《核电厂设计安全规定》

本规定是中华人民共和国核电厂安全法规的第二部分

本规定自一九九一年七月二十七日起实施

本规定由国家核安全局负责解释

1 引言

1.1 目的

本规定提出了陆上固定式热中子反应堆核电厂的核安全原则，确定了保证核安全所必需的基本要求。这些要求的适用范围包括安全重要的构筑物、系统和部件以及有关规程和程序。规定中只强调设计中必须满足的要求，对于如何满足这些要求则不作具体规定。

附录 I 所列安全导则是对本规定的说明和补充。

本规定适用于核电厂设计、制造、建造、运行和监督管理。

1.2 范围

本规定阐述了构筑物、系统和部件为满足安全运行以及防止（或减轻）可能危及安全的事件后果所应遵守的设计方法和设计要求。可能危及安全的事件统称为假设始发事件。假设始发事件用于确定核电厂物项的设计基准。它们包含多种可能单独地或相互组合后影响安全的因素。这些因素有如下几种类型：

（1）与核电厂厂址及其环境有关联的因素；

（2）由人员行动引起的因素；

（3）源自核电厂本身运行的因素。

本规定不考虑下列事件：

（1）极不可能发生的事件（对严重事故的考虑见 3.5 条）；

（2）能导致核电厂厂址区域的全面破坏而又不能加以防范的人为事件和自然事件；

（3）绝无可能影响核电厂安全的工业事故；

本规定不考虑核电厂对环境的非放射性影响。第 5 章和第 9 章的某些要求只适用于水冷堆。

2 安全原理

2.1 安全目标

核能与任何一种对于人类和环境具有一定风险的工业活动一样，均须尽力降低风险。核能的风险与电离辐射（以下简称辐射）有关。因此核安全的最终安全目标为：

建立并保持对辐射危害的有效防御，保护厂区人员、公众和环境。

具体而言，辐射防护的目标为：

保证厂区人员和公众在运行状态下所受到的辐射照射低于规定限值并保持合理可行尽量低；保证减轻事故引起的照射。

与事故状态有关的目标为：

保证从总体上防止事故的发生，保证在出现核电厂设计中在考虑到的所有事故序列（即使是概率很低的序列）时，其放射性后果不大；通过预防和缓解措施保证发生严重后果的事故的可能性极低。

2.2 纵深防御

纵深防御概念是安全原理的重要组成部分。此概念必须贯彻于安全有关的全部活动，包括与组织、设计或人员行为有关的方面，以保证这些活动均置于重叠措施的防御之下，即使有一种防御失效，亦将得到补偿或纠正。

设计过程中必须贯彻纵深防御概念，从而提供多层次的保护。这方面的实例为：

（1）设置多种手段以保证每个基本安全功能（反应性控制、余热排出和放射性包容）的执行；

（2）除固有安全特性外，采用可靠的保护装置；

（3）通过安全系统的自动触发和运行人员的行动，加强对核电厂的控制；（4）提供设备和规程以支援事故预防措施、控制事故发展过程和限制事故后果。

作为一条基本要求，任何时候各防御层次都必须按照不同运行方式的规定一一备齐。在缺少一个防御层次而其他防御层次虽在的条件下，继续运行就没有足够的基础。

纵深防御概念在设计过程中的第一种应用如下：提供多层次的设备和规程，用以防止事故，或在未能防止事故时保证适当的保护。

（1）第一层次防御的目的是防止偏离正常运行。这一层次要求按照恰当的质量水平和工程实践正确并保守地设计、建造和运行核电厂。为达到此目的，对设计规范和材料的恰当选择以及部件制造和核电广施工的控制，均应十分注意。对于核电厂的检查、维护和试验规程，以及进行这些活动时良好的可达性、核电厂的运行条件和运行经验的利用等项，亦应予以关注。

（2）第二层防御的目的是检测和纠正偏离正常运行的情况，以防止预计运行事件升级为事故工况。这是由于尽管注意预防，核电厂在其寿期内仍然会发生假设始发事件。这一层次要求设置专用系统并制定运行规程以防止或尽量减小这些假设始发事件所造成的损坏。

（3）第三层次防御是基于以下假定：尽管极少可能，某些预计运行事件的升级仍有可能未被前一层次防御所制止，因此必须提供附加的设备和规程以控制由此引起的事故工况的后果。设置这一层次防御的另一主要目的是使核电厂在事故工况后达到稳定的、可接受的状态。

在第三层之后可借以进-步保护公众和厂区人员的措施为：核电厂用于减轻超设计基准事故后果的特定的补充设施、应急计划和准备。

纵深防御概念的第二种应用是核电厂设置多道实体屏障，防止放射性物质外逸。这些屏障通常包括燃料本身、燃料包壳、反应堆冷却剂系统压力边界和安全壳。设计必须保证每一屏障的有效性，并为之提供保护。

3 设计总准则

3.1 辐射防护①

必须提供措施，以保证 2.1 条所提出辐射防护目标的实现。

核电厂安全设计中辐射防护接受准则必须遵循以下原则：导致高辐射剂量或放射性物质大量释放的核电厂状态的发生概率要低，而发生概率较高的状态的辐射后果要小。

接受准则通常仅为与核电厂的正常运行、预计运行事件和事故相对应的为数有限的几组准则。接受准则必须由国家核安全部门认可。

3.2 安全功能②

把安全视作整个设计过程中的内在要素，对于达到充分安全至为重要。本规定中所提出的安全对策的目的是：使核电厂保持在正常运行状态中；保证发生假设始发事件后，电厂能立即作出正确的近期响应以及在事故工况后便于处理。

为保证安全，必须满足下列总的设计要求：

（1） 必须提供安全停堆手段，使在运行状态中和事故工况期间及事故工况后的反应堆安全停堆，并使之保持在安全停堆状态。

（2） 必须提供排除余热的手段，使停堆后（包括事故工况停堆后）从堆芯排出余热。

（3） 必须提供减少放射性物质释放的可能性的手段，并保证任何释放在运行状态期间低于规定限值，在事故工况期间低于可接受限值。

对安全功能进行考虑是系统地满足上述设计总要求的一个处理方法。安全功能包括厂内各系统在运行状态中和事故工况期间及事故工况后为保证电厂安全所必须执行的所有功能。

① 有关设计中辐射防护的进一步指导见安全导则 HAF0209。

② 有关安全功能及其应用的进一步指导见安全导则 HAF0201。

3.3 电厂安全特性

纵深防御概念的基本思想也反映在电厂的下列特性中。

核电厂设计的一个总体要求是电厂对假设始发事件的敏感性必须合理地低。电厂对任何假设始发事件的预计响应可用下列（1）-（3）中的一项特征表示。核电厂的设计和运行应能促使任何假设始发事件的后果按下述顺序排列，并在合理可行的条件下尽可能接近于（1）。

（1）依靠核电厂的固有特性，假设始发事件不产生与安全有关的重大影响或核电厂只产生趋向安全状态的变化。

（2）在发生假设始发事件后，依靠在此状态中连续运行的系统动作，以控制该假设始发事件，使核电厂趋于安全。

(3)在发生假设始发事件后，依靠对该事件作出响应而投入工作的系统动作使电厂趋于安全。

3.4 设计基准

设计基准必须规定核电厂在确定的辐射防护要求范围内适应规定的运行状态范围和事故工况的必备能力。设计基准包括正常运行技术规格、假设始发事件引起的状态、重要的假设以及在某些情况下特定的

