2017年第3期 总126期
ISSN 1674-9804 CN 31-1614/V

DOI：10.19416/j.cnki.1674－9804.2017.03.005

# 基于构型项目分类的民机系统适航符合性证据体系结构研究

# Research on Configuration Item Classification Based on Civil Aircraft System Airworthiness Compliance Evidence System Structure

卢 艺[1,2] 郝 莲[1] 李承立[1] 张曙光[2]/ LU Yi HAO Lian LI Chengli ZHANG Shuguang

（1. 上海飞机设计研究院，上海 201210；
2. 北京航空航天大学，北京 100191）

（1. Shanghai Aircraft Design and Research Institute, Shanghai 201210, China;
2. Beijing University of Aeronantics and Astronautics, Beijing 100191, China）

**摘 要：**
民机型号合格审定程序要求型号申请人通过系统性规划和实施型号研制过程，向局方提出正确、完整和可追溯的适航符合性证据，用“设计保证”确保产品符合适航规章要求。基于系统工程中“双V模型”（Validation & Verification，简称“双V模型”）理论，以“研制规划保证回路”和“研制过程回路”为两条核心路径，辨识了证据体系与构型管理、民机系统研制过程及型号合格审定过程之间的接口关系，以飞机、系统和设备层级下的构型项目类型为框架，提出了以“规划保证”、“需求定义”、“逻辑/物理方案实现”、“确认数据”和“验证数据”五个维度构成的符合性证据体系，明确了证据链数据间的传递关系。

**关键词：**型号合格审定；适航要求；符合性证据体系；构型项目

**中图分类号：**V221+.91 **文献标识码：**A

[**Abstract**] Civil aircraft type certification procedure requires the type applicant to submit correct, complete and traceable airworthiness compliance evidences to the certification authority, following the systematic planning and implementation of type development processes. Such evidences show the development assurance on products against airworthiness regulation requirements. Based on the Vee model theory of the system engineering, this paper chooses the development planning and assurance loop and development process loop as two core routines to identify the interfaces of evidence system with the configuration management, system development and type certification processes. Using the configuration item type classification under the aircraft, system and equipment levels as a framework, a compliance evidence system consisted by five dimensions of plan assurance, requirement definition, logical/physical solution, validation data and verification data is proposed, which specifies the transferring relationship between the data links.

[**Keywords**] type certification; airworthiness requirements; compliance evidence system; configuration items

## 0 引言

大型客机适航取证是确保大型客机满足按公众要求制定的、可接受的最低安全标准(适航标准)的管理和技术实现过程[1]。现代民机是一个高度复杂的系统,由大量的适航规章条款、等效安全、专有条件等构成飞机型号的合格审定基础[2-3]。满足复杂的飞机级功能需要大量的交互的复杂系统来共同达成,而各子系统往往执行或贡献于多个飞机级功能;这使得民机产品在向适航审定局方表明规章符合性存在不利的后果:复杂系统行为和失效模式很难通过传统解耦分析和分离部件试验获知,难以保证最终产品的安全性,尤其是需求和设计错误无法通过"试错法"予以穷举,对于这类系统的规章符合性应综合使用"设计保证"来表明[4-5]。然而在实际工程中,面向局方针对民机产品研制 所提出的"过程控制"与 "构型管理"要求,申请人虽然拟定了如构型管理文件体系计划、设计保证手册等相应的规划文档,但由于型号设计文件(过程)与需求文档(计划)关系不清、需求描述滞后和完整性缺陷等问题的存在,尚未形成系统性、结构化的合格审定证据,可能为民机系统适航取证带来难以承受的额外时间和经济成本。

面对上述问题,本文基于系统工程理论,结合局方认可的面向合格审定建议方法的工业指南,建立适航合格审定符合性证据体系,提出构建适航符合性证据体系的结构化框架和元素类型,为通过系统性策划和管控民机研制过程研制数据,为确保适航符合性证据构建过程的合理性、完整性与准确性提供建议,推动民机型号研制适航取证工作的顺利开展。

