

基于模型的航空发动机系统安全性研究

鲍梦瑶^{1,2}, 李 果², 丁水汀²

(1. 中国民航管理干部学院 航空器适航审定系, 北京 100102;

2. 北京航空航天大学 能源与动力工程学院
航空发动机气动热力国家级重点实验室, 北京 100191)

摘 要: 在分析概括传统系统安全性分析的基础上,提出了一种基于模型的航空发动机系统安全性评估流程和分析方法,其从航空发动机系统自身特点出发,统一安全性分析和发动机性能设计模型,实现安全性设计和性能设计之间的平衡交互,以保证安全性分析结果的一致性、完整性和客观性。经概括,该流程方法所需突破的3个关键技术有:①失效模式的描述方法;②关键影响因素的分级和定位方法;③安全性分析验证方法。

关 键 词: 航空发动机; 适航; 系统安全性; 基于模型; 流程方法

中图分类号: V234.1

文献标志码: A

Research on model-based safety analysis for aero-engine

BAO Meng-yao^{1,2}, LI Guo², DING Shui-ting²

(1. Department of Aircraft Airworthiness Certification,

Civil Aviation Management Institute of China, Beijing 100102, China;

2. National Key Laboratory of Science and Technology on Aero-Engine Aero-thermodynamics,
School of Energy and Power Engineering,
Beijing University of Aeronautics and Astronautics, Beijing 100191, China)

Abstract: By introducing and summarizing the traditional safety analysis method, a model-based safety analysis process and method for aero-engine were proposed. From the property of the aero-engine, unified safety analysis and performance design achieved the goal of balance between them. This could guarantee the consistency, integrity and objective of the analysis results. The three key technical breakthroughs during the safety analysis process and method are: (1) the description method of failure modes; (2) the classification and location methods of the key impact factors; (3) safety analysis verification methods.

Key words: aero-engine; airworthiness; system safety; model-based; process and method

航空发动机是飞机的心脏,其安全性通过设计赋予、制造实现、验证表明、局方确认、维护保持来得以保障。随着航空发动机复杂程度的增高,对安全性分析方法的要求日益严苛^[1]。

世界各国适航当局以确保安全为目的颁布各类适航规章、审定规范,在世界先进航空发动机设

计国/制造国中:美国联邦航空局(FAA)颁布了FAR33《Airworthiness Standards: Aircraft Engines》^[2]、欧洲航空安全局(EASA)颁布了CS-E《Certification Specifications for Engines》^[3]。随着航空工业界国际化趋势的发展,国际合作研制发动机成为必然趋势,在这种背景下为减少适航

收稿日期:2015-07-21

基金项目:国家自然科学基金(61440034,51306008)

作者简介:鲍梦瑶(1985—),女,北京人,讲师,博士,主要从事民航适航技术及系统安全性方法研究。

审定方的审定难度和成本,提高审定效率,同时也为工业方建立发动机系统的通用设计和功能目标,FAA与EASA在有关发动机系统的适航审定、适航规章等方面已趋于统一.我国仿照FAR33颁布了中国民用航空规章CCAR33《航空发动机适航规定》^[4].在以上适航标准中,FAR33,CCAR33的§33.75条款及CS-E 510条款是专门针对发动机及其子系统安全性要求而提出的,明确指出在航空发动机设计阶段申请人必须对发动机及其控制系统进行安全分析,以确保航空发动机的安全水平.

然而,适航规章是一种法规条文,为表明适航规章某一条款的符合性,需要使用与之相对应的符合性方法来证明并向局方表明.所以,对于33.75条款中所明确要求进行的安全分析,需要在航空发动机研制过程中开展系统安全性评估流程和分析方法的研究,其对保证其设计和型号取证的顺利进行具有重要的理论意义和工程应用价值.

1 传统的航空发动机系统安全性评估流程及分析方法

1.1 传统的航空发动机系统安全性评估流程

20世纪七、八十年代,随着飞机及其机上系统复杂性日益增大,为了使适航部门和工业部门对安装在飞机上的复杂系统在适航审定工作上能有一个共同的工作基础,美国自动化工程协会(Society of Automotive Engineers, SAE)会同适航部门和工业方的专家形成工作组,该工作组包括了在大型商用飞机、支线飞机、航电系统、发动

机和发控系统的审定和设计方面有直接经验的人员,从适航审定符合性证明的角度对工业部门的系统开发流程与安全性评估流程和分析方法进行了总结,并于1996年形成了两部航空建议文件(Aerospace Recommended Practice, ARP):ARP 4754《高度综合或复杂飞机系统的审定考虑》^[5]和ARP 4761《民用机载系统和设备执行安全评估过程的指南和方法》^[6].

ARP 4754和ARP 4761均指出,尽管该文件最初为民用机载系统准备,但文件同样适用于飞机其他系统和相关适航规章,如发动机系统及其子系统和FAR33.因此,FAA与EASA于2005年先后在航空发动机安全性分析FAR 33.75/CS-E 510相关的咨询通告AC33.75^[1]/指导文件AMC E510^[3]中将上述文件作为指导文件,认可上述方法作为向局方表明航空发动机安全性的符合性方法,所以将飞机级系统安全性评估流程和分析方法引进到发动机系统安全性评估流程和分析方法中是可行的.

需要指出的是,ARP 4761和ARP 4754中均指出飞机级及其系统级安全性评估流程按工作内容和时间区段可分为功能危险分析(functional hazard assessment, FHA)、初步系统安全性分析(preliminary system safety assessment, PSSA)和系统安全性分析(system safety assessment, SSA)三个阶段.图1给出典型的发动机系统安全性评估一般流程“V”型顶层视图,可以看出评估流程涉及FHA, PSSA和SSA三个阶段.

