doi:10.11959/j.issn.1000-436x.2015277

机载嵌入式软件的安全性机制研究

李亚晖，张亚棣，郭鹏
（中航工业西安航空计算技术研究所 机弹载计算机航空科技重点实验室，陕西 西安，710065）

摘 要：通过深入分析机载软件的开发和运行过程，在满足适航标准和信息安全标准的要求下，给出了与机载系统软件安全性相关的因素和威胁，并提出了基于嵌入式可信计算基的 MILS 机载软件架构安全性防护技术，为机载嵌入式软件的安全性机制研究提供了基础。
关键词：安全关键系统；嵌入式软件；故障分析；安全威胁
中图分类号：TP309 **文献标识码**：A

Research on safety methods of airborne embedded software

LI Ya-hui, ZHANG Ya-di, GUO Peng
(Airborne and Missile-borne Computer Aviation technology Key Lab, Aeronautical Computing Technique Research Institute, Xi'an 710065, China)

Abstract: By analyzed the process of development and running of airborne software with the standards of airworthiness and information security, the factors and threats related with airborne software safety were presented, and the security protected mechanisms based on embedded TMP and MILS software architecture were provided, which all support the research on safety of embedded software on aircrafts.
Key words: safety-critical system; embedded software; fault analysis; security threat

1 引言

在航空领域，随着机载系统中软件所占比重的逐步增大，软件失效可能引起的后果也越来越严重，轻者导致无法完成任务，重者导致设备损毁，甚至危及人的生命。机载嵌入式软件对于安全性的要求格外的高，其面临的问题也更加复杂。主要原因包括机载软件的运行剖面多样化和复杂，软件系统层次多、任务多，大量周期性任务和非周期性任务并存，任务之间的耦合关系复杂，涉及的硬件类型多，传感器数量大等。

在机载综合化电子系统的开放环境下，机载软件系统除了保证不同安全关键级别的任务软件运行期间互不影响外，还要防护系统遭受来自外部环境（包括网络、维护人员、电磁信号等）恶意攻击。面对这种情况，国外研究多级别安全性（MILS，multiple independent levels of security）关键系统软件架构。其采用分层隔离的思想，通过可形式化验证的微内核提供系统架构的安全基础，利用时空隔离的分区机制将多种安全界别的任务进行隔离部署，从而减少故障引发的关联失效，以及提供自底向上的信息安全防护支撑机制，使运行于各分区中的任务软件能够收到系统架构提供的有效安全防护。这种机制能够便于机载系统软件的独立开发和增量化验证。

然而，机载嵌入式软件的安全性需求是一个系统性需求，不仅涉及软件系统架构，同时还涉及软件方法、开发过程和运行环境等各方面因素。本文将从机载嵌入式软件的安全性方面展开系统性的分析，对故障引发的安全性（safety）和恶意攻击导致的保密性（security）进行发生机理、引入原因和防护机制等方面的研究，从而为机载嵌入式软件安全性防护提供技术支撑。

收稿日期：2015-10-24
基金项目： 航空科学基金资助项目(2013ZC31005)
Foundation Item: The Aeronautics Science Fund (2013ZC31005)

2　机载软件的安全性

2.1　软件安全性定义

关于软件的安全性，Leveson[1]的定义是：“指确保软件在系统上下文中执行不会导致系统发生不可接受的风险。”软件安全性之所以未能有效付诸实践的 2 个主要原因是“软件安全性概念在开发人员或用户未能正确理解哪些要素可以确保系统安全”和“未能在更大的或更宽泛的系统中考虑软件安全性”。软件保密性融合了可用性、机密性和完整性，着重关注如何保护软件使其不被恶意攻击。

软件安全性和保密性是针对内部缺陷和外部威胁而考虑的两个方面需求，二者之间是相互关联的，主要表现在：安全性主要处理危及人员生命财产安全的风险，而保密性主要防御造成敏感信息的隐私性泄漏的威胁；安全性着重关注由于内部缺陷引起系统故障而造成的风险，而保密性则主要关注外部恶意行为非授权访问造成的威胁；软件的外部攻击往往利用软件设计时引入的内部缺陷来获取非授权的访问控制权限，而针对软件保密性的外部攻击往往导致软件系统出现运行故障，造成功能失效而引起安全性事件。

