http：//myfj. cnjournals. com myfj_sadri@163. com （021）20866796

DOI：10. 19416/j. cnki. 1674-9804. 2023. 04. 023

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

杨海云* 李宜恒 林 波 于莉莉 窦兆起 董 旭 初源梓逸

（零重力（合肥）飞机工业有限公司，南京 210000）

摘 要：近年来，电动垂直起降（electric vertical takeoff and landing，简称 eVTOL）飞行器在城市空运中得到快速发展。eVTOL 被看作是最具发展前景的，可作为城市空中交通运输的有效运载工具。安全性分析是 eVTOL 飞行器运行载人过程中，减少灾难性事故以及保证高可靠性和高安全性的最重要条件。利用功能危害性评估（functional hazard assessment，简称 FHA）可确定 eVTOL 飞行器中潜在的失效状态、预计失效状态以及其他的危险失效状态，从而能够全面找出潜在的灾难性和危险失效状态，进而有针对性地进行控制，最后能够全面降低灾难性事故的发生，以确保 eVTOL 飞行器的安全性。基于 FHA 分析，对 eVTOL 整机的安全性分析，并通过灾难性失效状态得出安全关键功能，为其功能设计提供依据。

关键词：eVTOL；安全性分析；FHA 分析；失效状态；功能设计

中图分类号：V37 **文献标志码**：A **OSID**：

0 引言

发展绿色航空是人类社会形成的基本共识，电动垂直起降（electric vertical takeoff and landing，简称 eVTOL）飞行器为实现绿色航空提供了一条光明的技术途径。eVTOL 飞行器可以充分利用三维空间资源，有效解决城市道路拥堵，极大提高人们的出行效率，为城市交通带来了质的飞跃。同时，eVTOL 飞行器将在城市空中出行、高维货运、应急救援、特色旅游等领域拥有广阔的市场[1-4]。由于 eVTOL 飞行器大部分是要进行载人飞行的，所以对其设计过程中进行安全性分析尤其重要。此外，进行制定安全性分析目标的 FHA 分析是实施安全性分析的第一步。因此，将功能危害性评估方法引入 eVTOL 飞行器的安全性评估中，为其安全性分配及设计提供依据。首先说明了做功能危害性评估（functional hazard assessment，简称 FHA）分析的目的，其次描述了 FHA 分析的基本过程，再次列出了 eVTOL 飞行器的部分重要功能以及飞行任务剖面，最后选取 eVTOL 飞行器某个案例进行了 FHA 分析。

1 FHA 安全性分析方法

FHA 是 eVTOL 飞行器首先要做的安全性分析，它识别危险并为飞行器或系统设定安全性目标。随后，综合飞行器或系统安全性评估将显示设计的飞行器或系统符合 FHA[1] 制定的安全性目标。这使得 FHA[5-6] 对交付飞行器或系统的最终安全性论证至关重要，除非首先识别和评估危害，否则不可能说危害已得到充分缓解。其次，通过初步系统安全性评估（preliminary system safety assessment，简称 PSSA）对 FHA 提出的安全性目标进行初步分配。最后，通过系统安全性评估（system safety assessment，简称 SSA）来验证 FHA 中提出的安全性目标是否已经实现。其中，故障模式影响（failure mode and effects analysis，简称 FMEA）对部件的单一失效进行安全性分析，故障树[7]（fault tree analysis，简称

* **通信作者**. E-mail：yanghaiyun123@nuaa. edu. cn

引用格式：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. YANG H Y，LI Y H，LIN B，et al. Research on eVTOL aircraft based on FHA analysis[J]. Civil Aircraft Design and Research，2023(4)：158-166(in Chinese).

