



(12) 发明专利

(10) 授权公告号 CN 107660289 B

(45) 授权公告日 2021.04.02

(21) 申请号 201680029813.0

C·麦克达涅尔斯三世

(22) 申请日 2016.05.20

G·K·林格

(65) 同一申请的已公布的文献号  
申请公布号 CN 107660289 A

(74) 专利代理机构 北京市金杜律师事务所  
11256

(43) 申请公布日 2018.02.02

代理人 王茂华 姚杰

(30) 优先权数据

(51) Int.Cl.

14/722,006 2015.05.26 US

G06Q 10/06 (2012.01)

(85) PCT国际申请进入国家阶段日  
2017.11.22

G06Q 10/10 (2012.01)

H04L 12/26 (2006.01)

(86) PCT国际申请的申请数据  
PCT/US2016/033389 2016.05.20

(56) 对比文件

CN 103473019 A, 2013.12.25

(87) PCT国际申请的公布数据  
W02016/191228 EN 2016.12.01

US 2007083588 A1, 2007.04.12

WO 2011046559 A1, 2011.04.21

(73) 专利权人 微软技术许可有限责任公司  
地址 美国华盛顿州

US 2013036422 A1, 2013.02.07

US 2013055247 A1, 2013.02.28

US 8856953 B2, 2014.10.07

CN 103988538 A, 2014.08.13

(72) 发明人 D·R·科内尔 W·T·伯伊德  
R·K·林兹 K·梅尔-马格鲁德  
B·L·瓦里纳 D·S·里雷

审查员 石佼

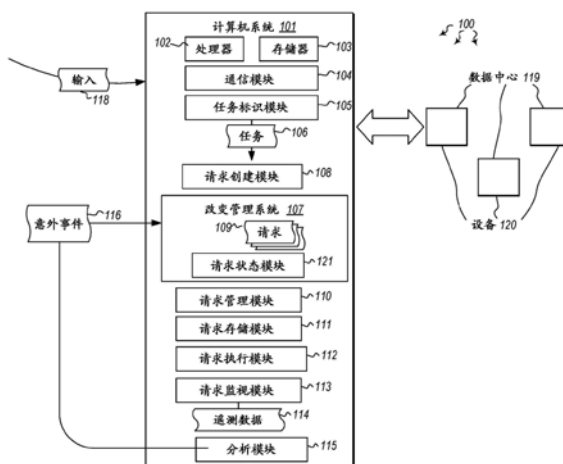
权利要求书2页 说明书11页 附图10页

(54) 发明名称

自动网络控制

(57) 摘要

实施例涉及跨数据中心自动地控制网络和服务质量。在一种场景中,计算机系统标识在数据中心内将被执行的部分工作。计算机系统在改变管理系统中创建针对改变的请求(请求),其中改变管理系统被配置为存储和管理数据中心内的请求的实现。然后,在实现所创建的请求时,计算机系统轮询请求的状态以确定是否现在可以执行请求中标识的工作的部分,并且在确定可以执行在请求中标识的工作的部分,计算机系统根据请求执行工作的部分。根据请求的指定的工作的执行允许基于请求来控制工作流。



1. 一种用于自动地控制在数据中心内的网络和服务的方法,在包括至少一个处理器的计算机系统处被实现,所述方法包括:

标识在数据中心内将被执行的任务;

创建包括标识的所述任务的指示的、针对改变的请求,所述请求由改变管理器来存储和管理;

在创建所述请求时,监视创建的所述请求的处理,所述监视导致遥测数据的一个或多个部分;

分析所述遥测数据,以标识一个或多个意外事件,所述一个或多个意外事件与对在所述请求中标识的所述任务的处理有关;以及

在标识出至少一个意外事件时,存储生成的用于解决所述意外事件的针对改变的第二请求。

2. 根据权利要求1所述的方法,还包括:生成自动执行所述任务的自动化 workflow,所述任务在由所述请求指定的所述数据中心内将被执行。

3. 根据权利要求2所述的方法,还包括:使用所述请求来控制所述自动化 workflow,使得所标识的任务基于所述请求的状态而被执行或不被执行。

4. 根据权利要求3所述的方法,其中控制所述自动化 workflow 包括以下至少一项:使用所述请求来停止所述自动化 workflow、暂停所述自动化 workflow 和取消所述自动化 workflow。

5. 根据权利要求1所述的方法,还包括生成解决所述意外事件的针对改变的所述第二请求,针对改变的所述第二请求包括一个或多个特定任务,所述一个或多个特定任务当被处理时处置所述意外事件。

6. 根据权利要求1所述的方法,其中所标识的所述任务包括执行软件或固件升级。

7. 根据权利要求1所述的方法,还包括:

自动地检测所标识的所述任务的执行已经发生故障;以及

停止或暂停所述请求,使得根据所述请求的所标识的所述任务的执行将被停止或暂停。

8. 根据权利要求1所述的方法,其中所标识的所述任务在防止有影响改变的安全模式下根据所述请求被执行。

9. 根据权利要求1所述的方法,其中所标识的所述任务在允许有影响改变发生的模式下根据所述请求被执行。

10. 根据权利要求1所述的方法,还包括实例化至少一个数据中心设备上的功能的一部分,所述功能的一部分将网络业务从所述数据中心设备转移到另一数据中心设备上。

11. 根据权利要求1所述的方法,还包括将被处理的所述任务的状态作为所述请求的一部分报告给至少一个实体。

12. 根据权利要求1所述的方法,其中所标识的所述任务包括从旧的软件版本升级到新的软件版本。

13. 一种计算机系统,包括:

至少一个处理器;

工作部件,被配置为标识在数据中心内将被执行的任务;

改变管理部件,被配置为创建针对改变的请求以执行所述任务,所述改变管理部件被

配置为存储和管理所述数据中心内的请求的实现；

监视部件，所述监视部件在确定所述请求已被创建之后，监视所述请求的处理，所述监视导致遥测数据的一个或多个部分；

遥测部件，用于分析所述遥测数据，以标识与所述请求的所述处理有关的一个或多个意外事件；以及

数据存储装置，用于在标识出至少一个意外事件时，存储生成的用于解决所述意外事件的针对改变的第二请求，针对改变的所述第二请求包括一个或多个特定任务，所述一个或多个特定任务在被处理时处置所述意外事件。

14. 根据权利要求13所述的计算机系统，其中所述遥测数据包括以下至少一项：警报日志数据的检查、设备状态数据的检查、网络业务性能数据的检查、警报时间、解决时间、启动设备的时间、到数据的相同性能的时间或用于修复的响应时间。

15. 根据权利要求13所述的计算机系统，还包括在针对改变的所述请求的实现之前生成预期事件的指示。

16. 根据权利要求13所述的计算机系统，还包括在确定意外事件已经发生时生成一个或多个警报。

17. 根据权利要求16所述的计算机系统，还包括针对所述意外事件的解决时间。

18. 一种计算机可读存储介质，在所述计算机可读介质上存储有用于跨数据中心自动地控制网络和服务质量的计算机可执行指令，所述计算机可执行指令当由计算系统的一个或多个处理器执行时，使得所述计算系统执行动作，所述动作包括：

标识在数据中心内将被执行的任务；

访问包括标识的所述任务的指示的、针对改变而生成的请求，所述请求由改变管理服务来存储和管理；

在访问所述请求时，监视创建的所述请求的执行，所述监视导致遥测数据的一个或多个部分；

分析所述遥测数据，以标识一个或多个意外事件，所述一个或多个意外事件与对在访问的所述请求中标识的所述任务的处理有关；

在标识出至少一个意外事件时，生成用于解决所述意外事件的针对改变的第二请求；以及

存储针对改变的所述第二请求。

19. 根据权利要求18所述的计算机可读存储介质，所述动作还包括：在标识出所述至少一个意外事件时，创建包括解决所述意外事件的一个或多个自动实现的任务的自动化 workflow。

20. 根据权利要求18所述的计算机可读存储介质，所述动作还包括：标识所述意外事件的解决时间，以及监视以确定在所述意外事件被解决之前的实际时间长度。

## 自动网络控制

### 背景技术

[0001] 当今的数据中心包括许多不同的联网、处理和其他设备。这些设备需要自动地被监测、修补和测试。这些设备的冗余也被管理,以确保故障转移自动发生。

### 发明内容

[0002] 本文描述的实施例涉及自动地控制网络和跨数据中心地服务传递。在一个实施例中,计算机系统标识在数据中心内将被执行的任务,并且创建包括标识的任务的指示的、针对改变的请求,其中该请求由改变管理器来存储和管理。然后,在创建请求时,计算机系统监视创建的请求的处理。监视导致遥测数据,所述遥测数据被分析以标识与请求中所标识的任务的处理有关的意外事件。

[0003] 然后,在标识至少一个意外事件时,计算机系统存储所生成的用于解决意外事件的针对改变的第二请求。此处理确保当意外事件发生时,数据中心设备可以在执行所需的任务。这种自动地和平衡地响应故障或其他意外事件的能力导致提高的数据中心可靠性。可被自动执行的数据中心任务的示例包括但不限于修补或执行软件升级、重新启动设备、关闭设备、卸载部件、实现配置改变、控制或重定向网络业务流程、评估和更改处理器利用率、执行数据收集(包括聚集遥测数据(诸如性能数据、来自服务器的计数器、聚合服务器日志、事件日志等))或执行低级调试(例如跟踪信息收集)的进程转储(“process dump”)。许多其他任务可以由计算机系统执行,这将在下面解释。

[0004] 提供本发明内容以便以简化的形式介绍将在下面的具体实施方式中进一步描述的概念的选择。本发明内容不旨在标识所要求保护的主题的主要特征或基本特征,也不旨在用作辅助确定所要求保护的主题的范围。

[0005] 附加的特征和优点将在下面的描述中阐述,并且在描述中对于本领域的普通技术人员而言部分将是显而易见的,或者可以通过本文的教导的实践而被了解。本文描述的实施例的特征和优点可以通过在所附权利要求中特别指出的手段和组合来实现和获得。从下面的描述和所附的权利要求中,本文描述的实施例的特征将变得更加明显。

