

从 WASH-1400 到风险指引型监管：美国安全概率风险评估发展史

1954 年《原子能法》（Atomic Energy Act of 1954）开启了美国商业核能开发。此后相当长时间，美国核安全监管主要采用以“设计基准事故”（Design Basis Accident, DBA）为核心的确定性方法，通过保守假设、安全裕度和多重安全屏障判断核电站安全。

这套源于曼哈顿计划时期工程实践的框架在核电发展初期发挥了重要作用。但随着反应堆规模增大、安全系统日益复杂，传统方法难以一致衡量不同事故和安全措施对总体风险的贡献，对更加系统的风险评估方法的需求逐渐显现。

概率风险评估（Probabilistic Risk Assessment, PRA）正是在这一背景下得以发展。它推动美国核安全监管从主要依赖确定性准则，逐步走向风险指引型监管（Risk-Informed Regulation, RIR）。从 1975 年 WASH-1400 发布，到 1995 年美国核监管委员会（Nuclear Regulatory Commission, NRC）确立 PRA 政策，历时约二十年，其间经历了方法发展、政治争议、重大事故推动和监管理念转变。

一、前 PRA 时代：确定性方法的统治与局限（1940s—1960s）

美国早期核安全思想可追溯到曼哈顿计划。杜邦公司工程

师在汉福德反应堆设计中强调系统独立性、冗余、大的安全裕度和多重放射性屏障，这些实践后来逐步发展为“纵深防御”（Defense-in-Depth）原则。

在此基础上，美国原子能委员会（Atomic Energy Commission, AEC）形成了以 DBA 为核心的确定性监管框架，安全被定义为核电厂能够抵御一组由 AEC 专家判定的最重要不利事件的能力。

纵深防御主要体现为五项原则：设置多重能动和/或非能动工程屏障，防止单一故障导致放射性释放；设置较大的设计裕度，以应对知识不足带来的不确定性；实施设计和制造质量保证；在规定的安全限值内运行；通过持续测试、检查和维护保持原有设计裕度。

但 AEC 也认识到，纵深防御和 DBA 并不能消除所有风险。1967 年 AEC 一份工作组报告指出，如果“应急堆芯冷却系统”（Emergency Core Cooling System, ECCS）失效，失水事故（Loss of Coolant Accident, LOCA）可能威胁安全壳完整性。安全壳不再被简单视为绝不会失效的最后一道屏障。这一认识为反应堆监管发展的一个关键里程碑。

到 20 世纪 60 年代后期，随着安全系统越来越复杂，保守设计和确定性准则在不同安全措施之间可能产生不一致的保护程度，对更加系统、一致的安全评估方法的需求日益明显。

二、WASH-1400 的诞生（1972—1975）

20 世纪 60 年代，概率思想开始进入核工程安全研究。1967 年，英国学者 F.R. Farmer 发表了《反应堆安全与选址：一个风险准则的提议》提出以事故概率和后果之间的关系建立风险准则，并形成后来著名的 **Farmer 曲线（Farmer Curve）**。1969 年，《Science》发表《社会效益与技术风险》（*Social Benefit versus Technological Risk*），进一步讨论了技术风险、社会效益和风险认知。同期，航空航天工业也在发展概率安全分析方法。波音公司与贝尔实验室在“民兵”导弹项目中应用了**故障树分析（Fault Tree Analysis, FTA）**，随后又将其用于波音 747 设计。这些经验为核工业 PRA 提供了重要的方法借鉴。

20 世纪 70 年代初，随着核电厂数量和反应堆规模快速增加，公众对核安全的关注上升，ECCS 可靠性也成为争议焦点。AEC 在爱达荷开展的小尺度试验一度显示，事故中蒸汽积聚可能影响堆芯注水，引发对 ECCS 性能的进一步担忧。

在技术、政策和公众压力共同作用下，AEC 于 1972 年启动**反应堆安全研究（Reactor Safety Study, RSS）**。研究由诺曼·拉斯穆森（Norman Rasmussen）教授领导，研究团队约 40 人，来自工业界、学术界和政府机构。研究历时三年，耗资约 400 万美元，最终于 1975 年 10 月发布 **WASH-1400《反应堆安全研究》**，即著名的《拉斯穆森报告》。

研究最初尝试以故障树作为主要工具，但事实发现整座核电站的总体故障树过于复杂。于是引入了**事件树分析（Event Tree Analysis, ETA）**。事件树从某一始发事件出发，追踪后续安全系统成功或失败的不同组合路径；事件树中关键系统失效概率则通过 FTA 计算。这种“ETA+FTA”的组合，使大型复杂核电系统的风险分析在工程上成为可能。

