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（二）

汉福德核反应堆设计之初所考虑的设计基准事故很简单：**假设核反应堆发生重大事故会导致放射性扩散至1.5英里外。**应对方式也很简单：**让核反应堆远离公众。**因此第一批核反应堆往往距离人口中心有数英里之远。后来的评估显示：在假设若干最坏情况下，**最严重的事故后果会造成的人员和经济损失尚可控。**因此研究重点转向核事故发生的概率。

以航空安全为例，行业内通常用“每亿乘客英里的死亡率”作为量化标准。在核电领域，若某核反应堆存在每年1%的爆炸概率，人们必然倾注大量资源以迅速降低其风险；而当反应堆的爆炸概率降至百万分之一，这一远低于洪水、地震等自然灾害的发生概率时，核事故对周边居民的潜在威胁则微乎其微。

因此，百万分之一，即 10^{-6} 就逐渐成了大家可接受的安全标准的“化身”，并很快影响到其他领域。每当需要主观判断可接受的死亡风险时，各领域专家往往会不约而同地援引 10^{-6} 左右的概率作为参考标准。

危机中的设计基准

在解决了反应堆失控问题后，设计者和监管者所关注的设计基准事故主要为冷却剂丧失事故（LOCA）。美国原子能委员会（AEC）将LOCA视为最值得关注的最大可信事故开展研究。它成为世界上几乎所有轻水堆普遍使用的设计基准事故，也成了稳固的安全壳构筑物和冷却系统的有效设计标准。

当民用核能工业在20世纪60年代早期得以推动发展之际，AEC仍然坚持“3D”理念（即确定论、设计基准事故和纵深防御）。AEC下的独立咨询机构—反应堆安全保障咨询委员会（ACRS）主张民用设计应该具有一些固有安全特性、贯彻纵深防御理念并在远离城市中心的郊区进行选址。ACRS甚至要求建设坚固的安全壳构筑物以应对最严重的LOCA问题。当时，人们对LOCA期间反应堆行为所知甚少，AEC以确定论的方式考虑了这些不确定性，并假设事故进程的每一环节都遭遇最恶劣的条件。但由于缺乏量化事故风险的能力，AEC采用定性安全方法来评估事故风险，而定性安全方法的基础是专家判断。

在那段时期，反应堆订单激增和设计的快速变化对“3D”安全理念提出了新的挑战。随着供应商设计出更大型的核电厂，新的安全问题也随之而来。这些新电厂不只是早期电厂的放大版本，有些甚至变更了核电厂设计以寻求经济优势。就这样，持续演变的设计带来了意想不到的安全问题。

1964年12月，AEC许可委员会只给Oyster Creek核电厂颁发了**有条件的建造许可**。因认为该电厂的40年设计寿期内，安全壳完整性会受到“能动系统潜在故障”的影响，功率的增加和安全设备成本的降低增加了“不确定性”，因此不宜颁发完整的建造许可。监管人员甚至无法从定性角度确定重大事故风险是否处于可接受的低阈值范围。

然而，核工业界认为Oyster Creek核电厂设计足够成熟、足够安全，因此反对AEC的许可决议，并指出AEC的安全标准一直在变。AEC认为设计不一致，而供应商认为监管不一致。订购反应堆的公用事业单位想要规模经济性，而核能供应商在相关创新设计尚无运行经验情况下，竞相将小型电厂外推扩容为大型电厂，这导致了运行经验暴露出不少问题，且运行业绩令人失望。AEC最终通过限制新反应堆订单最大输出功率的方式终止了这一局面，并指出“这些电厂功率不断增加将导致过多设计变更，AEC监管人员不得不增加审查工作，以确保安全水平不降低”。

很多人批评AEC的安全理念。设计基准事故让设计人员对危险程度无所适从，可信事故和不可信事故之间的分界线成为“纯粹主观的”判定。由于关注重大事故，设计基准事故“可能会忽视那些看起来不太严重的事故，而此类事故因发生频率高更应得到重视”。当然，发生概率极低的不可信事故也可能很重要，因为社会无法承受任何灾难性后果。而“概率论方法”彼时应运而生，究其原因是能够考虑更大范围核事故的先进性。

