

复杂系统的 MBSE 建模及可靠性评估方法

李子航¹, 王国新¹, 马君达¹, 鲁金直^{2*}, 阎艳¹

(1. 北京理工大学机械与车辆学院, 北京 100081; 2. 洛桑联邦理工学院, 瑞士 洛桑 1015)

摘要:针对复杂系统设计过程缺乏早期可靠性评估的问题,提出一种基于模型的系统工程方法支持复杂系统的设计及可靠性评估。结合复杂系统的研发特点,提出一种基于“使命、运行、功能、逻辑、物理、可靠性”的基于模型的系统工程(model-based systems engineering, MBSE)建模方法,支持复杂系统设计和可靠性评估;利用基于“图、对象、属性、点、关系、角色”的系统建模语言 KARMA 对上述过程进行统一表达;通过 KARMA 的代码生成功能实现图模型到计算模型的映射,完成复杂系统可靠性的评估;将方法应用于液压系统案例,结果表明所提方法对于复杂系统设计和评估具备有效性。

关键词:贝叶斯网络;系统可靠性;故障树;MBSE;特定域建模;KARMA 语言

中图分类号:N945 **文献标志码:**A **文章编号:**1001-2486(2025)02-183-10



MBSE modeling and reliability evaluation method for complex system

LI Zihang¹, WANG Guoxin¹, MA Junda¹, LU Jinzhi^{2*}, YAN Yan¹

(1. School of Mechanical Engineering, Beijing Institute of Technology, Beijing 100081, China;

2. École Polytechnique Fédérale de Lausanne, Lausanne 1015, Switzerland)

Abstract: To solve the problem of lack of early reliability evaluation in complex system design process, a MBSE (model-based system engineering) method was proposed to support the design and reliability evaluation of complex systems. With the characteristics of complex system development, a MBSE modeling method based on MOFLP-R (mission, operation, function, logic, physics and reliability) was proposed to support design and reliability assessment of complex system. KARMA, a system modeling language based on GOPRR (graph, object, property, point, relationship and role), was used to express the MOFLP-R process. Then, in order to evaluate the reliability of the complex system, the code generation was used to map the diagram to the numerical model. Finally, the method was applied to a hydraulic system case and the results showed that the proposed method is effective for complex system design and evaluation.

Keywords: Bayesian networks; system reliability; fault tree; MBSE; domain-specific modeling; KARMA language

随着技术革命和产业革命的加深,现代各领域的产品系统与装备复杂程度不断升级,过去单一的“机械”系统正在向“机械、电气、通信”等多领域组成的复杂系统发展。复杂系统的开发具有研发周期长、成本高、跨领域等特点,这对系统的可靠性提出了更高的要求。

故障树分析法和贝叶斯网络是常用的系统可靠性分析方法^[1],这些方法主要应用于真实系统场景的可靠性评估。利用二者在复杂系统设计阶

段进行早期可靠性评估的难点在于,当前阶段的系统形式是文字,评估人员难以根据海量的设计文档整合系统结构,进而得出故障树或贝叶斯网络。此外,目前复杂系统设计和可靠性评估处于彼此割裂的状态,评估人员要么缺乏对复杂系统的理解,其设计的可靠性评估模型往往是根据专家经验而建,模型缺乏一致性,评估范围不准确,甚至偏离真实系统^[2];要么缺乏对复杂系统的早期可靠性评估,增加复杂系统实际构建时各方面

收稿日期:2022-11-21

基金项目:国家部委基金资助项目(50923010101;2019-JCJQ-ZD-133-01)

第一作者:李子航(1997—),男,河北石家庄人,硕士,E-mail:3120200350@bit.edu.cn

*通信作者:鲁金直(1988—),男,辽宁鞍山人,研究员,博士,E-mail:jinzhi.lu@epfl.ch

引用格式:李子航,王国新,马君达,等.复杂系统的 MBSE 建模及可靠性评估方法[J].国防科技大学学报,2025,47(2):183-192.

Citation:LI Z H, WANG G X, MA J D, et al. MBSE modeling and reliability evaluation method for complex system[J]. Journal of National University of Defense Technology, 2025, 47(2): 183-192.

的风险^[3]。

基于模型的系统工程 (model-based systems engineering, MBSE) 是解决复杂系统设计问题的一种关键手段^[4]。MBSE 是一种系统工程方法,通过建立系统模型,实现对复杂产品系统的描述,从概念设计阶段开始支持系统整个生命周期的需求、设计、分析、验证和确认活动。然而,目前 MBSE 的主流建模语言、建模方法和建模工具主要侧重于复杂系统的设计和方案验证,不支持在设计的同时对复杂系统的可靠性进行评估。

在基于 MBSE 的系统设计和可靠性评估的结合方面,国内学者展开了一定的研究工作。胡云鹏等^[5]将蒙特卡罗分析融入系统建模语言 (systems modeling language, SysML) 参数图中,将事件发生的逻辑关系映射成参数计算的逻辑关系并进行打靶仿真,得到可靠性的结果。这种方法占用大量运算资源,效率较低。种婧宜等^[6]提出基于 SysML 的卫星故障分析框架,利用追溯矩阵表达故障影响的功能范围,通过对活动图的行为仿真,识别故障处置方案的潜在问题,然而这项研究不涉及系统故障的定量分析。王宗仁等^[7]利用 SysML 定义系统需求和功能架构,根据上述输入利用 AltaRica 语言定义组件架构,自动生成系统故障树。这项研究的不足之外在于系统模型被分割到两个建模平台,模型数据异构,不利于设计人员进行操作和模型管理。

针对现有系统设计与可靠性评估过程中模型异构、部分方法计算速度慢的问题,为了提升系统早期设计阶段的开发和评估效率,本文提出了一种基于 MBSE 的复杂系统建模及可靠性评估方法,实现了对复杂系统的前期设计及可靠性评估。从使命、运行、功能、逻辑和物理方面出发,在建模工具 MetaGraph 内利用统一建模语言 KARMA 对系统模型和故障分析模型 (基于贝叶斯网络的故障树模型) 进行特定域建模,实现其 MBSE 的形式化表达,然后利用 KARMA^[8]语言的代码生成功能在建模工具上一体化地对模型可靠性进行早期定量评估。

