

人因可靠性分析方法

张 力** 黄曙东*** 何爱武 杨 洪

(南 华 大 学)

【摘 要】 回顾了人因可靠性分析(HRA)的发展历史;总结了近几十年来的各种人因可靠性分析方法;详细介绍了人的失误率预测技术(THERP)、人的认知可靠性模型(HCR)、成功自然指数法(SLIM)的背景、使用步骤、特性等;分析了 THERP-HCR 的优势,并给出了一个应用实例。最后,指出了目前 HRA 方法的不足并预测了 HRA 的发展趋势。

【关键词】 人因 可靠性 分析 方法

1 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-机系统的可靠性和安全性愈来愈取决于人的可靠性。据统计,(20~80)%的系统失效与人有关,其中直接或间接引发事故的比率为(70~90)%,这其中包括许多重大灾难事故,如印度 Bhopal 化工厂毒气泄漏、切尔诺贝利核电站事故、三里岛核电站事故、挑战者航天飞机失事等^[1]。因此,如何把人的失误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。而这些都以详尽和准确的人因可靠性分析(HRA; Human Reliability Analysis)为基础。

2 HRA 方法综述

HRA 的方法发展得很快,种类也较多,有些已在 HRA 中正式得到应用,有些仅是提出作为 HRA 的可选择方法。表 1 汇总了部分重要方法的主要特点与资料来源。

表 1 人的可靠性分析(HRA)方法汇总^[2~4]

序号	全 称	来 源	评 价
1	THREP 人误率预测技术 Technique of human error rate prediction	A. D. Swain, H. E. Guttman, Handbook of Human Reliability Analysis with Emphasis on Nu- clear Power Plant Applications, NUREG/CR-1278, 1983	①迄今为止最系统的人因可靠性分析方法; ②有较好的数据收集条件; ③在应用于事故下的规则性失误分析时,可获得 信赖的结果; ④有一套较完整的表格,查表可量化人因失误。

* 国家自然科学基金资助项目(79870004)国防军工技术基础计划项目(Z012000A003);
湖南省自然科学基金资助项目(98JJY20066)。

** 教 授

*** 工程师

序号	全 称	来 源	评 价
2	OAT 操作员动作树 Operator action tree	R. E. Hall, J. Fragola, J. Wreathall, Post Event Human Decision Errors; Operator Action Tree/Time Reliability Correlation. NUREG/CR-3010, 1982	①早期开发的一种方法,用于诊断或与时间有关情况; ②可用于操作员的决策分析; ③宜仅用于粗略分析。
3	AIPA 事故引发与进展分析 Accident initiation and progressing analysis	K. N. Fleming, P. H. Raabe, G. W. Hannaman, W. J. Houghton, Accident Initiation and Progression Analysis Status Report, GA/A13617 Vol. II UC-77, General Atomic Co., San Diego (USA), 1975	①用于与响应时间相关联的情况; ②用于估算在高温气冷堆运行中的操纵员响应概率; ③类似于 TRC 模型; ④对 PSF 的修正考虑较少。
4	HCR 人的认知可靠性模型 Human cognitive reliability model	G. W. Hannaman, A. J. Spurgin, Y. Lukic, Human Cognitive Reliability Model for PRA Analysis, NUS-4531, 1985	①适用于诊断的决策行为的评价; ②将人的行为进行简化的处理后,再考虑一个不完全独立于时间的 HEP; ③模式已考虑人员间的相关性。
5	PC 成对比较法 Paired comparison	D. A. Seaver, W. G. Stillwell, Procedures for Using Expert Judgement to Estimate Human Error Probabilities in Nuclear Power Plant Operations, NUREG/CR-2743, 1983	①在简单估计 HEP 情况下,采用专家判断结果; ②对复杂任务 HEP 获得困难。
6	DNE 直接数字估计法 Direct numerical estimation	D. A. Seaver, W. G. Stillwell, Procedures for Using Expert Judgement to Estimate Human Error Probabilities in Nuclear Power Plant Operations, NUREG/CR-2743, 1983	①要求有较好的参考数值; ②不适用完全的 HRA 情况; ③在多位专家中进行有效的讨论。
7	SLIM 成功似然指数法 Success likelihood index methodology	D. E. Embrey, P. Humphreys, E. A. Rosa, B. Kirwan, K. Rea, NUREG/CR-3518, 1984	①较好的灵活性,无法验证; ②是一种专家判断的技术; ③较好的理论基础; ④不过份强调外界可观察的错误而选用较确切的失误概率值; ⑤不考虑 PSF 的相互作用。
8	STAHK 社会-技术人的可靠性分析法 Socio-technical approach to assessing human reliability	L. D. Phillips, P. Humphreys, D. E. Embrey, D. L. Selby, A Socio-Technical Approach to Assessing Human Reliability (STAHK). In: Pressurized Thermal Shock Evaluation of the Calvert Cliffs Unit 1 Nuclear Power Plant, Appendix D, NUREG/CR-4022, 1985	①一种依赖于主观推测和心理分析结合的方法; ②可以考虑比较复杂的,更为仔细的 PSF 相依问题; ③一般在 PSA 中不采用; ④具有较强的灵敏度分析能力; ⑤利用影响图进行技术上的分析,而社会分析是指对影响图中技术因素影响的分析。
9	CM 混合矩阵法 Confusion matrix	L. M. Potash, M. Stewart, P. E. Dietz, C. M. Lewis, E. M. Dougherty Jr., Experience in Integrating the Operator Contributions in the PRA in Actual Operating Plants. In: Proceedings of the ANS/ENS Topical Meeting on Probabilistic Risk Assessment, Port Chester, NY, September 1981, Vol. II, pp. 1054-1063. American Nuclear Society, 1981	①用于分析在初因事件诊断中的混淆错误; ②很强烈地依赖于专家判断; ③是一种定性的分析。

