文章编号:1674-8190(2024)01-135-06

系统安全性评估中飞行机组人为因素的分析方法

刘会星,阮宏泽,黎先平,冯臻
(上海飞机设计研究院 飞机架构集成工程技术所,上海 201210)

摘 要: 随着飞机系统日益高度综合复杂和自动化水平逐渐提高,飞行员在应对失效或应急情况时通常准备不足,纠正动作可能是不正确、不及时或不完整的,因此系统安全性评估中迫切需要考虑飞行机组人为因素问题。通过分析CCAR25.1309(b)和(c)条款的要求和飞行机组对失效的处理过程,基于功能危险性评估中的失效状态,提出人为因素需求的捕获方法和人为因素分析方法;通过在型号中应用这些方法,从失效状态向告警和程序的角度实现安全性正向设计,建立安全性评估中飞行机组人为因素的完整适航符合性证据链。结果表明:本文提出的方法可有效表明对CCAR25.1309(b)和(c)条款中人为因素相关的适航符合性。

关键词: 功能危险性评估;人为因素;假设;失效状态;告警;程序
中图分类号: V216.7; V221 **文献标识码:** A
DOI: 10.16615/j.cnki.1674-8190.2024.01.15

Analysis method of flight crew human factors in system safety assessment

LIU Huixing, RUAN Hongze, LI Xianping, FENG Zhen
(Aircraft Architecture Integration Engineering Technology Institute, Shanghai Aircraft Design and Research Institute, Shanghai 201210, China)

Abstract: With the improvement of high complexity and automation level of the aircraft systems, pilots are often ill-prepared to cope with an actual emergency or failure, and their corrective actions may be erroneous, delayed or incomplete. Therefore, there is an urgent need to consider flight crew human factors in system safety assessment. By analyzing the requirements of CCAR25.1309(b) and (c) and failure processing process of flight crew, based on the failure conditions in functional hazard assessment, the methods of requirements capture and analysis of flight crew human factors is proposed. By applying these methods in the aircraft development, the top down design for safety which from failure condition to alert and procedures is achieved, and a complete chain of compliance evidence for human factor of safety is established. The results show that the proposed method can effectively demonstrate airworthiness compliance with human factors of CCAR25.1309(b) and (c).

Key words: functional hazard assessment; human factors; assumption; failure condition; alert; procedure

收稿日期: 2022-12-23; **修回日期:** 2023-10-07

通信作者: 刘会星(1985—),男,博士,高级工程师。E-mail: liuhuixing888@163.com

引用格式: 刘会星,阮宏泽,黎先平,等. 系统安全性评估中飞行机组人为因素的分析方法[J]. 航空工程进展,2024,15(1):135-140,156.
LIU Huixing, RUAN Hongze, LI Xianping, et al. Analysis method of flight crew human factors in system safety assessment[J]. Advances in Aeronautical Science and Engineering, 2024, 15(1): 135-140,156. (in Chinese)

0 引 言

根据对大型运输类飞机的统计，近10年由人为因素导致的致命事故占57%。2018和2019年两起B737-8空难的原因之一，是波音在机动特性增稳系统（Maneuvering Characteristics Augmentation System，简称MCAS）的安全性评估中没有充分考虑人为因素的影响[1-2]。根据美国《航空器审定、安全和责任法》第126节，政府授权在2021—2023的每个财年向联邦航空管理局（Federal Aviation Administration，简称FAA）拨款750万美元，以研究运输类飞机的设计和合格审定中人为因素的集成问题[3]。美国国家安全运输委员会（National Transportation Safety Board，简称NTSB）建议FAA开发有效的方法工具，以对飞行员识别安全性重要失效状态并作出响应的假设进行确认，并将其作为设计符合性过程的一部分[1]。可见，当前迫切需要在系统安全性评估中考虑人为因素问题。