### 附图说明

[0006] 为了进一步阐明本文描述的实施例的上述和其他特征,更具体的描述将通过参考附图而被呈现。可以理解,这些附图仅描绘了本文描述的实施例的示例,因此不被认为是对其范围的限制。将通过附图的使用以附加的特征和细节来描述和解释实施例,在附图中:

[0007] 图1图示了在其中本文描述的实施例可以操作、包括跨数据中心自动地控制网络和服务传递的计算机架构。

[0008] 图2图示了包括多个字段的请求数据记录的实施例。

[0009] 图3图示了用于跨一个或多个数据中心自动地控制网络和服务的备选示例方法的流程图。

[0010] 图4图示了在其中控制过程的部件被定义的实施例。

- [0011] 图5图示了描述由各种实体采取的步骤的状态图的实施例。
- [0012] 图6图示了描述由各种实体采取的步骤的状态图的附加实施例。
- [0013] 图7图示了描述由各种实体采取的步骤的状态图的附加实施例。
- [0014] 图8图示了描述由各种实体采取的步骤的状态图的附加实施例。
- [0015] 图9图示了设备角色特定工作流的实施例。
- [0016] 图10图示了描述由各种实体采取的步骤的状态图的附加实施例。

### 具体实施方式

[0017] 本文描述的实施例涉及跨数据中心自动地控制网络和服务传递。在一个实施例中,计算机系统标示在数据中心内将被执行的任务,并且创建包括对标示的任务的指示的、针对改变的请求,其中该请求由改变管理器来存储和管理。然后,在创建请求时,计算机系统监视创建的请求的处理。监视导致遥测数据,该遥测数据被分析以标示意外事件,该意外事件与请求中所标识的任务的处理有关。

[0018] 然后,在标识至少一个意外事件时,计算机系统存储所生成以解决意外事件的针对改变的第二请求。此处理确保数据中心设备可以在意外事件发生时执行所需的任务。自动地和平衡地响应故障或其他意外事件的这种能力导致增加的数据中心的可靠性,因为错误或意外事件可以被实时地响应。更进一步,通过在意外错误发生后自动地处理意外错误,下游错误可以被避免,其导致进一步的错误减少、更高的数据中心效率、以及增加的整体可靠性和可用性。

[0019] 可自动地执行的数据中心任务的示例包括但不限于修补或执行软件升级、重新启动设备、关闭设备、卸载部件、实施配置改变、控制或重定向网络业务流、评估和改变处理器利用率、执行数据收集(包括聚集遥测数据(诸如性能数据、来自服务器的计数器、聚合服务器日志、事件日志等))或执行低级调试(例如跟踪信息的收集)的进程转储。许多其他任务可以由计算机系统执行,这将在下面解释。

[0020] 以下讨论现在涉及可以执行的多个方法和方法动作。应当注意,尽管方法动作可以按照某种顺序来讨论或者在流程图中如以特定顺序发生来说明,但除非因为一个动作依赖于在该动作被执行之前完成另一动作而特别说明,或者是必需的,否则特定的顺序不必是必需的。

[0021] 本文描述的实施例可以实现各种类型的计算系统。这些计算机系统现在越来越多地采取各种形式。例如,计算系统可以是手持设备,诸如智能电话或特征电话、电器、膝上型计算机、可穿戴设备、桌面型计算机、大型机、分布式计算系统、或甚至通常不被认为是计算系统的设备。在本说明书和权利要求中,术语“计算系统”被宽泛地定义为包括任何设备或系统(或其组合),其包括至少一个物理和有形处理器以及物理和有形存储器,物理和有形存储器能够在其上具有可由处理器执行的计算机可执行指令。计算系统可以分布在网络环境中,并且可以包括多个组成计算系统。

[0022] 如图1所示,计算系统101通常包括至少一个处理单元102和存储器103。存储器103可以是物理系统存储器,其可以是易失性的、非易失性的或两者的一些组合。术语“存储器”在本文也可以用于指非易失性大容量存储装置,诸如物理存储介质。如果计算系统是分布式的,则处理、存储器和/或存储能力也可以是分布式的。

[0023] 如本文所使用的术语“可执行模块”或“可执行部件”可以指代可以在计算系统上执行的软件对象、例程或方法。本文描述的不同部件、模块、引擎和服务可以被实现为在计算系统上执行的对象或进程(例如,作为单独的线程)。

[0024] 在下面的描述中,参考由一个或多个计算系统执行的动作来描述实施例。如果这种动作以软件实现,则执行动作的相关联的计算系统的一个或多个处理器响应于已经执行了计算机可执行指令来指导计算系统的操作。例如,形成计算机程序产品的这样的计算机可执行指令可以体现在一个或多个计算机可读介质上。这种操作的示例涉及数据的操纵。计算机可执行指令(和操纵数据)可以被存储在计算系统101的存储器103中。计算系统101还可以包含允许计算系统101通过有线网络或无线网络与其他消息处理器通信的通信信道。

[0025] 本文描述的实施例可以包括或利用专用或通用计算机系统,其包括诸如例如一个或多个处理器和系统存储器的计算机硬件,如以下更详细讨论的。系统存储器可以被包括在整个存储器103内。系统存储器也可以被称为“主存储器”,并且包括可由至少一个处理单元102通过存储器总线寻址的存储器位置,在这种情况下,地址位置在内存总线本身上被断言。系统存储器传统上是易失性的,但是本文描述的原理也应用于在其中系统存储器是部分或者甚至完全是非易失性的情况。

[0026] 本发明范围内的实施例还包括用于携带或存储计算机可执行指令和/或数据结构的物理和其他计算机可读介质。这样的计算机可读介质可以是可以被通用计算机系统或专用计算机系统访问的任何可用介质。存储计算机可执行指令和/或数据结构的计算机可读介质是计算机存储介质。携带计算机可执行指令和/或数据结构的计算机可读介质是传输介质。因此,作为示例而非限制,本发明的实施例可以包括至少两种明显不同的计算机可读介质:计算机存储介质和传输介质。

[0027] 计算机存储介质是存储计算机可执行指令和/或数据结构的物理硬件存储介质。物理硬件存储介质包括计算机硬件,诸如RAM、ROM、EEPROM、固态驱动器(“SSD”)、闪存、相变存储器(“PCM”)、光盘存储、磁盘存储或其他磁存储设备、或者可以用于存储以计算机可执行指令或数据结构的形式的程序代码的任何其他硬件存储设备,其可以被通用计算机系统或专用计算机系统访问和执行以实现公开的本发明的功能。

[0028] 传输介质可以包括网络和/或数据链路,其可以用于携带以计算机可执行指令或数据结构形式的程序代码,并且其可以由通用计算机系统或专用计算机系统访问。“网络”被定义为使能计算机系统和/或模块和/或其他电子设备之间电子数据的传输的一个或多个数据链路。当信息通过网络或另一通信连接(硬连线、无线或硬连线或无线的组合)被传送或提供给计算机系统时,计算机系统可将连接视为传输介质。以上的组合也应被包括在计算机可读介质的范围内。

[0029] 此外,在到达各种计算机系统部件时,以计算机可执行指令或数据结构形式的程序代码可以从传输介质被自动地传送到计算机存储介质(反之亦然)。例如,通过网络或数据链路接收的计算机可执行指令或数据结构可以被缓存在网络接口模块(例如“NIC”)内的RAM中,然后最终被传送到计算机系统RAM和/或计算机系统内的较不易失性计算机存储介质。因此,应当理解,计算机存储介质可以被包括在也(甚至主要)利用传输介质的计算机系统部件中。

[0030] 计算机可执行指令包括例如指令和数据,该指令或数据当在一个或多个处理器处执行时使得通用计算机系统、专用计算机系统或专用处理设备执行特定功能或一组功能。计算机可执行指令可以是例如诸如汇编语言的二进制、中间格式指令、或甚至源代码。

[0031] 本领域技术人员将理解,本文所描述的原理可以被实践在具有许多类型的计算机系统配置的网络计算环境中,所述计算机系统配置包括个人计算机、桌面型计算机、膝上型计算机、消息处理器、手持设备、多处理器系统、基于微处理器或可编程的消费电子产品、网络PC、小型计算机、大型计算机、移动电话、PDA、平板计算机、寻呼机、路由器、交换机等。本发明还可以被实践在分布式系统环境中,其中通过网络链接(通过硬连线数据链路、无线数据链路、或通过硬连线数据链路和无线数据链路的组合)的本地和远程计算机系统均执行任务。这样,在分布式系统环境中,计算机系统可以包括多个组成计算机系统。在分布式系统环境中,程序模块可能位于本地存储器存储设备和远程存储器存储设备两者中。

[0032] 本领域技术人员还将理解,本发明可以被实践在云计算环境中。云计算环境可能是分布式的,尽管这不是必需的。当分布式时,云计算环境可以国际性地被分布在组织内和/或具有跨多个组织拥有的部件。在本说明书和以下权利要求中,“云计算”被定义为用于使得按需网络能够访问可配置计算资源(例如,网络、服务器、存储装置、应用和服务)的共享池的模型。“云计算”的定义不限于在适当部署时可以从这样的模型获得的其他许多优点中的任意一个。

[0033] 另外,本文描述的系统架构可以包括多个独立部件,每个独立部件都作为一个整体有助于系统的功能。这种模块化可以允许在解决平台可扩展性问题时提高灵活性,并为此提供各种优点。通过功能范围有限的小规模部件的使用,可以更容易地管理系统的复杂性和增长。通过这些松散耦合的模块的使用,可以增强平台容错能力。个别部件可以根据业务需求指示逐步增长。模块化开发也意味着新功能的上市时间缩短。可以在不会影响核心系统的情况下增加或减少新功能。

