国际原子能机构安全标准

保 护 人 类 与 环 境

制定和使用核电厂一级概率安全评定

特定安全导则

第 SSG-3 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。

制定和使用核电厂一级概率安全评定

国际原子能机构成员国

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
佛得角
柬埔寨
喀麦隆
加拿大
中非共和国
乍得
智利
中国
哥伦比亚
科摩罗
刚果
哥斯达黎加
科特迪瓦
克罗地亚
古巴
塞浦路斯
捷克共和国
刚果民主共和国
丹麦
吉布提
多米尼克
多米尼加共和国
厄瓜多尔
埃及
萨尔瓦多
厄立特里亚
爱沙尼亚
斯威士兰
埃塞俄比亚
斐济
芬兰
法国
加蓬
冈比亚
格鲁吉亚
德国
加纳
希腊
格林纳达
危地马拉
几内亚
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
荷兰王国
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-3 号

制定和使用核电厂一级概率安全评定

特定安全导则

国 际 原 子 能 机 构
2024 年 · 维也纳

版 权 说 明

国际原子能机构印刷
2024 年 9 月 • 奥地利

制定和使用核电厂一级概率安全评定

国际原子能机构，奥地利，2024 年 9 月
STI/PUB/1430
ISBN 978-92-0-533223-9（简装书：碱性纸）
978-92-0-533023-5（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）。

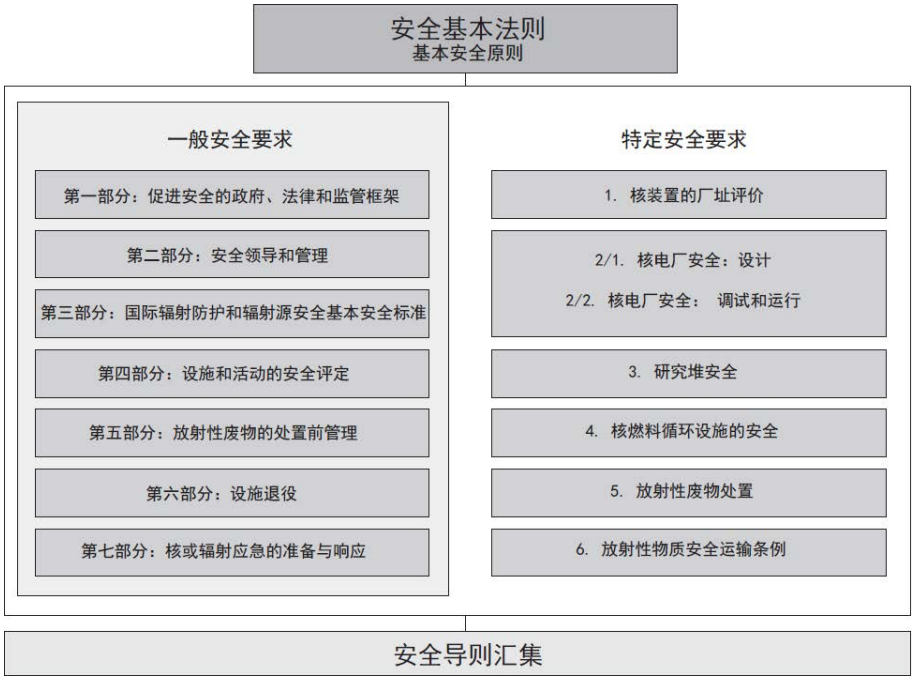

图 1. 国际原子能机构《安全标准丛书》的长期结构。

[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）、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。

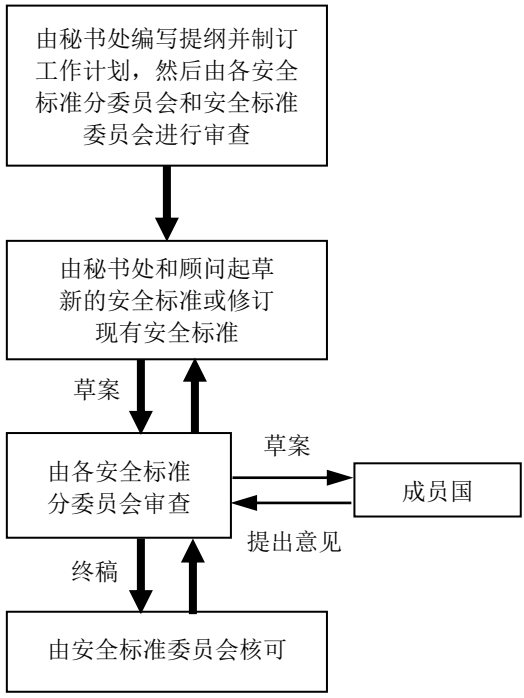

图 2. 制订新安全标准或修订现行标准的过程。

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 (1.1-1.8) 1
目的 (1.9-1.11) 3
范围 (1.12-1.16) 4
结构 (1.17) 5

2. 与概率安全评定实施和使用相关的总体考虑 (2.1) 5

概率安全评定的范围 (2.2-2.4) 5
概率安全评定的验证和评审 (2.5-2.6) 6
动态概率安全评定 (2.7-2.9) 7
参考值（安全目标或标准）(2.10-2.20) 8
概率安全评定在决策中的应用 (2.21-2.31) 10

3. 概率安全评定的项目管理和组织 13

概率安全评定项目目标和范围的定义 (3.1-3.2) 13
概率安全评定项目管理 (3.3-3.7) 14
方法的选择和程序的建立 (3.8-3.9) 15
团队选择与组织 (3.10-3.12) 15
建立概率安全评定质量保证计划 (3.13-3.14) 16
概率安全评定文档的概述 (3.15-3.22) 16

4. 熟悉电厂和收集信息 (4.1-4.3) 18

5. 满功率工况下、内部始发事件的一级概率安全评定 (5.1-5.2) 19

一级概率安全评定方法总览 (5.3-5.10) 20
始发事件分析 (5.11-5.39) 21
事故序列分析 (5.40-5.68) 26
系统分析 (5.69-5.85) 30
相关故障分析 (5.86-5.91) 33
共因故障分析 (5.92-5.95) 34
人的可靠性分析 (5.96-5.113) 35
其他建模问题 (5.114-5.120) 38
一级概率安全评定所需数据 (5.121-5.139) 39
分析的量化 (5.140-5.150) 41
重要度分析、敏感性研究和不确定性分析 (5.151-5.160) 43

6. 一级概率安全评定关于内部和外部危害的一般方法 45

概述 (6.1) 45
分析过程 (6.2-6.5) 46
初始信息的收集 (6.6-6.7) 48
危害识别 (6.8-6.13) 48
危害筛选 (6.14-6.25) 51

7. 内部危害一级概率安全评定详述 53

概述 (7.1) 53
对一级概率安全评定内部危害的边界评定和详细分析 (7.2-7.11) 54
内部火灾分析 (7.12-7.65) 56
内部水淹分析 (7.66-7.92) 67
其他内部危害 (7.93-7.114) 73

8. 外部危害一级概率安全评定详述 75

概述 (8.1) 75
外部危害边界分析的概述 (8.2-8.14) 76
外部危害的参数化 (8.15-8.28) 78
外部危害的详细分析 (8.29-8.32) 81
外部危害频率评定 (8.33-8.58) 81
结构和部件的易损性分析 (8.59-8.80) 86
外部危害与一级概率安全评定模式的整合 (8.81-8.100) 89
文档记录和结果描述 (8.101-8.111) 92

9. 低功率和停堆模式一级概率安全评定 95

低功率和停堆模式一级概率安全评定的概述 (9.1-9.3) 95
停堆类型和设备运行状态的规范 (9.4-9.10) 96
始发事件分析 (9.11-9.21) 98
事故序列分析 (9.22-9.30) 101
系统分析 (9.31) 103
相关故障分析 (9.32-9.35) 104
人的可靠性分析 (9.36-9.45) 105
数据评定 (9.46-9.55) 107
事故序列的量化 (9.56-9.57) 108
重要度分析、敏感性研究和不确定性分析 (9.58-9.60) 109
文档记录和结果描述 (9.61-9.71) 109

10. 概率安全评定的使用和应用 111

适合应用的概率安全评定范围 (10.1-10.5) 111

风险指引法 (10.6-10.7) 112
概率安全评定用于设 计评价 (10.8-10.27) 113
风险指引的技术规范 (10.28-10.35) 116
风险监控器 (10.36-10.54) 118
风险指引的在役检查 (10.55-10.64) 121
风险指引的在役试验 (10.65-10.69) 123
分级质量保证 (10.70-10.75) 123
基于概率安全评定的安全能指标 (10.76-10.77) 124
基于概率安全评定的事件分析 (10.78-10.83) 125
风险指引的规定 (10.84-10.89) 126

参考文献 127

附件 I 内部和外部危害的通用清单示例 129

附件 II 火灾传播事件树和地震事件树示例 136

附件 III 低功率和停堆模式概率安全评定的支持信息 138

参与起草和审订人员 155

国际原子能机构安全标准核可机构 157

1. 导言

背景

1.1. 人们普遍认为，与放射性物质相关的设施和活动带来利益的同时也产生辐射风险。为确保现在和未来工作人员、公众和环境免受电离辐射的有害影响，“安全基础”、“基本安全原则”[1]设定了一些原则，以强调评定和控制固有风险的必要性。特别是参考文献[1]原则 5（第 3.22 段）关于防护的最优化规定：

> “为了确定辐射风险是否处于合理可达尽量低的水平，必须事先（采用分级方法）对正常运行、异常工况或事故工况所造成的所有风险进行评定，并在设施和活动的全寿期内定期再评定。”

1.2. 原子能机构的若干“安全要求”出版物为核电厂的风险评定制定了更为特定的要求。《核电厂安全：设计》[2]（第 5.69 段）指出：

> “对核电厂的设计进行安全分析时，必须采用确定性分析和概率安全分析。基于此分析，对安全重要物项的设计基准必须得以确立和证实。”

参考文献[2]（第 5.73 段）也进一步指出：

> “必须进行电厂的概率安全分析，以便：
>
> (1) 提供一种系统性分析，为设计与总体安全目标相符提供确信；
>
> (2) 证明已实现了平衡设计，不会因特定的特性或 PIE [1] 造成对总体风险的贡献所占比例过大或特别不确定，并使前两级纵深防御承受确保核安全的主要负担；
>
> (3) 为防止电厂参数小偏差导致电厂严重异常行为（“陡边效应”）提供确信；
>
> (4) 评定严重堆芯损坏状态的发生概率，评定导致需要短期场外响应的重大场外排放的风险，特别是与安全壳早期故障相关的排放；
>
> (5) 对外部危害，特别是与场址相关的特有危害发生的频率和后果进行评定；

[1] PIE：假想始发事件

(6) 识别可降低严重事故的概率或缓解其后果而需做设计改进或需修改运行程序的系统；

(7) 评定电厂应急程序的充分性；和

(8) 核实是否符合概率安全目标（如有设定）。”

1.3. 因此，概率安全评定（PSA）被认为是一种重要的分析工具，用以分析与核电厂安全保证相关的潜在始发事件，此类事件可由设备的随机故障、人误以及内部和外部危害造成。

1.4. “安全要求”出版物《设施和活动安全评定》[3]（第 4.13 段）强调进行全面安全分析的必要性，该段指出：

> “安全评定必须包括安全分析，其包含一整套不同的定量化分析，通过分析以评价和评定在各种运行状态、预计运行事件和事故工况下的安全威胁。”

参考文献[3]（第 4.55 段）也指出：

> “概率安全评定的目标是确定设施或活动产生的对辐射风险有贡献的所有重要因素，并评定总体设计的平衡程度及其满足已定义的概率安全标准的程度。”
>
> 因此，需（开展）全面的概率安全评定来深入分析研究核电厂的安全。

1.5. 在确定性分析的基础上，概率安全评定被证明可提供重要的安全视角。概率安全评定提供一种方法论，用以识别广泛范围中各种始发事件发生后的事故序列，并包括以系统和实际的方式确定事故频率和后果。在国际实践中，普遍认可概率安全评定的三个级别：

(1) 在一级概率安全评定中，分析电厂的设计和运行情况，以识别可能导致堆芯损坏的事件序列，并估算堆芯损坏频率。一级概率安全评定针对已有或设想的防止堆芯损坏的安全相关系统及程序的优缺点提供深入了解和认识；

(2) 在二级概率安全评定中，按时间顺序对一级概率安全评定中识别出的堆芯损坏事故序列进行评定，包括对反应堆燃料严重损坏所引起现象的定量评定。二级概率安全评定识别源自燃料的放射性物质的相关排放可能导致向环境排放的方式，它还估算放射性物质向环境排放的频

率、数量和其他相关特征。该分析针对事故预防和缓解的各种措施以及放射性物质向环境排放的各实物屏障（例如安全壳厂房）的相对重要度提供更多的洞察和了解；

(3) 在三级概率安全评定中，估计公共健康和其他社会后果，例如由导致放射性物质向环境排放的事故序列引起的土地或食品污染。

1.6. 一级、二级和三级概率安全评定是顺序分析，每级评定的结果通常作为下一级概率安全评定的基础。一级概率安全评定针对设计缺陷和导致堆芯损坏的事故预防措施提供深入了解，这些堆芯损坏可能是导致放射性物质大量排放并对人类健康和环境造成潜在后果的事故前兆；二级概率安全评定针对导致堆芯损坏事故序列的相对重要度（以其引起放射性物质向环境排放的严重性来衡量）提供深入了解，也针对严重事故的缓解和管理措施的缺点和改进方法提供深入了解和意见；最后，三级概率安全评定提供事故预防和缓解措施的相对重要度（以其对电厂工作人员和公众健康以及对土地、空气、水和食品污染的不利后果来衡量）。另外，三级概率安全评定还针对与应急准备和响应相关的事故管理方面的相对有效性提供深入了解和意见。

1.7. 目前，世界上大多数核电厂都实施了一级概率安全评定。近年来，呈现出多种类型核电厂实施二级概率安全评定或有限二级概率安全评定（估算大量早期排放频率的二级概率安全评定）的趋势，此外，三级概率安全评定已在数个国家实施。

1.8. 本“安全导则”是在系统调研相关出版物的基础上编写的本“安全导则”。这些出版物包括参考文献[1－3]、其他安全导则的现有和正在修订中的修订版、国际核安全咨询组（INSAG）报告[4]以及其他涉及核电厂安全的出版物。

目的

1.9. 本“安全导则”目的是针对在实施或管理核电厂一级概率安全评定项目以及使用一级概率安全评定支持核电厂安全设计和运行方面如何满足参考文献[3]规定的要求提供建议。本“安全导则”适用于现有核电厂和升级改进的核电厂，但可能不完全适用于彻底革新型设计。本“安全导则”提供的建议旨在促进一级概率安全评定研究中的技术一致性，以便为概率

安全评定应用和风险指引的决策提供可靠支持。本“安全导则”的另一个深层目的是推荐一个标准框架，该框架便于对一级概率安全评定及其各种应用的监管评审或外部同行评审。

1.10. 本“安全导则”也为确保有效履行《核安全公约》[5]第 14 条规定的义务提供一种一致、可靠的手段。

1.11. 本“安全导则”提出的建议是基于国际公认的良好实践。但是，本“安全导则”这并非意味着要抢占先机、排斥或取代其他等效的新方法或替代方法。与此相反，本“安全导则”鼓励使用能够实现一级概率安全评定目标的任何方法。然而，本“安全导则”描述的概率安全评定框架预计将在可预见的未来适用。

范围

1.12. 本“安全导则”以国际公认的良好实践为基础，介绍一级概率安全评定的必要技术特点及在核电厂的应用。本“安全导则”规定的一级概率安全评定范围包括电厂的所有运行工况（即满功率、低功率和停堆）以及所有可能的始发事件和潜在风险，即：(a) 由设备随机故障和人误引起的内部事件；(b) 内部危害（例如内部火灾和水淹、汽轮机飞射物）；和 (c) 外部危害，包括自然灾害（例如地震、强风、外部洪水）以及人因引发危害（例如飞机坠毁、附近工业设施事故）。

1.13. 本“安全导则”主要关注反应堆堆芯，不涵盖现场的其他放射性物质来源，例如乏燃料水池。但是，在考虑低功率和停堆模式的一级概率安全评定时（第 9 部分），也涉及来自被移除反应堆外燃料的风险。

1.14. 恶意行为产生的危害不属于本“安全导则”的考虑范围。

1.15. 在实施一级概率安全评定时，最通常的实践是以满功率运行工况下、内部始发事件的一级概率安全评定为基础，在独立模块中对各种危害和运行模式进行分析，本“安全导则”遵循此方法。

