核安全导则　HAD 102/13-2021

核动力厂电力系统设计

(国家核安全局 2021 年 9 月 30 日批准发布)

国家核安全局

核动力厂电力系统设计

（2021 年 9 月 30 日国家核安全局批准发布）

本导则自 2021 年 9 月 30 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

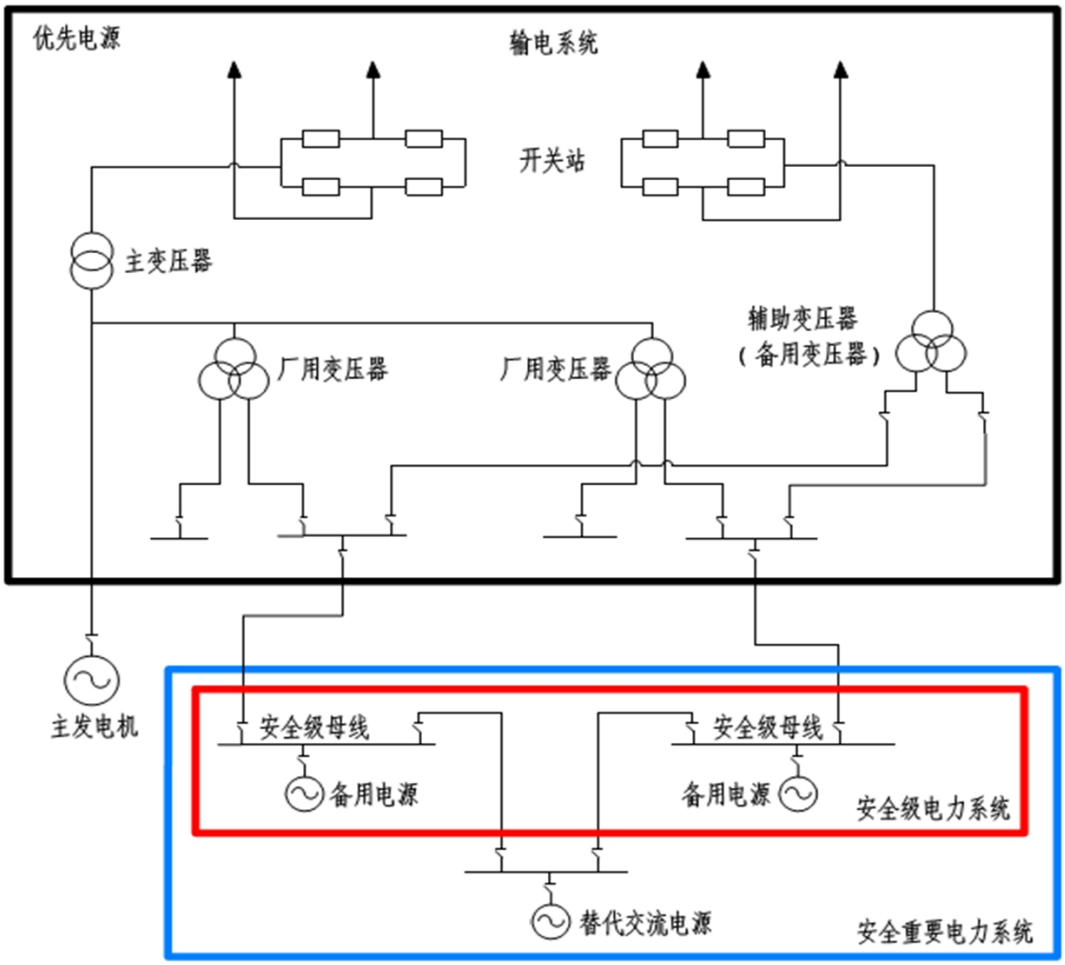
1.1.1 本导则是对《核动力厂设计安全规定》（HAF102）有关条款的说明和细化，其目的是给新建核动力厂电力系统的设计提供指导。本导则的主要内容可作为在役核动力厂设计修改和安全审查的参考。

1.1.2 本导则的附录为参考性文件。

1.2 范围

1.2.1 本导则中的核动力厂主要是指为发电或其他供热应用（诸如集中供热或海水淡化）而设计的，采用水冷反应堆的陆上固定式核动力厂。其他类型或采用革新技术的反应堆设计可参考本导则，但应经过细致的评价和判断。

1.2.2 本导则中电力系统包括厂外电力系统和厂内电力系统。厂内电力系统分为安全重要电力系统和非安全重要电力系统。安全重要电力系统、安全级电力系统和优先电源间的关系可参见图1。



注：

1. 本图以能动型安全系统的核动力厂为例来说明典型的电力系统设计；

2. 采用非能动安全特征设计的核动力厂，电力系统设计方案应满足其总体安全要求；

3. 本图未包含低压交流系统和直流系统；

4. 本图接线方式仅为示意。

图 1 核动力厂安全重要电力系统、安全级电力系统和优先电源间的关系

2 电力系统概述

2.1 总体要求

2.1.1 核动力厂电力系统应满足以下要求：

（1）系统和设备的性能和容量应具有足够裕度以满足执行

其预期安全功能的要求；

（2）紧急情况下，核动力厂电力系统可耐受持续性的过负荷、过电压，同时保留必要的保护动作，以保证安全级电力系统的功能；

（3）保护定值的选取应考虑厂内和厂外电力系统运行参数的预计变化范围。

2.1.2 应系统性地定义电力系统的结构、系统和设备，以保证执行安全功能的物项由相应安全级的电源供电，并通过合理的设计、试验、运行和维护来保证电力系统的可靠性。

2.1.3 为防止电力系统发生共因故障，需识别可能对电力系统安全造成威胁的事件并采取有效的预防措施，明确设计基准并定期复核。可采用电源多样性配置来防止电力系统发生共因故障。

2.1.4 应特别关注安全级电力系统和安全等级较低的系统之间的接口设计，需确保在核动力厂电力系统产生扰动时，非安全级设备不会对安全级设备造成不利影响。

2.1.5 应考虑电压和频率的暂态和短时波动对核动力厂电力系统和设备可能造成的影响。电网预期的电压和频率变化不应对核动力厂安全重要电力系统的功能造成不可接受的影响。

2.1.6 应采用合理的保护配置方案，以保证优先电源的扰动不会影响安全级电力系统及其负荷的安全运行。在应急情况下，安全级电力系统设备的保护装置可只保留必需的功能，以保证其优先执行安全功能。

2.1.7 当电气设备在开关操作、故障电流等作用下产生高温、弧光或机械应力时，应采取恰当的设计来保证人员安全并避免设

备遭受不可接受的损害。

2.1.8 应采取恰当的设计保证电力系统可承受各种工况下可能出现的过电压。

2.2 厂外电力系统

2.2.1 厂外电力系统在各种核动力厂状态下均向其提供电源。厂外电力系统也为电力送出提供通道。厂外电力系统对于核动力厂安全方面的重要作用体现在其通过高压厂用变压器或辅助变压器（备用变压器）为厂内电力系统提供可靠的电力供应。

2.2.2 厂内电力系统的设计应考虑厂外电力系统供电能力、供电质量及其对核安全的影响。

2.3 厂内电力系统

2.3.1 当厂外电力系统不可用时，厂内电力系统的作用是在核动力厂发生预计运行事件或事故工况后，将核动力厂带到并维持在可控状态或回到安全状态，直到厂外电源恢复。厂内电力系统由厂内电源和厂内配电系统组成。

2.3.2 厂内电力系统根据其安全重要性可分为安全重要电力系统和非安全重要电力系统，安全重要电力系统按照其应对的工况分为安全级电力系统和用于设计扩展工况的安全设施。

2.3.3 根据不同负荷的供电要求，厂内电力系统通常可分为三类：

（1）交流电力系统：由该系统供电的交流负荷允许一定时间的供电中断。交流电力系统包括部分优先电源、主发电机、备用电源和替代交流电源，当系统检测到优先电源和主发电机丧失

后，会自动启动和投入备用电源。

（2）直流电力系统：直流电力系统可由蓄电池向直流负荷不间断地供电。对不同安全级的负荷，宜由相应安全级别且相互独立的直流电力系统供电。若不同安全级的负荷由同一系统供电，不同安全级物项间的隔离应满足本导则第 3 章的相关要求。

（3）交流不间断电源系统：由直流电力系统或专设的蓄电池通过逆变器向交流不间断电源系统供电。在系统维护或故障情况下，交流不间断电源系统可通过旁路开关由交流电力系统向负荷直接供电。

2.4 优先电源

优先电源包含部分厂内电力系统和部分厂外电力系统，是在事故和事故后工况下，从输电系统优先给安全级电力系统供电的电源。

2.5 核动力厂接入电网要求

2.5.1 核动力厂和电网应从设计上进行合理的性能匹配，当其中一方运行状态发生显著变化时，另一方应通过适当的运行配合来保障双方的安全稳定运行。

2.5.2 电网的高可靠性对核动力厂电力系统的供电安全和稳定运行至关重要，同时，核动力厂的发电机组应能支持电网的稳定运行。

3 电力系统设计总体原则

3.1 总体要求

3.1.1 应确定核动力厂电力系统的设计基准，设计基准应包括电力系统执行的功能、具备的特性、达到的目标、运行工况、环境条件和可靠性要求。设计基准应考虑所有的运行模式和各种可能会影响核动力厂电力系统的事件。

