一种基于四变量模型的系统安全性建模与分析方法

胡 军[1,2] 石娇洁[1] 程 桢[1] 陈 松[1] 王明明[1]
(南京航空航天大学计算机科学与技术学院 南京 211106)[1]
(南京大学计算机软件新技术国家重点实验室 南京 210093)[2]

摘 要 近年来,基于模型的系统安全性分析与验证方法是安全关键系统工程领域中的一个重要研究方向。提出了一种基于四变量模型的系统安全性建模与分析验证方法,该方法利用 AltaRica 建模语言对系统进行建模。通过对四变量模型及 AltaRica 进行语义研究构建二者之间的映射规则,以民用飞机中机轮刹车系统(Wheel Brake System, WBS)为例来说明整个验证过程,即首先利用四变量模型从系统的需求层次上对 WBS 进行需求分析并根据映射关系构建 AltaRica 模型,接着利用故障树分析方法对 WBS 进行安全性研究,最后基于 AltaRica 配套工具 ARC 对系统的安全性属性进行验证。验证结果表明了该方法在系统安全工程领域中的实用性。

关键词 四变量模型,AltaRica 建模语言,故障树分析,ARC
中图法分类号 TP316.2 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.11.038

System Safety Modeling and Analysis Method Based on Four-variable Model

HU Jun[1,2] SHI Jiao-jie[1] CHENG Zhen[1] CHEN Song[1] WANG Ming-ming[1]
(Department of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China)[1]
(State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093, China)[2]

Abstract Recently, the system safety analysis and verification method based on model is an important research direction in the field of safety critical systems engineering. A system safety modeling and analysis verification method based on four-variable model was proposed based on the AltaRica modeling language. The mapping rule between four-variable model and AltaRica was constructed through the studying of their semantics. A case of wheel brake system(WBS) in civil aircraft was used as an example to illustrate the entire validation process. Namely, first we used four-variable model to analyze the requirements of WBS from the level of system requirements, and constructed the AltaRica model according to the mapping rule. Next, we used fault tree analysis method to study the safety of WBS. Finally, based on the tool ARC, which is associated with AltaRica, the system safety attributes was validated. The practicability of the proposed method in the field of system safety engineering is illustrated by the verification results.

Keywords Four-variable model, AltaRica modeling language, Fault tree analysis, ARC

1 引言

基于模型的系统安全性分析验证[1-3]在安全关键系统工程领域中占据重要位置,具备一套完整的工具框架,包括支持系统模型的形式化规范、形式化需求以及自动化验证等功能。模型开发过程中,为更方便地进行安全性分析与自动化验证工作,将系统正常行为与故障行为相结合构成扩展系统模型。而基于系统需求分析的安全性建模与分析验证方法是在对系统进行需求分析的前提下构建模型,该方法在安全关键系统工程领域中具备安全性和可靠性的特点。

传统风险建模形式包括故障树、马尔科夫链等,这些建模形式均存在一个共性问题,即模型与所研究的系统规范相差甚远,结果导致模型很难被设计并维持在系统的整个生命周期。AltaRica 建模语言[4-6]是一种适用于安全性分析的高级建模语言,由具有层次结构的可重用组件构成,每个组件都与图形化表示法相关联,使得模型与系统设计框架更加接近。AltaRica 设计模型在考虑系统故障行为的同时,可更好地反映系统功能和物理架构,以便更方便地进行系统安全性分析。

四变量模型[7,8]是由 Parns 和 Madey 等人在早期研究 A-7 飞机需求规范的过程共同提出,其主要思想是在系统需求层次上利用四变量模型的 4 类变量和 4 类关系分析确定系统行为需求及软件需求。利用四变量模型对系统进行需求分析的同时,结合 SCR(Software Cost Reduction)结构及 SCR 表对系统进行分析描述,从而使系统设计更加清晰完整。

到稿日期:2015-10-20 返修日期:2016-03-04 本文受国家重点基础研究发展计划(973 计划)(2014CB744903),南京航空航天大学青年科技创新基金(NS2014098)资助。

胡 军(1973—),男,副教授,CCF 会员,主要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,E-mail:hujun.nju@139.com;**石娇洁**(1990—),女,硕士生,主要研究方向为软件分析、模型检测,E-mail:shijiaojiexzs@163.com;**程 桢**(1990—),男,硕士生,主要研究方向为软件分析、模型检测;**陈 松**(1991—),男,硕士生,主要研究方向为软件分析、模型检测;**王明明**(1991—),男,硕士生,主要研究方向为软件分析、模型检测。

本文提出了一种基于四变量模型的系统安全性建模与分析方法，即在系统需求层面采用四变量模型的分析方法，在系统设计层面采用 AltaRica 的设计模型，并建立需求与设计两个层面模型之间的语义规则，从而更加有效地实施基于模型的系统安全性分析。本文第 2 节简要介绍四变量模型的基本结构及 AltaRica 建模语言的语法特征；第 3 节在分析研究四变量模型及 AltaRica 语义的基础上，构建二者之间的映射规则，并给出具体分析过程；第 4 节以民用飞机中机轮刹车系统(WBS)为例说明整个模型的构建及验证过程，包括对 WBS 构建四变量模型，根据所构建的四变量模型及映射规则实现 AltaRica 模型设计，利用故障树分析方法对模型进行故障分析并利用配套工具 ARC 对安全性属性进行验证，最后展示验证结果；最后总结全文。

2 四变量模型与 AltaRica

2.1 四变量模型

四变量模型是在系统需求层次上描述所需的系统行为及软件行为，包括系统与外界的交互行为以及系统内部的状态、模式变化的行为特征描述等[9,10]。

许多安全关键相关的应用可对物理过程进行控制，这些应用包括航空电子设备、医疗设备、核反应堆等，四变量模型可用于分析这些应用中各部件的行为需求，包括具体的系统行为及软件行为等，其形式如图 1 所示。

