航天嵌入式软件可信性保障技术及应用研究

杨孟飞^{①*}, 顾斌^②, 郭向英^②, 董晓刚^②, 王政^②, 陈睿^②

① 中国空间技术研究院, 北京 100094;

② 北京控制工程研究所, 北京 100190

* E-mail: yangmf@bice.org.cn

收稿日期: 2014-12-06; 接受日期: 2014-12-30

国家中长期科技发展规划重大专项和国家自然科学基金(批准号: 91118007)资助项目

摘要 研究了航天嵌入式软件可信性保障的问题和现状, 提出了航天嵌入式软件的可信保障技术体系, 并针对动态时序正确性、程序实现正确性和控制行为正确性保障等核心关键可信问题的理论方法和技术进行了深入研究, 在此基础上研制了相应的保障工具, 形成了航天嵌入式软件可信性保障集成环境. 本文的研究成果在月地高速再入返回飞行器软件研制中进行了应用, 为飞行任务的成功作出了贡献.

关键词
航天器
可信软件
嵌入式

1 引言

软件在航天器中的作用和地位越来越突出, 软件的可信性直接关系到航天任务的成败. 所谓可信, 是指系统提供可信赖服务的能力. 可信是正确性、可靠性、安全性、可用性、可维护性、完整性等属性的集合^[1]. 这是在传统的可靠、安全等概念基础上发展起来的一个学术概念. 一般认为, 可信是指一个实体在实现给定目标时其行为及其结果是可以预期的, 它强调目标与实现相符以及行为和结果的可预测性和可控制性. 软件的可信是指软件系统的动态行为及其结果总是符合人们的预期, 在受到干扰时仍能提供连续的服务^[2]. 对于航天型号软件, 可信性主要关注正确性、可靠性、安全性属性.

可信软件研究在国内外受到学术界、工业界和政府的广泛重视, 美国国防部先进研究项目局(DARPA), 美国国家科学基金会(NSF), 美国国家航空航天局(NASA), 美国联邦航空管理局(FAA), 美国

国防部(DoD)以及欧洲航天局(ESA), 欧盟的 FP5 和 FP6 计划也都把高可信软件作为软件技术发展的重点, 并先后支持了很多项目. 但尽管如此, 总体上来说, 由于问题的复杂性, 到目前为止, 可用的成果有限, 只是针对特定的某个问题有一些解决方法和工具, 还没有系统的解决方案可用.

本文面向我国航天任务对软件的可信保障需求, 详细分析了影响航天嵌入式软件可信性的几个核心问题, 提出了一种系统的可信保障技术体系, 并给出了相关研究内容的进展.

2 影响航天嵌入式软件可信的十个核心问题

嵌入式系统由硬件、软件和环境 3 部分组成, 与外部连续变化的物理环境不断交互和在特定的物理平台上运行是嵌入式系统的 2 个重要特征. 除此之外, 航天嵌入式软件还具有强实时、分布异构、运行环境

引用格式: 杨孟飞, 顾斌, 郭向英, 等. 航天嵌入式软件可信性保障技术及应用研究. 中国科学: 技术科学, 2015, 45: 198–203
Yang M F, Gu B, Guo X Y, et al. Aerospace embedded software dependability guarantee technology and application (in Chinese). Sci Sin Tech, 2015, 45: 198–203, doi: 10.1360/N092014-00485

恶劣和资源受限等特点, 根据嵌入式软件的这些特征, 通过对近 10 年来型号软件第三方评测和 AIT 阶段发生的问题进行分析研究, 影响航天嵌入式软件可信性的问题可总结为如下 10 个问题.

1) 时序问题. 对安全关键实时系统来说, 实时性就是一切. 实时系统的正确性不仅依赖于计算结果的正确性, 还依赖于输出结果的时间. 航天器实际上是一个分布的、网络化的嵌入式系统, 在这个系统中各个控制单元采用相同或不同的中央处理单元 (CPU) 及编程语言, 彼此之间通过各种串口、并口或总线, 采用中断或查询方式进行通讯, 在这样一个集中和分布、同构和异构、同步和异步、顺序和并发、离散和连续并存的系统中运行, 软件和系统的实时性问题十分复杂.

2) 内存使用问题. 嵌入式软件本质上都是基于物理模型的, 因此不可避免地会使用数组、指针, 结构体、联合体等数据结构, 数组越界、指针的非法使用问题时有发生. 嵌入式软件中存在很多与指针相关的运行时错误, 如空指针引用、指针变量未初始化、非法地址访问、内存泄露和重复释放等. 嵌入式软件运行在受限的堆栈资源上, 还容易出现堆栈溢出问题.

