附件 1

核动力厂设计安全规定（征求意见稿）

1 引 言

1.1 目的

为实现核动力厂的安全运行、以及防止或减轻可能危及安全的事件后果，本规定提出了核动力厂安全重要的构筑物、系统和部件的设计，以及规程和组织流程所必须满足的要求。

本规定适用于核动力厂设计、制造、建造、运行和退役阶段的分析、验证和审查，技术支持以及核安全监督。

1.2 范围

1.2.1 本规定提出了进行全面安全评价的要求，以确定核动力厂在各种运行状态和事故工况下可能产生的潜在危险。安全评价过程涉及确定论安全分析和概率论安全分析这两种互为补充的技术，分析中必须考虑假设始发事件，包括可能单独地或组合地影响安全的诸多因素。这些事件有如下几种类型：

（1）源自核动力厂运行本身；

（2）由人员行为引起；

（3）直接与核动力厂及厂址环境有关。

1.2.2 本规定不涉及极不可能影响核安全的一般工业安全和由核动力厂运行引起的非放射性影响。

1.2.3 本规定中的核动力厂主要指用于发电或其他供热应用(诸如集中供热或海水淡化）而设计的，采用水冷反应堆的陆上固定式核动力厂。

1.2.4 其他类型和采用革新技术的反应堆设计可参照本规定,但应经过细致地评价和判断。

2 安全目标和纵深防御概念

2.1 安全目标

2.1.1 基本安全目标:在核动力厂中建立并保持对放射性危害的有效防御，以保护人员和环境免受放射性危害。

2.1.2 为了实现基本安全目标，必须采取以下措施:

(1) 控制运行状态下人员的辐射照射和放射性物质向环境的释放;

(2) 限制导致核动力厂反应堆堆芯、链式反应、辐射源、乏燃料、放射性废物或任何其它辐射源失控事件发生的可能性;

(3) 如果上述事件发生，缓解这些事件产生的后果。

2.1.3 基本安全目标适用于核动力厂寿期内的所有阶段，包括规划、选址、设计、制造、建造、运行和退役，以及有关的放射性物质的运输、乏燃料和放射性废物的管理。

2.2 辐射防护设计

2.2.1 为了实现基本安全目标,辐射防护设计必须保证在所有运行状态下核动力厂内的辐射照射或由于该核动力厂任何计划排放放射性物质引起的辐射照射保持低于规定限值，并且减至可合理达到的尽量

低的水平，保证减轻任何事故的放射性后果。

2.2.2 基本安全目标要求核动力厂的设计和运行使得所有辐射照射的来源都处在严格的技术和管理措施控制之下。但不排除人员受到有限的照射，也不排除法规许可数量的放射性物质从处于运行状态的核动力厂向环境的排放。此种照射和排放必须受到严格控制，必须符合运行限值和辐射防护标准，并且可合理达到的尽量低。

2.3 安全设计

2.3.1 安全设计必须：

(1) 防止由于反应堆堆芯或其他辐射源失控引起有害后果的事故，并在一旦发生事故时减轻其后果；

(2) 确保在设施设计中考虑的所有事故的放射后果都低于相关限值，并保持在可合理达到的尽量低的水平；

(3) 确保有严重放射性后果的事故发生的可能性极低，并尽最大可能减轻这种事故的放射性后果。

2.3.2 为了证明在核动力厂的设计中实现了基本安全目标,必须对设计进行全面的安全评价，以便确定所有辐射照射的来源，并评估核动力厂工作人员和公众可能受到的辐射剂量，以及对环境的可能影响。此种安全评价要考察以下内容：(1)核动力厂的正常运行；(2)预计运行事件时核动力厂的性能；(3)事故工况。在分析的基础上，确认工程设计抵御假设始发事件和事故的能力，验证安全重要物项的有效性，以及确定应急计划的输入。

2.3.3 尽管采取措施将所有运行状态下的辐射照射控制在可合理达到的尽量低的水平，并将能导致辐射源失控事故的可能性减至最小，

但仍然存在发生事故的可能性。这就需要采取措施以保证减轻放射性后果。这些措施包括：安全设施和安全系统，营运单位制定的厂内事故管理规程，以及国家和地方有关部门制定的场外干预措施。

2.3.4 核动力厂的安全设计必须采取实际措施，以减轻核与辐射事故对人员的生命、健康以及环境造成的影响。必须“实际消除”可能导致高辐射剂量或大量放射性释放的核动力厂事件序列；必须保证发生概率高的核动力厂事件序列没有或仅有微小的潜在放射性后果。安全设计的基本目标是在技术上实现减轻放射性后果的场外防护行动是有限的甚至是可以取消的。

2.4 纵深防御概念

2.4.1 防止核动力厂发生事故和减轻事故后果的主要手段是应用纵深防御概念。该概念贯彻于安全有关的全部活动，涉及组织、人员行为、设计，以及核动力厂功率工况、低功率及各种停堆状态，以保证这些活动均置于各种独立的、不同层次措施的防御之下，即使有一种故障发生，它将由适当的措施探测、补偿或纠正。在整个设计和运行中贯彻纵深防御，以防止厂内设备故障或人因引起的各种预计运行事件和事故，并对由厂外事件引起的后果进行防护。

2.4.2 纵深防御概念的应用主要是通过一系列连续和独立的防御层次的结合，以防止事故对人员和环境造成危害。如果某一保护层次或屏障失效，则由后续层次或屏障提供保护。每一不同层次防御的独立有效性都是纵深防御的必要的组成部分。共有五个层次的防御：

（1）第一层次防御的目的是防止偏离正常运行及防止安全重要物项失效。这一层次要求：按照恰当的质量水平和经验证的工程实践，

正确并保守地选址、设计、建造、维修和运行核动力厂。为此，应十分注意选择恰当的设计规范和材料，对部件的制造、核动力厂的建造和调试进行质量控制。有利于减少内部灾害的可能的设计措施在这一层次的防御中起作用。还应重视有关活动的过程和规程，这些活动包括设计、制造、建造、核动力厂的运行方式和运行经验利用等方面，以及在役检查、维修和试验，包括实施这些活动时的良好可达性。整个过程是以确定核动力厂运行和维修要求及其质量管理要求的详细分析为基础。

（2）第二层次防御的目的是检测和控制偏离正常运行状态，以防止预计运行事件升级为事故工况。尽管注意预防，核动力厂在其寿期内仍然可能发生某些假设始发事件。这一层次要求在设计中设置特定的系统和设施，通过安全分析确认其有效性，并制定运行规程以防止这些始发事件的发生，或尽量减小其造成的后果，使核动力厂回到安全状态。

（3）设置第三层次防御是基于以下假定：尽管极不可能，某些预计运行事件或假设始发事件的升级仍有可能未被前一层次防御所制止，而演变成事故。在核动力厂的设计中，假定这些事故会发生。这就要求必须通过固有安全特性和（或）专设安全设施、安全系统和规程，防止造成反应堆堆芯损伤或需要采取场外行动的放射性释放，并能使核动力厂回到安全状态。

（4）第四层次防御的目的是减轻第三层次纵深防御失效所导致的事故后果。通过控制事故进展和减轻严重事故的后果来实现第四层次的防御。目标是“实际消除”导致早期或大量放射性释放的事故序列，严重事故下防护措施在区域和时间上是有限的，场外污染可避免或最

小化。

（5）第五层次，即最后层次防御的目的是减轻可能由事故工况引起潜在的放射性物质释放造成的放射性后果。这方面要求有配备恰当的应急响应设施以及制定用于场内、场外应急响应的应急计划和应急规程。

2.4.3 纵深防御概念应用的另一方面是在设计中设置一系列的实体屏障，并采用能动、非能动设施和固有安全特性的组合，以使实体屏障能够有效地将放射性物质包容在特定区域。所必需的实体屏障的数目取决于放射性核素的总量和同位素成份表征的初始源项、单个屏障的有效性、可能的内部与外部灾害以及各种失效的潜在后果。

3 设计安全管理

3.1 设计安全管理职责

营运单位必须保证提交国家核安全监管部门的设计符合所有适用的安全要求。所有从事与核动力厂安全设计重要活动相关的组织，包括设计单位，都有责任保证将安全事务放在最优先的位置。

3.2 质量保证

3.2.1 必须制定和实施描述核动力厂设计的管理、执行和评价的总体安排的质量保证大纲。该大纲包括确保核动力厂每个构筑物、系统和部件以及总体设计的设计质量的措施,包括确定和纠正设计缺陷、检验设计的恰当性和控制设计变更的措施。

3.2.2 设计，包括变更、修改或安全改进，必须按照合适的工程规范和标准所确定的程序进行，并必须体现适用的要求和设计基准。必

须确定和控制设计接口。

3.2.3 设计（包括设计手段和设计输入与输出）的恰当与否，必须由原先从事此工作的人员以外的个人或团体进行核实和验证。在设计和建造过程中应尽早完成核实、验证和批准,最迟不晚于核动力厂首次装料。

