

国际原子能机构安全标准

保护人类与环境

核电厂设计中的设计 扩展工况和实际 消除的概念

特定安全导则

第 SSG-88 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。

核电厂设计中的设计扩展工况和 实际消除的概念

国际原子能机构成员国

阿富汗	冈比亚	北马其顿
阿尔巴尼亚	格鲁吉亚	挪威
阿尔及利亚	德国	阿曼
安哥拉	加纳	巴基斯坦
安提瓜和巴布达	希腊	帕劳
阿根廷	格林纳达	巴拿马
亚美尼亚	危地马拉	巴布亚新几内亚
澳大利亚	几内亚	巴拉圭
奥地利	圭亚那	秘鲁
阿塞拜疆	海地	菲律宾
巴哈马	教廷	波兰
巴林	洪都拉斯	葡萄牙
孟加拉国	匈牙利	卡塔尔
巴巴多斯	冰岛	摩尔多瓦共和国
白罗斯	印度	罗马尼亚
比利时	印度尼西亚	俄罗斯联邦
伯利兹	伊朗伊斯兰共和国	卢旺达
贝宁	伊拉克	圣基茨和尼维斯
多民族玻利维亚国	爱尔兰	圣卢西亚
波斯尼亚和黑塞哥维那	以色列	圣文森特和格林纳丁斯
博茨瓦纳	意大利	萨摩亚
巴西	牙买加	圣马力诺
文莱达鲁萨兰国	日本	沙特阿拉伯
保加利亚	约旦	塞内加尔
布基纳法索	哈萨克斯坦	塞尔维亚
布隆迪	肯尼亚	塞舌尔
佛得角	大韩民国	塞拉利昂
柬埔寨	科威特	新加坡
喀麦隆	吉尔吉斯斯坦	斯洛伐克
加拿大	老挝人民民主共和国	斯洛文尼亚
中非共和国	拉脱维亚	南非
乍得	黎巴嫩	西班牙
智利	莱索托	斯里兰卡
中国	利比里亚	苏丹
哥伦比亚	利比亚	瑞典
科摩罗	列支敦士登	瑞士
刚果	立陶宛	阿拉伯叙利亚共和国
库克群岛	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	多哥
克罗地亚	马来西亚	汤加
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
斯威士兰	尼泊尔	委内瑞拉玻利瓦尔共和国
埃塞俄比亚	荷兰王国	越南
斐济	新西兰	也门
芬兰	尼加拉瓜	赞比亚
法国	尼日尔	津巴布韦
加蓬	尼日利亚	

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-88 号

核电厂设计中的设计扩展工况和 实际消除的概念

特定安全导则

国际原子能机构
2024 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（日内瓦）通过并于 1971 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。可以获得许可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。请见 www.iaea.org/publications/rights-and-permissions 了解详情。垂询可致函：

Publishing Section

International Atomic Energy Agency

Vienna International Centre

PO Box 100

1400 Vienna, Austria

电话：+43 1 2600 22529 或 22530

电子信箱： sales.publications@iaea.org

网址： <https://www.iaea.org/zh/chu-ban-wu>

© 国际原子能机构，2024 年
国际原子能机构印刷
2024 年 11 月 • 奥地利

核电厂设计中的设计扩展工况和实际消除的概念

国际原子能机构，奥地利，2024 年 11 月

STI/PUB/2055

ISBN 978-92-0-514224-1（简装书：碱性纸）

978-92-0-514324-8（pdf 格式）

ISSN 1020-5853

前 言

拉斐尔·马里亚诺·格罗西总干事

国际原子能机构（原子能机构）《规约》授权原子能机构“制定……旨在保护健康及尽量减少对生命与财产的危險的安全标准”。这些是原子能机构必须适用于其自身业务而且各国可以通过其国家法规来适用的标准。

原子能机构于 1958 年开始实施其安全标准计划，此后有了许多发展。作为总干事，我致力于确保原子能机构维护和改进这套具有综合性、全面性和一致性的、与时俱进的、用户友好的和适合目的的高质量安全标准。在利用核科学和技术的过程中正确地适用这些标准将为全世界的人和环境提供高水平的保护，并为持续利用核技术造福于所有人提供必要的信心。

安全是得到许多国际公约支持的一项国家责任。原子能机构的安全标准奠定了这些法律文书的基础，而且是有助于各方履行各自义务的全球基准。虽然安全标准对成员国没有法律约束力，但它们被广泛适用。对已在国家法规中采用这些标准以加强核能发电、研究堆和燃料循环设施中以及医学、工业、农业和研究领域核应用中的安全的绝大多数成员国而言，它们已成为不可或缺的基准点和共同标准。

原子能机构的安全标准以原子能机构成员国的实际经验为基础，并通过国际协商一致产生。各安全标准分委员会、核安保导则委员会和安全标准委员会成员的参与尤其重要，我向所有为这项工作贡献自己的知识和专长的人表示感谢。

原子能机构在通过评审工作组访问和咨询服务向成员国提供援助时，也使用这些安全标准。这有助于成员国适用这些标准，并使得能够共享宝贵经验和真知灼见。在安全标准的定期修订过程中，会考虑到这些工作组访问和服务的反馈，以及从使用和适用安全标准的事件和经历中汲取的教训。

我相信，原子能机构安全标准及其适用将为确保在使用核技术时实现高水平安全作出宝贵的贡献。我鼓励所有成员国宣传和适用这些安全标准，并与原子能机构合作，在现在和将来维护其质量。

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¹具有保护生命和健康以及保护环境的目的。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）。

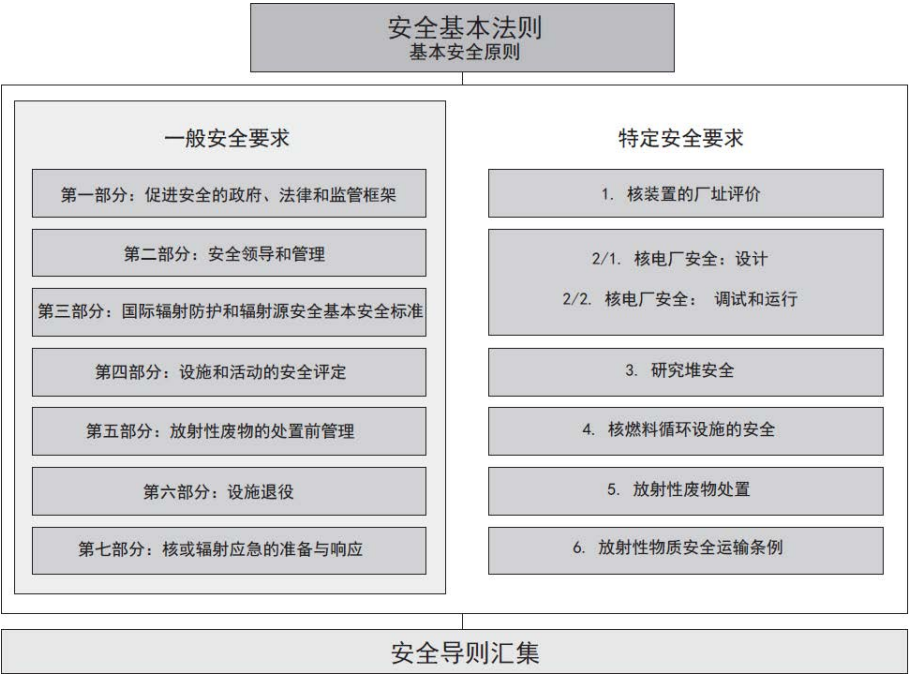


图 1. 国际原子能机构《安全标准丛书》的长期结构。

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）、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。

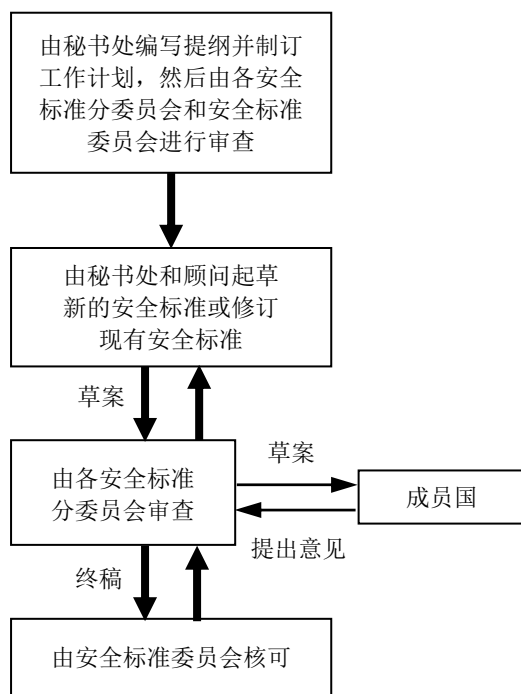


图 2. 制订新安全标准或修订现行标准的过程。

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

安全和核安保相关术语应理解为《国际原子能机构核安全和核安保术语》（见 <https://www.iaea.org/resources/publications/iaea-nuclear-safety-and-security-glossary>）中的术语。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	1
背景 (1.1-1.2).....	1
目的 (1.3-1.4).....	1
范围 (1.5-1.11).....	2
结构 (1.12-1.13).....	3
2. 事故的放射性后果设计方法考虑 (2.1-2.9)	3
3. 纵深防御概念内的设计扩展工况的实施与评定	5
纵深防御的全面实施 (3.1-3.36).....	5
纵深防御的实施的评定 (3.37-3.54).....	15
纵深防御的级别之间独立性 (3.55-3.63).....	18
纵深防御的级别之间的独立性的评定 (3.64-3.68).....	20
4. 电厂事件序列的实际消除可能导致早期放射性排放或 大量放射性排放 (4.1-4.9)	21
相关电厂事件序列的识别 (4.10-4.18).....	22
证实实际消除安全规定的识别和评定 (4.19-4.26)	25
证实实际消除 (4.27-4.42).....	27
实际消除方法的文件 (4.43)	30
5. 确保使用非永久性设备供电和冷却设计规定的实施 (5.1-5.18)	30
参考文献	35
附件 I 实际消除的案例	37
附录 II 按早期标准核电厂中设计扩展工况和实际消除的 设计概念的应用	46
定义	49
参与起草和审订人员	51

1. 引言

背景

1.1. 原子能机构《安全标准丛书》第 SSR-2/1 号《核电厂安全：设计》于 2012 年出版，随后于 2016 年修订为 SSR-2/1 (Rev.1) [1]¹，对核电厂设计要求进行了修改。这些变化包括以下加强应用纵深防御概念的措施：

- (a) 在设计中列入拟考虑的电厂状态之间的设计扩展工况；
- (b) 通过设计确保可能导致早期放射性排放或大量放射性排放的电厂事件序列²已被考虑用于“实际消除”³；
- (c) 包括能够使用非永久性设备供电和冷却的设计特点。

1.2. 将这些方面纳入新的核电厂设计将影响必要的安全评定。原子能机构《安全标准丛书》第 GSR Part 4 (Rev.1) 号《设施和活动安全评定》[3]确立了对所有类型的设施和活动进行安全评定的要求，包括纵深防御评定。SSR-2/1 (Rev.1) [1]规定了核电厂安全评定和安全分析的特定要求。

目的

1.3. 本“安全导则”的目的是为新的核电厂设计提供关于应用选定要求的建议。在 SSR-2/1 (Rev.1) [1]涉及纵深防御和实际消除可能导致早期放射性排放或大量放射性排放的电厂事件序列。本“安全导则”还提供了与纵深防御设计方面相关的建议，特别是与设计扩展工况相关的方面。

¹ 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）。

² 此处的“早期放射性排放”是指有必要采取场外防护行动但不太可能在适当时候完全有效的放射性物质的排放。“大量放射性排放”是指放射性物质的排放，其场外防护措施在时间和应用领域方面受到限制，不足以保护人类和环境[1、2]。

³ “实际消除”术语的定义，请参见本出版物末尾的定义部分。

1.4. 本“安全导则”旨在供参与核电厂安全核实、评审和评定的组织使用。它还旨在对参与核电厂设计、制造、建造、改造和运行以及为核电厂提供技术支持的组织以及监管机构有用。

范围

1.5. 本“安全导则”主要适用于新的陆基固定式核电厂，其水冷反应堆设计用于发电或其他制热应用（如区域供热或海水淡化）。（SSR-2/1（Rev.1）[1]第 1.6 段）。人们认识到，对于由其他介质冷却的反应堆或基于创新设计概念的反应堆，本“安全导则”的一些建议可能不适用或完全不适用，或者在应用时可能需要判断。

1.6. 对于根据早期标准设计的核电厂（SSR-2/1（Rev.1）[1]第 1.3 段），本“安全导则”在评定此类设计的潜在安全改进时可能有用，例如作为电厂定期安全评审的一部分。

1.7. 本“安全导则”着重于第 1.1 段提供的设计安全措施的实施和评定。这些措施在应用纵深防御概念方面发挥了重要作用，根据原子能机构《安全标准丛书》第 SF-1 号《基本安全原则》[4]原则 8，纵深防御是预防和缓解事故后果的主要手段。

1.8. 如 SSR-2/1（Rev.1）[1]第 2.13 段所述，核电厂的纵深防御包括 5 个级别。设计中考虑的电厂状态对应于一个或多个纵深防御级别。本“安全导则”是根据每个电厂状态所需的安全设施⁴的设计来构建，而不是根据每个纵深防御级别来构建。通过这种方式，强调了安全方法的设计扩展工况的意义和重要性。本“安全导则”的特定重点是作为主要放射源的核燃料，特别强调设计扩展工况。

