

# 国际原子能机构 安全标准

保护人类与环境

## 核电厂安全：设计

特定安全要求

第 SSR-2/1 (Rev.1) 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，国际原子能机构授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：

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

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](mailto: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。

# 核电厂安全：设计

下列国家是国际原子能机构的成员国：

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

《国际原子能机构规约》于1956年10月23日经在纽约联合国总部举行的国际原子能机构规约大会核准，1957年7月29日生效。国际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 SSR-2/1(Rev.1) 号

# 核电厂安全：设计

## 特定安全要求

本出版物随附一张只读光盘，其中收录了 2007 年版《国际原子能机构安全术语》和 2006 年版《基本安全原则》，并分别提供了阿拉伯文、中文、英文、法文、俄文和西班牙文文本。亦可单独购买只读光盘。

见：<http://www-pub.iaea.org/books>

国际原子能机构  
2016 年·维也纳

# 版权说明

国际原子能机构的所有科学和技术出版物均受 1952 年（伯尔尼）通过并于 1972 年（巴黎）修订的《世界版权公约》之条款的保护。自那时以来，世界知识产权组织（日内瓦）已将版权的范围扩大到包括电子形式和虚拟形式的知识产权。必须获得许可而且通常需要签订版税协议方能使用国际原子能机构印刷形式或电子形式出版物中所载全部或部分内容。欢迎有关非商业性翻印和翻译的建议并将在个案基础上予以考虑。垂询应按以下地址发至国际原子能机构出版科：

Marketing and Sales Unit, Publishing Section  
International Atomic Energy Agency  
Vienna International Centre  
PO Box 100  
1400 Vienna, Austria  
传真：+43 1 2600 29302  
电话：+43 1 2600 22417  
电子信箱：sales.publications@iaea.org  
<http://www.iaea.org/books>

© 国际原子能机构·2016 年  
国际原子能机构印制  
2016 年 11 月·奥地利

## 核电厂安全：设计

国际原子能机构，奥地利，2016 年 11 月  
STI/PUB/1715  
ISBN 978-92-0-509316-1  
ISSN 1020-5853

# 序言

## 一 总干事天野之弥

国际原子能机构《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体制的一个关键要素，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。对于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，同时不使核能对公平和可持续发展的贡献受到不适当的限制。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。





# 前 言

在 2011 年 3 月 11 日日本东部大地震和海啸后发生了日本福岛第一核电站事故。为了应对福岛第一核电站事故<sup>1</sup>，制订了“国际原子能机构核安全行动计划”（GOV/2011/59-GC(55)/14 号文件）。该行动计划于 2011 年 9 月获得原子能机构理事会核准和原子能机构大会核可（GC(55)/RES/9 号决议）。它包括一项题为“审查和加强国际原子能机构安全标准并加强对安全标准的执行”的行动。

这项行动要求安全标准委员会和原子能机构秘书处“以优先等级为序审查并在必要时修订原子能机构相关安全标准”，并呼吁成员国“尽可能广泛和有效地利用原子能机构安全标准”。

这种审查除其他专题外，包含了监管结构、应急准备和响应以及核安全和核工程方面（厂址选择和评价、极端自然灾害包括其综合影响评定、严重事故管理、厂内断电、丧失热阱、爆炸性气体积聚、核燃料行为和乏燃料贮存安全）。

2011 年，秘书处开始根据可获得的关于福岛第一核电站事故的资料对原子能机构《安全标准丛书》的“安全要求”出版物进行这种审查，这些资料包括 2011 年 6 月和 2011 年 9 月发表的日本政府的两份报告、2011 年 5 月 24 日至 6 月 2 日进行的原子能机构国际实情调查专家工作组访问的报告和国际核安全组（国际核安全咨询组）主席 2011 年 7 月 26 日致总干事的信函。作为优先事项，秘书处审查了适用于核电厂和乏燃料贮存的“安全要求”出版物。

该审查首先包括对这些报告的结论进行综合分析。根据这一分析的结果，随后系统地审查了“安全要求”出版物，以便决定是否需要通过修正来反映上述任何结论。

---

<sup>1</sup> 欲了解进一步的情况，请见国际原子能机构《福岛第一核电站事故 — 总干事的报告》，国际原子能机构，维也纳（2015 年）。

在此基础上，安全标准委员会在 2012 年 10 月会议上核准了通过对以下五份“安全要求”出版物进行修正的修订过程的建议：《促进安全的政府、法律和监管框架》（原子能机构《安全标准丛书》第 GSR Part 1 号，2010 年）、《设施和活动的安全评定》（第 GSR Part 4 号，2009 年）、《核电厂安全：设计》（第 SSR-2/1 号，2012 年）、《核电厂安全：调试和运行》，（第 SSR-2/2 号，2011 年）、《核装置的厂址评价》（第 NS-R-3 号，2003 年）。

2012 年和 2013 年，在编写这五份安全标准的建议修正文本草案过程中考虑了补充输入，包括原子能机构国际专家会议的结论和 2012 年 8 月《核安全公约》缔约方第二次特别会议上的专题介绍。还对若干国家和地区的报告进行了考虑。

关于对“安全要求”的审查，安全标准委员会主席 2014 年 1 月 6 日致总干事的信函中所反映的该委员会的结论是：

“审查迄今已确认了现行‘安全要求’的适当性。审查没有发现显著的薄弱领域，仅是建议进行少量修正，以加强这些要求和促进它们的执行。安全标准委员会认为，应当主要通过数年来一直在利用的充分成熟的审查和修订过程来加强原子能机构的安全标准。同时，安全标准委员会成员强调指出，审查和修订原子能机构安全标准的依据不应当限于福岛第一核电站事故的教训。这种依据还应当包括从别处取得的其他运行经验，以及从研究与发展方面的进步中获得的信息。安全标准委员会还强调，有必要更多地关注成员国和在成员国实施原子能机构安全标准的情况。”

秘书处在顾问会议上以及核安全标准分委员会、辐射安全标准分委员会、运输安全标准分委员会和废物安全标准分委员会在 2013 年上半年对这些修正草案进行了审查。还在 2013 年向核安保导则委员会介绍了这些修正草案，以资通报。这些修正草案随后提交给原子能机构各成员国征求意见，并在顾问会议上根据所收到的意见对其进行了修订。这些建议修正案此后在 2014 年 6 月和 7 月四个安全标准分委员会的会议上获得所有这些安全标准分委员会的核准，并在 2014 年 11 月安全标准委员会会议上得到该委员会的核可。

第 SSR-2/1 号的修订涉及以下主要领域：

- 通过加强电厂设计基准，防止严重事故；
- 防止严重事故对公众和环境造成不可接受的放射性后果；
- 缓解严重事故的后果，以避免或最大程度减少厂外放射性污染。

对具体段落作了以下修正。添加了以大写字母（A, B, ……）标示的新段落。此外，凡删除的段落均在文本中做了标示。

在本修订本中修改或添加了如下要求和段落：第 2.13 段、第 4.13A 段、第 5.1 段、要求 17、第 5.15A 段、第 5.15B 段、第 5.17 段、第 5.18 段、第 5.20 段、第 5.21 段、第 5.21A 段、第 5.22 段、要求 19、第 5.27 段、第 5.28 段、第 5.31 段、第 5.31A 段、第 5.55 段、要求 33、第 5.63 段、第 5.73 段、第 5.75 段、第 5.76 段、要求 53、第 6.19A 段、第 6.19B 段、第 6.28A 段、第 6.28B 段、第 6.39 段、第 6.40A 段、要求 67、第 6.42 段、要求 68、第 6.43 段、第 6.44A 段、第 6.44B 段、第 6.44C 段、第 6.44D 段、第 6.45A 段、第 6.68 段和第 6.68A 段。还作了一些编辑性的修改。

可向原子能机构（[Safety.Standards@iaea.org](mailto:Safety.Standards@iaea.org)）请求提供修改表。

在 2015 年 3 月 2 日开始举行的会议上，理事会按照原子能机构《规约》第三条 A 款第 6 项的规定将修订后的本“安全要求”出版物草案确定为原子能机构的一个安全标准，并授权总干事颁布修订后的本“安全要求”并将其作为原子能机构《安全标准丛书》的一份“安全要求”出版物印发。

2015 年 9 月原子能机构大会第五十九届常会鼓励成员国在国家一级、地区一级和国际一级执行确保核安全、辐射安全、运输安全和废物安全以及应急准备的措施，同时充分考虑到原子能机构安全标准；要求原子能机构尽可能广泛和有效地不断审查、加强和执行原子能机构安全标准；并支持安全标准委员会和各安全标准分委员会在福岛第一核电站事故背景下审查相关的安全标准以及原子能机构关于福岛第一核电站事故的报告中确定的教训<sup>1</sup>。

大会要求秘书处：

“在制订安全标准（包括但不限于环境保护）方面继续与联合国原子辐射效应科学委员会（辐射科委会）、国际放射防护委员会（国际放射防护委）和其他相关组织密切合作”。

原子能机构大会第五十九届常会还鼓励成员国在其国家监管计划中酌情使用原子能机构安全标准，并注意到有必要考虑根据国际公认标准和导则对国家条例和导则定期进行审查，并在相关安全公约条款规定的审议会等适当国际论坛上报告进展情况。

大会进一步鼓励成员国确保利用原子能机构的自评定工具并同时考虑到相关原子能机构安全标准对本国的核安全、辐射安全、运输安全和废物安全以及应急准备情况定期进行自评定。

# 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履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<sup>1</sup>具有保护生命和健康以及保护环境共同目的。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）。

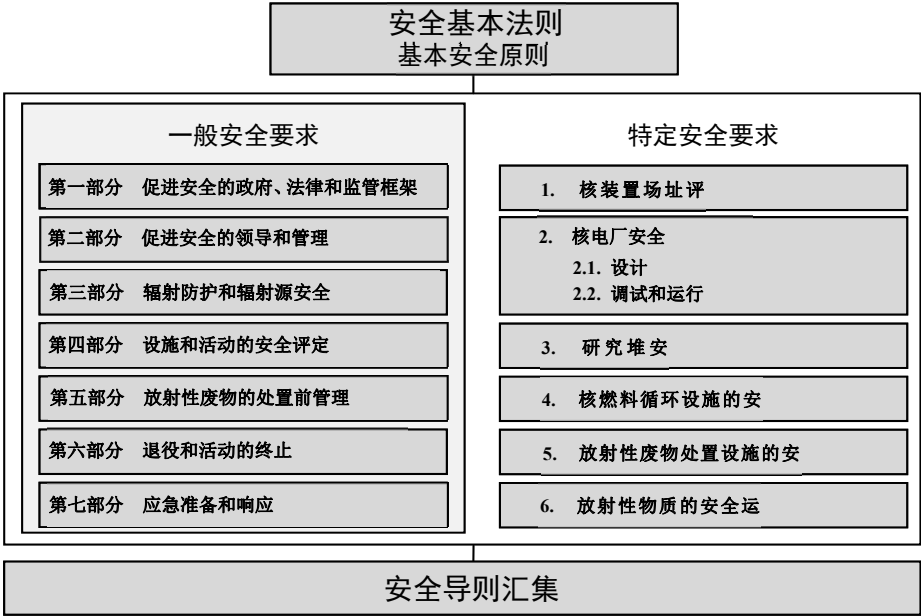


图 1. 国际原子能机构《安全标准丛书》的长期结构。

<sup>1</sup> 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。



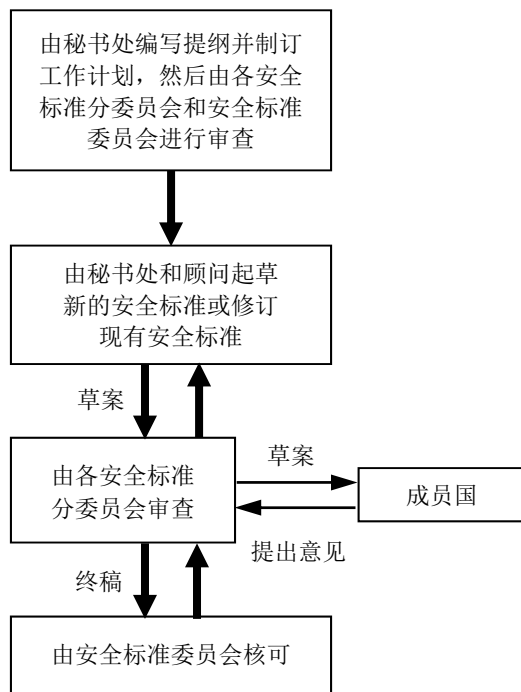


图 2. 制订新安全标准或修订现行标准的过程。

## 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。在其他情况下，则按照最新版《简明牛津词典》中赋予的拼写和意义使用词语。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

<b>1. 导言 .....</b>	<b>1</b>
背景 (1.1-1.3).....	1
目的 (1.4-1.5).....	2
范围 (1.6-1.8).....	2
结构 (1.9).....	2
<b>2. 适用安全原则和概念 (2.1-2.5) .....</b>	<b>3</b>
设计中的辐射防护 (2.6-2.7).....	4
设计安全 (2.8-2.11).....	4
纵深防御 (2.12-2.14).....	5
在电厂整个寿期内保持电厂设计的完整性 (2.15-2.18).....	8
<b>3. 设计安全的管理 .....</b>	<b>8</b>
要求 1: 电厂设计安全管理中的责任 (3.1).....	8
要求 2: 电厂设计管理系统 (3.2-3.4).....	9
要求 3: 电厂设计在电厂整个寿期内的安全性 (3.5-3.6).....	9
<b>4. 主要技术要求 .....</b>	<b>10</b>
要求 4: 基本安全功能 (4.1-4.2).....	10
要求 5: 设计中的辐射防护 (4.3-4.4).....	11
要求 6: 核电厂的设计 (4.5-4.8).....	11
要求 7: 实施纵深防御 (4.9-4.13A).....	12
要求 8: 安全与安保和保障之间的接口.....	14
要求 9: 经证明的工程实践 (4.14-4.16).....	14
要求 10: 安全评定 (4.17-4.18).....	14
要求 11: 建造规定 (4.19).....	15
要求 12: 纳入便于进行放射性废物管理和退役的特性 (4.20).....	15
<b>5. 电厂总体设计 .....</b>	<b>16</b>
设计基准 .....	16
要求 13: 电厂状态种类 (5.1-5.2).....	16

