软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2020,31(6):1654−1671 [doi: 10.13328/j.cnki.jos.005999]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于 AADL 的失效概率分配及安全性评估方法*

魏晓敏[1], 董泽乾[2], 肖明睿[1], 田 聪[2]

[1](西北工业大学 计算机学院,陕西 西安 710072)

[2](西安电子科技大学 计算机科学与技术学院,陕西 西安 710071)

通讯作者: 魏晓敏, E-mail: xmwei@mail.nwpu.edu.cn

摘 要: 当代航空系统是复杂的安全关键信息物理融合系统(cyber-physical system,简称 CPS).失效概率分配是民用航空系统及设备初步系统安全性评估过程的重要工作,AADL(architecture analysis and design language)适用于航电系统的设计开发,对 AADL 模型实施失效概率分配和安全性评估是不可或缺的.提出了基于 AADL 的失效概率分配方法,可将系统失效概率分配给子构件,作为其安全性需求.该方法综合考虑系统架构设计、模型复杂度和严酷度(severity)等级.通过结合失效概率分配方法和确定性随机 Petri 网(deterministic stochastic Petri-net,简称 DSPN),进一步提出了基于 AADL 的安全性评估方法,将系统的 AADL 模型转换为 DSPN 模型,以计算子构件的失效概率,并评估子构件是否满足安全性需求,直到设计出满足安全性目标的架构模型.最后给出了失效概率分配方法与安全性评估方法的实现算法和工具结构,并通过将所提出的方法应用到飞行控制系统,表明所提方法能够有效地完成失效概率分配和安全性评估.

关键词: AADL;失效概率分配;安全性评估;DSPN

中图法分类号: TP311

中文引用格式: 魏晓敏,董泽乾,肖明睿,田聪.基于 AADL 的失效概率分配及安全性评估方法.软件学报,2020,31(6):1654−1671. http://www.jos.org.cn/1000-9825/5999.htm

英文引用格式: Wei XM, Dong ZQ, Xiao MR, Tian C. Failure probabilities allocation and safety assessment approaches based on AADL. Ruan Jian Xue Bao/Journal of Software, 2020,31(6):1654−1671 (in Chinese). http://www.jos.org.cn/1000-9825/5999.htm

Failure Probabilities Allocation and Safety Assessment Approaches Based on AADL

WEI Xiao-Min[1], DONG Ze-Qian[2], XIAO Ming-Rui[1], TIAN Cong[2]

[1](School of Computer Science, Northwestern Polytechnical University, Xi'an 710072, China)

[2](School of Computer Science and Technology, Xidian University, Xi'an 710071, China)

Abstract: Modern avionics systems are complex safety-critical cyber-physical systems (CPSs). Failure probabilities allocation is the important work for civil airborne systems and equipment during the preliminary system safety assessment process. Architecture analysis and design language (AADL) is suitable for the design and development of avionics systems. It is indispensable to perform failure probabilities allocation and safety assessment for AADL models. This study proposes an AADL-based failure probabilities allocation approach, which considers the design of system architectures, model complexities and severity levels. It allocates failure probabilities to subcomponents as safety requirements. Furthermore, with the integration of the proposed allocation approach and deterministic stochastic Petri-net (DSPN), an AADL-based safety assessment method is proposed. It transforms AADL models to DSPN models to calculate failure probabilities of subcomponents and assesses if subcomponents can satisfy safety requirements, so that an architecture that satisfies safety objectives can be obtained. Finally, the algorithm and the structure of the tool are provided for failure probabilities allocation and

* 基金项目: 国家自然科学基金(61772423)
Foundation item: National Natural Science Foundation of China (61772423)
本文由"信息物理系统软件设计自动化"专题特约编辑卜磊教授、陈铭松教授、朱祺教授、刘超教授推荐.
收稿时间: 2019-08-29; 修改时间: 2019-10-23; 采用时间: 2020-01-13; jos 在线出版时间: 2020-04-18

safety assessment approaches. By assessing flight control systems, it is demonstrated that proposed approaches can effectively perform failure probabilities allocation and safety assessment.

Key words: AADL; failure probabilities allocation; safety assessment; DSPN

信息物理融合系统(cyber-physical system,简称 CPS)[1]融合了物理过程和计算过程,能够感知环境信息,可以响应真实世界的动态变化.CPS 已经广泛应用到航空、汽车、医疗卫生和物流等多个领域,其安全性问题受到越来越多的关注[2,3].当代航空系统是复杂的安全关键 CPS,在设计过程中,需要非常注重系统安全性.ARP 4754A[4]标准将安全性评估过程作为飞机和系统研制过程的一部分,以确保实现的飞机满足安全性需求.ARP 4754A 标准指出:依据 ARP 4761[5]标准在开发阶段实施安全性评估,将 ARP 4761 标准作为安全性评估的指南和方法.因为民用飞机的研制过程必须严格遵循 ARP 4754A 标准规定的流程才能取得美国和欧洲的适航认证,所以研究航空系统的安全性评估方法非常必要,可以为完成规定的安全性评估过程提供经验和技术.

航空领域常用的安全性分析方法有故障树分析(fault tree analysis,简称 FTA)、故障模式和影响分析(failure mode and effects analysis,简称 FMEA)、依赖图(dependence diagram,简称 DD)和马尔可夫分析(Markov analysis,简称 MA)等.ARP 4761 标准将这些方法运用到民用航空系统及设备安全性评估过程中,并给出系统安全性评估的 3 个过程,依次为功能危险性评估(function hazard assessment,简称 FHA)过程、初步系统安全性评估(preliminary system safety assessment,简称 PSSA)过程和系统安全性评估(system safety assessment,简称 SSA)过程.PSSA 的主要目的是确认系统架构满足 FHA 过程得到的安全性目标,并将安全性目标分解为子系统/项目(item)的安全性需求.

AADL(architecture analysis and design language)[6,7]是一种支持航空系统设计、可信属性分析、功能验证和实现的架构模型设计语言,可用于 CPS 建模、分析与验证[8,9],也可用于系统架构虚拟集成[10],以识别系统各部分设计模型之间的一致性问题.AADL 已受到空客、波音、Honeywell、欧洲航天局和卡耐基梅隆大学等科研和工业机构的广泛关注[11].基于 AADL 模型的设计和开发方法可以降低大规模航空系统设计的复杂度,提高从系统设计到实现的可追踪性.本文主要针对 ARP 4761 标准中 PSSA 过程的不足:它仅给出了基于 FTA,DD 和 MA 的 PSSA 过程,但是没有给出从失效概率分配到评估的完整的安全性评估过程,也没有明确的建议以何种方式将系统失效概率分配给子系统/项目.同时,它未提供基于 Petri 网的评估方法,FTA 和 DD 很难刻画多种失效模式之间的依赖关系,而 MA 和确定性随机 Petri 网(deterministic stochastic Petri-net,简称 DSPN)可以自然地刻画顺序依赖事件.DSPN 比连续时间马尔可夫链(continuous-time Markov chain,简称 CTMC)具有更强的建模和分析能力,因此,本文针对安全关键系统 AADL 模型提出失效概率分配方法,并且研究基于 DSPN 的安全性评估方法.当前,尽管 FTA 很难刻画出一个完整的系统(例如可修复系统),但是工业界仍然主要采用基于 FTA 的安全性评估过程,因为 FTA 是一种结构化的、易于理解的分析工具,而 MA 和 DSPN 分析对工程人员的理论要求较高且没有明确的文献指导说明.但是,Petri 网既有严格的数学表达形式,也有直观的图形化表达形式,能够描述依赖行为、并发行为等,可用于系统设计和可信属性分析.本文将明确给出基于 DSPN 的安全性评估流程,并实现该方法,以便于工程人员参考和使用 DSPN 理论评估系统的安全性.

目前,关于失效概率分配的研究文献比较少,尤其针对航空 CPS 领域,但是与其相关的可靠性分配领域有许多成熟的方法[12]可供参考,如等同分配法、模糊分配法和 AGREE(advisory group of reliability of electronic equipment)分配方法等.等同分配法操作简单,但是航空子系统可靠性水平差异较大,不适合直接使用此方法对整个系统进行分配.模糊分配法主要依赖于已有经验,对设计人员要求较高.文献[13]针对串联系统提出了基于模糊数学的可靠性分配方法.AGREE 分配方法是美国国防部电子设备可靠性顾问团提出,用于串联系统可靠度分配.尽管 AGREE 方法考虑了子系统复杂度和系统对整机的重要程度,但是它仅仅用子系统包含的单元数刻画复杂度,不能直接应用于同时包含子构件和构件之间的交互连接的 AADL 模型.此外,因为复杂的航电系统内部是串联结构和并联结构的混合体,只考虑串联或者并联无法满足实际需求,并且本文需要的失效概率分配方法要能够适用于层次化的 AADL 模型结构.已有相关研究人员对 AGREE 分配方法进行扩展.文献[14]对 AGREE 方法进行改进,结合复杂度和重要度,但是在复杂度方面只考虑构件数量,不适用于具有复杂交互连接

关系的 AADL 模型.文献[15]也对 AGREE 方法进行改进,以技术成熟度作为复杂度,以构件在电路循环中的重要性和相邻构件的重要性进行确定构件自身的重要度.这种可靠性分配方法是针对电源转换器的特征而提出,不适用于 AADL 模型.此外,文献[16]对主要的可靠性分配方法进行综述,包括 ARINC(aeronautical radio, Inc.)、AGREE、目标可行性法(feasibility-of-objectives)、Bracha、平均加权分配法(average weighting allocation method)和最大熵有序加权平均(maximal entropy ordered weighted averaging)等方法,其中,ARINC 和 AGREE 方法不能适用于并行系统.文献[17]提出基于广义伯恩鲍姆重要测度(generalized birnbaum importance measure)的系统可靠性分配方法,综合考虑了可靠性范围、制造复杂度和技术可行性,可以应用于串联和并联系统.但是该方法不适用于层次化的 AADL 模型,也不适用于包含大量软件系统的安全关键系统.

