DOI:10.19708/j.ckjs.2018.01.026



# 基于SCADE的航空发动机FADEC软件开发

周彰毅，黄　浩，方　伟，朱理化
（中国航发控制系统研究所，江苏 无锡　214063）

**摘要**：机载软件开发面临复杂性、安全性和成本等方面的巨大挑战。针对某航空发动机数控系统的研制，结合FADEC软件的开发特点和目标，探索SCADE基于模型开发在FADEC软件开发中的应用。探索了两种不同的SCADE基于模型开发解决方案，基于这两种方案分别完成两个FADEC软件配置项的应用软件开发。通过模型测试、模型覆盖率分析和软件硬件集成测试验证了开发结果的正确性。提出了联合SCADE和Simulink的基于模型开发流程并明确其注意事项。分析SCADE的两种基于模型开发解决方案的适用范围以及方案选择时的考虑因素，总结分析了SCADE用于机载软件开发的优势和不足。

**关键词**：FADEC；基于模型开发；SCADE；模型覆盖率；DO-331
**中图分类号**：TP311.1　　**文献标识码**：A　　**文章编号**：1000－8829(2018)01－0110－06

## Development of FADEC Software for Aero-Engine Based on SCADE

ZHOU Zhang-yi, HUANG Hao, FANG Wei, ZHU Li-hua
(AECC Aero-Engine Control System Institute, Wuxi 214063, China)

**Abstract:** The development of airborne software is faced with great challenges in complexity, security and cost. For the development of an aero-engine numerical control system, with the combination of the features and objectives of FADEC software, the application of SCADE in the development of FADEC software is explored. Two different SCADE model-based development(MBD) resolutions were researched and two FADEC applications were developed by these two resolutions respectively. The correctness of the development results was verified by model test, model coverage analysis and software and hardware integration test. A new development process was proposed by the combination of SCADE and Simulink, and some of the key notes were illuminated. The application scope of these two SCADE MBD resolutions is analyzed and considerations for choice are proposed. The merits and demerits of SCADE in the development of airborne software are analyzed and summarized.

**Key words:** FADEC; model-based development; SCADE; model coverage; DO-331

航空发动机全权限数字电子控制系统(FADEC)软件开发面临软件规模及复杂性不断增长、软件开发成本和可靠性之间的矛盾日益突出、安全性要求更严格、软件的全生命周期过程中需求变更和软件升级更频繁、软件的验证和分析工作量急剧增大等诸多挑战。基于模型开发(Model-Based Development，MBD)和自动代码生成(Automatic Code Generation，ACG)具有开发周期短、费用低、风险小等优点，已成为软件开发的重要方法[1-2]。在机载安全关键软件适航审定方面，美国航空无线电技术委员会(RTCA，Radio Technical Commission of Aeronautics)在2011年发行《机载系统和装备合格审定的软件考虑》(即DO-178C)的同时发行了补充指南《对DO-178C和DO-278A的基于模型开发和验证的补充文档》(即DO-331)。DO-331对MBD的软件生命周期的活动和目标进行了明确的定义，以指导软件开发机构使用MBD进行机载软件开发和适航认证[3-4]，这势必加速MBD技术在机载安全关键软件开发方面的应用。

SCADE(Safety-Critical Application Development Environment)是专注于高安全性系统和嵌入式软件的集成开发环境，其自动代码生成工具KCG是目前唯一

**收稿日期**：2017－01－24

**作者简介**：周彰毅(1985—)，男，贵州剑河人，侗族，硕士，工程师，主要研究方向为FADEC软件设计、基于模型开发；黄浩(1978—)，男，湖南常德人，硕士，研究员级高级工程师，主要研究方向为航空发动机控制、FADEC软件开发；方伟(1987—)，男，安徽六安人，硕士，工程师，主要研究方向为FADCE软件开发；朱理化(1984—)，男，江苏徐州人，硕士，工程师，主要研究方向为FADEC软件开发、基于模型开发。

通过 DO-178C 最高标准(适用 A 级软件)认证的代码生成器,充分保证模型和代码完全一致性[5-6]。国外航空发动机巨头 R&R、GE 和 P&W 等都用 SCADE 作为 MBD 开发环境,开发 FADEC 软件并通过适航认证。

