基于架构设计的新研航空发动机系统安全性评估方法研究与应用

Research and Application of System Safety Assessment Method for New Researched Aero Engine Based on Architecture Design

卢婷婷 韩冰 / 中国航发商用航空发动机有限责任公司

航空发动机的安全性是通过全生命周期的设计、评估、验证等活动赋予的，是一种产品的基本特性，更是产品制造商赖以生存的基本保证。通过科学、有效的安全性分析与评估，可识别产品运营阶段潜在的安全性风险，针对捕获的风险开展原因分析、风险控制并制定措施，开展有效性评估与验证，可以从源头提升产品的安全性水平，为产品的研发成功与市场成功保驾护航。

在民用飞机产品研制的全生命周期中，安全性设计、分析、评估与验证技术是研制的重点与难点，技术方法本身的正确性、适用性以及应用的科学性和有效性直接影响产品的安全性评估水平，进而对民用飞机产品项目研发成功、适航成功以及市场胜利产生重要影响[1]。为了攻克民用飞机产品安全性设计与评估的困难，国外标杆企业基于多年项目技术沉淀与产品运营经验，总结形成了《民用飞机和系统研制指南》（SAE ARP 4754）与《民用飞机、系统和设备安全性评估指南》（SAE ARP 4761）等行业指南[2-3]，制定了完整的产品全生命周期安全性评估的方法，供民用飞机研制企业开展安全性设计与评估工作参考。上述成熟国际标准涉及的方法十分依赖于成熟的设计、评估经验以及大量的产品运营数据，对新研航空发动机的安全性评估，直接照搬标准或指南中的方法并不完全适用，存在由于数据不足、经验缺乏等原因导致的安全性评估与产品设计出现脱节、评估数据源不可控、评估结果不可信等问题。为解决上述问题，笔者团队开展了基于产品架构设计的新研航空发动机安全性评估方法的研究与实践应用，保证了安全性评估面向正向的产品设计，确保了安全性评估与产品研发设计技术同频，提升了新研航空发动机产品安全性评估的有效性和正确性，为新研航空发动机成功获得适航许可、赢得市场信赖奠定安全性基础。

航空发动机安全性评估工作介绍

安全性评估是系统性、综合性地评估、评价所研发的航空发动机的设计与实施，以表明其满足相关安全性目标。发动机系统安全性评估结果的有效性和正确性，是发动机研制单位向局方、客户等利益攸关方表明产品安全性水平的重要工作。

在全生命周期的安全性评估流程中，可通过初步系统安全性评估（PSSA）和系统安全性评估（SSA）开展不同阶段的发动机安全性评估工作。初步系统安全性评估是针对发动机的架构开展一种自上而下的安全性需求分析、分配的方法；系统安全性评估是一种自下而上的验证活动，评估、验证发动机的设计能否满足安全性需求。从图1中可以看出，初步系统安全性评估是在系统工程双V模型的左半边，即开发与确认阶段；系统安全性评估在系统工程双V模型的右半边，即验证阶段。

开展发动机系统安全性评估可采用故障树分析（FTA）、依赖图（DD）、马尔可夫分析（MA）、基于模型的安全性分析（MBSA）等工具[4]。采用上述工具开展发动机系统安全性评估，可向利益攸关方表明发动机的安全性水平。对于成熟发动机型号，系统安全性评估工作依赖产品的历史运营统计数据。例如，对于发动机空中停车这一典型的安全性事件，成熟型号通过大量的运营数据，统计有效时间内导致空中停车的零组件失效等底层原因信息，通过底层原因统计信息与统计时间的比值确定发动机空中停车的评估值。同时，通过统计、分析，获得导致发动机空中停车后果的原因分

