文章编号:1674-8190(XXXX)XX-001-10

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

张子昂,张晓全
(中国民航大学 安全科学与工程学院,天津 300300)

摘　要: 仅采用系统理论过程分析(STPA)方法识别运行危险因素,处于定性分析阶段,无法准确分析各因素对系统安全的影响程度。为降低大型无人驾驶航空器运行事故风险,对其运行过程中主要角色职责和场景进行分析,采用STPA方法构建控制反馈结构识别危险因素;基于因素间的关联关系构建贝叶斯网络(BN),使用GeNIe软件对风险概率进行正向因果推理,并通过逆向推理、敏感性分析、影响强度分析确定关键因素等。结果表明:控制失效是导致事故发生的最关键因素,导航系统故障、恶劣天气、电池故障是高敏感性因素,本文分析结果能够为大型无人驾驶航空器运行风险防控提供依据。

关键词: 无人驾驶航空器;城市空中交通;风险分析;系统理论过程分析;贝叶斯网络
中图分类号: X949　　**文献标识码:** A
DOI: 10.16615/j.cnki.1674-8190.XXXX.XX.01

Operational risk analysis of large unmanned aerial vehicles based on STPA and fuzzy bayesian networks

ZHANG Ziang, ZHANG Xiaoquan
(College of Safety Science and Engineering, Civil Aviation of University, Tianjin 300300, China)

Abstract: The system theory process analysis (STPA) method used to identify the operational risk factors, which is in the qualitative analysis stage, can not accurately analyze the impact of each factor on system safety. In order to reduce the risk of accidents during the operation of large unmanned aerial vehicles, the main roles, responsibilities and scenarios in the operational process are analyzed. The system theory process analysis method is used to construct a control feedback structure to identify risk factors. Based on the correlation between factors, the Bayesian network (BN) is constructed, and the GeNIe software is used to carry out the forward causal inference on the risk probability, and the key factors are determined through reverse reasoning, sensitivity analysis and impact intensity analysis. The results show that control failure is the most critical factor leading to accidents. Navigation system failure, bad weather, and battery failure are highly sensitive factors, and the analysis results obtained in this paper can provide the basis for the prevention and control of large-scale unmanned aircraft operation risks.

Key words: unmanned aerial vehicle; urban air mobility; risk analysis; system theoretic process analysis; Bayesian network

收稿日期: 2024-05-11;　**修回日期:** 2024-08-10
通信作者: 张晓全(1971—),男,硕士,副教授。E-mail: xqzhang@cauc.edu.cn
引用格式: 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]. 航空工程进展, XXXX, XX(XX): 1-10.
ZHANG Ziang, ZHANG Xiaoquan. Operational risk analysis of large unmanned aerial vehicles based on STPA and fuzzy bayesian networks[J]. Advances in Aeronautical Science and Engineering, XXXX, XX(XX): 1-10. (in Chinese)

0 引 言

据摩根士丹利估算，2040年全球城市空中交通（Urban Air Mobility，简称UAM）的产业规模将高达1.5万亿美元。城市空中交通这一概念最早由美国国家航空航天局（National Aeronautics and Space Administration，简称NASA）[1]正式提出，而后空客（Airbus）[2]、优步（Uber）[3]等公司与机构都对这一新兴交通概念进行讨论并提出了未来运行幻想。即在城市内可利用载人和无人驾驶航空器实现乘客货物运输、医疗救护、消防灭火、应急救援等任务。该交通方式可大大提高城市居民交通出行的效率和城市交通运行效率，有望解决当前城市交通拥堵和环境污染的问题。

德勤公司（Deloitte）认为随着远程机长驾驶技术、集群管理技术的发展在2030年后大型无人驾驶航空器（large unmanned aerial vehicle，简称LUAV）将成为UAM的核心载具[4]。LUAV是指最大起飞重量超过150 kg的无人驾驶航空器。区别于传统航空器，它没有机载驾驶员主要由机载计算机和远程机组控制飞行，其运用分布式电力推进系统可实现垂直起降，具有低碳环保、噪声低、自动化程度高等优势。截止2023年11月美国垂直飞行协会（The Vertical Flight Society，简称VFS）宣布收录的LUAV设计概念已超过130个。中国亿航智能公司设计制造的大型无人驾驶航空器亿航216-S于2023年10月获得全球首个大型无人驾驶航空器系统型号合格证，预计在不远的未来可实现商业化运营。

资本市场和航空器设计制造商的持续火热，表明UAM有望实现运行，因此有必要对UAM场景下的大型无人驾驶航空器运行进行风险分析。进行风险分析并提出相应的风险防控建议，可降低事故发生概率、提升该航空器行业的安全水平，并可对未来国家相关部门制定对其进行安全监督管理的法规和行政规章提供理论和技术方面的帮助和支撑。

风险分析的关键步骤在于危险因素的识别和概率分析。在对无人驾驶航空器进行危险因素识别和风险概率分析，国内外研究者提出并应用了许多方法。危险因素识别方面，常用的方法包括复杂网络[5]、事件树[6]、危险和可操作分析[7]等。风险概率分析方面，常用的方法包括贝叶斯网络模型[8]、REICH模型[9]、深度神经网络[10]。

