学校编码：10384　　分类号＿＿＿密级＿＿
学号：32420131152285　　UDC ＿＿

厦门大学

硕 士 学 位 论 文

基于马尔可夫区间映射方法的核电站可靠性分析软件平台开发及研究

Developing and Research on the Nuclear Power Plant Reliability Analysis Software Platform Based on the Markov/Cell-to-Cell Mapping Technology

赵旭
指导教师姓名：李　宁　教授
缪惠芳　副教授
专　业 名 称：核工程与材料
论文提交日期：2016 年 04 月
论文答辩时间：
学位授予日期：

答辩委员会主席：＿＿＿＿＿＿
评　　阅　　人：＿＿＿＿＿＿

2016 年 04 月

基于马尔可夫区间映射方法的核电站可靠性分析软件平台开发及研究

赵旭

指导教师 缪惠芳 副教授

厦门大学

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文(包括纸质版和电子版)，允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘 要

我国核电发展以“安全高效发展核电”为基本要求，要求在核电建设、运行过程必须在采用国际最高安全标准、确保安全的前提下进行。目前在建核电站已全部采用数字化仪控系统，但在使用传统静态故障树/事件树方法对核电站可靠性分析过程中发现，该方法无法对数字化仪控系统中的软件、硬件、人因作用交互等方面问题进行描述。动态概率安全分析方法便基于此环境下发展而来。马尔可夫区间映射方法（Markov/CCMT）方法是现有动态概率安全分析方法中弊端最小，优点最多的方法之一，但国内外尚无可用商用软件。

随着我国核电规模的迅速扩大，对于应用于核安全领域的概率安全分析（PSA）技术，亟需开发一套能反映数字化仪控系统特性的 PSA 方法软件平台。本文基于 Markov/CCMT 方法理论体系，开发了一套适用于核电站数字化仪控系统的可靠性分析软件平台。该平台可以与任意仿真软件进行集成并提取数据进行实时有效的分析，进一步提高了 PSA 分析的时效性与可靠性。该软件平台可完成针对数字化仪控系统从仿真到配置的整套操作过程。软件平台对计算结果从系统失效路径及各种设备故障模式的发生频率、概率等方面进行分析，从而向决策者提供必要的系统可靠性信息。

此外，本文还通过建立简单数字化液位控制系统模型，将所开发软件平台与 Matlab 集成进行系统概率安全分析，同时对可靠性分析软件平台中的各项内容进行说明。首先对数字化仪控系统中常见的计算机与控制器进行建模与简化，通过对设备状态的合理简化，大幅度减少计算规模从而使其在可执行范围内。随后调用 Matlab 软件中建立的系统模型，实现提取系统模型的液位变化数据，并返回软件平台进行数据分析工作。通过对计算结果的分析，显示数字化仪控系统中的数字化设备故障对于系统失效具有显著贡献。

关键词： 数字化仪控系统；概率安全分析技术；马尔可夫区间映射方法

Abstract

Developing nuclear power in a safe and efficient way is the basic requirement of our country, which means that the construction and operation process is necessary to be carried out under the highest international safety standards. At present, all nuclear power plants under construction have already adopted the digital instrument and control systems. However, when using traditional static event tree/fault tree method to make reliability analysis of nuclear power plant, people found that this method could not describe problems such as the interaction among software/ hardware/ human behaviors. Dynamic probabilistic safety assessment (DPSA) is advanced on the basis of this environment and Markov/CCMT method, which is one of the most positive methods with least defects and most advantages among the DPSA methods nowadays. But there is still no available commercial software based on Markov/CCMT.

With the rapid development of nuclear power industry in domestic, it is urgent to develop a set of PSA software platform which can reflect characteristics of digital instrument and control system. Based on Markov/CCMT method, this paper develops the software platform. This platform can be integrated with arbitrary simulator and then extract simulate result for real-time and effective analysis, which will further improve the timeliness and reliability of PSA. This platform can complete the whole operation process from simulation to configuration, and then analyze the system failure results. By this way, the platform could provide the necessary safety and reliability information for decision making.