国际核社会也支持风险量化。加拿大反应堆有轻微的正反应性系数，因此其能动停堆系统和安全概率估算就至关重要。日本和欧洲国家因人口密度更高，导致在偏远地区选址十分困难，概率论方法因能提供更多的选址灵活性，而在欧洲得到了支持。但这些都不足以说服AEC，AEC监管人员仍然支持“3D”理念作为唯一可靠的安全策略。

WASH-740报告

1957年，AEC发布了一份关于重大反应堆事故后果研究报告，即WASH-740。该报告指出最严重事故可能导致上千人死亡和数十亿美元的财产损失（比此前的预估多一个数量级），但这样的事故发生概率“极低”。一些专家认为这种水平的概率“无法具象”。没有明确的风险数值，AEC的定性安全方法让人感觉信息混乱且缺乏逻辑，更做不到用简单的语言对其进行解释。WASH-740暴露了风险评估中最糟糕的问题—可怕的不切实际的后果，而对其发生概率又毫无概念。

1964年2月，国会议员敦促AEC更新WASH-740报告，并开展全面的风险研究工作。然而这次更新结果却比最初的研究结果更糟。原因很简单：除了反应堆更大并产生更多辐射外，研究工作的基本假设并未改变。假设的重大事故只会导致更多的假设死亡。在被要求更新WASH-740报告后，AEC分别与霍尔姆斯纳弗公司（Holmes & Narver）

和规划研究公司（Planning Research Corporation）签订了核电可靠性量化和事故概率研究的协议。

规划研究公司通过**两种方式**进行估算。一是根据运行经验来确定概率；二是采用通用电气公司此前针对汉福德的评估方法，根据部件随机故障率数据和专家判断来建立一些较为粗略的事故链。但两种方法都未能如愿。**采用第一种方式估算时**，由于反应堆运行经验仍然有限，规划研究公司只能得出在95％置信水平下重大事故概率不会高于500年一次。这一结果令人沮丧，因为根据工业界预计，到2000年将建设1000台核电机组，这就意味着一年可能发生两次重大事故。**第二种估算方式**是具有不确定性的“准量化”方法，它依赖于部件故障数据、专家判断和事故序列组合，其结果非常乐观：最好的预测仅为1亿年发生一次重大事故。最差的预测是约1000年发生一次事故。上述结论使AEC断定规划研究公司的概率估算毫无用处。

由于缺乏概率信息，AEC因更新WASH-740而再次陷入困境，于是AEC决定雪藏这些研究结果。与此同时，AEC继续资助霍尔姆斯纳弗公司开展可靠性和概率研究来分析主管道失效概率以获取更好的研究结果。至此，AEC尚未形成恰当的风险评估方法论，也没有办法从概率角度向公众解释核灾害。

故障树方法论和风险量化

发展概率论方法的部分难题在于核工程师无法对部件失效链进行可视化表达，也就无从获知灾难产生的全部

路径。1959年，英国人霍华德·雷法（Howard Raiffa）开发了决策树。1962年，贝尔实验室（Bell Labs）在美国弹道导弹计划中创建了表征布尔代数的“故障树”。不久，决策树和故障树传播到核技术的各个领域。

霍尔姆斯纳弗公司开发了故障率数据收集技术和一种故障树计算机模型，用于分析汉福德反应堆。民用核反应堆设计方（如通用电气公司和西屋公司）利用这些工具来评估水冷堆和非水冷堆设计中的反应堆安全系统，以及在LOCA期间全厂断电（SBO）的概率。一些专家开始期待通过结合自下而上的评估与自上而下的量化安全目标，从而确定安全设计标准。

1967年，英国原子能机构（Atomic Energy Authority）负责人法兰克·雷金纳德·法默（F. R. Farmer）提出，按照概率线确定反应堆的选址标准。他绘制了辐射照射与事故发生概率之间的关系曲线，把灾害心理学融入到该曲线。他认为公众更害怕单个大事故而不是众多小事故。因此，他向下弯曲了该限值曲线，使之成为“风险厌恶型”。“法默曲线”得到广泛应用。通用电气公司的伊安·沃尔（Ian Wall）把法默的工作成果集成进公司的概率论研究中，随后把该量化技术带到了AEC，并参与WASH-1400报告的相关工作。

