中文引用格式:肖国松,唐昊,董磊,等. 基于STPA-MBSA的航空发动机反推系统安全性分析[J]. 中国安全科学学报,2026,36(4):103-113.

英文引用格式:Xiao Guosong,Tang Hao,Dong Lei, et al. Safety analysis of aero-engine thrust reverser system based on STPA-MBSA[J]. China Safety Science Journal,2026,36(4):103-113.

基于STPA-MBSA的航空发动机反推系统安全性分析*

肖国松[1,2]实验师, 唐 昊[3], 董 磊[1,2]副研究员, 白 杰**[1,2]教授

(1 中国民航大学 民航航空器适航审定技术重点实验室,天津 300300;2 中国民航大学科技创新研究院,天津 300300;3 中国民航大学 安全科学与工程学院,天津 300300)

中图分类号:X949 **文献标志码**:A **DOI**: 10.16265/j.cnki.issn1003-3033.2026.04.0636

【摘 要】 针对航空发动机反推系统(TRS)的传统安全性分析方法在应对多层级耦合和多系统交联时存在系统交互和需求-设计闭环的局限,提出系统理论过程分析(STPA)与基于模型的安全性分析(MBSA)融合方法。通过构建从系统需求捕获到验证的全流程分析框架,采用系统建模语言(SysML)构建多视图系统模型揭示架构原理,结合STPA方法定义4类系统级损失(事故)和8类系统级危险,构建TRS反馈控制结构模型,识别11种不安全控制行为(UCAs)并得出致因场景,给出相应安全性等级,基于模型检验工具(NuSMV)构建名义模型与故障模型,并验证系统关键安全属性。结果表明:模型具有逻辑的完整性和正确性,反推空中非指令打开发生概率为1.95×10^{-10}/FH,满足小于10^{-9}/FH的安全性要求。

【关键词】 航空发动机; 系统理论过程分析(STPA); 基于模型的安全性分析(MBSA); 反推系统(TRS); 安全性分析; 系统建模语言(SysML)

Safety analysis of aero-engine thrust reverser system based on STPA-MBSA

Xiao Guosong[1,2], **Tang Hao**[3], **Dong Lei**[1,2], **Bai Jie**[1,2]

(1 Key Laboratory of Civil Aircraft Airworthiness Technology, Civil Aviation University of China, Tianjin 300300, China; 2 Science and Technology Innovation Research Institute, Civil Aviation University of China, Tianjin 300300, China; 3 College of Safety Science and Engineering, Civil Aviation University of China, Tianjin 300300, China)

Abstract: TRS is a safety-critical aero-engine system. In response to the inadequacies of conventional safety analysis techniques in addressing the complexities associated with multilevel coupling and cross-linking of multiple systems concerning system interaction and closed-loop design specifications, this study proposes a method that integrates STPA and MBSA. By establishing a whole-process analysis framework from system requirement capture to verification, an overall system model was constructed through the use of SysML to reveal the architectural principles. The STPA method was employed to define 4 types of system-level losses (accidents) and 8 types of system-level hazards, construct a TRS feedback control structure

* 文章编号:1003-3033(2026)04-0103-11; 收稿日期:2025-11-07; 修稿日期:2026-02-04

** 通信作者:白 杰(1963—),男,辽宁西丰人,硕士,教授,主要从事航空发动机使用可靠性及故障诊断、运输类飞机适航要求与符合性验证技术等研究。E-mail: 2023092123@cauc.edu.cn。

model, identify 11 unsafe control actions (UCAs), derive causal scenarios, and assign respective safety levels. Using the model checking tool new symbolic model verifier (NuSMV), fault and nominal models were constructed to verify critical system safety properties. The results demonstrate that the proposed model possesses logical integrity and correctness, and indicate that the probability of "Thrust Reverser Non-Command Open in Air," as determined from minimal cut set, is 1.95×10^{-10} per flight hour, thereby meeting the safety requirement of a failure probability of less than 10^{-9} per flight hour.

Keywords: aero-engine; systems-theoretic process analysis (STPA); model based safety analysis (MBSA); thrust reverser system (TRS); safety analysis; systems modeling language (SysML)

0 引 言

航空发动机反推系统(Thrust Reverse System, TRS)是民机的关键系统,不仅缩短了滑行距离,还为提高安全性、降低运营成本等作出重要贡献。其电子、机械、液压等多层级的强耦合与飞控、机轮刹车等多系统交联的复杂特性[1]。适航规章对 TRS 提出严格要求,《运输类飞机适航标准》[2]规定仅在预定地面使用发动机 TRS 必须设计成在飞行中处于任何反推力位置时,发动机不会产生大于飞行慢车状态的推力。美国联邦航空管理局[3]要求反推力装置空中意外展开发生概率为极不可能水平。现代发动机 TRS 朝着多电、全电的方向发展[4],多层级的耦合故障、多系统的交联反应可能引发灾难性后果,传统基于文档的安全性分析方法[5-6]已难以全面高效地开展安全性分析,亟需更优化的方法来应对这些挑战。

基于模型的安全性分析(Model Based Safety Analysis, MBSA)概念[7]在 2005 年被提出,于 2023 年正式写入标准[8]中,已被航空企业和设备制造商应用于其新一代飞行器设计研发中。国内外安全性研究人员开展诸多研究,闫锋等[9]提出使用马尔可夫和蒙特卡罗方法对航空发动机全权限数字电子控制系统限时派遣进行适航安全性分析;祁健等[10]对 S2ML 模型的自动解析和卫士转换系统语义模型自动生成方法展开研究,建立了一体化分析平台;Mhenni 等[11]提出利用 Simulink 建立了系统名义模型和拓展模型,通过故障注入分析系统响应;Krishnan 等[12]提出集成系统设计与安全框架,实现系统设计周期与安全性分析周期相结合;Gan Chenyu 等[13]提出 MBSA 时域解析框架以提升时许分析能力和工程应用场景拓展。然而,随着故障模式向系统的组合交互转变,尤其是对于具有强耦合、多交联特性的航空发动机系统,该方法同样面临系统交互和需求-设计闭环的挑战。

