DOI:10.16356/j.1005-2615.2025.01.020

机载软件层次化需求的形式化建模与分析

王康星[1], 胡 军[1,2], 王立松[1,2], 丁 鼎[1], 董亚炯[1], 戴嘉磊[1]
(1.南京航空航天大学计算机科学与技术学院,南京 211106; 2.软件新技术与产业化协同创新中心,南京 210007)

摘要: 越来越复杂的多层级功能需求给高安全机载软件的设计开发带来了重要挑战。本文给出了一个面向工程应用领域具有层次化语义特征的软件需求形式化建模与分析方法。首先,设计了一个层次化的形式化需求模型。层次化变量关系模型(Hierarchical variable relation model, HVRM)引入工程领域中典型的功能模块属性以及端口等概念来表达系统功能的层次化特征语义,同时也具备原有变量关系模型(Variable relation model, VRM)中基于表格形式的形式化语义,可表示包括条件型、事件型、多维度模式转换等多种类需求的语义信息。进而,基于需求的一致性完整性要求确立了VRM一致性完整性约束簇。其次,设计了一个将工程条目化需求建模为HVRM形式化需求模型的处理框架,并在一个机载软件需求工具平台(Hierarchical avionics requirement tools, HART)中进行了处理功能和需求追溯功能的实现和集成。最后采用某机型自动飞行系统中飞行模式转换软件逻辑需求进行了实例需求建模和模型分析。

关键词: 计算机软件与理论;需求工程;形式化方法;需求建模与分析;飞行控制系统
中图分类号: TP311.5 **文献标志码:** A **文章编号:** 1005-2615(2025)01-0195-10

Formal Modeling and Analysis Method for Hierarchical Requirements of Airborne Software

WANG Kangxing[1], *HU Jun*[1,2], *WANG Lisong*[1,2], *DING Ding*[1], *DONG Yajiong*[1], *DAI Jialei*[1]
(1. College of Computer Science and Technology, Nanjing University of Aeronautics & Astronautics, Nanjing 211106, China;
2. Collaborative Innovation Center of Novel Software Technology and Industry, Nanjing 210007, China)

Abstract: The increasingly complex multi-level functional requirements bring challenges to the design and development of safety-critical airborne software. A formal modeling and analysis method of software requirements with hierarchical semantic characteristics for avionics is proposed. Firstly, a hierarchical formal requirement model is constructed. Hierarchical variable relation model (HVRM) adopts the typical concepts, such as functional module attributes and ports in the engineering domain, to describe the hierarchical feature semantics of system functions, and it also has the formal semantics based on the table form in the original variable relationship model (VRM), which can represent the semantic information of various types of requirements, including conditional, event-based, and multi-dimensional modes transformation, etc. Especially, consistency and integrity constraints are established based on requirements consistency and integrity demand. Secondly, a processing framework is designed to model engineering itemized requirements into HVRM model, and the processing function and requirement traceability function are implemented and integrated in a hierarchical avionics requirement tools (HART), which is an airborne software requirement tool platform. Finally, taking an automatic flight control system as a case, the requirements of the flight mode logic function are modeled and analyzed.

基金项目: 国家自然科学基金(U2241216)。
收稿日期: 2024-07-31;**修订日期:** 2024-11-24
通信作者: 胡军,男,副教授,E-mail:hujun@nuaa.edu.cn。

引用格式: 王康星,胡军,王立松,等. 机载软件层次化需求的形式化建模与分析[J]. 南京航空航天大学学报(自然科学版),2025,57(1):195-204. WANG Kangxing, HU Jun, WANG Lisong, et al. Formal modeling and analysis method for hierarchical requirements of airborne software[J]. Journal of Nanjing University of Aeronautics & Astronautics (Natural Science Edition),2025, 57(1):195-204.

Key words: computer software and theory; requirement engineering; formal methods; requirement modeling and analysis; flight control system

机载软件是一类安全关键软件,要求其具有高安全性、高可靠性和高健壮性等特征[1]。DO-178C标准[2]给出了机载软件研发中的重点:强调基于需求的开发过程和验证目标[3-4],并引入了形式化方法。ARP-4754B标准则为飞机和系统的设计和开发提供了全面的指导[5]。尽管如此,将形式化方法与实际工程实践相结合,开发出适用于航空工程中机载软件需求的构建、分析和验证的有效方法和工具,依然是一个重大挑战[6]。

Collins Aerospace利用架构分析和设计语言(Architecture analysis and design language,AADL)进行OpenUxAS项目的构建与验证[7]。文献[8]利用系统建模语言(System modeling language, SysML)对EA-6B飞机进行建模与分析[8]。徐恒等[9]提出基于SysML的自动飞行系统模式转换需求的领域建模语言(Mode transition requirement discription language, MTRDL),是一种领域化调整的形式化建模语言。统一建模语言(Unified modeling language,UML)[10]、SysML[11]、AADL[12]等半形式化语言需转换为形式化模型或依赖插件以支持分析与验证,存在语义不一致的风险。大韩航空采用Simulink开发无人机控制软件[13]。Ansys则利用Python和高安全应用开发环境(Safety critical application development environment,SCADE)对座舱显示系统进行自动化测试[14]。尽管SCADE和Simulink具有数学模型支持,但细节过多,更倾向于详细设计。

变量关系模型(Variable relation model,VRM)模型及其航空需求工具平台(Avionics requirement toolset,ART)是在机载软件领域的长期工程实践中完善的。包含1个从自然语言需求到VRM模型的建模框架[15]、1个基于VRM模型和SysML的需求仿真方法[16]、1套基于VRM的多范式分析算法[17]、1种基于Simulink模型构建VRM模型的方法[18]。与同类工作相比,ART通过采用领域共享的概念库和规范化的需求模板,有效降低了建模的工作量。此外,VRM模型既是建模的基础,也可直接用于分析,消除了模型转换过程中的语义丢失风险。尽管如此,VRM模型在处理大规模需求实例时仍显示出一定的局限性。大规模的系统功能需求中通常包含系统的层级嵌套结构,此结构特征被本文定义为层次化。现有VRM模型理论中缺乏相关语义和分析方法,无法识别需求中有关层次结构的设计错误。这些错误最终会降低软件产品的可靠性和安全性。

