

HAF201

研究堆设计安全规定

(1995年6月6日国家核安全局批准发布)

本规定自1995年10月1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

1.1.1 本规定的目的是提供研究堆设计及其评价的安全基础,并提出与研究堆设计有关的安全监督管理、选址及质量保证等方面的要求。

1.1.2 本规定只强调研究堆设计必须满足的安全要求,对于如何满足这些要求则不作具体规定。

1.2. 范围

1.2.1 本规定适用于研究堆的设计,也适用于在现有研究堆上的重要新实验及对现有研究堆的改造。

1.2.2 功率达几十兆瓦的研究堆、快中子研究堆或小的实验性原型动力堆等可能还需另外的安全措施,因此在某些方面应遵守动力堆的有关安全规定。

1.2.3 某些研究堆(包括临界装置)实际上并不需要满足本

规定的全部安全要求^①。对这些情况,若能提供有说服力的证据证明其设计是合理的,则某一特定的设计可不满足第五章规定的某些要求。

1.2.4 本规定中研究堆一词包括反应堆堆芯,实验装置,以及反应堆厂址内的与反应堆或实验装置有关的一切其它设施。

2 安全目标

2.1 安全目标

2.1.1 研究堆的安全总目标是建立并维持一套有效的防御措施,以保护工作人员、公众和环境免受过量的放射性危害。

2.1.2 根据总目标,其相应的具体辐射防护目标是:确保研究堆的运行和使用满足辐射防护的要求;确保在各种运行状态下,厂区工作人员及公众的辐射照射低于国家规定的限值,并保持在合理可行尽量低的水平;确保事故引起的辐射照射得到缓解。

2.1.3 与事故相关的技术安全目标是:确保广泛地预防事故,确保设施设计中考虑到的所有事件序列(包括那些概率低的),其辐射后果要小,通过采用预防及缓解措施,确保有严重后果的事故发生的可能性极小。

2.1.4 为了实现这些目标,对最终确保研究堆安全运行的各个方面均提出了安全要求及建议,包括设计中及运行中需采取的措施。对设计及运行均必须实施充分的安全监督管理。

^① 实例之一为临界装置的堆芯冷却。因无功率输出,所以不需专用的堆芯冷却系统。

3 选址要求

3.1 选址要求

3.1.1 研究堆厂址选择的依据与许多因素有关,特别与研究堆的设计及预定用途有关。对某些低功率研究堆,选址的限制因素可能较少,而对功率高并用于大量实验工作的研究堆,则要提出比较严格的选址及设计要求。

3.1.2 研究堆选址的主要目的是保护公众及环境免受放射性物质的事故释放所引起的辐射影响。正常的放射性释放也必须加以考虑。在评价研究堆厂址的适宜性时,必须考虑下列因素:

(1)在某特定厂址所在区域发生的外部事件的影响(这些事件可为自然事件或人为事件);

(2)可能影响所释放的放射性物质向人体迁移的厂址特征及其环境特征;

(3)与实施应急措施的可能性和评价个人和群体风险有关的人口密度和分布以及其它的外围地带的特征。

3.1.3 必须调查和评价可能影响研究堆安全的厂址特征,特别是自然事件和外部人为事件。

3.1.4 必须调查运行状态和事故工况下,可能受辐射后果影响的区域的环境特征。对所有这些特征,在研究堆的整个寿期内必须予以观测和监控。

3.1.5 必须评价厂址所在区域内影响安全的自然因素和人为因素在设计寿期内可预见的演变。在研究堆整个寿期内,也必须监控这些因素,特别是人口增长率和人口分布。如有必要,必须采取适当措施,以保证总的风险保持在可接受的低水平上。

3.1.6 必须以发生概率为不可忽视的外部事件的严重性来确定研究堆的设计基准,以使总风险减少到可接受的水平。如果

研究堆及其所有安全设施均不能对付这些事件,而对公众的辐射照射会产生不可接受的风险,则必须认为此厂址是不适宜的。在分析所选厂址的适宜性时,必须考虑新燃料、乏燃料及放射性废物的贮存和运输问题。

3.1.7 应对厂区进行开工前的必要的辐射监测,以确定辐射本底水平,用以评价将来反应堆对厂区的影响。这对将来决定退役申请的可接受性是很重要的。

3.1.8 对每个推荐的厂址,必须对该区域的人口分布、饮食习惯、土地和水的利用情况以及该区域其它放射性释放物所产生的辐射影响等有关因素给予应有的考虑,以评价在运行状态和在事故工况(包括可能导致需采取应急措施的工况)下,对厂址所在区域的居民可能产生的辐射影响。

3.1.9 对可能影响安全和确定厂址设计基准参数的一切活动,都必须执行质量保证大纲^①。

4 设计总要求

4.1 概述

4.1.1 为达到第二章所定的安全目标,反应堆的设计应满足安全设计要求。各类研究堆的设计必须符合本章中的设计总要求。反应堆设计还须满足第五章中的具体设计要求。

4.1.2 这些要求应在设计的各个阶段贯彻执行,同时考虑相应的安全分析结果的反馈。

4.1.3 反应堆设计者不仅必须考虑反应堆本身,还必须考虑可能影响其安全的相关设施。设计者还必须考虑反应堆寿期内所有阶段的设计要求。

^① 参见 HAF003 及有关文件。

4.1.4 安全设计的成功需要反应堆设计者和营运单位之间紧密的联系。

4.2 纵深防御

4.2.1 设计中必须贯彻纵深防御的原则,从而提供多层次的保护,防止放射性物质释放。

(1)采用保守的设计裕量,执行质量保证大纲。

(2)设置多道实体屏障,防止放射性物质释放。这些屏障通常包括燃料基体、燃料包壳、主传热系统、堆池、反应堆厂房等。在纵深防御概念中,重要的因素是保护这些屏障使其不受破坏。

