

军用机载通信设备嵌入式软件的适航管理

随着计算机技术飞速发展及飞机型号性能要求的不断提高,现代飞机几乎所有重要功能都与软件有关,机载软件的应用规模飞速扩大,包括软件功能、结构和数据都愈加复杂。由于飞机经历的外部环境和内部运行状态千变万化,飞行安全和任务保障要求不断提高,使得机载软件具有实时性、高可靠性的特点,也因此对机载软件的管理提出了更高的要求。软件管理是机载设备中的关键技术之一,对软件进行适航管理是一种解决飞机安全性问题的方式,也是最基本的安全性要求。

1 适航的概念与创新实践

1.1 适航的概念与内涵

适航(Airworthiness)是来自民用航空的概念,1980年,美国科学院在《改进航空安全性》的报告中给出了定义:适航是“在预期的使用环境中和在经申明并被批准的使用期限之内运行时,航空器(包括其部件和子系统、性能和操作特点)的安全性和物理完整性”。

目前,对于民用飞机能否安全地完成各种客货运输业务,业界通常以其是否具有“适航性”来衡量,适航已经成为“安全性”一词在航空技术领域具有更深安全内涵的专用词语。

1.2 适航要求

我国的适航管理制度是参照美国的适航管理制度建立的,因此我国的机载设备适航管理技术要求也同样参照美国机载设备适航技术要求。美国机载设备适航技术要求是美国联邦航空局(FAA)颁发的“技术标准规定(Technology Standard Order, TSO)”,大部分TSO中的技术要求引用的是美国“美国机动车工程协会(SAE)”和美国“无线电技术委员会(RTCA)”的技术文件,例如计算机软件要求(RTCA DO-178B)、机载电子硬件设计的特别要求(RTCA DO-254)等。

我国的民用飞机机载设备适航技术文件要求是CTSO,但我国现在单独颁发的CTSO不是很多,进行机载设备适航合格审定时可以直接使用美国的FSO。

1.3 适航在军机上的创新

安全性是军用飞机的固有属性,但在军机研制中,安全性工作的开展相对比较薄弱,可供借鉴的经验较少,目前仅有安全性标准GJB900-1990《系统安全性大纲》,但这一标准可操作性不强,缺乏针对军机特色的具体技术和方法。在军机研制中引入适航理念,开展适航工作,是我国军机研制史上的一次大胆尝试和重大实践。适航条款的各项要求为军机的安全性设计提供了很好的借鉴。

2 软件适航管理

2. 1 软件适航性

软件适航性标准采用的是 RTCA DO-178B《机载系统和设备合格审定中对软件的要求》标准，该标准为机载设备嵌入式软件的研制提供指南，保证其按照适航要求的安全性实现其预期功能。

RTCA DO-178B 为机载设备嵌入式软件的开发过程提出了一系列相关的过程控制方法，包括软件等级划分、软件生命周期过程及之间的关系、软件验证过程、软件配置管理、软件质量保证等。机载设备研制单位按照 RTCA DO-178B 的要求对软件开发和各项活动分别实施规范化的工程管理、协调、监督和控制，保证机载设备嵌入式软件的整个开发过程有标准化管理，对每个要完成的目标输入都有对应的目标输出，根据各阶段要求输出对应的符合性文件、代码和记录。比如软件需求阶段，需要根据软件研制任务书和软件计划文档产生软件需求规格说明、软件评审报告及软件质量保证(Software Quality Assurance, SQA)记录等。

2. 2 软件工程化管理

软件工程化管理是软件适航管理中最重要的一项管理方法。机载设备嵌入式软件遵循适航工作管理规定及软件工程化大纲，对软件开发全过程和生命周期进行定义、规范、控制和管理，使软件的每一项活动都在受控状态下进行，保证了软件状态的一致性，并达到机载软件装机状态清晰、完整，确保飞行和维护保障的准确可靠。

2. 2. 1 软件产品的分析和设计

机载设备分析和设计阶段是软件研制的起始阶段，设备承研单位根据系统研制总要求、技术协议书的要求合理分配软、硬件功能和性能指标，确定设备软硬件体系结构，进行初步危险性分析并提出对设备的安全性要求，同时根据系统提出的功能、性能和信息接口要求，确定设备软件运行环境，编制软件研制任务书。

