

基于主机厂—供应商模式下的民用飞机机载软件构型管理方案研究

Research on Civil Aircraft Airborne Software Configuration Management Based on Airframer—Supplier Model

李林奇^{1,2} 陈一可^{1,2}

1 中国商飞上海飞机设计研究院 2 民用飞机模拟飞行国家重点实验室

摘要: 机载软件,即安装在飞机上作为飞机型号设计组成部分的软件,其构型管理活动贯穿从研发、集成、试验,到批产直至交付客户整个飞机研制的生命周期。如何对不同架次、不同构型的机载软件进行构型控制,是民用飞机研制和取证过程中的一个重要环节。

Abstract: Airborne software is installed in the aircraft as part of its type design, which configuration management activities continue throughout the aircraft development life cycle, from research, integration, testing, production, to customer delivery. How to control different aircraft, or different airborne software configuration, is an important issue in the civil aircraft development and type certificate process.

关键词: 民用飞机;机载软件;构型管理

Keywords: civil aircraft; airborne software; configuration management

0 引言

当前国产民用飞机的设计研发过程采用国际广泛流行的“主机厂—供应商”工作模式。对于机载软件开发过程来说,主机厂定义飞机需求、系统需求、接口控制规范,并对提出的需求进行确认和验证;供应商根据系统需求开发出设备需求和软件高级别需求,并依据软件高级别需求,按照RTCA/DO-178B作为符合性方法开发出实现预定功能的软件产品。

民用飞机机载软件具有研发周期长、版本更新频繁、相关工程资料密集等特性。由于全机各系统的软件由不同的供应商开发,因此各系统软件的设计保障等级、设计架构、实现方法、构型标识等方面亦有不同。基于机载软件的特点,参考局方在机载软件审查时对构型

管理的主要关注点,本文将从主机厂角度出发,讨论如何实现机载软件构型的高效、规范管理。

1 构型标识

构型标识是对构型项定义,它是每个构型项及其相关数据指定的唯一标识,软件作为一种无形的产品必须依附设备作为载体,因此软件的构型标识不能脱离设备。含软件的设备按照如下两个层级标识该构型项:第一层为设备的硬件件号(H/W Part No.)和序列号(Serial No.);第二层为设备所含软件的构型标识信息,通常包括软件的件号(S/W Part No.)和/或版本(S/W Version)。

对于软件生命周期资料来说,每份软件生命周期资料是一个构型项,其构

型标识通过文件编号和版本实现唯一标识^[1]。

1.1 软件兼容性矩阵

鉴于民用飞机机载软件数量众多、构型状态复杂,且同一软件也有多种构型状态等情况,主机厂需建立软件兼容性矩阵,以体现机上所有相互兼容的软件件号、版本以及含软件的硬件信息。

当软件兼容性矩阵被创建之后,它可以罗列出所有已得到工程批准的构型。在任何一架飞机上,同一个软件组件的构型应当被列在同一列中,此列中没有出现的任何软件件号或构型都不允许被装载在飞机上。举例而言,假定有3个软件组件,分别是航电计算机、定位处理系统GPS单元和航速监控器,其中有两个不同的GPS单元和两个不同的航速监控

器可供安装。航电计算机中的软件会根据飞机上不同的GPS单元和航速监控器选择加载的构型,如表1所示。若供应商A提供的GPS安装在飞机上,那么供应商X提供的航速监控器就必须被安装,对应的航电计算机软件AVC-SW-382 Rev.3必须被安装。在另一架不同构型的飞机上,若供应商B的GPS单元被安装了,那么供应商Y提供的航速监控器就必须被安装,对应安装的航电计算机软件必须是AVC-SW-682 Rev.1。

1.2 飞机软件构型矩阵

从飞行试验开始,主机厂应创建飞机软件构型矩阵并在飞机生命周期中随软件构型变化保持更新。通过该矩阵可以清晰地表明每架试验机上所有软件的构型信息(包括架次号,每架飞机上各设备安装的软件构型、软件设计保障等级、限制使用状态等),矩阵上的每一条输入都应与实际安装在指定飞机上的软件构型信息相一致。

飞机软件构型矩阵和软件构型兼容性矩阵是类似的。两者最主要的不同是,软件兼容性矩阵显示的是可以安装在某一架飞机上的软件部件的组合,而飞机软件构型矩阵显示的是不同架次飞机上所安装的所有软件构型。

