



基于AADL的IoP系统可靠性评估方法

施小东¹, 勉治宝², 高亚晴¹

(1.北方民族大学 计算机科学与工程学院, 银川 750021; 2.西北师范大学 计算机科学与工程学院, 兰州 730070)

摘要: 人联网(IoP)系统的架构复杂且存在海量、实时变化的数据,使得基于IoP系统的可靠性分析变得十分困难,目前仍缺乏一种健全的基于IoP系统的可靠性建模及评估方法。提出一种新型的IoP系统可靠性评估方法,利用AADL及其附件语言对IoP系统进行可靠性建模,并基于该模型从定性角度评估系统故障的根本原因和风险。此外,结合Ocarina模型转换技术提出一种基于连续时间马尔科夫链(CTMC)的定量评估算法,将AADL可靠性模型转换为CTMC模型,实现对系统动态、实时等特性的评估。在此基础上,设计一个IoP系统通用模型,并以此为案例验证所提方法的可行性。实验结果表明,该方法不仅能对IoP系统建模,而且能自动、准确地对其进行可靠性分析,具有良好的应用价值。

关键词: 人联网;架构分析与设计语言;可靠性建模及分析;连续时间马尔科夫链;Ocarina模型转换

开放科学(资源服务)标志码(OSID):



中文引用格式:施小东,勉治宝,高亚晴.基于AADL的IoP系统可靠性评估方法[J].计算机工程,2022,48(1):204-213.

英文引用格式:SHI X D, MIAN Z B, GAO Y Q. IoP system dependability evaluation method based on AADL[J]. Computer Engineering, 2022, 48(1): 204-213.

IoP System Dependability Evaluation Method Based on AADL

SHI Xiaodong¹, MIAN Zhibao², GAO Yaqing¹

(1.College of Computer Science and Engineering, North Minzu University, Yinchuan 750021, China;
2.College of Computer Science and Engineering, Northwest Normal University, Lanzhou 730070, China)

[Abstract] The Internet of People (IoP) is characterized by the complex architecture and massive changing data, which adds to the difficulty of the analysis on IoP-based system dependability. Currently, there is still no robust dependability modelling and analysis method for IoP systems. This paper proposes an Architecture Analysis and Design Language (AADL)-based dependability evaluation method for IoP systems. By using AADL and its annex language, the dependability of IoP systems is modeled to support the qualitative analysis on the causes of system failures and risks. Furthermore, by combining the Ocarina model transformation technology, a quantitative evaluation algorithm based on the Continuous-Time Markov Chain (CTMC) is proposed. The algorithm transforms the AADL dependability model to the CTMC model, so that the dynamic and real-time attributes of IoP systems can be evaluated quantitatively. On this basis, a general IoP system model is designed to demonstrate the feasibility of the proposed method. The experimental results show that the proposed method can be used to model the IoP systems, and perform dependability analysis automatically and accurately, displaying a high application value.

[Key words] Internet of People (IoP); Architecture Analysis and Design Language (AADL); dependability modelling and analysis; Continuous-Time Markov Chain (CTMC); Ocarina model transformation

DOI: 10.19678/j.issn.1000-3428.0059738

0 概述

随着可穿戴设备技术的发展,人的个体属性和社会属性都能向网络世界映射,以人为中心的集多种交互功能于一体的网络逐步形成,这种新兴互联网模式被称为人联网(Internet of People, IoP)^[1]。IoP系统可以提供医疗诊断、辅助残疾人等个性化服

务,但一旦系统发生故障,将对用户造成生命威胁。因此,基于IoP系统的可靠性分析变得至关重要。

IoP系统由多层软硬件构成,具有实时、动态的复杂特性。此外,随着大数据^[2]、人工智能^[3]、云平台^[4]等技术的推动,IoP系统的功能更加丰富多样。这些因素导致基于IoP系统的可靠性分析变得十分困难,系统故障的根本原因难以确定。因此,需要一种自动化的可

基金项目: 甘肃省教育厅青年博士基金(2021QB-022);甘肃省教育厅产业支撑计划项目(2021CYZC-06);西北师范大学2020年青年教师科研能力提升计划项目(NWNU-LKQN2020-15);宁夏重点研究与发展计划项目(2018BEE03019);宁夏自然科学基金(2019AAC03120);北方民族大学研究生创新项目(YCX20067)。

作者简介: 施小东(1995—),男,硕士研究生,主研方向为复杂系统的可靠性分析;勉治宝,副教授、博士;高亚晴,硕士研究生。

收稿日期: 2020-10-16 **修回日期:** 2021-01-03 **E-mail:** sxd73422@163.com

可靠性分析,以便在系统开发生命周期的各个阶段能反复验证系统可靠性能。但是,目前该领域缺乏一种自动、准确、可靠和可重用的分析方案。

基于模型的可靠性分析方法(MBDA)^[5]能为复杂系统提供自动且可重用的可靠性评估,已广泛应用于航空航天系统、信息物理系统、医疗系统等不同领域中,所以MBDA方法能为IoP系统提供一种自动的可靠性评估方案。

为了实现MBDA方法,本文对可靠性领域内的一些建模语言,如统一建模语言(UML)^[6]、系统建模语言(SysML)^[7]、架构分析与设计语言(AADL)^[8]、电子架构与软件技术-架构描述语言(EAST-ADL)^[9]等,从能否满足IoP系统可靠性建模和评估需求,以及能否提供高效的可靠性分析环境两方面进行了对比。在系统架构建模方面,IoP系统包含了复杂的软硬件架构和硬件绑定机制,AADL具有丰富的构件类型和实现,可详细地建模软硬件组件的功能、架构以及绑定机制。另外,IoP系统具有实时、动态的特性,AADL的MODE能建模系统的动态模式,并能通过与AADL的行为附件(BA)相结合来细化模式转变逻辑。在故障建模方面,AADL的错误模型附件(EMA)能详细建模系统故障信息,这为分析IoP系统的故障行为和传播提供了基础。此外,AADL的开源开发环境OSATE^[10]支持多种可靠性分析,例如故障模式及影响分析(FMEA)^[11]、故障树分析(FTA)^[12]、功能危险性评估(FHA)^[13]等,这为IoP系统提供了高效的评估环境,故AADL能为IoP系统提供可靠性建模及评估。

目前,AADL提供的FTA、FHA等分析方法虽然能详细地评估IoP系统故障的根本原因和危害,但是无法对IoP系统的动态、实时等特性进行定量分析。因此,本文提出一种基于AADL的IoP系统可

靠性评估方法,并设计一个IoP系统通用模型。利用AADL及其附件语言对IoP系统进行可靠性建模,并从定性和定量两方面进行分析。采用FTA和FHA方法定性评估系统故障的根本原因和危险,通过在OSATE中采用Ocarina^[14]模型转换技术将系统的AADL可靠性模型转换为连续时间马尔科夫链(CTMC)模型,进一步提出基于CTMC的定量评估算法,以对IoP系统的动态和实时特性进行评估。

