

一种基于AADL错误模型的软件安全性 分析技术研究

成静^{1,2}, 朱怡安¹, 屈华敏², 罗文波², 江叶春², 张涛²

(1.西北工业大学 计算机学院, 陕西 西安 710072; 2.西北工业大学 软件与微电子学院, 陕西 西安 710075)

摘要: 针对软件安全性问题, 提出一种新的软件安全性分析方法。首先探索将软件组件AADL错误模型转化为马尔科夫链模型, 计算组件处于不同危害级别状态概率, 分析组件安全性。并且进一步, 根据AADL错误模型组合实现定义, 由其内部组件安全状态概率计算分析软件系统的安全性, 避免状态爆炸问题。最后, 以飞控系统软件为例, 对算法进行实例验证。

关键词: AADL模型, 错误模型, 软件安全性, 马尔科夫链

中图分类号: TP311

文献标志码: A

文章编号: 1000-2758(2014)06-1007-04

随着软件在航空、航天、医疗等领域的广泛应用, 软件安全性问题也日益突出和严峻。目前, 软件安全性技术研究主要借鉴于故障树(FAT)、故障影响范围分析(FEMA)等传统系统安全性技术。但由于软件结构特点, 及其安全性影响因素的不同, 使得这些方法均不能完全满足软件安全性需求, 需要研究新的软件安全性技术^[1]。本文研究扩展AADL(architecture analysis and design language)模型, 使其适合多层次建模软件安全性, 为安全性分析奠定基础。

1 AADL 错误附件

AADL是一种设计和分析软硬件结构的嵌入式实时系统建模语言。AADL具有良好的可扩展性, 不仅能够建模软件系统结构、行为语义, 还支持描述系统非功能属性和故障模型, 使其在安全关键嵌入式系统有着良好的应用前景^[2]。

错误附件是AADL模型的一种标准扩展, 主要用于建模和描述系统及组件的安全性。错误附件采用行为状态机描述可能由内部错误事件或者外部错误传播触发的系统随机故障。AADL错误附件的主

要特点包括:

1) 层次化的错误类型定义。可自定义错误类型, 并且可定义已有错误类型的子类型, 形成层次化的错误本体库。不同分支的错误类型相互独立, 可能同时发生。

2) 组件之间的错误传播机制。可指定允许组件输入和输出的错误类型, 并基于错误流描述错误在多个组件之间传播路径, 以及建模平台资源故障对组件影响。

3) 组件内部行为错误描述。可指定组件的工作状态、错误事件、修复事件、组件故障、发生概率、危害级别、故障传播影响以及故障如何检测与处理等。

4) 组件错误行为组合机制。可描述组件错误是如何由其内部组件错误引发, 即将组件错误状态映射为其内部组件错误状态集, 支持不同级别的软件体系结构故障分析。

2 基于 Markov 链的安全性评估方法

2.1 AADL 错误附件到 Markov 模型映射

AADL模型是一种半形式化方法, 为了准确分

收稿日期: 2014-04-28

基金项目: 国家自然科学基金(61103003)与航天科技支撑计划(2014HTXGD)、西北工业大学基础研究基金(2012JC2016)与航空科学基金(20120718005)资助

作者简介: 成静(1982—), 女, 西北工业大学博士研究生, 主要从事软件测试、软件安全性研究。

析软件安全性 需要将 AADL 模型转换为 Markov 链等形式化模型,进行自动分析计算^[3]。本文则将 AADL 模型错误附件转换为 Markov 链模型,分析和评估软件组件及系统安全性。Markov 链模型描述系统状态迁移及其概率,而 AADL 错误模型同样描述系统/组件的故障状态及其迁移概率。为了方便安全性分析,本文提出一种扩展的 Markov 链模型。

定义 1 一个扩展马尔科夫链模型定义为: $MK = (S, \sum, P, Q)$ 其中

1) S 表示系统所有状态集合,是一个有限的随机状态集合。 S_i 表示 S 中的第 i 个元素 ($1 \leq i \leq n$)。 S_i 是二元组 $S_i = \{State, Level\}$ 。State 是状态名; Level 是该状态危害级别,分为 5 级: 正常 (Normal)、轻微 (Light)、较重 (Heavy)、严重 (Serious)、灾难 (Crash)。

2) \sum 表示引发系统错误状态迁移的事件集合。 \sum_i 表示 \sum 中的第 i 个元素 ($1 \leq i \leq n$)。其中, $\sum_i = \{TriggerName, TriggerType\}$, TriggerType 是事件类型,包括故障事件和故障传播; TriggerName 是事件名称。

