

DOI: 10.19452/j.issn1007-5453.2017.08.043

机载软件工具鉴定及重用先前鉴定工具研究

崔亮*, 王嘉良

中国航空无线电电子研究所, 上海 200233

摘要: 随着大量工具应用于民用飞机机载软件的开发, 越来越多的研制单位选择对工具开展鉴定活动, 以保证工具提供的置信度至少相当于其自动化的过程活动。本文基于相关适航标准要求, 定义了重用先前鉴定工具数据的策略, 并提出提高工具鉴定数据重用性的方法。

关键词: 民用飞机; 机载软件; 工具鉴定; 工具鉴定重用性

中图分类号: TP311.56 **文献标识码:** A **文章编号:** 1007-5453 (2017) 08-0043-04

随着民用飞机机载软件系统复杂性的不断提高, 软件工具在飞机研制过程, 尤其是在机载软件的开发、验证、管理支持活动中被越来越广泛地使用。软件工具的使用提高了工作效率、降低开发成本和风险, 并在一定程度上减少了常见的人为错误。但是如果软件工具本身存在缺陷或者对软件工具使用不当, 则可能导致机载软件出错或不能发现机载软件中的错误, 从而可能对机载软件的质量造成影响^[1-3]。为了规避这种风险, 适航要求中提出了对工具鉴定的要求, 以确保软件工具可提供同等的适航置信度。本文结合 DO-178B/C 以及 DO-330 等机载软件及工具鉴定适航标准, 对工具鉴定及其重用性进行梳理研究。

1 工具鉴定

1.1 工具鉴定的发展历程

1992 年 12 月, 美国航空无线电技术委员会 (Requirements and Technical Concepts for Aviation, RTCA) 颁布的 DO-178B^[4, 5] 首次提出了工具鉴定的概念并对工具鉴定提出了要求, 根据软件工具的功能和其在机载软件生命周期中的使用方法, 将需要考虑鉴定问题的软件工具分为了软件验证工具和软件开发工具两类, 并针对这两类软件工具提出了不同的适航要求和鉴定准则。

2004 年, 美国联邦航空局 (FAA) 和航空工业界的代表与 RTCA 进行沟通, 讨论针对 DO-178B 自 1992 年发布以来出现的软件新技术的修订问题。RTCA 和 EUROCAE 于 2004 年底启动了对 DO-178B 的修订工作, 并于 2011 年 12 月发布了 DO-178C (EUROCAE 发布了等效文档 ED-12C), 同时发布了一系列补充文档, 其中包括一份专门针对软件工具鉴定的标准——DO-330。

DO-178C 继承了 DO-178B 对工具鉴定的定义和必要性评估策略, 但是没有沿用 DO-178B 对软件工具的分类方法, 而是根据软件工具对机载软件的影响划分了 3 个准则 (准则 1~ 准则 3), 然后基于 3 个准则和机载软件的研制保证等级 (A~E) 指向了 5 个工具鉴定级别 (TQL-1~TQL-5), 对应关系如表 1 所示^[6, 7]。其中, 安全等级 A 级为灾难性, B 级为危险性, C 级为较重要, D 级为次重要, E 级为无影响。A 级别的审定要求最为严格, E 级别则没有规定特定要求。同样地, TQL-1 工具鉴定要求最高的级别, 是用于 A 级软件开发工具的鉴定。而 TQL-5 是鉴定级别最低的, 适用于 A-D 级别软件中实现单纯验证活动的工具鉴定。

作为工具鉴定的专用标准, DO-330 根据不同的工具鉴定级别分别给出了对应的工具鉴定目标、活动和数据要求,

收稿日期: 2017-05-15; 退修日期: 2017-05-31; 录用日期: 2017-06-15

* 通讯作者. Tel.: 13601829077 E-mail: cl_careri@163.com

引用格式: CUI Liang, WANG Jialiang. Research on airborne software tool qualification and reuse of previously qualified tools [J]. Aeronautical Science & Technology, 2017, 28 (08): 43-46. 崔亮, 王嘉良. 机载软件工具鉴定及重用先前鉴定工具研究 [J]. 航空科学技术, 2017, 28 (08): 43-46.

