# 基于模型的可靠性、安全性分析方法

张金辉,赵滟*,毛寅轩,卢志昂,杨卓鹏,张龙喜

**中国航天系统科学与工程研究院系统工程研究所,北京 100037**

**摘要**　随着系统日趋复杂,呈现出功能高度复杂、故障动态重构、各领域耦合关联等特点,传统可靠性、安全性分析方法的局限愈加明显。依托于基于模型的系统工程(MBSE)方法的迅速发展,可靠性、安全性工程师提出了基于模型的安全性分析方法(MBSA)和基于模型的可靠性分析方法(MBRA)。从故障模型与系统模型如何进行集成、如何提高安全性分析结果可读性、如何设计恰当的安全性分析流程等3方面综述了MBSA研究进展;从如何提高分析工具的自动化程度及适用范围、加强建模语言对可靠性分析的适配能力、构建不同模型间的映射转换规则等3方面综述了MBRA研究进展。从如何设计一套针对安全性、可靠性分析的集成分析流程和如何解决可靠性模型、安全性模型和系统模型之间的接口问题等2方面介绍了基于模型的可靠性、安全性集成分析方法,阐述目前该领域所存在的问题和未来的发展方向。

**关键词**　基于模型的安全性分析方法;基于模型的可靠性分析方法;基于模型的可靠性、安全性集成分析方法;协同设计;基于模型的系统工程

21世纪以来,计算机技术迎来了高速发展阶段,工程系统呈现出复杂程度日益增加、容错机制复杂化及任务多样化等特点。复杂工程系统技术体系及其研制环境在计算机技术及信息技术的影响下发生了重大变革,数字化研制模式正逐渐取代传统以文档为主要载体的研制模式。2007年国际系统工程学会(International Society of Systems Engineering, INCOSE)提出了基于模型的系统工程(model based systems engineering, MBSE)概念,称MBSE将会是未来复杂系统工程方法与技术的发展趋势,是系统工程领域即将迎来的再一次重大变革[1]。

MBSE通过将系统工程技术方法与数字化信息技术结合,提出以统一模型化形式语言的方式表示复杂系统各组件之间的交互关系;以系统工程的思维构建系统结构模型,在系统全生命周期内支持概念设计、需求分析、功能分析、综合设计、验证和确认等系统工程活动[2-3]。目前MBSE已在国外航

收稿日期:2022-09-08;修回日期:2022-11-04

作者简介:张金辉,硕士研究生,研究方向为基于模型的系统工程,电子信箱:515340288@qq.com;赵滟(通信作者),研究员,研究方向为系统工程,电子信箱:pindyck@126.com

引用格式:张金辉, 赵滟, 毛寅轩, 等. 基于模型的可靠性、安全性分析方法[J]. 科技导报, 2024, 42(8): 101-110;
doi: 10.3981/j.issn.1000-7857.2022.09.01340

空、航天、船舶等领域进行广泛应用,比如美国国家航天局(NASA)、波音公司、欧洲航天局(ESA)等。

一个系统功能性能提高通常伴随着复杂性的增加,这也导致了可靠性、安全性的分析变得更困难。尤其是航空、航天和医疗等领域,可靠性、安全性的设计、分析、优化及验证工作已逐渐成为各级系统及设备研制的关键环节。传统可靠性、安全性分析主要基于文档,纸质文件表述具有天然的二义性和模糊性,分析人员互相交流困难且容易造成歧义;其次,对于越复杂的系统,依靠工程师自身水平高低来人工推理故障逻辑关系的方式就越不现实;同时,传统可靠性、安全性分析无法做到与功能性能的协同设计,十分影响分析结果的全面性和准确性[4]。

部分研究人员受到MBSE理论的启发,提出了基于模型的安全性分析方法和基于模型的可靠性分析方法,尝试借助MBSE方法解决本领域遇到的问题,并取得了不错的效果。在此基础上,有研究人员指出这2种分析工作通常由不同的工程师进行,存在重复性工作多、效率低等缺陷,提出基于模型的可靠性、安全性集成分析方法,以实现系统功能性能与安全性、可靠性一体化建模与评估。

## 1 基于模型的安全性分析

基于模型的安全性分析(mode based safety analysis, MBSA)最先由明尼苏达大学Joshi等[5]于2005年提出,他们认为可以通过故障模型与物理系统之间的相关模型扩展原有的系统模型,使系统工程师和安全工程师可以创建并使用相同的系统模型,从而在一定程度上降低成本并提高安全分析的质量,并提出了后续MBSA研究主要需要解决的问题:故障模型与系统模型如何进行集成、如何提高分析结果可读性和如何设计恰当的分析流程等。

### 1.1 故障模型与系统模型集成方法

#### 1.1.1 基于SysML语言将故障模型与系统模型进行集成

国际系统工程委员会和对象管理组织(Object Management Group,OMG)定义的系统建模语言标准——SysML语言[6],可以很好地描述和分析复杂系统,成为解决故障模型与系统模型进行集成的有效措施之一,但是如何将SysML语言和安全性分析过程进行结合成为难题,主要有以下2种措施。