2 各阶段的机载软件构型管理

在民用飞机研制周期中,稳定的软件与良好的验证活动可以提升合格审定的置信度,主机厂需在不同研制阶段通

过执行有效的构型控制活动保证适航要求 and 工程要求得以满足。

2.1 工程设计阶段

在项目的工程设计阶段,需求还在不断地分解,测试用例和规程还在开发中,此时软件组件很不稳定,更改相对频繁。针对上述情况,主机厂在执行机载软件构型管理活动时应考虑以下方面。

1) 供应商提交的软件计划(软件合格审定计划、开发计划、验证计划、构型管理计划、质量保证计划)和标准(需求标准、设计标准、编码标准)应纳入主机厂的构型控制体系;

2) 所有给供应商的数据(如系统规范和接口控制文件)应来自主机厂构型控制之中;

3) 发现的软件问题应创建问题报告并进行跟踪处理,若相关问题涉及到供应商,则问题报告应与供应商的问题报告关联起来;

4) 使用软件兼容性矩阵和飞机软件构型矩阵追踪在试验环境或飞机上的软件,软件发生构型变化时,需更新软件兼容性矩阵和飞机软件构型矩阵,使其能反映出即将用于飞行试验的构型信息。

2.2 飞行试验阶段

在飞行试验阶段,软件和软件相关文档都已纳入构型控制。软件更改相对较少,但此阶段更改影响和风险更大,任何更改都必须被评审、批准和追踪。主机厂在此阶段机载软件构型管理应考虑以下方面。

1) 供应商提交的软件生命周期数据应纳入主机厂的构型控制体系;

2) 主机厂应将软件相关的试验结果纳入其构型控制体系;

3) 在试飞阶段发现的任何软件缺陷或偏离应创建相关的问题报告;

4) 保持对软件兼容性矩阵和飞机软件构型矩阵的更新;

5) 当软件本体、设计数据(如需求数据)等发生更改时,需进行软件更改影响分析,以判断是否对已完成的试验存在潜在的影响;

6) 如果发现了与飞行安全相关的问题,主机厂应建议暂停飞行试验直到问题被解决。

2.3 型号合格审定和服务阶段

该阶段是指型号取证已经完成,进入持续适航阶段。与型号设计相关的软件数据应该已经归档并可支持后续工作。如软件发生更改,则更改必须被批准并给飞机所有者(一般为航空公司)发送。主机厂在此阶段机载软件构型管理应考虑以下方面。

1) 新的构型、设备会加入软件兼容性矩阵中。一旦软件被局方批准,不得删除表中任何信息。

2) 飞机软件构型矩阵需要按每架机的信息进行更新直到飞机离厂。如果发出相关的服务通告,那么飞机软件构型矩阵也需要根据服务通告里的更改信息进行更新。

3) 更改一个已批准的软件应在服务通告中记录成文并发送给飞机所有者。与安全性相关的服务通告应与适航审定当局进行沟通。

3 构型控制

3.1 软件加载控制

在供应商交付前已加载完成的设备以及无法现场更改的软件,其软件加载控制活动由供应商负责。

对于外场可加载软件,主机厂需考虑以下几方面。

1) 可执行目标码或加载数据应存储

表1 软件兼容性矩阵样例

硬件件号	A飞机软件构型	B飞机软件构型
航电计算机 P/N AVC-12345	AVC-SW-382 Rev. 3	AVC-SW-682 Rev. 1
供应商 A GPS单元 P/N GPS-1122	GPS-SW-1243 Rev. 3	
供应商B GPS单元 P/N GPS-8877		GPS-8877-SW03 Rev. 5
供应商 X 航速监控器 P/N ASM-345	ASM-345 Mod. B	
供应商Y 航速监控器 P/N ASM-876		ASM-876-2387 Rev. -

在构型管理库中;

2) 软件构型索引文件(SCI)应包含软件加载过程和确认软件加载完整性的操作指南,或者有单独的文件描述软件加载和确认过程;

3) 在设备或软件用于适航验证试验前及设备装机前,应按照软件加载操作指南确认软件的标识和软件加载的完整性。

3.2 软件更改评审

型号研制过程中为保证各类试验的安全性以及有效性,全机各系统机载软件若发生构型变化,则各系统应在新版软件加载前,结合功能需求、更改内容等方面,在供应商的支持下从主机厂的角度组织进行更改评审。在评审中主要考虑以下问题。

