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

1.1.1　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。此独立验证是除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全面综合研究工作，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，独立验证一般与在设计过程中要部分地进行独立验证同步进行，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。

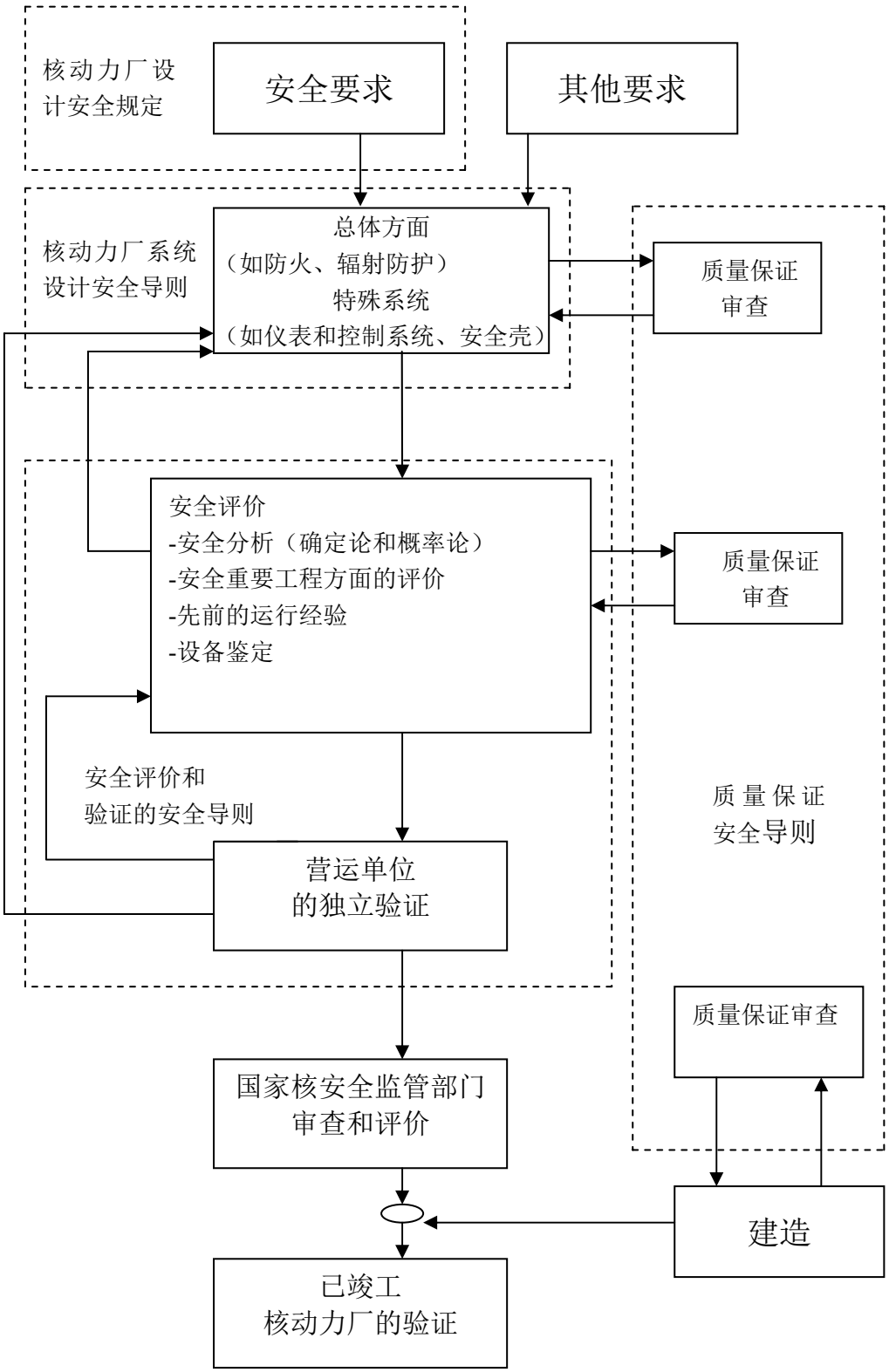

图 1 核动力厂设计安全规定和导则所涉及覆盖的领域

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。

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，在核动力厂设计阶段，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同时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，可要求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为设计单位和审查单位的评价工作提供有效支持。

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，有必要允许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辅助系统支持系统的，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操作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

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、控制、限制保护系统及其他监测监督设施

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，包括防止事故恶化和减轻严重事故后果 补充措施和事故管理

五　　减轻放射性物质大量释放的后果　厂外应急响应

表 1. 各防御层次的目的和主要手段

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。当某一如果一个层次失效时，更高的后一层次将加以弥补或纠正。实施不同防御护层次

是为了使其更高或更低不同层次的防御独立有效。各层次的防御护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，应该考虑采取前三个层次的防御措施。对于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，为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，应该考虑采取第四个层次的防御措施。

3.4.3　应该最优先考虑预防：过度地危及实体屏障的完整性；危及屏障时出现失效或旁路；某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立即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故障。

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保证辐射剂量辐射照射剂量低于规定限值；⑵保证辐射剂量辐射照射剂量处于合理可行尽量低的水平。应该比较通过将计算出的等效剂量当量与规定的剂量限值，对比来证实符合第一个目标。设计单位应评价对相关设计计算进行评价，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从目前具有良好运行记录的类似核动力厂得到射线照射剂量的参考值以及相关的设计措施。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射线照射。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　应该采取通过以下措施实践保持低的照射量，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剂量辐射照射剂量。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，例如在受高辐射剂量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　空间和设备和场地的设计（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量。

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等效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、系统和及部件的安全分级

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，以确定为每一物项的安全级别确定：

- 在部件的设计、制造、建造和检查中应用适当的规范法规和标准；

- 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的应对假设始发事件的系统的可用性或不可用性状态情况；

- 质量保证措施要求。

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，其分级会不同于可能和核动力厂其他系统分级不同；

- 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，用来确定决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以确认构筑物、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　应将要求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的加重。

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。这包括下列条件情况：

- 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引起的载荷，而不会造成任何必要物项的失效，这些必要物项是将核动力厂带到并保持在所有基本安全功能得到在长时间内保证所有基本安全功能的状态所必要的物项。

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建筑物做水淹分析。分析中应该考虑以下潜在的可能的水淹初因：承压部件出现泄漏和破裂、来自邻近构筑物的水淹、灭火系统的误动作开启、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。

3.9 与适用规范、标准和导则的一致性

3.9.1　为保证核动力厂的安全，构筑物、系统和部件的设计应该考虑其安全相关的重要性。对安全重要的构筑物、系统和部件的设计，应该根据以与其执行的安全功能的重要性相对应的设计要求进行设计为依据。构筑物、系统和部件的安全级别提供了确定用于其设计采用规范和标准的基础。

3.9.2　一般说来，设计所遵循的规范和标准的清单由营运单位以用户要求的形式给出，或者直接由国家核安全监管部门给出。但是，应对这些规范和标准进行审查和分析，以便依据现有知识和技术评价其对安全重要构筑物、系统和部件设计的适用性、恰当性和充分性。如果某些规范和标准不足以保证构筑物、系统和部件为执行重要安全功能而应具有的质量，就应该对这些规范和标准进行必要的补充或修改，以保证构筑物、系统和部件具备相称的质量。

3.10 载荷和载荷组合

3.10.1　安全级的构筑物和部件应该设计成能承受由运行状态和设计基准事故（包括内部和外部灾害）引起的所有相关载荷。

3.10.2　安全评价的一个重要部分为：

- 确定每项安全级构筑物或部件承受的相关载荷和载荷组合；

- 为每个载荷及载荷组合确定预计的事件发生频率；

- 评价安全级构筑物或部件在确定的载荷和载荷组合下的应力和应变；

- 在考虑了所有相关劣化退化（如蠕变、疲劳、老化）和其潜在

的相互作用后，评价在构筑物或部件中的单次和累加的损伤。

3.10.3　载荷和载荷组合应该是完整的，并且应与安全分析中的假定相一致。当合适时，应该依据合适的历史记录、运行经验、用户要求和及厂址特征对核动力厂运行寿期内事件预期频率和预期瞬态发生的总次数进行评价。

3.10.4　除所有相关物理量外，应力和应变的评价还应该考虑到每项载荷、每项载荷组合和适当的边界条件导致的环境条件和适当的边界条件。验收准则应该充分反映防止为减轻与假设载荷相关的灾害后果所需要的构筑物或部件发生的继发性失效。

3.11 材料的选择

3.11.1　材料应该满足设计和制造的标准和要求。确定材料的设计寿命应该考虑运行条件（如辐射环境和化学环境、一次或周期性的载荷）的影响。此外，还应考虑设计基准事故对其特性和性能的影响。

3.11.2　材料的适当性应基于试验，所有的试验结果均应该形成文件。

3.11.3　与放射性流体接触的材料应该具备抗御相关腐蚀机制的耐腐蚀性，并且在运行环境中耐化学反应。应该尽可能地避免碳钢和放射性物质接触。如果聚合材料用于包容放射性流体的系统中，该材料应具有耐辐照性能。

3.11.4　不锈钢或镍合金、与反应堆冷却剂接触的蒸汽发生器传热管、主管道材料及包壳材料应该具备足够的耐腐蚀性。低熔点元素，如铅、锑、镉、铟、汞、锌、铋、锡等及其合金不应该进入反应堆一

回路冷却剂系统或二回路系统，以防接触到由不锈钢或镍合金制造的的部件。应防止含有低熔点元素的轴承合金污染给水系统。为了减少运行辐射剂量辐射照射剂量，在与反应堆冷却剂接触的材料中，应尽可能限制钴的含量，当例外地使用钴合金时，应该给出其使用的恰当性。同时，还应该评价与冷却剂接触的材料中的镍向反应堆冷却剂的释放。

3.11.5　应通过设计来控制与不锈钢部件接触的材料（如管道保温层）中的卤素成分，以保证避免出现晶间应力腐蚀开裂。

3.11.6　对于反应堆冷却剂压力边界的铁素体材料，其在高温高压下的抗裂纹快速扩展的能力和抗疲劳的能力应该得到证实。所有的不锈钢焊接部件应该有抗晶界腐蚀的能力，同时也应该控制δ铁素体的含量，以将奥氏体不锈钢焊接中微裂纹的形成减少到最低程度。

3.11.7　应该特别注意所用材料与和水化学特性的相容性，以减弱腐蚀现象的发生。对于所有会受湿蒸汽或者强腐蚀性流体影响的设备，应该使用耐腐蚀和侵蚀的材料。可使用含铬（Cr>0.5%）的低合金钢。

3.11.8　应该选择在使用中副作用（如在停运时对工作人员造成的剂量、在发生事故时堵塞地坑）最小的保温材料。对于所选择的保温材料，应该对其由于事故中喷射力产生的碎片堵塞地坑的行为进行试验。

3.11.9　选择辐射环境中使用的材料时，应该考虑辐照对材料特性的影响辐照效应。例如，光纤维受到中子辐照时可能会损坏，这会

对所有使用此类光缆的系统（如基于计算机的控制和保护系统）执行安全功能产生了不利影响。

3.11.10 由于服役期间的辐照活化作用，在辐照环境中所用材料的选择会对核动力厂退役产生重要影响。在核动力厂的设计阶段应该予以评价这些方面。

3.12 单一故障评价和多重性/独立性

3.12.1 《核动力厂设计安全规定》中所述的单一故障准则的应用，即使假设安全组合 中任何一个部件单一故障，保证了设计基准范围内的假设始发事件发生后，即使假设安全组合 中任何一个部件单一故障时，所要求的安全功能仍然可以执行，并且设计基准中规定的限值均不会被超过。

3.12.2 单一故障准则的应用中，应该识别出作为假设始发事件的后果可能发生的任何一个故障，并且该故障应该包括在对于单一故障分析的起点中。

3.12.3 针对核动力厂所确定的每个假设始发事件，应该确定完成所需要的一组安全功能的安全组合。单一故障分析应该鉴别安全组合中各部件(包括其必需的辅助系统支持系统)所有可能的故障模式。此外，应该鉴别单一故障后果可能引起的所有故障，并且应该与单一故障一起包括在分析中。这类故障还应包括由于辅助系统支持系统（如电源或冷却水等）故障而导致的部件故障。但是，在单一故障分析中不考虑同时发生从不假定发生多于一个以上的随机故障。

3.12.4 应该在最薄脆弱的安全组合配置中应用单一故障准则。

特别是，核动力厂运行中允许设备停役相当长的一段时间以便进行维护、试验、检查或维修，并同时要求安全组合仍然具备可用性，在此的情况下，应该假定在核动力厂操作规程或技术规格书允许的设备最长停役时间时发生单一故障。尽管如此，正如《核动力厂设计安全规定》5.3.2.5 所述，对于规定的有限停役期间，不符合单一故障准则可能证明是适当的。对于所有这类情况，应该结合得出的允许停役时间，说明其合理性（见《核动力厂设计安全规定》5.3.5）。

3.12.5　单一故障分析中应该考虑的故障一般包括能动部件的故障（阀门按要求开启或关闭的故障以及水泵启动和运转的故障）和故障发生概率范围很广的非能动部件的故障（如安全系统管道的破裂故障）。在单一故障分析中，如果非能动部件不会受假设始发事件的影响，就可能不需要对设计、制造、检查和在役维修均处于高质量的非能动部件假设会发生故障。但是，对于在单一故障分析中省忽略的每一个部件的故障模式，应该证明其合理性。对于非能动部件，应该考虑在假设始发事件发生后部件预计运行的总时间。实际上，基于使用的质量标准，非能动部件的单一故障通常只在假设始发事件发生较长时间（如 24 小时）后才考虑。

3.12.6　单一故障分析不需要考虑发生频率很低的假设始发事件，也不需要考虑极不可能发生的假设始发事件的后果。

3.12.7　《核动力厂设计安全规定》规定，下述安全功能应根据单一故障假设由核动力厂相关系统执行：

- 快速停堆；

- 排出堆芯余热；

- 应急堆芯冷却；

- 安全壳隔离；

- 安全壳的排热；

- 安全壳的大气控制和净化。

3.12.8　实践中，为了得到足够高的可靠性或由于运行原因，可以提供比单一故障准则更高水平的多重性，如：⑴在要求安全组合有效的同时，为进行维护和修理，允许停役某些服役的设备进行维护和修理；⑵允许进行监督试验；或⑶减少在核动力厂布置中的问题。这意味着假设始发事件本身并不是一个事故，它只是引发一个运行事件、设计基准事故或严重事故的序列，这取决于发生的其他额外故障。典型的例子是：设备故障（包括管道破裂）、人员差错、人为事件和自然事件。安全系列之间的连接处应设计成单一故障不会导致丧失多于一个安全系列。多重安全系列应该有屏障分隔或距离分隔，以保证内部灾害不会丧失多于一个安全系列。