1)借助SysML语言的扩展特点,将安全性信息融入系统模型中。如Helle等[7]2012年提出的Safety Analyzer方法和Mhenni等[8]2014年提出的SafeSysE方法等。2016年,Mhenni又对SafeSysE方法进行了优化[9],使其能够更好地从早期设计阶段就开始集成安全分析,避免了后期设计过多的更改工作,能够使建模及安全性分析过程更高效、更大程度地减少成本。

2)通过建立SysML模型到安全性专业模型的映射规则,使这2种不同领域模型之间可以自动转换,实现自动化安全性分析功能与系统模型的集成。如唐红英2020年通过建立SysML设计模型到AltaRica分析模型的映射规则,实现了这2种不同模型之间的自动转换,提出一种基于SysML及AltaRica的系统安全性分析工具,并进行了实例验证[10-11]。

#### 1.1.2 基于其他建模语言或工具对故障模型与系统模型进行集成

除了利用SysML语言外,研究人员基于其他建模语言或者工具也做了很多研究探索。

1)基于架构分析与设计语言(AADL)对现有的安全性分析方法进行扩展,从而更好地描述故障发生的条件、故障之间的交互影响及其应对措施[12]。

2)利用Simscape模型具有的回路和时序表达的特点对安全性分析进行扩展,通过分析故障的拓展方式、时序性仿真以及模式的形式化等建模重要因素来构建基于Simscape模型的航空发动机系统安全性分析方法[13]。

3)在系统正常功能模型中借助Simulink进行故障注入的方法扩展系统模型,规避传统安全性分析方法中模型不统一带来的系统设计结果和安全性分析结果之间很难进行追溯的问题[14]。

### 1.2 提高MBSA分析结果可读性

安全性分析结果的呈现方式有很多种,有些呈

现方式对于一般用户可读性很低,会影响分析效率。对于某个需要查看分析结果的用户,如果其呈现方式是一种陌生的工具,还需要花费时间去学习该工具,不仅会花费过多时间,还可能造成阅读上的偏差,最终造成安全性需求反馈发生错误。所以在MBSA研究过程中,提高分析结果可读性也是一个主要的研究方向。

AltaRica为安全性分析领域使用最广泛的建模语言,其分析结果对用户而言可读性比较高。很多研究人员尝试在MBSA过程中通过AltaRica模型生成最终结果以提高可读性,Bernard等[15]在2007年以飞行控制系统为例,使用MBSA方法对系统结构和潜在故障进行建模,然后基于AltaRica模型对系统进行了安全性分析,提高了分析结果的可读性。唐红英[11]于2020年设计并实现了AltaRica 3.0模型的扁平化、故障树的生成与分析、单步仿真以及故障动态演示等。

结果的表达方式也同样重要,使用用户比较熟悉的失效模式及后果分析(FMEA)和故障树分析(FTA)等方式,同样会在一定程度上提高分析结果的可读性。如徐文华等[16]在2017年对基于SysML语言的系统结构模型添加安全性信息进行扩展,在扩展模型的基础上利用SysML语言的路径追溯能力查找所有可能导致顶事件发生的子事件组合,由此实现故障树自动建模。贾淑丽等[17]2021年基于模型的RCM分析框架,使用基于模型的可靠性分析技术如AADL,先对设备系统进行系统的架构和故障建模,进而利用AADL的开源平台OSATE自动生成FMEA。

### 1.3　明确MBSA分析流程

在实际应用中会遇到很多流程问题:故障模型是由系统工程师创建并由安全工程师审查还是直接由安全工程师创建;谁将负责系统更新后的安全分析工作;哪些工作需要自动/手动进行。传统的安全性分析流程自动化程度低,无法解决以上问题,故需要根据MBSA特点重新定义分析流程。

目前各研究人员在MBSA上所采用的技术不尽相同,其流程也自然有很大的差别。美国兰利研究中心[5]通过在传统安全性分析"V"流程中加入系统模型构建、自动安全性分析以及系统设计变化后的自动更新等特定概念,对MBSA流程进行了修改(图1)。修改后的流程明确了哪些流程自动进行、哪些流程需要人工进行,可以在分析失效时,给安全工程师自动发送系统模型修改的通知,同时系统工程师可以运行安全分析来确定设计变更的影响。安全工程师的任务将主要为审查生成的安全工件并确认系统和故障模型中的假设,安全分析结果更准确更完整,同时减少了没必要的人工工作。

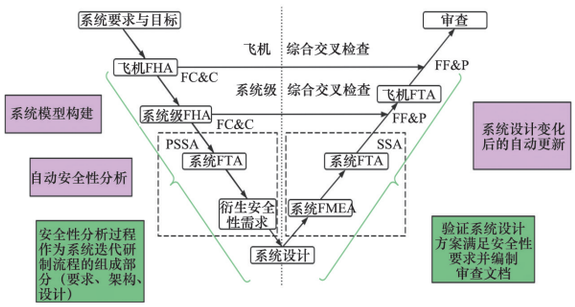


图1　修改后的MBSA流程

Morel[18]在2014年针对集成模块化航空电子设备早期安全性评估及验证困难的问题,提出从功能危险分析视图、功能视图、物理视图和分配视图等4个层次进行安全验证及评估流程,以便更好地支持集成系统灵活和快速原型设计,更易于评估和比较几种设想的架构及其合规性是否达到安全目标。

