使用先前开发机载软件的适航要求研究

Previously Developed Airborne Software Airworthiness Requirements Research

陈双／中国商飞上海飞机设计研究院

摘　要：先前开发的机载软件在民用航空领域获得了越来越广泛的使用，随之而来的适航问题也越发突出。本文结合国际相关指导性文件以及型号工作经验，对使用先前开发机载软件的适航要求进行研究和阐述。

关键词：先前开发机载软件；适航；DO-178B

Keywords：previously developed airborne software；airworthiness；DO-178B

1 先前开发机载软件的定义

目前，使用先前开发的软件是多数经验丰富的机载软件供应商的常规做法，特别是在对成熟产品进行改型时。先前开发机载软件是指在先前已经开发完成且随其他型号飞机取得过适航批准的机载软件项目，简称PDS。只要重新使用的软件在此之前是经过某型号审定的，则可将其定义为PDS。PDS的使用可以在一定程度上减少成本、缩短周期并降低风险，但从型号合格证审查的角度来说，所有的机载软件都必须符合DO-178B的要求。

2 使用先前开发软件的适航要求

使用PDS需考虑的问题包括：使用已更改的PDS、PDS安装在新的航空器环境上、PDS应用和开发环境变更、提高PDS的开发基线、软件构型管理和质量保证的考虑等。软件供应商如果希望使用PDS，则应在软件合格审定计划中明确说明。

2.1 使用已更改的PDS

PDS的更改原因大致可归纳为需

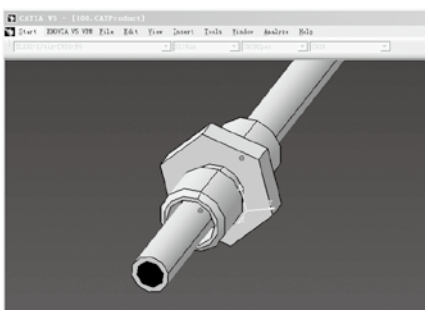

图4　添加了工作介质的管路装配件

中选择工作介质，完成后在设计树上选择所有管皮（管线不选），复制后粘贴到原始装配件中，删除原始装配件中的所有管线，如图4所示，工作介质此时已添加到了原始装配件中。

4 解决方案的验证

定制好专用材质库、管路库后，以此为基础进行液压能源系统设计，设计完成后，单击测量工具条（measure）测量惯量图标，光标变为一个卡尺状，左键单击设计树最上方零部件名称，弹出窗口，单击窗口下方三个按钮中间输出（Export）按钮，弹出对话框填写输出文件（.txt文件）的名称及存储路径后点击保存。用Excel打开文档，可以看到所有零件、装配件质量特性数据均已详实、准确列出。

5 结语

本文所述飞机液压能源系统装配件质量特性数据提取的解决方案是在充分研究了飞机液压能源系统构造及CATIA软件功能模块的基础上提出的，具有一定的创造性，采用这种方案可解决液压能源系统质量特性数据准确性差、质量属性数据提取工作效率低的问题，对从事飞机液压能源系统设计的人员可以提供一定的借鉴和帮助。 AST

参考文献

[1] 鲁君尚，等. 无师自通CATIA V5之装配设计与实时渲染[M]. 北京：北京航空航天大学出版社，2007.

[2] 宋静波.飞机构造基础[M].北京：航空工业出版社，2004.

[3] 飞机设计手册总编委.飞机设计手册[M]. 北京：航空工业出版社，1999.