软件研制任务书是软件工程化管理和研发工作的关键一步，主要描述软件开发的目的是、目标、主要任务、功能及性能指标等要求，是后续开发阶段的必要输入文件，为软件开发提供了设计基础。

2. 2. 2 明确软件生命周期过程和软件等级

(1) 软件生命周期

机载设备嵌入式软件生命周期包括 3 个过程：软件计划过程、软件开发过程和软件综合管理过程。

为保证机载设备嵌入式软件的质量，保障飞机的安全，根据软件生命周期的 3 个过程继而细化为 10 个阶段进行控制，分别是：设备分析和设计阶段、软件计划阶段、软件需求阶段、软件设计阶段、软件编码阶段、软件集成阶段、软件验收与交付阶段、系统集成阶段、定型阶段、软件使用与维护阶段。各阶段之间

是一个相互补充并不断重复的过程，阶段产品是一个反复迭代、持续改进过程的结果。

(2) 软件等级

RTCA DO-178B 根据软件所导致的失效状态类别，把软件等级划分为 A、B、C、D、E 五个等级，决定了设计保证活动的严格程度。软件等级划分如表 1 所示。

若机载设备嵌入式软件根据软件失效状态分析决定了软件等级为 C 级，则软件研制工作就按照软件适航要求中 C 级在每一软件生命周期过程中的目标要求和符合性方法进行，形成相应的软件生命周期文档。

2. 2. 3 软件配置管理

软件配置管理 (Software Configuration Management, SCM) 非常重要，它关系到软件研制工作的有效性、软件产品的可用性和可信性。SCM 是标识和确定系统或设备中软件配置项的过程，在整个软件生命周期内控制这些软件配置项的发放和更改，记录并报告配置的状态和更改要求，验证配置项的完整性和正确性。其中，软件配置项即软件产品在不同时期的组合，包括在软件生命周期各阶段产生的各种形式和各种版本的文档、程序和数据等。软件配置项随着开发工作的进展而不断变化。

(1) 制定软件配置管理计划

机载设备实施初期依据该设备的软件开发计划进行配置策划，明确配置管理内容，以便有计划地开展配置管理工作。同时根据软件开发计划等顶层文件确定配置管理的详细要求，由软件配置管理员制定软件配置管理计划初稿，包含配置管理组织、标识规定、软件配置项、基线定义、更改控制、状态报告和版本管理等。评审通过后，正式作为该设备配置管理活动的依据。

(2) 基线

基线 (baseline) 是软件生命周期各阶段末尾的特定点，也称为里程碑。基线是经过正式审核与同意的规格说明或产品，可用作下一步开发的基础。基线确定后，只能通过正式的更改管理办法变更。机载设备软件生命周期各阶段基线划分如图 1 所示。

(3) 变更管理

满足 RTCA DO-178B 要求的软件研发过程中，所有基线变更都应在有效的控制下进行。

机载设备嵌入式软件因为其开发难度和开发周期，在软件生命周期的各阶段是很容易出问题的。一旦发现问题，不管是文档还是代码，均需要通过变更来满足系统需求和相应的适航要求。软件变更前应提出申请，经过严格审批后才能实

施变更，防止随意修改造成的失控和混乱，导致软件工作的损伤。同时对软件更改还建立了问题报告单、更改申请、更改报告、问题归零、出 / 入库的可追踪管理制度。更改后的软件产品经过评审和审批后再纳入配置管理。

2. 2. 4 质量控制和监督

满足 RTCA DO-178B 要求的软件研发过程中，软件质量保证活动 SQA 是必不可少的。SQA 通过保证研制过程中符合批准的软件计划及标准，确保软件生命周期中的产品符合软件需求提供的置信度。

机载设备依据软件研制任务书及软件需求开展 SQA。在设备启动初期，软件质量师依据系统下发的软件质量保证大纲编制 SQA 计划，提出软件生命周期各阶段的质量管理要求，以持续监控整个软件生命周期过程并评审软件产品。