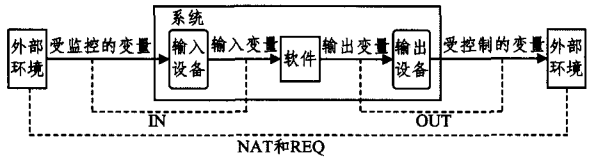

图 1 四变量模型

四变量模型主要由 4 个变量及变量之间的关系构成。

(1)受监控的变量(Monitored Variables，MV)：系统观察到并对系统行为做出回应的变量；

(2)受控制的变量(Controlled Variables，CV)：系统用于控制外部环境做出变化的变量；

(3)输入变量(Input Variables，IV)：软件读入的变量，该变量由输入设备将 *MV* 转化所得；

(4)输出变量(Output Variables，OV)：软件读出的变量，该变量经输出设备转化后得到 *CV*；

(5)*NAT*：定义系统环境中的自然约束，如飞机最大爬升率；

(6)*REQ*：定义系统需求，指明当 *MV* 发生变化时，*CV* 如何相应地发生变化；

(7)*IN*：定义 *MV* 与 *IV* 之间的关系；

(8)*OUT*：定义 *OV* 与 *CV* 之间的关系。

在四变量模型中，系统软件行为通过关系 *REQ*，*NAT*，*IN* 和 *OUT* 进行描述。具体来说，*NAT* 描述的是在不考虑系统本身内部结构以及系统行为的情况下系统中所存在的环境行为，而 *REQ* 描述的是系统环境如何被系统本身所约束。在四变量模型中用关系 *IN* 和 *OUT* 描述围绕在软件周围的硬件接口，主要反映了受监控的变量与输入变量、输出变量与受控制的变量之间的映射关系，同时也反映出了输入变量和输出变量分别与系统软件之间的交互过程。

与此同时，可使用另外 4 种结构以更加实际和简明的方式对四变量模型进行描述，分别是模式(mode)、项(term)、条件(condition)和事件(event)，将这 4 种结构称为 SCR(Software Cost Reduction)结构。其中，模式类是定义在 *MV* 上的状态机，状态机中的状态称为系统模式，状态转换由事件触发；项定义在 *IV*、模式或其他项上，用于描述某个场景；条件是定义在系统中某实体上的断言；实体值的变化由事件触发来完成。

SCR 表格定义在 SCR 结构上，包括条件表、事件表和模式转换表。条件表将 *OV* 或项描述为模式和条件之间的一种函数映射；事件表将 *OV* 或项描述为模式和事件之间的一种函数映射；模式转换表将系统模式描述为模式和事件之间的一种函数映射[11]。

表 1 是条件表的具体表现形式，共有 $n+1$ 行和 $p+1$ 列。条件表将输出变量或项 r_i 描述为关系 ρ_i，关系 ρ_i 定义在模式、条件和值上。简单来说，$\rho_i=\{(m_j,c_{j,k},v_k)\in M_{\mu(i)}\times C_i\times TY(r_i)\}$，其中 C_i 是一组条件集，TY 是某实体值与其合法值之间的映射。关系 ρ_i 必须满足如下 4 个属性：

(1)m_j 和 v_k 必须具备唯一性。

(2)$\bigcup_{j=1}^{n} m_j=M_{\mu(i)}$(必须包含模式类中的所有模式)。

(3)覆盖性，即每列所有条件组成的析取表达式总为 true。

(4)不相交性，即每列中的条件两两相交，交集必为空集。

表 1 条件表的具体表现形式

Modes	Conditions			
m_1	$c_{1,1}$	$c_{1,2}$	…	$c_{1,p}$
m_2	$c_{2,1}$	$c_{2,2}$	…	$c_{2,p}$
…	…	…	…	…
m_n	$C_{n,1}$	$C_{n,2}$	…	$C_{n,p}$
r_i	v_1	v_2	…	v_p

2.2 AltaRica 建模语言

AltaRica 是一种适用于安全性分析的高级建模语言，除系统功能外，主要针对系统安全性进行建模。本质上 AltaRica 是一种用于描述约束自动机的建模语言[12]，具有一定的层次性：每个组件都描述为一种约束自动机，组件与组件间通过同步机制实现结合。AltaRica 模型的基本特征总结如下：1)该语言具有层次性，利用事件(event)实现同步；2)事件间具有优先级；3)变量分为两大类(即状态变量和流变量)，状态变量位于组件内部，流变量的变化依赖于状态变量，描述组件接口；4)可通过变量实现自动机中存在的某些约束关系。

AltaRica 结点(node)是系统中的某个组件。结点与环境交互的接口分为两部分：事件和流变量。事件代表环境或组件本身的行为，事实上，任何现象的发生都会改变组件状态。流变量作为共享变量实现结点内部与外部的信息交互。结点中对状态变量和流变量的值分配称为一种组态(configuration)。利用转换(transitions)来描述基于事件的状态变量的变化。流变量和状态变量之间的关系描述通过断言(assertion)实现，可用于描述流变量与流变量、流变量与状态变量之间的关系，结点中的断言是由变量所构成的布尔公式，一个结点中的所有组态必须满足指定的断言。

3 基于四变量模型的系统安全性建模与分析

四变量模型主要用于描述所需的系统行为及软件行为，AltaRica 从功能设计方面对系统进行建模。本文提出的系统安全性建模与分析方法是在四变量模型的基础上利用 AltaRica 建模语言进行安全性建模及分析验证，由此需要建立二者模型元素的语义映射规则，从而实现从四变量需求模型

到 AltaRica 模型的安全性设计并进行分析验证。本节给出四变量模型与 AltaRica 模型的形式化定义，在此基础上构建二者间的映射规则。

3.1 四变量模型的形式化定义

由四变量构建的需求模型定义了一种特殊函数 TY，TY 指实体与其合法值之间的映射。需求模型在实体的基础上定义了系统状态，在系统状态的基础上又定义了条件，输入事件用于改变输入变量以便触发产生一个新的系统状态。

3.1.1 系统状态

假定存在如下集合：

MS 是 N 个非空且两两不相交的集合相结合而构成的，即 $M_1, M_2, \cdots, M_N$，称为模式类。模式类中每个成员都称为模式。

TS 是数据类型集，每个类型是值的非空集。

$VS = MS \cup TS$，是实体值集。

RF 是实体名集合，可分为 4 个子集：MR，模式类的名称集；IR，输入变量的名称集；OR，输出变量的名称集；GR，项的名称集。对于所有的 $r \in RF$，$TY(r) \subseteq VS$ 是实体名 r 的所属类型，对于所有的 $r \in MR$，存在 i 满足 $TY(r) = Mi$，那么称 r 为 Mi 的模式类名称。

系统状态是关于 RF 中的每个实体名到具体值之间映射的函数，更详细地，对所有的 $r \in RF$：$s(r) = v, v = TY(r)$。因此，通过假设，系统中任何一个状态 s 都对应于模式类中的某一模式，且每个实体都拥有唯一值。

3.1.2 条件

简单条件可以是 true，false 或一条逻辑语句 $r \odot v$，其中 $r \in RF$ 是一个实体名，$\odot \in \{=, \neq, >, <, \geqslant, \leqslant\}$ 是关系操作符，$v \in TY(r)$ 是常量值。条件是通过逻辑连接符 $\wedge$，$\vee$ 和 $\neg$ 将简单条件连接组成的逻辑语句。