1.16. 本“安全导则”的建议旨在尽可能保持技术中立，预计绝大多数建议可适用于不同类型的核电厂，然而，在必要的情况下，部分示例主要是

针对轻水堆核电厂提出的。在将某些建议应用于其他类型核电厂时，可能需要作出解释或判断。

结构

1.17. 第 2 部分就实施和使用概率安全评定的普遍性问题提供建议，包括概率安全评定的范围、概率安全评定的验证及动态概率安全评定；第 3 部分就概率安全评定的项目管理和组织以及关于概率安全评定文档的一般方面提供关键建议；第 4 部分讨论了概率安全评定工作团队熟悉核电厂的任务；第 5－8 部分就满功率运行工况下、各种始发事件和危害的一级概率安全评定方法提出建议；第 5 部分对内部始发事件的一级概率安全评定提供建议；第 6 部分总结关于内部和外部危害的一级概率安全评定通用方面的关键建议；第 7 部分和第 8 部分分别介绍内部和外部危害一级概率安全评定的特定情况；第 9 部分为低功率和停堆模式的一级概率安全评定提供关键建议；第 10 部分对一级概率安全评定的应用提出了关键建议。三个附件分别为：内部和外部危害的通用清单示例、火灾蔓延事件树和地震事件树示例以及低功率和停堆模式的概率安全评定支持信息。

2. 与概率安全评定实施和使用相关的总体考虑

2.1. 本部分描述关于在实践中实施概率安全评定和使用概率安全评定结果的一些一般性问题。尽管本“安全导则”的范围仅限于考虑一级概率安全评定，但本部分将从更广泛的角度描述此类问题，以呈现概率安全评定技术能力及其结果的全景。本部分的部分陈述不代表明确的建议，相反，它们只是为便于对本“安全导则”其他各部分中提出的其他陈述和建议的上下文语境的理解而提供支持性信息。

概率安全评定的范围

2.2. 针对满足要求 1 的分级方法和符合要求 14 关于概率安全评定[3]的安全分析范围，第 2.2－2.4 段提供了建议。概率安全评定承担的范围应当与国家安全目标或标准（如果已经有设定）相关。在高级别上，概率安全评定定量结果通常用于检验是否符合安全目标或标准，而这些安全目标或标

准通常是以堆芯损坏频率、不同类型放射性的排放频率和社会风险的定量估值来制定的，为此可能需要分别开展一级、二级或三级概率安全评定。安全目标或标准通常不会特定规定需考虑的危害和电厂运行模式。因此，为了利用概率安全评定的结果来验证与现有的安全目标或标准的符合性，应当开展涵盖完整的始发事件和危害清单以及电厂所有的运行模式的全范围概率安全评定，除非所制定的安全目标或标准明确限定了概率安全评定的范围，或者使用替代方法证明了模式中未涵盖的那些始发事件、危害和运行模式所导致的风险并不影响与安全目标或标准的符合性。

2.3. 若仅实施一级概率安全评定，则反应堆堆芯通常是分析的重点。若实施二级或三级概率安全评定，需要评定放射性物质排放的影响，则概率安全评定的范围可能包括现场其他放射性物质（如乏燃料和放射性废物）对风险的贡献。当旨在考虑核电厂对场址附近公众人员造成的总风险时，应当将堆芯外的那些放射源纳入概率安全评定。

2.4. 概率安全评定的主要优势之一是为风险评定中的不确定性分析提供了一个明确框架。应当将识别不确定性来源并了解其对概率安全评定模式和结果的影响作为任何概率安全评定的固有组成部分，以便在将概率安全评定结果用于支持决策时，把不确定性的影响纳入考虑。

概率安全评定的验证和评审

2.5. 为符合要求 18 对概率安全评定计算机程序使用和验证的规定，以及为符合要求 21 对概率安全评定独立校核的规定，第 2.5 段和第 2.6 段提出了建议。概率安全评定涉及许多分析方法。根据分析的范围（一级、二级或三级），这些分析方法包括用于分析事故序列的事件树和故障树逻辑模式的开发、用于求解逻辑模式的方法、诸如堆芯损坏后核电厂安全壳内可能发生的现象模式，以及放射性核素在环境中的输运模式，以确定其对健康和经济造成的影响，确定对健康和经济的损坏。在应用之前，应当证明这些分析方法能够充分说明所发生的过程。支持这些分析方法的计算机程序应当适合于分析的目的和范围，并且控制物理和逻辑方程式应当在计算机程序中正确编程（参考文献[3]第 4.60 段）。

2.6. 对于实施概率安全评定的组织而言，委托外部（有时是它国的）团体进行概率安全评定的独立同行评审是一个广为采纳的实践，其目的是从

一定程度上保证其范围、建模和数据的适当性，并确保其与当前的国际公认的概率安全评定良好实践相一致。参与概率安全评定评审的专家不能从事与被评审概率安全评定实施相关的任何活动，且应当来自独立于概率安全评定开发机构的其他组织。

动态概率安全评定

2.7. 第2.7—2.9段就如何满足要求24关于一级概率安全评定[3]安全评定维护的规定提出建议。在电厂运行的全寿期内，通常会对安全系统的设计或电厂运行方式进行改进。这些改进可能会对电厂相关的风险水平产生影响。在电厂运行期间，可得到更多关于始发事件频率和设备故障概率的统计数据。同样，可能会得到新信息和更复杂的方法和工具，它们可能会改变在分析时所做的部分假设，进而改变概率安全评定的风险估值。因此，概率安全评定应当在电厂的全寿期中保持更新，以确保其保持与决策过程的紧密相关。定期更新的概率安全评定称为“动态概率安全评定”。更新概率安全评定时应当包括电厂设计和运行的变化、新技术信息、可采用的更复杂方法和工具以及来自电厂运行的电厂新的特定数据（如用于评定始发事件频率或设备故障概率的数据）。概率安全评定的更新应当按照规定程序启动，并定期评审概率安全评定的状态，以确保其能保持作为电厂的代表性模式并符合预期目的。

2.8. 应当在电厂的全寿期内收集数据，以检查或更新分析。这些数据包括关于运行经验的数据，特别是关于始发事件的数据，关于设备故障及其在试验、维护和维修期间不可用的数据，以及关于人员行为绩效的数据。应当根据新数据，对分析结果定期进行再评定。

2.9. 应当鼓励开发动态概率安全评定，以协助电厂正常运行的决策过程。对诸如与电厂变化或暂时改变设备的允许大修时间相关的风险变化的评定等问题，都可以获得由概率安全评定所得出论据的支持。经验表明，这种动态概率安全评定可为营运组织带来实质性利益，其使用也受到监管机构的普遍欢迎。

参考值（安全目标或标准）

2.10. 第 2.10－2.20 段对如何满足参考文献[3]关于实施概率安全评定的要求 4 提供了建议。当概率安全评定目标是识别风险的重要贡献因素，或从各种设计选项和电厂配置之间进行选择时，参考值并非必需。然而，当概率安全评定旨在帮助就下列问题做出判断时：(1) 计算得到的风险是否可接受；(2) 建议的电厂设计或运行的变更是否可接受；或 (3) 某变更对降低风险水平是否属必要，则应当明确规定概率参考值，以指导设计人员、营运者、监管人员及其他相关各方为了以期望或要求的电厂安全水准、提供安全可靠的核能而各司其职。在一些国家，目前的实践是将参考值拟订为安全目标，即参考值代表被瞄准达到或实现的方向值。在其他国家，参考值是作为标准，规定应当遵守的严格限值。

2.11. 根据待评定的后果，概率安全评定将产生与不同级别风险相关的数值。可比照下列任何或全部度量参数来设定概率安全目标或标准：

(a) 特定安全功能或安全系统的故障概率；

(b) 堆芯损坏频率 [2]（一级概率安全评定）；

(c) 电厂放射性物质特定排放（例如，以排放的数量、同位素或时间来确定）的频率，或作为排放量（级）的函数的放射性物质排放频率（二级概率安全评定）；

(d) 对公众特殊健康影响的发生频率或特定环境后果的发生频率（三级概率安全评定）。

2.12. 参考文献[6]给出了一种可能的概率安全标准定义框架，其规定了“容忍度阈值”，如高于该阈值，则风险水平不可容忍，规定了“设计目标值”，低于该值的风险大体上均可接受。介于前述两种风险水平之间区域的风险，仅在采取了所有合理可行的措施以降低风险后方可接受。该方法已为部分国家采用，但更通常的实践是制定概率安全标准，将其定位为追求值、目的值、目标值、指导值或参考值。此外，与容忍度阈值和设计追求值对应的风险水平数值，各国并不相同。

[2] 如本“安全导则”第 5 部分所述，关于堆芯损坏的概念必须规定特定的标准。对于不同反应堆设计，标准可能有所不同。

2.13. 对于安全功能或安全系统故障概率，可根据安全功能水平或安全系统水平设置其概率目标值。概率目标值可用于校核所提供的冗余和多样性水平是否适当。目标值与特定的电厂设计相关，因而在此未对此类目标值的设置提供建议。在安全评定中，应当检查是否满足这些目标。若未满足，只要满足了更高级别的标准，设计仍然可以接受。但是应当特别考虑对相关的安全系统进行合理可行的改进。

2.14. 国际核安全咨询组基于核电厂设计和运行的目前经验，在 1999 年提出了现有的和建议的核电厂设计可以达到的数值。

2.15. 国际核安全咨询组（见参考文献[4]）分别就现有电厂和未来电厂的堆芯损坏频率提出了目标值。[3]

2.16. 堆芯损坏频率是最通常的风险衡量参数，因为大多数核电厂都至少经历过一级概率安全评定，而且方法已很成熟。在许多国家，正式或非正式地将该类型的数值用作概率安全目标或标准。

2.17. **放射性物质的大量场外排放：**放射性物质的大量排放将对社会产生严重影响，并需要实施场外应急安排。其可以通过多种方式加以特定规定，包括：

(a) 以最重要核素排放的绝对量（以贝克勒尔为单位）的方式；
(b) 以占堆芯存量份额的方式；
(c) 以场外受辐射最多人员受到规定辐射剂量的方式；
(d) 以导致“不可接受的后果”的排放方式。

在某些情况下，标准的制定与排放时间相关，特别是排放发生在早期还是晚期。在这种情况下，需对“早期”术语做定义。

[3] 参考文献[4]的堆芯损坏频率目标值是：(a) 对现有核电厂 1×10^{-4} / 堆•年；(b) 对未来核电厂 1×10^{-5} / 堆•年。参考文献[4]未明确指出这些数值所适用的概率安全评定范围，假想是指全范围概率安全评定。

2.18. 国际核安全咨询组还提出了需要短期场外响应的大量放射性物质场外排放的建议目标值。[4]

2.19. 虽然对大量场外排放的构成还未形成国际共识，但部分国家已制定了类似的概率标准。

2.20. **对公众健康的影响**：国际核安全咨询组未就公众健康影响的目标值提供指导。[5]

概率安全评定在决策中的应用

2.21. 参考文献[3]要求 23 是关于一级概率安全评定的运用，第 2.21－2.31 段为如何满足该要求提供建议。应当在电厂的全寿期运用概率安全评定，并结合确定性安全分析的结果和见解以及纵深防御的考虑，为决策提供输入。

2.22. 概率安全评定可为各相关各方提供有用的见解和输入，例如电厂工作人员（管理、工程、运行及维护人员）、监管机构、设计人员和供应商，就以下方面做出决策：

(a) 设计修改和电厂改造；
(b) 优化电厂运行和维护；
(c) 安全分析和研究计划；
(d) 监管问题。

2.23. 若将概率安全评定的结果用于支持决策过程，则应当为此建立正规的框架。决策过程的细节将取决于特定概率安全评定应用的目的、待决策的性质和待使用的概率安全评定结果。若使用概率安全评定的数值结果，则应当建立可与这些结果相比较的参考值。

---

[4] 需要短期场外响应的大量场外排放的目标值对现有电厂为 1×10^{-5} / 堆•年。参考文献[4]未对未来电厂的大量场外排放给出数值，但规定了以下定性目标：“对这些未来电厂的另一个目标是实际消除可导致大量早期放射性排放的事故序列，而对于暗含安全壳晚期故障的严重事故，应当在在设计过程中采用现实性假设和最佳估算分析加以考虑，以使其后果仅会引起在有限的区域和时间内采取保护措施。”

[5] 在一些国家，采取一名公众人员死亡风险的目标值为 1×10^{-6} / 堆•年。

2.24. 概率安全评定应当针对电厂实际的或对于在建或正在改造的电厂目标设计或运行，对此应当做出确识别并作为分析的基础。电厂状态可以以其在特定日期或一致认定的将完成改进的日期的状态来进行固化。这样做是为了给完成概率安全评定提供明确的目标。此后所做的改进可在动态概率安全评定计划（如第 2.7—2.9 段指出）的框架内加以考虑。

2.25. 对于处于设计阶段的电厂，概率安全评定的结果应当作为设计过程的一部分用以评定安全水平。在此情形下，应当将概率安全评定得到的结论与确定性分析得到的结论结合在一起考虑，进而对电厂的安全做出决策。关于电厂安全的决策应当是迭代过程的结果，旨在确保满足国家要求和标准、平衡设计且风险合理可达尽量低。

2.26. 此外，若概率安全目标或标准已在国家法规或导则中有规定，则应当将概率安全评定的结果与其进行比较。这种比较应当针对为电厂所定义的所有概率标准进行，包括系统可靠性、堆芯损坏、放射性物质排放、对工作人员的健康影响、对公众的健康影响和诸如土地污染和食品禁令的场外后果等的概率标准。

2.27. 概率安全评定应当从识别对风险有贡献的所有事故序列着手，并确定电厂的设计或运行是否存在缺陷。例如，可以使用概率安全评定来评定是否需要进行改进，以降低缺陷的安全影响。若分析未涵盖对风险的所有贡献（例如分析省略了外部危害或停堆状态），则概率安全评定针对电厂风险水平、所提供安全系统的平衡性、为降低风险欲做的设计或运行改进的必要性等得出的结论可能会有偏差。

2.28. 一级概率安全评定的结果应当用于识别电厂设计或运行缺陷。通过考虑始发事件组对风险的贡献、安全系统的重要性测量以及人误对总体风险的贡献可识别出缺陷。当概率安全评定的结果表明可以对电厂的设计或运行进行改进以降低风险时，则这些改进应当在合理可行的情况下予以采纳，并考虑到任何修改或改造的相对成本和收益。

2.29. 二级概率安全评定的结果应当用于判断是否已为预防或缓解假想堆芯损坏序列的影响提供了足够条件。在二级概率安全评定中，应当考虑安全壳是否足够坚固，以及诸如氢气混合和复合系统、安全壳喷淋和安全壳通风系统等保护系统是否能为防止大量放射性物质向环境排放提供足够水准的保护。此外，还应当考虑诸如接口系统冷却剂丧失事故等安全壳旁通

事件。再者，应当使用二级概率安全评定来识别和优化可用以缓解堆芯损坏影响的事故管理措施。这还可能包括确定其他措施，例如，可用于将水引入反应堆安全壳的措施。

2.30. 一旦获得二级概率安全评定和三级概率安全评定结果，则应当提供给公共部门，作为场外应急计划的技术输入。

2.31. 第 10 部分为监管机构和营运组织特定应用概率安全评定提供了详细建议。但为了方便和连续地涵盖概率安全评定的一般方面，以下概述了与概率安全评定应用相关的主要建议：

(a) 概率安全评定的结果应当用于制定事故应急程序，并为电厂的技术规范提供输入。特别是，应当使用概率安全评定的结果调查为试验或维护目的而解除在用设备项后所增加的风险，以及监视或试验的频率是否适当。应当使用概率安全评定来确认允许的大修时间不会导致不适当的风险，并指出应当避免的那些设备大修组合；

(b) 概率安全评定的运用应当贯穿电厂的设计和运行过程，用以对电厂安全的决策过程提供支持：

  (i) 对于新建电厂，概率安全评定应当在概念设计阶段启动，以检验安全系统中提供的冗余度和多样性是否足够。概率安全评定应当在详细设计阶段继续进行，以评定更详细的设计问题，并应当将其用于支持电厂的运行。在设计阶段，应当设置一个迭代过程，以确保从概率安全评定中获得的结果和意见反馈到设计过程中；

