基于核电站事故处理的人因可靠性研究

谷鹏飞,张建波,孙永滨

中广核工程有限公司,广东深圳 518124

摘要　近些年人因可靠性研究对于核电站安全性这一问题越来越重要。在核电站控制室采用数字化技术以后,计算机化的操纵员工作站带来了便捷操作方式,但庞大且集中的信息量也带来了操作任务可靠性的风险。因此,在核电站的设备可靠性大幅度提高的前提下,人因可靠性也需要不断提高,以保证核电站运行具有更好的安全性和经济性。根据美国布鲁克海文国家实验室最新发布的 NUREG 0700 标准,先进控制室(ACR)被定义为"采用数字化技术的控制室"。国内核电站数字化控制室自主化设计从岭澳二期项目首次开始实施,2010 年岭澳二期核电站顺利商运,标志着首个国内自主化设计的先进控制室的成功。本文正是针对数字化控制室的设计过程,将"失水事故"(LOCA)和"蒸汽发生器传热管破裂"(SGTR)选择为初始事件。同时,在此基础上,叠加一些设备或系统的失效。通过在事故状态下对操纵员在模拟机上处理事故的过程进行分析,以获得合理的人因绩效数据,从而更利于人因可靠性的分析,也能对核电站的设计,尤其是控制室的设计起到改善的作用。通过收集人因绩效,尤其是在事故状态下的人因绩效,将会对提高人因可靠性起到非常重要的作用。

关键词　人因可靠性分析;核电站安全性;失水事故;蒸汽发生器传热管破裂;人因绩效

中图分类号　TK08　　**文献标识码**　A　　**doi**　10.3981/j.issn.1000-7857.2012.21.007

The Human Reliability in the Accident Processing of NPP

GU Pengfei, ZHANG Jianbo, SUN Yongbin

China Nuclear Power Engineering Co., Ltd., Shenzhen 518124, Guangdong Province, China

Abstract　Recently, Human Reliability Analysis (HRA) is becoming more important to the safety of Nuclear Power Plant (NPP). Since the digital technology is adopted in the control room of NPP, the computerized operator workstations have brought flexible operation methods. However, huge and centralized information also could cause some risks for operation tasks. Therefore, as the reliability of the NPP equipments have been increased even higher, HRA should be developed in order to guarantee the better safety of NPP. According to the new revision of NUREG 0700 Standard published by Brookhaven National Laboratory in USA, Advanced Control Room (ACR) has been defined as the control room adopted the digital technology. In China, self-determination design involving ACR is first beginning with Lingao Phase II project. Lingao Phase II NPP has been in operation mode since the year of 2010. It indicates the success of first self-determination design involving ACR. The design process of ACR is focused on. In the analysis, the LOCA and SGTR are selected as the initiating events. And based on that, some failures of other equipments or systems have been added. Then the process that the operators deal with the accidents has been analyzed with the accident situations in order to obtain reasonable human performance data. By collecting human performance, especially in accident situations, it shows that enhancing the human reliability is very important. Therefore it would be benefit to analyze the human reliability. As a result, it also could be benefit to the design improvement of NPP, specially the design of main control room.

KeyWords　HRA; the safety of NPP; LOCA; SGTR; human performance

0　引言

随着科技发展,系统及设备自身的安全与效益得到不断提高,人机系统的可靠性能越来越取决于人的可靠性。据统计,国内外每年发生的各类伤亡事故中 60%以上与人的失误有关,而由此引发的重大灾难事故比率更是高达 80%以上[1-2]。前苏联切尔诺贝利核电站因设备维修保养不到位引发的 4 号机组爆炸事故、美国宾西法尼亚州三哩岛核电厂因维修人员与操作人员配合失误引发的核燃料泄漏事故、美国挑战者航天飞机

