

学校代码：10485  
密 级：

分类号：V275;V242  
UDC：629.7



鄭州航空工業管理學院

硕士学位论文

基于 STPA-BT-FBN 的 eVTOL 电池热失控安全风险分  
析与评价研究

姓 名：户志浩

学 号：2023022015

学 院：管理工程学院

学科、专业：交通运输

导师及职称：赵 健 教授（校内）

郭俊鹏 工程师（校外）

2026 年 4 月

# Safety Risk Analysis and Evaluation of Battery Thermal Runaway for eVTOL Based on STPA-BT-FBN

Dissertation Submitted to  
**Zhengzhou University of Aeronautics**  
in partial fulfillment of the requirement  
**for the degree of Master**

by  
**Hu Zhihao**

**Transportation Engineering**  
Dissertation Supervisor: Professor Zhao Jian  
Engineer Guo Junpeng

**Apr, 2026**

### 独创性声明

本人声明所呈交的学位论文是本人在导师指导下进行的研究工作和取得的研究成果，除了文中特别加以标注和致谢之处外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得郑州航空工业管理学院或其他教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示了谢意。

学位论文作者签名：                    签字日期：        年    月    日

## 学位论文版权使用授权书

本学位论文作者完全了解郑州航空工业管理学院有关保留、使用学位论文的规定。特授权郑州航空工业管理学院可以将学位论文的全部或部分内容编入有关数据库进行检索，提供阅览服务，并采用影印、缩印或扫描等复制手段保存、汇编以供查阅和借阅。同意学校向国家有关部门或机构送交论文的复印件和磁盘。

（保密的学位论文在解密后适用本授权说明）

学位论文作者签名：

导师签名：

签字日期：      年    月    日

签字日期：      年    月    日

## 摘 要

电动垂直起降飞行器（electric Vertical Take-Off and Landing, eVTOL）作为一种新型的城市空中交通系统的重要载体，凭借绿色低碳、高机动性与垂直起降能力等多重优势，在城市通勤、物流运输、应急响应、巡检作业等多个场景中展现出广阔的商业化前景。新能源电池作为 eVTOL 的核心动力来源，其安全性直接影响到飞行器运行的可靠性和安全性。然而，随着 eVTOL 产业的快速发展，已有多起电池热失控事故发生，对飞行器安全运行造成了严重威胁。电池热失控及由此引发的起火、爆炸等事故已成为新能源交通工具领域的主要风险之一。由于 eVTOL 同样依赖高能量密度电池系统，其电池热失控风险对飞行安全同样构成了严峻的挑战，并严重制约了 eVTOL 的安全运行与规模化推广。因此，本文针对 eVTOL 电池热失控进行风险分析与评价研究。

针对 eVTOL 电池系统在高能量密度、多工况耦合作用下易发生热失控的问题，首先从系统工程视角出发，结合其结构组成、运行环境及能量传递特性，对电池热失控的发生机理及演化过程进行系统分析。在此基础上，引入系统理论过程分析（System Theoretic Process Analysis, STPA）方法，从“控制—反馈”闭环结构出发，识别电池管理系统、热管理系统及运行操作过程中的不安全控制行为（Unsafe Control Actions, UCAs），并进一步挖掘其对应的致因场景与潜在约束缺失。在完成风险因素系统识别后，进一步结合 Bow-tie 模型的结构化优势，将 STPA 识别得到的致因因素与控制失效路径映射至“致因—顶事件—后果”的事故链框架中，构建 eVTOL 电池热失控的全过程演化路径模型，实现从初始诱因到事故后果的完整逻辑表达。该过程不仅提升了风险识别的系统性与完整性，也为后续定量建模提供了清晰的结构基础与路径支撑。

在上述事故链结构的基础上，进一步将 STPA-Bow-tie 模型进行形式化转化，构建 eVTOL 电池热失控的模糊贝叶斯网络（Fuzzy Bayesian Network, FBN）模型。通过将 Bow-tie 结构中的基本事件、中间事件及顶事件映射为贝叶斯网络中的节点，并依据逻辑关系建立节点间的因果依赖结构，实现从定性事故链到定量概率网络的转化。考虑到 eVTOL 领域实际运行数据有限且存在较强不确定性，本文引入模糊数学理论与专家评估方法，对关键节点的先验概率及条件概率进行模糊化处理与量化表达，从而有效缓解数据不足问题，提高模型的适用性与鲁棒性。在此基础上，利用贝叶斯网络的概率推理机制，开展正向推理与反向推理，实现电池热失控风险状态的动态更新。同时，通过敏感性分析识别对顶事件影响显著的关键因素与关键路径，为风险控制提供定量依据。

为验证所构建模型的有效性与工程适用性，选取典型 eVTOL 电池系统作为研

究对象，构建具体的贝叶斯网络实例并开展案例分析。基于实际系统结构与运行参数，对模型进行实例化建模，并通过仿真计算开展多场景下的风险推演分析。通过对模型进行正向推理、诊断推理及敏感性分析，系统识别影响电池热失控的关键风险因素及其作用路径，揭示多因素耦合作用下的事故演化机制。在此基础上，从电池设计优化、热管理强化、运行控制策略改进及应急处置机制等多个层面，提出针对性的风险管控措施与系统优化策略。

**关键词：**电动垂直起降飞行器；电池热失控；系统理论过程分析；因果模型；动态贝叶斯模型；

**分类号：**[V275;V242]

## Abstract

Electric Vertical Take-Off and Landing (eVTOL) aircraft, as an important carrier of emerging urban air mobility systems, have demonstrated broad commercial prospects in scenarios such as urban commuting, logistics transportation, emergency response, and inspection operations, owing to their advantages of low carbon emissions, high maneuverability, and vertical take-off and landing capability. As the core power source of eVTOL, new energy batteries directly determine the reliability and operational safety of the aircraft. However, with the rapid development of the eVTOL industry, multiple battery thermal runaway incidents have occurred, posing severe threats to flight safety. Thermal runaway and the resulting fire and explosion hazards have become one of the major risks in new energy transportation systems. Since eVTOL systems rely heavily on high energy-density battery systems, thermal runaway presents a critical challenge to flight safety and significantly restricts the safe operation and large-scale deployment of eVTOL. Therefore, this study focuses on the risk analysis and assessment of battery thermal runaway in eVTOL systems.

To address the susceptibility of eVTOL battery systems to thermal runaway under high energy density and multi-operating-condition coupling, this study first adopts a systems engineering perspective. By considering system structure, operational environment, and energy transfer characteristics, the occurrence mechanism and evolution process of battery thermal runaway are systematically analyzed. On this basis, the System-Theoretic Process Analysis (STPA) method is introduced to identify Unsafe Control Actions (UCAs) from the “control–feedback” closed-loop perspective, focusing on battery management systems, thermal management systems, and operational processes. Corresponding causal scenarios and potential constraint deficiencies are further extracted. After completing the systematic identification of risk factors, the structural advantages of the Bow-tie model are leveraged to map the identified causal factors and control failure paths into an integrated “cause–top event–consequence” accident chain framework. This enables the construction of a full-process evolution model for eVTOL battery thermal runaway, achieving a complete logical representation from initial triggers to accident consequences. This process enhances the systematicity and completeness of risk identification and provides a clear structural foundation for subsequent quantitative modeling.

Based on the constructed accident chain structure, the STPA–Bow-tie model is

further formalized into a Fuzzy Bayesian Network (FBN) model for eVTOL battery thermal runaway. By mapping basic events, intermediate events, and the top event in the Bow-tie structure into nodes of the Bayesian network, and establishing causal dependencies according to logical relationships, the transformation from a qualitative accident chain to a quantitative probabilistic network is achieved. Considering the limited availability of operational data and the inherent uncertainty in the eVTOL domain, fuzzy mathematics and expert judgment methods are introduced to quantify prior and conditional probabilities of key nodes. This effectively mitigates data scarcity and improves the applicability and robustness of the model. Furthermore, leveraging the probabilistic inference capability of Bayesian networks, both forward and backward reasoning are conducted to dynamically update the risk state of battery thermal runaway. Sensitivity analysis is also performed to identify key influencing factors and critical propagation paths, providing quantitative support for risk control.

To validate the effectiveness and engineering applicability of the proposed model, a representative eVTOL battery system is selected for a case study. A specific Bayesian network instance is constructed based on actual system structure and operational parameters, and simulation-based risk inference analyses are conducted under multiple scenarios. Through forward inference, diagnostic reasoning, and sensitivity analysis, key risk factors and their propagation paths influencing battery thermal runaway are systematically identified, revealing the accident evolution mechanism under multi-factor coupling. Based on these findings, targeted risk control measures and system optimization strategies are proposed from multiple aspects, including battery design optimization, enhancement of thermal management, improvement of operational control strategies, and emergency response mechanisms.

**Keywords:** Electric vertical take-off and landing aircraft; Battery thermal runaway; System theoretical process analysis; Causal model; Dynamic Bayesian model;

**Classification Number:**[V275;V242]



## 目 录

|                                             |     |
|---------------------------------------------|-----|
| 摘 要 .....                                   | I   |
| Abstract .....                              | III |
| 目 录 .....                                   | V   |
| 1 绪论 .....                                  | 1   |
| 1.1 研究背景与意义 .....                           | 1   |
| 1.1.1 研究背景 .....                            | 1   |
| 1.1.2 研究意义 .....                            | 2   |
| 1.2 国内外研究现状 .....                           | 2   |
| 1.2.1 动力电池故障研究现状 .....                      | 2   |
| 1.2.2 风险分析方法研究现状 .....                      | 4   |
| 1.3 研究内容和方法 .....                           | 6   |
| 1.3.1 研究内容 .....                            | 6   |
| 1.3.2 研究方法 .....                            | 7   |
| 1.3.3 技术路线 .....                            | 7   |
| 1.3.4 创新点 .....                             | 8   |
| 2 相关理论及方法 .....                             | 9   |
| 2.1 电池热失控基础理论 .....                         | 9   |
| 2.2 STPA、Bow-tie、BN 模型介绍 .....              | 10  |
| 2.2.1 STPA 分析模型 .....                       | 10  |
| 2.2.2 Bow-tie 模型 .....                      | 11  |
| 2.2.3 贝叶斯定理与贝叶斯网络理论 .....                   | 12  |
| 2.3 本章小结 .....                              | 13  |
| 3 基于 STPA-Bow-tie 的 eVTOL 电池热失控风险因素识别 ..... | 14  |
| 3.1 eVTOL 电池系统分析 .....                      | 14  |
| 3.1.1 eVTOL 电池线路集成 .....                    | 14  |
| 3.1.2 eVTOL 电池风险特性 .....                    | 15  |
| 3.1.3 eVTOL 电池热失控的危害 .....                  | 17  |
| 3.2 基于 STPA 的 eVTOL 电池热失控风险因素分析 .....       | 18  |
| 3.2.1 eVTOL 电池热失控风险因素识别 .....               | 18  |
| 3.2.2 eVTOL 电池热失控事故的系统安全控制目标 .....          | 20  |
| 3.2.3 基于 STPA 的不安全控制行为识别与致因场景构建 .....       | 21  |
| 3.2.4 UCA 致因场景分析 .....                      | 26  |
| 3.3 基于 Bow-tie 模型的电池热失控事故链构建 .....          | 28  |

---

|                                        |    |
|----------------------------------------|----|
| 3.4 本章小结 .....                         | 33 |
| 4 基于 FBN 的 eVTOL 电池热失控风险动态评估 .....     | 34 |
| 4.1 贝叶斯网络结构模型的构建 .....                 | 34 |
| 4.1.1 STPA-Bow-tie 模型与贝叶斯网络的转换 .....   | 35 |
| 4.1.2 贝叶斯网络节点的确定 .....                 | 36 |
| 4.2 贝叶斯网络参数的确定 .....                   | 37 |
| 4.2.1 基于模糊集理论的专家评定标准 .....             | 38 |
| 4.2.2 诊断推理分析 .....                     | 42 |
| 4.2.3 敏感性分析 .....                      | 43 |
| 5 应用分析 .....                           | 44 |
| 5.1 Lilium 飞行器电池应用与布局概况 .....          | 44 |
| 5.2 基于模糊贝叶斯网络的 eVTOL 电池热失控安全风险评价 ..... | 45 |
| 5.2.1 贝叶斯网络结构构建 .....                  | 45 |
| 5.2.2 贝叶斯网络参数的确定 .....                 | 46 |
| 5.3 贝叶斯网络结构结果分析 .....                  | 55 |
| 5.3.1 因果推理分析 .....                     | 55 |
| 5.3.2 正向推理分析 .....                     | 57 |
| 5.3.3 敏感性分析 .....                      | 58 |
| 5.4 关键因素风险管控措施 .....                   | 60 |
| 5.5 本章小结 .....                         | 61 |
| 6 总结与展望 .....                          | 62 |
| 6.1 研究总结 .....                         | 62 |
| 6.2 研究展望 .....                         | 62 |
| 参考文献 .....                             | 64 |
| 致 谢 .....                              | 69 |

# 1 绪论

## 1.1 研究背景与意义

### 1.1.1 研究背景

随着我国将低空经济作为新质生产力的重要组成部分和战略性新兴产业来发展，各省在全国低空经济领域展开竞争，已有二十多个省份相继出台专项政策支持低空产业发展。作为低空经济发展的核心载体之一，eVTOL 凭借其垂直起降、绿色低碳、高机动性、可载人飞行等特性，在城市通勤、物流运输、应急响应、农业巡检与消防救援等数十个应用场景中展现出巨大的商业化潜力。

然而，国家层面的《低空飞行管理条例》尚未制定完善，空域使用权限模糊、事故责任难以界定等诸多问题亟须规范，这也间接放大了 eVTOL 动力电池热失控安全风险：低空管理规则缺失使飞行空域与应急处置边界不清，一旦飞行途中发生电池热失控险情，无标准化迫降避险流程与管控预案，极易加剧火情蔓延与坠机次生危害；同时责任界定模糊弱化了电池安全防护的监管约束，企业缺乏强制合规压力，易简化热失控防护设计，进一步抬高安全隐患。与此同时，eVTOL 全球适航认证体系尚未形成统一标准：美国 FAA 构建“飞行器一场景一运营”三维认证体系、欧盟 EASA 依托 SC-VTOL 标准严格规范电池安全冗余与热防护设计，均对电池热失控抑制、隔热阻燃、故障预警设置刚性审定要求；而我国民航局仅发布通用无人机适航指南，并未出台针对 eVTOL 电池热失控防控的细化技术规范，行业缺少统一的电芯防护、热蔓延阻隔及应急消防设计准则。国际适航标准分化不仅阻碍海外先进热失控防控材料、BMS 温控技术与安全设计方案的跨国引进与技术合作，也导致国内 eVTOL 电池安全设计缺乏统一合规依据，安全冗余配置参差不齐，最终从法规监管与技术标准双重维度持续加剧电池热失控的安全风险。

由于缺乏安全标准和监管标准，在 eVTOL 产业爆发式增长的同时也带来了许多安全隐患。部分企业在生产时大幅压缩产品测试周期，大大增加了安全风险。例如，有型号 eVTOL 的电池组仅完成 2000 次循环实验（行业建议 5000 次），为安全埋下隐患。电池系统作为 eVTOL 的核心支撑技术之一，其安全性不仅直接影响到整机的续航性能与任务完成效率，更是影响风险事件发生频率、事故后应急处置等能力的关键因素。近两年，eVTOL 电池安全问题暴露了其短板。Lilium 原型机地面起火、Beta 和 Aura 电池故障事件，以及 Bell APT 物流无人机因电控系统失效导致的动力中断等事故的发生，都指出 eVTOL 电池系统稳定性与可靠性存在严重的技术不足。尽管这些事故未造成严重后果，但已表明 eVTOL 电池系统在高密度、多系统条件下的脆弱性。

综上所述，eVTOL 电池系统不仅是动力源，更是运行安全的核心风险点之一。当前适航标准与监管体系的不完善，本质上源于对电池热失控风险形成机理及其演化路径缺乏系统认知。在风险机理不清、致因关系不明的情况下，适航标准的制定与安全管理措施的设计将缺乏科学依据。因此，开展 eVTOL 电池热失控风险的系统分析与评价，是适航标准构建与安全监管完善的前提与基础。相关研究能够揭示关键风险因素及其耦合关系，为安全控制策略制定提供支撑，对于保障低空运行安全及促进低空经济发展具有重要意义。

### 1.1.2 研究意义

现有关于 eVTOL 安全性的研究多聚焦于飞行器总体设计、电推进系统、自动控制系统等技术领域，或从运行控制、飞行任务规划等角度对 eVTOL 运行安全问题展开分析。但对于 eVTOL 电池系统的本体安全风险，尤其是其充放电过程中的热管理失效、碰撞冲击等致因因素，尚缺乏系统化、动态化的风险识别与防控方法。而电池系统作为 eVTOL 的核心动力来源，其热失控事故具有突发性、链式反应性与不可逆性，一旦发生，不仅可能导致电池起火、系统失效，甚至可能导致飞行器坠毁，还可能对城市空域、地面设施及人员生命财产安全构成严重威胁。

针对上述问题，本文拟从 eVTOL 电池安全风险管理的角度出发，融合 STPA、Bow-tie 模型及 FBN 方法，构建能够动态揭示风险因果关系、失效传播路径的事故致因模型，并提出多阶段的安全屏障优化策略，以提升 eVTOL 电池热失控的安全水平。

本文研究的意义在于：一是将 STPA 模型、Bow-tie 模型与 FBN 方法融合，引入到 eVTOL 电池热失控风险分析中，全面揭示 eVTOL 电池热失控的致因路径、风险演化及多阶段安全防控措施，为 eVTOL 的电池系统级安全性设计与评估提供理论支撑，具有一定的理论创新意义；二是基于 FBN 进行 eVTOL 电池热失控风险状态的正反向动态评估与推理，提升风险预测与管控的实时性、智能性，并提出多阶段安全防控措施，这对 eVTOL 整机检测、运行监测及事故应急处置等环节具有重要的参考价值。

## 1.2 国内外研究现状

### 1.2.1 动力电池故障研究现状

随着新能源电池在交通运输、电力储能等领域的广泛应用，其事故率也大幅上升。近年来，国内外发生了一系列锂离子电池火灾或爆炸事故，仅 2022 年在中国，就有 18000 起电动自行车火灾和 3000 多起电动汽车火灾<sup>[1]</sup>，造成了严重的财产损失与人员

伤亡, 引发了学术界的广泛关注。锂电池的安全问题主要是由热失控引起的火灾或者爆炸<sup>[2,3]</sup>。热失控是由各种触发因素引发的一系列连锁反应现象<sup>[4]</sup>, 朱晓庆等人<sup>[5]</sup>从过充、短路、热滥用等诱因, 系统梳理了锂离子动力电池的热失控触发机制, 得出热扩散链式反应失效是引发热失控事故根本原因的结论。REN, Dongsheng 等<sup>[6]</sup>的研究证明, 锂电池受到过充、高温和机械力损伤等恶劣条件的影响时, 电池会破裂并释放危险的易燃气体, 从而引发电池热失控。Xuning Feng 等<sup>[7]</sup>从材料层面、电池层面和系统层面提出了预防电池热失控的策略。当热失控温度达到点火点时, 会引发火灾, 进而导致燃烧和爆炸, 对生命、财产和健康构成严重威胁<sup>[8]</sup>。当前针对锂电池热失效机理、诱因识别及传播路径的研究已逐步从定性认知向定量建模演化, 构建了一定的风险分析基础框架。

eVTOL 作为一种同样使用锂电池作为动力系统的新型航空器, Li W 等<sup>[9]</sup>介绍其运行环境、结构体系与传统固定翼或旋翼航空器有显著不同, 需要更稳定、可靠的电池提供动力。只有保障电池系统的健康状态, 才能使 eVTOL 安全可靠运行<sup>[10]</sup>。eVTOL 在运行中涉及空中导航、能量管理、飞行控制、任务规划等多个子系统的深度耦合与集成, Fatma Yamac Sagirli 等<sup>[11]</sup>从新型动力系统、复杂飞控集成与人机交互的复杂性等方面说明 eVTOL 运行带来了巨大的安全挑战。电池系统作为 eVTOL 的核心动力, 将是导致系统性事故的关键风险源之一<sup>[12,13]</sup>。近年来, 多起与电池热失控相关的航空器事故不断暴露出电动飞行器在电化推进系统稳定性方面的短板。杨娟等<sup>[14,15]</sup>的研究表明电池热失控风险是 eVTOL 运行安全领域亟待解决的核心问题, 王鹏等<sup>[16]</sup>从电池热失控风险、电池热失控监测与通讯功能失效方面对 eVTOL 热失控导致起火风险进行研究, 但是依然缺乏深度的研究。

eVTOL 的电池系统由多个部件组成, 从乔亚军等<sup>[17]</sup>的研究中可以看出其安全风险主要表现为电芯内部热化学反应失控引发的链式失效机理。Guang X Y 等<sup>[18-22]</sup>分别从过充、短路、碰撞、制造缺陷或环境因素触发等方面进行研究, 表明 eVTOL 电池系统的安全风险具有突发性强、蔓延快、难以抑制的特征。陈博宇等<sup>[23]</sup>认为 eVTOL 电池高倍率放电和频繁的快速充电是造成热失控重要原因。FENG Xuning 等<sup>[24]</sup>针对电池短路进行研究, 表明在电池使用过程中机械滥用会触发短路, 而短路会释放热量并引发热滥用问题, 在热滥用情况下, 电池温度极高, 很容易发生热失控故障, 需要对其加强防护管控。殷朕等<sup>[25]</sup>分析了 eVTOL 不同飞行阶段对电池的需求, 并从电、热、力角度探讨了固态电池管理系统的优化路径, 需要对其进一步研究。此外, SHASHANK S 等<sup>[26,27]</sup>还从 eVTOL 运行高度低、起降频繁、任务密度大等因素对 eVTOL 电池影响进行研究, 对 eVTOL 动力系统的循环充放与热负载提出更高要求。王鹏等<sup>[16]</sup>对 eVTOL 构型进行研究, 他们认为由于 eVTOL 的结构紧凑、电池系统集成度高, 一旦发生起火事件, 极易波及整机结构并危及人员生命安全。目前 eVTOL

正处在初步发展时期,并且新能源电池还在持续发展,难以获得足够精确的失效数据,导致对于电池热失控的安全性分析存在较为突出的不确定性问题。

要实现可持续的 eVTOL 电池系统风险管理,识别并管控热失控关键因素至关重要。风险评估是指对事故进行系统识别、分析和评价<sup>[28]</sup>。当前已有研究尝试采用系统安全分析方法识别 eVTOL 的运行风险,其中杨海云、张晓全等<sup>[29,30]</sup>分别使用 FHA 和贝叶斯网络识别 eVTOL 飞行器中潜在的失效状态,预测失效状态以及其他潜在的危险失效模式,从而全面找出潜在的灾难性和危险失效模式,进而有针对性地进行控制,以确保 eVTOL 飞行器的安全性。杨晓军等<sup>[31]</sup>使用 FTA 结合蒙特卡罗模拟,对电动飞机推进系统的可靠性进行分析,识别关键故障模式,评估系统的可靠性指标。在 eVTOL 电池热失控研究中,王鹏等<sup>[16]</sup>使用证据理论和区间分析对其进行安全性分析,识别出影响因素较大的风险因子,并对此提出相应的优化方案。在研究其他风险事故的安全分析中,目前常用的方法有复杂网络<sup>[32]</sup>、事件树<sup>[33]</sup>、危险和可操作分析<sup>[34]</sup>等。风险概率分析方面,常用的方法有贝叶斯网络模型<sup>[35]</sup>、REICH 模型<sup>[36]</sup>、深度神经网络<sup>[37]</sup>等。这些方法在风险因素静态条件下具备良好的结构表达力,但在面对 eVTOL 这种系统高度耦合、动态不确定性强的复杂系统时,存在响应迟滞、因果链割裂、定量建模能力不足等问题,难以全面揭示飞行器在不同运行状态间风险的动态演化路径。尤其是在电池系统的风险识别上,传统方法较难捕捉热失控事件中,从局部异常到系统蔓延再到安全失效的非线性耦合过程,难以满足现代航空器安全评估对高维、多源、不确定因素动态建模的需求。

### 1.2.2 风险分析方法研究现状

鉴于现有研究方法存在明显局限性,行业亟须构建一套兼具清晰结构表征能力与动态不确定性建模优势的复合型安全分析框架,从而实现对 eVTOL 电池起火风险的系统性识别、演化路径建模与风险预警推演。本文通过对现有的安全风险因素识别方法进行分析并整理归纳,从方法的含义和缺点方面对常用的风险识别方法进行对比,如表 1-1 所示。

表 1-1 风险识别方法对比

| 风险分析方法 | 含义                                          | 优点                      | 缺点                              |
|--------|---------------------------------------------|-------------------------|---------------------------------|
| 问卷调查法  | 问卷调查是一种通过设计结构化问题,向特定样本收集数据以分析其态度、行为或特征的研究方法 | 成本较低、可大规模收集标准化数据,便于统计分析 | 结果易受样本偏差和主观回答影响,且问题设计不当会降低数据可靠性 |

续表 1-1 风险识别方法对比

| 风险分析方法   | 含义                                    | 优点                                        | 缺点                             |
|----------|---------------------------------------|-------------------------------------------|--------------------------------|
| 故障树法     | 自顶向下分析系统失效原因，通过逻辑关系逐层分解导致事故的基本事件的安全分析 | 结构清晰、逻辑性强，能够直观识别关键致因和薄弱环节                 | 建模过程较复杂，对数据依赖较强，且难以处理动态和复杂耦合关系 |
| 头脑风暴法    | 通过集体自由发言、鼓励多样化想法以激发创造性思维的问题解决         | 能够在短时间内产生大量创意，激发参与者的创新思维与灵感，获取信息量大，考虑因素全面 | 容易受到从众心理或个别别人主导的影响，导致创意质量参差不齐  |
| 系统理论过程分析 | 基于系统理论，通过识别不安全控制行为来分析复杂系统的安全风险        | 能够从系统层面识别复杂耦合风险，适用于新型复杂系统                 | 分析过程依赖专家经验，主观性较强且实施复杂          |
| 文献检索法    | 通过系统查阅和分析已有研究成果以获取信息和支撑研究             | 成本低、效率高，可快速掌握研究现状和理论基础                    | 受已有研究质量限制，缺乏一手数据且可能存在信息滞后      |
| 蝴蝶结分析法   | 将事故原因（故障树）与后果（事件树）结合的可视化风险分析方法        | 结构清晰、可视化强，便于识别风险路径及防控措施                   | 难以表达动态演化过程，对复杂系统定量分析能力有限       |
| 德尔菲法     | 德尔菲法是通过多轮匿名专家咨询与反馈，逐步达成一致意见的决策分析方法    | 可整合专家经验，适用于数据不足或不确定性较高的问题                 | 耗时较长，结果受专家选择及主观判断影响较大          |

综合分析，以上几种方法都有各自的优点，但也都存在一定的局限性。结合 eVTOL 作为一种全新的飞行器涉及风险因素众多、复杂的特点，本文将文献检索法、系统理论过程分析和蝴蝶结分析法结合起来，对 eVTOL 飞行器以及电池风险进行大量抽样研究，并实现静态与动态风险识别，全面识别可能出现的风险因素。STPA 作为一种面向复杂系统控制结构与功能交互的现代安全分析方法，能够从控制理论出发，识别系统运行过程中因控制失效、不当执行、信息延迟等引发的系统危险状态，适用于高集成度、高自动化航空系统的风险识别<sup>[38,39]</sup>，但缺乏定量计算；Bow-Tie 模型则以“致因—事故—后果”链条为核心逻辑框架，形象展现风险起点与终点之间的防控链条结构，具有良好的可视化表达能力与屏障布局分析能力<sup>[40,41]</sup>，却无法定量地动态反映风险演化过程；贝叶斯网络作为概率图模型，可将风险事件的不确定因果关系以条件概率的形式表达，适合构建事故概率推演模型，并对关键环节进行量化评估与推理支持<sup>[42,43]</sup>，但在模型构建过程中极度依赖专家经验，易遗漏其他风险因子。目前已有学者

尝试将上述方法进行两两结合对风险因素进行研究，STPA 结合 Bow-Tie 模型已有应用于无人机全生命周期安全风险识别的趋势，能够系统追踪风险链条<sup>[44-46]</sup>，但该方法难以动态响应实时运行环境变化，而且缺乏量化模型的支持，只能进行理论性的分析；STPA 与 BN 模型则被用于对事故发生概率进行推演与分析，为构建主动安全预警系统提供支撑<sup>[42,47]</sup>，但缺乏对“事件链”和“安全屏障”显式表达，不利于表达安全防护逻辑结构。

因此，在事故分析中亟须一种能够实现系统控制失效、事故链演化、防护屏障布设及风险水平量化等多功能的综合分析方法。

## 1.3 研究内容和方法

### 1.3.1 研究内容

针对 eVTOL 电池热失控问题，本文重点综合 STPA、Bow-tie 及 FBN 等方法，对 eVTOL 电池热失控风险因素及其评估模型进行研究。主要研究内容包括：

