核动力厂设计安全规定

（2016年修订，2016年10月26日国家核安全局批准发布）

1 引 言

1.1 目的

为实现核动力厂的安全运行，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、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，分析中必须考虑各种假设始发事件，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）与核动力厂及厂址环境直接相关。

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

核动力厂运行所引起的非放射性影响。

1.2.3 本规定中的核动力厂主要是指为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 其他类型或采用革新技术的反应堆设计可参照本规定，但应经过细致的评价和判断。

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，以保护人与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）控制在运行状态下对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、乏燃料、放射性废物或任何其他辐射源失控事件发生的可能性；

（3）如果上述事件发生，减轻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的所有活动，包括规划、选址、设计、制造、建造、调试、运行和退役，以及有关放射性物质的运输、乏燃料和放射性废物的管理等。

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低于规定限值，且可合理达到的尽量低。同时，还应采取措施减轻任何事故的放射性后果。

2.2.2 为了实现基本安全目标，辐射防护设计必须使得核动力厂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，并符合运行限值和辐射防护标准，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所引起有害后果的事故，并在一旦发生事故时减轻其后果；

（2）保证在设计中考虑的所有事故的放射性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）保证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。此种安全评价要考虑以下内容：（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，营运单位制定的核动力厂事故管理规程，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故序列；必须保证发生频率高的核动力厂事故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，涉及核动力厂各种功率及停堆状态下有关的组织、人员行为或设计，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，以应对厂内设备故障或人因引起的各种预计运行事件和事故，以及外部事件引起的后果。

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，防止事故对人员和环境造成危害。如果某一层次的

防护失效，则由后一层次提供保护。每一层次防御的独立有效性都是纵深防御的必要组成部分。

（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的故障。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，并对部件的制造、核动力厂的建造和调试进行质量控制。在这一层次，降低内部危险可能性的设计措施有助于事故的预防。还应重视涉及设计、制造、建造、在役检查、维修和试验的过程和规程，以及进行这些活动时良好的可达性、核动力厂的运行方式和运行经验的利用等方面。整个过程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干预措施的放射性释放，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。安全目标是，在严重事故下仅需要在区域和时间上采取有限的防护行动，且避免场外放射性污染或将其减至最小。这要求可能导致早期放射性释放或者大量放射性释放的事件序列被实际消除。

（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的潜在放射性释放造成的放射性后果。该层次要求配备恰当的应急设施，制定用于场内、场外应急响应的应急计划和应急程序。

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。所需实体屏障的数目取决于放射性核素总量和同位素成份表征的初始源项、单个屏障的有效性、可能的内部与外部危险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务院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。该大纲包括保证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验证和确认。在设计和建造过程中应尽早完成验证、确认和批准,最迟不晚于核动力厂首次装料。

3.3 全寿期内保持核动力厂设计的安全和完整性

3.3.1 营运单位对安全负全面责任。营运单位必须建立一套正式的体系，在整个寿期内始终保证核动力厂设计的安全和完整性。

3.3.2 为便于安全分析报告、设计手册和其他设计文件等详细的设计资料转移至营运单位，应尽早设立全面负责设计过程的部门，并制定管理流程，在营运单位的管理体系内负责核动力厂设计安全和完整性。

3.3.3 核动力厂的设计工作可以由许多组织分担：工程公司、反应堆及其辅助系统供应商、主要设备供应商、电气系统的设计单位以及对核动力厂安全重要的其它系统的供应商等。营运单位必须对委托给外部组织的设计活动进行管理。

3.3.4 全面负责设计过程的部门必须保证核动力厂设计满足安全性、可靠性和质量方面的验收准则。这些准则符合相关的法律法规和标准规范。必须建立并明确工作范围和职责，以保证：

（1）设计符合其目标，并满足防护和安全最优化的要求，使辐射风险保持在可合理达到的尽量低的水平；

（2）持续保证设计安全的方式包括设计验证、确定工程规范和标准及要求、采用经验证的工程实践、提供建造经验反馈、批准重要工程文件、开展安全评价和保持安全文化；

（3）安全运行、维修（包括合适的试验周期）和修改所需的设计资料应该是可用的，设计资料应适当考虑以往的运行经验和经验证的研究成果，并由营运单位维护在最新状态；

（4）保持对设计要求和状态控制的管理；

（5）建立和控制责任设计者和参与设计工作的供应商之间必要的接口；

（6）营运单位需维护必要的工程专业资料和科技资料；

（7）所有设计变更都经过审查、验证、形成文档并批准；

（8）维护充分的文件，以便今后开展核动力厂退役工作。

4 主要技术要求

4.1 基本安全功能

4.1.1 必须保证在核动力厂所有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，导出乏燃料贮存设施所贮存燃料的热量；

