

基于 Simscape 模型的航空发动机 系统安全性分析方法

楚娜娜¹, 张曙光¹, 高艳蕾², 魏志远¹, 邵 年³

(1. 北京航空航天大学 交通科学与工程学院, 北京 100191;

2. 中国民用航空局 中国民用航空适航审定中心, 北京 100102;

3. 中国航空工业集团有限公司 航空动力控制系统研究所, 江苏 无锡 214063)

摘 要: 针对航空发动机系统安全性分析中的耦合情况, 研究基于 Simscape 模型的航空发动机耦合故障建模和安全性分析问题。在基于模型的安全性分析(MBSA)故障拓展一般特点的基础上, 分析了 Simscape 环境下进行故障外部拓展和建模语言内部故障拓展两种方式, 以建立耦合故障模型。以全权限数字式发动机控制(FADEC)主燃油控制子系统为研究示例, 进行独立和耦合故障形式化系统安全性分析。结果表明: 航空发动机系统安全分析 Simscape 模型基于系统设计环境, 可直接成为系统设计和安全性分析共同的工具, 便于保证设计和安全性分析的一致性; 该模型拓展方法和建模语言, 从故障数学原理出发, 对实际系统不同物理域的组件独立和耦合故障特性具有灵活和定量描述能力; 由此拓展的故障模型下的安全性分析具有形式化、直观性和客观性的优势。

关 键 词: 航空发动机主燃油控制子系统; 系统安全性分析; 故障拓展模型; Simscape 软件;
耦合故障

中图分类号: V23

文献标志码: A

Safety analysis method of aero-engine systems based on Simscape model

CHU Nana¹, ZHANG Shuguang¹, GAO Yanlei²,
WEI Zhiyuan¹, SHAO Nian³

(1. School of Transportation Science and Engineering,
Beijing University of Aeronautics and Astronautics, Beijing 100191, China;

2. Airworthiness Certification Center,
Civil Aviation Administration of China, Beijing 100102, China;

3. Aviation Motor Control System Institute,
Aviation Industry Corporation of China, Limited, Wuxi Jiangsu 214063, China)

Abstract: In view of the problem of coupling influence in the system safety analysis of aero-engines, the coupling fault modeling and safety analysis of aero-engines based on Simscape model were studied. Combined with the general characteristics of fault extension in model based safety analysis (MBSA), two ways of fault external expansion and internal fault

收稿日期: 2020-07-08

作者简介: 楚娜娜(1996—), 女, 硕士生, 主要研究方向为系统安全性分析。

通信作者: 张曙光(1969—), 女, 教授、博士生导师, 博士, 主要研究方向为飞行系统动力学与控制、航空器安全性与适航。

E-mail: gnahz@buaa.edu.cn

引用格式: 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. CHU Nana, ZHANG Shuguang, GAO Yanlei, et al. Safety analysis method of aero-engine systems based on Simscape model[J]. Journal of Aerospace Power, 2021, 36(4): 885-896.

expansion based on modeling language of Simscape model were analyzed, so as to establish a model considering the coupling faults. Taking the main fuel control subsystem in full authority digital engine control (FADEC) as a research example, formal safety analysis of the independent and coupling fault was conducted. The results showed that the Simscape model of aero-engines system safety analysis based on the system design environment can be used as a common tool for system design and safety analysis, which can ensure the consistency of design and safety analysis. Based on the principle of fault mathematics, the model expansion method and modeling language can flexibly and quantitatively describe the component independency and coupling fault characteristics in different physical domains of the actual system. The safety analysis based on the extended fault model had the advantages of formalization, intuitiveness and objectivity.

Key words: aero-engine main fuel control subsystem; system safety analysis; fault-extended model; Simscape software; coupling fault

保证安全性是航空发动机设计和制造的重要原则之一,适航规章中针对航空发动机系统安全性有专门条款要求,如 FAR 33.75^[1]、CS-E 510^[2]和 CCAR 33.75^[3]等。

作为高度综合的复杂系统,航空发动机整体和子系统之间存在广泛的耦合影响,使传统基于模块化方法在系统安全分析的深度和效果上存在局限性^[4]。在喘振和吸雨、吸雹等安全问题中涉及的航空发动机气动热力模型具有强耦合非线性特性^[5]。2000年,Xu等以涡轮增压器转子轴承子系统为例指出,航空发动机与其子系统之间气动上的滞后性,会造成故障模式之间、故障模式和故障影响之间相互耦合^[6]。同时,航空发动机系统的连续非线性使其失效模式与影响间也可能存在连续性的数据关系(如航空发动机转速与涡轮前温度的耦合)。因此,耦合性事件分析是航空发动机系统安全性分析中常见的复杂问题,需要审慎处理。

美国联邦航空管理局咨询通告 AC 33.75^[7]和欧洲航空安全局指导文件 AMC E510^[2]等局方文件均将协会标准 SAE ARP4754A^[8]和 SAE ARP4761^[9](以下简称 4761)作为表明系统安全性的可接受指导文件,其中主要引用的分析方法有故障树分析(fault tree analysis,FTA)、故障模式故障影响分析(failure mode and effect analysis,FMEA)等。FTA方法在故障树结构建立和定量分析中,除考虑事件间的发生顺序外,一般基于同级事件的独立性。FMEA方法主要考虑单个故障模式的故障影响,回避了故障模式及影响间的耦合性^[9]。对FMEA的发展,多是针对组件

功能建立系统故障传播逻辑和推理决策的独立安全性分析模型,进行半自动的独立故障和耦合故障 FMEA^[10-13]。此外,FMEA和 FTA方法应用耗时、繁琐、工作量大,且多基于经验和分析人员对系统的主观理解,容易出错^[14-16]。

针对传统分析方法的局限性,随着形式化系统开发过程和安全性分析语言的发展,2005年,Joshi等首次提出基于模型的安全性分析(model-based safety analysis,MBSA)^[17]的概念,提出了分析的一般框架包括:建立形式化语言描述的名义系统模型,定义形式化的故障影响和故障模式,将形式化的故障模型拓展到系统模型中,最终对拓展模型实现自动安全性分析^[18]。此外,国际自动机工程师学会(SAE)在 4761 的修改建议中提出纳入 MBSA 方法^[19]。

迄今,已经提出了多种技术和工具用于支持 MBSA 方法,本文总结了典型 MBSA 方法的技术特征,如表 1 所示。按照模型来源,MBSA 模型可分为两类:由分析人员建立的独立于系统模型的安全性分析模型和以系统设计模型为名义系统建立的故障拓展模型。此外,各技术的建模逻辑、适用的建模环境的差别,使得 MBSA 技术种类非常丰富,模型抽象度不同,每种方法适用的对象和分析阶段也不同。