1.9. 本“安全导则”以一般方式考虑了在不同纵深防御级别下实施的结构、系统和部件的独立性评定。然而，可能导致结构、系统和部件之间依赖性的因素，如环境因素、运行或人因以及外部或内部危害，在本“安全导则”没有详细说明。

⁴ 在本“安全导则”，“安全规定”是指应用于结构、系统和部件的设计解决方案以及相关的运行策略。

1.10. 本“安全导则”没有为设计扩展工况或设计中考虑的任何其他电厂状态特定安全特点的设计提供特定建议。此类建议在各种类型电厂系统设计的安全导则中提供，如原子能机构《安全标准丛书》第 SSG-56 号《核电厂反应堆冷却剂系统和相关系统的设计》[5]，第 SSG-53 号《核电厂反应堆安全壳和相关系统的设计》[6]，第 SSG-34 号《核电厂电力系统的设计》[7]，和第 SSG-39 号《核电厂仪器仪表和控制系统的的设计》[8]。

1.11. 本“安全导则”不考虑针对不同电厂状态进行的特定安全分析，因为这些分析在原子能机构《安全标准丛书》第 SSG-2 (Rev.1) 号《核电厂确定性安全分析》[9]有所涉及，第 SSG-3 (Rev.1) 号《制定和实施核电厂一级概率安全评定》[10]和第 SSG-4 号《制定和实施核电厂二级概率安全评定》[11]，视情况而定。但是，本“安全导则”考虑了这些出版物提供的建议。

结构

1.12. 第 2 部分列出了 SSR-2/1 (Rev.1) [1]要求，这些要求管理与防止放射性后果相关的核电厂设计方法，本“安全导则”的建议基于第 3 部分就纵深防御概念内设计扩展工况的实施和评定以及纵深防御级别所考虑的安全规定的独立性提出了建议；第 4 部分就实际消除可能导致早期放射性排放或大量放射性排放的电厂事件序列概念的应用提出了建议；第 5 部分提供了关于实施设计规定的建议，以便能够使用非永久性设备进行供电和冷却。

1.13. 附件 I 提供了会员国之间可能有所不同的实际消除案例的示例；附件 II 提供了将本“安全导则”的建议应当用于按照早期标准设计的核电厂的一些考虑因素（见 SSR-2/1 (Rev.1) [1]第 1.3 段）。

2. 事故的放射性后果设计方法考虑

2.1. 本“安全导则”侧重于核电厂设计特点，这些特点在事故工况下为公众和环境提供保护，并且应当评定其是否符合 SSR-2/1 (Rev.1) [1]许多要求。这些要求涉及电厂的一般设计，特别是电厂在没有不可接受辐射后果的情况下承受比设计基准事故更严重或涉及额外故障事故的能力。

2.2. 如 SSR-2/1 (Rev.1) [1]要求 5 规定：

“核电厂设计必须确保核电厂工作人员和公众的辐射剂量不超过剂量限值，在核电厂的整个寿命期间，在运行状态下保持在合理可达尽量低水平，并在事故工况下和事故发生后保持在可接受的限值以下和合理可达尽量低水平。”

2.3. SSR-2/1 (Rev.1) [1]第 4.3 段指出（脚注略）：

“设计必须确保可能导致高辐射剂量或大量放射性排放的核电厂状态已‘实际消除’，并确保发生可能性很大的核电厂状态不会产生或仅会产生轻微的潜在放射性后果。”

2.4. 此外，SSR-2/1 (Rev.1) [1]第 4.4 段指出（脚注略）：“必须根据监管要求，确定与相关类别电厂状态相关辐射防护目的的可接受限值。”

2.5. SSR-2/1 (Rev.1) [1]还规定了与设计中考虑的不同电厂状态（包括事故工况）的放射性后果相关的标准和目标的进一步要求，特定如下：

- “必须为每个电厂状态指定标准，以便频繁发生的电厂状态不产生放射性后果或仅产生轻微放射性后果，而可能产生严重后果的电厂状态的发生频率必须极低”（SSR-2/1 (Rev.1) [1]第 5.2 段）。
- “首要目标必须是管理所有设计基准事故，使其在场内外没有或只有轻微的放射性后果，并且不需要采取任何场外防护行动”（SSR-2/1 (Rev.1) [1]关于设计基准事故的第 5.25 段）。
- “设计必须确保‘实际消除’可能导致早期放射性排放或大量放射性排放条件的可能性”（SSR-2/1 (Rev.1) [1]关于设计扩展工况的第 5.31 段）。
- “设计必须确保就设计扩展工况而言，在时间长度和适用范围方面受到限制的防护行动必须足以保护公众，并必须有足够的时间采取此类措施”（SSR-2/1 (Rev.1) [1]第 5.31A 段）与设计扩展工况的关系）。

2.6. SSR-2/1 (Rev.1) [1]第 2.10 段指出：

“必须采取措施，确保缓解事故的放射性后果。这些措施包括提供安全设施和安全系统，由营运组织建立事故管理程序，并在可能的情况下由相关当局建立场外防护行动，在必要时得到营运组织的支持，以便在发生事故时缓解风险。”⁵

2.7. 如 SSR-2/1 (Rev.1) [1]第 2.13 段指出：“严重事故工况下的安全目标是，只有在时间长度和应用范围方面受到限制的防护行动才是必要的，并避免或尽量减少场外污染。”

2.8. 对公众有害的放射性后果只有在不受控制的事故发生时才会产生。因此，本“安全导则”的建议侧重于纵深防御概念的实施和评定，以及证实实际消除可能导致早期放射性排放或大量放射性排放的电厂事件序列的补充需求。

2.9. 原子能机构《安全标准丛书》第 SSG-90 号《核电厂设计的辐射防护方面》[13]提供了核电厂设计中的辐射防护建议。关于保护公众和环境的建议见原子能机构《安全标准丛书》第 GSG-8 号《公众和环境的辐射防护》[14]。

3. 纵深防御概念内的设计扩展工况的实施与评定

纵深防御的全面实施

3.1. SSR-2/1 (Rev.1) [1]第 2.12—2.14 段描述了核电厂设计中的纵深防御概念。如 SSR-2/1 (Rev.1) [1]第 2.14 段指出：

“为核电厂实施纵深防御的一个相关方面是在设计中规定一系列实物屏障，以及能动、非能动和固有安全特点的组合，这些特点有助于实物屏障在特定场址限制放射性物质方面的有效性。所需屏障的数量将取决于放射性核素的数量和同位素组成方面的初始源项、单一屏障的有效性、可能的内部和外部危害以及失败的潜在后果。”

⁵ 场外防护行动的建立属于第 5 级纵深防御不在本“安全导则”的范围内。原子能机构《安全标准丛书》第 GSR Part 7 号《核或辐射紧急情况的准备和响应》[12]规定了相关此类安排的要求。

3.2. SSR-2/1 (Rev.1) [1]关于在核电厂设计中应用纵深防御的要求 7 规定：“核电厂设计必须包括纵深防御。纵深防御级别必须尽可能独立。”SSR-2/1 (Rev.1) [1]第 4.9—4.13A 段阐述了这一总体要求。

3.3. 对于每个纵深防御级别的安全规定，应说明以下几点：

- (a) 在该级别执行安全规定的执行情况，以保持屏障的完整性；
- (b) 该级别的安全规定有足够的可靠性，以便能够以足够的信心确保某一电厂状况能够得到控制，而无需执行与下一级别纵深防御相关的安全规定；
- (c) 在切实可行的情况下，该级别的安全设施与先前纵深防御级别的安全设施保持独立，包括实物分隔⁶。

3.4. 通常，出于设计安全和运行安全的目的，各种纵深防御级别与设计中考虑的各种电厂状态有关联。在电厂状态之间引入设计扩展工况导致不同国家在解释设计中考虑的电厂状态与纵深防御级别之间的对应关系方面采取不同的方法。表 1 列出了其中两种方法。

3.5. 在方法 1 中，如表 1 左侧所示，无显著燃料退化的设计扩展工况与第 3 级纵深防御有关联。通过这种方法，每个级别都有一个明确的目标，反映事故的进展和屏障的保护（即，实施第 3 级是为了防止燃料损坏，实施第 4 级是为了缓解严重事故和防止场外污染）。如 SSG-2 (Rev.1) [9]第 3.39 段指出：

“在无显著燃料退化的设计扩展工况下，初步选择顺序时必须考虑到频率极低的单一始发事件或多次故障，以满足防止堆芯损坏的验收标准。”

⁶ 实物分隔是通过几何构型（距离、方向等）、适当的屏障或其组合进行的隔离[2]。

表 1. 纵深防御级别

防御级别	目标	重要设计手段	重要运行手段	防御级别
方法 1				方法 2
第 1 级	预防异常运行和故障	稳健的设计和高质量的建造正常运行系统，包括监控和控制系统	运行限值和条件以及正常运行程序	第 1 级
第 2 级	控制异常运行及检测失败	限制和保护系统和其他监视特点	异常的运行程序和/或应急运行程序	第 2 级
3a	控制设计基准事故	安全系统	应急运行程序	第 3 级
第 3 级	设计控制扩展工况防芯熔化	无显著燃料退化的设计扩展工况下的安全特点 ^a	应急运行程序	第 4 级
3b				
第 4 级	设计扩展控制工况以缓解严重事故的后果	堆芯熔化 ^b 设计扩展工况下的安全特点技术支持中心	严重事故管理导则	
第 5 级	缓解放射性物质大量排放的放射性后果	场内和场外应急响应设施	场内和场外应急预案和程序	第 5 级

^a 此类安全特点被理解为设计扩展工况下的附加安全特点，或具有防止严重事故后果扩展能力的的安全系统（见 SSR-2/1（Rev.1）[1]第 5.27 段）。

^b 此类安全特点被理解为设计扩展工况下的附加安全特点，或具有扩展能力的的安全系统，以缓解严重事故的后果或保持安全壳的完整性（见 SSR-2/1（Rev.1）[1]第 5.27 段）。

因此，在方法 1 中，在无显著燃料退化的情况下，设计扩展工况下预测放射性后果的可接受限值可能与设计基准事故的可接受限值相同或相似。此外，与设计基准事故和无显著燃料退化的设计扩展工况相关的实物现象是相似的，尽管在分析中可能存在差异。相比之下，与堆芯熔化的设计扩展工况相关的实物现象完全不同。

3.6. 在表 1 右侧所示的方法 2 中，无显著燃料退化的设计扩展工况和有堆芯熔化的设计扩展工况被一起考虑在第 4 级纵深防御中。这种方法强调在设计和安全评定中，适用于设计扩展工况的一套规则和适用于设计基准事故的一套规则之间的区别。

3.7. 尽管存在差异，但这两种方法都符合 SSR-2/1 (Rev.1) [1]第 5.29 (a) 段，并支持在切实可行的范围内实现安全系统与设计扩展工况下的安全特点之间的独立性。

正常运行和预计运行事件

3.8. 运行状态包括两组电厂状态：正常运行和预计运行事件。正常运行模式包括，例如，启动、功率运行、停堆、关闭和换料，并在管理电厂运行的文件中定义（例如，运行限值和条件⁷）。预计运行事件⁸可能由假想始发事件⁹发生，该事件涉及未能防止异常运行或预计在电厂运行寿命期间发生的设备故障。

3.9. SSR-2/1 (Rev.1) [1]第 4.13 段指出：

“设计必须确保在切实可行的范围内，第 1 级或至多第 2 级纵深防御能够防止在核电厂运行寿命期间可能发生的所有故障或偏离正常运行工况升级为事故工况。”

⁷ 在一些国家，使用“技术规范”术语，而不是“运行限值和条件”术语。

⁸ 预计运行事故是指运行过程偏离正常运行，预计在设施的运行寿命期间至少会发生一次，但根据适当的设计规定，不会对安全重要物项造成任何重大损坏或导致事故工况[2]。

⁹ SSG-2 (Rev.1) [9]第 3.28 段提供了相关假想始发事件的示例。

因此，为了保持用于密封放射性物质的第 1 个实物屏障（即燃料包壳）的完整性，并防止一回路冷却剂显著排放，运行状态的设计规定应当具备实现以下目标的充分能力：

- (a) 通过健稳的设计、符合经证实的工程实践和与这些设计规定对安全的重要性相称的高质量标准，防止故障或偏离正常运行；
- (b) 探测及拦截偏离正常运行工况，并使该电厂恢复正常运行状态；
- (c) 防止预计运行事件一旦开始就升级为事故工况。

3.10. 预计运行事件安全规定的可靠性应当确保向设计基准事故过渡的频率低于设计基准事故的假想始发事件的最高频率（通常低于每个反应堆年 10^{-2} 次）（见 SSG-2（Rev.1）[9]附件 II 表 II-1）。

设计基准事故

3.11. SSR-2/1（Rev.1）[1]要求 19 规定：

“设计中要考虑的一组事故，必须从假想始发事件中推导，目的是确定核电厂承受的边界条件，而不超过辐射防护的可接受限值。”

3.12. SSR-2/1（Rev.1）[1]第 5.24 段指出：“设计基准事故必须用于定义安全系统和其他安全重要物项的设计基准，包括性能标准，这些物项是控制设计基准事故工况所需要的。”

3.13. SSR-2/1（Rev.1）[1]第 5.25 段指出：

“设计必须确保在设计基准事故工况下，关键设备参数不超过规定的设计限值。首要目标必须是管理所有设计基准事故，使其在场内或场外不产生放射性后果，或仅产生轻微放射性后果，并且不需要采取任何场外防护行动。”

因此，应当实施特定的设计规定（即安全系统），通过防止显著燃料损坏和保持安全壳的完整性（即保持安全壳的结构完整性和维护其相关系统¹⁰）来防止和缓解设计基准事故的放射性后果。安全系统的目标是限制对公众和环境的辐射后果，使其不需要采取场外防护行动。

