核安全导则　HAD102/22-2022

核动力厂辅助系统和支持系统设计

（国家核安全局2022年11月2日批准发布）

国家核安全局

核动力厂辅助系统和支持系统设计

（2022 年 11 月 2 日国家核安全局批准发布）

本导则自 2022 年 11 月 2 日起实施

本导则由国家核安全局负责解释

本导则是指导性文件。在实际工作中可以采用不同于本导则的方法和方案，但必须证明所采用的方法和方案至少具有与本导则相同的安全水平。

目 录

1 引言

1.1 目的

本导则是对《核动力厂设计安全规定》（以下简称《规定》）有关条款的说明和细化，目的是给新建核动力厂辅助系统和支持系统的设计提供指导。本导则的主要内容可作为在役核动力厂设计修改和安全审查的参考。

1.2 范围

1.2.1 本导则适用于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辅助系统和支持系统的设计。其他类型或采用革新技术的反应堆设计可参照本导则，但应经过细致的评价和判断。

1.2.2 辅助系统和支持系统详细清单见本导则 2.2。本导则的范围不包括这些系统具体设备（如换热器等）的详细设计。

2 总则

2.1 辅助系统和支持系统的功能

2.1.1 核动力厂有以下主要系统：反应堆冷却剂系统、蒸汽动力转换系统和发配电系统、专设安全设施，以及用于设计扩展工况的安全设施。辅助系统和支持系统用于支持核动力厂主要系统执行其功能，以保障其运行（如提供动力、服务气体、服务用水、压缩空气、供暖通风与空调、燃料和润滑剂等），或者为核动力厂的运行提供服务（如通信、照明、升降物项等）。

2.1.2 辅助系统和支持系统可直接或间接地为实现安全功能提供支持，例如保证重要支持服务（提供动力、压缩空气、动力电源和润滑油），为安全系统或用于设计扩展工况的安全设施提供支持。

2.2 辅助系统和支持系统的范围

本导则考虑的辅助系统和支持系统如下:

（1）通信系统;

（2）热传输系统;

（3）工艺取样系统和事故后取样系统;

（4）工艺辐射监测系统;

（5）压缩空气系统;

（6）供暖通风与空调系统;

（7）照明系统;

（8）起重设备;

（9）放射性废物和放射性流出物处理和控制系统;

（10）除应急电力系统外的应急动力供应系统;

（11）应急电源和替代电源的支持系统;

（12）《规定》中未明确说明但通常归为辅助系统或支持系统的其他系统。

3 通用设计要求

3.1 设计目标

3.1.1 辅助系统和支持系统的设计应有助于实现核动力厂的基本安全功能。这些系统的具体设计根据厂址条件、反应堆类型、

系统设计和运行条件而有所差异。

3.1.2 辅助系统和支持系统的可靠性应与其对安全的重要性相匹配，因此辅助系统和支持系统及其设备的安全等级应考虑如下方面:

（1）所支持的系统或设备的安全等级;

（2）所支持的系统或设备所实现的安全功能，以及需要辅助系统和支持系统或部件运行的安全功能;

（3）辅助系统和支持系统失效的后果。

3.1.3 每一个提供重要支持服务的系统的容量、自持时间[1]、可用性、稳健性和可靠性应与其对应的安全功能相匹配，能够满足所支持的系统的最大化的必要需求，并有恰当的裕量。

3.1.4 对于依靠非能动安全系统的核动力厂，可根据其安全系统配置确定支持安全功能的辅助系统和支持系统。

3.1.5 安全功能的执行不仅取决于执行安全功能的主要系统的可靠性，也依赖于支持主要系统执行安全功能的辅助系统和支持系统的可靠性。辅助系统和支持系统的可靠性和设计要求应与其所支持的主要系统的可靠性相匹配。对辅助系统和支持系统的设计审查的详细程度应与其所支持的主要系统相一致。其设计还应适当考虑《规定》中对于构筑物、系统和部件的设计基准的要求。

3.2 设计基准

3.2.1 辅助系统和支持系统的安全级构筑物、系统和部件的设计基准应包括与需要其运行的正常运行工况、预计运行事件以

[1] 自持时间指系统可以自主地（即当其他系统失效时）持续运行的时间长度。

及事故工况（设计基准事故工况和设计扩展工况）有关的所有条件。

3.2.2 应对设计条件和设计载荷进行计算，适当地考虑对每个相关的核动力厂状态或危险的包络情况。

3.2.3 辅助系统和支持系统的构筑物、系统和部件的预期性能应取决于其所必须保证的安全功能的需求。

3.2.4 应确定辅助系统和支持系统的构筑物、系统和部件的设计基准，包括以下因素:

（1）构筑物、系统和部件需执行的安全功能;

（2）构筑物、系统和部件所需承受的假设始发事件;

（3）构筑物和部件所需承受的载荷和载荷组合;

（4）内部危险防护;

（5）外部危险防护;

（6）设计限值和验收准则;

（7）可靠性;

（8）防止同一系统内部或属于纵深防御不同层次系统之间发生共因故障的措施;

（9）安全等级;

（10）鉴定中所考虑的环境条件;

（11）设计规范和标准;

（12）布置的考虑;

（13）接口的考虑;

（14）对多机组核动力厂的考虑（如适用）;

（15）概率安全分析在设计中的应用。

3.3 安全功能

应详细描述辅助系统和支持系统所实现的安全功能，以便确定每个安全重要设备和部件的安全等级。

3.4 假设始发事件

应确保一个辅助系统和支持系统的故障不会导致假设始发事件。如果一个辅助系统和支持系统的故障导致假设始发事件是可预见的，设计上应有合适的手段进行缓解，同时考虑该故障对核动力厂其他系统的影响。

3.5 内部危险

3.5.1 应考虑起源于场内并会损害辅助系统和支持系统构筑物、系统和部件性能的内部危险。通常考虑的典型内部危险清单（包括但不限于）如下:

（1）高能管道破裂;

（2）重物坠落;

（3）内部飞射物;

（4）火灾和爆炸;

（5）水淹;

（6）电磁干扰。

3.5.2 应采取布置和设计措施以确保辅助系统和支持系统的构筑物、系统和部件免受内部危险效应的影响:

（1）应采取防护措施保证辅助系统和支持系统构筑物、系统和部件免受高能危险影响（内部爆炸、内部飞射物、管道甩击、喷射、重物坠落），或将其设计成能够承受这些危险产生的载荷或载荷组合。

（2）多重系统之间应尽量采用屏障分隔，或者根据需要采用足够的几何分隔和防护，防止系统的安全功能失效。

（3）实体隔离和防护措施应保证假设始发事件分析中已考虑的系统响应不会被内部危险所削弱。

（4）支持应对设计基准事故的安全系统的辅助系统和支持系统，应尽可能和支持应对设计扩展工况特别是堆芯熔化事故所需的安全设施的辅助系统和支持系统保持独立，降低由于单一危险导致共因故障的风险。

3.6 外部危险

3.6.1 用以支持缓解设计基准事故所必需的系统运行的辅助系统和支持系统应设计成能够承受或者防护设计基准外部危险效应，或防止产生共因故障。这些辅助系统和支持系统的设计要求应与此类缓解系统的设计一致，并应适当考虑辅助系统和支持系统的性能。

3.6.2 如任一构筑物、系统和部件的自身故障会影响到 3.6.1 所述辅助系统和支持系统的运行，则这些物项应设计成能够承受或者防护设计基准外部危险的影响，或防止产生共因故障。

3.6.3 如 3.6.1 所述的辅助系统和支持系统的任一构筑物、系统和部件失效会导致事故工况，则这些物项应设计成能够承受或者防护设计基准外部危险的影响，或防止产生共因故障。

3.6.4 对于每个外部危险，必须识别在灾害中或灾害后要保证可运行性或完整性的辅助系统和支持系统的部件，并在其设计基准中进行规定。

3.6.5 设计中采用的设计方法、设计和建造规范应保证适当

的裕量，以避免外部危险的陡边效应。

3.6.6 对设计基准外部危险来说，由辅助系统和支持系统执行的短期动作以及辅助系统和支持系统为满足事故工况下的限值和设计准则而必须执行的动作应通过在场内的系统来完成。这些系统动作所需的准备时间应与要执行的短期动作相适应。

3.6.7 辅助系统和支持系统支持安全功能执行的自持时间应长于场外支援到达的时间。应考虑特定灾害对多个机组甚至全厂机组同时产生影响的可能性，以保证使用厂区内及场区内的处理措施的自持时间是可信的。应考虑由外部危险引起的损害及不利条件对外部支援的影响。

3.6.8 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。

3.6.9 针对外部水淹，包容 3.6.8 所描述系统的所有构筑物都应在设计基准洪水位以上，或者采取足够的防护措施（如水密门）以保证其安全功能。

3.7 事故工况

3.7.1 设计辅助系统和支持系统时，需要考虑辅助系统和支持系统所支持的那些安全功能可能受到事故工况的不利影响。

3.7.2 某些辅助系统和支持系统的故障可能会导致事故工况恶化，甚至发展到严重事故。应特别关注并确保这些系统的高可靠性，尤其是与丧失厂外电源、丧失冷却功能、丧失最终热阱相关的系统。

3.7.3 当考虑导致设计扩展工况的多重故障时，应考虑支持

安全系统的辅助系统和支持系统的故障，或支持没有造成堆芯明显损伤的设计扩展工况的安全设施的辅助系统和支持系统的故障。

3.7.4 在事故工况中需要用到辅助系统和支持系统时，应在辅助系统和支持系统设计中将相关事故工况作为确定能力、负荷和环境条件的输入。

3.8 可靠性

3.8.1 可靠性考虑因素

对于支持安全功能的辅助系统和支持系统，为使其获得必要的可靠性，需考虑以下因素:

（1）安全分级及设计和制造中相关的技术要求;

（2）系统相关设计准则（例如多重的列数、抗震鉴定、环境鉴定、动力供应等);

（3）采用适当的方式预防共因故障的发生，如实体隔离和功能独立;

（4）系统布置中应防止系统受到内外部危险的影响;

（5）定期试验和检查;

（6）维护;

（7）设备采用故障安全设计。

3.8.2 应对设计基准事故的系统

3.8.2.1 针对需要某一辅助系统或支持系统的一部分投入的应对设计基准事故的安全功能，辅助系统和支持系统的设计应保证在假设始发事件和完成此项安全功能的安全系统或安全组合的任一假设单一故障所引起的任何继发故障的情况下，仍然能够

执行该安全功能。此外应考虑由维护、试验或维修造成的系统不可用。

3.8.2.2 核动力厂设计的应急动力源应有足够的能力为在设计基准事故中执行安全功能的设备提供动力。对于需要在事故工况中投入的辅助系统和支持系统及与之相关的设备，也需考虑使用应急动力源或替代动力源提供动力。