在发动机研制的初期,首先对发动机级功能执行FHA,然后由设计过程将发动机级功能分配

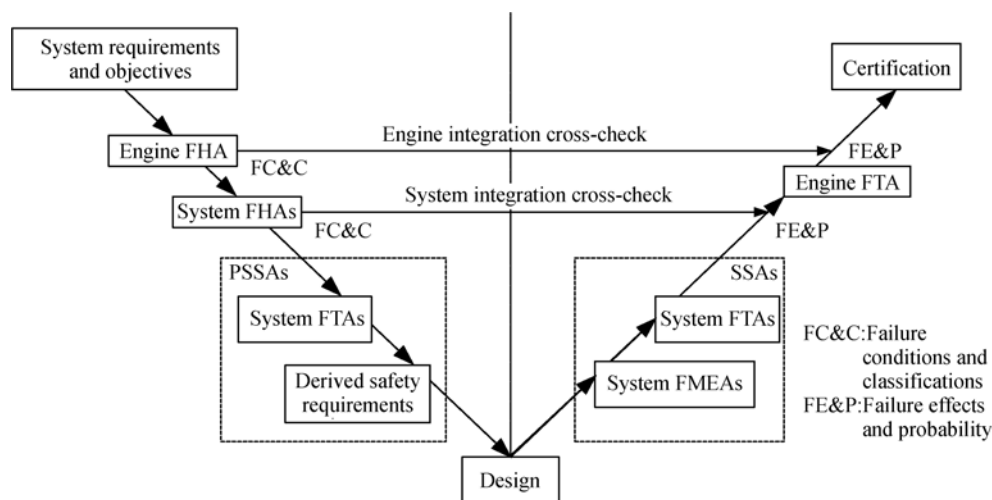


图1 传统的航空发动机系统安全性评估一般流程

Fig. 1 Traditional safety assessment process of aero-engine system

给各个系统后,由发动机级的安全性要求形成系统级的安全性要求,对各系统功能执行系统级FHA. FHA阶段的目的在于明确识别每一失效模式以及对其分类的基本理由,完成对系统架构的初步设计.

在系统架构初步设计完成后,对系统架构进行PSSA. PSSA阶段的目的是确定系统级FHA阶段予以识别的失效模式是如何引起的,并进一步导出安全保护措施,即为满足安全性目标可能需要的安全控制策略和架构特征(如:余度、非相似性、监控等),并在架构的约束下将对系统的安全性需求分解给软件和硬件. PSSA阶段与系统设计过程迭代进行,并随着系统设计过程的推进相应的对PSSA进行不断修订.

在SSA阶段,依照PSSA提出的要求将软件和硬件开发完成后,针对每一层级的PSSA阶段输出结果进行综合,直至最高层级的系统级SSA,其目的是去验证系统级所实施的设计措施满足从FHA得到的安全性目标和从PSSA得到的衍生安全性要求,并最终根据SSA的输出结果给出发动机级和系统级的安全性验证.

1.2 传统的航空发动机安全性分析方法

航空发动机系统安全性评估流程是与安全性分析方法紧密结合的,是以定性或定量分析为手段进行安全性分析以并表明对FAR/CCAR § 33.75条款要求的符合性. 目前,常用故障模式及影响分析(failure modes and effects analyses, FMEA)^[7]、故障树分析(fault tree analysis, FTA)^[8]和共因分析(common cause analysis, CCA)^[9-10]等.

2 传统航空发动机系统安全性评估的局限性

2.1 评估流程的局限性

尽管经过大量的工业实践证明,图1给出的“V”型系统安全性评估流程可以满足一般的安全性需要,但是将其按FHA阶段、PSSA阶段和SSA阶段对所涉及的具体发动机系统进行安全性分析时仍然存在一些问题.

在FHA阶段需要从发动机有效的需求文件中正确判断功能和其层级,FAR/CCAR § 33.75条款要求“为了评估预期可能发生的所有失效的后果,申请人必须对发动机及其控制系统进行安全性分析”. 发动机影响后果是相对于其对飞机级

影响而言的,且发动机的安全性分析包括发动机控制系统的安全性分析. 因此,若以其控制系统为例,Rolls Royce公司的Wilkinson和York大学的Dawkins等^[11-12]研究中指出,如为得到发动机控制系统某功能失效对飞机级的影响,首先要分析控制系统对相关功能子系统(比如燃油供油流量控制、尾喷管喉部面积控制、压气机放气活门面积控制等)的影响,然后分析这些子系统对发动机总体性能参数的综合影响,再分析单台发动机对于推进系统(对于多台发动机飞机)的影响,最后分析推进系统对飞机的影响. 可以看出:对于复杂系统,其分析过程是复杂的并且结果并不显而易见,若功能表述太抽象,则难以明确识别每一失效模式;若功能表述太详细,则FHA分析过程增长,随之产生大量无用信息,难以给出清晰的功能层级和范围来指引FHA过程. 究其原因,Xu等^[13-14]指出由于缺乏系统架构模型,导致发动机子系统/部件功能层级和功能范围的辨识困难.

此外,在PSSA阶段和SSA阶段需要辨识出发动机及其系统每一层级所有可能的失效模式和失效影响,但Xu等^[13-14]指出由于发动机和其子系统之间存在着气动连接,决定了其在反应上的滞后性,这种复杂联系造成失效模式之间、失效模式和失效影响因素之间相互耦合(如图2和图3所示);并且,Dawkins等^[12]指出对于复杂系统,如果将基于架构和关联关系不清楚情况下的FHA分析结果在PSSA阶段和SSA阶段进行使用,分析结果的可用性会存在较大问题;同时,功能之间的错综关系也带来对失效影响的难以直接判断和预料,造成PSSA阶段和SAA阶段的分析困难.

因此,Wilkinson等^[11]指出传统的系统安全性评估流程(FHA,PSSA和SSA)在应用时更适合对功能相对简单且独立的系统进行分析. 对航空发动机这类,具有高度复杂性且综合的系统在进行分析时存在诸多困难、且容易导致分析结果的不正确. 为解决上述问题,Wilkinson等^[11]建议采用建立“影响环”的方式,以求对发动机系统的各个功能及其之间的关系有充分的了解. 但由于影响环是部件模型示意图,因此只能看出各功能模块之间的定性关系,并不能分析功能模块参数的定量影响.

