http://myfj.cnjournals.com myfj_sadri@comac.cc (021)20866796

DOI: 10.19416/j.cnki.1674-9804.2021.01.017

民机主制造商对 MBD 软件供应商工程监控过程研究

廖 凯*

(上海飞机设计研究院,上海 201210)

摘 要: 基于模型的软件开发技术(Model-Based Development, 简称 MBD)具有可视化建模与仿真、自动生成符合适航要求的代码等特点,已在民用飞机机载设备研发领域被逐渐推广应用。越来越多使用 MBD 技术开发的机载软件的涌现,给民机机载软件适航符合性工作带来了前所未有的挑战。为解决这一问题,美国航空无线电技术委员会于 2011 年底发布了 DO-178C 作为民用航空界认可的机载软件符合性方法,并在此基础上发布了 DO-331 作为专门针对机载软件 MBD 技术的适航符合性要求的补充说明。通过对 DO-178C 和 DO-331 标准中 MBD 软件适用目标的研究,结合工程实践,总结归纳了一套民用飞机主制造商对 MBD 软件供应商的软件研发过程管控要求,用于在向适航当局表明符合性时提高适航置信度,以期对主制造商和供应商在处理 MBD 软件方面提供参考。

关键词: 基于模型的开发(MBD);适航符合性;符合性方法;工程监控;置信度

中图分类号:TP311.5; V247 **文献标识码**: A **OSID**:

0 引言

民用飞机 MBD 软件指的是应用了基于模型开发技术的机载软件。MBD 技术在民用航空领域的应用,给机载安全关键设备供应商在嵌入式软件开发和验证工作上带来了巨大便利。图形化的建模和仿真、自动化的代码生成技术,无论从时间成本,还是人力投入方面来看,都能够为设备供应商大幅节约开支。在民用飞机机载软件适航符合性验证方面,美国航空无线电委员会(Radio Technical Commission for Aeronautics,简称 RTCA)于 2010 年发布了 DO-178C[1],作为指导机载系统嵌入式软件生命周期过程的指南性文件。在 2011 年又发布了 DO-331《基于模型的开发和验证(对于 DO-178C 和 DO-278A 的补充)》[2],进一步细化了对应用 MBD 技术开发的机载软件的目标要求。美国联邦航空局(Federal Aviation Administration,简称 FAA)在 2013 年通过发布咨询通告的形式,中国民用航空管理局(简称 CAAC)通过发布问题纪要的形式,先后认可了 DO-178C 和 DO-331 作为局方可接受的机载软件对适航审定基础的符合性方法。MBD 技术在国外已发展多年,已经在该技术的应用和支持工具的开发方面积累了较丰富的经验。而国内的 MBD 技术尚处在起步阶段,目前只有为数不多的研究所做了初步尝试,在适航符合性验证方面的经验欠缺。

1 MBD 软件开发技术概述

民用飞机机载系统中,嵌入式机载软件的占比正稳步提高并日趋复杂。软件开发的成本既包括设计和编码的成本,也包括验证的成本。传统方式设计的商用软件中每百万行代码中约有 100 个缺陷,通常缺陷中的 20% 是验证等级的,1% 是灾难等级的。相对于商用软件,安全关键系统的软件缺陷可能会少一个数量级,即每百万行代码中约有 20 个,

* 通信作者. E-mail: liaokai@comac.cc

引用格式: 廖凯. 民机主制造商对 MBD 软件供应商工程监控过程研究[J]. 民用飞机设计与研究,2021(1):106-110. LIAO K. Civil aircraft manufacturer-supplier engineering monitoring process on MBD software supplier[J]. Civil Aircraft Design and Research,2021(1):106-110(in Chinese).

因此,在安全关键系统的软件中,每百万行代码中平均每 5 个缺陷中就至少有 1 个是严重的。由于安全关键系统的生命周期可能会持续几十年,考虑到后期的维护、改造和升级费用,传统方式设计的软件成本几乎不可控。MBD 技术既能够保证系统安全性,又能适当降低设计的复杂度,并在项目早期发现软件缺陷,从而降低开发成本。