第一章 绪论。系统阐述了研究背景与意义，分析了低空经济发展背景下 eVTOL 快速兴起所带来的电池安全问题，明确了电池热失控对飞行安全的关键影响；通过梳理国内外在电池故障机理及风险分析方法方面的研究现状，指出现有研究在动态性与系统性方面的不足；在此基础上明确本文研究内容、技术路线与方法体系，并提出融合 STPA、Bow-tie 与 FBN 的研究思路，为全文研究奠定理论基础与总体框架。

第二章 相关理论及方法。首先对电池热失控的基本概念及演化机理进行阐述；然后分别对 STPA 方法、Bow-tie 模型及贝叶斯网络理论进行系统分析，明确各方法在复杂系统安全分析中的适用性与局限性，为后续风险识别、建模与评估奠定方法基础。

第三章 基于 STPA-Bow-tie 的 eVTOL 电池热失控风险因素识别。首先结合电池系统结构与运行特性，分析其热失控机理与风险特征。基于 STPA 方法，从系统控制与功能交互角度识别不安全控制行为及其致因场景，提取关键风险要素，并引入 Bow-tie 模型，构建“致因—顶事件—后果”的事故链结构，并融合安全约束与防护措施，实现风险传播路径的可视化表达，为后续定量分析提供基础。

第四章 基于 FBN 的 eVTOL 电池热失控风险动态评估。通过将 STPA-Bow-tie 模型转化为模糊贝叶斯网络结构，构建风险概率推演模型；结合模糊集理论与专家评分方法确定网络参数，有效应对数据不足与不确定性问题；并利用贝叶斯网络的诊断推理与敏感性分析功能，实现风险状态的动态更新与关键影响因素识别，从而提升风险评估的定量性与动态性。



第五章 应用分析。通过建立贝叶斯网络结构，开展因果推理、正向推理及敏感性分析，识别电池热失控的关键风险因素与主要传播路径，并提出针对性的风险管控措施与优化策略，验证了融合模型在实际工程中的适用性与有效性，为 eVTOL 电池系统安全管理提供实践依据与决策支持。

第六章 总结与展望。总结 eVTOL 电池热失控的风险评价研究成果，探究不足和局限性，提出建议并对未来的研究趋势进行展望。

### 1.3.2 研究方法

本研究围绕 eVTOL 电池热失控问题，通过 STPA 方法对系统识别出 UCA、致因场景和事故后果。将 UCA 和事故后果转化为 Bow-tie 模型中导致顶事件左侧的主要威胁和右侧致因后果，安全约束与控制措施转化为 Bow-tie 两侧事前预防和事后缓解的管控措施。

在 Bow-tie 模型基础上构建贝叶斯网络时，Bow-tie 左侧的威胁原因被定义为 BN 的根节点，顶事件作为中间或目标节点，后果作为输出节点，同时防护措施在 BN 中作为调节因素，影响事件链中各节点之间的条件概率。由于实际运行数据稀缺，BN 中节点间的概率关系主要通过专家打分法获得，并引入模糊数学处理以表达认知不确定性，形成模糊贝叶斯网络。通过模糊化、去模糊化得到节点状态概率和非根节点与根节点的条件概率关系。这使得 BN 网络系统在时间片的运行过程中风险水平可随风险因素的发生与否实时调整，避免传统静态 BN 陷入单一时刻风险水平的缺陷。

综上所述，STPA 通过系统识别风险与事故后果，Bow-tie 可视化风险路径与防护机制，FBN 在不确定性条件下进行定量推理与动态预测的能力，通过三者融合，为 eVTOL 电池热失控风险评估提供科学、可靠的依据。

### 1.3.3 技术路线

本文的总体思路如图 1-1 所示。

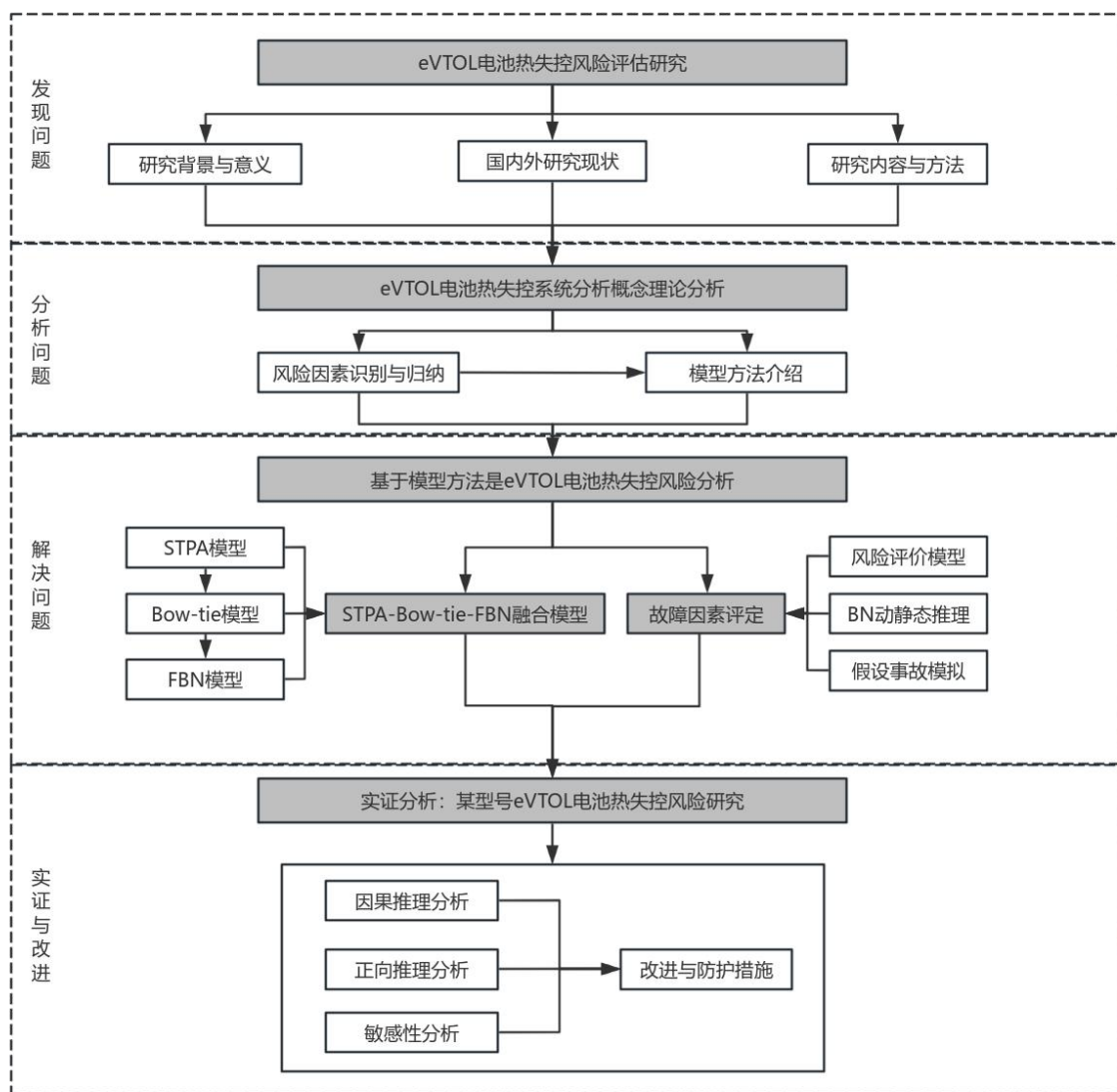


图 1-1 技术路线图

### 1.3.4 创新点

**研究内容创新性：**区别于传统研究侧重单体电芯或局部热失控机理，本文从 eVTOL 高动态运行特性出发，将多物理耦合载荷、环境因素及操作条件纳入统一分析框架，研究热失控的触发条件及其作用边界，实现由“局部机理分析”向“系统安全边界界定”的拓展。

**研究方法创新性：**针对现有方法定性与定量割裂、难以处理不确定性的不足，本文将 STPA、Bow-tie 与模糊贝叶斯网络有机融合，实现从致因识别、路径建模到概率推理的全过程分析，提升复杂系统风险分析的完整性与可计算性。

## 2 相关理论及方法

### 2.1 电池热失控基础理论

在学术研究中, 电池热失控通常被定义为: 当电池在运行过程中受到异常工况或内部缺陷影响时, 电池内部的放热反应速率超过系统的散热能力, 导致温度持续升高, 并进一步诱发一系列自加速的放热化学反应, 使电池温度呈现快速上升的不可控过程。这一过程中, 温度升高会促进电解液分解、固体电解质界面膜破裂、正负极材料分解以及隔膜失效等一系列放热反应, 从而形成“温度升高—反应加剧—热量增加”的正反馈机制。当该反馈过程不断强化并超出系统热平衡能力时, 电池将进入不可逆的热失控状态。

从机理角度来看, 电池热失控本质上是一种由电化学反应与热传递耦合引起的热稳定性破坏过程。在该过程中, 电池内部能量以热量形式快速释放, 并可能伴随气体生成、电解液蒸发及可燃气体喷射等现象。随着反应程度的加剧, 电池内部温度可在短时间内迅速升高至数百摄氏度, 从而导致电池结构损坏甚至引发燃烧或爆炸。因此, 电池热失控通常被视为动力电池系统最严重的一类安全失效模式, 也是电池安全性研究与风险评估的重要关注对象。

热失控一旦形成, 就会快速产生剧烈放热和气压升高, 甚至电池起火、爆炸等严重后果。热失控发展过程如图 2-1 所示。

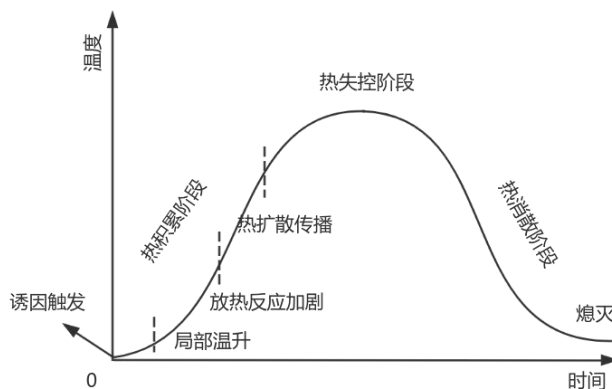


图 2-1 eVTOL 电池热失控发展阶段

上图清楚地表示了电池热失控的演化过程, 各阶段发展过程见表 2-1。

表 2-1 eVTOL 电池热失控发展阶段说明

| 热失控发展过程 | 各阶段状态       | 内部反应                                                        |
|---------|-------------|-------------------------------------------------------------|
| 热积累阶段   | 局部升温、放热反应加剧 | eVTOL 电池局部温度持续升高并形成热点, 若散热不足则热量逐步积聚并扩散, 最终达到临界温度触发不可逆热失控反应。 |

续表 2-1 eVTOL 电池热失控发展阶段说明

| 热失控发展过程 | 各阶段状态       | 内部反应                                                         |
|---------|-------------|--------------------------------------------------------------|
| 火灾发展阶段  | 热扩散传播、热失控阶段 | 电芯内部发生剧烈链式热化学反应，释放大量热能与可燃气体并引发燃烧或爆炸，导致热量迅速蔓延并可能造成失控失效和推进中断等。 |
| 火灾衰减阶段  | 热消散阶段       | 主要反应结束后仍存在残余高温与有毒气体释放，若处置不当可能发生复燃或次生灾害。                      |

## 2.2 STPA、Bow-tie、BN 模型介绍

该模型以系统理论过程分析作为上层系统控制逻辑的分析工具；识别系统级危险源、不安全控制行为及控制环节薄弱点；结合蝴蝶结模型对热失控诱因、故障传播路径及安全屏障进行结构化描述，明确事故前因后果链条；并进一步将蝴蝶结中的故障树与事件树转换为贝叶斯网络的节点及因果关系，从而构建能够反映动态风险演化的概率模型。

### 2.2.1 STPA 分析模型

Nancy Leveson<sup>[48]</sup>于 2004 年为了解决复杂系统中出现的新型风险问题，提出了系统理论事故模型与过程（System Theoretic Accident Model and Process, STAMP）。STAMP 将安全视为非单一部件可靠性决定的，而是由系统整体与系统演化所呈现的一种可靠性状态。STAMP 将安全问题转化为控制问题，通过构建有效的分层控制来确保系统整体的安全约束处于可持续状态。当控制环节出现缺陷、反馈机制错误或者安全约束失效，多种因素相互作用就有可能造成事故的发生。STAMP 是将复杂系统分为多层级的控制结构，通过各层级之间的控制与反馈关系，解释上层级对下层级的约束要求，从系统整体层面分析事故风险形成路径。

STPA 模型是在 STAMP 理论框架下发展而来的，是一种专注于系统结构安全分析的技术。其从根源识别可能导致系统损失的不安全控制行为（Unsafe Control Actions, UCA），包括指令未执行、指令执行时间错误、指令执行顺序错误等情况。通过分析控制结构与约束条件识别潜在风险，并提出改进措施<sup>[49]</sup>。由于 STPA 在系统设计阶段就可实施，因此能够在产品初始阶段使用 STPA 识别安全风险因素，以提升产品系统的可靠性与安全性。

STPA 分析过程通常包括以下四个关键步骤<sup>[50]</sup>：明确系统的安全目标和潜在损失事件；构建系统的控制结构图；识别每个控制环节中可能出现的 UCAs 及其触发条件；最后，分析事故因果路径并提出相应的安全约束与控制策略。该方法能够在系统设计早期提供对复杂系统行为进行系统化理解，从而为安全性提升提供理论支撑和设计指

导，其流程如图 2-2 所示。

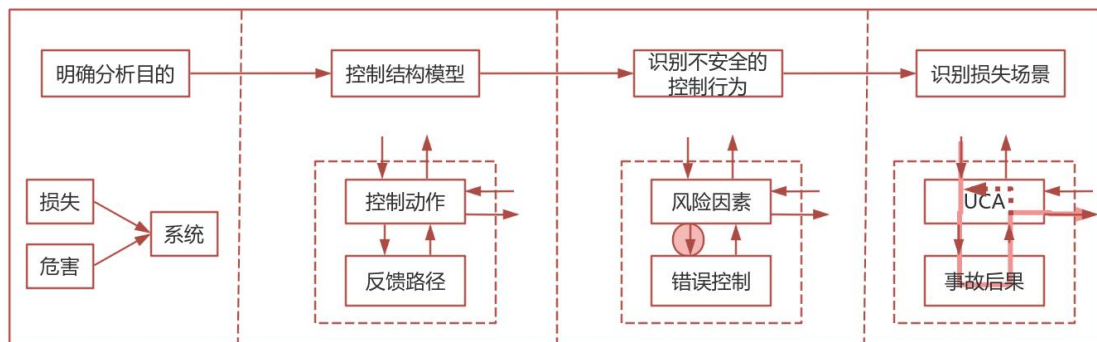


图 2-2 STPA 流程图

STPA 方法通过明确分析目标，对系统组成、运行功能、外部环境及影响因素进行系统梳理，界定研究对象的功能范围与边界条件，并识别系统失效或功能异常可能引发的风险事故，从而反向提出系统需满足的安全约束。在此基础上，构建控制结构模型，基于控制反馈回路理论，分析系统内部各控制单元之间、人与系统之间以及系统与环境之间的交互关系，明确控制器、执行机构、传感器及反馈通道的作用，并进一步解析控制器的决策逻辑，包括控制算法与过程模型。通过识别不安全控制行为（UCA），即在特定情境下可能导致危险后果的控制输出，通常包括未执行应有控制、不当控制、控制时序错误以及控制持续时间异常四类情形。然后，从控制过程与执行过程两个层面对 UCA 进行致因分析，追溯其根本原因，涵盖系统设计缺陷、算法偏差、人员操作失误、信息反馈失真及环境干扰等因素。

STPA 方法以系统整体结构与控制关系为核心，突破传统基于失效的分析思路，能够有效识别复杂系统中的潜在风险，为安全约束制定与风险防控提供理论支撑。

### 2.2.2 Bow-tie 模型

Bow-tie 风险分析模型是一种兼具系统性与直观性的风险分析与管理方法。其名称来源于其图形外观与蝴蝶结相似的特征：中间为一个关键的失控状态，即顶事件（Top Event），左右两侧分别展开为导致该事件发生的威胁（Threats）和事件发生后可能造成的后果（Consequences），从而形成一个完整的风险逻辑链条<sup>[51]</sup>。该模型的提出旨在弥补单一因果分析方法的不足，既继承了故障树分析（Fault Tree Analysis, FTA）在致因识别方面的优势，又吸收了事件树分析（Event Tree Analysis, ETA）在后果推演方面的优点，成为一种能够全面刻画风险发生机理及控制措施的工具。该方法最早由丹麦 Riso 提出，通过构建“蝴蝶结”式图形，将风险事件的成因和后果在一张图中直观展现出来，有效支撑风险识别、评估和控制策略制定的全过程<sup>[52]</sup>。

Bow-tie 模型以顶事件为核心构建风险演化结构，其中顶事件位于模型中心，是

系统由正常状态向失控状态转变的关键分界点，本质上代表一种潜在危险情景而非最终事故结果。在其左侧，模型借鉴故障树分析思路，系统识别导致顶事件发生的各类威胁因素，包括设备故障、操作失误、环境变化及管理缺陷等，并通过设置预防性屏障阻断风险向顶事件的传递，从而降低事故发生概率；在右侧，则基于事件树逻辑分析顶事件触发后可能产生的多种后果，如人员伤亡、财产损失及环境影响等，并通过缓解性屏障控制后果扩散与严重程度。通过在因果链两端嵌入屏障措施，Bow-tie 模型实现了风险识别、预防与应急控制的有机统一。相较传统方法，其具有结构清晰、直观性强和适用范围广等优势，已广泛应用于航空、能源与交通等高风险领域。但该模型多依赖定性分析，存在主观性强、难以量化及动态刻画不足等局限。

综上所述，Bow-tie 风险分析模型作为一种融合因果逻辑与控制措施的风险管理工具，不仅在理论层面完善了风险识别与控制的系统方法论，也在工程实践中展现出较高的应用价值。随着新兴复杂系统安全问题的不断涌现，如何进一步推进 Bow-tie 模型的定量化、动态化和智能化研究，已成为未来学术界和产业界共同关注的重要方向，其流程如图 2-3 所示。

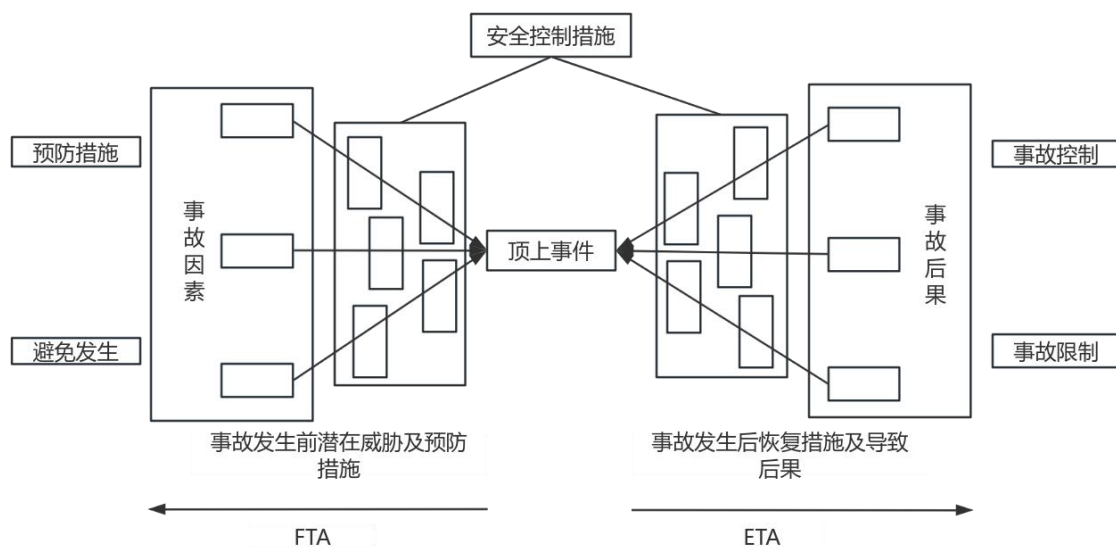


图 2-3 Bow-tie 流程图

### 2.2.3 贝叶斯定理与贝叶斯网络理论

贝叶斯定理（Bayes Theorem）是现代概率论和不确定性推理的核心原理，其主要思想是利用新获得的观测证据对事件发生的概率进行动态修正<sup>[53]</sup>。设事件 A 和证据 B 分别代表某一状态与已知观测信息，则贝叶斯定理可表示为：

$$P(A | B) = \frac{P(B | A)P(A)}{P(B)}$$

式中,  $P(A)$ ,  $P(B)$  分别为事件 A 的先验概率和事件 B 的先验概率, 反映在未获得任何新证据时对该事件的初始判断;  $P(B|A)$  描述在事件 A 发生条件下证据 B 的发生可能性; 而  $P(A|B)$  描述在事件 B 发生条件下证据 A 的发生可能性, 为将证据纳入考虑后的后验概率, 表示对事件发生概率的更新估计。由此, 贝叶斯定理提供了一种在不确定环境中基于证据进行推理的数学方法, 使概率随信息的不断累积而逐步趋于真实状态。

在贝叶斯定理的基础上发展出的贝叶斯网络 (Bayesian Network, BN) 理论是将因果图模型与概率推断相结合的不确定性建模方法<sup>[54]</sup>。贝叶斯网络由有向无环图 (Directed Acyclic Graph, DAG) 构成, 其中节点表示系统的随机变量, 边表示变量之间的因果依赖关系。为了刻画变量间的定量关系, 贝叶斯网络为每个节点配置相应的条件概率表 (Conditional Probability Table, CPT), 用于描述该节点在不同父节点状态下的概率分布。因而, BN 同时具备因果结构表达与概率量化推理的双重功能。

在 eVTOL 电池热失控风险分析中, 贝叶斯网络能够整合专家知识与运行数据, 量化致因路径概率并评估风险在屏障失效、运行环境变化、故障信号输入等条件下的动态演化规律, 从而为系统安全设计和运行安全管理提供有效支持。

## 2.3 本章小结

本章首先对 eVTOL 电池热失控相关理论基础进行阐述, 包括电池热失控的定义、诱发机理及航空电池系统的结构特点, 进一步总结 eVTOL 在垂直起降、载能密度需求、功能复杂性和高功率运行等条件下所呈现的风险特征。对三种方法的理论基础和适用场景予以说明: STPA 用于识别系统级危险源及不安全控制行为, Bow-tie 模型用于刻画热失控事件的致因链条与屏障体系, 而贝叶斯网络用于实现风险的动态概率分析。通过对上述方法的综合介绍, 本章为后续建立 eVTOL 电池热失控风险的系统建模框架奠定理论基础。



### 3 基于 STPA-Bow-tie 的 eVTOL 电池热失控风险因素识别

#### 3.1 eVTOL 电池系统分析

##### 3.1.1 eVTOL 电池线路集成

eVTOL 电池控制系统是一个复杂的系统，涵盖能量管理、健康管理、热管理与安全冗余等控制链路，形成了多层级、多回路的反馈机制，在各链路之间通过多个变量反馈实现协同运作，这种模式高度体现了系统的耦合性、实时性和动态适应能力。在某型号 eVTOL 的电池集成结构中，如图 3-1 所示，该电池系统包含接触装置、高压电源管理集成电路、高低压变压器、电压基准、隔离电源等，电池系统通过各种控制措施对其进行调节和限制。

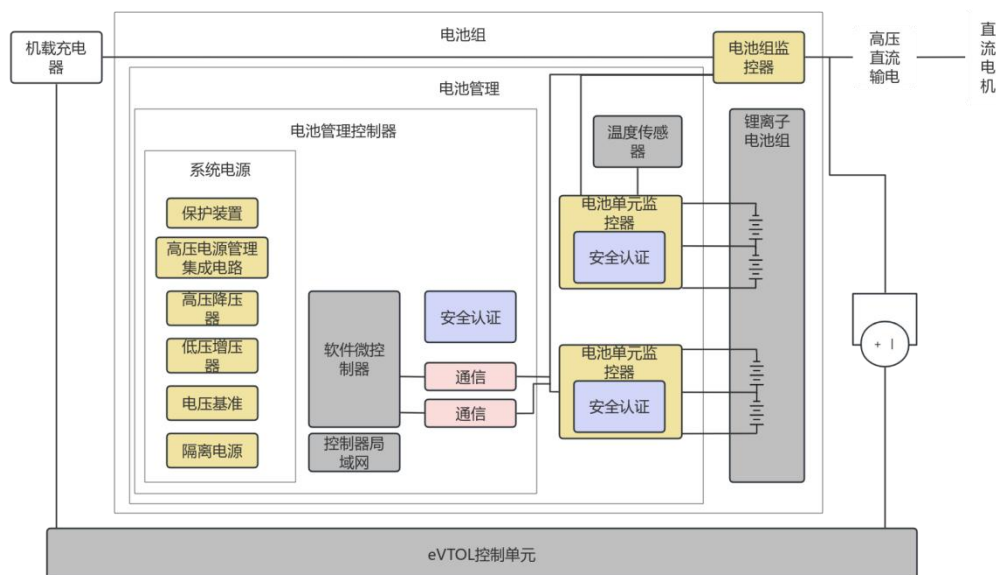


图 3-1 eVTOL 电池电路集成

电池系统通过在电芯、电池组和线组接口等地方布置多种类的传感器，来监视电池运行状态的生命周期。传感器监测到的数据直接反馈到 BMS 与飞行控制计算机上，形成实时状态评估与风险判断的强大反馈机制。其中 BMS 承担着不可或缺的地位，其主要作用包括：

- （1）状态估计：荷电状态、健康状态、功率能力预测等；
- （2）能量管理策略：在不同飞行阶段分配放电功率、优化能量利用率；
- （3）热管理调度：通过液冷、气冷或相变材料冷却实现温度场均衡；
- （4）电芯均衡与故障隔离：对偏差电芯实施均衡控制，并在异常时触发接触器断开实现物理隔离；
- （5）应急联锁与自恢复逻辑：在过热、电压偏差、绝缘下降、烟雾报警等场景下执行限制模式或故障安全模式。



通过上述反馈链路,系统可在正常模式、降额模式、故障安全模式、地面维护模式等运行状态之间动态切换,以适应飞行任务负载与外部环境温度变化,并确保在潜在热失控迹象出现时及时实施风险抑制。

此外,eVTOL 电池系统具有以下关键特征:

(1) 高功率密度与瞬时负载波动:起降阶段功率需求陡升,使电池处于高 C 倍率放电状态,热生成速率显著增加。

(2) 多物理场耦合特性:电池内部电—热—机械场相互影响,局部过热可能在短时间内演化为链式失效。

(3) 跨系统反馈耦合:电池系统与推进系统、飞控系统和热管理系统存在双向依赖,一处异常可能导致耦合放大效应。

(4) 高度依赖传感器与软件控制:任何测量误差、通信延迟或算法异常均可能导致状态估计偏差,从而误判风险等级。

(5) 热失控传播敏感性强:电池包布局紧凑、能量密度高,单体异常可能迅速影响相邻电芯,引发热失控蔓延。

eVTOL 电池系统是一个多层级、多回路、多防护相互作用的复杂控制系统,其包含供给能量控制、热管理控制和安全冗余等多项功能,直接影响着电池热应用的安全水平和电池使用寿命。对 eVTOL 电池系统的控制结构、反馈机制和潜在失效路径等进行全面的分析,是使用 STPA-Bow-tie-FBN 风险模型构建 eVTOL 电池热失控风险分析的基础。

### 3.1.2 eVTOL 电池风险特性

众多学者专家普遍试图将绿色环保、安全性高、寿命长的新能源电池推向新的高度。但热失控机理、热传播特性以及气体析出特征三个方面依旧是造成电池热失控的关键因素<sup>[56]</sup>,严重制约新能源电池的发展。对于 eVTOL 而言,受其运行环境、轻量化设计、能量密度等因素的影响<sup>[57]</sup>,造成电池热失控的诱因和事故后果均与新能源汽车和存储电池有明显的区别。

需要进一步指出的是,在贝叶斯网络参数化过程中,部分基础失效概率及条件概率仍参考了已有新能源汽车与储能电池的统计数据。这种“跨场景数据迁移”的处理方式,虽然在当前 eVTOL 运行数据匮乏的背景下具有一定的合理性,但不可避免地引入了模型适用性的局限性与结果偏差。

具体而言,一方面,eVTOL 电池通常处于高倍率充放电、频繁功率波动及复杂气动热耦合环境中,其热失控触发阈值及演化路径可能显著不同于地面车辆或固定储能系统,从而导致基于传统电池数据得到的失效概率在数值上存在系统性偏移;另一方面,eVTOL 多采用分布式电池布局及轻量化封装设计,其热传播路径更短、热耦合更强,这可能放大某些中间事件的条件概率,使得风险传播过

程呈现出更强的级联特征。因此，直接套用相关文献数据，可能在一定程度上低估极端工况下的事故概率，或高估部分缓慢演化过程的发生频率。

尽管如此，本文通过文献交叉验证与专家经验修正，对关键概率参数进行了区间约束与一致性校核，从而在一定程度上提高了参数设定的合理性。此外，所构建模型更侧重于风险传播路径与关键致因识别，其分析结果在结构层面仍具有较好的参考价值。未来研究中，应结合 eVTOL 实测运行数据、试验数据及事故案例，对模型参数进行动态更新与迭代修正，以提升风险评估结果的准确性与工程适用性。

