文章编号:1671-4598(2021)07-0247-07 DOI:10.16526/j.cnki.11—4762/tp.2021.07.048 中图分类号:V211.3 文献标识码:A

# 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

李 娇,隆金波,彭文胜,敖 亮
(中国航空综合技术研究所 装备服务产品部,北京 100020)

**摘要**:随着智能保障、PHM 等技术不断深入应用,可靠性、安全性、测试性(以下简称“三性")的重要性日益凸显,工程中迫切需要解决“三性" 重复工作、专业孤岛以及“两张皮" 现象;从系统工程出发,首先分析了“三性”主线工作内容,均紧紧围绕功能故障逻辑关系开展,统一建模,实现模型复用;其次,在功能模型基础上映射出故障逻辑关系,更接近故障传递的真实情况,解决“两张皮”现象;然后,全面分析“三性”建模要素和评估内容,对专用部分的信息进行处理,使得“三性”工作不再是孤岛;最后,以燃油系统为例展开了建模评估,基于功能故障逻辑模型,分别进行了可靠性、安全性、测试性建模与评估,实现了模型复用,减少重复工作;专业协同工作,提高了工作效率;紧密结合功能,有效解决“两张皮”现象。

**关键词**:可靠性;安全性;测试性;建模评估;MBSE

# Integration of Modeling and Evaluation Techniques of Reliability, Safety, Testability in MBSE Mode

LI Jiao, LONG Jinbo, PENG Wensheng, AO Liang
(Equipment Service Department, China Aero-Polytechnology Establishment, Beijing 100020, China)

**Abstract**: With the in-depth application of intelligent support, PHM and other technologies, the importance of reliability, safety and testability (hereinafter referred to as “three characteristics") is becoming increasingly prominent. It is urgent to solve the “three characteristics" of repetitive work, professional island and “two skin" phenomenon in engineering. From the perspective of system engineering, this paper first analyzes the main work contents of “three characteristics", which are all carried out closely around the logical relationship of function failure, unified modeling and model reuse. Secondly, based on the function model, the logical relationship of fault is projected, which is closer to the real situation of fault transmission and solves the “two skin" phenomenon. Then, the modeling elements and evaluation contents of the “three properties" are comprehensively analyzed, and the information of the special part is processed, so that the “three properties" work is no longer an island. Finally, the fuel system is taken as an example to carry out the modeling and evaluation. Based on the functional fault logic model, the reliability, safety and testability of the fuel system are modeled and evaluated respectively to achieve model reuse and reduce duplication of work; Professional collaboration improves work efficiency; Close combination of functions, solve the “two skin" phenomenon.

**Keywords**: reliability; safety; testability; modeling and assessment; MBSE

## 0 引言

随着科技的不断进步,智能保障、PHM 等技术成熟度较低、复杂程度高的新技术逐渐融入到航空装备系统中,这就造成了装备综合保障的过程将会变的更加复杂,安全性问题频发的燃油系统、起落架系统等也采取了复杂的保护机制,这使得“三性”工作的重要性也日益凸显。

从工程实际出发,“三性”工作中存在以下几个方面问题:首先,专业间的重复工作,工作效率低;其次,纸质资料,交流困难且容易造成歧义,工作准确率低;然后,没有从系统工程出发,不清楚成品实现整机功能的意义,各约定层次对初始约定层次影响关系不明确,做了上百页毫无意义的硬件 FMEA 分析;最后,也是最重要的一点,外场发生的部分故障是传统 FMEA 分析不出来的,工作效果差,一方面是原因分析不全面,另一方面与 FMEA 自身技术缺陷有着直接关系[1]。因此工程中迫切需要实现“三性”一体化建模和评估,快速、便捷地开展相关工作,有效解决传统 FMEA 中的技术缺陷,并且应与 MBSE 新模式接轨,满足时代需求[2]。

文献[3]以人工演绎推理为主的传统安全性、可靠性分析手段已经越来越不能满足要求,模型驱动的分析方法

**收稿日期**:2021-05-20; **修回日期**:2021-06-18。
**基金项目**:国家自然科学基金项目(71801198)。
**作者简介**:李 娇(1988-),女,河北石家庄人,工程师,硕士,主要从事军民机可靠性、安全性设计分析等方向的研究。
**引用格式**: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.