1 基于 MOFLP-R 方法的复杂系统设计流程

如图 1 所示,针对运行场景复杂导致需求向功能转化困难以及可靠性要求较高的复杂系统,参考“需求、功能、逻辑、物理”(requirement, function, logic, physics, RFLP) 架构模型的流程,本文提出了一种 MBSE 建模方法——使命、运行、功能、逻辑、物理、可靠性 (mission, operation, function, logic, physics, reliability, MOFLP-R) 方法,将需求分析融入使命、运行、功能、逻辑和物理分析中,通过使命和运行分析充分分析问题空间和场景,在实际的系统分析过程中定义各类需求模型,指导系统工程师从事建模活动,并在早期对系统可靠性进行快速的定量评估。

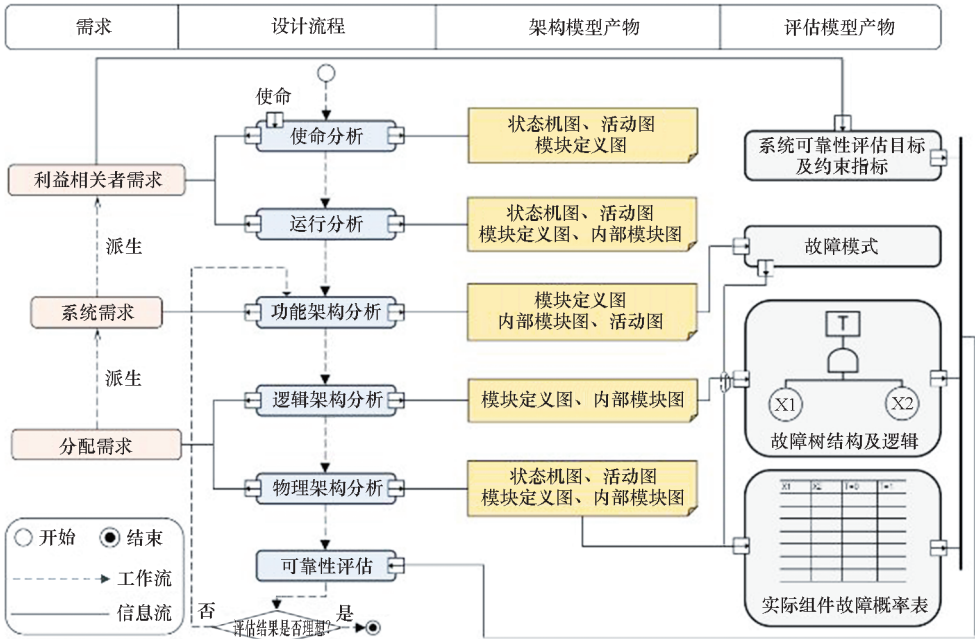


图 1 MOFLP-R 方法
Fig. 1 Methodology of MOFLP-R

由于所提方法涉及数学领域、故障分析领域和系统设计等多方面架构定义,传统的 MBSE 建模语言 SysML^[9]等无法满足多领域模型表达的需求。为避免系统架构模型和故障树模型的数据割裂并更好地表达 MOFLP-R 方法的流程,本文利用 KARMA 语言在 SysML 和故障树的基础上进行了融合和扩展,通过扩展定义新的元模型,构建了 MOFLP-R 方法的模型库,实现二者在同一建模工具的统一表达,维护架构模型与故障树模型的一真相源,提升可靠性评估的准确性。详细流程如下所述,扩展定义的部分术语解释见表 1。

表 1 MOFLP-R 方法术语解释
Tab.1 Term explanation of MOFLP-R

术语	含义
使命	需要实现的一系列目标的集合
目标	实现使命所期望达到的效果
效果	预期结果的描述
实体	实体可以参与目标的实现,或者它受到了目标的影响,涵盖利益相关者和实体
利益相关者	与使命有利害关系,但不参与使命实现的实体
能力	运行场景下可以实现的效果
任务	实体执行的活动
运行系统	运行场景下的系统
兴趣系统	运行系统的泛化
使命阶段	使命实现场景的一部分
运行阶段	从兴趣系统角度描述的使命阶段

1.1 使命分析

根据系统输入的使命,使命分析将定义系统的业务问题、表征问题空间、确定解决问题的潜在方案。主要包含以下活动:使命形式化,利用状态机图或活动图表征问题空间,获得使命阶段;确定不同使命阶段的实体、利益相关者以及运行系统,并利用模块定义图表达参与者的组织架构;利用活动图描述不同使命阶段中参与者所执行的任务,分析完成该阶段任务所需的能力。

这一阶段的需求分析首先通过对顶层使命的分析获得与使命方案各阶段相关的利益相关者、目标。然后,利用设计结构矩阵实现实体到目标的追溯。最后建立实体到实现使命所需能力的追溯。上述追溯的目的是确保运行系统、实体能够完整覆盖完成使命所需的能力。

1.2 运行分析

运行分析的目的是进一步分析外部实体(用户、外部系统等)将如何与兴趣系统(system of interest, SOI)交互,推动问题向功能的过渡,其中产生的用例场景将作为功能架构分析的输入,提高功能定义的精确性和完整性。主要包含以下活动:利用状态机图定义兴趣系统生命周期阶段,以此为系统分析的起点;定义兴趣系统执行使命的各个运行阶段,通过状态机图表达;按照泳道分配的方式,分析各个运行阶段中兴趣系统和外部实体所执行的任务;根据上一步活动图分析的实体之间的连接和流,利用内部模块图分析兴趣系统的运行环境组成,即兴趣系统和外部实体的关系。

这一阶段的需求管理活动要求加强同利益相关者的沟通、确认和验证,包括:追溯运行阶段到使命阶段及兴趣系统的生命周期阶段;从每个运行阶段中至少派生一个利益相关者需求;追溯利益相关者需求到使命分析过程所得到的能力。