MBSA 方法拥有不同层级模型的描述能力,具有在航空发动机系统安全分析各个阶段应用的潜力。从航空发动机设计模型出发,2012年,丁水汀等使用以部件为主的模块化方法建立航空发动机气动热力模型,辅助全权限数字式发动机控制(FADEC)可变放气活门系统功能危险性分析

表 1 不同 MBSA 技术特征对比

Table 1 Comparison of different MBSA technical characteristics

MBSA 技术	建模方式	方法特征	建模环境	应用特点	抽象度
FPTN(failure propagation transformation notation) ^[20]	独立模型	• 不对系统的正常行为进行建模 • 关注失效在系统中的传播路径 • 模块间的连接基于失效模式		• 没有工具辅助 • 工作量较大 • 实用性较差	很高
Hip-Hops ^[21]	部分设计模型	• 生成组合失效的 IF=FMEA 表格 • 模块间的连接基于系统架构 • 基于模型进行失效注释 • 故障树的合成为演绎过程	Hip-Hops	• 具备模型自动分析算法和故障树自动生成算法	极高
Altarica ^[22]	独立模型	• 以事件为中心 • 用变量来描述系统状态 • 对系统功能及失效进行建模	OpenAltarica	• 航空领域应用广泛	非常高
Modelica ^[23]	部分设计模型	• 基于对象的数学模型 • 支持连续和离散系统建模仿真计算 • 用户无需关注模型求解和编程实现	OpenAltarica	• 支持的仿真平台多 • 多用于航空航天,汽车领域	低
Sysml ^[24]	独立模型	• 图形化建模语言 • 描述和分析包含软硬件、人因、信息等的复杂系统		• 通用性强 • 功能强大	较低
4761A ^[19]	独立模型	• 基于失效逻辑建模	Stateflow statemate		高
Simscape ^[25]	部分设计模型	• 模型库提供物理组件模块 • 支持组件的自定义 • 建模基于组件物理模型的数学表达	Matlab- Simscape	• 对物理系统有较强表征能力	低

(function hazard analysis, FHA)^[26]。2020 年, Gan 等以非包容的高能碎片为例,结合 FHA,对不同参数(包括耦合性参数)建立航空发动机安全性影响上的转换链模型^[27]。而在更宏观层,2016 年,Peter 等在运行层级使用架构分析与设计语言(architecture analysis and design language, AADL)建立 FADEC 燃油流动的黑盒功能架构,基于状态机建立组件间故障传播路径,并融合 FHA 等方法分析故障危害性影响^[28]。但是这两类独立安全分析模型,前者偏向于航空发动机底层物理模型层级,后者偏向于航空发动机顶层的黑盒分析模型层级,对设计模型的描述细致程度差异较大,难以保证设计模型和安全分析模型的一致性,即存在“抛过墙”问题^[29]。

针对独立安全性分析模型的局限性,为有效避免设计和安全分析的“抛过墙”情况,并力图将设计(特别如航空发动机控制系统设计)和安全性分析纳入到统一框架下,2015 年,文献[25]在

Mathworks 的 Simscape 框架下建立舵面控制系统的物理模型和故障外部拓展模型,且在机轮刹车系统和 FADEC 主燃油控制子系统安全性分析模型上有一定建模基础^[30],并尝试针对模型进行独立故障的安全性分析。Simscape 提供不同物理域的组件库,且支持在 Simulink 环境中快速搭建自定义颗粒度的系统组件模型,组件物理特性的变量和参数化表达隐藏在组件内部建模语言中,使模型在对实际系统和故障模式具有很强的描述能力的同时,又具有对真实系统的直观性和拟真度表现。结合 Simscape 建模优势,本文在文献[30]的基础上,研究航空发动机基于模型的形式化系统安全性分析方法问题,重点探讨:

- 1) Simscape 环境对故障模式、时序性故障、故障耦合等拓展要素建模的适用性。
- 2) 基于 Simscape 模型的航空发动机独立和耦合故障系统安全分析的可行性。

1 基于 Simscape 的故障拓展

1.1 故障拓展模型要素分析和建模

形式化故障模型需要对物理模型进行抽象,考虑故障行为的不同类型、故障的触发、故障存在的时间等。本节对故障拓展模型的要素以及其在 Simscape 环境下的可实施性进行分析。

1.1.1 故障模式分类和形式化表达

在故障模式分类上,对于常用的电子电气元件、零部件等,故障模式及其失效率的确定可参照国内外标准、手册,如 MIL-HDBK-338B《电子设备可靠性设计手册》、《非电子零部件可靠性数据》等。文献[23]提出针对机械、电路、液压等不同物理域的形式化故障模式分类和建模。

在形式化建模中,为降低建模细节需求,并考虑实际组件故障发生概率的可能性,通常对组件定义最多 3 个故障模式,以此建立通用的故障模式分类定义方式,如表 2 所示。模式 1 通常指流通变量(v_{flow})变化表征的故障,如电路电流 $I \rightarrow 0$,机械力 F 、力矩 $M \rightarrow 0$;模式 2 通常指跨越变量(v_{pot})变化表征的故障,如电路电压 $U \rightarrow 0$,机械位移 x 、速度 v 、加速度 $a \rightarrow 0$;模式 3 包含一些非期望的功能或状态变化,如参数飘移、传感器等虚假信息输出等,也包括模式 1 和模式 2 不包含的失效情况。

表 2 通用组件故障模式定义

Table 2 General component fault modes definition

故障模式分类	故障模式描述
0	正常
1	流通变量表征的故障行为
2	跨越变量表征的故障行为
3	功能错误、非预期状态、参数飘移等

组件的失效不一定是绝对的完全丧失或错误(失效程度为 100%),也可能存在如阀门部分卡阻等一定程度的失效。Simscape 环境基于变量数学表达式来表征组件物理特性的特点,使其在连续性的 0~1 不同程度失效模拟上具有优势。

1.1.2 故障模式拓展方式

对故障行为的表现,Simulink/Simscape 环境下可采用下列两种方式。

1) 故障模型外部拓展

故障外部拓展对接入正常系统的组件外加故障触发端口和故障模式输入端口,故障触发端口

使该组件连接到失效模式,故障模式输入端口为故障模式提供特定的表现形式。Multiport switch(多端口选择开关)为常用的故障外部拓展工具,如图 1 所示。

如理想线性电阻元件的故障,可用其特征参数电阻值的不同取值来模拟,如表 3 所示,在 Simscape 环境下的故障外部拓展如图 2 所示。FM_resistance 是失效模式的触发端口,输入为 0,正常电阻接入系统,输入为 1 和 2,具有断路和短路故障的电阻分别接入系统。