（3）包容放射性物质、屏蔽辐射、控制放射性的计划排放，以及限制事故的放射性释放。

4.1.2 必须用全面、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，以及在核动力厂所有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，以保证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在整个寿期内受到的辐射剂量，在运行状态下不超过剂量限值，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，并必须保证发生可能性较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，必须制定与核动力厂各类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，满足国务院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管理规程和运行规程的实践（即运行限值和条件）。

4.3.3 设计必须适当考虑其他核动力厂在设计、建造和运行中获得的相关经验，以及相关的研究成果。

4.3.4 设计必须适当考虑确定论安全分析和概率论安全分析的结果，保证已经适当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。纵深防御的各层次之间必须尽实际可能地相互独立，避免一个层次防御的失效降低其他层次的有效性。

4.4.2 设计必须应用纵深防御概念，提供多层次防御，预防可能对人与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与环境，减轻事故后果。

4.4.3 设计必须适当考虑这样的事实：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）必须设置多道实体屏障，阻止放射性物质向环境释放；

（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、系统和部件以及规程，以控制超出安全系统能力的故障和偏离正常运行的进程，并尽实际可能地限制其后果；

（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，并减轻任何故障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

层次防御至多第二层次防御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（如用于减轻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 实物保护

4.5.1 必须设置实物保护措施，即核安保措施，包括实物保护系统和相关管理措施，以防止、侦查和应对涉及核材料和核动力厂相关设施的偷窃、蓄意破坏、未经授权的接触，非法转让或其他恶意行为，以及防范恐怖分子获取材料、破坏核动力厂等。

4.5.2 应根据保护目标的重要程度和潜在风险确定核动力厂实物保护的等级，并按照确定的等级进行实物保护系统设计。应合理布置核动力厂的控制区、保护区和要害区，实现分区保护，并为各区配备相应的设施和设备。

4.5.3 实物保护系统必须考虑出入口控制、探测、报警、集中控制、照明、通讯、供电和巡更等方面，并设置多重实体屏障。

4.5.4 核动力厂应配备武警或守卫，制定实物保护相关管理程序，使得管理措施与技防措施有机结合，以保证实物保护系统的完整、可靠与有效。

4.5.5 应对实物保护设计方案进行风险分析和有效性评估。

4.5.6 必须以统筹兼顾的方式设计和实施核动力厂的核安全措施、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 必须鉴别和评价用于核动力厂安全重要物项设计准则的规范和标准，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，或存在偏离已有工程实践的情况时，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、设施或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，以验证达到了预期效果。

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，并确认在竣工、运行和修改时交付的设计满足制造和建造的要求。

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 必须将安全评价形成文件以便于独立评估。

4.8 便于建造的要求

4.8.1 核动力厂安全重要物项的设计必须使其能够按照确定的流程进行制造、建造、装配和安装，以保证满足设计规范和所要求

的安全水平。

4.8.2 核动力厂的建造和运行，必须适当考虑从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 放射性废物管理和退役

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核动力厂退役和拆除的特性。

4.9.2 在设计中必须适当考虑：

（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（例如分离或分拣、表征、分类、预处理、处理和整备）和贮存核动力厂在运行过程中产生的放射性废物所需的设施，以及管理核动力厂在退役时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 必须确定核动力厂状态并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 核动力厂状态通常包括：

（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很低。

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危险导致的工况，详细说明其必需的能力、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。这些文件必须能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 必须使用系统化的方法确定一套全面的假设始发事件，以在设计中考虑所有可预见的具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，以表明已考虑所有可预见的事件。

5.1.4.3 假设始发事件必须包括在各种功率及停堆状态下，所有可预见的核动力厂构筑物、系统和部件失效、人员差错，以及内部和外部危险可能引起的失效。

5.1.4.4 必须对假设始发事件进行分析，以确定为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（按优先顺序）：

（1）依靠核动力厂的固有特性，使假设始发事件不会对安全产生重大影响，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，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，可借助为响应该事件而必须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，可借助执行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所有同类事件，并为安全重要物项的设计和运行限值提供基准。