3.13 多样性

3.13.1　使用相似部件构成多重性的安全系统的可靠性将受到共因故障的制约，因为共因故障会导致一定数量的多重部件的同时故障。为避免此缺陷，可以采用多样性来提高可靠性。

3.13.2　依据实施的设计方案可以，提供不同的多样性水平可以不同。如果当多样的系统以不同的物理方式和使用不同类型的设备执行同样的安全功能时，该系统就具有较高的多样性。例如停堆，多样

性的系统既可是固体中子吸收体插入堆芯，又可以是向一回路冷却剂中注入中子吸收剂溶液。但是，如果使用不同类型部件的当多样性的系统以同样方式仅使用不同类型的部件执行同样的安全功能时，该系统的多样性水平就较低。例如，一个应急给水系统，在系统不同部分的泵和阀门仅具有不同的型号，或由不同的制造商供货。

3.13.3　当系统需要非常高的可靠性时，应该使用多种方法来执行其安全功能。多样性的水平应该和执行安全功能手段所要求的可靠性相匹配。

3.13.4　安全系统内使用多样性时，应该证实其与所要求的系统可靠性相一致。为此，潜在的共同弱点（如共因故障）应该充分说明。例如，这些弱点可能是设计缺陷、制造缺陷、操作或维修错误、自然现象、人为事件或核动力厂中任何其他操作或故障引起的非预期的级联效应。

3.13.5　应该认识到，多样性措施会增加核动力厂的复杂性和费用，并在其运行和维修中带来困难和额外费用。这应该在设计过程中说明，并且应在安全系统可靠性的得益与提高和由此导致的附加的复杂性之间求得平衡。

3.14 安全重要物项的在役试验、维护、修理、检查和监测

3.14.1　除下一节提到的构筑物、系统和部件外，在核动力厂寿期内，其他安全重要构筑物、系统和部件的设计在其完整性和功能的能力的方面，均应该能在核动力厂寿期内对完整性和功能的能力设计为能对其进行定期试验、维护、修理、检查或监测。试验、维护、修

理、检查或监测的周期取决于物项的属性，可以从几天到几年不等。核动力厂带负荷运行期间维护得越频繁，其停役期间所需要的维护就越少。核动力厂的设计应该使得这些活动能按标准执行，这些标准与各系统所执行的安全功能的重要性相匹配，并且对厂区人员没有不适当的辐射照射。

3.14.2　如果安全重要的构筑物、系统和部件不能设计成以合乎要求的范围程度进行试验、检查或监测，则应该对可能尚未发现的故障采取足够的安全预防措施以弥补可能的尚未发现的故障。

3.14.3　设计单位应该编制专门的设计指南，用以保证检查和试验的可达性。在这方面，需要评价的关键问题包括：部件周围是否有足够的可用空间；通过减少一回路压力边界内的放射性物质的沉积或防护层来降低部件周围的辐射场；减少一回路水的泄漏；提供永久或可拆装移动的通道以及在构筑物上为部件移动设置为移动部件的悬挂设施点；在适宜的位置安装部件以便于检查和试验的部件。

3.14.4　在无法实现可达性的情况下，设计应能够提供永久的导轨和足够的空间，以允许适当地放置检查设备并用远距离传动装置操作。安全评价应该确定已考虑了这种可能性。

3.14.5　尽管在大多数情况下实施了上述措施有助于解决保持运行剂量低的需要和进行定期试验和检查的需要之间的矛盾，但在某些复杂情形下，应该运用在设计水平上的安全分析对二者的正确折衷选择做精确研究。

3.15 设备鉴定

3.15.1　设备鉴定主要应用于事故工况时需要执行安全功能的安全系统。

3.15.2　预计设备预计执行其安全功能时的条件工况可能不同于其正常情况下经受的条件工况，而且随着核动力厂的运行，其性能也会受到老化或工作环境的影响。作为设计过程的一部分，应该确定设备预计承受的环境条件。各类事故中应该预期的环境条件包括温度、压力、辐射、振动和湿度的极端情况以及喷射冲击等。

3.15.3　在整个核动力厂运行寿期内，设备所要求的功能能力应该得到维持。在设计阶段，注意给出老化效应导致的共因故障。应该根据恰当确定的环境条件、工艺条件、工作循环周期、维护安排、使用寿命、型式试验安排、更换部件和更换间隔时间等在设计中考虑设备的老化。

3.15.4　设备鉴定程序应该确认设备在其整个运行寿期内，经受在需要其工作时可能存在的所有环境条件（动力学效应、温度、压力、喷射冲击、辐射、湿度），仍然具备执行其安全功能的能力。这些环境条件应该包括在其正常运行、预计运行事件和事故工况时预计的各种变化。当要求如果设备在受到遭遇外界自然事件中或并预计在此该事件期间或在此后仍然能够执行其安全功能，就要在则鉴定大纲中应规定重现由该自然现象施加在设备上的条件。

3.15.5　鉴定大纲还应该包括能够由特殊运行工况（诸如定期安全壳泄漏率试验）引起并合理预计的异常环境条件。在可能的条件下，预计在严重事故中运行的设备应该通过试验、实验或工程分析，以合

理的可信度表明能够在严重事故工况下实现设计意图。

3.15.6　设备鉴定较好的方法是通过对其原型设备的试验来完成。当然，这对于大型部件的振动以及设备的老化并不总是可行的。在这些情况中，应该依赖于采用在相似条件下对的设备性能的外推、分析或者是试验加上分析作设备鉴定。

3.16 老化和磨损机理制

3.16.1　安全评价应该考虑到核动力厂的系统和部件会不同程度地受到老化效应的影响。某些老化效应是已知并可以采取措施加以解决的；另外一部分其他的老化效应，单凭经验不能预计，应使用合适的试验、检查和监督大纲，以探测发生的可能性。在设计阶段应该拟定出一份在核动力厂运行寿期内的完整的行动计划及制定为实施此计划制定的技术先决条件。定期安全审查是一个很好的方法，它可以确定是否正确考虑到了老化和磨损机理制，并且可以发现到许多未曾预计到的问题。

3.16.2　设计应该考虑到在核动力厂整个寿期内由来自堆芯快中子注量作用引起的压力容器的脆化。其防护应该依赖于防止过度脆化的良好设计、便利的脆化裂探测和可能的补救措施。由于尺寸效应和/或中子效应，压水堆较之沸水堆受此问题影响更大。焊缝处更易于受脆化的影响，因为焊接过程引入杂质，而使得焊缝区域对中子照射特别敏感。焊缝区域周围的热影响区域通常是微裂纹和剩残余应力累积的地方，这使得该区域对脆化裂效应更加敏感。

3.16.3　在燃料活性区的范围内应该尽可能地避免出现焊缝。

3.16.4　应该适当考虑限制和监测容器脆化。由于存在某些不确定因素，中子注量（在核动力厂运行的整个寿期内中子注量率的累计）应该保持低于某一水平，该水平保证容器具有足够的机械性能。应有适当的监测大纲，该大纲采用把压力容器焊缝取样本和处于具代表性条件的中子注量测量装置处于具代表性条件的中子注量率中进行监测。另外一个主要的老化过程会影响到压水反应堆的蒸汽发生器传热管系统。传热管的恶劣化有很多的原因，应该对其进行监测，以允许在传热管泄漏或故障前采取预防和补救措施，如改变水质、维修和堵管。应设计应通过足够的间隙、导轨和固定点便于对蒸汽发生器进行监督、维修和拆换。

3.16.5　依据过去的运行经验，以下列出过去运行经验表明的其他可能的老化效应。应该在核动力厂的设计应在设计阶段排除这些老化问题，或者包含能及时探测到其开始老化初始效应并执行采取适当纠正行动的方法：

- 压力管反应堆内管道氢化和脆化裂，这些可能会导致管道的更换；

- 堆内构件的腐蚀、振动和故障及其由适当监视方法监督措施进行探测的可能性；

- 堆芯接管及堆内构件裂纹；

- 接管和管道中的热瞬态和压力瞬态；

- 管道连接处的热交混；

- 管系内的热分层和部件中的其他管道腐蚀，这些应该可在定期

检查中探测并有由合适的设计措施保证其便于在定期检查中进行探测；

- 电缆有机绝缘材料或通风装置密封材料的老化，这些应该在设计中得到考虑，以便允许对其进行探测并且允许有可能更换。

3.17 人机接口和人因工程的运用

3.17.1 核动力厂的设计应该便于运行人员在核动力厂运行状态和事故中工作和促进人的能力最佳发挥。这应该通过认真关注核动力厂的设计、操作规程的制定和所有运行人员的培训来实现。

3.17.2 在早期的设计开发阶段，设计过程中应该系统地考虑人为因素和人机接口，并且此考虑应该贯穿于整个设计过程。

3.17.3 应该确定分配给运行人员的安全行动。这些安全行动是由负责监测和控制核动力厂的以及对承担故障和维修、试验和校准活动作出响应的运行人员来完成。

3.17.4 应该对安全行动作任务分析，以根据作出并执行的决定来评价在作出决策和执行行动方面对运行人员提出的要求。人机接口的设计说明书、需要提供的信息和控制、运行规程和培训大纲的准备，应由任务分析的结果确定。应该决定人机接口的设计说明书、需要提供的信息和控制、制定运行规程以及培训大纲。

3.17.5 应该提供充分的信息和控制，应该充分允许运行人员进行以下操作：

- 实现进行正常操作运行，例如改变反应堆的功率水平；
- 便易于评价核动力厂正常运行、预计运行事件以及事故工况中

时的总体状态况；

- 监测反应堆的状态和核动力厂所有设备的状况；
- 确定对安全有重要影响的核动力厂状态的变化；
- 确认预定设计的自动安全行动正在执行；
- 确定所有规定的行动并予以执行。

3.17.6 应该为运行人员提供足够的有关核动力厂每一个系统和设备的参数信息，以确认要求的安全行动已经实现，并且提供行动已达到了对行动达到了所期望的效果提供的反馈信息。

3.17.7 厂区人员的工作场所区域和工作环境应该按照人机因工程学原则进行设计，以使各项任务得以有效和可靠地执行。这应该包括控制室、辅助控制室、应急控制中心、核动力厂中所有就地控制站岗位、以及所有执行任何会进行维修和试验的工作区域的设计。应该特别留意显示系统、仪表盘布局和执行维修及试验操作人员工作的空间的通道。

3.17.8 人机接口应该设计成能够为运行人员作出正确决策和采取行动提供全面而的、易处理的信息。

3.17.9 需要运行人员在短时间内进行干预的需求情况应该维持在最低程度。对所有这些需要在短时间内需要的动作应该自动提供自动控制。应该在根据可证明是合理的最佳估算基础上对此时间容限进行评价。

3.17.10 对于所有运行人员的行动，任务分析应该证明：运行人员有足够的时间作出决定和采取行动执行；作出决定所必需的信息是

简单明了的;，并且在发生事件后在控制室或者辅助控制室及通往辅助控制室通道内的实际环境是可接受的。

3.17.11 核动力厂的设计应该能够承受人为差错人员差错。在合理实际可行的范围内，任何不适当人为的人为不适当的活动作应该是无效的。为此，应该审慎地选择运行人员行动和安全系统动作之间的优先权。一方面，一旦触发采用启动准则就不允许运行人员取消反应堆保护系统的动作；另一方面，在某些情况下，运行人员对于保护系统的干预却是必要的，例如为试验目的或为了改变运行状态采用触发启动准则而进行的手动旁通。此外，当万一反应堆保护系统内部发生严重故障时，为了应付超设计基准事故，在严格的行政控制下，运行人员应该具有干预保护系统的最终可能性。

3.17.12 由运行人员采取的所有行动，都应该提供书面规程，包括核动力厂正常运行以及从异常事件和事故（包括严重事故）恢复到正常状态的恢复过程。对异常事件和事故做出响应的规程，较好的方法更可取的是征兆定导向规程。这些规程应该通过预检操作和适当地时利用实体模型和模拟机来确认。

3.17.13 应该提供充分和可靠的通信手段，以便在核动力厂正常运行和事故后的恢复过程中，能使信息和指令在不同地点之间传送，以支持运行人员的行动。这应该包括控制室或应急控制中心与处于遥控位置的就地现场（？）工作人员（该工作人员可能必须采取影响核动力厂状态的行动）之间的通信，以及在事故情况下与厂外机构的通信。通信手段应该在所有相关事故工况下有效，并且不会干扰核动力

厂保护系统。

3.17.14 远距离就地控制点的布置和确定应该考虑到人的因素，如降低操作人员在选择远距离就地控制点时出错的可能性。

3.18 系统之间的相互作用

3.18.1 应该仔细评价同一个核动力厂系统之间、核动力厂和厂外电力设施之间可能的相互作用，以及同一厂址中不同核动力厂之间可能的相互作用。核动力厂所有的运行状态（包括外部灾害和严重事故）均应该考虑系统之间的相互作用。

3.18.2 分析不仅要考虑实体的连接，还要考虑系统运行、维护、误动作或者故障对其他安全重要系统物理环境的影响。环境的改变会影响系统执行预计功能的可靠性。例如，用于电子设备的空调系统故障以及会在安装安全系统设备区域内引起水淹或高湿度的液体系统的故障，都会对其他系统的性能造成负面影响。

3.18.3 对设计进行安全评价时，应该考虑与核动力厂安全重要系统供电可靠性相关的电网-核动力厂之间的相互作用。

3.18.4 安全重要构筑物、系统和部件通常不应该在两座个之间或更多座核动力反应堆之间所共用。但是，如果已共用，就应该通过试验、实验或工程分析以证实，处于任何状态的所有反应堆处于任何状态时，均能够满足所有的安全要求均能够得到满足。当某一座反应堆发生事故时，其余反应堆应该能依次停堆，并且能排出其衰变热能够排出。应该专门考虑可能会导致不止一个核动力厂发生事故的外部事件。共用辅助系统支持系统应该能够应付所有受影响的反应堆。