软件生命周期各阶段质量保证活动的输出产物为 SQA 记录，包括 SQA 评审或审核报告、软件符合性评审记录等，跟踪并确保评审问题或不符合项的解决和闭环。

同时，SQA 还对各个阶段的软件配置管理活动进行监督和检查，形成配置审核记录；对系统集成阶段设备装入分系统或系统联试期间发现的软件问题的纠正情况进行监督和检查，保证问题归零。

2. 2. 5 软件文档资料

软件文档是软件的重要组成部分。文档内容是根据软件开发过程中各阶段的工作任务而产生的，主要记载各阶段的主要活动信息和要求。

规范、细致地编制、管理和维护文档，对软件工程化管理具有非常重要的意义。

机载设备根据软件文档编制要求进行软件文档的编写，保证交付的文档完全符合工程要求且准确、完整和规范。交付的文档同时作为软件配置项纳入配置管理，严格控制文档的更改。

2. 3 软件设计和实现

2. 3. 1 软件设计遵循原则

机载设备嵌入式软件遵循以下设计原则：

- (1) 严格执行数字式电子类机械设备(软件部分)的研制通用要求；
- (2) 软件研制过程中，将可靠性和安全性放在首位；
- (3) 采取分层次、模块化设计，方便进行裁减和升级；

(4)减小应用软件和底层处理器硬件相关性，通过提供标准的接口规范，分离应用软件和特定硬件相关的代码。

2. 3. 2 软件设计和实现

(1) 设计方法

软件采用多处理器的分布式结构，以实时分布式方式并行运行在各处理器上。软件主要采用适合嵌入式软件的结构化方法，自顶向下按功能划分成几个能独立工作的软件模块进行开发和管理。

(2) 实现方案

各个功能模块软件驻留和运行于相对独立的 CPU 上。在各功能模块中设计接口控制管理层，使应用软件独立于硬件接口，既有利于隔离模块故障，又可以屏蔽硬件差异，将硬件选型对软件的影响降低到最小，灵活应对硬件变化，最大限度保护软件资源，有利于软件维护、升级、测试和系统可靠性的提高。

(3) 编程语言

现阶段计算机软件编程采用的语言主要是汇编语言和高级语言。目前，在航电系统上采用的高级语言主要为 C，C++。

鉴于高级语言在应用上的一系列问题还有待解决，故常将汇编语言与高级语言混合使用。比如，结合机载设备软件运行的 CPU 器件特性，在对中断及 I / O 口等寄存器进行初始化或者对 CMD 文件进行寄存器的配置时采用汇编语言，对设备功能处理方面采用 C / C++。

2. 4 软件验证

2. 4. 1 定义

RTCA DO-178B 对验证(Verification)的定义是：验证是软件开发过程和软件验证过程两者结果的技术评估。验证贯穿于软件开发过程中，包括了对需求的验证、对设计的验证、对代码的验证、对集成的验证及对验证过程的验证，目的就是检测和报告在开发过程中形成的错误。机载设备根据系统软件验证和确认要求及评审细则等首先形成软件验证计划，然后以软件验证计划、软件需求、源代码及可执行目标代码等作为输入 / 输出软件验证用例和规程、软件验证结果。

2. 4. 2 方法

不同于以往国军标如 GJB2786-1996 等，GJB2786 认为测试的本身就是保障的手段，着重从测试的方法入手，而 RTCA DO-178B 是将测试定义为验证的一部分，验证的方法包括评审、分析和测试，偏重于对整个验证过程的本身与活动，且明确验证是保障的手段。

(1) 软件评审

软件评审作为软件验证的一项重要活动，是软件质量保证的重要一环。

为保证嵌入式软件的研制质量，机载设备遵循系统制定的软件评审细则，规范软件评审活动。同时根据软件等级要求，对软件各阶段的工作成果进行符合该等级的评审要求和评审方式(外部评审或内部评审)。

为保证嵌入式软件的研制质量，在机载设备软件研制初期，在软件研制任务书、软件开发计划、软件验证计划中对各阶段生产的软件产品评审均进行了明确规划，按照质量要求，所有外部评审均有型号总师单位和军代表参加。