在系统安全分析方面，系统理论过程分析（System Theoretic Process Analysis，简称STPA）方法具备不同于传统分析方法的优势，即可在分析对象的早期概念分析中启动且能发现其他方法不能识别的故障场景[11]；同时，贝叶斯网络（Bayesian network，简称BN）在分析因果关系的不确定性系统时存在优势。鉴于此，本文选择将STPA方法和BN进行结合，通过构建控制反馈模型、量化危险因素之间的因果关系等方式，对UAM场景下大型无人驾驶航空器运行安全风险进行分析。

1 运行场景

本文研究的运行场景为城市空中交通中大型无人驾驶航空器执行载人运输任务。UAM系统主要由航空器、指挥调度平台、起降场、交互软件、数据链路等系统构成[12]。

1.1 确定主要角色及对应职责

依照美国联邦航空管理局（Federal Aviation Administration，简称FAA）发布的UAM管理体系[13]中，UAM运行场景中包含五个主要角色：政府管理部门、UAM服务供应商、UAM运营商、补充数据服务供应商、联合服务网络。五个主要角色的职责如表1所示。

1.2 描述运行场景

根据主要角色所明确的职责，可将一次完整的UAM服务分为三个阶段：飞行计划审批阶段，起飞与巡航阶段，进近与着陆阶段。

1.2.1 飞行计划审批阶段

首先，UAM运营商接收到乘客通过交互软件提交单个航班的请求（提交出行时间、乘客人数、起终点起降场等信息），然后再根据服务网络内PSU和SDSP共享的实时信息如UAM走廊容量、天气、起降场可用性等，评估飞行请求的可行性。在评估可行之后，UAM运营商将具体的飞行计划包括起降场、时刻、穿越UAM走廊及所需时间、航空器编号等信息提交给PSU。PSU再依据运行规则、空域限制等因素，二次评估UAM运营商提交飞行计划。如评估通过，PSU会将具体授权飞行计划发回，同时将计划信息更新共享在网络中。

如评估未通过,则驳回飞行计划请求,并向UAM运营商反馈原因,便于其二次申请。

1.2.2　起飞与巡航阶段

航空器在起点起降场候客阶段,可通过智能自检系统监测航空器关键设备状态,确保机载设备安全性。上客后,UAM运营商的指挥调度平台将飞行计划信息通过数据链路输入到机载计算机中。航空器自主驾驶完成起飞、巡航等操作,同时机载电子设备、地面传感器、摄像设备等通过数据链路实时向UAM运营商提供飞行状态、位置信息及航空器内外环境等信息,远程机组可通过仪表设备等对航空器运行状态进行监控,并可在紧急情况下对航空器进行远程控制。乘客在飞行全程与远程机组保持语音和视频通信。飞行过程中,UAM运营商通过网络平台与其他UAM运营商、PSU等角色共享信息。

1.2.3　进近与着陆阶段

当航空器接近终点时,起降场要确保降落平台的可用性,保证满足安全降落条件。如遇到不能在原起降场着陆的情况,UAM运营商及时向PSU汇报情况,PSU根据网络中周围起降场位置及可用性、其它可能冲突的飞行计划等因素,协调制定出备降方案。UAM运营商根据情况严重程度可选择通过数据链路飞控计算机自主驾驶或远程机组远程操纵的方式执行备降计划。起降场在航空器安全降落、乘客离机后,可通过机械装置清空起降平台,之后对航空器进行设备检查维修、更换电池、清扫机上卫生等工作,保障航空器可继续进行安全高效的城市空中交通运输服务。PSU通过服务网络监控航空器的着陆情况并发布该飞行计划安全完成的信息,至此一次完整的UAM服务结束。

表1　UAM运行场景主要角色及职责表

Table 1　The main roles and responsibilities of the UAM running scenario

角色	职责
政府管理部门	①组织制定并实施UAM监督管理制度;②运行原空中交通管制服务,明确UAM地理围栏,完成流量管控等操作;③与PSU共享数据包含UAM航空器飞行数据、限制条件、航线、特殊活动空域等信息
UAM服务供应商	①综合考虑UAM运行规则等因素,评估飞行计划,协调制定UAM总体运行计划;②将UAM实时运行计划、空域限制等信息通过联合服务网络向UAM运营商等角色共享;③建立并运行UAM数据库,用于分析、监管及对UAM运营商问责等
UAM运营商	①向PSU提交飞行计划并执行;②运营并维护交互软件、航空器、起降场;③与PSU通过联合服务网络共享UAM航空器飞行数据、起降场位置及可用性等信息
补充数据服务供应商	①通过联合服务网络向PSU、UAM运营商等角色提供地形、障碍物、实时天气等信息服务
联合服务网络	①为PSU、UAM运营商、SDSP等角色提供了共享UAM运行数据信息网络平台;②进行身份识别等操作,保障网络的安全性

2　基于STPA的危险因素识别

STPA是一种基于系统理论和控制理论的安全分析方法[14],将复杂系统视为多个由上而下的分层结构组成,上层结构通过向下方结构施加约束达到控制目的,将系统安全性问题转化为控制问题。

