

概率安全评价中 人因可靠性分析技术

张力 著



原子能出版社

国家自然科学基金资助项目(70271016)

国防军工技术基础计划项目(Z012002A001)

概率安全评价中 人因可靠性分析技术

张 力 著

原 子 能 出 版 社

图书在版编目(CIP)数据

概率安全评价中人因可靠性分析技术/张力著.

—北京:原子能出版社,2006.6

ISBN 7-5022-3678-3

I. 概… II. 张… III. 人-机系统—系统可靠性—系统分析 IV. TB18

中国版本图书馆 CIP 数据核字(2006)第 055665 号

内 容 简 介

本书基于人因工程学、认知心理学和行为科学,建立了人因可靠性分析技术基本理论。从工程角度分析了概率安全评价对人因可靠性分析的本质需求,对国际现行主要人因可靠性分析技术的性能、特征进行了比较研究,提出了与概率安全评价相适应的人因可靠性分析技术规范化的准则,进而构造了一种规范化、工程化、具有很强可操作性的人因可靠性分析技术。书中给出了该技术的一个应用实例。本书可供于可靠性工程、安全工程等专业的研究生、本科生和专业技术人员参考。

概率安全评价中人因可靠性分析技术

出版发行 原子能出版社(北京市海淀区阜成路 43 号 100037)

责任编辑 孙凤春

责任校对 冯莲凤

责任印制 丁怀兰 刘芳燕

印 刷 中国文联印刷厂

经 销 全国新华书店

开 本 850 mm×1168 mm 1/32

字 数 190 千字

印 张 7.125

版 次 2006 年 7 月第 1 版 2006 年 7 月第 1 次印刷

书 号 ISBN 7-5022-3678-3

印 数 1—500 定 价 25.00 元

版权所有 侵权必究(如有缺页、倒装,请与出版社联系调换)

网址: <http://www.aep.com.cn>

序

人因失误/人因事故已是大规模复杂人一机系统最主要的事故源之一,所以人因可靠性分析(HRA)也就成为系统安全分析与评价的极为重要的组成部分。目前,HRA在核工业领域应用广泛,并逐步向航空航天、石油化工等领域推广。其实,随着系统的大规模、复杂化,几乎所有的工业系统乃至工作系统、服务系统和生活系统均对HRA具有高度的需求,其发展、应用前景十分广阔。

张力同志撰写的这部图书,据我所知,是国内关于人因可靠性分析的第一部著作。该书基于人因工程学、认知心理学和行为科学,建立了人因可靠性分析技术基本理论。从工程角度分析了概率安全评价对人因可靠性分析的本质需求,对国际现行主要人因可靠性分析技术的性能、特征进行了比较研究,提出了与概率安全评价相适应的人因可靠性分析技术规范化的准则,进而构建了一种规范化、工程化、具有很强可操作性的人因可靠性分析技术。

管理科学的最终目的是要指导管理实践,而理论与实践之间需要技术作为桥梁与工具。我认为,张力同志的这

本著作在人因可靠性分析理论与实践应用之间架起了桥梁,这也正是该书的学术意义和应用价值所在。

正如张力同志所说,人因可靠性分析的理论、方法、技术正在发展之中。期望张力同志在该领域继续深入研究,勇攀高峰,获得更多的成果,做出更大的贡献。

中国工程院院士 何瑾书

2005年12月30日

前 言

大规模、现代化的人—机系统为我们带来了巨大的经济效益,也深刻地改变了人们的工作方式。然而,这样的系统也随之可能带来两方面的问题:在强调以人为中心的时代,它是否能适合人的特性、满足人的舒适性需求?更为突出的是,相当多这样的系统,一旦发生安全事故,则可能导致社会的巨大灾难,如三里岛核电站事故、印度 Bhopal 化工厂毒气泄漏、切尔诺贝利核电站事故、挑战者航天飞机失事等。造成这两个问题的根源在于,系统的安全与效益不仅取决于它自身的技术水平,还极大地取决于它与人和环境的协调程度。随着科技进步,系统设备(硬件和软件)可靠性不断提高,运行环境得到大的改善,但作为人—机系统极其重要的一方——人,一方面,由于其生理、心理、社会、精神等特性,既存在一些内在弱点,又有极大的可塑性和难以控制性;另一方面,尽管系统的自动化程度提高了,但归根结底还要由人来控制操作,要人来设计、制造、组织、维修、训练,要人来决策。因此,人在系统中的作用不是削弱了,而是更加重要和突出了。特别是从安全性来看,由人的因素而诱发的事故已成为系统最主要的事故源(之一)。因此,如何把人的因素对于风险的后果考虑进去,以及如何