作者简介

姜波，工程师，主要从事飞机液压系统设计研究工作。

求更改、错误更正和软件改进等，发生这些更改前统一都需要进行更改影响分析活动。

1）如果PDS的更改引起系统安全性评估文件的更改，则该文件及评估过程需要经过评审。

2）如果使用PDS，其软件等级进行了改变，需要考虑提升其开发基线。

3）分析软件需求及架构更改的影响，包括更改的软件需求对其他未更改的需求的影响以及对若干软件部件之间耦合的影响，都可能造成更改区域以外需要重新进行验证工作。

4）确定更改影响的区域，可通过数据流分析、控制流分析、时序分析及可追溯性分析等手段来完成。

5）确定更改影响的范围后，应以DO-178B第6章的相关内容为指导重新验证受更改影响的区域。

2.2 PDS安装在新的航空器环境上

将包含PDS的机载系统或设备安装在新的飞机上，最常见的情况是使用技术标准指令授权设备（TSOA），此类情况需要考虑三方面的要求。

1） 系统安全性评估过程要评估新航空器的安装环境，并确定软件等级与合格审定基础是否发生变化。如果与之前的机型相同，则不再要求完成其他的工作。

2） 如果安装在新机型上时需要更改功能或有其他方面的需求，则应参考使用已更改的PDS相关内容进行。此类情况多数需要重新申请TSOA。

3） 如果之前的软件开发活动的输出中无法证实能够满足新的安全性要求，则应参考提高PDS开发基线的相关内容进行。

2.3 PDS应用和开发环境变更

使用或更改PDS可能涉及到使用新的软件开发环境、新的处理器或其他硬件，以及与新的软件模块的集成。

1）如果新的开发环境引入了新的需要鉴定的软件工具，则应参考DO-178B第12.2节“工具鉴定”的相关指南。

2） 如果使用了不同的编译程序或编译选项，导致产生了不同的目标码，则PDS目标码相关的验证结果无效，需要重新进行验证。

3） 如果使用了新的处理器，则先前的软件/硬件接口验证结果不能在新的应用中使用，应重新执行软件/硬件集成测试，并重新进行软件/硬件兼容性的评审，甚至可能需要增加软件/硬件集成测试项目。

4） 将PDS用于不同的软件接口处时，则需要重新验证软件模块间接口。

2.4 提高PDS开发基线

如果PDS的生命周期资料是不充分的，无法满足新的安全性要求，需要考虑提升其开发基线。可能需要提升开发基线的软件包括：商用成品软件、非DO-178B标准下开发的机载软件（如之前以DO-178A为标准开发的软件）、按DO-178B标准开发但开发等级低于当前级别要求的软件。

提升开发基线的指南包括：

1） 主要使用先前已有的软件生命周期资料去满足DO-178B目标。

2） 基于系统安全性评估过程确定软件相关的失效状态和软件级别是否发生变化。

3） 为满足DO-178B的目标，可利用反向工程重新生成不充分或之前遗漏的软件生命周期资料。除此之外，可能需要增加一些验证活动以满足软件验证过程的目标。

4） 可以使用产品服务历史来满足DO-178B对提升开发基线的要求。

5） 申请人要在软件合格审定计划（PSAC）中明确定义出提升开发基线并能够符合DO-178B的方法，并与审查方就PSAC进行充分讨论以得到其认可和批准。

2.5 软件构型管理考虑

如果使用PDS，那么对新的整体软件而言，除了DO-178B第7章“软件构型管理”的指南外，软件构型管理过程还需包括：

1） 先前软件产品及其生命周期资料可追溯到新应用的软件。

2） 更改控制体系应确保问题报告机制有效。

2.6 软件质量保证考虑

如果使用PDS，那么对新的整体软件而言，除了DO-178B第8章“软件质量保证”的指南外，软件质量保证过程需确定在软件计划中定义了软件生命周期过程更改的情况。

3 结论

使用PDS的情况有很多种，其所对应的具体适航要求有所不同，在型号合格审定的适航工作中应注意区分PDS的服务历史，特别应注意应用在新型号飞机上的安全性影响和要求。在项目早期加强与软件供应商的沟通，确定PDS的生命周期数据，确认先前已完成工作的程度和证据，明确可以接受的符合性方法，并将上述内容反映在相应的软件合格审定计划中。此计划一旦与审查方达成一致，便可作为今后PDS符合性验证工作的基础。 AST

参考文献

[1] RTCA DO-178B Software Consideration in Airborne Systems and Equipment Certification[S]. 1992,12,16.

作者简介

陈双，助理工程师，主要从事飞机全机适航管理工作。