安全级数字化系统软件测试用例生成方法研究

周俊燚,吴一纯,蔡源凤,施纯森

(厦门大学,厦门 361102)

摘要: 基于概率风险评价(PRA)和物理仿真模型,本文提出了一种针对核电厂安全级数字化控制系统的软件测试用例生成方法。所产生的测试用例包含了风险指引信息,能定性描述软件实际操作场景。文中以某核电厂保护系统子系统软件为例,分析系统的故障模式和子系统软件输入空间,建立软件的运行剖面,结合 RELAP5 仿真模型,获得了可用于测试核电厂安全级数字化控制系统软件可靠性的测试用例。该方法产生的测试用例为开展核电厂安全级数字化控制系统的软件可靠性定量评估研究奠定了基础。

关键词: 风险指引; 软件测试; 测试用例; 物理仿真模型; 概率风险评价

中图分类号: TL 362.1 **文献标志码:** A **文章编号:** 0258-0934(2017)8-0819-05

数字化技术的引入使得基于计算机和微处理器的数字化分布式控制系统(DCS)能提供更高的可靠性、更好的设备性能及更多的诊断功能。相对于模拟控制系统,数字化 DCS 主要的差别在于软件。开发高可靠性的核电数字化仪控系统的重要环节之一是保证其软件的可靠性。由于 DCS 是由软件、硬件和固件共同组成,失效机理独特。其软件可靠性评估最为困难,尤其是安全级软件的可靠性定量评估[1-2]。现有的软件可靠性定量评估方法主要有:软件可靠性增长模型、贝叶斯信度网(BBN)、统计学测试(STM)、流网模型法(FNM)等[3]。

软件测试是保证软件可靠性的重要手段之一,在开发高质量的软件产品中起着至关重要的作用,并且提出了贯穿生命周期的验证和确认(V&V)方法以达到软件的高可信度[4-5]。本研究通过结合概率风险评价(PRA)技术与软件测试技术,提出了一种核电厂安全级 DCS 软件测试用例的生成方法,选取某核电厂保护系统的冷却剂流量低保护子系统为对象,进行测试用例产生研究,并分析了测试有效性。

收稿日期: 2017-08-30

基金项目: 厦门大学能源学院发展基金(2017NYFZ01);福建省科技计划(2016H0034)资助。

作者简介: 周俊燚(1992—),男,重庆人,在读硕士生,攻读方向为核电厂数字化仪控系统软件可靠性定量评估。

1 方法简介

图 1 所示为软件测试用例生成过程流程图。针对软件可靠性的定量评估中软件测试用例的生成过程,采用基于概率风险评价的软件测试用例生成方法,通过将概率风险评价技术用于软件可靠性测试的测试用例生成过程,使得所产生的测试用例包含了概率风险特性。

1.1 PRA 模型场景识别

由传统概率风险评价分析方法可得到系统故障模型,其中包含系统风险分析的事件树与故障树[4]。进一步分析与待测保护软件的保护作用相关的故障类型,可识别为更高层级的概率风险评价场景,即与软件输入相关的故障树。通过分析高层级概率风险评价场景,可求得引起顶事件的最小割集和其相对频率。

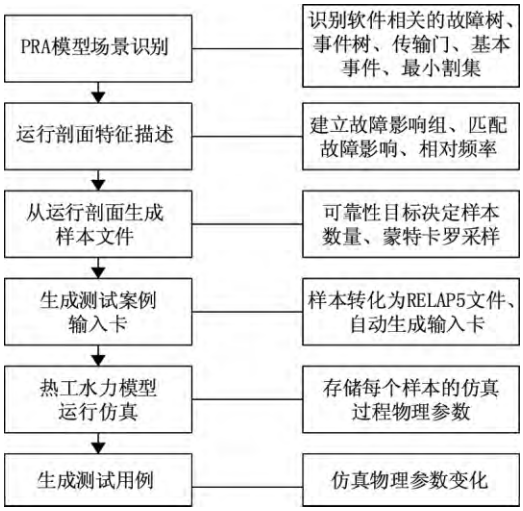

图 1　软件测试用例生成方法流程图

1.2　运行剖面特征描述

由系统特征建立故障影响组及相关概率失效模型，故障影响组用于定义系统故障类型，包含全部的故障影响，并能在搭建的物理仿真模型中注入故障影响组的故障。将最小割集依次与故障影响组进行匹配，匹配后的每组最小割集都有与其对应的故障影响组，结合最小割集的相对频率构成相关软件的运行剖面。所以，运行剖面包含了最小割集。相对频率以及对应的故障影响组，是用来描述软件的实际运行情况的。