本文的主要贡献是实现了VRM模型理论的层次化扩展,增强了VRM模型的表达能力和ART工具的模型分析能力,并提供了大规模的自然语言需求形式化建模工作的有效范例。具体而言,本文工作面向源自真实世界的飞行导引控制系统的大规模需求实例展开。在理论层面上,引入工程典型的功能模块属性以及端口来表达系统功能的层次化,增加端口一致性完整性约束。在工具层面上,基于模块重新设计建模和分析框架,重新编码实现相关算法。

1 背景知识

飞行控制系统(Flight control system, FCS)中的自动飞行系统(Automatic flight control system, AFCS)是确保飞机依据预设程序或环境条件自动选择并执行飞行模式的关键系统,对于大型商用飞机至关重要[19]。该系统逻辑结构如图1所示,涵盖飞行导引控制子系统(Flight guidance control sys-

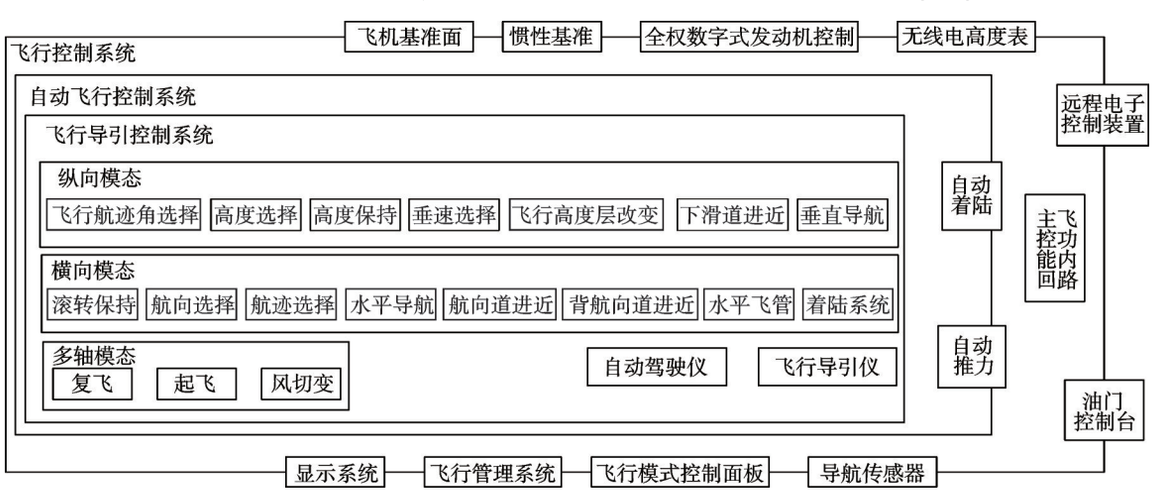

图1 自动飞行控制系统的顶层视图

Fig.1 Top level view of AFCS

tem，FGCS）、自动推力子系统和自动着陆子系统。AFCS与飞行模态控制面板、飞行管理系统和全权数字式发动机控制系统等外部子系统交互。图1直观地展示了系统与子系统之间的包含和生成关系，这不仅体现了本文所探讨的层次化特征，也是工程实践中系统层次划分的关键参考。

飞行导引控制系统包含自动驾驶仪和飞行导引仪等设备，在逻辑上可划分为模态控制逻辑和飞行控制律两大子系统。模态控制逻辑是自动飞行控制系统的重要功能组成部分，通常以机载关键软件的形式来承载[20]。FGCS的飞行模态作为自动飞行系统的重要组成部分，是一个复杂且关键的研究问题，并且具有明显的功能层次特征。本文将基于FGCS的模态控制逻辑系统的功能需求实例进行研究。本文实例中的机型提供了7种纵向模态、6种横向模态和3种多轴模态（图2）。其中飞管垂直导航模态和滚转保持模态又包含各自的子模态。

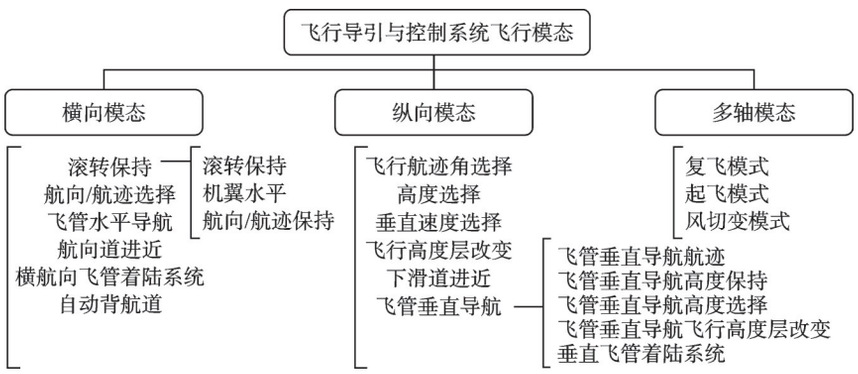

图2　飞行模态总览

Fig.2　Overview of flight modes

2　变量关系模型

层次化变量关系模型（Hierarchical variable relation model，HVRM）是一种专门针对航空软件领域调整的需求模型，源自四变量模型[21]。它整合了表格化表示和形式化语义，便于需求的明确表达。后续章节将借助文献[17，22-23]探讨HVRM模型的详细特性。

2.1　变量关系模型定义

条件和事件构成了系统行为建模的基础。条件c限制了变量取值。原子条件c^*是条件的最小单元，如表达式$(a=b)\wedge(a>c)$中的$a=b$。事件e约束变量在相邻时间点的取值，子事件e^*，通常采用EVENT(S)GUARD(D)形式，其中S和D均为条件。EVENT(S)指明触发事件的动作。GUARD(D)是事件触发的先决条件。表1详细说明了这些谓词符号的语义。$_S$和$_D$分别表示前置状态要满足S和D。