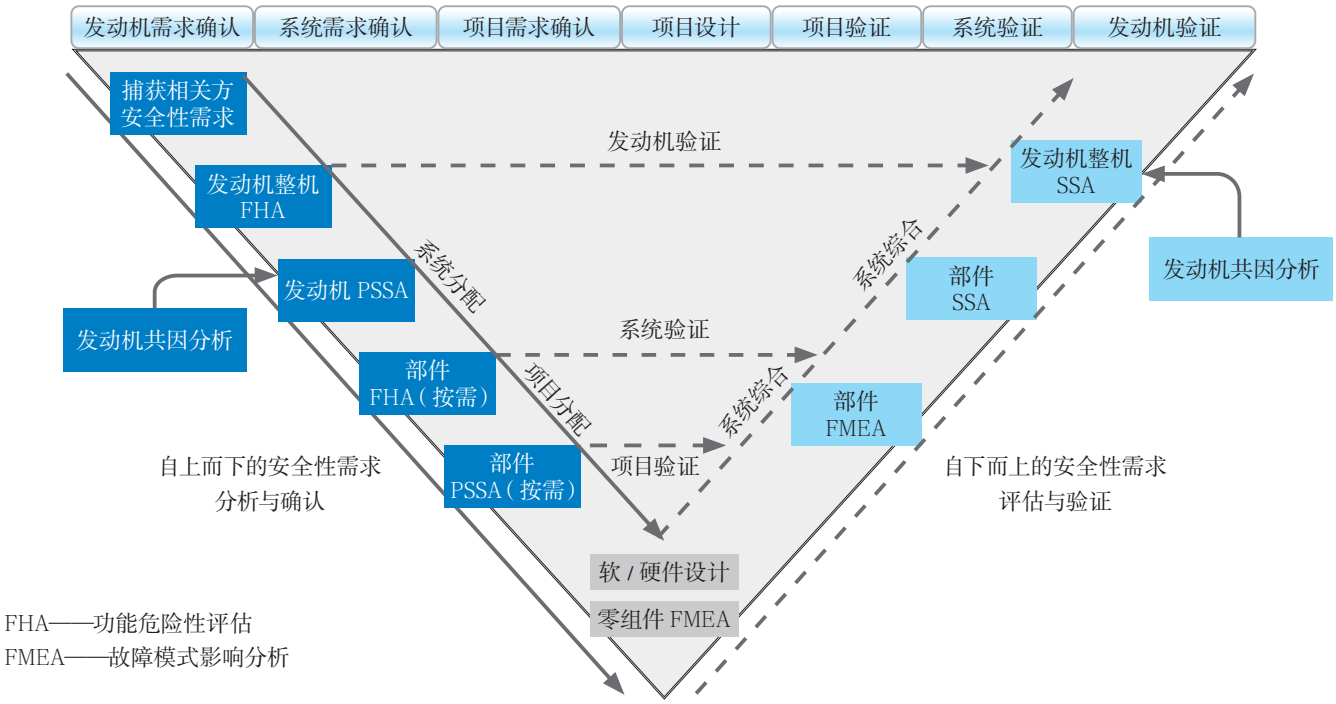

图1 发动机全生命周期的安全性评估活动

布，确定导致发动机空中停车的薄弱环节，并结合产品构型，有针对性地对发动机设计提出设计改进/使用维护的建议或要求[5-6]，以期在后续衍生型号、发展型号降低空中停车率，获得更好的发动机安全性水平，以及更优的市场竞争力。

新研航空发动机安全性评估现状分析

对于新研民用航空发动机产品，缺乏历史型号的运营数据、经验数据作为输入是开展安全性评估工作的最大难点和瓶颈。因此，新研航空发动机无法参考针对成熟型号采用的基于历史运营数据的系统安全性评估方法。此外，商用航空发动机有适航这一硬性门槛要求[7-8]，有效、科学、符合产品工程实际的安全性评估方法是新研商用航空发动机安全性评估工作亟待解决的问题。结合新研航空发动机正向研制的工程实际，开发一种对标需求、基于架构设计的发动机安全性评估方法可解决缺乏数据的问题。通过在型号工作中应用、实践，获得研发阶段有效、可信的安全性评估水平，支撑航空发动机产品的适航取证及需求符合性工作。

