面向可信的航空嵌入式软件开发方法框架

牛文生 李亚晖 吴 际

(中国航空工业集团公司 计算技术研究所, 西安 710068) (北京航空航天大学 计算机学院, 北京 100191)

摘 要: 针对航空综合化软件的可信内涵,即可靠性、安全性和实时性,开展了开发方法的研究,提出了针对性的可信内涵模型和相应的开发过程模型,并设计了基于模型的需求分析、组件化设计以及系统配置综合的开发方法框架. 在开发方法框架研究过程中,重点分析了航空综合化软件平台的特征,即因为物理资源的限制,软件任务之间存在复杂的交互、资源竞争和共享关系,并分析了这些特征对其可靠性、安全性和实时性的影响.

关 键 词: 软件可信性; 航空嵌入式软件; 模型化设计; 组件化设计

中图分类号: TP 311.5

文献标识码: A **文 章 编 号**: 1001-5965(2012)12-1577-05

Dependability oriented avionics embedded software development framework

Niu Wensheng Li Yahui

(Aeronautical Computing Technique Research Institute, Aviation Industry Corporation of China, Xi'an 710068, China)

Wu Ji

(School of Computer Science and Technology, Beijing University of Aeronautics and Astronautics, Beijing 100191, China)

Abstract: A systematic methodology was provided to facilitate the development of dependable embedded avionics software. The dependability primarily denotes to reliability, security and real-time. The dependability attribute model was defined to derive the key aspects to be specified in the stages of analysis and design. A V-model extended process model was proposed to support the co-modeling of system and software. At last, the dependability oriented development methodology was proposed. It consists of model-based requirement analysis, component-based design and system configuration and integration. During the design of the development framework, the characteristics were considered that software tasks embedded in a common integrated platform have to use the resources in a competitive and sharing way due to the limitation of resources. The effects of these characteristics on the reliability, security and real-time are also included in the design.

Key words: software dependability; embedded aviation software; model-based design; component-based design

如何保障软件的可信性已成为近年软件领域研究的重点. 根据 ISO/IEC15408 标准,可信软件的行为在任意操作条件下都具有可预测性,能抵御应用程序软件异常、病毒以及一定的物理干扰所造成的破坏. 一般而言,软件可信性的内涵丰富,主要包括可靠性、安全性、实时性等. 这些不同的"可信"要求具有共性特点,就是要求软件系统行为及其结果符合人们的预期,即使在受到干扰(如操作错误、环境影响、外部攻击等)时仍能正常工作.

航空嵌入式软件规模越来越大,已达数千万行,担负的任务和完成的功能越来越多. 对于安全关键软件,其失效率要求 $10^{-7} \sim 10^{-9}$ 故障/h,实时响应时间为 ms 级. 在综合化嵌入式软件系统中,

收稿日期: 2012-08-29; **网络出版时间**: 2012-11-29 11:04

网络出版地址: www.cnki.net/kcms/detail/11.2625.V.20121129.1104.005.html

基金项目: 航空科学基金资助项目(2010ZC31002)

作者简介: 牛文生(1967-),男,河北邯郸人,研究员,nwsheng@yahoo.com.

多个应用综合在一个平台上共享计算、存储、网络和端口资源等. 因此综合时需要针对平台的资源容量、各个应用的功能、通讯关系、优先级以及具体的可信要求等,确定应用的资源分配策略. 嵌入式软件的可信需求来自于系统(包括硬件、平台和软件)的设计,同时也影响着系统设计. 因为航空嵌入式软件的高质量要求,其开发要遵循强制性标准,如 DO-178B/C 等.