5.1.4.7 在设计中从已确定的假设始发事件清单中排除某一假

设始发事件，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，可允许依靠手动启动系统或操纵员的其他动作。从探测到异常事件和事故到采取行动之间必须有足够的时间，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。必须对因操纵员错误操作或错误诊断而导致事故序列恶化的可能性作出评价。

5.1.4.10 如果假设始发事件发生后，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，同时设置适当的控制措施以便于设备的手动操作。

5.1.4.11 设计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减轻丧失控制的后果。

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 内部和外部危险

5.1.5.1 必须识别所有可预见的内部和外部危险，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

核动力厂布置的设计和确定有关的安全重要物项的设计中使用的假设始发事件及其产生的荷载时，都必须考虑内部和外部危险的影响。

5.1.5.2 设计和布置安全重要物项，必须考虑其安全重要性，使其能够承受内部和外部危险的影响，或防御内部和外部危险及其产生的共因失效，同时适当考虑对安全的其他影响。

5.1.5.3 对多机组厂址，设计必须适当考虑特定危险同时影响厂址上若干或所有机组的可能性。

5.1.5.4 设计必须适当考虑内部危险，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、以及来自破损系统或现场其他设施的流体释放。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 设计必须适当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）。在假定可能的危险时，必须考虑其发生的原因和可能性。在短期内，核动力厂的安全不能依赖于诸如电力供应和消防服务等厂外服务。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 必须采取措施，使得设计基准外部事件发生时，包含有安全重要物项（包括动力电缆和控制电缆）的厂房与其他核动力厂结构之间的相互影响最小。

5.1.5.7 核动力厂设计必须提供适当的裕量，在设计基准外部危险（由厂址危险性评价确定的）发生时保护安全重要物项，并避免产生陡边效应。

5.1.5.8 核动力厂设计还必须提供适当的裕量，在超设计基准自然灾害事件发生时，保护用于防止早期放射性释放或大量放射性释放所需的物项。

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，并必须使其符合核安全法规和相关的监管要求，以及经验证的工程实践，同时适当考虑其与核动力厂技术的相关性。

5.1.6.2 设计必须采用保证稳健性设计的方法，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 安全运行的运行限值和条件

5.1.7.1 设计必须为核动力厂安全运行确定一套运行限值和条件。

5.1.7.2 核动力厂设计中确定的要求，以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的水平；

（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制；

（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。

5.1.8 设计基准事故

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

5.1.8.2 必须使用设计基准事故来确定控制设计基准事故所必需的安全系统和其他安全重要物项的设计基准，包括性能准则等，目的是使核动力厂返回到安全状态和减轻事故后果。

5.1.8.3 针对设计基准事故工况，设计必须使核动力厂关键参数不超出规定的设计限值。基本目标是控制所有的设计基准事故以使厂内、外没有或仅有微小的放射性后果，并且无需采取任何场外防护行动。

5.1.8.4 必须用保守的方法来分析设计基准事故。该方法包括在分析中假定安全系统的某些故障模式，规定设计准则，采用保守的假设、模型和输入参数等。

5.1.9 设计扩展工况

5.1.9.1 必须在工程判断、确定论和概率论评价的基础上得出一套设计扩展工况，目的是增强核动力厂应对比设计基准事故更严重的或包含多重故障的事故的承受能力，避免不可接受的放射性后果，以进一步改进核动力厂的安全性。设计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。

5.1.9.2 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预防核动力厂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。这可能会要求增设附加的用于设计扩展工况的安全设施，或扩展安全系统的能力，来预防严重事故的发生或减轻严重事故的后果，或保持安全壳的完整性。这些附加的用于设计扩展工况的安全设施或能力扩展的安全系统，必须保证具有控制事故工况的能力，这些事故工况可能导致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）。必须保证核动力厂能进入可控状态并维持安全壳功能，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。

5.1.9.3 必须使用设计扩展工况来确定安全设施和其他安全重要物项的设计规格书，这些设施和物项用于预防此类工况的发生或在此类工况发生后用于控制和减轻其后果。

5.1.9.4 所开展的分析必须包括确定用于或能够预防设计扩展工况并减轻其后果的设施。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。

5.1.9.5 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。

5.1.9.6 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。

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

5.1.10 事件组合

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。这种继发效应应视为初始假设始发事件的一部分。

5.1.11 商用飞机的恶意撞击

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

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

5.1.11.3 可根据核动力厂所处的地形条件和厂房布置，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商

