ICS 27.120.20
CCS F 65

中华人民共和国国家标准

GB/T 41090—2021

能动安全系统压水堆核电厂总设计要求

General design requirements of pressurized water reactor nuclear power plants with active safety systems

2021-12-31 发布　　2022-07-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国核能标准化技术委员会(SAC/TC 58)提出并归口。

本文件起草单位：中国核电工程有限公司。

本文件主要起草人：邢继、袁霞、范黎、张雪霜、李辉、李崇。

能动安全系统压水堆核电厂总设计要求

1 范围

本文件规定了能动安全系统压水堆核电厂(以下简称“核电厂”)的总体设计基本要求,以确保其可以安全、可靠地运行。

本文件适用于新建的能动安全系统压水堆核电厂,在役的能动安全系统压水堆核电厂可参考执行。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB 6249 核动力厂环境辐射防护规定

GB 11806 放射性物质安全运输规程

GB 18871 电离辐射防护与辐射源安全基本标准

NB/T 20035 压水堆核电厂工况分类

HAD 002/01—2019 核动力厂营运单位的应急准备和应急响应

HAF 102 核动力厂设计安全规定

3 术语和定义

下列术语和定义适用于本文件。

3.1

安全系统 safety system

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。

[来源:HAF 102—2016,名词解释]

3.2

能动安全系统 active safety system

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后果的能动系统。

[来源:GB/T 35730—2017,3.3,有修改]

3.3

能动安全系统压水堆核电厂 pressurized water reactor nuclear power plants with active safety systems

主要依赖能动安全系统完成设计基准事故内全部安全功能的压水堆核电厂。

注:简称“能动核电厂”。

[来源:GB/T 35730—2017,3.4,有修改]

3.4

安全功能 safety function

为了保证设施或活动能够预防和缓解核电厂正常运行、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。

[来源:HAF 102—2016,名词解释,有修改]

3.5

安全重要物项　items important to safety

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。

注:安全重要物项包括:安全有关系统、安全系统和用于设计扩展工况的安全设施。

[来源:HAF 102—2016,名词解释,有修改]

3.6

安全组合　safety group

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。

[来源:HAF 102—2016,名词解释]

3.7

事故工况　accident condition

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。

注:事故工况包括设计基准事故和设计扩展工况。

[来源:HAF 102—2016,名词解释,有修改]

3.8

设计基准事故　design basis accident

导致核电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,该核电厂是按确定的设计准则和保守的方法来设计的。

[来源:HAF 102—2016,名词解释,有修改]

3.9

设计扩展工况　design extension condition

不在设计基准事故考虑范围的事故工况,在设计过程中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。

注: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。

[来源:HAF 102—2016,名词解释,有修改]

3.10

严重事故　severe accident

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。

[来源:HAF 102—2016,名词解释]

3.11

安全状态　safe state

核电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。

[来源:HAF 102—2016,名词解释,有修改]

3.12

用于设计扩展工况的安全设施　safety features for design extension conditions

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。

[来源:HAF 102—2016,名词解释]

3.13

陡边效应　cliff edge effect

在核电厂中,由微小变化的输入引发核电厂工况的重大突变。

注：例如，由参数微小的偏离导致核电厂从一种状态突变到另一种状态的严重异常行为。

[来源：HAF 102—2016，名词解释，有修改]

3.14

大量放射性释放　a large radioactive release

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。

[来源：HAF 102—2016，名词解释]

3.15

早期放射性释放　an early radioactive release

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。

[来源：HAF 102—2016，名词解释]

3.16

实际消除　practically eliminated

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。

[来源：HAF 102—2016，名词解释]

3.17

单一故障　single failure

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。

[来源：HAF 102—2016，名词解释]

3.18

共因故障　common cause failure

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。

[来源：HAF 102—2016，名词解释]

3.19

多样性　diversity

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。

[来源：HAF 102—2016，名词解释]

3.20

实体隔离　physical separation

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。

[来源：HAF 102—2016，名词解释]

4　核电厂设计目标

4.1　核安全设计目标

4.1.1　基本安全目标

基本安全目标：在核电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。

为了实现基本安全目标，应采取以下措施：

a)　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；

b)　限制导致核电厂反应堆堆芯、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；

c) 如果上述事件发生，减轻这些事件产生的后果。

基本安全目标适用于核电厂的所有活动，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。

为了满足上述基本安全目标，能动核电厂应符合 HAF 102 对安全设计和辐射防护设计提出的总体目标要求。

具体的安全目标应按照下列标准执行：

a) GB 18871；

b) GB 6249；

c) GB 11806。

4.1.2 概率安全目标

应满足如下定量的概率安全目标：

a) 堆芯损坏频率应不高于 10^{-5}/堆年；

b) 大量放射性物质释放频率应不高于 10^{-6}/堆年。

4.1.3 其他安全指标

核电厂设计应保证在正常运行过程中，单台百万千瓦级电功率机组的废物包体积年产生量不超过 50 m^3。

核电厂设计应保证在核电厂整个寿期内的正常运行过程中，单台机组年平均集体职业照射剂量应小于 1 人·Sv。

4.2 总的经济目标

核电厂在设计中需要充分考虑核电厂的建造成本和全寿期发电成本，使其具有市场竞争力。

设计中主要需要考虑的对经济目标有影响的因素包括核电厂设计寿命、核电厂整体的建造周期、核电厂平均可利用率、核电厂非计划性停堆水平、换料周期、考虑厂址环境的条件使能量利用得到优化等。

5 核电厂总体设计要求

5.1 纵深防御设计

5.1.1 应用纵深防御设计的总体要求

核电厂设计应采用纵深防御措施，以提高多层次防御(固有特性、设备及规程)能力。为预防可能对人员和环境产生的有害影响，应贯彻预防和缓解平衡的安全理念，以保证在防护失效的情况下可以通过采取适当的缓解措施减轻事故后果以保护人员和环境。每一独立有效层次的防御都是核电厂纵深防御的基本组成部分，应确保与安全相关的活动能够被纳入独立的纵深防御层次。

纵深防御概念与纵深防御在设计中的应用原则按照 HAF 102 中规定的纵深防御的五个层次的要求执行。

5.1.2 纵深防御独立性设计

纵深防御各个层次之间应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。特别地：

a) 设计用于减轻堆芯熔化事故后果的安全设施尽实际可能独立于用于减轻设计基准事故的设备。

b) 用于缓解设计基准事故的安全系统(处于纵深防御第三层)需要独立于第一层次和第二层次。安全系统执行相应功能的能力不受假设单一始发事件或用于正常运行、预计运行事件的系统失效的影响。

c) 用于设计扩展工况的安全设施作为执行安全功能的构筑物、系统或部件的备用设施时,需设计成独立于在事故序列中已假设失效的构筑物、系统或部件。

5.2 核电厂工况与安全分析

5.2.1 核电厂工况

核电厂工况划分为正常运行、预计运行事件、设计基准事故和设计扩展工况。

每类工况的具体划分原则与工况清单可按照 NB/T 20035 执行。同时,应在工程判断、确定论和概率论评价的基础上得出一套设计扩展工况(包括没有造成堆芯明显损伤的设计扩展工况、堆芯熔化设计扩展工况)。