收稿日期:2012-05-21;修回日期:2012-06-21

作者简介:谷鹏飞,工程师,研究方向为核电站控制室及仪控系统设计,电子信箱:gupengfei@cgnpc.com.cn

因飞行操纵失误引发的失事事故、国内京沪高铁淮安段因驾驶员疲劳驾驶酿成撞车引发液氯泄漏事故、河北省唐山市开平区刘官屯煤矿因瓦斯检测设备老化及安检人员工作失职造成的井下爆炸事故、河南省新安县寺沟煤矿因矿主安全主题责任不落实而引发的透水事故等一系列残酷事实表明：如何将人的失误因素切实渗透到企业风险后果评估体系，如何采取必要手段研究人在应急情景下的动态认知过程，探究人的失误机理并建立模型来揭示系统的薄弱环节，以便在事故发生之前加以防范,正成为各高危行业亟待解决的重要课题[3]。

人因可靠性分析(Human Reliability Analysis,HRA)研究开始于20世纪50年代[4]。20世纪50年代末至60年代初已经有人开始探讨人为差错对系统可靠性的影响[5]。此后,随着工业生产尤其是核工业的发展，安全性问题越来越突出，HRA逐渐得到重视并发展。HRA的主要目标在于正确评估由于人为差错导致的风险和寻求降低人为差错影响的方式。这种定义方式涵盖的内容比较丰富。在实际应用中,找出人因可靠度并不是最终的目标,最终目标应该是寻找导致人因可靠性退化的诱因,并有针对性的加以控制。

“十一五”规划纲要提出,要积极推进核电建设,重点建设百万千瓦级核电站，逐步实现先进压水堆核电站的设计、制造、建设和运营自主化,预计到2020年要完成8000万千瓦装机容量。因此,人因可靠性研究对于核电站安全性变得越来越重要。因为在核电站控制室采用数字化技术以后,计算机化的操纵员工作站带来了便捷的操作方式,但庞大且集中的信息量也带来了操作任务可靠性的风险。因此,在核电站的设备可靠性大幅度得到提高的前提下,人因可靠性也需要不断提高,以保证核电站运行具有更好的安全性和经济性。

虽然在其他工业领域，人因可靠性分析形成了一系列的方法,取得了很好的成果,但在核工业领域,世界范围内数字化技术还刚刚在核电站全面采用,数字化控制室设计的研究也在逐步开展。与国外核电先进国家相比,中国在先进控制室系统及人因工程设计领域起步较晚,而且由于基础研究相对滞后,导致在设计过程中遇到实际问题时缺少理论指导和必要技术基础作为决策的依据。

根据美国布鲁克海文国家实验室最新发布的NUREG 0700标准,先进控制室(ACR)被定义为“采用数字化技术的控制室”[6]。国内核电站数字化控制室自主化设计从岭澳二期项目于2005年首次开始实施,在借鉴世界先进核电国家设计经验的基础上,中广核工程有限公司建设了岭澳二期人机界面验证平台来辅助开展人机接口的设计验证工作。2010年底岭澳二期核电站顺利商运,标志着首个国内自主化设计的先进控制室的成功。

在数字化技术使用后的主控室,由于核电站各种参数、画面、报警等信息的集中显示,对于核电站的操纵员来说,形成了“锁孔效应”,即在原来的基于模拟技术的控制室内,操纵员可以一览无遗地看到所有的地方,而基于数字化技术的控制室内,操纵员需要通过计算机画面及时有效地找到所需要的信息。由此可见,数字化技术的采用给操纵员的任务执行带来了一些风险,其人因可靠性是否能达到电站安全性和经济性的要求,需要认真分析。

在核电站数字化控制室设计过程中，对人因可靠性的分析可以转向人为差错的分析，具体过程可以分为差错辨识、差错频率确定和差错规避措施设计3个阶段。人为差错的主要诱因可以分为5类,分别为训练水平、任务本质、人机交互界面质量、环境因素和任务执行时间。本文正是根据在模拟机上模拟核电站典型事故的处理过程,分析这5类诱因的影响趋势。

