

一种嵌入式系统模型的安全性分析验证方法

石娇洁¹, 胡 军^{1,2}, 刘 雪¹, 马金晶¹, 黄志球¹, 程 桢¹

(1. 南京航空航天大学 计算机科学与技术学院, 江苏 南京 210016;

2. 南京大学 计算机软件新技术国家重点实验室, 江苏 南京 210093)

摘 要: 由于嵌入式系统模型设计周期越来越短, 功能越来越复杂, 其安全性分析与验证方法是近年来在安全攸关系统工程领域中出现的一个重要研究热点。针对这种情况, 文中提出一种基于模型驱动架构的面向 SysML/MARTE 状态机的系统安全性分析验证方法。具体包括: 构建了具备 SysML/MARTE 扩展语义的状态机元模型, 以及高级安全性建模与分析语言 AltaRica 的语义模型 GTS 的元模型, 然后建立了从 SysML/MARTE 状态机模型到 AltaRica 模型的语义映射模型转换规则, 并基于 AMMA 平台和故障树分析工具 XFTA 实现了对 SysML/MARTE 状态机的模型转换与系统安全性形式化验证框架的构建。最后给出了民用飞机系统中的机轮刹车系统设计模型的例子进行实例验证分析。实验结果表明, 提出的嵌入式系统设计模型的安全性分析与验证方法是具有代表性和可执行性的。

关键词: 系统安全性分析; 模型驱动; SysML/MARTE; XFTA; 状态机模型; 嵌入式系统模型

中图分类号: TP31

文献标识码: A

文章编号: 1673-629X(2015)10-0007-06

doi: 10.3969/j.issn.1673-629X.2015.10.002

A Verification Method of Security Analysis for Embedded System Model

SHI Jiao-jie¹, HU Jun^{1,2}, LIU Xue¹, MA Jin-jing¹, HUANG Zhi-qiu¹, CHENG Zhen¹

(1. College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics,
Nanjing 210016, China;

2. State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093, China)

Abstract: Because the design cycle of embedded system model is shorter and shorter, the function is more and more complex, in the field of safety critical systems engineering, its security analysis and verification method is an important research hotspot in recent years. In view of this, put forward a method based on model driven architecture for system security analysis verification, which is oriented SysML/MARTE state machine, including that constructed the state machine metamodel which has SysML/MARTE extension semantics, and the GTS metamodel which is the semantic model of AltaRica, high safety modeling and analysis language, then established semantic mapping model transformation rules from the SysML/MARTE state machine model to the AltaRica model, and based on the platform of AMMA and the fault tree analysis tools XFTA to realize the model transformation of SysML/MARTE state machine and the framework for system security formal verification. Finally give security verification example about wheel brake system design model. Experimental results show that the proposed verification method of security analysis for embedded system design model is representative and executive.

Key words: system safety analysis; model driven; SysML/MARTE; XFTA; state machine model; embedded system model

0 引 言

模型驱动工程 (Model Driven Engineering)^[1-4] 是近十年来在系统工程以及软件工程领域中出现的主流方法, 其基本思想是以系统模型设计、模型转换与分析/验证为工程的重要核心, 提高对复杂工程系统开发

与维护的能力和效率。与此同时, 建立基于模型的系统安全性分析方法并结合形式化方法进行验证也逐渐成为嵌入式安全攸关系统开发过程中的需求和重要挑战。例如, 在 2013 年最新版本的机载软件安全性适航标准 DO-178C 中, 已经正式提出了基于模型的系统

收稿日期: 2014-12-08

修回日期: 2015-03-11

网络出版时间: 2015-08-26

基金项目: 国家“973”重点基础研究发展计划项目 (2014CB744903); 回国留学人员科研启动基金 (2012); 611 航空科研基金 (2012); 南京航空航天大学青年科技创新基金 (NS2014098)

作者简介: 石娇洁 (1990-), 女, 硕士研究生, 研究方向为软件分析、模型检测; 胡 军, 副教授, CCF 会员, 研究方向为模型驱动的系统安全性分析、软件验证、嵌入式系统设计等; 黄志球, 教授, 博士生导师, 研究方向为软件工程。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20150826.1604.082.html>