1969年，加州大学洛杉矶分校工程系主任昌西·斯塔尔（Chauncey Starr）尝试了一个用于公共政策可接受风险的通用模型。斯塔尔的结论是，**公众很容易接受数量级**

为千分之一的自愿性风险，如开车或在家里爬梯子，**而不愿接受相同数量级的非自愿性风险**，如空气污染和核能事故。根据其计算结果，**核能已经比几乎其他任何自愿性或非自愿性风险要安全得多**。斯塔尔的工作有可能最终消除那些与定性安全相关的难以理解的用语，并用具体数值来定义《原子能法》中的“恰当保护”，且这些数值可以从日常生活风险的角度进行理解。

到20世纪60年代末，风险评估的各子项似乎汇聚成形，包括难以实现的事故概率。1967年，霍尔姆斯纳弗风险评估小组负责人约翰·加里克（John Garrick）提出了最早的复杂故障树图框之一，开展事故估算，并描述了“风险三元组”的早期概念。

这一领域的进步使得专家能够量化反应堆事故总概率和后果，从而“找到一个能用来量化安全的**品质因数**（即总风险的数值表达）”。

AEC监管人员认同风险评估取得了一些进展，但仍对其心存疑虑，因为英国和美国的模型都未能处理所有重大事故。此外，ACRS对能动安全系统的可靠性也有疑问，虽然相信应急堆芯冷却系统（ECCS）对事故预防至关重要，但同时认为ECCS“不能作为唯一可依赖的专设安全设施”。在假设最大可信事故时，应设定ECCS失效。

1965年，反应堆供应商试图开发造价相对较低的安全壳设计。通用电气公司提出了配备抑压系统的Mark-I型安全壳系统。但AEC监管人员报告称，抑压式安全壳无法承

受锆水反应和随后氢气释放产生的压力，并认为干式安全壳在这方面优于抑压式安全壳。通用电气公司则认为，其沸水堆在安全方面比竞争对手西屋公司的压水堆要好，虽然西屋公司的干式安全壳在应对显著堆芯损坏事故时更具优势，但沸水堆及其抑压式安全壳更有可能在第一时间预防堆芯熔毁，且沸水堆在紧急情况下不仅可以提供更多的可用水，还能够以更多方式将水送入堆芯。双方各执一词，其原因是当时几乎没有标准或数据能够清晰明确地判断出最佳的反应堆安全设计。

这些不确定性导致AEC内部对是否优先考虑静态安全壳产生了分歧。一些监管人员和ACRS委员认为，事故不可避免，因此“安全壳应该设计为能够抵御所有可信事故的最恶劣后果”。但是AEC部分技术人员相信质量控制可以保障反应堆安全，AEC没有必要对此进行安全研究，这些研究应由反应堆供应商来开展。ACRS则认为，质量保证不能完全消除事故发生的可能性，缓解系统和研究工作仍然至关重要。

“中国综合症”

AEC原本认为堆芯熔融不会导致反应堆压力容器泄漏。然而，1958年至1964年间的研究结果表明，燃料可能会在熔化后猛然跌落到容器底部，熔穿压力容器，最终落在安全壳底板上，然后破坏混凝土结构，直至熔穿底板。“中国综合症”就是对融熔物一路熔穿地球到达中国的夸张表达。

“中国综合症”打乱了AEC的“3D”安全方法。除非ECCS能发挥作用，否则在设计基准事故情景下安全壳损坏和裂变产物的致命性释放不可避免。通用电气公司和西屋公司提出了两种截然不同的解决方案。西屋通过增加“堆芯捕集器”来保持静态安全。通用电气则认为，安全应该依赖于ECCS而不是安全壳，在ECCS足够可靠的前提下。堆芯熔毁属不可信事故。

通用电气的上述意见引发了AEC和ACRS围绕冗余性、多样性和纵深防御三个关键安全理念的争辩。多名监管人员认为通用电气的设计具备足够的安全性，特别是其ECCS包括两列独立的冗余系统。ACRS的委员斯蒂芬·哈诺尔（Stephen Hanauer）认为，这种设计的冗余性不够，因其依赖于相同的运行原理，很容易出现共因故障，如火灾引发ECCS泵的电源被切断、同一型号阀门具有共性的制造缺陷等。而西屋公司的静态堆芯捕集器与ECCS是相互独立且多样性更优。这场辩论一直持续到1966年，无果。

