



(12) 发明专利

(10) 授权公告号 CN 101393430 B

(45) 授权公告日 2014. 04. 09

(21) 申请号 200810211401. 6

(22) 申请日 2008. 09. 18

(30) 优先权数据

11/857, 250 2007. 09. 18 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 大卫·马克·史密斯 布兰顿·希布
戴维·R·丹尼森
戈弗雷·R·谢里夫 加里·劳
凯尔·泰特迈耶

(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 19/02 (2006. 01)

G06F 9/445 (2006. 01)

(56) 对比文件

US 6501995 B1, 2002. 12. 31, 摘要、说明书第3栏第11-40行, 第5栏第26行至第7栏第64行、图 3A-3B.

US 5428769 A, 1995. 06. 27, 说明书第84栏第12-42段.

US 6501995 B1, 2002. 12. 31, 摘要、说明书第3栏第11-40行, 第5栏第26行至第7栏第64行、图 3A-3B.

US 7023795 B1, 2006. 04. 04, 全文.

CN 1169190 A, 1997. 12. 31, 全文.

US 6360363 B1, 2002. 03. 19, 全文.

US 4958270 A, 1990. 09. 18, 全文.

审查员 林峰

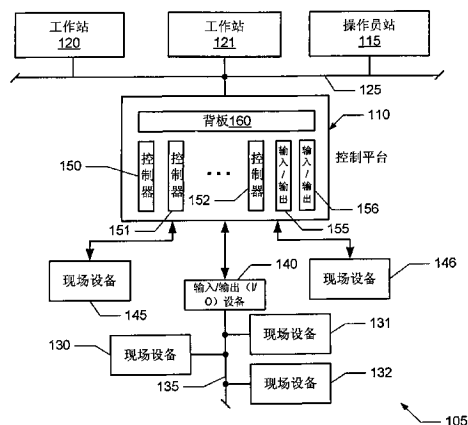
权利要求书2页 说明书10页 附图8页

(54) 发明名称

在过程设备中升级及提供控制冗余的方法及设备

(57) 摘要

本发明公开在过程设备中升级及提供控制冗余的方法及设备。所公开的一种升级过程控制系统的控制设备的软件的范例方法包括实例化所述软件的替代组件、将来自现有组件的状态数据复制到所述替代组件、以及在所述替代组件的第一状态与所述现有组件的第二状态匹配时将所述替代组件改变为主动模式。



1. 一种对过程进行控制的方法,其中在过程控制系统维持不间断过程操作的同时为过程控制系统的控制设备升级软件,所述方法包括:

执行所述控制设备中软件的现有组件,同时所述现有组件向所述过程控制系统中的不需要对所述现有组件的改变的第一控制算法发送输入;

实例化所述控制设备中软件的替代组件,其中所述替代组件向所述过程控制系统中的需要包含在所述替代组件中的改变的第二控制算法发送输入;

将来自所述现有组件的状态数据复制到所述替代组件,同时所述现有组件向所述过程控制系统的不需要包含在所述替代组件中的所述改变的所述第一控制算法发送输入;

在所述替代组件的第一状态与所述现有组件的第二状态匹配时,将所述替代组件改变为主动模式;以及

在第一过程控制应用程序与所述替代组件之间传送输入,其中输入继续在第二过程控制应用程序与所述现有组件之间传送,并且其中所述替代组件和所述现有组件同时执行。

2. 如权利要求1所述的方法,进一步包括在所述现有组件和所述替代组件同时发送输入之后的时间段,终止所述现有组件的执行。

3. 如权利要求1所述的方法,进一步包括在所述现有组件和所述替代组件同时发送输入之后的时间段,在所述第一过程控制应用程序与所述现有组件之间传送输入。

4. 如权利要求1所述的方法,其中所述替代组件被实例化为所述现有组件的冗余模块。

5. 如权利要求1所述的方法,其中所述替代组件由实时操作系统实例化为隔离过程。

6. 如权利要求1所述的方法,其中过程间通信用于复制所述状态数据。

7. 如权利要求6所述的方法,其中所述过程间通信包括可移植操作系统界面呼叫。

8. 如权利要求1所述的方法,进一步包括:

核验所述第一状态与所述第二状态匹配;以及

在所述第一状态与所述第二状态不匹配时复制附加状态数据。

9. 如权利要求1所述的方法,进一步包括在将所述替代组件改变为所述主动模式之前执行对所述替代组件的测试。

10. 如权利要求1所述的方法,其中所述软件升级在所述过程控制系统不遭受控制时间损失的情况下发生。

11. 如权利要求1所述的方法,其中所述替代组件包括一控制应用程序的一个子系统,及其中所述控制应用程序的其他子系统没有被升级。

12. 如权利要求1所述的方法,其中所述软件升级在没有使用另一控制设备的情况下发生。

13. 如权利要求1所述的方法,其中所述替代组件包括热修复。

14. 一种为过程控制系统的控制设备升级软件的设备:

实例化所述软件的替代组件的装置;

将来自现有组件的状态数据复制到所述替代组件的装置;

在所述替代组件的第一状态与所述现有组件的第二状态匹配时,将所述替代组件改变为主动模式的装置;

通过不需要包含在所述替代组件中的改变的第一控制算法继续使用所述现有组件的

装置 ; 以及

通过需要包含在所述替代组件中的所述改变的第二控制算法使用所述替代组件的装置。

15. 如权利要求 14 所述的为过程控制系统的控制设备升级软件的设备, 其中所述现有组件当前为主动。

16. 如权利要求 14 所述的为过程控制系统的控制设备升级软件的设备, 进一步包括终止所述现有组件的执行的装置。

17. 如权利要求 14 所述的为过程控制系统的控制设备升级软件的设备, 其中第一控制应用程序包括所述替代组件, 而第二控制应用程序继续包括所述现有组件。

18. 如权利要求 14 所述的为过程控制系统的控制设备升级软件的设备, 其中所述替代组件被实例化为所述现有组件的冗余模块。

19. 如权利要求 14 所述的为过程控制系统的控制设备升级软件的设备, 其中所述替代组件被实例化为实时操作系统的隔离过程。

20. 如权利要求 14 所述的为过程控制系统的控制设备升级软件的设备, 其中过程间通信用于复制所述状态数据。

21. 如权利要求 14 所述的为过程控制系统的控制设备升级软件的设备, 进一步包括 :
核验所述第一状态与所述第二状态匹配的装置 ; 以及
在所述第一状态与所述第二状态不匹配时复制附加状态数据的装置。

22. 如权利要求 14 所述的为过程控制系统的控制设备升级软件的设备, 进一步包括在将所述替代组件改变为所述主动模式之前执行对所述替代组件的测试的装置。

23. 如权利要求 14 所述的为过程控制系统的控制设备升级软件的设备, 其中所述软件升级在所述过程控制系统不遭受控制时间损失的情况下发生。

24. 如权利要求 14 所述的为过程控制系统的控制设备升级软件的设备, 其中所述替代组件包括一控制应用程序的一个子系统, 及其中所述控制应用程序的其他子系统没有被升级。

25. 如权利要求 14 所述的为过程控制系统的控制设备升级软件的设备, 其中所述软件的升级在没有使用另一控制设备的情况下执行。

在过程设备中升级及提供控制冗余的方法及设备

技术领域

[0001] 本公开总体上涉及过程设备,尤其涉及在过程设备中升级及提供控制冗余的方法及设备。

背景技术

[0002] 分布式过程控制系统—如那些用于化学、石油及/或其他过程、系统及/或过程设备的过程控制系统—典型地包括一个或多个过程控制器,过程控制器通过多种模拟总线、数字总线或模拟/数字混合总线的其中任何一种总线,与一个或多个现场设备通信连接。在这些系统及/或过程中,现场设备—例如阀、阀定位器、开关及/或传送器(例如温度传感器、压力传感器、料位传感器及流率传感器)—在所述过程环境内执行过程控制及/或管理功能,比如开启或关闭阀、测量过程参数等等。过程控制器也可以位于所述设备环境,它们接收指示由所述现场设备完成的过程测量的信号及/或其他与所述现场设备有关的信息。根据(例如)所接收的信号,所述过程控制器执行控制器应用程序,以实现任何数目及/或类别的控制模块、软件模块、软件子系统、例程及/或软件线程,从而发动告警、做出过程控制决定、产生控制信号、及/或与其他控制模块、及/或其他由现场设备执行的控制模块及/或功能块(比如 HART 及 Foundation Fieldbus 设备)协作。所述控制器中的所述控制模块通过所述通信线,向所述现场设备发送所述控制信号,以控制所述过程设备的操作。