5.2.2 确定论安全分析

设计中应进行确定论安全分析,并应涵盖 5.2.1 中规定的所有核电厂工况。确定论安全分析的目的是确认:

a) 安全功能能够可靠地执行;

b) 必要的构筑物、系统和部件,结合操纵员动作,足够保证核电厂放射性物质释放低于可接受限值,且具有合适的安全裕度。

确定论安全分析需要证明核电厂放射性屏障在所要求的范围内保持其完整性。确定论安全分析以概率安全分析作为补充后,也应有助于证明:

a) 在不同核电厂工况下,源项和潜在的放射性后果是可接受的;

b) 导致早期放射性释放或大量放射性释放的特定工况可被认为“实际消除”。

不同核电厂工况的确定论安全分析特定分析目标、分析方法、分析假设、陡边效应与不确定性处理以及验收准则,可结合导则中确定论安全分析的相关要求执行。

不同核电厂工况的放射性验收准则应满足 GB 6249 的规定,可采用现实模型和最佳估算方法来评价设计扩展工况。

5.2.3 概率安全分析

在核电厂的设计中,应完成核电厂的概率安全评价,以达到下述目的:

a) 提供系统性的分析,设计中需要适当考虑核电厂所有运行模式和所有状态(包括停堆工况),并将分析结果和已规定的风险准则进行比较;

b) 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(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)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;

c) 确认核电厂参数的小偏离不会引起核电厂性能严重异常(陡边效应);

d) 提供发生堆芯严重损伤状态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概率安全评价;

e) 提供外部危险(特别是核电厂厂址特有的那些外部事件)发生频率和后果的评价;

f) 鉴别出通过设计改进或运行规程的修改可能降低堆芯熔化事故概率或减轻其后果的系统;

g) 评价核电厂应急规程的充分性。

核电厂设计可参考 NB/T 20037(所有部分)进行概率安全评价。

5.2.4 实际消除的论证

设计中应结合确定论安全分析、概率安全分析与工程判断，论证可能导致早期放射性释放或大量放射性释放的工况已被实际消除。实际消除的事件序列包含以下几类：

a) 导致堆芯快速损伤并进而引起安全壳早期失效的事件，如：反应堆冷却剂系统的大型承压部件失效、不可控的反应性事故；

b) 导致安全壳早期失效的严重事故序列，如：安全壳直接加热、大规模蒸汽爆炸、可燃气体爆炸；

c) 导致安全壳晚期失效的严重事故序列，如：堆芯熔融物与混凝土相互作用导致的底板熔穿或安全壳旁通、丧失安全壳排热、可燃气体爆炸；

d) 安全壳旁通的严重事故。

对实际消除可能导致早期放射性释放或大量放射性释放工况的论证，可区分为物理上不可能发生、极不可能发生工况两类进行论证。被认为物理上不可能发生的工况，应审查系统固有安全特性并通过自然法则论证其不会发生；论证极不可能发生的工况时，不应仅基于分析得到的频率值低于选定的截断频率值来论证实际消除。但是，任何概率目标值的实现都不应被认为是不执行合理的设计或运行措施的正当理由。例如，不能以堆芯熔化事故发生的概率低为理由，而不对安全壳采取保护措施以应对严重事故工况。

5.3 安全分级

应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、建造和维修应使其质量和可靠性与这种分级相适应。

核电厂构筑物、系统和部件的安全分级需要综合考虑：该物项要执行的安全功能、未能执行其安全功能的后果、需要该物项执行某一安全功能的可能性、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等因素。

对构筑物、系统和部件进行安全分级的具体方法和流程可参考 HAD 102/03 或 GB/T 17569 的规定执行。安全分级过程主要基于确定论的方法进行，并适当辅以风险指引的概率论方法进行补充。

根据物项的安全分级确定相应的设计要求，如单一故障准则、实体隔离/电气隔离、应急供电、定期试验、危险防护、环境鉴定，以及设计规范的采用以及质量保证要求等。具体要求参考 HAD 102/03 或 GB/T 17569 的规定执行。

5.4 可靠性设计要求

安全重要构筑物、系统和部件应按照最新的或当前适用的规范和标准进行设计；其设计应是此前在相当使用条件下验证过的。

应对核电厂设计中所包括的每个安全组合都应用单一故障准则。单一故障准则的应用原则参考 GB/T 13626 的规定，安全重要流体系统应用单一故障准则的要求参考 NB/T 20402 的规定执行。

设计中需考虑安全重要物项发生共因故障的可能性，以确定应该如何以多样性、多重性、独立性原则来实现所需的可靠性。

a) 对于执行相同安全功能的系统或设备，宜采用多样化的特征以避免发生共因故障，这些特征可能包括不同的运行模式、不同的物理参数、不同的运行条件或来自不同的供应商等。

b) 独立性设计原则：尽实际可能确保冗余系列间的独立性；确保物项与需其投运的假设始发事件之间的独立性；维持不同安全等级物项之间的独立性，确保更低安全等级物项的失效不会影响更高安全等级物项执行其安全功能；尽实际可能确保不同纵深防御层次之间的独立性。独立性设计原则可通过实体隔离、电气隔离和/或功能隔离等措施来实现。

应通过设备鉴定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。设计中考虑的环境条件包括正常运行、预计运行事件、设计基准事故以及设计扩展工况(包括严重事故)环境条件。

需要适当考虑故障安全设计原则,并贯彻到核电厂安全重要系统和部件的设计中。核电厂宜设计成在该系统或部件发生故障时不妨碍预定安全功能的执行。

5.5 危险防护设计要求

5.5.1 总体要求

确定核电厂假设始发事件时需考虑相关厂址特定的内部危险和外部危险的影响(单独或组合)。内部危险和外部危险分析与假设始发事件分析不同。危险本身不作为假设始发事件,但危险可能引起的失效会导致假设始发事件。

对于多机组厂址,为确定厂址特定危险导致的假设始发事件,需考虑该危险同时影响若干或所有机组的可能性,尤其需考虑丧失外电网、丧失最终热阱和共用设备失效的影响。

设计中考虑的危险包括可信的内部危险、设计基准外部危险(外部自然事件和外部人为事件),根据审管部门要求,设计中还需考虑个别选定的超设计基准外部危险,如:商用大飞机的恶意撞击、设计基准洪水位叠加千年一遇降雨。

