DOI: 10.19452/j.issn1007-5453.2017.07.052

综合测试设备中的软件工具鉴定方法研究

崔亮*，杨漫
中国航空无线电电子研究所，上海 200233

摘　要：随着安全关键系统软件的复杂性和重要性的不断提高，软件工具在软件开发和验证过程中得到了越来越广泛的使用，工具鉴定问题日益突出。本文通过梳理 DO-178C 和 DO-330 中对于工具鉴定的要求，总结了综合工具的鉴定方法，并通过工程实践验证了综合工具鉴定方法的可行性，为复杂综合测试设备的工具鉴定提供了理论依据和实施指导。

关键词：机载软件；DO-330；工具鉴定；综合测试设备

中图分类号：TP311.56　　**文献标识码**：A　　**文章编号**：1007-5453 (2017) 07-0052-04

随着安全关键系统软件的复杂度和重要性的日益提升，对于软件开发和验证过程的要求也越来越严格。为了提高安全关键系统软件的开发和验证效率，软件工具得到了越来越广泛的应用。一套成熟的软件工具能够减少开发和验证的工作量，降低开发成本，并减少人为引入的错误，能为软件研制单位节省足够的资源。然而，如果软件工具不恰当地执行了其预期的功能，工具中的错误可能会对安全关键系统软件造成负面的影响。为了规避这种风险并确保工具功能的完整性，轨道交通领域的 EN 50128 标准[1]、重工领域的 IEC 61508/IEC 61511/IEC 62061 标准[2,3]、汽车电子的 ISO 26262 标准[4]、欧洲航空的 ECSS QA80、E40 标准，以及核电领域的 IEC 60880 标准均提出应该使用正确合理的研制流程来开发和验证软件工具[5]，航空领域 DO-178C、DO-330 也对机载软件的工具鉴定提出了明确要求。

DO-178C 和 DO-330 对工具鉴定过程及要求阐述得最为详细和具体。DO-178C 和 DO-330 均由美国航空无线电技术委员会（RTCA）于 2012 年正式颁布，是用于指导机载软件研制和软件工具鉴定的标准指南。相比其他领域对工具鉴定的要求，DO-330 中更加关注工具错误的影响分析及缓解技术，分析工具出现问题时造成的不利影响。这点在复杂综合工具的鉴定过程中体现的尤为突出。

本文以民用航空领域对工具鉴定的要求为出发点，梳理了综合工具的鉴定流程，并结合实际项目提出了案例实践解决方案，为综合工具的鉴定提供了实施参考。

1 航空领域对于工具鉴定的要求

在民用航空领域，工具鉴定是工具获得适航合格认证必需的过程，其目的是建立对工具功能的信心，确保工具提供的置信度至少等同于被省略、缩减或者自动化的过程[6]。工具鉴定的活动会根据工具错误对系统安全性的潜在影响，以及工具在软件生命周期中的使用情况而不同。工具错误对系统安全性产生不利影响的风险越高，对工具鉴定的要求就越严格。因此，工具鉴定过程不是一个固定的流程，而是需要具体项目具体分析的一个过程。

任何工具在开展鉴定工作前，都要进行确定性评估，明确是否要开展以及如何开展工具鉴定活动，即工具评估过程。整个工具鉴定的过程（包括工具评估过程）可划分为以下几个主要步骤：

（1）梳理机载软件生命周期中使用的工具，并明确每个工具的预期用途，主要针对软件开发工具和验证工具。

（2）评估工具鉴定的必要性，如果某个工具省略、减少或自动实现了开发过程或验证过程中的某个活动，而且也没

收稿日期：2017-05-15；　退修日期：2017-06-20；　录用日期：2017-06-30
* 通讯作者 . Tel.：13601829077　E-mail：cl_careri@163.com
引用格式：CUI Liang，YANG Man. Study of software tool qualification in multi-function testing equipment[J]. Aeronautical Science & Technology，2017，28(07)：52-55. 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(07)：52-55.

