基于DO-178C及CMMI的民用航空发动机控制软件质量保证研究

阎 迪

(中航工业商用航空发动机有限责任公司 控制系统部,上海 201108)

摘 要:随着嵌入式软件逐渐成为民用航空发动机控制系统这一复杂系统的最重要组成部分,对于其安全性和可靠性的要求也日渐提高,而软件因为其研发过程的特殊性,要保证其产品质量则必须依靠过程的监控与符合性检查。软件质量保证(SQA)就是评估软件生存周期过程及其输出,以保证目标得以满足,故障得以检测、评估、追踪和解决,并保证软件产品和软件生存周期资料符合合格审定要求的活动,是航空软件产品研发过程中重要的一环。以DO-178C为指导,结合CMMI三级关键过程域实践,总结出一套民用航空发动机控制软件的质量保证流程,为质量保证人员(QA)提供参考。

关键词:民用发动机控制系统 软件;质量保证;DO-178C;CMMI

中图分类号:TP311.52 **文献标识码**:A **文章编号**:1671-654X(2016)06-0080-04

Research on SQA of Commercial Engine Control Software Based on DO-178C and CMMI

YAN Di

(*Commercial Aircraft Engine Co. Ltd*, *AVIC*, *ShangHai* 201108, *China*)

Abstract: As the embedded software becomes the most important part of the commercial aircraft engine control system, the demand on its safety and reliability has increased day by day. While, due to the particularity of its development process, the quality of software must be assured by process monitors and conformity auditing. Software quality assurance (SQA) is an activity evaluating software life cycle and its outputs to assure that aim can be achieved, fault can be detected, evaluated, traced and solved, also the software product and its life cycle materials conform to the qualified approval requirement, which is an important part of aircraft software product development process. On the guidance of DO-178B, and taking the critical process area of CMMI 3 into account, a quality assurance process of the commercial aircraft engine control software is put forward to give a reference to the quality assurance engineer (QA).

Key words: engine control; software quality assurance; DO-178C; CMMI

引言

航空发动机控制系统已从简单的机械液压燃油控制系统,经历初始阶段、成长阶段、电子阶段、综合阶段,发展到用于所有燃气涡轮发动机的全权限数字电子控制系统(FADEC)。数字电子控制系统的功能越来越全面,其中的控制软件也越来越复杂,1985年和1996年,由美国发动机供应商提出,并经两位总工程师复核,对航空发动机控制系统元部件的重要性进行排名,在软件、电子部件、液压机械部件、执行机构、燃油泵5种主要元部件中,软件成为航空发动机控制系统的最重要部分,软件质量成为影响航空发动机功能、性能的关键因素之一,如何通过有效的质量保证手段提高发动机控制软件质量是目前需解决的现实问题。

软件质量保证就是通过实施必要的、已策划、系统化的活动,为软件产品或过程满足给定的需求提供证据及置信度。软件质量保证通过对过程和过程输出的监督和客观评价,确保软件全生命周期过程的实施及输出符合标准、规程和组织方针的要求,对保证软件质量起着关键的作用。

本文综合考虑了民用航空发动机控制系统软件开发的特殊性,以DO-178C《机载系统和设备合格审定中的软件考虑》为指导,结合能力成熟度模型集成(CMMI)中过程及产品质量保证过程域(PPQA)的最佳实践,研究了民用航空发动机控制软件质量保证的人员角色及职责、过程审计、产品审计、独立性要求、问题沟通解决等内容,给实际工程实践提供技术支持。

收稿日期:2016-05-26 **修订日期**:2016-09-08

作者简介:阎 迪(1983-),女,河北高阳人,工程师,硕士,主要研究方向为软件配置质量保证。

1　发动机控制软件的质量保证要求

2013 年 7 月 19 日,美国联邦航空管理局(FAA)在咨询公告 AC 20－115C 中明确指出,对于飞机、发动机、螺旋桨推进器中机载系统和设备所包含的软件,可使用 DO－178C 作为软件符合性方法,但不是唯一的方法。因此,DO－178C 是飞机、发动机中嵌入式软件研制应遵循的主要标准。