在热失控机理方面，机械损伤、电滥用与热滥用仍是造成 eVTOL 电池热失控的关键因素，然而受 eVTOL 运行条件的特殊性影响，其触发因素和事故后果被显著放大。由于 eVTOL 是一款可载人垂直起降的电动飞行器，其动力系统需要在短时间内实现高功率的收放，这会导致电池在短时间内承受高倍率充放电，损伤电池寿命。为满足 eVTOL 的续航和轻量化需求，电池组通常采用高能量、高集成的结构设计，限制了散热功率<sup>[58]</sup>，如图 3-2 所示。当电池组中单体电芯出现异常时，由于散热条件受限，电池组内部温度会快速上升，从而引发热失控连锁反应。所以 eVTOL 电池热失控的触发机制不仅包括外部因素，更受飞行器自身负载变化与热管理动态耦合效应的共同影响。

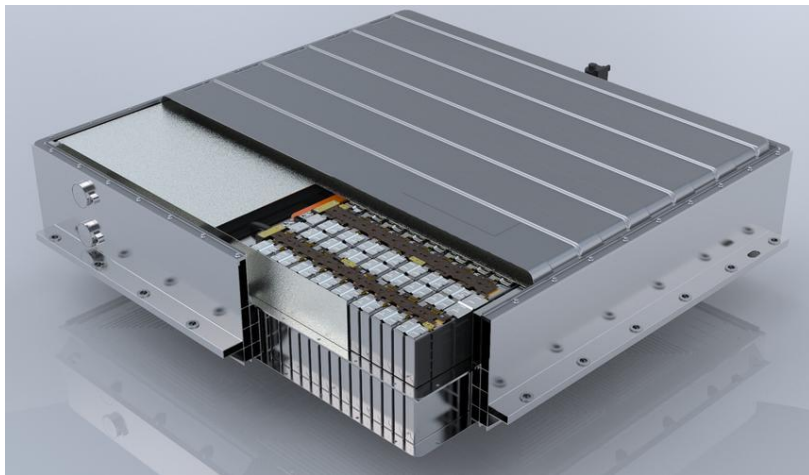


图 3-2 电池组示意图

在热传播特性方面，由于 eVTOL 和新能源汽车电池布局相似，其电池组具有结构紧凑的特性<sup>[59]</sup>，这使得电池热失控一旦发生，就会造成从电池组内部到电池组外部、电池组之间的快速传播效应。从电池布局来看，由于考虑到空间布局和重心平衡等问题，eVTOL 的电池舱通常位于飞行器的机体承力结构或推进系统附近，这就导致 eVTOL 电池散热路径短、传热性强。当电池发生热失控时，其热量会迅速传播到邻近电芯，引发连锁热反应。这种传播特性缩短了热失控的周期，会使飞行器快速陷入失去动力、结构损坏或者整机起火的重大风险中。

在气体特征方面，由于 eVTOL 通常是封闭或者半封闭的机舱<sup>[60]</sup>，舱内的容积和气体交换都受到严重限制，这就导致电池发生热失控时，电池电解液和电极材料燃烧，舱内气压升高并释放高热量的有毒可燃气体，对飞行器机舱环境和飞行系统造成严重威胁。同时，这些气体还可能腐蚀电子设备或干扰飞控与通信系统的正常运行，从而引发二次安全风险。

相较于航空燃料动力系统，eVTOL 电池在结构布置、能量密度、热管理难度、载荷响应等方面面临更为严峻的安全挑战，其风险特性具体体现如表 3-1 所示。

表 3-1 eVTOL 电池热失控风险特性表征

| 风险特性        | 表现特征                   |
|-------------|------------------------|
| 高能量密度风险     | 触发热失控因素，易造成灾难性后果       |
| 多源诱因非线性失效   | 热失控因素呈现出突发性与难预测性特征     |
| 高集成化传播性强    | 单体电芯失效极易向模块传播热量        |
| 起降频繁的疲劳积累效应 | 造成电池性能衰退与机械损伤          |
| 运行环境复杂适应性不足 | 使电池运行具有不确定性并可能诱发潜在安全隐患 |
| 实时监控与诊断技术滞后 | 难以实现对热失控风险的早期精准干预      |

综上所述，由于 eVTOL 本身存在局限性，地面电动车和其他热失控安全防护体系难以直接适用于 eVTOL 领域。因此亟须结合 eVTOL 特性和运行环境，构建一套系统级热失控风险识别与防护模型。

### 3.1.3 eVTOL 电池热失控的危害

电池热失控作为 eVTOL 运行过程中的关键风险之一，若发生热失控，就会造成多维度、多阶段、多系统的危害。其危害主要包括以下几个方面：

(1) 飞行器功能瘫痪。由于电池系统是 eVTOL 的核心能源来源，当发生热失控时，会导致电压骤降、电源断供，严重影响推进系统和飞控系统的正常运行，极易引发飞行中断、姿态失控、飞行器坠毁等灾难性后果，尤其在低空高密度城市环境中，容错空间极小，极端情况下可能在短时间内演变为无法挽回的飞行事故。

(2) 火灾与爆炸风险。热失控过程释放的大量热能和可燃气体极易引发高温燃烧与爆炸，形成火焰喷射、烟雾弥漫和毒气释放。紧凑的舱体结构与高集成的电池布局使火势极易蔓延至飞行器其他部位，引燃 eVTOL 其他飞行系统，加剧灾情扩散，严重威胁飞行器及乘员安全。

(3) 人员伤亡风险。若 eVTOL 处于载人通勤状态，热失控造成的高温、爆炸冲击及有毒气体释放将对乘员造成直接生命威胁，可能引发灼伤、窒息、中毒等伤害；若发生在城市上空或起降区域，还可能波及地面人群，产生次生伤害事故，进一步扩大事故影响范围。

(4) 设施与环境损害。eVTOL 运行往往依赖城市内起降点或综合交通枢纽，热失控事故可能导致地面基础设施损毁、通信中断、电力系统瘫痪等；释放的大

量烟尘与气体还将对周边环境造成污染，诱发火灾连锁效应，增加后续恢复与处置难度。

## 3.2 基于 STPA 的 eVTOL 电池热失控风险因素分析

锂离子电池热失控是由电池内部电化学、热、机械等因素协同作用引发的不可控的放热链式反应，随着热失控产生的温度升高，最终导致电池系统热平衡能力失效，出现电池组件被严重破坏、喷射火焰或释放毒气等严重后果。

本节基于电池热失效机理、典型滥用行为、电池管理系统保护功能、航空运行环境及人因失效等角度，形成五类一级指标，系统描述 eVTOL 电池热失控风险来源，为后续控制结构分析与概率建模提供依据。需要强调的是，这些风险因素在运行周期内动态交互、交替作用，形成了复杂的耦合风险传播网络。

### 3.2.1 eVTOL 电池热失控风险因素识别

#### （1）电池本身固有风险

电池本身固有风险主要来源于材料特性、制造工艺缺陷以及循环过程中的化学与结构退化，是最基础但最难完全避免的热失控诱因。研究表明，隔膜孔径不均、热稳定性不足以及金属颗粒等杂质污染均可能在高温条件下导致隔膜破裂或形成局部高电场，引发内部短路。焊接缺陷、极片卷绕不良、黏结剂脱落等制造偏差会使局部接触电阻升高，导致热点区域形成，从而显著提升热失控触发概率。

在电池使用与循环过程中，由于电池多次高倍率放电、快速充电及温度循环等工况的综合作用，电池内部会发生 SEI 膜剥落、电解液分解、活性物质损失和内阻升高等不可逆老化过程。上述老化现象不仅降低电池热稳定性，还可能导致 SOC 估算误差扩大，使 BMS 的保护阈值区间与电池实际状态逐渐偏离，从而增加热失控发生概率。

#### （2）滥用诱发风险

滥用行为是导致电池热失控最直接且最常见的外部诱因，可分为电气滥用、机械滥用和热滥用三类。

1) 电气滥用风险。过充放会造成电池内部材料氧化和结构破坏，并产生反应热、气体，形成金属枝晶，致使在后续充电或者高温条件下发生电池内部穿刺，从而产生内部短路。外部短路通常是由于机械损伤、电路故障等因素造成电流过大，产生大量热量而引发的。

2) 机械滥用风险。挤压、穿刺、撞击和坠落等外力会损伤隔膜与极片，破坏电化学隔离结构，导致局部短路。对于 eVTOL 而言，起降时机体振动、飞行中气压变化以及轻量化结构对外冲击的弱防护性均使机械滥用风险突出。

3) 热滥用风险。在强日照、高温停放、冷却系统效率下降或完全失效的情况下, 电池可能产生持续热积累。当某一单体电芯进入热失控后, 其释放的高温 and 可燃气体将诱导相邻电芯出现热蔓延, 这是动力电池组层面最具破坏性的失效模式。

### (3) 系统失效风险

系统层失效主要涉及热管理系统、电池管理系统、供电系统, 是航空电池热失控防护链中最关键的主动防线。单点的失效风险往往会触发链式反应, 造成多级的风险失效, 产生高度耦合的故障模式, 造成系统级失效, 从而触发电池热失控的关键风险点, 导致电池热失控的风险显著上升。

### (4) 人因风险

人为因素造成 eVTOL 电池热失控的主要来源是地面操作、检修维护和运行保障环节。由于操作人员的行为不符合规范, 未按照规定进行操作, 造成电池内外部损伤。另外, 由于工作人员疏忽, 未识别早期 eVTOL 电池热失控风险信号, 导致事故风险被搁置, 同样会造成热失控风险。

### (5) 环境风险

在各类风险事故中, 环境因素一直是一个不可忽视的重要因素, 其主要威胁来源于外界的物理冲击和极端气候变化等因素。当 eVTOL 受到外部冲击造成电池松动或者碰撞时, 就会对电池结构造成破坏, 引发电池短路。在天气极端变化时, 由于空气温度、空气气压、空气湿度和空气腐蚀等情况, 会导致电池的绝缘性能下降, 引发短路, 造成热失控。

### (6) 风险因素整合

综上所述, eVTOL 电池热失控风险因素具有多源性、层次性与动态耦合性。电气、机械、热、控制与人因等多维因素在运行周期内交替作用, 形成复杂的风险传播网络, 风险层级如表 3-2 所示。

表 3-2 eVTOL 风险识别层级表

| 目标层           | 一级指标        | 二级指标      | 三级指标              | 文献来源         |
|---------------|-------------|-----------|-------------------|--------------|
| eVTOL 电池热失控 A | 电池本身固有风险 X1 | 电芯缺陷 C1   | 电芯制造缺陷 D1         | [16]         |
|               |             |           | 正极材料热不稳定性 D2      | [61][64][66] |
|               |             |           | 负极材料锂析出风险 D3      | [61][64][66] |
|               |             | 电池老化衰减 C2 | 循环老化导致 SEI 膜失效 D4 | [61][68]     |
|               |             |           | 活性材料损耗与结构变形 D5    | [61][66]     |
|               |             |           | 老化导致热失控敏感性增加 D6   | [61][68]     |
|               | 滥用诱发风险 X2   | 机械滥用 C3   | 垂直起降冲击载荷下的结构损伤 D7 | [16][61][62] |
|               |             |           | 外部刺穿 D8           | [16][61][63] |
|               |             |           | 长期振动导致结构松动 D9     | [61][70]     |

续表 3-2 eVTOL 风险识别层级表

| 目标层 | 一级指标      | 二级指标          | 三级指标            | 文献来源                 |
|-----|-----------|---------------|-----------------|----------------------|
|     |           | 过充 D10        |                 | [16][61][64][65][66] |
|     |           | 电气滥用 C4       | 过放 D11          | [61][62]             |
|     |           |               | 内外部短路 D12       | [16][61][63]         |
|     |           |               | 充电电压/电流过大 D13   | [61][63][65]         |
|     |           |               | 高功率放电叠加环境高温 D14 | [16][61][71]         |
|     |           | 热滥用 C5        | 电池模组局部过热 D15    | [61][67][71]         |
|     |           |               | 相邻电芯热失控传导 D16   | [61][67][71]         |
|     |           |               | 空气冷却系统故障 D17    | [61]                 |
|     |           | 热管理系统失效 C6    | 液体冷却系统故障 D18    | [61]                 |
|     |           |               | PCM 冷却系统失效 D19  | [61]                 |
|     |           |               | 温度传感器故障 D20     | [16][61]             |
|     |           |               | 过充保护机制失效 D21    | [61][62]             |
|     | 系统失效风险 X3 | 电池管理系统失效 C7   | 过温保护机制失效 D22    | [16][61][62]         |
|     |           |               | 通讯系统故障 D23      | [16][62]             |
|     |           |               | 主控单元故障 D24      | [16][62]             |
|     |           | 供电系统失效 C8     | 线路连接接触不良 D25    | [61][70]             |
|     |           |               | 汇流排故障 D26       | [61][70]             |
|     |           |               | 违规充电 D27        | [61][65]             |
|     |           | 操作不当 C9       | 飞行前电池状态检查疏漏 D28 |                      |
|     | 人因风险 X4   |               | 维修误操作 D29       | [62]                 |
|     |           | 决策与应急失误 C10   | 风险环境强飞 D30      |                      |
|     |           |               | 热失控期间操作错误 D31   | [61]                 |
|     |           |               | 未按规程更换电池 D32    |                      |
|     |           | 极端气候环境 C11    | 高/低温环境 D33      | [16][61]             |
|     |           |               | 雷电天气 D34        | [61][62]             |
|     | 环境风险 X5   |               | 暴雨/潮湿环境 D35     | [62]                 |
|     |           | 复杂运行与外部环境 C12 | 复杂地形起降 D36      |                      |
|     |           |               | 高粉尘等天气 D37      | [61]                 |
|     |           |               | 高空低气压环境 D38     | [69]                 |

本文在既有锂离子电池通用风险因素框架下，通过嵌入 eVTOL 典型运行特征对原有风险因素进行情境化重构。具体而言，通过在指标层引入飞行阶段、载荷特征及系统结构约束等限定条件，使传统电池风险在 eVTOL 运行环境下表现出更强的触发敏感性与耦合放大效应，从而实现由“通用风险识别”向“特定运行场景风险表征”的转化。

### 3.2.2 eVTOL 电池热失控事故的系统安全控制目标

#### (1) 系统分析边界与功能定义

电池系统作为 eVTOL 电推进系统的核心能源模块，在飞行器执行飞行任务、进行能量控制、充放电控制和热管理等操作时依旧能够保持稳定工作。其主要功能包括：提供持续、稳定的电能输出以满足推进系统需求；与 BMS 协同实现充放电控制与电芯状态监测；实时响应飞行控制系统能量需求变化，实现功率动态

分配；在热、电、机械应力下维持热平衡与安全运行；当检测到异常状态时，触发主动安全保护机制，实现风险隔离与应急处置。

### (2) 系统安全控制目标 (SCG)

基于上述系统功能，针对热失控风险的安全控制目标如表 3-3 所示。

表 3-3 热失控风险系统安全控制目标

| SCG   | 系统事故                          | 控制目的            |
|-------|-------------------------------|-----------------|
| SCG-1 | 防止因过充、内短路等失控状态引发电芯温升异常        | 避免诱发热失控初始阶段的热积累 |
| SCG-2 | 在热积累初期识别危险信号，及时中断供电或冷却控制      | 防止热扩散与系统失衡      |
| SCG-3 | 限制热扩散路径，防止模块间蔓延               | 避免热失控链式反应       |
| SCG-4 | 确保热失控后果被有效遏制，避免引发结构解体、火灾等二次事故 | 减轻事故后果          |
| SCG-5 | 在设计阶段引入热冗余与监控机制，增强系统鲁棒性       | 增强系统鲁棒性与适航安全    |

### 3.2.3 基于 STPA 的不安全控制行为识别与致因场景构建

STPA 分析主要包含系统层级定义、控制结构构建、不安全控制行为识别、致因场景分析等核心步骤，下面将按照上述步骤对电池热失控的不安全控制行为识别与致因场景构建进行系统性分析。

#### (1) 定义分析目的与系统级事故识别

eVTOL 运行包含六个阶段：垂直起飞、爬升过渡、巡航爬升、定速巡航、进近下降、垂直着陆。当各阶段发生电池热失控时都会造成系统级事故，系统级事故主要是对人、机、环、管造成的严重后果。通过分析 eVTOL 飞行状态，识别出五个层级的系统级事故，系统级事故及描述如表 3-4 所示。

表 3-4 系统级事故识别

| 编号  | 系统级事故     | 描述                           |
|-----|-----------|------------------------------|
| A-1 | 机体坠毁      | 电池热失控导致动力或飞控系统断电，使飞行器失去推力或控制 |
| A-2 | 机上火灾      | 热失控蔓延至机舱，引发机上火灾，威胁乘客安全       |
| A-3 | 机体爆炸      | 电芯剧烈放热反应引发爆炸，造成结构性破坏         |
| A-4 | 地面人员与设施损害 | 停机或充电期间热失控引发人员伤亡与设备损毁        |
| A-5 | 环境二次灾害    | 坠毁或火灾导致城市基础设施受损或环境污染         |

系统级危险是从潜在风险状态角度出发，指可能引发事故的运行状态或条件。通过分析航空器运行过程中易发生的系统级事故以及当电池热失控发生后可能造成事故后果的严重度来分析系统级危险，其主要包括以下几个方面，系统级危险如表 3-5 所示。

表 3-5 系统级危险表

| 编号  | 危险     | 相关事故               |
|-----|--------|--------------------|
| H-1 | 地面运行危险 | A-4;A-5            |
| H-2 | 电池功能丧失 | A-1                |
| H-3 | 动力系统失效 | A-1                |
| H-4 | 飞行控制丧失 | A-1                |
| H-5 | 结构性破坏  | A-1; A-2; A-3      |
| H-6 | 机载火灾   | A-2; A-3; A-4; A-5 |
| H-7 | 二次能量释放 | A-2; A-3; A-5      |
| H-8 | 应急处置失当 | A-1; A-2; A-3; A-4 |

电池功能丧失（H-1）是指电池热失控引发容量骤降、电压崩溃，导致动力/控制/导航系统能源不足。

动力系统失效（H-2）是指推进电机因电池断供或 BMS 保护失效而停机，导致推力不足。

飞行控制丧失（H-3）是指电源异常使飞控系统失灵，飞行器无法维持姿态或航迹。

结构性破坏（H-4）是指热扩散导致电池舱、机身结构烧蚀或解体，削弱整体承力能力。

机载火灾（H-5）是指热失控火焰或高温气体进入客舱/货舱，产生烟雾、有毒气体和高温环境。

二次能量释放（H-6）是指热失控诱发相邻电芯连锁反应，形成大规模能量爆发。

应急处置失效（H-7）是指飞行员或自动应急系统未能在热失控初期采取有效隔离、断电或迫降措施。

地面运行危险（H-8）是指充电/储存过程中电池管理和冷却不足，诱发热失控并危及地面人员与设施。

## （2）建立控制反馈结构

eVTOL 电池控制系统是一个典型的“感知—决策—执行—反馈”多层闭环控制系统。其控制反馈结构可分为三个逻辑层次，并与“人—机—环—管—材”要素紧密耦合。

**任务与能量调度层：**该层由飞行控制系统与能源调度单元构成，是系统的上位控制中心。根据飞行阶段动态分配电池输出功率。接收来自下层的电池状态（SOC，SOH，温度，功率限制）反馈，实现“任务需求驱动—能量状态反馈”的高层能量优化。

**电池状态与安全控制层：**该层主要是以 BMS 为控制核心，通过数据采集，在执行过充放、失温等保护措施过程中，实现电池运行状态的实时监测与安全保护，其主要功能是提供安全防护。

**热—电物理反馈层：**该层由热管理系统控制单元负责执行，通过冷却/加热



执行机构调节电池温度场。通过温度传感器实时监测，构成热稳定反馈环，有效抑制热积累与热扩散。

### （3）不安全控制行为识别

根据控制反馈结构，识别系统中的不安全控制行为（UCAs）。依据 STPA 方法定义的四种存在安全隐患的不安全控制行为，列出航空器运行过程中的不安全控制行为，如下表 3-6 所示。

表 3-6 不安全控制行为

| 控制行为               | 未提供控制行为                                           | 提供了不适当或错误的控制行为                                         | 控制行为提供太早、太晚或顺序颠倒                                 | 控制行为停止太早或应用太久                                     |
|--------------------|---------------------------------------------------|--------------------------------------------------------|--------------------------------------------------|---------------------------------------------------|
| BMS 监测电池状态(C-1)    | UCA-1: 未监测到电池过温、过压等状态。<br>(H-1,H-2,H-5, H-6)      | UCA-2: 错误判断电池状态。<br>(H-1,H-2,H-5, H-6)                 | UCA-3: 监测到危险状态后, 报警或触发控制指令延迟。<br>(H-5, H-6, H-7) | —                                                 |
| BMS 发出冷却指令(C-2)    | UCA-4: 电池过温, 但未启动热管理系统。<br>(H-5, H-6)             | UCA-5: 在电池低温时错误启动强冷却, 或高温时启动加热。<br>(H-1, H-5)          | UCA-6: 启动冷却太晚, 未能及时抑制温升。<br>(H-5, H-6)           | UCA-7: 在温度已降低后仍未停止冷却, 导致电池过冷。<br>(H-1)            |
| BMS 发出充放电控制指令(C-3) | UCA-8: 未在过充/过放临界点切断电路。<br>(H-1, H-2,H-5, H-6)     | UCA-9: 发出错误的电流或功率指令。<br>(H-1, H-2, H-5, H-6)           | UCA-10: 切断过充/过放电路太晚。<br>(H-1, H-2, H-5, H-6)     | UCA-11: 过早恢复充放电, 或过流保护持续时间不足。<br>(H-1,H-2, H-5)   |
| BMS 执行电池均衡(C-4)    | UCA-12: 未对电芯进行均衡, 导致电芯长期过压/欠压。<br>(H-1, H-5)      | UCA-13: 均衡逻辑错误, 对本应放电的电芯充电, 或反之, 加剧不一致性。<br>(H-1, H-5) | UCA-14: 在电芯电压已严重偏离时才开始均衡。<br>(H-1, H-5)          | UCA-15: 均衡过程持续时间过长, 导致某些电芯被过充或过放。<br>(H-1, H-5)   |
| BMS 上报故障状态(C-5)    | UCA-16: 检测到内部严重故障但未向飞控或远程机组上报。<br>(H-5, H-6, H-7) | UCA-17: 上报了错误的故障等级或类型, 误导应急处置。<br>(H-5, H-7)           | UCA-18: 上报严重故障信息延迟, 错过最佳处置时机。<br>(H-5, H-6, H-7) | —                                                 |
| TMS 调节冷却流量(C-6)    | UCA-19: BMS 发出冷却指令后, TMS 未启动冷却泵或风扇。<br>(H-5, H-6) | UCA-20: TMS 错误调节冷却流量。<br>(H-5, H-6)                    | UCA-21: TMS 响应 BMS 冷却指令延迟。<br>(H-5, H-6)         | UCA-22: 冷却系统在已达到目标温度后仍未降速或关闭, 导致能源浪费或过冷。<br>(H-1) |

## (4) 致因场景识别

确定控制场景和类型的目的是更好地确定控制行为之间的因果关系, 结合不安全控制行为内容和控制行为发生的时机, 将控制场景定义为未提供控制行为 UCA1 (1)、提供了错误的控制行为 UCA2 (2)、提供控制行为的时机过早/过晚 UCA3 (3) 和提供的控制行为停止过早或者过晚 UCA4 (4), 将控制类型定义为不安全操作行为 (I)、不安全决策行为 (II) 和不安全感知行为 (III)。不安全控制行为分别对应其可能包含的控制场景和所属控制类型如表 3-7 所示。

表 3-7 致因场景识别

| 一级指标     | 二级指标     | 致因场景                                                                            | 控制行为主体        | 行为类型    | 关联控制场景     |
|----------|----------|---------------------------------------------------------------------------------|---------------|---------|------------|
| 电池本身固有风险 | 电芯缺陷     | UCA-1, 2 (未监测或误判由缺陷导致的微短路)<br>UCA-16, 17, 18 (未上报材料不稳定性引发的异常)                   | BMS, 传感器      | II, III | 1, 2, 3    |
|          | 电池老化衰减   | UCA-1, 2 (未准确评估 SOH, 导致对老化电池施加过大应力)<br>UCA-9 (充放电策略未适应老化电池的承受能力)                | BMS           | II      | 1, 2       |
|          | 机械滥用     | UCA-23, 24, 25 (FCS 未能有效避免或缓解碰撞、冲击)<br>UCA-16, 18 (BMS 未及时上报因振动/冲击导致的内部损伤)      | FCS, BMS      | II, III | 1, 2, 3    |
| 滥用诱发风险   | 电气滥用     | UCA-8, 9, 10 (BMS 未有效防止过充/过放/过流)<br>UCA-28 (操作员使用错误设备导致外部短路或过充)                 | BMS, 操作员      | II, I   | 1, 2, 3    |
|          | 热滥用      | UCA-4, 5, 6, 19, 20, 21 (BMS/TMS 未有效应对高温环境或局部过热)<br>UCA-24 (FCS 在高温环境下错误增大功率需求) | BMS, TMS, FCS | II, I   | 1, 2, 3, 4 |
|          | 热管理系统失效  | UCA-19, 20, 21, 22 (冷却执行器未正确动作)<br>UCA-1, 2, 3 (温度传感器故障, 提供错误或延迟信号)             | TMS 执行器, 传感器  | I, III  | 1, 2, 3, 4 |
| 系统失效风险   | 电池管理系统失效 | UCA-1 至 UCA-18 中的所有行为, 均是 BMS 功能失效的直接体现。                                        | BMS           | II, III | 1, 2, 3, 4 |
|          | 供电系统失效   | UCA-1, 2 (未监测到接触不良导致的压降/发热)<br>UCA-8, 10 (未及时切断因汇流排故障引发的短路)                     | BMS           | II, III | 1, 2, 3    |
| 人因风险     | 操作不当     | UCA-27, 28, 29, 30 (操作员/维护人员的所有不规范行为)                                           | 操作员/维护人员      | I       | 1, 2, 3    |
|          | 决策与应急失误  | UCA-23, 24, 25, 26 (飞行员或自动系统在空中的错误决策)<br>UCA-17 (被 BMS 错误信息误导而做出错误决策)           | FCS, 飞行员      | II, I   | 1, 2, 3, 4 |

续表 3-7 致因场景识别

| 一级指标 | 二级指标      | 致因场景                                             | 控制行为主体        | 行为类型    | 关联控制场景  |
|------|-----------|--------------------------------------------------|---------------|---------|---------|
| 环境风险 | 极端气候环境    | UCA-4, 5, 6 (TMS/BMS 未能应对极端温度)                   | BMS, TMS, FCS | II      | 1, 2, 3 |
|      |           | UCA-23, 24, 25 (FCS 未能应对雷电、暴雨等天气导致的紧急情况)         |               |         |         |
|      | 复杂运行与外部环境 | UCA-23, 24, 25 (FCS 未能在复杂地形起降或低气压环境下妥善管理能量与飞行路径) | FCS, 传感器      | II, III | 1, 2, 3 |
|      |           | UCA-1 (传感器因高粉尘、潮湿环境提供错误信号)                       |               |         |         |

### 3.2.4 UCA 致因场景分析

STPA 方法中, UCAs 的识别仅是风险分析的中间环节。若仅停留于行为分类层面, 而缺乏对其触发情境与致因机制的深入刻画, 则难以揭示系统失效的内在机理, 也无法为后续 Bow-tie 模型提供有效的因果输入。因此, 有必要进一步对各类 UCA 在具体运行条件下的触发过程进行细化分析。

#### (1) 感知层失效致因场景分析

感知层失效主要表现为系统对电池关键状态参数的获取完整度和准精确度, 从而导致控制决策的失效。

以 UCA-1 为例, 在 eVTOL 飞行巡航阶段, 电池长期处于高倍率放电状态, 导致局部电芯电阻差异形成热点。然而, 由于温度传感器布局存在检测盲区或者精度产生偏差, 导致局部热点异常未被识别。而且, 若系统采样频率较低或者数据化采用均值化处理, 从而覆盖了瞬态异常温度, 导致感应偏差。

对于 UCA-2, 其典型的情景一般出现在电池老化阶段, 随着电池的使用循环次数的增加, 使电池内部结构发生退化, SOC 与 SOH 之间的映射关系呈现显著的非线性变化。然而, 若 BMS 采用的是初始检测模型进行电池状态评估, 就会导致错误地识别电池的安全状态, 从而延误保护措施的实施。

#### (2) 决策层失效致因场景分析

决策层的失效主要表现为 BMS 或者飞行控制系统在获取状态信息后, 未能做出合理控制决策或控制决策存在偏差。

在 eVTOL 飞行爬升阶段, 电池负载迅速增加, 温度呈现快速上升趋势。若系统采用带有时间窗口的阈值判定策略, 则可能导致报警信号滞后, 触发 UCA-3 场景。在多模块协同决策机制中, 也有可能引入额外的延迟, 从而错过最佳干预时机。

