国际原子能机构安全标准

保 护 人 类 与 环 境

核电厂的确定性安全分析

特定安全导则

第 SSG-2 (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，国际原子能机构受权制定或采取旨在保护健康及尽量减少对生命与财产之危险的安全标准，并规定适用这些标准。

国际原子能机构借以制定标准的出版物以**国际原子能机构《安全标准丛书》**的形式印发。该丛书涵盖核安全、辐射安全、运输安全和废物安全。该丛书出版物的分类是**安全基本法则**、**安全要求**和**安全导则**。

有关国际原子能机构安全标准计划的资料可访问以下国际原子能机构因特网网站：

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

该网站提供已出版安全标准和安全标准草案的英文文本。以阿拉伯文、中文、法文、俄文和西班牙文印发的安全标准文本；国际原子能机构安全术语以及正在制订中的安全标准状况报告也在该网站提供使用。欲求进一步的信息，请与国际原子能机构联系（Vienna International Centre, PO Box 100, 1400 Vienna, Austria）。

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

相关出版物

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

核活动的安全报告以**《安全报告》**的形式印发，《安全报告》提供能够用以支持安全标准的实例和详细方法。

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

安保相关出版物以**国际原子能机构《核安保丛书》**的形式印发。

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

核电厂的确定性安全分析

国际原子能机构的成员国

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

国际原子能机构的《规约》于 1956 年 10 月 23 日经在纽约联合国总部举行的原子能机构《规约》会议核准，并于 1957 年 7 月 29 日生效。原子能机构总部设在维也纳，其主要目标是“加速和扩大原子能对全世界和平、健康及繁荣的贡献”。

国际原子能机构《安全标准丛书》第 SSG-2（Rev.1）号

核电厂的确定性安全分析

特定安全导则

国 际 原 子 能 机 构
2022 年 • 维也纳

版 权 说 明

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

国际原子能机构印刷
2022 年 11 月 · 奥地利

核电厂的确定性安全分析

国际原子能机构，奥地利，2022 年 11 月
STI/PUB/1851
ISBN 978-92-0-509322-2（简装书：碱性纸）
978-92-0-509422-9（pdf 格式）
ISSN 1020-5853

前　言

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

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

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

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

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

国际原子能机构安全标准

背景

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

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

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

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

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

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

原子能机构安全标准

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

为了确保保护人类和环境免受电离辐射的有害影响，原子能机构安全标准制定了基本安全原则、安全要求和安全措施，以控制对人类的辐射照射和放射性物质向环境的释放，限制可能导致核反应堆堆芯、核链式反应、辐

射源或任何其他辐射源失控的事件发生的可能性，并在发生这类事件时减轻其后果。这些标准适用于引起辐射危险的设施和活动，其中包括核装置、辐射和辐射源利用、放射性物质运输和放射性废物管理。

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

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

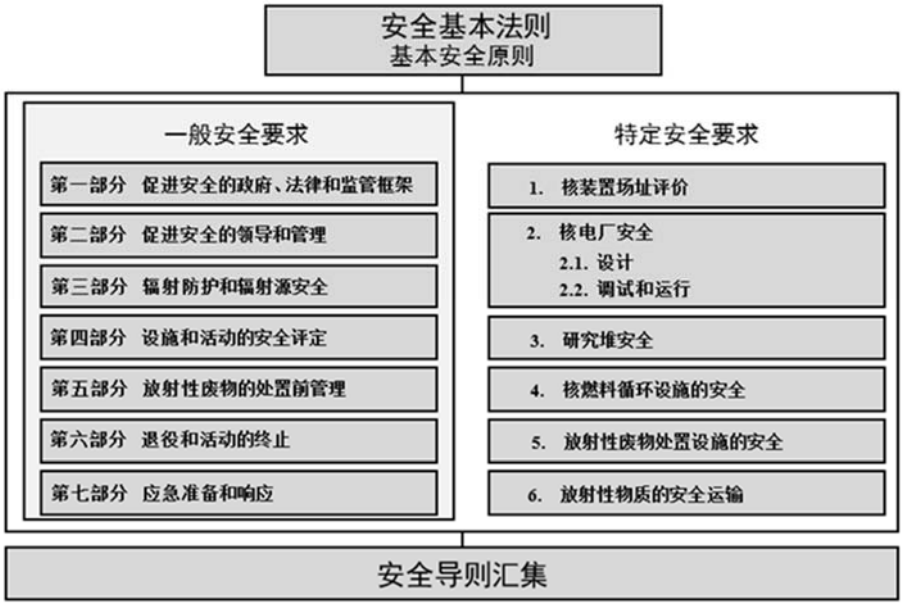

图 1. 国际原子能机构《安全标准丛书》的长期结构。

[1] 另见以原子能机构《核安保丛书》印发的出版物。

安全基本法则

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

安全要求

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

安全导则

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

原子能机构安全标准的适用

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

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

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

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

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

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

原子能机构安全标准的制定过程

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

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

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

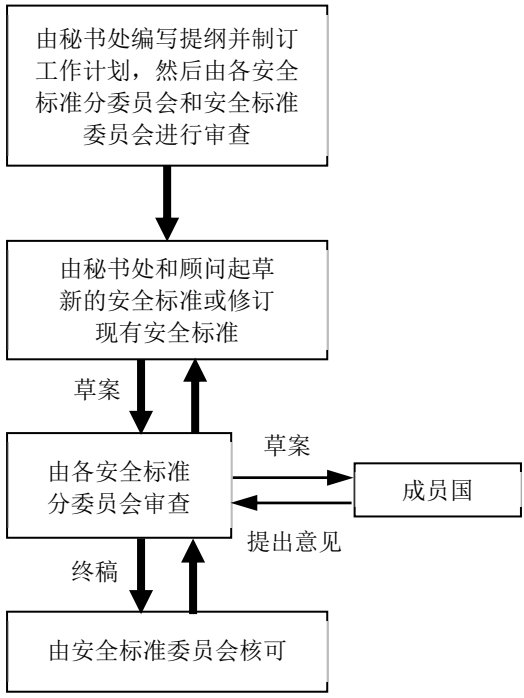

图 2. 制订新安全标准或修订现行标准的过程。

与其他国际组织的合作关系

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

文本的解释

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

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

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

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

目 录

1. 导言

背景

1.1. 根据原子能机构《安全标准丛书》第 SSR-2/1（Rev.1）号《核电厂安全：设计》[1]和第 GSR Part 4（Rev.1）号《设施和活动的安全评定》[2]中的要求，本“安全导则”就确定性安全分析的使用及其在核电厂中的应用提供建议和指导。

1.2. 当前，为确保核反应堆稳定和安全运行方面的开发工作与安全分析方面的进步密切相关。由 SSR-2/1（Rev.1）[1]和原子能机构《安全术语》[3]所界定的，针对正常运行、预计运行事件、设计基准事故和设计扩展工况，包括严重事故的确定性安全分析方法，是验证安全规定充分性的重要手段。

1.3. 本“安全导则”取代了 2009 年版的 SSG-2 [1]。纳入本“安全导则”的修改反映了确定性安全分析方法的最新成果，包括新核电厂设计的安全分析报告和对现有核电厂应用确定性安全分析的经验。为了反映从福岛第一核电厂事故中汲取的经验教训，原子能机构更新了相关“安全要求”出版物，为保持与这些相关“安全要求”出版物的一致性，本“安全导则”进行了相应的更新。

目的

1.4. 本“安全导则”的目的，就是为进行核电厂确定性安全分析及其应用时，向设计人员、营运组织、监管机构和技术支持组织提供建议和指导。导则还就确定性安全分析方法的使用在以下两个方面提出了建议：

(a) 证明或评定对监管要求的遵守情况；

(b) 识别可能改善安全和可靠性的改进项。

[1] 国际原子能机构《核电厂的确定性安全分析》，国际原子能机构《安全标准丛书》第 SSG-2 号，国际原子能机构，维也纳（2009 年）。

这些建议满足了 SSR-2/1（Rev.1）[1]和 GSR Part 4（Rev.1）[2]中规定的安全要求，并得到目前世界各地核电厂进行的确定性安全分析的实践和经验的支持。

范围

1.5. 本“安全导则”适用于核电厂。它着重执行确定性安全分析的方法，以实现满足安全要求的目的。这类分析主要是用于证明设计的安全功能可以充分履行，能确保放射性物质释放的屏障可以阻止放射性物质不受控制地释放到核电厂所在国家的环境中去，也可以用于证明运行限值和条件的有效性。另外，取决于不同电厂状态下屏障的状况，确定性安全分析方法还可以用于确定潜在释放的特性（源项）。

1.6. 本“安全导则”主要侧重于新核电厂设计安全的确定性安全分析，并在合理可行或可实现的范围内，也可适用于在营运组织评审现有核电厂安全评定时对现有核电厂的安全重新评价或重新评定。所提供的建议意在与 SSR-2/1（Rev.1）[1]第 1.3 段和第 1.6 段所述的适用范围保持一致，特别是针对水冷堆所做的确定性安全分析的经验。

1.7. 本“安全导则”提供的建议主要集中于确定性分析方法在设计中考虑的所有电厂状态应用的最佳实践，包括，从正常运行到预计运行事件和设计基准事故，再到设计扩展工况，以及严重事故。

1.8. 本“安全导则”主要论述的电厂系统（例如反应堆堆芯、反应堆冷却剂系统、安全壳、燃料贮存或其他含有放射性物质的系统）的人因失误和故障，它们可能影响安全功能的执行并因此导致防止放射性物质释放的物理屏障丧失。尽管在确定要分析的始发事件中包括了危害可能导致的电厂系统故障的影响和负荷，但就对危害本身的分析，无论是内部的还是外部的（自然的还是人为的），都不在本“安全导则”范围之内。

1.9. 本“安全导则”阐述了在设计或许可证申请过程中确定性安全分析方法的使用，即以充分的安全裕量展示对既定验收标准的遵从。

1.10. 本“安全导则”给出了应用确定性安全分析方法的可行的不同选项，即保守方法、不确定性量化条件下的最佳估算方法以及一种组合的方法。

1.11. 本“安全导则”集中于中子物理学、热工水力学、燃料（或压水式重水反应堆的燃料通道）和放射性分析。其他类型的分析，特别是结构和设备的结构分析，也是证明电厂安全的重要手段。然而，由于此类信息可在特定的工程设计指南中找到，因此本“安全导则”中未包含有关执行此类分析的详细指南。中子物理学和热工水力学分析为结构分析提供了必要的边界条件。

1.12. 本“安全导则”涵盖分析放射性物质释放各个方面，直至包括在预计运行事件和事故工况下确定释放到环境中的源项（第 2.16－2.18 段）。正常运行期间的放射性气体和液体流出物和排放物主要由运行措施控制，不在本“安全导则”的涵盖范围内。同样，放射性物质在环境中的扩散以及对人和非人生物群的辐射影响的预测也不在本“安全导则”的范围之内（见原子能机构《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》[4]）。虽然确定性安全分析的一般规则也可用于分析预计运行事件和事故工况的放射性后果，但本“安全导则”没有为这种分析提供具体指导。这种具体指导可在原子能机构其他安全导则中找到，例如原子能机构《安全标准丛书》第 GSG-10 号《设施和活动的预期放射性环境影响评定》[5]。

1.13. 本“安全导则”描述了进行确定性安全分析时应遵循的一般规则和过程。本“安全导则”没有说明具体现象，也没有系统地确定对以下方面至关重要的关键因素：中子物理学、热工水力、燃料（或燃料通道）和辐射分析。当在本“安全导则”中提供此类信息时，其目的是作为说明或示例，而不应被理解为是全面的说明。

1.14. 关于核安保的建议不在本“安全导则”的范围之内。一般而言，确定性安全分析过程相关的及其输出的文件和电子记录，所能提供的关于设备位置及其攻击脆弱性的信息有限，而关于电缆路线和电厂布局其他方面的信息则几乎没有。但无论如何，这类信息都需要评审，以识别可用于支持破坏行为的任何敏感信息，这类信息必须要适当保护。有关敏感信息和信息安全的指导见参考文献[6]。

结构

1.15. 本“安全导则”包括九部分和两个附件。第 2 部分介绍了确定性安全分析领域中使用的一些基本概念和术语，作为向其他各部分提供具体建议的基础。随后各部分的顺序对应于进行确定性安全分析的一般过程；第 3 部分介绍了假想始发事件和事故假想方案的系统识别、分类和分组方法，包括在不同电厂状态下，对分析事件选择的具体建议；这些都是确定性安全分析所要解决的问题；第 4 部分提出了确定性安全分析验收标准的总体概括，以便核电厂的设计和授权，并描述了验收标准的确定和使用规则；第 5 部分对计算机程序、其输入数据和电厂模型的选择，使用，核实和验证提供了指导；第 6 部分描述了确保充分安全裕量的一般方法，以证明对所有电厂状态的验收标准的遵守，重点是预计运行事件和设计基准事故；第 7 部分提供了对每个电厂状态进行确定性安全分析的具体指导；第 8 部分包含了关于确定性安全分析的记录、评审和更新的指导；第 9 部分就安全评定的独立核实提供指导，包括确定性安全分析的核实。

1.16. 附件 I 指出除核电厂设计和授权外，用于确定性安全分析的计算机程序的其他应用；附件 II 列出了一些国家用于新反应堆的预计运行事件的频率范围和设计基准事故类别。

2. 一般考虑事项

确定性安全分析的目的

2.1. 对核电厂进行确定性安全分析的目的是验证安全功能可以通过必要的结构、系统和部件按照必要的可靠性加以执行，结合相关运行人员的行动，能够在足够的安全裕量之下，充分有效地保持核电厂放射性物质的释放低于可接受的限值。其目标就是要证明阻挡核电厂放射性物质释放的屏障能够在要求的范围内保持其完整性。在补充了进一步的具体信息和分析（例如与制造、试验、检查和运行经验评定有关的信息和分析）以及概率安全分析之后，确定性安全分析也希望能有助于说明不同核电厂状态下的源项和潜在放射性后果是可以接受的，并且导致早期放射性释放或大量放射性释放的特定工况的可能性应该可以被视为“实际已消除了”（见第 3.55 段）。

2.2. 对不同电厂状态进行确定性安全分析的目的是希望将运行人员的假想行动结合在一起，通过证明符合既定验收标准，以论证工程设计的充分性。

2.3. 确定性安全分析可以独立地预测电厂对假想始发事件的响应，也可以结合其他的假想失效事件预测电厂对假想始发事件的响应。每个电厂状态都有指定的一组规则和验收标准可以应用。典型来说，这些分析侧重于中子物理学、热工水力学、热力机械、结构和放射性方面，并使用相应的计算工具对它们进行分析。特别对预定的运行模式和电厂状态进行计算仿真。

2.4. 计算结果是选定的物理变量随时间和空间变化的数值（例如中子通量、反应堆的热功率；一回路冷却剂的压力、温度、流量和流速；物理屏障的荷载；可燃气体浓度；放射性核素的物理化学组成；堆芯退化或安全壳压力状况；和释放到环境中的源项）。

确定性安全分析的验收标准

2.5. 为了论证核电厂的安全性，需要建立验收标准，以便在确定性安全分析中帮助判断分析结果的可接受性。验收标准可以用一般的、定性的术语或定量的限值来表达。公认有三类标准：

(a) 安全标准：基于维持安全功能的考虑，这类标准，不是直接与运行状态或事故工况的放射性后果有关，就是与防止放射性物质释放的屏障的完整性有关的标准；

(b) 设计标准：为满足安全标准（见 SSR-2/1（Rev.1）[1]要求 28）的重要先决条件，作为设计基准的一部分，对特殊的结构、系统和部件规定了设计限值；

(c) 运行标准：运行人员在正常运行和预计运行事件过程中所应遵守的规则，为满足设计标准和最终安全标准的提供先决条件。

2.6. 在本“安全导则”中，仅讨论了安全验收标准。这些验收标准，经监管机构核准，可包括与安全标准有关的裕量。

确定性安全分析中的不确定性分析

2.7. 本“安全导则”的第 6.21－6.29 段讨论了不确定性分析在确定性安全分析中的应用。实施不确定性分析的几种方法已经出版（例如参考文献[7]）。它们包括：

(a) 采用专家判断、统计技术和敏感性计算相结合；

(b) 缩比实验数据的使用；

(c) 边界假想方案计算的使用。

确定性安全分析方法

2.8. 针对保守等级不同的计算机程序分类（见第 5 部分）、电厂系统可用性假设分类以及分析的初始条件和边界条件分类，表 1 列出了目前可用于进行确定性安全分析的不同选项组合清单。

2.9. 选项 1 是一种保守的方法，其中假想的电厂条件和物理模型都是保守设定的。在保守的方法中，所有的参数将将赋予一个不利于相应验收标准通过的数值。在安全分析的早期，通常都采用保守的方法来简化分析，以较大的保守性来弥补在建模和对物理现象认识的不足。这是一种假定，即只要有一种方法可对许多类似的瞬态构成边界界定，则验收标准就可以满足所有被界定的瞬态。

