

基于 AADL 的嵌入式系统可靠性建模方法的探讨

杨 莉^{1,2}, 李 楠¹, 席 隆¹

(1. 中国科学院 空间应用工程与技术中心, 北京 100094;
2. 中国科学院大学 计算机与控制学院, 北京 100049)

摘 要:在航天嵌入式设备研制过程中,对于元器件与电路设计的可靠性评估手段已经比较成熟,但其视角有一定局限性,其评估结果无法直接反映任务要求的符合程度。AADL(Architecture Analysis & Design Language)可以为嵌入式系统的功能属性和非功能属性(如实时性和安全性)提供精确可执行的语义描述,提出利用 AADL 建立嵌入式系统可靠性模型的方法,可以有效解决这类问题。采用 AADL 核心语言建立系统级架构模型,为架构模型的建立与验证提供理论依据;采用 EMA(Error Model Annex)建立系统可靠性模型,给出故障类型、故障传播、故障行为及相关属性的描述方法。最后以数据采集存储系统为例,建立可靠性模型并进行可靠性分析,验证提出的嵌入式系统可靠性建模方法的有效性。

关键词:AADL;嵌入式系统;可靠性;系统级建模

中图分类号:TP311

文献标识码:A

文章编号:1673-629X(2015)08-0234-04

doi:10.3969/j.issn.1673-629X.2015.08.050

Discussion on Reliability Modeling for Embedded System Based on AADL

YANG Li^{1,2}, LI Nan¹, XI Long¹

(1. Technology and Engineering Center for Space Utilization, Chinese Academy of Sciences,
Beijing 100094, China;
2. College of Computer and Control Engineering, University of Chinese Academy of Sciences,
Beijing 100049, China)

Abstract:In aerospace embedded device development process, the method for reliability evaluation of components and circuit design is relatively mature, but its perspective has some limitations, its evaluation results cannot directly reflect the degree of compliance with the requirements. AADL (Architecture Analysis & Design Language) can provide accurate and executable semantic description for functional properties and non-functional properties such as real-time performance and security. A reliability modeling method of embedded system based on AADL is proposed in this paper, which can solve these problems effectively. The AADL core language is adopted to construct system-level architectural model and it provides theoretical basis for designing and validating the architectural model. EMA (Error Model Annex) is adopted to build the reliability of embedded system, then the usages of error type, error propagation, error behavior and related properties are provided. Finally, a data gathering and recording system is given as an example to illustrate the efficiency of the modeling method.

Key words:AADL; embedded system; reliability; system-level modeling

0 引 言

AADL(Architecture Analysis & Design Language)是由 SAE(Society of Automotive Engineers)于 2004 年提出,发布为 SAE AS5506 标准,可以为嵌入式软件系统及其目标平台提供可执行的语义描述^[1]。通过

AADL 对嵌入式系统进行建模,可以在开发阶段验证系统的体系结构和实现,进而实现系统的改进;有助于在嵌入式系统开发前期对系统的可靠性进行评估,以有效降低开发维护成本。

EMA(Error Model Annex)是一种添加组件安全

收稿日期:2014-09-22

修回日期:2014-12-25

网络出版时间:2015-07-21

基金项目:中国科学院空间科学与应用项目(Y2020400QY)

作者简介:杨 莉(1991-),女,硕士研究生,研究方向为空间电子工程;李 楠,助理研究员,研究方向为空间综合电子学;席 隆,正高级工程师,研究方向为空间综合电子学。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20150721.1439.040.html>

信息的标准 AADL 扩展语言,允许用户指定故障行为状态机^[2]。EMA 第 1 版由 SAE 于 2006 年发布为 AS5506/1 标准,定义了故障模型的声明规则及语义,利用 EMV1 建立故障模型的方法已较为成熟^[3-5]。EMA 第 2 版于 2013 年提出,相较于 EMV1 做出了一些改变,故障模型不再由类型(error model type)和实现(error model implementation)组合声明,而是由故障类型、故障传播、故障行为的方式分开说明,并且为故障模型元素添加了属性信息^[6]。文中给出了利用 EMV2 建立故障模型的方法。