基于架构设计的发动机系统安全性评估方法

基于架构设计的发动机系统安全性评估方法的核心要素是架构与方案设计信息，以解决新研发动机缺乏历史服役数据的问题。总结发动机系统安全性评估工作过程包括：基于需求确定评估目标；依托产品架构设计获取评估对象信息；基于设计（架构、方案），对标需求完成完整、综合的评估。图2为新研民用航空发动机系统安全性评估流程。

确定安全性评估目标

发动机的安全性评估目标包括型号安全性需求以及管理等其他安全性目标与约束。民用航空发动机产品的安全性需求来自不同的利益

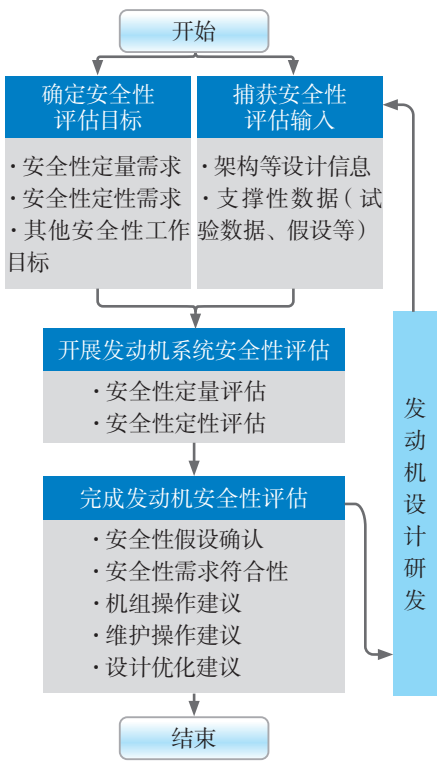

图2 民用航空发动机安全性评估流程

攸关方，包括局方、客户（飞机研制方、航空公司）以及其他国际标准/组织的要求。

适航是民用飞机产品进入市场的第一道准入门槛，是民用飞机产品必须达到的最低安全水平。《航空发动机适航规定》（CCAR-33）是中国民用航空局关于民用航空发动机最基本的安全法规。其中，CCAR-33第33.75条（CCAR-33.75）综合提出了发动机失效后果及其危险等级，以及发动机取证所需满足的安全性水平的要求。CCAR-33.75对于发动机型号的安全性要求可总结为以下几个方面：开展系统性的安全分析活动，确保捕获/识别的发动机风险具有可接受的水平；针对发动机设计目标开展安全分析，表明发动机失效或故障导致的重要的及危害性发动机后果的概率水平可接受；建立发动机安全性分析与评估流程，基于型号整体开发策划开展安全分析工作，建立安全分析与发动机设计的迭代机制，确保安全分析工作与发动机研发工作同步、同频，且可通过产品设计提升，达到可接受的安全性水平。

客户需求是发动机装机对象通过其安全性分析识别的对发动机的衍生安全性需求，包括定量安全性需求、定性安全性需求以及安全性管理等相关工作要求。典型的客户定量安全性需求如发动机空中停车的概率应≤1×10^{-5}次/发动机飞行小时；反推空中意外展开的概率应≤1×10^{-9}次/发动机飞行小时。典型的客户定性安全性需求如不应有导致灾难性后果的单点失效；在着火特殊场景下，不应发生反推空中意外展开。典型的客户安全性管理工作要求如建立安全性专业体系，以支撑型号安全性工作；建立安全性管理规范，确保安全性技术工作可有效管理。

民用航空发动机作为典型的民用航空器产品，包含发动机控制系统等典型复杂系统，可参考SAE ARP 4754/ SAE ARP 4761开展型号的安全性工作，以实现通过全生命周期的完整过程管控保障发动机产品的安全性水平满足利益攸关方的要求。

捕获安全性评估数据

开展基于架构设计的发动机安全性评估，首先要获得发动机的架构、方案设计信息，这是后续开展安全性评估建模、分析的基础，也是确保安全性评估融入设计、服务设计的重要保障。