3.1.3 事件

"@T"代表不同事件。原始事件表示为 $@T(r = v)$，r 是 RF 中的一个实体，$v \in TY(r)$。输入事件表示为 $@T(r = v)$，$r \in IR$ 是输入变量。基本事件表示为 $@T(c)$，c 是任意一个简单条件。简单条件事件表示为 $@T(c)$ WHEN d，$@T(c)$ 是基本事件，d 是简单条件或简单条件间的连接。任何一个基本事件 $@T(c)$ 可表示为简单条件事件 $@T(c)$ WHEN true。条件事件 e 是由逻辑操作符 $\wedge$ 和 $\vee$ 将简单条件事件连接组合而成。

3.2 AltaRica 形式化定义

AltaRica 是一种用于描述约束自动机的建模语言，其中约束自动机是一个元组集 $A = (D, S, F, E, T, A, I)$[13]，其中：$D$ 是一个有限或无限域；S 和 F 是两个变量集（称为状态变量和流变量），并且 $S \cap F = \emptyset$；E 是事件集；T 是转换集，转换是元组集 (g, e, a)，其中 $g(g \subseteq D^{|S \cup F|})$ 是基于 $S \cup F$ 的一种约束，称为该转换的卫士（guard），$e \in E$ 且 a 是后继状态的一种映射：$a: D^{|S \cup F|} \rightarrow D^{|S|}$；$A \subseteq D^{|S \cup F|}$ 是定义在变量值上的某种断言（assertion）；$I \subseteq D^{|S \cup F|}$ 定义了自动机中的初始（init）状态集。

3.3 四变量模型与 AltaRica 之间的映射

结合四变量模型与 AltaRica 各自的形式化定义，令四变量模型用 M 表示，AltaRica 模型用 N 表示，那么分别从四变量模型的 4 个变量及 4 个关系方面构建二者间的映射规则。图 2 是从四变量需求分析建模到 AltaRica 设计建模，然后进行安全性分析的流程图。

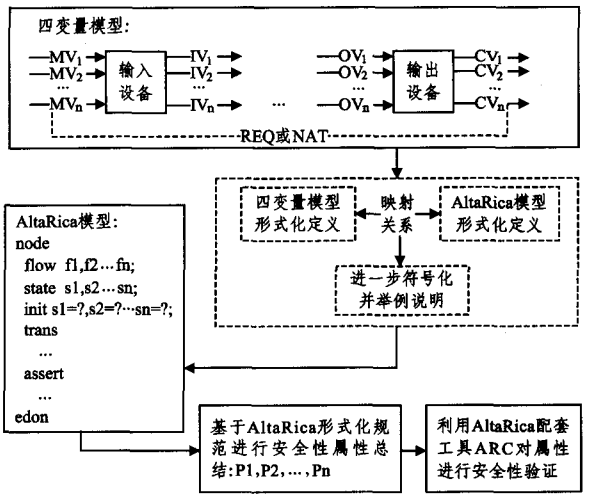

图 2 流程图

3.3.1 MV 和 CV 与 AltaRica 之间的映射

四变量模型中的 MV 和 CV 可看作是与外界环境交互的接口，通过 MV 和 CV 实现系统内部与外部间信息的传递，MV 是输入流，CV 是输出流，这一特点与 AltaRica 中的流变量一致，而流变量也可分为输入流（in）和输出流（out）。

考虑到一个四变量模型中 MV 和 CV 有多个，分别将其用两个集合表示，即 $MV = \{mv_1, mv_2, \cdots, mv_n\}$，$CV = \{cv_1, cv_2, \cdots, cv_n\}$。AltaRica 中，流变量用 F 表示，则 $F = \{f_1, f_2, \cdots, f_n\}$，其中，$f_i$ 具有 in 和 out 两种属性。那么，MV 和 CV 分别与 F 的对应关系如下：

$M: MV.mv_i \leftrightarrow N: F.f_i: \text{in}$

$M: CV.cv_i \leftrightarrow N: F.f_i: \text{out}$

以飞机中地形跟踪系统为例，飞机距地面高度始终保持一个固定值 $HEIGHT$，飞机的飞行速度（speed）、距离地面的实际高度（ActHeight）以及雷达测出的地面地形变化（RadarInfo）等信息输送到地形跟踪系统后，经一系列判断计算输出飞机垂直加速度（VertAccel）信息。其中，MV 包括 $speed$，$ActHeight$，$RadarInfo$；CV 包括 $VertAccel$。就 AltaRica 来说，流变量可定义为 $flow\ speed$：in；$ActHeight$：in；$RadarInfo$：in；$VertAccel$：out。图 3 详细给出了 MV 和 CV 与 $AltaRica$ 间的映射过程。

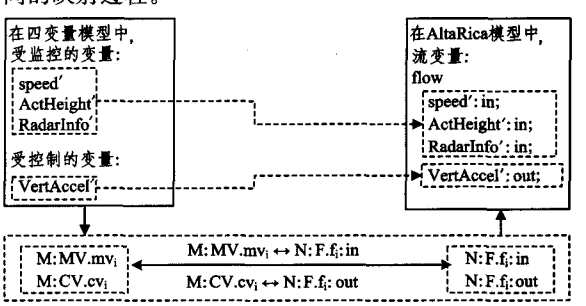

图 3 MV 和 CV 与 AltaRica 间的映射过程

3.3.2 IV 和 OV 与 AltaRica 之间的映射

IV 和 OV 在四变量模型中作为系统内部数据进行处理，根据 IV 和 OV 间的变化描述系统软件行为。在 AltaRica 中，结点内部工作模式完全由状态变量的变化来描述。基于该特点可将二者对应起来。

同样，考虑到 IV 和 OV 不止一个，分别用集合表示，那么 $IV = \{iv_1, iv_2, \cdots, iv_n\}$，$OV = \{ov_1, ov_2, \cdots, ov_n\}$。在 AltaRica 中，将状态变量用 $S = \{s_1, s_2, \cdots, s_n\}$ 表示，其中，s_i 分为输入流

in 和输出流 out。那么 IV 和 OV 与 S 之间的对应关系可表示为：

$M:IV.iv_i \leftrightarrow N:S.s_i:\text{in}$

$M:OV.ov_i \leftrightarrow N:S.s_i:\text{out}$

在地形跟踪系统中，飞行速度、实际高度以及雷达信息传送到系统后，会经过输入设备进行进一步处理，处理后的数据信息再传送至软件中心进行相关计算，并将计算后的飞机垂直加速度数据输出。假定用 $speed'$，$ActHeight'$ 和 $RadarInfo'$ 表示经输入设备处理后的数据，那么这些数据信息在四变量模型中即为输入变量，经计算产生的输出变量用 $VertAccel'$ 表示。在 AltaRica 模型中，对应的状态变量定义为 $state\ speed'$：in；$ActHeight'$：in；$RadarInfo'$：in；$VertAccel'$：out。图 4 示出了 IV 和 OV 与 AltaRica 间的映射过程。