2.1　定义分析的目的

大型无人驾驶航空器运行过程识别存在的系统层级事故,主要包括人员伤亡、航空器受损、地面设施受损,系统级事故如表2所示。人员包括乘客、起降场工作人员、城市地面行人等受伤或死亡(A-1);航空器受损(A-2)包括航空器机械电子设备、整体结构等损坏;地面设施受损(A-3)包括起降场、空中走廊的地面固定设施和移动设施。

表2　大型无人驾驶航空器运运行中的系统级事故

Table 2　System-level accidents in the operation of LUAV

编号	系统级事故
A-1	人员伤亡
A-2	航空器受损
A-3	地面设施受损

系统级危险是指系统的状态处于特定最不利环境条件下将会导致事故的发生[15]。通过分析航

空器运行过程中易发生的系统级事故来分析系统级危险，其主要包括控制失效、偏离预定航线、动力失效，系统级危险如表3所示。

控制失效(H-1)是指航空器在飞行过程中失去控制，航空器设备如控制设备等损坏、与远程机组通信中断、结构受损等原因皆可导致航空器失控。

偏离预定航线(H-2)是指航空器的导航或动力系统未能达到设计工效，导致航空器的实际飞行航线偏离预定，可能导致空中碰撞、与障碍物相撞等事故。

动力失效(H-3)是指航空器的动力系统在飞行过程中因环境、结构性损伤等原因导致的不能正常提供动力，可能导致坠毁等事故。

表3 大型无人驾驶航空器运行中的系统级危险
Table 3 System-level hazards in the operation of LUAV

编号	危险	相关事故
H-1	控制失效	A-1 A-2
H-2	偏离预定航线	A-1 A－2 A-3
H-3	动力失效	A-1 A-2 A-3

2.2 建立控制反馈结构

控制反馈结构主要由控制器、执行器、控制过程、传感器四个组件构成。根据LUAV运行情况，建立的控制反馈结构如图1所示。

远程机组(控制器)通过数据链路设置航空器为自动驾驶模式并输入航线等任务信息，同时也接受航空器位置、状态等信息的反馈。航空器导航系统及飞控系统(执行器)根据远程机组(控制器)发出的任务要求控制动力系统的输出，进而控制航空器的位置、状态。机载传感器(传感器)监测整个控制过程的执行。

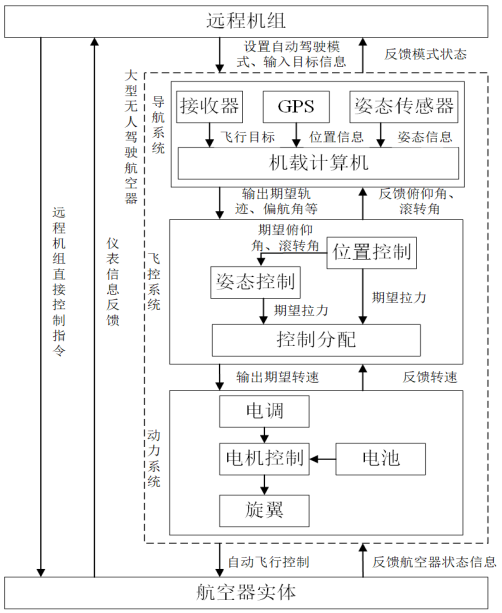

图1 大型无人驾驶航空器运行控制反馈结构
Fig. 1 LUAV operation control feedback structure

2.3 识别不安全控制行为

根据控制反馈结构，识别系统中的不安全控制行为。依据STPA方法定义的四种存在安全隐患的不安全控制行为[16]，列出航空器运行过程中的不安全控制行为，如表4所示。

表4 大型无人驾驶航空器运行过程中的不安全控制行为
Table 4 Unsafe control behavior during the operation of LUAV

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太晚
输入航线等指令(C-1)	—	UCA-1输入错误指令(H-1、H-2)	UCA-2输入指令顺序颠倒(H-1、H-2)	—
数据链路传输指令(C-2)	UCA-3数据链路故障导致通信中断(H-1、H-2)	UCA-4数据链路被攻击，传输错误信息(H-1、H-2)	UCA-5数据链路受干扰，信息传输延迟(H-1、H-2)	UCA-6数据链路受干扰，信息传输不完整(H-1、H-2)
接收器接受指令(C-3)	UCA-7接收器未成功接受信息(H-1、H-2)	UCA-8接收器未能接受准确信息(H-1、H-2)	UCA-9接收器接受信息存在延迟(H-1、H-2)	UCA-10接收器未能接受完整信息(H-1、H-2)
导航系统输入飞控系统指令(C-4)	UCA-11飞控系统未接受指令(H-1、H-2)	UCA-12飞控系统接受错误指令(H-1、H-2)	UCA-13飞控系统接受指令存在延迟(H-1、H-2)	UCA-14飞控系统未能接受完整指令(H-1、H-2)
飞控系统控制旋翼电机输出(C-5)	UCA-15电机不工作(H-1、H-3)	UCA-16电机输出不正确(H-1、H-2)	UCA-17电机输出时刻错误(H-1、H-2)	UCA-18电机停止输出时刻错误(H-1、H-2)