正在成为复杂系统安全性、可靠性设计所依赖的重要技术手段。

文献［4］等指出 MBSE 的落地应用，必然对科研生产模式产生冲击和影响，若产品研制全面转向 MBSE 模式，将在设计流程、设计验证工作量等方面出现众多难以预先克服或避免的问题。因此，应在体系化推进 MBSE 流程、方法和工具体系建设基础上，采取试点应用，由点及面的推广应用模式。

文献［5］等指出从传统的设计模式到目前的基于模型的系统工程的设计模式，都存在分析源头不统一的问题，这也影响了质量可靠性分析的效率、可信性和准确性。并提出了通过大量的结构、性能和行为特性模型的支撑，保证了在基于模型的系统工程的全寿命周期设计过程中，产品设计活动和数据的统一。

以上方法都指出了传统设计模型存在一定问题，均需要开展 MBSE 的相关研究，然而，胡晓义等人仅仅开展了基于 MBSE 的可靠性、安全性方法综述，忽略了测试性也可以一体化建模评估，且缺乏对“三性”一体化评估的具体方法研究和工程实践，本文从“三性”评估主线、评估内容和建模语言等方法进行调研分析，形成 MBSE 模式下的“三性”一体化建模与评估方法，并进行工程应用。

## 1 “三性”建模评估技术要点

### 1.1 “三性”评估主线

从工程实际情况出发，可靠性分析与评估的主线[6]是“功能架构－故障逻辑－故障判据”；安全性分析与评估的主线[7]是“功能架构－FHA－故障逻辑”；测试性分析与评估的主线[8]是“功能架构－故障逻辑－测试方案”。“三性”工作紧紧围绕“功能架构－故障逻辑”开展，“三性”工作是由各专业小组开展工作，三者均需要重复进行 FMEA 和 FHA 等故障逻辑分析，因此，功能故障逻辑模型是“三性”一体化的模型基础。

### 1.2 “三性”评估内容

目前国内对“三性”工作主要依据标准（如 GJB 450A－2004 装备可靠性工作通用要求、GJB 900－2012 装备安全性工作通用要求、GJB2547A－2012 测试性工作通用要求，以及 SAE－ARP－4761 民用机载系统和设备安全性评估过程的指南和方法）规定的定量、定性要求以及工作项目开展“三性”的设计分析与评估工作。可靠性工作项目主要包括：FMEA、建立可靠性模型，以及预计分配等，安全性工作项目主要包括：FTA、FHA 等，测试性工作项目主要包括：FMEA、建立测试性模型，以及定量定性分析等工作。

### 1.3 “三性”建模语言工具

安全性、可靠性等工作目标是检测导致系统从正常状态转变到失效状态的事件，并对事件进行量化分析，可分层次、分模块描述产品的功能/物理结构模型和故障信息等内容。

AltaRica 语言[9]是一种面向元模型的建模方法，最初由法国波尔多大学计算科学实验室（LaBRI）设计用来进行故障行为建模：首先通过定义系统的状态变量和触发事件，进而描述系统的状态转移；其次利用模型的重用性构建通过定义系统的输入和输出端口以建立系统的物理组成和功能关系，非常适合用来描述复杂系统的“三性”故障逻辑并进行分析计算。

通过将系统的功能或物理结构封装到分层级的“黑盒”里，“黑盒”间的输入输出端口通过“线”连接，这些“线”代表封装变量之间的约束条件。“黑盒”的所有状态可通过任务剖面构建故障判据来描述，故障模式可通过功能输出端口失效状态定义来描述。那么，引起输出端口的失效状态是由于输入端口失效状态和“黑盒”自身失效状态的某种逻辑关系引起的，即故障逻辑关系的分析过程[10]。

## 2 MBSE 模式下“三性”一体化评估方法研究

### 2.1 基于 MBSE 的“三性”一体化建模评估思路分析

经过“三性”评估的主线分析，确定功能故障逻辑是实现“三性”一体化建模的模型基础，基于功能故障逻辑模型可实现“三性”需求、功能、逻辑、物理、仿真等协同工作。

AltaRica 语言通过定义系统的输入和输出端口以建立系统的物理组成和功能关系，可实现功能和物理结构的有机融合，此外，该语言，定义系统的状态变量和触发事件，进而描述系统的状态转移，实现动态分析。

基于功能故障逻辑模型，通过收集专用部分信息，如信号与测试信息、任务失效判据、功能故障等内容，可实现建立完整的“三性”模型并进行评估。

经过以上分析，形成的建模评估工作总体思路如下：

1）数据准备。收集功能信息、结构信息以及信号与测试信息相关的数据。

2）建立共用模型，即功能故障逻辑模型。分析本层所有功能模块，并建立上层功能与实现本层功能的物理端口映射关系，完成本层次功能建模。然后，通过对模块端口和功能进行失效状态定义，在功能模型的基础上开展故障逻辑关系分析，同样方法分析下一层次直至最底层。

3）建立“三性”模型。基于顶层功能故障分析和功能匹配[11]，在功能故障逻辑模型基础上可进行安全性分析；在功能故障逻辑模型的基础上，分析任务剖面及任务失效判据可进行任务可靠性分析；在功能故障逻辑模型的基础上扩充信号和测试相关信息即可开展测试性建模与分析。