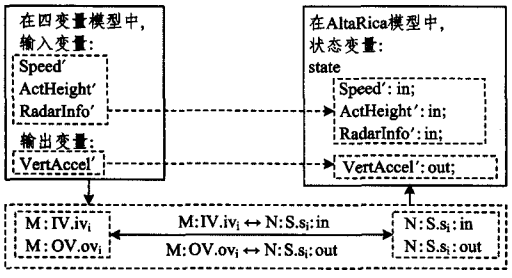

图 4　IV 和 OV 与 AltaRica 间的映射过程

3.3.3　关系 NAT 与 AltaRica 之间的映射

关系 NAT 用于描述系统固有属性，如飞机最大爬升率等，用于定义 MV 与 CV 之间本身存在的约束关系。在 AltaRica 中，流变量与流变量之间的约束关系可通过断言 assert 实现。因 AltaRica 中的断言也可描述状态变量与状态变量或状态变量与流变量之间的对应关系，而 NAT 仅仅描述 MV 与 CV 之间的约束关系，故 NAT 与断言之间是一种“包含于”的对应关系，并非可逆。

令符号⊕代表某种自然约束关系，那 NAT 与 assert 间的对应关系可表示为：

$$(M:MV.mv_i)\oplus(M:CV.cv_i)\rightarrow(N:assert F.f_i \oplus F.f_j)$$

3.3.4　关系 REQ 与 AltaRica 之间的映射

关系 REQ 描述的是系统中的附加约束，即 MV 发生变化时 CV 应如何变化，本质上仍然描述的是 MV 与 CV 之间的约束关系，与 NAT 类似，故将关系 REQ 与断言 assert 对应。

此时，令⊥代表某种附加约束关系，那么 REQ 与 assert 间的对应关系可表示为：

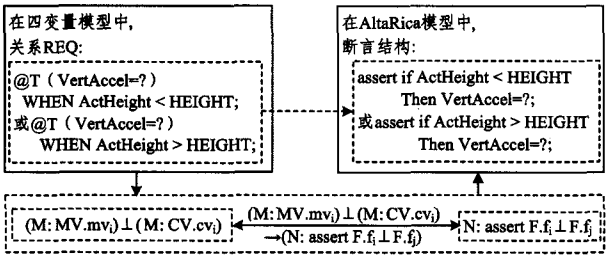

图 5　关系 REQ 与 AltaRica 间的映射过程

$$(M:MV.mv_i)\perp(M:CV.cv_i)\rightarrow(N:assert F.f_i \perp F.f_j)$$

例如，在地形跟踪系统中，假设飞机距地面实际高度 $ActHeight$ 与固定高度 $HEIGH$ 相差太大，超过了某一固定范围，那么输出的飞机垂直加速度 $VertAccel$ 就要相应发生变化，如增加或减少垂直加速度的值。在四变量模型中，该 REQ 关系可表示为“@ T ($VertAccel$ =?) WHEN $ActHeight$ < $HEIGHT$;”或“@ T ($VertAccel$ =?) WHEN $ActHeight$ > $HEIGHT$;”，其中“?”代表计算垂直加速度的某种方式。相应地用 AltaRica 模型表示则是“assert if $ActHeight$ < $HEIGHT$ then $VertAccel$ =?;”或“assert if $ActHeight$ > $HEIGHT$ then $VertAccel$ =?;”。图 5 详细给出了 REQ 与 AltaRica 间的映射过程。

3.3.5　关系 IN 和 OUT 与 AltaRica 之间的映射

关系 IN 和 OUT 在四变量模型中分别描述 MV 与 IV、OV 与 CV 之间的映射关系，从 MV 到 IV 之间存在某种转换规则，使得 MV 经该转换规则得到 IV。OV 与 CV 之间同样如此。在 AltaRica 模型中，流变量与状态变量之间的约束关系同样可通过断言 assert 来表示，故可将 IN 和 OUT 与 assert 相对应。

令“⊢”代表 MV 与 IV 或 OV 与 CV 间的映射关系，那么 IN 和 OUT 与 assert 间的对应关系可表示为：

$$(M:MV.mv_i)\vdash(M:IV.iv_i)\rightarrow(N:assert F.f_i \vdash S.s_i)$$

$$(M:OV.ov_i)\vdash(M:CV.cv_i)\rightarrow(N:assert F.f_i \vdash S.s_i)$$

3.3.6　四变量模型与 AltaRica 之间的映射框架

表 2 具体展示了四变量模型与 AltaRica 模型间的映射规则。其中，关系 NAT，REQ，IN 和 OUT 与 AltaRica 模型中的 assert 结构并非可逆对应，故用“→”表示。可基于该映射关系进行 AltaRica 模型构建。

表 2　四变量模型与 AltaRica 模型之间的映射

四变量模型中的基本结构		AltaRica 模型中的基本结构
基本结构映射：		
MV	↔	$F:f_i:\text{in}$
CV	↔	$F:f_i:\text{out}$
IV	↔	$S:s_i:\text{in}$
OV	↔	$S:s_i:\text{out}$
NAT	→	assert($f_i \oplus f_j$)
REQ	→	assert($f_i \perp f_j$)
IN	→	assert($f_i \vdash s_i$)
OUT	→	assert($f_i \vdash s_i$)

4　实例分析

4.1　机轮刹车系统工作原理概述

本文所研究的机轮刹车系统(WBS)[14]安装于飞机的两个主起落架上，在飞机滑行、着陆及中断起飞(RTO)阶段可通过其对主轮的制动来达到飞机安全停止的目的。具体工作原理为：WBS 包含一个数据控制单元，即刹车系统控制单元(Brake System Control Unit，BSCU)；一个液压子系统，其中有两条液压线路，即正常线路(Normal Line，NL)，又称绿液压线路，以及备用线路(Alternate Line，AL)，又称蓝液压子系统。整个 WBS 从外部环境读入自动刹车、减速率、飞机速度等信息，这些信息被送到 BSCU 子系统后，经计算产生刹车命令。同时，两条液压线路中布满各种机械部件，其中定义一些通用部件，如选择阀、限量阀等。WBS 的输出包括作用于机轮的正常压力值或备用压力值。

