(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 102214253 A
(43)申请公布日 2011.10.12

(21)申请号 201110083683.8

(22)申请日 2011.04.01

(30)优先权数据
12/753166 2010.04.02 US

(71)申请人 通用汽车环球科技运作有限责任公司
地址 美国密执安州
申请人 克勒格布尔印度理工学院

(72)发明人 D. 达斯 P. P. 查克拉巴蒂
P. 辛哈

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 姜云霞 杨楷

(51)Int.Cl.
G06F 17/50(2006.01)

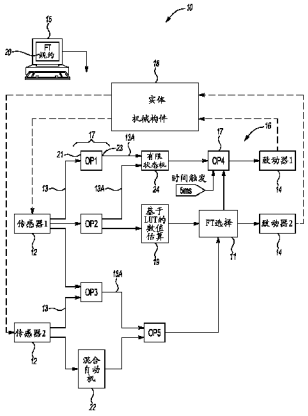
权利要求书 2 页 说明书 12 页 附图 14 页

(54)发明名称

用于操作层功能和退化故障分析的方法和装置

(57)摘要

提供了用于操作层功能和退化故障分析的方法和装置。具体提供了一种装置和方法，用于分析系统的容错性，并且对不同的容错系统设计选择进行“whatif?”分析。该容错分析方法处理源于信号值精度损失的逻辑故障和质量故障。该方法能够检测质量故障，这就能够允许建立起对精度损失有恢复性的系统。提供了两种分析步骤，一种是静态的，而另一种是基于仿真的，将其结合使用以检验机动车系统或其他系统的容错性。尽管基于仿真的方法可以在特定的测试实例和故障场景下检验故障的恢复性，但是静态分析方法可以快速地检验所有的测试实例和故障场景。静态分析方法进行估算同时执行分析，并利用基于仿真的方法复制任何检测到的故障。所有的分析操作都是在应用程序的操作层状态模型上进行的，由此降低了分析成本。



CN 102214253 A

1. 一种用于分析系统容错 (FT) 能力的方法，所述方法包括 ：

在可由主机存取的实体介质上记录定义了用于系统的功能规约的标准的 FT 要求集合 ；

利用主机来生成系统的操作层模型 ；

将系统中构件集合的状态自动地特征化为离散的查找表 (LUT)，如由模型所表示的 ；并且

利用主机通过离散的查找表和功能规约来分析系统的 FT 能力 ；

其中分析系统的 FT 能力包括分析系统的逻辑故障和质量故障的预定集合。

2. 如权利要求 1 所述的方法，进一步包括 ：

将用于系统的可选设计场景记录在实体介质上 ；以及

通过主机利用查找表和功能规约来自动分析可选设计场景。

3. 如权利要求 1 所述的方法，进一步包括 ：

作为第一组步骤，通过主机检验输入和功能规约中故障场景的所有可能的组合 ；以及

作为第二组步骤，通过主机利用查找表来检验系统在标准测试实例和故障场景集合下的 FT 状态。

4. 如权利要求 1 所述的方法，进一步包括 ：

在第一组步骤期间确定违反 FT 要求的存在性 ；以及

在第二模型中复制导致所述违反的系统状态集合。

5. 如权利要求 1 所述的方法，进一步包括 ：

将构件的特征化质量状态存储在查找表中 ；以及

利用主机处理查找表以确定系统的质量状态。

6. 如权利要求 1 所述的方法，进一步包括 ：

使用基于查找表的仿真方法以及基于离散查找表的静态分析方法中的至少一种来检测反例 ；以及

将反例自动复制在 FT 规约中 ；

其中反例描述了构件集合的不同构件中的故障值集合，其中所述故障值造成系统以违反 FT 要求这样的方式来表现。

7. 如权利要求 6 所述的方法，包括使用基于查找表的静态分析方法，其中使用基于查找表的静态分析方法包括使用以下方法中的至少一种 ：模型校验、布尔可满足性求解、可满足性模理论求解以及搜索算法。

8. 如权利要求 1 所述的方法，进一步包括 ：将每一种测试实例、故障场景以及容错要求规约都输入到主机内，其中 ：

故障场景是形式为位置、故障类型和测量值的三元组集合 ；

位置表示受到故障影响的信号 ；以及

故障类型和测量值分别表示误差的类型和测量值。

9. 如权利要求 1 所述的方法，其中所述模型包括 FT 选择模块，所述方法进一步包括利用 FT 选择模块来检测和选择无故障输入并将无故障输入传送至 FT 选择模块的输出端。

10. 一种适合用于分析系统容错 (FT) 能力的装置，所述装置包括 ：

主机 ；以及

可由主机存取的实体介质，并且在实体介质上记录定义了容错 (FT) 要求的形式化集合的功能规约；

其中主机适合用于：

利用主机生成系统的操作层模型；

将模型中构件集合的状态特征化为离散的查找表 (LUT)；以及

利用离散的查找表和功能规约来分析系统的 FT 能力，其中分析系统的 FT 能力包括分析系统的逻辑故障和质量故障的预定集合。

用于操作层功能和退化故障分析的方法和装置

技术领域

[0001] 本发明涉及一种用于在机动车或其他复杂系统中提供容错性分析的方法和装置。

背景技术

[0002] 随着电子设备和软件作为机动车和其他复杂系统内构建模块的推广，容错性已经逐渐成为基本的设计要求。因此，希望研发出即使在系统层的电子、通信和 / 或处理构件中存在误差时仍能保持其功能性的系统。某些电子构件中的故障可能会造成系统层的状态改变。例如，相对于有缺陷的机械式驾驶杆，适合用于在线控转向的机动车系统中提供电子信号的微处理器内的固定故障状态可能会在输出的转向扭矩中造成相对较大的改变。另外，机动车系统必须遵循严格的工业要求，包括特定的容错性要求。

[0003] 系统内的电子构件故障可能会由于构件缺陷以及与寿命相关的退化而出现。芯片、传感器、电源以及机电式致动器可能会永久或短暂地失灵或者简单地随着时间而变得越来越不准确。另外，硬件和软件错误可能会造成短暂和永久的故障，这些故障自身可能会表现为系统层控制器的输出中的误差，并且最终表现为设置在系统内的任意致动器功能中的误差。各个构件例如传感器、软件模块和硬件模块可能会引入范围从信号轨迹漂移到错误瞬态输出的偶发质量故障，这可能会造成信号精度的损失。

发明内容

[0004] 因此，本文中提供了一种基于计算机或主机的方法和装置，能够在机动车系统或其他相对复杂的系统中进行容错性 (FT) 分析，在设计的早期阶段例如在分析的操作层和 / 或设计 / 建模阶段就这样做。整体框架提供逻辑以及质量分析，并且也允许进行未来的可靠性分析扩展。除了分析机动车系统的容错性以外，本发明还如下所述对各种容错机动车系统设计选择进行“what if?”或假设分析。因此，本发明的方法和装置能够检测质量故障，这样相应地能够有助于构建对硬件和软件构件中的精度损失都有恢复性的系统。

[0005] 提出的方法包括两种分析方法或步骤，一种是静态的，而另一种是基于仿真的，结合使用这两种方法以评估指定系统的容错性。本发明中的 FT 分析方法的优点在于所有操作都是通过应用程序的操作或操作层状态模型例如使用 Simulink、MATRIXx 或其他建模软件来实现的，因此相对于常规方法就潜在地降低了分析成本。

[0006] 具体地，一种用于分析系统 FT 能力的方法包括在可由主机存取的实体介质上记录定义了功能规约的 FT 要求集合；利用主机来生成系统模型；将系统中构件集合的状态自动提取或特征化为离散的查找表 (LUT)，如由模型所表示的；并且利用主机通过离散的 LUT 和功能规约来处理或分析系统的 FT 能力。分析系统的 FT 能力包括分析系统逻辑故障和质量故障的预定集合。

[0007] 本文中还提供了一种装置用于分析系统的 FT 能力。该装置包括主机，该主机装有实体介质以及用于执行上述方法的算法。

[0008] 方案 1：一种用于分析系统容错 (FT) 能力的方法，所述方法包括：

在可由主机存取的实体介质上记录定义了用于系统的功能规约的标准的 FT 要求集合；

利用主机来生成系统的操作层模型；

将系统中构件集合的状态自动地特征化为离散的查找表 (LUT)，如由模型所表示的；并且

利用主机通过离散的查找表和功能规约来分析系统的 FT 能力；

其中分析系统的 FT 能力包括分析系统的逻辑故障和质量故障的预定集合。

[0009] 方案 2：如方案 1 所述的方法，进一步包括：

将用于系统的可选设计场景记录在实体介质上；以及

通过主机利用查找表和功能规约来自动分析可选设计场景。

[0010] 方案 3：如方案 1 所述的方法，进一步包括：

作为第一组步骤，通过主机检验输入和功能规约中故障场景的所有可能的组合；以及

作为第二组步骤，通过主机利用查找表来检验系统在标准测试实例和故障场景集合下的 FT 状态。

[0011] 方案 4：如方案 1 所述的方法，进一步包括：

在第一组步骤期间确定违反 FT 要求的存在性；以及

在第二模型中复制导致所述违反的系统状态集合。

[0012] 方案 5：如方案 1 所述的方法，进一步包括：

将构件的特征化质量状态存储在查找表中；以及

利用主机处理查找表以确定系统的质量状态。

[0013] 方案 6：如方案 1 所述的方法，进一步包括：

使用基于查找表的仿真方法以及基于离散查找表的静态分析方法中的至少一种来检测反例；以及

将反例自动复制在 FT 规约中；

其中反例描述了构件集合的不同构件中的故障值集合，其中所述故障值造成系统以违反 FT 要求这样的方式来表现。

[0014] 方案 7：如方案 6 所述的方法，包括使用基于查找表的静态分析方法，其中使用基于查找表的静态分析方法包括使用以下方法中的至少一种：模型校验、布尔可满足性求解、可满足性模理论求解以及搜索算法。

[0015] 方案 8：如方案 1 所述的方法，进一步包括：将每一种测试实例、故障场景以及容错要求规约都输入到主机内，其中：

故障场景是形式为位置、故障类型和测量值的三元组集合；

位置表示受到故障影响的信号；以及

故障类型和测量值分别表示误差的类型和测量值。

[0016] 方案 9：如方案 1 所述的方法，其中所述模型包括 FT 选择模块，所述方法进一步包括利用 FT 选择模块来检测和选择无故障输入并将无故障输入传送至 FT 选择模块的输出端。

[0017] 方案 10：一种适合用于分析系统容错 (FT) 能力的装置，所述装置包括：

主机；以及

可由主机存取的实体介质，并且在实体介质上记录定义了容错 (FT) 要求的形式化集合的功能规约 ；

其中主机适合用于 ：

利用主机生成系统的操作层模型 ；

将模型中构件集合的状态特征化为离散的查找表 (LUT) ；以及

利用离散的查找表和功能规约来分析系统的 FT 能力，其中分析系统的 FT 能力包括分析系统的逻辑故障和质量故障的预定集合。

[0018] 方案 11 ：如方案 10 所述的装置，进一步包括 ：

记录在实体介质上并且可由主机存取的可选设计场景，其中主机适合用于利用查找表和功能规约来自动分析可选场景。

[0019] 方案 12 ：如方案 10 所述的装置，其中所述主机被设置用于 ：

作为第一组步骤，检验输入和功能规约中故障场景的所有可能的组合 ；以及

作为第二组步骤，利用查找表来检验系统在标准测试实例和故障场景集合下的 FT 状态。

[0020] 方案 13 ：如方案 10 所述的装置，其中所述主机被设置用于 ：

在第一组步骤期间确定违反 FT 要求的存在性 ；以及

在原生的操作层模型中复制导致所述违反的系统状态集合。

[0021] 方案 14 ：如方案 10 所述的装置，其中所述主机被设置用于 ：

将系统中各个电子软件和机械构件的质量状态特征化 ；

将特征化的质量状态存储在至少一个查找表中 ；以及

处理存储的信息以确定系统的质量状态。

[0022] 方案 15 ：如方案 10 所述的装置，其中所述主机被设置用于 ：

使用基于查找表的仿真方法以及基于离散查找表的静态分析方法中的至少一种来检测反例 ；以及

将反例复制在操作层模型中 ；

其中反例描述了系统不同构件中的故障值集合，所述故障值造成系统以违反 FT 要求这样的方式来表现。

[0023] 方案 16 ：如方案 15 所述的装置，其中所述主机适合使用基于查找表的静态分析方法，并且所述基于查找表的静态分析方法包括以下方法中的至少一种 ：模型校验、布尔可满足性求解、可满足性模理论求解以及搜索算法。