功能危险性评估（Functional Hazard Assessment，简称FHA）是分析飞机系统功能的失效状态并按其严重性进行定级的过程，通过充分确认失效状态识别的完整性、影响等级的正确性以支持CCAR25.1309（b）条款的适航符合性验证[4]。一些失效状态的影响可以通过飞行机组识别和响应加以减缓，减缓的效果则取决于机组执行预期动作的能力以及在管理失效状态时不存在可能导致额外危险的机组差错（即CCAR25.1309（c）条款的要求）。此时，机组识别和响应相关的假设是否成立直接影响失效状态的定级和后续的安全性目标。因此，必须充分证明失效状态相关的飞行机组人为因素假设并确认影响等级的正确性，以支持对CCAR25.1309（b）和（c）条款的适航符合性验证。

董大勇等[5]研究了CS 25.1302条款的验证思路和方法，提出从预定功能与机组任务、操纵器件、信息显示、系统行为和差错管理等方面开展验证工作；宋海靖等[6]提出了试飞阶段人为因素的审定方法框架；孙世东等[7-8]确定了人为因素适航审定内容，规划了符合性验证方法和流程。上述研究主要针对人为因素专有条款14CFR/CS 25.1302，而针对系统安全性综合性条款CCAR25.1309，在CCAR/14CFR/CS 25.1309和25.1302及其指导材料[4,9-12]中，没有提供系统安全性中人为因素的符合性验证方法。针对14CFR/CS 25.1309，FAA和欧盟航空安全局（European Union Aviation Safety Agency，简称EASA）均认为无法对机组差错进行定量评估[9-10]。Kritzinger[13-14]提出一种减少机组差错的系统安全性评估流程，但该流程仅提供了理论框架，并未给出工程上可操作的具体方法流程；EASA提出了一种人为因素分析方法[15]，通过分析失效发生后的驾驶舱效应、机组感知和机组反应以确认失效状态定级的正确性，但该方法并未说明工程如何应用，在机组差错分析方面有漏项。

本文基于EASA的方法并针对以上不足，从安全性驱动告警和程序的正向设计角度，提出基于失效状态的人为因素分析方法，该方法包括两个部分：人为因素的需求捕获和人为因素分析。结合大型客机的工程应用示例，说明该方法可实现安全性评估中飞行机组人为因素的正向闭环设计并建立完整的适航符合性证据链，以期为民用飞机表明对CCAR25.1309（b）和（c）条款的适航符合性提供参考。

1 适航要求与分析

CCAR25.1309（b）条款主要针对失效状态做出相关要求，在符合性验证工作中，应对失效状态进行识别，对其影响进行评估，并考虑在某个失效或失效状态发生后可合理预见机组差错的影响、机组告警提示、所需的纠正动作以及机组检测故障的能力[9-10]。

CCAR25.1309（c）条款内容为：必须提供告警信息，向机组指出系统的不安全工作情况并能使机组采取适当的纠正动作。系统、控制器件和有关的监控与告警装置的设计必须尽量减少可能增加危险的机组失误。该条款包括3部分要求：

1）向机组提供系统不安全工作状态的信息；

2）使机组及时采取要求的纠正动作；

3）系统或控制器件（包括指示和通告）的设计可以将机组差错降至最低。

首先，系统不安全工作状态可以通过FHA的失效状态进行识别；其次，机组正确实施纠正动作的前提包括，充分识别失效状态、正确理解失效场景、制定适当的动作计划和充足的时间以理解失效场景并执行动作；最后，机组反应的预期效果取决于飞行机组执行动作的能力以及在失效管理时不会因人为差错导致其他的危险。

基于机组任务,飞行机组对失效的处理包括5个过程,如图1所示。

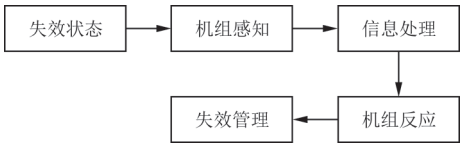


图1　飞行机组对失效的处理过程
Fig. 1　Failure handling process of flight crew

失效状态是整个过程的刺激因素,一个失效状态可能包含数个功能失效场景;对于不同失效场景,飞行机组可能通过不同的驾驶舱效应感知失效状态,包括视觉、听觉和触觉等;机组对驾驶舱提供的信息进行分析,以充分理解失效状态的原因并做出决策;机组可能需采取纠正/补偿动作以减缓失效影响;失效管理主要关注人为因素隐患,包括失效对飞行机组、飞机系统的影响,可能的机组差错等。