1.3　运行剖面生成样本

通过从运行剖面中随机取样来定义每个样本，样本代表系统运行过程中可能发生的故障工况。取样内容：根据系统初始状况的概率分布所选择的系统初始状况；从高层级的概率风险评价场景中选取一个割集；以及割集对应的故障影响组的概率失效模型。

1.4　搭建物理仿真模型

为了得到尽可能真实的测试结果，测试应尽量在真实的环境下进行，但是针对低需求操作模式的软件，在真实的环境下进行测试不切实际，因此通过搭建仿真测试环境，即构建物理系统稳态模型进行仿真。在失效引入之后，模型能逼真模拟样本事件的失效影响。将取样样本转化成相应 RELAP5 输入卡。

1.5　生成测试用例

仿真模型运行仿真得到仿真过程数据结果，即产生的输出文件。提取输出文件中软件输入变化情况作为一组测试用例，每一个样本对应一组测试用例。

2　冷却剂流量低保护子系统

反应堆保护系统是核电厂仪控系统中重要的一部分，保护系统主要包括，紧急停堆系统(RTS)和专设安全设施驱动系统(ESFAS)，在发生事故工况时触发紧急停堆，并驱动专设安全设施按设计逻辑实施保护动作，属于安全级仪控系统，其拥有多个逻辑保护通道。研究中，选用了一次冷却剂流量低保护这一典型的保护逻辑通道作为测试对象。

典型压水堆一回路冷却剂设有三个环路，每个环路设置了三套相互独立的流量计。当每套流量计监测的流量低于额定流量的 88.8% 时，本套流量计给出流量低的信号。这三套流量计按“三取二”逻辑给出该环路流量低的信号。另外该环路的冷却剂泵断路器打开，也会给出该环路流量低的信号。其架构如图 2 所示，冷却剂流量低保护子系统的输入参数有反应堆功率(P)、冷却剂流量(Flow)和泵断路器状态，输出为停堆信号。

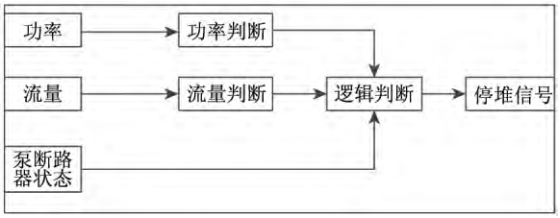

图 2　一次冷却剂流量低保护架构

冷却剂流量低保护子系统属于低需求操作模式软件，软件大多数时间内处于钝态，仅当特定状态发生时，软件才会执行设定功能，这类软件常与安全功能相关。传统的测试用例生成方法已不能满足软件测试需求，随机测试过程不能反映出实际系统运行状态，不能完全准确地测试软件响应过程。采用本文所述的测试用例生成方法可以有效克服上述缺陷，从而达到有效测试的目的。

