一种以安全性为中心的IMA软件体系结构设计方法

徐显亮[1] 张凤鸣[2] 褚文奎[1]
(空军工程大学工程学院 西安 710038)[1] (空军工程大学训练部 西安 710038)[2]

摘 要 在改进体系结构权衡分析法的基础上,提出了一种以安全性为中心的IMA软件体系结构设计方法。利用危险场景评价IMA软件体系结构的安全性,针对重大安全设计隐患,给出相应的危险预防、消除或减轻策略;利用契约捕获IMA体系结构求精所需满足的约束,推动IMA软件体系结构螺旋式求精。本设计方法有助于消除IMA软件中可能会影响综合航电系统以及飞机安全性的设计缺陷。

关键词 软件体系结构,软件安全性,安全性需求,综合模块化航空电子,体系结构权衡分析法
中图法分类号 TP311.5,TP309 **文献标识码** A

Safety-centered Architecture Design Method for IMA Software

XU Xian-liang[1] ZHANG Feng-ming[2] CHU Wen-kui[1]
(Institute of Engineering, Air Force Engineering University, Xi'an 710038, China)[1]
(Training Division, Air Force Engineering University, Xi'an 710038, China)[2]

Abstract Based on adaptation of architecture trade-off analysis method (ATAM), a safety-centered architecture design method was proposed for integrated modular avionics (IMA) software. Hazardous scenarios were used to evaluate the safety property of a designed IMA software architecture. Prevention, elimination or minimization actions to fateful hazards were derived. Contracts were used to document all the constraints which should be met in the next refined process of IMA software architecture. With the method, it will eliminate or reduce design bugs in the IMA software architecture, especially those that will contribute to hazards of the IMA system or fighters.

Keywords Software architecture, Software safety, Safety requirements, Integrated modular avionics (IMA), Architecture trade-off analysis method (ATAM)

1 软件体系结构与安全性

为了降低系统复杂性,提高软件复用性,综合模块化航空电子(integrated modular avionics, IMA)[1,2]采用了开放的三层堆栈式软件体系结构,引入了标准接口[1,3]和专用航电操作系统隔离硬件和应用软件的具体实现;引入了分区机制隔离分区功能的相互影响。文献[4]中已经讨论了比较具有影响力的IMA软件体系结构模型,包括ARINC 653模型、ASAAC模型等,此处不再赘述。

IMA软件是一种安全性关键软件[5],其失效、故障能够导致后果严重的飞行事件或事故。比如,2004年一架F-22战机就因为飞行控制软件故障而坠毁。软件体系结构是对系统行为的高度抽象。据文献[6]估计,70%~90%与安全性相关的决策需在项目的总体设计阶段做出。因此,IMA软件体系结构设计合理与否直接决定了包括安全性在内的IMA软件质量。由此,如何设计一个IMA软件体系结构,以合理预防、消除或减轻IMA软件可能引发的综合航电系统级或飞机级危险,就成了IMA软件开发面临的关键问题之一。

文献[7]从软件工程的视角讨论了软件安全性的设计方案、分析方法等。理论上而言,软件安全性分析是面向整个软件生命周期的,通过开展相应的安全性分析活动,消除能够降低系统安全性的软件缺陷,或将软件失效控制在一个风险接受级别[5]。与之不同的是,本文仅在软件体系结构设计阶段考虑如何设计一个以安全性为中心的IMA软件体系结构。

2 改进的体系结构权衡分析法A-ATAM

体系结构权衡分析法(architecture trade-off analysis method, ATAM)[8]是一种从安全性、可靠性、可修改性、可用性等质量属性角度评估系统或软件体系结构的方法。该方法以系统目标和用户观点为输入,针对体系结构析出可能威胁系统功能的质量属性,利用场景技术分析结构中存在的风险,通过反复的"设计-评估-修改(设计)"过程,使在体系结构的多个质量属性之间取得均衡。

借鉴ATAM的上述思想,本文提出一种改进的ATAM方法,称之为A-ATAM(adapted architecture trade-off analysis method)。针对设计的第 i 级体系结构 $Arch_i$,本方法利用