1.3 功能架构分析

功能架构设计主要关注功能定义,这基于运行分析所得到的兴趣系统在各场景下的任务(运行分析的输出为功能架构的输入)。首先基于运行分析中的任务,识别其所对应的功能,利用模块定义图建立整体功能架构;定义功能流,利用活动图定义兴趣系统运行过程中的功能流;功能分类,通过建模环境的树状结构对功能架构进行分类,以便储存和提高可重用性;定义功能模态行为,利用状态机图定义功能的实现模式及其内部的转换行为和触发条件。

系统需求与功能架构处于同一层级,定义系统需求的目的就是把功能性视图转换为交付产品时所需的评价视图,包括:定义系统需求,并建立系统需求到功能、功能流的追溯;建立利益相关者需求到系统需求的追溯,验证功能层与运行层的兼容性。

1.4 逻辑与物理架构分析

逻辑架构定义了兴趣系统的组成。在架构层面,逻辑分析通过模块定义图描述兴趣系统的架构,实现功能和功能流到逻辑架构的映射。此外,对兴趣系统进行逻辑分解,定义系统执行时所需的子系统/逻辑项目。最后,利用内部模块图定义逻辑架构模块的工作方式以及交互,表达预期功能结果。逻辑架构相对于物理架构仍保持了一定的抽象层级,它定义了所需的子系统类型和逻辑项目,但仍然为具体的技术实现(例如软件/硬件)保留了一定的余地。

物理架构模型是对物理元素的管理,是兴趣系统的解决方案,是架构和技术选择以及设计准则选择的结果,旨在满足逻辑架构元素和系统需求。通过对物理架构模型的参数研究,实现物理架构的权衡和整体优化,经过验证后,成为详细设计的基础。

该阶段产生最后一种需求类型——分配需求,用于分配到一个或几个模块,以便形式化地解释相应模块考虑到的需求。针对所得逻辑和物理架构细化系统需求到分配需求,最终可以确定一个能够实现预期功能的物理方案。

1.5 可靠性评估

故障树分析方法是评估系统可靠性的常用方法之一,故障树模型^[10]包括顶事件(最不希望发生的事件)、中间事件、底事件(故障根本原因)和具有若干表达节点之间逻辑的“门”,通过建立这些组件的逻辑关系可以清晰地描述复杂系统的故障逻辑,但是传统故障树分析的算法只考虑系统“工作”或“失效”两种情况,对多态情况不友好^[11]。在图模型特征上,故障树与贝叶斯网络存在一定的相似之处。因此,本文方法基于故障树的规则建立贝叶斯网络模型,可实现复杂系统定量的可靠性分析。

使命分析和运行分析是把使命转化为兴趣系统的过程,其中所得到的与可靠性相关的利益相关者需求将转化为系统可靠性评估的目标,即顶事件。

逻辑和物理架构定义了系统、子系统和组件级的具体组成,设计人员可以根据评估目标与其他模块的组合、泛化和关联等关系,快速确认故障树的具体故障部件,同时也避免了因故障树与系统架构模型设计过程割裂,而出现模型不一致的情况。具体方法为根据评估目标在模块定义图中与其他模块间关系,分别根据逻辑层和物理层模块向下定义故障树的中间事件和底事件(例如,目标模块由三个逻辑模块以组合关系连接,那么中间节点即为这三个子模块),其间的逻辑门关系可以综合考虑内部模块图中的流关系、运行系统阶段定义。

在确定了故障树的结构组成后,需要确定组成结构的具体故障原因。由于功能架构分析获得的系统功能都分配到了兴趣系统的各个模块,根据各模块所具有的功能,定义故障树组成结构的故障模式。

最后,确认具体物理组件发生相应故障的概率并制定中间节点的条件概率表(表示底事件的

状态通过逻辑门对中间事件的影响),完成整个可靠性分析模型的构建,利用该模型可以进行可靠性评估。在完成可靠性评估后,若结果不理想,可通过迭代功能、逻辑、物理架构模型,进行新一轮的可靠性分析模型构建及评估。

2 基于模型驱动的复杂系统可靠性评估

形式化的架构模型本身不具备可靠性计算推理的能力,可靠性的评估往往需要编写其他脚本语言实现。由于计算语言脚本与所构建的系统架构属于不同领域模型,其数据储存格式不同,传统的方法往往是定制开发插件接口实现数据流动,这种方式不仅不够灵活,而且增加了研发周期和研发成本。

本节基于模型驱动思想实现上述基于贝叶斯网络的故障树模型到 Julia 语言的模型转换,从而满足复杂系统的贝叶斯网络计算需求,实现“系统模型”的统一表达。基于所采用的建模语言 KARMA 所具备的跨领域模型统一描述的特性,利用 KARMA 语言的代码生成功能^[12]的语法,通过提取所构建的模型属性信息,实现系统架构模型到计算实现模型的模型转换,打通数据流信息,进而直接对所建模型进行可靠性评估。

算法 1 展示了本节提出的利用 KARMA 语言代码生成功能,实现故障树图模型形式化文本向数值计算模型转换的方案:定义生成的数值计算文件;对同类对象、点元模型的参数属性进行遍历提取;将提取的参数属性填入映射语言的固定模板;写入至文件。

算法 1 利用 KARMA 语言执行模型转换方案
Alg. 1 Implementation of a model transformation scheme using the KARMA language

```
1. codeGenerator 代码生成器名
2.   generate 函数名
3.     fileName “生成文件路径” write //新建文件并
      开始文件写入
4.     for 1:n(某个或某类 Object)
5.       for 1:j(Object 的某个属性)
6.         //提取形式化代码属性并按固定模板向
          某语言转换
7.         print(“固定模板” + valueof( this ) );
8.       end for
9.     end for
10.    ... //重复上述 for 循环,完成全部类型的映射
11.    close//关闭文件
12.  end 函数名
13. end 代码生成器名
```

以所提出的模型转换技术方案为基础,基于模型驱动的复杂系统可靠性评估流程如图 2 所示,该流程涵盖了图模型、KARMA 语言和 Julia 语言的转换,是一个一体三面的流程。

