 / 或光纤数据收发器，以便与现场设备 126a-c、128a-c、130a-c 及 132a-c 的有线、无线及 / 或光纤数据收发器进行通信。在所述图

解范例中，现场接线盒 (FJB)134b 及 134d 依次无线地通信连接到现场设备 128c 及 132c。在一选择性实施例中，调度柜 136a-b 可以省略，而且来自现场设备 126a-c、128a-c、130a-c 及 132a-c 的信号可以在没有中间结构（即没有调度柜 136a-b）的情况下，从现场接线盒 (FJB)134a-d 直接地路由到控制设备 120 及 122 的输入 / 输出卡 140a-d。在又另一实施例中，现场接线盒 (FJB)134a-d 可以省略，而且现场设备 126a-c、128a-c、130a-c 及 132a-c 可以直接地连接到调度柜 136a-b。

[0039] 现场设备 126a-c、128a-c、130a-c 及 132a-c 可以是符合 Fieldbus 协议的阀、启动器、传感器等等，在这种情况下，现场设备 126a-c、128a-c、130a-c 及 132a-c 通过使用所述广为人知的 FOUNDATION Fieldbus 通信协议的一数字数据总线进行通信。当然，其他类别的现场设备及通信协议也可以被使用。例如，现场设备 126a-c、128a-c、130a-c 及 132a-c 也可以是符合 Profibus、HART 或 AS-i、并通过使用所述广为人知的 Profibus 及 HART 通信协议进行通信的设备。在有些实施例中，现场设备 126a-c、128a-c、130a-c 及 132a-c 可以使用模拟通信或离散通信来传送信息，而不是使用数字通信来传送信息。此外，所述通信协议可以用于传送与不同数据类别相关的信息。

[0040] 现场设备 126a-c、128a-c、130a-c 及 132a-c 中的每一个现场设备配置成存储现场设备识别信息。所述现场设备识别信息可以是唯一地识别现场设备 126a-c、128a-c、130a-c 及 132a-c 中的每个现场设备的物理设备标记 (PDT) 值、设备标记名称、电子序号等等。在图 1 的图解范例中，现场设备 126a-c、128a-c、130a-c 及 132a-c 以物理设备标记值 PDT00-PDT11 的形式存储现场设备识别信息。所述现场设备识别信息可以由现场设备制造商及 / 或由涉及现场设备 126a-c、128a-c、130a-c 及 132a-c 的安装及 / 或调用的操作员或工程师存储或编程在现场设备 126a-c、128a-c、130a-c 及 132a-c 中。

[0041] 为了控制所述控制设备 120 及 122（及 / 或工作站 118）与现场设备 126a-c、128a-c、130a-c 及 132a-c 之间的输入 / 输出通信，控制设备区域 104 带有多个输入 / 输出卡 140a-d。在所述图解范例中，输入 / 输出卡 140a-b 配置成控制第一控制设备 120（及 / 或工作站 118）与第一及第二过程控制区域 110 及 112 中的现场设备 126a-c 及 128a-c 之间的输入 / 输出通信，而输入 / 输出卡 140c-d 配置成控制第二控制设备 122（及 / 或工作站 118）与第三及第四过程控制区域 114 及 116 中的现场设备 130a-c 及 132a-c 之间的输入 / 输出通信。

[0042] 在图 1 的图解范例中，输入 / 输出卡 140a-d 装置在控制设备区域 104 中。为了从现场设备 126a-c、128a-c、130a-c 及 132a-c 传送信息到工作站 118，输入 / 输出卡 140a-d 传送所述信息到控制设备 120 及 122，接着由控制设备 120 及 122 传送所述信息到工作站 118。同样地，为了从工作站 118 传送信息到现场设备 126a-c、128a-c、130a-c 及 132a-c，工作站 118 传送所述信息到控制设备 120 及 122，控制设备 120 及 122 接着传送所述信息到输入 / 输出卡 140a-d，然后输入 / 输出卡 140a-d 传送所述信息到现场设备 126a-c、128a-c、130a-c 及 132a-c。在一选择性实施例中，输入 / 输出卡 140a-d 可以通信连接到控制设备 120 及 122 内部的局域网 (LAN)124，使得输入 / 输出卡 140a-d 可以与工作站 118 及 / 或控制设备 120 及 122 直接地通信。

[0043] 为了在输入 / 输出卡 140a-d 的任何其中之一发生故障时提供容错操作，输入 / 输出卡 142a-d 配置成冗余输入 / 输出卡。也就是说，如果输入 / 输出卡 140a 发生故障，冗余

输入 / 输出卡 142a 承担控制功能并执行输入 / 输出卡 140a 原应执行的相同的操作。同样地，冗余输入 / 输出卡 142b 在输入 / 输出卡 142b 发生故障时承担控制功能、等等。

[0044] 如控制设备区域 104 中所示，一第一安全模块 150 直接连接到第一控制设备 120，而一第二安全模块 152 直接连接到第二控制设备 122。此外，安全模块 154、156 及 158 直接连接到相应的控制设备 126a、126b 及 126c，控制设备 126a、126b 及 126c 在这个范例中被描绘为现场设备。例如，安全模块 150-158 可以配置成具有似饰物形状的可移动地插入的设备（例如带有一保护盖或外罩及一可插入电气连接器的一电路卡）。在一选择性实施例中，安全模块 150-158 可以通过中间结构或设备，通信连接到控制设备 120 及 122 及 / 或 126a-c。

[0045] 安全模块 150-158 实质上提供过程控制系统 100 使用的所有安全软件及电子器件，以鉴定及调用控制设备 120、122 及 126a-c 及授权所述控制设备为响应所接收的要求或命令而采取的动作。更概括地说，安全模块 150-158 确保适当的控制设备在过程控制系统 100 中适当地连接，并确保这些设备以适当的方式使用。以下更详细地讨论范例安全模块 150-158 及它们的相关操作。

[0046] 在所述图解范例中，调度柜 136a-b、安全模块 150-158、输入 / 输出卡 140a-d 及 142a-d 以及控制设备 120、122 及 126a-c 促成将现有过程控制系统安装迁移到与图 1 的范例过程控制系统 100 的配置充分相似的配置。例如，由于安全模块 150-158 可以配置成包括任何合适的界面类别，安全模块 150-158 可以配置成通信连接到任何类别的控制设备。同样地，控制设备 120 及 122 可以配置成包括一已知局域网 (LAN) 界面，以便通过一局域网 (LAN) 传送信息到一已经安装的工作站。在有些实施例中，输入 / 输出卡 140a-d 及 142a-d 可以安装在已知控制设备中或通信连接到已知控制设备，使得不需置换已经安装在一过程控制系统的控制设备。

[0047] 在图 5 描绘的选择性范例中，安全模块 150 及 152 可以用于将相应的控制设备 120 及 122 连接到局域网 (LAN)124 或内部输入 / 输出总线 144。在该范例中，所有来自工作站 118 的通信由安全模块 150 及 152 处理，而且在适当时（如以下详述的那样）传送到相应的控制设备 150 及 152。此外，来自输入 / 输出卡 140a-d 及 142a-d 的所有通信也由安全模块 150 及 152 处理，而且在适当时传送到相应的控制设备 150 及 152。

[0048] 图 2 显示一安全模块 200 的一实施例，该实施例可以代表在此描述的任何范例安全模块。图 2 的范例安全模块 200 包括一外部总线界面 202，以使安全模块 200 能够与（例如）使用安全模块 200 来将一控制设备连接到局域网 (LAN)124 或内部输入 / 输出总线 144 的配置中的一输入 / 输出卡及 / 或一工作站进行通信。

[0049] 为了识别安全模块 200 的一地址及 / 或一控制设备的一地址，安全模块 200 带有一地址标识符 204。地址标识符 204 可以配置成在安全模块插入一控制设备时向所述控制设备查询一安全模块地址（例如一网络地址）。照这样，安全模块 200 可以在传送信息到所述控制设备或从所述控制设备传送信息时使用所述安全模块地址作为一源地址及 / 或目的地址。