1) 阐述更改的软件标识、软件需求、软件设计、软件源代码、软件可执行代码等,并证明有关软件更改符合DO-178B关于软件更改控制的要求;2) 测试用例或规程的更改影响评估;3) 分析软件更改对之前进行的符合性验证试验的影响;4) 分析软件更改对设备本身鉴定试验的影响;5) 飞机维护手册和飞行手册是否需要更改。

以上诸项应该被记录到软件更改评

审报告中以保证所有必须更改的内容都可见。

3.3 问题报告机制

问题报告(Problem Reporting)、追踪(Tracking)和纠正措施(Corrective Action)的目的是记录与软件计划和标准不符合的过程,记录软件生命周期过程输出的缺陷,记录软件产品的异常情况以确保以上这些问题得以解决。作为机载软件构型管理的重要部分之一,建立合理而规范的问题报告机制十分必要。

对于主机厂而言,从软件计划阶段开始就应建立型号的软件问题报告机制。一个完整的软件问题报告应该包括问题报告编号、问题报告名称、详细的问题描述、发生问题软件的版本号、相关的数据编号及版本号、问题报告的状态、发起人、相关责任人或部门、问题严重程度以及最终解决措施等。

从问题报告的发起到最终的关闭,需要有一个完整的控制流程。图1给出了一个典型的“主机厂—供应商”模式下的问题报告机制。

3.4 软件数据的归档和保存

软件数据是软件产品的有机组成部分,用以描述、规定、记录、报告软件工程的各项活动以及软件设计和实现的细节。主机厂应对所有的软件数据进行归档,使这些数据纳入到主机厂构型控制体系之中。同时,归档的软件数据应建一份新的拷贝进行异地保存,以确保数据不会因时间过长、意外灾害等情况发生而丢失或损坏。

主机厂应归档的数据包括飞机级软件计划或标准、软件需求文档(包括系统规范和接口控制文件)、软件详细设计文档、源代码、可执行目标代码、软件构型索引、软件完结综述等^[2]。

3.5 供应商控制

主机厂在机载软件构型管理活动中

对供应商的控制应考虑以下几方面。

1) 要求供应商依据RTCA/DO-178B编制其内部软件构型管理计划并提交主机厂批准;

2) 要求供应商按照主机厂批准的构型管理计划进行软件构型管理活动;

3) 通过一定方式监督和审核供应商的构型管理活动,判断其是否与构型管理计划相符合;

4) 供应商应将主机厂机载软件构型管理要求贯彻到其子供应商和转包商,并对子供应商和转包商的机载软件构型管理过程进行审核。

4 结论

民用飞机机载软件构型管理活动作为一个支持性过程,在整个软件生命周期过程中发挥着重要的作用,也是民用飞机在“主机厂—供应商”的工作模式下构型管理工作的难点。主机厂建立起一套完整、有效的机载软件构型管理体系,为合理、正确、有序地开展机载软件设计活动提供了必要的保障。作为对本文研究对象的实践,文中方案的内容已经在国产新支线飞机项目中得到运用,产生了良好的构型控制效果。 AST

参考文献

[1] RTCA/DO-178B, Software Considerations in Airborne Systems and Equipment Certification[Z]. RTCA/EUROCAE, 1992.

[2] Order 8110.49, Software Approval Guidelines[Z]. FAA, 2003.

作者简介

李林奇,工程师,主要从事机载软件管理方面研究。

陈一可,助理工程师,主要从事机载软件管理方面研究。

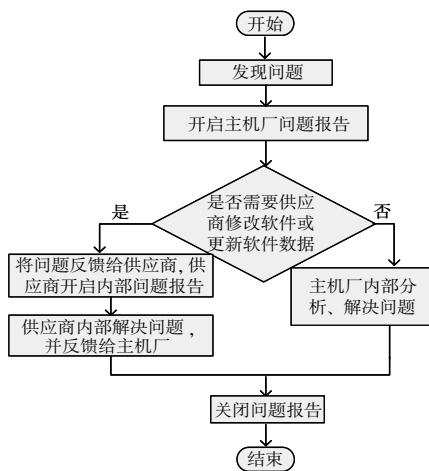


图1 “主机厂—供应商”模式下软件问题报告机制