在基于 AADL 的安全性分析和评估方面的研究,文献[18,19]提出了基于 AADL 的危险分析方法,制定出从 AADL 模型到 DSPN[20]模型的转换规则,并实现了自动的模型转换工具,然后对 DSPN 模型进行仿真计算,得到危险的发生概率.文献[21]为可重构系统建立 AADL 模型,提出了基于系统安全性的动态重构方法,并将 AADL 动态重构模型转换为 DSPN 模型,利用 DSPN 模型对系统进行仿真,分析系统的安全性.针对电网 CPS 的安全性,文献[9]将系统的正常运行与外部环境威胁刻画为相互博弈的过程,提出了基于 AADL 建模技术和双人博弈理论的安全性分析方法.文献[22]将概率模型检验方法结合到安全性分析方法中,通过制定模型转换规则,将 AADL 模型转换为 CTMC,并且能自动生成属性公式,然后基于概率模型的检验结果分析系统安全性.文献[23]基于 AADL 模型和概率模型检验,提出了自动的系统安全性分析方法,将 AADL 模型转换为概率模型,通过模型检验评估系统的安全性,最后生成代码支持软件仿真,对安全性评估进行确认.该方法覆盖了从高级建模到代码生成的整个设计过程,从平台独立模型到平台描述模型,再到平台相关模型,其中:平台独立模型由 AADL 软件构件刻画,平台描述模型由 AADL 硬件构件和 AADL 错误模型刻画,平台相关模型由 AADL 绑定属性刻画.文献[24]针对一类不确定性敏感(uncertainty-aware)的混成 AADL 模型,提出了一种基于统计模型检验的定量性能评估方法,扩展了 AADL 混成模型语义,制定了规则,将 AADL 模型转为 NPTA(network of priced timed automata)模型.文献[25]利用基于广义随机 Petri 网(generalized stochastic Petri net,简称 GSPN),提出了 AADL 模型可靠性分析评估工具.文献[26]扩展了 AADL 属性,提出了基于 AADL 的 FMECA(failure modes, effects and criticality analysis)方法,可以定性地分析系统安全性.文献[27]对 FMEA 进行了扩展,提出了基于 AADL 的安全关键嵌入式系统定量分析方法.COMPASS(correctness, modeling and performance of AeroSpace systems)是安全关键系统分析验证工具集[28,29],针对 AADL 语言的子集,在安全性分析方面支持 FTA 和 FMEA 分析方法.以上这些方法都不是针对 PSSA 过程而提出的.文献[30]依据 ARP 4761 标准提出了基于 AADL 的安全性评估方法,包括基于 AADL 的 FTA,FMEA,CTMC 和离散时间马尔可夫链(discrete-time Markov chain,简称 DTMC)等,但是没有考虑如何将系统失效概率分配给子构件.本文对此提出了解决方案,并进一步提出了基于 Petri 网的 AADL 模型安全性评估方法.

本文针对安全关键系统,提出了基于 AADL 的失效概率分配方法.该方法综合考虑 AADL 架构的层次化设计、模型复杂度和构件失效造成影响的严重程度,解决了安全性评估过程中如何分配失效概率的问题.结合失效概率分配方法,又提出了基于 DSPN 的 AADL 模型安全性评估方法,可以有效地评估系统安全性,将 FHA 过程得到的安全性目标分解为具体的子构件(包括子系统类型)安全性需求,也为 ARP 4761 标准补充了基于 Petri 网的安全性评估过程方法,为系统安全性评估的实际运用提供指导和参考案例.

本文第 1 节介绍 AADL 和经典的 AGREE 可靠性分配方法.第 2 节给出基于 AADL 失效概率分配方法及安全性评估方法的框架.第 3 节对本文提出的面向 AADL 模型的失效概率分配方法进行详细论述,包括串联结构和并联结构的失效概率分配方法.第 4 节首先给出本文所提方法的实现算法和工具实现结构图,然后以简单的飞行控制系统为典型的 CPS 应用案例解释说明失效概率分配和安全性评估方法,并与 ARP 4761 标准给出的安全性评估方法进行比较分析,再对一个复杂的飞行控制系统进行安全性评估,进一步说明方法的可用性.最后,在第 5 节总结全文和展望未来研究工作.

1 AADL 和 AGREE 分配方法

1.1 AADL

AADL[6,7]是架构分析与设计语言,可以将系统刻画为一种层次化的架构模型.下层构件(子构件)嵌套于上层构件(复合构件)内.AADL 模型中包含子构件的构件称为复合构件,复合构件可以包含的子构件有系统构件、硬件构件和软件构件.硬件构件也称为执行平台构件,包括设备、处理器、总线和存储器等.软件构件包括系统、进程、线程、数据和子程序等.子构件也可以包含子构件,AADL 允许构件之间层层嵌套.构件交互连接方式包括端口连接(connection)、数据访问、总线访问和子程序调用等.

错误模型附录(error model annex)[31]是 AADL 语言的一个补充,用于支持基于 AADL 模型的安全性、可靠性和可用性等可信分析.错误模型附录能够为架构模型刻画非功能属性信息:(1) 通过构件错误行为(component error behavior)语句,可以描述构件内的错误行为状态机,包括错误、错误事件和错误变迁;(2) 通过错误传播语句,基于构件之间的连接,可以描述构件之间的错误传播关系;(3) 通过复合错误行为(composite error behavior)语句,可以为复合构件建立复合错误行为,描述子构件的错误状态对复合构件错误状态的影响;(4) 通过错误模型属性描述语句,可以为错误行为描述属性信息,例如描述错误事件发生服从的概率分布类型和参数,以支持随机错误行为的刻画.通过在 AADL 架构模型的构件中建立错误模型,从而支持在早期设计阶段分析系统的可信属性.

1.2 AGREE分配方法

AGREE 分配方法是系统单元寿命服从指数分布的经典可靠性分配方法,提出该方法的目的是解决电子设备的可靠性分配问题,可以表示为

$$R^{\frac{n_i}{N}}=e^{-\frac{\omega_i t_i}{\theta_i}} \tag{1}$$

其中,R 表示系统可靠度,ω_i 表示子系统 i 的重要度,θ_i 表示子系统 i 的平均无故障时间,t_i 表示系统要求子系统 i 的工作时间,n_i 表示子系统 i 所包含的单元数,N 表示系统所包含的单元数.

根据公式(1)可以发现:AGREE 方法是按照各子系统的复杂性和重要性进行可靠度分配,不仅考虑了子系统的复杂性和重要性,而且考虑了它们与系统之间的失效关系.

2 基于 AADL 的失效概率分配及安全性评估方法

本文提出的基于 AADL 的安全性评估方法框架如图 1 所示,针对 FHA 给系统指定的安全性目标,将目标分解为具体的安全性需求,并评估子构件是否能够满足安全性需求,确认系统满足安全性目标:

第①步,为系统建立架构模型,包含子构件以及子构件之间的交互连接.再为子构件建立错误模型,为每个子构件描述正常状态、失效状态和状态之间的变迁关系以及变迁发生服从的分布与参数.同时,要根据 ARP 4754A 标准为失效状态定义严酷度等级,并刻画于模型中;还要为复合构件建立复合错误行为,描述上层构件失效与子构件失效之间的关系,由此建立系统的 AADL 模型.

第②步,为了分配失效概率,以系统的 AADL 模型作为输入,利用面向 AADL 模型的失效概率分配方法,根据模型的复杂度,为下一层构件生成失效概率分配表,作为子构件的安全性需求,详细的失效率概率分配方法将在第 3 节介绍.

第③步,借助文献[18,19]实现的从 AADL 模型到 DSPN 模型的转换工具,将 AADL 模型转换为 DSPN 模型,包括子构件内的错误行为状态机、子构件之间的错误传播、复合错误行为和触发条件中的逻辑表达式等,生成系统的 DSPN 模型.利用 TimeNet[32]工具对 DSPN 模型仿真计算,得到系统和子构件失效状态的发生概率.

第④步,生成安全性评估列表,包括失效状态、分配的失效概率 P_a、计算得到的失效概率 P_c 和这两类概率值的比较结果,由此判断系统的架构设计是否能够满足安全性需求.

- 如果 $P_a<P_c$,即 AADL 模型不能够满足安全性需求(分配的失效概率),那么很可能模型设计不能满足安

全性需求,需要修改架构模型和错误模型(本文通过调节参数值的形式来改进模型设计,这些参数是对系统设计和开发提出的安全性要求,设计人员可以通过重新设计、增加冗余构件等方式达到参数要求,未来将研究架构模型结构优化方法),然后根据第②步重新分配失效概率,其次,要根据第③步重新计算各个子构件的失效概率;

- 如果 $P_a \geqslant P_c$,即,AADL 模型能够满足安全性需求,那么此时既保证系统设计模型能够满足系统安全性需求,也完成将系统失效概率分配到各个子构件的目的.分配给子构件的失效概率将作为更低层级模型(子构件)安全性评估过程需要满足的安全性目标.

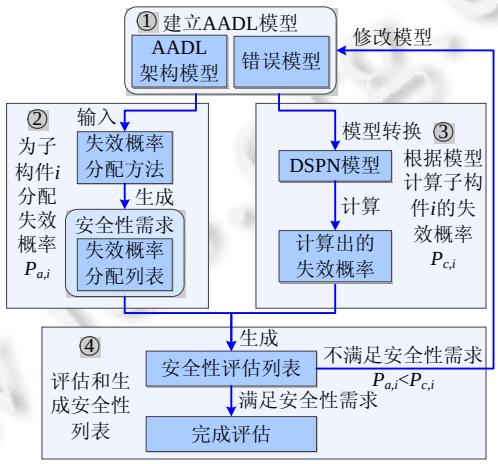


Fig.1 Framework of AADL-based safety assessment approach

图 1 基于 AADL 的安全评估方法框架

3 面向 AADL 模型的失效概率分配方法

假设 AADL 模型中各构件的可靠性服从指数分布,本文提出了面向 AADL 模型的综合的失效概率分配方法,其中,改进 AGREE 分配方法提出了 AADL 串联构件分配失效概率,还基于等同分配思想提出了 AADL 并联构件失效概率分配方法.