为此，AEC召集各方专家成立了**特别工作组**研究ECCS问题。有人认为，堆芯捕集器可靠性待验证且建造成本太高；也有人认为工业界不愿为应对ECCS故障而改变安全壳设计。而通用电气公司致力于研究概率论方法和像ECCS这样的能动系统，并一度宣称其所设计的更可靠的ECCS可以允许降低安全壳设计的安全裕量。

通用电气公司与AEC探讨“仅仅依靠反应堆安全保障能力（而不是像安全壳这样限制后果的装置）来预防事故”

的理念，建议AEC需更加熟悉用于事故分析的“概率论方法”，并更多地依靠ECCS，而非安全壳。因为对一系列事故进行详细的概率论评估可以比AEC仅关注设计基准事故获得更多的安全裕量。

通用电气公司认为，相比于概率论方法，AEC对“未经检验的事故状况后果的关注”对安全的贡献度比较低，并呼吁使用新的故障树和概率论方法，为事故分析提供更大的现实空间。通用电气公司可以“评估各种假设事故状况的相对重要性，而概率论方法能够成功应用于对安全保障措施的评价，从而服务于这一目标。决策理论的有关技术方法可以用来确定何种行动路线将产生最优安全系统设计。这种方法也将指明安全研究项目的具体领域，最有价值的安全技术改进就应该诞生在这些领域”。总而言之，通用电气公司认为概率论方法的经济性与安全性双优。

通用电气公司随后将概率论推广至国际舞台，加拿大、英国、西德率先倡导概率论。通用电气呼吁考虑更广泛的事故，并优化核电厂安全系统，从而能够根据风险的所占比例（而不是仅仅关注几个设计基准事故）来应对相应的事故情景。这种“系统性方法”将反应堆复杂的安全特性紧紧结合起来，形成一个互为强化的整体。ECCS已经能够防止堆芯熔毁，所以不要仅依赖安全壳独自阻止堆芯熔毁，安全壳只需要强大到能够应对其他LOCA情况即可。通用电气公司对其具有三个独立能动系统的ECCS的可靠性很有信心。其通过故障树分析给出了ECCS设计可

靠性的估算概率为0.99999，也就是说在LOCA期间，ECCS只有十万分之一的失效概率，这也就意味着重大反应堆事故的发生概率远远小于百万分之一。因此，通用电气公司将大规模的堆芯熔毁视为“不可能发生的严重事故”，从而不予考虑。

基于纵深防御理念，AEC不同意降低对安全壳的要求。特别工作组发布的报告也仅倾向于支持通用电气公司对预防性系统而非安全壳的重视。该报告第一次公开承认“中国综合症”可能发生，但也认为ECCS的可靠性足以有效预防。在ECCS的运行足以预防严重堆芯熔毁的情况下，安全壳厂房只需要限制其他LOCA后果。ECCS的可接受性应该建立“在严谨和量化基础上”。该报告还建议，AEC安全研究项目重心应是ECCS性能，并减少关注低概率的堆芯熔毁。

“中国综合症”颠覆了安全研究的轨迹。反应堆供应商认为反应堆管道的延展性可以排除管道突然破裂的可能性，且ECCS设计具有充裕的能力，能够预防堆芯熔毁。随着西屋公司作为堆芯捕集器方案的提出者都放弃了进一步验证该方案有效性，通用电气公司在政治、经济和技术方面均具备说服力。后来，工业界推动AEC取消了验证堆芯熔毁的“失流试验（LOFT）”，转而启动验证ECCS有效性的LOFT试验。这时，AEC内部也有更多的人开始支持事故预防研究，而非严重事故行为。直到1979年的三哩岛事故后，人们才重拾对堆芯熔毁行为的研究信心。

在AEC将工作重心转向ECCS，并为“中国综合症”提供及时的答案的同时，也产生了一个复杂的问题：升级更新后的ECCS能如设计期待地的那样发挥作用吗？即便可以，那么一些故障、错误或外部事件而导致其失效的概率是多少呢？在寻找答案时，令人不安的ECCS研究结果和新的可信事故情景均令AEC措手不及。为了跟随行业发展步伐并安抚公众，监管人员需要在新实验、计算机事故模型以及概率风险评估方面开展前瞻性工作。

本期策划　对外交流合作部