国际原子能机构安全标准

保 护 人 类 与 环 境

核电厂结构、系统和部件的安全分级

特定安全导则

第 SSG-30 号

IAEA
国 际 原 子 能 机 构

国际原子能机构安全标准和相关出版物

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之危险的安全标准，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。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**。

有关国际原子能机构安全标准计划的资料可访问以下国际原子能机构因特网网站：

www.iaea.org/zh/shu-ju-ku/an-quan-biao-zhun

该网站提供已出版安全标准和安全标准草案的英文文本。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以及正在制订中的安全标准状况报告也在该网站提供使用。欲求进一步的信息，请与国际原子能机构联系（Vienna International Centre, PO Box 100, 1400 Vienna, Austria）。

敬请国际原子能机构安全标准的所有用户将使用这些安全标准的经验（例如作为国家监管、安全评审和培训班课程的依据）通知国际原子能机构，以确保这些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站提供或按上述地址邮寄或通过电子邮件发至 Official.Mail@iaea.org。

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成员国的居间人。

核活动的安全报告以**《安全报告》**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以**《应急准备和响应》**出版物、**《放射学评定报告》**、国际核安全组的**《核安全组报告》**、**《技术报告》**和**《技术文件》**的形式印发。国际原子能机构还印发放射性事故报告、培训手册和实用手册以及其他特别安全相关出版物。

安保相关出版物以**国际原子能机构《核安保丛书》**的形式印发。

国际原子能机构《核能丛书》由旨在鼓励和援助和平利用原子能的研究、发展和实际应用的资料性出版物组成。它包括关于核电、核燃料循环、放射性废物管理和退役领域技术状况和进展以及经验、良好实践和实例的报告和导则。

核电厂结构、系统和部件的安全分级

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
安提瓜和巴布达
阿根廷
亚美尼亚
澳大利亚
奥地利
阿塞拜疆
巴哈马
巴林
孟加拉国
巴巴多斯
白俄罗斯
比利时
伯利兹
贝宁
多民族玻利维亚国
波斯尼亚和黑塞哥维那
博茨瓦纳
巴西
文莱达鲁萨兰国
保加利亚
布基纳法索
佛得角
布隆迪
柬埔寨
喀麦隆
加拿大
中非共和国
乍得
智利
中国
哥伦比亚
科摩罗
刚果
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
吉布提
多米尼克
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
斯威士兰
埃塞俄比亚
斐济
芬兰
法国
加蓬
冈比亚
格鲁吉亚
德国
加纳
希腊
格林纳达
危地马拉
圭亚那
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
老挝人民民主共和国
拉脱维亚
黎巴嫩
莱索托
利比里亚
利比亚
列支敦士登
立陶宛
卢森堡
马达加斯加
马拉维
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
黑山
摩洛哥
莫桑比克
缅甸
纳米比亚
尼泊尔
荷兰
新西兰
尼加拉瓜
尼日尔
尼日利亚
北马其顿
挪威
阿曼
巴基斯坦
帕劳
巴拿马
巴布亚新几内亚
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
卢旺达
圣基茨和尼维斯
圣卢西亚
圣文森特和格林纳丁斯
萨摩亚
圣马力诺
沙特阿拉伯
塞内加尔
塞尔维亚
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
多哥
汤加
特立尼达和多巴哥
突尼斯
土耳其
土库曼斯坦
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
瓦努阿图
委内瑞拉玻利瓦尔共和国
越南
也门
赞比亚
津巴布韦

国际原子能机构的《规约》于 1956 年 10 月 23 日经在纽约联合国总部举行的原子能机构《规约》会议核准，并于 1957 年 7 月 29 日生效。原子能机构总部设在维也纳，其主要目标是“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《安全标准丛书》第 SSG-30 号

核电厂结构、系统和部件的安全分级

特定安全导则

国 际 原 子 能 机 构
2023 年 · 维也纳

版 权 说 明

Marketing and Sales Unit,
Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
传真：+43 1 2600 22529
电话：+43 1 2600 22417
电子信箱：sales.publications@iaea.org
https://www.iaea.org/zh/chu-ban-wu

国际原子能机构印刷
2023 年 9 月 • 奥地利

核电厂结构、系统和部件的安全分级

国际原子能机构，奥地利，2023 年 9 月
STI/PUB/1639
ISBN 978-92-0-501223-0（简装书：碱性纸）
978-92-0-500224-8（pdf 格式）
ISSN 1020-5853

前　言

国际原子能机构（原子能机构）《规约》授权原子能机构“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”。这些标准是原子能机构在其本身的工作中必须使用而且各国通过其对核安全和辐射安全的监管规定能够适用的标准。原子能机构与联合国主管机关及有关专门机构协商进行这一工作。定期得到审查的一整套高质量标准是稳定和可持续的全球安全制度的一个关键要素，而原子能机构在这些标准的适用方面提供的援助亦是如此。

原子能机构于 1958 年开始实施安全标准计划。对质量、目的适宜性和持续改进的强调导致原子能机构标准在世界范围内得到了广泛使用。《安全标准丛书》现包括统一的《基本安全原则》。《基本安全原则》代表着国际上对于高水平防护和安全必须由哪些要素构成所形成的共识。在安全标准委员会的大力支持下，原子能机构正在努力促进全球对其标准的认可和使用。

标准只有在实践中加以适当应用才能有效。原子能机构的安全服务涵盖设计安全、选址安全、工程安全、运行安全、辐射安全、放射性物质的安全运输和放射性废物的安全管理以及政府组织、监管事项和组织中的安全文化。这些安全服务有助于成员国适用这些标准，并有助于共享宝贵经验和真知灼见。

监管安全是一项国家责任。目前，许多国家已经决定采用原子能机构的标准，以便在其国家规章中使用。对各种国际安全公约缔约国而言，原子能机构的标准提供了确保有效履行这些公约所规定之义务的一致和可靠的手段。世界各地的监管机构和营运者也适用这些标准，以加强核电生产领域的安全以及医学、工业、农业和研究领域核应用的安全。

安全本身不是目的，而是当前和今后实现保护所有国家的人民和环境的目标的一个先决条件。必须评定和控制与电离辐射相关的危险，同时杜绝不当限制核能对公平和可持续发展的贡献。世界各国政府、监管机构和营运者都必须确保有益、安全和合乎道德地利用核材料和辐射源。原子能机构的安全标准即旨在促进实现这一要求，因此，我鼓励所有成员国都采用这些标准。

秘书处的说明

国际原子能机构安全标准反映有关保护人类和环境免于电离辐射有害影响的高水平安全构成要素方面的国际共识。制定、审查和确定原子能机构标准的过程涉及原子能机构秘书处和所有成员国，其中许多成员国委派代表参加了原子能机构的四个安全标准分委员会和原子能机构安全标准委员会。