2.10. 实验研究显著增加了对物理现象的理解，计算机程序的发展提高计算结果的准确性，计算结果能够更好地与核电厂的实验结果和记录的事件序列相对应。由于计算机程序能力的提高和保守方法明显的缺点（例如可能掩盖重要现象，和不同参数可能互相抵消的保守性），目前很少使用选项 1，也不建议目前的安全分析使用选项 1，除非在科学知识和实验支撑受限的情况下。但选 1 仍然具有重大作用，因为它可以作为最终分析方法而应用。

表 1. 执行确定性安全分析的选项

选项	计算机程序类型	关于系统可用性的假定	初始条件和边界条件的类型
1.保守选项	保守型	保守假定	保守型
2.组合选项	最佳评定型	保守假定	保守型
3.最佳评定加不确定性选项	最佳评定型	保守假定	最佳评定型 部分最不利工况
4.实际选项 *	最佳评定型	最佳评定假定	最佳评定型

* 为简单起见，本“安全导则”中使用了“现实方法”或“现实分析”等术语，意指在没有不确定性量化的情况下进行的最佳评定分析。

2.11. 选项 2 是一种基于使用最佳估算模型和计算机程序替代保守模型和程序的组合方法（第 6.12 段）。最佳估算程序在应用时，需要将保守的初始条件和边界条件以及系统可用性的保守性假定结合在一起使用，并假定有关程序模型的所有不确定性都已很好地确定，且基于电厂运行经验，所使用的电厂参数都是保守的。最终的分析还要求使用敏感度研究来判断选择保守输入数据的正确性。选项 2 通常用于设计基准事故和预计运行事件的保守分析。

2.12. 选项 3 是一种“最佳评定加不确定性”的办法。这允许使用最佳估算计算机程序以及更加现实的假设。考虑到所有参数同时处于最悲观值的概率极低，可采用最佳评定和部分不利（即稍微保守）的初始条件和边界条件的混合方式。通常对系统的可用性做出保守的假设。为了保证设计基准事故分析整体保守性的要求，需要对不确定性进行识别、量化和统计学综合。选项 3 包含了一定程度的保守性，目前为部分设计基准事故和预计运行事件的保守分析所接受。

2.13. 原则上，选项 2 和 3 是截然不同的分析类型。然而，在实践中，经常采用选项 2 和 3 的混合应用。这是因为，只要有大量数据，就倾向于使用最佳评定输入数据，只要数据稀缺，就倾向于使用保守的输入数据。这些选项之间的区别在于不确定性的统计学综合。

2.14. 根据选项 1—3 进行的确定性安全分析被认为是保守的，保守程度从选项 1 到选项 3 逐渐下降（见第 2.9—2.13 段）。

2.15. 选项 4 允许使用最佳估算模型和计算机程序，以及系统可用性和初始条件及边界条件的最佳估算值。选项 4 适用于对预计运行事件进行现实分析，目的是评定控制系统能力（见第 7.17－7.44 段），同时，除了在现实分析中判断运行人员规定行动的合理性以外，选项 4，一般情况下可对设计扩展工况进行最佳评定分析（见第 7.45－7.67 段）。需要短期放松监管要求的运行事件的确定性分析也可能依赖于最佳估算模型。关于适用于不同选项的建模假设的更详细资料见第 7 部分。

放射性物质释放到环境中的源项

2.16. 作为预测放射性物质在环境中的扩散一个关键因素，同时为了确定放射性辐射对电厂工作人员和公众的终极辐射剂量和对环境的影响，确定性安全分析的一个重要组成部分是确定放射性物质释放的源项。源项是“从设施释放（或假想将释放）的放射性物质的量和同位素成份”[3]；并用于“放射性核素向环境的释放的建模，特别是在核装置事故或处置库中放射性废物释放的情况下”[3]。

2.17. 为了评价核装置的源项，必须识别辐射源，确定产生的放射性核素的清单，并掌握放射性物质从堆芯穿过装置进而释放到环境中的机理。在事故工况下，源项评价要求仿真程序能够预测裂变产物从燃料元件中的释放、模拟其通过一回路系统和安全壳或乏燃料池厂房的输送，以及这种输送相关的化学效应和放射性物质释放的形式。

2.18. 由于以下原因，需对运行状态和事故工况的源项进行评价：

(a) 验证设计得到优化，以致源项降至在所有电厂状态下合理可行尽可能低水平；

(b) 支持证明出现可能导致早期放射性释放或大量放射性释放的特定工况的可能性可视为“实际已消除”；

(c) 证明设计可确保满足辐射防护要求，包括剂量限值；

(d) 在紧急情况发生时，为在核电厂的应急计划 [2] 提供依据，保护核电厂生命、健康、财产和环境安全；

(e) 为需要承受事故工况的设备鉴定提供技术规范的支持；

(f) 为应急计划的相关培训活动提供数据；

(g) 为缓解严重事故后果的安全功能提供设计支撑，（例如安全壳过滤排放和可燃气体复合器；见原子能机构《安全标准丛书》第 SSG-54 号《核电厂的事故管理计划》[11]）。

2.19. 本“安全导则”中介绍的确定性安全分析的一般规则也适用于源项的确定。为了提醒读者这些规则对此特定应用的适用性，本“安全导则”中的几个段落介绍了与源项确定相关方面的问题。

3. 假想始发事件的识别、分类、分组和事故假想方案

3.1. 根据 SSR-2/1（Rev.1）[1]中“（在设计时考虑的）电厂状态”的定义，在进行确定性安全分析时应考虑的电厂状态包括：

(a) 正常运行；

(b) 预期发生的行动；

(c) 设计基准事故；

(d) 设计扩展工况，包括无明显燃料破损的序列和堆芯熔化的序列。

3.2. 确定性安全分析应可以处理所有的假想始发事件，这些假想始发事件可能发生在核电厂的任何部分，并有可能导致放射性物质向环境释放，这些事件既可单独发生，也可能可与其他故障相结合同时发生，如控制和限值系统 [3] 以及安全功能相关的系统。这些事件不仅包括可能导致放射性物质

[2] 该等安排的适用性及设立不在本“安全导则”的范围内。关于这些安排的要求见国际原子能机构《安全标准丛书》第 GSR Part 7 号《核或辐射应急准备和响应》[8]；关于这些安排的建议见国际原子能机构《安全标准丛书》第 GS-G-2.1 号《核或辐射应急准备的安排》[9]和第 GSG-2 号《核或辐射应急准备和响应使用标准》[10]。

[3] 在本“安全导则”中，术语“控制和限制系统”不仅指用于控制和限制装置变量的仪表系统，还指用于正常运行的系统和由装置变量触发的预计运行事件的系统。

从反应堆堆芯释放，而且包括从其他来源的放射性释放，例如贮存在核电厂的燃料元件和那些处理放射性物质的系统。

3.3. 在应用过程中，还应考虑一种可能性，即在多机组核电厂，或多个乏燃料贮存单元，以及在特定场址上存在多个其他潜在放射性释放源的情况下，由单一原因同时引发的几个或甚至所有反应堆故障的突发事件（SSR-2/1（Rev.1）[1]第 5.15(b) 段）。

3.4. 正常运行的所有模式下发生的假想始发事件，确定性安全分析都应可以处理。并应假定设备的初始条件在始发事件前，正常运行的设备处于稳态。

3.5. 应考虑停堆模式的每个技术状态，包括换料和维护。对于这些模式，所有可能发生并导致风险增加的故障或其他因素，都应在停堆期间加以考虑，例如：

(a) 不能自动或手动启动某些安全系统；

(b) 自动化系统被禁用；

(c) 设备正在维护或修理；

(d) 一回路中的冷却剂量减少，包括某些模式，二回路中的冷却剂量减少；

(e) 仪器关闭或不起作用，无法进行测量；

(f) 一回路打开；

(g) 安全壳打开。

3.6. 对于乏燃料池相关的假想始发事件，应考虑与燃料装卸和贮存有关的具体运行模式。

3.7. 在可以忽略的短周期的电厂运行模式中发生的假想始发事件，如果经过仔细地分析和定量评价验证，对总体风险，包括可能导致早期放射性释放或大量放射性释放的潜在风险可以忽略不计，则可将这些假想始发事件排除在确定性安全分析之外。但无论如何，都应逐案处理，并应安排合理的程序或手段防止或缓解这些事件的发生。

管理系统

3.8. 确定性安全分析实施和结果的使用应该考虑采纳原子能机构《安全标准丛书》第 GS-G-3.1 号《设施和活动管理系统的应用》[12]和第 GS-G-3.5 号《核装置管理系统》[13]建议，以满足 SSR-2/1（Rev.1）[1]要求 1－3 和原子能机构《安全标准丛书》第 GSR Part 2 号《安全的领导和管理》[14]要求。

正常运行

3.9. 确定性安全分析应包括对正常运行的分析，即在规定的运行限值和条件下的运行的分析。正常运行通常应包括以下运行工况：

(a) 反应堆从停堆到正常启动、逼近临界和提升至满功率；

(b) 功率运行，包括满功率和低功率运行；

(c) 反应堆功率的变化，包括负荷跟踪模式，如果可行，应包括在低功率下延长一段时间后再返回满功率的状态；

(d) 反应堆从功率运行到停堆；

(e) 热停堆；

(f) 冷却过程；

(g) 冷停堆；

(h) 在停堆期间或正常功率运行期间（如适用）进行的换料；

(i) 在换料模式下或维修工况停堆，以打开反应堆冷却剂或安全壳边界；

(j) 乏燃料池的正常运行模式；

(k) 贮存和装卸新燃料。

3.10. 应该考虑到，在正常运行某些情况下，由于电厂模式的转变或电厂功率输出的变化所导致的主要电厂参数的变化。证明电厂参数在正常运行期间发生的瞬变可以保持在规定的运行限值和条件内，是进行确定性分析的一个主要目的。

假想始发事件

3.11. 在电厂状态下电厂性能行为的预测，除正常运行外（预计运行事件、设计基准事故和设计扩展工况）应基于电厂假想始发事件的专门清单，以及特定事件序列的其他设备故障或人因失误组合。

3.12. 应编写一份假想始发事件的清单。清单应是全面的，以确保对电厂行为的分析尽可能完整，从而保证**“可能造成严重后果的所有可预见事件和发生频率很高的所有可预见事件都可以被预测并在设计中加以考虑”**（SSR-2/1（Rev.1）[1]要求 16）。

3.13. 假想始发事件清单应充分考虑运行经验反馈，根据相关数据的可用性，应包括实际核电厂或类似核电厂的运行经验。

3.14. 始发事件集合的设定应涵盖所有可信的故障，包括：

(a) 电厂结构、系统和部件的故障（也可以是相关的部分故障），包括可能的错误驱动；

(b) 由运行人员错误引发的故障，包括运行维护工作的错误或不完整，到控制设备限值设置不正确，以及错误的运行行动；

(c) 由内部和外部意外事故引起的电厂结构、系统和部件的故障。

3.15. 一个给定的假想始发事件在电厂中引发的所有后续故障应作为假想始发事件的一部分在电厂响应分析时加以考虑。这些应包括：

(a) 如果始发事件是一个配电系统发生了部分故障，则对预计运行事件、设计基准事故或设计扩展工况的分析时，应假定由该配电系统故障部分供电的所有设备都不可用；

(b) 如果始发事件是一个高能事件，例如一个压力系统的故障，会导致高温水释放或管道甩击，所以，预计运行事件、设计基准事故或设计扩展工况的分析应包括对可能受此类事件影响的设备的潜在故障的考虑；

(c) 对于火灾或洪水等内部危害，或地震等外部危害造成的故障，引起的假想始发事件的限定范围应包括所有既未做设计承受危害的设备也未做防护保护的设备。

3.16. 除了设定始发故障和后续故障之外，为在确定性安全分析中的保守性或为了纵深防御，还假定了其他故障标准，例如共因故障、设计基准事故中的单一故障标准。应该将假想始发事件的故障部分同由假想始发事件直接导致的故障区分开来。最后，可以添加一些故障来划定一组类似事件的范围，以限制分析的数量。

3.17. 假想始发事件应仅包括那些直接导致安全功能受到挑战并最终威胁到放射性物质释放屏障完整性的故障（初始的或后续的）。所以，危害，无论是内部的还是外部的（自然的或人为的），都不应被认为是假想始发事件本身。但是，不管怎样，与这些危害相关联的载荷都应被视为假想始发事件的潜在原因，包括由这些危害导致的多重故障。

3.18. SSR-2/1（Rev.1）[1]第 5.32 段指出：

> “在工程判断、确定性安全评定和概率安全评定的结果显示某一事件的组合可能会导致预计运行事件或事故工况时，应该将这类事件的组合视为设计基准事故或将其纳入设计扩展工况，这主要取决于它们发生的可能性。”

3.19. 应系统地确定假想始发事件集合。它应包括一种结构化的方法来确定假想始发事件，例如：

(a) 利用危害与可操作性分析、失效模式和效果分析、工程判断和主逻辑图等分析方法；

(b) 与类似电厂安全分析制定的假想始发事件清单进行比较（确保以前确定的缺陷不会传播）；

(c) 同类电厂运行经验数据分析；

(d) 使用概率安全分析的见解和结果。

3.20. 在确定性安全分析中，传统上将某些极限事故（如大破口丧失冷却剂事故、主蒸汽或给水管道的破口、压水堆控制棒弹出或沸水堆落棒）作为设计基准事故。这些事故应予以考虑，因为它们代表了反应堆必须防护的一类事故。不应将它们排除在设计基准事故类别之外，除非经过仔细地分析和定量评价，表明它们对于总体风险和潜在作用，包括出现的可能导致早期放射性释放或大量放射性释放的工况，可将它们排除在外。

3.21. 如果支持系统中发生的阻碍正常运行所需系统运行的故障并最终需要启动反应堆保护系统或安全系统，则该故障也应被视为假想始发事件。

3.22. 在进行设计和安全评定时，作为这两个活动之间迭代过程的一部分，应该再次对假想始发事件集进行审核。假想始发事件还应在整个电厂寿命周期内定期审核，例如作为定期安全评审的一部分，应确保其仍然有效。

识别预计运行事件和设计基准事故的假想始发事件

3.23. 考虑到假想始发事件的物理演变过程，假想始发事件应细分为具有代表性的事件序列组。每个组所包括的是导致对安全功能和屏障的类似挑战的事件序列，并且需要类似的缓解系统将电厂带回安全状态。因此，它们可以由某一个有代表性的事件序列来限定，在处理组序列问题时通常引用该序列（并且通常由相关的假想始发事件本身来标识）。这些群组也根据其发生频率进行分类（见第 3.27 段）。这种方法允许对同一代表性的事件序列分组下的所有假想始发事件，选择相同的验收标准和初始条件，并应用相同的假定和方法。作为示例，假想始发事件“主给水泵停止”、“所有主给水泵停止”和“主给水系统上的隔离性中断”通常都被分组在一个具有代表性的事件序列下，例如“主给水丧失”。

3.24. 代表性的事件序列也可以根据序列类型分组，如将重点关注在降低堆芯冷却和反应堆冷却剂系统加压、安全壳加压、放射性后果或受压热冲击等方面。在第 3.23 段例子中，代表性的“主给水丧失”事件序列属于“反应堆排热下降”事件序列类型。

3.25. 与预计运行事件和设计基准事故相关的假想始发事件应反映设计的具体特征。根据以下列出的典型序列类型，第 3.28 段给出了关于预计运行事件的一些典型的假设始发事件及其产生的事件序列，第 3.30 段给出了关于设计基准事故的一些典型的假设始发事件及其产生的事件序列。典型序列类型如下：

(a) 增加或减少通过反应堆冷却剂系统的排热；

(b) 增加或减少反应堆冷却剂系统的流量；

(c) 反应堆堆芯反应性和功率分布异常，或贮存中的新燃料或乏燃料反应性异常；

(d) 增加或减少反应堆冷却剂容量；

(e) 潜在旁通的安全壳发生了反应堆冷却剂系统泄漏；

(f) 安全壳外泄漏；

(g) 乏燃料贮存池中燃料冷却的减少或丧失；

(h) 在不停堆换料过程中燃料冷却丧失（重水压水堆）；

(i) 放射性物质从子系统或部件中释放出来（典型的是从放射性废物的处理或贮存系统中）。

3.26. 进行源项分析时，为更好地处理导致放射性物质向环境释放的不同途径，可能需要建立特定的假想始发事件分组。应特别注意放射性物质的释放可能会旁通过安全壳，因为即使在释放量相对较小的情况下，其后果也可能是严重的。

3.27. 在每组假想始发事件中，代表性的事件序列还应根据组中最经常出现假想始发事件的频率继续细分成若干类别。应通过合适的方法检查每个假想始发事件对应的频率范围。附件 II 表 II-1 列出了一些国家在新反应堆建设时预计运行事件和设计基准事故对应的频率范围。