¹⁰ 安全壳及其相关系统在 SSG-53[6]第 1.3 段描述。

3.14. 核电厂寿命期间最有可能发生的事故工况被归类为设计基准事故，其预期频率通常低于每个反应堆年 10^{-2} 次。设计基准事故应当包括由于第 1 级和第 2 级纵深防御故障而导致的单一始发事件¹¹。安全系统的设计应当通过确保安全功能的实现和屏障的维护来控制设计基准事故中考虑的假想始发事件。设计用于控制需要迅速和可靠行动的设计基准事故安全系统（见 SSR-2/1 (Rev.1) [1] 第 5.11 段）应当依靠自动驱动，并应当尽量减少运行人员短期行动的需要。安全系统的设计、建造和维护应当确保其可靠性与其安全意义相称。安全设计概念，如足够的裕度和冗余性，需要应用于安全系统的设计和建造（见 SSR-2/1 (Rev.1) [1] 要求 24 和第 5.21A 段、第 5.42 段和第 5.73 段）。安全系统鉴定计划中考虑的环境条件应当与设计基准事故和假想内部和外部危害引起的负载和不利环境条件相对应。相应的安全导则中提供了关于核电厂特定安全系统设计的进一步建议（见 SSG-56[5]、SSG-53[6]、SSG-34[7]和 SSG-39[8]）。

设计扩展工况

3.15. SSR-2/1 (Rev.1) [1] 要求 20 指出：

“必须在工程判断、确定性评定和概率评定的基础上制定一套设计扩展工况，以进一步改善核电厂的安全，提高核电厂在不产生不可接受的辐射后果的情况下承受比设计基准事故更严重或涉及其他故障事故的能力。这些设计扩展工况必须用于确定设计中要处理的额外事故假想方案，并为预防此类事故或缓解其后果制定切实可行的规定。”

3.16. SSR-2/1 (Rev.1) [1] 第 5.30 段指出：

“特别是安全壳及其安全特点必须能够承受极端情况，包括反应堆堆芯熔化等。这些假想方案必须通过工程判断和概率安全评定的输入来选择。”

¹¹ 在一些国家，使用术语“不频繁和限制性故障”（见 SSG-2 (Rev.1) [9] 表 II-1），而其他国家可能使用不同的术语。

3.17. 为了满足第 3.15 段和第 3.16 段提出的要求，可以确定两类不同的设计扩展工况¹²：无显著燃料退化的设计扩展工况¹³和有堆芯熔化的设计扩展工况¹⁴。这种区别反映了这样一个事实，即根据防止燃料退化的目标，最常见的设计扩展工况不应当导致燃料退化。

3.18. 如表 1 和第 3.4—3.7 段所示，各国对设计扩展工况采用以下两种主要实践：

- (a) 在一些国家，设计扩展工况分为燃料无显著退化的设计扩展工况和堆芯熔化的设计扩展工况。在一些国家，极低频率始发事件被视为无显著燃料退化的设计扩展工况。在其他国家，对于涉及多次故障的复杂序列，假设无显著燃料退化的设计扩展工况，而非常低频率的假设单次始发事件被视为设计基准事故。第 3.19—3.28 段提供了与燃料无显著退化的设计扩展工况相关的建议。第 3.29—3.36 段提供了与堆芯熔化的设计扩展工况相关的建议。
- (b) 有些国家没有根据燃料状况或故障次数细分设计扩展工况。在这种方法中，相同的高水平剂量限值和分析规则用于设计扩展工况的所有事件序列。采用这种实践的国家可酌情采用第 3.19—3.36 段的建议。

无显著燃料退化的设计扩展工况

3.19. 应当开发一个在无显著燃料退化性能的情况下全面识别设计扩展工况的流程。SSG-2 (Rev.1) [9]第 3.39—3.44 段提供了在无显著燃料退化的情况下确定设计扩展工况的建议。

3.20. 一般来说，在无显著燃料退化的情况下，设计扩展工况的控制应当通过专门为这种工况设计和鉴定的安全特点来实现。或者，无显著燃料退化的设计扩展工况可以由可用的安全系统来控制，前提是安全系统没有受到导致所考虑设计扩展工况的事件影响，并且它们能够并且经鉴定在相关的环境条件下运行。SSR-2/1 (Rev.1) [1]要求 13 规定：“**核电厂状态必须主要根据其在核电厂出现的频率进行识别并分成有限数量的级别。**”

¹² “设计扩展工况”的定义见 SSR-2/1 (Rev.1) [1]。

¹³ “无显著燃料退化的设计扩展工况”术语包括反应堆堆芯燃料和乏燃料水池燃料的分析情况。

¹⁴ 在一些国家，这些类别的设计扩展工况分别被称为“设计扩展工况 A”（燃料无显著退化）和“设计扩展工况 B”（堆芯熔化）。

3.21. 在无显著燃料退化的情况下，对设计基准事故和设计扩展工况的确定性安全分析可能具有相似的安全目标，即证实屏障的完整性将得到保持，并防止堆芯损坏或乏燃料水池中的燃料损坏（见 SSG-2（Rev.1）[9]第 7.28 段和第 7.45 段）。

3.22. 在不发生显著燃料退化的情况下，区分了设计基准、事故和设计扩展工况设计要求和使用不同的可接受限值或标准¹⁵或方法进行确定性安全分析。因此，对于无显著燃料退化的设计扩展工况，以下条件适用：

- (a) 可能适用比设计基准事故更宽松的设计要求。例如，无显著燃料退化的设计扩展工况的安全特点可能被分配到比安全系统更低的安全级别。
- (b) 确定性安全分析可接受比设计基准事故或最佳估计方法更保守的假设（见 SSG-2（Rev.1）[9]第 7.35—7.44 段和 7.47—7.55 段）。
- (c) 与设计扩展工况的放射性后果相关的总体限值或标准的要求见 SSR-2/1（Rev.1）[1]第 5.31A 段。各国可以选择对设计扩展工况适用更严格的限值或标准，而不会显著燃料退化。例如，一些国家可能选择对设计基准事故的辐射后果适用相同或相似的总体限值或标准（见 SSG-2（Rev.1）[9]第 7.32 段、第 7.33 段和第 7.46 段）。

3.23. 如果有可能使用现有安全系统来响应设计扩展工况而不会显著燃料退化，则仍然需要进行安全分析来证实其有效性（参见 SSR-2/1（Rev.1）[1]要求 42）。确定性安全分析可能使用比设计基准事故更保守的方法和假设（见第 3.22 段）。尽管如此，对确定性安全分析的结果仍应当有足够的置信度，避免陡边效应的安全裕度应当证实是足够的（见 SSG-2（Rev.1）[9]第 7.45 段、第 7.54 段和第 7.55 段）。

3.24. 要求以保守的方式分析设计基准事故（见 SSR-2/1（Rev.1）[1]第 5.26 段）。然而，无显著燃料退化的设计扩展工况有可能超过安全系统的既定能力。因此，根据最佳估计分析和比用于设计基准事故的假设更保守的假设，有可能证实一些在设计中具有扩展能力的安全系统能够并且经鉴定在无显著燃料退化的情况下缓解设计扩展工况。

¹⁵ SSR-2/1（Rev.1）[1]使用的“与放射性后果相关的可接受限值”和 SSG-2（Rev.1）[9]使用的“与放射性后果相关的可接受标准”被认为是相同的术语。

3.25. 与设计基准事故类似，在无显著燃料退化的情况下，在设计扩展工况下，应当尽可能合理地将放射性排放降至最低。

3.26. 预计运行事件和频繁设计基准事故以及安全系统故障应当被视为设计扩展工况清单的一部分，而不会出现显著的燃料退化（见 SSG-2（Rev.1）[9]第 3.40 段）。在许多电厂设计中，这些工况包括无应急停堆的预期瞬态和电厂断电¹⁶。

3.27. 在工程判断、确定性安全分析和概率安全评定的基础上，在确定为防止和减少安全系统故障造成的严重事故而实施的安全规定时，还应当考虑无显著燃料退化的设计扩展工况。如有可能，此类安全规定应当包括额外的多样化措施，以应对安全系统的共因故障。

3.28. 在无显著燃料退化的情况下考虑设计扩展工况，增强了设计的健稳性，以应对一些复杂和不太可能的故障序列，并平衡了电厂的整体风险状况。因此，在无显著燃料退化的设计扩展工况下，安全系统和安全特点的可靠性应当足够高，以通过使升级为严重事故的可能性极小来防止严重事故。

堆芯熔化设计扩展工况

3.29. 根据 SSR-2/1（Rev.1）[1]要求 42、第 5.9 段和第 5.30 段，并考虑到研究和开发的结果，应当假设一套具有代表性的堆芯熔化事故工况，为安全壳的设计和确保其功能的安全特点提供输入。在设计堆芯熔化的设计扩展工况的安全特点时，应当考虑这组代表性事故工况，并应当代表包络堆芯退化更有限的其他严重事故的边界情况。

3.30. SSR-2/1（Rev.1）[1]第 6.68 段指出（脚注略）：

“对于使用水池系统贮存燃料的反应堆，其设计必须防止在与乏燃料水池相关的所有电厂状态下燃料组件暴露，以便‘实际消除’可能导致早期放射性排放或大量放射性排放条件的可能性，并避免现场出现高辐射场。”

¹⁶ 见第 SSG-34[7]第 5.8 段，以界定全厂断电的定义。

因此，乏燃料水池中的显著燃料退化不应当被假定为这组设计扩展工况的一部分，相反，它需要被视为实际消除的条件之一（见第 4 部分）。

3.31. 应当进行详细的分析并记录在案，以识别和描述可能导致堆芯损坏以及挑战或安全壳旁路的事故工况。可能导致堆芯损坏的相关事故工况应当假定为设计扩展工况（见 SSG-2（Rev.1）[9]第 3.46 段和第 3.47 段以及 SSG-53[6]第 2.11 段），即使根据 SSR-2/1（Rev.1）[1]要求采取的防止此类事故的设计规定将使堆芯损坏的概率非常低。在设计堆芯熔化的设计扩展工况下的安全特点时，应当考虑影响事故进展以及影响安全壳响应和源项的方面（见 SSG-53[6]第 3.42 段）。

3.32. 应当评定堆芯熔化时设计扩展工况下安全特点的能力和可靠性，以确保它们足以满足其需要实现的安全功能。

3.33. 在建立事故管理程序和导则时，应当堆芯熔化设计扩展工况对电厂安全提出的挑战，以及合理预计设计缓解其后果的程度。这方面的建议见原子能机构《安全标准丛书》第 SSG-54 号《核电厂事故管理计划》[15]。

3.34. 为了避免过压对安全壳完整性造成的风险，应当控制安全壳内部的压力。这可以通过以下方式实现：在堆芯熔化的设计扩展工况下确保和保持反应堆安全壳气氛的充分冷却，通过过滤反应堆安全壳排气系统使安全壳压力降低，或通过其他设计特点或替代措施（见 SSG-90[13]第 11.8 段）。在堆芯熔化的设计扩展工况下，反应堆安全壳放射性排放物的过滤和未过滤直接泄漏的后果应当保持在根据 SSG-53[6]第 2.7 段和 SSG-90[13]第 2.10 段提供建议确定的设计目标以下。并根据 SSG-90[13]第 11.7 段提供建议进行评定，以便有足够的时间实施场外防护措施。在任何时候，都应当控制放射性排放，以满足避免被视为早期放射性排放或大量放射性排放的时间和数量标准。

3.35. 如 SSG-53[6]第 3.44 段和第 3.45 段指出：

“必须采取多种手段控制安全壳内发生事故时的压力积聚，通风（如有[包括在设计中]）必须仅作为最后手段使用。……排放系统的使用不应导致早期放射性排放或大量放射性排放”。

3.36. 设计的安全评定应当考虑严重事故现象及其后果的进展以及可接受的最终状态条件的实现，并应当考虑适用的专题问题。关于堆芯损坏后可能发生的一系列实物过程的更详细信息见 SSG-2 (Rev.1) [9]第 7.66 段。

纵深防御的实施的评定

3.37. 需要对核电厂设计中纵深防御的实施进行评定，以确保每一级别的安全规定都得到充分设计，以满足该级别在预防、探测、限制和缓解方面的目标。GSR Part 4 (Rev.1) [3]要求 13 指出：“在评定纵深防御时，必须确定是否在纵深防御的每个级别都做了充分的准备。”

3.38. GSR Part 4 (Rev.1) [3]第 4.45—4.48 A 段建立了纵深防御评定的附加要求。

3.39. 应当考虑到一套适用的分析规则，对所有电厂状态安全规定的性能和可靠性进行评定，安全规定的风险水平和安全意义。安全规定的设计应当保持屏障的完整性，达到相关电厂状态所需的程度，或缓解假想故障的后果。评定应当提供证据，证实与每一级纵深防御相关的安全措施的性能和可靠性是充分的。评定应当证实对于每个可信的始发事件，风险与事件的频率相称，并考虑到可能导致事件的内部和外部危害的所有后果。评定应当考虑来自工程方面的评定以及来自确定性安全分析和概率安全评定的见解，视情况适用于每个不同的电厂状态。

3.40. 防御级别的多样性不能成为依靠其他级别的效力来削弱某些级别效力的正当性。在合理和平衡的设计中，结构、系统和部件在每一防御级别，其表征在于与其功能和安全显著性相称的可靠性，并提供合理的安全裕度。