2020年,Krishnan基于MBSE方法将整个系统设计过程与安全生命周期进行集成,提出了综合系统设计和安全框架(ISDS)框架,该框架将MBSA流程分成了3个阶段:系统级分析、子系统级别分析和系统验证,并明确从系统SysML模型中自动生成FMEA和FTA等安全性分析结果[19]。

## 2　基于模型的可靠性分析

对于一些功能比较简单的系统,可以近似地认为每个组件故障之间是相互独立的,但是对于复杂系统,其组件之间大部分都存在时序相关性、依存性或者逻辑相关性,这时不能简单地用传统可靠性建模方法如FTA、RBD等进行建模[20]。基于MBSE

进行复杂系统的可靠性建模,才能更好地刻画其故障传播规律。

目前基于模型的可靠性分析(model based reliability analysis,MBRA)的相关方向包括:提高分析工具的自动化程度及适用范围、加强建模语言对可靠性分析的适配能力和构建不同模型间的映射转换规则。

### 2.1 提高分析工具的自动化程度及适用范围

#### 2.1.1 提高分析工具的自动化程度

传统安全性分析主要靠人工生成FMEA和FTA等结果,效率比较低,且准确度差,所以要实现分析结果的自动化生成,需要减少人工干预。David等[21]在2009年基于SysML模型的特点,通过结合可扩展标记语言(extensible markup language,XML)和功能失调行为数据库(dysfunctional behavior database,DBD)技术,实现了SysML模型自动生成FMEA。2019年,宛伟健[22]基于Profile的扩展方法确定SysML模块定义图的扩展方法,定义扩展后的SysML模块定义图元素到(动态)故障树节点的语义映射规则,实现了FTA分析结果的自动生成。

#### 2.1.2 提高分析工具的适用范围

复杂系统的失效模式不再只是针对单个组件,更多是涉及多组件或多层级的组合失效模式,但是传统FMEA分析只能识别单点失效模式的缺陷,适用范围受限。故部分研究人员对此进行了相关研究,如2009年Rudov-Clark等[23]通过对组件FMEA所涉及的各因素进行模型化抽象,建立了最低级别组件失效模式与最高级别系统功能失效模式之间的映射关系,根据这个映射关系进行仿真生成详细的FMEA表格,实现了对层级组合失效模式的识别。2015年,Sharvia等[24]提出危险源与传播分析(hazard origin and propagation studies, HIP-HOPS)方法,其针对传统FMEA分析只能识别单点失效模式的缺陷,引入了IF-FMEA表格替换FMEA表格,实现了对多点组合失效模式的识别。

### 2.2 加强建模语言对可靠性分析的适配能力

MBRA的模型构建是最主要的部分,构建模型可以通过很多种语言实现,重点是如何加强建模语言对可靠性分析的适配能力。目前该领域使用最多的建模语言有SysML语言、Modelica语言及AADL等,各自都有优缺点,基于这些语言如何更好适配可靠性分析工作,研究人员进行了相关研究探索。

2011年,Schallert等[25]提出一种基于Modelica语言进行可靠性分析的方法,首先评估系统模型,即组件和连接点的布置,将系统模型结构看作一个图,采用一种改进的深度优先搜索算法来寻找适当数量的候选最小径集。其次通过仿真检查候选最小径集,从大量候选中提取最小路径集。将分析工作分为深度优先搜索和仿真2个阶段,大大减少了总的计算工作量,并且可以自动确定系统的最小径集或最小割集、关键组件及其故障概率。

2013年,刘玮等[26]基于AADL语言模型设计了一种静态故障树自动生成算法,主要是利用AADL构建的物理架构模型和故障模型附件生成静态FTA结果,并由此进行相关可靠性分析工作。

2021年,Chabane等[27]提出一种基于SysML语言的故障模式分类方法,该方法主要包括3个工具:第一个工具是SysML语言,用于定义系统功能(功能分析);第二个工具是FMECA,便于表达可能的故障模式并揭示系统的不正常行为;第三个工具是K-Means算法,用来识别关键故障和对故障模式进行分类。K-Means算法主要有3个值参数——重要度、可检测性和频率,可以实现故障模式快速且系统的分类。该方法克服了传统基于SysML的可靠性分析方法不能进行故障模式分类的缺陷,更有利于从复杂系统设计阶段就开展可靠性分析,提高了SysML语言对可靠性分析的适配能力。

### 2.3 构建不同模型间的映射转换规则

SysML语言对于可靠性分析的支撑是不足的,通常需要结合其他模型语言进行分析。目前主要的思路是针对2种模型的"模型元素",提出一定的映射转换规则,从而实现2种不同模型间的转换。

2009年,David等[28]通过分析AltaRica Data-Flow和SysML 2种不同语言语义之间的联系,为两者建立映射规则,实现SysML模型在AltaRica Data-Flow中构建半自动模型。

2011年,董云卫等[29]描述了AADL可靠性模型

基本元素向GSPN模型元素的形式化转换规则,并以这些转换规则为基础,设计了可靠性分析与评估工具ARAM,完成了AADL可靠性模型向GSPN可靠性模型的自动转换,并最终实现嵌入式系统可靠性分析与评估。

