

中文引用格式:董磊,宋文佳,陈曦,等. 面向预期功能安全的 eVTOL 智能避障系统运行时保证方法[J]. 中国安全科学学报, 2024, 34(7):105-112.

英文引用格式:DONG Lei, SONG Wenjia, CHEN Xi, et al. Runtime assurance method for eVTOL intelligent obstacle avoidance system toward safety of intended functionality [J]. China Safety Science Journal, 2024, 34(7):105-112.

# 面向预期功能安全的 eVTOL 智能避障系统运行时 保证方法\*

董磊<sup>1,2</sup>副研究员, 宋文佳<sup>1,3</sup>, 陈曦<sup>\*\*1,2</sup>助理研究员, 刘嘉琛<sup>1,4</sup>, 梁博尧<sup>1,4</sup>

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

中图分类号: X949

文献标志码: A

DOI: 10.16265/j.cnki.issn1003-3033.2024.07.0198

基金项目: 民用航空器适航审定技术重点实验室开放基金资助(SH2023101701); 中央高校基本科研业务费(3122022044); 中央高效基本科研业务费(3122022QD07)。

**【摘要】** 为保障电动垂直起降飞行器(eVTOL)在城市空中交通(UAM)场景下的预期功能安全(SOTIF), 降低人工智能算法的验证难度, 建立基于运行时保证(RTA)方法的避障模型。首先, 使用人工势场法改进的柔性动作评价(SAC)算法作为 eVTOL 智能避障系统的复杂功能; 然后, 使用动态反应规划(DRP)作为智能航电系统的备用功能, 以减缓 SOTIF 危险, 同时, 使用监视和决策模块采集环境状态, 搭建 RTA 架构; 最后, 分别仿真仅使用复杂功能和具有 RTA 架构的避障系统, 对比避障效果。结果表明: 2 种方法均可实现避障, 但仅使用复杂功能的传统避障系统会带来 SOTIF 危险; 经过 RTA 架构设计, 可使 eVTOL 的安全飞行时长占比由 78.4% 提高到 98.15%, 总航路长度仅增加 0.95%, 在保障效率的同时, 降低了在运行场景中的风险。

**【关键词】** 预期功能安全(SOTIF); 电动垂直起降飞行器(eVTOL); 运行时保证(RTA); 城市空中交通(UAM); 智能避障系统

## Runtime assurance method for eVTOL intelligent obstacle avoidance system toward safety of intended functionality

DONG Lei<sup>1,2</sup>, SONG Wenjia<sup>1,3</sup>, CHEN Xi<sup>\*\*1,2</sup>, LIU Jiachen<sup>1,4</sup>, LIANG Boyao<sup>1,4</sup>

(1 Key Laboratory of Civil Aircraft Airworthiness Technology, Civil Aviation University of China, Tianjin 300300, China; 2 Science and Technology Innovation Research Institute, Civil Aviation University of China, Tianjin 300300, China; 3 Sino-European Institute of Aviation Engineering, Civil Aviation University of China, Tianjin 300300, China; 4 College of Safety Science and Engineering, Civil Aviation University of China, Tianjin 300300, China)

**Abstract:** To ensure the SOTIF of eVTOL vehicles in UAM and reduce the verification difficulty of artificial intelligence algorithms, an obstacle avoidance model was proposed based on RTA method.

\* 文章编号: 1003-3033(2024)07-0105-08; 收稿日期: 2024-01-13; 修稿日期: 2024-04-21

\*\* 通信作者: 陈曦(1987—), 男, 河北邯郸人, 博士, 助理研究员, 主要从事模式识别与图像处理方面的研究。E-mail: csxichen@outlook.com。

Firstly, SAC (soft actor-critic) algorithm improved by the artificial potential field method was used as the complex function of the eVTOL intelligent obstacle avoidance system. Then, dynamic response planning (DRP) was used as a backup function of the intelligent avionics system to mitigate SOTIF hazards. Moreover, monitoring and decision-making modules were adopted to obtain environmental conditions and develop an RTA architecture. Finally, the simulated obstacle avoidance performance was compared between the two systems using complex function and RTA. The results showed that both methods can achieve obstacle avoidance, but the traditional obstacle avoidance system using complex functions may impose SOTIF risk. The RAT architecture design increased safe flight time from 78.4% to 98.15%, with the total route length only increasing by 0.95%, reducing risks in operational scenarios while ensuring efficiency.

**Keywords:** safety of the intended functionality (SOTIF); electric vertical take-off and landing (eVTOL); runtime assurance (RTA); urban air mobility (UAM); intelligent obstacle avoidance system

