IAEA
国际原子能机构
安全标准
丛书

核动力厂安全：设计

要求

No. NS-R-1

IAEA
国际原子能机构

该出版物已被第 SSR-2/1（Rev. 1）号取代。

国际原子能机构安全相关出版物

国际原子能机构安全标准

根据国际原子能机构《规约》第三条的规定，国际原子能机构受权制定或采取旨在保护健康及尽量减少对生命与财产的危险的安全标准，并规定适用这些标准。

国际原子能机构借以制定标准的出版物以**国际原子能机构安全标准丛书**的形式印发。该丛书涵盖核安全、辐射安全、运输安全和废物安全以及一般安全（即涉及上述所有安全领域）。该丛书出版物的分类是**安全基本法则**、**安全要求**和**安全导则**。

安全标准按照其涵盖范围编码：核安全（NS）、辐射安全（RS）、运输安全（TS）、废物安全（WS）和一般安全（GS）。

有关国际原子能机构安全标准计划的信息可访问以下国际原子能机构因特网网址：

http://www-ns.iaea.org/standards/

该网址提供已出版安全标准和安全标准草案的英文文本。也提供以阿拉伯文、中文、法文、俄文和西班牙文印发的安全标准文本、国际原子能机构安全术语表以及正在制订中的安全标准状况报告。欲求详细信息，请与国际原子能机构联系（P.O. Box 100, A-1400 Vienna, Austria）。

敬请国际原子能机构安全标准的所有用户将其使用方面的经验（例如作为国家监管、安全评审和培训班课程的基础）通知国际原子能机构，以确保国际原子能机构安全标准继续满足用户需求。资料可以通过国际原子能机构因特网网址提供或按上述地址邮寄或通过电子邮件发至 Official.Mail@iaea.org。

其他安全相关出版物

国际原子能机构规定适用这些标准，并按照国际原子能机构《规约》第三条和第八条 C 款之规定，提供和促进有关和平核活动的信息交流并为此目的充任各成员国的居间人。

核活动的安全和防护报告以其他出版物丛书的形式特别是以**安全报告丛书**的形式印发。安全报告提供能够用以支持安全标准的实例和详细方法。国际原子能机构其他安全相关出版物丛书是**安全标准丛书适用规定**、**放射学评定报告丛书**和**国际核安全咨询组丛书**。国际原子能机构还印发放射性事故报告和其他特别出版物。

安全相关出版物还以**技术报告丛书**、**国际原子能机构技术文件丛书**、**培训班丛书**、**国际原子能机构服务丛书**的形式以及作为**实用辐射安全手册**和**实用辐射技术手册**印发。保安相关出版物则以**国际原子能机构核保安丛书**的形式印发。

核动力厂安全：设计

该出版物已被第 SSR-2/1（Rev. 1）号取代。

下述国家是国际原子能机构的成员国：

阿富汗
阿尔巴尼亚
阿尔及利亚
安哥拉
阿根廷
亚美尼亚
澳大利亚
奥地利
阿塞拜疆
孟加拉国
白俄罗斯
比利时
贝宁
玻利维亚
波斯尼亚和黑塞哥维那
博茨瓦纳
巴西
保加利亚
布基纳法索
喀麦隆
加拿大
中非共和国
智利
中国
哥伦比亚
哥斯达黎加
科特迪瓦
克罗地亚
古巴
塞浦路斯
捷克共和国
刚果民主共和国
丹麦
多米尼加共和国
厄瓜多尔
埃及
萨尔瓦多
厄立特里亚
爱沙尼亚
埃塞俄比亚
芬兰
法国
加蓬
格鲁吉亚
德国
加纳
希腊
危地马拉
海地
教廷
洪都拉斯
匈牙利
冰岛
印度
印度尼西亚
伊朗伊斯兰共和国
伊拉克
爱尔兰
以色列
意大利
牙买加
日本
约旦
哈萨克斯坦
肯尼亚
大韩民国
科威特
吉尔吉斯斯坦
拉脱维亚
黎巴嫩
利比里亚
阿拉伯利比亚民众国
列支敦士登
立陶宛
卢森堡
马达加斯加
马来西亚
马里
马耳他
马绍尔群岛
毛里塔尼亚
毛里求斯
墨西哥
摩纳哥
蒙古
摩洛哥
缅甸
纳米比亚
荷兰
新西兰
尼加拉瓜
尼日尔
尼日利亚
挪威
巴基斯坦
巴拿马
巴拉圭
秘鲁
菲律宾
波兰
葡萄牙
卡塔尔
摩尔多瓦共和国
罗马尼亚
俄罗斯联邦
沙特阿拉伯
塞内加尔
塞尔维亚和黑山
塞舌尔
塞拉利昂
新加坡
斯洛伐克
斯洛文尼亚
南非
西班牙
斯里兰卡
苏丹
瑞典
瑞士
阿拉伯叙利亚共和国
塔吉克斯坦
泰国
前南斯拉夫马其顿共和国
突尼斯
土耳其
乌干达
乌克兰
阿拉伯联合酋长国
大不列颠及北爱尔兰联合王国
坦桑尼亚联合共和国
美利坚合众国
乌拉圭
乌兹别克斯坦
委内瑞拉
越南
也门
赞比亚
津巴布韦

机构《规约》于1956年10月23日在纽约联合国总部召开的国际原子能机构规约会议上通过，于1957年7月29日生效。机构总部设在维也纳。机构的主要目标是“加速和扩大原子能对全世界和平、健康及繁荣的贡献”。

国际原子能机构印制
2005 年 1 月 • 奥地利
STI/PUB/1099

安全标准丛书 No. NS-R-1

核动力厂安全：设计

安 全 要 求

国 际 原 子 能 机 构
维也纳，2005年

该出版物已被第 SSR-2/1（Rev. 1）号取代。

这一套安全标准丛书还以阿拉伯文、英文、
法文、俄文和西班牙文出版。

核动力厂安全：设计

国际原子能机构，奥地利，2005 年
STI/PUB/1099
ISBN 92-0-517504-8
ISSN 1020-5853

序

总干事　穆罕默德•埃尔巴拉迪

国际原子能机构的法定职能之一是在为和平目的发展和应用核能中制订或采用旨在保护健康、生命和财产的安全标准，使这些标准适用于机构本身的工作及援助工作，以及应各方请求，使这些标准适用于依任何双边或多边安排所进行的工作，或应一国请求，适用于该国在核能领域的任何活动。

以下机构监督安全标准的制订：安全标准委员会、核安全标准委员会、辐射安全标准委员会、运输安全标准委员会和废物安全标准委员会。成员国在这些委员会中有广泛的代表性。

为确保取得最广泛的国际共识，在国际原子能机构理事会核准（**安全基本法则**和**安全要求**）之前或在出版委员会代表总干事核准（**安全导则**）之前，还将安全标准提交全体成员国征求意见。

国际原子能机构的安全标准对成员国不具法律约束力，但是，它们可以自行决定采纳这些标准以在有关其本国活动的国家条例中使用。这些标准就国际原子能机构本身的工作而言对其具有约束力，就国际原子能机构的援助工作而言对当事国具有约束力。对任何希望与国际原子能机构缔结协议以获得有关核设施的选址、设计、建造、调试、运行或退役或任何其他活动的援助的国家均要遵循安全标准中与协议所涵盖的活动有关的那些部分。然而，应当铭记，在任何审批程序方面的最后决定和法律责任都在于当事国。

虽然安全标准为安全奠定了必不可少的基础，但是，按照国家的实践纳入一些更详细的要求也可能是必要的。此外，将会有一些具体方面需要在个案的基础上予以评定。

在适当情况下提到了易裂变材料和放射性材料以及整个核动力厂的实物保护，但没有予以详细论述。各国在这方面的义务应当按照在国际原子能机构主持下制定的有关文书和编写的出版物加以处理。对工业安全和环境保护中的非放射学问题也没有明确审议。认识到各国应当履行其与此有关的国际承诺和义务。

某些按早期标准建造的设施可能不完全符合国际原子能机构安全标准中所提出的要求和建议。对这类设施如何适用这些安全标准，各国可以自行作出决定。

提请各国注意以下事实：国际原子能机构的安全标准尽管不具法律约束力，但是，它们的制定旨在确保能使各国以按照公认的国际法原则和规则（例如与环境保护有关的那些原则和规则）履行其义务的方式，开展核能和放射性材料的和平利用。按照这样一个普遍原则，一国的领土不得用来对另一国造成损害。因而各国都有义务不遗余力地以谨慎的标准行事。

在国家管辖范围内进行的民用核活动象任何其他活动一样，除遵守公认的国际法原则外，还必须遵守当事国根据国际公约可能履行的那些义务。期望各国在其国家法律制度范围内采用对有效履行其所有国际义务可能是必要的这类立法（包括条例）及其他标准和措施。

编者按

所列附录可视为该标准的一个不可分割的组成部分并具有与主文本相同的地位。利用所列的附件、脚注和文献目录为用户提供可能是有用的补充信息和实例。

安全标准在陈述有关要求、责任和义务时使用“必须”来表述。而在表示所期望选择方案的建议时则用“应当”来表述。

英文文本系权威性文本。

本导则由中国原子能工业公司翻译部翻译，由中国国家核安全局审查。

目　录

1. 引　言

背 景

1.1.　本出版物替代《核动力厂安全法规：设计》（1988年印发的安全丛书No.50-C-D（Rev.1））。它考虑了该设计法规上次修订以来在核动力厂安全方面的种种发展。这些发展包括安全基本法则出版物《核装置安全》[1]的印发，以及目前正在对各种安全标准和与安全有关的其他出版物进行的修订。有关核安全的种种要求，旨在确保充分保护厂区人员、公众和环境免受由核动力厂产生的各种电离辐射效应的危害。人们认识到，技术和科学知识方面的进步，以及核安全和所谓充分保护，都不是一成不变的。安全要求会随着这些发展而变化，本出版物所反映的就是人们目前的这种共识。

目 的

1.2.　本安全要求出版物考虑了安全要求方面的种种发展，例如，把设计过程中考虑严重事故也包括在内。已经得到更多注意的其他课题包括安全管理、设计管理、动力厂老化及消耗效应、基于计算机的安全系统、外部和内部的危害、人的因素、运行经验反馈，以及安全评定与核实。

1.3.　本出版物规定了一些用于界定确保核安全所需的各种要素的安全要求。这些要求适用于安全功能及相关的构筑物、系统和部件，并适用于核动力厂中的安全重要规程。本出版物打算主要用于陆基固定式核动力厂，其中装有为发电或其他供热应用（诸如集中供热或海水淡化）而设计的水冷反应堆。人们认识到，对于其他类型的反应堆，包括未来系统中的一些革新性质的发展，这里的有些要求也许是不适用的，或者在解释这些要求时也许需要做一些判断。各种安全导则将会提供解释和实施这些要求方面的指导意见。

1.4.　本出版物旨在供核动力厂设计、制造、建造和运行单位，以及监管机构使用。

范 围

1.5. 本出版物规定安全重要构筑物、系统和部件为实现核动力厂的安全运行和防止或缓解能危及安全的各种事件的后果而必须满足的设计要求。它还规定对全面安全评定的要求，这种评定的目的是为了找出或许由动力厂在各种动力厂状态（运行状态和事故工况）下的运行产生的潜在危险。这种安全评定过程涉及确定论安全分析和概率论安全分析这两种互补的技术。这些分析必须考虑假想始发事件（PIE），它们包括可以单独地或组合地影响安全的诸多因素。这些事件可能：

— 起源于核动力厂运行本身；
— 是由人的行动引起的；
— 是直接与核动力厂及其环境有关的。

1.6. 本出版物还论及极不可能发生的事件，例如可能导致放射性释放量较大的严重事故；而对于这种事件，在设计中提供预防性或缓解性设施也许是适宜的和切实可行的。

1.7. 本出版物不论及：

— 极不可能发生的外部自然事件或人因事件（诸如陨石或人造卫星撞击）；
— 绝不会影响核动力厂安全的常规工业事故；或
— 由核动力厂运行引起的非放射性效应，此类效应也许须满足另外的国家法规要求。

结 构

1.8. 本安全要求出版物的叙述次序仿效安全原则与安全目标和安全要求与安全准则之间的关系。第2章详述安全原则、目标和概念，它们是导出设计动力厂时必须满足的安全要求的基础。这些安全目标（第2章中的斜体字）抄自安全基本法则出版物《核装置安全》[1]。第3章涵盖设计单位在管理设计过程时需要应用的主要要求，以及有关安全评定、质量保证和采用成熟的工程实践和运行经验方面的要求。第4章提供纵深防御和辐射防护方面的主要的和比较一般的技术要求。第5章提供对主要要求进行补充的一般动力厂设计要求，以确保安全目标得到满足。第6章提供适用于反应堆堆芯、冷却剂系统和安全壳系统之类动力厂特定系统的设计要求。附件I详述假想始发事件这一概念的定义及其应用。附

件II讨论冗余性、多样性和独立性这些作为增强可靠性并防止共因故障的措施的应用。附录详述一些反应堆所需的安全功能。

2. 安全目标和概念

安全目标

2.1. 安全基本法则出版物《核装置安全》[1] 提出了三个基本安全目标，使核动力厂的有关风险减到最小的要求就是根据这些安全目标导出的。以下第2.2—2.6条直接抄自《核装置安全》第203—207条。