1 相关工作

1.1 IoP系统架构及其特性

目前国内外关于IoP系统架构的研究较少,缺乏具体的IoP系统模型。文献[1]提出一种基于IoP的数据管理范式,并对其特性进行了讨论。文献[2,4,15]提出的一些概念模型涉及到老人智能家居、大数据、云平台等方面。通过结合IoP特性以及对上述系统模型的总结抽象,本文提出一个通用的IoP系统模型。如图1所示,该模型主要分为4个系统模块:可穿戴感知系统(W系统),边缘智能系统(E系统),网络系统(N系统)和云平台系统(C系统)。其中,W系统以近端通信方式感知用户信息并传递给E系统。近端通信方式有多种,其中蓝牙的安全保密性较高且适用于传感设备通信。E系统是用户的智能代理,用户通过它参与到智能决策中。E系统首先接收W系统传递的用户信息(蓝牙信号)并进行处理,然后通过N系统构建的自组网和主干网2种连接策略,与社区内及远程设备平台进行交互,并为用户提供智能行程规划和健康管理等服务。N系统负责网络管理,并能自动地调整以连接不同类型网络。C系统是服务器集群,通过N系统与E系统交互,为用户提供大数据、人工智能推荐等计算服务。

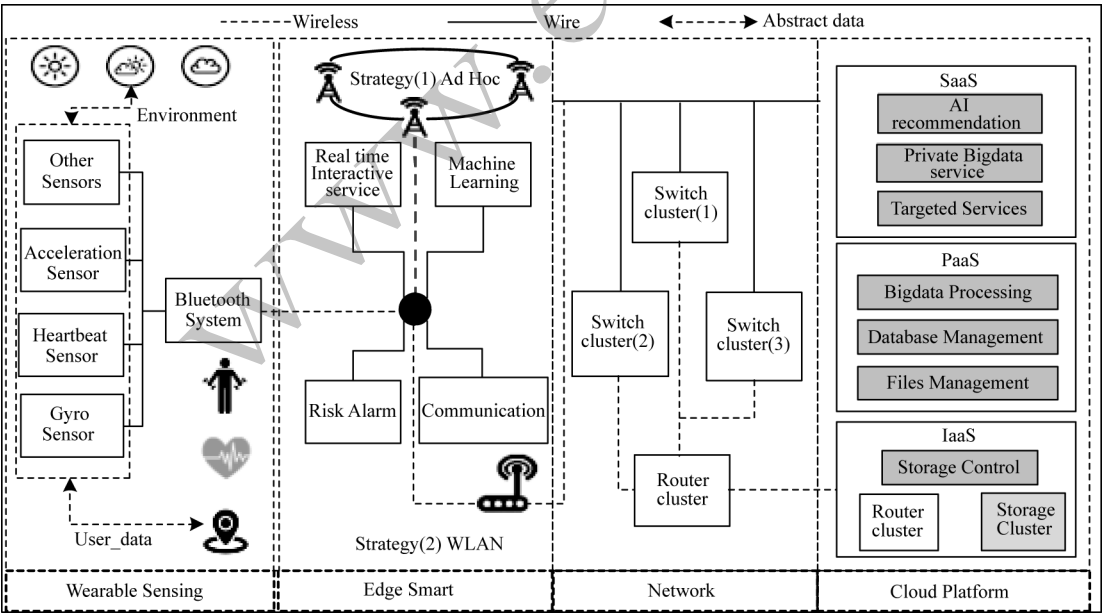


图1 IoP系统模型架构

Fig.1 Architecture for the IoP system model

由图1中的IoP系统架构模型可知,IoP系统不同于物联网系统^[16],它以设备和人为中心,使用户与设备协同管理海量数据。此外,IoP系统的底层网络系统具有健壮性,能根据不同的设备实时、动态地配置网络策略。另外,人工智能和云平台等新兴技术为IoP系统进行大数据分析提供了基础。因此,IoP系统具有实时、动态的特性以及多层、复杂的架构,基于IoP系统的可靠性分析十分复杂但具有重要研究意义。

1.2 基于模型的可靠性建模及评估方法

MBDA方法已被广泛应用于不同领域复杂系统的可靠性分析中。在航空航天系统领域,文献[17]提出基于模型的安全性分析方法,通过将故障模型嵌入架构模型中为系统提供一种自动化的安全性分析。在信息物理系统领域,文献[18]提出一种基于AADL的可靠性分析方法,通过对AADL及其附件进行拓展实现了对系统的建模及分析。在医疗系统领域,文献[19]提出一种基于AADL模型转换的可靠性分析方法,通过模型转换技术将AADL可靠性模型转换成双图误差传播模型^[20],实现了对医用检查设备的可靠性分析。本文将采用MBDA方法对IoP系统进行可靠性评估。

目前已有多种建模语言能实现MBDA方法,本文针对嵌入式实时、汽车电子、航空航天等系统领域的建模语言,即UML、SysML、EAST-ADL和AADL,从能否满足IoP系统可靠性建模和评估需求,以及能否提供高效的可靠性分析环境2方面进行对比。在架构建模方面,UML虽然提供了架构和行为模型图,并可建模软件系统,但无法描述IoP系统软硬件的绑定、分配等行为;SysML、EAST-ADL和AADL均能详细地描述软硬件交互行为,且均能对IoP系统的实时动态行为进行分析,但SysML在分析多层次系统的架构时,无法将各层架构模型统一;EAST-ADL是嵌入式汽车电子系统的专用建模及分析语言,而AADL包含了更丰富且通用的软硬件组件以及动态行为建模功能,所以AADL更适合分析IoP系统的架构和动态行为。在可靠性分析方面,AADL的EMA附件能完善地建模故障模型并结合FTA和FHA等分析方法对IoP系统进行详细的可靠性评估。在集成环境方面,AADL的开发平台OSATE为评估IoP系统可靠性提供了高效的环境。因此,AADL可以实现IoP系统的可靠性建模,并能够为评估系统故障的根本原因和危险奠定基础。

由于IoP系统的状态转变过程存在转移概率,且该过程仅受当前状态的影响,因此IoP系统的故障符合马尔科夫过程。另外,由于IoP系统具有实时和动态的特性,因此需要一种方法能在连续时域内对系统进行可靠性评估。文献[21]提出一种基于CTMC的可靠性分析方法,并在连续时域内对某智能电网系统进行了定量分析。文献[22-23]提出了基于CTMC的可靠性分析方法,并对嵌入式系统进行了定量分析。上述研究表明,CTMC能在连续时域内定量分析系统的可靠性,所以本文将采用CTMC评

