Computer Science and Application 计算机科学与应用, 2019, 9(7), 1232-1238
Published Online July 2019 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2019.97138

Hans汉斯

Research of Reliability and Safety Testing Method for FPGA Software

Yong Hu[1], Yun Liu[2], Cheng Gao[2], Yuecong Sun[2], Tingting Wang[2], Wei Meng[2]

[1]Beijing Special Mechatronics Institute, Beijing
[2]Beijing Jinghang Computing and Communication Institute, Beijing
Email: iamyunliu@hotmail.com

Received: Jun. 24th, 2019; accepted: Jul. 4th, 2019; published: Jul. 11th, 2019

Abstract

According to the characteristics of aerospace FPGA software, the reliability and safety testing technology of FPGA software is studied in the Software profile analysis. On the basis of the method, the reliability and safety test method of operation profile for aerospace FPGA software is developed, and the simulation is used. It can simulate a variety of faults and automatically collect the results of the output, to obtain FPGA inefficiency and other measurement data. Based on this method, a reliability and safety test tool based on running profile is developed, which can be used to generate the reliability and security test script of FPGA software test and obtain the measurement basic data such as failure rate required by reliability and safety measurement model of FPGA software, effectively improving the reliability and safety test of aerospace model FPGA software.

Keywords

FPGA Software, Reliability and Safety Test, Operation Profile, Test Tool

FPGA软件可靠性安全性测试方法研究

胡　勇[1]，刘　芸[2]，高　程[2]，孙跃聪[2]，王婷婷[2]，孟　伟[2]

[1]北京特种机电研究所，北京
[2]北京京航计算通讯研究所，北京
Email: iamyunliu@hotmail.com

收稿日期：2019年6月24日；录用日期：2019年7月4日；发布日期：2019年7月11日

摘　要

依据航天型号FPGA软件特点研究FPGA软件可靠性安全性测试技术，在软件剖面分析的方法基础上，形成适用于航天型号FPGA软件的运行剖面可靠性安全性测试方法，利用仿真工具对各种故障进行模拟并自

文章引用: 胡勇, 刘芸, 高程, 孙跃聪, 王婷婷, 孟伟. FPGA 软件可靠性安全性测试方法研究[J]. 计算机科学与应用, 2019, 9(7): 1232-1238. DOI: 10.12677/csa.2019.97138

动对输出的结果进行采集，获取FPGA失效率等度量数据。依据该方法开发了基于运行剖面的可靠性安全性测试工具，可用于FPGA软件可靠性安全性测试脚本的生成，以及获取FPGA软件可靠性安全性度量模型所需要的度量基础数据，有效地提高了航天型号FPGA软件可靠性安全性测试效率。

关键词

FPGA软件，可靠性安全性测试，运行剖面，测试工具

1. 引言

由于 FPGA 具有集成度高、体积小、功耗低、速度快等诸多优点，在航空、航天军用产品领域中获得了广泛应用，安全关键程度普遍较高。未来航空、航天领域 FPGA 的应用将呈现快速增长的趋势，FPGA 软件质量成为影响装备质量和战斗力生成的重要因素。与传统软件不同，FPGA 的设计过程繁杂，涉及的工具较多，因此容易在设计过程中引入影响安全性可靠性的问题。

目前软件可靠性安全性理论包括运行剖面、随机过程、软件可靠性模型、统计估计和顺序采样理论等方面。但在型号研制中，这些理论大多过于抽象、操作性较差，实际应用的效果并不理想。因此，课题中选取故障发生概率作为可靠性度量元，主要通过基于运行剖面的可靠性安全性测试方法来获取。

FPGA 与传统软件的运行方式不同，它采用的是并行执行的处理方式，在航天型号中，多用于配合处理器进行底层的协处理操作。航天型号 FPGA 与其它领域的 FPGA 及软件在安全性可靠性上有所差别，传统的剖面分析方法并不适用于航天型号 FPGA 软件的风险分析。因此，需根据航天型号 FPGA 运行特点，在软件剖面分析的方法基础上，形成适用于航天型号 FPGA 的剖面运行方法。同时利用仿真工具对各种故障进行模拟并自动对输出的结果进行采集，获取 FPGA 失效率等可靠性安全性度量数据。

