

技术规章条款制修订的安全性分析方法



胡天辰,蔡景

南京航空航天大学,江苏 南京 211106

摘 要:适航管理的首要目的是保障民用飞机的安全,而技术规章条款是落实适航管理的核心内容。由于我国缺乏制修订技术规章条款的经验,如何全面考虑技术规章条款制修订所涉及的安全因素,保证技术条款的安全性要求是目前面临的一个问题。本文将系统理论过程分析(STPA)融入技术规章条款制修订过程,提出了基于STPA方法的技术规章条款制修订的安全性分析方法。以运输类飞机前轮转弯系统为例,验证了欧洲航空安全局在制定相关条款时对安全因素考虑的合理性,表明所提方法的可行性和有效性,为我国制修订技术规章条款提供安全性分析方法。

关键词:技术规章条款;安全性分析;STPA方法;适航规章

中国分类号:X949

文献标识码:A

DOI: 10.19452/j.issn1007-5453.2023.01.005

适航作为民用飞机安全性的保证,已经成为业内的共识。以适航审定为核心内容的初始适航管理是保证民用飞机满足安全性的基础,其中技术规章条款是开展适航审定的基础。因此,技术规章条款的安全性要求是否充分和适宜对于民用飞机的安全至关重要。我国国产民用飞机的研制起步较晚,因此,在技术规章条款的制修订方面主要采取跟踪、参考美国联邦航空局(FAA)和欧洲航空安全局(EASA)的方式。由于我国民机的运行环境与欧美不同,再加上国产民机的研制技术水平与欧美有差距,因此,适合欧美的技术规章条款不一定适合我国。实践证明,技术规章条款制修订非常复杂,考虑因素众多,不仅需要考虑新技术、新材料在飞机上的推广应用,同时还需要考虑特定的运行环境、机队规模等因素。因此,在我国大力发展国产民用飞机的背景下,技术规章条款的制修订工作已成为我国适航管理中的重要工作之一。

技术规章条款制修订的核心内容是安全性,目前在安全性方面我国已经开展了大量的研究,如《ARP 4761:民用机载系统和设备安全性评估过程的指南和方法》中提出的功能危害性分析(FHA)、初步系统安全分析(PSSA)和系统安全性分析(SSA),以及由ARP 4754A提供的符合审定要求的全球通用性方法^[1-2]。而技术规章条款制修订是安

全、经济、技术、运行环境等众多因素综合权衡的结果,是一个系统性的工作,传统民机系统安全性设计、分析与评估的理论体系没有考虑危险因素与人为因素的相互影响,其用于分析软件密集型系统安全性的有效性正逐渐降低。为了综合考虑技术规章条款制修订所涉及的众多安全性因素,需要从系统中人、飞行器与环境等综合复杂因素及相互之间的关系出发,改进优化技术规章条款制修订的安全性分析方法。近年来,一种基于系统理论的过程分析(STPA)方法在针对软件密集型复杂系统安全性的分析上得到广泛应用。与其他方法相比,STPA利用系统和控制理论来考虑系统组件之间的相互作用对系统整体安全性的影响^[3]。

目前,基于STPA的安全性分析已被应用并扩展于各个领域。Dakwat等^[4]提出了一种将STPA和模型检查相结合的方法,提高了设计变更的一致性,以更好地解决STPA中确定安全约束的问题;Castilho等^[5]证明将STPA应用于闭环连续控制的可行性,识别轻型飞机侧风起飞的危险,以及使其执行更安全的缓解措施;刘金涛^[6]扩展了STPA的具体实施,并能够自动化实现,使其成为适合于高速列控系统的安全分析方法;赵长啸等^[7]提出了STPA-Bayes安全性分析与评价模型,支持了机载显示系统的安全性分析;史思杨^[8]

收稿日期: 2022-05-12; 退修日期: 2022-07-19; 录用日期: 2022-08-25

引用格式: Hu Tianchen, Cai Jing. Safety analysis method for formulation and revision of technical regulations[J]. Aeronautical Science & Technology, 2023, 34(01): 37-44. 胡天辰,蔡景. 技术规章条款制修订的安全性分析方法[J]. 航空科学技术, 2023, 34(01): 37-44.