4）进行“三性”评估。具体评估内容详见图 1。

### 2.2 安全性一体化建模评估技术

安全性分析是在功能故障分析与功能匹配的基础上，结合功能故障逻辑模型，通过对故障逻辑树的底事件发生概率，按照一定的算法计算，推算出某个功能故障发生的概率，同时支持分析模块状态失效时的影响范围[12]。

安全性评估内容主要包括：FHA、PSSA、SSA、CCA 等。

安全性一体化建模评估过程见图 2。

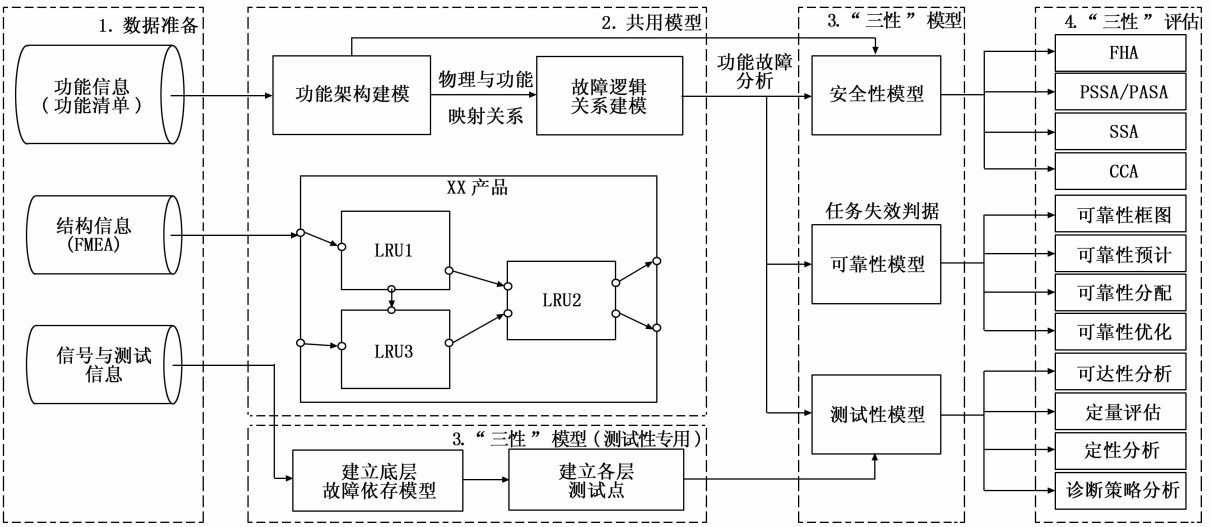


图 1　“三性”一体化建模评估总体过程

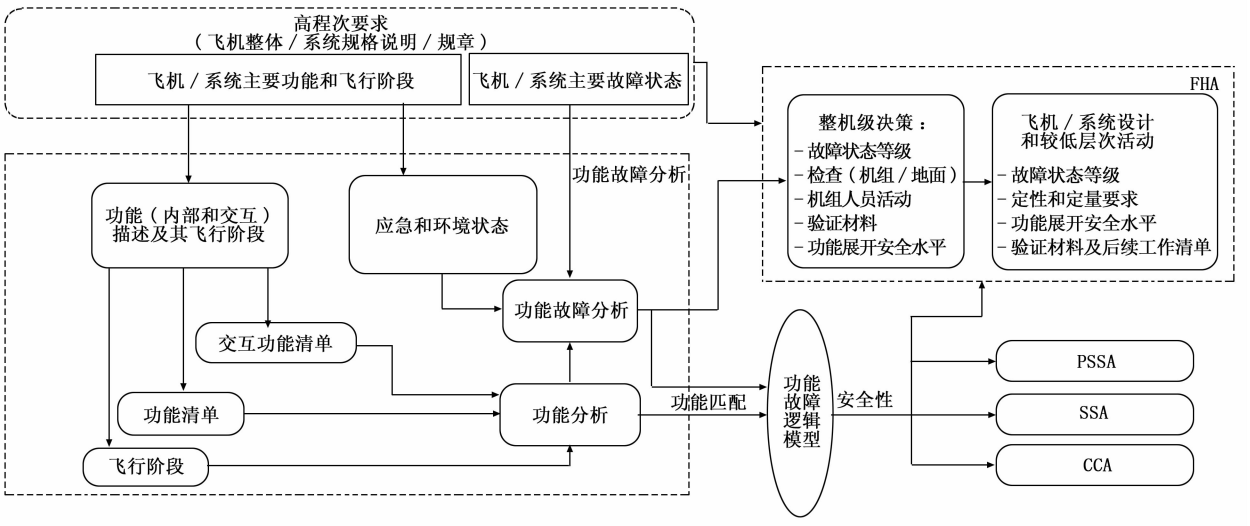


图 2　安全一体化建模评估过程

在对飞机、系统主要功能和飞行阶段进行描述形成功能分析，然后对飞机、系统主要故障状态及相关要求分析形成功能故障分析，在功能匹配、任务剖面设定基础上开展相关工作，在 FHA 基础上形成几种单一故障或故障组合为顶事件进行 FTA 分析，形成 PSSA 和 SSA。

