国家环境保护总局关于发布《核动力厂安全评价与验证》、《核动力厂营运单位的组织和安全运行管理》、《核动力厂定期安全审查》等三个核安全导则的通知 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/321/2021_2022__E5_9B_BD_E5_AE_B6_E7_8E_AF_E5_c80_321470.htm 国家环境保护总局关于发布《核动力厂安全评价与验证》、《核动力厂营运单位的组织和安全运行管理》、《核动力厂定期安全审查》等三个核安全导则的通知（国核安发〔2006〕92号）国防科工委、中核集团、广核集团、中电投有限公司，总局核与辐射安全中心，上海、广东、四川、北方核与辐射安全监督站，各有关单位： 为执行《核动力厂设计安全规定》（HAF 102）和《核动力厂运行安全规定》（HAF 103）， 提高我国核动力厂安全水平，促进核能事业健康发展，在充分研究国际核安全标准和我国现行标准及综合技术能力基础上，经广泛征求各方意见，我局修订了《核动力厂安全评价与验证》（HAD 102/17）、《核动力厂的营运单位》（HAD 103/06）、《核动力厂定期安全审查》（HAD 103/11）。现予以发布，自2006年7月1日起施行。 附件：1. 《核动力厂安全评价与验证》（HAD 102/17） 2. 《核动力厂营运单位的组织和安全运行管理》（HAD 103/06） 3. 《核动力厂定期安全审查》（HAD 103/11） 二〇〇六年六月十九日 附件1： 核安全导则 HAD102/17 核动力厂安全评价与验证 国家核安全局 核动力厂安全评价与验证 （2006年6月5日 国家核安全局批准发布） 本导则自2006年7月1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 1.2 范围 2. 安全评价、安全分析和独立验证 2.1 安全评价与安全分析 2.2 独立验证 2.3 设计、安全评价和独立验证之间的关系 3. 安全重要的工程技术方面 3.1 概要 3.2 经验证的工程实践和运行经验 3.3 创新的设计特性 3.4 纵深防御的实施 3.5 辐射防护 3.6 构筑物、系统和部件的安全分级 3.7 外部事件的防护 3.8 内部灾害的防护 3.9 与适用规范、标准和导则的一致性 3.10 载荷和载荷组合 3.11 材料的选择 3.12 单一故障评价和多重性/独立性 3.13 多样性 3.14 安全重要物项的在役试验、维护、修理、检查和监测 3.15 设备鉴定 3.16 老化和磨损机理 3.17 人机接口和人因工程的运用 3.18 系统之间的相互作用 3.19 设计过程中计算手段的使用 4.安全分析 4.1 概要 4.2 假设始发事件 4.3 确定论安全分析 4.4 概率安全分析 4.5 敏感性和不确定性分析 4.6 使用的计算机程序的评价 5.独立验证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》有关条款的说明和补充。1.1.2 本导则为设计单位在初始设计和设计修改过程中对核动力厂进行安全评价提供了建议，也为营运单位对于新核动力厂（使用新的或现有设计的）的安全评价进行独立验证提供了建议。实施安全评价的建议也适用于指导对现有核动力厂进行安全审查。依据现行的标准和实践对现有核动力厂进行安全审查，其目的在于确定是否存在影响核动力厂安全的任何偏离。本导则中的方法和建议同样适用于国家核安全监管部门进行的监管审查和评价。虽然本导则中大部分建议是通用的，并适用于所有类型的反应堆，但也有一部分特殊建议和范例主要用于水冷反应堆。 1.2 范围 1.2.1 本导则确定了在

