(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 1693921 B
(45)授权公告日 2010.04.28

(21)申请号 200510068995.6

(22)申请日 2005.04.30

(30)优先权数据
0404805 2004.05.05 FR

(73)专利权人 伊斯帕诺－叙扎公司
地址 法国科隆布

(72)发明人 于格·格拉涅尔
克里斯蒂安·布勒甘特
菲利普·托内利耶
马克·克鲁瓦·马里

(74)专利代理机构 永新专利商标代理有限公司
72002
代理人 夏青

(51)Int.Cl.
G06F 17/50(2006.01)
G01R 31/28(2006.01)
G01R 31/317(2006.01)

(56)对比文件
US 5909374 A,1999.06.01, 全文.
CN 1658199 A,2005.08.24, 摘要、说明书第9-14页、附图1,3-5.
US 2003/0191565 A1,2003.10.09, 全文.

审查员 齐爽

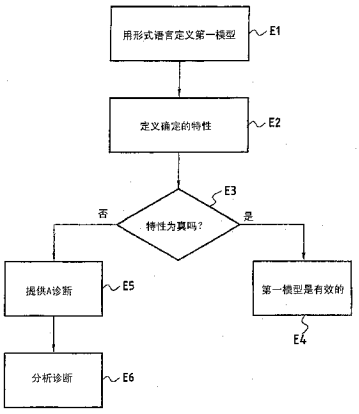
权利要求书 2 页 说明书 7 页 附图 6 页

(54)发明名称

检查物理系统模型的鲁棒性

(57)摘要

本发明提供用于一种检验物理系统模型的鲁棒性的系统和方法，该方法包括下列步骤：定义一个物理系统的第一模型(10)，该第一模型(10)包括一组(12)部件(12a、12b、12c)和至少一个用于插入输入值的输入接口(14)，该第一模型利用描述每个所述部件之工况和功能形式语言定义；用形式语言定义确定的特性，该物理系统的模型必须满足该确定的特性；用形式语言定义了一个第二模型(20)，该第二模型(20)对应于第一模型并且新增了故障引入机制(22)；以及使用形式检验装置自动搜索引起所述确定的特性失效的引入故障和/或输入值的组合。



CN 1693921 B

1. 一种验证物理系统之模型的鲁棒性的方法，该方法的特征在于：它包括以下的步骤：

定义物理系统的第一模型 (10)，该第一模型 (10) 包括一组 (12) 部件 (12a、12b、12c) 和至少一个用于插入输入值的输入接口 (14)，所述第一模型利用描述每个所述部件之工况和功能的形式语言定义；

利用所述形式语言定义所述物理系统的所述第一模型必须满足的确定的特性；

使用形式检验装置自动搜索若干输入值的组合，该组合引起所述确定的特性相对于所述第一模型 (10) 失效；

提供诊断，包含引起所述确定的特性失效的输入值的序列；

根据所述诊断，修正所述第一模型 (10) 以便满足所述确定的特性，或者证实通过所述形式检验装置发现的输入值的组合是不可能发生的；

在所述确定的特性被验证为相对于所述第一模型为真的情况下，利用所述形式语言定义所述物理系统的第二模型 (20)，该第二模型对应于第一模型并且新增了故障引入机制 (22)；以及

使用形式检验装置自动搜索引起所述确定的特性相对于所述第二模型 (20) 失效的引入故障和 / 或输入值的组合。

2. 如权利要求 1 所述的方法，其特征在于：该故障引入机制 (22) 包括经由故障输入接口 (24) 将至少一个故障引入到第二模型 (20) 中。

3. 如权利要求 2 所述的方法，其特征在于：该故障引入机制 (22) 还包括利用形式语言描述所述至少一个故障对所述物理系统的每个部件之功能或工况的影响。

4. 如权利要求 1 所述的方法，其特征在于：当形式检验装置不能发现引起所述确定的特性失效的引入故障和 / 或输入值的组合时，所述确定的特性被认为相对于第二模型 (20) 是真的。

5. 如权利要求 4 所述的方法，其特征在于：物理系统的模型被认为相对于所述确定的特性是鲁棒的。

6. 如权利要求 1 所述的方法，其特征在于：当形式检验装置发现至少一个引起所述确定的特性失效的引入故障和 / 或输入值的组合时，所述确定的特性被认为相对于第二模型 (20) 是假的。

7. 如权利要求 6 所述的方法，其特征在于：所述引起确定的特性失效的引入故障和 / 或输入值的组合对应于一个方案，该方案能使物理系统的模型被纠错，从而使它更鲁棒。

8. 如权利要求 1 至 7 中任意一个所述的方法，其特征在于：故障组合是从预先定义的故障集合中选择的。

9. 如权利要求 1 至 7 中任意一个所述的方法，其特征在于：所述确定的特性表示所述物理系统的状态或工况。

10. 如权利要求 9 所述的方法，其特征在于：所述确定的特性是所述物理系统的安全特性。

11. 一种用于验证物理系统之模型的鲁棒性的系统，该系统的特征在于：它包括：

定义所述物理系统的第一模型 (10)，该第一模型 (10) 包括一组 (12) 部件 (12a、12b、12c) 和至少一个用于插入输入值的输入接口 (14)，所述第一模型利用描述每个所述部件

之工况和功能的形式语言定义；

利用所述形式语言定义的预先确定的特性，其中所述物理系统的所述第一模型必须满足该预先确定的特性；

自动搜索若干输入值的组合的形式检验装置，该组合引起所述预先确定的特性相对于所述第一模型 (10) 失效；

提供诊断，包含引起所述确定的特性失效的输入值的序列的装置；

根据所述诊断，修正所述第一模型 (10) 以便满足所述确定的特性，或者证实通过所述形式检验装置发现的输入值的组合不可能发生的装置；

利用所述形式语言定义的所述物理系统的第二模型 (20)，该第二模型对应于所述第一模型并且新增了用于引入故障的机制 (22)，在所述预先确定的特性被验证为相对于所述第一模型为真的情况下，定义所述第二模型 (20)；和