3.28. 导致预计运行事件发生的假想始发事件序列的典型例子，根据序列类型排序，如下所示。这份清单大体上是指示性的，实际清单将取决于反应堆的类型和实际设计：

(a) 反应堆排热增加：误开蒸汽释放阀；压力控制故障导致蒸汽流量增加；给水系统故障导致排热率增加；

(b) 反应堆排热减少：给水泵跳闸；由于各种原因（控制故障、主蒸汽阀关闭、汽轮机跳机、外部负载丧失和其他外部电网扰动、功率丧失、凝汽器真空丧失）导致的蒸汽流量降低；

(c) 反应堆冷却剂系统的流量增加：启动主冷却剂泵；

(d) 反应堆冷却剂系统的流量减少：一个或多个冷却剂泵跳闸；错误隔离了一个主冷却剂系统回路（如果适用）；

(e) 反应堆堆芯反应性和功率分布异常：控制棒（或控制棒组）的意外提出；由于化学和体积控制系统（压水堆）的故障而造成的硼稀释；燃料组件的定位错误；

(f) 贮存中的新燃料或乏燃料反应性异常：乏燃料池中的硼稀释；

(g) 慢化剂循环的丧失或慢化剂热阱（重水压水堆）的减少或丧失；

(h) 反应堆冷却剂容量增加：化学和体积控制系统故障；给水流量过大（沸水反应堆）；应急堆芯冷却的误操作；

(i) 反应堆冷却剂容量减少：由于仪器仪表管路故障造成的冷却剂缓慢丧失；

(j) 乏燃料贮存池中燃料冷却的减少或丧失：厂外电源丧失；衰变热排热系统故障；燃料贮存池冷却剂泄漏；

(k) 由于反应堆冷却剂系统泄漏而导致放射性物质释放，可能通过旁通过安全壳；

(l) 由于子系统或部件泄漏而导致放射性物质的释放：放射性废物系统或流出物系统的小泄漏。

3.29. 应该识别可能导致设计基准事故的假想始发事件的子集。还应使用设计基准事故标准对所有被确定为预计运行事件起因的假想始发事件进行分析；从而证明“通过自动启动安全系统的安全动作，结合运行人员的规定动作（SSR-2/1（Rev.1）[1]第 5.75(e) 段）”来管理导致预计运行事件的假想始发事件是可能的。虽然这通常不包括发生频率很低的假想始发事件，但任何频率下限的确定都应考虑每个反应堆特有的安全目标。

3.30. 导致设计基准事故发生的假想始发事件序列的典型例子，根据序列类型排序，如下所示。这份清单大体上是指示性的，实际清单将取决于反应堆的类型和实际设计：

(a) 反应堆排热增加：蒸汽管线破裂；

(b) 反应堆排热减少：给水丧失；

(c) 反应堆冷却剂系统流量减少：主冷却剂泵卡死或断轴；所有冷却剂泵跳闸；

(d) 反应性和功率分布的异常：控制棒（或控制棒组）的失控抽出；控制棒弹出（压水堆）；落棒事故（沸水堆）；由于备用回路（压水堆）的启动而引起的硼稀释；

(e) 反应堆冷却剂容量减少：连续的冷却剂丧失事故；误开一回路系统卸压阀；一回路冷却剂泄漏到二回路系统中；

(f) 乏燃料贮存池中燃料冷却的减少或丧失：连接到乏燃料贮存池水的管道破裂；

(g) 在不停堆换料过程中燃料冷却的丧失（重水压水堆）；

(h) 慢化剂循环的丧失或慢化剂热阱（重水压水堆）的减少或丧失；

(i) 由于安全壳的旁路，来自于反应堆冷却剂系统的放射性物质泄漏，来自于子系统或部件的泄漏：包括乏燃料运输或贮存中的过热或损坏；废气或废液处理系统的破裂；

(j) 最终屏蔽的冷却故障（重水压水堆）。

3.31. 应使用概率分析来支持确定性分析，以证明依据假想始发事件发生频率进行分类的合理性。频率的计算应考虑假想始发事件发生所对应电厂运行状态的相关频率，例如满功率或热停堆等。应特别注意确保降低屏障完整性瞬变的归类应与屏障变化可能产生的效果相一致。

3.32. 应从每一类事件（见第 3.27 段）中选择一些被称为限定假想方案和演变假想方案极限案例。这些限定假想方案和演变假想方案应聚合性地包括对每项相关验收标准构成最大挑战的案例，且案例中应涉及安全相关设备性能参数的限值。为了一个限定假想方案能够完全包含这个组中所有可能的假想始发事件，可以将几个假想始发事件合并，并对它们的后果进行放大。安全分析应验证对始发事件的分组和捆绑限定是可接受的。

3.33. 在某些情况下，应以不同的验收标准从不同的角度对单一事件进行分析。一个典型的例子是冷却剂丧失事故，它可以从许多方面进行分析，包括堆芯冷却功能的破坏、安全壳压力的上升、放射性物质的传输和环境释放，特别是针对压水堆，也可以从一回路冷却剂泄漏到蒸汽发生器，以及沸腾冷凝工况下高压水热冲击和硼的误稀释（反应性事故）等方面进行分析。

3.34. 在进行新燃料和辐照燃料操作期间发生的事故也应进行评价。此类事故在安全壳内外都可能发生。

3.35. 还有一些其他类型的假想始发事件也会导致放射性物质释放到安全壳之外，其源项也应予以评价。这些事件包括：

(a) 当乏燃料池位于安全壳外部时，乏燃料池中燃料冷却减少或丧失；

(b) 新燃料或乏燃料的反应性增加；

(c) 从承载固体、液体或气体放射性物质的任何辅助系统意外排出；

(d) 用于正常运行期间减少放射性物质排放的系统或部件，如过滤器或缓冲箱发生故障；

(e) 当反应堆或安全壳处于打开状态时，换料或维护期间发生的事故。

3.36. 一个属于预计运行事件或设计基准事故的绑定在一起的事件序列的指定频率，应该是由已经分组在一起的假想始发事件建立的。

确定设计扩展工况的一般考虑事项

3.37. SSR-2/1（Rev.1）[1]要求 20 规定：

“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组设计扩展工况，以便通过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方案并对防止这类事故或减轻事故后果的实际规定做出规划。”

3.38. 应确定两类不同的设计扩展工况：没有明显燃料破损的设计扩展工况；和导致堆芯熔化的设计扩展工况（即严重事故）[4]。这两类设计扩展工况的确定性安全分析可以采用不同的验收标准和不同的规则。

无明显燃料破损的设计扩展工况的识别

3.39. 没有明显燃料破损的设计扩展工况序列的初步选择应在频率很低的单一始发事件或多重故障的事件中考虑，以满足关于防止堆芯损坏的验收标准。

3.40. 应编写一份确定性的没有明显燃料破损的设计扩展工况的导出清单。相关的设计扩展工况应包括：

(a) 可能导致超出设计基准事故安全系统设计能力的始发事件。一个典型的例子是压水堆蒸汽发生器中超出了设计基本假设的多管断裂；

[4] 在一些状态下，这些类别的设计扩展工况分别表示为“设计扩展工况 A”（没有显著的燃料破损）和“设计扩展工况 B”（带有堆芯熔化）。

(b) 预计运行事件或高频设计基准事故与多重故障（例如冗余系列中的共因故障）的组合，它们会阻止安全系统执行预定的控制假想始发事件功能。一个典型的例子是冷却剂丧失事故时没有启动安全射入的情况。支持系统的故障隐含地包括在安全系统的故障原因中。这些序列的识别应以安全分析中的任意一个安全系统完全失效对电厂影响的系统分析为基础，针对预计运行事件或设计基准事故展开，特别是那些高频率的预计运行事件或设计基准事故；

(c) 可信的假想始发事件可能包含了导致安全系统丧失的多个故障，而安全系统是作为正常运行的一部分履行其功能的。这适用于某些系统的设计，如，同一个的排热系统在事故工况下和停堆期间都会使用。这些序列的识别应通过正常运行中任意一个安全系统的完全失效对电厂的影响的系统分析来实现。

3.41. 设计扩展工况在很大程度上取决于技术和设计，但以下清单应作为无明显燃料破损的设计扩展工况的初步参考，应特别注意与电厂的类型和设计相适应：

(a) 典型的非设计基准事故的甚低频率的始发事件：

(i) 蒸汽发生器的传热管多管断裂（压水堆、重水压水堆）；

(ii) 主蒸汽管线破裂并导致蒸汽发生器传热管管断裂（压水堆、加压重水堆）。

(b) 预计运行事件或设计基准事故与安全系统中的多重故障并发：

(i) 未能紧急停堆的预计瞬变（ATWS）：预计运行事件与控制棒未能下插并发；

(ii) 全厂断电：失去厂外电源与应急柴油发电机故障并发或失去厂外电源与备用应急电源故障并发；

(iii) 给水完全丧失：主给水丧失与应急给水全部丧失并发；

(iv) 冷却剂丧失事故，同时完全丧失一种应急堆芯冷却功能（应急堆芯冷却系统的高压或低压部分）；

(v) 假想始发事件发生后所需安全系统长期丧失。

(c) 包含多重故障的假想始发事件：

(i) 设备冷却水系统或重要厂用水全部丧失；

(ii) 在冷停堆或换料过程中余热排出系统丧失；

(iii) 乏燃料池正常冷却和为设计基准事故设计的冷却系统丧失；

(iv) 失去进入最终热阱的正常通道。

3.42. 为了确定无明显燃料破损的设计扩展工况，应特别注意辅助和支持系统（例如通风、冷却和电源），因为其中一些系统可能在运行和安全系统中造成多个直接或延迟的后续的多重故障。

3.43. 应将产生类似安全挑战的无明显燃料破损的设计扩展工况的不同序列归并在同一分组中。应对每一组的限制假想方案进行分析以呈现对相关验收标准带来的最大挑战。

3.44. 应专门列出在无明显燃料破损设计扩展工况的每个序列中考虑的多重故障。

堆芯熔化设计扩展工况的识别

3.45. 应根据电厂安全目标，选择若干堆芯熔化（严重事故）的特定序列进行分析，以便建立缓解此类事故后果的安全设施的设计基准。为了表现堆芯熔化序列中涉及的所有主要物理现象，应选择这些序列，如一回路压力、反应堆衰变热或安全壳状态。

3.46. 应假定防止堆芯熔化的设施失效或不足，并且事故序列将进一步演变为严重事故。应通过增加额外故障或假设在应对设计基准事故或设计扩展工况序列以及概率安全分析中确定的主要事故序列时，运行人员进行不正确操作响应，来选择堆芯熔化设计扩展工况下代表性的事件序列。

3.47. 应根据每个验收标准，对堆芯熔化设计扩展工况的代表性事件序列进行分析，特别是那些可能对安全壳完整性带来挑战的序列，以确定极限工况。代表性事件序列应该用于安全壳的设计输入和那些缓解这类设计扩展工况的后果的安全设施的设计输入。

3.48. 设计扩展工况在很大程度上取决于技术和设计，但以下事故可作为堆芯熔化（严重事故）设计扩展工况的初步参考：

(a) 丧失堆芯冷却能力，例如，在部分或全部丧失现场交流电源时，厂外电源的持续丧失，同时丧失最终热阱的正常通道（确切序列取决于设计），或丧失最终热阱的正常通道；

(b) 完全丧失反应堆冷却剂系统，例如，在冷却剂丧失事故时，应急堆芯冷却系统不可用或超过其能力。

3.49. 即使一个堆芯熔化事故发生频率估算较低，也不是保护安全壳抵御此类工况失效的理由。无论在设计中实施何种规定，都应假想堆芯熔化工况。为排除安全壳失效，分析应能证明堆芯熔化事故可能导致的高能现象已得到预防（即，出现工况的可能性可认为“实际已消除”）。

3.50. 应选择堆芯熔化设计扩展工况的代表性事件序列，通过一个严重事故相关的现象，识别该严重事故产生的最严重的电厂参数。这些参数应用于电厂结构、系统和部件的确定性分析，以证明这种严重事故序列的放射性后果是有限的。在评定严重事故中使用的设备[5]（见 SSR-2/1（Rev.1）[1]要求 30）是否能够严重事故时履行其预期功能，这些序列的分析可以提供这些设备的环境工况。

由于内部和外部危害而产生的假想始发事件的识别

3.51. 假想始发事件的确定，应考虑由相关现场内部和外部危害引起的事件的效应和负荷，既要考虑单独效应和负荷，也要考虑组合效应和负荷（要求 17 和 SSR-2/1（Rev.1）[1]第 5.15(a)－5.21(a)段）。外部危害清单见原子能机构《安全标准丛书》第 SSR-1 号《核设施的厂址评估》[15]。对内、外部危害的分析不同于核电厂技术系统中单一故障或多重故障所导致假想始发事件和假想方案的分析[6]，也不同于错误人员动作所造成的直接影响基本安全功能实施的假想始发事件和假想方案的分析。危害本身并不代表始发事件，但它们与负荷相关联，负荷的变化可能触发此类事件。

3.52. 根据 SSR-2/1（Rev.1）[1]第 5.15(b) 段、第 5.19 段和第 5.63 段规定，在确定多机组场址内由特定危害引发的假想始发事件时，应考虑事件同时作用于场址几个或甚至所有机组的可能性。具体而言，应考虑失去电网、失去最终热阱以及共用设备故障的效应。

---

[5] 虽然设备鉴定不在本“安全导则”的范围内，但应理解，用于堆芯熔化设计扩展工况的典型设备鉴定方案并不总是适用的，对构筑物、系统和设备的可运行性的评定是可以接受的。一些电厂状态下使用“生存能力评定”一词进行这种评定。

[6] “基本安全功能”也称为“主要安全功能”[3]。

3.53. 通过概率方法或相应的工程设计方法进行的危害分析[7]，其目的旨在证明每一种危害，或是：

(a) 对风险的贡献微乎其微，因此可以筛选出该危害；

(b) 因核电厂设计的稳健性足以防止危害负荷所导致的始发事件造成的转变；

(c) 导致出现设计中考虑的始发事件。

3.54. 在始发事件是由危害引起情况下，分析应只考虑那些指定用于危害防护或者可以用于危害防护的构筑物结构、系统和设备的功能。

“实际已消除”的事件序列和事故假想方案

3.55. SSR-2/1（Rev.1）[1]第 2.13(4) 段指出：

> “严重事故情况中的安全目标是：只需要采取限制时间和限制适用空间的防护行动，就可以避免或最大程度地减少厂外污染。那些导致早期放射性释放或大量放射性释放[3]的事件序列，应该“实际已消除[4]。”
>
> “[3] 在这一语境中的“早期放射性释放”是指需要采取厂外防护行动但在后续时间内其防护效应不能发挥完全的放射性释放。“大量放射性释放”是指在通过时间和适用空间限制的厂外防护行动已不足以保护人类和环境的放射性释放。
>
> “[4] 如果这些工况从物理属性上来说根本不可能出现，或者如果有很大的把握认为这些工况极不可能出现，则出现这种特定工况的可能性可视为‘实际已消除’。”

3.56. 为具体核实“实际消除”的事件序列，要求对事件进行如下分类：

(a) 可能导致反应堆堆芯迅速损坏并导致安全壳早期失效的事件，如：

(i) 反应堆冷却剂系统中大型承压部件失效；

(ii) 反应性失控事故。

(b) 可能导致安全壳早期失效的严重事故序列，如：

(i) 高能的安全壳直接加热；

---

[7] 见国际原子能机构《安全标准丛书》第 NS-G-1.5 号《核电厂设计中的非地震外部事件》[16]、第 NS-G-1.7 号《核电厂设计中的内部火灾和爆炸防护》[17]和第 NS-G-1.11 号《核电厂设计中除火灾和爆炸外的内部危害防护》[18]进一步指导。

(ii) 大型蒸汽爆炸；

(iii) 可燃气体爆炸，包括氢气和一氧化碳。

(c) 可能导致安全壳后期失效的严重事故序列[8]：

(i) 熔芯－混凝土相互作用过程中基底穿透或安全壳旁通；

(ii) 安全壳长期丧失排热；

(iii) 可燃气体爆炸，包括氢气和一氧化碳。

(d) 安全壳旁通的严重事故；

(e) 贮存燃料池中的燃料严重破损和排放失控。

3.57. 可以视为“实际已消除”的事件序列的后果不是确定性安全分析的一部分。然而，确定性安全分析有助于证明设计和运行规定在“实际消除”这些序列方面是有效的（见第 7.68－7.72 段）。