在 eVTOL 的控制架构中, 热管理系统主要依赖于 BMS 指令进行被动的响应,

缺乏温度变化的主动预测控制能力。当电池内部局部热点形成时，而未能提前主动进行冷却，导致电池内部热量向周边扩散，增加热失控风险。

此外，在复杂环境条件下，如高空低气压环境中，冷却介质换热效率下降，在控制模型未考虑 UCA-20 等致因场景，则会导致冷却流量调节不足，进一步加剧温度升高的问题。

### （3）执行层失效致因场景分析

执行层失效主要表现在控制指令虽已生成，但未被正确执行或执行效果偏离预期。

在地面高温环境或飞行前阶段，电池初始温度已接近安全上限，但由于电池系统未将环境温度纳入考虑范围，或操作人员未执行预冷却流程，导致冷却系统未及时启动，从而引发 UCA-4。

对于 UCA-8 及 UCA-10，典型的场景主要出现在快速充放电过程中。由于电压采样误差、电芯一致性差或者保护策略偏保守，BMS 未能在临界阈值处及时切断电路，导致电池处于危险运行区间。

在执行机构本身出现故障，也会导致控制指令无法有效落实，形成控制行为缺失的失效模式。

### （4）信息传递与系统耦合致因场景识别

在 eVTOL 电池系统中，各控制单元之间通过通信网络进行信息交互，系统耦合程度较高。因此，信息传递延迟或失真同样会引发不安全控制行为。

当电池内部出现微短路或局部过热时，BMS 可能因故障分级策略设置不合理，仅将其识别为低等级异常，未向飞控系统或机组人员发送报警信息，导致风险被忽视，这就是典型的 UCA-16 未上报严重故障。

对于 UCA-18，其典型场景为热失控初期，异常信息需经过 BMS、飞控系统及人机界面逐级传递，在多级处理过程中产生延迟，使飞行员未能及时采取应急措施。

### （5）人因与外部环境耦合致因场景

除技术系统外，人因与环境因素同样在致因链中发挥重要作用。

例如，在地面维护过程中，若操作人员未能识别电池轻微鼓包或异常升温现象，且未按规定进行更换或检修，则带缺陷电池进入飞行阶段。在高负载运行条件下，该缺陷可能迅速演化为热失控事故。此外，在极端气候环境下，若系统未针对环境变化进行参数修正，也会显著增加控制失效概率。

人因失效通常源于认知不足、操作不规范及管理机制缺陷，其与技术系统失效相互耦合，进一步放大系统风险。

综上所述，eVTOL 电池热失控相关的不安全控制行为并非孤立事件，而是在

特定运行情境下，由感知失真、决策偏差、执行失效及信息传递滞后等多类因素耦合作用的结果。上述致因场景的识别，不仅揭示了系统控制失效的内在机理，也为后续 Bow-tie 模型中威胁路径的构建提供了清晰的因果依据，从而实现由“行为识别”向“机理解释”的深化转变。

3.3 基于 Bow-tie 模型的电池热失控事故链构建

根据 STPA 分析的 eVTOL 电池热失控风险级事故、风险因素以及不安全控制行为识别，建立 Bow-tie 事故因果综合风险模型。Bow-tie 事故因果模型左侧应用了 FTA 的逻辑结构，右侧应用了 ETA 的逻辑结构。

在本研究中，事故树的顶事件为 eVTOL 电池系统发生热失控。在 eVTOL 电池热失控的风险探究中，根据 3.2 的 STPA 分析结果，将五个一级风险因素及其相应的子因素以事故树的形式表征出来，如图 3-3 所示。由于这五个方面任意一个失效都会导致顶事件发生，因此之间的逻辑关系采用或门相联系。

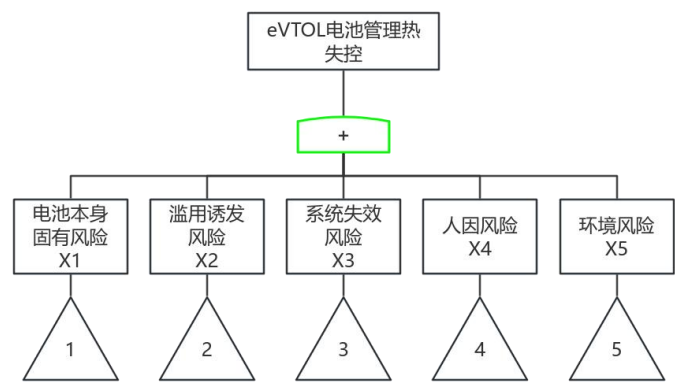


图 3-3 eVTOL 电池热失控故障树

电池本身固有风险主要有电芯结构、材料属性及衰退机理。电芯制造过程中可能存在的缺陷会导致局部反应活性异常，使电池在高倍率或持续载荷下更易形成热点；同时，正极材料的热不稳定性与负极金属锂析出风险进一步降低了电芯的热安全裕度。随着电池循环老化而出现的 SEI 膜退化、活性材料损耗及结构变形，会引起内部阻抗上升并提高局部温升敏感性，从而显著放大热失控触发概率。总体来看，电芯固有风险构成 eVTOL 电池热失控的基础致因链，是整个系统安全设计与监测策略必须重点关注的核心环节。

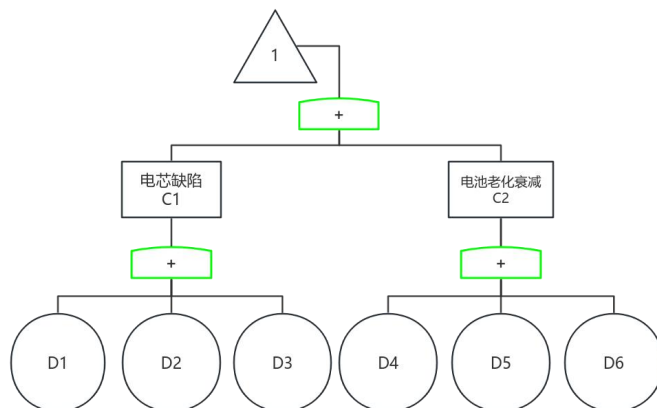


图 3-4 电池本身固有风险故障树

滥用诱发风险指电池在超出设计工况的外部作用下发生异常响应的可能性，主要包括机械、电气及热三类滥用情景。eVTOL 在起降、巡航及复杂气象条件下运行时常经历振动、冲击及外部刺穿等机械载荷，可能导致内部隔膜破裂或活性材料粉化，进而产生内部短路。而电气滥用如过充、过放或异常大电流充电，可能引起极片析锂、铜箔溶解与电解液分解，使电芯进入热失控前的危险状态。此外，热滥用场景如高温暴露或模组局部散热受阻，会使电芯温度持续升高并促使邻近单体发生热扩散。滥用诱发风险体现了外部工况对电池安全边界的破坏效应，是 eVTOL 热失控链条中高度不确定且需重点防范的风险源。

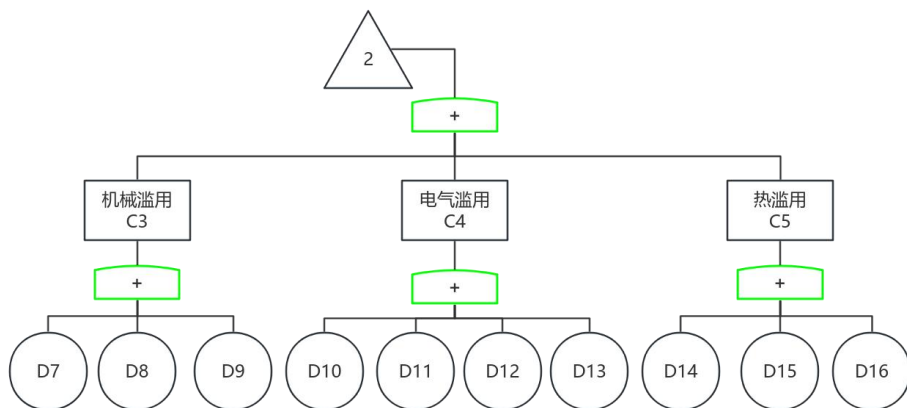


图 3-5 滥用诱发风险故障树

系统失效风险主要源于 eVTOL 电池系统中热管理、电池管理及供电系统等关键支撑子系统的功能异常，是导致热失控由局部问题向系统性事故演化的关键环节。热管理系统故障会使热量无法及时排出，导致模组局部过热；温度传感器漂移或失效则可能造成监测信息偏差，使控制系统无法准确识别危险状态。BMS 的过充/过温保护异常、通信链路失效或主控单元异常均可能导致控制逻辑偏移或失效，加剧电压、电流和温度上的风险累积。在供电系统中，如汇流排或接线端子出现接触不良，也会形成局部电阻发热甚至弧光损伤。

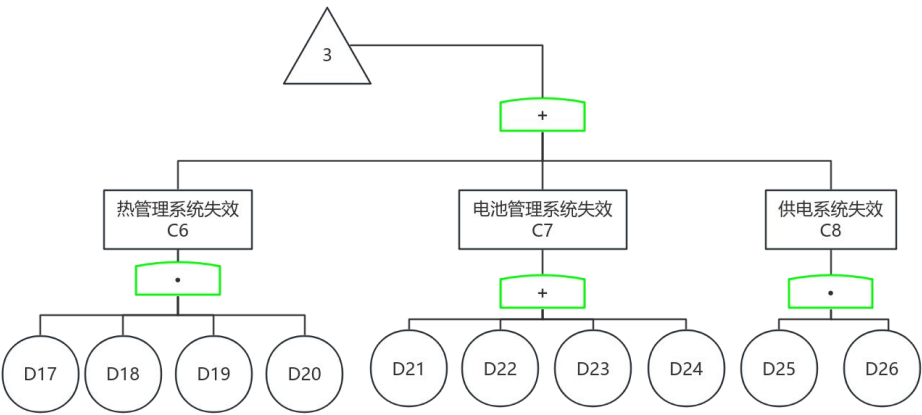


图 3-6 系统失效故障树

人因风险在各种风险评估中都存有一种不可忽视的因素，其在 eVTOL 电池热失控风险中主要体现为操作人员在充放电、飞行准备、维护检修及应急响应过程中的失误行为。eVTOL 运行场景复杂、时间敏感性强，如飞行任务压力或高风险环境下的强飞决策均可能导致操作者忽视电池状态异常信号，从而在热失控早期缺乏有效干预。违规充电、不按规定更换电池、飞行前检查环节疏漏以及维修过程中的误操作均可能直接破坏电池安全管理边界，甚至触发滥用型故障。而在热失控发生期间，错误的应急处置行为可能加速事故扩展或引发二次危害。人因风险是贯穿电池生命周期管理全流程的重要风险源，需通过规程优化、培训强化与智能辅助系统加以系统性控制。

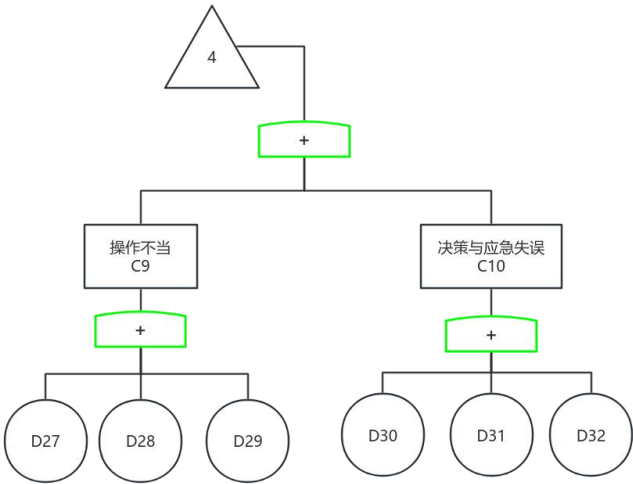


图 3-7 人为因素故障树

环境风险源于 eVTOL 运行所处外部环境对电池性能及安全阈值造成的影响，具有突发性强、不可控性高的特点。极端温度（高温或严寒）会显著影响电解液稳定性与电池内阻，进而改变电池的热稳定边界；雷电、暴雨、潮湿等天气条件可能导致机体受潮、绝缘降低或电气系统受干扰，间接引发短路或热敏事件。此



外，复杂地形起降、高粉尘天气以及高空低气压环境均会增加设备散热难度并加剧电池负载波动。环境风险多变性与不可预测性使其成为影响 eVTOL 电池热失控风险的重要外部因素，是运行规划与安全评估中必须充分考虑的关键变量。

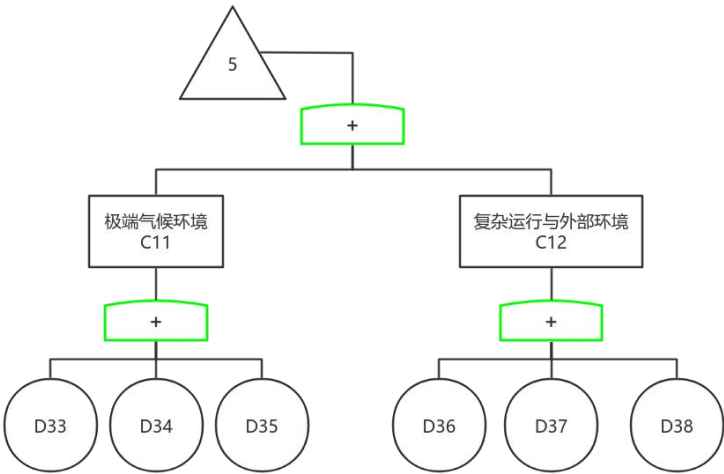


图 3-8 环境风险故障树

根据 STPA 的系统级事故识别重点关注的风险点所导致的事故为 eVTOL 电池热失控，因此针对 eVTOL 电池热失控制定应急处置方案及对应的事故后果等级并将其转换为事件树，作为 Bow-Tie 模型的后半部分，大体可将应急预案转换为如图 3-9 所示的事件树，可分为以下应急处置措施及后果等级其中标号如表 3-8 所示。

表 3-8 应急处置措施及后果等级

| 编号  | 危险     | 解释内容                                                                                | 相关事故          |
|-----|--------|-------------------------------------------------------------------------------------|---------------|
| H-1 | 地面运行危险 | 在地面充电、维护、起飞阶段发生热失控，可能导致地勤人员灼伤、中毒或起火蔓延至机场设施；同时影响机库、地面充电桩等附属系统安全。                     | A-4; A-5      |
| H-2 | 电池功能丧失 | 电池单体或模组因内部短路、SEI 膜破裂或老化退化导致容量骤降、电压异常，造成供能中断。此类功能丧失将直接引起动力中断或控制系统掉电，是飞行阶段最危险的初级失效之一。 | A-1; A-3      |
| H-3 | 动力系统失效 | 电池输出功率不足、BMS 限流错误或电机驱动控制逻辑异常，导致推力不平衡或全机推力丧失。该风险可由热失控诱发的电流异常、电缆烧蚀或高温退磁等机制引起。         | A-1; A-4      |
| H-4 | 飞行控制丧失 | 电池热失控造成控制电路过热、控制算法异常或信号中断，进而导致飞控系统丧失稳定控制能力。包括姿态控制失效、冗余通道烧毁等后果。                      | A-1; A-3; A-4 |
| H-5 | 结构性破坏  | 热失控过程中的高温 和压力骤升导致电池舱或载荷舱结构材料退化、变形或爆裂。若高温区蔓延至机体主承力结构，将造成灾难性坍塌。                       | A-1; A-2; A-3 |

续表 3-8 应急处置措施及后果等级

| 编号  | 危险     | 解释内容                                                                  | 相关事故                  |
|-----|--------|-----------------------------------------------------------------------|-----------------------|
| H-6 | 机载火灾   | 电解液可燃气体在热失控中大量释放，与空气形成爆炸性混合气体，引发舱内火焰喷射、明火燃烧或爆燃。此风险是电池热失控传播阶段的典型表现。    | A-2; A-3;<br>A-4; A-5 |
| H-7 | 二次能量释放 | 在初级热失控未受控制时，邻近模组、电子设备或燃料电池系统被引燃，引起连锁爆炸或二次热释放。此过程显著加剧事故后果，是“热蔓延”的关键环节。 | A-1; A-2;<br>A-3; A-5 |
| H-8 | 应急处置失当 | 热失控诱发的高温、高压和有毒气体使机载消防、隔热或紧急断电系统无法正常工作，或飞行员因信息延迟、传感误报而错失处置时机。          | A-1; A-2;<br>A-3; A-4 |

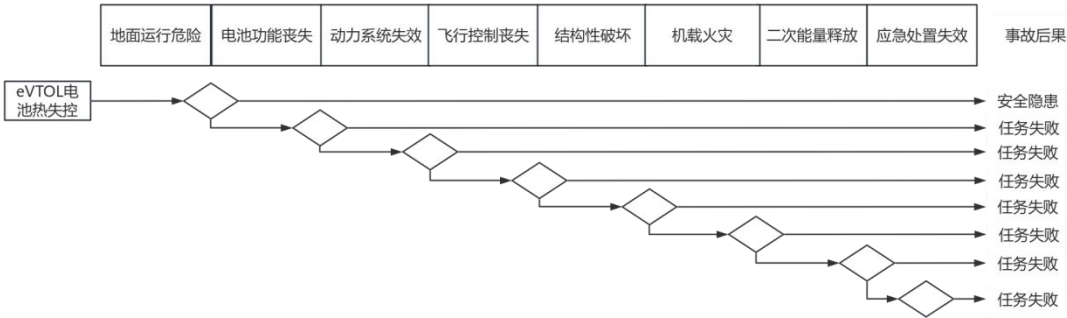


图 3-9 Bow-tie 右侧风险事件后果图

综上所述,根据eVTOL 电池热失控的静态和动态分析作为Bow-tie 风险因素,由 STPA 系统级风险作为 Bow-tie 的事故结果,可以得到一个完整的 Bow-tie 因果结构树,如图 3-10 所示。

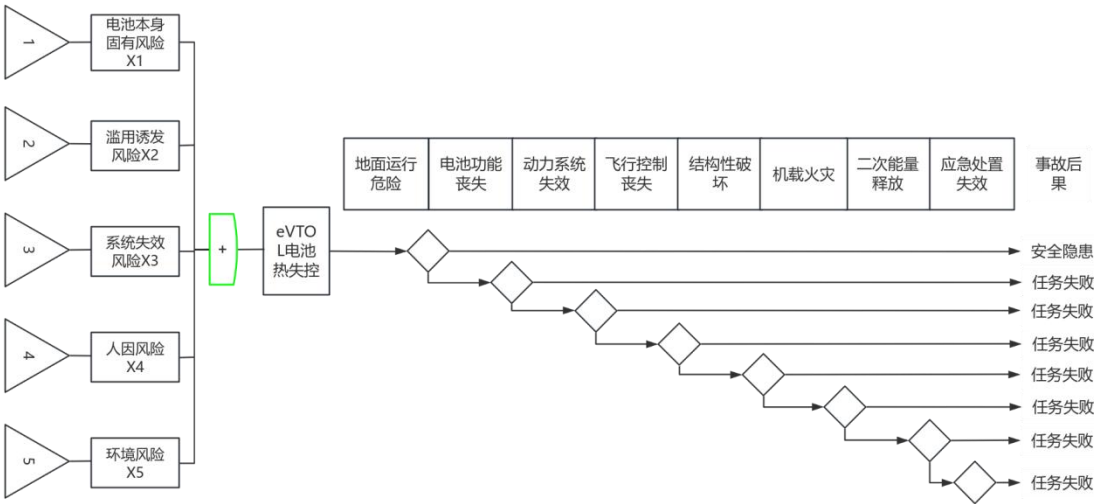


图 3-10 Bow-tie 风险因素因果图

由上图可以看出,左侧为 eVTOL 电池热失控风险影响因素,中间为 eVTOL 电池热失控风险事件,右侧为 eVTOL 电池热失控事故后果,形成了一张可视化

的 eVTOL 电池热失控风险因果关系图，从而对于 eVTOL 电池热失控风险因素概率和事故后果严重性的分析更有帮助。

### 3.4 本章小结

本章节以 eVTOL 电池系统为研究对象，首先基于 STPA 方法，从系统层级出发，对电池在设计、运行及环境耦合作用下可能引发热失控的风险因素进行系统性识别与结构化分析。具体包括对系统控制结构的构建、UCA 的识别，以及致因场景的逐层推演，从而明确电池热失控在不同运行阶段的潜在触发机制及其关键影响因素。在此基础上，将 STPA 分析得到的风险要素按照事故发展逻辑映射至 Bow-tie 模型中，分别构建以热失控为中心事件的致因路径（故障树）与后果演化路径（事件树），实现对事故发生机理与后果扩散过程的统一描述。进一步，通过整合多源风险因素与路径关系，构建电池热失控事故的因果风险模型，并以图形化方式呈现关键风险节点、传导路径及安全屏障位置，从而直观揭示事故演化规律及系统薄弱环节，为后续风险评估与安全控制策略设计提供理论支撑。

## 4 基于 FBN 的 eVTOL 电池热失控风险动态评估

第三章通过 STPA-Bow-tie 模型完成了 eVTOL 电池热失控风险因素的系统识别与事故链结构化建模，清晰地呈现了风险的致因路径、防护屏障与后果演化逻辑，但该模型仍存在局限性：一方面，传统 Bow-tie 模型以定性分析为主，难以量化风险因素间的概率依赖关系及风险动态演化特征；另一方面，其变量状态的二元离散化描述与电池热失控风险的连续性、渐进性形成矛盾，无法适应 eVTOL 复杂运行环境下的动态风险评估需求。基于此，本章将 STPA-Bow-tie 模型进一步转化为模糊贝叶斯网络（FBN）模型，通过节点映射、条件概率表构建，引入模糊数学工具处理数据不完备与认知不确定性，实现风险状态的动态量化推理，为精准识别关键风险因子、支撑实时性风险管控策略制定提供技术支撑。

### 4.1 贝叶斯网络结构模型的构建

在 eVTOL 飞行过程中，电池热失控风险受飞行任务载荷、环境温湿度、放电倍率、充放电策略、健康状态退化程度及冷却系统工况等多种因素的影响，呈现显著的动态变化特征。然而，现阶段对电池热失控的风险评估方法多仍停留在静态分析和单点层面，例如对材料、SEI 膜及温度预测等的研究。尽管本文第三章所构建的 STPA-Bow-tie 模型能够清晰地展示 eVTOL 电池热失控的致因链条、事故演化路径及防护屏障结构，但在风险概率的动态特征方面仍存在一定的局限性，无法实现动态风险状态随运行参数变化的实时更新。

一方面，传统的 Bow-tie 模型中的变量大多采用二元离散描述，通常仅区分“发生”和“不发生”两种状态，这与电池热失控风险形成过程的连续性和渐进性不相符合。另一方面，Bow-tie 图中事件之间的逻辑关系依赖简单的布尔函数，条件概率多被简化为 0 或 1，难以反映风险因素之间的概率性影响。例如，电池温度上升会显著影响热失控发生的可能性，但并非必然导致热失控事件，因此仅用布尔逻辑进行描述难以真实刻画风险传递机制。

基于上述局限，本文将 STPA-Bow-tie 模型转化为具备不确定性表达能力和动态更新机制的贝叶斯网络模型，通过文献统计结果等客观信息以及专家知识等主观信息对条件概率进行修正与训练，实现对电池热失控风险状态的动态评估。借助贝叶斯网络对节点状态和边概率的实时更新能力，可使 eVTOL 电池热失控风险评价结果更符合实际运行环境，从而为飞行前安全决策与在役状态监测提供更加科学与可靠的支持。

### 4.1.1 STPA-Bow-tie 模型与贝叶斯网络的转换

可将 STPA-Bow-tie 向贝叶斯网络的映射过程理解为故障树与事件树在贝叶斯网络结构和参数上的逐步转化。

#### (1) 故障树的转化

从结构层面来看，故障树中的各类事件对应贝叶斯网络中的节点，事件之间的因果关系保持一致，由原故障树中的逻辑门决定节点。也就是说，原故障树的拓扑结构在贝叶斯网络中直接保留。

因果关系图上的基本事件可以作为贝叶斯的叶节点，其先验概率由专家评估给出；中间事件和顶事件则根据逻辑门的类型（如“与门”和“或门”）构建相应的条件概率表（CPT）。其中，“与门”表示子节点必须同时发生才导致上层事件的发生，而“或门”表示任意子节点发生即可触发上层事件。通过这种方式，故障树中原本的布尔逻辑关系被量化为概率条件依赖关系，实现了由确定性逻辑向概率推理框架的转化，从而能够在不确定性条件下开展风险推断与动态更新分析。图 4-1 为逻辑门转化到贝叶斯的示意图，其中 0 表示事件未发生，1 表示事件会发生。

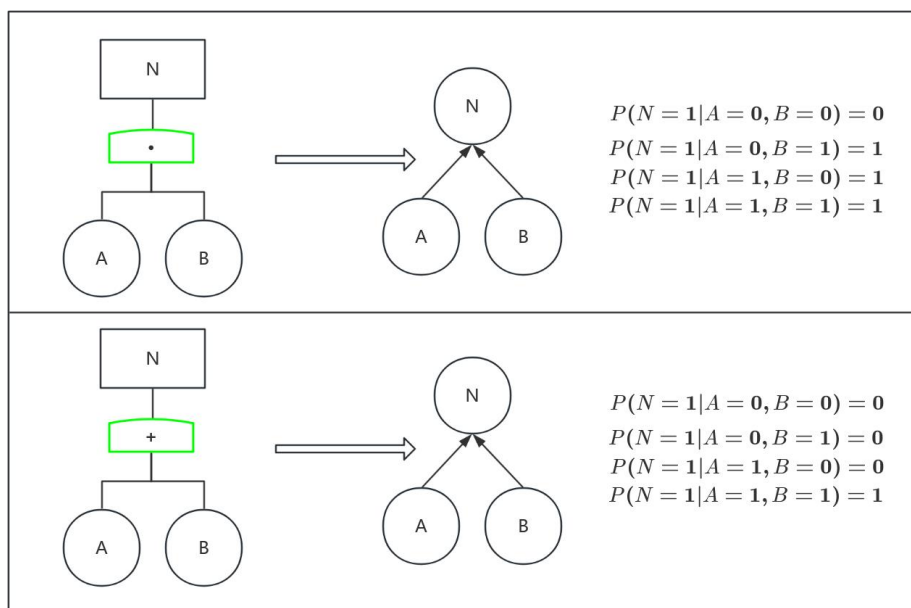


图 4-1 逻辑门到贝叶斯的转换

#### (2) 事件树的转化

事件树用于按时间顺序和事故演化逻辑对安全事故进行因果推理。在将事件树映射为贝叶斯网络时，将事件树中的初始事件和条件事件分别对应为贝叶斯网络中的节点，并依据事故后果及触发条件设置节点的状态和命名。根据事件之间的先后关系与依赖关系，确定贝叶斯网络节点之间的有向连接，从而反映事故演

化路径概率传递过程。

STPA-Bow-tie 向贝叶斯网络的转化实质上可视为将故障树和事件树同时映射到同一贝叶斯网络结构中：故障树提供事故致因侧的因果关系，事件树提供事故后果侧的演化关系，基础事件则对应为贝叶斯网络中的底层节点。通过这一转换，原本以逻辑门描述的确定性因果链被替代为可量化的条件概率依赖结构，实现风险传播的概率化和可更新化，如图 4-2 所示。

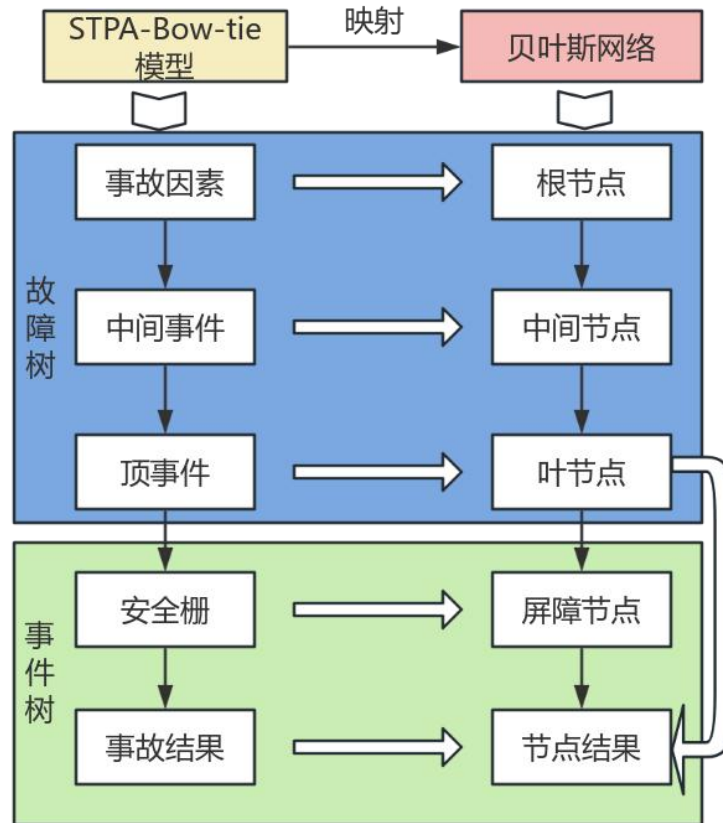


图 4-2 Bow-tie-BN 模型的转换

#### 4.1.2 贝叶斯网络节点的确定

根据 4.1.1 所述的 STPA-Bow-tie 转化成贝叶斯网络的过程，可将蝴蝶结模型中的电池热失控的故障树与事件树结构映射为贝叶斯网络模型。通过该转换，贝叶斯网络能够以概率的形式表达电池热失控致因、状态演练及结果后果之间的依赖关系，从而实现对 eVTOL 电池热失控风险的动态评估。当某一影响因素的状态概率发生变化时，其对应的根节点先验概率将随之调整，网络中相关中间节点的后验概率也会相应更新，最终导致热失控事故后果发生概率的动态变化。为了确保贝叶斯网络模型的完整性和合理性，本文将电池热失控后果节点按照 3.2.2