文中的研究内容为利用 AADL 进行嵌入式系统模型驱动开发,结合 EMV2 建立可靠性模型,并以数据采集存储系统为应用背景验证可靠性模型建立方法的有效性,对嵌入式系统的开发、验证及分析具有重要意义。

1 基于 AADL 的可靠性建模

EMA 对组件的各种可靠性信息,包括故障行为、故障传播等,进行描述,建立故障模型。将故障模型与 AADL 架构模型相结合,可以构成完整的嵌入式系统可靠性模型。该可靠性建模框架实现了故障模型和架构模型的分离,提高了可靠性模型的重用性。故障模型与架构模型的绑定使两者成为一个有机的整体,更易于理解系统的可靠性行为。图 1 为可靠性模型建立框架。

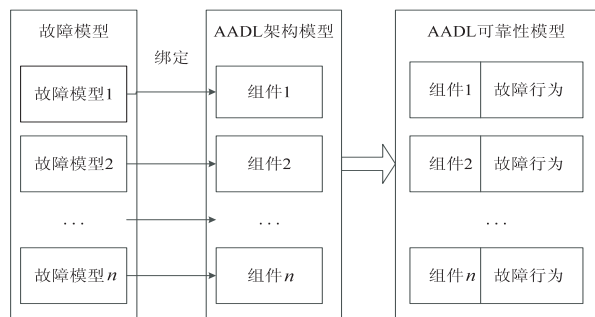


图 1 可靠性模型建立框架

1.1 AADL 架构模型

基于 AADL 的嵌入式系统架构模型的建立是将嵌入式系统的应用软件、计算机执行平台、物理系统映射为 AADL 的应用软件组件、执行平台组件及综合组件的架构级建模以及将嵌入式系统的信息交互、实时调度、中断处理、系统服务映射为 AADL 组件间的交互的行为级建模的过程。

1.1.1 架构级建模

架构级建模是为整个系统的体系结构建立框架,分为硬件架构设计和软件架构设计^[7-8]。硬件架构设计是利用 AADL 的执行平台组件(处理器、存储器、设备和总线)为嵌入式系统的硬件结构进行建模。软件

架构设计是利用 AADL 的应用软件组件(线程、线程组、进程、数据和子程序)为嵌入式系统的任务和中断服务程序进行建模。

1.1.2 行为级建模

在架构级模型的基础之上,针对系统的实时调度、中断处理、资源管理等进行行为级建模^[9]。行为级建模分为交互行为建模和执行行为建模两类。交互行为指任务之间的信息交互。执行行为指任务的实时调度、中断处理、资源管理和系统服务。图 2 说明了利用 AADL 建立行为级模型的方法。

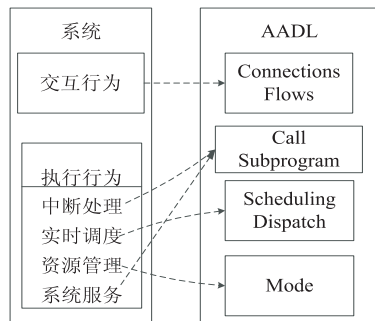


图 2 行为级模型建立框架

1.1.3 模型验证

AADL 拥有丰富的验证工具集^[10-12],可以在系统开发前期进行架构验证和行为验证。架构验证指对系统的结构模型进行形式化验证,如组件类型和数量的统计、检查端口连接的一致性、分析绑定总线负载、分析资源分配和预算等。行为验证主要是通过端到端的流延迟分析判断系统交互行为的正确性,通过实时调度分析验证系统执行行为的正确性。

1.2 故障模型附件

故障模型附件是 AADL 扩充语言的一种,主要用于支持可靠性模型建立^[13]。与 AADL 核心语言类似,故障模型附件为故障模型的建立提供了丰富的建模元素,包括故障类型、故障传播、故障行为、属性等。利用这些建模元素,可以对组件、连接的故障事件、故障概率、故障传播等进行建模,与结构模型绑定形成可靠性模型,方便进行可靠性分析。