2　FHA中人为因素的分析方法

2.1　需求捕获方法

根据SAE ARP4754A[16],初步设计阶段的安全性评估活动主要有飞机级FHA、初步飞机安全性评估(Preliminary Aircraft Safety Assessment,简称PASA)、系统级FHA和初步系统安全性评估(Preliminary System Safety Assessment,简称PSSA),详细设计阶段的安全性评估活动主要有系统安全性评估(System Safety Assessment,简称SSA)和飞机安全性评估(Aircraft Safety Assessment,简称ASA),如图2所示。

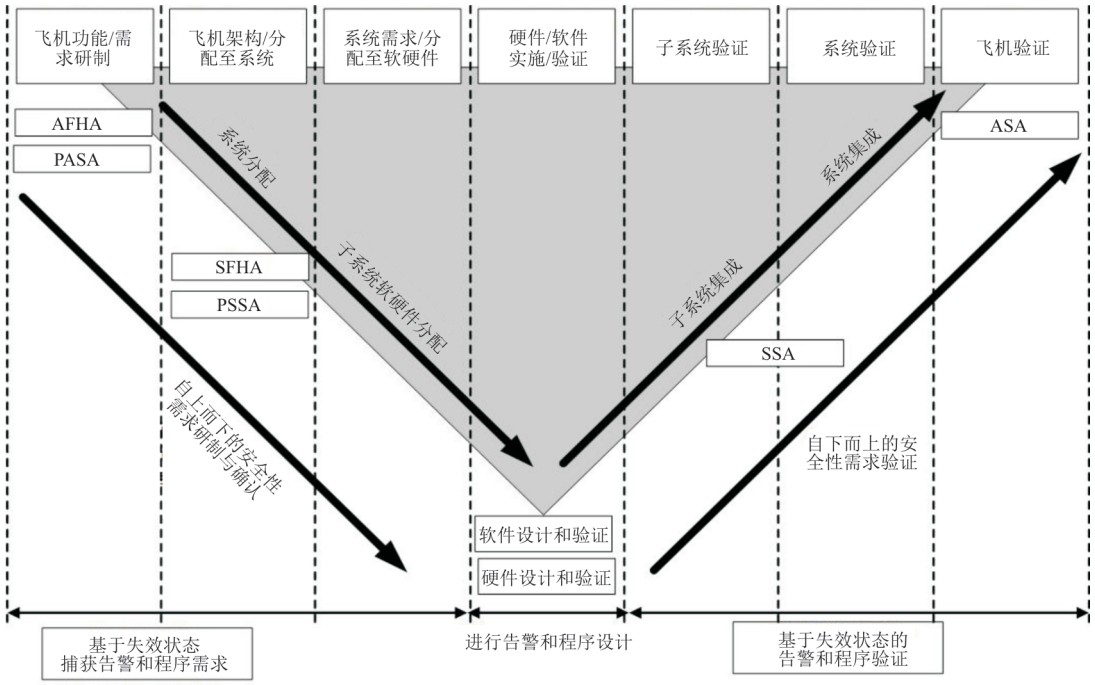
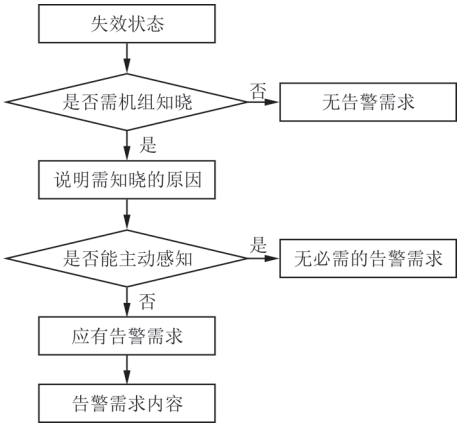