通过评价总体系统结构对于共因事件的敏感性，CCA 将对相应系统结构及其相关分系统的研制进行协助。对共因事件的评价可以以下方式进行：特殊风险分析、区域安全性分析和共模分析。在各个系统的 PSSA 和 SSA 中将要用到整机级别的共因分析的结论。

### 2.3　可靠性一体化建模评估技术

在功能故障逻辑模型的基础上，创建可靠性框图，通过可靠性分配确定各层级的可靠性要求，可靠性预计是对可靠性指标符合性的验证，并进行可靠性优化。针对任务可靠性，需要针对具体任务建立任务失效判据，并对每项失效判据进行功能故障分析，结合功能故障逻辑模型，进而建立任务失效逻辑。

可靠性建模与评估主要包括：可靠性框图、可靠性预计、可靠性分配和可靠性优化等。

可靠性一体化建模评估过程见图 3。

可靠性评估整体来说主要包括基本可靠性、任务可靠性评估和可靠性优化等，其中任务可靠性建模与评估是可靠性工作中的难点工作。任务可靠性预计是指通过设定各阶段的任务失效判据，构建任务 RBD，通过设置故障逻辑树的底事件发生概率，计算任务成功的可靠度，进而可以估量失效的功能对整个阶段或整个任务的影响。工程上，任务可靠性指标包括任务可靠度和 MTBCF，两者可相互转化。

针对系统的动态可重构特性可开展基于有限状态机模型的任务可靠性分析，可解决传统 FMEA 不可进行动态分析的技术缺陷。动态可重构系统任务可靠性分析具体过程

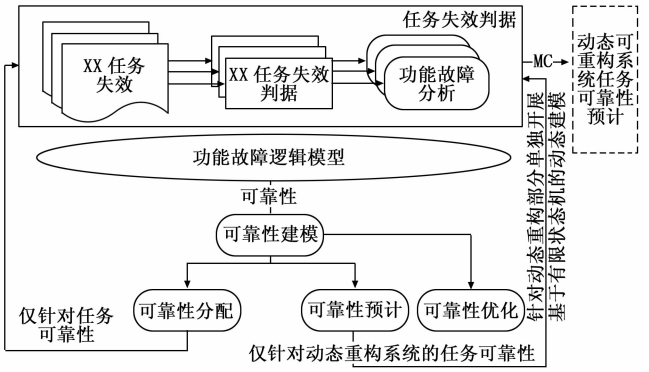


图 3 可靠性一体化建模评估过程

如下：

1）建立系统任务失效判据：

针对系统顶层功能定义开展功能 FMEA 分析，任务失效判据[13]建模用于确定系统功能故障对任务失效的影响关系，在模型中通过“任务剖面”模块进行实现。

2）任务可靠性建模：

根据系统容错设计机制，针对其动态重构部分单独开展基于有限状态机的动态建模过程。

3）系统任务可靠性分析评估：

基于蒙特卡罗仿真[14]进行任务可靠性仿真分析，在计算机模型中产生随机事件（如与系统故障相关的事件），包括：预定事件（如预防性维修行为）和条件事件（如由于其他事件出现而引起的事件），来产生一个模拟寿命片段尽可能接近一个真实寿命片段。

可靠性优化[15]是在满足系统已知物理、资源和经济约束下，通过提高成品可靠性水平或调整整机或系统结构，从而使得系统可靠度不小于目标值的方法。主要包括以下两种：

单元可靠性优化是在在不改变系统现有可靠性模型的条件下，并满足物理、资源和经济等约束条件，通过提高成品的可靠性水平来提高系统的可靠性水平。

余度设计优化是以系统现有可靠性模型为基础，并满足物理、资源和经济等约束条件，进行架构优化，通过增加或减少设备余度来优化系统的可靠性水平。

### 2.4 测试性一体化建模评估技术

基于多信号流的测试性模型[16]是将一组单信号的依存模型附加到结构模型上，形成底层故障依存模型，并对各层添加测试点及测试方式，形成测试性模型。多信号模型只捕获对系统故障诊断有用的必要信息，不管那些不必要的细节，与结构密切相关。