中划分为 5 个不同的事故等级和 8 个事故后果。后果严重性还受飞行高度、冗余推进系统可用性及应急处置策略有效性等条件因素的影响。

在完成致因因素梳理后，对蝴蝶结中涉及的热、电、机械及控制因素进行归类整合，确定贝叶斯网络节点名称及节点间的依赖关系，构建 eVTOL 电池热失控风险贝叶斯网络模型如图 4-3 所示，各节点名称及状态如 3.3 小节中事故树图所示。其中各节点的含义与图 3-10 蝴蝶结模型对应一致，其余节点名称根据其物理或运行意义直接命名。这样构建的模型可支持对 eVTOL 电池热失控风险进行多场景、多阶段的动态评估与预测，为运行安全管理和系统安全设计提供量化依据。

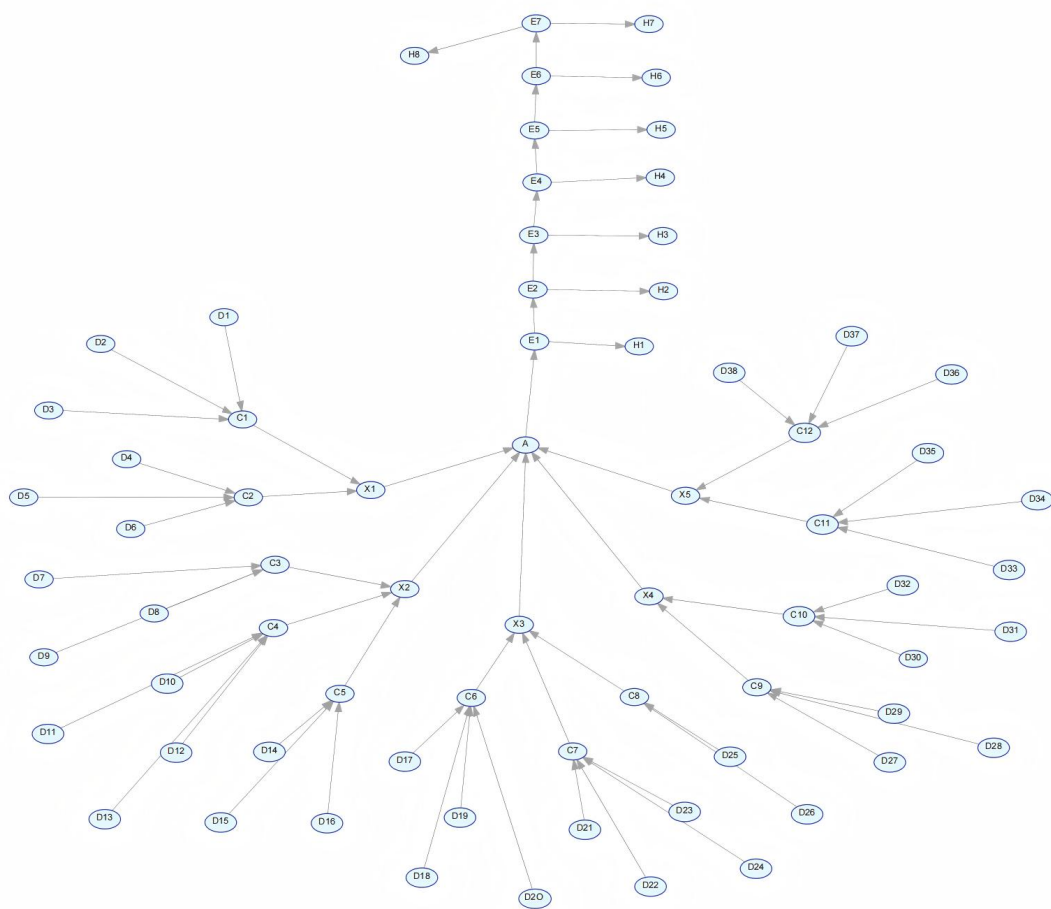


图 4-3 eVTOL 电池热失控贝叶斯模型

## 4.2 贝叶斯网络参数的确定

在前文中已基于 STPA-Bow-tie 模型结合电池热失控和飞行器坠毁案例，完成了 eVTOL 电池热失控风险的系统识别，并对热失控致因链条及事故演化路径进行了结构化展示。在此基础上，将蝴蝶结模型进一步转化为贝叶斯网络结构，利用贝叶斯网络能够处理不确定性和实现状态更新的特性，为 eVTOL 电池热失



控风险的动态分析提供了模型基础。然而,要实现热失控事故概率的动态量化,需要依赖较为完备和可追溯的数据支持。但当前阶段,电池运行与退化数据、冷却系统响应特性、人为因素等难以获取实际数据和存在巨大的不确定性,并且具有较强的场景依赖性。所以,本文采用专家咨询的方式获取关键参数信息,并引入模糊集理论对专家经验性描述语言进行量化处理,以实现贝叶斯网络条件概率参数的合理估计<sup>[72]</sup>。通过对多个专家评价结果的模糊综合赋权处理,可在数据缺乏和不确定性较高的情况下,构建相对可靠的 eVTOL 电池热失控贝叶斯网络风险模型,为后续的动态风险推演和安全预警提供可行的参数基础。

#### 4.2.1 基于模糊集理论的专家评定标准

依据专家经验的风险评估方法具有实施便捷、适应性强的特点,但其结果很容易受专家主观判断的影响,可信度相对较低。通常提高可信度的做法就是扩大专家参与数量或者提高专家专业深度与覆盖范围,但这会增加数据收集成本,并不利于快速形成评估结论。为兼顾可操作性与可信度,本文对参与评估的专家引入差异化权重分配机制。

所以,本文会根据选取所邀请专家的职务、工作年限、工作/研究相关性及学历四项指标进行量化评分权重的赋值。例如,工作年限较短的专家在该指标中得分较低,而学历层次较高者则获得相应较高的权重,如表 4-1 所示。

表 4-1 专家评分权重赋值表

| 指标       | 分类        | 分数 |
|----------|-----------|----|
| 专家职务     | 高级工程师/教授  | 5  |
|          | 副高级/副教授   | 4  |
|          | 中级/相关研究教师 | 3  |
|          | 初级/相关研究学者 | 2  |
|          | 其他        | 1  |
| 教育背景     | 博士        | 5  |
|          | 硕士        | 4  |
|          | 学士        | 3  |
|          | 专科        | 2  |
|          | 职专        | 1  |
| 工作年限     | >20 年     | 5  |
|          | 16~20 年   | 4  |
|          | 11~15 年   | 3  |
|          | 6~10 年    | 2  |
|          | 1~5 年     | 1  |
| 工作/研究相关性 | 完全相关      | 5  |
|          | 强相关       | 4  |
|          | 相关        | 3  |
|          | 弱相关       | 2  |
|          | 有所研究      | 1  |



每位专家在四项指标中的得分相加得到其综合权重得分，再对综合得分进行归一化处理，获得最终的专家权重系数。该系数用于对专家评价结果进行加权，从而有效降低单一专家意见对整体结果的影响，提高模型参数估计的稳健性，专家 A 评价权重计算公式如式 4-1 所示

$$W_A = W_{A1} + W_{A2} + W_{A3} + W_{A4} \quad (4-1)$$

$$P_A = \frac{W_A}{\sum_{i=1}^n W_i} \quad (4-2)$$

式中， $W_A$  表示专家 A 的权重得分， $W_{A1}$ 、 $W_{A2}$ 、 $W_{A3}$ 、 $W_{A4}$  表示对专家 A 的职务、工作年限、年龄及学历四项指标的权重分类得分； $P_A$  表示专家 A 的权重比例， $n$  表示专家数量。

同时，为解决专家在评价过程中采用的描述性语言难以精确量化的问题，本文引入模糊评价标准，将语言性判断转化为区间化概率取值。这样不但可以使描述性判断划分为由低到高的（0-1）区间，设置十档概率等级，用以表示从“基本不可能发生”到“一定会发生”的风险发生程度，对应的模糊评价标准见表 4-2。这样就可以将专家经验有效转化为可用于贝叶斯网络参数训练的量化数据。

表 4-2 模糊概率等级划分

| 评价语言 | 描述性语言    | 评定概率值   | 梯形模糊数             |
|------|----------|---------|-------------------|
| AL   | 基本不可能发生  | 0-0.1   | (0,0,0.1,0.2)     |
| QL   | 很难发生     | 0.1-0.2 | (0,0.1,0.2,0.3)   |
| L    | 发生的可能性很小 | 0.2-0.3 | (0.1,0.2,0.3,0.4) |
| ML   | 发生的可能小   | 0.3-0.4 | (0.2,0.3,0.4,0.5) |
| M    | 有一定可能发生  | 0.4-0.5 | (0.3,0.4,0.5,0.6) |
| MH   | 较可能发生    | 0.5-0.6 | (0.4,0.5,0.6,0.7) |
| H    | 可能发生     | 0.6-0.7 | (0.5,0.6,0.7,0.8) |
| QH   | 很可能发生    | 0.7-0.8 | (0.6,0.7,0.8,0.9) |
| AH   | 基本会发生    | 0.8-0.9 | (0.7,0.8,0.9,1.0) |
| B    | 一定会发生    | 0.9-1.0 | (0.8,0.9,1.0,1.0) |

为提高评价结果的可靠性，专家在判断某事件发生的可能性时通常会采用模糊性表达，比如“介于可能性较小与可能性较大之间”或“可能性不太确定，但不会太高”等。此类描述难以直接对应到单一确定的概率值，因此需要将专家的语言性判断转化为模糊数进行处理。所以，本文采用模糊数对专家判断进行量化，主要使用梯形模糊数来表示不确定概率区间。如图 4-4 所示，梯形模糊数表示为  $A2(0.6,0.7,0.8,0.9)$ ，分别对应不同程度的模糊性和专家判断区间范围，从而更准确地反映其主观认知的不确定性。

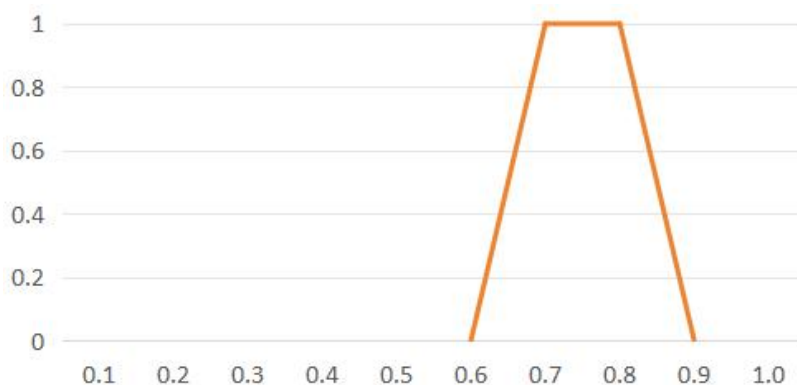


图 4-4 梯形模糊数图示

在所有专家对同一事件给出概率评价后,需要对多位专家提供的模糊数进行聚合,得到该事件的综合模糊数,用来表示整体专家意见。合并过程如下:首先将每位专家的模糊数按照其权重进行加权处理,再把加权的模糊数进行方根法并进行归一化处理,就得到了该事件的聚类模糊数。方根法求解过程如下所示。

#### (1) 建立层次结构模型

首先依据已建立的评价体系,将被评价体系分为目标层,准则层以及指标层三个层次,其中指标层根据实际情况和需要还可继续向下划分为一级指标、二级指标甚至三级指标等,随后依据上述三个层次建立结构模型。

#### (2) 建立判断对比矩阵

两两进行同等标准下的比较,得到判断矩阵  $A$ 。所采用的量化比较打分标准见表 4-3。

$$A_{n \times m} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{bmatrix} \quad (4-3)$$

表 4-3 判断矩阵要素比较尺度表

| 序号 | 标度含义                                                                             | 比值               |
|----|----------------------------------------------------------------------------------|------------------|
| 1  | 前者元素 $i$ 和后者元素 $j$ 相比较, $i$ 与 $j$ 同样重要                                           | $a_{ij}=1$       |
| 2  | 前者元素 $i$ 和后者元素 $j$ 相比较, $i$ 与 $j$ 略微重要                                           | $a_{ij}=3$       |
| 3  | 前者元素 $i$ 和后者元素 $j$ 相比较, $i$ 与 $j$ 明显重要                                           | $a_{ij}=5$       |
| 4  | 前者元素 $i$ 和后者元素 $j$ 相比较, $i$ 与 $j$ 强烈重要                                           | $a_{ij}=7$       |
| 5  | 前者元素 $i$ 和后者元素 $j$ 相比较, $i$ 与 $j$ 绝对重要                                           | $a_{ij}=9$       |
| 6  | 表示元素 $i$ 与元素 $j$ 的重要性介于上述判断之间                                                    | $a_{ij}=2,4,6,8$ |
| 7  | 若元素 $i$ 与元素 $j$ 的相对重要程度标度为 $a_{ij}$ , 则元素 $j$ 与 $i$ 的相对重要程度标度是 $a_{ji}=1/a_{ij}$ | 倒数               |

## (3) 计算判断矩阵相对权重

本文采取几何平均法（方根法）计算权重，公式如下：

$$W_i = \frac{\left( \prod_{j=1}^n a_{ij} \right)^{\frac{1}{n}}}{\sum_{i=1}^n \left( \prod_{j=1}^n a_{ij} \right)^{\frac{1}{n}}}, (i=1, 2, \dots, n) \quad (4-4)$$

通过这种计算方式不但保留了专家判断的不确定性，而且可以体现出对不同专家在评估过程中的影响程度，得到更精确的风险概率模糊数，如式 4-5 所示。

$$A_{aggregated} = \left( \sum_{i=1}^n \omega_i S_{i,1}, \sum_{i=1}^n \omega_i S_{i,2}, \sum_{i=1}^n \omega_i S_{i,3}, \sum_{i=1}^n \omega_i S_{i,4} \right) \quad (4-5)$$

式中， $A_{aggregated}$  表示事件聚类后的模糊数； $\omega_i$  表示第  $i$  名专家的权重比例； $S_{i,1}$  表示第  $i$  名专家对事件评价模糊概率中对应的数值； $n$  表示专家数量。

经过模糊集对专家模糊评价语言的处理，则模糊数与模糊语言之间的隶属度函数  $g(x)$  如式 4-6 所示。

$$g(x) = \begin{cases} 0, & (x \leq a) \\ \frac{x-a}{b-a}, & (a < x \leq b) \\ 1, & (b < x \leq c) \\ \frac{d-x}{d-c}, & (c < x \leq d) \\ 0, & (x > d) \end{cases} \quad (4-6)$$

使用质心指标法对聚类模糊数做进一步处理转化为可能的模糊数，其中质心指标法如式 4-7 所示。

$$FPS = \frac{\int g(x) x dx}{\int g(x) dx} \quad (4-7)$$

式中，FPS 表示模糊可能性得分； $g(x)$  表示隶属度函数。当  $A_{aggregated}$  为  $(a_1, a_2, a_3, a_4)$  时，模糊可能性得分如式 4-8 所示。

$$FPS = \frac{\int g(x) x dx}{\int g(x) dx} = \frac{(a_3 + a_4)^2 - a_3 a_4 - (a_1 + a_2)^2 + a_1 a_2}{3(a_3 + a_4 - a_1 - a_2)} \quad (4-8)$$

将模糊概率得分转化为实际概率，如式 4-9 所示。

$$FR = \begin{cases} \frac{1}{10^K}, FPS \neq 0 \\ 0, FPS = 0 \\ K = \left( \frac{1-FPS}{FPS} \right)^{\frac{1}{3}} \times 2.301 \end{cases} \quad (4-9)$$

#### 4.2.2 诊断推理分析

为精准辨识 eVTOL 电池热失控安全风险的核心影响因素，本文借助贝叶斯网络的逆向推理功能，将目标节点概率设定为 100%。在此情况下，网络中所有节点的概率状态会随之动态更新，依托该逆向推理流程，可快速锁定后验概率最高的节点，此节点对应着风险最为显著的影响因素。具体的推理流程如图 4-5 所示。

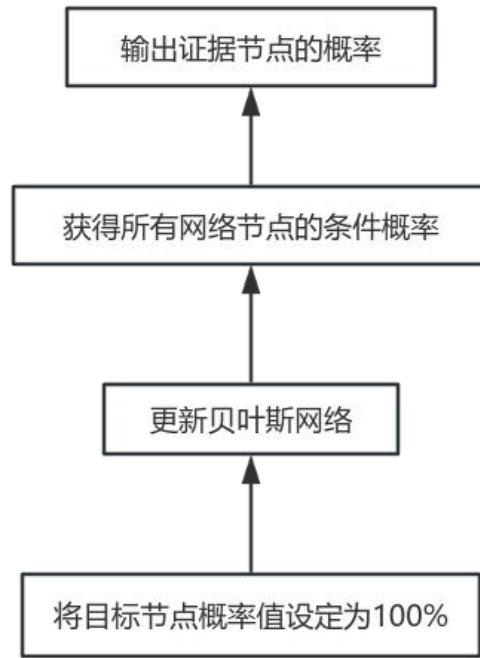


图 4-5 专断推断流程图

本文进一步开展概率推理验证工作：将 5 个二级指标分别设定为证据节点，观察单一因素变化时 eVTOL 电池热失控安全风险水平的波动情况，以此验证前期风险评估结果的可靠性。通过贝叶斯网络的数据更新机制，结合新增数据可重新测算 eVTOL 电池热失控安全风险事件的发生概率及底事件的概率重要度，进而获得更为精准的电池热失控安全风险评估结论。

### 4.2.3 敏感性分析

敏感性分析是一种聚焦于量化评估各类潜在影响因素对目标事件作用显著性的不确定性分析手段。其核心思路在于，从诸多变量中筛选出对目标事件结果起决定性作用的敏感性因素，进而深度分析这些因素发生变动时，会以何种方式影响目标事件的相关指标与最终结果，同时明确该类影响的强度及敏感性等级。借助这一分析过程，决策者能够更为清晰地把握目标事件在面对不确定因素波动时的承受能力与稳健水平，以此为依据制定出更具稳定性和适应性的策略方案。

敏感性分析的优势在于，能够从繁杂的变量体系中精准识别出起关键作用的“少数变量”，并对其影响程度进行量化，为精细化的风险管理与科学决策提供支撑，进而推动针对性改进措施的提出，降低风险事件的发生概率。

在贝叶斯网络的分析框架中，节点的后验概率是一项核心信息。该概率以先验概率为基础，经过数据或实证信息修正后得到，尽管能够间接反映节点的重要程度，但并非衡量节点重要性的唯一标准。其对应的数学原理如下：

假设存在某一响应函数  $D(x) = t(x)$ ， $X = x_1, x_2, \dots, x_n$ ，那么变量  $x_i$  的偏导数就代表响应函数  $D$  对该变量的敏感度，具体计算公式如式 4-10 所示。

$$SA_i = \frac{\partial D}{\partial x_i} \quad (4-10)$$

当  $SA_i > 0$  时，响应函数  $D(x)$  会随着变量  $x_i$  的增大而上升；当  $SA_i < 0$  时  $D(x)$  会随着  $x_i$  的增大而下降；当  $SA_i = 0$  时， $D(x)$  不会随着变量  $x_i$  的变化而产生改变。

贝叶斯网络下的敏感性分析，核心要点在于深入探究参数变化与目标节点条件概率之间的动态概率关联，这一过程充分彰显了贝叶斯自动推理机制的核心内涵。通过分析网络内各参数的细微变动，研究其对特定目标节点状态概率分布产生的影响并重新进行评估，能够帮助分析者深度洞悉系统的不确定性特征与预测结果的稳健性。除此之外，将敏感性分析的相关结果整合到决策支持系统中，还可实现对项目风险的实时监控与动态评估，助力管理者及时掌握风险态势以及各类变量间的相互作用关系，并根据实际需求调整风险管理策略，有效应对各类潜在的风险挑战。

## 5 应用分析

### 5.1 Lilium 飞行器电池应用与布局概况

2019 年，德国 Lilium 公司研制的空中出租车原型机是一款面向城市空中交通的 5 座级电动垂直起降飞行器，其总体构型采用固定翼与分布式电推进相结合的技术路线，在机翼与前翼上布置多组涵道电风扇，从而对电池系统提出了高比能与高比功协同优化的要求。在能源系统设计方面，Lilium 并未采用电池结构一体化方案<sup>[73]</sup>，而是构建了一种以模块化与冗余设计为核心的电池系统架构。其动力电源基于锂离子电池体系，并采用的是硅主导负极材料以提升能量密度与功率性能。

在系统层级，Lilium 电池系统由多个相互独立的电池包组成，每架飞行器配置约 10 个独立运行的电池模块，各模块在电气上具备独立监测、控制与故障隔离能力。当某一电池包发生异常时，电池管理系统能够迅速切断故障单元，避免故障向其他模块传播，同时依靠剩余电池包维持推进系统与飞行控制系统的基本供电，从而为飞行器争取应急处置与安全着陆时间。这种多电池包分布式冗余设计体现了当前 eVTOL 适航安全中“失效安全”与“容错运行”的核心理念，电池布局如图 5-1 所示。

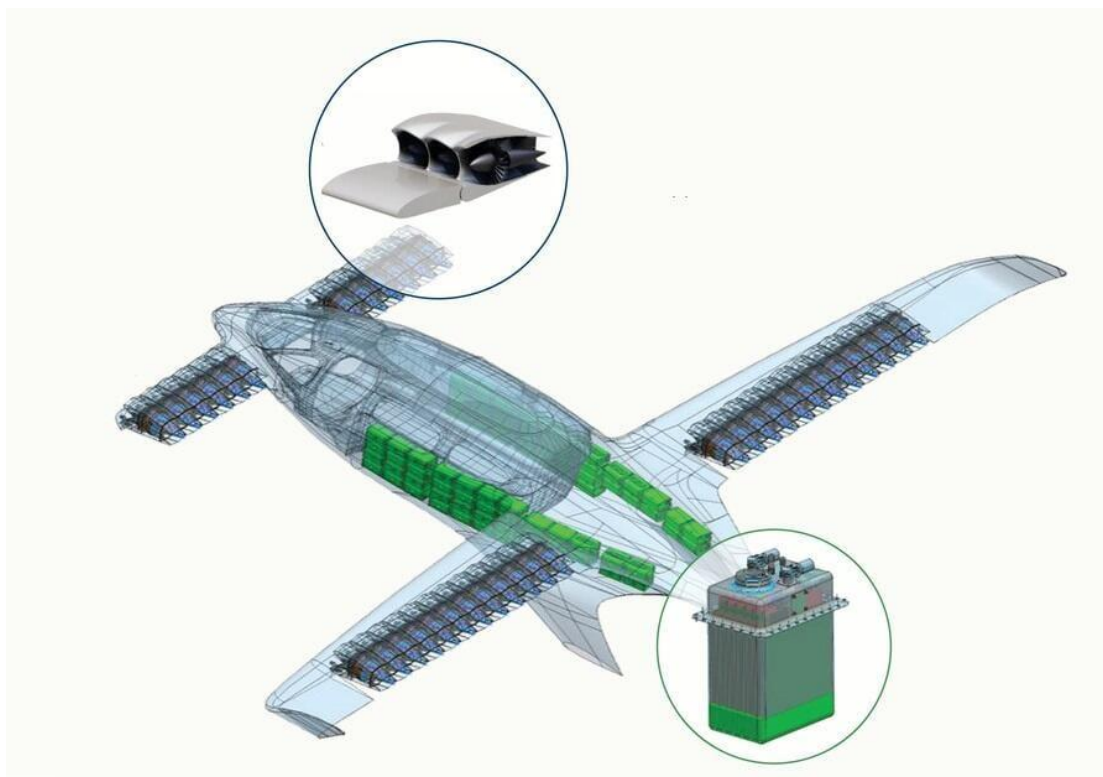


图 5-1 Lilium 电池布局

该 eVTOL 选用了高性能锂离子电池作为主储能单元。电池系统整体采用

800V—1000V 级高压平台，以降低大功率输出条件下的电流等级，从而减少导线损耗和热负荷，提高系统效率，电池参数如表 5-1 所示。

表 5-1 Lilium 电池参数

| 参数类别   | 指标内容                       |
|--------|----------------------------|
| 电池类型   | 高性能锂离子电池                   |
| 电池集成方式 | 模块化分布式集成，以独立电池包形式布置于机体内部   |
| 电池包数量  | 10 个独立电池模块                 |
| 系统标称电压 | 800V—1000V                 |
| 单体能量密度 | >300Wh/kg                  |
| 最大放电倍率 | 8C-10 C                    |
| 快速充电能力 | 支持快充（约 30min）              |
| 电池管理方式 | 分布式 BMS（每个电池包独立监测+系统级协调控制） |
| 未来技术路线 | 持续优化硅负极锂电池                 |

## 5.2 基于模糊贝叶斯网络的 eVTOL 电池热失控安全风险评价

### 5.2.1 贝叶斯网络结构构建

根据文献搜索等方式，归纳总结 eVTOL 电池热失控的风险因素，再结合 Lilium 电池布局与电池选用方案的现状分析，依据第 3 章构建的 eVTOL 电池热失控风险评价指标体系，构建 Lilium 电池热失控的模糊贝叶斯网络结构模型，贝叶斯结构模型如图 5-2 所示。

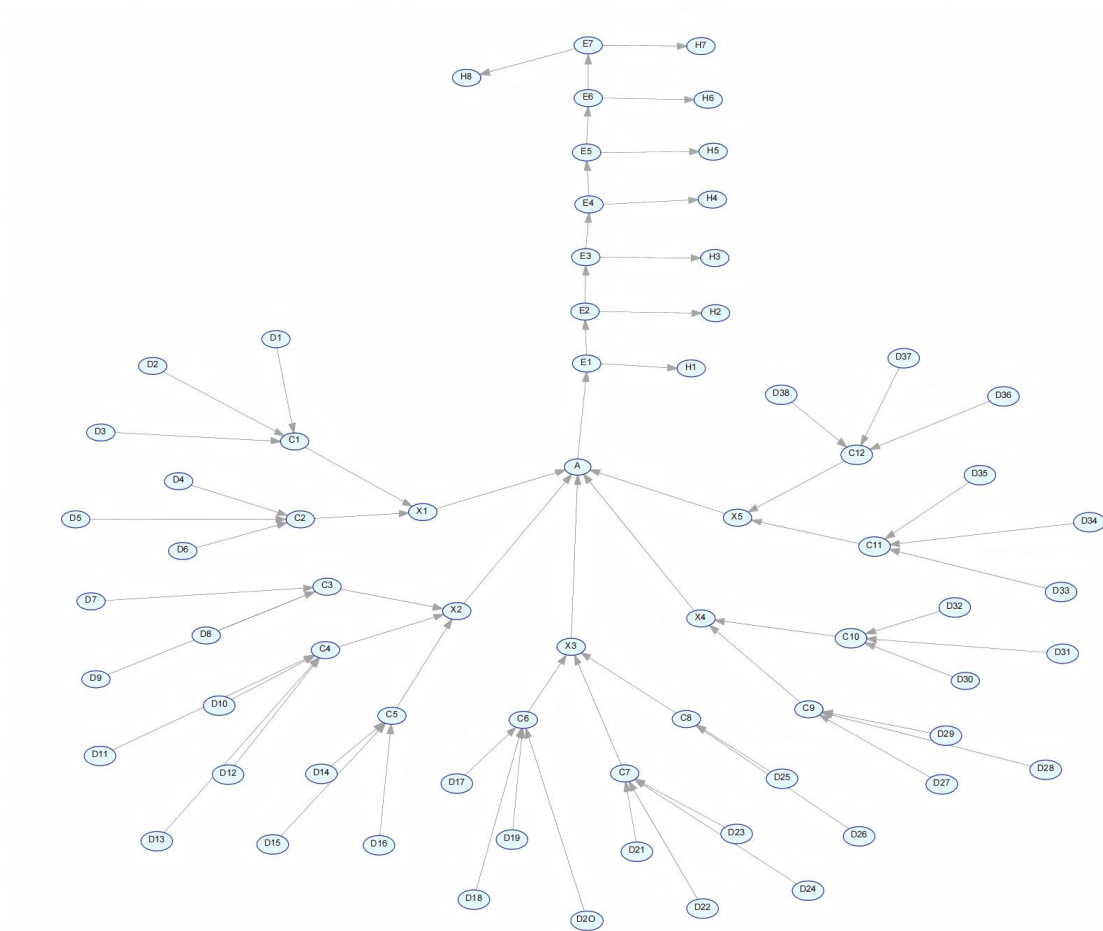


图 5-2 Lilium 电池热失控的模糊贝叶斯网络结构模型

## 5.2.2 贝叶斯网络参数的确定

### (1) 网络根节点先验概率的计算

#### 1) 模糊梯形 AHP 计算分析

为深化 eVTOL 电池热失控贝叶斯网络风险模型的概率分析，本研究确定了时间节点的先验概率和条件概率。由于 eVTOL 作为新兴的飞行器，目前仍处于试飞阶段，尚缺乏充分的电池热失控事故案例与历史数据，难以通过经验统计法获取可靠的概率参数。因此，根据第 4 章的相关内容说明，本研究采用专家模糊梯形评价法确定事件节点的先验概率。