[0003] 来自所述现场设备及/或所述控制器的信息通常通过数据高速通道或通信网络传送到一个或多个其他硬件设备,比如操作员工作站、个人计算机、历史数据库、报告产生器、集中式数据库等等。这些设备典型地位于控制室及/或位于相对远离苛刻过程环境的其他位置。例如,这些硬件设备运行应用程序,以使得操作员能够执行与过程设备的过程有关的多种功能中的任何功能,比如改变操作状态、改变所述控制例程的设置、更改所述控制器及/或所述现场设备内的所述控制模块的操作、检视所述过程的目前状态、检视由所述现场设备及/或过程控制器产生的告警、模拟所述过程的操作以供培训人员及/或测试所述过程控制软件、维持及/或更新配置数据库等等。

[0004] 作为一个例子,由费舍—柔斯芒特系统股份有限公司(Fisher Rosemount System, Inc.)—一家艾默生过程控制(Emerson Process Management)公司出售的DeltaV™数字自动化系统支持存储在位于过程设备内的潜在多变化的位置的不同设备内、及/或由位于过程设备内的潜在多变化的位置的不同设备执行的多个应用程序。位于一个或多个操作员工作站及/或由一个或多个操作员工作站执行的配置应用程序,使得用户能够创建及/或更改过程控制应用程序、及/或通过数据高速通道或通信网络将过程控制应用程序下载到专用分布式控制器。典型地,这些控制应用程序是由通信连接及/或互连的控制模块、软件模块、软件子系统、例程、软件线程及/或功能块构成,功能块根据所接收的输入,在所述控制方案内执行功能(例如过程控制及/或告警产生),及/或提供输出到所述控制方案内的其他功能块。所述配置应用程序也可以允许配置工程师及/或操作员创建及/或改变操作员界面,这些操作员界面(例如)由(例如)显示应用程序用于为操作员显示数据及/或用于

使所述操作员能够在所述过程控制例程中改变设置,比如改变设定点及/或操作状态。每个专用控制器(及在某些情况下还包括现场设备)存储及/或执行一个控制器应用程序,以运行被指定执行实际过程控制功能的所述控制模块。

发明内容

[0005] 本发明公开在过程设备中升级及提供控制冗余的方法及设备。所公开的一种用于为过程控制系统的控制设备升级软件的范例方法包括实例化所述软件的替代组件、将来自现有组件的状态数据复制到所述替代组件、以及在所述替代组件的第一状态与所述现有组件的第二状态匹配时将所述替代组件改变为主动模式。

[0006] 另一种公开的为过程设备控制系统提供控制冗余的范例方法包括提供控制输入到控制软件子系统的第一实例及控制软件子系统的第二实例,所述第一及第二实例充分同时地处理所述控制输入,并提供所述第一实例的输出或是所述第二实例的输出到过程设备现场设备。

附图说明

[0007] 图 1 为一原理图,其图解根据本发明的教导来建造的一种范例过程控制系统。

[0008] 图 2 图解实施图 1 的任何范例控制器或所有范例控制器的一种范例方法。

[0009] 图 3 及 4 图解用于图 1 的过程控制系统的范例冗余控制方案。

[0010] 图 5 为一流程图,其显示一范例过程,该范例过程可以用于实施所述范例冗余控制器及/或(更概括地)可以用于实施图 1 及/或 2 的任何范例控制器或所有范例控制器。

[0011] 图 6 为一流程图,其显示一范例过程,该范例过程可以用于实施图 2 的范例升级模块,以便升级图 2 的任何范例控制组件或所有范例控制组件。

[0012] 图 7A、7B、7C 及 7D 图解一范例过程,该范例过程可以实施来升级图 2 的任何范例控制组件或所有范例控制组件。

[0013] 图 8A 及 8B 图解一范例控制系统,该范例控制系统操作控制组件的两个版本。

[0014] 图 9 为一原理图,其图解一范例处理器平台,该范例处理器平台可以用于及/或编程为执行图 5、6 及/或 7A-7D 的范例过程,及(更概括地)可以用于实施图 1 及/或 2 的任何范例控制器或所有范例控制器。

具体实施方式

[0015] 现代的过程控制系统为过程设备的运行进行一天二十四小时、一年三百六十五天的工作。持续运行的过程设备的控制引致需要有效率及/或灵活的机制来升级控制设备的固件。这样的控制设备升级需要使控制设备停工期最小化及/或充分地消除设备操作中断。传统上,一直采用冗余控制设备来升级控制设备,以减低不可使用期。传统的程序升级整个备用控制设备、允许所述备用设备由主动设备配置、执行转换为所述备用设备、然后升级新的备用设备(即先前的主动设备)。

[0016] 一般上,在此描述的范例设备、方法及制造件可以用于减低及/或消除对冗余控制设备的需要,以便在控制设备升级期间提供不间断的过程设备操作。明确地说,所述控制设备及/或控制算法的功能被隔离、分离及/或分散为单独的组件(例如软件模块及/或

软件子系统),这使每个组件能够独立地升级。通过使用单独的组件,控制设备可以在逐一特性、逐一组件的基础上升级,及/或可以在不影响其他主动组件、所述控制设备及/或过程控制系统的部分的情况下升级,以解决特定组件中存在的问题。为了升级特定组件,替代组件在当前执行需要升级的特定组件的控制设备中实例化。通过使所述控制组件能够将运行时间及/或状态数据转换为所述相同的组件的其他版本,升级期间的不可利用期被消除。这样的智能允许现有组件在其将关键数据传输到其替代组件时可继续执行其功能。一旦所述新组件的状态被更新,所述替代组件以与原组件的状态信息相同的状态信息接管操作。通过促进特定组件的升级,对全部冗余控制设备的需要得以充分消除。此外,处理器控制器可以执行同一组件的多个版本。

[0017] 在有些范例中,控制设备包括及/或实施主升级模块,以便从用户接收更新的组件固件。所述升级模块通过创建所述替代组件的实例来安装所述新组件,并在所述替代组件及其需替代的组件之间启动数据更新。在更新完成之后,所述替代组件配置成主动模式,而所述旧组件可以终止。

[0018] 从事件(比如软件故障、硬件故障)快速恢复及/或在软件更新期间继续操作非常重要。传统上,过程控制系统一直试图通过使用专用的冗余控制设备来提供连续的控制操作。所述控制设备的冗余拷贝配置成模拟所述主动运行的控制设备的当前状态。在所述主动运行的设备(因一种或多种原因)不再能够完成其任务时,所述备用设备接管并运行所述主动运行的设备被分配的所有任务。然而,难以确保无缝及/或无扰的失效转移,这是由于无缝及/或无扰的失效转移需要所述备用设备不断地与来自所述主动运行设备的过程数据及/或状态信息同步。这个方法经常导致在多个时期不能利用所述备用设备来替代所述主动设备。

[0019] 一般上,通过允许在所述过程控制系统中分布冗余,在此描述的范例设备、方法及制造件可以用于替代对专用冗余控制设备的需要。使用分布方法,冗余操作利用其他主动控制设备的免费资源及/或所述主动控制设备本身中的免费资源来实施。实质上,所有控制组件被视为主动,因而拥有当前的过程数据及状态信息。

[0020] 在有些范例中,相同类别的多个控制组件同时执行,而每个控制组件执行一主动控制组件的动作。来自所有组件的输出被引导到网关,该网关使用表决算法来确定来自哪个控制组件的哪个输出将被传送到所述现场设备。在其他范例中,所述控制组件交换输出并共同地确定传送哪个输出到所述现场设备。

[0021] 如在此所述,相同类别的所述多个控制组件可以在相同的控制设备、处理器及/或控制器上执行及/或实施,及/或可以在两个或多个控制设备、处理器及/或控制器上实施。可以根据可利用的控制设备、处理器及/或控制器的处理负荷及/或数目,动态地确定控制组件在控制设备、处理器及/或控制器上的分配。此外,分配可以随着可利用的控制设备、处理器及/或控制器的处理负荷及/或数目的改变而改变。

[0022] 如在此所述,基于控制组件(而不是基于控制设备)来实施过程设备控制冗余降低硬件成本,并提供附加的冗余路径,而且实现较快的故障恢复及/或消除不可利用过程控制的时期。

[0023] 虽然在此描述的方法及设备通过允许在过程控制系统中分布冗余来替代对专用冗余控制设备的需要及/或减少及/或消除对冗余控制设备的需要,以便在控制设备升级

期间提供不间断的过程设备操作,但本领域的普通工程技术人员将可以理解,所述范例方法及设备可以用于为其他系统(比如过程设备的安全仪表化系统)实施冗余及/或执行升级。

[0024] 图 1 为一原理图,其图解一范例过程控制系统 105。图 1 的范例过程控制系统 105 包括一个或多个过程控制平台(其中一个过程控制平台以参考数字 110 标志)、一个或多个操作员站(其中一个操作员站以参考数字 115 标志)以及一个或多个工作站(其中两个工作站以参考数字 120 及 121 标志)。范例过程控制平台 110、范例操作员站 115 以及工作站 120 通过总线及/或局域网(LAN)125 通信连接,局域网(LAN)125 一般称为“应用程序控制网络”(ACN)。

