文章编号:1000-6893(2009)05-0938-08

综合化航空电子系统可信软件技术

沈玉龙[1],崔西宁[1,2],马建峰[1],牛文生[1,2]
(1.西安电子科技大学 计算机学院,陕西 西安 710071)
(2.航空计算技术研究所,陕西 西安 710068)

Trust Software Technology in Integrated Avionics Systems

Shen Yulong[1], Cui Xining[1,2], Ma Jianfeng[1], Niu Wensheng[1,2]
(1.School of Computer Science and Technology, Xidian University, Xi'an 710071, China)
(2.Aeronautics Computing Technology Research Institute, Xi'an 710068, China)

摘 要:航空电子系统要求航空任务的执行具有确定性、可预测和可控性。深入分析综合化航空电子系统软件安全性、可靠性、完整性和实时性需求,提出了综合化航空电子系统软件可信性的定义。首次将可信计算引入到综合化航空电子系统中,建立综合化航空电子系统可信软件体系结构,在此基础上,提出软件可信运行环境构建方法和可靠性增强技术。这些技术能够保障综合化航空电子系统的可预测性,对保证飞机任务的执行及其安全具有重要的作用,为研制适合于中国大飞机的综合化航空电子系统可信软件奠定基础。

关键词:综合化航空电子系统;可信软件;最小可信计算基;可靠性增强;安全系统
中图分类号:V243 **文献标识码**:A

Abstract: Avionics systems require aviation tasks to be definite, predictable and controllable. This article makes a thorough analysis of the requirements of an avionics system software in terms of security, dependability, integrity and real time. The definition of the trust software in integrated avionics systems is proposed. The trusted computing technology is introduced for the first time into an integrated avionics system, and the architecture of the trust software is established. Based on these, the execution environment of the trust software is established and the technology of its dependability improvement is presented. These developments will guarantee that the integrated avionics system tasks are predictable, which is of vital importance for task execution and security. These technologies lay the foundation for the development of trust softwares in integrated avionics systems which will be applicable to research on large airplanes in China.

Key words: integrated avionics system; trust software; mini trusted computing base; dependability improvement; security systems

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已不能够满足现代复杂的军事和民用需求,使得综合化航空电子系统得到了广泛关注[1]。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[2-3]。但是软件规模的急剧膨胀降低了软件的可靠性,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[4-5]。

综合化航空电子系统可信软件一直受到美国以及欧洲各国学术界的广泛关注。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[6],2002 年制定空管软件标准 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(Eurocontrol Safety Regulatory Requirement)[7]。在系统安全性方面,法国、德国、英国和美国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——联合标准化航电系统架构协会(Allied Standard Avionics Architecture Council,ASAAC)规范[8]。使得综合化航空电子系统安全体系结构和相关安全技术更为规

收稿日期:2008-08-12;修订日期:2009-03-03
基金项目:国家自然科学基金(60633020,60573036);国家"863"计划(2007AA01Z429,2007AA01Z405);航空科学基金(2007ZD31003,2008ZC31001)
通讯作者:沈玉龙 E-mail:ylshen@mail.xidian.edu.cn

范化和标准化。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(North Atlantic Treaty Organization Standardization Agreements) 4626 计划[9]。在学术界,研究人员试图使用传统方法来解决综合化航空电子系统的安全问题[10]。C. Weissman[11] 提议了一个未来航空电子系统的高确保安全体系结构 MLS—PCA(Multi Level Security—Polymorphic Computing Architecture),作为 DoD JV 2020 的安全解决方案。J. Swangim 等[12] 将信任概念引入航空电子系统,但是缺乏信任环境的构建方法。

这些技术均没有从根本上解决综合化航空电子系统可信软件问题,主要是:①虽然规范了软件开发的行为,但是缺乏对软件本身、行为以及平台的完整性校验,而这在软件分发和分布式软件运行中是非常重要的;②传统安全技术增加了系统运行的负担,难以保证任务的实时性,同样缺乏对软件行为和平台的完整性校验。

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可信软件概念,从完整性、可靠性、安全性和实时性方面保证综合化航空电子系统的可信性。利用可信计算技术,构建综合化航空电子系统可信软件体系结构,从根本上解决综合化航空电子系统软件可信性问题。在此基础上,建立航空电子系统软件的可信运行环境,提出综合化航空电子系统软件可靠性增强技术。希望通过这些技术的研究,为适合我国大飞机的综合化航空电子系统可信软件设计奠定基础。