4.2　WBS 四变量需求模型

4.2.1　BSCU 子系统的四变量模型

BSCU 子系统的四变量模型如图 6 所示。其中，受监控的变量分两种：1)从整个 WBS 外部接收到的数值信息；2)来自液压子系统的反馈值。这些数值信息经 BSCU 子系统内部处理，最终产生的受控制的变量分别是正常命令和备用命令，用于提供阀门位置命令，作用于 CMD/AS 限量阀和 AS 限量阀。

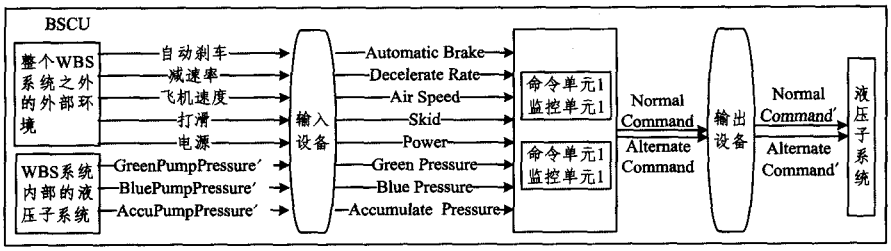

图 6　BSCU 子系统四变量模型

4.2.2　液压子系统的四变量模型

液压子系统的四变量模型如图 7 所示。受监控的变量来自 BSCU 产生的正常命令和备用命令，受控制的变量由两部分构成，即作用于机轮的正常压力值或备用压力值，以及某些组件的反馈值。

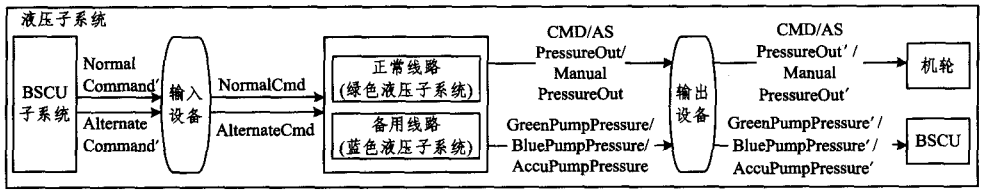

图 7　液压子系统四变量模型

4.2.3　WBS 的四变量模型及 SCR 表

WBS 四变量模型如图 8 所示。

从图 8 中可以看出 WBS 内部又分为 BSCU 子系统和液压子系统，BSCU 产生的受控制的变量即为液压子系统的受监控的变量，最终液压子系统产生的正常压力值或备用压力值即为整个 WBS 的受控制的变量，并作用于机轮。

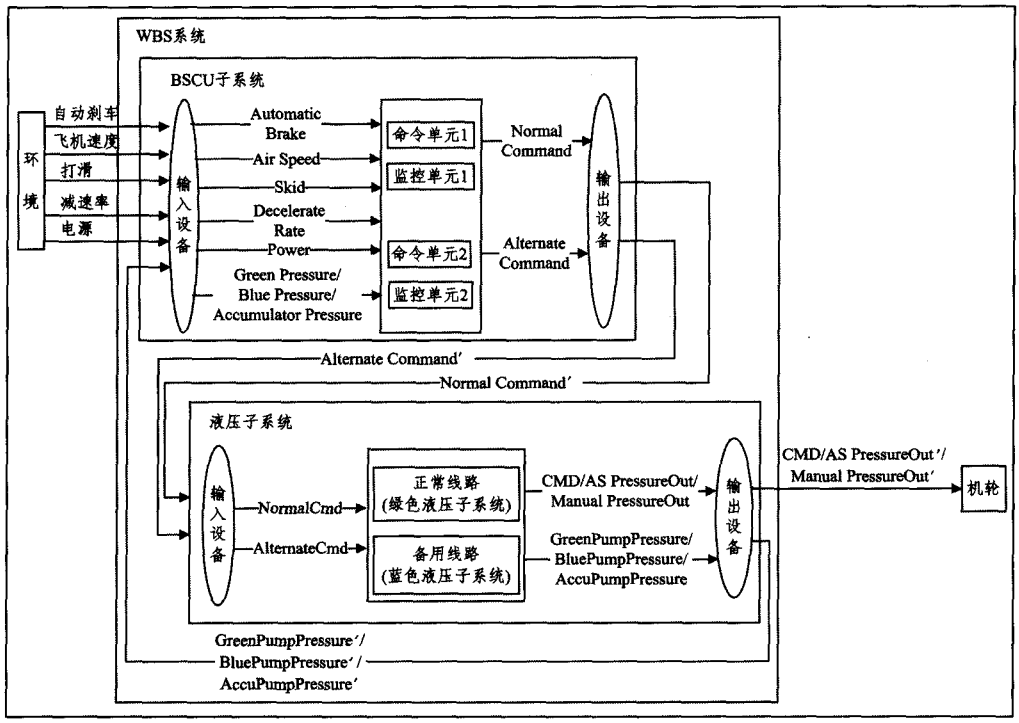

图 8　WBS 系统对应的四变量模型

表 3　模式转换表

Old Mode	Event	New Mode
NM	@T(BSCU: Normal) &@T(GreenPump. PipePressure≥Threshold) &@T(CMD_ASValve. PressureOut′≥Threshold)	NM
NM	@T(BSCU: Non-normal)	AM
NM	@T(GreenPump. PipePressure<Threshold)	AM
NM	@T(CMD_ASValve. PressureOut′<Threshold)	AM
AM	@T(BluePump. PipePressure<ThresHold)	EM

经分析，构造出 SCR 表，表 3 为模式转换表，对于整个 WBS，其工作模式分为 3 种：正常模式（Normal Mode，NM）、备用模式（Alternate Mode，AM）和紧急模式（Emergent Mode，EM）。当 BSCU 正常而绿液压泵液压值及正常线路最终液压值不低于阈值时，WBS 处于正常模式；否则，若有一个不符，则切换至备用模式。若蓝液压泵出现故障，WBS 由备用模式切换至紧急模式。

表 4 为事件表，其中表 4(a)描述 WBS 切换至备用线路这一动作，正常模式下，若 BSCU 出现故障，或绿液压泵产生的液压值小于阈值，或正常线路最终输出的液压值小于阈值，则执行切换至备用线路这一动作，用“TRUE”表示。在备用模式和紧急模式下，没有任何一个事件可执行切换备用线路这一动作，用“False”表示。相反，当 BSCU 正常，绿液压泵产生的液压值及正常管道最终输出的液压值不低于阈值，则一

