

# 核动力厂运行中人的因素

## 改善人和机器协同工作的途径

E. Swaton, V. Neboyan 和 L. Lederman

在大而复杂的交互性系统中，人为差错往往是系统发生故障的主要原因。核动力厂的运行经验表明，在与安全有关的意外事件中，很大一部分是由人为差错引起的。然而，经验也指出，如果对工厂的状况了解得很透，人的干预可以是很有效的。因此，合适的人—机衔接，不仅对防止人为差错很重要，而且对帮助操纵员应付意外情况也很重要。

人的可靠性可理解为定性术语，也可理解为定量术语。可以定性地把它说成人成功地完成各种必要的活动使系统能可靠地工作和可以被利用的本领。定量地看，它指可用于概率安全分析 (PSA) 等方面的故障率或差错概率之类的数据。

### 教育和培训

合格的运行人员，是保证核动力厂运行安全可靠的一个核心问题。为了使运行人员达到并保持必要的作业水平，必须对他们持续不断地进行教育。这种教育包括初次培训、再培训、以及更新和扩大知识和技能的活动。尽管每个国家一直在根据本国条件建立它自己的教育体系，但核动力厂运行人员应该掌握的特殊技能各处都是相同的。既然在核动力厂的安全可靠运行方面不可能有任何通融的余地，因此每个国家的核动力培训计划都必须达到相同的水平。

首要的技能（特别是在将来）是适应能力，即应付意外情况的能力。这意味着，应有能力发现、认识和简洁地阐述问题——并判定该问题是否应该解决以及如何解决。

教育主要指正规的学习和深造，而培训则着眼于

Swaton 女士，Lederman 先生和 Neboyan 先生都是核能和核安全司工作人员。

比较具体的任务。培训除在课堂或工作岗位进行外，利用模拟器达到此目的的做法，已引起人们的特别关注。大多数有核动力厂的国家都设有模拟器培训计划。一般说来，进展情况都比较好。但它们的价值可能受到模拟器的年龄、型号、大小和容量的限制。不管怎么说，对于提高工厂的运行安全性和提供正常和异常工况下工厂控制方面的知识和技能来说，模拟器培训和再培训是必不可少的。此外，可以预见，模拟器培训对下述的两个方面也有好处。其中一个方面是 PSA，从 PSA 获得的见识可以用来选择培训用的场景，反过来模拟经验也可以用来更新和改进 PSA。另一个方面关系到从人的因素角度评价工厂改进工作的可能性。这包括评价新装备，评价正常和应急操作程序的正确性和切实可行性，以及评价培训计划的调整和修改工作。

### 模拟器培训

多年来，全域模拟器一直在当作培训核动力厂操纵员的一种大型工具使用着，现已成为技术上成熟的设备。现在我们可以处理五年前还无法处理的一些培训场景。在今后五年中，我们能利用我们将要具有的计算能力做些什么呢？一方面，有些专家认为，为了提供更为广泛的培训，需要更强的计算能力。然而，普遍的感觉是，现有的计算能力已足以做好这项工作。与此同时，一种明显的动向是建立高保真度模型。过去的五年，重点一直放在反应堆堆芯模型和反应堆冷却剂系统模型的高保真模拟上。提高保真度是否正确，这是一个需要更周密思考的问题。提供更高的保真度是一回事，断定是否需要高保真度是更为重要的另一件事，因为现有的模型不能满足全部培训任务的需要。国际原子能机构 (IAEA) 于最近召开的核动

力厂培训用模拟器专家会议指出,有的设计人员发现了一些要求模型向前发展的培训要求。这是个好的迹象。培训用模拟器的设计方案确实应根据对学习目标的考察结果修改。这是过去从未有过的情况。

全域模拟器虽是一种强有力的工具,但由于复杂和昂贵,让它覆盖所有培训要求有时是不适当的。经估算,只要动用全域模拟控制室的25—30%,就能提供全部培训的75—80%。

为了进行只需了解工厂的一部分或少数功能的培训,正在使用“部分任务”模拟器。这些模拟器或是取工厂解析器或微型模拟系统的形式,或是取“功能”模拟器的形式。在这些情况下,为系统建立适当的“智力模型”是很重要的。由于重点注意了处理和利用空间信息的能力,因而这种模拟器为我们提供了对于应做的操作进行周密思考的机会。有人使用了一台比例为一比二的压水堆(PWR)冷却系统模型(称作玻璃模型),这是一个很好的实例。即使采用的压力与实际不一样,但能够直接观察热力学过程,这一点的培训价值就很大。

关于培训用模拟器的进一步发展,注意力已集中于人脑的活动过程这样一个问题上,即我们是如何学习的?如何在对人类的认识本领已经有了较好了解的基础上解决好人一机衔接问题,从而减少操纵员的超负荷并提高运行实绩?