形式检验装置，用于自动搜索引起所述预先确定的特性相对于所述第二模型 (20) 失效的引入故障和 / 或输入值的组合。

12. 如权利要求 11 所述的系统，其特征在于：用于引入故障的机制 (22) 包括一个故障输入接口 (24) 和故障应用装置 (26)。

13. 如权利要求 11 或 12 所述的系统，其特征在于：所述物理系统是一个电子系统，该电子系统包括两个用于控制飞机引擎的计算机。

检查物理系统模型的鲁棒性

技术领域

[0001] 本发明涉及检查面对故障出现时物理系统模型的鲁棒性的领域。

背景技术

[0002] 在多数行业中，例如在航空或者航天行业中，通常要依赖系统模型。例如，设计用于完成某些给定任务的物理系统的模型，并且该模型被用于评估系统和它所处环境之间的相互影响。这可以使用硬件手段或软件手段来完成。

[0003] 具体来讲，使用故障检测逻辑电路、重构逻辑电路和部件的冗余，以使系统可以容错。

[0004] 不幸的是，实际上，模型很难考虑到所有的可能性。经常会忘记一些特殊的情况，或者出现时序逻辑错误，使得故障的某些序列或者特定组合仍旧能导致系统失效。

[0005] 为了解决这些问题，真实的系统要通过标准检测程序的测试，以便验证它们的鲁棒性。但是，在发现真实系统中的缺陷时，必须重新设计该系统，这意味着大量新的工程上的费用开销、硬件和软件的返工和大量的时间损失。

发明内容

[0006] 因此，本发明的一个目的就是，通过提出一种验证电子系统模型当面对故障时的鲁棒性的方法来解决所述问题。

[0007] 为此，本发明提供了一种验证物理系统之模型的鲁棒性的方法，其特征在于：它包括如下步骤：

[0008] 定义物理系统的第一模型，该第一模型包括一组部件和至少一个输入接口，该至少一个输入接口用于插入输入值，所述第一模型是利用描述每个所述部件之工况和功能的形式语言来定义的；

[0009] 利用形式语言定义一个确定的特性，该物理系统的模型必须满足该确定的特性；

[0010] 利用形式语言定义第二模型，第二模型对应于第一模型并且新增了故障引入机制；以及

[0011] 使用形式检验装置自动搜索引起所述确定的特性失效的引入故障和/或输入值的组合。

[0012] 因此，第二模型使在面对故障时鲁棒的物理系统能够被设计出来，并且具体地由于可以在制造该系统之前实现，因此可以减少开发系统的花销。

[0013] 这种方法使得可以通过考虑系统的故障和/或输入值的各种组合，来验证系统的特性。

[0014] 同时，可以通过彻底检验任何可以想到的故障或故障序列，制造出具有高质量和高安全性的系统。

[0015] 根据本发明的一个特征，故障引入机制包括经由故障输入接口将至少一个故障引入到第二模型。

[0016] 根据本发明的另一个特征，故障引入机制还包括利用形式语言来描述所述至少一个故障对所述电子系统的每个部件之功能或工况的影响。

[0017] 当形式检验装置不能发现引起所述确定的特性失效的引入故障和／或输入值的组合时，所述确定的特性被认为相对于第二模型是真的。在该情况下，该物理系统的模型被认为相对于所述确定的特性是鲁棒的。

[0018] 当形式检验装置发现了引起所述确定的特性失效的至少一个引入故障和／或输入值的组合时，所述确定的特性被认为相对于第二模型是假的。在该情况下，所述引起所述确定的特性失效的引入故障和／或输入值的组合对应于一个方案，该方案能使物理系统的模型被修正，以便使它更鲁棒。

[0019] 优选地，从预定义的故障集合中选择故障的组合。

[0020] 确定的特性表示所述物理系统的一个状态或工况。它可以是所述物理系统的安全特性。

附图说明

[0021] 在阅读了以下通过非限定说明的方式和参照附图给出的描述后，会更清楚本发明的方法和系统的其它特征和优点，其中：

[0022] 图 1 是在本发明的方法和系统中实现的硬件装置的透视图；

[0023] 图 2 是根据本发明的用于设计物理系统的一个模型的示意图；

[0024] 图 3 是显示用于确定图 2 中所示第一模型的有效性的主要步骤的流程图；

[0025] 图 4 是显示根据本发明的第二模型的示意图，其中该第二模型对应于物理系统第一模型并且新增了故障引入机制；

[0026] 图 5 是显示根据本发明的用于验证物理系统的模型面对故障时的鲁棒性的主要步骤的流程图；

[0027] 图 6 是根据本发明的电子系统第一模型的例子的示意图，该第一模型模拟第一计算机，第二计算机和导线设备；

[0028] 图 7 是显示对应于图 6 所示的第一模型并且新增了故障引入机制的第二模型的示意图；以及

[0029] 图 8 是图 7 中用于引入故障的装置的示意图。

具体实施方式

[0030] 图 1 示出了一个可被用于模拟物理系统的系统。该系统包括一台用于运行计算机程序的工作站或计算机 1，该计算机程序用于实现本发明的方法。

[0031] 计算机 1 包括通常可以在这类设备中发现的硬件装置。更具体地说，该计算机包括一个中央单元 2，用于执行根据本发明的方法的程序指令序列；一个中央存储器 3，用于存储数据和正在执行的程序；数字数据存储介质（硬盘、致密盘 (CD)4、软盘 .....），用于长期存储使用中的数据和程序；输入外围设备（键盘 5、鼠标 6.....），以及输出外围设备（屏幕 7、打印机 .....），用于能够查看物理系统的模型。