为确保评估结果的科学性与代表性，本文选取 30 位与 eVTOL 电池热失控研究密切相关的专家参与打分，其中电池技术与能源系统方向专家 14 人，航空安全与适航领域专家 8 人，eVTOL 运行与工程应用相关专家 8 人；专家来源包括高校科研机构、航空制造企业及运行管理单位，兼顾理论与工程实践；大多数专家均具有 10 年以上从业经历，多数具备硕士及以上学历及中高级职称。根



据专家权重综合其职务层级、从业年限、学历背景及行业经验等因素进行确定，其权重值见表 5-2。

表 5-2 专家权重

| 专家 | 1      | 2      | 3      | 4      | 5      | 6      | 7      | 8      | 9      | 10     |
|----|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|
| 权重 | 0.0560 | 0.0265 | 0.0383 | 0.0413 | 0.0265 | 0.0324 | 0.0236 | 0.0413 | 0.0236 | 0.0295 |
| 专家 | 11     | 12     | 13     | 14     | 15     | 16     | 17     | 18     | 19     | 20     |
| 权重 | 0.0531 | 0.0295 | 0.0383 | 0.0236 | 0.0206 | 0.0236 | 0.0295 | 0.0413 | 0.0236 | 0.0531 |
| 专家 | 21     | 22     | 23     | 24     | 25     | 26     | 27     | 28     | 29     | 30     |
| 权重 | 0.0236 | 0.0354 | 0.0354 | 0.0354 | 0.0265 | 0.0354 | 0.0383 | 0.0324 | 0.0295 | 0.0324 |

本文以三级节点作为算例展示模糊梯形层次的计算过程。

专家 2 对一级指标 A 的评价为

$$A = \begin{bmatrix} 1 & \frac{1}{5} & \frac{1}{7} \\ 5 & 1 & \frac{1}{3} \\ 7 & 3 & 1 \end{bmatrix}$$

使用几何平均法（方根法）计算权重得到

$$W_{A1} = \frac{\left( \prod_{j=1}^n a_{ij} \right)^{\frac{1}{n}}}{\sum_{i=1}^n \left( \prod_{j=1}^n a_{ij} \right)^{\frac{1}{n}}} = (0.0719, 0.2790, 0.6491)$$

通过模糊等级划分可以得到权重对应的模糊数如表 5-3 所示。

表 5-3 计算概率对应的梯形模糊数

|    | 权重     | 模糊数               |
|----|--------|-------------------|
| D1 | 0.0719 | (0,0,0.1,0.2)     |
| D2 | 0.2790 | (0.1,0.2,0.3,0.4) |
| D3 | 0.6491 | (0.5,0.6,0.7,0.8) |

通过专家咨询与模糊数转换，并使用公式 4-5 对专家意见进行聚合，最终获得各事件节点的聚类模糊数及相应的先验概率。

$$A_{aggregated} = \left( \sum_{i=1}^n \omega_i S_{i,1}, \sum_{i=1}^n \omega_i S_{i,2}, \sum_{i=1}^n \omega_i S_{i,3}, \sum_{i=1}^n \omega_i S_{i,4} \right) = \begin{bmatrix} 0.1156 & 0.1770 & 0.2770 & 0.3770 \\ 0.2018 & 0.2959 & 0.3959 & 0.4959 \\ 0.2817 & 0.3599 & 0.4599 & 0.5599 \end{bmatrix}$$

则模糊性可能得分为

$$FPS = \frac{(a_3 + a_4)^2 - a_3 a_4 - (a_1 + a_2)^2 + a_1 a_2}{3(a_3 + a_4 - a_1 - a_2)} = (0.2334, 0.3469, 0.4135)$$

将模糊概率得分转化为实际概率

$$FR = (0.0380\%, 0.1441\%, 0.2599\%)$$

根据上面的推理过程，进而得出一级指标、二级指标和三级指标的其他风险因素的模糊风险概率。

将

## 2) 风险概率的确定

如前文所述，电池热失控风险的识别主要基于既有电池安全事故案例的系统梳理与归纳。在此基础上，采用蝴蝶结模型对电池热失控的致因机理及其潜在后果进行初步结构化分析，明确引发电池热失控的关键诱因以及事故可能演化产生的主要失效后果。由此构建的电池热失控蝴蝶结模型如图 3-10 所示。

为进一步实现对电池热失控风险事件及其发生概率的动态表征与量化分析，本文将上述蝴蝶结模型转化为贝叶斯网络结构，构建 STPA-Bow-tie-BN 复合风险分析模型，其对应的贝叶斯网络拓扑结构如图 4-3 所示。相关研究假设、技术路线以及数据来源为该 STPA-Bow-tie-BN 模型的概率推断与风险评估提供了必要的数据基础与理论支撑。

在此基础上，为开展 eVTOL 电池热失控风险的定量分析，还需对所建立的贝叶斯网络模型中各节点事件的发生概率进行合理设定，包括先验概率与条件概率的确定。正如第四章所述，本文中相关概率参数主要通过以下途径获得：一是基于历史事故数据及公开统计资料进行估计；二是引入专家判断并采用模糊方法进行综合确定。本文利用公开统计资料得到电池运行过程中处于高风险环境条件的发生概率，并参考相关文献资料，确定了电池内部关键部件故障及管理系统失效等事件的发生概率<sup>[6]</sup>，如表 5-4 所示。

表 5-4 基于历史数据和相应资料的风险因素概率

| 序号  | 事件        | 失效率                  |
|-----|-----------|----------------------|
| D1  | 电芯制造缺陷    | $1.3 \times 10^{-6}$ |
| D12 | 内外部短路     | $1.9 \times 10^{-6}$ |
| D13 | 充电电压/电流过大 | $5.0 \times 10^{-4}$ |
| D20 | 温度传感器故障   | $1.0 \times 10^{-6}$ |
| D21 | 过充保护机制失效  | $7.8 \times 10^{-6}$ |
| D22 | 过温保护机制失效  | $3.2 \times 10^{-6}$ |
| D23 | 通讯系统故障    | $1.6 \times 10^{-5}$ |
| D24 | 主控单元故障    | $1.5 \times 10^{-5}$ |

对于难以通过统计资料直接获取发生概率的事件，本文采用基于专家判断的模糊评估方法对其概率进行确定。在实例分析过程中，按照（1）模糊梯形 AHP 计算分析，得到对应事件的聚合模糊概率值，并完成对模糊可能性评分的计算和对实际概率的转化。部分节点的先验概率其结果汇总如下表 5-5 所示。

表 5-5 根节点先验概率表

| 事件节点 | 专家评估模糊数 |        |        |        | FPS    | 先验概率    |
|------|---------|--------|--------|--------|--------|---------|
| D2   | 0.2018  | 0.2959 | 0.3959 | 0.4959 | 0.3469 | 0.1441% |
| D3   | 0.2817  | 0.3599 | 0.4599 | 0.5599 | 0.4135 | 0.2599% |
| D4   | 0.2121  | 0.3121 | 0.4121 | 0.5121 | 0.3621 | 0.1663% |
| D5   | 0.3664  | 0.4540 | 0.5540 | 0.6540 | 0.5060 | 0.5218% |
| D6   | 0.0233  | 0.0808 | 0.1808 | 0.2808 | 0.1379 | 0.0058% |
| D7   | 0.1994  | 0.2994 | 0.3994 | 0.4994 | 0.3494 | 0.1476% |
| D8   | 0.0425  | 0.0903 | 0.1903 | 0.2903 | 0.1490 | 0.0077% |
| D9   | 0.3602  | 0.4507 | 0.5507 | 0.6507 | 0.5023 | 0.5083% |
| D10  | 0.0611  | 0.1130 | 0.2130 | 0.3130 | 0.1710 | 0.0128% |
| D11  | 0.2729  | 0.3404 | 0.4404 | 0.5404 | 0.3958 | 0.2242% |
| D14  | 0.4201  | 0.5201 | 0.6201 | 0.7201 | 0.5701 | 0.8045% |
| D15  | 0.1330  | 0.2153 | 0.3153 | 0.4153 | 0.2683 | 0.0610% |
| D16  | 0.0525  | 0.1032 | 0.2032 | 0.3032 | 0.1615 | 0.0104% |
| D17  | 0.3991  | 0.4929 | 0.5929 | 0.6929 | 0.5440 | 0.6766% |
| D18  | 0       | 0      | 0.1000 | 0.2000 | 0.0667 | 0.0003% |
| D19  | 0.1171  | 0.2038 | 0.3038 | 0.4038 | 0.2560 | 0.0521% |
| D25  | 0.5442  | 0.6442 | 0.7442 | 0.8442 | 0.6942 | 1.7756% |
| D26  | 0.1699  | 0.2699 | 0.3670 | 0.4670 | 0.3184 | 0.1083% |
| D27  | 0.1015  | 0.1614 | 0.2614 | 0.3614 | 0.2180 | 0.0301% |
| D28  | 0.1425  | 0.2292 | 0.3292 | 0.4292 | 0.2814 | 0.0716% |
| D29  | 0.3575  | 0.4510 | 0.5510 | 0.6510 | 0.5021 | 0.5075% |
| D30  | 0.1705  | 0.2676 | 0.3652 | 0.4652 | 0.3169 | 0.1065% |
| D31  | 0.0667  | 0.1274 | 0.2274 | 0.3274 | 0.1840 | 0.0166% |
| D32  | 0.3655  | 0.4587 | 0.5587 | 0.6587 | 0.5098 | 0.5358% |
| D33  | 0.1127  | 0.1785 | 0.2785 | 0.3785 | 0.2342 | 0.0384% |
| D34  | 0.1448  | 0.2324 | 0.3324 | 0.4324 | 0.2845 | 0.0743% |
| D35  | 0.3472  | 0.4398 | 0.5398 | 0.6398 | 0.4911 | 0.4692% |
| D36  | 0.0923  | 0.1504 | 0.2504 | 0.3504 | 0.2074 | 0.0253% |
| D37  | 0.3900  | 0.4814 | 0.5814 | 0.6814 | 0.5328 | 0.6277% |
| D38  | 0.1204  | 0.2168 | 0.3168 | 0.4168 | 0.2674 | 0.0603% |

## (2) 中间节点及叶节点条件概率的确定

在电芯缺陷因素方面，其节点分别为电芯制造缺陷、正极材料热不稳定性和负极材料锂析出风险。结合实际风险概率，根据专家经验判断，其贝叶斯网络节点概率如下表 5-6 所示。

表 5-6 电芯缺陷条件概率表

| 序号 | 节点事件 |    |    | 专家评估聚类模糊数 |        |        |        | FPS    | 先验概率     |
|----|------|----|----|-----------|--------|--------|--------|--------|----------|
|    | D1   | D2 | D3 |           |        |        |        |        |          |
| 1  | Y    | Y  | Y  | 0.0000    | 0.0168 | 0.1168 | 0.2168 | 0.0807 | 6.64E-06 |
| 2  | Y    | Y  | N  | 0.0180    | 0.0463 | 0.1463 | 0.2463 | 0.1083 | 2.25E-05 |
| 3  | Y    | N  | Y  | 0.0251    | 0.0870 | 0.1870 | 0.2870 | 0.1434 | 6.68E-05 |
| 4  | Y    | N  | N  | 0.0174    | 0.0699 | 0.1699 | 0.2699 | 0.1278 | 4.32E-05 |
| 5  | N    | Y  | Y  | 0.0206    | 0.0699 | 0.1699 | 0.2699 | 0.1284 | 4.39E-05 |

续表 5-6 电芯缺陷条件概率表

| 序号 | 节点事件 |    |    | 专家评估聚类模糊数 |        |        |        | FPS    | 先验概率     |
|----|------|----|----|-----------|--------|--------|--------|--------|----------|
|    | D1   | D2 | D3 |           |        |        |        |        |          |
| 6  | N    | Y  | N  | 0.0628    | 0.1425 | 0.2425 | 0.3425 | 0.1959 | 2.07E-04 |
| 7  | N    | N  | Y  | 0.0853    | 0.1735 | 0.2735 | 0.3735 | 0.2254 | 3.37E-04 |
| 8  | N    | N  | N  | 0.0853    | 0.1794 | 0.2794 | 0.3794 | 0.2303 | 3.63E-04 |

在机械滥用因素方面，其节点事件分别为循环老化导致 SEI 膜失效、活性材料损耗与结构变形和老化导致热失控敏感性增加。结合实际风险概率，根据专家经验判断，其贝叶斯网络节点概率如下表 5-7 所示。

表 5-7 电池老化衰减条件概率表

| 序号 | 节点事件 |    |    | 专家评估聚类模糊数 |        |        |        | FPS    | 先验概率     |
|----|------|----|----|-----------|--------|--------|--------|--------|----------|
|    | D4   | D5 | D6 |           |        |        |        |        |          |
| 1  | Y    | Y  | Y  | 0.0041    | 0.0136 | 0.1136 | 0.2136 | 0.0787 | 5.95E-06 |
| 2  | Y    | Y  | N  | 0.0124    | 0.0351 | 0.1351 | 0.2351 | 0.0980 | 1.50E-05 |
| 3  | Y    | N  | Y  | 0.0136    | 0.0534 | 0.1534 | 0.2534 | 0.1134 | 2.71E-05 |
| 4  | Y    | N  | N  | 0.0212    | 0.0608 | 0.1608 | 0.2608 | 0.1208 | 3.48E-05 |
| 5  | N    | Y  | Y  | 0.0599    | 0.1263 | 0.2263 | 0.3263 | 0.1819 | 1.59E-04 |
| 6  | N    | Y  | N  | 0.0549    | 0.1280 | 0.2280 | 0.3280 | 0.1825 | 1.61E-04 |
| 7  | N    | N  | Y  | 0.0375    | 0.1012 | 0.2012 | 0.3012 | 0.1572 | 9.40E-05 |
| 8  | N    | N  | N  | 0.0265    | 0.0646 | 0.1646 | 0.2646 | 0.1249 | 3.96E-05 |

在机械滥用因素方面，其节点事件分别为飞行碰撞/起降冲击、外部刺穿和长期振动导致结构松动。结合实际风险概率，根据专家经验判断，其贝叶斯网络节点概率如下表 5-8 所示。

表 5-8 机械滥用条件

| 序号 | 节点事件 |    |    | 专家评估聚类模糊数 |        |        |        | FPS    | 先验概率     |
|----|------|----|----|-----------|--------|--------|--------|--------|----------|
|    | D7   | D8 | D9 |           |        |        |        |        |          |
| 1  | Y    | Y  | Y  | 0.0041    | 0.0177 | 0.1177 | 0.2177 | 0.0821 | 7.16E-06 |
| 2  | Y    | Y  | N  | 0.0041    | 0.0324 | 0.1324 | 0.2324 | 0.0944 | 1.29E-05 |
| 3  | Y    | N  | Y  | 0.0150    | 0.0628 | 0.1628 | 0.2628 | 0.1215 | 3.56E-05 |
| 4  | Y    | N  | N  | 0.0286    | 0.0935 | 0.1935 | 0.2935 | 0.1494 | 7.78E-05 |
| 5  | N    | Y  | Y  | 0.0785    | 0.1667 | 0.2667 | 0.3667 | 0.2186 | 3.03E-04 |
| 6  | N    | Y  | N  | 0.0622    | 0.1440 | 0.2440 | 0.3440 | 0.1970 | 2.11E-04 |
| 7  | N    | N  | Y  | 0.0814    | 0.1696 | 0.2696 | 0.3696 | 0.2216 | 3.18E-04 |
| 8  | N    | N  | N  | 0.0752    | 0.1605 | 0.2605 | 0.3605 | 0.2129 | 2.77E-04 |

在电气滥用因素方面，其节点事件分别为过充、过放、内外部短路和充电电压/电流过大。结合实际风险概率，根据专家经验判断，其贝叶斯网络节点概率如下表 5-9 所示。

表 5-9 电气滥用条件概率表

| 序号 | 节点事件 |     |     |     | 专家评估聚类模糊数 |        |        |        | FPS    | 先验概率     |
|----|------|-----|-----|-----|-----------|--------|--------|--------|--------|----------|
|    | D10  | D11 | D12 | D13 |           |        |        |        |        |          |
| 1  | Y    | Y   | Y   | Y   | 0.0053    | 0.0201 | 0.1201 | 0.2201 | 0.0843 | 8.00E-06 |
| 2  | Y    | Y   | Y   | N   | 0.0248    | 0.0758 | 0.1758 | 0.2758 | 0.1340 | 5.17E-05 |
| 3  | Y    | Y   | N   | Y   | 0.0041    | 0.0348 | 0.1348 | 0.2348 | 0.0964 | 1.41E-05 |
| 4  | Y    | Y   | N   | N   | 0.0372    | 0.0858 | 0.1858 | 0.2858 | 0.1444 | 6.86E-05 |
| 5  | Y    | N   | Y   | Y   | 0.0071    | 0.0354 | 0.1354 | 0.2354 | 0.0973 | 1.47E-05 |
| 6  | Y    | N   | Y   | N   | 0.0581    | 0.1283 | 0.2283 | 0.3283 | 0.1833 | 1.64E-04 |
| 7  | Y    | N   | N   | Y   | 0.0139    | 0.0440 | 0.1440 | 0.2440 | 0.1056 | 2.04E-05 |
| 8  | Y    | N   | N   | N   | 0.0195    | 0.0416 | 0.1416 | 0.2416 | 0.1046 | 1.96E-05 |

续表 5-9 电气滥用条件概率表

| 序号 | 节点事件 |     |     |     | 专家评估聚类模糊数 |        |        |        | FPS    | 先验概率     |
|----|------|-----|-----|-----|-----------|--------|--------|--------|--------|----------|
|    | D10  | D11 | D12 | D13 |           |        |        |        |        |          |
| 9  | N    | Y   | Y   | Y   | 0.0221    | 0.0466 | 0.1466 | 0.2466 | 0.1092 | 2.33E-05 |
| 10 | N    | Y   | Y   | N   | 0.0316    | 0.0634 | 0.1634 | 0.2634 | 0.1248 | 3.94E-05 |
| 11 | N    | Y   | N   | Y   | 0.0153    | 0.0534 | 0.1534 | 0.2534 | 0.1137 | 2.74E-05 |
| 12 | N    | Y   | N   | N   | 0.0245    | 0.0513 | 0.1513 | 0.2513 | 0.1135 | 2.72E-05 |
| 13 | N    | N   | Y   | Y   | 0.0330    | 0.0708 | 0.1708 | 0.2708 | 0.1312 | 4.77E-05 |
| 14 | N    | N   | Y   | N   | 0.0150    | 0.0484 | 0.1484 | 0.2484 | 0.1095 | 2.36E-05 |
| 15 | N    | N   | N   | Y   | 0.0239    | 0.0587 | 0.1587 | 0.2587 | 0.1196 | 3.34E-05 |
| 16 | N    | N   | N   | N   | 0.0142    | 0.0360 | 0.1360 | 0.2360 | 0.0990 | 1.57E-05 |

在热滥用因素方面，其节点事件分别为高温环境暴露、电池模组局部过热和相邻电芯热失控传导。结合实际风险概率，根据专家经验判断，其贝叶斯网络节点概率如下表 5-10 所示。

表 5-10 热滥用条件概率表

| 序号 | 节点事件 |     |     |        | 专家评估聚类模糊数 |        |        | FPS    | 先验概率     |
|----|------|-----|-----|--------|-----------|--------|--------|--------|----------|
|    | D14  | D15 | D16 |        |           |        |        |        |          |
| 1  | Y    | Y   | Y   | 0.0242 | 0.0720    | 0.1720 | 0.2720 | 0.1307 | 4.70E-05 |
| 2  | Y    | Y   | N   | 0.0307 | 0.0926    | 0.1926 | 0.2926 | 0.1490 | 7.70E-05 |
| 3  | Y    | N   | Y   | 0.0218 | 0.0619    | 0.1619 | 0.2619 | 0.1219 | 3.60E-05 |
| 4  | Y    | N   | N   | 0.0124 | 0.0664    | 0.1664 | 0.2664 | 0.1240 | 3.85E-05 |
| 5  | N    | Y   | Y   | 0.0776 | 0.1599    | 0.2599 | 0.3599 | 0.2128 | 2.76E-04 |
| 6  | N    | Y   | N   | 0.0811 | 0.1646    | 0.2646 | 0.3646 | 0.2174 | 2.97E-04 |
| 7  | N    | N   | Y   | 0.0699 | 0.1596    | 0.2596 | 0.3596 | 0.2113 | 2.70E-04 |
| 8  | N    | N   | N   | 0.1100 | 0.1991    | 0.2991 | 0.3991 | 0.2509 | 4.86E-04 |

在热管理系统失效因素方面，其节点事件分别为空气冷却系统故障、液体冷却系统故障、PCM 冷却系统失效和温度传感器故障。结合实际风险概率，根据专家经验判断，其贝叶斯网络节点概率如下表 5-11 所示。

表 5-11 热管理系统失效条件概率表

| 序号 | 节点事件 |     |     |     | 专家评估聚类模糊数 |        |        |        | FPS    | 先验概率     |
|----|------|-----|-----|-----|-----------|--------|--------|--------|--------|----------|
|    | D17  | D18 | D19 | D20 |           |        |        |        |        |          |
| 1  | Y    | Y   | Y   | Y   | 0.0071    | 0.0218 | 0.1218 | 0.2218 | 0.0860 | 8.75E-06 |
| 2  | Y    | Y   | Y   | N   | 0.0260    | 0.0826 | 0.1826 | 0.2826 | 0.1398 | 6.08E-05 |
| 3  | Y    | Y   | N   | Y   | 0.0053    | 0.0236 | 0.1236 | 0.2236 | 0.0872 | 9.27E-06 |
| 4  | Y    | Y   | N   | N   | 0.0177    | 0.0463 | 0.1463 | 0.2463 | 0.1082 | 2.25E-05 |
| 5  | Y    | N   | Y   | Y   | 0.0147    | 0.0431 | 0.1431 | 0.2431 | 0.1050 | 1.99E-05 |
| 6  | Y    | N   | Y   | N   | 0.0242    | 0.0661 | 0.1661 | 0.2661 | 0.1258 | 4.06E-05 |
| 7  | Y    | N   | N   | Y   | 0.0853    | 0.1705 | 0.2705 | 0.3705 | 0.2230 | 3.25E-04 |
| 8  | Y    | N   | N   | N   | 0.0183    | 0.0611 | 0.1611 | 0.2611 | 0.1206 | 3.45E-05 |
| 9  | N    | Y   | Y   | Y   | 0.0147    | 0.0437 | 0.1437 | 0.2437 | 0.1055 | 2.03E-05 |
| 10 | N    | Y   | Y   | N   | 0.0251    | 0.0906 | 0.1906 | 0.2906 | 0.1463 | 7.20E-05 |
| 11 | N    | Y   | N   | Y   | 0.0038    | 0.0487 | 0.1487 | 0.2487 | 0.1079 | 2.22E-05 |
| 12 | N    | Y   | N   | N   | 0.0139    | 0.0628 | 0.1628 | 0.2628 | 0.1213 | 3.53E-05 |
| 13 | N    | N   | Y   | Y   | 0.0133    | 0.0504 | 0.1504 | 0.2504 | 0.1109 | 2.48E-05 |
| 14 | N    | N   | Y   | N   | 0.0086    | 0.0395 | 0.1395 | 0.2395 | 0.1010 | 1.71E-05 |
| 15 | N    | N   | N   | Y   | 0.0239    | 0.0587 | 0.1587 | 0.2587 | 0.1196 | 3.34E-05 |
| 16 | N    | N   | N   | N   | 0.0292    | 0.0714 | 0.1714 | 0.2714 | 0.1310 | 4.75E-05 |

在电池管理系统失效因素方面，其节点事件分别为过充保护机制失效、过温保护机制失效、通讯系统故障和主控单元故障。结合实际风险概率，根据专家经验判断，其贝叶斯网络节点概率如下表 5-12 所示。

表 5-12 电池管理系统失效条件概率表

| 序号 | 节点事件 |     |     |     | 专家评估聚类模糊数 |        |        |        | FPS    | 先验概率     |
|----|------|-----|-----|-----|-----------|--------|--------|--------|--------|----------|
|    | D21  | D22 | D23 | D24 |           |        |        |        |        |          |
| 1  | Y    | Y   | Y   | Y   | 0.0171    | 0.0404 | 0.1404 | 0.2404 | 0.1032 | 1.86E-05 |
| 2  | Y    | Y   | Y   | N   | 0.0206    | 0.0490 | 0.1490 | 0.2490 | 0.1109 | 2.48E-05 |
| 3  | Y    | Y   | N   | Y   | 0.0142    | 0.0490 | 0.1490 | 0.2490 | 0.1098 | 2.39E-05 |
| 4  | Y    | Y   | N   | N   | 0.0041    | 0.0189 | 0.1189 | 0.2189 | 0.0831 | 7.54E-06 |
| 5  | Y    | N   | Y   | Y   | 0.0038    | 0.0159 | 0.1159 | 0.2159 | 0.0806 | 6.60E-06 |
| 6  | Y    | N   | Y   | N   | 0.0083    | 0.0445 | 0.1445 | 0.2445 | 0.1052 | 2.01E-05 |
| 7  | Y    | N   | N   | Y   | 0.0041    | 0.0271 | 0.1271 | 0.2271 | 0.0900 | 1.06E-05 |
| 8  | Y    | N   | N   | N   | 0.0198    | 0.0708 | 0.1708 | 0.2708 | 0.1290 | 4.47E-05 |
| 9  | N    | Y   | Y   | Y   | 0.0183    | 0.0469 | 0.1469 | 0.2469 | 0.1088 | 2.30E-05 |
| 10 | N    | Y   | Y   | N   | 0.0336    | 0.0997 | 0.1997 | 0.2997 | 0.1554 | 8.99E-05 |
| 11 | N    | Y   | N   | Y   | 0.0277    | 0.0882 | 0.1882 | 0.2882 | 0.1448 | 6.93E-05 |
| 12 | N    | Y   | N   | N   | 0.0342    | 0.0855 | 0.1855 | 0.2855 | 0.1437 | 6.73E-05 |
| 13 | N    | N   | Y   | Y   | 0.0422    | 0.1077 | 0.2077 | 0.3077 | 0.1634 | 1.08E-04 |
| 14 | N    | N   | Y   | N   | 0.0168    | 0.0549 | 0.1549 | 0.2549 | 0.1152 | 2.88E-05 |
| 15 | N    | N   | N   | Y   | 0.0487    | 0.1103 | 0.2103 | 0.3103 | 0.1667 | 1.16E-04 |
| 16 | N    | N   | N   | N   | 0.0534    | 0.1189 | 0.2189 | 0.3189 | 0.1746 | 1.38E-04 |

在供电系统失效因素方面，其节点事件分别为线路连接接触不良和汇流排故障。结合实际风险概率，根据专家经验判断，其贝叶斯网络节点概率如下表 5-13 所示。

表 5-13 供电系统失效条件概率表

| 序号 | 节点事件 |     | 专家评估聚类模糊数 | FPS    | 先验概率   |        |        |          |
|----|------|-----|-----------|--------|--------|--------|--------|----------|
|    | D25  | D26 |           |        |        |        |        |          |
| 1  | Y    | Y   | 0.0083    | 0.0307 | 0.1307 | 0.2307 | 0.0936 | 1.25E-05 |
| 2  | Y    | N   | 0.0074    | 0.0404 | 0.1404 | 0.2404 | 0.1016 | 1.74E-05 |
| 3  | N    | Y   | 0.0572    | 0.1354 | 0.2354 | 0.3354 | 0.1890 | 1.82E-04 |
| 4  | N    | N   | 0.1124    | 0.2047 | 0.3047 | 0.4047 | 0.2560 | 5.20E-04 |

在操作不当因素方面，其节点事件分别为违规充电、飞行前电池状态检查疏漏和维修误操作。结合实际风险概率，根据专家经验判断，其贝叶斯网络节点概率如下表 5-14 所示。