用飞机撞击的措施。

5.1.11.4 评价结果应表明，设计可以维持反应堆堆芯的冷却或安全壳的完整性，以及乏燃料的冷却或乏燃料水池的完整性。

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 在核动力厂安全系统中相互冗余的设备（包括电缆和电缆管道）必须易于识别。

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的方法，必须主要基于确定论方法，并适当辅以概率论方法。使用概率论方法时，应考虑以下因素：

（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）假设始发事件发生后，需要该物项执行某一安全功能的时刻或持续时间。

5.3.3 设计必须防止物项之间的相互影响，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，从而

保证安全功能的执行。

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，必须保证设备可鉴定、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

设备的设计必须适当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 不符合单一故障准则的情况必须是极个别的，并必须在安全分析中明确证明是正当的。

5.4.5.4 设计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，并保持其功能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任一失效，同时影响安全系统的多重部件或执行多样化安全功能的安全系统。

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 设计应保证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，以在设计基准规定的所有条件下保证其执行功能的能力并保持功能的完整性。

5.5.1.2 核动力厂布置必须便于执行标定、试验、维护、修理或更换、检查和监测等活动。这些活动能够按照相关的规范和标准执行，并必须与所执行的安全功能的重要性相一致，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。设计必须考虑在停堆期间执行安全重要物项标定、试验、维护、修理、更换或检查的有关措施，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，必须采取下列方法以说明其正当性：

（1）指定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，以应对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，这些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、温度）引起的老化效应。对于易遭受到外部自然事件的影响并需要在这种事件中及事件后执行其安全功能的安全重要物项，鉴定程序必须通过试验、分析或者两者的结合的方式，尽可能地复现安全重要物项所经受的工况。

5.5.2.4 在鉴定程序中必须考虑合理可预计的环境条件，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。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。设计必须提供适当的裕度，以考虑有关老化、中子辐照脆化和磨损机理，以及与服役年限有关的性能劣化的可能性，从而保证安全重要物项在其整个设计寿期内执行所必需的安全功能的能力。

5.5.3.2 必须考虑到在所有正常运行状态，包括试验、维修和维修停役，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期到的行为或性能劣化。

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系统地考虑人因（包括人机接口），并贯彻于设计全过程。

5.6.1.2 必须规定运行人员的最低配置，以满足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 应尽实际可能地促使有类似核动力厂运行经验的运行人员积极参与设计过程，以保证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，并必须限制操作差错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、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。向操纵员提供的用于决策和行动所需的信息必须简洁明了且无歧义。

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在需要时自动触发，且

相关系统按预期要求执行功能；

（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，并必须证明操纵员有足够的时间作出决策和采取行动。

5.6.1.9 设计必须能够保证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），以确认操纵员确需采取的动作，并确认这些动作能够正确执行。

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，设计应适当考虑允许多机组核动力厂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

核动力厂中所有可能含有易裂变或放射性物质的系统的设计，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；保证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；便于减轻事故的放射性后果。

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 核动力厂内必须设置足够数量的撤离路线。这些路线必须具有持久醒目的标识，并配备可靠的应急照明、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 设计中考虑的内、外部事件或多个事件的组合发生后，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 必须设置适当的警报系统和通信手段，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，以及与相关场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 必须适当布置各种构筑物，使核动力厂与其周围环境隔离，并控制核动力厂的出入口。

5.7.6.2 必须在厂房设计和厂区布置时，采取必要的措施控制运行人员和（或）设备（包括应急响应人员和车辆）进出核动力厂，并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 防止擅自接近或干扰安全重要物项

必须防止未经批准接近或干扰安全重要物项，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 如果存在要求核动力厂安全重要系统同时运行的情况，必须评价其可能的不利相互作用，并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，或必须采取措施防止在较低压力下运行的系统出现超出其设计压力的情况。

5.7.9 电网对核动力厂的影响

核动力厂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 必须对核动力厂的设计进行安全分析，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在核动力厂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，以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批准的排放限值和剂量限值，并能够满足事故工况下的可接受限值。

5.8.1.3 安全分析必须保证在核动力厂设计中已实施纵深防御。

5.8.1.4 安全分析必须保证在核动力厂设计中适当考虑了不确定性。尤其是应有适当的裕量，以避免出现陡边效应以及早期放射性释放或大量放射性释放。

5.8.1.5 必须基于当前状态或竣工状态，更新和验证核动力厂

设计中所采用的各项分析假设、方法的适用性和保守程度。

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序列，以确认鉴定要求；

（4）将分析结果与验收准则、设计限值、剂量限值以及可接受限值进行比较，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