实施安全评价和独立验证过程中的关键建议，并且提供了支持《核动力厂设计安全规定》的详细指导，尤其是在其安全分析领域。但是，它并不能包括目前所有可用的技术细节，关于具体的设计问题和安全分析方法，可参照相关安全导则和参考核安全法规技术文件。1.2.2 由于对核动力厂的某些系统的安全评价已有专门的安全导则，因此，本导则不包括对这些系统安全评价的具体建议。2.安全评价、安全分析和独立验证 2.1 安全评价与安全分析 2.1.1 本导则中的安全评价是一个系统性过程，它贯穿于整个设计过程，以保证核动力厂设计满足所有的相关安全要求。这些要求包括营运单位和国家核安全监管部门确定的安全要求。安全评价包括（但并不仅限于）正式的安全分析（见第4章）。设计和安全评价都是核动力厂设计单位进行的同一迭代过程中的组成部分，该迭代过程直到设计满足所有安全要求为止，其中也可能包括在设计过程中提出的安全要求。 2.1.2 安全评价范围包括核实设计是否满足《核动力厂设计安全规定》第3章至第6章中给出的安全管理要求、主要技术要求以及核动力厂设计和核动力厂系统设计要求，并核实已完成全面的安全分析。 2.1.3 《核动力厂设计安全规定》第3章中提出的安全管理要求，论及与经验证的工程实践、运行经验和安全研究有关的问题。 2.1.4 《核动力厂设计安全规定》第4章中提出的主要技术要求，包括保证提供充分的纵深防御措施，保证最大程度地考虑了事故预防措施和辐射防护。 2.1.5 《核动力厂设计安全规定》第5章中提出的核动力厂设计要求，与以下一些问题有关，如设备鉴定、老化以及通过多重性、多样性和实体分隔来提供安全系统的可靠性等。 2.1.6 《核动力厂设计安全规定》第6

章中提出的核动力厂系统设计要求，包括有关堆芯、反应堆冷却剂系统和反应堆安全系统（如安全壳以及应急堆芯冷却剂系统）的设计问题。 2.1.7 对于安全分析，《核动力厂设计安全规定》第5.9节规定：“ 必须对核动力厂设计进行安全分析，在分析中必须采用确定论和概率论分析方法。在这种分析的基础上，必须制定和确认安全重要物项的设计基准。还必须论证所设计的核动力厂能够满足各类核动力厂状态下放射性释放的所有规定限值和潜在的辐射照射剂量的可接受限值，并论证纵深防御已起到作用。 ”关于确定论和概率安全分析的范围和目的在本导则的4.1.3.1-4.1.3.6节中给出。 2.2 独立验证 2.2.1 《核动力厂设计安全规定》3.6节要求：“ 在提交国家核安全监管部门以前，营运单位必须保证由未参与相关设计的个人或团体对安全评价进行独立验证。 ”2.2.2 独立验证应该在营运单位负责下由一组专业人员完成，这组专业人员应尽可能独立于该核动力厂的设计者和进行安全评价的人员。如果这些专业人员未参与任何部分的设计和安全评价，则可认为是独立的。此独立验证是在设计单位内部进行的质量保证审查的补充。 2.2.3 安全评价是设计单位在整个设计过程中为满足所有相关安全要求而进行的综合研究工作，而独立验证是由营运单位完成或在其名义下完成的工作，可仅与送国家核安全监管部门报批的设计有关。 2.2.4 由于独立验证需要涉及的设计和安全评价问题的复杂性，一般在设计过程中要部分地进行独立验证，而不只是在核动力厂设计完成以后才进行。 2.2.5 营运单位对独立验证负有完全责任，即使独立验证的部分工作委托给一些独立机构执行也仍然如此。 2.3 设计、安全评价和独立验证之间的关系 2.3.1 图1给出了在核

动力厂设计过程中的安全评价、独立验证、安全分析及其他活动之间的关系，也给出了本导则与设计过程有关的其他规定和导则之间的关系。 图1 核动力厂设计安全规定和导则所覆盖的领域（略） 2.3.2 在设计工作由最初的概念直到最终完成的过程中，设计单位需要考虑营运单位和国家核安全监管部门提出的所有安全要求以及其他要求。由于核能规划的发展以及引入新的设计，在设计过程中，设计要求可能会被修改或澄清；在创新设计情况下，随着设计的深入可能会提出更具体的要求。 2.3.3 在设计过程中，安全评价和独立验证由不同的小组或机构完成，然而他们都是迭代的设计过程中的一部分，且二者的主要目的均是保证核动力厂满足安全要求。基于这个原因，本导则对二者均有论述。某些情况下，国家核安全监管部门也会在核动力厂设计阶段介入。 2.3.4 在核动力厂设计过程的一些阶段（如在建造前或首次装料前）设计工作将要被冻结，在此期间将完成安全分析报告，该报告将描述到此时为止所完成的核动力厂的设计和安全评价。该报告要提交国家核安全监管部门供审查和评价。 2.3.5 由于安全问题的讨论和澄清越早，解决起来就越容易。因此独立验证和设计及安全评价相继开展就会使独立验证更有效。当设计工作还在进行时，任何为改进设计和安全评价的建议都更容易被采纳。但另一方面，太密切的联系将给验证的独立性带来疑问。因而，应该找到有效性和独立性之间的平衡。 2.3.6 在设计过程中所做出的重大设计决策，营运单位应进行专项独立设计审查，这种审查仅限于该决策的范围并考虑符合适用于决策问题的安全要求。 2.3.7 设计工作应该依据质量保证大纲进行，质量保证大纲包括对所有设计文件进行独立