4. 确定性安全分析的验收标准

4.1. GSR Part 4（Rev.1）[2]第 4.57 段指出，“用于安全判断的标准，必须在安全分析中确定，以充分满足设计方、营运组织和监管机构的要求。”

4.2. SSR-2/1（Rev.1）[1]第 5.75 段指出，“确定性安全分析应主要提供：……(d) 验收标准、设计限值、剂量限值和用于辐射防护目的可接受限值分析结果的比较”。确定性安全分析应证明与验收标准的一致性。

4.3. 应为所有运行状态和事故工况建立验收标准。这些标准的目的应是防止放射性物质释放的相关屏障受到损害，以防止超出可接受限值的释放（及其后果）。标准的选择应确保标准与屏障完整性丧失的物理限值之间有足够的裕量。

4.4. 验收标准应与相关工况的频率相关。发生频率更高的工况，如正常运行或预计运行事件，其验收标准应比发生频率较低的工况更加严格，例如设计基准事故或设计扩展工况的验收标准。

[8] 在确定“实际消除”的情况时，需要分析这些工况。然而，第 3.56(c) 段 (i) 和 (ii) 的后果一般可通过实施合理的技术手段加以缓解。

4.5. 验收标准应在两个层次上确定，如下所示：

(a) 高放（放射性）标准，涉及电厂运行状态或事故工况的放射性后果。这些通常以活度水平或剂量表示，通常由法律或法规要求加以界定；

(b) 详细的（导出的）技术标准，涉及放射性物质释放屏障的完整性（例如燃料基体、燃料包壳、反应堆冷却剂系统压力边界和安全壳）。这些在法规要求中定义，或由设计方在法规认可的前提下建议，用于安全的核实。

4.6. 只要合适，放射性验收标准应以核电厂工作人员、公众或环境，包括非人类生物群的有效剂量、等效剂量或剂量率表示。关于剂量的放射性验收标准应根据适用的安全要求（见 SSR-2/1（Rev.1）[1]要求 5 和 81）加以确定。

4.7. 以剂量表示的放射性验收标准可转换为不同放射性核素的可接受活度水平，以便使核电厂的设计特点与环境特点解耦。

4.8. 正常运行的放射性验收标准通常应表述为电厂工作人员和电厂附近公众的有效剂量限值，或电厂计划排放活动的授权限值（见 SSR-2/1（Rev.1）[1]要求 5）。

4.9. 由于预计运行事件的频率更高，预计运行事件的放射性验收标准应比设计基准事故的放射性验收标准更加严格。

4.10. 设计基准事故的放射性验收标准应确保符合 SSR-2/1（Rev.1）[1]要求 19 和第 5.25 段要求。

4.11. 设计扩展工况的放射性验收标准应确保满足 SSR-2/1（Rev.1）[1]要求 20 和第 5.31A 段要求。

4.12. 技术验收标准应根据那些支配挑战屏障完整性的物理过程的变量来设定。通常的工程经验是使用与屏障物完整性有关的代理变量 [9] 来建立验收标准或确保屏障物完整性的组合标准。在确定这些验收标准时，应包括足够的保守性，以确保有足够的安全裕量防止屏蔽完整性的丧失。

[9] 在本“安全导则”中，“替代变量”是一个可测量的变量，它提供了无法直接测量的另一个变量的间接测量。

4.13. 在制定技术验收标准集合时，应根据具体的设计解决方案酌情考虑下列标准分组和示例：

(a) 与核燃料基体完整性有关的标准：最高燃料温度和最大径向平均燃料焓（同时考虑燃耗、燃料成分和添加剂，如可燃吸收剂，的两个值）；

(b) 与燃料包壳完整性有关的标准：最小偏离泡核沸腾比；最高包壳温度；和局部包壳最大氧化；

(c) 与整个反应堆堆芯完整性有关的标准：充分的次临界；包壳氧化最大产氢量；堆芯燃料元件的最大损坏；燃料组件的最大变形（根据冷却、插入控制棒和拆卸控制棒的要求）；和排管容器完整性（用于重水压水堆）；

(d) 与反应堆外部的核燃料完整性有关的标准：充分的次临界、燃料组件上方有足够的水位和充分的排热；

(e) 与反应堆冷却剂系统完整性有关的标准：最大冷却剂压力；最高温度、压力和温度变化以及在冷却剂系统压力边界中产生的应力和应变；并且没有因反应堆压力容器的假想缺陷引发脆性断裂或塑性破坏；

(f) 与二回路完整性相关的标准（如果相关）：最大冷却剂压力；以及二回路设备中的最高温度、压力和温度变化；

(g) 与安全壳完整性和释放到环境的限制有关的标准：最大和最小压力的值和持续时间；作用在安全壳壁上的最大压力差；最大泄漏量；易燃或爆炸性气体的最高浓度；系统运行的可接受工作环境；和安全壳内的最高温度；

(h) 与限制辐射照射所需的其他部件的完整性有关的标准，如重水压水堆中的屏蔽端：最大压力、温度和升温速率。

4.14. 对于在停堆模式或其他情况下发生的任何屏障失能或屏障完整性下降的始发事件，如果可能，应使用更严格的标准，例如避免开放的反应堆容器或乏燃料池中的冷却剂沸腾，或避免燃料组件的裸露。

4.15. 一般而言，对于发生频率较高的工况，与屏障完整性有关的技术验收标准应更加严格。对于预计运行事件，任何物理屏障（燃料基质、燃料包壳和反应堆冷却剂压力边界或安全壳）都不应有实质性的破坏和燃料损坏（如在运行限值内，授权在正常运行时允许发生轻微的燃料泄漏，而不是额外的燃料破损）。对于设计基准事故和没有明显燃料破损的设计扩展工况，核电

厂释放放射性物质的屏障应在所需范围内保持其完整性（见第 4.10 段和第 4.11 段）。对于堆芯熔化的设计扩展工况，应保持安全壳的完整性，并防止安全壳旁通，以确保防止早期放射性释放或大量放射性释放。

4.16. 应明确规定每项标准的适用范围和工况。例如，燃料熔化温度或燃料焓升的技术规范应与燃料燃耗和可燃吸收剂含量的技术规范相关联。同样，对于放射性释放的限制，应具体规定释放的持续时间。验收标准会因工况的不同而有很大差异。因此，验收标准应与用于安全分析中充分详细的工况和假设相关联。

4.17. 虽然安全分析中可能没有明确涉及对安全很重要的工程方面的评定，但它是安全评定的一个相关部分。应用于结构、系统和部件设计的安全裕量应与它们可能必须承受的载荷的不确定性及其失效的后果相当。

4.18. 除了所有相关物理量外，应力和应变的评价还应考虑到每种载荷和每种载荷组合所产生的环境条件以及相应的边界条件。验收标准应充分反映阻止结构或部件严重失效的情况，这些结构和部件对于缓解与假想载荷相关的事件的后果是必要的。

5. 确定性安全分析计算机程序的使用

计算机程序选择和使用的基本规则

5.1. GSR Part 4（Rev.1）[2]要求 18 规定，“**对安全分析所使用的任何计算方法和计算机程序都必须进行核实和验证。**”用于确定性安全分析的计算机程序中使用的模型和方法应适用于此目的。必须验证和核实的范围以及实现的手段取决于应用的类型和分析的目的。

5.2. 关于计算机程序的选择，应当验证：

(a) 用于说明过程的物理模型是合理的；

(b) 模型中的简化假设是合理的；

(c) 用于表示物理过程的相互作用是合理的，并且它们的适用性限制已确定；

(d) 程序的适用范围应该是确定了的。这一点很重要，当某些模型或计算方法被设计出来仅用于对特定范围工况内的物理过程进行建模时，该程序不可应用于此范围之外的工况；

(e) 该程序所用的数值方法准确、健稳；

(f) 在程序的设计、编码、调试和文档编写方面采用了系统的方法；

(g) 源代码与其在系统程序文档中说明的一致性已完成评定。

5.3. 对单一计算机程序的准确性评定应包括以下一系列步骤：

(a) 识别支持性实验数据中的重要现象和预期电厂行为；

(b) 估算程序中使用的数值方法的不确定性；

(c) 估算程序中使用的主要模型的不确定性；

(d) 确定重要过程对主要变量值的敏感性。

5.4. 关于计算机程序的输出，应验证程序的预测数据与以下数据进行了比较：

(a) 重要现象模型的实验数据。这通常包括与“单一效果测试”和“整体效果测试”进行比较，如第 5.25 段所述；

(b) 可用的电厂数据，包括调试或启动过程中的试验数据，以及运行事件或事故的数据；

(c) 独立开发并使用不同方法的其他程序的输出；

(d) 标准问题和/或数值基准的答案，如果这些问题和基准是可用和可靠的。

5.5. 虽然在开发更准确和可靠的事故分析计算机程序方面取得了重大进展，但用户仍然对分析的质量有重大影响。应确保：

(a) 程序的所有使用者均已接受足够的培训，并对程序所用的模型和方法有足够的理解；

(b) 用户或其主管在程序使用方面有足够的经验和理解，同时对具体应用情况（如冷却剂丧失事故）有相应的限制也是充分了解的；

(c) 使用者对程序的使用有充分的指导；

(d) 用户遵循程序使用建议，特别是那些与正在进行分析的特定应用程序相关的建议。

5.6. 关于计算机程序的使用，应当验证：

(a) 节块化（见第 5.39 段）和电厂模型很好地反映了电厂的行为；

(b) 输入数据正确；

(c) 在实际可行的范围内，节块化选定的模型和假设应与用于鉴定单一效果测试和整体效果测试所选定的模型和假设一致；

(d) 对程序的输出进行充分的评价和理解，并正确地使用。

与计算机程序使用有关的过程管理

5.7. 所有影响计算机程序质量的活动都应使用专门确保软件质量的程序来管理。对安全至关重要的软件的开发和维护，应运用成熟的软件工程经验。应在程序的整个生命周期内建立形式化的流程和指令，包括程序开发、核实和验证，以及持续的维护过程，并特别注意错误的报告和更正。

5.8. 程序开发人员应该确保，为提供程序满足功能要求的信心所必须的计划和系统的行动，已经付诸实施。这些流程至少应涵盖开发控制、文档控制、程序配置以及调试和纠正措施等工作。

5.9. 为了将程序开发中的人因失误降至最低，只有资质合格或受监督的人员才能参与程序的开发、核实和验证。同样，在用户组织中，只有资质合格或受监督的人员才能使用该程序。

5.10. 开发和维护计算机程序的活动应包括：

(a) 为开发人员和用户编写和更新程序手册；

(b) 核实和验证活动及其文件；

(c) 错误报告和纠正措施及其文档；

(d) 验收测试，包括非回归测试、程序安装和程序手册升级；

(e) 配置管理；

(f) 接口控制；

(g) 程序的版本控制。

5.11. 如果将程序开发、核实或验证的任务委托给外部组织，则应在外部组织内管理这些任务，以确保质量。用户组织应评审外部组织内的安排，并对其实施情况进行监查。

5.12. 当开发新版本的计算机程序时，应使用新版本模拟一组已建立的测试用例，与先前版本相比结果中的任何显著差异都应进行识别和理解。合适的话，此类模拟应由程序开发人员和用户联合进行。

计算机程序使用中有关安全与安保之间的接口

5.13. 计算机安保措施应到位，以保护程序和开发环境免受恶意行为和漏洞的引入。关于核设施的计算机安保导则见参考文献[19]。

计算机程序的核实

5.14. GSR Part 4（Rev.1）[2]第 4.60 段指出，计算机程序的核实必须包括模型核实和系统程序核实。

5.15. 计算机程序的核实应包括证实程序（源代码和算法）准确描述了真实系统的数学模型（模型核实）并与程序文档相符合（系统程序核实）。一般而言，数值方法是将方程转化为数字计算方案进行求解的算法，核实工作应确保数值方法、用户选项和约束条件根据技术规范得到了正确的实施。

5.16. 计算机程序核实工作可以通过设计评审、过程检查和质量监督进行。应提供检查清单供设计评审和过程检查。可对选定的项目进行质量监督，以确保质量。

5.17. 计算机程序的核实工作，应根据程序文档中的说明对源代码进行检查，应包括对设计概念、基本逻辑、流程图、算法和计算环境的评审。

5.18. 如果计算机程序在后续运行的硬件或软件平台（例如，操作系统）与执行核实过程的硬件或软件平台不一样，则应重新评定程序核实在后续平台上的有效性。

5.19. 应对程序源代码进行核实，以证实其符合公认的编程实践，并且其逻辑与程序文档一致。

5.20. 复杂的计算机代码可能包含了较简单代码的集成或耦合。在这种情况下，复杂代码的核实应确保代码之间的链接和/或接口被正确地设计和实现，以满足程序文档的要求。

计算机程序的验证

5.21. 为了确定程序中使用的数学模型充分展示了建模的真实系统，应对计算机代码进行验证，应尽可能，将代码的输出结果与实际系统的观测结果或实验数据进行比较。

5.22. 计算机程序的验证，应确保代码可按真实性和保守性要求，对安全参数或其他有兴趣的值进行预测。验证提供的可信度应与分析的类型相适应。例如，对于严重事故分析中使用的程序，鉴于现有的实验数据有限，验证的范围可以放宽，在这种情况下，应更多地依靠核实（见第 5.14－5.20 段）。

5.23. 应执行计算机程序的验证，以评定程序预测的参数值中的不确定性。程序的输出应与相关的实验数据进行比较，如有可能，应与代表重要现象即将发生的运行瞬态数据进行比较。

5.24. 复杂分析中使用的计算机程序的验证应分两个阶段进行：开发阶段，由程序开发人员进行验证评定；而在独立评定阶段，验证评定应由程序用户执行。

5.25. 理想情况下，验证工作应该将程序输出与四种不同类型测试的结果进行比较：

(a) 基本测试：这些是简单的测试用例，可能与核电厂没有直接关系。这些测试可以具有分析解，或者可以利用实验中得出的数据或相关性进行核实；

(b) 单一效果测试：这些测试旨在突出核电厂可能发生的具体现象，但不涉及可能同时发生的其他现象。理想情况下，应执行全尺寸的单一效果测试。如果没有，则应适当注意可能产生的比例效应（见第 5.30－5.32 段）；

(c) 整体效果测试：这些是与核电厂直接相关的测试用例。要同时展示所有或大部分相关的物理过程。然而，与核电厂相比，这些测试可以小规模进行，可以使用替代材料，或者可以在不同的边界条件下进行；

(d) 通过运行瞬态进行核电厂级测试和验证：核电厂级测试是在实际核电厂上进行的，例如在试运行阶段。通过核电厂调试的运行瞬态进行验证，这是核电厂模型鉴定合格的重要手段。

5.26. 对照测试数据进行验证是验证工作的主要手段。但是，如果没有办法获得用于验证第 5.25(b)－(d) 段所述类型的测试的相应数据，可以通过程序对程序的比较或使用工程限定条件判断弥补在充分验证方面的局限性，以此来增强对结果的信心。验证所采用的方法和程序的使用应该是正确的。

5.27. 理想情况下，验证工作应涵盖计算机程序所建模型中使用的全部参数数值、条件和物理过程，在特殊的应用中这些参数都会使用到。

5.28. 程序用户的验证工作范围应与计算机程序的预期用途一致。验证的范围还应与程序的复杂性及其所表示的物理过程的复杂性相一致。

5.29. 对于复杂的应用程序，计算机程序可能以高精度预测一组测试数据，但对于其他数据集则不准确。对于这种情况，应该为程序的验证开发一个验证矩阵，这个矩阵是为即将验证的应用定制的。

5.30. 验证矩阵应包括来自不同实验设施和同一设施中不同条件组的测试数据，理想情况下应包括基本测试、单一效果测试、整体效果测试和核电厂级测试。在每一验证级别上选择的模型和相关假设应该彼此一致，并且对于不同类型的测试不应该不同。如果无法从全尺寸实验获得足够的数据，则应使用缩小尺寸实验的数据，并适当考虑缩放效应。从验证矩阵中测试的数量和选择可以判断，它足以满足计算机程序的预期应用。

5.31. 应在尽可能接近核电厂的条件下，确保计算机程序的验证，所以应确保每次测试的边界条件和初始条件都是适当的。如果使用与其他条件有关的数据，则应考虑缩比效应。缩比的实验设施不能用来展示与全尺寸设施相关的所有现象。因此，对于验证过程中使用的每个缩比试验设施，都应将正确展示的物理现象和非正确展示的物理现象一一识别出来。没有得到正确展示的物理现象的效应，应在考虑适当保守性的情况下，以其他方式进行处理。

5.32. 在对照实验数据进行验证时，所测量数据的不确定性公差，应纳入计算机程序不确定性的预测中。此外，基于缩比实验结果的不确定性评价应转移到实际电厂应用中，并且在评价结果的总体不确定性时，应评价并判断这种转移的合理性。

5.33. 应在验证报告中记录中明确经验证的计算机程序的有效性范围和局限性。

5.34. 验证工作的结果应该用于确定计算机程序计算结果的不确定性。对结果的不确定性的评定应该用不同方法。

5.35. 对于点数据，使用计算机程序计算的值与实验结果数值之间的差，既可以直接确定，或者在一组实验结果的情况下，通过使用描述性统计来确定。对于与时间相关的数据，至少应对不确定性进行定性评价。

