

信息。如果运行或性能没有受影响或没有受到显著的影响,且如果认为机组采取纠正动作比无动作更为危险时,信息和告警指示可以在飞行的某些特殊阶段得到抑制。

定期维修或飞行机组检查以探测不期望发生的重大潜在失效,不应替代实际的和可靠的失效监控和指示。CS 25 AMC 25.1309 第 12 段落提供了定期维修和飞行机组检查的进一步指导。

需特别关注开关或其他互相关联的控制装置,目的是最小化不利的错误机组动作的发生可能,尤其在紧急情况或高工作负荷的阶段。额外的防护,例如使用防护的开关,有时可能是需要的。

3.3 电传飞行控制系统构造相关的主要专用条件和解析

3.3.1 操纵面位置感知

3.3.1.1 专用条件内容

对采用电传操纵系统的飞机,操纵面位置感知专用条件建议如下:

除了满足 CCAR 25.143, 25.671, 25.672 和 25.1322 的要求,当不是由机组人员操作而导致的操纵面接近极限位置时,需要机组人员操作返回正常飞行包线和(或)继续安全飞行时,应该向机组人员提供适当的飞行操纵面位置指示,除非已存在的指示足以提示机组人员相关的动作。

3.3.1.2 背景说明

电传飞行控制系统采用指令响应的方式来对飞机进行控制,飞行控制计算机对操纵面的操纵权限从以前增稳系统的部分权限变为全权限。在飞行机动过程中,驾驶员的操纵输入与操纵面的偏度没有直接的对应关系,驾驶员并不确切知道操纵面的偏转位置。一些非正常飞行条件,如大气状态、飞机、发动机故障等,可能导致操纵面达到或接近满偏。如果机组人员没有意识到多出的操纵面偏转或接近满偏,驾驶员或自动驾驶系统继续操纵可能导致飞机失控,或者其他不安全的操纵和性能特征。

目前,适航规章并没有涵盖电传飞行控制系统此新颖设计特征的相应要求,需制订相应专用条件,提出达到与规章相同安全水平的适航要求。

3.3.1.3 专用条件解析

专用条件中“适当的指示”含义为:需要考虑一些驾驶员需要进行的与飞机性能极限相关的机动情况(如快速滚转),这种情况下舵面也可能达到极限位置。因此,如果一个简单的舵面位置指示系统可能在驾驶员有意操纵导致的舵面满偏和无意进入的舵面满偏两种情况都会发出指示,则需要进行某种平衡,即能够给出需要的位置感知但又不会对驾驶员的操纵造成干扰。

3.3.1.4 建议的符合性方法

对该专用条件,建议的符合性方法如下:

- (1) MC1(设计说明),对主飞行控制系统架构描述、CAS信息逻辑描述。
- (2) MC6/MC8(飞行试验/模拟器试验),飞行控制系统和操纵品质试飞或模拟器试验。

3.3.2 指令信号完整性

3.3.2.1 专用条件内容

除考虑CCAR25.671和CCAR25.672要求以外,飞机还应满足如下要求:

- (1)无论飞机集成系统环境出现任何故障,或环境内部或外部的干扰,飞行控制系统都必须能持续地执行其预期的功能。
- (2)任何气动力回路内发生故障的系统,不应产生不安全水平的非指令性动作,并应具有在故障影响消除后,自动恢复执行关键功能的能力。
- (3)气动力回路内的系统,在暴露于任何故障源之中或暴露后,不应受到不利的影响。
- (4)由于故障、内部或外部干扰导致的单个单元或组件损坏,同时这些损坏需要通告机组,要机组采取措施,则必须经审查组识别和批准,以保证机组能够识别,同时还应保证建议的机组动作能产生预期的效果,使飞机继续安全飞行和着陆。
- (5)由虚假信号,如内部或外部干扰,或是功能故障引发的,导致系统从正常模式到降级模式的自动转换,必须满足适当的概率要求。
- (6)暴露于内部或外部干扰,或是功能故障的虚假信号,不应导致大于允许概率的危害。必须评估对操纵品质的影响。
- (7)必须表明飞行控制系统信号或者不能被无预期地改变,或者已被改变的信号满足以下要求:
 - a. 对所有的操纵面闭环系统,能保持稳定的增益和相位裕度,这一要求不包括飞行员控制输入。
 - b. 应提供足够的俯仰、滚转和偏航能力来提供持续安全飞行和着陆所需的控制。
 - c. 对气动力回路内部的系统,由虚假信号引发的影响,一定不能产生使飞机性能不可接受的瞬变或降级。尤其是会造成控制面作动器明显非指令动作的信号必须易于被检测和抑制,或是通过其他方法使舵面动作得到有效的控制,小幅值的剩余振荡是可接受的。
- (8)必须表明控制面闭环系统的输出不会导致飞行控制面非指令性的持续振荡。对于较小的不稳定性影响,通过充分的评审、记录和认知是可接受的。

3.3.2.2 背景说明

对于采用电子飞行控制系统(EFCS)的飞机,飞机的飞行控制系统包含数字设备、软件及电子接口,并通过发送指令信号来控制飞机。这些信号对干扰可能是敏感的,可能导致不可接受的系统响应。因此,必须保证从机组和(或)任何自动飞行设备发出的指令信号不会因其内部或外部干扰的单独或共同作用而发生不利的

改变。

传统的飞行控制系统通常采用机械或液压-机械方式将指令信号传输到主、辅控制面。

由于可将失效状况划分为有限数量的类别(如维修错误、卡阻、脱开、机械元件的失控或失效、液压元件的结构失效等),因此,能够相对直接地确定干扰指令传输的原因。此外,传统飞行控制系统,几乎总能辨识出最严酷的失效状况,这些失效状况可以覆盖引发相同后果的其他状况。但对于包含数字设备、软件和电子接口的EFCS而言,经验表明来自内部和(或)外部的干扰源对电子数字传输线路上的信号产生干扰不是不可能的。而且考虑到EFCS设备的复杂性,失效状况并不能像传统机械控制系统那样容易被预测、分类和处理。

现行CCAR25中的相关条款(如第25.671和25.672条)主要是针对传统飞行控制系统制订的,这些条款没有对指令的完整性和控制信号不得因内外干扰而改变规定专门要求。因此,根据CCAR21.16的要求,需要制订专用条件以保持和现行CCAR25部等效的安全水平。

3.3.2.3 专用条件解析

本专用条件所指“干扰”,是在任何条件下生成的能够使指令信号背离其预期特性的信号,这种干扰可分为下列两类。

1) 可能修改指令和控制信号的内部原因

- (1) 数据位的丢失。
- (2) 有害的瞬变。
- (3) 计算机能力饱和。
- (4) 微处理机对信号的异步处理。
- (5) 传输延迟的不利影响。
- (6) 数字信号的低分辨率。
- (7) 传感器噪声。
- (8) 不可靠的传感器信号。
- (9) 混淆效应。
- (10) 不合适的传感器监控门限。
- (11) 相互作用并可能反馈进入系统运行的结构影响。

2) 可能修改指令和控制信号的外部原因

- (1) 闪电。
- (2) 电磁干扰影响(EMI)(如马达效应,机载电源干扰、电源切换瞬变,影响飞行控制的小幅值信号及电气失效瞬变等)。

(3) 高强度辐射场(HIRF)。由上述两类中任何干扰生成的虚假信号和(或)错误数据可能会导致飞行控制系统功能不正常,这种功能不正常可能会产生不可接受的系统响应,这些响应同样会在传统机械控制系统中出现,例如:有限周期/振荡失

效、非指令运动/急偏、断开、锁死和错误的指示/告警。既然上述系统任一响应都表现为一种飞行危险。那么,就必须强制要求指令信号保持连续,并能不受内部和外部虚假信号源干扰和共因失效影响。因此,应该使用特殊的设计手段使系统完整性保持在至少等效于传统的液压-机械设计所具有的安全水平。如果对研发方法和定量/定性符合性证据给予了特别的关注,这些专门的设计手段可通过系统安全性分析过程进行监控。

3.3.2.4 建议的符合性方法

对该专用条件,建议的符合性方法如下:

(1) MC1(设计说明)——通过说明系统设计的架构和逻辑来表明满足专用条件要求。

(2) MC3(安全评估)——通过对主飞行控制系统的安全性分析和共模分析来表明信号改变不会导致灾难性情况。

(3) MC4(实验室试验)——对于改变型号的探测软件,按照 DO178B 和 DO254B 要求进行软硬件试验。

(4) MC6/MC8(飞行试验/模拟器试验)——进行飞行控制系统该故障条件下的试飞或者模拟器试验,特别是关注在故障后飞行控制系统重构过程中的过渡过程试验。

3.3.3 经协调一致的第 25.671 条

3.3.3.1 专用条件内容

ARAC 2001 年 3 月 19 日起草并提出的最终版本的第 25.671 条提案可以按照 CCAR21.16 关于专用条件的规定作为专用条件,具体内容如下。

第 25.671 条总则

(1) 每个操纵器件和操纵系统对应其功能必须操作简便、平稳和确切。操纵系统应被设计成能够持续工作并且不能妨碍飞机从任何姿态恢复。

(2) 飞行操纵系统的每一元件必须在设计上采取措施以使由于装配不当而导致系统失效而无法执行其期望功能的概率减至最小。仅在设计手段无法实现的情况下,可以采用在元件上制出明显可辨和永久性标记的方法。

(3) 必须用分析、试验或两者兼用来表明在正常飞行包线内,发生飞行操纵系统和操纵面(包括配平、升力、阻力和感觉系统)的下列任何一种失效,包括卡阻后,不要特殊的驾驶技巧或体力,飞机仍能继续安全飞行和着陆。可能出现的失效必须只产生微小的影响,而且必须是驾驶员易于采取对策的:

a. 除(c)(3)款中定义的失效类型以外的任何单个失效。

b. 未表明是概率极小的失效的任意组合。此外,当操纵系统中已存在任何单个失效的情况下,任何额外的、会妨碍持续安全飞行和着陆的失效状态,其组合概率应小于 1/1000。本条不包括(c)(3)款中定义的失效类型。

c. 任何导致操纵面或驾驶员操纵卡阻的失效或事件,卡阻指由于物理冲突,操

纵面或驾驶员操纵器件被固定在某个位置处。卡阻必须按照下列情况进行评估：

- (a) 必须考虑任何正常使用位置的卡阻；
 - (b) 必须假设，可能出现的单个失效或失效组合发生在除着陆前瞬间的正常飞行包线内的任何位置。考虑到起动改回的时间延迟，着陆前瞬间不足以实现改回；
 - (c) 当已存在本小条规定的单个卡阻情况下，任何额外的、会妨碍持续安全飞行和着陆的失效状态，其组合概率应小于 1/1000。
 - d. 任何飞行操纵器件滑移到不利位置的失控情况，如果这种失控可由单个失效或失效组合引起，且不是极不可能的。
- (4) 飞机必须设计成所有发动机在飞行中的任何点全部失效的情况下仍可操纵，且有从进近和平飘至着陆的可能。如果表明分析方法是可靠的，则可以通过分析来表明满足本要求。
- (5) 系统设计必须保证任何时候主要控制器件接近控制权限限制时，能够被机组适当地感知。
- (6) 如果系统的设计使其具有多种工作模式，则当任何工作模式显著改变或降低飞机的正常操纵特性或品质时，必须向机组提供指示信息。

3.3.3.2 背景说明

CCAR25.671 用于确保飞行控制系统的基本完整性和可用性，确保服役过程中曾发生的任何失效是飞行机组能处理的，且不妨碍飞机持续安全飞行和着陆。

FAA 的一个 ARAC 工作组已经提供一份关于第 25.671 条修订的新提案以及相关的咨询材料。启动该提案研究的原因包括：协调各方要求的工作结果、国家运输安全委员会(NTSB)对事故调查的分析结果以及更新近年来用于处理电子飞行控制系统(EFCS)专用条件的要求。ARAC 协调工作组提供的第 25.671 条修正提案以及相关咨询材料中就非正常姿态下的恢复、防止维修差错风险、特定的隐性失效风险、飞行控制卡阻和失控、所有发动机故障下的可控性以及飞行机组感知操纵权限限制，提出新的要求或明确原文要求。

3.3.3.3 专用条件解析

相较于现行的 CCAR25.671，该专用条件的变化包括：

- (1) 第 25.671(a)条增加了可以在任何飞行姿态下操纵的要求。
- (2) 第 25.671(b)条将“设计手段无法实现的情况下”作为“仅通过标记来确保正确装配的”前提。
- (3) 第 25.671(c)(1)条澄清了何种卡阻将从“任何单个故障”中排除。将“极不可能”从可接受的符合性方法中去除。
- (4) 第 25.671(c)(2)条在数值分析中加入了 1/1000 的特定风险值，说明何种卡阻故障将被排除。
- (5) 第 25.671(c)(3)条提供了卡阻定义。将“极不可能”从可接受的符合性方法中去除。在附加失效状态中加入 1/1000 的特定风险分析。增加了覆盖着陆前的

时间段难度的认知。

(6) 第 25.671(c)(4)条重点考虑了滑移到失控的要求。要求针对单个故障情况进行考虑,无论可能性大小。

(7) 第 25.671(d)条在飞行中任何情况下,将考虑的全发失控故障,要求飘降能力。

(8) 新增第 25.671(e)条增加了对操纵器件达到控制权限限制时的感知要求。

(9) 新增第 25.671(f)条增加了对飞行控制系统控制模式通告的要求。

3.3.3.4 建议的符合性方法

对该专用条件,建议的符合性方法如下:

(1) MC1(设计说明)——通过系统设计和逻辑描述来表明满足专用条件要求。

(2) MC2(分析/计算)——分析第 25.671(d)条要求的飞机在所有发动机失效情况下继续受控飞行、进近和拉平落地的能力。

(3) MC3(安全评估)——通过对飞行控制系统的安全性分析来表明导致不能继续安全飞行和着陆的故障概率为极不可能。

(4) MC6/MC8(飞行试验/模拟器试验)——进行飞行控制系统在故障条件下的试飞或者模拟器试验,表明在专用条件第 25.671(c)条指定的故障条件下仍能继续安全飞行和着陆。演示第 25.671(e)(f)条要求的信息通告功能。

4 面向适航的电传飞行控制系统的设计

4.1 概述

现代民机通常都包含高度复杂或综合的可实现飞机级需求的系统。飞机级需求包括客户/乘客要求、适航/安全性需求、成本要求以及项目管理和开发者团队等需求。为取得民机适航证,需要在飞机及电传飞行控制系统的设计中,将适航规章的要求(法规要求)作为飞机开发的顶层需求或要求,由于适航规章本身并不是直接可引用的工业标准或工程设计规范,所以需要有一种方法,即民机系统设计中所谓的“form must follow function”方法,将相当部分的适航规章要求,典型的如第25.1301、25.1309条,通过飞机级功能及其FHA(功能危害性评估)转换成工程需求,并传递到飞机的有关系统如电传飞行控制系统。因此,为确定电传飞行控制系统的需求,需要从飞机级的功能(功能性需求)和功能危害性分析着手,采用典型的自上而下的正向设计方法落实适航规章要求。

4.1.1 飞机级功能定义过程

为使电传飞行控制等飞机的系统设计满足飞机开发的顶层需求,一个清晰的和结构化的飞机级功能定义过程和主要活动如下:

- (1) 详细的飞机顶层需求文件。定义了期望满足客户等利益相关方的需求,其中包括适航规章的要求。
- (2) 飞机级功能的识别。
- (3) 飞机级功能到其他项目需求的分配和实现。
- (4) 详细的飞机级ATA分解(物理分解)。
- (5) 详细的功能需求文件和功能描述文件。详述了每个顶层飞机级功能需求并提供了充分的细节以进行后续的设计活动。
- (6) 详细的顶层系统级需求文件,每个顶层系统级需求文件包含哪些功能需求文件中的功能,将通过相应的ATA系统予以实现,这一过程活动是可以选择的。
- (7) 飞机级需求的进展管理。
- (8) 飞机级需求的确认。

该定义过程的主要输出是飞机级功能定义，并由顶层飞机级需求文件和功能需求文件/功能描述文件组成。

顶层飞机级需求文件应与功能需求文件/功能描述文件和顶层系统级需求一起作为一组协调的飞机级需求，指导后续的设计活动，以验证实现的飞机产品满足其设计需求（实现过程验证）。

包含在顶层飞机级需求文件、功能需求文件和功能描述文件中的需求应进行确认。

4.1.2 飞机级功能

功能定义为：飞机的部分正规典型活动，如完成任务、行动或活动以达到一个期望的结果（ANSI/EIA - 632），预期的产品行为（SAE ARP4754A）等。

运输类飞机的飞机级功能定义通常从飞机的基本功能开始，反映了可理解的飞机产品使用目的，这样的定义或功能识别来自于多年的飞机设计经验和行业工程师的共同认识。将识别出的飞机级基本功能分解为主要功能和次要功能，由此，产生了飞机级功能的层级关系，形成了飞机级的功能分解结构。原则上，飞机级功能的层次以2~3层为宜，飞机级功能的上层对应飞机级顶层需求，其下层连接将开发的飞机系统。典型的运输类飞机的基本功能示例如表4-1所示。

表4-1 典型的运输类飞机的基本功能示例

基本功能	主要功能	次要功能
从起点到终点的移动	在地面，对飞机的控制	在地面，对飞机速度的控制
		在地面，对飞机方向的控制
	飞行中，对飞机的控制	速度控制
		滚转控制
		偏航控制
	导航	提供导引
		提供预测
载荷调节	内部空气控制	压力控制
		通风控制

飞机功能的性能需求：对特定功能的满意程度进行定量的描述。

4.2 飞机级功能定义过程的最佳实践

4.2.1 过程目标

1) 飞机级别功能定义过程的目标

(1) 除去其他项目需求（项目管理需求、商务需求等）之外，满足飞机顶层所识

别出的需求。

(2) 提供所需要的数据以保证飞机和系统的开发。

2) 飞机级功能定义的过程

(1) 需求的追溯贯穿整个飞机生命周期(通过需求工程过程应用予以实现)。

(2) 对飞机顶层需求文件、功能需求文件、功能描述文件和顶层系统需求文件的一致性和完整性进行评估。

(3) 对飞机级需求进展进行管理。

(4) 所有的利益相关方对公共需求共同管理。

3) 飞机级功能定义的组成

(1) 建立飞机部件或系统需求的源文件。

(2) 建立飞机验证过程的源文件。

(3) 在概念设计阶段,准备、计划和进行飞机项目支持活动的源文件。

(4) 飞机标准规范的源文件。

(5) 飞机文件的源文件(如《飞机维护手册》等)。

利益相关方将输出的部分信息直接用于飞机开发或关联到开发过程(如客户、试验阶段、适航等)。这将通过飞机项目管理进行授权。

4.2.2 过程描述

飞机设计应通过对来自用户要求或其他外部需求的顶层飞机需求的识别开始。这些需求在客户所需适航需求中的顶层飞机需求文件中进行定义。

飞机设计过程要求将顶层飞机需求向下一级进行分解。采用功能向下分解的方法,首先对飞机级功能进行识别,然后生成功能需求文件和功能描述文件。

顶层飞机需求文件是生成功能需求文件/功能描述文件的主要源文件。

在认可的组织架构中,按程序要求生成顶层系统需求文件,其可以对组织管理飞机开发过程到负责组织 ATA 章节开发的合作伙伴之间的信息传递进行控制。这一活动是可选择进行的,因为,这些信息已经在功能需求文件和功能描述文件中了。

飞机物理分解应与飞机功能定义同时进行决策,这可以对实现飞机功能所必需的物理组件进行识别。

当对飞机的功能进行分析时,飞机功能定义过程与安全性评估过程关联紧密。如果没有对飞机功能有彻底的理解,安全性分析就不能进行。这两个过程必须是同时且迭代地进行的。

飞机功能定义过程必须与飞机销售过程紧密相关,尤其是进行权衡研究之时。

图 4-1 表明了飞机功能定义的过程。

系统、结构、支持等对飞机功能的实现都是必需的。图 4-2 解释了飞机功能在系统、结构和其他专业的分配。

在系统专业,SAE ARP4754A 是应用到系统设计中的文件,它要求系统开发过程应能从飞机功能需求的识别、飞机功能到系统的分配追溯到飞机级。功能需求文

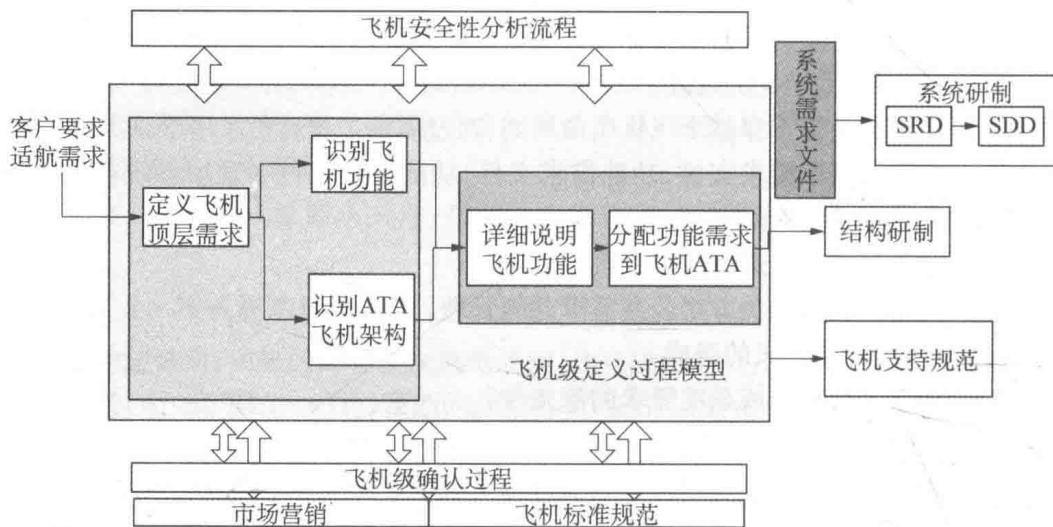


图 4-1 飞机能功能定义过程示意

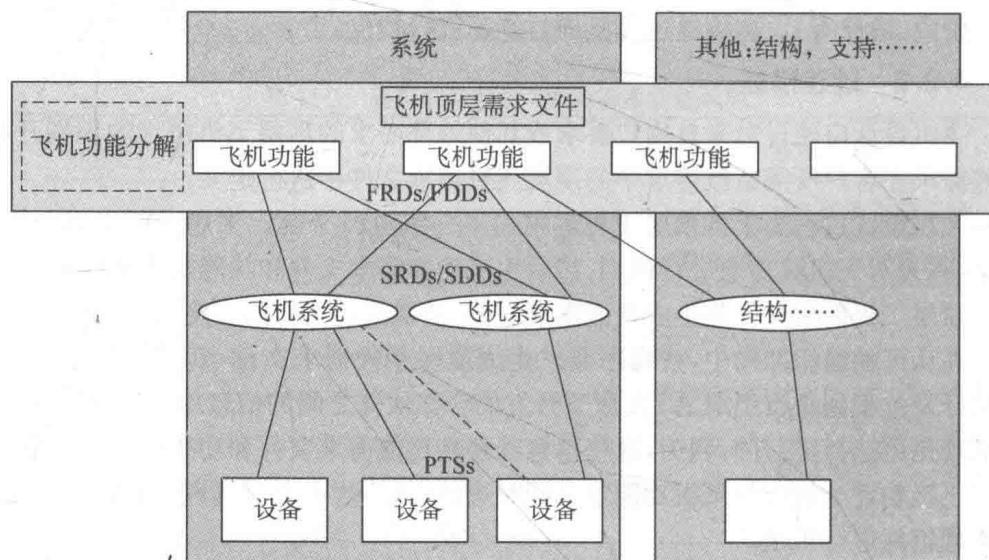


图 4-2 飞机能功能在系统、结构等领域的分配

件/功能描述文件的目的就是为实现这一活动：

- (1) 功能需求文件的目的是识别功能需求。
- (2) 功能描述文件的目的是定义飞机系统和结构在功能实现过程中的工作范围。

功能需求文件/功能描述文件是系统规范制订过程的主要输入文件(可参考系统需求文件/系统描述文件)。

如果系统参与几个飞机功能的实现, 几个功能需求文件/功能描述文件或许就

会要求产生系统需求文件。

如果一个飞机级功能是由几个系统共同完成的,那么,功能需求文件/功能描述文件就应用于生成这几个系统的需求文档。

推荐生成顶层系统需求文件的方式:从功能需求文件/功能描述文件中选取所有 ATA 章节需要的所有功能需求,这使飞机级开发过程和系统级开发过程之间的信息交流更为方便。