2.4　识别致因场景

致因场景描述的是导致不安全控制行为及危险的诱发因素。根据控制反馈结构,从主动控制和反馈两个方面分析运行过程中的危险因素,如表5所示。

表5　大型无人驾驶航空器运行过程中的危险因素
Table 5　Risk factors during the operation of LUAV

类型	控制结构组件	序号	危险因素
主动控制	远程机组	1-1	远程机组操作失误
		1-2	远程机组应急反应能力差
	数据链路	1-3	数据链路设备故障
	导航系统	1-4	接收器故障
		1-5	GPS组件故障
	飞控系统	1-6	飞控设备机械故障
		1-7	飞控算法存在缺陷
		1-8	人机交互界面崩溃
	动力系统	1-9	电池故障
		1-10	机身结构损坏
		1-11	电机故障
反馈	地面仪表	2-1	地面仪表设备故障

3　基于模糊贝叶斯网络的风险分析

通过STPA分析方法识别出运行危险因素,但仍处于定性分析阶段,无法准确分析各因素对系统安全的影响程度。故选择使用贝叶斯网络进行定量分析,利用上文识别出的危险因素作为节点构建贝叶斯网络,并进行逆向推理、敏感性分析和影响强度分析,明确关键因素和敏感因素。分析结果可以为管理者规避和管控风险提供更多依据和参考。

3.1　网络模型构建

贝叶斯网络适用于因果关系的不确定系统的推理预测,其表现形式为由节点和有向边构成的有向无环图,节点表示随机变量,有向边表示父、子节点之间的条件依赖,用条件概率表(Conditional Probability Tables,简称CPT)表示其关系强度。条件概率可用贝叶斯定理来计算,其Bayes公式为

$$P(X_i|Y)=\frac{P(Y|X_i)P(X_i)}{\sum_{j=1}^{n}P(Y|X_j)P(X_j)} \tag{1}$$

式中:$P(X_i)$、$P(Y_j)$为先验概率;$P(X_i|Y)$为后验概率;$P(Y|X_i)$、$P(Y|X_j)$均为条件概率。

以识别出的危险因素作为节点,因素之间的因果关系为依据,构建LUAV运行风险的贝叶斯网络。另外由于STPA分析方法主要分析识别控制系统内部的危险因素,缺乏考虑外部环境因素,故需要加入2个环境危险因素节点:恶劣天气、强电磁干扰。构建的贝叶斯网络模型,如图2所示。

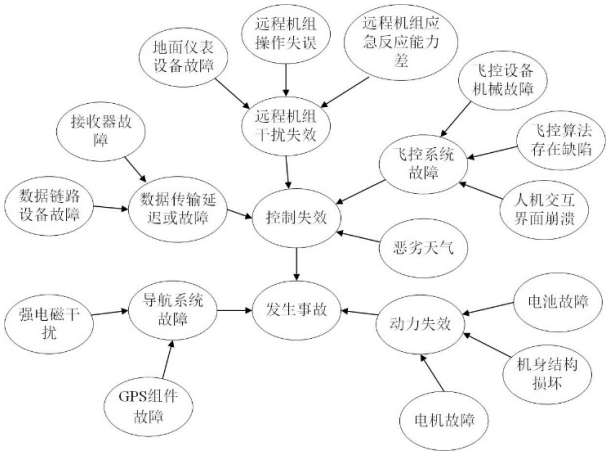

图2　大型驾驶航空器运行风险贝叶斯网络模型
Fig. 2　Bayesian network model of operational risk for LUAV

3.2　确定模型参数

模型参数包括父节点的先验概率和中间节点的条件概率。由于当前LUAV未大量运行数据缺少,故不能通过统计数据的方法来确定事件的发生概率。模糊集理论对解决精确性低和模糊性问题有较大的帮助[17],符合模型的基本情况。因此本文选择通过基于模糊集理论的专家打分法确定模型参数。

3.2.1　确定父节点的先验概率

为将专家对事件发生概率打分的结果通过模糊数表达,需引入语言变量。Wickens[18]认为事件的发生概率可使用七种语言值来描述:很低(VL)、低(L)、偏低(FL)、中等(M)、偏高(FH)、高(H)、很高(VH)。各语言变量对应的模糊数表现形式和λ－截集如表6所示。

表6 模糊数形式
Table 6 Fuzzy number form

代号	模糊数形式	λ－截集
VL	(0,0,0.1,0.2)	[0,−0.1λ+0.2]
L	(0.1,0.2,0.3)	[0.1λ+0.1,−0.1λ+0.3]
FL	(0.2,0.3,0.4,0.5)	[0.1λ+0.2,−0.1λ+0.5]
M	(0.4,0.5,0.6)	[0.1λ+0.4,−0.1λ+0.6]
FH	(0.5,0.6,0.7,0.8)	[0.1λ+0.5,−0.1λ+0.8]
H	(0.7,0.8,0.9)	[0.1λ+0.7,−0.1λ+0.9]
VH	(0.8,0.9,1,1)	[0.1λ+0.8,1]