在 DO－178C 中对软件质量保证提出的目标包括:

1)确保软件计划及标准被开发、评审,并且与 DO－178C 要求一致;

2)确保软件生存周期与已批准的软件开发计划相一致;

3)确保软件生存周期与已批准的软件开发标准相一致;

4)确保软件生存周期过程中的转换准则得以满足;

5)确保实施软件符合性评审。

DO－178C 标准中要求的质量保证活动如表 1。

表 1　质量保证活动

序号	内　　容
1	质量保证过程应在软件生存周期过程活动中扮演积极的角色,应使质量保证人员具有一定的职权、明确的职责并独立行使职权,以保证 SQA 过程目标得到满足。
2	质量保证过程应保证软件计划和标准被编写、评审,与 DO－178C 标准要求一致。
3	质量保证过程应保证软件生存周期过程与已批准的软件计划和标准一致。
4	质量保证过程应对软件生存周期中各过程进行审计,已保证:第一软件计划可用;第二对软件计划和标准的偏离得到检测、记录、评估、追踪和解决;第三已批准的实施偏离得以记录;第四软件开发环境已按照软件计划提供;第五问题的报告、追踪和纠正措施过程符合软件配置管理计划;第六系统安全性评估过程提供给软件生存周期过程的输入得到处理。
5	质量保证过程应确保软件生存周期过程转换准则与已批准的软件计划一致。
6	质量保证过程应确保软件生存周期数据按照控制分类要求受到控制的保证。
7	在软件产品正式提交之前,应进行软件符合性评审。
8	质量保证过程应产生相应的记录,包括对作为合格审定申请一部分的每个软件产品所进行的符合性评审的审计结果和完成的证据。
9	质量保证过程应提供对供应商过程及输出符合已批准的计划和表征的证据。

可以看到,在 DO－178C 中提出的软件质量保证过程活动可分为以下几类:1)对角色和职责的定义;2)对过程的审计,保证过程的实施与计划一致;3)对产品的审计,保证软件产品和标准要求的一致;4)对发现问题的解决。这与 CMMI 中过程与产品质量保证过程域(PPQA)的要求几乎一致。在CMMI 中,PPQA 过程域有两个专用目标:SG1 客观评价过程和工作产品;SG2 提供客观深入的了解。这两个目标共包含 4 个专用实践:SP1.1 客观评价过程;SP1.2 客观评价工作产品和服务;SP2.1 交流并确保解决不符合项;SP2.2 建立记录。专用目标及专用实践之间的关系如图 1。

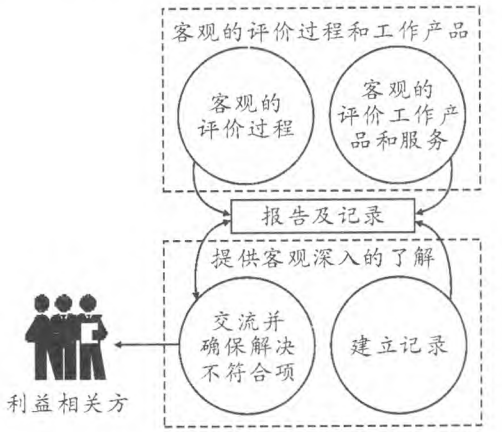

图 1　CMMI PPQA 过程域的目标和实践

2　航空发动机控制软件质量保证技术

通过对 DO－178C 软件质量保证过程和 CMMI PPQA 过程的综合分析,可以看出航空发动机控制软件质量保证的关键是要解决以下问题:1)质量保证组织角色和职责;2)质量保证的工作流程;3)过程审计;4)产品审计;5)审计问题的处理和分析。

