SCADE 在航空发动机 FADEC 软件开发中的应用

方　伟,周彰毅
(中航工业航空动力控制系统研究所,江苏无锡 214063)

摘要:为了探索 SCADE 开发环境在基于模型设计(MBD)的软件开发中的优势,理解其建模和自动代码生成机制,研究其在基于模型的测试和覆盖率分析中的实现方法,基于某型航空发动机 FADEC 系统的健康管理软件开发,应用了 SCADE 开发环境的建模、仿真、测试及覆盖率分析、代码生成与集成的全流程的 MBD 开发方法,并进行了完整的系统测试,测试用例全部通过。系统测试的结果验证了基于 SCADE 开发环境进行 FADEC 软件开发的正确性和可靠性,为 SCADE 开发环境在航空发动机 FADEC 软件开发中的应用提供了技术指导和工程借鉴。

关键词:MBD;覆盖率分析;自动代码生成;SCADE;航空发动机
中图分类号: V233.7　　**文献标识码**:A　　doi:10.13477/j.cnki.aeroengine.2016.05.008

Research on SCADE for Aeroengine FADEC Software

FANG Wei, ZHOU Zhang-yi
(**AVIC Aeroengine Control System Institute, Wuxi Jiangsu 214063, China**)

Abstract: To explore the advantage of Safety Critical Application Development Environment (SCADE) development environment in software development using Model Based Development (MBD) method, apprehend its modeling and auto-code generation mechanism, research its implement method of test and coverage analysis based on models, the full MBD development processes, include modeling, simulation, test and coverage analysis, code generation and integration were used based on the health-monitor software development of an aeroengine. The totally system test was completed and all the test scripts were passed. The correctness and reliability of FADEC software development, based on SCADE development environment, were verified according to the results of the system test. The technique and project guidance of SCADE development environment on aeroengine FADEC software development are supplied by these researches.

Key words: MBD; coverage analysis; auto-code generation; SCADE; aeroengine

0　引言

传统的软件开发是以代码为中心的 V 型开发流程,软件生命周期的重点是编码。以编码为核心的软件开发严重依赖编码者的项目经验和编码水平,容易引入语法和逻辑错误,可靠性和效率较低,在软件开发早期很难及时发现软件中潜在的错误;调试工作繁琐复杂,开发周期长,且需要借助复杂的专业工具软件进行单元测试和覆盖率分析,增加了软件开发的成本。验证工作在软件开发的后期进行,工作量大、难度高,且无法对验证工作进行定量评价,导致软件交付的周期长、成本高。

在基于模型的开发(MBD)中,设计人员根据系统需求建立模型,并对模型进行仿真测试,及早发现其中的缺陷并不断进行修正和验证迭代,最后直接通过模型生成和移植可执行的嵌入式代码。基于模型的开发在设计阶段就能不断暴露软件缺陷并进行封闭,且省去了手工编码和单元测试的工作,开发人员把更多精力集中到软件设计和控制算法优化上。

SCADE (Safety Critical Application Development Environment)是 1 个基于模型的应用开发环境,专注于高安全性系统的开发[1]。GE、PW 和 RR 公司基于 SCADE 开发了多款航空发动机的 FADEC 系统。在基于 SCADE 进行航空发动机 FADEC 系统开发方面,

收稿日期:2016-03-01　　**基金项目**:国家重大基础研究项目资助
作者简介:方伟(1987),男,硕士,从事 FADEC 软件研发工作;E-mail:fangwei1702@163.com。

引用格式:*方伟,周彰毅. SCADE 在航空发动机 FADEC 软件开发中的应用初探[J].航空发动机,2016,42(5):43-47. FANG Wei, ZHOU Zhangyi. Research on SCADE for aeroengine FADEC software[J]. Aeroengine, 2016, 42(5):43-47.*

PDF pdfFactory Pro　www.fineprint.cn

国内尚未见使用，探索 SCADE 在航空发动机控制领域的应用，建立 1 套以 SCADE 为核心的 FADEC 软件开发方法具有十分重要的意义。

本文深入分析 SCADE 开发环境的建模机制，并结合其在某型航空发动机健康管理软件中的具体应用，探索了基于 SCADE 进行 FADEC 软件开发的基本流程和技术要点，验证了基于 SCADE 进行 FADEC 软件开发的正确性和可靠性，为其在航空发动机 FADEC 软件开发中的应用提供了工程借鉴。