5.36. 作为验证过程的结果，计算机程序计算中的不确定性和代码的验证范围应当是已知的，并且应当在诠释安全分析计算的任何结果时加以考虑。

5.37. 对于一个特定验收标准，计算机程序都应是趋于保守的，应当证明，与实验数据相比，该标准的程序预测是保守的（即，负面后果的预测比可能的实际后果差）。

5.38. 计算机程序产生的结果对用户做出的决策非常敏感，例如计算机程序中选择的模型以及节点使用的结构和数量。在结果不能与电厂数据或实验数据相比较的情况下，这种用户效应可能特别大。应仔细拟订和遵守规程、程序文档和用户指南，以尽量减少这种用户效应。例如，用户的规程应包括关于如何编译输入数据集？如何在程序中选择相应的模型以及如何准备节块化计算的一般规则等问题的指导。

5.39. 节块化工作应该足够详细，以展示假想方案中的所有重要现象和核电厂的所有重要设计特性。在进行核电厂分析时，对相同的假想方案应尽可能使用已经成功的与实验结果一致的合格的节块输出程序。当使用缩比试验来评定计算机程序时，应该使用与节块化一致的思想体系来进行测试和电厂的全尺寸分析。应对节块化结果进行足够的灵敏度分析，以确保计算结果没有不稳定的变化。

输入数据的鉴定

5.40. 计算机程序的输入数据包括展示全部或部分核电厂模型的表格。在如何进行电厂的建模和节块化时，通常具有一定程度的灵活性。用于执行确定性计算的输入数据应符合使用计算机程序的最佳实践指南（如《用户手册》中所示），并应进行独立检查。输入数据应是有效技术图纸、运行手册、规程、设定值列表、泵性能图、工艺流程图、仪器仪表图、控制图和其他电厂文件中的信息汇编。

计算机程序的文档

5.41. 每种计算机程序都应该有充分的文档记录，以便于模型和相关性运用的评审，并应保证重要现象的模型是适当的，并且保证模型的使用没有超出其有效性的范围。文档还应说明重要模型和在典型应用时，程序总体的不确定性。程序文档还应包括用户指南和输入说明，以确保用户能够正确使用程序。还应包括，程序中使用的实验数据或其他关键数据的说明、验证工作中所考虑的计算机选项的说明、以及对验证工作结果的说明。文件应向所有用户提供。

5.42. 尽管指南可能因为计算机程序的复杂性和用户可用的建模参数而变化，但用户指南或验证文档应就重要建模参数的影响、程序典型应用的建议、要使用的节块类型和预期的重要趋势向用户提供一些指导。通常，一套完整的文档将包括一份程序摘要、一份理论手册、一份用户手册和一份输入说明、一份程序员手册和一份验证报告。

5.43. 跟踪错误并报告其正确状态应该是一个连续的过程，并且应该是程序维护的一部分。应评定此类错误对已完成并用作电厂安全评定的一部分的分析结果的影响。

6. 确定性安全分析中确保安全裕量的一般方法

一般考虑事项

6.1. 确定性安全分析应表明，相关的安全要求已经得到满足，并且在实际可达到的重要参数的实际值与防止放射性物质释放的屏障失效的阈值之间存在足够的裕量（取决于电厂状态）。保守性可能以多种方式引入，例如在验收标准中，或者通过物理模型中的保守假设，以及在初始条件和边界条件中的保守假设。

6.2. 计算机程序预测中的不确定性应通过可适用的方法隐式考虑，或通过量化不确定性的最佳估算方法显式考虑（见第 2 部分表 1）。这对于极限工况（验收标准裕量最小的工况）尤为重要。

6.3. 为证明预计运行事件与验收标准的一致性，应考虑两种互补的办法：使用电厂控制和限制系统的真实方法（第 7.17－7.26 段）；和只使用安全系统的更保守的方法（第 7.27－7.44 段）。

6.4. SSR-2/1（Rev.1）[1]第 5.26 段指出（见本“安全导则”第 2.14 段）：

> “应以保守的方式分析设计基准事故。这种方法包括假想安全系统中的某些故障，规定设计标准，并在分析中使用保守的假设、模型和输入参数。”

6.5. SSR-2/1（Rev.1）[1]第 5.27 段指出，关于设计扩展工况的确定性安全分析，“可根据最佳估算方法分析确保安全壳功能的规定的有效性”（尽管可根据具体法规要求使用更严格的方法）。

6.6. 在采用最佳估算分析时，仍应确保屏障完整性丧失的充分裕量。敏感度分析应证明，陡边效应 [10]，可能导致早期放射性释放或大量放射性释放是能可靠避免的。在用于设计扩展工况的最佳估算分析的情况下，特别是对

[10] 在原子能机构《安全术语》[3]中，“陡边效应”的定义是“在参数发生小偏差或输入值发生小变化之后，设施的一种状态突然转变为另一种状态，造成严重异常情况的一种情况”。本定义中的“参数”一词可广义解释为可能影响设备或电厂性能的任何电厂物理变量、设计方面、设备状况或危害程度。

于严重事故而言，这一论证尤为重要，因为严重事故具有较高的屏障退化的可能性，从而导致早期放射性释放或大量放射性释放。

6.7. 应确定分析结果最敏感的参数。应通过对计算结果有重要影响的关键输入变量进行系统变化，来进行敏感性分析。这些分析应该用于确定对安全构成最大挑战的参数值，并证明在真实情况下，可预见的参数变化不会导致陡边效应。同时应该注意到，当通过一次改变一个参数进行灵敏度分析时，可能会得到误导性的结果，因为当多个参数同时改变时可能产生的补偿或累积效应不一定会反映出来。

6.8. 出于实际原因，在敏感性分析中只能考虑数量有限的参数——那些被确定为对结果有较大影响的参数。在给定范围内，这些参数的值的变化旨在识别导致所选验收标准裕量最小化的值，并且这些值依赖于标准。此外，任何参数的重要性在瞬态期间都可能发生变化。应注意避免选定参数的任意变化（其实这些参数是非独立的）而导致的数据不一致（如违反质量平衡）。

6.9. 确定性安全分析应包含一定程度的保守性，与安全分析的目标相称，并取决于电厂状态。关于对预计运行事件和设计基准事故的保守分析（见第2.14段），应考虑以下两种选项之一或两者的组合，而不是完全保守的方法：

(a) 结合保守的输入数据使用最佳估算计算机程序；

(b) 结合最佳估算输入数据使用最佳估算计算机程序，而不管其如何与程序模型和输入数据中的不确定性的量化相关联。

在前一种情况下，结果用一组参数的计算保守值表示，这组参数应由验收标准确定；在后一种情况下，结果用计算参数的百分比即概率分布表示。

6.10. 应仔细遵循规程、程序文档和用户指南，以限制用户在执行确定性安全分析时的影响。

6.11. 初始条件和边界条件的选择应考虑到核电厂几何图形的变化、燃料燃耗和与老化有关的变化，例如锅炉或蒸汽发生器的结垢。

预计运行事件和设计基准事故确定性安全分析的保守方法与组合方法

6.12. 在保守方法或组合方法中，保守的初始条件和边界条件应在电厂运行限值和工况规定的参数范围内选择（见第 2 部分表 1）。初始条件的例子是反应堆功率水平、功率分布、压力、温度和一回路中的流量。边界条件的例子是诸如电厂系统泵和电源的驱动定值和性能特性，质量与能量的外部源和阱，以及其他在瞬态过程中变化的参数。关于系统可用性和运行人员行动的保守性假设及其选择将在第 7 部分中针对个别电厂状态单独讨论。

6.13. 输入数据和建模假设的选择不仅应考虑预计运行事件和设计基准事故的中子物理学和热工水力方面，而且还应考虑辐射方面。特别是，为了分析向环境释放的源项，应考虑以下因素：

(a) 燃料（堆芯或乏燃料池）中裂变产物和其他放射性核素的存量；
(b) 反应堆冷却剂系统中的放射性活度，包括在事件（尖峰释放）发生之前或事件发生期间挥发性裂变产物的释放；
(c) 燃料损坏的时间进程和范围（包壳泄漏）；
(d) 燃料释放出的放射性核素份额；
(e) 放射性核素在一回路冷却系统和安全壳泄漏通道中的滞留；
(f) 裂变产物在冷却剂的蒸汽相和液相之间的分配；
(g) 安全壳系统的性能（喷雾、通风、过滤、沉积和再悬浮）；
(h) 安全壳泄漏率和泄漏位置；
(i) 释放的时序和持续时间；
(j) 放射性物质的化学和物理形态的释放，特别是碘；
(k) 释放到环境中的有效高度，应该考虑释放的能量。

6.14. 当最佳估算程序与保守输入和假设结合使用时，应确保与最佳估算程序相关的不确定性由保守输入充分补偿。分析应包括程序验证、保守性的应用和敏感性研究的组合，以评价和考虑与程序模型有关的不确定性。这些研究可能因瞬态的类型而不同，因此应针对每个研究进行确定性安全分析。

6.15. 对于保守方法或组合方法，初始条件和边界条件设置，应导致安全相关参数值，与验收标准相比，更加保守的结果。单一的一组保守的初始条件和边界条件不一定会导致每个安全相关参数即验收标准的保守结果。因此，应根据具体的瞬态和验收标准，分别选择相应的保守初始条件和边界条件。

6.16. 在选择用于分析的保守输入参数时，应考虑以下因素：

(a) 有意的保守性可能并不总是导致预期的结果的保守性，例如，如果不同的假设会导致补偿效应和“抵消”保守性；

(b) 保守性的程度可以在事件过程中改变，一个假设可能不会在整个瞬态过程中持续处于保守状态；

(c) 使用一些保守的假设可能产生或误导不真实的事件预测序列和时间尺度序列；

(d) 如果基于工程判断来选择保守值，就会存在这样高风险，即这种选择未被用户正确地进行，且不会导致保守的结果。

因此，应进行灵敏度计算，以支持为每个验收标准保守地选择输入参数。同时也建议，至少在为特别重要的结果选定假想方案时，还应对最佳估算分析进行验证，对不确定性进行量化。

6.17. 由于使用保守的计算机程序可以隐藏某些现象的影响或显著改变它们的时间顺序，因此对这些现象的分析应以适当的敏感性分析进行增强和补充，以证明保守程序并没有隐藏重要的安全问题。

6.18. 在保守的安全分析中，根据灵敏度分析，应使用在电厂寿命期内预计最受限制的初始条件。如始发事件，应考虑假设在反应堆初始工况不利的时刻发生，比如整处于功率运行或停堆的电厂模式，包括功率水平、余热水平、裂变产物存量、反应性条件以及反应堆冷却剂系统温度、压力和存量。

6.19. 不能同时发生的初始条件组合不需要在分析工作中考虑。例如，限制衰变热和限制峰值因子根本不能同时发生在燃料的运行活动中。然而，所考虑的初始条件应包括可能出现的最不利的组合。

6.20. 在选择保守初始条件时，可忽略低频率发生的且持续时间非常有限的运行条件可能不需要考虑。

对预计运行事件和设计基准事故不确定性量化条件下的最佳估算确定性安全分析

6.21. 不确定性，特别是预计运行事件和设计基准事故的不确定性，可以在确定性安全分析中通过使用最佳估算计算机程序来解决，其中需要考虑模型、初始条件和边界条件以及其他输入参数中的不确定性。为了获得保守的安全分析结果，应确定和评定这些不确定性对结果的影响，以验证实际电厂参数将限制在计算结果的上限和下限之间，并具有足够的置信度。

6.22. 在对不确定性进行量化之前，应确保：用于分析的最佳估算计算机程序得到充分验证；用户的影响已适当考虑（例如，值的选择可能不当）；计算平台（硬件和软件）对计算结果的影响已降至最低；评定不确定性的方法已验证合格。

6.23. 必须对不确定性进行可靠的评定，以便进行稳健的“不确定性的量化条件下的最佳估算”分析，特别应该识别和区分偶然性和认知上的不确定性来源 [11]。在进行不确定性分析时，应区别对待这些不同来源的不确定性。程序与数据的比较是量化认知不确定性的首选方法。不管怎样，敏感性研究、程序间比较和专家判断的组合也是可用作评定输入的（GSR Part 4（Rev.1）[2]第 4.59 段）。对偶然不确定性评价的首选方法是收集与所评定事件有关的核电厂初始条件和边界条件相关的数据。

6.24. 不确定性的量化应基于电厂工况和计算机程序模型中不确定性的统计组合（见第 2.7 段），以确保在规定的概率下，有足够多的计算结果符合验收标准。为了分析预计运行事件和设计基准事故，通常要求保证提供 95%或更高的置信度，使得至少 95%的结果符合电厂适用的验收标准。但，无论如何，国家法规都可以要求不同的概率水平。

6.25. 在所考虑的不确定性方法中，不确定性既可以使用输入不确定性的传播也可以使用输出不确定性的外推来评价。在前一种方法中，通过改变不确定的输入参数，并进行大量的计算，来评价输出中的总体不确定性。在后

[11] 偶然不确定性是一种现象所固有的不确定性，与随机发生的事件或现象有关，例如设备项目的随机故障。认识论上的不确定性是指由于对一种现象的认识不完整而导致的不确定性，这种不确定性会影响对其建模的能力[3]。

一种方法中，通常基于输出（计算结果）与实验数据之间的比较来评价输出的总体不确定性。

6.26. 对于“输入不确定性的传播”方法，不确定输入参数的变化应至少包括最重要的输入参数。应根据相关实验、参数测量、电厂运行参数记录或其他相应来源，给选定输入参数的值指定范围和概率分布。如果这不可行，则应使用该范围内的保守值。选定的输入参数既可以相互独立，也可以是对不确定输入参数之间的依赖关系的识别和量化；应对这些结果进行具体处理。

6.27. 不确定输入参数的选择变化以及概率分布对于结果的可靠性至关重要，因为它们强烈地影响结果的不确定带的宽度，而这对于工程应用是至关重要的。

6.28. 通过使用来自输入参数集合和相应输出值的回归或相关技术，“输入不确定性传播”的不确定性方法，允许根据不确定输入参数对输出不确定性的贡献对其进行排序。这种排序表明哪些参数应得到最大的关注。然而，应当考虑到，回归或相关技术也可能给出不清楚或误导的结果，特别是在响应不是线性的或相关效应重要的情况下。

6.29.与计算机程序的结果相关的参数中的不确定性，专家可借助对所分析的每个事件的“现象识别和排序表”进行判断，并以此进行不确定性的估算。每个表都应尽可能根据现有数据，确定必须确保程序适当性的最重要现象。重要参数应根据各自的概率分布随机变化，以估算总体不确定性。相同的过程可以用来评价计算机程序或计算工具模拟选定事件的适用性。

7. 不同电厂状态的确定性安全分析

一般考虑事项

7.1. 确定性安全分析应处理与不同电厂状态相对应的假想始发事件和事故序列，并应遵循第 4－6 部分所论述的一般规则，对验收标准、计算机程序使用和不确定性处理并确保安全裕量的建议方法进行选择。

7.2. 如本部分所述，在分析的目标、验收标准的选择、电厂各系统的可用性的考虑、运行人员的行为、不确定性的处理以及针对各个电厂状态的分析的其他假设等方面，还应遵循更具体的指导进行确定性安全分析。在确定性

安全分析中，应只考虑满足与相关电厂状态相关要求的结构、系统和部件，并考虑其应有的安全分类（见原子能机构《安全标准丛书》第 SSG-30 号《核电厂结构、系统和部件的安全分级》[20]）。

7.3. 在进行确定性安全分析时，关于保守程度的决策应包括以下方面的数据输入或假设：

(a) 计算机程序模型；
(b) 电厂运行参数；
(c) 控制和限制系统；
(d) 能动安全系统；
(e) 非能动安全系统；
(f) 设计扩展工况的安全特性；
(g) 运行人员行动。

7.4. 对源项有影响的现象的每种故障，应分别进行源项分析。典型的故障包括：

(a) 反应堆冷却剂和裂变产物从堆芯释放到安全壳的冷却剂丧失事故；
(b) 安全壳旁通事故或安全壳以外发生的事故，如乏燃料池内发生的事故；
(c) 辐照后燃料操纵过程中的事故；
(d) 放射性气体和液体废物处理和贮存系统的事故排放。

7.5. 对于许多类型的假想事故，放射性核素的重大释放都是从反应堆堆芯释放到反应堆冷却剂系统中，然后再释放到安全壳中的。因此，对源项的评价应包括对放射性核素通过这一途径直至其释放到环境中行为的预测。

正常运行的确定性安全分析

分析的具体目标

7.6. 正常运行的确定性安全分析应使用迭代过程来支撑运行限值和工况的开发，并验证其充分性。应借助过程变量值、系统要求、监视或试验要求来表示运行的限制条件。

7.7. 正常运行确定性安全分析中使用的限值和工况，如反应堆功率和冷却剂装量这类的变量，都应包括所有重要的初始条件和边界条件，这些数据在随后的预计运行事件分析、设计基准事故和设计扩展工况的分析中都将被使用。

