经验介绍

TIA 前机载软件成熟度评估的相关研究

居　慧　陈一可
（上海飞机设计研究院综合航电系统设计研究部，上海　200436）

Related Research on the Assessment of Airborne Software Maturity Prior to TIA

Ju Hui　Chen Yike
（Avionic System Department of SADRI，Shanghai 200436，China）

摘要：率先引入了 FAA（美国联邦航空局）提出的软件成熟度的概念。局方正式签发 TIA（型号检查核准书）前，在软件的构型和符合性均未达到最终冻结状态的情况下，通过对软件的成熟度进行有效评估，可以为验证试飞前软件的工程批准提供有力的支持与保障，在一定程度上降低局方飞行试验的风险，保障适航验证试飞活动的顺利开展。由于机载软件成熟度是一个新兴的概念，目前局方（FAA、CAAC）对于如何进行成熟度评估尚未形成正式的、通用的政策性指导文件，国内主机厂对此问题也没有相关的处理经验和具体的操作方法。基于机载软件本身的特点，参考局方在机载软件审查时的主要关注点，提出了 TIA 前机载软件成熟度评估的基本考虑要素与分析重点。

关键词：TIA；机载软件；成熟度；评估

【Abstract】 This paper first introduces the software maturity concept proposed by FAA. In the condition that the software configuration and compliance status are not frozen before TIA, assessing the software maturity efficiently can provide powerful support and assurance to the engineering approval of the software, as well as reduce the risk of the certification credit flight test to a certain extent and ensure successful flight test activities. Presently, as the software maturity is a new concept, the certification authority (FAA, CAAC) hasn't released the formal and general policies or guidance, and domestic airframer doesn't have any related experience or methods either. This paper proposes some basic consideration factors and analysis points based on the characteristics of the airborne software and on referencing the key points that the certification authority pays special attention to in the software certification.

【Key words】 TIA; airborne software; maturity; assessment

0　引言

随着航空科学技术的不断发展，机载软件正逐步成为实现完整的机载系统功能不可或缺的一部分，软件实现的功能也愈加复杂和强大，因此软件功能的正确执行对于飞机飞行的安全性有着重要影响。按照适航要求，在进入局方的验证试飞试验前，即局方正式签发 TIA（型号检查核准书）前，相关试验件及其所含的软件构型状态必须冻结或接近最终冻结状态，即软件已完成最终阶段评审，否则含软件的机载系统无法满足局方验证试飞前有关的规章要求。

对于一般民机型号审定项目而言，上述要求实际无法达到，但是局方对于含软件的机载系统/设备必须获得较高的合格审定置信度，才能允许其进行相应的试飞科目，由此局方提出了一个新的概念：软件成熟度评估。为了确保局方验证试飞的安全性和有效性，顺利完成预定的试飞科目，TIA 前必须对软件的成熟度进行有效评估，这不仅仅是局方所关注的重点，也是主机厂必须要完成的工作。

目前，FAA（美国联邦航空局）和 CAAC（中国民用航空局）对于机载软件的成熟度评估还没有发布正式的政策性指导文件，国内主机厂对此也没有相关的处理经验和具体的操作方法。基于机载软件本身的特性，参考 CAAC 对于机载软件审查的主要关注点，并结合国内主机厂的实际情况以及国外合格审定咨询专家的建议，本文提出了 TIA 前机载软件成熟度评估的考虑要素和分析重点，供主机厂借鉴和参考。

1　机载软件成熟度评估的前提

在对含软件的机载系统/设备进行软件成熟度评估之前，应首先对用于试验的软件的构型状态进行评估，通过分析将进行的系统试验项目以及试验中验证的系统需求，进而明确用于试飞验证试验的软件构型。

这一评估工作需要机载软件供应商按照 RTCA/DO-178B（机载系统和设备合格审定中的软件考虑）指南文件中有关要求提供相应的软件生命周期数据予以支持。在获得所需软件资料后，通过进一步评审确认软件的具体构型，在此过程中同时关注供应商对软件的构型管理过程是否符合被批准或认可的软件构型管理计划，以增强软件构型受控的置信度。评审工作主要体现在以下两个方面要求。

1）构型状态明确软件的具体构型信息通过软

件构型索引(SCI)文件或类似等效文件(如软件版本描述文档 VDD)予以展现,所有软件相关的构型标识唯一、清晰,且具有可追溯性。如果供应商未正式发布相应的构型描述数据,则必须提供足够的、有效的构型信息,由主机厂编制等效文件向局方表明软件的构型。构型文件至少包括以下内容:

①软件标识;

②可执行目标代码构型标识以及数据完整性校验值;

③源代码构型标识;

④已发布的软件生命周期数据/文档编号、版本信息;

⑤软件发布时所有已知的开口问题;

⑥软件归档 & 发布介质。

2) 软件制造符合性检查确认。在局方制造检查代表进行正式的软件制造符合性检查前,通过对含软件的机载系统/设备进行自检,确认试验用软件构型是否符合暂时冻结的软件设计状态,是否能够满足试验所需软件构型要求。

2 软件成熟度评估考虑

在明确了用于验证试飞试验软件构型的情况下,可进入对软件成熟度的具体评估。为了实现对软件成熟度充分、有效的评估,本文采用了一种多元考虑的方法,从以下两个方面及其各子项要素对软件成熟度进行综合的评估和考量。

2.1 软件功能评估

对软件功能进行评估主要是通过验证和确认软件当前构型所具备的功能,从功能成熟度的角度判断当前软件能否支持将要进行的试飞科目,重点考虑以下两个方面。

2.1.1 工程研发试验完成情况评估

TIA 前含软件的机载系统/设备通常已完成大量的实验室试验、机上地面试验以及工程研发试飞试验。通过对上述试验完成情况的评估,分析软件实现的功能情况和存在的问题,同时对比软件全功能状态进行适当分析以明确软件使用限制并做出相关考虑和保障措施,例如在飞行员操作手册中明确相关替代方法或注意事项。

2.1.2 适航验证风险评估

在系统的试飞科目及需要验证的适航条款确定的前提下,通过评估已完成的地面适航验证试验以及工程研发试飞情况,并结合供应商提供的系统试飞安全性分析文件,对适航验证的风险进行评估,判断系统及软件当前构型所具备的功能是否支持完成预定的验证试飞科目,进而符合相应的适航条款。

2.2 软件符合性评估

除了上述的软件功能评估外,软件成熟度评估的另一考虑要素就是软件自身的符合性评估,主要是评估软件的研制过程与 DO-178B 目标的符合性。DO-178B 作为 FAA 推荐的机载软件合格审定的指南性文件,提供了一种结构化的软件设计保证方法,有助于提高软件研制过程的置信度,目前已成为民用飞机项目软件开发普遍采用和遵循的符合性方法。在含软件的机载系统/设备进行验证试飞试验前,确认软件的生命周期过程符合 DO-178B 的适用要求是必要的,也是必须的。缺乏这一评估基础,将使得试飞具有不可控的风险,尤其是高级别软件(A 级或 B 级)的机载系统/设备。

基于 DO-178B 中所述的软件生命周期过程中的目标与活动,需要对软件的计划、开发、验证、集成、构型管理和质量保证等各个过程进行评审,本文在此提出几个需要特别关注的评估要素:软件追溯性、衍生需求、软件验证过程和活动、开口的软件问题报告以及工具鉴定,下面对这些要素的评估重点逐一展开说明。

2.2.1 软件追溯性及衍生需求评估

软件追溯性评估主要是确认系统需求与软件需求,软件各层级需求,软件需求与软件代码之间是否具有双向追溯性,如图 1 所示,要求做到:

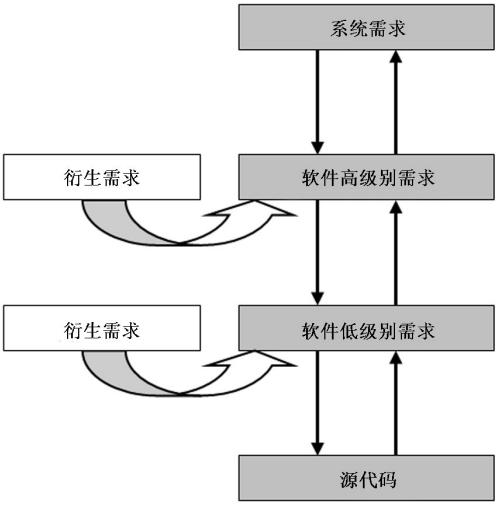

图 1　软件追溯性关系图

1)软件高级别需求发布且构型受控,符合系统需求,与系统需求之间具有双向追溯性,并可通过低级别需求和代码实现。

2)软件低级别需求发布且构型受控,符合软件

高级别需求,与软件高级别需求之间具有双向追溯性,并可通过源代码实现。

在对软件追溯性进行评估的同时,还需重点关注衍生需求在软件需求的各个层级是否有明确定义,且具有向下可追溯性。主机厂可基于内部的衍生需求评估机制,对供应商反馈的影响到系统需求或系统间接口定义的衍生需求进行分析和评估,确保其对系统和飞机无安全性影响,从需求层面充分满足软件的符合性要求。

