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

DOI: 10.19416/j.cnki.1674-9804.2023.02.001

电传飞控共模适航要求及审定考虑

黄铭媛* 揭裕文 宋智桃 戴闰志

(中国民航上海航空器适航审定中心,上海 200232)

摘 要: 梳理和分析电传飞控系统共模相关适航要求,创新建立“电传飞控系统共模认知-控制审定流程模型”并提出针对共模问题的审查原则和考虑,有助于全面分析、识别并确定可能的共模失效、提出独立性设计要求,权衡设计解决方案等。应用该模型和审查考虑对某机型电传飞控系统有关复杂电子硬件差错共模的审查案例开展分析,识别确认共模因素和共模失效并分析各设计方案的可行性。研究成果对电传飞控系统及其它复杂系统共模的审查和设计具有指导和借鉴意义。

关键词: 电传飞控;系统安全性分析;共模;适航;审查;终极备份

中图分类号: V249 **文献标识码**: A **OSID**:

0 引言

民用飞机电传飞控系统具有高度集成和复杂的特点,安全性、可靠性要求高,其功能失效将产生灾难性影响,故应多采用冗余架构设计来保证安全性,即在单个或若干个设备发生故障时飞控功能仍然可用,以保证飞机的可操纵性。但是,如果因共模问题破坏冗余架构并导致丧失电传飞控系统控制功能,将带来巨大安全隐患。因此,在电传飞控系统的设计、验证和审查中,需识别、消除和/或缓解潜在共模失效带来的安全性影响。

FAA 和 EASA 发布系统安全性条款 25.1309 系统、设备及安装的咨询通告/可接受的符合性方法“系统设计和分析”文件中[1-4],要求开展包括共模分析在内的共因分析,识别破坏独立性假设从而导致单点失效的问题,并采取相应安全保障措施。工业标准 SAE ARP4761《民用飞机机载系统和设备进行安全评估过程的指南和方法》则进一步给出结构化共模分析方法。

1 适航要求

针对电传飞控系统共模问题,CAAC、FAA 和 EASA 通过规章/等效安全、咨询通告以及符合性方法类问题纪要/审定评审项目(CRI)等形式,建立有关共模的适航要求体系,自上而下建立单个失效不计概率不得导致灾难性失效状态、“失效-安全”设计理念、单个失效考虑、共因分析(包含共模分析)以及针对复杂电子硬件单粒子翻转等要求,共模适航要求体系如表 1 所示[2-6]。

表 1 共模适航要求体系

类 型	编 号	要 求
规章/等效安全	25.1309(b)(1)	单个失效不计概率不得导致灾难性失效状态
咨询通告/问题纪要	符合性方法要求	“失效-安全”设计理念、单个失效考虑、共模、复杂电子硬件单粒子翻转等要求
行业标准/最佳实践	SAE ARP4761	共模分析方法的具体要求

例如,某大型民用飞机审查中,审查组建立了关于 CCAR 25.1309(b)(1)条款的等效安全,对单个失效提出了明确的要求,具体如下:

飞机系统与有关部件的设计,在单独考虑以及与其它系统一同考虑的情况下,必须符合下列规定:

* **通信作者**. E-mail: huangmingyuan_hd@caac.gov.cn

引用格式: 黄铭媛,揭裕文,宋智桃,等. 电传飞控共模适航要求及审定考虑[J]. 民用飞机设计与研究,2023(2):1-7. HUANG M Y,JIE Y W,SONG Z T,et al. Common mode airworthiness requirements and certification considerations for fly-by-wire [J]. Civil Aircraft Design and Research,2023(2):1-7(in Chinese).

每一个灾难性的失效状态

(i) 是极不可能的;并且……

(ii) 不会由单个失效造成;并且……

同时,通过建立符合性方法问题纪要,提出“失效-安全”设计理念要求,即在任何一次飞行中,对于任何系统或子系统,应假设任何单个元件、组件或连接的失效都会发生,而无论其发生概率,且这样的单个失效不应导致灾难性的影响。

在“单个失效考虑”中进一步说明,系统安全性分析需考虑的这类可能导致灾难性影响的单个失效,包括系统的单个组件、部件或元件的失效,以及共因失效。即,单个失效包括任何不能表明相互独立的失效的集合。共模失效,作为共因失效的一类,将破坏冗余的独立性,从而形成单个失效。