  (ii) 对于现有电厂，概率安全评定的实施或作为定期安全评定的一部分，或为了给建议改进的安全示例提供支撑。尽管概率安全评定的要求保持不变，但所使用的数据可能会随着经验的积累而变化。此外，根据设施的年限、剩余的使用寿命、拟实施改进的费用和其他相关考虑，在合理实施哪些改进可降低风险上将会存在差异。前述的考虑还应当包括电厂延寿的可能性，不管是否已经申请延寿或正在考虑中。

(c) 概率安全评定应当用于确定安全系统是否包含足够的冗余度和多样性，以及确定总体设计是否平衡。作为平衡设计的标志，概率安全评定的结果应当表明：

  (i) 无设计或始发事件组的特定特性对风险造成特别重大的贡献；

(ii) 总体低水平风险的实现不依赖于具有重大不确定性风险贡献者。设计缺乏平衡通常表明有机会通过采取合理可行的措施来降低风险。

3. 概率安全评定的项目管理和组织

概率安全评定项目目标和范围的定义

3.1. 为满足参考文献[3]关于一级概率安全评定目标的要求 4 以及涉及一级概率安全评定范围的要求 14，第 3.1 段、第 3.2 段提供了相关建议。确定概率安全评定的目标及其预期和潜在用途是在开始开展概率安全评定过程之前的一个重要步骤。概率安全评定的范围由分析级别（一级、二级或三级）、所考虑的始发事件和危害以及所处理的运行模式（即满功率、低功率或停堆状态[6]）来确定。概率安全评定的范围应当与分析的目标和现有的资源和信息相匹配，即必要的程序和方法、人员、专家意见、资金和分析所需的时间。例如，若概率安全评定的目的是依据规定的安全目标验证电厂运行引起的风险，则意味着应当开展完整的风险评定，即全范围的概率安全评定，包括始发事件和危害全面清单以及电厂的全部运行模式，并应当为概率安全评定分析提供充分的资源。此外，取决于所制定的安全目标，可能还需要分析其他辐射源（例如乏燃料水池）。

3.2. 应当认识到，概率安全评定的预期应用可能对概率安全评定的范围、建模方法和详细级别提出额外要求。若在概率安全评定项目的计划阶段考虑到这些额外要求，将有助于避免所得到结果和见解的不一致。例如，若计划将概率安全评定用于制定严重事故管理计划，则应当执行二级概率安全评定。再如，若计划将概率安全评定模式用作风险监控的基础，概率安全评定模式在始发事件建模方面应当是“对称”的。应当不采用通常的将始发事件建模简化为其总是发生在一个特定通道中。例如，应当以一个特定回路受到影响的适当概率（例如，两通道电厂是 1/2，三通道电厂是 1/3）为每个回路冷却剂丧失事故建模，而非一个回路中的一个单一事件。第 10 部分提供了概率安全评定在各种应用中所必需的概率安全评定特点的更多细节。

---

[6] 低功率和停堆状态的概率安全评定通常是作为同一研究的一部分来开展的。

概率安全评定项目管理

3.3. 为满足参考文献[3]关于安全评定准备的要求 5，以及关于安全评定管理的要求 22，第 3.3－3.14 段提供了建议。概率安全评定的项目管理很大程度上取决于一个国家的特定情况，即：

(a) 参加概率安全评定项目的组织；
(b) 参加组织的参与方式和程度；
(c) 概率安全评定分析的目标和范围。

在概率安全评定的目标和范围确定后，应当制定概率安全评定项目管理计划，包括方法选择和程序设立、实施概率安全评定的人员选择和团队的组织、团队培训、概率安全评定项目进度计划的准备、所需经费的估算和筹措、质量保证程序和同行评审程序的建立。

3.4. 概率安全评定分析通常由下列之一委托进行：

(a) 电厂设计方；
(b) 电厂营运组织；
(c) 监管机构。

概率安全评定可由上述团体或顾问、研究所、大学或其组合来实施。无论那种情况下，作为运行经验的来源以及由概率安全评定所得结果和意见的受益方，营运组织都应当参与。

3.5. 通常希望在电厂寿期内尽早启动概率安全评定的实施过程。相比于直至电厂运行后仍然存在的缺陷，及早发现的设计缺陷或程序缺陷能以较低代价得到纠正或改进。尽管概率安全评定可以在电厂寿期的任何阶段启动，但概率安全评定模式和文档应当在电厂的全寿期中得到维护和定期更新，以提供持续受益。

3.6. 为了对电厂竣工或运行状态进行建模，概率安全评定研究应当考虑一个特定的“冻结日期”。若在概率安全评定项目之初就已知针对电厂设计和运行的某些改进将在概率安全评定完成之前的短期内实施，则应当在概率安全评定的早期阶段决定是否将其纳入概率安全评定中予以考虑。若确

定要考虑将来的改进，则相应地确定冻结日期，且概率安全评定应当针对改进后电厂的状态。

3.7. 应当以清晰、可追溯、系统和透明易懂的方式编写概率安全评定文件，以便有效地支持概率安全评定的评审、应用和未来升版。

方法的选择和程序的建立

3.8. 在项目开始时，应当制定适当的工作方法和程序，以使项目进展期间对这些程序进行的修改最少。方法和程序不必要的反复可能会导致概率安全评定项目的延期。本出版物的后续章节就方法论工具和分析方法提供了总体指导。一旦选定了工作方法，应当将各种程序性步骤与质量保证和培训任务结合起来，以制定详细的任务计划，包括项目的进度表。

3.9. 完成概率安全评定所需的资源如参与专家的专家意见、人力资源、计算机时间、日历时间等，很大程度上取决于概率安全评定的范围（其又受制于总体目标）和概率安全评定团队的专业知识。在制定详细程序后，应当进行活动的安排和计划，并对人员的可用性做出说明。

团队选择与组织

3.10. 实施概率安全评定的团队成员可以以其所代表的组织和其所提供的技术专长为表征。一旦确定了必要的人员，就应当建立联系渠道并分配特定任务。应当根据概率安全评定的活动来确定和计划必要的培训。团队组建和培训任务与质量保证的相应任务密切相关。

3.11. 实施概率安全评定所需的专业知识应当提供两个基本要素：电厂知识和概率安全评定技术知识。根据概率安全评定范围，前述专业知识可以在深度上有所不同，但如有可能，应当预见有电厂设计方和营运组织的参与。更特定而言，应当从对正常和事故工况下的电厂设计和运行有广泛认知的人员处获得必要的关于电厂知识的专家意见。

3.12. 应当为首次实施概率安全评定的团队提供培训，以获得成功完成分析研究所需的专门知识。

建立概率安全评定质量保证计划

3.13. 概率安全评定质量保证[7]计划包括下列活动：达到概率安全评定的适当质量所必需的活动和核实已达到适当质量所必需的活动。对于概率安全评定来说，适当的质量意味着正确和可用的最终结果，且满足概率安全评定的目标并实施了规定范围的概率安全评定。质量保证计划对影响概率安全评定质量的所有活动规定严格方法，包括在适当情况下核实每项任务是否已圆满完成并采取了必要的纠正措施。

3.14. 概率安全评定的质量保证应当被视为和成为概率安全评定项目管理的组成部分，且质量保证程序也应当是概率安全评定程序的组成部分。质量保证程序应当规定与概率安全评定的组织、技术工作和文档方面相关活动的控制。质量保证程序在应用于技术工作时，旨在确保目标、范围、方法和假设之间的一致性以及方法应用和计算的准确性。质量保证程序应当包括概率安全评定文档控制。文档控制的一般要求见参考文献[7]第 2 部分。

概率安全评定文档的概述

文档的目标和内容

3.15. 为符合参考文献[3]要求 20 关于一级概率安全评定文档的规定，第 3.15－3.22 段提供相关建议。概率安全评定文档的主要目标应当是满足用户的需求，并与概率安全评定的特定应用相适应。概率安全评定的可能用户包括：

(a) 核电厂营运组织（管理及运行人员）；
(b) 设计方和供应商；
(c) 监管机构和为其提供技术支持的人员或组织；
(d) 其他政府机构；
(e) 公众。

[7] 参考文献[7]使用的不是“质量保证”术语，而是“管理系统”术语。本“安全导则”保留“质量保证”术语，以符合概率安全评定领域中广泛接受的现行实践和所使用的术语。

其中一些用户（如公众）可能主要使用概率安全评定摘要报告，而另一些用户将使用全部概率安全评定文档，包括计算机模式。

3.16. 概率安全评定文档包括概率安全评定的工作文件、计算机输入和输出、通信、中间报告和最终报告。概率安全评定文档应当保持完整、结构良好、清晰，且易于理解、评审和更新。它应当以可追溯和有序的方式呈现，即在最终文档中出现的分析顺序应当尽可能遵循实际进行分析的顺序。此外，还应当为可能的分析拓展提供手段，包括整合新专题、使用改进模式、扩展所考虑的概率安全评定范围以及用于其他应用。对所做假设、对概率安全评定的扩展和解释的排除和限制做明确陈述对于用户也是至关重要的。

3.17. 文档应当在报告内（或参考现有材料）提供重现研究结果的所有必要信息。所有不会在任何外部报告中公布的中间子分析、计算、假设等应当以记录、工作文件或计算机输出等形式予以保留。这对于将来重现和更新分析的每个细节非常重要。

文档的结构

3.18. 概率安全评定研究的最终报告应当分为三个主要部分：

(1) 摘要报告；
(2) 主报告；
(3) 主报告的附录。

3.19. 摘要报告旨在提供概率安全评定动机、目标、范围、假设、结果和结论的总览，其应当达到对广大反应堆安全专家读者群有用并适合于高级别评审的深度。摘要报告应当设计成能够：

(a) 支持概率安全评定的高级别评审；
(b) 将研究的关键方面传递给相关各方；
(c) 为读者或用户在查阅主报告之前提供一个清晰的框架和导则。

概率安全评定摘要报告应当包括一个关于报告结构的小章节，扼要描述主报告各章节和各附件的内容，并说明概率安全评定各部分之间的关系。

3.20. 主报告应对完整的概率安全评定研究进行清晰、可追溯的介绍，包括电厂描述、研究目标、使用的方法和数据、所考虑的始发事件、电厂建模结果及结论。主报告及其附件应当设计成能够：

(a) 支持概率安全评定技术评审；
(b) 将关键的详细信息传递给利益相关或感兴趣的用户；
(c) 允许概率安全评定模式和结果的有效和多样化应用；
(d) 便于模式、数据和结果的更新，以支持电厂的持续安全管理。

3.21. 附件应当包含详细数据、工程计算记录、详细模式等。附件的结构应当尽可能使其直接对应于主报告的章节和子章节。

3.22. 本部分就概率安全评定文档提供了一般性建议，本“安全导则”其他章节则提供文档的特定建议，例如，针对内部始发事件、内部火灾、内部水淹、外部危害、以及低功率和停堆状态的概率安全评定文档的建议。

4. 熟悉电厂和收集信息

4.1. 为符合参考文献[3]关于一级概率安全评定准备的要求 5，本部分提供了相关建议。概率安全评定团队应当熟悉电厂的设计和运行，包括应急程序、试验和维护程序。可用于熟悉电厂的信息来源包括：

(a) 电厂安全分析报告；
(b) 电厂技术规范；
(c) 系统描述；
(d) 竣工（现状）系统图（管道和仪器仪表图）；
(e) 电气线路图，包括电气母线保护系统的电路图和停堆标准；
(f) 控制和驱动电路图；
(g) 正常运行程序、应急程序、试验程序和维护程序；
(h) 关于系统任务成功标准的决定性因素分析；
(i) 来自电厂或相同或其他国家类似电厂的运行经验，以及事件报告和分析；
(j) 运行人员日志；
(k) 与运行人员的讨论；

(l) 电厂运行记录和停堆报告；

(m) 电厂数据库和/或维护的计算机化管理系统（如有）；

(n) 电厂布置图；

(o) 管道位置和布线图；

(p) 电缆定位和布线图；

(q) 电厂巡视报告；

(r) 监管要求；

(s) 其他相关电厂文件。

应当收集涉及分析所需信息的电厂文件，并将其提供给概率安全评定团队。取决于概率安全评定的范围，可能需要更特定的信息，例如外部危害概率安全评定所需的电厂布置图、现场和周围的地形图。必要时，可与非概率安全评定团队成员的运行人员沟通，以澄清和获得更多信息。

4.2. 目前，许多国家要求将概率安全评定的实施作为安全分析报告的一部分。此种情况下，概率安全评定文档可以参考安全分析报告诸如系统描述等的相应部分。应当清楚地给出所有参考文献以易于找到被引用的信息。

4.3. 电厂熟悉是内部和外部危害概率安全评定的关键要素。应当进行彻底的电厂巡视，以核实关于危害源和因危害而易损坏的电厂特点信息。应当为针对内部和外部危害的电厂熟悉提供特定指导。

5. 满功率工况下、内部始发事件的一级概率安全评定

5.1. 如何满足参考文献[3]关于内部始发事件一级概率安全评定的要求 6—13，本部分提供了相关建议。本部分提出的建议是针对在开展满功率下由设备随机故障或人误所致内部始发事件的一级概率安全评定时，需要解决的技术问题。

5.2. 关于一级概率安全评定的建议包括：

(a) 一级概率安全评定方法总览；

(b) 始发事件分析；

(c) 事故序列分析；

(d) 系统分析；

(e) 相关故障分析；

(f) 共因故障分析；

(g) 人的可靠性分析；

(h) 非能动系统和计算机系统的建模；

(i) 一级概率安全评定所需数据；

(j) 概率安全评定模式的整合与量化；

(k) 敏感性研究及重要度和不确定性分析。

分析的总体框架如图 1 所示。

一级概率安全评定方法总览

5.3. 第一步应当确定用于一级概率安全评定的总体途径和方法。总体途径和方法应当能够从始发事件开始对可能发生的故障序列进行建模，并且能够识别可导致堆芯损坏的安全系统故障、支持系统故障和人误的组合。

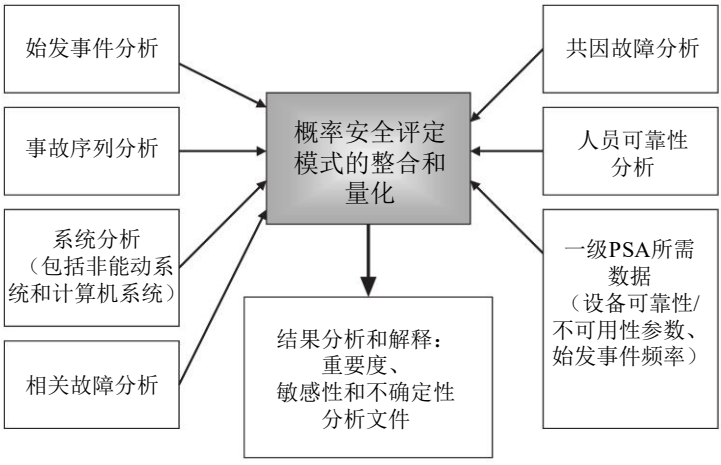

图 1. 内部始发事件一级概率安全评定分析的总体框架。

5.4. 概率安全评定的实施可采用若干种技术。然而，通常的方法是使用事件树和故障树的组合。事件树和故障树的相对规模（复杂性）在很大程度上取决于分析团队的偏好，也取决于所使用计算机软件的特点。

5.5. 事件树和故障树的组合是通用方法之一，一般称为故障树联接法。事件树概括出事故序列的广泛特征，其从始发事件开始，取决于缓解的安全和安全相关系统的成功或失败，导致成功的结果或堆芯损坏（详见第 5.42－5.43 段），或电厂损坏状态之一（二级概率安全评定所需的）。故障树用于对执行安全功能的安全系统和支持系统的故障进行建模。

5.6. 另一种通用方法是采用大事件树和小故障树进行分析。此方法是在事件树中对安全功能、安全系统和支持系统的故障进行建模。此方法被不同地称为大事件树法、联接事件树法或带边界条件的事件树法。也可以仅采用事件树或故障树单独进行分析。但是，在后一种情况下，高层故障树结构通常来自或基于事件树或事件树集。

5.7. 总体目标是计算堆芯损坏频率的最佳估计值，同时尽可能避免引入过多的保守性，因为这可能会不必要地给结果带来偏差。因此，一级概率安全评定应当基于最佳估算模式、假设和数据。然而，在不确定性高的情况下，为了避免不合理的乐观估计，一定的保守仍可能是必要的。