1.2.1 故障类型

故障类型(Error Type)使用户以一个统一的方式说明故障状态、故障事件、故障传播的特征。故障类型主要分为:

- ServiceError—服务类型的故障,例如遗漏错误(ItemOmission);
- TimingRelatedError—时间相关的故障,例如延迟(LateDelivery);
- ValueRelatedError—值相关的故障,例如超过边界值(OutofRange);
- ReplicationError—重复故障,主要发生在冗余系

统中不对称时间、遗漏故障时;

• **ConcurrencyError**—并发性故障, 主要发生在访问共享逻辑或物理资源时。

另外, 用户也可自定义需要的故障类型。

故障类型声明时, 在故障状态、故障事件、故障传播后 `}}` 中表明故障是属于哪种类型, 例如“`AD_ef2; error source AD {ServiceOmission};`”说明故障类型为 `ServiceOmission`。

1.2.2 故障传播

故障传播 (Error Propagation) 研究的内容是不同组件在故障状态下是如何影响其他组件的。故障传播分为传出 (outgoing) 故障和传入 (incoming) 故障。所谓传出故障是指某组件传播出去的故障类型, 传出故障具有随机参数即故障传播概率; 传入故障是指不会被传播但某组件会接收的故障类型。

在故障模型中, 需要定义可以产生传出故障传播的故障状态, 当源组件处于这种故障状态时, 就可能触发传出故障。当产生传出故障时, 该事件就会影响一个或多个目标组件, 使目标组件转移至故障状态。其中, 目标组件的识别通过名字匹配实现, 同名的传出、传入故障传播表示了故障传播的起点和终点。其中, `error flows` 中会指出故障传播起点 (error source)、终点 (error sink) 和路径 (error path)。故障传播声明举例如下:

```
error propagations
ADdata; in propagation {ValueError};
ADreset; out propagation {ServiceOmission};
flows
AD_ef1; error sink ADdata {ValueError};
AD_ef2; error source ADreset {ServiceOmission};
end propagations;
```

1.2.3 故障行为

故障行为 (Error Behavior) 主要定义了故障事件、故障状态以及事件是如何影响故障状态的。分为组件故障行为和综合故障行为。

组件故障行为: 对于每一个组件, 定义故障事件、它们发生的概率, 以及它们和传入故障一起是如何影响故障状态的, 传出故障在什么条件下会发生, 故障行为什么时候被组件发现和处理。图 3 为组件故障行为声明举例。

综合故障行为: 对于有子组件的组件而言, 说明子组件的故障状态和组件的故障状态的映射关系, 这种关系反映了故障树逻辑, 可以在结构的不同层次进行故障分析。

1.2.4 属性

定义与故障分析有关的一些属性, 例如发生的概率、分布 (OccurenceDistribution), 严重性级别 (Severi-

ty), 可能性 (Likelihood), 危害性 (Hazards) 等^[14]。

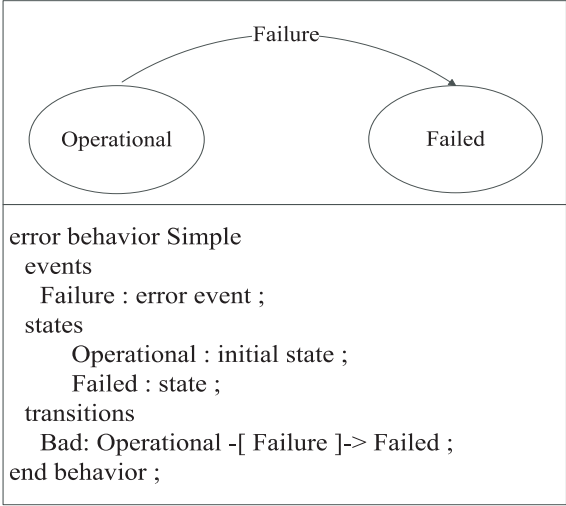


图 3 组件故障行为声明举例

2 实例

以数据采集存储系统 (Data Gathering and Recording System) 为例, 对可靠性模型建立方法进行说明。

数据采集存储系统由 ADS1258、上位机 PC、Nand-Flash、看门狗和 CPU (TMS570) 组成, 如图 4 所示。CPU 接收 ADS1258 传来的数据, 并在 NandFlash 中存储, 上位机 PC 用于串口通信, 看门狗用于复位。