[0050] 范例安全模块 200 也带有一外部总线通信处理器 206，以便通过一外部总线、与其他系统组件交换信息。在所述图解范例中，外部总线通信处理器 206 打包供传送到另一系统组件的信息，并解包接收自其他系统组件的信息。所述打包信息传送到外部总线界面

202，以便通过一外部总线传送。在所述图解范例中，外部总线通信处理器 206 产生需传送的每个包的标题信息，并读取来自所接收的包的标题信息。范例标题信息包括一目的地址（例如一输入 / 输出卡的一网络地址）、一源地址（例如安全模块 200 的网络地址）、一包类别或数据类别（例如模拟现场设备信息、现场设备信息、命令信息、温度信息、实时数据值等等）及检错信息（例如循环冗余校验 (CRC) 信息）。在有些实施例中，外部总线通信处理器 206 可以使用相同的微处理器或微控制器来实施为一处理单元 208。

[0051] 为了控制安全模块 200 的多种操作，安全模块 200 带有处理单元 208。如以上所述，在一实施例中，处理单元 208 可以使用一微处理器或一微控制器来实施。处理单元 208 传送指令或命令到安全模块 200 的其他部分，以控制这些部分的操作。

[0052] 处理单元 208 带有一阅读器 210，或通信连接到一阅读器 210；阅读器 210 用于从所述控制设备获取控制设备信息，包括（例如）鉴定信息，比如存储在所述控制设备中的一秘密。阅读器 210 也从安全模块 200 的一存储器 212 获取信息。所述存储器可以包括任何类别的可配置数据库，而且可以包括（例如）用于鉴定一控制设备的共享秘密信息、加密信息（包括用于授权所述控制设备的动作的加密密钥）、与所述控制设备相关的调用信息、配置信息（例如一设备标识符或一控制参数）及任何其他信息。

[0053] 处理单元 208 也带有一比较器 214，或通信连接到一比较器 214。比较器 214 可以用于评估已接收及 / 或已存储信息。例如，比较器 214 可以对包括接收自与安全模块 200 连接的一控制设备的一第一秘密的信息与存储在存储器 212 中的一第二秘密进行比较。比较器 214 可以评估所述第一与第二秘密之间的互相关程度，以确定它们构成一共享秘密（例如充分匹配或相同的安全信息）。比较器 214 可以近一步对一要求或命令或任何其他通信中的信息与存储在存储器 212 中的一密钥进行比较，然后评估所述二者之间的相互关系的程度，以便确定所述通信是否经过授权。

[0054] 处理单元 208 也带有一鉴定器 216，或通信连接到一鉴定器 216。虽然被描绘为分别的块，但在有些范例中，鉴定器 216 及比较器 214 可以使用软件及 / 或其他结构来结合。在这个范例中，在比较器 214 确定来自所述控制设备的所述信息与存储在安全模块 200 中的所述秘密（例如一共享秘密）充份地互相关，安全模块 200、鉴定器 216 调用所述控制设备。

[0055] 为了控制提供给与安全模块 200 连接的一控制设备的电力数量，安全模块 200 带有一电力控制器 218。在所述图解范例中，（例如）可能是位于调度柜 136a-b 的其中之一中或与一控制设备相关的一电源（例如图 5 的电源 504）提供电力予安全模块 200，以便向一通信频道界面提供电力，以使得能够与所述控制设备进行通信。在所述图解范例中，电力控制器 218 配置成调节、控制及提高及 / 或降低由一外部电源提供给安全模块 200 的电力。在有些实施例中，电力控制器 218 配置成限制用于与控制设备通信的电力数量及 / 或限制传输到所述控制设备的电力数量，以便充分地减低或消除易燃或可燃环境中发火花的风险。

[0056] 为了将接收自一电源的电力变换为用于安全模块 200 的电力，安全模块 200 带有一电力变换器 220。在所述图解范例中，用于实施安全模块 200 的电路使用一个或多个电压水平（例如 3.3V），这些电压水平不同于与安全模块 200 连接的所述控制设备需要的电压水平。电力变换器 220 配置成使用经由所述电源接收的电力提供所述不同的电压水平，以便

安全模块 200 与所述控制设备进行通信。在所述图解范例中，由电力变换器 220 产生的电力输出用于驱动安全模块 200 及与其连接的控制设备，以及用于在安全模块 200 及所述控制设备之间传送信息。有些控制设备通信协议比其他通信协议需要相对较高或较低的电压水平及 / 或电流水平。在所述图解范例中，电力控制器 218 控制电力变换器 220，以提供所述电压水平来驱动所述控制设备以及与所述控制设备通信。

[0057] 为了使安全模块 200 的电路与所述控制设备及 / 或同安全模块 200 连接的所述系统的任何其他组件电气隔离，安全模块 200 带有一个或多个隔离设备 222。隔离设备 222 可以使用电化隔离器及 / 或光学隔离器来实施。以下详细描述与图 5 有关的一范例隔离配置。

[0058] 为了在模拟信号及数字信号之间转换，安全模块 200 带有一数字 - 模拟转换器 224 及一模拟 - 数字转换器 226。数字 - 模拟转换器 224 配置成将接收的数字表示值（例如测量值）或信息转换为模拟值或信息，以供进一步在一系统（例如图 1 的过程控制系统 100）中传送。同样地，模拟 - 数字转换器 226 配置成将接收的模拟值或信息转换为数字表示值或信息，以供进一步在一系统（例如图 1 的过程控制系统 100）中传送。在所述系统中的通信是完全数字及 / 或完全模拟的一选择性实施例中，可以从安全模块 200 中省略数字 - 模拟转换器 224 及模拟 - 数字转换器 226。

[0059] 为了控制与同安全模块 200 连接的一控制设备之间的通信，安全模块 200 带有一控制设备通信处理器 228。控制设备通信处理器 228 确保信息是需传送到与安全模块 200 连接的所述控制设备的正确格式及电压类别（例如模拟或数字）。控制设备通信处理器 228 也配置成打包或解包信息，如果与安全模块 200 连接的所述控制设备配置成使用数字、打包信息进行通信。此外，控制设备通信处理器 228 配置成提取接收自一控制设备的信息，并将所述信息传送到模拟 - 数字转换器 226 及 / 或传送到外部总线通信处理器 206，以供随后传送到另一系统组件。

[0060] 范例安全模块 200 也带有一控制设备界面 230，控制设备界面 230 配置成将安全模块 200 通信连接到与其物理地连接的所述控制设备。例如，由控制设备通信处理器 228 打包的信息传送到控制设备界面 230，以通过与安全模块 200 连接的所述控制设备中的一内部总线传送。

[0061] 在所述图解范例中，控制设备通信处理器 228 也可以配置成时间戳所接收的信息。在安全模块 200 产生时间戳便于使用亚毫秒范围中的时间戳准确性来实施事件顺序 (SOE) 操作。例如，所述时间戳及相应信息可以传送到工作站 118。由（例如）工作站 118（图 1）（或任何其他处理器系统）执行的事件顺序操作可以接着用于分析一特定操作状态（例如一故障模式）之前、期间及 / 或之后发生了什么，以便确定什么原因导致所述特定操作状态发生。在所述亚毫秒范围中时间戳也使得能够使用相对较高的间隔尺寸来俘获事件。在有些实施例中，控制设备通信处理器 228 及处理单元 208 可以使用相同的微处理器或微控制器来实施。

[0062] 为了显示与所述控制设备或安全模块 200 相关的秘密、编码、指令、标识、状态或其他信息，安全模块 200 带有一显示器 232。如果鉴定器 216 不调用一控制设备，显示器 232 可以提供关于一失败调用企图的信息。如果安全模块 200 需要一份两人的授权，显示器 232 可以提供信息（包括接收自一控制设备及 / 或安全模块 200 的授权信息、指令等等）到涉及所述授权的人员的其中之一。此外，显示器 232 可以用于显示控制设备活动信息（例如