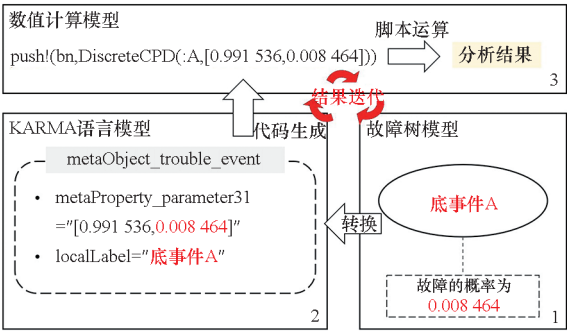


图2 基于模型驱动的复杂系统可靠性评估流程

Fig.2 Model-driven reliability evaluation process for complex systems

第1面为故障树模型。设计人员在建模工具MetaGraph中依据MOFLP-R建模方法建立系统模型及可靠性模型,例如图2中底事件A故障的概率为0.008 464。

第2面为KARMA语言模型。在MetaGraph中,设计人员所建立的故障树图模型由KARMA语言自动转化为形式化代码。图2的2号面,展示了底事件A的KARMA语言形式化代码,KARMA语言同样描述出了该对象的底事件为A,概率属性为“[0.991 536,0.008 464]”,事件故障代号为“A”;然后,根据KARMA语言代码生成的语法编写代码生成脚本,通过遍历相关对象元素,提取形式化代码属性,并添加相应的固定模板约束参数属性,使其成为Julia求解器的可执行脚本。图中实例代码片段旨在提取metaObject_trouble_event一类元模型对象(底层事件属于该类元模型对象)中的必要信息——故障代号和概率,并按照“push!(bn,DiscreteCPD(故障代号,概率))”的映射规则生成Julia语言,中间事件、顶层事件按照相同的方法利用代码生成向Julia语言映射。

第3面为数值计算模型。执行KARMA语言脚本的代码生成后,将输出Julia求解器可执行文件,从而支持贝叶斯网络计算。如图2顶面所示,“底事件A”图模型对象所映射生成的Julia代码为“push!(bn,DiscreteCPD(:A,[0.991 536,0.008 464]))”,括号内的内容“A”和“[0.991 536,0.008 464]”即为第一步中KARMA语言对此对象形式化的属性,其余为固定模板;最后,调用Julia工具运行该脚本,获得最后的可靠性分析

结果。

如果可靠性评估结果不理想,可以对系统模型进行修改,同时也要相应修改评估故障树。无须更改已经编写的KARMA语言代码生成脚本,直接执行故障树模型的代码生成,即可快速迭代计算新系统的可靠性,提升研发效率。

3 案例验证

舰船动力推进装置保障了舰船的行驶,其性能直接影响了舰船的行驶速度、灵活性和平稳性。目前,以螺旋桨为动力的舰船主要采用调距桨驱动^[13]。随着科学技术的进步以及性能要求的提高,调距桨系统已经从单一的物理系统发展成为机电液通信多学科融合的复杂系统,调距桨设计过程的复杂性也随之增长,传统的基于文本设计方法严重影响了调距桨系统的设计效率^[14]。此外,调距桨的液压系统是调距桨调距的核心,其结构组成复杂、运行环境恶劣,其可靠性在很大程度上决定了船舶运行的安全性^[15]。然而,舰船液压系统的可靠性评估主观性较强,依赖于后期的试验验证,这增大了设计成本^[16]。以设计能够改变舰船推力、方向,并抵抗恶劣环境的调距桨为使命,采用本文所提基于MBSE的复杂系统建模及可靠性评估方法对调距桨系统展开设计,以实例分析验证所提设计流程的有效性和可靠性。

3.1 液压系统使命分析

根据所提使命描述问题空间,使命的实施包含了驾驶员操作舰船、指令信号发送、桨叶调距和舰船行驶速度或方向改变四个使命阶段。如图3所示,在桨叶调距的使命阶段中,执行调距的关键运行系统为调距桨液压系统,另外还包括6个实体,其具体执行的任务为:①驾驶员,根据舰船运行情况,实时操作,向系统发送指令;②电控系统,发送信号并控制调距桨液压

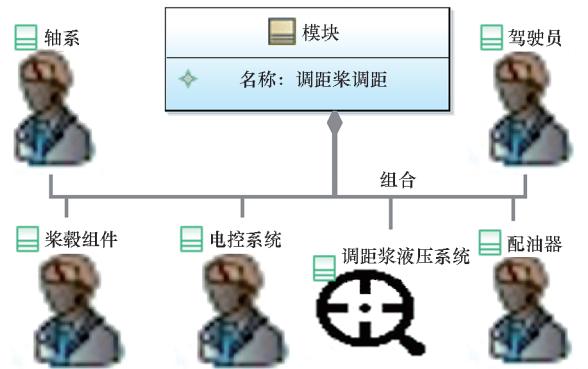


图3 使命分析

Fig.3 Mission analysis

系统调距;③调距浆液压系统开始调节油路;④配油器,分配液压系统产生的高低压油;⑤轴系将高低压油的液压力转换为驱动力;⑥桨毂组件螺距移动实现完成调距。

3.2 液压系统运行分析

根据运行系统和兴趣系统的定义,利用 SysML 的泛化关系继承使命分析中运行系统的全部特征,具象地获得设计所需的兴趣系统,即液压系统。液压系统的生命周期包括调距浆液压系统开发、生产、装配、拆除、在役、维护、退役以及调距浆整体维护八个阶段。为了完成使命,从兴趣系统在执行使命过程中运行的角度对运行的方案进行分析。如图 4 所示,一旦兴趣系统接收到调距指令,就会进入液压调节阶段。考虑到舰船行驶过程中的复杂状况,该阶段分为三种模式:大螺距调距,旨在快速改变行驶状态;小螺距调距,旨在精确改变行驶状态;故障调节,在液压系统丧失部分调距能力的情况下,仍保有冗余的调距能力。供油阶段同理,考虑正常和故障状态下的两种工作模式。对正常供油阶段进行分解,稳压供油后液压油经过调节产生相应的液压力传给外部实体。因此,为了完成改变舰船推力、方向的使命,需要关注调距浆液压系统的可靠性。