秘书处、各安全标准分委员会和安全标准委员会定期对作为全球安全制度之关键要素的原子能机构标准进行审查。秘书处收集关于在适用原子能机构标准方面的经验信息以及从事件后续行动中获得的资料，以确保这些标准继续满足用户的需求。本出版物反映直至 2010 年所积累的反馈和经验，并经过了对标准而言的严格审查过程。

从研究 2011 年 3 月 11 日灾难性地震和海啸后日本福岛第一核电站事故中可能汲取的教训将在今后经修订和印发的这一原子能机构安全标准中予以反映。

国际原子能机构安全标准

背景

放射性是一种自然现象，因而天然辐射源的存在是环境的特征。辐射和放射性物质具有许多有益的用途，从发电到医学、工业和农业应用不一而足。必须就这些应用可能对工作人员、公众和环境造成的辐射危险进行评定，并在必要时加以控制。

因此，辐射的医学应用、核装置的运行、放射性物质的生产、运输和使用以及放射性废物的管理等活动都必须服从安全标准的约束。

对安全实施监管是国家的一项责任。然而，辐射危险有可能超越国界，因此，国际合作的目的就是通过交流经验和提高控制危险、预防事故、应对紧急情况和减缓任何有害后果的能力来促进和加强全球安全。

各国负有勤勉管理义务和谨慎行事责任，而且理应履行其各自的国家和国际承诺与义务。

国际安全标准为各国履行一般国际法原则规定的义务例如与环境保护有关的义务提供支持。国际安全标准还促进和确保对安全建立信心，并为国际商业与贸易提供便利。

全球核安全制度已经建立，并且正在不断地加以改进。对实施有约束力的国际文书和国家安全基础结构提供支撑的原子能机构安全标准是这一全球性制度的一座基石。原子能机构安全标准是缔约国根据这些国际公约评价各缔约国遵约情况的一个有用工具。

原子能机构安全标准

原子能机构安全标准的地位源于原子能机构《规约》，其中授权原子能机构与联合国主管机关及有关专门机构协商并在适当领域与之合作，以制定或采取旨在保护健康及尽量减少对生命与财产之危险的安全标准，并对其适用作出规定。

为了确保保护人类和环境免受电离辐射的有害影响，原子能机构安全标准制定了基本安全原则、安全要求和安全措施，以控制对人类的辐射照射和放射性物质向环境的释放，限制可能导致核反应堆堆芯、核链式反应、辐射源或任何其他辐射源失控的事件发生的可能性，并在发生这类事件时减轻其后果。这些标准适用于引起辐射危险的设施和活动，其中包括核装置、辐射和辐射源利用、放射性物质运输和放射性废物管理。

安全措施和安保措施 [1] 具有保护生命和健康以及保护环境的共同目的。安全措施和安保措施的制订和执行必须统筹兼顾，以便安保措施不损害安全，以及安全措施不损害安保。

原子能机构安全标准反映了有关保护人类和环境免受电离辐射有害影响的高水平安全在构成要素方面的国际共识。这些安全标准以原子能机构《安全标准丛书》的形式印发，该丛书分以下三类（见图 1）。

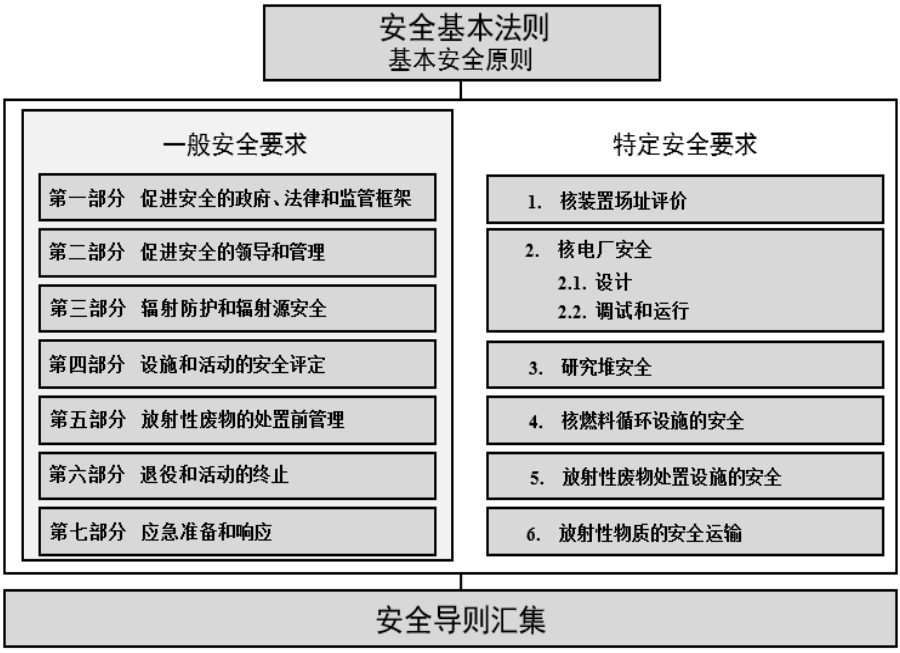

图 1. 国际原子能机构《安全标准丛书》的长期结构。

[1] 另见以原子能机构《核安保丛书》印发的出版物。

安全基本法则

“安全基本法则”阐述防护和安全的基本安全目标和原则，以及为安全要求提供依据。

安全要求

一套统筹兼顾和协调一致的“安全要求”确定为确保现在和将来保护人类与环境所必须满足的各项要求。这些要求遵循“安全基本法则”提出的目标和原则。如果不能满足这些要求，则必须采取措施以达到或恢复所要求的安全水平。这些要求的格式和类型便于其用于以协调一致的方式制定国家监管框架。这些要求包括带编号的“总体”要求用“必须”来表述。许多要求并不针对某一特定方，暗示的是相关各方负责履行这些要求。

安全导则

“安全导则”就如何遵守安全要求提出建议和指导性意见，并表明需要采取建议的措施（或等效的可替代措施）的国际共识。“安全导则”介绍国际良好实践并且不断反映最佳实践，以帮助用户努力实现高水平安全。“安全导则”中的建议用“应当”来表述。

原子能机构安全标准的适用

原子能机构成员国中安全标准的使用者是监管机构和其他相关国家当局。共同发起组织及设计、建造和运行核设施的许多组织以及涉及利用辐射源和放射源的组织也使用原子能机构安全标准。

原子能机构安全标准在相关情况下适用于为和平目的利用的一切现有和新的设施和活动的整个寿期，并适用于为减轻现有辐射危险而采取的防护行动。各国可以将这些安全标准作为制订有关设施和活动的国家法规的参考。