3.1.2 核动力厂电力系统应满足设计基准中的稳态和瞬态工况的所有功能要求。引起厂内电力系统对称或不对称扰动的始发事件如下：

（1）厂外输电系统中的核动力厂并网、解列、停机，以及由于电网故障或电压和频率变化超限导致的核动力厂与电网断开连接；

（2）主发电机跳闸引起的厂内电力系统连接至厂外或其他厂内电力系统；

（3）厂内电力系统中电动机启动、单相接地故障或开关操作冲击。

应评价此类事件对所有厂内交流和直流电力系统的影响，并应通过分析确认其满足规定的电压、频率要求，同时也应确认保护系统满足要求。

3.1.3 应通过暂态稳定性分析证明核动力厂能耐受电网的扰动并保持与电网的连接，而不会导致发电机失去和电网的同步。

3.1.4 应将全厂断电作为设计扩展工况进行考虑和分析，其发生频率应足够低。全厂断电主要考虑核动力厂内重要的和非重要的配电装置母线全部失去交流电源(例如，在失去厂外电源的同时，汽机脱扣并且厂内应急交流电源故障)，但是未失去由蓄

电池经过逆变或替代交流电源供给的交流电源。

3.1.5 在全厂断电工况下，应分析核动力厂维持基本安全功能的能力。在设计中应采取有效措施，防止在全厂断电时堆芯和乏燃料出现严重损伤。

3.1.6 提高核动力厂应对全厂断电能力的措施包括：

（1）增加为安全级仪表、控制设备以及其他重要设备供电的蓄电池容量；

（2）设置机组间的互相连接；

（3）配置多样化的替代交流电源。

3.1.7 应基于确定论方法划分安全重要电气物项的安全重要性，并适当辅以概率论方法。使用概率论方法时，应考虑以下因素：

（1）该物项要执行的安全功能；

（2）未能执行其安全功能的后果；

（3）需要该物项执行某一安全功能的可能性；

（4）假设始发事件发生后，需要该物项执行某一安全功能的时刻或持续时间。

3.1.8 电力系统分类分级应符合《核动力厂设计安全规定》及其相关导则的要求。

3.2 可靠性设计

3.2.1 安全重要物项的可靠性应与其安全重要性相适应。应对所有安全重要系统进行系统性评价，以确认设计基准中提出的可靠性要求已在系统设计中落实。

3.2.2 在设计安全级电力系统时，应采用多重性、多样性、

提高故障耐受能力、保持设备和系统独立性、避免共因故障、提高可试验性和可维护性、采取故障安全设计以及选择高质量设备等措施来保证安全功能的可靠性。

3.2.3 安全级电力系统应根据设计基准中的可靠性要求进行多重配置。安全级电力系统的多重配置情况，应符合可靠性目标并符合单一故障准则。为了充分发挥多重作用，不同的安全序列间须保持独立性。

3.2.4 应考虑安全级物项发生共因故障的可能性，可采用多样性、多重性和独立性原则来保证其可靠性。

3.2.5 应采用实体隔离、电气隔离、功能独立和通讯（数据传输）独立等措施，防止安全系统的多重序列之间发生相互干扰。

3.2.6 安全级电力系统应与安全等级较低的系统之间保持独立，如无法满足上述要求，则需采取有效的隔离措施，以防止低安全级别物项的故障影响高安全级别物项执行其预期安全功能。

3.2.7 独立性是为了防止安全级电力系统的多重序列间，以及不同纵深防御层次的系统间同时受到某一故障或内外部危险的影响，需要考虑的因素包括：

-. 设计基准事故造成的故障；

-. 受相同的内、外部危险影响；

-. 公用支持系统的故障；

-. 系统间或序列间的电气连接；

-. 系统间或序列间的数据交换；

-. 设计、制造、运行、维护中的共性缺陷。

3.2.8 安全级物项不应受到所需应对事故的影响。

3.2.9 多重的安全序列应彼此独立，以确保其在事故期间和之后执行预定的安全功能。

3.2.10 电力系统、设备和设施的局部故障不应造成其余部分不可用。

3.2.11 安全级电力系统的辅助支持设施的功能失效不应破坏安全级电力系统多重序列之间或安全级电力系统与安全等级较低的系统之间的独立性。例如，将房间通风设施划分为与其支持的安全级电力系统相同的序列，可防止一列安全级电力辅助支持设施的机械功能丧失导致另一列电力系统安全功能的丧失。

3.2.12 不同安全等级系统之间的隔离装置的分级应与较高安全等级的系统保持一致。

3.2.13 应证明实体隔离、电气隔离和相关电路设计的合理性，以满足独立性要求。

3.2.14 实体隔离可通过设置屏障、保持隔离距离或两者相结合的方式来实现。

3.2.15 电气隔离用于防止系统内部的电气故障影响与其连接的其他系统。一般情况下，安全级电力系统不应向非安全级负荷供电。当安全级电力系统需要向非安全级负荷供电时，应使用安全级隔离装置进行隔离。

3.2.16 应采取保持分隔距离、设置隔离装置、采用屏蔽、合理布线等措施或多种措施相结合的方式，以满足电气隔离的要求。

3.2.17 安全级电力系统的多重序列之间不应互相连接。若安全评价表明不同安全序列之间的连接可以显著增加电源的可靠

性，并可保证不同序列间的独立性，则可允许在多重序列之间建立临时连接，这些临时连接可用于应对全厂断电。

3.2.18 若核动力厂电力系统满足以下要求，则可在停机期间实施多重序列之间的临时连接。

（1）具备有效的闭锁措施，不能通过简单的开关操作解除；

（2）临时连接对核动力厂安全可靠性的影响和对诱发共因故障的影响是可接受的。

3.2.19 如果在安全级电路和安全等级较低的电路之间无法提供有效的电气隔离，则安全等级较低的电路应该：

（1）通过分析或试验证明其不会对与之相关的安全级电路造成不可接受的影响；

（2）确定其为安全级电路的相关电路。

3.2.20 安全级电力系统应由多样化的电源供电。通常情况下，安全级电力系统的电源来自：

（1）作为正常电源或带厂用电负荷运行的主发电机；

（2）通过优先电源供电的厂外电力系统；

（3）在厂外电力系统和主发电机均失去时，为安全级电力系统供电的备用电源；

（4）应对全厂断电时的电源，如替代交流电源。

3.2.21 如果将非电动力系统作为多样化手段来完成特定安全功能，则其相关的动力源、仪表和控制系统应独立于其多样化对应的原系统。多样化的非电动力系统可使用蒸汽或发动机直接驱动的设备。

3.2.22 在安全级电力系统及其支持系统的设计、试验、维护和运行过程中，应考虑发生共因故障并导致其无法执行安全功能的可能性。

3.2.23 应采取应对电力系统电压瞬态的措施，以使发生共因故障的风险降至可接受的水平。

3.2.24 应对源自电网共因故障的主要防护措施包括：

（1）建立全面的设计基准和安全规范，明确可能对安全级电力系统构成威胁的所有事件；

（2）通过本质特征或继电保护，证明安全级电力系统应对这些事件的能力；

（3）证明电网的电压/频率偏移不会传递至由整流器和逆变器供电的母线。

3.2.25 应对备用电源共因故障的主要措施包括：

（1）建立全面的设计基准和安全规范，明确所有可能对备用电源的控制、启动和运行构成威胁的事件；

（2）通过恰当的设计，证明备用电源具备应对这些事件的能力，包括加载期间的瞬态性能；

（3）多重的控制电路和设备可保证启动的可靠性和运行的连续性，并避免误跳闸。

3.2.26 为尽量减少软件设备共因故障的风险，电气软件的多样性应遵循核动力厂仪表和控制系统设计相关导则的要求。

3.2.27 应恰当地考虑故障安全设计原则，并落实到核动力厂安全重要系统和设备的设计中。当适用时，应将安全重要系统和设备设计为故障安全，使其自身的故障或支持设施的故障不影响

预期安全功能的执行。

3.2.28 应定义安全重要电气设备的故障模式，应可通过定期试验排查安全重要电气设备的故障。

3.3 设备额定值

3.3.1 电气设备的额定值应有足够的裕度，并考虑后续核动力厂优化和改造的需求。电气设备选择应满足如下条件：

（1）在允许的电力系统电压波动范围内，可承载回路工作电流；

（2）满足负荷运行要求而不超过温度限值；

（3）可承受规定切除时间内的系统短路电流；

（4）可承受短路峰值电流而不超过其机械强度。

3.3.2 应定期并至少在主要设备更换、核动力厂修改和定期安全审查时对设备额定参数的裕度进行验证，验证应基于保守假设和可信方法。

3.3.3 用于驱动安全重要物项的电动机应具有足够的输出转矩，以允许在电力系统设计基准规定的最低电压条件下起动。电动机额定功率、安全级电气设备容量和过载保护装置的整定值应与电动机实际负载以及输出转矩相匹配。