有对工具的输出进行验证，那么这个工具就需要进行工具鉴定。

(3) 确定工具鉴定级别 (Tool Qualification Level，TQL)，根据 DO-178C 第 12.2 条 [6] 给出的判定规则决定待鉴定的工具属于 TQL1-TQL5 中的那个鉴定级别，如表 1 所示。

(4) 根据不同的工具鉴定级别，确定并开展工具鉴定生命周期活动[7]。对于 TQL-1 的工具，其工具鉴定生命周期等同于 A 级机载软件的研制生命周期，要求最为严格。而对于 TQL-5 的工具，只需要进行基于工具操作需求的测试，要求最为简单。

表 1 工具鉴定级别

Table 1 Tool Qualification Level (TQL)

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

从表 1 可知，准则 1 中，工具的输出是软件的一部分，并且可能直接导致软件出错；准则 2 中，工具自动化了某个验证过程，并且可能导致没有检测出软件的错误，另外，工具的输出结果还被用来证明省略、减少如下过程的合理性：被本工具自动化的验证过程之外的验证过程或开发过程；准则 3 中，工具在其预定的使用方式下可能无法检测出软件的错误。

由此可见，开展工具鉴定所需要的成本、难度和研制机载软件不相上下，因此，实际开展工具鉴定工作时，需要权衡工具鉴定级别、审定信用、工具鉴定成本各个因素。基于工具鉴定级别，确定工具鉴定生命周期，评估工具鉴定成本，并在工具鉴定和审定信用之间进行权衡，选择对项目最优的工具鉴定解决方案[8]。

2 综合工具的鉴定要求

上文简要描述了民用航空领域对工具鉴定的适航要求。在现实工程场景中，经常会面临一个工具同时具备多种功能的情况。不同的功能对机载软件的影响是不同的，因此，可能有不同的工具鉴定级别，这类工具称之为综合工具。对于综合工具的鉴定与其他工具的鉴定的考虑会有所不同。

综合工具的鉴定主要取决于它的用法，对综合工具的鉴定过程进行细化，概况起来一共包含 5 个步骤 (1) 分解工具所具备的功能；(2) 确定在机载软件生命周期中使用到的功能；(3) 确定是否信任这些功能来省略、减少、自动化 DO-178B/C 要求的目标；(4) 根据各功能对机载软件生命周期过程和目标的影响，来确定每个被信任的功能相应的鉴定级别；(5) 确定具体的鉴定方法。

可以看到，相比单一功能的鉴定，具有多种功能的综合工具需要对于每种功能进行评估分析，确定每种功能的鉴定级别，从而确定具体的工具鉴定生命周期活动。

当综合工具包含了不同工具鉴定级别的多种功能时，有两种鉴定方法：

(1) 以最高的鉴定级别来鉴定整个综合工具：为整个工具编写一套工具鉴定计划、工具操作需求等鉴定数据，并按照相同工具鉴定生命周期活动完成对所有功能的鉴定工作。

(2) 把工具鉴定的各种功能按照各自鉴定级别分开鉴定，但需要先进行如下步骤的详细评估，如图 1 所示。

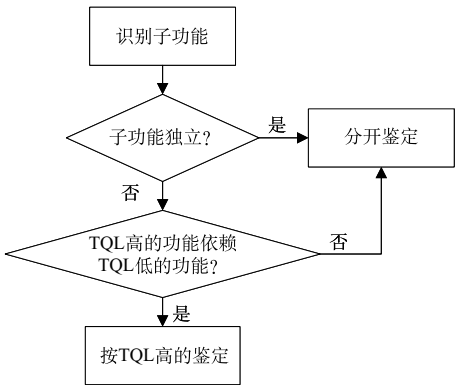

图 1 多功能综合工具的鉴定流程

Fig.1 Qualification process of multi-function tools

对综合工具的各个功能进行有效地识别，并明确它们之间的依赖和交互关系；完全独立的功能可以分开鉴定；鉴定级别较高的功能依赖于鉴定级别较低的功能时，则不能分开鉴定，如某个开发功能用到了验证功能中的某些函数；鉴定级别较低的功能依赖于鉴定级别较高的功能时，则可以分开鉴定。

根据 DO-178C，如果生成这项数据和验证该数据需要独立性，则必须说明这两个功能的独立性，相互之间没有依赖。

以上关于工具鉴定的决策需要体现在相关的工具计划文件 (如工具鉴定计划 TQP) 中，并得到审定机构的认可[9, 10]。

3 综合测试设备中的软件工具鉴定实践

Tech S.A.T. 公司研发的第二代航电开发系统 ADS2 系列产品是应用于航空领域的系统级开发测试平台。基于 ADS2 系统模块式的体系架构，可以根据用户不同的项目需

