文章编号:1674-8190(2023)04-189-06

基于DO-330的机载软件工具鉴定分析及应用

周培[1],陈晓强[2],张啸晨[3]
(1.中航雷华柯林斯(无锡)航空电子设备有限公司 质量适航部,无锡 214063)
(2.中航雷华柯林斯(无锡)航空电子设备有限公司 工程部,无锡 214063)
(3.航空工业雷华电子技术研究所 民机中心,无锡 214063)

摘 要: 随着软件工具在满足DO-178C的机载软件开发和验证过程中的使用日益增多,为了保证其适航性和安全性,将DO-330作为DO-178C软件工具鉴定过程指南,存在商用货架(COTS)工具无法满足特定项目开发和验证要求的问题。以DO-330的工具鉴定等级、工具鉴定的生命周期过程及目标为指导依据,分析DO-330工程实践中的主要关注点及疑难点,结合实际项目给出自主研发工具满足DO-330的工具鉴定过程。结果表明:本文提出的工具鉴定5级(TQL-5)的自研工具鉴定过程具备工程可行性且已取得实质性进展,针对COTS,需要按照DO-330要求进行自研工具鉴定的组织提供了参考与指导。

关键词: 机载软件;DO-330;工具鉴定;工具生命周期;适航
中图分类号: V24; V328.3; TP311.5 **文献标识码:** A
DOI: 10.16615/j.cnki.1674-8190.2023.04.20

Airborne software tool qualification analysis and application based on DO-330

ZHOU Pei[1], CHEN Xiaoqiang[2], ZHANG Xiaochen[3]
(1. Quality, Lean & Certificate Department, AVIC Leihua Rockwell Collins Avionics Company, Wuxi 214063, China)
(2. Engineering Department, AVIC Leihua Rockwell Collins Avionics Company, Wuxi 214063, China)
(3. Civil Aviation Center, AVIC Leihua Electronic Technology Research Institute, Wuxi 214063, China)

Abstract: With the increase of software tools used in the airborne software development and verification process to meet DO-178C, in order to ensure its airworthiness and safety, DO-330 is taken as a guide for software tool qualification process of DO-178C. At present, the commercial off-the-shelf (COTS) tools cannot meet the requirements of specific project development and verification. The evaluation tool qualification level, life cycle process and objective of tool qualification in DO-330 are used as the guidance basis. The main concerns and difficulties in the process of DO-330 engineering practice are analyzed. Combined with the actual project, the qualification process of self-developed tool to meet the requirements of DO-330 is given. The results show that the self-developed tool qualification of tool qualification level 5 (TQL-5) proposed in this paper has engineering feasibility, and has made substantial progress, which provides reference and guidance to meet specific project requirements and perform software tool qualification according to DO-330 requirements.

Key words: airborne software; DO-330; tool qualification; tool life cycle; airworthiness

收稿日期: 2022-08-01; **修回日期:** 2022-09-26
通信作者: 周培, 993735244@qq.com
引用格式: 周培, 陈晓强, 张啸晨. 基于DO-330的机载软件工具鉴定分析及应用[J]. 航空工程进展, 2023, 14(4): 189-194.
ZHOU Pei, CHEN Xiaoqiang, ZHANG Xiaochen. Airborne software tool qualification analysis and application based on DO-330 [J]. Advances in Aeronautical Science and Engineering, 2023, 14(4): 189-194. (in Chinese)

0 引 言

机载软件适航符合性标准DO-178C《机载系统和设备合格审定中的软件考虑》在第12章节补充了对工具鉴定的要求[1],并以DO-330《软件工具鉴定考虑》的形式提供了软件工具鉴定指南[2]。美国联邦航空管理局(FAA)在ORDER 8110.49中指出:若使用工具的结果是判断一个或多个目标被满足的唯一证据,则该工具必须鉴定[3-4]。