到稿日期:2011-04-12 返修日期:2011-08-23 本文受总装备部国防预研基金(9140A17020307JB3201)资助。
徐显亮(1982-),男,博士生,CCF会员,主要研究方向为信息系统工程与智能决策、综合航空电子系统,E-mail:qdxuxianliang@hotmail.com;张凤鸣(1963-),男,博士,教授,博士生导师,主要研究方向为信息系统工程与智能决策、综合航空电子系统;褚文奎(1980-),男,博士,讲师,CCF会员,主要研究方向为综合航电系统、软件安全性。

危险场景分析其存在的能够明显影响系统安全性的问题，然后给出相应的危险预防、消除、减轻措施；利用安全性评估标准剖析 $Arch_i$ 的求精之处和为此需要保持的契约。这些危险减轻措施、求精方案、契约等用作了第 $i+1$ 级体系结构 $Arch_{i+1}$ 的需求规约。本方法实际上实现了“体系结构设计-安全性评估-需求规约-体系结构设计”的螺旋式演化过程，最终实现一个从安全性角度可以接受的 IMA 软件体系结构，如图 1 所示。其中，$Arch_{i+1.1}$、$Arch_{i+2}$、$Arch_{i+3}$ 是 $Arch_{i+1}$ 的内部结构，是对 $Arch_i$ 的进一步细化求精，每一次螺旋对应一个版本的体系结构。

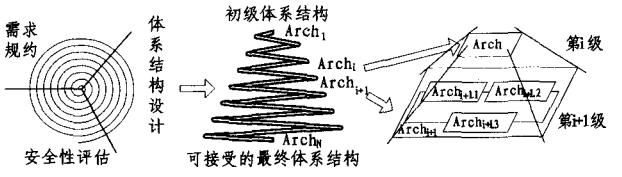

图 1　A-ATAM 螺旋设计

A-ATAM 方法用到的危险场景、安全性论据、契约等术语定义如下。

定义 1(危险场景，hazardous scenario)　危险场景建立在已确认的危险基础上，表明在何种系统状态和前提条件下系统将失效并进入危险状态。危险场景包括危险名、生成原因、导致后果，可表示为三元组：

$$hazardous\_scenario=(hazard,causes,effects)$$

其中，危险是一个系统状态或状态集合[9]，在其它条件辅助作用下，将能导致事故发生。比如飞机起落架不能放下是一个危险，在着陆阶段，这一危险就可能导致机毁人亡事故。危险由初步危险识别(preliminary hazard identification，PHI)和初步危险分析(preliminary hazard analysis，PHA)两个系统分析活动[10]得到。值得指出的是，利用这两个分析活动可能仅捕获有限的，特别是比较明显的危险，而一些潜在危险则要靠系统安全性初步评估(preliminary system safety assessment，PSSA)、系统安全性评估(system safety assessment，SSA)等系统分析活动才能进一步捕获。

一个危险场景示例如下：飞机在雷达高度表失灵下危险飞行=(雷达高度表失灵，雷达高度表数据溢出故障，飞机坠毁)

定义 2(安全性论据，safety argument)　安全性论据论证了安全性目标或需求在指定上下文中能够得到实现或满足——实现或满足证据可以是其它安全性目标声明或具体的解决方案等。第 i 级安全性论据 $Safety\_Arg_i$ 说明了第 i 级体系结构 $Arch_i$ 要实现的安全性目标集合 $Safety\_obj_i$ 在 $Arch_i$ 上下文 $context_i$ 中可以由第 $i+1$ 级体系结构 $Arch_{i+1}$ 提供的支撑安全性目标集 $Safety\_obj_{i+1}$ 予以满足。可描述如下：

$$Safety\_Arg_i=(Safety\_obj_i,Safety\_obj_{i+1})\,|_{context_i}$$

针对图 1 给出一个安全性论据示例，内容包括：①$Arch_{i+1}$ 的安全性目标与 $Arch_i$ 的安全性目标相一致；②$Arch_{i+1}$ 细化后的 $Arch_{i+1.1}$、$Arch_{i+1.2}$、$Arch_{i+1.3}$ 及其间交互能实现 $Arch_{i+1}$ 的安全性目标。