[0024] 方案 17 ：如方案 16 所述的装置，其中所述主机适用于将每一种测试实例、故障场景以及容错要求规约都记录在实体介质上，并且其中 ：

故障场景是形式为位置、故障类型和测量值的三元组集合 ；

位置表示受到故障影响的信号 ；以及

故障类型和测量值分别表示误差的类型和测量值。

[0025] 本发明的上述特征和优点以及其他的特征和优点将根据以下结合附图时对本发明最佳实施方式的详细说明而变得显而易见。

附图说明

[0026] 图 1 是可用于执行机动车或其他系统的容错性分析的操作层模型和主机的示意图；

图 2A 是可以通过本方法评估的第一种类型信号误差的曲线图；

图 2B 是可以通过本方法评估的第二种类型信号误差的曲线图；

图 2C 是可以通过本方法评估的第三种类型信号误差的曲线图；

图 2D 是可以通过本方法评估的第四种类型信号误差的曲线图；

图 2E 是可以通过本方法评估的第五种类型信号误差的曲线图；

图 2F 是可以通过本方法评估的第六种类型信号误差的曲线图；

图 3 是用于在信号中引入误差的故障注入机构的示意图；

图 4 是根据一个实施例的系统的基于质量中心仿真的分析的示意图；

图 5A 是质量中心的静态分析框架中的第一步骤的示意图；

图 5B 是质量中心的静态分析框架中的第二步骤的示意图；

图 5C 是质量中心的静态分析框架中的第三步骤的示意图；

图 6A 是输入信号相对于时间的曲线图；

图 6B 是输出信号相对于时间的曲线图；

图 6C 是可用于本方法的查找表；以及

图 7 是用于图 5A-5C 中操作层模型的质量分析的布尔电路的示意图。

具体实施方式

[0027] 参照附图，其中相似的附图标记表示从图 1 开始的各视图中相同或类似的构件，操作层模型 10 可以利用主机 15 生成，其中可以通过主机 15 运行指定系统的容错性 (FT) 自动电路分析。主机 15 包括其上记录有 FT 规约 20 的实体介质。利用主机 15 和本文中介绍的方法，就能够对机动车和其他的复杂系统进行 FT 分析。

[0028] 主机 15 可以被设置为数字计算机，通常包括微处理器或中央处理单元、只读存储器 (ROM)、随机存取存储器 (RAM)、电可擦除可编程只读存储器 (EEPROM)、高速时钟、模拟 - 数字转换 (A/D) 和数字 - 模拟转换 (D/A) 电路以及输入 / 输出电路和设备 (I/O)，还有适当的信号调制和缓冲电路。驻留在主机 15 内或可存取的任意算法因此可以被存储在可记录介质上并且可以由主机执行以提供相应的功能。

[0029] 主机 15 还提供了对各种系统设计选择进行“what if?”或假设设计修正分析的能力。如本文中所用，“what if?”分析允许采用一种设计工作的设计者对设计进行修正以期改进该设计的 FT。为了确认修正事实上有效，设计者必须要检验系统的 FT 是有所提高还是有所降低。因此允许设计者探询如果对设计进行了这些改变那么将会发生什么情况。提出的方法就与设计者的这个源于 FT 预测的问题有关。应该注意到可以有其他的工具用于根据例如功耗预测来进行“what if”分析。

[0030] 图 1 中的模型 10 包括传感器 12、致动器 14、具有不同软件操作 17 的控制逻辑 16 以及实体层模型 18。操作层建模语言例如 Simulink、MATRIXx 等可以被用于提供通用框架以对机动车和其他系统的各个方面和提取的特征建模。所得模型不但能够表示机动车系统的功能层模型，而且还能够表示机动车系统据此运行的结构平台的某些细节，例如映射到处理器、缓冲器、总线等。

[0031] 控制逻辑 16 可以包括各种关联或涉及的软件操作，例如图 1 中的 OP1-5。实体模型 18 可以是指定系统（例如相对复杂的机动车系统，譬如根据一个可行实施例的线控转向或制动设备）中的各种互连或机械构件的数学动态模型，不过在本发明的保护范围内也可以分析非机动车系统。

[0032] 模型 10 包括操作 17，其中每一种操作都具有输入端口和输出端口，还包括送入输入端口 21 内的输入信号 13 和从输出端口 23 送出的输出信号 13A。信号 13，13A 表示不同操作之间的虚拟连接，并且可以与物理量例如由滤波器生成的输出电压相对应，或者可以对应于由软件模块生成的数据值。

[0033] 图 1 中的每一种操作 17 都对应于被诊断的特定系统中的功能构件，其中功能构件的范围涵盖了传感器 12、软件代码模块和模拟构件等。本文中将离散事件的语义设想为若干操作 17 被映射至软件构件，也就是在离散的步骤中对采样信号进行操作。每一个信号 13 都表示在每一个时隙通过“源”操作更新的数值。

[0034] 图 1 示出了一种可行的模型，该模型宽泛地类似于机动车系统的若干种操作层模型的示意性表示。模型 10 中的每一种操作 17 都对应于特定的控制应用程序、传感器操作、致动器操作中的某项任务或者是对应于由模型 18 表示的实体中的机械部件 / 构件。每一种操作 17 都可以由逻辑或算术函数、状态机例如有限状态机 (FSM)24 或混合 I/O 自动机 22 表示。模型 10 在基于 LUT 的数值估算模块 19 中使用查找表 (LUT)。FT 选择模块 11 选择输入，例如在图 1 的实施例中是从 OP5 和基于 LUT 的估算模块 19 中进行选择，并将数值传送至其输出端。为了进行这种选择，FT 选择模块 11 根据用户定义的标准检测两个输入中是否有一个有错误，例如检查输入值是否落在一定的范围内，并随后选择无错误的输入。如果两个输入都没有错误，那么 FT 选择模块 11 就选择预定的输入例如来自 OP5 的输入。要注意的是基于 LUT 的估算模块 19 并不涉及以下介绍的特征化步骤中构建的质量 LUT。在很多机动车系统中，LUT 被用于根据不同于 A 的信号来估算信号“A”的值。这样有助于在信号 A 的来源失效的情况下提高系统的 FT。

[0035] 在大多数感兴趣的机动车系统中，控制逻辑 16 几乎全部是基于软件的，因此信号 13 可以被立即转化为作为输入提供给控制软件构件的数据项。而且，很多控制构件可以是时间触发的，以使它们在特定的时刻开始或恢复运行。例如，图 1 中的 OP4 可以被设置为仅在预定时段例如从开始运行起经过了譬如 5ms 之后才执行，即使是输入可以更早获得也是如此。图 1 中标记为 OP1，OP2，OP3 和 OP5 的其他操作 17 可以根据模型 10 以类似或不同的方式执行。各操作之间的连线表示它们之间的虚拟函数连接，其将来源操作的输出轨迹映射为用于目标操作的输入轨迹。

[0036] 用于容错性分析的方法

还是参照图 1，提供了一种用于通过主机 15 自动分析指定 FT 系统例如机动车系统的方法。该方法包括结合使用的两种分析方法或步骤的集合，以检验机动车系统对于各种逻辑和质量故障的恢复性 :(Ⅰ) 静态分析步骤，以及 (Ⅱ) 操作层故障注入和仿真步骤。静态分析对预定的故障场景集合进行近似但快速的评估。随后，对于每一种故障场景和导致违反标准 FT 要求的输入，基于仿真的确认步骤验证这种违反的真伪。

[0037] 操作层模型和分析通常都仅在实现层进行。这就需要将实现层的错误适当地提取至操作层，并将相关的实现细节在合适的操作层模型中建模。下文中讨论的是将各种类型

的故障提取为操作层模型中合适的表现形式。本方法没有集中在质量中心分析上，而是有助于推出例如故障注入式机动车系统中的状态偏差来取代推出机动车系统信号的轨迹。基于仿真的框架提供了无故障和故障注入的系统状态之间的偏差跟踪。另一方面，静态分析步骤仅仅是推出各种信号误差的质量或数量而并未深入到实际信号轨迹的细节中。

[0038] 操作层模型基于仿真的分析

还是参照图 1，大多数分析和综合步骤都是在操作层模型例如模型 10 上进行的，用于在更高的间隔层上发挥使转变和分析时间更快的作用。操作层故障仿真框架中最为重要的要求之一就是在操作层提取时对各种质量和逻辑故障的建模。故障的起源通常位于电路层或分配层的实现细节中。例如，软件误差会造成存储器单元或寄存器中的瞬时位翻转，或者传感器电源中温度引发的漂移会造成输出信号的漂移。这些故障被提取到操作层模型例如模型 10 的层级中，同时仍然保留故障影响信号值的方式实质。

[0039] 可以在操作层模型例如图 1 的模型 10 中提取各种类型故障的影响。例如，可以提取 :(1) 导致在输出中增加的噪声以及在输出信号轨迹中增加漂移的传感器故障，例如噪声和漂移故障 ;(2) 丢失来自传感器的数据，在某些时隙中导致随机的传感器输出或尖峰，例如丢失了来自摄像头的数据的示例 ;(3) 自身不会在每一次运行流程中都表现出来的软件缺陷和硬件错误可以被视为是在对它们进行训练的某些时隙中的尖峰故障。这些尖峰故障由于在所述时隙内生成了用于信号的最大可能值而夸大了由缺陷 / 错误引发的故障 ;以及 (4) 软件构件中的精度损失作为轨迹漂移而被建模。这些漂移可能会由于类型转换错误以及由于嵌入式机动车平台的端口控制软件可能不支持太多的高精度和浮点操作而出现。

[0040] 还可以提取 :(5) 由硬件层中的适当构件检测到以使得能够实现故障静默的逻辑故障。操作被假定为仪表化操作以使得如果有任何的主要输入信号指示故障静默，那么这些操作就是故障静默的 ;(6) 时钟 / 脉冲的偏移 / 时滞导致的延时故障，延时故障表现为输出信号的时间线失真以及与计时器相关联的延时改变。软件任务中运行延时的改变也可能会造成采样和信号生成速率的改变，从而导致延时故障 ;以及 (7) 硬件恢复的软错误，表现为尖峰也就是信号上突然和短暂的改变，例如尖峰故障。

[0041] 上述故障中的一部分并非源于机动车系统中的软件控制构件。但是，由于故障的传播，它们的影响除其他因素外仍然可以在各种软件控制构件的输出中观察到。因此，任何分析方法都应该关注上述故障在来自于实体模型 18 的不同类型的软件、硬件和机械构件上的传播。

[0042] 依次参照图 2A-2F，可以将每一种类型的质量退化与用于表示质量退化程度也就是误差的适当测量值相关联。图 2A 表示“原始”或无故障的信号 30。图 2B 表示信号 30 的信号轨迹中的漂移误差，其中质量由信号 30 和信号 30A 在全部时刻内的信号值之间的最大偏差表示。图 2C 表示信号噪声，其中质量由叠加的附加噪声信号 30B 的振幅表示，附加噪声信号 30B 包括白噪声、高斯噪声等。