估IoP系统的动态和实时特性。

CTMC模型定义为如式(1)所示的四元组:

$$C_{CTMC} = (S, T, M, P) \quad (1)$$

其中: S 表示组件的有限状态空间集, $S_m \subseteq S$,且 $S_0 \in S_m$, S_0 表示初始状态,对应IoP系统中组件的初始状态, S_m 表示故障状态的有限空间子集,对应IoP系统中组件的故障状态; $T \subseteq S_m \times S_m$ 表示状态转移集合,对应IoP系统中组件的状态转变; $M = [\lambda_{ij}]$ ($\lambda_{ij} \in [0, 1]$)表示状态转移矩阵, λ_{ij} 表示状态 s_i 到状态 s_j ($s_i, s_j \in S_m$)的转移概率; $P = [P_0(t), P_1(t), \dots, P_i(t)]$ 表示组件的概率向量,其中 $P_i(t)$ 为组件在 t 时刻处于状态 s_i 下的概率。初始条件为 $P_i(t=0)=1, i=0$,当 $P_i(t=0)=0, i \neq 0$ 时,说明组件开始处于 S_0 状态下。求解系统整体的可靠度的步骤如下:

1) 根据系统故障的转移集合和概率,生成对应的状态转移矩阵 M 。

2) 构建如式(2)的时域微分方程,并通过Laplace变换和反演^[24],解得稳态下的概率 $P_i(t)$,最终得到式(3),即IoP系统整体的可靠度,其中 N 和 m 为系统所有非故障终态数。

$$\frac{dP_i(t)}{dt} = P_i(t) \times M, i = 1, 2, \dots, N, N > 1, t > 0 \quad (2)$$

$$R(t) = \sum_{i=1}^m P_i(t), i = 1, 2, \dots, m, m > 1, t > 0 \quad (3)$$

上述研究为本文定量分析IoP系统可靠性提供了一定基础,但IoP系统架构复杂、数据量庞大,若直接采用上述方法对IoP系统进行评估,需要构建系统的CTMC模型,这将产生CTMC状态空间爆炸的问题,所以需要一种CTMC定量评估算法能基于AADL构建的IoP系统可靠性模型进行自动分析。文献[25]提出一种Ocarina的模型转换技术,该模型转换技术以抽象语法树(AST)的形式实现了对系统架构模型的转换,但无法对系统故障模型进行转换。文献[26]针对上述研究进行了改进,实现了对系统可靠性模型的转换,但转换结果不包含CTMC模型。本文提出的可靠性评估方法结合改进的Ocarina模型转换技术将AADL可靠性模型转换为CTMC模型,实现了自动的CTMC定量评估。

2 基于AADL的可靠性评估方法

文献[27]提出一种基于模型的IoP系统可靠性分析方法,该方法通过对系统的架构和故障进行建模,最终采用状态机和FMEA对系统可靠性进行评估。本文考虑了IoP系统实时和动态特性,提出基于AADL的IoP系统可靠性评估方法。该方法不仅对系统的架构和故障行为进行完善地建模,而且还能对系统的动态行为进行模式建模,最后从定性和定量两个角度进行可靠性评估。图2所示为本文方法的框架,该方法被分为A、B两个部分,A部分为基于AADL的IoP系统可靠性建模的过程,B部分为可靠性分析的过程。

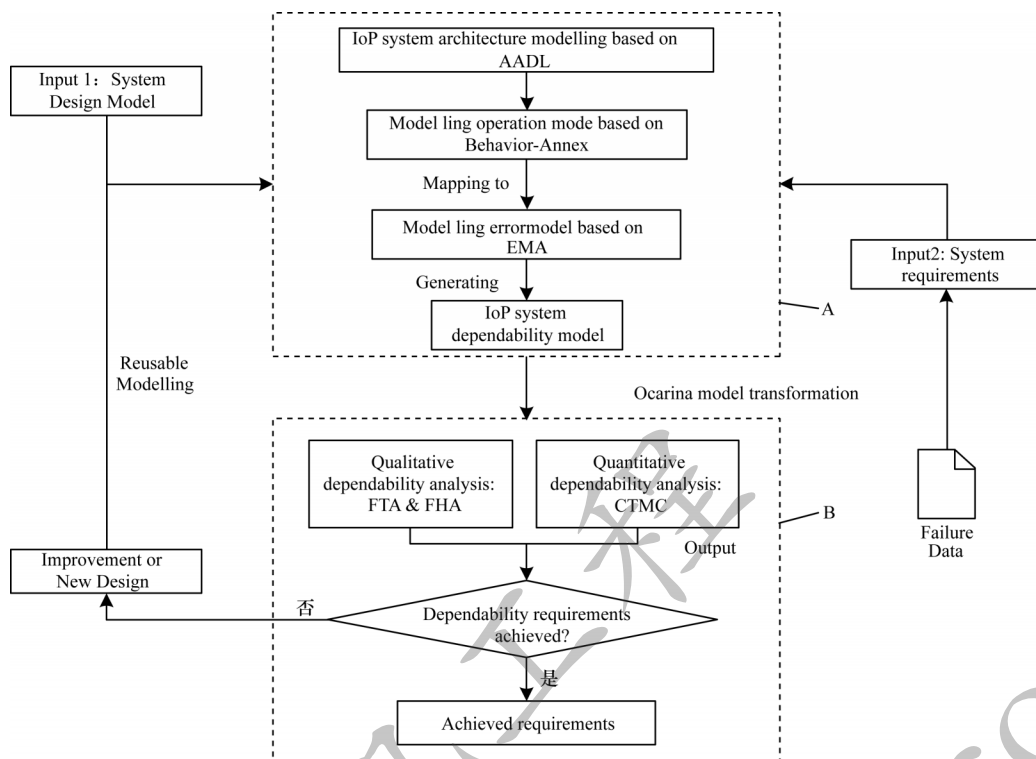


图2 基于AADL的IoP系统可靠性分析方法框架

Fig.2 IoP system dependability evaluation method framework based on AADL

2.1 基于AADL的IoP系统可靠性建模

基于AADL的IoP系统可靠性建模过程(如图2中A部分)分为以下4步:

步骤1 基于AADL的IoP系统架构建模。由于IoP系统具有多层架构,需要先分解组件实体,再根据不同组件实体定义其内部的拓扑结构、功能和行为。以下为具体分析流程:

1)抽象IoP系统的架构层次,横向划分为软件和硬件等类别,纵向由子组件组成,由此划分出组件实体。其中复合组件为系统、子系统、进程和线程等,不可再分组件为设备和子程序等,每个实体都与AADL中的组件类型对应。

2)抽象组件类型的功能和实现。其中功能被表示为组件的端口、属性和数据流。组件类型的实现,定义了绑定、调用、连接等交互行为。

步骤2 基于BA的IoP系统动态行为建模,即基于第1步的系统架构模型,利用AADL的MODE和BA建模IoP系统的动态行为。具体的分析流程如下:

1)将系统动态行为抽象为具体的操作模式。不可再分组件的模式表示为属性和行为,如时间的延迟和操作的执行。复合组件的模式表示为子组件的连接方式。

2)建模系统的模式转换,并将组件的属性、工作模式及其子组件连接方式的变化,作为触发转换的条件。

3)根据模式建模,利用附件BA描述模式转换逻辑,并描述转换所导致的时延、行为操作等产生的影响。

步骤3 根据步骤1、2构建的动态架构模型,利用EMA对IoP系统进行故障建模。故障建模主要是对故障的行为、传播、类型等建模。详细的分析过程如下:

1)声明故障行为库,并定义故障类型、事件、状态。
2)进行故障建模。首先采用组件错误行为状态

机对组件的故障传播源和路径进行建模和分析。然后描述故障状态的转变以及触发转变的事件,并为故障指定传出端口以及设置属性,如概率和风险等。然后采用复合错误行为状态机为复合组件映射其子组件的故障逻辑。

3)操作模式到故障状态的映射。由于系统操作模式的变化与系统实际配置的变化相关,而系统的故障会引发配置变化,因此将操作模式与故障状态相映射,使两者具有关联和实际意义。

步骤4 将生成一个包含架构、动态行为和故障行为的可靠性模型,并完成了图2中A部分。最终生成可靠性模型文件(.aadl和.aadx12),为之后自动地进行可靠性分析提供基础。

2.2 可靠性分析

可靠性分析过程(对应图2中B部分)分为以下3步:1)基于FTA和FHA的定性可靠性分析;2)基于CTMC模型的定量可靠性分析;3)判断系统是否满足可靠性需求。

2.2.1 基于FTA和FHA的定性可靠性分析

本节介绍基于FTA和FHA的定性可靠性分析,首先以文件“.aadxl2”为输入,利用OSATE平台自动生成FTA图和FHA表。FTA自顶向下逐层进行演绎分析,为评估系统故障的根本原因提供了帮助。FHA以组件为关注点,对故障严重度(Severity)和发生频率(Likelihood)进行了分类,并详述了故障模式(Failure mode)和故障发生阶段(Phase)等信息。另外,FHA将严重度分为“1~5”5个递减的程度,并将发生频率分为“A~E”5个递减的等级,这些级别的划分允许以定性的方式来分析和确定FHA结果。具体的分析过程如下:

1)根据 FTA 生成结果,采用逻辑表达式的形式分析顶事件的故障,然后进一步根据 FTA 逐层简化逻辑表达式,最终可以确定某些关键组件的故障组合是导致系统故障的根本原因。

2)利用 FHA 评估关键组件的故障风险。首先分析故障的严重度和频率,然后根据故障模式和发生阶段等信息来评估风险,最后结合 FTA 结果确定优先处理顺序,并在合适的阶段制定系统架构调整方案。

2.2.2 基于 CTMC 模型的定量可靠性分析

本节提出基于 CTMC 定量评估算法,首先将 IoP 系统可靠性模型转换为 CTMC 模型并进行自动定量分析,然后生成 IoP 系统空间树,其根节点包含子系统和进程(中间层组件)的故障信息,最后求解所有路径的概率,得到 IoP 系统的可靠度,从而完成基于 CTMC 模型的定量可靠性分析。详细的算法如下:

算法 1 基于 CTMC 的定量评估算法

输入 可靠性模型(.aadl 文件)

输出 系统可靠度 $R(t)$

步骤 1 利用 Ocarina 将 AADL 可靠性模型转换为对应的 C/C++ 源代码文件。

步骤 2 接收 Ocarina 转换的组件故障数据,并生成 CTMC 模型。首先利用接收函数 $\text{Receive}(\text{Components}, S, T, \lambda, P, M)$ 接收组件数据并处理为 CTMC 类型的数据结构,其中:参数 Components 表示组件 ID;参数 S 表示组件的故障状态; T 表示组件故障状态的转换逻辑,它记录了状态转换和故障事件(故障事件包含了组件内的子部件的故障); λ 表示故障转换概率; P 表示组件稳态概率; M 表示故障转移矩阵。然后利用存储函数 $\text{Memory}(R(), \text{Status})$ 保存组件的 CTMC 模型,其中参数 Status 表示组件处理状态, $R()$ 保存接收函数中的组件信息。

步骤 3 判断组件类型并生成对应的空间树。首先利用判断函数 $\text{Judge}(R())$ 从 $\text{Memory}()$ 调用组

件的信息,然后判断所接收组件的类型,若为进程或子系统且处理状态为未处理,则将组件信息输出。接着利用空间树生成函数 $\text{GenerateTree}(\text{Root}(), \text{Path}[])$ 接收 $\text{Judge}()$ 输出的组件故障信息,并按照故障转移逻辑 T ,由上至下生成树,直至其内部的子组件均被生成在分支中,其中根节点 $\text{Root}()$ 保存该组件的故障数据,解路径集 $\text{Path}[]$ 保存根节点的 T 。

步骤 4 求解根节点的概率。首先利用转移矩阵生成函数 $\text{GenerateMatrix}(S, T, \lambda)$,并遍历 $\text{GenerateTree}()$ 中的根节点的空间树,接收对应的故障信息以生成转移矩阵 M 。然后利用 Laplace 变换和反演函数,即 $\text{LT}(P, M)$ 和 $\text{ILT}(P, M)$,接收 M 并求解式(2)的方程,并将解得的 P 返回给 $\text{Memory}()$,以更新对应组件的故障信息和状态。

步骤 5 将步骤 3、4 作为循环体,从中间层组件向下处理 IoP 系统所有子组件。首先遍历 $\text{Memory}()$ 中的进程类组件并调用循环处理,然后遍历子系统类组件并执行循环处理,最后将 IoP 系统所有子系统节点的概率结果求和,即可求得系统整体可靠度 $R(t)$ 。

结合上述定性和定量分析,在第 4 步对系统可靠性进行综合评估,以判断系统是否满足可靠性需求,若不满足需求,则需要重新调整系统架构,直至满足需求。

3 案例分析

3.1 基于 AADL 的 IoP 医疗系统可靠性建模

在实际应用中,本文将以 IoP 医疗系统为案例来描述基于 AADL 的可靠性建模过程。

3.1.1 基于 AADL 的 IoP 医疗系统架构建模

本节基于 AADL 的 IoP 医疗系统架构建模,并将系统架构抽象为 4 层,即系统、子系统、进程、线程。图 3 所示为 2 层 AADL 架构建模结果(对应图 2),其中 4 个外层系统模块分别对应 W 系统、E 系统、N 系统和 C 系统。

