# 航空机载软件适航性审定标准DO-178C与软件管理标准GJB5000A的比较分析

李超[1],黄百乔[2*]

**1. 中国民航科学技术研究院,北京 100028**
**2. 中国船舶工业系统工程研究院,北京 100036**

**摘要**　航空机载软件适航性审定是验证软件安全性是否满足飞行要求的重要手段,审定依据的标准DO-178C是航空企业软件设计所必须遵循的规范要求,但在软件管理领域,还存在着重要的能力成熟度集成模型标准GJB5000A。比较分析了DO-178C与GJB5000A的异同,得出机载软件适航性审定在对软件开发过程的管理方面存在不足,提出需要加强企业在项目监控、过程测量与分析和风险管理方面的要求,并按照DO-178C标准的形式要求,给出了参考的改进方案。

**关键词**　DO-178C;CMMI;GJB5000A;机载软件适航性审定

自20世纪60年代爆发“软件危机”以来,人们在不断寻找着能够解决软件危机的“银弹”。1968年,“软件工程”概念的提出是软件开发史上一次大的飞跃,使软件开发开始了从“艺术”、“技巧”和“个体行为”向“工程”和“群体协同工作”转化的历程[1]。在软件工程的发展历程中,国际航空无线电技术委员会(Radio Technical Commission for Aeronautics,RTCA)的DO-178C标准占有非常重要的地位,该标准称作“机载系统和设备合格审定中的软件考虑”。为了规范机载软件研制过程中的安全性设计与验证过程,1982年,美国航空无线电委员会(RTCA)组织了SC-145特殊委员会,即“数字航空软件”委员会,开发和编制了一个面向民航领域的软件研制与验证的标准,即DO-178标准[2],并分别于1985年、1992年和2011年对该标准进行了修订,目前中国广泛采用的是1992年颁布的DO-178C版本,而2011年发布的最新版DO-178C[3]除了继承DO-178B的核心内容外,还增加了基于模

收稿日期:2020-07-02;修回日期:2020-09-18

作者简介:李超,工程师,研究方向为人力资源管理、适航性审定,电子信箱:lichao0726@163.com;黄百乔(通信作者),高级工程师,研究方向为系统工程,电子信箱:seafury@buaa.edu.cn

引用格式:李超, 黄百乔. 航空机载软件适航性审定标准DO-178C与软件管理标准GJB5000A的比较分析[J]. 科技导报, 2020, 38(21): 187-191; doi: 10.3981/j.issn.1000-7857.2020.21.023

型的开发和验证、面向对象编程和形式化方法的支持,是对软件开发技术发展的与时俱进的适应性改进。

DO-178C标准借鉴了制造业中通过控制和改进工艺流程来提高产品质量的思想,通过规范的开发过程来提高软件开发的质量,通过对过程目标的验证来检验软件的质量。这与产生于同一时期的另一个系统设计领域的标准CMMI有异曲同工之处。CMMI标准最早产生于软件领域,称作SW-CMM(software capability maturity model)标准,即软件能力成熟度模型,最早在1987年由美国软件工程研究所(SEI)提出,随着SW-CMM的成功,在其他领域也相继推出了类似的模型,如系统工程能力成熟度模型(SE-CMM)、集成产品和过程开发能力成熟度模型(IPPD-CMM)和人员能力成熟度模型(P-CMM)等。SEI整合了SW-CMM、IPPD-CMM与SE-CMM,开发出了集成能力成熟度模型CMMI[4],应用于整个系统的设计,不仅适用于软件,目前已发展到1.3版本[5]。为提升中国军用软件的研发质量,在CMMI1.2版本的基础上,结合中国军用软件研制过程特点,中国发布了GJB5000A《军用软件能力成熟度模型》标准[6],用于规范军用软件承研单位的软件研制过程。

DO-178C标准与CMMI标准在规范软件研制过程、提高软件研制质量方面都发挥了重要作用。二者具有一致的核心思想,但又各有特色。其中DO-178C标准主要面向民用机载软件领域,侧重于软件安全性设计与验证,因此它在验证和确认方面有详细的严格的要求。另外DO-178C也并不是一个孤立的标准,它是一个标准族,与ARP4754、ARP4761、DO-254一起构成了现代航空机载系统(特别是高度综合和复杂系统)安全性设计与评估的一组指导材料。而GJB5000A标准是面向所有软件领域的通用标准,它适合所有类型的软件开发组织的软件研制过程。GJB5000A最根本上是一个过程改进模型,致力于促进组织的软件研制过程的能力不断提升。组织建立自身的质量管理体系文件趋向于综合不同标准间形成"one book",因此关于不同质量标准之间的比较分析也是质量管理领域的研究方向[7-10]。通过对2个适航审定标准的要点进行对比,分析各自的适用范围和优缺点,以期对机载软件审定过程提出完善建议,并按照DO-178C标准中审定要求的形式给出修改的参考方案,实现DO-178C和GJB5000A的融合。软件的质量既是设计出来的,也是管理出来的。鉴于此,本文提出机载软件审定过程的修改建议,给出参考的修改方案,体现DO-178C与GJB5000A的融合。