In addition, by establishing a model of simple digital liquid level control system, this paper explains each aspects of reliability analysis software platform, and integrates Matlab with the platform to analyze the system safety and reliability. Firstly, this paper explains the modeling and simplified process of the digital system. And the calculation scale is definitely reduced to the executable range by reasonable simplification. Subsequently, this paper extracts the simulation result to compute the system failure probability and show the analysis result about the contribution of each component state

to the system failure.

Keywords: Digital instrumentation and control systems; Markov/CCMT; Probabilistic Safety Assessment

目 录

Contents

第一章 绪论

1.1 研究背景与意义

《核安全公约》中华人民共和国第六次国家报告中指出，核能作为一种安全、清洁、可靠的能源，对优化中国能源结构，保障能源安全，保护环境，应对全球气候变化，提升机电产业设备的装备制造能力等方面具有重要意义，也是中国能源与环境、经济协调发展的客观需要和战略要求[1]。截至 2016 年初，我国运行的核电机组 30 台，总装机容量 2831 万千瓦；在建的核电机组 24 台，总装机容量 2672 万千瓦。其中，在建的核电机组数量排名世界第一，总机组数量位居世界第三。2012 年 10 月，国务院审议通过了《核电安全规划》（2011-2020 年）和调整完善后的《核电中长期发展规划》（2011-2020 年）。规划提出以国际社会最新的核安全标准建设中国的核电厂并安排了核电建设规模，计划至 2020 年，运行核电装机容量达到 5800 万千瓦，在建 3000 万千瓦左右。预计到 2050 年，我国的核电装机容量将从目前的占电力总装机容量的 2%提高到 16%。

核能发展必须始终把核安全放在首要位置。概率安全分析技术是保证核电安全性的有效手段之一。2004 年修订发布的《核动力厂设计安全规定》及《核动力厂运行安全规定》明确提出了必须完成核动力厂的概率安全分析、以及必须考虑使用概率安全评价作为定期安全审查的输入等要求。2010 年，国家核安全局发布《概率安全分析技术在核安全领域中的应用》（试行）的通知，指出在保证核安全方面，确定论安全分析方法和概率安全分析方法是互为补充的；确定论安全分析方法采取保守的假设和分析，在以往对保证核动力厂的安全方面发挥了重要的作用；而概率论安全分析方法则使对安全问题的认识更加全面和深入，并且改进了确定论安全分析方法的某些不合理之处和局限性，是对确定论分析方法的补充或扩展；概率安全分析方法提供了对核动力厂风险水平的深入了解，这些有关风险的深入了解应该在决策过程中得以适当的体现[2]。

概率安全评价(Probabilistic Safety Assessment, PSA)又称概率风险分析(Probabilistic Risk Analysis, PRA)，是 20 世纪 70 年代以后发展起来的一种系统工程方法。它采用系统可靠性评价技术和概率安全分析方法对复杂系统的各种可能

事故的发生和发展过程进行全面分析，综合考虑他们的发生概率以及造成的后果，从而全面研究核电站系统设计和运行的风险[3]。

传统的静态 PSA 方法已经被用于核电站数字化仪控系统的可靠性建模，它主要采用故障树/事件树（Fault Tree/Event Tree，FT/ET）分析技术，目前工程上常用的软件是瑞典 Relcon Scandpower 公司开发的基于 FT/ET 的 RiskSpectrum 软件。中科院等离子体物理所于 2010 年开发了一套基于 FT/ET 的概率安全/可靠性分析专业软件系统 RiskA，该软件还没有工程应用。

仪控系统是监测核电站的安全与运行状况，并帮助调整应对核电站运行和维护的需要。与传统的模拟仪控系统相比，数字化仪控系统能提供更高的可靠性、更好的设备性能及更多的诊断功能。目前核电站正逐渐使用数字化仪控系统更新或取代传统模拟仪控系统，二代加、三代核电技术均将全部采用数字化仪控系统。由于数字化仪控系统包含硬件和软件，与单纯的硬件系统相比具有不同的失效模式，在计算机冗余软件的开发、故障统计数据的外推和共因故障模式的预测和验证等方面都存在困难，这些因素均导致目前对核电站数字化仪控系统的安全性和可靠性进行定量评估和风险分析成为核工业界公认的难题[4]。

