

配电系统安全性分析技术研究¹

李阳阳* 姚磊 周俊童²

(天津航空机电有限公司研发中心,天津市 300308)³

摘要:为了保证配电系统的安全可靠,结合SAE ARP4761针对配电系统的特点对评估流程和方法作适应性改进,包括功能危害性分析(FHA)、初步安全性分析(PSSA)、安全性分析(SSA)、共模分析(CMA)。同时提出了安全性分析与系统研制流程的融合关系,提出了配电系统安全性分析与零组件安全性分析的衔接方法,为配电系统安全性分析提供了指导。在故障树分析分配中采用了基于模型的分析方式,可减少故障树分析造成的工作量,便于安全性分析在系统研发中的应用。

关键词:配电系统;安全性;故障树;共模分析⁵

中图分类号:V242.4⁶

文献标识码:⁷

0 引言⁸

飞机配电系统是实现电能到用电设备输送、分配和控制保护的系统,它由馈电电缆、汇流条、配电板以及配电器件等组成。目前,飞机正朝着多电化和全电化的方向发展,机载电气电子设备的数量急剧增加,飞机供配电系统正变得日趋庞大和复杂,飞机供配电系统的可靠运行是关系飞机飞行安全的关键因素^[1-3]。在飞机配电网络的设计阶段,需要对供配电系统进行可靠性分析和预测,寻找系统设计中的薄弱环节,优化供配电系统的设计方案,从而大幅降低后期出现问题时因更改设计而产生的时间和金钱成本。因此,开展对大型飞机供配电系统安全性评估的研究非常重要。

经过长期发展,美国已形成了针对民用运输机的系统安全性设计、分析预评估的理论体系。该体系由功能危害性分析(functional hazard analysis, FHA)、初步系统安全性分析(preliminary system safety assessment, PSSA)、系统安全性分析(system safety assessment, SSA)以及共因分析(common

cause analysis, CCA)四大部分组成,形成了完整的¹¹指导文件体系,如SAE ARP4761、SAE ARP4754、DO-178B、DO-254等^[4-5]。国内多采用故障树分析法(fault tree analysis, FTA)对飞机配电系统进行安全性评估^[6-8]。但是国内外关于飞机配电系统安全性分析技术研究的公开发表文献较少,无法有效指导配电系统进行安全性分析。

当配电网比较庞大和复杂时,传统的安全性¹²分析方法是采用故障树分析法对网络系统进行建模和分析。然而,这种方法工作量较大,需要根据网络系统的具体特点进行针对性的分析方法研究。系统的复杂性导致了分析工作的繁重,进而使得安全性评估的进度滞后于系统研发的进度^[9]。

文献[10]将一种基于Petri网的故障树分析法¹³运用于飞机配电系统的可靠性分析中,这种方法有效地简化了传统飞机配电系统可靠性分析方法的复杂性,减少了计算量,从而弥补了传统故障树分析法的不足。近年来,欧洲和美国兴起了一种基于模型的形式化安全性分析和评估方法,这种方法旨在提高安全性分析的效率,减少误差,其一大优势

收稿日期: 2024-02-25

* 通信作者. E-mail:whyyzfn@163.com

引用格式: 李阳阳,姚磊,周俊童. 配电系统安全性分析技术研究[J]. 民用飞机设计与研究,2025(4):74-79. LI Y Y, YAO L, ZHOU J T. Research on safety design technology for power distribution system [J]. Civil Aircraft Design & Research, 2025(4):74-79(in Chinese).

就是能对目标系统进行自动化分析和结果生成^[1]¹。然而,由于其算法的复杂性,这种方法在实际工程应用中并不适用。

因此,本文结合SAE ARP4761标准,针对配电系统的²特点对评估流程和方法作适应性改进,为配电系统安全性分析提供了指导。同时,该方法采用故障树模型的方式,可减少传统故障树分析造成的巨

大工作量,便于安全性分析在系统研发中的应用^[3]³。

1 功能危害性分析⁴

根据电源系统的功能清单,分析配电系统的⁵功能,经分析与配电系统相关的飞机级功能主要为:提供电源、提供电源状态信息、告警信息等,根据飞机级功能分解为配电系统功能清单,如表1所示。