序号	全 称	来 源	评 价
10	MAPPS 维修个人行为模拟模型 Maintenance personel performance simulation model	A. I. Siegel, W. D. Bartter, J. J. Wolf, H. E. Knee, Maintenance Personnel Performance Simulation (MAPPS) Model; Description of Model Content, Structure, and Sensitivity Testing. NUREG/CR-3626, 1984	①是一种较适合于分析 PSA 中有关维修工作的方法; ②技术性较强的一种方法,结果较难理解。
11	MSFM 多序贯失效模型 Multiple-sequential failure model	P. K. Samanta, J. N. O'Brien, H. W. Morrison, Multiple Sequential Failure Model; Evaluation of and Procedure for Human Error Dependency. NUREG/CR-3837, 1985	①是一种研究以维修为导向的计算机软件模型; ②提供为 PSA 用的维修活动的数据库; ③方法本身是一种事件树的模拟,为分析人员提供有用的信息。
12	SHARP1, SHARP1 系统化的人的行为可靠性分析程序 Systematic human action reliability procedure	G. W. Hancock, A. J. Spurgin, V. Joksimovich, J. Wreathall, D. D. Orvis, Systematic Human Action Reliability Procedure (SHARP). EPRI NP-3583 (1984), (1992)	美国电力研究院(EPRI)进行人因分析的标准步骤,可使分析结果更加系统化、条理化
13	INTENT 估计人决策失误的方法 Method for estimating HEPs for decision-based errors	D. I. Gertman, H. S. Blackmann, L. N. Haney, K. S. Seidler, H. A. Hahn, INTENT: A Method for Estimating Human Error Probabilities for Decision Based Errors. Reliability Engineering & System Safety Vol. 35(1992)	①适合进行操作员决策失误的评价方法; ②一种类似于 THERP 的方法,它可更广泛地描述人的 Commission 错误; ③可对意向性失误的概率定量化。
14	COGENT 认知事件树系统 Cognitive event tree system	D. I. Gertman, Representing Cognitive Activities and errors in HRA trees. ECG-HFRU-10026. Idaho National Engineering Laboratory, 1992	①是对 THERP 中 HRA 事件树的一种扩展,可描述几种认知失误; ②对认知失误的分类基于 SRK 框架和 slips, lapses 及 mistakes 的组合。
15	ATHEANA 人误分析技术 A technique for human error analysis	S. E. Cooper, A. M. Ramey-Smith, J. Wreathall, et al, A Technique for Human Error Analysis (ATHEANA). NUREG/CR-6350, 1996	①提出了迫使失误情景的概念; ②当前最新的 HRA 方法之一; ③其成熟性尚未证明,且可用数据缺乏
16	CREAM 认知可靠性与失误分析方法 Cognitive reliability and error analysis method	E. Hollnagel, Cognitive Reliability and Error Analysis Method. Elsevier Science Ltd, 1998	①基于认知心理学而提出的 HRA 最新方法; ②使用较为复杂,可操作性尚待强化。

3 几种常用的 HRA 方法

人的可靠性评价的主要目的,在于提供事故序列中所定义的人员动作有一个合理可信的人误概率值,同时为系统可靠性的改善提供决策参考^[7]。由于人员行为的多样性和高度复杂性,故不存在一种对任何行为模式都适用的可靠性分析方法。针对系统操作和认知判断是现代人一机系统最普遍的作业,现介绍几种常用且较为成熟的人员可靠性分析方法,并讨论它们的特点和局限性。

3.1 人的失误率预测技术(THERP ; Technique for Human Error Rate Prediction)

3.1.1 THERP 背景描述

20 世纪 80 年代初,Swain A. D. ,Guttmann H. E. 等著名人因分析专家,经过多年艰苦细致的工作,完成了研究报告“Handbook of Human Reliability Analysis with Emphasis on Nuclear