3) 数据使用问题. 嵌入式软件中数据的种类和数量很多, 对数据类型定义、数据的完整性和一致性等有严格要求, 变量未初始化, 变量取值超出指定范围等问题时有发生; 另外嵌入式软件中不可避免的会包含大量数值计算, 由于涉及许多整型、浮点型变量, 很容易导致除零错、算术溢出等运行时错误; 中断或多任务机制会引起程序中复杂的数据交互, 如果同步、互斥机制设计不当, 将产生数据竞争、原子性破坏等数据访问冲突问题.

4) 数值计算误差问题. 计算机本身存在着很多局限性, 特别是在处理以浮点数表示的数据方面, 由于受到选用的浮点系统精度的限制, 大部分实数都无法被计算机精确存储 (舍去了若干位有效数字), 而这些不精确的存储将会影响计算结果. 此外, 在浮点表达实数的计算中, 新的误差也会随着一步步的中间运算不断产生. 迭代、大数与小数相加或相除等都直接影响着运算结果精度.

5) 通讯协议正确性问题. 嵌入式软件运行时要与外部环境进行大量交互, 软件的运行结果依赖于从外部获得的各种数据和指令, 软件必须能够及时

发送和接收数据, 并具有较强的容错能力和抗干扰能力. 通信协议主要用于规定各种数据的传输规则, 对发送和接收之间进行同步的协调, 确保发送和接收的正确性. 如果缺少一个严格、规范的通信协议, 将无法保证数据传输的正确性和通信的可靠性.

6) 状态转换问题. 计算机控制系统是一种离散系统, 它通过执行程序实现控制功能, 控制程序由若干功能模块和分支组成, 程序的执行实际上就是依据不同的条件, 在这些程序分支和模块间的转移, 具有有限状态机的特征. 航天嵌入式控制软件就是这样的一种系统, 通常它由若干飞行模式 (或状态) 组成, 根据各种线性或非线性条件、时间或地面指令等进行转换. 各种状态的转换 (进入退出条件) 是否存在冲突、遗漏和死锁, 是否有不可达分支等都将影响系统控制行为的正确性.

7) 故障处理问题. 嵌入式软件的输入输出充满了不确定性, 对航天软件来说, 严酷的空间环境还时刻可能会改变其运行状态. 各种容错、纠错和检错技术、故障的诊断隔离与恢复 (FDIR) 技术以及健康管理和运行时监控等技术可缓解这种不确定性带来的风险, 但不安全状态的存在始终危害着软件提供服务的能力. 系统正常行为和异常行为的刻画、异常行为的传播与控制等是正确进行故障处理的关键. 故障处理正确性是指在系统和软件出现故障时, 对故障进行合理的识别、规避和处理, 使软件在故障情况下行为可预测.

8) 编译等价性问题. 编译程序的实现算法较为复杂. 这是因为它所翻译的语句与目标语言的指令不仅有一一对应关系, 还有一对多的对应关系; 同时也因为它要处理递归调用、动态存储分配、多种数据类型, 以及语句间的紧密依赖关系. 正是由于编译过程的复杂性, 编译本身会引入错误, 编译也不能保证源程序和目标程序的等价性. 使用不同的编译器对同一个源程序编译生成的目标程序, 可能有不同的运行结果.

9) 编码问题. 嵌入式系统普遍采用 C 语言和汇编语言编程. C 语言灵活的编程方式和语法规则存在许多不安全性, 如其弱类型机制将导致程序中不同类型的隐式转换、数组越界、指针非法引用等安全问题. 此外, 在程序跳转、过程调用、循环控制、类型转换、比较判断、运算处理、初始化等方面. 如何避开所有可能带来危险的编程方式, 编写出更为安全、

健壮的代码是提高软件可信性的基础。

10) 各阶段一致性问题. 软件的开发过程本质上是基于文档的, 自然语言的文档只能由人阅读和理解, 难以严格分析和推理, 从非严格的需求和设计到复杂的最终程序, 跨越距离太大, 使人难以评判它与需求的关系^[3,4]. 此外, 从源程序到最终运行的目标程序, 中间还要经过编译, 如何保证各阶段的一致性永远是一个巨大的挑战, 测试发现问题的能力很有限, 不能成为评判标准。