2.2　机载嵌入式软件的安全性问题

机载嵌入式软件规模大、逻辑复杂，各种类型的软件组件数量多，组件之间交互关系多，功能耦合多。机载嵌入式软件的安全性要求来源于机载系统的安全性需求，也受制于运行平台的安全性保障机制（如分区的时空隔离、中断保护等）。随着机载软件系统综合化程度的不断提高，大量的软件高度共享综合核心处理计算机等硬件资源，软件之间相互影响进一步加剧，故障的传播途径多，“牵一发而动全身”。为了解决因规模、复杂度和综合化程度对安全性带来的挑战问题，相关组织和部门为机载嵌入式软件开发制定了严格的过程规范，如 DO-178B/C，它强调严格的过程评审和验证，并在研制过程中综合应用多种试验手段，以尽早发现可能导致安全事故的隐藏缺陷。DO-178B 按照失效后果的严重程度对机载嵌入式软件的安全级别进行了定义，并针对每个级别明确了必须开展的验证活动和验证要点，这使得针对不同级别的机载嵌入式软件进行设计时，软件的验证和测试活动必须满足该级别所要求的相关准则。

随着航空电子信息综合能力的增强，智能化是综合航空电子系统发展的方向，飞机平台和飞行员对航空电子综合系统的依赖程度也越来越高。然而，作为现在战争信息网络系统中的一个节点，航空电子系统需要保持与外界的信息交互，必然有遭受信息攻击和破坏的可能。因此，系统的信息安全和保障是未来网络化作战环境中机载系统的一个关键。2013 年 7 月，美国 FAA 的计算机安全专家开始向企业、高校和政府部门寻求信息安全研究工作的合作方案，用于开展航空飞行器的信息安全研究和发展计划。

3　机载软件的安全性影响因素

3.1　安全性因素的机理

1）安全性因素

机载嵌入式软件安全性和软件可靠性既有联系，也有区别。安全性关注故障的后果严重程度，可靠性则关注系统连续运行时间。容错是安全性设计和可靠性设计中共同关注的问题，但是安全性设计往往需要根据故障的严重程度设计相应的预防、功能降级等针对性措施，而可靠性设计则往往针对故障的发生概率和传播机制等设计统一的故障处理机制。此外，软件安全性需求来源于系统安全性需求，必须针对系统安全性需求分析软件需要处理的各种安全性故障，并确保软件在运行过程中不能引发可能导致安全事故的故障。

机载嵌入式软件安全性需求来源于系统安全性需求，必须针对系统安全性需求分析软件需要处理的各种安全性故障，并确保软件在运行过程中不能引发可能导致安全事故的故障。因此，机载嵌入式软件安全性研究在安全性故障分析基础上，重点关注这些故障的触发条件和处理措施，并对安全性设计提出具体的处理要求。

由于机载嵌入式软件安全性主要针对故障进行分析，且所关注的故障涉及多种类型，包括运行平台故障、外部硬件设备故障、内存访问故障、并发与同步控制故障等。对这些不同类型故障的认识和描述是开展软件安全性分析和设计的基础，因此必须在分析阶段识别可能发生的故障及其导致的后果，在设计阶段对故障发生机理和处理措施进行分析和验证，在测试阶段通过故障注入手段对安全性进行测试，在评估阶段对安全性相关的故障失效率、故障风险等进行分析。

2）保密性因素

安全关键系统的信息安全问题能够导致系统的可靠性和安全性受到危害，从而引发系统的失效，是系统造成人身、设备以及环境的损害。信息安全缺陷引入的机理[4,5]主要分为以下几个方面。

①系统的安全防护设计缺失。由于没有在系统设计时考虑信息安全防护的需求，导致系统当处于开放环境中时，可以被恶意人员利用合法指令进行违反系统运行规则的行为，导致系统失效。例如：2010 年，伊朗核电站的离心机由于感染“震网”病毒，使控制系统发出超负荷运转指令，造成布什尔核电站的 1 000 台离心机报废。

②系统在开发过程中存在信息安全隐患。由于安全关键系统中的安全防护措施不严密，导致恶意人员利用安全缺陷成功入侵系统，造成系统敏感信息的丢失。例如 2011 年，VxWorks 操作系统的远程登录程序密码算法缺陷，使恶意人员可以入侵到系统获取权限，从而使我国大范围使用该操作系统的路由器收到攻击，泄露了大量的用户信息。