表1　子事件谓词语义

Table 1　Sub-event predicate semantics

谓词		谓词语义	谓词		谓词语义
EVENT	@T	$(\neg \_S)\wedge S$	GUARD	WHEN	$\_D$
	@F	$\_S\wedge(\neg S)$		WHILE	D
	@C	$((\neg \_S)\wedge S)\vee(\_S\wedge(\neg S))$		WHERE	$\_D\wedge D$
	—	True		—	True

HVRM模型被定义为$\{V,T,MC,MT,C,E,IP,OP\}$。领域元素集V由4个子集构成：常量集CV、输入变量集IV、中间变量集TV和输出变量集OV。在不要求严格区分各个变量类型时，可以使用变量标识符v来表示变量iv、tv或ov。这里讨论的输入输出是指系统级别的，与后续提到的模块级输入输出不同。模块级的输入输出分别用输入参数和输出结果来明确表述。T表示领域数据类型的集合，其中的每一个领域数据类型type都是值的非空集合。MC表示模式集mc的集合。MC集合中的任意一个模式集mc，都被定义为(M,SM,m^*)。m^*表示当前模式集的父层级模式。M构成源自需求中定义的1组工作模式。SM则定义了这组工作模式之间如何进行切换。其中模式转换表的1行$sm=\langle m',e,m\rangle$，m'为源模式，m为目标模式。

表2给出了1个EICAS的模式转换表的实例，模式集mcDecluttered包含模式On（激活）、Off（关闭），显示了EICAS的布局方式变化情况。模式转换依赖于3个布尔类型的中间变量。

集合MT表示模块集，其中每个模块mt为系

表2 mcDecluttered的模式转换表

Table 2 The mode transition table of mcDecluttered

源模式	模式转换事件	目标模式
Off	@T((ipLandingGearDecluttered = True) ∧(ipFlapDecluttered = True) ∧(ipSlatDecluttered = True))	On

统层次结构的抽象,由端口port和父模块mt^*定义。模块定义不包含具体行为,而是用于声明系统结构。每个模块都有输入和输出端口,通过这些端口与系统的其他元素交互。父模块保留了层次结构的追溯路径。

条件表集合C由条件ct组成,每个条件由变量v和条件集合F_C定义。条件集合F_C包括一系列条件行cr,每行定义了在特定模式m下,满足条件c后的变量赋值a。事件表集合E由事件et组成,每个事件由变量v和事件集合F_E定义。事件集合F_E包括一系列事件行er,每行定义了在特定模式m下,响应事件e后的变量赋值a。条件和事件表通过变量和端口的关联性追溯至对应的模块。表3条件表中,SelectOrDeselect_ROLL(简写为Select),Is_No_Nonbasic_Lateral_Mode_Active(简写为$\mathrm{Var_1}$)和When_Nonbasic_Lateral_Mode_Activated(简写为$\mathrm{Var_2}$)均为布尔变量。模式集Modes包含模式On和Off。

表3 条件表实例

Table 3 Example of a condition table

变量	条件行		
	依赖模式	条件	赋值
Select	—	($\mathrm{Var_1}$ = True)∧(Modes = On)	True
	—	($\mathrm{Var_2}$ = True)∨(Modes = Off)	False

集合IP定义了端口输入关系,其中每个输入关系ip由变量v和模块mt组成,表示变量v为模块mt的输入参数。集合OP定义了端口输出关系,每个输出关系op由模块mt和变量v组成,表示变量v为模块mt的输出结果。

表3条件表关联至模块Roll Hold,输入关系有〈$\mathrm{Var_1}$, Roll Hold〉和〈$\mathrm{Var_2}$, Roll Hold〉,输出关系有〈Roll Hold, Select〉。因此,变量$\mathrm{Var_1}$、$\mathrm{Var_2}$为模块Roll Hold的输入参数,变量Select为输出结果。为保持与现有VRM模型的兼容性,模块的输入输出未被显式定义。

为系统化地处理变量、模式、条件、事件以及模块间的关系,定义了如下函数。$VR(v|mc)$函数参数为v时返回变量的值域,为mc时返回模式集的所有模式。$VM(v)$确定变量v所依赖的模式集。$VF_C(v)$、$VF_E(v)$获取与变量v关联的条件行、事件行。$\mathrm{IPV}(mt)$、$\mathrm{OPV}(mt)$分别获取模块输入参数和输出结果变量集合。$\mathrm{MCV}(mc)$收集所有影响模式集mc中模式切换的变量。$MF_C(mt)$、$MF_E(mt)$分别获取模块关联的条件表和事件表集合。

2.2 一致性完整性约束

现有形式化分析工作多是基于特定模型、特定领域进行,目前仍未形成统一的标准或成熟工具[9]。HVRM基于DO-178C标准对需求提出的完整性、无二义性等要求,采用多种一致性、完整性约束来尽可能地保证模型的质量,以减少需求撰写和建模过程中引入的错误。完整性的要求是包含与特定系统或部件定义有关的所有内容。无二义性/一致性要求需求彼此之间不矛盾或不重复,所有相同项使用相同术语。

端口一致性是确保系统在层次化架构中避免变量重复赋值的关键约束。该原则规定,任何系统中间变量或输出变量仅能从单一模块接收赋值。端口一致性描述为

$$\forall mt_i, mt_j \in MT$$
$$((mt_i \neq mt_j \wedge \mathrm{OPV}(mt_i) \cap \mathrm{OPV}(mt_j) = \varnothing) \vee$$
$$(mt_i = mt_j \wedge \mathrm{OPV}(mt_i) = \mathrm{OPV}(mt_j))) \quad (1)$$

端口完整性确保了在层次化设计中实体行为与其预定语义的一致性。输入变量作为来自系统外部的量,应仅在系统内部使用,而非内部赋值或输出的对象。中间变量,作为系统内部量,仅在系统内部赋值且必须使用,因此它们应既是模块输入参数也是某模块输出结果。若输入变量、中间变量未被列为输入参数,它们应参与模式的变更。输出变量在系统内部获得赋值,必须作为输出结果。由于模型专注于系统内部行为,对外部传递的约束不是考虑的重点。端口完整性可描述为

$$\left(\forall v \in IV(\forall mt \in MT(v \notin \mathrm{OPV}(mt)))\right) \wedge$$
$$\left(\forall v \in TV \cup OV(\exists mt \in MT(v \in \mathrm{OPV}(mt)))\right) \wedge$$
$$(\forall v \in IV \cup TV((\exists mt \in MT(v \in \mathrm{IPV}(mt))) \vee$$
$$(\exists mc \in MC(v \in \mathrm{MCV}(mc))) \quad (2)$$