2.2 分析方法的局限性

传统航空发动机安全性分析其基础概念是将单独的重要和危害性发动机风险控制到可以接受

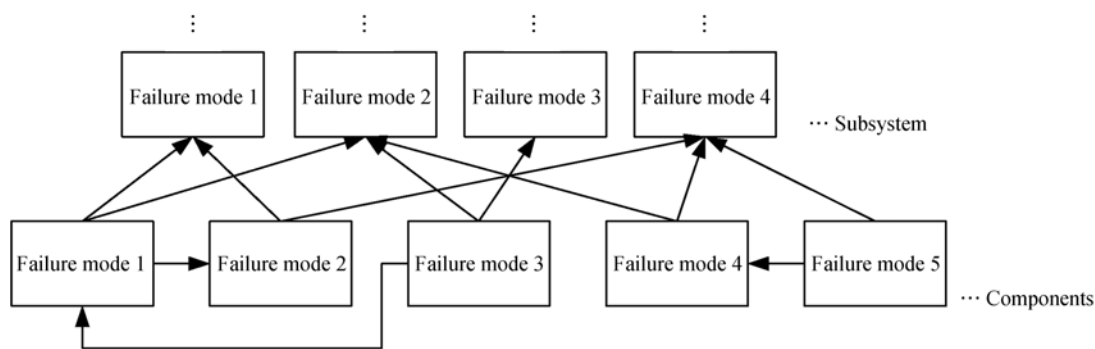


图 2 不同层级间的失效模式耦合关系示意图

Fig. 2 Schematic of coupling relationship of failure mode between different levels

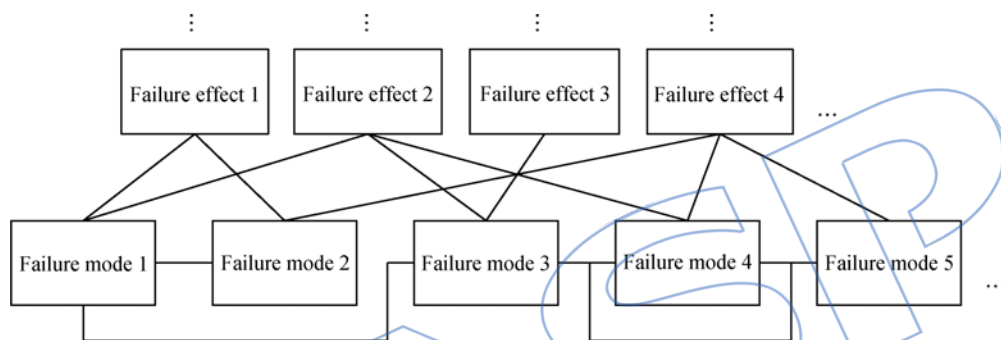


图 3 失效模式和失效影响因素间的耦合关系示意图

Fig. 3 Schematic of coupling relationship between failure mode and failure effect

的水平,从而使总体发动机设计风险可以接受^[1,3],主要采用 FTA, FMEA 对孤立分系统或者部件进行安全性分析.但随着航空发动机复杂程度的增长,其整体性、耦合性逐渐显现出来.因此, Fenelon 等^[15]指出分析时还需考虑由于系统综合引起的相互耦合关系.

但在采用 FTA, FMEA 进行系统耦合关系建模时,由于这些方法是基于自然 (informal) 语言的形式描述,在缺乏系统架构模型的情况下易导致以下两方面的问题:

1) Xu 等^[13-14]指出复杂系统往往具有多层级或多部件, FMEA 对失效模式、失效影响的描述范围可能过大或过小、过重或过轻,难以描述其间的耦合关系,分析结果易偏离实际.

2) Wang 等^[16]指出 FTA 依赖于安全性分析人员的个人经验并具有高度的主观性,即使针对同一系统不同人员所建立的 FTA 模型也可能有所不同,且由于 FTA 本身的重用能力较差,在 PSSA 阶段即使更改设计架构非常小的部分,整个 FTA 也经常需要重新检查,造成其对于复杂系统的全面验证该“顺序化”分析高昂的设计成

本,同时给实际应用带来很大困难.

从 2.1 章节和 2.2 章节分析可见,将现有评估流程和分析手段直接应用于实际的发动机系统或者其中一些较低层级的复杂子系统的安全性评估流程中时,存在应用上的一些问题和困难.究其原因 Lisagor 等^[17]、Joshi 等^[18-19]指出:在实际分析复杂系统时,由于缺乏对系统架构模型,其本身的复杂性往往会导致安全性工程师对系统架构和失效模式缺乏了解、难以判断,使得安全性工程师不得不耗费大量精力和时间从不同的地方搜集系统架构的细节,仍很难采用传统安全性评估流程和分析方法对系统进行描述和建模,分析结果更无法做到完整、一致,进而难以满足日益增长的安全性需求.

3 基于模型的系统安全性评估流程和分析方法

为克服第 2 章节所述传统安全性评估流程和分析方法处理复杂系统时的局限性,基于模型的系统安全性分析方法被发展出来,即应当将研究对象的系统模型引入到安全性评估流程中. Mi-

chael 等^[20], Berry^[21] 和 Hinchey 等^[22] 也在其研究中明确指出,随着基于模型技术的发展以及各种形式化验证工具的不断成熟,基于模型的系统安全性分析方法可不断应用于高安全苛求的复杂系统的开发,并有效弥补 FTA, FMEA 等方法的不足。

本章节将从 3 个方面论述基于模型的系统安全性分析方法,即基于模型的开发过程、基于模型的系统安全性分析以及形式化方法。

3.1 基于模型的开发过程

基于模型的开发过程(model-based development, MBD)是构建对系统架构模型的过程,即依靠数学模型和仿真进行的一种设计方式,可以在开发过程中的任何阶段通过仿真对系统进行测试和验证^[23]。将基于模型的开发过程与传统开发过程进行对比^[24],如图 4 所示,可以看出,基于模型的开发过程简化了传统开发过程的步骤,且很大一部分开发工作依靠系统的同一个模型将设计、实施和测试步骤结合起来,从而有效缩短了开发周期;并且使用该模型,可以采用模型检验方法进行多种分析,如:系统仿真、完整性和一致性分析等^[25]。