目前在国内的机载软件合格审定过程中,大多采用由工具供应商提供的商用货架(COTS)工具及其工具鉴定包[4]来满足DO-330的要求[5-7],COTS是独立于特定项目、供多类使用者使用的工具,以购买工具鉴定包支撑工具鉴定材料[4],而自研工具、准备工具鉴定数据以满足DO-330要求进行适航审定的经验非常少。对自研工具进行鉴定时,首先需识别工具的预期用途及其取消、减少和自动化的软件过程;其次需判定工具是否需要进行鉴定和工具鉴定等级(Tool Qualification Level,简称TQL),并基于TQL确定工具生命周期过程中所需满足的目标[8]。

本文首先对DO-330标准进行解读,给出TQL的判定准则、工具生命周期过程和数据、不同鉴定等级的工具所需满足的目标;其次从三大准则的区别与工具鉴定等级的确定,工具操作需求和工具需求的区别,工具鉴定5级(TQL-5)的可操作性三个方面对DO-330软件工具鉴定实践进行阐述;最后结合项目验证,给出DO-330软件工具鉴定的建议和结论。

1 软件工具鉴定标准分析

1.1 工具鉴定等级

工具鉴定活动是依据其预期用途开展的,鉴定过程始于工具对软件生命周期影响的评估。为确定使用的工具对软件过程的影响,DO-178C定义了以下准则[1]:

准则1:工具的输出是机载软件的一部分,因此可能引入错误。

准则2:工具使验证过程自动化,因此可能检测不出错误,其输出用来证明省略或减少如下过程的合理性:

1)被工具自动化的验证过程之外的验证过程;

2)可能对机载软件产生影响的开发过程。

准则3:工具在其预期使用范围内可能无法检测到错误。

工具鉴定的必要性可以基于以上三个准则进行判断。当工具符合任一准则时则需对工具进行鉴定,根据软件等级及工具符合的准则来确定TQL,确定TQL的矩阵如表1所示。

表1 工具鉴定等级确定矩阵

Table 1 TQL determination matrix

软件等级	准则		
	1	2	3
A	TQL-1	TQL-4	TQL-5
B	TQL-2	TQL-4	TQL-5
C	TQL-3	TQL-5	TQL-5
D	TQL-4	TQL-5	TQL-5

1.2 工具生命周期过程

DO-330作为DO-178C对软件工具鉴定要求的指南,保持了与DO-178C相同的文档架构[9-10]。DO-330定义的工具生命周期过程[2,4]包括:

1)工具计划过程(Tool Planning Process)。

2)工具开发过程(Tool Development Process)。

3)工具综合过程(Tool Integral Process)。该过程细分为工具验证过程,工具配置管理过程,工具质量保证过程和工具鉴定审定联络过程[2]。

工具生命周期过程的内部关系和接口如图1所示。

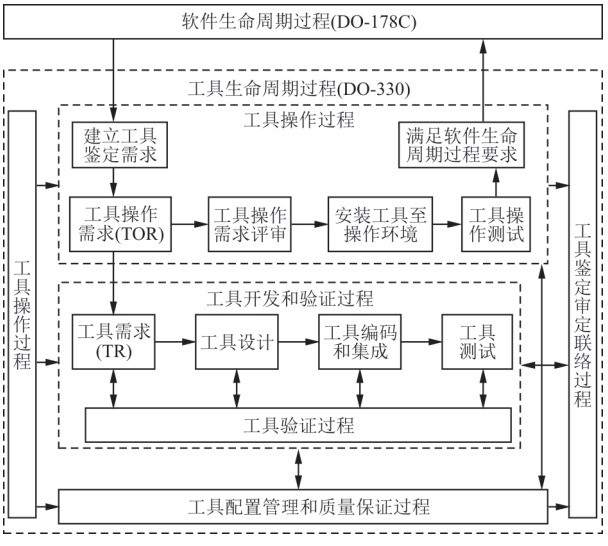

图1 工具生命周期过程[11]

Fig. 1 Tool life cycle processes[11]