## 1 SCADE 基于模型开发解决方案

在基于模型的安全关键软件开发方面,SCADE 提供了如下两种 MBD 解决方案。

(1) 基于 SCADE 工具集的完整 MBD 解决方案。

该方案中 SCADE 提供完整的 MBD 集成开发环境,包括软件设计(建模、模型测试和验证)、自动代码生成、自动文档生成以及软件生成周期过程的追溯管理[7]。SCADE 的软件开发过程见图 1。

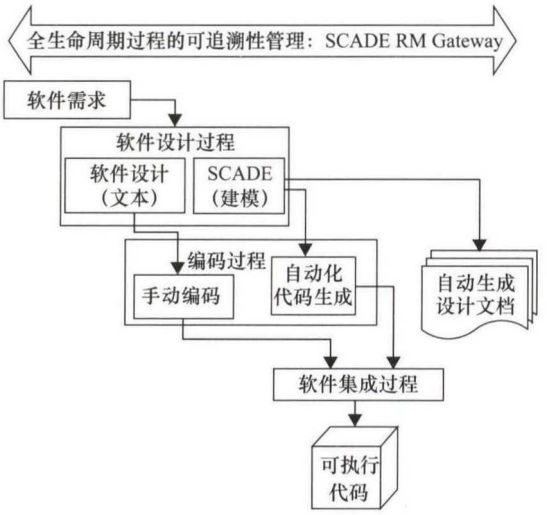



图 1 基于 SCADE 的软件开发过程

软件设计阶段,对基于模型开发的软件部件(通常是应用软件,主要是信号处理、控制逻辑和控制算法等),使用 SCADE 完成模型设计和验证,然后通过 KCG 自动生成代码。对其他软件部件(主要是操作系统和跟硬件接口进行交互的部分),软件设计阶段形成文本形式的软件设计说明,然后依据设计说明进行手工编码。最后将手工代码和自动生成的代码进行集成和编译,形成可执行文件。SCADE 报告生成器 Qualified Reporter(经 A 级认证)可以自动生成设计文档,便于模型审查和软件设计文档的配置管理。此外,SCADE RM Gateway 用于软件全生命周期的追溯管理,包括需求和设计(设计文档或模型)的追溯、是模型测试用例和需求的追溯等。

在模型验证方面,SCADE 提供经认证的测试环境 QTE(Qualified Testing Environment),支持模型的仿真测试和覆盖率分析,模型验证场景见图 2。基于软件需求设计模型测试用例,在 QTE 中启动测试执行引擎(Test Execution Engine,TEE)运行测试用例,再使用模型测试覆盖率工具(Model Test Coverage,MTC)分析模型覆盖率,并自动生成模型覆盖率报告和相应的代码覆盖率报告。

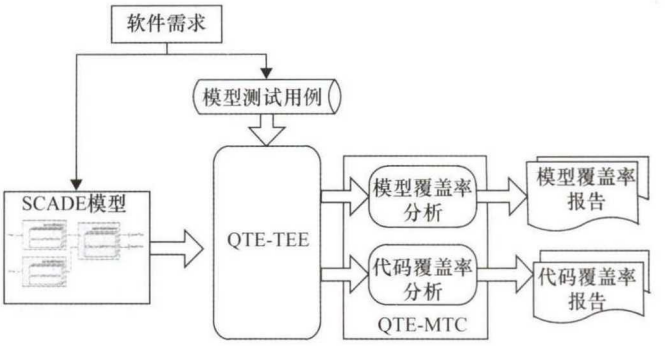



图 2 SCADE 模型验证示意图

(2) SCADE 和 Simulink 和联合 MBD 解决方案。

为继承系统原型设计阶段和软件需求分析阶段的成果、缩短研发周期、减少用户在技术和资金上的重复投入,SCADE 提供了多种接口,支持跨平台的联合开发,包括与 Rhapsody、Simulink、LabVIEW 等工具的交互开发。在与 Simulink 的联合开发方面,SCADE 提供了 Simulink Gateway 和 Simulink Wrapper,支持两者的交互式开发[8],见图 3。

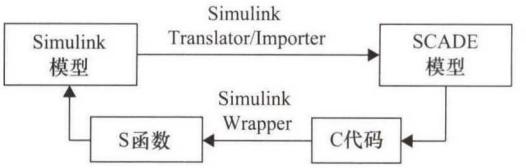



图 3 SCADE 与 Simulink 交互开发示意图

其中,SCADE Simulink Gateway 包括 Simulink Translator 和 Stateflow Importer 两个部分,能将 Simulink 模型转换成 SCADE 模型。Simulink Wrapper 可将 SCADE 模型集成到 Simulink 模型中并在 Simulink 环境下进行联合仿真,包括两种方式:① 将 SCADE 模型生成代码后封装成 S 函数,集成到 Simulink 中进行仿真,称为黑盒仿真;② Simulink 仿真器直接驱动 SCADE 仿真器来实现 Simulink 和 SCADE 的联合仿真,称为白盒仿真。