开发和形式化方法分析的要求。

传统的嵌入式系统设计与开发中是由安全工程师来直接构造故障树、马尔可夫链等进行系统安全性分析,不足以应对近年来规模和复杂度迅速增长的嵌入式安全攸关系统的设计开发与升级维护的要求,需要在系统设计开发过程中尽可能采用统一的模型形式、建立有效的系统模型转换方法并结合形式化分析技术来提高系统安全性分析的效率^[5]。SysML^[6] (System Modeling Language)是目前系统工程应用开发的标准建模语言规范,支持包括对复杂嵌入式系统进行规约、设计和分析。MARTE^[7] (Modeling and Analysis of Real-Time Embedded)是主要提供了嵌入式系统中的时间约束、资源分配等非功能属性的建模与分析。通常这两者结合起来可以有效地描述嵌入式实时系统的功能行为。AltaRica 是一种以卫式转换系统为语义基础的进行系统安全行为建模与分析的语言及工具,已在航空电子设备系统架构安全评估中得到应用^[8]。

1 AltaRica 模型

基于模型的安全性分析 (Model-based Safety Analysis) 是近年来在实时嵌入式系统工程领域出现的重要研究方向,其基本思想是在系统设计过程中进行系统安全性分析时,首先建立包括系统功能行为和故障行为的模型,然后基于模型展开安全性分析与验证。AltaRica 就是一种基于形式化的卫式转换 (Guarded Transition System, GTS) 的安全性建模语言,可以用来对复杂安全攸关系统进行建模分析。

AltaRica 模型可以分为语法和语义两个层面。其中,语法层面的表示形式是将系统建模为具备层次结构的节点 (node) 集合,每个节点具有多个状态、事件、转换、输入/输出、数据变量等特征,其具体的行为使用类似于自动机的形式来表达。

AltaRica 在语义层面上是一个卫式转换系统的形式化模型^[9],其严格的定义为一个五元组 $\langle V, E, T, A, i \rangle$ 。其中, V 是一组变量,为一组状态变量 S 和流变量 F 的正交并集; E 是一组事件; T 是一组转换,每个转换是一个三元组 $\langle e, G, P \rangle$,其中, e 是 E 的一个事件, G 是一个建立在变量 V 上的布尔表达式, P 是一个建立在变量 V 上的操作。通常将转换 $\langle e, G, P \rangle$ 表示成 $e:G \rightarrow P$ 的形式。

AltaRica 的语法模型通过编译转换成 GTS 模型再转换成故障树模型,以及进一步构造相应的时序逻辑公式等后续分析工作。

当从 AltaRica 模型获得系统行为的故障树模型后,就可以进一步展开基于故障树安全性分析^[10]。文中采用一个基于 AltaRica 的开源分析工具 XFTA 来进

行分析。XFTA 是基于输入的故障树模型可以从 AltaRica 模型编译生成^[11]。输出的结果信息包括典型的最小割集分析,顶/基本事件概率重要度等。

2 系统安全性验证框架

本节给出基于 SysML/MARTE 模型转换的嵌入式系统设计的安全性验证框架。首先给出验证框架中总体上模型转换与验证的过程说明,然后是从 SysML/MARTE 状态机模型到 GTS 模型的转换方法,以及将 GTS 模型自动生成故障树并在 XFTA 下进行安全性验证的架构。

