

AADL 模型的形式化研究

刘 玮,李蜀瑜

(陕西师范大学 计算机学院,陕西 西安 710062)

摘 要:在嵌入式系统建模领域,AADL 以其软硬件协同建模的特点已经逐渐成为业界的标准。围绕 AADL 的形式化特点,国内外众多学者展开了热烈的讨论。为了帮助系统开发人员深入了解 AADL,指导软件开发进程,提高基于 AADL 模型的软件开发效率,分别从 AADL 模型可靠性分析、可调度性分析以及 AADL 模型测试这三个不同角度综述了已经出现的各种 AADL 形式化验证理论,对比分析了它们的优点和不足。简要介绍有关 AADL 验证工具,研究基于 AADL 模型的嵌入式开发平台的构建。

关键词:模型驱动;结构化分析和设计语言;形式化研究;开发平台

中图分类号:TP31

文献标识码:A

文章编号:1673-629X(2013)09-0043-03

doi:10.3969/j.issn.1673-629X.2013.09.011

Research on Formalization of AADL Model

LIU Wei,LI Shu-yu

(College of Computer,Shaanxi Normal University,Xi'an 710062,China)

Abstract:In the embedded system modeling field,the AADL has gradually become the industry standard because it has the characteristics of modeling hardware/software collaborative. Based on the AADL formal characteristics,many domestic and foreign scholars launched a warm discussion. In order to help the system developers better understand AADL,guide the software development process,improve software development efficiency, discuss the AADL model from reliability analysis, schedulability analysis and AADL model testing on the three different viewpoint of the AADL formal verification theory. By contrast,it analyzes their advantages and disadvantages. Briefly introduce the AADL verification tool,then focus on the issue that how to construct embedded software development platform based on AADL.

Key words:model driven;AADL;formalization research;development platform

0 引 言

随着计算机应用领域的不断扩张,计算机软件的开发规模逐渐扩大,软件复杂度不断增加,开发周期和开发成本也不断增长。为了解决这些问题,对象管理组织(OMG)提出了模型驱动结构方法(Model Driven Architecture)^[1]。MDA 的核心思想是以模型为中心,将模型和实现分离,使软件开发过程简化为建立业务逻辑模型后由机器自动生成特定计算平台的代码。在 MDA 中,建模语言不仅仅是设计语言,也是编程语言。图 1 为使用 MDA 方法的软件开发过程。

针对嵌入式领域中的软件开发复杂度问题,业界提出一种基于 MDA 方法的体系结构建模语言-体系结构分析设计语言(Architecture Analysis and Design Language,AADL)^[2]。AADL 是用于设计和分析安全

关键的嵌入式实时系统的软件和硬件体系结构的建模语言。从数学的角度来考虑,AADL 模型只是一种半形式化的建模语言,只是对构件相应的属性进行了描述,例如线程执行时间描述、构件的安全等级描述、构件的模型错误附录树的描述。如果想对 AADL 模型架构的非功能属性进行分析,还需要对模型构件的属性进行形式化验证。AADL 的形式化验证就是将 AADL 模型降阶转化为其他的形式化工具,通过形式化的方法找出 AADL 模型中的错误,然后通过对 AADL 模型进行纠正改进,进而获得高可靠性的 AADL 模型,为开发大规模复杂、安全可靠的嵌入式系统打下坚实的基础。在国内,目前围绕 AADL 模型的形式化研究已经成为了一个热点,针对当前 AADL 模型的形式化研究,综述了它们的研究理论和不足,为嵌

收稿日期:2012-11-27

修回日期:2013-03-02

网络出版时间:2013-05-09

基金项目:中央高校基本科研业务费专项资金(GK2010002011);教育部科学教育重点项目(107106)

