航空科学技术
Aeronautical Science & Technology
Aug. 15 2014 Vol. 25 No.08 05-08

机载软件计划阶段评审研究

朱宇蒙*，金平，孙全艳，章晓春
上海飞机设计研究院 飞控系统设计研究部，上海 201210

摘 要：本文针对机载软件研制流程，分析了机载软件适航审查，包括4个阶段：软件计划阶段评审（SOI#1）、软件开发阶段评审（SOI#2）、软件验证阶段评审（SOI#3）和软件最终审定评审（SOI#4）。本文在对高升力系统软件功能进行分析的基础上，给出了高升力系统软件SOI#1审查的软件生命周期数据、SOI#1评审目标和过程，为软件后续评审奠定了基础。

关键词：机载软件；适航；高升力系统；DO—178B

中图分类号：TP311.5　　**文献标识码**：A　　**文章编号**：1007-5453（2014）08-0005-04

机载软件广泛用于现代民用飞机，而其正确性无法通过直接检查、穷举测试等方法来确认，只能通过特定的过程审查来确保。为满足14CFR/CS/CCAR 25.1309（设备、系统及安装），工业界也出台了一些相应的标准指导民用飞机软件的研制（如RTCA DO-178B）。在民用飞机的适航认证活动中，为了监控软件的生命周期过程，并确定其与DO-178B的符合性，对软件的适航评审主要采用SOI（介入阶段）评审的方式。其中，软件计划阶段评审（SOI#1）评审是几次适航评审的基础。本文主要研究了SOI#1评审的原理和流程，并总结了审查方在SOI#1评审中关注较多的问题。

1 机载软件适航审查原理

机载软件是指安装在机载系统和设备中为了实现某个系统功能的软件，为型号的设计组成部分。民用飞机对机载软件的安全性有着非常严格的要求。为此，国际航空无线电委员会(RTCA)和欧洲民航装备组织(EUROCAE)针对民用航空电子系统的软件开发制定了DO-178B/ED-12B标准。该标准基于在系统安全性评估过程中确定的软件对潜在失效条件的影响，将软件划分为 A~E 五个等级[1]，如表1所示。软件等级越高，需要满足的目标和要求越高。其中，A级别软件对应的失效条件为灾难级失效条件，需要满足DO-178B中的66个目标，其中25个目标需独立满足（即开发和验证人员独立）。

表1 机载软件等级
Table 1 The level of airborne software

软件级别	失效条件	178B目标	独立目标	覆盖率要求
A	灾难	66	25	MC/DC（修改条件/决条件）覆盖率100%+B级要求
B	危险	65	14	判定覆盖率100%+C级要求
C	较重	57	2	语句覆盖率100%+D级要求
D	较轻	28	2	需求覆盖率100%
E	无影响	0	0	无

DO-178B定义的软件研制过程和阶段如图1所示[2]。

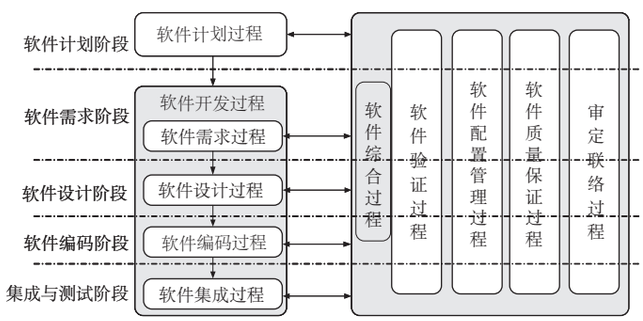

图1 DO—178B定义的软件研制过程和阶段
Fig.1 The software development process and phase defined in DO-178B

收稿日期：2014-04-01；　录用日期：2014-06-05
*通讯作者．Tel.：021-20866611　E-mail：zhuyumeng@comac.cc
引用格式：ZHU Yumeng，JIN Ping，SUN Quanyan，ZHANG Xiaochun. Research of airborne software plan phase review [J]. Aeronautical Science & Technology，2014,25(08):05—08. 朱宇蒙,金平,孙全艳,章晓春. 机载软件计划阶段评审研究[J]. 航空科学技术，2014，25(08)：05—08.

