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

DOI：10. 19416/j. cnki. 1674-9804. 2024. 03. 021

ARP4754B 与 ARP4754A 的对比分析与实施建议

钱　馨[1]　郭　泰[2*]　任文明[2]　李翊唐[2]　江雨航[2]　张　昭[3]

(1. 中航西飞民用飞机有限责任公司，西安 710089；
2. 中国航空综合技术研究所，北京 100028；
3. 中国商用飞机有限责任公司北京民用飞机技术研究中心，北京 102211)

摘　要：ARP4754 是民机和系统研制领域的关键标准，其对研发保证要求的更新受到民机研制单位和各国适航当局的广泛关注。针对 SAE 最新颁布的 ARP4754B，开展与 ARP4754A 的详细对比分析，对 ARP4754B 的修订背景、修订内容进行全面研究，结合参与 ARP4754B 的修订讨论情况给出重点的修订要点，并结合型号研制经验和适航审查情况针对研制保证规划、飞机和系统研制过程、必要(integral)过程、更改贯彻给出后续研制保证实施建议，从而为研制单位更好地理解 ARP4754B 研制保证要求，并在型号研制中真正贯彻落实 ARP4754B 提供有效参考。

关键词：研制保证；系统工程；民机研制；研制错误

中图分类号：V37　　**文献标识码**：A　　**OSID**：

0　引言

随着飞机各系统之间集成程度的不断提升，尤其当电子技术和软件技术的高度集成系统出现之后，发生错误的可能性大幅提高，特别是那些由多系统共同执行的功能。为此，上世纪九十年代，美国联邦航空局(FAA)邀请国际自动机工程师学会(SAE)制定了一份定义飞机系统及信息的特征和范围的指南，以证明高度综合或复杂的航电系统对适航规章的符合性，并于 2010 年对此指南进行了第一次修订，发布了 ARP4754A[1]，ARP4754A 在 ARP4754 研制保证等级概念基础上进一步提供正确分配研制保证等级的方法，并进一步加强与 ARP4761[2]、DO-178B、DO-254[3]之间的协调。同时在 ARP4754A 中将范围扩展到飞机与系统，并正式提出研制保证的概念，明确了 FDAL 与 IDAL 的概念，同时协调 RTCA 以保证与 DO-178C[4]的一致性。在 ARP4754A 正式颁布后，FAA 在 AC20-174 中明确认可将 ARP4754A 作为构建研制保证过程的可接受方法[5]。

ARP4754 提出了一种基于过程的风险管控方法，旨在确保飞机和系统的安全性和运行需求得到充分识别并维持，该方法在工业方得到广泛认可和应用。2023 年 12 月，ARP4754B[6]正式发布，ARP4754B 最初修订的主要目的是保证内容与 ARP4761A[7]的一致性，在修订过程中针对是否将现有范围扩展，将工业界采用的新的系统研制技术纳入进行了广泛的讨论，最终考虑到 ARP4761A 的出版时间，ARP4754B 决定控制扩展的范围，并在 C 版修订时扩展内容。同时在 ARP4754B 中强调，ARP4754 是最佳实践，不应该作为强制性的规定，可通过等效方法表明对适航的符合性。同时 ARP4754 不涉及对于研制组织的结构划分以及适航活动的职责划分，在参考过程中应避免过度引申。

本文通过对 ARP4754B 与 ARP4754A 进行详细对比分析，结合标准修订目的和工程实践对 ARP4754B 修订内容进行要求解读，明晰标准的主要修订内容、修订缘由和实施重点等，从而为民机

* **通信作者**. E-mail：guotai101@126. com

引用格式：钱馨，郭泰，任文明，等. ARP4754B 与 ARP4754A 的对比分析与实施建议[J]. 民用飞机设计与研究，2024(3)：137-147. QIAN X，GUO T，REN W M，et al. Comparative analysis and implementation recommendations for ARP4754B and ARP4754A[J]. Civil Aircraft Design and Research，2024(3)：137-147(in Chinese).

研制主制造商、系统研制单位提供参考,促进国内工业方与局方对 ARP4754B 的共同理解。

1 总体修订情况

通过对 ARP4754B 与 ARP4754A 的内容进行对比,以及对 ARP4754A 修订历程的跟踪分析,结合 ARP4754B 的章节结构调整,对总体情况进行了分析。主要修订可划分为以下几类:

1) 引用更新

主要是标准引用文件的更新,同时在 ARP4754B 修订过程中与 EASA、RTCA 等组织进行了大量沟通,以保证术语、概念的一致性。

2) 概念澄清

在 ARP4754B 修订过程中,将与 ARP4761A、ARP5150A 共用的术语定义进行了统一。删除验收(acceptance)、一致性(agreement)等共 15 项,新增共因(common cause)、设备(equipment)等共 10 项;修改评估(assessment)、保证(assurance)等定义共 13 项。以“非预期行为”为例,将 A 版中“非预期功能”(unintended function)修正为“非预期行为”(unintended behavior)。