下面基于 SCADE 工具集,采用第一种 MBD 解决方案进行发动机健康管理模块应用层软件开发,并联合使用 SCADE 和 Simulink 进行发动机推力矢量模块的应用层软件开发。

## 2 健康管理应用软件开发

航空发动机的健康管理系统包括发动机故障诊断、监视告警、事件记录和寿命统计等功能,是 FADEC 系统的重要组成部分[9]。在软件顶层架构上将健康管理软件分为应用层软件和操作系统层软件,其中应

用层软件为核心部分，完成健康管理的主要功能。

### 2.1　模型设计开发

模型设计和开发主要包括以下 3 个方面：

① FADEC 模型库。开发通用的 FADEC 模型库，在软件架构和低层需求层级进行复用，以加速开发过程和降低开发成本。主要包括计数器模型（Lib_Counter）和故障确认模型（Lib_FaultConfirm）等。

② 可调整参数的设计考虑。FADEC 软件生命周期长，在设计定型前，为摸索发动机或飞机的性能，用户要求设置大量的可调整参数，以满足不同阶段的试验任务需要。在模型设计上使用 SCADE 提供的 Sensors 数据元素作为可调整参数。Sensors 数据类型作为全局变量在数据流中使用，且具有只读属性，在整个循环周期内数值不会改变。

③ 顶层模型设计。顶层模型设计上以模块的独立性为出发点，降低功能耦合和数据耦合，尽量减少模型间的数据传递个数。在接口设计方面遵循简单原则，使模型接口简单清晰，便于与手工代码集成，提高软件的可维护性。

健康管理软件的 SCADE 顶层模型见图 4。

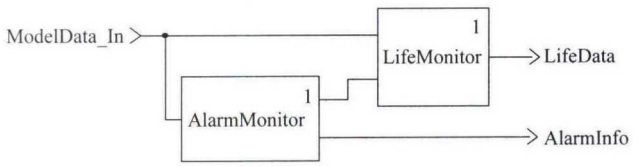



图 4　发动机健康管理软件 SCADE 顶层模型结构图

### 2.2　模型验证和覆盖率分析

模型验证考虑两点，一方面是模型对健康管理软件高层需求的 100% 覆盖，即所有的软件需求已经在 SCADE 模型中实现，通过基于高层需求的模型测试以及需求和模型的双向追溯来共同保证；另一方面是模型的结构覆盖，主要是验证 SCADE 模型中没有非预期的功能，通过模型测试和模型覆盖率分析来验证，以达到 100% 的模型结构覆盖。

FADEC 软件为 A 级安全关键软件，DO-178C 中对 A 级软件的模型覆盖率要求是基于 MC/DC 覆盖准则模型 100% 覆盖。基于健康管理软件高层需求编写 TCL 脚本形式的模型测试场景，使用 QTE 对模型进行测试，并使用 MC/DC 准则对模型进行测试验证，最后通过 MTC 进行覆盖率分析，见图 5。

完成基于高层需求的模型测试后，模型覆盖率报告显示，健康管理 SCADE 模型总分支数为 651 个，基于软件高层需求的测试所覆盖的分支数为 605 个，其余 46 个分支为模型设计阶段所引入（属于衍生需求）。衍生需求往往是风险最大的部分，对这些分支进行充分的分析，防止模型中存在非预期的功能，并补充模型测试用例，达到 MC/DC 标准的 100% 模型结构覆盖。


图 5　模型测试和覆盖率分析图

### 2.3　代码生成和集成验证

完成模型验证后，使用 KCG 自动生成可移植的 C 代码，对生成的代码无需进行代码审查和单元测试，直接与手工代码进行集成。在集成过程中主要考虑模型输入输出参数的配置。顶层模型对应的函数作为主函数，在周期任务中被调用。