软件研制可分为软件计划阶段、需求阶段、设计阶段、编码阶段、集成与测试阶段，分别对应软件计划过程、需求过程、设计过程、编码过程、集成过程，其中后四个过程可统称为软件开发过程；此外，软件验证过程、配置管理过程、质量保证过程、审定联络过程贯穿整个软件生命周期，可统称为软件综合过程。

FAA Order 8110.49(软件审查指南)中明确了可以采用SOI(介入阶段)评审对机载软件进行审查，并对其进行了明确定义，共分为4个阶段[3]：

(1) SOI#1 ——软件计划阶段评审；

(2) SOI#2 ——软件开发阶段评审；

(3) SOI#3 ——软件验证阶段评审；

(4) SOI#4 ——软件最终审定评审。

软件适航审查原理如图2所示[2]。

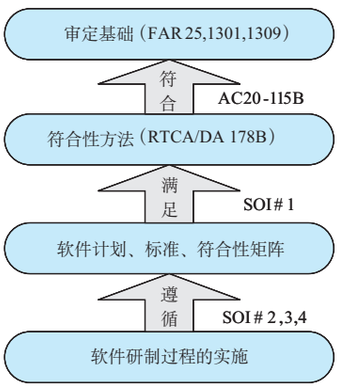

图2 软件适航审查原理

Fig.2 Principle of software airworthiness reviews

机载软件的适航审查基础是FAR Part25.1301和25.1309。咨询通告FAA AC20-115B认定DO-178B为可接受的符合性方法。SOI#1评审判定软件计划、标准、符合性矩阵是否满足符合性方法(DO-178B)，SOI#2/3/4评审判定软件研制过程的实施是否遵循软件计划、标准、符合性矩阵。

在进行各阶段SOI评审之前，民用飞机的主制造商往往会对供应商进行若干次工程审查，主要包括：计划阶段评审(PPR)；初步设计评审(PDR)；关键设计评审(CDR)；测试就绪评审(TRR)；符合性评审(CR)。

工程评审与适航评审之间的关系如图3所示。

PPR评审在SO1#1之前进行，PDR和CDR评审(两次评审可依次分别进行或合并进行)在SOI#2与SOI#3之间进行，TTR评审在SOI#2与SOI#3之间进行，CR评审在SOI#3与SOI#4之间进行。

工程评审的记录和结论可作为后续审查方SOI适航评审的重要支持性证据。

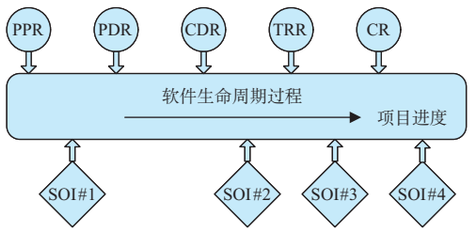

图3 软件工程评审与SOI适航评审

Fig.3 Software engineering reviews and SOI airworthiness reviews

软件适航审查在软件研制流程中的实施示例如图4所示[2]。

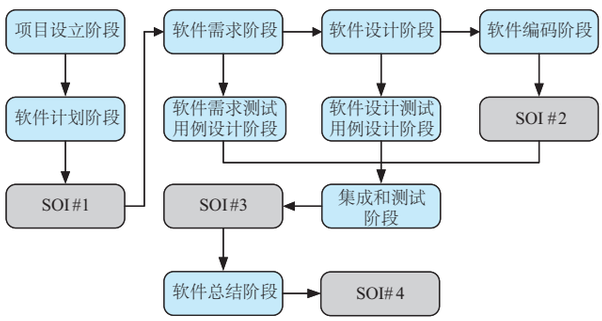

图4 软件适航审查在研制流程中的实施

Fig.4 Implement of software airworthiness reviews in development process

2 高升力系统软件功能

本文研究的高升力系统为电信号控制，液压动力驱动。驾驶员操纵襟/缝翼控制手柄发出指令信号，襟/缝翼电子控制装置(FSECU)接收信号后进行计算并控制驱动线系运动，使襟翼和缝翼按照一定顺序放下或收回，以增大机翼的面积和弯度，从而增加升力和阻力，缩短飞机起飞和着陆时的滑跑距离。驻留系统功能软件的FSECU完成系统的控制和监控。

高升力系统机载软件提供双通道的指令监控控制以实现下述基本功能：

(1) 襟/缝翼伸出、收回、锁定功能；

(2) 向显示系统提供高升力系统显示和告警信息；

(3) 人为错误的防护功能；

(4) 向飞行数据记录系统提供高升力系统飞行数据信息、状态、故障信息、飞行操作数据；

(5) 高升力系统维护、调整测试功能；

（6）向机载维护系统提供高升力系统部件数据信息、计算机软件代号；

（7）高升力系统软件构型改进功能。

3 高升力系统软件SOI#1审查

高升力系统软件计划阶段评审（SOI#1）是审查方首次介入审核，审查对象为软件各类计划文件和标准。SOI#1主要评审的软件生命周期数据及其对应的DO-178B章节号如表2所示。

表2 SOI#1审查的软件生命周期数据

Table 2 Software lifecycle data reviewed in SOI#1

软件生命周期资料	DO-178B章节号
软件合格审定计划（PSAC）	11.1
软件开发计划（SDP）	11.2
软件验证计划（SVP）	11.3
软件构型管理计划（SCMP）	11.4
软件质量保证计划（SQAP）	11.5
软件需求，设计，编码标准（SRDCS）	11.6,11.7,11.8