③系统运行过程中的安全防护。由于当前的安全关键系统普遍运行于网络系统上，依赖网络进行大量的数据交换，一旦网络收到恶意人员的攻击，就可能造成网络阻塞，从而造成系统无法正常工作。例如在 2011 年，伊朗宣称“俘获”一架美国 RQ-170 哨兵无人机，主要通过噪声干扰其通信，切断美国无人机与指挥部之间的联系，使无人机被迫转为自动驾驶，并利用 GPS 坐标“哄骗”无人机“自动着陆”，无人机根据程序认为降落地点位于阿富汗总部，而实际上在伊朗境内。

④系统在维护过程中引入安全缺陷。由于系统在维护和升级过程中，维护人员具有系统的修改权限，一旦引入恶意程序就可能造成系统的敏感信息损坏和泄露。例如，某地面系统由于维护人员操作不当，将“摆渡”木马通过维护升级程序感染系统，险些造成敏感数据的丢失。

3.2　机载软件安全性因素的引入

机载软件的开发过程采用“V”字模型，需要融合系统工程与软件工程的交叉学科的软件系统工程来提供目标系统的领域知识，以便软件工程师充分理解系统需求，从而在软件设计中减少需求和设计缺陷，增强系统的安全性。根据实践研究指出，70%的故障是在软件寿命的早期引进来的，而其中 80%直到综合测试以后才以 10 倍以上的修复成本抓到[6]。图 1 显示了故障引进、发现和成本因素的百分比。

系统的综合化和模块化导致新一代飞机系统越来越复杂，形成了新型的机载“系统的系统”。而复杂机载系统的功能越来越依赖软件实现，其设计方法和过程模型在机载综合化系统中的作用越来越重要。当前的“先构建，后综合”的开发过程已经证明对航空工业是不合适的。整个设计的生命周期后端（集成测试和工程化）发现了近 80%的问题，解决这些问题是前段发现和解决问题成本的 16~110 倍，导致系统开发的成本、周期和风险难以控制。

3.3　机载软件安全性因素分类

1) 软件需求缺陷。由于缺乏需求工程的严格分析与定义，针对安全性需求的准确描述方法缺乏，系统的安全需求正确转化为软件的安全需求难以保证。往往依赖于个人的经验来形成软件安全性需

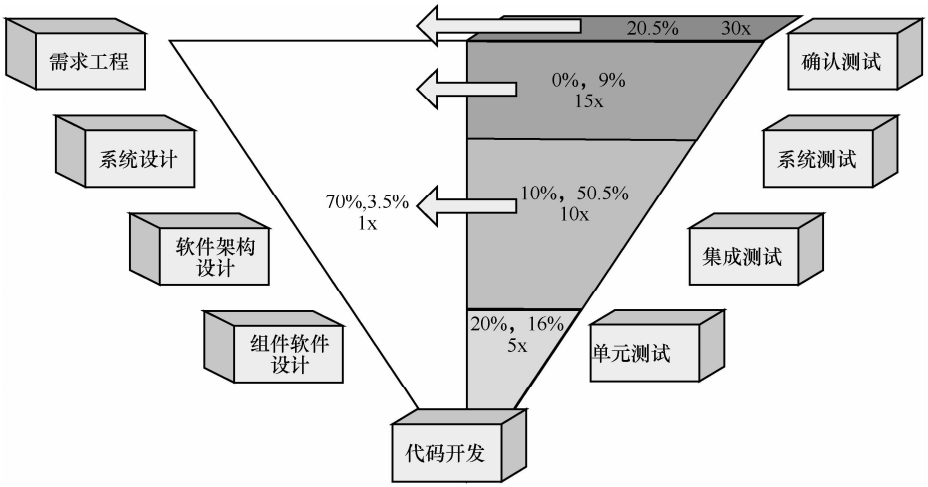

图 1　安全关键软件的缺陷分析

求，其完备性和正确性难以得到保证。软件需求缺陷涉及的范围包括：故障检测、定位、隔离和恢复，冗余容错管理，边界条件的约束、时序和逻辑关系限制等。

2) 软件设计缺陷。由于在软件设计阶段缺乏对安全性的描述方法，容易造成设计人员对需求理解的误差，设计过程会引入安全性的缺陷。设计阶段引入的缺陷主要体现为安全性需求与安全性设计的一致性难以保证，造成安全性设计缺陷。