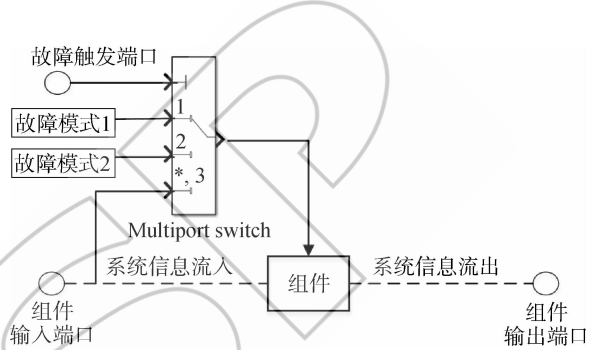


图 1 组件故障外部拓展示意图
Fig. 1 Component fault external extension

表 3 电阻故障模式举例
Table 3 Resistance fault modes example

故障模式编号	0	1	2
故障模式描述	正常	断路	短路
电阻值/ Ω	R	0	∞

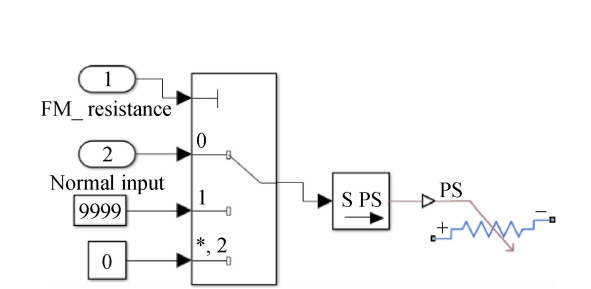


图 2 电阻独立故障模式拓展
Fig. 2 Independent resistance fault-extended model

2) 故障模型组件内部拓展

Simscape 除提供不同物理域的组件库外,还支持用户基于 Simscape 语言自定义组件。由此考虑将故障模式添加到组件建模过程中,进行组件故障模式内部拓展,建立自定义故障模式拓展组件。

故障模式的内部拓展主要基于组件底层数学模型,建立组件不同故障模式 i 下的变量 $V_{\text{fm},i}$ 和组件正常流通变量、跨越变量的函数关系,如:

$$V_{fm,i} = f_i(v_{flow}, v_{pot})$$
$$i = 0, 1, 2, 3 \text{ 表示故障模式} \quad (1)$$

此方式从组件故障的内部物理模型出发,用数学关系建立故障表现形式。

如电流传感器故障模式及其物理表达式:电流测量值 I 与此组件的名义系统流通变量 i_1 (电流)的关系如表 4 所示。

表 4 电流传感器故障及物理表达式

Table 4 Current sensor fault and physical expression

故障模式 编号	故障模式描述	故障物理 表现形式
0	正常	$I = i_1$
1	测量的电流值偏大一倍	$I = 2i_1$
2	测量的电流值偏小一半	$I = 0.5i_1$

1.1.3 故障存在的时序性

组件故障还存在时序性问题,仿真时需要考虑实际组件故障形式触发和保持的时间长短。根据组件故障的时序性将故障分为永久故障和瞬态故障。

永久故障:组件的故障特性不随时间变化,如 $t=0$ 时刻开关断开,断开状态具有永久性,不主动随时间恢复。永久性故障用变量形式化表达为

$$V_{fm} = f(v_{flow}, v_{pot}), \quad t = (0, \infty) \quad (2)$$

其中 V_{fm} 为组件的故障模式特征变量值, $t=0$ 时刻故障发生。

瞬态故障:组件故障模式表现出随时间呈离散性或连续性变化的特征。故障模式随时间离散性变化的形式化表达为

$$V_{fm,t} = \begin{cases} f_1(v_{flow}, v_{pot}, t), & 0 < t < t_1 \\ f_2(v_{flow}, v_{pot}, t), & t_1 \leq t \leq t_2 \end{cases} \quad (3)$$

其中 $V_{fm,t}$ 为 $t=0$ 时刻组件开始故障后, t 时刻的故障模式特征变量值。

故障模式随时间的连续性变化可能是基于 t 的故障程度递推累积,即

$$V_{fm,t(k+t)} = V_{fm,t(k)} + f(t), \quad k < t < k + t \quad (4)$$

其中 $V_{fm,t(k+t)}$ 为组件 $k+t$ 时刻的故障特征变量值, $V_{fm,t(k)}$ 为组件 k 时刻的故障特征变量值。

另外情况,如组件故障模式随时间的变化始终为连续性微分关系,即

$$V_{fm,t} = f(v_{flow}, v_{pot}, t), \quad t = (0, \infty) \quad (5)$$

对于故障时序性的模拟,针对故障外部拓展方式,使用 signal builder 设计组件每个时刻的故障模式。如设定电阻在 10 s 内从前 4 s 正常到第 5 s 短路,之后一直处于断路状态的故障触发端口取值,如图 3 所示。

针对组件内部故障拓展的建模方式,通过在 m 文件中建立该组件故障模式及其特征参数随仿真时间变化的关系,也可实现组件故障的时序仿真。

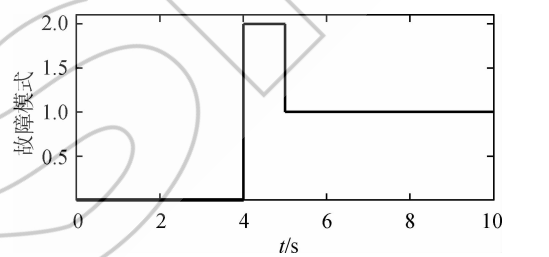


图 3 电阻故障时序建模

Fig. 3 Resistance fault timing modeling

1.2 耦合故障建模

基于文中第 1.1 节描述的组件故障拓展要素,研究耦合故障的形式化建模。故障耦合实际上是故障模式、故障表现形式和故障时序等要素的组合情况。对耦合关系进行分类和形式化定义,耦合要素的部分举例如表 5 所示。

对故障模式之间耦合关系的模型化表达,如图 4 所示,在 a 组件故障模型的触发条件(FM_trigger a)中纳入 b 组件故障触发条件(FM_trigger b),来模拟 b 组件故障模式与 a 组件故障模式的耦合。

表 5 故障耦合关系描述

Table 5 Fault coupling relationship description

故障耦合分析要素	耦合要素分析	形式化语言描述举例
耦合故障类型	故障模式之间、故障模式与故障影响之间	b 组件的故障模式 i 引起 a 组件的故障模式 j
		$F_{mode,a,j} = f(F_{mode,b,i})$
		b 组件的故障影响引起 a 组件的故障模式 j
		$F_{mode,a,j} = f(F_{effect,b})$
		$i, j = 0, 1, 2, \dots$, 表示故障模式