原子能机构《规约》规定这些安全标准在原子能机构实施本身的工作方面对其有约束力，并且在实施由原子能机构援助的工作方面对国家也具有约束力。

原子能机构安全标准还是原子能机构安全评审服务的依据，原子能机构利用这些标准支持开展能力建设，包括编写教程和开设培训班。

国际公约中载有与原子能机构安全标准中所载相类似的要求，从而使其对缔约国有约束力。由国际公约、行业标准和详细的国家要求作为补充的原子能机构安全标准为保护人类和环境奠定了一致的基础。还会出现一些需要在国家一级加以评定的特殊安全问题。例如，有许多原子能机构安全标准特别是那些涉及规划或设计中的安全问题的标准意在主要适用于新设施和新活动。原子能机构安全标准中所规定的要求在一些按照早期标准建造的现有设施中可能没有得到充分满足。对这类设施如何适用安全标准应由各国自己作出决定。

原子能机构安全标准所依据的科学考虑因素为有关安全的决策提供了客观依据，但决策者还须做出明智的判断，并确定如何才能最好地权衡一项行动或活动所带来的好处与其所产生的相关辐射危险和任何其他不利影响。

原子能机构安全标准的制定过程

编写和审查安全标准的工作涉及原子能机构秘书处及分别负责应急准备和响应（应急准备和响应标准委员会）（从 2016 年起）、核安全（核安全标准委员会）、辐射安全（辐射安全标准委员会）、放射性废物安全（废物安全标准委员会）和放射性物质安全运输（运输安全标准委员会）的五个安全标准分委员会以及一个负责监督原子能机构安全标准计划的安全标准委员会（安全标准委员会）（见图 2）。

原子能机构所有成员国均可指定专家参加四个安全标准分委员会的工作，并可就标准草案提出意见。安全标准委员会的成员由总干事任命，并包括负责制订国家标准的政府高级官员。

已经为原子能机构安全标准的规划、制订、审查、修订和最终确立过程确定了一套管理系统。该系统阐明了原子能机构的任务；今后适用安全标准、政策和战略的思路以及相应的职责。

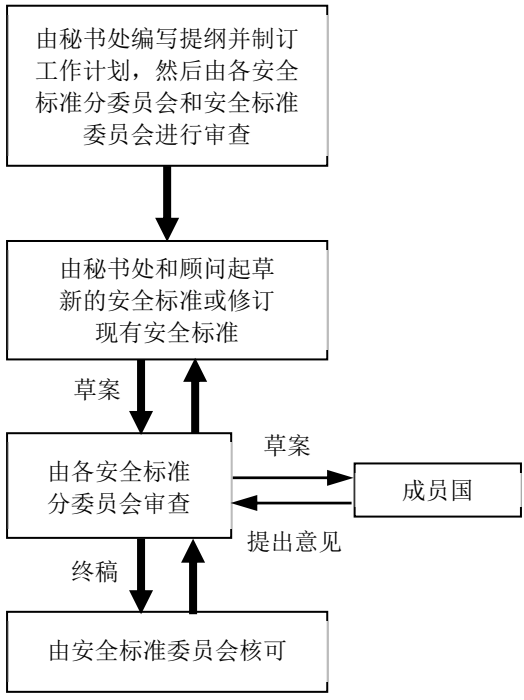

图 2. 制订新安全标准或修订现行标准的过程。

与其他国际组织的合作关系

在制定原子能机构安全标准的过程中考虑了联合国原子辐射效应科学委员会的结论和国际专家机构特别是国际放射防护委员会的建议。一些标准的制定是在联合国系统的其他机构或其他专门机构的合作下进行的，这些机构包括联合国粮食及农业组织、联合国环境规划署、国际劳工组织、经合组织核能机构、泛美卫生组织和世界卫生组织。

文本的解释

安全相关术语应按照《国际原子能机构安全术语》（见 http://www-ns.iaea.org/standards/safety-glossary.htm）中的定义进行解释。否则，则采用具有最新版《简明牛津词典》所赋予之拼写和含义的词语。就“安全导则”而言，英文文本系权威性文本。

原子能机构《安全标准丛书》中每一标准的背景和范畴及其目的、范围和结构均在每一出版物第一章“导言”中加以说明。

在正文中没有适当位置的资料（例如对正文起辅助作用或独立于正文的资料；为支持正文中的陈述而列入的资料；或叙述计算方法、程序或限值和条件的资料）以附录或附件的形式列出。

如列有附录，该附录被视为安全标准的一个不可分割的组成部分。附录中所列资料具有与正文相同的地位，而且原子能机构承认其作者身份。正文中如列有附件和脚注，这些附件和脚注则被用来提供实例或补充资料或解释。附件和脚注不是正文不可分割的组成部分。原子能机构发表的附件资料并不一定以作者身份印发；列于其他作者名下的资料可以安全标准附件的形式列出。必要时将摘录和改编附件中所列外来资料，以使其更具通用性。

目　录

1. 导言

背景

1.1. 自从开始进行反应堆设计和运行以来，人们就认识到需要根据设备在核电厂安全的重要性，对其进行分级管理。结构、系统和部件（SSCs）的安全分级方法一直伴随着现有核电厂设计和运行经验而不断进步和发展。尽管多年来人们都默认安全功能必须为安全而设置这样一个基本原理，但是，如何完成从基本安全目标中导出核电厂安全重要结构、系统和部件的工作？它应该遵守什么样的流程？在原子能机构早期关于结构、系统和部件安全分级的导则中却并没有给出相应的描述。因此，在实践中，这个被认为对安全具有最高重要性的分级具体的方法，在大多数情况下都是基于核电厂的实践经验和具体设计而专门确定的。

1.2. 本“安全导则”是根据原子能机构的安全标准计划编写的。1979 年原子能机构《安全丛书》第 50-SG-D1 号发布的安全导则，用于沸水堆、压水堆和压力管式堆（BWRs、PWRs 和 PTRs）的安全功能和部件分级，因其中所载的内容被认为不符合原子能机构 2000 年出版的原子能机构《安全标准丛书》第 NS-R-1 号《核电厂安全：设计》内容对安全的要求，已于 2000 年被撤销。

1.3. 在制定本“安全导则”时，对原子能机构的相关出版物都进行了考虑。包括《基本安全原则》[1]，以及相关安全要求出版物，如《核电厂安全：设计》[2]和《设施和活动的安全评定》[3]。

1.4. 安全分级的目标是根据结构、系统和部件在预防事故或限制事故发生时的作用，对其进行识别并分级，以保护人类和环境免受放射性和电离辐射的有害影响。在分级的基础上，结构、系统和部件就可以根据已制定的程序进行设计、制造、建造、安装、调试、运行、试验、视察和维护，从而确保达到设计规格书的要求和所期望的安全性能水平。按照参考文献[2]，所有安全重要物项是根据功能及安全性质 [1] 进行识别和分级的。