采用概率论方法或工程判断方法进行危险分析,目的为论证对于每个危险需符合下列条件之一:

a) 由于对风险贡献可忽略,该危险可以筛除;

b) 核电厂设计足够强健,可预防危险产生的荷载导致始发事件;

c) 危险导致的始发事件已被设计中考虑的某一工况所包络。

如果危险导致了始发事件,始发事件分析时应认为只有可抵御危险荷载或不受危险影响的物项可用。在进行此类始发事件分析时,应适用 5.2.2 规定的确定论安全分析要求。

危险分析的总体验收目标原则上应满足:

a) 可信的内部危险后果应被设计基准事故的验收准则所包络,并需尽实际可能不引发设计基准事故工况;

b) 设计基准外部危险后果应被设计基准事故的验收准则所包络,并需尽实际可能不引发设计基准事故工况;

c) 可信的内部危险或设计基准外部危险不会导致冗余安全系列同时丧失安全功能;

d) 设计考虑的超设计基准外部危险后果,应被针对严重事故的验收准则所包络。

核电厂设计应提供适当的裕量,在由厂址评价确定的设计基准外部危险发生时保护安全重要物项,并避免产生陡边效应;同时,在超设计基准外部危险发生时,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。

5.5.2 外部自然事件的防护

安全重要的构筑物、系统和设备应合理地设计以抵抗自然事件的影响,例如在地震、极端风、外部洪水、极端温度等自然事件的影响下不会丧失安全功能。重要的安全构筑物、系统和设备的防护设计基准应:

a) 适当地考虑厂址以及周围地区有历史记载的最严重的自然事件,并在相对精度、数量以及历史数据积累时间跨度上都具有充分裕度;

b) 将正常和事故工况下的荷载与自然事件的荷载进行适当组合;

c) 与其执行的安全功能的重要性相匹配。

厂址应避开高地震活动区和伴随地震活动可能出现地表破裂的危险区,并尽可能选在地震活动水

平低的地区，以降低地震危险性。

应对厂址的工程水文条件进行详细调查，并结合厂址的水文特征，确定可能影响厂址安全的洪水因素，如对于滨海厂址，包括天文潮、风暴潮及波浪、假潮、海啸、海平面异常等因素及其组合，对内陆厂址，包括因降雨、溃坝、河道阻塞等因素及其组合产生的洪水。在确定厂址设计基准洪水位的评价中，需考虑极端洪水事件及洪水事件组合的影响。对于厂区排水需考虑可能最大降雨产生的影响，而且要考虑适当的超设计基准水淹场景(如设计基准洪水位情况下，叠加千年一遇降雨)。

应对可能影响厂址的火山活动进行详细调查，厂址应避开可能活动的火山区域。

5.5.3 外部人为事件的防护

核电厂设计需考虑厂址所在地区的潜在外部人为事件。这些危险可能由附近的工业活动、运输事件等所引起。

核电厂设计需考虑由永久工业和军事设施以及紧邻地区的管线所产生的危险。此类潜在危险包括火灾、爆炸、飞射物、有毒与易燃气体释放等。

核电厂设计需考虑由运输造成的厂址地区危险，包括陆地车辆爆炸、冲撞、飞机坠毁和水上运输船舶爆炸。应结合厂址信息论证不予考虑这些危险的原因，否则应作为厂址设计基准外部危险在设计中予以考虑。

核电厂设计需考虑商用飞机的恶意撞击，应制定一套普遍认可的评价方法对商用飞机撞击产生的各类效应(整体效应、局部效应、振动效应以及火灾效应)进行评价，可采用针对超设计基准外部危险的分析方法和假设条件，评价结果应表明可以维持反应堆堆芯的冷却或安全壳功能完好，以及乏燃料水池的完整性或乏燃料的冷却。

5.5.4 内部危险的防护

核电厂设计需考虑发生诸如以下内部危险的可能性：飞射物、构筑物倒塌和物体坠落、管道损坏及其后果、管道甩动、喷射效应、水淹、火灾和爆炸。对于基于核电厂本身特性识别出的可信内部危险，应提供适当的预防和缓解措施，以保证满足 5.5.1 规定的验收要求。

5.6 性能设计要求

5.6.1 设计寿期

核电厂应按至少 60 年的设计寿期进行设计，并且：

a) 对于不可更换设备或部件，应按核电厂设计寿命进行设计；
b) 对于可更换的设备或重要部件，规定其设计寿命，并在设计中考虑人员、设备的可达性与操作空间；
c) 流体系统的设计瞬态按核电厂设计寿命确定。

5.6.2 核电厂平均可利用率

设计应满足在有代表性的不小于 20 年核电厂运行年周期内，考虑计划停堆时间、非计划停堆时间等因素在内，核电厂设计平均可利用率不小于 90%。

5.6.3 换料周期

核电厂设计应能满足 18 个月换料周期要求，并具有进一步延伸至 24 个月换料的能力。

同时，燃料机械设计应能满足组件燃耗不小于 60 000 MWd/tU。

5.6.4 负荷跟踪能力

在每个换料循环长度的至少90%内，核电厂宜具备日负荷跟踪能力，例如：24 h内，初始状态为100%满功率运行，2 h～3 h内降低至50%功率水平，维持50%功率水平运行2 h～10 h，然后2 h～3 h内提升至100%满功率，并在24 h内的其他时间维持满功率运行。

5.6.5 运行性能

核电厂设计应满足如下运行性能要求：

a) 100%功率运行时，汽轮机停机（自身故障）不会造成反应堆紧急停堆或主蒸汽安全阀打开；
b) 一台主给水泵或一台凝结水泵的停运，不会造成反应堆紧急停堆或汽轮机停机；
c) 10%的功率阶跃负荷变化，不会造成反应堆紧急停堆；
d) 在正常换料循环长度内，100%功率运行时发生主电网故障，可切换至带厂用电运行模式而不引起反应堆紧急停堆；
e) 24 h内从冷停堆模式过渡到热停堆模式；
f) 在指定的负荷跟踪运行时，可以补偿由汽轮机微小负荷变化导致的频率变化和反应性变化；
g) 具备适应电网参数变化的能力，在正常工况下可满功率长期连续运行，在不同扰动工况下具备一定的连续满功率运行时限和寿期内累计时限。