[0034] 图1图示了在其中至少一个实施例可以被采用的计算机架构100。计算机架构100包括计算机系统101。计算机系统101可以是任何类型的本地或分布式计算机系统,包括云计算系统。计算机系统101包括用于执行各种不同功能的模块。例如,通信模块104可以被配置为与其他计算系统进行通信。通信模块104可以包括可以从其他计算系统接收数据和/或向其他计算系统发送数据的任何有线通信部件或无线通信部件。通信模块104可以被配置为与数据库、移动计算设备(诸如移动电话或平板计算机)、嵌入式或其他类型的计算系统交互。

[0035] 通信模块104可以进一步被配置为接收输入118。输入118可以指示某些任务要被发起、或者该请求数据将被生成、或者某些自动化请求将被启动、停止或暂停。实际上,取决于上下文,输入118可以具有各种不同的含义和用途。计算机系统101还包括任务标识模块105。任务标识模块105可以与数据中心119的设备120进行通信,并且可以使用各种方法来标识将被执行的自动化任务106。数据中心119可以包括许多不同类型的设备120,包括联网设备、存储设备、处理器、存储器、服务器机架或其他类型的硬件。自动化任务106可以包括例如用更新的软件来升级设备节点上的软件、重新启动设备、自动关闭设备、或可能需要执行的任何其他自动化任务。

[0036] 自动化任务数据106可以被输入到改变管理系统107中。改变管理系统107可以负

责控制和监视对数据中心设备120所做的改变。其他模块可以被改变管理系统107访问以监视和控制请求的自动实现,其包括请求管理模块110、请求存储模块111、请求执行模块112、请求监视模块113和分析模块115,分析模块115可以用于分析从数据中心119的设备聚集的遥测数据114。请求状态模块121可以存储请求109的状态,并向查询实体提供请求109的状态。应当注意,这些请求模块中的每一个可以被本地包含在计算机系统101内,或者可以是另一计算机系统的一部分。

[0037] 请求本身(109)可以被称为针对改变的请求或请求数据记录,或简称为请求。如图2所示,请求数据记录201可以包括关于该请求的不同类型的信息。请求201可以包括标识请求应用到的数据中心的数据中心标识符202。例如,如果请求是特定于一个数据中心中的设备、软件或服务的,则数据中心ID可能特定于该数据中心。请求数据记录201还可以包括已经由任务标识模块105所标识的任务203的指示。这些任务可以是例如在确定数据中心设备将被更新或重新启动或重新配置时被自动地执行的自动任务。

[0038] 实际上,由模块105所标识的可以被自动地执行的任务106包括但不限于修补或执行软件更新、重新启动设备、关闭设备、卸载部件、实现配置改变、控制或重定向网络业务流、评估和改变处理器利用率、执行数据收集(包括聚集诸如性能数据、来自服务器的计数器、聚合服务器日志、事件日志等的遥测数据)、执行用于低级调试的进程转储(例如跟踪信息的收集)、或与可以在数据中心内被自动地执行的其他任务有关的信息。

[0039] 返回图2,请求数据记录201可以进一步包括受影响的服务或设备的指示。这些是在所标识的任务203中的一个或多个的实现时将会受到影响的服务或设备。请求数据记录201也可以包括将被执行的任务的描述205以及其执行的理由206。例如,诸如升级或重新启动的某些任务的执行可能会导致停机时间,该任务可能需要一定程度的调整以便于使其执行。请求数据记录201还可以包括所标识的任务203的估计完成时间207以及建议的或计划的开始时间。开始时间208可以在首先检查改变管理系统107时计算。如果改变管理系统107处于锁定模式,则开始时间将被延迟。如果改变管理系统107不处于锁定模式,则将为该任务计算估计的持续时间,并且开始时间将基于该任务的估计持续时间来生成。

[0040] 在大规模服务中,通常存在许多不同类型的设备,其具有要被管理、监视、打补丁和测试的不同命令集。给定数据中心设计的冗余可以被定期测试以确认其操作并标识可能阻止这些数据中心设备120之间的无缝故障切换的问题。该过程还可包括验证数据中心正确地监视检测问题、测量分辨率、设计被正确地实现。本文描述的实施例以自动的方式执行这些功能,由改变管理系统107以可视和可跟踪的方式集成和控制。

[0041] 实际上,本文所描述的实施例可以执行许多不同的功能,包括但不限于以下项:实施例可以与改变管理系统107集成为用户控制界面并且允许跟踪自动化在做什么,并且进一步计算估计的持续时间。实施例可以遵守在改变管理系统107中配置的锁定日期。要执行的任务106可以由本文的针对改变的请求或“请求”来控制。请求109可以包括要作为请求的一部分而被执行的一个或多个特定任务。然后任务列表可以通过控制请求来控制。也就是说,当请求开始、停止、暂停或取消时,改变管理系统会自动地采取相关联的动作。如果在任何时候检测到不可恢复的故障,则任务106的自动执行将停止处理附加项目,并经由电子邮件、文本消息、自动页面、事件票据或其他通知方法的任意组合来发送通知。

[0042] 实施例还提供了在网络设备上使用本地脚本来迁移和移动设备之间的网络业务



的能力。“混乱(“chaos”)”模式可以被实现以通过引起故障、测量影响水平以及当服务不能处置故障时生成和存储错误数据以主动测试容错网络设计。实施例还提供了理解不同设备角色和角色组健康、确认设备状态、比较在改变之前和之后的配置以确保健康和网络功能已经恢复、并且通过从其他系统提取警报数据来关联在服务中发生的事件的能力。如果需要,自动配置备份可用于自动回退。在某些情况下,在针对与当前正在维护的特定设备有关的设备和服务器的“安全”维护期间,警报可以被抑制。

[0043] 另外,实施例允许在网络设备上运行脚本或服务以促进网络和服务控制。工作流引擎可以被实时配置,允许调整并发设备组的数量以及每个组中设备的数量。实施例还提供使用安全外壳协议(或一些其他协议)和暴露的应用程序编程接口(API)来运行控制命令的能力。

[0044] 因此,如上所述,进程可以被实现以自动搜索和标识需要执行的任务。这些进程自动执行诸如修补的维护工作,还可以可选地执行“混乱”模式任务来测试为容错而设计的数据中心架构的冗余。这些进程管理同时的任务,并确保相同数据中心设备不存在重叠任务。无论操作模式如何(即“混乱”或“安全”),该进程标识任务106并自动生成和记录对自动工作的请求。在运行状态中时,改变管理系统可以用作用于控制自动化的用户界面。开始、停止、暂停和取消命令受到进程的重视和挑选,并在自动化中采取对应的动作。

[0045] 在执行维护的同时,该进程可以以试图避免对数据中心数据路径的影响的“安全”模式进行操作。数据中心设备120在维护之前和之后被测试。可以执行比较以确保配置、路由表和接口匹配正确的操作状态(如在请求状态模块121中存储的)。相邻设备也可以在维护之前被测试以验证在执行任务106之前其状态和处置现有网络业务的能力。在网络设计支持的情况下,可以实现特殊的网络设备侧脚本,以执行到相邻设备的平稳故障切换或重新路由网络业务。

[0046] 当在“混乱”模式下操作时,该进程不执行平衡的转换,并且相反,故意测试数据中心设计中的故障场景。在适当的条件下,所有的数据中心设备都应当能从故障复原。在测试期间,模拟设备故障的影响还会被监测,并且收集数据。在监视和售票系统中注入故障的主动警报被确认。相关的警报也是相关的。所检测的故障持续时间、警报时间和解决时间都可以根据服务等级协议(SLA)而被测量、记录和匹配。任何偏差都会停止当前正在运行的任务并触发调查和根本原因分析。其他通知可以经由售票、错误、任务、自动页面、短信或电子邮件发送。

[0047] 因为该进程理解每个设备角色,所以它可以确定在两个模式中的每个模式中应当采取哪些步骤。例如,在“安全”模式下,它理解需要将业务重新路由到相邻设备、需要发生排空、并且需要为每个设备角色执行特定的健康和/或状态检查。在“混乱”模式下,进程使用相同的关系数据来监视伙伴设备、检查执行以及连接对参与角色的其余相邻设备的影响。正在执行的工作被记录并可以通过各种接口查询。由于该进程正在执行已知任务,因此它还具有抑制或确认正在由有关设备和服务器生成的警报的选项。这允许特别是在执行维护时的无噪音操作。

[0048] 在一些情况下,任务标识模块105可以标识在数据中心119内将被执行的一个或多个任务106。如上所述,任务可以包括升级数据中心119的设备120中的任意一个硬件部件、固件部件或软件应用。例如,部件或应用可以从较旧的版本被升级到较新的版本。其他任务

可能包括重启设备、关闭节点用于维护、或执行其他任务。数据中心设备120可以包括联网设备,诸如路由器、负载均衡器、防火墙和网卡。数据中心设备120还可以包括处理设备,诸如CPU、GPU和微控制器。另外,数据中心设备120可以包括存储设备,诸如硬盘驱动器、光盘驱动器、存储网络、或者作为数据中心的一部分或者可以被用在数据中心中的任何其他设备。

[0049] 计算机系统101的请求创建模块可以为标识的任务106创建请求109。请求106连同其他先前生成的请求109可以由请求存储模块111存储。请求创建模块108可以是许多部件中的一个部件,其是改变管理系统107或“改变管理者”的一部分。至少在一些实施例中,改变管理系统107可以负责创建、存储、管理、执行、和监视请求。在一些实施例中,改变管理系统107还可以负责分析遥测数据或其他数据以标识意外事件116的发生。

[0050] 在实现所创建的请求109时,请求管理模块110可以被配置为轮询请求的状态以确定在请求中被标识的任务是否可以被执行。然后,在确定所标识的任务106可以被执行时,根据请求来执行任务。因此,例如,一旦请求管理模块110确定可以执行请求(例如,因为它已经被批准或者因为之前的条件已经被满足),则请求执行模块112可以然后在数据中心119内执行请求的任务。以这种方式,请求可以确保在实现之前对数据中心所做的改变是已知的并且被批准。