审查。3. 安全重要的工程技术方面 3.1 概要 3.1.1 本章为评价设计是否符合《核动力厂设计安全规定》第3章至第5章的要求提供建议和需要考虑的重要事项。这些要求覆盖总的安全重要的工程技术方面，并适用于所有的核动力厂系统。在安全分析中可能没有明确论及如何评价该方面要求的正确实施，但它是安全评价的一个相关部分。对于某些方面，没有明确的验收准则可供使用，因此对其符合安全要求的评价在很大程度上就只能依赖于良好的工程判断。 3.2 经验证的工程实践和运行经验 3.2.1 对于改进型的各类反应堆，应该尽可能采用在运行核动力厂中已成功应用的构筑物、系统和部件的设计，至少应该借鉴其他核动力厂中取得的相关运行经验。 3.2.2 在安全评价中，应该考虑可用的运行Q经验，以保证在设计中充分考虑了安全领域中的所有有关教训。运行经验应作为改进核动力厂纵深防御的基本信息来源。 3.2.3 应该充分利用大量的运行资料作为设计和安全评价的运行经验反馈。 3.2.4 从一个真实的事件序列进行外推分析，即假定在有额外失效（对比于现实情况中发生的失效）的情况下核动力厂最终将可能会发生什么，这个方法已被证明是一种有用的设计方法。 3.2.5 通用的安全研究项目的成果也会有效支持设计单位和审查单位的评价工作。 3.3 创新的设计特性 3.3.1 基于由运行经验、安全分析和安全研究得到的经验教训，有必要考虑超出现有实践的设计改进的需求和价值。当引入创新的或未经验证的设计或设计特性时，应该通过适当的支持性验证计划证实它们符合安全要求，并且在投入运行前，对这些特性进行充分试验。 3.3.2 例如，非能动安全系统是不依赖于诸如电力等外部支持系统的，并且有可能较能动系统而言更加

简化和可靠，但其实际性能及可靠性应该由适当的和周密的研发、试验和分析程序来得到可信的验证。 3.3.3 现代技术应用的另一个实例是采用基于计算机的安全系统和控制系统。与老式的硬件连接系统相比，计算机化的系统具有很多潜在的优点，如它具有更强的功能、更好的试验能力和更高的硬件可靠性。但是在某些实际情况下，这些优点可能是以降低系统的简易性和透明度为代价的，因此必须尽可能在接近实际运行环境下对计算机化的系统（包括其软件）进行广泛的评价和试验，以确认其性能和总体可靠性。 3.4 纵深防御的实施 3.4.1 正如《核动力厂设计安全规定》2.2.2所指出的，纵深防御概念的目的有两方面：首先是预防事故的发生；其次是如果预防失效，探测事故和限制其潜在后果，并且防止其演变为更加严重的工况。 3.4.2 纵深防御一般可分为五个不同层次。如果一个层次失效，后一层次将加以弥补或纠正。实施不同防御层次是为了使不同层次的防御独立有效。各层次的防御目的和其达到该目的的主要手段列于表1中。前三个层次的防御措施在设计基准范围内考虑，为了保证维持堆芯结构的完整性，并限制对公众的潜在辐射危害。超设计基准应该考虑第四个层次的防御措施，在考虑到经济和社会因素后，使核动力厂出现严重工况的可能性和放射性物质的释放处于合理可行尽量低的水平。 表1. 各防御层次的目的和主要手段