定义 3(契约，contract)　契约描述了软构件在体系结构内正常交互而应满足的约束集合[11]，比如功能需求、性能需求、安全性需求、环境需求等。可描述成

$$contract=(func,perf,safe,envi)$$

其中，功能需求 func 是指系统应提供的功能、输入输出范围等；性能需求 perf 是指软构件的执行时间、系统存储容量、保密性；安全性需求 safe 侧重于危险预防、消除、减轻等策略；环境需求 envi 泛指为实现系统功能、性能、安全性而应需要的支撑条件等。

契约的一种基本表达形式是记录参与交互的软构件、交互行为、交互得以执行的前置条件以及交互后需要满足的后置条件。以悬挂物管理程序(记为 SM)与悬挂物构件(记为 Store)之间的交互为例，SM 在要求 Store 释放炸弹前，必须先核实选中了正确的悬挂物，然后确认飞机不低于安全高度(即飞机飞行高度大于炸弹爆炸杀伤半径)，Store 在释放炸弹后，必须反馈释放成功。这种交互关系表达成如表 1 所列的契约。

表 1　契约表达形式

交互方	交互行为	前置条件	后置条件
SM，Store	Release()	CheckSelectStore()=true CheckLowerHeight()=false	Release()=true

3　基于 A-ATAM 的 IMA 软件体系结构设计

基于 A-ATAM 方法，本文提出以安全性为中心的 IMA 软件体系结构设计过程，如图 2 所示。过程主要包含了从 S_0 到 S_{11} 共 12 个活动。下面详细阐明这些活动所做的工作。

S_0：首先生成一个包含飞机平台级需求、IMA 系统级需求的初级 IMA 软件需求集 PreSpecSet。

S_1：由 PreSpecSet 设计一个 IMA 软件体系结构 $Arch_i$，用作安全性评估的基准对象。

S_2：利用危险场景库中的危险场景评估 IMA 软件体系结构 $Arch_i$ 的安全性，析出该体系结构是否会产生危险或产生哪些危险。假设产生的危险集合是 Hazards。

S_3：针对 Hazards 中的每一项危险，派生相应的危险预防、消除或减轻措施，记为 Hazard_Against，即是体系结构之修改需求。

S_4：利用 Hazard_Against 更新需求集合，即

PreSpecSet ← PreSpecSet+Hazard_Against

S_5：由 S_1 生成的 $Arch_i$，建立安全性论据 $Safety\_Arg_i$，内容包括：①$Arch_i$ 的安全性目标；②实现该目标的支撑安全性目标；③$Arch_i$ 有关的设计声明，比如遵守的公理、环境假设等。

S_6：由 $Safety\_Arg_i$ 定义的安全性目标生成安全性评估标准，包括要实现的安全性目标、所要遵守的上下文等。

S_7：利用 S_6 得到的安全性评估标准评价已设计的 $Arch_i$ 是否能够满足目标。如果不能满足，则执行 S_3；如能满足，则执行 S_8。

S_8：由针对 $Arch_i$ 的安全性论据 $Safety\_Arg_i$ 确定体系结构求精设计方案。比如图 1 中，$Arch_i$ 求精为 $Arch_{i+1}$ 后，包含了 3 个子构件，即 $Arch_{i+1.1}$、$Arch_{i+1.2}$、$Arch_{i+1.3}$。

S_9：由 S_8 获得的求精设计方案，捕获求精体系结构的性能、功能、安全性等约束，比如 $Arch_{i+1.1}$、$Arch_{i+1.2}$、$Arch_{i+1.3}$ 的功能、性能、安全性以及 3 者之间的交互关系，形成体系结构求精所需要遵守的契约 Contract。