(3)提供多种手段,确保下列基本安全功能:

——在所有运行状态或事故工况下,均能停堆并使之保持在安全停堆状态;

——足以排除停堆后(包括事故工况停堆后)堆芯余热;

——包容放射性物质,尽量减少向环境的释放。

(4)利用设备及管理性程序,以实现下列要求:

——防止偏离正常运行状态;

——防止可能导致事故工况的预计运行事件;

——控制及缓解事故工况及事故后果。

(5)制定应急计划,一旦大量放射性物质释入环境,即可缓解对公众产生的影响^①。

4.2.2 对 4.2.1 节(3)中所述的三项基本要求——停堆、冷却和包容——可选用下列各项措施的适当组合来得到满足:

——设计中包括固有安全特性;

——提供适当的安全系统及专设安全设施;

——反应堆整个寿期内均贯彻管理性程序。

固有安全特性的例子有:借助堆芯材料及堆芯几何形状的选

^① 为实施应急计划,可能要求设计者采取应有的设计措施(参见 4.16),然而,对潜在辐射风险低的研究堆,厂外应急计划可能是不必要的。

择使之具有瞬发负反应性温度系数。

4.2.3 通常利用安全系统来满足 4.2.1 节(3)中的三项基本要求。安全系统的设计必须保证高度可靠性,以及包括便于定期检查、试验和维修的各项措施。

4.2.4 管理性程序可包括由安全分析报告确定的安全运行限值及条件。由于研究堆的灵活性,所以必须特别注意建立充分的管理性控制和程序。

4.3 设计的安全分析

4.3.1 必须对反应堆的安全进行分析和评价,以论证反应堆具有足够的安全性。安全分析的进展和反应堆设计是相互关联的互补过程。

4.3.2 安全分析报告必须包括反应堆安全分析的结果。

4.3.3 反应堆的安全评价必须包括分析反应堆对一系列可能导致预计运行事件或事故工况的假设始发事件^①(例如设备的误动作或故障、运行人员误操作或外部事件)的响应,也应包括实验装置本身的安全及其对反应堆的影响。这些分析必须作为确定反应堆运行限值及条件的基础。在制定运行程序、定期试验和检查大纲、记录保管程序、维修大纲、修改建议和应急计划时,若条件许可,也应利用这些分析。

4.3.4 假设始发事件必须包括影响反应堆安全的所有可信事故,特别是应确定设计基准事故。对超设计基准事故必须进行分析,以便制定应急计划及进行事故处理。

4.3.5 至少必须参照本规定附件中的一览表拟定分析用的假设始发事件。

4.3.6 必须以下列方式分析假设始发事件及其后果:

(1)事故按类型分组,以便只对每组中的极限事件进行定量分析;

^① 参见 HAF102 之附件 A。

(2)说明极限事件的进程及其可能的后果;

(3)论证与反应堆运行有关的风险及安全裕量是可接受的。

4.3.7 对每一假设始发事件,在评定时必须考虑下列问题的定性及定量资料:

(1)输入参数、初始条件、边界条件、假设、模型和所使用的计算机程序;

(2)事件序列和反应堆系统的性能;

(3)对单一故障模式和共因故障的敏感性;

(4)对人为因素的敏感性;

(5)裂变产物释放及引起照射的可能性。

4.3.8 对所考虑的每一事故序列,必须说明在事故工况下要求安全系统和任何未失效的工艺系统执行功能的程度。

4.3.9 通常用确定论法来评价这些事件,概率论法应作为评价的补充。这些补充分析的结果应作为安全系统的设计及其功能要求的依据。概率论法的评价也可发现设计中仍可能有的薄弱点。

4.4 参数的设计限值

4.4.1 必须对反应堆的每一种运行状态及事故工况规定有关参数的设计限值,这些限值必须能确保在运行状态及事故工况下,堆芯不会发生明显的损坏,并且放射性物质的释放将在所规定的辐射防护要求的范围内。

4.4.2 必须对事件序列进行比较,以确定各个系统及部件设计的最关键的参数,同时还必须包括对各项实验的考虑。所得之限制参数值必须以合理的裕量用于各个系统和部件的设计。

4.5 安全功能

4.5.1 安全功能是与确保反应堆安全的系统相关的基本特

征。安全功能必须根据具体的反应堆设计来确定^①。需在正常运行时执行安全功能的设备为运行系统,通常这些系统还必须由专设安全设施加以补充,以便在预计运行事件和事故工况下完成其功能。