[0043] 继续参照图 2D，尖峰 30C 是由于硬件恢复的软错误、软件缺陷、瞬时硬件误差和 / 或瞬时传感器误差例如丢失了传感器数据而造成的。质量由尖峰 30D 的数量表示。如果信号是数字信号，那么尖峰 30D 的峰值要受到操作范围或数据类型上限的约束。图 2E 表示产生适当信号 30D 的延时，其中质量退化的测量值即为或正或负的延时。

[0044] 延时故障经常会如图 2F 中所示导致某种尖峰或随机噪声的引入。如图 1 中所示，

如果直到 t_{pre} 个时间单位才通过一种操作 (OP1) 并随后通过另一种操作 (OP2) 生成信号轨迹，那么就可能会发生这种情况。例如，假设 OP1 由于延时故障在 $t_{pre}-\tau$ 个时间单位内完成运行并且假设 OP2 直到已经过 t_{pre} 个时间单位之后才开始。在此情况下，在 $t_{pre}-\tau$ 到 t_{pre} 的时段内就没有操作会产生信号，并且因此在该时段内的信号轨迹就可能是随机的或者是一组尖峰。

[0045] 基于仿真的容错分析框架有三种输入，也就是 (1) 测试实例，(2) 故障场景以及 (3)FT 要求规约。测试实例通常描述了一组由机动车系统执行的典型并且关键的操作或工作序列。另外，测试实例也可以被生成用于执行机动车系统的定向分析。通常，通过这些测试实例对来自于用户的传感器输入进行建模。如果仅测试了系统的一部分，那么来自于由图 1 中的实体模型 18 表示的“实体”的响应于来自其他一些子系统的控制信号而生成的某些信号也被包括在测试程序中。

[0046] 基于仿真的故障注入框架的第二输入是故障场景的描述，在此故障场景下必须对系统进行分析。故障场景可以通过列举必然会发生的故障集合来清楚地描述。在质量故障的情况下，除了发生了哪种故障的信息以外，质量退化的测量值也必须列出。因此故障场景是三元集合的形式 (位置、故障类型、测量值)，其中位置表示被故障影响到的信号，并且其中故障类型和测量值分别表示误差的类型和测量值。要注意的是测量值与逻辑故障无关。例如故障场景可以具体描述为“最多五个尖峰，这也就是通过全部的软件构件可以引入的类型和测量值”。

[0047] 在将故障场景具体描述为分析框架的输入的同时，说明各种故障之间的相关性也很重要。显然，映射至同一处理器的软件任务将会遭遇由于处理器而产生的一些共同的故障。类似地，来自同一厂商的传感器通常也会遭遇类似的故障，同时共用电源会在其供电的所有传感器内引发若干种相关的噪声和信号漂移故障。这些相关性必须被收集到任意的 FT 分析框架中。如果用 0 到 1 之间的相关系数或者 0% 到 100% 之间的相关性来描述故障之间的相关性，那么就可以如本领域所公知的那样执行多次蒙特卡罗故障仿真用于进行分析。

[0048] 除了清楚的故障场景描述以外，描述故障场景的另一种方式是通过设定关于在系统的一次运行期间故障集合发生概率的下限来隐含地描述。如果个体故障的概率以及故障之间的相关性已知，那么就可以计算故障集合的概率。随后概率边界就描述了其中上述计算的概率超出边界的所有故障场景。这样的概率边界通常与机动车系统的安全性要求 (例如根据 IEC 的安全完整性等级) 有关。

[0049] 可以注意到在质量故障的情况下，不仅必须要提供发生故障的概率，而且还必须提供获得各种质量退化测量值的概率。实际上，质量故障的概率可以由以下函数表示：$P_{quality}$ ：测量值→ [0,1]，将质量退化的测量值映射为具有该测量值的故障发生的概率。测量值为零 (0) 表示没有发生故障。在生成测试实例用于定向 FT 分析时，不仅是测试实例的操作变量 (例如传感器输入) 需要生成，而且对应的故障场景也需要生成。另外，经常要对“正确的”控制信号和故障信号之间的差异而不是单独对故障信号进行 FT 分析。这些因素对用于 FT 分析的测试实例生成问题增加了额外的维数。

[0050] 基于仿真的故障分析框架的第三输入集合是系统必须要满足的 FT 要求集合。这些 FT 要求构成了系统即使在存在故障时也必须要遵守的规约。存在各种方式来指定 FT 要求。指定系统设计意图的逻辑和时间性质可以被用作用于 FT 分析步骤的规约。另外可以

指定用于检验质量退化边界的特性例如叠加噪声量的上限。除此以外，可以写入更多涉及到的性质，其中可接受的质量退化是时间的函数。

[0051] 对FT分析框架给出三种输入，基于仿真的FT机构包括故障注入、操作层模型仿真以及对应于FT要求性质的检验判定。因此在这里提出向信号中引入不同（和多种）类型误差的“故障注入”操作。这些误差根据要分析的故障场景而对应于每一种操作故障。该操作将用于每一种不同类型质量故障的质量故障类型和质量退化的测量值作为输入。

[0052] 另外，关于逻辑故障的信息也被“故障注入”操作作为输入。根据被分析的特定故障场景来获得将质量故障量化并指明了在特定信号上是否存在逻辑故障的这些输入。“故障注入”操作随后根据该操作的输入来引入质量故障和逻辑故障。可以注意到并不是每一种类型的信号中都可以引入全部类型的质量故障。例如，由软件构件生成的表示浮点数随时间而变化的信号（数据信号）就不会受到通常仅限于传感器和模拟构件的质量故障例如“噪声”的影响。但是，如果在一个时隙中调用了软件缺陷，那么这样的信号可能会受到“尖峰”故障的影响。另外这样的信号在移植到嵌入式平台时由于浮点到定点转换或者由于类型转换错误而有精度损失的情况下可能会受到“漂移”故障的影响。

[0053] 参照图3，示出了故障注入操作40的一个示例。故障注入机构40在信号线或输出42中引入噪声误差和漂移误差。该操作的输入是信号线或输出42、故障类型44、偏差量46和噪声振幅48。输入的故障类型控制被引入信号中的误差类型，误差类型可以是噪声或漂移或两种误差都有或者两种误差都没有。输入的偏差量和噪声振幅分别表示被引入的漂移量和被叠加的噪声信号的振幅。因此，设计者能够控制被引入信号中的精度误差的类型和数量。“故障注入”操作将选定的误差叠加在信号“输出”上以生成“注入误差的输出”49。该“注入误差的输出”49可以随后成为某些其他操作的输入，由此传播注入的误差。

[0054] 根据一个实施例，每一种信号上都设置一种“故障注入”操作，由此使引入故障的基本结构能够对应于任何用户定义的故障场景。用同一种建模语言例如Simulink将这些“故障注入”操作写成操作层模型。随后，用测试实例和故障场景作为输入，利用合适的操作层仿真框架来仿真图1中的模型10以使故障仿真得以进行。利用由仿真框架提供的验证程序或者通过转存并分析在离散的时间步长中收集的记录来检验对信号值的判定。

[0055] 参照图4，在简单的机动车系统中示意性地示出了质量中心的基于仿真的分析50，该系统包括一个传感器12、一个致动器14以及一个控制操作。在图4上部示出了“理想模型”50A，而在下部则示出了故障注入模型50B。在不同信号上进行故障注入以获得各种构件故障的影响。获得并推出相对于无故障模型的轨迹差异。

[0056] 如上所述，除了用于分析具有故障注入的操作层模型的框架以外，我们还关注执行质量中心分析。质量中心分析推出信号质量而不是信号的真实值。因此，我们关注的是由故障系统根据无故障系统产生的信号而生成的信号轨迹的偏差。为此可以使用的仿真设置中同时对原生/理想模型50A和故障注入模型50B进行仿真，并通过差分操作52来获得信号54A,54B之间的差值。

[0057] 该差值56表示故障信号54B与无故障信号54A之间的偏差。推出信号质量也就是与无故障状态之间偏差的判定程序随后检验作为差分操作52的输出获得的记录。所用的故障信号偏差定义以及差分操作52的类型取决于被分析的故障类型。使用最为广泛的差分操作具有Simulink中“减法”操作的语义，并在操作层模型中据此实现。

[0058] 该语义可以由作为“差分”操作的输入给出的示例性离散信号对表示，以使其具有相同的时间步长（δ），并且在时间步长 t_i 中的信号幅值分别是 v_i^1 和 v_i^2。该操作的输出是一种轨迹，具有时间步长为 δ，并且在每一个时间步长 t_i 所具有的信号幅值都是两个输入信号在步长 t_i 中的幅值差值 $\left(v_i^1 - v_i^2\right)$。这种类型的差分操作在推导漂移、噪声（用于列筛选）和尖峰误差时是很有效的。另一种类型的差分操作在频域内进行信号偏差分析，目的是为了推导延时故障。根据分析的范围和要求也可以使用若干种其他类型的差分操作而并不背离本发明的保护范围。

[0059] 无论是质量中心还是其他类型，任意基于仿真的设置中的一个重要组成部分是对提供的测试程序进行基于仿真的验证的覆盖率的评估方法。基于检验访问状态或代码覆盖、转换或分支覆盖以及变量值的常规覆盖率方法可能不足以用于容错分析。上述的覆盖率方法经常只能提供包括无故障和故障恢复在内的被测运行环境的大体情况。但是，这些方法不足以估算实际剩余的仿真工作余量，原因在于很多测试的运行和故障场景可能是被分析的容错要求的等价模量。

[0060] 通过含有故障类型、故障量值和故障位置的三元组来表述故障退化。一种故障仿真流程就与故障仿真期间在不同信号（位置）显现的质量退化三元组的集合有关。由于操作层模型中不同操作之间的因果关系，因此在这些三元组之间也存在因果关系（例如，对于具有输入信号 I 和输出信号 O 的操作，由于信号 I 上的误差 B 就会造成信号 O 上的误差 A）。可以将覆盖率定义为在误差仿真期间显现的质量退化三元组之间存在的此类因果关系的数量。其他类似的技术也可以使用，例如对显现的故障三元组进行计数就是另一种测量覆盖率的方法。如果若干种三元组对于给定的误差类型和位置或者在其他标准的基础上具有类似的误差量值，那么这些三元组可以被认为是等价的。在此情况下，可以适当地修正三元组之间的因果关系。

[0061] 操作层模型的静态分析

参照图 5A-5C，提出的容错系统设计方法中的一个重要组成部分是快速分析所有故障场景和以用户规定的提取水平为模的测试实例的静态分析方法。这种静态分析方法是质量中心的分析方法，因为它推出的是信号的质量退化而不是实际的信号轨迹。图 5A-5C 概括了这种分析方法的步骤。

[0062] 静态分析方法分为两步进行，也就是特征化步骤（图 5B）和符号分析步骤（图 5C）。在图 5B 的特征化步骤中，在各步操作例如图 5A 的 OP1-OP4 中对不同的测试实例以及输入信号中变化的质量误差量进行仿真，同时记录输出信号中的质量退化。通过在输出信号中被引入质量误差并且改变输入信号中引入的质量误差来进行另外的特征化仿真。

[0063] 输入和输出信号的质量退化都通过图 5C 中所示的符号查找表 60A-60D 也就是 LUT 而被量化和代码化。这就能够将记录下来的输入和输出质量被表示为 LUT。因此，在特征化之后，每一种操作的状态都是通过 LUT 60A-60D 提取的，这样只能根据图 5A 推出量化的操作输入质量和输出质量。

[0064] 参照图 6A-6C，在图 6C 中示出了用于漂移误差的示例性质量 LUT，表示用于轨迹漂移的各种输入质量、到饱和操作的三角波输入（分别在图 6A 和 6B 中示出）的输出质量。饱和操作将输入信号截断为图 6A 中的用户定义上限 57。在该实例中，考虑将饱和操作实现为