要求 14: 安全重要物项的设计基准 (5.3).....	16
要求 15: 设计限值 (5.4).....	16
要求 16: 假想始发事件 (5.5-5.15).....	17
要求 17: 内部和外部危害 (5.15A-5.22).....	18
要求 18: 工程设计规则 (5.23).....	20
要求 19: 设计基准事故 (5.24-5.26).....	20
要求 20: 设计扩展工况 (5.27-5.32).....	21
要求 21: 安全系统的实体分隔和独立性 (5.33).....	23
要求 22: 安全分类 (5.34-5.36).....	23
要求 23: 安全重要物项的可靠性 (5.37-5.38).....	23
要求 24: 共因故障.....	24
要求 25: 单一故障准则 (5.39-5.40).....	24
要求 26: 故障安全设计 (5.41).....	24
要求 27: 支持服务系统 (5.42-5.43).....	25
要求 28: 安全运行的运行限值和条件 (5.44).....	25
确保电厂寿期间安全运行的设计.....	26
要求 29: 安全重要物项的校准、测试、维护、维修、更换、 检查和监测 (5.45-5.47).....	26
要求 30: 安全重要物项验证 (5.48-5.50).....	26
要求 31: 老化管理 (5.51-5.52).....	27
人为因素.....	27
要求 32: 确保操纵员最佳绩效的设计 (5.53-5.62).....	27
其他设计考虑因素.....	29
要求 33: 多机组核电厂各机组的安全系统和设计扩展工况 安全特性 (5.63).....	29
要求 34: 含有易裂变材料或放射性物质的系统.....	29
要求 35: 用于热电联供、产热或海水淡化的核电厂.....	29
要求 36: 电厂的撤离路线 (5.64-5.65).....	29
要求 37: 电厂通讯系统 (5.66-5.67).....	30
要求 38: 电厂出入控制 (5.68).....	30
要求 39: 防止擅自接触或干扰安全重要物项.....	30

要求 40: 防止安全重要系统之间有害的相互作用 (5.69-5.70)	30
要求 41: 电网与电厂之间的相互作用	31
安全分析	31
要求 42: 电厂设计的安全分析 (5.71-5.76)	31
<b>6. 电厂特定系统的设计</b>	<b>33</b>
反应堆堆芯和相关特性	33
要求 43: 燃料元件和燃料组件的性能 (6.1-6.3)	33
要求 44: 反应堆堆芯的结构能力	34
要求 45: 反应堆堆芯的控制 (6.4-6.6)	34
要求 46: 反应堆停堆 (6.7-6.12)	35
反应堆冷却剂系统	35
要求 47: 反应堆冷却剂系统的设计 (6.13-6.16)	35
要求 48: 反应堆冷却剂压力边界的过压保护	36
要求 49: 反应堆冷却剂的装量	36
要求 50: 反应堆冷却剂的净化 (6.17)	36
要求 51: 反应堆堆芯的余热排除	37
要求 52: 反应堆堆芯的应急冷却 (6.18-6.19)	37
要求 53: 将热量传输到最终热阱 (6.19A-6.19B)	37
安全壳结构和安全壳系统	38
要求 54: 反应堆安全壳系统	38
要求 55: 控制放射性从安全壳释放 (6.20-6.21)	38
要求 56: 安全壳隔离 (6.22-6.24)	38
要求 57: 进入安全壳 (6.25-6.26)	39
要求 58: 安全壳工况控制 (6.27-6.30)	39
仪器仪表和控制系统	41
要求 59: 提供仪器仪表 (6.31)	41
要求 60: 控制系统	41
要求 61: 保护系统 (6.32-6.33)	41
要求 62: 仪器仪表和控制系统的可靠性和可测试性 (6.34-6.36)	42
要求 63: 基于计算机的设备在安全重要系统中的使用 (6.37)	42
要求 64: 保护系统和控制系统相分离 (6.38)	43

要求 65: 主控室 (6.39-6.40A).....	43
要求 66: 辅控室 (6.41).....	44
要求 67: 现场应急响应设施 (6.42).....	44
应急电源 .....	44
要求 68: 能够经受住丧失厂外电源的设计 (6.43-6.45A).....	44
支持系统和辅助系统 .....	46
要求 69: 支持系统和辅助系统的性能 .....	46
要求 70: 热传输系统 (6.46).....	46
要求 71: 工艺取样系统和事故后取样系统 (6.47).....	46
要求 72: 压缩空气系统 .....	46
要求 73: 空调系统和通风系统 (6.48-6.49).....	46
要求 74: 消防系统 (6.50-6.54) .....	47
要求 75: 照明系统 .....	48
要求 76: 桥式起重设备 (6.55).....	48
其他功率转换系统 .....	48
要求 77: 蒸汽供应系统、给水系统和汽轮发电机 (6.56-6.58).....	48
放射性流出物和放射性废物的处理 .....	49
要求 78: 废物处理和控制系统 (6.59-6.60).....	49
要求 79: 流出物的处理和控制系统 (6.61-6.63).....	49
燃料装卸和贮存系统 .....	50
要求 80: 燃料装卸和贮存系统 (6.64-6.68A).....	50
辐射防护 .....	52
要求 81: 辐射防护设计 (6.69-6.76) .....	52
要求 82: 辐射监测手段 (6.77-6.84) .....	53
<b>参考文献 .....</b>	<b>55</b>
<b>定义 .....</b>	<b>57</b>
<b>参与起草和审查的人员 .....</b>	<b>59</b>

# 1. 导 言

## 背景

1.1. 本出版物替代 2012 年作为国际原子能机构《安全标准丛书》第 SSR-2/1 号印发的“安全要求”出版物《核电厂安全：设计》<sup>1</sup>。它考虑了 2006 年出版的《基本安全原则》[1]。促进核安全的各种要求旨在确保达到“可以合理实现的最高安全标准”，以保护工作人员、公众和环境免受核电厂和其它核设施可能引起的电离辐射的有害影响[1]。人们认识到，技术和科学知识都在向前发展，因此，需要从目前的知识水平出发考虑核安全和提供充分保护以防止辐射危险。安全要求需要与时俱进，本“安全要求”出版物所反映的是目前已有的共识。

1.2. 许多现有核电厂和新核电厂的设计已经提高到包括采取补充措施，以减轻涉及多重故障的复杂的系列事故和严重事故的影响。许多现有核电厂已经加装了具有新能力的互补系统和设备，以有助于预防严重事故和减轻其后果。对大多数现有核电厂提供了关于减轻严重事故后果方面的导则。新核电厂的设计现在明确包括了考虑严重事故假想方案和战略，以促进对其进行管理。核电厂的设计还考虑了国家核材料衡算和控制系统相关要求和安保相关要求。安全措施和安保措施的一体化将有助于确保两者之间不相互掣肘。

1.3. 将本“安全要求”出版物中有关设计的所有要求适用于已在运行或在建的核电厂也许并不切实可行。此外，修改已得到监管机构核准的设计可能也行不通。就对这种设计进行安全分析而言，预计将例如作为电厂定期安全评审的一部分按照现行标准进行一次比较活动，以确定是否可以通过实施实际合理的安全改进进一步加强电厂的安全运行。

---

<sup>1</sup> 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）。

## 目的

1.4. 本出版物规定对于核电厂结构、系统和部件以及对安全重要程序和组织过程的设计要求，这些都是为实现核电厂安全运行和防止可能危及安全的各种事件或在发生这种事件的情况下减轻其后果而必须满足的要求。

1.5. 本出版物供从事核电厂设计、制造、建造、改造、维护、运行和退役和开展分析、核实和评审及提供技术支持的组织和监管机构使用。

## 范围

1.6. 本出版物预计主要用于装有为发电或其他供热应用（诸如区域集中供热或海水淡化）而设计的水冷反应堆的陆基固定式核电厂。就其他类型的反应堆而言，本出版物在经过判断后也可适用于确定在它们的设计中必须考虑的要求。

1.7. 本出版物不述及：

- (a) 原子能机构其他“安全要求”出版物（如原子能机构《安全标准丛书》第 GSR Part 4 (Rev.1) 号《设施和活动的安全评定》[2]）中具体涵盖的要求；
- (b) 与核安保或国家核材料衡算和控制系统有关的问题；
- (c) 决不可能影响核电厂安全的传统工业安全；
- (d) 由核电厂运行所引起的非放射影响。

1.8. 本出版物中的术语将根据原子能机构《安全术语》[3]中的定义和说明加以解释，除非本出版物中另有说明（见“定义”）。

## 结构

1.9. 本“安全要求”出版物依据安全目标与安全原则之间以及对核安全功能的要求与安全设计准则之间的关系进行叙述。第 2 章详述安全目标、安全原则和概念，它们是导出必须予以满足的核电厂安全功能要求以及安



全设计准则的基础。第 3 章至第 6 章规定经编号的总体要求（黑体字），并适当时在其后各段落中规定补充要求。第 3 章规定设计组织要在设计过程的安全管理中加以满足的一般要求。第 4 章规定对安全的主要技术设计准则的要求，包括对基本安全功能、实施纵深防御和建造准备的要求；对安全与核安保以及与国家核材料衡算和控制系统相互接口的要求；以及对确保由核电厂引起的辐射危险水平保持在可合理达到的尽量低的要求。第 5 章规定对电厂总体设计的要求，这些要求是对主要技术设计准则所作的补充，目的是确保安全目标得到实现和安全原则得到实施。对电厂总体设计的要求适用于所有安全重要物项（即结构、系统和部件）。第 6 章规定适用于反应堆堆芯、反应堆冷却剂系统、安全壳系统以及仪器仪表和控制系统等电厂特定系统的设计要求。

## 2. 适用安全原则和概念

2.1. 《基本安全原则》[1]规定了一项基本安全目标和 10 项安全原则，从而为促进保护人类和环境免于辐射危险以及为引起辐射危险的设施和活动的安全要求和措施奠定了基础。

2.2. 必须在不对产生辐射危险的设施的运行或活动的开展施加不当限制的情况下实现该基本安全目标和实施这 10 项安全原则。为确保核电厂的运行和活动的开展能够达到合理的最高安全标准，必须采取措施以实现以下目标（见《基本安全原则》[1]第 2.1 段）：

- (a) 控制运行状态中对人的辐射照射和向环境的放射性释放；
- (b) 限制可能导致核电厂核反应堆堆芯、核链式反应、辐射源、乏核燃料、放射性废物或任何其他辐射源失控事件发生的可能性；
- (c) 在发生这类事件的情况下减轻其后果。

2.3. 基本安全目标适用于核电厂寿期内的所有阶段，包括规划、选址、设计、制造、建造、调试和运行以及退役。这包括放射性物质的相关运输以及乏核燃料和放射性废物的管理（见《基本安全原则》[1]第 2.2 段）。

2.4. 《基本安全原则》[1]第 2.3 段指出：

“为了实现这一基本安全目标，制订了 10 项安全原则，在此基础上制订了安全要求，并将执行安全措施。安全原则是一套整体适用的原则，尽管在实践中针对具体情况各项原则的重要性可能有所不同，但所有相关原则均需适当地加以适用。”

2.5. 本“安全要求”出版物规定对核电厂的设计特别重要的那些安全原则的适用要求。

## 设计中的辐射防护

2.6. 为了履行安全原则，必须确保对核电厂的所有运行状态和对任何相关活动而言，将来自电厂范围内的辐射照射剂量或由于电厂放射性物质的任何已计划的释放所引起的照射剂量保持在剂量限值以下，并且保持在可合理达到的尽量低的水平。此外，还必须在出现任何事故的情况下采取减轻事故放射后果的措施。

2.7. 为了实施安全原则，还必须将核电厂设计和运行在使一切辐射源处于严格的技术和行政管理控制之下。但是，该原则不排除有限的照射，也不排除处于运行状态的核电厂向环境释放规定数量的放射性物质。这种照射和放射性释放必须受到严格的控制，并保持在符合监管和运行限值以及辐射防护要求可合理达到的尽量低的水平[4]。

## 设计安全

2.8. 为了在核电厂的设计中达到合理的最高安全水平，应当为以下目的采取与国家验收标准和安全目标相一致的措施[1]：

- (a) 防止由于反应堆堆芯或其他辐射源失控引起的具有有害后果的事故，并减轻所发生的任何事故的后果；
- (b) 确保对装置设计中考虑到的所有事故而言，任何放射后果都将低于相关限值，并将保持在可合理达到的尽量低的水平；

(c) 确保有严重放射后果的事故发生的可能性极低，并将这种事故的放射后果减少到尽实际可能的最小程度。

2.9. 为了证明在核电厂的设计中实现了基本安全目标[1]，必须对设计进行全面的安全评定[2]。评定的目的是查明一切可能的辐射源，并估算出电厂运行使装置内的工作人员和厂外公众可能受到的辐射剂量及对环境可能产生的影响。必须进行安全评定，以审查：(1) 电厂的正常运行情况；(2) 电厂在发生预计运行事件情况下的性能；(3) 事故工况。在进行这种分析的基础上，就能确定设计对假想始发事件和事故的承受能力、验证安全重要物项的有效性和确定对应急计划的输入（先决条件）。

2.10. 应当采取各种措施，以便将所有运行状态下的照射控制在可合理达到的尽量低的水平，并将可能导致辐射源失控事故的可能性减至最低程度。尽管如此，但仍有可能发生事故。应当采取各种措施，以确保减轻事故的放射后果。此类措施包括：提供安全设施和安全系统；营运组织制订事故管理规程；主管部门在可能的情况下制定并在必要时得到营运组织支持的厂外防护行动，以减轻发生事故情况下的照射。

2.11. 核电厂的安全设计必须适用采取实际措施减轻核事件或辐射事故对人类生命和健康及环境的影响的如下安全原则（《基本安全原则》[1]原则 8）。必须“实际上消除”可能导致高辐射剂量或大规模放射性释放量的电厂系列事件<sup>2</sup>，发生频率高的电厂系列事件不得存在潜在的放射后果或只能存在轻微的放射后果。一个重要的目标是采用技术手段限制甚至排除采取厂外防护行动以减轻放射后果的必要性，但负责部门或许仍会要求采取此类措施。

## 纵深防御

2.12. 防止核电厂事故和发生事故情况下减轻事故后果的主要手段是应用纵深防御概念[1、5、6]。该概念适用于所有安全相关活动，而不论是组织

---

<sup>2</sup> 如果某些工况的出现完全不可能，或者如果有很大的把握认为这些工况极不可能出现，则出现这些工况的可能性可以被视为已“实际上消除”。

的、行为的还是与设计有关的活动，也不论是处在满功率、低功率还是各种停堆状态。这是为了确保所有安全相关活动都遵守独立存在的各种不同层级的规定，以便在发生故障时能够利用适当的措施探查和补救或纠正故障。在设计和运行的整个过程中应用纵深防御概念，就能保护免于发生预计运行事件和事故，包括由厂内设备故障或人因事件引起的那些事故，并免于出现源于厂外事件的后果。