3.3.4 阀门电动装置应能够在电力系统电压和频率低限时仍可提供足够的转矩来打开或关闭阀门，且在电力系统电压和频率高限时不超过最大允许转矩。阀门电动装置的保护与力矩开关的定值应互相配合，以避免在运行过程中保护装置误动作。

3.3.5 驱动安全重要物项的电动机及其供电回路设备应能够

承受设计基准定义的稳态、短时和瞬态运行工况所导致的电压和频率波动。

3.3.6 电气设备及电缆的选择和鉴定应符合其使用条件和环境条件。电气设备及电缆应具有足够的阻燃性以防止火灾蔓延。

3.4 电缆及电缆通道

3.4.1 在计算电缆导体温度时，需考虑的因素包括：

（1）最高环境温度；

（2）正常电流和故障电流；

（3）负载率；

（4）在同一或附近通道中其他电缆的布置情况；

（5）电缆通道、穿墙、穿楼板、防火堵料和阻燃涂层对电缆发热的影响。

3.4.2 母线、电缆通道（即电缆桥架或电缆保护管）及其支架应设计成能够承受电缆及其附件的机械载荷，并留有适当的裕度。

3.4.3 安全级电力系统的母线、电气间隔和电缆应得到充分的保护，以应对假设始发事件可能造成的损害。可能影响母线、电气间隔和电缆的灾害包括火灾，以及流体系统、机械或结构设备的故障或失效。

3.4.4 安全级电缆应采取合理的敷设和防护措施，使其因火灾、旋转机械设备故障或支撑系统故障等外部事件损坏的电缆不超过安全分析中论证过的可接受的最小范围（通常是任一完整安全功能中的一个序列）。机械设备故障包括管道甩动、喷射冲击、旋转设备或其他高能系统故障产生的飞射物及其可能造成的后

果。

3.4.5 电缆和通道应采用永久标牌来标识列别。可在电缆和电缆通道的两端和固定间隔处设置永久标识，每根电缆应有适当的标识以确保其敷设在正确的通道中。

3.4.6 安全级电缆和设备之间的连接应使用经鉴定合格的连接装置。禁止在桥架内使用电缆接头。

3.4.7 应采用适当的方法对以下对象进行隔离：

（1）安全级与非安全级电缆；

（2）属于不同安全序列的电缆；

（3）不同电压等级的电缆。

3.4.8 可靠接地的金属保护管可作为有效的隔离屏障。

3.5 接地系统

3.5.1 接地系统通常包括系统接地、保护接地、防雷保护接地、信号接地，它们在物理上并不需要完全独立，所有的接地系统应连接到一个总接地网。

3.5.2 所有设备和装置的金属框架均应接地，或采取额外的措施来确保安全。

3.5.3 中压交流电力系统的中性点接地方式应结合核动力厂总体安全要求和电力系统安全要求综合考虑。在备用电源孤岛运行方式下，系统应采用高阻抗接地或者不接地方式。

3.5.4 当中压交流电力系统采用非有效接地方式时，应对电力系统接地故障进行监测，监测系统应易于识别故障地点，当出现对地绝缘降低时，应发出报警并维持设备继续运行。

3.6 防雷及浪涌保护

3.6.1 应采取有效措施防止雷击影响电气和仪控系统执行其安全功能。系统的防雷可采用外部或内部防护措施，也可采用内外部防护措施相结合的方式。

3.6.2 外部防护措施通常采用接闪器或由建构筑物金属部分构成的法拉第笼，以保护建构筑物及其设备免受雷击影响。外部防雷装置应就近接地，并使雷电电流在厂房外入地。

3.6.3 内部雷击防护通常采用屏蔽和避雷器，用于防止雷电流引起的感应过电压和传递过电压的危害。内部接地保护装置应与防雷接地系统连接，同时应避免人员和设备遭受传递过电压的伤害。

3.6.4 防雷保护系统与接地网之间的连接线应合理敷设，以保证雷电放电效应不影响安全级电力系统的安全功能。

3.6.5 为防止过电压超过被保护设备的允许电压限值，应在系统中合理配置浪涌保护器或避雷器。

3.7 设备鉴定

3.7.1 应制定安全级物项的鉴定大纲并开展鉴定活动，以证明核动力厂安全级物项能够在其整个设计寿期内以及支配性环境条件下执行其必要的预期功能，这里考虑的环境条件包括维修和试验。用于设计扩展工况的安全设施可根据其执行的功能确定是否需鉴定以及鉴定要求。

3.7.2 应对安全级电力系统和设备进行鉴定，以确保其能在使用寿期内执行预定的安全功能，鉴定应确保设备具有与其安全分级相对应的可信度。鉴定内容应包括：

（1）功能及性能的适用性和正确性鉴定；

（2）设备的环境鉴定；

（3）设备的内部和外部危险鉴定；

（4）电磁兼容鉴定；

（5）软件验证与确认（如有）。

3.7.3 鉴定方法应根据具体的系统或设备而定，可采用以下一种或几种方法的组合：

（1）型式试验；

（2）运行经验；

（3）分析法。

对已有运行经验物项的鉴定，宜采用运行经验法和分析法，并用设计制造记录和出厂试验作为补充。

3.7.4 设备鉴定程序应证明建构筑物、系统、设备以及软件的设计满足所有要求，包括在相关设计基准和设备技术规格书中要求的安全重要的性能、容量和可靠性。对于已竣工的电力系统和已安装的设备，应证明这些系统和设备能正确执行设计功能。

3.7.5 应在设备鉴定报告中论证鉴定理论、方法和假定条件的正确性。应保证每个已安装的被鉴定设备及其鉴定相关的依据可被追溯，不仅可追溯设备本身，也应可追溯其通过鉴定时的条件和实际安装的条件之间的差别和变化。

3.7.6 当采用运行经验作为设备鉴定方法时，应表明该运行经验与被鉴定对象的用途和环境条件相适应，所参考运行经验的设备应经过试验法鉴定。

3.7.7 在核动力厂各种状态下，安全级电力系统和设备应能适应相应运行环境的影响。环境鉴定应证明安全级电力系统和设备在设计基准规定的环境条件下可满足安全要求，环境鉴定只需要证明某一设备能够执行其安全功能，但不要求证明其所有功能完全可用。

3.7.8 应证明设备在考虑老化效应后（例如辐照老化和热老化）的鉴定寿命末期仍能执行预期功能。老化鉴定应足够保守，以应对无法预计到的老化机理。

3.7.9 在制定设备鉴定计划时，应考虑可信的最恶劣的环境条件组合，包括与运行条件之间的叠加效应。如果需要将被鉴定物项在不同环境条件下分别试验（例如分别进行辐照老化试验和热老化试验），应证明试验实施的顺序恰当地模拟了被鉴定物项在组合环境条件下的性能劣化。

3.7.10 当用保护屏障将设备与潜在环境影响隔离时，这些保护屏障本身也应经过鉴定。

3.7.11 在核动力厂设计时应考虑保护安全级电力系统和设备免受设计基准火灾、水淹、地震等内、外部危险的影响或将其设计成能承受这些内、外部危险并通过鉴定予以证明。

3.7.12 应通过对整个核动力厂的具体分析来明确电力系统和设备电磁兼容性能的详细要求。

3.7.13 电气、电子设备应能承受所在环境中的电磁条件，并通过相应的电磁兼容鉴定。

3.7.14 电磁兼容鉴定应证明电力系统和设备性能符合电磁兼容性能要求。电磁兼容鉴定包括：

（1）通过系统设计和设备设计使电磁噪声与电气元件的耦合最小；

（2）通过试验证明设备能承受预期电磁噪声水平；

（3）通过试验证明电磁发射在可接受的水平以内。

3.7.15 工业环境条件下的电磁兼容标准可作为核动力厂对电磁兼容的基本要求，必要时应对这些标准进行补充，以涵盖核动力厂设备对电磁兼容性能的更高要求。

3.8 老化管理

3.8.1 应确定核动力厂安全重要物项的设计寿命。设计寿命应充分考虑热老化、辐照老化和运行老化等与服役年限有关的性能劣化，从而保证安全重要物项在其整个设计寿期内执行所必需的安全功能的能力。

3.8.2 应考虑在核动力厂所有正常运行状态，包括试验和维修状态，以及在假设始发事件中及其后的老化效应。

3.8.3 应采取监测、试验、取样和检查措施，以评价设计阶段预计的老化机理，以及识别在使用中可能发生的未预期到的行为或性能劣化。

3.8.4 应确定显著影响电气设备的老化机理及劣化的跟踪方法。应制定维护程序、监测程序和老化管理程序，以识别可能导致设备不能执行其安全功能的性能劣化趋势，并采取有效的缓解措施。

