HAF102

核动力厂设计安全规定

（2004 年 4 月 18 日国家核安全局批准发布，2004 年修改）

本规定自 2004 年 4 月 18 日起实施

本规定由国家核安全局负责解释

1 引 言

1.1 目的

本规定提出了陆上固定式热中子反应堆核动力厂的核安全原则，确定了保证核安全所必需的基本要求。这些要求适用于核动力厂安全功能及相关的构筑物、系统和部件，并适用于核动力厂中的安全重要规程。规定中只强调设计中必须满足的要求，对于如何满足这些要求则不作具体规定。

附件Ⅰ、Ⅱ与本规定具有同等法律效力。

附录Ⅰ是对本规定的说明和补充。

本规定适用于核动力厂设计、制造、建造、运行和监督管理。

1.2 范围

1.2.1 本规定阐述了安全重要构筑物、系统和部件为实现核动力厂的安全运行和防止或减轻可能危及安全的事件后果所必须满足的设计要求。本规定还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。这种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补的技术。这些分析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) 由人员行动引起；

(3) 直接与核动力厂及其环境有关。

1.2.2 本规定还涉及到极不可能发生的事件，例如可能导致大量放射性释放的严重事故，设计中对此类事件提供预防或缓解措施是适当的和可行的。

1.2.3 本规定不考虑下列事件：

(1) 极不可能发生的外部自然事件或人为事件(诸如陨石或人造卫星撞击）；

(2) 极不可能影响核动力厂安全的工业事故；

(3) 由核动力厂运行引起的非放射性影响。

1.2.4 本规定中的核动力厂主要系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。

本规定原则上也适用于其他类型的陆上固定式热中子反应堆核动力厂。

2 安全目标和纵深防御概念

2.1 安全目标

2.1.1 总的核安全目标：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、社会和环境免受危害。

2.1.2 总的核安全目标由辐射防护目标和技术安全目标所支持，这两个目标互相补充、相辅相成，技术措施与管理性和程序性措施一起保证对电离辐射危害的防御。

(1) 辐射防护目标：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合理可行尽量低，保证减轻任何事故的放射性后果。

(2) 技术安全目标:采取一切合理可行的措施防止核动力厂事故，并在一旦发生事故时减轻其后果；对于在设计该核动力厂时考虑过的所有可能事故，包括概率很低的事故，要以高可信度保证任何放射性后果尽可能小且低于规定限值；并保证有严重放射性后果的事故发生的概率极低。

2.1.3 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。辐射防护目标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,并且必须符合运行限值和辐射防护标准。

2.1.4 为了实现上述安全目标，在设计核动力厂时，要进行全面的安全分析，以便确定所有照射的来源，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(见4.4.1条）。此种安全分析要考察以下内容：(1)核动力厂所有计划的正常运行模式；(2)发生预计运行事件时核动力厂的性能；(3)设计基准事故；(4)可能导致严重事故的事件序列。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,验证安全系统和安全相关物项或系统的有效性，以及确定应急响应的要求。

2.1.5 尽管采取措施将所有运行状态下的辐射照射控制在合理可行尽量低,并将能导致辐射来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：专设安全设施、营运单位制定的厂内事故处理规程以及国家和地方有关部门制定的厂外干预措施。核动力厂的安全设计适用以下原则：能导致高辐射剂量或

大量放射性释放的核动力厂状态的发生概率极低；具有大的发生概率的核动力厂状态只有较小或者没有潜在的放射性后果。

2.2 纵深防御概念

2.2.1 纵深防御概念贯彻于安全有关的全部活动，包括与组织、人员行为或设计有关的方面，以保证这些活动均置于重叠措施的防御之下，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，以便对由厂内设备故障或人员活动及厂外事件等引起的各种瞬变、预计运行事件及事故提供多层次的保护。

2.2.2 纵深防御概念应用于核动力厂的设计，提供一系列多层次的防御（固有特性、设备及规程），用以防止事故并在未能防止事故时保证提供适当的保护。

(1) 第一层次防御的目的是防止偏离正常运行及防止系统失效。这一层次要求：按照恰当的质量水平和工程实践，例如多重性、独立性及多样性的应用，正确并保守地设计、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，并控制部件的制造和核动力厂的施工。能有利于减少内部灾害的可能、减轻特定假设始发事件的后果或减少事故序列之后可能的释放源项的设计措施均在这一层次的防御中起作用。还应重视涉及设计、制造、建造、在役检查、维修和试验的过程，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。整个过程是以确定核动力厂运行和维修要求的详细分析为基础。

(2) 第二层次防御的目的是检测和纠正偏离正常运行状态，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。这一层次要求设置在安全分析中确定的专用系统，并制定运行规程以防止或

尽量减小这些假设始发事件所造成的损害。

(3) 设置第三层次防御是基于以下假定：尽管极少可能，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，而演变成一种较严重的事件。这些不大可能的事件在核动力厂设计基准中是可预计的，并且必须通过固有安全特性、故障安全设计、附加的设备和规程来控制这些事件的后果，使核动力厂在这些事件后达到稳定的、可接受的状态。这就要求设置的专设安全设施能够将核动力厂首先引导到可控制状态，然后引导到安全停堆状态，并且至少维持一道包容放射性物质的屏障。

(4) 第四层次防御的目的是针对设计基准可能已被超过的严重事故的，并保证放射性释放保持在尽实际可能的低。这一层次最重要的目的是保护包容功能。除了事故管理规程之外，这可以由防止事故进展的补充措施与规程，以及减轻选定的严重事故后果的措施来达到。由包容提供的保护可用最佳估算方法来验证。

(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。这方面要求有适当装备的应急控制中心及厂内、厂外应急响应计划。

2.2.3 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，以包容规定区域的放射性物质。所必需的实体屏障的数目取决于可能的内部及外部灾害和故障的可能后果。就典型的水冷反应堆而言，这些屏障可能是燃料基体、燃料包壳、反应堆冷却剂系统压力边界和安全壳。

3 安全管理要求

3.1 管理职责

营运单位对安全负全面责任。但是，所有从事安全重要活动的单位，都有责任保证将安全事务放在最优先的位置。设计单位必须保证核动力厂设计满足营运单位的要求，包括用户[①]的标准化要求；保证设计考虑了安全方面的最新进展；保证设计与设计规格书和安全分析一致；保证设计满足国家有关监管要求；保证设计满足有效的质量保证大纲的各项要求；并保证正确地考虑了任何设计变更的安全性。为此，设计单位必须遵循下述要求：

(1) 明确划分职责以及相应的权限范围与联系渠道；

(2) 保证它在所有层次上都拥有足够的技术上合格且受过适当培训的人员；

(3) 明确地规定负责设计的不同部分的各个小组之间的接口，并明确设计单位、用户、设备供应厂商、建造单位和其他承包单位之间恰当的接口；

(4) 制定并严格遵守完备的程序；

(5) 定期审查、监督和监查一切与安全有关的设计事务；

(6) 保证保持良好的安全文化水平。

3.2 设计管理

3.2.1 核动力厂设计管理必须保证安全重要构筑物、系统和部件有合适的性能、技术规范和材料成份，使得安全功能得到执行，并使核动力厂在其整个设计寿命期间能够安全运行和具有必要的可靠性，且能防止事故的发生和把保护厂区人员、公众和环境作为首要任务。

[①] 这里用户系指营运单位、电力公司和供热公司等。

3.2.2 设计管理必须保证满足营运单位的要求，并对营运单位人员的能力和局限性给予适当的考虑。设计单位必须提供充分的安全设计资料，以保证核动力厂的安全运行、维修和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（即运行限值和条件）的实践。

3.2.3 设计管理必须考虑确定论安全分析和补充性的概率论安全分析的结果，并通过合适的迭代过程以保证适当考虑防止事故的发生及减轻其后果。

3.2.4 设计管理必须保证采用合适的设计措施以及运行与退役实践，使产生的放射性废物的活度和体积保持尽可能的小。

3.3 经验证的工程实践

3.3.1 只要可能，安全重要构筑物、系统和部件就必须按照经批准的最新的或当前适用的规范和标准进行设计；其设计必须是此前在相当使用条件下验证过的；并且这些物项的选择必须与安全所要求的核动力厂可靠性目标相一致。对于用作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，以保证最后的质量与所需的安全功能相适应。

3.3.2 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，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。这种开发性工作必须在投入使用前经过充分的试验，并在使用中进行监测，以便验证已达到了预期效果。

3.3.3 选择设备时必须考虑到误动作和不安全的故障模式（例如要求脱扣时不能脱扣）。对构筑物、系统和部件预期会发生故障并需采取设计措施的地方，必须优先选择具有可预见的和已揭示的故障模式的且便于修理或更换的设备。

3.4 运行经验和安全研究

设计必须充分考虑从运行的核动力厂中取得的相关运行经验和相关研究的成果。

3.5 安全评价

3.5.1 必须进行全面的安全评价，以证实交付制造、建造和竣工的设计满足设计过程开始时提出的安全要求。

3.5.2 安全评价必须成为设计过程的一部分，同时在设计和证实性分析活动之间存在迭代过程，而且随着设计计划的进展其范围不断扩大和详细程度不断提高。

3.5.3 安全评价必须基于安全分析得到的数据、以往的运行经验、支持性研究的成果，以及经验证的工程实践。

3.6 安全评价的独立验证

在提交国家核安全监管部门以前，营运单位必须保证由未参与相关设计的个人或团体对安全评价进行独立验证。

3.7 质量保证

3.7.1 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。这个大纲必须由每个构筑物、系统和部件的更详细计划来支持，以便始终保证设计质量。

3.7.2 设计，包括后来的变更或安全的改进，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。

3.7.3 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或核实。验证、确认和批准必须在做施工设计之前完成。

4　主要技术要求

4.1 纵深防御要求

4.1.1 第 2 章中所描述的纵深防御概念必须在设计过程中加以体现：

(1) 设计必须提供多重的实体屏障，防止放射性物质不受控制地释放到环境；

(2) 设计必须是保守的，建造必须是高质量的，从而为使核动力厂的故障和偏离正常运行减至最少并为防止事故提供了可信度；

(3) 设计必须利用固有特性和专设设施在发生假设始发事件期间及之后控制核动力厂的行为，即必须通过设计尽可能地使不受控制的瞬变过程减至最少甚至排除；

(4) 设计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，以便在假设始发事件的早期阶段尽量减少操纵员的动作，附加控制包括操纵员的动作；