2.1 基于模型转换的安全性验证框架

图 1 给出了在 MDE 架构下文中所设计的基于 SysML/MARTE 模型转换的嵌入式系统设计安全性质的形式化验证框架。

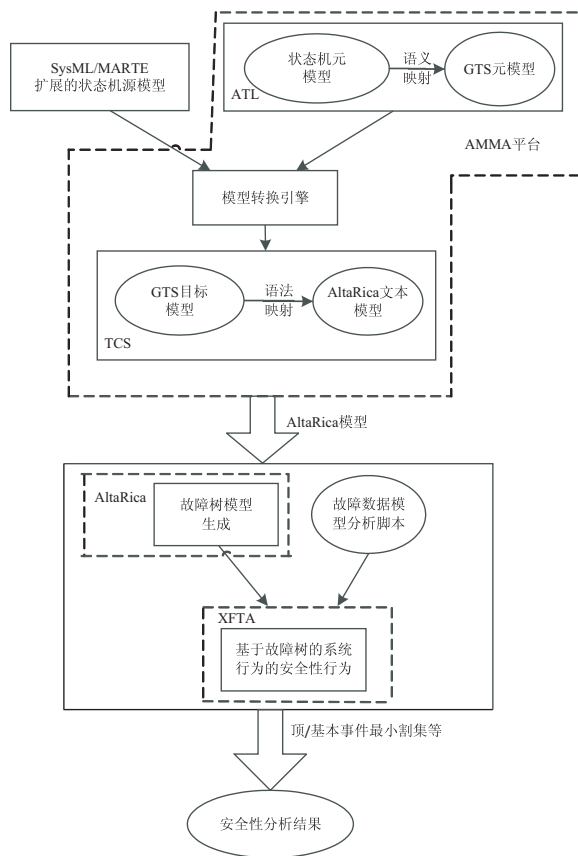


图 1 SysML 状态机图安全性验证框架

首先,使用扩展形式的 SysML/MARTE 状态机模型对嵌入式系统的故障行为进行建模,作为模型转换的源模型;与此同时构建扩展的状态机元模型与 GTS 元模型之间的语义映射规则。这样就可以通过 AMMA 平台的模型转换引擎将状态机源模型自动转换为 GTS 目标模型;然后通过 AMMA 平台中的 TCS^[12] 组件,从语法层面将 GTS 目标模型转换为 AltaRica 的文本模型。这样就可以使用 AltaRica 工具来自动构造与系统

故障行为相关的故障树模型。其次,为故障树分析编写脚本,将第一部分生成的故障树作为模型载入到 XFTA 中。运行 XFTA 工具,在命令行中运行脚本,对故障树进行相关分析,进而完成对系统的安全性验证。

2.2 扩展的 SysML/MARTE 状态机元模型

文中首先主要是采用 MARTE 中有关时间方面的建模元素来对 SysML 中的状态机模型进行扩展,并进一步构建其相应的元模型。由于 MARTE 自身的扩展机制是基于增加模型元素的注释来实现的,因此,可以采用同样的增加状态机模型中的注释的形式来进行扩展并建立元模型。

在 MARTE 库中定义了标准物理数据类型,如图 2 所示。其中有一个常见的抽象数据类型即 NFP_CommonType,它包含很多被其他所有物理类型所共享的可

选属性;expr 属性被 VSL_Expression 标记,当需要使用一个表达式指定的值,而不是一个文字值时被使用,但是表达式类型必须与属性类型匹配;在嵌入式系统中常用一些概率函数来赋值,表示成功或者失败的概率;source 属性被 SourceKind 枚举类型所标记,当需要指定数据项是如何获得时使用,其中 SourceKind 提供以下选项:est、meas、calc、req;ststQ 参数当值是一个统计量时使用,并且是用来进一步限定其本质的,ststQ 参数被 StatisticalQualifierKind 枚举类型所标记,它包含以下几种选择:max、min、mean 等值;dir 参数用来定性对比两个相同类型但不同值的数据,dir 参数被 DirectionKind 所标记,它定义了两种可能:incr (上升)和 decr (下降)。其中 incr 意味着高值代表高质量(如可靠性),然而 decr 意味着低值代表高质量(如故障率)。

