(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 107783530 B
(45)授权公告日 2020.12.01

(21)申请号 201710728185.1

(22)申请日 2017.08.22

(65)同一申请的已公布的文献号
申请公布号 CN 107783530 A

(43)申请公布日 2018.03.09

(30)优先权数据
15/246793 2016.08.25 US

(73)专利权人 通用汽车环球科技运作有限责任公司
地址 美国密歇根州

(72)发明人 S•萨米

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 刘桢 安文森

(51)Int.Cl.
G05B 23/02(2006.01)

审查员 张姗姗

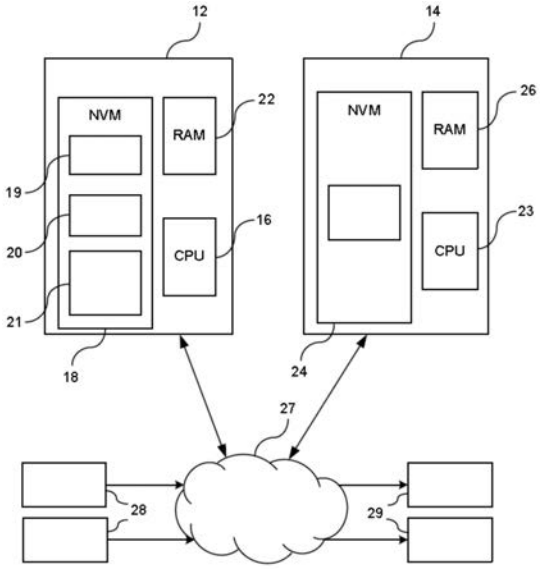
权利要求书1页 说明书5页 附图3页

(54)发明名称

基于软件代码迁移的失效可操作的系统设计模式

(57)摘要

一种失效可操作的控制系统包括迁移控制器,迁移控制器具有非易失性存储器、RAM、以及CPU。迁移控制器包括储存在迁移控制器的非易失性存储器中的软件代码。由迁移控制器的CPU执行的、储存在迁移控制器的非易失性存储器中的软件代码专用于相应系统。相应系统不在来自另一系统的主控制器的控制下。响应于在系统操作的执行期间需要备用控制器的另一系统的主控制器的系统操作的启动,将储存在另一系统的主控制器的非易失性存储器中的失效可操作的软件代码转移至迁移控制器的RAM。迁移控制器在另一系统的主控制器中的系统操作的执行期间临时用作备用控制器。



CN 107783530 B

1.一种失效可操作的控制系统,其包括:

主控制器,所述主控制器包括非易失性存储器以及用于执行储存在所述主控制器的所述非易失性存储器中的软件代码的中央处理单元,储存在所述主控制器的所述非易失性存储器中的所述软件代码包括在非失效状态和失效状态期间由所述主控制器的所述中央处理单元执行的非关键软件和失效可操作的软件;

迁移控制器,所述迁移控制器包括非易失性存储器、随机存取存储器、以及中央处理单元,所述迁移控制器包括储存在所述迁移控制器的所述非易失性存储器中的软件代码,由所述迁移控制器的所述中央处理单元执行的、储存在所述迁移控制器的所述非易失性存储器中的所述软件代码专用于相应系统,所述相应系统不在所述主控制器的控制下;

其中,响应于在系统操作的执行期间需要备用控制器的所述主控制器的所述系统操作的启动,将储存在所述主控制器的所述非易失性存储器中的与所述系统操作有关的失效可操作的软件代码转移至所述迁移控制器的所述随机存取存储器,其中,所述迁移控制器在所述主控制器中的所述系统操作的所述执行期间临时用作备用控制器。

2.根据权利要求1所述的失效可操作的控制系统,其进一步包括通信网络,其中,储存在所述主控制器的所述非易失性存储器中的所述失效可操作的软件代码经由所述通信网络被转移至所述迁移控制器的所述随机存取存储器。

3.根据权利要求1所述的失效可操作的控制系统,其中,当所述主控制器中的所述系统操作被启动时,所述失效可操作的软件代码的转移是从所述主控制器的所述非易失性存储器转移至所述迁移控制器的所述随机存取存储器。