[0025] 图 1 的范例工作站 120 及 121 可以配置成应用程序站,以执行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。例如,应用程序站 120 可以配置成主要执行过程控制相关的应用程序,而另一应用程序站 121 可以配置成主要执行通信应用程序,使过程控制系统 105 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)与其他设备或系统通信。操作员站 115 及工作站 120 及 121 可以使用一个或多个工作站及/或任何其他合适的计算机系统及/或处理系统来实施。例如,操作员站 115 及/或工作站 120 及 121 可以使用单处理器个人计算机、单处理器工作站或多处理器工作站等来实施。

[0026] 图 1 的范例局域网(LAN)125 可以使用任何期望的通信媒介及协议来实施。例如,范例局域网(LAN)125 可以基于固定及/或无线以太网(Ethernet)通信方案。然而,本领域的普通工程技术人员将可以理解,可以使用任何其他合适的通信媒介及/或协议。此外,虽然图 1 中图解单一局域网(LAN)125,但可以使用超过一个局域网(LAN)及/或其他替代性的通信硬件,在图 1 的范例系统之间提供冗余通信路径。

[0027] 图 1 的范例控制平台 110 通过数字数据总线 135 及输入/输出(I/O)设备 140,连接到多个智能现场设备 130、131 及 132。智能现场设备 130-132 可以是遵守 Fieldbus 协议的阀、促动器、传感器等等,在这种情况下,智能现场设备 130-132 使用广为人知的 Foundation Fieldbus 协议,通过数字数据总线 135 进行通信。当然,也可以改为使用其他类别的智能现场设备及通信协议。例如,智能现场设备 130-132 可以改为遵守 Profibus 及/或 HART 协议的设备,这些设备使用广为人知的 Profibus 及 HART 协议,通过数据总线 135 进行通信。附加的输入/输出(I/O)设备(与输入/输出(I/O)设备 140 相似及/或相同)可以连接到控制平台 110,以使附加的智能现场设备组群(其可以是 Foundation Fieldbus 设备、HART 设备等等)能够与控制平台 110 通信。

[0028] 除了范例智能现场设备 130-132 之外,一个或多个非智能现场设备 145 及 146 可以通信连接到范例控制平台 110。图 1 的非智能现场设备 145 及 146(例如)可以是传统 4-20mA(毫安培)或 0-10VDC(伏特直流电)设备,它们通过各自的固定链路与控制平台 110 通信。

[0029] 图 1 的范例控制平台 110 可以是(例如)由费舍—柔斯芒特系统股份有限公司(Fisher Rosemount System, Inc.)——一家艾默生过程控制(Emerson Process Management)公司出售的 DeltaV™ 控制器。然而,可以改为使用其他控制器。此外,虽然图 1 中只是显示一个控制平台 110,但任何期望类别及/或多类别的结合的附加控制平台及/或控制器可以

连接到局域网 (LAN) 125。无论那种情况, 范例控制平台 110 执行已经由使用操作员站 115 的系统工程师及 / 或其他系统操作员产生的、与过程控制系统 105 相关的、以及已经下载到控制平台 110 及 / 或在控制平台 110 中实例化的一个或多个过程控制例程。

[0030] 为了执行一个或多个控制算法, 图 1 的范例控制平台 110 包括一个或多个控制器 (即控制设备) (其中三个控制器以参考数字 150、151 及 152 标志)。图 2 的范例控制器 150、151 及 152 包含一个或多个处理器 (即控制设备), 以执行一个或多个操作系统、控制算法、控制组件及 / 或软件子系统。如在此采用的定义一样, “控制设备”一词指的是控制器 (例如范例控制器 150、151 及 152 中的任何一个) 及 / 或处理器、中央处理器 (CPU) 及 / 或控制器的处理器芯核。为了方便讨论, 以下公开涉及使用控制器以促进控制组件的冗余及 / 或升级。然而, 在此描述的方法及设备可以基于及 / 或应用于任何类别的控制设备 (例如处理器、中央处理器 (CPU) 及 / 或控制器的处理器芯核)。如以下更详细描述的那样, 范例控制器 150-152 在不需要显式冗余及 / 或备用控制器的情况下促进控制组件的冗余及 / 或升级。由范例控制器 150-152 执行的控制算法被隔离、分离及 / 或分散为单独的组件 (例如软件模块及 / 或软件子系统), 以使每个组件能够独立地升级。以下连同图 2 描述用于实施图 1 的范例控制器 150-152 中的任何范例控制器或所有范例控制器的范例方法。

[0031] 图 1 的范例控制器 150-152 包括及 / 或实施主升级模块, 以允许由一控制器 150-152 执行的每个控制组件独立地升级。为了升级特定组件, 替代组件在当前执行需要升级的特定组件的控制器 150-152 中实例化。通过使所述控制组件能够将运行时间及 / 或状态数据转换为所述相同的组件的其他版本, 升级期间的不可利用期被消除。这样的智能现有组件在其将关键数据传输到其替代组件时可继续执行其功能。一旦所述新组件的状态被更新, 所述替代组件以与原组件的状态信息相同的状态信息接管操作。如以下连同图 8A 及 8B 进行描述的那样, 一控制器 150-152 可以附加地或可选择地执行相同组件的多个版本。

[0032] 相同的控制组件的多个拷贝可以由相同的及 / 或不同的控制器 150-152 执行, 以便为图 1 的范例过程控制系统 105 实施控制冗余。所述控制组件拷贝可以由相同的控制器 150-152、由不同的控制器 150-152 及 / 或由不同的控制平台 110 执行。如以下连同图 3 进行描述的那样, 相同的控制组件的每个所述拷贝接收来自现场设备 130-132、145 及 / 或 146 的相同输入, 并执行相同的软件子系统。所述控制组件的所述输出可以接着用于 (例如进行比较) 确定传送哪个输出到现场设备 130-132、145 及 / 或 146。例如, 多数表决可以由输入 / 输出 (I/O) 网关 (例如范例输入 / 输出 (I/O) 网关 155 及 / 或 156 的其中之一) 执行, 以确定应传送哪个输出到现场设备 130-132、145 及 / 或 146。附加地或可选择地, 所述控制组件拷贝可以交换输出并共同地确定应传送哪个输出到现场设备 130-132、145 及 / 或 146。

[0033] 为了将范例控制器 150-152 通信连接到现场设备 130-132、145 及 / 或 146 及 / 或输入 / 输出 (I/O) 设备 140, 图 1 的范例控制平台 110 包括一个或多个输入 / 输出 (I/O) 模块及 / 或网关 (其中两个输入 / 输出 (I/O) 模块及 / 或网关以参考数字 155 及 156 标志)。图 1 的范例输入 / 输出 (I/O) 网关 155 及 156 配置成在控制器 150-152 与现场设备 130-132、145 及 / 或 146 季节 / 或输入 / 输出 (I/O) 设备 140 发送数据。范例控制器 150-152 及范例输入 / 输出 (I/O) 网关 155 及 156 通过任何类别的背板 160, 在控制平台 110 中通信连接。如图 1 所示, 范例控制平台 110 实施为架子及 / 或搁板, 而范例控制器 150-152 及输入

/ 输出 (I/O) 网关 155 及 156 为卡片及 / 或模块, 输入 / 输出 (I/O) 网关 155 及 156 在被插入搁板及 / 或架子时通信连接到背板 160。附加地或可选择地, 控制器 150-152 及输入 / 输出 (I/O) 网关 155 及 156 单独地实施, 并通过局域网 (LAN) 125 通信连接。

[0034] 虽然图 1 图解的范例过程控制系统 105 (其中所述方法及设备在过程设备中升级及提供控制冗余) (以下将进行更详细描述) 可以方便地使用, 但本领域的普通工程技术人员将可以理解, 如果需要, 在此描述的在过程设备中升级及提供控制冗余的方法及设备可以方便地用于复杂性比图 1 的图解范例高或低 (例如具有超过一个控制平台) 的其他过程设备及 / 或过程控制系统。

[0035] 图 2 图解实施图 1 的任何范例控制器 150-152 或所有范例控制器 150-152 的一种范例方法。虽然图 1 的任何范例控制器 150-152 或所有范例控制器 150-152 可以以图 2 的设备表示, 但为了方便讨论, 图 2 的设备将称为控制器 150。图 2 的范例控制器 150 包括至少一个通用可编程处理器 205。图 2 的范例处理器 205 执行存在于处理器 205 的主存储器 210 中 (例如在随机存取存储器 (RAM) 及 / 或只读存储器 (ROM) 中) 的编码指令。处理器 205 可以是任何类别的处理单元, 比如处理器芯核、处理器及 / 或微控制器。处理器 205 除了执行别的以外, 还可以执行实时操作系统 (RTOS) 215、升级模块 220、冗余控制器 225 及 / 或一个或多个控制组件 230。范例实时操作系统 (RTOS) 215 是来自 QNX 软件系统有限公司 (QNX Software Systems Ltd.) 的 QNX™ 实时操作系统 (RTOS)。图 2 的范例主存储器 210 可以由处理器 205 实施及 / 或在处理器 205 中实施, 及 / 或范例主存储器 210 可以是电气连接到处理器 205 的一个或多个存储器及 / 或存储器设备。