系统理论过程分析(System-Theoretic Process Analysis, STPA)[14]从系统角度出发,不仅关注单一组件故障,更能够识别出系统级危险和复杂交互中的潜在问题,体现系统视角的全面性。左辰翠等[15]提出使用 STPA 结合模型检验提升非线性交互系统的形式化分析水平;闫森浩等[16]基于系统建模语言(Systems Modeling Language, SysML)构建功能-可靠性集成模型,保证系统协同设计和安全性分析的一致性;Pennington 等[17]将 STPA 融入风险分析和评估建模语言以提升约束到验证的可追溯性与可验证性;Sun Minghui 等[18]提出 STPA+的安全性方法论应对复杂的多重交互系统的安全分析需求;席永涛等[19]基于 STPA 构建可视化安全控制结构实现系统不安全状态监控与路径追溯。尽管 STPA 在定性分析和系统交互风险识别方面展现出良好的适用性与有效性,但缺乏定量验证支撑,难以直接支撑系统设计优化的闭环需要。

因此,受航空发动机强耦合、多交联的特性的影响,笔者拟采用 STPA 和 MBSA 结合的方法,提供面向 TRS 的安全性分析框架,在 TRS 空中非指令展开事件基础上进一步识别致因机制,补充传统安全性分析,以期为复杂安全关键系统设计初期安全性分析提供更全面的解释信息。

1 STPA-MBSA 过程原理

系统安全性工作的核心是通过系统化可追溯、可验证的方法识别、评估和控制潜在危险,以确保系统在整个生命周期内能够安全运行。基于目前研究成果,MBSA 主要体现在由系统硬件失效导致的危险,偏向于开展定量分析;STPA 从系统整体和控制过程出发,适用于分析人为因素和复杂交互,更偏向于开展定性分析。由此以 SysML 语义为载体构建面向航空发动机 TRS 的 STPA-MBSA 方法,形成需

求建模-风险分析-验证优化的分析框架,具体分析步骤如图 1 所示。

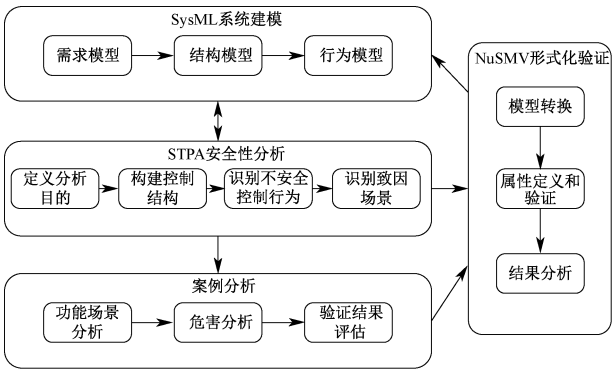

图 1　STPA-MBSA 分析步骤

Fig. 1　STPA-MBSA analysis steps

首先,对 TRS 开展 SysML 系统建模,得到分析后的需求模型、反应系统原理的结构模型和反应系统功能的行为模型,形成后续分析与验证的系统统一模型;然后,在该模型基础上开展 STPA,通过以系统级事故和危险为起点,结合由块定义图(Block Definition Diagram,BDD)和内部块图(Internal Block Diagram,IBD)抽象得到的控制结构识别不安全控制行为(Unsafe Control Actions,UCAs),并将 UCAs 及其致因转化为安全性需求(Safety Requirement,SR),安全约束返回到需求图(Requirement Diagram,Req)与时序图(Sequence Diagram,SD)与状态机图(State Machine Diagram,STM)中;最后,依据形式化模型中展现的端口、信息流与状态转换关系,通过模型语义映射转换构建新符号模型检测器(New Symbolic Model Verifier,NuSMV)形式化验证模型,同时将 STPA 产出的 SR 编码成可验证的时序性质,以此验证 SR 并得出导致 UCAs 发生致因,提出可能的缓解措施并进行影响等级和概率要求的划分,同时迭代需求约束、判别逻辑,提升系统安全性。STPA 各阶段与 SysML 图类型对应关系见表 1。

表 1　STPA 阶段与 SysML 图类型对应关系

Table 1　Correspondence between STPA stage and SysML diagram type

STPA 阶段	SysML 图类型
定义事故和危害	Req
构建控制结构	BDD、IBD
识别 UCAs	STM、活动图
识别致因场景	STM、SD

2　基于 STPA-MBSA 的 TRS 安全性分析

2.1　系统形式化模型的构建

通过分析适航规章,结合 TRS 的功能要求,建立系统需求框架,其以用户需求为顶层节点,逐步将顶层需求按照层级分解为更具体的技术规格。TRS SysML 需求图如图 2 所示,利用其建立需求追溯结构,以功能性需求、性能需求以及 SR 为关键类别,通过满足、精化需求等关系形成有机整体。对于功能性需求包括该系统必须能够展开和收回反推力装置、系统必须具有可靠的锁定和解锁机制、系统必须对飞行员的控制输入作出响应并保持稳定;对于性能需求包括“系统必须在规定时间内运行、系统必须达到规定的可靠性目标、系统必须在规定的环境条件下正常运行;对于安全需求包括系统必须具备完善的故障处理机制、必须存在系统保护机制防止在空中误作动。

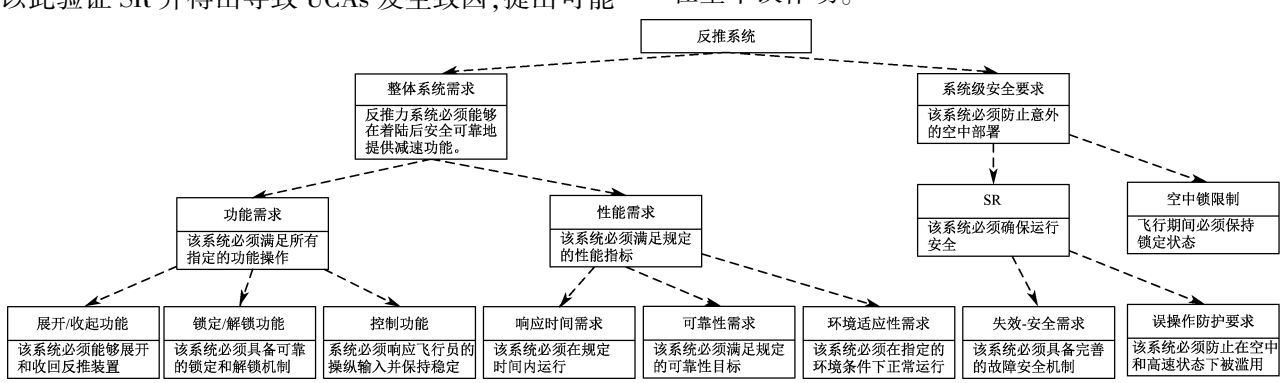

图 2　TRS SysML 需求图

Fig. 2　SysML Req of thrust reverser system

TRS 组成结构复杂且为系统级分析,因此未对较低层级过多展开,仅对主要的 TRS 整体和其中的全权限数字电子控制系统、液压控制组件(Hydraulic Control Unit,HCU)和机械作动机构等内部模型构建。