分析方法。

3.4.1 正常运行

设计过程中必须针对电厂安全正常运行的要求，制定一组运行要求和限制，包括：

（1）过程变量和其他重要参数的限制；

（2）安全系统整定值；

（3）电厂维护、试验和检查的要求，以保证构筑物、系统和部件的功能与设计规定相符。

这些要求和限制是制定运行限值和条件的依据。

3.4.2 假设始发事件

核电厂设计中必须认识到纵深防御的各个层次都可能受到考验，因此设计中必须采取措施以保证安全功能的执行，并实现安全目标。上述考验来自假设始发事件。假设始发事件的选择系基于确定论法或概率论法，或两者的某种组合。不同类型的假设始发事件及其可能的组合见附件 A。应指出，独立事件同时发生的可能性通常不予考虑。

3.4.3 设计规范

应有国家核安全部门认可的工程设计规范，作为系统和部件设计的接受准则。

3.4.4 厂址特征 ①

在确定核电厂设计基准时，必须考虑到核电厂与环境之间的各种相互作用，包括人口、气象、水文、地质和地震等因素。还必须考虑到为获得电厂安全和保护公众可依托的厂外服务（如电力供应和消防设施）可能遇到的困难。

3.5 严重事故

正常运行、预计运行事件和事故工况的设计基准对于防止反应堆堆芯的严重损坏以及抑制放射性物质的释放，使之在运行状态下低于规定限值并在事故工况下低于可接受限值，必须提供高的可信度。

但是应该意识到某些低概率的事件序列有导致严重的堆芯损坏的可能。

从安全观点出发，还以在一定限度内计及严重事故为妥。对于严重事故的考虑可基于现实的分析，而毋需严格地运用确定设计基准时所采取的保守的过程方法。根据运行经验，结合安全分析和安全研究的结果，设计中应考虑的事项有：

（1）针对特定设计，确定能导致严重事故的重要事件序列；

（2）考虑电厂的已有能力，包括超越其预定功能和设计基准时利用某些系统的可能，以及利用某些暂设系统使电厂恢复到受控状态并减轻严重事故的后果；

（3）应对能降低这些事件出现的概率或能减轻这些事件后果的可能的设计修改作出评价。若通过适当努力能提高总的安全性，则应进行这种设计修改。

（4）在计及有代表性的和起主导作用的严重事故的条件下，制定事故处理规程。

① 进一步指导见 HAF0100（91）《核电厂厂址选择安全规定》及其安全导则。

3.6 核电厂质量

必须明确规定构筑物、系统和部件的全部安全功能。构筑物、系统和部件必须按其安全的重要

性进行分级。

为保证高度的功能可靠性，对于与质量有关的各个方面，诸如构筑物、系统和部件的设计，材料的选择、技术规格、建造、运行、维护和试验规程以及合格人员的配备，必须予以极大关注，使之适应所赋与的安全功能。不仅对于不同防御层次中的工艺和安全系统及其辅助设施有此要求，对于防止放射性物质外逸的各道实体屏障尤其如此。

凡属可行，设备必须按照适用的、经认可的标准设计，其设计必须是此前在相当使用条件下验证过的；设备的选择必须与安全所要求的电厂可靠性目标相一致。对于所采用的标准和规范，必须加以鉴别和评价，以确定其适用性、恰当性和权威性，并根据需要进行补充和修正，以保证设备的质量符合安全功能的要求。

选择设备时必须考虑到误动作和不安全的故障模式（例如要求脱扣时不脱扣）。系统或部件有发生故障的可能并需要在设计中针对此种故障作出适应性措施之处，则必须先选择具有可预见的故障模式并便于修理或更换的设备。①

3.7 在役试验、维护、检查和监测的措施

安全重要构筑物、系统和部件的设计必须符合下列要求：它们的可靠性达到足够高的水平；为保持其执行功能的能力，可在核电厂的寿期内进行标定、试验、维护、修理和检查或监测；完成这些活动时所达到的标准与所执行安全功能的重要性相当，且厂区人员不致于由此而受到过量的照射。

安全重要构筑物、系统和部件的设计不足以适应试验、检查或监测的需要时，必须采取适当的补充措施，以消除潜在的未发现的故障影响。

3.8 系统和部件的可靠性设计 ②

① 这方面的进一步指导见 HAF0400（91）《核电厂质量保证安全规定》及其有关导则。另见安全导则 HAF0302《核电厂在役检查》、HAF0307《核电厂维修》和 HAF0308《核电厂重要物项的监督》。

②关于系统可靠性和设计措施的进-步指导见安全导则HAF0203、HAF0204、HAF0205、HAF0206、HAF0207、HAF0213.

本条所列的几种措施可用于达到和保持与全部三个防御层次内所执行安全功能的重要性相当的可靠性。如有必要，可使用这些措施的组合。

表示不同防御层次的可靠性要求，不能采取通用的定量指标。但第一层次无疑应视作重点。这与营运单位为了生产电力保持核电厂高可用率的目标也是吻合的。

为保证安全功能的执行具有必需的可靠性，经国家核安全部门同意，对某些安全系统可制定最大不可用率的限值作为基准或用作接受准则。

3.8.1 多重性

为完成一项特定安全功能而采用多于最少套数的设备，即多重性，它是提高安全重要系统的可靠性并借以满足单一故障准则（见 3.8.2）的重要设计原则。在运用多重性原则的条件下，一套设备出现故障或失效是可承受的，不致于导致功能的丧失。例如，在某一特定功能可由任意两台泵完成之处，设置三台或四台泵。为满足多重性要求，可采用相同的或不同的部件。

3.8.2 单一故障准则

满足单一故障准则的设备组合，在其任何部位发生单一随机故障时，仍能保持所赋予的功能。源自单一故障的各种继发故障，均视作单一故障不可分割的组成部分。

对于构成核电厂设计的每个安全组，都必须运用单一故障准则。安全组是用以完成各项为抑制特定假设始发事件的后果使之不超过设计基准所规定限值所需要的动作的设备组合。

为检验核电厂是否符合单一故障准则的要求，必须对各有关安全设备组进行下述分析：假设单一故障及其全部继发故障依次出现在设备组合的各个单元上，并逐一进行分析，直至完成此组合内的全部故障分析为止，对各有关组合依次一一进行分析，直至完成所有组合和全部故障的分析为止。有关特定安全系统需要符合单一故障准则的叙述见后。单一故障准则在上述系统中的假设是此前已作了描述的过程中的一部分。单一故障分析中，不考虑同时发生一个以上的随机故障。

如上述分析的结果表明，每个安全组在计及假设始发事件的影响后均能完成各有的功能，则认为，设计达到了单一故障准则的要求。

单一故障分析中，对于设计、制造、在役检查和保养的质量达到极高水平的非能动部件的故障，可不予考虑。但在排除非能动部件发生故障的可能时，必须计及始发事件后需要部件发挥作用的全时程，并对基于此种假设的分析方法的正确性作出论证。

乱真动作必须视为故障的一种模式。

对于下列各种情况，毋需遵守单一故障准则：

（1）极为罕见的假设始发事件；

（2）假设始发事件极不可能的后果；

（3）某些设备因进行维护、修理或定期试验，在有限的时间内停止使用。

对某些安全系统可能需要提出多重性或多样性的附加要求。例如在相同部件用于几种安全功能或同时用于安全和非安全目的之处、有共因故障的可能之处以及定期试验的有效性受到限制之处，均可据以提出附加要求。