1　模拟机实验

1.1　工作环境

相关实验是在岭澳二期验证平台上进行的，岭澳二期的验证平台完全按照与真实主控室1:1的模式来搭建，实验环境如下[7-9]：

(1) 保证4台完整的OWP(操纵员工作站)供实验使用；

(2) 保证后备盘BUP(验证平台软后备盘)的可用性,机组长和安全工程师可以通过软后备盘查看相关参数,以保证SOP规程(状态导向规程)的顺利执行；

(3) 保证大屏幕的可用性,可以提供电站概貌一览；

(4) 保证紧急控制盘(ECP)的可用性(ECP也是采用的软ECP,即用计算机方式代替硬接线)；

(5) 保证数字化规程可用性,准备纸质规程作为备份；

(6) 保证仿真模型的稳定性,以适合正常和事故工况下的实验。如果有些模型方面的问题,需要提前做好修改,并给出提醒(介绍平台可利用状况)列表,确保实验过程中不会发生(或涉及)影响事故处理的事件,以保证实验的连续性和可操作性。

实验过程中，需要以下人员完成整个实验的操作和数据记录：

(1) 4组运行人员(每组包括2名有经验的操纵员、1名机组长、1名安工,其中2组在验证平台接受过培训,2组没有接受过培训)；

(2) 1—2名人因工程专家；

(3) 1—2名分析数据的工程师(与设计者分离)；

(4) 控制室系统设计者、规程画面设计者(至少各1名)；

(5) 2—3名平台维护人员。

1.2　实验场景

实验阶段时,验证平台的某些局部功能开发并没有完善,通过人因专家对验证平台状态的评估,结合高级操纵员的建议，选择失水事故（LOCA）和蒸汽发生器传热管破裂事故(SGTR)作为典型事故来处理,期间叠加失去一些监视屏以及场内辐射监测系统失效来增加判断难度,从而分析人为差错的五大诱因影响。

1.3　实验过程

在事故工况下，以 SGTR 和 LOCA 这两种事故为参照进行测试[10]，需要走 ECP1、ECP2、ECP3、ECP4 和 ECS 规程(ECP1、ECP2、ECP3、ECP4 为核岛的 4 类事故操作规程，ECS 为常规岛的事故操作规程)。LOCA 事故的初始状态为 100 FP%、冷端 Leg 1 发生 1.78cm 破口。1 号屏作为监控画面 YST，2 号屏作为规程框架，3 号屏作为操作画面 YCD；SGTR 事故的初始状态为 100 FP%、5 管破裂(SG1)1 号屏作为监控画面 YST，2 号屏作为规程框架，3 号屏作为操作画面 YCD。测试情况如表 1 和表 2 所示。通过测试，执行 LOCA 事故处理共用时 59min。经过这段时间的处理，虽然主程序框架在操作过程中经常被覆盖，但还是可以完成事故处理的操作，能够保证反应堆处于安全状态；执行 SGTR 事故处理共用时 43min。经过这段时间的处理，还是可以完成事故处理的操作，能够保证反应堆处于安全状态。

表 1　LOCA 事故测试过程

Table 1　LOCA test process

时间	核岛操纵员操作步骤	时间	常规岛操纵员操作步骤
14:06	核岛操纵员进入 DOS 报警，开始执行 DOS 规程	14:07	常规岛操纵员进入 DOS 报警，执行 DOS Water and Steam
14:13	因为发生跳堆，安注动作，所以重新开始走 DOS 规程	14:26	常规岛操纵员进入 ECS 规程
14:26	核岛操纵员进入 ECP2 规程	14:31	常规岛操纵员进入 ECS 规程的 Sequence 3
14:37	进入 ECP2 的 Sequence 2	15:05	常规岛操纵员完成 ECS 规程
15:01	完成 ECP2 的 Sequence 2		

表 2　SGTR 事故测试过程

Table 2　SGTR test process

时间	核岛操纵员操作步骤	时间	常规岛操纵员操作步骤
15:26	核岛操纵员进入 DOS 报警，开始执行 DOS 规程	15:27	常规岛操纵员进入 DOS 报警，执行 DOS Water and Steam
15:35	核岛操纵员完成 DOS 规程判断，进入 ECP3 规程	15:35	常规岛操纵员进入 ECS 规程
15:39	核岛操纵员进入 ECP3 的 Sequence 1	15:47	常规岛操纵员进入 ECS 规程的 Sequence 4
15:53	进入 ECP3 的 Sequence 1 循环	16:03	常规岛操纵员完成 ECS 规程
16:09	完成 ECP3 的 Sequence 1		