(5) 设计必须尽实际可能提供控制事故过程和限制其后果的设备和规程；

(6) 设计必须提供多种手段来保证实现每项基本安全功能，即控制反应性、排出热量和包容放射性物质，从而保证各道屏障的有效性和减轻任何假设始发事件的后果。

4.1.2 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) 屏障在需要它发挥作用时失效；

(3) 一道屏障因另一道屏障的失效而失效。

4.1.3 除极不可能的假设始发事件外，设计必须使第一层次至多第二层次防御能够阻止所有假设始发事件升级为事故工况。

4.1.4 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是继续进行功率运行的充分条件。虽然对于除功率运行以外的各种运行模式来说，可视情况规定某些放松条件，但在功率运行下所有各层次防御都必须总是可用的。

4.2 安全功能

4.2.1 整个安全措施的目标必须是：提供充分的手段使核动力厂保持正常的运行状态；保证发生假设始发事件之后立即作出正确的短期响应；以及发生任何设计基准事故期间和之后及发生那些所选定的超设计基准事故的事故工况之后便于对核动力厂进行管理。

4.2.2 为了保证安全，在各种运行状态下、在发生设计基准事故期间和之后，以及尽实际可能在发生所选定的超设计基准事故的事故工况下，都必须执行下列基本安全功能：

(1) 控制反应性；

(2) 排出堆芯热量；

(3) 包容放射性物质和控制运行排放，以及限制事故释放。

这三项基本安全功能进一步详细划分的实例见附录Ⅰ。

4.2.3 必须用全面的、系统的方法来确定在发生假设始发事件后的各个时期中完成这些安全功能所必需的构筑物、系统和部件。

4.3 事故预防和核动力厂安全特性

核动力厂设计必须使其对假设始发事件的敏感性减到最小。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（以重要性为序）：

(1) 依靠核动力厂的固有特性，使假设始发事件不会产生与安全有关的重大影响，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，核动力厂借助非能动安全设施或

在此状态下连续运行的安全系统的作用，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。

4.4 辐射防护和验收准则

4.4.1 为了在设计核动力厂时实现 2.1.1—2.1.2 条中给出的安全目标，必须逐一确定并适当考虑所有现实的和潜在的辐射来源，并必须采取措施，保证这些辐射来源保持在严格的技术和管理控制之下。

4.4.2 必须采取措施保证实现 2.1.2 条中给出的辐射防护目标和技术安全目标，并保证公众和厂区人员在包括维修和退役的所有运行状态下受到的辐射剂量不超过规定限值并且合理可行尽量低。

4.4.3 设计必须以防止或减轻（在无法防止时）由设计基准事故和选定的严重事故引起的辐射照射作为目标。设计必须采取措施保证公众和厂区人员可能受到的辐射剂量不超过可接受限值并且合理可行尽量低。

4.4.4 必须将有可能导致高辐射剂量或放射性释放的核动力厂状态发生的概率限制在很低的水平，并必须保证发生概率高的核动力厂状态仅产生微小的潜在放射性后果。必须以这些要求为基础，规定核动力厂设计的放射性验收准则。

4.4.5 通常有为数有限的几组放射性验收准则，并与核动力厂不同的状态相对应。这些核动力厂状态一般包括：正常运行、预计运行事件、设计基准事故和严重事故。这几种状态的放射性验收准则，作为一个最低的安全水平，必须满足国家核安全

监管部门的要求。

5 核动力厂设计要求

5.1 安全分级

5.1.1 必须首先确定属于安全重要物项的所有构筑物、系统和部件，包括仪表和控制软件，然后根据其安全功能和安全重要性分级。它们的设计、建造和维修必须使其质量和可靠性与这种分级相适应。

5.1.2 划分某一构筑物、系统或部件安全重要性的方法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，同时考虑如下因素：

(1) 该物项要执行的安全功能；

(2) 未能执行其功能的后果；

(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。

5.1.3 必须在不同级别的构筑物、系统和部件之间提供合适的接口设计，以保证划分为较低级别的系统中的任何故障不会蔓延到划分为较高级别的系统。

5.2 总的设计基准

5.2.1 概述

5.2.1.1 设计基准必须规定核动力厂的必备能力，以适应在规定的辐射防护要求范围内所确定的运行状态和设计基准事故。设计基准必须包括正常运行技术规格、假设始发事件造成的核动力厂状态、安全分级、重要假设，以及在某些情况下特定的分析方法。

5.2.1.2 在正常运行、预计运行事件和设计基准事故的设计基准中，必须采用保守的设计措施和良好的工程实践，以保障不会发生反应堆堆芯的任何重大损坏；辐射剂量保持在规定限值内，并合理可行尽量低。

5.2.1.3 除设计基准外，设计中还必须考虑核动力厂在特定的超设计基准事故包括选定的严重事故中的行为。这些评价所使用的假设和方法可以最佳估算为基础。

5.2.2 核动力厂状态分类

必须确定核动力厂状态并按其发生的概率分成几类。这些类别通常包括正常运行、预计运行事件、设计基准事故和严重事故。必须为每个类别确定验收准则，并且这些准则考虑到如下要求：频繁发生的假设始发事件必须仅有微小的或根本没有放射性的后果，而可能导致严重后果的事件的发生概率必须很低。

5.2.3 假设始发事件

设计核动力厂时，必须认识到纵深防御的各层次都可能受到考验，因而必须提供设计措施，以保证完成所需的安全功能和满足安全目标。这些考验来源于假设始发事件，这些事件是根据确定论方法或概率论方法或这两者的组合选定的。在设计中通常不考虑概率很低的各种独立事件同时发生。

5.2.4 内部事件

必须分析假设始发事件（见附件Ⅰ），以便确定所有可能影响核动力厂安全的内部事件。这些事件可能包括设备故障或误操作。

5.2.4.1 火灾和爆炸

设计和布置安全重要构筑物、系统和部件时，除满足其他安全要求外，还必须尽量降低外部或内部事件引发火灾和爆炸的可能性及其后果。必须保持停堆、排出余热、包容放射性物质和监测核动力厂状态的能力。为满足这些要求，必须通过采

用多重部件、多样系统、实体分隔和故障安全设计的适当组合，以便实现下述目标：

(1) 防止火灾发生；

(2) 及时探测发生的火灾并迅速灭火，以限制火灾后果；

(3) 防止未扑灭的火势蔓延，以使其对核动力厂重要功能的影响减至最小。

必须进行核动力厂火灾危害性分析，以确定所需的防火屏障耐火能力，并且提供必要能力的火灾探测系统和灭火系统。

必要时，灭火系统必须能自动启动，系统的设计和布置必须保证在其出现破裂、误动作或意外操作时不至于显著损害安全重要构筑物、系统和部件的功能，并不会同时影响多重安全组合而使为满足单一故障准则所采取的措施变得无效。

在整个核动力厂中，尤其是在诸如安全壳和控制室等场所中，只要可行，必须采用不可燃的或阻燃的和耐热的材料。

5.2.4.2 其他内部灾害

核动力厂设计必须考虑发生诸如以下内部灾害的可能性：内部水淹、飞射物、管道甩动、喷射流冲击或者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，以保证核安全不受到损害。一些外部事件可能引发内部火灾或水灾和可能导致飞射物的产生。适当时，也必须在设计中考虑这种外部和内部事件的相互影响。

如果不同压力下运行的两个流体系统是相互连接的，那么这两个系统或者都必须按较高的压力设计，或者必须采取措施，防止发生单一故障时在较低压力下运行的系统超过设计压力。

5.2.5 外部事件

5.2.5.1 必须针对计划的厂址和核动力厂的组合确定作为设计基准的外部自然事件和外部人为事件。必须考虑所有那些可能造成重大放射性风险的事件。必须组合使用确定论方法和概率

论方法来选定核动力厂设计应承受的一组外部事件，并确定设计基准。

5.2.5.2 必须考虑的外部自然事件包括在描述厂址特征时已确定的那些事件，如地震、洪水、狂风、龙卷风、海啸（潮汐波）和极端气象条件。必须考虑的外部人为事件包括描述厂址特征时已确定的那些事件和由此导出设计基准的事件。在设计过程初期必须重新评价这些事件清单的完整性。

5.2.6 厂址特征

5.2.6.1 在确定核动力厂设计基准时，必须考虑核动力厂与环境之间的各种相互作用，包括人口、气象、水文、地质和地震等因素。还必须考虑核动力厂安全和保护公众可能依赖的电力供应和消防服务之类的厂外服务的可用性。

5.2.6.2 必须对在热带、干旱或火山附近地区选址的核动力厂项目进行专门评价，以确定因该厂址的特征可能需要的特殊设计设施。

5.2.7 事件的组合

若随机发生的单个事件的组合能可信地导致预计运行事件或事故工况，则必须在设计中考虑到这种组合。某些事件可能是其他事件的后果，如地震后发生水灾。这种随之发生的效应必须视为原假设始发事件的一部分。

5.2.8 设计规范

5.2.8.1 必须规定构筑物、系统和部件的工程设计规范，并且必须使其符合国家有关监管机构认可的合适的国家标准和工程实践（见 3.3 条），或国际上使用的、其使用是合适的、而且是国家有关监管机构认可的标准或实践。

5.2.8.2 核动力厂的抗震设计必须提供充分的安全裕度，以抵御地震事件的影响。

5.2.9 设计限值

必须为各种运行状态和设计基准事故规定一套与每个构筑物、系统或部件的主要物理参数相适应的设计限值。

5.2.10 运行状态

5.2.10.1 核动力厂必须设计成能够在规定的各种参数（例如压力、温度和功率参数）范围内安全运行，并且最低限度必须有一套特定的安全系统辅助设施（例如辅助给水能力和应急电源）是可用的。核动力厂的设计必须是，对范围广泛的预计运行事件的响应允许核动力厂安全运行或必要时停堆，不必采取超出纵深防御第一层次或至多不超出第二层次的措施。

5.2.10.2 在诸如启动、换料和维修之类的低功率和停堆状态下，安全系统的可用性可能降低，在设计中必须考虑此时发生事故的可能性，并且必须规定对安全系统不可用性的适当限制。