3.8.3 多样性

采用多样性原则能减少某些共因故障的可能，从而提高某些系统的可靠性。应考查这类潜在故障的原因，以确定在何种场合能有效地应用多样性原则。

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

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

3.8.4 独立性

为提高系统的可靠性可在设计中采用下列独立性原则：

（1）保持多重系统部件之间的独立性；

（2）保持系统中各部件与假设始发事件效应之间的独立性，例如，假设始发事件不得引起为减

轻该事件后果而设置的安全系统或安全功能的失效或丧失；

（3）保持不同安全等级的系统或部件之间适当的独立性；

（4）保持安全重要物项与非安全重要物项之间的独立性。

独立性可在系统设计中通过功能隔离或实体分隔实现。

（1） 功能隔离

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

（2） 部件的实体分隔和布置

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

这些原则包括：

空间分隔（距离、方位等）；

屏障分隔；

上述两种方法的组合。

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

核电厂内的某些场所，有可能成为不同安全重要性的各种设备或线路的自然汇合点，例如安全壳贯穿区、电动机控制中心、电缆走廊、设备间、控制室和核电厂的工艺控制电脑等。在这些场所，必须尽实际可能采取适当的措施以防止共因故障。

3.8.5 故障安全设计

在设计核电厂的安全重要系统和部件时，应尽可能贯彻故障安全原则，即系统或部件发生故障时，电厂应能在毋需任何触发动作的情况下进入安全状态。

3.8.6 辅助设施

为保持电厂安全状态所必需的辅助设施有供应电力、冷却水、压缩空气或其他气体的设施及润滑设施等。辅助设施用于支持构成安全重要系统部分的设备时，必须视作安全重要系统的一部分。它们的可靠性、多重性、多样性、独立性、用于隔离和功能实验的措施必须具有与所支持系统相对应的可靠性。

3.8.7 共因故障

若干装置或部件的功能可能由于出现单一特定事件或原因而失效。这种事件或原因可能是设计缺陷、制造缺陷、运行或维护差错、自然事件、人为事件、信号饱和、环境条件的变化或电厂内任何其他运行或故障所引起的意外的级联效应。必须尽实际可能在设计中采取适当措施尽量减少这种效应。

3.8.8 设备停役

核电厂及其安全系统的可靠性设计中，必须计及设备停役的影响，包括预计的维护、试验和修理工作对于各个安全系统的可靠性所产生的影响。如系统的可靠性在设备停役的条件下不能满足设计和运行所采用准则的要求，且临时停役的部件不能在规定时间内进行更换或重新投入时，核电厂必须停止运行或置于安全状态之下。核电厂开始运行前必须明确规定可用于各种情况下部件的更换或重新投入的时间和应采取的行动。

3.9 运行人员操作优化的设计①

从安全观点出发，厂区人员的工作场所和工作环境必须按人机工效学原则进行设计。

对人的因素和人机关系的全面考虑应始于设计的早期阶段，并贯彻于设计全过程。

控制室内必须以协调的方式向操纵员提供反映本规定 3.2 条中各种安全功能所必需的全部设备和系统现状的各种参数的清晰的显示。在辅助控制点内也必须提供类似设施（见 6.3 条）。

若将操纵员视为承担双重任务，即设备操作和系统管理（包括事故处理）的人员，则有助于确立信息显示和控制的设计原则。

为进行系统管理，操纵员需要借以作出下述判断的信息：

（1）在任何状态下（即正常运行、预计运行事件或事故工况），迅速评估电厂的概况，并确认预定的自动安全动作正在进行；

①进一步指导见安全导则 HAF0203、HAF0208 和 HAF0303。

（2）决定应采取的恰当行动。

为进行设备操作，操纵员需要各系统和设备有关参数的信息。

设计必须利于操纵员在有限的时间内、预计的周围环境中和有心理压力（的状态）下能采取成功的行动。应尽量减少操纵员在短期内进行干预的必要性。设计时应考虑这种干预可予接受的前提是：设计者能够证明操纵员有足够的时间作出决定并采取行动，操纵员据以决定采取行动的必要信息系以简单和明确的方式呈现，在该事件发生后控制室内或辅助控制点内及其通道中的环境是可接受的。

3.10 余热向最终热阱的输送①

必须设置传热系统，向最终热阱输送来自安全重要构筑物、系统和部件的余热。这些系统在正常运行、预计运行事件和事故工况下都必须具有极高的可靠性。用于输送热量的各系统，包括传递热量、提供动力以及向余热输送系统供应流体的设计都必须与它们的整个余热输送系统中所分担的功能相适应。

为实现系统的可靠性，必须恰当地选择经考验的部件，并采用多重性、多样性、实体分隔、相互连接以及隔离等。

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

3.11 防火和防爆②

设计和布置安全重要构筑物、系统和部件时，除满足其他安全要求外，还必须尽量降低外部和内部事件引起火灾和爆炸的可能性及其后果。作为最低要求，必须保持停堆、排出余热和包容放射性物质的能力。为实现这些要求，必须采取多重部件、多样系统、实体分隔适当组合和故障安全设计。

①进一步指导见安全导则 HAF0206。

②进一步指导见安全导则 HAF0202。

在整个核电厂中，尤其在诸如安全壳和控制室等场所中，凡属可行，必须采用不可燃的或阻燃的和耐热的材料。

必须设置足够容量和能力的火警检测和灭火系统。在必要的场合，这些系统必须能自动触发。灭火系统的设计和布置必须保证在其出现破裂、误动作或意外操作时，对安全重要构筑物、系统和部件

的能力不致于产生显著的影响。

3.12 设备故障的影响①

安全重要构筑物、系统和部件的设计必须能经受运行状态和事故工况的影响并适应这两种状态的环境条件（对于严重事故，尽实际可能予以考虑）。为防止能加重初始事件对安全所造成的后果的次级故障，这些构筑物、系统和部件必须采取适当的布置方式，或为之采取保护措施，以防止设备损坏时可能出现的飞射物、管道甩动、流体喷射和淹没等动力作用的破坏。如果这些条件不能满足，必须在设计中采取其他合适的措施。

安全重要的流体系统与工作压力较高的另一流体系统相连接时，必须按较高的压力设计，或设置符合单一故障准则的过压保护。

3.13 多堆共用的构筑物、系统和部件

两个或两个以上的动力堆，一般不应共用安全重要构筑物、系统和部件。共用的方式如予采用，必须证明：此种方式能满足每一座堆的全部安全要求；一座堆发生事故时，其它各堆能有秩序地停堆、冷却并排出余热。

3.14 含有可裂变或放射性物质的系统②

必须保证核电厂内可能含有可裂变或放射性物质的所有系统在运行状态和事故工况下均有足够的安全性。

3.15 撤离路线和通讯手段

核电厂必须设置有简捷、以醒目而持久的标志识别的安全撤离路线，并配备为安全使用这些路线所必需的可靠的应急照明和其他辅助设施。撤离路线必须符合工业安全、辐射分区、防火和电广保卫方面的要求。

为使厂区人员即使在事故状态下也能得到警告指令，必须设置适当的报警系统和通讯手段。

安全必须的核电厂厂区内部以及对外的通讯联系，必须保持昼夜畅通。进行通讯设计和选择多样性措施时，必须计及这一要求。

①进一步指导见安全导则 HAF0204。

②进一步指导见安全导则 HAF0204

3.16 核电厂出入口控制

为严密控制出入口，必须以适当的构筑物的布置方式，使核电厂与其周围相隔离。进行厂房设计和厂区布置时，尤其须注意此点，并为保卫人员或监测设备作出安排，以防未经批准的人员和物品进入核电厂。