通过块定义图(图 3)描述 TRS 所包括的飞行控制、发动机接口组件(Engine Interface Unit, EIU)和 HCU 等模块,展现了电子控制、液压作动等多层级子系统间的组合关系。同时全权限数字电子控制系统、HCU 和机械作动机构分别具有发动机电子控制器(Electronic Engine Control, EEC)、N2 转速传感器、隔离阀等内部结构,由此形成了 TRS 的层次化表达。

图 4 为 TRS 的 IBD,给出了各个组件之间流的传输关系,对系统组件以 HCU 为例,构建详细 IBD(图 5),接口来自液压组件的液压流输入和向发动机电子控制器输出作动筒位置信号和锁状态。

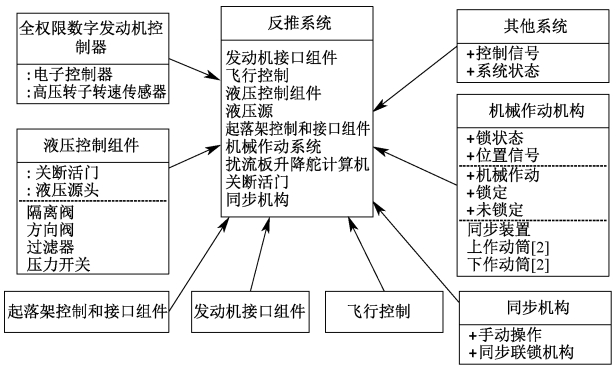

图 3 TRS SysML BDD

Fig. 3 SysML BDD of TRS

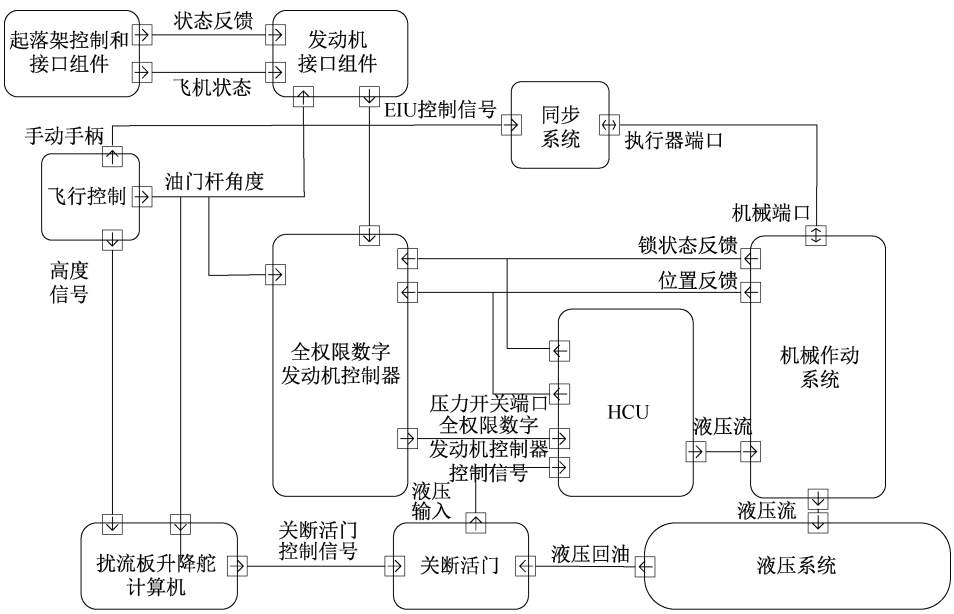

图 4 TRS SysML IBD

Fig. 4 SysML IBD of TRS

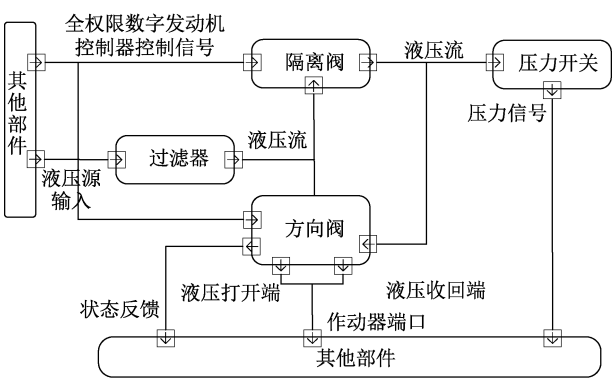

图 5 HCU SysML IBD

Fig. 5 SysML IBD of HCU

TRS 的 STM 如图 6 所示,反推装置从“收起并锁定”转变至“已打开”状态的状态转换过程以及转换逻辑,为 STPA 中进行 UCAs 为的识别提供了动态视角。系统从“收起并锁定”状态开始,即 groundStatus = ture, engineRunning = true, tlaPosition = 5.0。当接收到飞行员给出的打开指令并满足系统打开所需的地面条件和发动机运行条件时,系统进入到“解锁”状态执行 monitorLockStatus 指令,待完全解锁后,系统进入“打开”状态;在位置传感器反馈滑移套筒到达位置信息后,反推已经完成打开,系统进入“已打开”状态。系统关闭过程由“关闭”和“锁定”2 个状态实现。此外,此 STM 还展现了系统的故障处理机制,包括打开故障、关闭故障和锁机构故障 3 种类型。依据不同的检测条件检测故障,系统将转换到相应的故障子状态中,并提供了故障缓解的处理路径,以此保证 TRS 在各种飞行条件下的安全运行。