## 0 引言

近 10 年来,随着分布式电力推进技术、计算机技术以及通信技术的迅猛发展,国内外航空管理局、民航研究组织以及工业方竞相进入针对电动垂直起降 (electric Vertical Take Off and Landing, eVTOL) 航空器的研究与开发中<sup>[1]</sup>。城市空中交通 (Urban Air Mobility, UAM) 是利用低空空间进行各种交通活动的总称<sup>[2]</sup>。在复杂的 UAM 场景中,保障航空器安全出行、有效避免与地面障碍物的碰撞冲突,是亟待解决的技术难题。《绿色航空制造业发展纲要》<sup>[3]</sup>指出,围绕智能化、体系化、网络化技术趋势,结合 eVTOL 航空器性能优势和 5 G、大数据、人工智能等新技术,开展辅助驾驶技术研究,将是未来 UAM 重要的应用区域。然而,随着智能化技术的快速发展,许多包含复杂功能的算法、组件、功能或系统难以或无法通过传统的航空研制保证体系的符合性验证。即使在整机层预期功能的规范足够完备,由于系统组件的性能局限和场景的多样性,感知、决策和控制等功能的实现可能不符合预期<sup>[4]</sup>。因此,采取恰当的方式从技术可信性等方面向公众和利益相关方证实智能航电系统的适航安全性,并预防由于预期功能安全 (Safety Of The Intended Functionality, SOTIF) 所导致的危害,是民用航空工业从自动化发展体系向智能化发展体系过渡需要面对的关键问题,亦是采用智能化机载技术的 eVTOL 航空器进入市场的重要前提<sup>[5-6]</sup>。

运行时保证 (Run-Time Assurance, RTA) 作为一种典型的安全风险减缓技术,受到包括美国国家航空航天局 (National Aeronautics and Space

Administration, NASA)<sup>[7]</sup>、欧洲航空安全局 (European union Aviation Safety Agency, EASA)<sup>[8]</sup> 和德国宇航中心<sup>[9]</sup> 等机构的重点关注。RTA 通过在智能化系统的执行过程中提供额外的监控和备用功能,规定智能化系统的运行范围,修正其可能带来潜在风险的输出,确保系统的行为始终位于安全范围内。诸多研究将 RTA 与智能化机载技术相结合,如 DARREN 等<sup>[10]</sup> 基于美国材料与试验协会发布 (American Society for Testing Materials, ASTM) 的 ASTM F3269-17 的 RTA 架构,使用多种 RTA 监视组件限制学习型组件的行为。SALMAN 等<sup>[11]</sup> 提出一种在具有分布式航空电子架构的多旋翼飞行器上实现 RTA 切换逻辑的方法,以保障遇到故障时飞行的连续性。ZACK<sup>[12]</sup> 探究了一种基于 RTA 架构的通用航空飞机轨迹预测算法,以预防碰撞和失控情况。上述将 RTA 架构应用于智能化飞行器的研究多局限于飞行的稳定性与连续性,与实际 UAM 场景中同时避开动态与静态障碍物、保证 SOTIF 安全的任务需求仍存在一定差距。

鉴于此,笔者拟使用 RTA 架构保证 SOTIF,由人工势场法改进的柔性动作评价 (Soft Actor-Critic, SAC) 算法实现复杂功能,基于动态反应规划 (Dynamic Reactive Planning, DRP) 备用功能,与监视关键参数的决策模块共同组成 RTA 架构,实时检查该复杂避障输出的安全性,并修正超出安全区域的行为,保证智能避障系统输出的安全性,以期减缓 SOTIF 危险。

## 1 eVTOL 避障系统的 SOTIF 分析

无论是汽车工业中的 V 模型产品开发流程,还

是民用飞机研制过程中的双 V 模型,出发点仍是基于需求的定义和迭代。由于驾驶舱智能系统使用场景的复杂性和人工智能基于数据驱动的特点,与智能系统安全相关的很多问题在设计阶段无法预见,无法准确定义需求。国际标准化组织针对智能系统中影响更广泛的非故障安全领域,发布了 *Safety of the intend-ed functionality*<sup>[13]</sup>。该标准围绕自动驾驶系统的性能限制或人员可预见的误用造成的危害,从安全性和已知性的角度,将 eVTOL 运行场景划分为 4 个区域,如图 1 所示。在系统研制初期,区域 2 和区域 3 的比例较高,而 SOTIF 的目的就是评估潜在风险,通过改善系统功能、限制运行设计域 (Operational Design Domain, ODD) 和反馈测试结果 3 种手段,尽可能缩小区域 2 和区域 3 的场景比例,确保场景控制在安全范围内<sup>[14]</sup>。

智能机载技术则面临着 SOTIF 问题,eVTOL 避障功能的 SOTIF 危险产生机制如图 2 所示。由于智能航电系统在感知、决策等方面易受外界环境干扰,即使系统并未发生故障,也可能由于黑盒输出的不稳定性导致预期功能发生偏离。针对 eVTOL 智能化避障系统的可信性问题,目前,从 SOTIF 角度出发的功能改进方法众多,通过功能冗余的方法来解

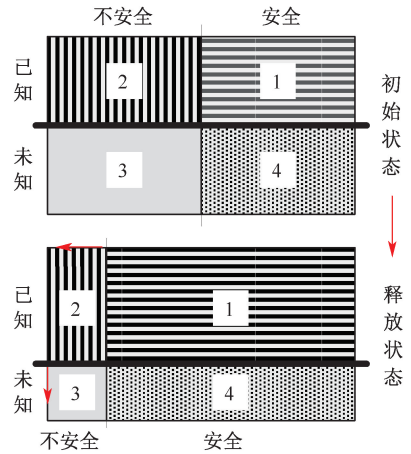


图 1 SOTIF 运行场景类别划分

Fig. 1 SOTIF operation scenario classification

决智能系统带来的不确定性问题简单且行之有效。

针对上述问题,RTA 方法用监控模块和控制模块包围不安全的 AI/ML 组件。监控模块通过检测系统复杂功能的输入输出和内部状态变量,以此判断系统是否在正常功能域内运行。若系统在运行时检测到异常,RTA 切换器将会进行重新配置,用备用功能代替异常的复杂功能,最大限度地将安全理念融入到人机环系统的全生命周期<sup>[15]</sup>。