3.17 退役

在设计阶段对便于核电厂退役的措施必须给以关注，还必须为厂区人员和公众在退役期间所受

到的辐射照射保持于合理可行尽量低的水平，以及充分有效地保护环境防止放射性污染作出努力。

4 反应堆堆芯

4.1 反应堆设计

为保证在所有运行状态下不超出设计规定的可接受限值，反应堆堆芯和有关冷却剂系统、控制和保护系统的设计必须留有适当的裕量。

组成反应堆堆芯的部件和反应堆压力容器内靠近堆芯的其他部件的设计和装配，必须符合下述要求：在运行状态和事故工况中所预计到的静、动荷载的作用下，可保持必要的结构稳定性，以保证安全停堆和堆芯冷却。

4.2 燃料元件

燃料元件的设计必须适应各种劣化过程后仍能满意地承受所预计的堆内辐照的要求。

设计燃料元件时必须考虑下列劣化因素：冷却剂外压、燃料内裂变产物所造成的附加内压、燃料和燃料组件中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、包括流体所引起的，振动和机械振动在内的动载荷以及变形或化学效应所引起的传热性能的变化等。设计必须为数据、计算和制造中的不确定因素留有裕量。

燃料元件在正常运行中，必须保持于设计规定限值之内（包括裂变产物的容许泄漏值）；预计运行事件中的各种瞬态影响不得造成元件显著的进一步劣化，裂变产物的泄漏量必须保持于现实可行的最低水平，燃料组件的设计应计及便于检查其结构和零件的要求；在事故工况中，燃料元件必须能保持原位，其变形不得发展到有碍于堆芯在事故后保持足够有效冷却的程度，并且不得超过燃料元件在事故工况下的规定限值。

①进一步的指导见安全导则 HAF0214。

4.3 反应堆堆芯控制

堆芯的中子通量的水平和分布，各种状态下，包括停堆后，换料期间和换料后的状态、以及预计运行事件和事故工况引起的状态在内，必须符合 4.2 条的规定。用于检测上述通量分布的手段必须总能保证堆芯内不存在任何未能检测到的违反 4.2 条规定的部位。堆芯设计应尽量减少依赖控制系统使通量分布在各种运行状态下保持在规定限值内。

4.4 反应堆停堆

必须备有在运行状态和事故工况下安全停堆的手段。必须保证，即使在堆芯具有最大后备反应性的情况下，仍能保持停堆状态。停堆手段的有效性、动作速度和停堆深度必须足以保证反应堆不超出规定的限值。

停堆手段必须由两个不同的系统组成。

两个系统中，至少有一个系统能在单一故障情况下独立行使使反应堆从运行工况和事故工况迅

速进入有足够深度的次临界的功能。

即使在堆芯具有最大后备反应性情况下，两个系统中至少有一个系统能独立使反应堆从正常运行工况进入次临界，并以足够的深度和高的可靠度保持次临界状态。

判断停堆手段是否足够时，必须高度重视发生在核电厂任何部位的、可能导致一部分停堆手段失去作用的故障。

停堆手段必须足以防止反应堆失控地转向临界。为满足这一要求，必须考虑到停堆期间能增加反应性的各种预定操作（诸如维护和换料操作时移动中子吸收体）及停堆手段中的单一故障。

必须通过检测和试验保证停堆手段处于所要求的状态。

如能在全部正常功率运行期间保持停堆能力，则部分停堆手段可用于反应性控制和通量整形。

5 反应堆冷却剂系统①

5.1 反应堆冷却剂系统的设计

反应堆冷却剂系统及其有关的辅助系统、控制和保护系统必须具有足够的裕量，以保证冷却剂的压力边界在任何运行状态不超过设计条件。为达到此目的所设置卸压装置的动作，即使在事故工况下，也不得导致核电厂放射性物质的向外释放超过可接受的程度。

包容反应堆冷却剂的部件，如反应堆压力容器或压力管、管道和接头、阀门、配件、循环泵和热交换器以及用于固定这些部件的器件，必须能在所有运行状态和事故工况下承受预计的静、动载荷。

反应堆冷却剂压力边界必须具有能保证任何微裂纹缓慢扩展（如微裂纹可检测性、先漏后破）的特性。必须避免属于反应堆冷却剂压力边界的部件可能呈现脆性的设计和工况。所设计和制造的反应堆压力容器、压力管必须在材料选择、设计标准、可检查性和加工方面均具有最高质量。

设计中必须考虑到压力边界材料在运行、维护、试验和事故工况下的所有条件，并对使用中可能出现劣化（诸如由于侵蚀、蠕变、疲劳、化学环境、辐射环境和老化）以及在确定部件初始状态和劣化速率时的任何不确定因素，留有适当的裕量。

必须尽量减少反应堆冷却剂压力边界范围内的部件，诸如泵的叶轮和阀门零件在各种运行状态和事故工况下发生故障的可能性以及此种故障对一回路系统内其他安全重要物项造成的损伤，并对使用中可能发生的劣化留有适当的裕量。

①本章的某些要求仅适用于水冷反应堆，进一步的指导见安全导则 HAF0213。

5.2-回路压力边界的在役检查

一回路压力边界内部件的设计、制造和布置，必须便于在核电厂整个寿期内对边界定期进行充分检查和试验。应采取措施，贯彻材料监督大纲，借以确定反应堆压力容器和其他重要部件的结构材料的辐照效应和老化效应。

一回路压力边界的各部件必须具有与其安全重要性相对应的直接或间接的可检查性，以验明不存在不可接受的缺陷或劣化。

此外，必须设置指示器以监测一回路压力边界完整性（如泄漏检测）。设置此种监测手段，对

于安全所必需的在役检查的选择可能产生影响。

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

5.3 反应堆冷却剂装置

必须采取措施保证冷却剂的装载量和压力在任何运行状态下，在计及容积变化和泄漏后保持在设计规定的限值之内。为满足这一要求，执行上述功能的系统必须具有足够的容量（流量或储量）。这些系统可由用于发电过程的部件或专门为此而设置的部件组成。

5.4 反应堆冷却剂净化

必须采取措施，清除反应堆冷却剂中的放射性物质，包括从燃料泄漏的裂变产物。相应系统的能力必须基于设计所规定的燃料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合理的低水平和释放量低于规定限值的条件下运行。

5.5 堆芯余热的排出

必须为排出堆芯的余热提供手段。它们的安全功能是在不超过规定的燃料设计限值和冷却剂压力边界设计条件的前提下，以一定速度从堆芯排出裂变产物的衰变热和其他余热。

为了在单一故障的前提下足以可靠地实现上述要求，余热排出系统的设计必须具备适当的多重性、多样性以及诸如泄漏检测、适当的相互连接和隔离能力等特征。

5.6 应急堆芯冷却

为限制冷却剂丧失事故时裂变产物的外逸，必须设置应急堆芯冷却系统。此系统必须具有下述冷却效能：

（1）包壳温度不超过事故工况的容许设计值；

（2）可能出现的化学反应限制在容许水平内；

（3）燃料和堆内构件的变形不致于显著降低应急堆芯冷却手段的有效性；

（4）堆芯冷却保持足够长的时间。

为了在单一故障的前提下也足以可靠地实现上述要求，应急堆芯冷却系统的设计必须具备适当的多重性、多样性及诸如泄漏检测、适当的相互连接和隔离能力等的设计特征。

5.7 应急堆芯冷却系统的检查和试验

应急堆芯冷却系统及其重要部件必须具备进行定期检查和定期试验的条件，以保持下述性能：

（1）系统中各部件的结构和密封的完整性；

（2）正常运行期内系统中各能动部件可达到的最佳可运行性和工作性能；

（3）作为一个整体，系统按现实可能与设计基准条件相接近的可运行性，例如为系统投入运行所需全部操作顺序的执行，包括保护系统中有关部分的操作、正常和应急动力源之间的切换，以及有关