1 SCADE 的优势及其机制分析

1.1 SCADE 的优势

SCADE 作为高安全性嵌入式软件开发环境，覆盖了嵌入式开发的整个流程：需求建模、图形化模型搭建、静态检查、模拟仿真、形式验证、覆盖率分析、代码自动生成、文档生成等[2]。多个客户的实践经验表明，使用 SCADE 工具，可以生成 70%以上的嵌入式代码，节约 50%以上的开发时间[3]。相比于传统的手工编码开发流程，其具有如下的特点和优势：

(1)采用形式化设计方法[4]，以严格的数学理论保证了设计的完整性和无二义性；

(2)使用图形化建模方式[5]，易学易用，降低了对开发人员编程经验和熟练度的依赖，也减少了开发人员的工作量；

(3)通过 DO-178B 质量认证的代码生成器KCG，可以自动生成高质量的产品级 C 代码，代码与模型严格一致。简化了传统开发模式中的编码过程，且避免了手工编写代码引入的人工错误，提高了软件的可靠性。此外，无需对所生成的代码进行单元测试，节省了开发时间，提高了开发效率[6]；

(4)提供高效可靠的仿真和测试手段，可对各软件开发阶段进行定量的验证[7]。

1.2 SCADE 的建模机制

SCADE 建模的核心是同步设计程序语言 LUSTRE。LUSTRE 语言基于反应式系统和同步假设的概念，构成了 SCADE 建模的基础，在此之上进行模型构建、静态检查、模拟仿真、形式验证、覆盖率分析、代码自动生成等工作[8]。SCADE 提供建模的方式主要有 2 种：数据流图和安全状态机。

采用面向过程的思想描述系统数据流图。首先将系统模型描述为从输入到输出的信息流和数据变换过程，然后应用图形化的操作符搭建模型。这种方式适合于连续控制系统的建模，以用户定义的输入输出变量为接口，采用类似于 C 语言中函数概念的操作符为基本功能单元，在操作符内部选择使用图形或文本方式实现逻辑处理。操作符之间通过运算符，如算术运算符、逻辑运算符、比较运算符、时序运算符、选择操作符等组成更加复杂的层次结构，相互连接组成大的节点，最终实现以图形化的方法搭建软件模型。

安全状态机是有限状态机的图形化实现。通过引入丰富的形式化方法[9]来处理复杂的状态结构，适用于离散化控制逻辑。它提供了顺序、优先级、层次、并行的状态结构。安全状态机的图形化方法可以很好地对反应系统建模，用一系列的状态、转移和信号来表示反应系统的控制逻辑。用状态间的转移来表示系统的进展，用外部中断或内部事件处理结果来触发转移。状态代表系统的模式，分为“激活”和“不激活”2 种状态。不同的状态之间有互斥和并行 2 种组合关系：互斥意味着同一时刻仅有 1 个状态处于激活状态；并行则代表所有的状态都可能在同一时刻处于激活状态。并行的状态应该在其父状态被激活时同时被激活，激活顺序一般按照“从外至里，从上至下”的规则进行[10]。

1.3 SCADE 的代码生成机制

SCADE 代码自动生成的原理是根据建模平台的当前目标系统模型，由代码生成器 KCG 自动生成某种语言的源代码[11]。具体来说，生成代码的信息来源有 2 个：模型属性(控制代码生成方式)和元素规范(控制代码生成内容)[12]。由 SCADE 图形开发界面生成高质量的嵌入式代码。先将图形转换为 LUSTRE 语言[13]，如前文所述，SCADE 的图形描述符实质上是建立在 LUSTRE 语言基础上的，这一步就是把参数块、方程式等图形转化为 LUSTRE 语言描述，后删除图形信息，并将多个文件进行整合；再将 LUSTRE 描述文件转换为 C 代码，并生成可追踪文件。

可控制的生成过程如图 1 所示。将用于生成代码的 SCADE 模型作为 KCG 的输入文件，根据目标平台选择相应的 KCG 版本及所需的优化选项，最后一键式或者用命令行方式生成代码，其间会同时产生代码生成日志和错误信息以供参考。