图3描述了不满足端口一致性完整性的各种情形。违反模块完整性:输入变量1、中间变量1(未使用),输入变量2(用作输出结果),中间变量2、输出变量2(未作为输出结果)。中间变量1、

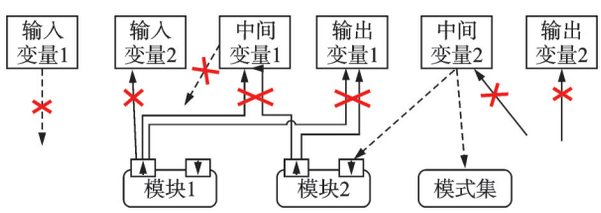

图3 端口一致性完整性错误示例

Fig.3 Error cases of port consistency and integrity

输出变量1违反模块一致性，同时用做模块1和模块2的输出结果，存在赋值冲突的风险。

输入完整性确保所有条件表、事件表和模式转换表都全面覆盖所有可能的工作模式。这里的输入概念指条件表、事件表中的依赖模式以及模式转换中的源模式。输入完整性可保证在任何工作模式下，变量都有确定取值，模式都有可切换的模式。输入完整性约束描述为

$$\forall v\in V((\{m|(m,c,a)=cr\wedge cr\in VF_C(v)\}=M_{VM(v)})\vee(\{m|(m,e,a)=er\wedge er\in VF_E(v)\}=M_{VM(v)}))\wedge\forall mc\in MC(\{m'|(m',e,m)=sm\wedge sm\in SM_{mc}\}=M_{mc}) \tag{3}$$

表2违反输入完整性。模式集mcDecluttere有Off和On两个模式，但是模式转换表的源模式只有Off。{Off}≠{Off, On}，这违反了输入完整性。

输出完整性确保每个条件表和事件表都涵盖相关变量的所有可能取值。这种完整性约束有助于防止某些部件虽设计有特定的响应动作，但在需求文档中却未被适当使用，造成需求的不完整。输出完整性描述为

$$\forall v\in IV\cup TV\cup OV((\{a|(m,c,a)=cr\wedge cr\in VF_C(v)\}=VR(v))\vee(\{a|(m,e,a)=er\wedge er\in VF_E(v)\}=VR(v))) \tag{4}$$

表4展示了EICAS实例中1个违反输出完整性的案例。变量opLandingGearIndicatorRemoved的可能取值为{True, False}，并且依赖于模式mcEngineLayout。然而，在所有工作模式下，该变量在可达事件中均未出现取值False的情况，这违反了输出完整性的要求。

表4　opLandingGearIndicatorRemoved事件表

Table 4　Event table of opLandingGearIndicatorRemoved

变量	事件行		
	依赖模式	事件	赋值
opLandingGearIndicatorRemoved	mNormal	@T(mcDecluttered=On)	True
	mCompressed	@T(mcDecluttered=On)	True

条件完整性要求将条件表根据条件行所依赖的模式进行分组，分组内的条件通过析取操作后得到一个永真式，确保在所有可能的情况下，相关变量都有明确的取值。这种完整性确保了需求中没有遗漏任何条件，这在处理多个条件组合时尤为关键。条件完整性描述为

$$\forall v\in TV\cup OV(\forall m\in VM(v)(\bigcup_{m_i=m\wedge(m_i,c_i,a_i)\in VF_C(v)}c_i=\text{True})) \tag{5}$$

条件一致性要求将条件表根据条件行所依赖的模式进行分组，要求组内任意两个赋值不同的条件合取后为永假式，确保变量不会同时被赋予两个不同的值。这种一致性有助于消除需求规范中的条件歧义，防止出现条件相关的二义性问题。条件一致性描述为

$$\forall v\in TV\cup OV\neg\exists(m_i,c_i,a_i)\in VF_C(v),(m_j,c_j,a_j)\in VF_C(v)(m_i=m_j\wedge a_i\neq a_j\wedge(c_i\cap c_j\neq\text{False})) \tag{6}$$

表3不满足条件完整性，在特定条件组合下，即Modes=on∧Var$_1$=False∧Var$_2$=False，Select的取值无法确定。此外该表也不满足条件一致性，因为在条件Var$_1$=True∧Modes=On成立时，Select的取值无法确定。

事件一致性要求将事件表根据事件行所依赖的模式进行分组，要求组内任意两个赋值不同的事件合取后为永假式，确保变量不会同时被赋予两个不同的值。这种一致性有助于消除需求规范中的事件歧义，防止出现事件相关的二义性问题。事件一致描述为

$$\forall v\in TV\cup OV(\neg\exists(m_i,e_i,a_i)\in VF_E(v),(m_j,e_j,a_j)\in VF_E(v)(m_i=m_j\wedge a_i\neq a_j\wedge(e_i\cap e_j\neq\text{False}))) \tag{7}$$

表5事件表不满足事件一致性。在模式Permitted下，两个事件行合取的事件表达式(@T(Block=on)WHEN(Reset=on))∧(@T(Pressure=High)WHEN(Reset=on))不是永假式，导致在模式Permitted下这一事件发生时Overriden′的取值无法确定。

表5　Overriden′事件表

Table 5　Event table of Overriden′

变量	事件行		
	依赖模式	事件	赋值
Overriden′	Permitted	@T(Block=On)WHEN(Reset=On)	True
	Permitted	@T(Pressure=High)WHEN(Reset=On)	False

3 航空需求工具平台

航空需求工具平台ART是一个面向DO-178C/DO-333机载软件适航标准的软件需求分析与验证工具集,它是一个集成平台,包括需求建模、分析、验证以及测试用例自动生成等功能。ART工具目前仍处于快速迭代中,航空多层次需求工具平台(Hierarchical avionics requirement tools, HART)是ART的进化版本,它在原有工具的基础上,进一步融入了大规模工程实践的需求。HART工具的工作界面,主要分为工程树、菜单栏、页面区域和日志栏。本文研究的重点在于需求建模和需求分析。