总结应急工况模拟器培训工作的经验,表明有安全意义的事件提供给操纵员的有关这一事件的发生和发展规律的情况,往往与在模拟器上见过的景况差得相当多。此外,由于应急工况是不多见的事件,因而预测和分析人的行为能力存在一定困难。然而,对于恶劣的工厂工况而言,模拟器培训的有用性和重要性是公认的。如果设计事故场景时能做到事件顺序可以从不同的功率水平开始,而且模拟工作一直可以进行到堆芯变质为止,则情况尤其是这样。此外,如果学员在处理某种特殊情况时出错,模拟工作可以停下来,指出所犯错误并进行讨论。随后,可以恢复这一场景,从而为教员和学员双方提供有价值的反馈。借助监测学员行为的自动化系统或建立向教员报告差错的图表,可以有系统地收集数据。PSA正在日益增多地利用从模拟器培训期间收集到的有关人的行为的数据。

### 收集人为差错数据

对异常事件的分析和PSA的研究结果,已经显

示出大部分意外事件都有人为差错方面的原因。核动力厂运行经验是有关人的行为/人为差错信息的主要来源。目前除了有向本国管理部门报告与安全有关事件用的国家系统外,还有若干国际性的报告系统。经济合作和发展组织核能机构(NEA/OECD)的事故报告系统(IRS),收集来自西欧、加拿大、日本和美国的典型实例。IAEA-IRS<sup>1</sup>与NEA/OECD-IRS基本相同,但它还包括来自东欧和发展中国家的报告。另一个系统——伊斯普拉联合研究中心的异常事件报告系统——收集包含在某些国家系统中的情报。然而,在这些报告系统中,没有专门对人为差错做出鉴定,因而需要建立一些单独列出人为差错在事故原因中所占比重的分析方法。只有在为数不多的事例中,电力公司建立的几个系统才致力于鉴定人为差错在意外事件中的作用。

已确定的几种普遍存在的情况是:

- 试验和维修之类操作不当是发生差错的常见根源。采用自动操作程序可以使某些问题得到缓解。
- 在可利用率或冗余度较低,或自动化程度较差的系统中,人为差错比较频繁。
- 在报警信号刚被触发后的异常工况下,较易发生人为差错。
- 不合理的设计(从系统工程学、控制室布局和人类工程学原理的观点看)是发生人为差错的主要根源。
- 运行人员换班时情况交接不清是发生差错的普遍原因。

PSA在确定工厂的哪些系统需要人干预和根据类似任务共同原因分门别类汇集这些干预情况方面,能够提供有价值的见解。然而,由于普遍缺乏有关人的行为(特别是在异常工况下的行为)的客观数据,因而它的应用是有限的。在这方面,应当把PSA结果仅仅看作人因方面可能有问题的“指示剂”,而不是把它看作人的行为的预言者。

### 信息反馈

事故分析在某种程度上提供了了解人为差错的可能性。操纵员必须获得反馈,但问题是如何建立评价这种反馈的规范。

在解决与人为差错和操作经验含意有关的问题方面,有的国家似乎把重点放在数据库上,而另一些国家则放在模拟器上。在这种情况下,可以提出这样的

问题：我们应当如何收集操纵员的经验，以及人们怎样才能对不同方面的各种好处做出判断？设计人员是否要有坚定的策略？许多专家的看法是：在这方面的研究必须沿着不同的方向继续进行，看来搞好协调是必要的。\*

目前，几个研究中心正在对人的因素在重大事件中的作用方面的反馈信息进行分析。美国核管理委员会（NRC）已经制定了一项正式的事故调研计划（IPP）。一个目的是确保利用系统的、技术上完善的方法，对运行事件进行调查研究。每次紧急停堆都必须向 NRC 报告，IPP 的目的是如实地叙述情况。