揭示系统的薄弱环节，在事故发生之前加以防范，便成为亟待解决的重要问题。而这些都基于详尽和准确的人因可靠性分析基础之上。

人因可靠性分析(Human Reliability Analysis, HRA)以人因工程、系统分析、认知科学、概率统计、行为科学等诸多学科为理论基础，以对人的可靠性进行定性与定量分析和评价为中心内容，以分析、预测、减少与预防人的失误为研究目标，是目前正在逐渐形成的一门新兴学科。概率安全评价(Probabilistic Safety Assessment, PSA)是一种对来自系统运行各个水平上的损害和其他不期望后果进行辨识，并对相关事件作出定性定量分析、评价、预测的系统安全/风险评估方法。将人因可靠性分析应用于人一机系统概率安全评价是目前人因可靠性分析学科研究的中心内容之一和推动该学科发展的主要动力，也是国际系统管理科学界的一项重要前沿课题。

作者于1987年到日本早稻田大学研修人因工程时初次接触到人因可靠性分析研究的文献资料，自此便与人因可靠性分析研究结下了不解之缘。近20年来，在国家自然科学基金、国防科研计划等的长期支持下，作者完成了一系列有关人因可靠性的基础理论研究，然后将这些理论成果转换为工程技术并应用于实践。先后主持完成了大亚湾核电站、岭澳核电站、秦山核电站的人因可靠性分析项目，对人因可靠性分析的研究和应用积累了较丰富的体验。然

而,也正是在这一过程中,作者深深感到,现行的人因可靠性分析方法和技术尚存在诸多不足,对人因可靠性分析以及概率安全评价结果的质量和可信性造成很大的影响和冲击。这其中一个重要原因就是缺乏方便实用的规范化的人因可靠性分析技术。本书正是试图在该方面作出贡献,通过研究 PSA 中 HRA 的任务、技术、实施程序等,建立一种规范化、工程化的 HRA 技术,以推进 HRA 在 PSA 中的应用。

本书的研究和写作是在国家自然科学基金资助项目(70271016)“人误分析技术及应用研究”和国防军工技术基础计划项目(Z012002A001)“人因可靠性技术与应用研究”及秦山核电公司委托项目“秦山核电站 PSA 中人因可靠性分析”的资助下完成的。尤其是国家自然科学基金委员会管理科学部对作者的研究给予了长期的支持和热情的鼓励,作者对此深表谢意。

我的妻子王以群,也是我进行人因可靠性研究的合作伙伴,对本书的写作提出了许多很好的建议和改进意见。

在研究和写作过程中,得到了课题组同事黄曙东、戴立操的大力协助;清华大学黄祥瑞教授、赵炳全教授、何旭洪博士也参加了部分工作,我们共同研究,一起探讨,书中有的观点也是他们的真知灼见。我的导师湖南大学许康教授、中国科学院和中国工程院赵仁恺院士、于景元研究员和汪寿阳博士在研究方法方面也给予了热情的指导,作者对

他们表示衷心的感谢。

还要特别感谢大亚湾核电站及其黄卫刚、张宁、郭建兵,岭澳核电站及其苏圣兵、陈捷飞、郝海英,秦山核电公司及其章逸民、王永民、尹志刚、骆雪莲等诸位朋友为作者的研究提供了条件和巨大的帮助。

中国工程院院士何继善教授多年来一直关注和支持作者的研究,本次又拨冗为本书作序,使作者备受鼓舞,也深表感谢。

人因可靠性分析的理论、方法正在发展,其在概率安全评价中的应用也正在发展。本书仅是对作者前一研究阶段工作的一个总结,一定存在许多不完善之处,敬请读者给予批评指正。

张力

2005年12月31日

目 录

插图索引	VI
附表索引	IX
第 1 章 绪 论	1
1.1 研究意义	1
1.2 国际 HRA 发展历史与研究动态	5
1.3 我国 HRA 研究与应用情况	9
1.4 现行 HRA 方法缺陷分析	10
1.5 研究背景和主要研究内容	13
1.5.1 研究背景	13
1.5.2 主要研究内容及拟解决的关键问题	13
1.6 著作结构	15
第 2 章 概率安全评价对人因可靠性分析的需求研究	16
2.1 PSA 框架	16
2.1.1 PSA 的主要功能与作用	16
2.1.2 PSA 的基本分析方法	17
2.2 PSA 对 HRA 的需求分析	17
2.2.1 PSA 主要程序工作分析	17
2.2.2 PSA 对 HRA 的本质需求	19
2.2.3 PSA 中人因事件分类	21
2.2.4 HRA 基本框架	23
2.2.5 PSA 中 HRA 过程范式	24
2.3 本章小结	25
第 3 章 现行 HRA 方法分析	27
3.1 人的失误率预测技术 (THERP)	27