测试性建模与评估主要包括：可达性分析、定量评估、定性分析和诊断策略分析等。

测试性一体化建模评估过程见图 4。

1）模型可达性分析：

用于检查模型中故障模式和测试的依存关系[17]是否正确，以及不同的工作模式或任务重构情况下的依存关系是否正确。还可以辅助信号流检查。

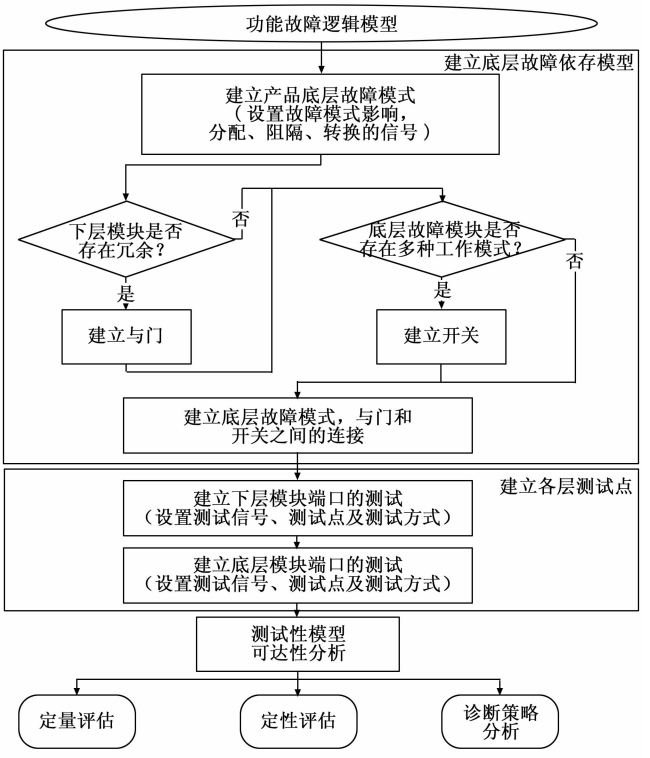


图 4 测试性一体化建模评估过程

2）测试性动态分析：

用于评估使用各种测试手段下（加电 BIT、在线 BIT、ATE、人工测试等）产品的故障检测率和故障隔离率（隔离到 1、2、3 个可更换单元）。采用对测试性模型的动态分析进行测试性定量评估[18]，通过模拟在设定时间内所发生的事件集（设备故障/修复），对整个模型状态的影响，通过故障逻辑验证、仿真计算的实现。

3）测试性静态分析：

用于发现测试性检测与隔离的缺陷[19]，依据建立的产品测试性模型，通过静态分析所有测试手段下的依存矩阵，进而分析测试性设计的故障检测覆盖和隔离情况，如未检测故障、模糊组、冗余测试、隐藏故障、掩盖故障和反馈环等，支持设计的权衡优化。

4）诊断策略生成：

用于表征对被测对象进行故障检测和故障隔离的测试顺序及诊断分支。充分考虑了故障模式在同一层次和不同层次之间的影响关系，同时使用了故障隔离的优化算法[20]，因此基于模型形成的各诊断策略可作为机上各诊断要素（测试手段）和机下各诊断要素（测试手段）编写测试逻辑的基础，同时也是机上机下、不同产品层级之间开展综合诊断设计的基础。

## 3 燃油系统“三性”一体化评估案例分析

### 3.1 功能故障逻辑模型构建过程

某直升机的燃油系统采用两个机内标准燃油箱，具有

重力加/放油、地面/悬停压力加油、空中应急放油等能力。发动机起动、正常工作和 APU 工作时，采用增压供油，当一个油箱低油位告警或一条供油管路故障时，可进行交叉供油，满足双发供油要求，在发动机失火或直升机坠毁等应急情况下，实现断油功能，切断向发动机的供油。燃油系统功能模型如图 5 所示。

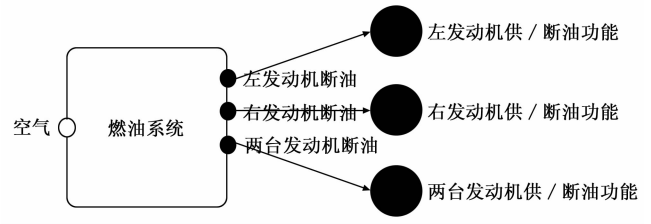


图 5　某直升机的燃油系统

将燃油系统功能“映射”到具体的物理架构，进行燃油系统内部功能关系构建，详见图 6。

燃油系统主要由燃油系统、通气系统、供油系统、地面/悬停压力加油系统、应急放油系统、外挂油箱系统等组成，其中供油系统存在 3 种工作模式，在供油管中设置供油选择阀，通过电动控制开关实现直接供油、交叉供油、断油 3 种模式切换。供油选择阀的失效模式如图 7 所示。

在燃油系统中，3 种场景工作模式切换存在复杂备份机制，如若不考虑，则不能真实反映燃油系统实际供油情况，较传统 FMEA 存在明显优势。

此外，传统 FMEA 分析中，不考虑外因，只考虑自身原因，本文在分析左供油选择阀故障逻辑分析时除了考虑阀门自身泄露、堵塞外，还考虑燃油输入问题、右供油选择阀、无通告、误动作等方面问题。