航空嵌入式软件系统涉及任务和应用多,一般由多家开发单位协同开发,研制要求和整体需求由总体单位确定. 开发单位根据给定的要求和平台特征独立进行开发,在达到了相应技术要求后交由总体单位进行集成和综合. 由于不同嵌入式软件应用之间存在着复杂的交互、资源共享和竞争关系,这种各自独立的开发方式并不能保证软件的可信性,主要因为:①嵌入式软件的可信内涵模糊,缺乏有效的技术手段来分析综合方法对软件可信性的影响;②缺乏可信属性的模型化表示方法,无法在需求和设计阶段对可信属性进行相应的描述和分析;③缺乏针对多个可信属性间制约关系的设计方法,无法确保一个满足可信要求的软件综合后仍然能够满足相应要求. 由此可见,传统的面向单个软件的开发过程已经不能满足综合化航空嵌入式软件的开发要求,必须要研究相应的开发过程模型和方法.

1 相关研究

模型化方法近年来在嵌入式软件开发中应用很广. 由于航空嵌入式软件的复杂性,配置依然是一个困难的问题. 模型驱动方法能有效降低配置的复杂程度,能够帮助设计者进行早期的错误检查和确认[1],该方法针对 ARINC653 航电系统,实现从高层体系结构模型生成系统配置表.

基于统一建模语言(UML, Unified Modeling Language)的需求描述方法应用广泛. UML 用例模型提供了直观的描述手段,通过文本式的用例模板对用例及其关联关系进行描述. 由于自然语言文本的语义模糊性,使得用例描述之间、用例描述和用例模型视图之间易出现不一致. 受约束用例建模方法(RUCM, Restricted Use Case Modeling)是在对多种用例建模方法的综合分析[2]基础上提出的一种方法,它综合了自由文本和形式化语言的特点,既保证了需求的易理解性和精确性,同时又能够对需求进行自动化分析与验证[3-4]. 同时,RUCM 需求模型可以转换为高质量的系统分析模型.

尽管在软件和硬件领域都取得了广泛应用,组件化设计在嵌入式系统开发中仍然面临挑战,如软件设计如何和硬件协同,如何考虑平台和环境的异构性、资源限制性使用下的高性能要求等. 解决这些问题的关键是组件模型如何能够支持功能和非功能特性的描述,如何支持整个开发周期. 异构富组件(HRC, Heterogeneous Rich Component)模型[5]是一个突出代表,其定义的组件包括形式化契约,能够支持在早期进行设计验证. 体系结构模型也是组件化设计涉及的一个重要内容,基于契约的体系结构[6]独立于任何范型,可以表达软件结构、行为、数据流以及服务质量. 组件接口及组件契约的形式化描述方法多年来一直是嵌入式软件建模领域的重要研究问题,这些描述方法往往都是针对组件的特定技术特征或者属性进行应用,如接口自动机[7]用于描述组件接口的行为,时间自动机[8]用以描述组件的实时行为,进程代数[9]则关注并发系统中的组件之间同步和异步行为,Petri 网[10]关注资源约束对组件行为的影响等.

2 可信内涵分析及其模型

一般认为,软件可信性涵盖可靠性、安全性、实时性等属性. 软件的可靠性、实时性和安全性是机载系统的核心可信指标,国际组织通过相应标准给出了强制性要求. 即便如此,由于嵌入式软件缺陷而导致的重大灾难和事故仍然屡见不鲜:2004 年 12 月,由飞控软件故障导致 F/A-22 战斗机坠毁;1996 年 6 月,由火箭导航软件发生故障导致阿丽亚娜 5 型火箭发射 37 s 后失败. 因此,如何保证软件的可靠性、安全性和实时性已经成为航空嵌入式软件开发方法的首要关注问题.

航空嵌入式软件通常包括飞行管理、机电管理、显示控制、导航、通讯等. 影响其可信性的因素主要包括:①系统的内存、计算、通信等资源受到质量、能耗、空间等问题的限制,难以通过增加资源来解决可信性问题;②在综合化嵌入式系统中,多个软件组件之间相互影响;③软件系统代码规模巨大,分析和设计错误难以避免,测试难以充分;④系统工作环境恶劣且快速变化,给软件带来严重干扰.