3.1 HVRM模型构建

HVRM模型构建流程如图4所示,与VRM模型构建不同,增加了模块和端口的构建环节且需求条目规范化过程按模块进行。初始阶段,从领域概念库中提取系统级的常量CV和数据类型T。随后,根据规范化需求中形成的模块树来构建模块集合MT。每个模块的需求被逐一分析,以需求主体变量为索引,创建集合并收集相关条件和事件,进而生成条件表C和事件表T。在此过程中,记录需求主体变量与模块输出端口的关联,并为输入端口关系IP做准备。同时,分析所有原子条件,提取相关变量,并将其与模块的输入端口关联,以确立输出端口关系OP。最终,从领域概念库中派生出模式集MC,完成HVRM模型的构建。

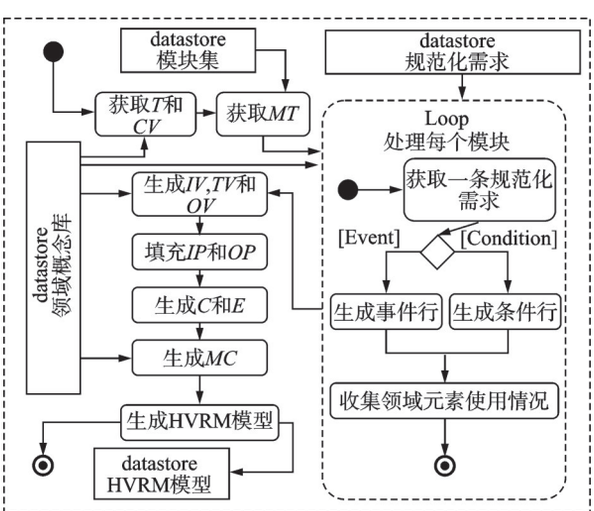

图4 HVRM模型构建

Fig.4 Process of generating an HVRM model

3.2 HVRM模型分析引擎

HART工具内置了一个模型自动分析引擎。该引擎不仅在现有分析算法[17,24]的基础上进行了优化和重新编码,还根据实际工程案例对算法执行流程进行了调整。具体而言,引入了端口一致性完整性分析和将层次化模型分解为子模型的环节。

如图5所示,HVRM模型的分析过程遵循一系列严格的步骤。首先进行的是基本语法分析,这是分析流程的基础。只有当基本语法分析未发现错误时,才能继续执行更深层次的分析。端口一致性完整性分析确保模型中的模块能够正确转换为单层子模型,一旦模型违反此约束,分析将被终止。每个子模型的分析首先从输入完整性分析开始,如果发现错误,则会跳过其他步骤,直接进行输出完整性分析。条件一致性完整性分析和事件一致性分析是并行的,它们之间没有先后顺序。模式集作为系统级别的共享属性,其分析过程独立于其他步骤,主要包括输入完整性和事件一致性分析。

对于基于模块构建的VRM子模型,分析过程则仅限于基本语法分析和子模型特有的分析活动。

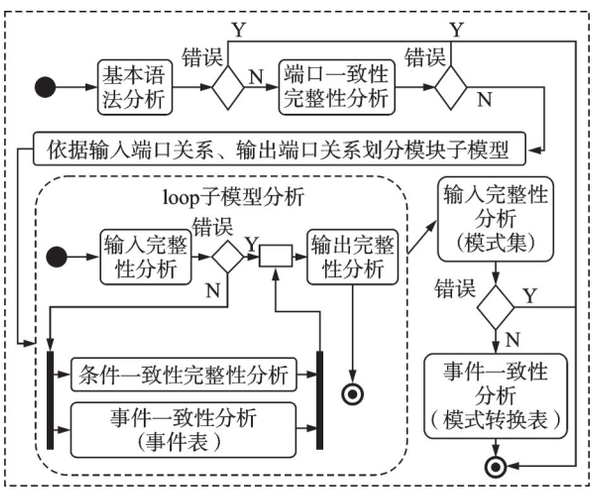

图5 HVRM模型分析的活动图

Fig.5 Activities of mode checking based on HVRM

4 飞行导引控制系统的形式化建模

本节详细介绍了一个对自动飞行系统中飞行导引控制系统子系统的功能需求进行建模和分析的案例。

4.1 条目化自然语言需求预处理

无论是从零开始构建工程还是基于已有的领域概念库进行工程构建,都必须在应用ART工具前进行需求的预处理。预处理阶段要达成两个目标:(1)划分系统的层次关系;(2)将需求条目进行分类。

模块划分应基于系统工程视角下抽象出的系统功能逻辑结构。工程人员提供的自然语言需求文档通常已经根据这一逻辑结构进行了章节划分,这些章节可以直接定义为模型中的模块。如果文档中没有明确的结构划分,则需要与工程人员沟通。

建模人员需要按模块将待建模的原始需求逐条分类为条件型需求、事件型需求和模式转换型需

求，并排除与建模任务无关的需求。对系统的原始需求进行模块化分类时，必须确保这一过程符合工程人员的预期语义，因此工程人员应参与此过程。表6是对FGCS实例需求的分类示例。

表6　条件型需求、事件型需求和模式转换型需求示例

Table 6　Example requirements of conditions, events and mode transitions

需求分类	需求条目
条件型需求	当以下条件均满足时，飞行控制模块应判定飞机满足自动驾驶仪/飞行导航仪接通最小构型状态：2升降舵均有效；2副翼均有效；2对多功能传感器有效；方向舵有效；水平安定面有效；4台作动器控制电子装置均处于飞行控制模块指令模式；1个发动机有效
事件型需求	当以下条件均满足时，飞行控制模块应接通当前的飞行导航仪模态：自动驾驶仪 Engage 从 False 变为 True；飞行导航仪接通
模式转换型需求	当高度选择模式接通且以下条件满足时，飞行控制模块应从高度选择模式模态转为飞行航迹角模态：高度旋钮拨动