设计必须适当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，且纵深防御的各层次应尽实际可能独立；

（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

设计必须使核动力厂燃料元件和燃料组件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，能够承受预期的堆内辐照和环境条件。

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）燃料元件内裂变产物叠加氦气导致的附加内压；

（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。

设计必须为数据、计算和制造中的不确定性因素留有裕量。

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

在运行工况以及除严重事故外的其他事故工况下，设计必须使核动力厂燃料元件和燃料组件及其支撑件能够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（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超过设计限值的部位。

6.1.3.3 反应性控制装置的设计，必须适当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）

或可能引起共因故障的故障。

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 即使在堆芯处于反应性最大的状态下，必须至少有一个系统能够独立地以足够的深度和高可靠性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、换料操作期间或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的意外临界。

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所规定的状态。

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，并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保证避免使反应堆冷却

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 必须使反应堆冷却剂压力边界内部件（如泵的叶轮和阀门部件）的设计，在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

必须采取措施保证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，以在核动力厂任何运行状态下（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 必须在核动力厂内设置适当的设施，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源自燃料的裂变产物）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和保守的裕量，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

在核动力厂停堆状态下，必须为排出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），能够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保证：

（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）及考虑适当的多重性和多样性，以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 在核动力厂所有状态下，都必须保证具有将热量传输到最终热阱的能力。

6.2.7.2 在必须由热量传输系统实现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 在比设计基准自然灾害（由厂址危险性评价确定的）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 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）保护反应堆使其免受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的水平，在运行状态下不高于监管排放限值，以及在事故工况下满足可接受的限值。

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，在安全壳的所有贯穿件安装完成后和在核动力厂运行寿期内，必须能够进行泄漏率试验，并在安全壳的设计压力下能够进行泄漏率试验。

6.3.2.3 安全壳贯穿件的数量必须保持尽实际可能的少，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，使其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 在依靠安全壳密封性，防止放射性物质向环境的释放超过可接受限值的事故中，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每根管线，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止回阀，并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，安全壳隔离阀或止回阀必须尽实际可能地靠近安全壳，每个阀门能够可靠和独立地动作及进行定期试验。如采取其他的设置方式则应论证其满足设计要求。

6.3.3.3 对于仪表管线等特定类别的管线，或在应用第 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，但既非反应堆冷却剂压力边界的组成部分，又不直接与安全壳内大气相通的管线，必须至少设置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侧，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 运行人员必须通过若干道气封闸门进入核动力厂安全壳。这些闸门是联锁的，以保证反应堆功率运行和事故工况期间，至少有一道闸门是关闭的。

6.3.4.2 当运行人员出于监督目的进入安全壳时，设计必须采取特定措施，以保证运行人员的防护和安全。如果有设备气密闸门，设计中也必须采取措施，以保证运行人员的防护和安全。

6.3.4.3 贯穿安全壳的设备或材料运输闸门的设计，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，控制裂变产物或其他气态、液态或固态物质的任何积累，这些物质可能在安全壳内释放并可能影响安全重要系统运行。

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，必须能够保证在事故工况压力平衡期间产生的压力差，不会对承压结构或减轻事故工况后果的重要系统造成不可接受的损坏。

6.3.5.3 必须保证安全壳的排热能力，以在发生任何高能流体意外释放事故后，能够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，以保证排热功能得到实现。

6.3.5.4 必须采取设计措施以防止在核动力厂所有状态下丧失安全壳结构的完整性。该措施必须不会导致早期放射性释放或大量放射性释放。

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

6.3.5.6 必要时，必须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）控制事故工况下安全壳大气中的氢气、氧气和其他物质的浓度，以防止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，并必须明确规定其使用方法，以保证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，以保证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从设计预期释放位置外逸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

必须设置适当且可靠的控制系统，使得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 必须设置能够探测不安全状态并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）必须能够执行用于启动安全系统的各种安全动作，以在预计运行事件或事故工况开始后的合理时间范围内无需操纵员干预；

（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的条件，包括各通道分别进行试验的可能性，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 设计应考虑，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，在此期间应采取适当的措施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，必须确定或制定用于开发和测试/验证计算机软、硬件的适当的标准和规范，并在整个寿期内执行，特别是在软件开发过程中应执行这些标准和规范。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，且不能高置信度的证明设备具有必要的高可靠性时，必须提供多样化手段以保证安全功能的执行；