5.8. 所产生的一级概率安全评定模式应当能够用于预计应用，并且能够为将来可能的应用对其进行更新。

5.9. 应当使用具有以下功能的计算机程序进行分析：

(a) 能够处理核电厂非常大型和复杂的逻辑模式；

(b) 能够在合理的短时间内对概率安全评定模式进行定量化；

(c) 能够提供必要信息以解释一级概率安全评定，例如堆芯损坏频率、割集（导致堆芯损坏的始发事件和故障和/或人误的组合）的频率、重要度以及不确定性和敏感性分析的结果。

5.10. 一级概率安全评定是一个迭代过程，直至生成精确、足够详细的模式。

始发事件分析

5.11. 一级概率安全评定的起点是识别始发事件集。始发事件是可直接导致堆芯损坏（如反应堆压力容器破裂）或给正常运行带来威胁的事件，要求采用防止堆芯损坏的安全或非安全系统对其成功缓解。

5.12. 本部分讨论对满功率运行期间可能出现的内部始发事件的识别。第 6 部分介绍了针对内部和外部危害的一级概率安全评定的一般方法；第 7 部分和第 8 部分则分别提供了详细建议；第 9 部分就低功率和停堆模式下可能出现的始发事件识别的特定问题提供了建议。

始发事件的识别

5.13. 应当采用系统的方法来识别在一级概率安全评定中要处理的始发事件集，其涉及以下方法：

(a) 分析法，诸如危害和可运行性研究、故障模式和影响分析或其他相关方法，用于分析安全系统，以确定其（部分或全部）故障是否会导致始发事件；

(b) 演绎法，如主逻辑图，以确定会威胁正常运行并导致始发事件的基本故障或基本故障的组合；

(c) 比较法，与类似电厂一级概率安全评定产生的始发事件清单和现有安全标准和导则作比较；

(d) 经验法，以所研究的电厂和类似电厂的运行经验为基础，识别始发事件；

(e) 评审法，对确定性设计基准事故分析、超设计基准事故分析和安全分析报告进行评审、评定。

5.14. 作为一级概率安全评定基础的内部始发事件集应当尽可能全面。须承认，不可能证明已识别出所有可能的始发事件。但是，通过对第 5.13 段所列各种方法进行充分全面的组合应用，可以为已识别出尽可能全面的电厂始发事件集获得信心。

5.15. 在识别始发事件时，应当特别考虑所分析电厂的新的或独有的设计特点，其可能是新始发事件的潜在来源。对于缺乏或没有运行经验的新核电厂尤其重要，需要特别注意识别其特定设计所独有的始发事件、故障模式、事故序列和相关性。应当使用第 5.13 (a) 段规定的分析技术对所有的运行前沿系统、支持系统和备用系统进行分析，以识别可能由于运行故障、部分运行故障或意外运行而导致的始发事件（或可构成始发事件的继发性故障）。

5.16. 一级概率安全评定包括的主要始发事件类别是威胁安全功能（如反应堆堆芯余热的排出、一回路冷却剂装量的控制、一回路完整性的保持和堆芯反应性的控制）的事件。

5.17. 识别出的始发事件集应当包括功能和系统的部分和完全故障，例如，多个蒸汽发生器的给水减少或单一蒸汽发生器的给水丧失，以及所有蒸汽发生器给水的完全丧失。因为涉及部分故障的始发事件可能会给风险带来重要贡献，应对此予以重视。

5.18. 识别出的始发事件集应当包括在所有允许的电厂功率运行模式（例如，切除或不带某条环路的电厂运行）下可能发生的始发事件。

5.19. 始发事件集应当包括频率很低但潜在后果很重大的事件，例如，反应堆压力容器破裂或接口系统冷却剂丧失事故。若一级概率安全评定将被用作二级概率安全评定（可能是三级概率安全评定）的基础，则将接口系统冷却剂丧失事故纳入始发事件集就尤为重要。

5.20. 对于有多台核电机组的场址，应当识别会同时影响多个机组的始发事件集，例如，丧失场外电源。此外，应当识别出一台机组发生的始发事件而导致另一机组发生的始发事件，例如，关于内部危害的一级概率安全评定，所分析机组的始发事件可能因临近机组汽轮机解体产生的飞射物撞击导致。

5.21. 如第 5.13 段指出，应当将识别出的电厂始发事件集与类似电厂的始发事件集进行比较，确保所有相关的始发事件都包括在内。在发现差异时，应当补充纳入其他始发事件，或说明这些始发事件不相关的正当性。

5.22. 应对电厂（如果已运行）和类似电厂的运行经验进行评审，以确保所有已实际发生过的始发事件都被纳入一级概率安全评定所考虑的始发事件集中。

5.23. 应当识别始发事件的原因并在分析中加以考虑。对于有多个起因的始发事件，或者始发事件的发生需由多个故障引起的情形，通常方法是使用故障树分析来为始发事件建模。

瞬态

5.24. 一级概率安全评定应当基于可能发生的完整瞬态集。可能发生的瞬态类型的示例包括：

(a) 反应堆余热排出增加，例如打开二回路排放阀或蒸汽管线破裂；

(b) 反应堆余热排出减少，如主给水丧失或给水管线破裂；

(c) 反应堆冷却剂系统流量降低，如反应堆冷却剂泵停堆、卡泵或断轴；

(d) 反应性和功率分布异常，如控制棒的失控抽出、控制棒弹棒或硼稀释；

(e) 反应堆冷却剂装量增加，例如应急冷却剂注入系统的意外投运；

(f) 导致反应堆停堆或立即停堆的事件。

5.25. 应当将丧失场外电源作为内部始发事件纳入瞬态集。涉及丧失场外电源的始发事件应当说明其发生频率、丧失场外电源的持续时间，考虑到场外电源恢复的可能性。这应当基于与电厂所接入电网相关的设计和运行经验的细节。

5.26. 丧失场外电源可能归因于内部危害（如场内火灾）和外部危害（如极端环境条件或地震），当在针对这些危害的概率安全评定中对丧失场外电源进行明确建模时，为内部始发事件模式对丧失场外电源做的定义中应当排除前述原因以避免在一级概率安全评定中双重计算。

5.27. 始发事件集还应当包括支持系统的故障，例如电力系统、仪器仪表气源、冷却水系统、室内冷却系统、仪器仪表和控制系统。这对因支持系统的故障可能导致反应堆停堆且支持系统自身在反应堆停堆后承担作用的情形尤为重要。

冷却剂丧失事故

5.28. 在一级概率安全评定中应当考虑可能导致冷却剂丧失事故的完整始发事件集。

5.29. 识别出的冷却剂丧失事故集应当包括所有可导致一回路冷却剂丧失的破口的不同尺寸和位置。应当根据电厂的实际设计和布局确定可能的位置，冷却剂丧失事故集应当包括管道和阀门的故障，特别是排放阀的故障。

5.30. 应当识别出可导致一回路冷却剂在安全壳外部排放的冷却剂丧失事故集。其典型地包括蒸汽发生器传热管破裂和接口系统的冷却剂丧失事故。在这类事故中，来自破口的一回路冷却剂被旁流至安全壳外，因此不能用于安全壳地坑再循环。

5.31. 应当根据为防止堆芯损坏而必须投运的安全系统的成功标准，对识别出的冷却剂丧失事故集进行分类和分组。对于压水堆，主要基于对缓解冷却剂丧失事故的冷却剂注入系统的性能要求，通常将冷却剂丧失事故分

为大、中、小三类。根据电厂的设计，可能需要一套不同的设备来为例如涉及反应堆冷却泵密封故障的极小破口冷却剂丧失事故提供保护。

始发事件分组

5.32. 为了将一级概率安全评定所需的分析限制在可控的规模，在进行事故序列分析前应当首先进行分组。

5.33. 若为了进一步将概率安全评定模式限制在可控规模，则应对一些始发事件组进行筛选，将部分始发事件组排除在考虑之外，且所建立的筛选标准应当与实施概率安全评定的目的相一致，以免排除对风险有重大影响的因素。即使已进行了筛选，为实现特定概率安全评定的应用可能仍然需要对筛选结论重新检查。

5.34. 始发事件应当按组排列，同组始发事件具有以下相同（或极为相似）的属性：

(a) 始发事件后的事故进展；
(b) 缓解系统的成功标准；
(c) 始发事件对安全系统和支持系统可用性和运行的影响，包括需要的触发保护行动或阻止系统驱动的信号条件；
(d) 预计电厂运行人员响应。

5.35. 用于一个特定始发事件组的缓解系统成功标准，应当是对该组内所有单一事件而言最严格的标准。

5.36. 若已将事故进展和/或缓解系统成功标准有细微差别的始发事件分在了同一组，事故序列分析应当为这些始发事件的所有潜在事故序列和后果给定边界。

5.37. 对始发事件进行分组时，应当以不在分析中引入过度保守的方式进行。

5.38. 可能导致安全壳旁路的始发事件（例如蒸汽发生器传热管破裂或接口系统冷却剂丧失事故）应当不与事故后安全壳仍然保持有效的其他冷却剂丧失事故分在同一组。

5.39. 一级概率安全评定文档中应当包括为电厂识别出的所有始发事件的清单，并描述每起始发事件及提供识别其所使用方法的充分信息，如危害和可运行性分析、故障模式和影响分析，主逻辑图或运行经验评审。

事故序列分析

5.40. 分析的下一步是确定电厂对每个始发事件组（根据前述程序所识别出的）的响应，始发事件组要求安全系统运行以执行安全功能从而防止堆芯损坏。这种安全功能通常包括反应堆停堆并使其保持次临界状态、从反应堆堆芯中排出热量等（见第 5.45 段）。

5.41. 在事故序列中识别出的事件与安全系统的成败以及在执行始发事件组所要求安全功能时采取的人员行动相关。事故序列模式的终点对应于所有要求的安全功能都已成功实现后的安全稳定状态或堆芯损坏。

堆芯损坏

5.42. 对于构成堆芯损坏或特定程度的堆芯损坏 [8] 的特定内容，应当制定一项标准（或在适当时多项标准）。例如，对于轻水堆，通常假设若任何燃料参数（如包壳温度）超过其设计基准限值或更高的限值（若正当），则会发生堆芯损坏。

5.43. 然而，构成堆芯损坏的规范条件通常是采用间接标准。例如，对于压水堆，当堆芯顶部长时间裸露或包壳温度超过规定的最大值后，则假设发生堆芯损坏。若在堆芯顶部裸露后需要相当长时间才造成堆芯损坏的，则应当在对堆芯损坏做实际定义时予以考虑。

安全功能、安全系统和成功标准

5.44. 如第 5.3－5.39 段所规定，应对每个始发事件组进行事故序列分析。

5.45. 应当为每个始发事件组确定为防止堆芯损坏所需要执行的安全功能。所需的安全功能取决于反应堆类型和始发事件的性质，通常包括：

---

[8] 根据堆芯损坏程度，可规定堆芯损坏的若干状态。例如，在石墨通道型反应堆中，通常会根据结果严重性来考虑不同数量通道的损坏。确定堆芯损坏程度的另一个因素是时间，例如，延后的堆芯损坏。

(a) 始发事件和反应堆跳堆探测；

(b) 反应堆停堆并保持次临界状态；

(c) 反应堆堆芯热量排出；

(d) 保持一回路和安全壳的完整性。

5.46. 应当识别执行每个安全功能所需的安全系统和操纵员行动，包括用于执行安全功能的安全系统的成功标准。

5.47. 每个安全系统的成功标准应当确定为实现安全功能所需的最低性能水平，并考虑每个序列的特定特点。当涉及安全系统的冗余通道时，成功标准应当确定为需要运行的通道数。若涉及到多样性安全系统，则成功标准应当考虑每个多样性系统所需的性能。这可包括由最佳估计安全分析支撑的每个多样性系统的部分运行。

5.48. 应当识别由始发事件导致故障的安全系统并在制定成功标准时纳入考虑。例如，始发事件所致的支持系统（如电源和冷却水系统）故障，或由始发事件导致安全相关设备所在区域的严酷环境）。在两种情况下，都可能导致所需安全系统的故障。另一个示例是在压水堆大的或中等的冷却剂丧失事故的情况下，若破口出现在冷段，则来自应急堆芯冷却系统与该段相连通道的冷却剂流量将会丧失，这在确定成功标准时应当予以考虑。

5.49. 成功标准应当规定安全系统的任务时间，即需要安全系统运行的时间，以使反应堆达到安全、稳定的停堆状态，并允许采取长期措施以保持该状态。在许多情况下，对于大多数始发事件，需要 24 或 48 小时。对于提供了延迟堆芯损坏特点的新设计，可能需要考虑更长的任务时间。

5.50. 应当基于直接执行安全功能的前沿系统的成功标准，在成功标准中还应当明确对支持系统的要求。

5.51. 成功标准应当确定正如电厂程序规定的运行人员应当采取的行动，以使电厂达到安全、稳定的停堆状态。好的实践是由电厂运行人员、系统分析人员、人的可靠性分析人员共同协作来确定运行人员应当采取的行动。

5.52. 一级概率安全评定文档中应当包括为将反应堆带入安全、稳定的停堆状态，每起始发事件所要求的安全功能、安全系统、支持系统和运行人员行动的清单。

成功标准的支持性分析

5.53. 一级概率安全评定中使用的安全系统和支持系统的成功标准应当通过支持性分析来验证。支持性分析包括瞬态和冷却剂丧失事故后衰变热排出的热工水力分析、反应堆停堆及停堆后的保持的中子物理分析等。

5.54. 若可能，应当在一级概率安全评定中确定和使用基于最佳估计支持性分析的现实性成功标准。

5.55. 然而，若针对任何事故序列一级概率安全评定的部分安全系统采用了基于保守设计基准分析的保守成功标准则应当加以记录，同时应当仔细对整体分析结果进行评审，以确保这种保守性不会主导风险从而模糊一级概率安全评定分析得到的结论和意见。

5.56. 对如何满足关于一级概率安全评定计算机程序使用的参考文献[3]要求 18，本段提供了相关建议。用于证明成功标准的计算机代码应当很好地用于对瞬变进行建模，冷却剂丧失事故和所分析的事故序列进行建模，并获得最佳估计预测结果。计算机程序只应当在确定的适用范围内使用，并且只应当由经鉴定的计算机程序用户使用。应当尽可能使用避免了不必要保守性的最佳估计输入数据和假设。

事故序列建模

5.57. 应当识别每个始发事件组之后发生的事故序列。这通常是通过为每个始发事件组构建事件树来完成，它模拟安全系统、支持系统和人员行动在执行安全功能时的成功或失败。好的实践是，在构建事件树之前绘制详细的事件序列图（包括人员交互作用）。

5.58. 始发事件组事件树应当涵盖成功标准所规定的所有需要执行的安全功能和需要运行的安全系统。针对始发事件组的前沿安全系统的状态（成功或失败）通常构成特定事件树的标题，有时称为“事件树顶事件”。标题还可包括任何直接影响事故过程的运行人员行动，特别是根据应急运行程序规定应当采取的行动。对序列有直接和显著影响的任何其他事件也可以用作标题。

5.59. 事件树结构应当考虑表示运行人员行动和系统驱动的事件树标题的时间序列。最自然的实践是按照对系统或运行人员要求的时间顺序进行排序。

5.60. 事件树结构应当考虑由设备故障和人误导致的功能和实物的相关性（见第 5.87 段）。安全系统之间的相关性（通常称为系统交互）也应当在事件树中表示。

5.61. 事故序列分析应当包括安全系统响应始发事件组的成功或失败的所有相关组合，并应当识别因足够的安全系统已投运并执行了始发事件必需的所有安全功能带来成功结果或导致堆芯损坏状态的所有事故序列。

事故序列和电厂损坏状态终点

5.62. 事故序列分析将识别出两种事故序列：第一种是完全执行所有必需的安全功能，从而避免堆芯损坏；第二种是未执行一个或多个安全功能以致假想会发生堆芯损坏。若分析仅止步于一级概率安全评定，这种区分通常已经足够。然而，若目的是把一级概率安全评定结果作为二级概率安全评定的输入，通常实践是把引起堆芯损坏的事故序列按电厂损坏状态分组，由此形成一级概率安全评定和二级概率安全评定之间的接口。若将电厂损坏状态的确定作为一级概率安全评定的一部分，则更有裨益（而非将确定电厂损坏状态延后作为二级概率安全评定的第一步）。

5.63. 若正在进行二级概率安全评定，则应当定义一组核电厂损坏状态，其中应当考虑每个导致堆芯损坏事故序列的特征，堆芯损坏可能影响安全壳响应或导致放射性物质向环境排放。一级概率安全评定分析人员和二级概率安全评定分析人员之间应当合作确定电厂损坏状态。