3.8.5 设备鉴定寿命的再评定可以表明该设备的鉴定寿命是有效的，或表明该设备的使用寿命与鉴定寿命不符。设备的再鉴定信息可用于增加或减少该设备的鉴定寿命。

3.9 访问控制

3.9.1 应防止擅自接触或干扰包括计算机硬件和软件在内的安全重要物项。

3.9.2 应限制对安全重要设备的访问，尤其是对定值调整和设备校准的控制，以防止未经授权的访问并减少出错的可能性。

3.9.3 关于访问控制和计算机应用安全的更多要求见核动力厂仪表和控制系统设计相关的核安全导则。

3.10 可试验性

3.10.1 所有安全重要系统应具备可试验手段，包括适当的内置检测功能。为满足系统和设备的可用性要求，试验手段应与试验程序相协调。在确定试验频率时需考虑试验导致的故障率，并考虑某些试验只能在换料停运期间执行。

3.10.2 为保证安全级电力系统的可靠性，在核动力厂运行期间进行定期试验通常是必要的。如果试验会影响核动力厂的安全运行，则需避免在核动力厂运行时进行试验。

3.10.3 在包括功率运行的所有正常运行模式下，如需对安全级电力系统设备进行试验和校准，应能保持安全级电力系统执行其安全功能的能力。

3.10.4 如果安全级设备在功率运行期间不具备试验的条件，应符合以下要求：

（1）证明无法试验的影响是可接受的；

（2）应能在停堆期间进行试验。

3.10.5 应制定安全重要系统的试验程序，试验程序通常包括：

（1）试验目的；

（2）试验的系统和设备；

（3）主要试验安排；

（4）试验基准、依据及试验间隔；

（5）验收准则；

（6）所需文件和报告的说明；

（7）程序有效性的定期审查；

（8）用于管理试验实施的独立程序。

3.10.6 试验的范围和频率应符合功能需求和可用性要求。试验结论一般包括以下内容：

（1）系统和设备的客观状态；

（2）对设备劣化的评价；

（3）协助检测设备劣化的趋势数据；

（4）系统内出现早期故障的迹象；

（5）在重做失败的试验之前，为确定重复试验可操作性而应进行评价的要求。

3.10.7 在重复试验之前，应对试验失败的原因及采取的纠正措施进行评价和记录，重复试验的结果应可证明系统或设备的可用性。纠正措施可包括校准、维护或修理设备，或修改试验程序。

3.10.8 对电力系统中电子元器件的试验程序，包括含电子元器件的保护装置，还应满足核动力厂仪表和控制系统设计相关的

核安全导则中的相应要求。

3.10.9 应确定定期试验方法，并满足以下要求：

（1）在试验期间确保核动力厂的安全；

（2）定期试验既不影响安全级电力系统的独立性，也不增加发生共因故障的可能性；

（3）不应超过设计使用条件而使核动力厂的任何设备劣化（例如，在空载或频繁快速启动时，柴油机的可操作性或可靠性可能会降低）；

（4）为快速评价系统或设备的总体状态，应对各试验项目的实施顺序进行排序；

（5）确认系统和设备满足设计基准的功能和性能要求；

（6）试验程序应包括验收准则；

（7）应测试所有安全重要功能的输入和输出，如报警、指示、控制和驱动装置的动作；

（8）尽量减少任何安全动作误启动的可能性，尽量减少试验对核动力厂可用性造成的其他不利影响；

（9）尽可能减少设备退出运行的时间；

（10）尽可能在系统实际或模拟运行条件下实施试验；

（11）完成试验后，需验证任何因定期试验而受到影响的物项都已正确地回归到原来的正常运行状态。

3.10.10 如果设计上有考虑连接试验设备的接口，那么待试验的安全重要设备可以临时接入试验装置。

3.11 可维护性

3.11.1 安全重要电力系统的设计和安装应便于检测和维护，

便于维护人员和工具适时介入，并在故障的情况下容易诊断和维护，以尽量降低维护人员的人身伤害风险。

3.11.2 为便于电气设备的日常维护、故障排除和维修，设计上需考虑：

（1）设备不宜布置在通常处于极端温度或极端湿度的区域；

（2）设备不宜布置在可能有高辐射水平的区域；

（3）在执行所需的维护活动时人因的影响（能力和局限性）；

（4）应在设备周围留有足够的空间，以确保维护人员能够在正常工作条件下完成维护任务。

3.11.3 安全重要电力系统的维护方式对核动力厂安全造成的影响应可接受。

3.12 试验或维护期间退出运行的规定

3.12.1 当电气设备退出运行时，应确保其被正确隔离，以保护人员人身安全和避免误操作。

3.12.2 如果使用外接设备进行试验或维护，则外接设备的接口应具备硬件闭锁，以确保在没有人工干预的情况下，被试验或维护系统不能与试验或维护设备进行交互操作。

3.12.3 除非可以证明系统的运行可靠性是可接受的，否则安全级电力系统中任何单一设备退出运行都不应导致系统丧失最低的多重性要求。满足此要求的安全级电力系统应允许对其一部分进行定期试验，而其余运行部分可继续执行要求的安全功能。

3.13 多堆核动力厂的共用系统和设备

3.13.1 多堆核动力厂的每台机组都应配置相互隔离和独立

的安全级电力系统。安全级直流电源不应在机组间共用，安全级交流电力系统不宜在机组间共用。机组间如果需要共用安全级电力系统或设备，必须证明共用部分不会对安全级电力系统执行安全功能产生不可接受的影响。

3.13.2 应证明在机组之间共用系统或设备不会增加事故、共因故障发生的可能性或后果的严重性，也不会增加在维护共用系统的共用设备时导致一个或多个机组停机的可能性。

3.13.3 分析具有共用系统的单一故障准则符合性时，应满足以下条件：

（1）当共用系统或设备或与其有接口的支持系统出现单一故障时，所有机组的安全级电力系统仍可执行其安全功能；

（2）当各机组的非共用系统同时发生单一故障时，每个机组的安全级电力系统仍可执行其安全功能。

3.14 标记与识别

3.14.1 在核动力厂安全系统中的多重设备（包括电缆和电缆通道）之间的标识应易于识别且不需要经常查阅图纸或其他资料。不同安全序列或不同安全等级的设备应易于区分。标记可以采取标签或颜色编码的形式。

3.14.2 在核动力厂设计、建造和运行的各阶段，应使用协调一致的方法来命名和标识所有电气设备。

3.15 电气贯穿件

3.15.1 电气贯穿件是实现放射性包容安全功能的设备，应满足安全分级要求。

3.15.2 电气贯穿件应能够耐受持续工作电流和短时故障电

流并保持结构完整性，且泄漏率不会超过规定的水平。对于不影响贯穿件结构完整性的电气功能的安全分级，应和与其连接的安全壳内部设备保持一致。

3.15.3 电气贯穿件额定值的选择应当满足：

（1）贯穿件的额定持续工作电压不小于所在系统的标称电压；

（2）贯穿件的额定冲击耐受电压不小于所在系统最大预期的暂态过电压；

（3）贯穿件应能持续承载各种运行状态下的预期负荷电流，而不超过导体允许的温升限值或导致压力边界的劣化；

（4）在预期的电压波动条件下，贯穿件应能够安全地承受从短路发生至保护装置切除故障期间的短路电流。

3.15.4 安全壳贯穿件应配置多重的安全保护装置，且应动作于断开不同的开关设备。若分析表明非能动保护装置（例如熔断器）不会失效且假设始发事件不会影响其功能，则可选用单一的非能动保护装置（例如熔断器）来保护贯穿件。若贯穿件能长期承受安全壳内部故障导致的最大预期电流，则不需要配置多重的保护措施。在设定保护装置整定值时，应考虑电气贯穿件持续额定电流值和短时耐受电流值。

3.16 配电系统

3.16.1 每个配电系统应有足够的容量和性能，以满足下列要求：

（1）在所有设计工况下给所需的负荷供电；

（2）在电气故障情况下承受短时过电流；

（3）在设计基准中的稳态、短时和瞬态运行工况下不会损害配电设备。

3.16.2 电气保护配置及配合应达到可接受的水平以防止电气故障导致其安全功能的丧失。安全级电力系统的保护装置应作为安全级电力系统的一部分。数字化保护装置应按其执行的安全功能进行验证。

3.16.3 应正确选择并合理整定保护装置，以防止配电系统主回路和分支回路的设备、母线和电缆在过载和故障条件下损坏。所有主回路和分支回路应有过载和短路保护，并应对接地故障进行监测并在适当情况下给予保护。