3.1 AADL模型失效概率分配方法

AADL 系统模型中,复合构件的复合错误行为能够描述复合构件失效状态与其直接子构件失效状态之间的关系.本文提出的失效概率分配方法基于系统的复合错误行为.如果子构件的失效状态没有在复合错误行为中出现,那么不需要为其分配失效概率,因为它不会对复合构件失效状态造成影响.在复合错误行为中,子构件的状态组合(复合错误行为的发生条件)对复合构件状态的影响既可以通过逻辑连接词 AND(与)和 OR(或),也可以通过逻辑原语 ORMORE(或者多于)和 ORLESS(或者少于),其中,逻辑原语可以转换为逻辑连接词 AND 和 OR 的组合[18].因此,在失效概率分配过程中,只需要考虑复合错误行为包含 AND 和 OR 的情况.本文提出的 AADL 模型失效概率分配方法主要包括以下 3 步.

1) 首先,为了分配失效概率,对复合错误行为的触发条件进行拆分,每个 AND 部分作为一个整体,将发生条件改写为只包含 OR 的逻辑表达式,即析取式.错误行为的触发条件 tc 可以表示为析取式 $tc=es_1 \mathrm{OR} es_2 \mathrm{OR} \ldots \mathrm{OR} es_m$,其中,$es$ 可以是子构件的失效状态,也可以是子构件失效状态的 AND 组合.通过将 tc 转换为析取式,实现子构件之间串联和并联关系的重新划分;
2) 其次,从复合构件的角度来看,OR 逻辑表达式的各个组成部分是串联的关系,即复合构件由子构件串联而成.复合构件失效的发生概率受串联的子构件的发生概率影响.因此,对于 OR 逻辑表达式中的各个子构件,利用第 3.2 节提出的针对 AADL 串联构件的改进过的 AGREE 分配方法分配失效概率,运

用后文公式(9)将失效概率分配给子构件的失效状态 $es_i(0<i\leqslant m)$,即,将失效概率分配给每个子构件(这里的子构件可以是 AND 组合);

3) 最后,对于每个 AND 组合,其相当于多个子构件并联而成.当 AND 组合内各个组成部分都失效时,AND 组合失效,所以各组成部分的失效概率的累积等于 AND 组合的失效概率.利用第 3.3 节提出的针对 AADL 并联构件的失效概率分配方法分配失效概率,运用后文公式(13)为 AND 组成的各个组成部分分配失效概率.

在 AADL 模型的复合错误行为中,OR 逻辑表达式的多个组成部分可能都包含同一个子构件的失效状态,即同一个子构件的失效状态出现了多次.对于这种情况,上述面向 AADL 的失效概率分配方法会为同一个子构件分配多个失效概率.系统安全性是安全关键系统必须要保证的属性,所以当子构件被分配了多个失效概率时,选取最小的失效概率值作为子构件的安全性需求,也就是以最高的安全性要求约束子构件.

由此,通过结合面向 AADL 串联结构的改进过的 AGREE 失效概率分配方法和面向 AADL 并联结构的失效概率分配方法,可对 AADL 模型进行失效概率分配.

3.2 AGREE分配方法的改进

FHA 分配给系统的失效概率,作为 PSSA 过程的输入,由此可以进一步得到复合构件的可靠度.可靠度与失效概率的关系可以表示为[5]

$$R=1-FP \tag{2}$$

其中,R 表示构件可靠度,FP 表示构件失效概率.

子构件 i 的失效率 f_i 与其平均无故障时间 θ_i 之间的关系表示为

$$f_i=\frac{1}{\theta_i} \tag{3}$$

将公式(2)和公式(3)带入公式(1),子构件 i 的失效率 f_i 可以表示为

$$f_i=\frac{n_i(-\ln(1-FP))}{N\omega_i t_i} \tag{4}$$

AADL 模型是一种层次化结构模型,构件之间存在交互连接,本文主要考虑端口连接(数据端口、事件端口和事件数据端口连接)、数据访问、总线访问和子程序调用.子构件之间以及子构件内部的交互连接数之和(c_i)以及子构件包含的子构件数(s_i)都是由架构设计决定,这里用 c_i 和 s_i 代表架构模型的复杂度,将架构的设计和复杂度结合到失效概率分配方法中.为了将 c_i 和 s_i 结合到失效概率分配公式,公式(1)中的 N 和 n_i 修改为

$$n_i=c_i+s_i \tag{5}$$

$$N=\sum_{i=1}^{m}(c_i+s_i) \tag{6}$$

公式(5)中,c_i 表示子构件 i 与其他子构件的交互连接数和子构件内部的交互连接数之和,s_i 表示子构件 i 自身构件及其所包含的子构件数之和.公式(6)中,m 表示复合构件所包含 m 个子构件.

对于安全关键系统,系统的安全性极为重要,因此,本文根据失效状态的严酷度等级定义子构件的重要程度.失效发生所造成的影响分为 5 个等级:catastrophic(致命性的)、hazardous(灾难性的)、major(严重的)、minor(轻度的)和 no effect(没有影响),catastrophic 表示最严重,往后依次降低.本文制定了严酷度等级与重要度 ω_i 的对应关系,它们分别对应重要度值 0.9,0.7,0.5,0.2 和 0.001,严酷度等级越高,重要程度越高.重要度值可以针对不同的系统,根据专家的经验进行重新调整和设定.当子构件失效状态的严酷度等级是 no effect 时,不需要考虑其失效概率,因为它不会对系统造成影响,在计算过程中直接忽略此子构件.此外,OR 逻辑表达式中 AND 组合的 ω_i 值,取 AND 组合的各组成部分的重要度平均值 $\bar{\omega}$.

将公式(5)和公式(6)带入公式(4),新的失效率计算公式表示为

$$f_i = \frac{(c_i + s_i)(-\ln(1-FP))}{\left(\sum_{i=1}^{m}(c_i + s_i)\right)\omega_i t_i} \tag{7}$$

已知子构件失效率 f_i 与可靠度 R_i 的关系为

$$R_i = e^{-f_i t_i} \tag{8}$$

将公式(8)带入公式(2),子构件失效概率计算方法是

$$FP_i = 1 - R_i = 1 - e^{-f_i t_i} \tag{9}$$

其中,FP_i 表示子构件 i 的失效概率,R_i 表示子构件 i 的可靠度.

由此,通过计算架构模型的复杂度(子构件数和交互连接数)和子构件的重要度(失效状态发生的严酷度等级),进而根据公式(9)可以将失效概率分配给子构件.这也符合 ARP 4761 标准提出的:PSSA 的实施依赖于架构设计、复杂度和失效状态的严酷度等级等.传统的方法考虑了复杂度和重要度等因素,主要用于可靠性分配,目前没有文献针对 AADL 提出失效概率分配方法.经典的 AGREE 方法仅仅以子系统包含的单元数作为复杂度,不能充分反映架构设计.本节针对 AADL 串联构件提出的改进的 AGREE 分配方法,综合考虑子构件数和交互连接数,用它们衡量 AADL 模型复杂度,更符合 AADL 模型层次化、构件互连的特征.为了对整个 AADL 模型分配失效概率,后文还提出了 AADL 并联构件失效概率分配方法.

本文提出改进的 AGREE 分配方法的前提是:各构件的可靠性要服从指数分布.然而,AADL 模型中可能存在服从确定性时间分布的错误事件,使得从 AADL 模型转换得到的 DSPN 模型可能包含确定性时间迁移(非指数迁移).这也是合理的,因为在计算稳态(steady-state)概率时,可用指数迁移替代确定性时间迁移,即通过对确定性时间迁移的延迟时间参数,即发生率(firing rate)取倒数作为对应的指数分布的率参数(rate parameter)[20].

3.3 AADL并联构件失效概率分配方法

OR 逻辑表达式中的 AND 组合相当于一组并联构件.改进的 AGREE 分配方法能够对串联的子构件分配失效概率,不适用于并联的子构件.等同分配法适用于并联结构,但是其假设各个子模块的失效概率相同,没有考虑子模块之间的可靠度差异,不适用于复杂安全关键 CPS.因此,本节基于等同分配思想提出了 AADL 并联构件失效概率分配方法,并联结构的整体失效概率计算公式为

$$FP_p = \prod_{t=1}^{h} FP_{p,t} \tag{10}$$

其中,FP_p 表示第 p 个 AND 组合的失效概率,h 表示第 p 个 AND 组合有 h 个组成部分,$FP_{p,t}$ 表示分配给第 p 个 AND 组合的第 t 个组成部分的失效概率.

实际的子构件之间的可靠度差异较大,所以本文将架构模型的设计和复杂度结合到并联构件分配方法中,子构件的复杂度越高,其失效概率越大,同时要将构件的重要性考虑在内,重要性越高,其失效概率越小.利用公式(5)的 n_i(c_i 与 s_i 之和)表示模型设计和复杂度,AND 组合中子构件失效概率之间的关系表示为

$$\frac{FP_{p,t}}{FP_{p,k}} = \frac{n_{p,t}}{w_{p,t}} \Big/ \frac{n_{p,k}}{w_{p,k}} = \frac{n_{p,t} w_{p,k}}{n_{p,k} w_{p,t}}, 0 < t \leqslant h, 0 < k \leqslant h \tag{11}$$

其中,$n_{p,t}$ 表示第 p 个 AND 组合的第 t 个组成部分的复杂度,而 $w_{p,t}$ 是其重要度值.

