

基于领域构件的余度管理软件平台研究与实现

刘海亮, 屈华敏, 武方方, 姚龙辉

(中航工业西安飞行自动控制研究所 软件工程中心, 陕西 西安 710065)

摘 要: 采用基于面向特征领域分析方法对余度管理进行领域分析与建模的技术, 构建了余度管理软件需求与设计构件库, 并建立构件库管理分类检索机制, 实现了一种余度管理软件共性构件快速配置和组装方法, 搭建了具备跨平台验证和开发能力的层次化余度管理软件通用开发平台. 实践证明, 该软件开发平台可以有效提高余度管理软件的可靠性, 并显著缩短软件开发周期.

关键词: 飞控系统; 余度管理; 领域分析; 共性构件

中图分类号: TP311.5

文献标识码: A

文章编号: 1000-7180(2015)12-0100-05

Research and Implementation of Domain Components Based Software Development Platform of Redundancy Management

LIU Hai-liang, QU Hua-min, WU Fang-fang, YAO Long-hui

(Software Research Center of AVIC Xi'an Flight Automatic Control Research Institute, Xi'an 710065, China)

Abstract: This paper researched on domain analysis and modeling technology on redundancy management (RM) based on feature-oriented domain analysis method, and generated a requirement and design component library with classification retrieval mechanism. A rapid configuration and assembly method for general components was proposed, and a layered RM development platform which is equipped with cross-platform verification and development capability was constructed at last. The practice proved that this platform could greatly improve RM software reliability and reduce development time.

Key words: flight control system, redundancy management, domain analysis, general component

1 引言

在飞行控制系统软件中, 余度管理软件通过为飞控系统增加多重软件资源, 实现对多重软件资源的有效管理, 提高飞行控制系统软件的容错能力、可靠性和安全性. 余度管理软件的主要功能包括采集信号的监控表决、计算机余度管理、总线设备监控、伺服作动器监控以及故障申报与综合等功能.

随着多余度飞控系统设计日趋复杂, 传统的余度管理软件开发过程中存在的问题逐渐暴露. 首先, 余度管理软件在需求阶段不能有效进行需求复用, 在设计阶段无法有效实现构件复用; 其次, 余度管理软件体系架构不具备很好的可扩展性, 其中控制平面的通用算法逻辑与型号定制算法逻辑没有实现完

全解耦合, 导致在进行具体项目的余度管理软件开发时, 往往需要根据项目特定需求对通用算法进行适应性更改, 影响了软件的可靠性; 再次, 在余度管理软件的数据平面, 存在大量传感器信号、离散开关信号以及总线信号等复杂信号, 通过传统人工编码方式实现数据平面工作量繁重, 并且容易出错; 最后, 目前的余度管理软件与具体的机载操作系统、硬件驱动接口紧密关联, 如果系统实验环境不具备, 缺乏仿真环境对余度管理软件进行有效验证.

研究表明, 基于领域工程的领域构件技术利用了领域工程的内聚性和稳定性等特点, 使其更有利于提高软件的复用和软件质量^[1-3]. 其中, 面向特征提取的领域分析方法 (Feature-Oriented Domain Analysis Method, FODA) 是由卡内基-梅隆大学的软

件工程研究所提出的面向特定领域进行领域共性特征分析、领域建模和实现的指导性方法^[4-6]。

2 FODA 领域分析方法

面向特征的领域分析方法 FODA,将面向特征的需求规格组织方式引入到领域工程的研究中,通过记录领域具有的相对稳定的特征以及特征之间的关系反映整个领域的软件需求。领域模型以系统的方式捕捉、表示分析结果,并通过模型形式化地表示所获得的知识,以支持软件复用。FODA 的过程分为三个阶段:上下文分析、领域建模与构架建模^[7-9]。

上下文分析的目标是定义领域的范围,划分领域的边界,在这个阶段要分析领域与外部领域间的关系以及输入/输出交互。

在确定领域范围后,在领域建模阶段会分析领域中应用的一致性和差异性,并产生领域模型。领域建模阶段主要包含三种行为。

(1)特征分析:在特征分析阶段,要获得客户或最终用户对一类系统的一般能力的理解,即特征。特征描述了领域应用的上下文、需要的操作和属性,以及表示的变化。

(2)信息分析:在信息分析中,需要定义和分析领域中应用所需的领域知识和数据需求。信息分析的目标是用领域实体及其相互之间的关系表示领域知识,从而在操作分析和构架建模中可以用来派生对象和数据定义。

