2025 年 第 25 卷 第 20 期
2025, 25(20): 08714-11

科 学 技 术 与 工 程
Science Technology and Engineering

ISSN 1671—1815
CN 11—4688/T

DOI:10.12404/j.issn.1671-1815.2405472
引用格式:孙晓哲, 王家璇, 杨建忠. 基于 STPA-Bayes 模型的航空事故致因分析与风险评估[J]. 科学技术与工程, 2025, 25(20): 8714-8724.
Sun Xiaozhe, Wang Jiaxuan, Yang Jianzhong. Cause analysis and risk assessment of aviation safety accidents based on STPA-Bayes model [J]. Science Technology and Engineering, 2025, 25(20): 8714-8724.

基于 STPA-Bayes 模型的航空事故致因分析与风险评估

孙晓哲, 王家璇, 杨建忠
(中国民航大学安全科学与工程学院, 天津 300300)

摘 要 通过系统理论过程分析(system-theoretic process analysis, STPA)方法识别航空事故危险因素,属于定性分析过程,无法定量地评估各因素对事故的影响程度。针对上述问题,提出 STPA 与贝叶斯网络(Bayesian network, BN)结合的定性与定量分析方法。以捷蓝航空 A320 飞机襟翼事故为例,通过 STPA 方法构建了襟翼控制系统的控制结构模型并全面地分析了潜在的不安全控制行为及相关致因场景。随后将 STPA 定性分析结果转化为可定量分析的贝叶斯网络模型,从而识别出事故中的内部交互逻辑以及影响度较高的致因因素,提出全面的安全性建议。分析结果表明:导致事故的主要因素为液压源故障,而动力传输组件(power transmission unit, PTU)故障和液压管路泄漏是导致液压源失效的主要原因,关键重要度分别为 0.688 和 0.299。

关键词 事故分析; 系统理论过程分析(STPA); 贝叶斯网络(BN); 致因分析; 风险评估
中图法分类号 V249; **文献标志码** A

Cause Analysis and Risk Assessment of Aviation Safety Accidents Based on STPA-Bayes Model

SUN Xiao-zhe, WANG Jia-xuan, YANG Jian-zhong
(School of Safety Science and Engineering, Civil Aviation University of China, Tianjin 300300, China)

[**Abstract**] The identification of aviation accident risk factors through the system-theoretic process analysis (STPA) method is a qualitative analysis process that does not allow for a quantitative assessment of the extent to which each factor contributes to an accident. To address the above problem, a qualitative and quantitative analysis method combining STPA and Bayesian network (BN) was proposed. Taking the JetBlue A320 aircraft flap accident as an example, the control structure model of the flap control system was constructed by STPA method, and the potential unsafe control behaviors and related causal scenarios were analyzed comprehensively. Then, the results of STPA qualitative analysis were transformed into a Bayesian network model that could be quantitatively analyzed, so as to identify the internal interaction logic and the highly influential factors in the accident, and put forward comprehensive safety recommendations. The analysis results show that the main factor leading to the accident is the failure of hydraulic source, while the failure of power transmission unit (PTU) and the leakage of hydraulic line are the main causes of hydraulic source failure, with a critical importance of 0.688 and 0.299, respectively.

[**Keywords**] accident analysis; systems-theoretic process analysis(STPA); Bayesian network(BN); causal analysis; risk assessment

航空安全是航空行业重要的关注领域,为保障乘客和机组人员的安全,必须持续提升安全水平并减少事故发生率。航空安全事故的致因错综复杂[1],其中系统故障是事故链条中的关键环节。因此,及时识别和评估这些故障的风险是提升航空安全的关键。然而,民机系统的复杂性及其高度集成,给风险的识别和评估带来了前所未有的挑战,对安全性分析提出了更高的要求。传统的系统安全性评估方法,如故障树分析(fault tree analysis, FTA)、功能危害分析(functional hazard analysis, FHA)和失效模式及其影响分析(failure mode and effects analysis, FMEA)等,可以很好地解释系统的运作方式并将系统安全性问题转化为组件可靠性问题,并且已经在民机系统安全性研究中广泛应

收稿日期: 2024-07-21; **修订日期**: 2025-04-12
基金项目: 国家重点研发计划(2022YFB4301000)
第一作者: 孙晓哲(1983—),女,汉族,河北石家庄人,博士,副教授。研究方向:民用飞机飞控作动系统容错控制、飞控系统架构安全性设计与评估。E-mail:xzsun@cauc.edu.cn。

用[2]。但对于内部存在复杂交互关系的系统,传统方法难以进行准确建模和全面有效的分析。

系统理论过程分析(system-theoretic process analysis, STPA)是基于系统理论和控制理论的安全分析方法,该方法认为系统是由多个组成部分相互作用而成的复杂整体,这些组成部分之间存在着动态的关系和相互影响[3]。与其他安全性分析方法相比,该方法不仅能准确描述组件间的异常交互,还能全面地识别系统安全隐患,使其更适合应用于复杂系统的分析。近年来,中国在航空安全领域取得了显著进展,STPA 已在中国航空安全领域被广泛应用,并取得了不错的效果。在机轮刹车系统中,STPA 可以全面地识别机轮刹车系统在飞机降落过程中的不安全控制行为(unsafe control actions, UCA),从系统整体角度完成对刹车系统的风险辨识和影响分析[4]。为了防止低空无人机冲突解决过程中危险进近或事故的发生,文献[5]基于 STPA 识别了低空无人机冲突解决过程中的 UCA,并分析产生不安全控制行为的关键致因。文献[6]应用 STPA 方法分析空中加油中的“软管甩鞭问题”,充分考虑了系统的非线性交互,实现了系统控制思维在空中加油安全性分析中的应用。虽然 STPA 可以全面分析系统存在的潜在缺陷,但缺少对系统的定量分析和概率计算,无法描述潜在致因场景对系统不安全控制行为的影响程度。

贝叶斯网络(Bayesian network, BN)基于贝叶斯定理和图论的概念,是一种用于表示变量间的依赖关系并进行概率推理的概率图模型,可以对复杂系统中的非线性关系形式化建模,捕捉变量之间的非线性依赖关系来量化分析系统,且在航空安全领域中有着多方面的应用。在风险评估方面,为降低城市物流无人机碰撞风险,文献[7]基于贝叶斯网络对无人机的碰撞风险因素进行了逆向推理、敏感性和影响强度等的分析,并根据分析结果针对性提出防控建议。为了分析民机着陆超限风险及其影响因素,文献[8]基于中国某航空公司 B737-800 机队飞行数据建立着陆超限风险贝叶斯网络,量化评估各飞行参数变化对着陆超限风险的影响,有效分析着陆超限事件的交互关系。文献[9]基于贝叶斯网络对电动垂直起降飞行器控制失效场景进行分析,包括失控坠地和中间场景的正向和逆向推理分析,深入理解系统内部的复杂交互机制。