3.3 全寿期内核动力厂设计的完整性

营运单位对安全负全面责任。营运单位应尽早设立全面负责设计过程的部门，并制定管理流程，以在从运行至退役阶段的全寿期内保持核动力厂设计的完整性。

4 主要技术要求

4.1 基本安全功能

4.1.1 必须保证在各种核动力厂状态下实现以下基本安全功能：

（1）控制反应性；

（2）排出堆芯余热和所贮存燃料的热量；

（3）包容放射性物质、屏蔽辐射、控制计划的放射性排放，以及限制事故的放射性释放。

4.1.2 必须用全面的、系统的方法来确定完成基本安全功能所必需的安全重要物项，以及在各种核动力厂状态下用于实现或影响基本安全功能的固有特性。

4.1.3 必须提供对核动力厂状态进行监测的手段，以确保实现所要求的安全功能。

4.2 辐射防护

4.2.1 设计必须保证工作人员和公众受到的辐射剂量，在寿期内运行状态下不超过剂量限值且在事故工况下不超过可接受限值，并可合理达到的尽量低。

4.2.2 设计必须“实际消除”可能导致高辐射剂量或大量放射性释放的核动力厂状态，并必须保证发生概率高的核动力厂状态没有或仅有微小的潜在放射性后果。

4.2.3 基于辐射防护目的，必须建立与各类核动力厂状态相对应且符合监管要求的可接受限值。

4.3 设计管理

4.3.1 设计必须保证核动力厂及其安全重要物项具有合适的性能，以保证其能可靠地执行安全功能；在设计寿期内核动力厂能够在运行限值和条件范围内安全运行，并能够安全退役；对环境的影响最小。

4.3.2 设计必须保证满足营运单位的安全要求，满足国家核安全监管部门和相关法律法规的要求，并适当考虑营运单位人员的能力与局限性以及可能影响人员行为的各种因素。必须提供充分的设计资料，保证核动力厂的安全运行和维修，并允许以后能对核动力厂进行修改。同时推荐可纳入核动力厂的管理规程和运行规程的实践。

4.3.3 设计必须充分考虑其他核动力厂在设计、建造和运行中获得的相关经验和相关研究的成果。

4.3.4 设计必须充分考虑确定论安全分析和概率论安全分析的结果，确保已经充分考虑了事故的预防和事故后果的缓解。

4.3.5 设计必须保证采用合适的设计措施以及运行和退役实践，使产生和排放的放射性废物活度和体积达到实际可行的最低水平。

4.4 纵深防御的应用

4.4.1 设计必须体现纵深防御。纵深防御的各个层次之间必须尽实际可能地相互独立，避免一个层次的失效降低其他层次的有效性。

4.4.2 必须应用纵深防御概念，提供多层次防御，预防可能对人类和环境产生有害影响的事故后果，并保证在防护失效时，采取适当措施保护人类和环境，减轻事故后果。

4.4.3 设计必须考虑到这样的事实：当缺少某一层次防御时，多层次防御的存在并不能作为继续运行的基础。纵深防御的各层次必须总是可用的，对任何特定运行模式下的放松，都必须进行论证。

4.4.4 设计：

(1)必须在放射性物质和环境之间设置多道实体屏障；

(2)必须采用保守的设计和高质量的建造，以保证核动力厂的故障和偏离正常运行减至最少；保证尽实际可能地预防事故；保证核动力厂不存在陡边效应；

(3) 必须利用固有特性和工程设施控制核动力厂的行为，尽可能减少或排除那些需要启动安全系统的故障和偏离正常运行；

(4) 必须对核动力厂提供附加控制，这些附加控制采用安全系统的自动触发，以便能够高置信度地控制那些超出控制系统能力的故障和偏离正常运行，并且使得早期阶段对操纵员动作的需求减至最少；

(5) 必须提供构筑物、系统、部件和规程，以控制失效和偏离正常运行的进程，尽实际可能地限制其后果，并防止其超出安全系统的能力；

(6) 必须提供多种手段来保证实现每项基本安全功能，从而保证

各道屏障的有效性和减轻任何失效和偏离正常运行的后果。

4.4.5 为了贯彻纵深防御概念，设计必须尽实际可能地防止：

(1) 出现影响实体屏障完整性的情况；

(2) 一道或多道屏障失效；

(3) 一道屏障因另一道屏障的失效而失效；

(4) 运行和维修差错产生有害后果的可能性。

4.4.6 在核动力厂运行寿期内，设计必须尽实际可能地使第一层次至多第二层次能够阻止可能发生的所有故障或偏离正常运行升级为事故工况。

4.4.7 用于设计扩展工况的安全设施（例如对于缓解燃料熔化事故后果的设施）应尽实际可能地与安全系统独立。

4.5 安全与安保之间的接口

必须以统筹兼顾的方式设计和实施核动力厂的安全措施、核安保措施及国家核材料衡算和控制体系，以免其相互制约。

4.6 经验证的工程实践

4.6.1 用作安全重要物项设计准则的规范和标准必须加以鉴别和评价，以确定其适用性、恰当性和充分性，并根据需要进行补充或修改，以保证设计质量与所需的安全功能相适应。

4.6.2 核动力厂的安全重要物项必须是此前在相当使用条件下验证过的，否则该物项必须具有高质量且其技术经过鉴定或试验。

4.6.3 当引入未经验证的设计或设施，或存在着偏离已有的工程实践时，必须借助适当的支持性研究计划、特定验收准则的性能试验，或通过其他相关的应用中获得的运行经验的检验，来证明其安全性是

合适的。新的设计、新的设施或新的实践必须在投入使用前经过充分的试验，并在使用中进行监测，以便验证是否达到了预期效果。

4.7 安全评价

4.7.1 必须在核动力厂的整个设计过程中进行全面的确定论安全评价和概率论安全评价，以保证在核动力厂寿期内的各个阶段满足全部设计安全要求，并确认交付使用的设计满足制造、建造、竣工、运行和改造的要求。

4.7.2 设计过程中必须尽早开展安全评价。随着设计和确认性分析活动之间的不断迭代，安全评价的范围和详细程度随着设计计划的进展不断地扩大和提高。

4.7.3 应该将安全评价形成文件以便于独立评估。

4.8 建造规定

4.8.1 核动力厂安全重要物项的设计必须使其能够按照所确立的流程进行制造、建造、装配和安装，这些流程确保满足设计规范和所要求的安全水平。

4.8.2 在建造和运行规定中，必须适当考虑其他类似核动力厂及其相关构筑物、系统和部件建造中获得的相关经验。如果采用其他相关工业的良好实践，则必须表明其适用于核动力厂。

4.9 便于放射性废物管理和退役的特性

4.9.1 在设计阶段，必须专门考虑便于核动力厂放射性废物管理以及未来核动力厂退役和拆除的特性。

4.9.2 在设计中必须考虑：

(1) 材料的选取，以使放射性废物量尽实际可能地少，并便于去

污；

(2) 必要的可达性和可操作性；

(3) 管理（例如，分离（分拣）、表征、分类、预处理、处理和整备）和贮存核动力厂运行过程中产生的放射性废物所需的设施，以及管理核动力厂退役所产生的放射性废物的措施。

5 核动力厂总体设计

5.1 总的设计基准

5.1.1 核动力厂状态分类

5.1.1.1 必须识别核动力厂状态,并且主要按发生频率将核动力厂状态分成有限的几类。

5.1.1.2 典型的核动力厂状态包括：

(1) 正常运行；

(2) 预计运行事件，即在核动力厂运行寿期内预计会发生的事件；

(3) 设计基准事故；

(4) 设计扩展工况，包括堆芯熔化事故。

5.1.1.3. 必须为每类核动力厂状态确定准则，使得发生频率高的核动力厂状态必须没有或仅有微小的放射性后果，而可能导致严重后果的核动力厂状态的发生频率必须非常低。

5.1.2 安全重要物项的设计基准

5.1.2.1 安全重要物项的设计基准必须针对有关的运行状态、事故工况以及由内部和外部灾害导致的工况，规定必需的能力、可靠性和功能，以在核动力厂整个寿期内满足特定的验收准则。

5.1.2.2 必须系统地论证安全重要物项设计基准的合理性并形成文件。这些文件必须为营运单位安全运行核动力厂提供必要的信息。

5.1.3 设计限值

针对运行状态和事故工况，必须为安全重要物项规定一套相应的设计限值。设计限值必须符合核安全法规和相关的监管要求。

5.1.4 假设始发事件

5.1.4.1 在核动力厂的设计中必须使用系统化的方法识别一套全面的假设始发事件，以在设计中考虑所有可预见的有严重后果的事件和发生频率高的事件。

5.1.4.2 必须在工程判断、确定论和概率论评价相结合的基础上确定假设始发事件。必须论证确定论安全分析和概率论安全分析的应用范围，来表明已考虑所有预期的事件。

5.1.4.3 假设始发事件必须包括功率工况、低功率及停堆工况下，所有可预见的核动力厂构筑物、系统和部件失效，以及误操作和内、外部灾害可能引起的失效。

5.1.4.4 必须对核动力厂的假设始发事件进行分析，以确定执行所要求的安全功能所必需的预防和缓解措施。

5.1.4.5 核动力厂对任何假设始发事件的预期响应，必须是下列可合理达到的情况（以优先排序）：

（1）依靠核动力厂的固有特性，使假设始发事件不会产生安全重要的影响，或只使核动力厂产生趋向于安全状态的变化；

（2）发生假设始发事件后，核动力厂可借助非能动安全设施或在此状态下连续运行的系统的作用，以控制该事件，使核动力厂趋于安

全；

（3）发生假设始发事件后，借助为了响应该事件而必需投入运行的那些安全系统的作用使核动力厂趋于安全；

（4）发生假设始发事件后，借助专门规程使核动力厂趋于安全或使核动力厂状态得到控制。

5.1.4.6 在核动力厂总体安全评价和详细分析中，用于确定安全重要物项性能要求的假设始发事件，必须划分成若干具有代表性的事件序列。这些具有代表性的事件序列包络同类事件，并为安全重要物项的设计和运行限值提供基准。