---

[1] 确定安全重要物项的安全重要性相关要素在参考文献[2]第 5.34 段，为了方便起见，在本“安全导则”第 2.2 段中重申。

1.5. 在本“安全导则”的编写过程中已对运行核电厂和新设计中采用的现有安全分级方法进行了广泛评审。本“安全导则”介绍了安全分级步骤，这些步骤通常不系统地表述和记录在各国分级方法中。

目的

1.6. 本次发布主要面向各种组织的使用，包括核电厂设计单位、监管机构及其技术支持单位。它也可适用于其他核设施，但须根据设施类型和具体设计进行适当调整。

1.7. 本“安全导则”的目标：为满足在参考文献[2、3]确立的要求提供建议和指导，以识别安全重要结构、系统和部件，并根据其功能和安全性质进行分级。通过建立并满足相关的质量要求和可靠性目标来确保高水平的安全性。考虑到核电技术的相关性，必须对核电厂安全有重要意义的物项的工程设计规则做出明确的规定，并遵守相关的国家或国际规范和标准以及成熟技术经验。有关核安保方面的结构、系统和部件分级不在本出版物的范围之内。关于这些方面的建议详见原子能机构《核安保丛书》（例如参考文献[4、5]）。

范围

1.8. 本“安全导则”适用于核电厂安全重要所有结构、系统和部件的设计，即核电厂整个寿期的所有核电厂运行状态，包括所有正常运行工况。

1.9. 本“安全导则”使用技术中立的术语编写，所提出的办法适用于新的核电厂，或许不适用于采用较早分级原则建造的现存电厂。本“安全导则”适用于这种核电厂的方式取决于各个国家。

结构

1.10. 第 2 部分提供了对结构、系统和部件进行识别和分级的基础和一般方法，对结构、系统和部件的独立安全性质进行了评定，并以此对结构、系统和部件的安全重要性进行了排序；根据上述原则，第 3 部分推荐了一个可应用于结构、系统和部件安全分级的流程；第 4 部分提供了基于结构、系统和部件的安全等级选择工程设计规则的一般性建议。

2. 一般方法

2.1. 一般方法是在确定结构、系统和部件功能和安全性质的基础上提供一种用于识别并对其安全重要程度的进行分级的框架和方法。一旦结构、系统和部件被分级，就可以确定一种适当的工程设计规则，保证它们在设计、制造、建造、安装、调试、运行、试验、视察和维护中有足够的质量来满足预设执行的功能，并最终实现主要安全功能[2]，以符合参考文献[2]安全要求。

基本要求

2.2. 为了方便，这里对参考文献[2]基本分级要求再重申一遍。而相关的额外要求见参考文献[3]。

“要求 4：基本安全功能

“下列核电厂的基本安全功能，必须在所有电厂状态下均确保得到满足： (i) 反应性控制； (ii) 排除反应堆和燃料贮存水池中的热量；(iii) 封闭放射性物质，屏蔽辐射和控制已计划的放射性释放，以及限制放射性物质的事故排放。

“4.1. 必须采取系统性方法来识别那些实现基本安全功能所必需的重要物项，确认其在所有电厂状态下满足或影响电厂基本安全功能的固有特性。

“4.2. 必须提供对电厂状况进行监控的手段，以确保所要求的安全功能得到满足。”[2]

“要求 18：工程设计标准

“基于核电技术的相关性的考虑，对核电厂安全重要物项的工程设计标准，必须做出明确规定，并且必须符合相关国家或国际规程和标准以及成熟的工程经验。”[2]

[2] 根据原子能机构《安全术语》[6]，以前被称为“基本安全功能”的功能现在被命名为“主要安全功能”。在原子能机构安全标准中，术语“基本安全功能”应理解为“主要安全功能”。

“要求 22：安全分级

“必须对所有安全重要物项进行识别和确认，并根据其功能和安全重要性对其进行分级。”

“5.34. 安全重要物项安全重要性的划分必须主要基于确定性方法，并酌情辅以概率方法，同时适当考虑以下因素：

(a) 该物项要执行的安全功能；
(b) 执行安全功能失效的后果；
(c) 该物项被唤醒执行某一安全功能的频率；
(d) 假想始发事件发生后需要该物项执行安全功能的时间或时间段。

“5.35. 设计必须确保可以阻止安全重要物项之间的任何干扰，特别是确保较低安全级别的系统中的安全重要物项的任何失效都不会蔓延到较高安全级别的系统。

“5.36. 执行多重功能的设备必须划入与该设备所执行的最重要功能相一致的安全等级。”[2]

“要求 27：重要动力系统

“对确保设备运行能力并构成安全重要系统一部分的重要动力系统必须相应进行分级。”[2]

一般性建议

2.3. 安全分级是一个迭代过程，需要贯穿整个设计过程始终，并在电厂的整个寿期中定期进行。对任何结构、系统和部件特定安全等级的划分和判断都应使用确定性安全分析来证明，并辅以来自概率安全评定的结论，得到工程判断的支持。

2.4. 安全分级应在电厂设计、系统设计和部件设计阶段得到执行，并应在电厂的建造、调试、运行和使用寿期的后续阶段，对安全分级任何相关的变更进行评审。

2.5. 考虑到对现有安全功能接口以及现有结构、系统和部件安全等级的影响，新的或改变过的假想始发事件的分析应同结构、系统和部件一起在安全分级过程中处理。

2.6. 本“安全导则”中推荐的安全分级流程与参考文献[2]所阐述的纵深防御概念是一致的，应考虑在所有五级纵深防御中执行的功能 [3]，然后根据其安全重要性对相关的结构、系统和部件进行分级。同样，设计规定也应分级（见第 3.8 段和第 3.9 段）。

2.7. 分级的依据和分级结果应以可监查记录的形式列入文件。结构、系统和部件的最终分级应由负责质量保证的组织和监管机构完成并可供监查。由于分级可能会受到电厂后续设计变更的影响（在其运行期间），因此分级记录应作为电厂配置控制的一部分包含在管理系统中。

安全分级流程概述

2.8. 本“安全导则”提出了一种结构化过程用于对结构、系统和部件的识别和分级，如图 1 所示。

2.9. 分级是一个自上而下的过程，起始于对电厂设计、安全分析以及执行要安全功能的基本理解。基于这些认识，所有电厂状态所需的功能和设计规定（见第 3.9 段），包括正常运行各种模式，被系统地确定下来。利用安全评定的结论和认知，如对假想始发事件的分析，根据其安全性质对功能进行分级。然后，属于某个功能分级的结构、系统和部件则根据它们在该功能分级中的作用加以识别和分级。当然，因其假想失效的严重后果已经决定了其安全等级，作为相应设计规定执行结果而产生的结构、系统和部件应该可以直接进行分级，而无需再对相关安全功能的分级进行任何详细分析。