3) 结构调整

在 ARP4754B 修订中,有部分标准结构性调整,主要包括以下几个方面:

a) 将 A 版中必要(integral)过程(注:考虑到第 5 章的流程活动是整个研制活动的最基础部分,因此在此处翻译为必要过程,意味着这些流程是为保证安全性目标实现的最基本、最基础的研制保证活动)中的“审定局方协调”调整到研制保证规划章节,强调与局方的协调和联络是研制保证规划的活动内容,用于支持适航审定过程。

b) 在飞机和系统研制过程章节,增加“研制保证过程输出的总结”,对研制保证的输出数据予以明确。

c) FDAL/IDAL 分配的一般原则保留在 ARP4754B,但详细的 FDAL/IDAL 分配活动转移到 ARP4761A 中进行阐述。

d) 将原有 AIR6110 调整到 ARP4754B,在附录 E 中给出了详细的飞机系统研制过程示例。

4) 要求调整

在 ARP4754B 中,针对研制保证规划、飞机和系统研制过程、必要(integral)过程、改型过程、研制保证目标(附录 A)的要求,均有不同程度的调整,主要针对 ARP4754A 在工业方应用及局方审定过程中存在的模糊进行澄清。主要包括以下几个方面,在后续章节针对不同章节进行详细的对比分析。

a) 研制保证规划方面

将 A 版“研制规划”(development planning)修订为 B 版“研制保证规划”(development assurance planning),同时将原有章节内容中的“研制过程”(development processes)全部替换为“研制保证过程”(development assurance processes),消除了 A 版中将 ARP4754 标准误解为与产品研制相关的系统工程标准,忽略了 ARP4754 标准实质上是一个关于飞机或系统研制的研制保证要求的标准,并将相关研制保证计划要素进行了调整更新。

b) 飞机和系统研制过程方面

为使飞机与系统研制过程进一步清晰化、规范化,在原有 A 版基础上,将其按照系统工程过程划分为飞机功能与需求研制、飞机架构研制及功能分配到系统、系统需求研制、系统架构研制及需求分配到项(item)、实施,使研制过程更加符合系统工程原理[8],相比 A 版更加明确。

c) 必要(integral)过程方面

将飞机安全性评估过程进一步明确为飞机级功能危害评估(aircraft functional hazard assessment,简称 AFHA)、飞机级初步安全性评估(preliminary aircraft safety assessment,简称 PASA)、系统级功能危害评估(system functional hazard assessment,简称 SFHA)、系统级初步安全性评估(preliminary system safety assessment,简称 PSSA)、系统级安全性评估(system safety assessment,简称 SSA)、飞机级安全性评估(aircraft safety assessment,简称 ASA),其余作为支持安全性评估的方法,删除了原有不同研制保证等级推荐的需求确认、实施验证符合性方法和数据。

d) 更改贯彻方面

改为采用工业界对更改大小的定义,重点是澄清了更改贯彻与必要(integral)过程内容之间的关系。针对 A 版中对于改型的分类存在模糊的情况,在 B 版中进行了较为详细的描述,将改型分为新的应用、修改、影响、未修改/无影响,并针对不同的改型影响分类给出相应的研制保证活动要求。

e）研制保证目标方面

ARP4754B 对研制保证目标进行了更新调整,不同研制保证等级对应的研制保证目标数量均有所调整,且具体目标也进行了适应性修订,ARP4754A 与 ARP4754B 研制保证目标数量对比情况如表 1 所示。

表 1　A 版与 B 版不同 FDAL 对应研制保证目标数量对比

版本	不同研制保证等级对应目标数量				
	A	B	C	D	E
A 版	34	34	33	11	2
B 版	29	29	29	11	3

2　研制保证规划对比分析

2.1　修订要点

通过对研制保证规划章节的内容修订,进一步将 ARP4754 标准明确为飞机或系统研制的研制保证要求标准,是以满足飞机、系统安全性为目标的系统工程要求,并不代表完整的系统工程研制过程。研制保证规划章节的修订要点主要包括:

1）明确规划范围

将 A 版中带有模糊或歧义的“规划过程”、“研制规划”、“研制过程”等表达均明确为“研制保证”相关表述。(注:ARP4754B 中的 planning 在本文中翻译为“规划”,表示开展研制保证的计划性活动,而 plan 翻译为“计划”,作为研制保证过程规划的输出。)

2）调整研制保证规划要素

规划要素由八大要素改为七大要素,其中“合格审定”要素删除,“需求管理”改为“需求捕获”,“确认”进一步明确为“需求确认”。被删除的“与局方沟通”过程,纳入到研制保证规划进行说明。

3）新增研制保证计划内容

B 版新增了审定局方协调的主要内容,同时明确研制保证计划应参考引用文件中 3.2.1 节的“设计描述”。

2.2　实施建议

根据研制规划修订要点,针对国内民机型号研制给出具体的实施建议:

1）强化对研制保证的规划活动

研制保证规划过程是保证飞机或系统满足需求并以足够的置信度符合审定基础的研制方式定义,研制保证过程规划的输出就是一份或者多份计划文件,对计划文件的形式不做强制性要求,但是要注意不同规划要素形成计划文件时互相的一致性,形成的研制保证计划也将作为与局方沟通和协调的重要文件。

2）持续与局方保持沟通

B 版指出民用飞机和系统研制过程中与适航局方的协调过程是一个在研制过程中持续不断的过程,并明确将与局方沟通协调纳入研制保证计划内容,目的是尽早就如何满足规章需求和工业标准与局方达成一致,并识别研制保证活动如何有效发挥作用以及确定合适的研制保证数据表明符合性。与局方的沟通协调从规划阶段开始,贯穿整个产品研制过程。

3）更改贯彻要纳入研制保证计划

B 版中也明确指明,根据型号研制的实际情况,如涉及已有产品的重用或改型,应将对现有机型或系统的更改贯彻相关的内容纳入研制保证计划中。对于衍生机型的研制保证计划,建议从衍生机型的可行性论证阶段开始按照 ARP4754B 完成更改贯彻管理过程定义和更改贯彻影响评估,确定衍生机型的更改类别,定义与更改类别相关的研制保证活动,确认重用数据和资料范围,制定衍生机型研制保证计划。