3) P 是错误状态迁移的概率集合。 P_i 表示 P 集合中的第 i 个元素 ($1 \leq i \leq n$)。

4) Q 表示状态之间的迁移关系: $S \times \sum \rightarrow S$ 。

这里,表 1 给出 AADL 错误附件与扩展 Markov 链模型元素之间映射关系定义。

表 1 AADL 错误附件与 Markov 链模型元素映射关系

Markov 链模型	AADL 安全附件
S	error_state
TriggerType	Error /propagation
Probability	Occurrence
Q	transitions

2.2 基于 Markov 链模型的组件安全性分析

设组件由 n 个错误状态,则其 Markov 链模型可表示为一个 $n \times n$ 的转移矩阵 P 。其中 P_{ij} 表示组件从当前状态 S_i 迁移到下一个状态 S_j 的转移概率,满足 $0 \leq P_{ij} \leq 1$ 。如果 $P_{ij} = 1$,则表示以 S_i 为起始状态的状态迁移只有一个;而 $P_{ij} = 0$ 表示不存在从当前状态 S_i 到下一个状态 S_j 的迁移。并且,同一起始状态的转移概率之和等于 1,即 P 中每一行的转移概

率之和等于 1。

由 AADL 错误附件转换的 Markov 链模型,其状态迁移概率 P_{ij} 是不变的,因此是齐次 Markov 链。依据齐次 Markov 链的遍历性,经过有限的 n 步状态迁移后,其各个状态概率会达到其稳态概率。因此,经过长期运行后,可以根据(1)式和(2)式计算软件组件在各个错误状态的稳态概率。这里 π 表示组件处于状态集 S 中各个状态的概率, π_i 表示组件处于状态 i 的概率 P 表示转移矩阵。

$$\pi = \pi * P \tag{1}$$

$$\pi_i = \sum_{j=1}^{j=n} \pi_j P_{ji} \tag{2}$$

软件安全性分析,主要分析组件处于不同危害级别状态的概率。因此,将相同危害级别状态概率相加,即可分别计算组件处于灾难、严重等级别的可能概率,如(3)式 P_L 表示组件在危害级别状态 L 的概率。

$$P_L = \sum_{i \text{ level} = L} \pi_j \tag{3}$$

2.3 软件系统安全性分析

AADL 错误附件能够描述其故障行为组合,即将系统状态定义为其内部组件状态的组合。因此,系统安全性分析也可基于其内部组件安全性分析计算。在 AADL 错误附件中,其组件状态组合逻辑操作包括: or, and, ormore, orless,其含义分别为: or 表示只要其中任意一个内部组件状态符合; and 表示所有内部组件状态全部符合; n ormore 表示至少 n 个内部组件状态符合; n orless 表示至多 n 个内部组件状态符合。

因此,可根据各个组件状态概率,按照其逻辑组合关系,计算系统在各个状态概率。然后将相同危害级别状态概率相加,即可分别计算系统处于不同危害级别状态的概率。例如,假设系统状态 $S1$ 定义为: $S1 \text{ when } 1\text{ormore}(\text{sub1.f1}, \text{sub2.f2}, \text{sub3.f3})$, 则其概率为: $p_{s1} = 1 - p_{\text{sub1.f1}} * p_{\text{sub2.f2}} * p_{\text{sub3.f3}}$ 。

通过状态组合,能够直接计算系统状态概率。而避免由于将系统内部各个组件状态直接映射为系统状态,所导致的系统状态爆炸问题,从而提高安全性分析计算效率。

3 实例分析

飞行控制软件具有很高安全性,其故障将直接

影响飞机飞行安全。下面以图 1 所示的某无人机飞行控制系统软件为例,建立其 AADL 模型和错误模型,分析其软件安全性。该系统包括:姿态控制子系统 Pose_Ctl_System、导航制导分系统 Nav_Ctl_System 和遥控遥测分系统 Tele_Ctl_System。图 2 给出其中姿态角速度信号组件 T_Ang_Reader 的错误模型示例。