在日本，必须在 48 小时内向数据库提供事件的初步报告，并在 30 天内提供全面的报告。人为差错造成的事件约占全部事件的 10%。半数以上（54%）的事件导致了自动停堆，15% 造成工厂功率下降；31% 未产生影响。造成人为差错的原因中，有一半（51%）是维修不够造成的，29% 是操作不当造成的。

一位比利时专家的估算指出，在 7 座反应堆的 40 次紧急停堆中，70% 有某种人为因素。由法国电力公司（EDF）完成的较深入的统计分析指出，在活动极少的夜间，还有午餐期间，人为差错相对来说要少些。最常见的差错类别包括疏忽和操作不及时。至于差错的机制，最常见的是忘记完成某种操作和没有找到正确的操作，连带的问题是对系统状况的诊断不当。

模拟工作虽然也能提供操纵员行为方面的有效反馈，但是有效的研究需要花大量金钱和精力。例如，为了能迅速获得操纵员经验方面的反馈，法国就建造了一台计算机化控制室的全域模拟器。

### 操纵员辅助系统

操纵员辅助系统是指附加到核动力厂控制室内的一套设备，目的是帮助操纵员完成其工作，并减少人为差错的几率。这套设备包括的范围很广，从简单的诸如把一组类似的显示互相区别开的色标显示，到复杂的诸如由计算机组合的影象显示，这种显示把分散

在控制室各处的大量指示器的许许多多读数，集中成一组简明扼要的显示，并让它呈现在操纵员面前。人们一直把主要精力用于发展计算机化的操纵员信息和辅助系统。

鉴于预定的目的不同，已经做了各种系统的概念设计。早期的系统主要致力于关键安全功能的监测以及各种不正常现象的探测和定位。后来的系统则超出了这个范围，它们可另外提供工厂在不同运行方式下正常工作时的信息，并预测工厂的行为。

对计算机化操纵员辅助系统的信赖日益增加，这种信赖应根据打算完成的任务加以检验，因此需要注意人和计算机各自的长处和短处。

鉴别。虽然计算机在识别预先设定的模式方面是胜任的，但人在识别任何可能发生的模式方面略胜一筹。而且，人还能处理不完整的信息。计算机的长处在于能对测量值进行判断和验证，能处理复杂的计算。对于鉴别来说，计算机主要依靠根据给定规则进行推断。

分析和推断。计算机虽然能够快速而可靠地进行复杂的演算，但应用直接推断方法的能力有限。与此相反，人可以利用判断、经验和掌握的知识，透过现象看到本质。

比较。大量精确数据的处理和重新组合，以及根据预先规定的规则对这些数据进行比较，显然是计算机的长处。然而，人能够使用来源不同形式不同的数据，进行比较时主要依靠经验，其次才依靠精确的推断。

规划。对于为明确的问题找出最优解决方案这样的任务，计算机当然具有优越性。但对于问题反复变化但变化又不大的情况，人将显示出其长处，他能迅速调整现程序来适应这种情况，必要时甚至可以设计新程序。

总的说来，计算机仅在被处理的问题、知识以及规则或程序都很明确的条件下，才能有效而可靠地发挥作用。操纵员不仅能够与上述条件相同的情况下完成任务，而且也能处理不够明确的问题、不完整的知识以及不齐全的规则或规章。所以，在计算机一旦不能工作的情况下，人仍然能够控制这个系统。因此，计算机能较好地地完成某些任务这一点，不应成为可以让它取代操纵员的理由。

### 供安全决策用的 PSA 情报资料

在过去的 15 年中，PSA 已逐渐成为评价反应堆

\* 这是参加 IAEA 专家会议的与会专家们的一致意见。会议是 1987 年 5 月在罗斯基勒召开的，论题是“在核动力中人的因素信息的反馈：运行经验与系统分析和运行的关系”。

安全性的主要手段。已经完成了 30 多项 PSA，其成果已经为工厂的设计和运行提供了非常宝贵的知识。尽管其潜力很大，但在决策方面实际应用这些分析结果的事例一直很少。一个原因是，在 PSA 报告中，有用的结果与大量的和决策者无关的技术情报混杂在一起。另一个原因是，PSA 报告只有精通方法学的人才能看懂。