为解决航空事故分析中 STPA 无法定量评估的问题,将 STPA 与贝叶斯网络方法相结合,STPA 能够透彻分析系统级别的交互和依赖关系,以全面地识别复杂系统中可能存在的系统故障或错误传播路径。贝叶斯网络则可以以形式化方式将系统内部交互逻辑建模并描述出来,为 STPA 提供概率推断和风险评估的支持,使得安全分析结果不仅依赖于定性判断,从而更好地分析和评估系统的潜在风险,增强了分析的客观性和可信度。采用 STPA-Bayes 方法对航空安全事故进行研究,识别出导致事故发生的潜在致因因素,并量化评估事故风险,可为航空安全事故风险分析提供理论指导。

1　事故分析理论与方法

1.1　系统理论过程分析

系统理论过程分析是一种危害分析的系统方法[10],它不仅可以系统地识别与组件故障相关的危险,还可以识别如组件交互故障、有缺陷的控制行为、人为错误、设计错误等相关的危险,从而更全面地评估系统的安全性和可靠性。分析过程如图 1 所示。

STPA 通过创建系统的安全控制结构,详细描绘系统内部组成及其之间的控制和反馈路径,使用致因分析框架来识别致因场景,如图 2 所示。

1.2　贝叶斯网络

贝叶斯网络是一种用图形方式表示变量之间依赖关系的模型,常用于机器学习和人工智能领域[11]。作为概率图模型的一种,贝叶斯网络利用图形化的方式清晰地展现复杂的概率关系,在其图形化模型中,节点代表变量,边则代表变量之间的概率依赖关系,通常用箭头来表达因果关系。图 3 为一个简单的贝叶斯网络结构,条件概率表以 X_5 节点为例(概率表中,0 为正常、1 为故障)。

贝叶斯网络的主要优点是结构直观,能够清楚地呈现出变量之间的依赖关系,并且结合一些变量的观测,可以使用贝叶斯网络来推断其他变量的概率分布。

1.3　STPA-Bayes 分析流程

结合两者的优势,图 4 为 STPA-Bayes 方法整体流程。首先是根据事故场景建立控制结构模型,通过识别不安全控制行为和相关致因场景得到可能导致事故的原因及对应的定性安全性需求,根据转换规则建立相应的 BN 结构模型,最后代入条件概

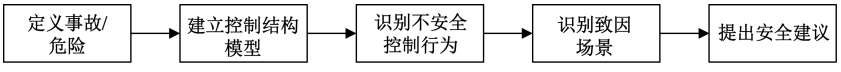
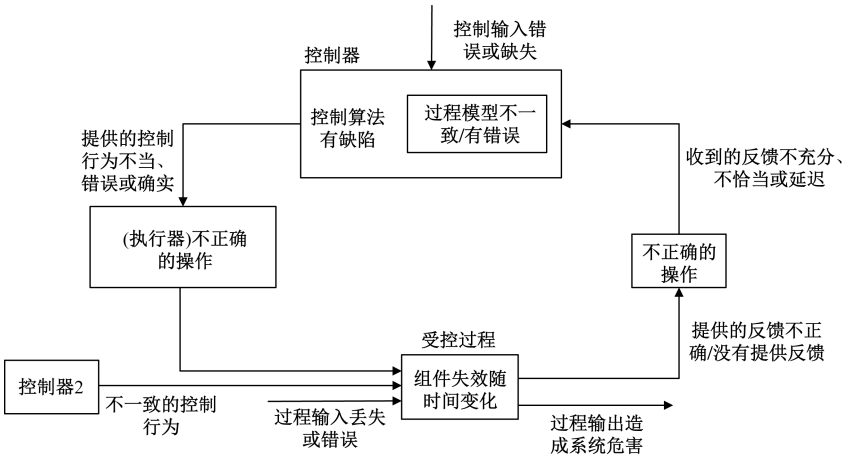


图 1　STPA 分析流程

Fig. 1　STPA analysis process



向下箭头指示可施加的控制指令;向上箭头指示可由控制器监控并做出决策的信息和反馈

图 2 STPA 通用致因分析框架

Fig. 2 Generic causal analysis framework for STPA

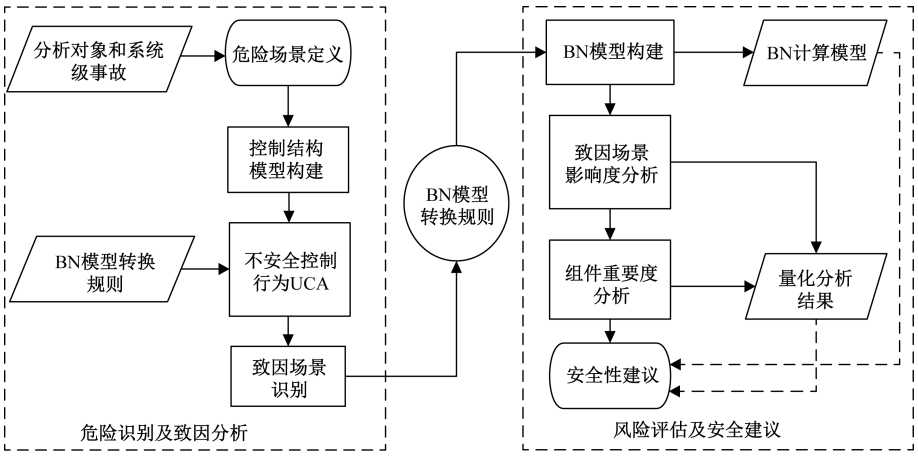
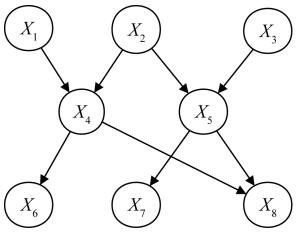


图 4 STPA-Bayes 整体流程

Fig. 4 Overall flow of the STPA-Bayes method



X_2	X_3	X_5
1	1	1
1	0	0.85
0	1	0.75
0	0	0

图 3 简单贝叶斯网络示例

Fig. 3 Example of a simple Bayesian network

率表进行计算,量化评估 UCA,并根据分析结果给出相应安全建议。

1.4 模型转换规则

根据 STAMP 控制结构模型和通用致因因素框架(图 2),可以识别系统中可能的不安全控制行为及相应的潜在致因场景。接着,根据致因场景中的系统组件、失效模式等因素构建贝叶斯网络模型。具体模型转换规则如下。