Power Plant Applications”(人因可靠性分析手册)。在该报告中提出了一套完整的人员可靠性分析方法——人的失误率预测技术(THERP)。这套方法问世以来,已被美国等多个国家广泛用于核电站、石化工业、大型武器系统等领域的风险评价之中^[8]。

3.1.2 THERP 方法描述

用 THERP 方法完成人的失误概率量化计算包括 4 个阶段:①系统熟悉阶段;②定性分析阶段;③定量分析阶段;④应用阶段。共有 10 个步骤,如图 1 所示。

1) 系统熟悉阶段

该阶段对系统的考察访谈与资料收集,需完成以下任务:①了解核电站 PSA 事件树和故障树中有关的人的失误事件;②了解与基本事件有关的人员任务;③人进行此项任务时的边界条件,包括:控制室的特点;系统的总体布置;行政管理系统;任务的时间要求;工作人员的指定职能技术要求;报警症状;恢复因子等。

2) 定性分析阶段

(1) 任务分析

了解人员每项任务的内容并将它分解为相应的一系列相连贯的动作或子任务序列;找出人一机系统相互作用的界面;判断人在完成任务时所产生的失误的类别;对于分解得到的每一项子任务,同时必须查明以下几点:①动作实施的设备或仪表;②要求操作人员的动作;③可能潜在的人因失误;④控制器、显示器、操纵阀的位置等。当任务是由不同的人员完成时,还需了解人员之间的监督关系对人员动作失误的恢复关系。

(2) HRA 事件树的建造

★建造 HRA 事件树的一般规则。HRA 事件树在人员任务分析的基础上,以两状态事件树的形式描述,以时间为序的人的各项行为与活动的过程。一般情况下,用人因可靠性事件树进行人的失误分析时,每一个分支节点上都只存在两种决策可能,即进行此项操作时失败或成功的两种可能性。图 2 给出了一个简单的 HRA 事件树。建树的有关规则如下:^[9]①用大写字母(如 A)表示某一项子任务失败和它的失败概率,相应的小写字母(如 a)则表示该项子任务成功和它的成功概率;②位于 HRA 事件树各序列末尾的字母 S 和 F 分别表示人员完成任务的成功和失败,如图 2 中的串联任务的情况,存在 1 个成功分支序列和 3 个失败分支序列;③HRA 事件树的每个节点上有两个分支,左侧的分支表示成功,右侧分支表示失败,对于表示系统中硬件状态的分支点,从左至右按照失误的严重状态予以排列;④对于极小概率的分支事件可以从事件树中删去,并忽略恢复因子的影响;⑤在 HRA 事件树中,将相依的人员动作事件合并为

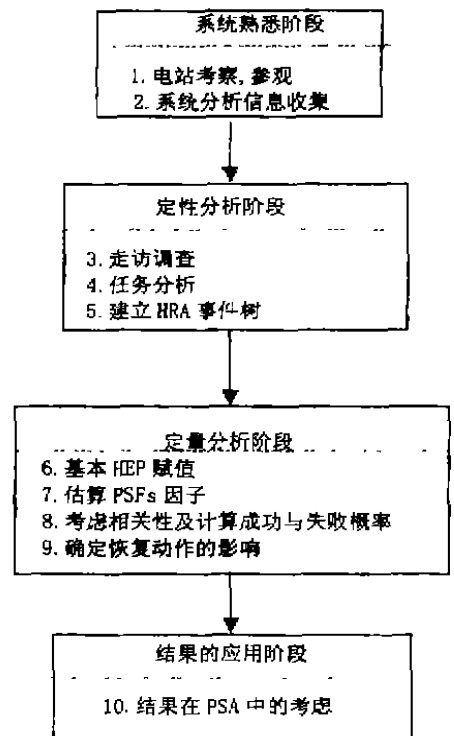


图 1 人的可靠性分析中 THERP 应用过程示意图

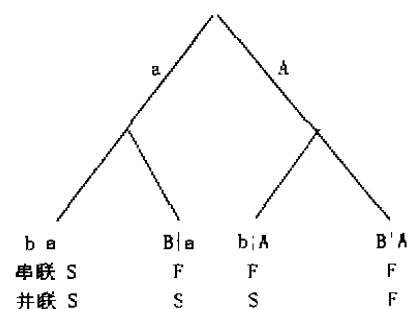


图 2 串联和并联系统的 HRA 事件树

一个子任务分支;⑧对于 HRA 事件树中的失败或成功节点,如果事件树中的一个支路已鉴别出其分析任务为成功或失败,这一个节点不再进一步分解。

★HRA 事件树的定量评价。图 2 中的 HRA 事件树,可按如下方法进行定量评价:

①如果任务是串联型,即该任务要求人连续先后完成两项动作单元,那么人完成任务的成功概率或失败概率分别为:

$$P(S) = a(b|a) \quad P(F) = 1 - a(b|a) = a(B|A) + A(b|A) + A(B|A)$$

②如果任务是并联型,则只要求完成两项动作单元中的任何一项任务则系统成功,在这种情况下人完成任务的成功概率或失败概率分别为:

$$P(S) = 1 - A(B|A) = a(b|a) + a(B|a) + A(b|A) \quad P(F) = A(B|A)$$

式中, $P(S)$ 人员完成任务的成功概率; $P(F)$ 人员未能完成任务的失败概率。

(3) 行为形成因子(PSF)与任务相关性修正

在 HRA 事件树中,某一项子任务的失败概率(如 A)由基本 HEP(BHEP)表示。它依据该项子任务的动作类型,由相关的 THERP 表格查找而得。但由于在 HRA 事件树中,人的失误概率因人员差异有很大差别。因此,为了得到在 HRA 事件树中子任务的实际概率 HEP,必须用行为形成因子(PSF)进行修正。一般而言,修正可用以下通式表示: $HEP = BHEP \cdot (PSF)_1 (PSF)_2 \dots$, HRA 事件树的每一项子任务之间可能具有相关性,按照 Swain 手册提供的方法,可将任务之间的相关情况分成 5 类:完全相关(CD),高相关(HD),中相关(MD),低相关(LD),以及零相关(ZD),相应的人误概率的计算公式为:

$$CD, P(B|A) = 1 \quad HD, P(B|A) = \frac{1+P(B)}{2} \quad MD, P(B|A) = \frac{1+6P(B)}{7}$$

$$LD, P(B|A) = \frac{1+19P(B)}{20} \quad ZD, P(B|A) = P(B)$$

3.1.3 THERP 表格介绍

THERP 表格是汇集一般工业与核能工业人员在操作上的失误概率与种类,经汇总后整理而得。使用 THERP 量化人为失误率,先要找到合适的表格。THERP 表格共 27 个(在本文中略),可分为 7 个部分。各表格的大致内容如下:

表 20-1 及表 20-2 为不同状态下粗值筛选所决定,由于对不需深入量化的人为失误,皆以 0.1 作为粗值,所以这两个表格较少使用。表 20-3 和表 20-4 为在短时间内产生报警数目与运转员判定系统状态失误的关系。表 20-5 至表 20-8 为针对有无程序书的各种情况下,评估运转员忽略了某些步骤的可能性,在量化维修、测试时的人为失误时常常使用。表 20-9 至表 20-14 则为操作失误率的相关表格,对于各种类型的按钮、旋钮、阀门等的操作失误机率有极细的分类。表 20-15 至表 20-19 为 PSF 的选择依据及相关性的参量。表 20-20 至表 20-21 为不准度范围判断的依据。最后,表 20-22 至表 20-27 为动作的相关性表格。

3.1.4 THERP 模式的特性

THERP 为人因分析者提供了大量用于确定人员操作失效的数据,用于评价人员的操作失效比较方便。但应注意,THERP 由查表量化所得的值仅为单一操作员的失误率。人因可靠性分析往往需要模拟整个运行班组的行为,因此,在使用 THERP 时需另外考虑运行班组之间成员的相关性,否则所得的结果将过于保守。同时,THERP 使用行为修正因子(PSF),其 PSF 的影响也由查表的方式决定。这些数据常由分析人员主观选择,因此,其结果有不确定性。虽然 THERP 存在一些不足之处,但它仍是较成熟、使用较普遍的人的可靠性分析方法。

总之,THERP 最本质的优点在于提供了 HRA 事件树及基本 HEP 数据库,因而人员可靠

性分析者在了解系统及运行班组的状况后,就可利用 THERP 模式查表量化人因失误。

3.2 人的认知可靠性模型(HCR: Human Cognitive Reliability)

3.2.1 HCR 的背景

由于 THERP 主要是描述与时间无关的人因失误,而现代的人—机系统常常是与人的认知判断有关,HCR 法就是为了评价运行班组未能在有限的时间内完成动作的概率而开发的。

3.2.2 HCR 方法描述

1) HCR 的两个假设

HCR 有两个很重要的基本假设。第一个基本假设:它认为所有的人员动作的行为类别可

以根据图 3 所示的逻辑,依据是否为例行的工作、程序书的情况及训练的程度等,分为技能型、规则型及知识型等 3 种。①如操作员经过很好的培训,有完成任务的动机,清楚地了解任务并具有完成任务的经验,这

