

文章编号: 1674-8190(2021)06-161-06

基于 DO-178C 的机载软件质量保证与管理

周培

(中航雷华柯林斯(无锡)航空电子设备有限公司 质量适航部, 无锡 214063)

摘要: DO-178C 作为机载软件适航可接受的符合性标准, 明确要求机载软件综合过程中必须包含软件质量保证(SQA)过程。以机载软件的软件生命周期定义、过程和数据为基础, 从目标、活动和符合性评审三个方面分析基于 DO-178C 的软件质量保证过程的实施; 结合软件项目质量管理技术和工具, 从规划软件质量管理、管理软件质量和控制软件质量三个过程研究基于 DO-178C 的软件质量管理方法并给出工程实践建议。结果表明: 本文将软件质量保证与质量管理紧密结合, 形成了适航要求的相关证据, 提供了符合需求的民用机载软件, 有效保证了机载软件的质量和持续改进措施。

关键词: DO-178C; 机载软件; 质量保证; 质量管理; 适航

中图分类号: V247; V328.3; TP311.5

DOI: 10.16615/j.cnki.1674-8190.2021.06.20

文献标识码: A

开放科学(资源服务)标识码(OSID):



Airborne Software Quality Assurance and Management Based on DO-178C

ZHOU Pei

(Quality, Lean & Certificate Department, AVIC Leihua Rockwell Collins Avionics Company, Wuxi 214063, China)

Abstract: DO-178C as an acceptable compliance standard for airborne software airworthiness, it is clearly required that the software quality assurance (SQA) process must be included in the airborne software integration process. Based on the software life cycle definition, process and data of airborne software, the implementation of the software quality assurance process is analyzed from three aspects of objectives, activities, and compliance review based on DO-178C. In combination with software project quality management techniques and tools, the DO-178C-based software quality management method is studied from the three processes of software quality management planning, software quality management and software quality control, and some practical engineering suggestions are given. The results show that, by combining software quality assurance and quality management, the evidence of airworthiness requirements are generated, the civilian airborne software meeting the requirements is provided, and the quality and continuous improvement measurement are effectively ensured.

Key words: DO-178C; airborne software; quality assurance; quality management; airworthiness

收稿日期: 2020-12-11; 修回日期: 2021-04-13

通信作者: 周培, 993735244@qq.com

引用格式: 周培. 基于 DO-178C 的机载软件质量保证与管理[J]. 航空工程进展, 2021, 12(6): 161-166.

ZHOU Pei. Airborne software quality assurance and management based on DO-178C[J]. Advances in Aeronautical Science and Engineering, 2021, 12(6): 161-166. (in Chinese)

0 引言

随着民用机载软件的功能、种类和规模日益增长,对软件适航的相关要求、方法和技术也不断提高。DO-178C《机载系统和设备合格审定中的软件考虑》^[1]于 2011 年正式发布,作为 1992 年的 DO-178B^[2]的升级,除了在错误与不一致、术语一致、措辞改进等方面进行修订之外,主要在目标与活动、补充、工具鉴定、协调系统与软件层面等方面进行了更新与改进^[3-4]。DO-178C 作为机载软件适航可接受的符合性标准,明确要求机载软件综合过程中必须包含软件质量保证(SQA)过程。

国内,各军民用软件研制单位都在积极开展软件质量保证工作,常采用 GJB 5000A^[5]+DO-178C 的模式。基于 GJB 5000A 的软件质量保证与质量管理研究较多^[6-9],但 GJB 5000A 未明确说明软件质量保证过程的过渡准则。而美国航空无线电技术委员会(RTCA)颁布的 DO-178C 仅提出相关目标和指南性描述,并未具体说明产生适航要求的质量数据方法^[10-11]。

本文从软件生命周期的定义、过程和数据出发,首先探讨实施软件质量保证的原因和必要性;其次基于 DO-178C 软件质量保证过程的目标、活动和符合性评审三个方面分析该过程的实施;最后结合软件项目质量管理技术和工具,从规划软件质量管理、管理软件质量和控制软件质量三个过程探究基于 DO-178C 的软件质量管理方法并给出工程实践建议。