安全系统辅助设施的操作等。

6 信息和控制①

6.1 总的要求

必须设置能在正常运行、预计运行事件和事故工况下对变量和系统进行全程监测的仪表，以获取核电厂现状的充分信息。必须设置能测量所有影响裂变过程、反应堆堆芯完整性、反应堆冷却剂系统和安全壳完整性的主要变量的仪表以及借以获取核电厂的安全可靠运行所需的任何信息的仪表。对安全重要的导出参数，如冷却水的过冷度，必须配置足够的自动记录装置。

必须设置适当的控制手段将上述变量保持在规定的运行范围以内。控制系统的设计应采取适当的可达到高度可靠性的手段。

必须设置检测仪表和记录装置，用以获取为跟踪事故工况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自设计部位外逸的数量和位置。应视实际可能使检测仪表中有一定数量的仪表提供在严重事故期间反映电厂现状和据以作出决策的信息。

①进一步的指导见安全导则 HAF0208。

6.2 控制室①

必须设置主控制室，借以进行下述活动：在各种运行状态下安全地运行核电厂；出现事故工况和控制室设计中所采用的设计基准事件后，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。 必须采取适当措施保护控制室内的人员，防止事故工况下形成的过量照射或有毒气体之类险情的危害，以保持其采取必要行动的能力。

控制室内仪表的布置和信息显示的方式必须便于运行人员正确掌握核电厂现状和性能的全貌。

必须设置光示装置，并在相宜之处设置音响装置，以效果良好的方式指示偏离正常和可能危及安全的运行工况和过程。

6.3 辅助控制点②

必须在一个独立于主控室的专用控制点（二者之间采取电气和实体分隔）配置足够的检测仪表和控制设备，借以在主控室丧失执行基本安全功能时，完成下述任务：使反应堆进入并保持于停堆状态，排出余热并监测核电厂的主要变量。

6.4 应急控制中心

应设置一个与核电厂控制室相分离的应急控制中心，作为发生应急情况时集合应急工作人员的场所。应急控制中心内应提供电厂主要参数和核电厂内及其外围放射性状况的信息。应急控制中心应备有通往核电厂控制室及其他重要地点和厂外应急机构的通讯手段。应尽实际可能，采取适当措施，借以在相当长的时间内有效地保护应急控制中心内的人员，从而防止严重事故对他们的危害。

①见 3.9 条。

②见 3.9 条。

③进一步的指导见安全导则 HAF0203。

7 保护系统①

7.1 保护系统的功能

保护系统必须具有下述功能：

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

（2）检测到事故工况并触发为减轻其后果所需的系统动作；

（3） 抑制控制系统自身的不安全动作。

7.2 保护系统的可靠性和可试验性

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

（1）单一故障不致于导致保护功能的丧失；

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

必须保证正常运行、预计运行事件和事故工况对多通道的影响不致于导致保护系统功能的丧失，或者必须根据其他基准证明该保护系统是可以接受的。必须在实际可行的范围内采用各种设计技术，如可试验性（必要时包括自检能力）、故障安全性能、功能的多样性、部件设计或工作原理的多样性等以防止保护功能的丧失。

除非能通过其他方法获取必要的可靠性，否则保护系统必须具有可在反应堆运行时进行定期功能试验的条件，包括各通道分别进行试验的可能性，以查明可能发生的故障和多重性丧失的缺陷。

设计中必须采取措施尽量减少由于运行人员的行动引起保护系统失效的可能性。

7.3 保护系统和控制系统的分隔

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

8 应急动力供应①

安全重要的各种系统和部件，在发生某些假设始发事件后，需要应急动力。应急动力的供应必

须足以适应任何假设始发事件与外电源丧失相耦合的要求。所需应急动力的功率因假设始发事件的性质而异。确定各种安全功能所需应急动力的手段时，包括其数量、可用率、持续时间、容量和不间断性等，需要计及所执行的安全功能的性质。

可供选用的应急动力供应措施有许多种，如水轮机、汽轮机、燃气轮机、柴油机和蓄电池等。动力的供应可采取直接驱动设备或通过应急电力系统的方式。

所选用应急动力源设备组合的可靠性和方式，必须与作为其供应对象的安全系统对安全的全部要求相一致，并在发生单一故障情况下满足功能要求。应急动力源必须具有进行功能能力试验的条件。

9 安全壳系统②

9.1 目的

未能证明可使用其他方法限制放射性物质的释放量时，必须设置安全壳系统以抑制事故工况下放射性物质往环境释放，使之保持在可接受限值内。安全壳系统可由密闭的厂房或边界，压力抑制（抑压）子系统（适用于沸水堆）和净化系统组成。安全壳系统可按设计要求采取不同的工程处理方案。

安全壳系统的设计基准中必须考虑到已确定的各种假设始发事件。此外还应考虑用于减轻严重事故后果的设施及严重事故情况下用于保持安全壳完整性的措施。

①进一步的指导见安全导则 HAF0207。

②本章的某些要求仅适用于水冷反应堆，进一步的指导见安全导则 HAF0212。

9.2 安全壳结构的强度

安全壳结构（包括通道闸门、贯穿件和隔离阀）必须根据事故工况下所产生的内压（高于或低于大气压）、温度以及飞射物和反作用力等动态效应进行计算，并留有足够的裕量。设计中还必须考虑到其他潜在的能量来源，如化学和辐射分解反应的影响。安全壳结构强度计算中还必须计及自然事件和人为事件的作用。

9.3 安全壳的泄漏

安全壳系统必须按事故工况期间的泄漏率不超过规定的最大值的要求进行设计。承压的第一级安全壳可部分或全部置于第二级包容壳内，以收集和控制第一级安全壳在事故工况期间的泄漏释放或储存其泄漏物。

安全壳构筑物以及其他与系统密封性有关的设备和部件的设计和施工，必须适应贯穿件全部安装完毕后的设计压力下进行泄漏率测试的要求。安全壳系统还必须具备在堆的寿期内定期在设计压力或较低压力下重新测定泄漏率的条件，借以作出安全壳设计压力下泄漏率的估计。

9.4 安全壳压力试验

安全壳构筑物的设计和建造必须适应核电厂运行前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。

9.5 安全壳贯穿件

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

带有弹性密封或波纹管状胀缩节的贯穿件，必须具有进行与安全壳整体泄漏率测定无关的检漏试验的可能性。

9.6 安全壳隔离

为在事故工况下保持安全壳的密闭性，防止放射性物质向环境的释放超过可接受的限值，贯穿安全壳且属于反应堆冷却剂压力边界的组成部分或直接与安全壳空间相连的管线在事故工况下必须能可靠地自动封闭。为达到此目的，在这些管线上一般应串联设置两个合适的安全壳隔离阀。两个隔离阀通常分别装设在安全壳的内侧和外侧。每个阀必须能可靠地独立动作。隔离阀必须尽实际可能靠近安全壳。安全壳的隔离必须满足单一故障准则。

应用上述准则有损于贯穿安全壳系统的可靠性时，可采用其他的隔离方式。

贯穿安全壳、但既非反应堆冷却剂压力边界的组成部分，又不直接与安全壳空间相通的管线，最低限度必须设置一个隔离阀。隔离阀必须位于安全壳外侧，并尽可能靠近安全壳。

9.7 安全壳构筑物的气密闸门

人员进入安全壳必须通过双道气密闸门。两道闸门应相互联锁，以保证反应堆运行和事故工况期间至少有一道闸门处于密闭状态。

上述的要求也适用于设备的气密闸门。

9.8 安全壳内部结构

安全壳内的隔间之间必须开口，以保持气流畅通。开口的截面必须足以保证事故工况下压力平衡过程中的压差不损坏承压结构或其他对限制事故工况影响有重要作用的系统。

9.9 安全壳的排热

反应堆安全壳必须具有排出热量的能力，安全壳排热系统的安全功能是在发生高能流体的任何释放事故后，降低壳内的压力和温度，使之保持在可接受的低水平。为安全壳设置的排热系统，必须按单一故障准则的要求具有足够的可靠性、多样性和多重性。