2. 软件运行剖面构造方法及充分性分析

2.1. 软件运行剖面构造方法

在软件可靠性安全性测试领域，运行剖面一直是研究的核心内容，美国的 AT&T 实验室的 Musa 教授提出了运行剖面及其构造方法，将软件运行剖面定义为“操作和它们的发生概率的简单集合”[1]，在运行剖面的建立过程包括：构建客户剖面、用户剖面、系统模式剖面、功能剖面和运行剖面。

一般情况下，软件可靠性安全性测试都是按照用户实际使用软件方式来进行测试[2]，最常用的用户实际使用软件方式是用运行剖面来实现的，这一方法有助于生成软件可靠性测试数据，支持测试的执行。国际上最常用的运行剖面是由 Musa 提出的，包括构建运行剖面的五个步骤[1]，分别是：确定客户剖面、定义用户剖面、定义系统模式剖面、确定功能剖面和确定运行剖面。Musa 定义的运行剖面主要强调操作及其发生概率，而不严格强调输入之间的相互约束和时序关系。

2.2. 测试充分性

基于 Musa 运行剖面的软件可靠性安全性测试是以失效率这一软件可靠性指标是否满需要求作为测试充分性的判定标准。失效率是指单位时间内发生的失效数[3]，数学表达式为：

$$FI = \frac{f}{t} \tag{1}$$

FI (failure intensity)代表故障率，f代表发生故障总数，t代表软件的执行时间。基于运行剖面的测试中，设运行剖面$OP = \{(O_1, P_1), (O_2, P_2), ...(O_n, P_n)\}$，$f_i$为操作$O_i$发生的概率，$t_i$为操作$O_i$测试过程中的执行总时间。则失效强度可以表示为：

$$FI = \sum_{i=1}^{n} \frac{f_i p_i}{t_i} \tag{2}$$

由于运行剖面的精确性对失效率估计的准确性影响较低[4]。测试得到时效率可以视为软件实际的故障强度，因此可以用失效强度作为可靠性测试充分性的判定指标[5]。这样既考虑了软件自身的功能性，也考虑了使用方式等外部因素对软件可靠性安全性的影响。

3. FPGA 软件特点分析及运行剖面构造方法

3.1. FPGA 软件特点分析

FPGA (Field Program Gate Array)软件为高层次的硬件描述语言，完成逻辑功能设计，加上约束文件经过综合和布局布线，生成烧写文件，下载到 FPGA 芯片上，完成所需要的逻辑功能。FPGA 实时高效性、硬件的相关依赖性等方面的特点和嵌入式软件系统相似，但是 FPGA 软件的专业背景很强，根据其特点从接口数据、实现过程及运行环境三个方面与嵌入式软件进行比对分析，如表 1 所示。

Table 1. Comparison between embedded software and FPGA Software
表 1. 嵌入式软件与 FPGA 软件特点比较

比较点	嵌入式软件	FPGA 软件
接口数据	输入数据有约束关系，无参数时序要求	输入数据有约束关系，且遵循一定的接口参数时序要求
实现过程	包括源代码设计及集成两个阶段	包括源代码设计、逻辑综合、布局布线及配置文件加载四个过程
运行环境	运行环境与硬件密切相关	FPGA 运行环境与硬件密切相关，FPGA 本身是硬件电路

3.2. FPGA 软件运行剖面构造方法

根据航天型号 FPGA 运行特点，在软件剖面分析的方法基础上，可形成适用于航天型号 FPGA 的剖面运行方法。首先按照功能层次结构，自顶向下的把用户使用软件的输入空间划分为系统模式剖面，把系统模式剖面划分为功能剖面，最后把功能剖面划分为运行剖面[6]。依据 FPGA 的运行剖面，开展测试用例的设计。根据不同功能的使用概率，合理的分配测试用例，使发生概率高的功能分配到更多的测试用例。

构造运行剖面的步骤如下：

- 首先，按照需求规格说明中的功能要求分解为若干的被测功能，生成一个功能清单。
- 其次，为每个被测功能确定与接口激励之间的因果关系，构造功能剖面。
- 最后，确定每一个激励发生的概率，完成运行剖面的构造。

由于 FPGA 在运行过程中各个接口工作并行度非常高[7]，且航天型号 FPGA 与其它领域的 FPGA 及软件在安全性可靠性上有所差别，在进行剖面分析的时候需要同时分析各个接口的作用和影响，以形成对可靠性安全性产生影响的运行场景，如图 1 所示。