4.2　领域概念库构建

构建领域概念库是一个从原始需求中提炼建模元素的严谨过程。建模人员在提取领域概念时，必须避免主观归类，而应与工程人员反复核实，确保概念的准确性和清晰性。例如，在表6所示的条件型需求中，确定“自动驾驶仪/飞行导航仪接通最小构型状态”是作为内部使用的中间变量，还是作为向系统外部传递的输出变量，这一决策需要与工程团队深入沟通才能明确。领域概念库的设计不反映系统功能的具体层级，是一个扁平化的字典库。

图6为工作流程包括以下步骤。首先，根据需求文档的语言特征，构建专用于填充需求规范化模板的领域特定术语。接着，从模式转换型需求中提取模式集信息，并初步构建1个不包含模式转换的模式集。然后，从所有需求中提取实体信息，并汇总每个实体的取值、精度等属性。基于这些汇总信息，进一步定义领域数据类型。一旦所有构建变量所需的属性都已确定，便可以按照与工程人员协商后的类别，构建变量，并形成领域元素集。最终，利用这些变量填充模式转换表，完成模式集的构建。FGCS需求实例中常见的领域数据类型如表7所示。其中NCD（No computed data）表示无计算数据。部分变量如表8所示。

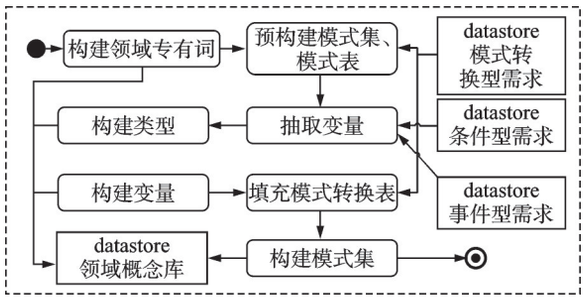

图6　领域概念库构建

Fig.6　Construction of domain concept library

表7　领域数据类型

Table 7　Domain data types

领域数据类型	真实类型	值域	精度
Boolean	Boolean	True，False	—
EulerAngle	Double	−180.0，180.0	0.1
Angle	Double	0.0，360.0	0.1
Valid	Enumerated	Valid，Invalid	—
Calculate_Value_Status	Enumerated	Valid，Invalid，NCD	—

表8　领域元素集中的部分变量

Table 8　Variables in the domain item set

变量名	领域数据类型	类别	初始值	关联模式集
iv_Roll_Angle_Value_Valid	Valid	输入变量	Invalid	无
iv_IR_Roll_Angle_Value	EulerAngle	输入变量	0.0	无
iv_Horizontal_Stabilizer_Valid	Valid	输入变量	Invalid	无
tv_Min_CONF_Of_APFD_Enable	Boolean	中间变量	False	无
tv_When_ASEL_Armed	Boolean	中间变量	False	无
tv_When_FPA_Engage	Boolean	中间变量	False	无
ov_Is_FPA_Engage	Boolean	输出变量	False	无
ov_Is_ASEL_Armed	Boolean	输出变量	False	无

4.3　需求规范化

在需求规范化阶段，建模人员负责对所有条件型和事件型原始需求条目进行逐一规范化处理。每项原始需求根据其类别，选取相应的条件型或事件型模板，并填充必要要素以形成规范化表示。原始需求与规范化需求之间存在一对多的关系，意味着单一原始需求可能对应多个规范化需求，且这些规范化需求应采用统一的模板。需求规范化的具体活动流程见图7。

首先，将需求条目导入HART工具，然后，构建模块集并将需求分配至模块中。最终，对每个需求条目进行循环处理，通过填充选定的规范化模板来生成对应的规范化需求。

表格化表达在数学逻辑的精确性上不输于传

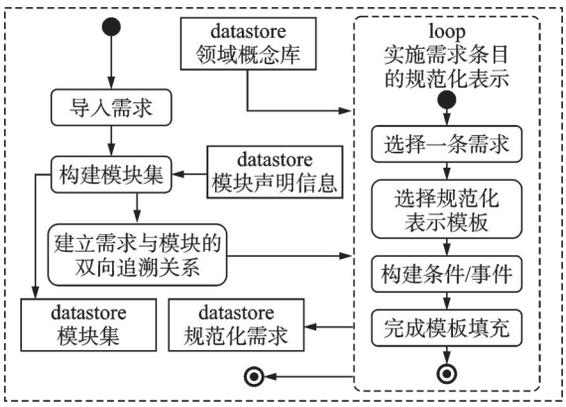

图7 需求规范化活动图

Fig.7 Normalization of requirements

统符号,同时在可读性和易用性方面表现更佳。鉴于表格是工程人员最常接触的文档类型,HART工具采用了RSML[25]的AND-OR表来构建HVRM模型中的条件与事件,并通过自动转换机制,将这些表格转化为对应的逻辑表达式,以便于生成标准化的工程文档。

以表6中条件型需求为例,阐述HART中进行需求规范化的主要操作。对于条件型需求,建模人员选中需求后使用"通用的条件型需求规范化"规范化模板进行规范化处理。接着构建AND-OR表表达式。模板格式为:当满足条件<需求前提><飞机/系统/设备/实体>应该能够<功能><对象/取值>。保存后AND-OR表会自动转换为逻辑表达式插入模板中并生成原始需求对应的一条规范需求。

表6中的条件型原始需求和事件型原始需求经过需求规范化之后对应的规范需求如表9所示。

HART工具具备自动构建HVRM模型的功能,能够从规范需求和建模元素中提取模型关键信息,生成的模型可导出为XML文件。

表9 规范需求示例

Table 9 Examples of normalized requirements

原始需求条目	规范化模板	规范需求
当以下条件均满足时,飞行控制模块的"AFCS接通断开逻辑"功能应判定飞机满足自动驾驶/飞行导航仪接通最小构型状态:2升降舵均有效;2副翼均有效;2对多功能传感器有效;方向舵有效;水平安定面有效;4台作动器控制电子装置均处于飞行控制模块指令模式;1个发动机有效	通用条件	当满足以下条件: tv_Min_CONF_Of_APFD_Enable应能够设置为True: (iv_Elevator_Valid=2 & iv_Flap_Valid=2 & iv_MFS_Valid=2 & iv_Rudder_Valid=Valid & iv_Horizontal_Stabilizer_Valid=Valid & iv_ACES_Mode_In_FCM_Command=4 & iv_Engine_Valid≥1)
当以下条件均满足时,飞行控制模块应接通当前的飞行导航仪模态:自动驾驶仪Engage从False变为True;飞行导航仪接通	通用事件	当满足以下事件: tv_When_Modes_On应能够设置为True: {@T((mcAP=mEngage & mcFD=mEngage)|(mcAP=mEngage & mcFD=mStandby))}