2　机载软件适航符合性过程和工程监控过程

2.1 机载软件适航符合性过程

目前国内外主流的民用飞机研发模式采用“主制造商-供应商”的模式,即由供应商提供机体结构和机载设备/系统,主制造商负责集成。

大型民用飞机的审定基础为 CCAR 25 部,其中机载软件作为机载设备产品的一部分,相关的适航条款为 CCAR25. 1301 和 CCAR25. 1309。2013 年,FAA 发布咨询通告 AC20-115C,认可 DO-178C 及其补充标准作为相关适航规章的符合性方法。CAAC 目前虽然尚未认可 DO-178C 作为符合性方法,但 DO-178C 及其补充标准中的部分要求以问题纪要的形式在某型客机项目上提出,并在机载软件研制过程中贯彻[3,5]。

为了评估机载软件研制过程对 DO-178C 及其补充标准、适用的问题纪要的符合性,审查方通常要对机载软件研制过程进行阶段适航符合性评审。FAA Order 8110. 49 Chg1[6]将适航符合性评审分为以下四个阶段:

1) 软件计划评审(SOI#1):软件计划评审的目的是评估软件的计划和标准是否满足 DO-178C 的要求并且按照研制过程的要求进行了内部评审和构型管理,以及质量保证人员对软件计划过程的监控。软件计划评审中,审查方还需评估当软件研制过程遵循软件计划和标准时,是否能满足 DO-178C 及其他适航要求;

2)软件开发评审(SOI#2):软件开发过程包括软件需求、设计、编码和集成过程以及对应的软件验证、构型管理、质量保证和适航联络等整体过程。软件开发评审的目的是评审上述过程的输出,以评估软件计划和标准在开发过程中的贯彻程度,以及输出对 DO-178C 及其他适航要求的符合性;

3)软件验证评审(SOI#3):软件验证过程包括评审、分析、测试等活动以及对应的软件验证、构型管理、质量保证和适航联络等整体过程。软件验证评审的目的是评估上述过程的输出,以评估软件计划和标准在验证过程中的贯彻程度,确保软件的需求、设计、编码进行了充分的验证,测试结果进行了评审和分析;

4)软件最终评审(SOI#4):软件最终评审是针对用于系统/设备审定的软件构型,确保软件生命周期过程完整,遵循了被批准的软件计划和标准,符合 DO-178C 及其他适航要求。同时,还要对 SCI、SAS 以及质量符合性评审记录进行评审。

2.2 机载软件工程监控过程

根据适航审定当局制定的适航符合性介入审查要求,民机主制造商应定义相应的工程监控过程,以国内某型飞机研制为例,可在软件生命周期过程中划分 4 次~5 次工程监控活动,由主制造商检查供应商的软件研发过程、活动和输出物是否符合适航要求。工程监控活动包括计划阶段评审、设计开发阶段评审、测试阶段评审和最终阶段评审,其中设计开发阶段可分为初步设计评审和详细设计评审两个阶段,分别检查软件的高级别需求和低级别需求。

3　主制造商对传统机载软件供应商工程监控

民用飞机机载软件采用 RTCA/DO-178C 作为符合性方法,主制造商可对供应商的软件研制过程进行一系列的工程评审,以监控供应商的软件研制过程对 RTCA/DO-178C 中目标的符合性。这些工程评审活动可包含软件计划阶段评审(Planning Process Review)、软件初步设计评审(Preliminary Design Review)、软件详细设计评审(Critical Design Review)、软件测试就绪评审(Test Readiness Review)和软件符合性评审(Software Conformity Review,简称 SCR)等。设计评审的介入由主制造商来决定,可以定义比上述评审活动更多的介入点,也可以定义更少的介入点,主要根据项目特点和工程监控的程度决定。主制造商对机载软件供应商的工程监控活动,不是适航符合性规章的要求,而是主制造商为控制项目风险对供应商进行的技术监控[7]。

4　主制造商对 MBD 软件供应商的工程监控

4.1 计划过程

MBD 软件除满足 RTCA/DO-178C 计划阶段要求外，还应满足 DO-331 中的目标 A1.5 要求（见表 1），需要编制软件模型标准，规范机载软件建模准则、方法、工具、流程等[4,8]。软件计划阶段还应该满足下列要求：

1）在软件计划文件中清晰地描述了哪些软件模块采用基于模型开发和验证技术；

2）采用哪种模型（规范模型或设计模型）以及在什么需求层级上应用；

3）与传统开发的软件模块如何集成、接口如何验证；

4）采用哪些模型开发和验证工具，是否需要鉴定以及获得的适航置信度；

5）对问题纪要或其它审定要求的符合性计划。

表 1　MBD 软件计划过程要求

条款	目标		活动	各软件级别的适用性				输出	
	描述	参考	参考	A	B	C	D	数据项	参考
A1.5	软件开发标准已定义	MB.4.1.e	MB.4.2.b MB.4.2.g MB.4.5	○	○	○		软件需求标准 软件设计标准 软件编码标准 软件模型标准	11.6 11.7 11.8 MB.11.23