WASH-1400 详细分析了六类 LOCA 始发事件，包括不同尺度的管道破裂、反应堆压力容器严重破裂、蒸汽发生器严重破裂，以及与反应堆冷却剂系统相连接系统的破裂。LOCA 发生后，事件树继续追踪工程安全设施的动作，包括安全壳、ECCS 以及事故冷却相关设施，以将复杂事故过程分解为一系列可估算概率的离散失效事件。

除 LOCA 外，WASH-1400 还分析了除 LOCA 外的多类反应堆瞬态，即关键运行参数明显偏离正常状态。初步分析表明，较重要的情景包括厂外电源和电厂热量排出系统丧失。

事故后果分析同样具有重要意义。研究考虑了五种公众辐射照射途径：烟羽外照射、烟羽吸入内照射、地面沉积外照射、再悬浮吸入内照射，以及地面污染后的摄入内照射。基于 1974 年美国 68 个已建或计划建设核电厂址的人口和气象数据，研究计算了早期死亡、早期疾病和长期健康效应三类后果。

研究估计，压水堆的堆芯熔化频率约为 6×10^{-5} /堆年，沸

水堆约为 3×10^{-5} /堆年。更重要的是，WASH-1400 改变了此前主要关注大破口 LOCA 的风险认知。对于压水堆，小破口 LOCA 对总体风险的贡献最高；对于沸水堆，重要风险则更多来自某些瞬态事故序列，如需停堆时未能快速停堆，以及瞬态停堆后余热排出系统失效。这表明，**后果最严重的事故，并不一定对总体风险贡献最大**。发生概率较高、单次后果相对较小的事故，也可能成为主要风险来源。

三、争议、挫折与转折（1975—1979）

WASH-1400 虽然具有开创性，但自发布起就伴随着争议。1975 年 NRC（于 1975 年建立替代 AEC 的核安全监管职能）公开草案后，外界对其中的事故后果、辐射健康效应以及 ECCS 分析等提出了质疑。随后，NRC 成立独立的风险评估审查组，由刘易斯（Harold Lewis）主持，于 1978 年发布评审报告。

一方面，审查组充分肯定了 WASH-1400 的开创性，认为它提供了当时关于核反应堆事故概率最完整的单项研究，并认为在数据充分的情况下，故障树和事件树是量化这些概率的最佳可用工具。另一方面，审查组也指出了多项问题。

首先是数据不足。许多组件失效概率的不确定性达到 10—100 倍，个别极低失效概率的误差因子甚至达到 1000。其次，WASH-1400 对不确定性的识别和传播说明不够清晰，包括模型不确定性、电厂间差异、假设引入的误差以及总体不确定性的

计算。健康效应分析也存在较大争议。当时人类辐射照射数据有限，低剂量效应、长期癌症效应和剂量率影响等问题本身尚无充分共识。

此外，审查组认为部分分析缺乏足够的可审查性，对共因失效、人因和某些外部事件的处理仍有明显局限。

审查组尤其批评了 WASH-1400 的执行摘要，认为与其说是报告摘要，不如说是一份具有明显“倡导性”（advocacy）的文件。更关键的批评针对的是报告的使用方式。审查组指出，WASH-1400 不应被直接用于判断核电风险是否“可接受”，也不应在忽视其宽泛不确定性的情况下，被视为核事故绝对风险的精确估算。

刘易斯报告发布后，NRC 撤回了对 WASH-1400 数值结果的支持，并与其执行摘要划清界限。但 NRC 并未否定 PRA 方法本身，内部仍有人推动概率方法的监管应用。然而，当时大多数监管人员熟悉的是确定性分析，对 PRA 缺乏了解和接受度，因此其推广一度陷入停滞。

1979 年 3 月，三哩岛事故（Three Mile Island Accident, TMI）发生，二号机组约一半堆芯熔化。事故并未造成大规模放射性释放，却表明严重事故并不一定由传统许可重点关注的大型 DBA 开始。TMI 印证了 WASH-1400 的一项重要认识：小破口 LOCA 对总体风险的重要性可能高于传统 DBA 重点关注

的大破口 LOCA。事故还突出显示了人因的重要作用。

TMI 之后，NRC 明显加强了对人因、人员培训、小设备故障引发严重事故、应急计划和运行经验的关注，PRA 也重新获得重视。

四、从实践到制度化：PRA 的推广与监管改革（1980s—1990s）

TMI 之后，NRC 开始实质性推动 PRA 发展。1979—1982 年间，NRC 人员启动了一系列 PRA 研究，其中两项主要计划：

“反应堆安全研究方法应用计划”负责将 WASH-1400 方法论推广至其他堆型；“临时可靠性评估计划”则致力于开发和标准化可靠性评估方法。

随着 PRA 实践增加，正式实施指南也逐渐形成。1983 年发布的《PRA 程序指南：核电厂概率风险评估实施指南》（*PRA Procedures Guide*），为核电厂开展 PRA 提供了较系统的方法指导。

