综合化航空电子系统软件接口研究

崔西宁[1,2] 胡林平[2] 叶 宏[2] 白晓颖[3]
(西安电子科技大学计算机学院 西安 710071)[1] (中国航空计算技术研究所 西安 710068)[2]
(清华大学计算机科学与技术系 北京 100084)[3]

摘 要 综合化航空电子系统软件对系统的综合性能具有较高的要求。全面分析了综合化航空电子系统的性能需求,定义了综合化航空电子系统性能评估模型,首次对综合化航空电子系统进行全面评估,建立了综合化航空电子系统体系结构和功能软件的评估模型,分析和对比了综合化航空电子系统软件现有接口标准规范。在航空电子系统软件开发中将多个标准结合起来参考使用,将有利于提高机载软件的重用性、移植性、安全性和可靠性。

关键词 综合化航空电子系统,ARINC653,ASAAC,APEX,APOS
中图法分类号 TP311 **文献标识码** A

Research on Software Interfaces of Integrated Avionics System

CUI Xi-ning[1,2] HU Lin-ping[2] YE Hong[2] BAI Xiao-ying[3]
(School of Computer and Science, Xidian University, Xi'an 710071, China)[1]
(Aeronautics Computing Technique Research Institute, Xi'an 710068, China)[2]
(Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China)[3]

Abstract Avionics system requires aviation tasks to obtain more comprehensive capabilities. A deep analysis was made on the requirements of avionics system software, the definition of the Framework for Evaluating Avionics System Capabilities was proposed. The comprehensive capabilities evaluating was firstly introduced into the integrated avionics system, and the framework of the capabilities evaluating was established. Based on these, the analysis and comparison of the current interface specifications were presented and the evaluation result of these specifications was illustrated. It is benefit for the improvement of the reusable, transplantable, secure and available capabilities of the avionics system software to combine the merits of the several specifications.

Keywords Integrated avionics system, ARINC653, ASAAC, APEX, APOS

随着航空电子技术的快速发展,原有的独立式、联合式航空电子系统不能够满足现代复杂的军事和民用需求,综合化航空电子系统得到了广泛关注[1,2]。综合化航空电子系统具有资源高度共享、数据高度融合和软件高度密集等特点。软件是航空电子系统的核心,飞机每一个动作的完成都离不开软件的支持,80%的航空电子功能由软件实现[3-5]。但是软件规模的急剧膨胀会降低软件的可靠性,资源高度共享容易受到非法访问,系统容易受到恶意代码侵蚀,综合化航空电子系统可信软件面临巨大的挑战[6-9]。

综合化航空电子系统可信软件一直受到美国、欧洲各国以及学术界的广泛关注。美国和欧洲分别从软件可靠性和系统安全性角度制定了一系列的标准和规范。在软件可靠性方面,为规范软件开发行为,保证软件质量,美国于1992年制定了Do-178B标准[10,11],2002年制定了空管软件标准Do-278;欧洲空中导航安全机构(Eurocontrol)将Do-178B与软件能力成熟度模型结合,在2003年形成了空中导航安全机构强制性标准ESARR4[12]。在系统安全性方面,法、德、英和美政府建立了联合标准航空电子结构委员会,为2005年以后新设计和改型的飞机航空电子结构制定一组开放式标准、概念和指南ASAAC(Allied Standard Avionics Architecture Council)规范,其中规范了综合化航空电子系统安全体系结构和相关安全技术[13,14]。英国国防部对ASAAC进行修订,形成了自己的标准。北约也对ASAAC进行改版,开展了NATO STANAG 4626计划[15]。

美国航空电子工程协会AEEC于1997年为航空民用飞机的模块化综合航空电子系统定义的一种应用程序接口标准—航空电子应用软件标准接口(Avionics Application Software Standard Interface),以ARINC653规范的形式发布,其应用程序与操作系统的接口定义为APEX(application/execution),即应用执行接口[16]。ASAAC规范中定义了应用到操作系统的接口APOS(Application to Operating System Interface)。