[0032] 根据本发明，图 2 示出了一个第一模型 10，用于设计物理系统。该物理系统可以例如是一个电子系统，该电子系统一旦被制造，就可以支持给定的应用，例如监视或者控制用

于管理引擎的设备。

[0033] 第一模型 10 包括 :一组 12 部件 12a、12b、12c,它们之间相互通信 ;至少一个输入接口 14,用于插入输入值 ;以及至少一个输出接口 16。当然,所述部件组 12 可以在一个依赖于物理系统模型精确度或特征的抽象级别或比例上定义。

[0034] 该第一模型 10 是一个数字模型,它代表将要制造的物理系统的结构。它由“信号(Signal)”类型的形式语言定义,包括字母或变量、逻辑量词、以及逻辑连接符,从而描述了每个部件 12a、12b、12c 的工况和功能。因此,第一模型 10 使物理系统能被动态的表现。

[0035] 图 3 是示出了用于确定第一模型 10 的有效性的主要步骤的流程图。

[0036] 在步骤 E1,利用形式语言定义第一模型。

[0037] 然后,在步骤E2,也利用形式语言定义物理系统的模型必须满足的确定的特性。该特性的形式描述包括 :基于模型的变量或信号,例如利用信号语言,定义对应于所述特性的事件和对此事件进行编码。所述确定的特性通常是一个“这样的事件永远不会发生”类型的安全属性,但它也可以是一个“从该状态,在有限长的时间结束时,能够到达一个其它状态”类型的响应属性。然后,该特性必须满足或者描述第一模型的特征。

[0038] 形式语言具有形式检验装置,例如在 SILDEX™ 软件中的“形式验证器 (formal prover)”或者“检验器 (checker)”,用于相对于输入到第一模型的任何值或任何值的组合,在语义上验证所述确定的特性的真实性。

[0039] 因此,步骤 E3 是相对于输入值的任何组合来测试所述确定的特性的真实性。在这一步中,形式检验装置自动搜索引起该确定的特性失效的输入值的组合。

[0040] 如果形式检验装置不能发现引起所述确定的特性失效的输入值的组合,那么在步骤 E4 中,第一模型 10 被认为相对于所述特性是有效的。

[0041] 相反,如果所述确定的特性被认为是假的,例如,如果在步骤 E3 形式检验装置发现了至少一个引起确定的特性失效的输入值的组合,那么该方法移至步骤 E5。

[0042] 在步骤 E5,提供了一个诊断,包含引起所述确定的特性失效的输入值的序列。

[0043] 在步骤 E6,依靠上一步骤中提供的诊断,第一模型 10 或者被修正以便满足所述确定的特性,或者证实通过形式检验装置发现的输入值的组合是不可能发生的。

[0044] 根据本发明,图 4 是第二数字模型 20 的示意图,第二数字模型 20 对应于物理系统的第一模型 10 的第二数字模型 20 的示意图并且新增了故障引入机制 22。

[0045] 第二模型 20 与第一模型的不同点在于,除了包括部件 12a、12b、12c 的组 12 和输入接口 14、输出接口 16 以外,它还包括一个故障引入机制 22,故障引入机制 22 包括一个故障输入接口 24 以及一个故障应用装置 26,其中至少一个故障或故障组合通过故障输入接口 24 被引入。

[0046] 从预先定义的故障集合中选择故障或故障组合。利用形式语言模拟每个故障对第二模型 20 之工况的影响,并且故障对给定部件的影响结果在所述部件的工况图中被描述。在第二模型 20 的最小部件上的所有已知可能的故障被列出,这样将每个部件的工况图放入数据库中,该数据库存储于例如工作站或计算机 1 的中央存储器 3。

[0047] 换句话说,故障引入机制 22 包含 :利用形式语言来描述任何故障对模拟物理系统的第二模型 20 的每一个部件 12a、12b、12c 的功能或工况的影响。

[0048] 因此,第二模型对应于增加了的额外布尔输入的第一模型 10,并且作为与可预见

的故障相关联来处理。一个特定故障的输入可取值“假”或“真”之一。例如，值“假”能够对应于“无故障引入”的状态，值“真”能够对应于“故障引入”的状态。

[0049] 当故障接口 24 的所有输入都是“假”时，则第二模型在额定条件下运行。当故障输入是“真”时，它会触发与部件的工况图的应用有关的用于施加故障给该部件的逻辑。

[0050] 此外，当故障输入是“空”时，形式检验装置能在任何时间引入故障，以便搜寻一个能引起所述确定的特性失效的故障和 / 或输入值的序列或组合。

[0051] 形式检验装置是一个工具，它将逻辑规则应用到用于第二模型 20 之部件 12a、12b、12c 的公理和 / 或工况图，直到得到一个描述确定的特性的公式。

[0052] 这个形式证明工具能够通过 SILDEX™ 类型的软件提供，该软件在一个模拟期间的任何时刻，都能经由故障引入机制 22 将故障应用到第二模型 20 的部件或者功能上。

[0053] 具体地，为了证实第二模型 20 的一个确定的特性，起动 SILDEX™ 类型的形式语言的动态编译。如果编译成功，那么该确定的特性是有效的。否则，形式检验装置给出了一个包括故障和 / 或输入值序列的方案 (scenario)，该方案导致被模拟的系统具有与所述特性相矛盾的状态。

[0054] 图 5 是说明用于验证物理系统的模型面对故障出现时的鲁棒性的流程图。

[0055] 在步骤 E11，利用形式语言定义第二模型 20，其对应于新增了故障引入机制 22 的第一模型 10。

[0056] 此后，验证在图 2 的流程图的步骤 E2 定义的并且已经对于第一模型 10 验证为“真”(步骤 E4) 的所述确定的特性对于第二模型是否仍然为“真”。