将公式(11)带入公式(10),得到公式(12):

$$FP_p = \left(\prod_{t=1,2,\ldots,k-1,k+1,\ldots,h} \frac{n_{p,t}}{w_{p,t}}\right)\left(\frac{w_{p,k}}{n_{p,k}}\right)^{h-1} (FP_{p,k})^h, 0 < k \leqslant h \tag{12}$$

根据公式(5)和公式(12),得到第 p 个 AND 组合的第 k 个组成部分的失效概率计算公式为

$$FP_{p,k}=\sqrt[h]{\frac{FP_p\left(\frac{n_{p,k}}{w_{p,k}}\right)^{h-1}}{\prod_{t=1,2,\ldots,k-1,k+1,\ldots,h}\frac{n_{p,t}}{w_{p,t}}}}=\sqrt[h]{\frac{FP_p\left(\frac{c_{p,k}+s_{p,k}}{w_{p,k}}\right)^{h-1}}{\prod_{t=1,2,\ldots,k-1,k+1,\ldots,h}\left(\frac{c_{p,t}+s_{p,t}}{w_{p,t}}\right)}},0<k\leqslant h \tag{13}$$

由此,按照公式(13),依据 AND 组合(合取式)中子构件的复杂度差异,将失效概率分配给 AADL 并联子构件.

4 工具实现与案例分析

本文提出的失效概率分配方法和 AADL 模型安全性评估方法已实现为 Eclipse 插件,第 4.1 节介绍实现算法以及工具实现结构图.然后,以简单的飞行控制系统[33]为典型 CPS 案例,在第 4.2 节~第 4.4 节对提出的基于 AADL 的失效概率分配及安全性评估方法进行解释说明,第 4.5 节将所提方法与 ARP 4761 标准中的安全性评估方法进行对比分析.最后,第 4.6 节对一个复杂飞行控制系统进行分析与验证,进一步说明所提方法的可用性.

4.1 工具实现

基于 AADL 的失效概率分配及安全性评估方法的实现算法如图 2 所示.

	输入:系统实例 *SysInstance*;
	输出:安全性评估列表.
1	将系统 *Sys* 复合错误行为的触发条件修改为析取式 es_1ORes_2OR…ORes_m,由 *es* 构成集合 *ES*;
2	若 *es* 是单个子构件的失效状态,放入 *ESSingle* 集合;
3	若 *es* 是多个子构件构成的 AND 组合,放入 *ESMulti* 集合;
4	**for** *Sys* 的子构件 sub_i **then** //计算 c_i,s_i 和 ω_i
5	计算 sub_i 的 c_i;
6	计算 sub_i 的 s_i;
7	获取 sub_i 的严酷度等级,得到 ω_i;
8	**end for**
9	**for** $es_i \in ES$ **then** //OR 组合,使用 AADL 串联构件失效概率分配方法
10	**if** $es_i \in ESSingle$ **then** //为单个子构件分配失效概率
11	根据公式(9)计算 FP_i;
12	**else if** $es_i \in ESMulti$ **then** //为 AND 组合分配失效概率
13	计算 es_i 的 c_{es_i} 和 s_{es_i};
14	es_i 的重要度值 ω_{es_i} 取各子构件严酷度值的平均值;
15	根据公式(9),为 es_i 分配失效概率 FP_{es_i};
16	**end if**
17	**end for**
18	**for** $es_k \in ESMulti$ **then** //AND 组合,使用 AADL 并联构件失效概率分配方法
19	es_k 内的子构件构成集合 ES_k;
20	**for** $es_{k,sub} \in ES_k$ **then** //为 AND 组合的组成部分分配失效概率
21	根据公式(13),为 $es_{k,sub}$ 计算失效概率 $FP_{es_{k,sub}}$;
22	**if** $es_{k,sub}$ 已经被分配了失效概率 $oldFP_{es_{k,sub}}$ **then** //一个构件只分配一个失效概率
23	比较 $oldFP_{es_{k,sub}}$ 和 $FP_{es_{k,sub}}$ 值,选小的值作为 $es_{k,sub}$ 的失效概率;
24	**end if**
25	**end for**
26	**end for**
27	得到分配给每个子构件的失效概率;
28	将系统 AADL 模型实例 *SysInstance* 转换为 DSPN 模型;
29	对 DSPN 模型进行计算,得到每个子构件的失效概率;
30	综合分配的失效概率和计算得到的失效概率,生成安全性评估列表;

Fig.2 Algorithm of the AADL-based safety assessment approach

图 2 基于 AADL 的安全性评估方法实现算法

首先,在第 1 行将系统复杂错误行为的触发条件改写为析取式,由此进一步实施失效概率分配和安全性评

估.第 4 行~第 27 行,利用本文提出的基于 AADL 的失效概率分配方法,将失效概率分配给子构件,作为安全性需求.其中:第 4 行~第 8 行计算每个子构件的 c_i,s_i 和 ω_i,以支持后续的失效概率分配;第 9 行~第 17 行利用面向 AADL 串联构件失效概率分配方法,将失效概率分配给析取式中的每个部分;第 18 行~第 27 行利用 AADL 并联构件失效概率分配方法,将概率值分配给 AND 组合中的子构件.第 28 行、第 29 行利用 DSPN 转换工具[18]生成 DSPN 模型,并计算得到子构件的失效概率.第 30 行对比分配的失效概率和计算得到的失效概率,生成安全性评估列表,结束一次安全性评估.

依据安全性评估列表,如果 AADL 模型不能满足安全性需求,那么修改 AADL 模型,然后按照图 2 给出的算法重新对系统模型进行评估.以这种方式不断重复模型修改过程和安全性评估过程,直到建立的 AADL 模型能够满足安全性需求.

本文提出的基于 AADL 的安全性评估方法工具实现结构图,分为 4 个层次,如图 3 所示:工具在 Eclipse 集成开发环境(第 1 层)上开发;基于 AADL 开源工具 OSATE(open source AADL tool environment)[34]进行扩充,OSATE 提供了基本的模型设计功能(第 2 层),支持第 3 层的 AADL 建模和模型实例化;第 4 层的 AADL 模型安全性评估功能,以 AADL 实例模型为输入,能够为子构件自动分配失效概率,能够将 AADL 实例化模型转换为 DSPN[18],CTMC[22],DTMC 和随机多人博弈(stochastic multi-players game,简称 SMG)[9]等模型.本文主要关注 DSPN 转换.为了计算 AADL 模型中子构件的失效概率,可以利用现有的计算工具,如 TimeNet、概率模型检验工具和 SMG 验证工具等.由此,在第 4 层的失效概率分配、模型转换和失效概率计算等功能的基础上,可以进一步实施 AADL 模型安全性评估.

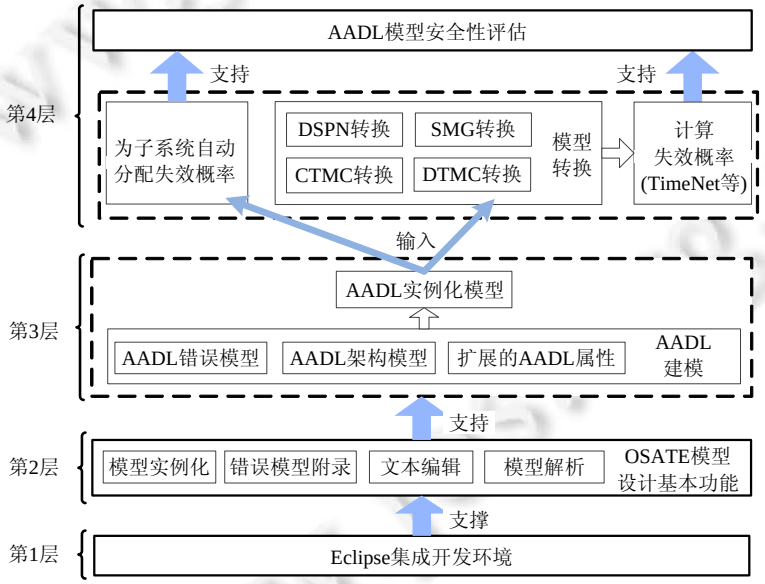


Fig.3 Structure of the tool for the proposed approach

图 3 本文提出方法的工具结构图

4.2 建立飞行控制系统的AADL模型

作为 CPS 系统,飞行控制系统(flight control system,简称 FCS)的 AADL 架构模型如图 4 所示.系统包含了两个通道(channel1 和 channel2)、一个数据采集系统(DataCollect)和一个数据输出系统(output),每个通道包含 3 个子构件,数据采集系统包含一个子构件,数据输出系统包含两个子构件.飞行控制 CPS 通过数据采集系统从外界采集数据,并将数据传输给两个通道;两个通道分别处理数据,然后将处理结果传给输出系统;飞控 CPS 通过输出系统将控制数据发送给作动设备.FCS 内部构件之间的连接如图 4 所示.

本文采用的一次飞行时间是参照 ARP 4761 标准的案例,平均飞行时长为 5 小时,按一次飞行对飞行控制系

统进行失效概率分配.假设从 FHA 得到飞行控制系统的一次飞行的失效概率是 1.0E−4.

为飞行控制系统的每个子构件建立错误模型,每个构件包含 3 个状态:正常状态(operational,简写为 O)、瞬时错误状态(transient,简写为 T)和失效状态(failed,简写为 F).正常状态由一个错误事件(ee1)触发到达瞬时错误状态,瞬时错误状态由一个恢复事件(re1)回到正常状态;瞬时错误状态可能会由一个错误事件(ee2)触发到达失效状态,失效状态由一个修复事件(re2)回到正常状态.各个子构件中的 ee1,re1,ee2 和 re2 服从的概率分布、发生概率和事件发生需要的时间,如表 1 的第 3 列~第 5 列所示.其中,两个通道发生瞬时错误或失效的概率不一样.因为实际应用过程中,为了防止两个通道因为相同的原因失效,通常以不同的方式实现相互冗余的系统.此外,按确定性时间延迟分布发生的事件是在一定时间之后必然发生的,所以发生概率是 1.0.