3) 软件代码缺陷。编码过程中由于人为因素引入代码缺陷，代码缺陷涉及的范围包括数据定义与使用、代码接口、代码逻辑、使用资源、运行模式、类型转换和临界条件等。

4) 硬件升级引发的缺陷。当硬件环境发生变化，已有软件产品在适应新的硬件环境时，安全性需求难以进行全面验证，容易引入软件安全性防护的缺陷。

5) 保密性的缺陷。由于当前的机载嵌入式系统内部几乎没有考虑任何保密性的问题，当机载系统发展为网络化、综合化的架构时，保密性难以得到有效防护。

4　机载嵌入式软件的安全性保证技术

4.1　安全性的保证技术

在航空领域，针对机载嵌入式软件的开发过程中的安全性分析给出了严格的规定[7, 8]。机载嵌入式系统的安全性分析主要分为系统需求阶段的初步危害识别、体系结构设计阶段的初步危害分析、详细设计阶段的安全性初步评估和实现阶段的共因分析，如图 2 所示。

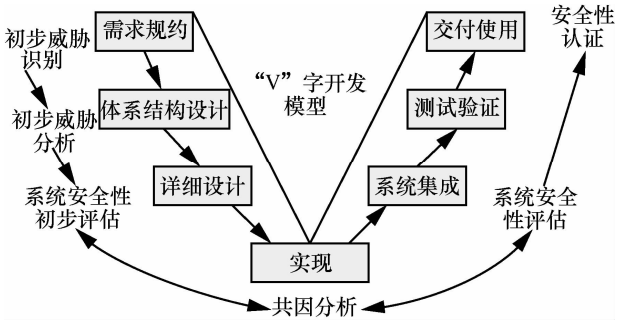

图 2　机载嵌入式软件的开发过程

航空领域针对机载嵌入式系统的安全性[9]，提供了有关功能危险性评估、初步系统安全性评估、系统安全性评估、故障树分析、相关图、马尔可夫分析、失效模式和影响分析、失效模式和影响摘要、区域安全性分析、特定风险分析和共模分析等方面信息[10]。

4.2　保密性的保证技术

1) 机载系统的软件保密性防护机制

随着机载系统的网络化、综合化的快速发展，机载嵌入式软件作为使能技术，承担着越来越多的功能实现。面对来自网络空间、维护保障系统和复杂电磁环境的恶意攻击威胁，需要构建基于可信计算基的机载系统安全防护架构，提供主动的安全防御机制。机载软件系统中可参考的保密性技术如图 3 所示。

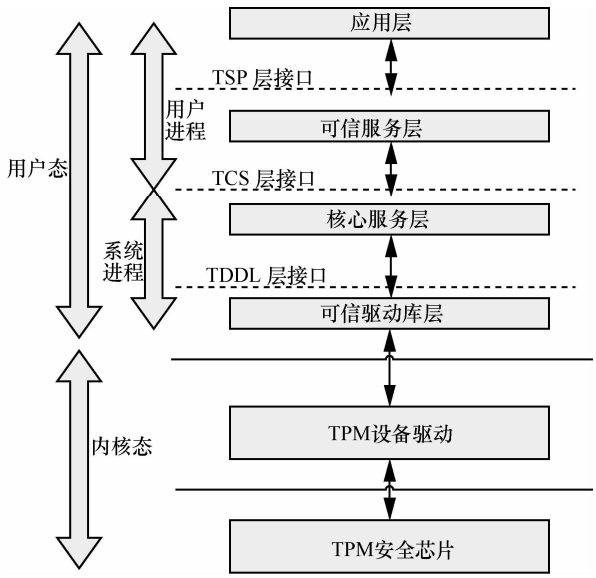

图 3　可信软件栈结构

机载系统的主动安全防护需要基于硬件可信根来提供软件运行环境的安全检测、防御措施。机载软件需要依托可信计算基提供的密码学算法和功能来构建可信软件协议栈，通过分布式验证机制为整个机载系统提供可信安全服务。机载系统的可信软件栈，具体功能包括密码算法服务、平台可信验证服务、远程可信认证服务、敏感数据安全存储、密钥安全管理、证书管理和审计信息记录等。