4.6 可靠性设计^②

4.6.1 为保证执行安全功能所需的可靠性,对某些安全系统或部件应确定其最大不可利用率限值,经国家核安全部门认可后,作为基准或用作验收准则。

4.6.2 为达到和保持按系统和部件执行安全功能的重要性所要求的可靠性,应采用下列各项措施,必要时可组合使用。

4.6.2.1 多重性和单一故障准则

多重性原则应作为提高安全重要系统可靠性的重要设计原则。设计必须保证单一故障不会使系统丧失其执行预定安全功能的能力^③。

不能分别进行试验的多组设备,不应看作具有多重性。

所采用的多重性的程度必须考虑会降低可靠性的不可探测故障的可能性^④。

4.6.2.2 多样性

多样性原则能减少共因故障的可能,从而可提高可靠性。只要切实可行,就应采用这一原则。

4.6.2.3 独立性

若条件许可,必须采用独立性原则(如功能独立或依靠距离、屏障或反应堆部件的布置来实现的实体隔离),以提高系统的可靠性,尤其是发生共因故障时的可靠性。

① 选定的安全功能一览表列于本规定附录中,这些安全功能与安全重要的物项有关,其具体的设计要求列在第五章中。

② 参见 HAF102。

③ 参见 HAJ0006。

④ 凡无法用试验或检查方法发现的潜在故障,则必须看作为不可探测故障。

4.6.2.4 故障安全设计

在设计安全重要部件时,在切实可行的情况下应贯彻故障—安全原则,即系统或部件发生故障时,反应堆应能在毋需任何触发动作的情况下进入安全状态。

4.6.2.5 可试验性

反应堆所有部件的设计及布置,均必须能根据其安全重要性在条件许可的情况下进行相应的调试前和调试后的定期检查、试验及维修。如不能满足可试验性要求,则应在安全分析中考虑到此设备的不可探测故障。

4.7 质量保证要求^①

4.7.1 为实现安全总原则,对原始设计和随后在反应堆整个寿期内的设计修改均需采用有计划的、系统化的方法,并必须在批准的质量保证大纲的范围内实施。必须在设计阶段开始时制定概述反应堆设计要求的质量保证大纲,并由营运单位实施。必须根据此大纲制定每一系统、构筑物 and 部件的更详细的实施程序,以始终确保反应堆的设计质量。

4.7.2 HAF003 和 HAD003/06 为核动力堆规定了制定设计质量保证大纲的原则和目标。在制定研究堆设计质量保证大纲时应按不同程度来考虑上述两个文件的总原则,但对某一特定的反应堆的设计所要求的质量保证大纲的详细程度将取决于反应堆的潜在危险性及国家核安全管理要求。

4.7.3 营运单位必须确定安全设计重要的物项、服务和程序,将它们列入质量保证大纲,并要特别注意安全重要物项。设计的组织机构、设计人员的资格、各类活动的管理及设计质量保证的分级均包括在质量保证大纲的要求中。还应建立下列各项程序:有关各方之间的信息交换、文件控制、采购控制、设备及器材控制、材料工艺控制、检查和试验控制、不符合项控制、纠正措施、审评、

^① 参见 HAF202《研究堆运行安全规定》。

准则的确定、质量级的规定、设计验证、监查和程序修订的控制。

4.8 规范和标准

4.8.1 必须确定适用于系统、构筑物和部件的规范和标准,并证明使用是正确的。特别在同一物项或系统的不同方面采用不同的规范和标准时,必须论证其一致性。规范和标准所涉及的典型领域如下:

- (1)机械设计;
- (2)结构设计;
- (3)抗震设计;
- (4)材料的选择;
- (5)设备和部件的制造;
- (6)制造完工的和安装完毕的系统、部件和构筑物的检查;
- (7)热工水力和核设计;
- (8)电气设计;
- (9)仪表和控制系统设计;
- (10)屏蔽和辐射防护;
- (11)防火;
- (12)与设计有关的检查、试验和维修。

4.8.2 对尚无有关规范或标准的系统、构筑物和部件,可引用类似设备的现有规范或标准。如果也没有这类规范和标准时,可应用经验、试验、分析或其综合结果,但必须论证其正确性。

4.9 实验应用中要特别考虑的问题

4.9.1 需特别考虑实验设备的故障,因为故障可能引起下列后果:

- (1)可能的直接危险;
- (2)通过对研究堆安全运行的影响而引起的间接危险;
- (3)通过其后续故障和对事件序列的影响而增加反应堆始发事件的危险。

4.9.2 研究堆的利用和运行的变化很大,同时反应堆的堆芯

和辐照装置又易于接近,因此随堆型不同可能造成特殊的潜在辐照危险。

4.9.3 由于某些研究堆的灵活性及运行状态的多变性,因此在设计中需采用特殊预防措施,以避免人为差错。

4.9.4 对可能显著影响安全的每一项新实验或反应堆的修改,必须遵循 HAF202《研究堆运行安全规定》中所要求的各项程序。

4.10 运行状态的设计要求

4.10.1 基本设计

研究堆必须设计成能在所有运行状态下按所设定的参数范围安全运行,并且反应堆及其相关系统对广泛的事件的响应必须能导致安全运行或在必要时使功率降低,而无需借助于安全系统。

4.10.2 人为因素

在设计初期和整个设计过程中,必须系统地考虑人为因素和人机接口问题。人为因素是研究堆安全要求的一个重要方面,因为反应堆的状态经常变化,并且运行人员又要较多地接近堆芯和实验设备。控制室的设计应贯彻人机工效学原则。必须为运行人员提供安全重要参数的清楚显示及声响信号。设计中应考虑尽可能减少对运行人员的要求,以提高其操作的正确性,同时也应在设计中采取适当的自动化操作,以进一步减轻对运行人员的要求。由于这些人为因素,设计人员必须考虑可能需要实施联锁、信号旁路、键控和指令等措施。