按照 ISO-9126,质量可层次化分解,且得到了大量应用. 但这种分解在实际软件项目应用中却面临问题:①分解时未能明确相应的技术要求,无法指导软件分析、设计和验证;②假设同一层次属性之间相互独立,不符合实际情况;③对于机载嵌

入式软件而言,无法体现其综合化要求. 在综合化平台中,软件之间形成共享和竞争关系. 不仅如此,对于同一个软件而言,由于其所能使用的平台资源固定,单独提升某一个可信属性必然会导致消耗更多的资源,往往会导致其他可信属性的降低.

影响综合化航空嵌入式软件可信的要素诸多,需要建立可信属性内涵模型来分析这些要素. 软件组件及相互间的连接和通讯关系、软件运行环境和平台技术提供的接口、平台提供的资源容量、平台的配置和综合策略等都是需要考虑的因素. 同时,系统的整体可信指标与各个软件组件的可信指标之间也密切关联. 针对这些特点,本文提出了如图 1 所示的可信内涵模型. 其中可靠性方面主要关注的内涵包括故障率、故障传播路径、故障传播范围和故障层次;安全性方面关注信息机密性、信息完整性、访问控制和信息流;实时性关注事件准备时间、运行周期、事件执行截止时间和事件优先级.

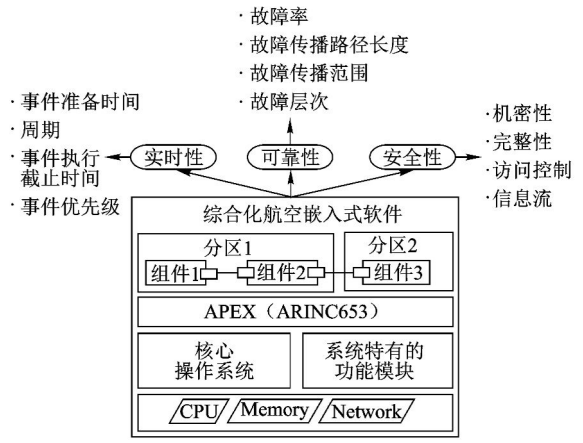


图 1　综合化航空嵌入式软件的可信属性内涵模型

由此可见,软件系统的可靠性、安全性及实时性主要决定于软件组件及其交互(包括分区内交互和分区间交互). 软件组件的可信属性由其设计和实现特性决定,受资源分配、调度和平台可信属性的影响. 操作系统所提供的组件交互机制往往在时间延迟、信息传输、故障传播等方面具有不确定性,也影响着相应的可信属性. 此外,组件之间在资源的竞争性使用使得不同可信属性之间关系复杂,必须进一步明确各个可信属性的技术内涵从而在软件设计模型中加以描述和分析. 这也是本文提出可信内涵模型的动机.

3　航空嵌入式软件开发过程模型

如前所述,可信内涵模型的一个重要作用就是指导软件开发. 事实上,当前大多数开发过程模型(如瀑布模型、螺旋模型、增量式模型和敏捷模型)都以阶段划分为主线,强调软件功能性,对可信属性涉及较少. 对于航空嵌入式软件而言,由于适航认证是强制要求,DO-178B/C 标准对需要开展的活动都进行了详细的规定. 据此,本文提出了包括 5 个阶段的可信开发过程模型.

5 个阶段分别是系统分析与设计阶段、软件分析设计阶段、软件实现与测试阶段、可信验证与分析阶段、软件配置与综合阶段. 和传统的软件开发过程模型相比,面向可信的开发过程模型强调:①软件与系统的综合分析和设计;②关注安全性、实时性和可靠性的分析、设计、实现和测试;③在公共平台上按照相关要求对多个应用进行综合和配置,以确保应用的可信属性;④各个阶段都要进行验证,以达到 DO-178B/C 和适航要求;⑤结合系统配置和综合策略进行测试,对整体可信属性进行验证和分析.

如图 2 所示,该过程是一种 V 模型. 由于系统配置与综合会对可信属性产生影响,因此需要针对配置与综合策略对软件进行重新确认测试,以对可信属性进行验证和分析.