图2　安全性评估过程中的人为因素分析
Fig. 2　Human factor analysis in safety assessment

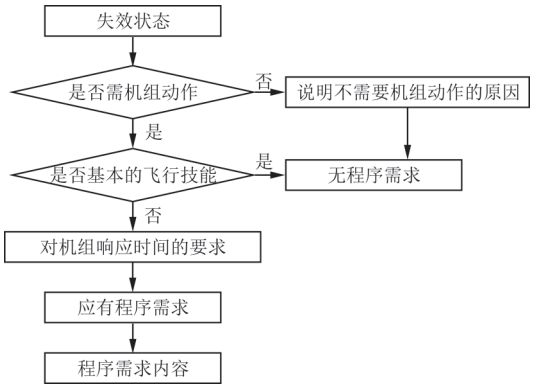
在初步设计阶段开展FHA时,飞行机组人为因素分析主要是正向捕获失效状态定级时所作的告警和操作程序相关的需求,并传递至告警和程序设计专业。在详细设计阶段完成告警和程序设计后,飞行机组人为因素分析主要是对失效状态相关联的告警和操作程序进行验证,以证明机组可以知晓系统失效并及时采取纠正/补偿动作,同时将机组差错的危险降至最低,从而确认失效状态定级的正确性,最终表明对CCAR25.1309(b)和(c)条款的适航符合性。

作为CCAR25.1309(b)和(c)条款的适航符合性的基础之一,为了充分识别FHA中失效状态定级时的人为因素假设,提出告警和操作程序的需求捕获方法,如图3所示。需要分析飞机级和系统级FHA中每一项失效状态的发觉方法和纠正/补偿动作,作为FHA中失效状态定级的假设。针对机组感知,机组发觉失效的方式主要有主动感知(例如身体感知、目视观察等)和被动感知(例如机

组告警系统、语音或灯光等告警信息)。如果需要机组知晓失效且机组无法主观感知,则必须提出告警需求。针对机组动作,如果需要机组执行操作,且该操作不是基本的飞行技能,则应提出操作程序需求。此外,机组响应时间确定了告警等级的最低要求,例如,要求机组立即知晓、随后采取纠正或补偿动作的失效应设计至少警戒级(Caution)的告警消息。



(a) 告警需求



(b) 程序需求

图 3 基于失效状态的告警和程序需求捕获方法
Fig. 3 Requirement capture method for alert and procedures based on failure conditions

2.2 人为因素分析方法

为了证明飞行机组人为因素假设、确认失效状态定级的正确性,以表明对 CCAR25.1309(b)和(c)条款的适航符合性,提出失效状态的人为因素分析方法,如表 1 所示。

表 1 失效状态的人为因素分析方法
Table 1 Human factors analysis method of failure condition

失效处理过程	适用于告警等级为警告、警戒和咨询级	适用于其他的驾驶舱效应
失效状态	失效状态名称、飞行阶段、运行和环境条件、失效影响、影响等级	同左列
机组感知	失效是否需要机组立即感知 告警的等级 告警的感知方式(视觉、听觉、触觉) 告警的表达方式(视觉信号的位置、使用的模式数目、告警的属性和特征) 机组感知到告警的最大时间	对应的初始失效、机组发现初始失效的方式 受影响的系统及其关联的驾驶舱效应 其他可观察的驾驶舱效应清单 关联的飞机物理反馈 所有驾驶舱效应出现的顺序 机组感知到告警/驾驶舱效应的最大时间
信息处理	不适用,因为机组预期可直接从告警执行程序或记忆项	假设机组能够诊断失效状态的推理过程 机组如何确定初始失效关联的系统影响的优先级 假设机组从发觉失效到作出反应的时间
机组反应	是否需要机组立即反应 在失效管理时假设使用哪一部分飞行训练大纲 假设使用的记忆项清单 假设使用的程序清单/检查单 机组是否使用基本的飞行技能 机组反应是否包括过度的工作负担、注意力集中或控制力	假设飞行机组完成动作的顺序,需描述机组动作的种类、动作的方式(即控制和信息)和顺序 是否有机组反应时间限制 在失效管理时假设使用哪一部分飞行训练大纲 假设使用的记忆项清单 假设使用的程序清单/检查单 机组反应是否包括过度的工作负担、注意力集中或控制力
失效管理	失效状态对飞机系统的影响(不工作项、不可用系统、状态可逆性等) 失效导致的运行限制(例如高度、速度、温度等) 是否有程序延迟项 使机组知晓系统状态、运行限制和程序延迟项的方法 由于失效对剩余飞行的影响,机组需手动完成哪些操作 失效是否导致过度的机组负担、注意力集中或飞行控制力 是否容易出现对飞行机组生理有影响的情况(驾驶舱内温度失控、噪音或震动过大或能见度下降等) 机组执行操作程序时可能存在的差错类型 机组执行操作程序时可能存在的具体差错 采用差错检测、差错恢复、防差错或容错的设计措施	同左列