FTA)对部件的组合失效进行安全性分析。

飞机级的 FHA 为 eVTOL 飞行器安全性分析与评估的第一步。将 eVTOL 飞行器视为研究对象,研究在各个飞行阶段内 eVTOL 飞行器设计,归纳出可能影响飞行器安全飞行的飞机级功能失效。通过系统综合地列出飞行器的完整功能,识别功能的失效状态,并根据失效影响的严重程度对其进行分类,从而为新机型设计或改进设计确立安全性要求目标。飞行器级 FHA 是飞行器安全性要求产生和分配的起点,飞行器级 FTA 以飞行器级 FHA 的结果为输入,为系统分配安全性要求。飞行器级 FHA 结果及相关的飞行器级 FTA 或系统级 FHA 的输入,是 PSSA 和 SSA 的基础。

2　eVTOL 飞行器 FHA 分析的基本过程

FHA[7]分析的基本过程,分为以下 7 个步骤:

1) 归纳出飞行器级相关的所有功能,其中包括内部功能和级联相关功能;

2) 列出飞行器功能的所有失效状态(failure condition,简称 FC),其中包括所有的单一和组合失效状态;

3) 相同的失效状态处在不同飞行阶段所产生的影响也是不同的,所以需要确定特定 FC 的飞行阶段;

4) 确定特定 FC 对 eVTOL 飞行器、人员(机组人员包括地面站机组和乘客)及相关地面人员的影响;

5) 确定特定 FC 的危害性等级,根据特定 FC 对飞行器、人员以及相关地面人员的影响程度对其进行危害等级分类;

6) 列出 FC 危害性等级的所有原因;

7) 提出缓解影响的措施。

3　eVTOL 飞行器功能列表

首先建立一个核心功能列表,进行功能分解,以便为识别危险提供一个起点。然后,评估这些危害的潜在后果和相关严重性,再根据严重性和危害源推测缓解措施。进行飞行器级 FHA 首先需要确定飞行器各级别的所有功能,建立功能清单。在进行飞行器级功能定义时,根据 eVTOL 飞行器设计目标与要求,在总体专业所定义的飞行器级功能的基础上,进行确认与完善,确定了各层级的功能,列出部分 eVTOL 飞行器功能清单,见表 1。

航空界(包括 FAA)普遍认为:飞行、导航和通信是飞机的主要功能,其中飞行是最高优先级[8]。这与飞机类型、任务和其他变量(例如自主程度)无关。例如,无论是飞行员控制还是软件控制,首要任务是驾驶飞机。在积极控制下,其他顶级功能是将飞机导航到目的地,并按照规定与空中交通管制(ATC)等机构进行通信,以便维持空域管理。以航空为顶级功能进行功能分解,其下级功能包括控制飞行、控制地面运动和控制子系统,其中控制飞行又包括控制飞行路径、控制空地过渡和传递系统状态,依次进行逐级分解,详细内容如表 1 所示。

表 1　eVTOL 飞行器功能分解列表

1 航空			
1.1	控制飞行		
1.1.1		控制飞行路径	
1.1.1.1			控制高度
1.1.1.2			控制姿态
1.1.1.3			控制速度
1.1.1.4			控制推进
1.1.1.5			稳定性管理
1.1.2		控制空地过渡	
1.1.2.1			控制动力的启动和停止
1.1.2.2			控制起飞到悬停,悬停到着陆

表1(续)

1.1.2.3			收起和放下起落架
1.1.2.4			控制紧急着陆
1.1.2.5			稳定性管理
1.1.3		传递系统状态	
1.2	控制地面运动		
1.2.1		控制地面飞行器	
1.3	控制子系统		
1.3.1		控制动力装置	
1.3.2		飞行器健康监测	
1.3.2.1			维护/保护结构完整性
1.3.2.2			电池健康监测

4 飞行任务剖面

eVTOL 飞行器的飞行任务剖面具体由以下 8 个阶段构成:

1) 爬升到悬停(起飞)。飞行器从起点起飞和着陆区域(take-off and landing area,简称 TOLA)处垂直起飞并达到适合转换的高度。

2) 过渡到前飞。飞行器从依赖垂直升力机构转变为依赖前飞升力机构。

注意:这种转变可能涉及也可能不涉及重新配置,例如旋翼倾斜,具体取决于概念设计。

3) 爬升到巡航。飞行器继续增加高度,直到达到航路飞行的目标高度。

4) 巡航。飞行器在目标高度飞行。

5) 避障。飞行器进行机动飞行,以避免与检测到的碰撞危险冲突。

注意:冲突探测可以依赖于某种程度的自动化,具体取决于概念。在这个试验中,机上飞行员仍然有责任根据 14 CFR 91.113[9] 观察到并避开。

6) 进近。飞行器降低高度,直到达到转换的目标高度。

7) 过渡到悬停。飞行器从依赖向前飞行升力机构过渡到依赖垂直升力机构。

注意:这种转变可能涉及也可能不涉及重新配置,例如旋翼倾斜,具体取决于概念设计。

8) 下降(着陆)。飞行器通过剩余高度垂直下降并降落在目的地 TOLA 的停机坪上。

5 FHA 分析案例

以飞行为顶级功能、控制飞行为二级功能、控制飞行路径为三级功能和控制高度为四级功能进行 FHA 分析[10]。飞行阶段包括爬升到悬停、过渡到前飞、爬升到巡航、巡航、避障、进近、过渡到悬停和下降。确定控制高度功能在不同的飞行阶段的不同 FC 对飞行器、人员以及相关地面人员的影响,通过对影响进行分析,从而确定危害性等级,进而找到原因与提供缓解措施。在功能失效状态中应该根据功能清单逐层分析,做到不重不漏,具体的 FHA 分析如表 2 所示。

表 2 FHA 分析表格

编 号	功 能	飞行阶段	失效状态	危险对飞机、地面远程控制组、乘客和地面人员的影响	危害性分类	影响等级的支撑材料	验证方法
1	飞行						
1.1	控制飞行						
1.1.1	控制飞行路径						

表2(续)

编　号	功　能	飞行阶段	失效状态	危险对飞机、地面远程控制组、乘客和地面人员的影响	危害性分类	影响等级的支撑材料	验证方法
1.1.1.1.1	控制高度	爬升到悬停	非指令上升	飞机:不受控制的上升,可能无法悬停并对飞机产生很大的损害,最终有可能会坠毁 地面控制组:较大地增加了工作负担 乘客:可能由于飞机的损毁而绝大部分或者全部死亡 地面人员:人员伤亡	灾难性的	模拟器试验和分析材料	FMEA FTA CCA
			上升失效	飞机:停留在地面上 地面控制组:增加了工作负担 乘客:无影响 地面人员:无影响	无安全性影响的	飞行试验	无
			非指令下降	飞机:可能导致坠机,飞机损毁 地面控制组:增加了工作负担 乘客:可能由于飞机的坠毁而绝大部分或者全部死亡 地面人员:人员伤亡	灾难性的	模拟器试验和分析材料	FMEA FTA CCA
			与指令上升有微小偏差	飞机:可能没有影响 地面控制组:无影响 乘客:无影响 地面人员:无影响	无安全性影响的	飞行试验	无
		过渡到前飞	不完整/错误的过渡	飞机:可能导致坠机,飞机损毁 地面控制组:增加了工作负担 乘客:可能由于飞机的坠毁而绝大部分或者全部死亡 地面人员:人员伤亡	灾难性的	模拟器试验和分析材料	FMEA FTA CCA
			非指令上升/下降	飞机:可能导致坠机,飞机损毁 地面控制组:增加了工作负担 乘客:可能由于飞机的坠毁而绝大部分或者全部死亡 地面人员:人员伤亡	灾难性的	模拟器试验和分析材料	FMEA FTA CCA
			与指令上升/下降有微小偏差	飞机:可能没有影响 地面控制组:无影响 乘客:无影响 地面人员:无影响	无安全性影响的	飞行试验	无

表2(续)