评审时，提交评审的所有文档必须已经通过逐级审签。每次评审后必须形成评审报告，评审通过后将其和相关软件产品纳入配置管理。阶段产品必须进行并通过评审。

机载设备在软件生命周期中设立了一系列阶段评审点：设备分析和设计阶段、软件计划阶段、软件需求分析阶段、软件设计阶段、软件实现(编码与单元测试)阶段、软件集成阶段(软件集成测试、系统测试)、软件验收与交付阶段。

评审针对各阶段的工作成果。在各阶段工作成果评审通过后才允许建立相应的基线，才能进行后续阶段的开发工作。

(2) 软件测试

软件测试是保证软件质量的重要手段，完整的软件测试工作贯穿整个软件生命周期，它包括两方面的含义：一是软件开发的不同阶段都有软件测试工作；二是软件测试工作的各个步骤分布在整个软件生命周期中。

为保证研制质量，按照软件测试流程，机载设备嵌入式软件开展了软件测试活动。在设备分析和设计阶段，遵循系统制定的软件测试细则，依据软件研制任务书编写软件测试计划，确定软件测试范围、目的、测试指标、进度安排及最终形成产品等，根据软件等级明确要求测试类别和测试方法及测试技术要求。

软件测试计划通过评审后即刻开展测试活动，在计划阶段、需求阶段和设计阶段主要执行了测试策划、测试设计和实现；从编码阶段开始进入测试执行，直到软件集成阶段系统测试结束进行测试总结。在测试工作

中，机载设备根据测试执行情况对上述四个过程反复迭代(包括软件回归测试)，直至达到测试要求为止。

(3) 一般测试要求

软件测试类别主要为单元测试、部件测试、配置项(集成)测试、系统测试。

软件测试方法主要分为白盒测试和黑盒测试。

软件单元测试时，采用代码审查、静态分析方法和白盒测试的方法完成；软件部件、软件配置项测试和系统测试测试时，均采用了黑盒测试方法辅助以白盒测试的方法完成。

(4) 机载软件测试的特点

机载设备软件为机载嵌入式软件，机载嵌入式软件具有以下几个显著特点：

①软件和硬件结合紧密，软件脱离特定运行环境是肯定无法运行的，软件失效与硬件故障有时难以区分，甚至互相干扰；

②开发环境和实际运行环境不同；

③机载软件实时性强；

④机载软件属于安全关键软件。

目前机载设备嵌入式软件的测试工作也仅限于对纯软件的测试，但是，嵌入式软件的前两个特性给软件测试提出了新问题，比如软硬件错误的界定、硬件特性对软件测试的影响等。

机载嵌入式软件的第三个特性说明了机载软件是实时多任务处理软件。如机载设备需要在同一时间段处理多个任务，为了不漏掉任一任务的处理，软件设计了中断握手管理。软件测试时就对中断握手管理执行的语句进行了验证。

机载嵌入式软件的第四个特性说明了机载软件若性能不可靠将带来灾难性后果，因此对其可靠性和安全性要求很高。在机载软件设计时均采用了一些提高可靠性、安全性的先进技术，比如容错技术、安全监控等，在软件测试中则充分考虑设计测试用例对这些软件语句进行了验证。

机载设备软件的最后一项测试即飞行测试，也就是我们常说的试飞阶段。试飞测试是在飞机飞行中进行的一些特殊测试，包括根据适航要求进行的适航试飞。通过上述方式的软件测试，将大大保证军用航电系统机载通信设备软件有较高的置信度。

(5) 软件测试结果

软件测试过程中即软件生命周期各阶段的测试产物主要包括各级(单元级、部件级、配置项级、系统级)软件测试计划、测试说明、测试报告、测试问题报告、测试总结报告及评审结果等。软件测试结果在生命周期各阶段均进行了管理、跟踪和控制，并将其纳入了配置管理。

3 、 结语

军机嵌入式软件适航工作以提高军机的安全水平为宗旨，不脱离现有军机研制管理模式，不改变军机研制流程，在技术上充分借鉴，在管理上大胆创新，在

引入适航理念和方法的过程中不断积累经验，探索形成规范的、有中国特色的军机嵌入式软件研制适航工作途径，推动军机软件研制质量与安全水平的不断提高。

OFweek电子工程网