5.7 其他设计要求

5.7.1 设计简化

设计中宜尽可能考虑简化系统、部件与简化运行的要求，但系统或部件的简化不能损害执行安全功能的总体可靠性。

设计应有利于减少操纵员动作次数，简化或延缓操纵员动作需求。

5.7.2 标准化设计

核电厂宜采用标准化设计，标准设计的厂址参数具有包络性。核岛设计做到最大程度的标准化，具备较大的厂址覆盖性。

5.7.3 数字化设计

核电厂宜采用数字化设计，实现设计的模型化和一体化，可支持厂址适应性定制设计。设计资料宜尽可能采用数字化移交。

5.7.4 可运行性和可维护性设计

设计应充分吸取现役压水堆核电厂运行、维修的经验和教训，并充分利用相关数据反馈，提高核电厂的可运行性和可维护性，提高核电厂可利用率和设备可靠性：

a) 通过采用先进的数字化和智能化技术，用于监测、控制和保护功能，优化核电厂运行；并用于故障诊断与预测、运营决策功能，优化核电厂维修；
b) 核电厂设计裕量足以应对偏离正常运行的工况；
c) 除为了应对共因故障而采用多样性设备外，需要维修的设备类型宜尽可能少；
d) 便于更换可更换设备；
e) 设备的检查、健康评估、监督试验和维修应尽量简便，并尽量利用基于状态的维修决策等先进技术减少维修需求；

f) 设备布置需考虑维修便利，包括设备出入、维修空间等；
g) 为设备试验和维修活动提供良好的工作环境，包括温度、剂量控制、通风和照明等。

5.7.5 缓解严重事故后果的能力

核电厂应具备如下缓解严重事故后果的能力：
a) 采取适当措施提高严重事故条件下的一回路卸压能力，避免出现高压熔堆；
b) 设置完善的可燃气体控制系统，控制严重事故下可燃气体的浓度；
c) 采取适当措施进行严重事故下堆芯熔融物的冷却；
d) 采取适当措施确保安全壳排热，防止安全壳超压失效；
e) 安全壳压力边界设计考虑严重事故工况下的载荷，确保安全壳完整性；
f) 具有严重事故管理导则；
g) 能够对严重事故状态进行必要的监测；
h) 在设计时采取措施为核电厂应急提供条件，为应急决策提供必要的辅助支持。

缓解严重事故所必需的安全措施尽实际可能独立于缓解设计基准事故的安全系统，包括这些安全措施的支持系统，如设置专门用于缓解严重事故的电源系统。

5.7.6 核电厂自治时间要求

核电厂自治时间应能满足以下要求：
a) 操纵员不干预原则：在确定论安全分析中，对于预计运行事件及事故工况，假设主控制室出现第一个重要信号后 30 min 内主控制室无操纵员动作、1 h 内无就地操作，应能满足相应工况的放射性验收准则；
b) 对于设计基准工况与设计扩展工况，72 h 内不需要任何厂外支援，仅依靠厂内措施便可缓解事故。

5.7.7 多机组核电厂的考虑

多机组核电厂中的每台机组，应具备独立的安全系统和用于设计扩展工况的安全设施，即在确定论安全分析中来自其他机组的支援不是必须的。但为了进一步提高安全性，设计中也需要适当考虑允许多机组核电厂各机组间相互连接的手段。

5.7.8 移动设备

设计中需考虑能安全使用移动设备恢复反应堆排热、安全壳排热和乏燃料水池补水，以及恢复必要的电力供应，这些移动设备不必在厂区贮存。

6 专业领域总体设计要求

6.1 总体布置要求

一台核电机组厂房包括核岛厂房、汽轮机厂房和核电厂配套设施厂房。核岛厂房应按照功能划分，包括反应堆厂房、燃料厂房、核辅助厂房和电气厂房等。

核岛布置应遵循如下准则：
a) 高放射性区需尽可能紧凑；
b) 反应堆厂房需布置在核电机组的中心；
c) 安全系统需尽可能设置在靠近反应堆厂房的位置；
d) 其他核岛厂房与反应堆厂房连接区需尽可能宽敞些，以布置足够的安全壳贯穿件；

e) 与反应堆厂房连接的燃料厂房应正对着燃料元件的运输通道。

汽轮机厂房应采用沿核岛径向的有利布置方案，以减少汽轮机飞射物的影响。

核电厂配套设施厂房应根据厂区进行布置。

核电厂的总平面设计可参考 GB/T 50294 执行。

系统布置应保证运行人员安全，尤其是要对工作人员进行电离辐射防护，还要保证对有检查和监督要求的设备的可接近性。

6.2 反应堆堆芯设计

6.2.1 设计裕度

反应堆的堆芯以及相关的冷却剂系统、控制和保护系统应设计适当的裕度，以确保在任何运行状态和事故工况下不会超过规定可接受的燃料设计限值并符合辐射安全标准。

6.2.2 反应堆核设计

反应堆核设计应给出堆芯内燃料组件、固体可燃毒物与控制棒组件的合理布置，提供足够的剩余反应性与控制手段，确定满足安全要求的堆芯功率分布、燃耗分布与反应性系数。

应具备探测反应堆堆芯内中子注量率分布及其变化的充分手段。

反应堆的堆芯以及相关的冷却系统应设计成在任何运行状态和事故工况下，堆芯具有负的功率反应性系数，反应堆固有的瞬时核反馈的净效应可以补偿反应性的快速增长。

反应性系数的最小和最大限值是多种参数(例如功率水平、硼浓度、燃耗等)的函数，应通过适当研究证实用于分析各种运行工况和事故工况所采用的反应性系数包络值的合理性。

反应堆的堆芯以及相关的冷却剂、控制、保护系统设计成应保证不可能发生超过规定的燃料设计限值的功率振荡工况，或者在发生那些工况时，能可靠而迅速地监测并被抑制。

反应堆堆芯核设计的基本要求可参考 NB/T 20057.1 中的规定。

6.2.3 反应堆热工水力设计

反应堆热工水力设计的总目标，是为反应堆提供与堆芯产生热量能力相匹配的传热能力，并确定合理的一回路系统压力、温度等热工参数，在保证限制放射性产物释放的安全屏障满足各类工况的安全要求前提下，使核电厂具有良好经济性。

具体的反应堆热工水力设计可参考 NB/T 20057.2 中的规定。

6.2.4 燃料元件和组件

燃料元件和组件(包括相关组件)应设计成能够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。

设计燃料元件时需考虑下列劣化因素：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。设计应为数据、计算和制造中的不确定因素留有裕量。

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

燃料组件的设计需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，燃料元件应保持在原位，其变形不应达到有碍于堆芯在事故后保持足够有效冷却的程度，以及不妨碍控制棒

的插入，并且不应超过燃料元件在设计基准事故下的规定限值。

在燃料设计过程中，应在极限功率参数条件下保证足够的裕量。

燃料相关组件是直接与燃料组件相关的控制棒组件、中子源组件、可燃毒物组件（如有）和阻流塞组件的总称。除控制棒组件外的所有燃料相关组件定义为固定式燃料相关组件。

具体的燃料组件及其相关组件的设计可参考 NB/T 20057.3 和 NB/T 20057.4 中的规定。

6.3 反应堆冷却剂系统压力边界设计

反应堆冷却剂系统以及相关的辅助、控制和保护系统的设计应有足够的裕度，以保证在任何正常运行包括预计运行事件期间都不会超过反应堆冷却系统压力边界的设计条件。

反应堆冷却剂系统应具备在各种运行模式下的超压保护功能，特别要关注低温水密实工况下的超压保护。

反应堆冷却剂系统压力边界的设计、制造、安装以及试验应保证异常泄漏、裂纹的迅速扩展以及整体破裂发生的概率极低。

设计中需考虑到反应堆冷却剂系统压力边界材料在运行状态包括维修、试验工况以及事故工况下的所有条件，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。