2.2 系统级事故、危险确定

结合 TRS 的运行场景和功能逻辑,识别并确

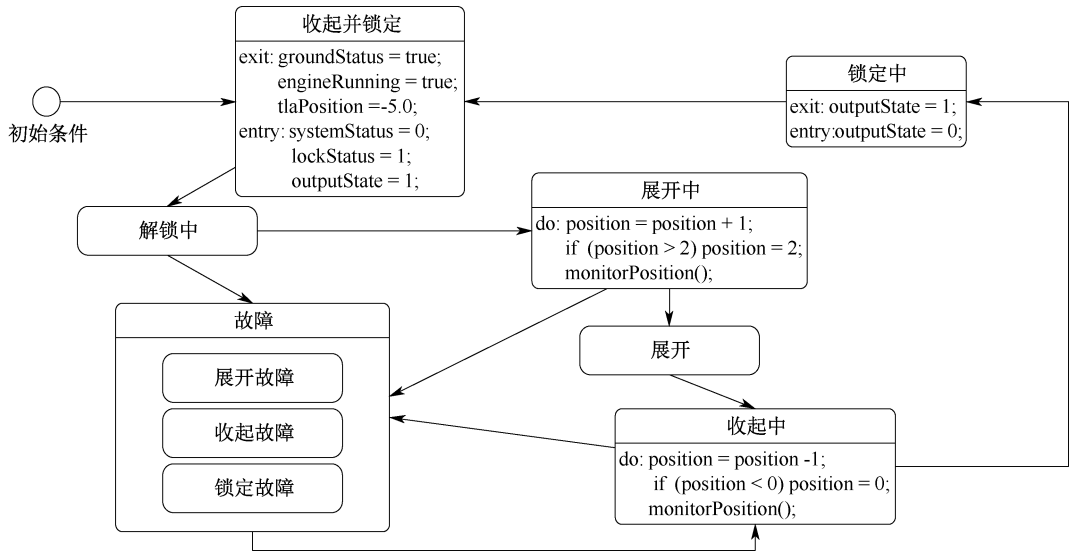

图 6　TRS SysML STM

Fig. 6　SysML STM of TRS

定 4 类系统级损失(事故)[14],见表 2。其中,人员伤亡涵盖飞行过程中可能出现的乘客、机组及地面人员伤亡事故;飞机损失主要包括反推装置损坏、发动机及飞机机体结构损坏等不可逆的设备损失;地面设施损坏涉及跑道路面、机场配套保障设备等地面设施的损毁;任务失败包含无法完成预定着陆、需要复飞、紧急撤离等影响航班正常运行的事故。

表 2　TRS 的系统级损失(事故)

Table 2　System-level loss (accident) of thrust reverser system

序号	损失(事故)
A-1	人员伤亡
A-2	飞机损失
A-3	地面设施损坏
A-4	任务失败

在系统级的损失(事故)确定后,根据在特定最不利环境条件下使得损失(事故)发生的系统的状态或存在的一定条件,识别为系统级危险[15]。因此,识别出的系统级危险包括飞机在飞行过程中违反最低间隔标准(H-1)、飞机机体完整性受损(H-2)、飞机偏离预定的航线/跑道(H-3)、飞机与地面设施距离过近(H-4)、TRS 非指令激活(H-5)、N_2 转速超限(H-6)、液压系统压力异常(H-7)、系统控制信号丢失或错误(H-8)。由于一种危险可能导致一种或多种损失(事故)发生,因此追溯每种危险对应的损失(事故),危险与损失(事故)对应关系见表 3。

表 3　TRS 的系统级危险

Table 3　System-level danger of thrust reverser system

序号	危险	关联损失(事故)
H-1	飞机在飞行过程中违反最低间隔标准	A-1, A-2, A-4
H-2	飞机机体结构完整性受损	A-1, A-2, A-4
H-3	飞机偏离预定的航线/跑道	A-1, A-2
H-4	飞机与地面设施距离过近	A-1, A-2, A-3
H-5	TRS 非指令激活	A-1, A-2, A-4
H-6	N2 转速超限	A-2, A-4
H-7	液压系统压力异常	A-2, A-4
H-8	系统控制信号丢失或错误	A-4

2.3　TRS 控制结构模型

分层控制结构是由反馈控制回路组成的系统模型[14]。在此控制结构中,控制器提供控制信号和控制作动来实现功能,并且对功能行为实施约束。过程模型通过监控被控过程反馈的信息进行调整更新。航空发动机 TRS 控制架构如图 7 所示,该控制架构简化了部分开关、阀门,反映了航空发动机 TRS 典型的多系统协同特点。该控制架将 IBD 中的端口连接映射为控制结构中的指令和反馈信息,BDD 中的块映射为控制结构中的控制器和被控过程。