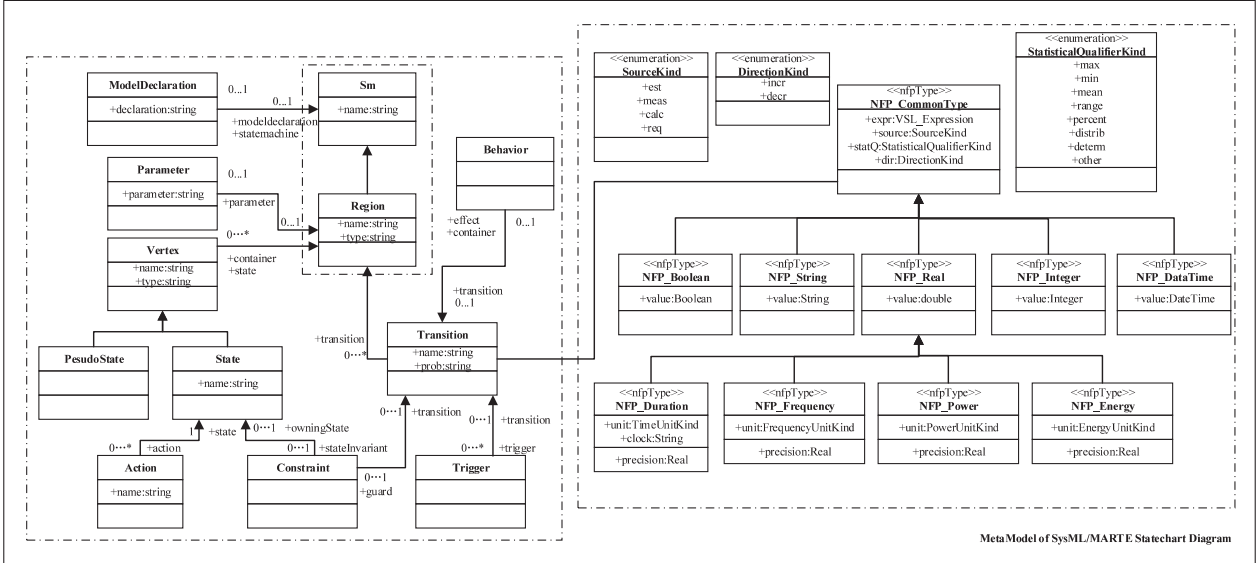


图 2 SysML/MARTE 扩展形式的状态机元模型

由上可知,概率函数在表达概率的过程中是十分重要的。尤其在某些情况下(如实时系统中),指明某一直是符合某一概率函数的概率是必不可少的。以下给出文中基于 SysML 规范中状态机中模型元素的定义以及 MARTE 中时间相关建模元素的分析所构建的 SysML/MARTE 扩展形式的状态机元模型(见图 2)。

这个元模型图逻辑上可分为两个部分,其一是 SysML 中的状态机元模型,其中:状态机图(State-Machine;Sm)由顶点(Vertex)、转换(Transition)、参数(Parameter)三部分组成。区域类(Region)包含状态机图所有的状态、状态分组以及状态属性;文中将由 MARTE 中的抽象物理数据类型附加到状态机图元模型的 Transition 的属性 prob 中,这样就能在 SysML 状态机图任何一个元素上添加概率信息。变迁有一定的约束条件,变迁发生会触发一些动作,还会发生一些行为,状态可以定义不变式,说明状态的约束条件。另一部分是 MARTE 中的概率相关的元模型,其中:NFP_

CommonType 代表常见的抽象数据类型,NFP_Boolean 表示 NFP 中的布尔数据类型,含有值 value,其类型为布尔型。文中主要用到 NFP_Real 这一数据类型,它表述其存储的数据类型为实数型,以它为父类,还可以衍生出 NFP_Energy(表示能源消耗)、NFP_Rrequency(表示频率)等数据类型。

2.3 SysML/MARTE 状态机与 GTS 的元模型转换

为了完成上述的模型转换与验证框架,需要建立 SysML/MARTE 状态机元模型与 GTS 元模型之间的语义映射;但是目前在 AltaRica 的相关材料中并没有提供 GTS 相应的元模型,因此本节根据 AltaRica 标准文档中模型元素的说明构建了一个包含其核心建模概念的 GTS 元模型架构(见图 3)。

在此架构中,一个 GTS 模型包含多个 Node(节点,即系统组件)以及与数据相关的 Domains 和 ConstantValues 等元素。其中:Domains 包含 Basic Domain 和 Compound Domain,基本域是指布尔型、整型或范围、枚

举等类型,复合域则表示结构、数组等类型;Node 模型元素中则包括了 Transition、Event、Parameter 以及 Variable 等。Transition 中包含卫式(Guard)、事件(Event)和一系列的赋值(Assignment);Sysc 用于定义 Node 之间的同步,Parameter 用于表示在状态前移过程中触发

可能事件所需的参数;Variable 包含 State Value(状态变量)和 Flow Value(流变量),其中状态变量的值只有在事件发生时才会改变,流变量是用来表示节点输入/输出接口上数据通信的共享变量。