针对复杂电子硬件,通过问题纪要对单粒子翻转提出要求,包括开展单粒子翻转分析、安全性影响分析并表明可抑制或消除单粒子翻转对可编程电子硬件器件的影响。单粒子翻转是由于空间粒子辐射现象而导致的微电子电路的状态改变。虽然单粒子翻转效应是瞬态的、非破坏性的,但单粒子翻转可能会改变微电子电路的存储器构型、对可编程电子硬件器件所执行的功能造成不利影响。

总之,各类型的共模将破坏冗余独立性假设、导致原本假设独立的设备发生相同模式失效或级联失效从而变为单个失效,且这类单个失效将造成灾难性失效状态的不可接受的后果,因此审查需重点关注可能导致灾难性失效状态的共模问题的符合性。

2　审定流程模型

SAE ARP4761系统安全性评估指南给出了共模分析的定义及方法,但目前缺少系统性的方法来识别和确认共模问题。本文基于审查经验和实践,提出电传飞控系统“共模认知-控制审定流程”模型。

认知,即对可能的共模失效和共模因素的识别和确认;控制,即对特定共模因素导致共模失效造成的安全性风险的控制,将其控制在可接受的范围内。模型如图 1 所示,主要流程如下:

1) 通过认知模型识别和确认潜在的共模失效及共模因素:

(1) 评审电传飞控系统功能危害分析文件(FHA),识别并确认所有灾难性失效状态,将所有灾难性失效状态作为潜在的共模失效分析对象[9-10]。

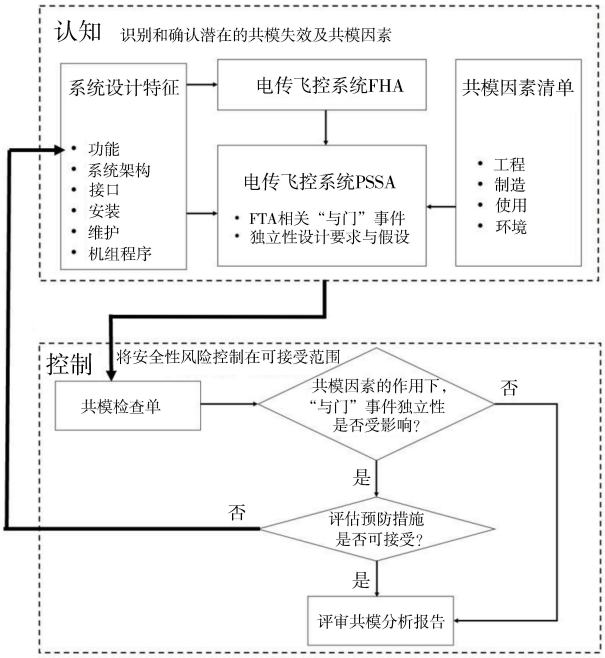

图 1　电传飞控系统共模问题认知-控制审定流程模型

(2) 结合电传飞控系统设计描述文件(SDD),对照初步安全性分析故障树所有与灾难性失效状态相关的“与门”事件,评审独立性设计要求与假设,识别并确认与设计独立性要求有关的“与门”事件。

(3) 形成共模因素清单,包括工程因素、制造因素、使用因素及环境因素等。

2) 通过控制模型将安全性风险控制在可接受范围:

(1) 针对各“与门”事件,将共模因素清单对照排查,形成“共模检查单”;

(2) 对照共模检查单,评估在各种共模因素的作用下,各“与门”事件独立性是否受影响;

(3) 如不受影响,评审并确认申请人的共模分析报告相关分析记录及理由;

(4) 如受影响,要求申请人提出预防措施并且评审预防措施是否可接受;

(5) 评估预防措施是否可接受,如不接受,返回“认知”流程,申请人需更改系统设计或补充验证以控制共模失效带来的安全性风险;

(6) 如接受,评审并确认申请人共模分析报告

相关记录及证据。

3　研制差错共模因素审查考虑

3.1　基本原则

由共同原因引起多个故障模式相同的失效,且这些多重失效之间无因果关系,这类失效定义为共模失效,审查针对的潜在共模失效指的是灾难性的失效状态。对电传飞控系统共模问题的基本审查原则如下:

1)对于潜在共模失效,建议按照 SAE ARP4761开展结构化的共模分析工作。申请人应建立特定的检查单、确定共模分析要求、对设计进行分析,以确保满足检查单和共模分析要求,并将结果形成共模分析报告。

2)对于飞机、系统、复杂电子硬件和软件的开发均可使用适当的研制保证来减少研制过程中可能产生的差错。但是对于研制差错带来的对飞机的安全性影响和风险,单独采用研制保证和质量保证、高加速应力筛选、验收测试,仍不足以完全消除,还应采取必要的减缓手段或技术来降低研制差错导致的失效对飞机安全性的影响至可接受的水平。基于全机安全性策略,电传飞控系统设计有必要采取故障检测、故障容错、故障排除和故障避免等基本安全性技术。

3)对共模因素的考虑应全面和完整,需关注研制差错相关共模因素。其中,研制差错相关工程共模因素是审查关注重点。

3.2　电传飞控共模审查考虑

由于电传飞行控制系统需达到规章要求的安全性水平,针对共模因素中的研制差错,电传飞控系统的具体审查考虑和要求如下:

1)应采用充分的研制保证。至少需包括飞控系统需求确认和实施验证的完整性和正确性,飞机与飞控系统之间需求传递的正确性,飞控系统与其他关键系统之间需求传递及实现的正确性以及申请人对供应商的研制保证过程监督以及供应商的研制保证过程。

2)应采用有效的减缓措施。仅通过研制保证来表明符合性是不充分的,需要在系统架构设计上采取措施,综合运用故障检测、故障容错、故障排除和故障避免这类减缓技术手段将可能的研制差错带来的安全性风险降低到可接受的安全性水平,即因研制差错导致系统功能丧失的安全性影响不得是灾难性的。对于设计采取的相关措施,可以通过分析、试验、演示验证等来证明措施可以防止因共模失效导致灾难性失效状态。

在审查时应注意,相似设计特征不一定会导致灾难的共模问题。需通过分析确定相关失效模式是否对灾难性失效状态有贡献,受哪些共模因素的影响以及设计所采取的相关预防措施是否可以避免或减缓安全性风险至可接受的水平来识别和确定共模问题。可通过审查流程模型开展结构化的分析,以识别确定共模问题及独立性要求。

3.3　国际上针对共模问题的处理方法

解决电传飞控系统共模问题,理论上可从元器件级、设备级和系统级提出技术解决措施。

当前全球主流民机采用电传飞控系统的架构设计通常采用系统级解决措施,例如波音、空客及主流干线飞机在飞控系统架构上均有不同形式的终极备份设计,即独立于电传飞控的一套简单的能够完全理解和验证的,具备一定操纵能力的飞行控制系统,如简易电控、机械操纵等。

从历史发展看,在电传飞控系统技术日益成熟的情况下,终极备份没有简化反而越来越强,部分民机的终极备份设计如表 2 所示。

表 2　部分民机电传飞控系统备份设计

机　型	终极备份设计
A320	水平安定面和方向舵机械控制
A330/340	水平安定面和方向舵机械控制,方向舵控制带偏航阻尼
A340-500/600	水平安定面机械控制,模拟 BCM 电控方向舵
A380	模拟 BCM 控制:电控升降舵、电控副翼、电控方向舵,水平安定面
A350	数字 BCM 控制:液压副翼、液压升降舵、液压方向舵
波音 777	两对扰流板和水平安定面机械控制
波音 787	一对扰流板和水平安定面电控
湾流 G650	BFCU 控制所有舵面(副翼、升降舵、方向舵、扰流板、水平安定面
C 系列	AFCU 控制副翼、升降舵和方向舵

4　审查案例分析

4.1　某电传设计特征

某机型采用电传飞控系统实现对飞机三轴的控制功能,高度集成,侧杆操纵。飞行员操纵指令通过 4 个作动器电子控制装置(ACE)和 3 个飞控计算机(FCM)解算,由 ACEs 将指令信号输出至远程控制组件(REUs),控制作动器驱动舵面偏转以实现对飞机的控制。系统架构和主要信号流如图 2 所示。