提出了一种新的系统安全性分析方法——MB-STPA,识别了波音737-NG系列飞机刹车系统的风险致因;陈苗芳^[9]提出形式化的STPA控制结构的危险分析方法,对飞行器自动油门控制系统进行危险分析。在现有的研究以及与传统分析方法的对比评估中,STPA发现了传统方法可以发现的所有因果方案,并且它也发现了传统方法没有发现的软件相关非故障的场景。

通过以上分析可知,STPA分析方法具有同时考虑系统中人、飞行器与环境等综合复杂因素及相互之间关系的优点,与技术规章条款制修订需要考虑的因素非常契合。因此,本研究将STPA方法融入技术规章条款制修订过程,提出基于STPA的技术规章条款制修订的安全性分析方法,并以飞机前轮转弯系统相应的技术条款为例,验证该方法的可行性和有效性,为我国今后技术规章条款制修订提供安全性分析。

1 系统理论过程分析(STPA)方法

1.1 STPA方法简介

STPA方法由N. G. Leveson^[10]提出,这是一种适用于复杂系统危险致因的安全性分析技术,而危险可能是由部件之间的不安全相互作用以及部件故障和失效引起的。STPA基于系统一理论事故模型和过程(STAMP)来分析已识别系统危险的致因。STAMP的三个核心要点是安全约束、分层安全控制结构和过程模型^[11],认为损失是由未能有效实施安全约束造成的,而系统安全的重点从预防失效转向实施安全约束。因此,其不仅可以分析组件的失效,还可以分析组件的多方交互作用。

在具体分析过程中,STPA以控制为中心,以系统中的不安全控制行为为重点,用分层控制结构描述系统组件之间的控制关系。通过过程模型、分类和分析不安全控制行为,找出系统危险和问题的根本原因,最后根据问题的原因导出相应的安全要求。

1.2 STPA方法分析步骤

STPA方法主要分4个步骤,如图1所示。

(1) 定义分析目的。通过定义分析目的,明确该分析所要避免的损失,确定被分析的系统与系统边界。定义分析目的分为定义损失(事故)、识别系统层级危险、确定系统层级安全约束提炼危险(可选)4部分。

(2) 建立一个系统模型,称为控制结构。控制结构通过一组反馈控制回路对系统建模,以捕捉功能关系和交互。控制结构通常从更抽象的层次开始,并进行迭代调整以捕

获更多的系统细节。

(3) 识别不安全控制行为,旨在分析控制结构中的控制行为,以验证此类行为如何导致第一步中提到的损失。不安全控制行为(UCA)指的是在特定情境及最坏环境下可能导致危险的控制行为。在完成了事故与危险的识别,以及控制结构的搭建后,即可以通过评估系统设计中的安全控制来确定导致危险状态的可能性。对于不安全控制行为的分析可以分为4种情况:未提供控制行为导致危险、提供控制行为后导致危险、提供可能安全的控制行为但时间节点或顺序错误导致危险和控制行为持续时间不当导致危险。

(4) 识别致因场景,主要是识别系统中可能出现不安全控制的原因。构建适当情境以解释以下内容:出现不安全控制行为并导致损失;提供了安全控制行为却没有恰当地遵守或执行并导致损失。

一旦识别了分析对象的场景,即可用于生成其他需求、确定缓解措施、改进系统架构以及提出设计建议。

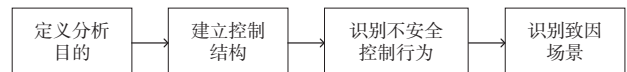


图1 STPA方法分析流程

Fig.1 STPA method analysis process

2 融入STPA的技术规章条款制修订安全性分析流程

结合过去技术规章条款制修订案例可知,飞机及发动机结构或部件发生事故、新技术的出现,以及跟随其他规章的修制订都会启动条款制修订机制。随后需要判断危险致因是否明确,如果致因不明确,则重点在于明确条款所涉及的系统,经过STPA方法分析识别出不安全控制行为与相应的致因场景;相反,如果危险致因是明确的,则无须再进行STPA分析。最后,将分析结果作为参考依据或判断现有条款对全部致因场景的包含情况对条款进行制修订。融入STPA方法进行技术规章条款制修订安全性分析的流程如图2所示。

2.1 技术规章条款涉及的系统分析

考虑到技术规章条款的持续修订和航空技术的发展,需要对适航标准进行系统的技术分析,跟踪条款的修订历史,解读适航要求的安全意图和技术含义,正确理解和把握符合性验证方法^[12]。每一条款都会针对一个特定的系统进行解释说明或要求,因此在分析技术规章条款制修订的安