定不会启用备用线路这一动作，用“FALSE”表示；在备用模式和紧急模式下，无论触发任何事件，都不会启用备用线路，用“True”表示。表 4(b)描述 WBS 切换至紧急模式这一动作，备用模式下，蓝液压泵出现故障，执行切换至紧急模式这一动作；若正常，一定不会启用紧急模式。

表 4 事件表

(a)事件表(切换至备用线路)

Mode	Events	
NM	@T(BSCU:Non-normal)| @T(GreenPump.PipePressure<Threshold)| @T(CMD_ASValve.PressurOut′<Threshold)	@T(BSCU:normal)& @T(GreenPump.PipePressur≥Threshold)& @T(CMD_ASValve.PressureOut′≥Threshold)
AM	False	True
EM	False	True
切换至 AL	TRUE	FALSE

(b)事件表(切换至紧急模式)

Mode	Events	
NM	False	True
AM	@T(BluePump.PipePressure<Threshold)	@T(BluePump.PipePressure≥Threshold)
EM	False	True
切换至 EM	TRUE	FALSE

表 5 为条件表。其中表 5(a)描述产生正常压力值并作用于机轮，正常模式下，正常线路工作且最终压力值不低于阈值时，该压力值可作用于机轮；相反，正常模式下，正常线路工作但最终压力值小于阈值时，该压力值不符合条件。表 5(b)描述产生备用压力值并作用于机轮，备用模式下，备用线路和蓝液压泵正常工作且最终备用压力值不低于阈值时，该压力值可作用于机轮，否则不能。紧急模式下，蓄压泵提供压力值，且最后输出的压力值不低于阈值，该压力值同样可作用于机轮，否则不能。

表 5 条件表

(a)条件表(产生正常压力值)

Mode	Conditions	
NM	Normal_Line& CMD_ASValve.PressureOut′≥Threshold	Normal_Line& CMD_ASValve.PressureOut′<Threshold
AM	False	True
EM	False	True
产生正常压力值	TRUE	FALSE

(b)条件表(产生备用压力值)

Mode	Conditions	
NM	False	True
AM	Alternate_Line& BluePump.PipePressure≥Threshold& ManualValve.PressureOut′≥Threshold	Alternate_Line& (BluePump.GreenPressure<Threshold| ManualValve.PressureOut′<Threshold)
EM	Alternate_Line& AccuPump.AccumulatorPressure>0 &.ManualValve.PressureOut′≥Threshold	Alternate_Line& AccuValve.AccumulatorPressure>0 &.ASValve.PressureOut′<Threshold
产生备用压力值	TRUE	FALSE

4.3 基于 WBS 四变量模型构建 AltaRica 设计

根据以上所建立的 WBS 四变量模型以及 SCR 表，可根据 3.3 节中构建的四变量模型与 AltaRica 模型间的映射规则，进一步设计出 WBS 系统的 AltaRica 模型。

4.3.1 BSCU 子系统的 AltaRica 模型设计

图 9 示出了 BSCU 子系统的 AltaRica 模型，用 BSCU 结点表示。

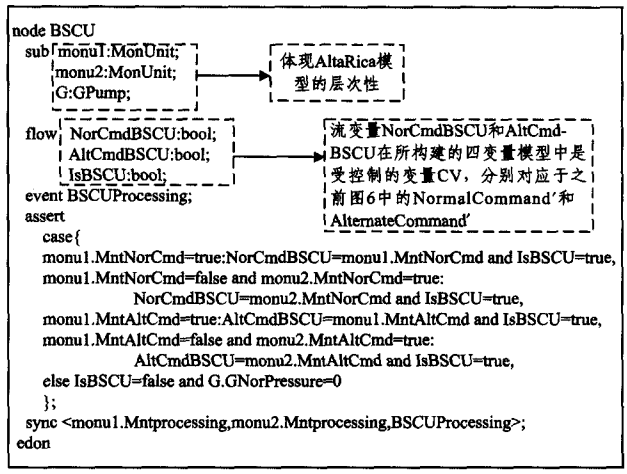

图 9 BSCU 子系统的 AltaRica 模型

图 9 中，流变量包括 *NorCmdBSCU*，*AltCmdBSCU* 和 *IsBSC*。断言 assert 主要说明以下几种情况：1)若第一个监控单元中的正常命令或备用命令有效，则用第一个监控单元中的正常命令或备用命令；2)若第一个监控单元中的正常命令或备用命令无效，但第二个监控单元中的正常命令或备用命令有效，则用第二个监控单元中的正常命令或备用命令；3)若两个监控单元中的正常命令和备用命令均无效，则 BSCU 无效且无任何命令输出。最后用 sync 来构建 BSCU 子系统内部的同步机制[15,16]。

4.3.2 CMD/AS 限量阀的 AltaRica 模型设计

CMD/AS 限量阀的 AltaRica 模型设计如图 10 所示。

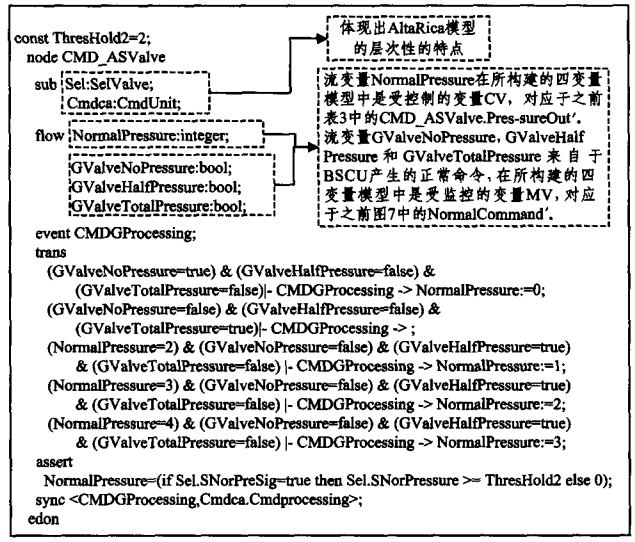

图 10 CMD/AS 限量阀的 AltaRica 模型设计

用 *CMD_ASValve* 来表示该结点组件，其中 *ThresHold* 代表固定阈值，流变量包括 *NormalPressure*，*GValveNoPressure*，*GValveHalfPressure* 和 *GValveTotalPressure*。在 *trans* 转换关系中体现出了针对不同的阀门位置命令液压值的不同换算方法，具体为：1)当阀门位置命令为 *GValveNoPressure* 时，液压值由原来的值换算为 0；2)当阀门位置命令为 *GValveNoPressure* 时，液压值换算为原来的一半；3)当阀门位置命令为 *GValveTotalPressure* 时，液压值保持不变。同样利用

sync 来实现结点间的同步机制。

4.4 系统安全性分析与验证

在前面建立的模型的基础上可以展开系统的安全性分析工作，包括构建 WBS 系统的故障树模型[17,18]，以及进行系统安全性质验证等工作。

4.4.1 构建故障树

故障树分析(Fault Tree Analysis，FTA)方法是一种进行可靠性、安全性分析的重要工具，主要以概率计算为基础，通过对底事件的概率分析得出顶事件发生的概率。FTA 围绕某些特定的状态进行层层分析，以清晰的故障树图形表达组件与系统之间的逻辑关系，最终求出导致系统故障的最小割集并计算顶事件发生的概率，对事件发生频率、损失以及费用作出相应评价。图 11 即为所构建的故障树。通过预计故障概率来确定“正常刹车系统故障”的类别(绿液压系统故障、液压元件故障及 BSCU 不能按指令控制刹车的故障)。