表 5-14 操作不当条件概率表

| 序号 | 节点事件 |     |     | 专家评估聚类模糊数 |        |        |        | FPS    | 先验概率     |
|----|------|-----|-----|-----------|--------|--------|--------|--------|----------|
|    | D27  | D28 | D29 |           |        |        |        |        |          |
| 1  | Y    | Y   | Y   | 0.0292    | 0.0882 | 0.1882 | 0.2882 | 0.1450 | 6.97E-05 |
| 2  | Y    | Y   | N   | 0.0041    | 0.0401 | 0.1401 | 0.2401 | 0.1008 | 1.69E-05 |
| 3  | Y    | N   | Y   | 0.0083    | 0.0501 | 0.1501 | 0.2501 | 0.1098 | 2.39E-05 |
| 4  | Y    | N   | N   | 0.0109    | 0.0608 | 0.1608 | 0.2608 | 0.1191 | 3.29E-05 |
| 5  | N    | Y   | Y   | 0.0490    | 0.1301 | 0.2301 | 0.3301 | 0.1832 | 1.63E-04 |
| 6  | N    | Y   | N   | 0.0422    | 0.1212 | 0.2212 | 0.3212 | 0.1747 | 1.38E-04 |
| 7  | N    | N   | Y   | 0.0628    | 0.1395 | 0.2395 | 0.3395 | 0.1934 | 1.98E-04 |
| 8  | N    | N   | N   | 0.0590    | 0.1304 | 0.2304 | 0.3304 | 0.1852 | 1.70E-04 |

在决策与应急失误因素方面，其节点事件分别为风险环境强飞、热失控期间操作错误和未按照规程更换电池。结合实际风险概率，根据专家经验判断，其贝叶斯网络节点概率如下表 5-15 所示。

表 5-15 决策与应急失误条件概率表

| 序号 | 节点事件 |     |     | 专家评估聚类模糊数 |        |        |        | FPS    | 先验概率     |
|----|------|-----|-----|-----------|--------|--------|--------|--------|----------|
|    | D30  | D31 | D32 |           |        |        |        |        |          |
| 1  | Y    | Y   | Y   | 0.0215    | 0.0386 | 0.1386 | 0.2386 | 0.1025 | 1.81E-05 |
| 2  | Y    | Y   | N   | 0.0097    | 0.0339 | 0.1339 | 0.2339 | 0.0966 | 1.42E-05 |
| 3  | Y    | N   | Y   | 0.0531    | 0.1136 | 0.2136 | 0.3136 | 0.1702 | 1.25E-04 |
| 4  | Y    | N   | N   | 0.0578    | 0.1460 | 0.2460 | 0.3460 | 0.1980 | 2.15E-04 |
| 5  | N    | Y   | Y   | 0.0147    | 0.0472 | 0.1472 | 0.2472 | 0.1085 | 2.27E-05 |
| 6  | N    | Y   | N   | 0.0224    | 0.0749 | 0.1749 | 0.2749 | 0.1328 | 5.01E-05 |
| 7  | N    | N   | Y   | 0.0684    | 0.1537 | 0.2537 | 0.3537 | 0.2061 | 2.47E-04 |
| 8  | N    | N   | N   | 0.0785    | 0.1690 | 0.2690 | 0.3690 | 0.2206 | 3.13E-04 |

在极端气候环境因素方面，其节点事件分别为高/低温环境、雷电天气和暴雨/潮湿环境。结合实际风险概率，根据专家经验判断，其贝叶斯网络节点概率如下表 5-16 所示。

表 5-16 极端气候环境条件概率表

| 序号 | 节点事件 |     |     | 专家评估聚类模糊数 |        |        |        | FPS    | 先验概率     |
|----|------|-----|-----|-----------|--------|--------|--------|--------|----------|
|    | D33  | D34 | D35 |           |        |        |        |        |          |
| 1  | Y    | Y   | Y   | 0.0147    | 0.0454 | 0.1454 | 0.2454 | 0.1070 | 2.15E-05 |
| 2  | Y    | Y   | N   | 0.0150    | 0.0457 | 0.1457 | 0.2457 | 0.1073 | 2.17E-05 |
| 3  | Y    | N   | Y   | 0.0056    | 0.0274 | 0.1274 | 0.2274 | 0.0905 | 1.08E-05 |
| 4  | Y    | N   | N   | 0.0782    | 0.1490 | 0.2490 | 0.3490 | 0.2038 | 2.38E-04 |
| 5  | N    | Y   | Y   | 0.0224    | 0.0543 | 0.1543 | 0.2543 | 0.1156 | 2.93E-05 |
| 6  | N    | Y   | N   | 0.0720    | 0.1434 | 0.2434 | 0.3434 | 0.1981 | 2.15E-04 |
| 7  | N    | N   | Y   | 0.0333    | 0.0622 | 0.1622 | 0.2622 | 0.1241 | 3.86E-05 |
| 8  | N    | N   | N   | 0.0767    | 0.1596 | 0.2596 | 0.3596 | 0.2124 | 2.75E-04 |

在复杂运行与外部环境因素方面，其节点事件分别为复杂地形起降、高粉尘等天气和高空低气压环境。结合实际风险概率，根据专家经验判断，其贝叶斯网络节点概率如下表 5-17 所示。

表 5-17 极端气候环境条件概率表

| 序号 | 节点事件 |     |     | 专家评估聚类模糊数 |        |        |        | FPS    | 先验概率     |
|----|------|-----|-----|-----------|--------|--------|--------|--------|----------|
|    | D36  | D37 | D38 |           |        |        |        |        |          |
| 1  | Y    | Y   | Y   | 0.0145    | 0.0445 | 0.1445 | 0.2445 | 0.1062 | 2.09E-05 |
| 2  | Y    | Y   | N   | 0.0097    | 0.0425 | 0.1425 | 0.2425 | 0.1037 | 1.90E-05 |
| 3  | Y    | N   | Y   | 0.0121    | 0.0490 | 0.1490 | 0.2490 | 0.1095 | 2.36E-05 |
| 4  | Y    | N   | N   | 0.0224    | 0.0451 | 0.1451 | 0.2451 | 0.1080 | 2.23E-05 |
| 5  | N    | Y   | Y   | 0.0245    | 0.0637 | 0.1637 | 0.2637 | 0.1238 | 3.83E-05 |
| 6  | N    | Y   | N   | 0.0150    | 0.0460 | 0.1460 | 0.2460 | 0.1075 | 2.19E-05 |
| 7  | N    | N   | Y   | 0.0398    | 0.0796 | 0.1796 | 0.2796 | 0.1397 | 6.05E-05 |
| 8  | N    | N   | N   | 0.0823    | 0.1614 | 0.2614 | 0.3614 | 0.2148 | 2.86E-04 |

根据上述计算过程，同样可以推导出二级指标的条件概率表。

在复杂运行与外部环境因素方面，其节点事件分别为复杂地形起降、高粉尘等天气和高空低气压环境。结合实际风险概率，根据专家经验判断，其贝叶斯网络节点概率如下表 5-18 至 5-23 所示。

表 5-18 电池本身固有风险条件概率表

| 序号 | 节点事件 |    | 专家评估聚类模糊数 |        |        |        | FPS    | 先验概率     |
|----|------|----|-----------|--------|--------|--------|--------|----------|
|    | C1   | C2 |           |        |        |        |        |          |
| 1  | Y    | Y  | 0.0150    | 0.0416 | 0.1416 | 0.2416 | 0.1038 | 1.91E-05 |
| 2  | Y    | Y  | 0.0484    | 0.1186 | 0.2186 | 0.3186 | 0.1735 | 1.35E-04 |
| 3  | Y    | N  | 0.1121    | 0.2059 | 0.3059 | 0.4059 | 0.2569 | 5.27E-04 |
| 4  | Y    | N  | 0.1345    | 0.2245 | 0.3245 | 0.4245 | 0.2762 | 6.72E-04 |

表 5-19 滥用诱发风险条件概率表

| 序号 | 节点事件 |    |    | 专家评估聚类模糊数 |        |        |        | FPS    | 先验概率     |
|----|------|----|----|-----------|--------|--------|--------|--------|----------|
|    | C3   | C4 | C5 |           |        |        |        |        |          |
| 1  | Y    | Y  | Y  | 0.0348    | 0.0664 | 0.1664 | 0.2664 | 0.1278 | 4.32E-05 |
| 2  | Y    | Y  | N  | 0.0142    | 0.0410 | 0.1410 | 0.2410 | 0.1032 | 1.86E-05 |
| 3  | Y    | N  | Y  | 0.0212    | 0.0732 | 0.1732 | 0.2732 | 0.1312 | 4.77E-05 |
| 4  | Y    | N  | N  | 0.0053    | 0.0327 | 0.1327 | 0.2327 | 0.0948 | 1.32E-05 |
| 5  | N    | Y  | Y  | 0.1201    | 0.2109 | 0.3109 | 0.4109 | 0.2624 | 5.66E-04 |
| 6  | N    | Y  | N  | 0.0581    | 0.1348 | 0.2348 | 0.3348 | 0.1887 | 1.81E-04 |
| 7  | N    | N  | Y  | 0.0708    | 0.1593 | 0.2593 | 0.3593 | 0.2112 | 2.69E-04 |
| 8  | N    | N  | N  | 0.1431    | 0.2375 | 0.3375 | 0.4375 | 0.2884 | 7.77E-04 |

表 5-20 系统失效风险条件概率表

| 序号 | 节点事件 |    |    | 专家评估聚类模糊数 |        |        |        | FPS    | 先验概率     |
|----|------|----|----|-----------|--------|--------|--------|--------|----------|
|    | C6   | C7 | C8 |           |        |        |        |        |          |
| 1  | Y    | Y  | Y  | 0.0080    | 0.0271 | 0.1271 | 0.2271 | 0.0906 | 1.09E-05 |
| 2  | Y    | Y  | N  | 0.0147    | 0.0407 | 0.1407 | 0.2407 | 0.1030 | 1.85E-05 |
| 3  | Y    | N  | Y  | 0.0174    | 0.0546 | 0.1546 | 0.2546 | 0.1150 | 2.87E-05 |
| 4  | Y    | N  | N  | 0.0383    | 0.0740 | 0.1740 | 0.2740 | 0.1348 | 5.29E-05 |
| 5  | N    | Y  | Y  | 0.0112    | 0.0224 | 0.1224 | 0.2224 | 0.0872 | 9.27E-06 |
| 6  | N    | Y  | N  | 0.0206    | 0.0398 | 0.1398 | 0.2398 | 0.1033 | 1.87E-05 |
| 7  | N    | N  | Y  | 0.1062    | 0.1717 | 0.2717 | 0.3717 | 0.2274 | 3.48E-04 |
| 8  | N    | N  | N  | 0.1304    | 0.2121 | 0.3121 | 0.4121 | 0.2651 | 5.86E-04 |

表 5-21 人因风险条件概率表

| 序号 | 节点事件 |     | 专家评估聚类模糊数 |        |        |        | FPS    | 先验概率     |
|----|------|-----|-----------|--------|--------|--------|--------|----------|
|    | C9   | C10 |           |        |        |        |        |          |
| 1  | Y    | Y   | 0.0263    | 0.0761 | 0.1761 | 0.2761 | 0.1345 | 5.24E-05 |
| 2  | Y    | Y   | 0.0180    | 0.0484 | 0.1484 | 0.2484 | 0.1100 | 2.40E-05 |
| 3  | Y    | N   | 0.0670    | 0.1481 | 0.2481 | 0.3481 | 0.2012 | 2.27E-04 |
| 4  | Y    | N   | 0.1112    | 0.2015 | 0.3015 | 0.4015 | 0.2531 | 5.01E-04 |

表 5-22 环境风险条件概率表

| 序号 | 节点事件 |     | 专家评估聚类模糊数 |        |        |        | FPS    | 先验概率     |
|----|------|-----|-----------|--------|--------|--------|--------|----------|
|    | C11  | C12 |           |        |        |        |        |          |
| 1  | Y    | Y   | 0.0251    | 0.0625 | 0.1625 | 0.2625 | 0.1230 | 3.72E-05 |
| 2  | Y    | Y   | 0.0301    | 0.0581 | 0.1581 | 0.2581 | 0.1201 | 3.40E-05 |
| 3  | Y    | N   | 0.1260    | 0.2171 | 0.3171 | 0.4171 | 0.2686 | 6.12E-04 |
| 4  | Y    | N   | 0.1333    | 0.2265 | 0.3265 | 0.4265 | 0.2777 | 6.85E-04 |

表 5-23 一级指标风险因素条件概率表

| 序号 | 节点事件 |    |    |    |    | 专家评估聚类模糊数 |        |        |        | FPS    | 先验概率     |
|----|------|----|----|----|----|-----------|--------|--------|--------|--------|----------|
|    | A1   | A2 | A3 | A4 | A5 |           |        |        |        |        |          |
| 1  | Y    | Y  | Y  | Y  | Y  | 0.0307    | 0.0746 | 0.1746 | 0.2746 | 0.1340 | 5.17E-05 |
| 2  | Y    | Y  | Y  | Y  | N  | 0.0310    | 0.0705 | 0.1705 | 0.2705 | 0.1306 | 4.69E-05 |
| 3  | Y    | Y  | Y  | N  | Y  | 0.0242    | 0.0617 | 0.1617 | 0.2617 | 0.1221 | 3.62E-05 |
| 4  | Y    | Y  | N  | Y  | Y  | 0.0593    | 0.1375 | 0.2375 | 0.3375 | 0.1911 | 1.90E-04 |



续表 5-23 一级指标风险因素条件概率表

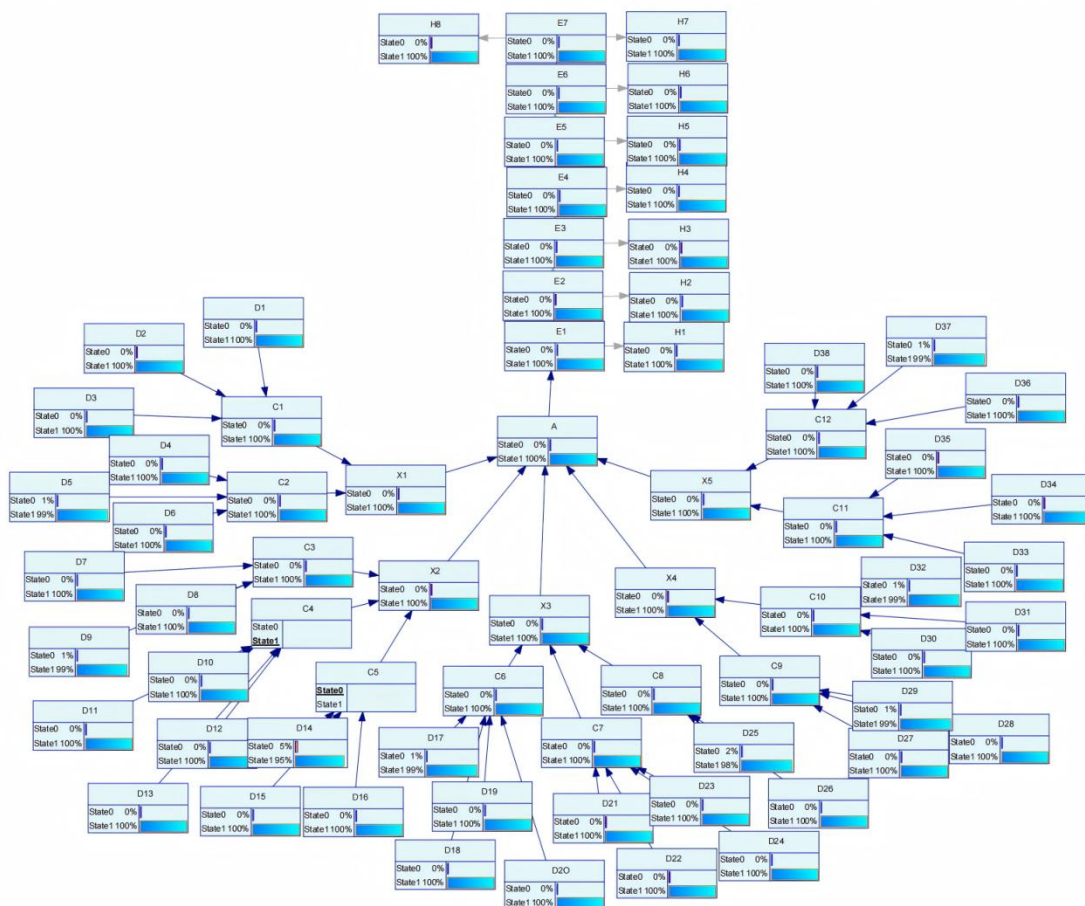
| 序号 | 节点事件 |    |    |    |    | 专家评估聚类模糊数 |        |        |        | FPS    | 先验概率     |
|----|------|----|----|----|----|-----------|--------|--------|--------|--------|----------|
|    | A1   | A2 | A3 | A4 | A5 |           |        |        |        |        |          |
| 5  | Y    | N  | Y  | Y  | Y  | 0.0537    | 0.1230 | 0.2230 | 0.3230 | 0.1781 | 1.48E-04 |
| 6  | N    | Y  | Y  | Y  | Y  | 0.0437    | 0.0988 | 0.1988 | 0.2988 | 0.1563 | 9.19E-05 |
| 7  | Y    | Y  | Y  | N  | N  | 0.0460    | 0.1209 | 0.2209 | 0.3209 | 0.1751 | 1.39E-04 |
| 8  | Y    | Y  | N  | Y  | N  | 0.0876    | 0.1796 | 0.2796 | 0.3796 | 0.2310 | 3.67E-04 |
| 9  | Y    | N  | Y  | Y  | N  | 0.0100    | 0.0292 | 0.1292 | 0.2292 | 0.0927 | 1.20E-05 |
| 10 | N    | Y  | Y  | Y  | N  | 0.0395    | 0.1083 | 0.2083 | 0.3083 | 0.1635 | 1.08E-04 |
| 11 | Y    | Y  | N  | N  | Y  | 0.0236    | 0.0605 | 0.1605 | 0.2605 | 0.1210 | 3.50E-05 |
| 12 | Y    | N  | Y  | N  | Y  | 0.0345    | 0.1006 | 0.2006 | 0.3006 | 0.1562 | 9.18E-05 |
| 13 | N    | Y  | Y  | N  | Y  | 0.0740    | 0.1528 | 0.2528 | 0.3528 | 0.2063 | 2.48E-04 |
| 14 | Y    | N  | N  | Y  | Y  | 0.0130    | 0.0555 | 0.1555 | 0.2555 | 0.1150 | 2.87E-05 |
| 15 | N    | Y  | N  | Y  | Y  | 0.0587    | 0.1357 | 0.2357 | 0.3357 | 0.1895 | 1.84E-04 |
| 16 | N    | N  | Y  | Y  | Y  | 0.0501    | 0.1106 | 0.2106 | 0.3106 | 0.1672 | 1.18E-04 |
| 17 | Y    | Y  | N  | N  | N  | 0.0398    | 0.1139 | 0.2139 | 0.3139 | 0.1682 | 1.20E-04 |
| 18 | Y    | N  | Y  | N  | N  | 0.0419    | 0.1133 | 0.2133 | 0.3133 | 0.1680 | 1.20E-04 |
| 19 | N    | Y  | Y  | N  | N  | 0.0416    | 0.1133 | 0.2133 | 0.3133 | 0.1680 | 1.20E-04 |
| 20 | Y    | N  | N  | Y  | N  | 0.0265    | 0.0805 | 0.1805 | 0.2805 | 0.1382 | 5.82E-05 |
| 21 | N    | Y  | N  | Y  | N  | 0.0496    | 0.1156 | 0.2156 | 0.3156 | 0.1713 | 1.28E-04 |
| 22 | N    | N  | Y  | Y  | N  | 0.0469    | 0.1242 | 0.2242 | 0.3242 | 0.1780 | 1.47E-04 |
| 23 | Y    | N  | N  | N  | Y  | 0.0448    | 0.1177 | 0.2177 | 0.3177 | 0.1722 | 1.31E-04 |
| 24 | N    | Y  | N  | N  | Y  | 0.0442    | 0.0994 | 0.1994 | 0.2994 | 0.1569 | 9.32E-05 |
| 25 | N    | N  | Y  | N  | Y  | 0.0239    | 0.0525 | 0.1525 | 0.2525 | 0.1144 | 2.81E-05 |
| 26 | N    | N  | N  | Y  | Y  | 0.0413    | 0.0897 | 0.1897 | 0.2897 | 0.1483 | 7.57E-05 |
| 27 | N    | N  | N  | N  | Y  | 0.0652    | 0.1319 | 0.2319 | 0.3319 | 0.1874 | 1.77E-04 |
| 28 | N    | N  | N  | Y  | N  | 0.0705    | 0.1472 | 0.2472 | 0.3472 | 0.2011 | 2.27E-04 |
| 29 | N    | N  | Y  | N  | N  | 0.0265    | 0.0720 | 0.1720 | 0.2720 | 0.1311 | 4.76E-05 |
| 30 | N    | Y  | N  | N  | N  | 0.0681    | 0.1360 | 0.2360 | 0.3360 | 0.1913 | 1.90E-04 |
| 31 | Y    | N  | N  | N  | N  | 0.1342    | 0.2304 | 0.3304 | 0.4304 | 0.2810 | 7.13E-04 |
| 32 | N    | N  | N  | N  | N  | 0.1534    | 0.2510 | 0.3510 | 0.4510 | 0.3014 | 9.01E-04 |

## 5.3 贝叶斯网络结构结果分析

### 5.3.1 因果推理分析

贝叶斯网络的正向因果推理旨在通过已知风险因素的概率分布，定量刻画系统整体安全状态的演化结果。在已明确各前置影响因素触发系统失效概率的基础上，可利用贝叶斯推理机制，自底向上逐层传播概率信息，进而计算目标节点的状态概率。通过这种方式，能够获得各节点“不失效”状态的后验概率，从而实现对系统安全韧性水平的量化评估，为风险防控与决策优化提供数据支撑。

在模型实现过程中，将前文计算得到的各根节点先验概率以及非根节点的条件概率表（CPT）输入 GeNIe 软件平台，依托其概率推理引擎开展正向因果推理计算。通过对网络结构与参数的联合求解，最终构建形成 Lilium 电池热失控安全风险的概率评估模型（见图 5-3）。该模型实现了从底层致因事件到顶层风险状态的概率传递与聚合分析，能够动态反映不同情景参数变化下系统整体风险水平的变化趋势，为后续安全控制策略优化与韧性提升路径设计提供定量依据。



如图 5-3 Lilium 电池热失控安全风险因果推理结果

表 5-24 非根节点风险概率

| 风险概率        | A          | X1         | X2         | X3         | X4         | X5         |
|-------------|------------|------------|------------|------------|------------|------------|
| State0=100% | 5.1760e-05 | 1.9064e-05 | 5.6600e-04 | 1.0881e-05 | 5.2443e-05 | 3.7225e-05 |
| State1=100% | 0.9999482  | 0.9999809  | 0.999434   | 0.9999891  | 0.9999476  | 0.99996728 |

结合各级指标权重及排序分析可知，该 eVTOL 电池整体风险发生概率结合一级指标权重综合判定为  $5.1760e-05$ 。从图中可以看出，五个部分的失效概率分布情况。总体上来说  $X2$  滥用诱发风险  $> X4$  人因风险  $> X5$  环境风险  $> X1$  电池本身固有风险  $> X3$  系统失效风险。系统失效风险  $X3$  的发生概率最小，是因为其发生通常需要热管理系统、电池管理系统和供电系统等多个子系统同时或连续失效，而在工程设计中各子系统均具备独立防护与冗余机制，使系统级同时失效的可能性被显著降低。

由于完善的应急处置与安全控制机制的存在，即便发生异常工况，最终演化为严重事故的概率仍然维持在较低水平。系统静态部件失效率相对较高的阶段，各类事故后果的发生概率依然较小：根据专家评分过程可分析，H1 的事故发生率为  $0.000145$ ，H2 的事故发生率为  $4.6903e-05$ ，H3 的事故发生率为  $3.0518e-05$ ，

H4 的事故发生率为  $7.5241\text{e-}05$ ，H5 的事故发生率为  $0.000353$ ，H6 的事故发生率为  $9.1101\text{e-}05$ ，H7 的事故发生率为  $9.1101\text{e-}05$ ，H8 的事故发生率为  $1.6000\text{e-}05$ 。

这表明，在 eVTOL 电池系统出现热失控诱发因素时，通过及时启动 E1 类干预措施，如快速切断充放电回路、降低电池负载功率、启动主动冷却系统以及实施电池模组隔离等操作，可以有效抑制温度持续升高，阻断热失控链式传播路径。即使在局部电芯已发生剧烈放热、单一控制措施难以完全消除风险的情况下，后续的分级应急响应流程仍能够进一步削弱事故后果的严重程度，从而显著降低 eVTOL 电池热失控对整机运行安全带来的整体风险。

### 5.3.2 正向推理分析

在得到各个节点的风险概率之后，本文使用 GeNie 软件对假设场景进行具体的 eVTOL 电池热失控风险事件分析。

Lilium 的电池系统在提升安全冗余能力的同时，也引入了较高的系统复杂性。电池包之间的电气连接与能量调度增加了潜在故障路径，而高能量密度电池在高功率运行条件下易产生显著热积累，一旦局部电芯发生异常，可能触发热失控并向电池包级别演化。

事故场景发生在对 eVTOL 的维修过程中，具体事故场景如下：Lilium 在 Oberpfaffenhofen Airport 开展地面维护作业期间，其首架全尺寸 Lilium Jet 验证机在例行电池系统检测过程中发生起火事故。事故发生时飞行器处于非飞行状态，但电池系统仍处于通电运行工况，可能伴随较高荷电状态（SOC）及外接地面电源支持。在持续运行条件下，电池包内部某一电芯因潜在制造缺陷或早期损伤产生微观短路，导致局部电流密度异常升高并形成初始热点。由于该异常具有较强隐蔽性，BMS 未能在早期阶段及时识别，叠加高 SOC 工况对副反应速率的放大作用，局部温升逐渐失控，并最终突破热稳定阈值，触发单体电芯热失控。

随着热失控发展，电芯内部剧烈放热反应引发热量向相邻电芯扩散，形成典型的热蔓延过程；与此同时，在维护模式下热管理系统可能处于非完全工作状态或散热效率受限，进一步加剧了系统内热量积聚。多个电芯相继失控后，大量高温气体及可燃电解液蒸气被释放至相对封闭的电池舱空间，在通风受限条件下迅速积聚并形成可燃混合气体环境。当其接触到高温表面或电气火花等点火源时即被引燃，最终导致电池舱起火并蔓延至机体结构，造成飞行器严重损伤。该事故情景体现出“电芯缺陷—高 SOC 工况—热管理受限—空间约束”多因素耦合作用下的链式演化特征，其中电池内在缺陷为初始诱因，运行工况与系统控制失效为关键放大机制，而封闭环境则促成了事故由热失控向明火燃烧的跃迁。

在上述各种因素的共同作用下，使得 eVTOL 飞行的安全系数大幅降低，由

电池局部的热量积累发展为单体热失控，并通过蔓延效应扩展到相邻电芯，最终造成电池热失控事故，其 GeNie 风险演化如图 5-4 所示。

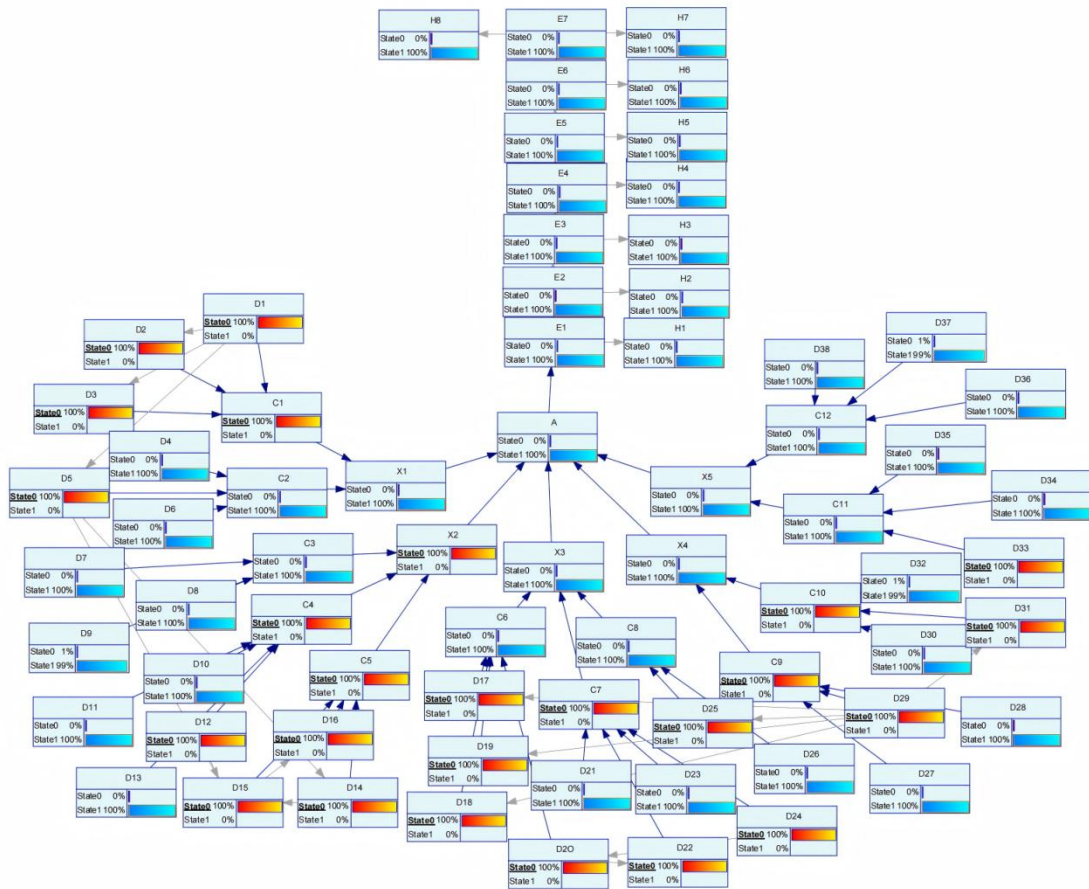


图 5-4 eVTOL 飞行场景电池热失控风险因素演化

根据上述的推理过程，eVTOL 电池热失控的风险概率上升到  $1.2013\text{e-}04$ ，与原来的  $5.1760\text{e-}05$  相比，eVTOL 电池热失控的  $SAI=1.3009$ ，这表明 eVTOL 电池热失控的发生概率大大增加。但是从图中可以看出基础因素对最终事故后果的影响较小，也容易更正，应加强前期的监管与管控。而一旦事故后果发生，就会产生碰撞、坠机、着火和爆炸等一系列事故，使事态进一步恶化，这对未来事故后果恶劣程度的确定非常关键。