4.10.3 试验和检查

反应堆的设计必须能对所有安全重要物项进行必要的功能试验和检查,以确保这些系统在需要时执行其安全功能。这对于非能动部件和不能以日常运行来验证其功能的系统是特别重要的。必须考虑的重要因素为实施试验和检查的可实施性,以及试验和检查能代表真实情况的程度。如有可能和需要时,在电器和电子系统中应设置自检电路。

4.10.4 维护和修理

设计必须采取措施,以提供适当的可达性、足够的屏蔽、远距离操作和去污,以便于维护和修理。

4.10.5 材料选择

在设计阶段,为适应材料在其使用寿命末的预计特性,应留有适当的安全裕度。当无材料数据可取时,必须执行合适的材料监督计划,并用所得结果对设计的适宜性作定期评价。这可能要求采取设计措施,以监测那些在服役中会由于应力腐蚀或辐射等引起机械性能改变的材料。选用高强度或高熔点材料可提高其安全系数。

4.11 事故工况的设计要求

4.11.1 当需要以迅速而可靠的动作来响应假设始发事件时,反应堆设计必须设置自动触发装置,以使必要的安全系统动作。事故发生后,在某些情况下可能需要运行人员采取进一步的行动以使反应堆处于长期稳定状态。设计应尽可能减少对运行人员的要求,特别是在事故工况期间和事故后(参见 5.6)。

4.11.2 对所有假设始发事件,反应堆保护系统必须能自动触发所需的保护动作以安全地终止事件。这种能力应考虑到系统部件的可能失效(单一故障准则)。在某些情况下,运行人员的手动可认为是充分可靠的,但要具备下列条件:

- (1)时间足够;
- (2)信息的处理和提供恰当;
- (3)诊断简单,并且操作的规定明确;
- (4)对运行人员的要求不过分。

4.11.3 安全重要物项的设计应能经受事故工况所产生的极端荷载和环境条件(例如:极端的温度、湿度、辐射)的影响。事故后长期稳定停堆状态可能不同于起始停堆状态,所以设计中必须采取措施,使反应堆达到长期稳定停堆状态。

4.11.4 必须提供监测手段,以便在事故期间和事故以后对

所有重要的过程和设备进行监测。必要时,必须设置远距离监测及停堆手段。

4.11.5 保护系统必须独立于控制系统。

4.12 辐射防护

4.12.1 设计必须根据 2.1 节中的总体辐射防护目标,在所有运行状态和事故工况下,为屏蔽、通风、过滤和衰变系统以及为辐射和气载放射性物质监测仪表制定足够的措施。

4.12.2 最大设计剂量水平的确定必须留有足够裕量。在所有运行状态和事故工况下,反应堆及其相关设施的屏蔽、通风、过滤和衰变系统必须考虑到运行中的不确定性(满足 2.1 节的要求)。

4.12.3 必须仔细选用结构材料,特别是堆芯附近的材料,以使工作人员在完成运行、检查、维修以及其它职能期间所受的剂量最小。在制订厂区人员和公众的辐射防护措施时,必须考虑到反应堆工艺系统中由中子活化所产生的放射性核素(如 ^{16}N 、 ^3H 、 ^{41}Ar 、 ^{24}Na 、 ^{60}Co)的影响。

4.12.4 设计必须为进入放射性水平超过正常允许值的区域提供必要控制措施。

4.13 实物保护

设计中必须采取充分的措施,以防止未经批准而进入厂区或厂房。主要目的是防止核材料的失窃或未经批准的移动,以及防止对反应堆的破坏。

4.14 调试

设计中应增加便于反应堆调试所必需的设计性能。

4.15 运行限值和条件^①

必须制定详细的反应堆运行限值和条件。运行限值和条件必须经国家核安全局批准。

① 参看 HAF202《研究堆运行安全规定》。

4.16 应急计划^①

必须根据反应堆的潜在危险考虑应急计划所需的设计特征,包括设置有应急照明的简捷的撤离路线、可靠的通讯手段和特殊的辐射监测仪表。需要时,也必须考虑与反应堆控制室分开的应急中心。

4.17 退役^②

在反应堆设计中,必须注意便于退役的有关因素。为此,必须注意使工作人员和公众在退役期间所受的照射符合合理可行尽量低的原则,并确保环境免受放射性污染。

5 具体设计要求

5.1 概述

第四章给出的设计总要求必须与本章给出的要求结合使用,以确定特定反应堆的具体设计要求。应该认为,不同类型的反应堆可能只须满足本章中的某些要求。是否可不执行本章中的一些具体设计要求的主要准则仍然是要考虑在运行状态和事故工况下,厂区工作人员和公众所受辐射照射的可接受性。此外,还必须考虑防御外部事件。