软件构件。对于这种软件实现，轨迹可以由适当离散化的定点 / 浮点数序列表示，每一种都表示在某些离散的时隙处的信号值（振幅）。

[0065] 考虑图 6A 中具有振幅 57 的三角形轨迹的预期（理想）输入信号，而错误的输入信号则是具有大于振幅 57 水平的不同振幅的三角形轨迹。因此，错误的输入信号具有偏离理想输入的轨迹漂移，其被特征为错误信号和理想信号振幅之间的最大差异。可以利用不同的符号来对振幅中的量化漂移进行编码，目的是为了表示输入信号的质量。例如，如果振幅漂移在 0 到 10 之间，那么符号“1”可以被用于表示这种情况。类似地，“2”可以被用于表示 10 到 20 之间的漂移，“3”则表示 20 到 30 之间的漂移等。

[0066] 例如，图 6A 中的输入信号“偏差 1”具有 20 到 30 之间的振幅漂移，并且因此被特征化为符号“3”。对于该饱和模块的示例，理想输出应与具有振幅 57 的三角波输入相同。但是，具有的振幅大于振幅 57 的水平的错误输入信号被饱和操作截断。在此情况下，在图 6B 中通过竖直线 65 示出了用于错误输出信号的振幅中的最大漂移。通过使用符号来表示这些漂移，正如对输入信号所做的那样，即可获得各种错误的输出轨迹的质量。例如，对应于输入信号“偏差 1”（质量“3”）的输出信号在振幅方面具有的与理想输出之间的漂移在 10 到 20 之间，并且因此具有的质量为“2”。

[0067] 由此，对于输入质量“3”，输出信号质量为“2”。特定符号“0”表示在理想的输入 / 输出中没有漂移。图 6C 中的查找表 60 包含从输入到输出质量的映射，用于与用户定义的量化振幅漂移相对应的所有输入质量。对于图 6A-6C 中的示例，质量符号在统一量化理想信号和错误信号之间振幅漂移的基础上进行选择。这种统一的量化包括将振幅漂移分为尺寸为 10 的区间，例如区间 [10,20]。

[0068] 但是，通常，统一量化可能不是构建 LUT 的基础。例如，振幅漂移可以在 [0,10] 之间被量化为五个等级而在 [10,20] 之间仅被量化为两个等级。这种不统一的量化水平可以由容错分析的要求来引导。质量中心分析的另一个重要方面源于操作的输出信号质量不仅取决于输入信号质量而且还取决于信号类型（对于当前示例来说是“三角波”）和操作状态（例如可重构操作的各种结构）的事实。

[0069] 因此，被称为特征的另一种属性被用于区分不同类型的输入信号和操作状态。例如，“三角波”是用于图 6A-C 的示例中的输入特征。用于这种类型输入信号的质量 LUT 不同于一些其他类型信号（例如方波信号）的质量 LUT。LUT 因此存储用于不同特征的输入 - 输出质量。尽管为了特征化单个操作模块可能必须要执行若干种仿真流程，但是该特征化步骤是一次性的工作，并且所获得的 LUT 可以在不同的设计中重复使用。一旦特征化步骤完成，即可通过针对给定故障场景和测试实例的一系列查找表操作来进行质量中心分析。

[0070] 参照图 7，通过将质量退化（与预期状态的偏差）划分为多个区间，每一个 LUT 项都可以通过表示该区间归属的符号来代码化。因此，在量化之后，LUT 就将符号输入映射为符号输出项，并且可以接受数学分析。通过将符号编码为布尔逻辑值，即可利用布尔电路 70 对每一个查找表建模。由于操作层模型包括操作以及操作之间的连接，因此完整操作层模型的质量状态可以被表示为布尔电路 70，包括表示 LUT 的支路以及它们之间的适当连接。

[0071] 在量化间隔中的所有故障场景和测试实例都可以通过求取可满足性来进行检验，也就是用于对操作层模型的质量状态建模的布尔电路 70 的 SAT 解决方案。除了静态的基于 SAT 的分析以外，在本领域中可以理解的可满足性模理论（SMT 解决方案）或者基于仿真

的方法也都可以使用，只要每一种操作都可以被特征化并通过质量 LUT 表示即可。在操作层模型的框架内执行这种分析的一种由 Simulink 提供的方法是将操作替换为质量 LUT 并随后执行对该模型的仿真。

[0072] 量化降低了分析精度，并且因此在布尔分析设置中发现的错误流程必须在操作层模型中进行检验。为此，必须要得到造成错误流程的故障场景（包括了每一种故障的测量值）和测试实例。这些实体是对质量状态进行建模的布尔电路的输入并且由 SAT 求解程序提供用于可满意的情况。因此通过 SAT 分析检测出的错误流程可以在操作层仿真设置中复制。

[0073] 还是参照图 7，关于这种框架的一个问题是提供量化总是会过分估计误差的证据。在此情况下，如果通过静态分析找不到错误流程，那么即可保证在操作层模型中没有错误流程。在图 7 的电路 70 中，图 5A 中的操作 OP1, OP2, OP3 和 OP4 的查找表被表示为支路 QC-OP1, QC-OP2, QC-OP3 和 QC-OP4。实体的特征化模型被表示为电路 QC- 实体。完整的电路具有六个输入，也就是输入质量、输入特征、op1 故障、op2 故障、op3 故障和 op4 故障。

[0074] 信号输入质量和输入特征分别是传感器的输入质量（符号）以及待分析的测试实例。传感器的初始输入被假定为理想情况，并且因此每一种输入信号的质量都被预先指定为常值“0”。可能的不同类型的输入信号轨迹对应于不同的测试实例，被假定为事先已知的，并且因此“输入特征”可以被设定为有限符号集合中的任意一种，其中每一个符号都表示一种信号类型。例如 α 可以表示振幅为“1”的正弦波，而 β 可以表示振幅为“1”的余弦波，同时 γ 可以表示振幅为“2”的正弦波。

[0075] 在大多数设计中，类似于本文中讨论的以及图 5A 和图 7 中示出的情况，从实体的输出到传感器的输入可以有反馈回路。该反馈回路对于质量中心分析来说可以去除，原因在于质量是在完整的仿真窗口（执行仿真的时间段）上定义的，并且基于查找表的分析在无需任何反馈的情况下覆盖用于仿真窗口的分析。待分析的故障场景是该电路的输入，并且用于每一种操作的故障集合都通过输入的 op1 故障、op2 故障、op3 故障和 op4 故障进行分配。这些输入分别引导通过操作 OP1, OP2, OP3 和 OP4 表现出来的误差类型和强度。

[0076] 如果已经将若干操作映射到单个处理器中，那么在每一种操作所经历的故障类型之间就有相关性。这可以通过附加的布尔约束来建模。除了对应于机动车系统操作的电路模块以外，还有两个附加的电路模块来确保对于合理预期的故障场景，任何低质量的输出都会被发现。第一模块检验最终输出质量是否低于用户确定的限制（模块输出为真）。第二模块（故障有效性检验程序）检验被分析的故障场景是否是设计者关注的故障场景。

[0077] 例如，（根据安全完整性等级）考虑分析设置，其中通过在机动车系统故障的预期概率上施加边界，和明确不同故障发生的概率，以及假定故障之间没有相关性来明确地限定故障场景。在此情况下，故障有效性检验程序可以被用于检验故障场景发生的概率是否大于系统预期的故障发生概率 (P_{system})。为了构建该示例中的故障有效性检验程序模块，假定故障之间没有相关性，首先获得对于任何操作来说发生故障的最小概率 ($p_{smallest}$)。然后，对于每一种故障类型 f，计算 $count_f=[Sp_f/p_{smallest}]$，其中 S>1 为比例因子。随后，对于每一种电路评估，“故障有效性检验程序”都针对所有有效的故障 f 来计算全部的 $count_f$ 之和。然后检验该总和是否小于上限：

$[SP_{system}/p_{smallest}](\Sigma fisenabled^{count}{}_f<[SP_{system}/p_{smallest}])$。如果该情况成立，那么“故

障有效性检验程序”就给出真的输出以表明故障场景是可允许的。可以注意到尽管 [Sp_f/$p_{smallest}$] 低估了 $Sp_f/p_{smallest}$ 的值，但是由 [$SP_{system}/p_{smallest}$] 提供了 $SP_{system}/p_{smallest}$ 的过高估计。这样就确保了通过上述方法进行的这部分分析是过高估计的。

[0078] 容错机动车系统的综合

将操作的质量状态提取为符号查找表提供了多种可能来设计出用于容错机动车系统的综合算法。如上所述，各个操作的质量状态可以被建模成电路，也可以被建模成用于推导故障场景发生概率的机构。这就允许我们将可用的电路综合方法加以应用以通过组合对应于不同操作的支路（以及用于推导故障场景发生概率的支路）来建立电路。如果能够将具有所需输出质量集合的电路加以综合，那么通过用综合机构推出的拓扑结构中的对应操作来代替质量提取查找表支路即可得到所需容错机动车系统中的功能层模型。

[0079] 上述方法允许使用基于 LUT 的仿真以及基于离散 LUT 的静态分析方法中的一种或两种来检测反例，并且也允许复制图 1 中的 FT 规约 20 中的反例。反例描述了系统不同构件中的故障值集合，其中故障值导致系统以违反 FT 规约 20 中列举的 FT 要求这样的方式表现。使用基于 LUT 的静态分析方法可以包括使用模型校验、布尔可满足性求解、可满足性模理论求解、搜索算法等。

[0080] 如本文中所用，术语“反例”在 FT 的背景下是指不同构件中的故障值集合，例如图 1 的传感器 12 中的噪声振幅、漂移和 / 或尖峰数量，图 1 的模型 10 中在不同的软件模块内的尖峰数量等，它们会造成被评估系统以违反作为功能规约而获取的 FT 要求这样的方式表现。例如，如果在图 1 中传感器 1 的输出上有 5% 的噪声水平，并且在相同附图内 OP5 的输出上有 1% 的漂移，那么最终输出就有 12% 的漂移。如果 FT 要求的功能规约是三元组 < 最终输出 , 10%, 漂移 >，表示“最终输出”的漂移幅度应该小于 10%，那么 12% 的漂移就违反了这项要求。在此的反例就是“传感器 1 输出上 5% 的噪声以及 OP5 输出上 1% 的漂移”，该条件将系统驱动为由 FT 要求所规定的故障状态。当在原生模型中复制反例时，反例可以被用于提高操作层模型到离散 LUT 的状态提取的精度。

[0081] 尽管已经详细介绍了实现本发明的最佳模式，但是熟悉本发明所涉及领域的技术人员应该能够在所附权利要求的保护范围内设想出用于实现本发明的各种可选设计方案和实施例。