1 软件生命周期

1.1 软件生命周期定义

一个项目的通过为每个过程选择活动,为活动指定顺序,并为活动分配职责来定义一个或多个软件生命周期。项目属性决定了过程顺序,软件开发过程的通常顺序是需求、设计、编码和集成^[12]。

软件生命周期的过程可能是迭代的,也就是输入和重新输入。迭代的时间和程度因系统功能的增量开发、复杂性、需求开发、硬件可用性、对先前过程的反馈以及项目的其他属性而变化。所选软件生命周期的各个部分通过增量集成过程和软

件验证过程活动的组合联系在一起。

1.2 软件生命周期过程

DO-178C 的软件生命周期过程包含以下四个方面。

(1) 软件计划过程 (Software Planning Process, 简称 SPP)^[12]。

(2) 软件开发过程 (Software Development Process, 简称 SDP)。该过程输出软件产品,分为需求、设计、编码和集成四个过程^[13]。

(3) 软件综合过程 (Software Integration Process, 简称 SIP)。该过程分为验证、配置管理、质量保证和审定联络四个过程^[14]。综合过程与开发过程在整个软件生命周期并行。

生命周期过程之间的关系如图 1 所示,可以看出:软件质量保证过程是软件综合过程中必不可少的一部分。

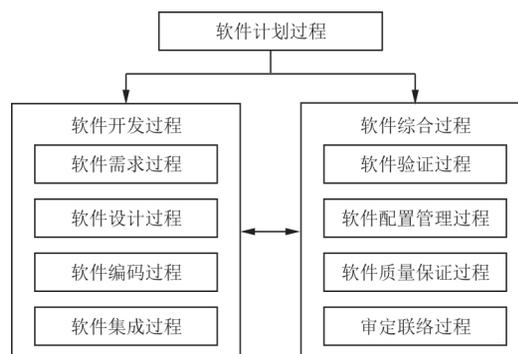


图 1 DO-178C 的软件计划、开发与综合过程的关系
Fig. 1 Relationship between software planning, development and integration process of DO-178C

1.3 软件生命周期数据

软件生命周期过程会生成软件生命周期数据,这些数据是机载软件产品的表现形式,也是软件生命过程的记录,更是软件适航取证的基本依据^[15]。软件生命周期过程所产生的软件生命周期数据如图 2 所示,其中 5 大计划包括软件开发计划(SDP)、软件验证计划(SVP)、配置管理计划(SCMP)、质量保证计划(SQAP)和软件审定计划(PSAC)^[14];3 大标准包括软件需求标准(SRS)、软件设计标准(SDS)和软件编码标准(SCS)。软件质量保证计划用以指导软件质量保证过程的工作开展。

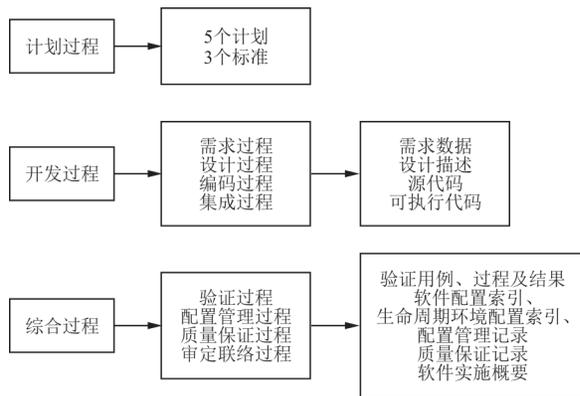


图 2 DO-178C 的软件生命周期数据
Fig. 2 Software life cycle data of DO-178C

2 基于 DO-178C 的软件质量保证过程

DO-178C 明确要求确保软件质量保证(SQA)过程。SQA 过程根据软件规划过程和软件质量保证计划的定义进行应用。SQA 过程活动的输出记录在软件质量保证记录或其他软件生命周期数据中。

SQA 过程评估软件生命周期过程及其输出, 以确保目标得到满足, 缺陷得到检测、评估、跟踪和解决, 软件产品和软件生命周期数据符合取证要求^[16]。

2.1 软件质量保证过程目标

SQA 过程目标通过确保这些过程按照已批准的软件计划和标准执行, 为软件生命周期过程产生符合其需求的软件坚定了信心。

SQA 过程的目标是确保下述流程。

- (1) 开发和审查软件计划和标准, 以符合 DO-178C 并保持一致性。
- (2) 软件生命周期过程符合已批准的软件计划和标准。
- (3) 满足软件生命周期过程的转换标准。
- (4) 对软件产品进行符合性评审。