S_{10}：利用契约更新需求集合，即

PreSpecSet←PreSpecSet+Contract

S_{11}：生成安全性可接受的最终 IMA 软件体系结构 $Arch_N$。

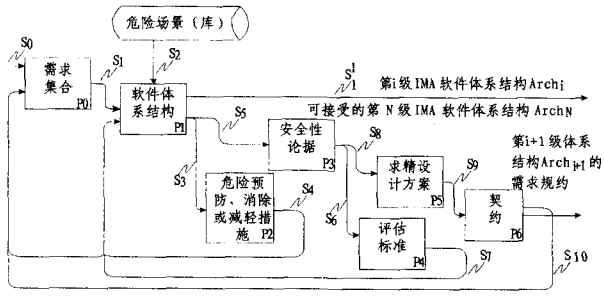

图 2　基于 A-ATAM 的 IMA 软件体系结构设计过程

可见，在图 2 所示的 IMA 软件体系结构设计方法中，存在 3 个主循环过程：①“S_5-S_6-S_7-S_5”，利用由安全性论据派生的评估标准评价体系结构，分析其中可能存在的、能够影响系统安全性的缺陷；②“S_2-S_3-S_4-S_1-S_2”，针对某种软件体系结构设计，应用危险场景进行评估，分析其安全性缺陷，给出危险预防、消除、减轻措施，然后更新需求集合，并修改或重新设计结构，直至其能够被接受；③“S_5-S_8-S_9-S_{10}-S_1-S_5”，根据论据解析出所有可能的设计方案，并以契约为需求反馈信息，不断求精 IMA 软件体系结构。这 3 个过程实现了“需求-设计-评估”递归。危险场景确保了某一级 IMA 软件体系结构的安全性，契约推动了 IMA 软件体系结构层级递进、求精。

4　应用案例

机载悬挂物管理系统（stores management system，SMS）[12]是现代战机遂行空中打击任务不可或缺的一个重要航空电子系统，其核心功能之一是控制悬挂物的投射。正常投射的基本流程如下：①SM 在接收到飞行员的投射请求后选择悬挂物；②SM 发出投射命令；③悬挂物从挂架上移除。据此核心功能构建的 SMS 软件体系结构如图 3(a)所示。

针对图 3(a)初始 SMS 软件体系结构，首先考虑图 2 中的第一个循环。其安全性论据包含的一个基本目标是保证投射行为不危及飞机自身安全。因此，在评价已设计的软件体系结构时要以该目标为出发点。显然，设计的初始体系结构是不能确保该目标完全实现的，需要对初步体系结构进行求精，并且求精设计不能违背此基本目标。

针对图 2 中的第二个循环，下面考虑两种危险场景：①投射了非期望的悬挂物。比如，空战时拟投射导弹，但却误投弃了副油箱，其可能后果是飞机无足够燃油返航。②飞机在武器杀伤半径以内投射武器。比如飞机向地面投射了航空炸弹，那么可能造成本机与地面人员伤亡和财产损失。初始 SMS 软件体系结构表明，悬挂物在选中后即可投射——这不能消除上述两种危险。可能的预防措施是：①增加悬挂物核准功能，通过悬挂物管理程序与飞行员进行交互，确认选中了理想的悬挂物；②增加危险区外校验功能，确保飞机在武器杀伤半径之外投射武器。将这两种危险预防措施用作 SMS 软件体系结构求精需求，求精后的体系结构如图 3(b)所示。

针对图 3(b)所示的软件体系结构，考虑图 2 中的第三个循环。为了保证“投射正确的悬挂物并保证投射行为不危及飞机自身安全”基本目标的实现，契约需要记录“悬挂物核准”、“危险区外核准”两项功能确实执行并且结果符合要求，如表 1 所列。这些契约内容将有助于 SMS 软件体系结构的进一步求精，结果如图 3(c)所示。