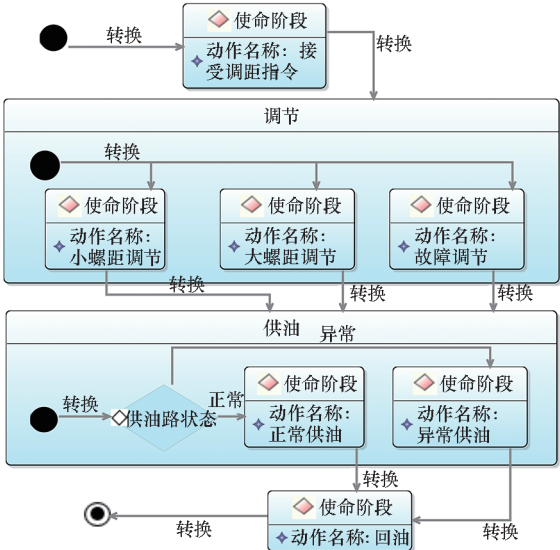


图 4 运行分析

Fig. 4 Operation analysis

3.3 液压系统功能架构分析

综合考虑运行方案中各个阶段执行的任务,识别任务对应的功能并将其分类,从而获得调距浆液压系统的整体静态功能架构。液压系统有稳压控油、接受电控系统指令、液压控制、回油 4 大

类功能,底层功能包括 12 种。分解静态功能架构,建立功能模态行为,其中液压控制的模态行为见图 5。在实际功能执行中,调距浆液压系统的功能还包括保证腔体内的压力一定、防止海水深入、为其他外部实体提供润滑油^[17],本次分析主要考虑调距过程的可靠性,因此图中没有考虑这些功能。

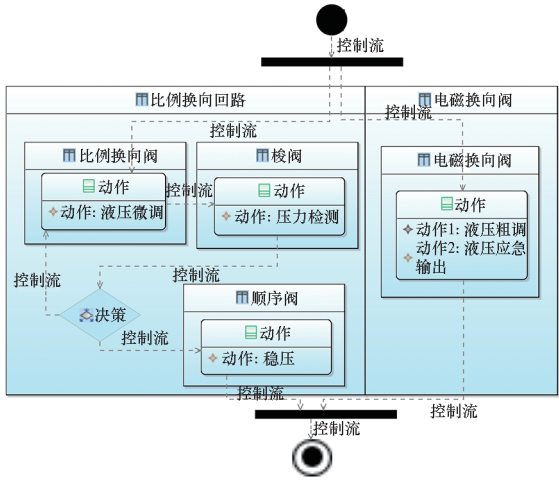


图 5 功能模态行为

Fig. 5 Function mode behavior

3.4 液压系统逻辑与物理架构分析

液压系统逻辑和物理架构如图 6 所示,逻辑架构用于承载功能,物理架构是逻辑架构的最终实现元素。根据运行、功能架构分析的结果综合考虑,液压系统应包括换向回路、供油路、回油路三个子系统,换向回路子系统包括大螺距调距组件和小螺距调距组件,供油路子系统包括主供油组件和备用供油组件,回油路子系统包括回油组件。在物理层,选取具体的对象将抽象的逻辑层组件具象化,如主供油组件由三联泵和压力滤器组成。

最后利用泳道等方式将功能模态行为分配给具体逻辑组件。以图 5 液压控制功能的分配为例,液压控制功能的行为被分配到比例换向阀回路和电磁换向阀。当比例换向阀回路和电磁换向阀回路同时工作时,系统处于液压粗调状态;当只有比例换向阀回路工作时,系统处于液压细调状态;当只有电磁换向阀回路工作,则表示系统进入了应急输出状态。

3.5 液压系统可靠性评估

在使命和运行分析过程中,执行船舶推进使命的关键系统为调距浆液压系统,本文将该系统作为可靠性评估的顶层事件。首先定义故障树的结构。图 5 和图 6 分别给出了调距浆液压系统的系统组件和结构组成之间的逻辑关系。从图 4 的