5 实例模型与模型分析结果

在对实例建模过程中,从3个顶层视角观察系统,分别是飞行导引仪的工作视角、自动驾驶仪的工作视角、飞行模态的视角。在飞行模态的视角下,又可进一步在垂直模态接通状态和水平模态接通状态这样更低的视角下进行分析。表10为不同视角下建模的6个模式集。

表10 不同视角下建模的6个模式集

Table 10 Six mode classes for modeling from different perspectives

模式集	工作模式	父模式
mcAP	mDisengage, mAvailable, mEngage	—
mcFD	mStanby, mAvailable, mEngage, mDisengage	—
mcModes	mOn, mOff	—
mcVertical_Mode	mVStandby, mFPA, mASEL, mALT, mVS, mFLC, mGS	mcModes/mOn
mcLateral_Mode	mLStandby, mROLL, mLNAV, mLOC, mBC, mHDG_TRK_SEL	mcModes/mOn
mcRoll_Mode	mUndefined, mRoll_Hold, mWings_Level, mHDG_TRK_Hold	mcLateral_Mode/mROLL

表11展示了实例建模的统计结果,从需求条目、领域元素和模型规模3个维度进行评估。预处理阶段从174条FGCS需求中筛选出101条相关需求,划分为19个逻辑模块。需求分类包括12个条件型、24个事件型和65个模式转换型。建模过程中识别出6个模式集、26个工作模式和86个模式转换事件。共提取145个实体作为变量,包括93个输入变量、32个中间变量、20个输出变量和16个数据类型。规范化需求流程产出了135条规范化需求,分为33个条件型和102个事件型需求,并构

建了25个条件表和29个事件表。

表 11　FGCS实例建模规模

Table 11　FGCS instance modeling scale

统计项目	详细分类	数量
需求条目规模	原始需求条目	174
	可建模条目	101
	条件型需求	12
	事件型需求	24
	模式转换型需求	65
	规范化需求	145
领域建模元素规模	模式集	6
	工作模式	26
	输入变量	93
	中间变量	32
	输出变量	20
	领域数据类型	16
模型规模	模块	19
	条件	33
	事件	102
	模式转换事件	86

HART工具利用模型分析引擎执行HVRM模型的一致性完整性分析，并自动生成报告，以协助工程师识别和定位模型与需求的潜在错误。

表12将模型分析结果进行汇总，在6个模块和1个模式集中有1个输入完整性错误条目，5个条件完整性错误条目，1个事件一致性错误条目，12个输出完整性错误条目。

表 12　FGCS需求模型分析结果统计

Table 12　Analysis results of FGCS model

输入完整性	条件一致性	条件完整性	事件一致性	输出完整性
1	0	5	1	12

模式集mcModes违反了输入完整性，缺少离开模式mOn的转换。需求分析显示，仅1条需求描述了模态接通，缺失了断开的描述。

FGCS模块存在5个条件完整性和7个输出完整性错误，其中5个错误重合。另外2个输出完整性错误可定位到tv_When_Modes_On和tv_When_FD_Engage所关联的事件表。需求中缺少工作状态断开的描述可导致完整性问题。例如表6中的条件型需求未指定何时取消最小构型状态，建议增加“否则判定不满足”来明确。高度选择、航向道进近和背航道进近模块的完整性错误也因需求未说明模态预位的取消条件。需求未明确状态间的互斥关系也会导致错误，如飞行导航仪的Engage、Available、Standby状态。

水平导航（Lateral navigation，LNAV）中事件一致性错误所关联的是表13所示的需求。需求中对预位设置为真时的飞行管理系统（Flight management system，FMS）状态有约束，但解除预位的事件未明确，且模态预位与接通无明确互斥关系，导致实体取值不确定。

表 13　违反事件一致性的需求

Table 13　Requirement containing event consistency error

原始需求
当飞行模式控制面板上的LNAV按钮由断开变为接通时，飞行控制模块应作出如下反应： 1.若LNAV模态未预位或接通，且满足下列所有条件时，预位LNAV模态： 自动着陆未被接通。 （1）自动飞行控制系统检测到有唯一有效的主FMS； （2）FMS的滚转指令有效或NCD。 2.若LNAV模态未预位或接通但自动着陆被接通时，无任何反应。 3.若LNAV已预位时，解除预位LNAV模态。 4.若LNAV已激活时，无任何反应。

6　结　　论

本文提出了HVRM模型，为机载软件领域提供了一种结合系统工程与形式化方法的途径。HVRM通过模块化和端口概念实现需求的层次化表达，并采用表格形式明确条件、事件和模式转换。本文还基于一致性完整性原则，扩展了HVRM模型的一致性完整性分析方法，并通过HART工具链实现需求建模、分析和验证的无缝对接。HART工具的领域概念库功能，有效降低了从自然语言需求中提取建模元素的成本，且基于模块的建模和分析方式适应了计算资源有限的工程实际，降低了分析的计算成本。本文在HART平台上对飞行导引控制系统进行了完整的建模与分析，展示了形式化方法在工程实践中的应用潜力。

未来，将继续深化工程应用，秉承“从工程中来，到工程中去”的原则，从实际问题出发，不断优化VRM模型和ART工具。计划引入时序语义，增强模型对多时序状态的支持，并同步更新相关算法。同时，将进一步提炼自动飞行领域的需求描述语言结构，发展面向该领域的规范化模板，以提升需求建模的效率和准确性，期望为机载软件的形式化建模和分析提供更加成熟、实用的解决方案。

参考文献：

[1] LEVESON N G, THOMAS J P. Certification of safety-critical systems[J]. Communications of the ACM, 2023, 66(10): 22-26.

