2002年第2期

新建核电厂设计中几个重要安全问题的技术政策

国家核安全局

2002年8月

1 引言

世界核电数十年的发展历史以及中国核电近20年的开发经验表明， 核电是一种安全、清洁的能源，迄今为止核电厂运行安全记录是良好的。然而美国三哩岛核电厂事故和前苏联切尔诺贝利核电厂事故也表明，尽管核电厂发生严重事故的频度极低，由于其后果相当严重，仍然不能忽视它的风险。

目前，国际核工业界和核安全管理部门已形成共识并正在作出巨大的努力，使未来核电厂在提高经济性的同时具有更高的核安全水平。达成这一共识的基础是：

（1）近年来，核安全研究的深入、技术的发展以及核电厂运行经验的反馈，使大家进一步认识到现有核电厂在核安全方面的薄弱环节，找到了用较低成本加以改进的途径。核技术的发展使得同时提高安全性和经济性成为可能；

（2）经验表明：一个重大的核事故将对公众和潜在的核电运营者产生很大的负面影响，要使公众和电力工业界接受核电，就必须增加公众和电力工业对核安全的信心。这要求进一步降低核电厂发生事件和事故的频度；

（3）当前对核电厂风险水平的评估还有一定的不确定性，因而需要进一步提高安全水平，为核电厂安全留有更大的裕度；

（4）随着核电厂数量和核电容量的不断增加，必须进一步提高核电厂的安全水平，使其在总体上对社会的风险不再增加。

国家核安全局成立后，参考国际原子能机构所发布的一系列标准，建立了一套比较完整的核安全法规体系，使我国在核安全标准上与国际水平接轨，基本满足了前段时期中国核安全管理的需求。实践证明这套核安全法规体系是行之有效的，在新建核电厂的设计中仍需遵守。 但是由于对未来核电厂的核安全水平提出了更高要求，国际原子能机构和许多国家的核安全当局已经或正在修订核安全法规和标准，以适应这种变化。为了跟踪这个趋势，使我国的核安全要求和核安全水平与国际上保持一致，需要对现行核安全法规某些方面，例如严重事故等领域的要求进一步明确。鉴于修订法规需要一定周期，为了适应当前我国核电发展的需要，国家核安全局对可能影响新建核电厂设计的几个重要安全问题，以发布技术政策的形式表达原则立场，并准备在今后的一段时间内逐步将他们具体体现到修订的核安全法规中。必须指出，本技术政策只是现行核安全法规在某些方面的一些原则性延伸，而不是对新建核电厂安全要求的全面阐述。

2 安全目标

核安全的总目标是：通过在核电厂建立并保持对辐射危害的有效防御，保护厂区人员、公众和环境。

核安全的总目标由互相关联的下列两个具体安全目标所支持：

（1）辐射防护目标：保证厂区人员和公众在核电厂各种运行状态下所受到的辐射照射和由核电厂放

栏目纵览

综 述
核 电 设 计
工 程 管 理
工 程 建 造
运 行 维 护
核 安 全
核 电 前 期
核 电 论 坛
核 电 经 济
核 电 国 产 化
质 量 保 证
核 电 信 息

射性物质的计划排放所导致的辐射照射低于规定限值并保持合理可行尽量低；保证减轻所有事故的放射性后果。

（2）技术安全目标：采取一切合理可行的措施预防核电厂的事故，并在一旦发生事故时减轻其后果；保证在核电厂设计中所考虑的所有可能的事故，包括概率很低的事故的放射性后果很小并在规定限值之内；保证放射性后果严重的事故发生的可能性极低。

为满足上述核安全目标，在核电厂的设计中，应该完成完整的核安全分析，以评估核电厂工作人员和公众受到的辐射剂量及可能的环境后果。完整的安全分析应该包括：

--所有正常运行工况；

--预计运行事件下的核电厂状态；

--设计基准事故；

--可能导致严重事故的事件序列。

通过分析，可以确定工程设计对假设始发事件和事故的抵御能力，验证安全系统和安全相关物项或系统的有效性，制定应急响应的各项要求。

现有核电厂已经采取了许多有效控制辐射照射和减少事故发生的措施，尽管如此，发生事故的可能性依然存在，因而仍然要求采取减轻放射性后果的措施。这类措施包括专设安全设施、制订和实施各类厂内事故管理规程及必要时能够采取的厂外干预措施。核电厂的安全设计应该遵循的原则是：导致高辐射剂量或放射性物质大量释放的事件的发生频度极低，发生频度较高的事件没有或只有较小的辐射后果。