5.64. 虽然通常由分析人员自行确定电厂损坏状态的特征，但其一般包括以下内容：

(a) 已发生的始发事件类型（完整的一回路或冷却剂丧失事故）；
(b) 已发生的、导致堆芯损坏的安全系统（反应堆保护系统、余热排出系统或应急堆芯冷却系统）故障；
(c) 堆芯损坏时一回路压力状态（高或低）；
(d) 堆芯损坏发生时间（相对于反应堆停堆时间的早或晚）；
(e) 安全壳完整性（完整、故障、隔离失效、由于蒸汽发生器传热管破裂或接口系统冷却剂丧失事故导致的旁路）；
(f) 具备或丧失压力控制能力的冷却剂丧失事故（用于沸水堆）；

(g) 堆芯损坏时抑制池的状态（过冷或饱和）（用于沸水堆）；

(h) 安全壳保护系统的可用性（安全壳喷淋、排热系统和氢气混合或复合）；

(i) 交直流电源的可用性和相关恢复时间；

(j) 已尝试且失败的运行人员行动。

上述内容仅适用于满功率运行工况下的概率安全评定。对于低功率和停堆状态，适用于一套与此不同的电厂损坏状态特征。

5.65. 导致堆芯损坏事故序列的表征应当根据每一事故序列导致核电厂的总体物理状态以及防止或缓解放射性物质泄漏的安全系统可能的可用性来确定。

5.66. 一级概率安全评定文档应当提供已经绘制的事件树，以确定事故序列进展，并且应当描述事件树结构背后的逻辑。这之所以重要，是因为事件树图本身不提供推理，只提供推理的结果，若不伴以文字描述作参考，则难以完全理解。

5.67. 文档应当就事件树标题提供解释性信息。例如，事件树标题可以表示简单功能，也可以表示复合事件（在一个标题下包含多个功能）。应当清楚地给出并阐释在事件树开发过程中所做的假设和相应的标题定义。

5.68. 文档还应当描述电厂损坏状态，并说明其是如何确定的。

系统分析

5.69. 分析的下一步是对事故序列分析中识别出的系统故障进行建模。其通常是通过故障树分析来进行的，故障树的顶事件被作为事件树分析所识别的系统故障状态。故障树将分析延伸到单一基本事件，通常包括部件故障（泵、阀、柴油发电机等发生的故障）、维护或试验期间部件不可用、冗余部件的共因故障以及代表人误影响的人因故障事件。

5.70. 需要绘制的故障树范围取决于事件树的大小和复杂性，事件树越详细，故障树就越简单。[9]

[9] 其他技术也可能用于概率安全评定的特定方面。然而，通常方法是采用故障树和事件树的组合，并假设采用此方法（详见第 5.4－5.6 段）。

故障树分析

5.71. 故障树开发旨在就事件树分析识别出的安全系统故障状态提供一种逻辑的故障模式。

5.72. 为每个安全系统功能故障树顶事件提供的故障标准应当与如第 5.47－5.56 段指出事故序列成功标准在逻辑上互逆。某些情况下，同一安全系统可能需要多个故障树模式，以处理对不同始发事件组所确定的成功标准，或在事件树不同分支中处理所确定的成功标准，这取决于对系统要求之前的事件序列。解决措施包括开发不同的故障树模式或根据成功标准使用逻辑开关（所谓的“房子事件”）来禁用或启用故障树模式的相关部分。

5.73. 故障树中建模的基本事件应当与可用的部件故障数据相匹配。在故障树中建模的部件范围和部件故障模式应当与部件故障数据中定义的相一致。这对于能动和非能动部件都同样有效。

5.74. 故障树模式开发应当达到单一部件（泵、阀门、柴油发电机等）重要故障模式级别以及单一人因故障级别，且应当包括所有的基本事件，该等事件可能直接单独导致或与其他基本事件共同导致故障树顶级事件。分析级别通常由分析人员自行决定，但它应当与可用的部件故障数据和所建议的一级概率安全评定应用相一致。

5.75. 在故障树中建模的基本事件集应当通过系统分析进行识别（例如，通过故障模式和影响分析，该分析已作为设计评定的一部分得以实施，以识别部件重要故障模式），还根据任务分析对运行人员行动做评审，以识别潜在人因故障。

5.76. 故障树模式应当包括所有需要运行的安全系统部件和支持系统部件。故障树模式还应当包括非能动部件，其故障可能导致系统故障，例如，未被探测出的过滤器堵塞和管道泄漏。开发故障树模式应当确保清楚明确地考虑了功能关联性和部件故障关联性。忽视或遗漏前述关联性的模式可能会使结论发生严重偏差并低估支持系统的相对重要度。

5.77. 故障树中的部件分辨级别应当足以确保对所有硬件关联性进行建模。例如，在同一系统向多个部件提供冷却水的情况下，应对该冷却水系统进行明确建模。可用的部件可靠性数据也应当在确定分辨级别时加以考虑（可能获得整台泵的可靠性数据，但不能得到泵的组成部分的可靠性数

据，如转轮、联轴器、轴承等）。此外，在确定故障树中部件分辨级别时，还应当考虑概率安全评定所要求的对电厂设备或设备单一零部件的风险重要度的意义。

5.78. 将单一部件组合在一起并使用复合事件对其故障进行建模时，应当证明复合事件中每个部件的故障模式对系统的影响与复合事件自身对系统的影响是相同的。此外，模式中包含的所有复合事件在功能上都应当是独立的，即单一部件应当不出现在多于一个复合事件中，或作为基本事件在别处出现。

5.79. 故障树模式应当考虑安全系统中的单一部件或设备通道，其可能在电厂寿期中因试验、维护或维修而停用。在故障树分析中，应当就前述部件或设备通道进行明确的识别和建模。这可以通过例如在故障树中包含表示部件停用的基本事件来完成。

5.80. 由于维护而导致系统不可用的建模方法应当与电厂的技术规范 [10] 和维护实践相一致。

5.81. 在故障树模式中，应当开发一个对每个逻辑门和基本事件进行唯一编码或标签的系统，并在为一级概率安全评定开发的完整逻辑模式中始终如一地使用该系统。

5.82. 模式开发应当与建议的一级概率安全评定的应用相一致。例如，若一级概率安全评定用于风险监控应用，模式应当与之相对称，对可能发生在所有位置的始发事件进行建模，包括所有一回路环路、安全系统的所有通道、常规运行系统的所有运行和备用通道。对称模式的开发允许直接使用一级概率安全评定计算机程序计算重要度 [11]。

所需系统信息

5.83. 应对在一级概率安全评定中建模的每个安全系统进行功能描述，以确保为开发中的逻辑模式提供有效和可审核的基础。功能描述通常包括以下内容：

---

[10] 在维护停用建模时，通常假设电厂在技术规范规定的运行限值和条件下运行。

[11] 关于重要度计算的示例见第 5.15 段。

(a) 系统功能；
(b) 系统故障模式；
(c) 系统边界；
(d) 与其他系统的接口；
(e) 正在建模的运行模式（适用于具有多个模式的系统）；
(f) 需要运行的或需要改变状态和正常配置的部件；
(g) 部件运行需手动还是自动；
(h) 部件接收自动信号必须具备的条件。

5.84. 应当为每个系统配备简化示意图，以显示故障树中建模的系统，包括：

(a) 在故障树中建模的系统所有部件；
(b) 部件的正常配置；
(c) 连接各部件的管段或接线段；
(d) 支持系统接口（动力、电气、冷却等）。

5.85. 安全系统的功能描述和示意图应当为故障树开发提供明确的依据。一级概率安全评定文档中应当提供如何在故障树开发中使用这些信息的说明。

相关故障分析

5.86. 应当特别考虑在为一级概率安全评定开发的逻辑模式中处理关联性，因为在过去已进行的概率安全评定中发现，相关故障是堆芯损坏频率的主要贡献者之一。

5.87. 有可能发生四种不同类型的关联性：

(1) **功能关联性**包括由电厂工况引发的关联性，例如，泄压失败导致低压注入不可用，以及由于共用部件、共用驱动系统、共用隔离需求或共用支持系统（动力、冷却、仪控、通风等）而产生的关联性；
(2) **实体关联性**（也称为**空间交互关联性**）由于可能导致安全系统设备故障的始发事件引起的。这可能是由于管道甩动、飞射物撞击、飞机坠毁或环境影响造成的；

(3) **人因交互关联性**是由于人因故障引发或导致始发事件，或造成一个或多个安全系统设备的不可用或故障，以致其在始发事件后无法按要求发挥作用；

(4) **部件故障关联性**是由于设计、制造或安装方面的错误或电厂运行期间的人员错误而导致的。此类关联性可以通过共因故障分析来处理（见第 5.92－5.95 段）。

5.88. 应对电厂的设计和运行进行系统的评审，以识别可能出现的潜在关联性，这些关联性可导致安全系统部件在应对始发事件时不可用或可靠性降低。

5.89. 所有功能和实体关联性应当在事件树或故障树模式中明确建模。人因交互关联性和部件故障关联性也应当建模，这些将在第 5.96－5.113 段关于人的可靠性分析和第 5.92－5.95 段关于共因故障分析中做进一步讨论。

5.90. 在故障树模式中，应当考虑系统中可能出现的所有功能关联性，并在故障树分析中就此进行明确识别和建模。对于分析人员来说，良好实践是将所有这些关联性列在一个系统关联性矩阵中，它可以用作构建故障树的基础，并且有助于评审人员进行检查。在系统的共因故障概率中，功能关联性应当不包括在部件故障关联性中。相反，部件故障关联性应当为尚未明确识别出来的不确定关联性作预留，通过 β 因子和类似模式进行量化。

5.91. 由于共用部件或支持系统而可能出现的系统间功能关联性时，应对此在故障树分析中明确识别和建模。值得注意的是，在联接事件树法中（见第 5.6 段），可使用边界条件法处理系统间的功能关联性。这种关联性可能出现在执行相同安全功能的独立安全系统中，也可能出现在相关的支持系统中，均应当明确包含在故障树中。

共因故障分析

5.92. 对于可能出现部件故障关联性的情形，应当识别出冗余设备集并包含在一级概率安全评定部件共因故障分析模式中。在一级概率安全评定中，可采用多种方法对共因故障建模，所选择的方法应当得到所收集数据的支持。良好实践是系统内和系统间的共因故障事件都加以处理。

5.93. 可能影响冗余部件组的共因故障，应当使用概率安全评定软件的适当功能进行识别和建模，这通常在故障树中完成。分析应当识别所有相关的部件组和重要故障模式。应当在一级概率安全评定文档中陈述为防范共因故障所做的任何假设。

5.94. 应当为一级概率安全评定中包含的部件每个故障模式的共因故障概率说明正当性。为此应当考虑系统的冗余度、部件的设计方面、系统布局（分隔、隔离、部件鉴定等方面的水平），以及系统的运行、试验和维护情况。

5.95. 在可能的情况下，共因故障概率应当基于电厂的特定数据，并考虑类似电厂的运行数据和通用数据。如使用通用的共因故障参数计算共因故障概率，则应当分析并论证这些数据的适用性。通用数据源中的部件边界、故障模式和故障根因应当与概率安全评定中的假设相一致。若采用专家判断法为共因故障参数赋值（当电厂特定数据和通用数据均不可用时），应对数据提供适当的解释，同时，所赋的误差因子应当与在确定共因故障参数过程中的不确定性相匹配。

人的可靠性分析

5.96. 应当识别出可能导致安全系统故障的人因故障，并将其包含在逻辑模式中。应当采用结构化和系统化的方法来识别人因故障，将这些故障纳入电厂逻辑模式（事件树和故障树）中作为人因故障事件，并量化此类事件的概率，即人因故障概率。采用结构化、系统化的方法进行全面的分析，以确定所有类型人因故障对堆芯损坏频率的贡献，使结论更具置信度。鉴于现有核电厂设计中通常包含了安全系统的高度冗余性、多样性和可靠性，涉及导致始发事件或无法对其进行缓解的人因故障的故障序列，往往对堆芯损坏频率有重大贡献。一个有用的起点是将所采用的方法与通常使用的方法作对比，以确保实施了人的可靠性分析所需的所有步骤。

5.97. 第 5.98－5.113 段所提出的建议涉及在一级概率安全评定中对人员行为的经典静态表现，这是最常用的方法。但在近年来采用了更先进的方法，考虑人员行为在与工作环境动态交互中的认知层面因素，但此处不就此展开。

5.98. 尽管近年来人的可靠性分析技术有所改进，但方法众多，该领域的技术水平仍在不断提高。应当正确地应用和记录所选择的方法。

5.99. 人的可靠性分析的目的应当是获得人因故障的概率，此类概率彼此相容，且应当与在一级概率安全评定其他部分所进行的分析一致。

5.100. 开展人的可靠性分析时应当与电厂运行和维护人员密切合作，以确保分析可反映电厂的设计特点及其在正常和事故工况下的运行情况。此若不可行（例如，若要在设计阶段对电厂进行分析），分析人员应当使用其他或类似电厂的信息，或者应当清楚地说明分析所基于的假设。

人员交互的识别

5.101. 应当通过结构化和系统化的程序来识别需要包含在一级概率安全评定中的人员交互行为，包括所有类型的人员交互，如第 5.102－5.105 段指出，其故障可能对堆芯损坏频率产生贡献。

5.102. 人的可靠性分析应当包括在始发事件发生前可能导致与安全相关的设备和系统故障或不可用的人因故障（通常称为 A 类人员交互）。这些人因故障可能发生在维修、维护、试验或校准任务期间。若这些故障一直未被发现，受其影响的部件或部件组将在始发事件后需求时不可用。特别重要的是，此类交互作用可能导致安全系统多个通道的同时不可用。这些不可用来源包括在部件、通道或系统级的模式中。

5.103. 应对电厂程序进行系统评审，以识别电厂运行人员为一级概率安全评定中已建模系统所进行的维修、维护、试验和校准任务，从而确定 A 类人员交互。评审应当确定发生故障的可能性以及这些潜在故障对安全系统设备的可用性或故障的影响。

5.104. 应当进行系统的评审，以识别可能导致始发事件的潜在人因故障（B 类人员交互）。至少应当通过评审确保在评价分析中所使用的始发事件频率已考虑了可能导致始发事件的人因故障。

5.105. 应对电厂程序进行系统的评审，以识别在发生始发事件（C 类人员交互）后电厂运行人员需要采取的关键行动。评审应当确定发生故障的可能性，以及这些潜在故障对部件或系统的可用性或故障的影响。C 类人员交互通常对堆芯损坏频率有重要贡献，因此通常是在一级概率安全评定中识别的最重要人员交互。

5.106. 为了表示人因故障的影响，应当将人因故障事件作为基本事件纳入故障树中，或者用作事件树标题。

人因故障概率的推导

5.107. 推导出的人因故障概率应当针对不同情形且反映可能影响运行人员表现的各种因素，包括压力大小、执行任务的可用时间、运行程序的可用性、受培训程度、环境条件等，这些因素（通常称为“表现修正因素”）应当通过任务分析予以识别。

5.108. 用于推导人因故障概率的方法应当与一级概率安全评定中通常使用的方法一致，或者应当明确证明其正当性。

5.109. 每个关键的人员交互都应当进行定性描述，应当详细说明与电厂运行人员行动相关的所有重要事项，通常包括以下内容：

(a) 行动的时间；
(b) 电厂相关程序；
(c) 实施行动所处的环境；
(d) 运行实践，例如运行人员团队的机构及其职责；
(e) 先前行动对当前行动的影响；
(f) 运行人员可获得的信息、所受过的培训等。

5.110. 应当使用适当的技术对特定的人员交互模式进行评审，例如，演练或通话程序。此外，通过模拟机练习中观察运行人员的表现和人员交互将为支持人的可靠性分析提供有用信息。

5.111. 电厂的安全文化也将对人因故障概率造成影响，但目前在认识人因故障概率方面还没有一个公认的方法将安全文化考虑在内。

处理人因故障事件之间的关联性

5.112. 逻辑模式中的人因故障事件之间可能存在相互关联性。这种相互关联性可能是由于使用共同的提示或程序步骤、错误的程序、错误的诊断或错误的执行应对方案等而产生。若同一序列的人因故障事件之间具相关联性，可能显著增加人因故障概率。在分析中应当识别和量化人因故障事件之间的相互关联性。

5.113. 所有涉及多重人因故障事件的可测量割集（见第 5.9 段）应当予以识别。可通过将人因故障概率设置为高值（例如 0.9）并重新计算堆芯损坏频率来识别此类割集，涉及多重人因故障事件的割集将出现在割集清单的顶层。应当评审在同一割集中合并的人因故障事件集，以确定它们之间的关联程度；模式量化中使用的人因故障概率应当反映这种关联程度。