作者简介:刘 玮(1984-),男,硕士研究生,研究方向为嵌入式软件;李蜀瑜,副教授,硕士生导师,研究方向为 Web 服务与组合、嵌入式系统。

网络出版地址:<http://www.cnki.net/kcms/detail/61.1450.TP.20130509.1058.024.html>

嵌入式软件的早期开发提供参考。

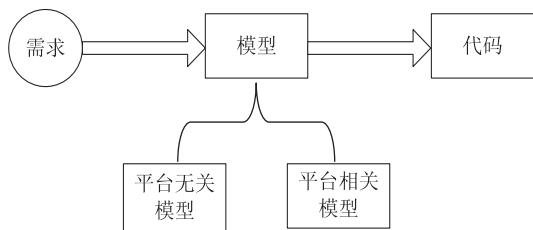


图 1 使用 MDA 方法的软件开发过程

1 AADL 的可靠性研究

基于 AADL 的可靠性分析评估主要通过将 AADL 转换成 Petrie 网形式化模型,通过一些形式化工具来验证。目前已经有很多学者基于这个思路来分析 AADL 模型的可靠性。文献[3]提出将 AADL 嵌入式系统模型转换成可靠性计算模型广义随机网(GSPN),基于 GSPN 可靠性计算模型对嵌入式系统进行可靠性验证,实现了可靠性分析评估的自动化。并且根据模型转换的形式化方法,设计实现了 AADL 的可靠性评估工具 ARAM(AADL Reliability Assessment Model)。文献[4]提出了将 AADL 模型转换为广义随机网的可靠性验证方法,不过它在已有的基本转换规则的基础上,重点讨论了系统中组件之间错误传播以及系统发生模型转换的 Guard_Transition 属性到 GSPN 的转换规则,并以飞行控制系统数据发送和处理单元为实例,验证了转换规则和可靠性建模与评估的可靠性。文献[5]分析了软件内部各种错误状态及其之间的错误传播,构建了 AADL 软件系统错误模型,并根据基本的转换规则将其转换为广义随机网,使用现有的工具对其进行了计算,从而实现了软件容错系统的可靠性评估。文章以航空交通控制系统(ATC)为应用场景进行实验,分析了部分构件的失效率,收到较好的效果。

AADL 模型到广义随机网的可靠性计算模型的转换是目前最主要的可靠性评估方式,因为它既考虑了单个构件的验证,也考虑了构件之间的依赖关系,因此它可以从整体上考虑系统的可靠性。AADL 模型可靠性在验证过程需要反复迭代来获取,这可以帮助工程开发人员深入理解系统模型结构和属性。

2 AADL 可调度性分析

由于嵌入式软件系统对系统的非功能要求非常严格,尤其是系统的响应时间,因此设计基于 AADL 模型的嵌入式系统时,如何能够实时快速的响应系统是 AADL 可调度性分析的关键。文献[6]针对 AADL 模型的可调度验证问题,提出了利用模型检测工具 UPPAAL 对其线程组件在非抢占性调度策略下的可调度性进行形式化分析和验证并实现了从 AADL 模型到

UPPAAL 中模型的模型转换工具。文献[7]则更进一步实现了 AADL 行为模型的分析验证。文章首先基于行为附件的文法结构以及行为描述方式提出了 AADL 模型与 UPPAAL 下时间自动机的模型转换规则。然后在转换规则的基础上,设计和实现了模型转换的原型工具。并以航天器控制中制导、导航与控制计算机从陀螺取数的 AADL 模型为例,经自动转换规则得到的自动模型在 UPPAAL 下仿真、验证其行为正确性,同时也证明了模型转换的有效性。虽然 UPPAAL 是一种良好地分析 AADL 模型可调度性的工具,但是在实践中它也有自己的缺点,例如难以描述进行可抢占调度策略下的 AADL 模型的可调度验证。文献[8]则对此进行了补充,它根据 AADL 与带约束的时钟自动机理论概念,设计了一种对 AADL 模型的可调度性进行验证分析的工具 UCaaS。并对 UCaaS 工具的性能进行了测试。不过虽然 UCaaS 实现了可抢占策略下的 AADL 模型的可调度性,但是它的执行效率比较低,稳定性不够。还需要进一步完善算法,提高执行效率。

在基于 AADL 的可调度性上,时间自动机是一种重要的形式化方法。将 AADL 降阶转换为时间自动机,利用基于时间自动机的验证工具进行验证是目前的主要方法。在基于 AADL 模型可调度性分析上,也有其他一些理论方法。文献[9]提出了将 AADL 模型转换成时间 Petri 网的形式化验证方法,并介绍基于时间 Petri 网的模型检测工具 TINA 的结构。这个工具的工作原理是首先将 AADL 模型转换成 Fiacre 中间语言,然后将 Fiacre 模型用抽象时间自动机编译验证,从而间接验证 AADL 模型调度的正确性。这个工具已经作为一个插件被集成在 TOPCASED 工具里。以上的基于 AADL 模型的分析主要就是针对 AADL 的调度性进行形式化建模,是确保嵌入式系统实时性的关键。