代码集成完毕后，在硬件在环仿真环境中对健康管理模块进行软硬件集成测试，系统测试用例全部通过。

## 3　推力矢量应用软件开发

为继承该型号推力矢量控制器系统原型开发阶段的 Simulink 模型，并充分发挥 SCADE 在嵌入式软件开发的高安全性优势，本节研究基于 Simulink Gateway 的 Simulink 和 SCADE 联合开发。将成熟的 Simulink 模型转换成 SCADE 模型，在 SCADE 中进行模型验证并生成代码，最后进行集成验证。推力矢量的 Simulink 模型包括 SCM_INP 和 SCM_EXE 两部分，其中 SCM_EXE 是模型的主体，包含大量的数据流模型和多个状态机模型，是控制算法和控制逻辑的核心部分。

### 3.1　数据流模型转换

出于无歧义和安全性考虑，数据流模型转换器 Simulink Translator 对 Simulink 数据流模型有明确的要求，Simulink 数据流模型需遵循以下规则：

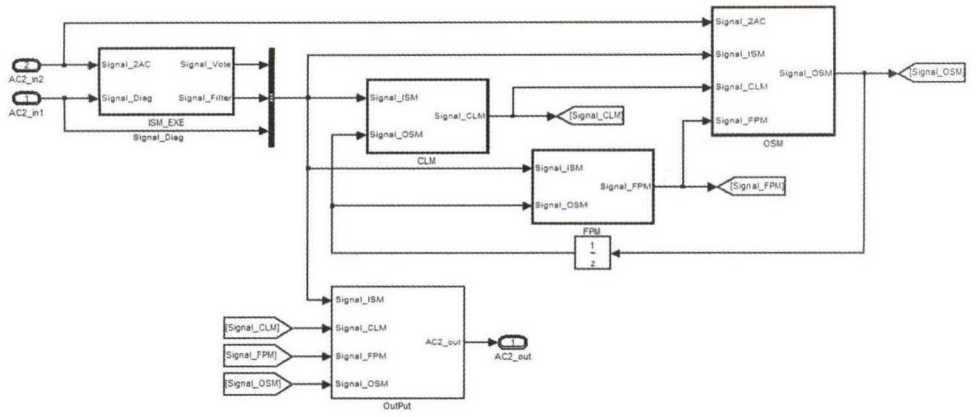
① 模型必须是离散的；

② 模型只有一个根节点；

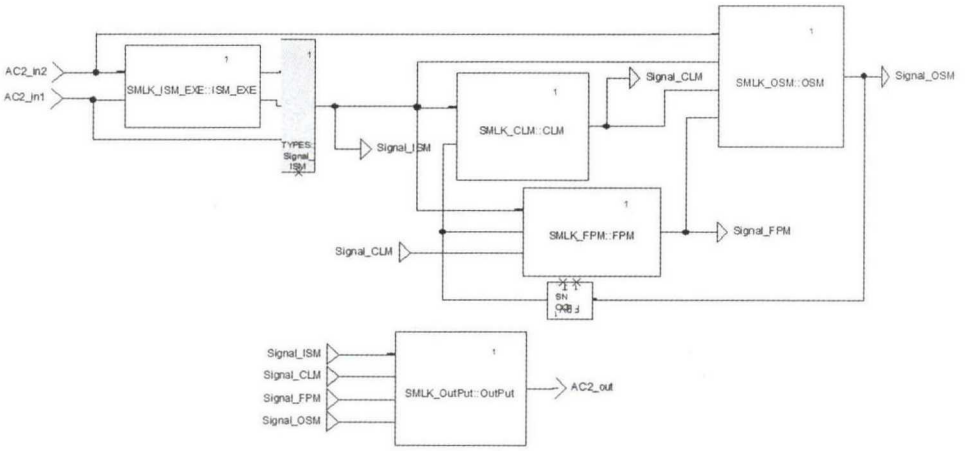
③ 模型中不包含代数环，代数环容易产生歧义，并可能产生执行时间越界；

④ 建模必须使用 Simulink Gateway 支持转换的模块元素，典型的不支持转换的模块是与高安全性嵌入式系统不兼容的模块，如状态空间模块等。

通过 Simulink Translator 对推力矢量的 Simulink 数据流模型进行转换，转换结果见图 6。




(a) Simulink模型




(b) 转换后的SCADE模型

图 6 顶层数据流模型转换结果图

转换结果显示,从 Simulink 转换来的 SCADE 模型有以下特点:

① 结构保留,即相同的层级结构;

② 图形形式保留,即元素位置和大小比例基本一致;