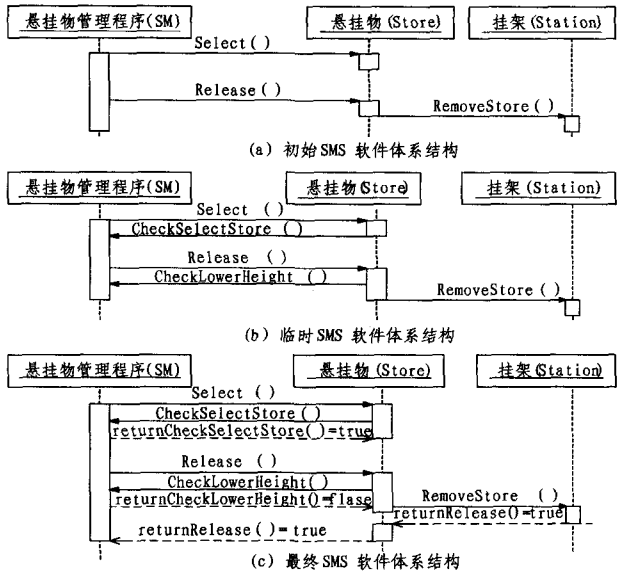

图 3　SMS 软件体系结构设计示意

5　相关研究

本文提出的 IMA 软件体系结构设计方法的思想来源于 ATAM。与 ATAM 致力于在软件体系结构设计阶段均衡实现多种质量属性不同，本文旨在保证 IMA 软件安全性的最优化。这种以安全性为中心的软件体系结构设计方法与经典的软件开发模型——螺旋模型[13]有相似之处。螺旋模型的核心在于软件开发之初无需将所有事情定义得一清二楚，可抓住最重要的功能予以定义并实现。本文层次化设计软件体系结构也是这种抓住主要矛盾、不断细化求精的思想。与螺旋模型每轮都需要进行风险分析一样，本文也要求利用危险场景对每个抽象层次的软件体系结构进行安全性评估。本文方法与螺旋模型的不同之处在于：①本文方法针对的是软件体系结构设计阶段，而螺旋模型涉及到整个快速原型开发周期；②在进行安全性评估时，本文方法侧重静态分析，而螺旋模型侧重动态测试；③推动螺旋演化的动力，螺旋模型仅在于风险，而本文方法除了危险场景外，还在于安全性评估标准和契约。

结束语　IMA 软件体系结构表征了 IMA 软件的基准安全性。本着以安全性为中心的思想，本文改进了 ATAM 方法。在改进的方法中，引入了危险场景评价 IMA 软件体系结构的安全性；引入安全性论据析出 IMA 软件体系结构评估标准和求精方案；引入契约捕获不同抽象层次的 IMA 软件体系结构需求之间的关系。通过一个具体应用案例，验证了以安全性为中心的 IMA 软件体系结构设计方法的可行性。

下一步的工作是细化契约的结构内涵，形式化表示不同抽象层次的体系结构之间的需求关系。

参 考 文 献

[1] NATO. STANAG 4626—2005 Modular and open avionics architecture (Part II: software)[S]

[2] Moir I, Seabride A G. Military avionics systems[M]. Chichester: John Wiley & Sons, 2006: 83-96

（下转第 162 页）

$(j=1,\cdots,k)$；

5) 计算$\sum_{i=1}^{k}\sum_{j=1}^{ti} d_{ij}(x_j,c_i)$；

6) until 每个聚类不再发生变化。

FHE-DK-MEANS 算法——从站点：

1) 从站点 $S_i(i=1,\cdots,n,n\geqslant 3)$分别接收主站点发送的 k 个初始聚簇中心；

2) repeat；

3) 从站点 $S_i(i=1,\cdots,n,n\geqslant 3)$根据主站点发来的初始聚簇中心计算其与本站点数据集 D_i 包含的 $m_i(i=1\cdots n,n\geqslant 3)$ 个对象的距离，确定每个 $m_i(i=1,\cdots,n,n\geqslant 3)$的所属聚类；

4)计算各从站点的聚类中心点及相应的对象个数 $m_{ij}(i=1,\cdots,n,j=1,\cdots,k,n\geqslant 3)$，完全同态加密后 c'_{ij} 和 m'_{ij} 发送到主站点；

5) until 每个聚类不再发生变化。

3 实验结果和分析

本文基于 Weka 平台封装了 FHE-DK-MEANS 算法，对 Weka 的 2 个数据集和 UCI 机器学习数据集中的 3 个数据集进行了 FHE-DK-MEANS 算法和 DK-MEANS 算法的对比实验，实验结果见图 1 和图 2。FHE-DK-MEANS 算法的聚类精度与不加隐私保护的聚类算法聚类精度一致。隐私保护度最高为 91%，最低为 82%。从实验结果可以得出结论，FHE-DK-MEANS 算法在保持较高分类精度的同时也能取得较好的隐私保护效果。

FHE-DK-MEANS 算法中数据在主、从站点间收发，收发的数据均为加密数据，整个过程中任何参与站点均无法获取其他站点的原始真实信息，所以 FHE-DK-MEANS 算法很好地保护了分布式各站点信息的隐私。从实验结果得出 FHE-DK-MEANS 算法的执行时间略高，这是因为加密过程增加了算法的执行时间。