3　飞机和系统研制过程对比分析

3.1　修订要点

飞机和系统研制过程的范围及过程与 A 版基本保持一致,并且 ARP4754 与其它标准,如 ARP4761、DO178、DO254 等标准,在飞机、系统、设备和机载软硬件研制过程中相互协同确保飞机产品安全的关系并没有发生显著变化。这也从侧面印证,这些标准要求在确保民用飞机、系统、设备和机载软硬件安全性方面已经在工业界和相关的适航局方达成了基本共识,并且通过 ARP4754B 和 ARP4761A 标准的修订,强化了相关方法在工业实践中的有效性和可接受性。

具体修订要点如下:

1）明确安全性目标和安全性需求

B 版消除了 A 版中关于安全性目标和安全性需求的模糊之处。A 版中对于安全性目标并没有给出特别的说明和解释,默认将安全性目标也纳入安

全性需求范围,所以在 A 版文字中声称飞机级安全性需求是 AFHA 产生的结果,系统级安全性需求是 SFHA 产生的结果。这种表述对于飞机和系统研制中通过需求管理区分 AFHA 和 SFHA 获得的结果与 PASA 和 PSSA 获取的结果带来了困扰。

2) 强调飞机级架构评估

相比 A 版,在 4.3 节飞机架构研制和飞机功能分配到系统方面,增加了飞机级架构的工作内容,根据功能分析和性能分析及 PASA 评估过程对候选的飞机级架构进行多次迭代评估,最终确保满足飞机顶层安全性目标。

3) 研制系统级功能和需求显性化

作为 B 版新增的独立章节,该部分研制流程在 A 版中属于"飞机功能分配到系统"的内容,在 B 版中进一步明确说明。飞机级功能被分配到系统后,系统级功能需要依据系统在飞机级架构中的角色确定。

4) 系统架构研制和系统需求分配合并

考虑到系统级架构研制和将系统级需求分配到机载软硬件(item)级两个流程紧密耦合,在 B 版中将 A 版中的 4.4 节(研制系统架构)和 4.5 节(将系统需求分配给机载软硬件)两个章节进行了合并。

5) 产品实施过程的精准化修订

此章节名称由系统实施(system implementation)更改为实施(implementation),主要是现代飞机产品的研制都采用了分层、分级和主制造商-供应商的模式,不同层级的产品研制过程都需要遵循系统工程过程,所以 A 版采用的"系统实施"(system implementation)容易误解为是系统层级产品的实现过程,所以 B 版中修订为"实施"(implementation)则是覆盖了飞机、系统、设备和机载软硬件多层级产品的实现过程。

6) 新增研制保证过程输出总结

B 版相比 A 版新增了研制保证过程输出总结,强调应总结研制保证计划中建立的活动,详细说明每个活动对应的产品构型,对研制过程中偏离研制保证计划进行说明和给出理由,总结附录 A 要求的研制保证数据和资料,总结未封闭问题报告(OPR),得出研制保证活动的结果。

3.2 实施建议

1) 持续推动基于系统工程的正向研制

ARP4754 标准中飞机和系统的研制过程是开展整个研制保证活动的主线,国内型号研制应持续强化系统工程的正向设计理念,按照系统工程过程和分层、分级的研制模式,重视对公司级研制程序的定义,将需求工程、验证和确认等研制活动落实到不同研制阶段、不同里程碑节点。更好地理解和贯彻系统性地管理和控制飞机、系统、设备、机载软硬件研制过程中的错误也是实现飞机产品安全性目标的重要工作内容。

2) 重视功能分析工作

在 A 版和 B 版中均强调对飞机功能适当分组是该过程的主要活动,在型号研制中应该对功能如何组织和分组予以更多关注,考虑的关键因素包括产品实现中可能的约束、失效影响和生命周期保障。A 版和 B 版都强调了功能分配过程中产生的假设将是系统需求包中非常重要的内容,B 版更补充强调了应该像需求一样对假设开展确认活动。

3) 明确与软硬件研制过程的接口

B 版中关于硬件设计生命周期过程和软件生命周期过程之间的信息传递内容与 DO178C 和 DO254 的内容基本一致。目前,国内各型号研制均遵循这些研制保证要求。在依据 ARP4754B 开展飞机和系统研制,以及根据 DO-178C、DO-254 开展软硬件开发过程中,应着重关注接口数据的管理。

4) 集成验证工作的系统化

按照 ARP4754B 最新要求,建议在型号研制中针对"非预期行为",制定相应的策略或方法,确定试验验证的层级(如系统内的试验、系统间的试验或飞机级试验)和试验的类型(如基于场景的试验测试、基于目标的试验测试或由有一定资质或经验的人开展的机会测试等)。

4 必要(integral)过程对比分析

4.1 安全性评估

4.1.1 修订要点

为保证与 ARP4761A 内容一致,具体修订要点如下:

1) 共因分析不作为安全性分析流程

B 版明确了安全性评估包括 AFHA、PASA、SFHA、PSSA、SSA 和 ASA 六个流程。不再将 CCA(common cause analysis)和其包含的 PRA(particular risk analysis)、CMA(common mode analysis)、ZSA