3.1.1	THERP 背景描述	27
3.1.2	THERP 方法描述	27
3.1.3	THERP 数据库	31
3.1.4	评析	31
3.2	人的认知可靠性模型(HCR)	32
3.2.1	HCR 的背景	32
3.2.2	HCR 方法描述	32
3.2.3	HCR 的特性与限制	35
3.2.4	评析	36
3.3	操纵员动作树(OAT)	36
3.3.1	简介	36
3.3.2	评析	37
3.4	事故引发与进展分析(AIPA)	37
3.4.1	简介	37
3.4.2	评析	38
3.5	成对比较法(PC)	38
3.5.1	简介	38
3.5.2	评析	39
3.6	成功似然指数法(SLIM)	39
3.6.1	简介	39
3.6.2	评析	40
3.7	人因可靠性社会技术评估方法(STAHR)	41
3.7.1	简介	41
3.7.2	评析	42
3.8	混淆矩阵(CM)	43
3.8.1	简介	43
3.8.2	评析	45
3.9	人误评估与减少技术(HEART)	45

3.9.1	简介.....	45
3.9.2	评析.....	45
3.10	估计人决策失误方法(INTENT)	46
3.10.1	简介	46
3.10.2	评析	47
3.11	人误分析技术(ATHEANA)	47
3.11.1	ATHEANA 的指导思想	47
3.11.2	ATHEANA 基于的行为模型	49
3.11.3	ATHEANA 的分析框架	49
3.11.4	ATHEANA 法的实施	54
3.11.5	评析	56
3.12	认知可靠性与失误分析方法(CREAM)	56
3.12.1	CREAM 的主要特点	57
3.12.2	COCOM	57
3.12.3	分类方案	58
3.12.4	分析技术	59
3.12.5	评析	61
3.13	HRA 方法的综合评价	61
3.14	本章小结	63
第 4 章	HRA 技术的基础理论研究	64
4.1	HRA 基本概念讨论	64
4.1.1	人的失误与人的可靠性.....	64
4.1.2	人的失误与人的非安全行为.....	64
4.1.3	人的失误特点.....	66
4.1.4	人一系统交互作用.....	67
4.1.5	人的行为类型.....	67
4.1.6	人的行为形成因子(PSFs)	68

4.2 大规模复杂人一机系统运行控制特征及对人因的影响	69
4.3 人的认知行为模型	71
4.3.1 认知控制模式与认知规则	71
4.3.2 刺激—调制—响应(S-O-R)模型	73
4.3.3 人的信息处理模型	73
4.3.4 认知模拟机	75
4.3.5 大规模复杂人一机系统人员认知行为模型	75
4.4 大规模复杂人一机系统人因失误的分类与产生机制分析	77
4.5 诱发大规模复杂人一机系统人因事故的主要因素	80
4.6 组织管理因素对人因事故的作用和影响	83
4.7 人因失误模式与其根本原因的关联性	85
4.7.1 人因失误模式分布	86
4.7.2 各类根本原因分布	86
4.7.3 根本原因与人误模式之间的关联性	87
4.8 人因失误结构	89
4.9 人因事故成因模型	90
4.10 本章小结	90
第5章 规范化 HRA 技术的建立——模型与程序	92
5.1 PSA 中规范化 HRA 技术的要素及其关系	92
5.2 规范化的定义及准则	93
5.3 HRA 分析模型——THERP+HCR	93
5.3.1 建模分析	93
5.3.2 THERP+HCR 分析模型的建立	95
5.4 HRA 规范化技术程序	98
5.4.1 事故前 HRA 技术程序	98
5.4.2 激发初因 HRA 技术程序	103