表1 配电系统功能清单(以提供电源为例)⁶

序号	相关飞机级功能要求	功能编号	配电系统功能	功能描述	7
1	提供电源	F-24-07	一次直流配电	向全机直流用电设备提供合适的电能	
2		F-24-08	一次交流配电	向全机交流用电设备提供合适的电能	
3		F-24-09	应急直流供电	对蓄电池及用电负载进行过流保护、超温警示	
4		F-24-10	交流外电源供电	对外部电源提供电接口 针对交流外部电源,应具有过压、电压、过频、欠频和反相序保护	
5		F-24-11	直流外电源供电	对外部电源提供电接口 针对直流外部电源,应具有过压、欠压和反极性保护	

根据飞机级分配的安全性指标、配电系统的⁸基本架构,考虑飞机和电源系统各种可预期的环境条件和运行条件,同时考虑了功能失效的形式,包括全部丧失、部分丧失、功能失调等,最终确定了配电

系统的失效状态清单,表2为部分示例。通过FHA⁹分析共识别出灾难级失效状态4项、危险级功能故障7项、较大的失效状态13项、较小的功能故障2项。

表2 配电系统失效状态示例¹⁰

功能及编号	失效状态	飞行阶段	失效状态编号	失效状态对其他系统的影响	失效状态对飞机、机组及乘客的影响	影响等级	支撑材料	验证方法	11
F-24-07	左正常通电失效	一次直道直流供电	T/F/L FC-24-07-A1	机上部分重要和正常直流、部分交流用电系统和设备无法工作	a)部分用电设备不工作,显著地降低飞机运行能力或安全裕度 b)显著地增加机组工作负担 c)无	III	工程经验 and effects analysis, FMEA)	失效模式及影响分析(failure mode and effects analysis, FMEA)	
F-24-07	左应急通道和右正常通电丧失	一次直道直流供电	T/F/L FC-24-07-A6	机上部分重要直流用电系统和设备无法工作	a)机上部分重要直流用电设备不工作,极大地降低飞机运行能力或安全裕度 b)极大地增加机组工作负担和心理压力 c)个别乘员受到严重伤害甚至死亡	I	工程经验	FTA FMEA CCA	
								

2 初步系统安全性分析¹²

在系统研制过程中,将安全性需求纳入系统¹³需求的范畴,随后进行系统架构设计。系统的初步架构设计(图1)完成后,紧接着进行初步的系统

安全性分析。这一流程确保了安全性需求从项目¹⁴初期就被纳入考量,并贯穿整个系统设计和开发过程。

对FHA分析中识别出的安全性需求进行分析¹⁵后,需开展配电系统安全性设计/架构决策。以“左

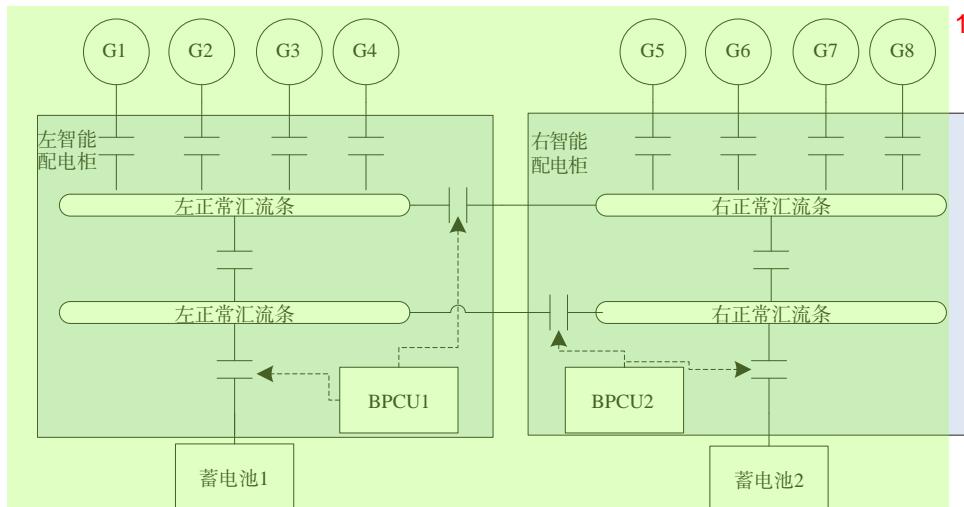


图 1 系统初步架构图

应急通道和右正常通道直流供电丧失”为例阐述架构决策过程如下：

1) 左应急通道和右正常通道直流供电丧失会导致部分关键设备失电，影响等级为灾难级（I）。

2) 左应急通道和右正常通道直流供电丧失，可能由丧失直流发电机引起，也可能由一次配电系统失效引起。

3) 配电系统中，由一次配电系统接收来自直流发电机及蓄电池的电功率，并分配至了左中央、左应急、右中央、右应急汇流条，左应急和右正常通道分别位于左智能配电柜、右智能配电柜 2 个配电盘中，互相之间独立安装，并且汇流条间均设有接触器及熔断器，防止单个汇流条的故障蔓延至多个供电通道。