4.2.3 输入/输出

飞机功能定义过程如图 4-3 所示。

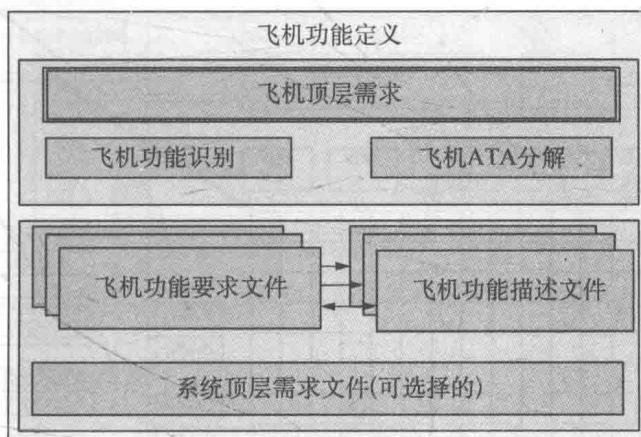


图 4-3 飞机功能定义过程

飞机功能定义过程输出如图 4-4 所示。

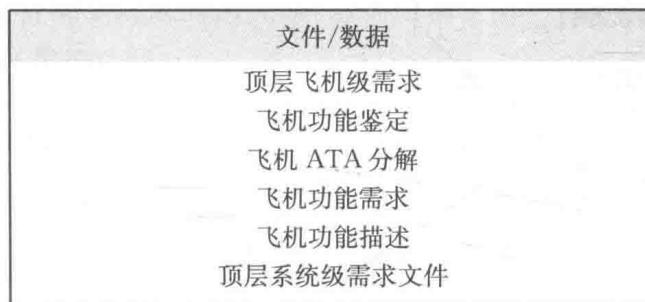


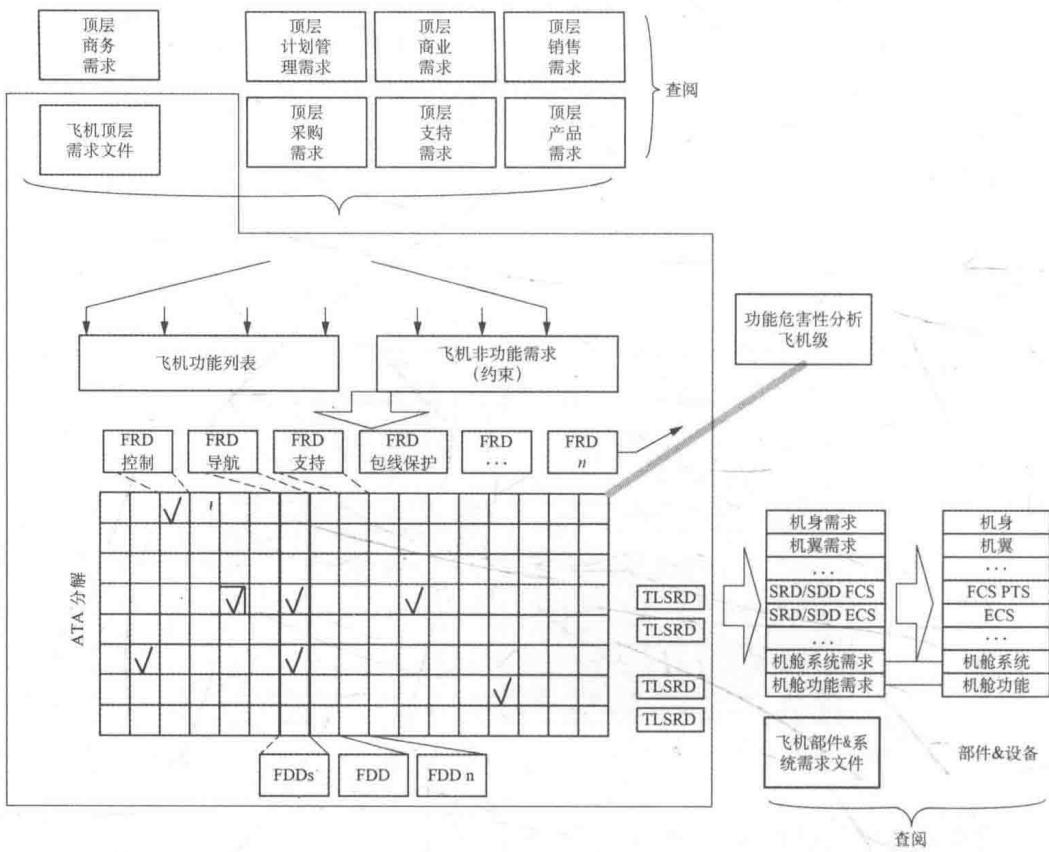
图 4-4 飞机功能定义过程输出

注:虽然这个文件给出了飞机功能定义数据的建议内容,对它的形式也没有做任何假定,它可能是一份或几份文件:

- (1) 一份包含顶层飞机需求的文件,一份飞机功能需求和描述的文件。
- (2) 一份包含顶层飞机需求的文件,一份飞机功能需求文件和一份功能描述文件。

(3) 其他。

图 4-5 对飞机内部开发过程之间的接口关系进行了阐释说明。



术语

TLARD: 顶层级飞机需求文件。

FRD: 功能需求文件。

FDD: 功能描述文件, 分配飞机功能给系统。

SRD: 系统需求文件。

SDD: 系统描述文件。

FHA: 功能危害性分析。

TLSRD: 顶层系统需求文件。

图 4-5 飞机内部开发过程之间的接口关系

4.2.4 利益相关方的需求

对飞机环境要求不一致而导致要求有冲突的利益相关方应进行分析和表述。

- (1) 客户: 航空公司, 运行人;
- (2) 乘客和货物发送人;
- (3) 空勤人员和地勤人员;
- (4) 自然环境: 噪声、污染等;
- (5) 运行环境: 飞行、地面、空中交通、导航、通信等;

- (6) 规章:适航、保险;
- (7) 厂商(安全、可支持性、制造等)。

4.2.5 过程活动及输出与项目管理的关系

顶层飞机需求文件/功能需求文件/功能描述文件/顶层系统需求文件是飞机功能定义过程中主要活动的交付物,这些活动是飞机开发过程中的活动,是项目管理里程碑定义的重要基础。图 4-6 给出了上述交付物与飞机开发里程碑之间的关系。

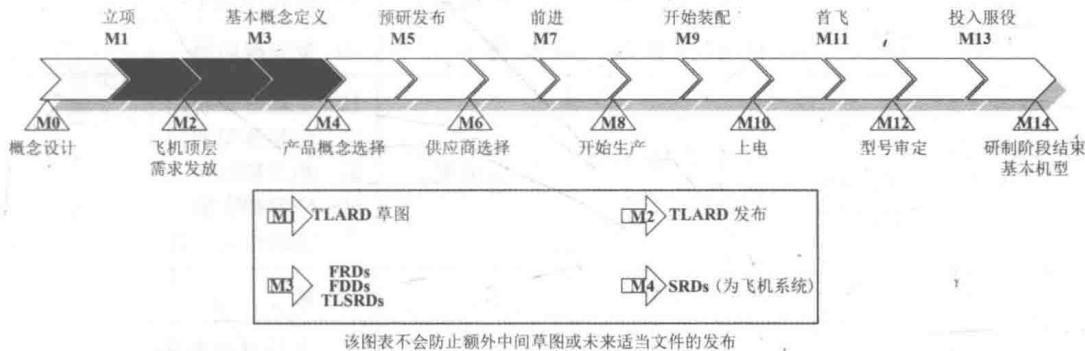


图 4-6 过程交付物与飞机开发里程碑之间的关系

4.2.6 通用飞机功能

为便于理解飞机功能,确定相关功能性需求,本节给出了一个建议的通用飞机功能列表,可用于民机功能识别及飞机级 FHA 过程,源自于工程经验和先前飞机 FHA 经验。为适应在研飞机的管理要求和技术特征,可对通用飞机功能目录进行更新。

飞机功能目录基于飞机功能的 3 个层级。建议的目录是一个表格形式,该表格考虑了飞机与可分配系统之间的关联,系统是基于 ATA 章节和子章节定义的(SBS),如表 4-2 所示。

注:(1) 系统关注的结构部分(ATA51 到 ATA57)没有在通用飞机功能目录中予以考虑,并且在本附件的最后一页列出仅是为了回忆。

(2) 与每个功能相关的数字是一个参考数字,不代表重要等级。

表 4-2 通用飞机功能目录

飞机 FHA 功能目录			链接到系统(ATA 目录)	
飞机功能	飞机子功能	相关系统功能	受影响的系统	详细的系统功能(子 ATA 章节)
1 地面控制飞机	1 地面速度控制	1 控制地面扰流板	27 飞行控制	60 扰流板和速度刹车 90 电子飞行控制系统
		2 控制机轮刹车	32 起落架	40 机轮和刹车
		3 推力换向控制; 3' 反向/桨叶角控制	78 排气 61 推力	30 推力换向 20 控制

(续表)

飞机 FHA 功能目录			链接到系统(ATA 目录)	
飞机功能	飞机子功能	相关系统功能	受影响的系统	详细的系统功能(子 ATA 章节)
1 地面控制飞机	2 地面方向控制	1 控制方向舵	27 飞行控制	20 方向舵 90 电子飞行控制系统
		2 控制前轮转向	32 起落架	50 转向
		3 控制差动刹车	32 起落架	40 机轮和刹车
		4 控制差动推力	78 排气	30 推力换向器
	3 提供地面构型	1 控制起落架收回/伸出	32 起落架	10 主起落架和门 20 前起落架和门 30 伸出和收回 60 位置和告警 70 辅助传动装置
		2 控制燃油泵	28 燃油	30 泵
	4 提供地面控制数据	1 为地面控制提供飞机数据(速度、起落架状态等)	34 导航	10 飞行环境数据/大气数据惯导 30 着陆和滑行帮助
			32 起落架	40 机轮和刹车
2 空中控制飞机	1 滚转控制	1 滚转轴控制	27 飞行控制	10 副翼 90 电子飞行控制系统
		2 滚转配平控制	22 自动飞行	10 自动驾驶 20 速度-高度修正 40 系统监控器
	2 偏航控制	1 偏航轴控制	27 飞行控制	20 方向舵 90 电子飞行控制系统 40 系统监控器
		2 偏航配平	22 自动飞行	10 自动驾驶 20 速度-高度修正 40 系统监控器
	3 俯仰控制	1 俯仰轴控制	27 飞行控制	30 升降舵 40 可配平的水平安定面 50 襟翼 80 升力增加(缝翼) 90 电子飞行控制系统
		2 俯仰配平控制	22 自动飞行	10 自动驾驶 20 速度-高度修正 40 系统监控器

(续表)

飞机 FHA 功能目录			链接到系统(ATA 目录)	
飞机功能	飞机子功能	相关系统功能	受影响的系统	详细的系统功能(子 ATA 章节)
2 空中控制飞机	3 俯仰控制	2 俯仰配平控制	28 燃油	10 存储量 50 燃油管理
			31 指示/记录系统	44 重量和平衡系统
	4 提供导航数据	1 提供飞机导航数据(位置、航向、姿态等)	34 导航	10 飞行环境数据/大气数据 惯性导航系统 20 姿态 & 方向/备份导航 30 着陆和滑行帮助 40 独立位置确定 50 依赖位置确定 60 位置计算 70 电子显示仪器
				46 信息系统
			80 起动	10 起动 11 风力起动器和阀系统
			61 螺旋推进器	10 推进器组件 20 控制 40 指示 50 推进器刹车系统
3 推力控制	2 推力控制	1 推进器控制(涡轮螺桨飞机发动机) 2 发动机推力控制	70 实际标准	
			71 动力装置	
			72 发动机	
			73 发动机燃油和控制	
			74 点火	
			75 引气	
			76 发动机控制	
			77 发动机指示	
			78 排气	
		3 自动推力控制	22 自动飞行	30 自动油门 40 系统监控器

(续表)

飞机 FHA 功能目录			链接到系统(ATA 目录)	
飞机功能	飞机子功能	相关系统功能	受影响的系统	详细的系统功能(子 ATA 章节)
4 驾驶舱、客舱和货舱的环境控制	1 空气控制	1 对压力、温度、湿度和给机组/乘客和货物的通风进行控制	21 空调	10 压缩 20 分配 30 增压控制 40 门区域加热 50 冷却 60 温度控制 99 支架和空调支持
	2 提供生命支持	1 让机组/乘客满意和舒适(厕所、厨房、座椅、声音传播控制等)	25 设备/家具	10 飞行分区/驾驶员舱 20 乘客分区/客舱 30 餐具柜和厨房 40 厕所 50 货舱分区 60 应急 70 附加分区 80 热和声的隔绝
				娱乐项目
	3 允许进出	1 控制机组/乘客/货物进入和退出的机械装置	52 门	
	4 提供照明	1 提供内部照明(驾驶舱、客舱和货舱的照明)	33 灯	10 飞行分区/驾驶舱 20 乘客分区/客舱 30 货物和服务区 50 应急照明
		2 提供外部照明	33 灯	外部
5 提供人机接口	1 提供数据、控制、指示和告警	1 为飞行机组人员配备	31 指示/记录	10 仪表和控制板 20 独立仪表 30 记录器 40 中央计算机 50 中央告警系统 60 中央显示系统/电子仪表系统
				10 中央维护系统(CMS) 20 上传和下载数据加载系统 40 打印 50 架构监控器

(续表)

飞机 FHA 功能目录			链接到系统(ATA 目录)	
飞机功能	飞机子功能	相关系统功能	受影响的系统	详细的系统功能(子 ATA 章节)
6 提供通信	1 内部通信	1 机组通信	23 通信	10 语音通信 20 数据传输 & 自动呼叫 30 乘客请求和娱乐 40 内部电话 50 音频综合 60 静态放电 70 音频/视频监控/内部通信 80 综合自动调整 90 数据总线系统通信
	2 外部通信	2 与地面通信	23 通信	
		3 与其他飞机通信	23 通信	
7 对自然的和诱发的环境问题提供保护	1 针对环境危害提供保护措施	1 提供闪电和电磁 提供保护	所有 ATA 章节	
		2 单个事件颠覆保 护	所有 ATA 章节	
		3 冰、雨和除雾保 护	30 提供对冰 和雨的保 护	10 机翼 20 进气口 30 皮托管和静压 40 窗户、风挡玻璃和门 50 天线和(雷达)天线屏器 60 螺旋推进器/转子 70 水位 80 冰探测
				21 空调 20 分配(窗户和挡风玻璃)
		4 防撞击保护(其 他飞机、鸟撞)	33 灯	
			34 导航	40 T4 CAS
		5 风切变和突风防 护	27 飞行控制	70 突风锁系统
			22 自动飞行	60 飞行包线
		6 反恐防护	所有 ATA 章节	
	2 提供对 内部危 害的防 护	1 发动机/轮胎爆 裂防护	所有 ATA 章节	
		2 降压防护(应急 生命支持)	35 氧气	10 机组氧气 20 乘客氧气 30 便携式氧气

(续表)

飞机 FHA 功能目录			链接到系统(ATA 目录)	
飞机功能	飞机子功能	相关系统功能	受影响的系统	详细的系统功能(子 ATA 章节)
7 对自然的和诱发的环境问题提供保护	2 提供对内部危害的防护	3 防火	26 防火保护	10 探测 20 灭火 21 发动机灭火 22 APU 灭火 23 货舱区灭火 30 防火/防爆
8 消耗品和动力供应	1 消耗品的供应	1 燃油供应	28 燃油	10 贮藏(量) 20 分配 40 指示 50 燃油管理
		2 水的供应	38 水/废水	10 饮用水 20 废水 30 废水处理 40 供气源 99 支架和支撑——水/废水
		3 氧气供应	35 氧气	10 机组氧气 20 乘客氧气 30 便携式氧气
	2 动力供应	1 液压动力供应	29 液压动力	10 主液压动力 20 辅助液压动力 30 指示
		2 电力供应	24 电源	10 发电机驱动 20 AC 交流电 30 DC 直流电 40 外部电源 50 AC 电负载配电 60 DC 电负载配电 90 虚拟电路布线
		3 气动力供应	36 气动	10 分配 11 发动机引气供应系统 12 APU 引气和交叉引气 20 指示 21 压力和温度监控 22 泄漏探测
		4 计算能力供应		综合模块化航电 (integrated modular avionics, IMA)

(续表)

飞机 FHA 功能目录			链接到系统(ATA 目录)	
飞机功能	飞机子功能	相关系统功能	受影响的系统	详细的系统功能(子 ATA 章节)
8 消耗品和动力供应	2 动力供应	5 辅助动力供应	49 机载辅助动力	10 动力装置 20 发动机 30 发动机燃油和控制 40 点火和起动 50 空气 60 发动机控制 70 指示 80 排气 90 滑油
9 结构载荷和振动的减缓	1 颤振控制			
10 与运行相关的特殊功能	1 空中燃料补给 2 空投			
11 结构(for memory)	1 提供静态容积	1 提供驾驶舱容积 提供客舱容积 提供货舱容积	51 结构	10 损坏分类 20 密封/程序 30 修理材料表 40 紧固件 50 飞机修理和校准支撑 60 气动平滑性/结构配平 70 修理 80 机身排水
			53 机身	60 地板 70 常规交叉点结构
	2 隔离/连接容积	1 驾驶舱/客舱隔离 货舱隔离	52 门	10 乘客/机组 20 应急出口 30 货舱 40 服务 50 固定内部 60 进门楼梯 70 门告警 80 起落架 90 其他
		2 窗和风挡玻璃	56 窗	10 驾驶舱 20 客舱 30 门 40 检查和观测

(续表)

飞机 FHA 功能目录			链接到系统(ATA 目录)	
飞机功能	飞机子功能	相关系统功能	受影响的系统	详细的系统功能(子 ATA 章节)
11 结构 (for mem- ory)	3 提供气 动外形		53 机身	10 主框/前机身前端 20 辅助结构/前机身 30 蒙皮-中机身 40 连接接头/后机身 50 气动整流装置/尾锥-后机 身 80 后机身 90 固定连接接头
			54 吊舱/吊挂	10 吊舱/吊舱前部 20 辅助/吊舱中部 30 外壳/吊舱后部 40 连接接头 50 吊挂 90 固定连接接头
			55 安定面	10 水平安定面 20 升降舵 30 垂直安定面 40 方向舵 90 固定连接接头
			57 机翼	10 中央翼 20 外翼 30 翼尖 40 前缘和前缘装置 50 后缘和后缘装置 60 副翼 70 扰流片 90 固定连接接头

4.2.7 飞机级需求及功能在电传飞行控制系统中的分配

飞机级功能“空中控制飞机”是一种目的性或用途性的功能,识别目的性或用途性的功能,解决飞机按用户等 Stakeholder 的要求设计飞机的意图,从“user case”的角度定义和识别飞机产品。为便于用户与工程师之间对产品的理解一致,通常可以将飞机级用途性的功能转换为某种原理性的功能(principle),尤其是具有工程原理性的功能。典型的转换为将“空中控制飞机的功能”转换为“俯仰控制”“滚转控制”和“偏航控制”3个子功能,这次转换既给了用户中的飞行员等较专业人士清晰的功能实现路径,也给了飞机设计工程师明确的设计意图,即用空气动力学和力矩控制方式实现“空中控制飞机的功能”,隐含不会采用直接力控制的方式实现“空中控制

飞机的功能”。假如“空中飞机控制的功能”分解为“直接力控制”和“力矩控制”，这也是可以的。就目前的技术和发动机能力，如推力矢量控制，在两种分解下未来的系统设计实现肯定不一样。

原理性的功能只给出了工程设计实现的方向，但以什么具体路径去实现还需要明确，所以仍需将原理性的功能(principle)进一步分解为过程性功能(process)或需要的能力(capability)，典型的如将“滚转控制”分解为“滚转轴控制和滚转配平控制”；“偏航控制”分解为“偏航轴控制和偏航配平控制”；“俯仰控制”分解为“俯仰轴控制和俯仰配平控制”。飞机级功能分解到该层级时，事实上已将原理性功能及功能需求分解和细化到了可用工程技术实现的飞机级需求，并进一步将可用工程技术实现的需求分配到飞机的各个系统，产生系统开发或设计的需求。

仅有上述飞机级功能性需求，并不能推断在飞机设计中一定采用电传飞行控制系统，某种程度上传统的机械式飞行控制系统也是能够实现“俯仰轴、滚转轴及偏航轴”的控制的，正如第1章和第2章所述，所以决定采用电传飞行控制系统的理由肯定存在其他的需求或要求。通常来讲，飞机级的需求(无论需求的层级)可以分为两大类，一类为功能性需求(自然也就包含性能的需求)，另一类为非功能性需求或者约束性需求，非功能性需求包括重量的需求、采用特定技术以解决先进性的需求、延续以前开发的系统或部件以及可靠性、可用性、维护性等许多方面的需求。电传飞行控制系统相比于传统机械系统的优势包括布局方便、有利于提高飞机的飞行控制精度和降低驾驶员飞行控制负荷、为主动控制技术的发展提供了很好的技术基础以及在飞机上可以实现更多更好的功能等，这些优势如果变成飞机级的需求，既包含了功能性需求，也包含了非功能性需求，那么，为满足飞机级需求，自然就会考虑采用电传飞行控制系统了。

为满足第25.1309条的要求，需要利用飞机级的功能危害性分析(AFHA)捕获飞机级的安全性需求，并将此安全性需求传递到系统，作为系统开发的顶层需求。由于本节中飞机级功能分为三层，以哪一层功能应用FHA呢？按ARP SAE 4761的要求，飞机级FHA应该在功能层次中以合适的层级开展，那么什么是合适的层级呢？很多从事安全性分析和捕获的方法或学者，对于上述问题的回答是靠经验。从AFHA来讲，是产品危害性工程理论，即产品危害三要素，包括危害源、危害触发机制和危害后果在航空产品开发上安全性分析方面的应用，是航空产业飞机产品开发多年积累并得到认可的经验总结，并纳入到适航规章的符合性方法中(AC25.1309)。AFHA本身是一种方法而不是一种理论，因此很难用一种非常严格的概念定义和逻辑推演或解析模型来解决。

由于飞机级危害的判断来自功能危害对飞机和机上乘员安全程度的影响，作者认为合适的层级来自能够表现出飞机某种行为的功能层级(behavior)，这个说法与SAE ARP 4754A对功能的定义是一致的。对于飞机级功能，作者更倾向于以原理性功能层级作为开展AFHA分析的层级，一是原理性的功能能够便于分析功能失

效的后果,二是通常原理性的功能层级高于向系统分配的飞机功能层级,便于考虑某个飞机级功能分配到多个系统时的飞机级需求在相关系统落实的权衡问题,即所谓的 PASA。

由于飞机级功能不涉及更多的技术和系统架构等,仅从飞机级功能和功能危害性分析来看,看不出电传飞行控制系统与传统的如机械式等系统的差别。从另一个角度说,细节被隐藏了,被“飞机”遮蔽了,也就是说,谈飞机级功能或功能危害性时,是飞机的所谓外特性影响,电传或是非电传飞行控制系统只是有此外特性的内涵,还有待深入挖掘,或求解,或未来去开发,所谓飞机级功能或飞机级功能需求只构成了将开发系统的能力需求,是系统整体需求的一部分。对于运输类飞机,飞机级功能可以认为是相对不变的一类需求,但在不同型号的飞机上功能性需求中,性能需求可能存在较大差异。

对于电传飞行控制系统,一个非常重要的飞机级需求是飞机的电传飞行控制控制律。控制律是指飞机的舵面指令与飞行员飞行控制杆指令,不同的运动传感器信号,飞机的高度、速度和马赫数等之间的运算关系。控制律的设计方法以及引入多少种传感器信号作为控制量,不是本书研究的内容,但是,应属于功能及功能性需求捕获和分析的工作,因此飞机如采用电传飞行控制系统,控制律构成了飞机级实现控制飞机的功能的核心内容,是飞机级的需求,是待开发的电传飞行控制系统的顶层需求,至少电传飞行控制系统要具备完成控制律的实时计算的功能。

工程实践中,飞机级的需求捕获、分析和向系统级进行分配,以及系统通过架构满足需求等活动不是绝对的前后关系,实质上有相互迭代的活动,甚至需求与需求的确认、需求的验证中的某些工作是并行开展的,即所谓复杂系统的设计既是“top-down”的,也是“bottom-up”的。为解决开发上下游的复杂关系,需要应用构型管理的相关策略。

4.2.8 与飞行控制系统有关的典型的飞机级功能及失效条件

对于空中控制飞机功能的失效条件(failure conditions),其危害是灾难级的如下:

- (1) 结冰条件下未通告的不能维持空气动力(失去);
- (2) 失去偏航控制并结合发动机停车和严重侧风;
- (3) 失去俯仰轴控制;
- (4) 失去人工飞行控制功能;
- (5) 飞行控制面的结构失效(也可能是危害级的);
- (6) 未设权限的自动飞行故障;
- (7) 接近地面时的推杆器故障;
- (8) 未通告的滚转轴控制故障;
- (9) 未通告的偏航轴控制故障;
- (10) 未通告的俯仰轴控制故障;

- (11) 未通告的电子配平故障(根据机型);
- (12) 未通告的在警示高度下的自动着陆故障。

对于空中控制飞机功能的失效条件,其危害是危险级的如下:

- (1) 在自动着陆中未通告的失去自动飞行功能;
- (2) 设权限和多轴的自动飞行故障;
- (3) 飞行中未通告的襟翼故障;
- (4) 飞行中推杆器故障;
- (5) 飞行中失去推杆器功能并处于失速状态;
- (6) 失去偏航控制并结合发动机停车和严重侧风;
- (7) 失去滚转控制但偏航控制可用;
- (8) 起飞时飞行指引只提供侧向指示。

对于失去增稳功能或人工感觉功能,其危害等级依机型不同;对于增稳功能或人工感觉功能故障,其危害等级依机型不同。

对于地面控制飞机功能的失效条件及其危害等级如下:

- (1) 未通告的刹车功能失去,危害等级为灾难级;
- (2) 失去起落架控制功能,其危害等级为危险级;
- (3) 起落架控制功能故障,其危害等级为危险级或主要级;
- (4) 起落架收放功能故障,其危害等级为危险级;
- (5) 刹车功能故障,其危害等级为危险级。

从上述飞机级 FHA 结果来看,仍然看不出与电传飞行控制系统的直接关联性,需要分配到系统并作为系统的开发需求(安全性需求)后,从系统级的 FHA 捕获电传飞行控制系统的指标要求。