5.4.3	事故后 HRA 技术程序	106
5.5	HRA 规范化文档模式	112
5.6	本章小结	114
第 6 章	HRA 技术基本数据研究	116
6.1	HRA 数据需求	116
6.1.1	THERP 模型所需数据	117
6.1.2	HCR 模型所需数据	117
6.1.3	ATHEANA 模型所需数据	117
6.2	HRA 数据采集的难点	117
6.3	数据采集的基本准则	118
6.4	数据源	119
6.5	数据分析	119
6.6	HRA 数据管理系统	121
6.6.1	系统模型	121
6.6.2	数据结构设计分析	123
6.6.3	数据来源	124
6.6.4	数据结构	125
6.6.5	计算模块	125
6.6.6	系统主要功能	126
6.7	秦山核电站操纵员可靠性模拟机实验	127
6.7.1	实验背景	127
6.7.2	操纵员响应失误数据分析理论概述	128
6.7.3	实验过程	131
6.7.4	实验结果	133
6.7.5	秦山核电站操纵员 HCR 模型参数与国外数据比较	133
6.7.6	实验结论与讨论	139
6.8	本章小结	140

第 7 章 人因可靠性分析实例	141
7.1 分析目标	141
7.2 原始数据收集	141
7.3 事故序列建模	142
7.3.1 事件树建模	142
7.3.2 系统故障树分析	150
7.4 SGTR 人因事件分析	151
7.4.1 人因事件题头	151
7.4.2 事件背景	152
7.4.3 事件描述	152
7.4.4 事件成功准则	152
7.4.5 调查与访谈结论	152
7.4.6 事件分析	153
7.4.7 建模与计算	154
7.5 本章小结	157
第 8 章 结 论	158
8.1 概述	158
8.2 本书的主要工作	158
8.3 主要结论	159
8.4 本书的不足及今后努力方向	161
参考文献	162
附录 秦山核电站操纵员可靠性模拟机实验资料	173
附录 A 选择事件情景描述	173
附录 B 秦山核电站 300MW 机组操纵员事故响应时测试数据	179
附录 C 秦山核电站模拟机实验操纵员响应时数据处理	197

插图索引

图 1.1	HRA 方法年代分布	8
图 2.1	PSA 的主要程序及 HRA 的介入	19
图 2.2	核电站 PSA 中人因事件/人的失误行为类型	22
图 2.3	HRA 基本框架	24
图 3.1	HRA 中 THERP 应用过程示意图	28
图 3.2	串联和并联系统的 HRA 事件树	29
图 3.3	HCR 行为类型辨识树	33
图 3.4	基本的 OAT	37
图 3.5	STAHHR 影响图	41
图 3.6	序贯式行为模型	49
图 3.7	ATHEANA 法分析框架	51
图 3.8	ATHEANA 法应用流程	55
图 3.9	COCOM	58
图 4.1	人的非安全行为分类框架	65
图 4.2	Wickens 应用于人一机界面的人的信息处理模型	74
图 4.3	人的决策阶梯模型	75
图 4.4	大规模复杂人一机系统操作人员认知行为模型	76
图 4.5	操作人员行为动态模型	78
图 4.6	人误分类体系	80
图 4.7	人因失误模式分布(分类不独立)	86
图 4.8	各类根本原因的百分比(分类不独立)	87
图 4.9	人因失误结构模型	89
图 4.10	人因事故成因模型	90
图 5.1	规范化的 HRA 技术组成要素及其关系	92

图 5.2	C 类人因事件演进模式	95
图 5.3	C 类人因事件时间分割函数	97
图 5.4	A 类 HRA 技术程序	98
图 5.5	A 类人因事件树	102
图 5.6	B 类 HRA 技术程序	103
图 5.7	C 类 HRA 技术程序	107
图 6.1	数据采集、分析与预测之间的关系	121
图 6.2	大规模复杂人一机系统人因数据管理系统功能模块	122
图 6.3	秦山核电站 HCR 模型技能型操纵员响应概率曲线 ...	136
图 6.4	秦山核电站 HCR 模型规则型操纵员响应概率曲线 ...	137
图 6.5	秦山核电站 HCR 模型知识型操纵员响应概率曲线 ...	137
图 6.6	秦山核电站与 IAEA 的 HCR 模型操纵员 S·R 型 界面响应概率曲线比较	138
图 6.7	秦山核电站与 IAEA 的 HCR 模型操纵员 K 型界面 响应概率曲线比较	139
图 7.1	核电站一回路和二回路系统示意图	142
图 7.2	SGTR 功能事件树	144
图 7.3	SGTR 事故序列事件树	144
图 7.4	SGTR 人因事件在 PSA 模型中的基本位置	151
图 7.5	操纵员隔离破管蒸汽发生器 HRA 事件树	155