防御层次	目的	主要手段
一	异常运行和故障的预防	保守设计和高质量的建造和

运行 | ├──────┼──────────────────────────────┤ | 二 | 异常运行的控制和故障的探测 | 控制、保护系统及其他监督设施 | ├──────┼──────────────────────────────┤ | 三 | 设计基准事故范围内的控制 | 专设安全设施及 | | | 应急规程 | ├──────┼──────────────────────────────┤ | 四 | 核动力厂严重工况的控制，包括防止事故 | 补充措施和事故管理 | | 恶化和减轻严重事故后果 | | ├──────┼──────────────────────────────┤ | 五 | 减轻放射性物质大量释放的后果 | 厂外应急响应 | └──────┴──────────────────────────────┘

3.4.3 应该优先考虑预防：危及实体屏障的完整性；屏障失效或旁路；一道屏障的失效引起另一道屏障的失效；以及放射性物质的大量释放。 3.4.4 应评价核动力厂的设计，以确认有专门措施来保证第一到第四层次防御的有效性。 3.4.5 应通过完整的安全分析来证实是否能符合大量的核安全要求，从而完成对纵深防御实施情况的评价。此评价应确认各纵深防御层次足以应付可能出现的各种始发事件，以保证执行基本的安全功能和控制放射性物质的释放。 3.4.6 评价过程应特别注意内部和外部灾害，这些灾害可能会同时影响到不止一个防御层次，或者使得安全系统的多重设备同时出现失效。 3.4.7 设计应尽可能提供探测各防御层次失效或旁路的措施。应确定每种运行模式要求的防御层次（例如：在特定的停堆模式下，可以允许打开安全壳，

在核动力厂处于该模式时应始终能具备确定的防御层次）。3.5 辐射防护 3.5.1 有关辐射防护设计的详细建议可参照专门的安全导则。辐射防护评价应证实其符合在《核动力厂设计安全规定》中确定的辐射防护目标。 3.5.2 对于正常运行及预计运行事件，应该考虑两项设计目标：⑴保证辐射照射剂量低于规定限值；⑵保证辐射照射剂量处于合理可行尽量低的水平。应该比较计算出的剂量当量与规定的剂量限值，来证实符合第一个目标。设计单位应评价相关设计计算，以保证计算中输入数据的正确性和所用计算方法的有效性（见第4章）。 3.5.3 第二个设计目标（即满足合理可行尽量低的原则）意味着在考虑到经济和社会因素后，所有剂量应保证处于合理可行尽量低的水平。辐射防护的最优化过程应该在一定程度上使代价（费用）和利益（安全增益）相平衡。在此最优化过程中，辐射照射剂量的参考值以及相关的设计措施可以取自目前具有良好运行记录的类似核动力厂。安全评价应该考虑运行经验及附加的设计措施或改进，以进一步降低工作人员和公众的辐射照射。这些附加的措施既可以是直接的（改进屏蔽），也可以是间接的（减少设备维修的时间）。 3.5.4 应该采取以下措施保持低的照射量，如将包壳缺陷降低到最少、使用耐腐蚀的材料、减少长寿命腐蚀产物和活化同位素的形成、降低一回路冷却剂泄漏、尽量减少高辐射区域维修的时间、以及使用遥控操作工具和机器人。 3.5.5 在设计过程中，应该系统地评价诸如检查和维修所需的足够的空间、辐射防护屏蔽的充分性和核动力厂设备的正确安装。 3.5.6 核动力厂设计单位和安全评价人员还应该考虑核动力厂在最终退役期间操作的辐射照射剂量。为减少高活度放射性废物的数