(1)所分析的不安全控制行为作为 BN 模型的终端叶节点。

(2)与 UCA 直接或间接相关的致因场景,如襟翼控制器故障、控制手柄故障等作为中间叶节点。

(3)UCA 对应致因场景所涉及的所有组件/模块作为 BN 模型的根节点。

(4)UCA 对应致因场景所涉及的所有组件/模块的故障率作为各根节点先验概率。

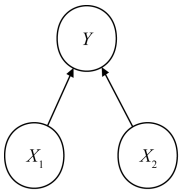
(5)根节点与叶节点、叶节点与叶节点之间的依赖关系,即条件概率表,如图 5 所示。

2 基于 STPA 的致因分析

根据美国捷蓝航空 A320 事故信息建立襟翼系统控制结构模型,分析系统控制流,捕获系统的不安全控制行为,以识别出导致不安全控制行为的潜在致因场景。

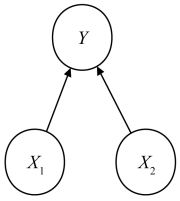
2.1 事故概述

2012 年 6 月 17 日,美国捷蓝航空一架 A320 飞



$P(X_1)$	$P(X_2)$	$P(Y\|X_1、X_2)$
1	1	1
1	0	1
0	1	1
0	0	0

(a)“or”关系条件概率表



$P(X_1)$	$P(X_2)$	$P(Y\|X_1、X_2)$
1	1	1
1	0	0
0	1	0
0	0	0

(b)“and”关系条件概率表

0 为正常;1 为故障

图 5　贝叶斯网络节点依赖关系

Fig. 5　Bayesian network node dependencies

机在从拉斯维加斯出发后不久,飞机由于液压系统泄露,导致襟翼系统告警并失去控制。飞行员紧急处置,最终飞机实现紧急着陆,液压系统损坏,未发生人员伤亡。美国国家交通安全委员会在事故报告中给出了事故过程和原因,具体如下。

(1)事故过程。飞机从拉斯维加斯麦卡伦国际机场起飞后不久,由于绿色液压系统泄漏导致压力下降,随后动力传输组件过热并失效,导致黄色液压系统也失去压力。飞机失去两个液压系统后,襟翼无法操作,刹车和前轮转向功能受限,飞控系统切换到备用模式。机组人员选择在 3 600 m 的高度保持等待,燃烧燃油减轻飞机重量,并与地面控制人员、维修人员和调度人员沟通。最终,飞机在黄色液压源恢复后实现紧急着陆,没有造成人员伤亡。

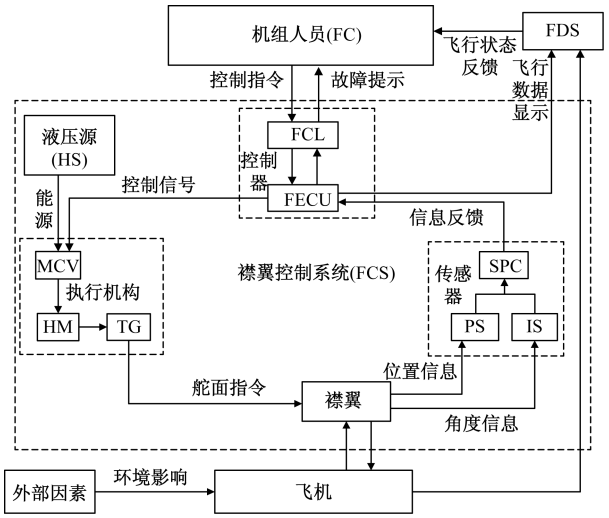
(2)事故原因。绿色液压系统软管发生泄漏,导致动力传输单元长时间运行并超温失效,随后黄色液压系统压力下降,导致黄绿液压源全部失效,控制通道全部失效。此外,飞机在起飞前有一个襟翼控制通道失效,但根据美国联邦航空管理局(Federal Aviation Administration,FAA)批准的最小设备清单进行延期维护。

2.2　控制结构模型建立

(1) 定义系统级事故。机组人员及乘客伤亡(记为 A-1)、飞机结构完整性受损(记为 A-2)和地面设施或建筑损坏(记为 A-3)。

(2) 定义系统级危险。飞机在进近时速度过大(记为 H-1)、飞行员失去控制飞机的能力(记为 H-2)和飞机偏离或冲出跑道(记为 H-3)。

(3) 安全控制结构建模。对飞机飞行过程中襟翼功能直接关联的物理部件、控制系统、机组人员以及环境因素进行分析,建立飞机降落过程中的襟翼控制系统安全控制结构模型。如图 6 所示,控制结构建模涉及的有控制器、液压源、执行机构、传感器、襟翼、机组人员和环境因素等。



襟翼控制杆(flap control lever, FCL);襟翼电子控制单元(flap electronics control unit, FECU);液压源(hydraulic source, HS);主控阀(main control valve, MCV);液压马达(hydraulic motor, HM);传动机构(transimission gear, TG);位置传感器(position sensor, PS);倾斜传感器(inclination sensor, IS);信号处理电路(signal processing circuitry, SPC);飞行显示系统(flight display system, FDS)

图 6　安全控制结构模型

Fig. 6　Security control structure model

机组人员 FC 是整个系统的输入端,并通过控制杆 FCL 对襟翼控制系统进行操作;襟翼电子控制单元 FECU 接收 FCL 的输入指令并进行处理,通过电信号将得到的控制指令传递给主控阀;主控阀 MCV 控制液压油的流向和压力,从而驱动液压马达;液压马达 HM 通过液压油在马达内部施加压力,推动马达内部的机械组件旋转,转化为机械运动,进而通过传动机构 TG 使得执行元件的移动转化为襟翼的角度和位置变化。位置传感器 PS 和倾斜传感器 IS 收集襟翼的位置和角度等信息,经过信号处理电路 SPC 处理后,反馈给襟翼电子控制单元 FECU,驾驶舱的飞行显示系统 FDS 将飞行状态信息反馈给机组人员 FC。

2.3　UCA 识别

基于控制结构分析每个控制动作,以了解它可能导致危险的方式。根据 STPA 分析指导对每个控制动作考虑以下 4 个问题:①提供这种控制措施如何导致危险?②不提供这种控制措施如何导致危险?③过早/过晚提供此控制措施如何导致危险?④提供此控制操作的时间过长或停止过早会如何导致危险?针对捷蓝航空空客 A320 飞机事故,基于以上 4 种危险场景分析给出 UCA,如表 1 所示。