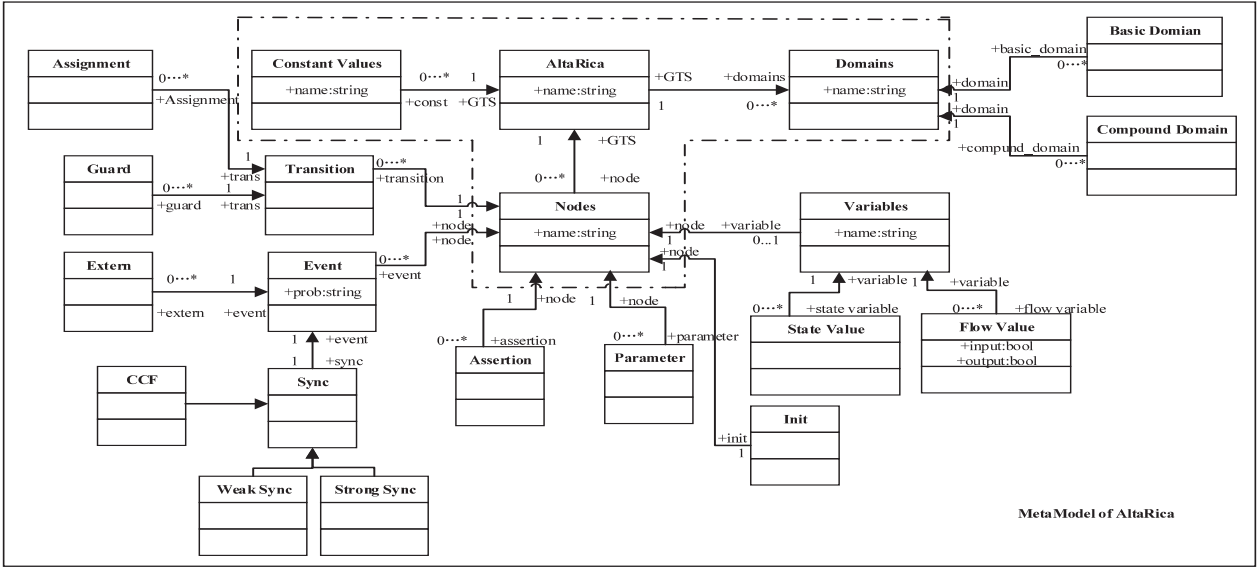


图 3 GTS 元模型

结合 2.2 节中构造的 SysML/MARTE 状态机的元模型及其语义信息,给出从 SysML/MARTE 状态机元模型到 GTS 元模型之间的语义映射规则。以下设定 S 为 SysML/MARTE 状态机的元模型, G 为 GTS 的元模型,二者之间的语义关系 Γ 即定义了从 S 到 G 的映射规则集合,表示为: $\Gamma(S) \mapsto G$ 。 Γ 的映射主要分为行为和基本类型结构两个方面的规则,如图 4 所示。

SysML/MARTE 状态机模型	GTS 模型元素
基本类型映射:	
$\Gamma(\text{Integer})$	GTS::Integer
$\Gamma(\text{String})$	GTS::String
$\Gamma(\text{Boolean})$	GTS::Boolean
$\Gamma(\text{DateTime})$	GTS::Integer
$\Gamma(\text{Real})$	Range
概率属性映射:	
$\Gamma(\text{NFP_CommonType})$	event.prob
同步&行为映射规则:	
$\Gamma(\text{Sync})$	GTS::Sync
$\Gamma(\text{Sm})$	GTS
$\Gamma(\text{Region Node})$	node
$\Gamma(\text{Transition.trigger})$	event
$\Gamma(\text{Transition})$	GTS::transition
$\Gamma(\text{InitialNode})$	init
$\Gamma(\text{Transition.guard})$	GTS::guard
$\Gamma(\text{state})$	statevalue
$\Gamma(\text{state.action})$	flowvalue

图 4 SysML/MARTE 状态机与 GTS 元素映射

映射规则简要说明如下:在行为映射中,一个 Sm 映射为一个 GTS;Region 包含状态机图中的所有定义和元素,映射到 Node;SysML/MARTE 状态机图中的 trigger 触发转移,而 GTS 的 Event 是触发转移的前提,

根据用途因此映射到 GTS 的 Event;状态机的 Transition 与 GTS 的 Transition 语义是相同的,故而映射;SysML/MARTE 状态机图中的初始状态是 InitialNode,直接映射到 GTS 中的初始状态 Init;SysML/MARTE 状态机图中的 guard 作为转移时必须满足的条件,与 GTS 上的 guard 语义相同,直接映射;状态机图中的状态(state),映射到 GTS 中的 statevalue,因为它是作为状态变量,表明系统中各个状态的变化;状态机图中的 action 与 GTS 的 flowvalue(表示系统中的数据流动)映射。在同步约束映射中, SysML/MARTE 状态机图中的 Sync 代表状态机中的同步, GTS 中的 Sync 表示各个状态转移的同步性,因此相互映射。在概率属性方面的映射中, SysML/MARTE 中的 NFP_CommonType 用于存储概率相关数据,因此映射到 GTS 事件中的 prob 属性上。此外,在基本类型结构映射中, SysML/MARTE 中支持 Integer、String、Boolean、DateTime、Real, GTS 的基本数据类型有 Integer、String、Boolean、Range, 根据语义可以直接将 Integer、String、Boolean 映射为 Integer、String、Boolean; DateTime 映射为 Integer; Real 映射为 Range,其中小数点前的数表明范围开始点,小数点后的数表明范围结束。