3.18.5　应该在安全评价中校核其他设计和运行接口，包括技术规格书和运行规程。

3.19 设计过程中辅助计算手段机辅助的使用

3.19.1　工程设计使用很多的大量软件工具，如图表、单线图、公式、运算法则和计算机程序（中子物理学、流体动力学、结构分析等）。这些工具以及其中所用的数学模型应该遵守相应的质量保证大纲，包括其在本导则第 4 章（4.6.1-4.6.8）中所描述的计算机程序的验证与确认。

3.19.2　所有的数学模型应该通过对比、独立分析和质量鉴定说表明其可靠性，以保证其固有的不确定性水平能符合整个设计项目所要求的可靠性。

4.安全分析

4.1 概要

4.1.1　引言

4.1.1.1 安全分析的目的是通过用适当的分析工具建立并确认安全重要物项的设计基准，并且保证在核动力厂每一工况类别内，其核动力厂总体设计可以满足为核动力厂每一工况类别规定的和可接受的辐照剂量和释放的限值。设计、制造、建造和调试均应该纳入安全分析中，以保证设计意图已体现在竣工的核动力厂中能够满足设计意图。

4.1.1.2 作为设计过程的一部分，应该由负责核动力厂安全的两个机构进行安全分析。这两个机构是：

- 设计单位：设计单位应把安全分析作为设计过程的一个重要组成部分并一直持续到核动力厂的制造和建造的整个过程；

- 营运单位：营运单位利用安全分析来保证竣工设计能够如期望的一样在运行中实现，并且确认该设计在核动力厂设计寿期内的任何情况下均能满足安全要求。

4.1.1.3 用安全分析作为核动力厂取证的安全评价一部分的安全分析，应该与设计过程同时进行，并且两种活动之间相互迭代。安全分析的范围和详细程度应该随着设计过程的进展而不断增加，以使便最终的安全分析反映按此最终建造的最终核动力厂设计。

4.1.1.4 在设计过程中进行安全分析的建议也可以用于指导运行核动力厂的定期安全分析，或判断拟议的设计修改的安全合理性。定期评价的要求在《核动力厂运行安全规定》及相关导则中论述。

4.1.1.5 在设计阶段及整个核动力厂寿期内（包括退役过程），核动力厂设计模型和数据（这些是安全分析的重要基础）应该不断更新。在设计阶段，该工作是设计单位的责任，而在核动力厂的整个寿期内,则是营运单位要履行的职责。

4.1.1.6 更新过程应该引入能得到的可用的新信息；涉及提出新出现的新问题；采用可得到的更精确的工具和方法；以及评价在整个核动力厂寿期内可能考虑的设计和运行规程的修改。

4.1.1.7 本导则第 3 章中描述的安全重要的工程技术方面的评价和本章中描述的安全分析应该同步进行。

4.1.2　安全分析的目的

4.1.2.1 安全分析应该评价核动力厂在各种不同运行工况、假设始发事件及其他情况（其中大部分可能在实际的核动力厂运行中从未出现）下的性能，以便对核动力厂在这些情况下的预计工作情况性能有一个完整的了解。安全分析还应该证实核动力厂能够保持在由设计单位确立的安全运行状态内。

4.1.2.2 安全分析应该对照由营运单位、国家核安全监管部门以及（如果没有，可参照其他国家或、国际有关机构）制定的适用的安全和放射性释放的目标或准则，正式评价核动力厂在各种运行工况和事故工况下的性能。

4.1.2.3 安全分析应该发现设计中可能存在的缺陷，评价提出的设计改进和证实设计满足安全要求及核动力厂的风险处于可接受的低水平。这应该与确定的风险准则相比较。

4.1.2.4 安全分析应该作为在制定和确认核动力厂保护及控制系统的整定值和控制参数中的重要工具来支持核动力厂的安全运行。安全分析还应该用于制定和验证核动力厂的技术规格书和限值、正常和异常运行规程、应急规程、维修和检查要求以及正常和应急规程。

4.1.2.5 在核动力厂寿期内出现新的问题时，安全分析应该为核动力厂的管理部门和国家核安全监管部门的决策过程提供支持。在核动力厂的整个寿期内，应该保持核动力厂初始安全分析和再进行全部或部分的安全分析的能力，以解决新的技术问题。这意味着核动力厂最新的、实际的设计信息和运行性能数据，必要时应该放入核动力厂模型，以便支持该安全分析过程。

4.1.2.6 安全分析应该协助揭示早期设计阶段未曾充分考虑的问题、核动力厂工况和始发事件。同样地，安全分析能够识别其他的问题，如不必要的假设始发事件和规定的验收准则（也就是说，当进一步深入分析时，由于发现它们发生的频率很低，可忽略的条件概率或是其潜在后果影响甚微，因此它们并不对核动力厂的安全有所影响或贡献）。

4.1.2.7 安全分析应该评价：

- 是否为核动力厂提供了充分的纵深防御以及各防御层次是否能尽早抑制可能的事故序列；

- 核动力厂是否能承受会经历将要经受的物理和环境条件，这包括极端的环境状况及和其他条件情况；

- 是否已充分涉及了人为因素及人的行为问题；

- 已识别、监视和管理在整个核动力厂寿期内可能会导致核动力厂可靠性会降低其可靠性的长期老化机理（如通过升级、整修或更换）是否均已识别、监视和管理（如通过升级、整修或更换），以保证核动力厂安全性不受影响安全性且风险不会增加风险。

4.1.2.8 安全分析应该通过试验、评价、计算或工程分析证实：用于防止预计运行事件升级、或者设计基准事故升级为严重事故并且减轻其后果的设备、以及应急运行规程和事故管理措施，可有效在将风险降低到可接受的水平方面都是有效的。

4.1.2.9 安全分析过程应该在足够的范围、质量、完整性和精确性方面都应该是高度可信的，以增强设计单位、国家核安全监管部门、

营运单位和公众对核动力厂设计安全性的信心。安全分析的结果将以高的置信度保证核动力厂将会按设计来运行并在调试及整个寿期内均能够符合所有设计验收准则。

4.1.3　确定论和概率论评价

4.1.3.1 应该主要以确定论方法证实核动力厂具备高水平的安全性。但是，安全分析应该采用确定论和概率论相结合的方法。确定论和概率论的方法是相互补充的，并且这两种方法应该用于对拟取得许可证的核动力厂的安全性和能力方面进行决策的过程中。在确定论方法不能处理的某些方面，如核动力厂性能、纵深防御以及风险，概率论分析方法却可以对其进行深入分析。

4.1.3.2 确定论方法的目的是给出核动力厂在特定的预定运行状态及事故工况下的行为，并且运用一组特定的规则判断设计的充分性。

4.1.3.3 用于设计的确定论分析通常应该是保守的。超设计基准事故的分析一般不如设计基准事故的分析来得保守。

4.1.3.4 概率安全分析应该侧重于确定所有造成核动力厂风险的重要贡献，并且应该评价总体系统配置设计是良好平衡的，、确定没有风险遗漏和设计符合基本概率安全目标。概率安全分析应最好采用最佳估算方法。

4.1.3.5 应该在决策过程中同时采用从确定论分析和概率安全分析中得出的结论。一般来说，来自确定论分析和概率安全分析的结论是一致的。特别是，在核动力厂设计或运行中确定识别的缺陷往往

与用于执行一个或多个安全功能的安全系统的多重性或多样性的不足有关。

4.1.3.6 也存在确定论分析和概率安全分析得到的结论不一致的情况。这时应该具体问题具体分析。

4.1.4　重要信息

4.1.4.1 安全分析应基于完整而准确的核动力厂设计资料。这些资料应该包括核动力厂所有的构筑物、系统、部件、与厂外的接口关系以及厂址特征。

4.1.4.2 核动力厂设计应该形成文件，并且随着核动力厂设计的批准、竣工和修改，文件而不断更新。

4.1.4.3 对于正在运行的核动力厂，安全分析（如用于设计修改）应该使用核动力厂实际的运行数据。这些数据包括核动力厂正常运行时运行人员的辐照剂量和放射性物质从厂区的日常排放。对核动力厂系统，采集的数据应该包括正常运行的温度、压力、水位和流量以及对所有运行事件的瞬态响应特性和运行事件的时间持续。

4.1.4.4运行数据还应该包括下述有关信息：系统和部件的性能、始发事件频率、部件故障率数据、故障模式、维修或试验期间系统的不可用性以及系统和部件的维修次数。

4.1.4.5 对于设计阶段的核动力厂，使用的数据应该取自类似设计的运行核动力厂的通用数据，或来自研究或试验结果。对正在运行的核动力厂，随核动力厂自身的运行和维修数据以及试验和检查结果的特定数据的积累，通用数据库中的某些数据可能会随时间增加。

4.1.4.6 安全分析应该包括核动力厂中所有放射性物质的所有来源。除反应堆堆芯外，放射性物质还包括运输中的和储存中的辐照过的过的燃料以及储存的放射性废物。

4.1.5 安全分析的验收准则

4.1.5.1 对于确定论评价和概率安全分析都应该确定验收准则。这些既验收准则通常反映了设计单位或和运行人员营运单位应用的准则，也与国家核安全监管部门的要求相一致。

4.1.5.2 准则应该能够充分满足《核动力厂设计安全规定》中叙述规定的总的核安全目标、辐射防护目标和技术安全目标。

4.1.5.3 应该制定详细的准则以保证符合更高级别的目标（见4.3.1.9.3.1-4.3.1.9.3.6）（见 4.3.2.9.3.1~4.3.2.9.3.6）。这通常将使分析简化。

4.2 假设始发事件

4.2.1 假设始发事件的确定

4.2.1.1 安全分析的起始点是需要涉及的一组假设始发事件组。假设始发事件按照《核动力厂设计安全规定》的定义是“在设计时确定的能导致预计运行事件或事故工况的事件”。假设始发事件包括设备故障、人员差错、人为事件以及自然事件。确定论安全分析和概率安全分析通常应该采用一组通用的假设始发事件。

4.2.1.2 为安全分析而制定的一组假设始发事件组应该是全面的，并且应该以这样方法确定，即覆盖包括在核动力厂的任何运行模式（如启动、停堆和换料）期间可能发生的核动力厂系统、部件所有

可信的故障以及人员差错。这应既包括内部和始发事件又包括外部始发事件。

4.2.1.3 应该用以系统的方法确定一组假设始发事件。这应采用结构型的方法来确定假设始发事件，它包括：

- 采用如危害性和可运行性分析、故障模式和效果分析以及主逻辑图的分析方法；

- 与类似核动力厂安全分析用的假设始发事件清单进行对比（但是该方法不应该不加选择地广泛使用，因为可能传播或继承先前的错误）；

- 对类似核动力厂的运行经验数据进行分析。

4.2.1.4 涉及提出的一组假设始发事件组还应该包括可能会对风险有重大贡献的设备的部分故障。

4.2.1.5 随着设计和安全评价的进展，应审查假设始发事件组，并且这两种活动之间应有一个迭代过程。

4.2.1.6 假设始发事件组还应该包括概率极低或后果不大的事件，至少在过程起始时应该包括它们。排除掉某些假设始发事件是有可能的。然而，任何假设始发事件的排除都应有充分论证，并且将其理由形成文件。许多假设始发事件将保留直到至分析结束，并仅在得出分析结论时才被确定是不重要的。

4.2.1.7 所有假设始发事件的发生频率均应加以定量。它应定量地用于概率安全分析中，定性地用于确定论中。

4.2.2 内部假设始发事件

4.2.2.1 为了确定那些对可能影响基本安全功能可能的影响问题，应该明确内部假设始发事件（那些在核动力厂内部发生的事件）。执行安全功能的方式取决于反应堆的具体设计。但已确认的始发事件的类别一般包括：

- 反应堆冷却剂系统排出热量的增加或减少；
- 反应堆冷却剂系统流量的增加或减少；
- 反应性和功率分布异常；
- 反应堆冷却剂装量的增加或减少；
- 来自于子系统或部件的放射性物质释放。

4.2.2.2 内部假设始发事件组的确认还应该考虑安全系统和部件的各种故障形式，以及会影响到基本安全功能的或安全系统的非安全系统和部件的故障。这些故障中的大部分均能够归结到上述类别中的某一种。但是，其中某些基于故障的假设始发事件的故障并不属于上述的类别，应该对其单独分组。到目前为止，已由已做的概率安全分析确定的这些部分其他故障的实例包括：⑴辅助系统支持系统故障，如设备冷却水或厂用水丧失；⑵来自由于循环水、厂用水、消防系统或高架波动水箱等的破损造成的内部水淹；⑶虚假的安全壳隔离信号导致的主冷却剂泵的冷却丧失；⑷卸压阀的误启动作。

4.2.2.3 内部假设始发事件组的确认过程还应该计及反应堆压力承压边界的各种故障模式。这应该包括所有可能位置（包括可能发生在安全壳外）的管道破裂，包括会出现在安全壳外的管道破裂。

4.2.2.4 内部假设始发事件应该包括核动力厂所有运行模式中

可能出现的故障模式（例如，初始堆芯临界时的反应性瞬态和安全壳敞开时换料模式期间的冷却剂装量损失），但持续时间可忽略的运行模式除外。只有在慎重考虑并通过保守分析证实这些运行模式与由其他假设始发事件计算的堆芯损坏频率相比是不重要时，才能够排除这些持续时间可忽略的模式。

4.2.2.5 假设始发事件组应该包括作为人为差错人员差错的后果而会引发的初因事件组。这些人为差错人员差错的范围是从不合格的错误或不完善的维修操作到错误地设定置控制设备的限值以及或运行人员的误操作。这些假设始发事件不一定与由设备故障导致的假设始发事件类似，因为其除始发事件外，还可能引发共因故障。

4.2.2.6 内部假设始发事件组还应该包括火灾、爆炸、汽轮机飞射物冲撞击和源自内部的水淹，它们可能影响反应堆安全和导致对该始发事件提供保护的某些安全系统设备的故障。这些假设始发事件已经在第 3 章中讨论。

4.2.3 外部假设始发事件

4.2.3.1 所确定的假设始发事件组应该包括发生在核动力厂外部的可能并会影响对核动力厂安全造成影响的所有事件，包括自然发生的事件和人为引起的事件。这些外部始发事件可能导致内部始发事件，并且可能会导致用于事件保护的某些安全系统设备故障。例如，地震除了能够导致厂外电源丧失外，还会引起核动力厂设备故障。