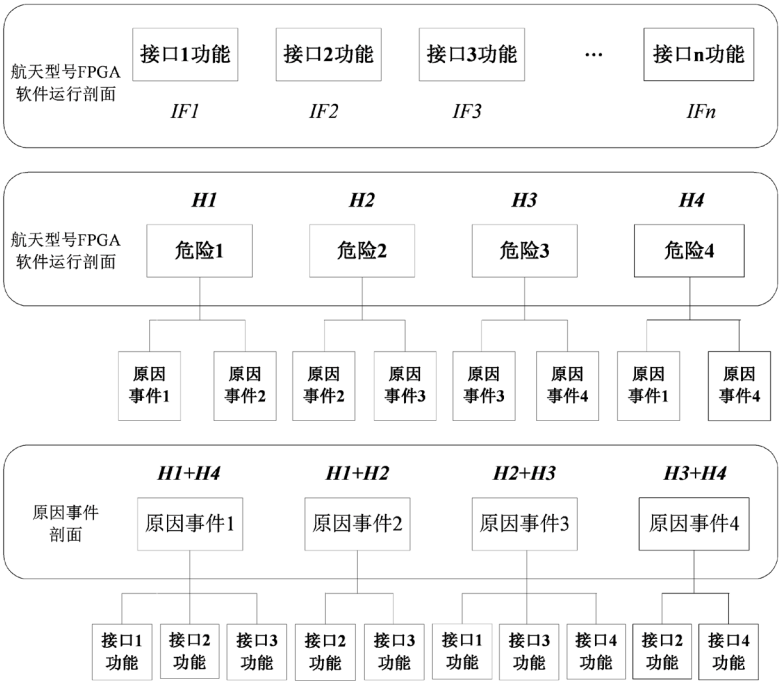

Figure1. Analysis of risk profile of space model FPGA software
图 1. 航天型号 FPGA 软件风险剖面分析

分析结束后，需要构建大量的场景级测试用例并执行。传统方法对于 FPGA 的测试一般是采用实物测试的方式，由于 FPGA 芯片工作在电路版上，在开展实物测试过程中，验证的剖面只能基于 FPGA 的接口运行剖面。而对于 FPGA 的危险剖面和原因事件剖面，往往由于缺少故障注入或结果采集的手段而难以被验证，导致测试不充分，无法获取到开展可靠性安全性评估所需要的度量元基础数据。

采用 EDA 仿真测试方法对 FPGA 软件开展可靠性安全性测试。通过借助 EDA 仿真工具，我们能够在数字化的环境中，对 FPGA 的程序开展测试。在数字化环境中，我们可以通过编程的方式很容易的实现对各种故障的模拟[8]，从而充分的验证 FPGA 实现的功能。

在仿真时，我们能够按照所设置的约束条件自动生成 FPGA 的测试激励，利用仿真工具能够自动对输出的结果进行采集，再通过计算得出某一故障的发生概率，即可用于 FPGA 可靠性安全性度量元的计算。例如，针对单粒子事件的模拟，可以约束单粒子事件发生的概率，随机在门级网表中注入该故障，在 TESTBENCH 工具中自动对功能模块的输出结果与预期结果进行比较，统计一段时间内发生错误的次数，即可得到该功能模块的失效率。

采用 EDA 仿真测试方法针对 FPGA 接口测试时，还可以结合所积累的典型测试用例库以及典型仿真接口模型库，通过对测试用例以及测试激励的重用，使测试的效率获得大幅的提高。另外，由于脱离了硬件环境，仿真工作还能够在多台计算机上同时开展，使所需的测试时间进一步被缩短。

4. 基于运行剖面的可靠性安全性测试工具

由于在不同的航天型号的通讯过程中存在各种不同类型接口的数据帧和命令帧，不同种类的 I/O 指令，它们的数据体的格式、边界、类型可能各不相同，相关的 I/O 指令发出时刻以及约束条件区别很大。在实施相关动态测试用例时，他们均需要准确定义。在可靠性安全性测试时，这些数据的数据量是庞大的，靠人工生成会导致工作效率低下且可能测试用例不充分的情况，所以开展基于运行剖面的可靠性安全性测试，需研制基于运行剖面的可靠性安全性测试工具。