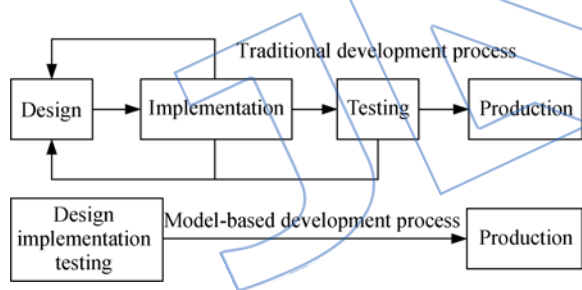


图 4 传统的开发过程与基于模型的开发过程对比

Fig. 4 Compare with traditional development process and model-based development process

3.2 基于模型的安全性分析

基于模型的系统安全性分析的实质是基于模型的开发过程与安全性分析领域的结合。2005 年,由明尼苏达大学计算机科学与工程学院的 Joshi 和 Heimdahl 与罗克韦尔柯林斯先进技术中心的 Miller 和 Whalen 共同研究,将基于模型的开发过程引入到 ARP4761 所述的系统安全性评估流程中,提出了一种基于模型的安全性分析(model-based safety analysis, MBSA)^[18-19]。

2006 年, Joshi 等^[18] 在 NASA 报告中进一步具体的说明了基于模型的系统安全性评估流程和分析方法的基本思想,给出了基于模型的系统安

全性评估流程与传统的系统安全性评估流程进行对比,如图 5 所示。

从图 5 可以看出,基于模型的系统安全性评估流程沿用了传统的系统安全性评估流程,但在分析模型的基础上与其他方法相结合。该分析的基本思想是:通过系统模型和形式化方法,验证系统模型在正常情况和失效情况下是否满足安全性要求,其基本步骤包括:建立标准模型(正常情况下系统模型)、确定失效模式,建立扩展模型(失效情况下系统模型)、安全性分析。这种系统安全分析的途径,使设计人员及安全性分析人员使用共同的系统模型,而通过加入故障模式来扩展系统模型,为安全性分析提供了很大帮助。由于设计人员及安全性分析人员使用共同的系统模型,所以在降低开销的同时,提高了安全性分析的质量。

最终,报告以 ARP4761 刹车系统为例说明,采用 Matlab/Simulink 对刹车控制系统建模,在此基础上将 Matlab/Simulink 模型联立 SCADE (safety-critical application development environment) 的模型检验器中验证系统安全属性,即验证所有机轮刹车都失效的概率小于 5×10^{-7} 每次飞行的安全性要求。分析结果表明:这种引入模型的分析方法可以更好地利用设计过程中的系统信息,使设计人员及安全性分析人员工作于一个共同的系统模型,有效避免了设计与安全评价转换的不确定因素,从而减少对分析人员经验的依赖。

3.3 形式化验证方法

基于模型的系统安全性分析自 2005 年出现后被许多航空航天机构不断研究和应用^[26-27],主要是在模型基础上对系统安全性是否满足安全性要求进行验证,其研究对象大多数集中于机载控制系统软件部分,并具体采用了形式化验证方法(formal method, FM)中的模型检验法(model checking, MC)。通常采用该方法进行安全性分析时,模型检验的输入应分别是待检测的软件系统模型和用于安全性分析的安全是违反安全属性的反例^[28]。其优点是模型检验利用遍历算法:一方面,可以从数学上保证搜索出系统的所有状态,降低安全隐患;另一方面,可以利用计算机检验工具,实现自动分析过程,减少人为主观判断导致的分析错误。

正是因为以上优点,2013 年 7 月 19 日, FAA 颁布 AC 20-115C 正式确定机载系统和设备的软件开发和适航审定可以采用 DO-333 形式化验证方法和 DO-331 基于模型的开发过程等方法作为

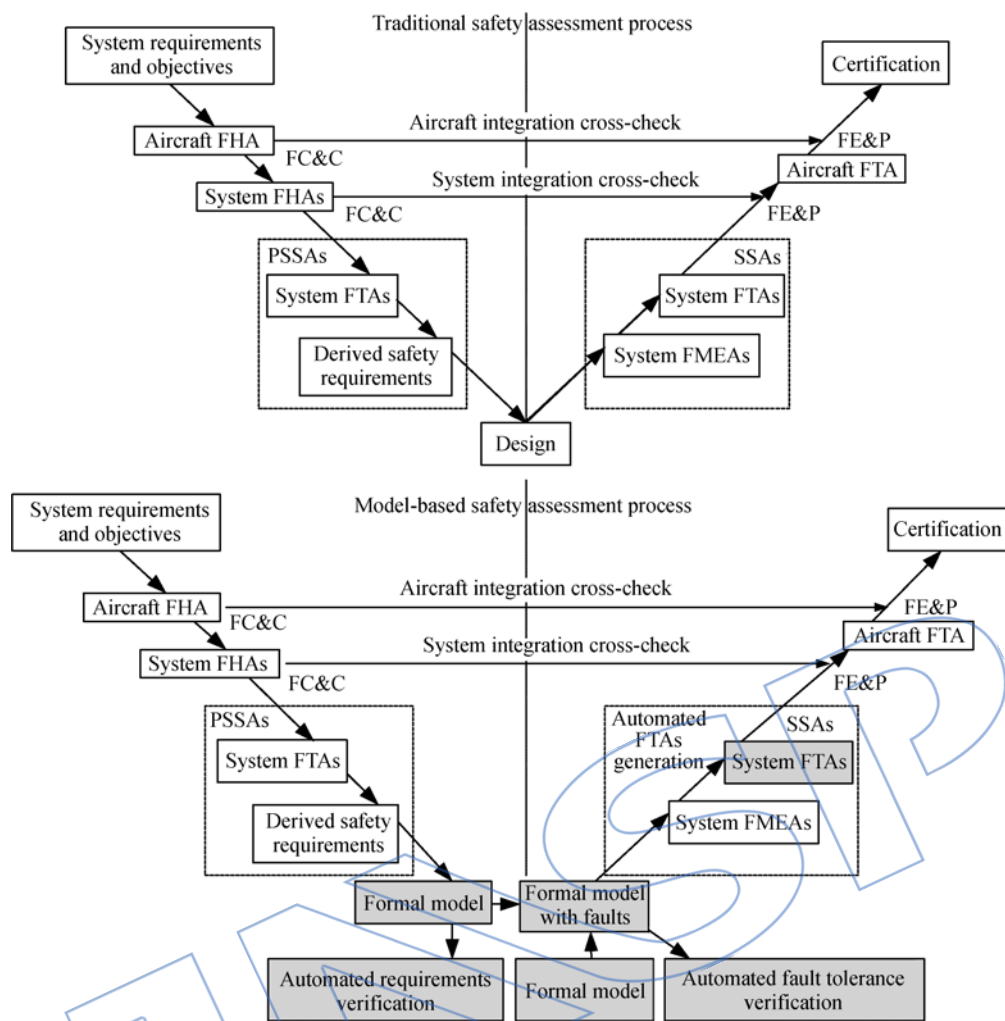


图 5 传统的系统安全性评估流程与基于模型的系统安全性评估流程对比

Fig. 5 Comparison of traditional system safety assessment process and model-based system safety assessment process

FAA 可接受的符合性验证方法并逐渐被实际工程应用^[29].