表 1 进近过程襟翼系统 UCA

Table 1 UCA of the flap system during the approach process

控制行为	提供错误的控制行为 UCA-1		未提供控制行为 UCA-2		过早/过晚提供此控制行为 UCA-3		控制操作的时间过长或停止过早 UCA-4	
	编号	详情	编号	详情	编号	详情	编号	详情
进近过程	UCA-1.1	飞行员正确操作后,襟翼偏转角度或位置错误,并未反馈告警信息	UCA-2.1	飞行员正确操作后,襟翼未发生偏转,并反馈告警信息	UCA-3.1	飞行员正确操作后,襟翼偏转延迟	—	—
	UCA-1.2	飞行员正确操作后,襟翼偏转角度或位置正确,反馈告警信息	UCA-2.2	飞行员正确操作后,襟翼未发生偏转,并未反馈告警信息	UCA-3.2	襟翼偏转角度或位置错误,告警信息反馈延迟	—	—

表 2 UCA-2.1 对应的潜在致因场景

Table 2 Potential cause scenarios corresponding to UCA-2.1

编号	潜在致因场景内容
Pcs-1	襟翼控制手柄 FCL 故障,导致输出错误的控制命令/未能输出控制命令
Pcs-2	襟翼电子控制单元 FECU 故障,导致输出错误的控制命令/未能输出控制命令
Pcs-3	襟翼控制功能故障,导致输出错误的控制指令/未输出控制指令
Pcs-4	液压源 HS 故障,导致执行机构接收错误的控制指令/未接受控制指令
Pcs-5	主控阀 MCV 故障,导致输出错误的控制命令/未输出控制命令
Pcs-6	液压马达 HM 故障,导致输出错误的舵面指令/未输出舵面指令
Pcs-7	传动机构 TG 故障,导致襟翼执行错误的舵面面指令/未执行舵面指令
Pcs-8	襟翼执行机构故障,导致襟翼执行错误的舵面指令/未执行舵面指令
Pcs-9	位置传感器 PS 故障,导致输出错误的位置信息/丢失位置信息
Pcs-10	倾斜传感器 IS 故障,导致输出错误的角度信息/丢失角度信息
Pcs-11	信号处理电路 SPC 故障,导致输出错误反馈信号/丢失反馈信号
Pcs-12	襟翼传感器功能故障,导致未反馈/反馈错误的状态信息

2.4 致因场景识别

识别出控制行为变得不安全的所有方式后,就可以识别可能导致此类不安全控制行为的场景。根据事故调查,以 UCA-2.1“飞行员正确操作后,襟翼未发生偏转,并反馈告警信息”为例,根据图 2 所描述的通用致因因素得到以下潜在致因场景(potential causal scenario, PCS),如表 2 所示,展开进一步分析。

最终得到共 12 个关于 UCA-2.1 的致因场景(Pcs1 ~ Pcs12),其中与控制器相关的致因场景有 3 个(Pcs1 ~ Pcs3),与液压源有关的致因场景为 Pcs4,与执行机构相关的致因场景有 4 个(Pcs5 ~ Pcs8),与传感器相关的致因场景有 4 个(Pcs9 ~ Pcs12)。

3 基于 BN 的风险评估

3.1 贝叶斯统计

贝叶斯统计是一种基于贝叶斯定理的数据分析方法,其中有关统计模型中参数的可用知识会根据观测数据中的信息进行更新。假设一个贝叶斯网络包含一系列的变量(X_i,X_a,…,X_n),那么对于这个网络中任何变量 X_i($i=1,2,\cdots,n$),给定其父变量 Parents(X_i)的情况下 X_i的条件概率可以从网络直接获得,通过链式规则来定义,可表示为

$$P(X_1,X_2,\cdots,X_n)=\prod_{i=1}^{n}[P(X_i\mid \mathrm{Parents}(X_i))] \tag{1}$$

历史知识被表示为先验概率,并以似然函数的形式与观测数据相结合,以确定后验概率[12]。逆向分析表达式为

$$P(A\mid B)=\frac{P(A)P(B\mid A)}{P(B)} \tag{2}$$

式(2)中:$P(A)$为 A 的先验概率;$P(A|B)$为已知 B 发生后 A 的条件概率,也称为 A 的后验概率;$P(B|A)$为给定变量 A 的情况下,观察到证据 B 的概率,也称为似然;$P(B)$为 B 的先验概率,这里称为标准化常量。

3.2 贝叶斯网络模型建立

通过分析发现,与 UCA-2.1 相关的致因场景由 9 个组件/模块组成:FCL、FECU、MCV、HS、HM、TG、PS、IS 和 SPC。根据系统的安全控制结构和 BN 模型转换规则,转换得到 UCA-2.1 的 BN 模型,如图 7 所示。

UCA-2.1 向下与直接相关致因场景相连,这些节点作为导致UCA发生的直接因素,直接致因再向

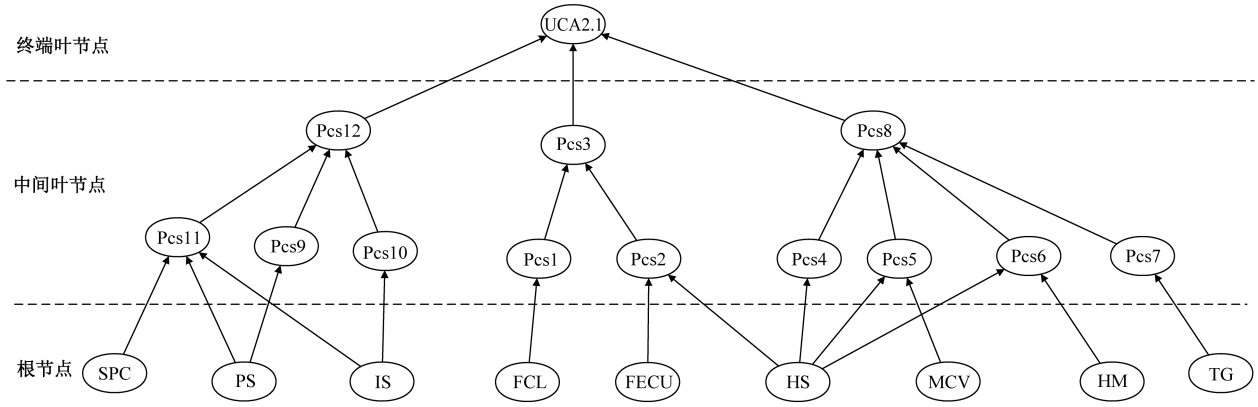


图 7　UCA-2. 1 贝叶斯网络结构模型

Fig. 7　Bayesian network structure model ofUCA-2. 1

表 3　终端叶节点条件概率

Table 3　Terminal leaf node conditional probability

中间叶节点			终端叶节点 UCA-2. 1
Pcs3	Pcs8	Pcs12	
1	1	1	1
1	1	0	1
1	0	1	1
0	1	1	1
0	1	0	1
0	0	1	1
1	0	0	1
0	0	0	0