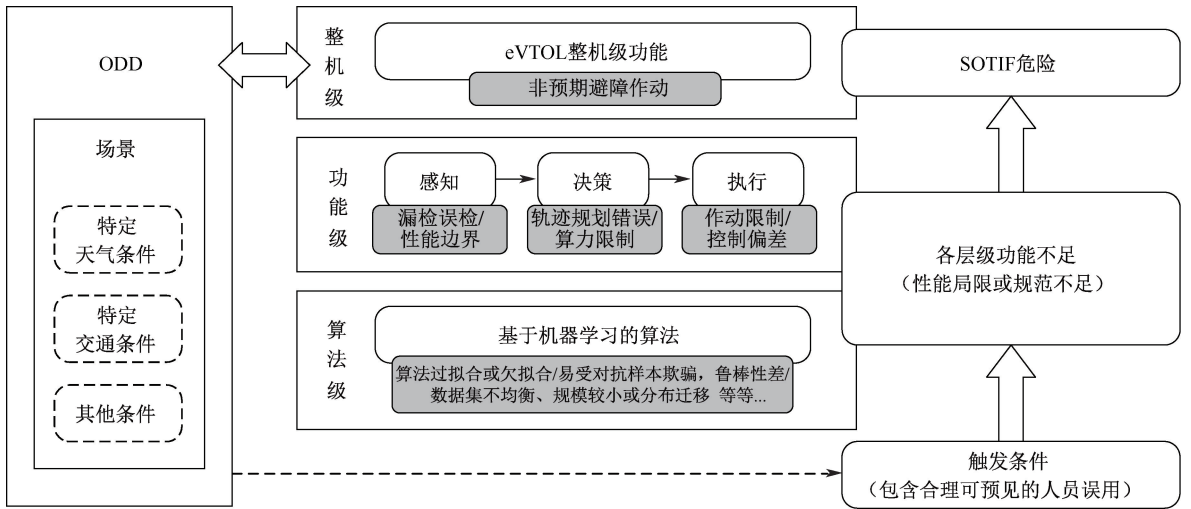


图 2 eVTOL 避障功能的 SOTIF 危险产生机制

Fig. 2 SOTIF hazard generation mechanism for eVTOL obstacle avoidance function

## 2 eVTOL 避障系统的 RTA 方法

RTA 的系统架构主要由被控对象、复杂功能、备用功能和监控与决策控制模块组成,如图 3 所示。在航空器飞行过程中,RTA 监视器不断记录和计算系统的运动状态和环境状况,并进行检测分析,记安

全环境状态为  $\phi_s$ ;若检测到有异常状况和非预期功能问题的突发情况,记此时的环境状态为  $\phi_u$ 。当 RTA 监视器检测到有环境状态  $\phi_s$  和  $\phi_u$  之间的转化时,RTA 会将系统的控制权从复杂功能移交给备用功能,以保障 SOTIF。

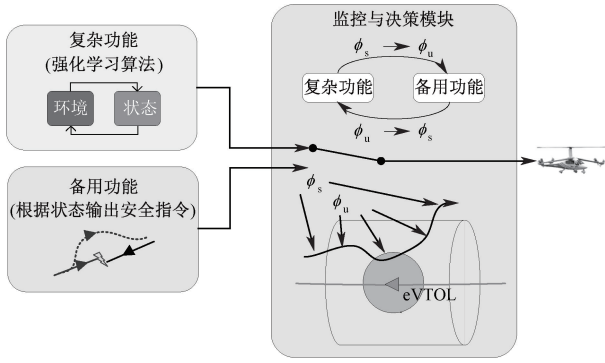


图3 RTA 架构

Fig. 3 RTA framework

## 2.1 基于 SAC 的复杂避障功能设计

SAC<sup>[16]</sup>算法是一种适合连续动作空间的强化学习算法,该算法具有1个 Actor 网络、2个 Critic 网络和2个 Critic 目标网络。记 Actor 网络的参数为  $\theta$ , 2个 Critic 网络的参数分别为  $\psi_1$  和  $\psi_2$ , 2个 Critic 目标网络的参数分别  $\bar{\psi}_1$  和  $\bar{\psi}_2$ ,  $t$  为时间步, Actor 网络接收输入的环境状态  $s_t$ 。根据输出的动作空间概率分布的均值和方差,生成动作  $a_t$ 。根据目前采集到的状态和动作,使用人工势场法 (Artificial Potential Field, APF) 计算当前位置受到的障碍物的斥力和目标的引力,优化动作  $a_t$ ,以生成高效且安全的新动作  $a'_t$ ,执行后动作  $a'_t$  转移至新状态  $s_{t+1}$ 。利用 Critic 网络评估新动作  $a'_t$ ,得到奖励值  $r_t$ 。利用 Critic 目标网络评估当前状态,得到  $Q$  值; Actor 网络输出的动作使得动作熵和 Critic 网络输出的动作价值变大,表明采取的动作是一个较好的动作,使 Critic 目标网络对当前状态的价值评估值变大,则更新网络参数。APF 改进 SAC 算法伪代码见表1。