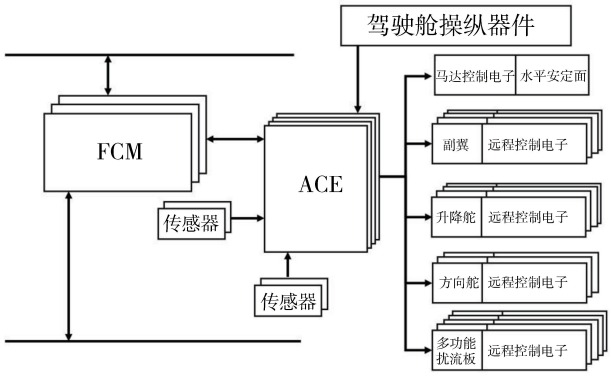

图 2　某飞机电传飞控系统系统架构图

4.2　应用审定流程模型

通过应用电传飞控系统“共模认知-控制审定流程”模型,对该电传设计开展评估,识别、确定共模问题,评估措施有效性,并且探讨预防措施能否接受的准则。具体如下:

1)使用认知模型识别和确认潜在的共模失效及共模因素:

(1)通过评审电传飞控系统功能危害分析文件(FHA),识别并确认灾难性失效状态“丧失三轴控制功能”作为潜在的共模失效分析对象。

(2)结合电传飞控系统设计描述文件,分析系统设计特征可知,系统正常模式和直接模式都通过 ACE,因此重点关注控制功能关键路径中的 4 台 ACE 的设计架构,如果 4 台 ACE 同时失效,将导致丧失三轴控制功能的灾难性失效状态。

ACE 由命令支路和监控支路组成,各支路由正常模式分区、直接模式分区和公共分区组成,正常模式和直接模式都需使用到公共分区,且指令支路公共分区和监控支路公共分区是相同的板卡。

通过对照初步安全性分析故障树所有与灾难性失效状态相关的“与门”事件,评审独立性设计要求与假设,识别确定“ACE 指令通道公共分区处理失效”和“ACE 监控通道公共分区处理失效”与门事件是潜在的受影响对象,丧失三轴控制功能故障树分析如图 3 所示。

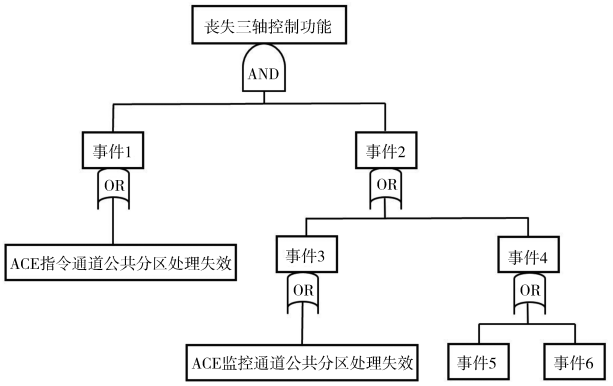

图 3　丧失三轴控制功能故障树分析

(3)形成共模因素清单,如表 3 所示。

表 3　共模因素清单

类　型	共模因素
1 概念与设计	A 架构设计
	B 技术、材料、设备型号
	C 规范
2 制造	A 制造
3 安装、综合和试验	A 安装和综合
4 操作	A 操作
	B 维护
5 环境因素-特定风险	A 机械和热
	B 电气和辐射
	C 化学和其他

2)通过控制模型将安全性风险控制在可接受范围:

(1)针对各“与门”事件,将共模因素清单对照排查,形成“共模检查单”,如表 4 所示。

表 4　共模检查单

ACE 指令通道公共分区和监控通道公共分区不能同时丧失				
共模类型	共模源	共模失效/错误	设计采取的防护措施及可接受方法	可以接受的额相关证明或更改设计的建议
技术、材料、设备	硬件	复杂电子硬件研制错误	1. 按照 DO-254 中 DAL A 级规定的研制流程进行硬件研制	《复杂电子硬件研制保证计划及完成综述》
			2. 公共分区完全可测试可分析	《公共分区测试分析报告》

（2）对照共模检查单,评估得知在复杂电子硬件差错的共模因素作用下,该“与门”事件将受到影响,即存在由于复杂电子硬件差错导致 ACE 公共分区指令和监控同时丧失进而引起丧失三轴控制的灾难性事件发生的风险。