1.4　结果分析

对比初步安全分析报告第 15 章的内容(如表 3 所示)，在小破口事件序列时，从发生到开始进行反应堆冷却的安全可控时间约为 64min，而在验证平台的实验过程中，其耗时约为 59min，满足安全分析的需要[11]。

表 3　小破口事件(LOCA)序列

Table 3　LOCA sequence

事件	时间/s
破口发生	200
反应堆停堆信号	415.3
控制棒完全插入	419.5
安注信号	447.5
安注投入	477.5
反应堆冷却开始(56°C/h)	4077.5

对比初步安全分析报告第 15 章的内容（如表 4 所示），在蒸汽发生器管子破裂事件序列时，从发生到开始进行反应堆冷却的安全可控时间约为 52min，而在验证平台的实验过程中，其耗时约为 43min，满足安全分析的需要。

在核电厂系统中，人员行为是多种多样的，尤其是当一

表 4　蒸汽发生器破裂(SGTR)序列

Table 4　SGTR sequence

事件	时间/s
管子开始破裂	0
稳压器低压力信号	1210
·反应堆紧急停堆	
·汽轮机跳闸	
稳压器低-低压力信号	1235
·SI 注射泵(2 列)启动	
操纵员参考 A3 规程进行干预	1835
·第 1 列 SI 注射泵停止	
·RCP 开始卸压和冷却(56°C/h)	
第 2 列 SI 注射泵停止	2745
瞬变结束	3100
破损蒸汽发生器一次侧与二次侧压力达到平衡	

个需要操纵员响应并干预的核电事故发生后,操纵员首先是感知各种信息,包括报警、显示、记录等,然后根据所感知到的信息对事故进行诊断,并按诊断进入相关事故规程。在规程中,操纵员按规程的要求实施具体的操作作业干预。即在一个需要人员干预的事件中,人员的行为通常包括3个阶段:感知、判断和作业反应。

在感知阶段,外界信息首先通过操纵员的视觉、听觉等感觉器官传入大脑,此时对感知阶段的差错进行纠正或部分纠正后,依据操作经验和记忆做出判断和决策,并依据感知–判断和判断两种途径对出现的差错进行纠正或部分纠正后执行动作,同时通过感知–判断–作业反应、判断–作业反应和作业反应三种方式对差错予以纠正,从而完成一次操作。如果将人的这一行为过程定义为作业成功单元,相应的操作失误则定义为操作差错单元,简称为差错元,而每一阶段的失误就为差错子元。差错子元与差错元的关系如图1所示。

核电厂的运行操作是由感知–判断–作业反应组成的操作单元在时间、延续性和目标性等制约下的不断往复进行的过程,因此操纵员的可靠性也应该由感知可靠性、判断可靠性和作业反应可靠性3个可靠性子元串联而成,而人机界面因素对操纵员可靠性的影响也应当贯穿于这3个操作单元当中。如果3个操作单元进展顺利,人的行为就表现出正确性和准确性,反之,就会出现失误导致可靠性下降。

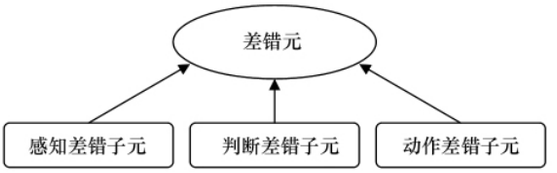

图1　差错子元与差错元的关系

Fig. 1　Relationship between mistake subsets and mistake set

在实际操作过程中对人机界面的情况进行了评价[13–15],评价标准为:满分为10;较好(≥8);基本满意(6—8);亟需改进(<6),评价情况如表5所示。结果表明人机界面设计能够使得操纵员在各方面感到基本满意,保证了人机界面良好的可用性。