求定制各种综合测试设备。以网络交换机项目为例，Tech S.A.T. 公司在 ADS2 的基础上开发了一套特定的综合测试设备，可以将特定格式的测试用例发送给网络交换机进行测试，并将获取的实际运行结果与预期结果进行对比，得出测试结果是否通过的评价。

根据上文中列出的航空领域对于工具鉴定的要求，在以上场景中，ADS2 工具自动化了一系列测试执行、测试结果比对等工作，并为测试人员提供了测试结果是否通过的最终评价。当测试人员不再对 ADS2 的结果进行人工检查时，就需要对 ADS2 进行工具鉴定，以确保 ADS2 提供的置信度等同于被其省略的自动化过程。

ADS2 是一个复杂的综合测试设备，具有测试用例编辑、测试驱动封装、网络配置加载、数据分析等功能。如果将 ADS2 工具作为一个整体进行工具鉴定，其难度和工作量都远远大于工具本身省略的工作，因此，在工程上更加倾向于将其按综合工具的方式进行工具鉴定。

3.1 分解 ADS2 工具所具备的功能

通过对 ADS2 进行功能分解，得到 ADS2 的功能架构及功能模块，如图 2 所示。

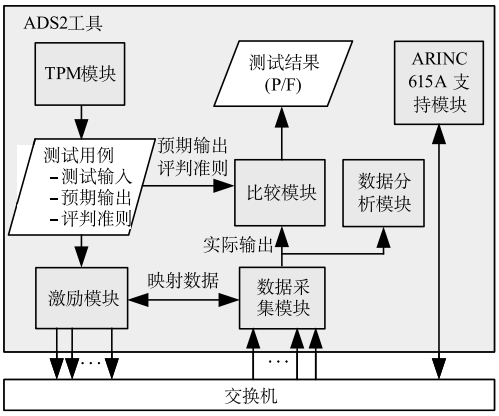

图 2 ADS2 工具的功能架构

Fig.2 Function architecture of ADS2 tool

TPM 模块，用于进行测试用例 / 测试规程的编辑；激励模块，基于测试用例 / 规程和映射数据封装 A664 信号，发送给交换机；数据采集模块，获取交换机的信号，并基于映射数据解包出实际输出；比较模块，比较预期输出和实际输出，得到测试是否通过的结论 (P/F)；数据分析模块，实时展示收发数据帧的统计信息，用于调试时使用；ARINC 615A 支持模块，自动加载并建立虚拟链路的配置表。

3.2 确定在软件生命周期中使用的 ADS2 功能及独立性

ADS2 的六大模块中前 4 个模块是与软件测试的准备和执行相关，属于软件生命周期过程中使用到的功能，需要确定这些功能是否省略、减少、自动化了 DO-178B/C 中的目标。而数据分析模块提供了对网络数据的分析功能，ARINC 615A 支持模块实现了网络配置表加载的功能。这两个模块都属于系统支持功能，没有实现任何 DO-178B/C 的目标，因此，不需要进一步分析。

ADS2 的六大模块之间仅通过输入 / 输出接口进行数据传递，从功能角度而言是相互独立的。

3.3 确定是否信任 ADS2 功能

DO-178B 中提到的测试过程有 3 个要素：测试用例、测试规程和测试结果。对于测试的三要素，DO-178B/C 提出了以下两个目标要求：

(1) 需要验证“测试规程是正确的”，对应 DO-178B 附件 A 中表 7 的第一个目标 (A7-1)；

(2) 需要验证“测试结果是正确的，且差异得到解释”，对应 DO-178B 附件 A 中表 7 的第二个目标 (A7-2)。

在 ADS2 工具的使用过程中，TPM 模块、激励模块和数据采集模块实现的功能包括：设计测用例，将测试用例进行封装成测试驱动，发送给测试对象，再从测试对象中获取反馈信号，并进行解包得到实际输出。这个过程的本质是属于测试规程。因此，TPM 模块、激励模块和数据采集模块被定位成测试规程，应根据 DO-178B/C 标准中的 A7-1 的要求进行人工验证，不需要对这些模块进行工具鉴定。