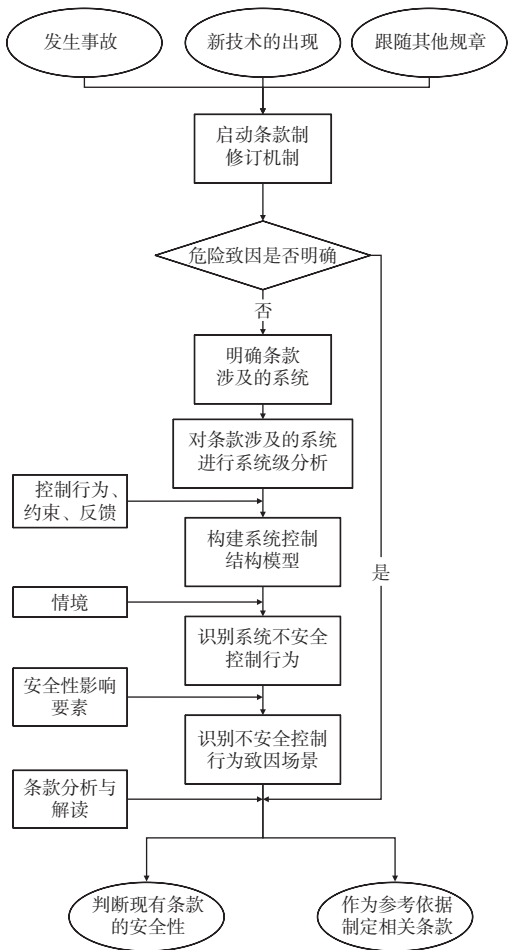


图2 融入STPA方法的技术规章条款制修订安全性分析流程

Fig.2 Safety analysis process for preparation and revision of technical regulations with STPA method

全性前,应该明确条款所涉及的系统,并且应用STPA方法进行系统级分析,以识别系统事故对应的损失以及危险。

STPA可针对利益相关者不可接受的任何损失。如果涉及多个损失,如失去生命或遭受人身伤害、交通工具丢失或受损、交通工具外部物品丢失或受损、任务失败以及客户满意度受损。由于每个STPA结果都可以追溯到一个或多个损失,因此可以简单地根据所涉及的损失按主次顺序排列分析结果。

接下来需要识别系统事故及对应的危险,对所分析的系统风险形成全局认识。系统级危险是通过识别在最恶劣环境条件下会造成损失的系统条件或状态来定义的。

2.2 构建系统控制结构

分层控制结构指的是由反馈控制回路组成的系统模型。有效地控制结构可以将约束施加到整个系统的行为

上。分层控制结构由图3中所示的反馈控制回路组成。通常,控制器可以通过提供控制行为来控制程序,并对受控过程的行为施加约束。控制算法代表控制器的决策过程,即决定提供哪些控制行为。控制器还具有其过程模型,该模型代表其先前决策的内部思想。过程模型可以包含关于受控过程或系统/环境的其他相关方面的想法。过程模型可以通过用于观察受控过程的反馈进行部分更新。一般情况下,大多系统都有几个重叠且交互控制回路。如图4所示,多个交互控制回路可通过一个分层控制结构进行建模。

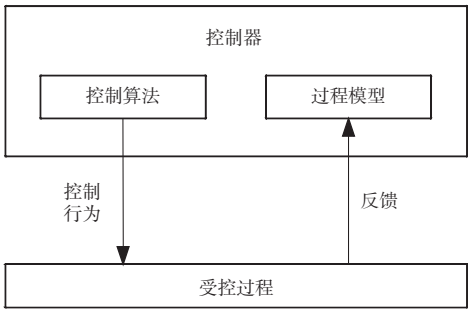


图3 一般控制回路

Fig.3 General control loop

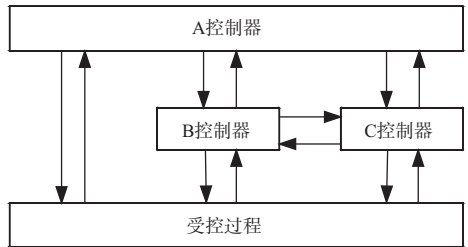


图4 一般层级控制结构

Fig.4 General level control structure

2.3 识别系统不安全控制行为

不安全控制行为指的是在特定情境及最坏环境下可能导致危险的控制行为。一旦识别出系统事故、系统级危险以及相关的安全约束,并确定了安全控制结构,即通过评估系统设计中的安全控制来确定导致危险状态的可能性。

不安全控制行为应说明在何种情境下控制行为是不安全的。每个不安全控制行为都包含5个部分:(1) 可以提供控制行为的控制器;(2) 情境;(3) 不安全控制行为的类型;(4) 控制行为或命令本身;(5) 关联所可能导致的危险。

2.4 识别致因场景

致因场景描述的是可能导致不安全控制行为以及危险的诱发因素。此时,需要考虑两类致因场景:导致不安

全控制行为的致因场景和控制行为执行不当或未被执行的致因场景。

2.4.1 识别导致不安全控制行为的致因场景

此类致因场景可通过以不安全控制行为作为起始点,反向解释是什么导致控制器提供或不提供控制行为进行创建。可导致不安全控制行为的致因场景包括:与控制器相关的故障(仅针对实际控制器)、不充分的控制算法、不安全的控制输入与不充分的过程模型。