3 基于 AMMA 平台的模型转换与安全性验证方法实现

本节中首先给出了前述所设计的模型转换与安全

性验证框架在 AMMA 平台下的具体实现方法,然后给出了一个简要的示例说明。

3.1 基于 AMMA 平台的模型转换方法的实现

基于 AMMA 平台实现模型之间的语义映射过程实质上是通过 ATL 语言定义 ATL 转换规则的过程。通过 ATL 中的命令式指令来声明源模型 (SysML/MARTE 状态机模型) 和目标模型 (GTS 模型) 之间的元素关系,然后通过 ATL 虚拟机的执行将源模型转换为目标模型。在 AMMA 平台中定义的 SysML/MARTE 状态机元模型与 GTS 元模型,通过 ATL 虚拟机对转换规则的执行,就可以将 SysML/MARTE 状态机源模型转换成 GTS 目标模型。

3.2 实例说明

以下给出了一个机轮刹车系统的简单实例说明。机轮刹车系统 (Wheel Brake System, WBS) 安装在两个主起落架上,主要是通过对主轮制动达到飞机安全停止的目的。刹车系统控制组件 (Brake System Control Unit, BSCU) 是 WBS 的关键组件,会对其重点介绍。

地面刹车可以通过刹车踏板脚蹬进行人工控制,也可以在没有刹车踏板脚蹬输入的情况下通过自动刹车进行控制。该型飞机的八个主轮均采用多片式碳刹车。每一个刹车都由两套相互独立的液压系统来控制。一套是绿色液压系统,在正常模式下为主用刹车系统提供液压源;另一套是蓝色液压系统,为备用刹车系统提供液压源。当绿色液压供应系统本身出现损失或 BSCU 的移动存在故障时,自动选择器就会启用备用刹车系统。

在正常模式下,刹车踏板脚蹬的位置会通过电信号反馈到刹车系统控制计算机中,然后转换成相应的控制信号输出给刹车。为了满足可用性与集成性要求,该飞机起落架 BSCU 由两套完全独立的 BSCU 组成,称为 BSCU₁ 和 BSCU₂,各 BSCU 包含独立的检测通道。在正常情况下,BSCU₁ 系统提供刹车与防滑指令给机轮刹车系统。当 BSCU₁ 系统通过它的系统有效性监控器发现存在故障时,将会自动切换到 BSCU₂ 系统来输出控制指令。如果 BSCU₂ 随后也发生故障,那么所有的 BSCU 输出将失效,BSCU 有效性监控器也将失效。

首先利用建模工具 Rhapsody^[13] 给出机轮刹车系统部分的 SysML/MARTE 状态机模型。根据 2.1 节所建立的模型转换框架进行模型转换。当得到目标 GTS 模型后,则可以继续通过 AltaRica^[14] 工具获得系统故障树模型,进而得到 XFTA 的输入文件。

从生成的 GTS 模型中可以看出 WBS (见图 5) 包括选择阀、隔离阀、BSCUs 和刹车踏板脚蹬四个子节点。其中 BSCU 主要是对刹车系统控制组件进行简单

的描述。BSCUs 主要是声明了两个 BSCU 子节点,本系统用的是两个 BSCU。isoValve 描述的是隔离阀的功能,隔离阀与蓝色和绿色液压泵相连接,当隔离阀处于工作状态时,若没有 pressure,则无输出,若给其一个 presser,那么就会有信号输出。pedal 描述的是刹车踏板脚蹬的功能,当给踏板脚蹬一个刹车动作时,踏板脚蹬就处于工作状态,同时有刹车信号输出。sigbrake 代表刹车信号。selectValve 主要描述的是选择阀的功能。选择阀用于选择在什么情况下由正常刹车系统转换至备用刹车系统。比如当正常刹车系统本身失效,或者绿色液压泵出现故障或 BSCU 也出现故障时,就会由正常刹车系统转换到备用刹车系统。由于篇幅有限,文中只展示该模型中最核心的一个节点:WBS 节点。