几年前就开始着手为比较直接和交互式地使用 PSA 报告中的情报创造条件。这些工作的目标是建立一种使运行安全管理部门容易学会的“实况性 PSA 模型”。

在同一时期，小型计算机，特别是个人计算机获得了惊人的发展。所以，目前许多工业领域都在应用小型计算机，有的作为独立设备使用，有的作为与大一些的计算机相连的工作站使用。

同样，人们一直在研制用于组合 PSA 情报的一体化系统，这种系统利用了小型计算机工艺学的最新研究成果。由于这些系统具有高度的交互性和“方便用户”的特点，特别适用于 PSA 情报的更新和回答“如果……那就……”一类提问。

PSA 情报在运行安全管理部门的一些应用，是建立在工厂构形的变化也许会影响整个工厂的安全性这一基础之上的。这些应用包括控制和评价主要安全系统的状况；修改运行程序；改变技术要求（特别是有关试验和维修的技术要求以及允许的停役次数）；排列待修物项的轻重缓急；从工厂各系统间的相互作用角度评价设计变更；排列检查活动的轻重缓急。

眼前的开发工作的目标是，为工厂处于正常运行工况下的决策提供情报。软件包中有一个根据失效树分析和事件树分析的结果建立的工厂模型。电力公司的运行人员和管理机构的工作人员是这些软件包的主要用户。

最近已开发出的两个系统是：

**PRISIM**（概率法安全情报管理系统）。这是一个供个人计算机用的软件包，用它可以快速存取与 PSA 有关的情报。该数据库包含从基本的 PSA 结果中抽出的经过预处理的情报，还有一个允许对由工厂条件改变引起的工厂安全性变化进行评估的工厂安全模型。涉及工厂构形变化的安全问题，可以用一种允许用户（根据方框图或组件一览表）规定新的工厂状态并计算出最终的安全裕度的模型来处理。为了给安全系统和操纵员的动作排次序，引入了衡量重要性的各种尺度。这套代码还能研究安全系统对特定故障

的响应情况。这项研究能揭示出设计中的薄弱环节，诸如辅助系统容易产生故障之类的弱点。来自 PSA 基本结果的经过预处理的情报，包括对最重要的事故顺序的描述；操纵员的恢复性动作；辅助系统的衔接点；技术规范库；有关安全有关系统、子系统、部件和操纵员动作的轻重缓急的排列顺序。**PRISIM** 是为美国 NRC 开发的，用于协助检查员。目前已安装在几座核动力厂，如阿肯色 1 号核电厂 1 号机组，桃花谷 -2 和塞瑞 -1。

**ESSM**（基本系统状态监视系统）。ESSM 是根据失效树分析技术建立的软件系统，它给工厂操纵员提供了一种在线设备。它使操纵员能够在交互气氛中迅速对工厂系统进行某些概率评估工作。中央控制室的键盘和可视显示监视器用来输入并显示工厂物项的当前状态和构形。操纵员在任何时候都可以要求 ESSM 评估基本系统的整体可利用性。ESSM 将在考虑工厂当前部分设备停机和当前构形所产生效应的情况下，分析复杂系统的失效树（它用来模拟冗余系统和复杂系统的相互作用）。然后把采用概率准则得出的基本系统的可利用状况显示给操纵员。ESSM 还同时监视确定论的运行规则。如果违反运行规则的现象需采取补救措施，则与此有关的所有情报都将显示给操纵员。除评估外，ESSM 还能给操纵员提供紧急维修方面的推荐意见，并提供制定维修规划的便利条件。最近，英国的汉沙姆 -2 核电厂已经安装了 ESSM。

### 国际合作

在核动力厂运行中强化人的因素方面，存在着许多可能性。这可以通过采取改进装备之类的工程技术措施，或采取能改善操纵员行为的措施来实现。然而，在应采取什么措施和应把重点放在何处的问题上，似乎还没有形成普遍同意的意见。这就是 IAEA 召开核工业中人 - 机衔接（控制设备和仪器仪表，机器人学和人工智能）国际大会的理由。\* 这次会议于 1988 年 2 月 15 - 19 日在日本东京召开，是由日本政府作东道主并在 NEA / OECD 和欧洲共同体委员会（CEC）合作下组织的。会议论题包括，分析工厂运行中人的行为，评议用来改善人的行为能力的人因工程措施，和向操纵员提供更多、更完善信息的重要性。

\* IAEA 将出版论文汇编。