表 4　中间叶节点条件概率(传感器部分)

Table 4　Intermediate leaf node conditional probability table(sensor part)

Pcs9	Pcs10	Pcs11	Pcs12
1	1	1	1
1	1	0	1
1	0	1	1
0	1	1	1
0	1	0	1
0	0	1	1
1	0	0	1
0	0	0	0

表 5　中间叶节点条件概率(控制器部分)

Table 5　Intermediate leaf node conditional probability table(controller part)

Pcs1	Pcs2	Pcs3
1	1	1
1	0	1
0	1	1
0	0	0

下与间接致因场景相连,它们共同作为中间叶节点,之间的依赖关系见条件概率,如表 3 ~ 表 6 所示;最后,中间叶节点涉及的物理组件作为网络的根节点。

表 6　中间叶节点条件概率(执行机构部分)

Table 6　Intermediate leaf node conditional probability table(actuator part)

Pcs4	Pcs5	Pcs6	Pcs7	Pcs8
1	1	1	1	1
1	1	1	0	1
1	1	0	1	1
1	0	1	1	1
0	1	1	1	1
1	1	0	0	1
1	0	1	0	1
1	0	0	1	1
0	1	0	1	1
0	1	1	0	1
0	0	1	1	1
1	0	0	0	1
0	1	0	0	1
0	0	1	0	1
0	0	0	1	1
0	0	0	0	0

3.3　UCA 定量分析

贝叶斯网络的定量分析包括预测和诊断分析[13],预测分析与故障树分析相似,基于已知根节点(基本事件)的先验概率,通过节点之间的条件概率关系来计算任意节点发生的后验概率,其中先验概率值一般来自元部件综合计算和故障数据统计。

根据 2. 2 节所定义的进近场景中襟翼控制系统的 UCA 可能导致相应的事故和危险,可能导致的危险有 H-1、H-2 和 H-3,可能导致的事故有 A-1、A-2 和 A-3。组件故障率数据来源于文献[14-17],将先验概率值赋给相应的根节点,配置相关的先验概率表,如表 7 所示。

基于各根节点先验概率,通过式(1)正向推理计算,可得 UCA-2. 1“通告的襟翼功能丧失”发生概率为 $2.078\ 98 \times 10^{-5}$/飞行小时。

表 7 根节点先验概率

Table 7 Prior probability of the root node

节点名称	先验概率	节点名称	先验概率
SPC	2.0×10^{-8}	HS	7.7×10^{-6}
PS	1.2×10^{-6}	HM	6.8×10^{-7}
IS	2.0×10^{-6}	MCV	1.6×10^{-6}
FCL	4.9×10^{-7}	TG	5.2×10^{-6}
FECU	1.9×10^{-6}		

注:先验概率表示单位飞行小时的发生概率。

3.3.1 致因场景影响度分析

为了探究各致因场景对 UCA-2.1 的影响,通过式(2)对与 UCA-2.1 相关的致因链做逆向推理计算,得到每一个致因场景的后验概率,如图 8 所示。

分析可知,导致 UCA-2.1 的直接致因场景按照影响程度从大到小依次为 Pcs8 > Pcs3 > Pcs12,间接致因场景影响程度从大到小依次为:Pcs2 > Pcs5 > Pcs6 > Pcs4 > Pcs7 > Pcs11 > Pcs10 > Pcs9 > Pcs1,即襟翼执行机构和襟翼控制器的功能故障对襟翼正常工作影响最大。分析产生这种结果的原因在于:①执行机构是襟翼控制系统中将飞行员或控制器输入指令转化为襟翼实际机械运动的核心组成部分,对于襟翼的正常功能至关重要;②襟翼控制器作为枢纽,负责将飞行员的指令转换为电信号,驱动执行机构来调整襟翼的位置。因此执行机构和控制器的失效对于 UCA-2.1 的贡献较大,相关致因场景有着较高的后验概率。

进一步分析系统中不同组件对 UCA-2.1 的影响,对贡献度最高的致因场景 Pcs8 和 Pcs3 中相关联的组件进行后验概率计算并分析与先验概率之间的差异(单位:每 10 000 飞行小时)。相关根节点后验概率数值如表 8 所示,后验概率与先验概率之间的差异如图 9 所示。

后验概率与先验概率之间的差异越大,说明根节点对 UCA-2.1 的影响更大[18]。结果表明,各组件对不安全控制行为的影响排序为:HS > TG > FECU > MCV > HM > FCL,即液压源、传动机构和电控单元对襟翼正常工作影响较大。根据以上分析结果分析可知:①液压源作为执行机构的动力来源,对UCA-2.1的影响最大,概率差值为0.293;

表 8 相关根节点后验概率

Table 8 Correlated root node posterior probability

根节点	后验概率
FCL	0.023 6
FECU	0.091 4
MCV	0.077 0
HS	0.370 0
HM	0.032 7
TG	0.250 0

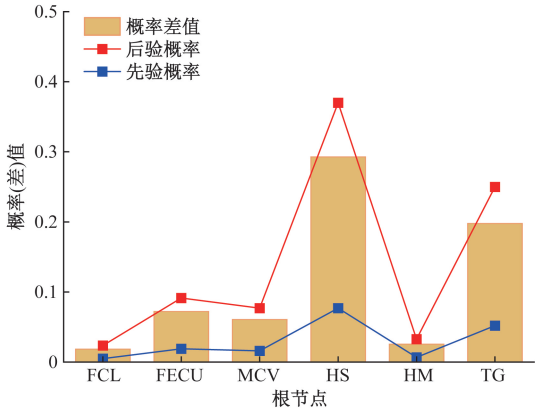


图 9 先验概率与后验概率及差值

Fig. 9 Difference between posterior and prior probability

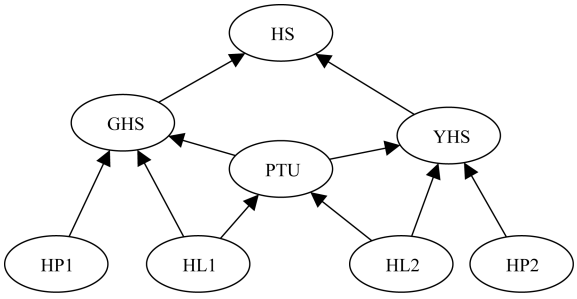
②传动机构负责将执行机构的动力转换为襟翼的物理移动,确保襟翼功能的高效执行,概率差值为0.198;③襟翼电子控制单元接受控制杆的操纵指令,以电信号形式传递给执行机构,概率差值为0.072 4。