## 1 DO-178C与GJB5000A要点分析

### 1.1 DO-178C标准要点

DO-178C标准规范了软件开发生命周期模型,为软件工程中经典的瀑布模型,即将开发过程分为软件需求过程、软件设计过程、软件编码过程、软件集成过程和软件验证过程。并提出了每个过程需要达成的目标,共66项。该标准按照软件失效影响的严重程度,将软件分为致命(A)、危险(B)、重要(C)、一般(D)和无影响(E)5个等级,软件等级从低到高,对于过程目标有增量的要求,其中A级软件需达成完整的66项目标。在审定时,对于目标的验证要求又分为一般验证与独立验证,其中独立验证是指不由被审方自己提供证据,而由审核方独立进行验证。基于上述特点,DO-178C的审核要求就构成了以不同软件等级、不同过程目标和不同验证要求组成的矩阵表[3]。

DO-178C是一个侧重于软件安全性设计与验证的标准。一方面,本标准的上一级指导为ARP4761标准,全称为《民用机载系统和设备安全性评估过程的指南和方法》,用于指导系统安全性分析的指导,分析的结果将分配到软件的安全性要求中,作为软件安全性需求的来源;另一方面,在本标准软件需求过程的目标要求中,也是侧重系统向软件分配的安全性需求的追踪与落实。特别是标准的6.4在软件测试过程中要求对代码结构的覆盖分析,不仅是对软件代码本身,还需要对软件代码编译后形成的目标代码进行结构覆盖分析。这是一项特别底层、特别基础的工作,对编程语言和编译环境有非常严格的要求,一些高级编程语言在编

译目标码时会引入很多外部库文件内容,会给目标代码的结构覆盖分析带来很大的技术难题,因此一般不建议使用。

DO-178C标准在软件管理方面是较弱的,主要由软件计划过程、软件配置管理过程和软件质量保证过程3个过程组成。虽然在软件质量保证过程的要求描述中提到了对软件计划的偏离的记录与监督,但并未如GJB5000A中要求的那样,软件计划、过程测量和过程监控之间形成过程控制的反馈回路,在标准附件1中的具体审定要求中也未明确提出审核要求。另外对于项目执行过程中的风险管理DO-178C标准也未提及。以上几点分析显示出DO-178C在软件过程管理方面存在重视不够的问题。作为航空机载软件的适航性审定来说,除了目的导向,确保软件安全性之外,也应该通过审定过程,查找被审单位的软件开发过程管理是否规范,是否能对软件安全性有持续性的保障。

### 1.2　GJB5000A标准要点

GJB5000A标准其实质是一个软件开发过程改进模型,致力于软件开发组织的过程改进。它把软件开发组织的软件开发能力分为5个等级:初始级、已管理级、已定义级、已定量管理级和优化级,并为软件开发组织提供了一个不断提高自身管理水平,提升组织能力成熟度层级的路线图。首先,在已管理级,通过建立基本的软件过程管理反馈循环来提升组织对软件开发过程的控制能力,如图1所示。通过项目策划、测量分析与项目监控3个过程域,构建一个及时的反馈控制闭环,来不断修正软件开发过程,通过过程控制来提高软件开发质量。然后,在已定义级通过规范软件工程过程,加入了需求开发、技术解决方案、产品集成、验证与确认等工程过程域构建了软件开发组织完整的软件开发与管理过程。同时已定义级也增加了组织级过程域,包括组织过程焦点与组织过程定义,配合过程改进组(EPG)来开展组织过程改进活动。在已定量管理级通过定量项目管理与组织过程性能2个过程域,强调全面的定量化管理,以支持组织过程改进,以致到优化级建立完善的组织内部过程改进机制,不断发动提升组织过程达到优化能力等级。GJB5000A标准的核心思想体现为2点,一是通过规范的过程来提升产品质量,二是通过组织内部不断的过程改进行为来提升过程的质量。这2点都体现了过程管理的重要性,产品质量是设计出来的,同时也是管理出来的。