人为因素分析方法包括两种情况,第一种情况适用于警告、警戒和咨询等级的失效告警,此时机组告警系统产生明显的告警,清晰地指向初始失效,并使飞行机组立即识别失效状态;第二种情况适用于其他的告警、指示或其他的驾驶舱效应。两种情况在机组感知和信息处理方面的分析侧重不同,第一种情况侧重于分析告警的感知方式和表达方式,第二种情况侧重于分析多种驾驶舱效应的出现对机组诊断失效并作出决策的影响。两种情况在机组反应和失效管理方面的分析基本相同。

上述方法也可用于公共资源级联影响分析,由于公共资源(例如迎角信号、轮载信号等)的级联失效可能导致多条失效状态并关联不同等级的告警或驾驶舱效应,因此公共资源的失效可能同时涉及表1的两种情况。由于AC/AMC 25.1302涉及失效状态的识别和差错管理等方面[12],可以使用14CFR/CS 25.1302相关的评估结果以补充安全性评估中飞行机组假设的分析。

3　工程应用示例

3.1　需求捕获示例

在初步设计阶段基于2.1节的方法从FHA中捕获告警和程序需求,实际应用时可进行适当裁剪,方法应用示例如表2所示。

表2　告警和程序需求捕获方法应用示例

Table 2　Example of requirement capture method for alert and procedures

失效状态					
失效状态名称	飞行阶段	运行/环境条件	失效影响		影响等级
示例:丧失一块升降舵俯仰控制	起飞、飞行中、着陆	正常条件	飞机:俯仰控制能力减弱 机组:为维持正常的俯仰,机组负担显著增加 乘客:可能感到不舒适		较大的(Major)
机组感知					
失效是否需要机组知晓	需要机组知晓的原因	机组能否主观感知失效	是否有告警需求	告警需求内容	
是	知晓该失效可以帮助机组提高情景意识,提高安全裕度	否	是	丧失一块升降舵俯仰控制时,应向机组提供至少为警戒级(Caution)的告警消息	
机组动作					
发生失效后机组是否需要执行操作	不需要执行操作的原因	是否使用基本飞行技能	对机组响应时间的要求	是否有操作程序需求	程序需求内容
是	不适用	否	立即知晓,随后采取纠正或补偿动作	是	丧失一块升降舵俯仰控制应设计专门的机组操作程序

运输类飞机通常有两块升降舵,以丧失一块升降舵俯仰控制为例,该失效状态通常定级为“较大的”,前提是机组能够知晓该失效并采取合适的纠正或补偿动作。发生该失效后,由于机组无法通过身体或目视等方式主观感知,因此应提出告警需求。由于机组需要采取纠正或补偿动作以维持正常的俯仰,且该动作不是基本的飞行技能,因此应提出操作程序需求。捕获的需求应纳入PSSA,作为告警和程序的正向设计输入。另外,在FHA的迭代更新时,应在相应失效状态的影响描述中增加机组发觉方法和机组动作的说明(例如:机组发觉,升降舵俯仰控制丧失相关的告警或指示;机组动作,使用剩余俯仰控制舵面控制飞机),以支持影响等级的确定。通过在大型客机安全性评估中应用该方法,确保了告警和程序相关假设的完整性,为CCAR 25.1309(b)和(c)条款的适航符合性验证建立了基础。