其中，PSAC是整个软件计划的总揽及其他计划和标准文件的总纲，同时也是审查方至少需要批准的三份软件生命周期数据之一（其余两份是软件构型索引（SCI）和软件完成综述（SAS））。因此，PSAC能否得到审查方的批准是SOI#1是否完成的重要指标之一。

高升力系统软件SOI#1的最终目的是要满足DO-178B附录A表A-1“软件计划阶段”、表A-8“软件构型阶段”（#1-4）、表A-9“软件质量保证阶段”（#1）和表A-10 “合格审定联络阶段”（#1-2）的所有目标。

主制造商进行的机载软件PPR工程评审的记录和结论也作为SOI#1评审的重要置信证据向审查方提交。PPR工程评审与SOI#1评审之间的关系如图5所示。

4 结论

在软件SOI#1评审中，系统分配给软件的需求与通过初步系统安全性分析（PSSA）给软件分配的安全性等级是审查方评审的重点；此外，面向对象的方法、先前开发软件、适航联络人工作计划等相关内容也会受到审查方较多的关注。

SOI#1评审的通过意味着审查方对软件研制过程的阶段性认可，为软件的后续研制奠定了基础，指明了方向。

SOI#1通过之后，审查方将继续对机载软件生命周期过程进行全面而详尽的监控，以保证软件的安全性。

AST

参考文献

[1] RTCA DO-178B, Software considerations in airborne system and equipment certification[S]. Washington D.C.: RTCA, 1992.

[2] 沈小明，王云明，陆荣国等.机载软件研制流程最佳实践[M].上海:上海交通大学出版社，2012.
SHEN Xiaoming, WANGYunming, LU Rongguo, et al. Best practice for airborne software production workflow[M].Shanghai: Shanghai Jiao Tong University Press,2012. (in Chinese)

[3] FAA Order 8110.49, Software approval guidelines[S].Washington DC. 2003.

作者简介

朱宇蒙（1986－ ） 男，硕士，助理工程师。主要研究方向：飞行控制系统机载软件开发与适航管理。

Tel：021-20866611

E-mail：zhuyumeng@comac.cc

金平（1976－ ） 男，硕士，高级工程师。主要研究方向：飞行控制系统电气接口定义，飞行控制系统机载软硬件开发与适航管理。

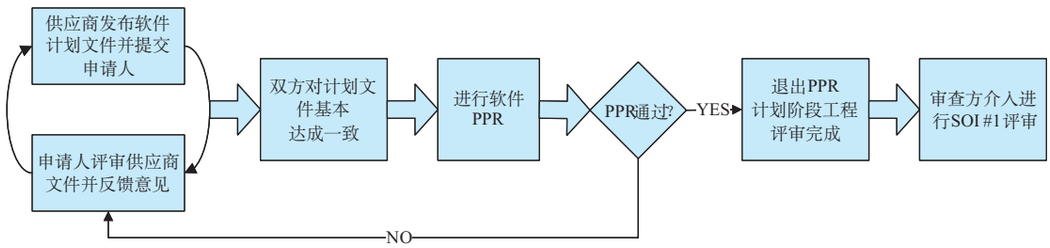

图5 PPR工程评审与SOI#1评审之间的关系

Fig.5 The relationship between PPR engineering review and SOI#1 review

Tel：021-20866612
E-mail：jinping@comac.cc
孙全艳(1983—) 女，硕士，工程师。主要研究方向：飞行控制系统机载软件开发与适航管理，软件工具鉴定。
Tel：021-20866610
E-mail：sunquanyan@comac.cc
章晓春(1985—) 男，硕士，工程师。主要研究方向：飞行控制系统机载软件开发与适航管理，自动飞行系统开发与适航管理。
Tel：021-20866628
E-mail：zhangxiaochun@comac.cc

Research of Airborne Software Plan Phase Review

ZHU Yumeng*, JIN Ping, SUN Quanyan, ZHANG Xiaochun

Flight Control Department, Shanghai Aircraft Design and Research Institute, Shanghai 201210, China

Abstract: Pointing at airborne software development process, this paper analyzed airborne software certification reviews, which included four phases: Software Plan Phase Review (SOI#1), Software Development Phase Review (SOI#2), Software Verification Phase Review (SOI#3), Software Final Phase Review (SOI#4). Based on the analysis of high lift system software functions, this paper gave the software lifecycle data that high lift system software SOI#1 reviewed, the SOI#1 review objectives and process, which are the basis of following software reviews.

Key Words: airborne software; airworthiness; high lift system; DO-178B

Received: 2014-04-01； **Accepted:** 2014-06-05

***Corresponding author. Tel.：** 021-20866611 **E-mail:** zhuyumeng@comac.cc