(3)操作分析:在操作分析中,主要实现识别领域中应用的行为特性,包括数据流和控制流的共同性和差异性,同时针对领域中的应用进行有限状态自动机模型等。

在构架建模阶段为领域中的应用提供软件整体解决方案。在这个阶段中需要进行体系架构设计,软件架构是对系统整体结构设计的,包括全局组织与控制结构,针对领域建模后形成的构件进行有效组织与管理,并可以快速针对领域构件进行检索与组装,有效形成软件整体解决方案,同时在这个阶段需要根据领域特征开发对应的领域工具,从而有效地提高领域软件的开发效率。FODA 主要步骤和相互关系如图 1 所示。

3 余度管理领域上下文分析

余度管理上下文分析的主要目的是确定余度管理领域范围、余度管理与其他相关领域的关系以及余度管理的输入输出等。

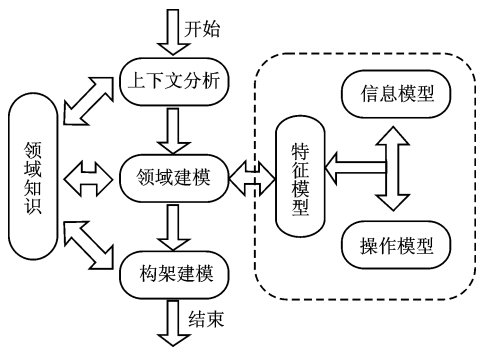


图 1 FODA 方法流程

余度管理软件负责整个多余度飞控系统信号的监控、表决与故障综合等任务,主要与数据接口单元、地面维护 BIT 软件、系统调度软件、常量只读存储器、控制律软件、故障记录非易失存储器等领域存在数据交互。余度管理软件上下文分析的结果如图 2 所示。

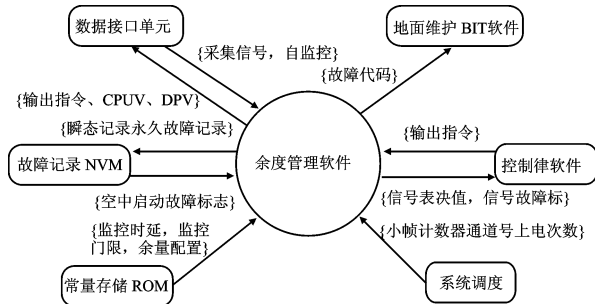


图 2 余度管理软件领域上下文分析

4 余度管理软件领域建模

根据 FODA 方法,余度管理领域建模主要包括特征分析、信息分析与操作分析,分别对余度管理领域的共性构成部分、数据需求和行为特性进行描述与建模,并以系统的方式捕捉和表示分析结果,通过模型化的方式表示所获得的领域知识。

(1) 特征分析

余度管理软件领域特征分析的主要工作是描述领域功能属性,以形成具备特定功能的可复用特征域构件。余度管理软件特征域包括传感器余度管理、离散量余度管理、数字量余度管理与故障恢复等模块,如图 3 所示。特征分析的结果是余度管理领域可以明确辨认的构成成分,具备相对独立的功能与可复用的价值,是余度管理软件领域的共性构成部分,它们存在于该领域的各个应用中。

(2) 信息分析

作为 FODA 领域建模的一个阶段,信息分析可以捕获并定义余度管理软件领域每个特征域中的数

据需求,以余度管理软件领域的传感器余度管理应用为例,信息分析如图 3 所示.信息分析阶段得到的数据需求在领域操作分析和领域构架建模中,可

以用来派生余度管理领域的对象和数据定义,是余度管理特征属性的定量描述.

