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

DOI: 10.19416/j.cnki.1674-9804.2024.01.020

关于某民机机载软件适航审查原则的研究

付 婷[1]* 熊小平[1] 李 宏[1] 段义乾[1] 李 腊[2]

(1. 中国民用航空江西航空器适航审定中心,南昌 330024;2. 航空工业江西洪都航空工业集团有限责任公司,南昌 330024)

摘 要: 某民用直升机拟装配先进航空电子系统,更多的功能将由软件实现,该型机在适航取证过程中将涉及大量机载软件的适航审查,需在项目早期明确机载软件的审查思路和原则。在调研国外审定局方关于机载软件适航审查的程序和方法的基础上,根据国内审定实践,结合该型机实际情况,对其机载软件的审查思路和原则进行了研究。具体提出了两方面审查原则,一是提出基于风险的方法确定审查介入程度,二是提出工具鉴定数据的复用原则,以及先前开发软件的可接受的符合性方法。作为对该型机机载软件的适航审查的预先研究,可为该型机的研制单位和适航审查团队提供一定的参考。

关键词: 机载软件;介入程度;适航;符合性方法

中图分类号: V243 **文献标识码**: A **OSID**:

0 引言

软件产品,即使是中等规模的程序,也是人类制造的最复杂制品之一,而软件开发项目是最复杂的事务之一。无论投入多少人力,花费多少时间和金钱,其结果仅仅是大致可靠而已。即便在最彻底和严格的测试之后,仍会留有一些 bug。无法用所有可能的输入去测试系统中的所有执行路线。在现代航空工业中,软件系统在航空器中所占比重正在不断增加,已经不可能回到纯模拟系统。因此,必须竭尽全力来确保软件密集型系统是可靠的和安全的[1]。

某型机更多的功能将由软件实现,大量机载软件需进行适航审查,因此,必须首先确定审查介入程度,以高效地利用局方审查资源。某型机软件取证构型中,存在不少先前开发软件,其中部分软件采用非 DO-178C[2] 的标准,甚至非民机标准开发,因此,有必要约定先前开发软件的复用或更改原则。此外,某型机新研软件多数涉及工具鉴定问题,且研制方进行 TQL-1 和 TQL-2 工具鉴定成本较高,希望最大程度地通过工具鉴定数据的复用以减轻负担,因此,有必要约定工具鉴定数据的复用原则。

国外航空界很早就开展了基于 DO-178B[3] 的机载软件适航审查。美国联邦航空管理局 FAA 发布了一系列的审定程序(Order 8110.49)[4] 和工作指导(job aid)[5] 用于指导机载软件的适航活动。相比之下,我国民机软件研制起步较晚,相关审定程序和咨询通告比较稀缺。因此,本文针对某型机软件审查问题,根据国内外审定局方相关指导文件,从机载软件审查的介入程度和可接受的符合性方法两方面对该型机的软件的审查原则进行了研究。

1 机载软件审查介入程度

在软件审查工作中,确定审查组直接介入范围和深度是审定项目的关键要素。早期项目的软件审查中,通常基于软件配置项的研制保证等级确定审查方的介入程度,可能造成对某些成熟度高且研制单位适航能力强的软件介入过深,而弱化了某些适航能力较差的研制单位研制的 C 级软件的介入。为了高效地利用局方审查资源,合理地将审查资源

* 通信作者. E-mail: fut@jxaacc.org

引用格式: 付婷,熊小平,李宏,等. 关于某民机机载软件适航审查原则的研究[J]. 民用飞机设计与研究,2024(1):128-131. FU T, XIONG X P, LI H, et al. Airworthiness review principles of airborne software for a certain civil helicopter [J]. Civil Aircraft Design and Research, 2024(1):128-131(in Chinese).