5.2 厂房和构筑物

5.2.1 安全重要的厂房和构筑物的设计必须考虑所有运行状态。但是,这些物项可能构成对付事故工况的专设安全设施,在5.8节给出了对厂房和构筑物的具体要求。

5.2.2 厂房和构筑物的设计必须能在所有运行状态下保持厂区内外的辐射水平及放射性释放符合合理可行尽量低的原则,

① 参看 HAF202/2《研究堆运行安全规定》。

② 参看 HAD202/03《研究堆和临界装置退役》。

并低于所规定的限值。

5.2.3 反应堆厂房或其它包容放射性物质的厂房和构筑物(如:游泳池堆的水池)的密封性及对通风系统的要求必须根据反应堆及其应用的安全分析结果来确定。

5.3 反应堆堆芯设计和控制

5.3.1 反应堆堆芯

5.3.1.1 燃料和燃料元件的设计必须全面考虑与反应堆有关的中子学、热工水力学、机械、材料、化学和辐照等限制因素。

5.3.1.2 反应堆堆芯的设计必须使其在事故工况下的燃料损坏保持在可接受的限值范围内。

5.3.1.3 反应堆堆芯(包括燃料元件或组件,反应性控制机构^①和实验装置等)的设计及建造必须使所有运行状态下规定的最大允许设计限值不会被超过。

5.3.1.4 反应堆的设计必须使反应堆能在所有运行状态及事故工况下停堆,并维持在次临界状态。

5.3.1.5 反应堆堆芯设计应尽可能采用固有安全特性,以将事故后果减至最小。

5.3.2 反应性控制系统

5.3.2.1 反应性控制机构必须有足够的负反应性,以便在实验布置具有最大的正反应性时,也能使反应堆在所有运行状态下进入次临界并维持在次临界状态。如果反应性控制机构起反应堆停堆系统的作用,则要满足 5.5 节的要求;如果除停堆系统外,反应性控制机构又起补偿或调节系统的作用,则也希望能满足此要求。

5.3.2.2 必须规定反应性控制系统或实验允许的最大正反应性引入速率,并将其值限制在安全分析报告所论证的范围内。

^① 反应性控制机构包括控制反应性的各种装置,即调节棒、控制棒、停堆棒和慢化剂的液位控制装置。

5.3.3 热工水力设计

5.3.3.1 反应堆堆芯(即燃料元件、冷却剂流道的几何形状、结构部件等)的设计必须能使其在所有运行状态下将燃料参数保持在所规定的限值内,从而不引起燃料破损。

5.3.3.2 确定这些限值时,必须考虑合适的裕量,包括误差及设计允许公差裕量。

5.4 反应堆冷却剂系统

5.4.1 反应堆冷却剂系统的设计必须使其能提供充分的堆芯冷却,并留有在安全分析报告中论证过的可接受的裕量。

5.4.2 冷却剂系统应能进行试验或监督,以防泄漏、快速增长的裂纹及脆裂的发生。可根据具体情况应用多层屏障原则(例如:一回路冷却系统可全部放在水池里,或用特殊的布置来对付潜在的破口)。

5.4.3 在堆芯高度的上水平面以下有贯穿件的水冷反应堆的设计中,必须特别注意防止堆芯裸露,应采取特殊措施(如破坏虹吸)和合适的隔离装置。高质量的设计和制造、可检查性和可试验性以及条件许可的地方应用多重性原则均为必须具备的特征。

5.4.4 反应堆冷却剂边界的设计必须便于所需的役前检查和在役检查及试验。

5.4.5 除主冷却系统外,还必须设置一个独立的充分可靠的余热排除系统。

5.4.6 对于采用瓣阀或相当的系统进行自然冷却的反应堆系统,必须应用适当数量的多重装置,并必须提供用以证实这些系统在需要时能起作用的方法。

5.4.7 反应堆冷却系统必须能长期可靠地把热量从燃料传导到最终热阱。

5.5 反应堆停堆系统

5.5.1 设计中必须至少采用一套停堆系统。根据反应堆的

特征,必须考虑并可能需要第二套独立的停堆系统。

5.5.2 停堆系统必须具有足够的停堆反应性,以便在所有运行状态及事故工况下,即使考虑到实验的反应性影响,也能使反应堆进入次临界,并维持在有足够停堆深度的次临界状态。

5.5.3 反应堆停堆系统的有效性、动作速度及停堆深度必须使所规定的限值 and 条件不会被超过。

5.5.4 停堆系统的单一故障不得阻碍该系统在需要时实现其安全功能。

5.5.5 停堆系统除自动触发外,还必须设置手动触发装置,同时也必须设置一个或多个适合应急停堆的手动触发装置。

5.6 保护系统

5.6.1 反应堆保护系统必须是自动的,并且独立于其它系统。此外,必须使手动停堆信号能输入到保护系统中去。

5.6.2 保护系统的设计应能保证当此系统一旦触发其必要的动作就不受手动操作的影响或阻碍,并且在事故发生后的短时间内不需要手动操作。

5.6.3 保护系统的设计应贯彻多样性原则,如可能,对每一个假设始发事件都至少用两种不同的方法加以探测。所需的保护动作必须自动触发。

5.6.4 保护系统必须至少有两套完全隔离的和独立的通道,以使单一故障不致于导致其功能的丧失。

5.6.5 保护系统的设计必须确保在保护系统出现共因故障时使反应堆处于安全状态。

5.6.6 保护系统的所有部件必须能进行功能试验。

5.6.7 保护系统一旦触发,相关的动作必须进行到完成为止。这些动作不得自行复位,只有运行人员有意识的操作才能使它恢复运行。

5.6.8 设计必须保证整定值的触发点和安全限值之间有一定的裕量,即保护系统触发的动作能在达到安全限值前起到控制

该过程的作用。此外,此裕量必须考虑下列因素:

- (1)仪表的不准确度;
- (2)刻度的不确定性;
- (3)仪器的飘移;
- (4)仪器和系统的响应时间。

为了增加安全性,可再增大裕量。

5.6.9 应采用适当手段,防止安全重要的联锁和保护停堆发生旁路。在安全分析报告中必须对联锁和保护停堆旁路的可能性进行慎密的评价。

5.7 应急堆芯冷却系统^①

5.7.1 应急堆芯冷却系统必须能在所有停堆工况(包括由反应堆冷却剂系统边界破裂造成的工况)下将堆芯温度保持在规定的安全限值内。

5.7.2 在出现安全分析报告中作为设计基准规定的冷却剂丧失事故工况时,应急堆芯冷却系统必须能防止燃料明显损坏。

5.7.3 应急堆芯冷却系统的设计必须有足够的可靠性,能在该系统发生单一故障事件时完成其预定的设计功能。

5.7.4 应急堆芯冷却系统的设计必须能使其部件便于进行定期检查,并能进行适当的定期功能试验,以验证安全分析报告中所规定的性能。

5.8 包容系统^②

5.8.1 本规定中,术语“反应堆厂房”包括反应堆厂房的构筑物、通风系统和贯穿件以及任何其它起重要包容功能的设施。

5.8.2 根据反应堆的潜在危险性,反应堆厂房的设计必须考虑事故工况下的极端荷载和环境条件的影响,包括附件中第6、7项列出的内部和外部事件引起的事故。

① 这些系统通常称为专设安全设施。

② 这些系统通常称为专设安全设施。

5.8.3 反应堆厂房的设计必须有适当的裕量,以承受设计基准事故工况下算得的最高压力和温度。

5.8.4 反应堆厂房的设计必须能可靠地控制正常运行工况下放射性物质的释放。

5.8.5 必须确立事故工况下可接受的放射性物质的释放率。这时要考虑某些类型反应堆可能存在的挥发性放射性物质的总含量以及与那些作为设计基准并为国家核安全部门所接受的最不利的事故工况有关的其它参数(如压力、温度)。

5.8.6 如果规定了反应堆厂房在给定压力下的泄漏率,则设计必须具有能进行初始的及定期的泄漏试验的特点。

5.8.7 必须制订措施以进行通风系统中过滤器的例行试验及更换。

5.9 仪表和控制

5.9.1 必须作好仪表和显示装置的选择及布置,并考虑人机工效学原则,为运行人员获取信息和采取恰当的安全相关的行动提供最佳条件,以减少运行人员误操作的可能。通常,应集中布置在有足够装备的反应堆控制室里。必须采取适当措施,以使控制室的人员得到保护。

5.9.2 反应堆必须设置足够的仪表,以监测反应堆在正常运行、换料和维修期间的运行和工艺系统,并记录所有安全重要的变量。

5.9.3 反应堆必须设置足够的指示和记录仪表,以监测反应堆在预期运行事件和事故工况期间及之后的重要参数。某些参数还可能在多处进行监测和记录。

5.9.4 设计应考虑在适当的条件下启动中子源及专用启动仪表的需要。

5.9.5 声光报警系统必须能早期指示可能导致反应堆安全性下降的运行工况的变化。

5.9.6 设计必须提供足够的措施,以便对安全相关仪表进行

定期检查、试验和维修。

5.10 电源系统

5.10.1 必须确定正常和应急电源设计的基准,其中必须包括在一切事故工况下向执行基本功能部件(如保护系统、仪表、应急照明等)供电的要求。

5.10.2 当冷却剂循环泵、应急通风系统或其他安全重要系统需要应急电源时,应急供电系统必须有足够的可靠性,以保证连续供电^①。

5.10.3 必须规定直流和交流电源的最大的可接受的中断时间,并在安全分析报告中论证其可接受性。

5.10.4 应急电源系统的设计必须考虑到由此系统供电的各种设备的启动负荷要求。

5.10.5 设计必须为应急电源供应系统提供适当的功能试验手段。

5.11 辅助系统

5.11.1 不论辅助系统对安全的重要性如何,其失效均不得危害反应堆的安全。必须采取足够的措施,以防止含放射性物质的辅助系统失效时放射性物质向环境的释放。

5.11.2 燃料的操作和贮存设施的设计必须考虑防止发生燃料的丢失和损坏。必须考虑临界、冷却、定期检查和试验、腐蚀、包容、屏蔽和通风问题。

5.11.3 必须在气载放射性物质浓度较高的反应堆区域设置足够的辐射监测系统和通风系统,包括相应的过滤装置。

5.11.4 设计中必须采取适当的防火和防爆措施,并在一旦发生失火、爆炸时防止其影响。应特别注意安全重要物项的防火和防爆^②。

① 参见 HAD102/13。

② 参见 HAD102/11。

5.11.5 必须提供足够的通讯系统,以保证反应堆和实验设施的安全。

5.12 实验装置

5.12.1 实验装置的设计必须能使其在所有运行状态下,不会对反应堆、其它实验、厂区人员或公众造成不可接受的后果,在设计中必须考虑实验装置内所含的放射性总量以及能量产生或释放的可能性。

5.12.2 实验设备的设计必须保证运行和失效均不会对反应堆造成不可接受的反应性变化。

5.12.3 必要时,应在反应堆控制室设置适当的实验参数监测仪表,以保证反应堆的安全。

5.12.4 必须对每一实验制定运行限值和条件。

5.13 放射性废物系统

5.13.1 研究堆的设计应以产生最少的放射性废物为原则。放射性废物处理系统必须有足够的控制和监测装置,以使放射性物质的释放符合合理可行尽量低的原则,并低于所规定的限值。