[0057] 在步骤 E13 期间，相对于任何引入的故障和 / 或输入值的组合，测试所述确定的特性的真实性。在这个步骤期间，通过形式检验装置执行自动搜索，该自动搜索是针对引起所述确定的特性失效的引入故障和 / 或输入值的组合的搜索。

[0058] 如果形式检验装置不能发现任何引起所述确定的特性失效的引入故障和 / 或输入值的组合，那么该特性被认为是真的，并且因此，在步骤 E14，物理系统的模型被认为在面临与确定的特性相关的故障时是鲁棒的。

[0059] 相反，如果在步骤 E13 期间，形式检验装置发现了至少一个引起所述确定的特性失效的引入故障和 / 或输入值的组合，那么所述特性被认为是假的，因此在步骤 E15，由形式检验装置提供一个诊断。这个诊断包含经由故障输入接口 24 和输入值输入接口 14 输入的并且能导致系统进入不希望的状态的输入方案或输入序列。

[0060] 在步骤 E16，分析该诊断，例如，在每个故障引入时，检查第二模型 20 上的操作序列。这个分析用于修正物理系统模型的设计，或者相反，用于证实由形式检验装置发现的所述方案是不可能的。

[0061] 图 6 至图 8 示出了检验物理系统模型鲁棒性的简化的例子。

[0062] 在这个例子中，被设计的物理系统是一个电子系统，该电子系统包括两个用于控制飞机引擎的计算机。在正常运行中，仅有一个计算机控制着引擎，并且在两个计算机之间会有对话或数据交换发生。因此，当一个计算机停止工作时，另一个计算机必需开始运行于单机模式。在这个例子中，系统失效是指两个计算机同时发生故障，或者是被动造成的，或者是主动造成的。

[0063] 因此，图 6 示出了物理系统第一模型 110 的例子，该模型模拟了一个第一计算机

112a，该112a有一个第一输入接口114a和一个第一输出接口116a，还模拟了一个第二计算机112b，该112b有一个第二输入接口114b和一个第二输出接口116b，还有一个计算机间的导线设备112c，该导线设备112c具有连接导线，其能使第一计算机112a和第二计算机112b进行对话或者数据交换。箭头F1表示由第一计算机112a传向第二计算机112b的信号或数据（用信号语言记为S_1_2），以及箭头F2表示由第二计算机112b传向第一计算机112a的信号或数据（用信号语言记为s_2_1）。

[0064] 图7示出了物理系统的第二模型120，其对应于图6中的第一模型110并且新增了故障引入机制122，故障引入装置122包含一个故障输入接口124和一个故障应用装置126。在这个例子中，故障应用装置126包括开关装置，该开关装置用于模拟单连接导线的断路故障，或者导线短路故障，或者导线设备112c没有连接的故障。箭头F1a表示离开第一计算机112a的信号s_1_2，箭头F1b表示在通过故障应用装置126后进入第二计算机112b的信号s_2_1_v。箭头F2b指明离开第二计算机112b的信号s_2_1，箭头F2a表示在通过故障应用装置126后进入第一计算机112a的信号s_1_2_v。当没有故障时，离开第一计算机112a或者第二计算机112b的信号分别无改动的进入到第二计算机112b或第一计算机112a。相反，当发生故障时，离开计算机112a或112b之一的信号无法到达它的目的地。用信号语言，这可以表示为下列等式：

[0065] s_1_2_v = s_1_2when not fault

[0066] s_2_1_v = s_2_1when not fault

[0067] 图8是示出了故障引入机制特别是图7中的故障应用装置126的示意图。故障应用装置126包括一个对应于“导线设备未连接”的第一故障输入124a，以及一个对应于“对话导线中断”的第二故障输入124b。第一和第二故障输入124a和124b被连接到一个逻辑“或(OR)”门132的输入端，该逻辑“或”门132的输出被施加到一个第一连接/断开装置134，用于向第二计算机112b传输或者不传输来自第一计算机112a的数据，以及被施加到一个第二连接/断开装置134，用于向第一计算机112a传输或者不传输来自第二计算机112b的数据。

[0068] 故障输入可以被想象为用于将故障施加到所模拟的部件的按钮。因此，在模拟中，可以在任何期望的时刻引入故障。

[0069] 当形式检验装置承担对引起确定的特性失效的引入故障和/或输入值的组合的自动搜索时，设置为“假”值的输入不涉及对相反例子(counter-example)的方案的搜索。只有空输入涉及这个搜索。

[0070] 因此，当没有故障被引入到第一连接装置134时，输入信号SA_e、SB_e、SC_e、SD_e分别等于连接装置134的输出信号SA_s、SB_s、SC_s、SD_s。在这种情况下，能够由第一连接装置134实现传输来自第一计算机112a的信号SA_1_2、SB_1_2、SC_1_2、SD_1_2，并且将它们传送到第二计算机，分别被写为：SA_1_2_v、SB_1_2_v、SC_1_2_v、SD_1_2_v。

[0071] 类似的，当没有故障被引入第二连接装置136时，输入信号SE_e、SF_e、SG_e、SH_e分别等于从连接装置输出的信号SE_s、SF_s、SG_s、SH_s。在这种情况下，能够由第二连接装置136实现传输来自第一计算机112b的信号SE_1_2、SF_1_2、SG_1_2、SH_1_2，并且将它们传送到第一计算机112a，分别被写为为：SE_1_2_v、SF_1_2_v、SG_1_2_v、SH_1_2_v。

[0072] 当对应于“导线设备未连接”的第一故障输入124a和/或对应于“对话导线中断”

的第二故障输入 124b 为空时，形式检验装置或“验证器”能在任何时间引入导线设备未连接和 / 或电路断开。在这种情况下，由计算机 112a 或 112b 之一传输的信号不能到达另一个计算机。