[2] Special Committee 205. Software considerations in airborne systems and equipment certification: DO-178C—2011[S]. Washington: Radio Technical Commission for Aeronautics, 2011.

[3] LEMPIA D L, MILLER S P. Requirements engineering management findings report: DOT/FAA/AR-08/34[R]. Washington: FAA, 2009.

[4] Federal Aviation Administration. Advanced avionics handbook[M]. South Carolina: CreateSpace Independent Publishing Platform, 2023.

[5] S-18 Aircraft and Sys Dev and Safety Assessment Committee. Guidelines for development of civil aircraft and systems: ARP-4754B—2023[S]. Warrendale: SAE International, 2023.

[6] ROGGENBACH M, SCHLINGLOFF B H, SCHNEIDER G. Formal methods for software engineering: Languages, methods, application domains[M]. Cham: Springer International Publishing, 2022.

[7] MERCER E, SLIND K, AMUNDSON I, et al. Synthesizing verified components for cyber assured systems engineering[J]. Software and Systems Modeling, 2023, 22(5): 1451-1471.

[8] ELAKRAMINE F, IBNE HOSSAIN N U, JARADAT R, et al. The application of system modelling language (SysML) in an aviation structure and maintenance system[C]//Proceedings of ASEM 41st International Annual Conference. Huntsville: American Society for Engineering Management, 2020.

[9] 徐恒, 黄志球, 胡军, 等. 基于MTRDL的自动飞行系统模式需求建模与验证方法[J]. 软件学报, 2024, 35(9): 4265-4286.
XU Heng, HUANG Zhiqiu, HU Jun, et al. Requirement modeling and verification for automatic flight system modes based on MTRDL[J]. Journal of Software, 2024, 35(9): 4265-4286.

[10] COOK S, BOCK C, RIVETT P, et al. OMG unified modeling language (OMG UML): Formal/17-12-05—2017[S]. [S.l.]: Object Management Group, 2017.

[11] BRON J Y. System requirements engineering: A SysML supported requirements engineering method[M]. Hoboken: ISTE Ltd/John Wiley and Sons Inc, 2020.

[12] AS-2C Architecture Analysis and Design Language. Architecture analysis & design language (AADL): AS5506D—2022[S]. [S.l.]: SAE International, 2022.

[13] MOON J H, SHIN S S, CHOI S K, et al. Development of UAV flight control software using model-based development (MBD) technology[J]. Journal of the Korean Society for Aeronautical & Space Sciences, 2010, 38(12): 1217-1222.

[14] COUADAU F, DERVAUX N, FAYOLLAS C, et al. Automated testing of ARINC 661 cockpit display systems: Factors to accelerate DO-178C certification[C]//Proceedings of 2023 IEEE/AIAA 42nd Digital Avionics Systems Conference (DASC). [S.l.]: IEEE, 2023.

[15] 胡建成, 胡军, 汪文轩, 等. 一种面向领域自然语言需求的形式化需求模型生成方法研究[J]. 小型微型计算机系统, 2021, 42(8): 1639-1648.
HU Jiancheng, HU Jun, WANG Wenxuan, et al. Constructing formal specification models from domain specific natural language requirements[J]. Journal of Chinese Computer Systems, 2021, 42(8): 1639-1648.

[16] 展万里. 基于形式化模型的需求仿真与架构安全性分析方法研究[D]. 南京:南京航空航天大学, 2022.
ZHAN Wanli. Based on the requirement of formalization model simulation and structure analysis method study[D]. Nanjing: Nanjing University of Aeronautics & Astronautics, 2022.

[17] 胡军, 吕佳润, 王立松, 等. 一个机载软件需求形式化建模与分析实例研究[J]. 软件学报, 2022, 33(5): 1652-1673.
HU Jun, LYU Jiarun, WANG Lisong, et al. A case study on natural language requirement based Formal modelling and analysis for an airborne display control software system[J]. Journal of Software, 2022, 33(5): 1652-1673.

[18] 李俊安, 胡军, 王立松, 等. 自动飞行模式转换逻辑的形式化建模与验证[J]. 南京航空航天大学学报, 2023, 55(5): 768-779.
LI Junan, HU Jun, WANG Lisong, et al. Formal modeling and verification of automatic flight mode transition logic[J]. Journal of Nanjing University of Aeronautics & Astronautics, 2023, 55(5): 768-779.

[19] SADRAEY M. Automatic flight control systems[M]. San Rafael: Morgan & Claypool Publishers, 2020.

[20] 王飞. 大型客机飞行导引控制系统工作模式仿真研究[D]. 天津:中国民航大学, 2021.
WANG Fei. Simulation research on operating mode of flight guidance control system for large passenger aircraft[D]. Tianjin: Civil Aviation University of China, 2020.

[21] MILLER S P, TRIBBLE A C. Extending the four-variable model to bridge the system-software gap[C]//Proceedings of the 20th Digital Avionics Systems Conference (No.01CH37219). Daytona Beach, FL, USA: IEEE, 2001.

[22] 石梦烨. 基于形式化模型的系统需求与设计安全性分析方法研究[D]. 南京:南京航空航天大学, 2020.
SHI Mengye. Research on system requirements and design safety analysis method based on formal model[D]. Nanjing: Nanjing University of Aeronautics and Astronautics, 2020.

[23] MILLER S P, TRIBBLE A C, CARLSON T M, et al. Flight guidance system requirements specification: NASA/CR—2003-212426[R]. Washington: NASA, 2003.

[24] 吕佳润. VRM需求模型的语义分析方法研究[D]. 南京:南京航空航天大学, 2023.
LYU Jiarun. Research on semantic analysis method of VRM requirement model[D]. Nanjing: Nanjing University of Aeronautics and Astronautics, 2023.

[25] LEVESON N G, HEIMDAHL M P E, HILDRETH H, et al. Requirements specification for process-control systems[J]. IEEE Transactions on Software Engineering, 1994, 20(9): 684-707.

(编辑:刘彦东)