3.16.4 多重序列的保护应保持独立。当系统发生异常会导致运行设备的降质或故障时，电气保护系统应及时将发生异常的部分系统切除。

3.16.5 保护装置应该具备以下功能：

（1）在检测到不可接受的状态时，保护装置应动作于开关装置并快速断开故障电流，以避免对系统设备造成危害并最大限度地减少扰动；

（2）在电力系统各种运行方式下，当发生短路和过载时，保护装置的动作应具备选择性；

（3）核动力厂的开关设备应具有适当的保护措施，以尽量减少潜在燃弧故障对开关设备造成的损坏，确保设备安全和运行维护人员人身安全；

（4）提供保护动作的指示和标识，记录和分析保护装置的

动作或试验结果；

（5）监测保护装置控制电源的可用性。

3.17 控制和监测

3.17.1 应在控制室配置适当的仪表和控制设备，以监测和控制厂外和厂内电力系统。

3.17.2 应提供足够的监测信息以评价安全级电力系统的可用性，这些信息包括：

（1）断路器位置；

（2）母线电压和电流；

（3）备用电源的电压、电流和频率。

3.17.3 应在主控室中显示安全级电力系统设备的不可用或旁通状态。对于频繁处于不可用或旁通状态的设备，其状态应在主控室中自动显示。安全级电力系统不可用或旁通状态的报警应由断电逻辑实现。

3.17.4 电力系统的所有安全动作应可自动启动。当满足下列要求时，安全动作也可采用手动操作：

（1）运行人员能从安全级电力系统的传感器和设备获得充分而明确的信息，以便对需要采取安全措施的必要性做出合理的判断；

（2）运行人员有足够的时间评价核动力厂的状况并完成所需的操作；

（3）运行人员有足够的控制手段来执行所需的操作；

（4）执行操作的运行人员之间的通信系统足以确保这些操

作的正确执行；

（5）为运行人员提供执行安全操作的书面程序和培训。

3.17.5 手动启动安全动作为防止自动控制系统的失效提供了一种后备方法，同时可支持长期的事故后操作。手动启动安全动作应可在系统级和设备级实施。

3.17.6 厂内电力系统的控制需包括以下功能：

（1）当正常厂外电源不可用时，应将特定负载自动切换到厂外辅助（备用）电源；

（2）当优先电源和主发电机异常且未恢复时，安全级电力系统应自动启动和接入备用电源，并按照规定顺序带载；

（3）替代交流电源宜采用手动方式接入系统；

（4）当正常电源恢复供电时，安全级电力系统宜能同期恢复到正常电源供电；

（5）在正常运行或停堆模式下，备用电源可手动切换至试验、维护和维修状态。

4 优先电源设计

4.1 总体要求

4.1.1 安全级电力系统的优先电源来自电网且相对独立。源自电网的干扰因素包括预期的电压和频率变化，上述干扰因素不得损害核动力厂安全重要物项的功能。在核动力厂启动、停机和紧急工况下，输电系统应向核动力厂稳定、持续地供电。在电网发生预计事件后，输电系统仍需与核动力厂保持连接。

4.1.2 当核动力厂处于功率运行时，安全级电力系统的电源来自主发电机，主发电机应适应电网的电压波动。对于具备孤岛运行模式的核动力厂，厂内电力系统应能适应机组从正常运行切换至孤岛运行过程中出现的电压和频率偏移等暂态过程。

4.1.3 在核动力厂所有运行模式下，每路厂外电源应有足够的容量和能力为所有用于缓解设计基准事故和预计运行事件影响的电气负荷供电。当核动力厂主发电机解列时，应注意电网电压变化对核动力厂厂内电力系统的影响。

4.1.4 核动力厂应设置两个或多个实体独立的厂外电源，以将厂外电源同时发生故障的可能性降低至可接受的程度。如果经安全分析论证满足要求，核动力厂（通常指具有非能动安全特征设计的核动力厂）也可采用一个厂外电源的设计方案。

4.1.5 当多堆核动力厂的多台机组共用厂外电源时，任何一台机组跳闸都不应影响其他机组厂外电源的可用性。

4.1.6 当厂用母线的主进线回路失电时，应自动切换至厂外辅助（备用）电源供电。应根据设计要求对厂用电源切换进行安全评价，安全评价应考虑切换过程中的电压波动和电流冲击。

4.1.7 应采取实际可行的设计方法，使核动力厂的两个厂外电源同时发生故障的可能性最小。

4.2 电网稳定性

4.2.1 在选择核动力厂厂址时，应进行电网稳定性评价。当电网稳定性不良时，可以考虑改善电网稳定性的措施，或在可能的情况下，选择另一个具有较高电网稳定性的厂址。

4.2.2 电网的稳定性与许多因素有关，包括：高峰和非高峰运行期间的系统发电容量和备用发电容量；旋转备用发电容量、发电机组的数量和容量及其特性；与邻近电力系统之间联络线的数量及其特性；输电线路的数量及其特性，包括其保护继电器和断路器的特性。

4.2.3 在增添新发电容量和设计电力系统网络时所采用的原则对电网的稳定性有直接的影响。例如，应按负荷潮流研究和稳定性分析来确定某特定系统的最佳机组容量及为保持系统稳定所需要的旋转备用容量。还应考虑电网其他扰动的可能影响，这些扰动可能导致系统电压和频率严重起伏并可能影响大电气设备（如反应堆冷却剂泵）的性能。

4.2.4 特别重要的是存在电网失去最大容量的发电机组造成电网不稳定输电而导致整个系统崩溃并因此而断开所考虑的电厂的厂外电源的可能性。一些电网当发电容量不足时通常采用卸去次要用户负荷的方法以维持系统频率稳定。如果频率降低过多，作为最终手段，使主发电机与电网解列。由于这些因素对电网的稳定性有影响，当为特定的电力系统选择核电机组时，应对其仔细考虑。

4.3 核动力厂和电网间的接口及通信

4.3.1 为保证核动力厂的安全运行和安全停机，电网公司和核动力厂营运单位需基于保证核安全、保证核动力厂供电安全的共同目标，建立特别的沟通配合机制。

4.3.2 核动力厂营运单位应将计划进行的以下活动告知电网公司，如停机、改造和维护，以及对核动力厂设计、配置、运行、

限值、电气保护系统或性能修改等可能影响电网向核动力厂供电能力的活动。

4.3.3 电网公司应将计划进行的以下活动告知核动力厂营运单位，如电网的停电、改造和维护等可能影响核动力厂厂外电源可用性和可靠性的活动。

4.3.4 核动力厂营运单位应与电网公司就电气保护和自动化方案进行配合，在电网发生故障时，应最大限度地保证核动力厂和电网的可用性。

4.4 开关站设计

4.4.1 应采取合理的开关站设计，以防止单台设备故障导致向安全级负荷供电的多回厂外电源同时故障。

4.4.2 开关站的控制电源应为开关站专用。主开关站和辅助（备用）电源开关站不应共用控制电源。

5 安全级电力系统设计

5.1 总体要求

5.1.1 在核动力厂各种运行模式下，均应保证电源系统的电压和频率波动不降低任何安全系统设备的性能。备用电源的电压和频率波动范围应在原动机和所供电负载的设计基准之内，不应影响正在启动、已加载或运行中的设备。在备用电源加载期间，允许出现电压和频率的短时偏差超出范围，但需确保电压和频率在下一个负载带载前恢复至可接受范围。

5.1.2 应系统性地识别由优先电源或厂内电源故障引发的安

全级母线电压和频率的稳态波动和暂态过程，应分析电力系统所有的运行模式以及对称性和非对称性故障，并确认保护配置的合理性。

5.1.3 应监测优先电源的异常状态（例如过电压、低电压、超频或低频）。当优先电源的异常状态超出设计要求的规定限值时，应自动断开受影响的安全级母线相应的电源回路。

5.1.4 为减少用电设备在电源切换期间经受的冲击，可延时投入厂外辅助（备用）电源，事故分析的结论应支持延时投入上述电源的合理性。

5.2 单一故障准则

5.2.1 为满足单一故障准则的要求，通常采用多重性、独立性、可试验性、连续监测、环境鉴定以及可维护性等设计原则。

5.2.2 出现下列情况时，安全系统应完成（导致预计运行事件或设计基准事故的）某一假设始发事件需要的全部安全功能：

（1）在安全系统内存在单一可探测故障，并同时存在可判别但不可探测的故障（不可探测的故障即不能通过定期试验、报警、异常指示来揭示的故障）；

（2）由上述单一故障引起的所有故障；

（3）导致需要安全系统执行安全功能的假设始发事件的所有故障和系统误动作，或由上述假设始发事件引起的所有故障和系统误动作。

5.2.3 可依据可靠性分析、概率评价、运行经验、工程验证或这些方法的结合，来判断安全级电力系统和设备是否满足单一故障准则要求。

5.2.4 不符合单一故障准则的情况应属于特例，且应在安全分析中充分说明其合理性。可接受的不符合单一故障准则的理由如下：

（1）假设始发事件非常罕见，并证明其发生的可能性足够小以至于可忽略；

（2）假设始发事件所导致的后果极不可能发生；

（3）由于维护、维修或定期试验，特定设备在有限时间内退出运行；

（4）只会在设计扩展工况出现的情形。

5.2.5 如果安全级电力系统和设备在试验或维护期间无法满足单一故障准则，应根据其重要性及其对堆芯损坏频率的潜在影响来确定其可退出运行的时间，且应符合核动力厂运行限值及条件。