5.2.10.3 设计过程中必须针对核动力厂安全运行的要求，制定一组运行要求和限制，包括：

(1) 安全系统整定值；

(2) 工艺变量和其他重要参数的控制系统和过程限制；

(3) 为保证各构筑物、系统和部件执行设计中预定的功能，对核动力厂规定维修、试验和检查的要求，并考虑合理可行尽量低的辐射防护原则；

(4) 明确地规定运行配置，包括安全系统停役情况下的运行限制。

5.2.10.4 这些要求和限制必须是营运单位制定核动力厂的运行限值和条件的依据，在这种条件下，营运单位将获准运行核动力厂。

5.2.11 设计基准事故

5.2.11.1 必须根据假设始发事件（见附件Ⅰ）清单得出一套设计基准事故，以便设定设计安全重要构筑物、系统和部件的边界条件。

5.2.11.2 在为响应某一假设始发事件而需要立即采取可靠行动时，必须采取措施自动启动所需的安全系统，以防止发展成可能威胁下一道屏障的更严重工况。在不需要立即动作的情况下，可允许手动启动系统或操纵员的其他行动，条件是需要有足够的时间来判断这种行动的必要性和确定合适的规程（如管理规程、运行规程和应急规程），以保证这些行动的可靠性。

5.2.11.3 必须考虑诊断核动力厂状态和使核动力厂及时地进入长期稳定停堆工况可能需要的操纵员行动，并必须通过设置适当的仪表以有利于监测核动力厂状态和监控设备的手动操作。

5.2.11.4 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，以保证需要时随时能用和在预计环境条件下允许人员接近。

5.2.12 严重事故

超设计基准事故中的某些概率很低的核动力厂状态，可能由安全系统多重故障而引起，并导致堆芯明显恶化，它们可能危及多层或所有用于防止放射性物质释放的屏障的完整性。这些事件序列被称之为严重事故。必须采用工程判断和概率论相结合的方法来考虑这些严重事故序列，针对这些序列确定合理可行的预防或缓解措施。可接受的方法应该基于现实的或最佳估算的假设、方法和分析准则，而不必运用确定和评价设计基准事故时所采用的保守的工程方法。根据运行经验、有关的安全分析和安全研究的结果，针对严重事故，设计中必须考虑的事项有：

(1) 必须采用概率论、确定论和正确的工程判断相结合的方法，确定可能导致严重事故的重要事件序列。

(2) 必须对照有关准则审查这些事件序列，以确定必须在设计中考虑哪些严重事故。

(3) 对于能降低这些选定事件发生的概率或者当这些选定事件发生时能减轻其后果的可能的设计修改或规程修改，必须加以评价，如属合理可行则必须实施这种修改。

(4) 必须考虑核动力厂整个设计能力,包括超过其原来预定功能和预计运行状态下可能使用某些系统（即安全系统和非安全系统）和使用附加的临时系统，使核动力厂回到受控状态和/或减轻严重事故的后果，条件是可以表明这些系统能够在预计的环境条件下起作用。

(5) 对于多机组核动力厂,必须考虑使用其他机组可利用的手段和/或支持，条件是其他机组的安全运行不会受到损害。

(6) 必须在计及有代表性和起主导作用的严重事故情况下制定事故管理规程。

5.3 构筑物、系统和部件的可靠性设计

安全重要构筑物、系统和部件必须设计成能以足够的可靠性承受所有确定的假设始发事件（见附件Ⅰ）。

5.3.1 共因故障

必须考虑安全重要物项发生共因故障的可能性，以确定应该在哪些地方应用多样性、多重性和独立性原则来实现所需的可靠性。

5.3.2 单一故障准则

5.3.2.1 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。

5.3.2.2 为检验核动力厂是否符合单一故障准则，必须对有关安全组合进行下述分析：假设单一故障（及其全部继发故障）依次发生在安全组合的各个单元上，直至分析了全部可能故障为止。然后对各有关安全组合逐一进行分析，直至考虑了所有安全组合和全部故障为止。（在本规定中，为获得所必需的可

靠性而必须采用多重性设计的那些安全功能或执行这些安全功能的系统均须由“假设单一故障”加以确认）在上述系统中假设单一故障是所述过程中的一部分。单一故障分析中，不考虑同时发生一个以上的随机故障。

5.3.2.3 当把此概念运用于一个安全组合或系统时，误动作必须视为故障的一种模式。

5.3.2.4 当按照下列条件应用上述分析时，如果表明每个安全组合均能完成各自的安全功能，则认为符合了单一故障准则的要求：

(1) 假定假设始发事件对该安全组合会发生任何可能的有害后果；

(2) 假设执行所需安全功能的安全系统处于许可的最不利配置，并考虑到维护、试验、检查和修理以及允许的设备停役时间。

5.3.2.5 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。

5.3.2.6 某一非能动部件的设计、制造、在役检查和维修均达到很高的质量水平，并且保持不受到假设始发事件的影响，则在单一故障分析中可以不必假设它会发生故障。但是，当假定某一非能动部件不发生故障时，必须从该部件所受的载荷、所处的环境以及始发事件发生后要求该部件执行其功能的全时程的角度来论证这种分析方法的合理性。

5.3.3 故障安全设计

故障安全设计原则必须恰当地考虑，并贯彻到核动力厂安全重要系统和部件的设计中。核动力厂系统必须设计成在该系统或其部件发生故障时不需要采取任何操作而使核动力厂进入安全状态。

5.3.4 辅助设施

辅助设施用于支持构成安全重要系统部分的设备时，必须视作安全重要系统的一部分，并必须相应地分级。它们的可靠性、多重性、多样性和独立性以及用于隔离和功能试验的措施必须与其所支持的系统的可靠性相当。保持核动力厂安全状态所必需的辅助设施包括供应电力、冷却水和压缩空气或其他气体的设施以及润滑设施等。

5.3.5 设备停役

设计必须通过采用诸如增加多重性等措施保证在毋需核动力厂停堆的情况下进行安全重要系统合理的在线维修和试验。必须考虑设备停役，包括系统或部件由于故障而不能使用，并且在这种考虑中必须包括预计的维护、试验和修理工作对各个安全系统的可靠性所产生的影响，以便保证仍能以所必需的可靠性实现该安全功能。在核动力厂开始运行前，必须分析和确定每种情况下允许设备停役的时间和要采取的行动，并将其包括在核动力厂运行规程中。

5.4 在役试验、维护、修理、检查和监测的措施

5.4.1 除 5.4.2 条所述的以外，为保持安全重要构筑物、系统和部件执行功能的能力，其设计必须符合下列要求：能在核动力厂整个寿期内进行标定、试验、维护、修理或更换、检查和监测，以证明满足可靠性目标。核动力厂布置必须便于进行这些活动，并能按照与所执行的安全功能的重要性一致的标准进行，同时系统可用性没有显著减少，且厂区人员不致于受到过量的照射。

5.4.2 安全重要构筑物、系统和部件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：

(1) 规定其他一些经验证的替代方法和（或）间接方法，如监视参考物项或使用经验证和确认的计算方法。

(2) 应用保守的安全裕度或采取其他适当的预防措施，以消除可能的预计不到的故障影响。

5.5 设备鉴定

5.5.1 必须采用设备鉴定的程序来确认安全重要物项能够在其整个设计运行寿期内满足处于需要起作用时的环境条件（如振动、温度、压力、喷射流冲击、电磁干扰、辐照、湿度或这些因素的任何可能组合）下执行其安全功能的要求。考虑的环境条件必须包括预计到的正常运行、预计运行事件和设计基准事故期间的变化。鉴定程序中，必须考虑到设备预期寿期内由各种环境因素（如振动、辐照和极端温度）引起的老化效应。对于位于易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取与有关自然现象对该设备影响的相同条件，通过试验或通过分析或两者的组合进行。

5.5.2 此外，在鉴定程序中必须列入可合理预计的和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。

5.6 老化

设计中必须为所有安全重要构筑物、系统和部件提供适当的裕度，以便考虑到有关的老化和磨损机理以及与服役期有关的可能的性能劣化，从而保证这些构筑物、系统或部件在其整个设计寿期内能够执行所必需的安全功能的能力。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和其后的核动力厂状态下的老化和磨损效应。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和鉴别在使用中可能发生的预计不到的情况或性能劣化。

5.7 优化运行人员操作的设计

5.7.1 人机的界面设计必须对操纵员是“友好的”，并必须以限制人为差错的影响为目标。必须优化核动力厂的布置和规程（管理规程、运行规程和应急规程），包括维修和检查，以利于运行人员和核动力厂之间的接口。

5.7.2 厂区人员的工作场所和工作环境必须按照人机工程学原则设计。

5.7.3 必须在设计过程初期就系统地考虑人为因素和人机接口，并贯彻于设计全过程，以保证适当而明确地区分运行人员与所提供的自动化系统之间的各项功能。

5.7.4 人机接口必须设计成不但能够为操纵员提供全面而易处理的信息，而且与作出决定和采取行动所需的时间相适应。必须为辅助控制室采取类似措施。

5.7.5 在适当阶段必须对人为因素进行验证和确认，以证实设计完全适合操纵员所有必要的操作。

5.7.6 为有助于制定信息显示和控制的设计准则，必须考虑操纵员能够承担系统管理者（包括事故管理）和设备操纵员的双重任务。

5.7.7 在操纵员作为系统管理者时，必须为其提供能够进行下列工作的信息：

(1) 在任何工况（即正常运行、预计运行事件或事故工况）下，迅速评估核动力厂的总体状态，并确认预定的自动安全动作正在进行；

(2) 确定操纵员要采取的适当的安全动作。

5.7.8 操纵员作为设备操纵员时，必须为其提供核动力厂各系统和设备有关参数的充分信息，以确认能够安全启动所必需的安全动作。

5.7.9 设计必须适当考虑有利于操纵员执行行动可利用的时间、预计的环境和对操纵员有心理压力的情况下成功地完成各种行动。必须把对操纵员在短时间内进行干预的要求降至最低。设计中必须考虑到这种干预可以接受的前提是：设计者能够证明操纵员有足够的时间作出决定和采取行动；向操纵员简单而明确地提供决定行动所需的信息；以及事件发生后，控制室内或辅助控制室内及通往辅助控制点的通道的环境是可以接受的。

5.8 其他设计考虑

5.8.1 反应堆之间构筑物、系统和部件的共享

安全重要构筑物、系统和部件通常不得在核动力厂内两座或多座反应堆之间共享。如果在特殊情况下，这种安全重要构筑物、系统和部件要在两座或多座反应堆之间共享，则必须证明对于全部反应堆来说在所有运行状态（包括维修）下和在设计基准事故中的所有安全要求都得到满足。在其中一个反应堆发生严重事故情况下，其他反应堆必须能够有序地完成停堆、冷却和余热排出。

5.8.2 含有易裂变或放射性物质的系统

设计必须保证核动力厂内可能含有易裂变或放射性物质的所有系统在运行状态和设计基准事故下均有足够的安全性。

5.8.3 用于热电联供、供热或海水淡化的核动力厂

拥有热利用装置（如地区集中供热）和/或海水淡化装置的核动力厂的设计必须防止放射性物质在正常运行、预计运行事件、设计基准事故和选定的严重事故的任何状态下从核动力厂转移到海水淡化装置或集中供热装置。