2 SCADE 基于模型的测试及覆盖率分析

根据高层需求建立的可视化 SCADE 模型，是对

PDF pdfFactory Pro www.fineprint.cn

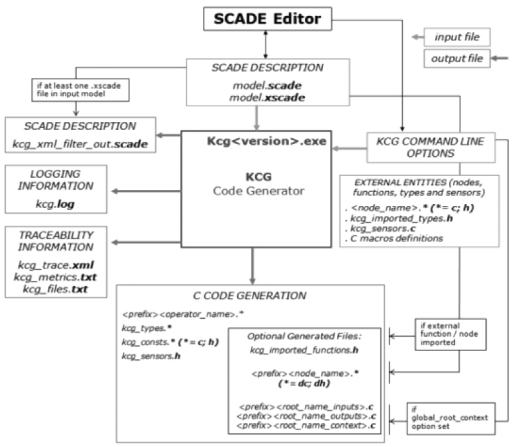

图 1　KCG 生成代码过程

控制逻辑和控制算法的详细描述,模型可用于早期的验证和测试,并进行覆盖率分析[14]。SCADE 基于模型的测试与基于源代码的测试不同。基于源代码的测试中,测试者忽视需求,仅确认代码完成其行为(甚至是错误行为),不能找出未实现的需求。SCADE 基于模型的测试则是基于高层需求的测试,测试者基于高层需求编写测试场景,通过 SCADE 的工具集 QTE(Qualified Testing Environment)和 MTC(Model Test Coverage)对模型进行测试和覆盖率分析。覆盖率分析包括模型对系统需求的覆盖(验证所有系统需求已通过 SCADE 模型实现)和 SCADE 模型的结构覆盖(验证 SCADE 没有实现非预期的功能)。在软件级别为 A 级的航空发动机控制软件中,DO-178B 要求的模型结构覆盖目标为 MC/DC 准则 100%覆盖。模型测试和覆盖率分析流程如图 2 所示。

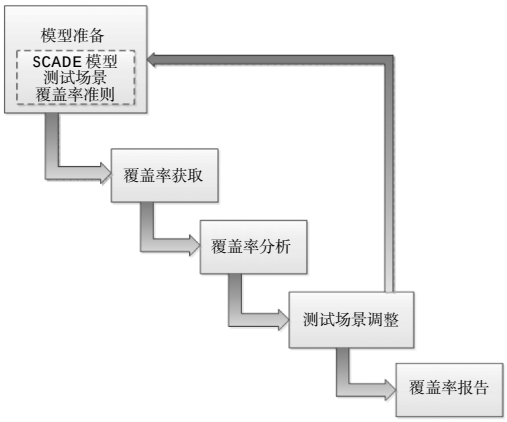

图 2　模型测试和覆盖率分析流程

3　基于 SCADE 的发动机健康管理模块应用层软件开发

某项目的健康管理模块主要实现发动机故障诊断、监视告警、寿命统计等功能,是发动机全权限数字电子控制系统控制软件的重要组成部分。健康管理模块分为应用层(AS)和操作系统层(OS),应用层作为控制律层,实现发动机健康管理和寿命统计功能。本节基于 SCADE 环境,采用基于模型设计的开发方式对 AS 层进行开发,探索 SCADE 在基于模型设计中的建模、仿真验证、测试及覆盖率分析、代码生成和集成验证的完整 MBD 解决方案。

3.1　控制律建模

首先利用 SCADE 提供的基本模块,搭建所需的自定义模型库,主要包括计数器模型(Counter)、故障确认和清除模型(Confirm And Restore)。故障确认和清除模型,用于监视告警模块中的故障确认和故障清除,利用计数器模型,当输入连续 Confirm Periods 个周期都为 True 时,输出结果为 True,确认故障;当输入值连续 Restore Periods 个周期都为 False 时,输出结果为 False,清除故障。其结构如图 3 所示。

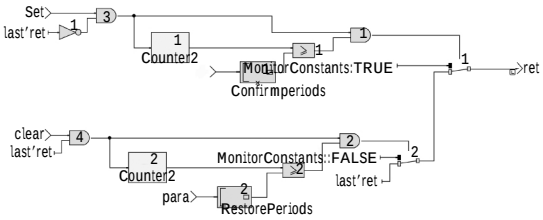

图 3　故障确认和清除模型

应用层模型采用层级结构,自底向上建模,底层使用自定义的模块库或 SCADE 自带的模块库,对各层级的模型进行封装,形成功能清晰的操作符,每个操作符对应嵌入式代码的 1 个源文件。顶层模型分为 Life Manage 和 Monitor2 大模块,如图 4 所示。对于控制软件中常用的可调整参数,在 SCADE 模型用 Sensor 类型参数来定义。