5.1.4.7 如果要在设计中将某一识别出的假设始发事件从假设始发事件清单中排除，则必须提供技术论证。

5.1.4.8 对于需要立即采取可靠响应行动的假设始发事件，设计中必须有自动安全动作来启动所需的安全系统，以防止发展为更严重的工况。

5.1.4.9 对于不需要立即采取响应行动的假设始发事件，可允许手动启动系统或操纵员的其他动作。条件是必须有足够的时间来探测到异常状况并采取行动，以及有适当的规程（如管理规程、运行规程和应急规程），以保证这些行动的执行。必须对因操纵员误操作或误诊断而导致事件序列恶化的可能性作出评价。

5.1.4.10 如果假设始发事件后需要操纵员的行动来诊断核动力厂的状态并使核动力厂及时进入长期稳定停堆工况，则必须设置适当的仪表以有利于监测核动力厂的状态，并恰当地控制设备的手动操作。

5.1.4.11 设计中必须确定必要的设备及所需的规程，以保持对核

动力厂的控制并缓解丧失控制的后果。

5.1.4.12 手动响应和恢复过程所需的任何设备必须放置在最合适的位置，以保证需要时可用和在预期环境条件下允许人员安全可达。

5.1.5 内部和外部灾害

5.1.5.1 必须识别所有可预见的内部和外部灾害，包括潜在的可能直接或间接影响核动力厂安全的人为事件，并评价其影响。在核动力厂布置设计、确定有关的安全重要物项设计中使用的假设始发事件及其产生的荷载时，都必须考虑灾害影响。

5.1.5.2 安全重要物项的设计和布置，必须按照其安全重要性，抵御灾害的影响，或防护灾害及其产生的共因失效机理，同时适当考虑对安全的其他影响。

5.1.5.3 对多机组厂址，设计必须充分考虑特定灾害同时影响厂址上若干或甚至所有机组的可能性。

5.1.5.4 设计必须适当考虑内部灾害，比如火灾、爆炸、水淹、飞射物、结构坍塌和重物坠落、管道甩击、喷射流冲击以及破损系统或现场其他设施中的流体释放。必须提供适当的预防和缓解措施，以保证安全不受到损害。

5.1.5.5 设计必须充分考虑在厂址评价过程中识别的自然和人为外部事件（即源于厂外的事件）。假定可能的灾害时必须考虑其发生的原因和可能性。在短期内，不允许核动力厂的安全依赖诸如电力供应和消防服务之类厂外服务的可用性。设计必须适当考虑厂址的特定情况以确定厂外服务就位需要的最大延迟时间。

5.1.5.6 必须提供措施，使包含有安全重要物项（包括动力电缆

和控制电缆）的厂房与核动力厂其他构筑物之间由于设计中考虑的外部事件产生的相互影响最小化。

5.1.5.7 由厂址灾害评价确定核动力厂设计必须提供适当的裕量，以保护抵御设计中考虑的外部灾害（由厂址灾害评价确定）的安全重要物项和避免产生陡边效应。

5.1.5.8 核动力厂设计还必须提供适当的裕量，以在超过设计中考虑的自然灾害事件（由厂址灾害评价确定）时，保护防止早期或大量放射性释放所必需的物项。

5.1.6 设计规范

5.1.6.1 必须规定核动力厂安全重要物项的设计规范，并且必须使其符合核安全法规和相关的监管要求及经验证的工程实践，同时适当考虑其与核动力技术的相关性。

5.1.6.2 核动力厂设计必须采用确保稳健性设计的方法，必须遵循经验证的工程实践，以保证在所有运行状态和事故工况下执行基本安全功能。

5.1.7 设计基准事故

5.1.7.1 必须根据假设始发事件清单得出一套设计基准事故，以便设定设计核动力厂需承受的边界条件，保证满足辐射防护限值。

5.1.7.2 必须利用设计基准事故来确定事故中所需的安全系统及其他安全重要物项的设计基准，包括性能准则等，目的是使核动力厂恢复到安全状态及减轻事故后果。

5.1.7.3 对设计基准事故而言，必须做到核动力厂关键参数不超出规定的设计限值。设计的基本目标是使所有的设计基准事故在厂内

或厂外均不产生或仅产生较小的放射性后果，并且不必启动任何厂外防护行动。

5.1.7.4 必须以保守的方法分析设计基准事故。该方法包括在分析中在对安全系统假定某些故障模式，规定设计准则，采用保守的假设、分析模型和输入参数输入等。

5.1.8 设计扩展工况

5.1.8.1 必须在工程判断、确定论和概率论评价的基础上推导出一套设计扩展工况，通过加强核动力厂在应对比设计基准事故更严重的事故或包含涉及多重故障时的事故的承受能力，避免不可接受的放射性后果，以进一步提高改进核动力厂的安全性。在设计中必须考虑这些设计扩展工况来确定额外的事故情景，并针对这类事故制定切实可行的预防和缓解措施。

5.1.8.2 必须对核动力厂开展设计扩展工况分析。考虑设计扩展工况的主要技术目标是防止发生超过设计基准事故的事故工况，或合理可行地减轻这类事故工况的后果。这可能会要求针对设计扩展工况增加额外的安全设施，或扩展安全系统的能力，来预防发生严重事故或减轻严重事故的后果，或保持安全壳的完整性。这些针对设计扩展工况而增加的额外的安全设施或能力扩展的安全系统，必须保证具有在安全壳内存在大量放射性物质（包括来自堆芯严重损伤所释放的放射性物质）的条件下管理事故工况的能力。必须保证核动力厂能进入可控状态，并维持放射性物质包容功能，从而能“实际消除”导致早期放射性释放或大量放射性释放的核动力厂状态发生的可能性。相关的分析可采用最佳估算方法。

5.1.8.3 必须使用设计扩展工况来确定安全设施，以及用于预防该类工况的发生或在该类工况发生后用于控制和减轻其后果的其他安全重要物项的设计规格书。

5.1.8.4 所开展的分析必须包括确定用于能够预防和缓解设计扩展工况的设施。这些设施需满足如下要求：

(1) 必须尽实际可能与发生频率更高的事故中使用的设施保持独立；

(2) 必须能在设计扩展工况对应的环境条件中执行预期功能；

(3) 必须有与要求其实现的功能相符的可靠性。

5.1.8.5 安全壳及其安全设施必须能够承受包括堆芯熔化在内的极端事故情景。必须采用工程判断和概率安全评价结果来选择这些事故情景。

5.1.8.6 设计必须做到“实际消除”可能导致早期放射性释放或大量放射性释放的核动力厂工况发生的可能性。

5.1.8.7 对于设计扩展工况，所采取的保护公众的防护行动在持续时间和范围上必须是有限的，且必须有足够的时间采取这些防护行动。

5.1.9 事件和故障的组合

如果由工程判断、确定论安全分析和概率论安全分析的结果表明事件组合将可能导致预计运行事件或事故工况，则必须主要根据其发生的可能性，将这些事件组合纳入设计基准事故或设计扩展工况。某些事件可能是其他事件的后果，例如地震后的水淹。这种继发效应视为原假设始发事件的一部分。

5.1.10 商用大型飞机的恶意撞击

5.1.10.1 如果核动力厂所处的地形条件使其有可能遭受大型商用飞机的恶意撞击，则设计上应该考虑这种撞击的影响。

5.1.10.2 应合理选定用于评价撞击影响的商用大型飞机的机型，并根据这种机型起降的机场和核动力厂的相对距离确定可能的飞机燃料装载量。

5.1.10.3 可根据核动力厂所处的地形条件确定可能的撞击角度和速度，并采用现实模型来评价和确定核动力厂抗大型商用飞机撞击的措施。

5.1.10.4 评价结果应该表明反应堆堆芯的冷却或安全壳的完整性可以维持，以及乏燃料的冷却或乏燃料水池的完整性可以维持。

5.2 安全系统的独立性

5.2.1 必须通过实体隔离、电气隔离、功能独立和通讯（数据传输）独立等适当手段防止安全系统之间或一个系统的冗余组成部分之间发生相互干扰。

5.2.2 在核动力厂中必须易于识别安全系统中相互冗余的设备（包括电缆和电缆管道）。

5.3 安全分级

5.3.1 必须识别所有安全重要物项，并根据其功能和安全重要性对其进行分级。

5.3.2 划分安全重要物项的安全重要性必须主要基于确定论方法，适当时辅以概率论方法和工程判断。必须充分考虑以下因素：

(1) 该物项要执行的安全功能；

(2) 未能执行其安全功能的后果；

(3) 需要该物项执行某一安全功能的可能性；

(4) 假设始发事件后，需要该物项投入运行的时刻或持续运行时间。

5.3.3 必须在不同级别的物项之间提供合适的接口设计，以保证划分为较低级别的物项中的任何故障不会蔓延到划分为较高级别的物项。

5.3.4 对执行多个功能的设备，必须按照其执行的最重要功能划分其安全等级。

5.4 安全重要物项的可靠性

5.4.1 安全重要物项的可靠性必须与其安全重要性相适应。

5.4.2 安全重要物项的设计必须确保：设备可鉴定、采购、安装、调试、操作及维修，使其能够承受该物项设计基准中规定的所有工况，并具有足够的可靠性和有效性。

5.4.3 选择设备时必须考虑到误动作与不安全的故障模式。必须优先选择具有可预见的和已揭示的故障模式的设备，且该设备便于修理或更换。

5.4.4 共因故障

必须充分考虑安全重要物项发生共因故障的可能性，以确定应该如何应用多样性、多重性、独立性原则来实现所需的可靠性。

5.4.5 单一故障准则

5.4.5.1 必须对核动力厂设计中所包括的每个安全组合都应用单一故障准则。

5.4.5.2 当把单一故障准则应用于一个安全组合或安全系统时，必须将误动作视为故障的一种模式。

5.4.5.3 在设计中，必须适当考虑非能动部件的故障，除非能够在具有高置信度的单一故障分析中证实：该部件的故障极不可能发生，并且其功能保持不受到假设始发事件的影响。