表5　人机界面评价情况

Table 5　HMI evaluation

编号	评价项目	得分
1	提取信息足以完成当前任务(任务导向法),并可以同时监视机组的当前状态,无信息缺失或无用的信息	7.7
2	图形对象使用正确	8.0
3	画面布局合理、美观、清晰,符合规范要求	7.8
4	相关链接数量足够,设置合理,指向正确	7.6
5	类似功能画面无重复	7.8
6	画面编码正确,画面命名合理	7.7
7	画面符合人因工程的要求	7.5
8	参数的表述正确,参数的布局合理	7.9
9	画面设计实现正确,相关信息显示正常	7.3
10	相关链接设置合理,指向正确	7.4

状态认知表示操纵员对电厂状态的把握,考虑操纵员是否能获取到有用的信息,并充分理解,在状态认知主观评价表中,操纵员对其操作过程的主观感受给出了评价[12]。认知的程度从0—7分为7个不同的等级,0代表完全没有认知,7代表认知非常好。评价结果如表6所示。

上述结果表明了现有人机界面设计能够基本保证操纵员

表6　操纵员认知评价

Table 6　Operator cognition evaluation

项目	描述	得分	分析
对电厂状态信息的认知度	是否容易获取到电厂状态的相关信息,包括动态参数、电厂总体工况等	5.1	表明操纵员对电厂状态信息的认知较容易
信息获取	是否已获取了执行相关序列操作所需要的定性和定量信息	5.1	表明操纵员在信息获取上较容易
对事故序列的理解	通过过程状态参数是否理解了执行的事故序列	4.4	表明操纵员在对事故序列的理解上较为一般
对MCR/MMI设计的理解	对所采用的人机界面设计是否容易理解	5.1	表明操纵员对MCR/MMI设计的理解较容易
信息理解	所获取的信息对预测后续事态的发展的帮助大吗	5.2	表明操纵员对信息的理解较容易
信息获取	在序列执行过程中是否获得了有助于预测事态发展的支持信息	4.7	表明操纵员在信息的获取上并不十分便利

的主观认知需求。同时在验证中还发现,一部分操纵员对数字化人机界面熟悉程度不高,寻找所需信息花费时间较长,对设备的控制操作也不大熟练。这是由于对数字化人机界面接触较少,相对陌生造成的,这一点影响了这部分人对数字化人机界面的认可程度。

2　结语

经过测试的录像分析,发现训练水平、任务本质、人机交互界面质量、环境因素和任务执行时间对操纵员的执行力和判断力影响颇大。

对验证平台熟悉的操纵员,其处理事件反应迅速;反之,对平台不熟悉的操纵员常常顾此失彼,甚至发生误安注现象。操作任务结构的合理性对操纵员也非常重要,经过测试发现,对于不同年龄段的操纵员,对操作任务结构有着不同的理解,相对而言,年长的操纵员绝大部分对结构的复杂性没有太多的抱怨,而年轻的操纵员则不然。

人机交互界面的质量对操作任务的完成有着极其重要的影响,在测试过程中,当操纵员们可以用作操作的屏幕数目减少时,其操作的难度和舒适性大大降低。在执行事故规程时,操纵员不知道其处于何处,这些都带来潜在风险——操纵员会对自己的判断产生怀疑,这增加了安全、快捷处理事故的难度。

同时,外部环境的压力对操纵员也有一定影响。在处理事故时,当机组长和安工同时处于操纵员身后并进行操作交流时,其工作效能成下降趋势,这为后续运行队伍的建设提供了一些合理鉴戒。

测试过程中,还发现下面有趣的现象:由于绝大部分操纵员知道合理的操作完成时间,因此,在越接近规定时间时,其工作效能反而有所提高,并不会因为紧张而降低。因为这是在模拟主控室内进行,其真实性有待进一步考证,但为以后的研究提供了进一步可参考的方向。

参考文献(References)

[1] 王洪德, 高玮. 基于人的认知可靠性(HCR)模型的人因操作失误研究[J]. 中国安全科学学报, 2006, 16(7): 51-56.
Wang Hongde, Gao Wei. *China Safety Science Journal*, 2006, 16(7): 51-56.