在开展新研航空发动机系统安全性评估时，应结合型号研发试验数据积累、查询可靠性数据手册（如非电子产品可靠性数据手册）、开展专项增长试验等方式，获取发动机系统安全性评估所需的失效率等数据。有效的发动机数据获取与分析，是安全性评估有效性和正确性的保证。

开展基于架构设计的安全性分析

新研航空发动机系统安全性评估的方法可采用故障树分析，故障树分析以安全性顶事件为分析对象，开展基于架构、自上而下的故障原因分析与定位。因此，故障树分析的逻辑、结构和结论依赖发动机产品的架构设计，从而实现了发动机安全性评估“从需求中来、到设计架构中去、回归需求验证”，确保安全性评估的有效性和正确性。

在基于架构的安全性评估过程中，应关注故障树分析时识别的隐蔽失效。对于可能影响发动机安全性的隐蔽失效，应定义有效、合理的维修检查间隔，补偿由于隐蔽失效造成的潜在安全性隐患。需要注意的是，安全性评估活动定义的维修检查间隔要与基于维修指导工作组（MSG-3）定义的维修任务间隔进行联合定义确保内容的一致性，同时保障发动机安全性目标。

发动机系统安全性评估

在完成上述工作后，开展新研航空发动机安全性评估。以基于发动机架构设计建立的故障树模型为基础，通过有效的底事件失效率数据，开展自底向上的发动机安全性评估，获得发动机产品的安全性水平，表明产品安全性需求的符合性。

发动机安全性评估与设计的迭代关系

开展基于架构的发动机系统安全性评估过程与发动机的研发过程是密切迭代的。发动机的架构设计、方案设计是开展系统安全性评估的输入；在进行安全性评估过程中如评估不符合，应针对基于架构分析的故障树进行影响因子分析与排序，针对影响因子较大的底事件或架构分支提出衍生的安全性需求，并通过需求与设计迭代流程在设计中落实衍生的安全性需求，实现安全性分析与设计的迭代，同时确保满足型号安全性需求。

评估方法在发动机空中停车中的分析应用与实践

发动机空中停车是一种会导致飞行器动力严重损失、推力不平衡、增加机组操作负担和难度的安全性事件。根据国内空中停车事件统计与分析，74%的发动机空中停车是由发动机设计缺陷导致，因此在研发过程中，通过有效、科学的安全性

评估方法，对发动机空中停车事件开展分析与评估，可及时定位设计问题并落实改进措施，实现降低运营阶段发生发动机空中停车事件概率的目的。

对新研航空发动机而言，由于缺乏历史运营数据，飞机研制方、局方、航空公司客户等尤其关注原始设备制造商（OEM）对发动机空中停车事件的分析、评估与管理。通过基于架构的发动机安全性评估方法，可实现对发动机空中停车事件的分析与评估，向利益攸关方表明发动机空中停车事件的评估水平。

综合当前行业技术能力与水平，以及客户、条款等关于发动机空中停车的定量需求，发动机空中停车的概率应≤1×10^{-5}次/发动机飞行小时。以发动机“产生推力功能”相关的架构设计、方案设计为输入，针对发动机空中停车事件开展故障树分析建模，形成如图3所示的故障树分析模型。

综合型号试验数据积累、查询可靠性数据手册、专项增长试验等方式，获取发动机空中停车事件安全性评估所需的底事件失效率数据，如表1所示。

在针对发动机空中停车的安全性评估过程中，为满足顶层安全性需求，识别了相关的假设。为确保假设的有效性以及安全性评估的科学性，应对识别的假设开展逐项确认工作。表2为在开展发动机空中停车安全性评估过程中识别的假设以及假设的确认情况。

通过上述基于架构设计的安全性分析、评估工作，对于“发动机空中停车的概率应≤1×10^{-5}次/发动机飞行小时”这一发动机顶层安全性定量需求，最终评估结果为7.65×10^{-6}次/发动机飞行小时，小于1×10^{-5}次/发动机飞行小时，满足要求。

结束语

安全性是民用航空发动机进入市场、赢得市场的基础，是守卫航空器、人员生命财产安全的重要保障[9]。系统安全性评估是一种综合性的、系统性的评估手段，向利益攸关方表明产品的安全性水平。应用基于架构设计的安全性评估方法，进行基于架构、方案设计的发动机安全性