续表

故障耦合分析要素	耦合要素分析	形式化语言描述举例
耦合关系	绝对致因关系	b 组件故障引起绝对的 a 组件故障
	潜在关系	b 组件故障是 a 组件故障的必要不充分条件
	即时性	组件故障立即引起 a 组件故障
耦合的时序性	延迟性	b 组件故障 t_s 后引起 a 组件故障
		if $t=t_0, F_{\text{Mode},b}=i \quad t=t_0+t, F_{\text{Mode},a}=j$
耦合故障表现形式 及时序性 (如 b 组件故障模式 i 引起 a 组件故障 模式 j)	耦合故障模式 j 不随 t 变化	if $F_{\text{mode},b}=i, \quad t=0$ $F_{\text{mode},a}=j, \quad t=(0,\infty)$
	耦合故障模式 j 随 t 连续变化	if $F_{\text{mode},b}=i, \quad t=0$ $F_{\text{mode},a,j}=f(F_{\text{mode},b,i},t) \quad t=(0,\infty)$
	耦合故障模式 j 随 t 离散变化	if $F_{\text{mode},b}=i, \quad t=0$
		$F_{\text{mode},a,j,t}=\begin{cases} f_1(F_{\text{mode},b,i},t), & 0<t<t_1 \\ f_2(F_{\text{mode},b,i},t), & t_1\leq t\leq t_2 \end{cases}$

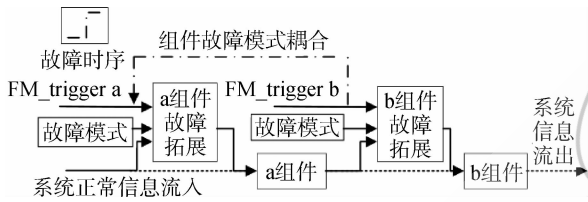


图 4 故障模式之间耦合关系建模

Fig. 4 Coupling modeling between fault modes

对故障影响与故障模式的耦合关系模型化表达,如图 5 所示,在系统中分别建立 b 组件故障影响模型,并将其纳入 a 组件的故障模式触发条件中。

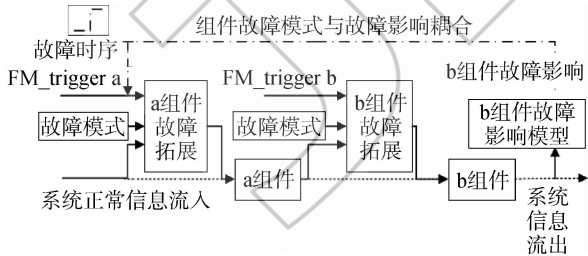


图 5 故障模式与故障影响耦合关系建模

Fig. 5 Coupling modeling between fault modes and fault effect

2 FADEC 主燃油控制子系统独立故障安全性分析示例

针对航空发动机 FADEC 主燃油控制子系统,以系统中各组件功能的物理行为模拟为主,基于前述故障拓展方式,建立拓展安全性分析模型,并进行形式化的单故障和多故障安全性分析,系

统选取和建模以通用性的分析为目的,不针对实际型号航空发动机。

2.1 主燃油控制子系统形式化建模

如图 6 所示,FADEC 系统的主燃油控制子系统能实现:在驾驶员给定期望航空发动机工作状态的操纵输入下,精确控制进入燃烧室的燃油流量。此外,当需要紧急关闭航空发动机时,驾驶员可通过紧急关断装置把关断指令传给高压燃油泵和飞机关断电磁阀,从而切断燃油。

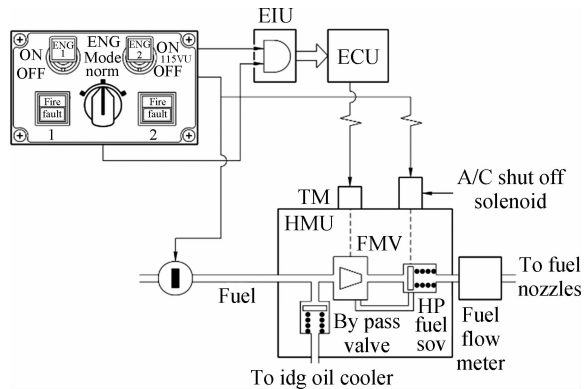


图 6 燃油供油控制功能组件^[31]

Fig. 6 Fuel supply control function components^[31]

从飞机燃油系统进入航空发动机的燃油要经过燃油分配系统进行清洁和加压,用于燃烧和液压。按照燃油流动的顺序,进入航空发动机的燃油主要经过低压燃油泵、燃油滤、高压燃油泵、由电子控制器(electronic engine controller,EEC)控制的燃油计量部分以及经过旁通支路作为伺服动作^[28]。

在 Simscape 环境中对上述 FADEC 系统的主燃油控制子系统进行形式化建模。模型主要包括 FADEC 燃油控制电路组件、从电信号到电液伺服阀的液压信号转换,以及燃油分配系统的作动组件,如燃油泵、燃油计量活门(fuel metering valve, FMV)。以下为各组件建模的详细描述。

FADEC 数字电子控制单元(electronic control unit, ECU)系统一般为双通道,本示例探讨其单通道的功能:

- 1) 接收操纵指令;
- 2) 进行燃油控制指令计算,得到驱动液压机械单元(hydro mechanical unit, HMU)的电信号;
- 3) 接收传感器的反馈信息

扭矩电动机(torque motor, TM)接收来自 ECU 的电信号,再将其转化为旋转位移,驱动 FMV。使用电气到机械转动电动机来模拟,如图 7 所示。

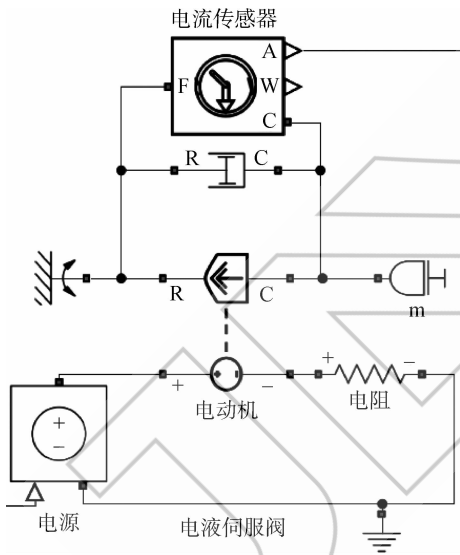


图 7 扭矩电动机名义模型

Fig. 7 Nominal model of torque motor

FADEC 系统中的燃油泵为系统提供液压动力,使用 Simscape 标准库中的开源液压源组件来模拟。对于正常状态下的恒压液压泵,无论流量多大,液压泵均能维持进出口的恒定压差。