2.1　质量保证组织架构及角色职责

依据 DO－178C 对质量保证活动独立性的要求,结合航空发动机控制系统软件研发和系统研制的关系,在实践中总结出质量保证组织结构要遵循以下两条原则:1)质量保证组应独立于软件开发组之外,其工作不受软件项目负责人的领导;2)质量保证对系统负

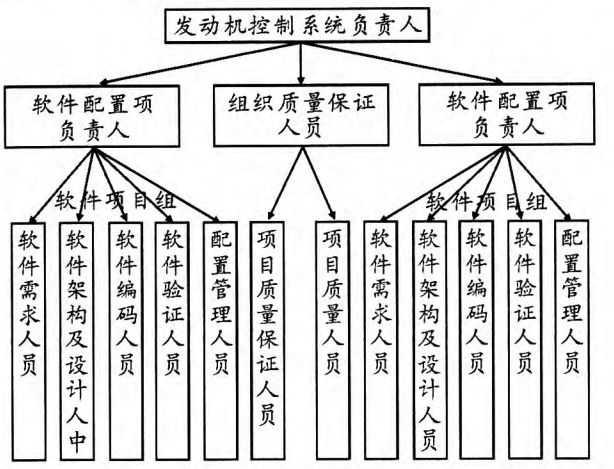

图 2　质量保证组织架构

责人或组织领导者有直接的汇报渠道。根据以上原则规划出的质量保证组织架构如图2。

根据组织架构图总结归纳出质量保证相关角色职责的描述如表2。

表2　质量保证角色及职责

角色	职　责
控制系统负责人	1)支持对软件过程活动和工作产品的审核,包括资源配备、人员安排; 2)听取软件质量保证组对于软件质量状态和问题的汇报,问责迟迟未纠正的质量问题; 3)协调解决需要跨部门或团队的难以纠正的质量问题。
软件项目负责人	1)配合软件质量保证组制定质量保证计划; 2)支持对软件过程活动和工作产品的审核,包括;配合审核人员安排,资源协调等; 3)确认并跟踪、协调解决质量保证组提出的不符合项。
软件开发组	1)了解需要审核的内容,为审核准备必须的客观的数据和记录; 2)配合对软件过程活动和工作产品的审核; 3)纠正质量保证组提出的不符合项; 4)反馈不符合项的纠正情况,汇报难以纠正,需要协调的质量问题。
组织质量保证组	1)参与项目计划及质量保证计划评审; 2)参与项目符合性审查; 3)对项目质量保证开展情况进行审查; 4)参与项目质量问题整改归零。
项目质量保证组	1)参与定义项目的软件过程,参与制订项目的开发计划; 2)制订项目的质量保证计划并参与计划评审; 3)根据项目生命周期的管理特点和要求调整QA审核检查单; 4)审核项目定义的软件过程,审核指定的软件工作产品,并记录审核结果; 5)根据审核结果建立不符合项,跟踪不符合项的处理; 6)上报迟迟未纠正、需要提升的不符合项; 7)对项目的软件质量活动进行度量分析和总结,并上报结果。
软件配置管理组	1)对审核过程和结果记录、问题跟踪提供配置管理和工具支持; 2)配合对项目软件配置管理活动的审核; 3)确认并跟踪纠正质量保证组提出不符合项。

2.2　SQA活动流程

PDCA模型是质量保证过程一种行而有效的工作方法,在该工作流程中体现“计划(P)－实践(D)－检查(C)－改进(A)”的循环,实现质量保证过程的闭环。根据PDCA模型设计出的发动机控制软件质量保证活动流程如图3。

在具体工作时,组织可以根据实际情况,将SQA的活动流程E化为工具实现,用信息化流程管理系统来管理SQA问题跟踪处理关闭过程的优势是显而易见的,它更有利于团队协同工作,并减少沟通成本。