③ 接口和名称保留,即变量名、操作符名称保持一致。

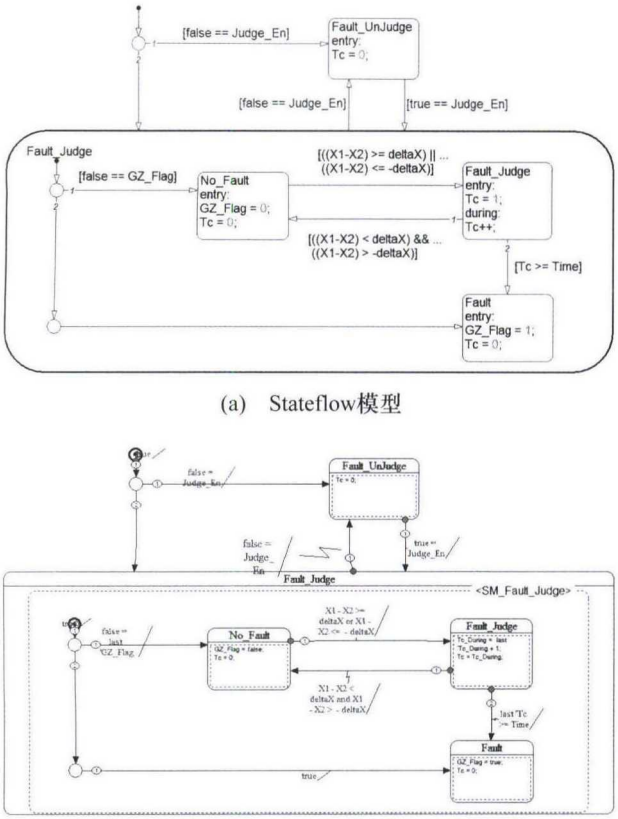
### 3.2 Stateflow 模型转换

状态流 Stateflow 在 Simulink 建模时多用于实现状态机、逻辑判断及选择和真值表等功能。对 Stateflow 模型的转换,Simulink Gateway 只支持标准状态机的转换。典型 Stateflow 模型的转换结果见图 7。对用于逻辑选择和真值表的 Stateflow 模型,不能转换为 SCADE 模型。此外,不支持转换的模型还有内部状态迁移、跨迁移的数据交互和 Embedded Matlab Function 等,对这些不支持转换的类型,应在 SCADE 中重新建模。

### 3.3 验证

完成模型转换和集成后,在 SCADE 中进行模型测试和验证。为提高模型验证的效率,采用测试用例复用的方法,使用自定义和开发的转换工具将系统原型阶段 Simulink 模型的测试用例自动转换成 TCL 测试脚本,然后用 TCL 脚本驱动 SCADE 模型测试。自动转换后的 TCL 测试脚本能完整实现对转换后模型的 MC/DC 100% 覆盖。对通过测试的 SCADE 模型,使用 KCG 生成代码,然后进行集成和软硬件集成测试,最后在硬件在环仿真平台上完成软硬件集成测试。

SCADE 和 Simulink 联合开发,能充分发挥两个工具各自的优势,基于目前的开发实践经验,提出两者联合开发的 MBD 流程,见图 8。软件开发人员和系统原型开发人员根据总体技术要求分解出各自的需求,并基于需求在不同的环境中进行模型开发。然后将 Simulink 模型中的控制律模型(离散模型,主要是控制算法部分)通过 Simulink Gateway 自动转换为 SCADE 模型。最后在 SCADE 中进行模型集成、测试,再使用 KCG 自动生成高安全性代码。需强调的是,考虑到模型转换的约束,系统原型开发人员在 Simulink 建模时只能使用 Simulink Gateway 支持转换的模块,特别是使用 Stateflow 时要严格遵循标准状态机的建模方法。因此,软件开发人员和系统原型开发人员应提前定制建模规范并对约束准则等达成一致。