2.2 软件质量保证过程活动

为满足 SQA 过程目标: SQA 过程应在软件生命周期过程的活动中发挥积极作用, 并使那些执行 SQA 过程的人具有权力、责任和独立性, 以确保 SQA 过程目标得到满足; SQA 过程应保证软件计划和标准的制定与评审的一致性; SQA 过程应确保软件生命周期过程符合批准的软件计划和标

准; SQA 过程应确保软件生命周期过程的过渡准则已符合批准的软件计划; SQA 过程应确保软件生命周期数据按照控制类别进行控制; 在交付作为取证申请一部分提交的软件产品之前, 应进行软件符合性审查; SQA 过程应产生 SQA 过程的记录, 包括作为取证申请的一部分提交的每个软件产品的审核结果和完成软件符合性评审的证据; SQA 过程应提供供应商过程和输出符合已批准的软件计划和标准的保证。

SQA 过程应包括在软件生命周期内对软件开发和集成过程的审核, 以确保:

- (1) 软件计划有效。
- (2) 对软件计划和标准的偏差进行检测、记录、评估、跟踪和解决。一般认为过程偏差的早期检测有助于有效实现生命周期过程目标。
- (3) 记录已批准的偏差。
- (4) 软件开发环境已按照软件计划的规定提供。
- (5) 问题报告、跟踪和纠正措施过程符合软件配置管理计划。
- (6) 通过正在进行的系统安全评估过程向软件生命周期过程提供的输入已得到处理。

2.3 软件符合性评审

软件符合性评审的目的是确保作为取证申请的一部分, 提交的软件产品的软件生命周期过程是完整的, 软件生命周期数据是完整的, 可执行目标代码是受控的, 并且可以重新生成。

审查应确定下述 9 个方面。

- (1) 已完成计划的软件生命周期过程活动, 包括生成软件生命周期数据, 并保留其完成记录。
- (2) 从特定系统需求、安全相关需求或软件需求开发的软件生命周期数据可追溯到这些需求。
- (3) 软件生命周期数据符合软件计划和标准并按照软件配置管理(SCM)计划进行控制。
- (4) 问题报告符合 SCM 计划, 已经过评估并记录其状态。
- (5) 记录并批准软件需求偏差。
- (6) 可执行目标代码可以从存档的源代码中重新生成。
- (7) 通过使用已发布的说明书, 可以成功加载已批准的软件。
- (8) 先前的软件符合性评审中的问题报告将

被重新评估以确定其状态。

(9) 如果为使用先前开发的软件寻求取证,则当前的软件产品基线可追溯到先前的基线以及对该基线的已批准更改。

3 基于 DO-178C 的软件质量管理探究

从 DO-178C 的软件质量保证要求可以看出,机载软件的质量管理可分为三大过程,即规划软件质量管理、管理软件质量和控制软件质量。

3.1 规划软件质量管理

通用的规划质量管理是识别项目及其可交付成果的质量要求和标准,并准备对策确保符合质量要求的过程^[17]。对于机载软件,则是根据 DO-178C 的 SQA 过程要求在规划阶段产生软件质量保证计划(SQAP)。该计划建立用于完成 SQA 过程目标的方法,应包括过程改进、质量测量指标和管理方法的描述,SQAP 需要包含下述内容。