2.4.2 识别控制行为执行不当或未被执行的致因场景

不安全控制行为可能导致危险,但如果控制行为执行不当或未被执行,没有不安全控制行为的情况下也可能导致危险。为了得到此类致因场景,我们必须考虑会影响控制路径和受控过程的因素。涉及控制路径和受控过程的致因场景包括控制行为未执行与控制行为执行不当。

2.5 依据致因对条款进行安全性评估

在识别出不安全控制行为对应的致因场景后,对现有条款进行分析,检查其是否已经涵盖了所有应该被考虑的致因场景。如果现有条款已经涵盖了所有的致因场景,可以认为其安全性满足要求,安全性评估程序结束;如果未涵盖所有致因场景,则应该考虑以此为依据启动条款制修订程序。

3 飞机前轮转弯系统技术条款案例分析

3.1 简述

飞机在地面的转向运动主要有三种转向模式:前轮转弯、不对称推力和差速制动。其中,前轮转弯可使飞机灵活转弯,并具有其他两种转向模式的功能。它还减轻了轮胎磨损和差速刹车时的局部高温现象,即使在主起落架轮胎泄漏的情况下仍能控制飞机。目前,国内外民用飞机和大多数军用飞机都使用这种方法。此外,飞机前轮转弯系统是飞机地面控制运动的重要组成部分。其各项性能指标对飞机整体地面运行的稳定性和地面机动性有着非常重要的影响^[13]。

一种飞机前轮转弯系统包含的部件有:(1) 旋转接头:旋转接头相对于L/G回缩轴同轴安装,并在齿轮延伸时提供液压电源。当齿轮开始收缩时,旋转接头切断液压电源。(2) 选择阀:当选择阀通电时,压力通过从动阀施加到伺服阀上。(3) 止回阀/过滤器:液压供电线路安装40 μ m过滤器和止回阀。(4) 伺服阀:伺服阀为偏转射流式。它配备了线性可变差动换能器(LVDT)传感器,用于检测滑动阀的位置。LVDT为转向控制提供位置反馈。(5) 可调节隔膜:

可调节隔膜用于调整流向每个驱动汽缸室的流量,从而调整机轮转向速度。(6) 止回阀:两个止回阀确保流体从蓄能器分配到转向执行器的腔室。(7) 旁通阀:在液压系统降压的情况下,旁路阀将转向执行机构的两个腔室互连。如果压力超过273bar(4000lb/in²,即27300kPa),旁通阀就会打开。(8) 防摆阀:每个转向执行器室有一个防摆阀,以防止摆振。(9) 转向执行器:转向执行器通过齿条和齿轮组件驱动旋转管,这是NLG结构的一部分。(10) 蓄压器:防摆振蓄压器在转向执行器的两个腔室之一出现气穴时提供加压液体。蓄能器可以提供压力高达15bar(220lb/in²,即1500kPa)的液体加压。(11) 放气螺钉:放气螺钉允许液块放气和减压。上述部件对应的一种飞机前轮转弯系统原理简图如图5所示。

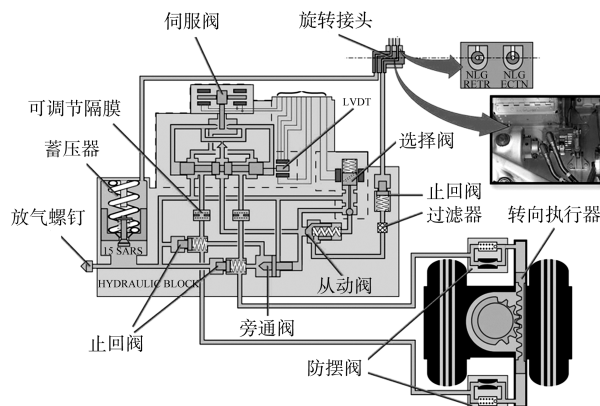


图5 飞机前轮转弯系统原理简图

Fig.5 Schematic diagram of aircraft nosewheel turning system

目前,FAA和中国民用航空局(CAAC)的适航规章尚无针对前轮转弯系统的条款。只有EASA发布的大型飞机审定规范(CS-25)部25.745条为针对前轮转弯系统的条款^[14],其针对前轮转弯系统在不同环境条件下的控制情况、与其他系统的干涉以及各部件失效对系统安全性的影响等方面提出了要求。

