学校编码：10384　　密级

学号：32420131152281

厦门大学

硕　士　学　位　论　文

简化 CPR1000 主给水系统及 AP1000 非能动安全壳冷却系统概率安全分析

Probability Safety Analysis of Simplified CPR1000Main Feedwater System and AP1000 Passive Containment Cooling System

侯恩通

指导教师姓名：　丁军教授

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

论文答辩日期：　2016 年 05 月

2016 年 6 月

CPR1000 主给水系统及 AP1000 非能动安全壳冷却系统概率安全分析

指导教师丁军教授　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

随着数字化仪控系统在核电厂中得到越来越多的应用，其可靠性对核电安全也越来越重要。传统概率安全分析方法已在模拟仪控系统中得到广泛应用，但在分析具有新设备和新技术的数字化仪控系统时还存在不足。动态概率安全分析方法中，Markov/CCMT 是较为符合数字化仪控特性的概率安全分析方法之一。

本文主要是应用故障树、Markov 和 Markov/CCMT 三种方法对简化 CPR1000 主给水系统和简化 AP1000 非能动安全壳冷却系统分别进行安全分析，其中简化 CPR1000 主给水系统在设置故障时偏重于数字类故障，简化 AP1000 非能动安全壳冷却系统在设置故障时偏重于机械类故障。期望通过分析结果的对比得到各个方法在分析数字化类型故障和机械类型故障时的特点和优势，为将来数字仪控系统可靠性分析方法的研究改进提供一些理论参考。

通过对两个系统三种安全分析结果对比可知，Markov/CCMT 更能体现主给水系统之间设备的复杂相互作用，也能弥补传统 PSA 方法在系统建模时相对保守的缺点；Markov/CCMT 得到的结果（如系统失效原因排序）更能反映设备故障对系统失效的贡献程度。而在分析具有机械类故障的系统时，更适宜用传统 PSA 方法。本文在分析非能动安全壳冷却系统时，三种方法得到的结果差别不大，但 Markov/CCMT 方法的计算量随着系统设备复杂度及设备数量的增加，呈几何级增长。

关键词：主给水系统非能动安全壳冷却系统故障树马尔可夫区间映射方法

Abstract

With the development of digital instrumentation and control (I&C) systems, nuclear power plants are in the process of replacing and upgrading aging and obsoleteinstrumentation and control (l&C) systems with digital I&C systems. However, there are no consensus methods for quantifying the reliability of digital systems. The ability of traditional probability safety analysis (PSA) methodologies like Event Trees/Markov to model digital I&C systems is in doubts. Some new technologies have been developed recent years for modeling digital systems, and Markov/CCMT is one of the most preferable methodology.

The main purpose of this paper is implementing PSA for main feedwater system of CPR1000 and passive containment cooling system (PCS) of AP1000 with Event trees (ET), Markov and Markov/CCMT respectively. The setting of failure modes of main feedwater system is focus on digital failure, and for comparison, the setting of failure modes of PCS is focus on enginery failure. The comparisons of different systems and different methodologies may display the feasibility of using traditional and dynamic reliability assessment methods for digital systems.

Through the comparisons of the PSA results of two systems with three different methodologies, we can see that, Markov/CCMT could model main feedwater system better than FT and Markov; Markov/CCMT could make up the conservation of traditional PSA methodologies; the results of Markov/CCMT could reflect more information than traditional PSA methodologies, especially with the fact that the failure data of digital systems are very rare. The PSA results of PCS, on the other hand, are similar and the enormous amount of calculation of Markov/CCMT will be huge.