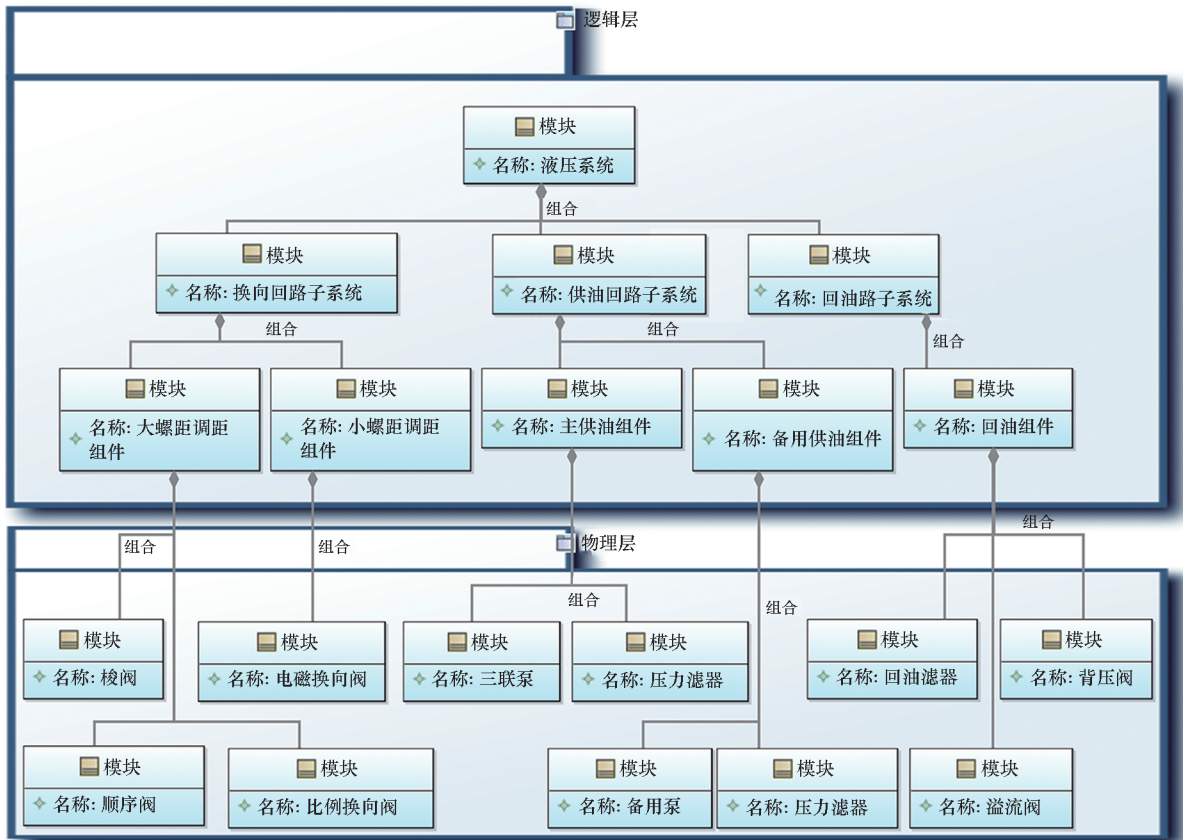


图 6 逻辑与物理架构分析
Fig. 6 Logical and physical analysis

运行方案上看,换向回路、供油回路和回油路子系统为串联关系,即或门。根据图 5,换向回路内部存在两个并联的小回路,两个小回路各自串联;供油路由于冗余的设计,两个供油子回路并联,子回路内部串联;回油路的稳压、安全保护动作同时触发后,回油滤油开始,三者属于串联关系。然后定义故障树的故障模式。根据整个系统的功能架构,换向回路子系统具有三个工作状态,因此系统可能的故障模式为换向回路的两个阀均正常、均失效或其一失效;溢流阀一旦发生泄漏,则将起不到安全保护的作用,因此按照泄漏程度分为正常、轻微泄漏和严重泄漏三种模式;滤器同理,分为正常、轻微堵塞和严重堵塞;其余组件均定义为两种故障状态,即正常和严重故障。所得故障树如图 7 所示。

最后,结合多态故障树条件分布规则和液压元件可靠性分析经验^[18],将相应的条件概率表填入对象属性中。取方玉茹等^[18]研究得到的推进元件模糊故障概率,并取隶属度为 1,赋予相关对象实际的故障概率,然后填入对象属性中。各根节点事件(黄色椭圆对象)的概率表见表 2。

利用 MetaGraph 的代码生成功能(技术路线参照第 2 节),完成图 7 模型信息到 Julia 语言的转化。在软件中直接调用所生成的 Julia 文件,根据所填先验概率,对所建 Julia 贝叶斯网络模型进行正向推理,推算各中间事件及顶层事件的故障概率,如图 8 所示。

其中,顶层事件——调距桨液压系统处于正常运行的概率为 95.194 29%,轻微故障的概率为 3.234 55%,严重故障的概率为 1.571 16%,结果与方玉茹等^[18]的故障树分析结果一致,验证了本文所提方法的有效性。其余部分中换向回路极易处于轻微故障状态,概率为 3.29%。因此,及时检查换向回路的状态,有助于提高整个液压系统的可靠性。如果系统的可靠性分析结果不满足利益相关者的需要,通过重新迭代系统模型,即可快速获得新一轮评估方案,提升设计效率。

此外,利用贝叶斯网络可以进行复杂网络的诊断推理,快速预测系统故障。本例分别假定液压系统在轻微故障和严重故障的情况下,诊断推理根节点物理组件的故障概率,如图 9 所示。