4.2 开发过程

MBD 软件应满足 DO-178C 开发阶段要求外，还应满足目标 A2. MB8、A2. MB9 和 A2. MB10 要求（见表 2）。软件开发阶段还应该满足下列要求：

1）按照软件计划文件中描述开发软件；

2）软件模型经过评审并正式受控；

3）软件模型符合软件建模标准；

4）软件模型和上层需求建立双向追溯关系；

5）识别衍生模型（即无法与上层需求建立追溯关系）；

6）软件模型是否按照自动生成代码工具生成源代码；

7）自动生成代码和手写代码是否完成集成活动；

8）模型开发工具鉴定活动是否已经完成。

表 2　MBD 软件开发过程要求

条款	目标		活动	各软件级别的适用性				输出	
	描述	参考	参考	A	B	C	D	数据项	参考
A2. MB8	标识出不用于实现任何高级别需求的规范模型元素	MB.5.1.1.c	MB.5.1.2.k	○	○	○	○	软件需求数据	MB.11.9
A2. MB9	标识出不用于实现任何软件架构的设计模型元素	MB.5.2.1.c	MB.5.2.2.h	○	○	○	○	设计描述	MB.11.10
A2. MB10	标识出不用于实现任何低级别需求的设计模型元素	MB.5.2.1.c	MB.5.2.2.h	○	○	○		设计描述	MB.11.10

4.3 验证过程

在 MBD 软件的验证过程中,除需满足 DO-178C 验证阶段要求外,还应满足 DO-331 中的目标 A3. MB8、A3. MB9、A3. MB10、A4. MB14、A4. MB15、A4. MB16、A7. MB10、A7. MB11 和 A7. MB12 要求(见表 3)。软件验证阶段还应该满足下列要求:

1)按照软件计划文件中的描述验证软件;

2)软件模型、测试用例/程序、测试结果建立了双向追溯关系;

3)验证了衍生模型;

4)模型仿真活动及仿真结果,模型覆盖率分析结果;

5)完成了模型验证工具鉴定活动。

表 3　MBD 软件验证过程要求

条款	目标		活动	各软件级别的适用性				输出	
	描述	参考	参考	A	B	C	D	数据项	参考
A3. MB8	仿真用例是正确的	MB. 6. 8. 3. 2. a	MB. 6. 8. 1 MB. 6. 8. 3. 2	●	○	○	○	软件验证结果	MB. 11. 14
A3. MB9	仿真程序是正确的	MB. 6. 8. 3. 2. b	MB. 6. 8. 1 MB. 6. 8. 3. 2	●	○	○	○	软件验证结果	MB. 11. 14
A3. MB10	仿真结果是正确的,且差异得以解释	MB. 6. 8. 3. 2. c	MB. 6. 8. 1 MB. 6. 8. 3. 2	●	○	○	○	软件验证结果	MB. 11. 14
A4. MB14	仿真用例是正确的	MB. 6. 8. 3. 2. a	MB. 6. 8. 1 MB. 6. 8. 3. 2	●	○	○		软件验证结果	MB. 11. 14
A4. MB15	仿真程序是正确的	MB. 6. 8. 3. 2. b	MB. 6. 8. 1 MB. 6. 8. 3. 2	●	○	○		软件验证结果	MB. 11. 14
A4. MB16	仿真结果是正确的,且差异得以解释	MB. 6. 8. 3. 2. c	MB. 6. 8. 1 MB. 6. 8. 3. 2	●	○	○		软件验证结果	MB. 11. 14
A7. MB10	仿真用例是正确的	MB. 6. 8. 3. 2. a	MB. 6. 8. 3. 2.	●	○	○		软件验证结果	MB. 11. 14
A7. MB11	仿真程序是正确的	MB. 6. 8. 3. 2. b	MB. 6. 8. 3. 2.	●	○	○		软件验证结果	MB. 11. 14
A7. MB12	仿真结果是正确的,且差异得以解释	MB. 6. 8. 3. 2. c	MB. 6. 8. 3. 2.	●	○	○		软件验证结果	MB. 11. 14