基于运行剖面的可靠性安全性测试工具主要包括：FPGA 激励注入功能、半自动化的测试数据生成功能、测试用例选择功能、测试结果分析功能、数据导入导出功能和测试数据事后处理功能。测试工具的功能框图如图 2 所示。

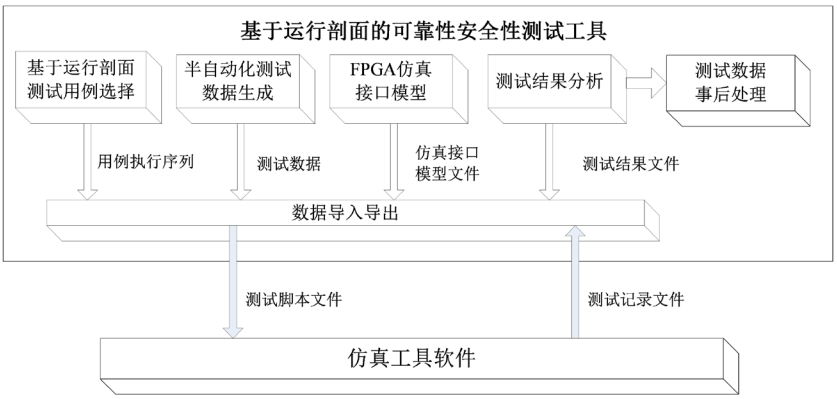

Figure 2. Functional diagram of reliability safety testing tool based on running profile
图 2. 基于运行剖面的可靠性安全性测试工具功能框图

主要完成的功能如下：

1) FPGA 激励注入功能

针对 FPGA 设计中典型功能、典型协议、典型接口及硬件环境，利用 FPGA 仿真接口模型搭建配置项仿真测试环境，结合测试数据生成功能产生的测试数据，实现故障注入功能。故障树分析功能图如图 3 所示。

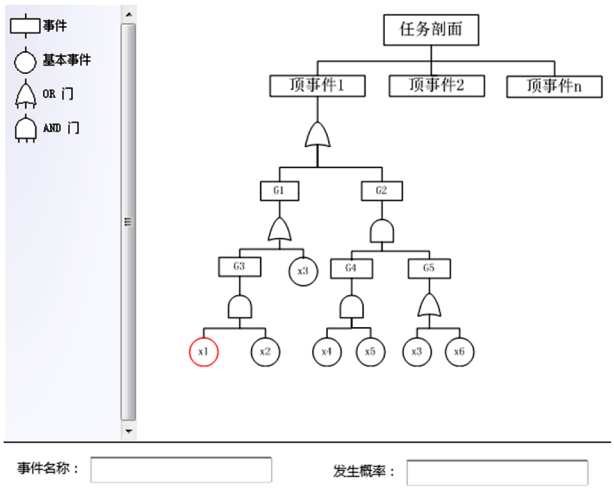

Figure 3. Tree analysis function diagram
图 3. 故障树分析功能图

2) 半自动化的测试数据生成功能

依据数据规则模型，定义待生成数据规则。依据数据生成规则，通过解析数据规则信息和选择待生成的数据类型，生成指定数量的数据。待生成的数据为正常数据时，系统从规则定义各字段正常值中自动选择对应数据类型的正常值；若生成为异常数据，可自定义需生成异常数据的字段，系统从规则定义各字段正常值范围外自动选择对应数据类型的异常值。测试用例设计功能图如图 4 所示。

Figure 4. Test case design function chart
图 4. 测试用例设计功能图

3) 测试用例选择功能

根据对应的功能执行层次以及执行概率，按既定的规则或随机选择测试用例，直到执行完整个软件的所有运行剖面。测试用例选择功能图如图 5 所示。

Figure 5. Test case selection function chart
图 5. 测试用例选择功能图

用例选择过程的基本步骤如下：

第一步：根据任务书以及需求规格说明书，人工创建软件功能列表，将各功能以唯一标志区分出来；

第二步：根据各上级功能要求，创建该功能条件下的子功能列表，将他们以唯一标志区分开来，并与其上级功能绑定在一起；

第三步：如果还有下级子功能，则继续第二步；

第四步：建立功能间以及功能本身的约束条件，可能包含以下内容：a) 功能 1 是功能 2 或功能 3 的必要条件；b) 功能 2 需要功能 3 的执行结果；c) 在某一段时间内，若不执行功能 1 则执行功能 2；d) 可以单独执行的子功能；e) 必须在主功能执行成功的条件下，才能使用相应子功能；f) 某一功能需重复执行多次；g) 在功能 1 执行不成功的情况下，不能执行功能 2。约束条件在生成用例序列时候可以用来判断该序列是否符合要求。