操作及维护信息等等）、数据类别信息（例如模拟信号、数字信号等等）及/或任何其他控制设备信息。如果安全模块 200 配置成通信连接到多个控制设备，显示器 232 可以用于显示与通信连接到安全模块 200 的所有控制设备相关的控制设备信息。在所述图解范例中，显示器 232 使用液晶显示器 (LCD) 来实施。然而，在其他实施例中，显示器 232 可以使用任何其他合适类别的显示设备来实施。

[0063] 安全模块 200 也带有一输入设备 234。输入设备 234 可以由操作员用于输入信息到安全模块 200 中，例如响应通过显示器 232 呈现的授权信息或其他信息。例如，如以下详细描述的那样，在两人授权期间，在所述控制设备处的一操作员可以输入一编码或命令到安全模块 200 内，以响应在显示器 232 中显示、而且产生自发送到所述控制设备的一要求或一命令的一秘密。输入设备 234 可以包括一键座、一触摸屏、一触摸板、一按键、一开关或任何其他合适的可以用于记录由一人员采取的动作的设备。

[0064] 此外，在安全模块 200 也包括用于所述控制设备的通信软件及电子器件的配置中，安全模块 200 带有一通信单元 236。一范例通信单元 236 在美国 12/236,165 号专利申请 (U.S.Application Serial Number 12/236,165) 中描述。

[0065] 图 3 描绘一顶视图，而图 4 描绘所述范例安全模块 200 及一范例控制设备 400 的一范例机械连接的一侧面图；范例安全模块 200 及范例控制设备 400 可以代表在此描述的任何范例安全模块及/或控制设备。在所述图解范例中，范例安全模块 200 包括一个或多个接触器 404（例如插销、调整片、走线等等），接触器 404 将控制模块 200 通信连接及/或电气连接到控制设备 400。在这个范例中，安全模块 200 通过一中间基部 402 连接到控制设备 400。基部 402 带有扣件 406（例如螺丝），扣件 406 可以是（例如）一设备界面，以便在一输入/输出总线将导电通信媒介（例如线端）系住、终接或固定。在安全模块 200 可移动地连接到基部 402 时，扣件 406 通信连接到一个或多个接触器 404，以使得能够在安全模块 200 与控制设备 400 之间进行信号传送及信息传送。在其他实施例中，基部 402 可以带有扣件 406 以外的任何其他合适类别的现场设备界面（例如一插座）。

[0066] 为了将安全模块 200 通信连接到控制设备 400，基部 402 带有一控制设备接触器或连接器 408。在用户将基部 402 插入控制设备 400 时，控制设备连接器 408 接合控制设备 400 的一内部总线。控制设备连接器 408 可以使用任何合适的界面来实施，包括使用一界面（例如一冲击块）来实施。为了使得能够在安全模块 200 与控制设备 400 之间传送信息，控制设备连接器 408 连接到安全模块 200 的一个或多个接触器 404。

[0067] 在所述图解范例中，安全模块 200 也包括一盖子 410（在图 3 中已移除），盖子 410 可以用于遮蔽安全模块 200 及/或安全模块 200 与控制设备的连接，以免受周围环境的影响。盖子 410 防止湿气及/或其他不利的或可能有损害的环境条件对可能经历这些条件的过程区域中的安全模块 200 造成有害影响。盖子 410 可以以任何合适的塑料、金属或其他适合密封或保护通信模块 400 的材料制成。

[0068] 如图 4 中所示，基部 402 可以带有一选择性的显示界面连接器 412，以便将安全模块 200 通信连接到一外部显示器。例如，如果安全模块 200 在没有显示器 232 的情况下实施，安全模块 200 可以使用显示界面连接器 412 来将指令、警告、错误、编码、值或任何其他信息输出到一外部显示器。

[0069] 图 5 描绘一隔离电路配置，该隔离电路配置可以连同图 1 的范例安全模块 150 实

施，以便将安全模块 150 从控制设备 120 及（例如）局域网 (LAN)124 及 / 或安全模块 144 电气隔离。然而，在图解安全模块 150 的这个范例中，任何其他安全模块可以以相同的或一相似的方式连接到任何其他控制设备。在所述图解范例中，安全模块 150 包括安全模块电路 502（例如以上描述的与图 2 有关的一个或多个块）。此外，安全模块 150 连接到内部输入 / 输出总线 144 及一电源 504。

[0070] 为了将安全模块电路 502 从内部输入 / 输出总线 144 电气隔离，安全模块 150 带有一隔离电路 506。照这样，如果控制设备 120 中发生电涌或其他电力变化，安全模块电路 502 可以配置成在不影响内部输入 / 输出总线 144 的电压以及不导致损坏输入 / 输出卡 140a（图 1）的情况下遵循（例如浮动）控制设备 120 的电压水平。隔离电路 506 及任何其他实施在安全模块 150 中的隔离电路可以使用光隔离电路或电流隔离电路来实施。

[0071] 为了将安全模块电路 502 从电源 504 隔离，安全模块 150 带有一隔离电路 508。通过将安全模块电路 502 从电源 504 隔离，与控制设备 120 相关的任何电力变化（例如电涌、刺波电流等等）将不会损坏电源 504。此外，安全模块 150 中的任何电力变化将不会损坏或负面地影响其他系统组件的操作，包括（例如）其他安全模块 152 的操作。

[0072] 典型地，所述控制设备中带有隔离电路，从减少可用于安全系统的空间的数量。然而，如图 5 的图解范例中显示的那样在安全模块 150 中提供隔离电路 506 及 508 使得能够选择性地对需要隔离的安全模块使用隔离电路。例如，图 1 的安全模块 150-158 可以在没有隔离电路的情况下实施。

[0073] 图 6 及 7 为范例方法的流程图，所述范例方法可以用于实施安全模块（例如图 1 及 2 的安全模块 150-158 及 200）。在有些实施例中，图 6 及 7 的范例方法可以使用包括由一处理器（例如图 8 的一范例处理器系统 810 中显示的处理器 812）执行的一编程的机器可读指令来实施。所述编程可以收录在存储在一有形计算机可读媒介或处理器可读媒介上，比如存储在一只读光盘存储器 (CD-ROM)、一软盘、一硬盘、一多功能数字光盘 (DVD) 或与一处理器相关的存储器及 / 或以广为人知的方式实施于固件及 / 或专用硬件。此外，虽然参考图 6 及 7 所示的流程图对所述范例方法进行描述，但本领域的普通工程技术人员将可以理解，可以选择使用许多其他方法来实施在此描述的范例安全模块 150-158 及 200。例如，所述流程块的执行顺序可以更改及 / 或所述流程块中的一些流程块可以更改、删除或结合。

[0074] 图 6 及 7 的范例方法以图 1 的范例安全模块 150 来描述。明确地说，图 6 及 7 的流程图用于描述范例安全模块 150 怎样鉴定控制设备 120 及授权与控制设备相关的动作。然而，图 6 及 7 的范例方法可以更普遍地用于实施任何其他安全模块（例如安全模块 152-158 及 200 等等）。

[0075] 现在详细参看图 6，最初安全模块 150 连接到控制设备 120，然后安全模块确定其是否已经检测到控制设备 120（流程块 602）。例如，如果安全模块 150 进行一电气连接、接收一中断信号或一状态寄存器、或以其他方式传感到控制设备 120，安全模块 150 检测控制设备 120。如果控制设备 120 没有被检测到，控件保持在流程块 602，直到控制设备 120（或任何其他控制设备）被检测到为止。

[0076] 一旦控制设备 120 已经被检测到，安全模块 150 获取控制设备信息（流程块 604）。例如，阅读器 210 检索存储在所述控制设备上的信息。这样的信息可以包括（例如）一需要、有关牌子及 / 或型号及可能与确定控制设备的类别及可能用途有关的任何其他信息。