2.4　UCAs 识别

UCAs 是一种控制活动,在特定环境和最坏情况下会导致危险的发生[14],根据 4 种可能存在 UCAs 的情况,识别出 TRS 的 UCAs(表 4)。

依据 TRS 的功能和使用场景,针对“反推空中非指令打开”这一 UCAs 构建 SD,如图 8 所示。纵

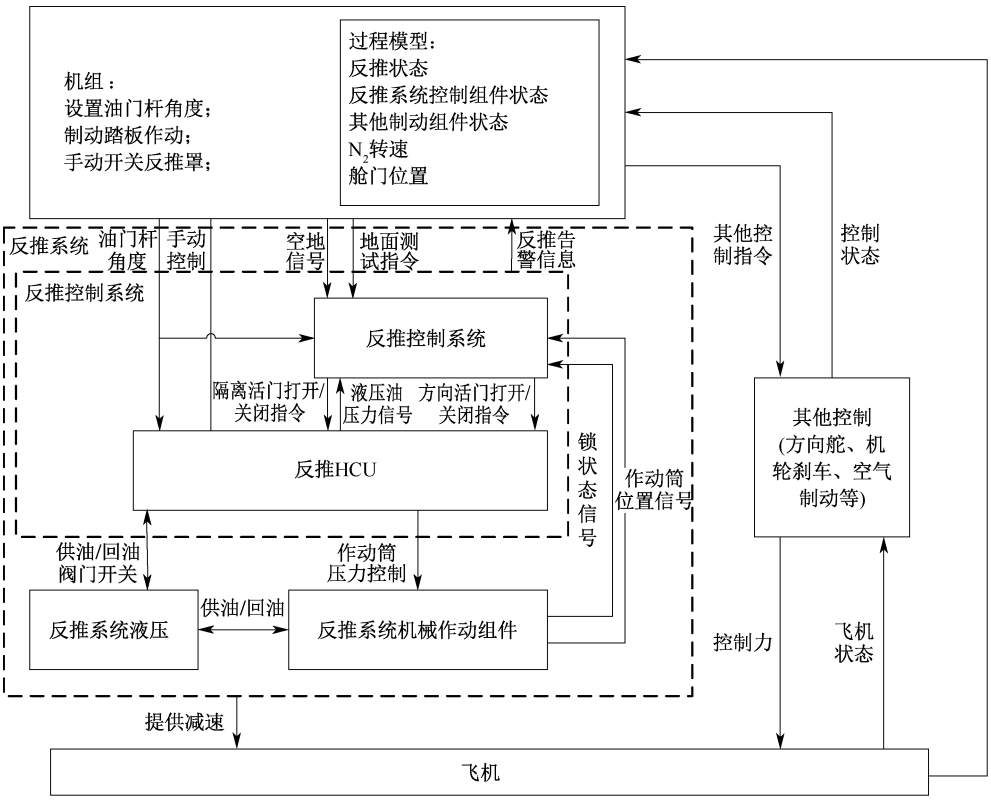

图 7　航空发动机 TRS 控制架构

Fig. 7　Aero-engine TRS control architecture

表 4　反推动作 UCAs

Table 4　UCAs of thrust reverser

控制器	控制动作	控制对象	序号	类型	描述	关联系统级危险
机组	设置油门杆角度	反推手柄	UCA-1	未提供控制行为导致的危险	当需要反推减速时机组未将油门杆置于反推位置	H-1,H-3,H-4
反推控制系统(电子)	发送隔离活门打开/关闭指令	反推液压控制组件	UCA-2		着陆滑跑阶段未发送隔离活门打开指令	H-2, H-3, H-4, H-8
反推液压控制组件	提供液压油压力信号	TRS 机械作动组件	UCA-3		隔离活门打开但未提供足够的液压压力	H-2, H-7, H-8
反推控制系统(电子)	发送方向活门打开/关闭指令	反推液压控制组件	UCA-4	提供控制行为后导致的危险	在起飞阶段错误发送方向活门打开指令	H-2, H-3, H-5, H-8
反推控制系统(电子)	控制作动筒解锁/锁定	TRS 机械作动组件	UCA-5		在未完全着陆前发送反推打开指令	H-1, H-2, H-3, H-5
反推控制系统(电子)	监控 N_2 转速	反推液压控制组件	UCA-6		N_2 转速超限时未限制反推使用	H-2, H-6, H-8
反推控制系统(电子)	协调油门杆角度与作动筒位置	TRS 机械作动组件	UCA-7	提供可能安全的控制行为但提供节点过早、过晚或顺序错误	油门杆位置变化与反推实际展开动作不同步	H-2, H-5, H-8
反推 HCU	系统协调左右发动机反推装置同步	TRS 机械作动组件	UCA-8		双发反推装置展开/收回不同步	H-2, H-3, H-5, H-8
反推控制系统(电子)	空地信号、油门杆角度信号响应	反推液压控制组件	UCA-9		系统响应延迟导致控制反推滞后	H-1, H-3, H-4, H-8
机组	控制反推使用时间	反推控制系统	UCA-10	控制行为持续过长或停止过早	反推使用时间过长导致系统过热	H-2, H-6, H-7
机组	控制反推收回	反推控制系统	UCA-11		过早收回反推导致减速不足	H-1, H-3, H-4

向生命线代表参与 UCAs 处理的关键功能单元,包括飞机系统、飞行员、EEC 等,消息流为在 UCAs 发生情况下的系统响应链,在确认 UCAs 后,系统过渡到飞行决策阶段,实施减速操作并调整飞行控制策略,最终形成着陆完成后的反推使用和 UCAs 的报告过程。