到稿日期:2010-03-19 返修日期:2010-06-14 本文受国防基础科研项目(C0520061364),航空科学基金(2008ZC31001)资助。
崔西宁(1964—),男,博士生,研究员,主要研究方向为并行分布式操作系统、实时控制与容错技术、信息安全技术等,E-mail:cuixining@tom.com;胡林平(1972—),男,高级工程师,主要研究方向为机载嵌入式操作系统、软件工程等;叶 宏(1961—),男,研究员,主要研究方向为机载嵌入式操作系统、软件测试、软件工程化等;白晓颖(1973—),女,副教授,主要研究方向为软件工程、机载系统软件技术等。

根据航空任务的执行具有确定性、可预测和可控性的需求，本文提出综合化航空电子系统性能评估模型，从功能层面、管理层面和系统层面评估综合化航空电子系统的性能，希望通过这种评估模型的研究，能够对现有的 APEX，APOS 和 GOA 等航空电子系统软件标准接口进行详细分析和全面评估，为我国航空电子系统的标准规范的制定和发展提供技术支持。

1 综合化航空电子系统的性能需求

机载软件在现代作战飞机中担负着从通信、导航、显示控制、信息/数据处理、飞行控制到火力控制、外挂管理、武器投放、电子战等为数众多的飞行任务和作战任务。飞机每一个动作的完成都离不开机载软件的支持，飞行员的每一个作战意图也必须依靠机载软件才能完成。据统计，新一代战斗机（如 F35）上的机载软件的代码已达到 800 万行。战斗机的航空电子系统是一个高度信息化的系统，不仅要处理飞机内部传感器的信息，而且要处理更多的飞机外部（如预警机）信息。新一代飞机航空电子系统由于软件密集，大大地增加了软件复杂性，从而引发了软件安全性与可靠性的降低。为了保证程序的可靠性，提高软件的可维护性和可移植性，有必要将航空电子应用软件与机载操作系统间的接口标准化、规范化，使基础软件与应用软件相对隔离、系统设计者与子系统设计者隔离，实现软件的模块化设计。我们充分考虑综合化航空电子系统的特殊性和复杂性，对系统提出了 7 个需求指标，从多方面描述系统的性能需求。

（1）可重用性

使用应用软件与机载操作系统接口可以为航空电子系统开发出可重用的应用代码。当一个程序代码被重用时，应用软件与机载操作系统接口可以减少所需的工作量。

（2）可移植性

应用软件与机载操作系统接口使软件移植很简便。如人们期望为一种专门的飞行器开发的应用软件只花费最小的努力就可以用于另外的飞行器类型上。

（3）可扩展性

系统能够对高新技术的插入提供支持，并支持系统规模的可变性。

（4）可维护性

能够对系统的健康状况进行监控，对系统的故障可以检测、隔离和维护；根据任务对系统进行动态配置和优化。

（5）互操作性

互操作主要是指与本地和远程系统的其它应用可进行互操作，以及通过简化用户移植性可在用户间进行互操作。航空电子系统应该能够提供安全和快捷的互操作接口，方便用户和系统功能的交互操作。

（6）可靠性

能够为航空电子系统提供稳定可靠的运行环境，利用分区分时技术对系统突发的故障能够进行危害控制，限制故障扩散，并能够实现局部功能的重启。

（7）安全性

能够对航空电子系统中各种实体进行强身份验证，为系统中的数据提供机密性、完整性和认证性等保护。

2 航空电子软件标准接口概述

2.1 ARINC653 标准及 APEX 接口

1997 年 1 月，美国制定了综合化、模块化航空电子应用软件标准接口（ARINC653），对综合化航空电子操作系统的需求进行了定义，提出了时空分区（Partition）的思想，解决了综合化后各个任务间隔离与资源时间分配问题，并明确定义出了机载软件的三层结构（应用层、操作系统层、模块支持层），使应用软件与操作系统、操作系统与硬件接口标准化，使硬件、操作系统、应用软件的升级成为可能，确保了应用软件的安全，使得航空电子应用软件安全、可靠地工作在一种抽象的工具中，标准经过修改与验证，于 2005 年完成最终版本。ARINC653 的主要目的是：