2.2. “**总的核安全目标**：*通过在核装置中建立并保持对放射性危害的有效防御，使个人、社会和环境免受伤害。*

2.3. “这条总的核安全目标得到了处理辐射防护和技术问题的两条补充性安全目标的支持。它们是互相依赖的：这些技术方面的措施与行政管理和规程方面的措施一道，共同确保防御起因于电离辐射的危害。

2.4. “**辐射防护目标**：*要确保装置内的或由有计划地从该装置释放出的任何放射性物质引起的射线照射，在一切运行状态下均低于规定限值和保持在合理可行尽量低的水平，并要确保任何事故的放射学后果能得到缓解。*

2.5. “**技术安全目标**：*要采取一切合理可行的措施防止在核装置中发生事故及一旦发生事故时缓解其后果；对于在设计该装置时考虑过的一切可能事故，包括概率非常低的事故而言，要以高可信度确保任何放射学后果都是小的和低于规定限值的；并要确保有严重放射学后果的事故的可能性极低。*

2.6. “安全目标要求将核装置设计和运行得使一切射线照射源处于严格的技术和行政管理控制之下。但是，这一辐射防护目标不排除人受到有限的照射，也不排除法规许可数量的放射性物质从处于运行状态的装置向环境的释放。不过，此种照射和排放必须受严格控制，并必须符合运行限值和辐射防护标准。”

2.7. 为了实现这三个安全目标，在设计核动力厂中，要进行全面的安全分析，以便找出一切照射源，并估计装置内的工作人员和厂外公众可能受到的辐射剂量，还要估计对环境的潜在影响（见第4.9条）。此种安全分析要考察以下内容：（1）动力厂一切有计划的正常运行模式；（2）发生预计运行事件时动力厂的表现；（3）设计基准事故；以及（4）可以导致严重事故的事件序列。以这种

分析为基础，就能求出已有的工程设计对假想始发事件和事故的承受能力、验证安全系统和安全相关物项或系统的有效性，以及求出应急方面的要求。

2.8. 虽然人们会采取措施将一切运行状态下的射线照射控制在合理可行尽量低（ALARA）的水平，并将能导致对辐射源的正常控制丧失的事故的可能性减至最小，但总还是存在可能发生事故的残余概率。因此，要采取措施确保此种事故的放射学后果能得到缓解。此类措施包括：专设的安全设施；由营运单位制定的厂区内事故管理规程；以及有关主管部门可能会制定的、目的在于真的发生事故时减轻射线照射的厂外干预措施。核动力厂的安全设计适用以下原则：能导致高辐射剂量或高放射性释放量的动力厂状态的发生概率（可能性）很低；具有显著发生概率（可能性）的动力厂状态只有小的或者没有潜在放射学后果。一个不可或缺的目标是，采取外部干预措施的必要性可以用技术手段加以限制甚至排除，尽管国家主管部门或许仍然会要求采取此类措施。

纵深防御的概念

2.9. 纵深防御概念当被用于无论是组织工作方面的、行为方面的还是与设计有关的一切安全活动时，它能确保这些活动能受到相互重叠的多种措施的约束，使得故障在真的发生时能被相应的措施察觉、抵销或纠正。自1988年以来，人们一直在进一步推敲这一概念[2，3]。在设计和运行的各个方面适用纵深防御概念，能就形形色色的瞬变过程、预计运行事件和事故，包括由动力厂内的设备故障或人的行动引起的那些事故，以及起源于厂外的事件，提供多层次保护。

2.10. 在设计动力厂时应用纵深防御概念，就能提供多层次的防御（固有特征、设备和规程），旨在防止事故的发生并确保一旦不能防止时仍有合适的保护。

(1) 第一层防御的目的是防止偏离正常运行和防止系统故障。这导致以下要求：按照合适的质量水平和工程实践，诸如应用冗余性、独立性和多样性，完善而保守地设计、建造、维护和运行动力厂。为了满足这个目标，应小心地注意选用合适的设计规范和材料，并注意控制好部件的制造及动力厂建造。那些能有助于减少造成内部危害的可能性（例如控制对假想始发事件的响应），减轻给定假想始发事件的后果，或减少事故序列之后可能出现的释放源项的设计方案对这一防御层是有作用的。还要注意与动力厂设计、制造、建造以及在役检查、维护和测试有关的规程，注意使这些活动易于进行，注意动力厂的运行方式以及注意如何利用运行经验。整个的这一过程要得到旨在为动力厂确定运行和维护要求的分析详细工作的支持。

(2) 第二层防御的目的是探知和截断对正常运行状态的偏离，以期防止预计运行事件上升为事故工况。这样做是出于以下的考虑：尽管在核动力厂的整个服役寿期内会注意对假想始发事件的预防，但还是可能会发生一些假想始发事件。这一层防御需要设置安全分析中确定的一些特定系统，并规定好运行规程，以便防止或尽量减小由此类假想始发事件造成的损害。

(3) 就第三层防御而言，前提是假定上一层防御也许没有阻止某些预计运行事件或假想始发事件升级，尽管这是非常不可能的，因而发展成了比较严重的事件。在动力厂的设计基准中要考虑到这些可能性不大的事件，并提供固有的安全特征、失效安全的设计、附加的设备和规程，以便控制其后果，并在发生此种事件之后实现稳定而可接受的动力厂状态。这导致提供专设安全设施这一要求，这些设施有能力首先把动力厂引导到可控制的状态，随后引导到安全停堆状态，并至少维持一道可以将放射性物质包容起来的屏障。

(4) 第四层防御的目的是处理也许会超过设计基准的严重事故，并确保放射性释放量维持在尽可能低的水平。这层防御的最重要目的是保护上述的包容功能。这可以靠能阻止事故发展的补充措施和规程，以及缓解某些严重事故的后果措施，再加上事故管理规程来实现。由这种包容功能提供的保护，可以用最佳估计方法加以验证。

(5) 第五层也是最后一层防御的目的，是缓解事故工况下可能释放出的放射性物质的放射学后果。这要求提供一个设备齐全的应急控制中心以及厂内应急计划与厂外应急计划。

2.11. 与实施纵深防御相关的一个方面，是在设计中提供一系列的实体屏障，用于将放射性物质包容在规定的场所内。所需要的实体屏障的数目取决于潜在的内部和外部危害，以及各种故障的潜在后果。对于水冷反应堆而言，这样的屏障一般可以采取燃料基体、燃料包壳、反应堆冷却剂系统压力边界和安全壳的形式。

3. 对安全管理的要求

管理方面的责任

3.1. 营运单位对安全负总责。但是，所有从事安全重要活动的单位，都有责任确保将安全事务放在最优先的位置。设计单位必须确保将装置设计得能满足

营运单位的要求，包括电力公司方面的任何标准化的要求；确保设计考虑了安全方面的最新进展；确保设计符合设计规范和安全分析；确保设计满足国家法规要求；确保设计满足有效的质量保证大纲的各项要求；并确保正确地考虑过任何设计变更的安全性。为此，设计单位必须：

(1) 明确划分责任以及相应的权限范围与联系渠道；
(2) 确保它在所有层次上都拥有足够的技术上合格且受过适当培训的职工；
(3) 明确地划分好负责设计的不同部分的各个小组之间的接口，并酌情划分好设计者、电力公司、供应者、建造者和承包者之间的接口；
(4) 制定并严格遵守完备的规程；
(5) 定期审查、监督和监查一切与安全有关的设计事务；以及
(6) 确保安全文化得到保持。

设计管理

3.2. 核动力厂的设计管理必须确保各个安全重要构筑物、系统和部件有合适的特性、技术规范和材料组成，使得安全功能得到发挥，使动力厂在其整个设计寿命期间能够安全运行和具有必要的可靠性，并能防止事故的发生，和将保护厂区人员、公众和环境作为首要任务。

3.3. 设计管理必须确保营运单位的要求得到满足，并对人的能力和人员局限性给予应有的考虑。设计单位必须提供充足的安全设计资料，以确保动力厂的安全运行和维护，允许以后能对动力厂进行修改，并推荐可纳入动力厂的行政管理规程和运行规程（即运行限值和条件）的实际做法。

3.4. 设计管理必须考虑确定论安全分析和补充性的概率论安全分析的结果，这样就产生一个迭代过程；必须利用这一过程确保对防止事故缓解及其后果已经给予应有的考虑。

3.5. 设计管理必须确保借助适当的设计措施以及合适的运行与退役实践，使放射性废物的产生从活度和体积两个方面保持尽可能的少。

经验证的工程实践

3.6. 只要可能，安全重要构筑物、系统和部件就必须按照经批准的最新标准或当前适用标准设计；其设计必须是在先前的相同应用中已证明是成熟的；并且必须认真地挑选这些物项，使之符合安全所需要的动力厂可靠性目标。必须认真地鉴别和评价被用作设计依据的规范和标准，以确定它们的适用性、充分

性和足够性，必要时必须加以补充或修改，以确保最后的质量与所需的安全功能相适应。

3.7. 当引入未经验证的设计或设施，或存在着偏离既定工程实践之处时，必须借助适当的支持性研究计划，或通过仔细地研究从相关的其他应用中获得的运行经验，来证明其安全性是足够的。这种开发性的工作必须在投入使用前经过充分的检验，并必须在使用中进行监测，以核实已达到预期的效果。

3.8. 在选择设备时，必须考虑误动作和不安全的故障模式（例如不能在需要时跳闸）。在设计不得不考虑和容忍某一构筑物系统或部件的故障的场合，必须优先考虑采用那种展示了一种可预测和已揭示的故障模式并便于修理或替换的设备。

运行经验和安全研究

3.9. 设计必须充分考虑从正在运行的动力厂中取得的相关运行经验和相关研究计划的成果。

安全评定

3.10. 必须进行全面的安全评定，以证实交付制造、建造和峻工的设计满足设计过程开始时提出的安全要求。

3.11. 安全评定必须成为设计过程的一部分，同时在设计活动和证实性分析活动之间存在迭代过程，而且其范围和详细程度随着设计计划的进展而不断增加。

3.12. 这种安全评定的基础必须是从安全分析导出的数据、先前的运行经验、支持性研究的成果，以及成熟的工程实践。

安全评定的独立验证

3.13. 营运单位必须确保，对安全评定的独立验证是在设计提交监管机构以前，由进行设计的那些人以外的个人或团体进行的。

质量保证[1]

3.14. 必须编写和实施描述关于动力厂的设计管理、完成和评定的总体安排的质量保证大纲。这个大纲必须得到每个构筑物、系统和部件的更详细计划的支持，从而使设计的质量始终得到保证。

3.15. 设计，包括后来的变更或安全改进，必须按照建立在合适的工程规范和标准基础上的既定程序进行，并必须体现出适用的要求和设计基准。设计接口必须加以明确和控制。

3.16. 设计，包括设计工具和设计的输入与输出，其充分性必须由原先从事此工作的那些人以外的个人或团体进行核实或验证。核实、验证和批准必须在进行详细设计之前完成。

4. 主要技术要求

对纵深防御的要求

4.1. 在设计过程中，必须如第2章中所描述的那样体现出纵深防御。因此，设计：

(1) 必须提供多重的实体屏障，防止放射性物质不受控制地释入环境；
(2) 必须是保守的，且建造必须是高质量的，从而使人相信动力厂的故障和偏离正常运行的情况被减至最少并防止了事故；
(3) 必须利用固有特征和专设设施在发生假想始发事件期间及之后控制动力厂的行为，即必须依靠设计本身尽可能地使不受控制的瞬变过程最少甚至被排除；
(4) 必须利用安全系统的自动触发对动力厂提供附加控制，以便在假想始发事件的早期阶段尽量减少操纵员的动作，同时也必须直接利用操纵员的动作来提供这种控制；
(5) 必须尽实际可能地提供控制事故过程和限制其后果的设备和程序；
(6) 必须提供多种手段来确保实现每项基本安全功能，即控制反应性、排热和包容放射性物质，从而保证这些屏障的有效性和缓解任何假想始发事件的后果。

[1] 更详细的指导，见参考文献[4]。

4.2. 为了确保纵深防御这一总的安全概念得到维持，设计必须尽实际可能地防止：

(1) 出现有损实体屏障完整性的问题；
(2) 屏障在需要它发挥作用时失效；
(3) 一道屏障因另一道屏障的失效而失效。

4.3. 设计必须使第一层至多第二层防御能够阻止一切假想始发事件（最不可能的除外）上升为事故工况。

4.4. 设计必须考虑这样的事实：当缺少某一层防御时，多层防御的存在并不是继续进行功率运行的充分条件。所有各层防御都必须总是可用的，尽管对于除功率运行以外的各种运行模式来说，按规定这一要求可以有所放松。

安全功能

4.5. 整个安全方案的目标必须是：提供足够的手段使动力厂保持正常的运行状态；确保发生假想始发事件之后立即做出正确的短期响应；以及有利于在发生设计基准事故期间和之后以及在那些超设计基准事故的特定事故工况中对动力厂的管理。

4.6. 为了确保安全，在各种运行状态下、在发生设计基准事故期间与之后，以及尽实际可能地在发生那些超设计基准事故的特定事故工况期间，以下一些基本安全功能都必须得到履行：