[0051] 在一些实施例中,自动化工作流可以被发起(例如,通过如下面讨论的图5的工作流引擎501),该自动化工作流自动地执行由请求指定的部分工作。该自动化工作流可以使用该请求进行控制。例如,在请求109中指定的任务106可以基于请求的状态而被执行或不被执行。如果例如请求的状态被批准并且正在操作,则可以执行所标识的任务106。另一方面,如果请求的状态被停止、暂停或取消,则所标识的任务106将不被执行。以这种方式,可以通过改变请求109的状态来控制数据中心任务的执行。

[0052] 请求监视模块113可以连续地监视数据中心119内的许多不同请求的执行。在一些情况下,请求监视模块可以自动检测任务中的至少一个的执行故障,并且因此可以停止或暂停请求,使得根据请求执行的任务将被停止或暂停。因此,改变管理系统的请求监视模块113也可以能够根据执行故障将请求的操作状态从执行改变为停止、暂停或取消。

[0053] 如上所述,任务可以以包括“混乱”模式或“安全”模式的各种模式被执行。当在安全模式下根据请求执行任务时,防止有影响的改变发生。因此,由于任务不影响任务(即将影响关键系统的任务),所以系统很有可能继续正常操作而不会由于执行任务而经历故障。另一方面,请求的任务可以以混乱模式或者“有影响”模式而被执行,混乱模式或者“有影响”模式允许有影响的改变发生,甚至标识和处理特别已知有影响的请求任务。这可以完成以测试数据中心部件的弹性来确定它们是否根据策略来实际故障切换。

[0054] 一些实施例可以被配置为在各种数据中心设备上实例化软件功能。该功能可以被配置为将网络业务从这些数据中心设备转移下来并转移到其他数据中心设备上。例如,诸如路由器或负载均衡器的联网设备可以被配置为在联网设备上实例化脚本,其将网络业务从该路由器或负载均衡器转移下来并转移到另一设备上。在请求的执行期间执行的任何任务可以由请求监视模块113监视。操作状态的报告可以按照策略向被发送给用户117或其他实体。监视可能会导致与任务的执行相关联的遥测数据。然后可以使用该遥测数据来发现要在数据中心119内执行的其他任务。这些概念将在下面关于图3的方法300进行解释。

[0055] 鉴于以上描述的系统 and 架构,参照图3的流程图将更好地理解可以根据所公开的主题实现的方法。为了简化说明的目的,方法被示出并被描述为一系列的框。然而,应当理解和了解,所要求保护的主体不受框的顺序的限制,因为一些框可以以不同顺序发生和/或与来自本文描绘和描述的内容的其它框同时发生。此外,并不是可能需要所有图示的框以实现下文所述的方法。

[0056] 现在转到图3,用于自动地控制数据中心内的网络和服务质量的方法300的流程图被图示。现在利用频繁参考环境100的部件和数据来描述方法300。

[0057] 方法300包括标识在数据中心内将被执行的一个或多个任务(310)。例如,计算机系统101的任务标识模块105可以标识在数据中心119内将被执行的工作106。方法300接下来包括创建包括标识的任务的指示的、针对改变的请求(请求),其中请求109由改变管理器107来存储和管理(320)。在创建请求109时,请求监视模块113监视创建的请求的处理,并且该监视导致遥测数据114的一个或多个部分(330)。

[0058] 方法300还包括分析遥测数据以标识一个或多个意外事件(340),该一个或多个意外事件与对在请求中标识的任务的处理有关。遥测数据可以包括关于给定任务的执行的许多不同类型的信息,并且因此可以阐明与任务106的处理有关的任何意外事件。遥测数据可以包括例如警报日志数据的检查、设备状态数据的检查、网络业务性能数据的检查、警报时间、解决时间、启动设备的时间、到数据的相同性能的时间、或者修复的响应时间。

[0059] 如果分析模块115在分析遥测数据114时标识至少一个意外事件,则自动创建并存储生成的用于解决意外事件的针对改变的第二请求(350)。针对改变的第二请求可以包括在处理时处置或解决意外事件的特定任务106。因此,例如,如果意外事件是服务器升级故障,则所标识的任务可以是重新启动服务器并再次尝试更新。任务的每一步都可以被自动地执行,无需人为干预。

[0060] 例如,监视模块113可以监视正在数据中心119中处理的一个或多个请求的执行。监视可以产生遥测数据114,遥测数据114可以被用于标识与请求的处理有关的意外事件。改变管理系统107的分析模块115可以被配置为分析这种遥测数据114以标识意外事件116。意外事件可以通过将指示发生了什么的遥测数据与在请求的实现之前生成的预期事件的指示进行比较而被标识。意外的事件可以包括,例如,服务器在被重新启动后不能启动、或者软件升级比预期花费更长的时间、或者服务器在更新进程中崩溃、或者经历硬件故障、或在数据中心内执行任务时可能发生的任何数量的其他问题。

[0061] 当这种意外事件发生时,请求监视模块113可以报告这些事件,并且可以将这样的事件的指示提供给售票服务或其他实体。售票服务可用于生成后续工作命令,意味着解决导致意外事件的问题。各种电子邮件、文本或其他基于应用程序的警报可以被用来通知指定的实体意外事件已经发生。改变管理系统107还可以被配置为监视意外事件的解决时间,并且从而通知实体解决导致意外事件的问题花费了多长时间。

[0062] 如上所述,生成用于解决问题或执行其他工作的工作流的自动化过程可以以模块化的方式来实现,并且可以由公共库集合构成,所述公共库集合可以跨针对设备模型的相同类型和特定模块的所有设备模型以及角色组合使用。跨多个站点扩展的自动化针对所有设备模型和角色组合运行多个并发工作流。当发现设备不符合当前标准时,自动化触发工作流。

[0063] 由改变管理系统107执行的自动化管理各种数据中心部件之间的交互。在一个实施例中,部件包括调度和执行管理部件之间的交互的代码并且针对单独的设备部件执行自动化的工作流的工作流引擎。数据中心部件还可以包括存储关于数据中心设备的元数据的配置管理数据库(CMDB)。连接信息、当前软件级别、以及期望的软件级别是从此源取回的数据类型的一些示例。另一部件是状态数据库(例如,请求状态模块121)。通过执行自动运行任务的过程,可能被认为对以后使用或记录有价值的任何数据可以被存储在这里。状态数据库还包含要执行的工作的运行副本及其当前状态。

[0064] 改变管理系统107是请求改变的记录被存储的位置。改变管理系统提供跟踪和察看在环境中被执行的任务,并强制执行锁定期。改变管理系统107进一步允许干预来开始、停止或暂停处理所标识的任务106的自动工作流。数据中心设备120是需要动作的设备,并且自动工作流与这些设备交互以实现期望的状态。

[0065] 如图4所示,控制过程可以被提供。控制过程是在数据中心设备被发现不合规时触发其他工作流的工作流。控制过程(至少)运行四个工作流:任务监视器401、请求创建工作流402、请求状态工作流403、和补丁控制工作流404。控制过程处置控制工作流的定时和协调并在状态数据库中记录状态。这确保所有的交互保持同步,并且适当数量的设备可以跨站点被升级。

[0066] 控制过程的第一阶段是寻找需要被执行的工作。这在图5中被图示出。工作流引擎501可以发起标识工作的过程,该过程通过查询CMDB 503以找到包含不合规的成员的数据中心设备角色组而被执行。然后将这些成员被匹配到同级(peer),并按站点分类。这些信息被记录在状态数据库502中,并被传递到过程的下一阶段。

[0067] 接下来,如图6所示,请求创建工作流(在工作流引擎601上运行)查询状态数据库602以查找先前由控制工作流记录的不具有有关请求的任务。该阶段还向CMDB 603查询请求有关的细节,诸如将被应用的软件版本和类别信息。基于状态数据库中针对有关角色和数据中心的配置,估计的请求开始时间和持续时间被计算,同时避免锁定。关于现有的锁定的信息由改变系统604提供。

[0068] 图7图示了控制过程的下一阶段,该过程移动到针对状态数据库702的队列中的任何请求收集请求状态信息。这些请求可以处于排队状态(如由改变系统704指示)、等待工程师703批准、或者可能当前在工作流引擎701上进行。用于取消、关闭或完成的请求的任何数据被移动到状态数据库702中的历史表格。

[0069] 图8中所示的更新控制工作流是控制过程中的最后一步,并协调正被执行的工作。如状态数据库802中所指出的,该过程通过检查处于就绪或运行状态的队列中的请求开始。存储在状态数据库802中的配置信息指定在设备组内多少个设备可以被同时更新,以及每设备角色同时多少个设备组。工作流引擎801处理的升级控制工作流然后将该信息与队列中的运行状态进行比较,并确定新的设备是否可以被启动。

[0070] 如果请求被暂停,则无论当前运行状态如何,都不启动新设备。当开始新设备升级时,设备基于设备类型和角色而被匹配到正确的工作流,并且改变系统803被通知升级。升级控制工作流还监视在状态数据库802中记录的任何故障。如果检测到故障,则这指示存在遇到的意外情况,并且针对该请求的任何附加工作将被停止,直到故障的原因可以被调查。

[0071] 一旦工作流已经被特定设备的控制过程触发,该工作流的职责是将通信处置回到

状态数据库。如图9所示,角色 workflow 903 包含执行针对该特定设备类型以及其在环境中执行的角色的更新的步骤和指令。该逻辑包含伙伴设备的知识以及如何平衡地执行设备的更新。

[0072] 在需要的情况下,设备特定角色 workflow 903 可以利用用于与跨所有设备类型的常用系统(即,监视系统、售票等)交互的核心模块 905 的共享库。由于设备类型可以跨多个角色,所以角色 workflow 还可以调用可以在角色之间共享的设备特定模块 901。设备特定模块可能包括特定于特定设备操作系统的可重用 workflow,并执行常见功能。例如,更新的安装对于具有相同操作系统的所有设备可以是相同的。角色特定 workflow 对于特定设备被实现的方式是专用的。例如,设备模型可能被配置为角色中的单个实体,但是可以被配置为另一角色中的完全冗余对,并且因此将需要用于更新过程的其自己的唯一指令。