可信软件栈从下到上分为 3 层：可信驱动层、可信核心服务层、可信服务层。其中，可信驱动层是内嵌在嵌入式操作系统内核的系统服务，用于直接与可信模块中的安全芯片直接交互，将核心服务的调度任务转交给安全芯片中的安全管理控制程序；可信核心服务层用于管理和调度系统核心服务运行，处理服务接口转发过来的调用请求，并通过

可信驱动层接口与安全芯片的内部控制管理接口交互，完成对服务调用的实时响应；可信服务层用于为机载嵌入式系统提供基于面向服务的接口，应用程序通过接口调用可信服务。

2) MILS 机载软件系统架构

基于 MILS[11,12]架构可以构建机载软件的安全体系架构，如图 4 所示，基于 TPM 构建嵌入式可信计算基[13]，结合微内核嵌入式操作系统的安全性增强机制，在保证微内核能够进行形式化验证的基础上，为用户态的保密性功能提供底层的可信支撑。系统中的各类安全功能都以组件的方式运行于用户态的分区中，基于安全微内核提供的最小特权和信息流隔离机制实现对分区中应用任务的多级安全保护，因而能够从底层实现安全防护支撑，并能够单独对用户态的访问控制和数据保密通信功能组件进行安全性验证，更加高效和安全地实现全系统的安全防护。

在系统可信软件系统架构中，可信计算基 TPM 的功能基于安全芯片及其上的安全控制管理软件和驱动实现，通过系统分区中的可信软件栈为应用程序提供可信服务功能。

MILS 架构的机载软件系统中的可信安全服务都部署在独立的系统分区中，应用分区中的任务请求安全服务时，只能通过分区内核的通信接口访问。机载系统需求具备的可信安全服务包括应用程序所需要管理自身使用密钥的密钥管理服务；应用程序需要进行鉴权认证的身份认证服务；应用需要进行安全数据传输的安全通信服务；应用需要进行多种安全级别敏感信息处理的安全分级服务；应用程序需要对系统所存储的敏感数据访问的安全访问控制服务。

MILS 架构的机载软件系统中，用于支撑访问控制和安全通信功能的安全策略将以独立系统分区的形式进行部署，通过专用配置接口管理和分级缓冲的机制为安全服务中的访问控制和安全通信提供基于强制访问控制 BLP 和基于角色访问控制 RBAC 的安全策略管理功能。

5　结束语

本文从机载嵌入式系统的安全性需求出发，深入分析了机载嵌入式软件的安全缺陷机理、分类方法和引入机制，并针对当前航空领域的标准所采用的安全性分析方法进行的分析，提出了基于嵌入式 TPM 可信计算基的 MILS 软件架构，为机载软件的安全性提供了保证措施，为机载嵌入式软件的安全性机制研究提供了完整的研究思路。

参考文献：

[1] 樊晓光, 褚文奎, 张凤鸣. 软件安全性研究综述[J]. 计算机科学, 2011, 38(5):8-13.
FAN X G, CHU W K, ZHANG F M. Surveys of software safety[J]. Computer Science, 2011, 38(5):8-13.

[2] SWIFT M M, BERSHAD B N, LEVY H M. Improving the reliability of commodity operating systems[J]. ACM Trans on Computer Systems, 2005, 23(1) : 77-110.

[3] JAEGER T, SAILER R, SHANKAR U. Prima: policy-reduced integrity measurement architecture[A]. Proc of the 11th ACM Symposium on Access Control Models and Technologies[C]. Lake Tahoe, USA, 2006. 19-28.