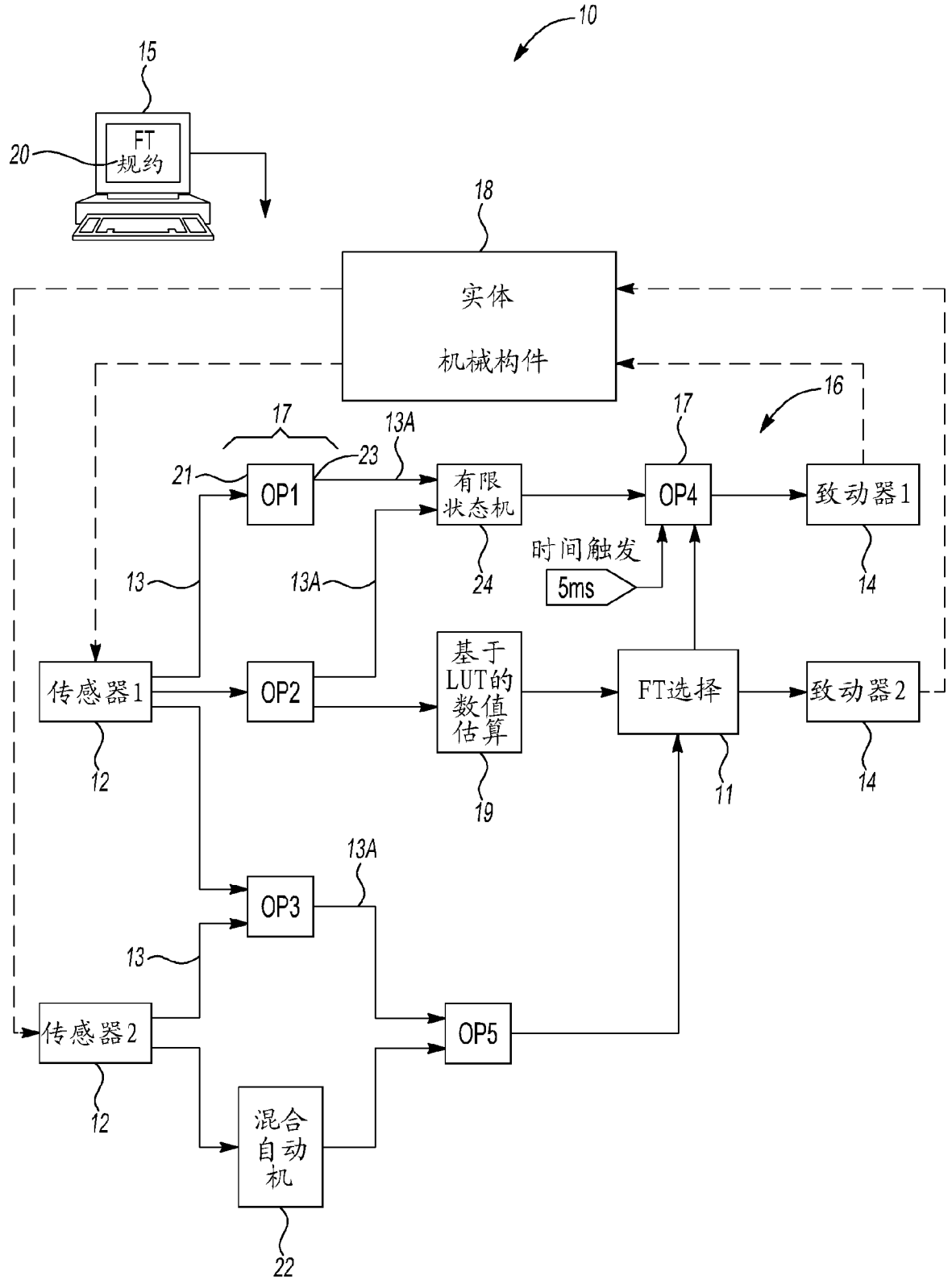

10
15
FT
规约
20
18
实体
机械构件
16
17
13A
17
21
23
OP1
有限
状态机
OP4
致动器1
时间触发
5ms
13
13A
24
14
传感器1
OP2
基于
LUT的
数值
估算
FT选择
致动器2
12
19
11
14
13A
OP3
13
传感器2
OP5
12
混合
自动
机
22