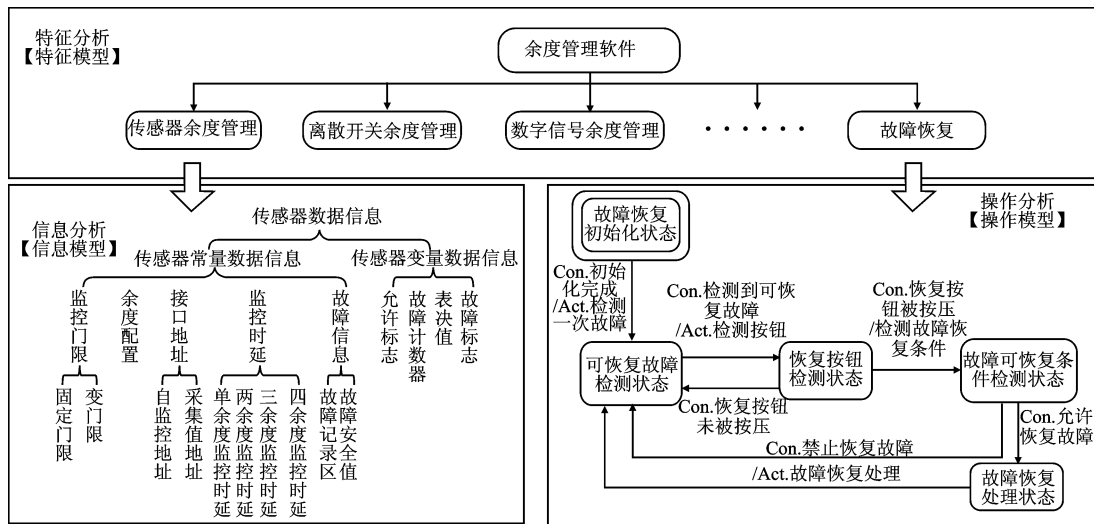


图 3 余度管理软件领域建模

(3)操作分析

操作分析的目的是为了获得领域的特征域的工作原理,提供一种直接理解领域中特征的方法,该阶段的重点在于捕获领域的行为特性.以余度管理领域中故障恢复应用为例,图 3 中描述了故障恢复的有限状态机操作模型,其中每个状态跳转表示特征域的一次操作,操作的数据参数即为跳转触发条件,触发条件来源自其他特征域交互,也可以来自领域边界外的数据输入.

综上的特征分析、信息分析和操作分析,完成余度管理软件领域的特征域的划分,特征域属性描述和行为方法描述,得出了领域构件设计的基本要素.

5 余度管理软件构架模型

余度管理领域构件的实现为余度管理软件复用提供了基础复用单元,但是应用领域中特定的应用环境差异仍会影响软件复用和软件质量,例如硬件接口、操作系统、运行配置等.余度管理软件通用平台是一个通用可配置的领域构件支撑架构平台,为余度软件开发提供构件管理、应用配置和跨平台特性.

飞控系统余度管理软件通用开发平台架构如图 4 所示,主要包括以下四层逻辑结构:余度管理应用层开发层,余度管理开发框架层,余度管理通用构件库以及操作系统与数据接口层.

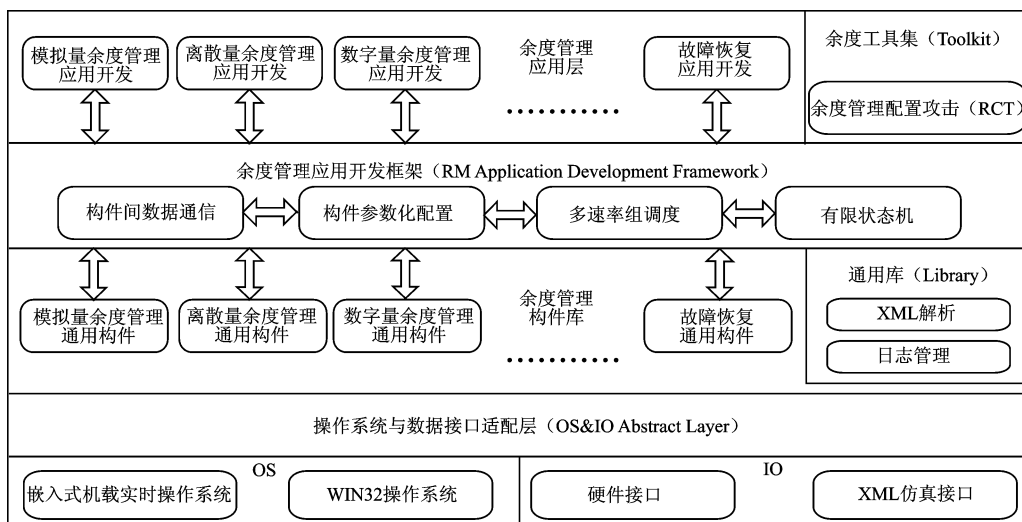


图 4 飞控系统余度管理软件通用开发平台架构

5.1 余度管理构件层

针对余度管理领域进行的领域分析与领域建模,从已有的余度管理系统挖掘出相对独立并且有复用价值的构件。余度管理构件层为余度管理通用体系架构的核心层,主要包括领域通用构件与基础应用构件。基于 FODA 领域分析方法,形成传感器余度管理、离散量余度管理、数字量余度管理以及故障恢复等领域共性构件库。同时包括 XML 解析库与日志管理等基础构件。在具体领域进行设计开发时,可以根据项目需求在通用构件库中进行构件的选型与集成,快速搭建余度管理软件解决方案。