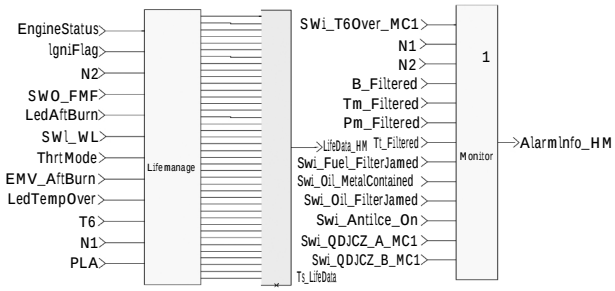

图 4　顶层模型结构

3.2　基于需求的模型仿真

SCADE 的仿真器能仿真调试 SCADE 模型。

PDF pdfFactory Pro　www.fineprint.cn

SCADE 仿真是 1 种基于后台代码的仿真，在起动仿真前，SCADE 首先将模型生成代码，在代码层级上进行仿真，而不是在对模型解析基础上的仿真[15]。针对健康管理模块中寿命统计模块的起动工作时间，根据需求设置对应的输入，仿真结果如图 5 所示。

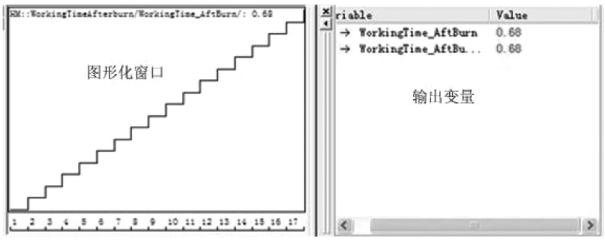

图 5 起动工作时间模块仿真结果

3.3 模型测试和覆盖率分析

仿真结束后，针对 AS 层的软件需求，编写测试场景，对模型进行测试和覆盖率分析，覆盖率准则为 MC/DC 覆盖准则，部分测试场景脚本如图 6 所示。根据获取的覆盖率数据，针对未覆盖的分支增加测试场景，对确定不需要经过的分支增加说明。根据 MC/DC 覆盖率准则，AS 层模型需要覆盖的分支为 651 个，满足 100%覆盖率编写的测试脚本为 812 行，并需增加 46 个说明。

```
# Test Fuel_FilterJamed 测试燃油忧虑堵告警功能
SSM::set Fuel_FilterJamed true
SSM::check HM::HealthMonitor/AlarmInfo_HM.Fuel_FilterJamed true
SSM::cycle 1

SSM::set Fuel_FilterJamed false
SSM::check HM::HealthMonitor/AlarmInfo_HM.Fuel_FilterJamed false
SSM::cycle 1

# Test Starter_NtcOver 测试起动机超转功能
SSM::set QDJCZ_A true
SSM::set QDJCZ_B false
SSM::check HM::HealthMonitor/AlarmInfo_HM.Starter_NtcOver true
SSM::cycle 1

SSM::set QDJCZ_A false
SSM::set QDJCZ_B true
SSM::check HM::HealthMonitor/AlarmInfo_HM.Starter_NtcOver true
SSM::cycle 1

SSM::set QDJCZ_A false
SSM::set QDJCZ_B false
SSM::check HM::HealthMonitor/AlarmInfo_HM.Starter_NtcOver false
SSM::cycle 1
```

图 6 测试脚本

3.4 代码生成和集成验证

SCADE 的代码生成器 KCG 通过了航空航天与防务领域的 DO-178B A 级标准。在经过模型仿真和测试后，通过 KCG 生成的代码与模型保持严格的一致性，生成的代码不需要作软件单元测试，可直接用于代码集成和系统验证。在 KCG 的配置时，为减少代码规模，对顶层模型外的所有模块进行扩展，以顶层模型的操作符为根节点，输入输出变量作为参数传递给根节点函数，只生成 1 个源文件。为输入输出变量配置接口函数，Sensor 类型的参数在生成的代码中没有定义，只进行了声明，所以需对该类型的参数进行定义。生成的代码作为嵌入式软件的一部分直接集成到软件中，在数控系统地检验证环境中对健康管理模块进行系统测试，应用层软件需求对应的测试用例全部通过验证，验证了模型和代码的正确性。

4 结束语

（1）通过对 SCADE 开发环境的机理分析，验证了 SCADE 开发环境所具备的易学易用、设计完整无二义的特点，加之其拥有通过 DO-178B A 级标准认证的代码生成器和完整可靠的仿真测试工具链等优势，极大的提高了软件开发效率、提升了软件安全性。

（2）在具体项目上的应用也证实了基于 SCADE 开发环境进行 FADEC 软件开发的正确性和可靠性，对其应用于 FADEC 软件开发具有工程指导意义。

参考文献：

[1] Jean-Louis C. Efficient development of airborne software with SCADE auite [M]. Elancourt: Esterel Technologies,2003: 1-2.

[2] Berry G. The constructive semantics of pure esterel draft V3[M]. Elancourt: Esterel Technologies, 1999: 4-6.