3.2　人因分析示例

在详细设计阶段基于2.2节的方法开展人为因素分析,实际应用时可适当裁剪,方法应用示例如表3所示。为了满足所捕获的需求,“丧失一块升降舵俯仰控制”通常设计有警戒级告警消息“FLT CTRL DEGRD”和操作程序“飞控系统性能

降级”。为了验证机组能够及时采取动作且机组差错风险已被降至最低，需分析机组负担和机组差错管理。程序“飞控系统性能降级”将显著(Significant)增加机组负担，结合模拟器试验结果，确认了失效状态“丧失一块升降舵俯仰控制”定为“较大的”是正确的。

分析完成后，应将分析结论纳入SSA和ASA中。通过在大型客机系统安全性评估中应用该方法，证明了失效状态关联的告警和程序假设的有效性，确认了影响等级的正确性，建立了失效状态、告警和程序之间完整的适航符合性证据链，表明了系统设计已尽量减少可能导致增加危险的机组差错；有效验证了CCAR 25.1309(b)和(c)条款的适航符合性，验证结果已获得相关审查机构的认可。

表3 人为因素分析方法应用示例

Table 3 Example of human factors analysis method

失效状态	机组感知	机组动作	
失效状态名称	告警显示方式	是否需立即执行动作	使用的程序
示例：丧失一块升降舵俯仰控制	视觉： CAS：FLT CTRL DEGRD 主告警灯：MASTER CAUTION 听觉：单谐音	否	“飞控系统性能降级”： 最大速度XXX节，小心机动 (操纵品质降级，俯仰、滚转和减速操纵能力由于可操纵舵面减少而下降) 若一侧升降舵失效：空中禁止使用减速板

失效管理					
不工作项	程序延迟项	机组负担	可能的机组差错类型	防差错设计措施	…
自动驾驶左或右侧副翼 左或右侧升降舵 两对或以上多功能扰流板减速板空中不可用(若一侧升降舵失效)	进近时：着陆构型，3卡位，超控襟翼告警 修正后的着陆参考速度：XXX节 最大侧风：XX节 修正后的实际着陆距离：XXX	显著增加	C4：对正确的目标进行了错误的检查/监控 C6：信息未获取	统一的信息显示格式 机组无需操作即可获取操作程序相关的告警信息	…

4 结 论

1) 在飞机初步设计阶段，通过人为因素需求捕获方法，识别了失效状态相关的告警和程序需求，为安全性驱动告警和程序的正向设计建立基础。

2) 在详细设计阶段，通过人为因素分析方法，确认了失效状态定级的正确性，建立了安全性评估中飞行机组人为因素的完整适航符合性证据链，实现了全寿命周期的系统安全性正向、闭环设计。本文方法的型号应用增强了审查方对申请方满足CCAR 25.1309(b)和(c)条款适航符合性的信心，填补了国产民用飞机系统安全性评估中飞行机组人为因素分析的空白。

参 考 文 献

[1] National Transportation Safety Board. Assumptions used in the safety assessment process and the effects of multiple alerts and indications on pilot performance: ASR-19-01 [EB/OL]. (2019-3-10) [2022-12-23]. https://www.ntsb.gov/investigations/accidentreports/reports/asr1901.pdf.

[2] Federal Aviation Administration. Joint authorities technical review Boeing 737 MAX flight control system [EB/OL]. (2019-10-11) [2022-12-23]. https://www.faa.gov/sites/faa.gov/files/2021-08/Final_JATR_Submittal_to_FAA_Oct_2019.pdf.

[3] Govtrack U. S. Aircraft certification, safety, and accountability: consolidated appropriations [EB/OL]. (2020-12-27) [2022-12-23]. https://www.govtrack.us/congress/bills/116/hr133.

[4] 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.
Civil Aviation Administration of China. Airworthiness standards of transport category aircraft: CCAR-25-R4[S]. Beijing: Civil Aviation Administration of China, 2011. (in Chinese)

[5] 董大勇，俞金海，李宝峰，等. 民机驾驶舱人为因素适航符合性验证技术[J]. 航空学报，2016，37(1)：310-316.
DONG Dayong, YU Jinhai, LI Baofeng, et al. Airworthiness compliance certification technology of civil aircraft flight

(下转第156页)