值得指出的是,构件的复用过程是从需求到代码实现全流程的复用组装,这就涉及到构件库管理问题。构件库管理共性构件的需求、设计和代码实现等知识资产,余度管理构件层构建应用需求到构件设计,构件设计到代码实现标识索引机制,实现开发过程正向索引和逆向可追踪等功能,如图 5 所示。在余度管理领域的具体应用中,首先根据领域应用的具体需求,在通用构件库中检索相关构件,进行参数化模块配置,并基于标准接口进行构件的快速复合组装。

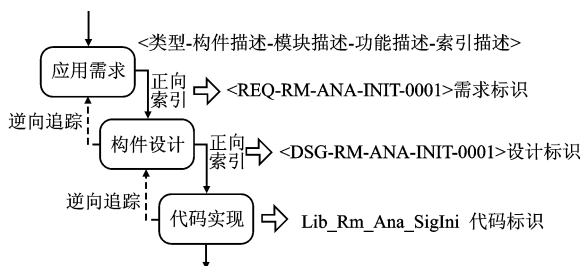


图 5 构件库管理原理

5.2 余度管理开发框架层

余度管理开发框架层支撑余度管理软件的体系结构,实现余度管理领域应用层与余度管理通用构件库的解耦合。主要包括构件间通信、参数化配置、多速率组配置与有限状态机设计。

余度管理领域构件具备标准的数据接口,开发框架层定义了标准构件之间的数据交互格式与数据通信方式。同时,针对不同的应用场景,开发框架层提供构件参数化配置机制,实现构件的定制,快速集成与组装。另外,不同的领域构件运行所属的调度速率组不尽相同,开发框架同样提供针对不同速率组对构件调度进行管理的功能,并实现与操作系统多速率组任务的统一调度接口。

5.3 余度管理应用开发层

余度管理应用开发层主要实现具体项目的余度

管理软件专用逻辑与算法,以满足不同项目的定制需求。该层利用配置工具选择构件组成,自动生成配置参数数据平面代码满足不同应用场景完成余度管理软件的快速开发。

余度管理配置工具基于 XML Schema 解决方案实现余度管理数据平面的配置与代码自动生成,如图 6 所示。余度管理配置工具主要包括规则配置器、配置编辑器、配置检查器以及配置生成器。其中规则检查器主要是用于编辑 Schema 文件,制定 XML 文件的逻辑结构;配置编辑器主要根据 Schema 文件编辑 XML 文件;配置检查器主要用于检查 XML 文件的关联规则;代码生成器根据 XML 文件生成定制的配置文件与数据文件。其中 Schema 用于描述和规范 XML 文档的逻辑结构,并验证 XML 文件逻辑结构的正确性。

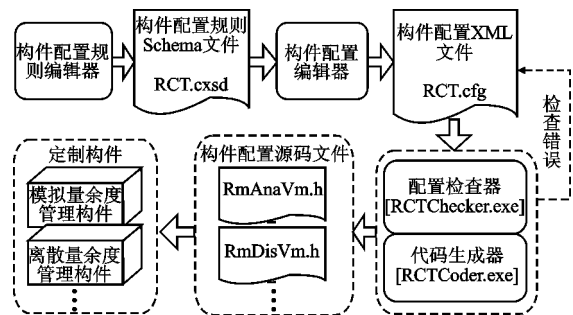


图 6 余度管理构件定制开发流程

5.4 操作系统与数据接口层

操作系统与数据接口层主要提供基础的操作系统功能以及数据接口访问功能,支持余度管理软件平台的可移植性。

为了支持余度管理软件的仿真功能,除了支持机载实时操作系统与硬件驱动接口外,还支持以 Windows 操作系统与 XML 数据接口为基础的余度管理软件仿真平台。同时,操作系统与数据接口层也为余度管理工具集中的余度管理验证工具提供了基础的平台与运行环境。

余度管理验证工具通过 XML 仿真数据接口,实现余度管理软件的自动化验证与故障场景数据还原。在余度管理验证工具中,通过数据接口适配层实现 XML 数据文件与余度管理内部数据接口的通信。余度管理软件跨平台综合验证流程工作原理如图 7 所示。