(1) 控制反应性；
(2) 排出堆芯热量；和
(3) 包容放射性物质与控制运行排放，以及限制事故释放。

这三项基本安全功能进一步详细划分的实例见附录。

4.7. 必须遵循系统化方法来确定在发生假想始发事件后的各个时期中履行这些安全功能所必需的构筑物、系统和部件。

事故预防和动力厂安全特性

4.8. 动力厂设计必须做到它对假想始发事件的敏感性被减到最小。动力厂对任何假想始发事件的预期响应，必须是可合理达到的如下结果（以重要性为序）之一：

(1) 依靠动力厂的固有特性，假想始发事件不产生与安全有关的重大影响，或只使动力厂产生趋向于安全的变化；或者

(2) 发生假想始发事件之后，动力厂借助非能动安全设施或在控制这种假想始发事件所必需的状态下连续运行的安全系统的动作进入安全状态；或者

(3) 发生假想始发事件之后，动力厂借助为了响应这种假想始发事件而必需投入运行的那些安全系统的动作进入安全状态；或者

(4) 发生假想始发事件之后，动力厂借助规定的程序性动作进入安全状态。

辐射防护和验收标准

4.9. 为了在设计核装置时实现第2.2—2.5条中给出的三个安全目标，一切真实的和潜在的辐射源都必须一一列出并得到认真的考虑，并必须采取措施，确保这些源受到严格的技术控制和行政管理控制。

4.10. 必须采取措施确保第2.4—2.5条中给出的辐射防护和技术安全目标得到实现，并确保公众和厂区人员在包括维护和退役的一切运行状态下受到的辐射剂量不超过规定限值且符合合理可行尽量低的原则。

4.11. 该设计必须将防止或在无法防止时减轻由设计基准事故和选定严重事故引起的射线照射作为一个目标。必须采取设计措施确保公众和厂区人员的潜在辐射剂量不超过可接受限值且符合合理可行尽量低的原则。

4.12. 必须将有可能导致高辐射剂量或高放射性释放量的动力厂状态的发生概率限制在很低的水平内，并必须确保发生概率不可忽视的动力厂状态只产生小的潜在放射学后果。必须以这些要求为基础，规定核动力厂设计的放射学验收标准。

4.13. 通常有数量有限的几组放射学验收标准，且常见的做法是将这些验收标准与若干种动力厂状态联系起来。这些种状态一般包括：正常运行、预计运行事件、设计基准事故和严重事故的工况。对这几种工况的放射学验收标准作为一个最低的安全水平，必须满足监管机构的要求。

5. 动力厂设计要求

安全分级

5.1. 必须首先确定属于安全重要物项的所有构筑物、系统和部件，包括仪表和控制（I&C）软件，然后根据其安全功能和安全重要性分级。它们的设计、建造和维护必须使其质量和可靠性与这种分级相适应。

5.2. 划分某一构筑物、系统或部件安全重要性的方法必须主要基于确定论方法，并适当辅以概率论方法和工程判断，同时考虑如下因素：

(1) 该物项要执行的安全功能；
(2) 未能执行其功能的后果；
(3) 需要该物项执行某一安全功能的概率
(4) 假想始发事件（PIE）后将需要该物项运行的时间或时期。

5.3. 必须在不同级别的构筑物、系统和部件之间提供设计合适的界面，以确保被划分为较低级别的系统中的任何故障不会蔓延到被划分为较高级别的系统。

总的设计基准

5.4. 设计基准必须规定动力厂能够在规定的放射防护要求范围内应付各种特定的运行状态和设计基准事故所需的能力。设计基准必须包括正常运行的规格、假想始发事件造成的各种动力厂状态、安全分级、重要假设，在某些情况下还应包括具体的分析方法。

5.5. 在正常运行、预计运行事件和设计基准事故的设计基础中，须应用保守的设计措施并遵循成功的工程实践，以便提供如下高度保证：不会发生对反应堆堆芯的任何重大损坏；辐射剂量保持在所规定的限值内，并符合合理可行尽量低的原则。

5.6. 除设计基准外，动力厂在超过设计基准的规定事故，包括选定的严重事故中的性能，也须在设计中加以处理。这些评价所使用的假设和方法可以最佳估计为基础。

动力厂状态类别

5.7. 动力厂状态必须按照其发生的概率加以确定和分成数量有限的类别。这些类别通常包括正常运行、预计运行事件、设计基准事故和严重事故。必须为每个类别指定验收标准，且这些准则考虑到如下要求：频繁发生的假想始发事件必须仅有很小或根本没有放射学后果，而可能导致严重后果的事件的发生概率必须很低。

假想始发事件

5.8. 在设计动力厂中，必须认识到纵深防御的所有层次都可能出现问题，因而必须提供设计措施，确保完成所需的安全功能和满足安全目标。这些问题根源于假想始发事件，后者是根据确定论技术或概率论技术或这两者的组合选定的。发生概率均很低的各种独立事件在设计中通常预计不会同时发生。

内部事件

5.9. 必须对假想始发事件（见附件I）进行分析，以便确定所有可能影响动力厂安全性的内部事件。这些事件可能包括设备故障或误操作。

火灾和爆炸

5.10. 安全重要构筑物、系统和部件的设计和布置必须与其他安全要求一致，使得外部或内部事件引发的火灾和爆炸的概率和影响减至最低限度。必须保持停堆、排出余热、包容放射性物质和监测动力厂状态的能力。这些要求必须通过适当采用冗余部件、多样化系统、实体分隔和故障时安全运行设计来满足，以便实现下述目标：

(1) 防止火灾发生；
(2) 探测刚发生的火灾并迅速灭火，从而限制破坏；
(3) 防止未灭掉的火灾蔓延，从而减少其对动力厂重要功能的影响。

5.11. 必须进行动力厂火灾危害分析，以确定所需的防火屏障级别，并且提供所需能力的火灾探测系统和消防系统。

5.12. 消防系统必须能在必要时自动启动，系统的设计和安置必须确保其破损或误动运行或意外运行不会对安全重要构筑物、系统和部件的能力造成重大破

坏，不会同时影响冗余安全组合，而使为满足单一故障准则所采取的措施变得无效。

5.13. 在整个动力厂内只要实际可行就必须使用不燃或阻燃材料或耐热材料，尤其是在安全壳和控制室等位置。

其他内部危害

5.14. 在设计动力厂时必须考虑发生诸如以下内部危害的可能性：洪水、产生飞射物、管道甩动、射流冲击或者破损系统或现场其他设施中的流体泄放。必须提供适当的预防和缓解措施，以确保核安全不受到损害。一些外部事件可能引发内部火灾或水灾和可能导致飞射物的产生。这种外部和内部事件的相互影响也必须在设计中适当加以考虑。

5.15. 如果在不同压力下运行的两种流体系统发生相互连通,那么这两种系统或者都必须设计成承受较高压力,或者必须采取措施,防止发生单一故障时在较低压力下运行的系统超过设计压力。

外部事件

5.16. 必须针对厂址和动力厂拟议的结合确定设计基准自然和人为外部事件。所有那些可能造成重大放射学危险的事件都必须予以考虑。必须结合使用确定论方法和概率论方法来选定动力厂设计能够承受的一组外部事件，并由此确定设计基础。

5.17. 必须考虑的自然外部事件包括在描述厂址特征时已确定的那些事件，如地震、洪水、狂风、飓风、海啸（潮汐波）和极端气象条件。必须考虑的人为外部事件包括描述厂址特征时已确定的那些事件和籍以导出设计基础的事件。在设计过程初期必须重新评价这些事件的清单，以确保完整性。

与厂址有关的特性 [2]

5.18. 在确定一座核动力厂的设计基准时，必须考虑动力厂与环境之间的各种相互作用，所指的环境包括人口、气象学、水文学、地质学和地震学等因素。

[2] 更详细的指导，见参考文献[5]。

还必须考虑动力厂安全和公众保护可能依赖的电力供应和消防服务之类的厂外服务的可获得性。

5.19. 对将选址在热带、两极、干旱或火山附近地区的核动力厂项目必须进行评定，以便确定因该厂址特性而可能需要的特殊设计特征。

事件的组合

5.20. 在随机发生的个别事件的组合肯定会导致预计运行事件或事故工况的情况下，必须在设计中考虑到这种组合。某些事件可能是其他事件的后果，如地震后发生水灾。这种相应而生的效应必须视为原来的假想始发事件的一部分。

设计规则

5.21. 必须规定构筑物、系统和部件的工程设计规则，并且必须使其符合已接受的适当国家标准工程实践（见第3.6条），或国际上已经使用的或另一国家已确立的标准或实践，而且其使用是适当的，也是为国家监管机构所接受的。

5.22. 动力厂的抗震设计必须规定充分的安全裕度，以防受地震事件影响。

设计限值

5.23. 必须为各种运行状态和设计基准事故规定一套与每个构筑物、系统或部件的主要物理参数相一致的设计限值。

运行状态

5.24. 动力厂必须设计成能够在规定的各种参数（例如压力、温度和功率参数）范围内安全运行，必须假设可提供一套最低限度的规定的安全系统辅助设施（例如辅助给水能力和应急电源）。该设计须是这样的：动力厂对各种预计运行事件的响应将允许安全运行或必要时停堆，但不必调用纵深防御第一层次或至多不过第二层次以外的措施。

5.25. 在启动、换料和维护之类低功率和停堆状态下安全系统的可利用率可能降低，在设计中必须考虑此时发生事故的可能性，并且必须规定对安全系统不可利用率的适当限制。

5.26. 设计过程必须为安全运行确立一套要求和限制，包括：

(1) 安全系统整定值；
(2) 工艺变量和其他重要参数的控制系统约束值和规程约束值；
(3) 为确保各构筑物、系统和部件发挥设计中预定的功能而对动力厂的维护、测试和检查要求，同时考虑ALARA原则；
(4) 明确规定运行配置，包括安全系统停役情况下的运行限制。

这些要求和限制必须是确定批准营运单位运营该动力厂的运行限值和条件的基础。

设计基准事故

5.27. 必须根据假想始发事件清单（见附件I）导出一套设计基准事故，以便设定须据以设计安全重要构筑物、系统和部件的边界条件，。

5.28. 在为响应假想始发事件而需要立即采取可靠行动的情况下，必须做好自动启动所需的安全系统动作的准备，以便防止发展成可能威胁下道屏障的更严重工况。在不需要立即行动的情况下，可允许手动启动系统或采取其他操纵员行动，条件是要在充分的时间内揭示这种行动的必要性和确定合适的规程（如行政规程、运行规程和应急规程），以确保这些行动的可靠性。

5.29. 对诊断动力厂状态和使动力厂及时处于长期稳定停堆工况可能需要的操纵员行动必须加以考虑，并通过提供适合监督动力厂状况和设备手动操作的控制装置的仪表加以促进。

5.30. 手动响应和恢复过程所需的任何设备必须放置在最合适的位置，以确保其需要时随时能用和在预计环境条件下允许人接近。

严重事故

5.31. 某些概率很低的动力厂状态属于超设计基准事故工况，可能归因于导致堆芯性能明显恶化的安全系统多重故障，它们可能有损于许多或所有用于防止放射性物质释放的屏障的完整性。这些事件序列被称为严重事故。必须采用工程判断和概率论方法相结合的办法来考虑这些严重事故序列，以确定那些可为其找到合理可行的预防或缓解措施的序列。可接受的措施不一定涉及应用设计基准事故确定和评价中所采用的保守工程作法，而是应该基于现实的或最佳估

计的假设、方法和分析准则。根据运行经验、有关的安全分析和安全研究结果，解决严重事故的设计活动必须考虑下列情况：

(1) 必须综合采用概率论方法、确定论方法和合理的工程判断确定可能导致严重事故的重要事件序列。

(2) 然后必须对照一套旨在确定设计中必须处理的严重事故的标准审查这些事件序列。

(3) 对于或者能够减少这些选定事件发生的可能性，或者当这些选定事件发生时必须缓解其后果的可能设计变更或规程变更，必须加以评价并在合理可行时予以实行。

(4) 必须考虑动力厂的整个设计能力，包括一些系统（即安全系统和非安全系统）在超过其原来预定功能和预计运行状态下的可能使用，和附加临时系统的使用，以便使动力厂回到受控状态和/或缓解严重事故的后果，条件是可以表明这些系统能够在预计的环境条件下发挥功能。

(5) 对于多机组动力厂来说，必须考虑使用其他机组的现有手段和/或支持，条件是其他机组的安全运行不会受到损害。

(6) 必须建立事故管理规程，同时考虑有代表性的和主要的严重事故情景。

构筑物、系统和部件的可靠性设计

5.32. 安全重要构筑物、系统和部件必须设计成能够以足够的可靠性承受所有确定的假想始发事件（见附件I）。

共因故障

5.33. 必须考虑安全重要物项发生共因故障的可能性，以确定必须在哪些地方应用多样性、冗余性和独立性原则来实现所需的可靠性。

单一故障准则

5.34. 必须对动力厂设计中所考虑的每个安全组合应用单一故障准则。

5.35. 为测试动力厂与单一故障准则的符合情况，必须以下列方式分析有关的安全组合。必须假设单一故障（及其所有继发性故障）依次发生在该安全组合的每个单元中，直至已分析所有可能故障。然后必须依次对每个重要安全组合进行分析，直至考虑了所有安全组合和所有故障。（在本安全要求出版物中，