[0073] 在初始化之后，上面的例子能够用信号语言写成如下形式：

[0074]
```
process xxx_process_sildex_1 =
        ( ? boolean SA_e、fault、SB_e、SC_e、SD_e ;
          |boolean SA_s、SB_s、SC_s、SD_s ;)
        (|      (|SA_s = SA_e when not fault
                 |SB_s = SB_e when not fault
                 |SC_s = SC_e when not fault
                 |SD_s = SD_e when not fault
                 |fault ∧= SA_e ∧= SB_e ∧= SC_e ∧= SD_e
                 |)
        |) ;
process xxx_process_sildex_2 =
        ( ? boolean SE_e、fault、SF_e、SG_e、SH_e ;
          |boolean SE_s、SF_s、SG_s、SH_s ;)
        (|    (|SE_s = SE_e when not fault
                |SF_s = SF_e when not fault
                |SG_s = SG_e when not fault
                |SH_s = SH_e when not fault
                |fault ∧= SE_e ∧= SF_e ∧= SG_e ∧= SH_e
                |)
        |) ;
```

[0094] 通常，在具有两个计算机的物理系统的模型中，能够检查下面的两个特性：“系统模型不能发现它自身具有两个计算机处于主动状态”，以及“系统模型不能发现它自身具有两个计算机处于被动状态”。

[0095] 此外，可以设计来模拟在系统接通时存在单个故障的状况。在这种情况下，可以验证在接通状态时的任何故障是否会引起系统呈现出上述特性。

[0096] 而且，可以设计来模拟两个计算计算机同时起动的操作时存在单个故障的情况。在这种情况下，假设每个单个故障都能在任何时刻被引入。为此，正在考虑的故障输入能够设置为空，同时保持其它所有的输入都为“假”。

[0097] 可以从预先定义的故障集合中选择故障，故障集合包括以下故障：无故障、自动检测失败、断路、短路、打断发送、导线设备未连接、同步故障、强迫为“假”的 NVM 故障、强迫为“真”的 NVM 故障、强迫为“假”的 PPAVM 信号故障、强迫为“真”的 PPAVM 信号故障、PPAVMTPB、计算机故障、强迫为“假”的 PH 信号故障、强迫为“真”的 PH 信号故障等等。