3.8.2.3 应识别用于支持安全系统的辅助系统和支持系统多重部件间可能的共因故障，并在设计及布置中采取措施使多重的部件尽量减少发生共因故障的可能性。

3.8.3 应对没有造成堆芯明显损伤的设计扩展工况的安全设施

3.8.3.1 对于执行既定安全功能的安全系统，其可靠性分析中应包含对支持该系统的辅助系统和支持系统的分析，以识别是否需要附加安全设施以完成这些安全功能。

3.8.3.2 应对多重安全系统间的共因故障与假设始发事件之间可能的组合进行分析。如果这种组合的后果超过了设计基准事故的限值，则应消除这种组合的可能性或者采用附加安全设施来应对这种情形。此种与安全功能相关的附加安全设施应考虑防止发生共因故障。

3.8.3.3 本导则 3.8.2 的要求同样适用于没有造成堆芯明显损伤的设计扩展工况，但无需考虑单一故障准则，同时应考虑到导致用于缓解设计基准事故的系统失效的共因故障一般不会导致相关的附加安全设施的失效。

3.8.3.4 针对伴随丧失应急动力源的设计扩展工况，其相应的

附加安全设施应由替代动力源提供动力。

3.8.4 缓解堆芯熔化的设计扩展工况（严重事故）的安全设施

3.8.4.1 缓解严重事故所必需的辅助系统和支持系统可由任何可使用的动力源提供动力。

3.8.4.2 在尽可能的情况下，设计中应采取措施保证安全系统和用于缓解严重事故的特定安全设施之间的独立性。尤其是，任一辅助系统或支持系统尽可能不同时用来支持安全系统和用于缓解严重事故的安全设施。

3.8.4.3 本导则 3.8.2 的要求同样适用于严重事故，但无需考虑单一故障准则，同时应考虑到导致用于缓解设计基准事故的系统失效的共因故障一般不会导致相关的附加安全设施的失效。

3.9 纵深防御

3.9.1 根据纵深防御概念，辅助系统和支持系统可能在不同核动力厂状态下运行，以保证一系列预期安全功能的实现。

3.9.2 以下建议用于帮助实现纵深防御层次间的互相独立:

（1）对于某个给定的安全功能，应识别从属于不同纵深防御层次的，且参与执行该安全功能的必要物项;

（2）应识别（1）中描述的容易发生共因故障的物项，并对失效后果进行评价。若安全功能的失效可能导致不可接受的后果，应尽可能地减少发生共因故障的可能性。特别地，用于缓解堆芯熔化事故后果的安全设施应尽可能地独立于缓解设计基准事故后果的安全系统;

（3）不同系统间的独立性不能被用于监控或触发这些系统

的仪控系统的共因故障所影响。

3.10 安全分级

3.10.1 应对支持某一安全功能实现的辅助系统和支持系统进行适当的安全分级。

3.10.2 某个构筑物、系统和部件的失效的影响应从安全功能的实现和放射性释放两个方面去考虑。如果失效后果与两个方面都相关，则为达到期望的可靠性所需的安全等级和相关的质量要求应考虑这两方面。无需包容放射性物质的物项，安全等级和质量要求应根据假定相应安全功能失效所造成的后果直接确定。

3.10.3 针对执行安全功能所必需的全部或一组系统，其技术要求（如与独立性、应急动力源等相关的要求）应与该系统的安全等级相一致。

3.11 环境和抗震鉴定

3.11.1 如果辅助系统和支持系统的构筑物、系统和部件用于支持安全功能的实现，则应对其运行前或运行期间所可能遭受的支配性环境条件进行鉴定以保证功能的实现，或通过设置充分的防护避免受到这些环境条件的影响。

3.11.2 事故发生前、事故发生期间和事故发生后相关的环境条件和地震条件，以及构筑物、系统和部件在核动力厂寿期内的老化，均需要在环境和抗震鉴定中进行考虑。

3.11.3 环境鉴定应采用试验法、分析法或运行经验法，如果需要，也可采用上述方法的组合。

3.11.4 环境鉴定应考虑温度、压力、湿度和辐照的因素，在特殊情况下应考虑局部放射性颗粒的聚集、振动、蒸汽冲击、水

淹以及与化学品的接触。安全裕量以及协同效应也应考虑。对于可能存在协同效应的情况，应针对最严重的效应或最严重的组合或序列进行鉴定。

3.11.5 在说明其合理性的前提下，可使用加速老化鉴定的技术。

3.11.6 对于受各种老化机理影响的部件，应确定其设计寿命或更换频率（如需）。在对这种部件的鉴定过程中，应在针对事故条件进行鉴定前，对样机进行老化以模拟其在设计寿期末的情况。

3.11.7 除非证明鉴定试验所使用的条件和方法不会导致设备本身的安全性能产生不可接受的降级，否则已被执行过鉴定试验的设备不应在后续核动力厂的建造中使用。

3.11.8 应对鉴定数据和结果进行记录，作为设计文件的一部分。

3.12 设计规范

3.12.1 对于已进行安全分级的辅助系统和支持系统的构筑物、系统和部件，应采用广泛采纳的或经过良好验证的设计规范。选择的设计规范应可以应用到具体设计中并应形成一套完整、全面、一致的标准和准则。如果对同一个构筑物、系统和部件的不同方面采用了不同的设计规范，则应证明所采用设计规范的相容性。

3.12.2 设计和建造应优先采用最新有效版本的设计规范，如需使用其他版本，则应有适当的说明。

3.12.3 规范和标准涵盖以下方面:

（1）机械设计;

（2）结构设计;

（3）材料选择;

（4）设备、部件制造;

（5）已制造或安装的构筑物、系统和部件的检测;

（6）电气设计;

（7）仪控设计;

（8）环境和抗震鉴定;

（9）防火;

（10）屏蔽与辐射防护;

（11）质量保证。

3.13 布置考虑

3.13.1 辅助系统和支持系统的布置应满足如下要求:

（1）应考虑便于制造、装配、安装、建造、调试、运行、在役检查、维修、退役和拆除;

（2）应保证合适的环境条件（如必要的可达性和提供充足的照明）以保证必要活动（如检查和维修）正常开展;

（3）在辅助系统和支持系统运行期间，应保证工作人员所受的辐射照射是可合理达到的尽量低;

（4）应保证在核动力厂所有状态下与其他构筑物、系统和部件之间的不利影响尽量小;

（5）应保证有适当的途径使得人员可进入辅助系统和支持系统开展现场手动操作;

（6）应至少有一条可供撤离或救援工作人员进出的安全路

径，并应保证应急照明。

3.13.2 应采取必要的措施防止未经授权的人员进入或干扰辅助系统和支持系统（包括通过计算机系统未经授权远程访问）。

3.13.3 辅助系统和支持系统的设计及布置应保证在发生故障或事故时不妨碍所支持安全功能的执行。

3.14 相互作用的考虑

辅助系统和支持系统的相互作用可彼此提供重要支持服务，但应避免安全级别较高的系统与安全级别较低的系统相互作用对安全级别较高的系统功能造成不利影响，除非可从安全的角度论证这种相互作用是有利的。一旦产生相互作用，应采取措施保证必要时重要支持服务可与其他支持功能隔离。

3.15 多机组核动力厂的考虑

3.15.1 设计应保证多机组核动力厂不同机组应对设计基准事故的安全系统不共用辅助系统和支持系统。

3.15.2 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。

3.16 设计中概率安全分析的使用

3.16.1 概率安全分析应作为安全性识别和有效性判断过程的一部分。

3.16.2 概率安全分析应为确定论分析提供一种补充分析手段，尤其是在检查和调整涉及辅助系统和支持系统的多重故障叠加清单和为了获得平衡设计去确定附加安全设施时。从这个方面来看，概率安全分析可认为是评价辅助系统和支持系统失效可能性及其后果的有效工具，但分析中应考虑概率安全分析的局限

性。

3.16.3 作为与建造、试验和检查相关的研究及与运行经验评估相关的研究的一种补充，概率安全分析应与确定论分析一同使用以确认在导致严重事故时，发生早期放射性释放和大量放射性释放的可能性极低。这其中需考虑支持某一安全功能的辅助系统和支持系统（例如供暖通风与空调系统）相关部件的可靠性和其他在二级概率安全分析中通常会考虑的方面。

4 详细设计原则

4.1 总体说明

4.1.1 本章对2.2节提及的核动力厂执行安全功能的辅助系统和支持系统提出了通用设计建议。对于其他类型核电技术，系统功能和配置可能存在差异，部分设计建议可能不适用，需根据相应系统是否执行安全功能确定其适用性。

4.1.2 本章所列系统包括在2.2节中列出的辅助系统和支持系统。对于在本章中未包括的辅助系统和支持系统，适用第3章的通用设计要求。

4.1.3 本章给出的原则，其目的是保证支持安全系统或用于设计扩展工况的安全设施的辅助系统和支持系统的高可靠性。

4.2 通信系统

4.2.1 总述

通信系统一般包括以下通信手段:

（1）警报系统（可设计成扩声系统），可在主控室或辅助控制室及应急控制中心触发，发出全厂或机组警报。系统应可提供

不同类型的警报进行区分：例如撤离警报、一般警报。

（2）呼叫通话系统，用于核动力厂工作人员之间的通讯，一般包括：

—有线通信系统，用于主控室（或者当主控室不可用时辅助控制室等其他场所）与就地操作站之间的直接通话；

—寻呼系统，用于实现核动力厂范围内的人员呼叫；

—用于提醒噪音区域人员的特定装置（如扬声器）。

（3）电话通信系统，一般包括：

—主电话系统，用于满足核动力厂一般通信需要，系统容量应当与核动力厂正常运行的需求相符；

—辅助电话系统，作为主电话系统的后备，设置在重要岗位，在主电话系统不可用时使用；

—无线通信系统，在正常与应急工况下均可使用。

（4）场外通信系统，提供与外部组织（如国家应急准备和响应部门）和设施的通信链路。

（5）视频监控系统，提供对重要部件（如反应堆冷却剂泵、安全壳内重要部位）或主控室外的重要维修活动的监控。

4.2.2 系统和设备功能

4.2.2.1 应设置合适的通信系统为核动力厂内各个位置的工作人员提供传递信息和指令的手段，以确保工作人员能够在正常运行、预计运行事件和事故工况下接收到报警和指令。通信系统也应当为移动中进行的运行操作提供适当的通信手段。

4.2.2.2 应在主控室提供通信手段，以确保核动力厂安全有效的运行。此外，应设有独立的广播系统和专用寻呼系统，用于主

控室与厂内负责核动力厂管理和监视的人员之间的通讯。

4.2.2.3 应急准备和响应设施应提供多样化的通信手段，提供主控室、辅助控制室、应急控制中心以及场外应急准备和响应部门之间的通信。

4.2.3 设计基准

4.2.3.1 对于核动力厂安全运行非常重要的通信系统，在正常运行、预计运行事件和事故工况下，及由相关的内外部危险引起的特殊工况下，其应可提供有效的厂内通信（核动力厂内部）及厂区与场外（核动力厂外部）之间的通信手段。

4.2.3.2 厂内通信系统及厂外通信系统均应设置备用电源。

4.2.3.3 与核动力厂安全运行相关的通信系统应具有恰当的安全等级。

4.2.3.4 通信系统不应受其他的电子、电气设备干扰。相应的，无线通信系统也不能对安全有关的设备产生干扰。

4.2.3.5 主控室应设计为核动力厂在正常运行以及事故早期阶段的通信中心。

4.2.3.6 警报系统应能:

（1）在可影响整个核动力厂的事故工况下提供全厂警报，这些警报信号能够广播至核动力厂所有区域;

（2）在仅影响核动力厂局部区域的事故工况下提供本区域警报。

4.2.3.7 声警报装置的声压级应当高于设备所在的区域背景噪声，并应考虑穿戴个人防护设备时的影响。在高噪音区域，除声警报装置以外，还需设置光警报装置。

4.2.3.8 寻呼系统应能够覆盖核动力厂的所有可达区域，包括室内与室外。主控室及辅助控制室应能够使用该系统，在所有可用的控制点中主控室具有最高控制权限。

4.2.3.9 主电话系统应具有足够的点位与通道数量，以满足核动力厂所有工作人员的使用需求。

4.2.3.10 当主电话系统不可用时，应由辅助电话系统提供核动力厂相关岗位间的电话连接。主电话系统与辅助电话系统应相互独立。

4.2.3.11 无线通信系统在正常与应急工况下均可使用，用于与场内和场外工作人员通信。无线通信系统应当与主电话系统及辅助电话系统相互独立。此外，无线通信系统应对无线信号进行测试以确定场内是否存在盲区。核动力厂中无线信号会造成严重电磁干扰后果（例如跳堆）的区域应被设为无线禁用区。

4.2.3.12 应提供用于应急准备和响应的厂外通信系统，与场外机构之间应具有安全、可靠、永久的双向语音线路。如果可能，这些线路应设计为无需拨号的直通点对点连接。当出现大规模的电力、网络故障时，这些通信系统应可持续使用。各个区域的通信设备数量应当与岗位的需求相匹配。

4.2.3.13 厂内通信与厂外通信系统的终端数量应当与应急准备和响应的需求相符合，包括应急演习。

4.2.3.14 在不可达区域应提供其他通信设备，包括用于对特殊区域（例如反应堆冷却剂泵、安全壳内重要部位）进行监控的视频监控系统。

4.2.3.15 通信系统多样性：

（1）主控室、辅助控制室和技术支持中心应与以下地点具有至少两种多样化的通信手段:

—在预计运行事件或事故工况下需要通信的场所;

—应急响应设施，如技术支持中心;

—相关设施，包括受当前机组运行影响的其他设施，例如同一厂址的其他机组。

（2）多样化的通信手段包括但不限于数据传输、固定电话、卫星和移动电话以及便携式无线电。

（3）4.2.3.15（1）、（2）中定义的多样化通信连接：应设计为不受相同的故障、内部危险、外部危险或假设始发事件的影响。

4.3 热传输系统

4.3.1 总述

4.3.1.1 本节所述的热传输系统是指用于导出运行状态和事故工况下必须运行的系统和设备中热量的系统，不包括反应堆冷却剂系统及其有关系统，以及乏燃料装卸和贮存系统。

4.3.1.2 本导则中涉及的热传输系统如下:

（1）用于冷却核动力厂系统或设备（如主泵热屏、化学和容积控制系统的下泄热交换器、泵电机和轴承）的冷却水系统，可以是闭式冷却水系统或开式冷却水系统;

（2）用于冷却供暖通风与空调系统的冷冻水系统;

（3）通过新风或盘管执行冷却功能的供暖通风与空调系统。

4.3.2 热传输系统总体要求

4.3.2.1 热传输系统应确保系统和部件被充分冷却，使其可以在运行状态和事故工况下具有执行并维持其设计功能的能力。

4.3.2.2 热传输系统的设计应考虑可能影响特定过程的所有形式的热负荷。通过换热器和冷却器等换热设备对构筑物、系统和部件提供足够的冷却使其不超过设计温度限值。

4.3.2.3 除热负荷外，热传输系统设计还应考虑热阱的设计基准温度（适当保守计算以考虑不确定度并留有适当的裕量）。

4.3.2.4 当热传输系统用以保证其冷却设备执行安全功能时:

（1）热传输系统安全等级应与其承担的安全功能一致，同时满足相应的设计要求（例如多重性、应急动力源、内部和外部危险防护、定期检查和试验、维修和质量保证）。此外，对于位于厂房外的输热管道，应考虑相应措施来应对极端低温天气及其他外部危险。

（2）应对热传输系统的可靠性进行评价，并应考虑可能的共因故障。如有必要，应考虑冷却系统相关部分的多样性设计。

4.3.2.5 应考虑反应堆冷却剂或冷却介质泄漏到系统边界外的风险，应从可能丧失冷却功能、潜在的放射性危害和硼水混合导致的稀释等方面评估泄漏的后果。

4.3.2.6 支持安全功能实现的热传输系统应包含监测冷却介质液位和/或直接探测泄漏的手段，当探测到冷却介质丧失时，应有相应措施提供补给。需提供足够的水量以确保事故工况下具有足够的冷却能力，并提供足够的补水以确保长期热量排出。

4.3.3 冷冻水系统

4.3.3.1 通常，冷冻水系统为供暖通风与空调系统（例如主控室通风系统、电气厂房通风系统或功率运行期间的安全壳通风系统）和一些其他工艺负荷提供冷却。冷冻水系统的冷水机组由设

备冷却水系统、空气冷却或自设冷却水系统进行冷却。

4.3.3.2 核动力厂一般设计有冷冻水系统，能为特定区域提供足够的冷冻水来保证供暖通风与空调系统（如电气厂房通风系统和主控室通风系统）和工艺负荷的冷却。

4.3.3.3 在设计基准事故下，用于支持冷冻水系统实现安全功能所需的部分应具有适当的安全等级，应满足相应的设计要求（例如多重性、应急动力源、内部和外部危险防护、定期检查和试验、维护和质量保证），并根据相关的规范进行设计和制造。

4.3.3.4 穿过安全壳的冷冻水系统管线应具备适当的自动或非能动的安全壳隔离。穿过安全壳的冷冻水系统的安全壳隔离部分应该是安全级的并应满足相应的设计要求。

4.3.3.5 安全冷冻水系统冷水机组的性能应基于下述因素确定:

（1）合适的极端设计温度——设备冷却水系统的极端水温或厂址极端设计条件（风冷）;

（2）最大冷负荷。

4.3.3.6 一般核动力厂设计中为安全重要物项服务的冷冻水系统和为非安全重要物项服务的冷冻水系统是相互独立的。如果没有采用独立分开的热传输系统设计，则应确保能采用充分的安全手段将两者进行隔离。

4.3.3.7 应评估热量传输到最终热阱的可靠性。必要时，应采取适当的多样化设计（例如冷水机组采用设备冷却水系统冷却或采用空气冷却）。

4.3.3.8 由于冷凝问题，冷冻水系统的所有冷部件需考虑保冷

隔热。

4.3.3.9 与室外空气接触的设备应考虑防腐（特别是位于海边的设备）和防冻。

4.3.4 设备冷却水系统（余热排出系统除外）

4.3.4.1 通常，设备冷却水系统是闭式冷却水系统，通过厂用水系统导出核动力厂安全系统和某些非安全系统及设备的热量到最终热阱。作为反应堆一回路和环境之间的一道屏障，能够防止放射性物质泄漏到环境，同时也可以防止厂用水系统介质进入安全壳或反应堆冷却剂系统中。

4.3.4.2 设备冷却水系统应执行以下功能:

（1）运行状态和事故工况下排出设备热量并将其传递至最终热阱;

（2）防止放射性物质进入最终热阱。

4.3.4.4 当设备冷却水系统冷却含有反应堆冷却剂的部件时（例如主泵热屏）:

（1）设备冷却水系统应为闭式回路以防止冷却剂泄漏到最终热阱;

（2）应控制设备冷却水系统的水化学条件以缓解腐蚀;

（3）应设置监测系统以探测设备冷却水系统的放射性;

（4）应防止由于高压换热器泄漏引起的设备冷却水系统超压，在这种情况下，应设置可靠的隔离手段防止反应堆冷却剂泄漏到安全壳外。

4.4 工艺取样系统和事故后取样系统

4.4.1 总述

工艺取样系统和事故后取样系统分别需要提供在运行状态和事故后需要分析的所有样品。根据不同分析要求，样品可被送至不同的设备（包括辐射监测系统）。

4.4.2 系统和设备功能

4.4.2.1 工艺取样系统应能提供正常运行期间必要的液体和气体样品，以分析反应堆冷却剂及其有关系统（如应急堆芯冷却系统、余热排出系统、化学和容积控制系统）、安全壳大气和二次侧系统的化学和放射化学特性。

4.4.2.2 工艺取样系统应能对所有需监测其样品以确认是否满足运行限值和运行条件的正常运行工艺系统和主要部件（包括必要的辅助系统和支持系统）进行取样（例如对压水堆安注箱的硼浓度进行取样）。

4.4.2.3 工艺取样系统应能在正常运行期间提供样品，用于识别可能危及反应堆冷却剂压力边界完整性的化学条件。

4.4.2.4 当取样样品为放射性介质时，工艺取样系统和事故后取样系统应能够包容放射性物质。该系统应收集、处理有代表性的流体（液体和气体）样品，并分配至一个或多个取样装置。

4.4.2.5 对于乏燃料水池，工艺取样系统和事故后取样系统应能探测可能导致放射性水平超标的工况，并提供用于控制池水化学条件的信息，该化学条件是燃料组件包壳完整性、乏燃料水池的内部结构和乏燃料冷却系统所必需的。

4.4.2.6 工艺取样系统和事故后取样系统应能监测运行状态和事故工况下可溶性中子吸收体的浓度。

4.4.3 设计基准

4.4.3.1 工艺取样系统的设计应能提供正常运行必需监测的样品，以保证满足设计要求和运行要求，应能提供监测手段以确认反应堆冷却剂及相关辅助系统和支持系统(例如重水堆的慢化剂及其辅助设备)、安全壳大气和二次侧系统中的液体和气体特性满足化学控制和运行要求。

4.4.3.2 事故后取样系统应满足设计基准事故和设计扩展工况下的取样和监测需求(例如在严重事故期间对安全壳内的气体和液体取样)，并应设计为能在相应的工况下运行。

4.4.3.3 取样点的选择取决于核动力厂的设计。对于每种类型的样品，应根据其重要性确定是否有必要使用安装在取样管线上的在线仪表连续监测，或仅依靠间断手动取样分析即足以满足要求。

4.4.3.4 通常在厂内实验室进行样品分析。但是，对于分析频率较低的样品，可在厂外实验室或厂区实验室分析。工艺取样系统和事故后取样系统的设计和布置应使取样和分析之间的时间尽可能短。通过减少距离和优化布置提高样品传输速度。取样管线的长度还应考虑放射性核素的衰变。

4.4.3.5 应提供措施保证从液体和气体工艺流体以及贮罐中获取的样品具有代表性。例如贮罐中的样品应从循环回路中获取以避免从低点或沉积区取样。对于工艺流体中的样品，取样点应布置在湍流区。如有必要，取样流体应经过冷却和降压后再进行分析。

4.4.3.6 正常运行期间，工艺取样系统应监测确保安全的参数和系统，包括影响裂变过程、堆芯完整性和反应堆冷却剂压力边

界完整性的参数。工艺取样系统应提供信息用于评估安全系统和其他安全有关系统能否免受异常失效的影响以及是否能执行预期安全功能。

4.4.3.7 工艺取样系统和事故后取样系统:

（1）应能提供措施确认一回路和二回路的水化学参数（包括重要参数，例如氯化物、氢浓度和氧浓度）在规定的限值以内，并确保抑制腐蚀，不会对反应堆冷却剂压力边界产生不利影响;

（2）对于压水堆，允许在正常运行期间提供措施确认硼浓度（例如换料水箱和安注箱）满足在相关事故工况下保证堆芯次临界的要求;

（3）应能提供样品用于确认喷淋化学添加箱（如有）中的化学品浓度在限值以内，以确保在事故工况下能够充分去除安全壳内的碘，同时不对设备造成损害。

4.4.3.8 应尽可能将排放的样品、冲洗吹扫样品回路的流体以及样品回路的疏水回收至被取样系统或排放至适当的废物处理系统。如在压水堆中将样品返回冷却剂系统（或重水堆返回至主热传输系统），取样部件的材料应满足有关导则中关于反应堆冷却剂系统材料的选取原则。

4.4.3.9 如取样管线设置有能动阀门，为防止放射性释放，这些阀门的故障安全位置应设置为关闭。

4.4.3.10 应采取措施限制反应堆冷却剂取样管线破裂时的放射性释放，例如配置非能动限流器。

4.4.3.11 工艺取样系统和事故后取样系统应根据执行的安全功能划分适当的安全等级，满足有关导则的分级原则。

4.4.3.12 连接位于安全壳内系统的取样管线要求配置自动安全壳隔离设施。反应堆冷却剂系统取样管线要求配置至少两道安全壳隔离阀。这些安全壳隔离设施应为安全级、满足相应的设计要求（例如多重性、应急动力源、内部和外部危险防护、定期检查和试验、维修和质量保证），并根据可接受的设计规范进行设计和制造。事故后，需能对一回路冷却剂取样验证硼浓度、测量放射性活度并确定裂变产物的组成。为此，当取样位置的辐射防护条件允许时，可在一段时间后重新打开一回路取样管线（如有需要，可采取特定的预防措施）。

4.4.3.13 该系统的设计和制造应使厂内工作人员受到的辐照剂量可合理达到的尽量低。

4.4.3.14 应提供适当的布置和设计措施（例如屏蔽、辐照和放射性活度报警、通风）减少操作工艺取样系统和事故后取样系统或在附近工作的人员接受的照射。为保护工作人员，输送高放射性流体的管道应布置在辐射屏蔽措施后，应远程显示经常使用的信息，应在辐射屏蔽措施之外操作驱动机构。

4.4.3.15 为减少工作人员的辐射照射，取样系统的设计应采取如下措施:

（1）需要定期维修的工艺取样系统和事故后取样系统部件周围的工作区域应辐射屏蔽来自其他系统的高水平辐照;

（2）应提供足够的空间对工艺取样系统和事故后取样系统部件进行检修;

（3）采取措施避免取样管线中放射性污泥沉积（例如冲洗、限制管线低点的数量）。

4.4.3.16 事故后取样系统的设计应允许在事故后收集并分析高放射性样品，例如反应堆冷却剂、安全壳地坑和安全壳大气样品，提供再循环水的 pH 值、安全壳大气中氢气和裂变产物浓度等信息。

4.4.3.17 放射性和潜在放射性样品的取样应与非放射性样品取样进行隔离，隔离的程度应考虑设备和地面疏水系统的需求以及流出物处理的安排。

4.4.3.18 在安全壳外进行样品分析时，如有风险超出核动力厂放射性废物管理能力的样品，高放射性样品应再注回安全壳内。

4.4.3.19 放射性液体样品应在手套箱或带屏蔽装置的取样设备中处理，手套箱由不锈钢等材料制成，其表面易于去污。为对工作人员处理样品时提供保护，手套箱或带屏蔽装置的取样设备应特殊加固，保持设备负压，并通过固定的碘过滤器连接到通风系统。此外，如有必要，应提供样品脱气装置，以降低液体样品中的放射性水平。

4.5 工艺辐射监测系统

4.5.1 系统和设备功能

4.5.1.1 在正常运行、预计运行事件、设计基准事故工况下以及尽可能在设计扩展工况下，工艺辐射监测系统应:

（1）确保对每道屏障的辐射监测;

（2）确保对放射性释放的监测并提供核动力厂放射性活度诊断所需要的信息;

（3）在必要时候，提供有辐射照射风险的警告;

（4）提供执行自动或手动限制放射性物质释放所需要的信息以减轻放射性后果。

4.5.1.2 工艺辐射监测系统应：

（1）监测蒸汽发生器的活度，以探测不可接受的蒸汽发生器传热管泄漏，并确定是否有必要对受影响的蒸汽发生器执行隔离操作；

（2）在冷停堆期间，监测安全壳内、燃料厂房以及其他任何可能发生燃料操作事故的厂房内的活度，以探测可能需要撤离报警和限制放射性物质措施的事故；

（3）监测气态流出物的活度以验证是否保持在允许的排放限值内；

（4）提供确保安全壳外控制区中放射性物质受控所需要的信息。

4.5.1.3 应设置通过实验室分析进行间断监测的取样点，特别是那些在正常运行工况下不运行的系统。

4.5.2 设计基准

4.5.2.1 应通过连续监测所有核动力厂状态下与屏障接触的流体的放射性活度（例如反应堆冷却剂和安全壳大气）来监测第一道和第二道屏障的完整性。

4.5.2.2 应监测通常不具有放射性但在屏障完整性丧失的情况下会被其他含有放射性物质的系统泄漏污染的流体（液体或气体）的放射性活度。

4.5.2.3 应连续监测反应堆厂房、燃料厂房、核辅助厂房、安全厂房和废物处理厂房通风系统排气的放射性活度水平。

4.5.2.4 为探测屏障的泄漏，应连续监测设备冷却水系统（以及压水堆和重水堆的蒸汽发生器二次侧）中液体的放射性活度。

4.5.2.5 对于一些事故后工况，如冷却剂丧失事故或者严重事故后，辐射监测系统应提供能够评估放射性向安全壳大气释放量的监测。

4.5.2.6 为保护工作人员，应连续监测安全壳和其他有可能发生放射性释放的厂房的大气，以触发人员撤离报警和考虑采取行动，特别是在发生燃料操作事故的情况下。此外，在所有包含大量放射性液体和固体废物的区域，应进行表面污染监测。

4.5.2.7 工艺辐射监测系统应提供可能需要采取行动保护工作人员和公众的任何放射性释放的信息。

4.5.2.8 在适用的情况下，应监测主蒸汽管道、蒸汽发生器排污管道和凝汽器中的放射性活度，以连续监测二次侧的放射性活度，为工作人员提供报警。

4.5.2.9 工艺辐射监测系统应连续监测气体放射性废物储罐或滞留管线排放气体的放射性活度，在排放异常时发出报警，以停止排放。

4.5.2.10 为确保在场区发生放射性污染时主控室的可居留性，工艺辐射监测系统应监测主控室进风口，并可启动主控室通风系统的碘吸附器和粒子过滤器。

4.5.2.11 应监测可能发生污染的房间（例如燃料厂房和核辅助厂房的房间）的主通风管道中空气放射性活度。在探测到空气污染的情况下，应隔离正常通风系统的相关部分，同时启动高效粒子过滤器（HEPA）和碘吸附器。

4.5.2.12 在事故工况下，应监测含有反应堆冷却剂系统泄漏出来放射性流体的储罐或地坑，以防止向放射性废液处理系统的可能排放，同时协助核动力厂工作人员决定流出物是否再注入到安全壳内。

4.5.2.13 放射性废液排放系统排放废液时，应连续测量排放废液的放射性活度浓度。如果测量结果显示超过了允许排放限值，应自动隔离排放管线，同时发出报警。

4.5.2.14 所有气态排放应通过通风烟囱排出。应在较大的活度浓度范围内监测烟囱内惰性气体的放射性活度，并应在超过允许的排放限值时触发报警。此外，应监测通过烟囱排放的放射性碘、氚和碳-14 的放射性活度水平。

4.5.2.15 应连续测量每个可能收集高污染水的污水坑的剂量率，以在剂量率超过预设阈值时，自动隔离污水坑向放射性废物处理系统的排放。

4.5.2.16 工艺辐射监测系统应能够提供执行应急计划所需的核动力厂内辐射状况的所有相关信息。

4.6 压缩空气系统

4.6.1 总述

通常，压缩空气系统向公用压缩空气系统、仪表和气动执行机构提供压缩空气。本导则重点阐述压缩空气系统为仪表和气动执行机构提供压缩空气的功能。

4.6.2 系统和设备功能

压缩空气系统为仪表和气动执行机构提供持续的压缩空气，压缩空气应满足用户所需的品质、流量和压力的要求。

4.6.3 设计基准

4.6.3.1 如果与压缩空气系统连接的安全重要物项设计成能在失去空气压力时可信地进入故障安全状态，则可将此压缩空气系统视为非安全有关的系统。如果安全重要物项需要使用压缩空气作为其执行安全功能的动力，则:

（1）为其提供压缩空气的系统部分应为安全系统；或

（2）设置专用的安全级压缩空气（或气体）储罐，储罐容量应满足 4.6.3.5 要求。

4.6.3.2 压缩空气系统执行安全功能的部分（或储罐）应满足相应的设计要求，例如多重性、应急动力源、内部和外部危险防护、定期检查和试验、维护和质量保证等。

4.6.3.3 如果压缩空气系统同时为安全重要物项和非安全重要物项提供空气，且安全重要物项需要使用压缩空气作为其执行安全功能的动力，则应设置适当的隔离装置，确保预计运行事件或事故工况下系统向安全重要物项供气的部分能与向非安全重要物项供气部分的可靠隔离。

4.6.3.4 在任何不利的环境条件、预计运行事件（包括丧失厂外电源）或事故工况下，如果安全重要物项需要使用压缩空气作为其执行安全功能的动力，则为安全重要物项供应空气的压缩空气系统应能确保其功能。如果压缩空气储罐安装在安全壳内，储罐的设计应考虑到在设计基准事故期间由于安全壳的温度升高而引起的压力升高。

4.6.3.5 如果在事故工况下需要气动执行机构动作，则压缩空气系统（例如通过压缩空气储罐）的供气时间应保证与完成安全

功能所需要的时间一致。

4.6.3.6 如果压缩空气储罐需要支持安全系统或用于设计扩展工况的安全设施，则压缩空气储罐的供气时间应大于等于完成系统功能所需要的时间，否则，应为压缩空气储罐配备相应等级的固定式或可移动式压缩空气补气设备，压缩空气储罐的容量应与补气设备重新充罐压缩空气储罐的时间匹配。

4.6.3.7 如果通过压缩空气储罐确保压缩空气系统的自动供气能力，则上游供气管道应设置止回阀，以防止压缩空气因上游管道泄漏而导致减压，从而保证了压缩空气对用户的供应。如果这些用户需要通过压缩空气储罐来执行安全功能，则应对这些止回阀的密封性进行定期试验。