4.3 电传飞行控制系统功能及安全性需求

电传飞行控制系统在飞机级分配而来的需求基础上,需要识别出系统级的功能,并定义出系统级的功能性需求,以及其他需求,形成系统级的需求(SRD)。有系统级的需求(SRD)后,开发电传飞行控制系统的架构满足 SRD 需求,满足 SRD 的架构文件通常称为系统设计描述(SDD)。SRD 也称为需求规范,SDD 称为架构规范,SRD+SDD 称为系统规范。

4.3.1 典型的电传飞行控制系统功能

空客某型飞机 A×××飞机主飞行控制系统定义的主要功能总结如下:

- 1) 人工指令和控制律计算
 - (1) 驾驶舱控制;
 - (2) 驾驶舱控制指令获得(正/副驾驶侧杆和脚蹬、减速板手柄、油门杆、俯仰和方向舵配平开关);
 - (3) 人工飞行导引指令和选择;

(4) 控制律重构(正常、辅助和直接模式)。

2) 舵面偏转指令计算

(1) 空中减速、地面扰流片、高升力副翼下垂、飞行控制指令与选择；

(2) 载荷减缓、乘坐品质控制律；

(3) 发送指令到作动器，实现对舵面的位置进行控制。

3) 舵面偏转伺服系统

(1) 作动器的工作模式和闭环控制；

(2) 作动器监控；

(3) 作动器工作；

(4) 作动器动力源监控。

4) 与机组人员接口

(1) 通知构型和状态；

(2) 提供警戒和告警。

5) 获得飞机飞行参数

(1) 惯导系统参数；

(2) 大气数据；

(3) 无线电高度；

(4) 飞机构型；

(5) 发动机参数；

(6) 备用仪表系统。

6) 飞行导引指令限制与选择

(1) 保护(迎角保护、速度保护)；

(2) 指令限制($\varphi_c, \dot{\varphi}_c, \beta_c, \dot{\beta}_c, N_{zc}$)。

7) 维护和测试

(1) 故障隔离和探测；

(2) 系统维护和测试；

(3) 维护数据存储；

(4) 计算机/系统管理；

(5) 采集计算机关闭/重启按钮通话器；

(6) 计算机失效、接通、重构；

(7) 系统构型；

(8) 舵面偏转指令计算；

(9) 侧向和俯仰飞行控制指令和选择；

(10) 与机组人员接口；

(11) 提供力感觉；

(12) 接管/自动驾驶自动断开管理；

- (13) 与其他系统的接口；
- (14) 与控制和显示系统接口；
- (15) 与数据记录器的接口；
- (16) 与中央维护系统、飞机状态监控系统接口。

波音某型飞机 B×××飞机主飞行控制系统定义的主要功能总结如下：

主飞行系统的功能是提供对飞机俯仰、滚转和偏航的人工飞行控制，并支持对飞机俯仰、滚转和偏航的自动化飞行控制。基于常规的驾驶杆/盘、脚蹬、俯仰配平开关和飞机传感器等的信号输入，FCE 计算出飞行控制面的飞行控制指令，并传到飞行控制面的作动器，获得预期的飞机响应。飞行控制系统功能的子功能如下：

- (1) 人工飞行控制；
- (2) 增加飞机稳定性；
- (3) 包线保护；
- (4) 乘坐品质增强；
- (5) 载荷减缓。

从上述两个实例可知，电传飞行控制系统就其主要功能来看，就是实现对飞机三轴的控制，从功能层面来说，其与传统的飞行控制系统是等价的，只是功能性需求有了很大的变化。由于电传飞行控制系统与传统的纯人工飞行控制系统相比有更多或者更大的权限，在飞行控制功能下的子功能有了更丰富的内容，可以满足飞机级的更多需求，如乘坐舒适性、载荷减缓、包线保护（或包线限制）、放宽飞机静稳定性以及更好的系统维修性等，电传飞行控制系统本身的需求以及需求在子系统的分配，电传飞行控制系统的集成等变得非常复杂，并具有相当的难度。

随着先进的数字技术应用和减少飞机成本的需求，现代民用飞机的系统集成度越来越高，按传统的系统分解方法如 ATA 章节，对于功能性分解与物理架构的分解的一致性有时会变得很困难，这是因为飞机级的需求分解和系统级的需求分解非常清晰，物理架构的分解也是非常清晰的，但是需求与物理架构的关系就复杂了，即同一架构要执行多种顶层的功能，如果以物理架构概念来确定系统的范围（通常是这样划分的），可以很方便地确定系统的安装接口以及物理接口，但确定系统的功能接口是比较难的，也是系统集成的关键。电传飞行控制系统的安全性需求很大一部分来自功能性的安全需求，加上需求本身的量级增加，据说国外现代飞机的电传飞行控制系统的系统级需求规模为数千条，这对电传飞行控制系统的架构和最终的实现提出了挑战，也为如何验证安全性需求带来了繁杂的工作量和完成的难度。为解决这一问题，最好的措施是将物理架构中的设备从传统的设备概念转换为子系统的概念，建立电传飞行控制系统从系统到子系统，甚至子子系统的各层需求，进行多层次的需求确认和验证，并对需求的追溯性保持良好的跟踪。

4.3.2 电传飞行控制系统功能危害性评估

与飞机级功能危害性评估（FHA）类似，需要识别系统级的功能并进行系统级

的 FHA。由于系统级架构的专业特性和物理属性更清晰,如 4.3.1 节所述,系统级定义两级或者三级功能是合适的。按 SAE ARP 4761 和 AC25.1309 的要求,采用结构化的 FHA 分析方法是适航审查可以接受的方法,但结构化的方法将带来不同功能的各种组合,组合的量级是非常可观的。由于系统级已经可以感知具体的子系统架构或物理架构,可以采用以下的方法,对潜在的系统安全性顶事件进行“屏蔽”,通过 PSSA 的多次迭代,减少了系统级的顶事件,并确保安全需求的正确性和完整性。

潜在的安全性危害和危害性条件有:

- (1) 功能性危害(与功能/系统/设备/部件有关);
- (2) 外部危害(来自环境的危害);
- (3) 内在危害(来自设备的内在危害);
- (4) 安装的危害;
- (5) 人活动的危害[飞行机组活动、客舱人员活动及地面人员活动(维修和运行)]。

所有上述危害在系统级都需要独立地考虑,并同时考虑相互的影响。为识别出所有的危害,在系统的设计阶段,需要采用系统化的危害减少过程,包括以下几个步骤:

- (1) 危害清除。对每一个潜在的危害,对在设计中是否保留的必要性进行证实(架构和实现清除)。
- (2) 危害级别最小化设计。当一个潜在的危害存在不能被清除时,应采用必要的设计措施,最小化该危害的危害性级别。通常采用的措施有失效检测、失效隔离、功能重构、失效影响抑制、非相似备份、健壮性设计和错误包容性设计等。
- (3) 保持对危害的控制。在上述两步以后,需要对余下的危害进行控制,即考虑危害的影响程度,对在飞机生命周期内发生该危害的概率控制在一个可接受的水平。

从适航性的角度,灾难级危害发生的概率小于 10^{-9} 事件,可以理解为危害清除(满足了适航规章的要求),但从安全性的角度,则可以理解为保持了对危害的控制,这也是适航性设计和安全性设计理念的一个差异(见第 1 章)。当然,系统的架构是清除危害和最小化危害级别的最有效手段。

4.3.1 节中空客某型飞机 A××× 经过 PSSA 后电传飞行控制系统的灾难级系统顶事件为:

- (1) 失去所有的飞行控制计算机;
- (2) 在起飞过程中,由于脚蹬失去方向舵控制+发动机失效或者侧风大于 15 kn;
- (3) 飞行过程中所有的计算机触发了过度的上电测试;
- (4) 失去两片方向舵,并且一台发动机失效或者很强的侧风;
- (5) 一片方向舵在飞行中丢失;

- (6) 方向舵振动,同时失去对振动的监控功能;
- (7) 失去四片升降舵的控制或者丢失四片升降舵(和 THS);
- (8) 升降舵振动,同时失去对振动的监控功能;
- (9) THS 松动到极限位置外;
- (10) THS 作动器主传力路径未探测的破坏;
- (11) 飞行中几片副翼和扰流片丢失;
- (12) 同时失去滚转和方向控制。

4.3.1 节中波音某型飞机 B××× 经过 PSSA 后电传飞行控制系统的灾难级系统顶事件为:

- (1) 俯仰控制的失去或降级导致飞机低于最小可接受的控制(MAC);
- (2) 错误的俯仰控制,包括急偏或振动,足以导致不安全的飞行轨迹或者结构失效阻止继续安全飞行和着陆(CSF&L);
- (3) 非指令性安定面移动导致不安全的飞行轨迹;
- (4) 滚转控制的失去或降级导致飞机低于最小可接受的控制(MAC);
- (5) 错误的滚转控制,包括急偏或振动,足以导致不安全的飞行轨迹或者结构失效阻止 CSF&L;
- (6) 错误的偏航控制,包括急偏或振动,足以导致不安全的飞行轨迹或者结构失效阻止 CSF&L;
- (7) 在起飞和着陆期间,方向舵控制不足以抵消发动机停车或侧风的效应造成不安全的飞行轨迹;
- (8) 失去驾驶杆力感控制导致不安全的飞行轨迹或结构失效阻止 CSF&L;
- (9) 在不正确的模式下运行导致不安全的飞行轨迹;
- (10) 增升能力不够导致离地速度高或结构失效阻止 CSF&L;
- (11) 失去颤振刚度或阻尼造成结构失效阻止 CSF&L;
- (12) 飞行中错误地触发维修测试导致不安全的飞行轨迹;
- (13) 失去俯仰稳定增强功能导致不安全的飞行轨迹;
- (14) 触发持续的错误的超速导致不安全的飞行轨迹;
- (15) 触发错误的增强失速保护导致不安全的飞行轨迹;
- (16) 失去主动的荷兰滚阻力导致不安全的飞行轨迹或结构失效阻止 CSF&L;
- (17) 错误的触发机翼对称飞行控制载荷减缓导致的不安全的飞行轨迹;
- (18) 失去推力非对称保护(TAP),同时一台发动机停车并加大另一台推力导致过度的。推力非对称,并且方向控制不能抵消,导致横向控制失去和不安全的飞行轨迹。

从上述两个机型的 FHA 结果来看,似乎有较大的差异。从飞机级功能及 FHA 来看,采用类似技术路线的电传飞行控制系统不应该差异很大,那么这些差异的来源是什么呢? 从开发过程来看:

(1) 基于类似的需求,不同的设计师采用的技术方案有差异,因此实现需求的架构肯定不同,由于系统级的 FHA 与架构(计算机选型、指令闭环)和实现(如选用不同的飞行控制面作动器)有紧密的关系,因此系统级 FHA 表现出差异。

(2) 前面谈到过,功能实质上是需求的组合,功能分解结构(FBS)和物理分解结构(SBS 或 PBS)在复杂系统上存在差异性,系统的范围界定和物理组件上分配到的具体需求存在差异。

(3) 即使类似的需求和系统架构,甚至同一公司的继承机型之间,不同的设计师对基于需求的功能行为的理解也存在差异,功能是功能需求的抽象,功能危害性分析是一种逻辑和方法应用的过程,就像搭建一个同样的积木,过程可以是不同的。

然而功能是产品的属性,既然飞机级功能及危害性类似,从构型演变的结果来看,系统级 FHA 之间也应存在某种类似。实际上,系统级功能或功能性需求,包括 FHA,最后都将落实到物理架构上,从底层物理架构表达的 FHA 一定看到相当多的类似。如 A×××的(1)顶事件认为失去计算机就是失去飞行控制功能,失去计算机不是简单的承担控制律计算的计算机失效,也包括飞行控制指令失效、大气数据失效(无数据源等),而 B×××的(1)、(4)等分别从俯仰控制、滚转控制等功能失去建立顶事件,但(1)、(4)顶事件中最大的贡献就是失去计算机。

所以,系统级 FHA 是捕获系统级安全需求的方法,其根本目的是根据飞机级的功能性需求(包括 FHA 要求)和非功能性需求,识别出系统级的需求,并保证需求的完整性和正确性(通过双 V,第 5 章)。

4.3.3 电传飞行控制系统的需求

电传飞行控制系统的需求应包括满足飞机级规范的可实现的所有适用需求,其需求通常包括:

- (1) 系统功能性;
- (2) 需要达到的性能;
- (3) 与其他系统的接口(物理、安装和功能);
- (4) 运行需求;
- (5) 适航需求;
- (6) 安全性需求;
- (7) 共同性/复用需求;

.....

严格意义上讲,上述每一条需求中都可能包含适航的需求,如电传飞行控制的功能性是通过控制率来定义的,而控制率的开发必须考虑 CCAR 25 部 B 分部的适航条款的要求,见第 3 章。本节就电传飞行控制系统需求中安全性需求和适航需求说明如下:

- (1) 安全性需求。
 - a. 定量需求,如 4.3.2 节;

b. 定性需求,通常为 A 级(ARP4754A),或 FDAL A(ARP4754A),DO-178, DO-254。

(2) 适航性需求。

CCAR25.671:关注舵面的卡阻等需求,a 和 b 条直接将规章内容作为需求;c 为验证的要求,反映到安全性需求中,特别有单点故障造成灾难性事件是不允许的;

CCAR25.672:可直接作为飞机级需求,结合(1)安全性需求;

CCAR25.675:可直接作为系统级需求;

CCAR25.677:可直接作为系统级需求;

CCAR25.679:可直接作为系统级需求,注意可以用其他装置如液压阻力,替代“突风锁”;

CCAR25.685:可直接作为系统级需求;

CCAR25.697:可直接作为系统级需求;

CCAR25.699:可直接作为系统级需求;

CCAR25.701:可直接作为系统级需求,系统结构的设计需求;

CCAR25.703:可直接作为系统级需求;

CCAR25.777:可直接作为系统或设备级需求;

CCAR25.779:可直接作为系统或设备级需求;

CCAR25.781:可直接作为设备级需求;

CCAR25.1301:识别并定义系统级需求 SRD(SDD 表明符合性);

CCAR25.1309:b、d 等同(1)安全性需求,c 为飞机级需求;

CCAR25.1310:可作为飞机级需求或系统级需求。

具体的要求参见第 3 章适航规章要求的解读,作为需求中具体的工程数值等需要与具体的型号关联,有些还需要计算和分析。

4.4 满足适航性要求的电传飞行控制系统架构和方法

4.4.1 对设计方法的适航要求

表明符合 CCAR25R4 部适航规章的方法中,有对设计过程和设计方法提出要求的。对设计过程的要求典型的是 ARP4754 和 ARP4754A 等,对系统设计方法的要求,来自于失效-安全设计理念的目标、原理或方法,在 AC25.1309 中,对系统架构或设计方法做出了约束。

1) 使用与失效有关的基本目标

(1) 在任何系统或子系统内,在任何一个飞行起落期间(从松刹车起至地面减速到停止),不管它的可能性如何,应该假定会有任何单个元件、部件或连接件的失效。上述的单个失效应该不妨碍继续的安全飞行和着陆,或显著降低飞机的性能或机组应付所产生的失效状态的能力。

(2) 在同一个飞行起落期间,还应假定有相继的失效(不管是探测到的或潜伏

的)以及它的组合,除非表明它们与最初的失效的联合概率是极不可能的。

2) 为了保证安全设计,失效-安全设计概念采用的设计原理或方法

只使用下面这些原理或方法之一是很难满足要求的。通常需要其中两个或更多个组合以用作失效-安全设计,即保证重大的失效状态是不大可能发生的,而灾难性的失效状态是极不可能发生的。

(1) 设计的完整性和品质,包括寿命的限制值,以保证预定的功能并防止失效;

(2) 多余度或备用系统在单个(或其他规定数目的)失效以后使能继续工作,例如两台(套)或更多台(套)的发动机、液压系统和飞行控制系统等;

(3) 系统、部件和元件的隔离,以便其中一个失效不会引起另一个的失效,隔离也称为独立性;

(4) 被证实的可靠性,以便在同一个飞行起落期间,多重、独立的失效不大可能发生;

(5) 提供检查的失效警告或指示;

(6) 在失效发现以后空勤组采取的措施,按照规定的机组纠正动作使之能继续安全飞行和着陆;

(7) 可检测能力,即检查部件工作状况的能力;

(8) 设计的失效影响限制,包括承受损伤的能力、限制失效对安全效果或影响的能力;

(9) 设计的失效路径,在某种程度上控制和支配失效的影响以限定它的安全效果;

(10) 对任何不确定的或未预见到的不利情况,考虑的安全裕度或安全系数;

(11) 差错-容限,这是在飞机设计、试验、制造、使用和维护期间考虑可预见的差错的不利影响。

4.4.2 满足适航要求的电传飞行控制系统的架构和方法

4.4.2.1 系统功能架构

功能架构,即功能、内部/外部功能接口和物理接口、相关的功能和性能需求以及设计约束按层级进行分布的结果。

能清晰描述系统将做什么的逻辑关系图,由若干个功能流程框图所组成,如图 4-7 所示。

飞行控制系统的功能架构及其控制律的设计是为了控制和稳定飞机,使飞机在整个飞行包线范围内具有令人满意的飞行品质(满足 AC25-7C)。

在方案阶段,控制律工程师要参与飞机气动布局的确定,包括飞行控制面的尺寸、伺服作动器参数、飞机重心位置的变化范围等;与飞机性能专业一起确定飞机的机动能力,如飞机最大迎角、最大机动过载等;提出飞行控制系统的控制律初步方案,初步选择控制律结构。

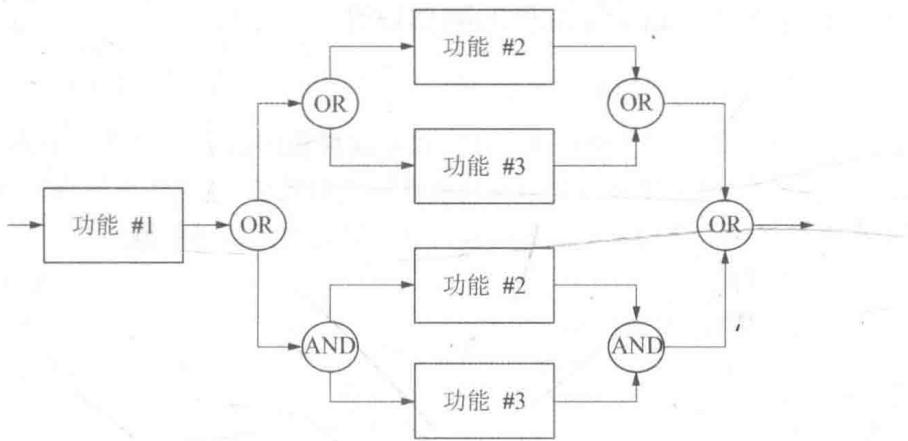


图 4-7 系统功能架构

在工程研制阶段,利用最优化程序和飞机六自由度仿真程序对控制律及其增益进行优化。同时,也要向载荷、结构和气动弹性专业提供数据。提供飞行控制面的偏转角速度作为确定液压系统功率的依据。另外,还要对子系统提出技术要求。

准备数据库,除正常数据外,还应该包括起落架对气动特性的影响、起落架的动态特性,以及结构弹性数据、飞机迎角数据等。进一步修改控制律增益,以全面满足飞机飞行品质要求。在这个阶段,需要飞行模拟器进行大量的驾驶员在环飞行模拟试验,通过评价飞行品质,检验控制律设计的合理性,完善和修改控制律,直至驾驶员满意为止。

4.4.2.2 系统物理架构

电传飞行控制系统架构就是将驾驶员指令(或控制指令)传输到舵面并控制其运动,以满足飞机以预期的方式运动的若干物理设备的有机组合,主要由驾驶舱飞行控制装置、电缆、计算机、总线、作动器控制电子、作动器、传感器、软件等设备和项目组成。

系统架构确立了系统的结构和边界,在该结构和边界范围内,实施具体的设计以满足所建立的需求。其主要工作包括:研究飞机飞行控制舵面的驱动方式,飞机最小可接受控制的配置方式,余度配置和等级、指令信号的完整性和有效性,监控器的设置和设计、接口、安装、维护、显示、信号和(或)部件丧失和(或)错误等对舵面运动功能可能造成的影响,以及确认和验证的方法等。可以考虑多个用于实现设计的物理架构,通过使用功能和性能分析、初步飞机安全性评估(PASA)/初步系统安全性评估(PSSA)和共因分析(CCA)等过程对候选系统架构进行迭代式的评估,以确定在满足分配到系统的功能和顶层安全性需求方面的可行性。同时,还考虑其他一些因素,如技术成熟度、设计实施进度、生产能力、合同义务、经济性、以往经验及行业领先状况等。最后,经过上述的综合权衡确定合适的系统物理架构。

4.5 电传飞行控制系统部件的隔离设计

4.5.1 共模/共区故障

对于由外部事件引起的共模/共区故障或损伤所造成的飞机安全问题,解决方案是系统设计满足系统部件隔离或功能性隔离的需求,包括防止维修人员错误或误操作的安装准则。飞行控制系统的功能设计和安装需考虑以下问题。

1) 物体碰撞

- (1) 转子爆破(发动机和 APU)。
- (2) 轮子和轮胎爆破/破碎：
 - a. 轮面抛出；
 - b. 轮面松弛；
 - c. 轮子爆破；
 - d. 轮胎爆破。
- (3) 鸟撞。
- (4) 空中碰撞。
- (5) 运动设备/部件。
- (6) 雨水/冰。
- (7) 地面碎片。

2) 电气故障

- (1) 线束起火或过热；
- (2) 设备或集成盒起火；
- (3) 联结器短路或耦合分离；
- (4) 线路破皮或破损；
- (5) 接地/搭接/防护联结错误；
- (6) 飞行试验测试设备不匹配；
- (7) 导线交叉。

3) 电源失效

4) 电磁环境

- (1) 电磁兼容(EMC)；
 - (2) 高强度辐射场(HIRF)；
 - (3) 电磁干扰(EMI)(内外部)；
 - (4) 抗静电能力；
 - (5) 单粒子反转。
- 5) 闪电攻击
 - (1) 直接效应；
 - (2) 间接效应。

- 6) 刹车过热或失效
- 7) 高压设备破裂
 - (1) 导管破裂；
 - (2) 蓄电池破裂。
- 8) 火
 - (1) 燃油；
 - (2) 液压；
 - (3) 电气；
 - (4) 厨房；
 - (5) 货舱；
 - (6) 驾驶舱和(或)客舱烟气污染。
- 9) 液压失效
- 10) 流体污染
- 11) 发动机和短舱分离
- 12) 粗暴或不安全的安装和维修活动
 - (1) 短路；
 - (2) 糟糕的文档；
 - (3) 过程更改；
 - (4) 未归档的更改；
 - (5) 没有经过培训的人员上岗；
 - (6) 未检测到的腐蚀；
 - (7) 手抓或踩踏传输线路。
- 13) 爆炸物
 - (1) 客舱区和货物区；
 - (2) 其他区域。
- 14) 结构损伤
 - (1) 快速失压；
 - (2) 蒙皮破裂；
 - (3) 隔板失效；
 - (4) 机翼部件脱落；
 - (5) 垂危部件脱落；
 - (6) 水平安定面部件脱落；
 - (7) 地板坍塌或受压弯曲；
 - (8) 飞行控制面分离(包括部分分离)；
 - (9) 高升力系统元件失效；
 - (10) 起落架折叠或分离；

- (11) 流体存储区受液压动力撞击;
- (12) 外来物穿透;
- (13) 后压力隔板失效。
- 15) 化学品溢出
- 16) 氧气和(或)可燃液体泄漏
- 17) 结冰
- 18) 尾部撞击或硬着陆
- 19) 火山灰、沙尘和灰尘
- 20) 燃油冲出
- 21) 雷达天线罩损坏

4.5.2 电传飞行控制系统部件物理隔离设计理念

系统部件隔离的主要目标是使由于共模或共用区故障带来功能损失的可能性最小，并阻止其他系统的失效影响 PFCS 的运行。该设计理念将导致冗余的、包含 LRUs 在内的飞行控制元件需要进行隔离或分离，与这些元件关联的导线和液压线路也需要尽可能地隔离或分离。

在隔离的设计理念下，通常解决共模/共用区故障问题的飞行控制系统或飞机设计方法如下。

(1) 飞行控制电子和电气设备安装位于不同的设备间，这样电源的分配和电子控制线路就实现了隔离。飞行控制计算机 PFC 和 ACE 在前后 EE 舱布局并安装在不同的 EE 舱，就可以避免由外部共模事件造成的系统失效引发的关键功能的生存性最大化。这类外部事件主要源头是爆炸或结构损伤，这样的设计将最大可能保持飞机的控制能力。

(2) 在同一设备间的所有设备需要适度的物理上的分离，典型的冗余 LRUs 的间隔目标是 6 ft。为实现这样的目标，LRU 内部的导线距离应最小化。

(3) 位于驾驶舱里的飞行控制系统设备和导线需要考虑鸟撞和外来物撞击的可能性(与飞机的布局和外形有关)。具体的设计措施包括冗余传感器集的物理隔离以及设备前面的结构加强或防护层设计。防护层的应用主要考虑驾驶舱前舱壁处的传感器组件，典型的是升降舵感知组件或线性可变差动传感器(LVDT)。为最小化鸟撞后结构变形造成脚蹬卡阻的可能性，采用单向弹簧单高跷式设计，当鸟撞碰撞到脚蹬时，让脚蹬倒塌，从而不影响脚蹬的位置传感器 LVDT 的位移输出。

(4) 电线和液压管路线在飞机结构上的布局应考虑潜在的共因失效区域的影响，典型的如发动机、轮胎或 APU 的爆破区域、旋转部件所在剖面，有液体污染以及流体泄漏等。飞机导线和液压系统设计应最大可能地进行冗余功能设备之间、与其他系统之间的物理和电器隔离。PFCS 模拟导线隔离包括套筒、护套以及外编织铜线，并以各种鲜艳的颜色以区分飞机的其他导线。同时，冗余的液压管路和飞行控