反应堆冷却剂系统压力边界的部件的设计、制造和布置应便于在核电厂整个寿期内对压力边界定期进行充分检查和试验。

具体的反应堆冷却剂系统设计可参考 NB/T 20187 中的规定。

6.4 安全壳系统设计

6.4.1 安全壳系统功能设计要求

安全壳系统设计应保证或有助于实现下述安全功能：

a） 在运行状态和事故工况下包容放射性物质；

b） 在运行状态和事故工况下的辐射屏蔽；

c） 防御外部自然事件和外部人为事件。

反应堆安全壳以及相关的系统提供了一个固有的密闭屏障，以防止放射性物质不可控地释放到环境中，并且在假定的事故工况所要求的时间内，对安全有重要作用的安全壳系统设计条件不会被超出。

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。

安全壳系统设计应保证其在核电厂所有状态下的完整性，包括设计基准工况和设计扩展工况（含严重事故），以确保不会导致早期放射性释放或大量放射性释放。

安全壳系统设计应能够确保放射性物质从核电厂向环境中的任何释放都保持在可合理达到的尽量低的水平、低于运行状态下的排放限值和低于事故工况下可接受的限值。

安全壳系统的功能设计要求可参考 NB/T 20097 的规定。

6.4.2 安全壳设计基准

反应堆安全壳结构，包括出入口、贯穿件和隔离阀以及安全壳热量导出系统的强度设计应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。设计中还需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。

6.4.3 安全壳泄漏率

安全壳系统应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，并应加强从安全壳泄漏出来的放射性物质的收集能力。

需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。

安全壳构筑物的设计和建造应适应核电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；同时，应允许在安全壳的设计压力下进行定期整体泄漏率试验。

安全壳结构整体性试验可参考 NB/T 20017 中的规定。安全壳密封性试验可参考 NB/T 20018 中的规定。

安全壳系统内部件和结构的覆盖层、保温材料和涂层的使用应保证其在使用期间或劣化时，不影响核电厂的安全功能。

6.5 仪表与控制

应设置仪表系统对正常运行、预计运行事件、事故工况下的核电厂变量和系统进行全程监测，以得到预期变化范围内的参数和系统状态，从而保证获取核电厂工况的充分信息，使反应堆运行在安全限值以内，并保持一定的安全裕度。应监测的参数和系统还包括那些可能会影响裂变进程、反应堆堆芯完整性、反应堆冷却系统压力边界、安全壳的完整性及其相关系统和参数，以及借以获取核电厂的安全可靠运行所必需的任何信息。

设计上需考虑提供适当而可靠的控制系统，以便将相关过程变量维持和限制在规定的运行范围之内。

对任何安全重要的导出参数，如冷却水的欠热度，应配置自动记录装置。针对所涉及的核电厂各种工况的安全重要仪表应经过环境鉴定，并且为应急响应需要，仪表应适合于测量核电厂各种参数，从而对各类事件进行分类。

应设置检测仪表和记录装置，用以获取为监测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。仪表和记录装置应足以为事故期间确定核电厂工况和为事故管理期间做出决策提供尽实际可能的信息。

设计需充分考虑预计工况、执行动作可利用的时间和对操纵员的心理要求，以有助于操纵员成功地完成各种动作。启动所需安全系统的安全动作应是自动触发的，以便在预计运行事件或事故工况开始的一段合理的时间内，不需要操纵员的干预。此外，操纵员应能够获取适当的信息以监视自动动作的效果。

在整个设计过程中需充分考虑人因问题。这不仅限于主控制室运行人员，而且包括现场运行、试验和维修等人员。在可能发生人机关系的各个方面都应提供良好完善的人机接口，以减少人员失误的可能性，还应充分重视运行经验反馈。

设计应有助于运行人员履行职责和执行任务，而且应限制操作失误对安全造成的影响。设计过程应注重核电厂布置和设备布置以及包括维护程序和检查程序在内的有关程序，以有利于运行人员和核电厂之间的相互作用。

核电厂安全仪控系统应设计具有与拟执行的安全功能相称的可靠性和可定期测试性。应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安全功能的丧失。

对于安全有关系统中基于计算机设备，应采用高质量和最佳实践的硬件和软件、整个开发过程系统地形成文件、由独立于设计者和供应商的专业人员进行评价等多种手段保证其可靠性；对于在安全功能实现和安全状态保持中至关重要、且不能高置信度证明设备具有必要的高可靠性时，应提供多样化手段以保证安全功能的执行；同时需考虑有软件引起的共因故障，提供防止系统运行意外中断或受到蓄意干

扰的保护措施。

安全重要的仪表和控制系统可参考 NB/T 20026 中的规定。

6.6 电力系统

核电厂需要提供一个厂内的和一个厂外的电力系统，以保证构成安全重要物项的构筑物、系统和设备可以正常执行其功能。

厂内电力系统包括蓄电池组和厂内配电系统，应有足够的独立性、冗余性和可试验性，能在假想单一故障情况下执行其安全功能。厂内应设有应急交流电源，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电力供应。厂内还应设有替代动力源，以在设计扩展工况下提供必要的电力供应。

核电厂设计中，需考虑核电厂安全重要系统供电可靠性有关的电网与核电厂的相互作用，包括电网供电母线的独立性和数量。从输电网到厂内配电系统的电力系统部分应采用两回实体独立的线路（路径不一定要分开传输）。这两回线路的设计和布置要使得在运行工况、假想事故工况和环境条件下同时故障的可能性降低到实际可行的最低程度。允许两条线路共用一个开关站。每回线路应设计成在丧失所有厂内交流电源和另一回厂外电力线路之后，能在足够长的时间内供电，以保证不会超过规定的可接受燃料设计限值和反应堆冷却剂压力边界的设计条件，这些线路中应至少有一回线路设计成在失水事故后的几秒钟内即可供电，以保证能维持堆芯的冷却、安全壳的完整性和其他一些较为重要的安全功能。