[0073] 一旦完成,成功状态被记录在状态数据库 904 中。如果在升级过程中存在遇到的错误,则该状态也将指示故障。以这种方式记录的故障将信号传送控制过程 902 以停止处理用于正被执行的特定请求的其他设备,并允许手动调查。图 10 图示了正在运转的角色特定 workflow 的示例,在角色特定 workflow 中工作引擎 1001、状态数据库 1002、CMDB 1003 和一个或多个数据中心设备 1004 进行交互以确保设备更新被成功执行并被适当地记录在系统中。

[0074] 权利要求支持:在一个实施例中,提供了一种在包括至少一个处理器的计算机系统处实现的、用于自动地控制数据中心内的网络和服务的方法。该方法包括:标识在数据中心 119 内将被执行的任务 106,创建包括所标识的任务的指示的、针对改变的请求 109,该请求由改变管理器 107 来存储和管理,一旦创建请求,监视创建的请求的处理,所述监视导致遥测数据 114 的一个或多个部分,分析遥测数据,以标识一个或多个意外事件 116,该一个或多个意外事件 116 与对在请求中标识的任务的处理有关,以及在标识出至少一个意外事件时,存储生成的用于解决意外事件的针对改变的第二请求。

[0075] 该方法进一步包括生成自动地执行所述任务的自动化 workflow,所述任务在由该请求指定的数据中心内将被执行。该方法还包括使用请求来控制自动化 workflow,使得标识的任务基于请求的状态而被执行或不被执行。控制自动化 workflow 包括以下至少一项:使用请求停止自动化 workflow、暂停自动化 workflow、和取消自动化 workflow 中。

[0076] 该方法进一步包括生成解决意外事件的针对改变的第二请求,针对改变的第二请求包括一个或多个特定任务,该特定任务当被处理时处置该意外事件。所标识的任务包括执行软件或固件升级。在一些情况下,该方法进一步包括自动地检测所标识的任务的执行已经发生故障,并且停止或暂停该请求,使得根据该请求所标识的任务的执行将被停止或暂停。该方法还包括实例化在至少一个数据中心设备上的功能的一部分,该功能将网络业务从数据中心设备转移下来并转移到另一数据中心设备上的,并且将作为该请求的一部分处理的任务的状态报告给至少一个实体。

[0077] 在另一实施例中,提供了一种计算机系统,其包括至少一个处理器;工作部件 105,被配置为标识在数据中心 119 内将被执行的任务 106;改变管理部件 107,被配置为创建针对改变的请求 109 以执行任务,改变管理部件被配置为存储和管理数据中心内的请求的实现;监视部件 113,在确定请求已经被创建之后,监视请求的处理,监视导致遥测数据 114 中的一个或多个部分;遥测部件 115,用于分析遥测数据以标识与请求的处理有关的一个或多个意外事件 116;以及数据存储装置 119,用于在标识出至少一个意外事件时,存储生成的用于解

决意外事件针对改变的第二请求,针对改变的所述第二改变请求包括一个或多个特定的任务,其在被处理时处置意外事件。

[0078] 遥测数据包括以下至少一项:警报日志数据的检查、设备状态数据的检查、网络业务性能数据的检查、警报时间、解决时间、启动设备的时间、到数据的相同性能的时间或用于维修的响应时间。计算机系统还在针对改变的请求的实现之前生成预期事件的指示。

[0079] 在另一实施例中,提供了一种用于实现用于跨数据中心自动地控制网络和服务质量的方法的计算机程序产品,所述计算机程序产品包括一个或多个计算机可读存储介质,在所述一个或多个计算机可读介质上存储有计算机可执行指令,所述计算机指令当由计算系统的一个或多个处理器执行时,使得计算系统执行该方法。该方法包括标识在数据中心119内将被执行的任务106,访问包括所标识的任务的指示的、针对改变而生成的请求109,所述请求由改变管理服务107来存储和管理,在访问请求时,监视创建的请求的执行,所述监视导致遥测数据114的一个或多个部分,分析遥测数据以标识一个或多个意外事件116,该一个或多个意外事件116与在所访问的请求中标识的任务的处理有关,在标识出至少一个意外的事件时,生成用于解决意外事件的、针对改变的第二请求,并存储针对改变的第二请求。

[0080] 该计算机程序产品进一步包括,在标识出至少一个意外事件时,创建包括解决意外事件的一个或多个自动实现的任务的自动化 workflow。更进一步,计算机程序产品包括标识意外事件的解决时间以及监视以确定在意外事件被解决之前的实际时间长度。

[0081] 因此,提供了跨数据中心和数据中心设备的自动地控制网络和服务质量的方法、系统和计算机程序产品。

[0082] 在不脱离其精神或描述特征的情况下,本文所描述的概念和特征可以以其他具体形式来实施。所描述的实施例在所有方面仅被认为是说明性的而不是限制性的。因此,本公开的范围由所附权利要求而不是由前面的描述来指示。在权利要求的等同物的含义和范围内的所有改变均将被包括在其范围内。