9.10 安全壳内气体的净化

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

（1）降低事故工况期间可能释放到环境的裂变产物的数量；

（2）控制事故工况期间安全壳内气体中的氢或氧和其他物质的浓度，以防止可能危及安全壳完整性的爆炸或爆燃。

安全壳内气体净化系统的部件和设施，必须按单一故障准则的要求具有足够的可靠性、多样性

和多重性。

9.11 覆盖层和涂层

为了保证安全壳系统内构筑物和部件的覆盖层和涂层的安全功能，并尽量降低其他安全功能在其劣化时所受到的影响，对覆盖层和涂层的材料必须审慎地进行选择，对其施工的方法必须作出专门规定。

10 辐射防护①

10.1 原则

辐射防护的目的在于防止任何可避免的照射，并降低一切不可避免的照射，使之保持在合理可行尽量低的水平。为实现这一目标的设计中必须采用下述办法：

（1）含有放射性物质的构筑物、系统和部件采用适当的布置方式，并设置屏蔽；

（2）核电厂和设备设计中贯彻减少辐射区内人员活动和厂区人员遭受污染的可能性的要求；

（3）放射性废物在厂内的处置或发往厂外的过程中，采用适当的方式和条件处理放射性物质；

（4）采取措施，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。

必须充分考虑到人员停留区域内辐射水平以及放射性废物的产生随时间递增的因素。

①进一步指导见安全导则 HAF0209。

10.2 辐射防护的设计

核电厂的设计中必须贯彻厂内外的辐射照射在运行状态下限制于规定限值和事故工况下限制于可接受限值以内的要求。设计中还必须贯彻合理可行尽量低的原则。

核电厂的设计和布置中必须采取合适的措施，以尽量减少来自各种放射源的照射和污染；这类措施必须包括在维护和检查期间降低辐射照射、屏蔽直接照射、采用技术规格适当的材料降低腐蚀产物的活度、监测手段、核电厂出入口的控制、按辐射和污染程度分区及合适的去污设施等方面的系统和部件的恰当设计。

屏蔽设计必须符合操作区的辐射水平不超过规定限值，并有利于在维护中降低维护人员所受的辐射照射。屏蔽设计中还必须贯彻合理可行尽量低的原则。

核电厂的布置必须符合下述要求：辐射区和污染区的出入要有控制措施，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。核电厂的布置要为高效率的运行、检查、维护和部件的更换创造条件，以尽量减少辐射照射。

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

10.3 辐射监测设备

必须配置用于在运行状态和事故工况中（并视实际可能在严重事故期间）进行充分辐射防护监

督的设备。其具体要求如下：

（1）在运行人员常驻之处以及在正常运行或预计运行事件中，由于辐射水平的变化需在一定时间内限制进入的场所，设置固定式剂量率仪表对当地的辐射剂量率进行监测；此外，必须在适当的地点安装固定式剂量率仪表，用以指示事故工况和严重事故下总的辐射水平；这些仪表必须向控制室或有关控制点提供足够的信息，以便运行人员及时采取必要的纠正措施；（2）在人员常驻之处及气载放射性水平可能高至要求防护措施的场所，设置测量空气中放射性物质活度的监测系统；测得高浓度核素时，这些系统必须向控制室或适当的控制点发出指示；

（3）在运行状态或事故工况下，为测定流体处理系统中和取自核电厂系统或空间的气体或液体样品中所选定的放射性核素浓度设置固定式设备或实验室装置；

（4）设置监测排出流向环境排放前或排放过程的固定式设备；

（5）设置用于测量放射性表面污染的仪器；

（6）设置用于测量人员所受剂量和污染的装置。

除了在核电厂内进行监测外，还必须为确定核电厂对邻近地区可能产生的任何放射影响作出安排。

10.4 放射性废物的处理

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

必须设置适当的系统，以处理放射性固态废物或浓缩废物。厂区内必须具有在一定期限内贮存废物的条件。向厂外运输固态废物，必须遵照有关当局的规定。

10.5 液态放射性物质向环境释放的控制

核电厂必须备有适当手段，以控制液态放射性物质向环境的释放，并控制其排放量使之保持在规定限值以下。释放的控制必须符合合理可行尽量低的原则。

10.6 气载放射性物质的控制

必须设置具有适当过滤能力的通风系统，借以达到下述目的：

（1）防止放射性物质在核电厂内不可接受的扩散；

（2）降低特定区域内气载放射性物质的浓度，使之符合进入该区域的规定要求；

（3）在正常运行和预计运行事件期间，防止核电厂内空气的放射性水平超过规定限值，并符合合理可行尽量低的原则；

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

（5）控制气载放射性物质向环境的释放，使之保持在规定限值以下，并符合合理可行尽量低的原则。

过滤系统必须足够可靠，并在预计的常遇条件下能得到必需的滞留因子。过滤系统必须具有测试其效果的条件。

11 燃料装卸和贮存系统①

① 进一步指导见安全导则 HAF0210。

11.1 未辐照燃料的装卸和贮存

未辐照燃料装卸和贮存系统的设计必须符合下述要求：

（1）采用物理手段和工艺（以安全的几何构型为宜），以防止最佳慢化条件下达到临界；

（2）对安全重要部件可进行适当的定期检查和试验；

（3）尽量防止燃料丢失或损坏的可能性。

11.2 已辐照燃料的装卸和贮存

已辐照燃料装卸和贮存系统的设计必须符合下述要求：

（1）采用物理手段或工艺（以安全的几何构型为宜），以防止最佳慢化条件下达到临界；

（2）在运行状态和事故工况下都能充分排出热量；

（3）对安全重要部件可进行适当的定期检查和试验；

（4）防止已辐照燃料丢失；

（5）防止乏燃料在运输过程中跌落；

（6）防止装卸时在燃料元件或燃料组件上产生不可接受的应力；

（7）防止乏燃料运输容器或起重设备等重物由于疏忽而跌落在燃料组件上；

（8）能贮存可疑或已损坏燃料元件或燃料组件；

（9）具有正确的辐射防护措施；

（10）为采用燃料贮存水池系统的反应堆提供下列措施：

（i）控制已辐照燃料在装卸和贮存池中的水质和放射性活度；

（ii）监测和控制燃料储存水池的水位及检测水池泄漏。

12 设计的确认①

①进一步指导见安全导则 HAF0211.