6 结束语

余度管理软件通用开发平台已经在多个重点课

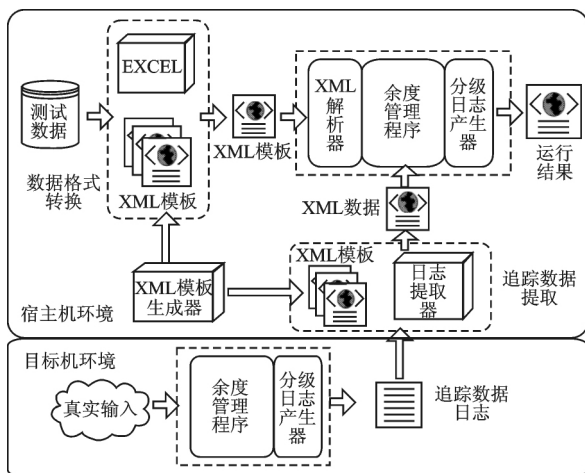


图7 余度管理跨平台综合验证原理

题中应用实践,与传统的余度管理软件开发相比,提高了余度管理软件开发效率与可靠性。在项目的软件需求分析阶段,可以有效地复用通用需求库中的共性需求,并针对项目专用需求进行分析,完成完整的软件需求过程。在项目的软件设计阶段,首先根据共性需求从通用构件库中进行构件选取与组装;其次根据项目专用需求完成定制算法的开发,完成完整的控制平面程序;最后利用余度管理配置工具录入配置信息,自动生成数据平面程序,对数据平面与控制平面进行集成,快速形成余度管理软件整体解决方案。最后可以依托操作系统与数据接口,结合XML数据接口仿真数据,即使在系统环境不具备的情况下,也可以有效地完成余度管理软件的验证与测试。实践证明,基于飞控系统余度管理软件通用开发平台可以提高软件设计的安全性、可靠性,缩短软件开发与验证的周期。

参考文献:

- [1] 杨美清,梅宏,李克勤. 软件复用与软件构件技术[J]. 电子学报,1999,27(2):69-75.

- [2] 张文,怀进鹏. 领域分析与建模研究[J]. 北京航空航天大学学报,2004,30(12):1225-1230.
- [3] Anderson William, Morris Ed, Smith Dennis, et al. COTS and reusable software management planning: A Template for Life Cycle Management[R]. Technical Report CMU/SEI-2007-TR-011, 2007.
- [4] 张伟,梅宏. 一种面向特征的领域模型及其建模过程[J]. 软件学报,2003,14(8):1345-1355.
- [5] Liu Mingyi, Zhou Xiaofeng. The application of domain engineering in MGIS development[C]// 2012 International Conference on Computer Science & Service System (CSSS). [s. l.]:IEEE, 2012.
- [6] Guo Ying, Wang Jun, Zhang Xiaoyan, et al. Domain service acquisition and domain modeling based on feature model[C]// IEEE International Conference on Computational Science and Engineering Dalian, Liaoning:IEEE,2011:26-33.
- [7] Robert Krut, Nathan Zalman. Domain analysis workshop report for the automated prompt and response system domain[R]. Technical Report CMU/SEI-96-SR-001, 1996.
- [8] 宋翔贵. 电传飞行控制系统[M]. 北京:国防工业出版社,2003.
- [9] 保鹏飞. 嵌入式软件的构件化模型的研究[D]. 长沙:国防科学技术大学,2011.

作者简介:

刘海亮 男,(1982-),硕士,工程师.研究方向为容错处理软件设计技术研究.

屈海敏 女,(1970-),本科,研究员.研究领域为安全性软件体系架构.

武方方 男,(1977-),博士,高级工程师.研究领域为安全性软件设计与验证.

姚龙辉 男,(1988-),硕士,助理工程师.研究领域为容错处理软件设计技术研究. E-mail: yaolonghui@126.com.

(上接第99页)

- [8] Allen G, Swift G, Carmichael C. Virtex-4VQ static SEU characterization summary [J]. JPL, NASA, 2008,15(6):68-83.
- [9] Monson J S, Wirthlin M, Hutchings B. Fault injection results of linux operating on an FPGA embedded platform[C]//Proc Int Conf ReConFig Comput. FPGAs: IEEE, 2010:37-42.
- [10] Carl Carmichael, Chen Wei Tseng. Correcting single-event upsets in virtex-4 FPGA configuration memory

[J]. xilinx Corporation,2009,10(1):128-134.

- [11] Johnson E. Estimating the Dynamic Sensitive Cross Section an FPGA design through Fault Injection[M]. Utah: Department of Electrical and Computer Engineering, Brigham Young University, 2005.

作者简介:

李林 男,(1990-),硕士研究生.研究方向为单粒子翻转故障注入算法. E-mail:lilin_jeas@163.com.