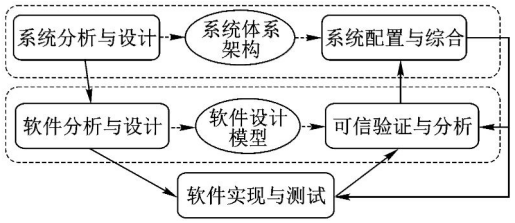


图 2　面向可信的航空嵌入式软件开发过程

在系统分析与设计阶段主要关注系统体系架构建模,描述包括的子系统及其交互关系、子系统包括的组件及其交互关系、组件端口及其支持的交互方式、组件故障处理以及可信属性描述(如延迟时间、故障模式)等. 基于系统体系架构模型,系统配置与综合阶段主要解决平台资源到软件组件的映射和配置、组件的故障处理配置以及调度表设计. 其中故障处理与调度表设计是重点,也是难点. 在故障处理配置中,需要定义故障类型、优先级和严重程度等,据此来配置故障的捕捉、处理和上报机制. 调度表设计的核心是规划 CPU 资源的使用,以确保能满足各个应用的实时性要求. 为了获得可预测的系统行为,航空嵌入式软件系统一般采用静态调度方式. 但是当面对大量非周期的中断事件时,这种调度方式面临着挑战. 系统分析与设计的结果为软件分析与设计提供了相应的需求. 对于高可信要求的航空嵌入式

软件而言,软件设计涉及组件化设计、契约设计、可信属性建模等.在可信验证与分析阶段,将针对软件设计模型和代码,以及测试发现的问题等,对可靠性、安全性和实时性进行分析和验证,如实时性分析、故障传播分析、可靠性估计、安全访问控制分析等.

在软件实现与测试阶段,主要是遵循相关的标准进行编码和测试.标准主要包括可靠性设计标准、安全代码规范和标准、DO-178B/C 代码验证标准等.在测试方面,强调单元测试、配置项测试、系统测试等.

4 可信航空嵌入式软件构造方法

本文的目标是针对航空嵌入式软件特点和要求,提出组件化、模型化和契约化的构造方法.组件化强调组件的接口设计,定义组件的交互模式和协作模式;模型化强调模型层次上的分析和设计,并提供针对可信属性的模型视图;契约化强调基于接口的契约设计,便于可信属性的验证.

一般而言,软件构造方法包括需求分析、设计、编码、测试、集成和测试等活动.由于航空嵌入式软件的编码和测试与一般嵌入式软件相比除了有更明确的相关标准约束外,方法上并无区别.限于篇幅,将重点阐述需求描述模型、组件化设计、配置和综合.针对航空嵌入式软件开发过程中难以准确描述可信属性需求,在软件需求阶段重点分析如何基于功能需求描述软件的非功能性要求,包括可靠性、安全性和实时性.包括非功能性描述的需求模型是后续设计、实现和测试的基础.

4.1 面向可信的需求描述模型

传统上,需求描述主要针对功能.本文在功能需求基础上,将可信属性细化为一系列指标,形成组件可信属性度量指标集.一般需要结合系统体系结构设计和可信要求,分别针对可靠性、安全性和实时性设计相应的度量指标,如图3所示.针对航空嵌入式软件的特点,可靠性度量指标包括故障发生概率、故障传播概率、故障传播路径、故障隔离概率、故障层次等;安全性方面,主要针对组件的机密性、完整性、访问控制及信息流,选择密钥长度、密钥管理方案、访问控制列表、组件接口安全级、机密信息可释放性等度量指标;实时性度量指标包括接口最坏处理时间(WCET)及其变化范围、通信延迟时间分布、调度周期、事件优先级、资源竞争等待时间分布等.针对度量指标的特征,需要选择合适的模型进行描述,如时态逻辑、标记迁移系统、概率模型、谓词逻辑等.