2019年,邓刘梦等[30]提出一套从SysML模型到NuSMV模型转换的语义规则,设计了一个自动转换程序,通过该程序可将SysML模型文件转换成NuSMV输入文件,进而利用NuSMV实现SysML模型的可靠性验证工作。

## 3　基于模型的可靠性、安全性集成分析方法

MBSA和MBRA均是从功能故障模型出发进行构建,且都需要进行FTA和FMEA等故障分析工作,以往通常由不同的工程人员进行建模分析,重复性工作比较多,故需要研究如何将两者进行集成。在MBSA和MBRA集成过程中,需要解决的关键性问题有:如何设计一套针对安全性、可靠性分析的集成分析流程;如何解决可靠性模型、安全性模型和系统模型之间的接口问题。

### 3.1　合理的集成流程设计

目前国外研究机构对于集成方法的主要思路是:在系统需求分析阶段利用功能清单和使用要求等信息进行初步危险分析,提出初步安全性、可靠性需求;在系统功能分析、逻辑架构设计阶段构建故障模型;在系统物理架构设计完成后,对正常模型和故障模型进行仿真评估,对安全性、可靠性需求进行更新修改。国外比较有代表性的集成方法有3种:MeDISIS、RAMSAS和SafeSysE。

GJB9001中提出可靠性、维修性、保障性、测试性、安全性、环境适应性等六性是产品实现策划必须要考虑和满足要求的,是武器装备产品开发中除功能特性外要满足的质量特性。所以国内研究机构一般研究如何将六性技术进行集成,主要思路为:通过分析六性技术方法特点,构建一个统一的故障模型,基于该模型开展功能/性能与六性的协同设计,以此解决系统功能、性能设计与六性设计"两张皮"的问题。

#### 3.1.1　国外集成方法流程设计

MeDISIS由法国PRISME实验室于2012年提出[31]。如图2所示,MeDISIS主要分为3个阶段:第一阶段主要根据系统的需求定义使用初步危险分析(preliminary hazard analysis, PHA)确定功能失效状态;第二阶段结合功能失效状态结果进行FFMEA分析(功能失效模式及影响分析);第三阶段根据系统架构和组件行为描述开展组件FMEA、性能分析及故障注入等工作,对系统设计进行完善。每个阶段产生结果时,都应该对系统需求进行检查和更新。

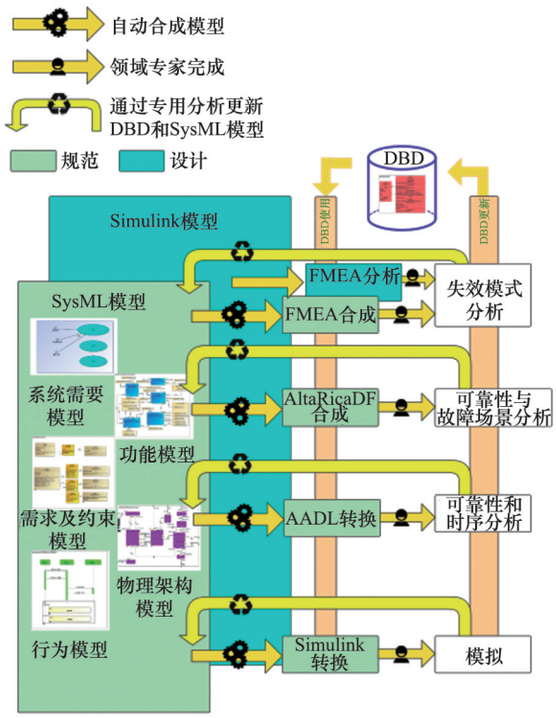


图2　MeDISIS方法框架

2012年,意大利DEIS学院团队也提出了RAMSAS集成分析方法[32],如图3所示,该方法主要由4个阶段组成:可靠性需求分析、系统建模、系统仿真和结果评估。和MeDISIS类似,RAMSAS的4个阶段也是迭代进行的。首先在可靠性需求分析阶段,主要工作为根据前期设计形成的系统设计模型、系统功能和非功能需求文档以及通过FMEA分

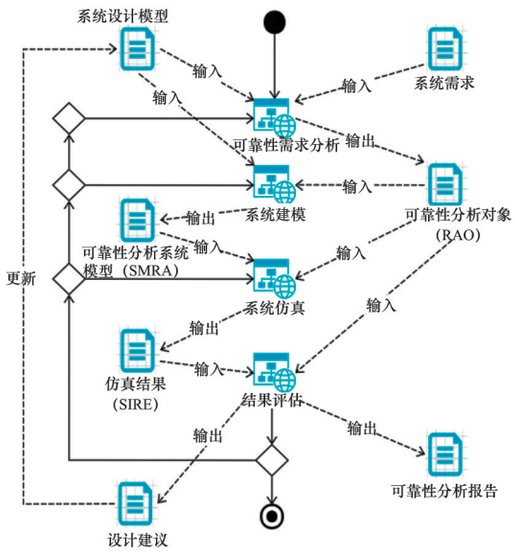


图3 RAMSAS集成方法流程

析得到的系统潜在故障来确定可靠性分析目标;在系统建模阶段主要工作是使用SysML语言对系统架构和行为建模,不同于以往的建模过程,此过程中需要同时建立故障行为模型;在系统仿真阶段,主要是把系统建模阶段得到的系统架构、系统行为和故障行为等3个模型转换成可供Simulink仿真的模型;结果评估阶段主要是根据系统可靠性需求对以上仿真结果进行分析,提出相关改进措施,并同步到可靠性需求分析阶段进行下一次分析迭代。