(zonal safety analysis)认为是安全性评估过程,而是将其确定为识别和评估独立性需求的安全性分析方法,如物理独立性、安装独立性等。

2) 将飞机级和系统级 FHA 进行区分

为了与 ARP4761 保持一致,将 AFHA 和 SFHA,PASA 和 PSSA,以及 ASA/SSA 都分别进行定义和描述,消除了可能引起的误解和困惑。

4.1.2　实施建议

开展安全性评估主要参考 ARP4761A 的标准内容,在 ARP4754B 中主要是为保证与 ARP4761A 的一致性,对主要的安全性分析过程进行说明,强调其它的必要过程都需要根据安全性评估过程的结果确定过程管理和控制的目标。

4.2　研制保证等级分配

4.2.1　修订要点

研制保证等级分配主要变化是将详细的研制保证分配过程调整到 ARP4761A 的附录 P 中,但保留了对于 DAL 的分配原则。具体修订要点如下:

1) 研制保证等级分配覆盖到 E 级

完善了研制保证等级分配的通用原则,B 版中补充了"无安全性影响"失效状态的研制保证等级分配原则,弥补了 A 版中仅描述 A 级~D 级研制保证等级分配原则的情况,完善了研制保证分配中的误解。也就是所有的飞机/系统功能或机载软件和电子硬件都应该分配有研制保证等级,符合文件 5.2.2 节所述条件的简单硬件器件可以不用分配 IDAL 等级。

2) 简单硬件可通过试验和分析进行安全保证

B 版补充了对简单硬件项的说明。这些简单硬件设备可以识别所有失效模式,设计特征和识别的失效模式可以通过试验和分析的组合方式完全得到保证。这些简单硬件设备无需分配 IDAL 等级,但是其支持的系统功能仍然需要分配 FDAL 等级。其验证和确认活动应该与已经建立和接受的产品研制程序和相关的技术一致。

3) 对不同独立性进行完整定义

B 版对于独立性属性(independence attributes)做出了补充说明,明确了四种独立属性,但在 FDAL/IDAL 等级的分配过程中,仅需考虑功能独立性和机载软硬件研制独立性这两种独立属性。

4.2.2　实施建议

研制保证等级的分配与系统安全性评估紧密耦合,也是作为开展研制保证活动的基础。详细的研制保证等级分配可参考 ARP4761A 的内容,在型号研制中开展研制保证等级分配应注意以下几点:

1) 运营因素纳入研制保证等级的确定

在 ARP4754B 中主要考虑飞机安全性因素,因此通过飞机和系统安全性评估来确定 FDAL,并随着安全性评估向下分配到机载软硬件,但从产品研制的市场成功角度来看,除考虑安全性因素外,也应将飞机运营因素在研制保证等级确定时予以考虑,对于影响任务可靠性较高但不影响安全的功能也可以通过 FDAL 等级的分配,以确保对可能影响飞机运营可靠性水平的错误控制。

2) 研制保证等级分配应综合考虑多种因素

在开展研制保证等级分配时,存在多种 FDAL 组合同时满足顶层要求的情形,应充分考虑不同功能对应产品的成熟度、可制造性、供应商能力等,对不同因素进行权衡综合考虑,确定适合型号的 FDAL 等级。

4.3　需求捕获

4.3.1　修订要点

需求捕获主要变化是聚焦需求捕获本身,对需求的分类以及需求捕获活动进一步明确说明。具体修订要点如下:

1) 删除详细设计活动必然引入需求的绝对描述

由于描述过于绝对,A 版中"详细设计活动必然会带来新的需求或更改现有的需求"这段表述被删除,尽管其本意是说明飞机、系统、设备和机载软硬件设计活动多轮迭代,需求和设计方案逐步成熟的特点。

2) 需求分类参考更为清晰、明确

A 版需求分类章节结构容易造成对需求分类理解的歧义,修订将 A 版审定需求、衍生需求、重用之前经过适航审定产品中的系统、设备、机载软硬件章节内容直接纳入了需求分类章节。同时明确标准给出的是通用的参考需求分类,不是唯一划分方式,强调需求的分类不是互斥的,也就是同一条需求可以属于多种需求分类,因此在实际型号研制中可对同一条需求进行不同分类进行标识。

3) 通过安全性评估获取需求的过程定义为"捕获"而非"衍生"

在安全性分析捕获安全性需求章节中,由安全

性评估过程得到安全性需求的过程明确为“捕获”而非“衍生”,进一步确认安全性需求来自于安全性的 PASA 和 PSSA 过程。另外在 B 版中强调安全性评估过程中需要识别和管理相关假设,直到假设被关闭。

4)明确应对衍生需求进行更高层级的评价

新增识别与评价衍生需求章节,明确应对衍生需求对更高层级的功能和安全性影响进行逐层评价,直到衍生需求不再对上层功能和安全性产生影响的层级为止。并且将识别和评估衍生需求方法文件纳入研制保证规划过程,与安全性评估过程的目标一致。

4.3.2 实施建议

随着系统工程在飞机研制中的贯彻落实,各型号研制均开展不同程度的需求捕获工作[9],结合修订要点和目前型号工作,对需求捕获的实施给出以下几点建议:

1)重视对假设的识别与管理

目前各研制单位均已开展大量的需求捕获工作,按照需求分类形成需求数据库,实现了对需求的管理,通常假设会与某些需求相关联,甚至是需求成立的前提,因此应强化对假设的识别、关联和管理,直到假设被关闭。这些假设需要被证实是否正确,且假设的证实结果必须反馈给安全性过程。

2)进一步规范“衍生”的概念

在实际型号研制中工业方与局方对于“衍生需求”的概念理解经常无法达成完全一致,在 ARP4754B 中对衍生需求给出修订后的定义,即“在原有更高层级需求之外引入行为或特征的需求”,且衍生需求由于无法直接关联追溯到更高层级需求,在需求捕获过程中应给出充分理由(rationale),并将衍生需求对更高层级的功能和安全性影响进行评价,保证不对更高层级功能和安全性产生影响。