(1) 环境:描述 SQA 的环境,包括范围、组织职责与联系、标准、程序、工具和方法。

(2) 权力:声明 SQA 的权力、职责和独立性,包括软件产品的批准权限。

(3) 活动:SQA 活动贯穿整个软件生命周期,包括 SQA 方法,例如评审、审计、报告、检查和监控等;问题报告、跟踪和纠正措施的相关活动;软件符合性评审活动。

(4) 过渡准则:明确进入 SQA 过程的过渡准则。

(5) 时间安排:在软件生命周期活动中 SQA 过程活动的时间安排。

(6) SQA 记录:定义 SQA 过程产生的记录。

(7) 监督供应商:描述确保供应商的实施过程和输出满足计划和标准的方法。

3.2 管理软件质量

管理软件质量即实施 SQA 过程,采用 SQAP 中定义的方法审计质量要求和质量控制测量结果,促进 SQA 过程持续改进。

在实施 SQA 过程中,通过用 SQAP 过程预防缺陷,或者在软件生命周期中对正在进行的工作检查出缺陷,来保证质量的确定性。在此执行过

程中,会产生一系列的 SQA 记录,如评审记录、审计报告^[18]、检查单、监控记录等,并以此触发纠正措施、预防措施或缺陷补救来提出变更请求。而变更请求需要全面考虑改进建议,因此,实施 SQA 过程是为过程持续改进创造条件。

3.3 控制软件质量

机载软件通常为瀑布模型,控制质量活动由特定人员在特定时间点执行。质量控制监督并记录质量执行结果,以便评估绩效,核实软件和工作已经达到主要相关方的质量要求,可供最终验收。通过绩效审查,测量、比较和分析质量测量指标,采用根本原因分析,书面记录质量控制测量结果,随之产生相应的确认变更和被核实的交付软件。

综上所述,基于 DO-178C 的软件质量管理过程如图 3 所示。

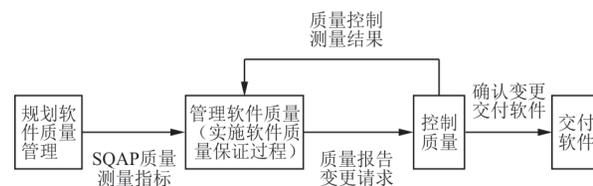


图 3 DO-178C 的软件质量管理过程

Fig. 3 Software quality management process of DO-178C

在机载软件质量管理过程中可采用的工具和方法为:质量成本分析,检查单^[19],同行评审,审计,问题解决方法^[20],检查。

3.4 基于 DO-178C 的软件质量管理建议

应充分给予软件质量人员(SQE)对软件相关过程和产品进行质量判断的职责和权力,包括停止交付不符合要求的软件产品和文档的权力。在产品发布前,必须由 SQE 批准产品中使用的所有软件或用于产品验收测试的所有软件和相关文档。在整个软件生命周期中,工程人员负责设计和开发软件以满足内部和外部客户以及监管机构的要求,而 SQE 的角色应是“客户的声音”,与工程合作以确保软件需求被理解,使用的设计方法能够产生可接受的软件产品。

灵活并高效使用机载软件质量管理过程的技术和工具。对组织过程资产的检查单库应进行维护更新,包括编码检查单、计划检查单、测试用例/测试步骤检查单等。切实落实同行评审,采用专

家判断,组织相关方和领域专家在软件需求、设计、测试和验收阶段有效开展同行评审,针对交付软件提出高质量的问题发现并实施纠正措施。对于阶段审计,不只是识别不符合项,更应识别并积累正在实施的最佳实践,对质量问题库进行更新以积累组织的经验教训知识库。灵活使用问题解决方法,通过定义问题,识别根本原因,生成可能的解决方案,选择最佳解决方案,执行并验证解决方案的有效性,解决发现的不符合项。

民用机载软件的质量管理目标在于使客户满意,“计划—实施—检查—行动(PDCA)”戴明环仍然是其持续改进的基础。管理层在其质量职责内应创造并保持真正使全员能充分参与实现质量目标的内部环境。由于使用民用机载软件的环境独特性和系统依赖性,也应增强与其他供应商的互利合作关系,以推动质量的保证,共同实现客户的需求和期望。

4 项目实践验证

以民用机载软件中某综合监视系统软件项目为例,在六个月的执行过程中,采用基于DO-178C的软件质量保证与管理方法。该软件项目的质量目标如表1所示,质量目标分为准时交付率、交付合格率与客户满意度。准时交付率=计算期内准时交付的交付物数量/计算期内计划交付的交付物数量;交付合格率=计算期内合格交付的交付物数量/计算期内实际交付的交付物数量;客户满意度满分为5分,3分表示满足客户的期望。

表1 某综合监视系统软件项目7~12月的质量目标
Table 1 Quality objective of integrated surveillance system software from July to December