2.13. 《基本安全原则》[1]第 3.31 段指出：

“纵深防御主要通过将一系列连续和独立的防护层结合起来加以实施，并且在人员或环境可能受到有害影响之前，这些防护层必须不能失效。如果某一层保护或屏障失效，后续保护层或屏障就应发挥作用。不同防御层的独立效能是纵深防御的一个必要组成部分。”

共有五个层级的防御：

- (1) 第一层级防御的目的是防止偏离正常运行和安全重要物项出现故障。这便导致提出了以下要求，即应当按照质量管理实践及适当且经过证明的工程实践可靠且保守地进行电厂的选址、设计、建造、维护和运行。为了实现这些目标，应谨慎地注意：选用合适的设计规程和材料；对部件的制造及电厂的建造进行质量控制；以及对电厂进行调试。减少造成内部危害可能性的设计方案有助于防止这一防御层级的事故。还要注意以下方面：与设计、制造、建造以及在役检查、维护和测试有关的工艺和规程；使这些活动易于进行；电厂的运行方式；以及如何利用运行经验。对这一过程提供支持的方式是开展详细的分析，以确定对电厂运行和维护的要求以及对运行和维护实践质量管理的要求。
- (2) 第二层级防御的目的是探知和控制偏离正常运行状态的情况，以防止电厂的预计运行事件逐步升级到事故工况。这是考虑到以下事实，即尽管在核电厂的运行寿命内千方百计防止发生假想始发事件，但还是有可能发生这种事件。这种第二层级的防御使得有必要：在设计中提供特定系统和设施；通过安全分析确认其有效性；并制订各种运行程

序，以防止发生此类始发事件或尽量减轻其后果，并使电厂回到安全状态。

- (3) 对第三层级防御所作的假设是，上一层级防御或许未能控制某些预计运行事件或假想始发事件的逐步升级，并可能由此酿成事故，尽管这是非常不可能的。在电厂的设计中，这种事故是假定会发生的。这便导致提出以下要求，即固有和（或）专设安全设施、安全系统和程序应当能够防止对反应堆堆芯造成损坏或防止需要厂外防护行动的放射性释放并使电厂回到安全状态。
- (4) 第四层级防御的目的是减轻第三层级纵深防御失灵所引起的事故后果。这通过防止此类事故发展和减轻严重事故后果来实现。严重事故情况中的安全目标是，将仅需要采取时间长度和适用范围有限的防护行动，以及避免或最大程度地减少厂外污染。需要“实际上消除”<sup>3</sup>将导致早期放射性释放或大规模放射性释放<sup>4</sup>的系列事件。
- (5) 第五层级也是最后一级防御的目的是减轻事故可能产生的放射性释放的放射后果。这就需要提供一套装备齐全的应急响应设施以及适用于厂内和厂外应急响应的应急计划和应急程序。

2.14. 核电厂纵深防御执行工作的一个相关方面是提供一系列实体屏障的设计以及将能动、非能动和固有安全特性结合起来，以促进发挥实体屏障在特定场所封闭放射性物质的有效性。所需屏障的数量将取决于放射性核素数量和同位素组成的初始源项、单个屏障的有效性、可能的内部和外部危害以及各种故障的潜在后果。

---

<sup>3</sup> 如果某些工况的出现完全不可能，或者如果有很大的把握认为这些工况极不可能出现，则出现这些工况的可能性可以被视为已“实际上消除”。

<sup>4</sup> 此范畴的“早期放射性释放”系将需要采取厂外防护行动但这些行动将未必适时产生全面效果的放射性释放。“大规模放射性释放”系时间长度和适用范围有限的厂外防护行动将不足以保护人员和环境的放射性释放。

## 在电厂整个寿期内保持电厂设计的完整性

2.15. 核电厂的设计、建造和调试工作可以由许多组织分担：工程公司、反应堆及其辅助系统供应商、主要部件供应商、电气系统设计公司以及对电厂安全具有重要意义的其他系统的供应商。

2.16. 对安全负主要责任的是对产生辐射危险的设施和活动负有责任的人员或组织（即营运组织）[1]。2003年，国际核安全咨询组已建议营运组织制订一项正式的过程，以便在电厂的整个寿期内即在运行寿期直至退役阶段维持电厂设计的完整性[7]。在该营运组织内部经正式指定的实体将承担起对该过程的责任。

2.17. 实际上，核电厂的设计只有在完整的电厂说明书（包括厂址细节）提交进行采购和许可证审批时才具有完整性。参考文献[7]强调了需要有一个经正式指定的实体总体负责设计过程，并负责批准修改设计和确保必要的知识得到维护。参考文献[6]还引入了“负责任的设计者”的概念，经正式指定的该实体可以指定这种设计者履行对电厂部分设计的具体责任。在申请电厂批准证书之前，设计责任将归属设计组织（即卖方）。一旦提出电厂批准证书的申请，有关安全的主要责任将归属申请者，尽管有关该设计的详细知识仍将归属“负责任的设计者”。这种平衡将随着电厂投入运行而发生改变，因为这其中的许多详细知识如安全分析报告、设计手册和其他设计文件中蕴含的知识将转让给营运组织。为了促进进行这种知识转让，将在早期阶段建立这种经正式指定的全面负责设计过程的实体结构。

2.18. 对经正式指定实体规定的在管理系统方面的要求也将适用于“负责任的设计者”。但有关维持电厂设计完整性的总体责任仍将归属经正式指定的实体，并因此最终归属营运组织。

## 3. 设计安全的管理

### 要求 1：电厂设计安全管理中的责任

核电厂建造和（或）运行许可证申请人必须负责确保提交监管机构的设计符合所有适用的安全要求。

3.1. 从事对核电厂设计安全具有重要性活动的组织包括设计组织<sup>5</sup>必须负责确保给予安全事项以最高优先地位。

## **要求 2：电厂设计管理系统**

**设计组织必须建立和实施管理系统，以确保在设计过程的所有阶段均考虑并实施为电厂设计所确定的所有安全要求，并确保在最后设计中达到这些要求。**

3.2. 管理系统<sup>6</sup>必须包括关于始终确保每一结构、系统和部件设计质量以及核电厂总体设计的规定。这包括查明和纠正设计缺陷、检验设计的充分性和控制设计变更的手段。

3.3. 电厂设计包括后来的变更、修改或安全改进必须按照建立在适当的工程规范和标准基础上的既定程序进行并须纳入相关要求和设计基准。它们之间的接口必须予以明确和得到控制。

3.4. 电厂设计包括设计工具和设计的输入与输出的充分性必须由独立于原先从事设计工作的个人或团体进行核实和验证。电厂设计的核实、验证和核准工作必须在设计和建造过程中尽实际可能尽快完成，而且无论如何应在电厂开始运行之前完成。

## **要求 3：电厂设计在电厂整个寿期内的安全性**

**营运组织必须建立一个正式的体系，以确保电厂设计在核电厂整个寿期内的持续安全性。**

3.5. 确保电厂设计持续安全性的正式体系必须包括一个经正式指定的实体，由其负责营运组织管理系统内电厂设计的安全。在各项安排中必须考虑对负责电厂具体部件设计的外部组织（被称为“负责任的设计者”）所赋予的任务。

---

<sup>5</sup> 设计组织是负责编制拟建电厂最后详细设计的组织。

<sup>6</sup> 国际原子能机构《安全标准丛书》第 GS-R-3 号《设施和管理系统》[8]确定了关于管理系统的要求。

3.6. 经正式指定的实体必须确保电厂设计达到安全、可靠性和质量方面与相关国家和国际准则以及标准、法律和条例相一致的验收标准。必须规定并实施一系列任务和职能，以确保：

- (a) 电厂设计与用途相符，并通过使辐射危险保持在可合理达到的尽量低的水平来满足防护和安全最优化的要求；
- (b) 确保电厂设计持续安全性的正式体系中包括设计核实、对工程规范和标准及要求的定义、采用经证明的工程实践、提供建造信息和经验反馈、关键工程文件的核准、开展安全评定和保持安全文化；
- (c) 可以获得电厂安全运行、维护（包括适当的测试间隔时间）和改造所需的设计知识，营运组织将这种知识维护到最新状态，并充分考虑以往的运行经验和经验证的研究结果；
- (d) 对设计要求的管理和配置控制得以维持；
- (e) 与负责设计者和参与设计工作的供应商之间必要的接口得到建立和控制；
- (f) 必要的工程专门知识和科技知识在营运组织内部得到维护；
- (g) 电厂的所有设计变更都经过审查、核实、成文记录和核准；
- (h) 适当的文件得以保留，以便利电厂今后开展退役工作。

## 4. 主要技术要求

### 要求 4：基本安全功能

在所有电厂状态下均须确保实现核电厂的以下基本安全功能：(1) 反应性控制；(2) 从反应堆和燃料贮存池排热；(3) 封闭放射性物质，屏蔽辐射和控制已计划的放射性释放，以及限制放射性的意外释放。



4.1. 必须采取系统性方案来确定实现基本安全功能所需的这些安全重要物项，以及确定正在促进实现或影响所有电厂状态下的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测的手段，以确保实现所要求的安全功能。

### **要求 5：设计中的辐射防护**

**核电厂的设计必须做到确保：电厂工作人员和公众所受辐射剂量不超过剂量限值；辐射剂量在电厂整个寿期的运行状态下保持在可合理达到的尽量低的水平；辐射剂量在事故工况下和之后仍低于可接受限值并仍保持在可合理达到的尽量低的水平。**

4.3. 设计必须做到确保已“实际上消除”<sup>7</sup>电厂出现可能导致高辐射剂量或高放射性释放量的状态，很可能出现的电厂状态将没有或只有轻微的潜在放射后果。

4.4. 必须按照监管要求确定与相关类型电厂状态有关的用于辐射防护<sup>8</sup>的目的的可接受限值。

### **要求 6：核电厂的设计**

**核电厂的设计必须确保电厂和安全重要物项具有适当的特性，以确保安全功能可以必要的可靠性得到发挥，电厂可以在其整个设计寿期在运行限值和工况范围内安全运行并可以安全退役，并且将对环境的影响减少到最低程度。**

4.5. 核电厂的设计必须做到确保全部满足对营运组织的安全要求、对监管机构的要求和对相关立法的要求以及适用的国家和国际规程和标准，并

---

<sup>7</sup> 如果某些工况的出现完全不可能，或者如果有很大的把握认为这些工况极不可能出现，则出现这些工况的可能性可以被视为已“实际上消除”。

<sup>8</sup> 国际原子能机构《安全标准丛书》第 GSR Part 3 号《国际辐射防护和辐射源安全基本安全标准》[9]确定了关于辐射防护以及设施和活动辐射源安全的要求。

确保充分考虑人的能力和局限以及可能影响人力绩效的各种因素。必须提供充足的设计资料，以确保电厂的安全运行和维护，并允许以后能对电厂进行改造。必须提供经推荐的实践，以便将其纳入电厂的行政管理程序和运行程序（即运行限值和工况）。

4.6. 设计必须充分考虑其他核电厂的设计、建造和运行中取得的相关可得经验以及相关研究计划的成果。

4.7. 设计必须充分考虑确定性安全分析和概率安全分析的结果，以确保充分考虑预防事故和减轻所发生事故的后果。

4.8. 设计必须做到确保借助适当的设计措施以及运行与退役实践，使放射性废物的产生和排放量从活度和体积两个方面均保持在实际的最低水平。

## **要求 7：实施纵深防御**

**核电厂的设计必须体现纵深防御。纵深防御的各个层级必须尽实际可能相互独立。**

4.9. 必须实施纵深防御概念，以提供多层次防御，预防可能导致对人类和环境产生有害影响的事故后果，并确保在防护失败的情况下采取适当措施保护人类和环境以及减轻后果。

4.10. 设计必须充分考虑这样的事实，即当缺少某一层级防御时，多层次防御的存在并不是继续运行的依据。必须保持所有层级的纵深防御措施始终存在和发挥作用，任何放松都必须证明拟采取的具体运行模式的正当性。

4.11. 设计：

(a) 必须提供多重实体屏障，防止放射性物质释入环境；

- (b) 必须具有保守性，且建造必须是高质量的，从而确保故障和偏离正常运行情况被减至最少，尽实际可能预防了事故，以及电厂参数的微小误差不会导致陡边效应；<sup>9</sup>
- (c) 必须规定通过固有和专设设施控制电厂行为，以便尽可能地依靠设计本身使需要启动安全系统的故障和偏离正常运行情况减到最少程度或者予以排除；
- (d) 必须规定通过自动启动安全系统对电厂控制加以补充，以便可以很有把握地控制超出控制系统能力的故障和偏离正常运行情况，并尽量减少操作人员在出现故障或偏离正常运行情况的早期阶段采取行动的必要性；
- (e) 必须规定通过系统、结构和部件以及程序控制超出安全系统能力的故障和偏离正常运行情况过程，并尽实际可能限制其后果；
- (f) 必须提供多重手段来确保实现每项基本安全功能，从而确保这些屏障的有效性和减轻任何故障或偏离正常运行情况的后果。

4.12. 为了确保纵深防御概念得到保持，设计必须尽实际可能地防止：

- (a) 对实体屏障的完整性提出质疑；
- (b) 一道或多道屏障失效；
- (c) 一道屏障因另一道屏障的失效而失效；
- (d) 运行和维护失误出现有害后果的可能性。

4.13. 设计必须做到尽实际可能地确保第一层级，至多第二层级防御能够防止核电厂运行寿期内可能发生的所有故障或偏离正常运行情况升级到事故工况。

---

<sup>9</sup> 在核电厂，“陡边效应”是这样一种情况，即由于电厂参数出现微小偏差后导致电厂从一种状况向另一种状况突变而引起电厂行为严重异常，从而造成在对输入数据中的微小变化作出响应时电厂工况突然发生大的变化。

4.13A. 纵深防御的各个层级必须尽实际可能相互独立，以避免一个层级的失灵减少其他层级的有效性。特别是，设计扩展工况的安全特性（尤其是用于减轻涉及燃料熔化的事故后果的特性）必须尽实际可能地独立于安全系统。

#### **要求 8：安全与安保和保障之间的接口**

必须以统筹兼顾的方式设计和实施核电厂的安全措施、核安保措施和国家核材料衡算和控制安排，以免其相互掣肘。

#### **要求 9：经证明的工程实践**

核电厂的安全重要物项必须按照相关国家和国际规程和标准进行设计。

4.14. 核电厂的安全重要物项必须最好属于已在以往相同的应用中得到证明的设计，否则，必须属于具有高质量和含有已得到认证和试验技术的物项。

4.15. 必须对被用作安全重要物项设计规则的国际规范和标准进行鉴别和作出评价，以确定它们的适用性、适当性和充分性，并须在必要时加以补充或修改，以确保设计的质量与相关的安全功能相适应。