1.3　工具生命周期数据

工具生命周期过程会产生工具生命周期数据,这些数据是过程的记录,也是工具鉴定的依据。工具生命周期数据如表2所示,各过程的输出数据可根据TQL进行裁剪。

表2　工具生命周期数据
Table 2　Tool life cycle data

过程	子过程	输出数据
工具计划过程	N/A	软件审定计划 工具鉴定计划 工具开发计划 工具验证计划 工具配置管理计划 工具质量保证计划 工具需求标准 工具设计标准 工具编码标准
工具开发过程	工具操作需求定义过程	工具操作需求
	工具需求过程	工具需求 包括高层需求和低层需求
	工具设计过程	工具设计描述
	工具编码过程	源代码
	工具集成过程	可执行代码
	工具操作集成过程	安装在操作环境的可执行目标码工具用户指南
工具综合过程	工具验证过程	工具测试用例 工具测试步骤 工具测试结果 工具操作验证和确认用例 工具操作验证和确认步骤 工具操作验证和确认结果
	工具配置管理过程	工具配置管理记录 工具配置索引 工具生命周期环境配置索引
	工具质量保证过程	工具质量保证记录
	工具鉴定审定联络过程	工具研制总结

从表2可以看出:工具验证过程包含两部分,工具需求的验证过程和工具操作的验证与确认过程。前者要求根据工具的预期功能验证工具开发者的活动;后者要求根据工具的预期用途验证工具使用者的活动[12]。

1.4　工具鉴定目标

DO-330附录中共包含11张过程目标表格(从Table T-0到Table T-10)。其中,Table T-0用来识别工具操作过程应满足的目标。不同TQL对应的目标数[8,13]/目标独立性要求如表3所示。

表3　工具鉴定等级对应的过程目标(含独立性要求)
Table 3　The process objectives of TQL (including independence requirements)

过程	目标数				
	TQL-1	TQL-2	TQL-3	TQL-4	TQL-5
工具操作过程	7/3	7/3	7/0	7/0	6/0
工具计划过程	7/0	7/0	7/0	2/0	0/0
工具开发过程	8/0	8/0	8/0	5/0	0/0
工具需求过程输出验证	9/6	9/6	9/0	8/0	0/0
工具设计过程输出验证	11/7	11/3	9/0	1/0	0/0
工具编码集成过程输出验证	7/3	7/1	6/0	0/0	0/0
集成过程输出测试	4/2	4/1	4/0	2/0	0/0
工具测试输出验证	9/9	7/3	6/0	2/0	0/0
工具配置管理过程	5/0	5/0	5/0	5/0	2/0
工具质量保证过程	5/5	5/5	5/5	2/2	2/2
工具鉴定审定联络过程	4/0	4/0	4/0	4/0	4/0
总目标数/独立目标数	76/35	74/22	70/5	38/2	14/2

从表3可以看出:对于TQL1～TQL3工具而言,其生命周期过程所需满足的目标远多于TQL-4与TQL-5工具,但所有TQL工具的质量保证过程都应满足独立性要求。

2　DO-330软件工具鉴定实践

2.1　三大准则的区别与工具鉴定等级的确定

在软件工具鉴定的工程实施中,面临的首要问题是确定TQL。其中,软件等级由系统安全性评估过程确定,可通过PSAC获得,但准则的确定是一大难点。

准则1相当于DO-178B中定义的“开发工具”,适用于自动生成软件开发过程输出的一部分的工具。该准则包含的工具用途有:将高层级需求转化成低层级需求(或不同形式的同层级需求

转化),转化成源代码、数据文件、配置文件或可执行代码。此外,不产生输出数据但可能在数据中注入错误也属于准则1[2]。准则2和准则3相当于DO-178B中定义的"验证工具",适用于验证或分析软件生命周期数据、计算软件特性等的工具。但这两类准则根据工具鉴定的审定信用有所区分:若审定信用仅用于工具执行的活动直接满足目标,则属于准则3[2](例如验证工具);若其他目标也通过使用该工具得到满足或部分满足,则属于准则2[2]。例如,一种验证工具若用于自动化某些源代码的验证,属于满足准则3的工具;若取证方声称该工具可检测某种特定类型错误,而减少本该进行的针对该类错误的测试活动,则属于满足准则2的工具。