制导线通常需要确定着色方案。

(5) 为防止主动冷却的失效,驱动控制、能源装置和飞行控制计算机应设计成能在失去主动冷却的情况下运行,环境温度通常考虑为60℃。采用主动冷却的目的是增强驱动控制的可靠性,并满足维修时维修设备的“触摸”温度要求。

(6) 采用液压融合的方法联结副翼有关的能源控制(PCU),以防止单个副翼非正常动作造成双液压能源的丢失。

(7) 对于飞行控制系统的数字式元器件,需要测试单粒子反转(中粒子辐射)对功能的影响。在给定的粒子反转率下,系统的冗余和部件的设计需要评估其符合性。PFC和ACE中采用一定数目通道或监视恢复措施以弥补这种“烦人”的影响。

(8) 为应对暂时性的液压压力下跌,为选中的PCUs增加检查阀以维持PCU的主动模态。同时,PFC增加“少于最小可接受控制”逻辑,并重置ACE监控门限,以防止任何共因事件驱使多个ACE监视器出现错误。

(9) 火山灰造成的皮托管或静压管都堵塞效应,将导致提供给PFC错误的速度和高度数据,并引发方向舵效率的持续变化。为保护方向舵限制,将采用PCU的减压器以提供500 ft雷达高度以上的备份限制。升降舵的减压器通常设置成低压,就火山灰导致的错误大气数据,PFC的正常模态控制律,通过限制和其他手段,设计成可提供可接受的操稳品质。当失去从ADIRS来的大气数据后,飞行控制系统将转换到辅助模式,辅助模式使用副翼数据以实现限制或预调功能。

(10) 雷达罩的损坏将影响皮托管和攻角传感器的测量,正常模式控制率设计应能在雷达罩损害造成错误大气数据或攻角数据的情况下,提供可接受的操稳品质。

(11) 为防止三套液压系统因外翼的结构损失而失去功能,只有两套液压系统的布局延伸到机翼的极端处(外翼绕流板)。结构上通常采用“撕掉”的设计特征,以最小化损伤的传播。两套液压装置通常在内翼处融合。

(12) 三套液压系统都会布局到垂直尾翼上,但有一套采用融合设计以防止垂直尾翼的结构失效造成所有的液压能源失去。采用“撕掉”的设计特征,以最小化损伤的传播。

(13) 起落架和刹车只使用两套液压系统,因此只有两套液压驱动靠近主起机轮。采用“撕掉”的设计特征,以最小化损伤的传播。

(14) 在轮胎的爆破区域内或者以收上机轮的轴为中心的3 ft圆柱体内,不会布局两套以上的冗余导线/液压管路。

(15) 为防止水平安定面的部分损伤或失效,在安定面内侧安装PCUs和系统,每一侧,只布置三套系统中的两套。

(16) 对于发动机转子爆破和APU转子爆破保护,采用广延的系统分离措施以及特殊的液压和导线布置。系统将安装到APU爆破影响区外。为发动机爆破的生

存性,对其中一套液压系统采用隔离设计。

(17) 采用特殊设计特征处理 HIRF、EMI 和闪电效应。所有的飞行控制系统导线在舱壁和联结处采用双重防护。同时,在 PSA 的底盘采用单点接地的方法,并通过 ACE 底盘让信号接地。PFC 和 ACE 在管脚输入设置了滤波阵列。

(18) 为防止水汽结冰,在导线易集结水汽的区域,PCUs 包含了排水孔和排水规定。

(19) 分析单发失效后的情况。分析时假定与失效发动机有关的液压系统失效,机翼前缘的 ACE 布线也失效,使用该布线缓冲的其他信号也失效。必须保证飞行控制系统仍不低于最小可接受控制的控制能力。

(20) 后压力隔板的设计用于保护对左 ACE 的线路和左液压系统的穿透。另外,在该区域的 ACE 线路用嵌合的不锈钢管进行保护,液压管路采用特殊的 CRES 材料以防止受撞击时泄漏。

(21) 为解决可能的地板坍塌,采用对飞行控制路径的垂直分离方法。可沿龙骨梁和地板支撑梁分别在机身顶部和液压管路布置飞行控制线路。

(22) 两个冗余的模态抑制传感器安装在后走廊下,相互之间分离空间很大。传感器安装在地板支撑梁外侧的机身梁的对边,以最大可能减少地板的坍塌引起的两个传感器的损坏。防止误安装的手段是:

- a. 采用非对称的安装板,因此安装板不会倒置;
- b. 替代的 ACE 测试验证了电信号连接不会出错;
- c. 3 孔非对称传感器安装布局,保证安装板上正确的传感器安装;
- d. 在飞机的右侧,安装在地板梁的背面可防止与座椅支撑轨道的干涉,左右传感器数据的不一致可能导致 PFC 失去功能;
- e. 安装后的功能测试需要目视的检查,检查传感器是否与地板梁的底部对齐;目视检查验证传感器安装在地板梁的前面一侧,同时连接器指向飞机的右侧。

冗余的导线和液压管路的设计隔离目标一般确定为 6 ft。在机翼和尾翼中,如存在由结构件如机翼主梁隔离的冗余,设计隔离目标值为 2 ft。

为了最小化维修的错误,系统设计中将设置安装部件或导管的机械上的难度,防止安装中导致对硬件的细微修改。还将采用连接器钥匙、程序接插件、S/W 零部件序列号的交叉检查,精确的线束长度。另外,为保证界面的正确连接和正确运行,需要维修后的替代测试和检查。

4.5.3 典型的功能性隔离设计

ACE 作动器控制功能是分布式布局的,以保证任一 ACE 或支持子系统失去功能后仍能够保持对所有轴的最大化控制。

电源分配给 PFC 和 ACE,以提供 L 28VDC 汇流条上最大化的物理和电流隔离,L、C 和 R FC 的 28VDC 电源供应同样提供功能性隔离,以保证任一或任两路电源汇流条失去后仍维持对所有轴的控制。对连接到 ACE 的导线,为每一轴控

制采用了分离式缓冲器。这样防止一个轴的 PCUs 上的导线失效影响传播到其他轴上。

在常规构型下, ARINC 629 总线功能分配与电源对准(即对于通信, L 28VDC 或者 PSA 加电的 LRUs 发射到 L ARNIC629 总线)。

尽管所有的 PFC 通道在 3 条 ARNIC 629 总线上侦听,但只有 L PFC 通道能够发射信号到 L ARNIC 629 总线,C PFC 通道发射到 C 总线,R PFC 通道发射到 R 总线,以防止 ARNIC 627 的一个发射机失效破坏了 3 条总线。这样的原理也应用到在飞行控制 ARNIC 总线上的 ACE 和其他 LRU 发射机。容错的 ADIRU 是个例外,其发射的信号可同时到 ARNIC629 的 L 和 R 总线。ADIRU 的分析和测试表明,不存在影响两个总线的不可侦测的共模失效。

PFC 和 ACE 只通过单一的 ARNIC 总线从唯一数据源获取数据,这样保证了在正常情况下的数据隔离。例如, R ACE 通常只从 R PFC 获取数据,L ACE 从 L ACE 获得数据等。

液压系统以同样的原理在一个或两个液压源失去功能后提供最大可能的作动器控制功能。一般来讲,L, C 或 R 飞行控制电子总线加载的电子部件分别控制 L, C 或 R 液压系统加载的驱动部件。对称的一对扰流板总是由同样的液压系统驱动。

4.5.4 非相似性设计

PFCS 设计的许多方面都涉及微处理器和 VLSI ASIC 电路。因微处理器存在很多状态,对设计采用完全的分析和测试以保证没有错误发生是非常困难的。ASICs 通常是状态机,它们是为某种特定的应用而专门设计的,这种设计并没有经过经验的证明。

设计错误将破坏冗余策略,甚至会导致多个计算机通道的关闭。为尽可能减少设计错误的影响,那些在 PFCS 设计中采用的非简单和广泛应用的或没有经过 100% 分析和测试过的部件,需要使用非相似冗余设计。这就意味着 PFCS 中可能采用各种非相似的 H/W 组合,非相似的控制/监控功能组合,以及不同的硬件设计团队,不同的部件制造厂家,或者不同的程序编译供应商。

关于非相似性分析和目标,通常假定通过实际采用的设计非相似策略和规划的充分的确认测试,由设计错误引发的共模故障发生的概率是极不可能的。分析和测试的方法概括如下。

1) PFC

- (1) 非相似处理器 & 编译器(相同的软件);
- (2) DO-178 开发过程;
- (3) 分析 & 测试。

2) ACE

- (1) 非相似监控器和控制功能;

- (2) ASIC 开发过程;
 - (3) 分析 & 测试。
- 3) Inertial Data
 - (1) 非相似 ADIRU/SAARU;
 - (2) DO - 178 开发过程;
 - (3) 分析 & 测试。
 - 4) ARINC 629
 - (1) 开发过程;
 - (2) 分析 & 测试;
 - (3) 绕过 ARINC 629 总线的 ACE 直接模式。

PFC 功能非常复杂,其失效的暴露涵盖所有的飞行组织方式。为最小化设计错误的影响,常常将选择多重非相似设计,如三重非相似处理器设计,L、C、R 3 个 PFC 通道是相同的,用一个零件号识别。每一个通道采用了 3 个非相似微处理器,加载的程序来自同样的软件但非相似的编译器。

ACEs 利用 ASIC 技术采用相似设计。需要非常细致的开发过程以验证这些 ASICs 的功能。另外,可采用隔离的非相似监视和控制功能以侦测故障。

4.6 共模分析

4.6.1 共模分析

共模分析(CMA)是一种定性的分析方法,是为确保功能、系统或组件之间的独立性,以满足安全性要求。

共模分析的主要目的是验证故障树/关联图和马尔科夫分析中的“与”事件的独立性问题。应对破坏独立性的设计、制造、维修差错以及系统部件的失效进行分析,同时,还应考虑功能及其各自的监控的独立性。典型案例是系统架构中(包括与其相关的外部信号)应用了相同的硬件和(或)软件,引起不正常的同属故障。

系统设计者根据安全性评估要求,通过共模分析对独立性原理进行验证,具体方法是参考 SAE ARP 4761 等通过 AFHA - SFHA - PSSA - SSA 予以实现。

共模分析主要关注的是灾难级的失效状态,和更一般的级联的和多重的失效,它们在安全性分析中被作为独立要素进行考虑。

共模失效影响分析就是对那些失效可以同时对多个独立性要素有影响的情况进行分析。

共模分析可以通过危害失效状态(所有或选择)完成。

在安全性活动开始之前,其定义的方法论应获得局方的认可。

典型的共模失效源类型如下:

- (1) 软件设计错误;

- (2) 硬件设计错误；
 - (3) 硬件失效；
 - (4) 制造和(或)维修错误；
 - (5) 与强度相关的事件(除非正常的飞行条件、非正常的系统构型等)；
 - (6) 安装错误；
 - (7) 需求错误；
 - (8) 环境因素(如温度、振动、湿度、闪电雷击等)；
 - (9) 内在的危害(除火灾、爆破)；
 - (10) 电磁干扰；
 - (11) 级联故障；
 - (12) 外部共源故障；
 - (13) 技术共模(新技术或供应商的新技术)；
 - (14) 差的制造质量；
 - (15) 维护错误。
-

共模分析的主要目标就是验证能够影响安全性失效状态的那些共模失效：

- (1) 已经被考虑；
- (2) 它们的影响已经被降低到可以接受的水平。

4.6.2 共模分析输入条件

一旦发生共模失效，将导致系统灾难的失效影响。

一般的输入条件如下：

- (1) 系统设计原理；
- (2) SFHA/PSSA。

由上述条件可以获得独立性需求和灾难级失效状态的列表，独立性需求指导系统架构中独立性的部件的设计。

例子：

- (1) 正常功能与应急功能之间没有共模点；
- (2) 正驾驶与副驾驶之间没有共模点；
- (3) 控制和监控之间没有共模点。

4.6.3 共模分析的起始时间

当系统 AFHA/SFHA 或 PASA/PSSA 开始之时，共模分析就随之开始(依赖项目成熟度)。

- (1) 应尽早生成足够的需求以识别共模；
- (2) 应确保上述需求已被应用，且那些共模已被最小化到可以接受的水平。

4.6.4 共模分析过程概述

4.6.4.1 FHA&设计准则(设计选择、隔离准则等)

共模分析的基本流程如图 4-8 所示。

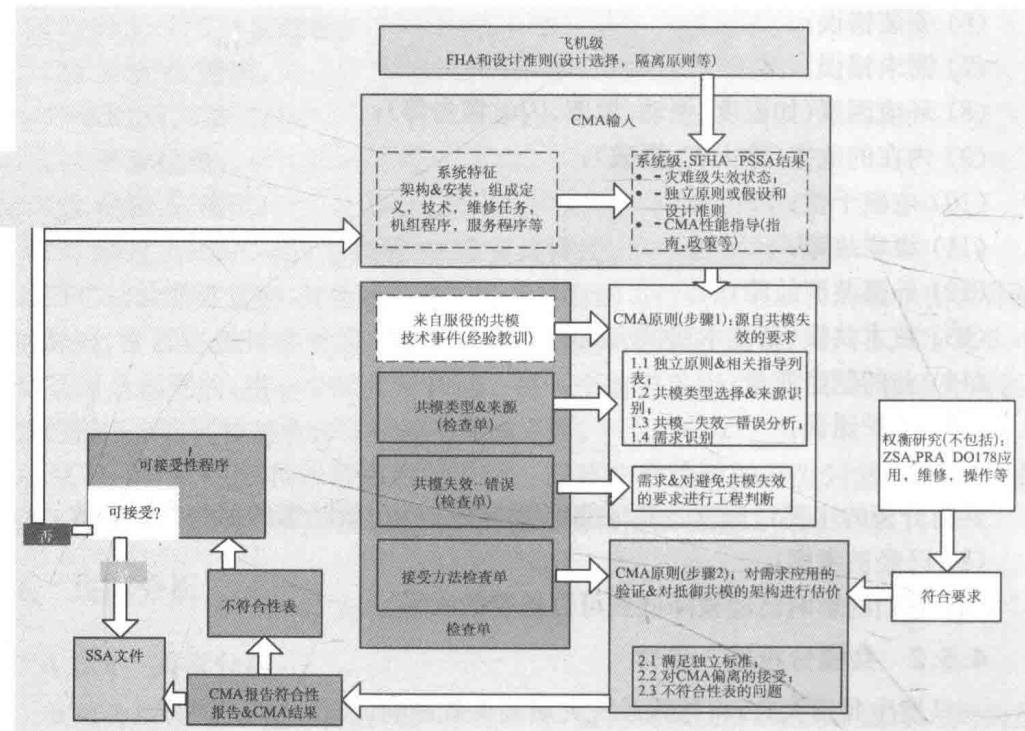


图 4-8 共模分析的基本流程

4.6.4.2 共模分析的过程——CMA 输入

共模分析需要知道与系统特性相关的内容(输入)。

1) 系统的运行和安装

- (1) 设计架构和安装计划;
 - (2) 设备和组成特性;
 - (3) 维护和试验任务;
 - (4) 机组程序;
 - (5) 系统、设备和软件规范;
-

2) 在一些地方采取防御措施以消除或减少共模的影响

- (1) 差异和屏障;
- (2) 试验和预防性的维护项目;
- (3) 设计控制和在设计过程中采取预防措施(质量程序、设计评审等);
- (4) 对程序或规范的评审;

(5) 人员培训；

(6) 质量控制。

4.6.4.3 共模分析的过程——检查单

为促进共模定性分析的实现，需要构建几个检查单。

1) 共模源和类型的识别

检查单应列出与共模类型相关的共模源。那些潜在不同的和可能的共模类型，可能是：

(1) 组成类型，设备类型；

(2) 制造或安装；

(3) 维护、试验和校准；

(4) 其他。

可能的共模源是：

(1) 温度范围；

(2) 共同的制造；

(3) 校准工具；

(4) 其他。

2) 共模失效-错误识别

检查单应列出所有识别出的共模源，不同的失效模式和错误，主要如下：

(1) 使用超过了适用的温度范围；

(2) 由于不恰当的员工培训，导致制造错误；

(3) 不正确的机床调整；

(4) 其他。

3) 可接受的识别方法

检查单的目标就是列出所有可接受的可以处理共模失效的不同方法。

4.6.4.4 共模分析的过程——需求偏离

步骤 1.1：独立性需求和相关指导列表（见图 4-8 共模分析基本流程）。

独立性需求的识别，相关的 SFHA/PSSA FCs 或服役经验和为满足独立性需求在设计中构建的独立性原则。

步骤 1.2：共模类型选择和来源识别（见图 4-8 共模分析基本流程）。

对于每个独立原则：

(1) 在 CMA 检查单中选择可以削弱独立性原则的潜在共模类型；

(2) 调查和识别与所选类型相关的详细共模源，其潜在的失效或错误类型可导致共模。

步骤 1.3：共模失效-错误分析。

对于每个共模源：识别共模失效和错误（使用共模检查单），它们均是被研究的失效模式和错误。

步骤 1.4: 需求识别。

对于每个潜在的共模失效/错误: 问题需求和进行工程判断的目的就是要规避或最小化可接受的共模失效的反复。

步骤 2.1: 符合独立性需求。

对于每个在步骤 1.4 中产生的需求(需求识别): 收集并接受对需求应用的工程判断。

步骤 2.2: CMA 等级偏离的可接受性。

共模失效可以被接受的条件主要依赖于: 在设计、产品、规范、软件等或先前的经验信任等级期间采用预警措施。CMA 分析采用了可接受的检查单方法作为指南。

步骤 2.3: 不符合清单的问题。

如果共模失效或错误不可接受, 可能的方案建议和不符合清单的问题将被执行, 为降低风险, 应对不符合清单采取追踪措施。

共模分析的过程(输出)做如下论述。

CMA 过程的输出是 CMA 报告:

- (1) CMA 报告包括符合独立性原则的判断性文件;
- (2) 如果还存在不可接受的 CMA 情况, 将发布一个详细而明确的不符合性清单;
- (3) 然后, 可接受的 CMA 活动的过程开始启动(CMA 独立过程);
- (4) 根据工程经验和对安全性的影响进行决策, 或者接受共模或者实施更改;
- (5) 这些决策过程应被记录以支持 CMA 报告。

共模分析结果总结包含在 SSA、ZSA 报告中, 人为错误分析(HEA)、可维护性和 PRA 不属于 CMA。但是, 它们的验证分析用以验证 CMA 需求应用满足了共模要求。

4.6.4.5 CMA 检查单示例

CMA 检查单示例如表 4-3 所示。

表 4-3 CMA 检查单示例

序号	阶段和设计	共模类型
1	概念和设计	A: 设计架构 B: 技术, 材料, 设备类型 C: 规范
2	制造	制造
3	安装、集成和试验	安装和集成
4	运行	A: 运行 B: 维护
5	环境因素-特殊风险	A: 机械的和热的 B: 电的和辐射 C: 化学的和其他

检查单包含在飞机 CMA 的操作指南中,该指南应根据型号经验不断更新、完善。表 4-4 给出了供参考的共模分析检查单。

表 4-4 共模分析检查单(供参考)

概念和设计→共模类型:架构设计

共模类型源	共模:级联失效-错误;场景描述	解决共模问题的需求	接受的方法	研究和理由记录
1) 外部共模源 (1) 通风,电的,冷却的,润滑油,空气/液压,数据/信息,重新服役,地面或地球参考点 (2) 其他	(1) 共同的失效源 (2) 共同的回路失效(破裂或堵塞) (3) 有缺陷的接地点(电路开路) (4) 电的瞬态	系统内部需求	(1) 表明需求应用 (2) 确定共模源失效不能导致不可接受的结果 (3) 表明其发生的概率是可以忽略的	(1) 系统描述注释 (2) 系统安全性分析 (3) 系统和依赖 SSA's (4) 依赖系统的 CMA (5) 技术规范
2) 内部共模要素 液压和通风管路,网络数据,电子箱,存储(油箱/数据存储器/能源)	共同元素的失效	系统和设备需求	(1) 确定共模源失效不能导致不可接受的结果 (2) 表明其发生的概率是可以被忽略的	(1) 系统描述注释 (2) 系统安全性分析 (3) 设备级/项目级的 CMA
3) 运行特性(正常运行,备份等)	不适当的运行模式,由于相同硬件失效所导致的降级	系统和设备需求	(1) 表明需求应用 (2) 表明设备的多样性	(1) 系统描述注释 (2) 经验
4) 功能依赖 一旦余度部件的失效导致运行特性的改变	级联失效对余度系统的运行影响	系统和设备需求	表明需求应用	(1) 系统描述注释 (2) 系统安全性分析 (3) 依赖系统的安全性分析

SAE ARP 4754 和 ARP 4761“推荐”实施共因分析(CCA)。ARP4761 中定义的 CCA 分为 3 类:区域安全性分析、特殊风险分析和共模分析(CMA)。CCA 和 CMA 在 ARP 4761 的附件 K 中有进一步的定义。CMA(见 K.3 节)提出“通有”软件研制错误、硬件研制错误和其他类型的错误会影响多个部件的冗余性和独立性;同时,该节也提供了一些处理和减缓这些错误的方法。

5 面向适航的电传飞行控制系统验证

5.1 CVV 活动概述

产品开发过程的典型活动是需求(捕获、分析、分配和分解)、架构和设计实现等,为确保需求的完整性、正确性以及设计实现了需求,需要开展一系列的 CVV (certification validation & verification) 活动,即需求的确认、需求的验证以及适航取证(适航审定活动),如图 5-1 所示。

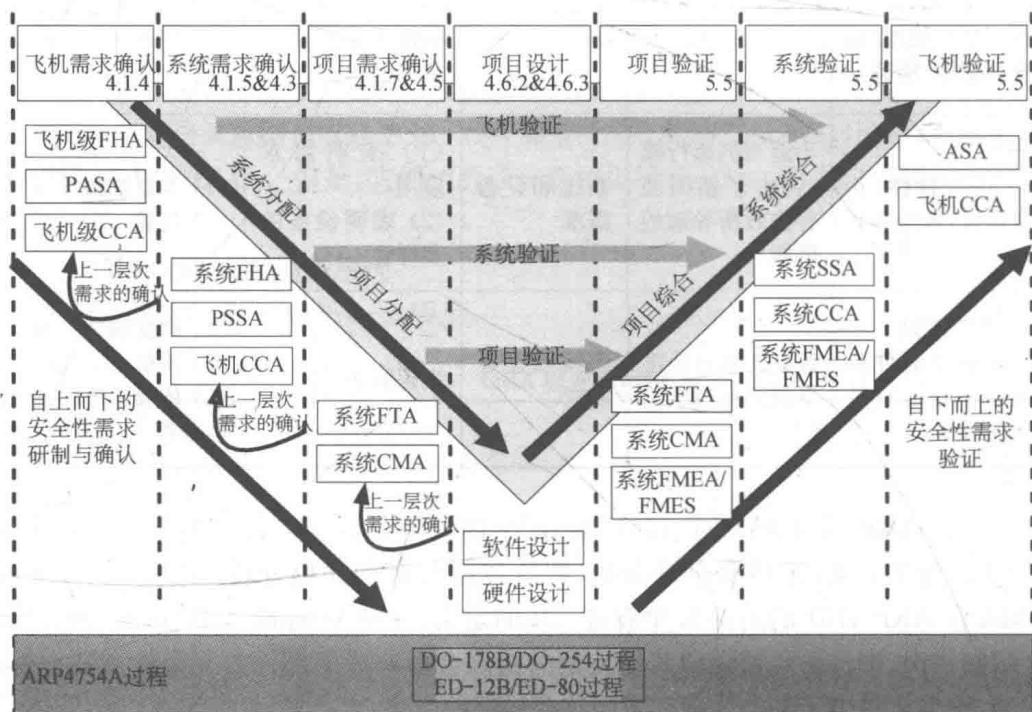


图 5-1 需求确认、验证及适航取证之间的关系

对于民机界典型的主制造商+供应商产品研制模式,主制造商的主要工作在双 V 的上层,即需求、需求的分解和分配,以及系统和飞机的验证;供应商的主要工作

在双 V 的下层,包括对主制造商所提需求的验证,以及所负责工作包开发中的需求分解、分配和设计实现。需求分解到双 V 底部的设计实现,需要在各个需求层级不断地进行需求的确认,代表了设计的成熟度或可行性,从双 V 的底部开始的验证到双 V 的结束,代表了产品开发的成熟度。因此,产品开发中,主制造商对接飞机的用户和市场,更多的任务在飞机级和系统级的需求的确认和系统集成、飞机级的验证,供应商对接主制造商的需求,在主制造商看来为更多的对需求的验证活动,特别是设备级和子系统的验证。主制造商的系统集成能力某种程度上就是需求的捕获、分析和分解的能力。

适航规章的符合性验证(compliance)和双 V 共同构成了 CVV 活动。适航验证活动要求从产品的顶层开始,采用“正向”去规划,而采用自下而上的验证,从系统工程的角度,C 活动应该是双 V 活动的子集或者存在交集。然而也不排除单独的适航验证活动,因为适航验证活动的符合性验证方法是被局方以咨询通报(AC)等要求强制约束的,对于没有足够适航取证经验的制造商,基于某种进度的考虑,先双 V 再 C 活动具备一定的合理性。