4.6.3.8 压缩空气系统的设计应避免安全壳旁路或安全壳升压。布置在安全壳内的需在事故后长期运行的系统，其安全功能的执行不应依赖压缩空气系统。

4.6.3.9 穿过安全壳的压缩空气管路应具有自动隔离功能。这些安全壳隔离功能应进行适当的安全分级，并应满足相应的设计要求（例如多重性、应急动力源、内部和外部危险防护、定期检查和试验、维护和质量保证）和按照相应的规范进行设计和制造。

4.6.3.10 压缩空气的品质受进气品质的影响，因此，应选择合适的进气位置（例如无尘环境、远离有害物质或有害气体），必要时增设进气过滤装置。

4.6.3.11 应设置压缩空气品质监测装置，以保证下游所有用气点的压缩空气品质（例如露点、固体颗粒含量和粒度分布、最大含油量或碳氢化合物含量、湿度和化学污染）；应采取措施防

止压缩空气中的水汽凝结聚集。

4.7 供暖通风与空调系统

4.7.1 总述

4.7.1.1 供暖通风与空调系统的设计要求应根据其执行的安全功能确定，通常将供暖通风与空调系统划分如下两类:

（1）参与控制放射性释放功能，尤其是对特定区域空气进行过滤的供暖通风与空调系统（或这类系统的一部分）。这类系统通常包括: 控制区安全专设设施房间空气过滤通风系统（如适用）、燃料厂房通风系统、放射性废物和流出物处理厂房通风系统、安全壳清洗通风系统以及环廊通风系统（如适用）;

（2）维持安全重要物项运行和主控室及应急响应设施可居留环境条件的供暖通风与空调系统，这类系统通常包括: 电气厂房通风系统、柴油发电机厂房通风系统、泵房通风系统以及控制室通风系统。

4.7.1.2 供暖通风与空调系统应将厂房环境条件（温度、湿度和气载放射性水平）维持在安全重要物项运行及人员进入可接受的范围。

4.7.1.3 为监测与限制正常运行、预计运行事件及事故工况下气态放射性释放，系统需考虑如下措施:

（1）放射性控制区内房间应维持负压，以防止在核动力厂运行期间放射性物质向环境扩散。一般可通过送风量小于排风量来实现。

（2）应维持空气由低污染区域流向高污染区域。

（3）污染区（或潜在污染区）空气需要过滤后排放以确保

气载放射性排放符合可合理达到的尽量低原则，并确保低于正常运行、预计运行事件的排放限值要求，在事故工况下低于可接受的限度。

（4）应监测控制区排风的放射性，控制区的排风应通过烟囱排放。

4.7.1.4 供暖通风与空调系统应有助于保护工作人员和（或）设备不受假设的内部事件（如内部火灾与爆炸）及外部事件（如极端气候条件、有毒气体）影响。

4.7.1.5 存在放射性碘污染风险的区域，尤其是在事故工况下存在含有大量气态放射性碘释放风险的放射性液体系统所在的房间，设计上应采取足够的措施以保证房间的放射性包容功能。

4.7.1.6 参与限制放射性释放功能的供暖通风与空调系统的设计应确保这类系统在正常运行、预计运行事件及事故工况下均可控制及限制放射性物质释放。

4.7.1.7 执行限制放射性排放功能的通风与空调系统采用预过滤器、HEPA 过滤器（必要时利用碘吸附器）对排风进行过滤后通过烟囱排放，过滤后气态流出物的放射性水平应低于排放限值要求。

4.7.1.8 需根据下述不同区域，合理确定换气次数:

（1）内照射风险较高的区域;

（2）内照射风险可忽略的区域;

（3）内照射风险不可忽略，但碘释放风险可忽略的区域。

4.7.1.9 参与限制放射性释放尤其是限制放射性碘释放功能的供暖通风与空调系统，需确保有足够的防护水平，同时需考虑

室外风的影响。

4.7.1.10 维持安全重要物项运行、人员进入及居留区域环境条件的供暖通风与空调系统，设计需考虑合适的内部及外部极端环境条件（例如温度、湿度以及这些环境条件的持续时间）。

4.7.1.11 设计基准事故工况下支持安全系统实现其安全功能所需的供暖通风与空调系统的相关部分应具有适当的安全等级并满足相应的设计要求，例如:

（1）采用多重设计以满足单一故障准则。

（2）系统采用应急供电。

（3）系统（包括进风口和排风口）具备抵御内、外部危险的能力。特别是采取多重列实体隔离、设备抗震的设计。除非经过充分的论证，通风系统设计应有助于防止爆炸性气体、有毒气体及热量由外部进入设置有安全重要物项的房间。

（4）系统定期检查及试验。

（5）设备部件的设计、制造、调试和测试需遵循适当的标准规范。

4.7.1.12 应考虑供暖通风与空调系统与防火系统的配合。

4.7.2 控制区安全专设设施空气过滤通风系统

4.7.2.1 控制区安全专设设施空气过滤通风系统服务区域（包括但不限于）如下:

（1）位于安全壳外的应急堆芯冷却系统房间;

（2）位于安全壳外的余热排出系统房间;

（3）位于安全壳外的安全壳喷淋系统房间。

4.7.2.2 控制区安全专设设施空气过滤通风系统的功能是维

持相应区域的环境条件，以确保人员进入及在核动力厂正常运行、预计运行事件、事故工况下所需的安全重要物项的运行。

4.7.2.3 控制区安全专设设施空气过滤通风系统应限制放射性物质的释放，以确保气载放射性物质的放射性水平不超过核动力厂规定的限值。

4.7.2.4 控制区安全专设设施空气过滤通风系统执行安全支持功能，或直接执行安全功能，因此应满足与其执行的安全支持功能或安全功能相一致的设计要求（例如多重性、应急动力源、内部和外部危险防护、定期检查和试验、维护和质量保证），并按照适当的规范进行设计和制造。

4.7.2.5 控制区安全专设设施空气过滤通风系统应确保气流从非控制区域流向控制区域。

4.7.2.6 应急堆芯冷却系统房间、余热排出系统房间和安全壳喷淋系统房间在事故工况下应按放射性碘污染区域考虑。

4.7.2.7 如果假设余热排出系统在安全壳外产生破口，则相应的通风系统的设计应考虑其影响。

4.7.2.8 在事故工况下应能自动隔离控制区安全专设设施空气过滤通风系统中非安全重要的部分。

4.7.3 燃料厂房通风系统

4.7.3.1 燃料厂房通风系统应能为燃料厂房提供维持安全重要物项运行及人员进入（必要时）所需的环境条件（例如温度、湿度、气载放射性水平）。

4.7.3.2 燃料厂房通风系统的设计应限制气载放射性物质的释放：在发生燃料操作事故时，限制放射性物质向环境释放，使

其保持在核动力厂的规定限值之内；在核动力厂正常运行和预计运行事件情况下，维持向环境释放的气载放射性水平在规定的限值之内，并符合可合理达到的尽量低的原则。

4.7.3.3 燃料厂房通风系统的设计应能控制乏燃料水池区域的气载放射性物质浓度，以允许人员在核动力厂正常运行、预计运行事件期间和燃料操作有关的设计基准事故后进入。

4.7.3.4 燃料厂房控制区一般被视为放射性碘污染风险区域，除非分析可以证明某些房间不受此类风险影响。

4.7.3.5 为应对燃料操作有关设计基准事故，用于限制放射性物质的释放或支持安全设备运行所必需的燃料厂房通风系统部件，应满足与其安全功能相一致的设计要求（例如多重性、应急动力源、内部和外部危险防护、定期检查和试验、维护和质量保证）。

4.7.3.6 燃料厂房通风系统的设计应确保气流从厂房的非控制区域（如有）流向控制区域。

4.7.3.7 燃料厂房通风系统设计应确保：

（1）必要时，设置监测手段以隔离控制区与非控制区（如有）的包容边界；

（2）必要时，隔离非安全重要的通风系统部件；

（3）触发专门用于事故工况的通风部件。

4.7.4 放射性废物和流出物处理厂房通风系统

4.7.4.1 放射性废物和流出物处理厂房通风系统应能维持厂房适宜的环境条件，以确保正常运行期间人员进出和设备的良好运行。

4.7.4.2 放射性废物和流出物处理厂房通风系统应确保在事故工况下，将放射性物质限制在厂房内。根据安全分析结果，可以采用静态包容或动态包容方式限制放射性物质的释放。

4.7.4.3 放射性废物和流出物处理厂房通风系统的设计应控制厂房控制区内的气载放射性水平，以便人员在核动力厂正常运行期间进入。

4.7.4.4 放射性废物和流出物处理厂房通风系统的设计应确保在正常运行时，向环境释放的气载放射性水平低于规定的限值，并符合可合理达到的尽量低的原则。限制放射性物质释放的通风系统部件应进行适当的安全分级。

4.7.4.5 放射性废物和流出物处理厂房的通风系统的设计应确保气流从厂房的非控制区域（如有）流向控制区域。

4.7.5 安全壳通风系统

4.7.5.1 执行反应堆厂房供暖通风与空调功能的系统，一般包括:

（1）维持反应堆厂房内环境温度的闭式循环通风系统;

（2）反应堆厂房清洗通风系统：在停堆期间运行，用于保证人员工作适宜的环境条件；当反应堆厂房内发生燃料操作事故时，该系统也用于限制放射性物质向环境的释放；正常运行期间，在人员进入安全壳之前，该系统可用于降低人员活动区域气载放射性水平。

4.7.5.2 反应堆厂房清洗通风系统需确保在反应堆厂房内发生燃料操作事故时放射性物质的包容。

4.7.5.3 反应堆厂房清洗通风系统的设计需保证气载放射性

物质浓度的控制和人员在冷停堆期间及燃料操作设计基准事故之后进行维修活动所需的环境条件。反应堆厂房清洗通风系统需降低在停堆期间由于惰性气体及含氚水蒸汽导致的气载放射性水平。

4.7.5.4 反应堆厂房清洗通风系统中保证放射性物质包容的部分应进行适当的安全分级，该部分应满足相应的设计要求（例如多重性、应急动力源、内部和外部危险防护、定期检查和试验、维修和质量保证），并应根据相应的规范进行设计和制造。尤其应满足在地震工况下执行其安全功能的能力。

4.7.5.5 反应堆厂房清洗通风系统应限制反应堆厂房燃料操作事故工况向环境的放射性物质释放，使其满足相应的限值。系统设计应考虑停堆时反应堆开口的情况。

4.7.5.6 反应堆厂房清洗通风系统应考虑在燃料贮存水池中运输乏燃料时，燃料包壳损坏可能导致反应堆厂房内某些区域的放射性气体和气溶胶释放。此外，反应堆厂房清洗通风系统的设计还需考虑:

（1）在冷停堆期间，保证释放到环境的放射性气溶胶在允许的限值之下，并可合理达到的尽量低;

（2）安全壳隔离，隔离设备应有适当的安全等级，并可承受事故时安全壳内较高的放射性水平;

（3）避免安全壳受过度负压影响;

（4）提高反应堆氢气控制系统的效率。

4.7.6 维持环境条件的供暖通风与空调系统的特殊考虑

4.7.6.1 含有安全重要物项的非控制区通风系统

本节仅涉及执行维持安全重要物项安全运行和人员进入所需环境条件的通风系统。根据布置情况，此类系统可能包括电气厂房、柴油机厂房、泵房、部分核辅助厂房（通常是包括应急给水系统和设备冷却水系统的部分）通风系统。设计要求包括:

（1）非控制区通风系统的设计应维持房间内适宜的温湿度及空气洁净度在安全重要物项运行和人员进入可接受的限值之内。

（2）在设计基准事故下，用于维持安全重要物项执行功能的非控制区通风与空调系统部分应进行适当的安全分级，满足相应的设计要求（例如多重性、应急动力源、内部和外部危险防护、定期检查和试验、维修和质量保证），并应根据相应的规范进行设计和制造。

（3）在全厂断电事故工况下，应保证缓解该事故所必须的电气厂房重要区域通风与空调系统的可用性。

（4）设有蓄电池的电气房间的通风系统应考虑氢气爆炸的风险。

（5）送入电气房间的空气应具有足够高的空气质量，以保护电气设备不受灰尘、污垢、沙粒及湿度的损伤。

4.7.6.2 主控室、辅助控制室和场内应急响应设施通风系统

利用主控室通风系统来维持主控室内设备正常运行及所有核动力厂状态下的可居留性，包括在外部环境出现烟气、爆炸、毒气、放射性污染的情况，通过维持环境条件（温度、湿度、空气洁净度、充足新风）和控制气载放射性物质浓度，保证主控室可居留性和设备运行的要求，则设计要求包括:

（1）主控室通风系统的设计应保证安全重要物项的运行，应进行适当的安全分级，满足相应的设计要求（例如多重性、应急动力源、内部和外部危险防护、定期检查和试验、维修和质量保证），并应根据相应的规范进行设计和制造。

（2）主控室通风系统的设计应能在核动力厂正常运行和事故工况下自动维持主控室相对大气的正压，以尽量减少厂内放射性污染事件时放射性物质进入主控室。

（3）主控室通风系统的设计应满足在发生厂内放射性污染事件时，通过设置合适的碘过滤器和空气粒子过滤器，维持送往主控室的空气清洁。

（4）主控室通风系统应确保主控室的隔离，以避免任何可能危害人员健康或设备运行的物质进入。

（5）主控室通风系统或相关系统应具备在火灾时排出主控室内烟气的能力。

辅助控制室通风系统不应与主控室共用通风系统。场内应急响应设施不应与主控室和辅助控制室中任何一个共用通风系统。场内应急响应设施的通风系统的设计应保证该设施合理可信的可居留性。

4.8 照明系统

4.8.1 总述

照明系统主要分为正常照明系统和应急照明系统。其中应急照明包括备用照明系统、安全照明系统和疏散照明系统，具体功能如下:

（1）正常照明系统为正常运行工况下的工作提供照明;

（2）备用照明系统在火灾、预计运行事件（包括失去厂外电源的情况）以及设计基准事故时提供照明;

（3）安全照明系统在核动力厂发生全厂断电工况时为核动力厂提供照明;

（4）疏散照明系统为人员疏散提供紧急出口照明。

4.8.2 系统功能

照明系统及其电源应能提供足够的照明，使核动力厂人员能够进入相应区域，并在所有工况下执行所有必要的手动操作（例如维护操作或紧急操作程序中的操作）以及在疏散情况下从各区域安全地撤离。

4.8.3 设计基准

4.8.3.1 备用照明系统应在正常照明系统故障时或在丧失厂外电源且应急电源系统还未可用期间立即可用。

4.8.3.2 应在（但不限于）安全相关区域以及通往这些区域的通道和救援通道中提供备用照明。具体包括以下区域:

（1）主控室;

（2）辅助控制室;

（3）场内应急响应设施区域;

（4）应急发电机区域;

（5）包含开关柜室、电机控制中心、蓄电池或逆变器的区域;

（6）在应急操作程序中确定的必须进行手动操作的核动力厂区域。

4.8.3.3 主控室中的备用照明应独立于主控室内的其他照明

系统。主控室中的平均照度水平应考虑显示器和屏幕的设计来进行调整，以减少反射和眩光以及其他与照明不足相关的影响。此外，主控室应设置多个照明区域，并能通过手动调光来提供适合操纵员执行任务的照明。

4.8.3.4 全厂断电工况下，应至少在主控室、辅助控制室、应急响应设施以及需要操作人员操作的区域提供足够的照度水平。

4.8.3.5 全厂断电工况下，照明系统需通过蓄电池在需要操作的相关区域提供足够时间的照明，直到恢复内部或外部电源。

4.8.3.6 疏散照明系统应提供必要的最低照度水平，以确保工作人员能够安全地撤离房间和建筑物。为该照明系统供电的电池应具有足够的容量，以确保提供足够的照明时间使人员在包括火灾在内的所有条件下疏散到安全区域。

4.9 起重设备

4.9.1 总述

起重设备主要包括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。环吊和乏燃料容器吊车属于本导则起重设备的一部分，换料机不在本导则的考虑范围内。

4.9.2 系统和设备功能

4.9.2.1 使用起重设备时应制定核动力厂内吊运重物的方案。

4.9.2.2 由起重设备吊运的重物包括但不限于下列设备:

（1）堆内构件;

（2）堆顶组件;

（3）主泵及主泵电机;

（4）乏燃料运输容器等。

4.9.3 设计基准

4.9.3.1 应采取保守的设计手段防止载荷意外跌落影响安全重要物项。这些措施包括限制起重设备的活动区域（通过设计或者联锁）使其远离燃料存储区域和实现安全功能的设备，或通过载荷跌落评估保证不会出现不可接受的后果。

4.9.3.2 应明确重物吊运的安全载荷路径，以最大程度地减小重物跌落到下述物项位置的可能性：反应堆压力容器、乏燃料水池中的乏燃料组件，以及其他安全级设备。

4.9.3.3 在额定载荷情况下，起重设备的结构、机构和部件（如传动链、钢丝绳等）应距离材料的屈服强度有足够的安全裕度。

4.9.3.4 起重设备应设计成在 SL-2 地震时能够持续保持住最大危险载荷。

4.9.3.5 在可能造成意外放射性泄漏的事故情况下，起重设备应禁止使用。

4.9.3.6 起重设备的设计应保证在失去电源、失去电机扭矩、机械故障的情况下可以手动下降载荷，或在采取一定的措施后可以手动下降载荷。

4.9.3.7 在失去电源或发生 SL-2 地震时，起重设备应避免对燃料组件或安全重要物项产生冲击破坏。

4.9.3.8 为避免超载，起重设备应配备载荷测量装置，该装置的显示器应始终对操作人员可见。载荷测量装置应同时包括过载保护系统。

4.9.3.9 失去电源时，起重设备的所有机电部件都应自动置于

安全状态。当电源恢复时，设备应始终处于安全状态，直到操作人员干预。

4.9.3.10 起重设备应配备上部高度限位开关、正常运动停止装置和紧急停止按钮。

4.9.3.11 对于可能破坏安全重要物项的起重设备，应配备安全机构，该安全机构可以是作用于卷筒的安全制动器或多重设置的起升机构。安全机构应通过多重的超速检测装置或者多重的起升机构失效探测装置来触发。探测装置应完全独立于操作人员的指令和控制。

4.9.3.12 位于安全壳内的起重设备（特别是吊车梁和吊车轨道）的设计应考虑周围环境引入的额外载荷，这些载荷可能由安全壳内冷却剂丧失事故产生。

4.9.3.13 起重设备投运之前，应进行载荷试验。核动力厂正常运行期间应实施定期检查和试验，以确保安全装置可正常使用，包括上部限位开关、超速保护、超载保护和限制区域联锁。

4.9.3.14 可能受到污染的吊车应采用表面光滑易于去污的涂层材料。

4.9.3.15 在初步退役计划中列入的重要起重系统应具备相应的设计寿命和特殊设计要求，以满足将来的退役需求。

4.10 放射性废物和放射性流出物处理和控制系统

4.10.1 总述

4.10.1.1 核动力厂的设计必须满足放射性废物安全操作、贮存、处理、转移和运输以及控制流出物排放的要求。在设计中还应考虑在转运过程中废物贮存和废物回取的规定。

4.10.1.2 设计必须具备安全处理并控制液态和气态流出物向环境排放保持在规定限值内，并可合理达到的尽量低的能力。

4.10.1.3 设计应尽量减少核动力厂运行及退役放射性废物的产生量。

4.10.1.4 放射性废物和放射性流出物的处理和控制包括放射性废物的收集、处理、整备或流出物排放，这些放射性废物来自于在正常运行期间系统疏排水、清洗、排气、泄漏以及其他操作。

4.10.1.5 便于放射性废物管理的设计措施包括以下内容:

（1）与放射性物质接触，特别是与反应堆冷却剂接触的材料的选取，以便在可行的范围内尽量减少放射性废物量，并利于去污。

（2）反应堆冷却剂和其他系统的水化学设计应尽量减少腐蚀产物的产生（例如通过氢浓度控制、注锌和 pH 控制等）。

（3）应采取措施以尽量减少腐蚀产物的沉积，这些腐蚀产物在通过反应堆堆芯时已活化或可活化。特别应尽量减少这种腐蚀产物在燃料组件和反应堆堆芯周围结构上的沉积。

（4）应明确划分非放射性废物区（即废物未受污染的区域）和放射性废物区（即废物可能受到污染的区域）。应作出规定以尽量减少放射性废物区。

（5）应在设计阶段制定相关规定，以便于将来的拆除活动。包括便于大型部件拆卸和运输的安装方式、用于拆卸活动的吊装装置的后续管理规定，便于安全拆除的辐射屏蔽设施、以及现场去污的规定等。

4.10.1.6 用于限制核动力厂运行期间产生的放射性废物照射

的相应措施应包括在设计中:

（1）对于在核动力厂内产生和运输或释放到环境中的放射性废物，应采取措施减少废物的数量和浓度;

（2）采取措施将放射性废物与工作人员和公众隔离，并制定相关规定对核动力厂潜在放射性污染和辐射照射进行辐射分区管理;

（3）应对液态流出物排放前的监测、收集和处理作出规定;

（4）应为人员和设备提供所需的去污设施。还应对去污活动产生的放射性废物的处理做出规定。

4.10.1.7 用于处理和控制放射性废物和放射性流出物的系统，应根据风险的性质和程度，防止内部和外部危险。例如在压水堆中，输送浓硼酸的回路应位于温度较高的厂房或设有伴热，以防止硼结晶。

4.10.1.8 用于处理和控制放射性废物和流出物的系统的设计，应具有能够对安全重要部件进行适当的定期检查和试验的措施，应设置适当的辐射防护屏蔽，以及适当的包容设施和过滤系统。

4.10.2 废气管理系统

4.10.2.1 废气处理系统的设计应实现以下功能:

（1）处理和监测气态流出物，以便其排放到公共排放点之前放射性核素滞留衰败时间满足最短时间要求;

（2）排放前对流出物的体积和放射性进行监测;

（3）对于可能超过释放限值情况，具有隔离排放路径的措施。

4.10.2.2 可以通过缓冲罐收集废气，然后加压输送到衰变装置；或通过滞留管线（例如活性炭滞留床）进行在线处理，处理后通过辅助厂房的通风系统排放到排放点（例如烟囱）。