5.8.4 核燃料和放射性废物的运输和包装

设计中必须包括适当的设施，以便于新燃料、乏燃料和放

射性废物的运输和装卸。必须考虑设施的可达性、吊装和包装能力。

5.8.5 撤离路线和通信手段

核动力厂必须设置足够数量的、具有醒目而持久标识的安全撤离路线，并配备为安全使用这些路线所必需的应急照明、通风和其他辅助设施。撤离路线必须符合有关的辐射分区和防火要求，以及有关的工业安全和核动力厂保安方面的要求。

为使核动力厂厂内和厂区全部人员即使在事故工况下也能得到报警和通知，必须设置适当的报警系统和通信手段。

核动力厂范围内、邻近地区内以及与应急计划中所规定的厂区外机构安全必需的通信手段必须保持昼夜畅通。在通信设计和选择通信方法的多样性时，必须考虑这一要求。

5.8.6 出入口控制

为严密控制出入口，必须以适当的构筑物的布置方式，使核动力厂与其周围相隔离。尤其是在进行厂房设计和厂区布置时，必须为控制出入口的保卫人员和/或监测设备作出安排，并注意防止未经批准的人员和物品进入核动力厂。

必须防止未经批准接近或以任何理由影响安全重要构筑物、系统和部件。在维修、试验或检查需要出入的情况下，设计中必须保证所需活动的进行不致明显降低安全相关设备的可靠性。

5.8.7 系统的相互作用

如果存在较大的可能性需要安全重要系统同时运行时，必须对其可能的相互作用进行评价。在分析中，不仅必须考虑实体的相互连接，还必须考虑一个系统的运行、误操作或故障对其他重要系统的物理环境的影响，以保证环境的变化不会影响到系统部件预定的在执行功能方面的可靠性。

5.8.8 电网与核动力厂之间的相互作用

核动力厂设计中，必须考虑与所要求的给核动力厂安全重要系统供电的可靠性有关的电网与核动力厂的相互作用，包括电网供电母线的独立性和数量。

5.8.9 退役

在设计阶段必须专门考虑核动力厂便于退役和拆除的措施。特别是设计中必须考虑以下事项：

(1) 材料的选取，以便把放射性废物的最终数量降至最少程度，并便于去污；

(2) 必要的可达性；

(3) 贮存核动力厂运行和退役中产生的放射性废物所需的设施。

5.9 安全分析

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分析方法。在这种分析的基础上，必须制定和确认安全重要物项的设计基准。还必须论证所设计的核动力厂能够满足各类核动力厂状态（见 5.2.2 条）下放射性释放的所有规定限值和潜在的辐射剂量的可接受限值，并论证纵深防御已起到作用。

安全分析中应用的计算机程序、分析方法和核动力厂模型必须加以验证和确认，并必须充分考虑各种不确定性。

5.9.1 确定论方法

确定论安全分析必须包括：

(1) 确认核动力厂运行限值和条件符合核动力厂正常运行设计的假设和要求；

(2) 适合于核动力厂设计和厂址假设始发事件（见附件Ⅰ）的特征；

(3) 源自假设始发事件的事件序列的分析和评价；

(4) 各项分析结果与放射性的验收准则和设计限值的比较；

(5) 设计基准的制定和确认；

(6) 论证通过安全系统的自动响应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。

必须验证所采用的各项分析假设、方法和保守程度的适用性。根据核动力厂配置的重大变动、运行经验、技术知识的进步或物理现象的了解，核动力厂的安全分析必须不断更新，并必须与当时的状态或竣工状态相一致。

5.9.2 概率论方法

必须完成核动力厂的概率安全分析，以达到下述目的：

(1) 提供系统性的分析，以确信设计符合总的安全目标；

(2) 证明整个设计是平衡的，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，并且保证纵深防御的第一和第二层次承担核安全的主要责任；

(3) 确认核动力厂参数小的偏离不会引起核动力厂性能严重异常（陡边效应）；

(4) 提供发生堆芯严重损坏状态的概率评价以及要求厂外早期响应的（特别是与安全壳早期失效相关的）放射性物质向厂外大量释放的风险的评价；

(5) 提供外部灾害事件（特别是核动力厂厂址特有的那些灾害）发生概率和后果的评价；

(6) 鉴别出通过设计改进或运行规程的修改可能降低严重事故概率或减轻其后果的系统；

(7) 评价核动力厂应急规程的充分性；

(8) 核实是否符合概率目标（如果已有的话）。

6 核动力厂系统设计要求

6.1 反应堆堆芯和相关设施

6.1.1 总体设计

6.1.1.1 反应堆堆芯和有关冷却剂系统、控制和保护系统的设计必须留有适当的裕量，以保证在考虑到现有不确定性条件下所有运行状态和设计基准事故中不超过规定的设计限值并符合辐射安全标准。

6.1.1.2 反应堆压力容器内的反应堆堆芯和其他相关的内部部件的设计和装配，必须符合下述要求：在运行状态、设计基准事故和外部事件中所预期到的静、动载荷的作用下，可保持必要的结构稳定性，以保证反应堆安全停堆、保持次临界状态和保证堆芯冷却。

6.1.1.3 在运行状态和设计基准事故中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，保持冷却能力和不会发生反应堆堆芯显著损坏。

6.1.1.4 设计中必须保证把假设始发事件后发生重返临界或反应性急剧上升的可能性减至最小。

6.1.1.5 反应堆堆芯和有关冷却剂系统、控制和保护系统的设计必须在整个核动力厂运行寿期内能对其进行充分的检查和试验。

6.1.2 燃料元件和组件

6.1.2.1 燃料元件和组件必须设计成能满意地承受伴随在正常运行和预计运行事件中可能发生的各种劣化过程所预计的堆芯内辐照和环境条件。

6.1.2.2 设计燃料元件时必须考虑下列劣化因素：膨胀差和形变差、冷却剂外压、燃料元件内裂变产物所造成的附加内压、燃料组件中燃料和其他材料的辐照效应、功率变化所造成的压

力和温度的变化、化学效应、静载荷、包括流致振动和机械振动在内的动载荷以及可能由变形或化学效应引起的传热性能的变化等。设计必须为数据、计算和制造中的不确定因素留有裕量。

6.1.2.3 燃料元件在正常运行中不得超过规定的设计限值（包括裂变产物的允许泄漏量）；并且，必须保证可能受预计运行事件影响的各种运行状态不得造成燃料元件显著的进一步劣化。裂变产物的泄漏量必须限于设计限值之内，并保持在最低值。

6.1.2.4 燃料组件的设计必须考虑到在辐照后对其结构和零件能进行适当的检查。在设计基准事故中，燃料元件必须保持在原位，其变形不得达到有碍于堆芯在事故后保持足够有效冷却的程度，并且不得超过燃料元件在设计基准事故下的规定限值。

6.1.2.5 在核动力厂整个运行寿期内，即使燃料管理方案改变或运行状态发生变化时，也必须保持上述的反应堆和燃料元件设计的各项要求。

6.1.3 反应堆堆芯控制

6.1.3.1 在各种堆芯的中子注量率水平和分布状态下，包括停堆后、换料期间和换料后、预计运行事件和设计基准事故引起的状态，必须符合 6.1.1-6.1.2 条的规定。用于检测上述中子注量率分布的适当手段必须总能保证堆芯内不存在任何未能检测到的违反 6.1.1-6.1.2 条规定的部位。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 必须采取措施清除包括腐蚀产物在内的非放射性物质，以免危及系统的安全（如堵塞冷却剂通道）。

6.1.4 反应堆停堆

6.1.4.1 必须备有在运行状态和设计基准事故下安全停堆的手

段。必须保证即使在堆芯具有最大反应性的情况下，仍能保持停堆状态。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限值。如果停堆能力总是保持有足够裕量，则在正常功率运行期间部分停堆手段可用于反应性控制和中子注量率分布的整形。

6.1.4.2 停堆手段必须至少由两个不同的系统组成，以提供多样性。

6.1.4.3 两个系统中，至少有一个系统能在假设单一故障下独立执行使反应堆从运行状态和设计基准事故迅速进入有足够深度的次临界的功能。如果不超出燃料和部件的规定限值，可例外地允许瞬态重返临界。

6.1.4.4 即使在堆芯具有最大反应性的情况下，两个系统中至少有一个系统能独立使反应堆从正常运行状态、预计运行事件和设计基准事故进入次临界，并以足够的深度和高的可靠度保持次临界状态。

6.1.4.5 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去作用（如控制棒不能插入）或引起共因失效的故障。

6.1.4.6 停堆手段必须足以防止或承受停堆期间（包括该状态期间的换料）的反应性意外增加。为满足这一要求，必须考虑到停堆期间能增加反应性的各种预定操作（诸如维修时移动中子吸收体、硼稀释操作和换料操作等）及停堆手段的单一故障。

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工况所要求的状态。

6.1.4.8 反应性控制装置的设计必须考虑到磨损以及辐照（如燃耗）、物理性质改变和气体产生的各种效应。

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 反应堆冷却剂系统及其有关的辅助系统、控制和保护系统的设计必须具有足够的裕量，以保证反应堆冷却剂的压力边界在任何运行状态不超过设计条件。必须采取措施，以保证即使在设计基准事故下，卸压装置的动作也不得导致核动力厂放射性物质的不可接受的释放。反应堆冷却剂压力边界必须设置足够的隔离装置，以限制放射性流体的任何流失。

6.2.1.2 包容反应堆冷却剂的部件，如反应堆压力容器或压力管、管道和接头、阀门、配件、泵、循环装置和热交换器以及用于固定这些部件的器件，必须能在所有运行状态和设计基准事故下承受预计的静、动载荷。用于部件制造的材料必须选用在辐照下最不易活化的材料。

6.2.1.3 反应堆压力容器、压力管的设计和制造必须在材料选择、设计标准、可检查性和加工等方面均具有最高质量。

6.2.1.4 反应堆冷却剂压力边界的设计必须使微裂纹发生的可能性极小；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（例如，应用先漏后破概念）。必须避免使反应堆冷却剂压力边界的部件可能出现脆性行为的设计和核动力厂状态。

6.2.1.5 设计中必须考虑到反应堆冷却剂压力边界材料在运行状态包括维修、试验工况以及设计基准事故下的所有条件，并考虑到预期受到侵蚀、蠕变、疲劳、化学环境、辐射环境和老化等众多因素影响后的寿期末特性以及在确定部件初始状态和可能的劣化速率时的任何不确定因素。