3.41. 纵深防御概念应当适用于核电厂中存在的所有辐射源。以下是核电厂可能存在的辐射源的示例：

- 反应堆堆芯；
- 新核燃料、辐照燃料和燃料桶；
- 中子源和其他放射源；
- 厂房内的空气放射性物质；

- 含有放射性物质的管道和加工设备（例如反应堆冷却剂系统，反应堆冷却系统，辅助系统，控制区的供暖、通风和空调系统，气态和液态流出物处理系统，固体废物处理系统）。

3.42. 对于反应堆堆芯和核燃料以外的辐射源，应当按照分级方法实施纵深防御，同时考虑到某些纵深防御级别可能不适用于核电厂内的许多辐射源。应当考虑到存在的放射性物质的数量和类型所带来的风险，由于其物理和化学性质，其扩散的可能性，以及在正常或异常工况下可能发生的核、化学或热反应的可能性以及这些反应的动力学。对于不同的辐射源，这些特征将有所不同，并将影响必要的纵深防御级别和每一级别的强度。

3.43. 在评定实施纵深防御的充分性时，设计中包括的实物屏障是一个重要的考虑因素。对于每个已确定的辐射源应当确定实物屏障，并根据分级方法评定其稳健性。评价中应当评定以下方面：

- (a) 每个屏障的设计都应当留有适当的裕度，并应当根据构成屏障设备的辐射风险或安全级别，采用分级方法评定各种屏障的稳健性。
- (b) 设计、制造或建造屏障时应当采用适当的规范和标准，制造或建造时应当使用经过证实的材料和技术。
- (c) 在运行状态和事故工况下可应用于屏障的所有负载和负载组合，包括由设计中考虑的内部和外部危害的影响所引起的负载，均须加以识别和计算，并须显示为小于适用的限值。
- (d) 设计中提供的屏障数量应当正当，为每个电厂国家选择的屏障应当为工作人员和公众提供合理预计最佳防护。
- (e) 屏障中用于防止放射性排放的阀门、其控制设备和其他设备的设计应当确保屏障在事故工况下的结构完整性。
- (f) 屏障偏离其正常配置（例如，当电厂处于关闭状态时，为容纳某些活度而进行的开放式安全壳）的任何情况都应当证实是正当的，证实尽管屏障处于临时配置（或运行），但仍保持了充分的保护。

3.44. 应当对可能挑战或降低安全功能性能的各种机制进行分析，以评定为防止此类机制的发生或阻止其发展而实施安全规定的充分性。如果不同的退化机制可能需要不同的安全规定，则应当对每种退化机制评定每种安全规定的充分性和有效性。

3.45. 安全规定的充分性和有效性应当通过执行确定性安全分析来评定，确定性安全分析应当模拟电厂对给定始发事件的响应，以代表每个事件的不同边界条件电厂状态。每个电厂状态都应当以一种确定性安全分析为表征，具有一套适用的分析规则、保守性水平和验收标准。SSG-2 (Rev.1) [9] 提供了对不同电厂状态进行确定性安全分析的建议。

3.46. 通过工程方面的评定和确定性安全分析来评定每个纵深防御级别的安全措施的性能，确定性安全分析涉及使用经过验证和核实的计算机代码和模式，以证实符合验收标准，并且有足够的裕度来避免陡边效应。SSG-2 (Rev.1) [9]第 5.14—5.39 段提供了进一步的建议。

3.47. 不同电厂状态下安全规定的可靠性分析，如第 3.39 段所示，通常使用概率技术，并考虑到电厂布局和针对危害影响的保护规定或鉴定，以及冗余性和多样性设备的设计、制造、维护和试验中的潜在共性。

3.48. 可靠性声明应当得到与被评定的结构、系统或部件相关的设备可靠性数据的支持，并得到试验数据、成熟技术和工程实践的使用以及运行经验反馈的支持。可靠性声明还应当通过核实结构、系统或部件是否符合适用的设计要求来支持。不同系统或纵深防御级别的可靠性分析可以整合到概率安全评定中，以评定整体电厂风险指标，如堆芯损坏频率或早期放射性排放或大量放射性排放的频率。

3.49. 如果这些系统的共因故障会导致不可接受的燃料损坏或不可接受的放射性后果，则应当核实在不同电厂状态下实现相同基本安全功能的系统设计中实施了足够的多样性。

3.50. 用于控制预计运行事件的结构、系统和部件的可靠性应当能有效减少对安全系统的挑战，并有助于防止事故工况的发生。

3.51. 安全系统和附加安全特点在设计扩展工况下的可靠性，在无显著燃料退化性能的情况下，应当使得堆芯损坏频率不超过设定的核电厂的任何安全目标（例如，对于新的核电厂，通常低于每个反应堆年 10^{-5} 次）。应当假设无显著燃料退化的设计扩展工况（见 SSG-2 (Rev.1) [9]第 3.39—3.44 段），并考虑适用的分析规则（见 SSG-2 (Rev.1) [9]第 7.45—7.55 段）进行分析，以实现安全目标。

3.52. 应当识别任何可能导致安全系统完全故障的漏洞，并评定此类故障与假想始发事件相结合是否会升级为堆芯熔化事故。对于所分析的每个此类组合，如果后果超过设计基准事故的可接受范围，并可能涉及不可接受频率的堆芯熔化，则应当实施隔离、独立和多样且不太可能因同一共因故障的安全特点（例如，在应急电源完全丧失的情况下使用备用交流电源，或使用隔离和多样的衰变热去除链）。

3.53. 堆芯熔化设计扩展工况下安全特点的能力和可靠性应当足以确保安全壳的完整性不会在任何假想堆芯熔化序列中受到损坏。在评定安全特点的可靠性时，应当考虑与堆芯熔化事故分析相关的任何大的不确定性。

3.54. 应当证实设计扩展工况下安全系统和安全特点的可靠性已考虑其支持系统的可靠性。

纵深防御的级别之间独立性

3.55. SSR-2/1 (Rev.1) [1]第 4.13A 段指出：

“纵深防御的级别必须尽可能独立，以避免一个级别的失效削弱其他级别的有效性。特别是，设计扩展工况下的安全特点（特别是缓解涉及燃料熔化事故后果的特点）必须在切实可行的情况下尽可能独立于安全系统。”

3.56. SSR-2/1 (Rev.1) [1]一些附加要求有助于确保纵深防御级别的独立性。例如，共享在不同电厂状态下执行功能的结构、系统或部件是可能损坏纵深防御级别独立性的一个因素。SSR-2/1 (Rev.1) [1]要求 21 规定：

“安全系统之间或系统冗余元件之间的干扰必须酌情通过实物分隔、电气隔离、功能独立和通信（数据传输）独立等手段加以预防。

3.57. 特别是对于保护系统和控制系统，SSR-2/1 (Rev.1) 要求 64 规定：“核电厂的保护系统和控制系统之间的干扰必须通过隔离、避免互连或适当的功能独立性来预防。”

3.58. 关于支持系统和辅助系统，SSR-2/1 (Rev.1) [1]要求 69 规定：“支持系统和辅助系统的设计必须确保这些系统的性能与它们在核电厂服务的系统或部件的安全意义一致。”

3.59. 共因故障的可能性是损坏纵深防御级别独立性的第二个因素。常见共因故障的典型根本原因是设计或制造中未被发现的人为错误，运行或维护中的人为错误，设备鉴定不足或对内部或外部危害的保护不足。SSR-2/1 (Rev.1) [1]要求 24 规定：

“设备的设计必须适当考虑到安全重要物项可能发生共因故障，以确定须要应用多样性、冗余性、实物分隔和功能独立的概念来实现必要的可靠性。”

3.60. 纵深防御级别的完全独立可能很难实现。核电厂设计应当考虑依赖性的所有潜在原因，并应当实施一种方法，在合理可行的范围内消除这些原因。对于同时发生故障会导致对人类或环境产生有害影响的系统，应当实现强大的独立性。

3.61. 在可行的情况下，应当避免共享安全系统或其一部分来执行不同电厂状态的安全功能。特别是，应当确保在可能跟随假想始发事件的事件序列中，在给定的电厂状态下被认为是响应的安全系统对于先前的电厂状态是不需要的。如 SSR/2-1 (Rev.1) [1]第 4.13A 段指出：“设计扩展工况下的安全特点（特别是缓解涉及燃料熔化事故后果的特点）必须在切实可行的范围内独立于安全系统。”

3.62. 不同设备状态所需的系统应当在功能上彼此隔离，这样，在给定设备状态下的系统中的失误或故障不会影响在不同设备状态下所需的另一个系统。然而，反应堆设计的实际限制在某些情况下可能需要豁免这种功能隔离，尽管每种情况都应当是正当的。

3.63. 用于缓解堆芯熔化设计扩展工况的系统应在功能和实物上尽可能与用于其他电厂状态的系统分隔。然而，如果可以证明，如果条件确实演变为堆芯熔化的设计扩展工况，这种使用不会破坏这些安全特点执行其主要功能的能力，那么出于充分的理由，堆芯熔化设计扩展工况的安全特点也可用于防止严重的堆芯损坏。例如，如果需要，用于堆芯熔化的设计扩展工况的电源可以用于为设计扩展工况的设备供电，而不会显著燃料退化。

纵深防御的级别之间的独立性的评定

3.64. 应当使用工程评定以及确定性和概率方法来评定纵深防御级别的独立性。应当确定每一个假想始发事件所需的结构、系统和部件，并应当通过工程分析证明实施每一级纵深防御所需的结构、系统和部件与其他级别的结构、系统和部件充分独立。假想始发事件通常是涵盖不同类型始发事件的边界事件，因此可能很难列出最初可能受特定设计扩展工况下假想始发事件影响的所有正常运行设备。因此，在设计扩展工况的安全评定中，应当极其谨慎地考虑将系统计入正常运行，并应当充分证实其正当性。纵深防御级别之间独立性的充分性也应当通过概率分析进行评定。

3.65. 评定应当证实连续防御级别之间的独立性足以限制偏离正常运行的进展，并防止在发生事故时对公众和环境产生有害影响。对纵深防御级别之间的独立性评定应当旨在核实声称独立的结构、系统和部件之间共因故障的脆弱性已被识别并在可行的范围内消除。这种常见原因故障可能源于布局、设计、制造、运行或维护。如果结构、系统和部件之间的功能依赖关系尚未消除，则应当在评定中判断这一点。

3.66. 评定应当证实用于应对事故的安全系统不会受到始发事件的危害。评定应当证实安全系统的可运行性不会因为正常运行而设计的系统故障而受到损坏。在始发事件之后，在预计运行事件中发生的故障不应当损坏安全系统管理设计基准事故的能力。

3.67. 评定应当证实支持系统的故障不会同时影响不同电厂状态的系统部件，从而损坏履行安全功能的能力。为此，评定应当提供证据，证实支持系统的可靠性、冗余性、多样性和独立性与被支持系统的安全重要性相称。

3.68. 应当对不同纵深防御级别可能需要的结构、系统和部件的独立性进行评定，以缓解单一危害或内部或外部危害可能组合对电厂造成的后果。应当证实假想始发事件和电厂中引发的故障不会导致结构、系统和部件的共因故障，这些结构、系统和部件是缓解不同纵深防御级别的危害后果所必需的。特别是，应当进行评定以确保共因故障不会同时影响 (i) 安全系统执行的安全功能或设计扩展工况下的一些安全功能，而不会显著燃料退化；以及 (ii) 堆芯熔化的设计扩展工况下必要安全功点的安全功能。

4. 电厂事件序列的实际消除可能导致早期放射性排放或大量放射性排放

4.1. SSR-2/1 (Rev.1) [1]第 2.11 段指出(脚注略):

“可能导致高辐射剂量或大量放射性排放的核电厂事件序列必须要‘实际消除’……一个基本目标是限制或甚至从技术角度消除为缓解放射性后果而采取场外防护行动的必要性, 尽管负责当局可能仍要求此类措施。”

4.2. 关于第 4 级纵深防御, SSR-2/1 (Rev.1) [1]第 2.13 段指出(脚注略): “需要‘实际消除’导致早期放射性排放或大量放射性排放的事件序列。”

4.3. SSR-2/1 (Rev.1) [1]第 5.31 段指出(脚注略): “设计必须确保‘实际消除’可能导致早期放射性排放或大量放射性排放条件的可能性。”

4.4. 虽然“早期放射性排放”术语主要用于 SSR-2/1 (Rev.1) [1], 但“高辐射剂量”术语出现在 SSR-2/1 (Rev.1) [1]第 2.11 段和第 4.3 段。它应当被解释为指由于早期放射性排放而可能发生的剂量, 因为无法及时有效地采取防护行动来防止这种剂量。

4.5. 实际消除的概念只应当适用于那些可能导致无法通过合理可行的手段缓解的不可接受后果(即早期放射性排放或大量放射性排放)的事件或事件序列。这种电厂事件序列的实际消除需要通过设计来确保(见 SSR-2/1 (Rev.1) [1]), 要么通过确保电厂事件序列在实物上是不可能的(见第 4.33 段和 4.34 段), 要么因为电厂事件序列被认为是极不可能出现的(见第 4.35—4.42 段)。

4.6. 实际消除的概念应当作为核电厂设计总体安全方法的一部分加以应用, 如 SSR-2/1 (Rev.1) [1]第 2 部分所述。由于充分实施了第 1 级、第 2 级、第 3 级和第 4 级纵深防御, 在大多数情况下, 事故可能导致场外放射性排放的可能性将非常低。然而, 有必要核实不存在无法有效和实际缓解并因此可能导致不可接受放射性后果的可信电厂工况。这就是实际消除概念的目的: 通过重点分析那些可能产生不可接受的放射性后果的条件, 补充在电厂充分实施纵深防御的工作。