因此,TQL的确定可从以下三个方面考虑:

1) 确定需要鉴定的工具是开发工具还是验证工具。

2) 若属于开发工具,适用于准则1,根据表1结合软件等级得出TQL。软件等级A~D对应TQL1~TQL4。

3) 若属于验证工具,明确工具使用范围来判断属于准则2或3。适用于准则2的TQL,若对应的软件等级是A或B,由于要求工具需具备更高级别的严密性以增加可信度,即为TQL-4,其他均为TQL-5。

2.2 工具操作需求和工具需求的区别

在工具开发过程中,可从以下五个方面区分工具操作需求(TOR)和工具需求(TR)。

1) 定义:TOR从软件生命周期过程的角度定义工具的功能和接口,而TR定义开发该工具所必须的功能和特性。TOR关注工具的用途,而TR关注工具的功能。

2) 相关方来源:TOR多来源于工具使用者,而TR由工具开发者定义。

3) 过程来源:TOR来源于工具操作需求定义过程,而TR来源于工具需求过程。

4) 需求层级:TOR一般作为工具"系统需求",而TR作为工具"高层需求"。TOR可被细化为一个或多个TR[14]。

5) 验证角度:工具验证过程类似于软件验证过程,而工具操作的验证和确认过程类似于系统生命周期对软件的验证和确认。TOR的"验证"表明工具的行为符合预期,而"确认"表明TOR的正确性。

2.3 工具鉴定5级(TQL-5)的可操作性

由于航空验证工具的专用性要求,将TQL设定为TQL-5对于工具使用者是操作性最强的。原因如下:

1) TQL-5相当于"验证工具"的鉴定级别,所需满足的目标数及目标独立性要求最低。

2) 由表3可知,与TQL-5相关的目标主要集中在Table T-0工具操作过程中,而这些目标都是面向工具使用者的。这表明工具鉴定过程不需要来自工具开发过程的任何数据,在工具供应商不提供任何数据的情况下,仍然有可能将工具进行鉴定为TQL-5。

3) 在实践中,满足TQL-4及更高等级的软件工具数量很少,原因是这些工具鉴定所需的花费比鉴定TQL-5多3~10倍[12]。以TQL-5为目标,能在工具鉴定项目的早期产生初步结果,这是符合项目可行性分析的。如果在未来需要提高TQL,在TQL-5的工具生命周期数据基础上,增加关于设计、验证和确认以及环境配置等新文档和证明数据,可以很容易地建立新的TQL。

3 项目验证

在某型号大飞机气象雷达收发机模块的机载软件项目中,项目组自主设计研发了专用自动化测试工具FPT Tool,在自动化测试环境中控制、监控和配置以太网总线上进出被测软件的光纤协议数据。该工具提供了一组功能函数,可用于验证光纤通讯功能和接口需求。因为该工具用自动化测试的方法取代人工测试且其输出没有被直接验证,所以需要进行工具鉴定。

由于该工具在预期使用范围内可能无法检测到错误,属于准则2,且被测软件需满足DO-178C设计保证等级为C的要求,由表1可知,该工具被定义为TQL-5。

根据图1和表2,FPT Tool的工具鉴定过程严格按照DO-330的要求进行。在工具计划过程中,创建了该工具的工具鉴定计划(TQP),以计划中的特定章节描述满足单独的TCMP和TQAP的要求。在被测软件计划过程中,将工具鉴定相关内容写入收发机模块PSAC的"工具评估和鉴定"章节中。TQP作为SOI 1审核的一部分递交给客户和局方。TQP的结构包括:简介(Introduction),鉴定相关(Qualification Aspects),工具综述(Tool Overview),鉴定活动项(Qualification Activities),工具鉴定数据(Tool Qualification Data),额外考虑(Additional Considerations),工具配置管理计划(Tool Configuration Management Plan),工具质量保证计划(Tool Quality Assurance Plan),附录(Appendix,包括但不限于评审检查单,鉴定考虑,DO-330目标符合性)。