[3] 对于本“安全导则”，功能被定义为单一或一组结构、系统和部件所执行的任何行动。

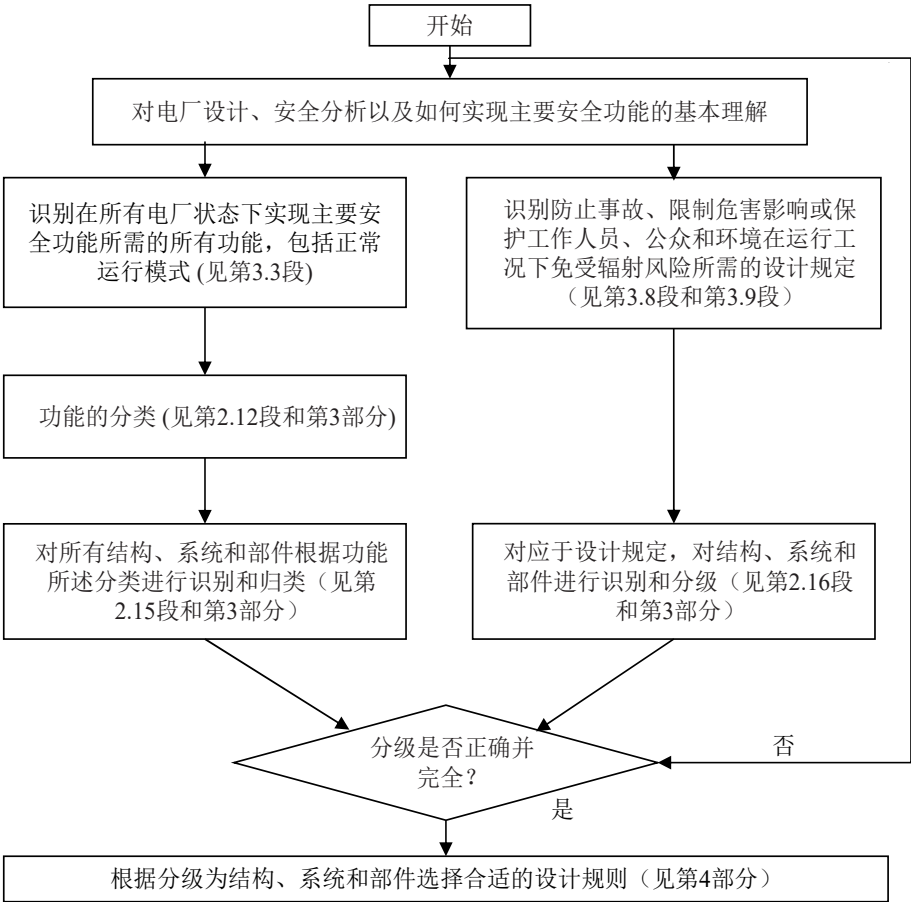
开始
对电厂设计、安全分析以及如何实现主要安全功能的基本理解
识别在所有电厂状态下实现主要安全功能所需的所有功能，包括正常运行模式 (见第3.3段)
识别防止事故、限制危害影响或保护工作人员、公众和环境在运行工况下免受辐射风险所需的设计规定（见第3.8段和第3.9段）
功能的分类 (见第2.12段和第3部分)
对所有结构、系统和部件根据功能所述分类进行识别和归类（见第2.15段和第3部分）
对应于设计规定，对结构、系统和部件进行识别和分级（见第2.16段和第3部分）
分级是否正确并完全？
否
是
根据分级为结构、系统和部件选择合适的设计规则（见第4部分）

图 1.　分级过程流程图。

2.10. 根据其安全性质对所有结构、系统和部件进行分级的过程应考虑以下要素：

— 电厂设计和它固有的安全特点；
— 所有假想始发事件[4]清单，根据参考文献[2]要求 16，还应考虑到在核电厂设计中假想始发事件的发生频率。

2.11. 应确定所有功能和设计规定，以实现在不同电厂状态下的，包括所有正常运行模式的，主要安全功能（如参考文献[2]要求 4 定义）。

2.12. 这些功能应根据其安全重要性分为数量有限的等级，考虑以下要素，来确定分级方法：

(1) 执行该功能失效的后果；
(2) 需要执行该安全功能的假想始发事件发生的频率；
(3) 该功能在实现可控状态或安全状态方面对安全重要性的贡献度（如参考文献[2]所定义）。

2.13. 对设计规定的功能进行分级是没有必要的，因为其相应的结构、系统和部件的安全重要性可以直接从其失效的后果中得出。因此，作为设计规定实现的结构、系统和部件可以直接分配到安全级别中，而不需要对安全功能分级进一步分析。

2.14. 该方法的下一步骤是确定安全重要所有结构、系统和部件的安全分级。通常应采用确定性方法，并在适当情况下通过概率安全评定和工程判断加以补充，以实现恰当的风险平衡，即对电厂设计中具有非常严重后果的事件只能有很低的预计发生频率。总体趋势示意图如图 2 所示，设计规定的实施主要是为了降低事故发生的概率，而功能的实施是为了使后果在其发生的概率下可接受。对于大多数始发事件，实施设计规定和功能的组合，以减少事故的发生频率，并使其后果可以接受且尽可能低。然而，对于一些始发事件，如果后果非常小并且不需要任何缓解规定，则可能不必实施限制后果的功能。设计规定和安全功能的效果将取决于物项的总体可靠性，而这一点由其分级决定。

---

[4] 参考文献[2]第 5.9 段指出：“在电厂总体安全评定和详细分析中，用于确定安全重要物项性能要求的假想始发事件，必须划分成若干具有代表性的事件序列。这些具有代表性的事件序列包络所有同类事件，并为安全重要物项的设计和运行限值提供基准。”