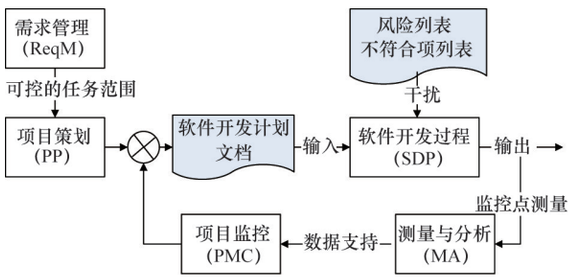


图1　CMMI二级软件管理闭环过程示意

## 2　DO-178C与GJB5000A的比较

对GJB5000A的分析可知,达到GJB5000A已定义级便构建好了组织内完整的软件设计与管理流程,已定量管理级和优化级主要用于组织内过程管理能力提升。因此将DO-178C标准的条款要求与GJB5000A已定义级要求中与软件研制相关的工程与管理过程域要求进行了比较,结果如表1所示。

通过比较分析可得,DO-178C是一个以确保软件安全性为目标的软件设计标准,侧重于软件安全性需求的追踪与验证,但与GJB5000A相比,在软件开发过程管理上存在较大不足,该标准只涉及软件开发计划一个管理活动,而计划中也未涉及风险管理计划与利益相关方参与计划等影响软件开发过程的重要活动计划。对于软件研制过程与软件计划之间的符合性监控,标准中虽有提及,但在附录A的审查要求中并未强调,可以认为,相较于GJB5000A,DO-178C在过程管理上重视不够。而只有让软件开发组织在软件研制能力上提升了,才能从根本上确保软件的质量与安全性,因此有必要在现有DO-178C中关于审定要求的基础上,增加对被审单位软件管理活动的审核,确保被审单位不仅有合格的产品,还有合格的管理过程。为此,对现有机载软件适航性审定要求提出改进建议。

表1 DO-178C与GJB5000A比较结果

| DO-178C(标准条款) | GJB5000A(过程域) | 比较结论 |
|---|---|---|
| 3.0:软件生命周期<br>4.0:软件计划过程 | 项目策划(PP) | 对于软件计划过程,GJB5000A有更详细要求 |
| 5.1:软件需求过程 | 需求开发(RD) | GJB5000A为通用要求,DO-178C侧重于安全性需求的分配与追踪 |
| 5.2:软件设计过程<br>5.3:软件编码过程 | 技术解决方案(TS) | GJB5000A为通用要求,DO-178C侧重于安全性需求的设计与实现 |
| 5.4:软件集成过程 | 产品集成(PI) | 基本一致 |
| 5.5:可追踪性 | 需求管理(ReqM) | GJB5000A除了强调追踪性外,还强调需求变更的管理 |
| 6.0:软件验证过程 | 验证(Ver)<br>确认(val) | DO-178C对验证测试有更详细的要求,如对目标码的结构覆盖分析,这属于DO-178C特有 |
| 7.0:配置管理<br>11.0:软件生命周期资料 | 配置管理(CM) | 基本一致 |
| 8.0:质量保证 | 过程和产品质量保证(PPQA) | GJB5000A要求更详细 |
| 9.0:合格审定联络过程<br>10.0:航空器或发动机合格审定综述<br>12.0:其他考虑 | — | 对软件审定过程的要求,不属于软件开发过程 |
| — | 项目监控(PMC) | DO-178C缺少由项目计划、测量分析与项目监控构建的管理反馈闭环,缺少风险管理 |
| — | 测量分析(MA) | |
| — | 风险管理(RskM) | |
| — | 供方管理(SAM) | |

## 3 对软件适航性审定要求的改进建议

针对DO-178C标准缺少对项目监控、测量与分析以及风险管理过程域内容的要求,在软件计划过程的检查项中增加相关内容(表2)。在软件质量保障检查项中增加对项目监控、项目测量与分析及项目风险管理的内容(表3),以确保被审定组织的软件设计与管理过程的规范性。通过增加测量分析过程(MA)与项目监控过程(PMC)的计划和执行检查,构建由项目计划、测量与分析及项目监控形成的管理反馈闭环(图1),同时将项目管理中必要的风险管理引入,以提升组织的项目管理能力。