(a)　Stateflow模型




(b)　转换后的SCADE模型

图 7　状态机转换结果

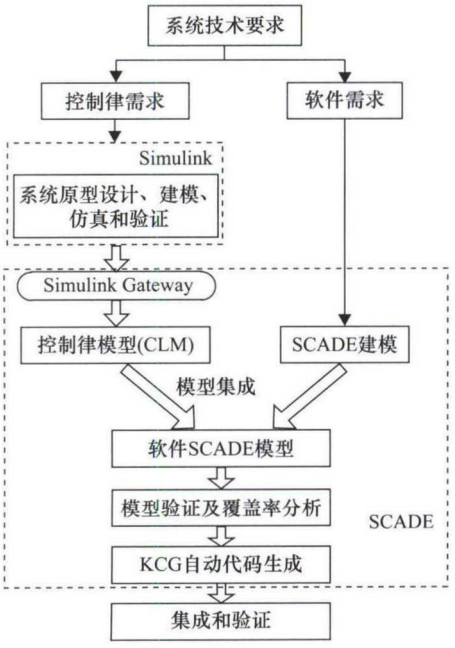



图 8　SCADE 和 Simulink 联合 MBD 流程

## 4　SCADE 用于机载软件开发的优劣分析及 MBD 方案选择

### 4.1　MBD 方案的选择考虑

在 SCADE 的 MBD 解决方案选择方面，主要从企业的技术积累、职能划分、软件规模、认证目标等方面进行考虑。

SCADE 和 Simulink 的联合 MBD 模式适用于小型软件开发。对于大型的复杂软件，这不是一种值得推荐的解决方案。一方面，大型复杂的 Simulink 模型转换工作量较大，模型接口数据的匹配和确认比较复杂。另一方面，系统原型阶段 Simulink 模型的仿真和验证并不能裁剪软件开发阶段的模型验证活动和目标，对转换后的 SCADE 模型仍需进行模型测试和模型覆盖率分析。对软件开发人员来说，验证和修改一个不熟悉的模型会耗费更多的精力和时间。系统人员更多地专注于系统功能，对软件的技术细节如时序、数据类型等通常缺乏充分的考虑。此外，系统人员很难按照软件开发流程和约束要求来建模。因此，在职能划分和管理上，这种联合 MBD 方案也存在一定的操作难度。

如果企业初次选择 MBD 技术进行软件开发，特别是以软件通过适航认证为目标，那么基于 SCADE 工具集的完整 MBD 方案是推荐的首选方法。一方面是 SCADE 开发环境的完整性和高安全性。它包括了软件的开发和验证工具，而且这些工具都是经过认证的，在适航认证时能够裁剪 DO-331 中规定的不少认证目标。另一方面，软件开发人员进行软件建模，更有利于模型的验证和升级维护。选择这个 MBD 方案时，企业应该从技术和管理两方面构建和完善自己的 MBD 流程。包括通用模型库的开发和验证、建模规范的制定、SCADE 工具集与企业当前的工具链融合（如模型的配置管理、追溯等）等。

### 4.2　SCADE 基于模型开发的优势

① 基于模型的开发技术已日渐成熟，RTCA 在 DO-331 中已经明确基于模型开发在适航审定中的活动及目标。国外主流的飞机和发动机研制单位已经广泛采用 MBD 来开发机载软件，SCADE 是他们的首选工具且反馈情况很好。

② 民航机载软件最终需要通过适航认证，而 KCG 是目前唯一通过了 DO-178C A 级认证的自动代码生成器，KCG 能节省编码过程并保证代码和模型的一致性，相应的验证工作也能大量裁减。此外，SCADE 的 Qualified Reporter 能自动生成很多与适航认证相关的文档，提高适航审定的质量和效率。

③ 与其他 MBD 工具比较。SCADE 支持与 DOORS 需求管理工具、Reqtify 追踪工具、IBM Rational 配置管理工具的交互，能快速融入到软件研发体系流程中。

### 4.3　SCADE 基于模型开发的不足

① SCADE 不支持包括单精度浮点型等多种数据类型。在生成代码后，需要设计人员对数据类型定义进行手工替换，若没有替换或替换不完全，极易造成

CPU 崩溃,风险很高。

② 为节约处理器资源,目前 FADEC 软件中大量使用位域结构,但 SCADE 不支持位域。

③ SCADE 不支持位运算。

④ FADEC 软件的可调整参数,在模型中使用 Sensors 类型时,生成的代码只生成头文件 Sensor.h,没有对应的源文件,需要开发人员手动定义,当可调整参数很多时,手动定义工作量大且易引入错误。

总的来看,使用 SCADE 作为 FADEC 软件开发工具是适合且十分必要的。一方面,基于模型开发与传统软件开发模式相比有很多优势。另一方面,与其他 MBD 开发环境相比较,SCADE 的高安全性更适合 FADEC 软件开发。但是,同所有开发工具一样,SCADE 也不是完美的,其存在的不足促使 SCADE 软件本身的不断优化升级。同时,也需要软件工程师不断探索和总结,以保证软件的质量和安全。