本研究融入STPA方法,对CS-25部25.745条飞机前轮转弯系统技术规章条款进行安全性分析,为将来我国运输类飞机前轮转弯系统相关及其他技术规章条款的建立提供安全性分析。

3.2 融入STPA的安全性分析

3.2.1 飞机前轮转弯系统技术规章条款制修订启动机制

未来,我国可能会跟随制定飞机前轮转弯系统相关技术条款,并且尚不明确可能导致系统危险的致因场景,因此需要应用融入STPA的安全性分析方法进行分析。

3.2.2 系统级分析

根据STPA的定义,可得到关于飞机前轮转弯系统的系统级事故包括:所有相关人员的受伤和死亡(A1)、飞机机体或各子系统遭到结构破坏或机械故障(A2)和所有相关的地面或移动设施和设备的损毁(A3)。

系统级危险是指可能导致A1~A3的一系列灾难性后果的事件。飞机前轮转弯系统在日常运行中出现的危险主要有^[15]:(1)转弯操纵无法脱开(H1),导致拖行时转弯机构受力过大而损坏,另外导致收放起落架时前轮没有处于中立位置,使舱门等部件损坏;(2)转弯操纵困难(H2),前轮转弯操纵费力或者左右偏转角度变小,会造成无法控制角度及反馈前轮位置等现象;(3)转弯功能失效(H3),是前轮转弯系统级危险中最为严重的,轻则导致航班延误,影响其他飞机的正常起飞,重则导致轮胎严重磨损甚至爆破,影响机上人员的安全。

针对事故A1,转弯功能失效(H3)为可能导致人员受伤或死亡的危险情况;事故A2涉及上述H1、H2、H3三种危险;事故A3涉及上述H2、H3两种危险。通过上述分析,可以得到系统级危险与事故的关联关系,见表1。

表1 系统级事故与危险对应表

Table 1 Corresponding table of system level accidents and hazards

危险编号	危险描述	对应的事故
H1	转弯操纵无法脱开	A2
H2	转弯操纵困难	A2, A3
H3	转弯功能失效	A1, A2, A3

3.2.3 控制—反馈结构的构建

转弯系统处于正常工作状态时,飞行员可以根据需要自主控制转弯系统的工作方式,通常包括手轮转弯、脚蹬转弯和转弯减摆三种方式。手轮转弯用于低速滑行时进行大角度转弯,可以使飞机获得良好的地面机动能力,转弯手轮手柄中心通常设有“脚蹬转弯断开”按钮,按下该按钮将断开脚蹬转弯功能,可以减少前轮胎的磨损;脚蹬转弯用于中高速滑跑过程中小角度修正滑跑方向,使飞机获得良好的保持方向的能力;当转弯开关断开时,转弯系统断开,前轮进入转弯减摆状态,此时前轮为无动力转弯。

根据飞机前轮转弯系统原理,飞行员和转弯控制单元(SCU)为控制器,转弯作动系统(控制阀、作动筒)、驾驶舱部件(手轮、脚蹬、开关)等为执行机构,机轮、液压系统为被控过程,传感器有前轮位置传感器、转弯指令传感器等,部件间存在逻辑和功能上的控制与反馈关系,图6为正常前轮转弯模式时系统的安全控制—反馈结构。

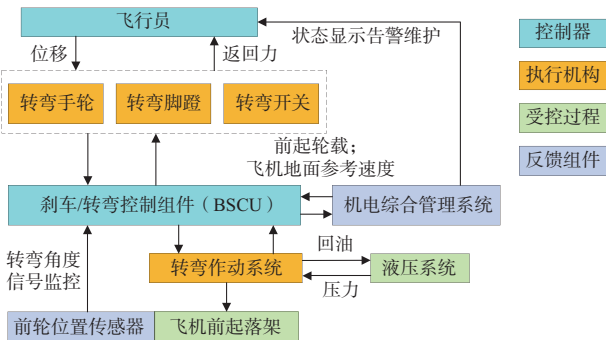


图6 飞机前轮转弯系统控制结构示意图

Fig.6 Control structure diagram of aircraft nosewheel turning system

3.2.4 识别不安全控制行为

转弯操纵无法脱开(H1)、转弯操纵困难(H2)、转弯功能失效(H3)均属于严重度较高的危险,涉及的事故类型也比较多,因此具有重要的研究意义。接下来将进行识别不安全控制行为的示例分析。

根据飞机前轮转弯系统原理和安全控制—反馈结构模型可确定系统中的控制器有飞行员和SCU,其中飞行员的控制行为有控制转弯系统工作方式(CA1)和操作驾驶舱转弯系统执行机构(CA2);SCU的控制行为有实施前轮转弯操作(CA3)和控制转弯系统开关状态(CA4)。可以识别出不安全控制行为见表2。