检验所确定的安全目标，特别是技术安全目标是否得到满足，可采用下述定量的概率安全目标：

--每堆年发生严重堆芯损坏事件的频率低于10-5；

--每堆年需要场外早期响应的大量放射性释放事件的频率低于10-6。

应当指出，上述概率安全目标并不能代替核安全法规的要求，　也不能作为颁发许可证的唯一依据，它仅仅是评估核电厂设计安全水平的一个指导性指标。

3 纵深防御

只要保障反应性控制、余热排出和放射性包容3个基本安全功能，核电厂的安全就有保证。纵深防御概念有助于做到这一点。

纵深防御概念应该应用于核电厂的全部活动中。据此，在核电厂设计中要求在设备和规程两方面提供多层次的保护，用以防止事故发生，或在未能防止事故发生时提供适当的防护。

从上述概念出发，在新建核电厂的设计中应明确下述的纵深防御层次：

（1）第一层次的防御是防止偏离正常运行工况与防止发生系统故障。这要求按照恰当的质量水平和工程实践，正确并保守地设计、建造和运行核电厂；

（2）第二层次的防御是及时监测到和纠正偏离正常运行工况，以防止预计运行事件升级为事故工况。这要求根据安全分析，设置专用的系统并制定运行规程，以防止或尽量减少假设始发事件所造成的损害；

（3）第三层次防御是基于以下考虑：虽然可能性很小，某些预计运行事件或始发事件的升级仍有可能未被前一层次防御所制止，可能发展为更严重的事件。这些可能性很小的事件是在核电厂设计基准中所预期的，因此必须利用固有安全特性、故障安全设计、附加的设备和规程来控制其后果，并在这些事件之后达到稳定的、可接受的状态；

（4）第四层次的防御是应付已超出设计基准的严重事故，并保证放射性后果保持在合理可行尽量低的水平。该层次最重要的目标是保持包容功能。通过附加的措施和规程防止事故发展，通过减轻所选定的严重事故的后果，加上事故处置规程可以完成这个目标；

（5）第五层次即最后层次的防御是减轻事故工况下可能的放射性物质释放后果。这要求有适当装备的应急控制中心、场区内和场区外应急响应计划。

实施纵深防御概念的一个重要内容是设置多道实体屏障，将放射性物质限制在确定的范围内。

4 严重事故

虽然现有核电厂已有高度可靠的设计来对付设计基准事故，以防止反应堆堆芯严重损坏和控制放射性物质的释放，但是应该认识到，某些极低频度的事件序列仍然可能导致堆芯的严重损坏。应该结合使用工程判断和概率论方法来考虑这些严重事故序列，确定合理可行的预防和缓解措施，并且充分注意预防措施和缓解措施之间的平衡。可接受的措施不需要使用如用于评价设计基准事故那样的保守工程实践，而可以采用现实的和最佳估算的假设、方法和分析准则。在运行经验的基础上，结合安全分析和安全研究的结果，设计中应对严重事故作如下考虑：

（1）使用概率论方法、确定论方法并结合合理的工程判断来确定可能导致严重事故的重要事件序列；

（2）对照一套准则审查这些事件序列，以确定哪些严重事故应该给予考虑；

（3）对于所选定的事件序列，应该评价设计和规程能否修改来减少其发生的可能性和减轻其后果。如果这些修改合理可行，就应该付诸实施；

（4）应考虑核电厂的全部设计能力，包括可能在超出预定的功能和预期的运行工况下使用某些系统（安全系统和非安全系统），和使用附加的临时系统，使严重事故返回到受控状态或减轻它们的后果。应证明这些系统在预期环境条件下可以起到这些作用；

（5）对于多堆厂址，可以考虑使用其他机组可用的手段和可能的支持，前提是不会危害其他机组的安全运行；

（6）对有代表性的和主导性的严重事故，应该制定相应的事故管理规程。

对于压水堆核电厂，需要考虑下述典型的严重事故预防和缓解措施：

（1）通过改进系统和设备的运行可靠性，降低发生始发事件的频率；

（2）通过对系统及其自动控制功能的合理设计，改善核电厂的瞬态特性，减少安全系统的动作和运行人员的干预；

（3）通过多重性和多样性的系统和设备，提高安全系统执行安全功能的可靠性，应特别注意减少导致共因故障的因素；

（4）应认真研究全厂断电的可能性和处理措施；

（5）应特别关注停堆状态和安全壳打开状态，特别是保证余热排出的可靠性；

（6）应采取适当的设计措施排除由于冷水或不含硼水的快速注入而导致的严重堆芯损坏；

（7）应采取设计措施排除安全壳旁路型严重事故；

（8）应采取高度可靠的手段避免高压堆芯熔融物喷射；

（9）压力容器的支撑和堆腔结构应能承受压力容器熔穿的影响，对安全壳内部构筑物应考虑局部氢爆燃等影响；

（10）在严重事故下应能维持安全壳的完整性。要考虑可燃气体的燃爆效应，必须消除威胁安全壳完整性的大体积氢爆燃，应研究可能威胁安全壳完整性的压力容器内和压力容器外的蒸汽爆炸，并采取适当的措施；