4.根据权利要求1所述的失效可操作的控制系统,其中,当禁止所述系统操作时,重新配置为用作备用控制器的所述迁移控制器从所述随机存取存储器中移除所述失效可操作的软件代码。

5.根据权利要求1所述的失效可操作的控制系统,其中,响应于所述主控制器中的失效,所述迁移控制器通过执行储存在所述随机存取存储器中的所转移的失效可操作的软件代码来用作指定主控制器。

6.根据权利要求1所述的失效可操作的控制系统,其中,所述失效可操作的软件代码所转移至的所述迁移控制器选自多个控制器。

7.根据权利要求6所述的失效可操作的控制系统,其中,基于所述迁移控制器当前是否在执行用于所述迁移控制器所专用的所述系统的软件代码来选择所述迁移控制器。

8.根据权利要求6所述的失效可操作的控制系统,其中,基于储存在所述迁移控制器的所述非易失性存储器中的所述软件代码是否与所述主控制器的所述失效可操作的软件代码有关来选择所述迁移控制器。

9.根据权利要求1所述的失效可操作的控制系统,进一步地,其中,所述迁移控制器响应于在所述主控制器中检测到的失效来执行从所述主控制器转移的并且储存在所述随机存取存储器中的所述软件代码。

10.根据权利要求9所述的失效可操作的控制系统,其中,所述迁移控制器执行储存在所述迁移控制器的所述非易失性存储器中的与所述迁移控制器的指定系统有关的所述软件代码的至少一部分,同时响应于所述检测到的失效而执行来自所述主控制器的储存在所述随机存取存储器中的软件代码。

基于软件代码迁移的失效可操作的系统设计模式

技术领域

[0001] 实施例涉及容错控制系统。

背景技术

[0002] 提供安全功能的系统通常使用冗余控制器通过关闭已经经历故障或者失效的功能来确保安全。这种系统被称为失效沉默系统。如果检测到故障，则关闭特征的控制装置并且该特征在系统中将不再可操作。

[0003] 一些系统试图使用失效可操作的系统来实施控制系统，其中，附加控制器用于确保可以继续进行一段时间的安全操作，诸如，双重双控制器。如果第一控制器失效并且陷入沉默，则第二控制器将被激活并且所有致动器将转换至依靠来自第二控制器的请求。使用非对称实施的控制器的其它类型的系统可以避免重复的硬件和软件故障。然而，在任一种情况下，使用专门用于仅仅作为主控制器的备用控制器的第二控制器是无效的，并且就资源使用(例如，存储器或者CPU使用)而言可能成本更高。

发明内容

[0004] 实施例的优点在于备用控制器的使用，备用控制器通过将执行软件从主控制器的非易失性存储器迁移至备用控制器的随机存取存储器来减小备用控制器的非易失性存储器。将软件代码迁移至备用控制器减小了在电子控制单元的失效可操作的架构中的非易失性存储器要求的使用，这也降低了成本并且增加了处理器设计的效率。该技术在启动和增加控制器整合时优化非易失性构件，从而降低部件成本。

[0005] 实施例设想了失效可操作的控制系统。主控制器包括非易失性存储器以及用于执行储存在主控制器的非易失性存储器中的软件代码的中央处理单元。储存在主控制器的非易失性存储器中的软件代码包括在非失效状态和失效状态期间由主控制器的中央处理单元执行的非关键软件和失效可操作的软件。迁移控制器包括非易失性存储器、随机存取存储器、以及中央处理单元。迁移控制器包括储存在迁移控制器的非易失性存储器中的软件代码。由迁移控制器的中央处理单元执行的、储存在迁移控制器的非易失性存储器中的软件代码专用于相应系统。该相应系统不在主控制器的控制下。响应于在系统操作的执行期间需要备用控制器的主控制器的系统操作的启动，将储存在主控制器的非易失性存储器中的与该系统操作有关的失效可操作的软件代码转移至迁移控制器的随机存取存储器。迁移控制器在主控制器中的系统操作的执行期间临时用作备用控制器。