12.1 安全分析

核电厂设计中必须进行安全分析，从而通过迭代过程制定和确认安全重要物项的设计基准，并保证整个核电厂的设计符合国家核安全部门为核电厂各种工况所制定的辐射剂量和放射性物质释放的规定限值和可接受限值。

核电厂安全分析的范围包括：

（1）运行限值和条件满足核电厂正常运行要求的验证；

（2）与电厂设计和核电厂位置相对应的假设始发事件特征的描述；

（3）源自假设始发事件的事件序列的分析和评价；

（4）分析结果与放射性接受准则和设计限值的比较；

（5）设计基准的制定与确认；

（6）预计运行事件和事故工况可通过自动安全系统的响应，并结合规定的运行人员的行动，进

行处理的验证。

必须验证分析方法的适用性，核电厂设计的安全分析必须根据电厂的重大变化和运行经验及时进行修正。

除了按上述过程制定设计基准之外，还应考虑严重事故的概率和后果，以达到下述目的：

（1）确认假设始发事件后果的突然升级不致于立即引发设计基准事故；

（2）确定可降低严重事故概率或减轻严重事故后果的设施；

（3）提供恰当的应急规程。

必要时应作概率安全评价。

12.2 设备的合格鉴定

设备合格鉴定的程序必须确定设备在整个寿期内，能满足处于需要作用时的环境条件（如振动、温度、压力、喷射流冲击、辐射、湿度）下执行安全功能的要求。上述环境条件必须包括预计到的正常运行、预计运行事件和事故工况期间的变化。在合格鉴定程序中必须考虑到设备预定寿期内各种因素的效应（如老化）。设备经受到外部自然事件的影响并需要在外部自然事件期间或事件发生后执行安全功能之处，合格鉴定程序中必须列入有关自然现象对设备影响的条件。

此外，在合格鉴定程序中必须列入与可合理预计的以及因特定运行工况引起的（如安全壳泄漏率定期试验期间的）异常环境条件有关的要求。预期需要在严重事故期间运行的设备（如某些仪表）应在可能范围内进行相应的合格鉴定。

12.3 质量保证①

必须制定并实施用于设计过程各个阶段的质量保证大纲，此大纲必须遵循 HAF0400（91）《核电厂质量保证安全规定》的要求。

名词解释

在核电厂安全规定中下列名词术语的含义为：

运行状态

正常运行或预计运行事件两类状态的统称。

正常运行

核电厂在规定运行限值和条件范围内的运行，包括停堆状态、功率运行、停堆过程、启动、维护、试验和换料。

预计运行事件②

在核电厂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，也不致导致事故工况。

事故（事故状态）

事故工况和严重事故两类状态的统称。

事故工况

以偏离③运行状态的形式出现的事故，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，严重事故不在其列。

设计基准事故

核电厂按确定的设计准则在设计中采取了针对性措施的那些事故工况。

严重事故

严重性超过事故工况的核电厂状态，包括造成堆芯严重损坏的状态。

①进一步指导见安全导则 HAF0406。

②属于预计运行事件的事例有：正常电源断电和汽轮机脱扣、核电厂正常运行中个别部件的误动作、控制设备中个别元件失灵和主泵断电等。

③偏离的例子有较大的燃料破损、冷却剂丧失事故等。

事故处理

为使核电厂恢复到受控安全状态并减轻事故后果而采取的一系列阶段性行动，行动阶段的顺序如下：

（1）事故序列在发展中，但尚未超出核电厂设计基准的阶段；

（2）发生严重事故，但堆芯尚未损坏的阶段；

（3）堆芯损坏后的阶段。

上述八个术语相互间的关系参见附图 1。

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、公众和环境免遭过量辐射危害。

安全系统①

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。

保护系统

有各种电器件、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。

安全执行系统

由保护系统触发用以完成必需的安全动作的设备组合。

安全系统辅助设施

为保护系统和安全执行系统提供所需的冷却、润滑和能源等服务的设备组合。

上述五个术语相互间的关系参见附图 2。

可接受限值

国家核安全部门认可的限值。

①安全系统包括保护系统、安全执行系统和安全系统辅助设施。安全系统的部件可以专用于执行安全功能，亦可在某些运行状态下执行安全功能而在另一些状态下执行非安全功能（见附图 2）。

能动部件①

依靠触发、机械运动或动力源等外部输入而行使功能，因而能以主动态影响系统的工作过程的部件（参见“非能动部件”）。

调试②

核电厂已安装的部件和系统投入运行并进行性能验证，以确认是否符合设计要求、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。

① 能动部件的例子有：泵、风机、继电器和晶体管等。应强调指出实际上这一定义只能是比较笼统的（非能动部件的定义也是如此）。某些部件，如爆破膜、逆止阀、安全阀、喷射器和某些固态电子器件等，需要对其特性进行专门研究后始可列属能动部件或非能动部件。

②审批过程通常以厂址选择、设计、建造、调试、运行和退役命名的六个主要阶段组成。六个阶段中若干阶段可交叉进行，如建造或调试和运行。

共因故障①

由特定的单一事件或起因导致若干装置或部件功能失效的故障。

建造

包括核电厂的部件制造组装、土建施工、部件和设备的安装及有关联的试验在内的过程。

退役

核电厂最终退出运行的过程。

设计

制定核电厂及其组成部分的方案和详细图纸，进行支持性计算并制订技术规格书的过程及其成果。

多样性

为执行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②。

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件。

功能隔离

为防止线路或系统的功能受到相邻线路或系统的运行方式或故障的影响所采取的措施。

检查

通过检验、观察或测量等手段，确定材料、零件、部件、系统、构筑物及工艺和程序是否符合规定要求的活动。

① 例如设计缺陷、制造缺陷、运行和维修差错自然事件、人为事件、信号饱和或源自其它操作、故障或环境条件改变的意外的级联效应。

②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、不同类型的设备。

许可证（执照）

由国家核安全部门颁发的，申请单位据以确定核电厂厂址、进行核电厂的建造、调试、运行和退役等特定活动的授权证书。

营运单位

持有国家核安全部门许可证（执照），负责经营和运行核电厂的单位。

运行

为实现核电厂的建厂目的而进行的全部活动，包括维护、换料、在役检查及其他有关活动。

运行限值和条件

经国家核安全部门认可的，为核电厂的安全运行列举参数限值、设备的功能和性能及人员执行任务的水平等一整套规定。

非能动部件①

毋需依赖外部输入而执行功能的部件。非能动部件内一般没有活动的组成部分，其功能的执行系在感受到某种参数，如压力、温度、流量的变化后完成。然而，基于不可逆动作或变化、又十分可靠的部件，可划为这个类别。

实体分隔

（1）几何分隔（增大间距、改变走向等）；

（2）设置适当的屏障；

（3）前两者的结合。

假设始发事件

经鉴明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②。

规定限值

由国家核安全部门确定或认可的限值。

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的系统化的活动。

①非能动部件的例子有：热交换器、管道、容器、电缆和构筑物。应强调指出，实际上这一定义只能是比较笼统的（能动部件的定义也是如此）。某些部件，如爆破膜、逆止阀、安全阀、喷射泵和某些固态电子器件等，需要对其特性进行专门研究后始可列属能动部件或非能动部件。