将高压关断电磁阀和燃油滤抽象为决定液压线路是否流通的隔离阀,使用 Simscape 开源液压孔来模拟。最基本的液压孔包含进口和出口,通过孔口的体积流量与孔口上的压差成正比,为

$$q_v = C_d A \sqrt{\frac{2}{\rho}} \cdot \frac{p}{(p^2 + p_{cr}^2)^{\frac{1}{4}}} \quad (6)$$

$$p = p_A - p_B \quad (7)$$

其中 q_v 为通过液压孔的体积流量(下文简称为流量), p 为液压孔两端的压差, p_A 和 p_B 为液压孔端口的表压, C_d 为流量系数, A 为孔口面积, ρ 为流体的密度, p_{cr} 为从层流过渡到湍流对应的最小压力值,根据层流到湍流的转换规则,有两种计算方式。第一种是通过压比计算:

$$p_{cr} = (p_{avg} + p_{atm})(1 - B_{lam}) \quad (8)$$

$$p_{avg} = \frac{p_A + p_B}{2} \quad (9)$$

其中 p_{avg} 是液压孔两个端口对应表压的平均值, p_{atm} 是标准大气压, B_{lam} 是层流和湍流状态的压比。

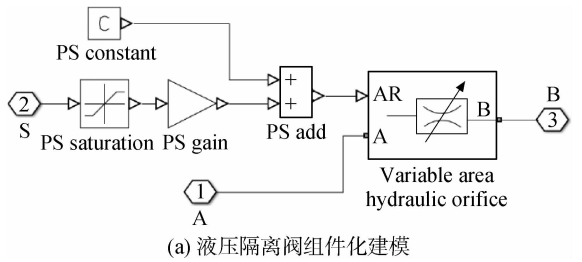
另一种是通过雷诺数计算湍流刚出现时的压力

$$p_{cr} = \frac{\rho}{2} \left(\frac{Re_{cr} u}{C_d D_h} \right)^2 \quad (10)$$

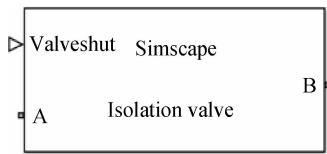
$$D_h = \sqrt{\frac{4A}{\pi}} \quad (11)$$

其中 D_h 是液压孔的直径, u 是流体速度, Re_{cr} 是临界雷诺数^[30]。

隔离阀的端口包括液压输入、输出的物理端口和根据外界信息决定隔离阀开闭的信号端口。阀门关闭,流通面积对应接近于 0,阀门全开,阀门流通面积对应最大。分别基于 Simscape 库中现有的组件对隔离阀进行建模和基于 Simscape 语言自定义隔离阀组件,如图 8(a)和图 8(b)所示。



(a) 液压隔离阀组件化建模



(b) 自定义液压隔离阀组件

图 8 液压隔离阀建模

Fig. 8 Hydraulic isolation valve modeling

FMV 是执行燃油流量控制的仪表阀,也将其抽象成能根据扭矩电动机输入的机械旋转信号控制流通面积开度,从而控制流量的液压孔。仪表阀的建模类似于隔断阀。

旁通阀使用 Simscape 标准库中的泄压阀来

模拟,如图 9 所示。当 FMV 前端压力大于阈值,部分燃油从泄压阀通过,流到燃油冷却器中。

燃油流量传感器能测量供入燃烧室的燃油流量值,使用 Simscape 库中的流量计模块模拟。

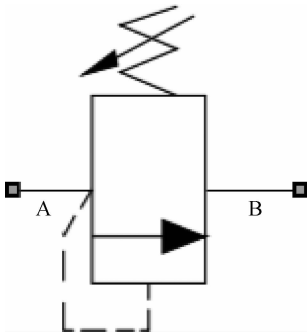


图 9 泄压阀
Fig. 9 Pressure relief valve

综合以上各组件模型,建立 FADEC 主燃油控制子系统的名义安全性分析模型,如图 10 所示。

2.2 独立故障形式化安全性分析

对图 10 的名义系统模型按照表 4 的故障模式定义进行故障拓展,建立电子类和机械类组件的扩展模型,可以进行 FMEA、时序故障和组合故障影响的仿真。将燃油流量的各种输出故障模式进行影响分析,结果如表 6 所示。

针对表 4 的系统故障模式,基于模型的自动安全性仿真分析结果如图 11 所示。其 4 种表现形式如流量输出正常、比期望值偏大、比期望值偏小和输出为 0。其中 $q_{V,cmd}$ 指期望燃油流量, $q_{V,real}$ 指系统实际燃油流量输出。

相比于传统 FMEA,上述分析结果也体现了基于模型的FEMA对故障影响图形化表达的直

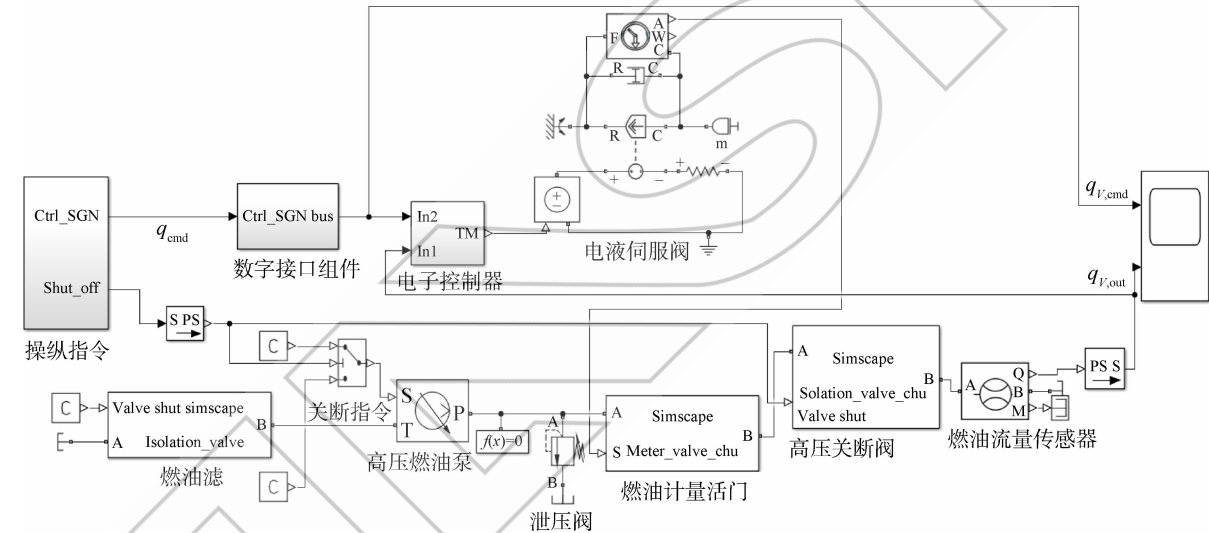


图 10 FADEC 主燃油控制子系统名义模型
Fig. 10 Nominal system model of FADEC main fuel control subsystem