5.13.2 设计中必须考虑适当的手段(如屏蔽和衰变系统)以减少工作人员所受剂量和减少放射性向环境的释放。

5.13.3 设计必须提供足够的放射性向环境排放的控制、取样和监测手段。

5.13.4 必要时,设计要为放射性废物的输送、收集、处理、贮存、处置或从厂区转移等提供适当的装置。输送液体废物时,还必须有检漏及废物回收措施。

名 词 解 释

本规定中下列名词术语的含义为:

可接受限值

国家核安全部门认可的限值。

事故工况

以偏离运行状态形式出现的事故。事故工况下放射性物质的释放可由恰当设计的设施限制在可接受限值以内。严重事故^①不在其例。

预计运行事件

反应堆运行寿期内预计可能出现一次或数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,这类事件不致于引起安全重要物项的严重损坏,也不导致事故工况。

调试

反应堆已安装的部件和系统投入运行并按设计要求进行性能验证,以确认是否满足性能标准的过程。调试由反应堆装载燃料前和反应堆进入临界、链式裂变反应在持续进行中两种条件下的试验组成。

共因故障

由特定的单一事件或起因导致若干装置或功能失效的故障^②。

包容

包围含放射性物质的反应堆主要部件的屏障,设计用以防止和缓解在运行状态或设计基准事故中放射性物质向环境的失控释放^③。

临界装置

一个具有足够可裂变材料和其它材料的装置,用以在低功率水平维持可控链式反应,并为研究堆芯布置及组成提供条件。

① 严重事故属于超设计基准事故。

② 例如设计缺陷、制造缺陷、运行和维修差错、自然事件、人为事故、信号饱和或源自其他操作、故障或环境条件改变的意外的级联效应。

③ 如果其设计也能在事故后的超压条件下完成其功能,则常称其为安全壳。

退役

反应堆最终退出运行的过程。

设计基准事故

研究堆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。

多样性

为某一确定功能设置多重部件或系统,这些部件或系统总起来说具有一个或几个不同属性^①。

排出流

释放到环境中的流体(液体或气体),流体中可能含固体微粒。

专设安全设施

(见安全系统)

实验装置

装在堆内或反应堆周围,利用反应堆中子通量和电离辐射束进行研究、开发、同位素生产以及其它工作的装置。

燃料(核燃料)

用于核反应堆中产生中子的含可裂变材料和可转换材料的化学混合元件。

燃料组件

作为一个整体装入堆芯,尔后又自堆芯撤除的燃料元件组。

燃料元件

以燃料为其主要组成部分的最小独立结构体。

维修

保持设备处于良好工作状态的活动,包括预防性的和纠正(或修理)性的两个方面。

正常运行

^① 不同属性的例子有:不同的运行条件、大小不等的设备、不同的制造厂、不同的工作原理以及基于不同物理方法或规律的不同类型的设备。

研究堆及其相关实验装置的运行,包括启动、功率运行、停堆过程、停堆状态、维护、试验和换料(参见运行状态)。

营运单位

持有国家核安全部门许可证(执照),负责经营和运行反应堆设施的单位。

运行限值和条件

经国家核安全部门认可的,为研究堆设施的安全运行而列举参数限值、设备的功能和性能及人员执行任务的水平等一整套规定。

运行状态

正常运行或预计运行事件两类状态的统称。

假设始发事件

经鉴别可能导致预计运行事件或事故工况及其后续故障效应的事件^①。

保护系统

由各种电器件、机械器件和线路(从传感器到执行机构的输入端)组成的产生与保护功能相联系的信号系统。

质量保证

为使物项或服务与规定的质量要求相符合并提供足够的置信度所必需的一系列有计划系统化的活动。

反应堆运行管理机构

由营运单位委任的负责指挥研究堆设施运行、并承担直接安全责任的机构。

多重性

通过设置数量高于最低需要的单元或系统(相同的或不同

^① 假设始发事件的主要原因有:可信的设备故障和操作人员差错(反应堆设施内外)、人为事件或自然事件。研究堆设施始发事件的清单(明细表)必须经国家核安全部门认可。

的),以达到任一单元或系统的失效不致于引起所需总体安全功能丧失的措施。

研究堆^①

主要用于产生和利用中子注量率和电离辐射作研究和其它目的用的核反应堆。

核安全(安全)

完成正确的运行工况、事故预防或缓解事故后果从而实现保护厂区人员、公众和环境免受过量辐射危害。

安全功能

为安全着想必须完成的特定目的。

安全限值

过程变量的各种限值,研究堆设施在这些范围内运行已证明是安全的。

安全裕度

安全限值与运行限值之间的差值,有时也用两限值之比表示。

安全相关物项或系统

不属于安全系统的安全重要物项或系统。

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和事故工况时启动有关自动保护装置的触发点。

安全系统^②

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事故工况的后果。

停堆裕度

当具有最大负反应性的控制装置移出堆芯和所有在运行期间

① 本规定中,研究堆也包括相关的实验设施以及临界装置。

② 安全系统的功能由来自保护系统的信号或手动触发。安全系统的某些设施称为专设安全设施,特别是涉及应急排热和包容。

可以改变位置或修改的实验处于最大反应性工况时,除维持反应堆无限期处于次临界状态所需的负反应性以外的负反应性。

停堆反应性

反应堆由控制装置引入最大负反应性而处于次临界状态时的反应性量。

停堆系统

由手动或由保护系统来以信号触发,并使反应性快速下降而执行停堆所需的系统。

单一故障

导致某一部件不能执行其预定安全功能的一种随机故障,由单一随机事件引起和各种继发故障,均视作单一故障的组成部分。

厂址、厂区

具有确定的边界,在反应堆运行管理机构有效控制下的反应堆所在区域。

附 件

典型的假设始发事件

1. 电源丧失

正常电源丧失。

2. 过量反应性引入

- (1)燃料装卸时达临界(燃料插入错误);
- (2)启动事故;
- (3)控制棒或控制棒随动体故障;
- (4)控制驱动或系统故障;
- (5)其它反应性控制装置(慢化剂、反射层等)故障;
- (6)棒位错乱;
- (7)结构部件故障或倒塌;