明确地说，所述控制设备信息可以包括一共享秘密或一共享秘密的一部分。

[0077] 安全模块 150 接着对在流程块 604 获取的信息（任何获取的秘密信息）与存储在安全模块 150 中的秘密进行比较（流程块 605）。在在流程块 605 进行比较之后，安全模块 150 确定所获取的控制设备信息是否包括一共享秘密（流程块 606）（即存储在安全模块 150 的秘密充分地或恒等地匹配获取自控制设备 120 的任何秘密信息）。例如，比较器 214 分析所述控制设备信息，并评估该信息中是否有任何与其他信息（包括（例如）存储在安全模块 150 的存储器 212 中的一共享秘密）匹配或互相关。如果未找到一相互关系，安全模块 150 可以显示一错误信息（流程块 608）。所述控制设备信息与所述共享秘密之间缺乏相互关系可能指示过程控制系统 100 的该位置的一不正确的控制设备。附加地或可选择地，所述相互关系的缺乏可能指示该特定控制设备的一不正确安全模块。例如，所述控制设备可能需要一带有不同或更限制性的安全特征的安全模块。预定用于一安全敏感性较低的控制设备的一安全模块将不会适当地保护及稳固这个范例中的系统。在已经确定所述控制设备信息与存储在安全模块 150 中的所述秘密之间缺乏相互关系时，防止调用所述控制设备（流程块 610），然后所述过程结束。在这种情况下，控制设备 120 保持不可操作。

[0078] 如果确定所述控制设备信息与所述共享秘密之间存在相互关系（流程块 606），安全模块 150 鉴定所述控制设备（流程块 612）。所述鉴定指示控制设备 120 是所述过程控制系统中的这个位置的适当设备，及 / 或指示安全模块 150 是控制设备 120 的适当安全模块（例如包含适当的安全特征）。为了提供所述鉴定指示，处理单元 208 的鉴定器 216 可以（例如）产生一信号指示控制设备 120 已鉴定，及 / 或所述鉴定器可以释放通信及 / 或电气限制或停止允许控制设备 120 进行操作。因此，所述鉴定为控制设备 120 确定一安全通信状态。此外，鉴定器 216 可以向控制设备 120 提供一身份（流程块 614），例如一包括文字及数字的字符，用于在所述系统中识别控制设备 120，以便（例如）在控制系统 100 中寻址通信。鉴定器 216 也分配一任务予控制设备 120（流程块 616）。所述任务可以提供控制设备 120 可以在所述系统中采取的动作的指示，所述指示可以包括（例如）控制设备 120 可以与之通信、可能监测及 / 或控制的现场设备；控制设备 120 可以给予的命令；及控制设备 120 可以采取的其他动作。此外，鉴定器 216 可以促成控制设备 120 的配置（流程块 618）。控制设备 120 的配置包括提供对控制设备 120 需要来执行其在所述系统中的任务的数据或任何其他信息或工具及 / 或控制参数的存取。

[0079] 在控制设备 120 已经被调用（例如流程块 612-618）之后，控制设备 120 在过程控制系统 100 的操作期间接收要求及命令。安全模块 150 监测控制设备 120 的通信，并确定是否在控制设备 120 接收一要求或命令（流程块 620）。如果没有要求或命令在所述控制设备被接收，控件保持在流程块 620。如果一要求或命令被接收，安全模块 150 确定控制设备 120 是否将被适当地使用，以响应所述要求或命令。为了确定控制设备 120 是否获授权采取一动作以响应所述要求或命令，安全模块 150 对所述要求或命令中的任何加密信息与存储在存储器 212 中的一个或多个加密密钥进行比较（流程块 622）。如果安全模块 150 的加密密钥指示一动作获授权（流程块 624），则安全模块 150 允许控制设备 120 处理所述要求或命令（流程块 626），然后控件返回到流程块 620，以进行后续的通信。

[0080] 附加地或可选择地，基于授权的所述加密可以以其他核准技术（包括校验、密钥管理及抗干扰技术）取代或替换。此外，在有些范例中，所述安全模块可以保持列出被允许

与控制设备 120 进行通信的设备或控制设备 120 可以执行的动作的一白名单。如果安全模块 150 保持一白名单或其他核准前清单，所述过程将在没有进行在图 6 的中间操作中执行的所述比较及其他动作的情况下，从接收来自一设备的一预先核准要求或命令及 / 或接收来自一预先核准设备的一通信（流程块 620）进入授权及处理所述通信中的所述要求或命令（流程块 626）。

[0081] 然而，如果确定一动作未经授权（流程块 624），安全模块 150 通过（例如）防止控制设备 120 采取动作（流程块 628）来响应所述通信（包括所述要求及命令），保护控制设备 120（及整个过程控制系统 100）免受未经授权动作的影响。

[0082] 图 7 描绘一范例方法的一流程图，所述范例方法可以用于实施图 1 及 2 的安全模块，以便实施一动作（例如一控制设备执行的一控制动作）的两人授权。在过程控制系统中，有些操作足够地安全敏感，它们需要（例如）所述控制室中的一操作员或工程师及在所述设备处的另一人授权，即控制设备 120 的所述动作需要两人授权方能执行。

[0083] 所述范例方法以确定与一第一人员（例如控制室 102 中的一人员）相关的一要求或命令的确定是否已经在控制设备 150 处被接收（流程块 702）为开始。如果没有这样的包含一要求或命令的通信被接收，控件保持在流程块 702 直到此一通信被接收为止。然而，如果此一要求或命令已经被接收，安全模块 150 或其他可以移动地连接到所述控制设备（例如与所述控制设备结合）的安全组件获取与由一第一人员发送的所述要求或命令相关的一秘密（流程块 704）。在有些范例中，需获取的秘密是由安全模块 150 或其他可以移动地连接到所述控制设备（例如与所述控制设备结合）的安全组件产生。所述秘密可以是任何类别的文字、编码、加密、脉冲、光源模式、声音或任何其他类别的私人通信或密钥。

[0084] 所述秘密接着被提供予一第二人员（例如控制设备 120 本地处的一人员）（流程块 706），第二人员提供用于一动作的授权（如果适当）以响应所接收的要求或命令。在有些范例中，所述秘密显示在显示器 232 上，供所述第二人员观察。在其他范例中，所述秘密可以通过安全模块 150 发送到任何其他显示器（例如工作站 118），或以其他方式呈现予所述第二人员。

[0085] 所述第二人员接着执行一动作，包括（例如）将所述秘密送返安全模块 150、所述第一人员及 / 或控制设备 120。在有些范例中，所述第二人员通过所述安全模块的输入设备 234 输入一动作，以便将所述秘密送返所述秘密，这可以包括输入指令以便将所述秘密转发到所述第一人员。在有些范例中，所述秘密从所述第二人员发送到所述要求的一源（例如控制室 102 中的工作站 118），然后返回到控制设备 120。在所述秘密被送返时，或在确定所述第二人员执行一动作来授权一控制设备动作（流程块 708）时，安全模块 150 识别一动作已经获得授权以响应所述要求或命令，而安全模块 150 授权所述控制设备处理所述要求或命令（流程块 710）。控件接着返回到流程块 702，直到另一通信被接收为止。例如，如果在一预定时间数量之后，所述第二人员尚未送返所述秘密（流程块 708），控件返回到流程块 702，直到另一通信被接收为止。因此，流程块 708 可以包括的操作包括在一预定时间间隔之后的暂停。

[0086] 图 8 为一框图，其显示范例处理器系统 810，范例处理器系统 810 可以用于实施在此描述的设备及方法。例如，相似或相同于范例处理器系统 810 的处理器系统可以用于实施图 1 的工作站 118、控制设备 120、122 及 126a-c、输入 / 输出卡 140a-d 及 142a-d 及 / 或

安全模块 150-158。虽然以下描述范例处理器系统 810 包括多个外围设备、界面、芯片、存储器等等，但这些元件中的一个或多个元件可以从用于实施工作站 118、控制设备 120、122 及 126a-c、输入 / 输出卡 140a-d 及 142a-d 及 / 或安全模块 150-158 中的一个或多个省略。

[0087] 如图 8 中所示，处理器系统 810 包括处理器 812，该处理器 812 连接到一互连总线 814。处理器 812 包括一寄存器或寄存器空间 816，该寄存器或寄存器空间 816 在图 8 中被描绘成完全在线，但其可以选择性地完全或部分离线并通过专用电气连接及 / 或互连总线 814 直接地连接到处理器 812。处理器 812 可以是任何合适的处理器、处理单元或微处理器。虽然图 8 中未显示，但所述系统 810 可以是多处理器系统，因此，其可以包括一个或多个附加的、与所述处理器 812 相同或相似并通信连接到互连总线 814 的处理器。