## 2.2 基于 DRP 的备用避障功能设计

备用功能负责航空器在运行过程中遇到异常状况或有 SOTIF 危险的突发障碍时接管避障控制权,以避免危险。与复杂避障功能相比,备用功能不追求避障的效率,仅用于输出安全的避障路径。

NASA 等在 2021 年改进了 DRP<sup>[17]</sup> 方法,该方法通过不断计算避免碰撞的方案,达到和障碍物保持安全距离、且不超出空中走廊的限制范围的目的。在 DRP 的研究基础上,提出基于航向指令和距障碍物距离随时间步获取避障指令的方法,直到水平和垂直方向上的安全域都不被侵犯,备用功能修正 eVTOL 航向的运行如图4所示。

表1 APF 改进 SAC 算法伪代码

Table 1 SAC algorithm pseudocode improved by APF

伪代码 1: APF 改进 SAC 算法

初始化参数  $\theta, \psi_1, \psi_2, \bar{\psi}_1, \bar{\psi}_2$

初始化经验池

for 轮次 = 1 到  $M$

接收初始状态  $s_1$

for  $t = 1$  到  $T$

依据策略  $\pi(\theta)$  和状态  $s_t$  生成动作  $a_t$

APF 优化  $a_t \rightarrow a'_t$

执行动作  $a'_t$ , 观察奖励  $r_t$  和新状态  $s_{t+1}$

将  $(s_t, a_t, r_t, s_{t+1})$  添加到经验池  $D$

for  $j = 1$  到 更新次数 do

经验池  $D$  随机采样一批数据

计算评论家目标网络的  $Q$  值

更新评论家网络参数  $\psi_1$  和  $\psi_2$

更新演员网络参数  $\theta$

软更新评论家目标网络参数  $\bar{\psi}_1$  和  $\bar{\psi}_2$

end for

令  $s_t \leftarrow s_{t+1}$

end for

end for

- 保持净空体积
- 最小分离距离
- 复杂功能航迹
- - - 备用功能航迹

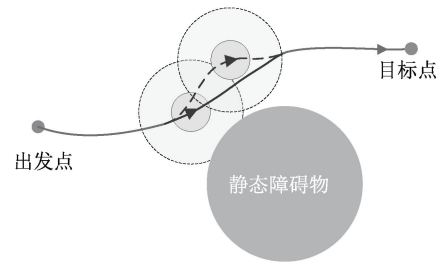


图4 备用功能控制 eVTOL 修正航向

Fig. 4 Baseline control eVTOL heading

首先,记航空器水平和垂直方向上的安全距离分别为  $d_h, d_v$ , 当前时刻距障碍物水平方向和垂直方向的距离分别为  $d_{(x,y)} \equiv (d_x, d_y), d_z$ 。通过定义圆柱范数  $\|d_c\|$  来表示航空器与障碍的归一化后的相对距离,公式如下:

$$\|d_c\| = \max\left(\frac{\|d_{(x,y)}\|}{d_h}, \frac{|d_z|}{d_v}\right) \quad (1)$$

当  $\|d_c\| \leq 1$  时,航空器不能保持由圆柱范数所定义的安全距离,备用功能所搭载的 DRP 控制器发挥作用,输出航向控制指令,同时,不断计算安全距离,直至恢复安全距离时,切换回基于 SAC 的复杂避障功能,航向控制指令计算如下:

$$V_i = \dot{X}_i \mathbf{i} + \dot{Y}_i \mathbf{j} + \dot{Z}_i \mathbf{k} \quad (2)$$

$$\dot{X}_i = V_i \cos(\gamma_i) \cos(\psi_i) \quad (3)$$

$$\dot{Y}_i = V_i \cos(\gamma_i) \sin(\psi_i) \quad (4)$$

$$\dot{Z}_i = V_i \sin(\gamma_i) \quad (5)$$

式中:  $V_i$  为当前时刻的速度;  $X_i$ 、 $Y_i$ 、 $Z_i$  为 3 个方向上的速度分量, m/s;  $\gamma_i$ 、 $\psi_i$  分别为航向角和俯仰角, rad。在不能保持安全距离的方向上, 输出航向沿障碍物切线的镜像对称 ( $\gamma'_i$ ,  $\psi'_i$ ), 随时间步更新 eVTOL 的航向, 获取备用功能控制下的避障路径, 直至 eVTOL 不再处于危险状态。

### 2.3 RTA 架构及功能切换逻辑定义

RTA 架构主要由复杂功能、备用功能和监控与决策模块组成。无论采取何种方法为具有高级、不可信组件的系统提供运行时保护, 主要目标是不严格限制或限制复杂功能的操作范围。文中开发的框架对先进系统的允许操作区域施加了限制, 复杂功能系统的运行范围仅限于  $\phi_s$  规定的安全范围。备用功能系统的操作范围需要大于复杂功能系统的操作范围, 必须覆盖  $\phi_s$ 。但备用功能主要是保障系统回到安全状态, 其路径效率并不关键, 故安全状态时使用复杂功能, 备用功能仅用于位于不安全的状态集合内。

RTA 的监视与决策模块系统有 2 个主要功能:

- ① 监视环境状态。一旦 RTA 监视器检测到环境状态有  $\phi_s$  和  $\phi_u$  之间的转换便会激活控制模块。
- ② RTA 的决策模块被激活后按上述规则会移交控制权, 以达到安全且高效的避障效果。

NASA 针对无人机避障功能研发了侦测与躲避 DRP 方法, 运用算法处理机载传感器的数据, 计算出到达安全距离限制的时间间隔, 并与其他飞机维持安全距离, DRP 避障分离规则如图 5 所示。

图 5 中, DRP 避障分离规则由 5 部分组成:

- 1) 保持最小距离。始终保持与其他航空器或障碍的最小横向与垂直距离。
- 2) 遵守 TCAS/RA。如果飞机不能达到规定的 RA 所规定的垂直或水平速度, 则使其固定为预设最大允许的安全速度。
- 3) 遵循航行优先权。遵循既定的空中航行优先权约束。
- 4) 躲避入侵航空器。根据入侵航空器动态行为规划避障路径。
- 5) 保持净空 (Well-Clear)。航线应与其他障碍

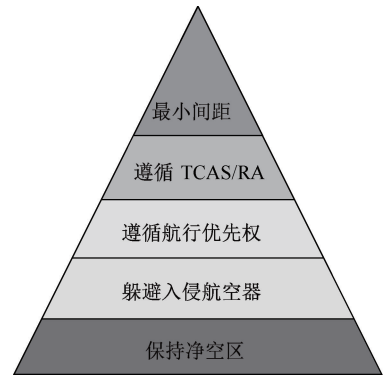


图 5 DRP 避障分离规则

Fig. 5 Notional DRP hierarchical constraints

或航空器保持良好的横向和垂直距离。

基于以上分类, 采用最关键的最小分离间距和保持净空体积规则设计 eVTOL 避障功能切换逻辑。eVTOL 距离分层设计如图 6 所示。当 eVTOL 运行域在保持净空体积外, 此时状态为  $\phi_s$ , 系统使用复杂功能控制动作输出。当 RTA 监视器检测到 eVTOL 在保持净空体积及以内出现障碍物, 此时, 由  $R_2$  定义的圆柱范数小于 1 时, 发生从  $\phi_s$  到  $\phi_u$  的状态转变。特别地, 若障碍物与 eVTOL 的距离小于  $R_1$ , 此时不能保持最小安全距离, eVTOL 处于极度危险的状态, 记为  $\phi_u^*$ , 有  $\phi_u^* \subset \phi_u$ 。当  $\phi \in \phi_u$  时, 为降低 SOTIF 危险, 将控制权移交给备用功能, 备用功能调整航向以降低风险。同时, RTA 的监视器不断计算障碍物与 eVTOL 的距离, 直至由  $R_2$  规定的圆柱范数再次大于 1, 即复杂功能规划的航迹不再位于  $\phi_u$  状态内, 视为脱离安全限制状态, RTA 监视器将控制权交还给复杂功能以保障运行效率。

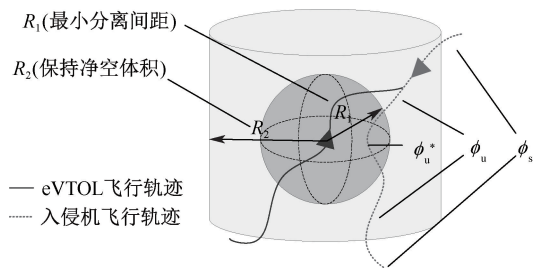


图 6 eVTOL 距离分层设计

Fig. 6 eVTOL distance layering design

根据 eVTOL 所处状态  $\phi$  作为划分依据, 结合文献 [13] 和 DRP 避障分离规则进行场景划分, 将 DRP 避障分离规则对应到 SOTIF 划分的 4 类场景中, 结果见表 2。

表2 基于DRP的SOTIF场景划分

Table 2 SOTIF scenario classification using DRP

SOTIF 场景	DRP 类型	运行状态
已知安全	$\phi \in \phi_s$	安全
已知不安全	$\phi \in \phi_u^*$	非常危险
未知安全	$\phi \in \phi_u$ 且 $\phi \notin \phi_u^*$	危险
未知不安全	$\phi \in \phi_u$ 且 $\phi \notin \phi_u^*$	

### 3 实例验证

设计基于UAM的三维复杂场景,开展eVTOL避障系统算法的训练、测试和有效性分析。仿真基于Windows 10与Python 3.8的软件环境运行,深度强化学习试验参数见表3。

表3 深度强化学习试验参数

Table 3 Parameters for deep reinforcement learning

参数	数值
熵正则化系数 $\alpha$	0.2
训练批次大小	128
经验池大小	$10^6$
探索函数	随机动作

为验证仅使用传统强化学习能否应对SOTIF要求,设计了既包含静态障碍物、又在正常运行过程中遇到突发障碍物的复杂场景。在选取的试验场景中,以eVTOL为中心,标定最小安全距离和保持净空区。保持净空体积的半径设置为30m,高度为30m;最小分离体积半径为15m。场景中的静态障碍物构成主要为城市中禁飞区和高层静态障碍物,使用圆柱体近似。以1表示禁飞区,2表示高层静态障碍物突发动态障碍物来源于其他eVTOL,该突发障碍物出现在eVTOL的预定航路中。记录eVTOL起终点与运行状态,见表4。