4 基于模型的航空发动机系统安全性评估流程和分析方法

通过第 3 章节的详细论述,可以看出现阶段基于模型的系统安全性分析方法主要集中在机载控制系统,且现有研究仍处于底层的部分软件系统,较少涉及整机系统,尚鲜见在航空发动机系统上的应用.

但从 ARP 4754 和 ARP 4761 的推荐(如 1.1 章节所述),并且从该方法的逻辑架构(如第 3 章节所述)来分析,基于模型的系统安全性评估流程和分析方法,为处理由于缺乏分析对象的系统架构模型而导致的发动机系统安全性问题分析困难,提供了一条有效途径.即,在发动机系统安全性问题中:通过模型参数化表达,可以建立系统

及部件的失效模式和安全边界,进而实现系统安全性分析的定量表达;同时,该系统模型也能够一定程度上反映失效模式之间的耦合关系,克服传统安全性分析方法的局限性.然而,该方法目前对系统的故障模式和作用在故障模式上的影响因素缺乏深入研究.所以,基于模型的系统安全性方法应用于航空发动机是可行的,但仍需进一步发展.

因此,在借鉴 ARP4761 所述系统安全性评估流程的基础上,本文作者将现有基于模型的安全性分析思想引入航空发动机系统安全性分析领域并将其发展,探索形成一种基于模型的发动机系统安全性评估流程;并在此基础上,给出所对应的基于模型的发动机系统安全性分析方法.

4.1 基于模型的航空发动机系统安全性评估流程

基于模型的航空发动机系统安全性评估流

程,通过保证性能设计和安全性所用模型的统一,将安全性分析贯穿整个性能设计流程并保证实时交互,从而实现性能和安全的同步平衡设计.图6给出了典型的基于模型的发动机及其系统安全性评估流程示意图.

从图6中可以看出,与图1中传统的系统安全性评估流程相比,在原“V”型评估流程的基础上,引入的模型开发过程中所涉及的系统模型与系统安全性评估及设计流程之间存在交互作用,以保证开发过程中的任何阶段对系统进行测试、分析和验证.而存在的这种交互作用,就要求在交互方式上建立起有效的框架,其可以从流程结构和交互对象两个方面加以描述.

在流程结构上,作为一种通用分析方法及工具,模型可以被应用到系统安全性分析及设计的各个具体流程,包括FHA阶段、PSSA阶段和SSA阶段.对于本文研究中所针对的航空发动机级FHA的目的是明确每个失效状态以及其严重性的分类理由,其输出是将其失效状态的原因分解到起作用的子系统的失效模式,作为子系统FHA的输入.对于PSSA阶段,由于其目的是确定FHA阶段予以识别的失效模式是如何引起的,因此在PSSA阶段应使用模型来分析那些对FHA阶段被识别出的失效模式可能起作用的影响因素,将这些影响因素进行分解和参数化表达,并进一步导出安全保护措施(如:余度、非相似性、监控等).最终在SSA阶段,将PSSA阶段输出的结果进行综合,验证系统所实施的设计是否满足硬件和软件的安全性要求.

在交互对象上,模型与其他分析方法(如:对应分析)紧密结合.其中,针对子系统级FHA阶段识别的失效状态可首先通过模型实际输出的系统运行工作边界与设定的系统运行安全边界进行比较后判断获得;然后,在PSSA阶段当模型输出被判断为失效时,采用分析的方法识别出导致这种失效模式的可能的影响因素,进而确定该失效模式(顶事件)下不同影响因素(底事件)的重要程度并给出相应的安全保护措施,以辅助系统设计的改进;最后,通过对所实施的设计进行安全性验证,包括依据FHA阶段和PSSA阶段所定义的失效模式和影响因素进行定量分析以得出失效概率和依据PSSA阶段衍生出的软件系统关键逻辑部分安全性要求进行模型检验.

从以上分析可以看出,基于模型的发动机系统安全性评估流程与传统的ARP4761系统安全性方法最大的不同在于:①在描述方法上,基于模型的系统安全性分析方法包含与开发过程同步的发动机系统模型,从而可以将FHA阶段识别出的失效模式进行具体的、客观的参数化(formal)描述,以更全面的反映出产生失效的影响因素间的耦合作用;②在数据要求上,基于模型的发动机系统安全性分析方法,通过模型计算对发动机和系统间的各种结构参数和性能指标建立起对应关系,避免人为主观经验判断,同时节省大量的中间试验环节,降低确保安全性要求所需的成本.