3.2.5 识别致因场景

在确定可能导致危险的不安全控制行为后,需要根据飞机前轮转弯系统的控制—反馈结构图以及不安全控制行为分类依据进一步确定其产生的原因。根据第二节所述致因场景分类,识别出的全部致因场景包括与控制器相关致因10条,与不充分的控制算法相关致因4条,与不充分的控制输入相关致因2条,与执行器及受控过程相关的故障及缺陷相关致因14条,与和反馈有关的故障及缺陷相关致因7条。部分致因场景见表3,其中致因标号的第一位表示由对应编号控制行为的不安全控制行为识别而来。

3.2.6 依据致因进行安全性评估

从EASA发布的《大型飞机的审定规范和可接受的符合性方法》(CS-25)^[16]查阅得到,涉及飞机前轮转弯系统的条款第25.745条包括以下内容:

(1) CS-25.745(a)条款除非前轮转向系统仅限于低速操纵,否则其设计必须确保在起飞和着陆期间(包括侧风情况)以及在起飞运行期间的任何阶段动力装置突然发生故障时,其使用不需要特殊技巧。这必须通过测试来证明。

表2 不安全控制行为列表
Table 2 List of Unsafe Control Activities(UCAS)

控制行为(CA)	没有提供安全控制行为	提供了导致危险的控制行为	提供安全控制行为时序不当	提供安全控制行为持续时间不当
CA1: 控制转弯系统工作方式	UCA1-1-1: 在飞机滑跑阶段, 没有选择转弯系统工作方式	UCA1-2-1: 低速滑跑时采用脚踏控制前轮转弯; UCA1-2-2: 中高速滑跑时采用手轮控制前轮转弯	UCA1-3-1: 滑跑时断开转弯开关, 使飞机失去前轮转弯动力; UCA1-3-2: 地面拖行时没有断开转弯开关	
CA2: 操作驾驶舱转弯系统执行机构	UCA2-1-1: 未提供前轮转弯操作	UCA2-2-1: 操作转弯系统执行机构压力过大; UCA2-2-2: 操作转弯系统执行机构压力过小	UCA2-3-1: 在飞机滑跑进入弯道前提供前轮转弯操作; UCA2-3-2: 在飞机滑跑进入弯道后仍未提供前轮转弯操作	UCA2-4-1: 持续提供前轮转弯操作; UCA2-4-2: 过早结束提供前轮转弯操作
CA3: 实施前轮转弯操作	UCA3-1-1: 在飞机滑跑时, 未提供前轮转弯操作	UCA3-2-1: 提供的前轮转弯操作幅度过大; UCA3-2-2: 提供的前轮转弯操作幅度较小	UCA3-3-1: 飞机还未进入弯道便提供前轮转弯操作; UCA3-3-2: 在飞机进入弯道后仍未提供前轮转弯操作	UCA3-4-1: 持续提供前轮转弯操作; UCA3-4-2: 过早结束提供前轮转弯操作
CA4 控制前轮转弯系统开关状态	UCA4-1-1: 在飞机滑跑时未控制前轮转弯系统开关状态		UCA4-3-1: 滑跑时提供断开转弯开关操作, 使飞机失去前轮转弯动力; UCA4-3-2: 地面拖行时没有提供断开转弯开关操作	

表3 致因场景列表(部分)
Table 3 Causal scenario list (part)

致因分类	不安全控制行为致因场景
与控制器相关的故障(飞行员/SCU)	RC1-1: 飞行员对地面情况及地面参考速度认识不足; RC2-1: 飞行员间误认为对方提供了前轮转弯动作, 且无提示; RC3-1: SCU中输入卡故障, 导致无指令输入; RC4-1: 驾驶舱显示装置失效, 导致飞行员收到的速度信号无效
不充分的控制算法	RC3-5: 滑跑时, 实施前轮转弯的安全飞机地面速度设置不当; RC3-7: SCU控制律设置不当, 对实施前轮转弯指令计算错误
不充分的控制输入	RC3-9: SCU的输入通道失效, 导致传输数据无效; RC3-10: 传输通道受电磁干扰, 导致收到的数据信号错误
与执行器及受控过程相关的故障及缺陷	RC3-11: 转弯控制阀老化、故障, 无法传输液压压力; RC3-12: 转弯作动筒失效、卡滞, 导致无响应; RC3-24: 液压系统管路接头未密封, 油液外漏, 液压油无法输入; RC4-3: 两个前轮胎压相差过大, 造成滑偏; RC4-6: 主起落架一侧或者一个刹车因为故障产生了非指令性的刹车, 导致产生额外侧向力, 发生不当偏转
与反馈有关的故障及缺陷	RC2-3: 机电综合管理系统未向飞行员反馈故障告警维护状态; RC3-25: 传感器故障, 导致监测值失效, SCU对飞机滑跑状态不能做出正确的判断; RC4-7: 传感器失效, 反馈信号延迟, 导致检测信号时间过长