5.2 电传飞行控制系统需求确认过程

我们研究的对象是全时、全权限电传飞行控制系统(fly-by-wire, FBW),它是现代民机先进性的重要标志之一,它为提高飞机的性能,改善飞机的飞行品质,减轻驾驶员的工作负荷,增强飞机的安全性、可靠性、维修性以及实现机载分系统的综合控制等,提供了必要的技术手段和工程途径。

目前,FBW 系统向着高度综合的方向不断发展,在获得益处的同时也增加了系统的复杂度,这将导致出现研制错误(需求的确定和设计错误)和不良产品或更大的非预期影响的风险。

传统上用于确定性风险或常规的、非复杂系统的设计和分析方法,已无法向 FBW 系统提供充分的安全性保证。因此,过程保证和确认与验证(validation and verification, V&V)体系组合的研制保证技术已大量应用于 FBW 系统的研制,以确保安全性需求得到满足和把引起失效状态的研制差错降低至可以接受的安全性范围内。

根据民机研制流程标准 SAE ARP4754A《民用飞机与系统研制指南》,需求的确认过程是为了确保所提出的需求是足够正确的、完整的和一致的,且产品能够满足客户、供应商、维护人员、审定局方以及飞机、系统和项目研制人员的需求。对于高度综合的 FBW 系统而言,需求确认是贯穿全部研制周期的一个持续过程,在需求确认的各个阶段,会不断增强对于需求正确性、完整性和一致性的置信度,并最终确保 FBW 系统需求满足适航、客户以及民机制造商要求。

5.2.1 民机 FBW 系统需求确认过程概述

民机 FBW 系统确认过程主要由需求定义、系统确认和问题追溯 3 部分组成,如图 5-2 所示。

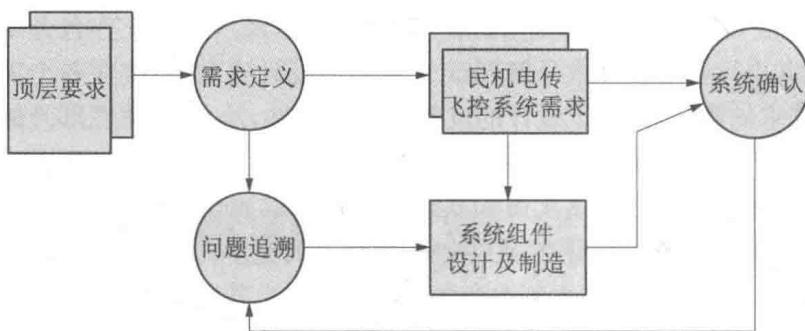


图 5-2 系统需求确认过程

需求定义是对飞机功能及其相关功能需求的确定,包括功能接口和相应安全需求,是建立系统架构和开展设计工作的基础。

需求确认是对各种设备、子系统和系统需求的确认活动,确保产品开发“做对的事情”。

问题追溯为需求定义和系统设计及实现提供闭环反馈,为系统需求、确认活动和确认状态之间的关系提供追溯。

5.2.2 民机 FBW 系统需求定义和确认

需求定义是一个不断细化和反复迭代的过程,主要包括需求定义、文档形成、确认和批准。

1) 需求定义

需求定义采用自上而下的方法,由顶层需求定义主要设计,再进一步到底层需求和设计,主要是通过权衡研究和技术协调完成。

民机 FBW 系统架构权衡研究如图 5-3 所示。应将公司的要求、FAA 的要求、EASA 的要求、客户要求、其他项目上的经验等作为设计要求和目标。系统的候选架构应满足设计要求和目标,将可靠性、成本、重量、气动外形等作为架构选择的权衡要素进行研究。如放宽静稳定性可以减轻飞机重量和减小飞行阻力,但这一要求需要容易实现俯仰增稳的电传飞控系统作为其实现的平台;结构重量也是采用电传飞控系统的优点;通过权衡研究比较机械系统和电传飞控系统的可靠性是相当的;

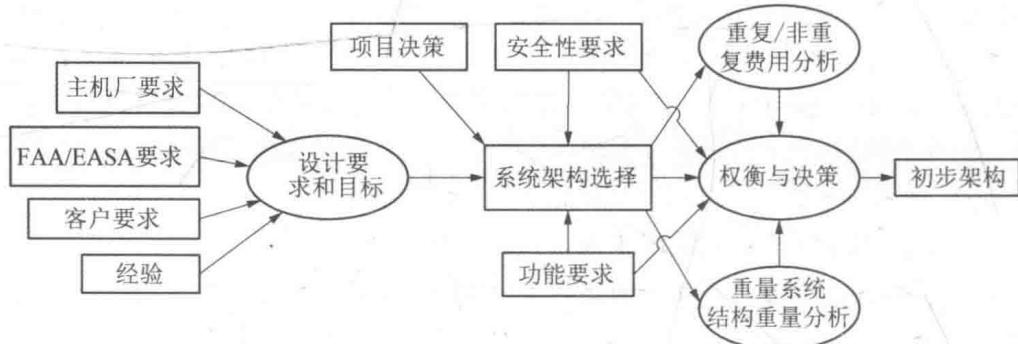


图 5-3 系统架构研制过程

某些 FBW 系统架构比已选择的架构更轻,但是因可靠性低而没有选择;权衡研究的最终结果是一个满足设计要求和目标,并在成本、重量、可靠性和安全性等方面最合适的初步架构。

在定义了飞机需求并选定了系统的初步架构之后,进一步定义下一级系统和部件需求(见图 5-3)。继续进行权衡分析和技术协调,分配各个 LRU 的功能要求和性能要求,定义相应的详细要求以确保满足上层需求。

2) 文档形成

根据需求定义,形成了 FBW 系统的要求和目标文件,该文件涵盖了 FBW 系统的设计理念、定义、设计要求、目标以及设计决策等,阐述了系统的功能、性能、可用性、安全性、隔离、机组操作和维护等信息。

3) 需求确认

需求确认主要是通过追溯、工程评审、分析、仿真和试验等系统确认活动完成,将确认过程中的系统问题不断地反馈,以保证需求的正确性、完整性和一致性,如图 5-4 所示。在系统后期实施阶段,需求确认和系统验证是交替进行的。在大部分硬件和软件可用之前,应完成所有需求的确认,并将其作为详细设计的重要输入。

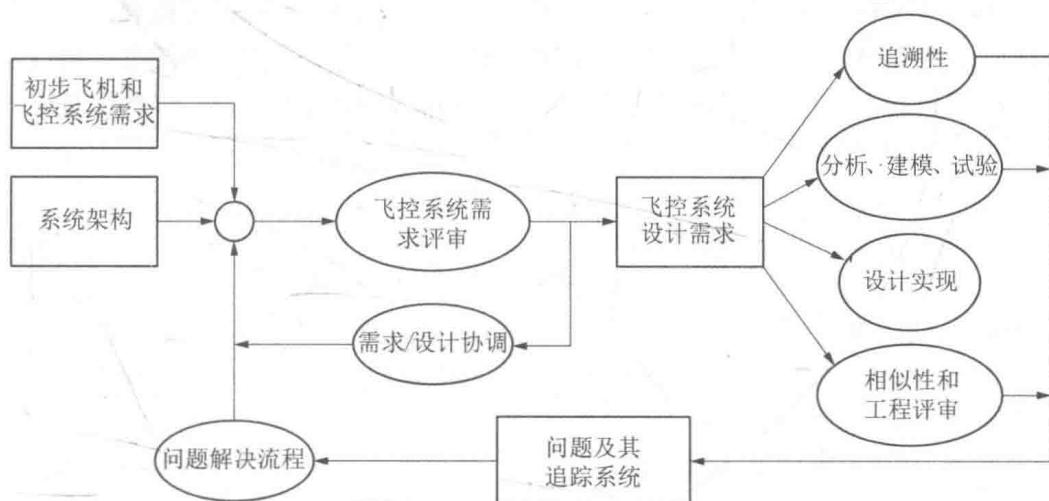


图 5-4 FBW 系统需求捕获及确认过程

(1) 追溯性。

追溯性是较低层级需求与较高层级需求之间所建立的满足关系。在设计决策或设计细节中,有时会增加额外的需求,从而需要获得相应的依据,有些底层需求不能追溯到上一层需求(如衍生需求),这些需求可通过相应的依据来证明其有效性。

(2) 工程评审。

型号早期阶段评审主要是需求的确认。正式评审活动有系统设计评审(SDR)、系统初步设计评审(PDR)和系统关键设计评审(CDR)。应邀请航空公司、适航当局、制造商、供应商、其他项目的同行、与 FBW 系统相关的飞机/系统接口等经验丰

富的人员参加评审。评审工作主要从工程、运行、设备及客户等方面对定义需求的正确性和完整性做进一步的详细评估，并对其中的问题给出反馈建议，同时，后期的任何更改也应进行此类评审。

初期的系统设计评审(SDR)主要集中在系统的总体要求、系统架构、基本设计及项目研制计划。初步设计评审(PDR)提出详细的系统需求和设计思路，并表明在系统确认初始阶段如何证明设计是满足需求的。关键设计评审(CDR)涵盖了从初步设计评审到最终系统评审的所有更改，包括组件的维修性和易达性等。在每个阶段的评审中，都应包含对各个系统性能和安全性分析状态的评审。

(3) 分析。

分析的主要目的是为规避项目后期需求更改所可能产生的高昂费用和进度等方面的风险。该过程主要包括功能危险性评估、安全性分析、性能分析、接口分析和公差分析等，以保证需求的正确性。

FBW 系统的性能分析是为了确认在正常和失效条件下伺服回路和系统的稳定性等相关的需要，包括公差对系统的影响。通过对系统总的累计公差的分析，以确认组件公差需求的合理性和可行性。在项目早期阶段，通过失效及安全性分析，确认与系统安全性相关的需求。功能危险性评估主要是分析潜在的、可能导致系统失效的危险性事件，以便在设计中采取相应的措施加以规避或减缓。系统电气接口分析主要是评估系统电气接口相关软硬件对闪电和高能磁场的兼容性，以确保系统内的信号与 LRU 危险等级相一致。

(4) 仿真。

仿真主要用于确认与控制律相关的需求，以及在不同的操作条件下，从驾驶舱输入到舵面响应整个系统的性能，如稳定性、准确性和快速性等。余度管理仿真确认系统在异步和多余度工作情况下，对系统的影响等相关的需求，包括故障探测、隔离及瞬态抑制等。通过工程模拟器确认系统的操纵品质、人机接口及在正常和失效条件下系统操作等需求。

另外，利用三维软件(如 CATIA、UG 等)将系统中的部件按协调好的位置装配在电子样机中进行仿真分析，以确认相关的需求，主要包括维护性、易达性、与其他设备间可能的相互影响评估等。

(5) 试验。

在项目早期，针对新研发的产品应采用各种已有的试验台和试验手段对与其相关的需求进行确认。如 B777 飞机飞控计算机和作动器控制电子均是航线可替换单元且都是新研发的设备，在项目初始阶段都在试验台上进行了试验分析，用于 B777 上的新作动器在 B757“铁鸟”台上进行了试验，以对其需求进行确认；对 B757 做了专门的适应性更改，以实现对 B777 控制律和驾驶员人机接口需求的确认；利用验证机的飞行试验确认许多系统性能和操纵品质方面的相关需求，包括阵风抑制和推力非对称补偿等新颖特征。

4) 需求批准

FBW 系统的初步设计需求和目标由飞控部及与其系统相关的气动、液压、电源、航电等外部部门共同批准。同时,该文件的后期更改应进行控制。

系统设计需求与目标是系统性能、安全性、维护性和系统功能等项目设计的主要需求来源。

5.2.3 民机 FBW 系统需求确认的实施

系统需求确认工作就是要确保按需求设计的系统能满足设计需求和目标文件中所定义的功能、性能和安全性等方面的要求,确认应考虑设计评审和分析、FBW 系统参与的飞机级的确认活动以及供应商的验证活动等,如图 5-5 所示。

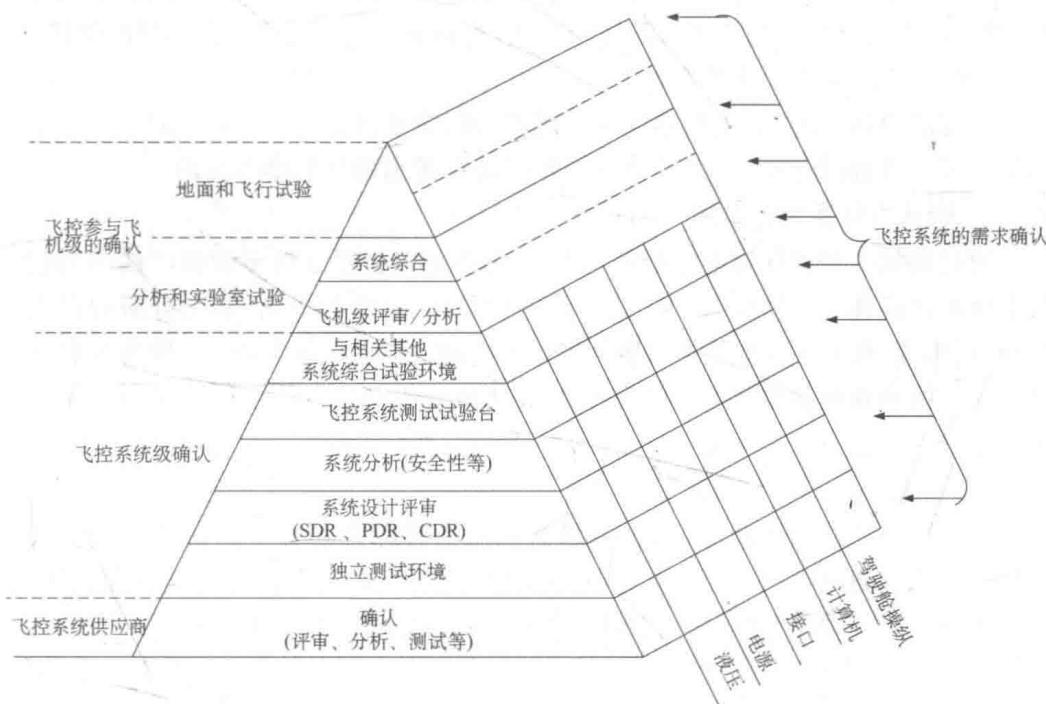


图 5-5 FBW 系统需求确认过程

1) 系统需求的确认

确认所构建的系统满足系统设计需求与目标,确认活动就是将每一条需求严格地对应到合适的确认方法(如试验和分析方法),将所有的确认内容形成确认矩阵的正式文档,且该文档应被批准和存档。

确认的方法和手段主要有正式设计评审、专门评审和分析、供应商验证管理、各阶段验证方法和试验等验证手段,验证按照需求设计的系统是否满足设计需求和目标,是否满足顶层安全性要求等。

(1) 转阶段设计评审。

转阶段设计评审是需求确认过程和系统确认过程的一部分。电传飞控系统和

组件的设计需求进行系统顶层设计评审(SDR)、初步设计评审(PDR)和关键设计评审(CDR),在系统开发的主要转阶段节点上表明系统如何满足相应的需求,并开展相应的构型管控。同时,作为供应商验证过程一部分的部件级评审也相应进行。

(2) 专题的设计评审和分析。

对系统的功能性及性能需求进行确认,分析系统内接口定义和系统间接口定义,包括信号定义、信号内容、域特征、传输频率、延迟和故障模式等。

系统接口分析是确认飞机内部系统信号的兼容性,包括接口控制文件定义的信号名称、刷新率、范围和分辨率等。

(3) 支持飞机级需求确认的系统需求确认。

飞机级的需求确认包括飞机级需求的评审和分析、综合实验室试验和飞行试验。FBW 系统直接参与飞机级的需求确认,为系统提供了精确的和即时的确认。

(4) 供应商验证活动的管理。

供应商完成系统部件或子系统的设计评审、分析和试验,以验证部件或子系统的设计满足详细设计要求,同时,对 FBW 系统的需求确认提供支持。

2) 确认方法及实施阶段

通过确认方法确保对需求的符合性。这些方法主要由初步试验(“铁鸟”试验、机上地面试验和飞行试验等)和分析(稳定性分析、安全性分析、静态分析和误差分析等)所组成,根据不同的研发阶段(分为飞机级、系统级、子系统级、设备级和部件级试验)、效费和难易度等对每项详细要求选择最适合的方法以证明系统对设计要求的符合性。

(1) 试验。

为提供必需的试验验证手段,可能需采用多种综合实验室的试验设施。FBW 系统试验过程如图 5-6 所示,在独立的试验台上对 LRU 需求进行充分的确认;系统级综合试验分别在“铁鸟”台、系统综合试验台和工程模拟器上完成。

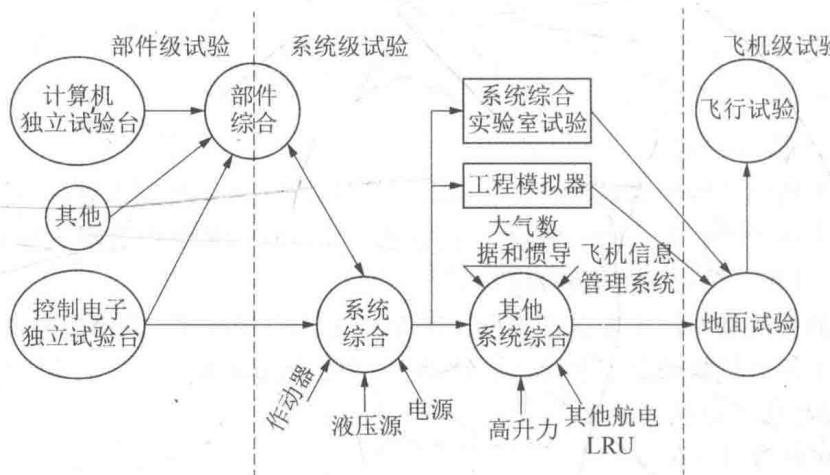


图 5-6 FBW 系统综合试验过程

FBW 系统“铁鸟”试验台主要用于飞控和液压系统试验验证及有限的对飞机需求的确认。该试验台由 FBW 系统、舵面、液压系统、电源及其他对实现系统功能较为关键的飞机 LRU 所组成。

系统综合试验台和工程模拟器主要用于对飞机级的 FBW 系统需求进行确认。系统综合试验台由所有与 FBW 系统有关的航电系统的 LRU、完整的电源系统和驾驶舱显示和控制部件所组成；工程模拟器用于飞行员评估飞机操纵品质和系统的可操纵性，由所有的视觉系统和对飞行员操作比较关键的 LRU 组成。飞机级综合试验在试飞机地面试验和飞行试验中完成。

当某组件更换后，需要在独立的试验台上完成其与接收时同样的测试程序，然后在综合试验台上完成综合测试，并在飞机上完成最终试验，形成试验分析报告、试验总结和正式文件。

(2) 分析。

确认分析分为三类：性能、可用性和安全性。性能分析用于评估在典型环境容限和失效条件下系统的性能和操作，采用线性和非线性时域/频域建模和多种仿真方法。可用性分析主要是静态分析，用于评估系统能满足非安全性需求的能力。安全性分析主要是表明在正常和非正常操作条件下系统都能提供必需的安全等级。

(3) 支持系统的分析和试验。

有些分析和试验被分配到 FBW 系统以外的部门进行确认，这些被其他部门确认的需求应能支持 FBW 系统对其自身需求的确认，如液压系统、电源系统等。

(4) 其他。

还有其他一些对系统需求的确认有较小影响的方法，如检查、相似性以及供应商的试验和分析。

3) 需求分解和分配

在确认过程中，应对在一个或多个确认阶段需开展的确认工作分配相应的需求，并将其落实到具体负责的工作团队，同时，将分组的需求进行文档管理，例如，对特定功能的所有需求放入一个测试文档中进行管理，这个活动的输出是确认符合性矩阵，如图 5-7 所示。

(1) 试验。

试验应是表明需求符合性最理想的方法。采用的试验方法是基于其他系统影响的评估和（或）飞机环境对需要精确控制和监控系统响应的试验结果应是匹配进行选择的。如系统内余度管理最好在独立的试验台上进行评估，而在丧失单发状态下评估系统降级操作（包括飞行员的反应）对飞机要求的评估应在飞行模拟器或试飞试验中进行。

(2) 分析。

由于受项目经费和时间的限制，有些不能通过试验证明的需求，就需要通过分析方法来完成。如基于系统余度等级和期望的部件故障率，分析系统性能、可靠性

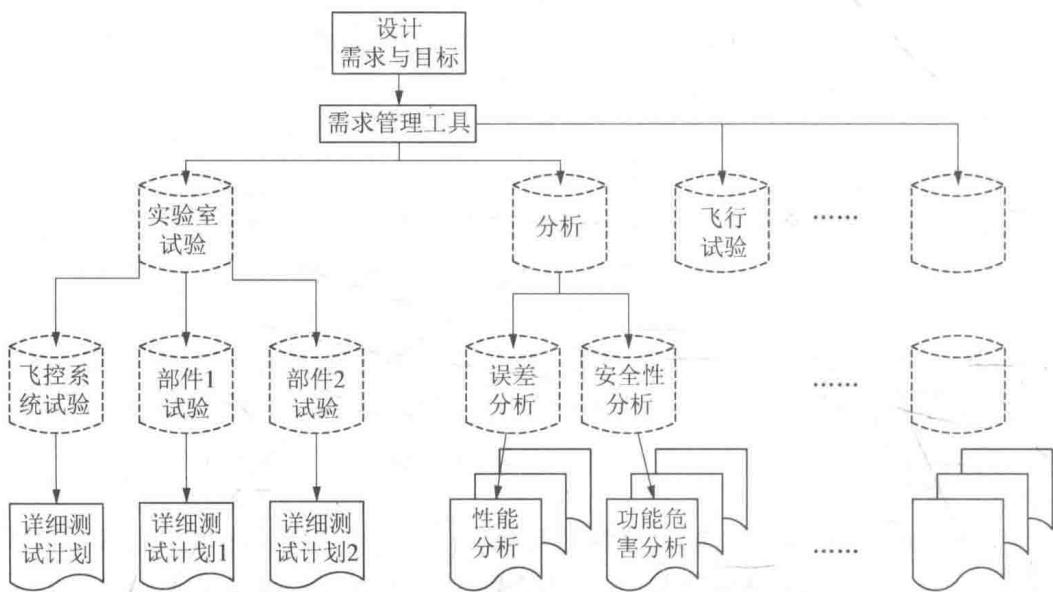


图 5-7 系统需求分配到确认方法的流程

和安全性预估。分析常用于减少那些需要通过确定关键试验条件才能确认的需求试验范围。也用于一些太危险而不能采用飞行试验等进行需求验证的项目。

(3) 检查。

为充分表明安装或文件的评审对需求的符合性，可采用检查的确认方法。

(4) 相似性。

当系统实现是相同的或与早前系统是可比较的，且早前其已被证明满足性能和可靠性特性时，相似性可作为一种确认方法。相似性永远不能作为单独的确认方法。通过证明早前的实现满足当前系统需求的分析或试验以支持相似性的确认方法。

(5) 供应商的试验和分析。

供应商完成大量的试验和分析工作以验证其设计满足规范和图纸的要求，该方法可用于确认系统需求和目标与规范和图纸的共同需求。为采用该确认方法，要求系统需求和目标与规范和图纸之间的追溯路径必须清晰。

支持系统分析和试验：该方法用于那些对系统有影响，却已超出飞控组织责任范围的需求的确认，这些需求已被分解到各自的系统需求和目标中，并通过相关人员进行确认。

4) 覆盖率和可追溯性

通过将设计需求和目标中的每条需求都分配到一个或多个确认活动中，以确保确认覆盖率是完整的。完整的系统覆盖率是通过的每条开发需求都具有一定的严酷度等级。通过委任工程代表批准确认文件，确保相应需求的确认活动是可接受的和完整的，完成的确认文件应归档，当需要时可以查阅。不符合的需求将通过严格

的反馈程序进行管理,决定是否更改系统。需求管理工具用于追溯需求分配确认活动、校核确认过程的完整性等,提供了严格的确认覆盖率和可追溯性、构型控制、确认文件和问题报告等。

5) 需求管理工具

通过需求管理工具保存符合性的条件和结果,从中可获取设计需求、顶层安全性事件、适航计划和相关的验证数据等。

6) 系统需求确认对全机需求确认的支持

系统确认活动的目的是确认系统满足操纵、性能和安全性等方面的飞机级需求,并支持不同飞行构型下其他系统的要求。

飞机级确认包括各种飞机级评审和分析、飞机级综合实验室试验和飞行试验。飞控系统直接参与飞机级确认。同时,为系统确认过程提供准确和及时的反馈。

(1) 设计评审。

对共因故障进行飞机级评审,包括特殊风险分析,如转子爆破、轮胎爆破、鸟撞和坠撞,区域安全性分析和共模分析等。这些评审主要是考虑组件、导线、液压隔离;通过电子样机检查飞控系统的详细安装情况。由可靠性、驾驶舱、试飞员、客户服务和维修培训代表等组成的评审组对各种机组告警信息和部件维修信息进行评审。

(2) 分析。

完成电源中断和上电分析以确保飞控系统对电源变化的反应是可预测且可接受的,包括地面热启动、冷启动、机内自检测、飞行中电源瞬态和飞行后的关断电源等。

另外,就是对潜伏性故障的分析,其目的就是确定系统的失效会否传播到另外一个系统,并对其影响进行评估(包含单个和多个失效的影响)。通过选择实验室和飞机的失效试验来支持分析结果。

(3) 飞机级试验。

试验平台确认用于FBW系统对最终的飞行硬件和软件需求的确认,包括“铁鸟”台、系统综合试验台、工程模拟器和飞行试验机。

系统综合试验台包含了系统大部分的LRU和电源系统,不包含液压系统和作动系统,其主要用于确认整个飞机内部系统间的运行是否满足相关要求。在该试验台上可以确认LRU的失效对FBW系统的影响。