5.2.6 当遵守单一故障准则不足以满足可靠性要求时，应提供附加的设计方案或对设计进行修改以确保系统满足可靠性要求。

5.3 备用电源（应急电源）

5.3.1 当能动型核动力厂丧失优先电源和主发电机时，备用电源可在任何预计运行事件或设计基准事故下为核动力厂提供必要的动力供应。下述对于备用电源的要求仅适用于能动型核动力厂的安全级应急电源。

5.3.2 对于不要求备用电源执行安全功能的核动力厂（如非能动核动力厂），为满足纵深防御的功能需求，应配置可靠的后

备电源作为安全级电力系统的补充电源，以降低安全级电力系统失电的风险。

5.3.3 每列安全级电力系统宜配置一套备用电源，应避免多台发电机并列运行。如果每列安全级电力系统采用多个电源，应证明该配置方案是安全可靠的。

5.3.4 在各种设计工况下，备用电源均应具备足够的容量和能力来启动对应序列的全部负载并保持连续供电，包括以下运行工况：

（1）负载处于惰转运行状态；

（2）发电机处于允许的电压和频率范围下限或上限运行时导致负载特性的改变；

（3）环境条件变化导致发动机降容运行。

5.3.5 在应急运行模式下，备用电源应在设计规定的电压和频率范围内运行。

5.3.6 备用电源应具备在设计基准要求的时间周期内持续运行且无需停机维护的能力，且应具备在 24 小时内以 10%的过载率持续运行 2 小时的能力。

5.3.7 当安全级母线失去优先电源和主发电机电源时，备用电源应能自动启动。即使安全级母线未失电，备用电源也可由应急信号触发而自动启动。

5.3.8 备用电源的实际启动和接入时间应与安全分析中明确的启动时间相匹配。

5.3.9 厂内燃油及其他消耗品（如润滑油）应足够支持备用电源运行至厂外电源恢复。

5.3.10 备用电源的运行不应依赖与其不同序列的动力和控制电源。

5.3.11 只有当优先电源和主发电机均不可用时，厂内备用电源才能投入。

5.3.12 只有满足本导则 4.2 节的相关要求时，安全级电力系统才能向非安全级负载供电。安全级电力系统与非安全级负载之间的隔离装置应作为安全级电力系统的一部分。

5.3.13 备用电源应能自动卸载所有非安全级负载，非安全级负载不宜自动加载。在备用电源的加卸载程序中，非安全级负载的加载取决于备用电源是否有足够容量来启动和运行。

5.3.14 当安全级电力系统母线由备用电源切回优先电源供电时，应采用手动操作方式。当某一列安全级母线切回优先电源供电后，应确认其对应的备用电源已恢复至正常备用工况，才能允许其他序列母线切回优先电源。禁止多列安全级母线同时从备用电源切回优先电源供电。

5.3.15 应明确核动力厂运行期间备用电源的定期试验方法。在一列备用电源试验期间，应确保其余列备用电源仍能够执行安全功能。试验程序不应破坏安全级电力系统的独立性，也不应引入产生共因故障的可能性。应考虑每一个跳闸功能和旁通功能的独立试验方法。

5.3.16 为保证多重性和独立性，安全级备用电源的支持系统（如通风系统、冷却水泵及润滑系统）应由本列电源供电。

5.3.17 备用电源的辅助及支持系统的容量应满足电厂安全

分析的总体要求。

5.4 安全级直流电源

5.4.1 每组蓄电池应至少设有一套充电器，为了提高系统运行的灵活性和可用性，可配置备用充电器。

5.4.2 每套充电器应具有足够的容量以满足以下要求：

（1）在正常运行中保持蓄电池处于充满状态；

（2）在可接受的时间内将蓄电池从完全放电状态恢复到充满状态，同时可满足最大的持续负荷和间断负荷组合的供电需求。

5.4.3 充电器应能够在不连接蓄电池的情况下直接为负荷供电，但不宜在这种模式下长期运行。充电器为负荷直接供电时的输出性能需满足负载运行要求。

5.4.4 充电器的交流侧和直流侧应设置开关元件。

5.4.5 在充电器不可用的情况下，每套蓄电池应能满足所有设计基准工况条件下的负载要求，并考虑设计裕量、温度效应和老化效应等因素。

5.4.6 蓄电池间应配置通风设施，以保持可燃气体浓度低于限值，并应设置氢气探测报警装置。如需配置机械通风，蓄电池室的通风系统应由与蓄电池相同序列的电源供电。

5.4.7 为证明蓄电池的可用性并检测其异常情况，蓄电池应进行定期试验和检查。

5.5 安全级交流不间断电源

5.5.1 安全级交流不间断电源系统应向需要不间断供电的安全重要负荷提供电源。

5.5.2 每列安全级交流不间断电源系统应由安全级直流电源

系统供电的逆变电源、对应的交流电源以及用于这两个电源之间自动切换的设备组成。

5.5.3 交流不间断电源系统的电气特性和供电连续性应满足负荷要求。

5.5.4 交流不间断电源系统的设计应满足负荷以及负荷间相互作用的特性和设计要求。例如，逆变器应确保本身以及负荷引起的谐波电压不会导致系统功能异常。

5.6 保护与监测

5.6.1 每列备用电源应当配置独立的保护和监测系统，并符合以下规定：

（1）在安全级母线上设置两级不同延时的低电压保护，第一级用来监测安全级母线是否失去厂外电源，第二级用来监测安全级母线电压的异常程度；

（2）当监测到优先电源出现不可接受的过电压时，应自动将其与安全级母线断开，过电压保护的整定值和延时设定应与设备的过电压能力相配合；

（3）应避免电动机起动或其他瞬态导致优先电源意外断开；

（4）应监测安全级母线三相电压和频率，信号送至主控室。

5.6.2 在备用电源的任何运行模式下，防止备用电源本体遭受破坏的保护均应投入跳闸，例如超速保护和发电机差动保护。

5.6.3 在备用电源应急运行期间，用于应对 5.6.2 所述故障之外的保护装置跳闸功能应旁路（或采用符合逻辑投入），但在备用电源正常运行和试验期间应保持可用。

5.6.4 当备用电源使用专用蓄电池时，应监视其异常及失效状态，使其与其他安全级蓄电池具有同等可用的状态。

5.6.5 备用电源的所有保护动作报警均应在主控室显示。

5.6.6 安全级交流电力系统的低电压和延时整定值应根据安全级用电负荷的需求电压来确定。

5.6.7 用于备用电源启动、接入、运行以及保护的控制系统应由同列的直流系统供电。

5.6.8 安全级直流电源系统和交流不间断电源系统应配置欠压报警。

5.6.9 不接地的直流电源系统应配置接地监测系统，并在系统对地阻抗值降低至可能发生故障之前发出警报。

5.6.10 应监测直流系统蓄电池熔丝或断路器的状态。

5.6.11 直流系统的充电器应具有防止反向电流的措施，具有限流功能或过载保护，以及具有输出超压保护。

5.6.12 蓄电池充电器应避免直流侧与交流侧的瞬态互相影响，尤其当充电器作为逆变器的电源时，充电器应具有相应的保护功能，以保证在交流电源侧故障和发电机甩负荷至孤岛运行期间保持直流电压运行在允许的范围内。

5.6.13 直流配电系统和交流不间断电源系统应满足保护配合要求。

6 替代交流电源

6.1 在全厂断电工况下，若核动力厂还需要交流电源驱动的负载才能将核动力厂带入可控状态，则应在核动力厂内或厂区附

近设置替代交流电源。替代交流电源应便于接入相应负载所在的母线。若设计中未设置替代交流电源，则应满足相关安全分析要求。

6.2 替代交流电源应具备足够的容量为相关系统运行提供必要的电力供应，并在规定时间内将核动力厂带入并维持在可控状态。

6.3 应确保替代交流电源能够应对全厂断电工况，包括确保反应堆热量导出、维持一回路完整性、维持反应堆次临界状态以及乏燃料余热导出，并为其他电源可靠恢复提供足够的时间窗口。

6.4 替代交流电源应能够在核动力厂安全分析和全厂断电分析中规定的时间内为相应负载供电。

6.5 替代交流电源应采用多样化设计，且不应受到厂内和厂外电源失电的影响。

6.6 在正常情况下，为某一机组配置的替代交流电源不应该与该机组的厂内电力系统相连。只有在安全级电力系统与其他电源断开连接后，才能由替代交流电源供电。

6.7 对维持替代交流电源处于热备用状态的支持系统，可由一台或多台机组供电，并确保其电源配置不会影响替代交流电源的可用性。

6.8 应尽量降低备用电源与替代交流电源共因失效的可能性。不应存在因恶劣天气、外部事件或单一故障引发的单一缺陷，进而导致某一机组的备用电源失效，并同时造成所有厂外电源及替代交流电源失效。