4.7. 不应当将实际消除视为缓解严重事故后果的替代方法（即实施第 4 级和第 5 级纵深防御）。相反，实际消除的应用可能导致 (i) 通过明确识别那些无法合理管理的堆芯熔化序列，确定补充设计中纵深防御的额外规定；以及 (ii) 实施额外的手段来防止这些堆芯熔化序列。此外，根据 SF-1[4] 原则 9 和 GSR Part 7[12]要求，实际消除可能导致早期放射性排放或大量放射性排放的电厂事件序列并不能排除应急准备和响应的需要。

4.8. SSR-2/1 (Rev.1) [1]没有为事故工况的放射性后果提供定量验收限值或标准，也没有为被视为早期放射性排放或大量放射性排放的幅度提供定量验收限值或标准。与设计或术语的特定定义无关，早期放射性排放或大量放射性排放将挑战第 5 级纵深防御的规定。在一些国家，考虑到对及时实施场外防护行动的限制，对特定场址的早期放射性排放进行了定义。在另一些国家，大量排放被认为是远远超过堆芯熔化验收标准的排放，对公众或环境造成非常显著的影响。另一些国家根据监管要求或目标，制定了用于辐射防护目的的放射性排放的可接受限值，以及用于证实堆芯损坏事故发生频率较低的概率标准或目标值。

4.9. 在新建核电厂中，应当从早期阶段起就采用实际消除的概念，因为这一阶段的设计和建造更加切实可行实施额外的安全特点¹⁷。这些特点的结合应当是一个迭代的过程，应当以互补的方式使用来自工程经验、确定性安全分析和概率安全评定的见解。此外，人们认识到，在电厂的整个生命周期中，可能需要采取运行措施，以确保满足设计假设。

相关电厂事件序列的识别

4.10. 证实实际消除可能导致早期放射性排放或大量放射性排放的电厂事件序列的第 1 步是识别这种电厂事件序列。该识别过程预计将产生一个电厂事件序列清单，该清单可以在为电厂识别的严重事故中被分组到一个较小的电厂工况集合中。识别过程应当得到相关信息的判断和支持。

¹⁷ 这些额外的安全特点包括在评定后实施的任何设计规定，以支持实际消除一些电厂事件序列的证实。一些设计规定已经实施，以支持其他安全目标和分析，也可以支持证实实际消除。

4.11. 在严重的事故中，大量的放射性物质存在，并且不局限于燃料或反应堆冷却剂系统内。此外，严重的事故现象可以非常迅速地产生大量的能量。总之，这些都对放射性物质的密封提出了挑战，因为可能会产生不可接受的放射性后果。

4.12. 因此，如果发生严重事故，需要确保核燃料排放的放射性物质受到密封。特别是，在有限密封的情况下（例如，在涉及燃料贮存事故中，或者当安全壳打开而不能及时关闭时，或者当安全壳旁路不能隔离时），防止不可接受的放射性后果的唯一方法是防止这种严重事故的发生。在这种情况下，有必要通过证实事故在实物上不可能发生或通过高置信度证实这种严重事故极不可能发生来证实实际排除。因此，当考虑是否应当实际消除特定的电厂事件序列时，问题是事件序列导致密封功能失效的可能性。

4.13. 为了帮助确保证实实际消除是可管理的，应当将可能导致不可接受的放射性后果的整套单一电厂事件序列进行分组，以形成有限数量的边界情况或事故工况类型（另见第 4.15 段）。应当考虑以下 5 种一般类型的电厂事件序列，这取决于它们对特定设计的适用性：

- (a) 可能导致反应堆堆芯迅速损坏和随后的早期安全壳故障的核电厂事件序列，例如：
 - (i) 反应堆冷却剂系统中的大型压力保持部件发生故障；
 - (ii) 不受控制的反应性事故。
- (b) 可能导致早期安全壳故障的核电厂事件序列，例如：
 - (i) 高能直接安全壳加热；
 - (ii) 大的蒸汽爆炸；
 - (iii) 氢气和一氧化碳等可燃气体爆炸。
- (c) 可能导致安全壳后期故障的核电厂事件序列，例如以下内容：
 - (i) 熔融堆芯熔融物与混凝土相互作用期间，地基垫穿透或对安全壳完整性的其他损坏；
 - (ii) 安全壳排热的长期丧失（例如安全壳排热系统故障）；
 - (iii) 氢气和一氧化碳等可燃气体爆炸。

- (d) 具有安全壳旁路的电厂事件序列，例如：
 - (i) 可能导致泄漏的冷却剂丧失事故经由支持系统（即，接口系统中的冷却剂丧失事故）在安全壳外部¹⁸；
 - (ii) 产生相应安全壳旁路的电厂事件序列（例如，引发蒸汽发生器管破裂）；
 - (iii) 堆芯熔化的电厂事件序列，包括安全壳内有乏燃料水池且安全壳打开的电厂乏燃料水池序列¹⁹（例如处于关闭状态）。
- (e) 乏燃料水池中的燃料显著退化。

4.14. 第 4.13 段的分组与 SSG-53[6]第 3.67 段和 SSG-2 (Rev.1) [9]第 3.56 段建议一致，并强调了一些电厂事件序列的示例，供实际消除时考虑。

4.15. 分组的其他标准也是可能的。第 4.13(c) 段 (i) 和 (ii) 事故的后果事实上可以通过实施合理的技术手段来缓解。此外，第 4.13(d) 段的一些旁路序列可能涉及放射性物质的充分自然保留以实现安全目标。在这种情况下，对于不在实际消除考虑范围内的假想方案，应当提供缓解措施的有效性和适当可靠性的证据。为了便于所拟议的分组，应当分析每种类型的电厂事件序列，以确定电厂设计特有的、有可能导致密封功能失效的相关故障组合或相关实物现象。

4.16. 第 4.13 段和第 4.15 段所述的识别和分组应当酌情结合以下方法：

- (a) 在应急运行程序或严重事故管理准则中采取行动：现象学（自上而下）方法，在这种方法中，考虑在严重事故之前或过程中可能挑战密封功能的现象，以确定一个全面的电厂事件序列清单（即 4.13 段所列）。
- (b) 以序列为导向（自下而上）的方法，评审所有可能导致严重事故的电厂事件序列。对于每个序列评定对密封功能的任何挑战（这可能涉及评定安全壳上的负载以及通过泄漏和旁路的可能排放路线）。序列导向方法补充现象学方法与更广泛的筛选，以确定所有相关的电厂事件序列。

¹⁸ 由于安全壳的功能可能会受到始发事件的危害，必须对任何燃料严重退化的升级进行分析，并在相关情况下考虑实际消除。

¹⁹ 在许多轻水堆设计中，用于设备舱口的技术可能不够快而无法确保在放射性排放发生之前重新关闭和恢复安全壳的完整性。

4.17. 设计中应当考虑的维护相关因素包括：电厂所有可能的正常运行模式（如启动、功率运行、停堆、关闭和换料），包括运行模式具有开放性的遏制，在识别相关事件序列的过程中应当予以考虑。

4.18. 在确定识别相关核电厂事件序列的过程中，应当考虑所有贮存核燃料的核电厂位置和厂房（包括乏燃料水池）。

证实实际消除安全规定的识别和评定

4.19. 旨在以设计和运行特点的形式确定安全规定的评定应当考虑以下方面，这些安全规定可用于证实每个相关电厂事件序列的实际消除：

- (a) 核科学技术的最新水平；
- (b) 核电厂运行经验和事故经验；
- (c) 经证实的安全规定在技术和工业上的可行性；
- (d) 安全规定为处理不确定性和避免陡边效应提供足够裕度的能力；
- (e) 安全规定的潜在缺陷，这些缺陷可能只有在电厂投入运行后才会显现出来（例如，运行约束或虚假驱动）；
- (f) 可能对以下方面构成危害的严重事故现象动力学安全壳的完整性或其渗透性；
- (g) 减少进行场内行动或使用场外人员或设备需要的手段。

4.20. 确定安全规定需要从确定性、概率和工程判断的角度对所涉及的实物现象进行全面分析，可能有必要根据第 4.16 段所述的方法进一步完善事件序列的确定。

4.21. 设计人员应当建立一个决策过程，以确定合理可行的安全规定，从而实现实际消除。当考虑了安全规定的几个选项时，应当记录选择安全规定最终设计的正当性。

4.22. 为证实实际消除相关核电厂事件序列而确定的安全规定，应当循序渐进与适当的纵深防御级别或核电厂状态相联系，特别是需要中断事件序列以防止不可接受的放射性后果的级别。应当核实是否遵循了适当的工程设计规定（例如，针对内部和外部危害引起共因故障的故障安全驱动和保护）以及该纵深防御级别或电厂状态下安全规定的技术要求。这种核实的

目的是确保安全规定能够实现其安全功能，并有足够的裕度来考虑主要工况下的不确定性（例如，与严重事故相关的恶劣环境条件）。在应用工程设计规定和技术要求时，在相关的情况下，应当应用适当的试验，应当遵循运行程序，并且在运行中应当进行监视以及运行中的试验和视察。工程设计规定和技术要求应当应用于安全规定制定的所有步骤，从设计到运行，包括电厂的制造、建造或实施及其调试和定期试验。

4.23. 证实实际消除某些严重事故工况的安全规定可包括设计规定和运行规定的需要，因此它们可涉及运行人员的行动（例如，打开一回路减压阀以防止高压堆芯熔化工况）。运行人员必要行动的数量应当保持在较低水平，当不可避免时，人因评定应当成为支持任何运行人员的行动高可靠性主张的正当性的一部分。人因评定应当解决以下问题：

- (a) 从控制室或本地提供给运行人员执行行动的信息的可用性，执行行动的程序或导则的质量，以及运行人员的培训。
- (b) 执行行动的环境（例如进入局部区域、要装卸的部件、部件位置的识别、环境条件）。如果期望在恶劣的环境条件下采取本地行动，这可能会降低实际消除示范的可靠性。
- (c) 执行行动的时间表，包括实现预期成果的足够裕度。

4.24. 一些声称有助于实际消除某些电厂事件序列的安全规定可能容易受到事故发生前可能发生的人为错误的影响。这种人为错误可能会引入潜在的风险，当在事件或事故中调用系统或部件时，这些风险可能会阻止系统或部件的成功运行。在这种情况下，用于执行运行的系统或部件应当遵守相关的运行规定（例如，定期试验、运行中视察和监视、维护后的鉴定试验和定期系统校准检查），以限制此类人为错误的风险。

4.25. SSR-2/1（Rev.1）[1]第 5.21A 段指出：

“电厂设计还必须留有足够的裕度，以保护最终必要的物项，防止早期放射性排放或在自然灾害水平超过根据场址危害评价推导的设计考虑的水平时发生大量放射性排放。”

因此，证实实际消除的某些安全规定应当设计成以适当的裕度承受相关的内部和外部危害（即事故工况引起的或可能同时发生的危害）。

4.26. 如果证实实际消除的安全规定依赖于支持功能，则相关支持系统的设计都应当符合必要的标准，以确保其具有与安全规定相同的可靠性。设计应当结合使用冗余性、分离性、多样性和对危害的健稳性等安全设计原则，以实现相关安全功能的预期可靠性。或者，安全规定应当容忍支持功能的丧失。

证实实际消除

4.27. 应当通过包括工程判断、确定性分析和概率评定在内的安全评定来证实为证实实际消除而确定和纳入的安全规定的总体有效性。证实实际消除应当作为电厂设计和安全评定过程的一部分进行，包括制造、建造、调试和运行期间的必要视察和监视过程。

4.28. 为防止第 4.13 段发生电厂事件每组序列而制定的所有安全规定应当加以分析。所指出的任何现象或事故工况都不应当被忽视，因为它们发生的可能性很低。可信的研究结果应当用来支持安全规定有效性的主张。

4.29. 对于考虑实际消除的电厂事件每组序列应当进行评定，以证实相关安全规定的有效性。要么证实事件序列在实物上不可能出现（见第 4.33 段和第 4.34 段），要么以高置信度证实事件序列极不可能出现（见第 4.35—4.42 段）。实际消除一个事件序列的正当性最好依赖于它发生的实物不可能性的证实。如果这是不可能实现的，应当以高置信度证实这样的电厂事件序列是极不可能发生的。

4.30. 从第 4.13 段可以明显看出，要考虑实际消除的各种电厂事件序列本质上是非常不同的。因此，应当在个案基础上证实如何实际消除这些现象。

4.31. 在进行工程分析以及确定性安全分析和概率安全评定时，应当考虑到由于对某些实物现象，特别是严重事故现象的了解有限而产生的不确定性，以便确保结果具有高置信度。

4.32. 用于支持证实实际消除的计算机代码和计算应当得到核实和验证，所使用的模式应当反映对所涉及的实物现象的最佳理解，以便对电厂事件序列和所涉及的现象提供可接受的预测。SSG-2（Rev.1）[9]第 5 部分提供了关于使用计算机代码进行确定性安全分析的建议。

电厂事件序列的实际消除，因为它们在实物上是不可能的

4.33. 如果声称核电厂事件序列可以实际消除，因为它们在实物上是不可能的，则应当证实系统或反应堆类型的固有安全功能是这样的，即根据自然法则，核电厂事件序列不会发生，并且基本安全功能（见 SSR-2/1 (Rev.1) [1]要求 4）将始终得到满足。