[0006] 实施例设想了失效可操作的控制系统。迁移控制器包括非易失性存储器、随机存取存储器、以及中央处理单元。迁移控制器包括储存在迁移控制器的非易失性存储器中的软件代码。由迁移控制器的中央处理单元执行的、储存在迁移控制器的非易失性存储器中的软件代码专用于相应系统。该相应系统不在来自另一系统的主控制器的控制下。响应于在系统操作的执行期间需要备用控制器的另一系统的主控制器的系统操作的启动，将储存在另一系统的主控制器的非易失性存储器中的失效可操作的软件代码转移至迁移控制器

的随机存取存储器。迁移控制器在另一系统的主控制器中的系统操作的执行期间临时用作备用控制器。

[0007] 一种用于重新配置用于失效可操作的条件的控制器的方法。迁移控制器被选择用于在来自另一系统的主控制器的失效期间转移失效可操作的软件代码。迁移控制器不再主控制器所控制的另一系统的主控制器的控制下。在主控制器的系统操作的执行期间，启动要求备用控制器的主控制器的系统操作。将主控制器的非易失性存储器中的失效可操作的软件代码转移至迁移控制器的随机存取存储器。迁移控制器包括储存在迁移控制器的非易失性存储器中的、专用于与主控制器所控制的系统不同的另一系统的软件代码。在主控制器中检测到故障。响应于在主控制器中检测到故障，在迁移控制器的随机存取存储器中执行失效可操作的软件代码。

附图说明

[0008] 图1是集成的失效沉默和失效可操作的控制系统的架构框图。

[0009] 图2是用于将失效可操作的特征软件从主控制器迁移至另一特征控制器的流程图。

[0010] 图3图示了示出了至另一特征控制器的RAM的软件迁移的框图。

[0011] 图4图示了两个控制器中的软件迁移和重新配置的时间线。

具体实施方式

[0012] 如下详细描述意在进行图解说明以理解实施例的主题，并且不意在限制主题的实施例或者这些实施例的应用和使用。词语“示例性的”的任何使用均意在被理解为“用作示例、实例、或者图例”。本文所陈述的实施方式是示例性的并且不意在被理解为比其它实施方式优选或者有利。本文的描述不意在受到在前述背景技术、详细描述或者说明书、发明内容、或者如下具体实施方式中所呈现的任何明示的或者暗示的理论的约束。

[0013] 本文可以按照功能块部件和/或逻辑块部件、并且参照可以由各个计算部件或者装置执行的操作、处理任务、以及功能的象征代表来对技巧和技术进行描述。这些操作、任务、以及功能有时被称为是计算机执行的、计算机化的、软件实施的、或者计算机实施的。应理解，附图中示出的各个块部件可以由配置为执行指定功能的任何数量的硬件、软件、以及/或者固件部件来实现。例如，系统或者部件的实施例可以采用各种集成电路(例如，存储器元件、数字信号处理元件、逻辑元件、查阅表等，其可以在一个或多个微处理器或者其它控制装置的控制下执行各种功能)。

[0014] 当在软件中进行实施时，本文所描述的系统的各个元件基本上是执行各个任务的代码段或者计算机可执行指令。在某些实施例中，程序或者代码段被储存在有形处理器可读介质中，有形处理器可读介质可以包括可以储存或者转移信息的任何介质。非暂时性和处理器可读介质的示例包括电子电路、微控制器、专用集成电路(ASIC)、半导体存储装置、ROM、闪存存储器、可擦ROM(EROM)、软磁盘、CD-ROM、光盘、硬盘等。

[0015] 本文所描述的系统和方法学可以用于维持在控制系统中执行软件功能的控制器中的安全控制功能。尽管下文参照车辆应用中所使用的控制器对方法和方法学进行了描述，但本领域的普通技术人员会理解，汽车应用仅仅是示例性的，并且本文所公开的概念也

可以应用至任何其它合适的通信系统，诸如，例如，通用工业自动化应用、制造和装配应用、航空电子学、航空航天、以及游戏。

[0016] 本文所描述的术语“车辆”可以被广义地理解为不仅包括乘用车，而且包括任何其它车辆，包括但不限于：铁路系统、飞机、越野运动车辆、机器人车辆、摩托车、卡车、运动型多用途车(SUV)、休闲车(RV)、海洋船舶、航空器、农用车辆、以及施工车辆。