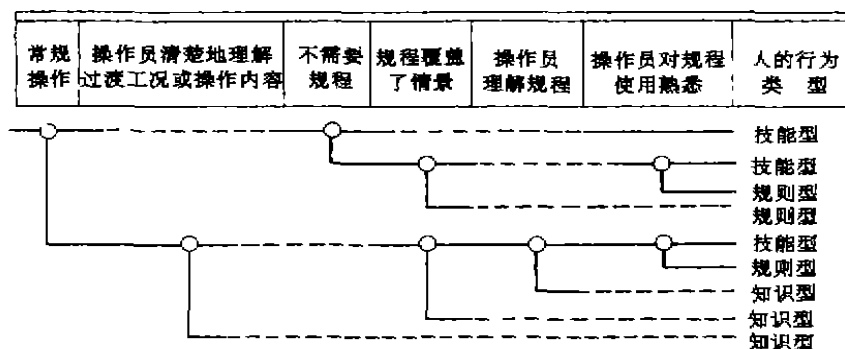


图 3 HCR 行为类型辨识树

类行为可以划归为技能型。②如操作员在过渡工况响应条件下,能够清楚地理解其所需运用的运行规程,则这类行为应划归为规则型。③如不符合上述两类状况或操作员必须理解电厂状态条件,解释一些仪表的读数或者作出某种困难的诊断时,这类行为应归划为知识型。

第二个基本假设:它认为每一种行为类别的失误概率,仅与允许时间(t)和执行时间($T_{1/2}$)的比值有关。根据此假设,HCR 模式由模拟机训练所收集的数据,归纳得到如下的公式:

$$P = e^{-\left(\frac{t}{T_{1/2}}\right)^{\alpha}} \quad (1)$$

式中, α 、 β 、 γ 是由数据归纳而得与行为类别有关的参数,它们服从威布尔分布。由于每个运行班组的执行时间可能因各类情况而有所不同,故在使用公式之前要用修正因子修正。在 HCR 模式中所考虑的关键的行为形成因子有 3 个,训练(K_1)、心理压力(K_2)及人—机界面(K_3)。修正的公式表示如下:

$$T_{1/2} = T_{1/2, \text{nominal}} \times (1 + K_1) \times (1 + K_2) \times (1 + K_3) \quad (2)$$

式中, $T_{1/2, \text{nominal}}$ 为一般状况(如模拟机训练)的执行时间。有关参数 α 、 β 、 γ 和 K_1 、 K_2 、 K_3 的选取见表 2 和表 3 所示。

表 2 参数 α 、 β 、 γ 选取表

行为类型	α	β	γ
熟练(SKILL)	0.407	1.2	0.7
规则(RULE)	0.601	0.9	0.6
知识(KNOWLEDGE)	0.791	0.8	0.5

2) HCR 使用步骤

使用 HCR 模式并没有固定的先后步骤,但必须执行以下步骤,其次序仅供参考:①决定

允许时间;在决定使用 HCR 模式量化人员动作之前,已认定此动作与时间有关。由于允许时间的长短对量化结果有决定性影响,因此,必须和系统分析员或有关安全分析专家讨论,并了解决定允许时间的依据。

②决定行为类别:据图 3 所示的逻辑,判定人员动作类别,再从表 2 中决定 α 、 β 、 γ 等参数的取值。

③决定一般执行时间:经由访谈或模拟机的经验,获得一般状况下运行人员对系统状况的反应情形;也可根据程序书的步骤,判定运行人员动作所需的时间。④决定修正因子:由访谈结果、事件的紧迫性与重要性及对控制室盘面的

表 3 HCR 模型的行为形成因子和相关的系数

因 子		系 数
操作员经验(K_1):	1. 行家,培训水平优秀	-0.22
	2. 一般知识水平	0.00
	3. 新手	0.44
应激水平(K_2):	1. 严重应激情景	0.44
	2. 潜在应激情景	0.28
	3. 优化,无应激	0.00
	4. 低度应激	0.28
人机界面(K_3):	1. 优秀	-0.22
	2. 好	0.00
	3. 一般	0.44
	4. 低劣	0.78
	5. 极端低劣	0.92

的观察,根据表 3 决定 K_1 、 K_2 、 K_3 3 个修正因子,并将其带入公式(2),修正一般执行时间,得到较符合实际的执行时间。⑤量化失误概率:将以上步骤所得的允许时间、修正后的执行时间及根据行为类别决定的参数,代入公式(1)量化失误机率。

3.2.3 HCR 的特性与限制

前面介绍过,公式(1)由模拟机训练的数据归纳而得。因数据本身模拟的人员失误是整个运行班组的行为,所以,人员间的相关性已包含在内,毋须再作考虑。另外,当允许时间对执行时间的比值太大时,以 HCR 模式量化而得的失误概率很可能小于 10^{-4} ,甚至极接近于零。一般认为,即使非常简单的工作,也不能排除万一的失误概率,因此,假设 10^{-4} 为最小的截止值。

3.2.4 对 HCR 的评价

HCR 模型提供了一种用模拟机实验数据,将其作为进行人—机交互作用过程中的人因可靠性分析的有力工具,但问题是人的决策过程往往是综合利用各种能力的过程,很多情况下难以将其明确地划分为技能型、规则型或知识型,而这种划分理论上的依据也不足。另外,威布尔分布中的 3 个参数来源于模拟机实验,它受到班组成员的知识水平、模拟机界面、人的应激水平等条件因素的影响,这更也限制了 HCR 模型的实际应用^[10]。其次,HCR 模型中的 $T_{1/2}$ 值往往需要专家判断确定,这增加了模型的不确定性。但由于它首先使用了模拟机的实验手段,结果较为客观并开始深入到人的失误的内在机理的研究领域,这是 HRA 研究分析的一大进步。