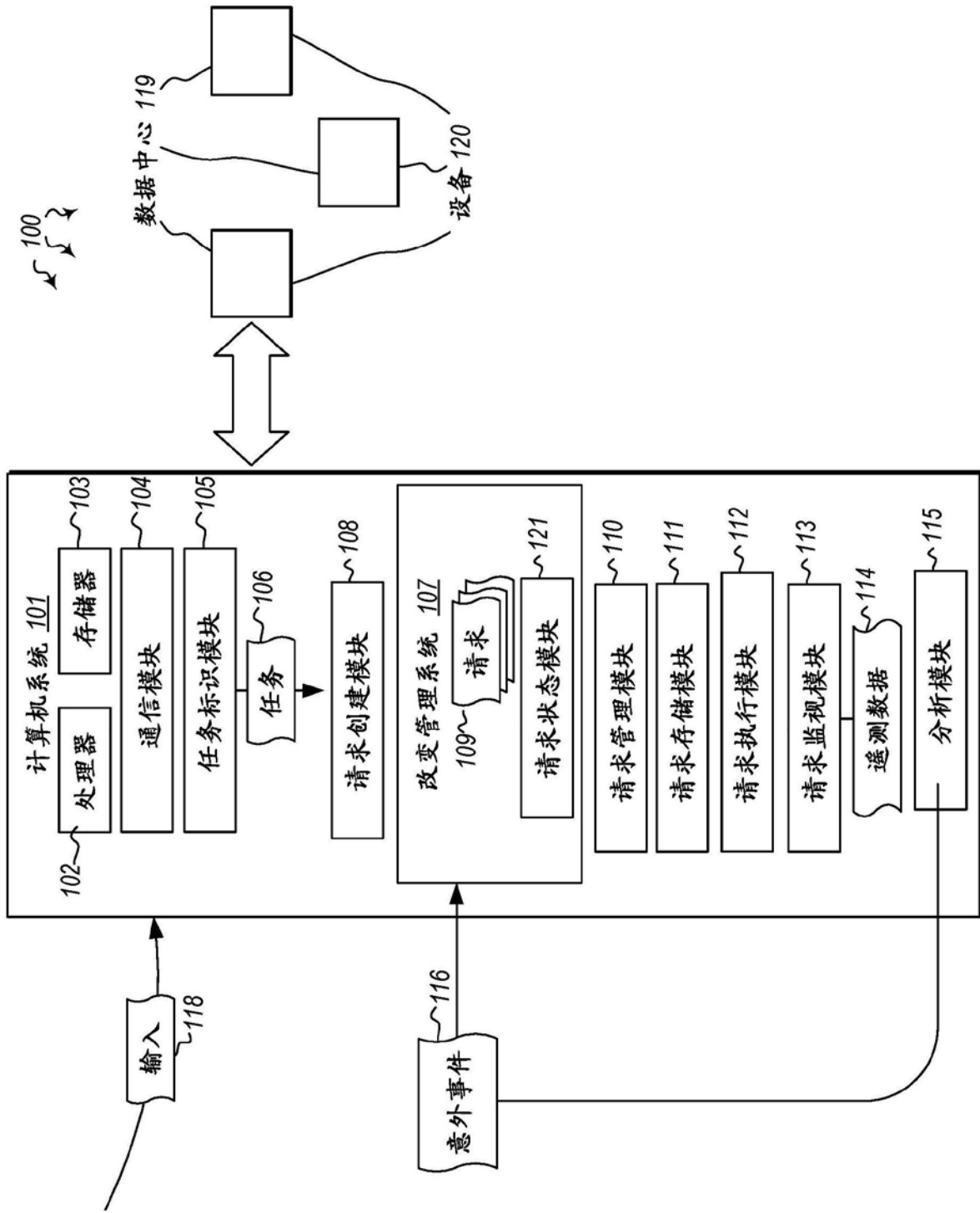


图1

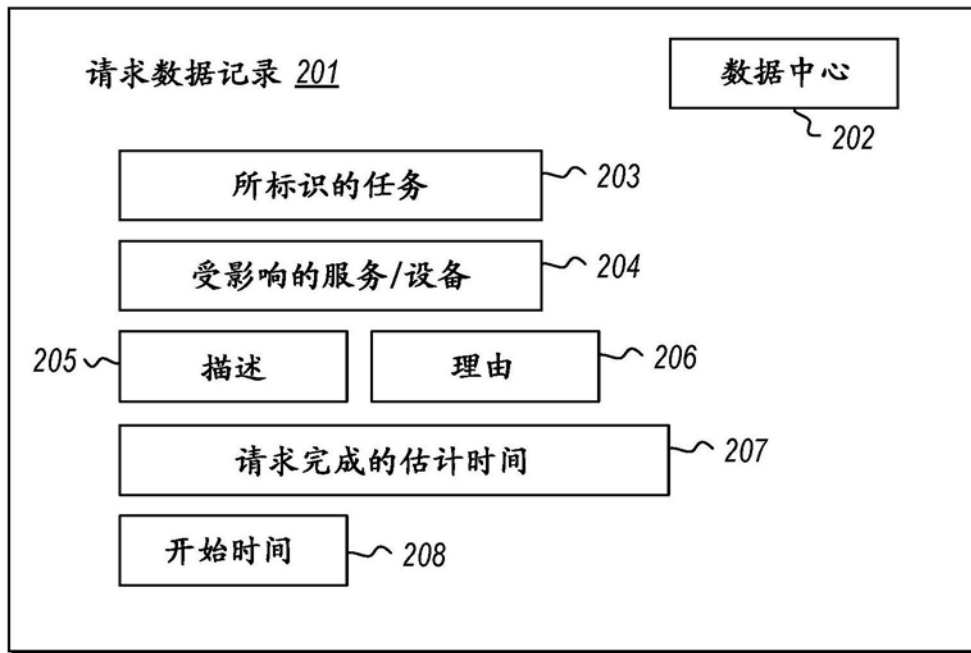


图2



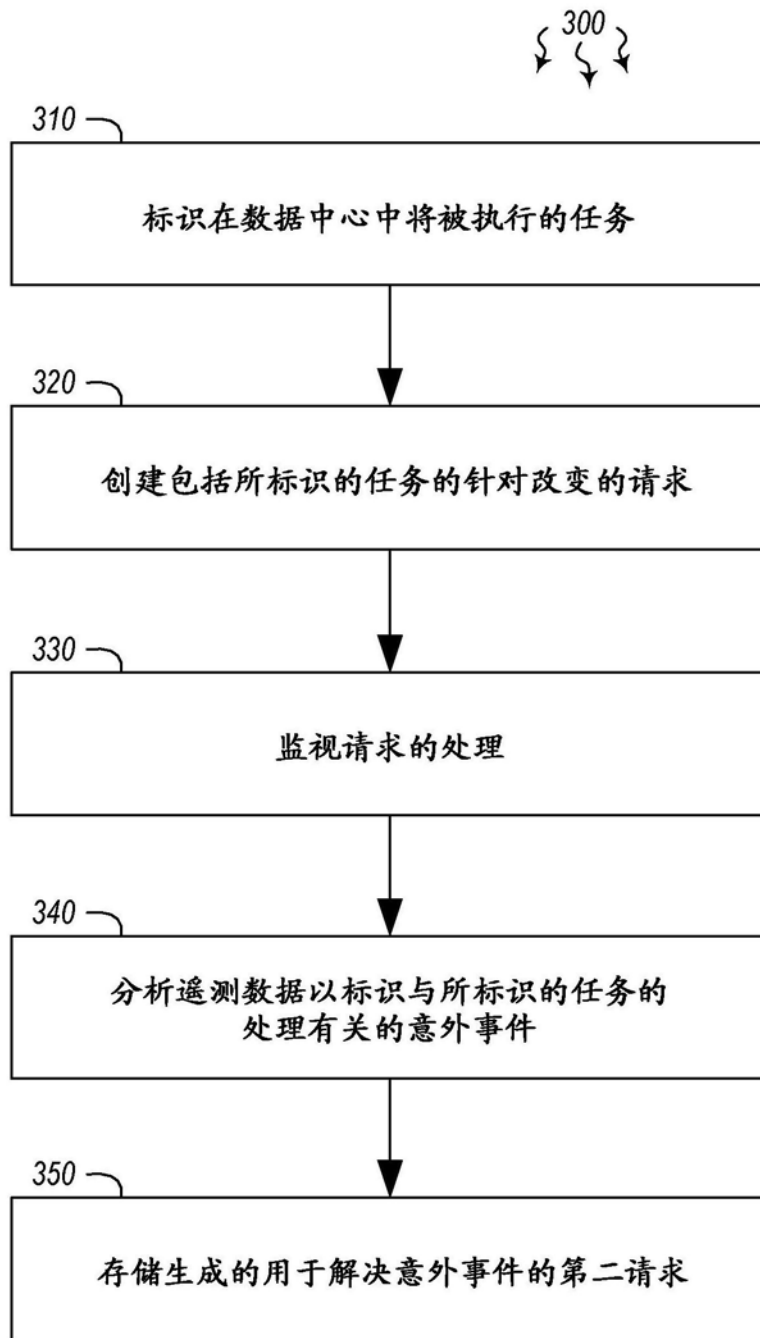


图3