20 世纪 80 年代初，NRC 还开始利用 PRA 分析传统 DBA 之外的安全问题，如预期瞬态未停堆、全厂断电、核电厂改造要求以及运行事件的风险重要性。同期，核工业自身也开展了越来越多的电厂 PRA。一些研究发现，地震和火灾等外部事件对特定核电厂的风险贡献并不像 WASH-1400 早期估计的那样可以忽略，但总体上仍验证了 WASH-1400 的许多基本风险认识。

1986 年，NRC 启动了后来形成 NUREG-1150 《美国五座核电厂严重事故风险评估》的研究。NUREG-1150 于 1990 年发布，是 WASH-1400 之后美国一次重要的大型 PRA 更新。相比 WASH-1400，NUREG-1150 拥有十余年新增的核电运行经验、更丰富的数据以及更成熟的方法和模型。其严重事故风险估算总体低于 WASH-1400，但仍落在 WASH-1400 较宽的不确定性范围内。

1988 年，NRC 发布通用函件 88-20（**Generic Letter 88-20**），要求美国核电厂开展**个体电厂检查**，明确鼓励使用 PRA 方法，识别各自核电厂特有的严重事故薄弱环节，主要包括：
①认识严重事故的行为和发展过程；②了解本厂最可能发生的严重事故序列；③提高对堆芯损伤和裂变产物释放概率的定量认识；④必要时通过修改设备和规程降低严重事故风险。通用函件还指出，PRA 可以支持许可证相关活动、许可证延续、风险管理和综合安全评价。

到 1992 年，美国已经完成 74 份 PRA，覆盖 106 座核电机组。PRA 由此从研究工具逐步进入核工业的大规模实际应用。

20 世纪 80 年代中后期，NRC 还开始建立核电安全目标，并尝试将定量风险分析纳入监管决策。1990 年，NRC 将 10^{-4} /堆年的堆芯损伤频率（**Core Damage Frequency, CDF**）称为一个“非常有用的辅助性基准”。对于演进型轻水堆设计，NRC

还认可了 0.1 的条件安全壳失效概率，由此对应约 10^{-5} /堆年的大释放频率。这些数值后来逐步发展为常用的 10^{-4} /堆年 CDF 和 10^{-5} /堆年大量早期释放频率（Large Early Release Frequency, LERF）基准。

到 1995 年，PRA 在美国核工业中的应用已经相当成熟。NRC 正式发布 PRA 政策声明，确立了“风险指引型监管”新范式，其核心是在传统的确定性分析基础上，有机地结合 PRA 结果进行监管决策。

为支撑这一新范式，NRC 于 1998 年发布了一系列管理导则，为 PRA 在各类监管活动中的具体应用提供了技术框架：RG 1.174（许可证变更）、RG 1.175（在役测试）、RG 1.176（分级技术规格书）、RG 1.177（技术规格书）和 RG 1.178（管道在役检查）。同年推出的“反应堆监督过程”建立了七大安全基石，其中始发事件、缓解系统、屏障完整性和应急准备四个基石的底层逻辑直接源自 PRA 的风险认知。该体系还引入三类“交叉性”要素：人员业绩、管理层安全关注与工人提出安全问题的能力（即“安全意识工作环境”）、以及问题发现与解决机制。

2000 年以后，NRC 继续推进 RIR，包括风险指引型许可基础变更、10 CFR 50.44 氢气控制要求、10 CFR 50.46 ECCS 验收准则、技术规格书、防火分析、PRA 标准、承压热冲击筛选准

则，以及安全壳失效、乏燃料贮存、人因可靠性和技术中立型监管等工作。

五、历史启示

从 WASH-1400 发表到 PRA 真正制度化，经历了超过十二年的漫长过程。阻碍不仅来自技术方法的待完善，更源于“监管文化与思维惯性的深层冲突”——习惯于确定性思维的工程师对概率方法存在广泛的不信任与不理解，而管理层也因研究报告早期的政治争议而犹豫不决。

最终，PRA 融入美国核安全体系，是重大事故推动、方法持续改进、运行数据积累以及熟悉概率风险方法的专业人员进入监管和决策岗位等多种因素共同作用的结果。PRA 并未取代纵深防御等传统原则，它真正带来的价值是帮助核电厂和监管机构识别安全系统中的薄弱环节，判断不同事故和系统对总体风险的相对贡献，并据此更合理地配置安全资源。

对外交流合作部 逯馨华 供稿

编译自《概率风险评估发展及其在核工业界应用的历史回顾》

文章内容不代表本公众号观点