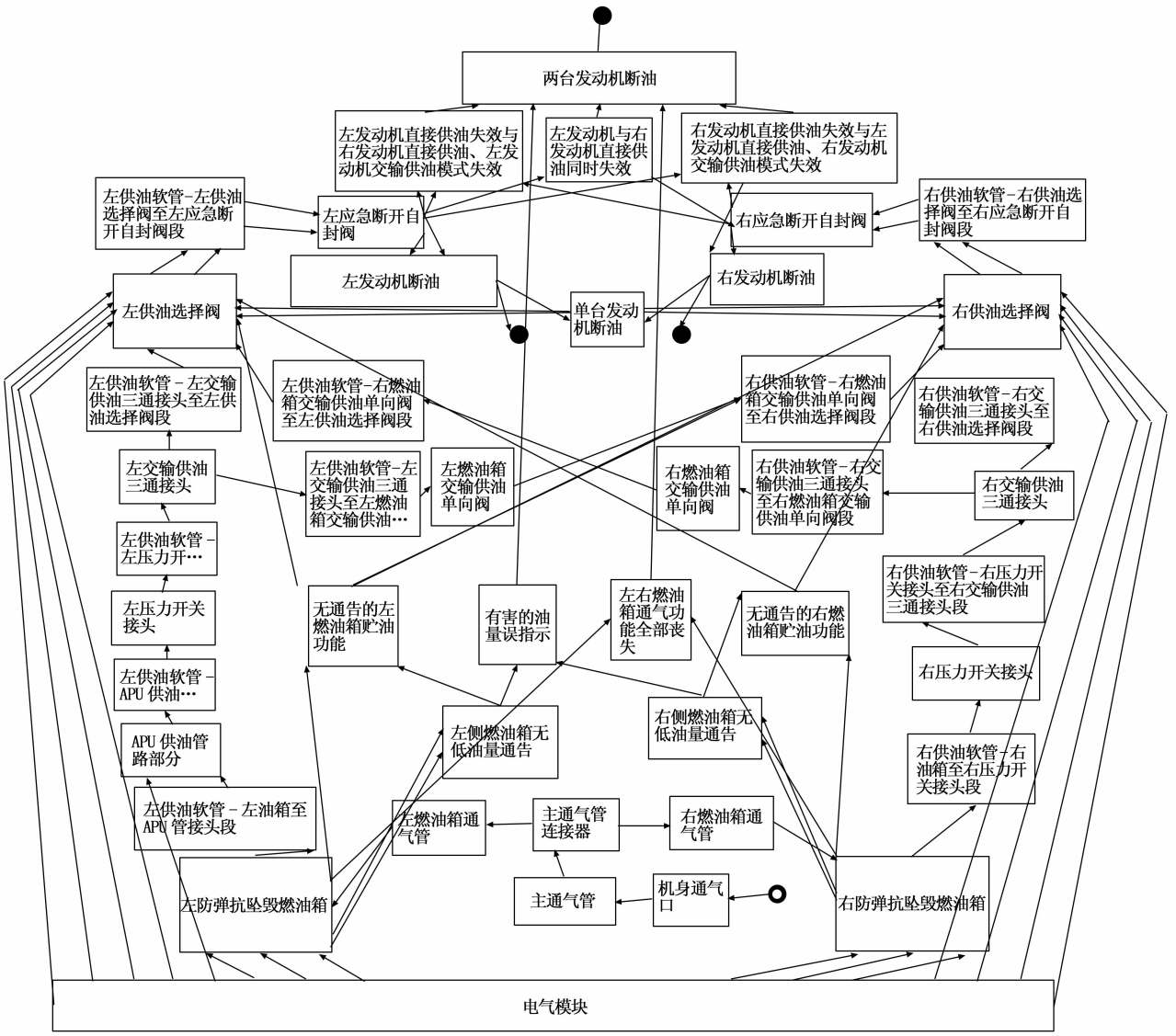


图 6　燃油系统功能与物理映射关系

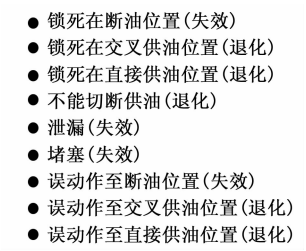


图 7 供油选择阀的失效模式

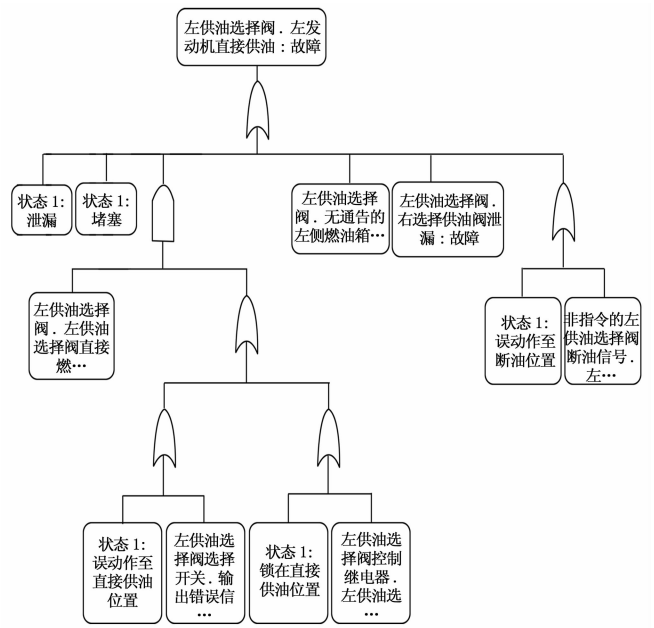


图 8 左供油选择阀供油故障逻辑关系

经过以上分析，基于功能故障逻辑关系更加符合实际情况，可解决传统 FMEA 只考虑单因素技术缺陷问题。

### 3.2 安全性建模评估过程

1）基于模型的 FHA 分析过程：

针对左发动机供断油故障、右发动机供断油故障、两台发动机供断油故障 3 项进行功能故障分析。

针对燃油系统的顶层输出端口，分别计算了顶事件各输出端口功能失效的功能危害性分析，计算出某项功能失效的概率（不可靠度）。

2）基于模型的 FTA 分析过程：

安全性指标分配、各顶事件故障树计算以及故障传递。功能故障逻辑的构建过程以及 FHA 分析过程，即 FTA 构建过程。

经 FTA 分析确定燃油系统的单点故障有 3 个：左供油选择阀、油供油选择阀和机身通气孔。建议加强对三者的可靠性设计或适当考虑余度设计。

### 3.3 可靠性建模评估过程

1）基本可靠性分析过程：

基本可靠性模型（RBD）是依据故障逻辑模型生成，在此基础上完成了基本可靠性预计、分配。

2）任务可靠性分析过程：

