全球核能安全动态

生态环境部核与辐射安全中心　　2025 年特刊

目 录

《足够安全吗？核电和事故风险简史》（一）

美国核监管委员会历史学家Thomas R. Wellock所著《足够安全吗？》回顾了概率安全分析应用于核能和美国核监管委员会风险指引型监管方式的发展和使用。该书围绕风险评估的适用性引发的激烈争论再现了当年在核电安全的拥趸和反对者之间相互博弈的真实画面。

“悲观者总是正确，乐观者总在前行”。1972年美国原子能委员会启动的反应堆安全研究中，概率论方法在支持和反对声中前行。作为其成果的拉斯姆森报告（WASH-1400）的命运也是跌宕起伏。“所有模型都不正确，但有些模型却可用”。悲观者看到了前者，乐观者看到了后者。

作为核安全监管人员，《足够安全吗？》让我们受益匪浅，因此我们决定翻译并与大家分享这本书。在接下来一段时间内，我们将连载发布本书摘编。我们相信这是在做一件有意义的事情。

故事概要

上世纪60-70年代，美国原子能委员会（AEC）试图回答一个迄今无法回答的技术问题，即核电厂发生重大事故的概率是多少？

受AEC委托，来自麻省理工学院的拉斯姆森教授率领团队历时三年，开创性地完成了编号为WASH-1400的《反应堆安全研究》报告（也称“拉斯姆森报告”）。拉斯姆森教授提出了一个适用于描述事故风险的“数值”，例如将事故后果量化为事故概率与后果的乘积，这样的表现形式既简单易懂，也具备一定说服力。

在如核电这样高度复杂的技术领域，如何才能量化一个从未发生过的事故概率？ 拉斯姆森报告给出的方案是通过“事件树”、“故障树”等分析技术来计算核电厂安全部件尽可能多的故障组合及其可能导致事故的概率，当然也包括可能导致灾害的其他内外部因素。

此项工作的繁复程度令人瞠目，且即便梳理完成不计其数的故障组合并将发生概率量化为具体数值，也无人能保证这一结果是否包络全部重要的故障路径。尽管如此，AEC还是承担了诸多风险并推动相关工作，虽然过程并非一帆风顺，但拉斯姆森报告在核安全领域里程碑式的地位，验证了AEC决策的科学性和前瞻性。

拉斯姆森报告首次提出的概率风险评估方法使得罕见灾难性事件的未知风险变得可知。尽管该报告提出的分析工具颇具价值，但事实也证明其并非完美的监管和政策

工具。核工业界内外都有人质疑其方法论、准确性和推广动机。由于核电因其保守的设计裕量、工程判断和定性工具等，具有良好的安全记录，因此一些监管者认为，概率风险评估与已经验证的安全理念存在一定偏差，从而可能导致风险。业外人士则担心，概率风险评估因其高度技术性，可能将公众排除在关键讨论之外，从而进一步强化业内人士的话语权。

上世纪70年代起，美国核监管委员会（NRC）一直在寻求AEC无法达到的监管模式，即安全、经济、透明、公众接受的“风险指引型”监管。在众多专家的努力下并通过从技术和社会科学领域汲取经验和见解，风险模型越来越强大，能够更好地用数值量化硬件、人员表现和组织文化。

进入21世纪后，随着“911”事件和日本福岛核事故的冲击，开始有人质疑NRC花费大量时间制定的风险指引型监管法规是否值得。但NRC仍然认为概率风险评估是最佳工具，能够在安全标准、监管稳定性和竞争性电力市场中的运营效率需求之间取得平衡。

可是，概率风险评估却常令人失望。工程师们期望有一个精心设计的模型，能够将核反应堆的风险提炼成直观的数字，保障安全同时缓解公众焦虑。然而现实是，这些数字经常出错，始终无法让公众确信核电是“足够安全”的。但他们始终在没有放弃。

本书通过梳理这段历史，解释了工程师们坚持使用概率风险评估的原因和取得的成就。

反应堆何时是安全的?

在原子时代最初的25年里,工程师和技术人员知道如何运行一个反应堆,但不知道重大事故的发生概率。从位于华盛顿州东部的汉福德工程厂(Hanford Engineering Works)第一个战时钚生产堆启动开始,安全保障就依赖于“3D”。3D指的是确定论(Determinism)、设计基准事故(Design Basis Accident,DBA)和纵深防御(Defense in Depth,DiD)。

第二次世界大战后,通用电气公司(GE)从杜邦公司手中接管了汉福德。由于战时生产导致的老化,反应堆状况变得非常糟糕。通用电气认为:这些设施事故的发生概率正在上升。汉福德工程师承认,“汉福德反应堆的安全系统显然无法满足”现行安全标准。然而,由于美国处于战时状态,关闭汉福德的后果不堪设想。因此,反应堆安全保障委员会(RSC)恳请通用电气寻求创新性方式,让汉福德反应堆足够安全地运行。

但是“足够安全”是多安全?理想情况下,该问题需要风险量化才能回答,即事故概率和后果的乘积。通用电气设想了若干最恶劣情景。1953年,RSC与另一咨询委员会合并,更名为反应堆安全保障咨询委员会(ACRS)。ACRS敦促通用电气研发“傻瓜式”的安全特性,从而保证失控状态“不可能”发生。通用电气考虑了很多方案,但是始终未能找到这种神奇的安全系统。

为证明汉福德足够安全，通用电气使用一种新的概率论方法，来论证能动安全系统的可靠性。1953年，汉福德统计学家提议开展首次概率风险评估，它采用自下而上的方法，通过事故链分析来计算“灾难概率”。他们认为，灾难是由一些小的故障和错误累积的最终结果。首先详细评价这一系列事件中的单个事件概率，然后组合考虑这些结果以获得期望的概率，这种方法也许可行。事故链分析成为后来风险评估的基本组成部分。这是通用电气首次涉足量化风险评估的努力，但结果“令人失望”。其主要原因在于数据不充分、对反映事故复杂性的建模能力不足等。

1957年，可靠性工程被确定为正式学科。可靠性研究重点关注部件或系统在给定时间内执行其预期功能的概率，并为更广泛的风险研究提供关键数据。20世纪50年代末，汉福德的工程师着手分析安全系统的可靠性，并制定了量化的系统可靠性目标。

通用电气认为，概率论方法能够识别最重要的安全改进并确定其优先顺序，从而提高反应堆安全性，而不需要ACRS所寻求的那种造价高却不切实际的设计变更。汉福德反应堆是用量化的可靠性指标来补充定性安全目标的一个实验舞台，这种方法使反应性事故风险维持在可接受的低阈值范围内。通用电气的概率论导向也影响了后来其民用核电厂的安全方法。通用电气所尝试的量化战略，比

依赖专家判断的定性“3D”理念更加透明。自此，量化风险评估显露出风险决策的雏形。

本期策划　对外交流合作部