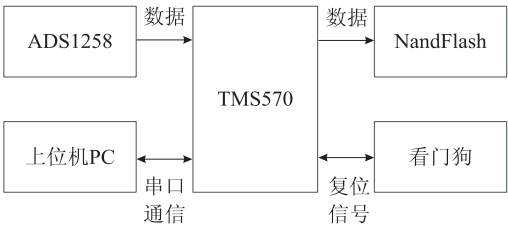


图 4 数据采集存储系统组成框图

首先利用 AADL 建立系统的架构模型, 如图 5 所示。然后给系统的 AADL 结构模型中的每个组件增加相应的故障模型, 下述为设备 ADS1258 的故障模型, 其他组件的故障模型在此省略。

```
device ADS1258
features
ADdata; out data port dummy1;
annex EMV2 { * *
use types ErrorLibrary;
use behavior DGRSys_errordlib.:Simple;②
error propagations
ADdata; out propagation {ServiceOmission, ValueError, LateDelivery};①
flows
AD_ef_0; error source ADdata {ServiceOmission} when Failed;
AD_ef_1; error source ADdata {ValueError} when Failed;
AD_ef_2; error source ADdata {LateDelivery} when Failed;③
end propagations;
```

```

properties
EMV2::severity => 1 applies to Failure;
EMV2::likelihood => C applies to Failure;
EMV2::hazards =>
( [ crossreference => "1.1.1";
failure=> "No output data";
phases=> ("all");
description=> "No data out due to ADS1258 failure";
comment => " Becomes major hazard, if no redundant
ADS1258";])applies to Failure;④
* * };
end ADS1258;

```

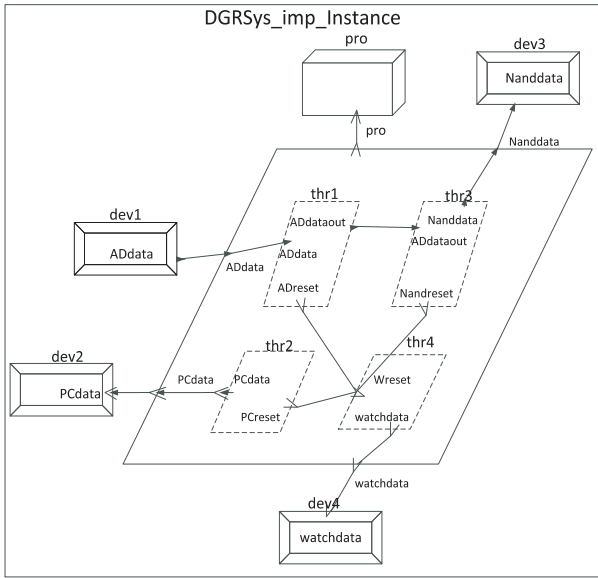


图5 数据采集存储系统AADL架构

①部分为故障类型说明,ADS1258的故障类型有:ServiceOmission—ADS1258无服务即无数据传给CPU;ValueError—传出的数据是错误的;LateDelivery—传出时间延迟。

②部分为故障行为说明,ADS1258的故障行为如图3所示,有Operational和Failed两个状态。

③部分为故障传播,当ADS1258处于Failed状态时,会产生与三种故障类型相对应的故障传播,并且ADS1258为故障起点。

④部分为关于严重性级别、可能性、危害性的属性说明。

至此,基于AADL的数据采集存储系统的可靠性模型建立完成,可进行可靠性相关的分析,如FHA(Fault Hazard Analysis)、RBD(Reliability Block Diagram)、FTA(Fault Tree Analysis)、Fault Impact等。