5.4.6 故障安全设计

必须恰当地考虑故障安全设计原则，并贯彻到核动力厂安全重要系统和部件的设计中。在适用时，应将安全重要系统和部件设计为故障安全，使其自身的故障或支持设施的故障不妨碍预定安全功能的执行。

5.4.7 支持系统和辅助系统

5.4.7.1 支持系统和辅助系统用于保证构成安全重要系统部分的设备可运行性时，必须相应地分级。

5.4.7.2 支持系统和辅助系统的可靠性、多重性、多样性和独立性，以及用于其隔离和功能试验的措施，必须与其所支持的系统的安全重要性相适应。

5.4.7.3 不允许支持系统和辅助系统的某一失效能够同时影响某一安全系统或某一执行多样化安全功能系统的多重部件，并损害这些系统执行其安全功能的能力。

5.4.8 安全运行的运行限值和条件

5.4.8.1 设计必须为核动力厂安全运行确定一套运行限值和条件。

5.4.8.2 核动力厂设计中确定的要求及运行限值和条件必须包括：

(1) 安全限值；

(2) 安全系统整定值；

(3)正常运行限值和条件；

(4) 工艺变量和其他重要参数的控制系统限制和规程限制；

(5) 对核动力厂的监督、维修、试验和检查的要求，以保证各构筑物、系统和部件执行设计中预定的功能，并使辐射风险保持在可合理达到的尽量低；

(6) 规定的运行配置，包括在安全系统或安全相关系统不可用时的运行限值；

(7) 行动说明，包括在响应偏离运行限值和条件时所采取行动的完成时间。

5.5 核动力厂全寿期内的安全运行设计

5.5.1 安全重要物项的标定、试验、维护、修理、更换、检查和监测

5.5.1.1 核动力厂设计中应确保安全重要物项能够进行标定、试验、维护、修理或更换、检查和监测，必须确保其执行功能的能力及保持在其设计基准中规定的所有条件下的完备性。

5.5.1.2 核动力厂布置必须便于进行标定、试验、维护、修理或更换、检查和监测等活动，并能按照与所执行的安全功能的重要性一致的规范和标准进行，且工作人员不致于受到过量的照射。

5.5.1.3 在功率运行期间，设计必须使安全重要物项在进行标定、试验或维护时各系统安全功能的可靠性没有显著降低。在设计中必须考虑有关在停堆期间进行安全重要物项标定、试验、维护、修理、更换或检查的措施，以便于在开展这些活动时相关物项所执行的安全功

能的可靠性没有显著降低。

5.5.1.4 如果某项安全重要物项的设计不能满足试验、检查或监测的要求时，必须采取下列方法以说明其正当性：

(1) 其他经过验证的替代方法和（或）间接方法，如监视参考物项的试验或使用经过验证和确认的计算方法；

(2) 采用保守的安全裕度或其他适当的预防措施，以消除可能预计不到的故障。

5.5.2 安全重要物项的鉴定

5.5.2.1 必须采用安全重要物项的鉴定程序来确认核动力厂安全重要物项能够在其整个设计寿期内以及支配性环境条件下执行其必要的预期功能，这里考虑的环境条件包括核动力厂的维修和试验。

5.5.2.2 在核动力厂安全重要物项的鉴定程序中所考虑的环境条件必须包括核动力厂设计基准中所预期的周围环境条件的变化。

5.5.2.3 安全重要物项鉴定程序必须考虑到安全重要物项预期寿期内由各种环境因素（如振动、辐照、湿度或温度）引起的老化效应。对于遭受到外部自然事件的影响并且需要在这种事件中及事件后执行其安全功能的设备，鉴定程序必须尽可能地通过试验、分析或者两者的结合复现外部自然事件对安全重要物项施加的影响。

5.5.2.4 在鉴定程序中必须考虑可合理预计的环境条件,以及可能由特定运行工况（如安全壳泄漏率定期试验）引起的异常环境条件。

5.5.2.5 在可能的范围内,应该以合理的可信度表明在严重事故中必须运行的设备（如某些仪表）能够达到设计要求。

5.5.3 老化管理

5.5.3.1 必须确定核动力厂安全重要物项的设计寿命。在设计中必须提供适当的裕度，以便考虑有关老化、中子辐照脆化和磨损机理，以及与服役年限有关的潜在的性能劣化，从而确保安全重要物项在其整个寿命期间执行所必须的安全功能的能力。

5.5.3.2 必须考虑到在所有正常运行工况、试验、维修、维修停役、以及在假设始发事件中及其后的核动力厂状态下的老化和磨损效应。

5.5.3.3 必须采取监测、试验、取样和检查措施，以便评价设计阶段预计的老化机理，以及识别在使用中可能发生的未预计到的现象或性能劣化。

5.6 人因

5.6.1 优化运行人员效能的设计

5.6.1.1 必须在核动力厂设计过程初期就对人因（包括人-机接口）进行系统性考虑，并贯彻于设计全过程。

5.6.1.2 核动力厂的设计必须规定运行人员的最低配置，以满足实施使核动力厂进入安全状态所需全部同步操作的要求。

5.6.1.3 应尽实际可能地让已从类似核动力厂获得了运行经验的运行人员积极参与设计过程，以确保在设计过程中尽早考虑未来的运行和设备维护的需求。

5.6.1.4 设计必须支持运行人员履行职责和执行任务，而且必须限制操作失误的可能性及其对安全造成的影响。设计过程必须适当考虑核动力厂布置和设备布置以及包括维修程序和检查程序在内的有关程序，以便于在核动力厂各种状态下运行人员和核动力厂之间的互动。

5.6.1.5 人机接口的设计必须能按照决策所需时间和行动所需时

间给操纵员提供全面且易于管理的信息。操纵员做决策和行动所需的信息必须简洁明了、无歧义。

5.6.1.6 必须向操纵员提供能够进行下列工作的必要信息：

(1) 评估核动力厂在任何工况下的总体状态；

(2) 在系统和设备规定的参数限值（运行限值和条件）内运行核动力厂；

(3)确认启动安全系统所需的安全动作能够在需要时自动触发，且相关系统能够执行预期功能；

(4) 确定手动启动特定安全动作的必要性和时间。

5.6.1.7 在适当考虑可用时间、预期工况和操纵员心理压力的情况下，设计必须有利于操纵员动作的成功执行。

5.6.1.8 必须把对操纵员在短时间内进行干预的需求降至最低，且必须证明操纵员有足够的时间做出决策和采取行动。

5.6.1.9 设计必须能够确保当某一影响核动力厂的事件发生后，控制室或辅助控制室以及通往辅助控制室的通道的环境条件不会损害运行人员的防护和安全。

5.6.1.10 运行人员的工作场所和工作环境的设计必须符合工效学概念。

5.6.1.11 在适当阶段必须对人因有关的特性进行验证和确认（包括使用模拟机），以确认操纵员所要采取的必要动作得到确定并能够正确执行。

5.7 其他设计考虑

5.7.1 多机组核动力厂的安全系统和用于设计扩展工况的安全设施

5.7.1.1 多机组核动力厂中的每台机组必须具备各自的安全系统和用于设计扩展工况的安全设施。

5.7.1.2 为进一步提高安全性,在设计中应适当考虑多机组核动力厂允许各机组间相互连接的手段。

5.7.2 含有易裂变或放射性物质的系统

在核动力厂中所有可能含有易裂变或放射性物质的系统设计必须能够：防止可能导致放射性不受控制地向环境释放的事件发生；防止出现意外临界和过热；确保放射性释放量在正常运行工况下保持在允许的排放限值内，在事故工况下保持在可接受的限值内，并可合理达到的尽量低；便于缓解事故的放射性后果。

5.7.3 用于热电联产、供热或海水淡化的核动力厂

与热利用装置（如区域集中供热）和/或海水淡化装置连接的核动力厂的设计必须能够防止在运行状态和事故工况下放射性核素从核动力厂迁移到海水淡化装置或区域集中供热装置。

5.7.4 撤离路线

5.7.4.1 核动力厂必须设置足够数量的、具有醒目且永久标识的撤离路线，并配备为安全使用这些路线所必需的可靠的应急照明、通风和其他辅助设施。

5.7.4.2 撤离路线必须符合辐射分区、防火、工业安全，以及核动力厂安保方面的有关要求。

5.7.4.3 在发生设计中考虑的内、外部事件或多个事件的组合后，必须至少有一条路线可供位于场区内工作场所和其他区域的人员撤离。

5.7.5 通信系统

5.7.5.1 必须在整个核动力厂范围内设置有效的通信手段，以有助于所有正常运行模式下的安全运行，并在所有假设始发事件后和在事故工况下可用。

5.7.5.2 必须设置适当的报警系统和通信手段，以便在各种运行状态下和事故工况下，所有在核动力厂现场和厂区的人员都能得到警报和指令。

5.7.5.3 必须设置适当且多样化的通信手段，以满足在核动力厂范围内和毗邻区域的安全所需以及与相关厂外机构进行通信的需要。

5.7.6 核动力厂出入口控制

5.7.6.1 必须通过对各种构筑物进行适当的布置，将核动力厂与其周围环境隔离，从而能对核动力厂的出入口进行控制。

5.7.6.2 必须在进行厂房设计和厂区布置时，采取必要的措施来对运行人员和（或）设备（包括应急响应人员和车辆）进入核动力厂进行控制，而且必须考虑防止未经授权的人员和物品进入核动力厂。