安全功能，或有助于执行这些安全功能的系统（为实现所需的可靠性，它们需要有冗余性）已通过关于“单一故障假设”中的说明确定）。该系统中的单一故障假设是所述过程的一部分。在单一故障分析中的任何方面都没有假设发生超过一个的随机故障。

5.36. 误动作必须视为将该概念用于某一安全组合或系统时发生的一种故障模式。

5.37. 当按照下列条件应用上述分析时，如果已表明每个安全组合完成了其安全功能，则必须认为符合该准则已实现：

(1) 对该安全组合，假设发生了假想始发事件的任何可能有害后果；和
(2) 在考虑维护、测试、检查和修理以及允许的设备停役时间的情况下，假设执行所需安全功能的安全系统有最差的可容许配置。

5.38. 不符合单一故障准则必须是例外，并且必须在安全分析中予以明确证明。

5.39. 在单一故障分析中，可以不必假设某一设计、制造、在役检查和维护的非能动部件未达到极高质量，只要它保持不受到假想始发事件的影响。不过，在假设某一非能动部件不发生故障时，必须证明这种分析方法的合理性，同时要考虑负荷和环境条件，以及始发事件后需要该部件执行功能的总时间。

故障安全设计

5.40. 必须考虑故障安全设计原则，并适当将其纳入动力厂安全重要系统和部件的设计中：如果某一系统或部件发生故障，动力厂系统必须设计成在不必启动任何动作的情况下就可以进入安全状态。

辅助服务

5.41. 支持构成安全重要系统一部分的设备的辅助服务必须视为该系统的一部分，并必须相应地划定级别。它们的可靠性、冗余性、多样性和独立性以及提供隔离和测试功能能力的特性必须与其所支持的系统的可靠性相适应。保持动力厂处于安全状态所需的辅助服务可以包括电力、冷却水和压缩空气或其他气体的供应以及润滑手段。

设备停役

5.42. 设计必须通过应用增加的冗余性等手段确保可以在不关闭动力厂的情况下进行安全系统的合理在役维护和测试。必须考虑设备停役，包括系统或部件安全由于故障的而不能使用，并且在这种考虑中必须包括预期维护、测试和修理工作对每个安全系统的可靠性的影响，以便确保仍能够以所需的可靠性实现该安全功能。在动力厂开始运行前，必须分析和确定每种情况下允许设备停役的时间和要采取的行动，并将其纳入动力厂运行说明中。

在役测试、维护、修理、检查和监测的提供

5.43. 除第5.44条所述的以外，安全重要构筑物、系统和部件必须设计成能够在核动力厂整个寿期内就发挥其功能的能力进行校正、测试、维护、修理或更换、检查和监测，以证明正在满足可靠性目标。动力厂布置必须是这样的：这些活动得到促进，并能够按照与要执行的安全功能的重要性相适应的标准得到执行，同时在系统可利用率方面没有任何重大减少和没有对现场工作人员造成超剂量照射。

5.44. 如果安全重要构筑物、系统和部件没能设计成能够进行所希望程度的测试、检查或监测，那么必须采取下列方案：

— 必须规定其他一些经证明的替代方法和/或间接方法，如监视参考物项或使用经核实和确认的计算方法。
— 必须应用保守的安全裕度或采取其他适当的预防措施，以弥补可能的意外故障。

设备的合格鉴定

5.45. 必须采取合格鉴定规程来确认安全重要物项能够在其整个设计运行寿期内满足执行其功能的要求，同时当需要时能够承受主导的环境条件（振动、温度、压力、射流冲击、电磁干扰、辐照、湿度或这些因素的任何可能组合）。要考虑的环境条件必须包括正常运行、预计运行事件和设计基准事故中预计的变化。在合格鉴定计划中，必须考虑在设备预计寿期期间由各种环境因素（如振动、辐照和极端温度）引起的老化效应。在设备受到外部自然事件影响和需要在这种事件中和事件后执行安全功能的情况下，合格鉴定计划必须尽可能或通过测试或通过分析或两者的组合再现自然现象对该设备造成的条件。

5.46. 此外，任何可合理预计的和可能由具体运行状况引起的异常环境条件，如安全壳泄漏率的定期测试中的异常环境条件，均须包括在鉴定计划中。在可能的程度上，应该以合理的可信度表明必须在严重事故中运行的设备（如某些测量仪表）能够实现设计意图。

老 化

5.47. 设计中必须为所有安全重要构筑物、系统和部件提供合适的裕度，以便考虑有关老化和磨损机制和与服务期有关的潜在性能恶化，从而确保这些构筑物、系统或部件在其整个设计寿期内能够执行所需的安全功能。还必须考虑正常运行条件、测试、维护、维护停役、假想始发事件中和假想始发事件后动力厂状态中的老化和磨损效应。还必须为监测、测试、取样和检查做好准备，以便评定设计阶段预测的老化机制和在使用中可能发生的意外的行为或性能恶化。

人为因素

最佳操纵员表现的设计

5.48. 设计必须是“对操纵员友好”的，并必须以限制人的差错的影响为目标。必须注意动力厂布置和规程（行政规程、运行规程和应急规程），包括维护和检查，以利于运行人员和动力厂之间的接口。

5.49. 现场工作人员的工作区域和工作环境必须按照人机工程学原则设计。

5.50. 必须在设计过程初期就人为因素和人机接口进行系统化考虑，并必须在整个过程中保持下去，以确保适当而明确地区分运行人员与所提供的自动化系统的功能。

5.51. 人机界面必须设计成不但能够为操纵员提供全面而容易管理的信息，而且要为做出决定和采取行动留出所需的时间。必须为辅助控制室采取类似措施。

5.52. 在适当阶段必须包括对人为因素各方面的核实和确认，以确定设计充分适合所有必要的操纵员动作。

5.53. 为有助于确立信息显示和控制的设计准则，必须考虑操纵员具有双重作用：系统管理者的作用（包括事故管理），和设备操纵员的作用。

5.54. 在系统管理者的作用中，必须为操纵员提供能够进行下列工作的信息：

(1) 随时评定动力厂的总体状态，它处于哪种工况，是处于正常运行、预计运行事件还是事故工况，并证实设计的自动化安全行动正在被执行；和

(2) 确定操纵员要采取的适当的安全行动。

5.55. 作为设备操纵员，必须为操纵员提供有关动力厂各系统和设备参数的充分信息，以证实能够安全启动所需的安全动作。

5.56. 设计的目的必须是在充分考虑执行动作可利用的时间、预计的实体环境和对操纵员的心理要求的情况下促使操纵员成功地完成各种动作。操纵员在短的时间范围内进行干预的必要性必须保持在最低程度。设计中必须考虑到干预的必要性，只有在下列条件下才是可接受的：设计者能够证明操纵员有充分的时间做出决定和采取行动；向操纵员简单而毫不含糊地提供决定行动所需的信息；以及事件发生后，控制室或辅助控制室及通往辅助控制室的通道的实体环境是可以接受的。

其他设计考虑

反应堆之间构筑物、系统和部件共享

5.57. 安全重要构筑物、系统和部件通常不得在核动力厂两座或以上反应堆之间共享。如果在特殊情况下，这种安全重要构筑物、系统和部件要在两座或以上反应堆之间共享，则必须证明对于所有处于运行状态（包括维护）下和设计基准事故中的所有反应堆来说，所有安全要求都得到满足。在涉及这些反应堆之一的严重事故情况下，其他反应堆必须能够完成有序的停堆、冷却和余热排出。

含有易裂变材料或放射性物质的系统

5.58. 可能含有易裂变材料或放射性物质的核反应堆内的所有系统都必须设计成能够在运行状态和设计基准事故中确保充分安全。

用于热电联供、供热或海水淡化的动力厂

5.59. 伴有热利用机组（如用于区域供热）和/或海水淡化机组的核动力厂必须设计成能够在正常运行、预计运行事件、设计基准事故和选定的严重事故的任何工况下防止放射性物质从核动力厂迁移到淡化或区域供热机组。

燃料和放射性废物的运输和包装

5.60. 设计中必须含有便于新燃料、乏燃料和放射性废物运输和操作的适当设施。必须考虑通往设施的通道及起吊和包装能力。

撤离路线和通信手段

5.61. 必须为核动力厂提供数量充分并有明确和持久标记的安全撤离路线，以及可靠的紧急照明、通风和安全利用这些路线所必不可少的其他建筑物服务。这些撤离路线必须符合有关的国际辐射分区和消防要求及有关的国家工业安全和动力厂保安要求。

5.62. 必须提供适当的报警系统和通信手段，以便在动力厂和现场工作的所有人员即使在事故工况下都能得到警告和通知。

5.63. 必须总是确保核动力厂范围内、最接近的邻近地区和应急计划中所规定厂外机构获得安全所需的通信手段。必须在设计中考虑这一要求和选择多样化的通信手段。

通道控制

5.64. 动力厂与周围环境必须以通往动力厂的通道能够得到永久控制的方式通过结构构件的适当布置来隔开。尤其是，在建筑物的设计和现场布置中，必须为人员和/或设备作好安排以控制进入，并注意防止人员和货物未经批准就进入动力厂。

5.65. 必须防止未经批准就进入或出于任何原因干扰安全重要构筑物、系统和部件。在为维护、测试或检查而需要进入的情况下，在设计中必须确保所需活动的进行没有明显降低安全相关设备的可靠性。

系统的相互作用

5.66. 如果有需要安全重要系统同时运行的明显可能性时，必须对其可能的相互作用加以评估。在分析中，必须不仅考虑实体的相互联系，而且必须考虑一个系统的运行、误操作或故障对其他重要系统的实体环境的可能影响，以便确保环境变化不会影响系统部件按预定功能发挥可靠性。

电网与动力厂之间的相互作用

5.67. 在动力厂设计中，必须考虑关系到动力厂安全安全重要系统的电力供应所需的可靠性的电网与动力厂的相互作用，通往动力厂的供电线路的独立性和数目。

退 役

5.68. 在设计阶段，必须特别注意把将便于动力厂退役和拆除的设施考虑进去。尤其是，在设计中必须考虑：

（1） 材料的选择，以便把放射性废物的最终量减至最低程度，并有利于去污；
（2） 可能需要的接近能力；和
（3） 贮存动力厂运行和退役中产生的放射性废物所需的设施。

安全分析

5.69. 必须进行动力厂设计的安全分析，在分析中，必须用确定论和概率论分析的方法。在这种分析的基础上，必须建立和确认安全重要物项的设计基准。还必须证明所设计的动力厂能够满足对每类动力厂状态所规定的放射性释放的限值和可接受的（见第5.7条）潜在辐射剂量，以及纵深防御已起到作用。

5.70. 安全分析中所用的计算机规程、分析方法和动力厂模型必须加以核实和确认，并必须充分考虑各种不确定性因素。

确定论方法

5.71. 确定论安全分析必须包括下列情况：

(1) 证明运行限值和条件符合动力厂正常运行设计的假设和意图；

(2) 表征适合于动力厂设计和厂址的假想始发事件（见附件I）；
(3) 分析和评价由假想始发事件产生的事件序列；
(4) 分析结果与放射学验收标准和设计限值的比较；
(5) 建立和确认设计基准；和
(6) 证明可以通过安全系统的自动响应与所规定的操纵员动作的结合来管理预计运行事件和设计基准事故。

5.72. 必须核实所用的分析假设、方法和保守程度的适用性。对动力厂设计的安全分析必须根据动力厂配置方面的重大变化、运行经验及对物理现象的技术知识和了解方面的进步不断更新，并必须与现有或竣工状态相一致。

概率论方法

5.73. 必须进行动力厂的概率论安全分析，以便：

(1) 提供系统化分析，以便给出设计将符合总体安全目标的保证；
(2) 证明已达到平衡设计，以致任何具体设施或假想始发事件都不会对总体危险造成大得不成比例的或明显不确定的贡献，纵深防御的前两个层次能够承受确保核安全的主要重担；
(3) 提供有关将防止可能造成动力厂状况严重异常（“陡边效应”）的动力厂参数微小偏差的保证；
(4) 提供对发生严重堆芯损坏状态概率的评定和需要短期厂外响应的重大厂外释放风险的评定，尤其对于早期安全壳损坏有关的释放来说；
(5) 提供对外部危害发生概率和后果的评定，尤其是动力厂厂址所特有的那些危害；
(6) 确定设计改进或运行规程的修改能够减少严重事故概率或缓解其后果的系统；
(7) 评定动力厂应急规程的充分性；和
(8) 核实与概率性目标（如果规定了的话）的符合情况。

6. 动力厂各系统的设计要求

反应堆堆芯和相关设施

总的设计

6.1. 反应堆堆芯和相关的冷却剂、控制与保护系统，必须设计得留有适当的裕量，以确保不超过规定的设计限值，并在考虑到已有不确定性的情况下，确保辐射安全标准在所有运行状态和在设计基准事故条件下得以适用。

6.2. 位于反应堆压力容器中的反应堆堆芯和相关的堆内构件，必须设计和安装得在确保反应堆能安全停堆、保持反应堆处于次临界状态和确保堆芯得到冷却所需的范围内能承受在各种运行状态、设计基准事故和外部事件下预期会发生的静载荷和动载荷。