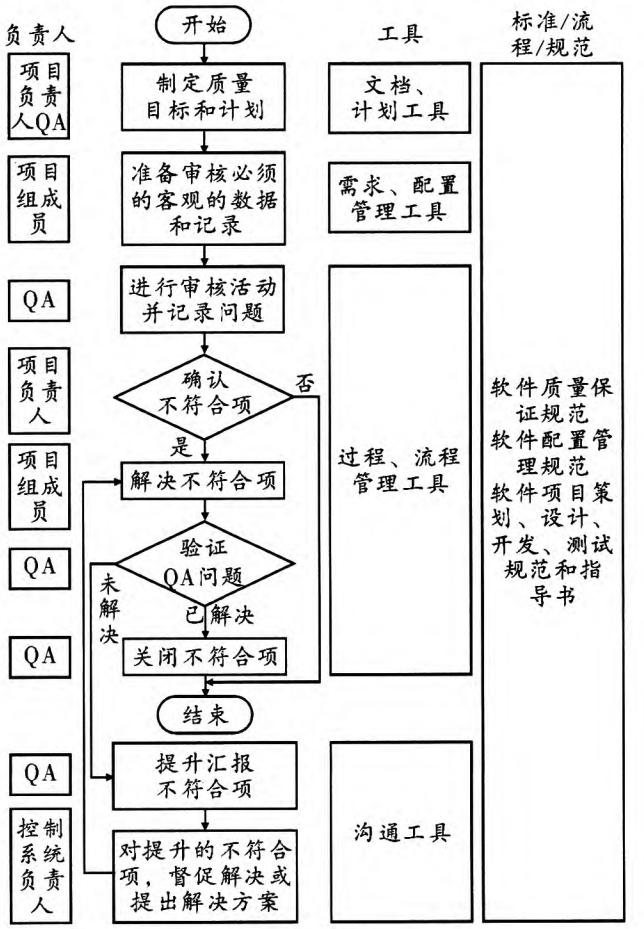

图3　质量保证活动流程

2.3　质量保证审核

按照DO－178C的要求,质量保证审核对象应包括过程和产品。过程审核是通过对过程活动的检查,对过程质量控制的正确性、有效性进行分析评价的方法,审核的重点应针对软件生命周期中的关键或特殊过程,如计划过程、开发过程、综合过程等。产品审核是通过对产品的全面或抽取的定量检查分析来评价产品质量的方法,审核的重点应针对软件生命周期中的重要或主要产物,如:需求规格说明、源代码等。

根据DO－178C的过程和产品要求,总结航空发动机控制软件过程审核和产品审核的内容如表3。

2.4　客观性要求

质量保证审核的客观性,是项目成功的关键。客观评价指由审核者对照已定义准则开展过程和工作产品评审,以便最大限度地减少主观性和偏见。

客观性的关键是独立性和准则两个方面,对航空发动机控制软件,可使用组合方法,一方面由专职质量保证人员或非本软件开发人员按照准则采用非正式方法进行日常评价、审核,另一方面,定期则采用正式的

方法,可以保证客观性。执行客观评价的方法包括由独立于组织的质量保证机构进行的正式审核、各种不同正式程度的同行评审、在工作现场执行的深入工作评审、对工作产品的分布式评审和评论等。

表 3　质量保证审核表

过程		过程审核	产品审核
计划过程		策划过程审核	软件合格审定计划 软件开发计划 软件配置管理计划 软件质量保证计划 软件验证计划 软件需求标准 软件设计标准 软件编码标准
开发	需求	需求过程审核	软件需求数据
	设计	软件设计过程审核	软件设计描述
	编码	编码过程审核	源代码
	集成	集成过程审核	目标代码
综合	验证过程	验证过程审核	验证用例及程序 软件验证结果
	配置管理	配管管理过程审核	环境配置索引 软件配置索引 问题报告 配置管理记录
	质量保证	质量保证过程审核	质量保证记录 软件完成总结 追踪数据