基于 DO-178B/C 中关于工具鉴定的定义，结合 ADS2 工具的实际使用情况，比较模块自动化实现的是“测试结果比对”功能，自动化实现 DO-178B 标准 A7-2 目标，这部分功能需要进行工具鉴定。

3.4 确定被信任的功能的相应的鉴定级别

根据 DO-330 附件 B 中对工具鉴定级别 (TQL) 的定义，比较模块适用于工具鉴定等级评价准则 3：工具在其预定的使用方式下可能无法检测出机载软件的错误。考虑到 ADS2 工具所应用的网络交换机属于 A 级软件，依据表 1 确定比较模块的工具鉴定级别为 TQL5。

3.5 确定 ADS2 的鉴定方法

通过上文对于 ADS2 功能模块的拆分和分析，确定了真正需要进行工具鉴定的模块及其工具鉴定级别，就可以根据 DO-330 中的目标要求开展工具鉴定活动，准备适航审定数据。对于 TQL-5 级工具，需要进行的工作包括：编写并核查工具鉴定计划；开发并核查工具操作需求；基于工具操作需求开发工具鉴定测试用例 / 规程，并建立追踪关系；核查工具鉴定

测试用例 / 规程及追踪关系；安装工具，编写工具安装报告；搭建工具鉴定测试环境；执行工具鉴定测试规程，获取并分析测试结果；编写并核查工具鉴定测试报告；编写并核查工具完成综述、工具配置索引；开展配置管理和质量保证活动。

4 结束语

本文通过梳理 DO-178C 和 DO-330 中对于工具鉴定的要求，总结了综合工具的鉴定方法，并通过工程实践验证了综合工具鉴定方法的可行性，为民用飞机系统复杂综合测试设备的工具鉴定提供了理论依据和实施指导。 AST

参考文献

[1] CENELEC. EN50128 Railway applications-communications, signaling and processing systems-software for railway control and protection systems [S]. Europe：CENELEC，2001.

[2] IEC. IEC61508 Functional safety of electrical/electronic/programmable electronic safety-related systems [S]. Switzerland：IEC，1998.

[3] Boulanger J L. CENELEC 50128 and IEC 62279 standards, Chapter 9 Tool qualification [M]. USA：Wiley Online Library - John Wiley & Sons，2015.

[4] Conrad M，Sandmann G，Munier P. Software tool qualification according to ISO 26262 [R]. USA：SAE International，2011.

[5] 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.

[6] RTCA. DO-178C Software consideration in airborne systems and equipment certification [S].USA：RTCA/EuroCAE，2011.

[7] RTCA. DO-330 Software tool qualification considerations [S]. USA：RTCA/EuroCAE，2011.

[8] Taft T，Bordin M. Towards a lean tool qualification process[C]// Digital Avionics Systems Conference，2014 IEEE/AIAA 33rd Digital Avionics Systems Conference (DASC)，USA：Colorado Springs，2014：1-40.

[9] Department of Transportation Federal Aviation Administration. Order 8110.49 Chg1 Software approval guidelines [S]. USA：U.S. Department of Transportation Federal Aviation Administration，2011.

[10] 孙全艳，赵京洲，章晓春．基于 DO-178B 的民用飞机机载软件工具的鉴定和应用 [J]. 民用飞机设计与研究，2011 (1)：56-61.
SUN Quanyan，ZHAO Jingzhou，ZHANG Xiaochun. Research and application on civil airborne software tool qualification based on DO-178B [J]. Civil Aircraft Design and Research，2011 (1)：56-61. (in Chinese)

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

Study of Software Tool Qualification in Multi-function Testing Equipment

CUI Liang*，YANG Man

China Aeronautical Radio Electronics Research Institute，Shanghai 200233，China

Abstract：With the increasing complexity and significance of the safety-critical software systems，more and more software tools have been used in the software development and verification processes. This paper analyzed the requirements of tool qualification in DO-178C and DO-330，summarized the qualification methods of multi-function tools，and proved the feasibility of the methods by project practice，it will providing the theoretical and practical guidance of software tool qualification in multi-function testing equipment.

Key Words：airborne software；DO-330；tool qualification；multi-function testing equipment

Received: 2017-05-15； **Revised:** 2017-06-20； **Accepted:** 2017-06-30

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