5.7.7 防止未经批准接近或影响安全重要物项

必须防止未经批准接近或影响安全重要物项，包括计算机硬件和软件。

5.7.8 防止安全重要系统间不利的相互作用

5.7.8.1 必须对核动力厂要求同时运行的安全重要系统可能的不利相互作用进行评价，并且必须防止任何不利相互作用的影响。

5.7.8.2 在安全重要系统可能的不利相互作用分析中，必须适当考虑实体的相互连接，以及一个系统的运行、误操作或故障对其他重要

系统局部环境的影响，以保证环境条件的变化不会影响到系统或部件执行预定功能的可靠性。

5.7.8.3 如果两个安全重要流体系统相互连接，并在不同的压力下运行，则两个系统都必须设计成能够承受较高的压力，或者必须采取措施防止较低压力下运行的系统超出其设计压力。

5.7.9 电网对核动力厂的影响

核动力厂内安全重要物项的功能应不受电网扰动（包括预期的电网电压和频率变化）的影响。

5.8 安全分析

5.8.1 核动力厂设计的安全分析

5.8.1.1 必须对核动力厂设计进行安全分析，在分析中必须采用确定论和概率论的安全分析方法来论证核动力厂在各类状态下是否安全。

5.8.1.2 在安全分析的基础上，必须确认安全重要物项的设计基准及其与始发事件和事件序列的联系。必须论证所设计的核动力厂能够满足各类运行状态下放射性释放的监管限值和剂量限值，并能够满足事故工况下的可接受限值。

5.8.1.3 安全分析必须确保核动力厂设计中已实施纵深防御。

5.8.1.4 安全分析必须论证核动力厂设计中适当考虑了各种不确定性，尤其是有适当的裕量以避免出现陡边效应以及早期或大量放射性释放。

5.8.1.5 对于核动力厂设计中所采用的各项分析假设、方法的适用性和保守程度，应基于当前状态或竣工状态进行更新和验证。

5.8.2 确定论方法

确定论安全分析方法必须包括：

(1) 制定和确认所有安全重要物项的设计基准；

(2) 表征与核动力厂设计和厂址相适应的假设始发事件；

(3) 分析和评价假设始发事件导致的事件后果，以确认鉴定要求；

(4) 比较分析结果与验收准则、设计限值、剂量限值以及可接受限值，以满足辐射防护要求；

(5) 论证通过安全系统的自动响应并结合所规定的操纵员动作能够管理预计运行事件和设计基准事故；

(6) 论证通过安全系统的自动响应和利用安全设施功能并结合预期的操纵员动作能够管理设计扩展工况。

5.8.3 概率论方法

设计必须充分考虑核动力厂所有运行模式和所有状态（包括停堆工况）下的概率安全分析，特别是：

(1) 论证整个设计是平衡的，没有任何一个设施或假设始发事件对于总的风险会有过大的或明显不确定的贡献，而且纵深防御的各层级是尽实际可能独立的；

(2) 确认核动力厂不存在陡边效应；

(3) 将分析结果和已规定的风险准则进行比较。

6 核动力厂系统设计要求

6.1 反应堆堆芯和相关特性

6.1.1 燃料元件和燃料组件性能

核动力厂燃料元件和燃料组件的设计必须使其能够保持结构完整性，并在考虑运行状态下所有可能导致其性能劣化的因素后，能够承受预期辐照水平。

6.1.1.1 需考虑如下原因引起的性能劣化：

(1)膨胀差和形变差；

(2)冷却剂外压；

(3)由于裂变产物和氦气在燃料元件内累积导致的内压；

(4)燃料组件中燃料和其他材料的辐照效应；

(5)功率变化引起的温度和压力变化；

(6)化学效应；

(7)静态和动态载荷，包括流致振动和机械振动；

(8)由于变形和化学效应导致的传热性能变化。

必须为资料、制造和计算中的不确定性留有裕量。

6.1.1.2 燃料设计限值必须包括预计运行事件中容许的燃料裂变产物泄漏量限值，从而使燃料仍能继续使用。

6.1.1.3 燃料元件和燃料组件必须能够承受燃料吊装过程中的载荷和应力。

6.1.2 反应堆堆芯结构性能

核动力厂燃料元件和燃料组件及其支撑件的设计，必须使其能够在运行工况以及除严重事故外的其他事故工况下，维持可冷却的几何形状且不妨碍控制棒插入。

6.1.3 反应堆堆芯控制

6.1.3.1 在核动力厂各种状态下(包括停堆后、换料期间和换料后、

预计运行事件和未导致堆芯严重损伤的事故工况）下，堆芯中子注量率分布必须具有固有稳定性。堆芯设计应尽量减少依赖控制系统使中子注量率分布、水平和稳定性在各种运行状态下保持在规定限值内。

6.1.3.2 必须提供用于检测堆内中子注量率分布以及变化的适当方法，保证堆芯内不存在任何未能检测到的违反设计限值规定的部位。

6.1.3.3 反应性控制装置的设计必须考虑到磨损以及辐照效应(如燃耗、物理特性的变化和气体的产生）。

6.1.3.4 在运行状态和未导致反应堆堆芯严重损伤的事故工况下必须对最大的正反应性引入量及其引入速率加以限制，以保证不致引起反应堆压力边界失效，维持堆芯冷却能力和防止反应堆堆芯严重损伤。

6.1.4 反应堆停堆

6.1.4.1 必须提供在运行状态和事故工况下安全停堆的手段。必须保证即使在堆芯具有最大反应性的情况下，仍能维持停堆状态。

6.1.4.2 停堆手段的有效性、动作速度和停堆深度必须足以保证不超出规定的燃料设计限值。

6.1.4.3 判断停堆手段是否足够时，必须考虑到发生在核动力厂任何部位的、可导致一部分停堆手段失灵（如控制棒插入故障）或可能引起共因失效的故障。

6.1.4.4 反应堆停堆手段必须至少由两个多样化的且独立的系统组成。

6.1.4.5 即使堆芯处于反应性最大的状态，这两个不同系统中也必须至少有一个系统独自有能力，以足够的深度和高可靠度使反应堆保

持次临界状态。

6.1.4.6 停堆手段必须足以防止在停堆期间、换料操作期间，以及停堆状态下其他例行或非例行操作期间出现的任何可预见的反应性增加而导致意外临界。

6.1.4.7 必须设置仪表并规定各项试验，以保证停堆手段总是处于核动力厂状态所要求的形态。

6.2 反应堆冷却剂系统

6.2.1 反应堆冷却剂系统的设计

6.2.1.1 核动力厂反应堆冷却剂系统部件的设计和制造，必须具有高质量的材料、恰当的设计标准、可检查性和高质量的加工，以尽量降低其发生故障的可能性。

6.2.1.2 与核动力厂反应堆冷却剂系统压力边界相连接的管道必须设置适当的隔离装置，以限制放射性流体（一回路冷却剂）的任何丧失，以及防止冷却剂通过接口系统流失。

6.2.1.3 反应堆冷却剂压力边界的设计必须使产生裂纹的可能性极小，已产生的裂纹也极不易于按快速裂纹扩展方式发展成为失稳断裂，以便允许及时探测到裂纹。

6.2.1.4 反应堆冷却剂系统的设计必须确保避免使反应堆冷却剂压力边界的部件可能出现脆性断裂的核动力厂状态。

6.2.1.5 反应堆冷却剂压力边界内包含的部件（如泵的叶轮和阀门部件）的设计必须使所有运行状态和设计基准事故下失效的可能性以及随后对一回路系统内其他安全重要部件造成的损伤最小，并为使用中可能发生的性能劣化留有适当的裕量。

6.2.2 反应堆冷却剂压力边界的超压保护

必须采取措施确保卸压装置的动作能够避免反应堆冷却剂系统压力边界出现超压，并且不会导致放射性物质从核动力厂向环境直接释放。

6.2.3 反应堆冷却剂的装量

必须采取措施来控制反应堆冷却剂的装量、温度和压力，以便在核动力厂运行状态下（恰当考虑容积变化和泄漏）使其均不超过规定的设计限值。

6.2.4 反应堆冷却剂的净化

6.2.4.1 必须在核动力厂设置适当的设施,以去除反应堆冷却剂中的放射性物质（包括活化腐蚀产物和来源于燃料的裂变产物）和非放射性物质。

6.2.4.2 所需系统的能力必须基于规定的容许燃料泄漏设计限值，且有保守的裕量，以保证核动力厂可在回路中的放射性水平可合理达到的尽量低的情况下运行，同时保证放射性释放低于规定排放限值，并可合理达到的尽量低。