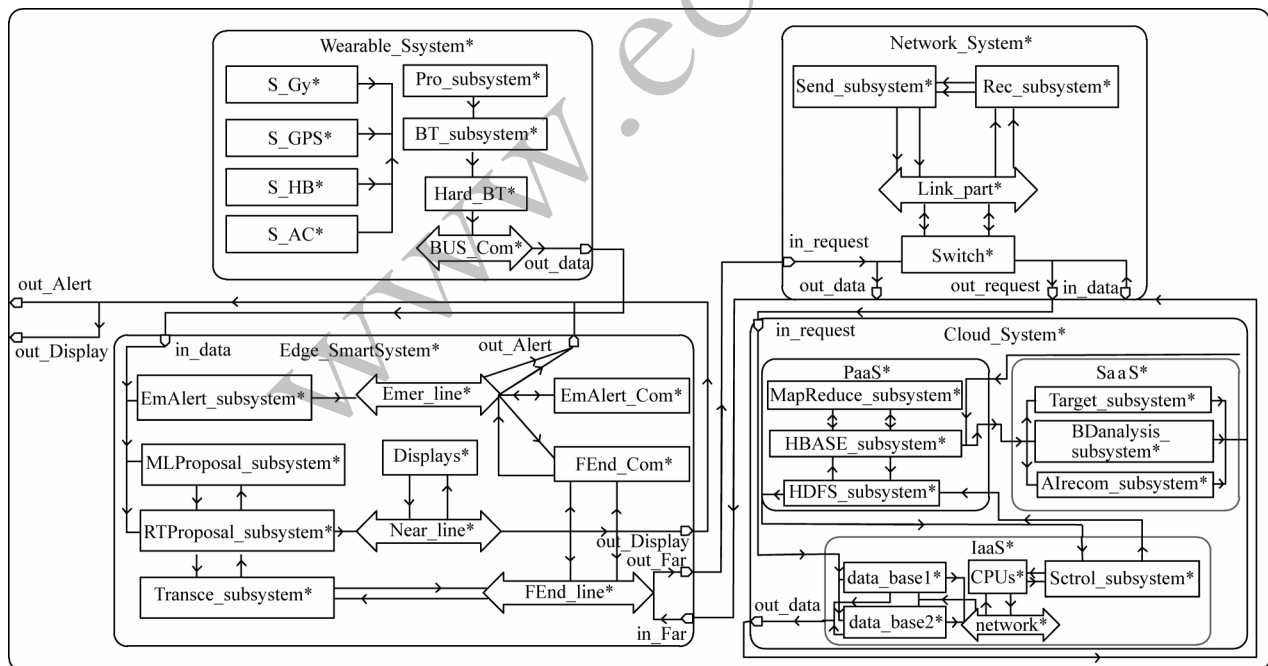


图 3 IoP 医疗系统的 AADL 架构

Fig.3 AADL architecture for IoP healthcare system

W系统主要包含传感器(S_HB和S_AC等)、数据处理子系统(Pro_subsystem)和蓝牙模块(BT_subsystem和Hard_BT),其中传感器接收用户数据并传递给处理系统进行处理,之后由蓝牙模块输出。E系统主要包含紧急通信模块(EmAlert_subsystem和EmAlert_Com)、远程通信设备(FEnd_Com)和服务子系统(例如 RTPProposal_subsystem),当用户面临危险时,紧急通信模块从W系统收到用户数据并向医院和家属发出求助信号。在日常情况下,服务子系统为用户提供健康检测和智能推荐服务,并通过远程通信设备与C系统交互以获得大数据服务等。N系统主要包含协议处理系统(Rec_subsystem和Send_subsystem)。C系统主要包含基础设施(IaaS)、平台(PaaS)和服务(SaaS)3个子模块,其中IaaS包含存储控制模块(Sctrol_subsystem和CPUs)和冗余存储集群模块(data_base),PaaS包含了分布式数据库的核心系统(例如 HBASE_subsystem和HDFS_subsystem),SaaS包含了大数据服务子系统(例如 BDanalysis_subsystem)。通过远程网络连接,C系统可与E系统进行交互并反馈大数据和人工智能服务。

3.1.2 基于AADL的IoP医疗系统模式和故障建模

本节对IoP医疗系统的操作模式和故障模型建模。首先建模操作模式,Normal_operate(N)为初始模式表示系统正常工作,Softtolerant_limit(S)和Hardtolerant_limit(H)表示系统以最大限度容忍软、硬件故障且能正常工作的模式,此时各子系统中至少包含1个可作为备份使用的冗余件,Stops为终止模式,表示系统停机。图4展示了模式建模结果,其中虚线表示触发模式转变的条件,箭头表示模式转变,即系统配置的动态调整。当IoP医疗系统某软硬件出现故障时,系统将启动冗余组件以排除故障,之后系统将从N模式转为S或H模式。如果此时软硬件容错机制执行失败,则说明系统中软硬件组件的故障已超出系统可容忍范围,系统将强制进入Stops模式并停止工作。最后将操作模式与故障行为为映

射,使故障能触发模式转变。

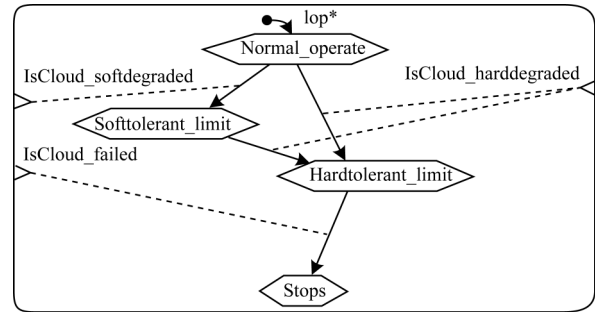


图4 IoP医疗系统的操作模式

Fig.4 Operation mode for IoP healthcare system

图5展示了IoP医疗系统的组件错误行为状态机,IoP系统最初处于Operational状态。当W子系统发生EmergFailure故障时,IoP医疗系统由初始态转变为DefectStop终态,一旦处于该状态,系统将传出Nodata事件并保持等待。当C子系统发生Nodata故障时,IoP医疗系统将从初始态转变为Inadequate等待终态,之后系统保持该状态并传出NoService事件,表示某些云平台服务缺失。当C子系统发生PaaS_degraded故障时,IoP医疗系统由初始态转变为Soft_degraded中间状态,若此时再发生IaaS_degraded故障,系统将转变为Hard_degraded状态,表示云平台中某些软硬件发生故障。若C子系统全部软硬件均失效,则发生ServiceOmission故障,导致IoP医疗系统陷入SeriousStop终止状态,此时系统将传出ServiceOmission事件并停止运行。在初始状态时,若W、E和N子系统中任何1个发生ServiceOmission故障,IoP医疗系统将直接陷入SeriousStop终止状态,表示系统的接收、处理或网络等关键功能失效。图6为EMA建模的文本实现,EMA将故障模型嵌入到架构模型中,最终完成IoP医疗系统的可靠性建模,即完成图2中A的实现。