1　综合化航空电子系统软件可信性

可信是一个复杂的概念,在 ISO/IEC 15408 标准中给出的定义是:可信的组件、操作或过程的行为在任意操作条件下是可预测的,并能很好抵御应用程序软件、病毒以及一定的物理干扰造成的破坏。可信软件强调的是软件行为的可预测,综合化航空电子系统要求软件的行为是预先确定的,软件的可信性已成为综合化航空电子系统研究的热点问题之一[13]。

先进的综合化航空电子系统高度信息化,具有综合化、模块化特点。软件已经成为新一代飞机航空电子系统研制成败的决定因素。新一代机载计算机强调系统的鲁棒性设计,以增强机载计算机的容错能力,允许在一定条件下"带病工作",提高完成任务的概率和作战飞机的出勤率[14]。这对新一代机载计算机体系结构、软硬件设计均提出了较高要求[15]。综合化航空电子系统要求软件执行的操作是可预测、可控制的,并能够抵御各种攻击。可信就意味着综合化航空电子系统软件行为是可信任的。可信的概念正好与综合化航空电子软件要求相吻合。保证综合化航空电子系统软件行为可预期、可控制,并能够抵御各种攻击,就需要保证综合化航空电子系统软件具有安全性、可靠性、完整性和实时性。对软件进行度量和检测是综合化航空电子系统可信运行的基础,将可信计算技术引入综合化航空电子系统为其软件运行提供可信根源,是保证综合化航空电子系统软件可信的新方法。目前的综合化航空电子系统 ASAAC 规范提出相应的信息安全、可靠性等需求,但是没有从根本上解决其可信问题。以下从 4 个方面对综合化航空电子系统可信性进行分析:

(1) 综合化航空电子系统高安全性(Security)

航空电子系统综合化后,各子系统之间相互联网通信,资源高度共享[16],相比独立式航空电子系统,综合化航空电子系统存在巨大安全隐患。ASAAC 规范分析综合化航空电子系统存在的安全隐患,主要表现为被窃听、环境干扰、非授权访问、(人为)干扰、设计中的缺陷、物理攻击、病毒攻击、开发人员有意破坏、非法篡改以及操作错误等。ASAAC 规范建立了综合航空电子系统安全体系结构,并提议了相应的安全模式。不同于其他系统,综合化航空电子系统要求的安全级别最高,需要达到信息技术安全评估准则 CC(Common Criteria) 描述的最高级别安全,即形式化验证的设计与测试[17]。研究航空电子系统软件安全技术,为软件提供安全运行环境是综合化航空电子系统面临的新挑战。

(2) 综合化航空电子系统高可靠性(Dependability)

综合化之后,引发了新的航空电子系统软件的可靠性问题[18],主要体现在 3 个方面:①综合化航空电子系统是软件密集型,软件规模急剧膨胀,原有以硬件为单位的"子系统"概念已变化成软件组件,从而增加了软件复杂性,引发了软件可靠性的降低;②航空电子系统综合化后,综合核心处理机需要同时处理多个任务,保证各个任务之间相互独立,以阻止单个模块错误的扩散,避免影响其他任务的执行;③综合化航空电子软件子系统具有重用性高,可移植等特点,各个软件子系统

之间存在依赖关系，降低了综合化航空电子系统可靠性。这些因素影响飞机的安全性(Safety)，研究软件可靠性增强技术是综合化航空电子系统的迫切需求。

(3) 综合化航空电子系统完整性(Integrity)

综合化航空电子系统软件可信性的基础是完整性校验。主要原因是：①综合化之后各子系统相互通信，交换信息，具有信息的完整性要求；②通过飞机之间通信来协调飞机自由行情况下的飞行线路，信息传输的完整性是飞机之间安全协调的基础；③飞机软件动态分发决定飞机执行的任务，执行错误的软件，可能产生严重后果：在战场上，执行敌人软件将导致毁灭性打击；④飞机自身软件的执行同样需要完整性度量，以防止病毒、木马等非法程序的运行。因此，可信计算技术为系统提供信任根源，具有保证数据完整性和软件度量的功能。对平台和软件进行度量，保证数据完整性是复杂环境下的综合化航空电子系统必须解决的根本问题。

(4) 综合化航空电子系统软件实时性(Real-time)

飞机任务的执行具有确定性需求，不可预测事件的发生是影响飞机安全的重要因素之一[19]。在综合化航空电子系统中，时间错误是最重要的故障之一。实时性是飞机可靠的重要因素，在航空电子系统内部，核心服务缺乏实时性将导致整个飞行任务不能完成；在战场上，飞机高速飞行，没有在指定时间执行相应任务，将错失对敌攻击的时机，失去对战争主动权的把握[20]。