（1）向未来的航空电子设备制造商指出制造新设备所必需考虑的意见，而这些意见是航空技术人员在业界的基础上经过了反复思考的；

（2）对新装备的设计加以引导并且在不严重影响创新的前提下，最大可能的标准化会影响设备互换性的物理和电气特性。

ARINC653 详细规定了应用软件与执行软件之间的接口，这些接口在某种程度上描述了相应的操作系统功能。ARINC653 不是操作系统（OS）或硬件的规格说明，但它假定由 OS 或硬件提供支持。ARINC653 定义了分区的概念，一个分区基本上等同于单一应用环境下的一个程序，它由数据、自己的代码、配置属性等组成。对大的应用，一个单一的应用可划分成多个分区。

ARINC653 定义的应用与操作系统之间的接口为 APEX，从应用的角度看，APEX 接口可以被看作一种高级语言的规范说明；从 OS 的角度看，APEX 接口可以被看作参数和入口机制的定义。APEX 也可以包括一层，把高级语言翻译成适当的入口机制，这种翻译直接与 OS 实现及硬件平台有关，也可能与应用软件使用的编译程序有关。如果使用了库程序，库程序需要打包进应用代码，保持强分区性。图 1 显示了 ARINC653 的核心模块组成关系。

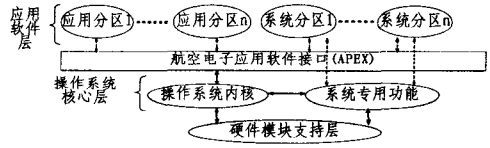

图 1 ARINC653 的核心模块构成关系

APEX 接口为应用软件提供了通用的逻辑环境。这种环境使得独立开发的软件可以在同一硬件上一起执行。APEX 接口的首要目标是为应用软件和综合化、模块化航空电子系统中的 OS 提供一个通用的接口。

2.2 ASAAC 规范及 APOS 接口

法、德、英和美政府建立了联合标准航电结构委员会 ASAAC，1997 年开始为 2005 年以后新设计和改型的飞机先进航电结构制定一组开放式标准、概念和指南。其目标是形成应用于未来军用飞机的嵌入式航空电子系统的核心处理的标准。

ASAAC 规范为欧洲未来战机的航空电子系统软件从结构体系上、功能上、各层接口标准上规定了详细的要求，如

ASAAC 将航电软件分为了三级(飞机级 AC、综合区级 IA、资源元素级 RE),在安全保障方面提出了健康监控 HM、故障管理 FM 和配置管理 CM,从而使系统的容错透明性增强。尤其值得重视的是,为了确保航空数据的安全,解决综合化后的安全隐患,专门在安全方面提出了安全性管理规范,解决不同关键级别的飞行任务的操作权限、数据的加密、认证与授权等问题,使综合化数据融合更加安全,防御了外界的非法侵入。

ASAAC 包括 5 个标准 7 个指南,分别是结构标准、软件标准、通用功能模块标准、封装标准、网络和通信标准以及系统管理指南、故障管理指南、系统初始化与下电指南、系统配置/重构指南、时间管理指南、保密指南和安全指南。5 个标准 7 个指南完整地描述了综合化、模块化航空电子核心处理机的方方面面。

体系结构标准定义了新一代综合化、模块化航空电子核心处理机的体系结构;软件标准确定了设计和开发模块化航空电子系统软件结构的统一需求;网络和通信标准确定了在定义一个符合 ASAAC 标准的网络时要考虑的问题。ASAAC 标准规定独立于具体技术,包括网络技术;通用功能模块标准定义了通用功能模块,并制定了设计和构造通用功能模块的统一需求;封装标准确定了符合 ASAAC 标准的模块化航空电子系统封装的统一需求,定义了模块的物理接口,包括机械、冷却、电源分布、相互连接及电磁标准;指南是对标准的补充。

ASAAC 把软件分为三个层,应用层、操作系统层和模块支持层,称为三层栈结构 TLS。ASAAC 的软件结构适用于综合化航空电子系统的分布式结构,其软件结构模型如图 2 所示。应用层包括应用程序、应用管理程序(AM)。操作系统层包括通用系统管理(GSM)、核心操作系统(OS)。模块支持层是与硬件相关的软件部分。