其他建模问题

非能动系统

5.114. 当前的趋势是在改进的电厂设计中加入执行安全功能的非能动系统，如衰变热排出和应急堆芯冷却。非能动系统被认为比能动系统具有更高的可靠性，因为它们不依赖支持系统（如电力和冷却水），并且可能不需要保护系统的能动启动。

5.115. 应当通过热工水力分析、实验和试验来建立各非能动系统运行的边界条件。这些边界条件涉及系统的温度、压力、装量等。若满足边界条件，则可假想非能动系统将运行。若不满足边界条件，则假想非能动系统将无法执行其功能。

5.116. 应当在分析中模拟非能动系统的故障并评定故障概率。非能动系统的建模应当考虑到无法满足系统运行边界条件的概率，并应当使用标准故障树建模技术来处理部件故障（止回阀或安全阀打开失败、管道堵塞等）、设置系统时的人因故障以及启动失败（若需要外部启动）。还应当考虑支持性分析中的不确定性。

基于计算机的系统

5.117. 基于计算机的系统将越来越多地用于核电厂的控制和保护系统中，预计这种趋势将持续下去。基于计算机的系统依赖于硬件和软件。硬件的可靠性可以用标准技术来评定，软件的可靠性一定程度上可以通过核实和确认程序加以解决。然而，在一级概率安全评定中为基于计算机的系统建立可靠性模式比纯硬件系统的建模难度更大，因为对于如何就软件的故障建模还未形成共识。

5.118. 因故障的总概率可能主要取决于软件的故障，同时目前无法推导出一个软件故障 [12] 的概率模式，所以应当基于软件生产的质量进行判断，即软件编程过程中是否遵循充分的流程以减少软件生产中错误的可能性，是否进行了充分的检查以发现软件中的错误（静态分析），是否对已完成的软件进行了充分的试验（动态试验）。

5.119. 软件可靠性目前是一个活跃的研究领域。但是，若考虑到软件设计、生产和试验的所有相关因素对软件可靠性作出了判断，则可将其纳入一级概率安全评定模式。

5.120. 当控制和保护系统或者执行相同安全功能的两个多样性系统都是基于计算机的系统，应当考虑这两个计算机系统硬件和软件是否存在关联性，如有，则应当在一级概率安全评定中予以考虑。

一级概率安全评定所需数据

5.121. 第 5.121－5.139 段就始发事件频率、部件故障概率、部件大修频率和持续时间所需数据提出了建议。第 5.95 段和第 5.107 段分别讨论了共因故障概率和人因故障概率所需的数据。第 5.121－5.139 段也就如何满足参考文献[3]要求 19 关于使用运行经验数据的建议。

5.122. 需要解决的主要问题之一是，若电厂特定经验有限或缺乏，现有数据是否适用于本电厂的设备设计和运行机制。

5.123. 应当尽可能使用电厂自身的数据，并在表明其合适性的情况下辅以类似电厂的相关数据，这将提供更广泛的数据来源。但是，对新电厂或只运行了相对较短时间的电厂而言，缺乏电厂自身的数据。此种情况下，应当使用来自类似电厂的数据。若无法获得前述数据，则应当使用来自所有类型核电厂运行的通用数据。

5.124. 若可用的运行数据未表明故障的发生，则应对始发事件频率和部件故障概率的取值进行合理论证。

---

[12] 此处，“软件故障的概率模式”是指始发事件后，虽然正确的参数值已输入计算机系统，但由于软件错误导致未产生正确输出的概率以及由软件错误所引起的后果。

5.125. 应对用于一级概率安全评定的数据提供论证。通常的实践是比较来自许多不同来源的数据并确定是否可以解释任何差异。一般来说，在选择最优数据源时需要进行判断。

5.126. 如需组合使用电厂自身数据和来自不同来源的通用数据，则应当说明用于选择自身数据或合并来自多个来源数据的方法。这可以用贝叶斯方法或通过判断来实现。

5.127. 对于发生频率低的始发事件或故障概率低的设备，即使是基于通用数据库，数据也稀少或缺失，需通过基于知识和经验的判断来选取一级概率安全评定中使用的数值。应对这种判断所依据的理由进行解释。

始发事件频率

5.128. 应对在一级概率安全评定中建模的每个始发事件组确定一个频率。在确定频率时，应当考虑所识别出的导致始发事件的所有原因。

5.129. 除了第 5.123－5.127 段提到的技术之外，评定始发事件频率的另一种方法是使用故障树。该故障树提供所有设备故障和人因故障的逻辑模式，这些设备故障和人因故障的组合可导致始发事件的发生。应当检查故障树的预测结果是否与运行经验相一致。

5.130. 频繁发生始发事件频率的取值应当与所考虑的电厂和类似电厂的运行经验相一致。

5.131. 应当计算始发事件组的频率。始发事件组的频率应当为纳入该组中所有单一始发事件的频率之和。

5.132. 一级概率安全评定报告应当给出为电厂所识别的每个始发事件及始发事件频率的均值、给频率取值的正当性以及不确定性程度。

部件故障概率

5.133. 应当给分析中的每个部件或每类部件的故障概率赋值。故障概率的确定应当与部件的类型、运行机制、一级概率安全评定模式中确定的部件边界及其故障模式相一致。

5.134. 应对一级概率安全评定量化所用的部件故障概率数据提供论证。

5.135. 对于在停堆后需运行一定时间的部件，例如泵，应当明确其任务时间。任务时间的确定应当考虑达到安全、稳定的长期停堆状态和完成长期恢复操作所需的时间。对于某些始发事件，如冷却剂丧失事故，任务时间可能会很长。

5.136. 一级概率安全评定文档应当给出一级概率安全评定量化所用的所有部件故障数据，包括部件边界、故障模式、平均故障概率、与数据相关的不确定性、使用的数据源以及所使用数据正当性的描述。

部件大修频率和持续时间

5.137. 一级概率安全评定的量化应当考虑到部件和系统因试验、维护或维修所致的不可用。部件大修频率和持续时间所用的数值应当真实地反映电厂在用的或计划的实际情况。

5.138. 在可能的情况下，应当根据从电厂维护记录和部件不可用记录的分析中获得的电厂自身数据，确定大修频率和持续时间，并辅以类似电厂的数据。若此无法做到，只要能证明这些数据可反映电厂运行的实际情况，也可使用通用数据或制造商的数据。

5.139. 一级概率安全评定报告应当提供部件不可用性数据，并应对所使用的数值提供论证。

分析的量化

5.140. 一级概率安全评定开发的逻辑模式应当使用第 5.121－5.139 段所示的数据进行量化。应当使用始发事件频率、部件故障概率、部件大修频率和持续时间、共因故障概率和人因故障概率的数据计算事故序列频率。

5.141. 对于使用小事件树和大故障树组合的方法（故障树联接法请参阅第 5.5 段),应对采用事件树和故障树为每个始发事件组开发的逻辑模式进行布尔约简。在量化一级概率安全评定之前，应当注意确保模式中不存在逻辑循环。如有，量化前应当先打破循环。一级概率安全评定报告应当给出模式中任何逻辑循环被打破的方式和细节。

5.142. 为满足参考文献[3]（关于一级概率安全评定使用计算机程序）要求 18，第 5.142 段和第 5.143 段提供了建议。一级概率安全评定的量化应当使

用经过充分验证和确认的计算机程序进行。许多复杂的一级概率安全评定计算机程序可用于分析，这些计算机程序可由商业渠道获得，或已由不同的国家开发。

5.143. 使用计算机程序的用户应当具有充分的经验，并且理解计算机程序的使用和限制。

5.144. 一级概率安全评定模式量化的总体结果应当包括以下内容：

(a) 堆芯损坏频率（点估计和不确定性界限或概率分布）；
(b) 每个始发事件组对堆芯损坏频率产生的贡献；
(c) 割集和割集频率（对故障树链接法）或假想方案和假想方案频率（对带边界条件的事件树方法）；
(d) 敏感性研究和不确定性分析结果；
(e) 用于解释一级概率安全评定的重要度（如基本事件的风险增加值和风险减少值）；
(f) 提供一级概率安全评定和二级概率安全评定之间接口的电厂损坏状态频率，其中一级概率安全评定结果将用作二级概率安全评定的输入。

5.145. 分析人员应当根据概率安全评定开发过程中所做的的假设，检查由求解一级概率安全评定模式识别出的的事故序列或割集确实会导致堆芯损坏。这种检查应当针对序列的样本进行，重点关注对风险有重大贡献的序列。此外，还应当进行检查，以确认预计会导致堆芯损坏的始发事件和部件故障组合的割集已确已包含在生成的割集清单中。

5.146. 分析人员应对在第 5.145 段使用“对风险有重大贡献”术语进行定义。该定义可以采用绝对标准或相对标准的形式（例如相对于总堆芯损坏频率）。

5.147. 应当检查已经在割集上执行的后处理（移除互斥事件或引入未明确包含在一级概率安全评定模式中的恢复运行）产生了正确的结果。后处理通常用于故障树联接方法。

5.148. 一级概率安全评定文档应当提供一级概率安全评定的量化结果，并应当描述最重要的序列和割集（对故障树联接方法）以及已执行的任何后处理。

5.149. 分析人员应当提供第 5.148 段使用的术语“重要序列”和“重要割集”的定义，可采用绝对标准或相对标准的形式（例如相对于总堆芯损坏频率）。

5.150. 为了量化一级概率安全评定，需要规定截断值来限制分析所需的时间。通常方法是设置一个频率截断值，使分析中不包括低于此频率的割集（也可以规定阶次截断值，使分析中不包含阶次大于规定水平的割集）。应当说明截止值已被设置在足够低的水平，既使一级概率安全评定整体结果收敛，截段又不会导致对堆芯损坏频率的严重低估。截断值的选择可因概率安全评定的应用而异。

重要度分析、敏感性研究和不确定性分析

重要度分析

5.151. 应对基本事件、基本事件组、安全系统、始发事件组等的重要度进行计算，并将其用于解释概率安全评定的结果。在一级概率安全评定中使用的重要度通常包括：

(a) F-V 重要度 [13]；

(b) 风险减少值 [14]；

(c) 风险增加值 [15]；

(d) 伯恩鲍姆（Birnbaum）重要度 [16]。

衡量重要度的不同尺度可提供一个视角，即哪些基本事件对当前的风险评定贡献最大（F-V 重要度，风险减少值），哪些对保持安全水平贡献最大（风险增加值），结果对哪些基本事件最敏感（伯恩鲍姆重要度）。

[13] 对于特定的基本事件，F-V 重要度是指包括该特定基本事件的所有事故序列对总堆芯损坏概率的贡献份额。

[14] 风险减少值是指当特定的故障模式概率被认为是零时，堆芯损坏概率的相对下降值。风险减少值是设备可靠性的直接函数，并可被用于评定故障模式对堆芯损坏频率的贡献。

[15] 风险增加值是当某一特定设备项的故障是确定时，堆芯损坏概率的相对增加值。风险增加值是衡量设备所执行功能的重要性。它可以识别设备在安全方面所起的作用，即使该设备的故障率非常低。

[16] 伯恩鲍姆（Birnbaum）重要度是衡量部件故障相较于其正常运行时在风险方面的增加。

不确定性的类型

5.152. 第 5.152－5.160 段提供了如何满足参考文献[3]要求 17（关于一级概率安全评定的不确定性和敏感性分析）的建议。需认识到，在一级概率安全评定所开发的模式和使用的数据中存在着不确定性。当使用概率安全评定的结果来分析风险或支持决策时，应当处理这些不确定性。可以通过进行适当的敏感性研究或不确定性分析来实现。一级概率安全评定的不确定性通常分为以下三大类：

(1) **不完整性不确定性**：一级概率安全评定的总体目标是进行系统分析，以识别对堆芯损坏频率有贡献的所有事故序列。但无法保证此过程的完整性，也不能保证已识别出所有可能的情况并得到适当的评定。这种潜在的不完整性在分析结果和结论中引入了一种难以评定或量化的不确定性。要清晰无误地处理这种不确定性是不可能的；

(2) **建模不确定性**：这种不确定性是由于对分析中所使用的方法、模式、假设和近似的适当性方面缺乏完整的认知所引起的。可通过敏感性研究来处理其中某些因素的重要度；

(3) **参数不确定性**：这是由于在一级概率安全评定量化中使用参数的不确定性引起的。该类不确定性通常通过不确定性分析来处理，分析中指定所有参数的不确定性分布并通过分析进行传播。

5.153. 在设计评价和决策过程中，需考虑如何利用不确定性信息。然而，应当注意到，堆芯损坏频率的风险标准或目标通常涉及点估计 [17] 而非不确定性分布。一级概率安全评定用于识别薄弱点的方式也与点估计相关，而不是与不确定性分布相关。

敏感性研究

5.154. 应当开展敏感性研究以确定一级概率安全评定结果对所作假设和所使用数据的敏感性。

5.155. 敏感性研究应当针对具有显著不确定性水平的假设和数据来进行，这些假设和数据可能对一级概率安全评定的结果产生显著影响。敏感性研

[17] 在此处，点估计可以是通常由概率安全评定计算机程序计算出来的点估计或另一参数或概率分布的分位数，例如平均数或中位数。

究应当通过使用替代假设或使用可反映不确定性水平数据的一系列数值进行重新量化分析。

5.156. 分析人员应当提供“对一级概率安全评定结果的显著影响”术语（如在第 5.155 段所用）的定义。该定义可以采用绝对或相对形式的数值标准（见第 5.146 段）、定性标准（例如引入新的事故序列）或定量和定性标准的结合（例如引入新的重大事故序列）。

5.157. 敏感性研究的结果应当被用来说明从概率安全评定获得结论的置信度水平，即是否已满足堆芯损坏标准或目标、设计是否平衡、在电厂设计和运行方面是否存在可能的薄弱点，这些薄弱点在一级概率安全评定基准情况下（敏感性情况与其相比较）没有被特别强调。

5.158. 值得注意的是，敏感性研究通常每次只针对一个假设或一个参数展开，研究的结果没有统计学意义。也可以就相关假设组合的敏感性进行分析。

不确定性分析

5.159. 应当通过不确定分析确定一级概率安全评定的结果中的不确定性，该不确定性来自用于一级概率安全评定量化的数据。

5.160. 应当确定一级概率安全评定量化所用参数的不确定性分布。这可作为数据分析的一部分来完成。这些不确定性分布应当通过分析进行传播，以确定始发事件组发生频率、堆芯损坏频率等的不确定性。这些不确定性应当用于反映达到风险标准或目标的置信度水平。

6. 一级概率安全评定关于内部和外部危害的一般方法

概述

6.1. 除了可能导致内部始发事件的部件随机故障和人因故障（如第 5 部分所述）之外，故障序列可能是由其他危害造成的损坏引起。本部分就如何满足参考文献[3]要求 6－13（关于一级概率安全评定的其他危害）提出建议。其他危害可分为：

(a) 源自核电厂场址范围内（包括厂房内和厂房外）的**内部危害**。内部危害包括内部火灾、内部水淹、汽轮机飞射、现场运输事故和从现场存储设施排放的有毒物质；

(b) 源自核电厂场址范围之外的**外部危害**。外部危害包括地震危害、外部火灾（例如源自附近森林火灾并影响到现场的火灾）、外部洪水、强风及风致飞射物、场外运输事故、场外存储设施有毒物质排放和严酷气候条件。

上述危害可能会损坏电厂的部件，从而产生可能导致堆芯损坏的事故序列（或其他需要在一级概率安全评定中考虑的最终状态）。通常，这些危害可能同时影响许多不同的设备，并对电厂人员造成不利影响。在一级概率安全评定中应当包括内部和外部危害。[18]