十大可信问题具有共性, 类似的问题在航空、轨道交通、汽车电子等安全关键领域也存在, 但在不同的领域问题的表现形式不同, 不同的领域关注的重点也可能不同. 十大可信问题本质上反映的是影响一个嵌入式系统不确定性的各种因素, 如果这些因素的可信性得到保障, 我们认为系统的可信性会相对得到保障。

3 可信保障技术体系

软件可信性是一个内涵广泛的概念, 并不存在一种单独的方法能够完全保证软件可信. 保证软件的可信性需要在软件生命周期的各个阶段避免、消除、预测导致软件不可信的因素. 没有任何单独的一种方法或技术可以解决十大可信问题中的任何一个问题, 单纯依靠经验, 在软件中采取一些局部的安全防范措施是一种简单的、不完善的方法, 单独解决一两个方面的问题也并不能保证软件的可信性, 只有建立一套软件可信性保障技术体系, 即运用系统工程的方法, 将问题分解, 通过在软件研制各阶段综合采用各种方法或技术, 这些问题才可能有效预防或解决。

本文提出了一种基于可信要素的可信性保障五维体系结构模型(图 1), 即针对每个可信问题, 首先应识别出该问题在软件研制各阶段的要素或子要素, 然后针对每个要素或子要素, 研究相应的理论、方法或技术, 在此基础上, 将其中可物化的理论、方法或技术形成工具, 将难以物化的形成相应的规范、指南或规则、检查表等. 要素回答的是做什么的问题, 即解决这个问题要从哪些方面做工作, 做些什么, 要关注些什么. 理论、方法、技术或工具回答怎么做的问题, 即每个要素用什么方法去解决, 度量回答的则是否做到位, 即做的好坏问题。

图 1 基于可信要素的可信性保障五维体系结构模型

可信要素指的是影响可信性的最重要的、本质的因素, 是可信性保障技术体系的核心. 可信要素表述了解决各可信问题时需关注的主要工作内容, 是软件可信性保障的基本工作单元, 针对前面提出的 10 个可信问题, 要素给出了软件产品研制各阶段中需开展的基本工程活动, 它表征了主要内容和项目. 子要素表述了各个工作项目需要细化的要点, 子要素是要素的展开和细化, 是为落实各要素而确定的基本工作要点, 也是可信保障的核心对象, 所有的可信保障活动均应根据子要素展开实施. 可信要素可从下到上即从知识体系中得出, 也可从下到上即从经验教训中提炼总结, 它体现了一种正向的设计思想。

只有全面深入地把握航天嵌入式软件的可信性要素、各可信性要素之间的关联、影响可信性要素的各种内在外在因素、以及可信性在软件研制各阶段间的传递, 才可能构造出可信的航天嵌入式软件. 以时序正确性保障为例, 在一个典型的中断与任务并存的嵌入式系统中, 在分析设计阶段, 需要关注的要素包括超时问题、并发过程引起的数据竞争问题以及逻辑顺序违反问题. 时序问题主要在分析和设计阶段解决, 编码作为一种加工实现, 对实时性并没有显示的影响, 但是否按规则编程对程序的时序分析会有影响. 在测试阶段, 如何测试和验证各种实时性需求是否得到满足? 除进行强度、余量和边界等测试外, 还应通过改变输入的时刻、时间、先后顺序和间隔进行, 如加快指令(如遥测、遥控)的频率、加快或拉长事件连续发生的间隔、改变 2 个不同事件的先后顺序、模拟各种事件同时发生、数据传输量超过设计允

许的最大值、长时间(保持在极限状态下)运行等。

4 关键技术研究进展

本文重点研究了十大可信问题中 6 种问题正确性保障的相关理论、方法和技术。6 种问题归纳为动态时序正确性保障、程序实现(内存使用问题、数据使用问题、编码问题)正确性保障和控制行为(数值计算误差问题、状态转换问题)正确性保障 3 大类, 下面简要介绍其中一些关键技术研究进展。