综上所述，综合化航空电子系统可信性为

可信性 = 安全性 + 可靠性 + 完整性 + 实时性

综合化航空电子系统软件可信性与安全性、可靠性、完整性和实时性的关系如图 1 所示。

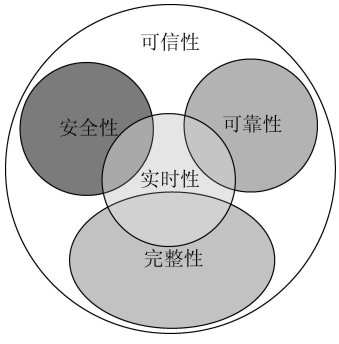

图 1 综合化航空电子系统软件可信性示意图

Fig. 1 Illustration of trust software in integrated avionics system

安全性是航空电子系统综合化之后引入的新问题，是可信性的重要组成部分；由于软件密集、重用以及同时处理多个任务，航空电子系统综合化之后，可靠性有所降低，保证软件可信性要求增强航空电子系统可靠性；综合化航空电子系统要保证执行的软件、软件运行平台以及相关数据是合法的，完整性是可信性的重要方面；综合化航空电子系统的软件必须具有实时性，缺乏实时性，发生时间错误将导致软件行为不可预测，丧失可信性。

2 综合化航空电子系统可信软件体系结构

综合化航空电子系统可信软件体系结构是在现有的航空电子系统软件体系基础上，使用可信计算理论和方法建立的。基于 ASAAC 规范，在综合化航空电子系统中嵌入可信芯片可信平台模块(Trusted Platform Module，TPM) 作为信任的根源，基于 TPM 构建适合于综合化航空电子系统的最小可信计算基(Mini Trusted Computing Base，Mini TCB)[21]。Mini TCB 是系统软件可信的根源，在该根源上进行信任的向上传递，构建航空电子系统微内核操作系统(Operating System，OS)。在此基础上，进行航空电子系统的安全管理、可靠性管理，建立综合化航空电子系统可信软件环境，保证航空电子系统任务的可信运行。同时，可信度评测模块在对影响可信性的多种因素进行多维度量的基础上，对系统可信性进行综合测评。其体系结构如图 2 所示。

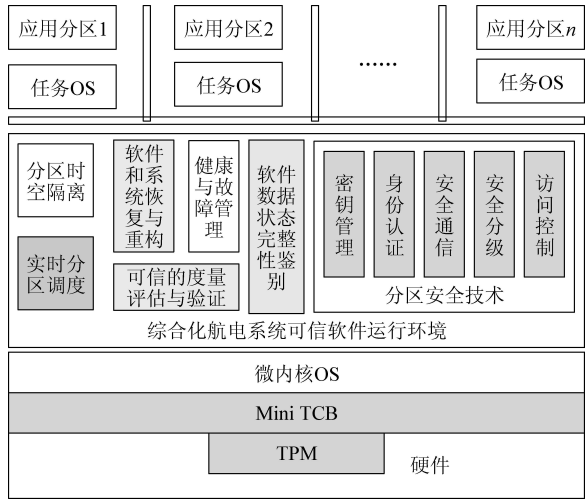

图 2 综合化航空电子系统可信软件体系结构

Fig. 2 Trust architecture of integrated avionics system

在综合化航空电子系统中构建 Mini TCB，该 Mini TCB 是航空电子系统可信的根源，在此基础

上给出综合化航空电子系统软件的完整性定义、描述、度量、评估和管理的方法。通过信任传递,来保证整个航空电子系统软件(包括微内核 OS,应用软件)没有被植入病毒、木马,没有遭受破坏,并被正确地加载,以此来保证航空电子系统软件静态的安全性。当整个系统运行后,通过 Mini TCB 所提供的功能接口进行安全管理,实现以下 5 个功能:①可信功能调用,对系统调用进行检测;②安全通信,保证分区间通信的机密性、完整性;③身份认证,保证通信双方身份的真实性;④安全分级,对不同的数据进行分级,对安全级别不同的数据实行不同的管理策略;⑤访问控制,保证航空电子系统严格按照预先设定的安全策略来对数据进行访问。以此来保证航空电子系统动态的安全性。

可靠性主要体现在分区管理方面,实现以下 2 个功能:①分区的时空隔离,保证分区的独立性;②健康管理,对分区进行管理,即对分区时空隔离,分区恢复与重构的管理。

3　综合化航空电子系统可信软件运行环境

航空电子系统综合化之后,综合核心处理机同时处理多个任务,为了保证系统的可靠性,采用分区时空隔离技术,此技术限制了分区故障的扩散。分区的时空隔离是综合化航空电子系统与其他系统的最大区别。在时空隔离体系的基础上,构建基于 Mini TCB 的综合化航空电子系统可信软件环境。