工程模拟器使用了飞行员界面相关的硬件,可进行相关操纵品质、机组程序、系统响应及通告等进行评估,包括风切变条件下系统的性能,飞行中无法实现的或者太危险而不能在飞机上完成的试验。

飞机地面和飞行试验为最终飞机系统综合、飞行员操纵品质评估、操作影响和故障影响确认,如在各种影响飞行员操纵品质的故障条件下进行试飞,包括单发和双发停车、单套和两套液压系统丧失、发电机故障及各种备份模式。

在民机研制过程中,系统需求的确认工作是一项非常庞杂的系统工程,其贯穿整个系统的研制过程,该项工作对系统的研制将有直接的影响。

5.3 电传飞行控制系统的典型试验规划(V&V 活动中试验)

5.3.1 设备级测试

所有的飞行控制设备都需要完成适航的设备鉴定测试和分析,通常适航的设备鉴定测试包含了设备接受程序 ATP 的内容或设备验证的有关试验。在电传飞行控制系统进行 TIA 之前,主要设备的鉴定测试应完成。TIA 前完成的主要设备测试鉴定内容如下。

- (1) 各设备独自的功能、性能测试;
- (2) 温度、高度、湿度;
- (3) 随机振动;
- (4) 电源和液压源的瞬变和降级效应;
- (5) 静力测试(限制载荷和极限载荷);
- (6) 25%的耐久性;
- (7) 液压设备的冲击测试;
- (8) 输入功率限制和功率瞬变;
- (9) 多脉冲闪电效应-只检查单粒子反转;
- (10) EMI 敏感度和辐射。

5.3.2 集成试验测试

通常在实验室利用集成测试平台(integrated test vehicle, ITV)或工程模拟器,尽可能地完成集成的电传飞行控制系统的需求确认。在包括正常运行和不同失效状况下,对于主飞行控制系统满足各种飞行运行体制的确认将通过 ITV 实施。

ITV 测试要求使用真实的飞控电子(FCE),而许多测试用例也使用真实的作动器和液压系统完成。当考虑人机界面或飞行员进入测试时,操纵器件和力感系统是真实的,其他试验台架上的飞行员操纵器件等可用模拟的。至于飞控软件,根据试验需要可以设置许多版本,但一些重要的测试应该使用与取证构型近似的软件版本。

在 ITV 上开展的主要试验项目有:

- (1) 包线保护,包括包线保护功能、包线保护功能可用性、倾斜角;
- (2) 直接模式及该模式下俯仰增强功能;
- (3) 飞行员的通用操作;
- (4) 飞行最小可操纵面(MAC);
- (5) 飞行控制信息;
- (6) 飞行控制模式及转换;
- (7) 俯仰控制——升降舵反应;

- (8) 俯仰控制——操纵杆力数据获取；
- (9) 俯仰控制操纵杆力敏感度测试；
- (10) 俯仰控制舵面作动器失效；
- (11) 俯仰控制舵面作动器限制；
- (12) 俯仰控制飞行员指令输入；
- (13) 俯仰控制水平安定面控制；
- (14) 俯仰控制水平安定面限制；
- (15) 俯仰控制水平安定面作动器失效；
- (16) 俯仰控制水平安定面控制反应；
- (17) 俯仰控制水平安定面切断特性；
- (18) 俯仰控制水平安定面配平；
- (19) 滚转控制副翼作动器非正常模式反应；
- (20) 滚转控制副翼作动器反应；
- (21) 滚转控制襟翼作动器失效；
- (22) 滚转控制襟翼作动器限制；
- (23) 滚转控制襟翼作动器反应；
- (24) 滚转控制在高升力状态下的襟翼和副翼反应；
- (25) 滚转控制副翼作动器限制；
- (26) 滚转控制飞行员指令输入；
- (27) 刹车和扰流片工作——下垂精度需求；
- (28) 刹车和扰流片工作——下垂精度；
- (29) 刹车和扰流片工作——作动器反应；
- (30) 刹车和扰流片工作——自动收放；
- (31) 刹车和扰流片失效；
- (32) 刹车和扰流片工作——地面反应；
- (33) 刹车非作动器失效；
- (34) 偏航控制——方向舵直接模式监控；
- (35) 俯仰控制——驾驶杆切断监控；
- (36) 结构保护——力平衡；
- (37) 瞬态操纵面失效的操纵品质；
- (38) 偏航控制——飞行员指令输入；
- (39) 偏航控制——降低方向舵权限；
- (40) 偏航控制——方向舵作动器反应；
- (41) 偏航控制——方向舵配平；
- (42) 偏航控制——方向舵配平指示；
- (43) 偏航控制——方向舵配平开关监控；

- (44) 飞控控制功能力纷争监控；
- (45) 飞控控制功能软件回归分析；
- (46) 偏航控制——方向舵配平正常模式监控；
- (47) 方向舵指令限制；
- (48) 飞控控制功能振荡监控；
- (49) 飞控计算机通道跟踪；
- (50) 扰流片分解器偏差监控；
- (51) 控制律性能；
- (52) 控制律高迎角性能；
- (53) 失效情况控制律性能；
- (54) 横向控制面配置；
- (55) 扰流片破升功能；
- (56) 倾斜角保护功能；
- (57) 刹车运用；
- (58) 着陆高度修正；
- (59) 横向阵风抑制功能；
- (60) 横航向直接模式；
- (61) 横航向和俯仰陷波滤波器性能；
- (62) 横航向时间延迟和相位延迟；
- (63) 失速保护功能；
- (64) 超速保护功能；
- (65) 俯仰轴空地信号转换；
- (66) 垂向阵风抑制；
- (67) 纵向时间延迟和相位延迟；
- (68) 纵向直接模式；
- (69) 纵向辅助模式；
- (70) 其他。

5.3.3 系统集成测试

还可利用 ITV 或工程模拟器完成电传操纵系统与其他系统间的集成测试，在这种测试里，尽量选用真实的系统和接近取证构型的软件版本实施，这些测试工作大多数在首飞前完成。应编制较为详细的测试程序，以完成如下的测试工作。

- (1) 电源品质测试(首飞前)；
- (2) 飞控系统联试(首飞前)；
- (3) 双重非相似失效测试(首飞前)；
- (4) 发动机失效(首飞前)；
- (5) 大气数据系统故障；

- (6) 单个飞控电子(FCE)柜失效；
 - (7) 多个飞控电子(FCE)柜失效；
 - (8) FCE 柜中部分模块失效(首飞前)；
 - (9) 空地信号失效(首飞前)；
 - (10) 大气数据失效/攻角信号失效(首飞前)；
-

5.3.4 原型机上的测试

通常在数架原型机上开展多项飞行试验,以确认电传操纵系统的功能性需求。主要的试飞科目如下(一般民机可选装多型发动机):

- (1) 带不同发动机的地面最小操纵速度；
 - (2) 带不同发动机的空中最小操纵速度；
 - (3) 带不同发动机的失速特性研究；
 - (4) 带不同发动机的失速特性；
 - (5) 带不同发动机的飞机纵向操纵；
 - (6) 带不同发动机的飞机横向操纵；
 - (7) 带不同发动机的飞机航向操纵；
 - (8) 带不同发动机的飞机机动特性；
 - (9) 带不同发动机的飞机纵向静稳定性；
 - (10) 带不同发动机的飞机横向静稳定性；
 - (11) 带不同发动机的飞机横航向静稳定性；
 - (12) 带不同发动机的反推控制；
 - (13) 带不同发动机的配平特性；
 - (14) 带不同发动机的高速特性；
 - (15) 带不同发动机的侧风起飞和着陆特性；
 - (16) 人工冰型飞行试验；
 - (17) 构型偏离清单(CDL)；
 - (18) 电传飞行控制系统模拟失效飞行试验；
-

5.4 适航验证活动

适航验证活动(compliance)就是产生对适航规章要求的符合性验证数据或生成相关资料的活动。通常将符合性验证活动分为 4 类,从局方的观点来看它们分别是:

- (1) 工程试验；
- (2) 工程检查(如飞机客舱内部检查)；
- (3) 分析；

(4) 飞行试验。

站在制造商的角度,更喜欢从产品开发过程谈相关的活动,因此对上述验证性活动,通常的分类是:

- (1) 设计评估;
- (2) 分析;
- (3) 工程试验;
- (4) 飞行试验;
- (5) 供应商验证活动;
- (6) 制造商验证活动。

适航审查双方的实质性接口是申请人提交的经申明的符合性资料,在申请人提交的符合性证据或资料基础上,局方判定适航规章的符合性,而在申请人的符合性验证活动中,局方是选择性介入,介入的方式是批准试验大纲、目击试验等。因此,按业界工作习惯和已有的工程经验,设计了表明适航符合性的 10 种方法,为统一申请人和适航审查双方的认识和信息交流,为统一申请人和适航审查双方的认识和信息交流,设计了表明适航符合性的 10 种方法,如表 5-1 所示

表 5-1 符合性方法定义

代码	名称	使用说明
MOC0	符合性声明	通常在符合性检查单、符合性记录文件中直接给出
MOC1	设计说明	技术说明、安装图纸、计算方法、证明方案、各类飞机手册等
MOC2	分析和计算	载荷、静强度和疲劳强度、性能、统计数据分析,与其他型号的相似性
MOC3	安全性评估	飞控系统初步风险分析、故障树分析、失效模式影响和危险性分析、软件质量计划等(用于规定安全目标和演示已经达到这些目标的文件)
MOC4	实验室试验	在真实的飞控系统和其他能真实反映机上的工作环境下,通过试验(主要是故障试验),验证飞控系统的设计满足相关适航条款或适航专用条件的要求
MOC5	地面试验	通过机上功能试验,验证飞控系统的设计满足相关适航条款或适航专用条件的要求
MOC6	飞行试验	对于飞控系统适用的适航条款或专用条件,在规章明确要求时,或用其他方法无法完全演示符合性时采用
MOC7	航空器检查	如系统的检查隔离、检查和维修的规定等
MOC8	模拟器试验	通过在工程模拟器上进行飞控系统试验,验证飞控系统控制律设计符合适航要求,评估飞控系统故障对飞机的影响,确认飞控系统 FHA 中定义的故障等级,并为试飞风险科目提供支持,验证《飞行手册》中应急程序的可用性
MOC9	设备合格鉴定	如对预期功能的适合性,在临界环境中的性能等(可能被记录于设计和性能声明中)

所有的适航验证活动将在 CP(compliance planning)中进行规划。对于电传飞行控制系统,下面几节将表述适航验证中主要的设计评审、试验等活动内容。

5.4.1 设计评审

5.4.1.1 舵面卡阻评审

第 25.671(c)(3)条明确提出了设计中应考虑的操纵器件卡阻要求,这种要求是一种定性的要求。尽管在电传飞控系统的需求和设计实现中,制造商通常采取措施防止卡阻出现,但是必须证明出现卡阻是极不可能的。工程实践中,往往将出现特定的设计不能够保证卡阻是极不可能的,或者充分证明是极不可能的,所以会采用卡阻后的减缓措施,以保证即使有卡阻的出现,飞机也能继续安全飞行和着陆。

常采用的卡阻减缓方法有局部的结构失效,或者采用剪切,或过载匹配的载荷减少装置等。设计评估通常由制造商的飞控系统、结构工程师及有关供应商做出初步评估,然后进行有局方人员参加的正式评估,评估的对象为电传操纵系统,包括升降舵、方向舵、副翼、襟翼及扰流板的作动器设计(图纸和实物)或(和)剪切装置等(图纸和实物)。

5.4.1.2 区域/隔离措施的评审

设计评审的目的是确保系统的安装设计满足部件隔离的需求。隔离的需求保证了类似轮胎失效和非包容性转子爆破等事件造成飞控功能的完全丧失,通常采用高真实度的数字样机按区域分区进行,重点检查液压导管和电气连结线。由于受飞机物理空间限制,如果发现隔离需求不能得到满足,应记录所有影响飞控电气连接线的偏离,这种偏离还可以通过机上的安全性工程评审来解决。

5.4.1.3 安装和标识的评审

对于飞控系统安装的评审是保证对第 25.611、25.671(b)、25.685(a)(b)(c)条的符合性,即:

- (1) 检查、更换零件和润滑的可达性;
- (2) 标识以防止装配错误;
- (3) 防止 FOD 进入驾驶舱;
- (4) 防止卡阻、摩擦、干扰。

按 MSG-3 和 CMR 维修任务要求,提供可达性和合适的检查任务支持。

对于飞行员操纵器件,主要的措施为:

- (1) 装配销孔;
- (2) 驾驶杆扭力管的特征检视法;
- (3) 侧向力感杆的特征检视法;
- (4) 方向舵脚蹬主轴检视法。

为正常更换或调整零件提供手段。适用的零件通常包括:

- (1) 手轮、操纵台和方向舵配平的开关;
- (2) 力传感器;

- (3) 位置传感器；
- (4) 方向舵配平和升降舵力感作动器以及推杆器；
- (5) 操纵台模块。

识别潜在的卡阻的设计特征如下：

- (1) 留有维修人员放置物件的位置；
- (2) 可以让器件直接落入到有害位置的区域；
- (3) 紧固件扭出导致超出正常运行范围的操纵卡阻；
- (4) 不能排水的区域，可能积聚水汽结冰导致卡阻或者其他部件损伤。

具备上述特征的一些典型的操纵器件为：

- (1) 方向舵盖板；
- (2) 驾驶杆灰尘封条；
- (3) 槽封垫条；
- (4) 驾驶杆扭力管 FOD 盖板；
- (5) 脚蹬 FOD 挡板。

临近操纵器件区域的部件，应保证在飞机的动态飞行环境下不碰撞操纵器件，并且在运动部件或系统运行时互相不能碰撞。

5.4.2 分析

5.4.2.1 安全性分析

安全性分析的目的是评估飞控系统的设计对安全性需求的符合性。安全性分析中应包含细节的符合性判定、对事件的准确描述以及数量分析结论（概率的计算），也包括安全性分析中某些假设的试验验证等信息，最后用 SSA 等材料证明对规章的符合性。

5.4.2.2 电传飞行控制系统的性能分析

性能分析的目的是按预期的运行模式和条件，电传操纵系统能够在整个飞行包线范围内实现预期的功能。这也是适航规章第 25.1301 条的要求和符合性。性能分析将重点关注稳定性裕度、操纵容差、功能性反应、机动控制和实际的时间延迟、振荡失效的解决措施以及作动器监控的设计方法、力纷争疲劳监控等。

5.4.2.3 飞机级的分析

飞机级的分析是选择几个关键的飞机级功能，并分析这些功能集成后的行为和性能。选择的功能将涉及多个 LRUs 和子系统，也涉及与全机布置资源之间的界面处理。飞机级分析是一种自上而下的需求确认，是从正常运行条件及全功能运行的角度来实施的，因此，这些分析将确认飞机能够在正常运行条件下运行，使用的通用方法如下：

- (1) 识别出飞机级功能，以及飞机级功能派生的或分解的系统级功能；
- (2) 确认系统的架构实现了飞机级分配的和系统级分配的功能；
- (3) 确保飞机级功能和系统级功能被合适地验证和确认。

参与飞机级分析的典型电传飞行控制系统功能为空中操纵和控制飞机、地面操纵和控制飞机以及结构完整性。

5.4.3 试验

5.4.3.1 全姿态的模拟机或 ITV 试验

模拟非常规和极限姿态下的飞机操纵特性,同时考察全姿态下飞行控制与驾驶舱显示之间的协调性,可以邀请飞行员参与。全姿态包括横滚、 $\pm 90^\circ$ 俯仰机动,验证显示和飞行控制中的奇点或非连续性。在这样的试验中,通常将失去自动飞行功能。

5.4.3.2 飞控系统失效条件的演示

通常利用工程模拟机演示飞控系统的失效条件,这些失效条件比正常运行涉及更高的风险。试验主要完成某些特定飞控系统失效条件下飞机的操纵性和操纵品质,以证明在真实飞机上无法验证的功能的正确运行和具备的性能。演示的科目和内容将在相关的符合性验证活动计划(CP)中规划。

典型的演示科目有:

- (1) 反应式风切变警告系统(起飞);
- (2) 反应式风切变警告系统(近进);
- (3) HOSP(hardened overspeed protection),阵风颠倾;
- (4) HOSP,无意的操纵器件移动;
- (5) HOSP,俯冲;
- (6) HOSP,临近 V_d/Ma 的横向操纵;
- (7) 推力控制故障适应(TCMA)(起飞);
- (8) 推力控制故障适应(TCMA)(中断起飞);
- (9) 推力控制故障适应(TCMA)(着陆);
- (10) 推力控制故障适应(TCMA)(复飞);
- (11) 驾驶杆卡阻;
- (12) 脚蹬卡阻;

5.4.3.3 飞机飞行试验

通过安全性分析数据,可以得到需要飞行试验确认的系列工况。需飞行试验确认的工况主要是与监视、瞬态效应、结构需求、系统重构或驾驶操纵品质显著相关的单部件失效条件,这些失效可以通过 FMEA 评估获得;也包括不是极不可能的单个部件失效的组合条件,这些组合条件用于确认分析的假设,或验证最小的操纵可接受水平。有些工况派生于服役中的事故或事故征候报告。

典型的通过飞行试验验证的电传操纵系统失效条件及操纵品质要求如下:

- (1) 直接模式运行,操纵品质要求为“合适的”;
- (2) 失去一个飞控计算机,操纵品质要求为“满意的”;

- (3) 辅助模式运行,操纵品质要求为“合适的”;
 - (4) 襟翼非对称,操纵品质要求为“合适的”;
 - (5) 前缘襟翼非对称,操纵品质要求为“合适的”;
 - (6) 内侧扰流片急偏,操纵品质要求为“合适的”;
 - (7) 单个液压系统失去,操纵品质要求为“满意的”;
 - (8) 双液压系统失去,操纵品质要求为“合适的”;
 - (9) 放 RAT 运行,操纵品质要求为“合适的”;
 - (10) 失去所有的雷达高度信息,操纵品质要求为“合适的”;
-

对于电传飞行控制系统功能正常(非故障情况下)的适航验证飞行试验,需要验证的科目与第 5.3.4 条确认活动中的科目基本一致,具体科目在 CP 中进行规划,只不过适航验证的要求高于或等于确认活动的要求,适航验证必须按照 AC25-7C 中规定的符合性方法进行飞行试验和修正有关的飞行试验数据。

6 电传飞行控制系统研制中的典型适航关注问题

6.1 概述

从宏观的角度,电传飞行控制系统的开发方法和开发过程与其他系统没有本质上的差异,适航要求和对适航规章的符合性方法非常清晰,规划一个较为完整的符合性验证活动,并提供相应的试验项目计划也是容易实现的。但在实践中,电传飞行控制系统的开发往往遭遇较大的困难,包括控制律的开发、系统架构的开发和软件的开发,需要非常复杂的技术和烦琐的工作。据统计,国外新型号飞机一个好的控制律开发需要 50 人的团队工作 3 年多才能完成,需要上百人的团队数年的工作确定架构并完成 CVV 活动,更需要各种模拟器、“铁鸟”台甚至飞机作为开发中的支持手段,以及许多的软件工具等。

同时,从事适航取证和适航审定的工程师也面临诸多困境。根据“适航就是数据,数据就是安全”这一原则,大家普遍感到电传飞行控制系统的适航问题找不到切入点,抓不住关键问题,也难以把握适航的证据或数据,对符合性的判定更是缺乏相应经验。适航工作中出现了关注过程活动和底层失效事件多,关注系统行为和系统的适航性较少的情况,这或许与我国民机电传飞行控制系统的开发方法、开发过程等与国外存在较大的差异有关,与开发经验较少和电传飞行控制系统的典型适航性特征把握不够有关,当然也与相关关键技术的缺失有关。

本章中,将对电传飞行控制系统开发中的典型适航性问题进行阐述,目的是在前面章节的基础上,能够结合具体的飞机型号开发,把握电传飞行控制系统的关键系统行为和适航性特征。

6.2 共模问题

对于共模失效,局方关注的是由相同的、冗余部件的通道和网络设备设计实现的关键功能更易受到通有设计错误的影响,继而导致灾难性的或危害性的飞机级故障的发生。

依据 ARAC 推荐的 AC 25.1309 Arsenal,尽管不能将错误看作是故障,但错误

可能导致故障。在高度复杂且综合化的系统环境中,应当关注单个通有的设计错误在多个、相同部件中出现,继而导致危险或灾难性的失效状态。

AC 25.1309 Arsenal 的 11. b(1)节表明,“根据第 25.1309b(1)(ii)条的要求,一个灾难性的故障状态不能由系统中单个部件、组件或要素引起。系统设计中应有故障抑制措施来抑制单点故障影响的传播,从而消除灾难性故障状态。另外,不应存在同时影响多个部件、零件、要素及其故障抑制功能的共因故障。”

对局方来说,飞机必须满足 FAR 25.1309 - 1B 的要求。依据 FAR 25.1309 - 1B,不管采用了什么样的高可靠性的实现技术,均不接受由单个通道实现的功能丧失的概率小于 10^{-9} 的情况。同时,飞机也必须满足 FAR 25.671。所以,在实践中对飞行关键功能余度通道失效的探测、识别和隔离技术应表明其功能丧失概率小于 10^{-9} (在所有可能的故障或失效情况下,功能可用性和连续性必须满足飞机的继续安全飞行和着陆)。

申请人可以采用非相似的软件和硬件的余度架构,或任何其他的故障或失效影响减缓策略,包括失效-安全设计技术,如转到备用独立功能等,但必须达到上述适航要求。

6.3 电传系统设计的完备性及适航审定考虑

6.3.1 完备性考虑

设计极端可靠的飞机系统要处理两个主要的可靠性因素:物理部件失效和设计差错。物理部件失效可以采用余度和表决的办法来处理。设计差错是在开发阶段而不是运行阶段引入的。设计差错问题包括系统规范中的问题、规范与设计之间不一致的问题、硬件和软件设计实施中的问题等。鉴于完备性无法量化,必须专注于正确的设计和实施,而不是在产品制造出来以后做定量分析的方法去开发。

因此,系统设计的完备性,根据系统设计流程,主要考虑如下几个方面:

1) 系统设计的流程保证

在系统设计过程中应遵循 ARP 4754A、ARP 4761、DO - 178C、DO - 254 等标准,依据 CCAR 25 和相关专用条件等,进行系统设计规范的实施、软硬件开发等。系统的确认和验证,已在第 2 章做过介绍。

2) 系统初步设计

系统设计时应考虑基本设计需求和目标、适航要求、安全性要求、可靠性要求、维修性要求等。结合人-飞机-飞行环境组成的系统,可分为电传飞行控制系统和控制律两个方面,分别考虑电传飞行控制系统各子系统设计和控制律设计的完备性。

(1) 适航要求。

飞机设计时考虑到应能获得中国民航总局、美国联邦适航审定局和欧洲联合适航审定局的批准。飞行控制系统应根据现行有效的 CCAR25/FAR25/CS - 25 部进行适航,且在设计结束前考虑详细所有 FAR 修正案及 FAA 和 EASA 的专用条件

和问题纪要。

电传飞行控制系统应能满足所有电传飞行控制类飞机的适航要求,所选用的货架产品应具有一定期限内的持续适航能力。

(2) 安全性要求。

飞机飞行控制系统及其子系统应根据 SAE ARP4761 进行安全性评估。AC25.1309 要求的危险和灾难要求应满足,每个部件的可靠性应支持系统安全性分析,每个部件的维护任务应支持安全性分析,综合事件导致的重大潜伏故障降低到最少,对于危险性或灾难性故障影响的最大故障暴露时间应受到 CMR 的控制。

飞行控制系统安全性分析应考虑不同的系统输入和系统接口对系统操作的影响,如液压系统、电源系统、大气数据系统、导航系统、刹车系统、机组告警系统、飞行管理系统、中央维护系统等。

飞行控制系统架构设计应最大限度考虑与飞机主要危险源,如高能转子爆破非包容区、鸟撞、火、轮胎爆破的隔离,进而将危险源引起的系统关键功能丧失降低到最小。

飞行控制系统方案必须考虑任何潜伏故障的影响,导致重大安全事件的重大潜伏故障应尽一切可能消除。考虑重大潜伏故障后,一次飞行中的继发故障不论其潜在还是显性,都应在方案中组合,且其不应导致灾难性影响,除非这一故障与前一故障的组合表明为极不可能。

飞行控制系统及其子系统,一次飞行中任何单个因素、部件或连接器,不论其故障概率有多小,此类单点故障不应导致灾难性影响。

造成灾难性或危险性故障影响的最小割集中的单点明显事件故障率应小于 1×10^{-6} /飞行小时或小于 1×10^{-4} /飞行小时。

两个或更多的显性故障与潜在的功能组合时,造成灾难或危险的影响的每个显性故障的概率不应大于 1×10^{-3} /飞行小时。

飞行控制系统应设计成故障不会从系统的一个部分传播到另一部分。该要求适用于硬件、软件和系统。采用故障隔离技术限制故障影响的传播。系统级故障影响的隔离应是鲁棒性的隔离,包括系统个别部件内的故障识别与和隔离,以便将故障对飞机性能的影响减到最小。同时,应考虑由于共同原因可能引起的故障及其级联故障。