[0098] 这样，本发明可以在制造物理系统之前验证模型面对故障时的鲁棒性，由此能够制造具有良好安全性的系统，同时减少系统开发的开销。

[0099] 当然，本发明也能够验证已制造的物理系统的鲁棒性。在这种情况下，使用形式语

言的模型，模拟该物理系统，并且以上述参考面对故障时的系统之确定特性所定义的标准描述的方式，检查物理系统模型的鲁棒性。

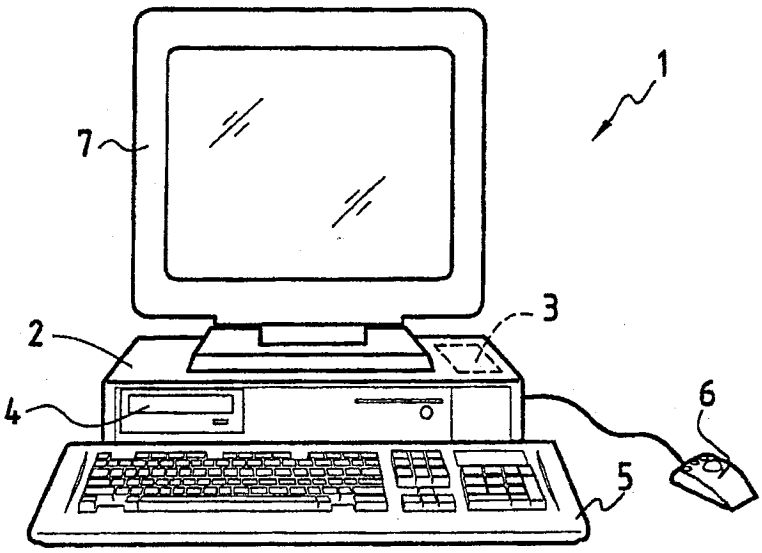


图 1

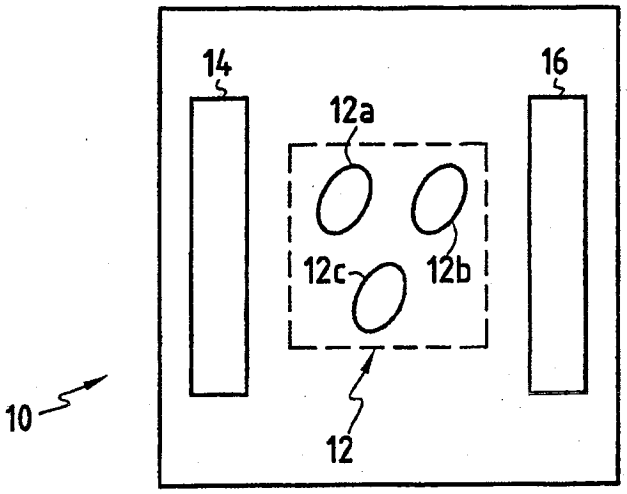


图 2