（3）经评估,在复杂电子硬件差错的共模因素作用下,该“与门”事件独立性将受到影响。

（4）由于独立性受影响,要求申请人提出预防措施并且评审预防措施是否可接受;申请人提出以下两种预防措施和/或解决思路,审查组应用审查原则评估后结论如表 5 所示。

表 5　评审预防措施、解决思路

申请人预防措施/解决思路	审查结论及理由
复杂电子硬件层级,按照 DO-254 中 DAL A 级规定的研制流程进行硬件研制	不接受。对于研制差错带来的对飞机的安全性影响和风险,仅使用研制保证是不充分的,需要采取相关减缓手段来表明符合性,因此不接受申请人仅采用“研制保证”的预防措施
证明公共分区完全可测试可分析	不接受。由于复杂电子硬件的复杂程度根据门的数量呈指数型增长,除非提出新的完全可测试可分析标准并且被认可,否则按现有标准 DO-254 认为,证明其完全可测试和可分析是不切实际的

（5）由于不接受,返回认知流程,建议申请人从架构上采取措施,通过系统设计更改来减缓或消除因复杂电子硬件差错共模因素攻击导致的共模失效风险。申请人提出两项备选的系统设计更改方案:一是 ACE 公共分区采用不同的 FPGA 芯片,通过非相似设计消除共模失效的风险,如图 4 所示;

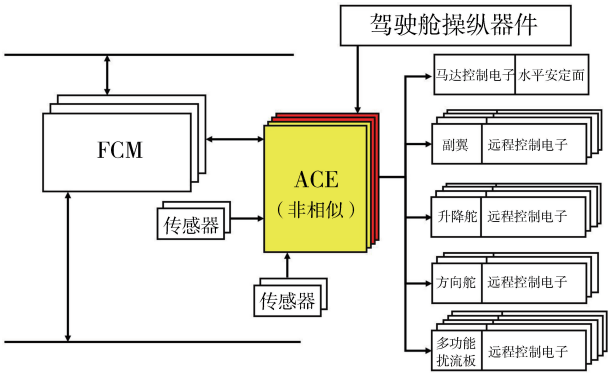

图 4　备选方案一:ACE 非相似设计

二是新增操纵器件直接控制水平安定面和一对扰流板的控制通路,在假设由于共模问题导致 ACE 失效后,通过简单的电子控制方式,确保飞控系统仍具备可操纵飞机和稳定飞机姿态的能力,即终极备份设计,如图 5 所示。

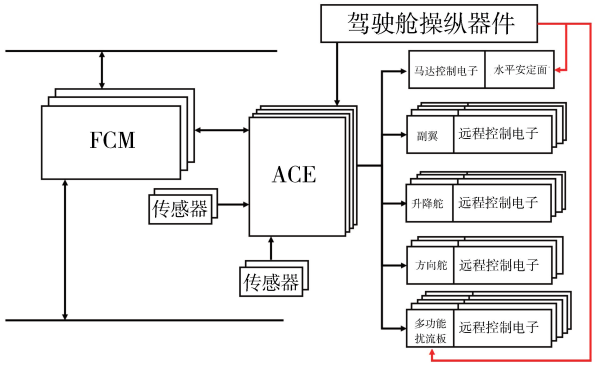

图 5　备选方案二:新增水平安定面及一对多功能扰流板电控设计

审查分析认为,备选方案一是从设备/元器件级提出的解决思路,是针对复杂电子硬件差错的共模因素的直接解决办法,但由于复杂电子硬件特性,引入另一套非相似的复杂电子硬件,可能引入新的风险,例如兼容性、指令完整性、故障监测等问题导致 ACE 被错误切断、频繁重启以及骚扰性告警等安全性问题,因此需要全面评估并进行充分的试验来表明符合性。

备选方案二是从系统级提出的解决思路,通过系统功能终极备份的方式,对 ACE 共模造成的安全性影响进行缓解,使得共模的安全性影响不再是灾难性的。并且,由于备选方案二的功能备份是简单电控系统,能够被完全分析和理解,可靠性高,可以作为有效的缓解措施,但也需避免与主控制通路产生干扰等问题。