6.2.1.6 设计必须尽量减少反应堆冷却剂压力边界范围内的部件，诸如泵的叶轮和阀门零件在各种运行状态和设计基准事故

下发生故障的可能性以及此种故障对一回路系统内其他安全重要物项造成的损伤，并为使用中可能发生的劣化留有适当的裕量。

6.2.2 反应堆冷却剂压力边界的在役检查

6.2.2.1 反应堆冷却剂压力边界的部件的设计、制造和布置必须便于在核动力厂整个寿期内对压力边界定期进行充分检查和试验。必须采取措施，执行反应堆冷却剂压力边界（特别是处于高辐射区域）和其他重要部件的材料监督大纲，以确定结构材料的辐照、应力腐蚀开裂、热脆化和老化等诸多因素的冶金学效应。

6.2.2.2 必须保证能够按照反应堆冷却剂压力边界的部件的安全重要性直接或间接地对其进行检查和试验，以验明不存在不可接受的缺陷或对安全有影响的劣化。

6.2.2.3 必须对用于反应堆冷却剂压力边界的完整性的指标（如泄漏率）进行监测。在确定哪些检查对安全来说是必要时，必须考虑这些测量的结果。

6.2.2.4 如果核动力厂的安全分析表明二回路冷却剂系统中的某些特定故障有可能导致严重后果时，其有关部分必须具有可检查性。

6.2.3 反应堆冷却剂装量

必须采取措施来控制冷却剂装量和压力，以便在任何运行状态下包括计及容积变化和泄漏的情况下使其均保持在设计规定的限值之内。为满足这一要求，执行上述功能的系统必须具有足够的容量（流量和储量）。这些系统可由动力生产过程所需的部件或专门为此而设置的部件组成。

6.2.4 反应堆冷却剂净化

必须设置足够的设施，以清除反应堆冷却剂中的放射性物质，包括活化腐蚀产物和从燃料泄漏的裂变产物。所需系统的

能力必须基于燃料设计规定的容许泄漏限值和保守的裕量，以保证核动力厂可在回路中的放射性水平处于合理可行尽量低的情况下运行，同时保证放射性释放量低于规定限值，并符合合理可行尽量低的原则。

6.2.5 堆芯余热的排出

6.2.5.1 必须为排出堆芯的余热提供手段。它们的安全功能是在不超过规定的燃料设计限值和反应堆冷却剂压力边界设计基准限值条件下，以一定的速率从堆芯排出裂变产物的衰变热和其他余热。

6.2.5.2 为了在假设单一故障、失去厂外电源的前提下，并结合适当的多重性、多样性和独立性足够可靠地实现 6.2.5.1 条的要求，余热排出系统的设计必须具备相互连接和隔离能力以及其他适当的设计特征（如泄漏检测）。

6.2.6 应急堆芯冷却

6.2.6.1 为了在冷却剂丧失事故中使燃料损伤最少和限制裂变产物的外逸，必须设置应急堆芯冷却系统。所提供的冷却必须保证：

(1) 包壳或燃料完整性参数（如温度）极限值不得超过设计基准事故下的可接受值（针对适用的反应堆设计而言）；

(2) 可能出现的化学反应限制在容许水平内；

(3) 燃料和堆内构件的变形不致于显著降低应急堆芯冷却手段的有效性；

(4) 堆芯冷却保持足够长的时间。

6.2.6.2 为了在假设单一故障的前提下对于每个假设始发事件足够可靠地实现上述要求，应急堆芯冷却系统的设计必须具备部件的适当的多重性和多样性，以及诸如泄漏检测、适当的相互连接和隔离能力等设计特征。

6.2.6.3 必须充分考虑在严重事故下从堆芯排出余热的能力。

6.2.7 应急堆芯冷却系统的检查和试验

应急堆芯冷却系统的设计必须能够对重要部件进行定期检查和对系统进行定期试验，以便确认：

(1) 系统中各部件的结构和密封的完整性；

(2) 正常运行期内系统中各能动部件能达到的可运行性和工作性能；

(3) 作为一个整体，系统按实际可能在设计基准中规定的核动力厂状态下的可运行性。

6.2.8 余热向最终热阱的输送

6.2.8.1 必须设置传热系统，向最终热阱输送来自安全重要构筑物、系统和部件的余热。这些系统在各种运行状态和设计基准事故下都必须具有很高的可靠性。用于输送热量的各系统，包括传送热量、提供动力以及向余热输送系统供应流体的设计都必须与它们在整个余热输送系统中所分担的功能相适应。

6.2.8.2 为实现系统的可靠性，必须恰当地选择包括使用经验证的部件、多重性、多样性、实体分隔、相互连接和隔离等措施。

6.2.8.3 在设计这些系统、选择最终热阱和传热流体贮存系统的多样性方案时，必须考虑到自然事件和人为事件的影响。

6.2.8.4 必须充分考虑在严重事故下向最终热阱输送堆芯余热的能力，以保证一旦发生严重事故时，在具有包容放射性物质的安全重要功能的构筑物、系统和部件的温度能够保持在可接受的范围内。

6.3 安全壳系统

6.3.1 安全壳系统设计

6.3.1.1 为保证设计基准事故下释放到环境中的放射性物质低于规定限值，必须设置安全壳系统。根据设计要求，安全壳系

统可包括：密封的构筑物；用于控制压力和温度的有关系统；以及用于隔离、管理与排除可能释放到安全壳大气中的裂变产物、氢、氧和其他物质的设施。

6.3.1.2 安全壳系统设计中，必须考虑到所有已确定的设计基准事故。此外，为了限制放射性物质向环境释放，还必须考虑设置用于减轻某些选定的严重事故后果的设施。

6.3.2 安全壳结构的强度

6.3.2.1 安全壳结构（包括通道闸门、贯穿件和隔离阀）的强度必须根据预期由设计基准事故下可能产生的内部超压、负压力、温度、飞射物撞击之类动态效应以及反作用力等进行计算，并留有足够的安全裕量。设计中还必须考虑到其他潜在的能量来源，如化学和辐射分解反应的影响。安全壳结构强度计算中还必须计及自然事件和人为事件的作用。必须采取措施监测安全壳及其相关构件的状态。

6.3.2.2 必须考虑严重事故下保持安全壳完整性的措施。特别是必须考虑预计发生的各种可燃气体的燃烧效应。

6.3.3 安全壳压力试验的能力

安全壳构筑物的设计和建造必须适应核动力厂运行前和整个寿期内在规定压力下进行压力试验的要求，从而验证其结构的完整性。

6.3.4 安全壳泄漏

6.3.4.1 安全壳系统必须按设计基准事故中的泄漏率不超过规定的最大值的要求进行设计。第二层包容壳可部分或全部包容承压的第一层安全壳，以收集和有控制地释放或储存第一层安全壳在设计基准事故中的可能的泄漏物。

6.3.4.2 安全壳构筑物以及对系统的密封性有影响的设备和部件的设计和施工，必须适应在贯穿件全部安装完毕后在设计压力下进行泄漏率测试的要求。安全壳系统还必须能够在堆的整

个寿期内定期在设计压力或在能估算出安全壳设计压力的泄漏率的较低压力下测定泄漏率。

6.3.4.3 必须充分考虑在严重事故下控制放射性物质从安全壳向外泄漏的能力。

6.3.5 安全壳贯穿件

6.3.5.1 安全壳的贯穿件的数量必须保持在实际可行的最少水平。

6.3.5.2 安全壳的所有贯穿件必须满足与安全壳构筑物本身相同的设计要求。必须采取保护措施防止管道位移或飞射物、喷射力和管道甩动等事故载荷所产生的作用力损伤贯穿件。

6.3.5.3 带有弹性密封（如弹性体密封件或电缆贯穿件）或膨胀补偿波纹管的贯穿件，必须设计成有可能在安全壳设计压力下进行独立于测定安全壳整体泄漏率的泄漏试验，以验证贯穿件在核动力厂整个寿期内保持完整性。

6.3.5.4 必须充分考虑在严重事故下贯穿件保持执行功能的能力。

6.3.6 安全壳隔离

6.3.6.1 为在设计基准事故下保持安全壳的密封性，防止放射性物质向环境的释放超过可接受限值，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空间相通的管线在设计基准事故下必须能可靠地自动封闭。为达到此目的，在这些管线上必须至少串联设置两个合适的安全壳隔离阀（通常，一个阀装在安全壳外侧，另一个装在内侧，但是，根据设计，也可采用其他布置）。每个阀门必须能可靠地独立动作。隔离阀必须尽实际可能靠近安全壳。安全壳的隔离必须在假设单一故障下完成。应用上述要求有损于贯穿安全壳的安全系统的可靠性时，可采用其他的隔离方式。

6.3.6.2 贯穿安全壳，但既非反应堆冷却剂压力边界的组成部

分，又不直接与安全壳空间相通的管线，必须至少设置一个合适的隔离阀。隔离阀必须位于安全壳外侧，并尽可能靠近安全壳。

6.3.6.3 必须充分考虑在严重事故下隔离装置保持执行功能的能力。

6.3.7 安全壳气密闸门

6.3.7.1 人员进入安全壳必须通过双道气密闸门。两道气密闸门必须相互联锁，以保证反应堆运行和设计基准事故期间至少有一道闸门处于密闭状态。当在低功率运行期间为监督目的需要人员进入安全壳时，必须采取措施，以保证操作期间人员的安全。如果有设备气密闸门，上述要求也适用于设备的气密闸门。

6.3.7.2 必须充分考虑在严重事故下安全壳气密闸门保持执行功能的能力。

6.3.8 安全壳内部结构

6.3.8.1 安全壳内的隔间之间必须提供足够的气流通道，以保持气流畅通。隔间之间气流通道的截面尺寸必须足以保证设计基准事故下压力平衡过程中的压差不损坏承压结构或其他对限制设计基准事故影响有重要作用的系统。

6.3.8.2 必须充分考虑安全壳内部结构承受严重事故的各种效应的能力。

6.3.9 安全壳的排热

6.3.9.1 反应堆安全壳必须具有排出热量的能力。安全壳排热系统必须实现在发生任何高能流体排放的设计基准事故后，降低安全壳内的压力和温度的安全功能，并使之保持在可接受的低水平。执行安全壳排热功能的系统必须在假设单一故障下要求具有足够的可靠性和多重性，以保证完成其功能。