表 6 基于 MBSA 的组件 FMEA
Table 6 Components FMEA based on MBSA

序号	组件名称	故障模式	故障模式描述	故障影响
1	EEC	1	指令丢失	燃油输出为 0
		2	指令偏大	燃油量输出偏大
2	主控通道电液伺服阀	1	卡在最大位置	燃油流量输出始终在最大值
3	主位移传感器	1	信号丢失	燃油流量为 0
		2	信号偏大	燃油流量输出偏小
4	燃油滤	1	燃油滤堵塞	燃油流量输出偏小
5	燃油泵	1	丧失液压供应	燃油流量输出为 0
		2	液压供应减小到所需的一半	燃油流量输出为期望值的一半

续表

序号	组件名称	故障模式	故障模式描述	故障影响
6	FMV	1	卡在关位	燃油输出始终为 0
		2	卡在全开位	燃油输出始终为最大值
		3	卡在中间位置	燃油输出始终为最大值的一半
7	高压燃油关断阀门	1	失去关闭功能	当有关断指令,且燃油泵始终供油时,燃油流量存在输出
		2	只能部分关闭	当有关断指令,且燃油泵始终供油时,燃油流量存在输出
8	燃油流量计	1	信号丢失	燃油流量测量值为 0,但实际系统流量输出正常
		2	监测值偏大	燃油流量实际输出偏小

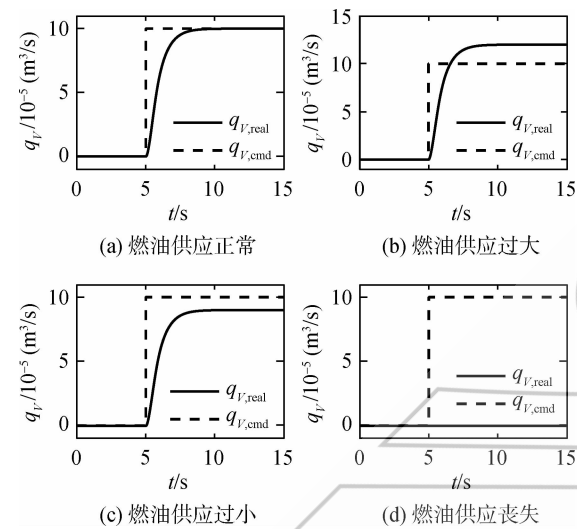


图 11 FADEC 主燃油控制子系统失效影响
Fig. 11 FADEC main fuel control subsystem fault effect

观性,以及对定量故障模式自动分析及其结果表达的确定性。关于 MBSA 方法的准确性,可参考文献[25,30],包括对基于模型的多故障影响分析和最小割集自动提取的方法及示例研究,以及针对 4761 中机轮刹车系统示例的基于模型的自动 FMEA 和传统 FMEA 结果对比。

对于时序故障的仿真如图 12 所示,其中当 FMV 在第 8 s 之后开度卡在最大面积的 10% 时,系统燃油流量输出减小为期望值的 20%。

对组合故障的仿真如图 13 所示,当 FMV 开度卡在最大面积的 10% 和燃油泵能提供的需用燃油流量减小直至为零故障同时存在时,能直观看到实际的燃油流量输出从期望值的 20% 逐渐减少至为零。图 12 和图 13 仿真曲线在第 8 s 处出现输出为零的尖点,是仿真过程中改变系统参数设置使系统重新开始仿真导致。

由此可见,进行模型形式化故障拓展后,能辅

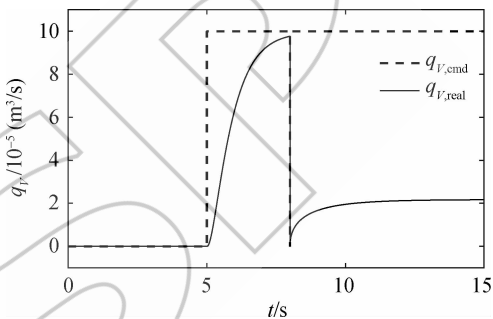


图 12 FMV 卡在最大开度的 10% 的影响
Fig. 12 Effect of FMV stuck at 10% of maximum area

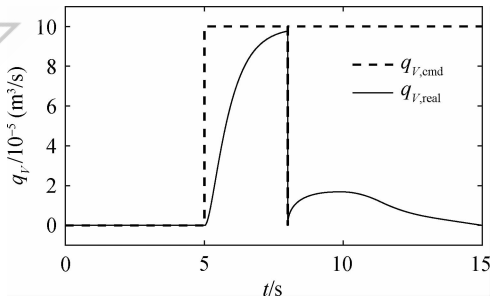


图 13 FMV 卡住且燃油泵供流能力线性下降
Fig. 13 Effect of FMV stuck and the fuel pump's supply capacity linear decline

助实现基于 Simscape 模型的自动 FMEA 安全性分析,以及故障组合情况和故障时序性影响分析。

3 FADEC 主燃油控制子系统耦合故障安全性分析示例

文中第 2.1 节 FADEC 主燃油控制子系统中,电子元器件的故障相对独立,而机械和液压组件之间物理性能联系紧密,故障耦合性更为明显。如燃油滤的畅通性会影响燃油流通压力,而燃油泵前后端的压力差会影响其性能进而影响系统最终的燃油流量输出。同时,对于没有依赖关系的

两个故障模式之间,故障发生的不同时序也可能产生不同安全性影响。因此,本节主要进行不同液压组件之间故障及故障时序性耦合影响分析。

3.1 燃油滤堵塞与燃油泵供流能力下降的故障耦合影响分析

建立燃油滤堵塞导致燃油泵供流能力下降的耦合关系模型,如图 14 所示。燃油滤部分堵塞使燃油流量输出减小但不为 0,同时假设其导致燃油泵的供流能力分段降低(通过燃油泵的流量输入变化来模拟,保证燃油正常输出的初始燃油泵流量输入 $q_{V,pump}=2.4\times 10^{-5}\text{ m}^3/\text{s}$ 。

