半数字化核电厂控制室人因可靠性分析

戴立操 著

中国原子能出版社

国家自然科学基金项目:复杂工业系统数字化对人因可靠性的影响研究(No. 70873040);
国家自然科学基金项目:大规模数字化控制系统中人的认知行为研究(No. 71071051)

半数字化核电厂控制室人因可靠性分析

戴立操　著

中国原子能出版社

图书在版编目(CIP)数据

半数字化核电厂控制室人因可靠性分析/戴立操著.
—北京:中国原子能出版社,2012.8
ISBN 978-7-5022-5657-9

Ⅰ.①半… Ⅱ.①戴… Ⅲ.①核电厂-人-机系统-系统可靠性-系统分析 Ⅳ.①TM623②TB18

中国版本图书馆 CIP 数据核字(2012)第 193913 号

本书由南华大学资助出版

半数字化核电厂控制室人因可靠性分析

出版发行	中国原子能出版社(北京市海淀区阜成路 43 号 100048)
责任编辑	王 青
责任校对	冯莲凤
责任印制	潘玉玲
印 刷	保定市中画美凯印刷有限公司
经 销	全国新华书店
开 本	880 mm×1230 mm 1/32
印 张	5 **字 数** 120 千字
版 次	2012 年 8 月第 1 版 2012 年 8 月第 1 次印刷
书 号	ISBN 978-7-5022-5657-9 **定 价** **38.00 元**

网址:http://www.aep.com.cn **E-mail:atomep123@126.com**
发行电话:010-68452845

前　言

核电厂是一个复杂社会—技术系统，包括技术设备、人和组织及环境三大元素以及它们的子系统。安全是核电厂存在和发展的基础。核电厂一旦发生事故，不但造成重大的人员和经济损失，同时会产生超出自身范围的巨大社会负面影响。

安全分析对核电厂运行安全至关重要。据此，概率安全评价(Probabilistic Safety Assessment，PSA)被提出和不断发展。它用基于事故场景的方法和思路分析研究核电厂系统，通过运用多种安全性分析技术，鉴别其可能的后果，计算出各种危险因素导致事故发生的概率，达到安全分析的目的。在PSA中，人因可靠性分析(Human Reliability Analysis，HRA)是事故序列和在总风险中人与系统的交互作用对风险贡献重要性的关键所在，它影响着事故序列的进程，对核电厂的安全风险具有显著的影响。

传统的HRA方法研究的对象主要是传统的(一、二代)核电厂控制室。操纵员从模拟量表、打印机、报警器、指示灯等中获得信息，通过手动的控制键、控制钮、操纵杆等对核电厂进行控制操纵。核电厂控制室半数字化(三代)和全数字化(四代)以后，人机界面发生了巨大变化。半数字化控制室中，信息显示和操纵控制一方面采用传统控制室的盘台显示和控制方式，另一方面，使用核电厂显示系统(Plant Display System，PDS)和计算机显示终端(Vedio Display Unit，VDU)等为操纵员集中显示更多的辅助信息，以便操纵员进行诊断和决策。人机界面改变了控制室内的人员行为模式，这种改变迫切需要建立与之相适应的新的人行为模型和HRA方法。

与界面相适应的HRA方法的研究一直是国际PSA界研究的重点问题。然而，由于人的行为的随机性、易变性和可塑性，HRA也是PSA研究中的难点。本研究采用实验的方式，观察事故后操纵员的人员行为，抽象总结出重水堆半数字化人机界面中人员行为的基本特征，建立半数字化控制室（以CANDU6重水堆主控室为例）中操纵员诊断的PABI模型，在考虑组织因素对人员行为影响的基础上，结合考虑人员的操纵特征，对THERP进行改进，建立了适合于重水堆半数字化人机界面特征的HRA模型。

本课题研究受到国家自然科学基金项目：复杂工业系统数字化对人因可靠性的影响研究（No. 70873040）和大规模数字化控制系统中人的认知行为研究（No. 71071051）的支持。本课题同时受到秦山第三核电有限公司的PSA-HRA委托项目的支持。