本文使用算数平均法得到多个专家对同一事件的发生频率的综合评价结果：

$$P_j=\frac{F_{1j}+F_{2j}+\cdots+F_{mj}}{m}\ j=1\cdots n \tag{2}$$

式中：P_i为第i个事件的模糊发生概率；F_{ij}为第i个专家对第j事件频率评价值；n为事件总数目；m为专家总人数。

在得到基于专家经验的模糊评价结果后，需进行模糊数求解，其重点在于求解代表模糊集合的单值，即实现将估值转换为实际数值的目的。本文选择采用较易于理解且计算简便的积分值法。积分值法解模糊数的公式具体如下：

$$I(P)=\varepsilon I_R(P)+(1-\varepsilon)I_L(P) \tag{3}$$

式中：$I(P)$为模糊数P解模糊值；ε为乐观系数，$\varepsilon\in[0,1]$，当$\varepsilon=0$和$\varepsilon=1$时$I(P)$为解模糊值的上下界，当$\varepsilon=0.5$时为解模糊值的代表值；$I_L(P)$和$I_R(P)$分别对应模糊数左右隶属度函数反函数的积分值。

$$I_R(P)=\frac{1}{2}\left[\sum_{\lambda=0.1}^{1}\lambda_R(P)\Delta\lambda+\sum_{\lambda=0}^{0.9}\lambda_R(P)\Delta\lambda\right] \tag{4}$$

$$I_L(P)=\frac{1}{2}\left[\sum_{\lambda=0.1}^{1}\lambda_L(P)\Delta\lambda+\sum_{\lambda=0}^{0.9}\lambda_L(P)\Delta\lambda\right] \tag{5}$$

运用Matlab软件对结果进行计算可得，各父节点的先验概率为0.47，0.35，0.65，0.56，0.54，0.43，0.18，0.23，0.44，0.38，0.56，0.43，0.69，0.70。

3.2.2 确定中间节点的条件概率

由于LUAV缺少完备的运行数据库，而Leaky Noisy-or Gate扩展模型[19]可在有效数据不充分的情况下依据专家知识来确定贝叶斯网络的参数。

Leaky Noisy-or Gate扩展模型假设了一个简单的模型即一个子节点有2个相互独立的父节点，分别为X_i和X_{all}(除X_i外的因素合并而成)，P_i和P_{all}是其连接概率，则有：

$$P(Y|X_i)=P_i+P_{all}-P_iP_{all} \tag{6}$$

$$P(Y|\bar{X}_i)=P_{all} \tag{7}$$

根据式(6)和式(7)获得父节点的连接概率P_i后，再结合未知因素及其连接概率P_L，从而得出子节点的条件概率为

$$P_i(Y)=1-(1-P_L)\prod_{i:X_i\in X_p}(1-P_I) \tag{8}$$

由先验概率可确定各子节点与其父节点之间的连接概率，再利用Leaky Noisy-or Gate扩展模型计算得到条件概率表[20]。以节点控制失效为例，其条件概率表如表7所示。

表7 控制失效条件概率表
Table 7 Failure condition probability table

数据传输延迟故障	远程机组干扰失效	飞控系统故障	恶劣天气	数据条件概率	
				Yes	No
Yes	Yes	Yes	Yes	0.94	0.06
			No	0.81	0.19
		No	Yes	0.88	0.12
			No	0.63	0.37
	No	Yes	Yes	0.89	0.11
			No	0.66	0.34
		No	Yes	0.79	0.21
			No	0.35	0.65
No	Yes	Yes	Yes	0.92	0.08
			No	0.73	0.27
		No	Yes	0.84	0.16
			No	0.49	0.51
	No	Yes	Yes	0.85	0.15
			No	0.53	0.47
		No	Yes	0.71	0.29
			No	0.10	0.90

3.3 参数学习

参数学习是利用先验概率和样本数据来获得对未知样本的估计[21]。本文选择GeNIe分析软件进行贝叶斯网络的参数学习以及后续的定量分析。将节点、有向边输入到GeNIe中，将收集到的数据进行规范化处理后设置到对应节点，网络构建成功后进行参数学习，得到的结果如图3所示。

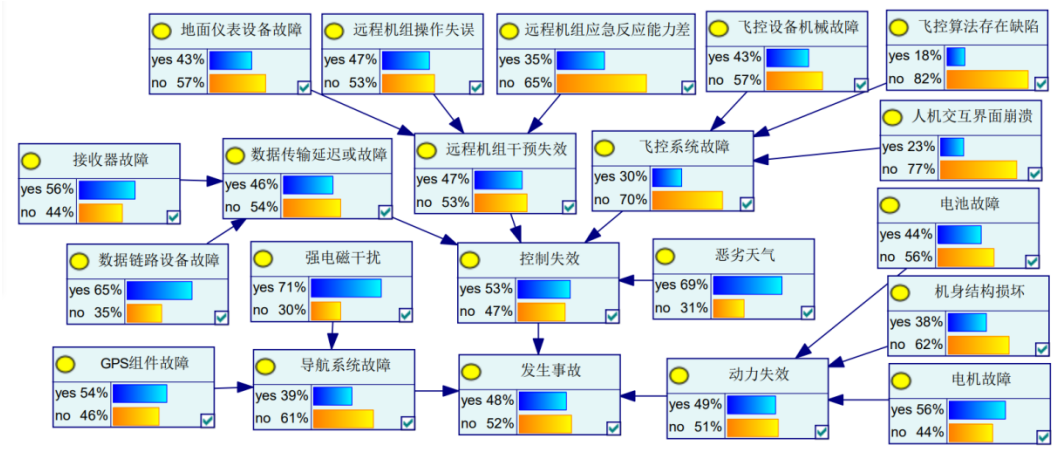

图3　贝叶斯网络参数学习结果

Fig. 3　Bayesian network parameter learning results

3.4　模型定量分析

对网络进行参数学习后,得到LUAV事故发生的概率分布情况,但因素间的定量关系仍不能确定。因此需要利用贝叶斯网络的逆向推理、敏感性分析以及影响强度分析对危险因素间的关系进行分析。