4.34. 实际上，实际不可能的证实仅限于非常特定的情况（见附件 I）。实物上不可能的证实不能依赖于涉及活动部件或运行人员行动的措施。

实际消除被认为极不可能出现的电厂事件序列，具有很高的置信度

4.35. 某些电厂序列极不可能发生的证实应当依赖于工程方面的评定和确定性考虑，在可行的范围内由概率考虑支持，并考虑到由于对某些实物现象的有限知识而产生的不确定性。虽然可以设定概率目标（例如堆芯损坏或放射性排放的频率），但不能仅通过概率手段来证实实际消除。概率洞察力应当用于支持确定性和工程分析。仅满足概率目标并不能成为排除进一步确定性和工程分析以及可能实施额外的合理可行安全规定以降低风险的正当性。因此，发生堆芯损坏事故的可能性很低，这并不是不考虑进一步考虑保护安全壳免受此类事故产生的工况影响的正当性。相比之下，根据 SSR-2/1 (Rev.1) [1]第 5.30 段，要求在设计中假设堆芯熔化的设计扩展工况。

4.36. 在证实电厂事件序列可以实际消除时，应当酌情考虑以下几点：

- (a) 一套适当的安全规定，包括设备和组织规定；
- (b) 这些安全规定的健稳性（例如，足够的裕度、足够的可靠性、符合运行工况）；
- (c) (a) 和 (b) 点所述设备安全规定之间的独立性（即冗余性、实物分隔、多样性和功能独立性的适当结合）。

4.37. 在可行的范围内，应当使用现实的方法对严重事故进行确定性安全分析（见 SSG-2 (Rev.1) [9]表 1 选项 4）。由于现象的复杂性和实验数据的不足，不确定性的明确量化可能不切实际，因此应当进行敏感性分析，以证实结果的健稳性并支持安全分析的结论。敏感度分析也可用于确认边界分析中考虑的选定严重事故的充分性和代表性。

4.38. 当使用概率论证来支持某一特定核电厂事件序列已被实际消除的说法时，应当确保所考虑的所有不同事件序列的累积贡献不超过早期放射性排放或大量放射性排放的目标频率，如果设计人员或营运组织在核电厂安全评定中声称或监管机构已经确定了这样一个目标。

4.39. 对于预计应用，应当确认所使用的任何概率模式的有效性。支持这一点的假设应当有充分的正当性和验证。

4.40. 应当确定与证实实际消除使用的模式相关的不确定性的局限性，同时考虑到概率安全评定的局限性与概率建模以及支持确定性保守或最佳估计分析相关。

4.41. 如果实际消除的电厂事件序列是单一始发事件的结果，如大型保压部件在正常运行中的故障，证实实际消除应当依赖于在部件寿命的所有阶段（即其设计、制造、实施、调试和运行，包括定期试验和运行监督，如有）达到高质量水平的证据，以防止任何可能导致部件故障的缺陷的发生和传播。²⁰ 因此，应当考虑实际消除单一始发事件的发生（如大型保压部件的故障）和随之而来的事件（如反应堆堆芯的迅速损坏和随之而来的早期安全壳失效）。

4.42. 如果实际消除的电厂事件序列是一个事件序列的结果，在该事件序列中，密封功能退化到在堆芯熔化发生之前不可能充分保留放射性物质的程度，那么应当以高置信度证实堆芯熔化是可以防止的。这意味着，至少，一般的水平应当实施纵深防御（即针对预计运行事件、设计基准事故和无显著燃料退化的设计扩展工况），并在必要时进行增强，以防止堆芯熔化的设计扩展工况。

²⁰ 在一些国家，这种证实与其他概念联系在一起，如“故障的不可预测性”“破裂排除”“高完整性部件”和“不可破裂部件”，而不是与实际消除的概念联系在一起。

实际消除方法的文件

4.43. 核电厂的安全分析报告应当反映为证实实际消除了可能导致早期放射性排放或大量放射性排放的核电厂事件序列而采取的措施。安全分析报告应当直接或通过引用包括证实的所有要素，包括用于识别此类事件序列的方法、为确保此类事件序列出现的可能性已实际消除而实施的设计和运行安全规定，以及相应的分析。

5. 确保使用非永久性设备供电和冷却设计规定的实施

5.1. 作为 SSR-2/1 (Rev.1) [1]要求 14 的应用，安全重要物项的设计基准应当考虑它们需要运行或保持其完整性的最具限制条件。这包括内部和外部危害造成的情况。根据 SSR-2/1 (Rev.1) [1]要求 17，需要评定内部和外部危害以及相关危害组合的影响。对于外部危害，这是电厂场址评定的一部分（见原子能机构《安全标准丛书》第 SSR-1 号《核装置场址评价》[16]）。

5.2. 在有些情况下，一些外部自然灾害，如极端地震和海啸，已经超过了根据场址危害评价推导的设计中考虑的外部危害水平。SSR-2/1 (Rev.1) [1]第 5.21A 段指出，要求在设计中提供足够的裕度，以防止此类情况下的外部危害。

5.3. 为了提供额外的复原力，以抵御超过设计基准的事件序列，例如外部危害水平超过设计考虑的水平，从场址危害评价中推导，SSR-2/1 (Rev.1) [1]确立了几项要求，涉及在设计中纳入一些特点，以使非永久性设备能够安全使用用于以下目的²¹：

- (a) 恢复必要的电力供应（SSR-2/1 (Rev.1) [1]第 6.45A 段）；
- (b) 恢复安全壳散热的能力（SSR-2/1 (Rev.1) [1]第 6.28B 段）；
- (c) 确保足够的水库存，用于乏燃料的长期冷却和提供辐射屏蔽（SSR-2/1 (Rev.1) [1]第 6.68 段）。

²¹ SSR-2/1 (Rev.1) [1]这些要求是福岛第一核电站事故反馈的结果。因此，这些措施主要是在考虑到极端外部危害的情况下采取的。

5.4. 确保足够的水库存，用于乏燃料的长期冷却和提供辐射屏蔽（SSR-2/1（Rev.1）[1]第 6.68 段）。

5.5. 非永久性设备主要用于在事故工况的长期阶段和极少数可能影响现场安装的设计特点能力和可用性的事件后防止不可接受的放射性后果²²。使用非永久性设备的目的是恢复已经丧失的安全功能，但其使用不应当成为应对短期设计基准事故或设计扩展工况的常规手段（另见 SSG-2（Rev.1）[9]第 7.51 段和 7.64 段）。

5.6. 为了满足 SSR-2/1（Rev.1）[1]规定的要求（另见第 5.2 段和 5.3 段），应当考虑超过设计考虑的危害水平（即从场址危害评价中推导的危害水平），并评定其后果，作为纵深防御方法的一部分。对于自然外部危害，并不总是能够对某一危害水平的发生频率有足够的信心来定义设计基准水平。在这种情况下，不应当试图将水平与频率联系起来，而应当通过增加足够的裕度来定义超过设计考虑水平的自然灾害级别，这是从场址危害评价中推导的。应根据非永久性设备的潜在使用情况（例如部署的应对时间）评定结构、系统和部件因这些水平产生的负载参数而产生的行为。

5.7. 应当进行评定，以证实电厂能够应当对严重程度超过设计考虑水平的外部危害，这种危害是根据对场址危害评价推导的，基于以下两方面：

- (a) 对达到安全状态所必需的结构、系统和部件的适当设计裕度进行分析，并与由此产生的结果作对比可能存在的更高负载；
- (b) 分析在危害的主要影响过去后使用非永久性设备恢复必要的安全功能的情况。

5.8. 对于每一个涉及外部危害水平超过设计考虑水平的相关假想方案，从场址危害评价中推导，评定应当确定电厂响应能力的限制，并应当制定应对这些限制的策略。评价还应当确定将用于恢复安全功能以及达到和保持安全状态的各种应对措施、事故管理措施和设备（即贮存在场内或场外的固定或非永久性设备）。评价应当包括以下内容：

- (a) 对一组对安全具有重要意义的相关物项进行稳健性分析，以估计这些物项能够承受超过设计中考虑的危害水平的程度；

²² SSG-54[15]提供了与非永久性设备相关的进一步考虑。

- (b) 评定核电厂在何种程度上能够承受安全功能的丧失，而不会对公众和环境造成不可接受的放射性后果；
- (c) 限制和缓解可能导致相关安全功能丧失的假想方案后果的应对策略；
- (d) 对必要资源（即人力资源、设备、后勤和通信）的估计，以确认应对策略的可行性；
- (e) 证实在安全功能丧失之前的可用时间为执行恢复安全功能的所有必要行动所需的时间提供了足够的裕度。

5.9. 非永久性设备使用的某些方面和相关的安全评定在设计阶段无法得到充分详细的考虑则应当在调试和运行阶段考虑。然而，在新的核电厂设计阶段，或在适用的情况下，在按照早期标准设计的核电厂实施改造期间，应当考虑使用非永久性设备确保运行人员辐射防护的特定规定。

5.10. 评价应当考虑同一场址的多机组可能同时受到外部危害水平的影响，这种影响水平超过了根据场址危害评价推导的设计考虑水平，包括地震等自然外部危害。该评价应当用于确定所需非永久性设备的数量。

5.11. 对于超设计考虑水平的自然外部危害，与部署、安装和使用非永久性设备相关的电厂响应和应对策略应当在现实方法的基础上进行评定，并应当在相关情况下（例如，在陡边效应的情况下）通过敏感性分析进行补充，其中建模中的假设或重要的运行人员行动被识别为策略可信度的基本因素。

5.12. 应当确定应对策略，并根据第 5.8 段规定和设计与部署、安装和使用非永久性设备相关的应对措施，同时考虑到可能的情况。

5.13. 为了使应对策略更加可靠，应当在固定设备和非永久性设备之间实现充分的平衡。这种平衡应当根据每种应对策略需要实施的时间期限（“应对时间”）、安装非永久性设备所需的时间、为不同目的使用设备的灵活性、人的可靠性、人力资源的可用性以及整个应对策略所需的运行人员行动总数来确定。对于短期行动的实施，应当优先使用固定设备。

5.14. 非永久性设备的使用应当使设备安装和投入使用所需的时间少于规定的应对时间，并为时间敏感的运行人员行动留出特定的裕度。在陡边效应发生之前，应当为实施运行人员行动建立适当的时间裕度。在可能的情况下，应当根据演习期间记录的时间或验证运行人员行动的其他方法推导该时间段。交付和运行的能力还应当展示在现场不利条件下准时使用的非永久性设备，特别是在现场内外极端危害可能导致基础设施和道路严重退化的事件中。应当考虑将非永久性设备存放在远离设备的地方，以防出现极端危害。

5.15. 非永久性设备的安装和使用应当记录在案，并应当定期进行全面的培训、试验和演习，以保持运行人员熟练使用设备和相关程序。在可行的范围内，演习应当考虑到真正的紧急情况。

5.16. 一旦确定并验证了应对策略，就应当建立并记录对运行人员的导则以及策略的技术基础（例如，在应急运行程序或严重事故管理导则中）。

5.17. 为确保应对策略的成功和可靠性，应当特定规定必要应对措施的性能标准，并应当根据适当标准设计设备，并在相关情况下对设备进行鉴定，以确保其在极端外部危害或其他极端工况造成的工况期间和之后发挥作用。

5.18. 应对策略和应对规定的适当性，在外部危害超过设计考虑水平造成的环境条件下实施这些策略和规定的可行性以及事故的放射性后果都应当得到评价。

参 考 文 献

- [1] 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 (Rev.1) 号，国际原子能机构，维也纳（2016 年）。
- [2] 国际原子能机构《核安全与安保术语：用于核安全、核安保、辐射防护、应急准备与响应》（2022 年暂定版），国际原子能机构，维也纳（2022 年），<https://doi.org/10.61092/iaea.rrxi-t56z>。
- [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 (Rev.1) 号，国际原子能机构，维也纳（2016 年）。
- [4] 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），<https://doi.org/10.61092/iaea.hmxn-vw0a>。
- [5] 国际原子能机构《核电厂反应堆冷却剂系统和相关系统的设计》，国际原子能机构《安全标准丛书》第 SSG-56 号，国际原子能机构，维也纳（2020 年）。
- [6] 国际原子能机构《核电厂反应堆安全壳和相关系统的设计》，国际原子能机构《安全标准丛书》第 SSG-53 号，国际原子能机构，维也纳（2019 年）。
- [7] 国际原子能机构《核电厂电力系统的设计》，国际原子能机构《安全标准丛书》第 SSG-34 号，国际原子能机构，维也纳（2016 年）。
- [8] 国际原子能机构《核电厂仪器仪表和控制系统的设计》，国际原子能机构《安全标准丛书》第 SSG-39 号，国际原子能机构，维也纳（2016 年）。
- [9] 国际原子能机构《核电厂确定性安全分析》，国际原子能机构《安全标准丛书》第 SSG-2 (Rev.1) 号，国际原子能机构，维也纳（2019 年）。

- [10] 国际原子能机构《制定和实施核电厂一级概率安全评定》，国际原子能机构《安全标准丛书》第 SSG-3 (Rev.1) 号，国际原子能机构，维也纳（准备中）。
- [11] 国际原子能机构《制定和实施核电厂二级概率安全评定》，国际原子能机构《安全标准丛书》第 SSG-4 号，国际原子能机构，维也纳（2010 年）。（修订版准备中）
- [12] 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、国际刑警组织、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）。
- [13] 国际原子能机构《核电厂的辐射防护设计》，国际原子能机构《安全标准丛书》第 SSG-90 号，国际原子能机构，维也纳（准备中）。
- [14] 国际原子能机构、联合国环境规划署，《公众和环境的辐射防护》，国际原子能机构《安全标准丛书》第 GSG-8 号，国际原子能机构，维也纳（2018 年）。
- [15] 国际原子能机构《核电厂事故管理计划》，国际原子能机构《安全标准丛书》第 SSG-54 号，国际原子能机构，维也纳（2019 年）。
- [16] 国际原子能机构《核装置场址评价》，国际原子能机构《安全标准丛书》第 SSR-1 号，国际原子能机构，维也纳（2019 年）。