无论单独或同时失去核电机组电源、电网电源或厂内电源，都应设置相应措施使保留的任意电源失去的可能性最小，并优先考虑恢复厂外电源的措施。

对安全重要的电力系统的设计应允许针对重要区域和参数（例如：线路，绝缘，连接部位，配电盘等）进行定期检查和试验，以评价系统的连续性及其部件的状态。系统应设计为可进行以下定期试验：

a) 系统部件的运行或操作性能以及功能特性，比如：厂内电源，继电器以及开关和母线；

b) 系统整体的运行或操作性能和在尽可能接近实际设计条件下，按完全的操作顺序使系统投入运行，包括保护系统中相应部分的操作，核电机组之间的供电、厂外及厂内之间的电源切换等。

具体的厂用电系统设计准则可参考 NB/T 20051 中的规定。

6.7 主控制室

应设置主控制室，借以进行下述活动：在各种运行状态下安全地运行核电厂；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，以保持核电厂的安全状态或使之返回安全状态。应采取适当措施和提供足够的信息保护主控制室内的人员，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。

主控制室应具备足够的辐射防护以便在事故工况下工作人员能进入主控制室并在内工作，在整个事故期间从事干预人员所受到辐射的有效剂量不应超过 HAD 002/01—2019 的规定。

主控制室内仪表的布置和信息显示的方式应便于运行人员正确掌握核电厂现状和性能的全貌。在主控制室设计中需考虑人机工程学的因素。应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。

主控制室屏幕显示的应用可参考 NB/T 20058 中的规定。主控制室操纵员控制器可参考 NB/T 20059 中的规定。主控制室报警功能与显示可参考 NB/T 20027 中的规定。

6.8 辅助控制室

应在与主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，以在主控制室丧失执行重要安全功能时完成下述任务：

a) 快速热停堆，并保证反应堆在热停堆过程中处于一个安全的状态；
b) 排出余热并监测核电厂的重要参数；
c) 通过适当的操作规程使反应堆达到冷停堆。

6.9 反应堆保护系统

6.9.1 保护系统功能设计要求

应提供保护系统，以便探测不安全状态并自动触发安全动作，并启动必要的安全系统来实现和维持核电厂安全状态。

保护系统的设计应能够：

a) 自动启动相应的系统包括反应堆停堆系统，在发生预计运行事件情况下，确保不会超过规定的燃料设计允许限值；
b) 能够检测到是否发生事故工况，并启动安全重要相关系统把该事故后果限制在设计基准事故工况范围内；
c) 抑制控制系统自身的不安全动作；
d) 在运行状态和事故工况下防止由于操纵员的行动引起保护系统失效的可能性，但不应阻碍操纵员在事故工况下采取正确的行动。

6.9.2 保护系统的可靠性以及可测试性

保护系统的设计应确保其具有相当高的功能可靠性以及在线测试能力，以适应其需要执行的安全功能。保护系统的设计过程中需考虑足够的冗余性以保证：

a) 不会因单一故障导致保护功能丧失；
b) 任何一个部件和通道解列退出运行时，不会造成丧失最低要求的多重性，除非用其他方法能够证明保护系统运行具有可接受的可靠性。

保护系统应设计成允许在反应堆运行时对其功能进行定期试验，包括可以独立地试验各个通道，以确定可能已发生了的故障和丧失冗余性。除非能通过其他方法获取必要的可靠性，否则保护系统应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。设计应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。

6.9.3 保护系统的独立性和多样性

保护系统的设计应具有足够的冗余通道，在自然现象的影响下，以及正常运行、预计运行事件和设计基准事故下，不会丧失其保护功能，或者根据其他明确的基准来证明保护系统是可以被接受的。应通过实体隔离、电气隔离、功能独立和通讯（数据传输）独立等适当手段，防止保护系统的冗余组成部分之间发生相互干扰，以及保护系统和控制系统之间的相互干扰。在切实可行的程度内，采用诸如功能多样性或部件设计多样性和运行原理的多样性等设计技术来防止保护功能的丧失。

6.9.4 保护系统的故障模式

保护系统应设计成在遇到诸如系统断开、失去动力源（如电源）或者假想的不利环境（如极热、极冷、火灾、压力、蒸汽、水和辐照）等情况时，系统能处于安全状态，或处于根据其他明确的基准证明是可以接受的状态。

6.9.5 控制系统与保护系统的分离

安全保护系统在一定程度上需要与控制系统分离，这样可以保证在任何单个部件或通道发生故障，

或者保护系统中属于控制和保护系统公用的任何单个部件或通道发生故障或退出运行时，保护系统仍能保持完整，并满足保护系统的所有可靠性、多重性和独立性要求。保护系统与控制系统相互之间的连接应局限在确保不严重妨碍安全的范围内。为避免控制系统对保护系统的干扰，应避免由控制系统向保护系统的信号传输，必要时采取适当的隔离措施。

6.9.6 反应堆停堆故障的保护系统需求

保护系统的设计应保证当反应堆停堆系统发生任何单一失效时，例如控制棒意外提出（不是弹出或脱落），不超过规定的燃料设计允许限值。

6.10 反应堆停堆系统

应设置两套独立的、设计原理不同的反应堆停堆手段。其中一套系统应使用控制棒，以有效的方式插入控制棒，通过控制棒能可靠地控制反应性变化，以确保在运行状态和事故工况下，以及考虑比如最恶劣卡棒之类故障的适当裕量后，也不会超过规定的燃料设计允许限值。在控制棒插入故障导致第一套停堆手段失灵的情况下，另一套停堆手段通过快速注入硼酸实现反应堆紧急停堆。

即使在堆芯具有最大反应性的情况下，两套系统中至少有一套系统能独立使反应堆从运行状态和事故工况下进入次临界，并以足够的深度和高的可靠度保持次临界状态。

6.11 反应堆冷却剂的装量

需要提供一套系统，来控制反应堆冷却剂的装量，以在核电厂任何运行状态下（恰当考虑容积变化和泄漏），使其均不超过规定的设计限值。该系统可以通过使用维持反应堆冷却剂装量的管道、泵以及阀门来完成其功能。

6.12 反应堆冷却剂净化

应设置足够的设施，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。所需系统的能力应基于燃料设计规定的容许泄漏限值和保守的裕量，以保证核电厂可在回路中的放射性水平处于可合理达到的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，并符合可合理达到的尽量低的原则。

6.13 余热排出

需要设置一套反应堆余热排出系统，这套系统的安全功能就是要以一定的速率排出反应堆堆芯中的裂变产物产生的衰变热以及其他的剩余热量，以确保燃料的规定可接受设计限值以及反应堆冷却系统压力边界的设计条件不会被突破。