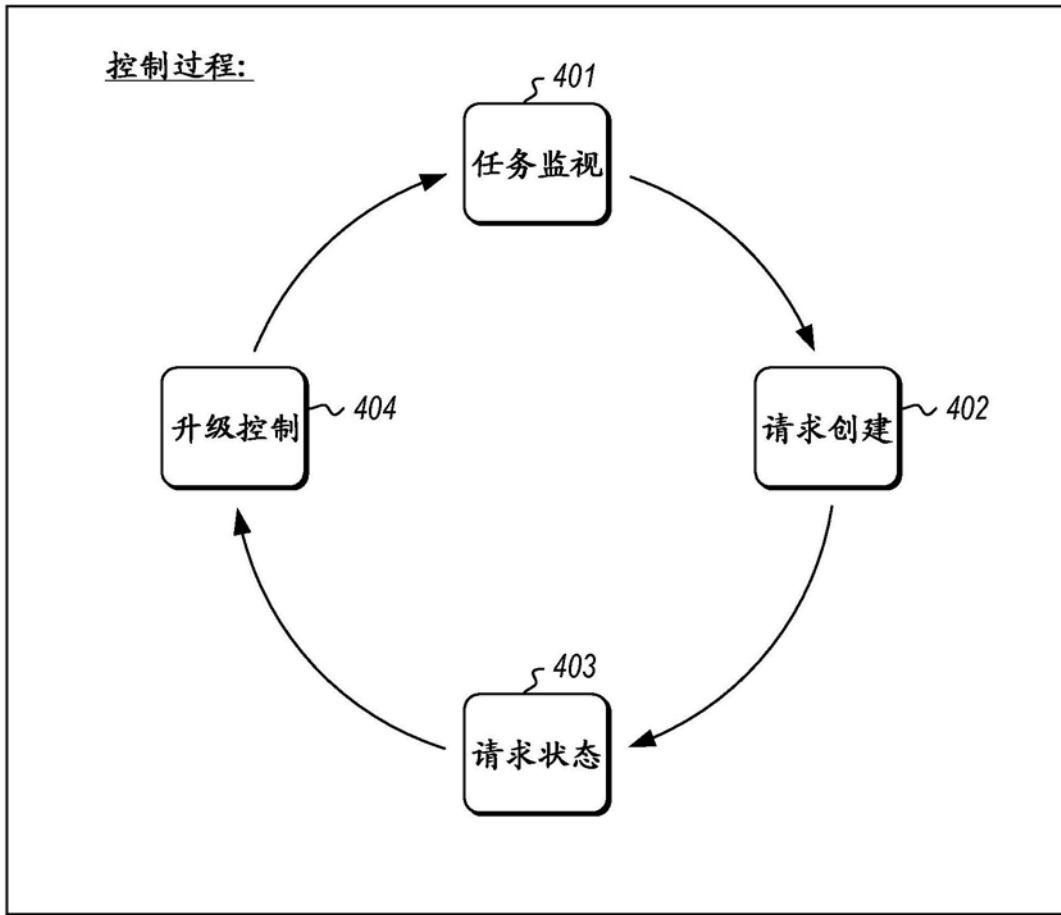


图4

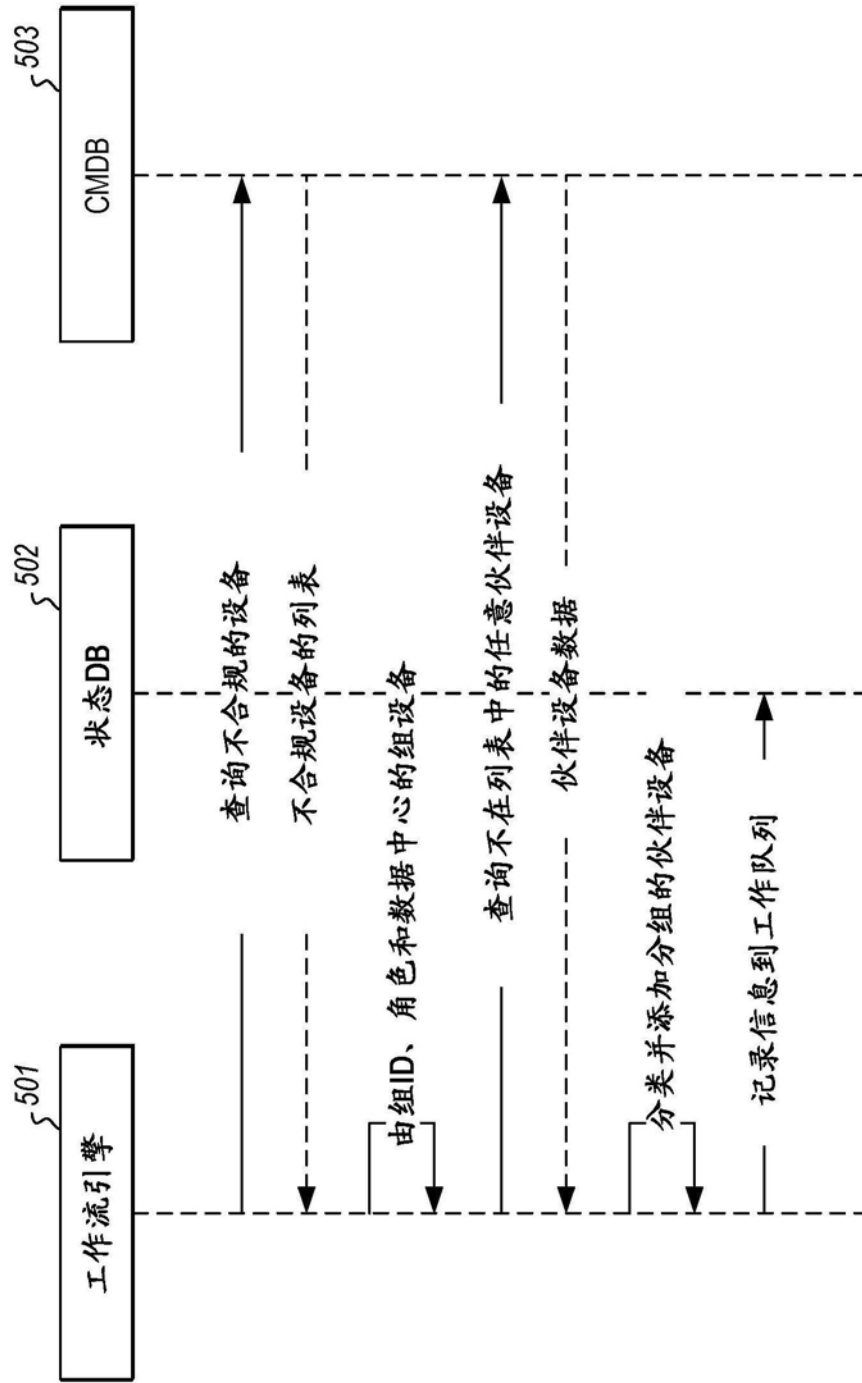


图5

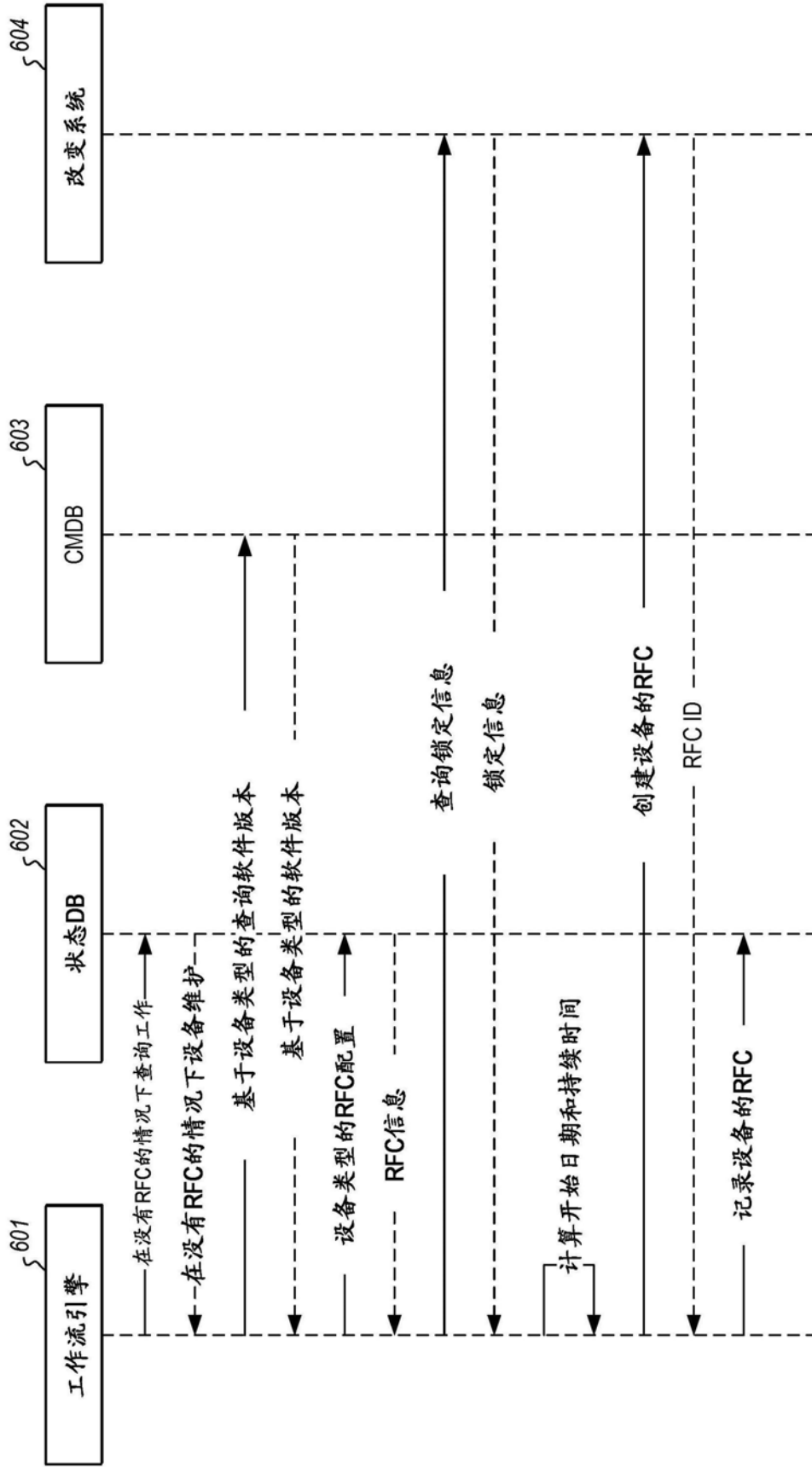


图6

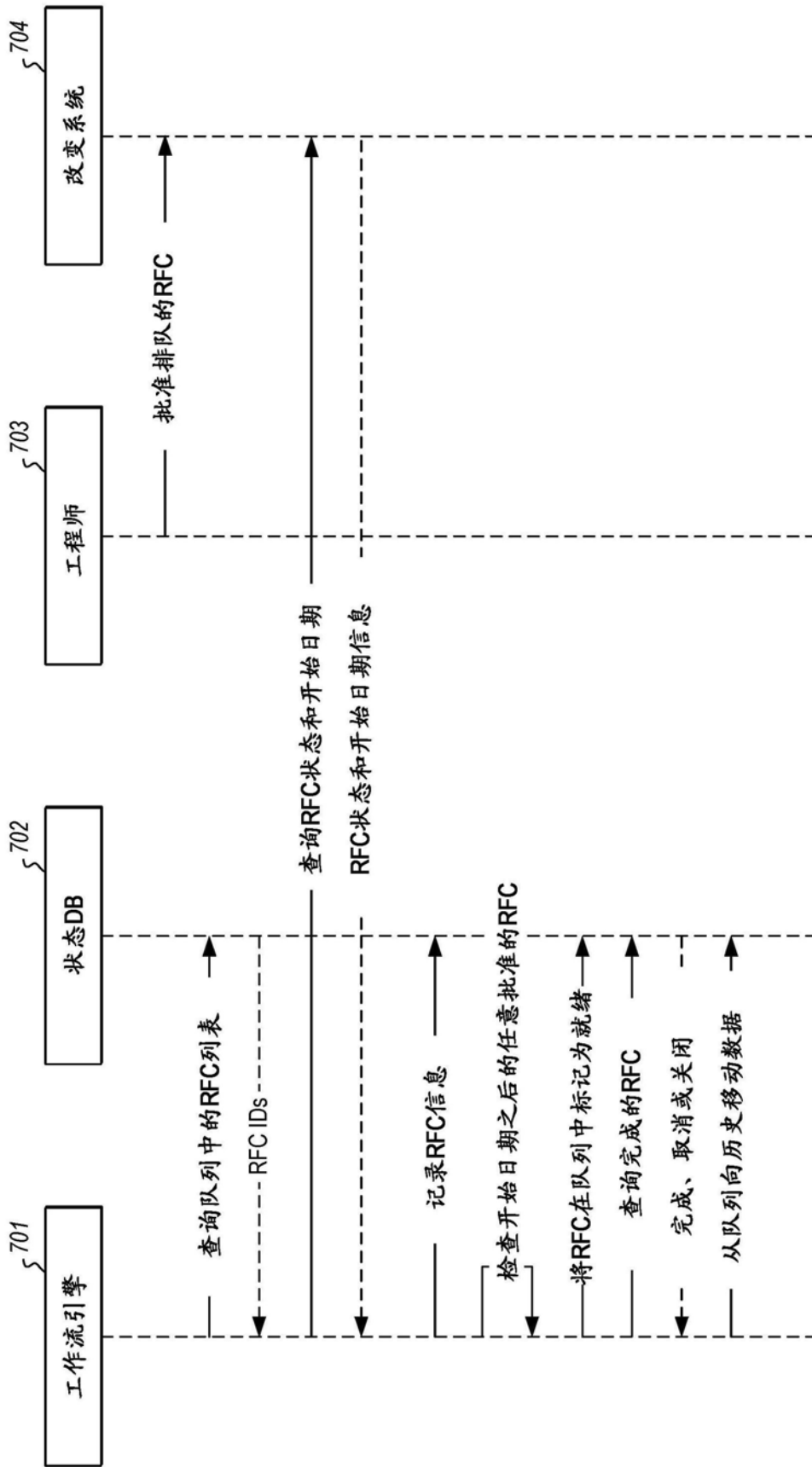