3 结束语

文中利用AADL语言建立嵌入式系统架构模型,给出了系统架构级和行为级建模以及可靠性建模的策略。这种基于组件的模型架构方法体现了设计的灵活

性和验证的有效性。

在架构模型的基础上,利用EMV2建立嵌入式系统可靠性模型,描述故障传播、故障行为等对系统的影响。在开发前期对系统进行可靠性分析,为系统的改进及设备在轨工作健康管理策略设计提供理论依据。

基于AADL的嵌入式系统可靠性建模方法可以应用于航空航天电子设备、空间应用、控制工程、应用软件工程、电子工程等领域。

参考文献:

- [1] Society of automotive engineers,SAE-AS5506,architecture analysis and design language [EB/OL]. 2004. <http://standards.sae.org/as5506a/>.
- [2] Society of automotive engineers,SAE-AS5506/1,Architecture Analysis and Design Language (AADL) annex volume 1; annex e; error model annex [EB/OL]. 2006. <http://standards.sae.org/as5506/1/>.
- [3] 杨志斌,皮磊,胡凯,等.复杂嵌入式实时系统体系结构设计与分析语言:AADL[J].软件学报,2010,21(5):899-915.
- [4] 董云卫,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.
- [5] Zhang Q,Wang S,Liu B. Some improvements on the rules for exchanging between error model annex and AADL to fault tree [C]//Proc of international conference on information technology and applications. Washington,DC:IEEE,2013:338-342.
- [6] Larson B,Hatchiff J,Fowler K,et al. Illustrating the AADL error modeling annex (v.2) using a simple safety-critical medical device [C]//Proceedings of the 2013 ACM SIGAda annual conference on high integrity language technology. [s.l.]: ACM,2013:65-84.
- [7] 汤小明,苏罗辉,宋科璞.飞行管理系统AADL建模与分析[J].计算机技术与发展,2010,20(3):191-194.
- [8] 刘玮,李蜀瑜.AADL模型的形式化研究[J].计算机技术与发展,2013,23(9):43-45.
- [9] 刘博,李蜀瑜.基于NuSMV的AADL行为模型验证的探究[J].计算机技术与发展,2012,22(2):110-113.
- [10] 宋翠叶,杜承烈,李刚.基于AADL的软件开发技术研究[J].计算机应用研究,2009,26(9):3361-3364.
- [11] 刘雪琴,桂盛霖,罗蕾,等.AADL模型代码自动生成技术研究[J].计算机应用研究,2008,25(12):3631-3635.
- [12] Feiler P. Open Source AADL Tool Environment (OSATE) [C]//Proc of AADL workshop. Paris:[s.n.],2004.
- [13] Feiler P H,Gluch D P. Model-based engineering with AADL: an introduction to the SAE architecture analysis & design language [M]. [s.l.]: Addison-Wesley,2012:185-207.
- [14] Feiler P H,Greenhouse A. Osate plug-in development guide [EB/OL]. 2006. <http://www.aadl.info/aadlinfosite/downloads/Plug-in%20Guide%202005-06-16%201030.pdf>.

基于AADL的嵌入式系统可靠性建模方法的探讨


作者:

杨莉, 李楠, 席隆, [YANG Li](#), [LI Nan](#), [XI Long](#)

作者单位:

[杨莉, YANG Li \(中国科学院 空间应用工程与技术中心, 北京 100094; 中国科学院大学 计算机与控制学院, 北京 100049\), 李楠, 席隆, LI Nan, XI Long \(中国科学院 空间应用工程与技术中心, 北京, 100094\)](#)

刊名:

[计算机技术的发展](#)

英文刊名:

[Computer Technology and Development](#)

年, 卷(期):

2015(8)

引用本文格式: [杨莉. 李楠. 席隆. YANG Li. LI Nan. XI Long 基于AADL的嵌入式系统可靠性建模方法的探讨](#)[期刊论文]-[计算机技术的发展](#) 2015(8)