3.3.2 组件重要度分析

基于以上致因场景影响度分析的结论,对影响最大的组件——液压源展开深入分析以探究事故的主要根源。根据液压源 HS 的工作原理建立相应的 BN 模型并对相关组件进行关键重要度分析。

BN 模型如图 10 所示,液压源 HS 向下与黄/绿色液压源之间,黄/绿色液压源向下与液压泵、液压管路和动力传输组件之间均以“or”关系相连,即任一子节点失效,父节点功能都会受到影响。

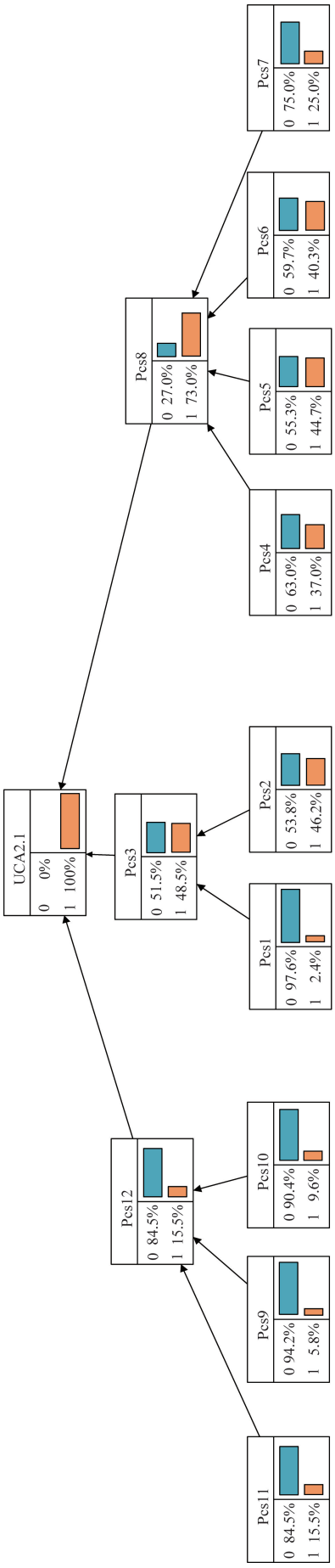
关键重要度反映了根节点失效概率的变化程度与因其失效使得叶节点失效概率变化程度的比值,关键重要度越大,说明对相应部件采取措施时,能够大概率减少风险事件的发生,计算公式为



黄色液压源(yellow hydraulic source, YHS);绿色液压源(green hydraulic source, GHS);动力传输组件(power transmission unit, PTU);液压泵(hydraulic pump, HP);液压管路(hydraulic line, HL)

图 10 液压源 BN 模型

Fig. 10 Bayesian network model of hydraulic source



状态0代表事件未发生;状态1代表事件发生

图8　UCA-2.1发生条件下各致因场景后验概率

Fig.8　Posterior probability of each potential causal scenario under UCA-2.1 condition

$$I(X_i) = \{P(X_i = 1)[P(Y = 1 \mid X_i = 1) - P(Y = 1 \mid X_i = 0)]\}[P(Y = 1)]^{-1} \quad (3)$$

根据式(3)计算分别得到各组件对于液压源 HS[图 11(a)]和黄色液压源 YHS[图 11(b)]的关键重要度,如图 11 所示。

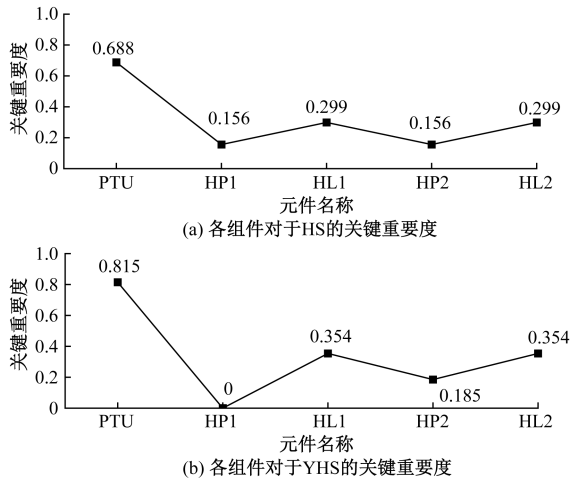


图 11 组件关键重要度对比

Fig. 11 Comparison of key importance of components

计算后的关键重要度数值在 0 ~ 1,数值越大说明该组件故障对(黄色)液压源故障的贡献程度越大。如图 11 所示,各组件对液压源 HS 的关键重要度从高到低排序为:PTU > HL1 = HL2 > HP1 = HP2,对黄色液压源 YHS 的关键重要度从高到低排序为:PTU > HL1 = HL2 > HP2 > HP1,即动力传输组件和液压管路的重要度较高。

由图 11(a)可知,动力传输组件 PTU 是液压系统中至关重要的组件,负责在黄绿液压系统之间平衡液压压力,确保系统的正常运作,对于液压系源 HS 的关键重要度高达 0.688;液压管路 HL1 和 HL2 是飞机液压系统的“血管”,负责将液压油从泵输送到飞机各个液压设备,对液压源 HS 的关键重要度为 0.299。

由图 11(b)可知,黄色液压管路 HL2 和绿色液压管路 HL1 对黄色液压源具有同等影响(重要度均为 0.354);绿色管路 HL1 的泄露会导致黄色液压源的失效的原因是在绿色液压源压力较低的情况下交互组件“动力传输组件 PTU”超负荷工作导致故障,而 PTU 的失效进而导致黄色液压源内部压力失衡(PTU 对黄色液压源的重要度为 0.815)。