4.2 基于模型的航空发动机系统安全性分析方法

针对基于模型的航空发动机系统安全性评估

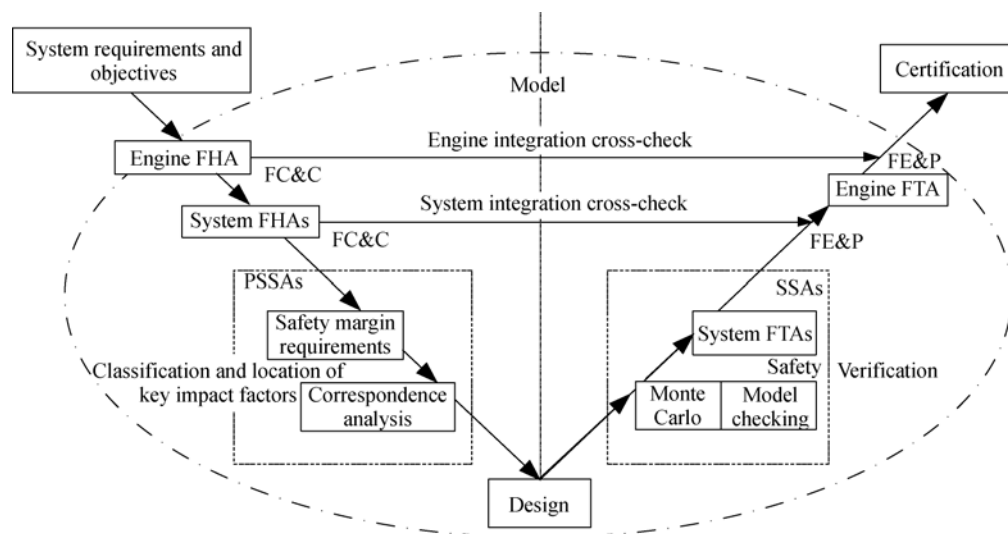


图6 基于模型的航空发动机系统安全性评估流程

Fig. 6 Model-based system safety assessment process of aero-engine system

流程的特点,其对应的系统安全性分析方法中所需突破的关键技术有:①失效模式的工作边界与安全边界描述方法,即将航空发动机系统失效模式参数化表达后,通过工作边界与安全边界的包容关系对失效进行判断;②作用在失效模式上的影响因素的分级和定位方法;③安全性分析验证方法,即通过蒙特卡洛法与模型检验法,分别给出整个系统定量的安全性水平以及软件的关键逻辑部分定性的安全性水平.以上所述的关键技术也同时对应于基于模型的航空发动机系统安全性评估流程的 FHA 阶段、PSSA 阶段和 SSA 阶段.本章节将逐一进行分析.

4.2.1 失效模式的工作边界与安全边界描述方法

对于航空发动机系统,在 FHA 阶段需明晰其工作边界和安全边界,所以本章节将从发动机级的工作边界和安全边界的角度加以阐述.

1) 失效模式的工作边界

对于航空发动机系统安全性,其系统安全是指各个子系统结合在一起时的整个系统的最佳安全性状态,而不是通过某个子系统的最佳安全状态而得到满足^[30],即通过考虑系统的输入、输出和系统模型这三者之间的关系,确保系统的安全性,如图 7 所示.当一组信息输入系统时,若存在可能造成系统发生危险的各种影响因素,系统对其反映的综合结果可以通过输出表现出来.这时系统状态存在 3 种可能性:①无危险发生,系统安全运行;②有危险发生,但是得到控制和排除,系统安全运行;③可能有一个或者几个危险发生,至少有一个危险没有得到控制,导致系统处于不安全状态(事故征候),最终导致系统失效、甚至事故的发生.所以,由于系统模型的输出可以反映系统运行状态,而系统运行工作状态可通过其工作区域表征,该工作区域的边界即为系统运行工作边界(以下简称工作边界).

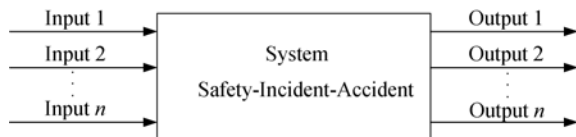


图 7 开放型系统(安全-事故转换图)

Fig. 7 Open systems (transformation between safety and accident)

2) 失效模式的安全边界

通常而言的安全边界是对失效模式(顶事件)的一种约束限制,是研究对象能够安全工作的参

数最大容许范围.在数学模型上可反映为顶事件不发生情况下的功能特征值或安全可行域的参数化表达^[31].

按照上文所述的基于模型的航空发动机系统安全性评估流程,发动机子系统的安全性也必须从整个系统的角度进行研究,因此在 FHA 阶段需明晰发动机级安全性要求,且所涉及的每个层级的安全性要求可以分别通过发动机系统安全边界来表征,即由发动机运行的安全边界首先分析出安全工作状态下所要求的工作参数的最大容许范围,然后在此基础上下达子系统级安全边界要求,从而确保子系统与整机匹配的安全性.

3) 失效模式的边界判断

在系统工作边界和安全边界确定以后,即可以在 FHA 阶段通过安全边界与工作边界的包容关系判断系统是否失效(非独立的单一顶事件).而参照 ARP4761 的要求,可以在 PSSA 阶段使用模型对 FHA 阶段予以识别的失效模式(边界判断为失效情况)上可能的影响因素进行分析(对应分析法).

在基于模型的航空发动机系统安全性分析中,失效与边界的关系如图 8 所示.图中 p_c 表示增压压力, G_c 表示空气流量.以某发动机增压系统举例来说,其分别由压气机喘振线(surge line)、涡轮允许最高温度线 $T_{\max}$ 、增压器所允许的最高转速线 $n_{c\max}$ 、发动机的最小稳定转速线 $n_{\min}$ 和发动机标定转速线 n_c 组成. E_0, E_1, E_2, E_3 代表不同工况下,系统运行工作边界上的状态点.若点 E_1 从安全区域运行到在安全边界上的点 E_2 位置时,系统表现为正常运行但存在安全隐患;若点 E_2 从安全边界上运行到安全边界以外的不安全区域中点 E_3 位置时,系统不能再正常运行,可表现为单一失效甚至耦合失效模式.即,可通过工

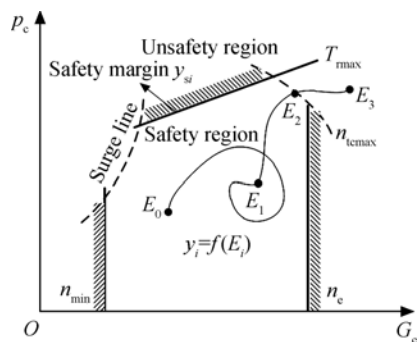


图 8 失效模式的边界判断

Fig. 8 Boundary judgment for failure model

作边界与安全边界的包容关系对失效进行判断。

因此,不妨设代表失效模式约束限制的安全边界为 $y_{sm}(m=1,2,\dots,n)$,代表系统运行状态的工作边界为 $y_{om}(m=1,2,\dots,n)$ 。其中,针对每一个安全边界 y_{sm} 和工作边界 y_{om} , $G(E)$ 是判断其失效模式的工作边界安全裕度所对应的系统极限状态函数,且各个工作边界安全裕度可以通过一组系统极限状态函数来加以表示

$$G(E) = \frac{y_{sm} y_{om}}{y_{sm}}$$

其中当 $G(E) < 0$ 时,说明系统运行在安全边界以外,即不安全区域时,则可认为是不安全的工作状态;当 $G(E) = 0$ 或 $G(E) > 0$ 时,说明系统运行在安全边界上或安全区域内,则认为是安全的工作状态。