表4 eVTOL运行参数与状态

Table 4 eVTOL operating parameters and status

编号	起点	终点	状态
1	(330,0,225)	(0,225,225)	已知安全
2	(330,0,105)	(0,225,180)	未知安全/ 未知不安全
3	(330,75,225)	(0,75,75)	已知安全
4	(330,75,105)	(0,75,180)	已知安全
5	(330,105,75)	(0,0,225)	已知安全
6	(330,225,225)	(0,0,75)	已知安全
7	(330,225,75)	(0,0,225)	已知安全
8	(330,225,180)	(0,0,180)	已知安全

多次运行仿真的避障效果如图7所示。从图7可以看出,eVTOL在动静态障碍物并存的情况下仍

可以保持良好的避障能力,满足SOTIF,仅在第2次仿真中不能保持净空,出现SOTIF危险的情况。该场景下,eVTOL和动态障碍物恰好在相近高度汇流,同时还需要避开静态障碍物,RTA的监控器实时检查智能避障系统的输出,发现智能避障系统不能完全保证SOTIF的要求,出现距静态障碍物2过近的情况,此时,eVTOL处于未知安全/未知不安全的状态,存在SOTIF危险。

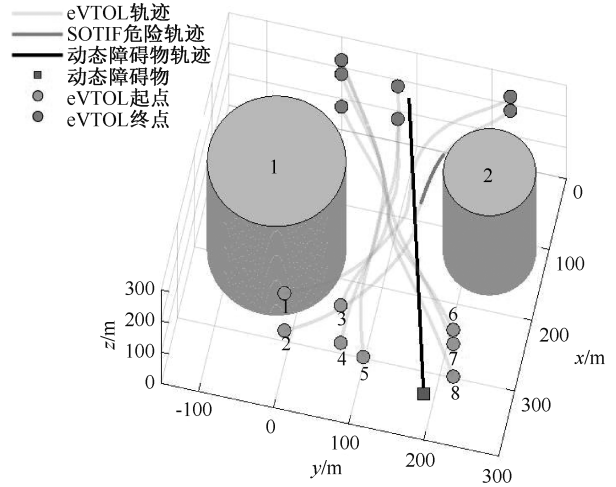


图7 eVTOL多次仿真动静态避障

Fig. 7 eVTOL simulations for dynamic and static obstacle avoidance

针对出现SOTIF危险的第2次仿真进行详细分析,仅使用传统强化学习的避障航迹如图8所示。由图8a和图8c可以看出,第2次仿真中,仅使用人工势场法改进的SAC算法,eVTOL可以根据障碍物所在位置计算引力场和斥力场大小,同时避让静态障碍物和动态突发障碍物,自主规划航路,并到达终点;从图8b可以看出,行驶过程中出现eVTOL不能保持水平方向的安全距离的时刻,不能满足保持净空的要求。

第2次仿真过程的eVTOL高度变化如图9a所示。eVTOL在水平和垂直方向上都满足避开动态障碍物的需求,并且到达终点。但是,在避让突发障碍物的过程中,eVTOL向右行驶,经计算距离后发现,虽然在水平方向上与突发动态障碍物相遇时,eVTOL高度高于突发障碍物,避免了碰撞,但与静态障碍物2距离过近(图9b),在A、B点之间的时刻会出现同时避让多个障碍物时不能保持净空体积的状态,这使eVTOL处于危险的状态。尽管在设计时可以满足规划航路的需要,但是,在应对复杂场景时,即使功能未发生故障,仍会出现由于性能缺陷而导致的危害,应该对强化学习的运行域加以限制。