量和便于其移出，应注意材料的选择和为拆卸设备和工具的预留空间，例如在受高辐射照射剂量的构筑物中使用的“牺牲层”（即在压力容器外围的混凝土屏蔽层）。 3.5.7 设备和场地的设计（诸如乏燃料的储存和装卸设施，以及放射性废物的储存）应采取措施，以尽量减少因其失效可能引起的放射性物质的释放。 3.5.8 设计单位应该证明，依据《核动力厂设计安全规定》，已具有足够有效的设计措施来实施辐射防护的充分监测。 3.5.9 应将安全分析中计算出的放射性物质释放量和剂量与国家核安全监管部门规定的或接受的限值进行对比，以评价事故工况下保护措施设计的充分性。为减轻超设计基准事故的放射性后果，可能要求在核动力厂厂区以及核动力厂周围采取一些特殊措施（如事故管理和应急响应计划）。在安全评价中，设计单位应该保证把事故管理和应急计划的相关参数充分地纳入核动力厂的设计中。 3.6 构筑物、系统和部件的安全分级 3.6.1 应该确定所有构筑物、系统和部件的安全重要性，并按照《核动力厂设计安全规定》中的规定建立安全分级体系，为每一安全级别确定： - 在部件的设计、制造、建造和检查中应用适当的规范和标准； - 系统相关的特征，如多重性的程度，以及对应急动力供应和环境条件鉴定的需求； - 在确定论安全分析中考虑应对假设始发事件的系统的可用性或不可用性状态； - 质量保证措施。 3.6.2 一般应该建立以下的分级体系，并且应该验证其恰当性和一致性： - 系统分级依据其对安全功能所起作用的重要性； - 承压部件分级依据其失效后果的严重性、机械复杂性和额定压力； - 抗震分类依据所考虑的构筑物或部件在地震中和地震后保持其完整性和执行其功能的要求，并计及余震及其后续

的附加破坏；- 电力、仪表和控制系统的分级依据其安全功能或安全支持功能，由于该系统是一个特殊领域，而且已经存在广泛使用的分级方法，其分级会不同于核动力厂其他系统分级；- 质量保证要求的分级。 3.6.3 对构筑物、系统和部件的安全分级的确定应该基于国家核安全监管部门规定的方法，并且应该适当地依据确定论和概率论分析以及工程判断。 3.6.4 在确定论安全分析中，用来确定符合验收准则的安全功能应只利用安全级的构筑物、系统和部件来执行。 3.6.5 在设计阶段，可使用概率安全分析来确认构筑物、系统和部件分级的适当性。 3.6.6 一个安全级别中的系统和/或部件的故障不应引起较高安全级别的系统和/或部件的故障。对于指定为不同安全级别且不同的并可能相互影响的系统，应该评价其是否具有充分的隔离和分隔。 3.7 外部事件的防护 3.7.1 在安全评价中涉及的外部事件取决于核动力厂选定的厂址，但是一般应包括：外部自然事件，如：- 极端的气象条件；- 地震；- 外部水淹；外部人为事件，如：- 飞机坠毁；- 由于运输和工业活动造成的灾害（火灾、爆炸、飞射物、有毒气体的释放）。 3.7.2 设计基准应该适合于所选厂址并以历史的和实际的数据为依据，并由一组数值进行表达，这些数值是按照规定阈值根据各事件总的概率分布而选择的。 3.7.3 当所得数据缺乏可信度而不能进行这种概率评价时，应该依据包络准则和工程判断使用确定论分析方法。 3.7.4 执行基本安全功能的构筑物、系统和部件应设计成能承受设计基准事件引起的载荷，并应能在这些事件发生时和发生以后执行其功能。这应该通过恰当的结构设计、多重性和分隔来实现。 3.7.5 应该使与外部事件有关的放射性风险不超过源自内部事故引起