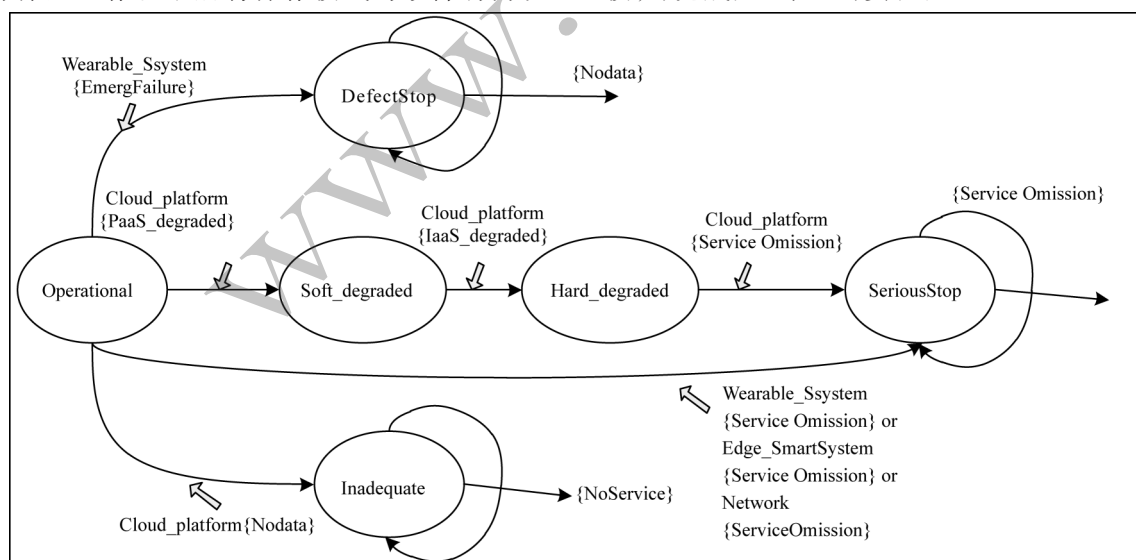


图5 IoP医疗系统的错误行为状态机

Fig.5 Error behavior state machine for IoP healthcare system

顶事件 T_1 、 T_2 和 T_3 对应 IoP 医疗系统处于 D、I 和 S 状态时的事件。由 FTA 生成结果可知, 引起 T_1 的根本原因是 W 系统的心跳传感器发生故障; 引起 T_2 的根本原因为 C 系统内的 SaaS 模块发生故障; 引起 T_3 , 即 IoP 系统严重故障的主要原因是 W 系统、E 系统、N 系统或 C 系统发生了故障, 式(4)为上述逻辑分析结果。对结果进一步分析可知, 心跳传感器、W 系统、E 系统和 N 系统的失效会使 IoP 医疗系统立即失去信息收集、分析以及紧急通信功能, 进而导致系统瘫痪。因此需要着重处理这部分组件的故障。在实际情况中, C 系统不涉及紧急服务, 可为该系统设置容错机制。

$$T = T_1 + T_2 + T_3 = t_{\text{SenH_FailStop}} + t_{\text{SaaS_FailStop}} + t_{\text{C_FailStop}} + t_{\text{W_FailStop}} + t_{\text{E_FailStop}} + t_{\text{N_FailStop}} \quad (4)$$

表 1 所示为一部分重要的 FHA 结果, 由 FHA 表

中故障严重度 Severity 可知, S_HB 传感器危险等级为 1 级, E 系统的 2 个通信设备 EmAlert_Com 和 FEnd_Com 的危险等级均为 2 级, 这些组件的危险等级高。S_AC 传感器的危险等级为 3 级, 其严重度相对较低。分析 Likelihood 和 Phases 两项可知, 上述组件具有发生频率低影响时间长的特性, 所以需要重点预防这些硬件的故障, 特别是要在早期设计阶段考虑双重备份设计。结合 FTA 和 FHA 可知, W 系统和 E 系统故障的危险等级高且属于关键系统, 所以需要优先处理。其中传感器和紧急通信模块的故障可能直接导致用户信息丢失和紧急通信失效, 进而造成重大影响。因此在设计传感器时可增加冗余结构, 在设计通信模块时可增加独立供电系统。另外也不可以忽视其他系统故障影响, 若无法正确地分析用户状态, 同样会造成重大危害。

表 1 IoP 医疗系统的部分 FHA 分析结果
Table 1 Partial FHA analysis results for the IoP healthcare system

组成部分	故障模型元素	描述	交叉引用	失败	运行阶段	严重程度	可能状态
Wearable_SSystem/S_HB	"HB_damage on HB_Failures"	"failed; User extrusion "	"Error Manual example"	" Chemical erosion "	"Re-ceive"	1	D
Edge_SmartSystem/FEnd_Com	"FECOMFailure on Internal_Failure"	"failed; Unable to communicate "	"Error manual example"	" Electronic jamming "	"all"	2	C
Edge_SmartSystem/Em-Alert_Com	"EmCOMFailure on Internal_Failure"	"failed; Can't output EM-Signal "	"Error manual example"	" Electronic jamming "	"all"	2	C
Wearable_SSystem/S_AC	"AC_damage on AC_Failures"	"failed; User extrusion "	"Error Manual example"	" Can't recovery "	"Re-ceive"	3	D

3.2.2 基于CTMC的可靠性定量分析

基于 CTMC 的定量分析算法评估 IoP 医疗系统的可靠性, 首先利用 Ocarina 将系统的可靠性模型转换为 CTMC 模型, 并生成对应的空间树抽象结构, 最

后得到系统的转移矩阵 M 和式(2)的解。式(5)~式(7)所示为系统处于 N 模式、S 模式和 H 模式下的概率分布。

$$P_{\text{normal}}(t) = e^{-(\lambda_{W_D} + \lambda_{C_P_D} + \lambda_{C_In} + \lambda_{W_F} + \lambda_{E_F} + \lambda_{N_F}) \times t} \quad (5)$$

$$P_{\text{soft}}(t) = \frac{\lambda_{C_P_D} \times (e^{-\lambda_{C_I_D} \times t} - e^{-(\lambda_{W_D} + \lambda_{C_P_D} + \lambda_{C_In} + \lambda_{W_F} + \lambda_{E_F} + \lambda_{N_F}) \times t})}{\lambda_{C_In} - \lambda_{C_I_D} + \lambda_{C_P_D} + \lambda_{W_D} + \lambda_{W_F} + \lambda_{E_F} + \lambda_{N_F}} \quad (6)$$