在工具开发过程中,基于TOR开发了工具架构,如图2所示,该工具由功能模组和人机交互模组两部分组成。功能模组提供了一组可以被自动化测试环境调用的功能函数,通过数据发送模块调用其软件接口库中的函数将测试数据发送至被测软件,通过数据接收模块调用其软件接口库中的函数捕获被测软件发出的数据。人机交互模组提供图形用户界面,通过Microsoft基础类(MFC)库显示特定光纤协议信息数据值。

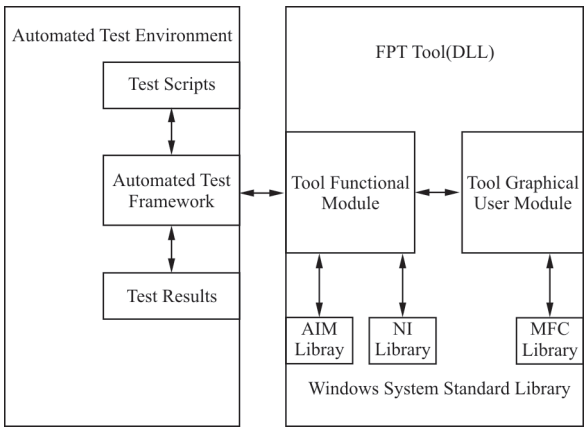

图2　工具架构

Fig. 2　Tool architecture

在被测软件所属系统的系统需求文档(SyRD)、软件需求文档(SRD)和相应接口控制文件(ICD)输入后,从系统和用户的角度开发TOR。TOR不仅反映该工具的功能和技术特征,也包括操作环境、安装、操作模式(包括故障模式)和异常输入条件等方面的需求。使用Jama工具开发TOR,需求基本属性包含需求名(Name)、描述(Description)、是否为需求(_Req?)并生成相应的工具操作需求文档,TOR顶层架构如图3所示。

图3　工具操作需求顶层架构

Fig. 3　TOR top architecture

按照计划和详细设计,主要验证工作通过编写测试脚本进行自动化测试,测试结果遵循DO-178C的要求采用人工评审。在工具验证过程前,考虑到"未使用库函数验证"的验证策略:一些Windows操作系统的标准库函数未被该工具使用,这些库函数不应影响工具的输出而产生任何错误。为确保这一点,使用分析的方法验证不正确的信息不会被未使用的库函数直接或间接(通过呈现给用户的显示界面)合并到生成的工具文件中。分析将重点关注可执行文件未使用的,与数据格式相关,或可能对输出产生影响的库函数。

在工具配置管理过程方面,目前开发阶段所产生的工具生命周期数据(TQP,TOR和工具架构等)均受控于SVN中,遵循收发机模块的SCMP要求进行了配置识别、基线和可追溯性、同行评审和变更控制。虽然控制类别2(CC2)的数据不需要变更控制,但仍选择使用Jira管理变更并归档至SVN。

在工具质量保证过程方面,软件质量工程师遵循收发机模块的SQAP要求参与支持了相关工具生命周期数据的同行评审,并生成独立的审查记录,所有质量记录归档至SVN。

在工具鉴定审定联络过程方面,目前完成的TQP已被客户TCR或取证主体单位作为SOI 1评审的一部分递交,在软件最终符合性评审第四阶段SOI 4将编制工具研制总结(TAS)以表明与表2工具生命周期数据的符合性。

4 结 论

1）当使用软件工具取消、减少或自动化DO-178C的过程时，需要按照DO-330的要求对该工具进行鉴定。作为机载软件适航取证的额外考虑因素，工具鉴定是向局方展示计划和证据的重要组成部分。

2）由于工具鉴定过程的复杂性，如果无法使用商用货架工具满足DO-178C项目的开发和验证要求，应尽早策划并开始自研工具鉴定。本文提出的工具用于鉴定5级（TQL-5）的自研工具鉴定过程具备工程可行性，对组织开展自研工具鉴定工作具有切实可行的参考与指导。

参 考 文 献

[1] RTCA Inc. Software considerations in airborne systems and equipment certifications: DO-178C[S]. Washington: RTCA Inc., 2011.