目前实时UML已广泛应用于嵌入式软件的需求分析.针对图3给出的可信属性及其描述要求,图4给出了相应的模型视图设计,其中可靠性、安全性和实时性模型是功能模型的扩展.

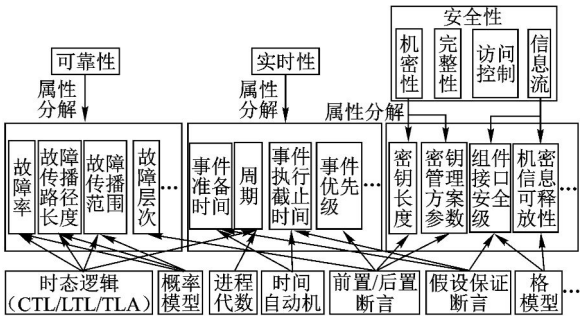


图3 可信属性度量指标分解及其描述

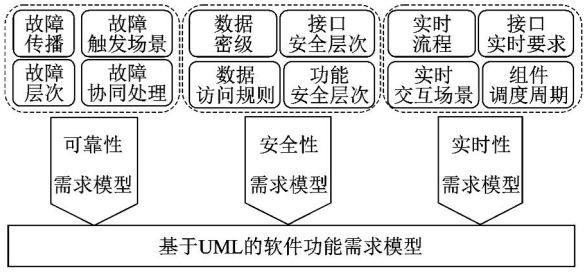


图4 面向可信属性的需求模型视图

在可靠性需求模型中,共有4个视图(圆角矩形),分别是故障传播视图、故障层次视图、故障触发场景视图和故障协同处理视图;在安全性需求模型中,包括数据密级视图、接口安全层次视图、数据访问规则视图和功能安全性层次视图;在实时性需求模型中,包括实时流程视图、实时交互场景视图、接口实时要求视图和组件调度周期视图.需要说明的是,有些模型视图表现为UML图,有些则是UML图中元素的属性描述,如数据密级、接口安全层次、接口实时要求等.

4.2 组件化设计方法

软件组件是一种功能相对完整,能够运行于特定平台上的软件模块.可信组件是指其运行不仅能够满足功能要求,而且具有可信性(实时、可靠、安全).传统软件组件的描述主要关注组件接口规格和功能,可信组件还需要针对可靠性、安全性和实时性进行描述,如输入输出的时间特征(实时性)、组件数据访问接口的安全级别(安全性)、组件的故障处理策略(可靠性)等.在保证软件功能需求的前提下,契约用以对非功能需求进行更加规范的设计.契约设计要求准确规定组件之间的通信,并定义通信过程中的相互责任和预期的结果.因此可信组件设计需要从接口规格、接口契约和可信属性等多个视角来建立模型.

组件化设计的核心是如何识别组件接口契约

和组件可信属性,通过接口和交互机制来组成一个功能完整和满足可信要求的软件系统. 由于组件之间、组件与平台之间存在交互,因此在确定组件接口及其可信契约时需要组件与平台环境参数(如网络带宽、存储空间、时间片分配、组件执行时间阈值等)和组件交互通道(包括网络、堆栈、队列、Socket 通讯链路等)信息.

为了精确描述和设计可信组件的可靠性、安全性和实时性,一般建议采用规范和严格的形式化方法. 主要原因包括:①对可信组件语义的精确描述可确保其需求的确定性、精确性和完整性;②精确的可信组件描述使得可以在开发过程中进行严格验证,能够在设计早期发现潜在的问题;③针对给定的系统设计和可信组件描述,可以使用形式化方法来分析和预测系统的可靠性、安全性和实时性.

4.3　系统配置与综合

系统综合关注如何把多个应用集成到给定的平台上,并能保证整个系统的功能、实时性、可靠性和安全性等达到要求. 系统配置往往是系统综合结果的具体表现,包括平台资源的划分(如网络和设备端口分配)、健康监控策略、调度表等. 系统配置文件在系统加载时读入内存,从而给应用分配资源,进行调度和故障处理等.