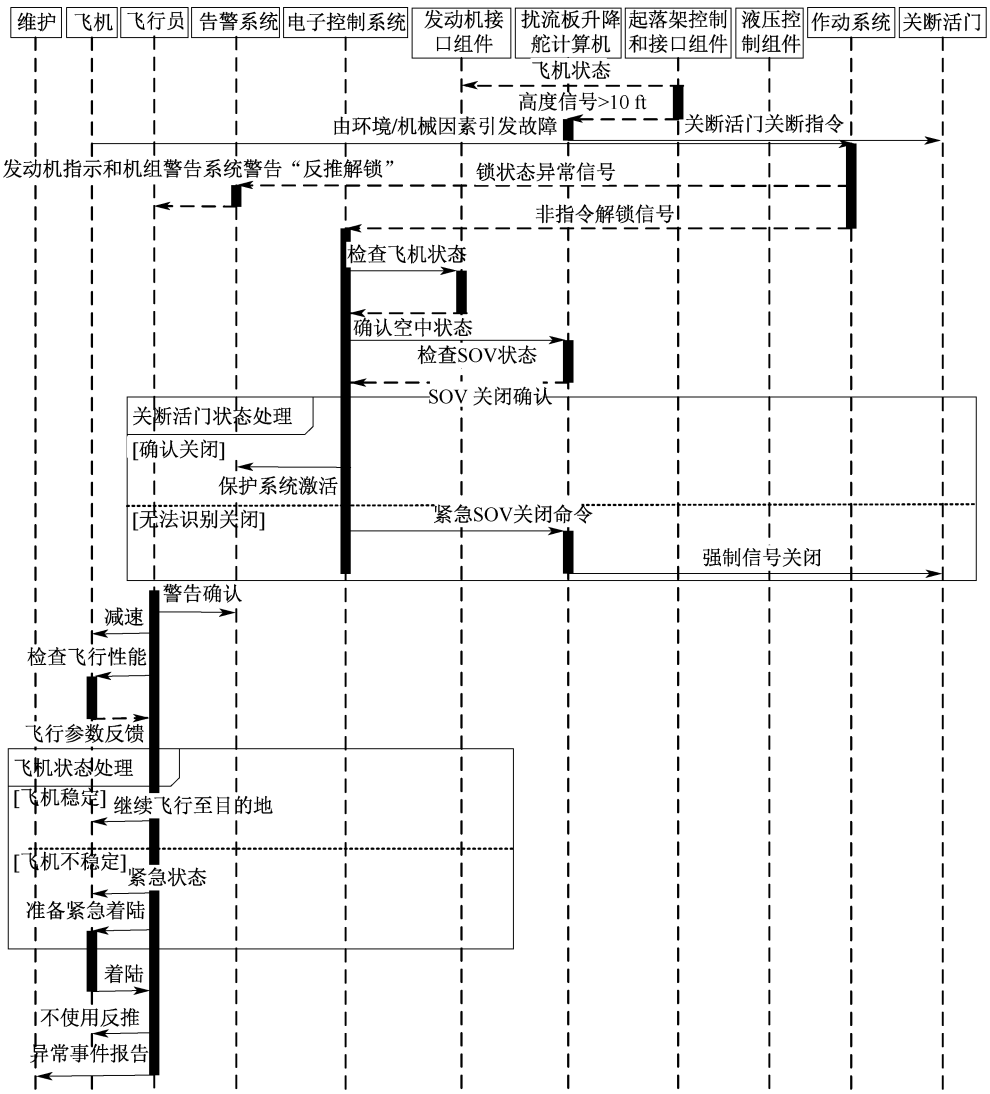

图 8　“反推空中非指令打开”SD

Fig. 8　SD of “thrust reverser non-command open in air”

2.5　致因分析

以 TRS 的控制结构模型和 UCAs 为基础分析可能导致 UCAs 的致因,包括因 UCAs 导致的危险和因不恰当的反馈信息导致的危险。因 UCAs 导致的危险其致因场景主要包括飞行员的操作因素,如未能正确设置反推手柄位置;控制系统因素,如 EEC 未能在 N_2 转速超过限制值时进行转速限制;液压系统因素,如压力不足无法提供反推展开所需要的液压力。因不恰当的反馈信息导致的危险其致因场景主要包括信息产生阶段的问题,如地面状态传感器故障;信息传输阶段的问题,如锁定状态信号错误;外部因素的影响,如电磁干扰导致信号失真。

在 STPA 方法框架下,以 UCA-4 为对象开展致因场景分析,具体如下:

1) 致因场景 1。在起飞阶段空地信号传输错误,发动机电子控制器误认为处于着陆阶段,在起飞过程中错误向液压控制组件发送活门打开指令。

2) 致因场景 2。锁作动筒位置传感器故障,在锁定状态下,发动机电子控制器误识别不安全状态,导致反推非预期打开。

3) 致因场景 3。液压系统活门泄露导致液压压力积累,在起飞状态下锁失效,导致反推非预期

打开。

4）致因场景 4。双通道信号传输中断导致控制系统接到不相同的状态信息，系统错误判断认为处于安全状态而激活 TRS。

5）致因场景 5。维护人员在系统检查后未能正确恢复控制参数，TRS 因此处于预激活状态。

分析 UCAs 致因场景，建立 UCA 和 SR 的对应关系，见表 5。

表 5 UCA 与功能需求对应关系

Table 5 Corresponding relationship between UCA and functional requirements

序号	关联 UCA	SR	影响等级	概率要求
SR-1	UCA-4、UCA-5	在飞行阶段，TRS 必须保持关闭，防止非预期打开	Ⅰ	$<10^{-9}$
SR-2	UCA-5、UCA-11	TRS 在运行时必须具有可靠的安全机制，防止不当操作	Ⅲ	$<10^{-5}$
SR-3	UCA-7、UCA-8	控制系统必须确保油门杆角度信号与实际反推展开动作同步	Ⅱ	$<10^{-7}$
SR-4	UCA-1、UCA-2、UCA-9	控制系统必须在全运行阶段提供准确的状态反馈和控制响应	Ⅲ	$<10^{-5}$
SR-5	UCA-3	TRS 液压必须提供足够压力并具备压力异常监测	Ⅲ	$<10^{-5}$
SR-6	UCA-6、UCA-10	发动机控制系统必须持续监控 N2 转速，防止其超限运行	Ⅲ	$<10^{-5}$
SR-7	UCA-2、UCA-3	系统液压控制必须确保液压活门按指令动作且液压压力充足	Ⅲ	$<10^{-5}$
SR-8	UCA-8、UCA-10	双发 TRS 必须保证同步协调，并监测不对称行为	Ⅱ	$<10^{-7}$

3 基于 NuSMV 的安全性验证

NuSMV 作为设计初期模型检验工具，通过人为或随机故障注入与逻辑一致性检验来识别小概率、强耦合的问题，其以模型抽象为基础，通过 NuSMV 强逻辑完整性与故障追溯性的检验，从不同层级、不同角度与性能边界、适航验证的物理验证为主的地面试验、试飞等真实模拟相辅相成。

根据 SysML 输出的 XML 文件，参照文献[20]，提取关键信息进行语义转化，构建所需的 NuSMV 模型。针对表 5 所列 SR，NuSMV 名义模型的验证语句和验证结果见表 6。

表 6 SR 验证语句及结果

Table 6 SR validation statements and results

序号	安全性需求	NuSMV 验证语句	验证结果	注释
SR-1	在飞行阶段，TRS 必须保持关闭，防止非预期打开	AG（inFlight -> AG!（TRS. state = deployed | TRS. state = deploying））	true	在爬升、巡航和进近阶段，TRS 不处于已打开或正在打开状态，验证符合
SR-2	TRS 在运行时必须具有可靠的安全机制，防止不当操作	AG（minAirspeed = critical -> !（TRS. state = deploying | TR_System. state = deployed））	false	在临界状态下，TRS 不处于打开或正在打开状态，验证不符合
SR-3	控制系统必须确保油门杆角度信号与实际反推展开动作同步	AG（（（FlightCtrl. tlaPosition < 4.8 &. groundStatus = True）& TRS. state = unlocking）-> AX（FlightCtrl. throttleValue < 0 & AF（TRS. state = deployed -> FlightCtrl. throttleValue < 0）））	false	当油门杆角度小于 4.8 且地面状态信号为真，反推处于解锁状态时，下一状态油门杆角度必须为负，验证不符合
SR-4	控制系统必须在全运行阶段提供准确的状态反馈和控制响应	AG（TRS. state = deployed -> FlightCtrl. throttleValue < 0）	true	当 TRS 处于已打开状态时，油门杆位置必须为负，验证符合
SR-5	TRS 液压必须提供足够压力并具备压力异常监测	AG（（TRS. state = deploying | TRS. state = deployed）-> AG（Hydraulic. pressure = True & AX Hydraulic. pressure = True））	false	当 TRS 处于打开或正在打开状态时，液压压力必须正常，验证不符合