图7

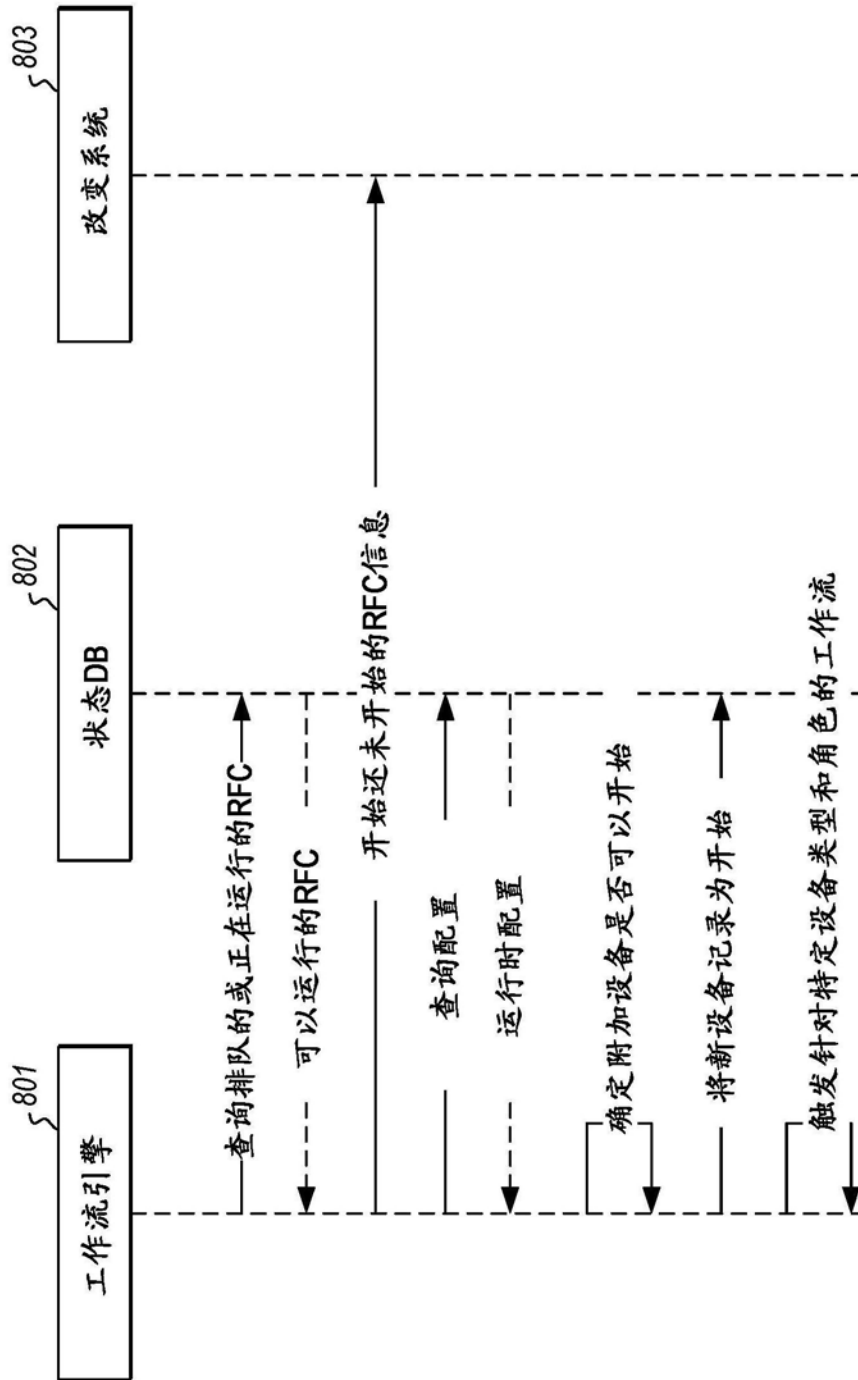


图8

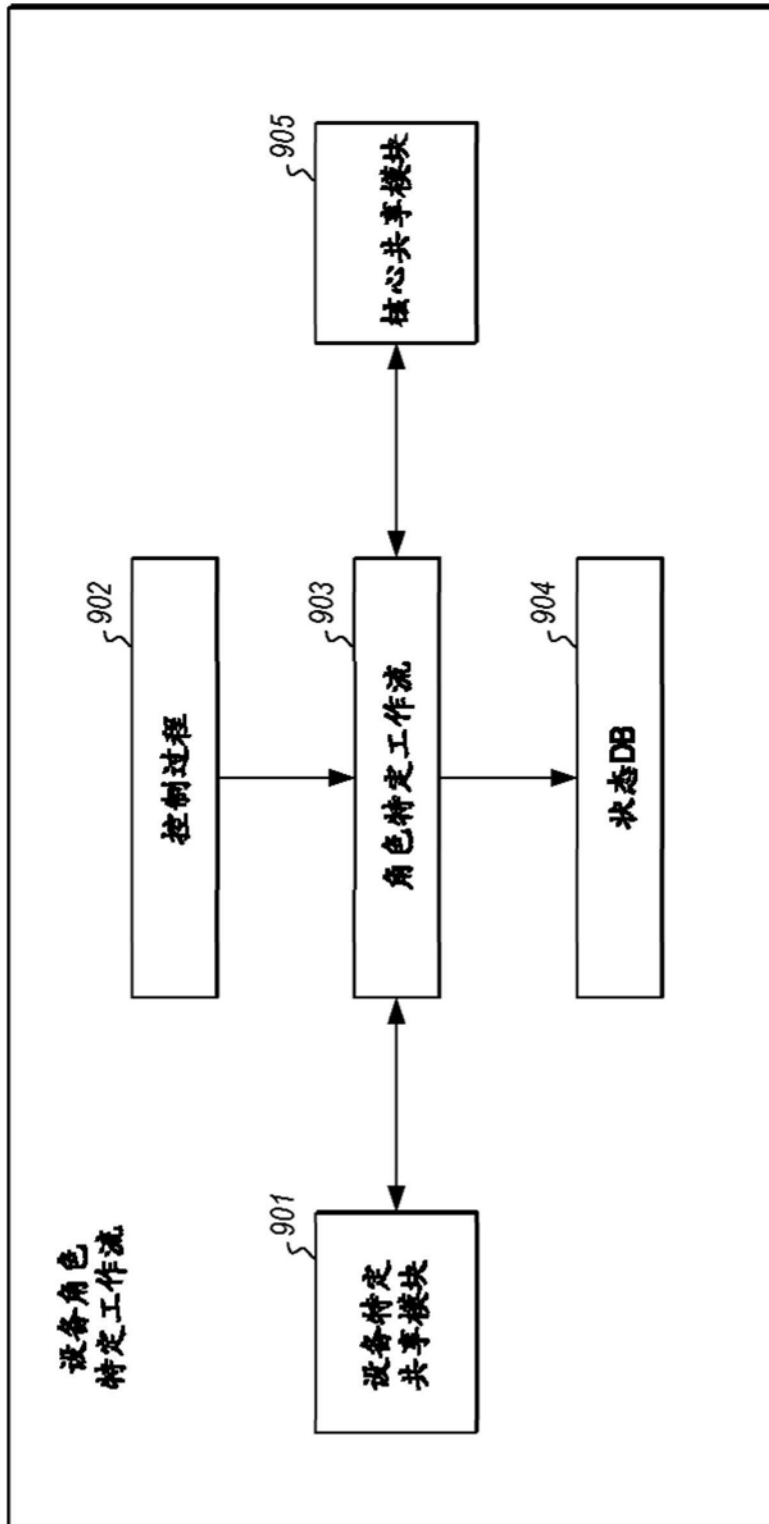


图9

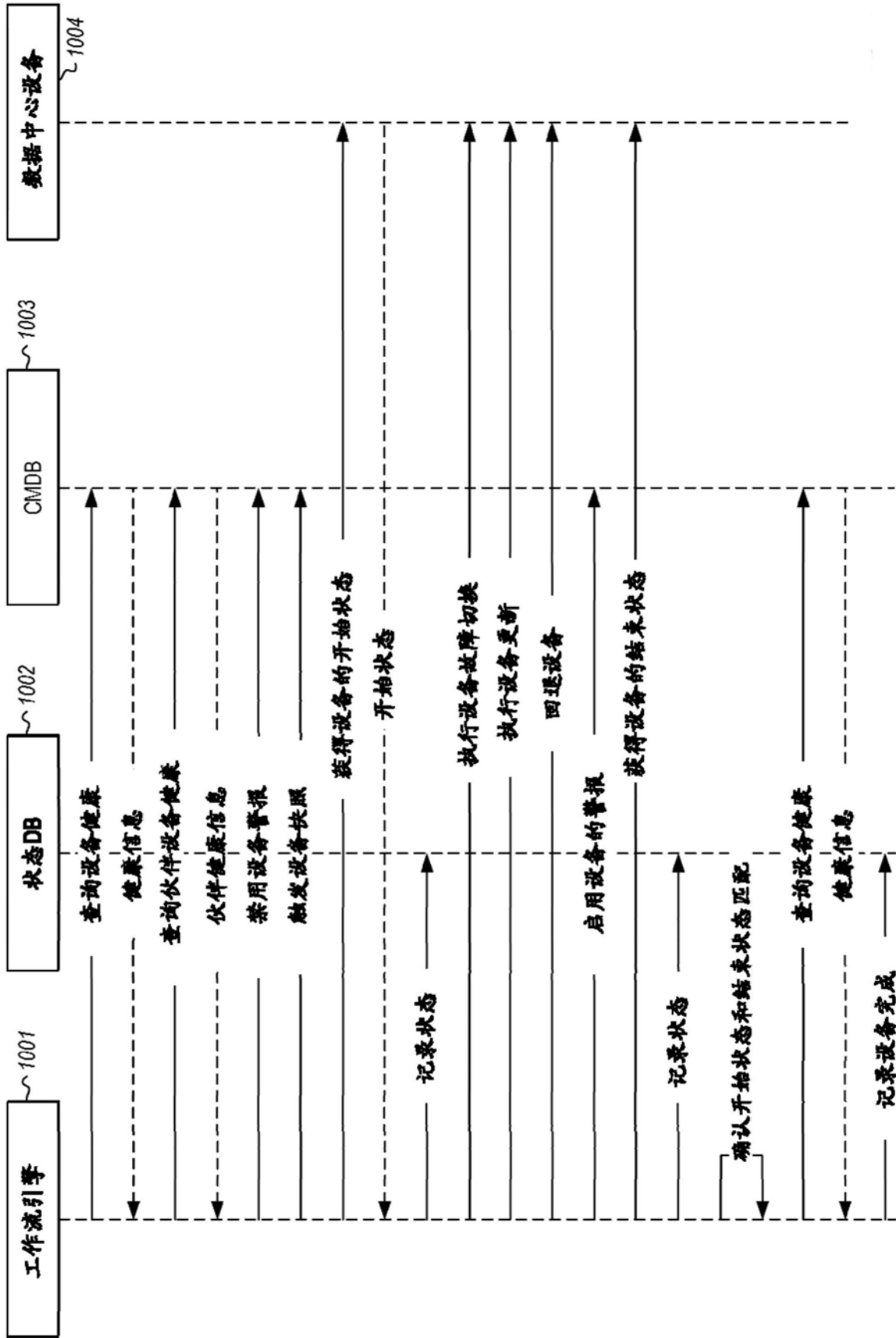


图10