[0017] 图1中示出了示例性集成控制系统的架构框图。这种控制系统通常使用两个控制器，从而如果主控制器发生硬件错误，则备用控制器可以容易地被启动以控制该控制系统的特征或者为错误特征的有限功能提供控制。

[0018] 图1中示出了集成失效可操作的控制系统的架构框图。如果控制系统(包括但不限于：使用安全临界系统或者自治系统的车辆、飞机、以及船舶)内发生错误，则该控制系统需要容错对抗措施。这种控制系统通常使用两个控制器，从而如果主控制器发生错误(由于故障所导致)，则备用控制器可以容易地被启动以控制该控制系统的特征或者为错误特征的有限功能提供控制。

[0019] 在图1中，示出了包括主控制器12和其它特征控制器14(例如，迁移控制器)的相应系统。如本文所描述的示例性系统是基于车辆，但如早前所描述的，该架构可以应用至非车辆系统。主控制器12包括用于执行软件的至少一个中央处理单元(CPU)16。主控制器12进一步包括用于储存非关键软件19、失效沉默软件20、以及失效可操作的软件21的非易失性存储器(NVM)18。用于在非故障条件期间和在故障条件期间执行软件的所有操作指令都被储存在主控制器12的NVM 18中。主控制器12进一步包括用于存取临时储存的其它数据或者指令的RAM 22。

[0020] 其它特征控制器14包括类似架构，该类似架构包括至少一个CPU 23、NVM 24、以及RAM 26。其它特征控制器14是专用于另一系统或者由多个系统共享的控制器。在具有专用于当前系统的备用控制器的常规系统中，专用的备用控制器将在NVM中具有用于在非失效状态和失效状态期间执行操作的相同操作软件、以及非关键软件、失效沉默软件、以及失效可操作的软件。如本文所描述的，其它特征控制器14专用于另一系统或者由另一系统共享。如果主控制器的NVM不能储存附加指令(即，失效可操作的备用软件)，则将需要附加指定控制器，或者另一特征控制器将需要升级为具有附加NVM存储器(否则该附加NVM存储器将不可用)。

[0021] 为了克服该问题，在其它特征控制器14上执行软件代码迁移和重新配置。如果主控制器12中发生失效，则将主控制器12的失效可操作的软件转移至其它特征控制器14的RAM 26以便允许其它特征控制器14控制失效系统的操作。

[0022] 使用通信网络27，通信网络27允许主控制器12和其它特征控制器14彼此进行通信并且将软件代码从主控制器12的NVM 18转移至其它特征控制器14的RAM 26。应理解，通信网络可以包括但不限于：通信区域网络(CAN)、CAN-FD、FlexRay、以太网切换网络、无线通信、或者使用网关的多个网络。通信网络27允许各个控制和传感器/致动器彼此进行通信。主控制器12和其它特征控制器14还使用通信网络27来在传感器28与致动器29之间接收和传递数据。

[0023] 图2图示了关于将软件迁移至其它特征控制器的流程图。在框51中，启动需要备用控制器的系统特征。这种系统的示例包括但不限于：自适应巡航控制、自主泊车、以及车道

定中。

[0024] 在框52中，响应于在主控制器发生失效的情况下需要备用控制器的系统操作的启动，将软件代码从主控制器迁移至其它特征控制器的RAM。其它特征控制器的非易失性存储器具有用于另一专用系统的软件代码。从主控制器传递至其它特征控制器的并且被储存在其它特征控制器的RAM中的软件代码将保持被储存在其它特征控制器的RAM中直到当前启动的特征操作被禁止。

[0025] 在步骤53中，执行用于系统特征的其它特征控制器的重新配置。这可以包括：停止其它特征的一些或者所有的执行以便允许失效可操作的备份变得可操作并且作为热备份进行操作。只要其它特征不是需要在被储存在RAM中且在RAM中被执行的其它特征接合且可操作时被执行的关键软件，这就是可接受的。