本项目的研究旨在提出一种新的适合于特定人机界面的HRA方法以期提高核电人因安全水平，并为进一步研究全数字化核电厂控制室中的HRA方法奠定基础。

由于作者水平有限，时间有限，错误实属难免，恳请读者批评指正。如有疑问，欢迎来信交流 dailicao@yahoo.com.cn。

南华大学　戴立操

2012年3月于深圳大鹏

英文缩写说明

缩写	全　称	中　文
AECL	Atomic Energy of Canada Limited	加拿大原子能公司
ARO	assistant reactor operator	辅助操纵员
ASEP	accident sequence evaluation program	事故序列评估技术
ATHEANA	a technique for human event analysis	人因事件分析技术
BHEP	basic human error probability	基本人误概率
BOP	balance of power	热平衡系统
CD	core damage	堆芯损伤
CDF	core damage frequency	堆芯损伤频率
CREAM	cognitive reliability and error analysis method	认知可靠性和失误分析方法
CRT	cathode-ray tube	阴极射线管
CSP	critical safety parameter	关键安全参数
CSPM	critical safety parameter monitoring	关键安全参数监视
DBA	design-based accident	设计基准事故
ECC	emergency core cooling	应急堆芯冷却
ECCS	emergency core cooling system	应急堆芯冷却系统
EDG	emergency diesel generator	应急柴油发电机
EOC	error of commission	执行型失误
EOI	error of intention	意向错误
EOO	error of omission	疏忽型失误
EOP	emergency operation procedure	应急运行规程
EWS	emergency water system	应急给水系统

续表

缩写	全　称	中　文
EPRI	Electric Power Research Institute	美国电力设计院
EPC	error producing conditions	失误产生环境
FW	feed water	给水
HCR	human cognitive reliability	人的认知可靠性
HEART	human error assessment and reduction technique	人误评估与减少技术
HEP	human error probability	人因失误概率
HFE	human factor error	人因失误
HHMI	hybrid human-machine interface	混合式人机界面
HMM	Hidden Markov Model	隐马尔可夫模型
HR	human reliability	人的可靠性
HRA	human reliability analysis	人的可靠性分析
HTA	hierarchical task analysis	层次任务分析法
HTS	heat transmitting system	主热传输系统
IAEA	International Atomic Energy Agency	国际原子能机构
IDA	information, decision and action	信息,决策和行动
IE	initiating event	始发事件
INTENT	method for estimating human error probabilities for decision based errors	估计人决策失误方法
LLOCA	large loss of coolant accident	大破口事故
LOCA	loss of coolant accident	冷却剂丧失事故
MCR	main control room	主控制室
NRC	Nuclear Regulatory Commission	美国核管会
NSSS	nuclear steam supply system	核蒸汽供应系统
ORE	operator reliability experiment	操纵员可靠性实验
PABI	process analysis based on interface	基于人机界面的诊断流程分析法

续表

缩写	全　称	中　文
PC	pair comparison	成对比较法
PDS	plant display system	电厂显示系统
PHT	primary heat transport	主热传输系统
PORV	pilot-operated relief valve	稳压器释放阀
PRA	probabilistic risk analysis	概率风险分析
PSA	probabilistic safety assessment	概率安全评价
PSF	performance shaping factor	人员行为形成因子
RCS	reactor coolant system	反应堆冷却剂系统
RF	recovery factor	恢复因子
RO1	reactor operator 1	反应堆操纵员 1
RO2	reactor operator 2	反应堆操纵员 2
SCA	secondary control area	次要(二级)控制区
SG	steam generator	蒸汽发生器
SGTR	steam generator tube rupture	蒸汽传热管破裂
SHARP	systematic human action reliability procedure	系统化的人行为可靠性分析程序
SLI	success likelihood index	任务的可靠度指数
SLIM	success likelihood index method	成功似然指数法
SLOCA	small loss of coolant accident	小破口事故
SOP	state-oriented procedure	症状导向规程
SPAR-H	standardized plant analysis risk human reliability analysis	标准的电厂分析风险人因可靠性分析方法
SS	shift supervisor	值长
TA	task analysis	任务分析法
THERP	Technique for Human Error Rate Prediction	人因失误率预测技术

续表

缩写	全　称	中　文
TLA	time-line analysis	时间序列分析
TRC	time reliability curve	时间可靠性曲线
VPA	verbal protocol analysis	口头报告分析
WANO	World Association of Nuclear Operators	世界核营运者协会

目　录

第一章 绪 论

1.1 研究背景

中国经济的快速发展需要更多的能源供应，核电发展已经成为我国能源战略重要组成部分。截止到 2011 年 7 月，中国核电装机容量达 1 082 MW，约占全国电力供应的 1.5%，有 13 个反应堆正在运行，27 个反应堆在建，50 个反应堆正在规划或筹建。核电被称为复杂社会—技术系统，包括技术设备、人的群体和组织三类元素的大型经济实体，属科技密集型产业。对于核电厂而言，安全是核电存在和发展的基础，一旦发生事故，不但造成重大的人员和经济损失，也会产生超出自身范围的巨大社会负面效应(张力，2001)。