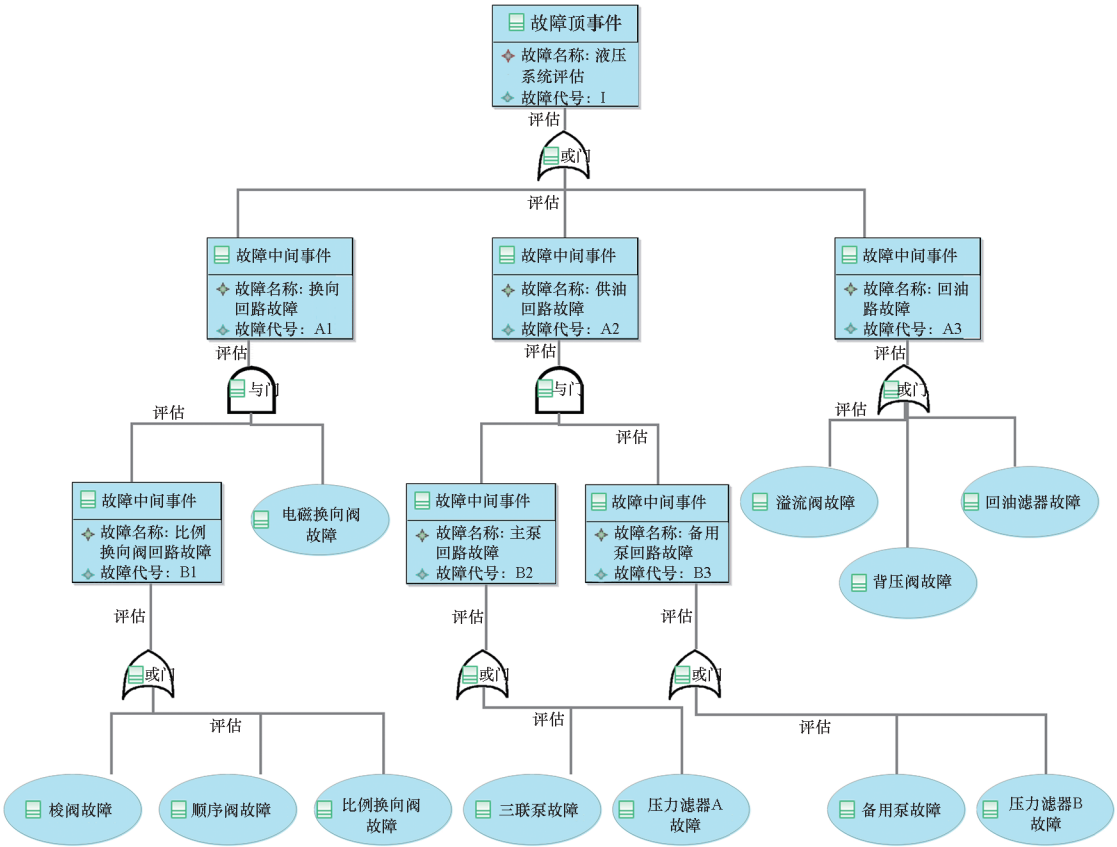


图 7 液压系统故障树

Fig.7 Fault tree of hydraulic system

表 2 底层事件先验概率

Tab.2 Basic event priori probability

底层事件名称	评估概率
梭阀故障	[0.997 931,0.002 069]
顺序阀故障	[0.995 411,0.004 589]
比例换向阀故障	[0.991 536,0.008 464]
电磁换向阀故障	[0.981 651,0.018 349]
三联泵故障	[0.992 509,0.007 491]
压力滤器 A 故障	[0.999 100,0.000 600,0.000 300]
备用泵故障	[0.986 591,0.013 409]
压力滤器 B 故障	[0.999 100,0.000 600,0.000 300]
溢流阀故障	[0.982 948,0.011 368,0.005 684]
背压阀故障	[0.997 862,0.002 138]
回油滤器故障	[0.999 100,0.000 600,0.00 0300]

可以看出,液压系统轻微故障状态下,整个比例换向阀回路(包括比例换向阀、顺序阀和梭阀)以及电磁换向阀的故障概率极高,但是由于整个换向回路的冗余机制,换向回路在轻微故障状态下故障的概率不高;液压系统严重故障状态下,回油路

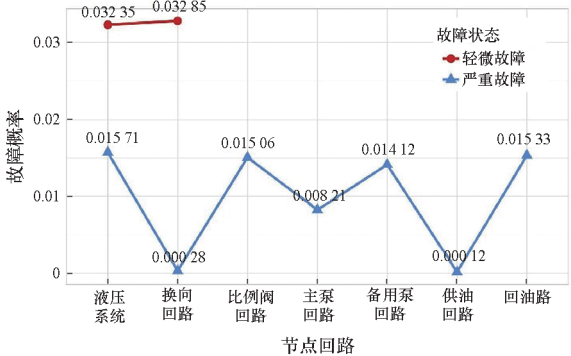


图 8 液压系统的可靠性评估结果

Fig.8 Reliability evaluation result of hydraulic system

故障概率达到了 97.543%,其中溢流阀发生轻微和严重故障的概率分别是 43.506%和 36.177%,是当前设计的薄弱环节,需要再进行更详细的优化。对于实际舰船运行过程,故障诊断有助于快速排查系统故障,恢复系统正常行驶,提升舰船的环境适应性和运行能力。相比王玉茹等^[18]的研究,运用本文所提 MOFLP-R 方法对调距桨液压系统开展基于模型的系统工程建模,加强了系统整体模型的管理,提高了系统设计模型的一致性和故障树模型的准确性,不仅有助于复杂系统的架构设计,而且在复杂系统的可靠性评估上更具优势。

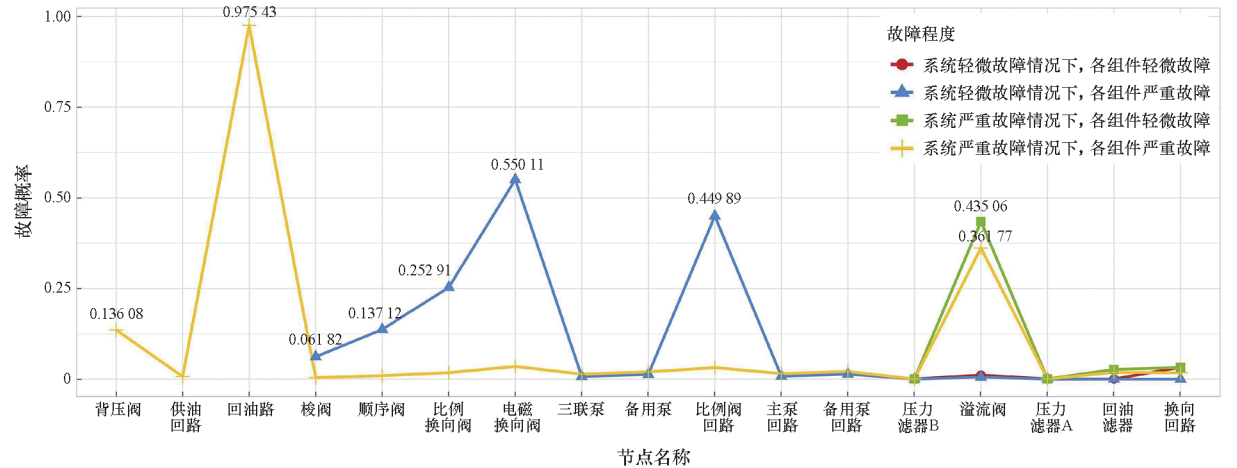


图 9 液压系统的故障诊断结果

Fig. 9 Fault diagnosis result of hydraulic system

4 讨论

相比传统的复杂系统设计过程,本文所提方法具备了以下几个方面的优势:

1) 细化复杂系统设计流程: 本文提出的 MOFLP-R 建模方法将 RFLP 模型架构进一步扩展定义为使命、运行、功能、逻辑、物理和可靠性,并给出了对应的图模型形式,为设计人员提供了详细的建模指导,提高了建模效率。

2) 支持复杂系统可靠性设计的模型库: 本文利用 KARMA 语言对 SysML 和故障树模型进行统一描述,并在这个基础上根据 MOFLP-R 建模方法的建模流程,构建了专用的元模型库,支持系统设计及可靠性评估。相对于其他的同类研究,本研究开发的模型库使设计人员在同一建模软件就可以完成建模和求解的闭环过程,有利于系统整体的管理。

3) 提升前期可靠性评估和模型迭代的效率: 本文所提方法借助 KARMA 语言,实现了图模型、文本式的模型描述代码、Julia 数值计算语言的模型转换。在前期设计阶段相对于蒙特卡罗仿真,基于贝叶斯网络的故障树的计算更快速,模型参数迭代效率更高。

5 结论

针对复杂系统设计流程模型异构、可靠性评估效率低的问题,本文研究了基于 MBSE 的复杂系统建模及可靠性评估方法,主要贡献包括:提出了基于 MBSE 的复杂系统可靠性建模方法,不仅支持复杂系统的设计,还支持复杂系统模型的可靠性评估;提出了基于模型驱动的复杂系统可靠