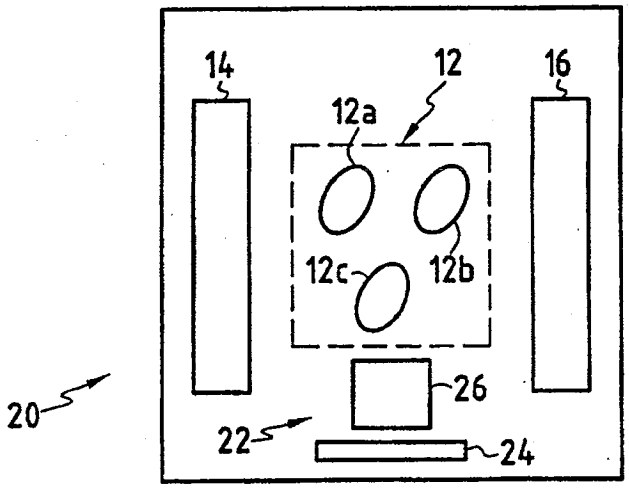


图 4

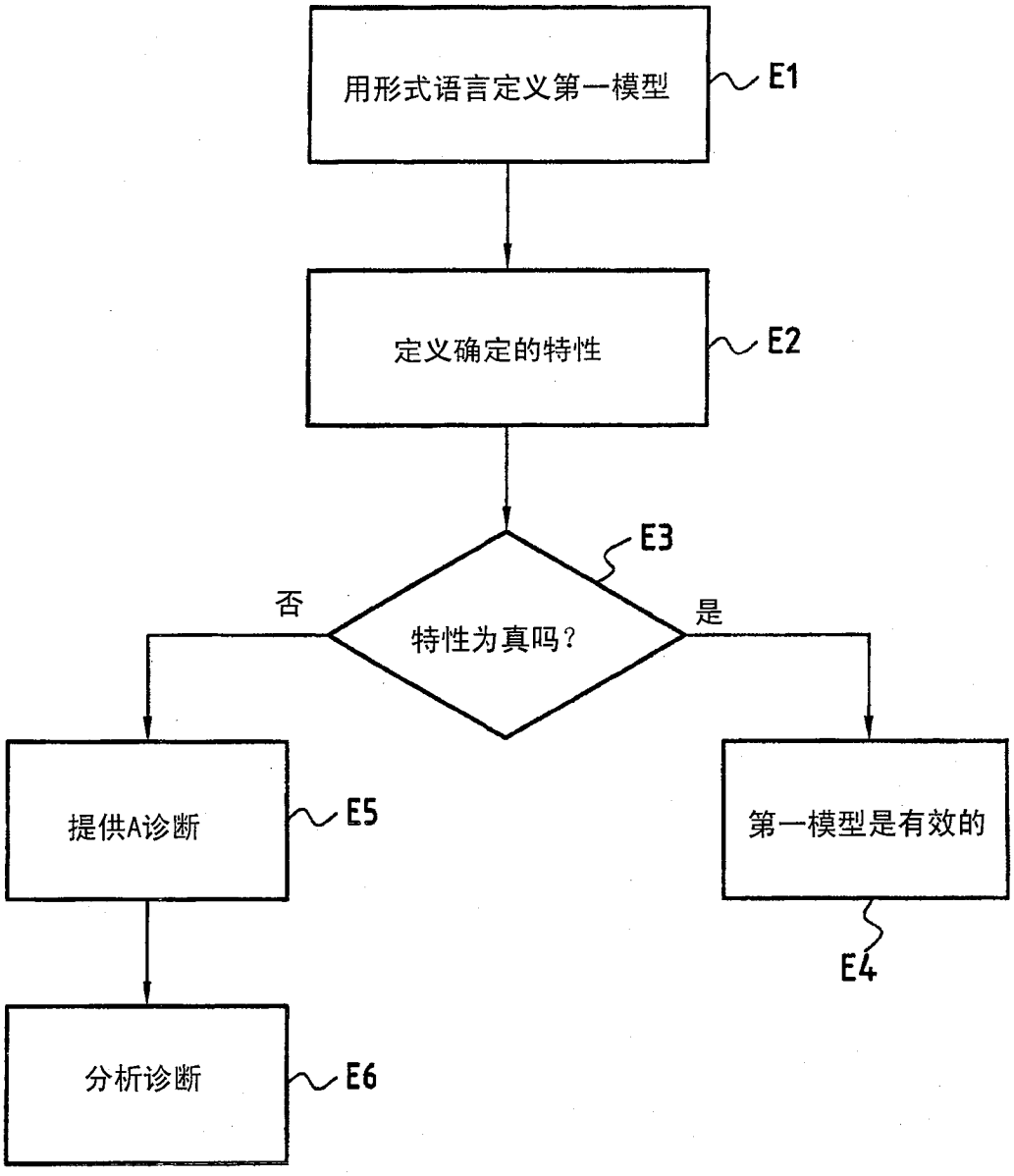

用形式语言定义第一模型
E1
定义确定的特性
E2
E3
特性为真吗？
否
是
提供A诊断
E5
第一模型是有效的
E4
分析诊断
E6

图 3

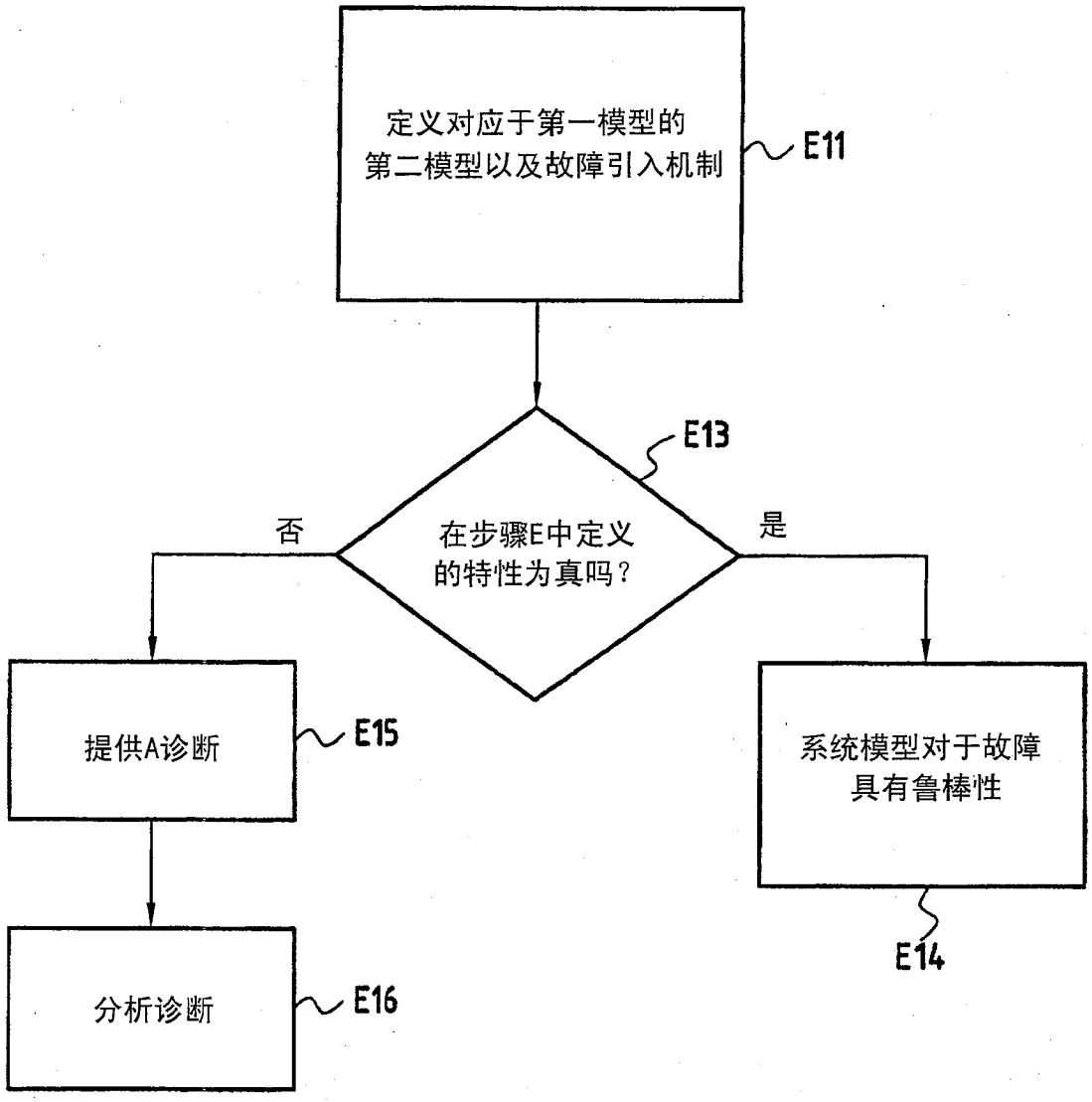

定义对应于第一模型的
第二模型以及故障引入机制
E11
E13
在步骤E中定义
的特性为真吗？
否
是
提供A诊断
E15
分析诊断
E16
系统模型对于故障
具有鲁棒性
E14