6.3.9.2 必须充分考虑在严重事故下反应堆安全壳的排热能

力。

6.3.10 安全壳内气体的控制和净化

6.3.10.1 必要时，必须设置用以控制可能释放到反应堆安全壳内的裂变产物、氢、氧和其他物质的系统，借以：

(1) 减少设计基准事故下可能释放到环境的裂变产物的数量；

(2) 控制设计基准事故下安全壳气体中的氢或氧和其它物质的浓度，以防止可能危及安全壳完整性的爆燃或爆炸。

6.3.10.2 安全壳气体净化系统的部件和设施必须在假设单一故障下要求具有适当的多重性，以保证安全组合完成所要求的安全功能。

6.3.10.3 必须充分考虑在严重事故下控制可能产生或释放的裂变产物、氢和其他物质的措施。

6.3.11 覆盖层和涂层

为保证实现安全壳系统内构筑物和部件的覆盖层和涂层的安全功能，并尽量降低在其劣化时对其他安全功能的影响，必须审慎地选择覆盖层和涂层的材料，并必须规定专门的施工方法。

6.4 仪表和控制

6.4.1 安全重要仪表和控制系统总的要求

6.4.1.1 必须设置能在正常运行、预计运行事件、设计基准事故和在严重事故下对核动力厂变量和系统进行全程监测的仪表，以保证获取核动力厂状态的充分信息。必须设置能测量所有影响裂变过程、反应堆堆芯完整性、反应堆冷却剂系统和安全壳完整性的主要变量的仪表，以及借以获取核动力厂的安全可靠运行所必需的任何信息的仪表。对任何安全重要的导出参数，如冷却水的欠热度，必须配置自动记录装置。针对所涉及

的核动力厂各种状态的安全重要仪表必须经过环境鉴定，并且为应急响应需要，仪表必须适合于测量核动力厂各种参数，从而对各类事件进行分类。

6.4.1.2 必须设置检测仪表和记录装置，用以获取为监测设计基准事故过程和主要设备现状所需的基本信息；按安全要求，预测放射性物质可能从设计预期部位外逸的数量和位置。仪表和记录装置必须足以为严重事故期间确定核动力厂状态和为事故管理期间作出决策提供尽实际可能的信息。

6.4.1.3 必须提供适当的和可靠的控制手段，以便将上述变量（见 6.4.1.1 条）保持在规定的运行范围以内。

6.4.2 控制室

6.4.2.1 必须设置控制室，借以进行下述活动：在各种运行状态下安全地运行核动力厂；出现预计运行事件、设计基准事故和严重事故后，采取相应措施，以保持核动力厂的安全状态或使之返回安全状态。必须采取适当措施和提供足够的信息保护控制室内的人员，防止事故工况下形成的过量照射、放射性物质的释放或爆炸性物质或有毒气体之类险情的继发性危害，以保持其采取必要行动的能力。

6.4.2.2 对于确定控制室内部和外部可能直接威胁其连续运行的事件必须给予特别的关注。设计中必须采取合理可行的措施，尽量减少这些事件的影响。

6.4.2.3 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。在控制室设计中必须考虑人机工程学的因素。

6.4.2.4 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。

6.4.3 辅助控制室

必须在与控制室在电气分隔和实体隔离的一个独立的地点

（辅助控制室）配置足够的仪表和控制设备，借以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主要变量。

6.4.4 基于计算机的系统在安全重要系统中的应用

6.4.4.1 当安全重要系统设计成依赖于基于计算机的系统的可靠性时，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的标准，并在系统的整个寿期，特别是软件在开发期间，就必须加以实施。整个开发过程必须执行适当的质量保证大纲。

6.4.4.2 系统所要求的可靠性水平必须与其安全重要性相适应，并必须在研制开发过程中每个阶段通过采用各种互补手段（包括有效的分析和试验）的综合性方法以及通过证实系统设计达到要求的确认方法来实现。

6.4.4.3 在安全分析中对基于计算机的系统所假设的可靠性水平必须包括规定的保守性，以考虑特有的技术复杂性和由此引起的分析上的困难。

6.4.5 自动控制

各种安全动作必须是自动的，以便在预计运行事件或设计基准事故开始的一段合理的时间内，不需要操纵员的干预。此外，操纵员必须能够获取适当的信息以监视自动动作的效果。

6.4.6 保护系统的功能

保护系统必须具有下述功能：

(1) 自动触发相应的系统动作，必要时包括自动触发停堆系统动作，以保证在发生预计运行事件时不超出规定的设计限值；

(2) 检测到设计基准事故，并触发为把该事故后果限制在设计基准范围内所需的系统动作；

(3) 抑制控制系统自身的不安全动作。

6.4.7 保护系统的可靠性和可试验性

6.4.7.1 保护系统必须具有与所执行的功能相适应的高度可靠性和定期可试验性。保护系统所具有的多重性和独立性至少必须足以保证：

(1) 单一故障不会导致保护功能的丧失；

(2) 保护系统的运行可靠性未经其他方法证明确实可接受时，其任一部件或通道的停役不得导致所需最低限度多重性的丧失。

6.4.7.2 必须保证正常运行、预计运行事件和设计基准事故对多通道的影响不会导致保护系统功能的丧失，或者必须根据其他基准证明该功能的丧失是可以接受的。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）、故障安全性能、功能的多样性、部件设计或工作原理的多样性等以防止保护功能的丧失。

6.4.7.3 除非能通过其他方法获取必要的可靠性，否则保护系统必须具有可在反应堆运行时进行定期功能试验的条件，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丧失的缺陷。设计必须允许在运行期间对于从传感器到最终的执行元件的输入信号的所有环节进行试验。

6.4.7.4 设计中必须采取措施，在正常运行和预计运行事件中尽量减少由于操纵员的行动引起保护系统失效的可能性，但在设计基准事故中不限制操纵员采取正确的行动。

6.4.8 基于计算机的系统在保护系统中的应用

如果确定保护系统中应用基于计算机的系统，在6.4.4.1-6.4.4.3条中必须补充下述要求；

(1) 必须使用最高质量和最佳实践的硬件和软件；

(2) 整个开发过程，包括设计修改的控制、试验和调试，必须系统地形成文件，并可供检查；

(3) 为了确认基于计算机的系统可靠性的可信度，必须由独

立于设计者和供应商的专家对基于计算机的系统进行评价；

(4) 在不能论证所需系统的完整性具有高可信度时，必须具备保证执行保护功能的其他不同的手段。

6.4.9 保护系统和控制系统的分隔

为防止保护系统和控制系统之间的相互干扰，必须避免两者之间的相互连接或采用适当的功能隔离。如果保护系统和控制系统共用相同的信号，必须采取适当的分隔措施（如有效的去耦），并证明 6.4.6-6.4.8 条所列各项安全要求均已得到满足。

6.5 应急控制中心

必须设置一个与核动力厂控制室相分离的厂内应急控制中心，作为发生应急情况时在此工作的应急人员汇集的场所。应急控制中心内应能获得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。应急控制中心应具有联络核动力厂控制室、辅助控制室及其他重要地点和厂内外应急机构的通信手段，以及实时在线传输核动力厂安全重要参数的能力。必须采取适当措施，在长时间内保护在场的人员，以便防止严重事故对他们的危害。

6.6 应急动力供应

6.6.1 安全重要的各种系统和部件，在发生某些假设始发事件后，需要应急动力。在任何运行状态或设计基准事故下并在假设同时发生丧失厂外电源的情况下必须保证应急动力供应满足要求。对动力的需求因假设始发事件的性质而异。选择各种安全功能所需动力的手段时，包括其数量、可用率、持续时间、容量和不间断性等，需要考虑所执行的安全功能的性质。

6.6.2 提供应急动力的组合手段（如水轮机、汽轮机、燃气轮机、柴油机和蓄电池等）的可靠性和方式，必须与作为其供应

对象的安全系统对安全的全部要求相一致，并在假设单一故障下执行其功能。应急动力供应必须能够进行功能能力试验。

6.7 放射性废物处理和控制系统

6.7.1 概述

6.7.1.1 为使放射性物质的排出量及其浓度保持在规定限值以内，必须设置适当的处理液态和气态放射性排出流的系统。必须贯彻合理可行尽量低的原则。

6.7.1.2 必须设置适当的系统，以处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，该期限与在厂区具备的处置途径的时间相一致。向厂外运输固态废物，必须遵守国家核安全监管部门的规定。

6.7.2 液态放射性物质向环境释放的控制

核动力厂必须具备有适当手段，以控制液态放射性物质向环境的释放，从而保证排放量和浓度保持在规定限值之内，并符合合理可行尽量低的原则。

6.7.3 气载放射性物质的控制

必须设置具有适当过滤能力的通风系统，以实现：

(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，使之符合进入该区域的规定要求；

(3) 在正常运行、预计运行事件和设计基准事故中，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，并符合合理可行尽量低的原则；