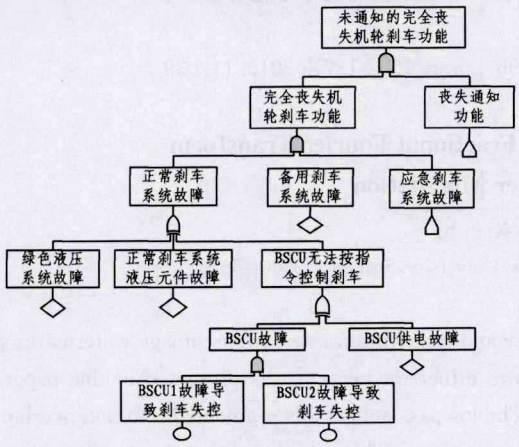

图 11 机轮刹车系统故障树

对 BSCU 复杂功能设计来说，6.6×10^{-6}的故障率预计是不现实的。因此，为了达到这一故障率的预计，BSCU 的能源供应来自于对冗余的 BSCU 概率计算的要求。

4.4.2 安全性属性总结及验证

结合 WBS 模型及故障树，可总结出如下安全性属性：

1)在飞机着陆和中断起飞过程中，所有机轮刹车功能失效的概率不能超过 5×10^{-7}。针对这一属性，由于在建模过程中并没有用到定量分析，因此对这一安全性属性进行简化，可进一步得到：在着陆和中断起飞过程中，“所有机轮的刹车功能失效”这种情况不会发生。为获得有效刹车，规定最终作用于机轮上的压力值不能小于阈值。

2)当机轮处于打滑状态时，刹车压力值需缓慢减弱或移除直到停止打滑。基于以上所观察到的情况，可总结出如下属性：在没有出现打滑的情况下进行刹车，此时无论是正常线路还是备用线路，其压力值都必须大于阈值。

针对以上属性，使用 AltaRica 规范写出对应的逻辑公式，分别如下：

```
1)P1 := (rsrc(HP. cmdas. NorPressure>=0)-
         rtgt(HP. cmdas. NorPressure>=2))&.
         (rsrc(HP. man. AltPressure>=0)-
         rtgt(HP. man. AltPressure>=2));
2)P2 := (rsrc(BS. cmdu1. Skidding=0)-
  [rtgt((HP. cmdas. NorPressure>=2)&.
  (HP. man. AltPressure>=2))])&.
  (rsrc(BS. cmdu2. Skidding=0)-
  [rtgt((HP. cmdas. NorPressure>=2)&.
  (HP. man. AltPressure>=2))]);
```

逻辑公式从反面进行描述，由于属性 1 要求最终压力值不小于阈值，而逻辑公式最后得出的是小于阈值的所有集合，在之后的验证中，仅需验证该集合为 0 则属性成立；属性 2 同样如此。

此处用到的 AltaRica 验证工具为 ARC。ARC 是一种与 Unix 系统中的 shell 程序相似的命令行工具，其中包含多种常用命令以及与 AltaRica 结点相关的命令等。在此验证过程中主要用 TEST 命令，命令方式及命令结果如图 12 所示。

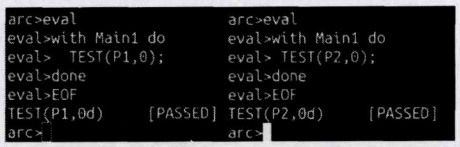

图 12 属性验证结果

结束语 与本文相关的研究工作可分为如下 3 个方面：1)主要研究四变量模型，结合 SCR 结构及 SCR 表对系统进行需求分析。文献[11]详细描述了这一需求分析过程，包括 SCR 方法描述、四变量模型与 SCR 之间的关系以及四变量模型的形式化定义等。2)主要研究 AltaRica 建模语言，结合其配套工具实现对系统的安全性分析。文献[19]介绍了关于 AltaRica 的基本概念，同时结合几个示例对 AltaRica 的模型设计方法以及分析验证工作展开详细描述。3)研究基于模型的系统安全性分析验证方法。文献[14]首先描述传统的安全性分析方法的利与弊，然后给出基于故障模型的安全性分析方法，通过对比得出该方法相比于传统的安全性分析方法更加实用。

相较而言，本文提出了一种基于四变量模型的系统安全性建模与分析方法，具体包括：给出四变量模型与 AltaRica 模型的形式化定义，通过形式化定义构建二者间的映射规则。接着以 WBS 为例说明整个分析验证过程，即首先利用四变量模型进行需求分析，然后根据映射规则利用 AltaRica 建模语言实现 WBS 系统的模型设计，最后通过故障树分析方法进行故障分析，并利用 ARC 完成安全性属性的验证。

进一步工作主要包括以下 3 个方面：

(1)对四变量模型进行进一步扩展。从文中可看出，四变量模型并没有显示地指明软件内部需求，而是通过 *REQ*，*NAT*，*IN*，*OUT* 边界条件进行约束。通过对四变量模型的扩展可以更加详细地对软件内部需求作出分析。

(2)建立四变量模型和 AltaRica 间的形式化语义。文中主要对四变量需求模型到 AltaRica 模型的转换规则进行说明。由于本文主要是研究从四变量模型到 AltaRica 模型转换的可行性，并给出相应的转换规则和实例分析，因此关于建立四变量模型和 AltaRica 间的形式化语义，并进一步展开严格的分析证明将是下一步工作。

(3)文中对模型进行分析，利用相关工具手动构建故障树。事实上，可由 AltaRica 的扩展工具(OpenAltaRica)直接生成故障树，但 OpenAltaRica 工程目前尚不成熟，在今后的工作中需投入更多时间和精力进行研究。

参 考 文 献

[1] Bouali A，Dion B. Formal Verification for Model-Based Development[J]. Sae Transactions，2005，114(7)：171-181