（5）必须考虑由软件引起的共因故障；

（6）必须提供防止系统运行意外中断或受到蓄意干扰的保护措施。

6.4.6 保护系统和控制系统的分隔

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

6.4.6.2 如果保护系统和控制系统共用信号，必须保证适当的分隔措施（如有效的去耦），且信号系统必须按照属于保护系统的一部分来分级。

6.4.7 控制室

6.4.7.1 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，以使核动力厂保持在安全状态或回到安全状态。

6.4.7.2 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、易爆或有毒气体的危害。

6.4.7.3 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。

6.4.7.4 控制室设计必须提供恰当的裕量，以应对比设计中考

虑的自然灾害水平（由厂址危险性评价确定的）更为严重的自然灾害。

6.4.7.5 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。

6.4.8 辅助控制室

6.4.8.1 必须在核动力厂内与控制室实体分隔、电气隔离和功能隔离的一个独立地点设置辅助控制室，并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，排出余热以及监测核动力厂的重要参数。

6.4.8.2 第 6.4.7.2 中的相关要求，如果适当也可用于核动力厂辅助控制室。

6.5 场内应急设施

6.5.1 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。

6.5.2 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。每个应急设施应适当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通信手段。

6.6 应急动力供应

6.6.1 应对丧失场外电源的设计

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

6.6.1.2 核动力厂应急动力源、替代动力源的设计，必须包括能力、可用性、持续时间、容量和持续性等方面的要求。

6.6.1.3 用于提供应急动力的综合手段（如柴油机、蓄电池、水轮机、汽轮机或燃气轮机），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。

6.6.1.4 在同时丧失场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。

6.6.1.5 用于减轻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。

6.6.1.6 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。

6.6.1.7 在交流电源丧失的情况下，应保证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。

6.6.1.8 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。

6.6.1.9 设计也应包含通过一些移动设备的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。

6.7 支持系统和辅助系统

6.7.1 热传输系统

6.7.1.1 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的热量。

6.7.1.2 热传输系统的设计必须保证其非关键部分能够被隔离。

6.7.2 工艺取样系统和事故后取样系统

6.7.2.1 必须设计工艺取样系统和事故后取样系统，以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。

6.7.2.2 必须在核动力厂内提供适当的手段，以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。

6.7.3 压缩空气系统

必须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。

6.7.4 空调系统和通风系统

6.7.4.1 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。

6.7.4.2 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，以便：

（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的原则；

（4）在不影响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，保持在规定限值之内，并可合理达到的尽量低。

6.7.4.3 核动力厂内污染较高的区域与污染较低的区域和其他可进入的区域之间，必须维持适当的负压差。

6.7.5 消防系统

6.7.5.1 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、防火封隔屏障以及烟雾控制系统。

6.7.5.2 安装的消防系统应能安全地处理各种类型假设火灾事

件。

6.7.5.3 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。

6.7.5.4 火灾探测系统必须能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。

6.7.5.5 应对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。

6.7.5.6 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。

6.7.6 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。

6.7.7 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）在有安全重要物项的区域使用的起重设备，需要进行抗震鉴定。

6.8 其他动力转换系统

6.8.1 蒸汽供应系统、给水系统和汽轮发电机

6.8.1.1 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保证在运行状态或事故工况下，反应堆冷却剂压力边界不超过设计限值。

6.8.1.2 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。

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

6.8.1.4 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。

6.9 放射性废物处理和流出物排放

6.9.1 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。

6.9.2 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，该期限应与相应的废物处置方案相适应。

6.9.3 核动力厂必须具备适当设施，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以及吊装和包装的能力。

6.9.4 核动力厂必须具备适当手段，以控制液态和气态流出物向环境的排放保持在规定限值以内，并可合理达到的尽量低。

6.9.5 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，并能更换滤芯且同时保持通风量。

6.10 燃料装卸和贮存系统

6.10.1 必须在核动力厂建立燃料装卸和贮存系统，以保证在燃料装卸和贮存期间始终保持燃料的完整性和特性。

6.10.2 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。

6.10.3 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。

6.10.4 燃料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，保证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）能够识别每个燃料组件；