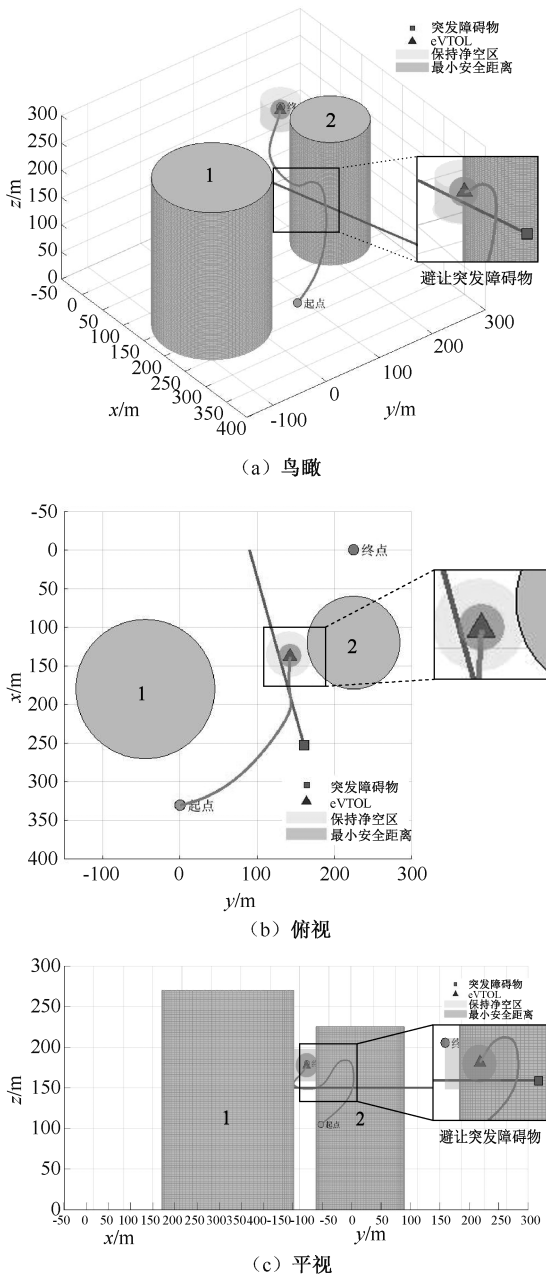
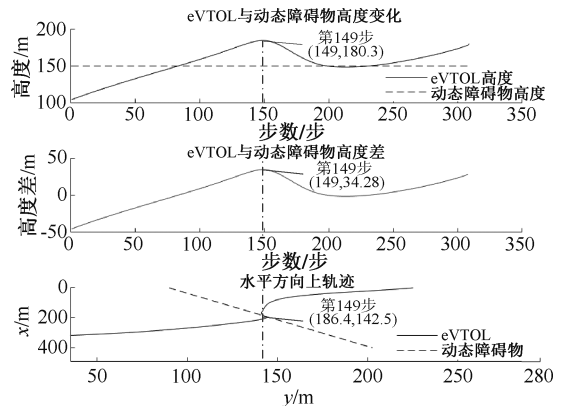
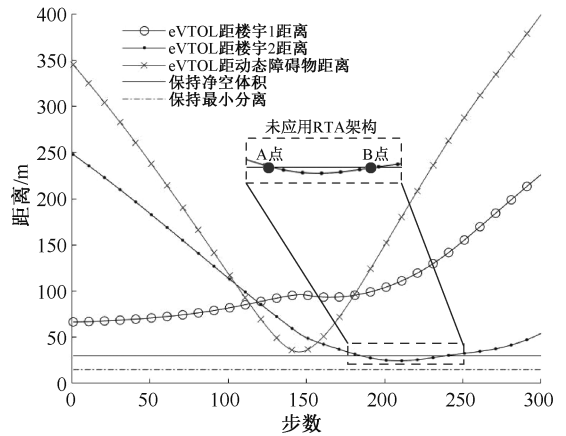


图 8 基于传统强化学习的 eVTOL 避障航迹  
Fig. 8 eVTOL obstacle avoidance trajectory based on traditional reinforcement learning

由于强化学习进行路径规划的过程完全基于数据驱动,过于依赖于奖励函数的设置,本身不具备风险量化的功能,并不会完全遵循保持净空区的安全准则,因此,需要进行相应功能拓展,以降低非故障风险。从 SOTIF 的角度出发,使用 RTA 方法解决此类由于功能不足导致的不合理风险,以应对复杂场景下的智能航电系统的性能局限和规范不足,仿真结果如图 10 所示。在 A 点,RTA 监视器检测到 eVTOL 的飞行状态脱离了规定的安全运行域  $\phi_s$ ,控制权随之移交给备用功能。备用功能 DRP 通过不



(a) eVTOL 高度变化



(b) 距不同障碍物的距离度量

图 9 eVTOL 距不同障碍物距离及高度变化

Fig. 9 eVTOL distance and height changes from different obstacles

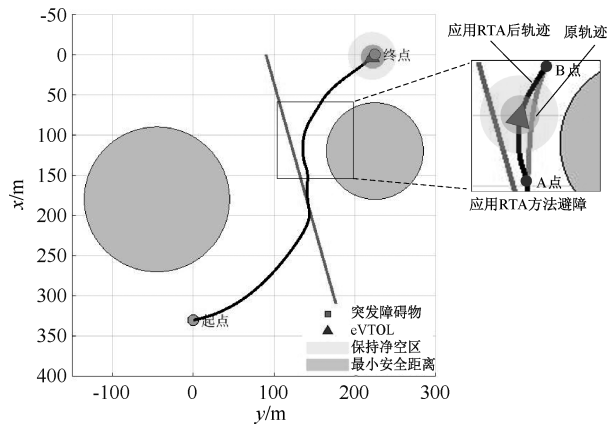


图 10 基于 RTA 方法的 eVTOL 避障路径规划  
Fig. 10 eVTOL obstacle avoidance path planning based on RTA

断计算与障碍物之间的距离,修正目前的航向,引导 eVTOL 回到安全运行域  $\phi_s$ 。在 B 点,RTA 监视器检测到 eVTOL 脱离碰撞风险,控制权再次交还给复杂功能以保障运行性能,算法性能对比见表 5。

由表 5 可以看出,在多障碍物的 UAM 复杂场景

表5 算法性能比对

Table 5 Algorithm performance comparison

方法	航路长度/m	安全时长占比/%
仅使用强化学习	324.98	98.15
RTA 避障	328.08	78.4

下,配备 RTA 功能的 eVTOL 避障功能的鲁棒性、逻辑完备性得到增强。在不使用 RTA 进行避障时,航路长度为 324.98 m,应用 RTA 方法后,航路长度为 328.08 m,总行程增加 0.95%,在复杂环境中安全时长占比为 98.15%,远高于仅使用传统强化学习的 78.4%,使用 RTA 后有效支持了城市空中交通场景