3 AADL 模型测试方法

目前 AADL 已经广泛应用于嵌入式系统领域,如何保证任务关键软件的质量,还需要给出 AADL 的测试模型,对 AADL 设计模型进行测试。基于这个问题,文献[10-11]分别提出了基于模型检测的 AADL 架构验证方法。该方法应用马尔可夫链描述 AADL 架构的行为,然后根据得到的马尔可夫链模型以及系统设计标准生成相应的测试用例和测试语言,并通过测试用例执行输出和期望值的比较判断 AADL 模型的正确性,实现对系统 AADL 模型的测试;最后通过案例分析证明了该方法的有效性。

基于马尔可夫链的 AADL 模型测试方法是一种静态测试方法,它的模型转换主要基于单个的构件,当考虑整个系统结构时可以采用分层的方式描述构件的操

作模式和错误状态。由于它仅仅是针对构件的迁移和状态进行测试,故缺少对构件之间连接通信的分析。目前基于马尔可夫链的模型测试方法只能停留在理论分析的层面,没有针对其理论的工具出现。而对于复杂结构的 AADL 模型,如何生成合适的测试用例使其能够达到测试模型所需要的覆盖率以及如何优化测试用例等也是需要进一步认真研究的地方。

在基于测试模型的构造研究上,文献[12]给出了体现系统拓扑结构的 AADL 测试模型的形式化定义以及由 AADL 构造该测试模型的算法。基于该测试算法可对 AADL 设计模型中构件交互的输入、输出端口序列和连接的正确性进行测试。文章最后以飞行控制系统的 AADL 设计模型为例,阐述了整个分析过程。由于 AADL 测试模型是检测 AADL 设计模型设计是否正确,设计模型中还存在哪些错误的重要途径。所以基于 AADL 的测试模型构造也是 AADL 研究的重点的内容。

4 基于 AADL 的形式化验证工具及软件开发平台

由于形式化方法在基于 AADL 模型的嵌入式开发中具有重要的地位,而一般形式化方法不便于广大软件开发人员使用,因此开发基于 AADL 模型的形式化分析工具变得十分迫切。

Cheddar 是法国 Brest 大学开发的实时系统可调度分析工具,采用仿真的方式对 AADL 模型进行可调度分析,支持单处理器、多处理器、共享资源等多种调度情况。它已经作为 TOPCASED, STOOD 的插件使用^[13]。基于进程代数语言(ACSR)^[14]的工具 Furness 结构简单,能够仿真实时调度和资源竞争的关系,也经常作为 OSTATE 的一个插件来使用。和它类似, TIMES 也能够分析模型的调度性,是嵌入式调度性方面的一个重要工具。TASM 则基于时间状态机来验证系统在执行过程中的行为,它也是 AADL 模型可调度性的一种有效支持工具。Maude 是在重写逻辑概念基础上产生的工具,它用时序逻辑来表示 AADL 的调度过程,并在此基础上生成的工具。

目前基于 AADL 模型的研究已经越来越多,基于 AADL 模型的验证角度和验证工具也多种多样。对于基于模型驱动的实时系统开发来说,如何将这些验证理论与验证工具整合,并结合自动代码生成技术,使开发人员在这个平台上能够设计系统模型,仿真系统的实时调度,验证系统的可靠性,测试系统并最终生成基于系统模型的代码等整个开发流程是需要关注的重点。在基于 AADL 模型驱动的实时系统开发流程平台的理论研究方面,文献[15]以 AADL 为研究对象,提