首先设置典型任务剖面，定义阶段和持续时间，如图 9，故障发生影响阶段任务完成作为判据，设定任务剖面内所有阶段的任务失效判据，如在飞行阶段两台发动机供断油故障的任务失效判据，详见图 10。

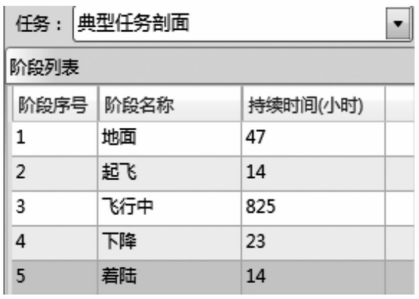


图 9 典型任务剖面设定

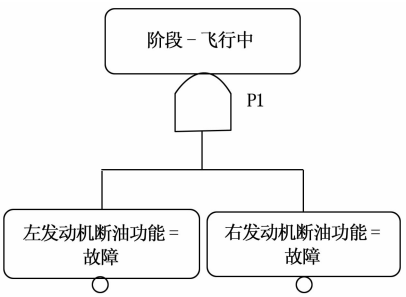


图 10 飞行阶段两台发动机供断油任务失效判据

基于任务剖面和失效判据设定，对燃油系统进行任务可靠度分析，与 FTA 分析的相应功能失效的概率（即不可靠度）结果一致。

### 3.4 测试性建模评估过程

（1）信号及测试设置：

在故障逻辑模型的基础上增加了 13 项测试，给各故障模式和测试分配相关的 86 项信号，设置了 4 个测试点，完成了测试与故障模式的相关性建模和可达性验证。

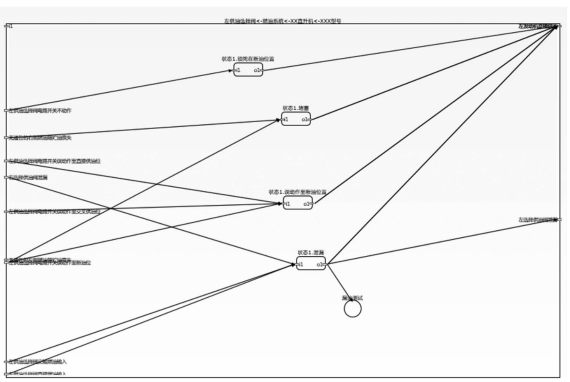

图 11 左供油选择阀测试性模型

（2）测试性分析及改进建议：

初步对燃油系统的故障检测率和故障隔离率进行了分

析，能够得出 BIT 检测率，故障检测和隔离主要通过 ATE 和人工进行的相关结论，能够对产品的测试性设计改提供参考和指导。

1）燃油系统的 BIT 故障检测率的要求值为 90%，而预计的值为 26.95%，远低于指标要求。从基层级故障检测率与故障隔离率表中可观察到，BIT 和 ATE 综合的故障检测率为 99.89%，由此可知，燃油系统的故障检测能力主要通过外部的测试设备实现。