的放射性风险。对于比设计基准事件稍微严重的外部事件，应该确认其后果不会不成比例地加重。 3.7.6 极端气象条件：应该对每一种极端气象条件确定设计基准事件。这包括下列条件： - 极端的风载荷； - 极端的大气温度； - 极端的降雨量和降雪量； - 极端的冷却水温度和冰冻； - 极端量的海植被。 3.7.7 设计基准应计及可以合理假设同时发生的各种极端气象条件的组合。 3.7.8 应该通过试验、实验或工程分析验证核动力厂的构筑物可以承受外部事件施加的载荷，而不会造成任何必要物项的失效，这些物项是将核动力厂带到并保持在所有基本安全功能得到长时间保证的状态所必要的。 3.7.9 应该通过试验、实验或工程分析证明安全系统能够在设计基准规定的条件范围内（如大气温度、海水温度和海平面高度）执行其安全功能。 3.7.10 应该利用核动力厂周边地域的地质勘察结果、该地域地震发生的历史记录和古地震资料确定核动力厂厂址的SL-2地震。SL-2地震应该用于确定核动力厂设计基准地震。 3.7.11 用于关闭核动力厂及维持核动力厂长时间处于安全稳定状态的构筑物、系统和部件应该设计成能够抵御设计基准地震而不丧失功能。 3.7.12 抗震鉴定应该包括结构分析、振动台试验以及适当时与运行经验进行对比。 3.7.13 外部水淹：应该对核动力厂的周边环境进行评价，以确定发生危及核动力厂安全的外部洪水的可能性。外部水淹应该包括由于高降雨量、高潮汐、河水溢出、堤坝坍塌以及其可能组合引起的水淹。 3.7.14 应该提供防护措施以避免外部水淹导致安全系统设备的故障。 3.7.15 应通过相关坠机的统计数据并考虑机场离核动力厂的距离、飞机的航线以及各型号飞机飞经核动力厂厂址的总的次数确定飞机坠毁于核动力厂的

预计概率。坠机统计数据应该在整个核动力厂运行寿期内不断更新。 3.7.16 如果预计的坠机概率大于可接受的值时，防护措施应该包括对包容安全重要系统和部件的构筑物进行加固，并要以设备多重系列分离和隔离的方法使其不会都被飞机撞击或随后的火灾所毁坏。对坠机的防护，应该集中在保证将核动力厂带到并维持在安全状态的安全功能所必需的物项上。 3.7.17 关于运输和工业活动所导致的灾害，应该鉴别靠近厂区的危险物品运输和能导致火灾、爆炸、飞射物、有毒气体释放的工业活动，并确定影响核动力厂安全的设计基准事件。 3.8 内部灾害的防护 3.8.1 设计中应该考虑由内部事件导致的作用在构筑物或部件上的特定载荷和环境条件（温度、压力、湿度、辐射），这些内部事件诸如：- 管道甩击；- 冲射力；- 由于管道、水泵及阀门的泄漏或破裂造成的内部水淹及喷淋；- 内部飞射物；- 重物跌落；- 内部爆炸；- 火灾。 3.8.2 应该确定管道破损的影响，诸如作用到部件、构筑物、电气设备、仪表及控制设备上的喷射冲击力、管道甩击、反作用力、压力波的作用力、压力增加、湿度、温度和辐射均得到充分考虑。特别应该表明：- 对于安全级设备、该设备的支承及相关构筑物的设计，均考虑了反作用力；- 对安全重要部件及其内部结构都已设计成能承受可信的压力波的作用力和流体的作用力；- 对于安全重要构筑物（诸如安全壳）已考虑了压力增加；- 对于安全重要的电气设备、仪表及控制设备已设计成在假定的泄漏和破裂的事件中，仍能够承受极端的温度、湿度和辐射。 3.8.3 关于内部水淹，应该对核动力厂的相关构筑物做水淹分析。分析中应该考虑以下潜在的水淹初因：承压部件出现泄漏和破裂、来自邻近构

筑物的水淹、灭火系统的误动作、水箱的溢流以及隔离设施的失效等。 3.8.4 安全重要构筑物、系统和部件，应该位于预计的最高水淹线以上，否则应予以足够有效的保护。 3.8.5 内部飞射物可能由诸如汽轮机之类的旋转部件的故障或承压部件的故障产生。对于可能的汽轮机飞射物，除非能证明潜在的飞射物不可能引起对安全重要构筑物、系统和部件的重大毁坏，否则应该考虑其可能的飞行路线，并且反映在汽轮机与安全级构筑物的相对方位上。类似地，对于安全级构筑物中的高能部件，应该尽可能限制其位置。 3.8.6 当相关的重物跌落可能导致核动力厂内或厂外辐射照射时，或者可能引起安全重要系统损坏时，设计时应该考虑其提升传动装置的故障。