[0036] 如以下连同图 7A-D 进行描述的那样, 图 2 的范例升级模块 220 控制一个或多个范例控制组件 230 的升级。如以下连同图 8A-B 进行描述的那样, 范例升级模块 220 可以附加地或可选择地控制一控制算法及 / 或控制组件 (例如软件子系统) 的不同版本的同时及 / 或并行执行。

[0037] 如以下连同图 3-5 进行描述的那样, 图 2 的范例冗余控制器 225 控制及 / 或选择传送给来自一集合的控制组件拷贝的哪个输出到现场设备 130-132、145 及 / 或 146。附加地或可选择地, 冗余控制器 225 确定哪个控制组件拷贝作为特定控制组件的主控制组件拷贝。虽然图 2 显示范例冗余控制器 225 与控制组件 230 分离, 但每个所述控制组件可以包括及 / 或实施一冗余控制器。

[0038] 图 2 的范例控制组件 230 实施及 / 或执行控制算法的全部或部分 (例如软件子系统)。范例控制组件 230 接收来自一个或多个现场设备 130-132、145 及 / 或 146 及 / 或另一控制组件 230 的输入, 并处理所述输入以构成 (例如计算) 一个或多个输出。所述输出可以导引到另一控制组件 230 (例如以执行控制算法的一个或多个步骤) 及 / 或导引到一个或多个现场设备 130-132、145 及 / 或 146。

[0039] 为了存储控制算法及 / 或控制组件 (例如软件子系统) 的图像 240, 图 2 的范例控制器 150 包括非易失性存储器 235。图 2 的范例非易失性存储器 235 存储一个或多个控制组件的图像 240。除了存储当前由处理器 205 执行的控制组件的图像 240 之外, 范例存储器 235 可以存储可以由处理器 205 执行的其他控制组件的图像 240。虽然图 2 图解范例存储器 235 与特定控制器 150 相关, 但存储器 235 可以存储于一集合的控制器 (例如图 1 的范例控制器 150-152)。存储器 235 可以由任何数目及 / 或类别的存储器及 / 或存储器设备实

施。

[0040] 为了与背板（例如图 1 的范例背板 160）通信，图 2 的范例控制器 150 包括背板界面 245。图 2 的范例背板界面 245 将范例处理器 205 电气地及 / 或通信地连接到控制平台（例如范例控制平台 110）的背板，而控制器 150 插入所述背板。

[0041] 虽然图 2 图解实施图 1 的任何范例控制器 150-152 或所有范例控制器 150-152 的一种范例方法，但图 2 中所图解的数据结构、元件、过程及设备可以结合、分开、省略、排除及 / 或以任何其他方式实施。此外，范例实时操作系统 (RTOS) 215、范例升级模块 220、范例冗余控制器 225、范例控制组件 230 及 / 或（更概括地）图 2 的范例控制器 150 可以由硬件、软件、固件及 / 或硬件、软件及 / 或固件的任何组合实施。此外，范例控制器 150 可以包括图 2 中图解者之外的附加的元件、过程及 / 或设备，或除了包括图 2 中图解者外，还可以包括附加的元件、过程及 / 或设备，及 / 或可以包括图解的任何或所有数据结构、元件、过程及设备中的数目多于一个的数据结构、元件、过程及设备。

[0042] 图 3 及 4 图解用于图 1 的过程控制系统 105 的范例冗余控制方案。在图 3 的图解范例中，来自一个或多个现场设备（例如图 1 的现场设备 130-132、145 及 / 或 146）及 / 或来自控制算法及 / 或控制组件的输入 305 被提供于特定控制组件（其中三个控制组件以参考数字 310、311 及 312 标示）的两个或多个拷贝。图 3 的范例控制组件 310-312 实施控制算法的全部或一部分（例如控制算法的软件子系统）。范例控制组件 310-312 可以由一个或多个控制器（例如图 1 的一个或多个范例控制器 150-152）来实施及 / 或执行。例如，所有控制组件 310-312 可以由一单一控制器执行，控制组件 310-312 中的每个控制组件可以由不同的控制器执行等等。控制组件 310-312 在控制器中的分配可以是静态及 / 或动态的。如果所述分配是动态的，所述分配可以（例如）根据可利用的控制器数目及 / 或所述可利用的控制器的当前及 / 或历史处理负荷来调整。此外，特定控制组件的冗余拷贝的数目可以是静态及 / 或动态的，例如视所述控制组件的相对重要性、可利用的控制器数目及 / 或所述可利用的控制器的当前及 / 或历史处理负荷而定。以下连同图 4 描述将不同控制组件（例如软件子系统）的冗余拷贝分配到不同控制器。

[0043] 图 3 的范例控制组件 310-312 实施及 / 或执行所述相同的软件子系统。在所有控制组件 310-312 适当地操作时（例如没有任何错误），所有控制组件 310-312 的输出 315 相同。在控制组件 310-312 的特定其中之一已经失效、正在失效、正在经历错误情况等等时，其输出 315 可能不同于其他控制组件 310-312 的输出 315。检测输出 315 的这种差异及 / 或输出 315 的不存在，可以从而识别已经失效、正在失效及 / 或发生错误的控制组件 310-312。

[0044] 在图 3 的图解范例中，主组件 320 配置成检测这样的已失效、正在失效及 / 或发生错误的控制组件、选择哪个控制组件 310-312 的哪个（些）输出 315 需传送到现场设备及 / 或相同及 / 或不同控制算法的另一控制组件。图 3 的范例主组件 320 可以是中央处理器、控制器及 / 或软件子系统，其专用于执行多数表决，从而检测已经失效、正在失效及 / 或发生错误的控制组件 310-312 及 / 或选择传送哪个（些）输出 315 到所述现场设备。附加地或可选择地，范例主组件 320 可以动态地选自控制组件 310-312。换句话说，控制组件 310-312 中的每个控制组件包括担当该控制组件的主组件 320 所需要的逻辑。在这样的范例中，范例控制组件 310-312 交换它们的输出 315，以允许控制组件 310-312 中的每个控制组件执行多数表决，从而检测已经失效、正在失效及 / 或发生错误的控制组件 310-312 及 /

或选择传送哪个（些）输出 315 到所述现场设备。如果当前不担当主组件 320 的一个控制组件 310-312 检测到主控制组件 310-312 已经失效、正在失效及 / 或发生错误, 该控制组件 310-312 可以接管成为主组件 320 并通知系统操作员（例如通过操作员站 115）有关已经失效、正在失效及 / 或发生错误的控制组件 310-312。可以使用主组件仲裁方案（比如单循环选择算法）来确定由哪个控制组件 310-312 接管成为主组件 320。

[0045] 图 4 图解多个控制组件（例如软件子系统）的冗余拷贝分配到不同控制器的一个范例。在图 4 的图解范例中, 软件子系统 L 的第一拷贝 405 被分配到控制设备（例如控制器）410, 软件子系统 L 的第二拷贝 415 被分配到控制器 410, 而软件子系统 L 的第三拷贝 420 被分配到第二控制设备（例如第二控制器）425。此外, 软件子系统 Z 的第一拷贝 430 被分配到控制器 410, 而其第二拷贝 435 被分配到第三控制器（例如第三控制器 440）。同样地, 软件子系统 B 的第一拷贝 445 被分配到控制器 425, 而其第二拷贝 450 被分配到控制器 440。

[0046] 在图 4 的图解范例中, 特定软件子系统的每个拷贝是该特定软件系统的主拷贝（例如第一级拷贝）或第二级拷贝。主拷贝或第二级拷贝的指定可以是静态及 / 或动态的, 及 / 或可以由所述这些软件子系统的所述拷贝确定, 及 / 或可以通过中央冗余控制过程来确定。如图中所示, 一特定控制器可以是一个软件子系统的第一级, 同时是另一软件子系统的第二级。此外, 每个软件子系统的冗余拷贝的数目可能不同。