4.2.3.2 用于安全分析的假设始发事件组，应该包括在选定厂址确实有可能发生的可信的自然事件。这些事件应该包括地震、发生在

核动力厂外部的火灾和洪水（包括由于水坝、河堤或防洪堤坍塌引起的洪水），极端的气象条件（温度、雨、雪、飓风）和火山爆发。

4.2.3.3 用于安全分析的假设始发事件组应该包括选定厂址确实有可能发生可信的人为引起的外部人为事件。这些事件应该包括坠机、附近工厂的影响和运输系统爆炸。

4.3 确定论安全分析

4.3.1　正常运行

4.3.1.1 引言

4.3.1.1.1　正常运行安全分析的目的在于评价：

- 核动力厂能够安全地正常运行，

由此确认：

- 工作人员和公众的辐照剂量在可接受限值内；
- 核动力厂放射性物质的计划释放量在可接受限值内。

4.3.1.1.2　正常运行的安全分析应该涉及针对核动力厂在没有内部或外部灾害时，且系统和设备按预期正常运行时的所有核动力厂工况。这包括核动力厂在整个寿期内处于正常运行和维修过程（包括功率运行和停堆）中的所有运行阶段。

4.3.1.1.3　核动力厂正常运行一般包括如下工况：

- 初首次逼近反应堆临界；
- 反应堆从停堆通过经临界到功率运行的正常启动；
- 包括满功率和低功率在内的功率运行；
- 反应堆功率变化，包括负荷跟踪模式（如果已使用）；

- 从功率运行到停堆；

- 以热备用模式停堆；

- 以冷停堆模式停堆；

- 以换料模式停堆或等效的维修模式停堆，即敞开反应堆冷却剂压力边界的主封盖；

- 以其他模式或在核动力厂具有独特的温度、压力和冷却剂装量的配置下停堆；

- 新燃料和辐照过的过的燃料的装卸和储存。

4.3.1.1.4　安全分析应该评价在核动力厂运行的参数值不超出运行限值时是否能安全地正常运行。

4.3.1.1.5 安全分析应该确定核动力厂安全运行的条件和限制，包括：

- 反应堆保护和控制系统以及其他专设安全系统的安全限值；

- 控制系统的运行限值和参考整定值；

- 运行过程控制的程序限制；

- 确定允许的运行配置。

4.3.1.1.6　正常运行设计的安全评价应该确认正常运行中只有当需要时才发生反应堆停堆或触发安全系统。误停堆和安全系统的误启动一般不利于核动力厂的安全。

4.3.1.2 正常运行时工作人员和公众的辐照剂量

4.3.1.2.1　正常运行的安全分析应该包括对核动力厂总体设计和运行的分析，目的是：预期工作人员和公众可能遭受的辐照剂量；

评价辐照剂量是在可接受的限值内；保证辐照剂量满足合理可行尽量低的原则。

4.3.1.2.2　对于现场工作人员的辐照剂量预期值，应该以其在核动力厂运转和服役中执行规定的具体操作为依据。辐照剂量的预期值既应该包括直接辐射的贡献又应该包括摄入的放射性物质的贡献。分析应该考虑每次活动的持续时间、频率和操作人数。应该估计出最高的个人辐照剂量和小组平均年辐照剂量。

4.3.1.2.3　对于公众，辐照剂量的预期值应该包括直接辐射的贡献和摄入的放射性物质的贡献，以及由核动力厂放射性物质排放结果而通过食物链受到的辐照剂量的贡献。辐照剂量应该对关键居民组进行评估。

4.3.1.2.4　当确定辐照剂量预期值的过程中存在不确定性时，应作采用保守的假设。

4.3.1.2.5　当辐照剂量预期值取决于由放射性物质存量总量累积或由污染水平引起的剂量率时，该预期值应该以核动力厂寿期内可能出现的最大值为依据。

4.3.1.2.6 辐照剂量估计值应该考虑所有相关的运行经验数据。这些数据可以从该核动力厂或类似的核动力厂的运行中推导得到。

4.3.1.2.7　剂量估计值应该与为核动力厂制定的辐射准则进行对比。该准则应该包括法规要求的或监管机构要求的剂量限值。

4.3.1.2.8　应该对剂量估计的结果进行评价，以确定核动力厂运行的所有设计或运行的缺陷或系统的缺陷，并应该对核动力厂进行

合理可行的改进。

4.3.1.3 核动力厂放射性物质的计划排放

4.3.1.3.1　正常运行的安全分析应该包括估计核动力厂放射性物质的计划排放。

4.3.1.3.2　核动力厂放射性物质计划排放的估计应该与为核动力厂制定的辐射准则(包括法规要求或监管机构的要求)进行对比，并且应该对是否符合按合理可行尽量低的原则进行审查。应对核动力厂的设计和运行情况进行评价，并且为了降低计划排放量，还应该对核动力厂进行合理可行的改进。

4.3.2　预计运行事件和设计基准事故

4.3.2.1 设计基准分析中考虑的核动力厂工况包括预计运行事件和设计基准事故。划分是基于事件的发生频率。

4.3.2.2 预计运行事件是比核动力厂正常运行时执行的操作更为复杂的事件，并且可能会影响反应堆安全。预计这些事件至少会在整个核动力厂寿期内预计这些事件会至少发生一次。一般来说，预计运行事件的发生频率大于每堆年１０－２。

4.3.2.3 设计基准事故的发生频率低于预计运行事件的发生频率。设计基准事故在核动力厂寿期内预计不会发生，但是，根据纵深防御原则，他们仍然需要在核动力厂的设计中予以考虑。设计基准事故的发生频率介于每堆年１０－２到１０－５之间，但是，设计基准分析习惯上包括对某些发生频率更低的假设始发事件组的分析。

4.3.2.4 设计基准分析的目的是为工程设计故障容限和安全系

统有效性提供强有力的证明。这种分析是通过考虑了构建模型中不确定性的保守分析来实现的。

4.3.2.5 导致预计运行事件的假设始发事件

4.3.2.5.1 对于多数假设始发事件，控制系统会补偿事件的影响，不会导致反应堆停堆，也不会要求安全系统动作（第二层次纵深防御）。但是，预计运行事件的范畴应该包括所有在核动力厂寿期内所有预计可发生的假设始发事件，并且在纠正其故障后，核动力厂能恢复运行。

4.3.2.5.2 导致预计运行事件的假设始发事件的典型实例可包括以下几类。下列清单有广泛的代表性，具体清单取决于反应堆的类型和核动力厂系统的实际设计：

- 反应堆排热增加：蒸汽卸压阀的误开启；二回路压力控制误动作导致蒸汽流量增加；给水系统误动作导致排热率增加。

- 反应堆排热减少：给水泵跳闸；由于各种原因导致的蒸汽流量减少（如：控制故障、主蒸汽阀关闭、汽轮机跳闸、失去外负荷、失去动力、失去冷凝器真空）导致的蒸汽流量减少。

- 反应堆冷却剂系统流量减少：一台主冷却剂泵跳闸；一个主冷却剂系统环路误隔离（如适用的话）。

- 反应性和功率分布异常：控制棒误抽出；化学和容积控制系统误动作引起的硼稀释（对压水堆而言）；燃料组件装错位。

- 反应堆冷却剂装量增加：化学和容积控制系统误动作。

- 反应堆冷却剂装量减少：仪表管破裂故障引起的非常极小的失

水事故。

- 放射性物质从子系统或部件引起的放射性物质释放：放射性废物系统的少量泄漏。

4.3.2.6 导致设计基准事故的假设始发事件

4.3.2.6.1 应该确定会导致设计基准事故的假设始发事件子集。引发预计运行事件的所有假设始发事件也应该考虑可引发设计基准事故。虽然通常不包括那些发生频率很低的假设始发事件引发设计基准事故，但是任何阈值的确定均应该考虑为该反应堆设置规定的安全目标。

4.3.2.6.2　导致设计基准事故的假设始发事件的典型实例可包括以下几类。下列实例有广泛的代表性，具体清单取决于反应堆的类型和核动力厂系统的实际设计：

- 反应堆排热增加：蒸汽管道破裂；

- 反应堆排热减少：给水管道破裂；

- 反应堆冷却剂系统流量减少：所有主冷却剂泵跳闸；主冷却剂泵卡轴或断轴；

- 反应性和功率分布异常：控制棒失控提升；控制棒弹出；非在役环路的启动导致的硼稀释（对压水堆而言）；

- 反应堆冷却剂装量增加：应急堆芯冷却系统的误运行；

- 反应堆冷却剂装量减少：各种可能的冷却剂丧失事故；主系统卸压阀的误开启；一回路系统冷却剂向二回路系统泄漏；

- 子系统或部件的放射性物质释放：用过的乏燃料在运输或储存

中的过热或损坏；气体或液体废物处理系统的破损。

4.3.2.6.3　应该指出，曾经作为设计基准事故处理的某些事故引发因素可能发生频率低于每年十万分之一。这些事件可能是一些假设始发事件的事例，如按现代标准设计和建造的核动力厂的大破口失水事故等。但是核安全法规仍然要求在设计基准事故的类别内考虑这类假设始发事件。

4.3.2.7 分组

4.3.2.7.1　大量的假设始发事件可以通过上面提供的指导加以确认，并不需要分析所有的假设始发事件。通常的做法是将其分组，对每一组，仅选择极端包络情况进行分析。

4.3.2.7.2　极端包络情况应是那些对已确定的每个主要安全功能给予最严重挑战的事故。在某些情况下，一个事故可能从某一个安全参数角度为最严重（如反应堆冷却系统压力峰值），而另一个事故，则可能从其他一个安全参数角度为最严重（如燃料温度峰值）。在这种情况下，所有这些事故序列在设计过程中均作为极端包络情况处理。

4.3.2.7.3　安全分析应该确认始发事件的分组和极端包络始发事件是可接受的。

4.3.2.8 预计运行事件和设计基准事故分析的目标

4.3.2.8.1　预计运行事件和设计基准事故的分析应该证实安全系统有能力满足以下安全要求：

- 关停闭反应堆并在设计基准事故工况期间及事故其后使反应堆维持在安全停堆状态；

- 在所有运行状态和所有设计基准事故工况停堆后从堆芯排出剩余热量；

- 减少放射性物质释放的可能性，并且保证在核动力厂处于运行状态时任何释放均低于规定限值；在设计基准事故期间，放射性释放低于可接受的限值。

4.3.2.8.2　安全分析应该表明，核动力厂各参数限值和放射性限值均未超出。特别是，应该证实用于防止放射性物质从核动力厂释放的某些或全部屏障将在所要求的程度内维持其完整性。

4.3.2.8.3　安全分析应该确定核动力厂的设计的能力和保护系统的整定值，以保证核动力厂总能维持其基本安全功能。设计基准事件是下列系统设计的设计基础：反应性控制系统、反应堆冷却剂系统、专设安全设施（如应急堆芯冷却系统、安全壳系统、安全壳保护系统），电力系统以及各种安全重要的辅助系统支持系统。

4.3.2.8.4　事件的应有评价事件的充分时间应该足够长，以确定设计基准事件的所有后果。这意味着，核动力厂瞬态的计算应该超出核动力厂停堆及安全冷却系统启动的时刻（即一直达到长期稳定状态为止）。

4.3.2.8.5　对新建的核动力厂和正在接受定期安全评价的核动力厂，应该对其设计基准事件进行全面的确认和评价。对现有核动力厂的修改，评价工作应该着重于受该修改影响的设计基准事件。

4.3.2.8.6　对现有核动力厂进行修改或重新评价时，由于下列原因，可能需要变更对原设计中使用的方法和假设进行修改：

- 原设计基准或验收准则可能不再适合；

- 原设计使用的安全分析工具可能已由更先进的工具所代替；

- 原设计基准可能已不再满足。

4.3.2.8.7　为预计运行事件而进行的安全分析在本实质上相同是与为于事故而进行的安全分析相同。但对于前者，预计运行事件分析时不需要不必具有对设计基准事故分析所具有的全部保守性。例如对预计运行事件进行分析时，不需要假设所有非安全系统和设备均不可用。

4.3.2.8.8　对主要用于防范设计基准事故的安全设备，预计运行事件不应该对其提出任何不必要的挑战。

4.3.2.9 预计运行事件和设计基准事故分析的方法和假设

4.3.2.9.1　方法

4.3.2.9.1.1　预计运行事件和设计基准事故的安全分析应该采用合适的中子物理学、热工水力学、结构和放射学的计算机程序，以便确定反应堆对考虑的运行事件和事故的响应。

4.3.2.9.1.2　应该对用于预计运行事件和设计基准事故分析的计算机程序进行适当地验证和确认。这包括用于计算反应堆堆芯行为的程序和热工水力学的程序，以及用于计算放射性物质释放及其后果的程序。此外，分析人员和程序的使用人员应该具有适当的资格、有经验并和经过培训。

4.3.2.9.1.3　用于对预计运行事件和设计基准事故进行安全分析的计算机程序应该引用从类似的核动力厂获得的运行经验和相

关的实验数据。由于预计运行事件在核动力厂寿期内预计会发生一次或更多，因此，对于这类瞬态，通常已经积累了这类瞬态的一些运行经验和数据。

4.3.2.9.1.4　作为应用基础的计算机程序的模型参数、初始条件和设备可用性假设按惯例是高度保守的，并且所有的分析参数均采用极端保守值。但是，以往的经验表明，这样有时会导致错误的事件序列、不切实际的时序和遗漏某些物理现象。考虑到这些缺陷和目前最佳估算程序的成熟性，在安全分析中，它们应使用最佳估算程序，该与选择合理保守的输入数据和，并充分评估结果的不确定性一起应用。

4.3.2.9.1.5　应用最佳估算程序与初始和边界条件作现实假设相结合的方法也可接受。该方法应该基于在规定的高可信度条件下相应的考虑了核动力厂工况和程序模型的统计组合的不确定性后以规定的高可信度，使计算结果满足验收准则。

4.3.2.9.1.6　安全分析应该遵守适当的质量保证大纲。特别是，数据的所有来源均应该指明出处并形成文件，整个分析过程应该记录并编档保存以便于独立检查。

4.3.2.9.2　假设

4.3.2.9.2.1　为设计基准分析作的典型保守假设典型地应包括如下列假设：

- 始发事件发生在反应堆初始条件最不利的时刻工况（包括功率水平、余热水平、反应性状态以及反应堆冷却剂系统的温度、压力和

装量）最不利的时间；

– 仅当某任一控制系统仅在其执行的功能会加剧始发事件的影响时，才假设其处于运行状态。应认为可减轻始发事件后果的控制系统的运行是不可信的；

– 对于正在作分析的假设始发事件，应假设所有未被指定及维持在安全级别（充分的质量保证、抗震和设备鉴定）的系统和设备都失效，其失效方式应该假设它们会以对被分析的假设始发事件造成最严重影响的方式失效；