4.4 需求确认

4.4.1 修订要点

需求确认的主要变化是对相关内容定义的修改和补充,具体修订要点如下:

1)删除推荐方法及需求确认方法及资料表

B 版删除了 A 版中的 5.4.6.1 章节推荐方法以及表 6 需求确认方法及资料,统一根据附录 A 中不同 DAL 等级的确认过程目标,结合 B 版 5.4.5 节和 5.4.6 节选择适合的确认方法和资料。

2)删除对假设进行确认的表述

将需求和假设在每个需求定义层级都要进行确认,调整为需求要在每个需求定义层级进行确认,而假设则需要管理。全文中不再包含对假设的确认文字描述,也不再有对假设进行确认的流程。这种做法与研制过程中的实际情况相符,因为在需求完全验证之前,假设可能无法得到确认,只有当与之相关的所有需求都被验证无误后,假设的正确性才能得到证实。

3)使用“确认途径(approach)”替换“确认严苛度”

不再仅是强调确认过程的严格程度,更多是对确认方式的描述,强调应保证研制保证等级 A、B、C 的飞机和系统需求的正确性和完整性,还建议保证 A 级和 B 级确认过程的独立性,D 级目标可与适航当局进行协商,并被记录在确认计划中。

4)确认方法(method)予以更明确指导

新增每个需求都必须建立追溯性的要求,每个衍生需求都要有理由说明,并通过工程评审表明每个需求的正确性和完整性。但对 FDAL A 级和 B 级的需求,如涉及复杂状态机、安全性监控定义、性能和容差定义、动态行为、假设中包括需要在产品实现中证实的数值等,不能仅通过上述需求追溯性、衍生需求说明及结合工程评审的方式表明需求正确性和完整性,必须在确认计划中定义一些额外的确认方法,并且在确认计划中具体说明额外的确认方法在具体功能上施加的程度。

5)增加确认计划内容的新要求

包括要描述需求确认的原则(正确性和完整性)、需求确认状态的追溯过程以及对需求进行更改时的追溯过程、确认活动过程中出现问题的处置流程、确认总结中应包含的数据等。已不再要求在审定计划中描述需求追溯过程,仅在需求确认计划中描述需求的追溯过程。

4.4.2 实施建议

如何保证需求的正确性和完整性是需求工程中的难点,根据对修订要点的分析,对需求确认的实施提出以下几点建议:

1)进一步重视对需求的确认工作

需求确认是保证需求正确性和完整性的重要手段[10],也是维护需求追溯性和对假设的管理的有效措施。只有通过切实有效的需求确认,才能保证

需求能够真正作为设计、验证的输入,否则容易造成实际设计活动、验证活动按照以往设计经验开展,而实际脱离解决方案所要应对的问题空间的情况。所以,应在需求捕获完成后,通过适当的需求确认方法开展有效的需求确认。

2）结合研制程序对需求确认方法的应用进行研究

目前确认与验证方法均可通过分析、仿真、试验、演示等方法开展,但两者的目的存在差异。在实际型号研制项目中,受项目周期和成本因素的考虑,需要对需求确认工作进行切实有效的规划,所采取的需求确认方法既能切实对需求质量进行把关,又能结合各阶段、各层级的研制活动,而不对项目研制进度产生影响,同时能够被局方认可。

3）关注需求确认的独立性要求

针对 A、B 级需求确认过程,除对需求确认方法额外考虑外,还应关注需求确认流程的独立性,需保证确认过程与捕获过程相互独立。

4.5　实施验证

4.5.1　修订要点

实施验证部分的修订更多的是对内容进行澄清,针对验证目标、验证过程、验证途径(approach)、验证方法、验证数据等局部表述进行调整。主要修订要点如下:

1）删除推荐验证方法及验证方法和资料

与需求确认一样,B 版删除了 A 版中的 5.5.5.6 章节推荐验证方法以及表 7 验证方法和资料,统一在附录 A 中给出不同研制保证等级的验证目标。

2）为验证过程严格程度提出具体要求

在验证过程的严格程度方面,B 版新增并强调了研制保证等级 A、等级 B、等级 C 相关的飞机和系统功能的需求应被证实已经得到满足,还建议保证所有 A 级需求和 B 级安全性需求的验证过程的独立性,D 级目标可与适航当局进行协商,并被记录在验证计划中。

3）补充两项新的规划阶段应开展的活动

在开展验证规划时,新增 2 项规划活动,包括确保验证方法和程序能够充分验证需求实施的手段以及对将要采用的验证环境的描述。

4.5.2　实施建议

实施验证工作是整个型号研制表明适航符合性和市场符合性的重要活动,重点在于验证活动的规划、实施及数据融合追溯等过程,主要有以下几个需要关注的工作:

1）注重研制全过程的验证规划工作

根据需求的符合性方法,面向型号研制全周期统筹考虑验证规划工作,包括设计验证、产品实现的验证工作,尤其关注验证方法的充分性和适当性,提出的验证规划应能够结合型号研制程序并具有可操作性,能够有效指导型号设计单位的验证与确认工程师以及相关验证承试单位制定试验任务书及试验大纲。

2）推荐研制单位编制验证需求

验证需求是指在设计需求基础上,根据不同的符合性验证方法,规定不同的验证活动。INCOSE 系统工程手册也指出为保证验证工作的质量,相关单位应明确验证需求,同时波音公司在其导弹等相关产品也明确采用验证需求,指导验证规划、验证实施等活动开展,关于验证需求的必要性分析可参考基于模型的民机验证需求捕获及应用技术相关研究[11]。