2）燃油系统的 BIT 故障隔离率（1 个 LRU）的要求值为 75%，而预计的值为 75%，也未达到指标要求。从基层级故障检测率与故障隔离率表中可观察到，BIT 和 ATE 综合的故障隔离率为 42.33%，由此可知，燃油系统外场发生故障时，约 42%的故障可通过 BIT 和 ATE 进行排故，而 58%的故障需要人工进行排故。

## 4　结束语

为解决工程中“三性”评估工作中存在孤岛、重复性工作量大、系统性不强、存在“两张皮”等工程问题，本文围绕“三性”一体化建模评估的可行性、建模语言以及评估过程进行了说明，并以安全问题频发的燃油系统为例进行了“三性”一体化建模评估说明。

本文以功能故障为核心，通过统一模型进行一体化评估，建立了专业间密切联系，快速、便捷、系统地开展相关工作。基于 MBSE 的“三性”一体化建模评估的优势在于：实现了模型复用，解决了专业间的孤岛问题；基于功能模型构建故障逻辑，更接近真实的故障传递情况，有效解决“两张皮”现象；基于 AltaRica 语言建模过程中充分考虑多状态和多因素问题，有效解决传统 FMEA 静态单因素等方面的技术缺陷问题。

**参考文献：**


[1] 故障模式、影响及危害性分析指南（GJB/Z1391－2006）[S]. 北京：轨道交通安全技术研究中心，2006.

[2] WU J，YAN S，ZUO M J. Evaluating the reliability of multi－body mechanisms：A method considering the uncertainties of dynamic performance [J]. Reliability Engineering & System Safety，2016，149：96－106.

[3] 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）：140－151.

[4] 张　兵，陈建伟，杨　亮，等. 基于模型的系统工程在航天产品研发中的研究与实践 [J]. 宇航总体技术，2021，5（1）：1－7.

[5] 马永耀，赖　喆，方子豪. 基于模型的质量可靠性设计分析实践 [J]. 电子产品可靠性与环境试验，2019，37（3）：25－32.

[6] 陈　颖，康　锐. FMEA 技术及其应用 [M]. 北京：国防工业出版社，2014.

[7] 孙征虎，角淑媛，李福秋. 型号 FMEA 工作中存在的问题及应对措施分析 [J]. 质量与可靠性，2013（3）：1－5.

[8] 危　虹，傅　耘. 基于模型的“四性”综保系统工程设计 [J]. 装备环境工程. 2015，12（6），53－58.

[9] 赵廷弟. 安全性设计分析与验证 [M]. 北京：国防工业出版社，2011.

[10] ZHOU Y Z，REN Y，LIU L L，et al. Binary Logic State Transition Oriented Formal General Reliability Model [J]. J. Shanghai Jiaotong Univ.（Sci.），2015，20（4）：482－488.

[11] PROSVIRNOVA T，BATTEUX M，BRAMERET P A，et al. The AltaRica 3.0 project for model－based safety assessment [C] //2013 11th IEEE International Conference on Industrial Informatics[s. l.]：IEEE，2013：741－746.

[12] RAUZY A B. Guarded transition systems：A new states/events formalism for reliability studies [J]. Journal of Risk and Reliability，2008，222（4）：495－505.

[13] ZHU Y Z，ZHANG J G，GONG Q，et al. Reliability and safety assessment with AltaRica for complex aircraft systems [C] //2011 9th International Conference on Reliability，Maintainability and Safety[s. l.]：IEEE，2011：588－593.

[14] LEVESON N G. Engineering a safer world：Systems thinking applied to safety [M]. Boston：MIT Press，2011.

[15] LEVESON N G. A Systems－theoretic Approach to Safety in Software－intensive Systems [J]. IEEE Transactions onDependable and Secure Computing. 2004，1（1）：66－86.

[16] CHRISTIAN S. Inclusion of reliability and Safety analysis methods in modelica [C] //Proceedings 8th Modelica Conference，2011：616－627

[17] BAJAJ M，BACKHAUS J，WALDEN T，et al. Graphbased digital blueprint for model based engineering of complex systems [J]. INCOSE International Symposium，2017，27（1）：151－169.

[18] TROUBITSYNA E. Elicitation and Specification of Safety Requirements [C]. Third International Conference of System，Cancun：2008.

[19] PROSVIRNOVA T，BATTEUX M，BRAMERET P A，et al. The AltaRica 3.0 project for model－based safety assessment [C] //2013 11th IEEE International Conference on Industrial Informatics [s. l.]：IEEE，2013：741－746.

[20] PENG H，FENG Q M，COIT D W. Reliability and maintenance modeling for systems subject to multiple dependent competing failure processes [J]. IIE Transactions，2010，43（1）：12－22.