[3] 林枫. 基于 SCADE 的形式化验证技术研究 [J]. 测控技术,2011,30(12):71-74.
LIN Feng. Research on SCADE-based formal verification technology[J]. Measurement and Control Technology,2011,30 (12):71-74. (in Chinese)

[4] 李耀，郭进，孔令晶，等. 基于 SCADE 的形式化验证技术的改进研究[J]. 计算机工程与设计,2013,34(6):2026-2030.
LI Yao, GUO Jin, KONG LingJing, et al. Research on improvement of SCADE-based formal verification technology[J]. Computer Engineering and Design, 2013,34(6):2026-2030.(in Chinese)

[5] 吴成富，侯晓梅，段晓军. 基于 SCADE 的机载余度管理软件开发[J]. 电子设计工程,2013,21(3):96-98.
WU Chengfu, HOU Xiaomei, DUAN Xiaojun. Development of the redundancy management software based on SCADE[J]. Electronic Design Engineering, 2013,21(3):96-98. (in Chinese)

[6] 林枫. 基于模型的民用飞机软件开发技术研究[J]. 工业控制计算机,2011,24(12):37-41.
LIN Feng. Research for model-based development technology of civil aircraft's software [J]. Industrial Control Computer [J]. 2011,24(12):37-41.

PDF pdfFactory Pro www.fineprint.cn

[7] 胡钢伟,李振水,高亚奎. SCADE 软件开发方法研究[J]. 系统仿真学报, 2009(20):286-288.
HU Gangwei, LI Zhenshui, GAO Yakui. A research on software development methods with SCADE [J]. Journal of System Simulation,2009(20):286-288. (in Chinese)

[8] 杜道山, 李从心. 模型驱动在数控系统开发中的应用研究 [J]. 青岛大学学报(工程技术版),2005,20(3):53-59.
DU Daoshan, LI Congxin. Application of model-driven development technology in open CNC system[J]. Journal of Qingdao University (Engineering and Technology Edition), 2005, 20(3):53-59. (in Chinese)

[9] 石刚,王生原,董渊,等. 同步数据流语言可信编译器的构造[J]. 软件学报,2014,25(2):341-356.
SHI Gang, WANG Shengyuan, DONG Yuan, et al. Construction for the trustworthy compiler of a synchronous data-flow language[J]. Journal of Software, 2014, 25(2):341-356. (in Chinese)

[10] 陈淑珍, 陈荣武, 李耀. 基于 SCADE 的安全软件开发方法研究[J]. 铁路计算机应用,2015,24(3):14-18.
CHEN Shuzhen, CHEN Rongwu, LI Yao. Method of SCADE-based safety software development [J]. Railway Computer Application, 2015, 24(3):14-18. (in Chinese)

[11] 金平. 基于 SCADE 的余度管理软件开发方法研究[J]. 软件导刊,2012,11(10):14-16
JIN Ping. Research on the development methods of redundancy management software based on SCADE [J]. Software Guide, 2012, 11(10):14-16. (in Chinese)

[12] 章晓春,金平,孙全艳. SCADE 平台下的图形化设计和代码自动生成[J]. 软件,2011,32(5):74-77.
ZHANG Xiaochun, JIN Ping, SUN Quanyan. Modeling and autogeneration of C code on SCADE bench[J]. Software, 2011, 32(5):74-77. (in Chinese)

[13] 张合军, 陈欣. 基于 SCADE 的无人机自主导航飞行软件设计[J]. 计算机测量与控制,2007,15(10):1400-1402.
ZHANG Hejun, CHEN Xin. Software design of autonomous navigation Flight for UAV based on SCADE [J]. Computer Measurement and Control, 2007, 15(10):1400-1402. (in Chinese)

[14] 张雅妮,李岩,李小勋. 基于 SCADE 的飞控软件的适航验证与确认[J]. 飞行力学,2012,30(1):34-37.
ZHANG Yani,LI Yan,LI Xiaoxun. Airworthiness validation and accreditation for SCADE- based flight control software [J]. Flifht Dynamics, 2012, 30(1):34-37. (in Chinese)

[15] 颜雯清,李秀娟. SCADE 平台下 C 代码的自动生成[J]. 计算机仿真,2007,24(10):264-267.
YAN Wenqing, LI Xiujuan. Auto-generation of C code on SCADE bench[J]. Computer Simulation, 2007, 24(10):264-267. (in Chinese)

(编辑:赵明菁)

PDF pdfFactory Pro　www.fineprint.cn