

全球核能安全动态

生态环境部核与辐射安全中心

2024 年 12 月

目 录

- 法国核安全理论五十年的演变

法国核安全理论五十年的演变

2024年8月28日，法国核学会发表《安全理论五十年的演变》文章。2024年是法国核电计划启动50周年，NRC成立50周年，WASH-1400报告发布接近50年（1975年），为此法国核学会召开了核安全理论演变的研讨并进行了总结。文章指出，在核能领域，安全理论是一种不断发展的理念和实践，而非固定不变的规则，这些安全理念随着时间和经验的积累而演变。以下为全文翻译。

最初的核安全原则

核能发展伊始就关注安全问题：1942年12月2日，在芝加哥进行第一次达临界时，一名操纵员准备用斧头砍断固定控制棒的绳子。意大利的物理学家恩里克·费米（Enrico Fermi）看到团队很紧张，于是中断了操作，并邀请他们共进午餐，好让他们恢复冷静。在法国，“反应堆安全”关注的是第一批反应堆（Zoé、G1等）可能发生的事故、后果和预防措施。彼时核安全还没有成为一门学科，也没有与设计和管理区分开来。在海军上将海曼·里克弗（Hyman Rickover）领导下，美国在宾夕法尼亚州的希平港设计了第一座大功率压水堆（继承自鹦鹉螺号核潜艇），并于1957年首次临界，这证明了核能发电在技术上的可行性，并为人员培训和运行规则奠定了基础。这也是第一座配备安全壳系统的反应堆。

正是在这个时期，制定了最初的核安全原则。氢弹之父爱德华·泰勒（Edward Teller）曾指出，风险不在于核爆炸，

而在于裂变产物的扩散。这种认识引出了3种关键核安全功能：反应性控制、余热排出和放射性包容。纵深防御经历了几个阶段，从让·布尔乔亚（Jean Bourgeois）提出的三个层次到今天所熟知的五个层次；应用单一故障准则增加了冗余性。核安全理论逐渐变得更加丰富和复杂，扩展到支持系统、非能动设备、事故长期阶段等。

随着压水堆的建造，20世纪70年代核安全理论关注的重点主要是设计基准事故。这些事故大多数是常规性的，涵盖了一小部分可能影响核蒸汽供应系统的主要物理现象（管道破裂、控制棒弹出、阀门打开等）。研究是在保守的假设条件下进行的，其目的是表明反应堆及相关系统在受到干扰（甚至是严重干扰）时能以稳定且安全的方式做出反应，并以此确定安全系统的容量。一回路破口是一个单独的类别，需要特别研究。美国式的方法与费斯内姆（Fessenheim）核电站一同被引入了法国。后来通过对事故每一个细节进行审查，我们逐渐从“设计基准”事故转向“事件”事故。

基于屏障、纵深防御和设计基准事故的原则，工程师们设计出了稳定而坚固的压水堆，以至于50年后的今天，这些压水堆预计还能继续运行至60甚至80年。随着经验反馈、首个概率安全分析研究和三哩岛事故的发生，核安全方法很快发生了变化。

三哩岛核电站：事与愿违

1979年3月28日，宾夕法尼亚州三哩岛核电站2号反应堆蒸汽发生器的正常给水出现故障。应急给水启动，但因为两个阀门被错误关闭，应急给水没有注入蒸汽发生器。几分钟后，蒸汽发生器干涸，一回路压力升高，随后安全系统相继自动动作，包括：紧急停堆、稳压器安全阀开启、安全注入系统启动注入冷却剂。有一个稳压器安全阀未成功关闭，但操纵员对此并不理解。稳压器顶部的破口导致传感器记录的稳压器水位上升，然而操纵员没有意识到这一现象，反而停止了安全注入系统。一回路系统冷却剂排空，导致堆芯裸露（主泵的关闭加速了这一过程），然后熔化。三小时后，安全注入系统重新启动，事故结束。由于采用了安全壳系统，放射性物质的释放量降到了最低。

三哩岛事件是核安全史上的标志性事件，反应堆在几乎正常运行状态下发生堆芯熔化事故。从一个日常的小失误开始，人与机器之间没能相互理解。无论是事故情形，还是事故后果，都超出了当时的安全认知范围。事实上，用了5年时间，直到在反应堆容器中安装探头后，才意识到堆芯已经熔化（达50%）。事故造成了许多短期和长期后果，并改变了核安全方法：组织和人为因素以及心理表征问题变得至关重要。发生的事故不一定是预先设想的（因此采用了“状态导向”事故规程），而且不能排除堆芯熔化的可能性。