2.2.2　软件验证工作评估

软件的验证活动是检验软件功能正确实现和软件运行稳定性的必要手段和途径。通常情况下,软件可通过评审、分析和测试的方法进行验证。软件的主要测试过程如图 2 所示。TIA 前,通常软件的验证工作并没有全部完成,但必须有一定水平的验证工作来确保所发布软件版本的置信度。通过评估软件验证活动的完成情况来确保软件验证工作量足够且验证内容和程度可接受,重点关注以下几个方面。

1)是否完成了软硬件集成测试,以确保软硬件的匹配性、兼容性;

2)是否完成了软件高级别需求的确认与验证活动,保证系统需求实现且结果可接受;

3)是否完成了 SOF(飞行安全分析)必要的软件功能测试;

4)是否完成了一定程度的覆盖分析,包括基于需求的测试覆盖分析和软件结构覆盖分析,特别是针对设计保障等级高的软件,建立了相应的覆盖分析策略,并对完成百分比做出了一定的限制;

5)测试不仅包括正常条件下的测试,也包括鲁棒性测试;

6)所有验证数据(测试用例、测试结果等)构型受控。

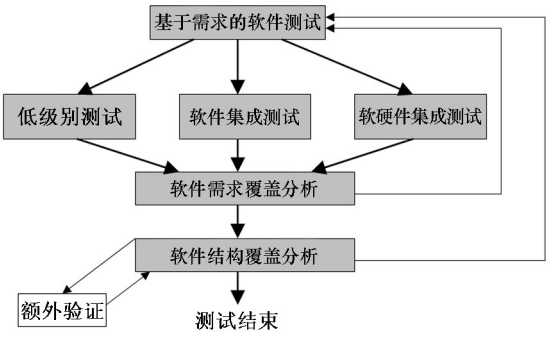

图 2　软件测试过程

2.2.3　开口的问题报告评估

TIA 前,软件的部分问题报告可能仍处在开口状态,这些问题的存在势必会在一定程度上影响软件的成熟度。因此通过评估软件开口的问题报告,判断其对安全性的影响程度也是软件成熟度的一个重要考量点。主机厂可通过对所有开口的软件问题报告进行梳理和分析,评估这些问题是否会对软件使用形成一定的限制,是否对飞机的安全性存在隐患,是否会对试飞科目造成不利影响;同时确认供应商是否已按照顶层构型管理要求对所有开口问题报告的影响程度进行分类,以确保对验证试飞有严重安全性影响的问题得以优先解决。

2.2.4　软件评审发现的不符合项评估

TIA 前,主机厂通常已完成了部分软件现场审核活动以及大量的软件远程评审工作,这些评审活动所产生的不符合项的记录控制、跟踪处理和关闭情况对于评判软件的符合性程度有着重要影响。在实际评估过程中,可通过对已完成的软件远程评审和现场审核活动中发现的所有不符合项进行汇总和分析,对以下问题进行确认:

1)所有发现的软件偏离和不符合项已被记录;

2)对软件偏离/不符合项进行了有效的评估和分析;

3)判断试飞前所有软件偏离/不符合项是否都能予以纠正;

4)重点分析未关闭的软件偏离/不符合项对试飞科目的影响。

2.2.5　工具鉴定

为了加快软件的研制进程,保证项目进度,供应商会在机载软件的研制过程中采用一些工具。工具的使用能在一定程度上自动化或减少部分人工工作量,降低开发成本,并减少人为引入的错误,为使用者带来极大便利,然而工具的引入也存在潜在的不利影响,其中最直接的不利影响在于工具自身的错误可能会通过工具的重复使用而不断放大。鉴于此种情况的发生,DO-178B 提出了工具鉴定的要求,因此工具鉴定问题也是评估软件的生命周期过程对于 DO-178B 符合性的一个重要关注点。因为在不打算进行人工评审的前提下,采用未经过鉴定的工具进行的软件开发或验证活动的输出缺乏相应的置信度,无法保证软件产品性能的可靠性与安全性。由于软件工具与软件本身相同,都是由代码表达的复杂逻辑组成,开发过程和环境都非常类似,所以通常使用类似用于软件本体的基于流程的研制保证方法对软件工具进行鉴定。