分析过程

6.2. 应当采用统一的方法来识别内部和外部危害，并分析其对堆芯损坏频率的贡献。内部和外部危害分析的主要步骤通常包括：

(1) 收集内部和外部危害的初始信息；

(2) 危害识别，包括单一危害和危害组合；

(3) 危害筛选分析，含定量和定性分析；

(4) 边界评定；

(5) 详细分析。

分析的总体方法如图 2 所示。

[18] 本“安全导则”不针对由战争或恶意破坏或恐怖行为等始发事件提供建议。但是，应当考虑军事设施或和平时期活动的偶发性危害（例如军机的坠毁）。

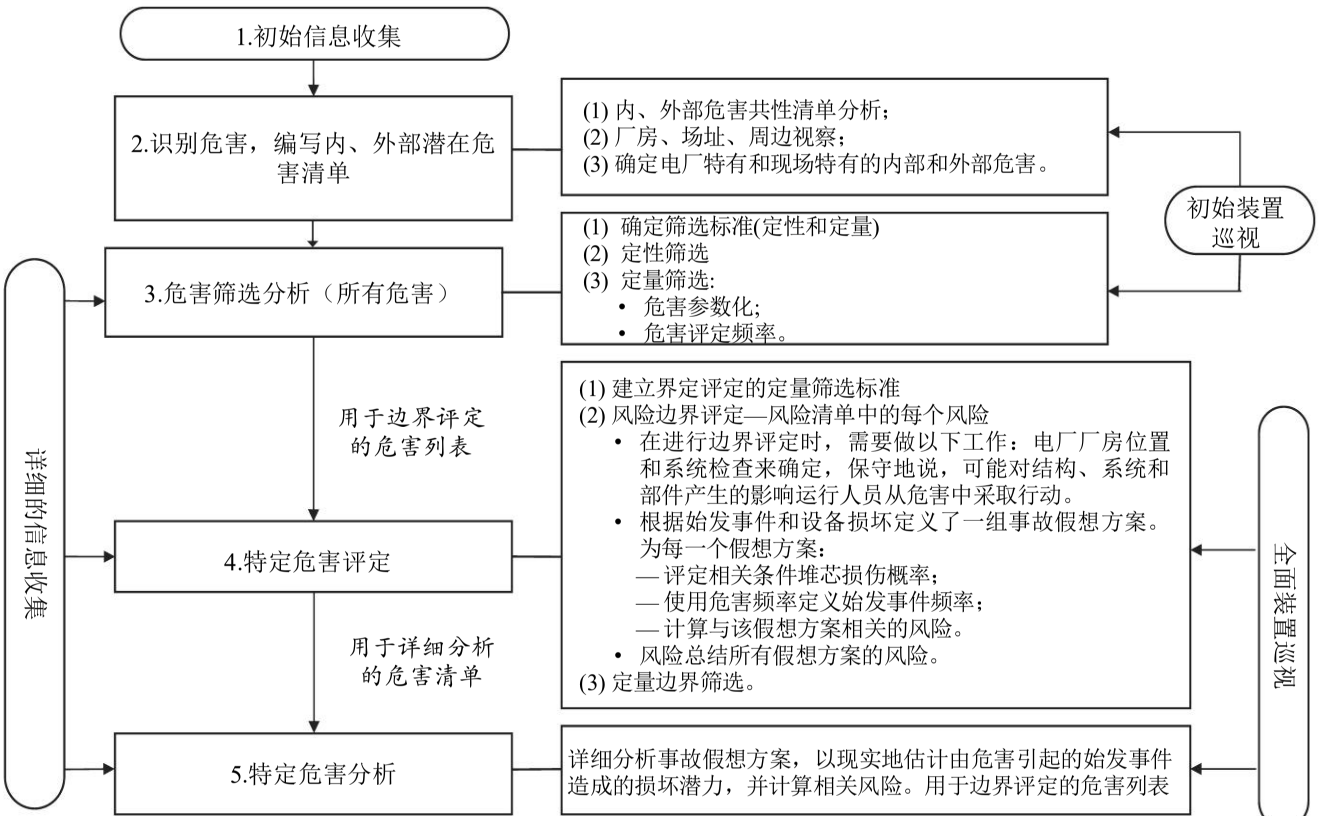

图2. 内、外部危害的一级概率安全评定分析总体方法

6.3. 虽然识别和筛选内部和外部危害的步骤是相似的，但对每一种危害的边界评定和详细分析可能涉及对该危害的特有任务，例如，在内部火灾情况下，需要对火灾蔓延进行分析。本部分讨论危害的识别和筛选工作，这些工作对内部和外部危害而言都是类似的，关于特定危害的边界评定和详细分析的特定建议，对内部危害见第 7 部分，对外部危害见第 8 部分。

6.4. 所有可能影响电厂的潜在内部和外部危害都应当加以考虑，并应当适当进行筛选分析、边界评定或详细分析。

6.5. 如第 5.141 段指出，在内部始发事件的一级概率安全评定中，为了消除逻辑循环，通过删除代表部件随机故障的子模式来建立精简的故障树模式。例如，为了消除供水和供电之间的逻辑循环，删除了特定总线的故障树链接。由内部和外部危害造成的这些部件（其随机故障已从逻辑模式中删除）的相关故障，应当纳入内部和外部危害的一级概率安全评定模式中。

初始信息的收集

6.6. 在内部和外部危害一级概率安全评定之初，应当收集所有与内部和外部危害相关的可用信息。这些信息至少应当包括：

(a) 安全分析报告中考虑的内部和外部危害相关的设计信息；
(b) 电厂厂房、结构、系统和部件的清单和布局；
(c) 场区布局和场址及周边的地形；
(d) 与危害物质相关的管道位置、运输路线以及厂、内外存储设施的信息；
(e) 场址周边工业设施的位置；
(f) 本场址及该区域内发生任何内部和外部危害相关的历史信息。

6.7. 在内部和外部危害一级概率安全评定的过程中，应当根据每个危害筛选分析、边界评定或详细分析所需的详细程度，对初始信息进行更新和扩展。

危害识别

6.8. 危害识别应当旨在生成一份内、外部潜在危害的综合清单。特定危害的示例包括：

厂房内的内部危害：

(a) 内部火灾；
(b) 内部水淹；
(c) 内部飞射物；
(d) 内部爆炸；
(e) 重物坠落。

外部自然灾害：

(a) 地震危害；
(b) 外部火灾；
(c) 外部洪水；
(d) 强风；
(e) 生物现象，例如，冷却池内鱼类数量异常等；
(f) 极端气象条件[19]。

外部人因引发危害：

(a) 场外爆炸；
(b) 场外有毒物质排放；
(c) 飞机坠毁。

6.9. 为了确保危害识别过程是全面和可追溯的，应当采用以下的两步法：

(1) 使用国际上已有的内部和外部危害分析方法。初始时，应当将原子能机构各种相关出版物（例如参考文献[8－10]）所列的和过去分析中涉及的危害纳入清单。附件 I 提供了一份潜在内部和外部危害的通用清单示例；
(2) 在一个可使全面的核实成为可能的结构化框架内识别场址和电厂的特有内部和外部危害。

[19] 根据参考文献[8]，极端气象条件包括极端温度、极端大气湿度、极端降雪（或暴雪）及浮冰、雷暴。其他的一些危害可与之相关，例如冰凌、霜冻和冰雹。

6.10. 对于已有的电厂，识别内部和外部危害过程的一个必需组成部分是场址调查和电厂巡视。

6.11. 应当列出潜在的危害组合清单。危害组合对电厂安全所造成的影响显著高于单一危害各自作用所造成影响的总和，且危害组合发生的频率可与单一危害发生的频率相当，例如，由于暴风雨引起的高水位与和由于暴风雨导致的大坝溃坝。识别危害的过程应当包括所有可能对风险重要的危害组合的识别。

6.12. 应当基于单一内部和外部危害的清单，识别可能的危害组合。在进行任何筛选分析之前，应当将整个潜在危害的清单用于此目的。通常，危害组合只涉及自然灾害（例如强风和高海水水位的组合）。然而，自然灾害和人因引发危害组合也是可能的，而且不能仅凭经验地排除（例如，严酷气候条件下增加船舶事故的风险）。

6.13. 用于识别一组实际危害组合的一般方法应当基于对所有内部和外部危害间关联性的系统检查。应当考虑以下可能出现危害组合的原因：

(a) 危害有在相同的条件下和同一时间（如强风和降雪）发生的可能；
(b) 一种外部危害可能会引发其他危害（例如地震引起的外部洪水并伴以溃坝）；
(c) 外部危害可能引起内部危害（例如地震引起的内部火灾或水淹）；
(d) 一种内部危害可能导致其他内部危害（例如内部飞射物引起的内部水淹）。

应当再评定危害组合对安全功能的影响，因它们可能以比单一危害更严重的方式影响不同的安全功能或同一安全功能。[20]

[20] 以下为潜在外部危害组合的示例：
(a) 干旱（由于高温）和强风及森林火灾引起的烟雾；
(b) 强风与闪电；
(c) 高气温及高水温；
(d) 降雪与强风；
(e) 飘雪与强风；
(f) 飘雪与强风和冰凌。

危害筛选

6.14. 通常应当建立连续的筛选过程，以尽量减少对风险重要性低的内部和外部危害的关注，并将重点放在对风险重要的危害分析上。连续的筛选过程应当始终如一地实施，同时建立筛选标准时应当确保不会遗漏任何对风险有重大贡献的与电厂和场址相关的内部和外部危害。应当在一级概率安全评定文档中给出筛选过程的结果。

6.15. 通常采用下列筛选标准，其可单独使用或组合使用：

(a) 基于定性论证，危害不会导致始发事件。对于外部危害，标准通常适用于当危害不可能发生在离电厂足够近的位置从而不会造成影响时。是否满足该标准也取决于危害的量级；

(b) 危害将缓慢发展，可以证明有足够的时间消除威胁的来源或进行充分响应；

(c) 危害已包含在另一危害的定义中；

(d) 与具有类似不确定性的其他危害相比，该危害的平均发生频率明显较低，且不会导致比其他此类危害更严重的后果。以这种方式被筛选掉的某种危害的频率估计中的不确定性被认为对总体风险没有显著影响。

6.16. 危害筛选的定量标准应当取决于一级概率安全评定的总体目标，并应当与内部始发事件以及内部和外部危害导致的堆芯损坏频率相关联。基于二级概率安全评定的目的，应当考虑其频率很低但可能造成放射性物质排放的严重后果的危害。

6.17. 第 6.15 段所列的标准均不适用于源自厂房内部的危害。这些危害应当不作为一个整体危害类别被筛选掉，而应当始终作为边界或详细分析的内容。

6.18. 应当确定与内部和外部危害的潜在损坏相关的最重要参数。若某一危害的潜在损坏不限于考虑单一参数，则应当确定多个参数。在进行筛选分析时，应当考虑到为危害所确定的所有参数（例如水位和流动压力）。

6.19. 下列外部危害应当不作为整体危害类别被筛选掉：

(a) 地震危害；

(b) 人因引发的危害；

(c) 风危害。

6.20. 为了排除强风类的特定危害，应当证明电厂所处位置的气候条件支持这些危害不足以对电厂造成损坏的假设（例如非沿海地区的飓风）。只有在证明超过某一特定风速的频率是可以忽略的情况下，才可筛选掉具有特定潜在破坏的风类危害。应当考虑风与其他危害组合，如降雨或洪水。在进行筛选时，有必要在分析中包括被风卷起的物体（主要是在龙卷风和飓风的情况下）变成飞射物的可能性。

6.21. 在外部洪水灾害的筛选过程中，应当考虑下列因素：

(a) 电厂位置相对于河流、海洋或湖泊的距离，以及任何洪水侵入场址的可能性；

(b) 预警时间 [21]：

(i) 对于位于河边的电厂，预警时间内足以实现停堆（例如提前一天以上）；

(ii) 对于沿海地区的电厂，一般来说预警时间较短，在当地发生海啸时，预警时间可能只有几小时或几分钟；

(iii) 除了预警时间之外，还应当考虑是否成功地收到警告以及是否成功地采取了可能的预防措施。

(c) 现有蓄水设施的构筑物类型；

(d) 当洪水发生时，其他邻近地区有可能被水淹，洪水水位可能会高于预期。位于狭窄洪泛区边缘的电厂比位于广阔三角洲地区的电厂更容易被水淹。

6.22. 对于发生于厂房外的每一种内部危害以及外部危害，在始发事件之后的各种消极假设都发生的情况下，应当确定其可能导致的近似最大影响，并用于筛选的过程。

6.23. 当筛选标准不适用于某类危害的整体，但适用于一定量级的危害时，该类危害的整体应当分成若干子类，然后将筛选标准应用于每一个子类，以避免筛选掉频率低但潜在损坏严重的危害。

---

[21] 预警时间是指洪水从主要源头（河流、上游盆地、堤坝等）到达场区的时间，因此也直接与预报的准确性相关。

6.24. 在电厂发生的始发事件可能是单一危害或两个及以上危害组合作用的结果。在使用筛选标准时，应当证明其综合影响可能导致重大后果的危害未被排除在进一步考虑之外，即使其中的每个危害单独考虑时对风险的贡献均可以忽略不计。[22]

6.25. 在应用筛选标准时，应对电厂和周围环境的实际状况进行评审，以验证原始设计条件的变化不重要或在概率安全评定中已将其考虑在内。特别是对于可能造成新的危害或导致某种量级危害的频率增加的变化应当予以仔细核实。[23]

7. 内部危害一级概率安全评定详述

概述

7.1. 本部分针对如何满足参考文献[3]要求 6－13（关于内部危害的一级概率安全评定）提供建议。针对电厂的下列内部危害（本“安全导则”未明确包括其他内部危害，但可采用类似的方法予以处理）的一级概率安全评定，提供了特定建议：

(a) 内部火灾；
(b) 内部水淹；
(c) 重物坠落；
(d) 汽轮机的飞射物；
(e) 内部爆炸。

---

[22] 此种危害组合的示例如强风及外部洪水。即使每一危害都可被筛选掉，但危害组合可能对电厂风险造成大得多的影响，例如当外部洪水伴以甚至是由强风所引发时。

[23] 举例说明此类变化如下：

(a) 场址 30 公里半径范围内的军事和工业设施的变化或附近运输线路的变化（即铁路、航空线路、公路、河流等），这些变化将导致人为所致外部危害的范围和量级的变化；
(b) 场址上游所建河坝的变化，其将导致外部洪水危害的潜在损坏的增加；
(c) 环境条件的变化（年平均风速及年最大风速、水位、温度、当地的降雨量等），其将增大外部自然灾害的发生频率及潜在损坏。

对一级概率安全评定内部危害的边界评定和详细分析

7.2. 电厂厂房内发生的危害应当在边界评定和/或详细分析的框架内加以考虑；保守的筛选分析通常被忽略（许多研究已表明，这些内部危害通常是总风险的重要贡献者）。对内部危害的一级概率安全评定，应当采用一致的方法进行边界评定和详细分析。它通常包括以下任务：

(a) 在可行的情况下，通过电厂巡视来收集场址和电厂的信息；

(b) 危害表征：危害识别、危害频率计算和危害影响分析；

(c) 内部危害的一级概率安全评定与内部始发事件的一级概率安全评定的整合：

  (i) 确认由内部危害引发的始发事件；

  (ii) 识别对内部始发事件的现有事件树和一级概率安全评定的故障树需要进行的修订；

  (iii) 分析特定的关联性和共因故障；

  (iv) 特定数据分析；

  (v) 对特定的人员可靠性方面的分析。

(d) 定性和/或定量筛选；

(e) 量化内部危害对堆芯损坏频率的贡献（结果分析、敏感性研究、不确定性和重要度分析）；

(f) 形成文档（特别注意考虑分析中所做的假设和使用的参考文献，包括质量保证）。

7.3. 一些内部危害（内部爆炸、火灾、水淹等）可发生在电厂的各个不同地点（房间、厂房或现场其他地方）。此种情况下，危害表征时应当明确：

(a) 首先，建立一个全局的电厂分析边界，以将所有对危害风险有贡献的地点均考虑在内；

(b) 其次，电厂封闭区域，假设电厂设计中现有的防护设施（实物分隔、隔离屏障、隔离设备等）将有效地把损坏控制在该区域内。

7.4. 在经过筛选过程后留下的内部危害对堆芯损坏频率的贡献，应当使用针对这些危害的一级概率安全评定来确定。内部危害的一级概率安全评定应当基于为内部始发事件开发的电厂响应模式，包括满功率、低功率和

停堆状态。内部始发事件的一级概率安全评定是开发内部危害一级概率安全评定的先决条件。除了在开展内部始发事件一级概率安全评定时发现的那些始发事件外，危害分析的结果可能会进一步产生新的始发事件（例如，火灾时在主控制室丧失所有信息）。此种情况下，应当开发新的事故序列并将其集成到一级概率安全评定中。