6.9 为应对全厂断电工况，除替代交流电源以外，还可考虑采用移动电源或其他场外临时电源用于恢复必需的电力供应，设计上应考虑其接入厂内电力系统的条件。

6.10 用于缓解堆芯融化事故后果所必需的设备应能够由任何可用的电源供电。

7 设计验证

7.1 应对核动力厂安全重要电力系统开展系统性评价，以确认设计方案满足设计基准中关于可靠性的要求，核动力厂电力系统的容量和能力应由分析确定并由试验验证。应进行如下论证且每项论证的过程应形成文件：

（1）论证电力系统能够完成设计基准中设定的安全功能；

（2）论证电力系统满足设计要求；

（3）论证安全级电力系统满足单一故障准则；

（4）论证电力系统可靠性满足设计要求；

（5）论证保护装置的动作经过充分配合；

（6）论证已充分实施应对全厂断电的措施；

（7）论证厂外电源回路的可靠性满足要求，并在电网规划变更后仍然满足为安全级负荷供电的可用性要求；

（8）论证每个厂外电源回路都有足够的容量及能力为缓解预计运行事件及设计基准事故后果的所有负荷连续供电。

7.2 对于安全重要系统的系统性评价，可综合采用确定性准则和可靠性定量分析的方法。

7.3 电气软件的验证与确认应遵循核动力厂仪表和控制系

统设计相关导则的要求。

7.4 应对电力系统设计及分析工作中使用的工具进行认证，且应基于试验数据或运行经验论证数学模型的有效性。

7.5 应采取适当的设计措施，来保证在下述试验实施过程中机组处于安全状态：

（1）预运行试验程序，用于证明系统在正常和应急工况下的可运行程度，证明系统满足设计要求，确认多重安全级电力系统之间互相独立；

（2）运行期间的试验程序，用于充分保障系统处于就绪状态并随时可按需投入运行；

（3）定期试验程序，用于证明系统的连续运行能力，并监测和识别系统或系统中设备的异常情况。

7.6 在系统投运前或在重大修改后，应确认安全级电力系统序列的独立性。通常采用如下验证：所有的厂内电力系统及其序列可以成功运行，且不会被其他序列电源的部分或全部功能失效所影响。

附录 A 电力系统的纵深防御

A.1 总述

A.1.1 核动力厂依赖电力系统实现各种安全功能，供电可靠性对于核动力厂的安全至关重要。不论其子系统的安全分级是否一样，电力系统都应作为一个整体来进行设计。

A.1.2 核动力厂电力系统对所有纵深防御层级都是必不可少的支持系统。在预计运行事件、设计基准事故和设计扩展工况下，可靠的电力供应对控制核动力厂预期运行偏差，以及对核动力厂保持供电、控制和监测是十分有必要的。

A.1.3 为保持可靠性和稳定性，不同的电力系统形成了不同层次的纵深防御体系，包括外部电网和厂内电力系统，包括安全级电力系统和非安全级电力系统。尽管安全级电力系统需要采用更加严格的标准并实施更多的设计验证，但厂内、厂外电力系统对实现一个稳定可靠的安全级电力系统都有着重要意义。

A.1.4 表 A-1 总结了电力系统对纵深防御的支持特征。

表 A-1. 为核动力厂纵深防御提供电力供应的支持

纵深防御	目　标	基本手段	应用于厂内电力系统[1]	本“安全导则”中的指南（对应章节）
1	防止异常运行和故障	保守设计、高质量的建造和运营	全面的设计基准，可靠的电网和电力系统	3.电力系统设计总原则 4.优先电源设计
2	异常运行控制及故障检测	控制系统、保护系统和其他监视功能	可靠的故障排除系统和保护配合，电源切换和孤岛运行	3.2.可靠性设计 4.优先电源设计
3	设计基准范围内的事故控制	专设安全设施和事故程序	可靠的安全电源系统，可靠的厂内备用电源	5.安全级电力系统设计
4	控制核动力厂	补充措施与事	可靠的替代交流	5.安全级电力系统

	的严重状态，包括防止事故发展和减轻设计扩展工况的后果	故管理	电源 直流及交流不间断电源	设计 6.替代交流电源
5	减轻重大放射性释放的放射性后果	场外应急响应	（本“安全导则”未涵盖）	

注 1：本处应用于厂内的电力系统仅为举例说明，并非在对应的目标下唯一可用的电力系统。

A.2 纵深防御的第一层次

A.2.1 设计准则

A.2.1.1 厂内电力系统的设计准则是实现可靠性和稳定性的基础。设计基准说明了电压和频率的持续运行范围、所有可能导致电压和频率瞬态、动态或持续变化的事件和危及电力系统可靠性的内外部危险。由于核动力厂本身就是一个产生电力的场所，因此其由于各种事件所引起的电压和频率与正常值的偏离，会不同于一般工业系统所引起的电压和频率的偏离。

A.2.1.2 不完整的设计基准将导致设备无法满足预期的功能，而且无法通过增加多重性或多样性得到弥补和纠正。

A.2.2 电网

A.2.2.1 对于核动力厂和安全级电力系统而言，电网是优先电源的组成部分。在功率运行期间，厂内电力供应通常来源于发电机，可以降低电网波动的影响。

A.2.2.2 电网应能提供稳定的厂外电源，且能够承受负荷的变化和没有超出电网电压和频率允许限值范围的预计运行事件。

A.2.3 厂内电力系统

A.2.3.1 厂内电力系统是互相连接的，因此在非安全级母线上发生的电气事件将很可能会影响安全级电力系统。对于电气负荷和其他设备而言，一个可靠的厂内电力系统故障率应足够低。

A.2.3.2 为实现厂内电力系统的稳定性和可靠性，需要对核动力厂的整体配置方案进行分析。

A.2.3.3 由于正常情况下安全级电力系统的多重序列连接到同一优先电源，则对于安全级电力系统不能完全排除其共因故障的可能性，因此采取一些预防性措施，例如实现电源的多样性是有必要的。

A.2.3.4 核动力厂的修改通常也会对电力系统产生影响，应评价负荷及其特性变化所带来的影响。

A.2.3.5 在处理运行的干扰和事件中，为照明和通信供电的电力系统十分重要，尽管他们通常不被归类于安全重要的系统。

A.3 纵深防御的第二层次

A.3.1 保护系统和保护配合

A.3.1.1 为了使电力系统发生故障时所带来的影响最小化，保护配合和故障切除系统应确保只会切除故障设备。

A.3.1.2 由于蓄电池充电器、逆变器和电动发电机通常都会在短路时贡献短路电流，因此要特别关注保护装置的配合以及可能会出现的故障电流。

A.3.1.3 保护配合需考虑核动力厂电力系统运行方式的变化。

A.3.2 电源切换能力

A.3.2.1 核动力厂通常采用至少两个在供电回路和位置上互相独立的厂外电源，以尽可能减少他们同时发生故障的可能性。

如果经安全分析论证满足要求，核动力厂（通常指具有非能动安全特征设计的核动力厂）也可采用一个厂外电源的设计方案。

A.3.2.2 厂外电源的切换通常是自动进行的，一般具备手动切换和自动切换两种可选择的方式。需关注母线切换之前、切换期间和切换之后对母线和电机的电压、相角和频率的影响。

A.3.3 孤岛运行的可能性

A.3.3.1 某些核动力厂具备孤岛运行的能力，即在甩负荷后反应堆不用停堆或者汽轮发电机不需要停机。

A.3.3.2 孤岛运行的切换之所以复杂，原因在于反应性的反馈和降功率时的控制。经验表明，如果能够承受初始的暂态效应，孤岛运行工况能够持续数小时，这为核动力厂的电源增加了多样性。

A.3.3.3 为实现孤岛运行成功，有必要在电网和核动力厂之间设置断路器，可使核动力厂从汽轮发电机或电网任一侧获得持续电源。

A.4 纵深防御的第三层次

A.4.1 厂内备用电源

A.4.1.1 核动力厂的安全级电力系统通常从主发电机、优先电源、厂内备用电源或者替代交流电源获得电源。

A.4.1.2 需定期对备用电源的可用性进行验证，对备用电源启动能力的试验应不会对其长期正常运行造成负面的影响。

A.4.1.3 对备用电源的启动能力和负载能力的验证通常被作为一个整体的试验和分析，以用于匹配设计基准事故

A.4.1.4 非安全级负荷的电力供应也可能来自于安全级电力系统。这些负荷在失去厂外电源以后不会全部立即自动启动，因为他们可能会影响安全负荷的可用性。只有在确保拥有足够的容量和能力来保证非安全负荷的启动和运转的时候，他们才可能会被启动。