(4) 在不损害控制放射性物质释放能力的条件下，维持含有惰性气体或有毒气体的房间的通风。

6.7.4 气态放射性物质向环境释放的控制

6.7.4.1 必须设置具有适当过滤系统的通风系统，以控制气载

放射性物质向环境的释放，并保持在规定限值之内，以及保证符合合理可行尽量低的原则。

6.7.4.2 过滤系统必须足够可靠，并在预计的主导条件下能得到必需的滞留因子。过滤系统必须具有测试其效率的条件。

6.8 燃料装卸和贮存系统

6.8.1 未辐照燃料的装卸和贮存

未辐照燃料装卸和贮存系统的设计必须符合下述要求：

(1) 通过采用物理手段或工艺（以几何安全布置为宜）并留有规定的裕量，以防止在最佳慢化的核动力厂状态下达到临界；

(2) 对安全重要部件可进行适当的维修、定期检查和试验；

(3) 尽量防止燃料丢失或损坏的可能性。

6.8.2 已辐照燃料的装卸和贮存

6.8.2.1 已辐照燃料装卸和贮存系统的设计必须符合下述要求：

(1) 采用物理手段或工艺（以几何安全布置为宜），以防止在最佳慢化的核动力厂状态下达到临界；

(2) 在运行状态和设计基准事故下能充分排出热量；

(3) 对已辐照燃料能进行检查；

(4) 对安全重要部件可进行适当的定期检查和试验；

(5) 防止乏燃料在转运过程中跌落；

(6) 防止装卸时在燃料元件或燃料组件上产生不可接受的应力；

(7) 防止乏燃料运输容器、起重设备或其他可能损坏物体等重物意外地跌落在燃料组件上；

(8) 能安全地贮存怀疑损坏或已损坏燃料元件或燃料组件；

(9) 具有正确的辐射防护措施；

(10) 每个燃料组件有适当的标识；

(11) 控制可溶吸收体的浓度水平（如果用于临界安全）；

(12) 燃料贮存和装卸设施便于维修和退役；

(13) 必要时燃料装卸和贮存场所及设备便于去污；

(14) 保证能执行适当的操作程序和衡算计量程序，以防止燃料的丢失。

6.8.2.2 对于采用水池系统贮存已辐照燃料的反应堆，其设计必须提供下列措施：

(1) 控制已辐照燃料在装卸或贮存水池中的水化学和放射性活度；

(2) 监测和控制燃料贮存水池的水位及检测水池泄漏；

(3) 防止在管道破裂事件中水池排空（即反虹吸措施）。

6.9 辐射防护

6.9.1 总的要求

6.9.1.1 辐射防护的目的在于防止任何可避免的照射，并使不可避免的照射保持在合理可行尽量低的水平。为实现这一目标，设计中必须采用下述办法：

(1) 含有放射性物质的构筑物、系统和部件采用适当的布置方式，并设置屏蔽；

(2) 核动力厂和设备设计中注意把辐射区内人员活动的次数和停留时间减至最少，以及减少厂区人员遭受污染的可能性；

(3) 把放射性物质处理成适当的形态，以便放射性废物的处置、在厂区内的贮存或发往厂外；

(4) 采取措施，以降低厂内所产生的散布于厂内或释放到环境的放射性物质的数量和浓度。

6.9.1.2 必须充分考虑到人员停留区域内辐射水平随时间可能累积并需尽量减少放射性废物的产生。

6.9.2 辐射防护设计

6.9.2.1 核动力厂的设计和布置中必须采取合适的措施，以尽量减少来自各种辐射来源的照射和污染。这类措施必须包括以下诸方面的构筑物、系统和部件的恰当设计：尽量降低维修和检查期间的照射、屏蔽直接的和散射的照射、控制气载放射性物质的通风和过滤、采用技术规格适当的材料限制腐蚀产物的活化、监测手段、核动力厂出入口的控制及相应的去污设施。

6.9.2.2 屏蔽设计必须使得操作区的辐射水平不超过规定限值，并必须便于维修和检查，以尽量降低维修人员所受的照射。必须贯彻合理可行尽量低的原则。

6.9.2.3 核动力厂的布置和规程必须符合下述要求：辐射区和可能污染区的出入要有控制措施，并把厂内放射性物质的转移和人员流动所引起的污染减少至最低限度。核动力厂的布置必须保证高效率的运行、检查、维修和部件必要时的更换，以尽量减少辐射照射。

6.9.2.4 必须为人员和设备提供合适的去污设施，并为处理在去污活动中所产生的放射性废物采取适当措施。

6.9.3 辐射监测设备

6.9.3.1 必须配置设备以保证在运行状态和设计基准事故下以及尽实际可能的在严重事故下有适当的辐射监测。其具体要求如下：

(1) 在运行人员常驻之处以及在正常运行或预计运行事件期间由于辐射水平的变化可能必须在一定时间内限制进入的场所，必须设置固定式剂量率仪表进行就地的辐射剂量率监测。此外，必须在适当的地点安装固定式剂量率仪表，用以指示在设计基准事故和尽实际可能的在严重事故下总的辐射水平；这些仪表必须向控制室或有关控制点提供足够的信息，以便运行人员及时采取必要的纠正措施；

(2) 在人员常驻之处及气载放射性水平可能高至要求防护

措施的场所，必须设置监测系统测量空气中放射性物质的活度。测得高浓度核素时，这些系统必须向控制室或其他的相应控制点发出指示；

(3) 必须设置固定式设备和实验室装置，以便在运行状态或事故工况下及时测定流体处理系统中和取自核动力厂系统或空间的气体或液体样品中所选定的放射性核素的浓度；

(4) 必须设置固定式设备，以便监测向环境排放前或排放过程中的排出流；

(5) 必须设置用于测量放射性表面污染的仪器；

(6) 必须设置用于测量人员所受剂量和污染的装置。

6.9.3.2 除了在核动力厂内进行监测外，还必须为确定核动力厂对邻近地区可能产生的任何放射性影响作出安排。特别是：

(1) 包括食物链在内的影响到居民的各类途径；

(2) 对当地生态系统的放射性影响（如果有的话）；

(3) 放射性物质在实体环境中可能的积聚；

(4) 任何可能的未经批准的排放途径。

附件Ⅰ　　假设始发事件

Ⅰ.1 本附件详细描述假设始发事件的定义及其概念的应用。

Ⅰ.2 假设始发事件定义为在设计时确定的能导致预计运行事件或事故工况的事件。这意味假设始发事件本身并不是事故；它是一个引发了一个序列的事件，并由不同的附加故障而导致运行事件、设计基准事故或严重事故的事件。典型的例子是设备故障（包括管道破裂）、人员差错、人为事件和自然事件。

Ⅰ.3 假设始发事件的后果可能较小（如某一多重部件的失效），也可能很严重（如反应堆冷却剂系统主管道的破裂）。设计的主要安全目标在于追求核动力厂所具有的特性能够保证：大部分假设始发事件的后果较小或甚至无足轻重；其余的假设始发事件导致设计基准事故，其后果是可以接受的；而如果导致严重事故，其后果可以通过设计措施和事故管理加以限制。

Ⅰ.4 对各类假设始发事件必须作出全面考虑，以保证潜在后果严重的和发生概率大的全部可信事件均在预计范围之内，且核动力厂设计足以承受这些事件。假设始发事件的选择并无严格的准则可供遵循。更确切地说，此种选择过程无非是一种综合运行设计和分析之间的迭代、工程判断以及以前核动力厂设计和运行经验的过程。排除某一特定事件序列需要论证。

Ⅰ.5 用于制定安全重要物项的性能要求和核动力厂总的安全评价的假设始发事件的数量应该加以限制。为使执行该项任务切实可行，详细分析可限于若干代表性的事件序列。具有代表性的事件序列包络所有同类事件，并为安全重要构筑物、系统和部件的设计的数字限值提供依据。

Ⅰ.6 某些假设始发事件可基于已有核动力厂的经验、国家核安全监管部门的特殊要求或潜在后果的严重程度等种种因素，通

过确定论法确定。另外一些假设始发事件，由于设计特征、核动力厂所在厂址或运行经验等因素可通过概率值加以定量表示，则可借助于诸如概率分析的系统方法加以确定。

假设始发事件的类型

内部事件

设备故障

Ⅰ.7 能直接或间接影响核动力厂安全的各个设备的故障可视为始发事件。列入清单的事件足以代表核动力厂系统和部件的全部可信故障。

Ⅰ.8 需要考虑的故障类型取决于所涉及系统和部件的类型。广义而言，故障包括如下两类：系统和部件丧失执行功能的能力；功能的执行情况与所期望的不符。例如，管道故障的表现形式可能是泄漏、破裂或流道堵塞。能动部件，例如阀门的故障形式有：在需要时不开启或不关闭，在不需要时开启或关闭，开不足或关不住，开启或关闭的速度不当。仪表或传送器之类的装置的故障有如下形式：误差大于允许范围、无输出、不变的最大输出、不稳定的输出或上述形式的组合。

Ⅰ.9 随着基于计算机的系统在安全领域和重大安全问题上的应用日益扩大，硬件故障或不正确的软件程序可导致有重大影响的控制动作，应该考虑这种可能性。

人员差错

Ⅰ.10 人员差错的后果往往与部件故障的后果相类似。属于人员差错范畴的有：错误的和不良的维修、控制限值的错误整定和操纵员的其他错误行动或疏忽（执行差错和疏忽差错）。

其他内部事件

Ⅰ.11 内部原因引起的火灾、爆炸和水淹对核动力厂安全也可能产生重要影响。通常将这些事件列入假设始发事件的清单。

外部事件

Ⅰ.12 核动力厂外部事件的事例以及设计基准输入的确定见核动力厂厂址选择安全规定（HAF101）及其有关导则。这些事件通常要求核动力厂物项设计考虑附加的振动、冲击和脉动型载荷。

Ⅰ.13 如能断定自然事件或人为外部事件引起某一安全重要构筑物、系统或部件故障的可能性通过设计和建造中所采取的措施可降低到可接受的程度，则由此引起的故障不必列入核动力厂的设计基准。

事件组合

Ⅰ.14 事故分析中对于单个事件的组合需要谨慎处理，以保证特定的组合有其合理性。事件的随机组合可表现为一种极不可能的情景，在概率安全评价中应证明此种情景发生概率极低，则可不作为假想事故考虑。在概率安全评价中，对于严重事故采用最佳估计分析方法；而对于具有相对较高发生可能性的假想事故，分析中应采用保守分析方法。

Ⅰ.15 在决定事件组合时，考虑以下三个时期是有益的：

(1) 事件发生前的长时期；

(2) 从事件发生到它的短期效应起作用的近期；

(3) 事件后的恢复期。

Ⅰ.16 如在核动力厂设计中已为识别第一个时期内发生的事件采取了正确的措施，且纠正行动可在短期内完成，则可以设想，在第一个时期发生的事件可在发生另一次事件前得到纠正。在这种情况下不必考虑此种事件的组合。

Ⅰ.17 上述第二个时期（通常持续几小时）内，根据每个单个事件的预计发生概率推断可以认为随机发生的组合是不可信的。

Ⅰ.18 事件后的恢复期（几天或更长）内，是否需要考虑附加的事件，视恢复期的长短和事件预计的概率而定。恢复期内必

须考虑事件组合中附加事件的严重程度，按低于核动力厂全寿期内所考虑的同类事故来考虑可能是合乎实际的。以失水事故后恢复期内需考虑的地震随机组合为例，其严重程度可按低于核动力厂设计基准地震计。

附件 II　　多重性、多样性和独立性

II.1 本附件所列的几种设计措施可用于达到和保持与有关纵深防御层次上所执行安全功能的重要性相当的可靠性。如有必要，可使用这些措施的组合。

II.2 表示纵深防御每个层次的可靠性要求时，虽然没有通用的定量指标，但第一层次无疑应视作重点。这与营运单位保持核动力厂高可用率的目标也是吻合的。

II.3 为保证执行安全功能所必需的可靠性，经国家核安全监管部门同意，对某些安全系统可制定最大不可用率的限值作为基准或用作验收准则。

共因故障

II.4 若干装置或部件的功能可能由于出现单一特定事件或原因而失效。这种失效可能同时影响到若干不同的安全重要物项。这种事件或原因可能是设计缺陷、制造缺陷、运行或维修差错、自然现象、人为事件、或核动力厂内任何其他操作或故障所引起的意外的级联效应。