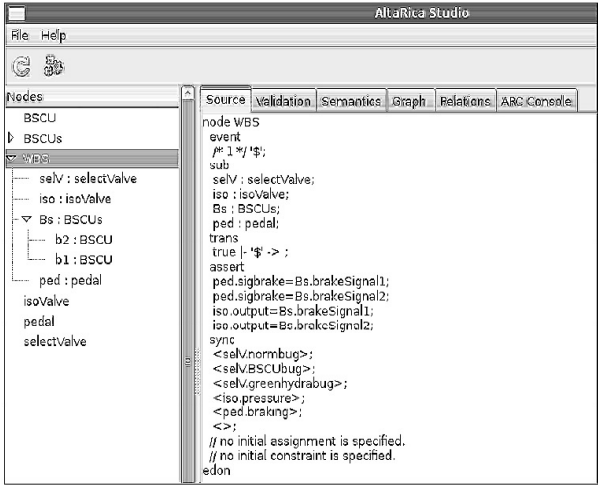


图 5 WBS 节点

经过 AltaRica 工具转换后得到故障树模型,编写执行脚本,利用 XFTA 对获取的故障树模型进行分析。

top-event	mission-time	probability				
LossOfBrakingCommands	0	2.5826e-008				
Basic-event	occurrences	Pr	MIF	CIF	DIF	
ValidityMonitorFailure	0	0	0	0	0	
MonitorSystemEnergy	1	0.02	8e-008	0.0619531	0.080714	
ErrorEnergyDataOfSystem	1	8e-008	0.02	0.0619531	0.0619531	
FailureOfSystemHardware	2	0.02	1.2113e-006	0.938047	0.939286	
ErrorChannelDesignOfSystem	0	0	0	0	0	
ErrorDataOfSystemCPUHardwareFailure	1	3.13e-008	0.02	0.0242391	0.0242392	
ErrorDataOfSystemCPUDesignFailure	0	0	0	0	0	
ErrorDataOfSystemI/OFailure	1	1.18e-006	0.02	0.913808	0.913808	
PerceptibleErrorOfSystem2	0	0.0004	0	0	0.0004	
SwitchError	0	0.0148	0	0	0.0148	

图 6 故障树分析结果

XFTA 执行脚本,部分分析结果如图 6 所示。文件前两行为顶事件的名称,任务时间和概率的事件,每个基本事件的重要因素与表格打印出来分开。每一行包含有以下数据,基本事件的名称,在最小割集中基本事件出现的次数 (occurrences),基本事件的概率 (Pr),基本事件的边际重要度 (MIF),基本事件的关键重要度 (CIF),基本事件的诊断重要度 (DIF),基本事件的风险成就价值 (RAW),基本事件的减少风险价值 (RRW)。因此,可以看出,事件 MonitorSystemEnergy

在最小割集中出现 0 次, $Pr=0.02$, $MIF=8e-008$, $CIF=0.061\ 953\ 1$, $DIF=0.080\ 714$, $RAW=4.035\ 7$, $RRW=1.066\ 04$ 。

4 结束语

与文中相关的研究工作可以分为如下三个方面:

第一类工作表明了 UML/SysML 与 MARTE 的结合使用能够有效地对复杂嵌入式系统的设计进行建模分析;如:文献[15]研究了将 UML 图结合 MARTE 转换成价格时间自动机并进行验证的方法;文献[16]设计了将 UML/MARTE 模型向 FIACRE 形式模型的转换框架,这些转换也是建立在 AMMA 平台上利用 ATL 和 TCS 来完成;文献[17]研究了基于 MDE 的实时系统 UML 模型到形式化模型的模型转换,并进一步进行系统安全性质的形式化证明。

第二类工作是与安全性建模和分析语言 AltaRica 相关的。

第三类相关研究工作是模型驱动工程与形式化方法相结合。

文中提出了一种基于模型驱动架构的面向 SysML/MARTE 状态机的系统安全性验证方法,具体包括:构建具备 SysML/MARTE 扩展语义的状态机元模型及安全性建模与分析语言 AltaRica 的语义模型 GTS 的元模型,然后建立了 SysML/MARTE 状态机模型分别到时间自动机模型以及 AltaRica 模型的语义映射模型转换规则,并基于 AMMA 平台和故障树分析工具 XFTA 设计实现了对 SysML/MARTE 状态机的模型转换与系统安全性形式化验证的框架。在接下来进一步的工作中,将对具有并发结构的状态机模型的语义转换展开研究,并结合实际工程中某机载航电系统的安全性分析需求对文中方法进行实际应用验证。

参考文献:

- [1] Roudier Y, Idrees M S, Apvrille L. Towards the model-driven engineering of security requirements for embedded systems [C]//Proc of international workshop on model-driven requirements engineering. Rio de Janeiro:IEEE,2013:55-64.
- [2] Hutchinson J, Rouncefield M, Whittle J. Model-driven engineering practices in industry [C]//Proc of 33rd international conference on software engineering. Waikiki, Honolulu:ACM, 2011:633-642.
- [3] Hästbacka D, Vepsäläinen T M A, Kuikka S. Model-driven development of industrial process control applications [J]. Journal of Systems and Software,2011,84(7):1100-1113.
- [4] 沙 静,杜玉越. 模型驱动工程在分布式实时嵌入式系统 QoS 评价中的应用 [J]. 计算机应用,2009,29(S1):265-268.
- [5] Reif W. Model based safety analysis [C]//Proc of dependable control of discrete systems. [s. l.]:[s. n.],2009.
- [6] 蒋彩云,王维平,李 群. SysML:一种新的系统建模语言 [J]. 系统仿真学报,2006,18(6):1483-1487.
- [7] 许海洋,王 萍. 基于 MDA 的 MARTE 模型形式化方法 [J]. 计算机应用研究,2012,29(8):3018-3021.
- [8] Bieber P, Bougnol C, Castel C, et al. Safety assessment with Altarica-lessons learnt based on two aircraft system studies [C]//Proc of 18th IFIP world computer congress. [s. l.]:[s. n.],2004.
- [9] Rauzy A B. Guarded transition systems:a new states/events formalism for reliability studies [J]. Journal of Risk and Reliability,2008,222(4):495-505.
- [10] 刘 磊. 软件时序故障树建模与分析技术研究 [D]. 长沙:国防科学技术大学,2011.
- [11] Rauzy A. An open-PSA fault tree engine [EB/OL]. 2011-11-15. <http://www.lix.polytechnique.fr/~rauzy/xfta/xfta.htm>.
- [12] Ruscio D D, Iovino L, Pierantonio A. Managing the coupled evolution of metamodels and textual concrete syntax specifications [C]//Proc of 39th EUROMICRO conference on software engineering and advanced applications. [s. l.]:IEEE,2013:114-121.
- [13] Harel D, Kugler H. The rhapsody semantics of statecharts (or, on the executable core of the UML) [C]//Proc of LNCS. [s. l.]:[s. n.],2004:325-354.
- [14] Rauzy A. AltaRica download [EB/OL]. 2014-11-13. <http://www.eclipse.org/m2m/atl/http://altarica.labri.fr/pub/tools/packages/current/arc-current.tar.gz>.
- [15] 刘 磊. 在 MDA 中基于元模型的模型转换方法研究 [D]. 昆明:昆明理工大学,2010.
- [16] 张 天,Frédéric JOUAULT,Christian ATTIOGBE,等. 基于 MDE 的异构模型转换:从 MARTE 模型到 FIACRE 模型 [J]. 软件学报,2009,20(2):214-233.
- [17] 刘亚萍. 基于 MDE 的 UML 模型到形式化模型的转换方法研究 [D]. 南京:南京航空航天大学,2009.

一种嵌入式系统模型的安全性分析验证方法

作者：

石娇洁，胡军，刘雪，马金晶，黄志球，程桢，[SHI Jiao-jie](#)，[HU Jun](#)，[LIU Xue](#)，[MA Jin-jing](#)，[HUANG Zhi-qiu](#)，[CHENG Zhen](#)

作者单位：

石娇洁,刘雪,马金晶,黄志球,程桢,[SHI Jiao-jie](#),[LIU Xue](#),[MA Jin-jing](#),[HUANG Zhi-qiu](#),[CHENG Zhen](#)([南京航空航天大学 计算机科学与技术学院, 江苏 南京, 210016](#))，[胡军](#),[HU Jun](#)([南京航空航天大学 计算机科学与技术学院, 江苏 南京 210016](#); [南京大学 计算机软件新技术国家重点实验室, 江苏 南京 210093](#))

刊名：

计算机技术与发展

ISTIC

英文刊名：

[Computer Technology and Development](#)

年，卷(期)：

2015(10)

引用本文格式：[石娇洁](#).[胡军](#).[刘雪](#).[马金晶](#).[黄志球](#).[程桢](#).[SHI Jiao-jie](#).[HU Jun](#).[LIU Xue](#).[MA Jin-jing](#).[HUANG Zhi-qiu](#).[CHENG Zhen](#) 一种嵌入式系统模型的安全性分析验证方法[期刊论文]-[计算机技术与发展](#) 2015(10)