基于ARP4754的民用飞机复杂系统研制过程保证方法研究

Research on Civil Aircraft Complex System Development Process Assurance Method Based on ARP4754

房海涛[1] 刘丹[2]/1 中国商飞上海飞机设计研究院 2 中国科学院上海高等研究院

摘 要：在民用飞机设计和研制中，对于高度综合或复杂的系统，如何通过研制过程确保安全性得到保证，并且验证被实施系统的安全性，是适航审定中一个重要的基础和考查环节。本文基于ARP4754所提供的指导材料，以民用飞机系统设计和研制为对象，从系统需求管理、需求确认和验证（V&V）、研制保证等级分配等方面，阐述了系统研制过程中研制保证的证明，表明系统对适用的适航要求的符合性。

Abstract: During the design and development of civil aircraft, for highly integrated or complicated system, how the safety can be assured by the development process, and verify the safety of implemented system, which are critical basis and audit step in airworthiness certification. Based on ARP4754 guidance, in aspects of system requirement management, requirement validation and verification, and development assurance level allocation, this paper illustrates the proof of development assurance in the process of system development, indicates system compliance for airworthiness requirement.

关键词：民用飞机；复杂系统；ARP4754；过程保证

Keywords: civil aircraft；complex system；ARP4754；process assurance

0 引言

随着现代飞机及系统综合复杂程度的增加，为表明对CCAR/FAR/CS 25.1309条款的符合性，仅用试验或分析确定所有的系统状态几乎是不可能的；或者即使可能，也因所需完成的试验数量太大而不切合实际。如何控制高度综合或复杂飞机系统研制过程中的风险，已经成为民用飞机系统开展安全性评估的新课题，也成为系统适航符合性验证的重点和难点。

我国对于“过程保证”的理解大多局限于对指导材料的理解，缺少深入的理论研究，没有足够的实践经验，在适航符合性设计和验证方面存在较大困难。

本文通过分析ARP4754和相关材料的背景、内容和目标[1]，分析研究民用飞机系统适航验证过程中贯彻实施过程保证的要求和方法。

1 研制过程保证的要求和方法

1.1 研制保证概念

研制保证是一个基于过程的方法，用于确保系统以足够严格的方法开发完成，从而限制了影响飞机安全性的研制差错出现的可能性，表明对CCAR/FAR/CS 25.1309条款的符合性。研制过程保证工作适用于新型号的设计和对现有设计的更改。

按照过程保证的概念，在系统研制过程中需要将飞机级需求分解并分配到系统，系统按照飞机级的需求和安全性目标确定构架，并根据系统架构分配需求到底层设备及软件、硬件；根据系统安全性评估过程的输出确定不同功能的设计保证等级，系统研制要根据研制保证等级（DAL）进行过程保证，系统综合过程中要表明系统的实现满足了适航规章的安全性要求和目标。系统研制过程中需要对系统需求获取、需求确认、需求验证及安全性评估、构型控制等进行过程控制[2]。

1.2 系统需求研制和追踪管理

需求及其相关的危害性分析是系统研制过程的基础。由于各种需求危

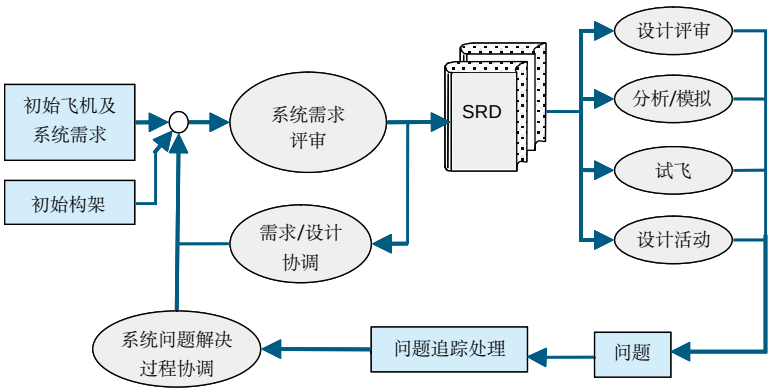

图1 系统需求制定过程模型

害的重要程度不同，所以贯穿系统架构研发过程中的需求分配，对系统合格审定证明方面有重大的影响。图1所示为系统需求制定过程模型。

飞机研制周期中，顶层过程包括确定飞机功能及与这些功能相关需求的定义。飞机功能（包括功能接口及相应的安全性需求）是制定系统架构的基础。架构的选择又会形成架构实现所必需的附加需求。在需求确定与分配过程的每一阶段（即系统和设备）都要确定已有需求和新增衍生需求的详细内容。实现过程中所做的选择和遇到的问题是衍生需求的主要来源，并可能需要增加新的系统安全性需求。详细的设计活动总会引入新的需求或更改已有的需求。

1.3 系统需求确认和验证

研制保证过程是一种被公认的确保飞机级和系统级研制过程满足安全性需求的可接受方法，而需求确认和验证是表明系统研制过程遵循过程保证原则的基本要求。

系统需求的确认和验证的目标完全不同，需求确认是要保证系统的需求正确与完整，而需求的验证是要保证系统的实现满足了系统的需求。需求确认和验证的严格程度取决于系统实现功能的DAL，不同DAL的等级要求的验证和确认策略完全不同，需求确认和验证是表明系统研制过程遵循过程保证原则的基本要求。在系统研制过程中需求确认过程和验证过程本身是交联的，合理的验证和确认策略是保证符合适航要求的关键。