针对嵌入式系统的设计模型和软件的可信属性特征,需要在模型上配置平台和软件的相关信息,并设计相应的调度表,从而支持在设计阶段对配置和综合进行验证. 一般而言,航空嵌入式软件系统的可配置信息主要包括组件交互方式、端口分配和连接、端口通讯时延、故障标识及其处理策略、组件数据的安全访问控制原则、组件数据密级、密钥强度设置等. 在调度表设计方面,主要考虑软件任务的周期性要求和计算资源的容量,目前针对航空电子应用软件接口标准(ARINC 653,操作系统分为 2 级:核心操作系统和分区操作系统),主要采用 2 层调度策略,即针对分区的时间片轮转调度,和针对分区内应用的优先级可抢占调度.

5　结 束 语

航空嵌入式软件系统涉及的任务和应用多,具有高安全、高可靠和强实时要求. 一般而言,开发单位根据总体单位给定的平台环境要求和软件需求独立进行开发,在达到了相应要求后交由总体研制单位进行集成和综合. 由于缺少针对性的开发和验证方法,使得独立满足要求的任务软件综合到一起时容易出现整体不能满足要求的问题. 因此,如何解决在综合过程中出现的可信问题一直是航空嵌入式软件领域的困难问题. 事实上,不同软件之间存在的复杂交互、资源共享和竞争关系是导致综合问题的主要原因. 工业领域当前采用的各自独立的开发方式无法充分考虑这些因素,此外当前采用的开发方法主要针对功能,也缺乏针对可信的考虑.

本文以航空嵌入式软件的可信问题和内涵作为切入点,提出了可信内涵模型. 在此基础上,提出了基于航空嵌入式软件的开发过程模型,并进一步提出了面向可信的软件构造方法,重点是需求建模、组件化设计、配置与综合方法. 本文所研究和提出的模型和方法已经在作者单位承担的重大工程项目中进行了部分成功应用,取得了很好的效果.

参考文献(References)

[1] Horvaúth A, Varró D, Schoofs T. Model-driven development of ARINC 653 configuration tables[C]//Chris Watkins. Proc of Digital Avionics Systems Conference (DASC). Salt Lake City: IEEE, 2010: 5. A. 5-1-5. A. 5-115

[2] Yue, T, Briand L C, Labiche Y. A systematic review of transformation approaches between user requirements and analysis models[J]. Requirements Engineering, 2011, 16(2): 75-99

[3] Yue, T, Briand L C, Labiche Y. Model driven engineering languages and systems[M]. Heidelberg: Springer, 2009: 484-498

[4] Yue, T, Briand L C, Labiche Y. Automatically deriving a UML analysis model from a use case model[M]. Ottawa: Carleton University, 2010

[5] Josko B, Ma Q, Metzner A. Designing embedded systems using heterogeneous rich components[C]//Schreinemakers P. Proc of INCOSE Inter Symp. Utrecht: Springer, 2008: 247-258

[6] Waignier G, Meur A F, Duchien L. Architectural specification and static analyses of contractual application properties[M]. Heidelberg: Springer, 2008: 152-170

[7] Luca de Alfaro, Mariëlle Stoelinga. Interfaces: a game-theoretic framework for reasoning about component-based systems[J]. Electronic Notes in Theoretical Computer Science, 2004, 97(22): 3-23

[8] Alexandre D, Larsen Kim G. Timed I/O automata: a complete specification theory for real-time systems[C]//Proc of the 13th ACM Inter Conf on Hybrid Systems: Computation and Control. New York: ACM, 2010: 91-100

[9] Nicola R D, Segala R. A process algebraic view of input/output automata[J]. Theoretical Computer Science, 1995, 138: 391-423

[10] Hamadi R, Benatallah B. A petri net-based model for web service composition[C]//Proc of the 14th Australasian Database Conference. Darlinghurst: ACM, 2003: 191-200

(编　辑:文丽芳)