7.8. 应分析所有正常运行模式和运行限值和工况所涵盖的相关电厂配置，特别注意相关的瞬态，如反应堆功率的变化、反应堆从功率运行停堆、反应堆启动、反应堆冷却、半环路运行以及新燃料和辐照燃料的装卸，包括将辐照燃料从反应堆卸载到乏燃料水池和将燃料装载到堆芯。

7.9. 正常运行的确定性安全分析应包括对核电厂放射性状态的分析并估算放射性物质向环境释放。这些是确定核电厂工作人员、公众和核电厂周围非人类生物群所受辐射剂量的必要输入。由于放射性分析的复杂性，特别是其对电厂运行的总体组织的强烈依赖性，关于正常运行状态下，核电厂放射性状态的分析和估算，本“安全导则”中没有提供相应的指导（例如，见GSG-10[5]）。

验收标准

7.10. 确定性安全分析应对电厂的正常运行评定，以确定电厂是否能够以参数值不超过运行限值和条件的方式运行。正常运行时的设计评定应核实，根据运行限值和条件定义，所有的运行模式，在所有瞬态过程中，都将避免反应堆停堆或启动限制和安全系统。另外，像运行导则所预期的从一种运行状态向另一种运行状态的过渡也应该在正常运行的设计评定中核实。

7.11. 正常运行的安全分析应包括对电厂总体设计和运行的分析：预测工作人员和公众可能受到的辐射剂量；评定这些剂量低于剂量限值（见SSR-2/1（Rev.1）[1]要求 5）；并确保这些剂量满足合理可行尽可能低的原则。然而，本“安全导则”未涵盖符合放射性验收标准的情况（见 GSR Part 3[4]和 GSG-10[5]）。

系统可用性

7.12. 对正常运行进行确定性分析的系统应限于正常运行系统，包括电厂控制系统。在正常运行模式相关的瞬态期间，不应启动其他电厂系统。

运行人员行动

7.13. 根据正常运行程序而执行的计划的运行人员行动应计入正常运行时的确定性安全分析中。

不确定性的分析假设与处理

7.14. 对正常运行的分析应能真实地反映电厂的行为。然而，应考虑系统性能方面的不确定性，包括仪器仪表测量和控制以及机械系统方面的不确定性，以便评定现有技术规定的充分性。

7.15. 根据运行限值和条件，所考虑的初始条件应代表所有预期和授权的电厂模式。所用参数的边界值应考虑参数的整个可接受范围。

7.16. 当剂量预测存在不确定性时，应做出保守的假设。这方面的详细指导超出了本“安全导则”的范围。

预计运行事件现实的确定性安全分析

分析的具体目标

7.17. 对预计运行事件，现实的确定性安全分析的主要目的是核实电厂的运行系统（特别是控制和限制系统）能够在宽泛的区间内防止预计运行事件演变成事故工况，并且电厂能够在预计运行事件发生后恢复正常运行。现实分析的目的就是为真实的始发事件提供电厂响应。

7.18. 分析中所考虑的假想始发事件及其所属预计运行事件的类别应包括电厂寿命期间可能发生的所有事件。对于许多假想始发事件，控制和限制系统，结合电厂的固有特性和运行人员行动，将弥补事件的影响，从而不会导致反应堆停堆，也不会对安全系统提出其他响应的要求。在这种情况下，错误纠正后可以继续运行。

7.19. 通常，预计运行事件不应导致对安全设备造成任何不必要的挑战，这些安全设备主要是设计用于在发生设计基准事故提供保护的。因此，建议在分析中证明，如果电厂控制和限制系统按预期运行，它们将能够阻止安全系统的驱动需求。然而，必须认识到，一些预计运行事件本身需要启动安全系统。

验收标准

7.20. 对预计运行事件的现实分析旨在证明，预计运行事件不会对任何物理屏障（燃料基质、燃料包壳和反应堆冷却剂压力边界或安全壳）或对安全相关系统造成任何潜在的损坏。此外，它们应力求尽可能核实反应堆停堆和安全系统没有启动。

7.21. 对预计运行事件的现实分析也想另外证明，当控制和限制系统可用时（例如，安全阀不启动），特定设计标准是可以满足的，它比保守分析预计运行事件的验收标准更加严格。

7.22. 防止物理屏障的失效通常通过风险保障（对于轻水堆）进行处理，所述保障在 95%置信度下具有 95%的概率，在堆芯中的任何地方都不会发生临界沸腾或烧干，在堆芯中的任何地方都不会发生燃料熔化，并且反应堆冷却剂系统和主蒸汽系统中的压力不会显著（即超过 10－15%）超过设计值。

7.23. 任何预计运行事件对核电厂附近以外的地区造成的辐射影响应可忽略不计。对剂量的放射性验收标准和每次预计运行事件相应的放射性释放应与正常运行的年度限值相当并且比设计基准事故更严格。可接受的有效剂量限值与正常运行的剂量限值相似。

系统可用性

7.24. 为了对预计运行事件进行现实分析，应该假想任何不受假想始发事件影响的系统都可用。分析应主要依靠控制和限制系统，以及固有的电厂特性。

运行人员行动

7.25. 根据正常和异常运行规程执行的计划运行人员行动应计入预计运行事件的现实分析中。通常，当假定控制和限制系统正确运行时，在相关联的瞬态期间就不在需要任何运行人员行动；否则，应对运行人员行动时间进行真实的估算。

不确定性的分析假设与处理

7.26. 对预计运行事件的现实分析应采用最佳估算方法，涵盖在确定假设始发事件时考虑的电厂的预期初始条件。通常，在实际分析预计运行事件时不考虑不确定性。出于运行考虑（例如电厂可靠性分析），不确定性的处理可以应用于控制和限制系统。

预计运行事件和设计基准事故的保守确定性安全分析

分析的具体目标

7.27. SSR-2/1（Rev.1）[1]第 5.26 段指出“应以保守的方式分析设计基准事故”。因此，应使用第 2 部分表 1 中的选项 1—3 保守的方法 [12] 中的一个；现实分析方法不应在设计基准事故使用。对预计运行事件和设计基准事故的保守分析应证明，只要满足以下安全条件，单一安全系统在短时间内或者连同运行人员行动一起在长期时间内系统能够达到安全状态：

(a) 在预计运行事件或设计基准事故工况期间和之后，停堆并达到次临界状态；

(b) 在所有预计运行事件或设计基准事故工况导致的反应堆停堆后排出堆芯的余热；

(c) 减少放射性物质释放的可能性，并确保在预计运行事件和设计基准事故工况过程中，任何释放都低于可接受的限值。

7.28. 安全分析应证明与适用事件相关的验收标准是可以满足的。特别是，应当表明，阻止放射性物质从核电厂释放的大部分或所有屏障都保持其所需程度的完整性。

7.29. 安全分析应规定安全系统和运行规程的性能特点和设定值，以确保基本的安全功能始终得以保持。该分析为反应性控制系统、反应堆冷却剂系统和专设安全设施（如应急堆芯冷却系统和安全壳排热系统）的设计提供了基础。

---

[12] 术语“保守方法”和“保守分析”应理解为指第 2 部分表 1 和第 2.14 段中的选项 1—3 中的任一选项。

验收标准

7.30. 为了保守地分析预计运行事件，与燃料完整性和放射性验收标准有关的技术验收标准原则上应与预计运行事件现实分析的技术验收标准相同。

7.31. 在预计运行事件或设计基准事故出现时，核电厂附近不应有或仅有轻微的放射性影响，无需采取任何厂外防护行动。轻微放射性影响的定义应由监管机构制定，但核电厂附近以外公众的可接受有效剂量限值通常为每次事件几毫希沃特。

7.32. 应确定具体的技术验收标准，以便能够证明在任何情况下都能确保这三项基本安全功能，并且在预计运行事件或设计基准事故中，大部分或全部屏障能够限制放射性物质向环境的释放。

7.33. 技术验收标准通常应包括以下内容：

(a) 如果不发生进一步的独立故障（加上满足任何单一故障标准的任何单一故障），任意一个事件不应产生更严重的电厂工况。因此，预计运行事件本身不应产生设计基准事故，设计基准事故不应产生设计扩展工况；

(b) 虽然安全系统可能部分地受到假想始发事件的影响，但不会因此而丧失缓解事故后果所必需的安全系统的总体功能；

(c) 用于缓解事故的系统应能承受所分析事故的最大载荷、应力和环境条件。这应通过分别分析环境条件和老化（如温度、湿度、辐射或化学环境）以及电厂构筑物和设备的热载荷和机械载荷来证明。设计中对于给定载荷所考虑的裕量应与载荷的概率相称；

(d) 根据超压保护规则，反应堆和主蒸汽系统中的压力不应超过现有电厂工况下相关设计的限值。为研究电厂工况对安全阀和卸压阀的影响，可能需要进行额外的超压分析工作；

(e) 对于每种假想始发事件，应限制燃料包壳破损的数量，以满足全球放射性标准，并将辐射水平限制在设备鉴定使用的标准以下；

(f) 对于燃料的裸露和加热的设计基准事故，应保持燃料组件（轻水堆）可冷却的几何形状和结构完整性；

(g) 任何事件都不应导致安全壳隔间之间的温度、压力或压差超过安全壳设计基准；

(h) 应保持停堆后反应堆内、新燃料贮存池和乏燃料水池中核燃料的次临界状态。临界状态的暂时恢复（例如，压水堆中的蒸汽管线破裂）对于特定事件和电厂运行模式可能是可接受的，前提是继续满足对燃料充分冷却的标准要求；

(i) 对于任何假想的设计基准事故，在电厂设计寿期内，反应堆压力容器不应存在引发脆性断裂或塑性破坏的假想缺陷；

(j) 在设计基准事故期间，反应堆内部部件应承受动态载荷，以维持反应堆安全停堆、反应堆次临界和堆芯的充分冷却。

7.34. 当任何屏障的完整性出现缺失或降级时（如反应堆打开、安全壳打开的情况或在乏燃料水池中发生的事件），此时发生的假想始发事件，应使用更严格的验收标准（如避免冷却剂沸腾或燃料裸露）。

系统可用性

7.35. 在分析电厂系统的可用性时通常应包括以下保守假设：

(a) 在假想始发事件开始时正在运行的正常运行系统，如果不受始发事件本身及其后果影响，应继续运行；

(b) 任何控制或限制系统只有在其功能会加重始发事件的影响时才开始运行。不应将始发事件影响的缓解归于控制系统的运行；

(c) 按照安全等级（根据质量保证、定期试验、设计规范和设备鉴定）设计和维持的安全系统应以保守的性能运行（见第 7.42 段）；

(d) 根据单一故障标准，除了始发故障和任何后果性故障之外，还应假想一个单一部件在始发事件触发的一组安全功能投入时发生故障。根据选定的验收标准，应假想单一故障发生在对安全系统造成最大挑战的系统或部件上；

(e) 为设计扩展工况而专门设计的安全设施不应计入分析中。

7.36. 如果允许对系统进行维护，则安全系统的相关系列不可用性应加以考虑。

运行人员行为

7.37. 为了安全分析的保守性，在经过规定的保守时间之前，不应在确定性分析中考虑运行人员对事件的诊断和采取的必要行动。应对每种特定反应堆设计，在分析中所假定的运行人员免干预时间的合理性进行判断并加以验证；例如，控制室免干预的指定最少时间可能是 30 分钟，或者现场行动的指定最少免干预时间可能是 60 分钟。

7.38. 必须有证据表明事件序列和电厂特定边界条件允许执行假想的行动时，才能在分析中考虑电厂工作人员为预防事故或缓解其后果而采取的正确行动。所要考虑的工况应该包括事件序列发生的前后次序、总体背景、控制场所的工作环境、可用的程序以及相关工作人员的培训状况和必要信息的获取。

7.39. 根据一些国家的实践经验，在执行恢复行动期间发生的额外的一个运行人员错误可被视为单一故障。

不确定性的分析假设与处理

7.40. 用于分析预计运行事件和设计基准事故的保守假设应考虑到初始条件和边界条件、电厂系统可用性和运行人员行动中的不确定性。第 6 部分中陈述的一般规则应完全适用于这类情况的电厂状态。其目的是以高的置信度证明安全限值有足够的裕量。

7.41. 预计运行事件的保守分析应包括与设计基准事故确定性分析中相同的保守假设，特别是那些假想始发事件期间用于维持安全功能的系统的保守假设。

7.42. 如果采用保守方法或组合方法，无论哪个给定验收标准更保守，都应假想安全系统在其最低或最高性能水平之间运行。对于反应堆停堆和安全系统的驱动系统，应假定触发动作发生在可能条件范围的最差的区间。如果采用最佳估算加上不确定性方法，则应将安全系统性能的不确定性纳入系统的总体不确定性分析中。

7.43. 除了假想始发事件本身之外，失去厂外电源也可被视为附加的保守假设。如果这种丧失被看作额外的故障，则可以假定其发生在对屏障完整性

具有最大负面影响的时间；在这种情况下，应调整一些验收标准，同时考虑到这种组合的概率。

7.44. 根据确定性安全分析的一般规则，预计运行事件和设计基准事故的源项评价应考虑事故期间发生的所有重要物理过程，并在电厂特定基础上使用初始数据和系数的保守值。

无明显燃料破损的设计扩展工况的确定性安全分析

分析的具体目标

7.45. 对无明显燃料破损的设计扩展工况进行安全分析的目的是证明，可以以足够的置信度防止堆芯熔化，并且有足够的裕量来避免所有陡边效应。

验收标准

7.46. 设计扩展工况的验收标准应符合 SSR-2/1（Rev.1）[1]第 5.31A 段指出，即：

> “设计必须做到，对于设计扩展工况，通过限制时间长度和适当区域这类的防护行动就足以保护公众，并必须为采取这类措施提供充足的时间。”

在切实可行的范围内，可考虑采用与设计基准事故相同或相似的技术和放射性标准应对这类工况。应合理可行尽可能低地将放射性释放降至最低。

系统可用性

7.47. 一般而言，只有在这类设计扩展工况下可运行的系统才应计入确定性安全分析中。

7.48. 在分析时，不受无明显燃料破损序列的设计扩展工况中假想故障影响的安全系统可以计入分析中。在假想故障（如内部水淹）条件下，评定安全系统独立性时，应特别注意影响安全系统（如地坑滤网堵塞）和支持系统（如电气、通风和冷却）的其他因素。

7.49. 对于无明显燃料破损的设计扩展工况，不需要应用单一故障标准。此外，由于维护导致的这类设计扩展工况的安全设施的不可用，在分析时可以不需要考虑。

7.50. 为了确保纵深防御层级之间的独立性，在分析设计扩展工况时，不应将正常运行系统，包括控制和限制系统，计入无明显燃料退化的设计扩展工况的分析中。这是因为：

(a) 一个给定的序列有可能覆盖几种假想始发事件，并且考虑到假想始发事件的起源和多重故障，可能难以证明运行系统总是可用的；

(b) 这些序列通常会造成室内封闭条件的破坏，分析中所考虑的系统应能充分满足这些条件。

但是，如果正常运行系统对事故过程有负面影响，则应予以考虑。

7.51. 在证明核电厂设计的符合性时，不应考虑非永久性设备。这类设备通常被视为长期序列运行的，并假设按照应急运行规程或事故管理导则获取这类设备。要求提供非永久性设备的时间应该是合理的。[13]

运行人员行为

7.52. 对于设计扩展工况安全分析中运行人员的行为，可以使用最佳估算假设。然而，针对设计基准事故所说明的一些保守假设，可以在可行的范围内使用。

不确定性的分析假设与处理

7.53. 那些针对设计基准事故而规定的计算机程序的选择、验证和使用要求，原则上可适用于无明显燃料破损的设计扩展工况的分析。

7.54. 对于无明显燃料破损的设计扩展工况，像适用于设计基准事故一样，原则上可以使用组合方法或具有不确定性量化（最佳估算加不确定性）的最佳估算方法。然而，在考虑第 7.55 段和第 7.67 段所述的注意事项和条件下，

[13] 一些国家目前的做法是，在安全分析中考虑非永久性设备的可用性，例如，设备在现场贮存 8 小时后，或设备在厂外贮存 72 小时后。

根据设计扩展工况分析的一般规则，也可采用没有不确定性量化的最佳估算分析。

7.55. 当进行最佳估算分析时，应证明避免出现陡边效应的裕量是足够的。这是可以做到的。例如，可以通过敏感性分析证明，在可行的范围内，当对支配性参数做出更保守的假设时，物理屏障完整性的丧失仍有裕量。