TIA 前,若存在需要鉴定的工具尚未完成鉴定的情况,鉴于不同类型的软件工具其安全性影响的

程度不同,可依据工具类型的不同分别进行评估,通过检查工具的鉴定进展情况,综合判断软件工具鉴定的状态,确认工具的鉴定进度是否先于软件开发进度,即工具的部分鉴定结果是否可以为软件的开发或验证活动提供一定的置信度,从而降低使用工具的风险,提高所开发软件的符合性。

2.3　总结

综上所述,TIA 前对机载软件进行成熟度评估主要是判断试飞构型下的软件所具备的功能以及软件的符合性状态能否支持即将进行的局方验证试飞科目,满足试飞试验的适航条款验证要求。软件的功能以及软件符合性状态两者的关系可用图 3 表示。图中,坐标轴的纵轴代表软件的功能水平,横轴代表飞机项目的时间进度。坐标轴包围的区域中描绘的直线代表软件最终达到的全功能水平,曲线代表软件对于 DO-178B 的符合性程度,竖虚线代表项目进展中的一些关键节点,如首飞、TIA 等。由图 3 可见,随着项目的不断推进,软件的功能日趋成熟,软件对于 DO-178B 的符合性也在不断完善,最终直线和曲线的最高点交汇,代表软件达到最终稳定状态,此时软件的成熟度最高。

TIA 前,软件的功能和软件的符合性均未达到最终冻结状态,主机厂可通过上述一系列的评估工作向局方表明此时软件的功能以及软件的符合性状态是合适的,即软件具备一定的成熟度,可以支持后续的验证试飞科目,验证相应的适航条款。

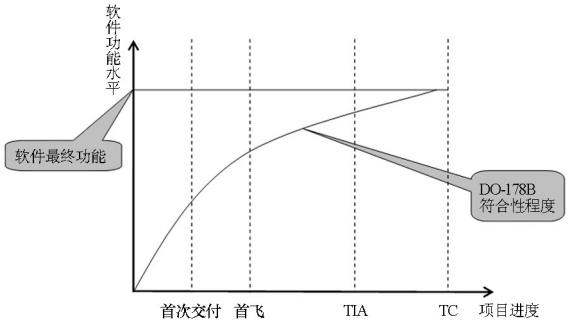

图 3　软件功能与软件符合性关系图

3　结论

软件成熟度的评估不仅能对民用飞机研制阶段的 TIA 签发前的软件工程批准提供有力的支持与保障,同时也能为保证飞行安全,成功完成局方验证试飞科目,顺利取得 TC 奠定有利基础,因此建立起符合适航条款要求和具有实际可操作性的软件成熟度评估准则与工程程序具有十分重要的意义,有待进一步深入地探索和研究。

参考文献:

[1] RTCA SC-167/EUROCAE WG-12. DO-178B Software Considerations in Airborne Systems and Equipment Certification [S]. Washington: RTCA, 1992.

(上接第 60 页)

表 1　中国典型机型故障高发系统章节分类表

项目序号	系统分类	关注度		
		高度关注	重点关注	一般关注
1	复杂电子系统	ATA34 导航	NA	ATA23 通讯 及其他
2	复杂机电系统	ATA32 起落架 ATA70-80 动力装置 ATA21 空调 ATA27 操纵	ATA29 液压 ATA24 电源 ATA36 气源 ATA30 防冰防雨 ATA33 照明	ATA49 APU ATA26 防火 及其他
3	承力系统部件	NA	ATA54 吊舱/吊架 ATA52 舱门 ATA53 机身	ATA56 窗 及其他

承力系统部件在日常运行中发生故障的数量比较少,但只要发生故障就会在很大程度上威胁到飞机的安全性,所以对其关注度可适当降低,但这并不意味着可以弃之不顾。

参考文献:

[1]姚红宇,等. 民用飞机失效分析实例选编[M]. 北京:中国民航出版社,2003.
[2]陆望龙. 实用液压机械故障排除与修理大全[M]. 湖南:湖南科学技术出版社,2002.
[3]中国民用航空局飞行标准司. 2006 年度国内航空器使用信息分析和工程管理,2007.
[4]中国民用航空局飞行标准司. 2007 年度国内航空器使用信息分析和工程管理,2008.
[5]中国民用航空局飞行标准司. 2008 年度国内航空器使用信息分析和工程管理,2009.