集中在可能不符合审定基础的高风险事项上,某型机的软件审查可采用基于风险的方法,基于不符合项发生的概率及其严重程度确定介入程度。本文首先根据《型号合格审定程序》[6]确定风险评估的要素为:研制单位的能力、新颖的特征、复杂程度和软件的研制保证等级。其中,研制单位的能力、新颖的特征、复杂程度代表发生概率,研制保证等级代表严重程度。其次参考 FAA Order 8110.49 中适用于国内行业现状的部分进一步具化了风险评估的要素,详见表 1。最后确定了软件的风险级别(见表 2)及其介入程度和审查工作。

表 1　风险评估要素

评估要素	评估细则	得分
研制单位的能力	应用 DO-178C 的经验	
	应用 DO-178B、DO-178A 或 DO-178 的经验	
	应用非 DO-178 系列的经验	
	软件在类似产品上发生问题的概率	
	软件质量保证体系和配置管理体系的健全	
	以往审查的介入程度	
复杂程度	系统体系结构、规模、功能和接口的复杂程度	
新颖的特征	新设计、新技术的使用	
	软件开发工具和验证工具的成熟度	
	替代方法、额外考虑的数量	
合计		总分

表 2　确定的风险级别

总分	研制保证等级			
	A 级	B 级	C 级	D 级
总分<XX	3 类	3 类	2 类	1 类
XX<总分<XX	3 类	2 类	2 类	1 类
XX<总分	2 类	2 类	1 类	1 类

FAA Order 8110.49 为表 1 中评估细则制定了得分标准,但可能不符合国内民机软件研制现状,因此,表 1 中得分标准以及表 2 中的总分区间需基于本项目软件供应商的现状确定。

1) 对于 3 类风险,确定为高介入程度软件,应由局方开展 SOI#1~SOI#4 审查,其中至少保证 SOI#2 和 SOI#3 为现场审查,且 4 个阶段审查不可合并,局方除批准软件合格审定计划、软件构型索引和软件完成综述外,研制单位还需提交全部计划文件和测试结果[7]。

2) 对于 2 类风险,确定为中等介入程度软件,应由局方开展 SOI#1~SOI#4 现场或桌面审查,可根据实际需要合并审查阶段,并批准软件合格审定计划、软件构型索引和软件完成综述。

3) 对于 1 类风险,确定为低介入程度软件,由 DER 开展 SOI#1~SOI#4 现场或桌面审查,可根据实际需要合并审查阶段,并由局方批准软件合格审定计划、软件构型索引和软件完成综述。

2　机载软件可接受的符合性方法

机载软件在表明其所适用的规章条款符合性时,可接受 DO-178C 及其补充文件作为符合性方法。

2.1　工具鉴定

对于软件研制过程中使用到的软件工具,研制单位应按照 DO-178C 中第 12.2 节的要求进行分析。如需鉴定,研制单位应按照 DO-330[8]推荐的过程和目标表明符合性。在相似的项目环境中,以往鉴定过的工具根据具体情况,其鉴定数据可提供一定程度的复用。某型机优先考虑在 DO-178C 项目中复用或更改经 DO-178B 标准鉴定的工具数据。

DO-330 的第 11.2 节给出了工具复用和更改的判定原则,FAQ D.4 为使用 DO-178B 标准鉴定的工具数据于 DO-178C 项目提供了建议。除了给出 DO-178B 和 DO-178C 中关于工具鉴定级别的对照外,其他建议并不具体。而国内尚未发布相关指导材料。

通过对比 DO-178B 和 DO-330 中的工具鉴定原则、过程和目标可知,DO-330 在延续 DO-178B 的体系结构和框架基础上,对要求进行了细化或补充。最重要的差别体现在两者对工具的分类要求不同,DO-330 中明确规定了对外部组件的要求,而 DO-178B 对 A 级工具有源代码与可执行目标码的追踪要求。

因此本文在考虑 DO-178B 和 DO-330 的差异,参考国内型号审查经验的基础上,确定在 DO-178C 项目中复用或更改经 DO-178B 标准鉴定的工具数据原则如图 1 所示。

图 1 中编号内容解释如下:

(1) DO-330 的 FAQ D.4 提供了 DO-178B 和 DO-178C 有关不同研制保证等级软件对应的工具

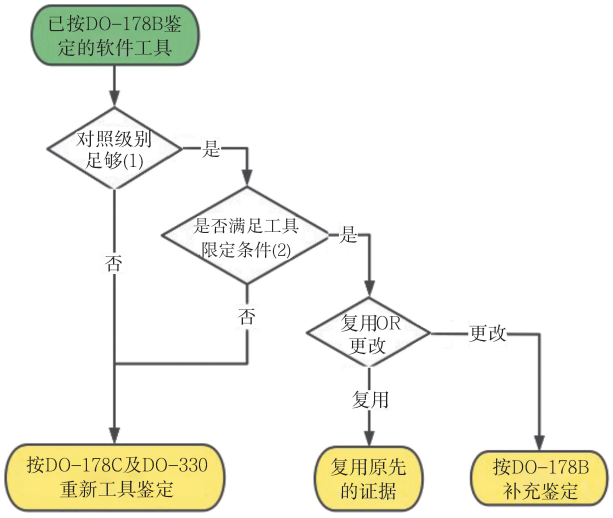

图 1　工具鉴定数据的复用或更改

类型和工具鉴定等级的对照关系的具体说明。

（2）若研制单位在 DO-178C 项目中选择复用或更改经 DO-178B 标准鉴定的工具数据，应确定当前工具鉴定满足以下全部限制条件：

a）按照 DO-178C 第 12.2 节的要求，验证工具的工具鉴定等级不能为 TQL-4；

b）不存在使用验证工具去检查开发工具输出物的情况，除非能提供 DO-330 中 FAQ D.7 的四个讨论项的符合性说明；

c）工具的研制未涉及新技术新方法，除非能够提供满足相关问题纪要的符合性证据；

d）工具不存在使用外部组件的情况，或者能提供 DO-330 T4.11 和 T7.5 两个目标的符合性证据。

2.2　先前开发软件

某型机中先前开发软件分别按 DO-178 系列和非 DO-178 系列开发。对于先前按 DO-178 系列开发的软件，FAA AC 20-115D[9] 给出了具体的指导。但是，对于先前按非 DO-178 系列开发的软件如何表明符合性，国内外并没有相关指导材料。由于无论采用何种标准开发软件，能达到与 DO-178C 要求的同等安全水平是先前开发软件复用或更改的主要准则。因此，本文基于这一原则，参考 FAA AC 20-115D 中关于按 DO-178 系列开发的先前软件的更改或复用流程，确定按非 DO-178 系列开发的先前软件的更改或复用原则如图 2 所示。

图 2 中编号内容解释如下：

（1）由于研制方想通过本流程来表明满足 DO-178C 的目标可能是困难的，尤其对于 A 级和 B 级软件，标准间的差距往往很大。因此，该型机中仅允许对先前按非 DO-178 系列开发的 D 级软件进行复用或更改评估。

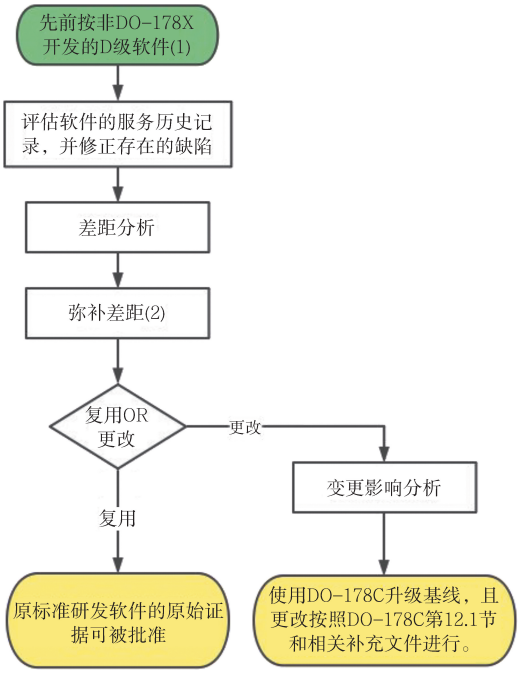

图 2　先前开发软件的复用或更改

（2）关于弥补差距的方法，DO-248C[10] 给出了相关指导，一般通过服役历史、过程认可、逆向工程、功能限制、体系结构缓解、附加测试等方法或者这些方法的组合来表明提供了与 DO-178C 同等安全水平。

3　结论

本文根据国内外审定局方相关指导文件，针对某型机需事先约定的原则性问题，进行了预先研究，研究成果为：

1）提出了基于风险的方法，从研制单位的能力、新颖的特征、复杂程度和软件的研制保证等级确定风险级别，根据风险级别确定审查介入程度及审查内容。

2）提出了该型机工具鉴定数据的复用或更改原则，以及先前按非 DO-178 系列开发的 D 级软件可接受的符合性方法。

参考文献：

[1] WIENER L R. Digital woes: why we should not depend on software[M]. U.S.: Basic Books, 1993:37.