## 1 民机系统工程"双 V 模型"概述

构建适航符合性证据体系的基础是应用于民机研发领域的系统工程理论和方法[6-8]。目前国内外相关组织总结了大量复杂系统研制经验,提出了基于系统工程的复杂系统设计保证方法指南,例如:(1)ISO/IEC-15288《系统和软件工程-系统生命周期过程》,其应用范围更广但方法细节度较低[9];(2) IEEE-1220 《系统工程过程的应用和管理标准》,其方法细节度较高但应用领域范围较小[10];(3)EIA-632《系统工程过程》的定位处于上述二者之间[11]。在民机和系统研制领域,最常用的是描述飞机系统研制过程的系统工程"双 V 模型"(双"V"是指 Validation & Verification),如图 1 所示。双 V 左臂建立了在飞机、系统和设备各层级中持续迭代的需求定义/分解,驱动系统设计的实施和同步持续的各层级实施过程向需求的确认活动。双 V 右臂开展了围绕各层级综合过程的验证活动。上述双 V 过程使"研制错误"能在项目初期就得到尽早发现,避免其向综合和验证阶段的累积。

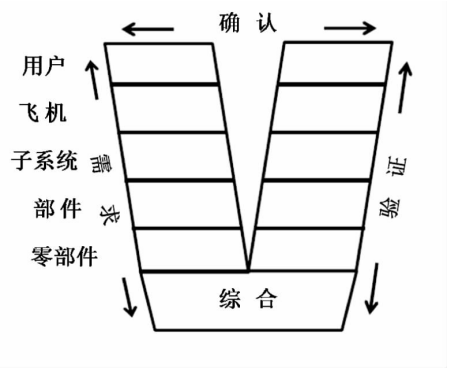


图 1 系统工程 Vee 模型图[12]

以波音公司自 1990 年起研制的波音 777 大型客机为例,该机相对于之前的型号具有更为复杂的功能需求和设计特征,如 ARINC629 电子总线、电传飞控及高集成度仪表等。波音基于以"双 V 模型"为路径的系统工程方法规划和确保了适航符合性证据的完整、正确和可追溯性,该机在 1995 年获得 TC 证和交付运营[13]:在型号研制技术成功的同时也实现了商业的成功。1996 年,国际自动机工程师协会(SAE)总结了以波音 777 为代表系统工程在民机领域的实践经验,提出了基于系统工程的复杂系统面向适航审定的工业指南 SAE ARP-4754[14-16],并在 2010 年更新为 ARP-4754A。目前国内外适航当局建议型号申请人采用 ARP-4754A 方法系统性规划民机研制,使需求和设计中的错误降低至最小,保证产品系统安全性符合适航要求;作为技术指南配套文件的 ARP-4761 对具体的系统安全性分析和评估提供了方法性指南,下属文件 DO-254 和 178B 对硬件和软件的开发保证进行了指导。上述指南的集合形成了一整套基于系统工程理论的复杂飞机系统开发保证流程建议,为民机适航符合性证据体系的构建提供了理论基础。

2017年第3期 总126期
ISSN 1674-9804 CN 31-1614/V

## 2 民机系统适航符合性证据体系框架

为明确型号合格审定的流程和关键环节，中国民用航空局（CAAC）制定了 AP-21-AA-2011-03-R4《航空器型号合格审定程序》，要求型号申请人依据已批准的审定计划，针对审定基础提供相关证据，形成“符合性验证资料（CD）”，表明对相应适航要求的符合性，该程序定义了生成符合性验证数据（或资料）的四个途径：（1）工程验证试验；（2）工程符合性检查；（3）分析；（4）申请人飞行试验。申请人所提供的符合性证据应依据从适航要求出发直到产生符合性声明结论的逻辑顺序，解释说明证据间内在联系，通过符合性论证使审查代表信服适航要求已得到满足。尤为重要的是，符合性验证资料的基础是民机型号设计资料，对此 CCAR-21-R3《民用航空产品和零部件合格审定规定》第 21.31 款明确了“型号设计资料”包括四类[17]：（1）定义构型和设计特征符合相关适航规章和环境保护要求所需的图纸、技术规范和清单；（2）确定结构强度所需的尺寸、材料和工艺；（3）持续适航文件中适航性限制部分；（4）通过对比确定同一型号后续适航性和使用环境保护要求。