概率安全评价：复杂的事故序列

1975年发表的拉斯姆森报告（WASH-1400），首次使用概率安全评价（PSA）方法对核能和其他活动的风险进行了比较。在三哩岛核电站事故之后，这些研究开始普及。法国在开展了对丧失电源、丧失热阱等事故的研究，并编制了H1至H3的事故规程之后，于1990年完成了首次全面的PSA，其中法国核安全与辐射防护研究院（IRSN）对900兆瓦级机组进行了研究，而法国电力集团（EDF）则对1300兆瓦级机组进行了研究，研究结果表明应对停堆工况、复杂事故序列（也有可能是类似三哩岛核电站发生的简单事故序列）、共因故障、支持系统故障和人因失误等风险进行关注。

PSA改变了人们理解核安全的方式，并对确定论方法起到了补充作用。确定论分析方法考虑的是有限的一系列包络工况，并以保守的假设进行研究（例如，仅使用安全级设备），而PSA则以现实的建模为基础，考虑所有的始发事件、所有事故情景的影响、所有可使用的设备（为其分配故障概率）以及操纵人员的行动（成功概率）。基于全球庞大的反应堆数量和法国核工业的标准化，大量的设备可靠性数据为这些模型提供了支持。

现在，PSA已经成为核安全实践的一部分。PSA的意义不仅仅在于结果的绝对值，更在于突出事件序列的相对重要性，基于风险评价结果对重要的事件序列予以关注。PSA的分析范围不仅包括内部事件，同时也已扩展到内、外部灾害（火灾、洪水、地震），分析对象包括堆芯和其他核设施风险（例如乏燃料水池）。要合理开展事件树、故障树分析（其

指数式增长可能变得不切实际）、建立恰当的分析模型、考虑设施的实际运行特点和人因失误，以从中汲取适当的风险见解。

当人不再画地为牢

尽管从一开始就意识到人的作用（如费米和希平港的例子所示），但核安全方法主要是技术性的。20世纪70年代，开始重点关注操纵人员的资格和程序。在20世纪末，包括三哩岛核电站在内的一些工业事故使人的因素受到更大关注：20世纪80年代，人们从运行值班组的运作、人机界面和自动化（空中客车A320、N4反应堆）的角度来解决这个问题；20世纪90年代，其他灾难，如博帕尔¹、挑战者号和切尔诺贝利事故，突出了组织和安全文化。2000年以来，有关组织的工作仍在继续，延伸到质量和安全管理体系、审查和领导力概念。这种趋势在2010年代进一步发展，导致了过度监管，甚至是固执己见，使人们忽视了“黑天鹅²”事件的可能。已经发生的事故（福岛事故，AF447³）“本不应该发生”。

人的因素已经从个人（假定一个操纵员一丝不苟地执行所有计划好的程序）转变为团队，从团队转变为组织，从组织转变为社会，同时也从确定性系统转变为复杂的社会-技术

¹ 译者注：1984年12月3日，印度博帕尔市的美国联合碳化物公司下属的印度公司一所农药厂发生氰化物泄漏，造成2.5万人直接致死，55万人间接致死，是历史上最严重的工业化学事故。

² 黑天鹅理论是由Nassim Nicholas Taleb提出的，描述了具有重大影响的不可预测的罕见事件。

³ 译者注：2009年6月1日，原定由巴西里约热内卢飞往法国巴黎的法国航空447号班机，起飞后在巴西圣保罗岛屿附近坠毁，机上216名乘客及12名机组人员全数罹难。此空难为法国航空成立以来最严重的空难。

系统，该系统具有多种交互，并非所有交互都是可预测的，而且都在不断发展。人的心理弹性在事件反应中占据越来越重要的位置，人们意识到，在当前或预测条件下的最优化是以在不可预见的情境下降低适应性或人的心理弹性为代价的。

如今的选择是扩大预测范围，将可预见的情景编入目录，或者“做好无准备的准备”，即将控制能力从上游（预测）转移到实时（反应能力）。因此有两种选择：一种是“一成不变”，预先确定对所有情景的反应，加强纪律和控制；另一种是认识到不可预测性并保持人的心理弹性。对风险管理的思考会让我们倾向于第二种选择。但对安全保障需求的日益增长、全面控制的法令和法律等社会变化都倾向于前者，这将导致个人失去参与的机会。