3.4.1　逆向推理

后验概率可用来判定各个危险因素对事故的影响程度。将发生事故设置为100%,逆向推理出各因素的后验概率,从而确定关键因素[22]。逆向推理结果如图4所示。直接导致发生事故的三大系统级危险从大到小依次是:控制失效72%、动力失效56%、导航系统故障47%。控制失效可导致航空器与建筑、其他航空器发生碰撞或坠地;动力失效可导致航器失速进而发生碰撞;导航系统故障导致偏离航线进而发生碰撞,三者是设备因素中最关键的因素。其他风险中从大到小前6种依次是:强电磁干扰72%、恶劣天气71%、数据链路设备故障67%、电机故障57%、接收器故障57%。该结果说明环境因素是导致航空器在UAM场景下发生事故的关键因素;此外,也说明了除了电机、接收器、电池等机载设备因素外,地面的数据链路设备也是较为关键的因素。

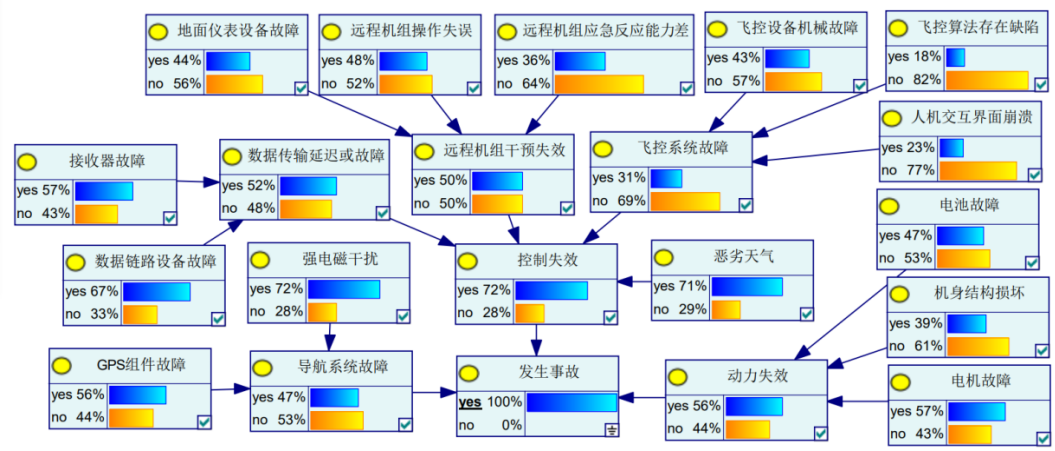

图4　贝叶斯网络逆向推理结果

Fig. 4　Bayesian network inverse inference results

3.4.2　敏感性分析

敏感性分析是研究网络中节点的数值变化对输出参数的影响程度。颜色的深度代表各因素的敏感性大小,颜色越深则敏感性越大。这里将“发生事故”作为目标节点分析,如图5所示,可以看出:导航系统故障、恶劣天气、电池故障、数据传输延迟或故障敏感性较大,GPS组件故障、接收器故障、强电磁干扰、远程机组应急反应能力差的敏感

