

浅析机载软件工具鉴定要求

The Requirements for Airborne Software Tool Qualification

刘建方 / 上海飞机设计研究院

摘要:随着大量工具应用于机载软件的开发,工具鉴定的问题日益突出。本文介绍了机载软件工具鉴定的原因和目的,并基于机载软件工具的分类介绍了工具鉴定的前提和准则以及工具鉴定的数据要求,最后提出了工具鉴定过程中需要关注和解决的问题。

关键词: 机载软件; 工具鉴定; 开发工具; 验证工具

Keywords: airborne software; tool qualification; development tool; verification tool

0 引言

机载软件开发验证过程中存在着大量重复性、易出错且高花费的工作,为了解决这一问题,各种软件工具不断地被应用于机载软件的开发、验证中。这些工具的应用,大大减少了重复性的劳动。如果机载软件工具的使用,使机载软件在不需人力介入的情况下自动达成了适航认证标准DO-178B的目标,而且机载软件输出的结果无需按DO-178B第6章的要求对达成的目标进行验证,机载软件就可作为适航审查的符合性证据使用,那么此情况下的机载软件工具就必须经过鉴定。机载软件工具鉴定的目的是为了保证工具输出的置信度至少等价于由于使用工具而消除、减少或自动化了的过程的置信度^[1]。

1 机载软件工具的分类

根据是否在机载软件中引入错误,将机载软件工具分为开发工具和验证工具两类,而联合工具实际上是这两类工具的集合。

1) 开发工具:输出的是机载软件的一部分,创建或修改机载软件的生命周期数据(如需求、设计、代码等)。开发

工具的失误将在最终交付的机载软件中引入错误。典型的开发工具是由软件的低级别需求直接自动生成代码。

2) 验证工具:验证工具通常用来表明软件生命周期数据的正确性、一致性和兼容性,不对软件的生命周期数据进行修改,因此不会向机载软件引入错误,但是有可能检测不到软件中已经存在的错误。典型的验证工具包括按照需求生成测试用例和规程的工具、自动运行测试用例并判断测试是否通过的工具以及结构覆盖率分析工具等。

3) 联合工具:同时具有开发工具和验证工具的功能。

2 机载软件工具鉴定的前提

按照DO-178B的规定,只有“确定性”的工具才能接受鉴定。从狭义上讲,“确定性”工具是指同一个输入总能得到同一个输出。但是,对于工具来说,“确定性”在广义上可以理解为确定输出正确性的能力。如果经过验证表明,对于给定的输入集合,工具的各种输出都是正确的,那么该工具也是“确定性”工具^[2]。

在开发机载软件项目之初,首先要

确定的就是软件工具是否需要鉴定。一般需要考虑三方面的问题:

1) 工具是否会在机载软件中引入错误或检测不到存在的错误;

2) 工具的输出是否不再经过进一步验证或人工评审;

3) 工具的输出是否被用来表明满足DO-178B附录A的任一目标。

如果以上三个问题的回答都是肯定的,则该工具需要进行工具鉴定,否则不需要。机载软件项目中所使用的工具列表以及是否需要鉴定的声明(即对以上三个问题的回答)应该包含在机载软件合格审定计划(PSAC)中。

3 机载软件工具鉴定的准则

DO-178B规定,开发工具的目标应与使用工具的机载软件的目标相同,即分配给开发工具的软件级别应与其开发的机载软件相同。同时,由于开发工具可能会向机载软件中引入错误,所以必须进行鲁棒测试。

验证工具不会向软件引入错误,只可能检测不到存在的错误。因此,只要验证是在正常条件下进行的,工具的输

出就符合操作需求。

对于联合工具,如果不能表明两类功能存在分区机制,则应按照开发工具的准则进行鉴定。

此外,机载软件的工具鉴定必须在特定的环境和使用限制下基于特定的项目进行。如果要使用先前项目的工具鉴定结论作为其鉴定结论,则必须证明两个项目中工具的使用环境和限制是完全相同的。

根据机载软件工具的不同类别,其鉴定准则如表1所示^[3]。

4 机载软件工具鉴定的数据要求

软件开发工具要满足的目标应与用其开发的机载软件应达到的目标相同,因此产生了DO-178B规定的20类生命周期资料。其中,工具鉴定计划(TQP)和工具完结综述(TAS)提交适航当局批准,其他开发和验证数据供局方审查时检查。同时,机载软件的合格审定计划(PSAC)和完结综述(SAS)应分别索引至TQP和TAS。

对于验证工具来说,TQP的内容可以包含在机载软件的合格审定计划中,TAS的内容可以包含在机载软件的完结综述中。工具操作需求、测试用例、规程和结果供局方审查时检查。但是,FAA推荐验证工具也要编制独立的TQP和TAS,便于今后项目复用工具的鉴定结论。

开发工具和验证工具的鉴定数据都要纳入软件构型控制体系。其中,开发工具的鉴定数据应按照CC1进行控制,验证工具的鉴定数据应按照CC2进行控制。机载软件工具鉴定数据要求如表2所示。

5 总结展望

DO-178B及FAA相关文件规定了

表1 机载软件工具鉴定准则

准则	适用性	
	开发工具	验证工具
只有确定性工具才能被鉴定	Y	Y
工具鉴定要基于指定的项目。对于工具是否要鉴定的声明要包含在PSAC中	Y	Y
除非能证明分区机制,联合工具应按照开发工具准则进行鉴定	Y	Y
软件构型管理和质量保证的目标适用于工具鉴定过程	Y	Y
工具鉴定过程需满足与使用工具的机载软件相同的目标	Y	N
通过试用期(试用期间,工具的输出被验证,工具的相关问题被记录、分析和纠正)表明对工具操作需求的符合性	Y	Y
在正常操作条件下,表明对工具操作需求的符合性	Y	Y
在鲁棒操作条件下,表明对工具操作需求的符合性	Y	N
基于需求的覆盖率分析	Y	N
工具鉴定结构覆盖率分析	Y	N
工具鉴定的鲁棒测试	Y	N
潜在错误分析	Y	N

表2 机载软件工具鉴定数据要求

数据名称	适用性		是否提交
	开发工具	验证工具	
软件合格审定计划(PSAC)	Y	Y	提交
工具鉴定计划(TQP)	Y	N	提交
工具操作需求(TOR)	Y	Y	可审查
软件完结综述(SAS)	Y	Y	提交
工具完结综述(TAS)	Y	Y	提交
工具验证记录(测试用例、规程、记录等)	Y	Y	可审查
工具开发数据(需求、设计、源代码等)	Y	N	可审查

机载软件工具的鉴定准则和数据要求,并根据是否在机载软件中引入错误对开发工具和验证工具的鉴定活动进行了区分。然而,整个过程中,没有考虑到机载软件工具应用于不同级别(A~D级)软件时,工具输出的重要程度。相信,在DO-178C的编制中将包含这个问题。

AST

参考文献

[1] RTCA. DO-178B software considerations in airborne systems and equipment certification[S]. Washington

DC, 1992.

[2] RTCA. DO-248B final report for clarification of DO-178B software considerations in airborne systems and equipment certification[S]. Washington DC, 2001.

[3] FAA. Order 8110.49 software approval guidelines[S]. Washington DC, 2003-6.

作者简介

刘建方,助理工程师,主要研究方向是机载软件管理。