3.1　基于TPM 构建 Mini TCB

为了构建综合航空电子系统可信软件支撑环境,在综合化航空电子系统中嵌入TPM 芯片,作为系统信任的根源。利用 TPM 的功能构建 Mini TCB,通过 Mini TCB 为综合化航空电子系统可信软件环境提供可信支撑。基于TPM 所提供的密码算法和可信度量、可信存储和可信报告等功能,使得病毒、木马等非法、恶意程序不能够被授权运行,从源头上切断这些安全威胁;TPM 可以充当可信第三方,使得现有的安全协议的设计有了可信依据,简化协议的设计,提高协议交互的安全性;TPM 本身可以执行相应的安全操作,与目前由软件实现安全操作相比,具有实时性强、效率高的特点。

3.2　可信功能调用(Trusted Function Call,TFC)

可信软件环境平台采用 3 层栈结构,各层间以虚拟接口的方式抽象出满足层间功能引用的虚拟资源(Virtual Resource)和虚拟结构(Virtual Architecture)。可信功能调用是 3 层间安全引用的关键,主要功能为对系统功能调用的访问控制。可信功能调用也是进程与操作系统之间传递数据与服务请求的机制。

TFC 提供一种安全机制,用于在服务请求者与服务提供者之间的数据传递。操作系统服务调用的数据传递同样适用TFC。在TFC 的基本机制上加入安全授权,即对每一笔服务调用、数据传输都根据系统安全策略进行授权。图 3 描述了进程 1 通过TFC 调用进程 2 服务的过程。TFC 机制将分隔的进程联系起来,同时保持分区的特性。

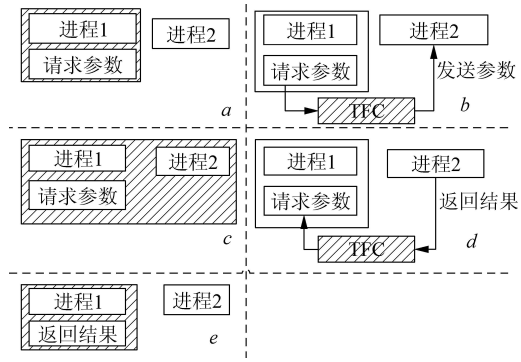

图 3　可信功能调用过程

Fig. 3　Trust function call process

3.3　基于 Mini TCB 的安全虚通道(Virtual Channel,VC)技术

密钥管理和身份认证是基于 Mini TCB 的。由于 Mini TCB 借助TPM 完成大量的安全操作,与现有的综合化航空电子系统密钥管理方式相比,基于 Mini TCB 的密钥管理和身份认证具有高安全性、高效率和强实时性的特点。

安全通信要求消息传输的机密性、完整性和来源的可认证性。现有的综合化航空电子系统分区之间的通信使用虚通道技术,其安全是通过通用管理系统中的安全管理提供的安全机制来实现的,其安全性、实时性和效率都较低。

采用 Mini TCB 技术,给各个分区分发密钥和身份的绑定凭证,并利用这些安全值,设计分区间的子安全协议,利用模块化设计思想组合构建分区间可信的认证及密钥交换密码协议,安全虚通道如图 4 所示。

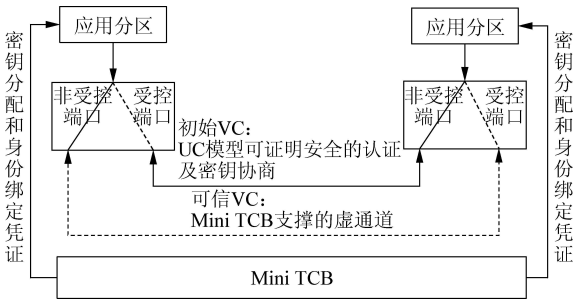

图 4 安全虚通道

Fig. 4 Trust virtual channel

3.4 基于BLP(Bell-LaPadula)模型的可信分区分级与访问控制机制

访问控制的目的是确保系统运行时系统服务和资源的访问权限,在综合化航空电子系统中,每个对系统服务的调用或对系统资源的访问,都需要检查是否具有相应的权限。为了防止分区应用对系统资源与系统服务的非授权访问与使用,破坏系统的可信特性,对应用分区划分安全级别,采用基于BLP 模型解决访问控制问题。