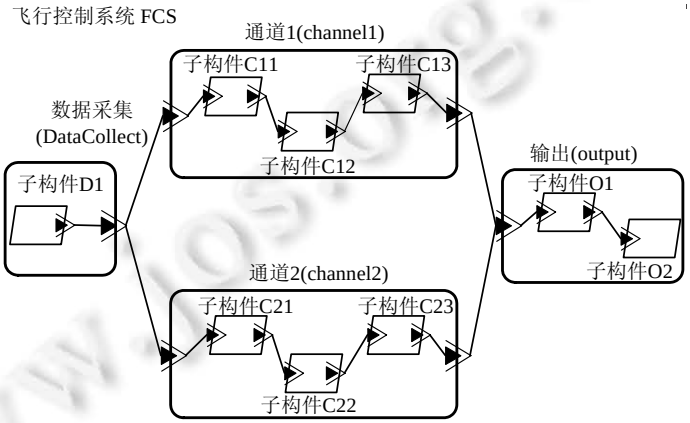


Fig.4 AADL architecture model of FCS

图 4 飞行控制系统 AADL 架构模型

Table 1 Distribution and parameters of events in the error model

表 1 错误模型中事件的分布和参数

构件	事件	分布类型	发生概率	发生时间	率参数λ	延迟时间(1/λ)
数据采集 Data Collect	Dee1	指数	0.98	大于 20h	2.8059E−7	3563878.8
	Dee2	指数	0.99	大于 60h	4.6529E−8	21491819.1
	Dre1	确定性时间延迟	1.0	22ms	45.45	0.022
	Dre2	指数	0.99	小于 10min	7.6753E−3	130.3
通道 channel1 和 channel2	C1ee1/C2ee1	指数	0.95/0.9	大于 5h	2.8496E−6/2.9267E−6	350923.1/341684.0
	C1ee2/C2ee2	指数	0.8/0.85	大于 30h	2.0661E−6/1.5048E−6	483993.4/664538.0
	C1re1/C2re1	确定性时间延迟	1.0/1.0	25ms/40ms	40/25	0.025/0.04
	C1re2/C2Re2	指数	0.95	小于 20min/15min	2.4964E−3/3.3286E−3	400.6/300.4
数据输出 Output	Oee1	指数	0.99	大于 10h	2.7918E−7	3581969.8
	Oee2	指数	0.97	大于 60h	1.4101E−7	7091451.7
	Ore1	确定性时间延迟	1.0	40ms	25	0.04
	Ore2	指数	0.99	小于 8min	9.5941E−3	104.2

已知指数分布的发生概率和发生需要的时间,根据指数分布公式可以计算出 DSPN 模型中迁移(指数迁移和确定性时间延迟迁移)的参数值.要先计算出各个迁移的指数分布率参数λ,由指数分布概率公式(14)可以计算出,如下:

$$F(t)=1-e^{-\lambda t} \tag{14}$$

$$\lambda=-\frac{\ln(1-F(t))}{t} \tag{15}$$

其中,t 是时间,$F(t)$是发生概率.

根据公式(15)可以计算出率参数λ,见表 1 第 6 列.因为 DSPN 计算工具 TimeNet 把所有类型的迁移发生时间统一描述为延迟时间,所以要将指数分布迁移的率参数要取倒数,作为延迟时间.对于确定性时间延迟分布迁

移的参数,迁移的延迟时间就是其延迟参数[20].依据 ARP 4754A[4]标准,为每个子构件失效状态发生的影响确定严酷度等级,两个通道的严酷度等级都是 hazardous,另外两个子系统的严酷等级都是 major,见表 2 第 5 列.飞行控制系统发生失效的复合错误行为是:当数据采集系统失效、数据输出系统失效或者两个通道同时失效时,飞行控制系统失效,即:

[DataCollect.DF1 **OR** channel.C1F1 **AND** channel2.C2F1 **OR** Output.OF1]→FCS.SF.

Table 2 List of failure probabilities allocation (one flight time)

表 2 失效概率分配列表 (一次飞行时间)

序号	失效状态	c_i	s_i	严酷度等级	ω_i	FP_i(一次飞行)	FP_i(每秒)
1	DataCollect.DF1	3	2	major	0.5	3.13E−5	1.74E−9
2	Output.OF1	4	3	major	0.5	4.38E−5	2.43E−9
3	channel1.C1F1 **AND** channel2.C2F1	12	8		0.7	8.93E−5	4.96E−9
4	channel1.C1F1	6	4	hazardous	0.7	9.45E−3	5.25E−7
5	channel2.C2F1	6	4	hazardous	0.7	9.45E−3	5.25E−7

由此构建出 AADL 模型如图 5 所示.

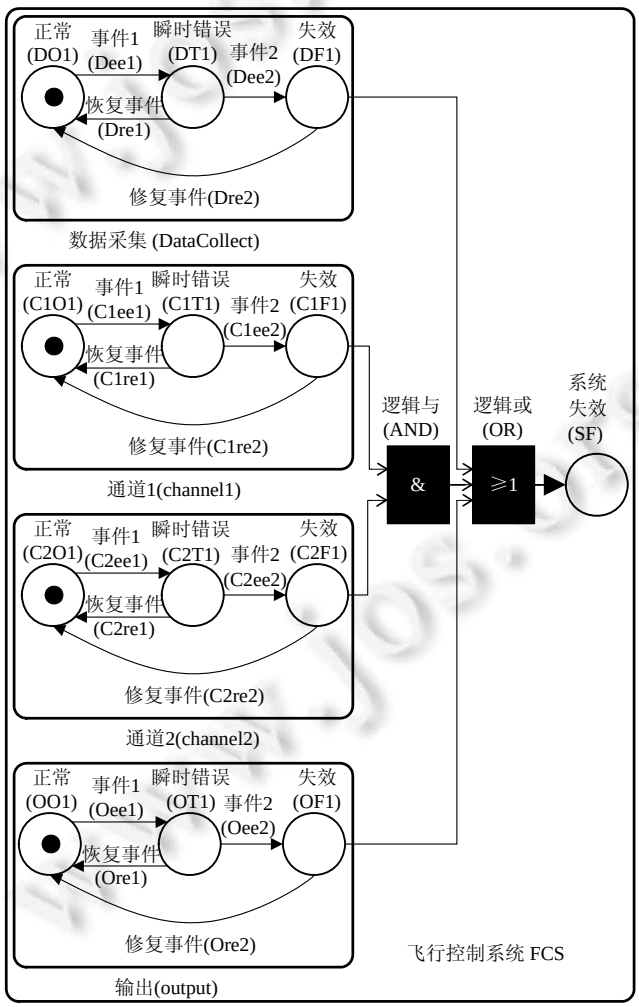


Fig.5 AADL model of FCS

图 5 飞行控制系统 AADL 模型

各个圆圈(○)表示错误状态,中间有一个黑点的圆圈(•)是初始错误状态,错误状态之间带实心箭头(→)的连线表示错误变迁,连线上的事件表示触发错误变迁的条件,逻辑 AND 组合表示通道 1 和通道 2 的失效状态的“与”关系,逻辑 OR 组合表示数据采集系统的失效状态、AND 组合的结果以及输出系统的失效状态三者的“或”关系并得到系统失效状态(SF).这里,系统的复合错误行为使用逻辑 AND 组合和 OR 组合表示.

4.3 分配系统失效概率

根据第 3 节提出的基于 AADL 的失效概率分配方法,将系统失效概率分配给子构件.依据飞行控制系统的复合错误行为,因为两个通道构成了一个 AND 组合,所以看作一个整体,使得复合错误行为由 3 部分的 OR 组合,即 DataCollect.DF1 **OR** (channel1.C1F1 **AND** channel2.C2F1) **OR** Output.OF1.对第 4.2 节构建的 AADL 架构模型和错误模型进行分析,可以得到公式(9)和公式(13)所需的参数(c_i,s_i 和 ω_i)如表 2 所示.进而根据第 3.2 节的公式(9),利用本文在第 3.2 节改进过的 AGREE 分配方法,为数据采集子系统、由两通道的 AND 组合和数据输出子系统分配失效概率,分配的失效概率值(FP_i)如表 2 前 3 行的倒数第 2 列所示.然后,对于两个通道的 AND 组合,根据第 3.3 节的公式(13),利用 AADL 并联构件失效概率分配法为两个通道分配失效概率,见表 2 第 4 行、第 5 行的倒数第 2 列所示,两个通道在一次飞行时间内的失效概率都是 9.45E−3.表 2 中,构件每秒的失效概率 FP_i(见最后一列)根据一次飞行的失效概率计算得到.

4.4 生成DSPN模型和安全性评估列表

将飞行控制系统的 AADL 模型转换为 DSPN 模型如图 6 所示.

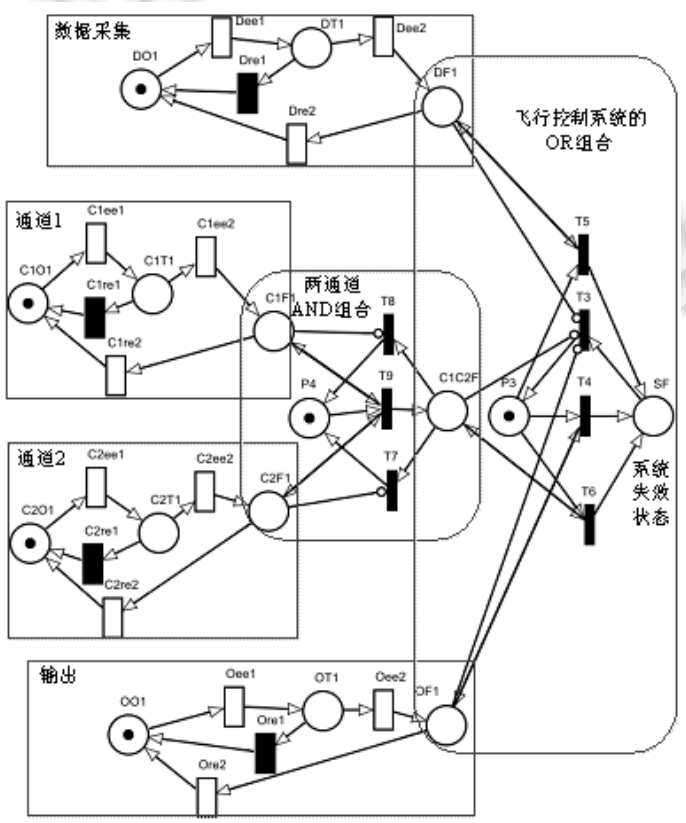


Fig.6 DSPN model transformed from the AADL model of FCS

图 6 从飞行控制系统 AADL 模型转换得到的 DSPN 模型

子系统的错误模型对应到长方形方框中的 DSPN 模型,系统的复合错误行为由两个圆角长方形圈出,一个

对应两个通道失效的 AND 组合,一个对应数据采集系统失效、AND 组合的结果和输出系统失效三者构成的 OR 组合.