3.3 成功似然指数法(SLIM: Success likelihood index methodology)

1) 当人因失误的数据非常缺乏时,对人的可靠性的评价就不得不依靠成功似然指数法^[10]。该法于 1984 年由 Embrey 首先提出,它是一种由专家集体进行评判的方法。主要用于多维因素影响状态下的人因可靠性分析,并且只有当对人员的各种响应的绩效形成因子已知的条件才可能进行定量化计算^[11]。

运用 SLIM 方法应完成 10 个步骤^[12]:①对情景和任务的集合进行定义;②PSF 选定;③对任务按 PSF 排序;④理想点的确定应便于换算;⑤相关性的检查;⑥赋权重值的过程;⑦计

算成功似然指数(SLI);⑧把 SLI 值换算成概率;⑨不确定性边界的分析;⑩成本-效益分析。

聘请的专家必须对所评价的任务进行打分,并对各项任务的 PSF 因子排序。各位评审员都是基于一个共同的参考点进行评分。每项任务的成功似然因子的计算可按下列公式进行:

$$SLI_j = \sum_i W_i R_{ij}$$

式中, SLI_j —第 j 项任务的成功似然因子; W_i —PSF _{i} 因素在任务完成中的权重值;

R_{ij} —第 i 种 PSF _{i} 因素的影响,由专家对 j 任务所确定的比分(the scaled rating)。

为将每项任务的成功似然因子转换为概率值,假定采用对数形式,就有下列关系式:

$$\log HEP = aSLI + b$$

式中,系数 a 和 b 分别由两个边界点(最坏情况和最好情况)的已知的人为失误概率值求解出来。这种权重平均的办法,在工程上十分方便,它与 THERP 法完全不同,不需要进行操作分析,因而也不需要各个操作失误概率进行确定。

3.4 THERP+HCR 模式

3.4.1 THERP+HCR 模式简介

现代人—机系统中,人的动作行为包含诊断和操作两方面。而从前述可知,THERP 主要是利用人因事件树对人因事件中涉及的所有人员行为按事件发展的过程进行分析,并在事件树确定失效途径后进行定量的计算。而 HCR 方法的着眼点在时间上,即认为对于一个人因事件中的一个人员行为,特别是对事故后的诊断行为,允许操纵员进行响应的的时间以及操纵员平均所需执行时间之比决定了人因失效的概率。因此认为,HCR 对确定事故后操纵员在进行事故诊断阶段中可能的人因失效较好,而 THERP 则为人因分析者提供了大量可确定人员操作失效的数据,用于评价人员的具体操作失效更为方便。因此,采用结合 THERP 与 HCR 分析方法定量评价事故行为较为合理,即在事故诊断阶段,用 HCR 对该阶段可能的人因响应失效概率进行评价,而用 THERP 及相关数据对在进行具体的干预操作行为中可能的失误进行评价。THERP+HCR 模式已在大亚湾核电站和岭澳核电站 PRA 分析中得到实际运用,所得到的分析结果对两个核电站的建设、安全设施的改进和安全运行发挥了很大的促进作用^[13,14]。尤其是大亚湾核电站的一级 PRA 分析已通过国家核安全局和国际原子能机构的评审。

3.4.2 应用实例

1) 事件描述

A 工况下发生蒸汽发生器(SG)传热管断裂事故,20 秒内引发二次侧放射性高报警,安全工程师由操纵员呼叫 5 分钟后到达主控室并进入 SPI 规程,监视有关参数,二回路操纵员根据规程识别且隔离故障 SG,高压安注失败(1 分钟完成该操作),安全工程师发现 $\Delta T_{sat} < 10^\circ\text{C}$ 且指令操纵员手动启动安注,但安注不可用,安全工程师决定进入 U 规程(SPI 执行时间为 10 分钟),安全工程师用 4 分钟鉴别安注及蒸汽发生器的可用性,安注不可用,指令二回路操纵员将排大气阀 GCT113V 和冷凝器阀 GCT117VV、GCT121VV 开至全开,对冷凝器进行快速冷却,操纵员用 1 分钟完成上述操作。60 分钟内若未成功实施快速冷却将导致堆芯熔化。

2) 事件分析

该事件失误概率分析可分为 3 个阶段:①操纵员发现二次侧放射性高报警信号进入 DEC 规程并呼叫安全工程师;失误概率 P_1 可认为非常小。②安全工程师先后进入 SPI、SPU 规程,作出二回路操纵员用冷凝器进行冷却的指令;其诊断行为属规则型,可用 HCR 模式计算其失