BLP 授权模型是典型的多级安全控制模型,是处理多级安全信息系统的设计基础,在处理机密数据时,防止高安全级别的分区把信息泄露给低安全级的分区,即防止机密信息从高到低的非法流动;在访问控制方面,给每个访问者和系统资源以及服务分配相应的安全等级。当访问者访问资源或者服务的时候,根据访问控制策略和主客体的安全级别来判断是否具有访问权限。

通过 Mini TCB 模块对航空电子系统中的应用分区分发公钥,并签发公钥和分区身份的绑定凭证;当用户提出资源访问请求时,BLP 模型的控制实施模块要求分区提交身份绑定凭证,对其凭证进行认证后,根据安全级别和访问控制策略,判断此分区是否具有访问资源的权限。基于 Mini TCB 模块的BLP 授权模型如图 5 所示。

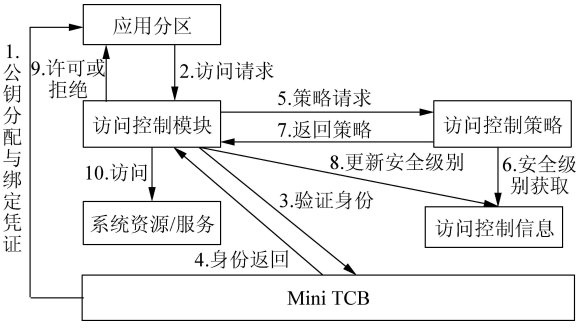

图 5 综合化航空电子系统分区访问控制模型

Fig. 5 Access control model of integrated avionics system

4 综合化航空电子系统可靠性增强方法

航空电子系统综合化后,软件急剧膨胀,软件可移植、可重用,降低了软件可靠性。目前综合化航空电子系统软件可靠性增强技术主要包括:分区时空逻辑隔离机制、软件系统健康管理、软件故障恢复与重构技术。

4.1 分区时空隔离机制

为了保证综合化航空电子系统可靠性,在综合化航空电子系统微内核操作系统上运行多个任务操作系统,每个任务操作系统运行着一个分区,每个分区完成指定的航空电子系统任务。通过时空隔离方式,各个任务分区相互独立,单个分区错误不影响其他分区的运行。

采用时空隔离的思想解决各分区中多个任务间隔离与资源分配问题。应用软件与操作系统、操作系统与硬件接口标准化,使得航空电子应用软件安全、可靠地运行,其结构如图 6 所示。

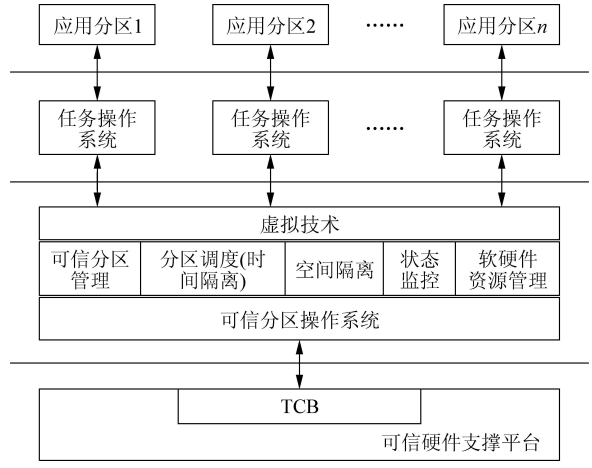

图 6 综合化航空电子系统可信分区结构

Fig. 6 Trust partition structure of integrated avionics system

4.2 健康管理

目前健康管理利用软件系统的各种数据信息,借助各种智能推理算法,评估系统自身的健康状态,在系统故障发生前对其故障进行预测,并结合各种可利用的资源信息实现系统故障恢复与重构。状态监测、健康评估和故障预测是健康管理的核心部分,在某种意义上它们都是一种推理过程,在实际构建健康管理系统时往往要根据系统的实际情况采用一种或多种技术和方法。

采用基于规则、案例和模型等的推理算法进行

状态监测和健康评估。收集各种监控数据监测系统当前的状态,根据预定的各种参数指标来提供故障报警能力。评估被监测系统的健康状态,产生故障诊断记录并确定故障发生的可能性。基于各种健康状态历史数据、工作状态等进行故障诊断。

基于特征进化/统计趋势的预测和物理模型的预测等,综合各种数据信息如监测的参数、使用状况、当前的环境和工作条件、早先的试验数据以及历史经验等,预计其未来的健康状态。利用数据融合技术提高状态监测、健康评估和故障预测推理的准确性以及推理结果的置信度。数据融合是指通过协作或者竞争的过程来获得更准确的推论结果。可以对 3 个层次的数据进行融合,数据层的数据融合针对直接监控的故障数据,以进行故障识别和特征抽取;特征层的信息融合针对抽取的特征信息,进一步融合获得故障诊断方面的信息;推理层的知识/决策融合将基于经验信息的预计结果同基于状态信息进行融合,用于系统级的预测推理和维修决策。