编号	功能	飞行阶段	失效状态	危险对飞机、地面远程控制组、乘客和地面人员的影响	危害性分类	影响等级的支撑材料	验证方法
1.1.1.1	控制高度	爬升到巡航	非指令上升	飞机:飞机一直爬升,无法巡航 地面控制组:增加工作负担 乘客:无影响 地面人员:无影响	较轻微的	飞行试验	FMEA
			上升失效	飞机:无法爬升,飞机可能重着陆 地面控制组:增加了工作负担 乘客:可能会有受伤 地面人员:可能有伤亡	危险的	模拟器试验和分析材料	FMEA FTA CCA
			非指令下降	飞机:无法爬升,飞机可能重着陆 地面控制组:增加了工作负担 乘客:可能会有受伤 地面人员:可能有伤亡	危险的	模拟器试验和分析材料	FMEA FTA CCA
			与指令上升有微小偏差	飞机:可能没有影响 地面控制组:无影响 乘客:无影响 地面人员:无影响	无安全性影响的	飞行试验	无
		巡航	上升/下降失效	飞机:飞机无法保持高度,在一定程度上失去控制 地面控制组:增加了工作负担 乘客:心里不舒服 地面人员:造成一定的危险	较重大的	模拟器试验	FMEA FTA
			非指令下降	飞机:无法爬升,飞机可能重着陆 地面控制组:增加了工作负担 乘客:可能会有受伤 地面人员:可能有伤亡	危险的	模拟器试验和分析材料	FMEA FTA CCA
			非指令的上升	飞机:飞机无法保持高度,在一定程度上失去控制 地面控制组:增加了工作负担 乘客:心里不舒服 地面人员:造成一定的危险	较重大的	模拟器试验	FMEA FTA
			与指令上升/下降有微小偏差	飞机:可能没有影响 地面控制组:无影响 乘客:无影响 地面人员:无影响	无安全性影响的	飞行试验	无

表2(续)

编　号　功　能	飞行阶段	失效状态	危险对飞机、地面远程控制组、乘客和地面人员的影响	危害性分类	影响等级的支撑材料	验证方法
1.1.1.1　控制高度	避障	上升/下降失效	飞机:飞机失去自动控制 地面控制组:增加了工作负担 乘客:可能会有受伤 地面人员:可能有伤亡	危险的	模拟器试验和分析材料	FMEA FTA CCA
		非指令上升/下降	飞机:飞机失去自动控制 地面控制组:增加了工作负担 乘客:可能会有受伤 地面人员:可能有伤亡	危险的	模拟器试验和分析材料	FMEA FTA CCA
		与指令上升/下降有微小偏差	飞机:可能没有影响 地面控制组:无影响 乘客:无影响 地面人员:无影响	无安全性影响的	飞行试验	无
	进近	上升失效	飞机:飞机无法复飞 地面控制组:增加了工作负担 乘客:心里不舒服 地面人员:造成一定的危险	较重大的	模拟器试验	FMEA FTA
		下降失效	飞机:飞机失去自动控制 地面控制组:增加了工作负担 乘客:可能会有受伤 地面人员:可能有伤亡	危险的	模拟器试验和分析材料	FMEA FTA CCA
		非指令上升/下降	飞机:可能导致坠机,飞机损毁 地面控制组:增加了工作负担 乘客:可能由于飞机的坠毁而绝大部分或者全部死亡 地面人员:人员伤亡	灾难性的	模拟器试验和分析材料	FMEA FTA CCA
		与指令上升/下降有微小偏差	飞机:可能没有影响 地面控制组:无影响 乘客:无影响 地面人员:无影响	无安全性影响的	飞行试验	无
	过渡到悬停	非指令上升/下降, 上升/下降失效, 不完整/错误过渡	飞机:可能导致坠机,飞机损毁 地面控制组:增加了工作负担 乘客:可能由于飞机的坠毁而绝大部分或者全部死亡 地面人员:人员伤亡	灾难性的	模拟器试验和分析材料	FMEA FTA CCA

表2(续)