给出了明确的指导意见,并提出了重用工具鉴定数据的额外考虑^[8]。

表 1 工具鉴定级别判定
Table 1 Determination of tool qualification level

软件研制保证等级	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 工具鉴定的目的和定义

在机载软件生命周期中使用软件工具自动化完成某些过程活动,可以提升开发效率,将重复性的开发或验证活动转化为一次性的工具活动,减少人工操作可能带来的错误。但同时为了保证工具本身的错误或不当的使用方法不会影响到机载软件产品的质量和安全性,需要对工具的开发和验证过程进行合适地监控,确保工具能够提供与其所自动化或节省的活动等效的适航置信度,从而无需再对工具的输出进行人工验证^[9]。

DO-178B/C 第 12.2 条中提到“当 DO-178B/C 要求的过程通过使用某一软件工具而省略、缩减或自动化,而被省略、缩减或自动化的过程的输出又不按照 DO-178B/C 中软件验证过程的要求进行验证时,需要对该软件工具进行鉴定”^[4, 5]。这就是工具鉴定的目的和定义。

1.3 工具鉴定的必要性评估

然而并非机载软件生命周期中所使用的所有软件工具都需要进行鉴定,为了避免不必要的人力和成本消耗,需要在实施工具鉴定前,先对整个项目的软件工具及其使用情况进行评估,以确定软件工具鉴定的必要性。

根据前文中已阐明的工具鉴定的目的和定义,可以通过评估以下两个问题来判定某个软件工具是否需要鉴定:

(1) 工具是否省略、缩减或自动化了 DO-178B/C 中的过程活动。

(2) 工具的输出是否由其他验证活动根据 DO-178B/C 软件验证过程的要求进行了验证。

如果第一个问题的答案为“是”且第二个问题的答案为“否”,那么该工具就需要进行工具鉴定,工具鉴定必要性的判定逻辑和流程如图 1 所示。

1.4 工具鉴定与机载软件审定

在机载软件生命周期中进行工具鉴定时,局方首先根据申请人定义的软件生命周期,对软件合格审定计划 (Plan for Software Aspects of Certification, PSAC) 和工具鉴定计划 (Tool Qualification Plan, TQP) 中描述的工具鉴定活动进行审查,然后申请人根据局方批准的 PSAC 和 TQP 对软件工具进行鉴

定,最后局方对已鉴定工具的实际使用方法进行审查。由此可见,工具鉴定是机载软件审定的一个环节^[10]。

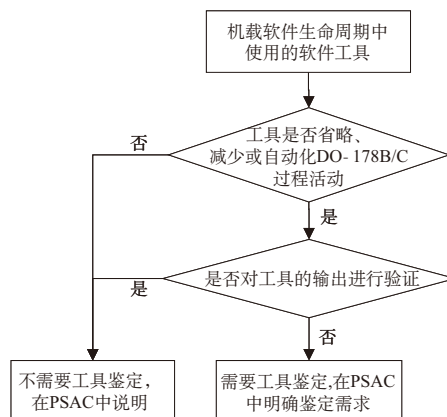


图 1 工具鉴定必要性判定

Fig.1 Determination if tool qualification is needed

DO-330 定义了软件工具生命周期的各过程及其目标、活动、数据及数据控制类别、独立性等,软件工具鉴定其实又是一次机载软件审定。软件工具生命周期与机载软件生命周期的对应关系如表 2 所示。

表 2 软件工具生命周期与机载软件生命周期的对应关系
Table 2 Relationship between software tool lifecycle and airborne software lifecycle

软件工具生命周期	机载软件生命周期
工具鉴定计划过程	软件计划过程
工具操作需求定义过程	系统需求定义过程 *
工具需求过程	软件需求过程
工具设计过程	软件设计过程
工具编码过程	软件编码过程
工具集成过程	集成过程
工具验证过程	软件验证过程
工具操作集成过程	系统集成过程 *
工具操作验证和确认过程	系统验证和确认过程 *
工具配置管理过程	软件配置管理过程
工具质量保证过程	软件质量保证过程
工具鉴定联络过程	审定联络过程

* 该过程为系统生命周期,不属于机载软件生命周期。

2 工具鉴定重用性

正如前文所述,工具鉴定来源于某个特定的软件审查项目,因此,局方通常不会对工具鉴定单独给出结论,而是依托于使用该软件工具的机载软件项目一起进行适航审定和批准。因此,当在新的机载软件项目中使用先前鉴定过的软件工具时,仍需要对该软件工具进行鉴定,但是可以评估先前工具鉴定数据的重用性,以减少在新项目进行工具鉴定的活动和工作量。

DO-330 定义了工具用户和工具开发者两类角色,并将工具操作和工具开发、验证进行了区分,将工具鉴定目标及活动、数据分配到了不同的角色,其附录 A 中表 T-0 和表