## 5 结束语

本文探索 SCADE 基于模型开发在航空发动机控制软件研制中的应用。研究了 SCADE 的两种 MBD 解决方案。使用 SCADE 建模仿真工具、QTE 和 MTC 模型测试分析工具以及 KCG 自动代码生成器,完成健康管理模块软件开发。以 Simulink Gateway 为桥梁,联合使用 Simulink 和 SCADE 完成推力矢量模块软件开发。并在模型层级和系统层级对两个软件进行了验证。分析了两种 MBD 方案的选择考虑和适用范围,并总结了 SCADE 用于机载软件开发的优势和不足。所探索的 SCADE 基于模型开发解决方案和工程应用实践,具有一定的工程指导意义。后续将对 SCADE 时间堆栈分析以及 SCADE 与 Simulink 的联合仿真等技术进行探索。

**参考文献:**


[1] 刘杰.基于模型的设计及其嵌入式实现[M].北京:北京航空航天大学出版社,2010.

[2] 邓焱弢,骆光照,陈哲,等.基于模型设计的处理器在回路联合仿真系统[J].测控技术,2011,30(3):45-48.

[3] RTCA,Inc. Model-Based Development and Verification Supplement to DO-178C and DO-278A: RTCA DO-331[S]. 2011.

[4] 邢亮,卢伟.机载适航标准 DO-178B/C 软件开发过程研究[J].航空计算技术,2016,46(6):73-75.

[5] 李虎,马晋,郑凤,等.SCADE 模型驱动开发过程研究及高安全性分析[J].航空电子技术,2013,44(1):15-19.

[6] 王群伟,吴成富,陈怀民,等.基于 SCADE 的无人机三余度飞控系统设计及验证[J].测控技术,2007,26(4):52-54.

[7] ESTEREL Technologies. Efficient Development of Safe Avionics Software with DO-178B Objectives Using SCADE Suit® [Z]. 2012.

[8] ESTEREL Technologies. Gateway Guidelines for Simulink® [Z]. 2014.

[9] 方伟,周彰毅.SCADE 在航空发动机 FADEC 软件开发中的应用[J].航空发动机,2016,42(5):43-47.


□

(上接第 95 页)


[4] 彭大志,王艳.基于混合粒子群算法的无线传感器网络路由协议[J].测控技术,2014,33(7):93-97.

[5] 韩进,陈树.受限节点的 WSNs 非均匀分簇算法应用研究[J].传感器与微系统,2014,33(2):19-22.

[6] 汪华斌,罗中良,曾少宁.一种能量均衡的无线传感器网络分簇路由协议[J].测控技术,2015,34(5):89-92.

[7] Heinzelman W B, Chandrakasan A P, Balakrishnan H. An application-specific protocol architecture for wireless microsensor networks[J]. IEEE Transactions on Wireless Communications,2000,1(4):660-670.

[8] 刘铁流,巫咏群.基于能量优化的无线传感器网络分簇路由算法研究[J].传感技术学报,2011,24(5):764-770.

[9] 郑国强,李建东,周志立.多跳无线传感器网络的高能效数据收集协议[J].软件学报,2010,21(9):2320-2337.

[10] 郑国强,李建东,李红艳,等.多跳无线传感器网络的高效中继节点快速选择算法[J].通信学报,2010,31(11):158-170.

[11] 刘唐,彭舰,陈果,等.基于密度控制的传感器网络能量空洞避免策略[J].计算机学报,2016,39(5):993-1006.

[12] 赵志信,郭继坤,彭保.基于功率控制的无线传感器网络节点定位算法[J].黑龙江科技大学学报,2012(2):168-171.

[13] 黄廷辉,伊凯,崔更申,等.基于非均匀分簇的无线传感器网络分层路由协议[J].计算机应用,2016,36(1):66-71.

[14] 廖福保,张文梅,李向阳,等.无线传感器网络中一种新的非均匀分簇路由协议[J].小型微型计算机系统,2015,36(6):1265-1270.

[15] 岳丽颖,戴月明,吴定会.一种能量优化 WSNs 非均匀分簇路由协议[J].计算机工程与应用,2015,51(15):80-85.

[16] 冯江,茅晓荣,吴春春.一种能量均衡有效的 WSN 分簇路由算法[J].计算机工程,2012,38(23):88-91.


□