[2] RTCA Inc. Software tool qualification considerations: DO-330[S]. Washington: RTCA Inc., 2011.

[3] Federal Aviation Administration. Software approval guidelines: ORDER 8110.49[S]. US: Federal Aviation Administration, 2003.

[4] 倪红英，崔明明. 民机适航软件工具鉴定考虑[J]. 航空电子技术，2018，49(2)：36-42.
NI Hongying, CUI Mingming. Software tool qualification consideration in civil aviation certification[J]. Avionics Technology, 2018, 49(2): 36-42. (in Chinese)

[5] 夏小凤，向柯. 基于DO-330的商业成品软件的工具鉴定方法及应用[J]. 计算机应用与软件，2018，35(4)：329-333.
XIA Xiaofeng, XIANG Ke. Tool qualification method and application of cots tool based on DO-330[J]. Computer Applications and Software, 2018, 35(4): 329-333. (in Chinese)

[6] 崔亮，杨漫. 综合测试设备中的软件工具鉴定方法研究[J]. 航空科学技术，2017，28(7)：52-55.
CUI Liang, YANG Man. Research on software tool qualification method in comprehensive testing equipment[J]. Aeronautical Science & Technology, 2017, 28(7): 52-55. (in Chinese)

[7] 闫雪奎，邓素英，杨凯. 商用货架类软件验证工具的鉴定实践[C]// 2020(第九届)民用飞机航电国际论坛. 北京：中国航空学会，2020：1-5.
YAN Xuekui, DENG Suying, YANG Kai. Practice of COTS tool[C]// 2020 (the Ninth) Civil Aircraft Avionics International Forum. Beijing: Chinese Society of Aeronautics, 2020: 1-5. (in Chinese)

[8] 吴绿原. DO-330标准对机载软件开发过程的考虑[J]. 电子技术与软件工程，2019(15)：21-24.
WU Lyuyuan. Considerations of the DO-330 standard for airborne software development process[J]. Electronic Technology & Software Engineering, 2019(15): 21-24. (in Chinese)

[9] LIU Jianfang, ZHANG Xinai, ZHAO Yi. Tool qualification requirements comparison and analyses between RTCA/DO-178B and RTCA/DO-178C+DO-330[J]. Journal of Physics: Conference Series, 2021(1): 012191.

[10] 周培. 基于DO-178C的机载软件质量保证与管理[J]. 航空工程进展，2021，12(6)：161-166.
ZHOU Pei. Airborne software quality assurance and management based on DO-178C[J]. Advances in Aeronautical Science and Engineering, 2021, 12(6): 161-166. (in Chinese)

[11] MARQUES J, CUNHA A M. COTS tool qualification using RTCA DO-330: common pitfalls[C]// 2017 IEEE/AIAA 36th Digital Avionics Systems Conference. US: IEEE, 2017: 1-6.

[12] IBRAHIM M, DURAK U. State of the art in software tool qualification with DO-330: a survey[C]// 2021 Software Engineering (Satellite Events) Conference. US: [s. n.], 2021: 1-5.

[13] 王小波，湛文韬，袁迹，等. 基于DO-330的民用飞机机载设备工具鉴定方法研究[J]. 长江信息通信，2021，34(12)：83-85.
WANG Xiaobo, ZHAN Wentao, YUAN Ji, et al. Research on tool qualification method of civil aircraft airborne equipment based on DO-330[J]. Changjiang Information & Communications, 2021, 34(12): 83-85. (in Chinese)

[14] POTHON F, POMIES L, COMAR C, et al. Do-330/ed-215 benefits of the new tool qualification document[R]. US: ACG Solutions, 2013.

作者简介：

周 培（1990—），女，硕士，高级质量工程师。主要研究方向：民用机载软件的测试验证、设计过程保证、工具鉴定。

陈晓强（1985—），男，学士，高级系统工程师。主要研究方向：民用航空电子系统的开发、测试和集成。

张啸晨（1994—），男，硕士，助理工程师。主要研究方向：机载软件质量保证。

（编辑：丛艳娟）