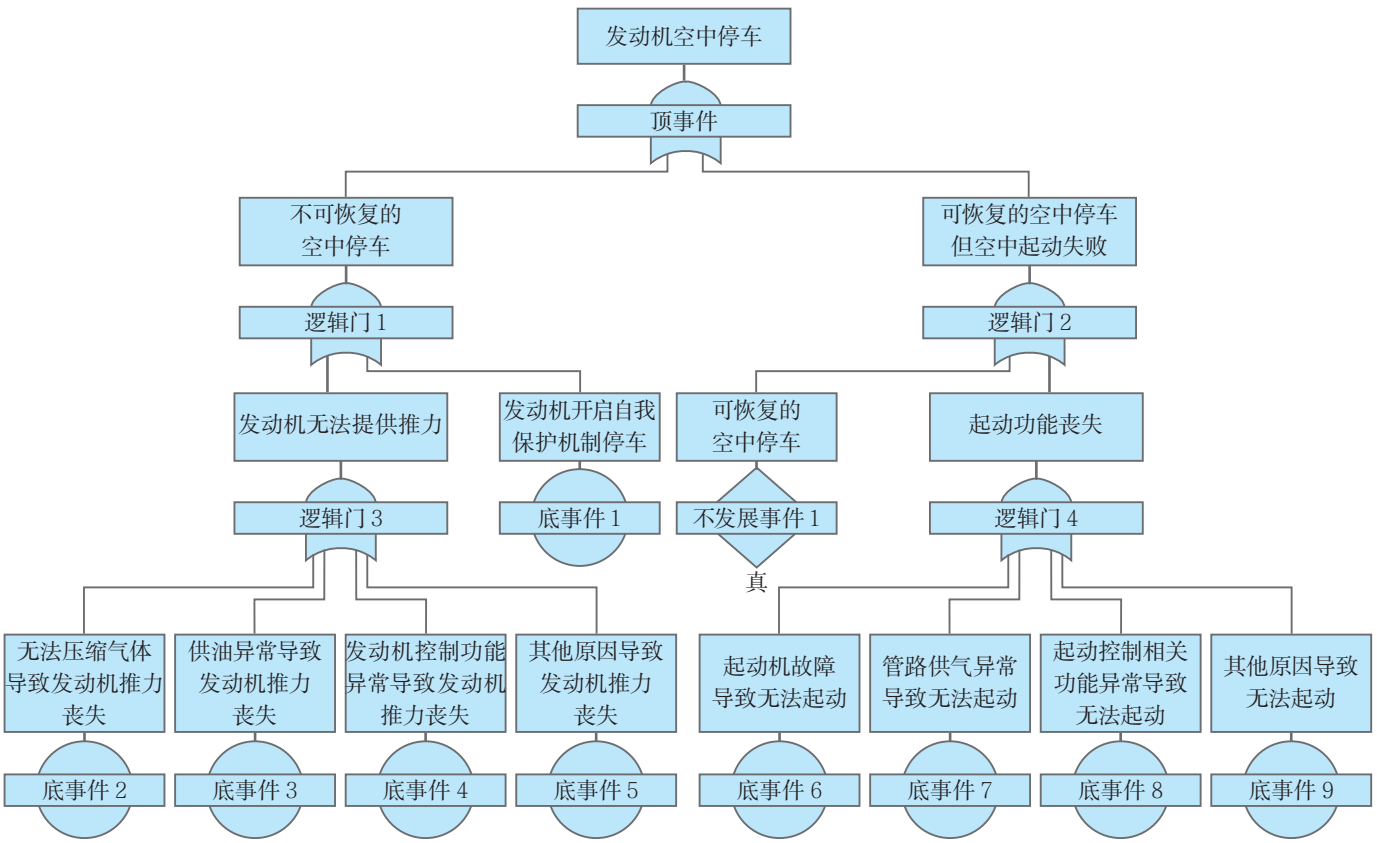

图3 基于架构设计的发动机空中停车故障树分析模型

表1 发动机空中停车评估底事件数据分析

序号	底事件描述	底事件发生率/（次/发动机飞行小时）	关联的故障模式	数据获取方式
1	无法压缩气体导致发动机推力丧失	6.5×10^{-8}	压气机叶片断裂； 调节机构装置断裂； 机匣组件断裂； 篦齿盘体断裂	试验数据积累分析
2	供油异常导致发动机推力丧失	7.89×10^{-7}	传动机构故障无法驱动附件工作	试验数据积累分析
3	发动机控制功能异常导致推力丧失	8.67×10^{-6}	传输发动机信号错误导致控制异常； 处理信号错误导致控制异常	成附件试验数据积累分析；成附件使用数据积累分析（相同成附件）
4	起动机故障导致起动功能丧失	7.4×10^{-7}	起动机故障无法传递扭矩	成附件试验数据积累分析；成附件使用数据积累分析（相同成附件）
5	管路供气异常导致起动功能丧失	8.34×10^{-7}	供气管路故障无法起动； 放气阀故障无法起动	管路试验数据积累分析；管路使用数据积累分析（相同管路）
6	起动控制相关功能异常导致无法起动	6.76×10^{-7}	起动信号处理异常无法起动； 起动程序执行异常无法起动； 燃油分配异常无法起动； 控制阀异常无法起动	成附件试验数据积累分析；成附件使用数据积累分析（相同成附件）
…	其他原因导致发动机推力丧失	…	…	…

表2 发动机空中停车评估涉及的假设分析

序号	假设描述	假设确认
1	飞机供给发动机的燃油温度过高的概率≤1×10^{-6}次/发动机飞行小时，以确保滑油温度过高导致的发动机空中停车的概率要求可接受	飞发公共数据维护管理该数据，假设有效
2	飞机供给发动机的燃油压力不足导致供油失败的概率≤2×10^{-6}次/发动机飞行小时	飞发公共数据维护管理该数据，假设有效