巴黎理工大学Mhenni团队在2016年提出如图4所示的SafeSysE集成分析方法[9],较于MeDISIS的模型映射规则,SafeSysE完全是在SysML模型上实

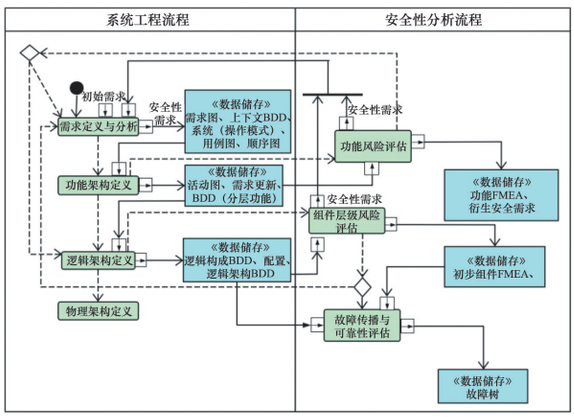


图4 SafeSysE集成方法流程

现的,主要基于SysML语言构建系统模型,然后通过元数据交换技术将SysML模型数据转化成XML文件,并由此开展组件FMEA和功能FMEA等分析工作。最后借助SysML的故障树生成算法和SysML模型与NuSMVSA模型的映射算法,对系统进行可靠性、安全性评估及行为仿真分析。

以上3种方法是目前为止相对成熟的集成方案,也经过了一些复杂工程系统的验证。SafeSysE虽然完全通过SysML模型实现安全性可靠性分析,无需进行不同模型之间的转换工作,但在直接生成故障树模型以及状态机验证系统模型等过程中,仍然需要大量人工的参与。RAMSAS主要注重于系统仿真阶段,对早期系统架构以及可靠性需求分析等过程不太重视,还算不上一套完全由模型驱动的方法。相比之下,MeDISIS的思路更完整。MeDISIS不但在不同阶段引入AADL、Altarica和Simulink等模型,同时引入DBD概念,使用户有机会在保留先前结果的同时更改建模语言或工具,实现故障数据可重复使用。MeDISIS主要是在建模阶段发现潜在故障来提高可靠性、安全性,无法贯穿整个系统寿命周期,故后续研究还需加强系统正常运行时的状态检测,通过传感器的实时数据变化,提前发现潜在的故障,才能在更大程度上提高系统的可靠性、安全性,增强系统的自主保障能力。

### 3.1.2 国内集成方法流程设计

2021年,北京航空航天大学可靠性研究团队以实现六性指标要求为目标,以故障的闭环消减和控制为核心,将六性工作项目合理地融入现有功能和性能为主线的研制过程,从而实现功能性能与六性工作的一体化协同,MBRSE综合设计流程的技术逻辑如图5[33]所示。同时,针对不同系统特点,该团队基于MBRSE,研发了机械产品可靠性综合仿真分析与设计优化平台、复杂集群系统RMS综合仿真与优化平台、可靠性数字孪生试验平台、电子产品可靠性综合仿真分析与设计优化平台,已推广到多家单位进行使用。