4.3　软件故障的恢复与重构机制

综合化航空电子系统软件故障的恢复,按粒度的不同分为软件级和系统级两个层次。对于软件运行过程中出现的微小故障,采用软件级的恢复较为高效简捷;对于复杂的软硬件故障,难以确定故障的发生原因,采用系统级的恢复与重构迅速屏蔽故障,恢复系统的功能。

本文提议的软件恢复是基于领域和系统的知识,为交互式和渐进地提取软件的结构而设计的易处理程序、所需的技术和支撑工具的过程。软件的恢复技术可分为两大类:基于聚类的技术和基于模式的技术。基于聚类的技术根据组件的相似性对组件分组,并生成体系结构组件;基于模式的技术先用建模的方法(如查询语言和框图等) 构成软件的高级模型,再用模式匹配、搜索并确定模式实例。相比较而言,模式匹配的方法具有计算量小、准确性高等优点。

系统中有的故障难以快速确定其起因,从而造成故障的扩散,这对于实时性要求较高的航空电子系统难以接受,需要进行系统级的恢复与重构。系统级的恢复是通过多版本软件冗余和备份等技术完成系统功能的恢复;系统的重构是通过管理故障系统的可用资源,按照系统服务的优先级,提供部分系统重要服务的过程。重构的目的是在系统故障无法完全屏蔽的情况下,保护系统的重要服务不受影响。

综合化航空电子软件系统故障管理从软件和系统两个层次对系统故障进行恢复与重构。对于出现的故障,在需要微小恢复的情况下,通过替换故障组件,进行软件恢复;在需要重大恢复的情况下,通过动态替换发生故障的软件恢复系统的功能,采用重新组织系统的可用资源,实现系统重构,保护系统的重要功能。软件和系统的恢复与重构是增强综合化航空电子软件系统可靠性的有效手段。本文提议的软件恢复与重构的流程如图 7 所示。

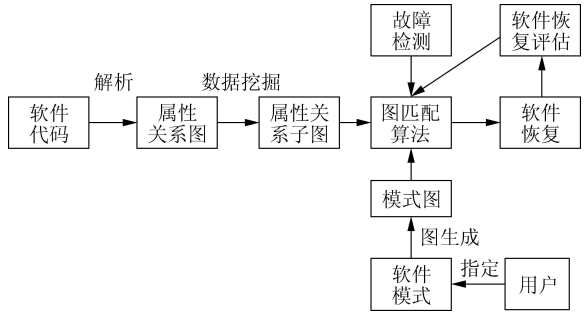

图 7　软件恢复与重构流程

Fig. 7　Process of soft ware recovery and restructure

由图 7 可知,首先对软件代码进行解析,提取软件的抽象表示方法,形成属性关系图,在此基础上,应用数据挖掘等技术,将属性关系图分解成能够进行模式图匹配的属性关系子图。用户预先指定相应的软件模式,并应用图生成的相关技术形成模式图。当软件故障被检测到的时候启动图匹配算法进行软件恢复与重构,然后对恢复和重构后的软件进行评估,如果没有达到预定的要求,重新启动图匹配算法,进行重新恢复。在这过程中的关键技术主要有:软件系统的抽象表示、软件恢复过程的可行性和系统的动态恢复和重构。

(1) 软件系统的抽象表示

以软件代码为基础,用组件、组件之间的交互和约束来抽象表示软件,并提取软件的行为特征。在软件系统的恢复过程中,软件系统的抽象表示是提取软件特性、分析软件特性的前提。抽象表示独立于编程语言,但是在保留的信息量和分析所需的抽象程度之间存在折中。

(2) 软件恢复过程的可行性

软件恢复过程中,根据提取的软件特征确定其结构模式,通过模式匹配进行组件故障的恢复。模式匹配阶段,在规模较大的数据库中搜索具有特定属性或属性组的组件计算量较大,对于实时性要求较高的综合化航空电子系统而言有时甚至

是不可行的。因此需要有效的方法来解决匹配算法的复杂性问题。

(3) 系统的动态恢复与重构

系统运行过程中,软硬件发生永久性故障,通过软件恢复无法恢复系统功能时,需要采用系统动态恢复与重构的方法,保护系统最重要的功能不受故障的影响。系统的动态恢复和重构是维护综合化航空电子系统安全性、可靠性和可生存性的最重要方法之一。