型号申请人通过系统性规划和实施研制过程并向适航局方提出正确、完整和可追溯的适航符合性证据，保证最终产品符合适航规章要求。民机系统研制过程可以分为飞机、系统、设备（软、硬件）三个层级的工作，每一个层级活动分别都由计划、执行过程、设计数据、确认/验证数据等构成。结合系统工程的“双 V 模型”理论，上述“型号设计资料（Type Design，简称 TD）”属于双 V 左臂部分开展的民机产品各层级从“自顶向下”设计需求分解和设计实施与需求确认过程中产出的相关证据，而“符合性验证资料（Compliance Data，简称 CD）”位于双 V 右臂，描述了民机产品各层级“自底向上”的系统测试与集成、飞行试验的过程与文档化结果，是产品实施相对于设计实施与综合（集成）面向需求进行验证过程产出的相关证据[18]。为了辨识、记录和控制符合性证据相关数据，民机型号申请人依照局方规定策划和管控“构型管理”过程，辨识以系统需求、合格审定资料等为主体的构型项目内容和内在联系，建立和控制民机系统全寿命周期研制和试验过程的“构型基线”，控制构型项的产生、更改和更新过程[16]。对型号设计和符合性验证资料的系统性、结构化是构型管理的核心，既是系统研制也是一项合格审定工作。构型基线的管控对象主要为适航审定计划与总结、研制过程和需求、安全性评估过程、验证程序、构型索引等构型项目，其提炼了系统研制、试验数据，为适航符合性证据的构建提供了基础。

参照 EIA-632 标准对技术研发过程的分解描述，民机系统的研发过程可视为“自顶向下”在飞机、系统和设备分层级中的一系列“提问—解问”过程，进而获得各层级的物理解决方案，以需求和设计结果为主要内容的构型项目形成了“构型基线”的主要控制对象。适航符合性证据体系在构型基线数据的基础上，依据构型项目的层级分类，开展面向需求的确认和面向实施的验证活动，生成面向规划的过程保证数据，构建符合性证据链，表明面向适航规章要求的预期系统功能和安全性达成。

## 3 基于构型项目类型的适航符合性证据体系关系链

基于民机构型管理所控制的构型项目的分类，本文基于民机和系统产品“研制规划保证回路”和“研制过程回路”两部分从“规划保证”、“需求定义”、“逻辑/物理方案实现”、“确认数据”、“验证数据”五个构型项目类型维度来描述符合性证据体系结构中的证据关系链。

### 3.1 基于计划实施的研制规划保证回路

通过研制规划过程在项目之初就明确民机系统的研制、试验和取证的过程和方法，确保必要的计划得以执行的保持，是系统工程在民机领域应用的重要特征。通过考虑民机系统的预期功能和使用环境，对相关的研制阶段、评审节点进行规划，“研制规划（Development Process）”过程明确了应满足的系统审定基础，飞机/系统的安全性目标、初步系统研制保证等级（DAL）等，并明确支持研制工作的组织架构和关键人员职责。基于已制定的计划开展“过程保证（Process Assurance，PA）”过程确保研制工作和过程是严格按照计划进行，并提供计划一致性的相应证据。上述规划保证回路与“研制过程回路”之间的交互关系体现在对研制、确认和验证活动的计划和保证上（见图 2），所产生的的合格审定计划、研制计划、过程保证计划、确认计划、验证计划、过程保证数据等是构型项目的控制对象，形