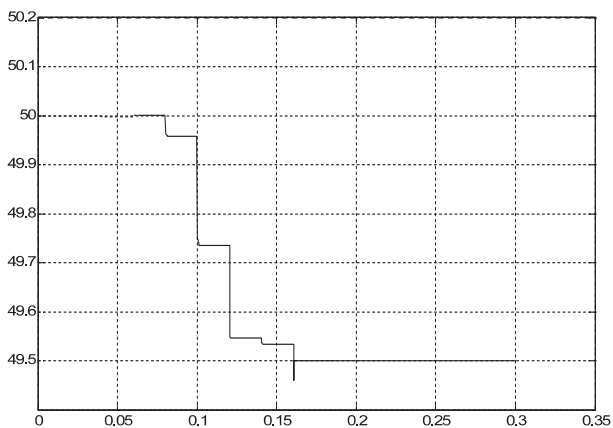
出了面向汽车电子的嵌入式软件开发平台。但是其研究主要集中于实现 AADL 系统模型和 simulink 功能模型的代码转换,搭建交叉编译环境,没有严格论证这个平台能够满足实时系统要求的非功能属性的正确性。文献[16]开发了嵌入式软件开发原型 LambdaMDE1.0。LambdaMDE 1.0 包含了建模、仿真验证、代码生成、测试等嵌入式软件开发的全过程。但是它还缺乏对错误模型的支持,对模型的验证能力还比较差,同时系统的执行效率和稳定性也不够完善。所以如何更好地结合形式化方法与理论建立可靠的嵌入式软件开发平台还需要进一步的探索。

5 结束语

AADL 是未来基于模型驱动的嵌入式系统开发领域的基石,它已经得到了业界众多组织的支持。目前 AADL 附件也在不断地扩展完善中,其形式化论证理论也继续进行,还没有建立标准的验证体系。基于驱动模型的形式化验证平台是基于模型驱动开发的基础。因此,还应该深入探讨 AADL 形式语义对于不同领域的影响和作用,完善它的形式化理论工具,整合整个开发平台,为 AADL 在基于模型驱动的嵌入式软件开发提供有效的支持。

参考文献:

- [1] 王金军. 模型驱动架构(MDA)开发模式研究及实践[D]. 上海:华东师范大学,2006.
- [2] SAE International. Architecture Analysis and Design References Language (AADL)[S]. AS5506,2004.
- [3] 董云伟,王广仁,张 凡,等. AADL 模型可靠性分析评估工具[J]. 软件学报,2011,22(6):1252-1266.
- [4] 高金梁,张 刚,经小川,等. 采用 AADL 的软件系统可靠性建模与评估方法[J]. 计算机科学与探索,2011(10):942-952.
- [5] 杨志义,张琛雨,董云卫. AADL 软件容错系统建模与评估[J]. 计算机测量与控制,2009,17(4):779-782.
- [6] 刘 倩,桂盛霖,李 允,等. 基于 UPPAAL 的 AADL 模型可调度性验证[J]. 计算机应用,2009,29(7):1820-1824.
- [7] 李振松,顾 斌. 基于 UPPAAL 的 AADL 行为模型验证方法研究[J]. 计算机科学,2012,39(2):159-169.
- [8] 刘 倩. AADL 模型可调度性分析工具设计与实现[D]. 成都:西南交通大学,2010.
- [9] Berthomieu B, Bodeveix Jean-Paul, Chaudet C, et al. Formal Verification of AADL Specification in the Topcased Environment[C]//Proc. of the 14th Ada-Europe International Conference on Reliable Software Technologies. Berlin: Springer-Verlag,2009.
- [10] 王 庚,周兴社,张 凡,等. AADL 模型的测试方法研究



(d) $c_f = 0.02 + 0.02\Delta f$, $C_{\text{norm}} = 1.0$, 盲区外检, 测成功

图 5 AFDPF 孤岛检测曲线

原理同 AFD, 利用算法参数自适应的方法, 改变 c_f 取值, 使检测失败转变为检测成功。

4 结束语

文中详细分析了移频孤岛检测方法的机理, 对不同负载类型检测失败的原因进行了归纳, 详细阐述了导致移频孤岛检测方法失败的负载相位角问题, 针对 AFD 以及 AFDPF 两种孤岛检测算法, 理清了参数, 盲区, 谐波之间的关系, 对参数设置提出了自适应原则, 使不同负载组合的检测盲区有效减小, 使电流畸变在遵循检测成功的基础上尽可能地降低。最后通过 Matlab/Simulink 仿真验证了上述理论的正确性。

参考文献:

- [1] 程启明, 王映斐, 程尹曼, 等. 分布式发电并网系统中孤岛检测方法的综述研究[J]. 电力系统保护与控制, 2011, 39(6): 147-154.
- [2] 张有兵, 穆森婕, 翁国庆. 分布式发电系统的孤岛检测方法

研究[J]. 电力系统保护与控制, 2011, 39(1): 139-146.