图 1

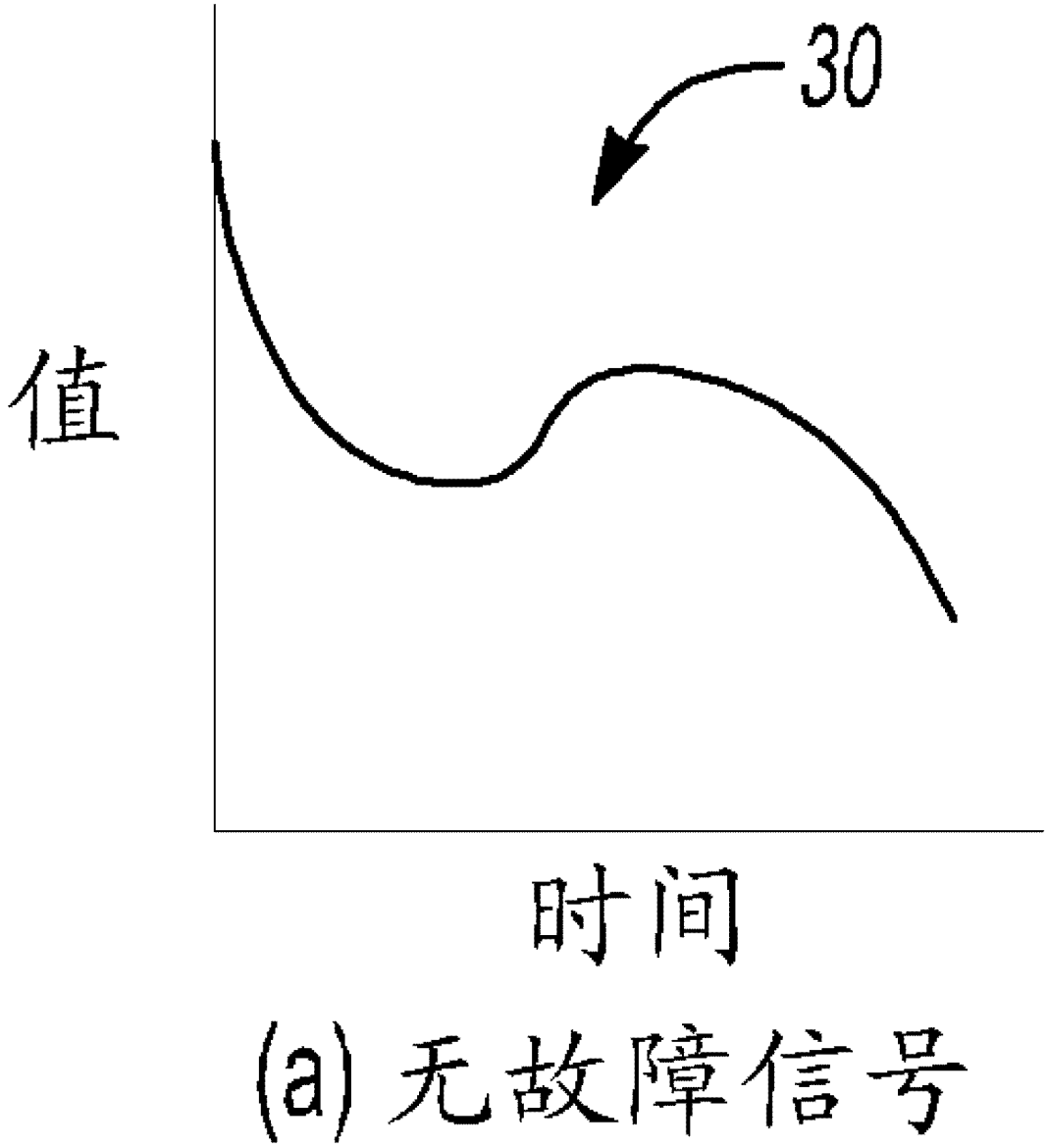


图 2A

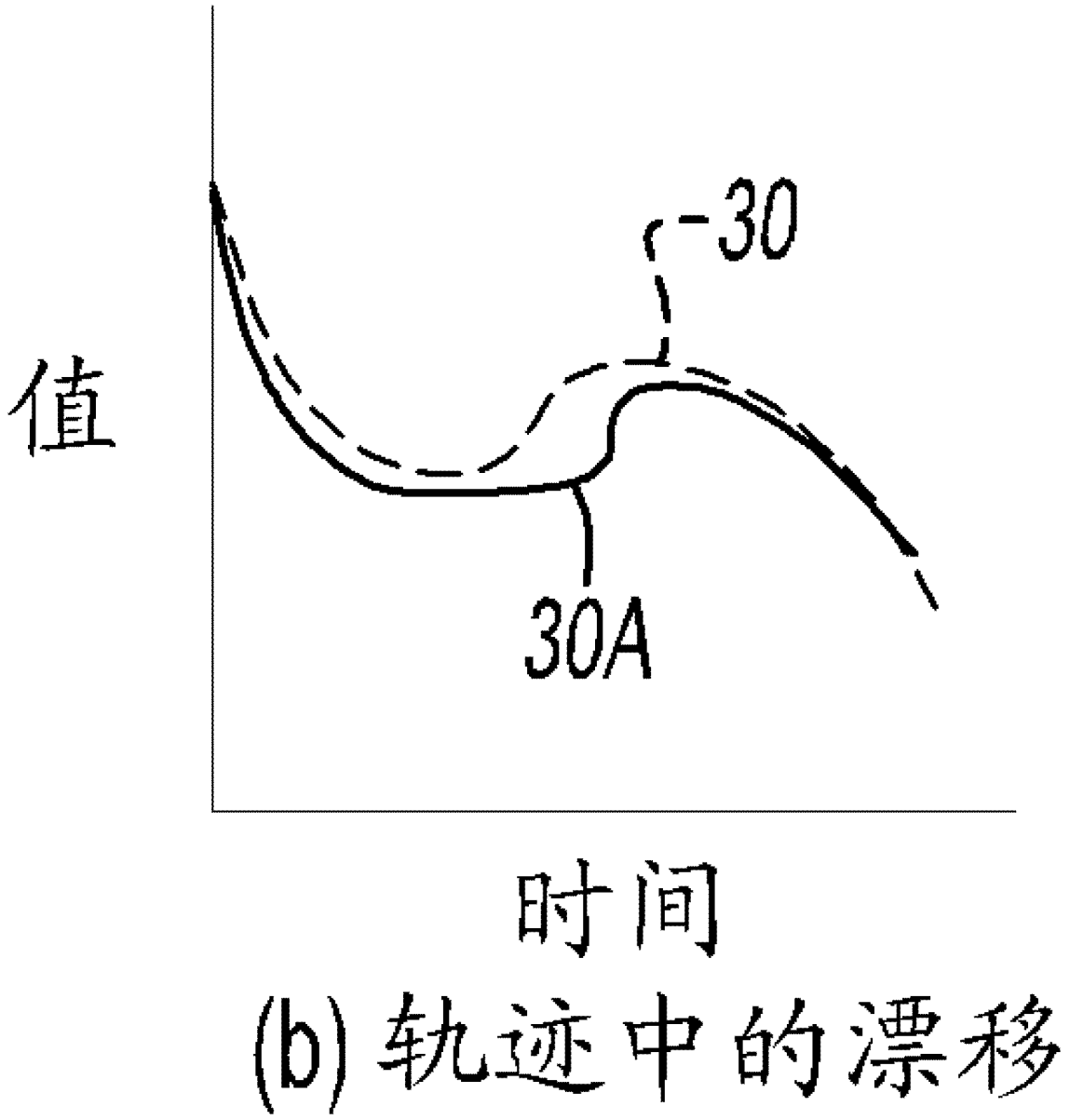


图 2B

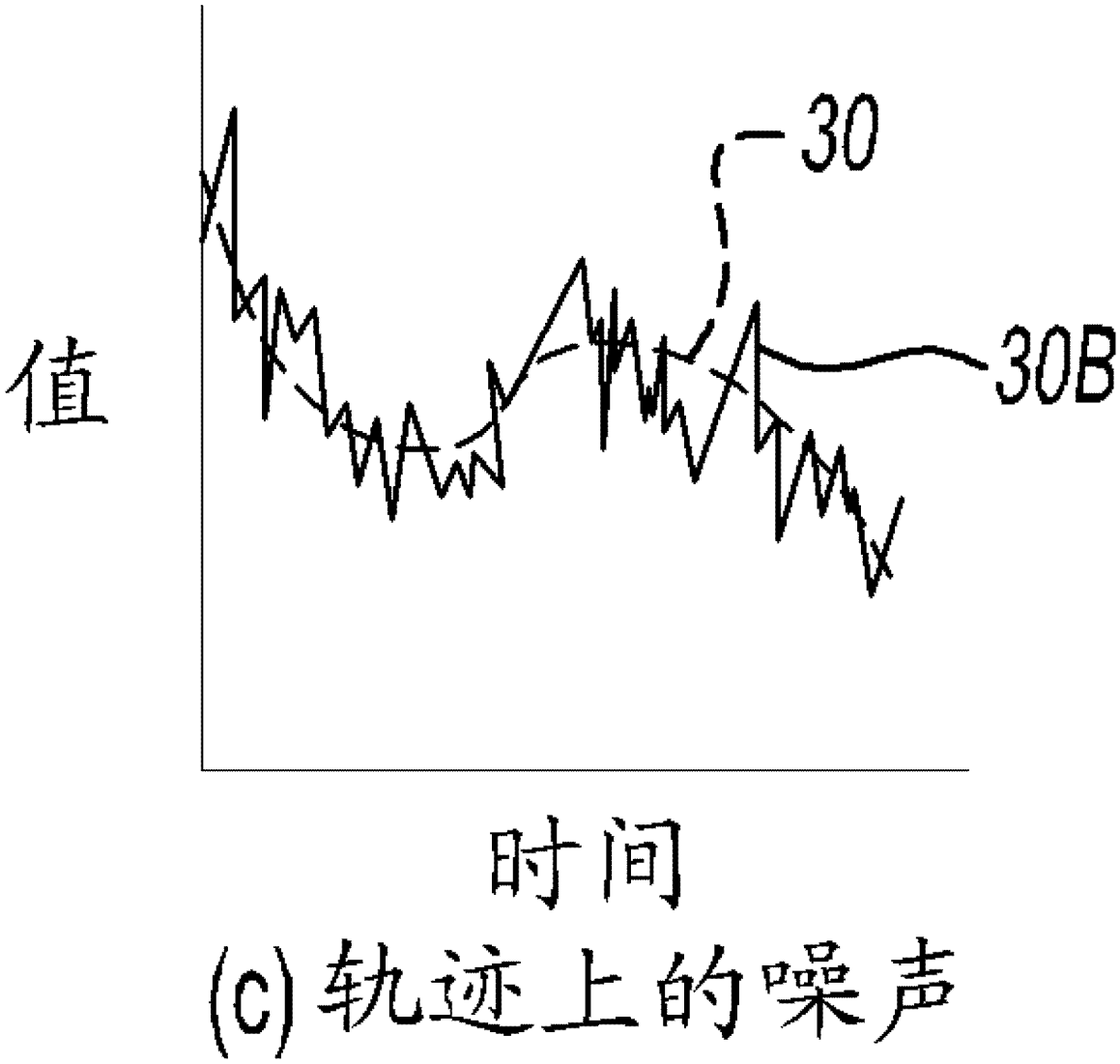


图 2C

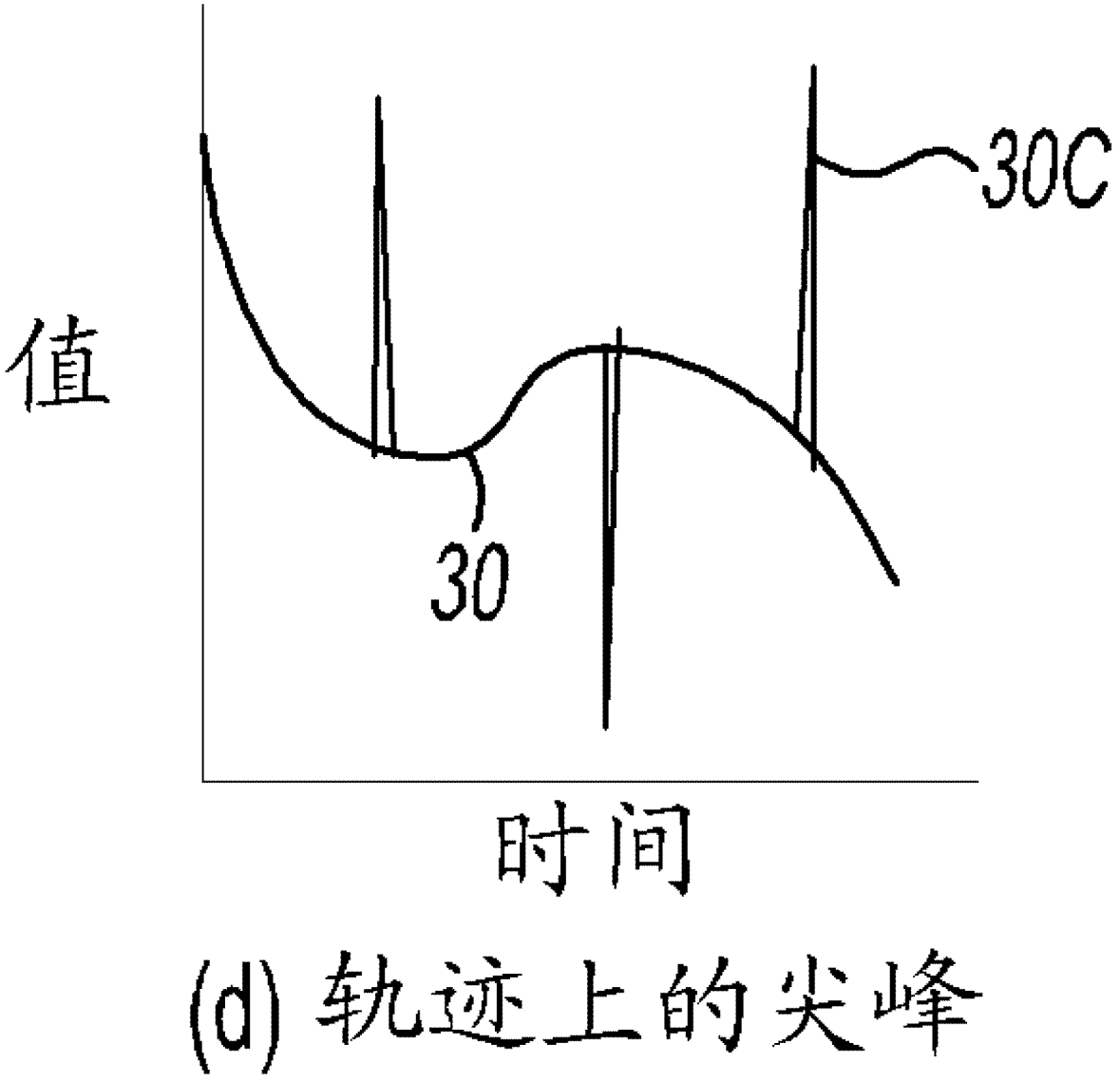
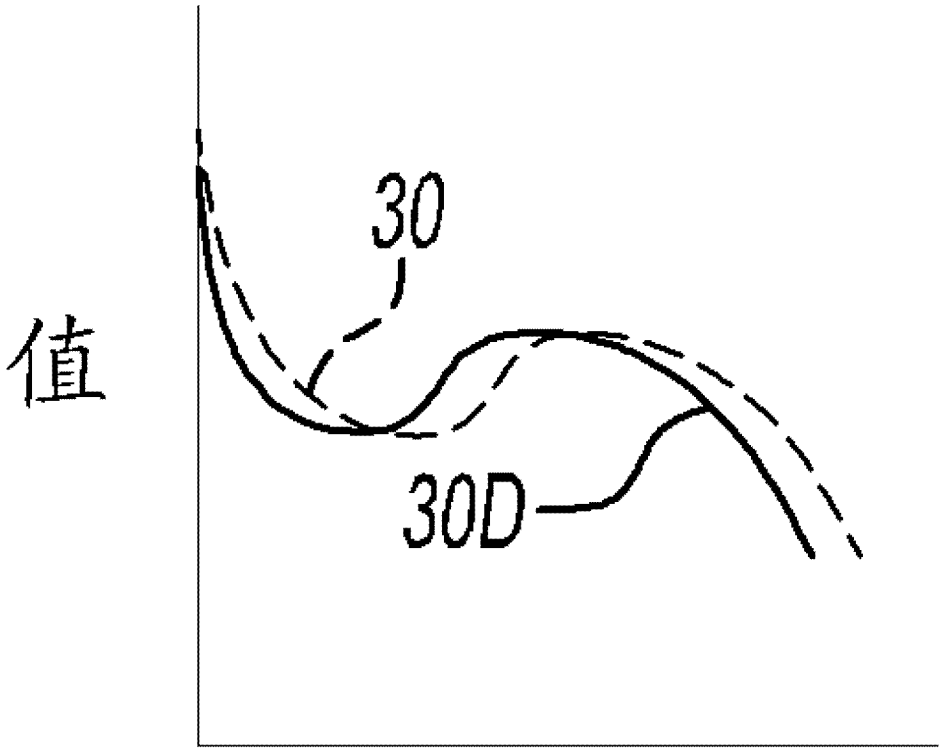