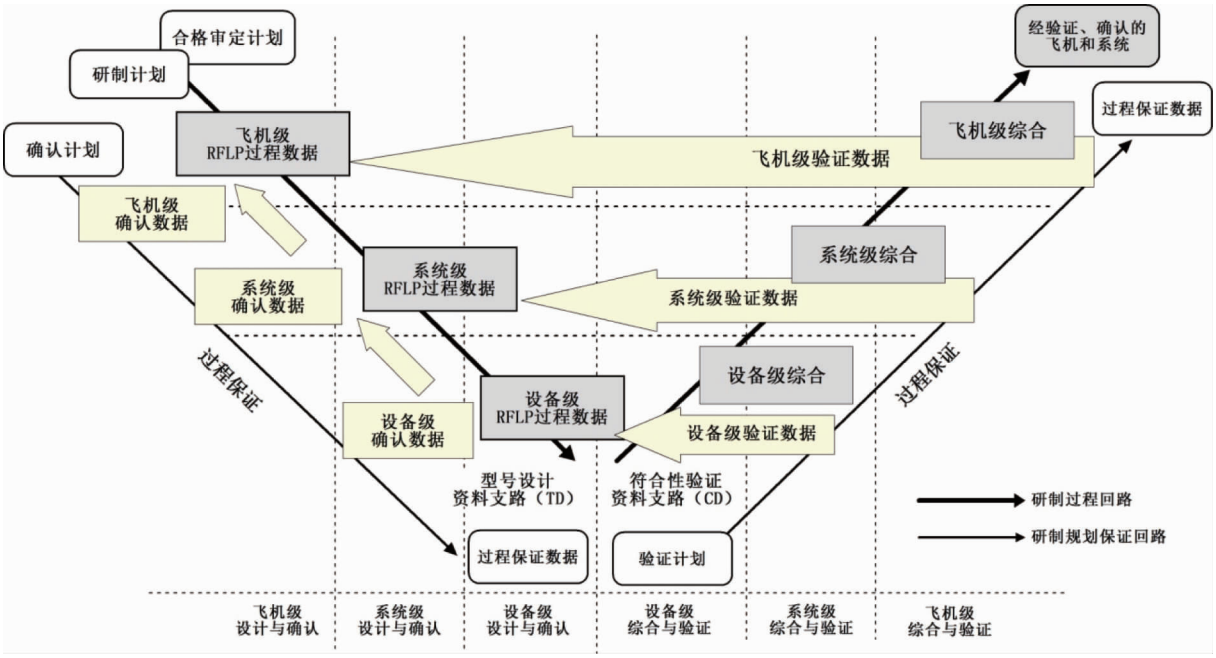


图 2　适航符合性证据体系结构图

成了符合性证据体系结构的“规划保证”维度。

### 3.2　基于“双 V 模型”的型号研制过程回路

#### 3.2.1 基于 RFLP 关系的型号设计资料(TD)支路

系统工程的双 V 模型左臂是民机系统产品研制“自顶向下”的设计过程,其通过“需求—功能—逻辑方案—物理方案(即 RFLP)”的顺序实现系统研制过程[11]。基于在该支路中的构型项目的类型,区分飞机、系统和设备三个层级,建立“需求定义”、“逻辑/物理方案实现”以及“确认数据”三个构型项目类型下的符合性证据体系。

型号设计资料支路起始于需要(Needs)辨识和需求(Requirement)定义(统称 Requirement,R 阶段)。需要(Needs)描述了期望的产品属性,是产品用户从使用和综合的角度定义的产品黑盒状态的技术约束,其中包括了自身需要、规范和标准、技术能力等约束。需求(Requirements)是对产品实现的可识别约束,但一般不包括具体的设计实现方式。产品的设计过程是一个求解黑盒为白盒的过程,通常使用产品的需求文档(RD)描述产品黑盒,主要从功能、性能、安全性、安装和维护、接口和使用、适航等方面建立需求。适航规章要求通过功能分析和需求捕获逐级分解、分配到上述几类需求中。高层级的需求在功能架构分析过程中分解、分配,从飞机级进入系统级最终到达设备层级的软/硬件。伴随设计开展的需求分析形成的各层级的需求和规范的集合是构型项目的控制对象,如:顶层飞机级需求 TLAR、飞机/系统/设备级功能需求文档 AFRD/SRD/ERD、飞机/系统/设备级设计规范 ATS/STS/PTS 等,形成了符合性证据的“需求定义”维度。

基于需求开展的设计活动起始于功能分析(Function,F 阶段),是产生解决方案逐步满足需求的过程(即黑盒解白)。功能架构的产生及即逻辑解决方案(Logical Solution,即 L 阶段)的形成,如飞机/系统级功能描述文档 AFDD/SFDD 和接口文档 AFICD/SFICD 等是构型项目中“设计描述”的控制对象。为满足各层级功能架构所预期达成的需求,驱动物理架构的产生,即物理解决方案(Physical Solution,P 阶段),如飞机/系统/设备级设计描述文档 ADD/SDD/EDD 及详细的接口描述文档等,这也是构型项目中“设计描述”的控制对象,形成了符合性证据的“逻辑/物理实现”维度。

尤为重要的是,伴随上述过程在各个层级中反馈驱动需求的更新和确认过程(Validation Process),确保各层级所需满足的需求和设计分析中产生的衍生需求足够正确和完整。确认的方法主要包括:试验、分析、建模、计算、相似性比较、评审、工程判断和追溯检查,逐步形成完整的技术需求集,成为相应的解决方案的输入和约束。基于构型项目类型,“确认数据”维度的符合性证据主要包括飞机/

2017年第3期 总126期
ISSN 1674-9804 CN 31-1614/V

系统级的特性数据、载荷报告、系统级 FTA/CCA/CMA 安全性分析报告、PASA/PSSA 安全性评估报告、各研制阶段评审报告等。

3.2.2 面向需求实施的符合性验证资料(CD)支路

在系统各层级确立相应需求后,预期的功能通过所计划的解决方案予以实施,为确保该实现的正确性及对应需求已满足,尤其是安全性分析的有效性,应在各层级内开展验证过程(Verification Process)。验证活动对应验证计划所确定的待验证的系统或设备的构型,明确具体的试验设施、判定准则和工作顺序,验证的严酷度对应于系统研发过程中的功能开发保证等级(FDAL)和项目保证等级(IDAL),主要验证方法包括:检查评审、分析、试验或演示及使用经验等,结构化记录的验证程序和验证结果用以表明追溯验证过程的状态。基于构型项目类型,本体系中"验证数据"维度的适航符合性证据主要包括飞机/系统级静力、试验室、地面、机上(如 OATP)和飞行试验大纲、分析报告、ASA/SSA/CCA 安全性评估报告、设备级鉴定/验收试验等。