该条款明确说明在起飞、着陆遭遇侧风及动力装置失效的情况下, 无须使用特殊技巧, 即专用设备——转弯手轮, 通过脚踏即可实现纠偏功能。此条涵盖 RC1-1 等与操作方式选择相关致因场景。

(2) CS-25.745(b) 条款必须证明, 在任何实际情况下, 飞行员转弯控制装置的移动(包括起落架缩回或伸展期间

或缩回后的移动)不会干扰起落架的正确缩回或伸展。

该条款主要描述了前轮转弯与起落架收放运动的干涉情况。具体需要通过控制器逻辑以及前起落架转轴处液压控制装置实现。此条主要涵盖 RC3-7 等 6 条与控制算法及模型相关致因场景。

(3) CS-25.745(c) 条款在故障条件下, 系统必须符合

CS-25.1309(b)和(c)的要求。系统的布置必须确保没有单一故障会使前轮处于导致危险影响的位置。如果依靠前轮转向来证明其符合CS-25.233条的要求,则必须证明前轮转向系统符合CS-25.1309条的要求。

该条款重点需要考虑“确保没有单一故障会使前轮处于导致危险影响的位置”。此条主要涵盖RC3-11等14条与执行器及受控过程相关致因场景。

(4) CS-25.745(d)条款前轮转向系统、牵引附件和相关元件必须通过适当的方式进行设计或保护,以便在通过独立于飞机的方式进行地面操纵操作期间,排除了影响前轮转向系统安全操作的损坏;如果可能发生损坏,则在开始滑行前向机组发出警报。

该条款主要描述了在“牵引”时,不会对前轮转弯系统产生损坏,如果可能产生损坏,则在开始滑行前向机组发出警报。此条主要涵盖RC2-3等7条与受控过程及反馈相关致因场景。

(5) CS-25.745(e)条款除非前轮在下降时自动处于前后姿态,否则必须在前轮最初处于所有可能的偏心位置时证明成功着陆。

该条款要求验证飞机前轮在任何可能偏转角度下都可以保证飞机成功着陆。此条款描述着陆过程,不在上述分析范围内,故不予分析。

由上述分析可以得出:对于飞机前轮转弯系统,EASA发布的审定规范CS-25.745条款将大多数控制器、执行器及反馈相关致因场景考虑在内,我国CCAR-25部在建立飞机前轮转弯系统条款制修订时,可以将以上致因作为依据进行符合性验证;而CS-25.745条款对RC2-1等飞行员之间的交流及决策过程等人为因素可能造成危险的致因没有进行充分考虑,在进行条款制修订时可作为参考进行补充。

4 结论

通过研究,可以得出以下结论:

(1) 本研究将系统理论过程分析(STPA)方法融入技术规章条款制修订的安全性分析,同时考虑系统控制结构中人、飞机与环境等维度及其相互关系,提出了基于STPA方法的技术规章条款制修订的安全性分析方法。

(2) 本研究以运输类飞机前轮转弯系统为例,利用所提的安全性分析方法,验证了EASA在制定相关条款时对安全考虑的合理性,表明方法的可行性和有效性,为我国制修订飞机前轮转弯系统相应及其他技术规章条款提供安全性分析方法。