4.4 构型管理和质量保证过程

MBD 软件构型管理、质量保证和审定联络过程与 DO-178C 要求一致,没有额外目标[9]。

软件构型管理过程贯穿整个软件生命周期,主要目的是对软件构型项进行标识和控制。软件构型管理过程的主要活动包括构型标识、基线和追溯性、问题报告/更改控制/更改评审、构型纪实、归档/检索/发布、软件生命周期环境控制等几个方面。软件构型管理过程的输出主要是构型管理记录。

软件质量保证过程贯穿整个软件生命周期,主要目的是通过质量保证人员的评审、审核、目击、检查等方法确保软件的实际研制过程遵循被批准的软件计划和标准[10]。软件质量保证过程的输出是质量保证记录。

5　结论

对于使用了 MBD 技术开发机载软件的供应商,主制造商应以 DO-178C 为基础,综合考虑对 DO-178C 和 DO-331 中目标的符合性。本文以民用飞机适航符合性过程为出发点,通过机载软件适航符合

性验证过程引出主制造商对供应商软件的工程监控,并基于 MBD 软件相较于传统机载软件的特殊性,导入了对 MBD 软件的工程监控过程要求。本文总结的主制造商对 MBD 软件供应商的工程监控过程要求,对国内民机主制造商在处理使用 MBD 技术开发机载设备/系统的嵌入式软件的适航符合性验证活动时具有参考价值。

参考文献:

[1] Radio Technical Commission Aeronautics. Software considerations in airborne systems and equipment certification: DO-178C[S]. Washington DC: Radio Technical Commission Aeronautics,2011.

[2] Radio Technical Commission Aeronautics. Model-based development and verification supplement to DO-178C and DO- 278A: DO-331[S]. Washington DC: Radio Technical Commission Aeronautics,2011.

[3] 陈勇, 严林芳, 孙景华. 民用飞机机载软件管理[M]. 北京: 航空工业出版社, 2015: 31-32.

[4] 居慧. RTCA/DO-331 标准研究[J]. 民用飞机设计与研究, 2018(3): 118-123.

[5] 童岳威, 孙景华. 民用飞机机载软件基于模型开发及工具鉴定研究[C]//中国航空学会.第五届民用飞机航电系统国际论坛论文集. 北京: 中国科学技术出版社,2016:460-464.

[6] Federal Aviation Administration. Software approval guidelines: ORDER 8110. 49 CHG1[S]. Washington DC: Federal Aviation Administration,2011.

[7] 吴海燕, 陈振兴. 民用飞机机载软件适航方法的研究[J]. 大众科技, 2014, 16(7): 102-103;109.

[8] 邢亮, 牟明. DO-178B/C 目标分析及阶段介入评审过程研究[J]. 航空计算技术, 2015, 45(5): 97-101.

[9] 申岳, 蔡喁. 民用机载软件的发展及适航相关考虑[C]//中国航空学会.第五民用飞机航电系统国际论坛论文集. 北京: 中国科学技术出版社,2016:476-480.

[10] 郑军, 黄志球, 徐丙凤. 机载软件适航认证标准新进展及展望[J]. 计算机工程与设计, 2012, 33(1): 204-208.

作者简介

廖　凯　男,硕士,工程师。主要研究方向:民用飞机机载系统软件符合性验证。E-mail: liaokai@comac.cc

Civil aircraft manufacturer-supplier engineering monitoring process on MBD software supplier

LIAO Kai *

(Shanghai Aircraft Design and Research Institute, Shanghai 201210, China)

Abstract: Software model-based development technology has been widely used in civil aviation airborne equipment area because of its convenience of visual modeling and simulation, automatic code generation and so on. More and more airborne software developed by MBD technology has brought significant challenges to the airworthiness compliance of civil aircraft on software. In order to solve this problem, at the end of 2011, the American Aeronautical Radio Technical Committee issued DO-178C as an airborne software compliance method recognized by the civil aviation industry, and on this basis, it issued DO-331 as a supplement to the airworthiness compliance requirements of airborne software MBD technology. Based on the research of MBD objectives in DO-178C and DO-331 standards, combined with engineering practice, this paper summarizes a set of engineering monitoring process requirements of main civil aircraft manufacturers for using MBD technology to develop embedded software suppliers of airborne equipment, which helps to improve airworthiness confidence, so as to provide reference for main manufacturers and suppliers in processing MBD software.

Keywords: model based development (MBD); airworthiness compliance; meanings of compliance; engineering surveillance; airworthiness confidence

* Corresponding author. E-mail: liaokai@comac.cc