表2 软件计划过程

| | 目标 | | 软件等级适用性 | | | | 输出 | | 软件等级的控制类 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 说明 | 参考 | A | B | C | D | 说明 | 参考 | A | B | C | D |
| 前7项(原有) | 协调软件计划等前7项要求 | 4.1 g<br>4.6 | ○ | ○ | ○ | | SQA记录<br>软件验证结果 | 11.19<br>11.14 | ② ② | ② ② | ② ② | |
| 8(新增) | 编制项目监控计划 | 4.1 h | ○ | ○ | ○ | ○ | 项目监控计划 | | ② | ② | ② | ② |
| 9(新增) | 编制测量与分析计划 | 4.1 h | ○ | ○ | ○ | ○ | 测量与分析计划 | | ② | ② | ② | ② |
| 10(新增) | 制定风险管理计划 | 4.1 i | ○ | ○ | ○ | ○ | 项目风险清单 | | ② | ② | ② | ② |

表3 软件质量保证过程

| | 目标 | | 软件等级适用性 | | | | 输出 | | 软件等级的控制类 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 说 明 | 参考 | A | B | C | D | 说 明 | 参考 | A | B | C | D |
| 前3项(原有) | 是否进行了软件综合性评审 | 8.1 c<br>8.3 | ● | ● | ● | ● | SQA记录 | 11.19 | ② | ② | ② | ② |
| 4(新增) | 是否按计划定期对软件开发过程与产品属性进行测量与分析 | 8.2 d | ● | ● | ● | ● | SQA记录 | 11.19 | ② | ② | ② | ② |
| 5(新增) | 是否按计划定期监控软件开发计划执行,必要时调整计划 | 8.2 d | ● | ● | ● | ● | SQA记录 | 11.19 | ② | ② | ② | ② |

## 4　结论

分析了软件质量管理领域重要的2个标准：DO-178C与GJB5000A的特点，并通过对二者要求的对比分析，指出了DO-178C标准在软件开发过程管理上存在的不足之处，包括缺少由项目计划、项目测量与分析以及项目监控过程构建的管理反馈闭环，缺少风险管理过程。为使软件适航性审定工作既能达到授人鱼又能达到授人以渔的目的，提出了改进方案，在软件计划过程与软件质量保证过程审核条款中增加相应内容。为航空企业基于DO-178C编制的质量管理文件的改进提供了参考。

### 参考文献(References)

[1] 杨芙清. 软件工程技术发展思索[J]. 软件学报, 2005, 16(1): 1-7.

[2] 李迅, 杨朝旭, 付泱. 浅析DO-178C标准在航空机载软件开发商的应用及发展[C]//中国航空学会控制与应用第十二届学术年会论文集. 北京: 中国航空学会, 2006: 467-471.

[3] RTCA DO-178C. Software Considerations in Airborne Systems and equipment Certification[S]. 2011.

[4] 黄凌凡. 军用软件能力成熟度模型(CMM)二级评估的项目管理研究[D]. 上海: 上海交通大学, 2010.

[5] CMMI. Capability maturity model integration version 1.3 [S]. Pittsburgh: SEI Administrative Agent, 2010.

[6] 闫宇华, 王黎明, 宋太亮, 等. 军用软件研制能力成熟度模型: GJB 5000A—2008[S]. 北京: 中国人民解放军总装备部, 2008.

[7] 刘煜, 尤海峰. GJB5000A与DO-178C的结合实施方案[J]. 计算机应用, 2013, 33(S1): 255-258.

[8] 王金林, 牟明, 邢亮. GJB5000A与DO-178B/C的综合应用研究[J]. 航空计算技术, 2015, l45(1): 100-107.

[9] 刘治学. GJB5000A与GJB9001B过程改进的研究[J]. 航空标准化与质量, 2013(1): 46-48.

[10] 袁晓军, 王绮卉. GJB5000A与DO-254差异分析[J]. 航空计算技术, 2018, l48(4): 130-134.

# Comparative analysis of for airborne systems and equipment certification standard DO-178C and software management standard GJB5000A

LI Chao[1], HUANG Baiqiao[2*]

1. Human Resources Development Center of Civil Aviation China, Beijing 100028, China

2. Systems Engineering Research Institute, China State Shipbuilding Corporation Limited, Beijing 100036, China

**Abstract**　Aviation airborne software airworthiness certification is an important means to verify that the safety of software meets flight requirements. The certification standard DO-178C is a standard requirement that aviation enterprise software design must follow. However, in the field of software management there is an important competence maturity integration model standard, called CMMI/GJB5000A. After a comparative analysis of DO-178C and GJB5000A, it is concluded that the airborne software airworthiness certification is insufficient in the sense of software development process management. To meet the gap it is proposed that enterprises need to strengthen project monitoring, process measurement, analysis and risk management requirements. In accordance with the formal requirements of DO-178C, a reference improvement plan is given.

**Keywords**　DO-178C; CMMI; GJB5000A; software considerations in airborne systems and equipment certification

（责任编辑　徐丽娇）