4.16. 在引入未经证明的设计或特性的情况下，或在存在偏离成熟的工程实践的情况下，必须通过适当的支持性研究计划、以实施具体的验收标准进行的性能测试或仔细地研究从相关的其他应用中获得的运行经验来论证安全性。还必须尽实际可能在新设计或新特性或新实践交付使用前对其进行充分试验，并在使用中进行监测，以核实电厂行为是否已达到预期效果。

#### **要求 10：安全评定**

必须在核电厂的整个设计过程中开展全面的确定性安全评定和概率安全评定，以确保电厂设计的所有安全要求在电厂寿期的所有阶段均得到满足，并确认所交付的设计满足对于制造和建设的要求以及在建造、运行和改造时也符合要求。

4.17. 必须在设计过程中及早开始进行安全评定<sup>10</sup>，同时反复交替进行设计活动和证实性分析活动，而且还必须随着设计计划的进展不断增加评定的范围和详细程度。

4.18. 必须以便于独立评价的形式将安全评定情况记录在案。

#### **要求 11：建造规定**

**核电厂安全重要物项必须设计得能够按照确保实现设计技术规格和所需安全水平的既定程序进行制造、建造、装配、安装和建立。**

4.19. 在有关建造和运行的规定中，必须充分考虑其他类似电厂及其有关结构、系统和部件的建造中已经取得的相关经验。在采用其他相关行业的最佳实践的情况下，这种实践必须表现出适合于具体的核应用。

#### **要求 12：纳入便于进行放射性废物管理和退役的特性**

**在核电厂的设计阶段，必须特别考虑纳入便于进行核电厂放射性废物管理以及今后进行退役和拆除的特性。**

4.20. 设计必须特别充分考虑：

- (a) 材料的选择，以便尽实际可能将放射性废物量减至最小，并便于去污；
- (b) 可能必要的接近能力和操作手段；
- (c) 管理（即分离、表征、分类、预处理、处理和整备）和贮存运行中所产生的放射性废物所需的设施以及关于电厂退役将产生的放射性废物的管理。

---

<sup>10</sup> 第 GSR Part 4 (Rev.1) 号[2]确定了设施和安全评定的要求。

## 5. 电厂总体设计

### 设计基准

#### 要求 13：电厂状态种类

必须确定电厂状态并须主要根据电厂状态在核电厂的发生频率将它们划分为有限数量的种类。

5.1. 电厂状态通常须涵盖：

- (a) 正常运行；
- (b) 预期在电厂运行寿期内发生的预计运行事件；
- (c) 设计基准事故；
- (d) 设计扩展工况，包括引起堆芯熔化的事故。

5.2. 必须为每种电厂状态规定准则，以使频繁发生的电厂状态不产生或仅产生轻微的放射后果，并使可能引起严重后果的电厂状态保持极低的发生频率。

#### 要求 14：安全重要物项的设计基准

安全重要物项的设计基准必须针对相关运行状态、事故工况以及内部和外部危害导致的工况规定必要的的能力、可靠性和功能性，以满足核电厂寿期内的具体验收标准。

5.3. 必须系统地证明每个安全重要物项设计基准的合理性并将设计基准形成文件。这种文件必须提供营运组织安全运行电厂所需的资料。

#### 要求 15：设计限值

必须为所有运行状态和事故工况规定一套与核电厂每一安全重要物项的关键物理参数相一致的设计限值。

5.4. 必须规定设计限值，而设计限值必须与相关国家和国际标准和规程及相关监管要求相一致。

#### **要求 16：假想始发事件**

**核电厂的设计必须采取系统性方案来确定整套假想始发事件，以便在设计中预测和考虑到全部具有潜在严重后果的可预见事件和全部具有较高发生频率的可预见事件。**

5.5. 必须在工程判断以及将确定性评定和概率评定相结合的基础上确定假想始发事件。必须提供对确定性安全分析和概率安全分析利用程度的理由，以表明业已考虑到了所有可预见的事件。

5.6. 假想始发事件必须包括电厂所有可预见的结构、系统和部件故障，以及运行误差和内部与外部危害可能引起的故障，而无论电厂是处于满功率、低功率还是停堆状态。

5.7. 必须对电厂的假想始发事件进行分析，以确定所需的预防措施和保护措施，从而确保实施所要求的安全功能。

5.8. 在任何假想始发事件中，电厂的预期行为均须做到能够实现以下状况（以重要程度为序）：

- (1) 假想始发事件将不造成重要的安全影响，或将只造成电厂趋于通过其固有特性实现电厂安全状况的变化。
- (2) 发生假想始发事件后，电厂将借助非能动安全特性或在控制这种假想始发事件所必需的状况下连续运行的系统动作进入安全状态。
- (3) 发生假想始发事件后，电厂将通过启动响应假想始发事件而需投入运行的安全系统进入安全状态。
- (4) 发生假想始发事件后，电厂将通过遵循规定程序进入安全状态。

5.9. 必须将用于制订安全重要物项的性能要求和进行电厂总体安全评定和详细分析的假想始发事件纳入规定数量的有代表性的事件序列种类，这些序列确定极端情况并为安全重要物项的设计和运行限值提供基准。

5.10. 必须提供以技术为支持的正当理由才能从设计中排除根据整套假想始发事件确定的任何始发事件。

5.11. 在需要为响应假想始发事件而立即采取可靠行动的情况下，必须在设计中规定自动安全动作，以使安全系统进行必要的启动，从而防止发展成为更严重的电厂工况。

5.12. 在不需要响应假想始发事件立即采取行动的情况下，可允许依靠手动来启动系统或由操纵员采取其他行动。就这类情况而言，发现异常事件或事故和采取所需行动之间的时间间隔应当足够长，并必须规定适当的程序（如行政程序、运行程序和应急程序），以确保这些行动的执行。必须对操纵员因设备误操作或对必要恢复过程作出不正确诊断而导致事件序列恶化的可能性作出评定。

5.13. 必须通过提供用于监测电厂状况的适当仪器仪表和供手动操作设备使用的适当控制装置，促进操纵员在发生假想始发事件后采取诊断电厂状态和使电厂及时处于长期稳定停堆工况所需的行动。

5.14. 设计必须规定提供所需设备并规定必要的程序，以便提供手段保持对电厂的控制和减轻失控所造成的任何有害后果。

5.15. 手动响应和恢复过程中采取行动所需的任何设备均须安放在最适宜的位置，以确保需要时能够随时使用和预期环境条件下能够安全地接触它们。

## **要求 17：内部和外部危害**

**必须确定所有可预见的内部危害和外部危害，包括人因事件直接或间接影响核电厂安全的可能性，并须评价它们的影响。必须在设计电厂布置**



**和确定假想始发事件和所产生的负荷时考虑各种危害，以用于电厂安全重要相关物项的设计。**

5.15A. 必须在适当考虑对安全的其他影响的情况下设计和布置安全重要物项，以便能够经受住各种危害的影响或根据它们的安全重要性防范危害和防范危害产生的共因故障机制。

5.15B. 对于多机组电厂厂址，设计必须适当考虑到特定危害导致对厂址上的若干机组或甚至所有机组同时造成影响的可能性。

### **内部危害**

5.16. 设计必须适当考虑内部危害，如失火、爆炸、发水、产生喷射物、结构坍塌和物体坠落、管道甩动、喷射冲击以及流体从破损系统或厂区其他装置的泄放。必须提供适当的预防和缓解特性，以确保安全不受到损害。

### **外部危害**

5.17. 设计必须包括适当考虑那些在厂址评价过程中已经确定的自然和人因外部事件<sup>11</sup>（如源于电厂以外的事件）。必须考虑在假想潜在危害时的因果关系和可能性。短期而言，不得允许电厂安全依赖于电力供应和消防服务之类的厂外服务的可获得性。设计必须适当考虑厂址特定条件，以确定厂外服务最迟需要到位的最大延迟时间。

5.18. 此段已删除，其内容经扩大范围后被移至新增第 5.15A 段。

5.19. 必须提供特性，尽最大限度减少包含安全重要物项（包括电力电缆和控制电缆）的建筑物和电厂任何其他结构之间因设计中考虑的外部事件而发生的任何相互作用。

5.20. 此段已删除，其内容经扩大范围后被移至新增第 5.15A 段。

---

<sup>11</sup> 国际原子能机构《安全标准丛书》第 NS-R-3 (Rev.1) 号《核装置的厂址评价》[10] 确定了对核装置厂址评价的要求。

5.21. 电厂的设计必须提供充分的裕度，以保护安全重要物项免于设计时将考虑的源于厂址危害评价的各种程度的危害和避免陡边效应。<sup>12</sup>

5.21A. 电厂的设计还必须提供充分的裕度，以便在发生超出设计时所考虑的源于厂址危害评价的自然危害程度的自然危害情况下，保护防止早期放射性释放或大规模放射性释放最终所需的物项。

5.22. 此段已删除，其内容经扩大范围后被移至新增第 5.15B 段。

### **要求 18：工程设计规则**

**核电厂安全重要物项的工程设计规则必须明确确定，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实践，同时适当考虑到它们与核电技术的相关性。**

5.23. 在核电厂的设计中，必须适用确保可靠设计的方法，并且必须遵守成熟的工程实践，以确保在所有运行状态中和所有事故工况下实现基本安全功能。

### **要求 19：设计基准事故**

**必须根据假想始发事件推导应当在设计中考虑的一系列事故，以便确定核电厂应承受的边界条件，而不超出可接受的辐射防护限值。**

5.24. 必须利用设计基准事故来确定安全系统和控制设计基准事故工况所需的其他安全重要物项的设计基准，包括性能标准，目的是使电厂恢复安全状态和减轻事故后果。

5.25. 设计必须做到就设计基准事故工况而言，电厂关键参数不超出特定设计限值。一个主要目标必须是控制所有设计基准事故，使之在厂内和厂外均不产生或仅产生轻微的放射后果，并且不需要采取任何厂外防护行动。

---

<sup>12</sup> 在核电厂，“陡边效应”是这样一种情况，即由于电厂参数出现微小偏差后导致电厂从一种状况向另一种状况突变而引起电厂行为严重异常，从而造成在对输入数据中的微小变化作出响应时电厂工况突然发生大的变化。

5.26. 必须以保守方式分析设计基准事故。这种方案涉及在分析中对安全系统的某些故障作出假想、确定设计标准及在分析中使用保守假设、模型和输入参数。

#### **要求 20：设计扩展工况**

**必须在工程判断、确定性评定和概率评定的基础上推导出一系列设计扩展工况，以便增强核电厂在不造成不可接受的放射后果情况下承受比设计基准事故更严重或涉及更多故障的事故的能力，从而进一步加强电厂的安全性。必须使用这些设计扩展工况来确定将在设计中处理的更多事故假想情况和对制订防止这类事故或减轻事故后果的实际规定做出规划。**

5.27. 必须对电厂开展有关设计扩展工况的分析<sup>13</sup>。考虑设计扩展工况的主要技术目的是提供关于电厂的设计能够防止未被视为设计基准事故工况的那些事故工况或实际合理地减轻那些事故工况的后果的保证。这可能要求针对设计扩展工况增加安全特性，或扩大安全系统以防止严重事故或减轻严重事故后果或维持安全壳完整性的能力。增加适合于设计扩展工况的安全特性或扩大安全系统的能力，必须确保对安全壳中存在大量放射性物质（包括反应堆堆芯严重降质导致产生的放射性物质）的事故工况进行控制的能力。电厂的设计必须做到能够将电厂置于受控制状态和能够保持安全壳的功能，从而“实际上消除”电厂出现可导致早期放射性释放或大规模放射性释放状态的可能性。<sup>14</sup>可在最佳估计方案的基础上分析对安全壳功能所做规定的有效性。

5.28. 必须利用设计扩展工况来确定安全特性的设计规格和防止产生这类工况或在这类工况产生后对其进行控制和减轻其后果所需的所有其他安全重要物项的设计基准。

---

<sup>13</sup> 可使用最佳估计方案对电厂设计扩展工况进行分析（亦可根据国家的要求，使用更严格的方案）。

<sup>14</sup> 如果某些工况的出现完全不可能，或者如果有很大的把握认为这些工况极不可能出现，则出现这些工况的可能性可以被视为已“实际上消除”。

5.29. 开展的分析必须包括确定旨在用于防止或能够<sup>15</sup>防止或减轻在设计扩展工况中所考虑的事件的特性。这些特性：

- (a) 必须在尽量实际的情况下独立于在更常见事故中使用的那些特性；
- (b) 必须能够在适当的情况下与这些设计扩展工况包括严重事故中的设计扩展工况有关的环境条件下发挥作用；
- (c) 必须具备与所要求满足的功能相称的可靠性。

5.30. 特别是，安全壳及其安全特性必须能够承受极端假想情况，这除其他外特别包括反应堆堆芯熔化。必须利用工程判断和源自概率安全评定的输入来选择这些假想情况。

5.31. 设计必须做到“实际上消除”出现可导致早期放射性释放或大规模放射性释放工况的可能性。<sup>16</sup>

5.31A. 设计必须做到，对于设计扩展工况，时间和适用范围有限的防护行动必须足以保护公众，并必须为采取这类措施提供充足的时间长度。

## **事件和故障并发**

5.32. 在工程判断、确定性安全评定和概率安全评定的结果显示事件的并发可能导致预计运行事件或事故工况的情况下，必须将这类事件的并发视为设计基准事故或将其作为设计扩展工况的一部分纳入设计扩展工况，这主要取决于它们发生的可能性。某些事件可能是其他事件的后果，如地震后发生的洪水。这种继发效应必须视为原来的假想始发事件的一部分。

---

<sup>15</sup> 为使电厂恢复安全状态或减轻事故后果，可考虑利用电厂的整个设计能力或临时利用附加系统。

<sup>16</sup> 如果某些工况的出现完全不可能，或者如果有很大的把握认为这些工况极不可能出现，则出现这些工况的可能性可以被视为已“实际上消除”。

## **要求 21：安全系统的实体分隔和独立性**

必须酌情通过实体分隔、电气隔离、功能独立和通讯（数据传输）独立等手段防止安全系统之间或系统冗余单元之间的相互干扰。

5.33. 就安全系统的每个冗余单元而言，电厂内的安全系统设备（包括电缆和线槽）必须易于识别。

## **要求 22：安全分类**

必须确定所有安全重要物项并根据其功能和安全性对其进行分类。

5.34. 划分安全重要物项的安全性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) 不能执行安全功能的后果；
- (c) 需要该物项执行某一安全功能的频率；
- (d) 假想始发事件后需要该物项执行安全功能的时间或时间段。