3）强化需求与验证数据的追溯性管理

构建有效的需求-验证方法-验证程序-验证结果的追溯路径,能够在型号研制过程中进行动态管理,尤其对在产品实现的验证过程中发生的问题报告,应明确具体的处置流程,开展安全性影响评估,相关内容应纳入构型管理过程。

4.6　构型管理(CM)

4.6.1　修订要点

构型管理具体修订要点如下:

1）构型项内容进一步扩展,包括执行计划过程中产生的生命周期数据和记录

合并了 A 版中的“建立构型管理计划”和“建立构型”,将工作内容表述为“识别和定义构型项”。将“计划”纳入构型项(configuration item)范围,并且计划的范围不仅限于构型管理计划,还包括了产生构型数据的活动对应的所有计划,如需求管理计划、需求确认和验证计划、产品实现计划等,以及执行这些计划过程中产生的产品生命周期数据和记录。

2）通过构型基线建立需求确认和产品验证关联

将 A 版关于“建立构型项的构型基线是为了用于需求的符合性说明”的表述修订为“建立构型项的构型基线是为了开展需求确认或对产品实施验

证”,将构型基线与研制保证中的需求确认过程和产品实施验证过程建立了关联关系,消除了阐述模糊的部分。在表述中不再采用“衍生基线(derivative baseline)可追溯到之前基线”的概念,而采用“新的基线(new baseline)可追溯到之前基线”的概念。

3) 新增构型管理数据章节涵盖构型索引和系统控制类别

构型索引的信息内容进行了较大调整,新增了计划、计划执行所产生的生命周期数据和记录。删除了“每个系统项的构型标识”(无需专门提出,纳入构型管理的生命周期数据和记录都会有构型标识)、“机载软硬件相互交联信息”(接口信息已经足以反映系统的交联关系)。将表述统一为“系统控制类别”(system control categories),不再采用“数据控制类别”(data control categories)。

4) 新增问题报告要求

B 版删除了构型管理计划在必要时需与适航审定局方达成一致的表述,但新增了对问题报告的要求,提出在适航批准之时需要对尚未关闭的问题报告(open problem report)进行审查,确定未关闭的问题是否具有安全性影响或运行限制。

4.6.2 实施建议

根据构型管理的修订要点,给出以下几点实施建议:

1) 应考虑产品生命周期数据和研制保证过程数据

新版标准将飞机、系统、设备、机载软硬件等产品层级的各类研制保证过程计划都纳入了构型项范围,明确了相关研制保证计划和执行计划中产生的产品构型数据都应纳入产品研制的构型管理业务范围,构型管理的对象范围包括了产品全生命周期构型数据和产生构型数据的业务数据。这就要求构型管理专业必须能够有效结合项目管理和系统工程专业,理解研制保证过程,融合信息化和数据管理专业过程,从产品研制体系层面和信息化技术层面实现产品数据和业务数据的融合才能满足相关要求。建议国内民机研制单位应将构型管理纳入企业级技术管理业务域,而不是将构型管理或技术状态管理作为一个工程设计专业进行对待,融合企业信息化架构,建立构型管理企业级政策和原则,从产品全生命周期和业务视角规划业务职责和管理范围。

2) 保证构型基线与需求确认和产品验证追溯

建立和维护构型项的构型基线是开展需求确认或对产品实施验证的基础。最终的产品基线由多个构型项的基线构成,需求确认和验证的基准来自于对每个构型项的正确维护,并建立完整的构型基线。通过需求确认过程或对产品实施的验证过程发现问题并开展相应的更改贯彻,对构型项的基线进行更改控制,确保产品基线始终得到有效管理和控制。在产品研制初期识别构型项后,就建立构型项的基线,并开始对构型项的基线进行管控,且与相关的需求确认和产品验证等研制保证过程活动建立追溯和关联是确保产品基线得到有效管理和控制的基础。

4.7 过程保证

4.7.1 修订要点

过程保证主要变化包括研制保证计划调整、过程保证评审调整等内容,具体修订要点如下:

1) 明确了过程保证计划的范围

B 版明确过程保证计划增加了“识别和管理对计划的偏离”、“记录过程保证活动和符合过程保证计划”、“过程保证活动独立于产品研制活动”等内容。同时将原版中要求其它项目计划的范围和内容必须与飞机功能、系统或机载软硬件的研制保证等级一致的要求改为对研制保证计划的范围和内容必须与飞机功能、系统或机载软硬件的研制保证等级一致的要求。旨在消除关于其它项目计划范围与内容的争议,确保过程保证计划的明确性和一致性。

2) 新增针对研制保证活动、数据和报告的评审

5.7.3.1 节调整为研制保证计划审查,增加了关于研制保证活动、数据和报告审查的要求,包括已批准的计划活动被执行、数据正确完整符合批准的计划、计划偏离被管理、数据与报告更新被适当追踪和控制等。

4.7.2 实施建议

根据过程保证的修订要点,给出以下实施建议:

1) 确保过程保证与研制活动的独立性

过程保证活动的主要目标是确保所有研制保证活动按照已批准的计划开展,应在型号研制过程中确保过程保证与产品研制的独立性,通常过程保

证活动由质量保证工程师负责,由其对产品研制活动进行检查。

2）适当处理过程保证活动与产品研制活动的关系

在型号研制活动中应建立适当的过程保证监督机制,构建产品研制组织或团队按计划执行和实施的意识,确保过程保证机制不会对产品研制活动造成干扰,将过程保证活动作为支持产品研制、确保产品质量和安全的有效保证手段,而非对产品研制相关人员造成额外负担,甚至影响产品研制项目进度的要求。