性次之,其余因素敏感性较小。

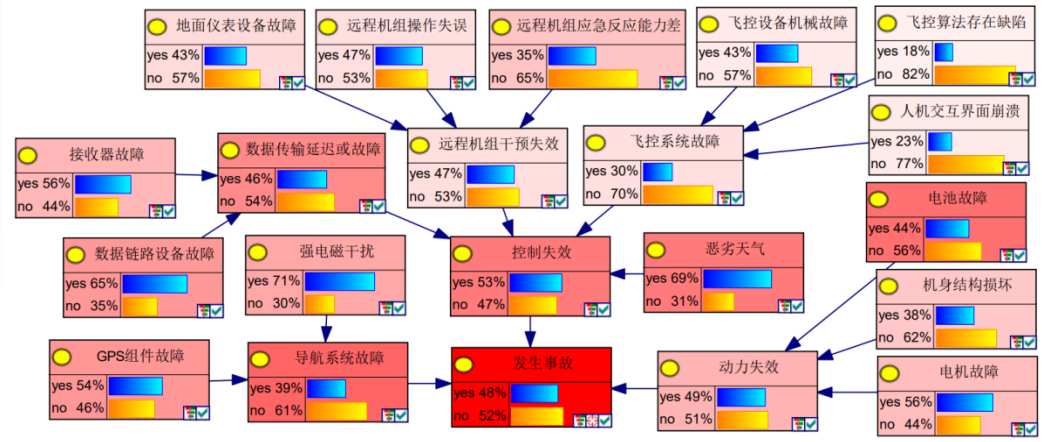

图 5 贝叶斯网络敏感性分析结果

Fig. 5 Bayesian network sensitivity analysis results

3.4.3 影响强度分析

影响强度分析用于研究节点间的依赖程度,管理者可依据影响强度分析的结果对依赖程度较高的风险进行统一化管理,将会取得更好的管理效果。影响程度的大小由节点间连线的宽度来表示,宽度越大影响强度越大。影响强度分析结果如图 6 所示。从图可知风险网络中影响强度最大的 4 条父子节点路径为:①电池故障→动力失效;②远程机组应急反应能力差→远程机组干扰失效;③数据链路设备故障→数据传输延迟或故障;④数据传输延迟或故障→控制失效。电池故障导致电机输出下降或不稳定,进而导致动力失效,此风险链对航空器运行安全影响最大。远程机组在紧急情况下的应急反应能力差导致操作或决策失误,进而导致机组远程干预失效,其影响程度次之。

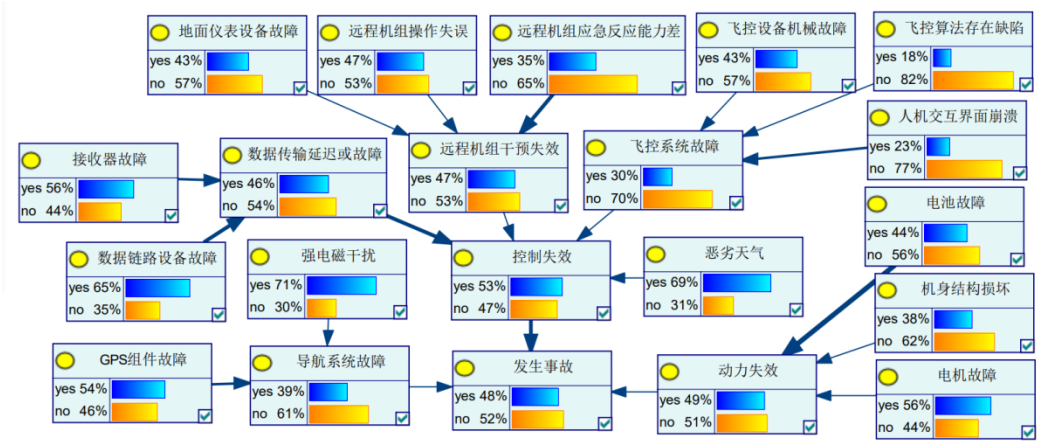

图 6 贝叶斯网影响强度分析结果

Fig. 6 Bayesian nets affect intensity analysis results

4 风险管控建议

研究结果显示关键危险因素为控制失效、动力失效等。根据 NTSB 于 2021 年 3 月 25 日发布的货运 eVTOL 的事故调查报告[23]可对分析结果进行实例验证。事故经历为飞行器转速控制器发生故障导致动力失效,随后飞控系统自动降低电机推力以保持姿态控制,从而导致整体推力降低发生坠机事故。这与本文危险因素传播链及结果相吻合,证明通过贝叶斯网络分析关键风险因素具有有效性。

依据分析结果从设备、人员、环境三个方面提

出大型无人驾驶航空器风险防控建议。

4.1 设　备

1) 飞控系统选择可靠性高、安全性好的系统,同时鼓励飞控系统设计时使用余度技术以提高系统可用性和安全性。

2) 对电机、电池等易发生故障的设备加强基础监测与管理,加强对关键设备航前检查的力度,同时积极使用远程监控等技术对关键设备状态进行监测。

3) 航空器结构设计时将罗磁盘的位置设计在避免受到城市电磁环境干扰的位置。

4.2 人　员

1) 制订详细的远程机组安全驾驶手册,进行定期培训和考查,同时制订地面仪表设备、数据链路地面基站定期检查维修制度,确保远程机组实时监控飞行器状态并可在突发情况下实现远程操控。

2) 对远程机组人员进行应急专业知识培训,提升应急反应能力,使远程机组能在突发情况下做出正确决策和操作。

4.3 环　境

1) 建立航路网规划系统,基于时空地理大数据、人工智能等技术,构建净空边界低空地理网格数据库,并研发契合空中廊桥优化与快速构建技术,实现低空公共路网规划功能。

2) 建立运行监管系统,基于三维地理信息等前沿技术,设计与构建云计算框架下的统一监管平台,实时监控航空器运行动态,实现高效和安全监管。

3) 建立高精度航路气象预报系统,基于自适应网络技术、无人机搭载小型气象站等新兴技术,满足UAM气象预报米级和小时级的要求,为航空器的安全运行提供气象保障。

5 结　论

1) 运用STPA方法驱动下的模糊贝叶斯网络对LUAV运行风险概率进行正向因果推理,并通过逆向推理等分析确定关键因素等,为管理工作者进行风险防控提供依据和参考。结果表明,控制失效是导致大型无人驾驶航空器事故发生的最关键因素;导航系统故障、恶劣天气、电池故障是高敏感性因素。

2) 由于UAM还未实现运行缺少数据,未来可考虑再导入运行数据库以提高运行风险分析的准确性和可靠性。

参 考 文 献

[1] KOPARDEKA P. Unmanned aerial system (UAS) traffic management (UTM): enabling low-altitude airspace and UAS operations[EB/OL]. (2014-04-01)[2024-05-11]. https://ntrs.nasa.gov/citations/20140013436.