误概率 P_2 。③操纵员将排大气阀 GCT133VV 和冷凝器阀 GCT117VV、GCT121VV 开至全开位置,其失败概率 P_3 可用 THERP 方法求出。

3) 建模与计算

事件失误率 $P = P_1 + P_2 + P_3$

(1) 根据事件分析中①,可令 $P_1 = 1.00 \times 10^{-4}$

(2) $P_2 = e^{-\frac{tT_{1/2,n}}{\alpha}}$

根据事故描述中有关数据,可得:

$t = 60 - 5 - (1 + 1) \times 1.44 = 52.12$ (分钟) $T_{1/2,n} = 10 + 4 = 14$ (分钟)

考虑紧张因子修正得 $T_{1/2} = T_{1/2,n} \times 1.28 = 14 \times (1 + 0.28) = 17.92$

规则型行为取 $\alpha = 0.601, \beta = 0.9, \gamma = 0.6$

$P_2 = 3.49 \times 10^{-2}$

(3) 操纵员所进行的动作,其人因事件树如图 4 所示。

a_1 操纵员成功完成安注

A_1 操纵员未成功完成安注

b_1 操纵员成功完成快速冷却

B_1 操纵员未成功完成快速冷却

a_2 值长成功纠正操纵员的错误并完成安注

A_2 值长未成功纠正操纵员的错误并完成安注

b_2 值长成功纠正操纵员的错误并完成冷却

B_2 值长未成功纠正操纵员的错误并完成冷却

查 THERP 表投入安注的失误概率为 6×10^{-4} , 考

虑紧张因子,修正为 1.2×10^{-3} 。

操作 GCT 阀的失误率为 3×10^{-4} ,修正为 6×10^{-3} 。

考虑值长与操纵员之间的相关性为低,其监测失误概率为:

$$[1 + 19 \times 3 \times 10^{-3}] / 20 = 5.29 \times 10^{-2}$$

该事件树的失误路径有两个, F_1, F_2 , 它们的失误率分别为:

$$P_{F1} = P_{A1} \times P_{A2} = 1.2 \times 10^{-3} \times 5.29 \times 10^{-2} = 6.35 \times 10^{-6}$$

$$P_{F2} = P_{B1} \times P_{B2} = 3 \times 10^{-3} \times 5.29 \times 10^{-2} = 1.59 \times 10^{-4}$$

总的操作失误为 $P_3 = P_{F1} + P_{F2} = 2.23 \times 10^{-4}$

事件总的失误率: $P = P_1 + P_2 + P_3 = 1.00 \times 10^{-4} + 3.49 \times 10^{-2} + 2.23 \times 10^{-4} = 3.53 \times 10^{-2}$

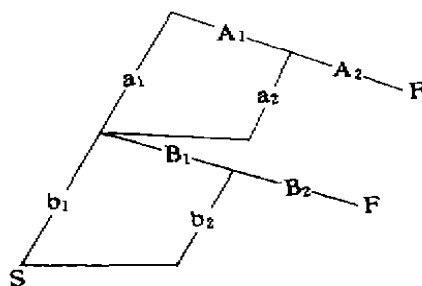


图 4

4 讨 论

4.1 现用 HRA 方法的不足之处

迄今为止, HRA 已有数十种方法, 这些方法对 HRA 的发展和应用起了良好的推动作用。但正如许多 HRA 专家所评论的那样, 它们均存在诸多不足^[2,3,15]。

1) 使用 HRA 事件树的两分法逻辑(成功与失败)不能真实、全面地描述人的行为现象, 因人在对系统的动态响应过程中, 可能有多种选择方式, 其优化价值不同。同时, 人的认知失败产生的失误行为的形式多种多样, 其对风险的后果不同, 决不能用简单的“失败”概括。

2) 缺乏充分的数据。人的可靠性数据的缺乏是一个严重的、长期未决的而困惑至今的老问题,这与数据收集方式和人的心理状态有很大关系。这些数据对于复杂系统中人的行为的定量化预测具有重要意义,它应包括与时间相关的和与时间不相关的人误数据。

3) 多依赖专家判断。由于缺乏在复杂系统中人在真实运行环境下或培训模拟机上的人员失误数据,只能采取弥补性质的模型(如时间相关性模型)和/或专家判断作为 HRA 的基础。专家判断法的使用难以显示出专家群体水平的一致性,并且预测的正确性和准确性受到很大的主观因素影响。

4) 缺乏对模拟机数据修正的一致认同。使用来自模拟机的数据,对专家判断的人的绩效数据进行修正必须得到足够的重视。但是模拟机实验并不能完全反映真实的运行环境,如何修正来自模拟机的数据以反映真实环境下的人的绩效一直是一个有待研究的课题。

5) HRA 方法的正确性与准确性难以验证。HRA 的各种方法,对于真实环境下的人的可靠性的预测的正确性几乎无法得到证明。特别是非常规任务中人的可靠性评价的正确性更是一个难题,例如与时间相关的误诊断、误决策的概率。