堆芯熔化设计扩展工况的确定性安全分析

分析的具体目标

7.56. 对严重事故的分析应确定由假想的堆芯熔化序列产生的电厂边界参数，并证明：

(a) 电厂可以回到安全壳密封功能长期保持的状态；

(b) 电厂结构、系统和部件（例如安全壳）和规程能够防止大量放射性释放或早期放射性释放，包括安全壳旁通；

(c) 控制区仍然适宜居住，以便执行必要的工作人员行动；

(d) 计划的严重事故管理措施是有效的。

7.57. 对严重事故的安全分析应表明，通过设计实施的电厂特性结合事故管理程序或导则的实施可以实现对验收标准的符合。

验收标准

7.58. 放射性验收标准，通常用公众剂量（或释放到环境中的剂量）进行表达，严重事故分析时则应代表这样的剂量水平，即，只需要在厂外采取限制时间长度和适当区域的有限的防护行动，并且有足够的时间实施这些行动，尽早使其生效。

7.59. 技术验收标准应代表保持安全壳完整性的工况。用于分析设计扩展工况的验收标准指标，例如，可包括，限制安全壳压力、安全壳水位、温度和可燃气体浓度以及熔化堆芯熔渣的稳定性。

7.60. 现场放射性验收标准应确保控制区域（即控制室、辅助控制室和其他应急响应设施和地点）以及用于在它们之间进行活动区域的可居住性。特别是，现场控制区域的辐射水平（如环境剂量率和空气中的放射性浓度）应按

照 GSR Part 7[8]要求 11 和 24，对其使用者，如应急工作人员提供充分的保护。

系统可用性

7.61. 在分析严重事故时，不应计入安全系统，除非以合理的可信度表明：

(a) 这些安全系统的故障不是严重事故序列所要涵盖任何假想方案的一部分；

(b) 在履行其预期功能所必需的一段时间内，该设备将在实际严重事故工况下存续。

7.62. 假设在严重事故工况下运行的设备，其可用性的考虑事项应包括：

(a) 适用的始发事件的前后原委和周边情况，包括由外部危害（如全厂断电和地震）造成的情况；

(b) 需要设备的环境（如压力、温度和辐射）和时间区间。

7.63. 对于堆芯熔化的设计扩展工况，不需要采用单一故障标准。此外，在确定性安全分析中不需要考虑由于维护而导致的系统或部件的不可用性。应为应对设计扩展工况所必需的系统或设备，其相应的试验和维护规则应该予以明确，以确保其可用性。

7.64. 在证明核电厂设计的符合性时，不应考虑非永久性设备。对于某些设计扩展工况，此类设备通常被认为是长期序列运行的，并假定应按照应急运行规程或事故管理导则获得此类设备。要求获得此类非永久性设备的时间应该是合理的。[14]

运行人员行为

7.65. 对堆芯熔化设计扩展工况下，运行人员行为的假设应与无明显燃料破损设计扩展工况下的运行人员行为的假设一致（见第 7.52 段）。

[14] 一些国家目前的做法是，在安全分析中考虑非永久性设备的可用性，例如，设备在现场贮存 8 小时后，或设备在厂外贮存 72 小时后。

不确定性的分析假设与处理

7.66. 除了在无堆芯熔化工况下发生的中子和热工水力现象之外，严重事故分析还应模拟堆芯破坏后可能发生的并且可能导致放射性物质释放到环境中的宽泛的物理过程。这些过程应酌情包括:

(a) 堆芯分裂过程和燃料熔化；
(b) 燃料－冷却剂相互作用（包括蒸汽爆炸）；
(c) 堆内熔融物的滞留；
(d) 压力容器熔穿；
(e) 安全壳直接加热；
(f) 一回路内的热量分布；
(g) 氢气的产生、控制和燃烧；
(h) 安全壳失效或旁通；
(i) 堆芯熔渣－混凝土相互作用；
(j) 裂变产物的释放和输运，包括通风，以防止安全壳内的超压；
(k) 压力容器内堆芯熔融物和压力容器外堆芯熔融物的冷却能力。

7.67. 对严重事故的分析应尽可能采用现实方法（第 2 部分表 1 选项 4）进行。由于现象的复杂性和实验数据的不足，不确定性的显式量化可能是不现实的，因此应进行灵敏度分析，以证明严重事故分析结果和结论的稳健性。

为支持“实际已消除”出现的可能导致早期放射性释放或大量放射性释放工况可能性的确定性安全分析

7.68. SSR-2/1（Rev.1）[1]第 5.31 段指出，“设计应使能够导致早期放射性释放或大量放射性释放工况的可能性‘实际已消除’”。监管机构可制定更具体的规则，说明证明“实际消除”的可接受方式。

7.69. “实际消除”能够导致早期放射性释放或大量放射性释放工况的可能性的论证应包括确定性的考虑和工程方面，例如结构、系统和部件的设计、制造、试验和检查，以及对运行经验的评价，并辅之以概率性考虑，同时应考虑由于对某些物理现象了解有限而产生的不确定性。

7.70. “实际消除”可能导致早期放射性释放或大量放射性释放工况的论证应酌情包括以下步骤：

(a) 识别可能危及安全壳完整性或安全壳旁通，导致早期放射性释放或大量放射性释放的工况；

(b) 执行设计和运行技术规定，以便“实际消除”出现这些工况的可能性。这些技术规定的设计应包括应付不确定性的足够裕量；

(c) 通过确定性安全分析、概率安全评定和工程判断，最终验证技术规定的充分性。

7.71. 虽然可以设定概率目标，但“实际消除”可能导致早期放射性释放或大量放射性释放工况的论证不应仅以低概率值为基础。此类事件序列应进行确定性定义，并应基于，安全特性的执行使事件序列极不可能出现，证明其“实际消除”。

7.72. 如果声明可能导致早期放射性释放或大量放射性释放的工况根本不可能发生，则有必要检查系统的固有安全特性，以证明根据自然法则，这些工况不可能发生，并且将实现基本的安全功能，即控制反应性、排出热量和隔离放射性物质，包括限制意外放射性释放（见 SSR-2/1（Rev.1）[1]要求 4）。在实践中，这种方法仅限于非常具体的情况。其使用的一个示例是反应性失控事故，通常通过负反应性系数为这类事故提供主要保护，而负反应性是由反应堆功率和冷却剂压力及温度的所有可能组合来保证的。

8. 确定性安全分析的记录、评审和更新

记录

8.1. GSR Part 4（Rev.1）[2]第 4.62 段指出，“安全评定的结果和结论应酌情以安全报告的形式加以记录，以反映设施或活动的复杂性及其相关的辐射风险。”GSR Part 4（Rev.1）[2]第 4.64 段指出，“安全报告应充分详细地记录安全评定，以支持得出的结论，并为独立核实和管理评定提供充分的输入。”

8.2. 虽然安全报告本身应足以满足这些目的，但通常还有其他文件，其中可包括确定性安全分析的说明和结果，也作为独立核实或管理评定的辅助

信息。类似于安全报告编写的规则可适用于所有拟提交给监管机构的确定性安全分析文件。

8.3. 安全报告应提供确定性安全分析中所考虑的所有核电厂状态的清单，并根据其频率和所处理的防止放射性物质释放的物理屏障完整性所面临的具体挑战进行适当分组。每个组中极限假想方案的选择应该是合理的。应证明能够导致早期放射性释放或大量放射性释放工况发生的可能性“实际消除”了。

8.4. 考虑进行确定性安全分析的独立核实或评价所必需的数据要求，应在安全报告的独立部分或单独的文件中，提供用于电厂模型开发的最重要的电厂数据（实际上是“确定性安全分析数据库”）。此类数据应包括关于反应堆的几何形状、热工参量和水力参数、材料特性、控制系统和系统定值的特性以及电厂仪器仪表测量装置中的不确定性范围，并应包括相关图纸和其他图形文档。如果这些数据在安全报告本身中没有得到充分的记录和证明，则应在安全报告中明确标识和引用用于准备电厂模型的其他可靠数据源。

8.5. 应简要说明确定性安全分析中使用的计算机程序。除了提及具体的程序文件外，该说明还应包括证明该程序适合给定目的的理由，并已通过用户的核实和验证（见第 5.14—5.39 段）。

8.6. 根据模拟的现象和每个分析假想方案的其他特点，应为每种假想方案选择一个相关的验收标准或一组标准，并与该假想方案的安全分析一起提供，同时明确说明标准适用的工况（见第 4 部分）。

8.7. 为了证明安全分析对每个特定验收标准符合性，应详细说明分析中使用的仿真模型和主要假设，包括模型的验证范围。每个电厂状态所使用的不同方法应予以说明（见第 6 部分）。

8.8. 如果确定性分析涉及了不同的计算机程序的顺序使用，则事故分析不同阶段之间的数据传输和/或顺序使用的计算机程序之间的数据传输，应清楚地予以说明，作为独立核实、理解和接受结果的必要条件，提供计算的可追溯性。

8.9. 分析和提供的任何假想方案所涵盖的时间跨度应延至电厂达到安全和稳定的最终状态的那一刻（尽管不一定要提供整个时间尺度的所有灵敏

度计算）。应当界定安全和稳定的最终状态的含义。通常，假定当堆芯被覆盖且堆芯和安全壳两者的长期排热已经建立，同时堆芯处于并保持次临界状态且保有给定裕量时，即所谓达到安全和稳定的最终状态。

8.10. 确定性安全分析结果文件的应该是结构化的且格式合理，以便对事故过程提供明确的说明和解释。可采用标准化格式已处理类似的分析，以方便结果的解释和相互比较。

8.11. 确定性安全分析结果的文档通常应包括以下信息：

(a) 按主要事件的计算顺序对主要事件说明；
(b) 根据选定的参数对事故的说明和评价；
(c) 显示所计算的主要参量变化的图；
(d) 对所达到的安全水平的可接受性的结论和关于对所有相关验收标准符合性，包括裕量是否充足的说明；
(e) 尽可能提供的敏感性分析的结果。

8.12. 确定性安全分析的记录应遵循相关的质量保证程序和质量控制[12—14]。

8.13. 关于列入安全分析报告不同部分的确定性安全分析记录的更详细资料，见原子能机构《安全标准丛书》第 SSG-61 号《核电厂安全分析报告的格式和内容》[21]。

记录中的敏感信息

8.14. 应查明和适当保护确定性安全分析报告中的敏感信息，这些未经授权信息一旦披露可能危及核电厂安保。这可以包括但不限于，关于所进行的确定性安全分析的假想始发事件和结果的识别和分类的信息。这类信息应根据信息安全导则的要求加以保护[6]。

确定性安全分析的评审和更新

8.15. 根据 GSR Part 4（Rev.1）[2]第 5.10 段要求，许可证审批流程中使用的确定性安全分析应定期更新，以考虑到核电厂技术状态、电厂系统和设备特性、运行参数、电厂规程、研究结果的变化以及物理现象知识和理解方面

的进展，包括计算机程序的变化，这些变化都可能对分析结果产生重大影响。

8.16. 除了定期升版外，在发现任何自然灾害类型出现时，或原来的灾害发生的概率或等级大小比之前假定的更大时，也应更新安全分析。

8.17. 在这种情况下，应重新评定安全分析，以确保其仍然有效，并符合分析确定的目标。这些结果应根据目前有关确定性安全分析、适用的实验数据、专家判断和与类似分析的比较进行评定。

8.18. 重新评定的结果，包括新的确定性安全分析（如果是必须的），应反映在最新的安全分析报告中，文档变化的层级应与变化的程度和相关影响相对应。

9. 许可证持有者进行的确定性安全分析独立核实

9.1. GSR Part 4（Rev.1）[2]要求 21 规定，**“营运组织应在安全评定被营运组织使用或提交给监管机构之前对其进行独立核实。”**GSR Part 4（Rev.1）[2]第 4.66－4.71 段进一步说明了这种独立核实的目标和范围。

9.2. 许可证持有者（营运组织）对安全分析进行独立核实的主要目的，是验证安全分析，特别是其他团体或组织，例如设计方、制造商及建造商所编写的部分，已经以可接受的方式进行实施，并满足相关的安全要求。根据许可证持有者的主要安全责任，许可证持有者至少也要核实设计是否符合有关的法规要求，以及验收标准是否满足。

9.3. 在原子能机构《安全标准丛书》第 SF-1 号《基本安全原则》[22]第 3.6 段指出的责任中，许可证持有者负责“核实设施和活动及其相关设备的设计是否适当和质量是否合格”。应通过安全评定来证明设计的符合性。

9.4. GSR Part 4（Rev.1）[2]第 4.13 段明确指出，安全分析是安全评定的一个基本组成部分。因此，GSR Part 4（Rev.1）[2]的相关要求完全适用于作为安全评定的基本组成部分进行的确定性安全分析。

9.5. 在整个设计过程中，安全分析和独立核实由不同的团体或组织进行。它们是迭代设计过程的组成部分，目的是确保电厂满足安全要求。然而，独

立核实应由营运组织或代表营运组织进行，仅设计相关部分应提交给监管机构核准。

9.6. 根据 GSR Part 4（Rev.1）[2]第 4.67 段指出，营运组织应确保在确定性安全分析提交给监管机构之前，由具有适当资格和经验的个人或不同于进行原始安全分析的团体对其进行独立核实。即使部分工作委托给不同的组织，营运组织也要对独立核实负完全责任。

9.7. 进行独立核实的人员如果没有参加最初的安全分析，则视为独立人员。如果核实组是在同一个设计组织或另一个密切相关的组织中设立的，则应特别注意其独立性。最好的解决办法是使用完全独立的组织。

9.8. 应该在确定其核实程度和范围之前，对执行独立核实的团体考虑进行所有质量保证评审。

9.9. 应特别注意，对按照较宽松的标准建造的设计较旧的核电厂安全分析进行的独立核实，以及，对采用新颖设计解决方案的进化或创新性设计进行的独立核实。

9.10. 独立核实可按原安全分析方法进行。然而，独立核实的范围可能会更窄，侧重于最重要的安全问题和要求，而不是所有这些问题和要求。GSR Part 4（Rev.1）[2]第 4.68 段指出“关于独立核实的范围和详细程度的决定应在独立核实中加以评审”。

9.11. 虽然核实可以方便地细分，以便在设计的不同重要阶段执行核实，但当设计完成时，应始终由营运组织执行安全评定的最终独立核实。

9.12. 独立核实通常涉及电厂建设开始前的阶段，并侧重于最初由设计组织进行的安全分析。然而，同样的办法应适用于随后的其他核实活动。

9.13. 独立核实的任何结果、建议和一般性结论应酌情使用下列方法之一加以证明：

(a) 与法律、法规或其他法律要求的比较；
(b) 与监管机构的指导意见进行比较；
(c) 与原子能机构安全标准或指南进行比较；
(d) 与同类项目进行比较；

(e) 利用以往项目的一般经验；

(f) 独立的核实计算。

9.14. 安全分析中使用的所有数值模型的可靠性应通过比较、独立分析和鉴定来证明，以证明其固有的不确定性水平符合整个设计项目所要求的可靠性。

9.15. 根据 GSR Part 4（Rev.1）[2]第 4.69 段，独立核实应包括两个主要部分：侧重于安全分析的质量和全面性的全面（定性）评审；以及对分析重要方面的具体详细评审，其中可包括将提交的分析结果与新的独立计算结果进行比较。核实的组成部分应酌情包括：

(a) 符合参考文献的要求（见第 9.13 段）；

(b) 文档的完整性；

(c) 输入数据的正确性；

(d) 始发事件或事故假想方案的选择；

(e) 验收标准的选择；

(f) 安全分析方法的选择；

(g) 安全分析计算机程序的选择和程序验证的符合性；

(h) 为确保安全裕量的假设的选择；

(i) 分析结果的说明和评价是否充分。

9.16. 应对选定的计算机计算进行独立检查，以核实其正确性。如果没有对原始计算机程序进行充分的核实和验证，则应使用不同的程序来核实计算机计算的准确性。最好使用不同的计算机程序进行独立核实，但如果电厂模型（包括节块化、初始条件和边界条件）是独立开发的，则使用相同的程序也可以满足评审的目地。

9.17. 如果执行独立的计算，则合理地从每组始发事件中选择至少一个案例，通常是在验收标准方面裕量最小的案例。然而，必须考虑到独立计算是一项耗时耗资源的工作。

9.18. 通常，确定性安全分析的独立安全核实应验证：

(a) 安全分析是根据相关法规、安全标准和其他相关导则进行的；

(b) 所选择的假想始发事件或事故假想方案反映了给定设计的特定特性，并包络了其他情况；

(c) 将单一事件和后果性故障的识别进行了充分的结合；

(d) 安全分析中使用的计算机程序已经过充分的核实，并针对给定的应用进行了验证；

(e) 计算模型反映了其开发的经验和适用指南，适合于对运行状态和事故工况进行可靠地预测；

(f) 每项分析中已充分说明了使用的假设和数据，以表明符合相关的验收标准，并有足够的裕量来防止陡边效应；

(g) 提供足够的敏感性计算或不确定性评价，以确保通过安全分析进行的安全论证具有足够的稳健性；

(h) 针对电厂系统在不同电厂状态下的可运行性的安排符合确定性安全分析的既定规则，并符合工业标准；

(i) 只有在诊断、决定和执行所需行动的背景边界条件都具备的情况下，才能假定通过自动系统或人员行动实现对相关验收标准的符合；

(j) 独立计算与原始分析合理定性和定量一致，均证明满足相关验收标准；

(k) 在安全分析中发现的任何差异都得到清楚的理解和解释，而且并没有对关于设计可接受性的结论产生疑问。

9.19. 独立核实及其结果最好记录在一份单独的核实报告中，说明核实的范围、详细程度和方法，以及定性和定量评价的结果和结论，包括对安全评定各个部分和独立计算结果的详细评论。