[2] AIRBUS. Blueprint for the sky: the roadmap for the safe integration of autonomous aircraft[EB/OL]. (2018-09-05)[2024-05-11]. https://storage.googleapis.com/blueprint/Airbus_UTM_Blue-print.pdf.

[3] Uber. Fast-forwarding to a future of on-demand urban air transportation [EB/OL]. (2018-09-05) [2024-05-11]. https://eVTOL.news/media/PDFs/UberElevateWhitePaperOct2016.pdf.

[4] ROBIN L, VINCENT R, AIJAz H. Change is in the air: the elevated future of mobility: What's next on the horizon? [EB/OL]. (2019-06-03)[2024-05-11]. https://www.deloitte.com/us/en/insights/focus/future-of-mobility/evtol-elevated-future-of-mobility-summary.htm.

[5] 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.
WANG Hongyong, WEN Ruiying. Research on assessment of risk in air traffic situation based on complex network[J]. China Safety Science Journal, 2018, 28(5): 172-178. (in Chinese)

[6] WEIBEL R, HANSMAN R J. An integrated approach to evaluating risk mitigation measures for UAV operational concepts in the NAS[C]// 2005 IEEE Infotech and Aerospace Conference. Reston: AIAA, 2005: 6957.

[7] WACKWITZ K, BOEDECKER H. Safety risk assessment for UAV operation[J]. Drone Industry Insights, 2015, 1: 31-53.

[8] 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.
QIAN Yu, LONG Tao. Risk assessment on transport aircraft exceeding tire speed rating based on cloud Bayesian network[J]. Advances in Aeronautical Science and Engineering, 2022, 13(3): 171-178. (in Chinese)

[9] 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.
LI Xinfei. Research on distribution network layout planning and security analysis of logistics UAV[D]. Nanjing: Nanjing University of Aeronautics and Astronautics, 2020. (in

Chinese)

[10] JEONG S, YOU K, SEOK D. 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.

[11] THOMAS J. Extending and automating a systems-theoretic hazard analysis for requirements generation and analysis[D]. Cambridge: MIT , 2013.

[12] 广州亿航智能技术有限公司. 亿航智能城市空中交通系统白皮书[EB/OL]. (2020-01-08)[2024-05-11]. https://www.ehang.com/cn/uam/.
Guangzhou EHang Intelligent Technology Co. White paper of EHang intelligent urban air traffic system [EB/OL]. (2020-01-08)[2024-5-11]. https://www.ehang.com/cn/uam/.

[13] FAA. Urban air mobility concept of operations v2.0 [EB/OL]. (2023-04-26) [2024-05-11]. https://www.faa.gov/sites/faa.gov/files/Urban%20Air%20Mobility%20%28UAM%29%20Concept%20of%20Operations%202.00.pdf.

[14] LEVESON N. A new accident model for engineering safer systems[J]. Safety Science, 2004, 42(4): 237-270.

[15] LEVESON N G. Engineering a safer world: Systems thinking applied to safety[M]. Cambridge: MIT Press, 2011: 165-171.

[16] 王军武, 潘子瑶, 王靖, 等. 基于STPA和模糊BN的装配式建筑吊装施工安全风险分析[J]. 中国安全生产科学技术, 2022, 18(4): 12-19.
WANG Junwu, PAN Ziyao, WANG Jing, et al. Safety risk analysis on hoisting construction of prefabricated building based on STPA and fuzzy BN[J]. Journal of Safety Science and Technology, 2022, 18(4): 12-19. (in Chinese)

[17] ZADEH L A. Fuzzy sets [J]. Information and Control, 1965, 8(3): 338-353.

[18] WICKENSC D. Engineering psychology and human performance[M]. New York: Harper Collins Inc. , 1992.

[19] 张俊光, 徐振超, 贾赛可. 基于Noisy-or Gate和贝叶斯网络的研发项目风险评估方法[J]. 科技管理研究, 2015, 35(1): 193-196, 206.
ZHANG Junguang, XU Zhenchao, JIA Saike. Risk assessment on research and development project based on noisy-or gate and Bayesian network [J]. Science and Technology Management Research, 2015, 35(1): 193-196, 206. (in Chinese)

[20] 董华珊, 侯学良. 基于Leaky Noisy-or Gate和贝叶斯网络的光伏发电项目施工风险评估方法[J]. 科技和产业, 2023, 23(2): 218-223.
DONG Huashan, HOU Xueliang. Construction risk assessment of PV project based on leaky noisy-or gate and Bayesian network[J]. Science Technology and Industry, 2023, 23(2): 218-223. (in Chinese)

[21] 陈远, 金蕊, 查亚闯. 基于贝叶斯网络的大型公共项目进度延误风险研究[J]. 郑州大学学报(工学版), 2022, 43(2): 91-97.
CHEN Yuan, JIN Rui, ZHA Yachuang. Research on delay risk of large complex public projects based on Bayesian network[J]. Journal of Zhengzhou University (Engineering Science), 2022, 43(2): 91-97. (in Chinese)

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

[23] National Transportation Safety Borad. Aviation accident final report: DCA21LA094[R]. US: National Transportation Safety Borad, 2021.

(编辑:丛艳娟)