附件 I

实际消除的案例

I-1. 本附件说明了实际消除的可能示例。需要指出的是，示例清单和相关内容因会员国而异。

反应堆冷却剂系统中一个大型部件的故障

I-2. 反应堆冷却剂系统中单一大型部件的突然机械故障可能引发反应堆冷却在短时间内丧失的事件，压力波或飞射物将损坏安全壳边界。纵深防御的安全规定在这种情况下不会有效，可能会出现早期放射性排放或大量放射性排放。这是一种非常特殊类型的始发事件，安全系统和安全特点不是为了缓解这种事件而设计的，因此需要非常有把握地证实这种始发事件发生的可能性非常低，以至于可以排除（即实际消除）在考虑范围之外。这对反应堆容器尤其重要，因为在反应堆容器中，破裂将会消除保持和冷却堆芯的能力。此外，需要证实稳压器或蒸汽发生器壳体故障的可能性极低，或者需要证实稳压器或蒸汽发生器壳体的故障不会导致安全壳不可接受的后果。

I-3. 安全论证需要特别健稳，相应的评定要求适当，以便能够对反应堆冷却剂系统中每个大型部件的以下关键方面作出工程判断：

- (a) 需要选择最合适的材料组成。
- (b) 金属部件或结构需要尽可能无缺陷。
- (c) 金属部件或结构需要容许缺陷。
- (d) 需要知道缺陷生长的机制。
- (e) 需要规定设计规定和适当的运行实践，以尽量减少一回路的疲劳、应力腐蚀、脆化、加压热冲击和过压。
- (f) 在加压运行期间需要持续的泄漏检测能力。
- (g) 有效的在役检查和监视以及化学控制在设备的制造、建造、调试和运行期间，需要制定计划，以检测任何缺陷或退化机制，并确保设备特性在电厂的整个生命周期内得到保护。

I-4. 此外，需要提供证据来证实反应堆冷却剂系统的大型部件将在最苛刻的情况下保持必要的完整性。

I-5. 有几套完善的技术标准可用于确保大型压力容器的可靠性，并且实际消除压力容器故障的证实必须基于这些技术标准的严格应用。这种技术标准还提供了在容器寿命期间核实压力容器状态的说明。

I-6. 因此，实际消除大型部件的故障是通过第 1 级纵深防御来实现的，而不依赖于后续的纵深防御。

I-7. 概率破裂力学评定可以补充低故障可能性的高置信度证明这是一种广泛认可和常用的技术。证实实际消除中的概率评定，尤其是在这种情况下，不限于使用布尔可靠性模式（如故障树、事件树）或从观察到的灾难性故障的统计分析中推导的故障率。概率破裂力学评定涉及材料破裂韧性和焊接残留应力等方面，进而考虑确定性分析、工程判断和监控值的测量。

轻水堆快速反应性插入事故

I-8. 快速反应性事故可能非常激烈，有可能摧毁燃料、燃料包壳和其他屏障。在切实可行的情况下，应当确保在第 1 级纵深防御中预防此类事故通过反应堆冷却剂系统和堆芯的适当设计，或者通过提供两种不同的、独立的关闭手段以达到第 3 级纵深防御。

I-9. 第 1 级纵深防御可由反应堆堆芯的核特征提供（如轻水堆中的负反应性系数），在反应堆功率、中子吸收剂浓度、冷却剂压力和温度的所有可能组合下，在任何干扰期间抑制反应堆功率的任何增加，并消除任何不受控制的反应性偏移。因此，这是一个通过事件序列的实物不可能性来证实实际消除的示例。

I-10. 不受控制的反应性偏移可能是由冷的或欠硼的水段塞突然插入反应堆堆芯引起的。根据设计，通过证实只能注入有限体积的未硼化水，不允许这种影响发生，事故可以被认为消除的。通过证实反应堆功率和冷却剂压力及堆芯循环温度的可能组合存在足够的负反应系数，也可以认为事故已经消除。然而，冷却剂特性突然变化的所有潜在风险都需要通过设计规定来识别和预防。在这种情况下，证实实际消除是因为事件序列被认为在实物上不可能发生。

I-11. 因此，证实实际消除主要依赖于通过总体反应性系数较小或为负的堆芯设计不可能发生反应性偏移，并得到其他设计措施的支持，以避免或限制反应性偏移，这些措施可以根据需要进行确定性和概率评定，以证实这些情况极不可能发生。

I-12. 然而，如果在严重事故中达到临界状态，可能会出现更复杂的情况。这一直是反应堆中特定堆芯熔化假想方案的关注专题，在这种情况下，控制棒材料的熔点和共晶形成温度低于燃料棒。如果在控制棒向下移动但燃料棒仍在其原始位置的情况下，用未硼化的水重新填充反应堆容器，可能会发生潜在的危害情况。这可能导致燃料重新临界，可能导致持续或中间产生额外的热量，这取决于水的存在。这也是通过考虑设计规定和严重事故管理特点来分析的一个方面，以便能够证实电厂序列已经实际消除，因为它被认为是具有很高的置信度且极不可能发生的。

直接安全壳加热

I-13. 在反应堆压力容器中，在高压下的堆芯熔化会导致熔化堆芯材料剧烈排放到安全壳大气中，这将导致由热熔和放热化学反应产生的直接安全壳加热。因此，当发现熔化不可避免时，涉及高压堆芯熔化的电厂事件序列实际上需要通过设计规定来消除，以降低反应堆冷却剂系统的压力，从而具有很高的置信度认为这些工况极不可能发生。

I-14. 相比之下，在加压重水堆中，由于高压下熔化堆芯的喷射而导致的直接安全壳加热被实际消除了，因为压力管在高燃料温度下会迅速失效。这将在堆芯熔化发生之前降低一回路系统的压力。这是一个实际消除事件序列的示例，因为它在实物上是不可能的。

I-15. 任何高压堆芯熔化情况显然都是由少量冷却剂泄漏或冷却剂沸腾以及通过安全阀或泄压阀排放蒸汽引起的。对于这种情况，需要有适当的设计规定，以很高的置信度确保这种小的冷却剂泄漏或冷却剂沸腾将以高可靠性导致低压堆芯熔化序列，从而可以实际消除高压堆芯熔化工况。减压需要使得在从反应堆容器中排出任何熔化堆芯熔化物之前可以达到非常低的压力。此外，重要的是，来自减压的动态负载不会对安全壳的完整性构成风险。设计规定需要到位，以确保很高的置信度地不会发生任何高压堆芯熔化情况。

I-16. 现有电厂安装了专用减压系统并为新的电厂设计。在压水堆中，这种系统基于简单而健稳的设备和运行人员的直接动作，这消除了错误的自动减压风险，但在需要时提供了足够的时间来行动。在沸水堆中，现有蒸汽排放系统通常提供减压设备，可能对阀门控制进行一些改造，以确保在非常低的压力下可靠的阀门开启和开启阀门位置。

I-17. 确定性安全分析对于证实减压系统在防止直接安全壳加热方面的有效性是必要的。传统的概率安全评定技术足以证实减压系统的高可靠性，包括由运行人员启动系统。这样，根据对特定设计规定的确定性和概率综合评定，可以很高的置信度地证实直接安全壳加热极不可能发生。

大蒸汽爆炸

I-18. 反应堆堆芯融化与水的相互作用，称为燃料—冷却剂相互作用，是一个复杂的技术问题，涉及许多热力学和化学现象。燃料—冷却剂相互作用可能发生在容器内，在退化堆芯的淹没过程中，或者如果融化堆芯重新定位到充满水的下压头中。如果在容器故障后融化堆芯碎片被喷射到充满水的反应堆堆腔中，这种相互作用也可能发生在容器外。每种情况都可能导致高能燃料—冷却剂相互作用，通常称为“蒸汽爆炸”，这对反应堆容器和/或安全壳的完整性构成了潜在的严重挑战。

I-19. 引发蒸汽爆炸的条件和各种情况下的爆炸能量已在反应堆安全研究计划中得到广泛研究。对于融化堆芯可能落入水中的所有堆芯融化情况，蒸汽爆炸的风险不能完全消除。

I-20. 为了实际消除可能损坏安全壳完整性的蒸汽爆炸，优选的方法是避免所有可能的事故假想方案都将融化堆芯放入水中。这种方法用于一些压水堆，其中融化堆芯外部冷却的可靠性已经得到证明以及一些具有单独堆芯收集器的新的反应堆。在一些现有沸水堆和一些新设计的沸水堆中，在所有严重事故工况下，融化堆芯将落入反应堆容器下方的水池中，并在水池中固化和冷却。在所有融化堆芯落入水中的情况下，需要根据各自假想方案中涉及的实物现象进行论证，证实由于事件序列的实物不可能性，破坏安全壳完整性的蒸汽爆炸风险已经实际消除。

可燃气体的爆炸：氢气和一氧化碳

I-21. 氢气燃烧是一种非常高能的现象，涉及足够量氢气的快速燃烧反应（爆轰）会对安全壳的完整性造成重大威胁。所有核电厂都需要专门的方法来防止氢气的产生及其在临界浓度下的积聚并消除氢气爆炸，尽管不同的电厂设计优选不同的方法。

I-22. 在相对较小的沸水堆安全壳中，防止氢气产生和积聚的主要手段是在功率运行期间用惰性氮气填充安全壳。在大型压水堆安全壳中，目前的实践是使用非能动催化重组器或其他设备来控制氧气和氢气的复合速率，以防止氢气爆炸。

I-23. 还需要通过分析和试验来确保和确认安全壳内气体和蒸汽的循环为氢气复合提供了适当的条件，并消除了过量的局部氢气浓度，同时考虑到如果提供惰化作用的蒸汽被冷凝，氢气爆炸的风险会增加。

I-24. 氢气燃烧的后果将取决于可想象的最高速率和安全壳内产生的氢气总量。目前安装在核电厂中的一些堆芯收集器可以显著减少甚至消除事故中熔化堆芯落入收集器时容器外氢气的产生，这也可以显著减少安全壳内产生的氢气总量。

I-25. 特别是需要评定防止氢气爆炸的设计规定，以证实实际消除了这一现象。该评定还包括考虑 (i) 在严重事故期间允许有限数量的氢气产生材料的适当选择；以及 (ii) 氢气在安全壳内的传播和混合。

I-26. 如果从反应堆容器中排出的熔化堆芯与混凝土结构相互作用，在严重事故中会产生一氧化碳。一氧化碳产生的数量和时间取决于特定的堆芯熔化情况、混凝土类型和几何因素。一氧化碳和空气的混合物也可能是爆炸性的，尽管这种化学反应的能量不如氢气燃烧，燃烧速度也较低。因此，一氧化碳对安全壳完整性风险的贡献通常较少受到关注。然而，一氧化碳的存在增加了安全壳中可燃气体的存量，也影响了氢气的燃烧限值和燃烧速度。因此，需要考虑一氧化碳的影响，以证实氢气燃烧的实际消除。将一氧化碳的影响降至最低的设计规定是使用石灰石含量低的混凝土。

安全壳排热长期丧失

I-27. 在堆芯衰变热不能通过传热系统转移到安全壳外部并进一步转移到最终散热器的情况下，或者在堆芯熔化并在安全壳内部产生蒸汽的严重事故中，冷却安全壳大气是防止其过压的优选方法。

I-28. 现有电厂和新的电厂设计中都有几个独立于安全系统的专用健稳安全壳冷却系统的示例，证实这些系统可能能够支持实际消除过压安全壳破裂的。

I-29. 安全壳冷却的一种替代方法是通过排气消除安全壳过压。这是必要的，特别是在一些沸水堆中，在这些反应堆中，安全壳的尺寸很小，并且在设计基准事故和堆芯熔化的设计扩展工况下可能需要压力限制。现有设备中的通风系统防止过压，代价是通风中涉及的一些放射性排放，在通风被过滤的情况下也是如此。然而，如果考虑到风险水平和对该策略的去污因素的适当评定，这些策略在技术上是正当的，则可能是严重事故管理的可接受策略。

I-30. 安全壳排气避免了因过压而对安全壳完整性造成的风险，但从长远来看，稳定堆芯和冷却安全壳仍然是必要的。

I-31. 安全论证需要基于设计中实施的应对严重事故现象的特定措施的能力和可靠性。二级概率安全评定可用于证实可能导致大量放射性排放的电厂事件序列的概率非常低（即实际消除安全壳热量排出的长期丧失，因为它被认为是极不可能发生的，具有很高的置信度）。

通过与熔化堆芯相互作用实现安全壳贯穿

I-32. 在堆芯熔化贯穿反应堆容器的严重事故中，如果熔化堆芯没有得到充分冷却，安全壳的完整性可能会被破坏。此外，堆芯碎片和混凝土之间的相互作用会产生大量额外的可燃气体、氢气和一氧化碳，以及其他不凝气体，这也可能导致安全壳最终过压失效。

I-33. 在几个国家开展的这一领域广泛的严重事故研究方案中，以及在国际合作下，已经开发并核对了替代手段。建议的方法包括：

- (a) 通过从外部冷却容器，将熔化堆芯保持在反应堆容器内；
- (b) 安装一个专用系统或设备，以便在熔化堆芯穿透反应堆容器壁后立即收集和冷却熔化堆芯。

I-34. 在这两种方法中，熔化堆芯的冷却在安全壳内产生蒸汽，并且还需要提供从安全壳中散热的特点，这些特点在可行的范围内独立于在更频繁的事故中使用的特点。

I-35. 虽然概率安全评定可以在评定建立外部反应堆容器冷却或堆芯收集器冷却（如果提供的话）的可靠性方面发挥作用，但通过安全壳边界实际消除熔化物的证实在很大程度上依赖于对以下因素的确定性分析设计规定，以证实这种安全壳贯穿可以被认为是极不可能出现的，具有高度的确定性。