[0026] 在步骤54中，确定主控制器中是否发生失效。如果未发生失效，则例程前进至步骤56，如若不然，则例程前进至步骤55。

[0027] 在步骤55中，响应于在主控制器中检测到的失效，其它特征控制器执行储存在其它特征控制器的RAM中的软件代码。其它特征控制器维持系统特征的操作直到系统特征完成或者直到驾驶员可以恢复控制自主操作。如果除了主控制器之外在其它特征控制器中也检测到故障，则主控制器可以检测到该故障并且立即采取行动，诸如，警告驾驶员立即控制该操作或者自主地移动至安全区域(例如，路边)并且致动各个安全特征(包括但不限于警报信号)。

[0028] 在步骤56中，在系统特征安全失活时，从RAM中移除软件代码。如果激活了需要备用控制器的下一系统特征，则其它特征控制器(如果可用的话)可以用作备用控制器，其中，将软件代码迁移和储存在RAM中。

[0029] 应理解，不只一个特征控制器可以用作备用控制器。在这种情况下，可以基于可用性来选择相应控制器。即是说，如果控制器当前由其专用系统使用并且不能用作备用控制器，则这时可以选择可用的另一特征控制器。

[0030] 图3图示了框图，该框图示出了主控制器12、其它特征控制器14、以及储存在相应分配存储器中的相应软件代码。

[0031] 主控制器12是，例如，用于检测对象和避免碰撞的外部对象计算模块(EOCM)控制器。软件代码被永久地储存在主控制器12的NVM 18中。管理相应特征的各类软件代码被识别为与失效可操作的特征或者失效沉默或者非关键特征有关。用于失效沉默或者非关键特征的软件的示例包括碰撞规避软件60和地图/HMI软件62。用于失效可操作的特征的软件的示例包括态势感知软件64、自适应巡航控制软件66、车辆动态软件68、以及车道定中控制软件70。

[0032] 其它特征控制器14是，例如，用于处理来自车辆的各个视频装置的视频的视频处理模块(VPM)控制器。软件代码被永久地储存在主控制器12的NVM 24中以控制视频处理操作。储存在NVM 24中的软件代码的类型包括：视频处理软件72、行人检测软件74、周围视图软件76、泊车辅助软件78、夜视软件80、以及车道感测软件82。这些软件代码专用于VPM以由VPM控制器执行处理。NVM 24包括用于视频处理的专用软件，而来自EOCM控制器的软件则经由通信网络27被迁移至并且储存在VPM控制的RAM 26中。如所示出的，仅仅将与EOCM的失效可操作的特征有关的软件转移至VPM控制器的RAM 26，其包括态势感知软件64、自适应巡航

控制软件66、车辆动态软件68、以及车道定中控制软件70。在主控制器12中的失效的情况下，将控制让渡给其它特征控制器14，其中，与储存在RAM 26中的失效可操作的特征有关的相应软件代码由其它特征控制器14的CPU 22执行。

[0033] 因此，通过不必维持双重控制器(其在等待主控制器中的失效的备用模式中被指定为备用控制器)，可以减小成本、部件(包括通信线路)以及复杂性。

[0034] 图4图示了用于在每个控制器中执行软件代码的时间线。时间线92表示用于主控制器的控制器处理，而时间线94表示用于备用控制器的控制器处理。在时间t_0处，两个控制器处理储存在其相应NVM中的软件以监测和操作其相应系统。在主控制器中，如时间线92上示出的96所代表的特征执行表示与非关键特征软件相关的软件代码，而如时间线92上示出的98所代表的特征执行则表示与失效可操作的特征有关的软件代码。在其它特征控制器中，其它特征控制器的NVM中的特征执行软件由100表示。该相应软件代码执行其它特征控制器专用于处理的特征操作。

[0035] 在时间t_1处，在主控制器和其它特征控制器中发起软件代码迁移102。当被识别为失效可操作的特征的相应特征由主控制器接合时，触发软件代码迁移。在主控制器中发生失效的情况下，失效可操作的特征需要备用控制器。响应于主控制器中的相应特征的执行，将软件代码从主控制器的NVM迁移至其它特征控制器的RAM。在软件代码被传递至其它特征控制器的RAM时，执行其它特征控制器的重新配置以便用作使用RAM中的软件代码的备用控制器。