设备和功能应有适当的冗余，应提供泄漏监测和隔离的能力，以确保在假想单一故障情况下，系统的安全功能都可以实现。

6.14 应急堆芯冷却

需要设置一个可以提供足够应急堆芯冷却的系统，使燃料损伤最少和限制裂变产物的外逸。此系统的安全功能是在发生任何一种冷却剂泄漏时，以足够的速率将热量从堆芯中排出，以保证：

a) 防止由于燃料、燃料包壳的损坏和堆内构件的变形，影响堆芯连续有效的冷却；

b) 水和金属包壳的反应，限制到可以忽略的程度；

c) 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；

d) 堆芯冷却保持足够长的时间。

应提供设备和功能适当的冗余和适当的交叉，泄漏监测、隔离及包容能力，以确保在假想单一故障

情况下，系统的安全功能均能实现。

6.15 安全壳热量导出

应提供一个用来导出反应堆安全壳内热量的系统。该系统的安全功能是在发生任何高能流体排放的设计基准事故后，与其他相关系统的功能共同作用下，迅速地降低安全壳内的温度和压力，并将其控制在一个可以接受的水平。应提供设备和功能适当的冗余，泄漏监测、隔离及包容能力，以确保在假想单一故障情况下，系统的安全功能均能实现。

宜设置一个独立的系统确保设计扩展工况下反应堆安全壳的排热能力。

6.16 安全冷却水系统

需要提供一个构筑物、系统以及安全重要设备中将热量导出到最终热阱的系统。这些系统在各种运行状态和设计基准事故下都应具有很高的可靠性。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排出的系统供应流体的设计都应与它们在整个余热排出的系统中所分担的功能相适应。

为实现系统的可靠性，应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。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，需考虑到自然事件和人为事件的影响。

应设置多样化的排热途径与最终热阱，以确保在严重事故下向最终热阱输送熔融物热量的能力。

具体的设备冷却水系统设计可参考 NB/T 20177 中的规定。具体的重要厂用水系统设计可参考 NB/T 20188 中的规定。

6.17 应急动力供应

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应保证应急动力供应满足要求。同时，还应设有替代交流电源，以在设计扩展工况下提供必要的动力供应。此外，一般还设置一组严重事故专用蓄电池，为严重事故工况下必需的阀门动作及严重事故专用仪表与控制系统提供动力。

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。

核电厂应配备足够容量的移动电源，并需考虑对必要的安全设施设置临时供电接口。

存储移动应急电源及相关设备的构筑物的设计要考虑足够的抗震能力，存放宜采取一定的减震措施、消防措施和防外部水淹措施。

具体的应对全厂断电设计准则可参考 NB/T 20066 中的规定。具体的蓄电池设计可参考 NB/T 20028.1、NB/T 20028.2 和 NB/T 20028.4 中的规定。不间断电源系统蓄电池组的设计可参考 NB/T 20062 中的规定。

6.18 燃料贮存和操作

燃料贮存和操作相关系统应从临界、热工、贮存容量、辐射屏蔽以及抗震等方面进行安全分析，采取相应的安全措施，确保安全性。总的设计要求包括：

a) 有允许对重要安全设备进行适当的定期检查和试验的能力；
b) 有适当的辐射防护的屏障；
c) 有适当的封闭，限制和过滤系统；
d) 具有在运行状态和事故工况下能充分排出余热的能力，其可靠性和可试验性反映出排出衰变热和其他余热对安全的重要性；
e) 可防止事故工况下燃料贮存系统中冷却剂装量显著下降；

f) 对已辐照燃料能进行检查；
g) 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；
h) 能安全地贮存怀疑损坏或已损坏燃料元件或燃料组件；
i) 控制可溶吸收体的浓度水平；
j) 燃料贮存和装卸设施便于维修和退役；
k) 必要时燃料装卸和贮存场所及设备便于去污；
l) 保证能执行适当的操作程序和衡算计量程序。

乏燃料水池需考虑最小贮存年限，确保安全贮存和满足乏燃料充分冷却等方面的要求。

乏燃料余热排出能力需考虑冗余设计，并且热量的排出速率应足以防止那些可能导致放射性物质释放的燃料组件或贮存系统或支持系统不可接受的劣化。应规定乏燃料余热排出系统的限值参数。

燃料贮存和操作系统中的临界问题应通过物理手段或工艺的方法来避免，宜采用几何安全布置。

需考虑通过移动泵和外界动力向乏燃料水池补水以带出余热的人工干预措施。

燃料装卸和贮存系统设计可参考 NB/T 20232 中的规定。

6.19 放射性废物管理

核电厂的设计中应包含合理的控制放射性气体和废液中的放射性物质释放以及处理在反应堆运行状态中产生的放射性固体废物的方式。

核电厂正常运行情况下，核电厂产生的固体废物包体积应符合 4.1.3 的要求(不包括维修过程中产生的大件污染设备)，并且设置放射性固体废物暂存库，其库容应与固体废物的产生量及暂存时间相适应。

为了滞留包含放射性物质的气体和液体流出物，应提供足够的放射性废物贮存能力和处理能力。放射性流出物的排放应满足 GB 6249 的规定。

核电厂的设计应采取适当的措施，以便于放射性废物的转移、运输和装卸；需考虑提供通往设施的通道及起吊和包装能力；中等水平放射性废液贮槽滞留池或所在的房间宜设置钢覆面，钢覆面的高度应确保能容纳贮槽漏出的全部放射性废物。

6.20 辐射防护

6.20.1 设计要求

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可合理达到的尽量低的水平。为实现这一目标，设计中应采用下述办法：

a) 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；
b) 核电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；
c) 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；
d) 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。

需充分考虑到人员停留区域内辐照剂量随时间可能累积并需尽量减少放射性废物的产生。

6.20.2 辐射防护设计

核电厂的设计和布置中应采取合适的措施，以尽量减少来自各种辐射来源的照射和污染。这类措施应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产生和活化、监测手段、核电厂出入口的控制及相应的去污设施。

屏蔽设计应使得操作区的辐射水平不超过规定限值，并应便于维修和检查，以尽量降低维修人员所受的照射。应贯彻可合理达到的尽量低的原则。

核电厂的布置和规程应符合下述要求：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。核电厂的布置应保证高效率的运行、检查、维修和部件必要时的更换，以尽量减少辐射照射。

应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。

具体的辐射屏蔽设计准则可参考 NB/T 20194 中的规定。辐射控制区的设计准则可参考 NB/T 20185 中的规定。辐射控制区出入口设计准则可参考 NB/T 20136 中的规定。

6.21 对常规岛的要求

核电厂对常规岛需考虑如下要求：

a) 应采取措施以提高汽轮发电机组的可利用率，使其满足核电厂的可利用率目标；
b) 汽轮发电机组的大修计划停机方案应与换料停堆方案相协调；
c) 汽轮发电机组应满足关于调节和对电网需要的响应要求，包括负荷跟踪、功率变化、调频、联络线热备用、电网解列响应等；
d) 汽轮发电机组应具有带厂用电负荷运行的能力；
e) 常规岛构筑物在地震情况下的损坏不应对核岛厂房造成不可接受的影响；
f) 常规岛给水系统的水化学特性应满足蒸汽发生器的水质要求。