[0088] 图 8 的处理器 812 连接到一芯片组 818，该芯片组 818 包括一存储器控制器 820 及一外围输入 / 输出控制器 822。广为人知的是，一芯片组典型地提供输入 / 输出及存储器管理功能以及多个通用及 / 或专用寄存器、定时器等等，这些设备可以由一个或多个连接到芯片组 818 的处理器存取或使用。存储器控制器 820 执行其功能，使得处理器 812（或多个处理器，如果有多个处理器）能够存取一系统存储器 824 及一大容量存储器 825。

[0089] 系统存储器 824 可以包括任何期望类别的易失性及 / 或非易失性存储器，例如静态随机存取存储器 (SRAM)、动态随机存取存储器 (DRAM)、闪速存储器、只读存储器 (ROM) 等等。大容量存储器 825 可以包括任何期望类别的大容量设备。例如，如果范例处理器系统 810 用于实施工作站 118（图 1），则大容量存储器 825 可以包括一硬盘驱动器、一光驱动器、一带存储器设备等等。可选择地，如果范例处理器系统 810 用于实施控制设备 120、122 及 126a-c、输入 / 输出卡 140a-d 及 142a-d 及 / 或安全模块 150-158，则大容量存储器 825 可以包括一固态存储器（例如闪速存储器、随机存取存储器 (RAM) 等等）、一磁存储器（例如硬盘）或任何其他适合在控制设备 120、122 及 126a-c、输入 / 输出卡 140a-d 及 142a-d 及 / 或安全模块 150-158 中实施大量存储的存储器。

[0090] 外围输入 / 输出控制器 822 执行其功能，使得处理器 812 能够通过一外围输入 / 输出总线 832、与外围输入 / 输出设备 826 及 828 以及一网络界面 830 进行通信。输入 / 输出设备 826 及 828 可以是任何期望类别的输入 / 输出设备，比如键盘、显示器（例如液晶显示器 (LCD)、阴极射线管 (CRT) 显示器等等）、导航设备（例如鼠标、跟踪球、电容式触控板、操纵杆控制器等等）等等。网络界面 830 可以是（例如）以太网设备、异步传输模式 (ATM) 设备、802.11 设备、数字用户线路 (DSL) 调制解调器、电缆调制解调器、蜂窝调制解调器等等，其使得处理器系统 810 能够与另一处理器系统进行通信。

[0091] 虽然存储器控制器 820 及输入 / 输出控制器 822 在图 8 中被描绘为芯片组 818 内的分别的功能块，但由这些块执行的功能可以在一个单一的半导体线路内集成，或可以使用两个或多个分别的集成电路来实施。

[0092] 在此描述的范例方法及系统方便地使一过程控制系统的操作员能够使用可以互换地连接到多个控制设备的多个安全模块。这使所述过程控制系统的操作员能够迅速及轻易地改变一控制设备的安全编程。例如，操作员可以将一控制设备的安全编程从一集合的安全功能、水平或特征改变为另一集合的安全功能、水平或特征，而所述另一集合的特征具有某些性能特性或其他好处对所述过程控制系统中的特定控制设备更为有利。此外，操作员可以以一经修改或升级的安全编程或在一控制设备原先制造时尚未存在的特定特征来

更新一控制设备。

[0093] 此外，包括在正式采用工业标准之前已经结合到所述过程控制系统的最先进的未公开设备及安全特征的一过程控制系统的操作员将能够将结合所述工业标准的、在此描述的范例安全模块的其中之一结合到所述未公开控制设备的其中之一，以便更新所述设备，从而符合适当的标准。

[0094] 以在此描述的范例安全模块实现的另一好处是，连接到一安全模块的控制设备可以改变，而所有所述安全特征、调用信息等等保持不变。此外，所述安全模块的有些范例可以包括诊断软件，所述诊断软件可以用于搜集来自所述控制设备的信息。操作员可以通过将所述安全模块改变为具有所期望的诊断软件的另一安全模块，存取更新、更好或更设备适当的诊断器件。例如，可以开发一新诊断测试，以便更好地评估一控制设备的一特定条件。有了在此描述的范例安全模块，所述新诊断测试可以在不需要改变所述控制设备或所述现有控制设备的电子线路板的情况下，实施在一固有的控制设备上。

[0095] 此外，控制设备的制造商可以将所述安全电子器件及软件及 / 或诊断电子器件及软件从所述控制设备的其余电子器件分离。因此，较少种类的用于所述控制设备的电路板需要开发、制造、库存等等。例如，如果一制造商在两个不同的安全编程中提供各五个控制设备，则将需要生产十个电路板（每个设备及协议组合用一个电路板）。使用在此描述的范例安全模块，将只需要生产五个电路板（每个设备用一个电路板）及两个类别的安全模块（每个编程用一个类别的安全模块），因此大大减少制造商的开发及存储成本。此外，所述安全模块可以与其他控制设备一起使用。

[0096] 此外，以上描述的关于图 5 的隔离电路保护连接到所述范例安全模块的电源及控制设备。如果发生刺波电流或因电工配线疏忽而导致不可接受的高电压或电流负荷，所述隔离电路促使所述安全模块吸收所述额外负荷。因此，只是所述安全模块可能需要替换，而所述控制设备的电路板将保持其功能，这大大地减少维护及修理成本。

[0097] 虽然在此已经描述某些方法、设备及制造件，但本专利包括的范围并未受其限制。相反地，本专利包括根据字面意义或等效原则正当地属于附此的权利要求范围的所有方法、设备及制造件。