飞行控制系统部件安装布置应满足区域安全性要求。共模故障不应影响飞行控制系统安全。复杂电子应考虑非相似,确保飞行控制系统最小控制构型等。

(3) 可靠性要求。

飞行控制系统尽量采用有成功使用经验的现成技术,并做好部件设计方法和材料选择。满足平均故障间隔时间(MTBF)要求,满足飞机派遣率的目标。

(4) 维修性要求。

利用机内自检测(BIT)和中央维护计算机提高维修能力。系统应有容错功能,

且只要可能,任何所需的维修工作能推迟到标准服务周期的结束。飞行控制系统执行的维护功能应提供(半)自动系统测试、自诊断和零位调整,使组装时间和使用中回程起飞准备时间最短。飞行控制系统的功能应保证实现在客户支持协议中规定的平均维修时间和维修人时/飞行小时。

3) 组件设计与开发

电传飞行控制系统的子系统和组件主要包括:驾驶员控制装置,如侧杆、方向舵脚蹬、减速板和襟翼/缝翼控制手柄、作动器控制装置、作动器、传感器、飞行控制计算机、总线和软件等。

6.3.2 适航审定的考虑

目前,采用电传飞行控制系统的民机大都包含了以下技术专题(有的内容也涉及飞机的其他系统):飞行包线保护;侧杆控制器;放宽静稳定性;电传飞行控制系统与飞机结构之间的互相影响;系统安全性评估;雷电的间接影响和电磁干扰;控制信号传输的完整性;电源;软件验证和文档编制,自动代码生成;系统确认;专用集成电路等。

电传飞行控制系统已成为典型的复杂机电系统,需要同时考虑能源、物料和信息的加工和传递,需要实时处理大量的计算和逻辑运算数据,更需要实现高可用性和高安全性目标。除常规的飞行控制系统适航审定工作,为解决电传飞行控制系统的新技术路径,局方将采用如下的专题工作:系统安全性评估;电传飞行控制系统中的子系统或组件的开发;控制律设计。

1) 系统安全性评估

对于安全性评估,现在主机单位往往是做系统集成,飞机主要系统均由供应商提供,相应系统的 PSSA、SSA 也由供应商提供。审定方除关注系统安全性评估各阶段分析的正确性与完整性,建议重点关注:
①安全性评估报告的严谨性,要做到有据可查,描述明确,经得起历史的考验(如相关引用文件改版,建议在系统级 FHA 中给出功能树,警告功能与主通道故障先后顺序应分开讨论,电源短暂中断本身不是故障但可能造成其他系统故障,哪些安全性分析不是由第 1309 条负责);
②飞机级 FHA, PASA(ARP 4754A 提出的要求);
③系统级 FHA 和 PSSA 中与其他系统有交联部分的内容;
④与多个飞机系统有关的功能的安全性评估。如航电系统,几乎与全部机载系统均有交联,要做到相关的功能都有系统负责分析。

特定风险分析是相关资料中提到较多在安全性评估中应注意的。据统计,2010 年我国民航发生事故征候 221 起,其中运输航空 196 起,通用航空 14 起。按事件类型统计,鸟击 109 起,占 49%;雷击 24 起,外来物击伤 24 起,各占 11%,发动机停车 18 起。2009 年发生次数最多的事故征候鸟击占 44%,发动机停车 15%,雷击 10%。说明鸟击、雷击、外来物撞击等特定风险占有很大比例,且有继续上升的趋势。特定风险分析是要重点关注的,同时对于系统集成商来说,CMA 和 ZSA 的正确性、完整性也是需要局方特别关注的。

2) 子系统开发

侧杆或杆/盘控制器、指令信号传输的完整性、电源、电磁干扰、软件验证和文档编制、系统需求的确认、专用集成电路可归为子系统或组件开发时予以考虑。任何一个航空设备开发项目中，无疑有大量的工程设计工作。局方较为关注的问题是系统需求、安全性评估、环境合格审定、软件质量保证、复杂硬件设计质量保证等。

(1) 侧杆。

对于传统的驾驶杆盘，控制舵面的偏转角度与其输入成比例关系，如果飞行控制杆回到中立位置则舵面也将返回中立位置，飞机依靠其自身稳定性也将回到平衡位置。若飞行员希望保持一定的飞行姿态，只能通过不断地飞行控制驾驶杆(盘)或对舵面进行配平。侧杆的输入指令与飞机的姿态角而不是舵面偏转角的变化速率成比例关系，该系统本身具有自动配平、姿态保持和稳定功能。即当侧杆飞行控制飞机到达要求的姿态，飞行员只需释放侧杆，侧杆回到中立位置即意味着告知计算机当前的飞行轨迹没有变化(姿态角变化速率为0)，飞机将自动保持姿态，不再需要飞行员进一步的飞行控制输入。

侧杆采用电子耦合方式，CCAR/FAR/JAR-25 没有说明这类控制器对飞行员力量及操作力的要求；CCAR/FAR/JAR-25 没有规定 A/P 快速释放控制器的配置和方式，而具有 FBW 和 A/P 的飞机通常都把该控制器置于侧杆控制器手柄上；CCAR/FAR/JAR-25 没有对侧杆控制器的飞行品质符合性进行规定。

(2) 人为因素。

美国国家运输安全委员会(NTSB)发布的年度飞行事故数据分析显示，自 1997 年以来，大约 80% 的飞行事故都涉及由飞行员或是地面操作人员引发的人为错误，约 50% 的事故受到恶劣天气等环境因素的影响，20% 是飞机本身存在问题。

下面列举几个人为因素导致空难的例子：

1993 年 7 月 23 号，从银川飞往北京的 BAe146-300 型飞机在银川机场未能离地，冲出跑道，造成机上 112 人中 56 人死亡，事故原因：①飞行员违反规定，起飞前未按规定念检查单，也没看襟翼指位表的指示；②飞行员未放襟翼于起飞位置，在襟翼未放出的情况下起飞，造成滑跑距离长，飞机拉不起来，冲出跑道，发生事故。

1993 年 4 月 6 日，一架 MD-11 型飞机，执行北京至洛杉矶航班。在距美国阿拉斯加州谢米亚以南大约 950 n mile 的巡航飞行中，飞机的前缘缝翼意外放出。飞机经过几次猛烈的俯仰颠簸，失去高度 5000 ft。在此期间，自动驾驶断开，机长手动飞行控制飞机，恢复稳定飞行后，改飞谢米亚美国空军基地备降，飞机正常降落。由于几次猛烈颠簸，飞机客舱内部设施，包括座椅、顶板等大面积损坏。机上 16 名机组人员中有 7 人受重伤，而 248 名乘客中，有 2 人死亡、重伤 53 人、轻伤 96 人。1999 年 10 月 17 日，执行昆明—香港航班的波音 B757 型飞机，发生了同类型差错。飞机在下降过程中，突然上仰随后又下俯；自动驾驶仪自动脱开并发出警告，数秒内，飞机从 21000 ft 俯冲到 19000 ft。结果，该航班的 160 位乘员中，有 47 人不同程度

度受伤。事件调查结论表明,某机型的襟翼操作手柄存在设计缺陷,容易让机组无意识中移出而放出前缘缝翼。

1994年6月6日,原中国西北航空公司所属的TY-154M型飞机执行航班任务。起飞之后飞机发生飘摆,机组无法控制,约10 min后飞机空中解体坠毁。机上146名乘客和14名机组人员全部遇难身亡。此次事故的直接原因是维修人员在更换ПКА-31安装架时,将倾斜阻尼插头(Ш7)和航向阻尼插头(Ш8)相互错插,地面通电试验检查不出故障,导致该机带着错插线路故障起飞。按TY-154《飞机飞行手册》第8.8.3条的规定,解除飘摆状态必须同时关断“航向”“倾斜”和“俯仰”阻尼器。从飞行试验结果看,关断阻尼器后飞机是可控制的,但是飞行员没能按照这一要求去做。遗憾的是在机长命令检查工作舵机及应急检查单时,机组成员中有人主张断开全部舵机,也有人认为不能断开舵机。而同样发生在俄方的数起事件中,俄方驾驶员轻而易举地进行了处置,即断开上述三套系统的全部控制电门,让飞机处于驾驶员人工操控状态,因此而没有损失任何飞机和乘员。

1992年7月31日,原中国通用航空公司所属的雅克-42型飞机,执行南京至厦门航班,在南京大校场机场冲出跑道,机上126人中109人死亡、17人受伤。此次事故的直接原因是飞行员未把全动式水平尾翼调到与飞机重心相适应的角度起飞,致使该机起飞滑跑过程中始终未能离地,最终造成冲出跑道,飞机解体。根据该航班飞机的起飞全重和重心位置,该机起飞前必须将平尾调到-10.3°位置,而当时是在0.2°。按雅克-42型《飞机使用手册》,平尾在1°至-5°范围内,飞机是拉不起来的,这就是滑跑起飞的飞机未能离地的主因。此外,该机的驾驶员在未按程序调对平尾位置的情况下,又盲目地解除了飞机的“起飞警告”。失去不正常起飞状态警告的提示作用,也是本次重大航空事故的重要原因。

上述例子表明,人为因素导致的事故往往是因为飞机设计而导致的问题,飞机设计时应考虑驾驶员-飞机-飞行环境组成的系统。如驾驶员诱发振荡,主要原因是飞机设计(特别是飞行控制系统)中存在不足导致驾驶员与飞机之间出现了不良耦合造成的。

3) 控制律设计

上述飞行包线保护、静稳定性、电传飞行控制系统与飞机结构的互相影响,除了飞机设计,还与控制律的设计有关,分析如下。

(1) 正常过载限制。

典型的机动包线,如图6-1所示(V-n图),边界上和边界内的空速和载荷系数的任一组合,均必须满足强度要求。在CCAR 25.1501中规定的飞机结构使用限制时也必须采用此包线。

飞行包线图中各项含义如下:

A点:飞机处于大迎角下达到的正限制载荷系数;

D点:飞机处于小迎角下达到的正限制载荷系数;

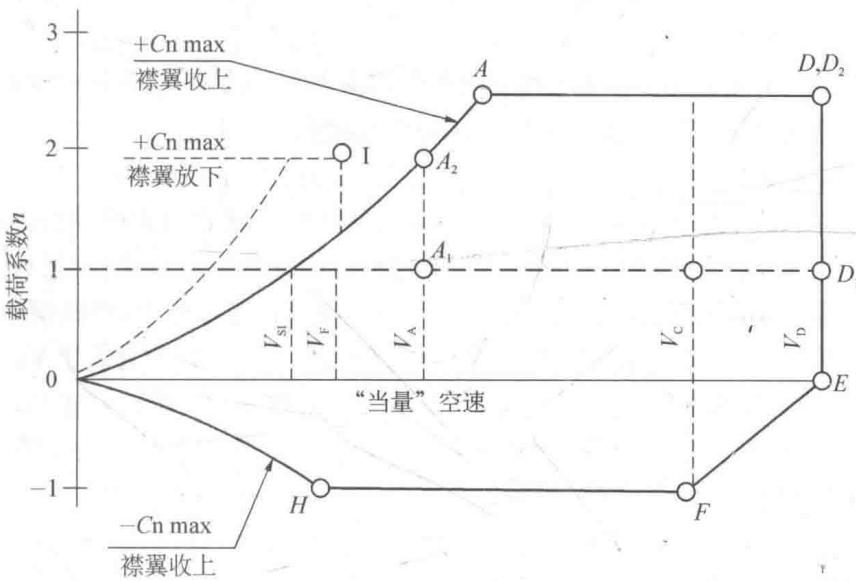


图 6-1 飞行包线

H 点：飞机处于大负迎角下达到的负限制载荷系数；

F 点：飞机处于小负迎角下达到的负限制载荷系数；

D_2 , D_1 和 E 点：表示在飞机最大俯冲速压下结构局部强度的最大受载情况；

V_c ：设计巡航速度；

V_d ：设计俯冲速度。

根据飞机结构强度设计及飞行包线的设计投入到商业运行的 A320《飞机飞行手册》规定了飞机正常操作时的机动载荷限制值。缝翼和襟翼都收起： $-1g$ 至 $2.5g$ ；缝翼放出，襟翼收起： $-1g$ 至 $2.5g$ ；缝翼和襟翼都放出： 0 到 $2.0g$ 。

(2) 非正常飞行状况。

对于飞行包线的设置没有特定的要求，但必须满足以下条件：

(1) 一般限制条件下的要求。

a. 正常操作：

每一个包线保护机构起始特性的设置必须平稳，而且要与飞机的类型和操作相适应，在驾驶员需要改变航向、速度、高度时不能对其产生相反的影响。

飞机设置的包线保护参数必须与以下一致。

(a) 飞机的结构限制。

(b) 飞机安全操控时的数值。

(c) 临界状态，飞机机动时不能产生危险的状态。机身和系统的耐受性，以及非稳态大气状况，都会产生一个与设计相异的限制值。

b. 故障状态：

飞行控制系统(包括传感器)的故障不能导致降低限制值，从而使得飞机不能获

得安全且可控的机动性。

(2) 非正常姿态。

为防止产生非正常姿态或导致飞机参数偏离正常包线范围,飞行控制系统包括自动保护功能,不能阻碍飞机回复到原来的正常状态。

(3) 超速保护。

§ 25.1505 对最大使用限制速度 V_{MO} 做出说明:最大使用限制速度 (V_{MO}/Ma_{MO} ——空速或 Ma 数,在特定高度取其临界者)指在任何飞行状态(爬行、巡航或下降)下,都不得故意超过的速度,但在试飞或驾驶员训练飞行中,经批准可以使用更大的速度。 V_{MO}/Ma_{MO} 必须定为不高于设计巡航速度 V_c ,并充分低于 V_D/Ma_D 或 V_{DF}/Ma_{DF} ,使得飞行中极不可能无意中超过后一速度。 V_{MO}/Ma_{MO} 与 V_D/Ma_D 或 V_{DF}/Ma_{DF} 之间的速度余量不得小于按第 25.335(b)节确定的余量,或按第 25.253 节进行试飞时认为是必需的余量。

第 25.335(b)节设计俯冲速度 V_D 必须选定 V_D 以使 V_c/Ma_c 不大于 $0.8V_D/Ma_D$,或使 V_c/Ma_c 和 V_D/Ma_D 之间的最小速度余量是下列值中的大者:

a. 从以 V_c/Ma_c 定常飞行的初始情况开始飞机颠倾,沿着比初始航迹低 7.5° 的飞行航迹飞行 20 s,然后以载荷系数 1.5($0.5g$ 的加速度增量)拉起。只要所使用的气动数据是可靠的或保守的,则上述机动中出现的速度增量可采用计算值。开始拉起之前假定具有第 25.175(b)(1)(iv) 条规定的功率(推力),开始拉起时可以假定功率(推力)减小并使用驾驶员飞行控制的阻力装置。

b. 最小速度余量必须足以应付大气条件的变动(例如,水平突风和穿过急流与冷峰),以及应付仪表误差和飞机机体的制造偏差。这些因素可以基于概率来考虑。但是在 Ma_c 受到压缩性效应限制的高度上,该余量不得小于 $0.07Ma$,除非用合理的分析考虑了所有自动系统的影响得到了更低的余度。在任何情况下,该余量不得小于 $0.05Ma$ 。

当飞机在俯冲过程中,速度大于最大使用限制速度 V_{MO} 或最大使用马赫数 Ma_{MO} 时,A320 的超速保护功能就限制了驾驶员的俯冲飞行控制权,使飞机不再做俯冲,将速度恢复到最大使用限制速度 V_{MO} 内。

第 25.235 节(滑行条件)当飞机在正常运行中可合理预期的最粗糙地面上滑行时,减震机构不得损伤飞机的结构。

专用条件:俯冲速度定义:

从小于 V_c/Ma_c 的初始情况开始,推力状态为保持该速度的水平定常飞行,飞机颠倾,沿着比初始航迹低 15° 的飞行航迹(或者小于 15° ,根据飞控系统允许的最大低头操纵权限实现最大的低头姿态)俯冲加速超过 V_c/Ma_c 。然后高速、大姿态或其他告警系统触发后 2 s,以载荷系数 1.5(0.5 的加速度增量),或者松杆状态下系统自动地以更大过载系数拉起。开始拉起时假定推力或功率减小,并且可以使用任何其他的再高速飞行要动过程中可以适用的减速装置。飞行员的连续操纵与

自动系统的时间间隔不小于 1 s。

4) 纵向静稳定性

C^* 准则用于飞行品质评价,按飞行员熟悉的参数确定飞机短周期飞行品质,飞行员通常是根据指令和扰动输入产生的飞机动态响应评价飞机的飞行品质, C^* 准则是一种随时间变化的动态响应要求。这种响应被认为主要是低速飞行控制品质参数的飞机俯仰角速度与高速飞行控制品质驾驶员位置处的法向加速度的组合。优点在于由于飞行员在飞行中实际飞行控制和感受的是 C^* 参数,所以 C^* 准则比较真实和直接地表达了飞行员所希望的飞行品质要求。只要算出它的 C^* 参数的时间过渡过程,便可与所要求的包络线边界进行对比检查,只要时间响应曲线没有超出准则的边界线就认为是满足要求的。

适航要求的静稳定性为获得并维持低于所规定的配平速度的速度,必须用拉力,为获得并维持高于所规定的配平速度的速度,必须用推力(侧杆-迎角)。

杆力-速度曲线的稳定的平均斜率不得低于 $1\text{N}/1.3\text{kn}$ ($1\text{kg}/13.2\text{kn}$; $1\text{lbf}/6\text{kn}$)。

基本上飞机的爬升、巡航等阶段都需通过杆力加以配平且杆力-速度曲线均必须具有稳定的斜率。

静稳定到静不稳定后可通过驾驶员的手动操作如侧杆操作来使飞机稳定,依然可控。

A320 是第一架放宽静稳定度设计的民用客机,放宽静稳定度的飞机,气动中心可以很靠近重心也可以重合,甚至在重心的前面,飞机的稳定度变得很小甚至不稳定,飞行中主要靠主动控制系统(即自动增稳系统)主动控制相应舵面,保证飞机的稳定性。这时为保持平衡只需要较小的甚至向上的平尾升力去平衡翼身组合体的正俯仰力矩(机头向上的力矩)。但是为配平由于翼身组合体升力升起的负俯仰力矩所需要的尾翼向下载荷比普通飞机要小,因而就可以大大减少尾翼尺寸和重量,使其在超声速状态也具有较高的升力,大幅提高飞机性能。

5) 大迎角保护

A320 具体的大迎角保护措施:在正常飞行状态下,当迎角增大时,飞机的速度逐渐减小。当速度减至自动油门接通时的最小速度时,此时自动油门若未断开,则该速度对应的迎角已为最大。如果自动油门断开,则飞行员可继续向后拉杆使迎角增大,速度继续减小直至达到第一级保护速度。如果此时飞行员仍继续拉杆,则迎角仍可继续增大,速度继续减小直至达到最大迎角保护速度,该速度对应的迎角已达到极限。如果此时飞行员松开侧杆,则飞机速度会自动返回到第一级保护速度,这样可以有效防止飞机失速。

失速速度(V_s)是飞机可以飞行控制的正常飞行(状态不变)的最小速度。当飞机速度小于失速速度时,机翼上表面出现气流分离现象,使升力系数降低 $V_s =$

$$\sqrt{\frac{W/S}{0.5\rho Cl_{max}}}.$$

(1) 在此失速速度时,推力为零,或者,如果所产生的推力对失速速度没有显著影响,则发动机处于慢车状态并收回油门。

(2) 螺旋桨桨距飞行控制装置(如果装有)处于符合本条(1)所需位置,而该飞机在其他方面(如襟翼和起落架)处于使用 V_s 进行试验所具有的状态。

(3) 重量为以 V_s 作为因素来确定是否符合所要求的性能标准时采用的重量。

起飞速度(V_2):飞机在一台发动机失效时到距离地面上空 35 ft 时所达到的速度。 $V_2 \geq 1.1V_{MCA}$, $V_2 \geq 1.2V_s$ 用于①双发和三发涡轮螺旋桨和活塞发动机飞机;②无措施使单发停车带动力失速速度显著降低的涡轮喷气飞机(V_{MCA} 为空中最小飞行控制速度)。

空中最小飞行控制速度 V_{MCA} :是指飞机在空中临界发动机突然失效时,在该发动机保持不工作的情况下,可恢复飞机控制,并且以零偏航或坡度不大于 5°,保持直线飞行的最小速度。

在下列条件下, V_{MC} 不得超过 $1.2V_s$:

(1) 发动机处于最大可用起飞功率(推力)状态。

(2) 重心在最不利的位置。

(3) 飞机按起飞状态配平。

(4) 海平面最大起飞重量(或验证 V_{MC} 所需的任何较小的重量)。

(5) 飞机处于腾空后沿飞行航迹最临界的起飞形态,但起落架在收起位置。

(6) 飞机已腾空,地面效应可忽略不计。

(7) 停车发动机的螺旋桨按适用情况处于下列状态之一:

a. 风车状态;

b. 在对于该螺旋桨飞行控制装置的特定设计最可能的位置;

c. 如果飞机具有表明符合 § 25.121 的爬升要求时可接受的自动顺桨装置,则顺桨。

失速速度使用以下方式获得最小速度:配平飞机使其以 $1.2V_s \sim 1.4V_s$ 的速度做直线飞行,在高于失速速度并保证定常飞行状态的速度上,飞行控制升降舵,其飞行控制速率使飞机的速度降低不超过 1 kn/s [1 节(kn)=1 n mile/h=1852/3600 m/s,是速度单位]。

满足第 25.203 条飞行特性规定:①直到飞机失速时为止,必须能飞行控制副翼和方向舵产生和修正滚转及偏航,不得出现反飞行控制现象,不得出现异常的机头上仰,直到失速以及在整个失速过程中,纵向飞行控制力必须是正的,此外,必须能以正常的飞行控制迅速防止失速和从失速中改出;②对于机翼水平失速,在失速和完成改出之间发生的滚转不得超过 20°;③对于转弯飞行失速,飞机失速后的运动不得过于剧烈或幅度过大,以致难以用正常的驾驶技巧迅速改出并恢复对飞机的飞行控制。改出期间出现的最大坡度不能超过:

(a) 对于小于并直到 1 kn/s 的减速率的情况,在原转弯方向大约 60°,或相反方

向大约 30° ；

(b) 对于超过 1 kn/s 的减速率的情况，在原转弯方向大约 90° ，或相反方向大约 60° 。

6.4 舵面震荡问题

俯仰舵面的急偏或震荡是飞行控制系统设计中需要考虑的一种典型故障模式，该模式将导致不安全的飞行轨迹或结构失效，从而妨碍飞机的继续安全飞行和着陆。

造成该种场景模式最大的贡献者通常是输出震荡指令的 ACE 某种失效模式；其次需关注的是姿态测量或惯性导航等系统上的(俯仰速率)失效，其错误的输出被标记为是有效的，产生了升降舵的震荡指令；随后是 ACE 的可以探测出的某种失效，如以 G 载荷机动和外部多样化的俯仰速率组合的形式等驱动的能量控制单元 (PCU)急偏。

在飞行控制系统常用的运行模式，如正常模式、辅助模式及直接模式下，如果失去俯仰增强的功能，也可能引发潜在的俯仰震荡。如果布置有两个 PCU 的飞行控制面的其中一个 PCU 震荡，另一个无故障的 PCU 尽管将极力阻止飞行控制面的震荡，但是，最终该飞行控制面仍将震荡。所以在设计中，应考虑识别出 PCU 的震荡失效模式。

失去升降舵的飞行控制的力感觉功能有可能导致飞行员诱发震荡或者过飞行控制。

6.5 最小可接受控制的定义

本节展示了最小控制面权限的一种定义。利用在可工作的 PCU 数量，评估出能够连续安全飞行和着陆的最小可接受控制权限，这些定义常适用于所有飞行控制系统运行模式。对于 B777 飞机，其 MAC 定义如下：

6.5.1 俯仰

1) 正常模式

- (1) 若自动卸载不运行，则每个升降舵有一个 PCU(全压)；
- (2) 若自动卸载运行，一侧升降舵有一个 PCU(全压)。

2) 直接或辅助模式

- (1) 一个升降舵上和人工或通道台配平各有一个 PCU(全压)；
- (2) 如果水平安定面配平不能工作，则每个升降舵有一个 PCU(全压)。

3) 所有模式

各升降舵有一个 PCU(全压)或，如果两对外侧扰流板对(但是不超过两对)和无内侧扰流板工作，则某一个升降舵上有两个 PCU。

4) 升降舵面卡阻(旋转时，更糟的情况)

非卡阻升降舵和正常水平安定面控制具有两个 PCU。

6.5.2 滚转

1) 发动机停车下的起飞/复飞(V_{mcg} , $V_1 \sim V_{2+15}$)

各副翼和 4 对扰流板(至少一对是内侧的)具有一个 PCU。

2) 副翼和扰流板锁定(高速下)

(1) 两对扰流板(一对是外侧的)工作;

(2) 各襟副翼上有一个 PCU 并且一对外侧扰流板工作。

3) 副翼不锁定(低速下)

(1) 每个襟翼上具有一个 PCU, 并且两对扰流板工作(至少一对是外侧的);

(2) 每个副翼上具有一个 PCU, 并且两对扰流板工作(至少一对是外侧的);

(3) 在一个副翼上有一个 PCU 和另一侧机翼襟副翼有一个 PCU, 并且两对扰流板工作(至少一对是外侧的)。

4) L. E. 或 T. E. 不对称或缝翼控制板的丢失

要求全横向控制。

6.5.3 偏航

1) 发动机停车下的起飞/复飞(V_{mcg} , $V_1 \sim V_{2+15}$)

两个 PCU(全压)。

2) 其他(抗 20 kn 侧风能力)

一个 PCU(全压)。

3) 方向舵控制卡阻(10 kn 侧风能力)

在无发动机失效时保持正常控制。

6.6 低高度下的系统失效导致不安全的飞行轨迹

6.6.1 起飞和着陆情况下系统失效导致不安全的飞行轨迹

起飞和着陆导致不安全飞行轨迹顶事件的原因可能有以下几种:

(1) 错误的输入触发倾斜角保护;

(2) 错误的水平安定面位置指示和告警电子系统的失效;

(3) 失去手轮感觉和手轮回中能力,失去保持手轮处于中心的摩擦力;

(4) 任意两对扰流板失效的非对称急偏;

(5) 一台发动机失效并结合错误的副翼或襟副翼低垂;

(6) 复飞时速度刹车卡阻导致的航迹偏离;

(7) 在低高度下错误的失速保护;

(8) 方向舵配平失控;

(9) TAC 失效引起的方向舵急偏(相对于 TAC 权限)。

6.6.2 双发停车后拉平控制(DEOFC)

本节涉及一个失效组合下的安全问题,即着陆时双发停车耦合某个接口失效,导致 DEOFC 功能停用。当出现错误的襟翼位置数据或丢失襟翼位置数据等故障时,DEOFC 功能停用,将不能在飞机拉平时修正升降舵的偏差,并导致错误的对地面的操作决策。对于 B777 飞机,因为低燃油量下的机组程序指示机组人员用襟翼 20° 着陆并且在襟翼 20° 着陆时并没有要求 DEOFC 满足性能需求,一个 9 h 飞行段中存在着陆阶段 6 min 发生双发停车的暴露时间。襟翼展开超过 20° 后,必定发生的双发停车事件,使得失去 DEOFC 导致灾难级事件。

6.7 着陆时造成飞机的不安全飞行轨迹或飞机冲出跑道的失效

着陆时的危害情况往往由不安全的飞行姿态或者飞行轨迹所致,表现为非跑道着陆和冲出跑道,多数情况下是在有侧风时系统的失效造成了偏航的控制能力小于了偏航的 MAC 能力。最可能的失效组合是小侧风下(如 10 kn)方向舵脚蹬卡阻、双液压动力的失去等。

值得注意的是,在理想的状况下,飞行员可能在整个飞行任务期间都没有操作过方向舵脚蹬,因此,发生脚蹬及方向舵失效的时刻极可能在执行飞行任务的早期,而不是在必须利用偏航控制功能的飞机着陆阶段,在型号飞机不设计失效侦测并通告的情况下,按着陆阶段时间计算失效的暴露时间有可能是错误的,按整个飞行时间作为暴露时间的计算是一种局方可以接受的保守的办法。

6.8 导致不安全飞行路径的多轴或多功能故障

飞行控制系统的功能通常是按三轴定义的,需要考虑同一时刻由于不止一个控制轴(俯仰、滚转、偏航)或不止一个功能发生故障的组合情况,以及该组合情况对飞机安全的影响。

空地逻辑的计算将提供一个信号给飞行控制系统,已决定俯仰轴控制率采用地面模式还是空中模式运行。如果空地逻辑发生错误,当飞机仍在空中时,给出了未通告的错误的飞机在地面的信号,主飞行控制将测试模式或者进入软件数据加载或者关掉俯仰增稳等功能。

如果型号飞机未设计空地逻辑错误的通告手段,计算失效的暴露时间应采用整个任务飞行小时数。

6.9 正常模式的可用性

尽管发生模式转换不是安全性分析的顶事件,但需要分析造成主飞行控制系统跳出正常模式运行的可能的底事件,已获得飞行控制系统的正常模式运行可用性。

跳出正常模式可能发生在一系列条件时,如 AOA 数据无效、惯性数据无效、大气数据无效、飞行员选择直接模式、飞行员操作信号失去等,以及主要的 ACE 不工

作(主要的指必须工作的 ACE 数目)。这些底事件在飞行控制系统的架构设计或安全性分析中是容易识别的,但还存在其他的失效组合触发飞行控制系统跳出正常模式,需要在设计过程中识别并验证,典型的如飞行控制计算机失效、数据总线故障、指令通道被禁止等。

值得注意的是,双发停车后将造成电源的丢失,由此导致皮托管停止加热,从而失去大气数据,跳出正常模式运行。国外飞机设计中,将双发失效后失去正常模式作为预期的后果,不是用 FTA 的办法来分析和解决的,而是作为飞行控制功能没有失去的辅助模式运行,并演示给局方,表明双发失效后飞机能够继续安全飞行和着陆。

6.10 电传飞行控制系统的适航验证试验

对于电传飞行控制系统而言,某些失效条件(及功能丢失或系统故障)需要通过飞行试验或飞行模拟机试验进行确认。由于安全问题,那些试验需要在飞机上完成或者可以在飞机上完成,一直存在争论。这里总结了国外主机厂的一些做法,给出可以或需要在飞机上完成的试验科目。

表 6-2 飞行控制系统失效的飞行试验科目

序号	失效条件	飞行控制品质要求
1	直接模式运行	合适的
2	失去一个飞行控制计算机	满意的
3	辅助模式运行	合适的
4	襟翼非对称	合适的
5	缝翼非对称	合适的
6	襟翼上反(预计角度)	合适的
7	升降舵力感作动器压力低	合适的
8	内侧扰流板极偏	合适的
9	单个液压系统失去	满意的
10	双液压系统失去	合适的
11	放 RAT 运行	合适的
12	失去全部雷达高度	合适的
13	失去左或右 WOW 信号	满意的

参 考 文 献

- [1] 宋翔贵,张新国,等.电传飞行控制系统[M].北京:国防工业出版社,2003.
- [2] HB 6486 - 2008 中国航空工业标准,飞机飞行控制系统名词术语[S].
- [3] 高金源.飞机电传操纵系统与主动控制技术[M].北京:北京航空航天出版社,2005.
- [4] 《飞机设计手册》总编委会.《飞机设计手册》04 册:《军用飞机总体设计》[M].北京:航空工业出版社,2005.
- [5] 鲁道夫·布鲁克豪斯.飞行控制[M].北京:国防工业出版社,1999.
- [6] 郭锁凤,申功璋,吴成福,等.先进飞行控制系统[M].北京:国防工业出版社,2002.
- [7] 《飞机设计手册》总编委会.《飞机设计手册》12 册:《飞行控制系统和液压系统设计》[M].北京:航空工业出版社,2003.
- [8] Ian Moir, Allan Seabridge. 民用航空电子系统[M]. 范秋丽,译.北京:航空工业出版社,2009.
- [9] Favre C. Fly-by-wire for commercial aircraft: the Airbus experience [J]. International Journal of Control, 1994,59(1):139 - 157.
- [10] Rolf Stüssel. The Airbus family progress and set-back in development of european commercial aircraft [J]. AIAA/ICAS International Air and Space Symposium and Exposition, AIAA 2003 - 2884,2003,6:14 - 17.
- [11] Philippe Goupil. Airbus state of the art and practices on FDI and FTC in flight control system [J]. Control Engineering Practice, 2011(19):524 - 539.
- [12] Aplin J D. Primary flight computers for the Boeing 777 [J]. Microprocessors and Microsystems, 1997,20:473 - 478.
- [13] Henning B, Robert M, Munir O, et al. 777 flight controls validation process [J]. IEEE Transactions on Aerospace And Electronic Systems, 1997,33(2):656 - 666.
- [14] Society of Automotive Engineers. Guidelines for Development of Civil Aircraft and Systems [C]. SAE ARP 4754A, 2010.
- [15] Society of Automotive Engineers. Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment [S]. SAE ARP4761,1996.
- [16] 中国民用航空局航空器适航审定司. AP - 21 - AA - 2011 - 03 - R4 航空器型号合格审定程序[S]. 2011.
- [17] 中国民用航空总局. CCAR21 R3 民用航空产品和零部件合格审定规定[S]. 2007.

- [18] 中国民用航空局. CCAR25 R4 运输类飞机适航标准[S]. 2011.
- [19] 朱亮, 黄铭媛, 欧旭坡, 等. 民用运输类飞机电子飞行控制系统适航审定关键技术分析[C]. 上海: 2010 中国制导、导航与控制学术会议, 2010.
- [20] 朱亮. 提升系统工程能力, 实现民航强国之梦[J]. 中国空管, 2012, 5: 55 - 59.
- [21] 朱亮, 张建鹏. “豁免”“专用条件”“等效安全”在适航管理中的差异[J]. 中国民用航空, 2012, 12(144): 67 - 69.
- [22] Federal Aviation Administration. Special Conditions: Airbus Industrie Model A320 Series Airplane [S]. Docket No. NM - 26; Special Conditions No. 25 - ANM - 23, 1988.
- [23] Federal Aviation Administration. Special Conditions: Boeing Model 777 Series Airplanes [S]. Docket No. NM - 79; Special Conditions No. 25 - ANM - 78, 1993.
- [24] Federal Aviation Administration. Special Conditions: Airbus Model A380 - 800 Airplane [S]. Docket No. NM305; Special Conditions No. 25 - 316 - SC, 2006.
- [25] Federal Aviation Administration. Special Conditions: Airbus Model A380 - 800 Airplane [S]. Docket No. NM340; Special Conditions No. 25 - 318 - SC, 2006.
- [26] European Aviation Safety Agency. Airbus A380 Type Certification Data Sheet [S]. TCDS A. 110, 2006.
- [27] Avner Engel. Verification, Validation, and Testing of Engineered Systems [M]. London: A John Wiley & Sons., INC., 2010.
- [28] 朱亮, 韩冰冰, 黄铭媛. 民用航空产品研发和审定活动中的需求分析与管理问题研究[J]. 2013, 109: 53 - 56.
- [29] Electronic Industries Alliance. Processes for Engineering a System, ANSI/EIA - 632 - 1998 [S]. 1998.
- [30] Defense Acquisition University. System Engineering Fundamental [M]. Fort Belvoir: Defense Acquisition University Press, 2001.
- [31] INCOSE. Systems Engineering Handbook, version 3. 2. 2 [M]. San Diego, CA, USA: International Council on Systems Engineering (Incosce), Incose - TP - 2003 - 002 - 03. 2, 2012.

缩 略 语

ACE	actuator control electronics unit	作动器控制电子装置
ACT	active control technology	主动控制技术
ADIRS	air data inertia reference system	大气数据及惯性基准系统
AFHA	aircraft functional hazard assessment	飞机功能危害性评估
AFM	Airplane Flight Manual	飞机飞行手册
ALPA	Airline Pilots Association	美国航线飞行员联盟
APU	auxiliary power unit	辅助动力装置
ARAC	Aviation Rulemaking Advisory Committee(FAA)	航空立法咨询委员会
ASA	aircraft safety assessment	飞机安全性评估
ATA	air transport association	航空运输协会
BCAR	the British Civil Airworthiness Requirements	英国民用适航要求
BCM	backup control module	备份控制模块
BIT	built-in test	机内自检测
BPS	buckup power supply	备份电源
CAAC	Civil Aviation Administration of China	中国民用航空局
CAR	Civil Aviation Regulation	民用航空规章
CCA	common cause analysis	共因分析
CDL	configuration deviation list	构形偏离清单
CDR	critical design review	关键设计评审
CL	completeness level	成熟度
CMA	common mode analysis	共模分析
CP	certification planning	审定计划
CR	certification review	适航审定评审
CRES	corrosion resistant steel	不锈钢
CSAS	control stability augmentation system	控制增稳系统
CSF&L	continues safety flight & Landing	继续安全飞行和着陆
CVV	certification validation & verification	适航确认 & 验证
DDR	detailed design review	详细设计评审
DEOFC	double engine out flare control	双发停车后拉平控制

EASA	European Aviation Safety Agency	欧洲航空安全局
EBHA	electrical-backup hydraulic actuator	电备份液压作动器
EFCS	electrical flight control system	电子飞行控制系统
EHA	electro hydrostatic actuator	电动静液作动器
EICD	electrical interface control documents	电接口控制文档
ELAC	eLavator and aileron computers	升降舵和副翼计算机
EMC	electro magnetic compatibility	电磁兼容
EMI	electrical magnetic interference	电磁干扰效应
EWIS	electrical wiring interconnection system	电气线路互联系统
FAA	Federal Aviation Administration	美国联邦航空局
FBL	fly-by-light	光传操纵系统
FBS	functional break structure	功能分解结构
FBW	fly-by-wire	电传操纵系统
FCDC	flight control data concentrator	飞行控制数据集中器
FCE	flight control electronics	飞控电子
FCPC	flight control primary computer	飞行控制主计算机
FCSC	flight control secondary computer	飞行控制主计算机
FCU	power control unit	动力控制装置
FDD	functional description document	功能描述文件
FFR	first flight review	首飞评审
FHA	functional hazard analysis	功能危害性评估
FRD	functional requirement document	功能需求文件
GTAR	the ground test accept review	地面试验接受评审
HAS	hardware accomplishment summary	硬件完成总结
HCI	hardware configuration index	硬件构型索引
HEA	human error analysis	人为错误分析
HIRF	high intense radiation field	高强度辐射场
HLR	high level requirements	顶层需求
HOSP	hardened overspeed protection	硬超速防护
HVP	hardware verification plan	硬件验证计划
ISIS	integrated standby instrument system	综合备份仪表
ITV	integrated test vehicle	集成测试平台
KCCU	key cursor control unit	键盘光标控制装置
LAR	laboratory accept review	实验室接收评审
LAS	load alleviation system	载荷减缓系统
LVDT	linear variable differential transformer	线性可变差动传感器
MAC	minimum acceptable control	最小可接受的控制
MFD	multiple-function display	多功能显示器
MICD	mechanical interface control documents	机械接口控制文档
MMEL	master minimum equipment list	主最低设备清单

MMR	multiple mode receiver	多模式接收器
MTBF	mean time between failures	平均故障间隔时间
NPRM	notice of proposed rulemaking	法规制定提案的通知
NTSB	the National Transportation Safety Board	美国国家交通安全委员会
PASA	preliminary aircraft safety assessment	初步飞机安全性评估
PBS	physical break structure	物理分解结构
PDR	preliminary design review	初步设计评审
PFC	primary flight computer	主飞行计算机
PFCS	primary flight control system	主飞行控制系统
PHAC	plan for hardware aspect certification	硬件适航审定计划
PMA	parts manufacturer approval	零部件制造人批准书
PRA	particular risk analysis	特殊风险分析
PR	planning review	计划评审
PSAC	plan for software aspect consideration	软件适航审定计划
PSSA	preliminary system safety assessment	初步安全评估
PSSA	preliminary system safety assessment	初步系统安全性评估
QTR	qualification test report	设备鉴定试验报告
RA	radio altimeter	无线电高度表
SAS	software accomplishment summary	软件完成总结
SAS	stability augmentation system	人工阻尼器或增稳系统
SCI	software configuration index	软件构型索引
SDD	system design description	系统设计描述
SEC	spoiler and elevator computer	扰流板和升降舵计算机
SFHA	system functional hazard assessment	系统功能危害性评估
SOW	statement of work	系统工作责任分工
SRD	system requirements document	系统需求文件
SSA	system safety assessment	系统安全性分析
STC	supplemental type certificate	补充型号合格证
STS	system technical specification	系统技术规范
TAP	thrust asymmetry protect	推力非对称保护
TC	type certificate	型号合格证
THS	trim horizontal stabilizer	水平安定面
TLARD	top level aircraft requirements document	顶层级飞机需求文件
TLSRD	top level system requirements document	顶层系统需求文件
WBBC	weight and balance backup computation	重量和平衡备份计算
ZSA	zonal safety analysis	区域安全性分析

索引

V&V 17, 19, 20, 23, 127, 136

A

安全性 1, 4, 5, 7, 10, 11, 15, 16, 20, 23—28, 38, 40—43, 45, 46, 58, 60, 63, 65, 67, 70, 78—81, 85, 86, 88, 89, 91, 103, 105, 107, 108, 110, 111, 113, 120, 121, 124, 125, 127—135, 140—143, 146—149, 157, 158

B

包线保护 6, 8, 9, 32, 33, 107, 136, 148, 150, 151

备份 7, 8, 27, 63, 74, 97, 108, 117, 125, 135

C

操纵品质 10, 29, 33, 83, 84, 130, 133, 135, 137, 143, 144

操纵性能 3, 9

颤振抑制 32, 40

超速保护 138, 152

乘坐品质 7, 106, 107

D

等效安全 28, 29, 32, 160

电传飞行控制系统 4, 6—10, 27—30, 32—34, 83, 89, 102—105, 107—113, 116, 126, 127, 136, 139, 141—148, 150, 158, 159

顶事件 108—110, 156, 157

独立性 15, 16, 112, 120, 121, 123—125

F

放宽静安定性 6

飞控计算机 130, 138, 143

飞行安全性 1

非相似 10, 108, 119, 120, 138, 146, 147

符合性 11, 12, 14, 16, 18—20, 22—25, 29, 30, 33, 38, 41—44, 46—51, 53—56, 58, 60, 62, 63, 65, 66, 68, 69, 75, 76, 78—81, 83, 85, 87, 103, 111, 117, 124, 127, 132—135, 139—145, 149

符合性证据 18, 28, 85, 140

覆盖率 15, 19, 134, 135

G

高度综合与复杂系统 11, 12

功能架构 112

功能危害 73, 89, 94, 103, 104, 110

功能性隔离 114, 118

共模分析 86, 120—125, 135

共模分析的过程 122—124

构型管理 14, 17, 18, 20, 23—25, 65, 104

故障隔离 5, 22, 106, 147

故障模式 40, 132, 155

故障状态 146, 151

光传飞行控制系统 4, 5

过程保证 13, 14, 18—20, 23, 24, 81, 127

过载限制 150

H

合格审定 11, 16, 28, 35, 43, 46, 49, 50, 53, 55, 58, 60, 63, 65, 66, 70, 149, 159

豁免 28, 32, 160

J

计划过程 12, 13

监控 7, 10, 19, 23, 24, 60, 67, 76, 77, 82, 85, 96—100, 106, 107, 109, 113, 117, 119—121, 133, 137, 138, 142

检查单 19, 22, 123—125, 136, 140, 149, 150

K

可靠性 1, 4, 7, 8, 26, 41, 44, 69, 82, 103, 112, 117, 127—129, 133—135, 146, 147

可用性 17, 78, 81, 87, 103, 129, 133, 136, 140, 146, 148, 157

控制律 4, 7—10, 29, 104—106, 110, 112, 113, 117, 130, 138, 140, 145, 146, 148, 150

控制律重构 106

控制增稳系统 3, 4

M

模拟器 38, 40—42, 47, 65—67, 77—80, 83, 86, 88, 113, 130, 132, 133, 135, 136, 138, 140, 145

模式转换 157

R

人工感觉系统 10

S

设计错误 119—121, 127, 145, 146

设计评审 20, 21, 122, 129—132, 135, 141

设计特征 12, 28, 32—34, 69, 83, 117, 118, 142

审定基础 16, 19, 28, 29, 32

失速保护 109, 138, 156

失效条件 104, 105, 130, 133, 143, 158

适航审定 12, 16, 20, 22—25, 28, 29, 126, 145, 146, 148, 159, 160

适航条款 27, 28, 30, 40, 110, 140

适航性 26, 27, 38, 74, 108, 111, 145

适航验证 16, 20, 127, 139, 141, 144, 158

适航要求 12, 27—29, 34, 74, 83, 111, 112, 140, 145—147, 153

双发停车后拉平控制 156

伺服回路 8, 9, 130

T

通道 4, 7, 8, 10, 74, 80, 117, 119, 120, 138, 145, 146, 148, 155, 158

W

完备性 27, 146

完整性 14, 17, 19, 33, 41, 78, 83, 85, 87, 91, 108, 110, 112, 113, 126, 127, 129, 130, 135, 143, 148, 149

维修性 7, 8, 26, 107, 127, 130, 146, 147

稳定性 1—3, 6, 7, 10, 30, 31, 33, 34, 39, 40, 84, 107, 128, 130, 132, 139, 142, 148—150, 153

物理隔离 116

物理架构 107, 108, 110, 113

X

系统工程 11, 127, 136, 160

系统规范 71, 72, 92, 105, 146

系统集成 6, 15, 107, 127, 138, 148

系统开发 5, 11, 12, 16, 91, 103, 132, 149

系统耦合 34

修正案 34, 35, 39, 40, 42, 43, 45, 46, 48, 50—59, 61, 62, 64, 67, 68, 75, 146

需求确认 14, 15, 17, 22—24, 107, 126—129, 131, 132, 135, 136, 142

需求验证 15, 18, 23—25, 134

Y

研制错误 16, 125, 127

- 验证试验 66
迎角 106, 112, 113, 138, 150, 151, 153
影响等级 21
诱发振荡 1, 2, 4, 9, 150
余度 4, 112, 113, 125, 130, 133, 146, 152
- Z**
- 灾难性故障 146, 147
载荷减缓 6, 40, 106, 107, 109
阵风载荷 8
振荡 79, 84, 85, 138, 142
- 指令 1, 4, 7—10, 36, 60, 63, 83—85, 104—
107, 109, 110, 113, 137, 138, 149, 153, 155,
158
指令信号 33, 83—85, 113, 149
置信度 127
主动控制技术 4—7, 32, 103, 159
专用条件 28, 29, 32—35, 83, 85—88, 140,
146, 152, 160
最小操纵速度 30, 32, 139
最小可接受控制 113, 117, 118, 155

大飞机出版工程

书 目

一期书目(已出版)

- 《超声速飞机空气动力学和飞行力学》(俄译中)
- 《大型客机计算流体力学应用与发展》
- 《民用飞机总体设计》
- 《飞机飞行手册》(英译中)
- 《运输类飞机的空气动力设计》(英译中)
- 《雅克-42M 和雅克-242 飞机草图设计》(俄译中)
- 《飞机气动弹性力学和载荷导论》(英译中)
- 《飞机推进》(英译中)
- 《飞机燃油系统》(英译中)
- 《全球航空业》(英译中)
- 《航空发展的历程与真相》(英译中)

二期书目(已出版)

- 《大型客机设计制造与使用经济性研究》
- 《飞机电气和电子系统——原理、维护和使用》(英译中)
- 《民用飞机航空电子系统》
- 《非线性有限元及其在飞机结构设计中的应用》
- 《民用飞机复合材料结构设计与验证》
- 《飞机复合材料结构设计与分析》(英译中)
- 《飞机复合材料结构强度分析》
- 《复合材料飞机结构强度设计与验证概论》
- 《复合材料连接》
- 《飞机结构设计与强度计算》

三期书目(已出版)

- 《适航理念与原则》
- 《适航性:航空器合格审定导论》(译著)
- 《民用飞机系统安全性设计与评估技术概论》
- 《民用航空器噪声合格审定概论》

- 《机载软件研制流程最佳实践》
- 《民用飞机金属结构耐久性与损伤容限设计》
- 《机载软件适航标准 DO-178B/C 研究》
- 《运输类飞机合格审定飞行试验指南》(编译)
- 《民用飞机复合材料结构适航验证概论》
- 《民用运输类驾驶舱人为因素设计原则》

四期书目(已出版)

- 《航空燃气涡轮发动机工作原理及性能》
- 《航空发动机结构强度设计问题》
- 《航空燃气轮机涡轮气体动力学:流动机理及气动设计》
- 《先进燃气轮机燃烧室设计研发》
- 《航空燃气涡轮发动机控制》
- 《航空涡轮风扇发动机试验技术与方法》
- 《航空压气机气动热力学理论与应用》
- 《燃气涡轮发动机性能》(译著)
- 《航空发动机进排气系统气动热力学》
- 《燃气涡轮推进系统》(译著)

五期书目

- 《民机飞行控制系统设计的理论与方法》
- 《现代飞机飞行控制系统工程》
- 《民机导航系统》
- 《民机液压系统》
- 《民机供电系统》
- 《民机传感器系统》
- 《飞行仿真技术》
- 《民机飞控系统适航性设计与验证》
- 《大型运输机飞行控制系统试验技术》
- 《飞控系统设计和实现中的问题》(译著)

六期书目

- 《民用飞机构件先进成形技术》
- 《航空材料连接与技术》
- 《民用飞机全生命周期构型管理》
- 《民用飞机特种工艺技术》
- 《飞机材料与结构检测技术》

《民用飞机大型复杂薄壁铸件精密成型技术》
《先进复合材料制造工艺》(译著)
《民用飞机复合材料构件制造技术》
《民用飞机构件数控加工技术》
《民用飞机自动化装配系统与装备》
《聚合物基复合材料——材料性能》(译著)
《复合材料夹层结构》(译著)
《ARJ21 飞机技术管理》
《新支线飞机设计流程》
《ARJ21 飞机技术创新之路》
《驾驶舱人素工程》
《支线飞机的健康监控系统》
《支线飞机的市场工程》

七期书目

《民机航空电子系统综合化原理与技术》
《民用飞机飞行管理系统》
《民用飞机驾驶舱显示与控制系统》
《民用飞机机载总线与网络》
《航空电子软件工程》
《航空电子硬件工程技术》
《民用飞机无线电通信导航监视系统》
《综合环境监视系统》
《民用飞机维护与健康管理》
《航空电子适航性设计技术与管理》
《民用飞机客舱与信息系统》

巍巍文大 百年书香
www.jiaodapress.com.cn
bookinfo@sjtu.edu.cn



丛书策划 刘佩英
钱方针
王珍
责任编辑 王珍
封面设计 朱懿
责任营销 陈鑫



大飞机出版工程

民机飞行控制技术系列

- 《民机飞行控制系统设计的理论与方法》
《民机导航系统》
《民机液压系统》（英文版）
《民机供电系统》
《民机传感器系统》
《飞行仿真技术》
《民机飞控系统适航性设计与验证》
《大型运输机飞行控制系统试验技术》
《飞行控制系统设计和实现中的问题》（译著）
《现代飞机飞行控制系统工程》



扫描二维码
关注上海交通大学出版社
官方微信



9 787313 141767 >

定价: 65.00元

ISBN 978-7-313-14176-7