4.8　审定联络

4.8.1　修订要点

审定联络的主要变化为适航审定和局方协调的内容,主要修订要点是删除了适航审定相关的描述内容,仅关注与研制保证过程相关的内容。

ARP4754B 并不能代表完整的适航审定过程,具体的产品适航审定过程和审定规划过程可以参考有关适航局方颁布的相关审定指导文件,如 FAA 的 Order 8110.4C 等。ARP4754B 仅关注与研制保证过程相关的内容,用于支持型号的适航审定过程。采用了“审定局方联络(certification authorities coordination)”,消除了被部分工业界或局方人员误解为适航审定过程(certification process)或者是将与局方的审定联络过程理解为适航审定过程(certification process)的情况。将“适航审定和局方协调”章节内容分配至第 3 章和新增的 4.7 节中,内容调整仅限于与适航局方的联络过程,并将适航审定联络过程纳入研制保证计划,适航审定过程的内容应该纳入适航审定计划中(CP 计划)。

4.8.2　实施建议

根据审定联络的修订要点,应注意区分合格审定过程与研制保证过程中的审定联络过程[12]。

审定联络过程应当注意避免出现与研制保证活动不相关的内容,特别是适航审定相关的描述内容,如适航审定规划、符合性方法、符合性说明和适航审定符合性数据等。新版标准明确审定联络并不能代表完整的适航审定过程,具体的产品适航审定过程和审定规划过程可以参考适航局方颁布的相关审定指导文件。

5　对飞机或系统的更改贯彻对比分析

与 ARP4754A 相比较,ARP4754B 中对于“飞机或系统的更改贯彻”(modification)章节做出了比较大的修订和改进,重点是澄清了更改贯彻与第 5 章内容之间的关系。针对 A 版对于改型的分类存在模糊的情况,B 版进行了较为详细地描述,将改型分为新的应用、修改、影响、未修改/无影响等几类,并针对不同的改型影响分类给出相应的研制保证活动要求。主要变化包括了以下几个方面:

1）将重用(reuse)与更改贯彻(modification)并列,首次采用了“更改贯彻/重用(modification/reuse)”,强调更改贯彻(modification)的范围包括飞机、系统、设备或机载软硬件,而重用(reuse)的范围仅包括系统、设备或机载软硬件。

2）明确指出在新飞机、新系统、新设备、新机载软硬件研制中,重用之前飞机型号或系统中的设计构型是常见的做法。飞机或系统方案中可能会有部分或者全部采用以前飞机型号或系统的设计构型方案,所以在重用以前飞机型号或系统的设计构型之前应进行评估。

3）将更改贯彻过程与相关研制保证过程的关系进行了清晰说明与定义,改善了 ARP4754A 第 6 章中更改贯彻过程与其它的研制保证过程之间相对模糊的情况。

4）明确更改贯彻/重用过程应在研制保证计划和安全性计划中进行考虑,对于飞机、系统、设备、机载软硬件的更改贯彻/重用的考虑不仅是对产品方案和贯彻的考虑,也要对相应的研制保证过程进行考虑。另外强调所有更改贯彻/重用都应评估对飞机级和系统级安全性和运行的影响,并纳入更改贯彻影响分析。

5.1　修订要点

对飞机或系统的贯彻更改,主要修订要点如下:

1）对更改贯彻过程内容进行局部调整

a）强调了更改贯彻管理流程的内容包括拟定更改贯彻所对应的适航审定策略和方式,进行适航审定规划,评估对审定基础的潜在影响,按照 Part21 部确定更改贯彻的等级(大改或小改,major/minor),并由局方最终批准更改贯彻和参照 Part21 部确定的等级。

b）将更改贯彻影响分析调整至执行更改贯彻之前,强调了更改影响分析应该在执行之前完成,符合更改贯彻过程逻辑次序。

c）强调不仅应对被更改的系统、设备或机载

软硬件开展更改贯彻影响分析,还应对重用的系统、设备、机载软硬件开展该项工作。

2) 扩大更改贯彻影响评估范围

A 版仅强调初始更改影响评估要包括更改贯彻方案对原有安全性评估结果的评估,B 版则明确指出更改影响评估还应包括对原有研制保证活动的评估。

3) 新增顶层改型影响分析过程

B 版给出了改型影响分析的顶层过程,并对每个步骤进行详细阐述。

5.2 实施建议

根据改型影响分析的修订要点,给出以下实施建议:

1) 重用应在产品概念方案阶段开始考虑

由于市场竞争激烈,客户需要迅速变化,研制进度要求高,现代民机研制过程大多会重用已有产品方案。所以应在产品的概念方案阶段对重用方案进行考虑和评估,确认重用方案在新产品应用中的影响,包括对产品功能和产品实现方面的影响,制定可行的计划,明确相应的研制保证过程要求,有助于飞机制造商与供应商、与局方之间建立合理和明确工作分工,达成可行的时间进度安排。对于飞机产品研制项目,无论新研或改型研制,建议在产品初步设计评审(preliminary design review,简称 PDR)之前按照 ARP4754B 第 6 章的要求完成对重用方案的评估和选择。