1.4 DAL分配策略

研制保证等级（DAL）是对应于功能或项目的失效所导致的危险状态规定的一系列等级，用于描述在功能和项目的研制过程中为了避免出错而采取的措施的方法，在安全性评估过程中确定的。

其目的是在系统和项目的研制中从安全性的角度选择质量程序，为相应的等级制定对应的工作程序及验证标准，以将需求或设计中的错误或遗漏减至最小。

研制保证等级的分配根据失效状态的严重性类别和各研制过程中能够限制研制错误影响可能的独立性而确定。失效状态类别严重性越高，用以减缓失效状态所需的研制保证等级也就越高。

表1 顶层功能DAL分配

顶层失效状态严重性类别	相应顶层功能DAL分配
灾难性的	A
危险的	B
重大的	C
轻微的	D
无安全影响的	E

根据失效状态最严重的类别对功能分配DAL，表1为飞机级或系统级功能危险性评估（FHA）中的每个功能分配DAL[3]。

2 过程保证方法在民机上的应用

基于ARP4754以及上述提到的研制保证过程要求和方法，以民用飞机系统研制的文件体系为研究对象，从系统需求管理、需求确认和验证、研制保证等级分配三个方面分析系统适航验证过程中贯彻实施过程保证的要求和方法。

2.1 民用飞机系统需求追踪管理

系统设计要求的输入文件包括整机级要求、合格审定机构要求、初步功能危险性评估、软件要求、E3要求、液压管路设计要求、电缆设计要求等文件。系统规范包括系统需求（SRD）、接口控制（ICD）等文件。系统的要求将分解成对硬件和软件的要求。供应商将根据系统的分解要求规范产品设备的要求。在进行后续设计阶段前，要同供应商进行正式设计确认，以确保这些要求能够被清晰地理解和一致同意。为了一些验证要求，需要提供系统的体系结构和实

表2 需求追踪表

序号	需求标识符	SRD章节号	需求内容	需求类型	需求来源	备注

表3 需求确认表

序号	需求标识符	SRD章节	需求内容	需求类型	确认方法	确认证据材料	确认结论	开口问题	备注

表4 需求验证表

序号	需求标识符	SRD章节	需求内容	需求类型	验证方法	验证证据材料	验证结论	开口问题	备注

现的详细资料以表明符合性。

针对民用飞机系统的需求分配和管理过程，建立系统需求与顶层要求及系统设计之间的联系，采用的需求追踪表如表2所示。

2.2 民用飞机系统需求确认与验证

按照ARP4754确立的需求确认和验证过程模型开展工作。针对民用飞机系统的顶层需求，分析系统实现过程中需求确认和验证的策略和方法，研究各种分析计算报告和试验报告与需求确认和验证工作之间的关联，梳理需求确认和验证的文件体系，建立系统需求确认和验证矩阵。采用如表3和表4所示的需求确认和验证表。

通过分析系统研制过程中产生的文件体系，根据系统需求确认和验证的基本原则和模型，建立系统的需求确认和验证矩阵。

民用飞机系统需求确认和验证的证据主要包括以下5类文件。

1）追溯的来源文件：需求的来源可以作为确认证据。

2）规定文件：如材料方面的“选用目录”等，作为确认。

3）系统符合性说明文件，作为验证。

4）分析报告：包括强度、载荷、安全性和维修性等方面。

5）试验：如设备鉴定试验（QT）、铁鸟和机上地面试验、飞行试验等。

其中4）和5）既可作为确认又可作为验证。

3 总结

本文介绍了过程保证概念中的需求捕获、需求确认、需求验证及研制保证等级分配等内容，分析了民用飞机系统设计规范中的需求，梳理系统研制过程中的各种文件，建立系统设计需求与飞机顶层及相关系统之间的联系，对系统设计规范中的需求进行追踪与管理；分析系统需求确认和验证的基本原则和策略方法，研究各种分析计算报告和试验报告与需求确认和验证工作之间的关联，总结和分析了系统顶层需求的设计实现和验证状态，建立系统需求确认和验证矩阵，为系统设计人员提供技术指导，为系统适航符合性验证工作提供支持和保证。AST

参考文献

[1] SAE ARP4754: Certification Considerations for Highly–Integrated or Complex Aircraft Systems [S]. Society of Automotive Engineers, Inc, December, 1994.

[2] 樊瑞. 民用飞机软件验证技术研究[D]. 南京：南京航空航天大学，2010.

[3] 尤琦，任和，郑占君. 基于系统构架的民用飞机研制保证等级分配[J]. 质量与可靠性，2012(1).

作者简介

房海涛，工程师，主要从事民用飞机飞控系统的设计与研发工作，研究领域为系统安全性评估、需求管理体系和双V验证流程。

刘丹，工程师，主要从事智能城网的方案规划，参与物联网系统的标准制定，研究领域为系统过程控制。