②假设始发事件的主要原因有：可信的设备故障和人员差错（核电厂内外）、人为事件或自然事件。核电厂假设始发事件的清单（明细表）必须经国家核安全部门认可。

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。

余热

放射性衰变和停堆后裂变所产生的热量以及积存在反应堆结构材料中和传热介质中的热量之总和。

安全功能

为安全着想必须完成的特定目的。

安全组合

用于完成某一特定假设始发事件下所必需的各种动作的设备组合，其使命是防止事件的后果超

过设计基准规定的限值。

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。

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的各种继发故障，均视作单一故障的组成部分。

厂址、厂区

具有确定的边界，在核电厂管理人员有效控制下的核电厂所在领域。

厂区人员

在厂内工作的全部人员，包括在编的和临时的。

厂址选择

为核电厂选择合适厂址的过程，包括针对有关设计基准的评定。

试验

为确定或验证物项的性能是否符合规定要求，使之置于一组物理、化学、环境或运行条考验之下的活动。

最终热阱

接受核电厂所排出余热的大气或水体，或两者的组合。

废物处理

有利于安全或经济的改变废物特性的处理过程，其三种基本途径为：（1）减容；

（2）去除废物中的放射性核素；

（3）改变成分。

设计基准外部事件

与某个外部事件或几个外部事件组合有关，能表达其特征，选定用于核电厂全部或其任何部分的设计参数值。

外围地带

直接围绕厂区、须在人口分布和密度、山地和水的利用等方面考虑采取应急措施的可能性的地带。

区域

足以把与某一现象有关的或某一特定事件影响所及的所有特征都包含在内的足够大的一个地理区域。

物项

材料、零件、部件、系统、构筑物以及计算机软件的通称。

客观证据

基于观察、测量或试验的、可被验证的、关于某物项或服务质量的定量或定性资料、记录或事实说明。

合格人员

符合特定要求、具备一定条件、而且被正式指定执行规定任务和承担责任的人员。

能动断层

在地表或接近地表处有可能引起明显错动的断层。

对供方的评价

对供方的管理体系进行评价，以确定供方是否有能力生产或提供规定质量的物项或服务，并是否有能力提供据以验收其物项或服务的证据。

运行人员

厂区人员当中参加核电厂运行的人员。

运行记录

记载着核电厂运行情况的历史资料，如仪表记录纸、各种证书、运行日志、计算机打印输出和磁带等。

核电厂运行管理者

由核电厂营运单位（或其主管部门）委任的负责指挥核电厂运行，并承担直接安全责任的人员（或组织）。

安全限值

过程变量的各种限值，核电厂在这些限值范围内运行已证明是安全的。 **记录**

为各种物项或服务的质量以及影响质量的各种活动提供客观证据的文件。

技术规格书（技术条件）

一种书面规定，说明产品、服务、材料或工艺必须满足的要求，气并指出确定这些规定的要求是否得到满足的程序。

文件

对于质量保证有关的活动、要求、程序或结果加以叙述、定义、说明、报告或证明的文字记录或图表资料。

检验

检查工作的一部分，包括对材料、部件、供应品或服务进行调查，在只靠这种调查就能判断的范围内确定它们是否符合规定的要求①。

不符合项

性能、文件或程序方面的缺陷，因而使某一物项的质量变得不可接受或不能确定。

监查

通过对客观证据的调查、检查和评价，为确定所制定的程序、细则、技术规格书、规程、标准、行政管理计划或运行大纲及其他文件是否齐全适用，是否得到切实遵守以及实施效果如何而进行的审核并提出书面报告的工作。

① 质量保证检验一般采用无损检验，包括手动检验、计量和测量。

附 件 A

假设始发事件

A1 概述

规定中列入此附件，是为了就假设始发事件用于本规定及其他有关文件的这一概念的定义和具体应用作进一步的阐述。

假设始发事件的正式定义是“经鉴明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“。从设备故障、人员差错、人为事件或自然事件之类的单一事件到各种事件的复杂组合均属于假设始发事件范畴内的事例。

假设始发事件的后果可能不大（如某一多重部件的失效），也可能很严重（如反应堆冷却剂系统主管道的破裂）。设计的主要安全目标在于追求电厂所具有的特性能够保证：大部分假设始发事件的后果较小甚或无足轻重；其余的假设始发事件，如有导致事故工况的可能，其后果仍然是可接受的。

对各类假设始发事件必须作出全面考虑，以保证潜在后果严重的和概率大的全部可信事件均在预计到的范围之内，且核电厂设计足以适应这些事件。假设始发事件的选择并无严格的准则可资遵循。更确切地说，此种选择过程无非是一种综合运用设计和分析之间的迭代、工程判断以及设计和运行经验的过程-排除某一特定的事件序列需要有力的论据。如多重失效可能导致严重事故，则多重失效的可能性亦应考虑在内。概率极低的事件序列则可不予 考虑。

用于改进安全重要物项的性能要求和电厂总的安全评价的假设始发事件的数量必须加以限制。为使这项任务切实可行，详细分析可限于若干代表性的事件序列①.具有代表性的事件序列包括所有同类事件，并为安全重要系统、构筑物和部件的设计的数字限值提供依据。

某些假设始发事件可基于已有电厂的经验、国家核安全部门的特殊要求或潜在后果的严重程度等种种因素，通过确定论法确定。另一些假设始发事件，由于设计特征、核电厂所在厂址或运行经验等因素可通过概率值定量表示的，则可基于概率法作出的规定。

典型假设始发事件一览表，见安全导则 HAF0211 附录。

①安全规定和导则中所用的“事件序列”一词是指某一假设始发事件和随后的运行人员行动或安全重要物项的动作的组合。

A2 假设始发事件的类型

A2.1 内部事件

A2.1.1 设备故障

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

需要考虑的故障类型取决于所涉及系统和部件的类型。故障的广义含义包括如下两类：系统或部件丧失执行功能的能力的功能的执行情况与所期望者不符。例如，管道故障的表现形式有泄漏、破裂和流道堵塞。能动部件，例如阀门的故障形式有：在需要时不开启或不关闭，在不应动作时开启或关闭，开不足或关不住，开启或关闭的时间或速度不当。仪表或传感器之类的装置的故障有如下形式：误差大于允许范围、无输出、不变的最大输出、输出不稳定或上述形式的组合。

A2.1.2 人员差错

人员过失的后果往往与部件故障的后果相类似。属于人员过失范畴的有：错误的或不良的维护、控制限值的错误整定和操纵员的其他错误行动。

A2.1.3 其他内部事件

内部原因引起的火灾、爆炸或淹没对电厂安全也可能产生重要影响。在汇编假设始发事件的清单时对此必须给以必要的考虑。

A2.2 外部事件

电厂的外部事件的事例及其设计基准的确定见安全导则 HAF0100 及其有关导则。特定厂址的各种可信自然事件和外部人为事件应在选址时确定，但在设计的早期阶段中必须对外部事件清单的完整性重新作出评定。

如能断定自然事件或外部事件引起某一安全重要系统、部件和构筑物故障的可能性通过设计和建造中所采取的措施可降低到可接受的程度，则由此引起的故障毋需列入电厂的设计基准。

A2.3 事件组合

随机发生的个别事件的组合能可倍地导致预计运行事件或事故工况时，必须视作设计基准。某些事件可能是另一些事件的后果，如地震后的洪水。这类后续故障效应必须视作原假设始发事件的一部分。

在决定事件组合时，考虑以下三个时期是有益的：

（1）事件发生前的长时期；

（2）从事件发生到它的短期效应起作用的近期；

（3）事件后的恢复期。

如在电厂设计中已为识别第一个时期内发生的事件采取了正确措施，且纠正行动可在短期内完成，则可以设想，在第一个时期内发生的事件可在发生另一次事件前得到纠正。在这种情况下毋需考虑此种事件的组合。

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

事件后的恢复期（几天或更长）内，是否需要考虑附加的事件，视恢复期的长短和事件预计的概率而定。恢复期内必须计及的事件组合中附加事件的严重程度，按低于电厂全寿期内所考虑的同类事故来考虑可能是合乎现实的。以失水事故后恢复期内需考虑的地震随机组合为例，其严重程序可按低于电厂设计基准地震计。

附 录 I

核电厂设计安全导则目录

HAF0201 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

HAF0202 核电厂防火

HAF0203 核电厂保护系统及有关设施

HAF0204 核电厂内部飞射物及其二次效应的防护

HAF0205 与核电厂设计有关的外部人为事件

HAF0206 核电厂最终热阱及其直接有关的输热系统

HAF0207 核电厂应急　动力系统

HAF0208 核电厂安全有关仪表和控制系统

HAF0209 核电厂辐射防护设计

HAF0210 核电厂燃料装卸和贮存系统

HAF0211 核电厂设计总的安全原则

HAF0212 核电厂反应堆安全壳系统的设计

HAF0213 核电厂反应堆冷却剂系统及其有关系统

HAF0214 核电广堆芯的安全设计