第五步：根据用户对测试对象的使用情况，生成运行剖面树，对于该树的每一个节点目前暂定有 3

个属性：a) 该功能在当前条件下的执行概率，b) 执行该功能时，正确执行所有操作的概率和出错的概率，c) 执行该功能所需要的时间。

第六步：根据运行剖面树，结合该树的第五步中的各项属性以及第四步的功能约束条件生成测试用例序列，直到树的顶端，并且可以按照设定的循环次数选择多次循环，生成不同的用例序列。

4) 测试结果分析功能

能够人工输入测试用例的预期输出结果以及通过准则，系统能够根据预期输出结果及通过准则自动对实测结果进行判断，确定实际输出结果是否正确，并给出测试用例通过与否的标志。

5) 数据导入导出功能

数据导入导出功能主要实现基于运行剖面的可靠性安全性测试工具与仿真工具之间的数据交换，将工具产生的用例信息转换为仿真工具能够识别的文件格式，由仿真工具来执行测试用例，在用例执行完毕后，再将测试结果文件读入到基于运行剖面的可靠性安全性测试工具中，以便进行结果分析。

6) 测试数据事后处理功能

为了计算软件可靠性，需要对测试过程中生成的故障数据进行计算，从大量的测试数据中找出导致软件故障的测试用例及相应的测试结果，根据故障数据进行某一故障的发生概率计算，并作为可靠性度量元。

5. 结语

本文依据 FPGA 软件的特点提出了基于运行剖面的 FPGA 软件可靠性安全性测试方法，并根据此方法开发了 FPGA 软件可靠性安全性测试工具，使用该测试工具生成测试用例效率高、功能覆盖全面。下一步工作将在本论文测试工具获取的可靠性度量元基础上，对 FPGA 软件可靠性安全性度量模型进行研究。

参考文献

[1] Musa, J.D. (1993) Operational Profiles in Software Reliability Engineering. *IEEE Software*, **10**, 14-32. https://doi.org/10.1109/52.199724

[2] 蔡建平. 软件可靠性测试方法新探[J]. 计算机工程与设计, 2009, 30(20): 4658-4661.

[3] 黄锡滋. 软件可靠性、安全性与质量保证[M]. 北京: 电子工业出版社, 2002.

[4] Musa, J.D. (1994) Sensitivity of Field Failure Intensity to Operational Profile Errors. *IEEE International Symposium on Software Reliability*, Monterey, 6-9 November 1994, 334-337. https://doi.org/10.1109/ISSRE.1994.341399

[5] 马成功. 基于马尔可夫链模型的软件可靠性测试方法的研究[D]: [硕士学位论文]. 成都: 电子科技大学, 2009.

[6] 陈雪松, 陆民燕, 阮镰. 软件可靠性测试数据生成方法研究[J]. 航空学报, 2001, 22(6): 510-512.

[7] Xilinx Inc. (2007) Virtex-II Platform FPGAs: Complete Data Sheet. DS031.

[8] 狄超, 刘萌. FPGA 之道[M]. 西安: 西安交通大学出版社, 2004.

知网检索的两种方式：

1. 打开知网首页：http://cnki.net/，点击页面中“外文资源总库 CNKI SCHOLAR”，跳转至：http://scholar.cnki.net/new，搜索框内直接输入文章标题，即可查询；
   或点击“高级检索”，下拉列表框选择：[ISSN]，输入期刊 ISSN：2161-8801，即可查询。
2. 通过知网首页 http://cnki.net/顶部“旧版入口”进入知网旧版：http://www.cnki.net/old/，左侧选择“国际文献总库”进入，搜索框直接输入文章标题，即可查询。

投稿请点击：http://www.hanspub.org/Submission.aspx
期刊邮箱：csa@hanspub.org