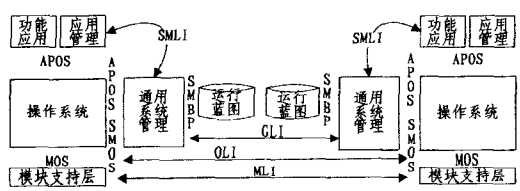

图 2 ASAAC 软件结构模型

2.3 GOA 标准及接口规范

新一代技术提供了足够的信息传输带宽、处理速度和存储能力,支持模块化、容错/重构、柔性降级、资源共享、二级维修、数据融合、座舱智能化,支持多传感器的多工作模式之间的协调和管理等,使航空电子跨入了一个崭新的时代。如何使已经实现的机上高度综合及多任务的机上航空电子系统适应未来战略发展的要求,成为需要面对的严峻问题。为此,SAE AS4893-5 GOA 工作组提出了通用开放式结构框架概念。GOA 框架用于规范系统顶层结构设计,对航空电子系统所需的接口进行分类,这种分类被认为是开放式系统标准向军用航空电子发展的一个至关重要的部分。

GOA 架构如图 3 所示。GOA 框架规定了软件、硬件和接口的结构,在不同应用领域中实现系统功能。GOA 框架规定了一组接口,规定 GOA 框架的最重要原因是建立确定关键组件及这些组件之间接口的框架,这些接口的确定用于支持可移植性和升级,以适应技术过时、功能的增加和技术的更新。

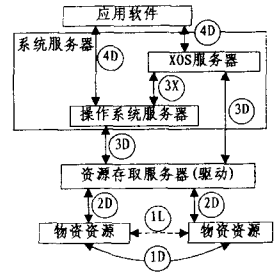

图 3 GOA 功能架构图

系统由逻辑节点(或模块)组成,节点可用作数据处理,包含一个或多个处理器。节点由包括电子元器件和电路的组件组成。典型的航空电子系统由多个节点组成,可通过底版总线对每个节点寻址,与处理功能节点相关的框架称之为 GOA 栈。

3 航空电子系统的性能评估

高度综合的航空电子系统主要可以分为 3 个层面,首先是构成软件系统的功能模块所组成的功能层面,其次是软件系统架构的管理层面,最后是软件可用性的系统层面。我们分别从 3 个层面总体评估航空电子系统软件标准接口的性能,共采用 7 个性能属性来评估航空电子系统的整体能力,如图 4 所示。在功能层面,我们考虑功能模块的性能需求,需要满足可重用性和可移植性;在管理层面,我们考虑系统整体的可管理性,需要满足可扩展性、可维护性和互操作性;在系统层面,我们考虑整体系统软件的可用性能,需要满足高可靠性和安全性。

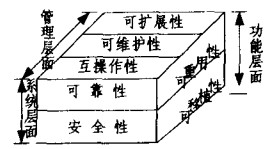

图 4 航空电子系统的性能评估

在表 1 中,我们对 3 种系统标准接口进行了对比,从对比的结果可以看出,APEX 接口标准是针对单机系统制定的,因而可扩展性稍差一些;而 APOS 接口标准主要针对分布式系统而制定,但其安全保护功能稍差一些;对于 GOA 架构只给出了系统结构分层和接口分类,没有详细的接口定义,总体在系统的可用性和可管理方面性能较弱。

表 1 各种标准接口的性能对比

	APEX	APOS	GOA
可重用性	好	好	好
可移植性	好	好	好
可扩展性	一般	好	一般
可维护性	一般	好	一般
互操作性	好	好	一般
可靠性	好	一般	差
安全性	好	一般	差

4 各种标准接口的性能对比

4.1 ARINC653,ASAAC 及 GOA 软件架构

SAE AS4893《通用开放式结构(GOA)框架》标准是一项重要的开放式系统结构标准,不但在美国被作为定义结构的

标准采用，也被欧洲航空电子系统标准化技术委员会结构工作组作为结构评估的参照模型。

SAE AS4893《通用开放式结构(GOA)框架》的模型概念主要是结构分层和接口分类，用于将开放式系统结构应用到航空电子软、硬件系统设计中以确定接口的分类。GOA 框架规定了软件、硬件和接口的结构，以便在不同应用领域中实现系统功能。但 GOA 框架标准只给出了层次和接口划分的要求，没有具体给出接口定义。