$$P_{\text{hardt}}(t) = \frac{\lambda_{C_I_D} \times \lambda_{C_P_D} \times e^{-\lambda_{C_I_D} \times t}}{(\lambda_{C_F} - \lambda_{C_I_D}) \times (\lambda_{C_In} - \lambda_{C_I_D} + \lambda_{C_P_D} + \lambda_{W_D} + \lambda_{E_F} + \lambda_{W_F} + \lambda_{N_F}) + \frac{\lambda_{C_I_D} \times \lambda_{C_P_D} \times e^{-\lambda_{C_F} \times t}}{(\lambda_{C_F} - \lambda_{C_I_D}) \times (\lambda_{C_In} - \lambda_{C_F} + \lambda_{C_P_D} + \lambda_{W_D} + \lambda_{E_F} + \lambda_{N_F} + \lambda_{W_F})} + \frac{\lambda_{C_I_D} \times \lambda_{C_P_D} \times e^{-(\lambda_{C_In} + \lambda_{C_P_D} + \lambda_{W_D} + \lambda_{E_F} + \lambda_{W_F} + \lambda_{N_F}) \times t}}{(\lambda_{C_In} - \lambda_{C_F} + \lambda_{C_P_D} + \lambda_{W_D} + \lambda_{E_F} + \lambda_{W_F} + \lambda_{N_F}) \times (\lambda_{C_In} - \lambda_{C_I_D} + \lambda_{C_P_D} + \lambda_{W_D} + \lambda_{E_F} + \lambda_{N_F} + \lambda_{W_F})} \quad (7)$$

其中: W 系统的故障转移率为 λ_{W_D} 和 λ_{W_F} ; E 系统的故障转移率为 λ_{E_F} ; N 系统的故障转移率为 λ_{N_F} ; C 系统的故障转移率为 λ_{C_F} 、 $\lambda_{C_I_D}$ 、 $\lambda_{C_P_D}$ 和 λ_{C_In} 。系统整体的可靠度计算式如式(8)所示:

$$R(t) = P_{\text{normal}}(t) + P_{\text{soft}}(t) + P_{\text{hardt}}(t) \quad (8)$$

如图 10(a)、图 10(b) 分别展示了系统处于各模式及其整体的概率分布情况, 结合 FTA 和 FHA 进行定性分析。在 IoP 医疗系统生命周期早期, 经过评估已确

定传感器和通信设备为关键故障组件。通过对其进行更换和维修使系统能可靠运行, 之后系统整体故障率稳定为 1×10^{-5} , 则系统整体及其初始工作模式(N 模式)的概率分布为指数分布。N 模式的概率随时间增长而不断下降, 表明系统因故障而无法继续以 N 模式运行, 此时 IoP 医疗系统通过转变为 S 或 H 模式来容忍自身软硬件故障, 以确保系统运行平稳。S 和 H 模式的概率在其早期随 N 模式概率下降而增长, 表示系统通过

容错机制不断排除自身故障。之后达到最高点0.5,表示系统进入生命周期中期且稳定运行。在18 000 h后IoP医疗系统整体可靠度及S和H模式的概率快速下降至0,说明此时系统容错能力达到极限且某些元器

件逐步老化。为进一步提升系统可靠性,本文在系统生命周期早期将传感器和通信设备更换成更可靠的组件(故障率为 1×10^{-6}),并为W、E等子系统设置冗余容错机制。

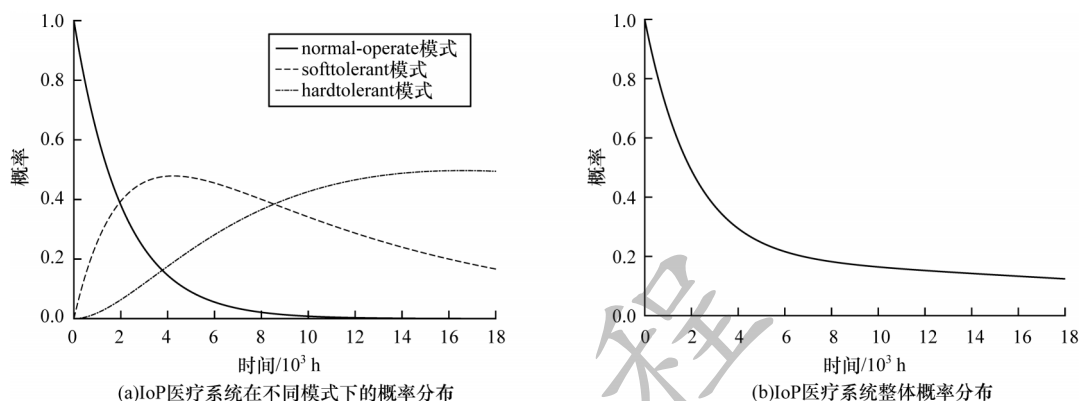


图10 IoP医疗系统架构调整前在不同情况下的概率分布

Fig.10 Probability distribution under different conditions of the IoP healthcare system before adjusting

如图11(a)、图11(b)所示,IoP医疗系统整体可靠度在18 000 h后仍下降缓慢,且系统在S和H模式下的概率也比组件故障率为 1×10^{-5} 时更高,可见经架构调整后元器件后期老化等故障降低,系统容错能力提升。综上,本文提出的可靠性分析方法将定性分析与定量分析相结合,不仅能够评估系统故障的根本原因和危险,还可以评估系统概率分布的原因

以及实时变化的情况,并提出架构调整方案,从而提升IoP医疗系统整体及各模式的可靠性,最终实现了图2中B部分。本文还采用MATLAB对系统各模式及整体的CTMC时域微分方程进行求解,以验证式(5)~式(7),并采用MATLAB数值求解法即龙格—库塔法验证概率计算结果,从而确保实验的准确性。

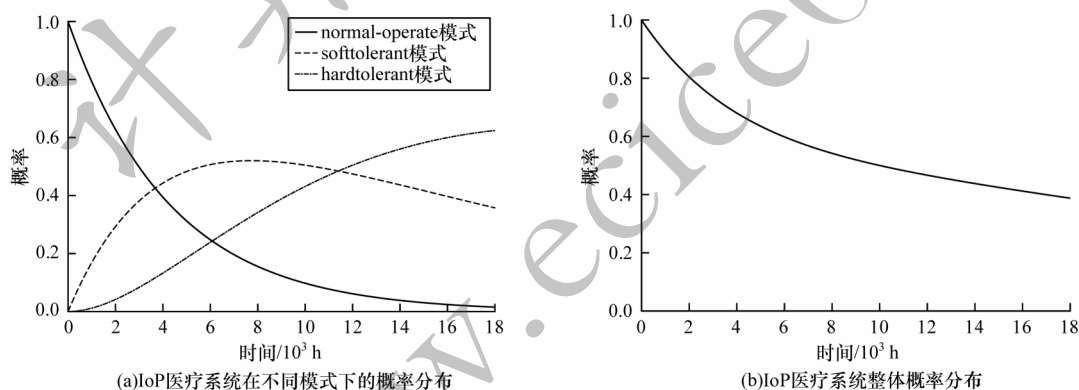


图11 IoP医疗系统架构调整后在不同情况下的概率分布

Fig.11 Probability distribution under different conditions of the IoP healthcare system after adjusting