6.2.5 反应堆堆芯的余热排出

必须为排出核动力厂停堆状态下的反应堆堆芯余热提供手段，以使燃料、反应堆冷却剂压力边界和安全重要构筑物不超出设计限值。

6.2.6 反应堆堆芯的应急冷却

6.2.6.1 必须提供冷却手段，以便在核动力厂事故工况下（即使没有保持一回路冷却剂系统压力边界的完整性），也能恢复和维持燃料的冷却。

6.2.6.2 冷却反应堆堆芯的手段必须能够确保：

(1) 不超过包壳或燃料完整性参数限值（如温度）；

(2) 可能出现的化学反应保持在可接受水平；

(3) 应急堆芯冷却手段可有效补偿燃料和堆内结构变形的影响；

(4) 反应堆堆芯的冷却能保持足够长的时间。

6.2.6.3 必须提供设计手段（如泄漏探测系统、适当的互相连接和隔离能力）及适当的多重性和多样性，以便对每个假设始发事件都切实地满足 6.2.6.2 节的要求。

6.2.7 热量向最终热阱的传输

6.2.7.1 对所有核动力厂状态都必须确保将热量传输到最终热阱的能力。

6.2.7.2 在热量传输系统必须实现其传热功能的核动力厂状态下，热量传输系统必须具有足够的可靠性。这可能要求采用多样化的最终热阱或者多样化的排热途径将热量传输至最终热阱。

6.2.7.3 在比设计中考虑的自然灾害（由厂址灾害评价确定）更严重水平下仍能够实现传热功能。

6.3 安全壳结构和安全壳系统

6.3.1 反应堆安全壳系统

必须设置安全壳系统，以保证或有助于核动力厂实现以下安全功能：

(1)在运行状态和事故工况下包容放射性物质；

(2) 保护反应堆免于外部自然事件和人为事件的影响；

(3) 在运行状态和事故工况下屏蔽辐射。

6.3.2 控制放射性从安全壳释放

6.3.2.1 安全壳的设计必须能够保证从核动力厂向环境的任何放射性释放是可合理达到的尽量低，运行状态下低于监管排放限值和事故工况下低于可接受的限值。

6.3.2.2 安全壳结构及影响安全壳系统密封性的系统和部件的设计和建造，必须使得：能够在安全壳的所有贯穿件安装完成后和必要时在核动力厂运行寿期内进行泄漏率试验，能够在安全壳的设计压力下进行泄漏率试验。

6.3.2.3 安全壳贯穿件的数量必须保持尽实际可能的少,并且所有贯穿件都必须满足与安全壳结构本身同样的设计要求。必须保护贯穿件能够承受由管道位移引起的反作用力，或承受诸如外部或内部事件产生的飞射物、喷射力和管道甩击引起的事故载荷。

6.3.3 安全壳隔离

6.3.3.1 对于依赖安全壳密封性来防止放射性物质向环境的释放超过可接受限值的事故中，作为反应堆冷却剂压力边界组成部分的或直接与安全壳大气相通的贯穿核动力厂安全壳的每根管线都必须能自动且可靠地封闭。

6.3.3.2 贯穿安全壳且属于反应堆冷却剂压力边界组成部分的或直接与安全壳大气相通的管线必须至少串联设置两个合适的安全壳隔离阀或逆止阀，并且必须配备适当的泄漏探测系统。通常应在安全壳内外各设置一个安全壳隔离阀或止回阀，安全壳隔离阀或逆止阀必须尽实际可能地靠近安全壳，如采取其他的设置方式则应论证其满足设计要求。安全壳隔离阀或止回阀都必须能够可靠和独立地动作及进行

定期试验。

6.3.3.3 对于仪表管线等特定类别的管线，或者在应用第 6.3.3.2 节中所述安全壳隔离方法将会降低包含安全壳贯穿件的安全系统可靠性的情况下，可允许第 6.3.3.2 节中所述的安全壳隔离要求存在例外情况。

6.3.3.4 贯穿安全壳，但既不是反应堆冷却剂压力边界的一部分，也不直接与安全壳内大气相通的管线，必须至少配备一个适当的安全壳隔离阀。安全壳隔离阀必须安装在安全壳外部，并尽实际可能地靠近安全壳。

6.3.4 安全壳的进入

6.3.4.1 运行人员必须通过装有若干道闸门的气封闸门进入核动力厂安全壳。这些闸门是联锁的，以确保反应堆功率运行和事故工况时，至少有一道闸门是关闭的。

6.3.4.2 当采取措施使运行人员出于监督目的进入安全壳时，设计中必须采取措施，以保证运行人员的防护和安全。如果通过设备气密闸门进入安全壳，设计中必须采取措施，以保证运行人员的防护和安全。

6.3.4.3 对于贯穿安全壳进行设备或材料运输的安全壳开口，设计时必须保证在需要对安全壳进行隔离时能够快速和可靠地关闭。

6.3.5 安全壳状态控制

6.3.5.1 必须采取措施控制核动力厂安全壳内的压力和温度，并控制裂变产物或可能在安全壳内释放并可能影响安全重要系统运行的其他气态、液态或固态物质的任何累积。

6.3.5.2 设计必须为安全壳内各独立隔间之间提供足够的气流通道。隔间之间各种开口的截面尺寸必须能够确保在事故工况下的压力平衡期间出现的压力差不会对承压结构或缓解事故工况后果的重要系统造成不可接受的损坏。

6.3.5.3 必须确保安全壳的排热能力,以便在发生任何高能流体意外释放事故后，降低安全壳中的压力和温度并使之维持在可接受的水平。执行从安全壳中排热功能的系统必须具有足够的可靠性和多重性，以确保这一功能得到实现。

6.3.5.4 必须采取设计措施在所有核动力厂状态下防止丧失安全壳结构完整性。措施必须不会导致早期或大量放射性释放。

6.3.5.5 设计中必须包含能安全使用移动设备恢复安全壳排热能力的设施，这些移动设备不必在厂区贮存。

6.3.5.6 在需要时,必须提供设计措施控制可能释放到安全壳中的裂变产物、氢气、氧气和其他物质，以便：

(1) 减少事故工况下可能释放到环境中的裂变产物数量；

(2) 在事故工况下控制安全壳大气中的氢气、氧气和其他物质的浓度，以防止发生可能危及安全壳完整性的燃爆或爆燃载荷。

6.3.6 覆盖层、保温材料和涂层

必须审慎选择安全壳系统内部件和结构的覆盖层、保温材料和涂层，而且必须明确规定其使用方法，以确保这些部件和结构的安全功能得到实现，并在覆盖层、保温材料和涂层劣化时尽量减少对其他安全功能的影响。

6.4 仪器仪表和控制系统

6.4.1 仪器仪表

6.4.1.1 必须设置用于以下目的的仪器仪表：确定可能影响核动力厂裂变过程、反应堆堆芯完整性、反应堆冷却剂系统完整性和安全壳完整性的所有主要变量的值；获得核动力厂安全和可靠运行所需的重要信息；确定核动力厂在事故工况下的状态以及用于事故管理的决策。

6.4.1.2 必须设置仪器仪表和记录设备，以确保获得必不可少的信息，用于监测重要设备的状况和事故过程、预测可能出现放射性物质释放的位置和设计释放位置的放射性物质释放量，以及进行事故后分析。

6.4.2 控制系统

必须设置合适且可靠的控制系统使得核动力厂相关的过程变量保持在规定的运行范围内。

6.4.3 保护系统

6.4.3.1 必须设置能够探测核动力厂不安全状态和自动触发安全动作的保护系统，以启动必要的安全系统来实现和维持核动力厂安全状态。

6.4.3.2 保护系统的设计必须：

(1) 能够超越控制系统的不安全动作。

(2) 具备故障安全特性，以便在保护系统发生故障时能使核动力厂达到安全状态。

6.4.3.3 设计：

(1) 必须防止操纵员在运行状态和事故工况下采取可能损害保护

系统有效性的动作，但不得阻碍操纵员在事故工况下采取正确行动；

(2) 在预计运行事件或事故工况开始后的合理时间范围内，用于启动安全系统的各种安全动作必须能自动执行，而无需操纵员干预；

(3) 必须向操纵员提供相关信息，用于监测自动动作的效果。

6.4.4 仪表和控制系统的可靠性和可试验性

6.4.4.1 核动力厂安全重要物项的仪表和控制系统必须具有与所执行的安全功能相适应的高可靠性和定期可试验性。

6.4.4.2 必须在实际可行的范围内采用各种设计技术,如可试验性（必要时包括自检能力）、故障安全特性、功能多样性、部件设计或工作原理的多样性等以防止安全功能的丧失。

6.4.4.3 安全系统必须具有可在核动力厂运行时对其功能进行定期试验，包括各通道分别进行试验的能力，以查明可能发生的故障和多重性的丧失。设计必须允许对包括从传感器到最终的触发驱动器和显示单元所有环节的定期试验。

6.4.4.4 在设计中应考虑,当安全系统或安全系统的一部分由于试验或维修而必须退出运行时，在此期间必须对保护系统旁通状态进行明确的指示。

6.4.5 基于计算机的设备在安全重要系统中的应用

6.4.5.1 当安全重要系统设计成依赖于基于计算机的设备时,必须确定或制定有关开发和试验/验证计算机硬件和软件的相应标准，并在系统的整个寿期，特别是在软件开发期间，就加以实施。整个开发过程必须遵循质量保证大纲。