[0047] 图 5 为一流程图, 其显示一范例过程, 该范例过程可以用于实施图 2 的范例冗余控制器 225 及 / 或（更概括地）可以用于实施在此描述的任何范例控制器 150-152 或所有范例控制器 150-152。图 6 为一流程图, 其显示一范例过程, 该范例过程可以用于实施图 2 的范例升级模块 220, 以便升级图 2 的任何范例控制组件或所有范例控制组件。图 5 及 / 或 6 的范例过程可以由处理器、控制器及 / 或任何其他合适的处理设备实施。例如, 图 5 及 / 或 6 的范例过程可以收录于存储在有形机器可存取或可读媒介上的编码指令中, 比如存储在与处理器（例如以下连同图 9 进行讨论的范例处理器 905）相关的闪速存储器、只读存储器（ROM）及 / 或随机存取存储器（RAM）上的编码指令中。可选择地, 图 5 及 / 或 6 的一些或所有范例操作可以使用专用集成电路（ASICs）、可编程逻辑器件（PLDs）、现场可编程逻辑器件（FPLDs）、离散逻辑、硬件、固件等等的任何组合来实施。此外, 图 5 及 / 或 6 中描绘的一个或多个操作可以手动地实施, 或以前述的任何技术的任何组合来实施, 例如以固件、软件、离散逻辑及 / 或硬件的任何组合来实施。此外, 虽然图 5 及 / 或 6 的范例过程以图 5 及 / 或 6 的流程图来进行描述, 但本领域的普通工程技术人员将可以理解, 图 5 及 / 或 6 的范例过程可以以许多其他方法来实施。例如, 可以改变流程块的执行顺序, 及 / 或可以改变、消除、分割或结合所描述的有些流程块。此外, 本领域的普通工程技术人员将可以理解, 图 5 及 / 或 6 的任何范例操作或所有范例操作可以按顺序地执行, 及 / 或（例如）由个别的处理线程、处理器、器件、离散逻辑、电路等同时执行。

[0048] 图 5 的范例过程以控制组件（例如图 2 的范例控制组件的其中任何一个）的拷贝接收来自另一控制组件及 / 或现场设备的输入为开始。所述控制组件拷贝处理所接收的输入（流程块 505），以构成（例如计算）一个或多个输出（例如图 3 的范例输出 315）。冗余控制器（例如范例冗余控制器 225）采集及 / 或接收由所述控制组件的其他拷贝计算的输出（流程块 510），然后对所采集的那些输出与由所述控制组件的所述拷贝计算的输出进行

比较（流程块 515）。

[0049] 如果所述控制组件拷贝是所述控制组件的主拷贝（例如第一级拷贝）（流程块 520），及如果所述主拷贝的输出与来自所述控制组件的其他拷贝的输出匹配（流程块 525），则所述控制组件将其输出发送到另一控制组件（控制算法相同及 / 或不同的另一控制组件）及 / 或现场设备（流程块 530）。控件接着从图 5 的范例过程退出。

[0050] 返回到流程块 525，如果所述主拷贝的输出与所述控制组件的其他拷贝的输出不匹配（流程块 525），当前的主拷贝放弃其作为主拷贝的角色（流程块 535）。控件接着从图 5 的范例过程退出。

[0051] 返回到流程块 520，如果所述控制组件拷贝当前不是所述控制组件的主拷贝（流程块 520），所述冗余控制器确定所述当前主拷贝是否正确地操作（流程块 540）。例如，如果所述主拷贝的输出与大多数所述其他控制组件拷贝的输出匹配，所述冗余控制器确定该当前的主拷贝正确地操作。附加地或可选择地，所述当前主拷贝及所述冗余控制器可以交换所谓“心跳”信号（定期及 / 或不定期的），这允许所述当前主拷贝及 / 或及所述冗余控制器确定所述其他设备是否发挥功能及 / 或响应。例如，如果所述冗余控制器接收来自所述主拷贝的心跳信号，所述冗余控制器确定所述当前主拷贝正确地操作。如果所述当前主拷贝正确地操作（流程块 540），控件从图 5 的范例过程退出。如果所述当前主拷贝不正确地操作（流程块 540），则所述冗余控制器拷贝起动所述控制组件的主拷贝的改变（流程块 545）。控件接着从图 5 的范例过程退出。

[0052] 图 6 的范例过程以用户期望升级特定控制组件为开始。升级模块（例如图 2 的范例升级模块 220）接收来自所述用户的二进制图像（流程块 605）并存储所述二进制图像（例如范例图像 235）（流程块 610）。所述升级模块以“待更新”模式创建所述新控制组件的实例（流程块 615）。在有些范例中，所述新控制组件实例化为实时操作系统（RTOS）的隔离过程。

[0053] 所述升级模块起动从所述旧组件到所述新组件的状态数据传送（流程块 620）。在有些范例中，所述状态数据以实时操作系统（RTOS）的过程间通信能力来复制，比如以可移植操作系统界面（POSIX）功能呼叫来复制。在状态数据的传送完成时（流程块 625），所述升级模块终止所述原控制组件（流程块 630），然后将所述新控制组件的模式改变成“主动”（流程块 635）。控件接着从图 6 的范例过程退出。

[0054] 在有些范例中，新组件可以在所述旧组件被终止之前测试。在这些实例中，如果所述新组件不正确地操作，则所述新组件可以被终止，而所述旧组件保持为主动组件。在其他范例中，新组件可能稍后被发现存在缺失及 / 或缺陷，而所述升级模块可以回复到原始组件，直到可利用新组件为止。

[0055] 图 7A、7B、7C 及 7D 图解一范例过程，该范例过程可以由升级模块（例如图 2 的范例升级模块 220）实施来升级控制组件（例如范例控制组件 230 中的任何控制组件或所有控制组件）。图 7A 图解两个过程控制应用程序 705 及 710 的初始状态，而过程控制应用程序 705 及 710 利用控制组件 715 及控制组件 720。在图 7A-7D 的图解范例中，需将控制组件 715 升级为新版本。

[0056] 如图 7B 所示，所述升级模块创建控制组件 715 的新版本的实例 725，作为一隔离过程。在图 7C 的图解范例中，原控制组件 715 将状态数据及 / 或信息 730 复制到新控制组件

725。如图 7D 所示,在新控制组件 725 的状态与原控制组件 715 的状态匹配时,所述升级模块将新控制组件 725 的模式改变成“主动”并终止原控制组件 715。

[0057] 图 8A 及 8B 图解一范例控制系统,该范例控制系统操作控制组件的两个版本。图 8A 图解两个过程控制应用程序 805 及 810 的初始状态,而过程控制应用程序 805 及 810 利用控制组件 815 及控制组件 820。在图 8A 及 8B 的图解范例中,需为控制应用程序 810 将控制组件 815 升级为新版本。如图 8B 所示,所述升级模块创建控制组件 815 的新版本的实例 825,并开始将过程控制应用程序 810 的输入发送到新控制组件 825 以及同时将过程控制应用程序 805 的输入传送到原控制组件 815。原控制组件 815 及新控制组件 825 继续使用相同的控制组件 820。

[0058] 同时执行特定控制组件的两个版本使过程控制系统在为现有控制组件添加新特性及 / 或修正缺陷时能够有额外的灵活性。例如,包含所谓“热修复”的尚未能够全面接受品质测试的新控制组件只可以由需要改变的那些控制算法引进及使用。其他不需要所述新控制组件的控制算法可以继续使用原控制组件,直到所述新控制组件被正式放弃为止。附加地或可选择地,控制组件的两个版本也可以在其被正式放弃之前用于测试新控制组件,及 / 或不能向后兼容的改变可以在所有其他受影响的控制组件被更新之前引进。

[0059] 图 9 为一原理图,其图解一范例处理器平台 900,该范例处理器平台 900 可以用于及 / 或编程为执行在此描述的任何或所有范例控制平台 110、控制器 150-152 及 / 或范例处理器 205。例如,处理器平台 900 可以由一个或多个通用处理器、处理器芯核、微控制器等等实施。

[0060] 图 9 的范例的处理器平台 900 包括至少一个通用可编程处理器 905。处理器 905 执行存在于处理器 905 的主存储器 (例如存在于 RAM915 及 / 或 ROM920) 的编码指令 910 及 / 或 912。处理器 905 可以是任何类别的处理单元,比如处理器芯核、处理器及 / 或微控制器。处理器 905 除了执行别的以外,还可以执行图 5、6 及 / 或 7A-D 的范例过程,以实施在此描述的范例控制平台 110、控制器 150-152 及 / 或范例处理器 205。处理器 905 通过总线 925,与所述主存储器 (包括 ROM920 及 / 或 RAM915) 进行通信。RAM915 可以由动态随机存取存储器 (DRAM)、同步动态随机存取存储器 (SDRAM) 及 / 或任何其他类别的随机存取存储器 (RAM) 器件实施,而 ROM920 可以由闪速存储器及 / 或任何其他期望类别的存储器器件实施。对存储器 915 及 920 的存取可以由存储器控制器 (图中未显示) 来控制。RAM915 可以用于存储及 / 或实施 (例如) 图 2 的范例主存储器 210。