故障树/事件树（FT/ET）分析方法得出的系统及其事故后果的静态分析结果对当前硬件状态和事故场景的历史情况有较好的描述[5]。随着核电站数字化仪控系统更新或取代传统的模拟仪控系统，当数字化仪控系统存在超过一种失效模式、控制环或软件/硬件/固件/人因等交互作用，FT/ET 分析方法就不能有效地对数字化仪控系统进行建模并解释两类交互动作[6-8]。此外，系统的不确定性也会影响事件发生的顺序[9]，而 FT/ET 分析方法的事件序列是由分析人员事先确定，而不同的事件序列会造成不同的事故后果[10]。在具有多个顶事件的控制系统中，由于顶事件之间存在相关性，在分析系统失效概率时，顶事件间的竞争关系可能会对顶事件的发生概率造成极大的影响，而 FT/ET 无法对此类竞争关系进行有效描述[11]。同时，在处理人因故障分析时，FT/ET 把人因故障按执行与不执行的二分法进行处理，而这种做法不能正确地分析人因故障对事故后果的影响[12]。Aldemir. T 等人的研究指出，在存在多重顶事件的过程控制系统中，顶事件间的竞争关系不仅与设备故障顺序有关，还与设备故障准确时间和设备故障时系统中过程变量的准确值有关[10, 11, 13, 14]，且这种关系会导致传统故障树/事件树方法在对控制系

统可靠性分析结果中与动态概率安全分析方法产生较大的差别。

虽然目前在可靠性与安全性领域对何种特定环境下需要使用动态概率安全分析方法尚未达成统一观点。在现行的核电厂系统可靠性分析中，仍主要以传统的静态事件树/故障树方法为主，如 AP600 和 AP1000 的 PSA 报告对于仪控系统就是应用传统 FT 方法得出计算结果[15]。但在对数字化系统和核电厂专设系统动态接口的可靠性分析以及对数字化系统本身硬件与软件的动态特性建模过程中，FT/ET 方法显得能力不足。需要使用动态 PSA 方法对具有软硬件与物理过程的交互作用的系统进行补充分析。因此建立一种新型的动态方法来模化数字化系统显得十分必要。

1.2 模拟仪控系统与数字化仪控系统

仪表和控制系统(Instrumentation and Control System，I&C)被认为是核电厂的中枢神经系统，核电站的安全性和经济性在很大程度上与仪表控制系统的性能水平有关[16]。自上世纪 70 年代开始，各国的核电站所采用的都是模拟反应堆仪控系统，其基于模拟器件，通过分立元件或者模拟集成电路以硬接线的方式实现其所有的功能[17]。

模拟系统经过长时间的应用与研究，在设计和应用方面已经积累了丰富的经验，具有响应速度快，设备的检验和分析鉴定相对简单，设计制造成本较低等优点，而且系统的可靠性和安全性也能满足要求，所以世界各国大多数在运行的核电厂直至本世纪初仍然使用模拟技术系统[18]。但是，模拟系统自身也的确存在着某些难于解决或无法解决的问题，其中最为突出的问题有[17]：

(1) 模拟技术系统算法简单而且精度较差，在某些情况下要求采取准确并且复杂的保护算法时，模拟系统难以实现；

(2) 由于模拟技术的特点，在超出维护周期的时候，可能会发生“仪表漂移”现象。“仪表漂移”是影响系统可靠性的一个重要的因素，而且其导致故障的概率将随时间增加以超线性的速度增长，这个问题仅依赖模拟技术很难解决；

(3) 系统定期检验所需的时间较长，而且系统不能实现实时在线检验功能；

(4) 模拟技术信息储存和显示的能力较差，难以显示监控变量的当前值与预

定值的关系以及变量的变化趋势，不能以符合人因工程的方式提供有关信息和状态显示；

(5) 数字化产品的普及，导致模拟系统备品备件缺少以及维修难度加大，这是已运行电站维修和更新换代中最为突出的问题之一，直接影响到核电站的经济性。

美国核管会(NRC)在对 LER (Licensee Event Report)数据库中 1994 年到 1999 年的数据进行统计的结果表明，有 8%的事件报告中包含了数字化控制系统失效的影响，有 9%的停堆事件是由数字化控制系统失效直接引起的[19, 20]。Bickel J.H 对美国第一代的七个核电站数字化反应堆保护系统所做的统计研究中，总计 127 万个小时的运行数据统计数据显示，总共发生的影响电站安全运行的事件有 141 起[21]。韩国原子能研究院的研究结果表明，数字化安全级控制系统失效对堆芯损毁的概率贡献在 6%到 10%之间。而据不完全统计，2000 年到 2005 年间，国内的 5 个在役运行核电站，共发生了非计划停堆 71 起，其中由控制系统导致的停堆就有 26 起之多[22]。