5.35. 设计必须做到确保防止安全重要物项之间的任何相互干扰，特别是确保较低安全类别的系统中的安全重要物项的任何故障都不会蔓延到较高安全类别的系统。

5.36. 必须将执行多重功能的设备划入与该设备所执行的最重要功能相一致的安全等级。

## **要求 23：安全重要物项的可靠性**

安全重要物项的可靠性必须与其安全性相称。

5.37. 安全重要物项的设计必须做到确保能够进行设备的验证、采购、安装、调试、运行和维护，使之能够以充分的可靠性和有效性经受物项设计基准中规定的所有工况。

5.38. 在选择设备时，必须考虑误动作和不安全的故障模式。在选择设备过程中，必须优先考虑那种展示出可预测和已揭示的故障模式且所作设计便于对其进行维修或更换的设备。

#### **要求 24：共因故障**

设备的设计必须适当考虑安全重要物项发生共因故障的可能性，以确定必须如何应用多样性、冗余性、实体分离和功能独立这些概念，从而实现所需的可靠性。

#### **要求 25：单一故障准则**

必须对电厂设计中所考虑的每个安全组应用单一故障准则。

5.39. 必须把误动作视为将单一故障准则<sup>17</sup>用于某一安全组或安全系统时发生的一种故障模式。

5.40. 设计必须适当考虑非能动部件的故障，除非已在单一故障分析中以非常高的置信度证明该部件的可靠性，即该部件发生故障的可能性非常小并且其功能仍将不受假想始发事件的影响。

#### **要求 26：故障安全设计**

必须酌情将故障安全设计概念纳入安全重要系统和部件的设计中。

5.41. 安全重要系统和部件的设计必须酌情纳入故障安全行为，以便其故障或某一支持特性的故障不妨碍执行预定安全功能。

---

<sup>17</sup> “单一故障”系指导致某一系统或部件丧失执行其预定安全功能能力的一个故障以及由此造成的任何继发故障。“单一故障准则”系指适用于某一系统以使该系统必须能在发生任何单一故障情况下执行其任务的准则（或要求）。

## 要求 27：支持服务系统

必须相应对确保设备运行能力并构成安全重要系统一部分的支持服务系统进行分类。

5.42. 支持服务系统的可靠性、冗余性、多样性和独立性以及提供对其实施隔离和进行功能能力测试的特性必须与其所支持的系统的安全重要性相适应。

5.43. 不得允许支持服务系统的一个故障能够同时影响一个安全系统或一个执行各种安全功能的系统的若干冗余部件以及损害这些系统执行其安全功能的能力。

## 要求 28：安全运行的运行限值和条件

设计必须确定用于保证核电厂安全运行的一套运行限值和条件。

5.44. 核电厂设计中确定的要求及运行限值和条件必须包括（国际原子能机构《安全标准丛书》第 SSR-2/2（Rev.1）号《核电厂安全：调试和运行》[4]要求 6）：

- (a) 安全限值；
- (b) 限制安全系统设定值；
- (c) 用于保证正常运行的限值和条件；
- (d) 工艺变量和其他重要参数的控制系统约束值和程序约束值；
- (e) 对电厂的监视、维护、测试和检查要求，以确保结构、系统和部件发挥设计中预定的功能，并通过使辐射危险保持在可合理达到的尽量低的水平来满足最优化要求；
- (f) 规定的运行配置，包括安全系统或安全相关系统不能使用情况下的运行限制；
- (g) 行动说明，包括在响应偏离运行限值和条件的情况下完成行动的时间。

## 确保电厂寿期期间安全运行的设计

### 要求 29：安全重要物项的校准、测试、维护、维修、更换、检查和监测

核电厂安全重要物项的设计必须使得能够对它们进行所需的校准、测试、维护、维修或更换、检查和监测，以确保它们执行其功能的能力及维持它们在设计基准中规定的所有工况中的完整性。

5.45. 电厂布置必须做到便于进行校准、测试、维护、维修或更换、检查和监测活动，而且这些活动能够按照相关国家和国际规程和标准进行。这类活动必须与将执行的安全功能的重要性相适应，必须在不对工作人员造成不适当的过量照射的情况下进行。

5.46. 在计划在功率运行期间对安全重要物项进行校准、测试或维护的情况下，各系统的设计必须使得能够在不显著减少安全功能的性能可靠性的情况下执行这些任务。必须在设计中纳入有关在停堆期间进行安全重要物项校准、测试、维护、维修、更换或检查的规定，以便能够在不显著减少安全功能的性能可靠性的情况下执行这些任务。

5.47. 如果安全重要物项不能设计得能够进行所希望程度的测试、检查或监测，则必须提供纳入了以下方案的强有力的技术理由：

- (a) 必须规定其他一些经证明的替代方法和（或）间接方法，如监视测试参考物项或使用经核实和确认的计算方法。
- (b) 必须应用保守的安全裕度或采取其他适当的谨慎措施，以弥补可能的意外故障。

### 要求 30：安全重要物项验证

必须实施安全重要物项验证计划，以核实核电厂的安全重要物项在其设计寿命期间始终能够在必要时以及在当时发生的主要环境条件下执行预定功能，同时在维护和测试期间适当考虑到电厂工况。



5.48. 核电厂安全重要物项验证计划中所考虑的环境条件必须包括电厂设计基准中所预期的周围环境条件的变化。

5.49. 安全重要物项验证计划必须包括考虑环境因素（诸如振动、辐照、湿度或温度条件等）在安全重要物项的预期使用期内引起的老化效应。在安全重要物项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时，验证计划必须尽实际可能地通过测试、分析或两者的结合重现自然外部事件施加给安全重要物项的条件。

5.50. 任何可合理预计的和可能由具体运行状态如安全壳泄漏率的定期测试所引起的环境条件，均须包括在验证计划中。

### **要求 31：老化管理**

必须确定核电厂安全重要物项的设计寿命。在设计中必须提供适当的裕度，以便适当考虑相关老化、中子脆化和磨损机理以及与年龄有关的降质可能性，从而确保安全重要物项在其整个设计寿命期间执行其必要安全功能的能力。

5.51. 核电厂的设计必须适当考虑所有运行状态中归因于某一部件的老化和磨损效应，这些状态包括测试、维护、维护性停堆、假想始发事件期间的电厂状态和发生假想始发事件后的电厂状态。

5.52. 必须对监测、测试、取样和检查做出规定，以便评定在设计阶段所预测的老化机理和帮助确定电厂的意外行为或使用过程中可能发生的降质。

## **人为因素**

### **要求 32：确保操纵员最佳绩效的设计**

必须在核电厂设计过程初期就对人为因素包括人-机接口进行系统性考虑，并须在整個设计过程中持续进行这种考虑。

5.53 核电厂的设计必须规定实施使电厂进入安全状态所需全部同步操作所要求的最低数量的运行人员。

5.54. 已从类似电厂获得了运行经验的运行人员必须尽实际可能地积极参与由设计组织实施的设计过程，以确保在设计过程中尽早考虑设备的未来运行和维护。

5.55. 设计必须有助于运行人员履行职责和执行任务，而且必须限制操作失误的可能性和对安全造成的影响。设计过程必须适当考虑电厂布置和设备布置以及包括维护程序和检查程序在内的有关程序，以有利于运行人员和电厂之间在电厂所有状态下的相互作用。

5.56. 人-机接口的设计必须做到能够根据需要作出决定和采取行动的时间为操纵员提供全面而易于管理的信息。必须以简洁明了的方式向操纵员提供其作出行动决定所需的资料。

5.57. 必须向操纵员提供必要资料，以便：

- (a) 评定电厂在任何工况下的总体状态；
- (b) 在与电厂系统和设备相关的规定参数限值（运行限值和条件）范围内运行电厂；
- (c) 确认启动安全系统所需的安全动作能够在需要时自动启动，并且相关系统能够发挥预定作用；
- (d) 确定手动启动规定安全动作的必要性和时间。

5.58. 设计必须能够在充分考虑到执行动作可利用的时间、预期工况和对操纵员的心理要求的情况下有助于操纵员成功地完成各种动作。

5.59. 操纵员在短时间内进行干预的必要性必须保持最低程度，并且必须证明操纵员有充分的时间作出行动决定和采取行动。

5.60. 设计必须能够确保在发生影响电厂的事件后，控制室或辅助控制室内以及通往辅助控制室的通道上的沿途场所的环境状况不损害运行人员的防护和安全。

5.61. 运行人员工作场所和工作环境的设计必须符合人机工程学概念。

5.62. 在适当阶段必须纳入对与人为因素有关的特性的核实和验证，包括使用模拟机进行这种核实和验证，以确认已经确定操纵员需要采取的动作而且这些动作能够得到正确执行。

## 其他设计考虑因素

### 要求 33：多机组核电厂各机组的安全系统和设计扩展工况安全特性

多机组核电厂的每台机组都必须具备自身的安全系统，并必须具备自身的设计扩展工况安全特性。

5.63. 为了进一步增强安全性，在设计中必须考虑使多机组核电厂各机组之间能够相互连通的办法。

### 要求 34：含有易裂变材料或放射性物质的系统

核电厂中可能含有易裂变材料或放射性物质的所有系统的设计必须能够：防止发生可能导致向环境不受控制的放射性释放的事件；防止出现意外临界和过热；确保放射性释放在正常运行工况下保持在管理排放限值以下，在事故工况下保持在可接受的限值以下，并保持在可合理达到的尽量低的水平；以及有助于减轻事故的放射后果。

### 要求 35：用于热电联供、产热或海水淡化的核电厂

伴有热利用机组（如用于地区集中供热的机组）和（或）海水淡化机组的核电厂的设计必须能够防止在运行状态下和事故工况下出现使放射性核素从核电厂迁移到海水淡化机组或地区集中供热机组的过程。

### 要求 36：电厂的撤离路线

必须为核电厂提供数量充分并带有明确和持久标志的撤离路线，以及可靠的应急照明、通风和安全利用这些撤离路线所必需的其他服务。

5.64. 核电厂的撤离路线必须符合相关国家和国际辐射分区与消防要求以及相关国家工业安全和电厂安保要求。

5.65. 在发生内部事件或外部事件或同时发生设计中已考虑到的各种事件后，必须至少有一条路线可供用于工作场所和其他有人区域的撤离。

#### **要求 37：电厂通讯系统**

必须在整个核电厂范围内提供有效的通讯手段，以有助于在所有正常运行模式下进行安全运行，以及供发生所有假想始发事件后和在事故工况下使用。

5.66. 必须提供适当的警报系统和通讯手段，以便在核电厂现场和厂区中的所有人员在运行状态下和事故工况下都能得到警报和指令。

5.67. 必须在核电厂范围内和毗邻区域提供确保安全所需的适当而多样化的通讯手段以及与相关厂外机构进行通讯所需的这类通讯手段。

#### **要求 38：电厂出入控制**

必须通过对各种结构要素进行适当的布局，将核电厂与其周围环境隔离开来，从而能够对出入电厂实施控制。

5.68. 必须在建筑物的设计和厂址布局中采取措施，对运行人员和（或）设备包括应急响应人员和车辆进入核电厂实施控制，而且必须对防止人员和物资擅自进入电厂给予特别考虑。

#### **要求 39：防止擅自接触或干扰安全重要物项**

必须防止擅自接触或干扰包括计算机硬件和软件在内的安全重要物项的情况。

#### **要求 40：防止安全重要系统之间有害的相互作用**

必须评价核电厂内可能需要同时运行的安全重要物项发生有害相互作用的可能性，并且必须防止任何有害相互作用造成影响。

5.69. 在分析安全重要物项发生有害相互作用的可能性时，必须充分考虑实体的相互连通以及一个系统的运行、误操作或故障对其他重要系统的局

部环境条件的可能影响，以确保环境条件的变化不影响系统或部件发挥预定功能的可靠性。

5.70. 如果两个具有安全重要性的流体系统相互连通并在不同的压力下运行，则或者必须使这两种系统的设计都做到能够承受较高压力，或者必须采取措施，防止在较低压力下运行的系统超过设计压力。

#### **要求 41：电网与电厂之间的相互作用**

不得让电网的干扰因素包括预期的电网供电电压和电频变化损害核电厂安全重要物项的功能。

### **安全分析**

#### **要求 42：电厂设计的安全分析**

必须对核电厂的设计进行安全分析，并且必须在这种分析中应用确定性分析和概率分析，以便能够评价和评定各类电厂状态中的安全挑战。

5.71. 在安全分析的基础上，必须确认安全重要物项的设计基准及其与始发事件和事件序列的联系。<sup>18</sup> 必须证明所设计的核电厂能够满足有关放射性释放的管理排放限值和所有运行状态下的剂量限值，并且能够满足事故工况下可接受的限值。

5.72. 安全分析必须提供关于已经在电厂设计中实施了纵深防御的保证。

5.73. 安全分析必须提供关于已经在电厂设计中充分考虑了各种不确定因素的保证，特别是提供充分的裕度，以避免陡边效应<sup>19</sup>和早期放射性释放或大规模放射性释放。

---

<sup>18</sup> 第 GSR Part 4 (Rev.1) 号[2]确定了设施和活动的安全评定要求。

<sup>19</sup> 在核电厂，“陡边效应”是这样一种情况，即由于电厂参数出现微小偏差后导致电厂从一种状况向另一种状况突变而引起电厂行为严重异常，从而造成在对输入数据中的微小变化作出响应时电厂工况突然发生大的变化。

5.74. 必须更新和核实电厂设计中所用的分析假设、方法和保守程度对当前设计或“在建”设计的适用性。

### **确定性方法**

5.75. 确定性安全分析必须主要包括：

- (a) 确定和确认所有安全重要物项的设计基准；
- (b) 表征适合于厂址和电厂设计的假想始发事件；
- (c) 分析和评价假想始发事件引起的事件序列，以确认验证要求；
- (d) 将分析结果与验收标准、设计限值、剂量限值和用于辐射防护目的的可接受限制进行比较；
- (e) 证明可以通过安全系统自动启动所需的安全动作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；
- (f) 证明可以通过安全系统的自动启动和安全特性的使用与预期的操纵员动作的结合来管理设计扩展工况。

### **概率方法**

5.76. 设计必须充分考虑电厂在所有运行模式和所有状态包括停堆状态下的概率安全分析，并特别涉及：

- (a) 确定已经实现平衡设计，使得任何特定特性或假想始发事件都不会对总体危险产生过大或明显不确定的贡献作用，而且纵深防御的各层级在实际的程度上具有独立性；

- (b) 提供关于将防止出现电厂参数微小偏差可能造成电厂工况很大变化（“陡边效应”）情况的保证；<sup>20</sup>
- (c) 将分析结果与已规定的危险接受标准相比较。