4) 左右智能配电柜汇流条间接触器受驾驶舱控制板开关的控制，左右智能配电柜的一次配电系统由两台 BPCU 进行控制。控制开关是简单硬件设备，汇流条电源控制组件 (bus power control unit, BPCU) 基于软件和复杂硬件实现。将 BPCU 的设计保证等级 (design assurance level, DAL) 分配为 B，将“控制开关”的 DAL 分配为 B，实际中开关作为简单硬件按照 DAL A 开发。

2.1 失效状态评估

选取配电系统的失效状态清单中定义失效状态作为顶事件。以 SAE ARP4761 为指南，采用了基于模型的故障树分析方法，本文以“左正常供电丧失”为例创建了如图 2 所示的故障树。故障树分析中应用的源数据，主要来源于配电系统故障模式

库。经分析能够满足 FHA 中确定的安全性指标要求。计算 I、II 类失效状态的一阶最小割集，识别是否有单点故障。若有单点故障，通过改进设计将该故障消除。以左应急通道和右正常通道直流供电丧失为例，该故障树无 I 阶最小割集，故无单点故障。

2.2 组件级安全性指标确定

根据 PSSA 故障树，对零组件安全性指标进行分配，分配的过程如下：

1) 将顶事件故障率设置为 FHA 中的要求值，分配值为 $1 \times 10^{-5}/FH$ ，故障率分配采用模型的故障率分配功能。故障率采用平均分配的方式，若实际故障率不满足要求，需重新分配，可把特定事件的故障率设置为固定分配值，重新分配。经迭代，分配概率均小于发生概率。故障率必须达到故障树分析中规定的故障率，任何不能满足给定值的事件必须得到系统设计的支持。

2) 对于 I、II 阶最小割集、隐蔽故障 (如应急转换开关故障、左右并联开关故障) 应重点关注。隐蔽故障需要对安全性维护需求提出要求。

经分配得出的零组件安全性指标见表 3。

根据上述对组件的功能及故障树分析，确定配电系统组件 (软/硬件) 的项目研制保证等级 (item development assurance level, IDAL) 见表 4。

3 共模分析

共因分析包括共模分析 (common mode analysis, CMA)、区域安全分析 (zonal safety analysis, ZSA)

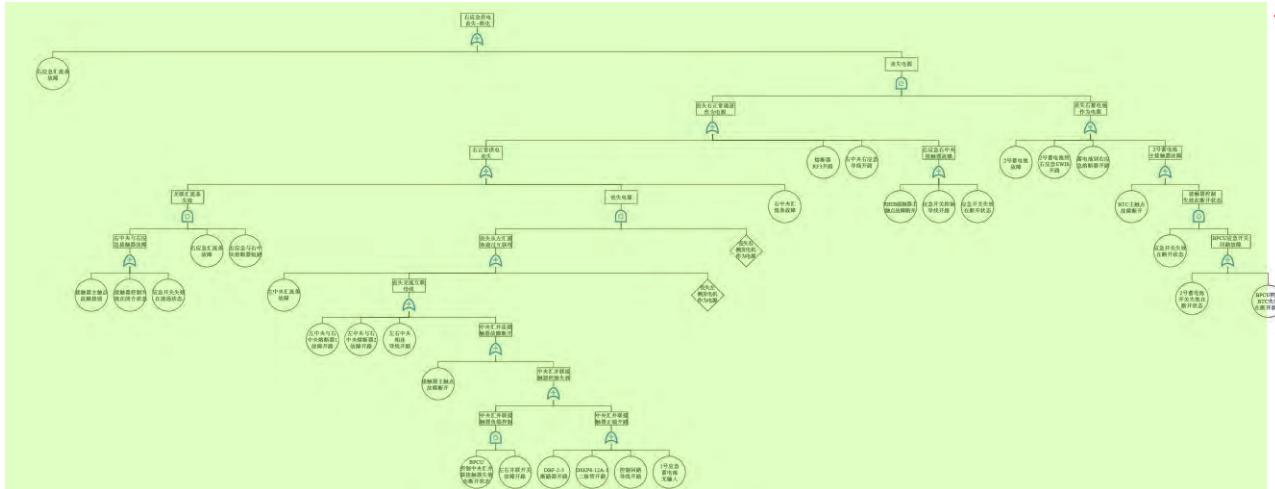


图2 “左正常供电丧失”故障树

表3 零组件安全性指标

序号	组件名称	节点名称	每小时故障率 λ	暴露时间t/h	来源	4
1	配电柜	左中央汇流条故障	3.33×10^{-6}	3	左正常供电丧失	
2	配电柜	熔断器1故障开路	3.75×10^{-6}	3	左正常供电丧失	
3	BPCU	BPCU控制连接接触器失效在断开状态	0.012 161	3	左正常供电丧失	
					