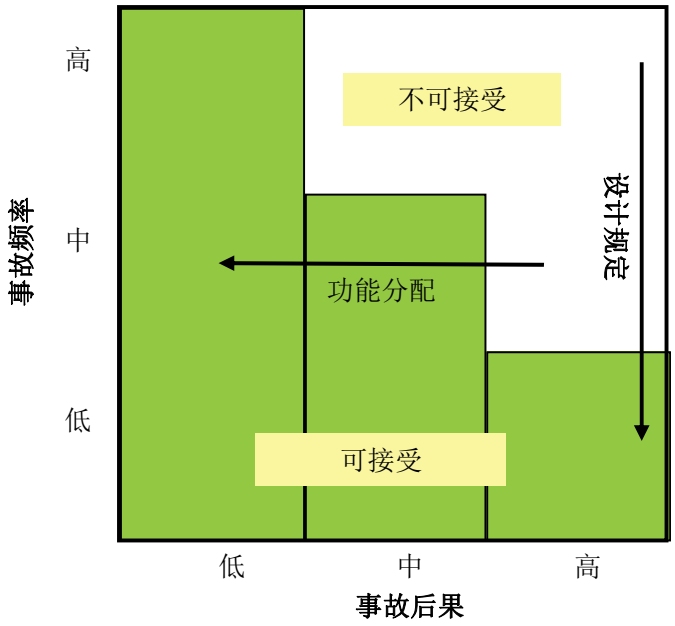

图 2. 频率与后果的基本原则。

2.15. 为了降低事故发生的频率并使其后果可以接受且尽可能低，应使用参考文献[2]要求 22 规定要素的流程，根据其安全重要性确定履行功能所需的结构、系统和部件并将其分级为有限数量的级别。

2.16. 作为设计规定实现的结构、系统和部件的识别和分级，应与执行安全功能所需的结构、系统和部件的分级体系一致。

2.17. 根据成员国的经验，在本“安全导则”中推荐了三个功能安全等级和三个安全重要结构、系统和部件的安全级别。可以使用更多或更少数量的等级和级别的其他方法，只要它们与第 2.12 段和第 2.15 段中提供的指导一致即可。

3. 安全分级流程

3.1. 本部分提供了更详细的指导，用于识别需要分级的功能和需要分级的结构、系统和部件，以确保找出所有对保护公众和环境免受电离辐射的有害影响必不可少的物项。

识别要分级的功能

3.2. 为简化目的，“功能”一词包括主要功能和预期执行的确保主要功能实现的任何辅助功能。

3.3. 被分级的功能是那些必需在不同的电厂状态实现主要安全功能所需要的那些功能，包括所有的正常运行模式。这些功能主要是那些被记入安全分析中的功能，包括在所有纵深防御五个层次执行的功能，即预防、监控、控制和缓解安全功能。

3.4. 虽然每个电厂状态的主要安全功能是相同的，但要分级的功能应分别针对每个电厂状态独立识别。

3.5. 所确定的功能列表可以由其他功能来补充，例如旨在降低反应堆紧急停堆触发频率和/或旨在纠正偏离正常运行的专设安全设施，包括旨在将主要电厂参数保持在电厂的正常运行范围内的功能。这种功能一般不记入安全分析。

3.6. 由于监控对安全的重要性，应考虑在发生事故时向电厂工作人员和场外应急响应组织提供足够可靠信息的监控功能，以便对安全进行分级。这应包括根据应急响应计划要求进行的监控和通信。

3.7. 在安全分析当中，为预防由于叠加独立故障导致的某些序列升级为严重事故，或缓解严重事故后果的功能，应包含在设计扩展工况相关的功能中。

设计规定的识别

3.8. 电厂的安全性也取决于不同类型设施的可靠性，其中一些设施是专门用于正常运行而设计的。为了本“安全导则”的目的，这些结构、系统和部件被称为“设计规定”。此类设计规定应予以识别并在安全分级的过程中考虑，其相应的结构、系统和部件将以足够的质量进行设计、制造、建造、安装、调试、运行、试验、视察和维护，以实现其预期的作用。

3.9. 设计规定应包括以下内容：

— 应通过高质量的设计来保证“设计规定”对应相关设备、系统及部件失效的可能性在理论上是消除了的 [5]。对于这些设计部件，电厂设计不再需要独立的安全系统来减轻其失效的影响。例如，反应堆压力容器或蒸汽发生器的外壳。这些设计部件可以很容易地通过严重程度高的后果来识别；
— 那些用于降低事故频率的部件或系统。例如，其失效将导致设计基准事故发生的高质量管道；
— 非能动部件或性能，旨在保护工作人员和公众免受正常运行辐射的有害影响。例如，屏障、土木结构和管道；
— 非能动部件和性能，旨在保护安全重要部件不被内部或外部危害损坏。例如专门为此建造的设备之间的混凝土墙；
— 在没有其他单一故障发生的情况，旨在防止假想始发事件发展成更严重的序列所需的部件和性能。例如防甩件和锚固件。

与设计规定对应结构、系统和部件应按第 3.22 段中推荐的方法进行分级，同时也取决于其失效后的后果评定。

功能分级

3.10. 在所有电厂状态下实现主要安全功能所需的功能，包括正常运行模式，应根据其安全重要性对其进行分级。每个功能的安全意义是在考虑第 2.12 段中所述的要素来确定的。在本“安全导则”所建议的方法中，如第 3.11 段所定义的那样，如果不执行该功能，将导致最严重后果，该后果严重程度（要素 1）被分为三个级别（高、中、低）。

3.11. 严重性的三个级别定义如下：

— 如果功能失效，严重程度应该被视为“高”，在最坏的情况：
  • 导致放射性物质的释放超过监管机构接受的设计基准事故的限值；或

[5] 某些工况的发生概率可以认为已经被“实际消除”，如果这种工况在物理上是不可能发生的，或者可以在高置信水平下认为这种工况极不可能出现。

- 使关键物理参数的值超过设计基准事故的验收标准[6]。

— 如果功能失效，严重程度应被视为“中”，在最坏的情况：
  - 导致放射性物质的释放超过为预计运行事件设定的限值；或
  - 使关键物理参数的值超过预计运行事件的设计限值。

— 如果功能失效，则应将严重程度视为“低”，在最坏的情况：
  - 导致工作人员的剂量高于监管限值。

如果同时满足以上这些定义，则应采用三个级别中最高的一个。对后果的评定是在假设该功能没有响应的情况下进行的。

对于预计运行事件，为避免“过度分级”，后果评定应在所有其他独立功能都在适当的时刻准确执行了的假设下完成。

3.12. 要素 2（见第 2.12 段）反映功能被唤醒的频率。该频率应主要根据相应假想始发事件的发生频率进行评价。

3.13. 包括要素 1 和要素 2，这里推荐的分级方法符合公认的设计原理，即具有最严重后果的事件应该具有最低的发生频率。这意味着，例如，专门用于减轻严重事故后果的功能所涉及的工程设计规则可能不如用于减轻设计基准事故后果的功能那么有说服力，因为严重事故的发生频率低于设计基准事故的发生频率。图 2 阐释了这个现象。