– 安全组最严重的单一故障应该假设发生在始发事件要求的安全组投运时。对于多重系统，通常假设最少数量的系列启动并运行；

– 应该假设安全系统在其最低性能水平下运行。对于反应堆停堆和安全系统触发系统，应该假设其动作发生在可能范围的最不利的时刻；

– 对于任何不能认为完全可运行的构筑物、系统或部件不能认为完全可运行的，或那些在事故发生期间达到限值而设计人员并未证明其完全可运行的极限构筑物、系统或部件，均则应该假设它们在事故发生时是其不可用的；

– 只有当仅在确认核动力厂工作人员有足够的时间执行要求的操作、有足够的信息用于事件诊断（考虑始发事件的影响和单一故障准则）、有足够的书面操作规程可供应用以及对核动力厂的工作人员提供了足够的培训时，工作人员为防止或缓解事故时的工作人员操作才可在分析中加以模拟。一般假设在事件发生 10 分钟以后，核动力

厂工作人员才开始进行操作。

4.3.2.9.2.2　所作的保守假设应该考虑反应堆初始条件状态中的不确定性，包括安全系统触发的整定值。

4.3.2.9.2.3　设计基准分析应该包括那些由于作为始发事件的后果而出现的故障（并且因此是假设始发事件的一部分）。这些故障通常包括：

如果始发事件是配电系统某一部分的故障，设计基准事故分析应该假设所有由该部分供电的设备均不可用；

如果始发事件是高能事件，例如导致高温水泄漏或管道甩动的承压系统破损，设计基准事故应该包括会受高能事件影响的设备的故障；

对内部事件（如火灾或水淹）或外部事件（如地震），设计基准事件应该包括所有未设计能承受这些事件影响的也未受到保护的设备的故障。

4.3.2.9.2.4　由于这些假设非常保守，设计基准分析常常提供强有力的证明，在安全限值被超过前存在大的裕度。但是，在应用该分析时必须保持谨慎，因为分析结果并不总是如此。

4.3.2.9.2.5　预计运行事件的安全分析也应该包括许多在确定论设计基准事故分析中所做的保守假设，尤其是在这些瞬态期间用于维持关键安全功能的系统有关的那些假设。但是，没有必要假设所有非安全系统和设备均不可用，也没有必要假设控制系统在减轻始发事件影响中不可信，除非假设始发事件使得这些系统均不可用。

4.3.2.9.2.6　评价的结果应该以适宜的格式书写并呈交，以便很好地了解事件过程，并易于核实是否满足每个验收准则。

4.3.2.9.3　验收准则

4.3.2.9.3.1　应该对《核动力厂设计安全规定》中规定的设计基准范围内的事件和工况制定验收准则。这些准则应该通过防止对放射性物质释放的屏障的损坏和防止放射性物质不可接受的释放，来保证核动力厂维持足够的纵深防御层次。

4.3.2.9.3.2　验收准则应该在如下两个层次内确定：

- 总的/高级别准则：涉及事故中公众遭受的辐照剂量以及防止在事故引起中随之发生的压力边界破损。这些准则由国家核安全监管部门规定。

- 由设计人员或分析人员规定的详细准则：选择这类准则的选择对满足总的验收准则是充分的，但不是必要的。另外，分析人员为了简化分析（如避免作极其复杂的计算），可以在更详细的层次上设置目标（更严的验收准则）。应该明确规定各项具体验收准则适用的范围和条件。

4.3.2.9.3.3　验收准则应该与事故的各种条件（如始发事件的发生频率或反应堆设计及核动力厂工况）有关。一般需要不同的准则为来判断各屏障的薄弱环节和验收事故后果的不同方面一般需要不同的准则。发生频率较高的事件常应用较严格的准则。

4.3.2.9.3.4　因为预计运行事件的发生频率较高，对所为其确定的放射性验收准则一般较为严格。总的来说，验收准则不容许任何

实体屏障失效（燃料基体、燃料包壳、反应堆冷却剂压力边界或安全壳）和燃料损伤（或者如果已经存在运行限值内的燃料轻微泄漏，则要求没有额外的燃料损伤）。

4.3.2.9.3.5　对设计基准事故的总的验收准则应该是无厂区外不会有放射性影响，或者在仅仅在隔离区外仅仅有轻微的放射性影响。轻微放射性影响的定义应该由国家核安全监管部门给出，但一般与非常严格的剂量限值一致，以便不需要厂外应急行动措施。

4.3.2.9.3.6　详细的验收准则应该包括如下一些考虑：

- 如果一个事件在没有不出现另外一个独立的故障发生时，则不应该产生相继发生后续更加严峻的核动力厂工况。因此一个预计运行事件不应该由其本身引发设计基准事故，并且这一事故不应该由其本身引发超设计基准事故；

- 一个事故不应该导致其后需要用来减轻其后果的安全系统功能的随之丧失；

- 用于事故缓解的系统应该设计成能够承受所分析事故产生的最大载荷、应力和环境条件状况。这应该由涵盖环境条件状况（如温度、湿度或化学环境）及核动力厂构筑物和部件所受热载荷和机械载荷的单独分析来评价；

- 对于现有的核动力厂工况，一回路和二回路的压力不应该超过相关设计限值。为研究安全阀和卸压阀失效的影响，可能需要进行额外的超压分析；

- 为满足总的放射性准则，对每一种类型的假设始发事件，都应

该确定为满足总的放射性准则允许燃料包壳发生的破损的数量；

- 在伴有燃料裸露和升温的冷却剂丧失事故中，应该维持燃料棒可冷却的几何形状和结构的完整性；

- 任何事件都不应该引起安全壳内的温度、压力及压差超过安全壳设计基准值。

4.3.3　超设计基准事故和严重事故的考虑

4.3.3.1 引言

4.3.3.1.1　比设计基准事故更加严重的事故称之为超设计基准事故，这些事故能够导致以下后果：

- 其结后果仍然在为设计基准事故规定的保守验收准则范围内，不过对于这种情况，虽然这需要用最佳估算分析予以证实；

- 其结后果超过了为设计基准事故规定的保守验收准则范围，但是根据最佳估算分析，表明不会导致严重的燃料损伤，或不会超过一回路破损限值；

- 由于多项故障和/或运行人员差错，安全系统一个或多个安全功能未能执行，导致堆芯严重损坏，危及防止放射性物质从核动力厂释放的其余屏障的完整性。这些事故称作严重事故。严重事故可能继续升级，从而导致：

⑴堆芯损坏加上一回路破损，但安全壳未失效；

⑵堆芯损坏加上一回路破损，并且安全壳也失效，导致放射性物质大量释放到环境中，并动用厂外应急响应措施。

4.3.3.1.2　安全分析应该致力于量化核动力厂的安全裕度，并

证实为这类事故提供了某种程度的纵深防御的程度。这包括如下一些合理可行的措施：

- 通过设置附加设备和事故管理程序，来防止事故升级为严重事故，控制严重事故的进一步发展和限制放射性物质的释放；

- 通过厂内厂外应急响应计划的措施，来减轻可能发产生的放射性后果。

对于那类假设的会导致安全壳早期失效的严重事故序列（如发生在压水堆中的高压堆芯熔化事故），应该证实有很高的可信度可以避免发生那类假设的会导致安全壳早期失效的严重事故序列（如发生在压水堆中的高压堆芯熔化事故）。

4.3.3.2 安全分析中严重事故的选择

4.3.3.2.1 严重事故分析应该提出安全系统已丧失功能计及一组有代表性的序列，在这些序列中安全系统出现了故障，并且一些防止放射性物质释放的屏障已失效或被旁路的一组有代表性的序列。这些序列应这样选择：加入额外的故障或操纵员的不正确响应到在设计基准事故序列中（包括安全系统故障）和到概率安全分析的主导事故序列中加入额外的故障或操纵员的不正确响应。

4.3.3.2.2 会导致严重事故的重要事件序列应该运用概率论和确定论方法以及与正确的工程判断相结合的方法，来确定那些会导致严重事故的重要事件序列。

4.3.3.2.3 确定严重事故序列的最严格的方法是应用一级概率安全分析（见 4.4.1.1.2）的结果。但是，也可以通过了解严重事故

序列所包括的物理现象、设计中存在的裕度和保留在设计基准事故中的系统多重度来确定代表性的或极端包络的序列。

4.3.3.2.4　引发严重事故的例子如下：

- 完全丧失堆芯余热排出；

- 冷却剂丧失事故伴随着应急堆芯冷却系统完全失效；

- 长时间完全失去电力供应。

4.3.3.2.5　需要进行分析的严重事故序列的细节随反应堆安全系统的设计会有所不同。

4.3.3.2.6 严重事故的评价应该考虑核动力厂的所有设计功能，包括利用超出某些安全系统和非安全系统原设计意图的功能将潜在的严重事故恢复到可控状态和/或者减轻其后果。如果这些系统的超常使用是可信的，则应该有能在分析中予以使用的假设依据了一个合理的依据来假定它们能够并将象分析所要求的那样被使用。

4.3.3.3 严重事故分析的方法和假设

4.3.3.3.1　对于严重事故分析，一般应该采用最佳的估算假设、数据、方法和决策准则。如果这不可能，应该作出合理的保守假设，以考虑对被模拟的物理过程理解的不确定性。

4.3.3.3.2　严重事故分析应该模拟在堆芯损坏以后可能发生和的以及可能导致放射性物质释放到环境中的广泛的宽范围物理过程，这些物理过程应包括（适用时）：

- 堆芯性能恶化过程及燃料熔化；

- 燃料和冷却剂的相互作用（包括蒸汽爆炸）；

- 压力容器内熔融物滞留；

- 压力容器熔穿；

- 一回路内的热分布；

- 熔融物的高压喷射或对安全壳的直接加热；

- 氢气的产生和燃烧；

- 安全壳损坏或旁路；

- 堆芯熔融物与安全壳底板混凝土的相互作用；

- 裂变产物的释放和迁移；

- 对压力容器内外堆芯熔融物的冷却能力；

4.3.3.3.3　严重事故分析通常使用不同程序的多层次方法（包括详细的系统和安全壳分析程序、较简化的风险估算程序和“单个效应”程序以及对源项和辐射影响的研究）。使用全部的程序将保证所有的预期现象均得到充分的分析。

4.3.3.3.4　评价应该保证反应堆堆芯、一回路和安全壳均被准确地模拟。这些模型对分析是极其重要的，并且将影响事故过程的确定。

4.3.3.4 验收准则

4.3.3.4.1　严重事故的验收准则通常以概率安全准则和确定论验收准则的形式表述。概率安全准则将在 4.4.7.1-4.4.7.2 中讨论。

4.3.3.4.2　确定论验收准则通常包括：

- 在严重事故发生后短期内不应该发生安全壳失效；

- 在严重事故发生后不应该有短期的健康效应；

- 严重事故后 Cs-137 的长期健康效应/释放应该低于规定的限值。

4.3.3.5 设计中对严重事故的考虑

4.3.3.5.1　严重事故分析的目的应该是：

-评价设计抵御严重事故的能力，并且确定设计的具体薄弱环节。这包括对评定用于事故管理的设备的评定和对监测事故过程的仪表的评定；

- 评价是否需要在核动力厂设计 中加入对严重事故提供纵深防御的设施；

- 确定用于减轻事故后果的事故管理措施；

- 制定用于超设计基准事故和严重事故的事故管理大纲；

- 为厂外应急计划提供输入。

4.3.3.5.2　在新建核动力厂的设计阶段就应考虑严重事故。但是，对正在运行的核动力厂，应制定严重事故管理大纲，以便可充分利用所有可用设备和规程来减轻事故的后果。这些措施可以包括使用备用的或多样的系统、规程和采用非安全级设备的方法，也可以使用外部设备临时代替原来的部件。

4.3.3.5.3　上述设计特性和事故管理措施在降低风险方面的有效性应该由概率安全分析予以评价。

4.3.3.6 应急计划

4.3.3.6.1　严重事故分析还应该为国家权力机构应急主管部门制定厂外应急计划和响应提供输入。

4.3.3.6.2　严重事故分析的结果应该用来确定源项，该源项可用于制定厂外应急计划。

4.3.3.6.3　源项也可以用于论证隐蔽、服用碘化钾片、食物禁令和撤离的有效性。

4.4 概率安全分析

4.4.1　引言

4.4.1.1 概述

4.4.1.1.1　概率安全分析提供一种综合的结构型分析方法，用来确认事故情景和导出风险的数值估计。核动力厂的概率安全分析通常进行可在如下三个级别上进行分析。

4.4.1.1.2　一级概率安全分析：确定导致堆芯损坏的事件序列，预估堆芯损坏频度，深入了解用于防止堆芯损坏的安全系统和规程的能力和不足。

4.4.1.1.3　二级概率安全分析：确定放射性物质从核动力厂释放的可能途径，并且预估其释放量和发生频度。该分析有助于深入了解事故预防和事故缓解措施(如反应堆安全壳的使用)的相对重要性。

4.4.1.1.4　三级概率安全分析：评估对公众健康的影响和其他社会风险，如对土壤和食物的污染。

4.4.1.2 概率安全分析是决策过程的组成部分

4.4.1.2.1　作为设计过程组成部分的概率安全分析的结果应该用于评价核动力厂的安全水平。核动力厂的安全决策既应该考虑确定论分析的结果，也应该考虑概率安全分析的结果。这应该是一个反复

迭代的过程，目的在于保证核动力厂满足国家的核安全要求和准则，并且其设计是平衡的（见 4.4.1.3.6），风险是合理可行尽量低的。

4.4.1.2.2　概率安全分析的结果应该用于确定识别核动力厂设计和运行中的薄弱环节不足。为了确定识别这些薄弱环节不足，需要考虑各组始发事件和安全系统重要程度对风险的贡献、以及人为差错人员差错对总风险的贡献。当如果概率安全分析的结果表明对修改核动力厂的设计或运行进行某些修改可以使降低其风险降低时，则在考虑该修改的相关代价和利益后，只要合理可行就应进行相关修改。

4.4.1.2.3　概率安全分析的结果应该与为核动力厂制定的概率安全准则（如果有）进行对比。核动力厂概率安全准则包括关于系统可靠性、堆芯损坏、放射性物质释放、工作人员和公众健康的效应及厂外后果（如土地污染和食物禁令）的准则等。