6.3. 在各种运行状态和设计基准事故中，必须对最大正反应性及加入反应性的最大增速加以限制，使得反应堆压力边界不会因此而发生失效、冷却能力能得到保持和反应堆堆芯不会发生明显的损坏。

6.4. 在设计中，必须确保把发生假想始发事件后重返临界或反应性急剧上升的可能性降至最低。

6.5. 反应堆堆芯和相关的冷却剂、控制与保护系统，必须设计得能够在动力厂的整个使用寿期内进行必要的检查和测试。

燃料元件和组件

6.6. 燃料元件和组件必须设计得能够令人满意地承受反应堆堆芯中的预期辐照条件和环境条件，这些条件与在正常运行和预计运行事件中可能发生的各种恶化过程并存。

6.7. 需考虑的恶化必须包括下述诸因素引起的恶化：膨胀差和变形差；外部的冷却剂压力；由燃料元件中的裂变产物造成的额外内部压力；燃料组件中的燃料和其他材料的辐照；由功率需求的变化引起的压力与温度的变化；种种化学效应；静载荷和动载荷，包括流致振动和机械振动；以及可能由变形或化学效应引起的传热性能变化。必须给数据、计算和制造中的不确定性留有余地。

6.8. 规定的燃料设计限值，包括允许的裂变产物泄漏量，在正常运行中不得被超过；并且必须确保，在预计运行事件中可能存在的运行状况不会引起明显的进一步的恶化。裂变产物的泄漏量必须受设计限值的限制，并保持在最低值。

6.9. 燃料组件必须被设计得容许在辐照后对它们的构件和部件进行必要的检查。在设计基准事故中，燃料元件必须保持原位，并且其变形不得达到使事故后的堆芯得不到充分有效冷却的程度；为燃料元件规定的与设计基堆事故有关的限值不得被超过。

6.10. 对反应堆和燃料元件设计的上述要求，在核动力厂的整个运行寿期中当燃料管理方针改变或运行状况发生变化时，也必须仍然适用。

反应堆堆芯的控制

6.11. 对于在堆芯的所有状态下，包括在停堆后和在换料过程中或换料后的那些状态下，以及由预计运行事件与设计基准事故引起的那些状态下可能出现的一切中子通量水平和分布来说，第6.3—6.10条的规定必须得到遵守。必须提供探测这些通量分布的适当手段，足以确保堆芯中不存在第6.3—6.10条的规定有可能不被察觉地违背的区域。堆芯的设计必须充分地降低对控制系统提出的 关于在所有运行状态下把通量分布形状、水平和稳定性保持在规定限值内的要求。

6.12. 非放射性物质，包括腐蚀产物，可能损害系统的安全性，例如造成冷却剂通道堵塞，必须采取措施予以排除。

反应堆停堆

6.13. 必须提供手段，确保有能力使处于运行状态下和设计基准事件中的反应堆停堆；并确保即使堆芯处于反应性最大的状态下也能保持停堆状态。停堆手段的有效性、动作速度和停堆深度必须做到使规定限值不被超过。在正常功率运行时，可以将部分停堆手段用于控制反应性和通量整形，条件是要始终使停堆能力保持充足的裕量。

6.14. 反应堆停堆手段必须至少由两个不同的系统组成，以提供多样性。

6.15. 根据单一故障假设，这两个系统中必须至少有一个有能力独自使处于运行状态的和设计基准事故中的核反应堆迅速进入次临界，并具有足够的停堆深度。例外的是，只要不超过规定的燃料和部件限值，可以允许瞬发重返临界。

6.16. 即使堆芯处于反应性最大的状态下，这两个系统中也必须至少有一个有能力独自使处于正常运行状态、预计运行事件和设计基准事故中的反应堆进入次临界状态，并且以足够的停堆深度和高度的可靠性使反应堆保持次临界状态。

6.17. 在判断停堆手段的充分性时，必须考虑动力厂任何部分发生的、可能使停堆手段的一部分不起作用（例如控制棒不能插入）或可能引起共因故障的故障。

6.18. 停堆手段必须足以防止或承受停堆期间因引导入反应性，包括在停堆状态下进行换料，而引起的反应性意外增加。为满足这项规定，必须考虑在停堆状态下的会增加反应性的有意行动（例如为了维护的目的移动吸收体、使硼含量稀释和换料行动）以及停堆手段方面的单一故障。

6.19. 为确保停堆手段总是处于针对给定动力厂条件规定的状态，必须提供测量仪表，并规定必须进行哪些测试。

6.20. 在设计反应性控制器件时，必须考虑消耗和各种辐照效应，例如燃耗、物理性质的变化和气体的产生。

反应堆冷却剂系统

反应堆冷却剂系统的设计

6.21. 反应堆冷却剂系统、与它相关的辅助系统以及控制与保护系统，必须被设计得拥有足够的裕度，以确保在各种运行状态下反应堆冷却剂压力边界的设计条件不被超过。必须采取措施确保卸压装置的工作，即使在设计基准事故中，也不会导致动力厂中的放射性物质发生不可接受的释放。反应堆冷却剂压力边界必须装备足够的隔离装置，以限制放射性流体的损失。

6.22. 包容反应堆冷却剂的部件，诸如反应堆压力容器或压力管、管道和接头、阀门、配件、泵、循环泵和热交换器，以及固定这些部件的器件，都必须设计得能够承受预期在所有运行状态下和设计基准事故中会遇到的静载荷和动载荷。必须选择用于制造这些部件的材料，以便使材料的活化降到最低程度。

6.23. 反应堆压力容器和压力管的设计和建造，必须在材料、设计标准、可检查性和可制造性方面达到最高的质量。

6.24. 反应堆冷却剂承压边界必须设计成这样：极不可能产生裂纹；已产生的裂纹会按极不易导致裂口快速扩展的失稳断裂方式扩展，以便及时探知裂纹（例

如应用先漏后破概念）。必须避免可能使反应堆冷却剂压力边界的部件出现脆性行为的那些设计和动力厂状态。

6.25. 设计必须反映对边界材料在运行状态（包括维护和测试状态）下以及在设计基准事故工况中的所有工况下所作的考虑，同时必须考虑受到侵蚀、蠕变、疲劳、化学环境、辐射环境和老化的影响后的寿期末性质，以及在测定部件初始状态和可能的恶化速率方面的任何不确定性。

6.26. 泵叶轮和阀门零件之类被包于反应堆冷却剂压力边界内的部件，必须设计得在所有运行状态下和在设计基准事故中发生故障并随之引起一回路冷却剂系统中其他安全重要物项受损的可能性降至最低程度，同时对服役期间可能发生的恶化留出应有的裕度。

反应堆冷却剂压力边界的在役检查

6.27. 反应堆冷却剂压力边界的部件，必须设计、制造和布置得在动力厂的整个使用寿期内，都有可能以适当的时间间隔对压力边界进行充分的检查和测试。必须采取措施为反应堆冷却剂压力边界，尤其是高辐照部位，实施材料监测计划和酌情为其他重要部件实施同样的计划，以测定由结构材料的受辐照、应力腐蚀开裂的形成、热脆化和老化之类的因素引起的冶金学效应。

6.28. 必须确保有可能按照反应堆冷却剂压力边界部件对安全的重要性，直接地或间接地检查或测试它们，以证明不存在不可接受的缺陷，或有安全意义的恶化。

6.29. 必须对反应堆冷却剂压力边界完整性的指示物（例如泄漏）进行监测。在判定哪些检查对安全来说是必要的时，必须考虑这些监测的结果。

6.30. 如果核动力厂的安全分析表明二回路冷却系统中的某些特定故障有可能导致严重的后果，则必须确保能够检查二回路冷却系统的这些相关部分。

反应堆冷却剂的装量

6.31. 必须采取措施来控制冷却剂的装量和压力，以便在考虑到体积的变化和泄漏的情况下，确保在任何运行状态下都不超过所规定的设计限值。履行这一功能的那些系统，必须有足以满足这个要求的能力（流量和贮存容量）。它们可以由发电过程所需的部件组成，也可以是为执行这一功能专门配备的。

反应堆冷却剂的净化

6.32. 为了清除反应堆冷却剂中的放射性物质，包括活化了的腐蚀产物和从燃料中泄漏出的裂变产物，必须提供适当的设施。必要的系统的能力，必须以规定的有关容许泄漏量的燃料设计限值为基础确定，并留有较保守的裕度，以确保核动力厂能够以可合理达到地较低的回路活度水平运行，同时确保放射性释放量满足合理可行尽量低原则和处于规定限值以内。

堆芯余热的排出

6.33. 必须提供用于排出余热的手段。这些手段的安全功能必须以足够大的速率从反应堆堆芯中排出裂变产物衰变热和其他余热，使规定的燃料设计限值和反应堆冷却剂压力边界的设计基准限值不被超过。

6.34. 为了在假定发生单一故障和失去厂外电源的情况下仍有足够的可靠性以及在纳入适当的冗余性、多样性和独立性的条件下满足第6.33条的要求，必须提供互连和隔离能力以及相应的其他设计特点（例如泄漏探测能力）。

应急堆芯冷却

6.35. 必须提供在发生冷却剂丧失事故时对堆芯进行冷却的能力，从而把燃料的损伤降至最低程度，并限制裂变产物从燃料中逸出。所提供的冷却能力必须确保：

(1) 包壳或燃料完整性的限制性参数（例如温度）一定不超过用于设计基准事故的可接受数值（对适用的反应堆设计而言）；
(2) 可能的化学反应被限制在容许的水平；
(3) 燃料中的变化和内部结构变化不会明显地降低应急堆芯冷却手段的有效性；和
(4) 堆芯的冷却能持续足够长的时间。

6.36. 为了能在假定发生单一故障的情况下，针对每个假想始发事件，以足够大的可靠性满足这些要求，必须提供一些设计特征（例如泄漏探测能力、相应的互连能力和隔离能力）与适当的部件冗余性和多样性。

6.37. 必须对发生严重事故后延长从堆芯排出热量的能力，给予适当的考虑。

应急堆芯冷却系统的检查和测试

6.38. 必须将应急堆芯冷却系统设计得能容许对重要部件进行适当的定期检查和进行适当的定期测试，以达到下述目的：

(1) 证实其部件的结构完整性和密封完整性；
(2) 尽可能证实系统中的能动部件在正常运行时的可运行性和性能；和
(3) 尽实际可能地证实系统作为一个整体在设计基准中规定的动力厂状态下的可运行性。

把热量传给最终热阱

6.39. 为了将余热从安全重要构筑物、系统和部件传至最终热阱，必须提供一些系统。在运行状态和设计基准事故中，必须以极高的可靠性实现这种功能。所有（通过给传热系统输送热量、提供动力或供应流体）对传送热量有贡献的系统，都必须根据它们对整个传热功能的贡献大小加以设计。

6.40. 这些系统的可靠性，必须通过选择适当措施来实现，包括使用经验证的部件、冗余性、多样性、实体分隔、互连和隔离。

6.41. 在设计这些系统时，以及在选择可能是多样性的最终热阱与供应传热流体的贮存系统时，必须考虑自然现象和人因事件。

6.42. 必须对延长向最终热阱传送堆芯余热的能力给予充分的考虑，以确保一旦发生严重事故时，对包容放射性物质这一安全功能来说重要的构筑物、系统和部件能够维持可接受的温度。

安全壳系统

安全壳系统的设计

6.43. 为确保发生设计基准事故时，释放到环境中的放射性物质都能低于规定的限值，必须提供安全壳系统。根据设计要求的不同，这个系统可以包括：一些密封的构筑物；用于控制压力和温度的相关系统；以及用于隔离、管理与排除可能释放到安全壳大气中的裂变产物、氢气、氧气和其他物质的设施。

6.44. 在设计安全壳系统时，必须考虑所有已被确认的设计基准事故。此外，还必须考虑提供用于缓解经选择的部分严重事故后果的设施，以便限制放射性物质向环境的释放。

安全壳构筑物的强度

6.45. 包括出入口、贯穿件以及隔离阀在内的安全壳构筑物的强度，必须依据预计由设计基准事故引起的潜在的内部过压、欠压和温度，飞射物撞击之类动态效应，以及反作用力，加以计算，并留出足够的安全裕度。对于其他潜在的能量来源，例如包括可能的化学反应和辐射分解反应，其效应也必须加以考虑。在计算安全壳构筑物所需的强度时，必须考虑自然现象和人因事件，并且必须采取措施监测安全壳及其相关设施的状况。

6.46. 必须考虑考虑万一发生严重事故时保持安全壳完整性的措施。尤其是，必须考虑预计有可能发生的可燃气体燃烧的效应。

安全壳承压能力试验

6.47. 安全壳构筑物必须设计和建造成能够按规定的压力进行压力试验，以验证其在动力厂运行前和动力厂整个寿期内结构的完整性。

安全壳的泄漏

6.48. 安全壳系统必须设计成在发生设计基准事故时，规定的最大泄漏率不被超过。承压的主安全壳可以部分或全部地被二次封闭结构所围绕，以便收集和有控制地释放或贮存发生设计基准事故时可能从主安全壳中漏出的物质。

6.49. 安全壳构筑物及对安全壳系统的密封性有影响的设备与部件，必须被设计和建造成这样：在所有的贯穿件安装好以后，可在设计压力下测试泄漏率。必须能够在反应堆的整个使用寿期内，按一定的时间间隔，在安全壳的设计压力或可以估算出在安全壳设计压力下的泄漏率的降低了的压力下，测定安全壳系统泄漏率。