编号 功能	飞行阶段	失效状态	危险对飞机、地面远程控制组、乘客和地面人员的影响	危害性分类	影响等级的支撑材料	验证方法
1.1.1.1 控制高度	过渡到悬停	与指令上升/下降有微小偏差	飞机:可能没有影响 地面控制组:无影响 乘客:无影响 地面人员:无影响	无安全性影响的	飞行试验	无
	下降	上升失效	飞机:可能导致坠机,飞机损毁 地面控制组:增加了工作负担 乘客:可能由于飞机的坠毁而绝大部分或者全部死亡 地面人员:人员伤亡	灾难性的	模拟器试验和分析材料	FMEA FTA CCA
		下降失效 1	飞机:飞机失去自动控制 地面控制组:增加了工作负担 乘客:可能会有受伤 地面人员:可能有伤亡	危险的	模拟器试验和分析材料	FMEA FTA CCA
		非指令上升	飞机:飞机失去自动控制 地面控制组:增加了工作负担 乘客:可能会有受伤 地面人员:可能有伤亡	危险的	模拟器试验和分析材料	FMEA FTA CCA
		非指令下降	飞机:可能导致坠机,飞机损毁 地面控制组:增加了工作负担 乘客:可能由于飞机的坠毁而绝大部分或者全部死亡 地面人员:人员伤亡	灾难性的	模拟器试验和分析材料	FMEA FTA CCA
		与下降命令有微小偏差	飞机:飞机在一定程度上失去控制 地面控制组:增加了工作负担 乘客:心里不舒服 地面人员:造成一定的危险	较重大的	模拟器试验	FMEA FTA
		下降失效 2	飞机:飞机无法自动下降着陆 地面控制组:增加工作负担 乘客:无影响 地面人员:无影响	轻微的	飞行试验	FMEA

参照 AC 23.1309[11]系统的安全性分析和评估条款选择安全性验证方法,其中验证方法为失效模式与影响分析(failure mode and effects analysis,简称 FMEA)、故障树分析(fault tree analysis,简称 FTA)和共因分析(common cause analysis,简称 CCA)。关于验证方法的详细信息,可参照文献[7]和[11]。

从以上 FHA 表中可以清晰地看到,在过渡到前飞阶段控制高度功能的不完整或错误的过渡存在灾难性危害。控制高度功能在其他飞行阶段的其他失效状态同样存在多个灾难性危害等级,如表中标红的全都是灾难性危害。因此,控制高度应根据不同飞行阶段实现其相关功能的不同类型设计。在研制保证等级分配中应首先保证灾难性危害等级功能的实现,并优先保证其缓解措施正确实施。

最后,通过其他安全性分析方法如 FMEA 和 FTA 等对实现控制高度功能的组件和设备进行分析,来验证 FHA 分析确定的安全性目标是否达到。

6　结论

近几年来,我国政府出台了多项政策以促进低空飞行的发展。作为低空飞行的重要组成部分,eVTOL 飞行器在技术及规模上得到了很大的发展。本文对 FHA 安全性分析方法进行了研究,其对 eVTOL 飞行器的安全性分析起到的作用如下:

1) FHA 分析为 eVTOL 飞行器的功能定义、功能失效状态分析和确定功能失效影响等级提供了思路和方法。

2) 通过 FHA 分析确定 eVTOL 飞行器中安全关键系统,为研制保证分配提供了输入。

3) 通过 FHA 分析确定 eVTOL 飞行器中影响等级高的功能失效状态,为其 PSSA 分析提供输入。

本文将 FHA 分析用在 eVTOL 飞行器的功能设计中,并得出了 eVTOL 飞行器的安全关键功能,为其安全性分配及设计提供依据。

参考文献:

[1] 李开省. 电动飞机核心技术研究综述[J]. 航空科学技术, 2019, 30(11):8-17.

[2] 黄俊, 杨凤田. 新能源电动飞机发展与挑战[J]. 航空学报,2016, 37(1): 57-68.

[3] 李凯, 陆崑, 吴沂宁,等. eVTOL 飞行器适航取证路径研究[J]. 航空维修与工程, 2022(9):43-45.