[0036] 在时间t_2处，主控制器维持失效可操作的特征操作和非关键特征操作两者的软件代码的执行。其它特征控制器被重新配置为执行储存在其它特征控制器的RAM中的失效可操作的特征操作98。其它特征控制器可以在其涉及储存在RAM中的特征操作的情况下进一步继续执行储存在其NVM中的软件代码104，或者可以在存在足够的CPU能力来执行所有软件代码的情况下继续执行所有软件代码。可替代地，可以关闭NVM中的其它特征软件或者关闭其部分。例如，如果用于车道定中控制的软件代码被储存在其它特征控制器的RAM中并且用于车道感测的软件代码被储存在其它特征控制器的NVM中，则其它特征控制器将继续执行涉及失效可操作的特征操作的车道感测。其它特征控制器将继续执行储存在其RAM中的软件代码直到需要备用控制器的相应特征操作已完成或者被关闭。

[0037] 尽管已经详细地描述了本发明的某些实施例，但熟悉本发明所涉及领域的技术人员将意识到用于实践如下权利要求所定义的本发明的各种替代设计和实施例。

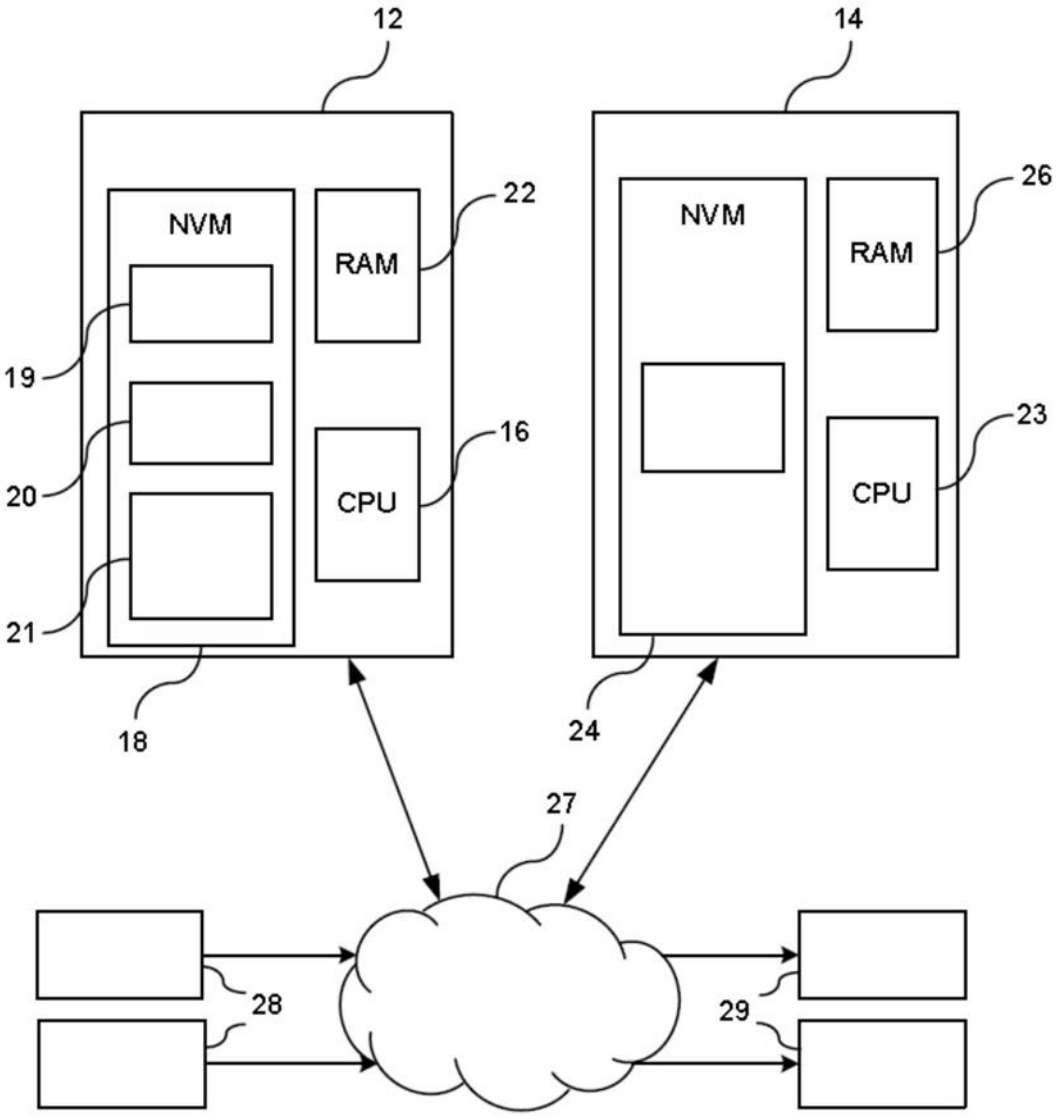


图1

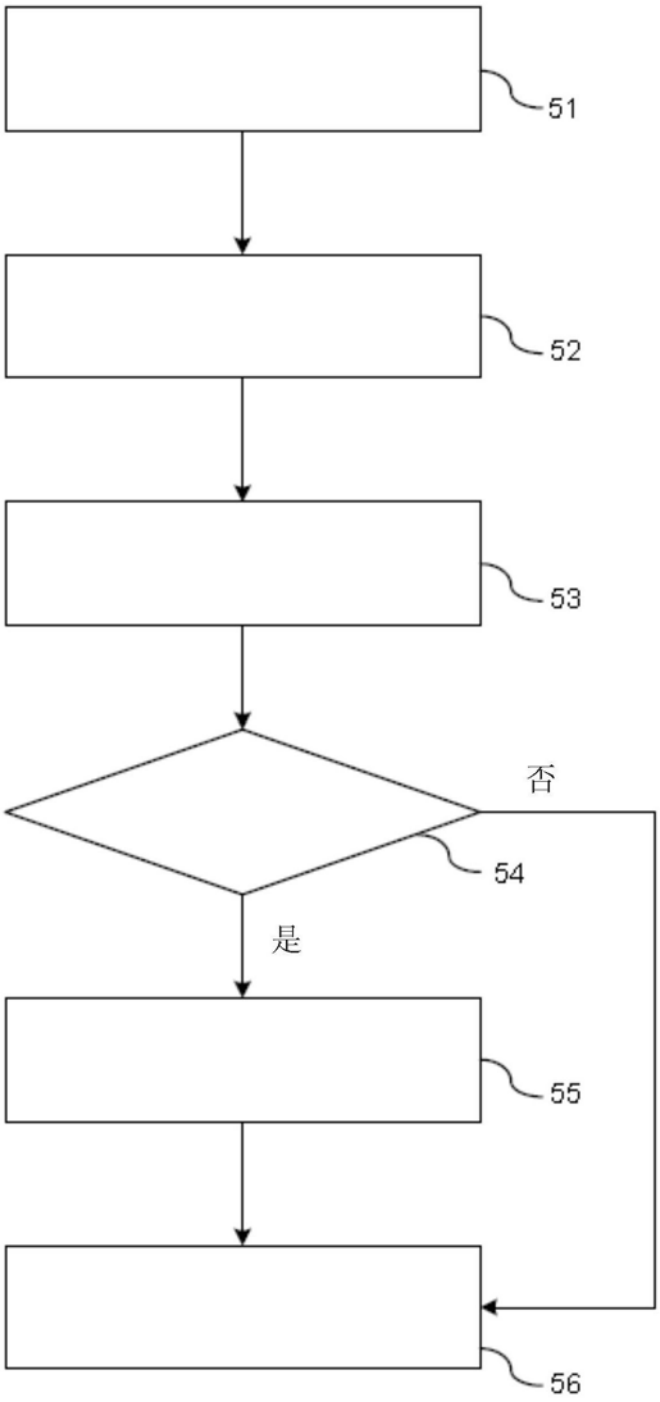