月份	准时交付率/%	交付合格率/%	客户满意度/分
7月	100	97.00	3.0
8月	100	97.40	3.0
9月	100	97.40	3.0
10月	100	97.50	3.3
11月	100	97.90	3.5
12月	100	97.00	4.0

从表1可以看出:虽然每个月准时交付,但是随着SQAP的建立,实施SQA过程并进行软件质量测量结果的控制,交付合格率逐渐提升,且客户对软件质量的满意度逐渐增加。

该软件项目的质量目标可分解为两个关键过程的关键绩效指标:纠正与预防措施过程,变更控制过程,如表2所示,其中纠正与预防措施过程包括纠正与预防措施的按时关闭率,变更控制过程包括软件变更请求的按时关闭率。SQA过程在每个月进行检查和评审,针对不合格项均开展根本原因分析并发起纠正或预防措施,并积极参与软件研发过程中的变更请求。

表2 某综合监视系统软件项目7~12月的关键绩效指标
Table 2 Quality KPIs of integrated surveillance system software from July to December

月份	纠正与预防措施过程/%	变更控制过程/%
7月	67	93.35
8月	67	93.51
9月	67	93.52
10月	75	93.66
11月	80	93.82
12月	100	93.87

从表2可以看出:纠正与预防措施的按时关闭率逐渐提高,软件变更请求的按时关闭率也逐渐增大,表明有效的软件质量保证与管理方法使问题减少且提高变更请求的效率。

5 结束语

民用机载软件的合格审定作为复杂的综合性工程研究内容,DO-178C为其可接受的符合性与适航性审定活动提供了明确的指南。质量保证过程作为DO-178C的要求,是贯穿软件全生命周期的必不可少的重要过程,过程产生的质量记录更是适航取证的必需数据。

基于DO-178C的软件质量保证与管理的落实,有利于推进民用机载软件质量的提升和适航取证,更有助于在当今采用多标准、多体系融合运行的趋势下提高软件质量保证能力,为符合需求的机载软件提供信心,力求缩小差异使客户满意,有效保证机载软件的质量和持续改进。

参考文献

- [1] RTCA Inc. Software considerations in airborne systems and equipment certifications: DO-178C[S]. Washington: RTCA Inc., 2011.
- [2] RTCA Inc. Software considerations in airborne systems and equipment certifications: DO-178B[S]. Washington: RTCA Inc., 1992.