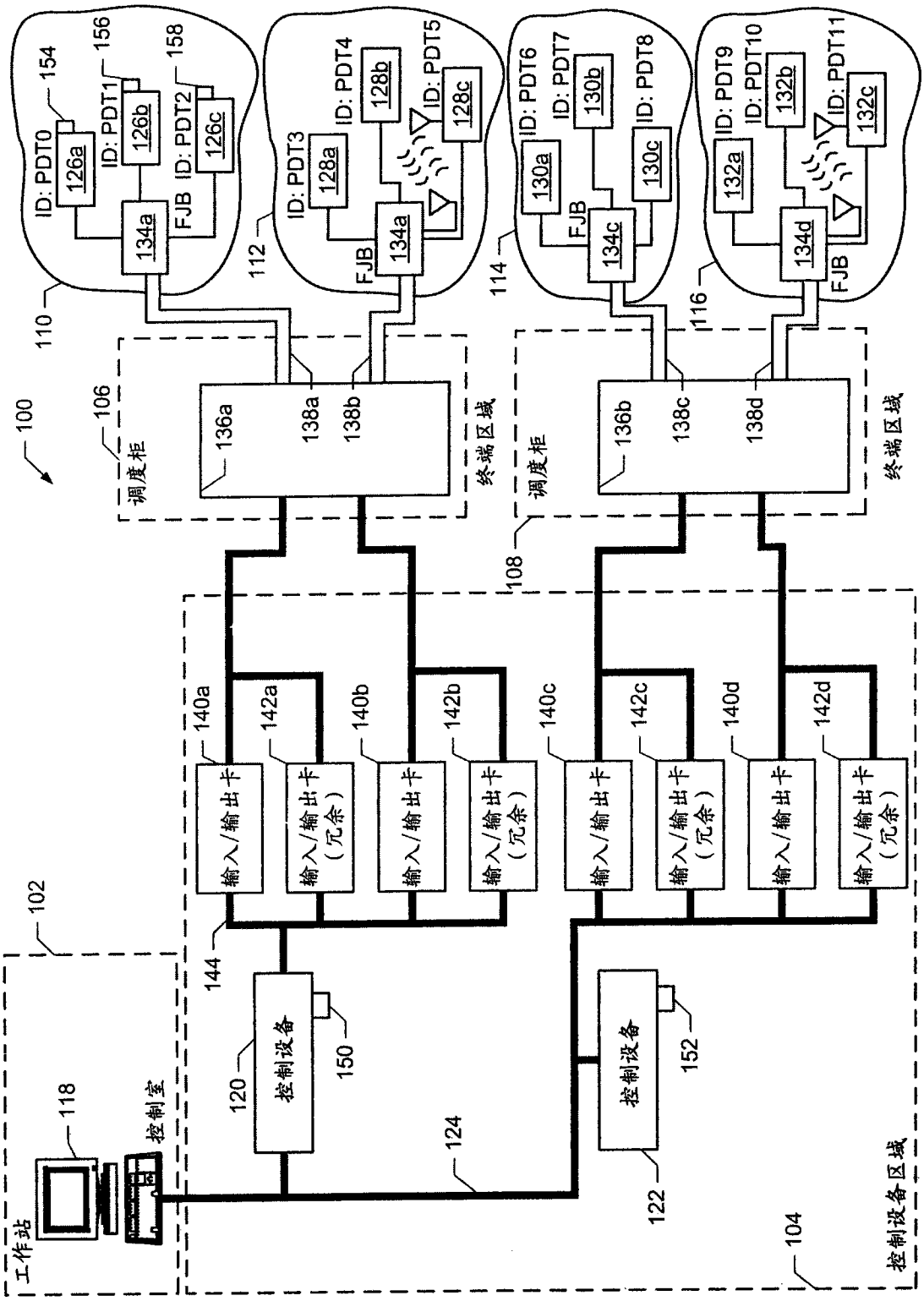

100
102
104
106
108
110
112
114
116
118
120
122
124
126a
126b
126c
128a
128b
128c
130a
130b
130c
132a
132b
132c
134a
134c
134d
136a
136b
138a
138b
138c
138d
140a
140b
140c
140d
142a
142b
142c
142d
144
150
152
154
156
158
ID: PDT0
ID: PDT1
ID: PDT2
ID: PDT3
ID: PDT4
ID: PDT5
ID: PDT6
ID: PDT7
ID: PDT8
ID: PDT9
ID: PDT10
ID: PDT11
FJB
调度柜
终端区域
输入/输出卡
输入/输出卡（冗余）
控制设备
控制室
工作站
控制设备区域

图 1

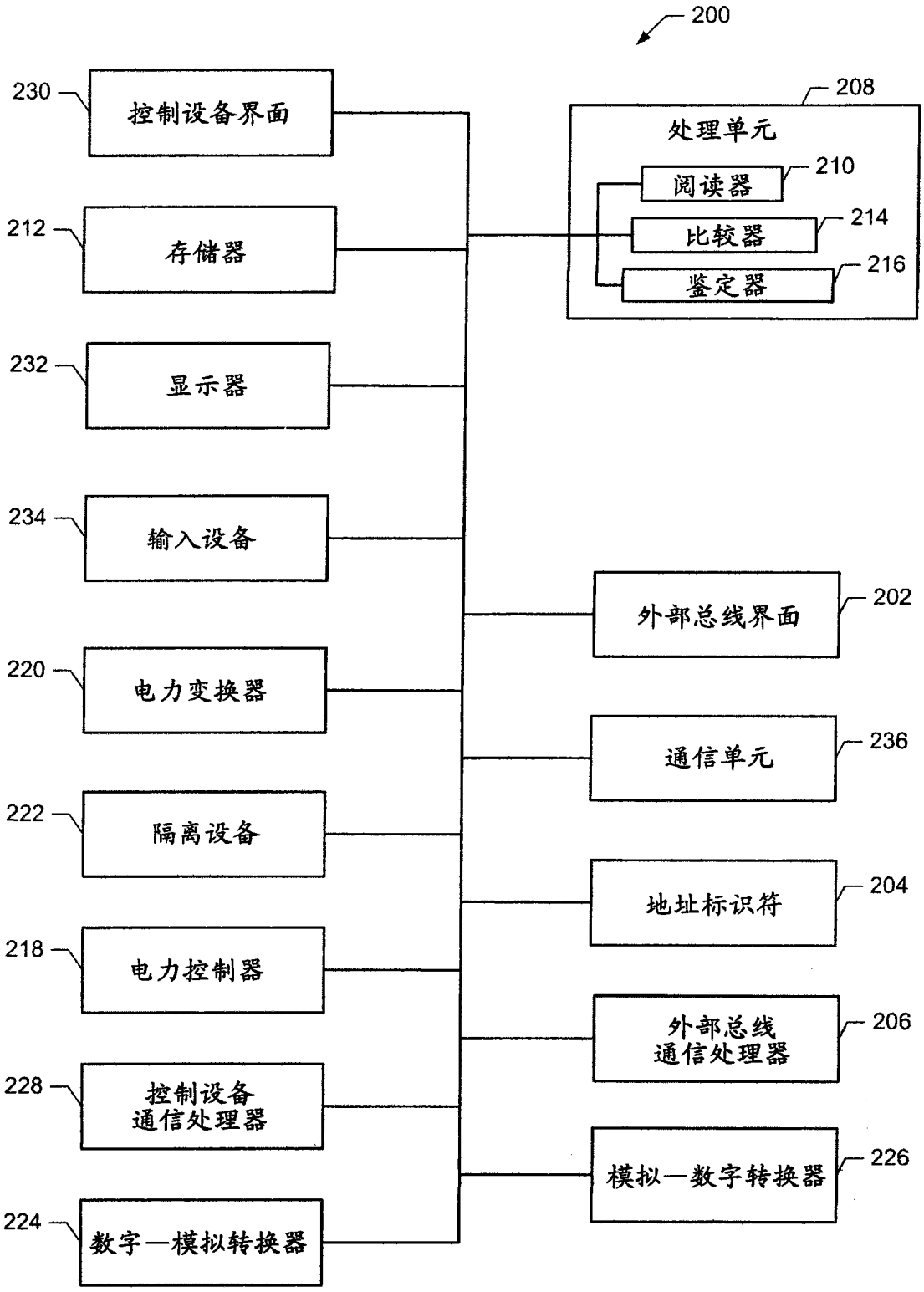

200
230
控制设备界面
208
处理单元
210
阅读器
214
比较器
216
鉴定器
212
存储器
232
显示器
234
输入设备
202
外部总线界面
220
电力变换器
236
通信单元
222
隔离设备
204
地址标识符
218
电力控制器
206
外部总线
通信处理器
228
控制设备
通信处理器
226
模拟—数字转换器
224
数字—模拟转换器