[2] 肖国清, 陈宝智. 人因失误的机理及其可靠性研究 [J]. 中国安全科学学报, 2001, 11(2): 22-25.
Xiao Guoqing, Chen Baozhi. *China Safety Science Journal*, 2001, 11(2): 22-25.

[3] 徐德蜀. 安全文化、安全科技与科学安全生产观[J]. 中国安全科学学报, 2006, 16(3): 71-82.
Xu Deshu. *China Safety Science Journal*, 2006, 16(3): 71-82.

[4] 黄祥瑞. 可靠性工程[M]. 北京: 清华大学出版社, 1990: 123-125.
Huang Xiangrui. Reliability engineering[M]. Beijing: Tsinghua University Press, 1990: 123-125.

[5] Williams H L. Reliability evaluation of the human component in man machine systems[J]. *Electrical Engineering*, 1958, 12(1): 78-82.

[6] Office of Nuclear Regulatory Research. NUREG-0700. Human-system Interface design review guidelines [S]. Washington DC: US Nuclear Regulatory Commission, 2002.

[7] Broberg H, Kolaczkowski A M. Constraints in designing simulator scenarios and identifying human failure events for testing hra methods[C]. 2007 IEEE 8th Human Factors and Power Plants (HFPP) and 13th Annual HPRCT Meeting, Monterey, CA, USA, August 26-31, 2007.

[8] Forester J, Kolaczkowski A M, Dang V N, *et al*. Human Reliability Analysis (HRA) in the context of HRA testing with empirical data[C]. 2007 IEEE 8th Human Factors and Power Plants (HFPP) and 13th Annual HPRCT Meeting, Monterey, CA, USA, August 26-31, 2007.

[9] Le Bot P, Cara F, Bieder C. MERMOS, a second generation HRA method: What it does and doesn't do[C]//Proceedings of the International Topical Meeting on Probabilistic Safety Assessment (PSA '99), 1999, Washington DC: American Nuclear Society, 2: 852-860.

[10] 核工业标准化研究所. EJ/T 562-2005. 核安全有关的操纵员动作时间响应设计准则[S]. 北京: 中国标准出版社, 2005.
Institute for Standardization of Nuclear Industry. EJ 562-2005. Time response design criteria for safety-related operator actions [S]. Beijing: Standards Press of China, 2005.

[11] International Electrotechnical Commission. IEC 61227-1993. Nuclear power plants-control rooms-operator controls [S]. Geneva: International Electrotechnical Commission. 1993.

[12] 核工业标准化研究所. EJ/T 1143-2002. 核电站控制室设计 功能分析与分配[S]. 北京: 中国标准出版社, 2002.
Institute for Standardization of Nuclear Industry. EJ/T 1143-2002. Nuclear power plants-design of control rooms: Function analysis and assignment[S]. Beijing: Standards Press of China, 2002

[13] 国家核安全局. HAF J 0055. 核电站控制室设计的人因工程原则[S]. 北京: 国家核安全局, 1995.
National Nuclear Safety Administration. HAF J0055. Nuclear power plants: Design for control rooms-HFE principle [S]. Beijing: National Nuclear Safety Administration, 1995.

[14] 国家技术监督局. GB/T 13630-1992. 核电厂控制室的设计 [S]. 北京: 中国标准出版社, 1992.
State Bureau of Technical Supervision. GB/T 13630-1992. Design for control rooms of nuclear power plants [S]. Beijing: Standards Press of China, 1992.

[15] 核工业标准化研究所. EJ/T 798-1993. 核电站控制室人机特性评价[S]. 北京: 中国标准出版社, 1993.
Institute for Standardization of Nuclear Industry. EJ/T 798-1993. Nuclear power plants: Control rooms-HMI characteristic evaluation[S]. Beijing: Standards Press of China, 1993.

(责任编辑　马晓晓)