需要指出的是:依据上述方法,在 FHA 阶段识别对系统功能有影响的所有可能的失效模式后,不需要对所有的失效模式进行同等细致度的安全性分析,而是针对失效模式的影响程度进行筛选。通常,若危害度被识别为“灾难性的(catastrophic)”或“危险的(hazardous)”,则需要在 PSSA 阶段采用模型对其影响因素进行辨识和分解,并在 SSA 阶段给出定性和定量的安全性验证;若危害度被识别“重大的(major)”且系统复杂程度较低,则可结合已有经验进行定性分析;若危害度属于“较小的(minor)”则可通过 FHA 分析报告进行说明。

4.2.2 影响因素的分级和定位方法

在系统级 FHA 阶段的失效模式确定后, PSSA 阶段需要使用模型对作用在失效模式上可能的影响因素进行分析。即一方面,需要确定失效模式与影响因素的相关程度,进行影响因素重要程度的。另一方面还需要根据观测的系统异常数据,对引起系统行为异常或偏离正常情况的可能的影响因素进行快速定位。通过影响因素的分级和定位给出相应的安全控制策略。

一般而言,模型参数可分为设计可控参数和设计不可控参数,如图 9 所示^[32]。图中 $X_1, X_2, \dots, X_p$ 表示设计可控参数,如系统几何结构参数; $Y_1, Y_2, \dots, Y_p$ 表示设计不可控参数,如人为因素、偶发因素等。对于设计不可控参数,可将其视为模型固定约束,即在设计和使用过程中无法对其控制改变。所以,应将设计可控参数作为安全控制手段,即选择模型中的设计可控参数作为关键影响因素的分析对象,并为达到可接受的安全

性要求,对模型参数进行约束和控制,以使系统工作边界处于安全边界以内。

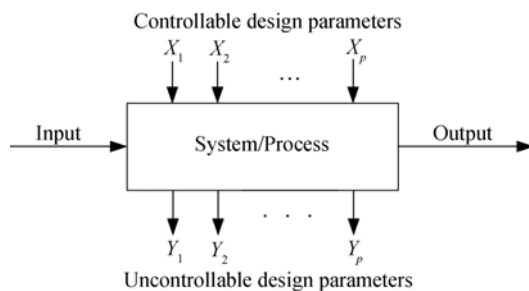


图9 设计可控参数及设计不可控参数示意图

Fig. 9 Schematic of controllable and uncontrollable design parameters

由于航空发动机系统属于连续非线性系统,且其失效模式与影响因素间存在连续型的定距数据关系(如,发动机转速变化与涡轮前温度变化的关系),所以在 PSSA 阶段传统安全性分析方法(如 FMEA 的表形结构,FTA 的线性树形结构)难以解决发动机与系统间的复杂联系造成的失效模式间、影响因素间的耦合关系,也很难直观的揭示失效模式和影响因素之间的联系。因此,为了一方面解决失效模式间及影响因素间的多重耦合问题,另一方面直观的揭示出失效模式和影响因素之间的关系,以便实现对关键影响因素的分级和定位,实际分析中可以引入改进的“对应分析法”到基于模型的安全性评估流程中,进行对作用在失效模式上的影响因素分级和定位的分析,作为一种对失效模式和影响因素分析的安全性方法。

4.2.3 安全性分析验证方法

在完成 PSSA 阶段的影响因素的分级、定位和导出相应的安全保护措施后, SSA 阶段将 PSSA 阶段输出的结果进行综合,并通过验证的手段表明系统符合安全性要求或安全性水平有所提高。针对航空发动机系统,应在 SSA 阶段通过分析的手段以表明其符合安全性要求或安全性水平有所提高。实际分析中可以分别引入“蒙特卡洛法”定量的评估系统设计变化(如:采用安全控制策略前后)系统失效模式及概率的差异,以判断安全控制策略的有效性;引入“模型检验法”定性的对控制系统软件逻辑部分进行建模分析,并判断该部分是否具有处理异常情况输入的能力。

5 结 论

本文研究直接针对我国航空发动机研制所遇

到的安全性问题,详细介绍了传统的安全性分析方法及其局限性,概述了一种基于模型的系统安全性评估流程和分析方法,从而为我国未来的军民航空发动机安全性设计和安全性验证工作提供研究基础和技术积累。

综合上述概述和其他相关资料可以得出以下结论:

1) 为保证航空发动机安全性需求,在研制过程中开展系统安全性评估流程和分析方法是现阶段国际上公认的较为有效的途径之一,但我国的系统安全性分析尚处于起步阶段。

2) 国际上通常使用的,将源于民用飞机的系统安全性评估流程直接运用到航空发动机这一复杂系统上时存在较大难度和制约:评估流程上由于缺乏系统架构模型造成子系统/部件功能层级和功能范围辨识困难;分析方法上由于传统的安全性分析依赖于安全性工程师的个人经验并具有高度的主观性,导致分析结果无法保证完整性、一致性;难以分解失效模式间及影响因素间的复杂双重耦合关系。

3) 为克服上述局限性,将基于模型的安全性分析思想引入到航空发动机系统安全性分析领域并将其发展,从而形成了基于模型的航空发动机系统安全性评估流程和分析方法,可以实现在系统架构发展的同时,统一模型的实时更新,且保证在系统开发设计的初期即实现系统安全性分析的客观同步进行。

基于模型的航空发动机系统安全性评估流程和分析方法所需突破的关键技术有:①航空发动机系统失效模式的参数化表达;②关键影响因素的分级和定位方法;③安全性分析验证方法。

参考文献:

- [1] U. S. Department of Transportation Federal Aviation Administration. AC 33.75-1A Guidance material for 14 CFR § 33.75, safety analysis[S]. Washington, America: Federal Aviation Administration, 2007:1-5.
- [2] U. S. Department of Transportation Federal Aviation Administration. FAR33 The United States code of federal regulations, title 14, aeronautics and space; Part 33 airworthiness standards; aircraft engines[S]. Washington, America: Federal Aviation Administration, 2009:1-5.
- [3] Certification Specifications Group. CS-E510 Certification specifications for engines [S]. Cologne, Germany: European Aviation Safety Agency, 2003:1-6.
- [4] 中国民用航空总局. CCAR33 中国民用航空适航规章第33部 R2 版, 航空发动机适航标准[S]. 北京: 中国民用航空总局, 2011:1-2.
- [5] Society of Automotive Engineers International. ARP 4754 Certification considerations for highly-integrated or complex aircraft systems[S]. Warrendale: Society of Automotive Engineers, 1996:1-12.
- [6] Society of Automotive Engineers International. ARP 4761 Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment[S]. Warrendale: Society of Automotive Engineers, 1996:4-6.
- [7] McDermott R E, Mikulak R J, Beauregard M R. The basics of FMEA[M]. Boca Raton: CRC Press, 1996.
- [8] Bruns G, Anderson S. Validating safety models with fault trees. [C]// Proceedings of 12th International Conference on Computer Safety, Reliability, and Security. Edinburgh: Springer-Verlag, 1993:21-30.
- [9] Schellhorn G, Ortmeier F, Reif W. Formal safety analysis of a radio-based railroad crossing using deductive cause-consequence analysis (DCCA) [C]// Proceedings of the 5th European conference on Dependable Computing. Hungary: Springer-Verlag, 2005:20-22.
- [10] Aftab A H, Aamer N. A survey of safety analysis techniques for safety critical systems[J]. International Journal of Future Computer and Communication, 2013, 2(2): 134-137.
- [11] 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.
- [12] Dawkins S K, Kelly T P, McDermid J A, et al. Issues in the conduct of PSSA[C]// Proceedings of the 17th International System Safety Conference (ISSC). New York: System Safety Society, 1999:77-86.
- [13] 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.
- [14] Xu K. Fuzzy assessment of FMEA for engine system[J]. Reliability Engineering & System Safety, 2002, 75(1): 17-29.
- [15] Fenelon P, McDermid J A, Nicholson M, et al. Towards integrated safety analysis and design [EB/OL]. [2013-09-24.]. <http://www-users.cs.york.ac.uk/~djp/publications/djp-acm.pdf>.
- [16] Wang Y. Development of a computer-aided fault tree synthesis methodology for quantitative risk analysis in the chemical process industry[D]. Texas: Texas A&M University, 2004.
- [17] Lisagor O, McDermid J A, Pumfrey D J. Towards a practicable process for automated safety analysis[C]// Proceedings of the 24th International System Safety Conference. New York: System Safety Society, 2006:596-607.
- [18] Joshi A, Miller S P, Whalen M W, et al. A proposal for model-based safety analysis[C]// Proceedings of the 24th

- Digital Avionics Systems Conference. New York: Springer-Verlag, 2005: 393-405.
- [19] Joshi A, Whalen M W., Heimdahl M P. Model-based safety analysis final report [EB/OL]. [2013-09-24]. <http://shemesh.larc.nasa.gov/fm/papers/Joshi-CR-2006-213953-Model-Based-SA.pdf>.
- [20] Michael W W, Darren D C, Steven P M, et al. Integration of formal analysis into a model-based software development process[C]// Proceedings of the 12th International Workshop on Industrial Critical Systems. Berlin: Springer-Verlag, 2007: 68-84.
- [21] Berry G. Synchronous design and verification of critical embedded systems using SCADE and Esterel[C]// Proceedings of the 12th International Conference on Formal Methods for Industrial Critical Systems. Berlin: Springer-Verlag, 2007: 1-2.
- [22] Hinchey M G, Bowen J. P. Industrial strength formal methods in practice[M]. London: Springer-Verlag, 1999.
- [23] Jackson D, Tannenbaum B, Jachimczyk W, et. al. Adoption, impact, and vision of model-based design[C]// Proceedings of the International Society for Optical Engineering. Natick: International Society for Optical Engineering, 2006: 12-17.
- [24] Ahmadian M, Nazari Z J, Nakhaee N, et al. Model based design and SDR[C]// Proceedings of the 2nd IEE/EUR-ASIP Conference on DSP Enabled Radio. Southampton: Institution of Electrical Engineers, 2005: 19-25.
- [25] Miller S, Heimdahl M P, Tribble A C. Proving the shalls [J]. International Journal on Software Tools for Technology, 2006, 8(4/5): 303-319.
- [26] Bozzano M. ESACS: An integrated methodology for design and safety analysis of complex systems[C]// Proceedings of the European Safety and Reliability Conference. Maas-tricht: Balkema Publishers, 2003: 237-245.
- [27] Akerlund O, Bieber P, Boede E, et al. ISAAC, A framework for integrated safety analysis of functional, geometrical and human aspects[C]// Proceedings of Electronic Reciprocal Transfer System. Toulouse, France: Tagungs-beitrag, 2006: 145-162.
- [28] Edmund M C, Grumberg O, Doron A. Model checking [M]. Cambridge: Massachusetts Institute of Technology Press, 1999.
- [29] U. S. Department of Transportation Federal Aviation Administration. AC 20-115C Airborne software assurance [S]. Washington, America: Federal Aviation Administration, 2013: 1-3.
- [30] Akerlund, O, Nadjm-Tehrani S, Stalmarck G. Integration of formal methods into system safety and reliability analysis[C]// Proceedings of 17th International System Safety Conference. New York: System Safety Society, 1999: 326-336.
- [31] Badreddin E, Abdel-gelil M. Dynamic safety margin principle and application in control of safety critical systems [C]// Proceedings of IEEE International Conference. Taiwan: IEEE Computer Society Press, 2004: 689-694.
- [32] 张根保, 何桢, 刘英. 质量管理与可靠性[M]. 北京: 中国科学技术出版社, 2005.

(编辑: 王碧琚)