2) 更改贯彻中应包括系统性的研制保证过程

为满足 ARP4754B 中对于更改贯彻的过程要求,建议国内型号研制中应首先建立问题管理流程和制度,构建问题管理流程和更改贯彻流程间的输入和反馈评估机制,将更改贯彻过程的责任主体由工程团队转换为型号研制项目中的项目管理或系统工程专业人员,建立体系化和结构化的更改贯彻流程,在产品实施工程更改的过程中,协调实施研制保证活动,确保更改贯彻的正确性和完整性。

6 结论

ARP4754 作为民机研制保证的核心关键标准,其修订情况受到国内外工业方和局方的广泛关注,通过对 ARP4754B 与 ARP4754A 内容进行详细的对比分析,主要结论如下:

1) 对 ARP4754B 最新情况进行跟踪

从 ARP4754 的发展历程对 ARP4754B 的修订背景进行了介绍,并从总体上对 B 版标准修订情况进行分析,按照引用更新、概念澄清、结构调整、要求调整四类对重点修订进行总结,明确最新修订的背景和重点变化。

2) 明确了 ARP4754B 主要修订要点

针对研制保证规划、飞机与系统研制过程、必要过程、更改贯彻等章节内容,对 ARP4754B 与 ARP4754A 的差异性进行了详细分析,给出了最新的研制保证要求的解读,并对修订要点进行提炼供行业参考,全面深入掌握标准修订要求。

3) 结合型号实际给出研制保证实施建议

根据 ARP4754B 的修订情况,结合国内型号研制实际及适航审查情况,针对研制保证规划、飞机与系统研制过程、必要过程、更改贯彻等方面,给出开展研制保证的实施重点,为民机研制的研制保证工作开展及审定提供有效参考。

参考文献:

[1] Society of Automotive Engineers. Guidelines for development of civil aircraft and systems: SAE ARP4754A[S]. Washington, D. C.: Society of Automotive Engineers, 2010.

[2] Society of Automotive Engineers. Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment: ARP4761[S]. Washington, D. C.: Society of Automotive Engineers, 1996.

[3] RTCA. Design assurance guidance for airborne electronic hardware: DO-254[S]. Washington, D. C.: RTCA, 2000.

[4] RTCA. Software considerations in airborne systems and equipment certification: DO-178C[S]. Washington, D. C.: RTCA, 2011.

[5] LI X, ZHU Y, FAN Y, et al. Comparison of SAE ARP 4754A and ARP4754[J]. Procedia Engineering, 2011, 17: 400-406.

[6] Society of Automotive Engineers. Guidelines for development of civil aircraft and systems: ARP4754B[S]. Washington, D. C.: Society of Automotive Engineers, 2023.

[7] Society of Automotive Engineers. Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment: ARP4761A[S]. Washington, D. C.: Society of Automotive Engineers, 2023.

[8] 贺东风,赵越让,钱仲焱,等. 中国商用飞机有限责任公司系统工程手册[M]. 上海:上海交通大学出版社, 2017: 1-16.

[9] 谢陵,方俊伟,徐州,等. 基于功能场景分析的飞机需

求捕获和确认方法研究[J]. 科技资讯,2015,13(18):83-84.
[10] 徐万萌,陈芳,齐林. 基于 ARP4754A 的飞行管理系统需求确认以及系统验证研究[C]//中国航空学会. 第八届民用飞机航电国际论坛论文集. 北京:航空工业出版社,2019:640-646.
[11] 郭泰,钱馨,宫綦,等. 基于模型的民机验证需求捕获及应用技术[J]. 北京航空航天大学学报,2022,48(10):1933-1942.

作者简介

钱　馨　男,硕士,高级工程师。主要研究方向:系统工程、系统安全性评估、研制保证、飞机产品研制体系。E-mail:ryanbrady@sina.com

郭　泰　男,硕士,工程师。主要研究方向:系统工程、研制保证。E-mail:guotai101@126.com

任文明　男,硕士,研究员。主要研究方向:系统工程、标准化。E-mail:15801562091@139.com

李翊唐　男,硕士,工程师。主要研究方向:系统工程、场景建模。E-mail:tomli22121@126.com

江雨航　男,硕士,工程师。主要研究方向:系统工程、场景建模。E-mail:forimbalance@163.com

张　昭　女,硕士,高级工程师。主要研究方向:MBSE、需求工程。E-mail:zhangzhao423@126.com

Comparative analysis and implementation recommendations for ARP4754B and ARP4754A

QIAN Xin[1]　GUO Tai[2*]　REN Wenming[2]　LI Yitang[2]　JIANG Yuhang[2]　ZHANG Zhao[3]

(1. AVIC XAC Commercial Aircraft Co., Ltd., Xi'an 710089, China
2. AVIC China Aero Poly-technology Establishment, Beijing 100028, China
3. COMAC Beijing Aircraft Technology Research Institute, Beijing 102211, China)

Abstract: ARP4754 is the most important development assurance standard for the development of civil aircraft and systems, and the revision of the requirements of development assurance has received extensive attention from civil aircraft development units and airworthiness authorities of various countries. In view of the latest ARP4754B issued by SAE, a detailed comparison and analysis of ARP4754B with ARP4754A is carried out. The background and content of the revision of ARP4754B are comprehensively studied. This paper gives key points of revision in combination with the discussion of the revision of ARP4754B, and gives follow-up development assurance implementation suggestions for development assurance planning, aircraft and systems development process, integral process, and change implementation in combination with the aircraft development experience and airworthiness review, so as to provide an effective reference for the development unit to better understand the requirements of ARP4754B development assurance, and to truly implement the ARP4754B in product development.

Keywords: development assurance; systems engineering; civil aircraft development; development error

* Corresponding author. E-mail: guotai101@126.com