对图 14 的燃油滤故障与燃油泵故障的耦合影响情况进行仿真观测,如图 15 所示。8 s 后燃油滤堵塞引起燃油泵供流随时间线性下降,耦合性会使燃油实际输出相应减小到逐渐为 0,即能直观展现耦合故障的定量影响。

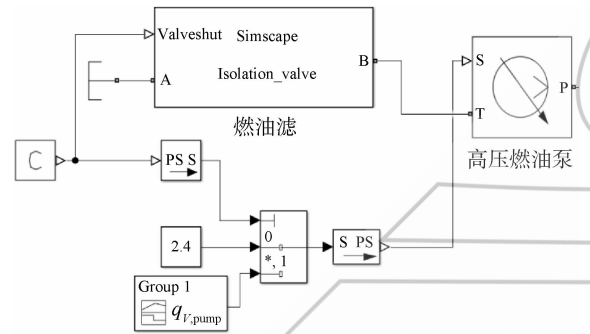


图 14 燃油滤堵塞与燃油泵供流能力下降耦合关系建模
Fig. 14 Modeling of the coupling between fuel filter blockage and fuel pump supply capacity decline

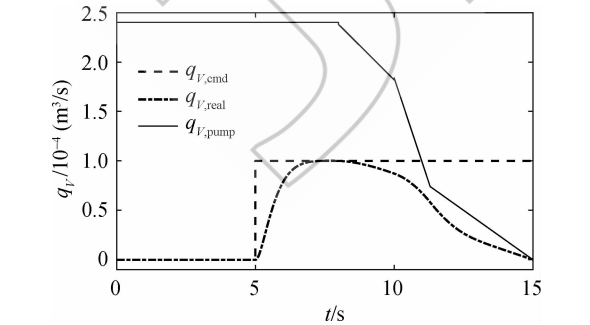


图 15 燃油滤堵塞导致燃油泵供流能力下降
Fig. 15 Fuel filter blockage leads to decline in the flow capacity of the fuel pump

3.2 高压关断阀门功能和燃油泵关断功能丧失故障的时序耦合影响分析

驾驶员启动燃油紧急关断指令,正常系统能实现燃油泵和燃油关断阀门都处于关闭,以保证

安全性。为探讨两者关断功能故障不同时序的耦合影响,对拓展模型建立不同时序的高压关断阀门和燃油泵关断功能丧失触发指令组合,如图 16 所示,0 表示关断功能丧失,1 表示功能正常。仿真结果如图 17 所示,当燃油泵关断功能丧失和高压关断阀门关闭功能丧失同时存在才会导致系统在关断指令下仍存在如期望油门指令的流量输出。

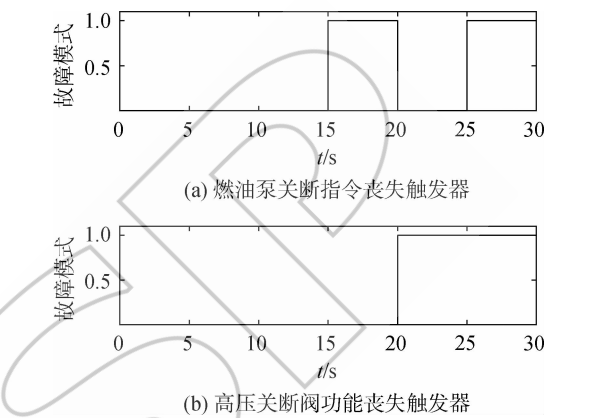


图 16 燃油泵关断和高压关断阀门功能丧失时序
Fig. 16 Different timing of fuel pump shut-off function and high-pressure shut-off valve function lost

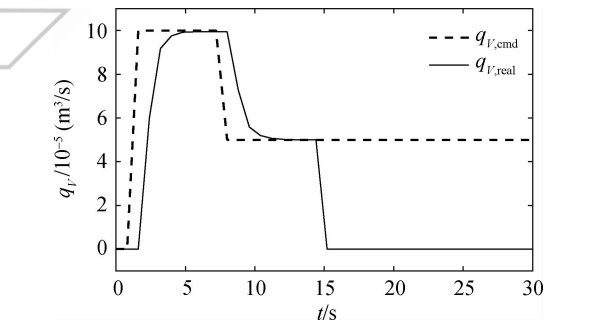


图 17 燃油泵关断和高压关断阀门关断功能丧失
时序耦合影响
Fig. 17 Timing coupling effects of fuel pump shut-off function and high-pressure valve shut-off function lost

在层级化的模型结构中,对于存在故障耦合情况,一般将耦合影响部分作为整体,不再细分耦合影响来源。例如,进行传统 FMEA 时,将故障影响层级定义在航空发动机燃油流量输出层级,FMEA 主要进行燃油滤堵塞和燃油泵供流能力下降这两种故障模式各自的故障影响分析,实则回避了两种故障模式的耦合关系,将燃油滤堵塞导致燃油泵供流能力下降的耦合部分处理成“黑

盒”,否则可能会导致分析层级混乱的问题。在 Simscape 等回路式模型结构中,可以对于液压、机械或其他系统普遍存在的故障耦合影响情况进行耦合关系建模,使得“黑盒”影响关系得以清晰展现。

4 结 论

MBSA 方法是处理航空发动机安全性分析中经常存在的时序、耦合影响的重要思路。本文利用 Simscape 提供的回路和时序表达的基本特征进行安全性分析扩展。分析故障模式形式化、故障拓展方式和故障时序性仿真等建模要素,构建基于 Simscape 的独立故障和耦合故障拓展方法。以 FADEC 主燃油控制子系统为物理对象,进行基于 Simscape 模型的独立和耦合故障安全性分析。得出的主要结论:

1) 在 Simscape 环境下,基于系统架构搭建的安全性分析模型对系统具有抽象度较低的直观表达,具有与实际系统拓扑结构上的相似性;相比于传统安全分析方法,该分析模型更接近基于物理特性的高精度系统设计仿真模型,便于系统安全分析阶段的安全性分析验证;且设计和安全性分析使用同一建模环境,易于保证设计和安全性分析的一致性。

2) 对于不同物理域的组件,Simscape 环境支持根据组件的物理模型自定义组件,使得独立故障和耦合故障拓展可根据故障在系统中的物理含义在组件内部建模语言中用数学关系考虑,从而可自定义故障拓展组件,使得基于 Simscape 环境进行故障拓展具有很大灵活性和定量性。

3) MBSA 方法中故障拓展形式化和仿真分析的自动化,以及分析结果的图形化,使其既能融合传统安全性分析方法,相比于传统 FMEA 和 FTA 方法又具有客观性、直观性和自动化高效率等优势。

本文为基于一定颗粒度下的设计系统细节和物理模型进行高度耦合的航空发动机系统安全性分析提供参考。

参考文献:

[1] US Federal Aviation Administration. Airworthiness standards Part-33:aircraft engines;14 CFR Part 33[S]. Washington DC:US Federal Aviation Administration,2016:46-47.
[2] European Aviation Safety Agency. Certification specifications for engines;CS-E Amendment-4[S]. Cologne, Germany:European Aviation Safety Agency,2003:44-46.