Keywords: Main feedwater system; PCS; FT; Markov/CCMT

目录

Table of Contents

第一章 绪论

1.1 研究背景与意义

随着化石能源的逐渐枯竭及其所带来的环境污染问题日趋严重，世界各国都在努力寻找能够替代化石能源的优质、干净的能源。核电以其清洁无污染、能量密度高等优势，逐渐受到各国青睐。但核电也有其自身缺陷，核电厂会产生放射性废料，具有危害人类和自然环境的放射性。从人类利用核能发电到现在，先后发生了数次核电事故，影响比较大的有三哩岛核电事故、切尔诺贝利事故和福岛核电事故，无论是否造成可怕后果，每次核电事故后，民众都会对核电产生比较大的畏惧心理，进而导致核电发展的冷淡期。因此核电安全是发展核电事业能否顺利发展的最重要因素之一。

为评估并限制核反应堆的风险，发展并形成了两种成熟的分析评价核反应堆安全性的方法，一种是基于主观的依据设计基准事故的确定论评价法（称为DBA），另一种就是概率安全分析法（Probabilistic Safety Analysis，PSA）[1]。概率安全分析法是至今仍在广泛使用的核电厂安全评估方法，其中最常用的有事件树/故障树（Event Tree/Fault Tree，ET/FT）方法、Markov 方法。这两种方法都能够比较精确地建模核电厂各系统模型，利用已知系统中组件故障数据得到系统故障概率及组件重要度等信息。

随着电子科技以及 IT 技术的发展，数字仪控系统逐渐在核电厂仪控设备中取代模拟仪控系统，其优势主要包括，硬件可靠性和稳定性好，故障检测能力强[2]。很多已经建成的核电厂有计划有步骤地进行数字化仪控系统的替换，我国在建及计划建设的核电厂也都将采用全数字化系统。采用数字化仪控系统带来的问题是，电站会采用大量的数字仪控组件，部件与系统间的通讯方式也采用了新的技术，而传统的 PSA 方法（如 ET/FT、Markov）能否对这些新设备和新技术进行安全分析，还存在一些不足[2]。同时，T. Aldemir 等学者也开发了许多新的 PSA 技术来对数字仪控系统进行安全分析[3, 4]。在这些技术中，较为符合数字仪控特

性的方法是马尔可夫/区间映射技术（Markov/Cell-to-CellMappingTechnique，Markov/CCMT）和动态流图方法（DynamicFlowgraphMethology，DFM）[5]。

本文主要是应用故障树、Markov 和 Markov/CCMT 三种方法对简化 CPR1000 主给水系统和简化 AP1000 非能动安全壳冷却系统分别进行安全分析，其中 CPR1000 主给水系统在设置故障时偏重于数字故障；简化 AP1000 非能动安全壳冷却系统在设置故障时偏重于机械类故障。期望通过分析结果的对比得到各个方法在分析数字化类型故障和机械类型故障时的特点和优势，为将来数字仪控系统可靠性分析方法的研究改进提供一些参考。

1.2 核电厂数字仪控系统可靠性分析现状

在 1995 年 PSA 政策声明里，NRC 鼓励使用 PSA 技术及其最新方法和数据来监管所有核电安全领域。尽管在风险指引管理领域已经完成了很多活动，但数字系统的风险指引分析过程还未有令人满意的发展[6]。因为，至今仍没有一种被一致认可的方法来进行数字化系统的可靠性建模[7, 8]。NRC 在 1997 年成立了一个专门对商业核电厂中的数字化仪控系统进行研究的委员会，并提出了一些建议，包括发展 PSA 技术评估失效概率[2, 9]；模型中应包含软件失效对系统可靠性的影响；发展专门的技术来增加数字化仪控系统的安全性，并做出量化评估；发展可信的先进技术来降低定量化评估中的不确定性[10]。

NRC 委托了布鲁克海文国家实验室、俄亥俄州立大学核能技术部及弗吉尼亚大学电力及计算机技术系等单位对数字化仪控系统可靠性分析的 PSA 技术做出了初步的研究。报告 NUREG/CR-6962 中对核电厂的数字化系统特性做出了总结性分析，其中认为核电厂的数字化仪控系统的交互应包括：TypeⅠ反应堆控制、保护系统与核电厂控制进程（如增压，加热等）的交互作用；TypeⅡ反应堆控制与保护系统本身各个部件之间的交互（如多级任务分配，多路传输等）[7]。研究指出这些交互可能会在事故工况期间产生触发式或随机事故，对预计的系统失效模式造成影响。