4 结束语

针对IoP系统实时、动态的特性,本文提出一种基于AADL的IoP系统可靠性评估方法。构建IoP系统的可靠性模型,从定性和定量两方面评估系统的可靠性,并提出基于CTMC的定量评估算法,实现对系统实时、动态等特性的评估。此外,将定性分析与定量分析相结合,为系统传感器和通信模块设计冗余、替换等架构调整方案。实验结果表明,本文方法能对IoP系统进行有效建模,且能自动、准确地对该系统进行可靠性分析。下一步将针对本文IoP系统的网络部分设计详细的拓扑结构,并拓展系统的应用

场景,提高该系统的完整性和通用性。另外,本文使用AADL的MODE对系统的动态行为进行了建模,后续将考虑拓展其属性集,使之在目前的基础上能针对时间变迁等动态特性进行建模与分析。

参考文献

- [1] CONTI M, PASSARELLA A, DAS S K. The Internet of People (IoP): a new wave in pervasive mobile computing [J]. Pervasive and Mobile Computing, 2017, 41(11): 1-27.
- [2] LÜ Z, CHIRIVELLA J, GAGLIARDO P. Bigdata oriented multimedia mobile health applications [J]. Journal of Medical Systems, 2016, 40(5): 120-127.
- [3] PAN Y H. 2018 special issue on artificial intelligence 2.0:

- theories and applications [J]. *Frontiers of Information Technology & Electronic Engineering*, 2018, 19(1): 4-5.
- [4] VARGHESE B, BUYYA R. Next generation cloud computing: new trends and research directions [J]. *Future Generation Computer Systems*, 2017, 79(3): 849-861.
- [5] SHARVIA S, KABIR S, WALKER M, et al. Model-based dependability analysis: state-of-the-art, challenges, and future outlook[J]. *Elsevier*, 2016, 13(3): 251-278.
- [6] SPECIFICATION O A. Data distribution service for real-time systems version 1. 2 [EB/OL]. [2020-09-10]. <https://www.omg.org/spec/DDS/1.2>.
- [7] OMG. Systems modeling language version 1. 1 [EB/OL]. [2020-09-10]. <https://www.omg.org/spec/SysML/1.1/>.
- [8] FEILER P H, GLUCH D P. Model-based engineering with AADL: an introduction to the SAE architecture analysis & design language [M]. Addison-Wesley Professional, 2012: 34-54.
- [9] ASSOCIATION E A. EAST-ADL domain model specification, version V2. 1. 12 [EB/OL]. [2020-09-10]. <http://www.east-adl.info/Specification/V2.1.12>.
- [10] FEILER P. Open source AADL tool environment (OSATE) [EB/OL]. [2020-09-10]. <http://osate.org>.
- [11] MEEKHOF J, BAILEY A B. Failure modes and effects analysis (FMEA) for cataloging: an application and evaluation[J]. *Cataloging and Classification Quarterly*, 2017, 55(7): 493-505.
- [12] RUIJTERS E, STOELINGA M. Fault tree analysis: a survey of the state-of-the-art in modeling, analysis and tools [J]. *Computer Science Review*, 2015, 15(3): 29-62.
- [13] HULSE D, HOYLE C, GOEBEL K, et al. Quantifying the Resilience-Informed Scenario Cost Sum (RISCS): a value-driven design approach for functional hazard assessment [J]. *Journal of Mechanical Design*, 2018, 141(2): 321-403.
- [14] HUGUES J, ZALILA B, PAUTET L, et al. From the prototype to the final embedded system using the ocarina AADL tool suite [J]. *ACM Transaction on Embedded Computing Systems*, 2008, 7(4): 1-25.
- [15] JIN Q, WU B, NISHIMURA S, et al. Ubi-Liven: a human-centric safe and secure framework of ubiquitous living environments for the elderly [C]//*Proceedings of International Conference on Advanced Cloud and Big Data*. Washington D. C., USA: IEEE Press, 2016: 304-309.
- [16] STERGIOU C, PSANNIS K E, KIM B G, et al. Secure integration of IoT and cloud computing [J]. *Future Generation Computer Systems*, 2016, 78(3): 964-75.
- [17] JOSHI A, HEIMDAHL M P, MILLER S P, et al. Model-based safety analysis: NASA/CR-2006-213953 [EB/OL]. [2020-09-10]. https://www.zhangqiaokeyan.com/ntis-science-report_other_thesis/0207179405.html.
- [18] RENYA H, LIJIN W, WEIHUA Z, et al. AADL-based reliability modeling method of cyber-physical systems [C]//*Proceedings of World Symposium on Software Engineering*. New York, USA: ACM Press, 2019: 47-58.
- [19] MOROZOV A, MUTZKE T, REN B, et al. Aadl-based stochastic error propagation analysis for reliable system design of a medical patient table [C]//*Proceedings of Annual Conference on Reliability and Maintainability Symposium*. Washington D. C., USA: IEEE Press, 2018: 1-7.
- [20] MOROZOV A, JANSCHKE K. Probabilistic error propagation model for mechatronic systems [J]. *Mechatronics*, 2014, 24(8): 1189-202.
- [21] SADU A, ROY G K, PONCI F, et al. Methodology for reliability analysis of cyber-physical MTdc grids [J]. *IEEE Journal of Emerging and Selected Topics in Power Electronics*, 2020, 17(9): 1-10.
- [22] ZHANG Q, WANG S H, LIU B. Approach for integrated modular avionics reconfiguration modelling and reliability analysis based on AADL [J]. *IET Software*, 2016, 10(1): 18-25.
- [23] LIM S, YIM D, KHUNTIA J, et al. A continuous-time markov chain model-based business analytics approach for estimating patient transition states in online health infomediary [J]. *Decision Sciences*, 2020, 51(1): 181-208.
- [24] BRZEZI SKI D W, OSTALCZYK P. Numerical calculations accuracy comparison of the inverse laplace transform algorithms for solutions of fractional order differential equations [J]. *Nonlinear Dynamics*, 2016, 84(1): 65-77.
- [25] HUGUES J, SINGHOFF F. AADLv2, an architecture description language for the analysis and generation of embedded systems [C]//*Proceedings of International Conference on Embedded Software*. Washington D. C., USA: IEEE Press, 2013: 11-23.
- [26] GABSI W, ZALILA B, JMAIEL M. Development of a parser for the AADL error model annex [C]//*Proceedings of the 16th International Conference on Computer and Information Science*. Washington D. C., USA: IEEE Press, 2017: 233-238.
- [27] MIAN Z B, BOTTACI L, JIANG J L, et al. A dependability modeling and analysis approach for an IoP-based service system [EB/OL]. [2020-09-10]. https://www.researchgate.net/publication/329469678_A_Dependability_Modeling_and_Analysis_Approach_for_an_IoP-Based_Service_System.

编辑 赖玉玲