9.20. 在设计阶段和整个电厂寿命期间，电厂设计模型和安全分析所必需的数据应保持最新。这应该是设计方在设计阶段和营运组织在整个电厂寿命期间的责任。建议集中维护相关文件或数据库，以确保所有评定人员、制作人员和评审人员使用相同的信息。

9.21. 在分享电厂数据方面，应通过适当的保密承诺，处理评定人员、作者和评审人员之间关于模型和其他专门知识的信息以及专有权的信息。

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《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）。

[3] 国际原子能机构《国际原子能机构核安全和辐射防护安全术语》（2018 年版），国际原子能机构，维也纳（修订版编写中）。

[4] 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）。

[5] 国际原子能机构、联合国环境规划署，《设施和活动的预期放射性环境影响评定》，国际原子能机构《安全标准丛书》第 GSG-10 号，国际原子能机构，维也纳（2018 年）。

[6] 国际原子能机构《核信息的安保》，国际原子能机构《核安保丛书》第 23-G 号，国际原子能机构，维也纳（2015 年）。

[7] 国际原子能机构《核电厂最佳安全分析评价：不确定性评价》，《安全报告丛书》第 52 号，国际原子能机构，维也纳（2008 年）。

[8] 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）。

[9] 联合国粮食及农业组织、国际原子能机构、国际劳工办公室、泛美卫生组织、联合国人道主义事务协调厅、世界卫生组织，《核或辐射应急准备的安排》，国际原子能机构《安全标准丛书》第 GS-G-2.1 号，国际原子能机构，维也纳（2007 年）。

[10] 联合国粮食及农业组织、国际原子能机构、国际劳工办公室、泛美卫生组织、世界卫生组织，《核或辐射应急准备和响应中使用的标准》，国际原子能机构《安全标准丛书》第 GSG-2 号，国际原子能机构，维也纳（2011 年）。

[11] 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）。

[12] 国际原子能机构《设施和活动管理系统的适用》，国际原子能机构《安全标准丛书》第 GS-G-3.1 号，国际原子能机构，维也纳（2006 年）。

[13] 国际原子能机构《核装置管理系统》，国际原子能机构《安全标准丛书》第 GS-G-3.5 号，国际原子能机构，维也纳（2009 年）。

[14] 国际原子能机构《安全的领导和管理》，国际原子能机构《安全标准丛书》第 GSR Part 2 号，国际原子能机构，维也纳（2016 年）。

[15] 国际原子能机构《核装置厂址评估》，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）。

[16] 国际原子能机构《核电厂设计中的非地震外部事件》，国际原子能机构《安全标准丛书》第 NS-G-1.5 号，国际原子能机构，维也纳（2003 年）。

[17] 国际原子能机构《核电厂设计中的内部火灾和爆炸防护》，国际原子能机构《安全标准丛书》第 NS-G-1.7 号，国际原子能机构，维也纳（2004 年）。（修订版编写中）

[18] 国际原子能机构《核电厂设计中除火灾和爆炸外的内部危害防护》，国际原子能机构《安全标准丛书》第 NS-G-1.11 号，国际原子能机构，维也纳（2004 年）。（修订版编写中）

[19] 国际原子能机构《核设施计算机的安保》，国际原子能机构《核安保丛书》第 17 号，国际原子能机构，维也纳（2011 年）。

[20] 国际原子能机构《核电厂结构、系统和部件的安全分级》，国际原子能机构《安全标准丛书》第 SSG-30 号，国际原子能机构，维也纳（2014 年）。

[21] 国际原子能机构《核电厂安全分析报告的格式和内容》，国际原子能机构《安全标准丛书》第 SSG-61 号，国际原子能机构，维也纳（修订版编写中）。

[22] 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）。

附件 I

确定性安全分析的应用

应用领域

I-1. 可以对一些应用进行确定性安全分析，包括：

(a) 设计方对核电厂的设计，或者营运组织对设计的核实；
(b) 为许可证审批目的（为授权）进行的安全分析，包括对新电厂的不同阶段进行授权；
(c) 监管机构对安全分析的独立核实；
(d) 在定期安全评审中更新安全分析，以确保最初的评定和结论仍然有效；
(e) 电厂改造的安全分析；
(f) 对实际运行事件的分析，或此类事件与超出正常运行限值的其他假设故障并发的分析（分析未遂事件）；
(g) 应急运行规程的编写和验证；
(h) 严重事故管理导则的编写；
(i) 成功标准的证明，以及一级和二级概率安全评定中事故序列的开发。

I-2. 可进行与核电厂（第 I-1(a)－(e) 段）的设计和授权（审批）有关的确定性安全分析，以证明符合既定的验收标准（以不同方式确保的设计基准事故和设计扩展工况的）并具有足够的安全裕量。运行事件分析、程序或导则制定以及概率安全分析相关的确定性安全分析（第 I-1(f)－(i) 段），通常不是为了证明符合验收标准，而是尽可能以现实的方式进行。

确定性安全分析在核电厂设计中的应用

I-3. 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 42 和第 5.71－5.74 段指出了对核电厂设计进行安全分析的安全要求。关于确定性安全分析的范围和目标，其更具体的要求见 SSR-2/1（Rev.1）[I-1]第 5.75 段。

I-4. 通过确定性安全分析确定的设计要求的主要组成部分，通常包括：设备标定尺寸；容量；系统启动、终止和控制参数的设定值；和工作（环境）条件。这确保了系统在所有相关电厂状态下的有效运行，并提供了足够的运行裕量。分析还包括对所有电厂状态的放射性效应的评定，以确保对核电厂未来授权的信心。

I-5. 设计方通常使用安全分析作为设计过程的一个整体部分，该设计过程通常由几个迭代组成，这些迭代可以在电厂的制造和建造过程中继续进行。设计中使用的安全分析应根据质量保证计划进行的。

I-6. 营运组织通常在必要的范围内进行或核实安全分析，以确保竣工图设计按运行的预期进行，并证明设计在电厂设计寿命的任何时间点满足安全要求。这种独立核实被认为是一种单独的附加检查，以确保设计安全和合理。

I-7. 虽然设计的确定性安全分析不是核电厂授权的直接输入，但其结果希望能为未来的授权提供足够的裕量。因此，它是按照授权相同的范围，遵循授权相同的或甚至更加严格的规则进行的，这在正文中作了说明。

确定性安全分析在核电厂审批中的应用

I-8. 遵守所有适用的规则和标准以及其他相关的安全要求对核电厂安全和可靠运行至关重要。通常，通过安全分析报告中的编写或更新，包括电厂寿命不同阶段的安全分析报告以及提交给监管机构的各种相关联的支持性安全分析报告，可以说明这一点。

I-9. 在为许可证审批进行的确定性安全分析的基础上，可以证明在所有运行模式和所有电厂状态下执行安全功能设计的稳健性。特别是，可以证明安全系统与规定的运行人员行为组合，对于预计运行事件和设计基准事故工况的有效性，以及安全特证与预期的运行人员行动组合对于设计扩展工况的有效性。

I-10. 用于许可证审批的分析通常根据既定的保守或现实规则进行，包括将分析结果与相关的验收标准进行比较。为了证明符合验收标准，考虑了分析中的不确定性。在正文中详细说明了进行确定性安全分析的规则。

监管机构在独立核实中对确定性安全分析的应用

I-11. 监管机构应单独进行独立评审，以检查用于许可证审批的确定性安全分析报告的完整性和一致性，并核实其设计符合监管要求。如原子能机构《安全标准丛书》第 GSR Part 4（Rev.1）号《设施和活动安全评定》[I-2]第 4.71 段指出，“监管机构的核实不是营运组织流程的一部分，营运组织不能将其作为其独立核实的一部分加以使用或提出要求。”

确定性安全分析在定期安全评审中的应用

I-12. 可能需要进行新的确定性安全分析，以便在定期安全评审的背景下完善或更新先前的安全分析，从而确保最初的评定和结论仍然有效。在这种分析中，通常需要考虑的是，在评定时间内，由于随着时间老化而可能降低的所有裕量。

确定性安全分析在电厂改造中的应用

I-13. 核电厂通常根据运行经验的反馈、定期安全评审的结果（在进行时）、法规要求的变化、知识的增长或技术的发展来升级改造。电厂改造包括构筑物、系统或设备的改变、电厂参数的改变、电厂配置的改变或运行规程的改变。

I-14. 电厂改造的目标往往是更经济地利用反应堆和核燃料。这种改造包括提升反应堆功率、使用改进类型的燃料和使用创新的堆芯换料方法。这类改造通常意味着降低运行限值的安全裕量，应特别注意确保不超过限值。

I-15. 确定性安全分析通常用于支持电厂改造。这种确定性安全分析的范围通常对应于改造的安全重要性。这种安全分析通常遵循设计和许可证审批的确定性分析规则。

I-16. 如需要对电厂进行重大变更的改造，像提升功率和达到更高的燃耗、更长的燃料循环和寿命延长，通常需要通过全面的确定性安全分析来解决，以证明符合验收标准。当同时进行多个改造时，要特别小心。

确定性安全分析在超出正常运行限值事件的分析中的应用

I-17. 确定性安全分析可以作为一种工具，用以全面了解核电厂运行期间发生的事件，是运行经验反馈的不可分割的组成部分。分析这些事件的目的如下：

(a) 检查早期假想始发事件选择的全面性；

(b) 确定安全分析报告中分析的瞬态是否包络事件；

(c) 提供参数值时间相关的附加信息，这部分信息不能使用电厂仪器仪表测量直接观察到；

(d) 检查运行人员是否按预期操作，电厂系统是否按预期运行；

(e) 检查和评审应急运行规程；

(f) 确定分析中出现的任何新的安全问题和疑问；

(g) 为事件分析中发现的潜在安全问题的解决提供支持；

(h) 分析在发生额外故障（如严重事故前兆）的情况下可能造成的后果的严重性；

(i) 验证和调整用于确定性分析的计算机程序中的模型和培训模拟器中的模型。

I-18. 事件分析通常使用现实（最佳估算）方法来执行。在可能的情况下使用实际电厂数据。如果缺少关于电厂运行参数的详细信息，则可以进行变化选定参数的敏感性研究。

I-19. 重大安全事件的评价是运行经验反馈的一个重要方面。现代的最佳估算计算机程序使研究和详细了解电厂行为成为可能。从这些分析得出的结论应被纳入处理运行经验反馈的电厂改造或电厂规程中。

确定性安全分析在应急运行规程的制定和验证中的应用

I-20. 执行最佳估算确定性安全分析通常是为了验证电厂从瞬态工况到正常运行工况的恢复策略，这些瞬态发生在预计运行事件、设计基准事故和无明显燃料破损的设计扩展工况中。这些策略通常在应急运行规程中反映，定义了恢复这类事件中所要采取的行动。确定性安全分析提供了指定运行人员所采取行动的必要输入，并在事故管理策略的评审中发挥着重要的作用。

在制定用于确定运行人员采取有效行动的可用时间段的恢复策略时，对运行人员必要的行动的时间进行敏感性计算，并且这些计算可用于规程优化。

I-21. 在制定应急运行规程之后，进行核实分析，以验证最终的应急运行规程与模拟的电厂行为一致。还对应急运行规程进行了验证。该验证通常使用电厂模拟机执行。验证是为了建立经过培训的运行人员能够在可用的时间段内完成指定的行动，并且电厂带回安全的最终状态的信心。敏感性分析应考虑电厂系统可能发生的故障和运行人员可能发生的错误。

确定性安全分析在严重事故管理导则制定中的应用

I-22. 当应急运行规程不能防止设计基准事故进展到堆芯熔化的设计扩展工况时，确定性安全分析，通常也用来帮助制定运行人员应遵循的行为策略。这种分析通常使用一个或多个可用的专用计算机程序来模拟相关物理现象。

I-23. 这些分析用于确定对屏障完整性或旁通可选路径的挑战，可以预计，随着事故进展，这些现象将要发生。这些分析可以为制定一套管理事故和缓解其后果的导则提供依据。

I-24. 分析通常从选择事故序列开始，如果没有运行人员的干预，事故序列将导致堆芯损坏。对具有相似特性的事故序列进行分组，用来限制需要分析的序列数目。这种分类可以电厂状态的几个指标为基础：假想始发事件；进入停堆状态；或进入应急堆芯冷却系统、冷却剂压力边界、二回路热阱、安全壳排热和安全壳边界系统的状态。

I-25. 事故管理措施大致可分为预防措施和缓解措施。为制定严重事故管理标准提供支持的分析通常侧重于缓解措施，这些措施是管理严重事故以缓解堆芯熔化后果的策略。对于水冷堆，这种策略可以包括：将冷却剂注入敞口的堆芯中；对一回路进行减压；启动安全壳喷淋系统；压力容器外堆芯熔渣冷却；可燃气体的复合；以及安全壳过滤排放[I-3]。要考虑作为采取缓解措施的后果而可能产生的不利影响，例如压力峰值、氢气生成、重返临界、蒸汽爆炸、热冲击或氢气爆燃或爆炸。对于其他设计的反应堆，应考虑适用于该设计的缓解措施。

I-26. 从应急运行规程向严重事故管理导则的过渡，如果它们是分离的，需要仔细界定和分析，以便运行人员，无论在何种故障序列情况下，始终能够得到关于必要行动和监控事故进展的指导。

确定性安全分析在一级和二级概率安全评定中的事故序列制定并成功核实中的应用

I-27. 确定性分析和概率评定是两种相互补充的手段，可以在整个频率-后果谱系内，电厂整体安全提供一个综合全面的评定。但，必须承认，一些残余风险仍将存在。

I-28. 确定性安全分析通过确定“成功标准”在向概率安全评定提供支持方面起着重要的作用。确定性安全分析通常用于识别对物理屏障完整性带来的挑战，确定当受到挑战时屏障的失效模式，以及确定事故假想方案是否会对几个屏障带来挑战。为概率安全评定提供支持的这类研究的目的是，针对设备故障和人因错误的各种组合，确定一套可防止核燃料破损的最低安全特性。确定性分析是以一种现实的方式进行的，尽管在必要时需对不确定性进行量化。

I-29. 更具体地说，要进行确定性分析以指定自动系统以及运行人员行动的行动顺序。它确定了在特定假想方案中运行人员行动可用的时间，并为预防和缓解措施所需系统的成功标准的说明提供支持。

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《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）。

[I-3] 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）。

附件 II

预计运行事件和设计基准事故类别的频率范围

II-1. 表 II-1 列出了一些国家用于新反应堆可能的预计运行事件和设计基准事故类别。

表 II-1. 特定电厂状态下使用的预计运行事件和设计基准事故类别示例

电厂状态	一些国家中选用的名称	指示性频率范围（每年）
预计运行事件	中等频率故障：DBC-2，PC-2	$f>10^{-2}$
设计基准事故	罕见故障：DBC-3，PC-3	$10^{-2}> f>10^{-4}$
	极限故障：DBC-4，PC-4	$10^{-4}> f>10^{-6}$

注释：DBC－设计基准工况；PC－电厂工况。标识 DBC-1 和 PC-1 用于正常运行。需要考虑频率小于 10^{-6} 的一些其他事故，因为它们代表反应堆必须做好防护的一类风险。

参与起草和审订人员

Boyce, T.	美国核管制委员会
Courtin, E.	法国法玛通
Harwood, C.	加拿大核安全委员会
Herer, C.	法国辐射防护与核安全研究所
Lee, S.	韩国核安全研究所
Luis Hernández, J.	法国辐射防护与核安全研究所
Misak, J.	捷克核研究所
Ochi, H.	日本核监管局
Ramon, J.	西班牙核安全理事会
Spitzer, C.	国际原子能机构
Steinrötter, T.	德国装置与反应堆安全公司
Villalibre Ares, P.	国际原子能机构
Virtanen, E.	芬兰辐射与核安全局
Yllera, J.	国际原子能机构

IAEA
国 际 原 子 能 机 构

No. 26

当 地 订 购

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

北美

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

世界其他地区

请联系您当地的首选供应商或我们的主要经销商：

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

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

单个订单：
www.eurospanbookstore.com/iaea

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

定价和未定价出版物的订单均可直接发送至：

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

通 过 国 际 标 准 促 进 安 全

国际原子能机构
维也纳