表4 配电系统软件和复杂硬件IDA5

序号	设备名称	设备数量	软件 DAL(DO-178B)	硬件 DAL(DO-254B)	合同签订等级是否满足要求
1	BPCU	2	B	B	是

和特定风险分析(particular risks analysis, PRA)。⁷ ZSA关注系统间的相互影响,PRA评估外部威胁对飞行安全性的影响,对于配电系统,ZSA分析和PRA分析不适用,故只需进行CMA分析。

根据通用CMA检查单模板,结合配电系统的实际设计,确定了适用于配电系统的共模分析检查单。8

基于配电系统 FHA 和 PSSA, 得出配电系统的 9 独立性需求共 6 项。针对每项独立性需求按照共模分析检查单进行检查, 经分析所有独立性需求均能得到满足。表 5 为以“左通道与右通道应相互独立”为例的共模分析方法。

有导致配电系统 I、II 类功能失效的故障模式。若¹³有，则需要设计改进。

在目前的研制过程中,存在着零组件 FMEA 中¹⁴严酷度定义不明确、零组件故障模式无法支撑上层系统安全性分析的问题。

零组件FMEA中严酷度等级为I类的通常为产品失效,严酷度等级为Ⅱ类的通常定义为重要功能失效,但重要功能的定义并不明确。通过从系统级到零组件的安全性分析得出,零组件FMEA中严酷度等级应与系统安全性分析协调一致,应根据系统功能的安全性等级,确认分配下来的功能的安全性等级,进而确定失效模式的严酷度等级。

零组件的FMEA故障模式应能支撑上层系统进行安全性分析,故零组件故障模式名称应与图1的底事件相一致。目前研制中的零组件FMEA故障模式笼统,如“BPCU XX 接触器控制功能失效”。而“BPCU XX 接触器控制功能失效在断开状态”和

4 系统安全性分析¹⁰

4.1 零组件 FMEA 分析

各零组件设计完成后,需对各零组件进行FMEA分析。通过FMEA分析,进一步识别是否具

表 5 “左通道与右通道应相互独立”共模分析

共模源	共模失效/差错	设计采取的防护措施	可以接受的相 关证明或更改	备注
公共外部源 (发电机驱动)	公共外部源 (发电机驱动)失效	电源系统中共设有 8 台独立的直流发电机(分别由 1、2、3、4 个发动机驱动)及 2 台蓄电池。因此,任一公共外部源(发电机、发动机)、蓄电池的失效不会导致多个供电通道失效	可以接受	2
公共外部源 (通风)	公共外部源 (通风)失效	左直流供电通道主要包括 LDP(left distribution panel)(集成有左中央汇流条、左应急汇流条、接触器等部件)、LBPCU、左蓄电池等设备及相关 EWIS 部件;右直流供电通道主要包括 RDP(right distribution panel)(集成有右中央汇流条、右应急汇流条、接触器等部件)、RBPCU、右蓄电池、飞控蓄电池等设备及相关 EWIS 部件。电源系统不同供电通道的设备安装于不同的区域,不会因单个区域通风系统的失效而导致多个供电通道同时失效	可以接受	
			

“BPCU XX 接触器控制功能失效在失效状态”会导致系统不同的失效模式,故零组件级的故障模式应细化为两种。

通过 FMEA 分析,确定了零组件各故障模式的失效率,识别了系统 PSSA 分析中未识别出的故障模式,并进行了迭代。

同时,经分析本系统中的配电柜、BPCU 均无导致配电系统 I、II 类功能失效的故障模式,无需进行设计改进。

4.2 零组件 FTA 分析

对各零组件进行 FTA 分析,评估零组件是否满足分配的 FTA 指标,同时得出 PSSA 中各底事件的

失效率

在 PSSA 底事件中,有些为零组件航线可更换部件(line replaceable unit, LRU)级的故障模式,通过零组件 FMEA 分析便可得出失效率。有些底事件为 FMEA 中 LRU 级故障模式的逻辑组合,需要运用故障树的方法进行运算,采用 2.1 节中的基于模型的故障树分析方法,其底层数据为 FMEA 各故障模式的失效率。