模型转换功能依据文献[18]给出的规则,错误状态转换为 DSPN 的位置(place),初始错误状态对应到带一个标记(token)的位置;错误事件转换为一个迁移(transition),可以是瞬时迁移(黑色细实心矩形)、指数迁移(宽空心矩形)和确定性时间迁移(黑色宽实心矩形),并且每个迁移可以带有一个延迟参数(见表 1 第 6 列);错误状态的逻辑 AND 组合按照一个模板进行转换,如图 6 中对应两通道失效 AND 组合的 DSPN 模型,为其添加一个带单个标记的位置(P4)、3 个瞬时迁移(T7~T9)和一个表示 AND 组合结果的位置 C1C2F,然后使用弧(空心箭头和圆圈箭头)作为它们的连接;同样的,错误状态逻辑 OR 组合也可以按照一个模板进行转换,最后得到与图 5 的错误状态 OR 组合对应的 DSPN 模型,详细的规则请参照文献[18].

采用 TimeNet 的稳态仿真(stationary simulation)功能的标准(standard)模式[35],通过仿真 DSPN 模型的稳态行为进行仿真计算.仿真计算工具配置为:置信度(confidence level)为 99%,最大相对误差(maximal relative error)为 5%,概率测度的允许差异(permitted difference for probability measures)为 5%,其他参数采用默认值.实验运行的环境是在 Intel(R)Core(TM)i7-3770 CPU@3.40GHz 和 16G 内存的平台上.通过对转换得到的 DSPN 模型进行仿真计算,得到系统和各个子系统的失效概率,见表 3 第 3 列.

系统的失效概率以及第 4.3 节分配的失效概率是一次飞行时间的失效概率,即 5 小时内的失效概率,转换为每秒的失效概率,见表 2 的最后一列.计算值与分配值进行比较,所有计算值都小于对应的分配值,因此,架构设计满足安全性需求,安全性评估列表见表 3.

Table 3 List of safety assessment (s)

表 3 安全性评估列表 (秒)

失效状态	分配的失效概率 FP_i	DSPN 模型计算出的失效概率	是否满足安全性
DataCollect.DF1	1.74E−9	1.131789E−9	满足
Output.OF1	2.43E−9	8.980342E−10	满足
channel.C1F1	5.25E−7	4.629636E−8	满足
channel2.C2F1	5.25E−7	2.706902E−8	满足
FCS.SF	5.56E−9	2.030337E−9	满足

从上述分析可以看出:本文提出的基于 AADL 的安全性评估方法可以对系统有效地实施评估,其中的失效概率分配方法也是可行的;同时,能够通过安全性评估的 AADL 模型是满足系统安全性的系统设计模型,在设计阶段保证了系统安全性.在实际运用过程中,可能要多次重复失效概率分配和安全性评估过程,才能最终完成安全性需求分解的过程和获得一个满足安全性需求的 AADL 模型.

4.5 安全性评估方法对比分析

本节主要将本文所提方法与 ARP 4761 标准中的安全性评估方法进行对比分析.ARP 4761 标准描述了利用 FTA,DD 和 MA 实施 PSSA 的过程,但是没有提供明确的方法指导工程人员如何将上层系统的失效概率分配给子系统或者项目,FTA,DD 和 MA 只是被用于验证分配的失效概率是否能够满足安全性需求.本文提出的基于 AADL 的安全性评估方法在两个方面优于 ARP 4761 给出的方法:(1) 本文提出了基于 AADL 的失效概率分配方法,综合考虑了模型的复杂度和系统架构模型特性,而 ARP 4761 标准没有给出失效概率分配方法;(2) 提供了详细的 AADL 模型安全性评估实施流程,能够指导实际的评估过程,实现了安全性评估工具,能够降低工程人员的 DSPN 理论学习要求,并且能够辅助评估过程.此外,通过结合 DSPN 计算方法,使得本文提出的安全性评估方法具备足够的安全性评估能力,与 ARP 4761 标准提出的方法具有相同的评估能力,详细的原因如下.

ARP 4761 标准明确说明了 FTA,DD 和 MA3 种方法可以相互替代,同时也说明了 FTA 和 DD 存在一些不足:FTA 和 DD 很难刻画多种失效模式之间的依赖关系;FTA 只能评估单个顶事件的原因和发生概率;FTA 很难刻画出一个完整的系统,例如可修复系统,因为这种系统的失效率和修复率是状态依赖的.而 MA 没有这些问题,可以很自然地刻画顺序依赖事件,具有更强的建模和分析能力.因此,这里主要将本文使用的 DSPN 分析方法与 MA 方法进行比较.

随机 Petri 网(stochastic Petri-net,简称 SPN)是状态之间变迁的发生满足指数分布延迟时间的 Petri 网,SPN 与连续时间马尔可夫链(CTMC)同构[36].广义随机 Petri 网(GSPN)[37]由 SPN 扩展而来,位置(place)状态之间迁移的发生既可以满足指数分布延迟时间的时间迁移(timed transition),也可以是立即发生的立即迁移(immediate transition).立即迁移的发生需要的时间为 0,它的优先级高于时间迁移.同样,可以将 GSPN 转换为一个等价的 CTMC,而且转换难度会比将 SPN 转换为 CTMC 更简单[36].DSPN 由 GSPN 扩展而来,在 GSPN 的基础上增加了一种时间迁移,迁移发生前的延迟时间是一个常量,即确定性时间延迟.本文使用的 DSPN,同一个位置状态上只能有一个确定性时间延迟分布的迁移.由此,基于 DSPN 与半马尔可夫链(semi-Markov chain)同构[36]的理论,可以将 DSPN 转换为等价的半马尔可夫链.半马尔可夫链是状态之间变迁的发生可以服从一般概率分布(general distribution)的时间延迟,即状态逗留时间可以是一般概率分布.当半马尔可夫链中状态变迁之间的时间分布是指数分布分布时,这个半马尔可夫链是一个 CTMC.当半马尔可夫链中状态变迁之间的时间分布只是一个时间点时,这个半马尔可夫链是一个 DTMC.

由上述内容可知:DSPN 的描述能力比 GSPN 强,GSPN 与 CTMC 同构,所以 DSPN 的描述能力比 CTMC 强.此外,在分析 DSPN 模型时,许多计算工具需要将 DSPN 转换为同构的半马尔可夫链,而不是 CTMC.所以基于现有的 DSPN 分析工具,本文提出的利用 DSPN 模型的安全性评估方法也能比利用 CTMC 的方法好.从整体方法的角度来看,本文提出的安全性评估方法比 ARP 4761 中的方法更为明确,包含了失效概率分配和验证失效概率是否满足安全性需求,实施过程更为具体、清晰.

4.6 复杂飞行控制系统分析

为了更好地验证本文所提方法可用于复杂系统,本节依据文献[18]给出的复杂飞行控制系统(FCS),对该复杂系统进行安全性评估,系统内部可以不是子系统,可以是进程和设备等,符合 ARP 4761 标准的要求,对子系统/项目分配失效概率并评估安全性.为系统建立 AADL 模型,如图 7 所示,包括架构模型和错误模型.