本文提议的综合化航空电子系统可靠性增强机制对故障可进行预测、定位、分析、防止故障扩散以及故障恢复。可靠性增强机制完成的相应功能如表 1 所示。

表 1 可靠性增强机制完成的功能

Table 1 Functions of mechanism to improve dependability

可靠性增强机制	故障预测	故障定位	故障分析	故障扩散	故障恢复
分区时空逻辑隔离	—	√	—	√	—
健康管理	√	√	√	√	—
软件恢复与重构	—	—	√	√	√

相比独立式航空电子系统和不采用可靠性增强的综合化航空电子系统,本文所提议的方法能够对故障进行准确地预测、定位、关联分析以及恢复,如表 2 所示。

表 2 可靠性比较

Table 2 Comparison of dependability

可靠性	独立式	无可靠性增强的综合化	可靠性增强的综合化
故障预测	不可预测	不可预测	可预测
故障定位	可以	不可以	可以
故障分析	不可以	不可以	可以
故障扩散	不扩散	扩散	不扩散
故障恢复	系统切换开销大	不可以	分区切换开销小

5 应用实例

从体系结构的角度出发,保证平台的完整性以及软件、数据和指令的完整性是解决综合化航空电子系统可信性的基础。随着可信计算的不断发展,综合化航空电子系统可信软件技术逐渐得到验证和应用。为了验证本文中提议技术方案的有效性,构建了综合化航空电子可信运行环境,如图 8 所示。

在此验证环境中,每个综合化航空电子系统模块均使用 Acoreos 653 操作系统,并在模块中植入 TPM 芯片,开发工具是 Rt Tools 。在此验证环境中,通过 FC 接口连接多个航空任务模块,包括:通信/导航、目标检测和跟踪、存储管理、航线管理和任务管理。

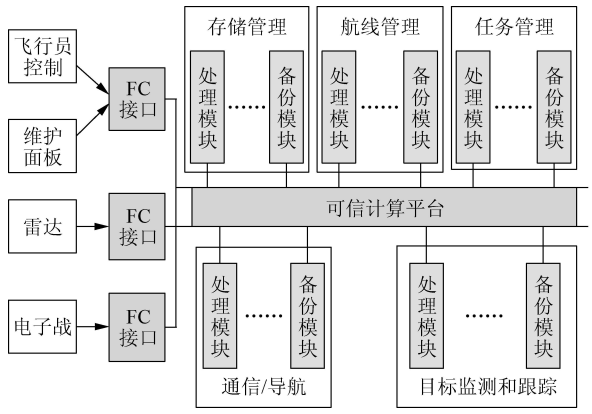

图 8 可信综合化航空电子系统验证环境

Fig. 8 Verification environment for integrated avionics system

在可信计算的支撑下,建立的综合化航空电子系统可信运行环境,并在此环境下验证可信功能调用机制、基于 Mini TCB 的安全虚通道机制、基于BLP 的授权模型、分区的重构与隔离机制、健康管理以及软件故障的恢复与重构机制。相比现有的综合化航空电子系统,本文提议的基于可信计算技术的体系结构合理,安全性、可靠性高。通过底层的TPM 芯片能够高效地进行完整性验证,保证系统软件运行的完整性以及实时性。

航空电子综合化、模块化和软件的动态分发等导致综合化航空电子系统具有强的可信性需求。本文所研究的可信软件技术已得到有效性验证。相信随着行业的发展,相关的研究成果必将得到国内外航空领域采纳和借鉴,对形成我国的综合化航空电子系统可信软件的标准化具有重要的作用。

6 结 论

针对综合化航空电子系统软件的安全性、可靠性、完整性和实时性要求,给出了综合化航空电子系统可信性定义,首次将可信计算技术引入综合化航空电子系统,建立基于 Mini TCB 的综合化航空电子系统体系结构和可信软件运行环境,并在此基础上,提出增强综合化航空电子系统软件可靠性方法。本文提出的保障综合化航空电子系统软件可信性的解决方法能够保障综合化航空电子系统的可预测性,对保证飞机任务的执行和其安全具有重要的作用,对发展我国自主知识产权的可信综合化航空电子系统软件具有重要的推动作用,为研制适合于中国大飞机的综合化航空电子系统可信软件奠定了基础。

致　谢

感谢中国航空计算技术研究所的周耀荣和谢克嘉研究员对本文研究给予的大力支持、帮助和指导。

参 考 文 献

[1] Boleat C, Colas G. Overview of soft errors issues in aerospace systems[C]//11th IEEE International On-Line Testing Symposium (IOLTS'05). 2005:299-302.