ARINC653，ASAAC 以及开放式系统架构标准 GOA 的软件架构及接口关系如图 5 所示。

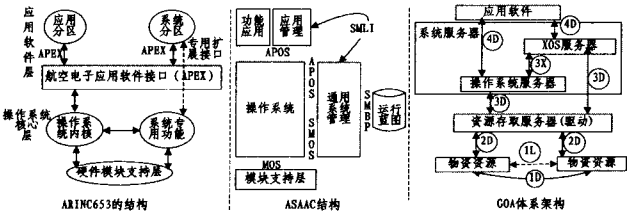

图 5　各标准的接口示意图

3 个软件结构对一般应用都提供了相应的接口(ARINC653 的 APEX，ASAAC 的 APOS，GOA 的 4D)，同时，对特殊服务也提供了专门的接口(ARINC653 的扩展接口，ASAAC 的 SMOS，GOA 的 3X)。

表 2 给出了 3 个软件结构的应用与 OS 的两类接口的对应关系，要注意的是在 GJB5357-2005《航空电子应用软件接口要求》和 ARINC653 标准中没有对系统分区的专用扩展接口给出定义，为了实现分布式系统管理，在行业标准《航空电子应用软件接口应用指南》中对系统分区提供了专门的扩展接口。

表 2　各标准的接口对应关系

接口类型	GJB5357	ASAAC	GOA
应用与操作系统的接口 API	APEX	APOS	系统服务与应用软件直接接口：4D
专用接口	系统分区与 OS 的接口：专用扩展接口	通用系统管理与 OS 的接口：SMOS	操作系统服务与扩展操作系统服务直接接口：3X

4.2　APEX 与 APOS 的归类对比

APEX 接口与 APOS 接口的归类对比见表 3。

表 3　APEX 接口与 APOS 接口归类对比

	ARINC653		ASAAC	
接口功能	APEX	专用扩展接口	APOS	SMOS
分区管理	分区管理	分区管理扩展	无	进程管理服务
线程管理	进程管理	进程管理扩展	线程管理	线程管理服务
时间管理	时间管理	时间管理扩展	时间管理	时间配置服务
分区通信	信号量、事件等	无	信号量、事件	无
健康管理	健康监控	健康监控接口扩展	故障处理	故障管理服务
文件服务	无	文件管理接口扩展	文件处理	无
数据传输	无	数据传输管理接口扩展	无	VC 配置服务，网络配置服务
安全管理	无	无	无	信息安全管理服务
日志管理	无	无	无	日志管理服务

通过对 ARINC653 的 APEX 接口与 ASAAC 的 APOS 接口进行比较，可以得出如下的结论：

(1)分区(或进程)管理：ARINC653 只有获取分区状态和设置分区工作方式两个服务；ASAAC 具有较全的进程管理服务；

(2)进程(或线程)管理：ARINC653 和 ASAAC 都有较完备的进程(或线程)管理功能；

(3)时间管理：ARINC653 和 ASAAC 都有一定的时间管理功能；

(4)存储区管理：ARINC653 和 ASAAC 均不提供动态存储区管理；

(5)消息队列：属于分间内通信，只 ARINC653 提供了消息队列机制。ASAAC 可使用分区间通讯机制实现同样功能；

(6)黑板：属于分间内通信，只 ARINC653 提供了黑板机制；

(7)信号量：属于分间内通信，ARINC653 和 ASAAC 均提供了信号量机制；

(8)事件：属于分间内通信，ARINC653 和 ASAAC 均提供了事件机制；

(9)分区间通信：ARINC653 和 ASAAC 分别提供了各自的分区间通信机制。ARINC653 采用端口机制；而 ASAAC 采用虚通道机制；

(10)健康监控或故障管理：ARINC653 和 ASAAC 均具有健康监控或故障管理；

(11)其它：ASAAC 具有文件管理、电源转换、调试、进程(线程)监控、虚通道配置、网络配置、通讯监控、信息安全性、自测试、CFM 信息、CFM 资源管理、日志管理等管理功能；ARINC653 没有定义这些管理功能。