[0061] 处理器平台 900 也包括界面电路 930。界面电路 930 可以以任何类别的界面标准实施,比如通用串行总线 (USB) 界面、蓝牙 (Bluetooth) 界面、外存储器界面、串口、通用输入 / 输出界面等等。一个或多个输入设备 935 及一个或多个输出设备 940 连接到界面电路 930。输入设备 935 及 / 或输出设备 940 可以用于 (例如) 实施图 2 的范例背板界面 245。

[0062] 虽然在此已经描述某些范例方法、设备及制造件,但本专利包括的范围并未受其限制。这些范例的性质属于非限制性的原理性范例,其并未限制本专利包括的范围。相反地,本专利包括所有根据字面意义或等效原则正当地属于附此的权利要求的范围的方法、设备及制造件。

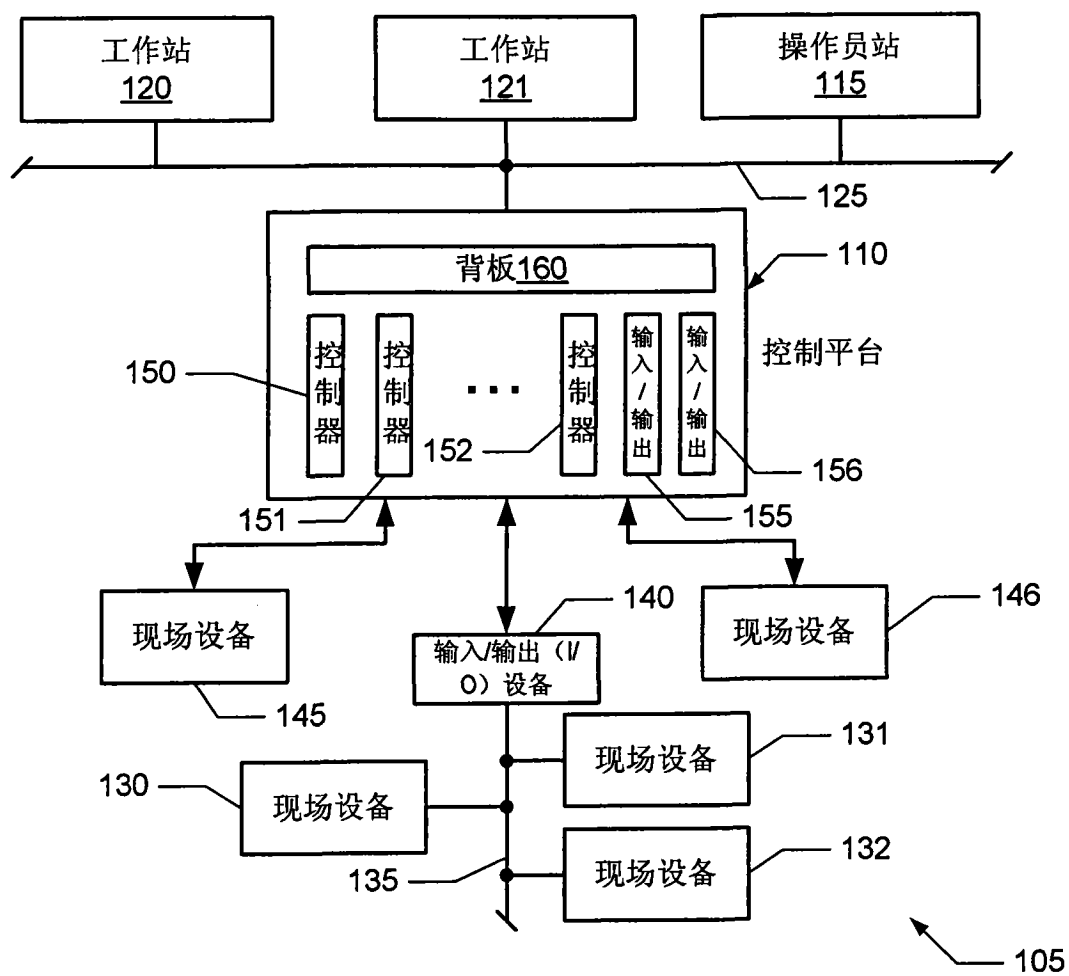


图 1

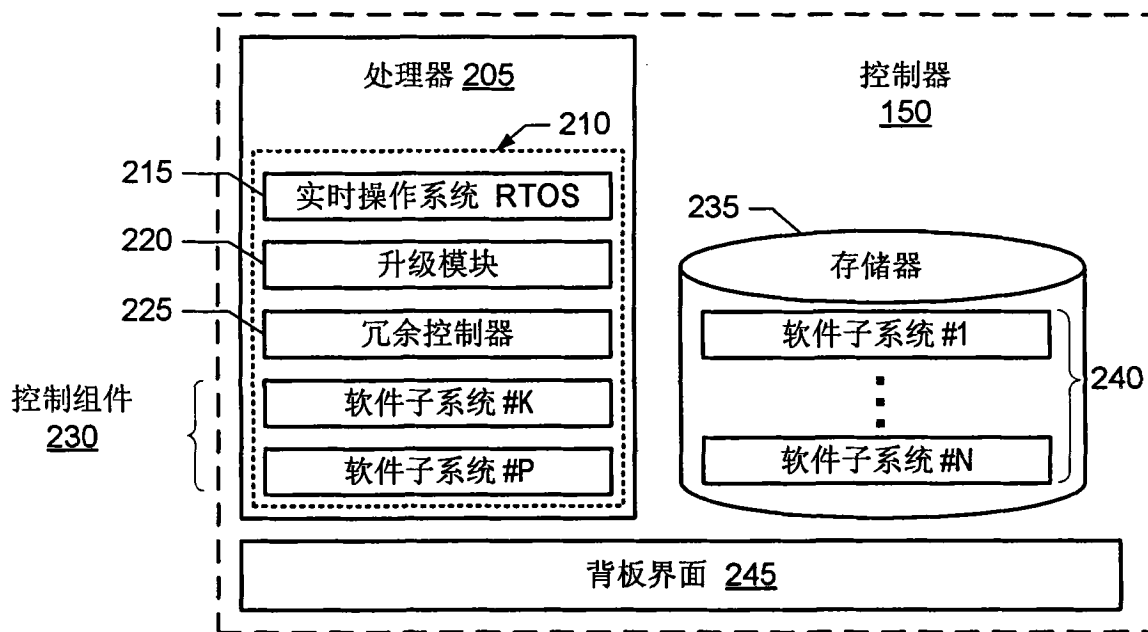


图 2

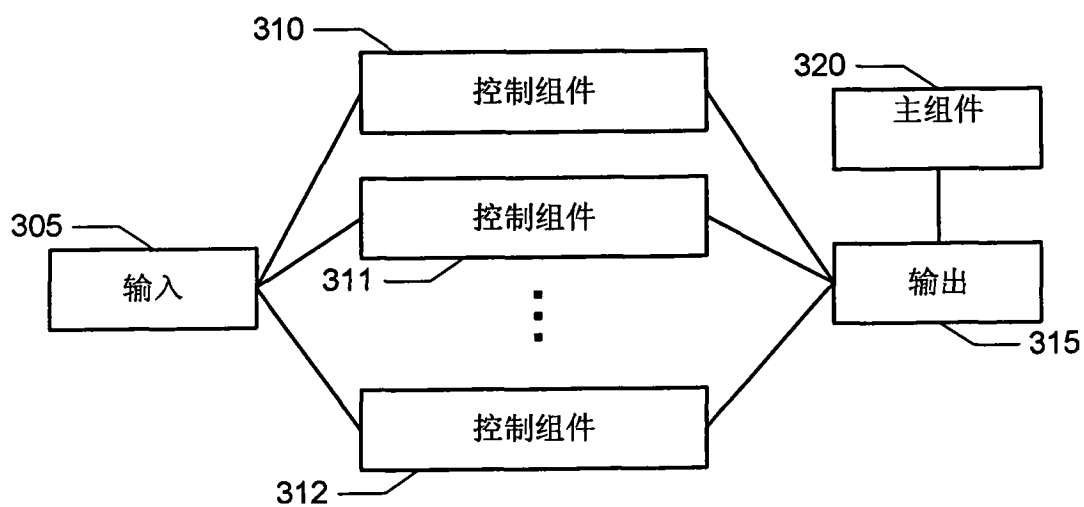


图 3

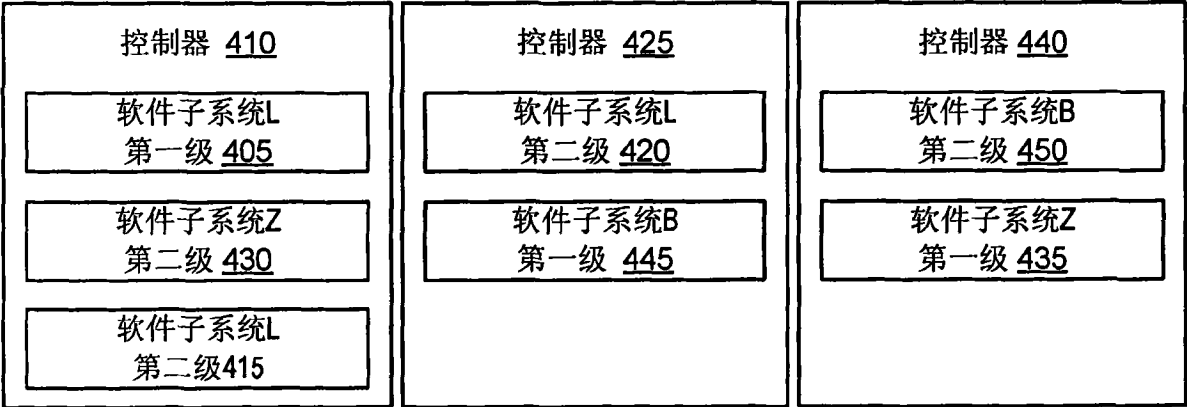


图 4

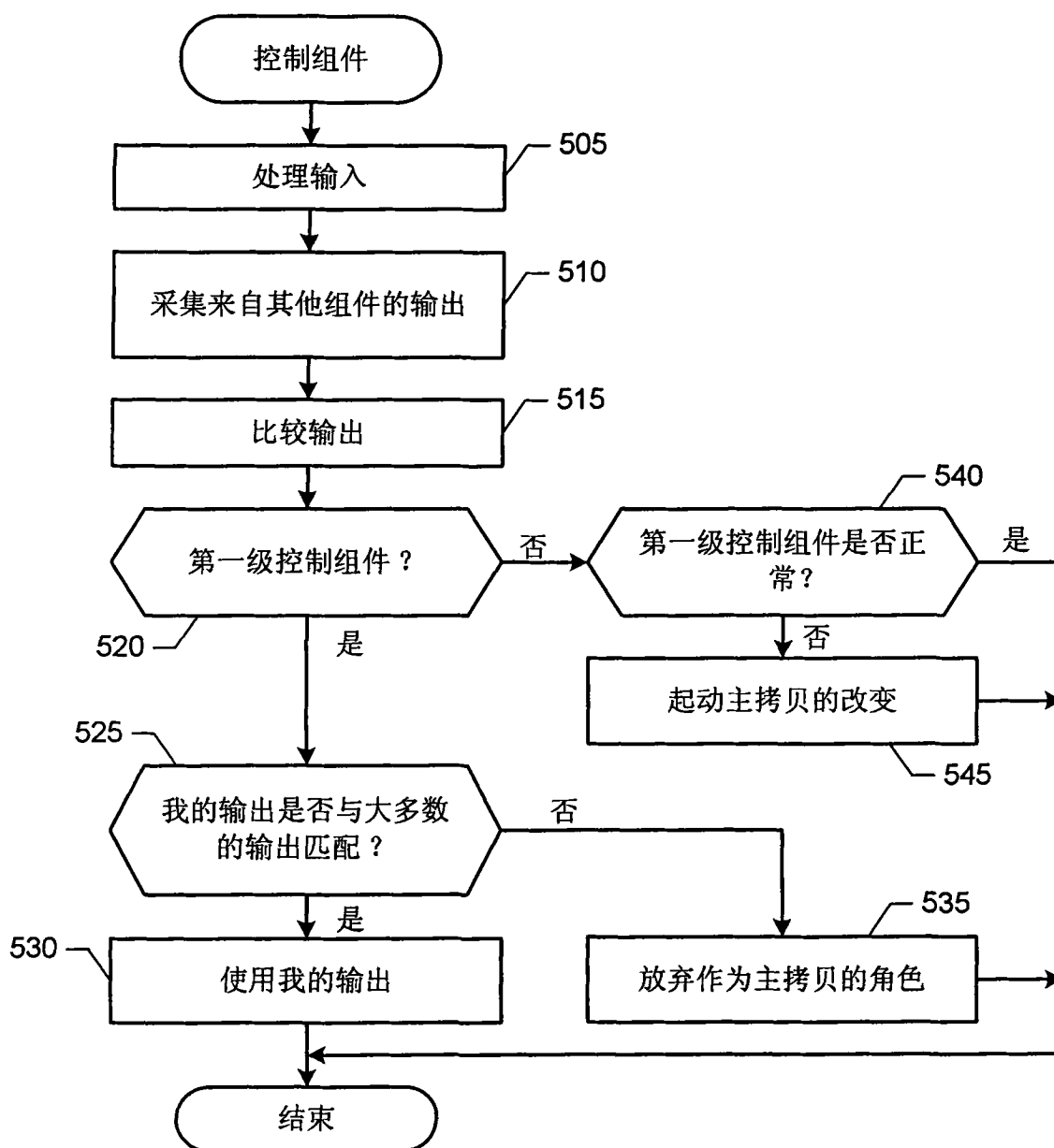


图 5

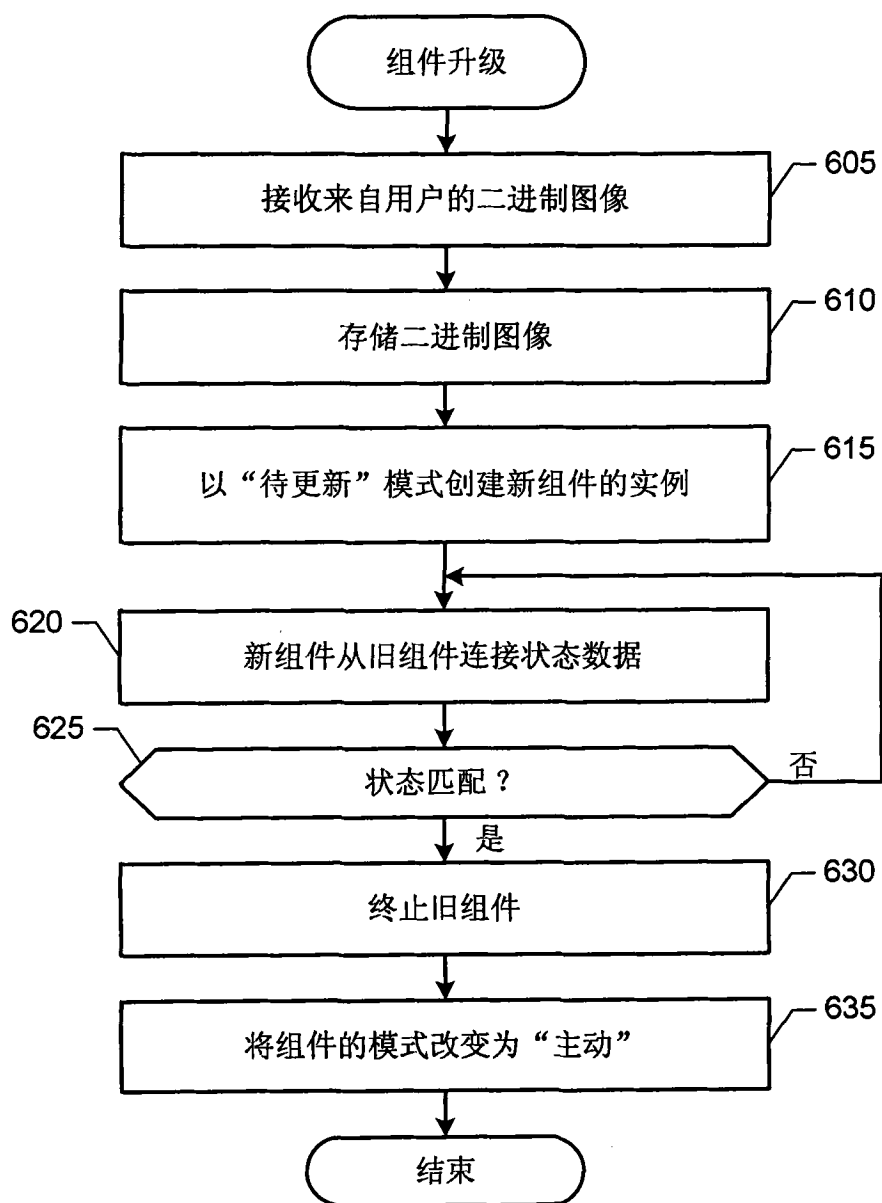


图 6