下的 eVTOL 安全避障。

## 4 结论

1) 相较于传统避障系统,RTA 可以通过改善系统功能和限制运行设计域的方式,在保证效率的同时,降低在运行场景中的运行风险,实现在复杂场景中的避障,安全时长占比由 78.4% 提高到 98.15%,保障 SOTIF 安全。

2) RTA 能够降低包含人工智能技术的航电系统的验证难度,修正智能化系统可能带来的潜在风险,提高智能化航电系统的安全性和适航置信度。

## 参考文献

- [1] MENOVAR H, GUVENC I, AKKAYA K, et al. UAV-enabled intelligent transportation systems for the smart city: applications and challenges[J]. IEEE Communications Magazine, 2017, 55(3): 22-28.
- [2] 李诚龙, 屈文秋, 李彦冬, 等. 面向 eVTOL 航空器的城市空中运输交通管理综述[J]. 交通运输工程学报, 2020, 20(4): 35-54.
- [3] LI Chenglong, QU Wenqiu, LI Yandong, et al. Overview of traffic management of urban air mobility (UAM) with eVTOL aircraft[J]. Journal of Traffic and Transportation Engineering, 2020, 20(4): 35-54.
- [4] 绿色航空制造业发展纲要(2023—2035 年)[EB/OL]. (2023-10-10). [https://www.gov.cn/zhengce/zhengceku/202310/content\\_6908243.htm](https://www.gov.cn/zhengce/zhengceku/202310/content_6908243.htm).
- [5] SCHWEIGER A, ANNIGHOFER B, REICH M, et al. Classification for avionics capabilities enabled by artificial intelligence[C]. 2021 IEEE/AIAA 40<sup>th</sup> Digital Avionics Systems Conference (DASC), 2021: 1-10.
- [6] DEY S, LEE S W. Multilayered review of safety approaches for machine learning-based systems in the days of AI[J]. Journal of Systems and Software, 2021, 176: DOI:10.1016/j.jss.2021.110941.
- [7] 董磊, 刘嘉琛, 陈曦, 等. 面向适航符合性的智能航电系统认证研究进展[J]. 航空工程进展, 2023, 14(3): 26-40.
- [8] DONG Lei, LIU Jiachen, CHEN Xi, et al. Research progress of AI-based avionics system certification for airworthiness compliance[J]. Advances in Aeronautical Science and Engineering, 2023, 14(3): 26-40.
- [9] HE Yuning, SCHUMANN J, YU Huafeng. Toward runtime assurance of complex systems with AI components[C]. PHM Society European Conference, 2022: 166-174.
- [10] EASA. Concepts of design assurance for neural networks (CoDANN) II[R], 2021.
- [11] SCHIRMER S, TORENS C, DAUER J C, et al. A hierarchy of monitoring properties for autonomous systems[C]. AIAA SCITECH 2023 Forum, 2023: 2 588-2 601.
- [12] COFER D, AMUNDSON I, SATTIGERI R, et al. Run-time assurance for learning-based aircraft taxiing[C]. 2020 AIAA/IEEE 39<sup>th</sup> Digital Avionics Systems Conference (DASC), 2020: 1-9.
- [13] GHORI S, KHAMVILAI T, FERON E, et al. Runtime assurance for distributed avionics architecture[C]. 2022 IEEE/AIAA 41<sup>st</sup> Digital Avionics Systems Conference (DASC), 2022: 1-6.
- [14] KIRKENDOLL Z. Automatic ground collision avoidance and loss of control prevention systems for general aviation using run-time assurance[C]. 2022 IEEE/AIAA 41<sup>st</sup> Digital Avionics Systems Conference (DASC), 2022: 1-10.
- [15] ISO/PAS 21448-2019. Safety of the intended functionality[S].
- [16] 罗崎瑞, 张道文, 周华, 等. 面向智能汽车预期功能安全的驾驶场景评价[J]. 中国安全科学学报, 2022, 32(8): 140-145.
- [17] LUO Qirui, ZHANG Daowen, ZHOU Hua, et al. Evaluation on driving scenarios for safety of intended functionality of intelligent vehicles[J]. China Safety Science Journal, 2022, 32(8): 140-145.
- [18] 董隴军, 王加闯. 智能安全人机工程学学科建设及内容体系研究[J]. 中国安全科学学报, 2022, 32(3): 1-8.
- [19] DONG Longjun, WANG Jiachuang. Research on discipline construction and content system of intelligent safety ergonomics[J]. China Safety Science Journal, 2022, 32(3): 1-8.
- [20] HAARNOJA T, ZHOU A, HARTIKAINEN K, et al. Soft actor-critic algorithms and applications[J]. arXiv Preprint, 2018: DOI:10.48550/arXiv.1812.05905.
- [21] COOPER J K, SCHIERMAN J D. A sense and avoid system for unmanned aircraft in formation flight[C]. AIAA Guidance, Navigation, and Control Conference, 2014: 967-986.



作者简介: 董磊 (1983—),男,天津人,博士,副研究员,主要从事民机安全性评估与适航审定技术、未来民机智能飞行与智能系统技术等方面的研究。E-mail:dlcauc@126.com。