EPR 安全目标的起源：设计中的超设计

EPR 安全目标的确定跨越了 20 世纪 90 年代初至 2000 年这一时期。在最后一批 1300 兆瓦机组投产和 N4 系列机组建造的同时，EDF 和法国政府开始考虑取代现有反应堆类型。核安全监管机构很早就参与其中，监管机构于 1991 年致函，1993 年再次致函，随后于 2000 年发布了“EPR 技术指南”。

这项工作由法国和德国共同完成，涉及行业和监管机构，并得到了各国政府的支持。由于每个国家在安全方面都有根

深蒂固的理念，因此要达成一致需要极大的意愿。例如，其中包括“破前漏”及“飞机撞击”。第一个问题是一个策略问题：我们创新反应堆设计应该是渐进式还是革新式的？选择革新型反应堆是基于这样一种信念，即通过将所获得的经验融入基于类似原则的反应堆概念中，可以在安全方面取得重大进展。十年定期安全审查、PSA 的出现、“超设计基准”的 H 程序和 U 程序的引入、三哩岛核事故和切尔诺贝利核事故的教训，以及三哩岛核电站之后约十年的严重事故研究工作等，都丰富了核安全方面的思考。

出现了三大类目标：

- 通过吸取经验教训和 PSA，将“超设计基准”因素纳入设计，并加强灾害防护，以降低堆芯熔毁的概率；

- 限制发生严重事故时的放射性后果，有两个目标：
(1) “实际消除”可能导致早期和大量释放（能量现象）的序列；
(2) 保护公众的措施必须严格限制其所涉及的时间和空间。“实际消除”是在反应堆常设咨询小组及其德国同行于 1992/1993 年举行的一次会议上确定的；

- 利用人因技术的进步，简化运行。

在致工业、研究和环境地区管理局的一封信中，核安全局用一句话概括了这些目标：“除了显著降低严重事故的后果之外，核安全目标之一是简化反应堆的运行和维护条件”。

EPR 的安全目标启发了西欧核监管者协会以及国际原子能机构的标准和“维也纳宣言”，尽管这些标准的应用仍不尽相同，特别是在严重事故方面。

福岛：自然与意外

2011 年 3 月 11 日，地震只对福岛第一核电站造成了轻微影响：外部电力供应中断，应急柴油发电机启动，1 至 3 号反应堆自动停堆，按照计划程序进行冷却。但一小时后，海啸摧毁了泵站，将 1 至 4 号反应堆的平台淹没在数米深的水下，导致大部分电气设备无法使用（柴油发电机、蓄电池、配电装置、泵、电动阀门、仪控）。3 月 11 日至 13 日期间，1 号至 3 号反应堆相继失去冷却，导致堆芯熔毁、安全壳失效以及放射性大量泄漏。

该事故证实，水淹可能是一种具有严重后果的常见模式。通过补充安全评估，对设施抵御极端自然灾害及其累积影响的能力进行了审查，引入了能够在最严重情况下保持安全功能的“硬核”措施，以完善纵深防御（如水源和应急柴油发电机），并建立了核快速反应组织，能够帮助核电厂管理此类危机。评估还确认了 EPR 的安全目标和稳健性。

几十年来，自然灾害在核安全方面的重要性与日俱增。虽然地震从一开始就是核电项目设计的核心，同时还要对洪水和爆炸进行一定程度的防护，但关于自然灾害的经验反馈

已逐渐融入核电设计中：1985 年和 1986 年的严冬（“极寒设计基准”）、1999 年布莱耶核电站洪水（加强外围防护）、植物/水母/鱼苗堵塞冷源等，都要求对自然环境提高警惕。

与三哩岛事故一样，福岛事故也提醒我们，旨在预测所有情况并提供应对措施的安全方法有其局限性。团队适应意外情况的能力是事故管理的关键因素。在人文科学的支持下，当今的安全优先事项之一就是创造条件，确保团队具备以“能够预测到”的能力来应对事故。

或许，核安全理论发展的下一步就是回归本源，让法国核安全领域的领军人物让·布尔乔亚的话成为现实：

“所有行动都必须基于这样一个简单的理念，即核电厂的安全最终取决于运营者自己如何处理核设施；因此，必须在这个层面上采取行动，如果能帮助核电厂运营者正确地完成其工作，而不是使其任务复杂化，那么这种行动就能有效提升安全水平”。

信息来源：

<https://www.sfen.org/rgn/cinquante-ans-devolution-des-doctrines-de-surete/>