图2

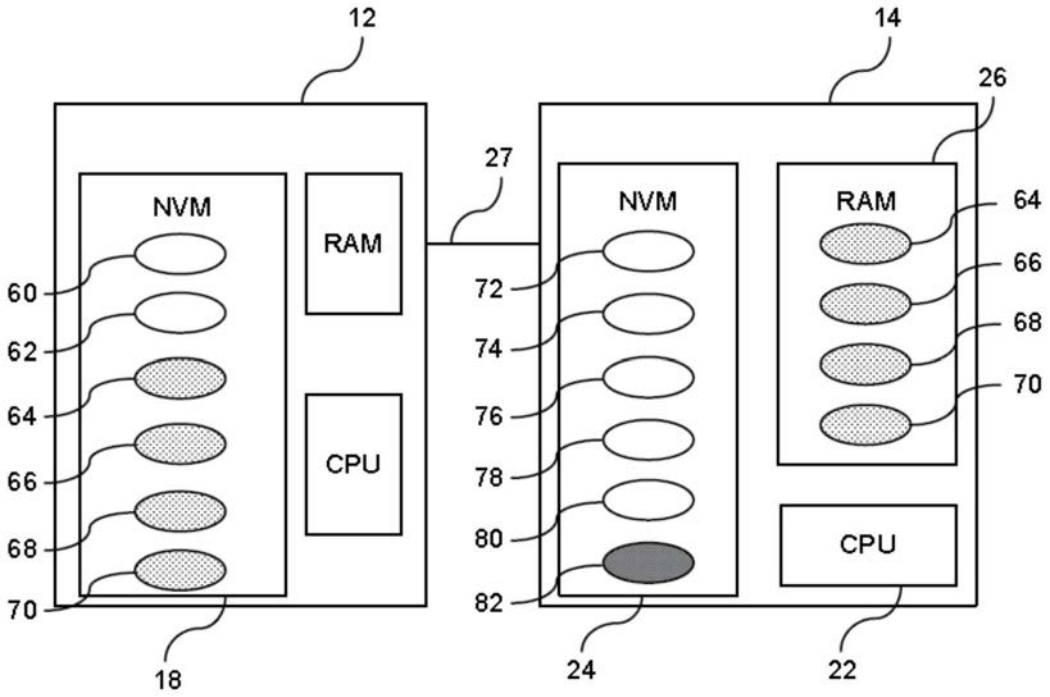

12
14
26
27
NVM
RAM
CPU
NVM
RAM
CPU
60
62
64
66
68
70
72
74
76
78
80
82
64
66
68
70
18
24
22

图3

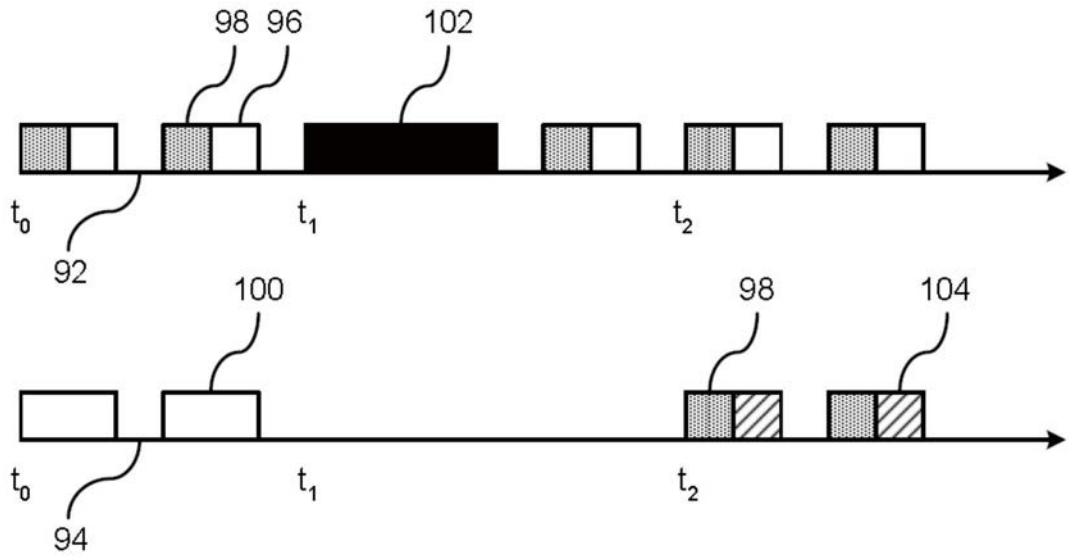

98
96
102
t_0
t_1
t_2
92
100
98
104
t_0
t_1
t_2
94

图4