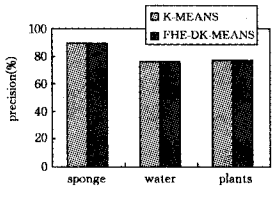

图 1 聚类精度比较

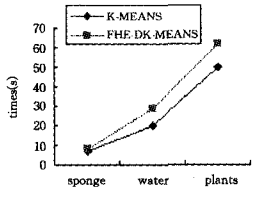

图 2 执行时间比较

结束语 本文针对面向分布式聚类数据挖掘算法中的隐私保护问题，提出了保护效果较好的 FHE-DK-MEANS 算法。算法对从站点数据集采用完全加密算法加密，加密后的数据发送到主站点。主站点对加密数据计算后，根据完全加密算法解密得到结果。主站点得到的结果与原始真实数据集明文传送得到的效果是一致的。理论证明和实验分析均表明该算法能较好地保护隐私数据，同时又能有效保持分布式数据集聚类挖掘的可用性。

参 考 文 献

[1] Rivest R L, Adleman L, Detrouzos M L. On Data Banks and Privacy Homomorphism[C]// Foundations of Secure Computation. New York: Academic Press, 1978: 169-179

[2] Domingo F J, Herrear J I J. A new privacy homomorphism and applications[J]. Information Processing Letters, 1996, 60(5): 277-282

[3] Gentry C. Fully Homomorphic Encryption Using Ideal Lattices [C]// Proc of the 41st Annual ACM Symposium on Theory of Computing (STOC'09). Bethesda, USA. New York, USA: ACM, 2009: 169-178

[4] Kamakshi P, Babu A V. Preserving Privacy and Sharing the Data in Distributed Environment Using Cryptographic Technique on Perturbed data [J]. Journal of Computing, 2010, 2(4): 115-119

[5] Lindell Y, Pinkas B. Privacy preserving data mining[J]. Jorunal of Cryptology, 2002, 15: 177-206

[6] Vaidya J, Lifton C. Privacy-preserving K-Means Clustering over Vertically Partitioned Data[C]// Proc the SIGKDD '03. Washington DC, USA, 2003: 24-27

[7] Kumar K A, Rangan C P. Privacy Preserving DBSCAN Algorithm for Clustering [J]. Advanced Data Mining and Applications, 2007, 4632: 57-68

[8] Li Xiong, Jurczyk P, Liu Ling. Mining Distributed Private Databases Using Random Response Protocols[C]// National Science Foundation Symposium on Next Generation of Data Mining and Cyber-enabled Discovery for Innovation. Baltimore, USA, 2007

[9] Ali İnan, Kaya S V, Saygln Y. Privacy preserving clustering on horizontally partitioned data[J]. Data & Knowledge Engineering, 2007, 63(3): 646-666

[10] 童云海，陶有东，唐世渭，等. 隐私保护数据发布中身份保持的匿名方法[J]. 软件学报，2010，21(4)：771-781

(上接第 130 页)

[3] Aeronautical Radio, Inc. ARINC Specification 653—2006 Avionics application software standard interface[S]

[4] 褚文奎，张凤鸣，樊晓光. 综合模块化航空电子软件体系结构综述[J]. 航空学报，2009，30(10)：1912-1917

[5] NASA. NASA-STD-8719. 13B—2004 Software safety standard [S]

[6] Johnson W G. MORT safety assurance systems[M]. Marcel Dekker, Inc., 1980

[7] 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)：8-13，27

[8] Kazman R, Klein M, Barbacci M, et al. The architecture tradeoff analysis method[C]// 4th International Conference on Engineering of Complex Computer Systems (ICECCS'98). 1998: 35-45

[9] Conmy P M. Safety Analysis of Computer Resource Management of Software [D]. Heslington (England): University of York, 2005

[10] SAE. ARP4761—1996 Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment [S]

[11] Bate I, Hawkins R, McDermid J. A contract-based approach to designing safe systems[C]// 8th Australian Workshop on Safety Critical Systems and Software. Canberra, 2003, CRPIT 33: 25-36

[12] 刘安. 基于模型驱动开发方法的开放式结构悬挂物管理系统研究[D]. 西安：空军工程大学，2010

[13] 郑人杰，殷人昆，陶永雷. 实用软件工程(第二版)[M]. 北京：清华大学出版社，1997