6) HRA 方法缺乏心理学基础。一些 HRA 方法/模型中缺乏对人的认知行为及心理过程的探索和研究;另一方面,尽管认知模型类型颇多,但难以找到与工程实际的结合点。

7) 缺乏对重要的行为形成因子的恰当考虑和处理。即使在较好的 HRA 方法中,一些重要的 PSF 也没有给予充分的考虑,例如组织管理的方法和态度、文化差异、社会背景和不科学行为等,在处理方法上也缺乏一致性和可比性。

4.2 HRA 的发展趋势

HRA 方法的模型是以多种学科为基础而建立的,着重研究产生人的行为的情景及它们是如何影响人的行为的,因此,笔者认为 HRA 将沿着下列方向发展:

1) 建立多种学科相结合的干扰信号图形事件描述。通过干扰信号图形的操纵员事件树,分析各个节点处的人的事物机理和可能的事物模式^[3]。

2) 建立人的信息处理理论上的人的行为通用模型,即带有反馈的序贯式行为模型。

该模型的研究重点是结合系统的实际运行经验和数据,探究和查找人的认知不同阶段的诱发失误环境与它如何通过人的失误机理产生人的非安全动作,并给出定量分析的方法^[2]。

3) 循环式的人的行为模型。即假设人的任何行为都是在意向或事件的驱动下产生的,人的动作过程不是事先规定而是依赖于当时情景条件建造出来的,这些动作之间高度相关。

4) 建立人因数据库。目前的单纯数字式数据或数字加简要条件式数据,不能满足人因分析者对数据所描述的人误的理解和对该数据的有效使用^[15],因此,需研究和使用的能保持失误因素间原始基本关系的新型数据。

5) 人的行为机理研究。对此,虽以 Reason1990 年的著作《Human Error》为里程碑而进入一个新的阶段^[16],但其后无多少具有实质性进展的成果问世。人的行为机理研究应建立在个体、群体和组织行为的基础上,系统地研究人的行为特性、行为模式、失误源、控制管理、失误形态等,完善和拓展人的行为机理研究的内涵。

(收稿:2000 年 8 月;作者地址:湖南省衡阳市;南华大学经济管理学院;邮编:421001)

参考文献

- 1 张 力. 在更广泛基础上预防和减少事故. 管理工程学报, 1998, 12: 59~63.
- 2 高 佳、黄祥瑞、沈祖培. 人的可靠性分析: 需求、状况和进展. 中南工学院学报, 1999, 6: 11.
- 3 Hollnagel E. CREAM. New York: Elsevier Science Ltd, 1998.
- 4 Hollnagel E. Reliability Analysis and Operator Modeling Reliability Engineering and System Safety, 1996, 52: 327~337.
- 5 G. W. Hannaman, A. J. Spurgin, Y. Lukic, Human Cognitive Reliability Model for PRA Analysis, 1985.
- 6 黄祥瑞. 可靠性工程. 北京: 清华大学出版社, 1991.
- 7 张 力、王以群、邓志良. 复杂人机系统中的人因失误. 中国安全科学报, 1996, 6(6): 38.
- 8 王 晋、鲍 麟. 人误率预测技术方法的几个问题及应用时的建议. 中南工学院学报, 1999, 6: 59.
- 9 Swain A. D., Guttman H. E., Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. NUREG/CR-1278, Washing, DC, 1983.
- 10 张 力、邓志良. 人员可靠性定量评价方法. 中南工学院学报, 1995, 6: 78.
- 11 NUREG/CR-2718. Washington, 1984.
- 12 D. E. Embrey, P. Humphreys, E. A. Rosa, B. Kirwan, K. Rea, SLIM-MAUD: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgement, 1984.
- 13 张 力等. 复杂人-机系统中人员可靠性研究. 国家自然科学基金项目 79570089 研究报告, 1998.
- 14 张 力、黄曙光、黄祥瑞等. 岭澳核电站人因可靠性分析. 中国核科技报告. 北京: 原子能出版社 (待刊).
- 15 张 力. 人因分析面临的问题及发展趋势. 中南工学院学报, 1999(6): 8.
- 16 Reason J. Human. Error. UK, Cambridge: Cambridge University Press, 1990.

Methods for Human Reliability Analysis

Zhang Li* Huang Shudong** He Aiwu Yang Hong

(Nanhua University)

Abstract

History of human reliability analysis (HRA) is reviewed. Methods frequently used in recent decades are compiled. Three kinds of HRA methods, namely THERP, HCR, and SLIM are emphatically introduced in detail, and their backgrounds, steps in application and characteristics are discussed. The advantages of THERP+HCR are analyzed, and exemplified by a case. The defects of HRA are indicated with the prediction of its developing trends.

Key words: Human Reliability Analysis Method

* Prof.

** Engineer