4.4.1.2.4　概率安全分析的结果应该用于制定应急运行规程，并且为核动力厂的技术规格书提供输入。特别是，概率安全分析的结果应该用于研究由于试验和维修使设备停役对风险的贡献，以及监督和/或试验频度的合适性。概率安全分析应该确认设备允许的停役时间不会导致风险过度增加，并且指出应该避免的同时停役的设备组合。

4.4.1.2.5　二级概率安全分析的结果应该用于决定是否已采取足够的措施以减轻一旦发生堆芯损坏所产生的各种后果。这将涉及安全壳是否足够坚固以及安全系统（如氢气混合/复合系统、安全壳喷淋系统和安全壳泄压系统）是否提供足够水平的保护，以能充分防止放射性物质向环境大量释放。此外，二级概率安全分析还应该用于确

定事故管理措施，这些措施主要用于减轻熔融堆芯的影响。这可能还包括确定可能采取向安全壳的反应堆腔室安全壳内注水的额外措施等。

4.4.1.2.6　如果可能的话，二级和三级概率安全分析的结果应该提交供给国家权力机构应急主管部门，作为其制定厂外应急计划条款的技术输入。

4.4.1.3 概率安全分析的要求

4.4.1.3.1　核动力厂的整个设计和运行期间均应该采用概率安全分析，以有助于涉及核动力厂安全的决策过程。

4.4.1.3.2　对于新建的核动力厂，概率安全分析最好在概念设计阶段开始进行，以便检验在安全系统中具有足够的多重性和多样性，并应该在更加详细的设计阶段继续进行，以便评价更加详细的设计问题，概率安全分析还用来支持核动力厂的运行。在设计阶段，应有一个迭代过程，以保证从概率安全分析得出的结论反馈到设计过程。

4.4.1.3.3　对于现有的核动力厂，应进行概率安全分析，既可作为定期安全评价的一部分，又可作为建议提出修改的安全论证的支持。尽管对不同阶段的概率安全分析的要求仍然是一样的，但数据库可能以不同。此外，由基于设施使用的期限、剩余的运行寿期、建议提出修改的费用和其他相关的考虑，为减轻风险所采取的修改将有所不同。

4.4.1.3.4　概率安全分析应该明确地以核动力厂实际的或预想的设计或运行作为分析的起始点。核动力厂的状态可以定在过去某个

具体日期时的届时状态或定在将来完成已同意的修改的届时的状态。

4.4.1.3.5　概率安全分析应该着手于：确定对风险有贡献的所有故障序列；确定核动力厂设计和运行中是否存在薄弱环节；并且评价是否需要对这些薄弱环节进行加强以便降低其对安全的重大影响。当分析没有计及所有对风险的贡献因素时（例如，可能忽略了外部事件或停堆状态），其所作出的结论（如核动力厂的风险水平、安全系统之间的平衡性以及为降低风险需要对核动力厂的设计和运行进行变更等）可能是不正确的。

4.4.1.3.6　概率安全分析应该确定安全系统是否具有足够的多重性和多样性，核动力厂是否具有足够的纵深防御，以及核动力厂整体设计是否平衡等。在平衡的设计中概率安全分析应该表明：

- 不存在对风险会造成不成比例的高贡献的特定的设计；

- 不存在对风险会造成不成比例的高贡献的始发事件组；

- 核动力厂达到的总的低风险不取决于相当大的不确定性的贡献；

- 防御的前两个层次起到了安全的主要作用；

- 在每一个防御层次内，没有一个安全系统比其他的安全系统具有不相称的较大的重要性度。

缺乏平衡的设计通常意味着还存在合理可行的降低风险的可能。

4.4.1.4 概率安全分析的范围

4.4.1.4.1　概率安全分析应该涉及在所有运行模式中所产生的对风险的贡献。但是，通常方便的做法是对核动力厂功率运行和停堆

模式分别进行分析。

4.4.1.4.2　如果只完成进行一级概率安全分析，则根据定义，反应堆堆芯便是分析的焦点。如果完成二级或三级概率安全分析，概率安全分析的其范围可能可包括由厂区其他放射性物质来源引起的对风险的贡献，例如用过的乏燃料及放射性废物。每当要确定核动力厂对厂区附近个人带来的总风险时，还应该包括这些堆芯外的来放射性源。

4.4.1.4.3　概率安全分析应该以完整的假设始发事件组（包括外部假设始发事件和内部假设始发事件）作为其分析起点。分析应该确定对风险有贡献的所有故障序列。这些故障序列应该计及部件故障、在维护和试验期间部件不可用、人为差错人员差错以及共因故障等，如果可能，还应该计及部件的老化。

4.4.1.5 概率安全分析方法

4.4.1.5.1　迄今为止，已经对各类核动力厂设计进行了大量的概率安全分析，因此，概率安全分析（尤其是一级概率安全分析）的方法也得到了良好的发展。但是必须认识到，概率安全分析过程中存在着固有的不确定性。这些不确定性不只存在于概率安全分析中，同样也存在于确定论安全分析中。但是，概率安全分析方法能够认识说明和量化其大部分不确定性中的大部分。对任何将要进行的新的概率安全分析，其方法均应该和当时国际上最佳实践保持一致。

4.4.1.5.2　概率安全分析应该始终尽量使用最佳的估算方法。这些估算方法包括支持安全系统成功准则进行的分析，对堆芯损坏后

安全壳内出现的现象进行的模拟，以及释放到环境中放射性物质的迁移分析。当这些不可能做到时，应该采用合理的保守假设。

4.4.2　一级概率安全分析：堆芯损坏频率分析

4.4.2.1 引言

4.4.2.1.1　一级概率安全分析的目的应该是确定堆芯损坏总的频率。这要求对构成明确定义堆芯损坏的明确定义，并要求将该定义转化为安全系统故障准则。一级概率安全分析应该确定对堆芯损坏频率贡献最大的故障序列和确定防止堆芯损坏起最重要作用的安全系统，并决定是否能由核动力厂设计和运行的修改来降低风险。

4.4.2.2 假设始发事件

4.4.2.2.1　概率安全分析的起始点应该是能直接导致或者与其他故障一起危及核动力厂安全的整个假设始发事件清单。在确定论安全分析中包含的继发性故障，在概率安全分析中同样应该在事件序列分析和系统分析中予以考虑。

4.4.2.2.2　所确定的这套假设始发事件组应该包括所有的内部事件和外部事件，并且应该包括在核动力厂设计阶段未曾考虑的发生低频率低而可能发生的事件。

4.4.2.2.3　概率安全分析应该包括所有核动力厂运行模式下可能发生的以及可能导致从厂区任何源释放放射性物质的假设始发事件。

4.4.2.3 安全系统要求的技术规格

4.4.2.3.1　对于确定的每一个假设始发事件，都应该确定为防

止堆芯损坏所需执行的安全功能。这些安全功能和设计基准分析中提到的一样，即对始发事件的探测、停堆、余热排出和安全壳防护。但是，考虑安全功能失效的限值将采用现实的限值，而不是设计基准分析中确定的保守限值。

4.4.2.3.2 应该规确定为执行这些安全功能所需要的安全系统。这应该基于最佳估计的瞬态分析，而不基于为设计基准分析所作的保守分析。还应该规定需要运行要求的多重系统及多样系统的系列数量应予以确定。

4.4.2.3.3 可以先识别出用所需要相同的或非常类似的安全系统动作的那些来确定假设始发事件的分组。为减少分析的数量，在概率安全分析中通常对这些假设始发事件进行分组，并一起分析，以减少分析的数量。始发事件组由具有最苛求的安全系统响应的始发事件作为代表，事件组中单个始发事件发生频率的总之和作为该事件组的发生频率。如果对假设始发事件进行分组的方法不应给分析带来不可接受的水平。比例如，当所选择的代表性事件的发生频率低，而组内所有其他事件对安全系统动作要求的苛刻程度远不及该事件，但是发生频率的总和却大得多远大于该事件。

4.4.2.4 事件序列分析

4.4.2.4.1 在事件序列的分析中，为始发事件组构造逻辑模型，以便确定可能导致堆芯损坏的故障序列。这些逻辑模型以基本安全功能为起点，并且考虑始发事件组要求的安全功能、安全系统和安全系统内的中单个部件以及人员响应。这些逻辑模型确定部件的故障如何

组合会能导致安全功能丧失和堆芯损坏。

4.4.2.4.2　对始发事件组进行的事件序列分析的目的是识别出安全系统设备所有会导致核动力厂不能保持在安全限值内而发生堆芯损坏的成功的或失效的组合。

4.4.2.4.3　在目前大多数概率安全分析中，事件序列的分析都是以事件树和故障树相组合的形式进行分析，因为经验证明，这是处理核动力厂所要求的大的逻辑模型最有效的方式。但是，单独使用事件树或故障树进行事件序列分析也是可能的，并且在特殊事件分析中，还可以使用时间相关的动态分析方法技术。

4.4.2.4.4　应该进行系统评价，以便确定哪些安全系统设备（包括其故障可能影响到该事件序列的那些安全相关或非安全相关的设备）故障可能以始发事件后果的形式出现发生；这些故障应该包含在表示可能发生的事件序列的逻辑模型中。

4.4.2.4.5　事件序列分析应该包括为能够可运行的执行所要求安全功能能够运行的安全系统设备的所有组合。

4.4.2.4.6　由于核动力厂中的某些安全系统共享公用触发系统或公用辅助系统支持系统，如电力系统、控制和仪表设备及冷却系统等，这就导致安全系统之间具有存在功能的相关性。对核动力厂设计和运行应该进行系统的评价，以保证在进行事件序列分析或系统分析时，对所有这些相关性均得到鉴别和清晰地模拟所有这些相关性。

4.4.2.5 安全系统故障分析

4.4.2.5.1　事件序列分析应该向下延伸到单个底事件的层次水

平。这些底事件通常包括部件故障、维护和试验期间部件不可用性、多重设备的共因故障以及运行人员差错等。

4.4.2.5.2　系统故障分析应该涉及安全系统设备单个部件所有的相关故障模式。这些故障模式通常已由作为设计评价一部分的故障模式和效应分析确定。系统模型中也应该包括假设始发事件引起的任何继发故障（如果这些故障没有在事件序列模型中充分考虑）。

4.4.2.5.3　所有必要的辅助系统支持系统均应该予以确定，并且包括在系统故障分析中，同时在逻辑模型中应清晰地表述由共用辅助系统支持系统引起的系统之间的相关性。

4.4.2.5.4　在核动力厂寿期内，单个物项或设备系列可能由于试验、维护或修理而停役，这将降低执行安全功能的安全系统的可用性。概率安全分析应该充分考虑这些设备的停役运问题。这可以通过在逻辑模型中引入底事件以反映设备停运问题，也可以通过或进行多次的概率安全分析。

4.4.2.6 数据

4.4.2.6.1　为了定量分析，需要以下具体数据：

- 始发事件频率；
- 设备故障概率；
- 设备停役用频率及停役用时间；
- 共因故障概率；
- 人为差错人员差错概率。

4.4.2.6.2　所采用的始发事件频率和设备故障概率应适用于核

动力厂的设计或运行。如果可能，应该使用核动力厂的专用数据。当这不可能时，应采用类似核动力厂的运行数据。如果这也不可能，只好采用通用的相关数据。对于发生频率低的始发事件，应该作出判断。

4.4.2.6.3　在确定设备故障率时，应该明确指出设备的边界，并应该包括所有相关的故障模式。例如一台泵，这应该包括启动失效、在规定投运时限内失效以及泵密封发生泄漏。

4.4.2.6.4　使用的统计数据应该包括始发事件的所有相关起因以及所有相关的设备的故障模式。

4.4.2.6.5　对于概率安全分析中涉及的某些方面，尤其是对某些极少发生频率极低的始发事件（如压力容器破损或严重的地震灾害）的频率，没有相关运行经验。如果认为这些事件对风险的贡献不重要，只要给出正当理由，则可把它们排除。否则，仍然需要对其发生频率进行判断，并且应该给出该判断的依据。特别是，用于地震灾害概率评价的方法已经得到了良好的发展，并可用于任何厂址。

4.4.2.7 共因故障

4.4.2.7.1　对于某一安全系统内设备的多重物项，有由存在共因引起故障的可能性，这限制约了系统的可靠性。在分析中这些共因故障在安全系统的层次上或在单个部件的层次进行模拟。一种做法是在表示系统共因故障的逻辑模型中通过引入底事件来模拟共因故障。目前有很多方法可以评价共因故障的发生概率，评价的方法包括使用运行经验数据以及使用诸如β因子及多希腊字母的理论模型等。

4.4.2.7.2　在分析中，应该对可能发生在多重安全系统中的共

因故障进行模拟，并且应该证明概率安全分析中所使用的共因故障模型及数据的合理性。只要可能，都应该对类似系统的运行经验予以考虑。

4.4.2.7.3　以往的分析和运行经验表明，非多样性安全系统对每次需求的故障概率将介于约千分之一到十万分之一的范围内，这取决于系统的多重性以及其他设计和运行因素。这也应该在分析中反映。

4.4.2.8 人因可靠性分析

4.4.2.8.1　人为差错人员差错可能影响一个事件序列的起因和发生频率。人为差错人员差错可能发生在事件序列开始之前、其间中或其后，既能缓解事故，也能使事故恶化事故，在概率安全分析中应该模拟人为差错人员差错这些情况。有关人因可靠性的数据应该由从以下来源导出，如事件报告、维修报告、各种概率安全分析报告以及模拟机中得到的观察资料等。

4.4.2.8.2　应该确定可能导致始发事件的人为差错人员差错，并且应该作为始发事件发生频率的一部分。

4.4.2.8.3　应该在事件序列和安全系统故障分析中，清晰地模拟可能导致安全系统故障和丧失关键安全功能的人为差错人员差错。

4.4.2.8.4　采用的人为差错人员差错概率应该反映能够会影响操纵员行为的因素，包括承受的压力、完成任务的可用时间、运行规程的可用性、培训水平和环境条件等。这些应由作为设计评价组成部分的任务分析来确定。

4.4.2.9 定量分析

4.4.2.9.1　建立的逻辑模型应该利用数据进行定量分析，以便确定堆芯总的损坏频率以及各始发事件组的贡献。

4.4.2.9.2　在定量分析中，应该得出始发事件组、部件故障、安全系统故障和运行人员差错的重要度，以便确定对风险有贡献因素的来源以及安全系统设计和运行中可能存在的薄弱环节缺陷。如果适用时，可采用重要度的定量度量。如果在模型和数据中存在的不确定性，则应该由敏感性分析来加予以支持。