(下转第 229 页)

硬件实现，适用于硬件资源有限且对安全性有一定要求的系统。将其作为密码系统的一个非线性部件，用于设计加密及认证算法，可满足低功耗无线传感器网络对密码算法的基本要求。

无线传感器网络节点配备的能源少，单节点计算能力低，存储资源有限，无线通信距离短，节点数目多，成本低，体积小。在这样的条件下，安全密码算法的可实现性就成为一个关键问题，传统密码算法很难满足其要求。提高无线传感器网络的安全性，必然要求提高传感器节点的计算能力，扩大存储容量，以实现安全性高的复杂密码算法，这必将提高无线传感器网络节点的成本；反之，要求无线传感器网络节点廉价，必然采用低成本的处理器和小容量的存储器，这又会降低运算能力，从而影响安全性高的复杂算法的实现；再者，由于无线传感器网络与应用密切相关，因此无线传感器网络的安全问题应该与实际运算处理能力结合，实现安全与成本的均衡考虑。动态整数帐篷映射用于保障无线传感器网络安全领域，有望解决无线传感器网络面临的信息安全问题。

参 考 文 献

[1] Akhshani A, Mobaraki A, et al. Pseudo random number generator based on quantum chaotic map[J]. Communication in Nonlinear Science and Numerical Simulation, 2014, 19(1): 101-111

[2] Cicek I, Pusane A E, Dundar G. A novel design method for discrete time chaos based true random number generators[J]. Integration , the VLSI journal, 2014, 47(1): 38-47

[3] Cheng Yan-yun, Song Yu-rong. Hash function Construction Based on Chaotic System of Coupled Map Lattice[J]. Journal of Applied Sciences, 2010, 28(1): 44-48(in Chinese)
程艳云，宋玉蓉. 基于耦合映象格子混沌系统的 Hash 函数构造[J]. 应用科学学报，2010，28(1)：44-48

[4] Radwan A G, Abd-El-Hafiz S K. Image encryption using generalized tent map[C]// 2013 IEEE 20th International Conference on Electronics, Circuits, and Systems(ICECS). IEEE, 2013: 653-656

[5] Ghebleh M, Kanso A, Noura H. An image encryption scheme based on irregularly decimated chaotic maps[J]. Signal Processing: Image Communication, 2014, 29(5): 29: 618-627

[6] Liu Jian-dong. One-way Hash Function based on Integer Coupled Tent Maps and Its Performance Analysis[J]. Journal of Computer Research and Development, 2008(3): 563-569(in Chinese)
刘建东. 基于整数耦合帐篷映射的单向 Hash 函数及其性能分析[J]. 计算机研究与发展，2008(3)：563-569

[7] Chen Shuai. Research on Chaos Encryption Theory and Key Technology for Wireless Micro-Sensor Network[D]. Chongqing: Chongqing University, 2006(in Chinese)
陈帅. 无线微传感器网络混沌加密理论及其关键技术研究[D]. 重庆：重庆大学，2006

[8] Liu Jian-dong. Extended integer tent maps and dynamic hash function[J]. Journal on Communications, 2010(4): 51-59(in Chinese)
刘建东. 扩展整数帐篷映射与动态散列函数[J]. 通信学报，2010(4)：51-59

(上接第 199 页)

[2] Feiler P H. Model-based validation of safety-critical embedded systems[C]// Proceedings of the Aerospace Conference. 2010 IEEE, 2010: 1-10

[3] Shokry H, Hinchey M. Model-Based Verification of Embedded Software[J]. Computer, 2009, 42(4): 53-59

[4] Battueux M, Prosvirnova T, Rauzy A, et al. The AltaRica 3. 0 project for model-based safety assessment[C]// 2013 11th IEEE International Conference on Proceedings of the Industrial Informatics(INDIN). 2013: 127-132

[5] Humbert S, Seguin C, Castel C, et al. Deriving Safety Software Requirements from an AltaRica System Model[M]// Computer Safety, Reliability, and Security. Springer Berlin Heidelberg, 2008: 320-331

[6] Li S, Su D. A Practicable MBSA Modeling Process Using Altarica[M]// Model-Based Safety and Assessment. Springer International Publishing, 2014: 1-13

[7] Patcas L M, Lawford M, Maibaum T. From System Requirements to Software Requirements in the Four-Variable Model[J/OL]. http://core. al. uk/display/23645454

[8] Patcas L M, Lawford M, Maibaum T. Implementability of requirements in the four-variable model[J]. Science of Computer Programming, 2015, 111(P2): 339-362

[9] Miller S P, Tribble A C. Extending the four-variable model to bridge the system-software gap [J]. Digital Avionics Systems dascconference, 2001: 4E5/1-4E5/11

[10] Farkas H, Noszticzius Z. Analytical investigation of a four-variable model of the BZ reaction[J]. Reaction Kinetics & Catalysis Letters, 1987, 33(1): 93-98

[11] Heitmeyer C L, Jeffords R D, Labaw B G. Automated Consistency Checking of Requirements Specifications[J]. Automated Consistency Checking of Requirements Specifications, 1996, 5(3): 231-261

[12] Point G, Rauzy A. AltaRica: Constraint automata as a description language [J/OL]. http://altarica. labri. fr/pub/publications/PR996. pdf

[13] Bieber P, Bougnol C, Castel C, et al. Safety Assessment with Altarica[J]. Journal of the American College of Cardiology, 2004, 53(11): 982-991

[14] Joshi A, Miller S P, Whalen M, et al. A proposal for model-based safety analysis[C]// Proceedings of the Digital Avionics Systems Conference, 2005(DASC 2005). 2005

[15] Cassez F, Pagetti C, Roux O. A Timed Extension for ALTARICA[J]. Fundamenta Informaticae, 2004, 62(3/4): 291-332

[16] Bozzano M, Cimatti A, Lisagor O, et al. Symbolic Model Checking and Safety Assessment of Altarica models[J/OL]. http://journal. ub. tu-berlin. de/eceasst/article/view/697

[17] Bieber P, Castel C, Seguin C. Combination of Fault Tree Analysis and Model Checking for Safety Assessment of Complex System[M]// Dependable Computing EDCC-4. Springer Berlin Heidelberg, 2002: 19-31

[18] Lee W S, Grosh D L, Tillman F A, et al. Fault Tree Analysis, Methods, and Applications ? A Review[J]. IEEE Transactions on Reliability, 1985, 34(3): 194-203

[19] Boulanger J L. Safety Analysis of the Embedded Systems with the AltaRica Approach[M]. Industrial Use of Formal Methods: Formal Verification. John Wiley & Sons, Inc. , 2013: 83-121