4.10.2.3 应在设计阶段提供通过烟囱排放的气态流出物的测量措施，排放过程的取样和监测措施。

4.10.2.4 废气贮存衰变系统的设计应确保废气贮罐的数量和容量足以使短寿命气体在释放到环境之前衰变到低于排放限值。

4.10.2.5 废气贮存衰变系统的设计应确保任一废气贮罐的破裂对厂内、厂外不会造成（或仅有轻微的）放射性后果，并且不需要任何厂外防护行动。

4.10.2.6 设计应：

（1）防止爆炸风险，如含氢废气贮罐房间应采取防止爆炸风险的措施。例如通过对相连设备进行连续氮气吹扫和氢氧复合，以防止氢气引燃；

（2）防止废气处理系统的管道破裂。

4.10.2.7 气态流出物排放系统的设计应包括限制放射性气体释放的措施。这应该通过配置高可靠性的设备、结构，进行放射性探测和包容的措施来实现。

4.10.2.8 穿过安全壳的废气处理管线需要具有自动隔离功能。应对安全壳隔离功能进行安全分级并满足相应的设计要求（例如多重性、应急动力源、内部和外部危险防护、定期检查和试验、维护和质量保证）。

4.10.3 放射性废液管理系统

4.10.3.1 放射性废液管理系统一般包括硼回收系统、放射性

废液处理系统和液态流出物监测和排放系统，其中硼回收系统也称为反应堆冷却剂贮存和处理系统。某些核动力厂因负荷跟踪期间不需要调硼，在设计上可不考虑设置硼回收系统。

4.10.3.2 硼回收系统:

（1）处理经具有下泄功能的系统（如压水堆的化学和容积控制系统）排放的反应堆冷却剂;

（2）脱除惰性气体和氢气，净化和分离硼与水，以便回收硼酸和补给水;

（3）监测所得产物，并依据监测结果，输送至反应堆硼和水补给系统进行复用，或输送至放射性废液处理系统、废液排放系统或固体废物处理系统。

4.10.3.3 核动力厂不同机组可以共用放射性废液处理系统。放射性废液处理系统在设计上应可贮存、充分处理和监测来自设备和地面排水系统收集的各种不可复用的废液，之后输送到排放系统。放射性废液处理系统设计应包括以下措施:

（1）根据各种废液的化学成分和放射性水平，对所有潜在受污染的废液进行选择性前端贮存;

（2）对每个贮罐中的废液分析后进行充分的处理，以使处理后的废液满足核动力厂可复用要求或满足排放到环境中的标准;

（3）监测输送至排放系统的贮存设备;

（4）将产生的固体废物（例如浓缩物、废离子交换树脂、废过滤器芯子）转移到固体废物处理系统。

4.10.3.4 液态流出物监测和排放系统收集来自每个机组和其

他设施排放的液态流出物，监测和记录放射性水平、化学和物理成分，并以受控的方式将流出物排放到环境中。排放到环境中的流量应根据流出物的放射性水平和环境的稀释能力来确定，以满足排放限值。在设计阶段应考虑下列关于液态流出物监测和排放系统的规定:

（1）监测排放液态流出物的体积;

（2）确定或调整排放流量，以确保符合排放要求;

（3）如果可能超过排放限值，自动隔离排放管线。

4.10.3.5 放射性废液管理系统的设计应该具有监测、控制、收集、处理、转运、贮存和处置放射性废液的能力，并且保持液态流出物可合理达到的尽量低地排放到环境中并低于排放限值。

4.10.3.6 放射性废液管理系统尽量避免与含有非放射性液体的系统安装在同一区域，以避免由于非放射性液体泄漏而导致的放射性废液体积的增加。或者，在设计中避免此类泄漏，或将非放射性废液与放射性废液分开收集。

4.10.3.7 所有装有放射性废液的贮罐均应设置一个具有高液位报警的液位监测装置，该装置可进行就地和控制室报警，用于提醒采取措施避免贮罐溢流。

4.10.3.8 为避免污染地下水，含有放射性废液的管路和设备应安装在有足够容量来容纳和包容全部废液泄漏的房间内，或者应采用其他方法来滞留全部废液。

4.10.3.9 放射性废液管理系统的设计应该使得任何废液贮罐的破裂没有（或仅仅是轻微的）放射性后果，并且不需要采取任何厂外防护行动。

4.10.4 固体废物处理系统

4.10.4.1 固体废物处理系统的设计应解决以下问题:

（1）固体废物的收集、处理和贮存，包括分拣、减容（例如粉碎和使用压实机或焚烧炉），可压缩废物或焚烧灰的整备、固体废物（例如废树脂和过滤器）的整备（例如在桶内）;

（2）在运输至许可的放射性废物处置设施之前，已整备好的固体废物应在现场贮存；应明确厂内贮存容量;

（3）监测并清除废物包装外表面的表面污染;

（4）测量以确定废物包的特性，建立废物包存量（例如放射性核素种类、活度和放射性废物包的质量、体积等）;

（5）包装标识;

（6）数据记录。

4.10.4.2 固体废物处理系统的设计应包括处理在正常运行和预计运行工况产生的固体废物，应控制固体废物处理过程中放射性废液和废气的产生。

4.10.4.3 固体废物处理系统的设计应考虑预计运行事件工况及事故工况下可能导致的高辐照水平情况，并能提供充分足够的防护和安全保障。

4.11 除应急电力系统外的应急动力供应系统

4.11.1 对于依赖于交流电源执行安全功能的核动力厂需设置应急电力系统和应急动力供应系统，执行本节应急动力供应系统的相关要求；而对于依靠浮力、重力或存储能源等不依赖于交流电源来执行安全功能的核动力厂而言，本节要求做适当参考，但不做功能性要求。

4.11.2 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厂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。

4.11.3 为安全系统提供应急动力源的应急动力系统应被当作安全系统的辅助设施，向安全系统和其他指定的安全重要物项提供和分配动力，以驱动泵、压缩机和发电机，操作阀门、仪表和控制设备。应急动力系统分为电力部分和机械部分:

（1）应急动力系统的电力部分即应急电力系统，包括为产生、变换电力和将电力分配到需要电力的安全系统所必须的部件和系统;

（2）应急动力系统的非电部分即机械部分，是指为向应急发电机组和安全重要部件供应机械动力或机械能（非电能）而设置的那一部分应急动力系统，包括汽轮机、水轮机、柴油发动机和启动发动机的压缩气罐等。

4.11.4 许多情况下，应急电力系统与机械部分有直接接口，以下各条款所述的设计准则，仅用于应急动力系统的非电部分，应急电力系统的相关设计在其他导则中进行阐述。

4.11.5 机械设备输入侧的边界包括在核动力厂设计要求的时期内向原动机提供足够燃料(例如压缩氮气、压缩空气或燃油等）的贮存容器[2]。应急动力系统在负荷侧的边界直至由应急动力系统提供动力的部件处。

4.11.6 应尽可能避免机械设备的多重序列之间的自动连接。

[2] 在由压水堆蒸汽发生器产生蒸汽的情况下，应急动力系统的边界位于与工艺系统连接的管道处。

若在多重序列之间设置任何连接，则必须证明：在满足所连接的安全系统的负荷要求中已考虑了故障从一个序列向另一序列扩展和电源过载的可能性。还必须考虑到事实上这种连接降低了各序列及其所连接的安全系统负荷的独立性。

4.11.7 应急动力系统机械设备的控制

4.11.7.1 控制应该是自动的。只有证明在考虑了人因的前提下手动控制的性能是足够可靠的，才允许采用手动控制。机械设备的控制功能应包括以下方面：

（1）如果正用于其他模式，则自动切换到完全专用于应急需求的模式；

（2）自动启动备用机组的功能；

（3）在根据（1）切换到应急模式的情况下，旁路那些仅用于对正常运行、试验和维修模式的设备进行保护的保护装置。

4.11.7.2 应提供手动控制，以易于实现核动力厂的各种模式（即正常运行、试验和应急动力系统的维修）。

4.11.7.3 应设置足够的设备以完全控制应急动力系统的每一序列，这些设备必须与控制其他序列的设备实体分隔，并被包容在与其所属序列相对应的结构内。控制设备如集中设置（例如设置在控制室内），则应在应急动力系统的不同序列的仪表和控制设备之间设置适当的实体分隔和隔离装置，使得任何影响上述仪表和控制设备的假设始发事件都不会妨碍应急动力系统执行其功能。

4.11.8 非电应急动力源

4.11.8.1 非电应急动力源必须包括具有全部辅助设备及其分

隔且独立的专用贮能源（例如油源和水源）的成套原动机组。

4.11.8.2 非电应急动力系统必须设计成具有在所有运行状态和事故工况下、当假定发生某单一故障时能成功地执行其安全功能的裕量和能力（在设计基准中规定）。此裕量和能力必须通过分析来确定，并通过试验加以验证。这些试验考虑了所有连续的、断续的和瞬时的负荷需求的作用（包括加负荷的顺序及必须向每一负荷提供动力的持续时间）。

4.11.8.3 非电应急动力源必须有足够的能力在预计运行事件和事故工况下，按设计基准中的规定启动所有负荷并向它们提供动力。

4.11.8.4 在预计运行事件或事故工况期间，应急动力系统设备应只专用于应急需求。在非应急工况下，可以利用应急动力系统满足正常运行和发电系统的动力需求。必须假定：当要求应急动力系统提供动力以应对假设始发事件时，不被自动断开的非安全重要负荷都处于接通状态，并且被包括在总负荷的计算值内。

4.11.8.5 确定非电应急动力源时必须满足的要求包括：

（1）按规定的加负荷顺序启动和带负荷的时间；

（2）工作性能包括在要求的时间内空载、轻载、带额定负载、启动负载以及过载运行的能力；

（3）在整个负载范围内分批带负荷的能力；

（4）非电应急动力源的启动可靠性。

4.11.9 压缩空气通常属于核动力厂的非电应急动力源，在任何预计运行事件或设计基准事故下，提供必要的动力以使得某些仪表或执行机构能执行其安全功能。

4.12 应急电源和替代电源的支持系统

4.12.1 总述

对于依赖于交流电源执行安全功能的核动力厂，其应急电源的支持系统应满足 4.12.2~4.12.7 的要求；对于依靠浮力、重力或存储能源等而不依赖于交流电源执行安全功能的核动力厂，4.12.2~4.12.7 的要求可供参考。

4.12.2 系统组成

每个应急电源应设有完全独立的支持系统。这些系统应包括:

（1）燃油贮存及输送系统;

（2）冷却水系统;

（3）润滑油系统;

（4）空气起动系统或直流电机起动系统;

（5）燃烧空气进气及排气系统。

4.12.3 通用要求

应急电源应急运行所必需的重要辅助系统和支持系统应被认为是支持完成安全功能的系统。这些辅助系统和支持系统应满足安全分级的要求，并满足下列设计要求:

（1）这些系统应由应急动力源提供动力。

（2）这些系统应免受内部危险和外部危险的影响。特别是，多重序列应保持足够的隔离，重要辅助系统和支持系统在经受 SL-2 地震后应保持功能可用。

（3）这些系统应能进行定期检查和试验。

（4）设备应根据适用的质量标准进行设计、制造、安装和

试验。

（5）设备应根据适用的规范进行设计和制造。

4.12.4 构筑物抗震要求

应急电源运行所需的辅助系统和支持系统应安装于抗震 I 类构筑物内。

4.12.5 燃油贮存及输送系统

4.12.5.1 通常情况下，每个应急电源配备一只日用油箱，该油箱由一只燃油主贮存罐进行供油。每个应急电源的日用油箱应具有足够的容量，以满足在操作人员介入并恢复油箱液位所需的时间内柴油机满负荷运行的要求。

4.12.5.2 燃油主贮存罐应能在设计基准事故所要求的时间内为应急电源满负荷运行独立提供燃油。

4.12.5.3 每个应急电源应设置独立、可靠的燃油贮存及输送系统，以确保在预计运行事件和设计基准事故下，同时考虑失去厂外电源时应急电源运行所需的燃油供应。

4.12.5.4 应具备在设计基准事故情况下对燃油主贮存罐进行补油的能力以确保应急电源能长期运行。此外，还应考虑厂外足够且适用的燃油油源的可用性和运输，以及对燃油主贮存罐进行补油的方法。

4.12.5.5 在由地震导致失去厂外电源的工况下（即厂外电源在长时间内不能恢复），场内燃油贮存量应足以确保核动力厂所有应急电源的运行。储存的燃油量的确定应基于恢复厂外电源所需的时间或重新供应燃油所需的时间。

4.12.5.6 应定期对燃油量进行验证，对燃油品质进行检测，

以确保能满足最低运行要求。

4.12.5.7 燃油贮存及输送系统应免受厂址相关危险的影响，例如地震和极端天气条件。

4.12.5.8 每只燃油主贮存罐应设有补油和通气管线。应对这些设备进行保护以最大限度地减小车辆或外部危险造成损害的可能性。燃油主贮存罐室外露天布置时，补油和通气口的位置应高于设计基准洪水位。

4.12.5.9 应采取措施减轻燃油贮存及输送系统的火灾和爆炸危险。设计中应考虑下列措施:

（1）燃油贮存及输送系统中不易进行巡检且易发生泄漏风险的部位的泄漏检测和控制的能力，包括泄漏严重时隔离系统部件的能力;

（2）油箱破损时包容燃油的防火堤;

（3）油罐的布置应远离主控室，以防止油罐爆炸和（或）火灾情况下对主控室操纵员或设备造成损害。

4.12.5.10 应设置日用油箱至燃油主贮存罐的溢流管线，以将燃油输送泵输送的多余燃油进行回流。

4.12.5.11 应急电源日用油箱的标高应确保机带燃油泵具有足够的正压头。如果需要设置燃油增压泵，该泵应由可靠电源供电，当柴油机燃油进机压力低于设定值时应自动启动。

4.12.5.12 如果使用双壁燃油主贮存罐（例如埋地储罐），内、外壁之间的环形区域应设置泄漏检测系统。

4.12.6 冷却水系统

4.12.6.1 每个应急电源应设置冷却水系统。一般情况下，该

冷却由集成在应急电源上的闭式循环提供。每套冷却水系统应包含缸套水加热器、循环泵、三通道恒温阀和润滑油冷却器，维持柴油机处于热备用状态，保证应急电源起动时不会导致机械损伤。

4.12.6.2 每个应急电源应设有将热量传导至最终热阱的冷却水系统，以维持应急电源的温度在设计规定的限值范围内。

4.12.6.3 设计中应采取措施防止长期腐蚀和有机污染导致冷却水系统的冷却水品质下降。应采取预防措施保证缓蚀剂或防冻液与设备材料相容。

4.12.6.4 当应急电源接收到起动信号，冷却水系统应自动提供所需的冷却（从备用状态切换至所需的冷却状态）。

4.12.7 润滑油系统

4.12.7.1 应急电源的润滑油系统由油底壳、润滑油冷却器、润滑油净化器和润滑油滤器组成。

4.12.7.2 每个应急电源应设有润滑油系统，该系统包含:

（1）润滑油过滤系统，维持柴油机运行所需的润滑油品质;

（2）润滑油冷却系统，维持润滑油温度在设计规定的限值范围内;

（3）当应急电源处于备用模式时保持润滑油单元加热和补油的系统。

4.12.7.3 润滑油系统应设有预防爆炸并减轻此类事件后果的措施（如放气口）。

4.12.7.4 润滑油系统的容量应足以保证地震导致失去厂外电源的工况下应急电源可运行。此外，场内润滑油的存储量应足

以保证应急电源可长期运行直至场内润滑油恢复供应为止。

4.12.8 替代电源的支持系统

4.12.8.1 每个替代电源应设有专用的辅助系统和支持系统，在失去厂外电源和应急电源工况下支持替代电源运行。这些系统包括燃油贮存及输送系统、润滑油系统、冷却水系统、燃烧空气进气及排气系统、起动系统和电气系统。尤其是，起动系统的设计应允许多次起动而不需要给起动空气瓶重新充气或给起动蓄电池组重新充电。

4.12.8.2 应急电源辅助系统和支持系统与替代电源辅助系统和支持系统之间的共因故障应降到最低。

4.12.8.3 替代电源重要辅助系统的设计应免受外部危险（如极端天气）和内部危险的影响。

4.12.8.4 替代电源辅助系统和支持系统的设计应保证这些系统在恢复厂外电源或应急电源所要求的时间内正常运行。存储的燃油量应根据恢复厂外电源或重新恢复燃油供应所需的时间确定。

4.12.8.5 替代电源的定期试验中，应验证辅助系统和支持系统的可用性以及燃油量。

4.13 其他系统

4.13.1 总述

本节针对《规定》中没有明确说明的辅助系统和支持系统给出设计建议。这些系统的设计考虑与本导则中的其他系统类似。

4.13.2 设备和地面疏水系统

4.13.2.1《规定》对设备和地面疏水系统没有具体的规定，

但是要求采取适当的手段将向环境排放的放射性废液保持在可合理达到的尽量低的水平。

4.13.2.2 设备和地面疏水系统应有选择地收集反应堆冷却剂系统、辅助系统和支持系统、换料水池和乏燃料水池产生的废液、废气以及核动力厂产生的潜在污染的废液（例如来自地面冲洗、洗衣和去污等活动），输送这些废液、废气到合适的贮存和废物管理系统。对于重水堆，来自含有重水的系统的所有泄漏应收集并泵送回该系统。

4.13.2.3 机组正常运行期间，设备和地面疏水系统应:

（1）监测反应堆冷却剂系统的泄漏和测量安全壳内的泄漏;

（2）通过尽量回收废液、优化放射性废液处理工艺以及控制流出物排放，限制流出物向环境的排放。

4.13.2.4 如果事故工况下产生的废液放射性水平过高导致短期内难以处理（如果采用贮存优先于处理的方式），则设备和地面疏水系统应具备将核辅助厂房或安全壳外的高水平放射性废液再注入到安全壳的能力。

4.13.2.5 正常运行期间，设备和地面疏水系统应有助于减少核岛厂房放射性物质的滞留，并通过放射性水平监测限制向环境中的排放。设备和地面疏水系统可提供内部水淹和爆炸的防护（例如防止含氢流体氢爆），直接有助于实现安全功能。

4.13.2.6 设备和地面疏水系统应设计成能够:

（1）收集废液，并根据废液是否回收或者其放射性特性将其转运到各个合适的系统;

（2）收集来自一回路系统的含氢废液或含氧废液，以便于

硼回收或硼循环利用（例如冷却剂贮存和处理系统）;

（3）收集的不可复用废液则转运送至放射性废液处理系统，根据需要进行处理或监测排放到环境中;

（4）排空一回路系统，例如在卸料和通风前的排空。

4.13.2.7 设备和地面疏水系统应具备足够的能力，可以收集核动力厂运行状态下的放射性和非放射性废液。放射性和非放射性液体应分开收集。

4.13.2.8 设备和地面疏水系统的部件应根据其功能和作为屏障的作用进行分级，并满足相应的设计要求（例如多重性、应急动力源、内部和外部危险防护、定期检查和试验、维护和质量保证）。以下设备通常为安全级:

（1）用于水淹分析的监测设备;

（2）执行安全壳隔离功能的设备。

4.13.2.9 设备和地面疏水系统贯穿安全壳的管线应具有满足单一故障准则的自动安全壳隔离特征。以上部分应属于安全级设备并满足相应的设计要求（例如多重性、应急动力源、内部和外部危险防护、定期检查和试验、维护和质量保证）。

4.13.2.10 含有放射性物质且其失效会导致厂外放射性后果的设备和地面疏水系统部件应被视为安全重要物项，并应有相应的安全等级。安全重要物项应该能够与非安全重要物项隔离。

4.13.2.11 在管道破裂、储罐泄漏和其他潜在来源（例如非抗震设计的储罐由于地震造成破损泄漏）导致水淹时，设备和地面疏水系统应不影响所在厂房的安全系统和设备。

4.13.2.12 设备和地面疏水系统的地坑应设置封盖，以阻止污

染流体进入大气，并避免污染其他可再复用的流体。地坑封盖的设计应避免正常运行时厂房地板上废液滞留。

4.13.2.13 设备和地面疏水系统的地坑潜水泵应满足低频率维修要求，应设置保护措施以防止各种可能损坏或阻塞泵的物体掉落到地坑中。

4.13.2.14 设备和地面疏水系统的地坑潜水泵应设置过滤装置，以防止地坑废液中可能含有的颗粒和碎片对泵造成损害。

4.13.2.15 设备和地面疏水系统的地坑，应配置液位仪表，当液位高时则触发报警提醒操作人员厂房内存在水淹的风险。必要时，每个地坑和箱体应配置一台液位测量仪表。

4.13.2.16 在可能产生污染的区域，设备和地面疏水系统的设计应能够防止污染扩散到其他区域。

4.13.2.17 为了保证在相邻防火区发生火灾情况下设备和疏水系统的可运行性，应尽可能将其独立于其他防火区的同类设备。

4.13.3 移动设备补水及水源

4.13.3.1 核动力厂应设置适当的移动设备和接口，在发生超过设计基准的极端外部危险（例如风暴、地震）时，为核动力厂有关系统进行补水以带走堆芯余热和乏燃料释放的热量。

4.13.3.2 设计阶段应对现场可用水源进行综合评价，并考虑对各补水操作水源的优先顺序和利用方式。在确定补水水源优先顺序时，应考虑下列因素:

（1）一回路补水优先选用含中子毒物（如硼酸）的水源和便于添加中子毒物的水源;

（2）优先考虑抗震水源;

（3）优先考虑附近可达且便于连接操作的水源;

（4）优先考虑淡水，在淡水失去或用完的情况下考虑对厂址附近海水的利用。

4.13.3.3 应考虑一回路或乏燃料水池应急补水中硼浓度稀释的风险。

4.13.3.4 在失去最终热阱或受到外部危害时，为了通过蒸汽发生器实现长期冷却，移动设备可为应急给水系统提供应急补水。

4.13.3.5 设置的应急补水接口、隔离装置应与接入系统具有相同的安全级别，隔离装置后抗震要求应与接入系统相同，接口的设置应方便人员操作。