图 2

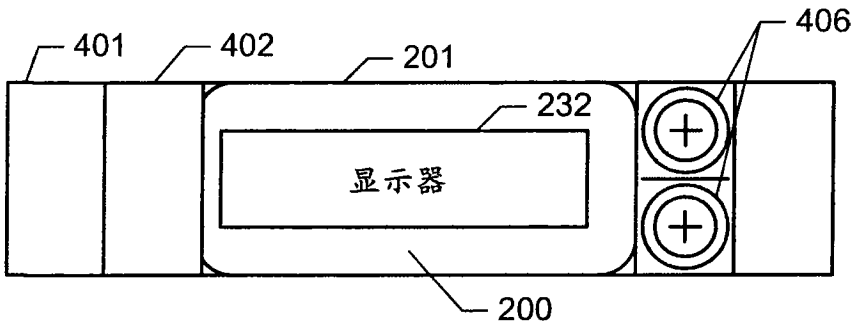


图 3

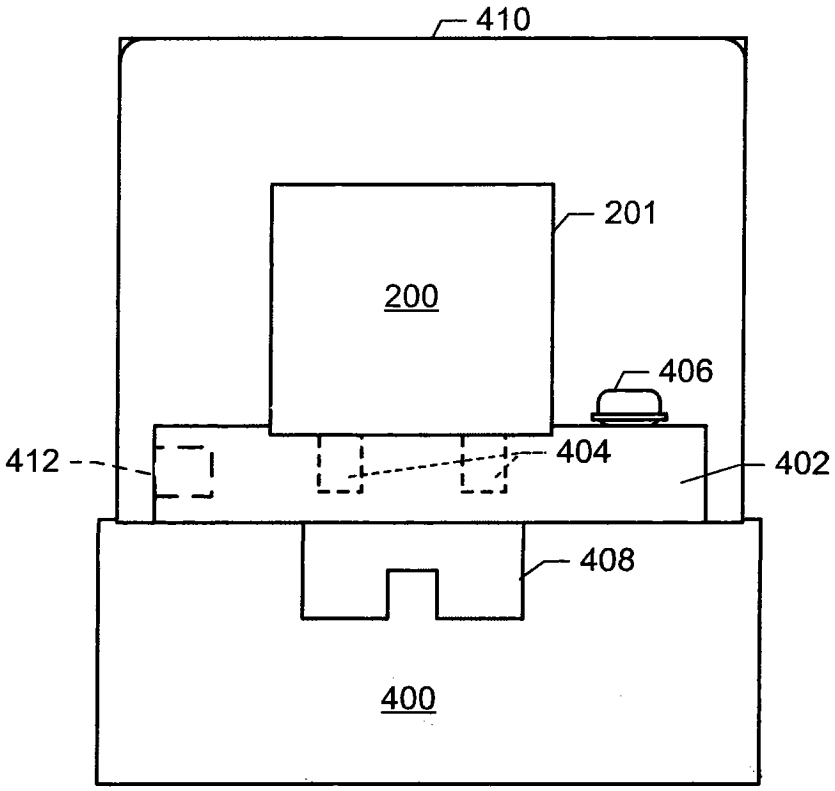


图 4

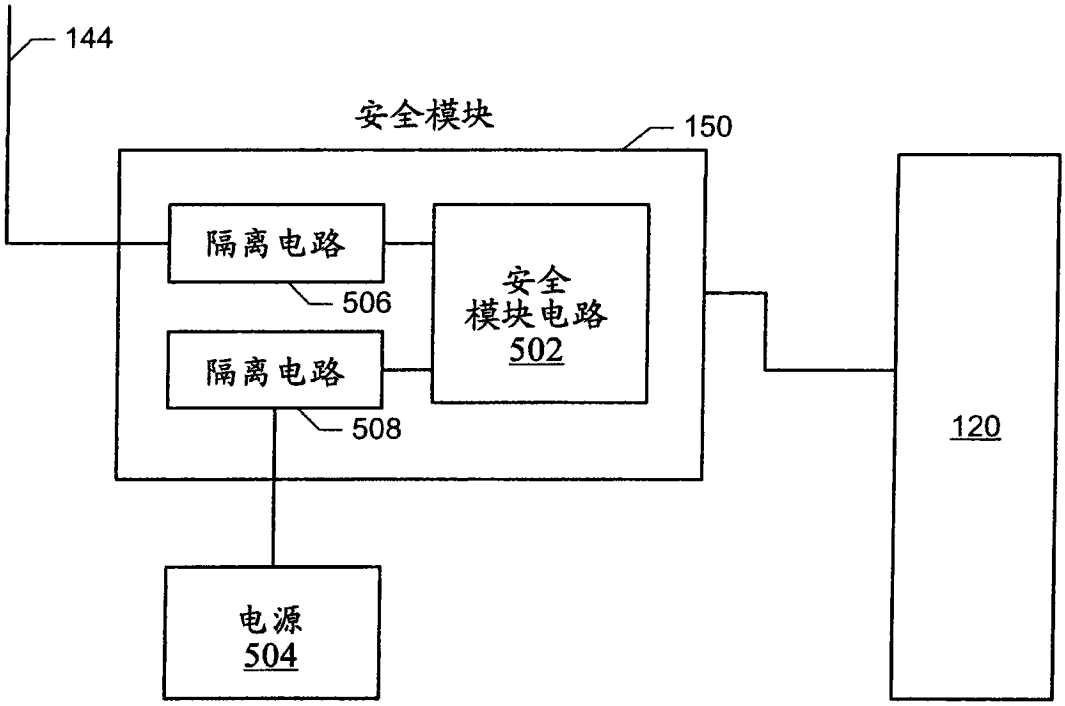


图 5

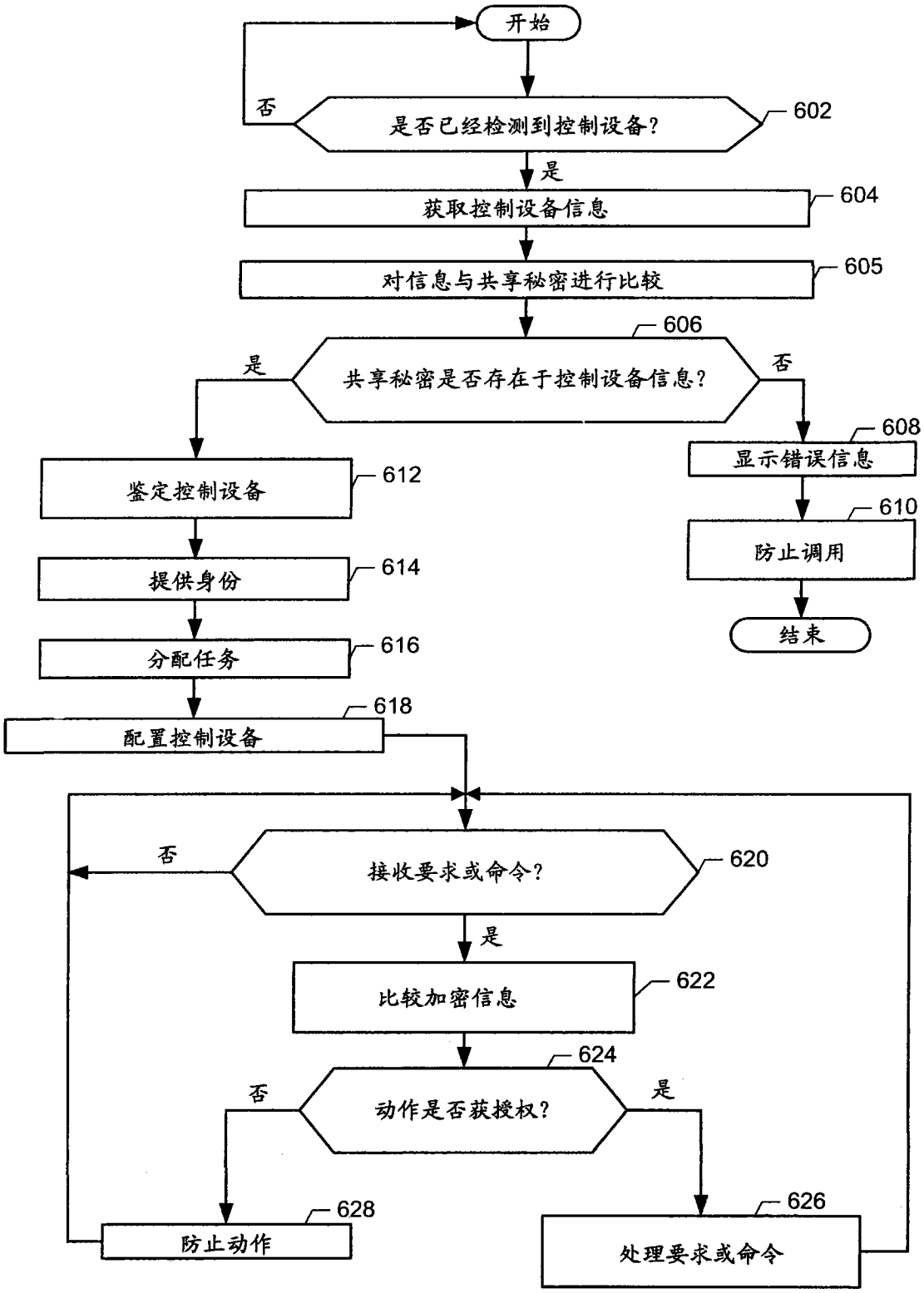

开始
是否已经检测到控制设备?
602
否
是
获取控制设备信息
604
对信息与共享秘密进行比较
605
606
共享秘密是否存在于控制设备信息?
是
否
鉴定控制设备
612
提供身份
614
分配任务
616
配置控制设备
618
显示错误信息
608
防止调用
610
结束
接收要求或命令?
620
否
是
比较加密信息
622
624
动作是否获授权?
否
是
防止动作
628
处理要求或命令
626