与面向民机型号合格审定的民机系统工程双 V 图相关联,在飞机、系统和设备层级中"研制规划保证回路"和"研制过程回路"的上述适航符合性体系的各维度之间关系如图 2 所示,其中"需求定义"和"逻辑/物理方案实现"维度共同构成"RFLP 过程"。

## 4 结论

民机研制始于顶层飞机级需求搜集和定义,其依据是用户需要、技术约束及工程经验,通过"自顶向下"的功能分析形成逻辑解决方案从而捕获需求,进而分解形成系统级设计需求并向子系统和设备级分配,各层级确认相应需求的正确性和完整性,驱动物理解决方案的构建和实施,基于物理实物开展"自底向上"的设备、系统综合试验验证预期的功能的实现,确保所有相关适航要求得以满足。依照上述原理,本研究明确了民机和系统研制、试验活动关键数据与适航符合性证据的接口,基于民机和系统产品"研制规划保证过程回路"和"研制过程回路"入手,基于构型项目分类,提出了由"规划保证"、"需求定义"、"逻辑/物理方案实现"、"确认数据"、"验证数据"五个维度所构成的符合性证据体系框架,分飞机、系统和设备三个层级辨识了证据数据类型及其内在联系。

### 参考文献

[1] 郝莲. 民机研制适航取证总体技术方案探讨[J]. 航空制造技术, 2012, 22: 62 – 65

[2] 陆中, 孙友朝, 周伽. 民用飞机适航符合性验证方法与程序研究[J]. 航空标准化与质量, 2007, 4: 6 – 8,19.

[3] CAAC. CCAR-25-R4 中国民用航空规章第 25 部:运输类飞机适航标准[S]. 北京: 中国民用航空局适航审定司, 2011.

[4] 郝莲, 哈红艳. 中国民用飞机主制造商设计保证系统的建立[J]. 中国民用航空, 2013, 9:32 – 34.

[5] CAAC. AP-21-AA-2011-03-R4 航空器型号合格审定程序[S]. 北京: 中国民用航空器适航审定司, 2011.

[6] Dickerson CE, Mavris DN. Architecture and Principles of Systems Engineering [M]. CRC Press, 2010.

[7] Checkland P. 系统论的思想与实践[M]. 左晓斯, 史然译. 北京:华夏出版社, 1990.

[8] 上海交通大学钱学森研究中心. 智慧的钥匙—钱学森论系统科学[M]. 上海:上海交通大学出版社, 2005.

[9] ISO/IEC 15288. Systems and Software Engineering-System Life Cycle Processes[S]. UK: Cranfield University, 2008.

[10] IEEE. IEEE Std1220 Standard for the Application and Management of the Systems Engineering Process[S]. USA: Institute of Electrical and Electronics Engineers, 1998.

[11] AMSI/GEIA. EIA-632. Process for Engineering a System [S]. USA: Electronic Industries Alliance, 2003.

[12] Jackson S. Systems Engineering for Commercial Aircraft-A Domain-Specific Adaptation. [M]. Burlington, VT, USA: Ashgate Publishing Company, 2015: 56 – 57.

[13] Petersen TJ, Sutcliffe PL. Systems Engineering as Applied to the Boeing 777[C]. AIAA 92 – 1010, 1992.

[14] SAE. ARP 4754 Certification Considerations for Highly-integrated or Complex Aircraft Systems [S]. USA: Warrendale, 1996.

[15] SAE. ARP 4761 Guideline and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment[S]. USA: Warrendale, 1996.

[16] SAE. ARP 4754A Guidelines for Development of Civil Aircraft and Systems[S]. USA: SAE International, 2010.

[17] CAAC. CCAR-21-R3 民用航空产品和零部件合格审定规定[S]. 北京:中国民用航空局适航审定司, 2011.

[18] 李承立. 需求驱动的民机系统研制过程及构型数据结构[C]// 第六届中国航空学会青年科技论坛文集. 北京: 航空工业出版社, 2014: 743 – 752.