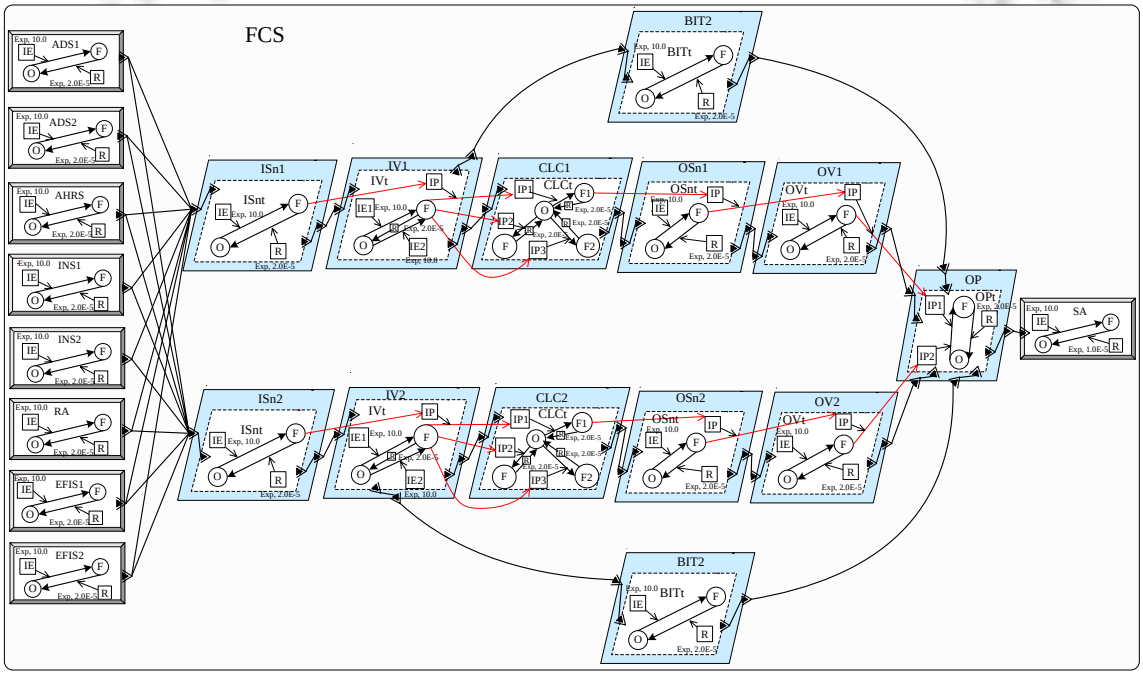


Fig.7 AADL model of the complex FCS

图 7 复杂飞行控制系统 AADL 模型

FCS 架构模型包括 9 个设备和 11 个进程,设备包括空气数据系统(ADS)、姿态和航向参考系统(AHRS)、

惯导系统(INS)、无线电测高仪(RA)、电子飞行信息系统(EFIS)和伺服作动器(SA),进程包括输入同步、输入表决、控制率计算、输出同步、输出表决、机内测试(BIT)和输出(OP).错误模型由图中的圆圈、方框和带箭头的连线构成,圆圈表示错误状态(O 表示正常状态,F 表示失效状态),方框表示错误事件(IE 表示构件内导致失效的错误事件,R 是恢复事件,IP 是错误传播导致的向内传播点),黑线表示错误变迁,红线表示错误传播.为了使图 7 更为清晰,直接用线程的失效状态表示进程的失效状态.依据文献[18]使用的参数,错误事件的分布类型和参数(Exp 表示指数分布),如图中所示.各个构件的严酷度等级见表 4 第 5 列.FCS 的复合错误行为是:[AHRS.F **and** RA.F **and** INS1.F **and** INS2.F **or** ADS1.F **and** ADS2.F **and** EFIS1.F **and** EFIS2.F **or** CLC1.F **and** CLC2.F **or** ISn1.F **and** ISn2.F **and** IV1.F **and** IV2.F **or** OSn1.F **and** OSn2.F **and** OV1.F **and** OV2.F **or** BIT1.F **and** BIT2.F **and** OP.F **and** SA.F]→FCS_F.

Table 4 List of failure probabilities allocation (one flight time)

表 4 失效概率分配列表 (一次飞行时间)

序号	失效状态	c_i	s_i	严酷度等级	ω_i	FP_i(一次飞行)	FP_i(每秒)
1	AHRS.F **and** RA.F **and** INS1.F **and** INS2.F	4	8		0.6	1.563E−5	8.68E−9
2	ADS1.F **and** ADS2.F **and** EFIS1.F **and** EFIS2.F	4	8		0.5	1.875E−5	1.04E−9
3	CLC1.F **and** CLC2.F	4	8		0.7	1.339E−5	7.44E−9
4	ISn1.F **and** ISn2.F **and** IV1.F **and** IV2.F	8	34		0.6	5.469E−5	3.04E−9
5	OSn1.F **and** OSn2.F **and** OV1.F **and** OV2.F	8	16		0.6	3.125E−5	1.74E−9
6	BIT1.F **and** BIT2.F **and** OP.F **and** SA.F	7	19		0.6	3.385E−5	1.88E−9
7	AHRS.F, RA.F	1	2	major	0.5	0.074391	4.132821E−6
8	INS1.F, INS2.F	1	2	hazardous	0.7	0.053136	2.952014E−6
9	ADS1.F, ADS2.F, EFIS1.F, EFIS2.F	1	2	major	0.5	0.065804	3.655761E−6
10	CLC1.F, CLC2.F	2	4	hazardous	0.7	0.003660	2.033125E−7
11	ISn1.F, ISn2.F	2	11	hazardous	0.7	0.092648	5.147095E−6
12	IV1.F, IV2.F	2	6	major	0.5	0.079820	4.434421E−6
13	OSn1.F, OSn2.F	2	4	hazardous	0.7	0.063190	3.510557E−6
14	OV1.F, OV2.F	2	4	major	0.5	0.088466	4.914779E−6
15	BIT1.F, BIT2.F	2	4	major	0.5	0.099883	5.549034E−6
16	OP.F	2	10	hazardous	0.7	0.142689	7.927191E−6
17	SA.F	1	1	hazardous	0.7	0.023782	1.321198E−6

与第 4.2 节相同,假设从 FHA 得到飞行控制系统的一次飞行的失效概率是 1.0E−4.依据第 3 节提出的失效概率分配方法,分配的一次飞行时间失效概率见表 4,进一步计算得到每秒的失效概率.再将 AADL 模型转换为 DSPN 模型,包括 108 个位置、141 个迁移和 413 条弧.通过使用 TimeNet 仿真计算得到各失效状态的发生概率(运行环境和工具配置与第 4.4 节相同),见表 5,耗时 4'16".

由表 5 的第 9 行、第 10 行、第 13 行、第 14 行和第 22 行可见,CLC1,CLC2,IV1,IV2 和 SA 不能满足安全性需求.

为了使系统 AADL 模型满足安全性要求,需要修改模型,通过调节参数值的形式来改进模型设计.降低 IV1 和 IV2 构件的错误事件 IE 的率参数,增加恢复事件 R 的率参数,提高它们的质量要求,即,要求在设计和开发过程中使 IE 发生的可能性足够低和 R 发生的可能性足够高.在详细设计 IV1 和 IV2 时,可以采用的方式有添加冗余构件或者增加防护措施等.对于 CLC1,CLC2 和 SA,也采用同样的方式.因此,通过将 IV1 和 IV2 的 IE 事件参数值调整为 5.0E−6,R 事件的参数调整为 30.0;CLC1 和 CLC2 的 R 事件的参数调整为 30.0;SA 的 IE 参数值调整为 1.0E−5,R 事件参数调整为 30.0.AADL 模型的其余部分不变,所以分配的失效概率也保持不变.最后进行仿真计算,CLC1.F,CLC2.F,IV1.F,IV2.F 和 SA.F 的发生概率分别是 1.656396E−7,1.657927E−7,3.322293E−7,3.327276E−7 和 3.353078E−7,系统及其子构件都满足安全性需求.为节省空间,不再列出新的安全性评估列表.

5 总结与展望

本文提出一种面向安全关键 CPS 的 AADL 模型失效概率分配方法,同时,利用失效概率分配方法和 DSPN 计算方法进一步提出基于 AADL 的安全性评估方法.分析 AADL 模型的特性,针对串联构件改进经典的 AGREE

分配方法,基于等同分配思想,提出 AADL 并联构件失效概率分配方法.结合这两种方法提出针对 AADL 模型的失效概率分配方法,在失效概率分配过程中综合考虑 AADL 模型的架构设计和复杂度,将子构件的交互连接数量和子构件数量综合到失效概率分配公式中.以此为基础,本文提出 AADL 模型安全性评估方法,能够先为子构件分配失效概率作为安全性需求,再将 AADL 模型转换为 DSPN 模型,然后计算每个子构件的失效概率,进而将计算的失效概率与分配的安全性需求进行比较,判断架构模型是否满足安全性需求.若不满足,修改 AADL 模型,重复进行面向 AADL 模型的失效概率分配和利用 DSPN 模型的失效概率计算,直到 AADL 模型满足安全性需求,完成对系统的安全性评估,将 FHA 过程得到的安全性目标分解为具体的子构件安全性需求.案例分析表明:本文提出的方法能够应用于失效概率分配,提出的 AADL 模型安全性评估方法结合了失效概率分配方法和 DSPN 计算模型,可以有效地运用到飞行控制系统安全性评估过程中,可作为 ARP 4761 标准中失效概率分配和基于 Petri 网的 PSSA 过程的参考方法.

Table 5 List of safety assessment (s)

表 5 安全性评估列表 (秒)

序号	失效状态	分配的失效概率 FP_i	DSPN 计算的失效概率	是否满足安全性
1	AHRS.F	4.132821E−6	2.030885E−6	满足
2	RA.F	4.132821E−6	1.976264E−6	满足
3	INS1.F	2.952014E−6	2.050184E−6	满足
4	INS2.F	2.952014E−6	1.993724E−6	满足
5	ADS1.F	3.655761E−6	1.911982E−6	满足
6	ADS2.F	3.655761E−6	1.987798E−6	满足
7	EFIS1.F	3.655761E−6	2.004445E−6	满足
8	EFIS2.F	3.655761E−6	2.036431E−6	满足
9	CLC1.F	2.033125E−7	2.038997E−6	不满足
10	CLC2.F	2.033125E−7	1.995506E−6	不满足
11	ISn1.F	5.147095E−6	1.94222E−6	满足
12	ISn2.F	5.147095E−6	1.967703E−6	满足
13	IV1.F	4.434421E−6	5.190607E−6	不满足
14	IV2.F	4.434421E−6	4.873762E−6	不满足
15	OSn1.F	3.510557E−6	2.047837E−6	满足
16	OSn2.F	3.510557E−6	2.026715E−6	满足
17	OV1.F	4.914779E−6	1.982949E−6	满足
18	OV2.F	4.914779E−6	1.962658E−6	满足
19	BIT1.F	5.549034E−6	2.003266E−6	满足
20	BIT2.F	5.549034E−6	2.01197E−6	满足
21	OP.F	7.927191E−6	1.972644E−6	满足
22	SA.F	1.321198E−6	2.013274E−6	不满足
23	FCS_F	5.555556E−9	3.941847E−12	满足

下一步,我们计划将本文提出的方法应用到更多类别的安全关键 CPS 系统中,为研究人员和工程人员提供更多的分析和评估案例.我们也将把更多的安全性分析方法结合到安全性评估过程中,例如基于随机多人博弈理论的安全性分析方法[9],在早期设计阶段将外部威胁考虑在内.另外,当通过模型计算得到的失效概率不能满足分配的失效概率时,如何重新设计和优化 AADL 模型结构以满足安全性需求,是我们需要进一步研究的工作.此外,随着系统开发过程的推进,AADL 模型被不断细化,模型包含的信息越来越多,如参数连接等,针对系统开发后期更为详细的 AADL 模型,需要改进 AADL 模型失效概率分配方法.