6.4.5.2 安全系统或安全有关系统中基于计算机的设备：

(1) 基于系统对安全的重要性，必须使用高质量和最佳实践的硬件和软件；

(2) 整个开发过程，包括设计变更的控制、试验和调试，必须系统地形成文件，并可供审查；

(3) 必须由独立于设计者和供应商的专业人员对基于计算机的设备进行评价，以保证其高可靠性；

(4) 在安全功能对实现和保持安全状态至关重要而且不能以很高置信度证明设备具有必要的高可靠性的情况下，必须提供多样化手段以确保安全功能的执行；

(5) 必须考虑软件的共因故障；

(6) 必须提供保护，防止系统运行意外中断或受到蓄意干扰。

6.4.6 保护系统和控制系统的分隔

6.4.6.1 必须防止核动力厂保护系统和控制系统之间的相互干扰，可以通过分隔、避免相互连接或采用适当的功能独立来实现。

6.4.6.2 如果保护系统和控制系统共用相同的信号,必须确保适当的分隔措施（如有效的去耦）且信号系统必须划分为保护系统的一部分。

6.5 控制室

6.5.1 核动力厂必须设置控制室，以进行下述活动：在各种运行状态下以自动或手动方式安全地运行核动力厂；出现预计运行事件和事故工况后，采取相应措施，以保持核动力厂的安全状态或使之回到安全状态。

6.5.2 必须采取适当的措施(包括在核动力厂控制室和外部环境之

间设置屏障），并且向控制室人员提供足够的信息，以在较长时间内保护控制室人员免于受到事故工况下形成的高辐照水平、放射性物质的释放、火灾、爆炸性物质或有毒气体的危害。

6.5.3 必须特别关注对可能危及控制室连续运行的（控制室）内、外部事件的识别。设计中必须采取合理可行的措施，将这些事件的后果减至最小。

6.5.4 控制室设计必须提供恰当的裕量,应对比设计中考虑的自然灾害水平（由厂址灾害评价确定）更为严重的自然灾害。

6.5.5 控制室设计必须考虑工效学的因素。控制室内仪表的布置和信息显示的方式必须便于运行人员正确掌握核动力厂现状和性能的全貌。必须设置有效的可视装置和适当的声响装置，用于指示偏离正常和可能危及安全的运行状态和过程。

6.6 辅助控制室

6.6.1 必须在核动力厂内与控制室在实体分隔、电气隔离、实体隔离和功能隔离的一个独立地点（辅助控制室）配置仪表和控制设备。辅助控制室应能在控制室丧失执行重要安全功能时完成下述任务：使反应堆进入并保持在停堆状态，排出余热并监测核动力厂的重要参数。

6.6.2 第 6.5.2 中的相关要求,如果适当也可用于核动力厂辅助控制室。

6.7 场内应急设施

6.7.1 场内应急设施通常包括应急控制中心、技术支持中心和运行支持中心，其设计必须保证工作人员在事故（包括严重事故）和灾害情况下能够在此执行预期的应急任务。

6.7.2 应根据需要向应急设施提供核动力厂重要参数和核动力厂内及其外围放射性状况的信息。每个应急设施应配备联络核动力厂控制室、辅助控制室和其他重要场所以及场内、场外应急响应组织的适当通信手段。

6.8 应急动力供应

6.8.1 应对丧失厂外电源的设计

6.8.1.1 核动力厂应设计有应急动力源，以在任何预计运行事件或设计基准事故下一旦丧失厂外电源时提供必要的动力供应。还应设计有替代动力源以在设计扩展工况下提供必要的动力供应。

6.8.1.2 核动力厂应急动力源、替代动力源设计必须包括能力、可用性、持续时间、容量和持续性的要求。

6.8.1.3 用于提供应急动力的综合手段（如水轮机、汽轮机、燃气轮机、柴油机或蓄电池）必须具备与需要其提供动力的安全系统所有要求相适应的可靠性和类型，必须能够进行功能试验。

6.8.1.4 在同时丧失厂外电源和应急动力源的情况下，替代动力源必须能够提供必要的动力，以保证反应堆冷却剂系统的完整性并防止堆芯和乏燃料出现严重损伤。

6.8.1.5 缓解反应堆堆芯熔化后果所必需的设备，必须能够通过任何可用的动力源提供动力。

6.8.1.6 替代动力源应与应急动力源相互独立并进行实体隔离，替代电源接入时间应与蓄电池组放电时间相匹配。

6.8.1.7 在交流电源丧失的情况下，应确保核动力厂关键参数监测

以及完成安全必要的短期行动的持续动力供应。

6.8.1.8 为安全重要物项提供应急动力源的任何柴油机或其他原动机的设计基准必须包括：

（1）相关的燃油贮存和供应系统在规定时间内满足需求的能力；

（2）原动机在所有规定工况下和在所要求的时间成功启动和运行的能力；

（3）原动机的辅助系统，如冷却系统。

6.8.1.9 设计也应包含通过一些移动设备安全投运来恢复必要的动力供应，这些移动设备不必在厂区贮存。

6.9 支持系统和辅助系统

6.9.1 支持系统和辅助系统的性能

支持系统和辅助系统的设计必须能够确保这些系统的性能与其所支持的核动力厂系统或部件的安全重要性相适应。

6.9.2 热传输系统

6.9.2.1 必须设置适当的辅助系统以排出核动力厂运行状态和事故工况下要求运行的系统和部件中的热量。

6.9.2.2 热传输系统的设计必须确保其非关键部分能够被隔离。

6.9.3 工艺取样系统和事故后取样系统

6.9.3.1 必须设计工艺取样系统和事故后取样系统,以便在所有核动力厂运行状态和事故工况下及时测定流体工艺系统中和取自核动力厂系统或环境的气体或液体样品中特定的放射性核素的浓度。

6.9.3.2 必须在核动力厂提供适当的手段,以便监测可能造成重大污染的流体系统的活度以及收集工艺样品。

6.9.4 压缩空气系统

需在压缩空气系统设计基准中明确为核动力厂安全重要物项服务的所有压缩空气的品质、流量和清洁度要求。

6.9.5 空调系统和通风系统

6.9.5.1 必须在核动力厂辅助房间或其他区域提供适当的空调、采暖、空冷和通风系统，以便在所有核动力厂状态下保持安全重要系统和部件所需的环境条件。

6.9.5.2 必须为核动力厂内的建筑物配备具有适当净化能力的通风系统，以：

(1) 防止气载放射性物质在核动力厂内不可接受的扩散；

(2) 降低特定区域内气载放射性物质的浓度，使之符合人员进入所要求的水平；

(3) 保持核动力厂内气载放射性物质的放射性水平在规定限值之内，并符合可合理达到的尽量低原则；

(4) 在不影响对放射性流出物的控制能力的条件下，维持含有惰性气体或有害气体的房间的通风；

(5) 控制气态放射性物质向环境的释放，并保持在规定限值之内，以及保持可合理达到的尽量低。

6.9.5.3 核动力厂内污染较高的区域相对于污染较低的区域和其他可进入的区域，必须维持适当的负压差。

6.9.6 消防系统

6.9.6.1 必须在适当考虑火灾危害分析结果的情况下设置消防系统，包括火灾探测系统和灭火系统、防火封隔屏障及烟雾控制系统。

6.9.6.2 安装的消防系统应能安全地处理各种类型假设火灾事件。

6.9.6.3 如果适当，灭火系统必须能够自动启动。灭火系统的设计和布置要保证其破裂、误动作或意外操作不会显著影响安全重要物项的性能。

6.9.6.4 火灾探测系统必须设计成能够及时为运行人员提供有关火灾位置和火灾蔓延情况的信息。

6.9.6.5 对付假设始发事件发生后可能的火灾所需的探测系统和灭火系统，必须具备抵御假设始发事件影响的适当能力。

6.9.6.6 必须尽可能使用不可燃或阻燃材料和耐热材料,特别是在安全壳和控制室内。

6.9.7 照明系统

在运行状态和事故工况下，必须为核动力厂内的所有操作区提供充足的照明。

6.9.8 核动力厂起重设备

核动力厂中用于吊运安全重要物项以及在安全重要物项附近区域吊运其他物项的起重设备，其设计应满足以下要求：

(1)应采取必要的措施防止超载；

(2)应采取保守的设计手段防止可能影响安全重要物项的重物的意外跌落；

(3)核动力厂厂房布置应考虑起重设备及其所吊物项的吊运安全；

(4)应保证起重设备在核动力厂规定的状态下完成操作（设置安全联锁）；

(5)在有安全重要物项区域使用的起重设备，需要进行抗震鉴定。

6.10 其他功率转换系统

6.10.1 蒸汽供应系统、给水系统和汽轮发电机

6.10.1.1 核动力厂蒸汽供应系统、给水系统和汽轮发电机的设计必须能够确保在运行状态或事故工况中，反应堆冷却剂压力边界不超过设计限值。

6.10.1.2 蒸汽供应系统必须设计有适当等级的、经鉴定的蒸汽隔离阀，其能够在运行状态和事故工况的特定条件下关闭。

6.10.1.3 蒸汽供应系统及给水系统应具备足够的能力，且设计中必须避免预计运行事件升级为事故工况。

6.10.1.4 必须为汽轮发电机提供适当的保护，如超速保护和振动保护，并且必须采取措施将汽轮发电机产生的飞射物对安全重要物项的可能影响降至最低。

6.11 流出物排放和放射性废物处理

6.11.1 为使放射性物质排放总量及浓度保持在规定限值以内并可合理达到的尽量低，核动力厂必须设置适当的处理放射性固体、液体和气体废物的系统。

6.11.2 必须设置适当的系统，以管理放射性废物和在一段期限内在现场安全地贮存这些废物，该期限与相应的废物处置方案相适应。

6.11.3 核动力厂必须具备有适当设施,以便于放射性废物的转移、运输和装卸。必须考虑设施的可达性及吊装和包装的能力。

6.11.4 必须在核动力厂内对放射性液态和气态流出物进行处理，使其向环境的排放对公众造成的辐射照射可合理达到的尽量低。

6.11.5 核动力厂必须具备适当手段，以控制液态流出物向环境的

释放可合理达到的尽量低，并保持在规定限值以内。

6.11.6 为使气载放射性物质向环境的释放保持在规定的限值以内，净化设备必须具备必需的滞留因子。过滤系统必须具有测试其效率的条件，能够在寿期内定期监测其性能和功能，并能更换滤芯而同时保持通风量。