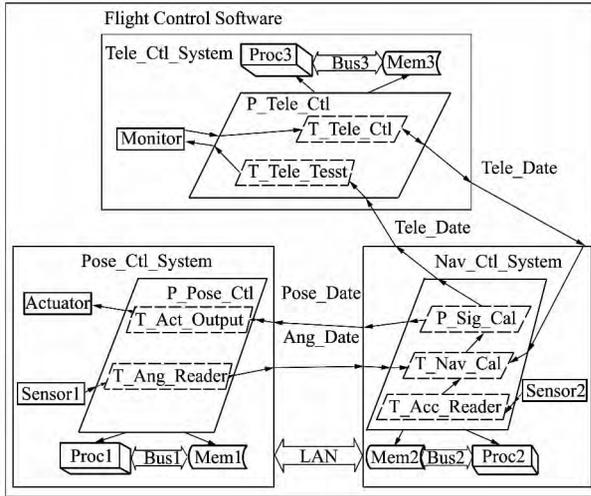


图 1 无人机飞行控制系统软件 AADL 模型

根据 (1) 式和转移矩阵编写程序计算 T_Ang_Reader 的状态概率为: $\pi = \{ 0.999\ 938, 1.249\ 92 \times 10^{-5}, 8.928\ 02 \times 10^{-6}, 4.075\ 83 \times 10^{-5} \}$ 。其中,只是 Failed 状态危害级别为灾难级,即可能因该软件组件故障导致灾难概率为: $4.075\ 83 \times 10^{-5}$ 。

可分别计算各个组件的状态概率,然后根据其错误状态组合实现关系,计算整个飞行控制系统软件分别处于正常、轻微、较重、严重、灾难等各个危害级别状态概率。

参考文献:

[1] Bhansali P V. Software Safety: Current Status and Future Direction[J]. ACM Sigsoft Software Engineering Notes, 2005, 30(1): 1-3
 [2] Dong YunWei, Wang GuangRen, Zhang Fan, Gao Lei. Reliability Analysis and Assessment Tool for AADL Model[J]. Journal of Software, 2011, 22(6): 1252-1266
 [3] Liu Xinning, Qian Hongbing. Software Dependability Metrics and Analysis Based on AADL Error Model[C]//Lecture Notes in Computer Science, 2011: 236-244

Error Model Type [T_Sensor_Reader]

Error model T_Sensor_Reader	// 错误模型类型
Features	// 错误模糊特征
Error_Free: initial error state;	// 初始状态
Erroneous: error state;	// 故障状态
Fault: error state;	// 故障状态
Failed: error state;	// 故障状态
Error: error event{ Occurrence =>Poisson λ_1 };	// 故障事件
Detect: error event{ Occurrence =>Poisson λ_2 };	// 故障事件
NonDetect: error event{ Occurrence =>Poisson $1-\lambda_2$ };	// 故障事件
Recovery: error event{ Occurrence =>Poisson λ_3 };	// 故障事件
Restart: error event{ Occurrence =>Poisson λ_4 };	// 故障事件
End T_Sensor_Error_Model Implementation [T_Sensor_Reader.imp]	
Error model implementation T_Sensor_Reader.imp	// 错误模型实现
Transitions	// 状态转移声明
Error_Free - [Error] -> Erroneous;	
Erroneous - [Detect] -> Fault;	
Erroneous - [NonDetect] -> Failed;	
Fault - [Recovery] -> Error_Free;	
Failed - [Restart] -> Error_Free;	
End T_Sensor_Reader.imp;	

图 2 姿态角速度信号组件 T_Ang_Reader 的错误模型

4 结 论

本文研究基于 AADL 模型的软件安全性分析技术,通过将 AADL 错误模型转化为 Markov 链,计算组件在各个危害级别状态概率,定量分析组件安全性。并且,通过组件故障状态组合实现,计算分析系统安全性。下一步,将研究开发软件安全性自动化分析工具,并针对大型系统,进一步开展实例验证研究。

Analyzing Software Safety with AADL Error Model

Cheng Jing^{1,2}, Zhu Yi'an¹, Qu Huamin², Luo Wenbo², Jiang Yechun², Zhao Tao²

(1. Department of Computer Science and Engineering, Northwestern Polytechnical University, Xi'an 710072, China)
(2. Department of Software Engineering, Northwestern Polytechnical University, Xi'an 710072, China)

Abstract: We propose a new model-based software safety analysis method, which can analyze software safety early in the software design phase. Firstly we define the rules for transforming the AADL error model into expanded Markov chain; the probabilities of different level component's safety states can be calculated with Markov model. AADL can define software system error behavior model in terms of the subcomponent error models, then safety of software system can be got directly in terms of subcomponent safeties. Finally an example is given to explain the use of the measurement method.

Key words: angular velocity, computer software, conformal mapping, design, errors, flight control system, Markov processes, mathematical models, matrix algebra, probability, unmanned aerial vehicles (UAV); AADL(Architecture Design and Design Language), error model, Markov model, safety