4.4.2.10　堆芯损坏频率的分析结果

4.4.2.10.1 应该对分析结果进行评价，以便确信该分析结果充分反映了核动力厂风险。若判定在某些方面风险评估是过分保守或过分乐观时，则应对分析进行修正，以使得分析结果更真实。当如果安全系统成功准则是基于保守的设计基准瞬态分析和保守的重要安全功能成功准则，而不是基于为概率安全分析推荐的最佳评估时，可能出现则分析结果会过分的保守。若不适当地的筛选掉潜在始发事件，则可能出现过分乐观的结果。

4.4.2.10.2 分析结果应该与对核动力厂建议的堆芯损坏频率安全准则进行对比。若评估的堆芯损坏频率高得不可接受时，则应该对核动力厂的设计和运行进行修改以降低风险。

4.4.2.10.3 即使堆芯损坏频率已低得可以接受，也还应该系统地审查概率安全分析的结果，以便确定核动力厂设计和运行中相对薄弱的环节和确定为降低堆芯损坏频率可做的改进。只要合理可行就应实施这些修改。判断什么是合理可行将取决于反应堆是处于设计阶段

还是处于运行中，以及修改的费用。在核动力厂设计阶段将不断重复这个过程，以使得堆芯损坏频率降到或低于设计目标值，以并得到平衡的设计。

4.4.3　二级概率安全分析：从堆芯损坏到放射性物质释放的事故进程分析

4.4.3.1 引言

4.4.3.1.1 这部分的分析考虑从堆芯损坏开始的事故进展过程，并考虑可能发生和会导致安全壳失效以及放射性物质向环境释放的某些现象。

4.4.3.1.2　分析考虑核动力厂设计以及为减轻堆芯损坏影响所提供设计制定的和事故管理措施的有效性，并提供估计发生放射性物质向环境大量释放的频率的估计，此频率可以和概率论安全准则进行对比。

4.4.3.2 核动力厂损坏状态的定义

4.4.3.2.1　应该对在一级概率安全分析中确定的会导致堆芯损坏的故障序列按核动力厂损坏状态分组，此状态是依据会影响安全壳响应或放射性物质向环境释放的诸多因素定义的。这些因素通常包括所发生始发事件的类型、反应堆冷却剂系统压力、应急堆芯冷却系统和安全壳保护系统的状态以及安全壳的完整性等。

4.4.3.3 堆芯损坏进程的模拟

4.4.3.3.1　对于从堆芯损坏至放射性物质释放的事故进程分析应该模拟影响安全壳完整性的或影响放射性物质释放的重要现象（见

4.3.32.3.2)。

4.4.3.3.2　分析应该使用逻辑方法模拟事件序列如何从堆芯损坏进展到放射性物质释放的事件序列进程。通常的做法是进行事件树分析。事件树分析是在以多个时间段的方式来构架内模拟事故序列，并使用一套（事件树）节点询问题模拟发生的事件的序列。构筑事件树需要由热工水力学计算以及模拟裂变产物在安全壳内释放和迁移模型来支持。

4.4.3.3.3　事件树分析应该包含具有足够数量的时间段构架和节点以便能够涉及处理安全壳内可能发生的所有重要现象。为核动力对每个核动力厂所有每种损坏状态，其构筑的事件树将使用同样的节点询问问题是相同的。但是，由于由核动力厂损坏状态表征的初始条件的不同，对每一个确定状态实际事件树在细节上对每一个确定状态并不完全相同。

4.4.3.3.4　事件树的终端终止状态确定已经发生的事件序列及安全壳的状态。安全壳可能完好无损或已经失效。其可能的故障失效模式是：旁路、隔离失效（这两种失效模式在核动力厂损坏状态定义中均已模拟）、泄漏、破裂或底板熔穿等。放射性物质的释放也还取决于在该事故序列中，安全壳失效是发生在事故序列的早期或还是晚期。

4.4.3.4 数据

4.4.3.4.1 事件树定量分析的相关数据是各分支点的条件概率。由于可能发生的现象具有相当程度的不确定性，其结果通常使用基于

专家判断的概率。

4.4.3.4.2　评价工作应该确认专家判断的体制是健全的，判断的依据是阐明的及已予说明并已尽可能证明是正确的。这评价应该考虑已经完成的热工水力分析、其他类似核动力厂的分析以及适用的研究数据。安全壳事件树的量化应该考虑被模拟的各种现象之间的相关性。

4.4.3.5 安全壳性能分析

4.4.3.5.1　需要涉及的重要问题之一是由于堆芯损坏引起安全壳在所承受载荷下的行为和安全壳如何发生失效。

4.4.3.5.2　在分析中应该涉及安全壳直接旁路（例如，由于蒸汽发生器传热管破裂或冷却剂排到接口系统在安全壳外的接口系统的失水冷却剂丧失事故出现冷却剂丧失事故）和安全壳隔离系统的故障。这通常包含在核动力厂损坏状态的定义中。

4.4.3.5.3　应该进行结构分析，以决确定由于蒸汽爆炸、不可凝气体或氢气燃烧可能引起的压力和温度条件下的安全壳的行为。该分析应该基于安全壳的实际设计，要考虑到闸门、贯穿件、密封和其他可能的薄弱区域。应该确定安全壳可能的失效模式，并应该评估作为压力和温度的函数的安全壳失效的条件概率。然后该信息可用来估计用于量化事件树的条件故障概率。

4.4.3.5.4　分析还应该确定在压力容器失效后，熔融堆芯与混凝土在压力容器失效后相互作用的结果如何导致安全壳底板将如何失效。，应该估计作为余热水平和熔融物质可得到的冷却的函数的底

板失效的条件概率。当如果安全壳底板上面有附加间分隔空间，时则应该特别注意，底板熔穿可能导致放射性物质经非过滤路径释放。

4.4.3.6 源项分析

4.4.3.6.1 在事件树分析中通常会有大量序列的终止状态终端，并且这些终端终止状态一般按具有类似放射性特征和厂外后果的释放和/或源项类别型进行分组。

4.4.3.6.2 确定释放类别型应该包括以下因素子，如所包含的每种同位核素的数量、出现时间、持续时间、位置地点、能量范围和颗粒大小的分布等。

4.4.3.6.3 对所确定的每项释放类别型都应该规确定其源项。这应该考虑影响源项的各种因素，包括放射性核素的挥发性、从燃料的释放、反应堆冷却剂系统内裂变产物的滞留和安全壳内裂变产物的滞留等。

4.4.3.6.4 每类释放的频率应该由汇总对是分配给各该类事件树中给定的该类每个终端终止状态的的所有频率之和来计算。当概率安全分析的范围包括厂区内所有放射性物质源项的释放时，则由堆芯外源项的释放应该计入该终端该终止状态。这可以包括确定的会涉及附加释放类别型的定义，其它们的厂外放射性影响较低但频率比由堆芯损坏的释放频率高。

4.4.3.7 二级概率安全分析的结果

4.4.3.7.1 二级概率安全分析的结果通常以源项类别型或释放类别型与各自的发生频率的表格形式给出。源项类别型或释放类别型

由各自的放射性核素成分（按其共同的化学及物理特性分为不同的裂变产物组）与相关释放特征（事故发生后释放发生的时间、持续时间、释放点高度及能量范围等）来确定。由从此信息能推导得出大量释放或早期大量释放的发生频率，以便与概率论安全准则中的数值进行对比较。“大量”指的是其数值大于某一规定的放射性物质的量，该规定量通常以堆芯放射性总量的份额形式给出。

4.4.3.7.2　与概率安全分析的其他部分一样，二级分析结果应该用于确定风险的主要贡献因素以及为降低风险在核动力厂的设计和运行方面能够做哪些修改。这应该考虑到二级概率安全分析中固有的重要现象不确定性。这些改进措施可能包括氢气控制系统（此系统具有足够处理堆芯损坏后的按一定速率产生氢气的能力）、安全壳过滤排气系统（可以在较长期间内防止安全壳超压）或用于熔融堆芯冷却的专用系统等。在考虑代价和利益后，当认为这样做是合理可行时，应将这些改进纳入到核动力厂的设计中。

4.4.3.8 厂内事故管理

4.4.3.8.1　在事故期间，运行人员可以采取行动，以防阻止事故进发展一步恶化或降低其影响。分析中经常包括的该这样一种事故管理措施的例子是，例如开启卸压阀以降低一回路压力并且防止熔融物质在高压下从反应堆压力容器在高压下向外喷射熔融物质，以及在堆芯熔融物从一回路流出后往安全壳内注水，以提供冷却介质。

4.4.3.8.2　二级概率安全分析应该用于确定哪些事故管理措施可以用于缓解熔融堆芯的影响。这些措施应该包括那些能对安全壳功

能有所支持的和那些可以抑制可能发生的放射性物质释放的措施。这些事故管理措施应该纳入到核动力厂事故管理大纲中，并且还应该对负责执行这些事故管理措施的运行人员进行培训。严重事故管理措施应该与核动力厂运行人员能够在该情况下合理使用的设备、仪表及诊断手段相适应。

4.4.4　三级概率安全分析：厂外后果分析

4.4.4.1 引言

4.4.4.1.1　厂外后果分析要模拟核动力厂放射性核素的释放，释放的放射性核素向环境的迁移，以及其对公众健康及经济的影响等。分析应该：(1). 提供生活在核动力厂附近居民的个人死亡风险评估；(2). 指给出一系列的厂外后果影响，包括对公众成员造成的早期和晚期健康影响；(3). 考虑其他经济后果影响。

4.4.4.2 源项分组

4.4.4.2.1　正如 4.4.3.6.1-4.4.3.7.1 中讨论，对于二级概率安全分析中确定的故障序列通常归类成于释放类别，该类别在影响大气弥散和厂外后果方面具有类似特征的释放类型。定义的一系列释放类别组型应该代表可能发生的从核动力厂发生的释放放射性物质释放的各种情况。确定这些释放类别型通常以释放的放射性核素成分的挥发性来分类。此外，释放类别型还应该确定从始发事件出现直到发生释放所经历的时间以及释放的持续时间，因为这些均和厂外应急计划制定有关。释放类别型的发生频率应该是该释放类别型包含的所有安全壳事件树终端终止状态的频率总和。

4.4.4.3 大气弥散模型

4.4.4.3.1 为进行厂外后果分析，需要输入关于核动力厂及厂址的专用数据，包括核动力厂的释放类别型和频率，该厂区及周边的气象、人口、农业和经济数据等。程序模拟放射性核素在环境中的迁移情况，包括大气弥散、沉积、再悬浮、食物链途径和照射途径（如烟云照射、吸入、污染、地面沉积、再悬浮和摄入等）以决确定对公众健康和厂外经济的后果。

4.4.4.4 气象数据

4.4.4.4.1 应该确定核动力厂厂址的气象数据。这些气象数据应该以该厂址附近连续多年搜集的数据为依据，通常包括风向、风速、稳定度类型、降雨量以及混合层深度度高度等（准确的数据通常取决于所用的计算机程序）。

4.4.4.5 人口、农业和经济数据

4.4.4.5.1 应该确定核动力厂厂址的人口、农业和经济数据。这些数据通常依据由对国家资料以及该厂址附近的区域调查所补充的国家的资料。必要的数据将取决于在分析中所包含的对公众健康影响效应和经济因素的选取。分析过程中如何准备数据取决于所采用的计算机程序的具体需要。

4.4.4.6 社会风险评估的结果

4.4.4.6.1 社会风险评估的结果应该与风险准则（为该核动力厂确定的风险准则）进行对比。

4.4.4.6.2 应该将社会风险评估的结果提供给国家权力机构应

急主管部门，作为其制定厂外应急计划决策过程的技术输入。

4.4.4.7 厂外应急计划

4.4.4.7.1　为应急计划和准备是指为防止工作人员和公众受到核动力厂放射性物质释放的影响，应急计划和准备涉及到而在核动力厂厂区内外可能进行的各项活动。可行的话，应该使用三级概率安全分析对这些防护策略进行研究。该分析应该既考虑短期防护措施（如隐蔽、撤离、服用碘化钾药片等）的作用，也应该考虑长期对策（如食物禁用令、搬迁、地面去污）的需要。同时，此分析还应该考虑对策的启动方式——是否自动启动，这取决于核动力厂状态或基准剂量。

4.4.4.7.2　三级概率安全分析的结果应该为制定应急计划和评价应急响应计划中各方面的相对有效性提供输入。

4.4.5　概率安全分析的确认

4.4.5.1 分析需要许多计算方法。这些方法范围很广，包括从事件序列分析中使用的逻辑事件和故障树模型，到堆芯损坏后安全壳内发生的各种现象的模型和放射性核素在环境中移迁以确定其对健康和经济的影响的模型等，以确定其对健康和经济的影响。应确认这些计算方法以证明其能够充分代表所发生的过程。对使用的计算机程序的评价将在 4.6 节给予说明。

4.4.5.2 下述做法正逐渐成为标准方法，即营运单位委托某外单位对概率安全分析进行独立的同行评议，以保证分析的范围、模型和数据是适当的，并且保证该分析与目前世界上的最佳实践一致。

4.4.6　概率安全分析的应用

4.4.6.1 概率安全分析结果的表述

4.4.6.1.1 应该审查研究概率安全分析的结果，以确定那些对风险贡献最大的故障序列。在某些情况下，概率安全分析可能会指出某一个贡献因素对风险起主导作用，但是进一步的研究可能认为该因素的主导性是由概率安全分析的有关该部分所做的过分保守假设引起，而不是对反应堆设计的反映。在这种情况下，应该考虑对分析的修正这些部分的分析进行修正以对风险提供较切合实际的风险评估。

4.4.6.2 活态概率安全分析

4.4.6.2.1 在整个核动力厂寿期内，都应该应用概率安全分析评价应该在整个核动力厂寿期内应用，以便为决策过程提供输入。在核动力厂运行期间，常对其安全系统设计或其运行方式进行修改，例如在维护和试验期间核动力厂配置的变更。这些修改可能对核动力厂的风险水平有影响。在核动力厂运行期间，将会得到有关始发事件频率和部件故障概率方面的统计数据。同样地，也可以得到一些新的信息和更复杂精确的方法与工具的使用，这样可会改变分析中所作的某些假设，并因而可能改变概率安全分析提供的风险评估。

4.4.6.2.2 在核动力厂寿期内，概率安全分析应不断及时更新结果，以使其有助用于决策过程。更新过程应该考虑到核动力厂设计和运行的变更、新的技术信息、更加精确的方法和工具、以及从核动力厂运行中得到的新数据等。应该对概率安全分析的状况进行定期审查以保证其能充分反映核动力厂的现状。