3　测试用例生成过程

针对冷却剂流量低保护子系统，提取由概

率风险评价所得到的 PRA 模型中与一回路流量相关的事件树与故障树，结合软件输入空间，建立以冷却剂流量低为顶事件的流量异常故障树，如图 3 所示。

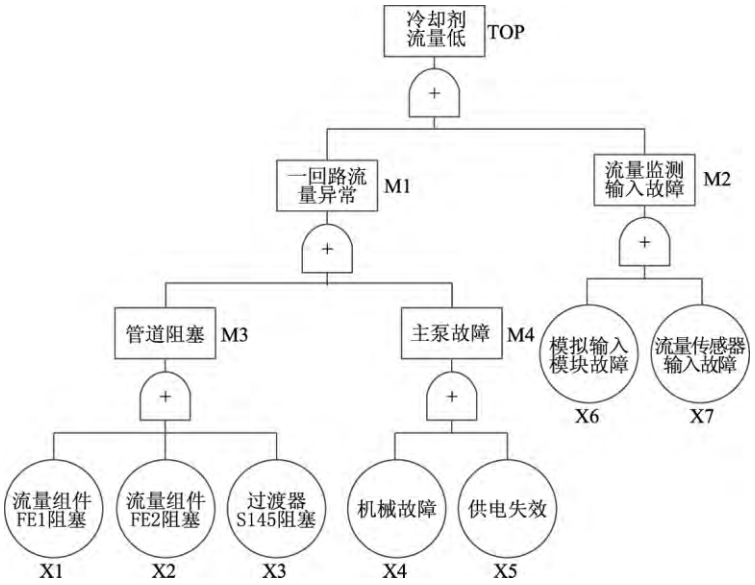

图 3　冷却剂流量低故障树

结合生成测试用例时并未使用具体割集，主要考虑的是故障影响，对主泵故障做了简化，例如主泵供电失效可以包含厂外电源失效、应急柴油发电机供电失效等。从系统的角度出发，将应急柴油发电机等供电系统作为一个整体部件考虑，其失效概率由风险分析获得，各部件失效概率数据参考了先进测试堆（ATR）系统 PRA 模型[6]。由 PRA 模型可知各底事件在引起冷却剂流量低事故中的相对频率，见表 1。

表 1　底事件相对频率数据

事件编号	X1	X2	X3	X4	X5	X6	X7
相对频率	5.36×10^{-3}	5.36×10^{-3}	3.91×10^{-1}	3.28×10^{-3}	5.58×10^{-1}	2.60×10^{-2}	1.10×10^{-2}

由系统特征及冷却剂流量低故障树，建立故障影响组：gFlow、gPump、gFctrlI[6]。三个故障影响组分别代表了管道阻塞故障、主泵故障、流量监测输入故障。结合底事件相对频率描述待测软件的运行剖面，见表 2。

表 2　系统运行剖面描述

编号	事件	相对频率	故障影响组	事件描述
1	X1	5.36×10^{-3}	gFlow	流量组件 FE1 堵塞
2	X2	5.36×10^{-3}	gFlow	流量组件 FE2 堵塞
3	X3	3.91×10^{-1}	gFlow	过滤器 S145 堵塞
4	X4	3.28×10^{-3}	gPump	主泵机械故障
5	X5	5.58×10^{-1}	gPump	主泵电气故障
6	X6	2.60×10^{-2}	gFctrlI	模拟输入模块故障
7	X7	1.10×10^{-2}	gFctrlI	流量传感器输入故障

运行剖面体现了软件输入变量与概率风险分析所得 PRA 模型的相关性，其故障影响组均能在物理仿真模型中仿真，进一步地，按照事件的相对频率进行蒙特卡罗随机采样事件及相关参数可获取样本，样本内容包含：（1）系统初始状况；（2）引起顶事件的一个底事件；（3）底事件对应的故障影响组及相关参数。一个样本即为一个测试场景，样本数量由软件可靠性目标决定。考虑到核电厂大部分时间处于满功率运行，在采样过程中，对系统初始状况做了简化处理，即系统初始状况为满功率运行。所得部分采样样本见表 3。

获得样本文件后，采用 RELAP5 构建系统热工水力模型，根据各样本文件产生对应的输入卡，运行输入卡获得样本条件下系统物理参

表 3　部分采样样本文件

样本编号	事件编号	故障影响组	相关参数 1	相关参数 2
1	X5	gPump	trip	1. 2
2	X3	gFlow	S145	5.650×10^{-4}
3	X4	gPump	seizure	0. 3
4	X6	gFctrlI	31. 28	NA

数变化情况。M310 改压水堆核电厂一回路系统由反应堆和 3 条并联闭合的冷却剂环路组成，每条环路包括 1 台主冷却剂泵、1 台蒸汽发生器以及相应管道和仪表组成，其中 1 条环路的热管段连接着稳压器[7]。由于 3 条环路基本一致，节点仅给出带有稳压器的一个环路，如图 4 所示。

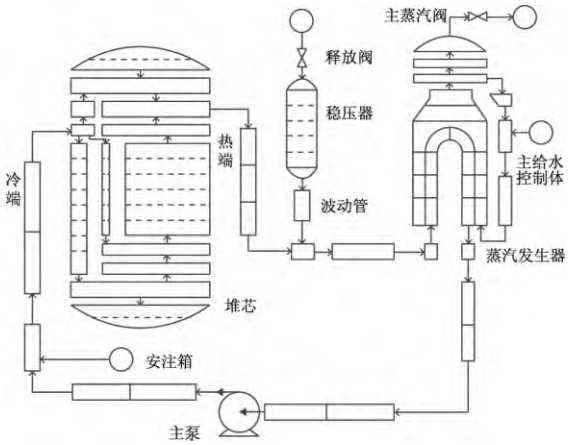

图 4　一回路系统节点图

所搭建的系统热工水力模型可针对故障影响组进行故障注入，根据样本产生对应的输入卡文件并进行仿真，得到系统物理参数变化情况。结合软件输入选择所需参数作为一组测试用例，针对一回路冷却剂流量低保护子系统，其输入包括反应堆功率(P) 、冷却剂流量(Flow) 和泵断路器状态(S) ，得到的测试用例为系统特定状况下软件输入空间的变化情况。样本编号 1 所得的测试用例，如图 5 所示，图 5 中曲线代表在主泵发生某种电气故障时，一回路流量变化情况，即待测软件输入变量冷却剂流量(Flow) 的变化情况。