李娇等[34]认为目前可靠性、安全性和测试性等“三性”分析工作存在专业孤岛、系统性不足、重复性工作较多和“两张皮”等问题,于2021年提出一

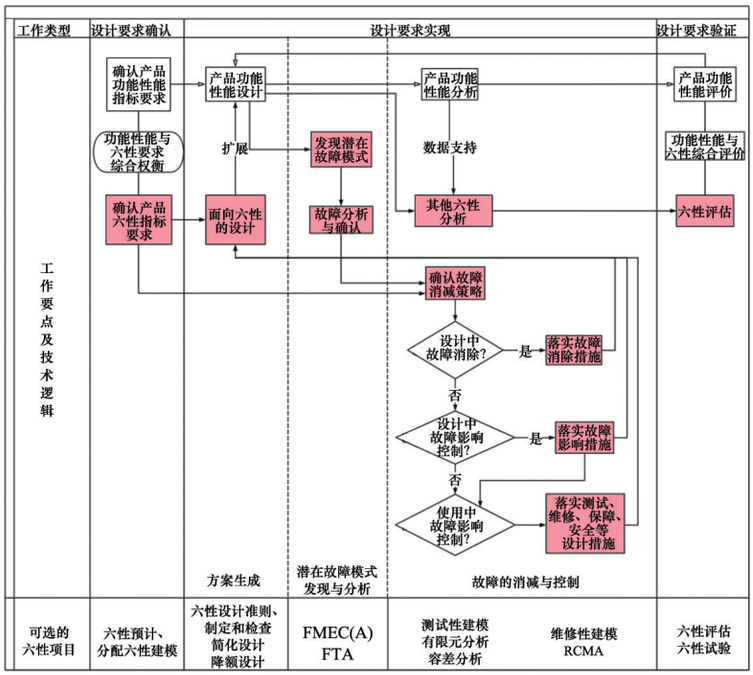


图5　MBRSE综合设计流程的技术逻辑

种基于MBSE的“三性”一体化建模评估方法。2015年,危虹等[35]结合Altarica故障建模方法,提出了一种在MBSE设计过程中能够实现基于模型的“四性”(可靠性、测试性、维修性、保障性)综合保障一体化设计的方法。但是这些研究给出的实例大多是一些较简单的系统,其方法对于复杂系统是否适用,还需今后进一步验证。

### 3.2　解决不同模型的接口问题

不同领域模型因为其建模语言及规则的不同,模型之间的接口问题成为难点。虽可通过映射规则及算法进行模型间的转换,但模型所表达的内容或多或少会发生变化,且模型的重复使用性也不高。故需要引入一种方法,可以使用同一套规则客观描述各模型不同概念的关系,实现领域知识的规范化及知识共享。

#### 3.2.1　实现各领域知识的规范化

各领域模型有各自的概念规则定义,通常很难进行集成。为解决以上问题,引入故障管理本体论方法,以统一的概念及关系规则对不同领域系统进行建模,彻底解决不同模型接口难的问题。

本体论(ontology)本是一个哲学概念[36],它研究存在本质的哲学问题,后被应用到计算机界[37],并在人工智能领域发挥越来越重要的作用。

Borgida等[38]于2007年提出了故障管理本体论(fault management ontology)概念,基于此,Ebrahimipour等[39]在2010年提出了FMEA本体模型。2016年,Castet阐述了故障模式、故障原因、故障传播理论以及冗余和故障控制区域等概念[40],并于2018年论述了系统工程师在模型中如何得到与故障相关的信息并自动生成FMECA和FTA结果[41]。2017年姚燕[42]通过FMECA本体模型构建故障相关知识体系,实现FMECA分析结果的格式化、规范化处理,为后续FMECA分析结果的软件工具化提供理论支持。结合上述研究成果,目前已有可以自动生成FMECA和FTA分析结果的MagicGrid插件。

#### 3.2.2　构建故障信息数据库

故障本体论仍是侧重理论层面的规则定义,只能实现知识的规范化,如要实现可靠性、安全性不同模型间数据共享与重用,还需创建一个存储故障信息的数据库。

David等[43]在2010年首次提出了DBD概念,解决了大批量故障信息存储的问题。2012年Cressent对DBD概念进行了优化[31],通过收集各种故障建模概念,使改进后的DBD模型涵盖不同粒度级别可靠性研究所需的全部相关数据,并允许连接到任何类型的可靠性分析工具或语言。

2010年,王志等[44]利用故障本体理论构建了矿井电机故障数据库模型,使矿井电机故障知识可以重用,但缺点是无法存储大批量故障数据和信息。2019年,吴康清等[45]基于故障本体建模技术,根据不同工作人员在机械零部件全生命周期内所需的故障知识建立了对应的故障数据库,极大地提高了故障数据的集成和使用效果。

## 4 结论

愈加复杂的系统催生了MBSE的提出,其在一定程度上解决了传统基于文档的系统工程方法的信息表达二义性、需求难以追溯、信息再利用能力差、领域设计之间存在鸿沟和软件测试工作量大等问题。同时,人工智能技术飞速发展,以数据为核心生产要素,构建数字化集成环境成为未来发展的一大趋势。构建面向系统全生命周期数字化集成MBSE模型迫在眉睫,这也对系统的可靠性、安全性提出了很高的要求。传统分析方法主观性太强,过于依靠工程师的水平,面对越复杂的系统,可靠性、安全性与功能性能的协同设计变得越来越困难。MBSA和MBRA虽然是解决以上问题的有效措施,但是两者单独建模分析存在太多的重复性工作,工作效率不高。基于模型的可靠性、安全性分析方法,将MBSA和MBRA进行了集成,更好地发挥了MBSE模型跨学科、可重复使用的优势。

目前基于模型的可靠性、安全性集成方法的研究还处于探索阶段,主要存在以下4方面问题。

1)分析流程不是很完备,没有相应的规范和标准。目前各研究机构提出的集成分析流程大多是侧重某些方面设计,其优缺点比较明显,同时没有相应的规范标准支撑,集成建模过程比较随意,应用举例也是选用比较简单的实例,在复杂实例应用过程中会出现很多问题。

2)缺乏故障信息数据库支撑。缺乏针对可靠性、安全性分析的数据库,无法实现建模信息的重用及共享,模型构建自动化程度也比较低,不符合数字化集成分析的要求。

3)无法实现系统全生命周期的可靠性、安全性分析。目前集成方法主要聚焦于系统的前期设计阶段,对于系统运行、维修保养等后期阶段基本没有涉及,还无法称得上是面向系统全生命周期的可靠性、安全性分析方法。