核电厂的风险主要来自事故工况下不可控的放射性核素的释放。如何减少由于核素释放对公众和环境造成的危害的问题称为核安全问题。核安全问题包括两个方面，一是核辐射安全问题，它要求在任何运行条件下，应确保公众和环境处于正常的辐射水平之下；二是核安全，它要求在反应堆设计和运行中必须考虑并采取相应措施排除不可控链式反应的偶然发生和发展的可能性(朱继洲，2004)。为了评价上述两个问题发生的可能性，核电厂安全分析的内容包括：1) 正常运行模式的安全状态；2) 预计运行事件下的核电厂状态分析；3) 设计基准事故；4) 可能导致严重事故的事件序列分析。以上分析可以确定

核电厂抵御始发事件(initiating event,IE)和事故的能力,验证安全系统和安全相关系统的有效性,提出减少电厂的风险的改进措施,维持电厂安全。

1.1.1　安全评价的两种方法:确定论和概率论

核电厂安全分析的方法主要有两种:确定论和概率论。这两种方法论是从不同的角度回答核电厂"安全达到什么水平,就足够安全了"这个问题(Hollnagel,1993b)。

1.1.1.1　确定论方法

在核电厂发展早期,安全分析是基于当时的认识水平和对事故出现的可能性大小判断的。它的基础是设计基准事故(design-based accident, DBA)。DBA 的定义是:核电厂按确定的设计准则在设计中采取了针对性措施的那些事故工况(Werner et al.,1995),即假定事故已经发生,分析和计算整个核电厂系统的响应。DBA 的选择主要依据工程判断、设计和运行经验进行保守假定。例如,对于冷却剂丧失事故(loss of coolant accident,LOCA),DBA 的定义为冷却剂管道的双端断裂,应急堆芯冷却系统(emergency core cooling system,ECCS)要设计成具有应付 LOCA 等事故的能力。

确定论方法广泛用于核电厂设计和运行,安全法规制定和安全分析中,但确定论方法存在几个主要问题:

1) 把事故人为地划分为"可信"和"不可信"。人们对于安全分析的研究往往保守地集中在极不易发生的事故,比如,大破口事故(large loss of coolant,LLOCA),而忽视了经常发生的运行瞬态和小破口事故 (small loss of coolant,SLOCA)。单一"可信"的事故分类无法真实反映核电厂可能的事故危害,无法与其他社会风险相比较,妨碍公

众对于核电厂的接受。

2）严重的始发事件并不一定导致严重的后果，而看来不严重的始发事件却能导致严重的后果。WASH1400（USNRC，1975）及其他研究报告（Spurgin，1987）认为，LLOCA 导致的堆芯损伤频率（core damage frequency，CDF）约占总 CDF 的 0.6%～6%，而 SLOCA 和运行瞬态引起的概率却占 74%～81%。

3）只考虑安全系统的单一故障，不考虑系统的完全失效。

4）安全没有被定量度量。

1.1.1.2 概率论方法

概率安全评价（probabilistic safety assessment，PSA）又称概率风险分析（probabilistic risk analysis，PRA），是 20 世纪七十年代以后发展起来的一种系统工程方法，始于美国在 1975 年发表的“反应堆安全研究”（WASH-1400）报告（USNRC，1975）。该报告首次采用 IE 发生频率及估算得出的安全系统失效概率计算导致堆芯损伤的事故序列发生概率，并计算核素释放到环境中的放射性对公众的风险。

PSA 认为，一切事故属于随机事件，不存在“可信”与“不可信”的截然界限，只有发生概率大小的区别。核电厂总的风险 R_n（n 个能导向环境释放物质的潜在事故）为核电厂事故发生的概率 P 与事故后果 C 的乘积的累加值：

$$R_n = \sum_{i=1}^{n} P_i \cdot C_i$$

核电厂事故会带来两种后果，一是经济损失，二是人员损失。PSA 分析中，考虑的电厂风险所致的后果是放射性对公众的风险，即造成的人员损失。其风险目标定性描述为（USNRC，1986）：

1）公众中的每个人都应当获得一定程度的保护，使他不承受因