[3] 中国民用航空局.中国民用航空适航规章航空发动机适航标准:CCAR33-R2[S].北京:中国民用航空局,2011:40-43.
[4] WILKINSON P J,KELLY T P. Functional hazard analysis for highly integrated aerospace systems[C]// Proceedings of the IEE Seminar on Certification of Ground/Air Systems. London:IEEE Computer Society Press,1998:3-6.
[5] 张曙光,魏志远,夏双枝.面向适航的航空发动机非线性气动热力建模方法综述[J].航空动力学报,2018,33(12):2885-2899.
ZHANG Shuguang,WEI Zhiyuan,XIA Shuangzhi. Review on methods of aircraft engine nonlinear aerothermal-dynamic modeling for airworthiness requirement[J]. Journal of Aerospace Power,2018,33(12):2885-2899. (in Chinese)
[6] XU K,ZHU M,FAN Z,et al. FMEA of turbocharged diesel engine system using fuzzy inferencing[C]//Proceedings of Society of Automotive Engineers, New York:American Technical Publishers Limited Company,2000:529-535.
[7] US Federal Aviation Administration. Guidance material for 14 CFR § 33.75;AC33.75-1A,safety analysis[S]. Washington DC:US Federal Aviation Administration,2007:1-5.
[8] Society of Automotive Engineers International. Certification considerations for highly-integrated or complex aircraft systems:ARP4754A[S]. Warrendale:Society of Automotive Engineers,2010:1-12.
[9] Society of Automotive Engineers International. Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment; ARP4761[S]. Warrendale,US:Society of Automotive Engineers,1996:4-6.
[10] XU K. Fuzzy assessment of FMEA for engine system[J]. Reliability Engineering and System Safety,2002,75(1):17-29.
[11] ZAMMORI F,GABBRIELLI R. ANP/RPN:a multi criteria evaluation of the risk priority number[J]. Quality and Reliability Engineering International,2012,28(1):85-104.
[12] TEOH P C,CASE K. An evaluation of failure modes and effects analysis generation method for conceptual design [J]. International Journal of Computer Integrated Manufacturing,2005,18(4):279-293.
[13] LI G,GAO J M,CHEN F M. A novel approach for failure modes and effects analysis based on polychromatic sets [J]. Artificial Intelligence for Engineering Design, Analysis and Manufacturing,2009,23(2):119-129.
[14] NOH K W,JUN H B,LEE J H,et al. Module-based failure propagation (MFP) model for FMEA[J]. International Journal of Advanced Manufacturing Technology,2011,55(5/6/7/8):581-600.
[15] WANG Y. Development of a computer-aided fault tree synthesis methodology for quantitative risk analysis in the Chemical process industry[D]. Canyon, Texas, US: Texas A&M University,2004.
[16] VON AHSEN A. Cost-oriented failure mode and effects analysis[J]. International Journal of Quality and Reliability

Management,2008,25(5):466-476.

[17] JOSHI A,MILLER S P,WHALEN M W,et al. A proposal for model-based safety analysis[C] // Proceedings of 24th Digital Avionics Systems Conference. Washington DC:IEEE,2005:393-405.

[18] JOSHI A,HEIMDAHL M P,MILLERET S P,et al. Model-based safety analysis[R]. NASA/CR-2006-21353,2006.

[19] WANG J. ARP4761 民用机载系统安全性评估流程[EB/OL]. [2020-12-25]. <http://www.sae.org.cn/seminars/seminars/c1245.htm>.

[20] FENELON P,MCDERMID J A. An integrated tool set for software safety analysis[J]. Journal of Systems and Software,1993,21(3):279-290.

[21] LISAGOR O,KELLY T,NIU R. Model-based safety assessment;review of the discipline and its challenges[C]// 9th International Conference on Reliability,Maintainability and Safety (ICRMS). Guiyang,China:IEEE,2011:625-632.

[22] PROSVIRNOVA T,BATTEUX M,BRAMERET P A,et al. The altarica 3.0 project for model-based safety assessment[J]. IFAC Proceedings Volumes,2013,46(22):127-132.

[23] SCHALLERT C. Integrated safety and reliability analysis methods for aircraft system development using multi-domain object-oriented models[D]. Berlin:Technische Universität Berlin,2016.

[24] HOLT J,PERRY S. SysML for systems engineering[M]. London:Institution of Engineering and Technology,2008.

[25] SHAO Nian,ZHANG Shuguang,LIANG Hui,et al. Model-based safety analysis of a control system using Simulink and Simscape extended models[R]. Chengdu:MATEC Web of Conference,2017.

[26] 丁水汀,邱天,刘晓锋,等. 基于气动热力模型的 FADEC 系统 FHA 方法[J]. 航空动力学报,2012,27(5):1185-1193.

DING Shuiting, QIU Tian, LIU Xiaofeng, et al. FHA method for FADEC system based on aero-thermodynamics model[J]. Journal of Aerospace Power,2012,27(5):1185-1193. (in Chinese)

[27] GAN Chenyu, QIU Tian, DING Shuiting. Safety critical parameters of model-based safety analysis method for aero-engine[R]. ASME Paper GT2020-14671,2020.

[28] PETER F,DAVID G,JOHN M. An architecture-led safety analysis method[R]. Pittsburgh,US:Software Engineering Institute, Carnegie Mellon University, CMU/SEI-2016-TR-012,2016.

[29] FENELON P,MCDERMID J A,NICOLSON M,et al. Towards integrated safety analysis and design[J]. ACM SIGAPP Applied Computing Review,1994,2(1):21-32.

[30] 邵年. 基于 SIMSCAPE 模型的安全性分析方法研究[D]. 北京:北京航空航天大学,2018.

SHAO Nian. Research on safety analysis method using SIMSCAPE models [D]. Beijing: Beijing University of Aeronautics and Astronautics,2018. (in Chinese)

[31] 林克·迪辛格·安德瑞. 民用涡扇发动机系统[M]. 北京:航空工业出版社,2015.

(编辑:陈 越)