若不满足,则需进行设计改进,通常采用的设计改进方法有余度设计、降额设计、提升元器件等级等。

经计算各零组件能够满足 PSSA 中分配的失效率要求,如表 6 所示,无需进行设计改进。

表 6 零组件 FTA 分析

序号	组件名称	节点名称	每小时故障率 λ
1	配电柜	左中央汇流条故障	1.1×10^{-7}
2	配电柜	熔断器 1 故障开路	6.09×10^{-7}
3	BPCU	BPCU 控制连接接触器失效在断开状态	3.152×10^{-6}
		

4.3 系统安全性分析

对系统安全性进行重新评估,评估过程与第 3 章相似。故障树分析中应用的源数据为 4.2 节计算的数据。经分析,配电系统能够满足安全性要求。以左应急通道和右正常通道直流供电丧失为例,经计算其概率小于 1×10^{-9} ,满足 I 类故障的失效率要求。

特点对安全性评估流程和方法作了适应性改进,包括 FHA 分析、PSSA 分析、SSA 分析以及系统安全性分析与零组件安全性分析的衔接方法,为配电系统安全性分析提供了指导。同时该方法采用故障树模型的方式,可减少故障树分析造成的工作量,便于安全性分析在系统研发中的应用。

参考文献

- [1] 蔡林,张玲,杨善水,等.大型飞机供配电系统可靠评估与分析[J].航空学报,2011,32(8):1488-1496.

- [2] 秦海鸿, 严仰光. 多电飞机的电气系统[M]. 北京¹北京航空航天大学出版社, 2016.
- [3] 郭博智, 王敏芹, 阮宏泽. 民用飞机安全性丛书 民用飞机安全性设计与验证技术[M]. 北京: 航空工业出版社, 2015.
- [4] ARP4754B. Guidelines for Development of Civil Aircraft and Systems. SAE International, Dec. 2023. URL: <https://www.sae.org/standards/content/arp4754b/>.
- [5] ARP4761A. Guidelines for Conducting the Safety Assessment Process on Civil Aircraft, Systems, and Equipment. SAE International, Dec. 2023. URL: <https://www.sae.org/standards/content/arp4761a/>.
- [6] 周素莹. 多电飞机电气系统的研究[D]. 西安: 西北工业大学, 2003.
- [7] 李彦锋. 复杂系统动态故障树分析的新方法及其应用研究[D]. 成都: 电子科技大学, 2013.
- [8] 张国防. 计入导线故障的民机安全性定量分析方法研
究[J]. 航空工程进展, 2012, 3(2):241-246.²
- [9] 王豪, 高亚奎, 戚永灵, 等. 基于功能模型的飞控系统安全性设计技术研究[J]. 测控技术, 2017, 36(5): 77-81.
- [10] 于开民, 孙时珍, 张树团, 等. 一种基于Petri网的飞机配电系统可靠性分析方法[J]. 电子设计工程, 2010, 18(10):133-135.
- [11] 董力. 基于模型的飞行控制系统安全性分析方法研究[D]. 南京: 南京航空航天大学, 2020.

作者简介

李阳阳 女, 硕士, 高级工程师。主要研究方向: 飞机配⁴电系统及产品设计。E-mail: whyyzfn@163.com

姚磊 男, 硕士, 研究员。主要研究方向: 飞机配电系统及产品设计。E-mail: yaolei1056@126.com

周俊童 女, 硕士, 工程师。主要研究方向: 飞机配电系统及产品设计。E-mail: z_j_tong@126.com

Research on safety design technology for power distribution system⁵

LI Yangyang^{*} YAO Lei ZHOU Junton⁶

(R&D Department of Tianjin Aviation Electro-Mechanical Co., Ltd., Tianjin, 300308, China)⁷

Abstract: This paper adapts and improves the safety assessment process and methods in accordance with the characteristics of the power distribution system, based on SAE ARP4761, including functional hazard analysis (FHA), preliminary safety analysis (PSSA), safety analysis (SSA), common mode analysis (CMA). The integration relationship between safety analysis and system development process is also proposed. The connecting method of power distribution system safety analysis and component safety analysis is then proposed. All provide guidance for distribution system safety analysis. Model-based analysis is adopted in fault tree analysis and allocation, which can reduce the huge workload caused by fault tree analysis and facilitate the application of safety analysis in system development.

Keywords: power distribution system; safety; fault tree; common mode analysis⁸

* Corresponding author. E-mail: whyyzfn@163.com