6.50. 对于万一发生严重事故时控制放射性物质从安全壳向外的任何泄漏的能力，必须给予适当的考虑。

安全壳贯穿件

6.51. 安全壳贯穿件的数目，必须保持实际可行的最低数目。

6.52. 安全壳的所有贯穿件，都必须满足与安全壳构筑物本身同样的设计要求。必须保护这些贯穿件免受由管道运动引起反作用力的影响，或由飞射物、喷射力和管道甩动引起的意外载荷的影响。

6.53. 如果有弹性的密封件（例如弹性体密封件或电缆贯穿件）或膨胀波纹管与贯穿件一起使用，则它们必须设计成有能力在安全壳设计压力下进行独立于确定安全壳整体的的泄漏率的泄漏试验，以验证它们在动力厂整个寿期内保持着完整性。

6.54. 必须适当考虑贯穿件在万一发生严重事故时仍能维持其功能的能力。

安全壳的隔离

6.55. 贯穿完全壳且作为反应堆冷却剂压力边界一部分的每条管线，或与安全壳的大气直接相通的每条管线，必须在发生设计基准事故时，能够自动地和可靠地封闭。在发生设计基准事故时，对于防止发生超过规定限值的向环境的放射性释放来说，安全壳的密封性是极其重要的。这些管线必须至少配备两个串接的合适的安全壳隔离阀（虽然一般情况下是将一个阀装在安全壳内侧，另一个装在安全壳外侧，但根据设计的不同，其他的安排也是可接受的），并且每个阀必须有能力可靠而独立地被触发。隔离阀必须安装在尽实际可能地靠近安全壳的位置。安全壳的隔离必须是在假定发生单一故障时可以实现的。如果适用这项要求会降低贯穿安全壳的安全系统的可靠性，则可使用别的隔离方法。

6.56. 贯穿反应堆主安全壳，而且既不是反应堆冷却剂压力边界的一部分也不是直接与安全壳大气相通的每条管线，必须至少配备一个合适的安全壳隔离阀。这个阀必须安装在安全壳外侧，并尽实际可能地靠近安全壳。

6.57. 必须适当考虑隔离装置在万一发生严重事故时保持其功能的能力。

安全壳的空气闸门

6.58. 人员出入安全壳时，必须穿过装有若干道门的空气闸门。这些门是联锁的，以确保反应堆运行期间和发生设计基准事故时，至少有一道门是关闭的。在规定人员可以在某些低功率运行期间进入安全壳进行监视的场合，必须在设

计中规定确保这些作业人员安全的措施。如果有设备空气闸门，这些要求也必须适用。

6.59. 必须适当考虑安全壳空气闸门在万一发生严重事故时保持其功能的能力。

安全壳的内部结构

6.60. 设计必须使安全壳内各个单独的隔间之间具有宽敞的气流通路。隔间之间各种开口的截面尺寸必须能确保在设计基准事故中的压力平衡期间发生的压力差，不会损坏承压结构或对于限制设计基准事故的效应来说重要的其他系统。

6.61. 必须适当考虑内部结构承受严重事故效应的能力。

排出安全壳中的热量

6.62. 排出反应堆安全壳中的热量的能力必须得到保证。在发生设计基准事故时意外地释放出高能流体以后，降低安全壳中的压力和温度并使之维持在可接受的低水平这种安全功能必须得到履行。根据单一故障假设，执行排出安全壳中热量这一功能的系统，必须有适当的可靠性和冗余性，以确保这种功能能得到履行。

6.63. 必须适当考虑万一发生严重事故时排出反应堆安全壳中热量的能力。

安全壳大气的监控和净化

6.64. 必须按下述需要提供一些系统，用于控制可能释放到反应堆安全壳中的裂变产物、氢气、氧气和其他物质：

(1) 减少发生设计基准事故时可能释放到环境中的裂变产物数量；和
(2) 发生设计基准事故时，控制安全壳大气中的氢气、氧气和其他物质的浓度，以防止发生可能危及安全壳完整性的爆燃或爆炸。

6.65. 根据单一故障假设，用于净化安全壳大气的系统在部件和设施方面必须具有适当的冗余性，以确保这类安全组合能够履行所需的安全功能。

6.66. 必须适当考虑万一发生严重事故时控制可能产生的或释放的裂变产物、氢气和其他物质的能力。

覆盖层和涂层

6.67. 必须仔细选择安全壳系统内的部件和结构的覆盖层和涂层，而且必须详细规定其使用方法，以确保这些部件和结构的安全功能得到履行，并在万一覆盖层和涂层质量变差时尽量减小对其他安全功能的干扰。

仪表和控制

对安全重要仪表和控制系统的总要求

6.68. 必须提供用于在正常运行、预计运行事件、设计基准事故和严重事故中使用的动力厂各种变量和系统的全程监测仪表，以确保能够得到有关动力厂状况的充足信息。必须提供用于测量能够影响裂变过程、反应堆堆芯完整性、反应堆冷却系统完整性和安全壳完整性的一切主要变量的仪表，以及用于获取可靠而安全地运行动力厂所需的动力厂任何信息的仪表。必须配备充足的自动记录装置，以测量冷却水的欠热裕量之类的任何安全重要导出参数。仪表必须针对有关的动力厂状况经环境合格鉴定，并足以测量动力厂的各种参数从而对事件进行分类以实施应急响应。

6.69. 必须提供仪表和记录设备，以确保得到进行下述两项活动所不可缺少的信息：监视设计基准事故的进程和最重要设备的状况；和尽可能按安全的需要，预测可能从设计中预定的一些部位逸出的放射性物质的位置和数量。仪表和记录设备必须足以按实际可能提供发生严重事故时判断动力厂状况和作出事故管理决定所需的信息。

6.70. 必须提供适当而可靠的监控设备，以便把第6.68条中提到的那些变量维持在规定的运行范围内。

控制室

6.71. 必须提供一个控制室，以便在那里使动力厂能够在其所有运行状态下安全运行，并且能够在那里采取措施，使动力厂保持在安全的状态之下，或在预计运行事件、设计基准事故和严重事故开始之后使动力厂返回到这样的状态。必须采取适当的措施和提供足够的信息，以保障控制室的人员免受继发性危害，例如由事故工况或释放的放射性物质引起的不适当的辐射水平，或出现爆炸性气体或有毒气体。这些因素都有可能妨碍操纵员采取必要的行动。

6.72. 必须特别注意找出控制室内部和外部的可能会直接威胁到控制室持续运行的事件。设计必须提供合理可行的措施，以便将这类事件的效应减至最小。

6.73. 仪表的布置和信息的显示方式，必须给运行人员提供有关动力厂状况和表现的充分而全面的描述。在设计控制室时，必须考虑人机工程学因素。

6.74. 必须提供这样的设备，它们能高效地给出已经偏离正常和可能影响安全的运行工况和过程的可视指示，如情况合适还给出可听的指示。

辅助控制室

6.75. 必须配备足够的仪表和控制设备，最好是一个在实体上和电气上与上述控制室相分离的单独场所（辅助控制室），以便万一在控制室丧失执行重要安全功能的能力时能够使反应堆置于和维持在停堆状态，能排出余热，并能监测最重要的动力厂变量。

在安全重要系统中使用基于计算机的系统

6.76. 如果设计可使一个安全重要系统借助于以计算机为基础的系统可靠地工作，则必须制定有关开发和试验计算机硬件和软件的相应标准与习惯做法，并在该系统的整个寿期，尤其是软件开发期内实施这些标准和做法。整个开发活动必须有相应的质量保证计划。

6.77. 系统所需要的可靠性水平必须与其安全重要性相称。所需要的这种可靠性水平，必须借助下述两种策略来实现：一是在这个过程的每个发展阶段使用各种相互补充的手段（包括有效的分析和试验制度）的全面策略；二是用来证实系统的设计要求已经实现的验证策略。

6.78. 在进行安全分析时针对以计算机为基础的系统假定的可靠性水平，必须包含规定的保守考虑，以补偿这种技术的固有复杂性，以及随之而来的分析方面的困难。

自动控制

6.79. 各种安全动作必须是自动的，以便在从预计运行事件或设计基准事故开始算起被证明是正当的一段时间内操纵员的动作是不需要的。此外，必须给操纵员提供相应的信息，以监视自动动作的效果。

保护系统的功能

6.80. 必须设计保护系统，以便：

(1) 自动促使相应系统运行必要时包括促使反应堆停堆系统运行，以确保不因所发生的预计运行事件而超过规定的设计限值；
(2) 探知设计基准事故，并促使必要的系统运行，以便把这种事故的后果限制在设计基准以内；和
(3) 能够克服控制系统的不安全动作。

保护系统的可靠性和可测试性

6.81. 保护系统必须设计得具有与拟执行的安全功能相称的高度可靠性和可定期测试性。设计中为保护系统提供的冗余性和独立性，至少必须足以确保：

(1) 任何单一故障都不会导致丧失保护功能；和
(2) 任何部件或通道的停役都不会导致丧失必要的最低限度冗余性，除非能够用其他方法证明该保护系统的运行可靠性仍然是可接受的。

6.82. 保护系统必须设计得能确保正常运行、预计运行事件或设计基准事故对冗余通道的影响不会导致其丧失功能；要不然就必须根据别的某种依据证明此种功能丧失是可接受的。必须尽实际可行地使用必要时包括自检能力的可测试性、故障安全的行为、功能多样性以及部件设计或运行原理方面的多样性之类的设计技术。

6.83. 保护系统必须设计得容许在反应堆运行时定期测试其履行功能的情况，包括有可能单独测试各个通道以确定是否可能已经发生了故障和丧失了冗余性，除非它的充分可靠性是借助别的某种手段确保的。设计必须容许从给出输入信号的传感器到最后的执行元件履行功能的所有环节，都能够在运行时得到试验。

6.84. 设计必须能在正常运行和发生预计运行事件时把操纵员的动作可能使保护系统的有效性丧失的可能性降至最小，但在发生设计基准事故时不否定操纵员采取的正确动作。

以计算机为基础的系统用于保护

6.85. 在打算将以计算机为基础的系统用于保护系统时，必须用下述要求补充第6.76—6.78条的那些要求：

(1) 必须使用质量最好的硬件和软件，并使用与这些硬件和软件有关的最好实践。

(2) 包括对设计变更的控制、测试和调试在内的整个开发过程，必须系统地形成文件，并且是可审查的；

(3) 为了坚定对以计算机为基础的系统的可靠性的信心，必须由独立于设计者和供应者的专家对这种以计算机为基础的系统进行评定；和

(4) 在无法以较高的置信度证明系统具有必要的完整性的场合，必须提供可保证能履行这种保护功能的其他不同的手段。

保护系统和控制系统的分离

6.86. 必须靠避免互连或靠适当的功能隔离，防止保护系统和控制系统互相干扰。如果信号是保护系统和任何控制系统共用的，则必须确保进行适当的分隔（例如采取能充分去耦合的措施）并且必须证明第6.80—6.85条的所有安全要求都能得到满足。

应急控制中心

6.87. 必须设置一个与动力厂的控制室分开的就地应急控制中心，作为万一发生紧急情况时应急人员集合并在那里进行操作的地点。那里必须能获得有关动力厂的重要参数和动力厂内及其邻近地区的放射学状况的信息。该中心必须备有必要的通信手段，以便与动力厂中的控制室、辅助控制室和其他重要地点以及现场和厂外应急机构联络。必须采取合适的措施保护这里的工作人员能足够长时间地免遭严重事故导致的危害。

应急动力供应

6.88. 在某些假想始发事件发生以后，各种安全重要系统和部件将需要应急动力。必须确保应急动力供应能够在任何运行状态或发生设计基准事故时，假定同时丧失厂外电源的情况下，供应必要的动力。对动力的需要将随假想始发事

件的性质的不同而不同。要执行的安全任务的性质将在选择每种任务所需的手段（例如它们的数目、可利用率、持续时间、容量和连续性）时得到反映。

6.89. 用于提供应急动力的复合手段（例如利用水轮机、汽轮机或燃气轮机、柴油机或蓄电池）必须具有与所要供应的安全系统的所有要求相一致的可靠性和形式，并必须假设发生单一故障时仍能执行其功能。必须能够试验应急动力供应履行功能的能力。

废物处理和控制系统

6.90. 必须为处理放射性的液体和气体流出物提供适当系统，以便把放射性排放物的数量与浓度保持在规定的限值以内。必须适用合理可行尽量低的原则。

6.91. 必须为操作放射性废物和为把这些废物在本厂区安全地贮存一段时间提供适当的系统。时间的长短与可在本厂区获得处置途径的时间相一致。从本厂区运出固体废物，必须按照主管部门的决定行事。

控制排入环境中的放射性液体

6.92. 核动力厂必须包括用于控制排入环境中的放射性液体的适当手段，以便符合合理可行尽量低原则，并确保排放量和浓度保持在规定的限值内。

控制气载放射性物质

6.93. 必须提供带有合适的过滤系统的通风系统，以便：

(1) 防止气载放射性物质在核动力厂内的扩散达到不可接受程度；
(2) 把气载放射性物质的浓度降到与进入特定区域的需要相容的水平；
(3) 把核动力厂内的气载放射性物质的水平保持在规定的限值以下，使合理可行尽量低原则在正常运行、预计运行事件和设计基准事故时得到适用；和
(4) 在不削弱对放射性释放的控制能力的情况下，给含有隋性气体或有害气体的房间通风。