（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材料衡算控制，以防止核燃料丢失或丧失对核燃料的控制。

6.10.5 已辐照燃料的装卸和贮存系统的设计还必须：

（1）允许在运行状态和事故工况下充分地排出燃料的热量；

（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的燃料元件或燃料组件；

（5）可溶中子吸收材料在用于临界安全时应控制其浓度水平；

（6）燃料装卸和贮存设施应便于维修和退役；

（7）必要时燃料装卸和贮存区域和设备应便于去污；

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

（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。

6.10.6 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，实际消除导致早期放射性释放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。

设计还必须包括能够使用移动设备进行补水，以保证水池有足够的水量来长期冷却乏燃料和辐射屏蔽。

6.10.7 设计必须包括：

（1）在运行状态和与乏燃料水池有关的事故工况下，具有监测和控制乏燃料水池池水温度和水位的手段；

（2）在运行状态下具有监测和控制乏燃料水池池水和空气放射性活度的手段，并在与乏燃料水池有关的事故工况下具有监测乏燃料水池池水和空气放射性活度的手段；

（3）在运行状态下具有监测和控制乏燃料水池水化学的手段。

6.11 辐射防护

6.11.1 辐射防护设计

6.11.1.1 必须采取措施保证核动力厂的工作人员接受的剂量不超过规定限值，并保持在可合理达到的尽量低的水平，并考虑相关的剂量约束。

6.11.1.2 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辐射风险保持在可合理达到的尽量低的水平，维持燃料元件包壳的完整性，控制腐蚀产物和活化产物的产生和迁移。

6.11.1.3 在合理可实施的情况下，用于制造构筑物、系统和部件的材料应选用不易辐照活化的材料。

6.11.1.4 必须采取措施防止来自核动力厂各种放射性物质、放

射性废物和污染的释放或扩散。

6.11.1.5 核动力厂的布置必须保证存在辐射危害和可能放射性污染区域的出入得到有效控制，并通过出入控制和通风的方式防止或减少运行人员所受的辐射照射和污染。

6.11.1.6 核动力厂的布置必须尽量减少运行人员在正常运行、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。

6.11.1.7 应根据在运行状态（包括换料、维修和检查）下区域的预期停留时间、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。通过屏蔽设计防止或降低辐射照射。

6.11.1.8 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。

6.11.1.9 必须为运行人员和核动力厂设备提供合适的去污设施。

6.11.2 辐射监测

6.11.2.1 必须设置相应的辐射监测设备，以保证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，以及在设计扩展工况下提供尽实际可行的辐射监测。

6.11.2.2 必须提供固定式剂量率仪表，在运行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，监测辐射剂量率。

6.11.2.3 必须在适当的地点安装固定式剂量率仪表，以反映在事故工况下核动力厂的总体辐射水平。在主控室或运行人员能够采取纠正行动的适当控制位置，固定式剂量率仪表必须给出充分的信息。

6.11.2.4 必须安装固定式监测设备，在运行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，测量空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。

6.11.2.5 必须设置固定式设备和实验室设施，在运行状态和事故工况下流体工艺系统中，及时测定选定放射性核素的浓度，以及在核动力厂系统或环境中采集的气体和液体样品中，及时测定选定放射性核素的浓度。

6.11.2.6 必须设置固定式设备，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的活度浓度。

6.11.2.7 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（如门式辐射监测仪、手足监测仪），以监测运行人员和设备。