3.14. 要素 3（见第 2.12 段）关注旨在到达特定电厂状态的功能。一般情况分为两种电厂状态，即可控状态和安全状态[7]。对于那些用以达到可控状态的功能，主要关注的是自动触发或短期触发，以便显著降低潜在危害。用于达到安全状态的功能是较长期的功能，并且应在达到可控状态后执行。反应堆在许多情况下，在事故瞬态之后投用的功能将首先实现可控状态，然后才实现安全状态。可控状态的典型的功能是反应堆停堆、衰变热导出和安全注入。反应堆和连接在一起余热排出系统的减压，以保证衰变热导出的长期功能是实现安全状态功能的良好示例。

---

[6] 见参考文献[2]要求 15、19。

[7] 定义见参考文献[2]

3.15. 本“安全导则”中推荐的功能分级基于以下三个安全分级：

安全分级 1：在预计运行事件或设计基准事故之后达到可控状态所需的任何功能，以及在受到挑战时其失效将导致“高”严重性后果的功能。

安全分级 2：这一级有三种可能性：

— 在预计运行事件或设计基准事故之后达到可控状态所需的任何功能，以及在受到挑战时其失效将导致“中”严重性后果的功能；或
— 达到和维持长期安全状态所需的任何功能，以及当受到挑战时其失效将导致“高”严重性后果的功能；或
— 任何为安全分级 1 中功能提供备份的功能，以及那些堆芯未熔化条件下，控制设计扩展工况。

安全分级 3：这一级中有五种可能性：

— 在预计运行事件或设计基准事故发生时启动的任何功能，以及那些如果受到挑战，它的失效将导致“低”严重程度后果的功能；或
— 任何需要达到和维持一个长期安全状态的功能，以及那些如果受到挑战，它的失效将导致“中”严重程度后果的功能；或
— 为减轻设计扩展工况的后果而需要的任何功能，除非已被要求归类为安全分级 2，以及那些如果受到挑战，它的失效将导致“高”严重性后果的功能；或
— 任何设计用来在偏离正常运行事件中降低反应堆停堆或专设安全设施触发频率的安全功能，包括设计用来将主要电厂参数保持在电厂正常运行范围内的功能；或
— 需要在发生事故时向电厂工作人员和场外应急服务提供完整足够可靠信息的监控功能（设计基准事故或设计扩展工况），包括作为应急响应计划（纵深防御 5 级）一部分的监控和通讯功能，除非已被分配到更高的等级。

3.16. 第 3.15 段所述的分级汇总在表 1 中。如果一个功能可以划分在不同分级中时（例如，因为一个以上的假想始发事件需要的功能），它应该被归类在这些分级中的最高级别。

表 1. 安全分级与安全评定报告中的规定假想始发事件分析的对应关系

安全评定报告中的标记的安全功能	如果功能执行时效所带来后果的严重性		
	高	中	低
在预计运行事件后回到可控状态的功能	安全分级 1	安全分级 2	安全分级 3
在设计基准事故发生后回到可控状态的功能	安全分级 1	安全分级 2	安全分级 3
达到并维持安全状态的功能	安全分级 2	安全分级 3	安全分级 3
超设计基准事故后果的缓解功能	安全分级 2 或 3（见第 3.15 段）	无分级 [a]	无分级 [a]

[a] 在缓解设计扩展工况的专用功能未响应的情况下，预计不会发生中等或低严重性后果。

结构、系统和部件的分级

3.17. 一旦完成功能的安全分级，执行这些功能的结构、系统和部件应该被归类到一个安全等级。

3.18. 执行安全分级的功能所需的所有结构、系统和部件应根据其安全重要性进行识别和分级，其过程应考虑参考文献[2]要求 22 规定的要素并转载于第 2.2 段。

3.19. 适用第 2.2 (a) 和 (c) 段中定义的要素，结构、系统和部件（包括支持结构、系统和部件）其初始安全等级应该与其功能的安全分级相对应。在本“安全导则”所建议的方法中给出了三个安全等级，与第 3.15 段所建议的三个等级相一致。

3.20. 考虑到第 2.2 (b) 和 (d) 段所定义的要素，应在必要时对初步分级进行修订。对于要素 (d)，考虑在功能调用之前假想始发事件之后的时间，可以允许结构、系统和部件移入较低的等级，前提是可以证明其预期的可靠性。例如，有证据表明，可以安排时间来修复或维持结构、系统和部件，或存在时间窗口，有利用备选结构、系统和部件来执行所需的安全功能的可能。

3.21. 如果一个结构、系统和部件对不同等级的几个功能都有贡献，它应该被分配给对应于这些等级中的最高级别（即需要最保守的工程设计规则的级别）。

3.22. 应用这些和其他相关的考虑因素（例如工程判断），结构、系统和部件的最终安全等级是可以选定的。

3.23. 正如第 2.9 段所解释的那样，设计规定所对应的结构、系统和部件可根据其失效后果的严重程度直接进行分级：

— 安全分级 1：任何失效会导致“高”严重程度后果的结构、系统和部件；
— 安全分级 2：任何失效会导致“中”严重程度后果的结构、系统和部件；
— 安全分级 3：任何失效会导致“低”严重程度后果的结构、系统和部件。

任何结构、系统和部件（例如，火灾或水淹屏障），如果它的失效会造成对危害分析中假设的挑战，应至少分配给安全分级 3。

3.24. 任何对某分级功能没有贡献但其失效可能对该分级功能产生不利影响的结构、系统和部件（如果不能通过设计排除），都应适当地进行分级，以避免该功能失效产生的不可接受的影响。

3.25. 如果相互连接或相互影响的结构、系统和部件之间安全等级不相同（包括安全等级中的结构、系统和部件连接到未分级的结构、系统和部件的情况），则应通过较高安全等级边的装置（例如光学隔离器或自动阀）以隔离两组结构、系统和部件之间的干扰，以确保较低安全等级的结构、系统和部件失效不会产生效应。

3.26. 一旦将每个结构、系统和部件分配给一个安全等级，就可以确定一组规则并将其应用于结构、系统和部件的工程、设计和制造，以保证适当的质量和可靠性。第 4 部分提供了关于分配工程设计规则的建议。

安全分级核实

3.27. 安全分级的适当性应通过确定性安全分析来核实，来自概率安全评定的见解和/或工程判断 [8] 的支持可以对其进行补充。

3.28. 结构、系统和部件对降低电厂整体风险的贡献是其安全分级的一个重要因素。确定性和概率方法之间的一致性可以提高对安全分级正确性的信心。通常而言，都是希望安全分级的概率标准会与确定性得出的标准相匹配。如果存在差异，无论如何，都应进行进一步的评定，以了解产生这些差异的原因，并应指定最终的安全等级，该等级应有合理的理由进行支持。