续表 6

序号	安全性需求	NuSMV 验证语句	验证结果	注释
SR-6	发动机控制系统必须持续监控 N2 转速,防止其超限运行	AG (EngineMonitor. engineStatus = overspeed -> AF ! (TRS. state = deploying | TRS. state = deployed))	true	当发动机处于超速状态时,最终 TRS 必须不处于打开或正在打开状态,验证符合
SR-7	TRS 液压控制路径	AG (HCU. isolationValveStatus = True -> (Hydraulic. hydraulicFlow = True | Hydraulic. pressure = Ture))	false	当隔离阀打开时,需有液压且有压力,验证不符合
SR-8	双发 TRS 必须保证同步协调,并监测不同步行为	AG ((TRS1. state = deploying & TRS2. state = deploying) -> AG (abs(TRS1. position - TRS2. position) <= 1))	true	当左右发 TRS 同时打开时,它们的位置差异不能超过限制,验证符合

注:全称全局算子(All Globally,AG);全称最终算子(All Finally,AF);全称下一状态算子(All Next,AX)。

由表 6 可知:TRS 架构暂不满足 SR-2、SR-3、SR-5 和 SR-7 4 项安全性需求,可能存在潜在架构缺陷。结合该需求名义模型验证结果的可追溯状态,从控制逻辑优化、指令传输和液压系统 3 个方面提出针对性模型架构改进建议。

在控制逻辑方面,对发动机电子控制器控制逻辑增添基于实时空速的判断条件,将空速与反推控制相关联,完善反推触发约束机制;在控制指令传输方面,采用高灵敏的传感器确保油门杆位置信号传输的实时性与准确性,保证油门杆位置和反推状态的一致;在液压系统方面,通过多冗余液压压力监控强化液压系统的故障检测能力,保证液压压力的正常供给,同时增设快速隔离装置,保障液压控制回路的功能完整性。

针对 SR-1,对“反推空中非指令打开”展开模型验证,表 6 名义模型验证结果显示符合,即在飞行状态下,TRS 不应处于已打开或者正在打开的状态。故障模型验证结果为不符合,并给出相应的反例,见表 7,状态 1.1 表示此时反推处于正常状态且飞机处于飞行阶段;状态 1.2—1.5 开始由于产生错误的地面状态信号,对飞机状态产生误判,同时锁机构异常导致反推进入解锁状态,在控制逻辑未给出反推展开指令时,液压作动系统错误作动将反推打开;在液压的持续作用下,反推最终处于打开位置,导致 1.6 状态的出现,综合飞机所处飞行阶段,认为违反 SR-1。

其关键因素包括起落架控制和接口组件提供错误的地面状态信号、控制单元发生故障导致错误指令传输、锁机构失效和液压系统状态异常,分析得出最小割集和事件列表,见表 8。由此“反推空中非指令打开”发生的概率约为 1.95×10^{-10}/FH,其满足文献[3]中概率小于 10^{-9}/FH 的要求,保证了系统架构设计的合理性。

表 7　针对 SR-1 的反推空中非指令打开验证反例路径

Table 7　Verifying counterexample paths for SR-1 “thrust reverser non-command open in air”

验证结果:反推空中非指令打开
State 1.1(部分):
TRS. state = stowedLocked
TRS. deploymentStatus = stowed
TRS. outputState = 0
TRS. position = 0
TRS. isUnlocked = false
TRS. faultType = 0
inFlight = true
minAirspeed = low
State 1.2 - State 1.5 状态转换
State 1.6:
TRS. state = deploying
FlightCtrl. engineRunning = false
EIU. directionValveCmd = false
EIU. eiuFault = false
Mechanical. lockStatus = true
Mechanical. faultDetected = false
Hydraulic. pressure = false
HCU. actuatorControl = extending
HCU. hcuFault = false
LGCIU. groundStatus = false
Mechanical. lockStatus = false
Hydraulic. pressure = false

4　结　论

1) 利用 SysML 语言充分考虑 TRS 的强耦合、多交联的特性构建形式化模型,可揭示系统跨层级间的交互机制,以需求与验证的映射支撑系统研制流程的开展,能够为 STPA 提供明确的参考依据。

表 8 “反推空中非指令打开”最小割集及概率

Table 8 “Thrust reverser non-command open in air” minimum cutsets and probabilities

序号	故障组合	割集元素	故障概率
1	地面压力感知故障与控制单元错误	LGCIU 空/地状态错误指示	8×10^{-6}
		EIU 控制器输出错误信号	7×10^{-7}
2	主锁故障与液压控制故障	主锁机构解锁失效	9×10^{-6}
		HCU 液压控制单元故障	6×10^{-7}
3	锁定状态错误与隔离阀故障	锁定状态传感器故障	7×10^{-6}
		HCU 隔离阀故障	5×10^{-7}
4	电子控制器故障与液压活门故障	EEC 控制逻辑错误	3×10^{-7}
		HCU 方向阀故障	6×10^{-6}
5	发动机控制器故障与液压压力异常	安全互锁失效	4×10^{-7}
		液压系统压力异常	8×10^{-6}
6	电子控制器故障、机械系统异常与飞行员错误	EIU 电子控制单元失效	2×10^{-7}
		机械连接异常	6×10^{-6}
		飞行员错误控制输入	4×10^{-7}

2）利用 STPA 方法与 NuSMV 形式化验证模型验证 TRS 使用过程中的 SR，证明所提方法具备一定可行性，有助于弥补风险识别与设计验证关联性差的不足。

3）以功能、性质验证结果支持早期设计的确认，可将安全性分析尽早融入系统设计，保证系统设计的正确性、合理性、完整性。在架构迭代深度上仍有不足，实际导致不安全控制行为发生的致因可能需要对更底层组件的失效和交互进行深入研究和迭代。

参 考 文 献

[1] 尹泽勇，米栋，张立章，等. 航空动力系统整机多学科设计优化方法[J]. 航空动力学报，2022，37(10)：2 025-2 045.
Yin Zeyong，Mi Dong，Zhang Lizhang，et al. Multidisciplinary design optimization method of overall aircraft power system[J]. Journal of Aerospace Power，2022，37(10)：2 025-2 045.