6.12 燃料装卸和贮存系统

6.12.1 必须在核动力厂建立燃料装卸和贮存系统，以确保在燃料装卸和贮存期间始终保持燃料的完整性和特征。

6.12.2 核动力厂的设计必须包括适当的设施，以便于新燃料和乏燃料的起吊、移动和装卸。

6.12.3 核动力厂的设计必须能够防止在燃料或屏蔽容器移动过程中或发生燃料或屏蔽容器坠落时对安全重要物项造成任何显著损坏。

6.12.4 已辐照燃料和未辐照燃料的装卸和贮存系统的设计必须：

(1) 通过采用物理手段或工艺措施（应优先采用几何安全布置）并留有规定的裕量，确保即使在最佳慢化的条件下也不会临界；

(2) 允许对燃料进行检查；

(3) 允许对安全重要部件进行维护、定期检查和试验；

(4) 防止对燃料造成损坏；

(5) 防止燃料在转运过程中跌落；

(6) 能够标识每个燃料组件；

(7) 提供满足相关辐射防护要求的适当手段；

(8) 保证具有适当的操作程序和核燃料衡算控制，以防止核燃料丢失或丧失对核燃料的控制。

6.12.5 已辐照燃料的装卸和贮存系统的设计必须：

(1) 允许在运行状态和事故工况下充分地排出燃料中的热量；

(2) 防止给燃料元件或燃料组件造成不可接受的操作应力；

(3) 防止乏燃料运输容器、起重设备或其他重物跌落在燃料上对燃料造成可能的损坏；

(4) 能安全地贮存疑似损坏或已损坏燃料元件或燃料组件；

(5) 控制可溶中子吸收材料的浓度水平（如果用于临界安全）；

(6) 燃料装卸和贮存设施便于维修和退役；

(7) 燃料装卸和贮存区域和设备（必要时）便于去污；

(8) 根据预定的堆芯管理策略和整个堆芯中的燃料数量，能够容纳反应堆中卸出的全部燃料并有足够的裕量；

(9) 便于从贮存设施中移出燃料和对其进行厂外运输的准备。

6.12.6 对于采用水池系统进行燃料贮存的反应堆，其设计必须防止在所有与乏燃料水池有关的核动力厂状态下发生燃料组件裸露，“实际消除”导致早期或大量放射性释放工况发生的可能性，以避免在厂区形成高辐射区域。核动力厂的设计：

(1) 必须提供必要的燃料冷却能力；

(2) 在乏燃料水池泄漏或管道破口工况下，必须提供相应的手段防止燃料组件发生裸露；

(3) 必须提供恢复水装量的能力。

设计必须还包括能够使用移动设备进行补水以确保水池有足够的水量长期冷却乏燃料和辐射屏蔽。

6.12.7 设计必须包含如下要求：

(1) 在运行状态和与乏燃料水池相关的事故工况下具有监测和控制乏燃料水池池水温度和水位，以及池水和空气放射性活度的手段；

(2) 在运行状态下具有监测和控制乏燃料水池水化学的手段。

6.13 辐射防护

6.13.1 辐射防护设计

6.13.1.1 必须采取措施确保核动力厂的工作人员接受的剂量不超过规定限值并且保持在可合理达到的尽量低，并考虑相关的剂量约束。

6.13.1.2 必须全面识别核动力厂的各种辐射源，将来自各种辐射源的照射和放射性风险保持在可合理达到的尽量低，控制腐蚀产物和活化产物的产生和迁移。

6.13.1.3 在合理可实施的情况下，构筑物、系统和部件制造的材料应该选用不易辐照活化的材料。

6.13.1.4 必须采取措施防止来自核动力厂各种放射性物质、放射性废物或表面污染的释放或扩散。

6.13.1.5 核动力厂的布置必须保证存在辐射危害和潜在放射性污染区域得到有效的控制，并通过出入控制和通风的方式防止或减少工作人员所受的辐射照射和污染。

6.13.1.6 核动力厂的布置必须尽量减少工作人员在正常运行、换料、维修和检查时的辐照剂量，贯彻可合理达到的尽量低原则。为满足上述要求，在设计上应充分考虑提供专用工具的必要性。

6.13.1.7 应根据运行状态（包括换料、维修和检查）对应区域的停留要求、辐射水平和表面污染水平，以及事故工况下潜在辐射水平和表面污染水平，将核动力厂划分为不同的辐射分区。应设置屏蔽以

避免或降低辐射照射。

6.13.1.8 必须将经常进行维护或手动操作的设备布置在剂量率较低的区域，以减少对工作人员的照射。

6.13.1.9 必须为工作人员和核动力厂设备提供合适的去污设施。

6.13.2 辐射监测

6.13.2.1 为了确保在运行状态下和设计基准事故工况下提供充分的辐射监测及在设计扩展工况下提供尽实际可行的辐射监测，必须设置相应的辐射监测设备。

6.13.2.2 必须提供固定式剂量率仪表，用于监测工作人员日常出入的场所和在运行状态下辐射水平的变化使得仅能允许在某些规定时段内出入的场所的辐射剂量率。

6.13.2.3 必须在适当的地点安装固定式剂量率仪表，以反映事故工况下核动力厂的总体辐射水平。固定式剂量率仪表必须在主控室或工作人员能够在必要时采取纠正行动的适当控制部位给出充分的信息。

6.13.2.4 必须安装固定式监测设备，用于在工作人员日常停留的区域和气载放射性物质的活度水平可能达到须采取保护措施程度的区域测量大气中放射性物质的活度。当探测到放射性活度高时，这些系统必须在主控室或其他适当地点给出指示。还必须在因设备故障或其他异常情况可能会造成污染的区域提供监测设备。

6.13.2.5 必须设置固定式设备和实验室设施，用于及时测定运行状态下和事故工况下流体工艺系统中的选定放射性核素的浓度以及从核动力厂系统或环境中采集的气体和液体样品中的选定放射性核素的

浓度。

6.13.2.6 必须设置固定式设备，用于在核动力厂向环境排放之前或在排放期间监测放射性流出物和可能被污染的流出物。

6.13.2.7 必须设置用于测量表面污染的仪器仪表。必须在辐射监督区和控制区的主要出入口设置固定式监测设备（如门式辐射监测器、手足监测器），以便监测运行人员和设备。

6.13.2.8 必须设置用于测量工作人员所受照射和污染的设施。必须制订用于评定和记录工作人员随时间所受累积剂量的程序。

6.13.2.9 必须作出安排，通过对剂量率或放射性浓度进行环境监测来评定核动力厂周围地区的照射和其他辐射影响，并特别涉及：

(1) 对人的照射途径，包括食物链；

(2) 对当地环境的辐射影响；

(3) 放射性物质在环境中的可能积聚和积累；

(4) 是否存在任何未经批准的放射性释放路径的可能性。

名 词 解 释

在核动力厂安全规定中下述名词术语的含义为：

可控状态

核动力厂在发生预计运行事件或事故工况后，能够确保基本安全功能并维持足够长时间（从而采取措施达到安全状态）的状态。

核动力厂状态

运行状态		事故工况		
			设计扩展工况	
正常运行	预计运行事件	设计基准事故	无燃料明显损伤	堆芯熔化

事故工况

偏离正常运行，比预计运行事件发生频率低但更严重的工况。

ⓘ：事故工况包括设计基准事故和设计扩展工况

设计基准事故

核动力厂按确定的设计准则和保守的方法在设计中采取了针对性措施的那些假想事故，并且该事故中放射性物质的释放被限制在可接受限值以内。

设计扩展工况

不在设计基准事故考虑范围，但按最佳估算方法在设计

过程中需要加以考虑的假想事故工况，并且该事故中放射性物质的释放被限制在可接受限值以内。

ⓘ：设计扩展工况包括未发生堆芯熔化的工况和发生堆芯熔化的工况。

安全状态

核动力厂在发生预计运行事件或事故工况后，反应堆处于次临界，并能够确保基本安全功能且长期保持稳定的状态。

用于设计扩展工况的安全设施

在设计扩展工况中执行某种安全功能或具有某种安全功能的物项。

安全系统整定值

为防止出现超过安全限值的状态，在发生预计运行事件或事故工况时启动有关自动保护装置的触发点。

陡边效应

核动力厂中的“陡边效应”指，核动力厂参数微小偏离后导致核动力厂从一种状态突变到另一种状态，从而在响应输入中的微小变化时突然发生大的变化的严重异常核动力厂行为。

原动机

原动机是在接到驱动装置的命令后将能量转化为动作的部件（如发动机、电磁操作器或气动操作器）。