性评估方法,实现了基于贝叶斯网络的故障树、Julia 语言和 KARMA 语言的模型转换,进而实现一站式求解。

参考文献 (References)

[1] 姚成玉, 陈东宁, 王斌. 基于 T-S 故障树和贝叶斯网络的模糊可靠性评估方法[J]. 机械工程学报, 2014, 50(2): 193 - 201.
YAO C Y, CHEN D N, WANG B. Fuzzy reliability assessment method based on T-S fault tree and Bayesian network [J]. Journal of Mechanical Engineering, 2014, 50(2): 193 - 201. (in Chinese)

[2] 王思琪. 基于时序故障树的实时系统安全性验证方法研究[D]. 南京: 南京航空航天大学, 2016.
WANG S Q. Research on real-time systems safety verification based on temporal fault tree[D]. Nanjing: Nanjing University of Aeronautics and Astronautics, 2016. (in Chinese)

[3] LU J Z, WANG G X, TAO X, et al. A domain-specific modeling approach supporting tool-chain development with Bayesian network models [J]. Integrated Computer-Aided Engineering, 2020, 27(2): 153 - 171.

[4] LU J Z, WEN Y J, LIU Q, et al. MBSE applicability analysis in Chinese industry [J]. INCOSE International Symposium, 2018, 28(1): 1037 - 1051.

[5] 胡云鹏, 彭祺攀, 武新峰, 等. 面向 MBSE 的航天任务风险分析方法[J]. 网信军民融合, 2022(增刊 2): 23 - 29.
HU Y P, PENG Q B, WU X F, et al. MBSE oriented risk analysis method for space mission [J]. Civil-Military Integration on Cyberspace, 2022 (Suppl 2): 23 - 29. (in Chinese)

[6] 种婧宜, 周昊澄, 袁文强, 等. 基于 SysML 的通信卫星故障分析方法研究[J]. 计算机仿真, 2022, 39(3): 57 - 61, 390.
CHONG J Y, ZHOU H C, YUAN W Q, et al. Research on fault analysis method of communication satellite based on SysML[J]. Computer Simulation, 2022, 39(3): 57 - 61, 390. (in Chinese)

[7] 王宗仁, 周苏润, 王丕东, 等. 基于 MBSE 的卫星产品系统与可靠性集成设计技术研究[C]//第三届体系工程学

- 术会议, 2021: 385–394.
- WANG Z R, ZHOU S R, WANG P D, et al. Research on integration design technology of satellite system and reliability based on MBSE [C]//Proceedings of the 3rd System of Systems Engineering Academic Conference, 2021: 385–394. (in Chinese)
- [8] GUO J M, WANG G X, LU J Z, et al. General modeling language supporting model transformations of MBSE (part 2)[J]. INCOSE International Symposium, 2020, 30(1): 1460–1473.
- [9] HOLT J, PERRY S. SysML for systems engineering: a model-based approach[M]. 2nd ed. London: Institution of Engineering and Technology, 2013.
- [10] TAO X, LU J Z, CHEN D J, et al. Probabilistic inference of fault condition of cyber-physical systems under uncertainty[J]. IEEE Systems Journal, 2020, 14(3): 3256–3266.
- [11] 尹晓伟, 钱文学, 谢里阳. 系统可靠性的贝叶斯网络评估方法[J]. 航空学报, 2008, 29(6): 1482–1489.
- YIN X W, QIAN W X, XIE L Y. A method for system reliability assessment based on Bayesian networks[J]. Acta Aeronautica et Astronautica Sinica, 2008, 29(6): 1482–1489. (in Chinese)
- [12] GUO J M, WANG G X, LU J Z, et al. General modeling language supporting model transformations of MBSE (part 2)[J]. INCOSE International Symposium, 2020, 30(1): 1460–1473.
- [13] 高键, 李众. 基于单片机技术的调距桨螺距控制系统[J]. 华东船舶工业学院学报(自然科学版), 2002, 16(3): 59–63.
- GAO J, LI Z. Pitch control system of controllable pitch propeller based on single-chip microcomputer[J]. Journal of East China Shipbuilding Institute(Natural Science Edition), 2002, 16(3): 59–63. (in Chinese)
- [14] 郝彬彬, 鲁金直, 李军, 等. 基于特定域建模方法的航空发动机 MBSE 实施方法[J]. 科技导报, 2019, 37(7): 88–95.
- HAO B B, LU J Z, LI J, et al. Domain-specific modeling approach for model-based systems engineering in aero-engine development[J]. Science & Technology Review, 2019, 37(7): 88–95. (in Chinese)
- [15] 霍国义. 舰船调距桨推进装置的建模与仿真分析[J]. 舰船科学技术, 2017, 39(11A): 4–6.
- HUO G Y. Modeling and simulation of controllable pitch propeller for ship[J]. Ship Science and Technology, 2017, 39(11A): 4–6. (in Chinese)
- [16] 钟欣. 某新型舰船主推进装置监控系统 FMECA 在维修性分析中的应用[J]. 上海船舶运输科学研究所学报, 2013, 36(1): 37–43.
- ZHONG X. The FMECA in maintainability analysis of a new-type ship main propulsion control and monitoring system[J]. Journal of Shanghai Ship and Shipping Research Institute, 2013, 36(1): 37–43. (in Chinese)
- [17] 张劲枫, 易小冬. 某型船调距桨装置液压系统的设计与制造[J]. 机电设备, 2007(7): 14–17.
- ZHANG J F, YI X D. Design and manufacture on hydraulic system for controllable pitch propeller of some naval vessels[J]. Mechanical and Electrical Equipment, 2007(7): 14–17. (in Chinese)
- [18] 方玉茹, 阚树林, 杨猛, 等. 模糊多态贝叶斯网络在冗余液压系统可靠性分析中的应用[J]. 计算机集成制造系统, 2015, 21(7): 1856–1864.
- FANG Y R, KAN S L, YANG M, et al. Application of fuzzy multi-state Bayesian networks in redundant hydraulic system's reliability analysis[J]. Computer Integrated Manufacturing Systems, 2015, 21(7): 1856–1864. (in Chinese)