4.3　APEX 与 APOS 的功能分析

ARINC653 标准和北约 ASAAC 规范都是面向航空电子系统(可以说是机载领域)标准，而 APEX 与 APOS 正是这两个标准对功能应用与操作系统的接口定义，它们都是通过接口调用完成功能应用对系统资源的享用，有很多相似之处。功能应用与操作系统的接口本质上反映的是对操作系统的功能的要求，现在从如下几个方面进行分析比较：

(1)功能上比较

ARINC653 标准是面向单模块设计的，强调分区的时空隔离、系统运行的确定性；而北约 ASAAC 规范是针对整个航空电子系统设计的，考虑的是分布式航空电子系统的软件架构、容错重构、时间管理等。

设计理念的不同导致功能的差异，ARINC653 标准针对一个模块，是不可配置的，即不能在运行的过程中改变配置，虽然对跨模块的通讯以及系统分区进行了专门说明，提出要对接口扩展，但没有具体定义出扩展接口；ASAAC 规范是针对分布式系统的，为了实现对分布式系统的管理，专门详细定义了 SMOS 接口。航标依据 ASAAC，对 GJB5357 的 APEX 接口进行了扩展，但不全面。

对硬件资源访问最终是通过 MSL 软件实现的，ARINC653 标准对 MSL 没有明确要求，可以不遵守标准，不支持重构。若要实现航空电子系统的容错重构，还需要增加接口；而 ASAAC 规范对 MSL 有明确要求，提出了 MOS 接口，并支持重构。

(2)健康监控

两个标准对健康监控(或故障管理)的的级别和范围不同，ARINC653 标准提出了 3 级管理：进程级、分区级和模块

级健康监控。ASAAC规范提出了4级故障管理:进程级、模块级、综合区级和飞机级。

(3)通讯方面的比较

ARINC653标准对通讯处理分为分区内、分区间,可以跨模块通讯,分区内通讯除采用端口外,还可以使用队列和黑板机制;分区间通讯采用端口机制,分为采样端口和队列端口两种方法。APEX提供了相应的系统调用函数,ARINC653标准对通讯底层实现没有具体规定,但接口丰富,通讯效率高。

ASAAC规范对通讯进行了严格的定义,明确提出虚通道机制,分为4个层次,应用层采用本地虚通道(LVC),操作系统层为全局虚通道(GVC),在模块支持层有传输连接(TC)和接口(IF),在IF处才考虑具体的通讯网络实体(FC网络、AFDX网络、VME等),通讯网络在蓝图中配置,应用软件不用改变程序代码,就可以把软件从一个模块迁移到另一个模块运行,有利于容错重构的透明性。

ARINC653标准和ASAAC规范对通讯的对应关系见表4。由于ARINC653标准对容错重构支持不够,如果需要容错重构就需在底层软件做改动。

表4 ARINC653和ASAAC对通讯处理的比较

层次	ARINC653	ASAAC	说明
应用层	端口	LVC	功能一致,但ARINC653配置端口时要指定通道
操作系统层	VC	GVC	功能一致
MSL层	驱动程序	TC IF、驱动	ARINC653没有TC、IF,为支持容错重构,需改造

(4)分区与进程

ARINC653标准对软件的处理单位为分区和进程,而ASAAC是进程和线程,它们有对应关系,但也有不同之处,主要为ARINC653标准具有分区时空隔离机制,而ASAAC规范则没有。ARINC653标准和ASAAC规范关于分区与进程的比较见表5。