3.4 结果对比与验证

为了确保 STPA-Bayes 的概率计算的准确性,将其与马尔可夫过程(Markov process,MP)的分析结果进行比较,表 9 为各个状态的解释。

表 9 各状态说明

Table 9 Description of each state

状态	状态说明	状态	状态说明
Safe	无故障状态	GH2	GHS 中 HP 故障
C1	FECU 功能失效	GH3	GHS 中 HL、HP 同时故障
C2	FCL 功能失效	YH1	YHS 中 HL 故障
C3	FECU、FCL 功能同时失效	YH2	YHS 中 HP 故障
A1	MCV/功能失效	YH2	YHS 中 HL、HP 同时故障
A2	TG 功能失效	A1	IS 功能失效
A3	HM 功能失效	A2	PS 功能失效
A4	TG、HM 功能同时失效	A3	SPC 功能失效
A5	MCV、HM 功能同时失效	A4	PS、SPC 功能同时失效
A6	MCV、TG 功能同时失效	A5	IS、SPC 功能同时失效
A7	MCV、TG、HM 功能全部失效	A6	IS、PS 功能同时失效
PTU	PTU 功能失效	A7	IS、PS、SPC 功能全部失效
GH1	GHS 中 HL 故障		

由表 9 可知,系统包括初始无故障状态在内共有 25 个状态,通过马尔可夫链对襟翼控制系统相关组件进行建模并计算,得到襟翼功能丧失的状态概率为 $2.079\ 002\ 19 \times 10^{-5}$/FH,Markov 链模型如图 12 所示。

将两种方法的计算结果进行对比,二者的误差值为 2.2×10^{-10},表明所采用的 STPA-Bayes 模型从转换到定量计算的过程和结果的正确性,能够有效对 UCA 进行定量分析。

4 安全建议及案例对比

4.1 STPA-Bayes 安全建议

通过上述 STPA-Bayes 的致因分析和风险评估方法对襟翼控制系统安全性进行审视,从系统和因果角度考虑可能的故障及故障间的交互特性,分析给出以下建议。

(1)在致因场景影响度分析中,液压源 HS、传动机构 TG 和电控单元 FECU 具有较高的概率差值(分别为 0.293、0.198 和 0.072 4)。因此建议:①引入冗余备份,通过增设液压系统和备用液压管路,提升系统对故障的恢复能力,减少单点故障带来的风险;②加强维护与检查,定期进行传动机构 TG 的维护检查,提前发现潜在问题并采取措施;③优化控制链路,增加电控单元 FECU 的控制通道并采用信号表决机制,不仅增强控制系统的鲁棒性,还能容错处理错误的输入数据,减少连锁反应带来的一系列风险。

(2)在组件重要度分析中,PTU 都有着较高的重要度(分别为 0.688 和 0.815),并且 PTU 的失效也会导致黄绿液压源之间产生影响(HL1 对 YHS 的重要度为 0.354)。因此建议:①优化控制策略,改

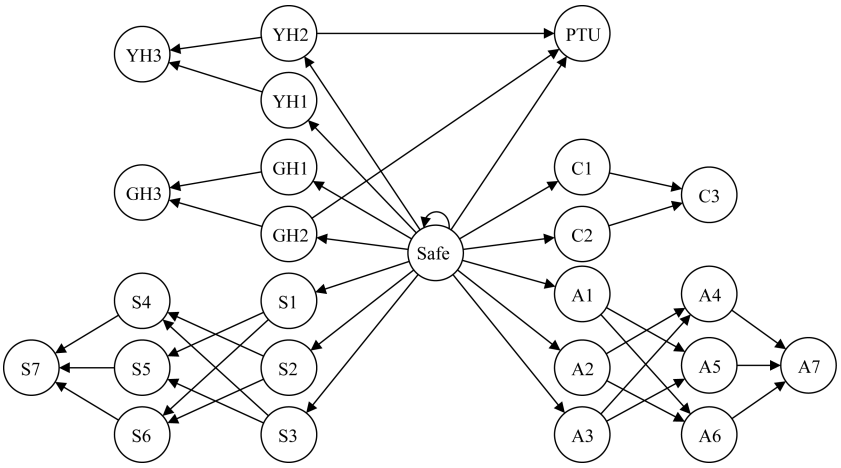


图 12　襟翼控制系统马尔可夫链

Fig. 12　Markov chain for the flap control system

进动力传输组件 PTU 的控制逻辑,使其能够在长时间超负荷工作中自动停止,防止过热而导致失效;②增加告警与监控,实时监控 PTU 的工作状态,监测其温度和压力,确保它们在正常范围内,并在超出阈值时及时发出告警信号。

4.2　安全建议对比

NTSB 针对这起事故提出以下安全建议。

(1)A-13-019。要求 FAA 重审其规定,以确保飞行员在起飞后能及时接收到动力传输装置(PTU)激活的警告,从而有效应对液压系统故障。

(2)A-13-020。建议 FAA 确保航空公司能够快速响应并执行服务通告,以进行必要的维护,防止未来的故障。

(3)A-13-021。要求空中客车公司审查并改进其液压系统设计,以便飞行机组在系统故障时能接收到及时、清晰的警告信息。

综上可知,STPA-Bayes 和 NTSB 都从系统级的角度出发,强调了液压系统及动力传输组件 PTU 的重要性,要求机组成员做好定期的维护和检查,并且增加详细的故障提示,以便及时发现故障迹象来预防危险事件。区别在于:STPA-Bayes 考虑的更全面和具体,通过控制理论和可靠性理论,额外强调了余度管理在襟翼控制系统的关键作用。在据致因场景影响度分析中,STPA 的优势得以体现,它能够全面地识别出所有潜在的致因场景,确保了分析的完整性。根据分析结果,建议增强液压系统与控制器通道的余度设计,以防止单点故障对系统的影响。在组件重要度分析中,贝叶斯网络展现了其独特的优势,它能够直观地建模出系统内部各组件间的交互关系。根据分析结果,建议对 PTU 的控制逻辑进行优化,并增强其状态监控与告警功能,以防止因过热失效而导致的双液压源同时失效的风险。

4.3　案例分析对比

随着中国民航业的快速发展,航空安全问题日益受到重视。2018 年 10 月 25 日,执行福州-重庆-拉萨任务的厦门航空 MF8411 航班[执飞该航班的是波音 737-700 型客机(编号 B5278)]在到达目的地前出现襟翼卡阻,导致飞机无法减速和爬升,最终机组启动应急措施,在拉萨机场上空盘旋减重,最终于 14:53 分安全着陆,机上旅客、机组 88 人无人伤亡[19]。该事故的类型与捷蓝航空事故有相似之处,但也存在一些差异,襟翼的卡阻可能由多种原因导致,通过对比分析可以更全面地理解航空事故的复杂性和多样性。