安全壳旁路严重事故

I-36. 安全壳旁路可以以不同的方式发生，例如通过连接到反应堆冷却剂系统的回路离开安全壳，或者由于蒸汽发生器管有缺陷（对于压水堆）。将安全壳大气连接到外部的非隔离贯穿件的严重事故序列以及安全壳打开的电厂关闭期间的严重事故序列也需要被视为安全壳旁路假想方案。离开安全壳并连接到一回路的管线故障，包括蒸汽发生器管破裂，同时也是事故引发因素，而其他开口贯穿件仅构成事故工况下的排放路径。然而，所有这些电厂事件序列须要通过设计规定实际消除，例如足够的管道设计压力和隔离机制。

I-37. 消除旁路序列的安全证实包括对所有潜在安全壳旁路序列的系统化评审，并涵盖所有安全壳贯穿件。

I-38. 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》[I-1]要求 56 规定了各种安全壳贯穿件的最低隔离要求。该要求解决了密封性和泄漏检测、冗余性和自动驱动等方面的问题。对于反应堆冷却剂系统中的接口故障也给出了特定规定。国家法规更详细地阐述了接口系统中安全壳隔离和防止安全壳旁路或冷却丧失事故的适用规定。

I-39. 根据设计要求或特定国家法规的实施以及电厂的运行视察和监视实践，分析必须评定旁路机制的频率。这种分析虽然具有概率性质，但需要在概率计算中结合工程判断和确定性分析的各个方面，并始终基于设计的冗余性和健稳性、相关设计规定的应用（如故障安全驱动）以及相关的视察规定和运行实践，就像在以前的案例中所做的那样。而安全壳贯穿件或蒸汽发生器的隔离分析是可行的对于传统的故障树和事件树分析，在适当考虑电源故障、隔离信号和运行人员操作的情况下，其他分析方面可能涉及使用其他概率方法以及确定性方法和工程判断，以证实安全壳旁路的实际消除。这将导致对与每次贯穿件相关的旁路机制进行可防御的低频估计。此外，基于常规概率评定的旁路路径隔离设计规定的可靠性将补充具有安全壳旁路的电厂事件序列已被证实实际消除。

乏燃料水池中显著燃料退化

I-40. 乏燃料贮存设施的设计需要确保实际消除可能导致早期放射性排放或大量放射性排放到环境中的电厂事件序列。为此，有必要确保贮存在燃料水池中的乏燃料始终被足够的水层覆盖，这涉及以下内容：

- (a) 提供一个旨在防止所有可能发生的可能损坏其完整性的内部和外部危害。
- (b) 避免将水从水池中吸出。
- (c) 为水池冷却提供足够可靠的手段，以消除长期丧失冷却功能的可能性（即在水烧开所需的时间内）。一个示例是冗余性、多样性和独立性的应用（见原子能机构《安全标准丛书》第 SSG-63 号《核电厂燃料装卸与贮存系统的设计》[I-2]）第 3.7 段。
- (d) 为水池水位监控提供可靠的仪器仪表。
- (e) 提供适当、可靠的手段，以补偿水库存的任何损失。

I-41. 机械燃料故障的风险需要通过以下手段消除：

- (a) 确保避免重型起重机（如运输桶）在贮存在燃料水池中的乏燃料上方移动的设计；
- (b) 消除重物跌落在燃料顶部可能性的结构。

I-42. 在乏燃料水池位于安全壳外部的设计中，燃料的暴露会导致燃料损坏，并且无法防止大量放射性物质排放。排空氢气的方法将防止可能造成进一步损坏的爆炸，并防止燃料随后的重新充水和冷却。因此，有必要通过设计规定确保已经实际消除了乏燃料元件的暴露。

I-43. 在一些设计中，乏燃料水池位于安全壳内部。在这种情况下，即使乏燃料损坏不会直接导致大量放射性排放，但大量燃料元件产生的氢气量以及熔化燃料容易穿透池衬里而无法稳定池衬里，以及其他恶劣影响，最终可能导致大量放射性排放。因此，还必须通过设计规定确保，在这种情况下，乏燃料元件的暴露已经实际消除。

附件 I 参考文献

- [I-1] 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 (Rev.1) 号，国际原子能机构，维也纳（2016 年）。
- [I-2] 国际原子能机构《核电厂燃料装卸与贮存系统的设计》，国际原子能机构《安全标准丛书》第 SSR-63 号，国际原子能机构，维也纳（2020 年）。

附录 II

按早期标准核电厂中设计扩展工况和实际消除的设计概念的应用

II-1. 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》[II-1]第 1.3 段指出：

“将本安全要求出版物的所有要求必须用于在运或在建的核电厂可能并不可行。此外，修改已经得到监管机构批准的设计可能不可行。对于这种设计的安全分析，预期将与现行标准进行比较，例如作为电厂定期安全评审的一部分，以确定是否可以通过合理可行的安全改进来进一步提高电厂的安全运行。”

这意味着 (i) 现有核电厂适应其当前设计基准中未考虑事故工况的能力；以及 (ii) 实际消除可能导致早期放射性排放或大量放射性排放的核电厂事件序列，需要作为定期安全评审过程的一部分进行评定，目的是在合理可行的情况下进一步提高安全水平。

II-2. 设计、扩展工况和实际消除可能导致早期放射性排放或大量放射性排放的电厂事件序列概念并不新鲜。事实上，实际消除的概念已经在 2004 年原子能机构《核电厂反应堆安全壳系统的设计》¹ 提出，这两个概念可能已经部分应用于一些现有核电厂设计中，尽管不一定是以系统的方式。随着时间的推移，许多核电厂都引入了应对断电或无应急停堆预期瞬态等工况的设计特点。一些可能导致早期放射性排放或大量放射性排放的事件序列也已经在许多设计中得到解决，尽管还没有进行实际消除这种电厂事件序列的特定证实。

II-3. 关于实际消除，可能已经采取了一些措施，例如，防止反应堆压力容器破裂、快速反应性插入事故或乏燃料水池中燃料严重退化。然而，现

¹ 见国际原子能机构《核电厂反应堆安全壳系统的设计》，国际原子能机构《安全标准丛书》第 NS-G-1.10 号，国际原子能机构，维也纳（2004 年）第 6.5 段，已被国际原子能机构《核电厂反应堆安全壳和相关系统的设计》，国际原子能机构《安全标准丛书》第 SSG-53 号，国际原子能机构，维也纳（2019 年）[III-2] 替代。

有安全规定足以要求实际消除此类电厂事件序列的证实可能没有按照 SSR-2/1 (Rev.1) [II-1]要求的方式和本“安全导则”的建议进行。

II-4. 然而，通常被认为是新的核电厂设计扩展工况的事故工况（例如，电厂断电、无应急停堆的预期瞬态）只能被认为是现有核电厂设计扩展工况，前提是在现有核电厂的原始设计中引入了安全特点以缓解这种工况的后果。对于电厂断电的情况，能够在足够的时间内及时向基荷供电直到外部或应急电源恢复的备用电源将是原始设计安全特点的一个示例。同样，无应急停堆的预期瞬态，在控制棒插入失败的情况下，能够使反应堆次临界的额外设计特点需要包括在原始设计中。如果原始设计中没有这些额外的设计特点，这些事故工况将需要被认为超电厂设计基准。

II-5. 一般来说，在定期安全评审或电厂安全再评定期间，或作为延长寿命或类似过程请求的一部分，应考虑与设计扩展工况和实际消除相关的合理安全改进的可行性。然而，在安装与新的核电厂设计中通常实施的相同类型的设计特点时可能会有约束，特别是对于堆芯熔化的设计扩展工况，例如在压水堆设计中实施容器外熔化物保留或容器内堆芯冷却策略。在同样的情况下，在确保与不同纵深防御级别相关的安全规定的独立性方面可能存在约束。

II-6. 设计扩展工况的安全规定，以及实际消除可能导致早期事故的电厂事件序列的设计特点放射性排放或大量放射性排放在与电厂系统设计相关的几个安全导则中有所涉及，包括 SSG-53[II-2]和原子能机构《安全标准丛书》第 SSG-56 号《核电厂反应堆冷却剂系统和相关系统的设计》[II-3]，第 SSG-34 号《核电厂电力的系统设计》[II-4]和第 SSG-39 号《核电厂仪器仪表和控制系统的设计》[II-5]。SSG-53[II-2]包含了堆芯熔化设计扩展工况的大部分设计特点，并解决了实际消除时要考虑的电厂事件序列。SSG-53[II-2]还包含一个与按照早期标准设计的核电厂相关的附录，该附录提供了与这些方面相关的电厂设计升级建议。

II-7. 现有电厂的安全系统是为设计基准事故而设计的，在设计中没有考虑预防和缓解更严重的事故。然而，设计中最初遵循的保守确定性方法可能会导致承受一些比现有电厂设计基准中最初包含的情况更严重情况的能力。如本“安全导则”第 3.22 段关于在无显著燃料退化的情况下设计扩展工况的规定中，对于假想始发事件比设计基准事故所考虑的事件频率低，

如果使用最佳估计分析和不太保守的假设，可以接受证实一些安全系统能够并有资格缓解此类事件的后果。对于现有核电厂，这有可能证实缓解设计中最初没有假想设计扩展工况的能力，例如蒸汽发生器管道的多次破裂。根据 SSR-2/1 (Rev.1) [II-1]第 5.27 段，现有核电厂还可以扩展安全系统的能力，使其能够缓解一些设计扩展工况。

II-8. 如第 5 部分所述，外部事件的规模超过了从场址危害评价中推导的原始设计基准应当予以考虑。虽然对于新的核电厂，设计扩展工况的缓解通常期望通过永久性设计特点来实现，并且非永久性设备的使用仅用于规模超过原始设计基准的极不可能外部事件，但对于现有核电厂，在某些情况下，使用具有足够连接特点的非永久性设备可能是唯一合理的改进。依靠非永久性设备可能是足够的，只要有正当性证实防止设备预期实现的安全功能丧失的应对时间足够长，可以在这些条件下连接设备并投入使用与事故相关。第 5 部分在这方面提出的建议是相关的。需要存储和保护非永久性设备，以确保其在必要时的可用性，同时考虑到外部事件（如洪水、道路损坏）可能导致的进入受限，并且需要核实其可运行性。

附件 II 参考文献

- [II-1] 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 (Rev.1) 号，国际原子能机构，维也纳（2016 年）。
- [II-2] 国际原子能机构《核电厂反应堆安全壳和相关系统的设计》，国际原子能机构《安全标准丛书》第 SSG-53 号，国际原子能机构，维也纳（2019 年）。
- [II-3] 国际原子能机构《核电厂反应堆冷却剂系统和相关系统的设计》，国际原子能机构《安全标准丛书》第 SSG-56 号，国际原子能机构，维也纳（2020 年）。
- [II-4] 国际原子能机构《核电厂电力系统的设计》，国际原子能机构《安全标准丛书》第 SSG-34 号，国际原子能机构，维也纳（2016 年）。
- [II-5] 国际原子能机构《核电厂仪器仪表和控制系统的设计》，国际原子能机构《安全标准丛书》第 SSG-39 号，国际原子能机构，维也纳（2016 年）。

定 义

实际消除

实际消除的概念适用于可能导致无法通过合理可行手段缓解的不可接受的后果（即早期放射性排放或大量放射性排放）的电厂事件序列。实际消除意味着须要证实这些电厂事件序列要么在实物上是不可能的，要么在高置信度的情况下，通过以设计和运行特点的形式实施安全规定，极不可能出现这种情况。

注：实际消除是设计安全的一般方法的一部分和补充充分落实纵深防御的概念。

参与起草和审订人员

Bernard, M.	法国电力公司
Buttery, N.	欧洲核装置安全标准
Courtin, E.	世界核能协会
Dakin, R.	英国核监管办公室
Delfini, G.	荷兰核安全与辐射防护管理局
Ermolaev, A.	俄罗斯联邦全俄核电厂运行科学研究所
Exley, R.	英国核监管办公室
Franovich, M.	美国核管制委员会
Garis, N.	瑞典辐射安全局
Gyepi-Garbrah, S.	加拿大核安全委员会
Hardwood, C.	加拿大核安全委员会
Ibrahim, M.A.	埃及核电厂管理局
Jansen, R.	荷兰核安全与辐射防护管理局
Järvinen, M.L.	芬兰辐射与核安全局
Kim, K.T.	韩国原子能研究所
Koski, S.	芬兰工业部
Kral, P.	捷克核研究所
Lignini, F.M.	世界核能协会
Luis Hernandez, J.	国际原子能机构
Müllner, N.A.	奥地利安全与风险科学研究所
Nakajima, T.	日本核监管局
Nünighoff, K.	德国装置与反应堆安全公司

Obenius Mowitz, A.	瑞典辐射安全局
Poulat, B.	顾问（法国）
Ranval, W.	欧洲核装置安全标准
Rodriguez Mate, C.	法国核安全局
Rogatov, D.	俄罗斯联邦核与辐射安全科学与工程中心
Schwarz, G.R.	顾问（加拿大）
Stoppa, G.	德国联邦环境、自然保护、核安全与消费者保护部
Tas, F.B.	土耳其核监管局
Titus, B.A	美国核管制委员会
Uhrik, P.	斯洛伐克核监管局
Virtanen, E.	芬兰辐射与核安全局
Wattelle, E.	法国辐射防护与核安全研究所
Wong, E.K.Y.	新加坡国家环境局
Yllera, J.	国际原子能机构

通过国际标准促进安全

ISBN 978-92-0-514224-1



9 789205 142241

国际原子能机构
维也纳