[2] CCAR-25-R4 运输类飞机适航标准[S]. 2016.
CCAR-25-R4 Airworthiness standards：transport category airplanes[S]. 2016.

[3] FAA，Information：equivalent level of safety (EOLS) finding for flight critical thrust reverser on the boeing model 787-8/-9/-10 and 747-8/-8F[S]. 2011.

[4] 付尧明，任善全，闫锋. 电反推系统适航分析[J]. 航空动力，2020(6)：52-54.
Fu Yaoming，Ren Shanquan，Yan Feng. Airworthiness analysis of electric thrust reverser system[J]. Aerospace Power，2020(6)：52-54.

[5] 刘新，伍俊楠，潘殿琦，等. 基于改进 FMEA 的污水厂设备故障风险评估模型[J]. 中国安全科学学报，2024，34(8)：101-107.
Liu Xin，Wu Junnan，Pan Dianqi，et al. Equipment failure risk assessment model of wastewater treatment plant based on improved FMEA[J]. China Safety Science Journal，2024，34(8)：101-107.

[6] 杨震，梁峻铭，郭梨，等. 基于混合因果逻辑的化工园区雷击储罐风险评估[J]. 中国安全科学学报，2024，34(9)：174-182.
Yang Zhen，Liang Junming，Guo Li，et al. Risk assessment of chemical industrial park storage tanks struck by lightning based on hybrid causal logic methodology[J]. China Safety Science Journal，2024，34(9)：174-182.

[7] Joshi A，Mmiller S P，Wwhalen M，et al. A proposal for model-based safety analysis[C]. Document Analysis Systems VI. IEEE，2005：DOI：10. 1109/dasc. 2005. 1563469.

[8] SAE ARP4761A-2023 Guidelines and methods for conduction the safety assessment process on civil airborne systems and equipment[S].

[9] 闫锋, 张彦昌, 徐文韬. 航空发动机 FADEC 系统限时派遣(TLD)适航安全性分析方法研究[J]. 民用飞机设计与研究, 2024(3):128-136.
Yan Feng, Zhang Yanchang, Xu Wentao. Research on airworthiness safety assessment method of time-limited dispatch (TLD) for the FADEC system of aero-engine [J]. Civil Aircraft Design and Research, 2024(3):128-136.

[10] 祁健. 基于 AltaRica 模型的系统安全性分析方法和工具研究[D]. 南京:南京航空航天大学,2022.
Qi Jian. Research on system safety analysis methods and tools based on AltaRica[D]. Nanjing: Nanjing University of Aeronautics and Astronautics, 2022.

[11] Mhenni F, Nguyen N, Choley J Y. SafeSysE: a safety analysis integration in systems engineering approach[J]. IEEE Systems Journal, 2018, 12(1): 161-172.

[12] Krishnan R, Bhada S V. An integrated system design and safety framework for model-based safety analysis[J]. IEEE Access, 2020,8:146 483-146 497.

[13] Gan Chenyu, Ding Shuiting, Qiu Tian,et al. Model-based safety analysis with time resolution (MBSA-TR) method for complex aerothermal-mechanical systems of aero-engines[J]. Reliability Engineering and System Safety, 2024,243:DOI: 10. 1016/j. ress. 2023.

[14] Leveson N, Thomas J. STPA handbook[EB/OL]. [2019-07-22]. http://psas. scripts. mit. edu. home/get_file. php?name=STPA_handbook. pdf.

[15] 左辰翠, 黄志球, 胡军,等. 基于 STPA 的飞行导引系统模式转换的安全性分析研究[J]. 计算机科学, 2026, 53(1): 341-352.
Zuo Chencui, Huang Zhiqiu, Hu Jun, et al. Research on safety analysis of mode transition of flight guidance system based on STPA[J]. Computer Science, 2026, 53(1): 341-352.

[16] 闫森浩, 陈余军, 杨清龙, 等. 基于 MBSE 的中继卫星捕获跟踪系统故障建模分析[J]. 航天器工程, 2025, 34(4): 71-77.
Yan Senhao, Chen Yujun, Yang Qinglong, et al. A MBSE approach to fault modeling and analysis of ATS in TDRS[J]. Spacecraft Engineering, 2025,34(4): 71-77.

[17] Pennington E, Johnson K, Colombi J, et al. Integrating STPA extended for coordination into SysML using RAAML[J]. INCOSE International Symposium, 2024, 34(1): 749-762.

[18] Sun Minghui, Fleming C H. A new safety-guided design methodology to complement model-based safety analysis for safety assurance[J]. IFAC-PapersOnLine, 2022, 55(41):101-106.

[19] 席永涛, 刘鹏杰, 胡甚平,等. 基于 STPA 和 FTPN 的海上自主水面船舶航行实时风险评估[J]. 中国安全科学学报, 2024,34(8):18-26.
Xi Yongtao, Liu Pengjie, Hu Shenping, et al. Real-time risk assessment for maritime autonomous surface ships based on STPA and FTPN[J]. China Safety Science Journal, 2024,34(8):18-26.

[20] 赖康, 陆中, 程大炜,等. 基于 SysML2NuSMV 的民用飞机电传飞控系统安全性分析[J]. 系统工程与电子技术, 2025,47(11):3 802-3 815.
Lai Kang, Lu Zhong, Cheng Dawei,et al. Safety analysis of civil aircraft fly-by-wire system based on SysML2NuSMV[J]. Systems Engineering and Electronics, 2025,47(11):3 802-3 815.

作者简介: 肖国松 (1982—),男,湖南衡阳人,硕士,实验师,主要从事航空器适航审定技术、航空发动机故障诊断及预测等方面的研究。E-mail: gsxiao@ cauc. edu. cn。