控制释入环境的气态放射性物质

6.94. 必须提供带有相应过滤系统的通风系统，以便控制气载放射性物质释入环境，并且确保这种排放符合合理可行尽量低原则和处于规定限值内。

6.95. 过滤系统必须是足够可靠的且设计成能在预期的主导工况下实现必要的滞留因子。必须把过滤系统设计得能测试其效率。

燃料装卸和贮存系统

未辐照燃料的操作和贮存

6.96. 必须设计未辐照燃料的操作和贮存系统，以便：

(1) 利用物理手段或过程，最好使用几何安全的构形，确保即使在动力厂最佳慢化状态下也不会达到临界，并有一定的余量；
(2) 容许对安全重要部件进行适当的维护、定期检查和测试；和
(3) 把燃料的丢失或损坏的可能性降到最低。

辐照燃料的操作和贮存

6.97. 辐照燃料的操作和贮存系统必须设计成能够完成下述功能：

(1) 利用物理方法或过程，最好使用几何安全的构形确保即使在动力厂最佳慢化状态下也不会达到临界；
(2) 在运行状态下和在发生设计基准事故时，容许充分地排出热量；
(3) 容许对辐照燃料进行检查；
(4) 容许对安全重要部件进行适当的定期检查和测试；
(5) 防止乏燃料在转移时跌落；
(6) 防止给燃料元件或燃料组件施加不可接受的操作应力；
(7) 防止乏燃料贮运容器和起重机之类的重物或其他有可能造成损伤的物体意外地跌落在燃料组件上；
(8) 容许安全贮存可疑的或已受损的燃料元件或燃料组件；
(9) 提供必要的辐射防护手段；
(10) 给每个燃料模件妥善加上标识；
(11) 控制可溶吸收体的水平，如果它被用于临界安全的话；
(12) 便于燃料贮存和操作设施的维护和退役；

(13) 便于燃料操作和贮存场所和设备在必要时进行去污；和
(14) 确保能够执行合适的运作和衡算程序，以防止燃料的丢失。

6.98. 对于利用水池系统贮存燃料的反应堆来说，其设计必须提供下述手段：

(1) 用于控制任何辐照燃料在其中被操作或贮存的水的化学成分和活度的手段；
(2) 用于监测和控制燃料贮存池中的水位以及用于探知泄漏的手段；和
(3) 用于防止万一管道破裂时贮存池被排空的手段（即反虹吸措施）。

辐射防护 [3]

总的要求

6.99. 辐射防护的目标，是防止一切可避免的射线照射，并使不可避免的照射保持合理可行尽量低。在设计中，必须通过下述手段实现这一目标：

(1) 适当布置和屏蔽包含放射性物质的构筑物、系统和部件；
(2) 在动力厂和设备的设计中，注意尽量减少人在辐射场中活动的次数和持续时间，并减少现场工作人员的可能沾污；
(3) 作好以适当形式和条件处理放射性物质的准备，以便于处置、现场贮存或从厂区运出；和
(4) 为减少在动力厂内产生和散布的以及释放到环境中的放射性物质的数量和浓度作出安排。

6.100. 必须充分考虑辐射水平在工作人员活动区域内可能随时间积累和尽量减少作为废物的放射性物质的产生量。

辐射防护设计

6.101. 在动力厂的设计和布置中，必须为尽量减少所有来源的照射和沾污作出适当准备。这种准备必须包括在以下方面适当设计构筑物、系统和部件：尽量减少维护和检查时的照射；屏蔽直接辐射和散射辐射；用于控制空气载带的放射性物质的通风和过滤；采用适当规格的材料来限制腐蚀产物的活化；监测手段；动力厂的出入控制；以及适当的去污设施。

[3] 进一步的指导，见参考文献[6]。

6.102. 屏蔽设计必须使得运行区域内的辐射水平不超过规定限值，并且必须便于维护和检查以尽量减少维护人员的照射。必须实行合理可行尽量低原则。

6.103. 动力厂布置和工作规程必须就辐射和潜在沾污区域的出入控制以及尽量减少由动力厂内放射性物质和工作人员的移动造成的沾污做出规定。动力厂布置必须为根据需要进行高效率的运行、检查、维护和更换准备条件，以尽量减少射线照射。

6.104. 必须为工作人员和设备提供适当的去污设施并为操作由去污活动产生的所有放射性废物作好准备。

辐射监测手段

6.105. 必须提供设备确保在运行状态、设计基准事故中和根据实际情况在严重事故中有足够的辐射监测：

(1) 为了在平常有运行人员活动的地方和在正常运行或预计运行事件中辐射水平的变化使得人员进入在某段时间内必须加以限制的地方监测局部辐射剂量率，必须提供固定式剂量率计。另外，必须安装固定式剂量率计，用以在设计基准事故和尽实际可能在严重事故下在适当的地点指示总的辐射水平。这些仪表必须在控制室或动力厂工作人员能根据需要采取纠正行动的适当控制地点给出充分的信息。

(2) 为了在平常有运行人员活动的区域和预期空气载带的放射性物质的活度水平偶尔会达到必须采取保护措施水平的场合测量大气中放射性物质的活度，必须提供监测器。当探测到高浓度放射性核素时，这些系统必须在控制室或其他适当地点给出指示。

(3) 为了及时测定流体工艺系统（如适用）中以及在运行状态和事故工况下从动力厂系统或环境所取气体和液体样品中的选定放射性核素浓度，必须提供固定式设备和实验室设施。

(4) 为了在排放到环境之前或排放过程中监测排出流，必须提供固定式设备。

(5) 必须提供测量表面放射性沾污的仪表。

(6) 必须提供监测工作人员个人剂量和沾污的设施。

6.106. 除了在动力厂内监测之外，还必须作出安排，测定动力厂周围的放射学影响，如果存在的话。具体来说，指：

(1) 接近居民的途径，包括食物链；

(2) 对当地生态系统的放射学影响，如果存在的话；

(3) 放射性物质在实物环境中可能的积累；和

(4) 存在任何未许可排放路径的可能性。

附 件 I

假想始发事件

I.1. 本附件详细叙述假想始发事件（PIE）的定义及其概念的应用。

I.2. 假想始发事件定义为在设计时确定的能导致预计运行事件或事故工况的事件。这意味着假想始发事件本身并不是事故；它只是引发了一连串的事件并且因为所发生的其他故障而导致运行事件、设计基准事故或严重事故。典型的例子是设备故障（包括管道破裂）、人为差错、人因事件和自然事件。

I.3. 假想始发事件可能是具有较小后果类型的，例如冗余部件的故障；它也可能具有严重后果，例如反应堆冷却剂系统的主要管道故障。设计的主要目标是使动力厂具有这样的特性：确保大多数假想始发事件具有较小甚至不明显的后果；如果其余的假想始发事件导致设计基准事故，确保后果是可以接受的；而如果导致严重事故，确保后果可以通过设计特征和事故管理加以限制。

I.4. 需要设想所有的事件，以便确保对所有具有潜在严重后果和显著概率的可信事件都作了事先准备，动力厂设计对它们都能承受。没有可靠的准则指导假想始发事件的选择；更确切地说，这是一个在设计与分析、工程判断及来自以前动力厂设计和运行的经验之间组合迭代的过程。排除一个特定事件序列需要经过合理判断。

I.5. 在制订安全重要物项的性能要求和进行动力厂全面安全评定时要用的假想始发事件的数目应该受到限制，以使得这项任务实际可行，而这是通过把详细分析限于若干有代表性的事件序列[4]来完成的。有代表性的事件序列确定了极限案例并提供了安全重要构筑物、系统和部件的数值设计限值的基础。

I.6. 某些假想始发事件可以根据以前动力厂的经验、国家许可证审批机构的具体要求，多半还有可能后果的严重程度等诸多因素用确定论方法加以规定。而另一些假想始发事件则可以用概率分析之类的系统方法加以规定，因为设计的具体特征、动力厂的位置或运行经验能使它们的特性用概率加以量化。

---

[4] 词组“事件序列”或“事件的序列”用来表示一个假想始发事件与随后的操纵员动作或安全重要物项动作的组合。

假想始发事件的类型

内部事件

设备故障

I.7. 始发事件可以是能直接或间接影响动力厂安全的个别设备故障。列有这些事件的事件表充分反映了动力厂系统和部件的所有可信故障。

I.8. 需要考虑的故障类型取决于所涉系统或部件的种类。最广泛意义上的故障，或者是系统或部件失去完成其功能的能力，或者是执行了不希望有的功能。例如，管道故障可以是泄漏、破裂或者流道阻塞。对于阀门之类的能动部件，故障可能采取这样的形式：当需要时不能打开或关闭；当不需要时打开或关闭；部分打开或关闭；或者以不当的速度打开或关闭。对于仪表传感器之类的装置，故障可能采取误差超出允许误差带、没有输出、恒定最大输出、不规则输出或以上情况的组合等形式。

I.9. 随着在安全应用和要害安全应用中基于计算机的系统的使用逐渐增多，硬件故障或不正确的软件程序可能导致重大的控制行动；应该考虑到这种可能性。

人为差错

I.10. 在许多情况下，人为差错的后果会类似于部件故障的后果。人为差错有多种情况，从错误的或不完全的维护操作，到不正确地设定控制设备限值或者错误的或遗忘的操纵员动作（工作差错和疏漏差错）。

其他内部事件

I.11. 由内部原因造成的火灾、爆炸和水淹也可能对动力厂的安全性能有重要影响，因此在编纂假想始发事件表时一般将它们列入其中。

外部事件

I.12. 在安全丛书No.50-C-S（Rev.1）《核动力厂安全法规：选址》[6]及其有关安全导则中给出动力厂外部事件的实例及有关设计基准输入数据的确定方

法。在动力厂物项的设计中，一般必须考虑这些事件造成的附加的振动、冲击和脉冲型载荷。

I.13. 如果可以推断一个安全重要构筑物、系统或部件因自然或人为外部事件造成故障的可能性由于适当的设计和建造而低到可以接受，由该事件引起的故障就不需要列入动力厂的设计基准。

事件组合

I.14. 在分析事故时需要注意各事件的组合，确保这种具体组合有一定的道理。事件的随机组合可能是一种极不可能的情景，在概率安全分析中应表现为十分少见而不必重视，勿需作为假想事故。在概率安全分析中，对严重事故采取使用最佳估计分析的方法；而对具有较高发生可能性的假想事故，在分析方案中应采取保守的方法。

I.15. 在确定把哪些事件组合在一起时，考虑以下三个时期是有用的：

— 长期，在所考虑的具体事件之前；
— 短期，包括事件的发生及其短期效应；和
— 事件后恢复期。

I.16. 对于在发生另一个事件很久以前发生的一个事件，如果在动力厂设计中已经纳入对其正确识别的措施而且采取纠正行动所需的时间很短，就可以认为已经对这一事件采取了纠正行动。在这种情况下，勿需考虑这些事件的组合。

I.17. 对于短期（持续时间通常为几个小时）来说，各个事件发生的预期概率可能是这样的：随机发生的组合将被认为是不可信的情景。

I.18. 对于事件后恢复期（几天或更长）来说，可能需要考虑另外的事件，这取决于恢复期的长短和事件的预期概率。对于恢复期可以现实地假定，必须考虑成为一个组合发生的一个事件的严重程度，不比在相当于动力厂寿期的时期内考虑同一种事件需要假定的严重程度大。例如在失去冷却剂事故的恢复期中，如果需要考虑与一次地震的随机组合，其严重程度可取为低于动力厂设计基准地震的严重程度。

附 件 II

冗余性、多样性和独立性

II.1. 为了达到和保持与在有关纵深防御层次上要执行的安全功能的重要性相称的必要可靠性，本附件提出几种设计措施，必要时可以综合使用。

II.2. 虽然对于每一纵深防御层次各自的可靠性要求不能给出普遍适用的定量指标，但是最大的重点应放在第一层次上。这也与营运单位关于动力生产厂应有高可利用率的目标一致。

II.3. 作为一项指导原则或者为了用作监管机构同意的验收标准，对于某些安全系统可以规定最大不可利用率限值，以确保执行安全功能所需的可靠性。

共因故障

II.4. 一个特定事件或原因可能引起若干装置或部件不能执行其功能。这种故障可以同时影响若干不同的安全重要物项。这个事件或原因可以是设计缺陷、制造缺陷、运行或维护差错、自然现象、人因事件或动力厂内任何其他作业或故障引起的意外级联效应。

II.5. 当若干同一类型的部件同时损坏时，也可能发生共因故障。这可能是由周围条件改变、信号饱和、重复的维护差错或设计缺陷等原因造成的。

II.6. 在设计中按实际可能采取尽量减小共因故障效应的适当措施，如冗余性、多样性和独立性。

冗余性

II.7. 冗余性，即使用多于最少套数的设备去执行一项给定的安全功能，是实现安全重要系统高可靠性和满足安全系统单一故障准则的一项重要设计原则。冗余性使得至少一套设备的故障或不可用能够被允许而不丧失功能。例如，为执行一项具体功能可以提供三四台泵，而有任何两台就足够了。为了实现冗余性，可以使用相同的部件，也可以使用不同的部件。