## 6. 电厂特定系统的设计

### 反应堆堆芯和相关特性

#### 要求 43：燃料元件和燃料组件的性能

核电厂燃料元件和燃料组件必须设计得能够维持其结构完整性和令人满意地承受反应堆堆芯中的预期辐射水平和其他工况连同运行状态下可能发生的所有降质过程。

6.1. 应考虑而降质过程必须包括下列因素引起的那些过程：

- 局部膨胀和变形；
- 冷却剂外部压力；
- 由燃料元件中的裂变产物和氦积聚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；
- 化学效应；
- 静载荷和动载荷，包括流致振动和机械振动；
- 可能由变形或化学效应引起的传热性能的变化。

---

<sup>20</sup> 在核电厂，“陡边效应”是这样一种情况，即由于电厂参数出现微小偏差后导致电厂从一种状况向另一种状况突变而引起电厂行为严重异常，从而造成在对输入数据中的微小变化作出响应时电厂工况突然发生大的变化。

必须给数据、计算和制造中的不确定因素留出裕量。

6.2. 燃料设计限值必须包括预计运行事件中容许燃料裂变产物泄漏量限值，从而使燃料仍适合于继续使用。

6.3. 燃料元件和燃料组件必须能够承受与燃料装卸相关的负荷和应力。

#### **要求 44：反应堆堆芯的结构能力**

核电厂燃料元件和燃料组件及其支撑结构的设计必须使得在运行状态下和除严重事故之外的事故工况下，能够维持允许充分冷却的几何形状和不妨碍控制棒的插入。

#### **要求 45：反应堆堆芯的控制**

在核电厂反应堆堆芯的任何状态下包括在停堆后和换料期间或换料后产生的状态以及预计运行事件和不涉及反应堆堆芯降质的事故工况所导致的状态下可能出现的中子通量分布，必须保持内在稳定性。必须最大程度地减少对控制系统提出的在所有运行状态下把中子通量形状、水平和稳定性保持在设计限值内的要求。

6.4. 必须提供探测反应堆堆芯内中子通量分布及其变化的充分手段，以便确保堆芯内不存在可能超出设计限值的区域。

6.5. 在设计反应性控制装置时，必须充分考虑磨损以及各种辐照效应，如燃耗、物理特性的变化和气体的产生。

6.6. 必须对运行状态下和不涉及反应堆堆芯降质的事故工况下的最大正反应性程度及正反应性引入速率增长加以限制或补偿，以防止反应堆冷却剂系统的压力边界因此而失效、保持冷却能力和防止反应堆堆芯发生任何明显损坏。



## **要求 46：反应堆停堆**

**必须提供手段，确保有能力使处于运行状态下和事故工况中的核电厂反应堆停堆，并确保即使反应堆堆芯处于最大反应性工况时也能保持停堆状态。**

6.7. 反应堆停堆手段的有效性、动作速度和停堆裕度必须做到使规定的燃料设计限值不被超过。

6.8. 在判断反应堆停堆手段的充分性时，必须考虑电厂任何部分发生的可能导致部分停堆手段失灵（例如控制棒不能插入）或可能引起共因故障的各种故障。

6.9. 反应堆停堆手段必须至少由两个不同且独立的系统组成。

6.10. 即使堆芯处于反应性最大的状态，这两个不同系统中也必须至少有一个系统有能力独自以充分的裕度和高度的可靠性使反应堆保持次临界。

6.11. 停堆手段必须足以防止在停堆期间或换料操作或停堆状态下的其他例行或非例行操作期间出现任何可预见的反应性增加而导致意外临界。

6.12. 必须提供仪器仪表，并必须规定应进行的测试，以确保停堆手段始终处于为特定电厂状态规定的状态。

## **反应堆冷却剂系统**

### **要求 47：反应堆冷却剂系统的设计**

**核电厂反应堆冷却剂系统部件的设计和制造必须做到最大程度减少因材料质量不够高、设计标准不适当、检查能力不充足或制造质量不够好而导致的故障风险。**

6.13. 与核电厂反应堆冷却剂系统压力边界相连接的管道必须配有足够的隔离装置，以限制放射性流体（一次冷却剂）的任何丧失和防止冷却剂通过接口系统丧失。

6.14. 反应堆冷却剂压力边界必须设计得极不可能产生裂纹，并且已产生的任何裂纹将以极不易导致不稳定断裂和导致裂口快速扩展的方式蔓延，从而能够及时探测裂纹。

6.15. 反应堆冷却剂系统的设计必须能够确保电厂不出现反应堆冷却剂压力边界部件发生脆化的状态。

6.16. 泵叶轮和阀门零件之类被置于反应堆冷却剂压力边界内的部件的设计必须做到最大程度减少在所有运行状态和设计基准事故工况下发生故障和随之引起一次冷却剂系统中其他安全重要部件损坏的可能性，同时为在役期间可能发生的降质留出应有的裕量。

#### **要求 48：反应堆冷却剂压力边界的过压保护**

必须采取措施确保卸压装置的运行将保护反应堆冷却剂系统的压力边界免于过压的影响，并且不会导致放射性物质从核电厂直接释放到环境中。

#### **要求 49：反应堆冷却剂的装量**

必须采取措施控制冷却剂的装量、温度和压力，以便在适当考虑到体积变化和泄漏的情况下，确保在核电厂的任何运行状态下都不超过规定的设计限值。

#### **要求 50：反应堆冷却剂的净化**

必须在核电厂提供适当的设施，用于清除反应堆冷却剂中的放射性物质，包括活化腐蚀产物和源自燃料的裂变产物以及非放射性物质。

6.17. 电厂必要系统的能力必须以规定的允许燃料泄漏量设计限值为基础，并留有一定的保守裕度，以确保能够以可实际合理的尽量低的回路活度水平运行电厂，同时确保满足使放射性释放处于可合理达到的尽量低的水平并低于管理排放限值的要求。

### **要求 51：反应堆堆芯的余热排除**

必须提供手段排除核电厂停堆状态下的反应堆堆芯中的余热，以使燃料、反应堆冷却剂压力边界和安全重要结构的设计限值不被超过。

### **要求 52：反应堆堆芯的应急冷却**

必须提供冷却手段，以便在核电厂事故工况下即便在不能维持一次冷却剂系统压力边界的完整性时，也能恢复和维持燃料的冷却。

6.18. 供用于冷却反应堆堆芯的手段必须能够确保：

- (a) 包壳或燃料完整性的限制性参数（如温度）将不被超过；
- (b) 可能的化学反应被保持在可接受的水平；
- (c) 反应堆堆芯冷却手段的有效性可补偿燃料和反应堆堆芯内部几何形状的可能变化；
- (d) 反应堆堆芯的冷却能持续足够长的时间。

6.19. 必须提供设计特性（如泄漏检测系统、适当的互连和隔离能力）及适当的冗余性和多样性，以便在每个假想始发事件中都以充分的可靠性满足第 6.18 段的要求。

### **要求 53：将热量传输到最终热阱**

必须确保在电厂所有状态下将热量传输到最终热阱的能力。

6.19A. 传输热量的系统必须在它们须满足热量传输功能的电厂所有状态下都具备充分的可靠性。这可能要求使用不同的最终热阱或不同的最终热阱通道。

6.19B. 对于其严重性超出设计所考虑的源于厂址危害评价的严重性的自然危害程度，必须满足热量传输功能。

## 安全壳结构和安全壳系统

### 要求 54：反应堆安全壳系统

必须提供安全壳系统，以确保或促进在核电厂执行以下安全功能：

(1) 在运行状态和事故工况下密封放射性物质；(2) 保护反应堆免于外部自然事件和人因事件的影响；(3) 在运行状态和事故工况下屏蔽辐射。

### 要求 55：控制放射性从安全壳释放

安全壳的设计必须能够确保从核电厂向环境中的任何放射性释放都保持在可合理达到的尽量低的水平、低于运行状态下的管理排放限值和低于事故工况下可接受的限值。

6.20. 安全壳结构及影响安全壳系统密封性的系统和部件的设计和制造方式，必须使得能够在安全壳的所有贯穿件安装完毕之后和必要时在电厂运行寿期期间进行泄漏率测试，并从而能够在安全壳的设计压力下进行泄漏率测试。

6.21. 安全壳贯穿件的数量必须保持实际的最低数目，并且所有贯穿件都必须满足与安全壳结构本身同样的设计要求。必须保护贯穿件免受由管道移动引起的反作用力的影响，或免受意外载荷如由外部或内部事件、喷射力和管道甩动所致飞射物引起的意外载荷的影响。

### 要求 56：安全壳隔离

作为反应堆冷却剂压力边界的一部分贯穿核电厂安全壳的每条管线或与安全壳内大气直接相通的每条管线，必须在发生安全壳的密封性对防止产生超过可接受限值的向环境的放射性释放至关重要的事故时，能够自动和可靠地封闭。

6.22. 作为反应堆冷却剂压力边界的一部分贯穿安全壳的管线和与安全壳内大气直接相通的管线必须至少配备两个适当的串接<sup>21</sup>安全壳隔离阀或逆止阀，并且必须配备适当的泄漏检测系统。安全壳隔离阀或逆止阀必须尽实际可能安装在离安全壳最近的位置，而且每个阀都必须能够可靠和独立地启动及定期得到测试。

6.23. 对于仪器仪表管线等特定管线类别，或者在应用第 6.22 段中所述安全壳隔离方法将会减少包含安全壳贯穿件的安全系统可靠性的情况下，必须允许第 6.22 段中所述的安全壳隔离要求存在例外情况。

6.24. 贯穿安全壳而且既不是反应堆冷却剂压力边界的一部分也不与安全壳内大气直接相通的每条管线，必须至少配备一个适当的安全壳隔离阀。安全壳隔离阀必须安装在安全壳外部，并尽实际可能地靠近安全壳。

#### **要求 57：进入安全壳**

运行人员进入核电厂安全壳时，必须穿过装有若干道闸门的空气闸门。这些闸门是联锁的，以确保在反应堆功率运行期间和发生事故工况时，至少有一道闸门是关闭的。

6.25. 在为监视目的对运行人员进入安全壳制订有规定的情况下，必须在设计中规定确保运行人员防护和安全的措施。在规定有设备空气闸门的情况下，必须在设计中规定确保运行人员防护和安全的措施。

6.26. 用于穿越安全壳进行设备或材料移动的安全壳开口必须设计得在需要对安全壳进行隔离时能够对其实施快速和可靠的关闭。

#### **要求 58：安全壳工况控制**

必须采取措施控制核电厂安全壳内的压力和温度，并控制裂变产物或可能在安全壳内释放和可能影响安全重要系统运行的其他气态、液态或固态物质的任何积聚。

---

<sup>21</sup> 多数情况下，一个安全壳隔离阀或逆止阀安装在安全壳外部，另一个安装在安全壳内部。但其他安排或许也可接受，这要视设计情况而定。

6.27. 设计必须为安全壳内各独立隔间之间提供足够的气流通道。隔间之间各种开口的截面尺寸必须能够确保在事故工况下的压力平衡期间发生的压力差不会对承压结构或对于减轻事故工况效应来说非常重要的系统造成不可接受的损坏。

6.28. 必须确保从安全壳中排热的能力，以便在发生高能流体的任何意外释放后，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。执行从安全壳中排热功能的系统必须具有充分的可靠性和冗余性，以确保这一功能得到实现。

6.28A. 必须为防止在电厂所有状态下安全壳结构完整性的丧失作出设计准备。这种准备的利用不得导致早期放射性释放或大规模放射性释放。

6.28B. 设计还必须包括能够安全使用非永久性设备<sup>22</sup>恢复从安全壳排热之能力的特性。

6.29. 必须提供控制可能释放到安全壳中的裂变产物、氢气、氧气和其他物质所需的设计特性，以便：

- (a) 减少事故工况下可能释放到环境中的裂变产物数量；
- (b) 在事故工况下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载荷。

6.30. 必须仔细选择安全壳系统内的部件和结构的覆盖层、热绝缘体和涂层，而且必须明确规定其使用方法，以确保这些部件和结构的安全功能得到实现，并在万一覆盖层、热绝缘体和涂层失效时最大程度减小对其他安全功能的干扰。

---

<sup>22</sup> 非永久性设备不必贮存在现场。

## 仪器仪表和控制系统

### 要求 59：提供仪器仪表

必须提供用于以下目的的仪器仪表：确定可能影响核电厂裂变过程、反应堆堆芯完整性、反应堆冷却剂系统完整性和安全壳完整性的一切主要变量；获得安全和可靠运行电厂所需的电厂重要信息；以及为事故管理的目的作出决定。

6.31. 必须提供仪器仪表和记录设备，以确保获得必不可少的信息，供用于监测基本设备的状况和事故过程、预测可能从设计中预定的部位释放的放射性物质的释放位置和数量以及进行事故后分析。

### 要求 60：控制系统

必须在核电厂提供适当而可靠的控制系统，以便将相关过程变量维持和限制在规定的运行范围之内。

### 要求 61：保护系统

必须在核电厂提供能够探测电厂不安全工况和自动触发安全动作的保护系统，以启动实现和维持电厂安全工况所需的安全系统。

6.32. 保护系统的设计必须：

- (a) 能够推翻控制系统的不安全动作；
- (b) 具备故障安全特性，能够在保护系统一旦发生故障时使电厂实现安全工况。

6.33. 设计：

- (a) 必须防止操纵员在运行状态和事故工况中采取可能损害保护系统有效性的动作，但不得阻碍操纵员在事故工况中采取正确行动；
- (b) 必须使用于启动安全系统的各种安全动作自动化，以便在预计运行事件或事故工况开始后的合理时间范围内无需操纵员采取行动；

(c) 必须向操纵员提供相关信息，供用于监测自动动作的效果。

#### **要求 62：仪器仪表和控制系统的可靠性和可测试性**

**核电厂安全重要物项的仪器仪表和控制系统必须设计得具有与拟执行的安全功能相称的高度功能可靠性和可定期测试性。**

6.34. 必须尽可能实际地使用必要时包括自检能力在内的可测试性、故障安全特性、功能多样性以及部件设计和运行概念方面的多样性等设计技术，以防止某个安全功能的丧失。

6.35. 安全系统的设计必须使得能够在电厂运行时定期测试安全系统的功能，包括有可能单独测试各个通道以探测故障和冗余性的丧失。设计必须允许对传感器、输入信号、最终启动器和显示器进行所有方面的功能测试。