图 2D



(e)导致漂移的延时误差

图 2E

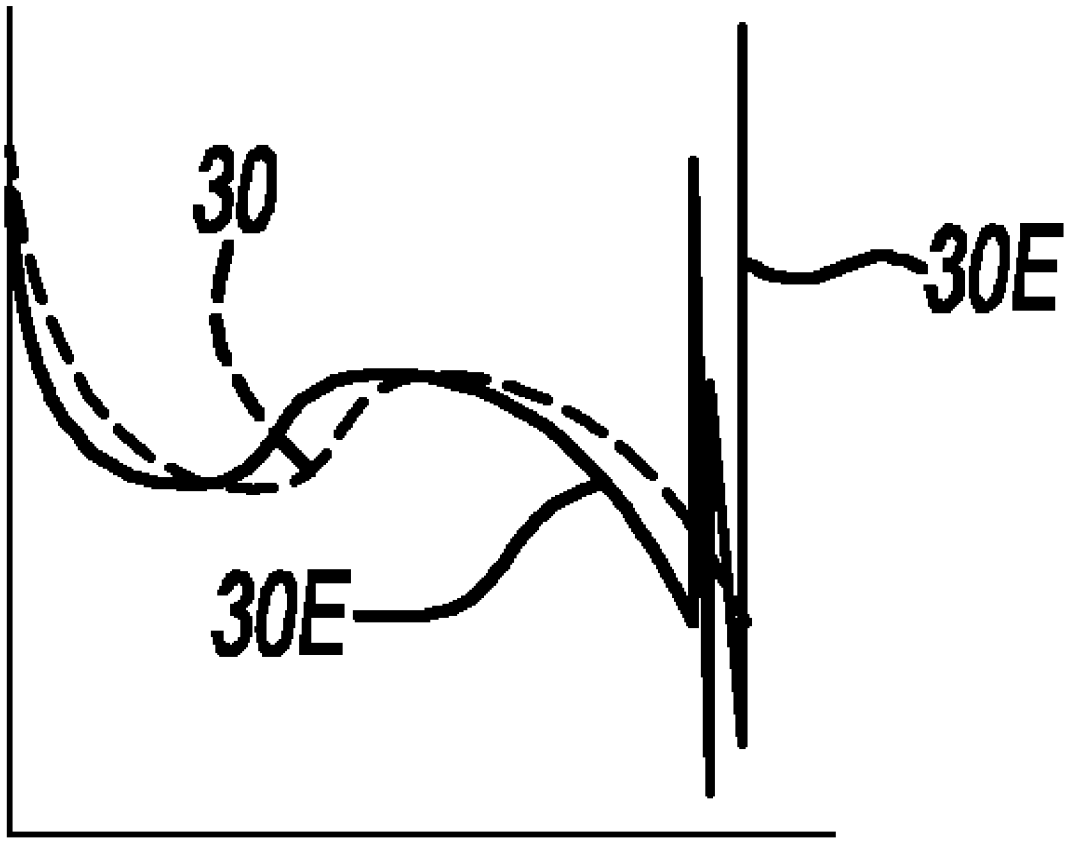


图 2F

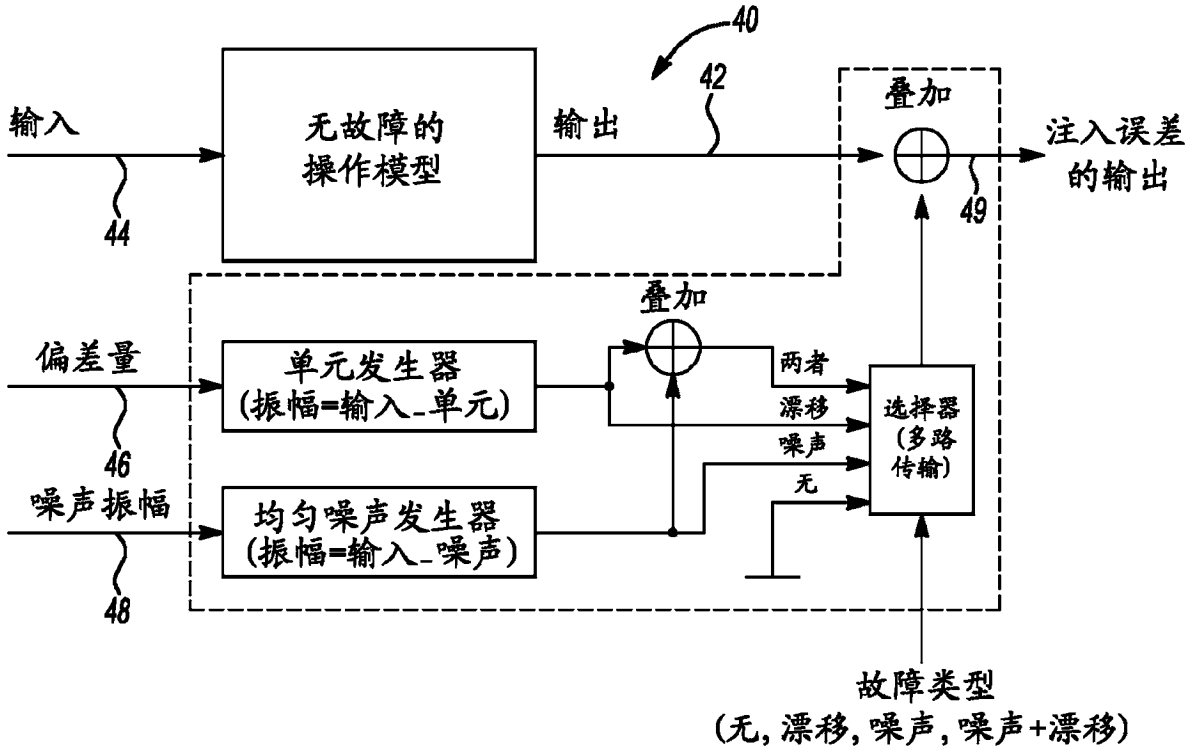

40
42
输入
无故障的
操作模型
输出
叠加
注入误差
的输出
44
49
叠加
偏差量
单元发生器
(振幅=输入_单元)
两者
漂移
噪声
无
选择器
(多路
传输)
46
噪声振幅
均匀噪声发生器
(振幅=输入_噪声)
48
故障类型
(无,漂移,噪声,噪声+漂移)

图 3

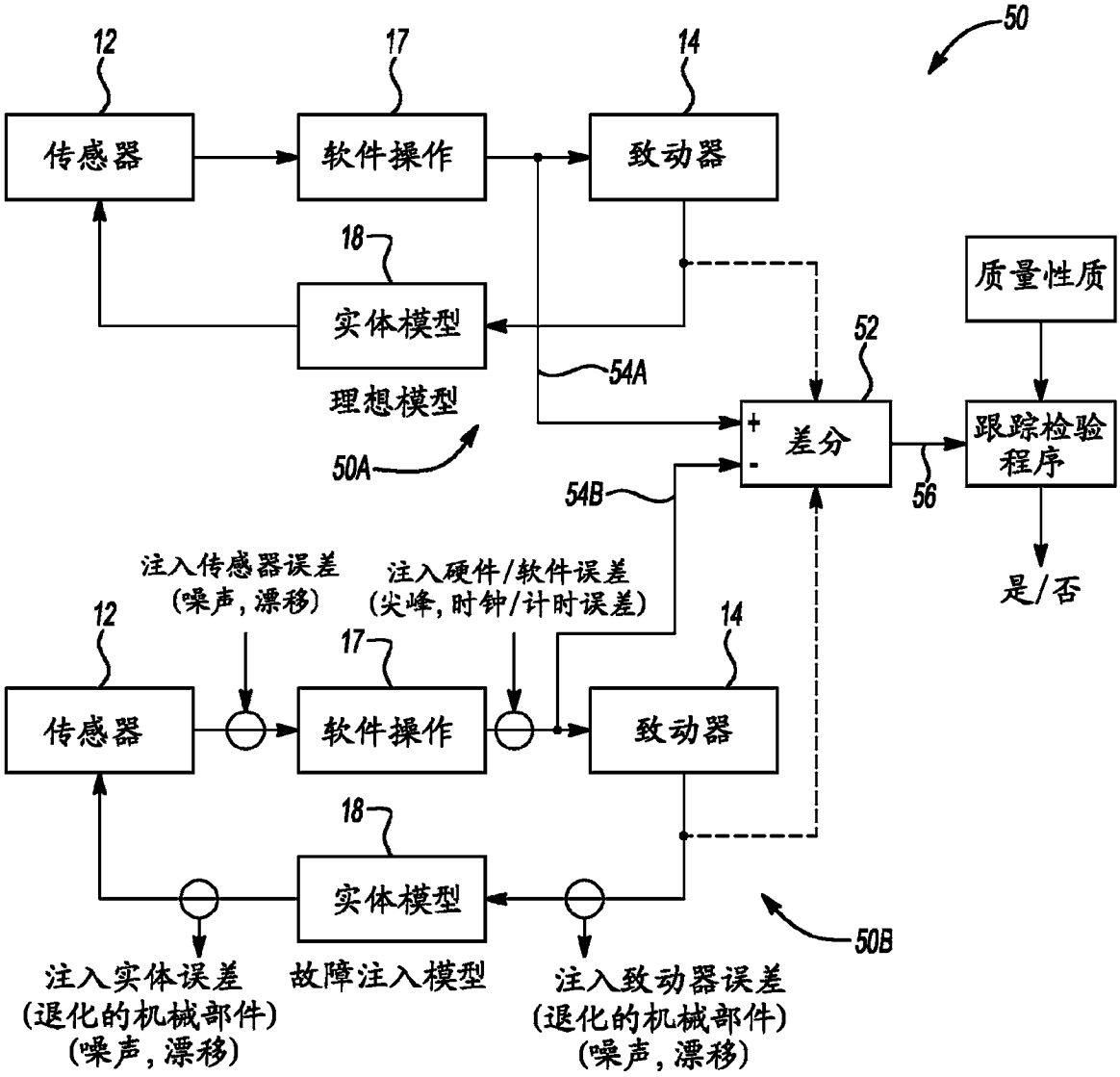
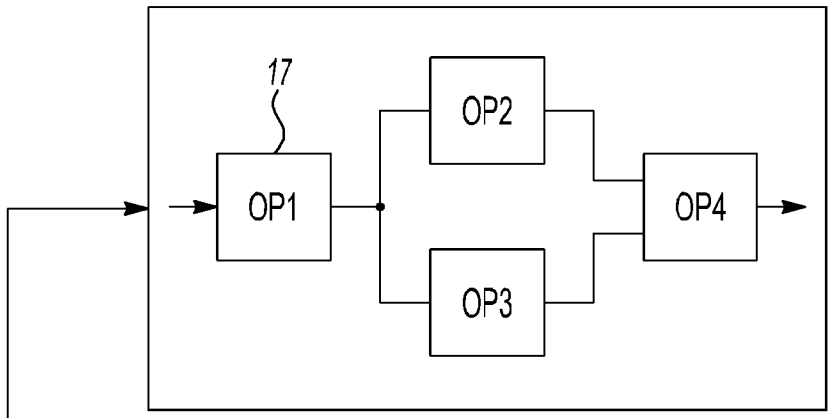

50
12
17
14
传感器
软件操作
致动器
18
实体模型
理想模型
50A
54A
质量性质
52
差分
跟踪检验程序
54B
56
是/否
注入传感器误差
(噪声,漂移)
注入硬件/软件误差
(尖峰,时钟/计时误差)
12
17
14
传感器
软件操作
致动器
18
实体模型
50B
注入实体误差
(退化的机械部件)
(噪声,漂移)
故障注入模型
注入致动器误差
(退化的机械部件)
(噪声,漂移)

图 4



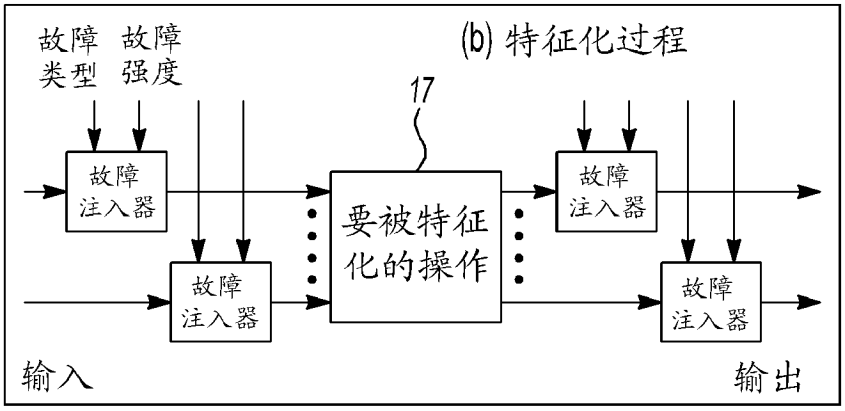
(a) 操作层模型

高精度
低速

操作层模型
(每一种操作都
通过数学/混合/
布尔函数建模)

图 5A

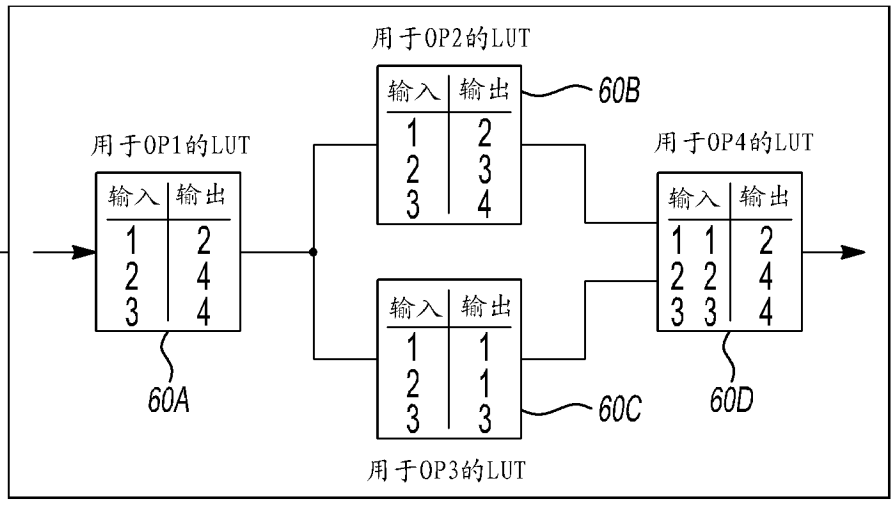
通过特征化
提取



将LUT模型中的
错误流程映射
到操作层模型
中的流程

图 5B

通过符号查找表
来替换操作



(c) 通过查找
表来替换
操作

低精度
高速

数学模型
(每一种操
作都通过质
量查找表/布
尔函数建模)