4.1 动态时序建模与验证技术研究

针对嵌入式软件的特点, 构造了各种任务与中断处理的自动机模型, 以刻画任务与中断处理的执行时间、中断触发条件与频率、中断优先级、中断与任务间关联、交互行为、共享资源存取、中断屏蔽等特性, 同时用时态逻辑将待验证的时序性质表示出来, 在此基础上, 采用基于空间遍历的模型检验算法和有界模型检验算法进行检验。前者是对时间自动机模型检验算法的改进, 可以完整遍历所有的状态空间并发现模型中的所有错误, 后者从初始状态出发, 使用深度优先的方式遍历所有长度小于等于 K 的路径。对于每条路径, 首先根据时间条件生成线性不等式, 并调用 SMT(satisfaction module theory)求解器进行求解, 以判断该路径是否可行, 并判断是否可能违反系统的时间规约, 这种方法可以使用有限的 CPU 和内存资源发现系统模型中存在的大部分错误。另外, 针对现有静态方法无法处理中断的问题, 研究了基于模型检验的、面向中断的最坏执行时间(WCET)分析技术, 以各中断处理程序的 WCET 作为输入, 分析得到动态情况下的 WCET 信息, 以适用于软件的 WCET 分析需求。

4.2 数据访问冲突检测理论与方法研究

数据访问冲突一直以来都是国内外研究的热点和难点, 也是当前航天嵌入式软件研制中突出问题之一, 这类问题难以通过传统的测试手段发现, 遗漏率较高。数据访问冲突发生在主程序与中断或低级中断与高级中断对同一个共享数据单元进行同时访问、且至少其中一次是写操作时。由于两次访问之间的次序不确定, 程序会因此产生非预期行为, 如数据的完整性被破坏以及信号丢失等。目前国内外大多

数研究面向多线程等并发机制, 由于航天嵌入式软件中通常采用中断实现并发, 这与线程在中断并发语义等方面存在较大差异, 这些成果难以适用。针对该问题, 本文从多个维度对该类缺陷的特征进行了系统地分析, 提炼出了 7 类缺陷模式, 在此基础上, 提出了一种基于变量访问序的静态中断数据访问冲突检测方法, 即通过轻量级程序模型检验技术建立整个软件系统的全局变量访问索引树, 然后对该树进行遍历, 查找其中违反特定访问序模式的场景, 进一步地根据缺陷场景的特征要素(如连续访问之间的距离、读写模式等)对缺陷危险程度进行排序。该方法基于实例研究的成果, 具有更强的缺陷针对性, 精确性较高。

4.3 需求建模与验证理论和方法

在需求分析阶段正确、清晰、无二义性地需求描述, 并进行分析和验证以便尽早发现可能存在的问题对可信软件的开发至关重要。航天嵌入式控制软件具有周期性、计算复杂、逻辑状态组合繁多、模式切换条件复杂等特征。针对这些特点, 提出并设计了一种航天需求形式化描述语言(SPARDL), 并基于该语言研究并实现了基于方程不动点的数据流分析问题求解方法与类型检查方法。在此基础上, 为了分析需求模型的正确性, 以区间时序逻辑(ITL)为基础, 给出了相应的性质描述语言, 通过引入 SPARDL 的随机语义(stochastic semantics), 设计了新的将线性时态逻辑(line temporal logic LTL)转化成相应自动机的验证算法与概率模型检查算法, 可有效地对 SPARDL 需求模型进行验证。根据 SPARDL 形式化模型, 还可以快速生成原型代码, 这样, 在需求分析阶段, 软件工程师就可以快速地对软件的动态行为进行仿真分析。与其他建模和分析验证工具相比, SPARDL 提供了针对航天嵌入式领域特点的建模元素, 因而具有效率高, 功能强等优点。

4.4 可信编程规范检查技术研究

编程规范被广泛认为是保障代码质量的有效手段。基于航天嵌入式软件的特征和可信需求, 本文提出了航天嵌入式软件可信编程规范, 构造了 1 个 C 语言可信子集。在此基础上, 研究了面向大规模嵌入式 C 程序的精确、高效的编程规范检查技术, 保证可信编程规范的有效实施。给定被分析软件的源代码, 首

先通过语法分析、语义分析获得程序的抽象语法树、符号表、控制流图、调用关系图、定义引用关系链等中间表示;然后,规则检查器采用语法树匹配、符号表检索、数据流信息查询、类型检查等技术实现对可信编程规范的检查.本文提出的编程规范检查技术采用了跨文件、跨过程的全局数据流分析,支持路径敏感的分析.同时,依靠对中间表示的快速序列化和恢复,可实现高效率的分析.实验验证和应用表明,本文提出的编程规范检查技术对数十万行的航天嵌入式 C 程序进行完整分析仅需要数十秒.

4.5 可信保障集成环境

按照可信性保障技术体系将软件可信性保障方面研究的理论、方法、技术和工具,以一定方法或模式组织起来,并使之相互协调成为一个有机整体,最终构造出嵌入式软件可信性保障集成环境 SpaceIDep.