（11）应有措施冷却堆芯熔融物并减轻堆芯熔融物与安全壳底部相互作用引起的后果；

（12）在严重事故下，安全壳的贯穿件、隔离装置和空气闸门应有足够能力维持它们的功能；

（13）在严重事故下，应有长期可靠的手段排出安全壳内的热量；

（14）在严重事故下，应有足够的能力控制放射性物质的泄漏。

应注意其中的某些措施，如系统和设备的多重性和多样性，在对付设计基准事故时已有要求，但在对付严重事故时可能需要作进一步延伸的考虑。

5 概率安全分析方法的应用

概率安全分析方法是确定论方法的辅助和补充，应该在核电厂设计中得到应用。完成概率安全分析是为了：

（1）确认核电厂有一个平衡的设计，以保证某个设施或始发事件对核电厂总的风险贡献不会过大，或有显著的不确定性；

（2）确认核电厂参数小的偏离不会导致核电厂性能严重异常；

（3）提供严重堆芯损坏概率的评价和需要场外早期响应的大量放射性释放的风险评价，以确认与概率安全目标的一致性；

（4）提供外部灾害事件发生概率及其后果的评价；

（5）确认通过系统设计的改进或运行规程的修改能够降低严重事故发生频度和减轻其后果；

（6）评价核电厂应急规程的充分性。

在不同的设计阶段，和为了不同的目的，可以分步完成概率安全分析工作，如概念设计阶段可以完成简化的概率安全分析，到工程设计阶段则完成完整的概率安全分析。

6 设计管理

核电厂设计管理的目的是保证安全重要构筑物、系统和部件具有适当的性能、技术规格和材料成分，以保证它们的安全功能和核电厂安全运行。设计管理也保证能够满足营运单位的要求，并切实考虑了运行核电厂人员的能力和限制。

设计单位应保证各级人员受过适当的培训，具有合格的技术水平；在设计的各个部门之间，及与用户、供货商、建造者和合同商之间， 都建立了良好的接口；制定并严格执行了有效的程序，来审查、校核和批准所有的安全相关设计；建立了良好的安全文化。

设计单位应提供足够的设计信息， 以保证核电厂的安全运行、维护，并允许以后可能的设计修改。设计单位也应推荐将纳入核电厂管理和运行规程（如运行限值和条件等）的实践。

设计管理应在确定论方法的基础上考虑概率安全分析的结果，以保证设计是经过反复迭代、不断完善的过程，并且切实考虑了事故的预防和缓解。

设计管理应该保证充分采用了合理的设计措施，充分吸取了运行、退役的实践经验，所产生的放射性物质的活度和体积都尽可能小。

营运单位在将设计提交核安全当局审查前，应保证安全评价已经过独立于设计的人员或单位的验证。

7 经验证的工程实践

安全重要构筑物、系统和设备的设计应该遵照经批准的最新的或当前应用的标准和规范，要评价和确定标准和规范是否适用、恰当和充分，并进行必要的补充和修改，以保证它们的最终质量与所需的安全功能相适应。

如果设计采用了未被批准过的设计或设施，或者与现有工程实践有差别，则需要用适当的研究结果来证明其足够安全，在投入使用前应完成足够的试验，在运行中还要适当监测，以证明达到预期的性能。

设计中应该充分考虑已有核电厂的运行经验和相关的研究成果。

8 人机接口

在整个设计过程中应充分考虑人因问题。这不仅限于主控制室运行人员，而且包括运行、试验和维修等人员。在可能发生人机关系的各个方面都应提供改进的人机接口，以减少人员发生差错的可能性。应充分重视运行经验的反馈。

应充分应用人机工效学原理，合理设计系统及其自动控制功能，减少运行人员的负担。应为运行人员提供足够的和易于管理的信息， 使运行人员能够清楚地了解核电厂所处状态，包括严重事故状态。在需要运行人员干预前，应为运行人员留有足够的宽容时间。

9 采用计算机的控制和保护系统

若安全重要系统的功能与所采用的计算机系统的可靠性有关，则应制定开发和试验计算机硬件和软件的相应标准，并在系统的整个寿期，特别是软件开发的全过程中加以实施。整个开发过程应当有适当的质量保证大纲。采用计算机的系统的可靠性应与安全重要系统的可靠性要求相适应，应使用相互补充的开发手段（包括分析和试验）和验证手段来确认达到了所要求的可靠性。

当采用计算机的系统应用于保护系统中时，应使用最高质量和实践效果最好的硬件和软件。应使整个开发过程（包括设计修改、试验和调试）系统地形成文件和便于审查。为了确认采用计算机的系统的可靠性，应由独立于设计者和供货商的专家进行审查。