A.4.1.5 当发生威胁电力系统的第一级和第二级纵深防御的外部灾害时，厂内的备用电源应能应对这类灾害事件。

A.4.2 安全级电力系统

A.4.2.1 由安全级电力系统供电的各类负荷对于核动力厂应对放射性物质泄漏的各种初始事件有着非常重要的作用。

A.4.2.2 源于优先电源的事件会导致在所有配电系统中发生共因故障，因此在设计、建造和运行环节中准备充分的应对措施是必要的。在丧失优先电源之后，如果备用电源分别只对一个供电序列供电，可以忽略由于电气事件所导致的共因故障。

A.4.2.3 共因故障发生的原因通常不考虑非能动电气设备上发生的电气事件。

A.4.2.4 直流电源系统对于安全级电力系统和其他厂内外电力系统的可靠性至关重要。优先电源和发电机的一个设计原则是源于厂外的干扰不应传导到直流电源系统和不间断交流电源系统，上述原则应作为设计基准的一部分，并且可以通过设计措施或保护装置来实现。

A.4.2.5 有必要了解用电负荷的机械特性，以确定不同运行模式下功率的消耗情况，这将有助于确定备用电源的容量和选择适当的保护配置。

A.5 纵深防御的第四层次

A.5.1 替代交流电源

A.5.1.1 应考虑全厂断电情况下核动力厂允许失去所有交流电源的持续时间，并应能在此时间内连接到一个替代交流电源。

A.5.1.2 有必要采取预防措施来保证替代交流电源在发生外部灾害时是可用的，并能在规定的时间内接入核动力厂。

A.5.1.3 替代交流电源应该尽可能独立于其他为安全级电力系统供电的电源。

附录 B 用于设计验证的电力系统分析

为证明核动力厂电力系统的设计裕量及可靠性，在设计阶段需开展必要的分析研究，这些分析可通过试验或运行经验进行检查和验证。本附录中提出了电力系统设计中一些关键的分析内容。

B.1 潮流分析

B.1.1 潮流分析是电力系统分析的重要部分，可以评价系统在正常运行状态和应急运行状态下的能力并建立边界条件。可用计算机软件实现潮流分析，仿真实际的电力系统稳态运行状况，并评价母线电压、功率因数、有功潮流、无功潮流及损耗。采用多种工况开展潮流分析有助于确保电力系统的设计满足性能标准。潮流分析通常用来评价如下内容：

（1）元件或回路加载情况；

（2）母线电压幅值和功率因数；

（3）有功潮流和无功潮流；

（4）电力系统损耗；

（5）变压器分接头设置；

（6）系统运行的边界条件；

（7）母线切换方案；

（8）回路配置优化；

（9）假设工况下的实际电压波动；

（10）指导设备技术规格书编制。

B.1.2 在潮流分析中，通常采用如下总体性设计准则：

（1）在所有考虑的运行工况下，所有母线的稳态压降在±5%额定电压范围内；

（2）在负荷加载工况下，暂态电压波动允许大于5%；

（3）在任何假设运行工况下，电气回路不能过载；

（4）在所有的运行工况下，无功潮流均在特定的限值之内。

B.1.3 在潮流分析中通常研究如下内容：

（1）最大及最小负载的极端运行工况，以检验厂内电源和厂外电源在正常运行工况及停堆工况下的适应性；

（2）偶然性工况。比如线路停运，厂外电源的变压器和发电机停运，同时厂内辅助系统（包括事故后用以缓解放射性后果的设备）处于最大或最小负载；

（3）核动力厂运行参数的优化。比如变压器分接头、发电机励磁特性、无功补偿装置及电缆选型；

（4）大型电动机启动。在额定电压直接启动时，大部分交流电动机的启动电流比正常满载电流大数倍，过大的启动电流会导致端电压的降落，并可能由于过低启动转矩导致电动机启动失败，导致低电压继电器的非必要动作或连接在系统中的其他投运电动机的停运。电动机启动分析有助于选择最佳的启动方式、适当的电动机设计及适当的系统设计，使电动机启动的影响降低至最小。

B.2 短路电流分析

短路电流计算提供了电力系统在故障状态下的电流和电压。这些信息可以用来：

（1）确定断路器在最大故障电流水平下的开断要求；

（2）校验继电保护系统设计的合理性、灵敏性和及时性。

短路电流计算需考虑所有在运电源的故障贡献，包括大型异步电动机。当厂内或厂外电源系统有重大变化或重大修正时，需重新进行短路电流计算，并且应周期性地开展评价。

B.3 电气保护配合分析

B.3.1 保护配合分析可确定故障发生后各时间段内流过电力系统的电流幅值，并且评价系统保护装置的选型及设置。目的是为电力变压器、开关柜、电动机控制中心、配电盘和其他电气设备提供必要的保护，并保证回路在过载工况或短路工况下有选择性地快速断开，从而将有必要隔离的设备范围最小化。

B.3.2 保护继电器是用来快速驱动用于隔离系统故障的设备，防止设备的损坏，并以对系统扰动最小的方式，保证电力系统不受影响部分的连续供电。保护继电器应能区分正常运行工况、异常运行工况和故障工况，并为它们提供特定的保护功能。继电保护配合计算需考虑继电器的运行特性、电气设备的正常运行及耐受特性，并为达到电力系统的高可靠性而设置最优的继电器定值。

B.3.3 针对不同的电气元件及运行状况，保护系统应提供相应的保护功能。

B.3.4 典型的保护分析包括：

（1）过载保护；

（2）过流保护；

（3）接地故障保护；

（4）最大负载电流下的保护配合；

（5）最小短路电流下的灵敏度校验；

（6）各类保护设备的特性配合；

（7）最大电动机启动电流及时间的配合；

（8）变压器励磁涌流配合；

（9）再加速电流的配合；

（10）主后备的配合；

（11）热稳定能力的配合；

（12）电动机安全堵转限值的配合。

B.3.5 设计过程中需要特别考虑接地故障保护，因故障电流的幅值决定于系统的接地方式，直接接地系统或低阻接地系统可能会有高水平的接地故障电流，这些高水平电流通常会要求快速的脱扣以将故障从系统中清除。高阻接地故障的检测较为困难，因为继电器需要测量幅值较小且伴有不平衡电流的接地故障电流，不平衡电流一般由线路相位及配置、负荷不平衡引起。

B.4 电压丧失及电压异常分析

为应对优先电源电压异常对安全母线的供电的影响，对安全重要的设备可设置两种低电压保护方案：

（1）如果电网电压突然大幅下降，且不能恢复到正常运行范围，可通过延时动作将厂内母线从电网中隔离，同时触发厂内备用电源的自动启动信号；

（2）安全重要设备的低电压保护应可适应系统持续低电压达数秒并随后恢复至正常运行范围的电压异常。电压异常工况通常发生在由电力不足导致的输电系统过载时，电力不足通常由丧

失发电机组、加载非预期负荷、输电元件丧失或系统故障导致。低电压保护方案对具体核动力厂需要额外的考虑，总体方法如下：

A) 通过潮流分析确定核动力厂和电网接口处的最小预期电压，并验证厂用电设备在正常运行、预计运行事件和事故工况下能够正常启动和运行；

B) 低电压保护的电压和延时定值由厂内各级配电系统中的安全重要负荷的运行需求确定，应基于下述情况选择延迟时间：

— 允许的延迟时间不超过在事故分析中假定的最大延迟时间；

— 延迟时间躲过短时电网扰动；

—各级配电系统中的电压异常的持续时间不会导致安全级电力系统或设备的失效。

B.5 暂态稳定分析

B.5.1 电力系统在经受严重的大扰动后的恢复能力对核动力厂的可靠及安全运行十分重要。影响电力系统暂态稳定的参数包括：

（1）同步电机的参数；

（2）主变压器的阻抗；

（3）汽轮发电机的转动惯量；

（4）输电线路的参数；

（5）断路器和继电器特性；

（6）系统地理接线；

（7）励磁系统、系统稳定器和发电机调速器特性；

（8）系统接地方式；

（9）自动重合闸、单极开关、甩负荷和系统惯量。

B.5.2 典型的暂态稳定分析内容包括：

（1）根据发电机稳态、暂态及次暂态参数建模；

（2）三相故障或线路接地故障的暂态仿真；

（3）电动机及负载的转矩、滑差、电流及加速曲线的建模；

（4）模拟发电机启动和电动机启动；

（5）断路器脱扣和闭合、隔离开关的打开和闭合及基于设定值的继电器动作的建模；

（6）在假定扰动后，发电机和电动机转速、电流、电压和功率曲线的绘制。

B.6 雷电防护系统和系统接地分析

B.6.1 雷电防护系统用来保护建构筑物不因雷击损坏，为了防止设备损坏和人员伤害，雷电流需通过低阻抗路径快速向大地释放。

B.6.2 外部雷电防护装置包括接闪器、引下线和接地装置，内部雷电防护装置包括等电位连接、与外部雷电防护装置的电气绝缘和浪涌保护器。