- (8)冷水引入;
- (9)慢化剂变化(如空泡、重水漏入轻水系统,等等);
- (10)实验和实验设施的影响(如溢流或形成空泡、温度影响、易裂变物质或吸收物质的引入或移出等);
- (11)停堆反应性不足;
- (12)意外的控制棒弹出;
- (13)反应性装置维修错误。

3. 流量丧失

- (1)主泵故障;
- (2)主冷却剂流量减少(如阀门故障、管道或热交换器堵塞);
- (3)实验故障或误操作的影响;
- (4)应急冷却系统故障;
- (5)主冷却剂边界破裂导致流量丧失;
- (6)燃料通道堵塞;
- (7)由于棒位错乱、堆芯内实验或装料引起的不合适的功率分布;
- (8)由于堆芯旁路引起的冷却剂减少;
- (9)反应堆功率控制故障;
- (10)系统压力偏离规定限值;
- (11)热阱丧失(如阀或泵故障、系统破裂)。

4. 冷却剂丧失

- (1)主冷却剂边界破裂;
- (2)水池破损;
- (3)水池吸空;
- (4)射线束管及其它贯穿件破损。

5. 设备或部件的误操作或故障

- (1)燃料元件包壳破损;
- (2)堆芯或燃料机械损伤(如燃料装卸、转运罐跌落在燃料上等);

- (3)燃料贮存中的临界;
- (4)安全壳或通风系统故障;
- (5)燃料转移或贮存时冷却剂丧失;
- (6)正常屏蔽的丧失或减少;
- (7)实验设备或材料故障(如回路破裂);
- (8)超过燃料的额定值。

6. 特殊的内部事件

- (1)内部火灾或爆炸;
- (2)内部水淹;
- (3)支撑系统丧失;
- (4)保卫事故;
- (5)反应堆实验误动作;
- (6)误入限制区。

7. 外部事件

- (1)地震(包括地震诱导的断层、滑坡和海啸);
- (2)水灾(包括上游溃坝、江河堵塞);
- (3)龙卷风和龙卷风飞射物;
- (4)飓风、风暴和闪电;
- (5)爆炸;
- (6)飞机撞击;
- (7)火灾;
- (8)毒物泄漏;
- (9)运输路线事故;
- (10)附近设施的影响。

8. 人为差错

附录 典型的安全功能^{*}

安全重要物项	安全功能
厂房和构筑物	(1)形成屏障,以防止放射性物质向环境的不可控释放; (2)防止内、外部事件对所包容的安全系统的影响; (3)作为辐射屏蔽。
反应堆堆芯	(1)维持燃料几何形状及必要的冷却剂流道,以确保在反应堆所有运行工况下的停堆及热量排除; (2)提供负反应性反馈; (3)提供慢化和控制中子通量的手段。
燃料基体和包壳	(1)形成屏障,以防止裂变产物从燃料中释放; (2)提供固定不变的排列。
反应性控制系统 (包括反应堆停堆系统)	控制反应堆堆芯反应性,以确保反应堆在任何运行状态下都能安全停堆,并且不超过燃料设计和其它限值。
反应堆冷却剂主回路	提供充分的堆芯冷却,并确保在反应堆任何运行状态下都不超过其规定的燃料和冷却剂限值。
应急堆芯冷却系统	冷却剂丧失事故后,以足够的速率将热量从反应堆堆芯排出,防止发生明显的燃料破损。
通风系统	(1)控制及尽量减少气载放射性排出流向环境的释放; (2)防止运行人员和研究人员受到过量辐照; (3)必要时,在包容系统的不同区域之间维持足够的压差; (4)为工作人员和安全重要物项提供合适的环境条件。

(续)

安全重要物项	安全功能
保护系统	(1)启动保护动作,以便停堆、冷却、包容放射性物质和缓解事故的后果; (2)在条件不满足时,控制联锁机构以防止操作错误。
其它安全相关 仪表和控制	(1)使反应堆各参数保持在运行限值之内而不达到安全限值; (2)为运行人员提供足够信息,以便确定保护系统的状态,并采取正确的安全相关的行动。
电 源	向系统和设备提供充足的、质量合格的电力,以确保它们在需要时有执行其安全功能的能力。
燃料操作和贮存系统	(1)尽量减少辐照; (2)防止意外临界; (3)限制燃料温度上升; (4)贮存新燃料及辐照过的燃料; (5)防止燃料的机械或腐蚀损坏。
辐射监测	提供测量及报警,以尽量减少运行人员和研究人员所受的辐照。
防 火	保证不使火灾和爆炸的有害影响妨碍安全重要物项在需要时完成其安全功能。

* 在此列出的安全功能并非全部适用于各类研究堆。