数字化仪控系统是指以微处理芯片构成的，以数字处理技术为特点的智能化电子设备和计算机系统，它除了具有常规测量仪表的测量和控制功能外，还具有极强的数据处理和通讯能力。它能将现场的信息通过计算机网络连到电厂的任何地方，从而使电厂操作员有可能对全厂各部分的设备进行集中监视、控制与管理。同时使得生产、运行、管理、维护、安全保卫、计算高度及行政部门都要能及时有效地利用这些信息，实现全厂信息共享，极大地提高核电厂运行安全性、可靠性及管理效率。相比于模拟仪控系统，数字化仪控系统有以下优点：

(1) 具有出色的控制精确性和很强大的逻辑运算处理、计算能力，显著提高了仪控系统的综合性能，完成模拟仪控系统所无法实现的复杂逻辑运算处理和计算功能；

(2) 以通信网络连接各系统设备，大大减少了连接电缆的数量，提高了数据传输的可靠性；

(3) 能够方便、有效地实现具有多重冗余、故障安全和容错等功能，提高了系统可用性和可靠性；

(4) 能够方便、有效地实现系统在线检查和自诊断功能，有助于故障分析和

判断；

(5) 系统扩展灵活性好、可组态性强，便于维护；

(6) 具有强大的数据处理、数据和存储能力，改善了人机接口

目前对于核电厂安全评估的研究焦点很多都集中在数字化仪控系统替代模拟仪控系统的转折点，但是对于模拟仪控系统和数字化仪控系统本身的特性却较少被描述。缺乏这些关键概念的认识将会导致我们不能正确地认识系统。因此，有效地评估使用数字化仪控系统之后对核厂的影响，尤其是对核电厂安全的影响变地困难[4]。此外数字化仪控系统与传统模拟仪控系统在功能性和可靠性的分析方法上，也存在很大区别，具体区别如下[4, 14, 23]：

(1) 数字化仪控系统的复杂性与其性能和功能相关

数字化仪控系统存在复杂的两类交互作用（数字化仪控系统的元件与物理过程或环境的第一类交互作用；数字化仪控系统内部元件之间的第二类交互作用），这使得失效模式之间存在着潜在的相关性。数字化控制器不仅依赖于所测数据，同时也与系统状态有关。

(2) 数字化仪控系统运行特性与数字化过程和设备本质相关

由于数字化系统运行时采用离散时间步长和实数二进制近似的方法，因此如果产生采样率过低或二进制截断误差错误时，可能会照成伪影或折叠失真的情况；数字化仪控系统依赖于有记忆的时序电路，因此数字化仪控系统的输出包含系统历史信息；数字化仪控系统有相对于模拟系统更小的操作环境温度范围，所受影响不同于模拟系统受电压、辐射干扰、温度、压力、震动等的干扰。；

(3) 数字化仪控系统的失效模式特点

数字系统的故障机制并不好定义，在设计和软件中的错误可能会使功能看起来正确，但在系统运行中却因为接收到某些特定输入而导致系统突然故障的情况；的可能；数字化系统中的各任务间存在资源竞争问题，因此需要协调好资源间的关系避免系统资源短缺；由于更高等级的数据共享和交互，数字化系统会引入新的失效模式。通讯协议使得不同系统间具有依赖性，例如一个设备故障后产生无效数据，无效数据通过通讯协议输入给其他设备，以此类推，导致所有系统的输入数据都发生错误；软件可能掩盖硬件系统的间歇性故障，并且软件可以通过容错能力和故障修复能力修正或减轻硬件故障；数字化系统更容易受共因故障的影