本文提出并实现了一种层次化的基于双层软件总线的体系结构模型,并定义了适用于该模型的集成环境接口规范.集成环境分为数据层、总线层、功能层和过程驱动层(图 2).局部总线提供特定研制阶段的中心数据模型,解决研制阶段内的工具与数据的互操作;全局总线则通过对最一般的工具操作和数据类型定义,实现阶段间的工具调用和数据传递.工具按照其工作阶段,通过适配器连接到不同的局部总线上.接口规范是实现工具集成和工具间交互的通信协议.接口规范包括工具集成规范、数据模型和应用编程接口定义 3 个部分,其中工具集成规范规定了工具适配器的组成、结构、工作方式,以及工具发现和工具注册的步骤与要求.数据模型定义则规

定全局总线和各局部总线的数据模型,为工具间的调用和数据交互提供依据.应用编程接口则具体实现了工具间的交互,具体包括工具功能调用接口(包括局部总线内调用和全局总线调用)、数据访问接口、界面编程接口 3 大类编程接口,供工具适配器在运行时调用,实现工具之间、工具与集成环境之间的功能调用和数据交互.

5 应用情况

本文的研究成果在月地高速再入返回飞行器中进行了应用.飞行器整器采用双冗余的二级 1553B 总线组成器上通信网络,利用嵌入式技术,构成功能密集、配置灵活的分布式容错计算机系统结构,并实现信息交互.数管分系统、制导导航与控制(GNC)分系统、工程参数测量分系统、测控数传分系统和供电分系统共配置有各类软件几十套,为了确保这些软件的可信性,利用 SpaceIDep 对其中的部分软件进行了专项检查,发现了一百余处规则违反、5 个有害数据竞争等问题、对关键的 GNC 软件中的数组越界、空指针引用、除零等问题进行了专项验证.应用结果表明 SpaceIDep 不仅可有效地预防和发现问题特别是一些隐藏较深不易发现的问题,而且可大大提高效率,如分析一个 3 万行代码中的数据竞争问题,原来没有工具,完全依靠人工分析需要 3~5 个人日,而且问题经常遗漏,现在用 SpaceIDep 检查只需要 3~5 人时,效率提高了约 8~10 倍、分析其中的可信编程规范问题,原来使用国外的商业工具如 QAC 等需要 10 人时,现在只需要 2 人时左右,效率提高了约 5 倍.

图 2 (网络版彩图)航天嵌入式软件可信性保障集成环境体系结构示意图

6 总结

本文深入研究了影响航天嵌入式软件可信性的几个关键问题, 初步研制完成了一个开放、可扩展的航天嵌入式软件可信集成环境 SpaceIDep, 部分研究

成果已在航天型号研制中应用并发挥作用, 为确保型号研制的顺利进行和成功做出了贡献. 下一步, 我们将继续探索和研究可信软件构造的新的理论、方法和工具, 以满足航天嵌入式软件的可信需求, 为国家航天任务的顺利实施提供支撑.

参考文献

- 1 Avizienis A, Laprie J C, Randell B, et al. Basic concepts and taxonomy of dependable and secure computing. *IEEE T Depend Secure*, 2004, 1: 11–33
- 2 刘克, 单志广, 王戟, 等. “可信软件基础研究” 重大研究计划综述. *中国科学基金*, 2008. 145–151
- 3 Abrial J R. Formal methods in industry: Achievements, problems, future. *ICSE*, 2006, 5: 761–768
- 4 Henzinger T A, Sifakis J. The embedded systems design challenge. *Lect Notes Comput Sc*, 2006, 4085: 1–15

Aerospace embedded software dependability guarantee technology and application

YANG MengFei¹, GU Bin², GUO XiangYing², DONG XiaoGang², WANG Zheng² & CHEN Rui²

¹ *China Academy of Space Technology, Beijing 100094, China;*

² *Beijing Institute of Control Engineering, Beijing 100190, China*

In this paper, the current status of software dependability guarantee in aerospace embedded domain is discussed, and the challenges in this topic are surveyed. The aerospace embedded software guarantee technology architecture is proposed. Moreover, theories and methodologies to keep the correctness about dynamic temporal, program implementation, and control behaviors are deeply researched. Based on these theories and methodologies, aerospace embedded dependable software guarantee integrated environment is developed. The most significant contribution of our research is that the achievements are applied in the development of embedded software which is deployed in the lunar-earth high speed re-entry return spacecraft, and make contribution to its success.

spacecraft, dependable software, embedded

doi: 10.1360/N092014-00485