从控制共模风险角度出发,方案一和方案二都可作为解决共模问题的措施,考虑到系统架构终极备份设计在当前全球电传飞控系统的设计占主要趋势,申请人可考虑从系统架构上进行功能备份设计,以达到与全球电传飞控系统同等的冗余水平。但审查不能干涉设计的选择,审查通过提出问题、评估风险并且基于符合性试验和证据等判定设计对规章的符合性。如申请人还有其它备选方案或解决路径,应尽早向审查组提出,并将适航要求作为需求输入,作全面的设计评估和权衡并选择最终

的解决方案。

(6) 在申请人重新完成架构设计更改及更新的共模分析后,形成电传飞控系统共模分析报告并提交审查组批准认可。

5 结论

电传飞控系统作为飞机关键系统之一,考虑到共模问题对系统冗余设计架构以及安全性的严重影响,共模问题的审查至关重要。

针对目前缺少共模审查指南的问题,本文提出“共模认知-控制审定流程”模型,有助于共模审查时理清思路并聚焦问题;本文提出的审查原则补充了系统安全性审查要素,可供适航审定和工业界参考;通过某机型电传飞控系统有关复杂电子硬件差错共模的案例,验证了该模型和审查原则应用的可行性。

同时,本文有关终极备份设计架构问题提出的审查考虑值得在业内开展研讨。未来,针对复杂电子硬件差错可能导致共模的减缓措施和符合性方法问题,包括判定该电子硬件是否有限复杂,判定是否完全可测试可分析的标准、方法和策略,较低层级非相似架构/局部非相似架构措施的有效性以及系统层级终极备份的必要性等方面,需要开展更为深入的研究。

参考文献:

[1] 中国民用航空局. 运输类飞机适航标准:CCAR-25-R4[S]. 北京:中国民用航空局,2011.

[2] EASA. Certification specifications and acceptable means of compliance for large aeroplanes:CS-25 amendment 27 [S]. Europe:EASA,2023.

[3] FAA. Airworthiness standards transport category airplanes:FAR-25[S]. U.S.:FAA,2022.

[4] FAA. System design and analysis: AC 25.1309-1B (Draft)[S]. U.S.:FAA,2002.

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

[6] SAE. Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment:SAE ARP4761[S]. U.S.:SAE,1996.

[7] 中国民用航空局. 民航航空产品和零部件合格审定的规定:CCAR-21[S]. 北京:中国民用航空局,1990.

[8] FAA. FAA system safety handbook, Chapter 2: System safety policy and process[S]. U.S.:FAA, 2000.

[9] 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.

[10] 唐志帅,刘兴华. 民机电传飞控系统安全性设计与验证[J]. 民用飞机设计与研究,2016(3):73-76.

作者简介

黄铭媛 女,硕士,高级工程师。主要研究方向:飞控系统、系统安全性、研制保证过程。E-mail: huangmingyuan_hd@caac.gov.cn

揭裕文 男,硕士,正高级工程师。主要研究方向:型号合格审定、适航管理、总体气动、人为因素、系统安全性。E-mail: jieyuwen_hd@caac.gov.cn

宋智桃 男,本科,正高级工程师。主要研究方向:机械系统适航审查、系统安全性、研制保证、适航管理。E-mail: songzhitao_hd@caac.gov.cn

戴闰志 男,硕士,高级工程师。主要研究方向:飞控系统、系统安全性、试飞。E-mail: dairunzhi@saacc.org.cn

Common mode airworthiness requirements and certification considerations for fly-by-wire

HUANG Mingyuan *　JIE Yuwen　SONG Zhitao　DAI Runzhi

(Shanghai Aircraft Airworthiness Certification Center of CAAC, Shanghai 200232, China)

Abstract: This paper combs and analyzes the airworthiness requirements related to the common mode issues of FBW flight control systems, innovatively establishes the "common mode cognitive-control certification process model for FBW flight control system" and proposes the review principles and certification considerations for the common mode issues, which helps to fully analyze, identify and determine possible common mode failures, propose independent design requirements and trade-off design solutions. By applying the model and certification consideration, the certification case of a complex electronic hardware error common-mode of an FBW flight control system was analyzed, the common mode factors and common mode failures were identified and confirmed, and the feasibility of each design solution was analyzed. The research results have guiding and reference significance for the certification and design of common mode issues of FBW flight control system and other complex systems.

Keywords: fly-by-wire(FBW); system safety analysis; common mode; airworthiness; certification; ultimate backup

* Corresponding author. E-mail: huangmingyuan_hd@caac.gov.cn