4.4.6.2.3 核动力厂运行人员营运单位应该在核动力厂整个寿

期内不断收集其运行数据，以便核实并更新概率安全分析。这应该包括以下方面的统计数据：始发事件频率、部件故障率以及在试验、维护或修理期间核动力厂的不可用性等。分析应该依据新数据予以评价。

4.4.6.2.4　在核动力厂正常运行期间，应该促进活态概率安全分析不断发展，以有助于在核动力厂正常运行期间的决策过程。这包括各项这样一些活动，例如应用概率安全分析帮助编制维修停役计划，以保证这些活动引起的风险足够低。

4.4.6.3 概率安全分析的局限性

4.4.6.3.1　概率安全分析是设计评价和安全分析过程的一个关键部分，该分析为整个核动力厂提供了整体的风险模型，并且允许可对可能事故的频率和后果进行统一的评价。但是，需要了解概率安全分析的局限性

4.4.6.3.2　需要了解概率安全分析的局限性，特别需要指出是，概率安全分析不应该认视为概率安全分析可以代替工程设计评价或确定论设计方法。更确切地说，应该认为概率安全分析提供了对为核动力厂的风险水平提供了相关的深入了解。这些有关风险的深入了解应该在决策过程中用来补充从确定论分析中得出的结论。

4.4.6.3.3　概率安全分析中使用的模型和数据均有不确定性。对于从大型数据库或相关运行经验中得出的部件故障概率，其不确定性相对来说是比较小的；但是，在很多其他方面，其不确定性可能大得多，甚至无法量化，例如：

- 无运行经验数据可依据的始发事件的发生频率和部件的故障

率；

- 大地震的发生频率及其地面运动情况；

- 对共因故障的模拟；

- 对人为差错人员差错的模拟；

- 对在严重事故中可能发生的现象的模拟；

- 估计核动力厂放射性物质释放的厂外后果。

在决策过程中利用概率安全分析的结果时应该认识到这些不确定性。概率安全分析的结果应该由不确定性分析或至少由敏感性分析给予支持。

4.4.7　概率论安全准则

4.4.7.1 准则的建立

4.4.7.1.1　当概率安全分析的结果用于支持决策过程时，应该为此建立一个正式框架。该过程的细节详细程度取决于使用专用概率安全分析实际应用的目的、决策的性质以及要使用的概率安全分析的结果。当在使用概率安全分析的定量结果时，应该设立确定可与之比较的相应的参考值，以便与该结果进行对比。

4.4.7.1.2　当概率安全分析的目的是为了确定风险的主要贡献因素，或是为了在多种核动力厂设计方案及配置之间作出选择时，可不需要参考值。

4.4.7.1.3　当概率安全分析的目的是为了帮助判定作出下列情况判断时，则应该制定概率安全准则，以便为设计单位、营运单位和国家核安全监管部门提供关于对核动力厂所要求的安全水平的指导，

例如：⑴计算的风险是否可接受的；⑵核动力厂的设计和运行的变更建议是否可接受的；⑶是否需要进行修改变更设计以降低风险水平，则应该制定概率论安全准则，以便为设计单位、营运单位和监管部门提供关于对核动力厂所要求的安全水平的指导。这些准则也用来确定设计单位、营运单位和国家核安全监管部门为在完成在核动力厂安全规定中规定的各自任务中必须达到的目标。

4.4.7.1.44.4.7.1.4 按照所计算出的后果的级别，概率安全分析将得给出处于在不同级别上的风险量的数值度量。在确定概率论安全准则时可能与下列度量中的部分或全部相关可以采用下列风险量设定概率安全准则，必要时，也可包括：

-安全功能或安全系统的故障概率（级别：0）；

- 堆芯损坏坏频率（一级别：1）；

- 放射性物质从核动力厂的某种特定的释放（如即数量、同位素等）的频率，或作为数值大小的函数的频率（二级别：2）；

- 安全功能或安全系统的故障概率（零级）；

-对公众的各种健康影响效应的频率或环境后果的频率（三级别：3）。

4.4.7.2 数值

4.4.7.2.1 安全功能或安全系统故障概率： 可以在安全功能级别或安全系统级别上设建立概率论目标。这对些目标用于核查多重性和多样性水平是否充分是有用的。这些目标随核动力厂的设计不同而不同，因此这里不作规定提供指导。安全评价应该核查这些目标是否

已经满足。如果没有达到这些目标，只要满足了较高级别的准则，设计仍可能被接受；但是，对该安全系统应该特别注意，以确定是否能对其进行合理可行的改进。

4.4.7.2.2　关于堆芯损坏频率的目标是：

- 对已有的核动力厂，每堆年１０－４；

- 对新的核动力厂，每堆年１０－５。

4.4.7.2.3　堆芯损坏频率是风险最通用的风险度量数值，这些数值应用作概率论安全准则。

4.4.7.2.4　放射性物质向厂外大量释放到厂外：放射性物质的大量释放将会对社会造成严重影响，并且将要求执行采取厂外应急安排措施。

4.4.7.2.5　关于放射性物质大量释放的目标是：

- 对已有的核动力厂，每堆年１０－５；

- 对新的核动力厂，每堆年１０－６。

4.5 敏感性和不确定性分析

4.5.1　在使用推荐的最佳估算程序进行确定论安全分析和概率安全分析时，需要由敏感性和/或不确定性分析作补充。

4.5.2　应该用敏感性分析（包括对程序输入变量和模拟型参数的系统性偏差变化的敏感性分析，应该用于）来确定分析所必需的重要参数，并表明输入变量的实际偏差变化不会导致分析结果的剧烈改变变化（“陡边”效应）。

4.5.3　确定论安全分析框架中的不确定性研究是指意味着对

核动力厂工况、程序模型及关于分析结果的相关有关现象对分析结果的影响的统计组合。该这些研究应该用于确认核动力厂的实际参数将限制在计算结果加上具有特定的高可信度的不确定性一个范围内，该范围是计算结果加上具有规定的高可信度的不确定性。通常将敏感性分析、程序对程序的比较、程序对数据对比以及专家判断等组合起来用于估计不确定性。

4.5.4　作为概率安全分析中的一个关键部分，概率安全分析也应该进行作为关键部分的不确定性分析。对不确定性的确认和分析是概率安全分析的基本优势。确定论分析中也会存在不确定性，但是，通常并不予确认或分析。在试图考虑不确定性时宁可审慎地采用保守性假设。但是，确定论分析中不确定性的程度并不相同，并可能导致不均衡的分析。概率安全分析的方法的优势可作为是确定论方法的补充，并且能够完全反映出对不确定性进行全面描述。对这种情况，不确定性也应该反映始发事件概率频率和部件故障概率的范围。

4.6 使用的计算机程序的评价

4.6.1　安全分析中要使用大量计算机程序，通常包括：

- 放射学分析程序：评估工作人员遭受的辐照剂量；

- 中子物理程序：模拟反应堆堆芯的行为；

- 燃料行为程序：模拟核动力厂正常运行期间及事故发生后燃料元件的行为；

- 反应堆热工水力学程序：模拟核动力厂正常运行及事故发生后反应堆堆芯及相关冷却剂系统的行为；

- 安全壳热工水力学程序：模拟发生冷却剂丧失事故或二回路管道破裂事故后，安全壳的压力和温度的行为状况；

- 结构程序：模拟各部件和构筑物在承受载荷及载荷组合下，各部件和构筑物的应力应变行为状况；

- 严重事故分析程序：模拟事故序列自堆芯损坏开始直到至安全壳失效的进展过事故序列进程；

- 放射性后果学分析程序：用于模拟放射性物质在厂区内外的迁移，以确定其对工作人员及公众的影响效应；

- 概率安全分析程序：构筑逻辑模型，以确定可能跟随在假设始发事件后可能发生的事故序列并估计其发生频率。

4.6.2　在安全分析中使用的所有计算机程序都应予以确认和验证。计算机程序中使采用的计算方法应该充分适合于使用目的，正确的物理控制方程物理和逻辑的关系式应该补充在计算机程序中正确地实现。

4.6.3　关于计算机程序，应该确定认：

- 用于描述过程的物理模型和相关的简化假设是合理的；

- 用于描述物理过程的关系式是合理的，其适用范围已确定；

- 程序的适用范围已确定。这一点很重要，因为当如果计算方法只是指定用来模拟一规定范围内的物理过程时，则该计算方法的使用那么在不应该超出此范围外，不应该使用该计算方法；

- 使采用的数值方法能够提供具有足够准确精度的解；

- 系统的方法已用于计算机程序的设计、编程写、调试和文件编

制；

- 已按照程序的技术规格对源程序进行了评价（对于大型程序可能无法实现）。

4.6.4　关于计算机程序的输出结果，应该确定程序的预测结果已经与如下参数以下数据和程序进行了比较：

- 所模拟重要现象的实验数据。这通常包括针对 “单项效应”和较大型的“整体”实验的比较；

- 核动力厂数据，包括在核动力厂调试或启动期间完成的试验，以及运行事件或事故；

- 独立开发的和使用不同方法的其它程序。这对模拟严重事故现象特别重要；

- 具有足够准确结果的基标准题和/或数值基准。

4.6.5　在安全分析时，应该对确认各每个程序在安全分析中的每种应用进行确认。

4.6.6　需要指出，对于已开发的某些程序，已经存在作多方面的确认工作的程序包了。但对于正在开发的程序和那些用于模拟并却未完全理了解的严重事故现象的程序，这种确认可能就不够完善了。

4.6.7　程序的使用者，应该保证：

- 接受了足够的培训并且理解所使用的程序；

- 在程序使用方面具有足够的经验，并且完全了解程序的用途和局限性；

- 在有合适的使用程序使用手册时有足够的使用指南；

- 可能的话，在进行开始安全分析工作之前使用者已经使用过该程序对基标准题进行分析。

4.6.8　关于计算机程序的使用，应该确定认：

- 节点化和核动力厂模型能很好地反映核动力厂的行为；

- 输入数据正确；

- 正确理解和使用程序的输出结果。

5.独立验证

5.1 独立安全验证的目的是确认安全评价满足适用的安全要求。

5.2　虽然验证工作可以方便地针对设计的各个重要阶段分段完成，但安全评价的最终独立验证应该总是在设计完成之后进行。独立验证可基本遵照本安全导则 2—4 章讨论的安全评价方法实施。但是，独立验证的范围较之安全评价要更窄一些，因为独立验证是集中最重要的安全问题和要求，而不是全部。

5.3　设计评价活动是质量保证总大纲的一部分，并且是在核动力厂设计阶段主要关心的问题。执行独立验证的小组可考虑先前完成的质量保证审查，以确定独立验证的内容和范围。

5.4　本安全导则主要涉及核动力厂建造开始以前进行的设计验证活动，并且重点集中于设计单位或其代理机构所进行的安全评价活动。但是，本安全导则也可适用于其他随后进行的类似验证活动。

5.5　安全评价的验证应该由熟悉目前反应堆技术发展及安全分析的专家完成。

5.6　执行独立验证的审查人员应该验证安全评价的过程是恰当

的。应该为审查人员提供所有的相关设计文件，包括计算模型、数据和假设等。另外，还应该允许审查人员进入核动力厂的所有区域（包括关键区域）进行巡查，从而确认安全评价充分反映了核动力厂的实际设施。

5.7　作为一个实例（不包括全部），审查的项目清单如下：

- 假设始发事件的选取；
- 应用的工业标准；
- 有关的安全及辐射防护评价问题；
- 为包罗所有类似情况对始发事件所假设的最不利的核动力厂初始条件；
- 单个事件与其故障后果的组合；
- 继发故障的确认；
- 安全系统、非安全系统及各部件在事故期间运行状态的假设；
- 假定的运行人员行动；
- 已验证适用于特定分析的计算机程序；
- 可靠性数据及其在特定分析中的适用性；
- 概率安全分析中事件树和故障树的构建；
- 共因故障；
- 每种特定放射性物质释放形式的大气弥散模型的应用；
- 不确定性分析；
- 超设计基准事故分析过程的充分性。

5.2 独立验证的实施可基本上遵照本安全导则 2—4 章讨论的安

全评价方法。但是，独立验证的范围较之安全评价要更窄一些，因为独立验证是着重于最重要的安全问题和要求，而不是全部。

5.3 独立验证应该由核动力厂营运单位和国家核安全监管部门分别独立进行。核动力厂营运单位通常会对进行设计单位实施的独立审查。

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。（此款挪到 2。2。5）

5.5 独立设计评价活动是质量保证总大纲的一部分，并且是在核动力厂设计阶段主要关心的问题。正如图表 1 所述，独立验证应该作为为保证设计安全和正确而进行的额外核对。在确定独立验证的程度和范围时，执行独立验证的小组可对先前完成的质量保证审查，以的质量保证审查予以考虑。

5.6 本安全导则主要涉及核动力厂建造开始以前进行的设计验证活动，并且重点集中于设计单位或其代理机构所进行的安全评价活动。但是，本安全导则也可适用于其他随后进行的类似验证活动。

5.5 安全评价的验证应该由对目前反应堆技术及安全分析的发展相当熟悉的专家完成。审查人员应该独立于核动力厂的设计人员。

5.8 执行独立验证的审查人员应该验证安全评价的过程是充分的。应该为审查人员提供所有的相关设计文件，包括计算模型、数据和假设等。另外，还应该允许审查人员进入核动力厂的所有区域（包括关键区域），以便进行巡查，从而确认安全评价充分反映了核动力厂的实际设施。

5.9 作为一个实例（不包括全部），审查的项目清单如下：

-假设始发事件的选取；

-适用的工业标准；

-有关的安全及辐射防护评价问题；

-包罗所有类似情况的，为始发事件假设的最不利的核动力厂初始条件；

-单个事件的组合及其故障后果；

-继发故障的确认；

-事故发生期间，对安全系统、非安全系统及各部件假设的运行状况；

-假定的运行人员行动；

-适用于特定分析的已验证计算机程序的选择；

-可靠性数据及其在特殊分析中的适用性；

-概率安全分析中对事件树和故障树的构筑；

-共因故障；

-对每种特定放射性物质释放形式的大气弥散模型的应用；

-不确定性分析；

-超设计基准事故分析过程的充分性。

5.105.8 应该对所选择的计算机计算结果进行独立核对验证，以保证分析的正确性。如果没有尚未对原初次使用的程序尚未进行完成充分的验证和确认的话，则应该使用其他替代程序对其验证准确其精度进行验证。