此方法基于 PRA 技术，所得到的测试用例包含实际系统的风险与故障概率信息。对于保护系统软件等安全级软件，只有在系统偏离正常状态时，才会激励相应功能进行保护操作，通

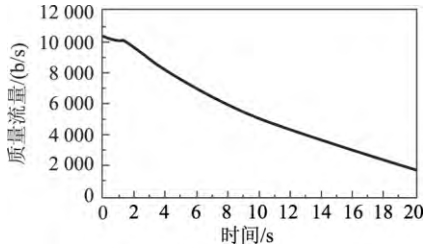

图 5　样本编号 1 所得测试用例

1 b = 10^{-28} cm^2

过结合物理模型仿真，突破了实际保护系统限制，可获得系统故障状况下的软件输入空间变化。可见，产生的测试用例能满足低需求操作模式软件的测试需求。

4　结论与展望

传统的软件测试用例生成方法不适用于诸如核电厂保护系统等低需求操作模式软件的可靠性定量评估需求，本课题从概率风险评价角度出发，结合物理模型仿真，生成用于核电厂安全级 DCS 软件可靠性测试的测试用例。并以某核电厂保护子系统软件为对象，获得包含实际系统的风险与故障概率信息的测试用例，提高了测试过程的合理性和有效性。综上所述，通过此方法产生的测试用例满足核安全级软件测试需求，可进一步用于此类低需求操作模式软件的可靠性定量评价测试。由于测试用例产生过程借助了软件模型仿真，该模型的精度将决定仿真结果与实际系统的偏差。提高建模精度、缩小偏差是本研究日后计划之一。

参考文献:

[1] 刘盈，杨明. 核安全级数字化仪控系统软件可靠性评估 [J]. 核动力工程，2016，37(1) : 143-147.

[2] 杨明，宋梦楚. 数字化仪控系统软件可靠性定量评估研究 [J]. 核动力工程，2014，35(1) : 54-58.

[3] Chu T L，Yue M，Martinez-Guridi G. Development of Quantitative Software Reliability Models for Digital Protection Systems of Nuclear Power Plants (NUREG/CR-7044) [R]. Washington，DC: USGPO，2013.

[4] 杨永祥，丁军. 核电站数字化仪控系统软件验证和确认实用手册 [M]. 厦门: 厦门大学出版社，2010.

[5] 水璇璇，吴一纯，吴志强，等. 反应堆 FPGA 保护子系统开发及验证 [J]. 核电子学与探测技术，

2015,35(10):1043-1047.
[6] Chu T L, Athi Varuttamaseni, Joo-Seok Baek. Development of A Statistical Testing Approach for Quantifying Safety-Related Digital System on Demand Failure Probability NUREG/CR-7234: [R]. Washington, DC: USGPO, 2017.
[7] 广东核电培训中心. 900 MW 压水堆核电站系统与设备 [M]. 北京: 原子能出版社,2005.

A Software Test Case Generation Method for Safety-Related Digital System

ZHOU Jun-yi, WU Yi-chun, CAI Yuan-feng, SHI Chun-sen

(Xiamen University, Xiamen 361102, China)

Abstract: Based-on probabilistic risk assessment (PRA) and the physical simulation model, a software test case generation method fit for nuclear power plant (NPP) safety digital control system is provided in this paper. The test cases generated by this method include risk-informed information, and could qualitatively describe the software operation scenarios. Using a NPP protection subsystem software as an example, by analyzing the system failure mode and the subsystem software input space, the operational profile is built. Combining with a RELAP5 simulation model, the test cases for safety-related digital system software reliability testing are obtained finally. The test cases generated with the method could be the base for software reliability quantitative assessment of NPP safety-related digital control system.

Key words: risk-informed; software testing; test cases; physical simulation model; probabilistic risk assessment