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（ET/FT）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。但在数字化系统和核电厂专设系统动态交互的可靠性分析，以及数字化系统本身硬件与软件的动态模化中，ET/FT 方法显得能力不足[11, 12]。Markov 方法也是一种传统且十分完善的系统可靠性分析方法，已广泛应用于工业界的非数字化系统的可靠性评估中，并在已经在一些制造工业的数字化系统模型中初步进行了尝试，但是在核电厂数字化仪控系统中，并没有一个明确的导则或方法进行使用[13]。核电厂数字化仪控系统的 Markov 模型的应用取决于模型是否能够现实地表征系统特性，是否有完好的数据来支持模型的定量化，以及是否有合适的系统可靠性推断[14]。Markov 方法能够结合软件的能力来模化硬件失效，但不能提供足够的信息来表达一些特定失效、自我诊断维修和通讯故障等。报告 NUREG/CR-6985 里面提出动态方法来建模数字化仪控系统，其方法综述与需求如下表所示[5]：

表 1.1 用于模化数字化系统的方法综述各项需求

Table 1.1 Methodologies and Requirementsofdynamic PSA

方法/需求	1	2	3	4	5	6	7	8	9	10	11
连续事件树(CET)	x	x	x	x	o	?	?	o	?	?	o
动态事件树(DET)	x	x	x	?	x	?	?	?	x	x	o
马尔可夫模型	x	x	x	x	o	?	x	x	?	?	o
蒙特卡洛模拟	x	x	x	x	?	?	?	?	?	?	o
Petri 网	x	x	x	x	o	?	?	?	?	?	O
动态流图	x	x	x	?	x	?	?	?	x	x	x
动态故障树（DFT）	x	?	?	?	x	?	x	?	x	?	x
事件序列图(ESD)	x	x	x	x	o	?	?	?	x	x	o
GO-FLOW 法	x	?	x	?	o	?	?	?	x	x	x
贝叶斯方法	x	?	?	?	o	o	?	?	?	?	X

基于测试方法	?	?	x	o	x	?	x	x	?	o	x
基于软件度量方法	o	?	o	o	?	?	x	x	o	o	x
施耐德模型(黑匣子)	x	?	?	?	?	?	?	?	o	o	x

x：满足要求 o：不满足要求？：仍不确定

由表可见，1）没有某种单一的模型可以满足所有的需求；2）没有任何一种已有的方法可以满足需求 6，即失效数据可信度普遍认同度不高；3）具有最多优点和最少缺陷的 DFM 方法、Markov/CCMT 方法可以作为推广方法来使用，但其认证程度有待检验[15-17]。

国内对于核电厂数字化仪控系统的可靠性分析主要开始于在引进美国 AP1000 技术后对 AP1000 的 PSA 模型中有关数字化仪控系统软件可靠性评价。目前我国岭澳二期、红沿河等一系列新堆型的设计中都对数字化仪控系统的可靠性给予了高度关注。目前国内大型核电厂使用的数字化仪控系统，特别是安全级的数字化仪控系统还不完全具备国产化条件。我国环保部近期发布的《核安全与放射性污染防治“十二五”规划及 2020 年远景目标》中指出，2015 年底前在建核电厂需要从设计、验证和故障分析等方面分析评估安全级数字化控制系统的可靠性，查找薄弱环节并实施相应的改进[18]。