在航空襟翼卡阻事件中,机组凭借专业的应急处置能力成功化解了危机,但此类事件也凸显了航空系统中潜在的安全隐患。STPA-Bayes 方法作为一种先进的安全分析方法,能够从系统层面深入剖析此类事故的成因,揭示襟翼卡阻可能涉及的系统设计缺陷、维护不足以及操作流程中的潜在风险。在确保系统安全的同时,还提供了针对性的改进建议,凸显了该方法相较于传统安全分析手段的显著优越性。

5　结论

采用的 STPA-Bayes 分析方法可以为航空事故的致因分析与风险评估提供支持,有效性也通过传统方法得到验证,且提出的安全建议可以帮助系统改进,以降低系统中潜在的风险并提高系统安全性。得出如下结论。

(1)在致因分析上,STPA 可以全面地识别襟翼控制系统中的薄弱环节,从执行机构、控制器和传感器 3 个方面出发,分析故障/错误传播路径,探究引发事故的潜在因素。

(2)在风险评估上,贝叶斯网络可以量化评估航空事故风险,以形式化方式建模并描述组件之间的交互关系,得出导致事故的主要因素为液压源故障,而 PTU 故障和液压管路泄漏是导致液压源失效的主要原因,关键重要度分别为 0.688 和 0.299。

参 考 文 献

[1] 张晗, 王强. 基于有向网络的航空安全事故风险识别与评估[J]. 系统工程与电子技术, 2024, 46(6): 1995-2001.
Zhang Han, Wang Qiang. Aviation safety accident risk identification and evaluation basedondirected networks[J]. Systems Engineering and Electronics, 2024, 46(6): 1995-2001.

[2] 张光炯, 孙军帅. 民用飞机高升力系统设计中安全性评估方案研究[J]. 航空工程进展, 2020, 11(2): 286-292.
Zhang Guangjiong, Sun Junshuai. Research on the safety assessment scheme applied to civil aircraft high lift system[J]. Advances in Aeronautical Science and Engineering, 2020, 11(2): 286-292.

[3] Sadeghi R, Goerlandt F. A proposed validation framework for the system theoretic process analysis (STPA) technique[J]. Safety-Science, 2023, 162: 106080.

[4] 郑磊, 胡剑波. 基于 STAMP/STPA 的机轮刹车系统安全性分析[J]. 航空学报, 2017, 38(1): 241-251.
Zheng Lei, Hu Jianbo. Safety analysis of wheel brake system based on STAMP/STPA[J]. Acta Aeronautica ET Astronautica Sinica, 2017, 38(1): 241-251.

[5] Liu T. Safety analysis of civil aviation flight and UAV operation based on STAMP/STPA[C]//E3S Web of Conferences. Paris: EDP Sciences, 2024, 512: 03033.

[6] 吕旭飞, 姚尚宏, 权家乐. 基于 STPA 法的空中加油软管甩鞭安全性分析[J]. 中国安全科学学报, 2022, 32(2): 152-157.
Lü Xufei, Yao Shanghong, Quan Jiale. Safety analysis on HWP in aerial refueling based on STPA[J]. China Safety Science Journal, 2022, 32(2): 152-157.

[7] 李航, 聂芳艺. 基于贝叶斯网络的物流无人机碰撞风险评估[J]. 科学技术与工程, 2023, 23(15): 6700-6706.
Li Hang, Nie Fangyi. Collision risk assessment of logistics UAV based on Bayesian network[J]. Science Technology and Engineering, 2023, 23(15): 6700-6706.

[8] 汪磊, 孙景陆, 王文超, 等. 基于 QAR 数据的着陆超限风险贝叶斯网络分析模型[J]. 安全与环境学报, 2023, 23(1): 26-34.
Wang Lei, Sun Jinglu, Wang Wenchao, et al. Bayesian network analysis model on landing exceedance risk based on flight QAR data[J]. Journal of Safety and Environment, 2023, 23(1): 26-34.

[9] 张晓全, 马晗. 基于贝叶斯网络的电动垂直起降航空器运行风险研究[J]. 科学技术与工程, 2022, 22(36): 16269-16276.
Zhang Xiaoquan, Ma Han. Operation risk of electric vertical takeoff and landing aircraft based on Bayesian network[J]. Science Technology and Engineering, 2022, 22(36): 16269-16276.

[10] Borges S F D S, Albuquerque M A F D, Cardoso M M, et al. Systems theoretic process analysis(STPA): a bibliometric and patents analysis[J]. Management & Production, 2021, 28(2): e5073.

[11] Marcot B G, Penman T D. Advancesin Bayesian network modelling: integration of mode-lling technologies[J]. Environmental Modelling & Software, 2019, 111: 386-393.

[12] Kitson N K, Constantinou A C, Guo Z, et al. A survey of Bayesian network structure learning[J]. Artificial Intelligence Review, 2023, 56(8): 8721-8814.

[13] Zhang D, Liu Q, Yan H, et al. A matrix analytic approach for Bayesian network modeling and inference of a manufacturing system[J]. Journal of Manufacturing Systems, 2021, 60: 202-213.

[14] 杨志丹. 民用飞机高升力控制系统的设计和安全性分析研究[D]. 上海: 上海交通大学, 2014.
Yang Zhidan. The research on design and safety analysis of civil aircraft high lift control system[D]. Shanghai: Shanghai Jiao Tong University, 2014.

[15] Ma J, Duan F. Application of GO methodology in reliability analysis of aircraft flap hydraulic system[J]. The Aeronautical Journal, 2020, 124(1272): 257-270.

[16] 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.
Li Jinxiang. Design and research of high lift control system for a certain aircraft based on safety[D]. Hangzhou: Zhejiang University, 2020.

[17] Zhou C, Chang Q, Zhao H, et al. Fault tree analysis with interval uncertainty: a case study of the aircraft flap mechanism[J]. IEEE Transactions on Reliability, 2020, 70(3): 944-956.

[18] Xu J, Tian W, Kan L, et al. Safety assessment of transport aircraft heavy equipment airdrop: an improved STPA-BN mechanism[J]. IEEE Access, 2022, 10: 87522-87534.

[19] 央广网. 厦航 MF8411 航班因襟翼系统故障迫降拉萨 人机平安[EB/OL]. (2018-10-26)[2024-07-01]. https://baijiahao.baidu.com/s?id=1615352671000932368&wfr=spider&for=pc.
CNR News. Xiamen Airlines Flight MF8411 made an emergency landing in Lhasa due to a flap system malfunction, ensuring the safety of both the aircraft and the crew[EB/OL]. (2018-10-26)[2024-07-01]. https://baijiahao.baidu.com/s?id=1615352671000932368&wfr=spider&for=pc.