表5 分区与进程的比较

ARINC653标准	ASAAC	说明
分区	进程	ARINC653对分区按时间片调度;ASAAC静态调度
进程	线程	功能一致

(5)系统配置

ASAAC规范支持动态配置,可以创建分区,改变逻辑配置等;ARINC653标准则不行。ASAAC配置灵活,但运行的开销相对大些。

结束语 综合化航空电子系统软件对重用性、移植性、安全性和可靠性具有较高的要求。本文定义了综合化航空电子系统性能评估模型,首次对综合化航空电子系统进行了全面评估,建立了综合化航空电子系统体系结构和功能软件的评估模型,分析和对比了综合化航空电子系统软件现有接口标准规范。ARINC653标准和ASAAC规范都是面向航空电子系统的相关标准,都规定了功能应用与操作系统的接口,功能基本一致,但也有差异,主要是ARINC653标准针对单机,ASAAC规范是面向分布式航空电子系统,而GOA架构由于只给出了结构分层和接口分类,因此给出的性能分析结果比较弱化模糊。

建议将ARINC653标准和ASAAC规范结合起来应用到实际的软件研发工作中,操作系统采用具有分区时空隔离机制的操作系统,应用软件与机载操作系统接口采用ARINC653标准,但为了实现对分布式的管理、容错重构以及分布式通讯,必须扩展接口。扩展接口参考ASAAC规范。这样,对新一代综合化模块化航空电子系统软件的开发具有很好的指导意义,有利于提高机载软件的重用性、移植性、安全性和可靠性。

参考文献

[1] Boleat C, Colas G. Overview of soft errors issues in aerospace systems, On-Line Testing Symposium[C]// 11th IEEE International IOLTS. Saint Raphael France, 2005: 299-302

[2] Harkness D, Taylor M S, Jackson G S, et al. An Architecture for System-Wide Information Management[C]// DASC'06. Portland, 2006: 1-13

[3] Robinson R, Li M, Lintelman S, et al. Electronic Distribution of Airplane Software and the Impact of Information Security on Airplane Safety[C]// The 26th International Conference on Computer Safety, Reliability, and Security. SAFECOM, Nuremberg, Germany, 2007: 28-39

[4] Black R, Fletcher M. Simplified Robotics Avionics System: An Integrated Modular Architecture Applied Across a Group of Robotic Elements[C]// DASC'06. Portland, 2006: 1-12

[5] McElhone C. Soft computations within integrated avionics systems[C]// Proceedings of the IEEE NAECON. Dayton ohio, 2000: 27-34

[6] Trevino L C, Brown T. Soft computing for propulsion control, Digital Avionics Systems[C]// DASC'01. Daytona, 2001: 3-8

[7] van Oorschot P C, Somayaji A, Wurster G. Hardware-Assisted Circumvention of Self-Hashing Software Tamper Resistance [J]. IEEE Transactions on Dependable and Secure Computing, 2005, 2(2): 82-92

[8] Kuehl C S. A process direction for common avionics developments using commercial hardware and software components: the avionics systems engineering challenge[C]// DASC'97. California, 1997: 64-69

[9] Beeby M. Aviation quality COTS software: reality or folly[C]// DASC'02. Irvine CA, 2002: 1-10

[10] Jacob J M. High assurance security and safety for digital avionics[C]// The 23rd Digital Avionics Systems Conference, DASC 04. Salt Lake City, 2004: 4-9

[11] Levine S, Levine L J L. An onboard pilot and remote copilot for aviation safety, security & savings[C]// DASC'07. Columbia MD, 2007: 11-23

[12] KleidermacherDN. IntegratingStaticAnalysisintoaSecureSoftware Development Process[C]// 2008 IEEE Conference on Technologies for Homeland Security. Bostonm, 2008: 367-371

[13] North Atlantic Treaty Organization Standardization Agreement, ASAAC(Allied Standard Avionics Architecture Council)[R]. 2004

[14] Weissman C. MLS-PCA: a high assurance security architecture for future avionics[C]// 19th Annual Computer Security Applications Conference. Las Vegas, Nevada, 2003: 2-12

[15] Pierce D, Littlefield-Lawwill J. Information Assurance and Open Architecture Integrated Modular Avionics[C]// 2nd Annual IEEE Systems Conference. Montreal, 2008: 1-8

[16] Arinc Specification 653, Avionics Application Software Standard Interface[S]. AEEC, 2003