…	…	…

评估建模，结合规范化、科学化的失效率数据积累，作为新研航空发动机安全性评估的输入。同步开展新研航空发动机系统安全性评估与产品设计开发的迭代，确保新研航空发动机安全性评估模型可靠、科学，评估工作输入有源、有效，评估工作过程可控、规范。实现了安全性评估与设计的有效迭代，解决了传统安全性评估与设计研发活动“两张皮”的问题。从方法上保障了发动机安全性评估可靠、科学，为型号提交局方适航审查以及向装机对象表明产品安全性水平提供了有效、可信、可追溯、可管理的技术保证。

航空动力

（卢婷婷，中国航发商用航空发动机有限责任公司，高级工程师，主要从事民用航空发动机安全性、维修性等特性设计工作）

参考文献

[1] 郭博智，王敏芹，阮宏泽.民用飞机安全性设计与验证技术[M].北京：航空工业出版社，2015.

[2] 丁水汀，李果，邱天，等.航空发动机安全性设计导论[M].北京：科学出版社，2019.

[3] 赵廷弟.安全性设计分析与验证[M].北京：国防工业出版社，2008.

[4] 朱日兴.航空发动机系统安全性评估流程及验证方法[J].质量与可靠性，2022(4):27-30.

[5] 毛浩英，孙有朝，李龙彪.航空发动机安全性评估与验证数据库系统设计[J].航空计算技术，2021,51(5):109-113.

[6] 于平超，陆中，陈果，等.航空器适航技术专业“航空发动机结构与安全性”课程建设与教学研究[J].工业和信息化教育，2021,(6):67-70+76.

[7] 成伟.民用飞机机载系统安全性设计与评估[J].国际航空，2008,(5):51-53.

[8] 李稷，胡挺.基于成本的民用飞机可靠性与安全性一体化设计[J].航空工程进展，2021,12(3):121-129.

[9] 李金祥.基于安全性的某型飞机高升力控制系统设计研究[D].杭州：浙江大学，2020.