6.36. 在必须使安全系统或安全系统的一部分停止运行以便进行测试时，必须对在整个测试或维护活动期间所需的任何保护系统旁通作出适当的规定并予以明示。

#### **要求 63：基于计算机的设备在安全重要系统中的使用**

**如果核电厂的安全重要系统依赖于基于计算机的设备，则必须制订开发和测试计算机硬件和软件的适当标准和实践并在该系统的整个使用期内特别是软件的整个开发周期执行这些标准和实践。必须将整个开发工作纳入质量管理体系的管理。**

6.37. 对于安全系统中或安全相关系统中基于计算机的设备：

- (a) 必须根据系统的安全重要性采用高质量的硬件和软件并利用最佳实践。
- (b) 必须系统地对包括设计变更的控制、测试和调试在内的整个开发过程形成文件，并且这些过程必须是可审查的。
- (c) 必须由独立于设计团队和供应商团队的专家对设备进行评定，以提供关于设备高度可靠性的保证。



- (d) 在安全功能对实现和保持安全工况至关重要而且不能以很高的置信度证明设备具有必要的高度可靠性的情况下，必须提供可确保执行安全功能的各种手段。
- (e) 必须考虑到源自软件的共因故障。
- (f) 必须提供保护，防止系统运行意外中断或受到蓄意干扰。

#### **要求 64：保护系统和控制系统相分离**

**必须以通过分隔、避免互连或实施适当的功能独立性来防止核电厂保护系统和控制系统之间的相互干扰。**

6.38. 如果信号由保护系统和控制系统共用，则必须确保其分隔（如通过适当的去耦合），并须将信号系统作为保护系统的一部分进行分类。

#### **要求 65：主控室**

**必须在核电厂设立一个主控室，以便能够在所有运行状态下从主控室以自动或手动方式安全运行电厂，以及能够从主控室采取措施使电厂保持安全状态或在发生预计运行事件和事故工况后使之返回到安全状态。**

6.39. 必须采取适当的措施，包括在核电厂主控室和外部环境之间建立屏障，并且必须提供足够的信息，以保护主控室内的人员在较长时间内免于事故工况所致高辐射水平、放射性物质释放、火灾、爆炸性气体或有毒气体等危害。

6.40. 必须特别注意查明主控室内部和外部可能危及主控室持续运行的事件，设计必须提供合理可行的措施，以便将这类事件的后果降至最低。

6.40A. 主控室的设计必须提供充分的裕度，以防范其严重性超出设计所考虑的源于厂址危害评价的严重性的自然危害程度。

## 要求 66：辅控室

必须配有仪器仪表和控制设备供随时使用，最好是在一个在实体、电气和功能上与核电厂主控室相分离的单独场所（辅控室）。辅控室的设备配备必须能够在主控室丧失执行这些关键安全功能的能力时将反应堆置于或维持在停堆状态，能够排出余热，并能够监测关键的电厂变量。

6.41. 第 6.39 段关于采取适当措施和提供足够信息以保护人员免于各种危害的要求也适用于核电厂辅控室。

## 要求 67：现场应急响应设施

核电厂必须包括必要的现场应急响应设施。核电厂的设计必须做到使工作人员能够执行预期任务，以管理事故和危害所致工况下的紧急情况。

6.42. 必须向相关应急响应设施<sup>23</sup>提供有关核电厂及其周边环境的重要电厂参数和放射状况的资料。各设施必须酌情具备与电厂主控室、辅控室和其他重要场所以及与厂内和厂外的应急响应组织进行通讯的手段。

## 应急电源

### 要求 68：能够经受住丧失厂外电源的设计

核电厂的设计必须包括能够在发生预计运行事件和设计基准事故时一旦丧失厂外电源的情况下提供必要电力的应急电源。设计必须包括在设计扩展工况下提供必要电力的备用电源。

6.43. 应急电源和备用电源的设计技术要求必须包括对所需供电能力、电源可用性和供电持续时间以及电源容量和电源持续性的要求。

---

<sup>23</sup> 国际原子能机构《安全标准丛书》第 GSR Part 7 号《核或辐射应急的准备与响应》[11]论述了应急响应设施。就核电厂而言，应急响应设施（与主控室和辅控室相分离）包括技术支持中心、运行支持中心和应急中心。

6.44. 用于提供应急电力的综合手段（如水轮机、汽轮机或燃气轮机、柴油机或蓄电池）必须具备与需要供电的安全系统所有要求相一致的可靠性和类型，而且它们的功能能力必须具有可测试性。

6.44A. 备用电源必须能够提供必要的电力，以便在丧失厂外电源和应急供电失败并发情况下保持反应堆冷却剂系统的完整性和防止堆芯与乏燃料遭受严重损坏。

6.44B. 减轻堆芯熔化后果所需的设备必须能够由任何可用电源供电。

6.44C. 备用电源必须独立于应急电源并在实体上与应急电源相分离。备用电源的连接时间必须与电池的耗尽时间相一致。

6.44D. 在发生丧失交流电电源情况下，必须维持供电的持续性，以监测电厂关键参数和完成保持安全所需的短期行动。

6.45. 为安全重要物项提供应急电源的任何柴油机或其他原动机<sup>24</sup>的设计基准必须包括：

- (a) 相关的燃料油贮存和供应系统在规定时间内满足需求的能力；
- (b) 原动机在所有规定工况下和在所要求的时间成功启动和运行的能力；
- (c) 原动机的辅助系统，如冷却剂系统。

6.45A. 设计还必须包括能够安全使用非永久性设备恢复必要电力供应的特性。<sup>25</sup>

---

<sup>24</sup> 原动机是在接到驱动装置的命令后将能量转化为动作的部件（如发动机、螺线管操作器或气动操作器）。

<sup>25</sup> 非永久性设备不必贮存在现场。

## 支持系统和辅助系统

### 要求 69：支持系统和辅助系统的性能

支持系统和辅助系统的设计必须能够确保这些系统的性能与它们在核电厂所伺服的系统或部件的安全重要性相一致。

### 要求 70：热传输系统

必须酌情提供用于排出需在运行状态和事故工况中发挥作用的核电厂系统和部件中热量的辅助系统。

6.46. 热传输系统的设计必须确保能够将热传输系统的非关键部件加以隔离。

### 要求 71：工艺取样系统和事故后取样系统

必须提供工艺取样系统和事故后取样系统，以便在核电厂所有运行状态和事故工况下及时测定流体工艺系统中的规定放射性核素的浓度以及从系统或环境中采集的气体和液体样品中的规定放射性核素的浓度。

6.47. 必须在核电厂提供适当的手段，以便监测可能造成显著污染的流体系统的活度和采集工艺样品。

### 要求 72：压缩空气系统

服务于核电厂安全重要物项的任何压缩空气系统的设计基准均须规定所供空气的质量、流速和清洁度。

### 要求 73：空调系统和通风系统

必须在核电厂辅助室或其他区域酌情提供空调系统、空气加热系统、空气冷却系统和通风系统，以便在所有电厂状态下保持安全重要系统和部件所需的环境条件。

6.48. 必须为核电厂内的建筑物提供具备适当空气清洁能力的通风系统，以便：

- (a) 防止气载放射性物质在核电厂内的弥散达到不可接受程度；
- (b) 将气载放射性物质的浓度降低到与工作人员需要进入该区域相符合的水平；
- (c) 使电厂内气载放射性物质的水平保持在低于管理限值和可合理实现的尽量低的水平；
- (d) 在不影响控制放射性排出流能力的情况下，对含有惰性气体或有害气体的房间进行通风；
- (e) 将向环境中的气态放射性释放控制在管理排放限值以下并使其保持在可合理实现的尽量低的水平。

6.49. 相对于电厂内污染较低的区域和其他可进入的区域，必须使污染较高的区域处于污染负压差状态（局部真空）。

#### **要求 74：消防系统**

**必须在充分考虑火灾危害分析结果的情况下在整个核电厂范围内提供消防系统，包括火灾探测系统和灭火系统、火灾封隔屏障及烟控系统。**

6.50. 在核电厂安装的消防系统必须能够可靠地应对所假想的各种类型的火灾事件。

6.51. 灭火系统必须能够在适当情况下自动启动。灭火系统的设计和布置必须能够确保其破损或误动作或意外运行不会对安全重要物项的能力造成重要损害。

6.52. 火灾探测系统必须设计得能够立即为运行人员提供有关所发生的任何火灾的位置和蔓延情况的信息。

6.53. 防范发生假想始发事件后可能出现的火灾所需的探测系统和灭火系统必须具备抵御假想始发事件影响的适当能力。

6.54. 在整个电厂内，特别是在安全壳和主控室等场所，只要实际可行，就必须使用非燃或阻燃材料和耐热材料。

#### **要求 75：照明系统**

在所有运行状态和事故工况下，都必须在核电厂的所有作业区域提供充足的照明。

#### **要求 76：桥式起重设备**

必须提供桥式起重设备，用于在核电厂升降安全重要物项和在安全重要物项附近升降其他物项。

6.55. 桥式起重设备的设计必须做到：

- (a) 能够采取措施，以防止过载；
- (b) 能够实施保守设计措施，以防止装载物发生可能影响安全重要物项的意外坠落；
- (c) 电厂布局允许安全移动桥式起重设备和所运输的物项；
- (d) 这种设备只能在规定电厂状态下使用（通过起重机安全联锁装置）；
- (e) 供安全重要物项所在区域使用的这种设备具有合格的抗震能力。

#### **其他功率转换系统**

##### **要求 77：蒸汽供应系统、给水系统和汽轮发电机**

核电厂蒸汽供应系统、给水系统和汽轮发电机的设计必须能够确保反应堆冷却剂压力边界的适当设计限值在运行状态或事故工况中不被超过。

6.56. 蒸汽供应系统的设计必须提供适当等级的、能够在运行状态和事故工况中的规定条件下关闭的合格蒸汽隔离阀。

6.57. 蒸汽供应系统和给水系统必须具备充足的容量，并且必须设计得能够防止预计运行事件升级为事故工况。

6.58. 必须为汽轮发电机提供适当的保护，如超速保护和振动保护，并且必须采取措施将汽轮产生的飞射物对安全重要物项的可能影响降至最小。

## 放射性流出物和放射性废物的处理

### 要求 78：废物处理和控制系统

必须在核电厂提供用于处理固态放射性废物和液态放射性废物的系统，以使放射性释放的数量和浓度低于管理排放限值并保持在可合理达到的尽量低的水平。

6.59. 必须在核电厂厂址上提供用于在一定时间内管理和贮存放射性废物的系统和设施，这种时间的长短必须与相关处置方案的可用性相一致。

6.60. 电厂的设计必须纳入适当的特性，以便于放射性废物的移动、运输和装卸。必须考虑提供通往设施的通道及提供起吊和包装能力。

### 要求 79：流出物的处理和控制系统

必须在核电厂提供用于处理液态和气态放射性流出物的系统，以使这些流出物的数量处于管理排放限值以下并保持在可合理实现的尽量低的水平。

6.61. 必须在电厂对液态和气态放射性流出物进行处理，以使环境排放对公众造成的照射量保持在可合理实现的尽量低的水平。

6.62. 必须在电厂设计中纳入适宜的手段，以使将向环境中的液态放射性释放保持在可合理实现的尽量低的水平，并确保放射性释放始终低于管理排放限值。

6.63. 气态放射性物质的清洁设备必须提供必要的滞留因子，以便将放射性释放保持在低于管理排放限值的水平。过滤器系统的设计必须使得能够

对其效率进行测试，能够在其寿期内对其性能和功能定期进行监测，并能够更换滤芯且保持空气通过量。

## 燃料装卸和贮存系统

### 要求 80：燃料装卸和贮存系统

必须在核电厂建立燃料装卸和贮存系统，以确保在燃料装卸和贮存期间始终保持燃料的完整性和特性。

6.64. 电厂的设计必须纳入适当的特性，以便于新鲜燃料和乏燃料的起吊、移动和装卸。

6.65. 电厂的设计必须能够防止在燃料或屏蔽容器移动过程中或发生燃料或屏蔽容器坠落时对安全重要物项造成任何显著损坏。

6.66. 辐照燃料和未辐照燃料的装卸和贮存系统的设计必须能够：

- (a) 通过物理手段或物理过程，最好通过使用几何安全构形，确保即使在最佳慢化条件下也不会达到临界，并有规定的裕度；
- (b) 允许对燃料进行检查；
- (c) 允许对安全重要部件进行维护、定期检查和测试；
- (d) 防止对燃料造成损坏；
- (e) 防止燃料在转移时坠落；
- (f) 能够识别每个燃料组件；
- (g) 提供满足相关辐射防护要求的适当手段；
- (h) 确保能够实施适当的运行程序及核材料衡算和控制系统，以防止核燃料丢失或丧失对核燃料的控制。



6.67. 此外，辐照燃料的燃料装卸和贮存系统的设计必须：

- (a) 允许在运行状态和事故工况下充分地排出燃料中的热量；
- (b) 防止乏燃料在转移时坠落；
- (c) 避免给燃料元件或燃料组件造成不可接受的操作应力；
- (d) 防止乏燃料屏蔽容器、起重机或其他物体之类的重物坠落在燃料上并对燃料造成可能的损坏；
- (e) 允许安全地保存可疑或受损燃料元件或燃料组件；
- (f) 在可溶吸收剂被用于临界安全的情况下控制可溶吸收剂的水平；
- (g) 便于燃料装卸和贮存设施的维护和未来退役；
- (h) 便于燃料装卸和贮存区域和设备在必要时进行去污；
- (i) 根据所预见的堆芯管理战略和整个堆芯中的燃料数量，以适当的裕度容纳从反应堆中移出的全部燃料；
- (j) 便于从贮存设施中移出燃料和对其进行厂外运输的准备。

6.68. 对于利用水池系统贮存燃料的反应堆而言，设计必须做到防止在与乏燃料水池具有相关性的电厂所有状态下发生燃料组件暴露，以便“实际上消除”<sup>26</sup> 出现可导致早期放射性释放或大规模放射性释放的工况的可能性以及避免现场出现高辐射区。电厂的设计：