4)缺少集成分析的工具平台。目前该领域主要通过各工具平台之间的数据交换进行建模分析,没有专门面向集成分析的智能化工具平台。

针对上述问题,该领域主要有3个发展方向。

1)优化基于MBSE的可靠性、安全性分析流程,提升各分析工具的自动化程度,并根据可靠性、安全性数据特点建立数据库,实现数据的可重复使用及共享。并将分析过程形成相应的分析规范及标准,规范建模流程,确保模型构建的正确性和严谨性。

2)研究系统后期运行及维修保养阶段特点,将其集成到原有系统模型中实现系统全生命周期的可靠性、安全性分析,更好地提升系统组件的可靠性、安全性水平。

3)研究可靠性、安全性集成分析的智能化工具平台,扩展集成分析能力,提高建模和分析效率。

### 参考文献(References)

[1] Friedenthal S, Griego R, Sampson M. INCOSE model based systems engineering (MBSE) initiative[C]//INCOSE 2007 symposium. San Francisco, USA: INCOSE International Symposium, 2007: 18-25.

[2] 邓昱晨, 毛寅轩, 卢志昂, 等. 基于模型的系统工程的应用及发展[J]. 科技导报, 2019, 37(7): 49-54.

[3] 王文跃, 侯俊杰, 毛寅轩, 等. 面向复杂产品研制的MBSE体系架构及其发展趋势研究[J]. 控制与决策, 2022, 37(12): 3073-3082.

[4] 胡晓义, 王如平, 王鑫, 等. 基于模型的复杂系统安全性和可靠性分析技术发展综述[J]. 航空学报, 2020, 41(6): 147-158.

[5] Joshi A, Miller S P, Whalen M, et al. A proposal for model-based safety analysis[C]//Document Analysis Systems VI. Florence, Italy: IEEE, 2005.
[6] 蒋彩云, 王维平, 李群. SysML: 一种新的系统建模语言[J]. 系统仿真学报, 2006, 18(6): 1483-1487.
[7] Helle P. Automatic SysML-based safety analysis[C]//International Workshop on Model Based Architecting & Construction of Embedded Systems 2012. Innsbruck, Austria: ACM, 2012: 19-24.
[8] Mhenni F. Safety analysis integration in a systems engineering approach for mechatronic systems design[D]. Paris: Ecole Centrale Paris, 2014.
[9] Mhenni F, Choley J Y, Nguyen N, et al. Flight control system modeling with SysML to support validation, qualification and certification[J]. IFAC PapersOnLine, 2016, 49(3): 453-458.
[10] 唐红英, 胡军, 陈朔, 等. 面向SysML的系统安全性分析工具与实例研究[J]. 计算机科学, 2020, 47(5): 284-294.
[11] 唐红英. 面向SysML模型的系统安全性分析方法研究[D]. 南京: 南京航空航天大学, 2020.
[12] Stewart D, Whalen M W, Cofer D, et al. Architectural modeling and analysis for safety engineering[M]. Cham: Springer International Publishing, 2017: 97-111.
[13] 楚娜娜, 张曙光, 高艳蕾, 等. 基于Simscape模型的航空发动机系统安全性分析方法[J]. 航空动力学报, 2021, 36(4): 885-896.
[14] 柯宇航, 李艳军, 曹愈远, 等. 基于模型的飞控系统安全性分析研究[J]. 系统工程与电子技术, 2021, 43(11): 3259-3265.
[15] Bernard R, Aubert J J, Bieber P, et al. Experiments in model based safety analysis: Flight controls[J]. IFAC Proceedings Volumes, 2007, 40(6): 43-48.
[16] 徐文华, 张育平. 一种基于航电系统架构模型的故障树自动建模方法[J]. 计算机工程与科学, 2017, 39(12): 2269-2277.
[17] 贾淑丽. 一种基于模型的RCM分析方法[D]. 银川: 北方民族大学, 2021.
[18] Morel M. Model-based safety approach for early validation of integrated and modular avionics architectures[C]//International Symposium on Model-based Safety & Assessmemt. Munich, Germany: Springer, 2014: 57-69.
[19] Krishnan R, Bhada S V. An Integrated system design and safety framework for model-based safety analysis[J]. IEEE Access, 2020, 8: 146483-146497.
[20] 王如平, 周一舟, 王鑫. 基于MBSE的复杂工程系统可靠性设计分析关键技术研究[J]. 航空标准化与质量, 2021(5): 42-51.
[21] David P, Idasiak V, Kratz F. Improving reliability studies with SysML[C]//Reliability and Maintainability Symposium 2009. Fort worth, Texas, USA: IEEE, 2009.
[22] 宛伟健. 基于系统设计模型的动态故障树构建与分析方法研究[D]. 南京: 南京航空航天大学, 2019.
[23] Rudov-Clark S D, Stecki J. The language of FMEA: On the effective use and reuse of FMEA data[C]//AIAC-13 Thirteenth Australian International Aerospace Congress. Australia: Australia Defence Science and Technology Organisation, 2009: 9-12.
[24] Sharvia S, Papadopoulos Y. Integrating model checking with HiP-HOPS in model-based safety analysis[J]. Reliability Engineering & System Safety, 2015, 135: 64-80.
[25] Schallert C. Inclusion of reliability and safety analysis methods in modelica[C]//8th International Modelica Conference. Dresden, Germany: DLR, 2011.
[26] 刘玮, 李蜀瑜. 基于AADL模型的静态故障树的自动生成[J]. 计算机技术与发展, 2013, 23(10): 99-102.
[27] Chabane A, Adjerid S, Meddour I. Dependability analysis in systems engineering approach using the FMECA extracted from the SysML and failure modes classification by K-means[J]. International Journal of Dynamics and Control, 2021, 10(3): 981-998.
[28] David P, Idasiak V, Kratz F. Automating the synthesis of AltaRica Data-Flow models from SysML[C]//ESREL 2009. Taylor & Francis Group, 2009: 8.
[29] 董云卫, 王广仁, 张凡, 等. AADL模型可靠性分析评估工具[J]. 软件学报, 2011, 22(6): 1252-1266.
[30] 邓刘梦, 葛晓瑜, 宛伟健. 基于NuSMV的SysML模型形式化验证[J]. 计算机技术与发展, 2019, 29(10): 153-156.
[31] Cressent R, David P, Idasiak V, et al. Designing the database for a reliability aware Model-Based System Engineering process[J]. Reliability Engineering & System Safety, 2013, 111: 171-182.
[32] Garro A, Tundis A. A model-based method for system reliability analysis[C]//Simulation Series-Part of the 2012 Symposium on Theory of Modeling and Simulation -DEVS Integrative M&S Symposium. Orlando, FL, USA: Wiley, 2012: 1-8.
[33] 孙博, 任羿, 王自力, 等. 基于模型的可靠性系统工程[M]. 北京: 国防工业出版社, 2021.
[34] 李娇, 隆金波, 彭文胜, 等. MBSE模式下可靠性安全性测试性一体化建模与评估技术方法[J]. 计算机测量与