通常,独立于项目的质量保证组提供这种客观性。在某些组织中,在没有这种独立性的条件下,也可采用一些灵活的方法,其最低要求是对过程和产品的审计不能由过程和产品的实施人员承担。为了确保客观性,必须解决几个问题:1)每个实施质量保证活动的人应经过质量保证方面的培训;2)实施工作产品质量保证活动的人应与直接参与开发或维护该工作产品的人分开;3)必须有独立向组织的适当层次管理者报告的渠道,使得必要时不符合项可以逐级上报。

2.5　不符合项的沟通和解决

不符合项是通过客观评价所标识出的问题,反映对适用的标准、过程说明或规程遵循的偏离、不足。不符合项的状态指示出质量趋势。质量问题应包括不符合项和质量问题趋势分析。当不符合项在项目内不能解决时,按所建立的上报机制,确保适当层次的管理者能解决该问题。对不符合项的解决的关键是建立组织级质量保证人员,对项目质量保证人员的工作进行跟踪,直至不符合项解决为止。

2.6　对质量保证人员的要求

对航空发动机控制软件的过程、产品进行有力监控,要求质量保证人员必须对发动机控制系统充分认识、充分理解。同时,航空发动机控制软件的研制涉及多领域、多学科,系统、硬件、软件研制技术繁杂,因此需要对质量保质人员进行不断培训,增强质量保证人员的技术能力,这要求做好培训规划、提供培训保障,同时考虑质量保质人员的结构层次,做到专业化的监控。

3　结束语

发动机控制系统研制是一项复杂的系统工程,作为其最重要组成部分的软件的开发,更是一个不断优化迭代的过程,而软件本身版本变化快速、缺陷不易暴露的特点决定了软件的质量保证即是过程的质量保证,DO－178C 和 CMMI 模型明确了软件开发和管理的目标和要求,但如何做的问题还需要在实践中不断地摸索和总结,只有将标准体系真正落地,与实际工作结合,才能切实做到软件的质量可控,最终获得适航的认可。

参考文献:

[1] 姚华. 未来航空发动机控制技术的发展趋势[J]. 航空科学技术,2012(6):32－36.

[2] RTCA DO－178C. Software Considerations in Airborne System and Equipment Certification[S]. USA:RTCA,2011.

[3] FA,AC 20－115C. Airborne Software Assurance[S]. USA:FAA,2011.

[4] 王青. 基于 ISO9000 的软件质量保证模型[J]. 软件学报,2001,12(12):1837－1842.

[5] 邵丽. 基于 ISO9001/CMM 的软件质量保证的对比研究[J]. 计算机应用研究,2002,19(7):32－35.

[6] 黄飞雪,李志洁,孙效里. 基于 PDCA 的印度软件质量保证模型研究[J]. 哈尔滨工业大学学报,2005,37(11):1583－1585.

[7] 袁安富,伏萍. 基于 CMMI 的软件质量保证[J]. 计算机技术与发展,2012,22(1):13－16.

[8] 王涛. 软件质量保证与软件质量控制[J]. 电脑知识与技术,2005(9):62－64.

[9] 刘涛,薛胜军. 基于 CMM/CMMI 的软件质量保证[J]. 交通信息与安全,2006,24(2):121－123.

[10] 刘文红,吴欣,张敏. 基于 CMMI 的软件质量保证[J]. 现代电子技术,2012,35(16):53－56.

[11] 夏侯赟,钟海. 软件质量保证与 CMM[J]. 科技广场,2006(9):125－126.

[12] 马闰娟,梁成才. CMM 二级 KPA 软件质量保证的一个实施方案[J]. 计算机工程,2003,29(2):112－114.

[13] 王乐鹏,施泉生. CMM 中软件质量保证在 ERP 实施中的应用研究[J]. 信息技术与标准化,2007(4):47－50.