T-10 主要适用于工具用户,而表 T-1 到 T-9 主要适用于工具开发者,这些要求为工具鉴定数据的重用提供了指南。

2.1 工具鉴定重用性评估

当在后续项目中计划重用先前鉴定工具的审定信用时,必须首先对该软件工具进行评估以确保满足下列两个必要准则:(1) 软件工具在局方已经批准的机载软件项目中鉴定过;(2) 申请人可以访问先前批准的工具鉴定数据。

如果任一准则不满足,则先前鉴定工具的审定信用不可重用。如果同时满足上述两个必要准则,则可以对该软件工具进行进一步评估,以确定先前工具鉴定审定信用的可重用程度,并确定需要重验证的活动。

根据先前鉴定工具的可重用程度可以将重用先前鉴定工具分为如下 4 个场景:(1) 场景 1: 工具本身和工具操作环境没有变化;(2) 场景 2: 仅工具操作环境发生改变;(3) 场景 3: 仅工具本身发生改变;(4) 场景 4: 工具操作环境和工具本身都发生改变。

其中场景 1 的可重用程度最高,场景 4 的最低。表 3 列出了场景 1~ 场景 4 的判断准则,“√”表示其标识的所有准则在该列的场景中全部满足,“×”表示其标识的所有准则在该列的场景中至少有一条不满足。

表 3 重用先前鉴定工具的场景
Table 3 Sceneries of reuse previously qualified tools

准则	场景 1	场景 2	场景 3	场景 4
(a) 工具重用过程中使用的 TQL 低于或等于先前鉴定的 TQL	√	√		
(b) 待重用的工具生命周期数据自先前鉴定后未更改	√	√		
(c) 工具操作环境与先前鉴定的环境是等效的	√		√	
(d) 工具操作需求与先前鉴定的相同	√	√		
(e) 申请人确保使用的工具版本与鉴定数据支持的版本相同	√	√		

(1) 对场景 1,其先前鉴定工具的工具鉴定数据可以直接重用。申请人需要在机载软件项目的 PSAC 和 TQP 中说明重用工具鉴定数据的目的和理由,并提交给局方批准。此外,需要分析评估工具鉴定后发生的问题报告。

(2) 对场景 2,如工具操作的工作站的操作系统已经升级,其先前鉴定工具的工具鉴定数据不可以直接重用,需要针对工具操作环境相关的更改进行如下活动:(a) 分析工具操作环境,应注意识别操作系统、附加硬件和软件组件等,以确保工具验证环境能够代表新的工具操作环境;(b) 评审和分析工具操作需求,以确保工具操作环境兼容性需求是完整的,并且适用于新的工具操作环境;(c) 在工具操作环境中对工具操作需求进行验证和确认,以确保工具安装到新的工具操作环境中依然符合软件生命周期过程的要求,主要活动有:基于工具操作

需求开发测试用例和测试规程;将可执行目标代码安装到工具操作环境并执行测试规程、记录测试结果;评审测试结果,必要时解释实际结果与预期结果之间的偏离;选择能够代表实际的工具使用及其在工具操作环境中接口的输入集合,运行软件工具,以确认工具操作需求的正确性和完整性。

申请人需要在机载软件项目的 PSAC 和 TQP 说明重用工具鉴定数据的目的和理由,先前鉴定后的更改及其影响分析,并提交给局方批准。

(3) 对场景 3,如工具版本升级、工具预期使用方式变化等,其先前鉴定工具的工具鉴定数据不可以直接重用。申请人需要对这些变化做影响分析以明确需要重新验证的内容,至少包括以下方面:(a) 工具操作需求;(b) 工具需求;(c) 工具设计描述;(d) 工具源代码;(e) 工具开发环境和开发过程。

软件工具本身发生变化后,其先前鉴定工具的工具鉴定数据可重用性程度取决于其变化类型(增加、修改或减少)、工具本身、变更影响域等。例如,如果增加或修改了某一条与其他多个模块有耦合的一条工具操作需求,那么会影响多条工具需求、设计、代码等,则该工具鉴定数据的重用性将会较低。而如果仅仅删除了一条独立性很高的工具操作需求,则其相关的工具需求、设计、代码等数据容易分析出来,那么只需要删除相关数据即可,其工具鉴定数据的重用性则相对较高。

(4) 对场景 4,工具本身和工具操作环境都发生了改变,其先前鉴定工具的工具鉴定数据可重用程度一般已很低,通常相当于重新对工具进行鉴定。

2.2 提高工具鉴定重用性的方法

基于工具鉴定数据重用的要求和方法,若希望提高工具鉴定数据的重用性,则要求工具鉴定数据具有良好的模块化、独立性、通用性、易维修性等。本文建议可采用如下方法来提高工具鉴定数据的重用性:

(1) 在初始工具鉴定生命周期中进行重用性相关的前瞻性考虑和计划,对工具鉴定生命周期的角色及其相关目标、活动、数据等进行合理组织和分配;

(2) 根据工具鉴定数据与软件工具本身的固有关系,可以把鉴定数据分为 3 类 a) 软件工具本身的生命周期数据:工具开发生命周期中产生的数据,如工具开发计划、工具需求、工具设计描述等,这些数据是工具本身固有的,只要工具不发生改变,这些数据就保持不变;(b) 工具功能、操作、操作环境相关的数据:工具操作相关过程中产生的数据,如工具操作需求过程的工具操作需求、工具操作集成过程的工具安装报告等,这些数据是工具对工具用户的接口,在工具鉴定过程中,工具用户将基于此类数据开发特定项目的工

具鉴定数据;(c) 工具在特定项目中的鉴定数据:工具在某特定机载软件项目中的使用方法、失效影响、鉴定要求等,如该项目的工具鉴定计划、工具操作需求等,这些数据是机载软件项目所固有的,不同项目中这些数据会不一样。

上述3类数据的可重用性并不相同,一般软件工具本身的生命周期数据的最高,而工具在特定项目中的鉴定数据的可重用性最低,将工具鉴定数据按可重用性进行分类并保持一定的独立性,可以提高工具鉴定数据的重用性。

3 结束语

随着机载软件工具鉴定的推广,更多层级的工具都开始考虑鉴定的问题,如飞机总体设计、系统设计、安全性分析等,工具鉴定及工具鉴定数据的重用性需求越来越高。本文阐明了工具鉴定的目的和定义、必要性评估方法、工具鉴定过程、工具鉴定数据重用的方法以及提高工具鉴定重用性的建议,希望帮助研制单位相关人员掌握相关概念和方法,减少不必要的工作量,提高项目资产复用程度,节省项目成本的同时保证产品质量。

AST

参考文献

- [1] Taft T, Bordin M. Towards a lean tool qualification process [C] // Digital Avionics Systems Conference, 2014 IEEE/AIAA 33rd Digital Avionics Systems Conference (DASC), Colorado Springs, 2014: 1-40.
- [2] Busser R D, Blackburn M. Guidelines for software tool qualification [EB/OL]. http://knowledgebytes.net/downloads/Guidelines_for_SW_Tool_Qual_ssci-2003064-D-P.pdf.
- [3] Camus J L, Dewalt M P, Ladier G, et al. Tool qualification in multiple domains: status and perspectives [C] // Embedded Real Time Software and Systems, France: Springer, 2014: 7991.
- [4] DO-178B Software considerations in airborne systems and equipment certification [S]. USA: RTCA/EUROCAE, 1992.
- [5] DO-248B Final report for clarification of DO-178B "Software considerations in airborne systems and equipment certification" [S]. USA: RTCA/EUROCAE, 2001.
- [6] DO-178C Software consideration in airborne systems and equipment certification [S]. USA: RTCA/EuroCAE, 2011.
- [7] DO-248C Supporting information for DO-178C and DO-278A [S]. USA: RTCA/EuroCAE, 2011.
- [8] DO-330 Software tool qualification considerations [S]. USA: RTCA/EuroCAE, 2011.
- [9] Rierson L N. Developing safety critical software [M]. USA: Taylor & Francis Group, TLC, 2013.
- [10] AIR-120, Order 8110.49 Chg1 Software approval guidelines [S]. USA: U.S. Department of Transportation Federal Aviation Administration, 2011.

(责任编辑 王潇一)

作者简介

崔亮(1979—)男,硕士,高级工程师。主要研究方向:机载软硬件研发及管理。

Tel: 13601829077

E-mail: cl_careri@163.com

Research on Airborne Software Tool Qualification and Reuse of Previously Qualified Tools

CUI Liang*, WANG Jialiang

China Aeronautical Radio Electronics Research Institute, Shanghai 200233, China

Abstract: With the increasing application of tools in the development civil aircrafts airborne software, tool qualification has been widely applied to ensure the confidence coefficient tool provided is at least equivalent to that of the processes automated. The paper defined the strategy of reuse of previously qualified tools and proposed a method to increase the reuse of tool qualification data based on airworthiness standard request.

Key Words: civil aircraft; airborne software; tool qualification; reuse of tool qualification

Received: 2017-05-15; Revised: 2017-05-31; Accepted: 2017-06-15

*Corresponding author. Tel. : 13601829077 E-mail: cl_careri@163.com