References:

[1] Lee EA. Cyber physical systems: Design challenges. In: Proc. of the 11th IEEE Int'l Symp. on Object and Component-Oriented Real-Time Distributed Computing (ISORC). IEEE, 2008. 363−369.

[2] Yin L, Chen XH, Liu J. Consistency analysis of timing requirements for cyber-physical system. Ruan Jian Xue Bao/Journal of Software, 2014,25(2):400−418 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4540.htm [doi: 10.13328/j.cnki.jos.004540]

[3] Luo CX, Wang R, Guan Y, Li XJ, Shi ZP, Song XY. Integrated modeling method of CPS for real-time data. Ruan Jian Xue Bao/Journal of Software, 2019, 30(7):1966−1979 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5753.htm [doi: 10.13328/j.cnki.jos.005753]

[4] SAE Int'l. Guidelines for development of civil aircraft and systems. ARP 4754A, 2010.

[5] SAE Int'l. Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment. ARP 4761, 1996.

[6] SAE Int'l. (R) Architecture analysis and design language (AADL). AS5506C, 2017.

[7] Feiler PH, Gluch DP. Model-Based Engineering with AADL: An Introduction to the SAE Architecture Analysis & Design Language. Addison-Wesley, 2012.

[8] Zhou XS, Yang YL, Yang G. Modeling methods for dynamic behaviors of cyber-physical system. Chinese Journal of Computers, 2014,37(6):1411−1423 (in Chinese with English abstract).

[9] Wei XM, Dong YW, Sun PP, Xiao MR. Safety analysis of AADL models for grid cyber-physical systems via model checking of stochastic games. Electronics, 2019,8(2):212. [doi: 10.3390/electronics8020212]

[10] Dong YW, Wei XM, Xiao MR. Overview: System architecture virtual integration based on an AADL model. In: Proc. of the Symp. on Real-Time and Hybrid Systems. Cham: Springer, 2018. 105−115. [doi: 10.1007/978-3-030-01461-2_6]

[11] Carnegie mellon software engineering institute. In: Proc. of the Architecture Analysis and Design Language. 2019. http://www.aadl.info/aadl/currentsite/

[12] Gao KQ. The research of reliability allocation and evaluation of the harbinger system [MS. Thesis]. Nanjing: Nanjing University of Aeronautics and Astronautics, 2017 (in Chinese with English abstract).

[13] Song BW, Xu DM. On improving reliability of complex engineering system with an allocation method based on fuzzy theory. Journal of Northwestern Ploytechnical University, 1998,16(02):271−275 (in Chinese with English abstract).

[14] He X, Sun Y, Li Y. An improved AGREE method with reliability mathematical model for complex system importance degree computation. In: Proc. of the 2016 11th Int'l Conf. on Reliability, Maintainability and Safety. 2016. 1−7.

[15] Du GP, He LD, Fang JX, Zhang B. A modified AGREE reliability allocation method research in power converter. In: Proc. of the 2014 10th Int'l Conf. on Reliability, Maintainability and Safety. 2014. 522−525.

[16] Catelani M, Ciani L, Patrizi G, Venzi M. Reliability allocation procedures in complex redundant systems. IEEE Systems Journal, 2017,12(2):1182−1192. [doi: 10.1109/JSYST.2017.2651161]

[17] Si SB, Liu ML, Jiang ZY, Jin TD, Cai ZQ. System reliability allocation and optimization based on generalized birnbaum importance measure. IEEE Trans. on Reliability, 2019,68(3):1−13.

[18] Wei XM, Dong YW, Li XL, Wong EW. Architecture-Level hazard analysis using AADL. Journal of Systems and Software, 2018, 137:580−604. [doi: 10.1016/j.jss.2017.06.018]

[19] Wei XM, Dong YW, Yang MM, Hu N, Ye H. Hazard analysis for AADL model. In: Proc. of the 20th IEEE Int'l Conf. on Embedded and Real-Time Computing Systems and Applications. Chongqing, 2014. 1−10. [doi: 10.1109/RTCSA.2014.6910512]

[20] Zimmermann A. Stochastic Discrete Event Systems. Berlin Heidelberg New York: Springer-Verlag, 2007.

[21] Wei XM, Dong YW, Xiao MR. Safety-Based software reconfiguration method for integrated modular avionics systems in AADL model. In: Proc. of the IEEE Int'l Conf. on Software Quality, Reliability and Security Companion. 2018. 450−455. [doi: 10.1109/QRS-C.2018.00083]

[22] Wei XM, Dong YW, Ye H. QaSten: Integrating quantitative verification with safety analysis for AADL model. In: Proc. of the Int'l Symp. on Theoretical Aspects of Software Engineering. 2015. 103−110. [doi: 10.1109/TASE.2015.10]

[23] Baouya A, Mohamed OA, Bennouar D, Ouchani S. Safety analysis of train control system based on model-driven design methodology. Computers in Industry, 2019,105:1−16.

[24] Bao YX, Chen MS, Zhu Q, Wei TQ, Mallet F, Zhou TL. Quantitative performance evaluation of uncertainty-aware hybrid AADL designs using statistical model checking. IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems, 2017,36(12): 1989−2002. [doi: 10.1109/TCAD.2017.2681076]

[25] Dong YW, Wang GR, Zhang F, Gao L. Reliability analysis and assessment tool for AADL model. Ruan Jian Xue Bao/Journal of Software, 2011,22(6):1252−1266 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4014.htm [doi: 10.3724/SP.J.1001.2011.04014]

[26] Gu B, Dong YW, Wei XM. A qualitative safety analysis method for AADL model. In: Proc. of the 8th Int'l Conf. on Software Security and Reliability-Companion. IEEE, 2014. 213−217. [doi: 10.1109/SERE-C.2014.41]

[27] Liu YL, Shen GH, Huang ZQ, Yang ZB. Quantitative risk analysis of safety—Critical embedded systems. Software Quality Journal, 2017,25(2):503−527.

[28] Bozzano M, Bruintjes H, Cimatti A, Katoen JP, Noll T, Tonetta S. COMPASS 3.0. In: Proc. of the 25th Int'l Conf. on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2019). 2019. 379−385.

[29] Bozzano M, Cimatti A, Katoen JP, Nguyen VY, Noll T, Roveri M. Safety, dependability and performance analysis of extended AADL models. The Computer Journal, 2010,54(5):754−775. [doi: 10.1093/comjnl/bxq024]

[30] Julien D, Feiler PH, Gluch D, Hudak JJ. AADL fault modeling and analysis within an ARP4761 safety assessment. Technical Report, CMU/SEI-2014-TR-020, 2014.

[31] SAE Int'l. (R) SAE architecture analysis and design language (AADL) Annex Volume 1: Annex E: Error Model Annex. AS5506/1, 2006.

[32] Zimmermann A. Modelling and performance evaluation with TimeNET 4.4. In: Proc. of the 14th Int'l Conf. on Quantitative Evaluation of Systems. Cham: Springer-Verlag, 2017. 300−303.

[33] Wang LY, Cai F. Reliability analysis for flight control systems using probabilistic model checking. In: Proc. of the 8th IEEE Int'l Conf. on Software Engineering and Service Science. 2017. 161−164.

[34] The OSATE Website. http://osate.org/

[35] Zimmermann A, Knoke M. TIMENET 4.0: A Software Tool for the Performability Evaluation with Stochastic and Colored Petri Nets: User Manual. Technical Report, Technische Universität Berlin, 2007.

[36] Marsan MA, Chiola G. On Petri nets with deterministic and exponentially distributed firing times. In: Proc. of the European Workshop on Applications and Theory in Petri Nets. Berlin, Heidelberg: Springer-Verlag, 1986. 132−145.

[37] Marsan MA, Conte G, Balbo G. A class of generalized stochastic Petri nets for the performance evaluation of multiprocessor systems. ACM Trans. on Computer Systems, 1984,2(2):93−122.

附中文参考文献:

[2] 尹玲,陈小红,刘静.信息物理融合系统的时间需求一致性分析.软件学报,2014,25(2):400−418. http://www.jos.org.cn/1000-9825/4540.htm [doi: 10.13328/j.cnki.jos.004540]

[3] 罗晨霞,王瑞,关永,李晓娟,施智平,Song XY.面向实时数据的CPS一体化建模方法.软件学报,2019,30(7):1966−1979. http://www.jos.org.cn/1000-9825/5753.htm [doi: 10.13328/j.cnki.jos.005753]

[8] 周兴社,杨亚磊,杨刚.信息-物理融合系统动态行为模型构建方法.计算机学报,2014,37(6):1411−1423.

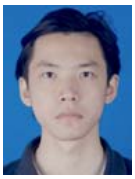
[12] 高坤奇.报信者系统的可靠性分配与评估问题研究[硕士学位论文].南京:南京航空航天大学,2017.

[13] 宋保维,徐德民.系统可靠性分配的模糊数学方法.西北工业大学学报,1998,16(02):271−275.

[25] 董云卫,王广仁,张凡,高磊.AADL 模型可靠性分析评估工具.软件学报,2011,22(6):1252−1266. http://www.jos.org.cn/1000-9825/4014.htm [doi: 10.3724/SP.J.1001.2011.04014]

魏晓敏(1990－),男,福建龙岩人,博士,CCF 学生会员,主要研究领域为系统安全,可信分析与验证.

肖明睿(1996－),男,硕士,主要研究领域为可信软件设计与验证.



董泽乾(1995－),男,硕士,主要研究领域为信息物理系统融合.

田聪(1981－),女,博士,教授,博士生导师,CCF 杰出会员,主要研究领域为形式化方法,时序逻辑,模型检测.