AST

参考文献

- [1] 徐小杰,宫蓁,吴洋,等. 基于模型的初步飞机安全性分析方法研究[J]. 航空科学技术, 2021, 32(11):64-69.
Xu Xiaojie, Gong Qi, Wu Yang, et al, Research on preliminary aircraft safety analysis method based on MBSA[J]. Aeronautical Science & Technology, 2021, 32(11):64-69. (in Chinese)
- [2] 宫蓁,张东辉. 基于ARP 4754A的民用飞机研制过程符合性应用实施研究[J]. 航空科学技术, 2021, 32(11):45-49+18.
Gong Qi, Zhang Donghui. Research on compliance application implementation of civil aircraft development process based on ARP 4754A[J]. Aeronautical Science & Technology, 2021, 32(11):45-49+18. (in Chinese)
- [3] 崔利杰,田宇,丛继平,等. STPA与ARP4761中的安全性分析方法对比研究[J]. 航空工程进展, 2020, 11(4):508-516.
Cui Lijie, Tian Yu, Cong Jiping, et al. A comparative study on the safety analysis methods of STPA and ARP4761[J]. Advances in Aeronautical Science and Engineering, 2020, 11(4):508-516. (in Chinese)
- [4] Dakwat A L, Villani E. System safety assessment based on STPA and model checking[J]. Safety Science, 2018, 109:1-15.
- [5] Castilho D S, Ligia M S. Urbina, Donizeti de Andrade. STPA for continuous controls: A flight testing study of aircraft crosswind takeoffs[J]. Safety Science, 2018, 108:5-14.
- [6] 刘金涛. 基于STPA的需求阶段的高速列车运行控制系统安全分析方法研究[D]. 北京:北京交通大学, 2015.
Liu Jintao. A safety analysis method for high-speed railway train control system in requirements phase based on STPA[D]. Beijing: Beijing Jiaotong University, 2015. (in Chinese)
- [7] 赵长啸,李浩,董磊,等. 基于STPA-Bayes模型的机载平视显示系统安全性分析与评价[J]. 系统工程与电子技术, 2020, 42(5): 1083-1092.
Zhao Changxiao, Li Hao, Dong Lei, et al. Safety analysis and evaluation of airborne HUD system based on STPA-Bayes model[J]. Systems Engineering and Electronics, 2020, 42(5): 1083-1092. (in Chinese)
- [8] 史思杨. 基于MB-STPA的飞机刹车系统安全性分析方法研究[D]. 天津:中国民航大学, 2020.
Shi Siyang. Research on safety analysis method of aircraft brake system based on MB-STPA[D]. Tianjin: Civil Aviation University of China, 2020. (in Chinese)

- [9] 陈苗芳. STPA中危害分析和安全性需求捕获的自动化技术研究[D]. 南京:南京航空航天大学, 2019.
- Chen Miaofang. Research on automation technology of hazard analysis and safety requirement capture in STPA[D]. Nanjing: Nanjing University of Aeronautics and Astronautics, 2019. (in Chinese)
- [10] Leveson N G, Thomas J. STPA handbook [EB/OL]. [2019-07-22]. http://psas.scripts.mit.edu/home/get_file3.php?name=STPA_handbook_chinese.pdf.
- [11] 李浩. 基于STAMP理论的机载显示系统安全性分析方法研究[D]. 天津:中国民航大学, 2020.
- Li Hao. Research on safety analysis method of airborne display system based on the STAMP theory[D]. Tianjin: Civil Aviation University of China, 2020. (in Chinese)
- [12] 杨建忠. 运输类飞机适航要求解读第三卷:设计与构造[M]. 北京:航空工业出版社, 2013.
- Yang Jianzhong. Interpretation of airworthiness requirements for transport aircraft, Volume III: Design and construction[M]. Beijing: Aviation Industry Press, 2013. (in Chinese)
- [13] 刘喜藏. 飞机前轮转弯系统仿真建模与分析[C]//第十五届中国航空测控技术年会, 2018.
- Liu Xicang. Modeling and analysis of aircraft nose wheel steering control system[C]//The 15th China Aviation Measurement & Control Technology Conference, 2018. (in Chinese)
- [14] 王浩. 大型民用飞机前轮转弯系统适航条款研究[J]. 科技视界, 2017(1):370-371.
- Wang Hao. Research on airworthiness terms of nose wheel steering system of large civil aircraft[J]. Science & Technology Vision, 2017(1):370-371. (in Chinese)
- [15] 刘伟. MA600前轮转弯系统常见故障分析[J]. 科技创新与应用, 2016(33):59-60.
- Liu Wei. Analysis of common faults of MA600 nose wheel steering system[J]. Technology Innovation and Application, 2016(33):59-60. (in Chinese)
- [16] CS-25 Certification specifications and acceptable means of compliance for large aeroplanes [S]. EASA, 2021.

Safety Analysis Method for Formulation and Revision of Technical Regulations

Hu Tianchen, Cai Jing

Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China

Abstract: The primary purpose of airworthiness management is to ensure the safety of civil aircraft, and the provisions of technical regulations are the core content of airworthiness management. Due to the lack of experience in the formulation and revision of technical regulations in China, how to comprehensively consider the safety factors involved in the formulation and revision of technical regulations and ensure the safety requirements of technical regulations is a problem. In this study, system theory process analysis (STPA) is integrated into the formulation and revision process of technical regulations, and a safety analysis method of technical regulations based on STPA method is proposed. Taking the front wheel turning system of transportation aircraft as an example, the rationality of EASA's consideration of safety factors in formulating relevant provisions is verified, which shows the feasibility and effectiveness of the proposed method, so as to provide a safety analysis method for the formulation and revision of technical regulations in China.

Key Words: technical regulations; safety analysis; STPA method; airworthiness regulations