- [3] ZHAO Zhiguang, CAO Qinghua. Head first DO-178C versus DO-178B[C]// 2014 International Conference on Computer, Network Security and Communication Engineering. [S. l.]: Advanced Science and Industry Research Center, 2014: 4.
- [4] 胡宁. 从DO-178C的新变化透视软件适航关注点[J]. 航空计算技术, 2014, 44(4): 94-98.
HU Ning. Study on airworthiness concerns of changes of DO-178C[J]. Aeronautical Computing Technique, 2014, 44(4): 94-98. (in Chinese)
- [5] 中国人民解放军总装备部. 军用软件研制能力成熟度模型: GJB 5000A[S]. 北京: 中国人民解放军总装备部, 2008.
The General Reserve Department of PLA. Capability maturity model for military software development: GJB 5000A [S]. Beijing: The General Reserve Department of PLA, 2008. (in Chinese)
- [6] 于晓春. 基于GJB 5000A要求的软件过程改进及其与质量管理体系的融合[J]. 航空标准化与质量, 2021(1): 24-27.
YU Xiaochun. Software process improvement based on GJB 5000A requirements and its integration with quality management system[J]. Aeronautic Standardization & Quality, 2021(1): 24-27. (in Chinese)
- [7] 刘畅, 郝佳宁. 基于GJB 5000A的软件质量保证[J]. 质量与可靠性, 2020(1): 58-62.
LIU Chang, HAO Jianing. Software quality assurance based on GJB 5000A[J]. Quality and Reliability, 2020(1): 58-62. (in Chinese)
- [8] 高家祺. GJB 5000A中质量保证方法在航天嵌入式软件中的应用研究[D]. 兰州: 兰州大学, 2019.
GAO Jiaqi. Application of quality assurance method in GJB 5000A in embedded space software[D]. Lanzhou: Lanzhou University, 2019. (in Chinese)
- [9] 匡婷. 基于GJB 5000A的软件质量管理研究[J]. 电脑知识与技术, 2020, 16(10): 238-240.
KUANG Ting. Research on software quality management based on GJB 5000A[J]. Computer Knowledge and Technology, 2020, 16(10): 238-240. (in Chinese)
- [10] 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GJB 5000A的比较分析[J]. 科技导报, 2020, 38(21): 187-191.
LI Chao, HUANG Baiqiao. Comparative analysis of for airborne systems and equipment certification standard DO-178C and software management standard GJB 5000A [J]. Science & Technology Review, 2020, 38(21): 187-191. (in Chinese)
- [11] 杨云强, 刘玉月. 对比DO-178C与GJB 5000A浅析软件适航关注点[J]. 信息系统工程, 2017(3): 105, 107.
YANG Yunqiang, LIU Yuyue. Comparison of DO-178C and GJB 5000A software airworthiness concerns[J]. China CIO News, 2017(3): 105, 107. (in Chinese)
- [12] 陈世航. 基于RTCA DO-178B的软件独立测试验证的研究和实践[D]. 广州: 华南理工大学, 2013.
CHEN Shihang. Study and practice of independent software testing and validation based on RTCA DO-178B [D]. Guangzhou: South China University of Technology, 2013. (in Chinese)
- [13] 周全健, 孙乾, 高虎. RTCA DO-178C标准中的软件验证过程分析[J]. 航空标准化与质量, 2018(3): 42-45.
ZHOU Quanjian, SUN Qian, GAO Hu. Analysis of software validation process in RTCA DO-178C Standard[J]. Aeronautic Standardization & Quality, 2018(3): 42-45. (in Chinese)
- [14] 饶培峰, 章晓春. 基于DO-178B的机载软件开发过程及其监控评审方法[J]. 科技视界, 2015(27): 83-84.
RAO Peifeng, ZHANG Xiaochun. The development process of airborne software based on DO-178B and the monitoring and evaluation method[J]. Science & Technology Vision, 2015(27): 83-84. (in Chinese)
- [15] 胡晓莉, 孙景华, 居慧. 基于RTCA/DO-178C标准的机载软件研制过程研究[C]// 第六届民用飞机航电国际论坛论文集. 北京: 中国航空学会, 2017: 45-49.
HU Xiaoli, SUN Jinghua, JU Hui. Research on the development process of airborne software based on RTCA/DO-178C Standard[C]// Proceedings of the 6th International Forum on Civil Aircraft Avionics. Beijing: Chinese Society of Aeronautics and Astronautics, 2017: 45-49. (in Chinese)
- [16] 马珂, 李大超. 基于DO-254的可编程逻辑器件设计的质量保证研究[J]. 软件产业与工程, 2014(5): 19-23, 47.
MA Ke, LI Dachao. Research on quality assurance of design of programmable logic devices based on DO-254[J]. Software Industry and Engineering, 2014(5): 19-23, 47. (in Chinese)
- [17] 李晖旻. 论定制化软件开发项目的质量管理[J]. 中小企业管理与科技, 2018(8): 17-18.
LI Xuanmin. Research on quality management of customized software development project[J]. Management & Technology of SME, 2018(8): 17-18. (in Chinese)
- [18] 沈斌. 深入开展软件质量保证工作的探讨[J]. 电子质量, 2020(1): 41-44.
SHEN Bin. Discussion on further developing software quality assurance[J]. Electronics Quality, 2020(1): 41-44. (in Chinese)
- [19] JIMÉNEZ J A, MERODIO J A M, SANZ L F. Checklists for compliance to DO-178C and DO-278A standards [J]. Computer Standards & Interfaces, 2017, 52: 41-50.
- [20] 胡庆林, 王一苇. 软件质量保证过程研究[J]. 电子质量, 2016(6): 60-63.
HU Qinglin, WANG Yiwei. The research of software quality assurance process[J]. Electronics Quality, 2016(6): 60-63. (in Chinese)

作者简介:

周培(1990—),女,硕士,中级工程师。主要研究方向:民用机载软件的测试验证,质量保证与管理。

(编辑:丛艳娟)