[2] Radio Technical Commission Aeronautics. Software considerations in airborne systems and equipment certifica-

tion: DO-178C[S]. Washington D. C.: Radio Technical Commission Aeronautics, 2011.
[3] Radio Technical Commission Aeronautics. Software considerations in airborne systems and equipment certification: DO-178B[S]. Washington D. C.: Radio Technical Commission Aeronautics, 1992.
[4] Federal Aviation Administration. Software approval guidelines: Order 8110.49[S]. Washington D. C.: Federal Aviation Administration, 2003.
[5] Federal Aviation Administration. Conducting software review prior to certification: job aid[S]. Washington D. C.: Federal Aviation Administration, 2004.
[6] 中国民用航空局. 型号合格审定程序: AP-21-AA-2022-11[S]. 北京: 中国民用航空局, 2022.
[7] RIERSON L. Developing safety-critical software: a practical guide for aviation software and DO-178C compliance[M]. U.S.: CRC Press, 2013:125.
[8] Radio Technical Commission Aeronautics. Software tool qualification considerations: DO-330[S]. Washington D. C.: Radio Technical Commission Aeronautics, 2011.
[9] Federal Aviation Administration. Airborne software development assurance using EUROCAE ED-12( ) and RTCA DO-178( ): AC 20-115D[S]. Washington D. C.: Federal Aviation Administration, 2017.
[10] Radio Technical Commission Aeronautics. Supporting information for DO-178C and DO-278A: DO-248C[S]. Washington D. C.: Radio Technical Commission Aeronautics, 2011.

作者简介

付　婷　女,硕士,工程师。主要研究方向:民用航空器电子电气系统适航审定。E-mail:fut@jxaacc.org

熊小平　男,硕士,高级工程师。主要研究方向:民用航空器适航审定。E-mail:xiongxp@jxaacc.org

李　宏　男,本科,高级工程师。主要研究方向:民用航空器适航审定。E-mail:lih@jxaacc.org

段义乾　男,硕士,高级工程师。主要研究方向:民用航空器适航审定。E-mail:duanyq@jxaacc.org

李　腊　女,硕士,工程师。主要研究方向:航空器设计。E-mail:973318629@qq.com

Airworthiness review principles of airborne software for a certain civil helicopter

FU Ting[1]*　XIONG Xiaoping[1]　LI Hong[1]　DUAN Yiqian[1]　LI La[2]

(1. Jiangxi Aircraft Airworthiness Certification Center, CAAC, Nanchang 330024, China;
2. Jiangxi Hongdu Aviation Industry Co., Ltd, Nanchang 330024, China)

Abstract: A certain civilian helicopter is planned to be equipped with advanced avionics systems, and more functions will be implemented by software. The airworthiness certification of the helicopter will involve a large number of software reviews. It is necessary to clarify the review ideas and principles of software in the early stages of the project. On the basis of investigating the procedures and methods of foreign certification authorities for airworthiness review of airborne software, and based on domestic certification practices, and combined with the actual situation of the helicopter, the review ideas and principles of its onboard software were studied. Specifically, two principles of review were proposed. Firstly, a risk-based approach was proposed to determine the level of review intervention. Secondly, the principle of reusing tool identification data was proposed, as well as acceptable compliance methods for previously developed software. As a preliminary study on the airworthiness review of the airborne software of this type of helicopter, it can provide certain references for the development department and the airworthiness review teams of this aircraft.

Keywords: airborne software; involvement level; airworthiness; compliance method

* Corresponding author. E-mail: fut@jxaacc.org