以 AP1000 为例，AP1000 数字化仪控系统的 PSA 建模方法与模拟仪控系统的建模方法是类似的。数字化仪控系统仍然模拟成一个支持功能来触发前沿系统。在支持功能连接到前沿系统方面没有区别。通常需要考虑的两个问题是：当需要时不能动作和误动作。由于缺乏系统级的统计数据，仍以传统的故障树方法作为一个评价仪控系统可靠性主要有效方法。在西屋公司提供的 AP1000 PSA 报告文件中，数字仪控触发逻辑通过子树与总模型相连接。这些子树直接与设备的支持动作信号相关联。每个子树的成功或失效由组成它的部件状态、硬件或软件、成功或失效的逻辑输出推导而来。

综合以上论述，国内的研究状况表明，仅就引进国外的数字化仪控系统可靠性分析而言，目前对数字化系统失效模式和失效机理的认识水平，以及数字化系统中软件可靠性数据可支持的程度，仅仅有了一个初步的探讨。而对核电安全级

的计算机软件失效模式、失效机理和共因失效，以及失效数据方面，还需要大量开展深入的研究工作。广东核电集团设计院等有关单位对相关内容进行了初步的研究，其依托我国正在建设的二代改进型核电厂工程，主要以传统 ET/FT 方法进行了分析和探讨。

1.3 本文研究内容

本文针对核电仪控系统的数字化趋势，选取简化 CPR1000 主给水系统和 AP1000 非能动安全壳冷却系统为研究对象，分别采用故障树、Markov 和 Markov/CCMT 对这两个系统进行安全分析，并通过分析结果的对比找到各个方法在分析数字化类型故障和机械类型故障时的优缺点。

第一章主要介绍了核电数字仪控系统可靠性现状，选题背景及意义；

第二章介绍了本文使用的三种 PSA 分析方法故障树、Markov 和 Markov/CCMT 的基本原理及应用步骤；

第三章分别使用故障树、Markov 和 Markov/CCMT 三种方法对简化 CPR1000 主给水系统进行 PSA 分析，并将三种分析方法得到的结果进行对比分析；

第四章分别使用故障树、Markov 和 Markov/CCMT 三种方法对简化 AP1000 非能动安全壳冷却系统进行 PSA 分析，并将三种分析方法得到的结果进行对比分析；

第五章为总结和展望。

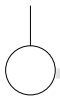
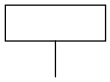
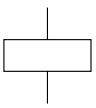
第二章 概率安全分析方法

2.1 故障树方法

故障树分析法，简称 FTA（Fault Tree Analysis），是一种特殊的倒立树状逻辑因果关系图，它用事件符号、逻辑门符号和转移符号描述系统中各种事件之间的因果关系。逻辑门的输入事件是输出事件的“因”，逻辑门的输出事件是输入事件的“果”。一个故障树图是从上而下逐级建树并且根据事件而联系，它用图形化“模型”路径的方法，使一个系统能导致一个不可预知的故障事件（失效），路径的交叉处的事件和状态，用标准的逻辑符号（与门，或门等）表示。表 2.1 为故障树分析中常用的符号。

表 2.1 故障树分析中常用符号[19]

Table 2.1 Conventional symbol in FT

名称	符号	定义
底事件		底事件是故障树分析中仅导致其他事件的原因事件
基本事件		圆形符号是故障树中的基本事件，是分析中无需探明其发生原因的事件
未探明事件		菱形符号是故障树分析中的未探明事件，即原则上应进一步探明其原因但暂时不必或暂时不能探明其原因的事件，它又代表省略事件，一般表示那些可能发生，但概率值微小的事件
结果事件		矩形符号，是故障树分析中的结果事件，可以是顶事件，由其他事件或事件组合所导致的中间事件，矩形事件的下端与逻辑门连接，表示该事件时逻辑门的一个输入。
顶事件		顶事件是故障树分析中所关心的结果事件
中间事件		中间事件时位于顶事件和底事件之间的结果事件
与门		它指只有在所有的输入事件都发生的时候，才会有输出事件发生。
或门		表示当有一个或一个以上的输入事件发生时，就会发生输出事件。