[4] 杜伟, 孙娜. 电动垂直起降飞行器的发展现状研究[J]. 航空科学技术, 2021, 32(11):1-7.

[5] SAE International. Guidelines for development of civil aircraft and system: SAE ARP4754A [S]. U.S.: SAE,2010.

[6] 王晓梅, 龚孝懿, 李棋. 民用飞机电传飞控系统功能危害性评估方法研究[J]. 民用飞机设计与研究, 2017(4):35-41.

[7] SAE International. Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment: SAE APR4761[S]. U.S.: The Engineering Society for Advancing Mobility Land Sea Air and Space,1996.

[8] FAA Aviation Safety. Fly the aircraft first[EB/OL]. (2018-07)[2023-09-11]. https://www.faa.gov/sites/faa.gov/files/2022-01/Fly% 20the% 20Aircraft% 20First.pdf.

[9] Code of Federal Regulations. Right of way rules: except water operations: Title 14 Part 91.113[S/OL]. [S.l.: s.n.], 2019. [2023-09-11]. https://www.faraim.org/faa/far/cfr/title-14/part-91/section-91.113/index.html.

[10] WASSON K, NEOGI N, GRAYDON M, et al. Functional hazard assessment for the eVTOL aircraft supporting urban air mobility (UAM) applications: exploratory demonstrations: NASA/TM-20210024234 [R/OL]. [2023-09-09]. https://ntrs.nasa.gov/api/citations/20210024234/downloads/NASA-TM-20210024234.pdf.

[11] U.S. Department of Transportation. Federal Aviation Administration. System safety analysis and assessment for Part 23 airplanes: AC 23.1309-1E[S/OL]. [2023-09-09]. https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_23_1309-1E.pdf.

作者简介

杨海云　女,博士。主要研究方向:eVTOL 飞行器的安全性和适航性的研究以及综合模块化航空电子系统的安全性分析研究。E-mail:yanghaiyun123@nuaa.edu.cn

李宜恒　男,硕士。主要研究方向:旋翼类飞行器总体设计。E-mail:liyiheng@lzlair.com

林　波　男,本科。主要研究方向:eVTOL 飞行器复合材料结构设计及强度验证。mail:linbolzlair.com

于莉莉　女,本科。主要研究方向:设计及质量保证。E-mail:yulili@lzlair.com

窦兆起　男,本科。主要研究方向:eVTOL 飞行器的产业链发展现状及难点研究。E-mail:douzhaoqi@lzlair.com

董　旭　男,本科。主要研究方向:eVTOL 飞行器结构设计和相关试验平台结构设计。E-mail:dongxu@lzlair.com

初源梓逸　女,本科。主要研究方向:飞行器结构设计。E-mail:chuyuanziyi@lzlair.com

Research on eVTOL aircraft based on FHA analysis

YANG Haiyun * LI Yiheng LIN Bo YU Lili DOU Zhaoqi DONG Xu CHUYUAN Ziyi

(Zero Gravity Aircraft Industry (Hefei) Co., Ltd, Nanjing 210000, China)

Abstract: In recent years, electric vertical takeoff and landing (eVTOL) aircraft has developed rapidly in urban air transportation. eVTOL is taken as the most promising and effective transportation vehicle in market. Safety analysis is the most important condition for reducing catastrophic accidents and ensuring high reliability and high safety during the manned operation of eVTOL. Using functional hazard assessment (FHA) analysis can determine potential failure conditions, expected failure conditions and other hazardous failure conditions in eVTOL, so that potential catastrophic and hazardous failure conditions can be fully identified, and then targeted controlling can finally reduce the occurrence of catastrophic accidents in an all-round way to ensure the safety of eVTOL. Based on the FHA analysis, this paper analyzes the safety of the eVTOL level, and obtains the safety-critical functions through the catastrophic failure conditions, providing a basis for its function design.

Keywords: electric vertical takeoff and landing (eVTOL); safety analysis; functional hazard assessment (FHA) analysis; failure conditions; function design

* Corresponding author. E-mail: yanghaiyun123@nuaa.edu.cn