6.11.2.8 必须设置用于测量运行人员所受照射和污染的设施。必须制定用于评定和记录工作人员随时间所受累积剂量的程序。

6.11.2.9 必须根据核动力厂周围区域剂量率或放射性浓度的环境监测，对照射和其他辐射影响的评价作出安排，特别是：

（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：

实际消除

如果该工况实质上不可能发生或高置信度极不可能发生，则认为该工况被实际消除。

能动部件

依靠触发、机械运动或动力源等外部输入而行使功能的部件。

共因故障

由特定的单一事件或起因导致两个或多个构筑物、系统或部件失效的故障。

多样性

为执行某一确定功能设置两个或多个独立（或冗余）的系统或部件，这些不同的系统或部件具有不同的属性，从而减少了共因故障（包括共模故障）的可能性。

功能隔离

防止一个线路或一个系统的运行模式或故障对另一个线路或系统造成有害后果。

安全重要物项

属于某一安全组合的一部分，其失效或故障可能导致对厂区人员或公众的辐射照射的物项。

非能动部件

不依靠触发、机械运动或动力源等外部输入而行使功能的部件。

实体隔离

由几何分隔（距离、方位等）、适当的屏障或二者结合形成的隔离。

事故管理

在超设计基准事故*发展过程中所采取的一系列行动：

（1）防止事件升级为严重事故；

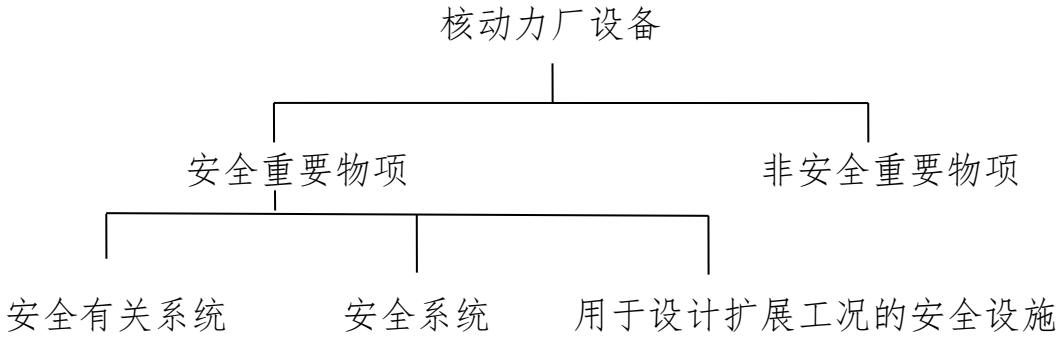
（2）减轻严重事故的后果；

（3）实现长期稳定的安全状态。

为了减轻严重事故后果的事故管理也称严重事故管理。

*超设计基准事故是指假定的比设计基准事故的事故工况更为严重的事故。

核动力厂设备



预计运行事件

在核动力厂运行寿期内预计至少发生一次的偏离正常运行的各种运行过程；由于设计中已采取相应措施，这类事件不至于引起安全重要物项的严重损坏，也不至于导致事故工况。

正常运行

核动力厂在规定的运行限值和条件范围内的运行。

运行状态

正常运行和预计运行事件两类状态的统称。

严重事故

严重性超过设计基准事故并造成堆芯明显恶化的事故工况。

假设始发事件

设计期间确定的可能导致预计运行事件或事故工况的假设事件。

保护系统

监测反应堆的运行，并根据探测到的异常工况信号，自动触发动作以防止发生不安全或潜在的不安全工况的系统。

安全功能

为了保证设施或活动能够预防和缓解核动力厂正常运行、预计运行瞬态和事故工况下的放射性后果，保证安全而必须达到的特定目的。

安全组合

用于完成某一特定假设始发事件下所必需的各种动作的设备组合，其使命是防止预计运行事件和设计基准事故的后果超过设计基准中的规定限值。

安全系统

安全上重要的系统，用于保证反应堆安全停堆、从堆芯排出余热或限制预计运行事件和设计基准事故的后果。

单一故障

导致单一系统或部件不能执行其预定安全功能的一种故障，以及由此引起的各种继发故障。

最终热阱

即使所有其他的排热手段已经丧失或不足以排出热量时，总是

能够接受核动力厂所排出余热的一种介质。这种介质通常是水体或大气。

可控状态

一种核动力厂状态，即在发生预计运行事件或事故工况后，核动力厂能够保证并维持基本安全功能，以便有足够的时间采取有效措施使其达到安全状态。

设计中考虑的核动力厂状态

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	没有造成堆芯明显损伤	堆芯熔化（严重事故）

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

导致核动力厂事故工况的假设事故，这些事故的放射性物质释放在可接受限值以内，该核动力厂是按确定的设计准则和保守的方法来设计的。

设计扩展工况

不在设计基准事故考虑范围的事故工况，在设计过程中应该按最佳估算方法加以考虑，并且该事故工况的放射性物质释放在可接受限值以内。设计扩展工况包括没有造成堆芯明显损伤的工况和堆芯熔化（严重事故）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，并能够保证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设计基准事故时启动有关自动保护装置的触发点。

陡边效应

在核动力厂中，由微小变化的输入引发核动力厂状态的重大突变。例如，由参数微小的偏离导致核动力厂从一种状态突变到另一种状态的严重异常行为。

原动机

可由驱动装置驱动，将能量转化为动力的部件（如发动机、电磁操作器或气动操作器）。

大量放射性释放

需要厂外防护行动，但是这些行动受到时间长度和使用区域的限制，从而不足以保护人员和环境而导致的放射性释放。

早期放射性释放

必要的场外防护行动在预期时间内不可能全面有效执行的放射性释放。