6.22 老化管理

在核电厂的设计阶段，需充分考虑核电厂整个寿期内的老化问题，确定核电厂安全重要物项的设计寿命。设计应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、部件在其整个设计寿期内能够执行安全功能的能力。需考虑到在所有正常运行工况、试验、维修、停役以及在假设始发事件中和其后的核电厂工况下的老化和磨损效应。评价并考虑能动和非能动的系统部件、构筑物可能影响安全功能的老化机理，包括热脆化、辐照脆化、疲劳、腐蚀、蠕变以及磨损等；并宜考虑相关经验（包括核电厂建造、调试、运行和退役阶段的经验）和研究成果。

应采取监测、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。

核电厂设计阶段，管道设计所涉及的老化管理要求可参考 NB/T 20152 中的规定，预应力混凝土安全壳设计所涉及的老化管理要求可参考 NB/T 20153 中的规定，反应堆压力容器设计所涉及的老化管理要求可参考 NB/T 20154 中的规定，安全级电气设备设计所涉及的老化管理要求可参考 NB/T 20155 中的规定。

6.23 退役

设计中应特别考虑便于核电厂退役和拆除的措施。特别是设计中宜适当考虑：

a) 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；
b) 必要的可达性和可操作性；
c) 管理（例如分离或分拣、表征、分类、预处理、处理和整备）和贮存核电厂在运行过程中产生的放射性废物所需的设施，以及管理核电厂在退役时所产生的放射性废物的措施。

在核电厂退役方面的设计可参考 GB/T 19597 中的规定。

6.24 实物保护

应严格按照标准和规范的要求，结合厂址特征，依据设计基准威胁，设计实物保护系统，从而防止蓄

意闯入核电厂，破坏与核安全相关的系统和设备，防止非法转移、盗窃和破坏核材料。核电厂的实物保护等级应按一级实物保护等级设计。应根据保护目标的重要程度和潜在风险，合理布置控制区、保护区、要害区和要害部位内的设施和设备，实现分区保护。实物保护系统应确保实现探测、延迟和响应的基本功能，并做到人防和技防措施有机结合，保证实物保护系统完整、可靠与有效。应设置多重实体屏障，配置多层次和不同技术类型的探测报警设备，实现纵深防御和均衡保护。实物保护系统应与厂区主体建筑同时设计、同时施工并在核燃料进厂之前具备使用条件。

核电厂实物保护系统应根据设计基准威胁的变化而不断调整，并定期进行评价，持续提高实物保护水平。实物保护系统设备可参考 NB/T 20147 中的规定。

参 考 文 献

[1] GB/T 13626 单一故障准则应用于核电厂安全系统

[2] GB/T 17569 压水堆核电厂物项分级

[3] GB/T 19597 核设施退役安全要求

[4] GB/T 35730 非能动安全系统压水堆核电厂总设计要求

[5] GB/T 50294 核电厂总平面及运输设计规范

[6] NB/T 20017 压水堆核电厂预应力混凝土安全壳结构整体性试验

[7] NB/T 20018 压水堆核电厂安全壳密封性试验

[8] NB/T 20026 核电厂安全重要仪表和控制系统总体要求

[9] NB/T 20027 核电厂主控制室报警功能与显示

[10] NB/T 20028.1 核电厂用蓄电池 第1部分:容量确定

[11] NB/T 20028.2 核电厂用蓄电池 第2部分:安装设计和安装准则

[12] NB/T 20028.4 核电厂用蓄电池 第4部分:维护、试验和更换方法

[13] NB/T 20037.1 RK 应用于核电厂的一级概率安全评价 第1部分:总体要求

[14] NB/T 20037.2 应用于核电厂的一级概率安全评价 第2部分:低功率和停堆工况内部事件

[15] NB/T 20037.3 应用于核电厂的一级概率安全评价 第3部分:功率运行内部水淹

[16] NB/T 20037.11 RK 应用于核电厂的一级概率安全评价 第11部分:功率运行内部事件

[17] NB/T 20051 核电厂厂用电系统设计准则

[18] NB/T 20057.1 压水堆核电厂反应堆系统设计 堆芯 第1部分:核设计

[19] NB/T 20057.2 压水堆核电厂反应堆系统设计 堆芯 第2部分:热工水力设计准则

[20] NB/T 20057.3 压水堆核电厂反应堆系统设计 堆芯 第3部分:燃料组件

[21] NB/T 20057.4 压水堆核电厂反应堆系统设计 堆芯 第4部分:燃料相关组件

[22] NB/T 20058 核电厂控制室屏幕显示的应用

[23] NB/T 20059 核电厂控制室操纵员控制器

[24] NB/T 20062 核电厂不间断电源系统蓄电池组

[25] NB/T 20066 核电厂应对全厂断电设计准则

[26] NB/T 20097 压水堆核电厂混凝土安全壳系统功能设计要求

[27] NB/T 20136 核电厂辐射控制区出入口设计准则

[28] NB/T 20147 核电厂实物保护系统设备准则

[29] NB/T 20152 核电厂管道老化管理指南

[30] NB/T 20153 核电厂预应力混凝土安全壳老化管理指南

[31] NB/T 20154 压水堆核电厂反应堆压力容器老化管理指南

[32] NB/T 20155 核电厂安全级电气设备老化管理

[33] NB/T 20177 压水堆核电厂设备冷却水系统设计准则

[34] NB/T 20185 压水堆核动力厂厂内辐射分区设计准则

[35] NB/T 20187 压水堆核电厂反应堆冷却剂系统设计准则

[36] NB/T 20188 压水堆核电厂重要厂用水系统设计准则

[37] NB/T 20194 压水堆核电厂辐射屏蔽设计准则

[38] NB/T 20232 压水堆核电厂燃料装卸和贮存系统设计准则

[39] NB/T 20402 RK 压水堆安全重要流体系统单一故障准则

[40] HAD 102/01 核电厂设计总的安全原则

[41] HAD 102/03 用于沸水堆、压水堆和压力管式反应堆的安全功能和部件分级

[42] 国核安发的〔2012〕98号 福岛核事故后核电厂改进行动通用技术要求(试行)

[43] 国家核安全局“十二五”新建核电厂安全要求(2013)

[44] IAEA TECDOC-1787 Application of the Safety Classification of Structures, Systems and Components in Nuclear Power Plants(2016)

[45] IAEA TECDOC-1791 Considerations on the Application of the IAEA Safety Requirement For Design of Nuclear Power Plants(2016)

[46] IAEA Safety Standards Series No. SSG-30 Safety Classification of Structures, Systems and Components in Nuclear Power Plants(2014)

[47] IAEA SSR-2/1 Safety of nuclear power plants: design(2016)