- [3] 吕兴德, 骆德汉, 姚长标, 等. 一种基于光伏系统的逆变电源设计[J]. 计算机技术与发展, 2012, 22(4): 179-182.
- [4] Singam B, Hui L Y. Assessing SMS and PJD Schemes of Anti-Islanding with Varying Quality Factor[C]//Proc. of First International Power and Energy Conference. Malaysia: [s. n.], 2006: 196-201.
- [5] 郭小强, 赵清林, 邬伟扬. 光伏并网发电系统孤岛检测技术[J]. 电工技术学报, 2007, 22(4): 157-162.
- [6] 程明, 张建忠, 赵俊杰. 分布式发电系统逆变器侧孤岛检测及非检测区描述[J]. 电力科学与技术学报, 2008, 23(4): 44-52.
- [7] 邓燕妮, 桂卫华. 一种低畸变的主动移频式孤岛检测算法[J]. 电工技术学报, 2009, 24(4): 219-223.
- [8] Hamzeh M, Mokhtari H. Power Quality Comparison of Active Islanding Detection Methods in a Single Phase PV Grid Connected Inverter[C]//Proc. of IEEE International Symposium on Industrial Electronics. Seoul Olympic Parktel, Seoul, Korea: [s. n.], 2009: 1852-1857.
- [9] 刘方锐, 余蜜, 张宇, 等. 主动移频法在光伏并网逆变器并联运行下的孤岛检测机理研究[J]. 中国电机工程学报, 2009, 29(12): 47-51.
- [10] 刘方锐, 康勇, 张宇, 等. 带正反馈的主动移频孤岛检测法的参数优化[J]. 电工电能新技术, 2008, 27(3): 22-25.
- [11] 肖巧景, 张宇翔, 郭敏. 一种新的频率偏移技术在光伏并网发电系统孤岛检测中的应用[J]. 现代电子技术, 2007(1): 107-108.
- [12] 刘芙蓉, 康勇, 段善旭, 等. 一种有效的孤岛检测盲区描述方法[J]. 电工技术学报, 2007, 22(10): 167-172.
- [13] 刘芙蓉, 康勇, 段善旭, 等. 主动移频式孤岛检测方法的参数优化[J]. 中国电机工程学报, 2008, 28(1): 95-99.
- [14] 刘芙蓉. 并网型户光伏系统的孤岛检测技术研究[D]. 武汉: 华中科技大学, 2008.

(上接第 45 页)

- [J]. 计算机科学, 2009, 36(11): 127-130.
- [11] 冯冰, 杨志义, 董云卫, 等. 一种面向 AADL 架构的模型测试方法[J]. 计算机测量与控制, 2010, 18(4): 778-781.
- [12] 马春燕, 董云卫, 朱宇峰, 等. AADL 测试模型的构造研究[J]. 西北工业大学学报, 2010, 28(6): 968-973.
- [13] 李建一. 基于模型驱动的嵌入式实时系统开发平台的研究与实现[D]. 成都: 电子科技大学, 2009.
- [14] Sokolsky O, Lee I, Clarke D. Process-Algebraic Interpretation of

AADL Model[C]//Proc. of Ada-Europ 2009. Berlin: Springer-Verlag, 2009.

- [15] 刘雪琴. 基于体系结构分析设计语言的实时系统模型开发平台应用研究[D]. 成都: 电子科技大学, 2009.
- [16] 陆少鹏, 桂盛霖, 李允, 等. 基于模型的嵌入式软件开发环境-LambdaMDE[J]. 计算机应用, 2010, 30(3): 607-611.

AADL模型的形式化研究

作者：[刘玮](#)，[李蜀瑜](#)，[LIU Wei](#)，[LI Shu-yu](#)
作者单位：[陕西师范大学 计算机学院, 陕西 西安, 710062](#)
刊名：[计算机技术与发展](#)

英文刊名：[Computer Technology and Development](#)

年，卷(期)：2013(9)

本文链接：http://d.wanfangdata.com.cn/Periodical_wjfz201309011.aspx