控制, 2021, 29(7): 247-253.
[35] 危虹, 傅耘. 基于模型"四性"综保系统工程设计[J]. 装备环境工程, 2015, 12(6): 53-59.
[36] Field H. Logic and ontology[M]. London: Science without Numbers, 2016.
[37] Gruber T R. Toward principles for the design of ontologies used for knowledge sharing[J]. International Journal of Human-computer studies, 1995, 43(5/6): 907-928.
[38] Borgida A, Brachman R J. Conceptual modeling with description logics[C]//The Description Logic Handbook: Theory, Implementation, and Applications. London: DBLP, 2003.
[39] Ebrahimipour V, Rezaie K, Shokravi S. An ontology approach to support FMEA studies[J]. Expert Systems with Applications, 2010, 37(1): 671-677.
[40] Castet J F, Bareh M, Nunes J, et al. Fault management ontology and modeling patterns[C]//AIAA SPACE 2016. Long Beach, California: 2016: 5544.
[41] Castet J, Bareh M, Nunes J, et al. Failure analysis and products in a model-based environment[C]//2018 IEEE Aerospace Conference. Yellowstone Conference Center, Piscataway, NJ: IEEE, 2018.
[42] 姚燕. 基于FMECA和本体技术的管制内话系统运行风险分析[D]. 天津: 中国民航大学, 2017.
[43] David P, Idasiak V, Kratz F. Reliability study of complex physical systems using SysML[J]. Reliability Engineering & System Safety, 2010, 95(4): 431-450.
[44] 王志, 夏士雄, 牛强, 等. 基于本体的矿井电机故障知识库构建[J]. 计算机工程, 2010, 36(10): 270-272.
[45] 吴康清, 黄利平, 李伯舒, 等. 基于故障知识库的机械零部件故障管理支持系统[J]. 图学学报, 2019, 40(3): 623-630.

## A survey of model-based reliability and safety analysis methods

ZHANG Jinhui, ZHAO Yan*, MAO Yinxuan, LU Zhiang, YANG Zhuopeng, ZHANG Longxi

China Aerospace Academy of Systems Science and Engineering Institute of Systems Engineering, Beijing 100037, China

**Abstract** With the increasing complexity of the system, showing the characteristics of highly complex functions, dynamic fault reconstruction and coupling correlation in various fields, the limitations of traditional reliability and security analysis methods are becoming more and more obvious. Relying on the rapid development of model-based systems engineering method (MBSE), reliability and security engineers put forward model-based security analysis method (MBSA) and model-based reliability analysis method (MBRA). This paper summarizes the research progress of MBSA from three aspects: how to integrate fault model and system model, how to improve the readability of safety analysis results and how to design appropriate safety analysis flow. This paper summarizes the research progress of MBRA from three aspects: how to improve the automation and scope of analysis tools, how to strengthen the adaptability of modeling language to reliability analysis, and how to construct mapping transformation rules between different models. Then the integrated analysis method of reliability and security based on model is introduced from two aspects: how to design a set of integrated analysis flow for security and reliability analysis and how to solve the interface problems among reliability model, security model and system model. Finally, the existing problems and future development direction in this field are described.

**Keywords** model-based security analysis method; model-based reliability analysis method; model-based reliability and security integrated analysis method; collaborative design; model-based systems engineering

（责任编辑　傅雪）