[2] 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'2007). 2007:28-39.

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

[4] Trevino L C, Brown T. Soft computing for propulsion control[C]//Digital Avionics Systems Conference, DASC'01. 2001:8B3-8B3/8.

[5] Beeby M. Aviation quality COTS software: reality or folly[C]//Digital Avionics Systems Conference, DASC'02. 2002:5D2-1-5D2-10.

[6] Levine S, Levine L J L, An onboard pilot and remote co-pilot for aviation safety, security and savings[C]//Digital Avionics Systems Conference, DASC'07. 2007:4.E.5-1-4.E.5-13.

[7] Kleidermacher D N, Integrating static analysis into a secure software development process[C]//2008 IEEE Conference on Technologies for Homeland Security. 2008:367-371.

[8] NATO STANAG 4626 ASAAC(Allied Standard Avionics Architecture Council)[S]. North Atlantic Treaty Organization. 2004.

[9] Pierce D, Littlefield-Lawwill J. Information assurance and open architecture integrated modular avionics[C]//2nd Annual IEEE Systems Conference. 2008:1-8.

[10] Jacob J M, High assurance security and safety for digital avionics[C]//Digital Avionics Systems Conference, DASC 04. 2004:8.E.4-8.1-9.

[11] Weissman C. MLS-PCA: a high assurance security architecture for future avionics[C]//Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC 2003). 2003:2-12.

[12] Swangim, J, Strauss J L, Kolkmeier T J, et al. Challenges of tomorrow—the future of secure avionics[C]//Proceedings of the IEEE 1989 National Aerospace and Electronics Conference. 1989:580-586.

[13] TCG trusted network connect TNC architecture for interoperability: specification revision 1.1[M/OL]. Revision 2. Beaverton, OR: TCG Published, 2006. http://www.trustedcomputinggroup.org.

[14] Algirdas A, Jean-Claude L, Brian R, et al. Basic concepts and taxonomy of dependable and secure computing[J]. IEEE Transactions on Dependable and Secure Computing, 2004, 1(1):11-33.

[15] 刘畅,刘斌,阮镰.航空电子软件仿真测试环境软件体系结构研究[J].航空学报,2006,27(5):877-882.
Liu Chang, Liu Bin, Ruan Lian. Software architecture of simulation testing environment for software in avionics[J]. Acta Aeronautica et Astronautica Sinica, 2006, 27(5):877-882.(in Chinese)

[16] Watkins C B. Integrated modular avionics: managing the allocation of shared intersystem resources[C]//Digital Avionics Systems Conference, DASC'06. 2006:1-12.

[17] Sagaspe L, Bieber P. Constraint-based design and allocation of shared avionics resources[C]//Digital Avionics Systems Conference, DASC'07. 2007:2.A.5-1-2.A.5-10.

[18] 徐亚军,张晓林,熊华钢.航空电子系统FC交换式网络的可靠性研究[J].航空学报,2007,28(2):402-406.
Xu Yajun, Zhang Xiaolin, Xiong Huagang. Study on reliability of FC fabric in avionic[J]. Acta Aeronautica et Astronautica Sinica, 2007, 28(2):402-406.(in Chinese)

[19] Bernstein M M, Chulsoo Kim. AOS: an avionics operating system for multi-level secure real time environments[C]//10th Annual Computer Security Applications Conference. 1994:236-245.

[20] Kuo T W, Yang W R, Lin K J. A class of rate-based real-time scheduling algorithms[J]. IEEE Transactions on Computers, 2002, 51(6):708-720.

[21] McCune J M, Parno B, Perrig A, et al. Minimal TCB code execution (extended abstract)[C]//IEEE Symposium on Security and Privacy(SP'07). 2007:267-272.

作者简介:

沈玉龙(1978—)　男,博士,副教授。主要研究方向:网络与信息安全,航空电子系统安全。
Tel: 029-88204749
E-mail: ylshen@mail.xidian.edu.cn

崔西宁(1964—)　男,硕士,研究员。主要研究方向:综合化航空电子系统软件。
Tel: 029-88151133
E-mail: cuixining@tom.com

马建峰(1963—)　男,博士,教授,博士生导师。主要研究方向:计算机安全、密码学。
Tel: 029-88204749
E-mail: jfma@mail.xidian.edu.cn

牛文生(1967—)　男,博士,研究员,博士生导师。主要研究方向:航空电子系统安全。
Tel: 029-88151016
E-mail: nwsheng@yahoo.com.cn

(责任编辑:鲍亚平,张利平)