### 5.3.3 敏感性分析

敏感性分析可以帮助验证贝叶斯网络的概率参数，通过先验概率和条件概率的微小变化后验概率的影响来实现这一目的。高度敏感的节点会更显著地影响目标节点的风险值，识别这些参数可以有针对性地分配检修任务，或加强对人为环境等动态因素的监管，从而最快地提升系统的安全性<sup>[74]</sup>。

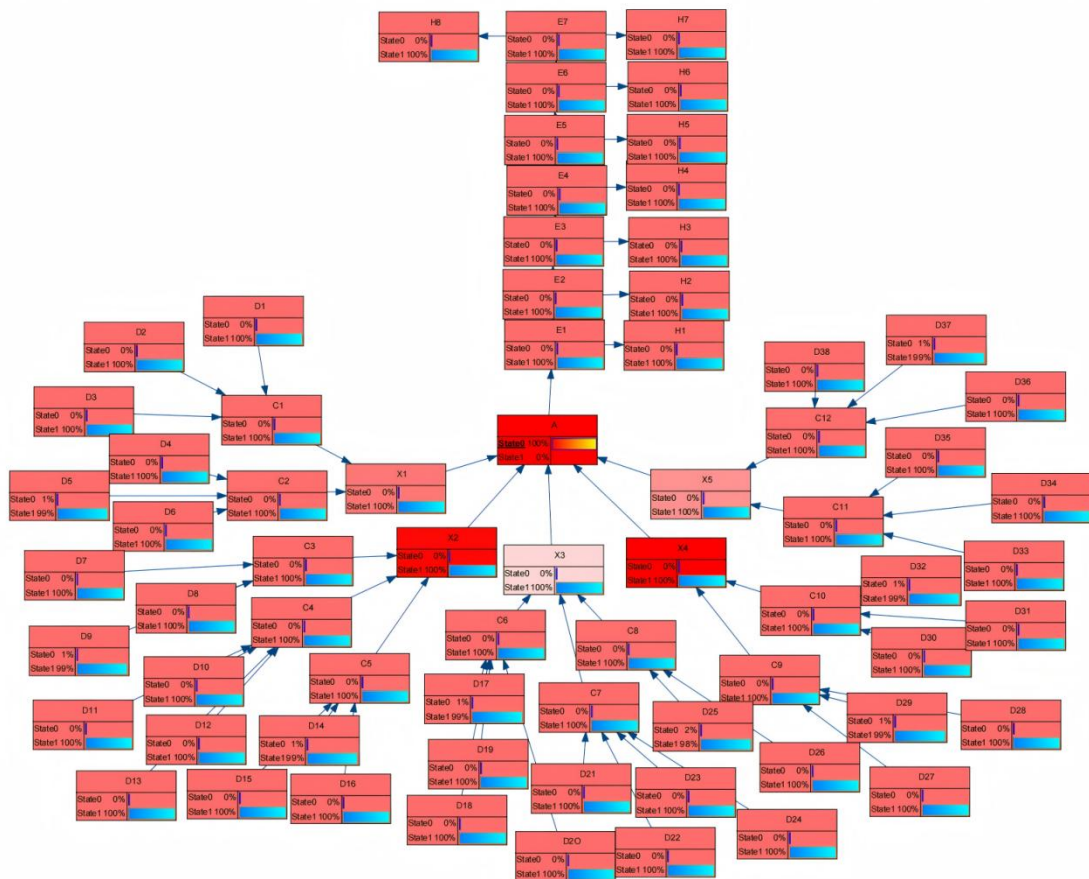


图 5-5 Lilium 电池热失控风险因素敏感性分析

在图 5-5 中，不同颜色深浅对应各影响因素的敏感程度，颜色越深表示该因素对目标结果的影响越显著。通过对各节点开展敏感性分析，可以直观识别系统中潜在的薄弱环节。这些环节在日常运行与管理过程中可能不易被察觉，但却对系统韧性水平具有关键影响。

敏感性分析是确定系统韧性失效关键节点的有效工具。常用方法之一为变异率法，通过比较节点先验概率与后验概率的变化情况，计算根节点风险的波动程度，即风险变异值  $SA_i$ ，其计算形式如式（4-10）所示。

假设 eVTOL 电池热失控安全系统韧性失效的概率为 100%，按上述计算方法计算得到前十根节点的  $SA_i$  值见表 5-25。



表 5-25 关键根节点排序

| 根节点             | $SA_i$   | 排序 |
|-----------------|----------|----|
| 液体冷却系统故障 D18    | 0.054044 | 1  |
| 老化导致热失控敏感性增加 D6 | 0.005098 | 2  |
| 相邻电芯热失控传导 D16   | 0.004261 | 3  |
| 过充 D10          | 0.003767 | 4  |
| 热失控期间操作错误 D31   | 0.001763 | 5  |
| 违规充电 D27        | 0.001441 | 6  |
| 复杂地形起降 D36      | 0.000984 | 7  |
| PCM 冷却系统失效 D19  | 0.000570 | 8  |
| 电池模组局部过热 D15    | 0.000438 | 9  |
| 雷电天气 D34        | 0.000152 | 10 |

## 5.4 关键因素风险管控措施

基于贝叶斯网络后验概率计算结果可以看出，在热失控事故已发生的条件下，液体冷却系统故障（D18）的解释贡献度最高，其次为电池老化导致热失控敏感性增加（D6）、相邻电芯热失控传导（D16）以及过充（D10）等因素。该排序反映出电池系统在主动热管理、寿命退化控制与热传播阻断方面存在明显薄弱环节。韧性优化应围绕高概率关键节点展开，通过结构强化、功能优化与运行管控提升系统整体抗扰动能力与恢复能力。

液体冷却系统作为主动热管理核心单元，一旦发生故障，热量无法及时排散，局部温升迅速累积并可能触发连锁失效。优化重点在于提升系统冗余度与可诊断性。采用双泵或双回路设计，构建分区独立冷却结构，可降低单点失效风险。结合流量、压差与进出口温差数据建立冷却效率评价模型，实现异常状态的实时识别。检测到效率下降时，系统自动进入降功率或分区隔离模式，限制热量继续积聚。模块化接口与快速维护结构能够缩短检修时间，提高系统恢复效率。

电池老化会引起内阻升高与极化加剧，单位功率下的热生成速率上升，系统对抗扰动的容忍度随之下降。运行策略应与健康状态联动，根据 SOH 分级设定功率上限与温度阈值，对高老化模组实施限载控制或提前更换。建立包含内阻变化率与温升速率的综合评估指标，将退化程度纳入飞行决策过程，可在早期阶段抑制风险扩展，减缓系统性能衰退带来的安全影响。

热失控传播具有显著的链式扩散特征，单体失效容易演化为模组级故障。结构优化应着重于物理隔离与延迟机制设计。在电芯之间布置高效隔热材料或气凝胶层，优化排气方向与通道布局，使高温气体定向释放，避免横向冲击相邻单体。相变材料可吸收瞬时热冲击，延长传播时间，为飞行控制系统提供处置窗口。这项措施提高了系统在极端工况下的缓冲能力。

过充风险主要来源于控制失效或传感误差。双重 BMS 架构与独立硬件熔断装置能够形成多层防护屏障。SOC 与电压数据交叉校验机制可降低误判概率，提高控制可靠性。通过软硬件协同设计，减少单一算法或传感器失效对系统安全的影响。

热失控处置阶段的人为操作偏差会放大事故后果。应急流程需要高度标准化，关键决策优先由自动控制系统执行，人工干预以确认和监督为主。通过极端场景模拟训练，提高操作人员对异常信号的识别能力。充电环节建立设备认证与通信加密机制，限制违规充电行为，从管理层面降低外部干扰因素。

复杂地形起降与雷电天气属于外部环境扰动因素。飞行前风险评估应纳入地形数据与气象信息，设定动态禁飞阈值。机体结构设计考虑防雷导流路径，减少极端气象条件下的附加风险。

后验概率排序结果揭示了电池系统热管理与退化控制环节的关键脆弱区域。围绕高风险节点实施结构冗余、健康感知与动态控制措施，可增强系统在扰动条件下的稳定性与恢复能力。通过多层防护与功能重构机制的协同作用，电动垂直起降飞行器动力电池系统的整体韧性水平能够得到显著提升。

## 5.5 本章小结

本章首先采用 GeNIe 软件构建 eVTOL 电池热失控风险分析模型，通过对试验数据与仿真结果的解模糊处理，分别获取证据节点与非根节点的先验概率及条件概率。随后，将所有量化结果导入 GeNIe 软件开展因果链推理，测算得出该类 eVTOL 电池发生热失控风险的概率为  $5.1760e-05$ 。与此同时，依托贝叶斯网络完成逆向诊断推理、概率推理验证及敏感性分析等辅助分析工作。根据贝叶斯的推理过程和前文梳理的五大类一级风险、12 项二级风险及 38 项三级风险，构建了对前十关键风险因素风险管控措施建议。

## 6 总结与展望

### 6.1 研究总结

本文通过对 eVTOL 电池热失控这一项目的风险管理进行研究，识别出 eVTOL 电池热失控分析概念所存在的安全问题，进行归纳整理，运用风险管理理论和手段，进行综合评价分析。对 eVTOL 电池热失控关键因素进行深入剖析，根据 eVTOL 的发展情况和生产标准，给出相应的改进措施，以提高 eVTOL 电池本身的安全性、可靠性和安全管理水平。通过对 Lilium 机型的安全风险因素分析，具体得出了以下主要结论：

本文基于 STPA 方法和文献调查对 eVTOL 电池热失控风险因素进行系统识别，并分析出因热失控产生的后果。通过分析不安全的控制行为识别出相应事故级风险等关键信息，构建 eVTOL 电池热失控的安全风险管理评价指标体系，该体系包含 5 个一级指标、12 个二级指标和 38 个三级指标。

采用 Bow-tie 方法将系统分析出的事故致因和事故后果构建出可视化的事故因果树，运用模糊综合评价方法，获得模糊综合评价结果。总体来说，eVTOL 电池热失控的安全风险管理整体属于事故率极低的水平，但并不能忽视其所隐藏的风险和严重的事故后果。将模糊评价结果和因素之间的条件概率关系结合起来，引入贝叶斯网络，并据此绘制出贝叶斯风险网络图，根据贝叶斯网络图中的各节点关系，可以清晰地看出节点之间的影响关系。通过后验概率的推理，可以得到影响因素较大的前十个风险因素，并据此进行系统的分析和改进，保持其有效的管理水平。

基于上述评价结果，eVTOL 电池热失控安全管理水平应在提升整体的基础上，对目前的 eVTOL 电池安全风险管理所存在的不足之处进行重点关注并提出相应的应对和改进措施。eVTOL 电池热失控风险主要集中于液冷系统失效、电池老化、热传播及过充等关键薄弱环节，表明系统在主动热管理、寿命退化控制与多层防护方面仍存在不足；因此，应以高风险节点为核心，通过构建冗余冷却结构、强化健康状态感知与分级控制、优化热隔离与传播阻断设计，并结合 BMS 多重防护与标准化应急机制，实现结构、功能与运行管控的协同优化，从而显著提升电池系统在复杂扰动条件下的安全韧性与恢复能力。

### 6.2 研究展望

通过对 Lilium 电池热失控风险因素的深入研究已经初步探讨了如何利用基础的原理和方法来分析 eVTOL 装载新能源电池的安全风险管理。然而，受当前



知识水平、实践能力以及数据稀缺等因素的局限，本文在研究过程中、选用方法 and 研究视角等方面仍存在一定的缺陷。为了进一步完善这一研究领域，本文将提出一些更为深入、具体、真切、具有针对性和可操作性的未来展望。

(1) 由于 eVTOL 仍处于发展初期，实际运行与事故数据较为匮乏，本文在贝叶斯网络参数确定过程中主要依赖专家打分与模糊评价方法，虽然在一定程度上弥补了数据不足问题，但仍不可避免地引入主观性偏差，可能对风险概率计算结果的准确性与稳定性产生影响。因此，未来可以通过引入实测运行数据与多源数据融合，以降低主观性偏差并提升模型精度。

(2) 本文在构建 STPA-Bow-tie-FBN 融合模型过程中，对部分影响因素及其相互关系进行了合理简化，尤其在电池热失控多物理场耦合（热—电—力）及飞行环境动态变化方面未进行深入刻画，导致模型对复杂非线性演化过程的表达能力仍存在一定局限。通过进一步引入多耦合建模结合动态贝叶斯模型，增强模型对电池热失控复杂非线性及动态演化过程的刻画能力。

(3) 本文虽以动态贝叶斯网络为研究目标，但当前模型仍停留在静态因果推理阶段，其动态性主要体现在运行情景划分层面。未来需通过引入时间片结构、状态转移概率及在线数据更新机制，实现对 eVTOL 电池热失控风险演化过程的动态刻画。

## 参考文献

- [1] Viswanathan V, Epstein A H, Chiang Y M, et al. The challenges and opportunities of battery-powered flight[J]. Nature, 2022, 601(7894): 519-525.
- [2] Jaguemont, J. & F. Bardé. A critical review of lithium-ion battery safety testing and standards[J]. Applied Thermal Engineering, 2023, 231: 121014.
- [3] Wang, Q.S., Ping, P., Zhao, X.J. et al. A review of lithium ion battery failure mechanisms and fire prevention strategies[J]. Progress in Energy and Combustion Science, 2019, 73: 95-131.
- [4] Xu, C.S., Zhang, Y., Liu, Z.Y. et al. Internal temperature detection of thermal runaway in lithium-ion cells tested by extended-volume accelerating rate calorimetry[J]. Journal of Energy Storage, 2020, 31: 101670.
- [5] 朱晓庆,王震坡等.锂离子动力电池热失控与安全管理研究综述[J].机械工程学报,2020,56(14):91-118.
- [6] Ren, D.S., Feng, X.N., Liu, X. et al. Investigating the relationship between internal short circuit and thermal runaway of lithium-ion batteries under thermal abuse condition[J]. Energy Storage Materials, 2021, 34: 563-573.
- [7] Feng, X.N., Ouyang, M.G., Liu, X. et al. Mitigating thermal runaway of lithium-ion batteries[J]. Joule, 2020, 4(4): 743-770.
- [8] Larsson, F., Andersson, P. & B. Mellander. Characteristics of lithium-ion batteries during fire tests[J]. Journal of Power Sources, 2014, 271: 414-420.
- [9] Li, W., Zhang, H., Wang, Y. et al. Energy consumption modeling and optimization of an eVTOL aircraft: Integrating weight, motor, and battery dynamics[J]. Energy, 2025, 325: 136229.
- [10] 杨驹丰,黄文新,孙久康,等.电动起降飞机用电池多维健康指标联合估算[J].航空学报,2025,46(14):321-333.
- [11] Sagirli, F.Y., Zhao, X.P. & Z. Wang. Human-computer interaction and human-AI collaboration in advanced air mobility: A comprehensive review[EB/OL]. arXiv, 2024.
- [12] 丁水汀,丁硕,孙爽,等.复合翼eVTOL电池需求及对动力总成安全性的影响[J].推进技术,2024,45(03):212-226.
- [13] Kuijpers T, Van Kampen J, Hofman T. System-level thermal and electrical modeling of battery systems for electric aircraft design[C]//2024 IEEE Vehicle Power and Propulsion Conference (VPPC). IEEE, 2024: 1-6.
- [14] 杨娟,胡佳宁,佟佳成,等.航空锂电池热失控高温喷射冲击实验研究[J].航空学报.
- [15] 邓景辉.电动垂直起降飞行器的技术现状与发展[J].航空学报,2024,45(05):55-77.
- [16] 王鹏,王晓聪,肖女娥,等.基于证据理论和区间分析的eVTOL热失控安全性分析[J].西北工业大学学报,2024,42(03):558-566.
- [17] 乔亚军,任怡茂,谭子健,等.锂离子电池单层电芯内短路建模与热失控触发特性[J].储能科学与技术,2024,13(10):3491-3503.
- [18] Guang X Y ,Teng L ,Shanhai G , et al.Challenges and key requirements of

- batteries for electric vertical takeoff and landing aircraft[J].Joule,2021,5(7):
- [19] Marm D .Balancing battery safety and performance for electric vertical takeoff and landing aircrafts[J].Device,2023,1(6):
- [20] Chen S Q , Wei X Z , Wu H , et al.Multi-functional thermal barrier suppresses battery thermal runaway propagation and degradation[J]. Renewable and Sustainable Energy Reviews,2025, 223: 116056..
- [21] Wang, Y. "Navigating Risks: A Comprehensive Functional Hazard Assessment of eVTOL Power Battery Systems." London Journal of Engineering Research 24.1 (2024): 1-22.
- [22] Ma X, Ding S T. Overview and Research on Airworthiness and Safety of Electrical Propulsion and Battery Technologies in eVTOL. No. 2023-01-7116. SAE Technical Paper, 2023.
- [23] 陈博宇,吴志威,郑晨明.eVTOL 电池热管理与热失控蔓延抑制研究及优化[J]. 电源技术,2025,49(06):20201-20209.
- [24] Feng, X.N., Ouyang, M.G. & X. Liu. Thermal runaway mechanism of lithium ion battery for electric vehicles: A review[J]. Energy Storage Materials, 2018, 10: 246-267.
- [25] 殷朕,朱建功,吕龙臣,等.面向 eVTOL 的固态电池技术路径与管理系统[J].汽车工程,2025,47(12):2289-2302+2365.
- [26] Shashank, S., Alexa, B. & V. Venkatasubramanian. A review of safety considerations for batteries in aircraft with electric propulsion[J]. MRS Bulletin, 2021, 46: 435-442..
- [27] 徐成善,孙烨,杨智凯,等.储能锂离子电池系统热失控诱发电弧研究进展[J].储能科学与技术,2025,14(08):3037-3050.
- [28] Jones, F.V. & Israni, K.C.Environmental risk assessment utilizing bow-tie methodology[C]//SPE international conference and exhibition on health, safety, environment, and sustainability?. SPE, 2012: SPE-156833-MS.
- [29] 杨海云,李宜恒,林波,等.功能危害性评估方法在电动垂直起降飞行器安全性分析中的应用[J].民用飞机设计与研究, 2023(4):158-166.
- [30] 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.
- [31] 杨晓军,赵飞扬.基于故障树-蒙特卡罗模拟的电动飞机推进系统可靠性分析[J].航空科学技术,2024,35(10):76-85.
- [32] 王红勇, 温瑞英 . 基于复杂网络的空中交通态势风险评估方法 [J] . 中国安全科学学报, 2018, 28 ( 5 ) : 172-178.
- [33] Weibel, R. & R.J. Hansman. An integrated approach to evaluating risk mitigation measures for UAV operational concepts in the NAS[C]// IEEE Infotech and Aerospace Conference. AIAA, 2005: 6957.
- [34] Wackwitz, K. & H. Boedecker. Safety risk assessment for UAV operation[J]. Drone Industry Insights, 2015, 1: 31-53.
- [35] 钱宇, 龙涛.基于云贝叶斯网络的运输飞机超轮速风险评估 [J] . 航空工程进展, 2022, 13 ( 3 ) : 171-178.
- [36] 李新飞.物流无人机配送网络布局规划与安全性分析研究 [D] .南京:南京航空航天大学, 2020.

- [37] Jeong, S., K. You & D. Seok. Hazardous flight region prediction for a small UAV operated in an urban area using a deep neural network[J]. *Aerospace Science and Technology*, 2021, 118: 107060.
- [38] Utne, I.B., Rokseth, B. & A.J. Sørensen. Towards supervisory risk control of autonomous ships[J]. *Reliability Engineering & System Safety*, 2020, 196: 106757.
- [39] 张建科,葛红娟,罗宇洲,等.基于 STPA 的多电飞机大功率机电驱动控制系统安全性分析[J].*测控技术*,2025,44(10):29-36.
- [40] Book, G. Lessons learned from real world application of the Bow-Tie method[C]// *SPE Middle East Health Safety Security and Environment Conference*. SPE, 2012.
- [41] Kim, D.Y., Sim, M.S. & J.M. Lee. A study on the improvement of safety management by port logistics industry using Bow-Tie analysis[J]. *Journal of Navigation and Port Research*, 2022, 46: 57-72.
- [42] 张子昂,张晓全.基于 STPA 和模糊贝叶斯网络的大型无人驾驶航空器运行风险分析[J/OL].*航空工程进展*,1-10[2025-06-03].
- [43] 李佳音,谭德强,钱祎祎.面向山岳风景区旅游用大型载人 eVTOL 的运行风险研究[J].*中国安全科学学报*,2025,35(S1):210-216.
- [44] Thomas, J.P. & J.G. Van Houdt. Evaluation of System-Theoretic Process Analysis (STPA) for improving aviation safety[R]. *Federal Aviation Administration*, 2024.
- [45] Pilko, A. Uncrewed aerial systems operational risk analysis[D]. *Southampton: University of Southampton*, 2024.
- [46] 肖扬,苏波,纪超,等.基于 STPA 和 Bow-Tie 模型的地面无人平台系统安全分析方法[J].*兵工学报*,2024,45(S2):153-161.
- [47] 耿增显,陈俊宇.基于模糊贝叶斯网络的低空无人机运行风险评估[J].*中国安全科学学报*,2024,34(08):53-60.
- [48] Leveson, N. A new accident model for engineering safer systems[J]. *Safety Science*, 2004, 42(4): 237-270.
- [49] 李耀华,魏金淇.改进 STPA 的电传飞控系统安全性分析[J/OL].*机械设计与制造*,1-7[2026-03-04].
- [50] 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.
- [51] Cockshott, J.E. Probability bow-ties: A transparent risk management tool[J]. *Process Safety and Environmental Protection*, 2005, 83(4): 307-316.
- [52] Nielsen, D.S. The cause/consequence diagram method as a basis for quantitative accident analysis[R]. *Risø National Laboratory*, 1971.
- [53] Animah, I. Application of Bayesian network in the maritime industry: Comprehensive literature review[J]. *Ocean Engineering*, 2024, 302: 117610.
- [54] 李兵,周蕾,黄永婷,等.基于贝叶斯网络的高等级公路施工风险评价[J].*四川建材*,2025,51(07):175-180.
- [55] Ye, J.N., Chen, H. & Wang, Q.S. Thermal behavior and failure mechanism of lithium ion cells during overcharge under adiabatic conditions[J]. *Applied Energy*, 2016, 182: 464-474.

- [56] Ohsaki, T., Kishi, T., Kuboki, T. et al. Overcharge reaction of lithium-ion batteries[J]. Journal of Power Sources, 2005, 146(1-2): 97-100.
- [57] Feng, X.N., Fang, M., He, X.M. et al. Thermal runaway features of large format prismatic lithium ion battery using extended volume accelerating rate calorimetry[J]. Journal of Power Sources, 2014, 255: 294-301.
- [58] Zhao, C.C., Sun, J.H. & Wang, Q.S. Thermal runaway hazards investigation on 18650 lithium-ion battery using extended volume accelerating rate calorimeter[J]. Journal of Energy Storage, 2020, 28: 101232.
- [59] Vendra, C.M.R., Shelke, A.V., Buston, J.E.H. et al. Numerical and experimental characterisation of high energy density 21700 lithium-ion battery fires[J]. Process Safety and Environmental Protection, 2022, 160: 153-165.
- [60] Beauregard, G.P. Report of investigation: Hybrids plus plug in hybrid electric vehicle[R]. 2008.
- [61] Shahid, S. & M. Agelin-Chaab. A review of thermal runaway prevention and mitigation strategies for lithium-ion batteries[J]. Energy Conversion and Management: X, 2022, 16: 100310.
- [62] Ju, H.J. Analysis of discharge characteristics of new energy batteries based on dynamic characteristics[C]// International Conference on Control Science and Electric Power Systems. IEEE, 2021: 211-214.
- [63] 李奎杰, et al. 锂离子电池热失控多维信号演化及耦合机制研究综述. 储能科学与技术, 2023, 12.3: 899-912.
- [64] Ma, X. & S. Ding. Overview and research on airworthiness and safety of electrical propulsion and battery technologies in eVTOL[C]// SAE Intelligent Urban Air Mobility Symposium. SAE Technical Paper, 2023.
- [65] 彭傲, 孙小琴, 彭启, 等. 大容量电池组动态浸没式液冷系统冷却性能研究[J/OL]. 储能科学与技术, 1-14[2026-03-04].
- [66] 席尚军. 新能源汽车电池包模组布局结构优化[J]. 汽车与新动力, 2026, 9(01): 1-4.
- [67] Zhang, J.C., Liu, Y.L. & Y. Zheng. Overall eVTOL aircraft design for urban air mobility[J]. Green Energy and Intelligent Transportation, 2024, 3(2): 100150.
- [68] 柴新波, 胡泊. 基于热滥用条件下的锂电池热失控分析[J]. 科技与创新, 2025, (20): 154-156+160.
- [69] 朱伟杰, 史尤杰, 雷博. 锂离子电池储能系统 BMS 的功能安全分析与设计[J]. 储能科学与技术, 2020, 9(01): 271-278.
- [70] Yamauchi, T., Mizushima, K., Satoh, Y. et al. Development of a simulator for both property and safety of a lithium secondary battery[J]. Journal of Power Sources, 2004, 136: 99-107.
- [71] Zeng, Y.Q., Zhang, Y., Zhang, M. et al. Overcharge investigation of lithium-ion polymer batteries[J]. Journal of Power Sources, 2006, 160(2): 1302-1307.
- [72] 何永勃, 霍志轩. 多旋翼电动垂直起降航空器推进系统可靠性分析与分配[J]. 科学技术与工程, 2025, 25(17): 7390-7397.
- [73] Zhao, C.C., Sun, J.H. & Wang, Q.S. Use of fuzzy fault tree analysis and Bayesian network for occurrence likelihood estimation of navigational accidents in the Qinzhou Port[J]. Ocean Engineering, 2022, 263: 112381.

- [74] 王馨玉.基于 Bow-Tie-BN 的油库运行安全动态风险预警模型的研究[D].昆明理工大学,2024.

## 致 谢

时光如水，岁月如歌。回望二十余载求学之路，晨昏交替之间，书卷为伴，风雨兼程。行至硕士论文落笔之际，往昔的点滴宛若长河微澜，在心中层层荡开。那些不为人知的艰辛与坚持，早已化作沉静力量，镌刻于时光深处，唯有亲历，方知其重与其美。值此别离与启程交汇之时，谨以至诚之心，致谢所有温暖与指引。

首先，衷心感谢导师赵健老师与陈洪根老师。二位导师学识渊博、治学严谨，于迷茫处为我点灯，于困顿时为我指路。从选题构思到论证推演，从字句斟酌到体系建构，皆倾注心血、悉心指导。师恩如山，润物无声；教诲似水，泽被心田。其严谨求实之学风与谦和笃行之品格，将长久照亮我前行的道路。诚挚感谢校外导师郭俊鹏老师。在论文研究与实践探索过程中，郭老师以深厚的行业经验与开阔的学术视野，为本研究提供了宝贵的指导与支持。其严谨务实的工作态度与精益求精的专业精神，亦让我受益匪浅。

亦当感谢求学途中所有曾授我以知、启我以思的师长。讲台之上，言传身教；岁月之中，潜移默化。诸位老师以星火之光，汇聚成我心中的浩瀚星河，使得我在求知的长夜中不失方向。

尤须感念家人。灯火可亲，岁月漫长，是你们以无言的守望与不变的支持，托举我跨越重重山海。每一次踌躇与低谷，皆因你们而得以重整行装，再赴远方。家之所在，心之所安，亦是我不竭的力量源泉。

同时，感谢同行的同学与朋友。风雨同舟，笑语相伴，在彼此扶持与激励中，共同走过这段充满挑战与温度的岁月。那些并肩而行的日子，将成为记忆中最温润的篇章。

至此落笔，不仅为一段求学生涯作结，更为新的人生征程启幕。愿此去繁花似锦，归来仍怀初心。

谨以此文，铭记过往，致敬来路。

时年：二〇二六年二月二十六日。