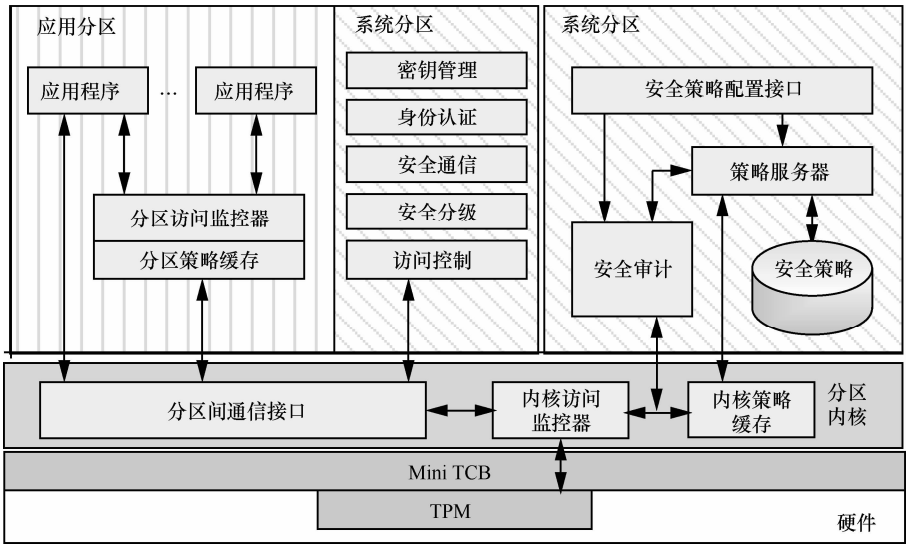

图 4　基于 MILS 的机载软件体系结构

[4] The statistics portal. Cyber crime incidents worldwide 2014, by victim industry and size[EB/OL]. www.statista.com/stat-istics/194246/ cyber-crime-incidents-victim-industry-size/.

[5] The statistics portal. Cyber crime: average company loss in selected countries 2014[EB/OL]. http://www.statista.com/statistics/293274/ average-cyber-crime-costs-to-companies-in-selected-countries/.

[6] FEILER P H. Challenges in validating safety-critical embedded systems[J]. SAE International Journal of Aerospace, 2010, (1): 109-116.

[7] SAE ARP4754A. Guidelines for Development of Civil Aircraft and Systems, Society of Automotive Engineers (SAE)[S]. 2009.

[8] 万明, 樊晓光, 南建国. 航电软件开发标准与过程研究[J]. 计算机工程与应用, 2010, 46(19): 71-73.
WAN M, FAN X G, NAN J G. Research on standard and process of avionics software development[J]. Computer Engineering and Applications, 2010, 46(19):71-73.

[9] SAE ARP 4761 Standard, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, Society of Automotive Engineers (SAE)[S]. 1996.

[10] 尹树悦, 杨云. 军机研制中安全性标准的应用[J] 航空标准化与质量, 2010, 237.
YI S Y, YANG Y. Applicaiton of safety standard in military plan[J]. Aeronautic Standardization & Quality, 2010, 237.

[11] GORDON M, UCHENICK W, MARK V. Multiple independent levels of safety and security: high assurance architecture for MSLS/MLS[A]. Military Communication Conference[C]. 2005.

[12] JIM A F, W. SCOTT H, PAUL O, *et al.* The MILS architecture for high-assurance embedded systems[J]. International Journal of Embedded Systems, 2005, 37(2).

[13] 张倩颖, 冯登国, 赵世军. 基于可信芯片的平台身份证明方案研究[J]. 通信学报, 2014, 35(8):95-106.
ZHANG Q Y, FENG D G. Research of platform identity attestation based on trusted chip[J]. Journal on Communications, 2014, 35(8): 95-106.

[14] 马赞, 王鹏, 肖女娥. SAE ARP4754A 中研制保证等级分配方法的应用研究[J]. 航空维修与工程, 2013, 2(2): 68-70.
MA Z, WANG P, XIAO N E. Application and study of development assurance level in civil aircraft development[J]. Aviation Maintenance & Engineering, 2013, 2(2):68-70.

作者简介：

李亚晖（1976-），男，湖南新邵人，博士，中航工业西安航空计算技术研究所高级工程师，主要研究方向为嵌入式计算机体系结构、嵌入式软件。

张亚棣（1968-），男，陕西西安人，博士，中航工业西安航空计算技术研究所研究员，主要研究方向为嵌入式系统和系统安全。

郭鹏（1987-），男，陕西渭南人，硕士，中航工业西安航空计算技术研究所助理工程师，主要研究方向为机载嵌入式软件、系统仿真与建模。