II.5 若干同类型部件同时失效时，也可能发生共因故障。这可能由诸如环境条件的变化、信号饱和、重复的维修差错或设计缺陷等原因所引起。

II.6 在设计中尽实际可能采取适当的措施，如应用多重性、多样性和独立性等，使共因故障的影响降低到最小程度。

多重性

II.7 为完成一项特定安全功能而采用多于最少套数的设备，即多重性，它是达到安全重要系统高可靠性和满足单一故障准则的重要设计原则。在运用多重性原则的条件下，至少一套设备出现故障或失效是可承受的，不致于导致功能的丧失。例如，

在某一特定功能可由任意两台泵完成之外，设置三台或四台泵。为满足多重性要求，可采用相同或不同的部件。

多样性

Ⅱ.8 采用多样性原则能减少某些共因故障的可能，从而提高某些系统的可靠性。

Ⅱ.9 多样性应用于执行同一功能的多重系统或部件，通过多重系统或部件中引入不同属性而实现。获得不同属性的方式有：采用不同的工作原理、不同的物理变量、不同的运行条件或使用不同制造厂的产品等。

Ⅱ.10 为保证所采用的多样性能提高所完成设计的可靠性，在运用多样性原则时必须审慎。例如，为降低共因故障的可能性，设计人员应用多样性原则时必须对材料、部件和制造工艺中有无任何相似之处，运行原理或公用的辅助设施中有无细微的类似之处给予关注。采用多样性的系统或部件时，应考虑诸如运行、维修和试验程序中额外的复杂性，或使用可靠性较低设备所带来的缺点，并取得此种附加措施有利于总体效益的合理保证。

独立性

Ⅱ.11 为提高系统的可靠性可在设计中保持下列独立性特征：

(1) 多重系统部件之间的独立性；

(2) 系统中各部件与假设始发事件效应之间的独立性，例如，假设始发事件不得引起为减轻该事故后果而设置的安全系统或安全功能的失效或丧失；

(3) 不同安全等级的系统或部件之间适当的独立性；

(4) 安全重要物项与非安全重要物项之间的独立性。

Ⅱ.12 独立性可在系统设计中通过采用功能隔离或实体分隔来实现。

(1) 功能隔离

应采取功能隔离，以减少多重系统或相连接系统中由正常运行或异常运行，或这些系统中任一部件的故障引起的设备和部件间不良相互作用的可能性。

(2) 部件的实体分隔和布置

在系统布置和设计中，应尽实际可能采用实体分隔原则以增强实现独立性的保证，对于某些共因故障尤其如此。

这些原则包括：

几何分隔（如距离、方位等）；

屏障分隔；

上述两种分隔的组合。

分隔方法的选择取决于设计基准中所考虑的假设始发事件，例如火灾、化学爆炸、飞机坠毁、飞射物、水淹、极值温度和湿度等效应。

Ⅱ.13 核动力厂的某些场所，有可能成为不同级别安全重要性的各种设备或线路的自然汇合点，例如安全壳贯穿区、电动机控制中心、电缆走廊、设备间、控制室和核动力厂的工艺控制计算机等。在这些场所，应尽实际可能采取适当的措施以防止共因故障。

附录Ⅰ 沸水堆、压水堆和压力管式反应堆的安全功能

Ⅰ-1 本附录给出 4.2.2 条中定义的三种基本安全功能的详细分类的示例。

Ⅰ-2 这些安全功能包括为预防事故工况以及为减轻事故工况后果所必需的安全功能。根据情况利用为正常运行、为防止预计运行事件发展为事故工况或为减轻事故工况的后果而设置的构筑物、系统或部件，就能完成这些安全功能。

Ⅰ-3 对各种反应堆设计的审查表明具有执行下述安全功能的构筑物、系统或部件就能满足现行的设计安全要求：

(1) 防止发生不可接受的反应性瞬变；

(2) 在所有停堆动作完成后，将反应堆保持在安全停堆状态；

(3) 在需要时停堆以防止预计运行事件发展为设计基准事故和停堆以减轻设计基准事故的后果；

(4) 在事故工况(不包括反应堆压力边界失效)期间和之后，保持足够的反应堆冷却剂总量用以冷却堆芯；

(5) 在设计基准中所考虑的所有假设始发事件期间和之后，保持足够的反应堆冷却剂总量用以冷却堆芯；

(6) 在反应堆冷却剂压力边界失效之后，从堆芯排出热量[①]以限制燃料损坏；

(7) 在反应堆冷却剂压力边界完整的情况下，在适当的运行状态和事故工况期间，从堆芯排出余热[①]；

(8) 将其他安全系统的热量传递到最终热阱[②]；

(9) 作为一种支持性功能，为安全系统提供必要的公用设施（如电、气、液压、润滑等）；

[①] 该安全功能系指热量排出系统的第一阶段。其余阶段包括在安全功能（8）中；

(10) 保持堆芯内的燃料包壳可接受的完整性；

(11) 保持反应堆冷却剂压力边界的完整性；

(12) 限制放射性物质在事故工况期间和之后从反应堆安全壳内向外释放；

(13) 在设计基准事故和选定的严重事故期间和之后，限制由反应堆安全壳以外的辐射源释放的放射性物质对于公众和厂区人员的辐射照射；

(14) 在所有运行状态下将放射性废物和气载放射性物质的排放或释放限制在规定限值以内；

(15) 对核动力厂内的环境状况保持控制，以便各安全系统能够正常运行，并为进行安全上重要操作的运行人员提供必要的可居留性；

(16) 在所有运行状态下，对在反应堆冷却剂系统以外，但仍在厂区以内运输或贮存中的已辐照燃料的放射性释放进行控制；

(17) 从贮存在反应堆冷却剂系统以外，但仍在厂区以内的已辐照燃料中排出衰变热；

(18) 使贮存在反应堆冷却剂系统以外，但仍在厂区以内的燃料保持足够的次临界度；

(19) 当某一构筑物、系统或部件的损坏会损害某一安全功能时，防止其发生损坏或限制其损坏所引起的后果。

Ⅰ-4 上述安全功能的清单可用来作为确定某一构筑物、系统或部件是否执行或有助于执行某一项或多项安全功能的基础，并为确定有助于执行安全功能的安全重要构筑物、系统或部件的适当分类提供基础。

---

[2] 这里指当其他安全系统必须执行其安全功能时所需要的支持功能。

名 词 解 释

在核动力厂安全规定中下述名词术语的含义为：

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多重部件或系统，这些不同部件或系统具有不同属性，从而减少了共因故障的可能性。

功能隔离

防止一个线路或一个系统的运行模式或故障影响到另一个线路或系统。

安全重要物项

属于某一安全组合的一部分和/或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。

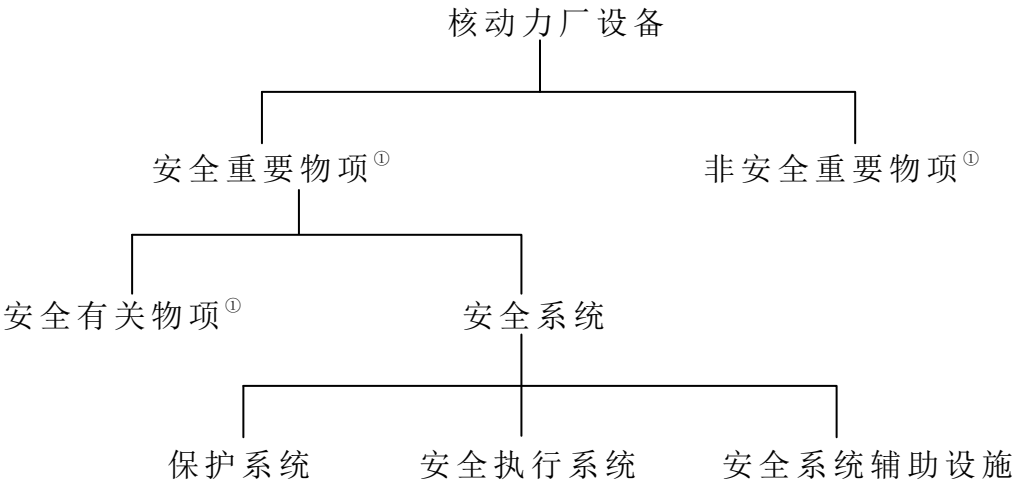
非能动部件

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。

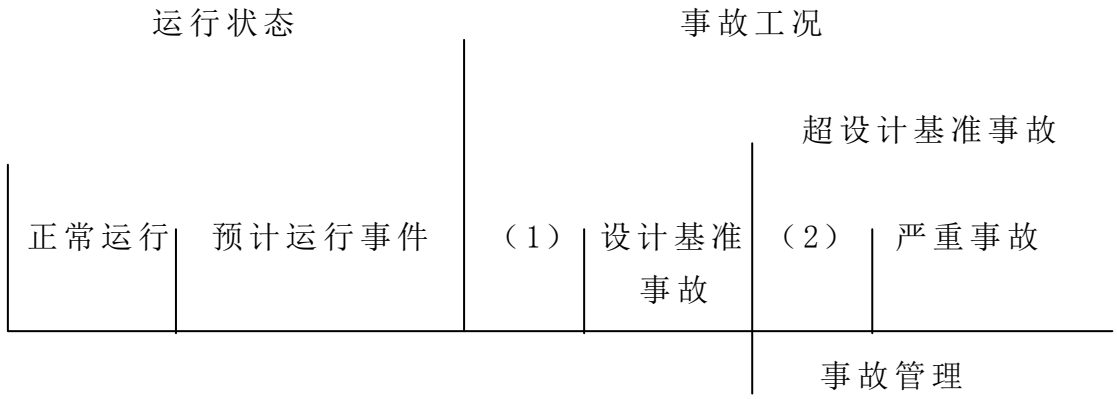
实体隔离

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。

核动力厂设备



核动力厂状态



(1) 没有明确地考虑作为设计基准事故，但可为设计基准事故所涵盖的那些事故工况。

(2) 没有造成堆芯明显恶化的超设计基准事故。

事故工况

比预计运行事件更严重的工况，包括设计基准事故和严重事故。

事故管理

① 在本名词解释中，物项系指构筑物、系统或部件。

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。

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。

设计基准事故

核动力厂按确定的设计准则在设计中采取了针对性措施的那些事故工况，并且该事故中燃料的损坏和放射性物质的释放保持在管理限值以内。

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[①]

设计期间确定的可能导致预计运行事件或事故工况的事件。

保护系统

监测反应堆的运行，并根据接收到的异常工况信号，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

为安全而必须达到的特定目的。

[①] 进一步解释见附件Ⅰ。

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。

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。

单一故障

导致某一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。