- (a) 必须提供必要的燃料冷却能力；
- (b) 必须提供防止在发生泄漏或管道破裂时发生燃料组件暴露的特性；
- (c) 必须提供恢复水存量的能力。

---

<sup>26</sup> 如果某些工况的出现完全不可能，或者如果有很大的把握认为这些工况极不可能出现，则出现这些工况的可能性可以被视为已“实际上消除”。

设计还必须包括能够安全使用非永久性设备确保乏燃料长期冷却和提供辐射屏蔽所需充足水存量的特性。<sup>27</sup>

6.68A. 必须在设计中纳入以下手段：

- (a) 用于监测和控制水温以便监测和控制运行状态和与乏燃料水池具有相关性的事故工况的手段；
- (b) 用于监测和控制水位以便监测和控制运行状态和与乏燃料水池具有相关性的事故工况的手段；
- (c) 用于监测和控制水和空气中的活度以便监测和控制运行状态的手段，以及用于监测水和空气中的活度以便监测与乏燃料水池具有相关性的事故工况的手段；
- (d) 监测和控制运行状态下的水化学的手段。

## 辐射防护

### 要求 81：辐射防护设计

必须采取措施确保核电厂运行人员接受的剂量处于剂量限值以下和保持在可合理达到的尽量低的水平，并考虑到相关的剂量约束。

6.69. 必须全面查明电厂范围内的辐射源，并且必须使与之相关的照射和辐射危险保持在可合理实现的尽量低的水平<sup>28</sup>；必须保持燃料包壳的完整性；还必须控制腐蚀产物和活化产物的产生和输运。

6.70. 必须对用于制造结构、系统和部件的材料进行选择，以便尽量在实际合理的情况下将材料活化降至最低。

6.71. 为了辐射防护的目的，必须采取措施防止放射性物质、放射性废物和放射性污染在电厂的释放或弥散。

---

<sup>27</sup> 非永久性设备不必贮存在现场。

<sup>28</sup> 第 GSR Part 3 号[9]确定了关于设施和活动的辐射防护和辐射源安全的要求。

6.72. 电厂的布置必须能够确保充分控制运行人员对辐射危险区域和可能的污染区域的进入，并通过此种手段及通过通风系统防止或减少照射和污染。

6.73. 必须将电厂划分为与其预期场地占用有关的区域、与运行状态（包括换料、维护和检查）下的辐射水平和污染水平有关的区域以及与事故工况下可能的辐射水平和污染水平有关的区域。必须提供屏蔽，以防止或减少辐射照射。

6.74. 电厂的布置必须使得能够将运行人员在正常运行、换料、维护和检查期间接受的剂量保持在可合理达到的尽量低的水平，并且必须充分考虑为满足这些要求而提供任何特殊设备的必要性。

6.75. 必须将须经常进行维护或手动操作的电厂设备放置在剂量率较低的区域，以减少对工作人员的照射。

6.76. 必须提供用于运行人员和电厂设备去污的设施。

## **要求 82：辐射监测手段**

**必须在核电厂提供设备，以确保在运行状态下和设计基准事故工况下以及在尽可能实际的设计扩展工况下能够进行充分的辐射监测。**

6.77. 必须提供固定式剂量率计，用于监测运行人员通常入出的场所和在运行状态下辐射水平的变化使得仅能允许在某些规定时段内入出的场所的局部辐射剂量率。

6.78. 必须安装固定式剂量率计，以显示事故工况下电厂适当地点的总体辐射水平。固定式剂量率计必须在主控室或运行人员能够在必要时采取纠正行动的适当控制部位给出充分的信息。

6.79. 必须提供固定式监测器，用于在运行人员通常占用的区域和气载放射性物质的活度水平可能达到须采取保护措施程度的区域测量大气中放射性物质的活度。当探测到高浓度放射性核素时，这些系统必须在主控室或

其他适当地点给出指示。还必须在因设备故障或其他异常情况可能会造成污染的区域提供监测器。

6.80. 必须提供固定式设备和实验室设施，用于及时测定运行状态下和事故工况下流体工艺系统中的选定放射性核素的浓度以及从电厂系统或环境中采集的气体和液体样品中的选定放射性核素的浓度。

6.81. 必须提供用于在电厂向环境中排放之前或在这种排放期间监测放射性流出物和可能被污染的流出物的固定式设备。

6.82. 必须提供用于测量表面污染的仪器仪表。必须在控制区和监视区的主要出口提供固定式监测器（如门式辐射监测器和手足监测器），以便于监测运行人员和设备。

6.83. 必须提供用于测量运行人员所受照射和污染的设施。必须制订评定和记录工作人员随着时间所受累积剂量的程序。

6.84. 必须作出安排，通过对剂量率或放射性浓度进行环境监测来评定在电厂周围地区的照射和其他放射影响（如有），并特别涉及：

- (a) 对人的照射途径，包括食物链；
- (b) 对当地环境的放射影响（如有）；
- (c) 放射性物质在环境中的可能积聚和积累；
- (d) 是否存在未经批准的任何放射性释放路径的可能性。

## 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、经合组织核能机构、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《设施和安全活动的安全评定》，国际原子能机构《安全标准丛书》第 GSR Part 4 (Rev.1) 号，国际原子能机构，维也纳（2016 年）。
- [3] 国际原子能机构《国际原子能机构安全术语》（核安全和辐射防护系列）（2007 年版），国际原子能机构，维也纳（2007 年）。
- [4] 国际原子能机构《核电厂安全：调试和运行》，国际原子能机构《安全标准丛书》第 SSR-2/2 (Rev.1) 号，国际原子能机构，维也纳（2016 年）。
- [5] 国际核安全咨询组《核安全纵深防御》，（第 INSAG-10 号），国际原子能机构，维也纳（1996 年）。
- [6] 国际核安全咨询组《核电厂基本安全原则》（第 75-INSAG-3 Rev.1 号、第 INSAG-12 号），国际原子能机构，维也纳（1999 年）。
- [7] 国际核安全咨询组《维持核装置在整个运行寿期内的设计完整性》，（第 INSAG-19 号），国际原子能机构，维也纳（2003 年）。
- [8] 国际原子能机构《设施和管理活动的管理系统》，国际原子能机构《安全标准丛书》第 GS-R-3 号，国际原子能机构，维也纳（2006 年）。（此出版物的修订版正在编制中，将作为第 GSR Part 2 号印发。）
- [9] 欧洲委员会、联合国粮食及农业组织、国际原子能机构、国际劳工组织、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《国际辐射防护和辐射源安全的基本安全标准》，

国际原子能机构《安全标准丛书》第 GSR Part 3 号，国际原子能机构，维也纳（2014 年）。

- [10] 国际原子能机构《核装置的厂址评价》，国际原子能机构《安全标准丛书》第 NS-R-3（Rev.1）号，国际原子能机构，维也纳（2016 年）。
- [11] 联合国粮食及农业组织、国际原子能机构、国际民用航空组织、国际劳工组织、国际海事组织、国际刑事警察组织、经济合作与发展组织核能机构、泛美卫生组织、全面禁止核试验条约组织筹备委员会、联合国环境规划署、联合国人道主义事务协调厅、世界卫生组织、世界气象组织《核或辐射应急的准备与响应》，国际原子能机构《安全标准丛书》第 GSR Part 7 号，国际原子能机构，维也纳（2015 年）。

# 定 义

以下新的和经修订的定义不同于《国际原子能机构安全术语：  
核安全和辐射防护系列》（2007年版）

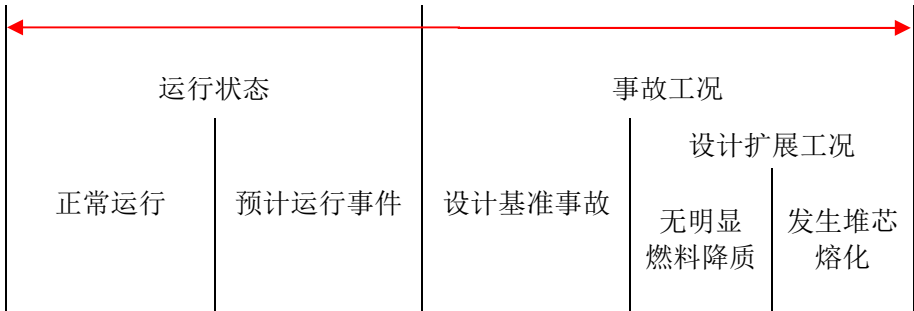
（国际原子能机构，维也纳（2007年））中的定义：

<http://www-pub.iaea.org/books/IAEABooks/7648/IAEA-Safety-Glossary>

符号“①”表示信息附注。

**受控状态。**电厂在发生预计运行事件或事故工况后的状态。在这种状态中，能够确保基本安全功能，并能够使基本安全功能维持足够长的时间，以供实施旨在实现安全状态的措施。

（在设计中考虑的）**电厂状态**



**事故工况。**比预计运行事件频率低但更严重的偏离正常运行的工况。

① 事故工况包括设计基准事故和设计扩展工况。

**设计基准事故。**根据确定的设计准则和保守方法学设计设施时必须加以防范的导致事故工况的假想事故。出现这种工况时，放射性物质的释放被保持在可接受限值以内。

**设计扩展工况。**不在设计基准事故考虑范围但在设施设计过程中根据最佳估计方法学加以考虑的假想事故工况。出现这种工况时，放射性物质的释放被保持在可接受限值以内。

- ① 设计扩展工况包括无明显燃料降质事件中的工况和堆芯熔化事件中的工况。

**安全状态。**电厂在发生预计运行事件或事故工况后的状态。在这种状态中，反应堆处于次临界，并能够长时间确保基本安全功能和使这些功能保持稳定。

**设计扩展工况安全特性。**在设计扩展工况中执行某种安全功能或具有某种安全功能的物项。

**安全系统设定值。**为防止超过安全限值，在发生预计运行事件或设计基准事故时自动启动安全系统的水平设定值。



## 参与起草和审查的人员

R. Antalík	斯洛伐克共和国核监管局（斯洛伐克）
Z.M. Aza	伊朗原子能组织（伊朗伊斯兰共和国）
I. Borysova	世界核协会
N. Buttery	英国能源生产公司（英国）
B. Carlucci	阿海珐集团（法国）
J.S. Cowley	顾问
D.J. Downing	球床模块式反应堆（南非）
M. El-Shanawany	国际原子能机构
B. Englebert	Suez-Tractebel 能源公司（比利时）
J.M. Evrad	辐射防护和核安全研究所（法国）
G.L. Fiorini	法国替代能源和原子能委员会（法国）
T. Froehmel	世界核协会
M. Gasparini	国际原子能机构
S.G. Ghadge	印度核电公司（印度）
C. Harwood	加拿大核安全委员会（加拿大）
M.L. Järvinen	辐射和核安全管理局（芬兰）
M. Kajimoto	日本原子能安全组织（日本）
L. Kurkowski	法国电力公司-热能和核能项目与研究服务公司（法国）
G. Le Cann	联邦核监管局（阿拉伯联合酋长国）
T. Matsumoto	日本原子能安全组织（日本）
M. Mertins	装置和反应堆安全公司（德国）

T. Ohshima	原子力安全和保安院（日本）
R. Pabarcius	立陶宛能源研究所（立陶宛）
J.R. Perez	法国核安全管理局（法国）
R. Semenas	国家核电安全检查局（立陶宛）
A. Thadani	核管理委员会（美利坚合众国）
C. Toth	国际原子能机构
M. Tronea	国家核活动管制委员会（罗马尼亚）
P. Uhrík	斯洛伐克共和国核监管局（斯洛伐克）
K. Valtonen	辐射和核安全管理局（芬兰）
G.J. Vaughan	核装置检查局（英国）
C. Wassilew	联邦环境、自然保护和核安全部（德国）
K. Yashimura	原子力安全委员会（日本）
W. Zaiss	欧洲原子公会
R. Zemdegs	加拿大原子能有限公司（加拿大）
M. Ziakova	斯洛伐克共和国核监管局（斯洛伐克）

### 参与修订本 1 起草和审查的人员

F. Adorjan	匈牙利原子能管理局（匈牙利）
H.A. Alkhafili	联邦核监管局（阿拉伯联合酋长国）
J.-Y. Barbaud	法国电力公司-热能及核能研究设计局，欧洲 核装置安全标准/欧洲原子工业公会
T. Boyce	核管理委员会（美利坚合众国）
O. Coman	国际原子能机构
D. Delattre	国际原子能机构

D. Delves	国际原子能机构
F. Feron	法国核安全管理局核电厂处（法国）
J. Francis	健康和局核监管办公室（英国）
M. Gasparini	国际原子能机构
S. Geupel	设施和反应堆安全公司（德国）
J. Haddad	国际原子能机构
S. Harikumar	原子能管理局（印度）
C. Harwood	加拿大核安全委员会（加拿大）
P. Hughes	国际原子能机构
M.-L. Jarvinen	辐射和核安全管理局（芬兰）
M. Kearney	国际原子能机构
Li Bin	环境保护部国家核安全局（中国）
Li Jingxi	环境保护部国家核安全局（中国）
F.M. Lignini	阿雷瓦核电公司，世界核协会/反应堆设计评价 和许可证审批合作
M. Lipar	国际原子能机构
S. Lungu	国际原子能机构
J. Lyons	国际原子能机构
F. Mansoor	巴基斯坦核管理局（巴基斯坦）
H. Mansoux	国际原子能机构
M.H. Marechal	国家核能委员会（巴西）
N. Mataji Kojouri	伊朗原子能组织、伊朗核管理局（伊朗伊斯兰 共和国）
D. Merrouche	核研究中心（阿尔及利亚）
R. Moscrop	健康和局核监管办公室（英国）

T. Nakajima	日本原子力安全组织（日本）
A. Nicic	国际原子能机构
T. Noda	原子力规制委员会（日本）
W. Orders	核管理委员会（美利坚合众国）
J. Parlange	国际原子能机构
J. Pauly	E.ON 核能公司（德国）
G. Petofi	匈牙利原子能管理局（匈牙利）
B. Poulat	国际原子能机构
N.K. Prinja	阿美科工程咨询有限公司欧洲电力和工艺公司，世界核协会/反应堆设计评价和许可证审批合作
M.M. Ramos	欧洲委员会
V. Ranguelova	国际原子能机构
M. Rueffer	联邦辐射防护办公室（德国）
R. Sairanen	辐射和核安全管理局（芬兰）
S. Samaddar	国际原子能机构
F. Scarcelli	国际原子能机构
G. Stoppa	联邦环境、自然保护、建设和核安全部（德国）
M. Svab	国际原子能机构
N. Tricot	联邦核监管局（阿拉伯联合酋长国）
A. Ugayama	国际原子能机构
P. Uhrík	斯洛伐克共和国核管理局（斯洛伐克）
P. Webster	常驻代表团（加拿大）
J. Yllera	国际原子能机构







## 通过国际标准促进安全

“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。国际原子能机构的安全标准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。”

总干事  
天野之弥

国际原子能机构  
维也纳  
ISBN 978-92-0-509316-1  
ISSN 1020-5853