多样性

II.8. 某些系统的可靠性可以通过使用多样性原理来减小发生某些共因故障的可能性而得到提高。

II.9. 多样性适用于执行同一安全功能的冗余系统或部件，方法是在这些系统或部件中纳入各种不同的属性。这种属性例如可以是不同的工作原理、不同的物理变量、不同的运行条件或由不同的制造商生产。

II.10. 应该小心确保所使用的任何多样性在竣工设计中实际达到所希望的可靠性提高。例如，为了减少发生共因故障的可能性，设计者应研究将多样性用于材料、部件和制造过程中的任何相似性或者工作原理或共用支持设施的细微相似性。如果使用了多样的部件或系统，就应合理保证在考虑了诸如运行、维护和测试规程的额外复杂性或因此而使用可靠性较低的设备之类不利因素后这种多样性的增加在总体上是有利的。

独立性

II.11. 系统的可靠性可以通过在设计中保持如下的独立性特征而得到改善：

— 各冗余系统部件之间的独立性；
— 系统部件和假想始发事件效应之间的独立性，例如一个假想始发事件不会引起缓解该事件后果所必需的安全系统故障或安全功能丧失；
— 不同安全级的系统或部件之间的适当独立性；和
— 安全重要物项和非安全重要物项之间的独立性。

II.12. 在系统设计中通过利用功能隔离和实体分隔实现独立性：

（1） *功能隔离*

应使用功能隔离来减少冗余或互联系统的设备和部件之间因正常或异常运行或者系统中任何部件的故障所造成的不利相互影响的可能性。

（2） *实体分隔和动力厂部件的布置*

在系统布置和设计中应尽实际可能采取实体分隔，以增强实现独立性的保证，尤其是对某些共因故障来说。

实体分隔包括：

— 利用几何条件（如距离或方位）分隔；

— 利用屏障分隔；或
— 利用上述二者结合分隔。

分隔方式的选择将取决于在设计基准中所考虑的假想始发事件，视具体情况例如火灾、化学爆炸、飞机坠落、飞射物撞击、洪水、极端温度或湿度的影响。

II.13. 动力厂的某些区域趋向于成为安全上重要的设备或各级（各类）导线的自然会聚中心。这种中心的实例可以是安全壳贯穿件、电机控制中心、电缆铺设室、设备间、控制室和动力厂过程计算机。在这样的地点应按实际可能尽量采取适当措施来避免共因故障。

参考文献

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, The Safety of Nuclear Installations, Safety Series No. 110, IAEA, Vienna (1993).

[2] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Defence in Depth in Nuclear Safety, INSAG-10, IAEA, Vienna (1996).

[3] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3 Rev. 1, INSAG-12, IAEA, Vienna (1999).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Quality Assurance for Safety in Nuclear Power Plants and other Nuclear Installations, Code and Safety Guides Q1-Q14, Safety Series No. 50-C/SG-Q, IAEA, Vienna (1996).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Code on the Safety of Nuclear Power Plants: Siting, Safety Series No. 50-C-S (Rev. 1), IAEA, Vienna (1988).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL LABOUR ORGANISATION, NUCLEAR ENERGY AGENCY OF THE ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, PAN AMERICAN HEALTH ORGANIZATION, WORLD HEALTH ORGANIZATION, International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources, Safety Series No. 115, IAEA, Vienna (1996).

附 录

沸水反应堆、压水反应堆和压力管反应堆所需的安全功能

A-1. 本附录给出把第4.06条中定义的三种基本安全功能进一步详细划分的实例。

A-2. 这些安全功能包括防止事故工况和缓解事故工况后果所需的功能。根据具体情况，它们可以利用为正常运行、为防止预计运行事件导致事故工况或为缓解事故工况后果而提供的构筑物、系统或部件来实现。

A-3. 对各种反应堆设计的考察表明，目前的设计安全要求可以通过采用执行下述安全功能的构筑物、系统或部件来满足：

（1） 防止不可接受的反应性瞬变；
（2） 在所有停堆行动后保持反应堆处于安全停堆状态；
（3） 为防止预计运行事件导致设计基准事故而在必要时停堆和为缓解设计基准事故的后果而停堆；
（4） 在不涉及反应堆冷却剂压力边界破坏的事故工况之中和之后保持有足够的反应堆冷却剂存量冷却堆芯；
（5） 在设计基准中考虑的所有假想始发事件之中和之后保持有足够的反应堆冷却剂存量冷却堆芯；
（6） 在反应堆冷却剂压力边界破坏之后从堆芯排热[1]以限制燃料损坏；
（7） 在适当的工作状态和反应堆冷却剂压力边界保持完整的事故工况下排出余热（见脚注1）；
（8） 从另外的安全系统向最终热阱传热[2]；
（9） 确保必要的服务（如电源、压缩空气源、液压动力源、润滑）作为对安全系统的一种支持功能；
（10）保持反应堆堆芯燃料包壳的完整程度可以接受；
（11）保持反应堆冷却剂压力边界的完整性；
（12）在事故工况下和事故后限制放射性物质从反应堆安全壳释放；

---

[1] 这一安全功能适合于排热系统的第一步，其他步骤包括在安全功能（8）中。

[2] 当另外的安全系统必须执行其安全功能时，这是对它们的一种支持功能。

（13）在设计基准事故和从反应堆安全壳以外的源释放放射性物质的选定严重事故之中和之后限制公众和现场工作人员的射线照射；

（14）限制所有运行状态下放射性废物和空气载带放射性物质的排放或释放，使之低于规定限值；

（15）对动力厂内的环境条件保持控制，以便于安全系统的运行并适合于进行安全重要操作所必需的工作人员在其中居留；

（16）在所有运行状态下对运至或贮存在反应堆冷却剂系统之外但仍在厂区之内的辐照燃料的放射性释放保持控制；

（17）从贮存在反应堆冷却剂系统之外但仍在厂区之内的辐照燃料排出衰变热；

（18）使贮存在反应堆冷却剂系统之外但仍在厂区之内的燃料保持足够的次临界度；

（19）对于其故障会引起安全功能破坏的构筑物、系统或部件，要防止其故障或限制其故障的后果。

A-4. 这张安全功能清单可以用作确定一个构筑物、系统或部件是否执行或有助于实现一项或多项安全功能的基础，并为有助于实现各种安全功能的安全构筑物、系统和部件指定适当的重要性等级提供基础。

术 语 表

能动部件。依靠触发、机械运动或动力源等外部输入工作的部件。

共因故障。两个或多个构筑物、系统或部件由单一特定事件或原因造成的故障。

多样性。有两个或多个冗余部件或系统执行同一功能，而这些不同的部件或系统具有不同的属性，从而减少了共因故障的可能性。

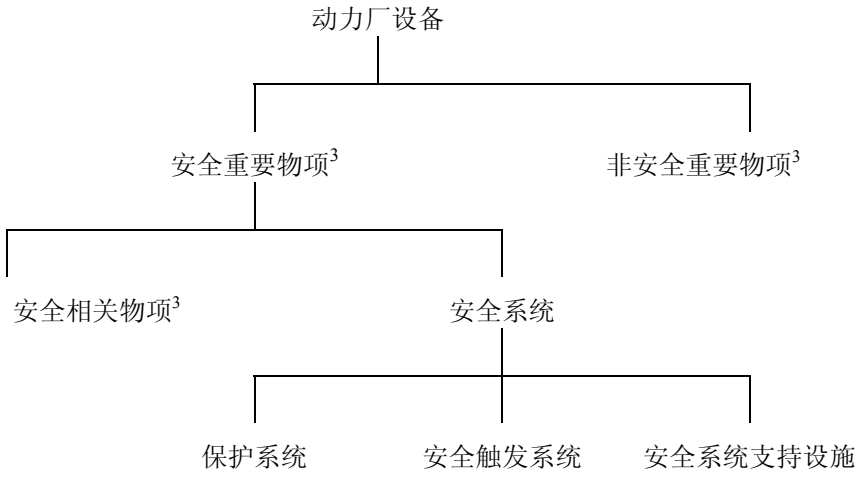
功能隔离。防止一条线路或一个系统的运行或故障模式影响另一线路或系统。

安全重要物项。属于一个安全组合的一部分和/或其失效或故障可能导致现场工作人员或公众受到射线照射的物项。

非能动部件。不依靠触发、机械运动或动力源等外部输入工作的部件。

实体分隔。由几何条件（距离、方位等）、适当的屏障或二者结合形成的隔离。

动力厂设备：



[3] 此处“物项”系指构筑物、系统或部件。

动力厂状态：

运行状态		**事故工况**			
				超设计基准事故	
正常运行	预计运行事件	(a)	设计基准事故	(b)	严重事故
				事故管理	

(a) 没有明确地被视为设计基准事故但被纳入设计基准事故范围的事故工况。

(b) 没有造成堆芯性能明显下降的超设计基准事故。

事故工况。比预计运行事件更严重地偏离正常运行，包括设计基准事故和严重事故。

事故管理。在超设计基准事故演变过程中采取一系列行动：

— 防止事件逐步升级为严重事故；
— 缓解严重事故的后果；和
— 达到长期安全稳定状态。

预计运行事件。在设施运行寿期内预计至少出现一次的偏离正常运行的运行过程。由于设计中已采取了相应措施，这类事件不会造成安全重要物项的严重损坏，也不会导致事故工况。

设计基准事故。在核动力厂的设计中按照已建立的设计准则作了针对性准备并且燃料损坏和放射性物质释放保持在许用限值内的事故工况。

正常运行。在规定运行限值和条件下的运行。

运行状态。正常运行和预计运行事件两类状态的统称。

严重事故。比设计基准事故更加严重并且造成堆芯性能明显下降的事故工况。

假想始发事件[4]。在设计时确定的能导致预计运行事件或事故工况的事件。

保护系统。监测反应堆运行并根据感知的异常工况自动触发防止不安全或可能不安全 工况的动作的系统。

安全功能。为安全而必须达到的特定目的。

[4] 进一步的资料见附件I。

安全组合。针对某一具体的假想始发事件，为完成确保不超过在预计运行事件和设计基准事故的设计基准中规定的限值所需要的全部动作而指定的设备的组合。

安全系统。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设计基准事故的后果。

安全系统整定值。为防止超过安全限值，在发生预计运行事件或事故工况时自动启动保护装置的触发点。

单一故障。造成部件失去完成其预定安全功能的能力的故障，以及由它所造成的所有继发性故障。

最终热阱。一种总是能把余热传输至其中的介质，即使所有其他排出余热的手段都已丧失或不足时也是如此。

参加起草和审定人员

Allen, P.	加拿大原子能有限公司
Cowley, J.S.	英国皇家核设施检查机构
De Munk, P.	荷兰社会事务和就业部
Feron F.	法国核设施安全部
Foskolos, K.	瑞士保罗•谢尔研究所
Frisch, W.	德国设施和反应堆安全公司
Gasparini M.	国际原子能机构
Hardin, W.	美利坚合众国核管理委员会
Kavun, O.	俄罗斯联邦原子能项目
Omoto, A.	日本东京电力公司
Park, D.	大韩民国核安全研究所
Price, E.G.	加拿大原子能有限公司
Simon, M.	德国设施和反应堆安全公司
Tripputi, I.	意大利国家电力公司
Vidard, M.	法国电力公司/Septen

认可安全标准的咨询机构

核安全标准咨询委员会

比利时: Govaerts, P. (主席); 巴西: da Silva, A.J.C.; 加拿大: Wigfull, P.; 中国: Lei, Y.; Zhao, Y.; 捷克共和国: Stuller, J.; 芬兰: Salminen, P.; 法国: Saint Raymond, P.; 德国: Wendling, R.D., Sengewein, H., Krüger, W.; 印度: Venkat Raj, V.; 日本: Tobioka, T.; 大韩民国: Moon, P.S.H.; 荷兰: de Munk, P., Versteeg, J.; 俄罗斯联邦: Baklushin, R.P.; 瑞典: Viktorsson, C., Jende, E.; 英国: Willby, C., Pape, R.P.; 美利坚合众国: Morris, B.M.; 国际原子能机构: Lacey, D.J. (协调员); 经济合作与发展组织核能机构: Frescura, G., Royen, J.

安全标准咨询委员会

阿根廷: Beninson, D.; 澳大利亚: Lokan, K., Burns, P; 加拿大: Bishop, A. (主席), Duncan, R.M.; 中国: Huang, Q., Zhao, C.; 法国: Lacoste, A.-C., Asty, M.; 德国: Hennenhöfer, G., Wendling, R.D.; 日本: Sumita, K., Sato, K.; 大韩民国: Lim, Y.K.; 斯洛伐克共和国: Lipár, M., Misák, J.; 西班牙: Alonso, A., Trueba, P.; 瑞典: Holm, L-E.; 瑞士: Prêtre, S.; 英国: Williams, L.G., Harbison, S.A.; 美利坚合众国: Travers, W.D., Callan, L.J., Taylor, J.M.; 国际原子能机构: Karbassioun, A. (协调员); 国际放射防护委员会: Valentin, J.; 经济合作与发展组织核能机构: Frescura, G.

该出版物已被第 SSR-2/1 (Rev. 1) 号取代。