图 5C

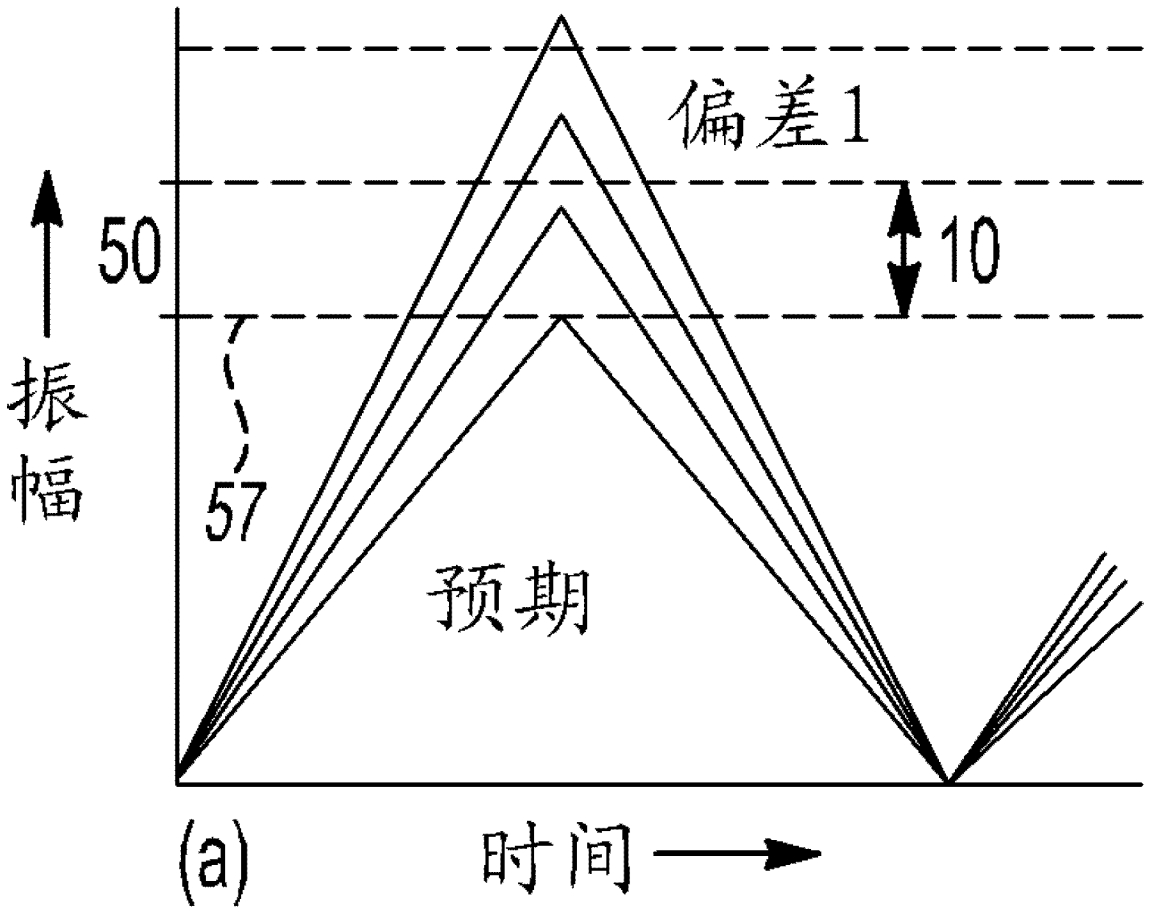


图 6A

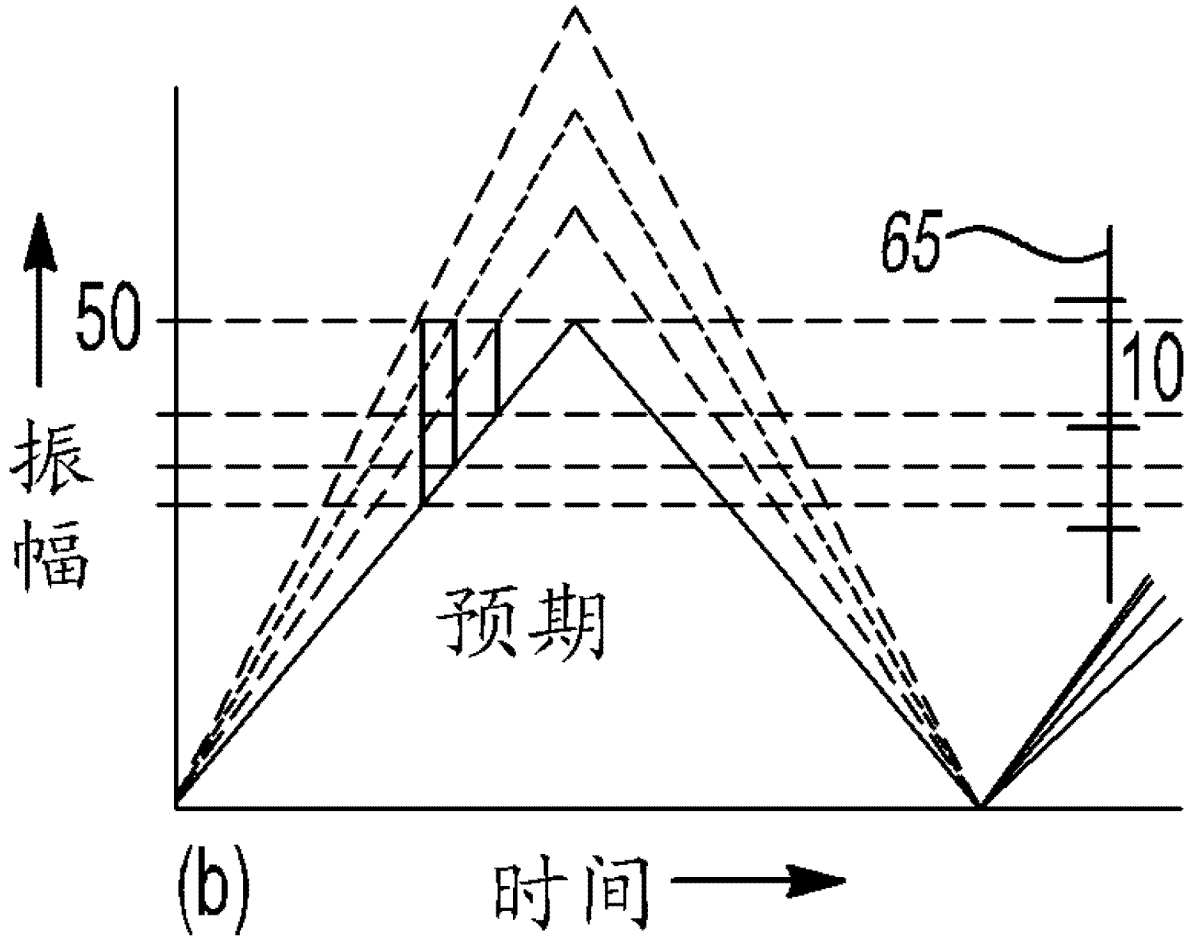


图 6B

输入质量	输出质量
假	假
1	1
2	2
3	2
0	0

(C)

图 6C

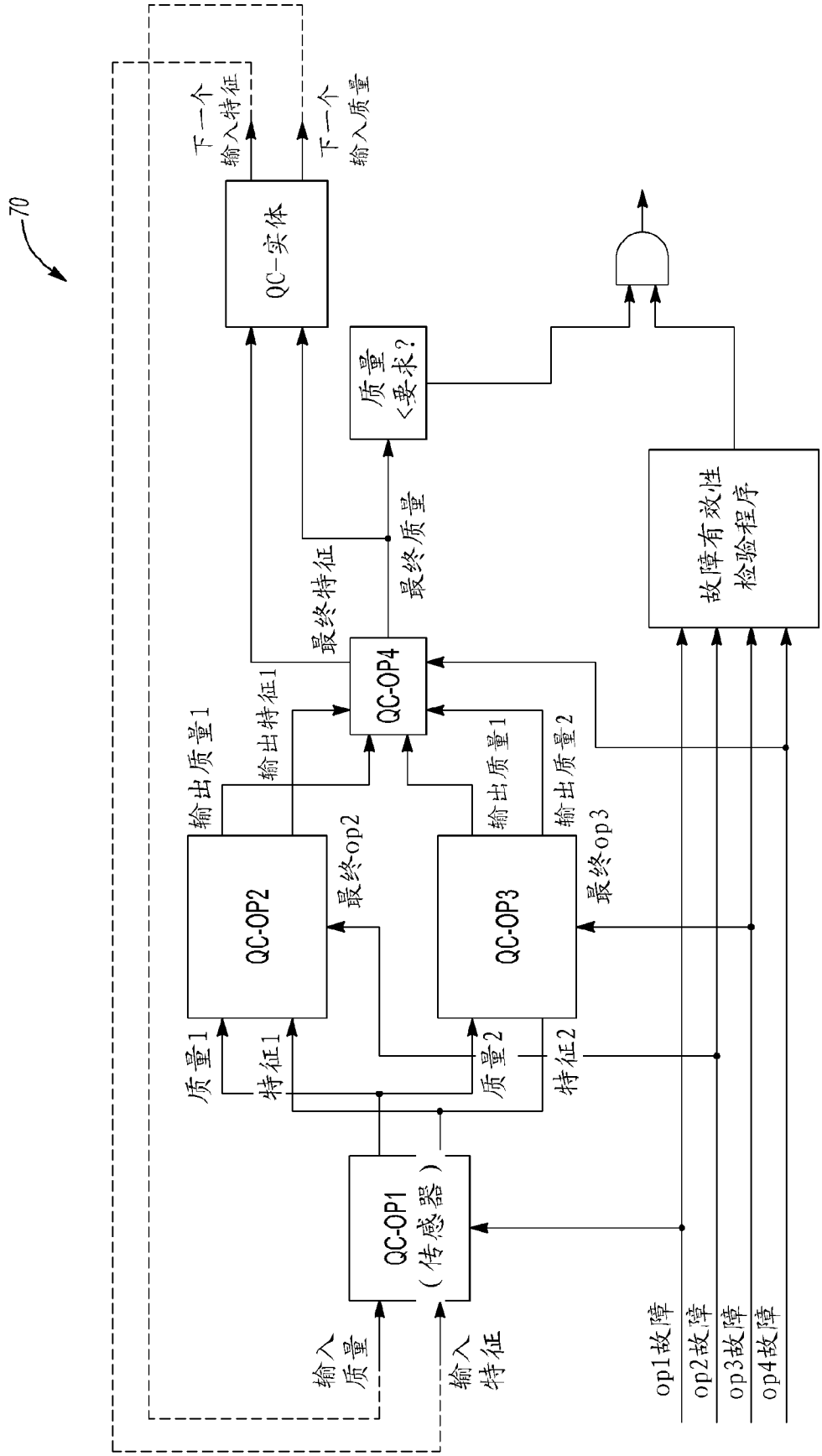

70
下一个输入特征
下一个输入质量
QC-实体
质量<要求?
故障有效性检验程序
最终特征
最终质量
QC-OP4
输出质量1
输出特征1
输出质量1
输出质量2
QC-OP2
QC-OP3
最终op2
最终op3
质量1
特征1
质量2
特征2
QC-OP1（传感器）
输入质量
输入特征
op1故障
op2故障
op3故障
op4故障

图 7