3.29. 核实安全分级的过程应该是迭代的，与不断展开的设计保持一致并相互信息通报。

4. 为结构、系统和部件选择适用的工程设计规则

4.1. 工程设计规则与各个国家的或国际的规范、标准和经过核实的工程经验相关，应恰当地适用于结构、系统和部件的设计，以满足切实可行的设计要求。

4.2. 一旦确定了结构、系统和部件的安全等级，就应该指定和应用相应的工程设计规则。应选择工程设计规则，以使电厂设计满足以下目标：最常见的假想始发事件很少产生或没有不良后果，而越极端的事件（具有最大后果的潜在事件）就越应该具有非常低的发生频率（见图 2）。

[8] 提供工程判断的专家组应包括知识渊博的来自电厂营运组织的人员，以及概率安全评定、安全分析、电厂运行、设计工程和系统工程方面的专家。

4.3. 工程设计规则涉及性能、可靠性（可信赖性）和健稳性三个特性：

(a) 性能是指结构、系统和部件根据需要执行其指定功能的能力；
(b) 可靠性（置信度）是指结构、系统和部件能够以与安全分析一致的足够低的失效率执行其所需功能的能力；
(c) 健稳性是确保由运行负载以及假想始发事件引起的负载不会对结构、系统和部件执行其安全功能的能力造成不利影响的能力。

这些特征应该在考虑不确定性的前提下清晰定义。

4.4. 应指定一套完整的工程设计规则，以确保结构、系统和部件的设计、制造、建造、安装、调试、运行、试验、视察和维护遵守适当的质量标准。为了实现这一点，设计规则应为性能、可靠性和鲁棒性确定合适的设计分级。设计规则还应适当考虑与安全级结构、系统和部件相关的监管要求。

4.5. 将适用于系统级别的设计要求与适用于个别结构和部件的设计要求区分开来分别处理的要求是合理的：

— 在系统级别应用的设计要求可能包括特定要求，如单一故障标准、冗余系统的独立性、多样性和可试验性；
— 适用于个别结构和部件的设计要求可能包括特定要求，如环境和抗震鉴定，以及制造质量保证程序。特别地，通过它指定适用的规范或标准来表示。

4.6. 许可证持有者或申请者应提供并证明安全等级与相关的工程设计和制造规则之间的对应关系，包括适用于每个结构、系统和部件的规范和/或标准。

4.7. 一旦确定了系统及其单一部件的工程设计要求，就应该核实系统是否能够以安全分析中假想的可靠性执行其功能。

参 考 文 献

[1] 欧洲原子能联营、联合国粮食及农业组织、国际原子能机构、国际劳工组织、国际海事组织、经济合作与发展组织核能机构、泛美卫生组织、联合国环境规划署、世界卫生组织，《基本安全原则》，国际原子能机构《安全标准丛书》第 SF-1 号，国际原子能机构，维也纳（2006 年）。

[2] 国际原子能机构《核电厂安全：设计》，国际原子能机构《安全标准丛书》第 SSR-2/1 号，国际原子能机构，维也纳（2012 年）。

[3] 国际原子能机构《设施和活动安全评定》，国际原子能机构《安全标准丛书》第 GSR Part 4 号，国际原子能机构，维也纳（2009 年）。

[4] 国际原子能机构《关于核材料和核设施实物保护的核安保建议》（INFCIRC/225/Revision 5 号文件），国际原子能机构《核安保丛书》第 13 号，国际原子能机构，维也纳（2011 年）。

[5] 国际原子能机构《放射性物质和相关设施的核安保建议》，国际原子能机构《核安保丛书》第 14 号，国际原子能机构，维也纳（2011 年）。

[6] 国际原子能机构《国际原子能机构核安全和辐射防护安全术语》（2007 年版），国际原子能机构，维也纳（2007 年）。

参与起草和审订人员

Barbaud, J.	法国电力公司
Bassing, G.	欧洲核能行业贸易协会-欧洲核设施安全标准反应堆安全小组（比利时）
Cook, S.	加拿大核安全委员会
Erasmus, L.	南非球床模块式反应堆有限公司
Fil, N.	俄罗斯联邦原子能公司
Fischer, K.C.	德国 TUV NORD&KG 股份有限公司
Froehmel, T.	世界核能协会
Hakata, T.	日本核安全委员会
Hamon, D	美国日立通用电气公司
Head, J.	美国日立通用电气公司
Hidaka, A.	日本原子能机构
Inabe, T.	日本原子能机构
Jarvinen, M.J.	芬兰辐射与核安全局
Jennings, R.	英国核监管办公室
Jung, I.	美国核管制委员会
Klapp, U.	德国阿海珐
Leong, J.	美国日立通用电气公司
Matsumoto, T	日本核能安全组织
Nunighoff, K.	德国装置与反应堆安全公司
Petzer, C.	南非球床模块式反应堆有限公司
Poulat, B.	国际原子能机构
Rensburg, J.	南非球床模块式反应堆有限公司

Ringdahl, K.	瑞典万滕福尔电力公司研究与发展部
Shchekin, I.	俄罗斯联邦原子能公司
Toth, C.	国际原子能机构
Tricot, N.	国际原子能机构
Upton, H.A.	美国日立通用电气公司
Valtonen, K.	芬兰辐射与核安全局
Waddington, J.	世界核能协会
Wattelle, E.	法国辐射防护与核安全研究所

IAEA
国 际 原 子 能 机 构

No. 26

当 地 订 购

国际原子能机构的定价出版物可从下列来源或当地主要书商处购买。
未定价出版物应直接向国际原子能机构发订单。联系方式见本列表末尾。

北美

Bernan / Rowman & Littlefield
15250 NBN Way, Blue Ridge Summit, PA 17214, USA
电话：+1 800 462 6420 • 传真：+1 800 338 4550
电子信箱：orders@rowman.com • 网址：www.rowman.com/bernan

世界其他地区

请联系您当地的首选供应商或我们的主要经销商：

Eurospan Group
Gray's Inn House
127 Clerkenwell Road
London EC1R 5DB
United Kingdom

交易订单和查询：
电话：+44 (0) 176 760 4972 • 传真：+44 (0) 176 760 1640
电子信箱：eurospan@turpin-distribution.com

单个订单：
www.eurospanbookstore.com/iaea

欲了解更多信息：
电话：+44 (0) 207 240 0856 • 传真：+44 (0) 207 379 0609
电子信箱：info@eurospangroup.com • 网址：www.eurospangroup.com

定价和未定价出版物的订单均可直接发送至：

Marketing and Sales Unit
International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
电话：+43 1 2600 22529 或 22530 • 传真：+43 1 26007 22529
电子信箱：sales.publications@iaea.org • 网址：https://www.iaea.org/zh/chu-ban-wu

通 过 国 际 标 准 促 进 安 全

国际原子能机构
维也纳