图 6

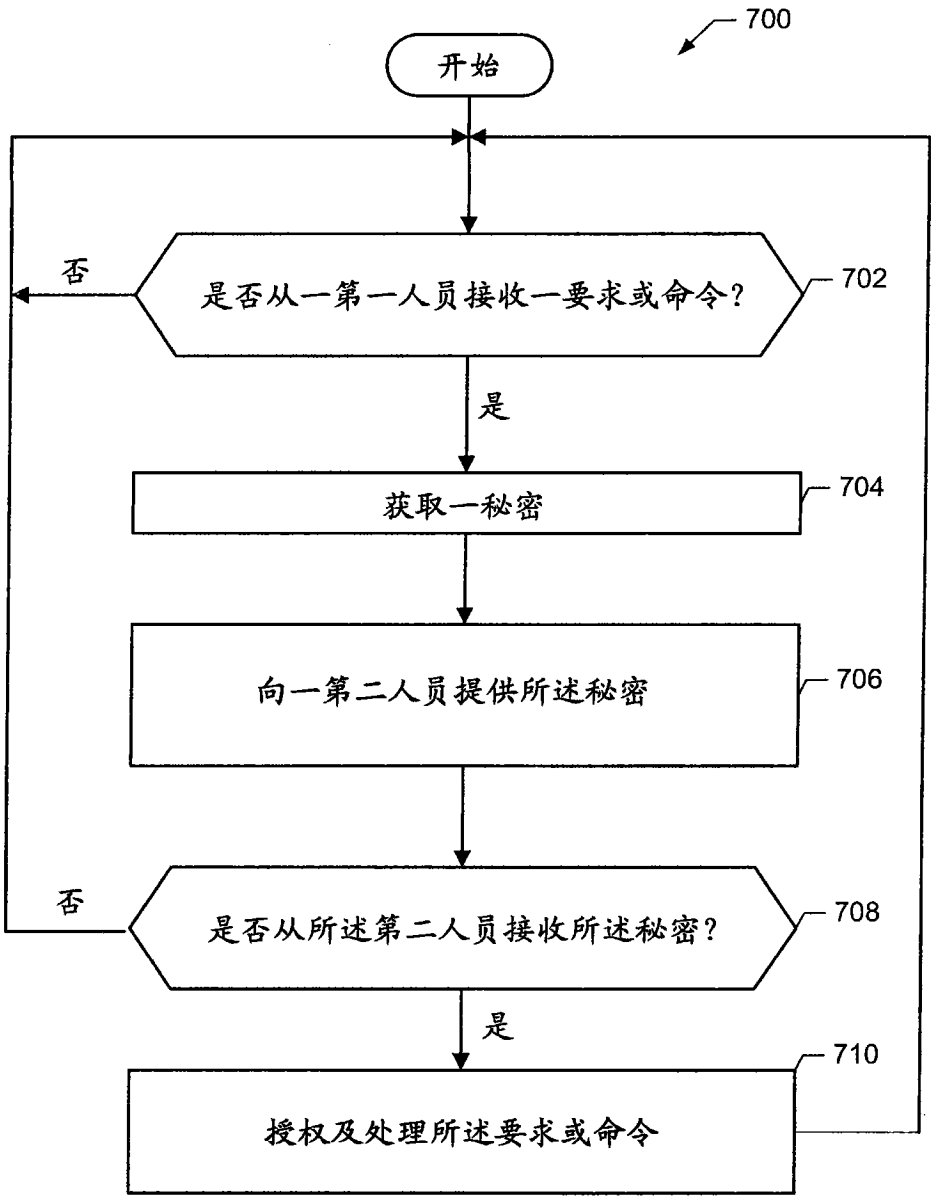

700
开始
是否从一第一人员接收一要求或命令?
否
702
是
获取一秘密
704
向一第二人员提供所述秘密
706
是否从所述第二人员接收所述秘密?
否
708
是
授权及处理所述要求或命令
710

图 7

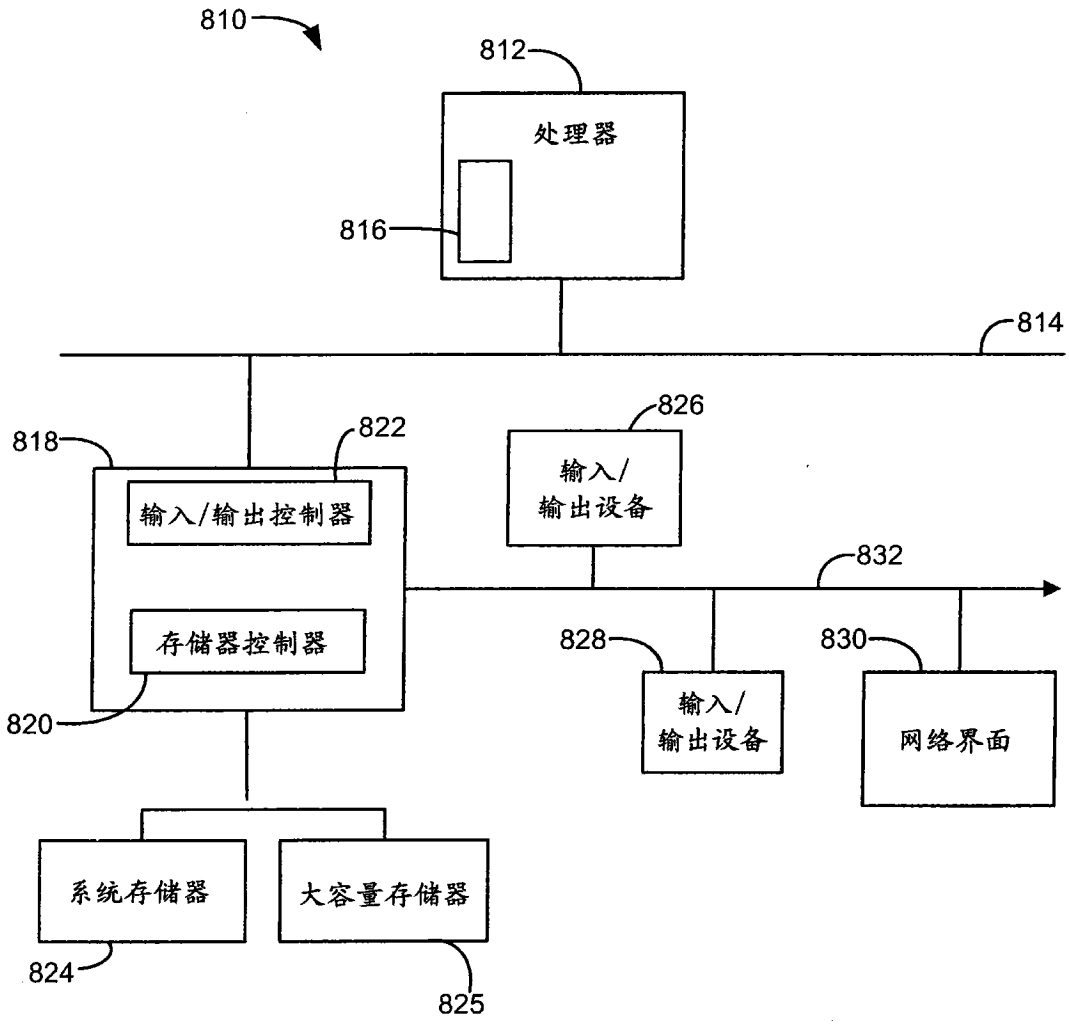

810
812
处理器
816
814
826
818
822
输入/
输出设备
输入/输出控制器
832
存储器控制器
828
830
820
输入/
输出设备
网络界面
系统存储器
大容量存储器
824
825

图 8