图 5

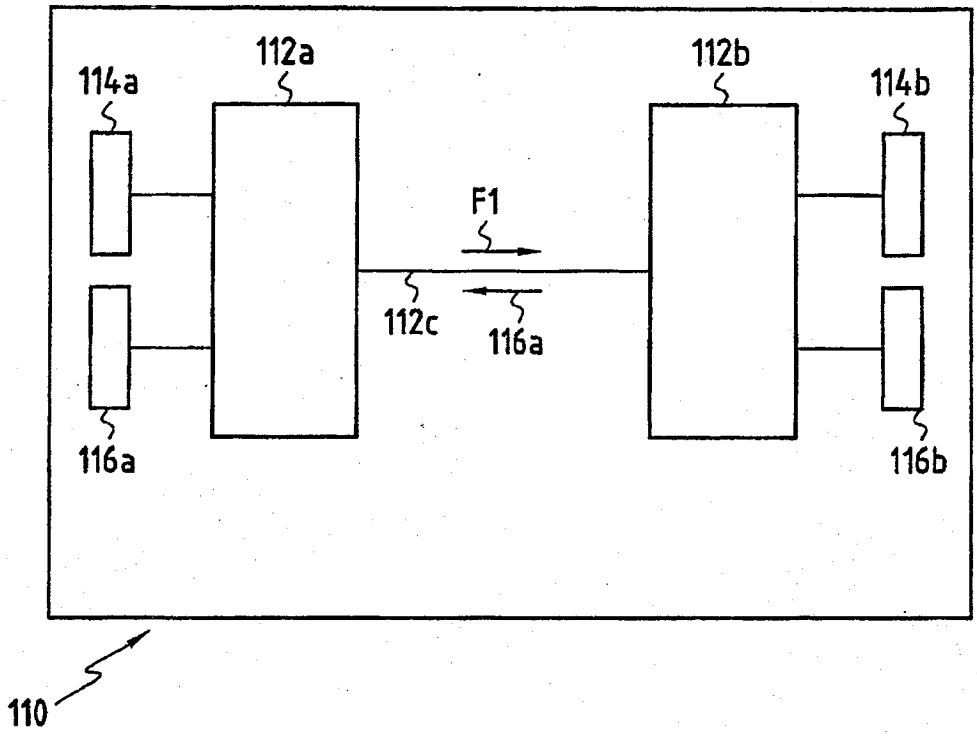

112a
112b
114a
114b
F1
112c
116a
116a
116b
110

图 6

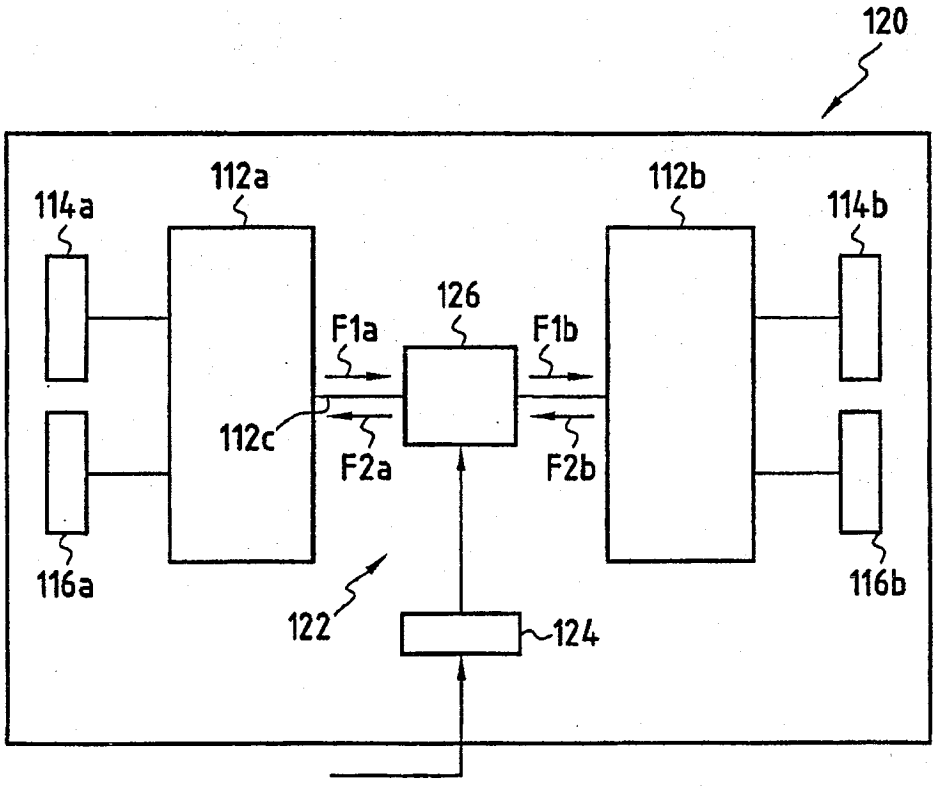

120
112a
112b
114a
114b
126
F1a
F1b
112c
F2a
F2b
116a
116b
122
124

图 7

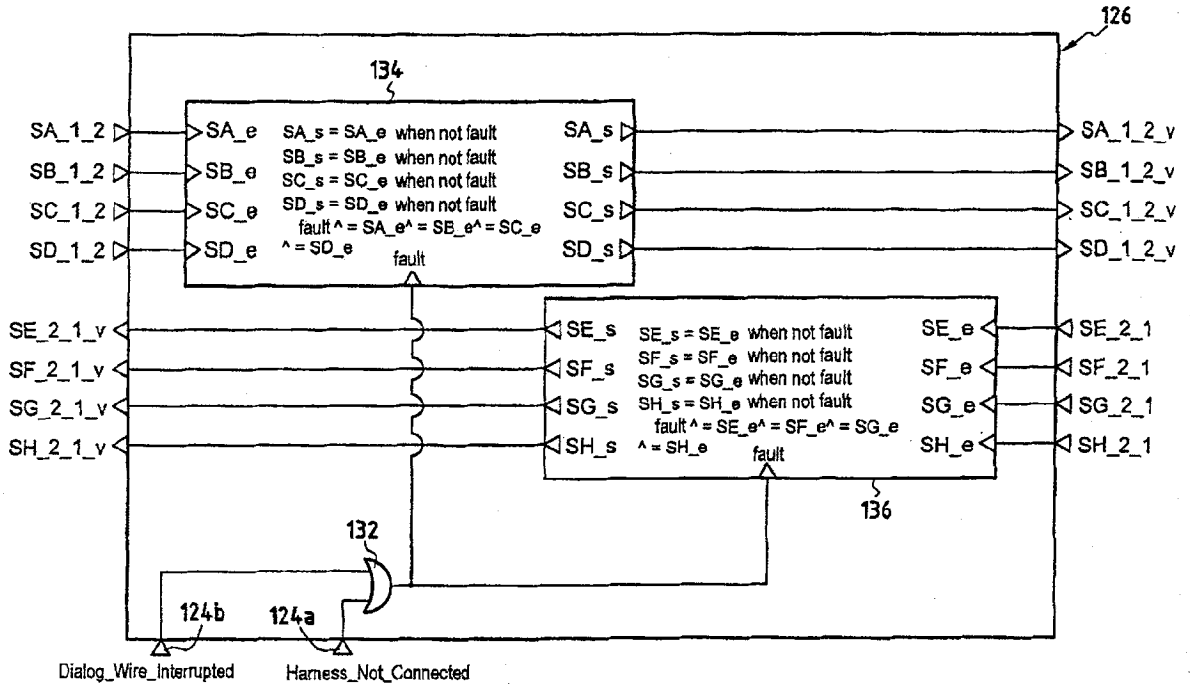

126
134
SA_1_2
SB_1_2
SC_1_2
SD_1_2
SA_e
SB_e
SC_e
SD_e
SA_s = SA_e when not fault
SB_s = SB_e when not fault
SC_s = SC_e when not fault
SD_s = SD_e when not fault
fault ^ = SA_e^ = SB_e^ = SC_e ^ = SD_e
fault
SA_s
SB_s
SC_s
SD_s
SA_1_2_v
SB_1_2_v
SC_1_2_v
SD_1_2_v
SE_2_1_v
SF_2_1_v
SG_2_1_v
SH_2_1_v
SE_s
SF_s
SG_s
SH_s
SE_s = SE_e when not fault
SF_s = SF_e when not fault
SG_s = SG_e when not fault
SH_s = SH_e when not fault
fault ^ = SE_e^ = SF_e^ = SG_e ^ = SH_e
fault
SE_e
SF_e
SG_e
SH_e
SE_2_1
SF_2_1
SG_2_1
SH_2_1
136
132
124b
124a
Dialog_Wire_Interrupted
Harness_Not_Connected

图 8