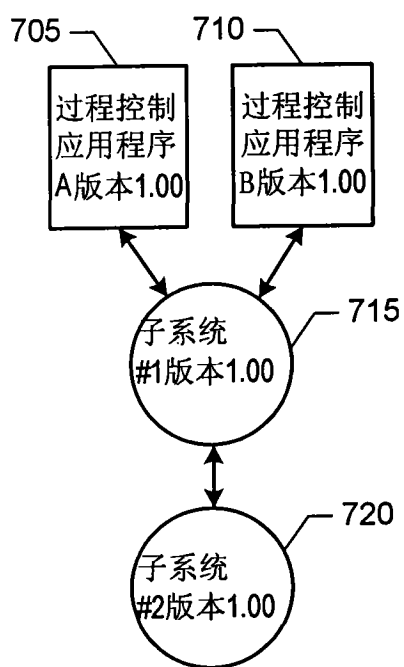


图 7A

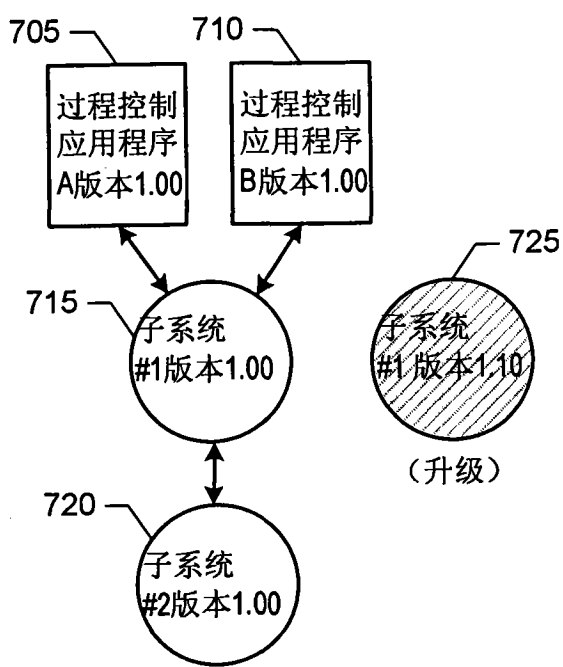


图 7B

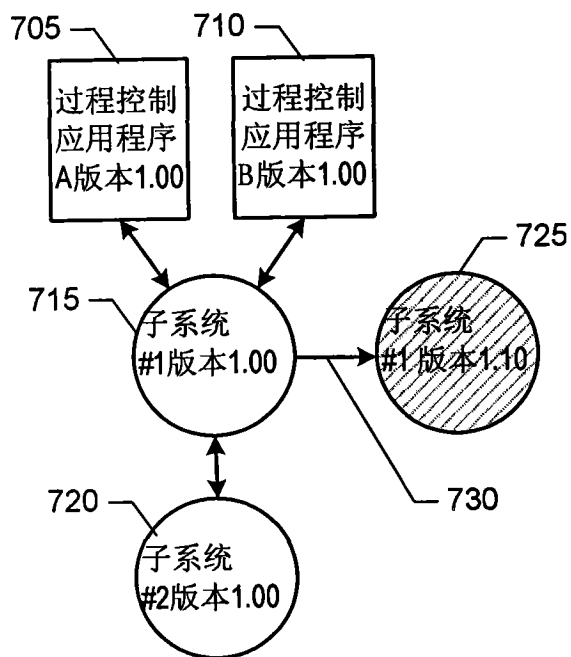


图 7C

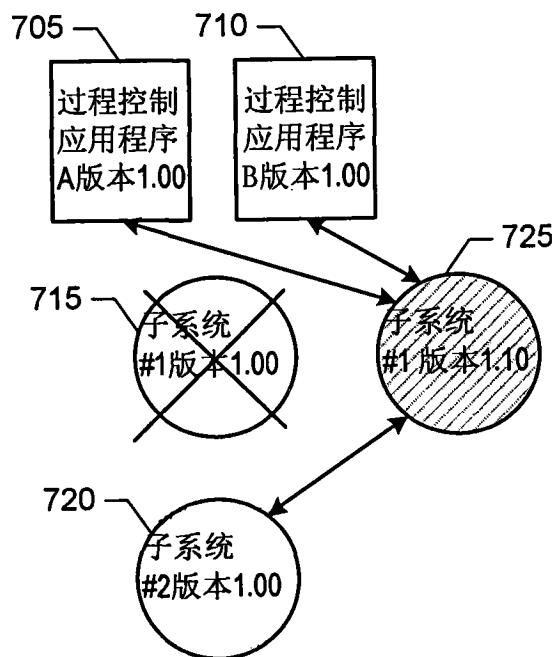


图 7D

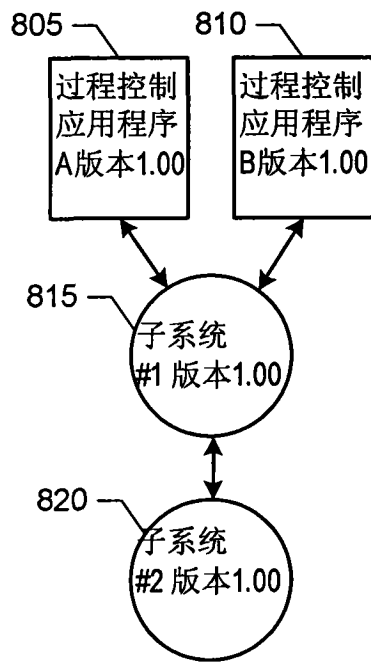


图 8A

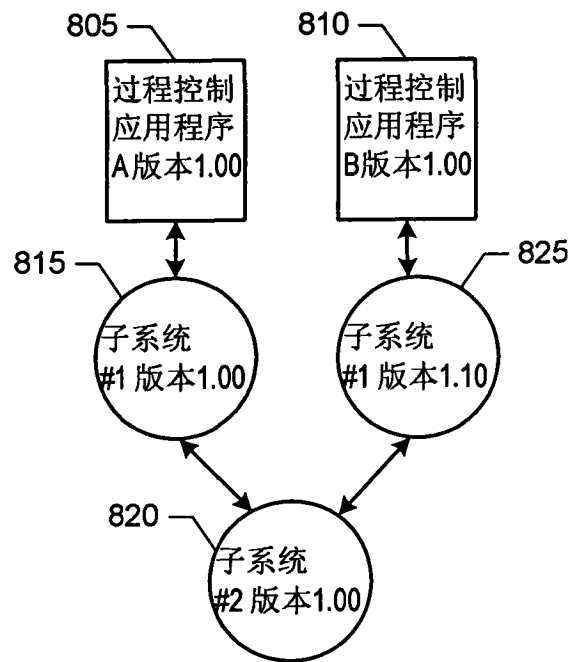


图 8B

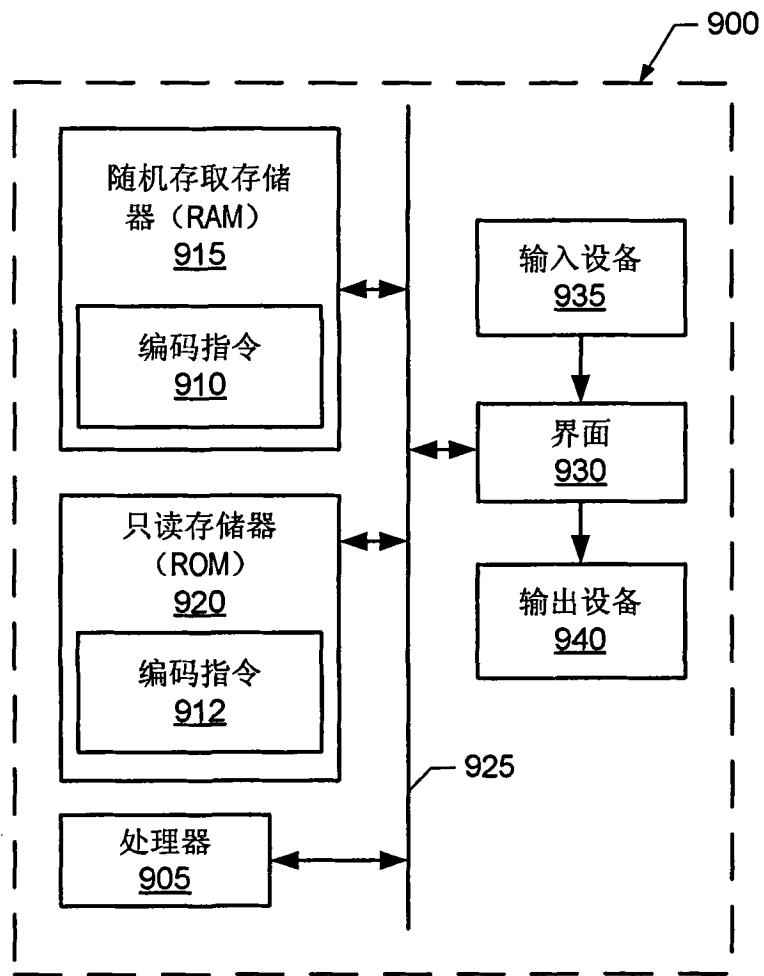


图 9