7.5. 为了对特定内部危害产生的风险进行定量简化评定或对如第 7.3 段指出的电厂封闭区域进行筛选，在没有内部危害一级概率安全评定详细模式的情况下，可以估计堆芯损坏频率。在这种情况下，计算特定内部危害对堆芯损坏频率的累积贡献的一般公式为：

$$f_{\text{堆芯损坏危害}} = \Sigma f_{\text{场内危害 } i} \times \text{CCDP}_i$$

式中：

$f_{\text{堆芯损坏危害}}$ 指特定内部危害对堆芯损坏频率的贡献；

$f_{\text{场内危害 } i}$ 指电厂区域“i”的特定内部危害的发生频率；

CCDP_i 指针对电厂区域“i”的堆芯损坏工况概率，它采用内部始发事件一级概率安全评定进行估算，并根据内部危害在电厂区域“i”的影响采用保守假设进行修正。

7.6. 影响分析应当考虑由危害引起的部件故障对概率安全评定中包含的始发事件和相关缓解性安全功能的影响。应当进行基于物理研究（例如模拟火灾假想方案或水淹假想方案）的详细分析，以降低过度保守性，避免对危害所致风险的过高估计。

7.7. 可能导致损坏扩散到其他地区的防护设施，如屏障或实物分隔等的潜在故障，应当通过特定详细的危害分析来处理。

7.8. 应当通过图纸或数据库获得基本的场址和电厂信息。对于在运电厂，这些信息应当通过电厂巡视来核实和完善。

7.9. 由于电厂巡视所得的信息可能是内部危害一级概率安全评定的重要输入，应对电厂巡视进行良好的计划、组织和完整详尽的记录。

7.10. 电厂巡视应当优先在内部危害一级概率安全评定开发过程的开始时进行，但是部分任务（例如对选定危害进行的详细分析）可能需要专门的电厂巡视。

7.11. 由危害引发的安全相关部件故障与一级概率安全评定模式中独立故障的概率组合将产生危害所致堆芯损坏频率。

内部火灾分析

概述

7.12. 内部火灾的一级概率安全评定是对核电厂现场发生的火灾事件及其对安全的潜在影响的概率分析。使用概率模式，内部火灾的一级概率安全评定应当考虑以下内容：

(a) 在电厂的任何地方发生火灾的可能性；

(b) 火灾可能向其他地方的蔓延；

(c) 火灾探测、灭火和禁火；

(d) 由于消防系统的启动而导致设备损坏的可能性（例如，消防系统所导致的喷淋和水淹可能会对本可经历火灾仍可用的设备造成损坏，或可能会改变设备的故障模式）；

(e) 火灾对设备（部件及其相关的仪器仪表、控制和电缆）的影响。所考虑的影响应当包括由“热短路”引起的设备虚假启动导致的新故障模式；

(f) 对这些设备造成损坏的可能性，以及在发生严重火灾时对电厂结构（墙壁、天花板、支柱、屋梁等）的完整性造成损坏的可能性；

(g) 设备随机故障和人因故障的影响；

(h) 火灾对运行人员行动的影响，包括直接的（如疏散控制室的需要）和间接的（如由虚假指示引起的混乱信息）影响。

7.13. 安全相关设备冗余通道之间的实物分隔（防火屏障）可以限制火灾损坏的程度。因此，用内部火灾一级概率安全评定模式来量化火灾对堆芯损坏频率的贡献时，通常应当包括不受火灾影响设备的随机故障概率以及试验或维护大修的可能性。

7.14. 在内部火灾一级概率安全评定中，应当特别考虑烟雾的如下影响：

(a) 烟雾可导致电子设备故障；

(b) 由于火灾事件所造成的异常环境条件（烟雾，可能是有毒的，也可能是刺激性的和高温），人因故障的概率可能更高；

(c) 烟雾的存在可能导致需要疏散主控制室。

7.15. 对于低功率和停堆模式下的内部火灾的一级概率安全评定，需要考虑以下特定方面：

(a) 如第 9 部分中介绍的在低功率和停堆模式下，内部始发事件一级概率安全评定方法的特定项；
(b) 为考虑较高的火灾负载和较多的潜在火源数量，特别是与在低功率和停堆模式下进行的维护操作相关的瞬态可燃物，筛选应当单独进行；
(c) 消防设施可用；
(d) 火灾传播可能的其他路径（例如，在低功率和停堆模式下部分门可能打开）。
(e) 在大修期间电厂不同地点的占用率增加可以改善火灾探测能力；
(f) 与火灾相关的电厂运行和配置改变，实施这些改变是为了控制可燃物以及为系统或部件停运提供补偿措施。

7.16. 在电厂设计过程中（见参考文献[9]）和运行期间（见参考文献[11]）进行的确定性火灾危害分析，应用以为内部火灾一级概率安全评定提供重要输入，例如，部件和电缆及其位置的清单，考虑到为设计防火设施而进行的功能和详细火灾影响分析的基础上将电厂分区为防火隔间。

7.17. 内部火灾一级概率安全评定方法应当基于对电厂边界内所有地点的系统分析。为便于检查，电厂应当细分为不同的实物单元（“防火隔间”[24]），然后对其分别进行详细检查。在设计中进行的电厂分区可以作为划分该物理区域的初始点。用于确定防火隔间的标准应当是正当的并记录在案。分析人员在定义用于一级概率安全评定的防火隔间时允许做一定的灵活变通。例如，若有利于筛选分析，分析人员可能更愿意将多个防火隔间视为一个防火隔间。至少在概率安全评定分析的早期阶段，可能不需要将电厂划分为大量的小块地点。

[24] 参考文献[9]，防火隔间被定义为建筑物或建筑物的一部分，其完全被防火屏障包围，即所有墙、地板和天花板。与此相反，在用于内部火灾概率安全评定的背景下，防火隔间可以是一个不一定被防火屏障包围的全封闭间。

7.18. 内部火灾一级概率安全评定的开发过程通常包括图 3 所示和第 7.19－7.65 段指出的任务。为本“安全导则”之目的，根据一个隔间内的点火源和火灾损坏程度来定义火灾假想方案。根据内部火灾一级概率安全评定分析的详细程度，与特定火灾假想方案相关的频率取决于起火频率和灭火概率。

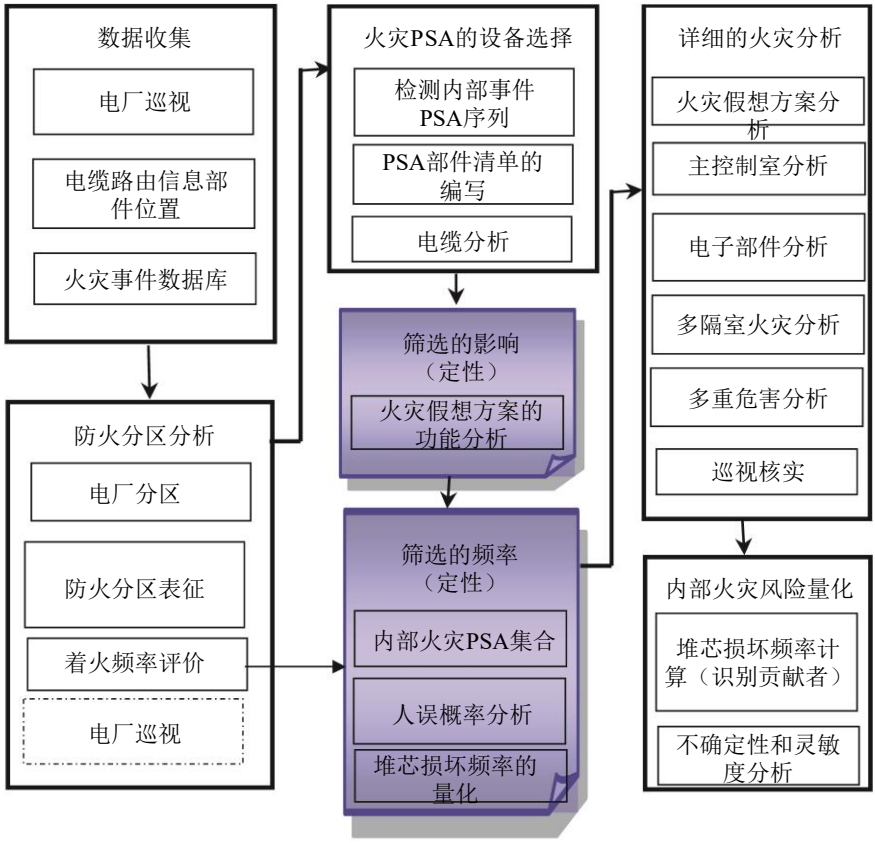

图 3. 内部火灾一级概率安全评定的开发过程。

数据收集

7.19. 内部火灾一级概率安全评定的数据收集和评定任务旨在准备必要数据。该项任务重点应当收集为建立火灾风险模式所需的电厂特定数据。然而，为考虑火灾所引发的工况，须对内部始发事件一级概率安全评定使用的部分数据进行再评定。

7.20. 内部火灾一级概率安全评定的电厂特定数据应当包括：

(a) 电厂电缆布线，包括电缆管道、导管、托盘和护栏；
(b) 防火隔间的物理特征及其存物清单（见第 7.22 段）；
(c) 火灾事件数据；
(d) 相关其可能成为点火源的部件特定信息（即可能引起火灾和瞬时可燃物的部件故障）；
(e) 火灾探测及灭火手段的可靠性估计；
(f) 火灾情况下的人员行动及人因故障概率；
(g) 是否有消防队可用及其能力；
(h) 消防系统的特点（系统行动的定时、可能造成设备损坏或妨碍运行人员进入消防隔间的灭火剂）；
(i) 由火灾和火灾损坏标准所引起的设备故障模式。

7.21. 考虑到为内部火灾一级概率安全评定所收集和保留信息的数量和性质，应当研究开发一个数据库作为支持工具。

防火隔间分析

7.22. 为内部火灾概率安全评定之目的，分析中所包括的所有厂房和构筑物都应当划分成不同的防火隔间，并单独进行研究（见第 7.17 段）。防火隔间的表征至少应当包括：

(a) 其实物边界（墙、门、阻尼器、贯穿件等）；
(b) 防火设施；
(c) 围绕隔间的防火屏障的阻燃性（防火等级）；
(d) 位于防火隔间内的部件和电缆；
(e) 邻近的防火隔间及与其的连接；
(f) 可将所分析的防火隔间与非毗邻的防火隔间连接起来的通风通道（管道）；
(g) 火灾负载（例如种类、数量、受保护或不受保护、地点、局部分布及其属永久的或暂时的）；
(h) 潜在点火源（例如：类型、数量、位置）；
(i) 可燃材料控制程序；

(j) 占用水平（即人员发现火灾的可能性）；

(k) 该地点的可达性（例如对消防队）。

7.23. 无论为了收集数据还是确定消防隔间的技术条件，在电厂巡视期间，应当在尽可能程度上对整个电厂的每个防火隔间进行目视视察，以对从电厂文件中获得的信息进行核实。核实应当旨在确保数据能代表电厂的当前实际状况。

7.24. 估计防火隔间的起火频率是内部火灾一级概率安全评定的一个重要组成部分，其应当在对所有防火隔间进行筛选前实施，或在对经过定性筛选后的最重要的防火隔间进行定量筛选之初进行（见第 7.41 段）。与点火源相关的起火频率应当采用第 5 部分中的建议进行评价，并尽可能使用电厂的自身数据。当电厂的自身数据不足时，应当采用通用数据和可用的电厂自身数据一起来估计起火频率，同时还应当针对实际起火源（包括动火作业所致的火源）和防火隔间内的永久性和临时性可燃物数量进行调整。

内部火灾一级概率安全评定设备的选择

7.25. 在对内部始发事件一级概率安全评定中涉及的电厂部件进行评审的基础上，应当建立需在内部火灾一级概率安全评定中建模的设备清单。清单中应当包括那些设备，其因火灾所致故障将：

(a) 可能导致始发事件；

(b) 可能影响安全功能缓解始发事件的能力（前沿系统和支持系统）；

(c) 可能影响由火灾导致的始发事件发生后运行人员的行动（C 类人员互动）；

(d) 在功率运行期间和停堆期间，可能导致对电厂产生其他不安全影响的功能的虚假启动。

诸如此类的故障可能是由于动力或控制电源故障，或由于热短路导致的误操作或电厂监控仪器仪表和警报的错误输出导致。对设备虚假启动的分析深度应当适应概率安全评定的范围，并应当侧重于在一级概率安全评定中尚未纳入考虑的设备或故障模式。

7.26. 应当识别出对内部火灾一级概率安全评定重要模式中的电厂部件和所有相关要素。应当系统地重新校验内部始发事件概率安全评定模式中对

部件故障模式做筛选或纳入的基础，以确定在火灾引发故障的背景下所做假设的有效性，并在必要时对内部始发事件模式进行扩展。

7.27. 本检验包括识别所有与第 7.25 段和第 7.26 段所规定的部件相关的电缆和电路以及分析电缆布线。此外，应当考虑由非电气线路如仪器仪表空气控制线路可能因火灾造成的损坏。

7.28. 应当拟订每个防火隔间的一级概率安全评定相关设备清单。在详细分析的稍后阶段，需更精确地确定防火隔间内部件的位置。

通过影响进行筛选

7.29. 在定性（‘以影响为导向’）标准的基础上，应当采用通过影响进行的筛选来消除非重要的火灾假想方案。筛选从确定关键的防火隔间和区域开始，再使用保守假设确定可能的单一和多隔间火灾假想方案。用于筛选特定火灾假想方案的以影响为导向的标准应当考虑到假想方案所涉及那些防火隔间的特征。

7.30. 若通过影响进行筛选，则至少应当基于以下标准或其组合。基于对电厂安全可以忽略的潜在影响，某个防火隔间可被筛选掉，如果：

(a) 火灾负载密度低于规定的可接受阈值；或

(b) 所有下列条件均成立：

(i) 隔间内没有可导致始发事件或需要手动停堆的设备；和

(ii) 无论是与安全相关的系统（即电厂安全停堆所必需的系统），还是它们的电缆或支持系统都不在隔间内；和

(iii) 将火灾影响扩散到其他装有安全相关设备防火隔间的可能性非常低。

7.31. 为筛选之目的，所有暴露在火灾下的部件和电缆都应当假想故障，即保守假设通常是火灾探测和灭火设施无效或不可用。通常不考虑其他防护措施，如防火护盾、防火涂层或防火密封。

7.32. 通过冲击进行筛选还应当包括在对火灾蔓延的保守假设下开发的多隔间火灾假想方案。对于每一个防火隔间，通过在每个隔间中添加所有相邻的隔间（各个方向），并添加虽与其不一定相邻但共享通风的所有相连隔间，来定义火灾可能传播的隔间组合。然后，应当针对火灾可能蔓延至相

邻（或相连）防火隔间的可能，对所有可能的防火隔间组合进行分析。为了限制需要考虑的组合数，可针对防火屏障组成要素的可靠性和有效性（例如，可认为各防火屏障极不可能同时发生独立故障）作出通用假设。

7.33. 分析时应当考虑到火灾从厂房外蔓延至厂房内的防火隔间的可能性（例如，火灾可能从变压器区域蔓延至汽轮机大厅）。

7.34. 对于多机组场址，在分析时应当考虑到火灾从一个机组蔓延到另一个机组防火隔间的可能性。此外，还应当考虑在公共区域（如摆动式柴油机（即机组间共用柴油机）、开关站）发生火灾的可能性。

通过对堆芯损坏频率的贡献进行筛选

内部火灾与内部始发事件一级概率安全评定的整合

7.35. 应当在定量标准的基础上，根据其对堆芯损坏频率的贡献进行防火隔间筛选，旨在对通过影响进行的定性筛选后保留下的防火隔间或多重防火隔间的联合体做进一步消除。

7.36. 在此步骤中，应当使用基于现有的内部始发事件一级概率安全评定开发的概率模式计算火灾对堆芯损坏频率的贡献。此类模式通常用于计算特定火灾假想方案工况下堆芯损坏工况概率。在此阶段，为评价火灾假想方案的发生频率及其需求安全功能由于火灾所致的相关条件不可用度，应对火灾的生长和蔓延以及火灾对设备和相关人员行动的影响（即降低火灾影响的行动）做保守假设：在自身消防隔间内的所有设备均悲观认为不可用，探测和灭火手段也不可信。

7.37. 在前述假设条件下，对于每一防火隔间，应当修改内部始发事件一级概率安全评定模式，以映射隔间内火灾影响、相关始发事件和设备故障模式。这样，可计算每个防火隔间室对堆芯损坏工况概率，从而使用第 7.5 段所给的公式可计算出火灾对堆芯损坏频率的总贡献。

人误概率分析

7.38. 在确定火灾导致堆芯损坏频率或计算堆芯损坏工况概率时，应当考虑到与应急运行程序和火灾缓解的特定程序的偏差，对内部始发事件一级概率安全评定模式中的人误概率进行评审。对于与内部始发事件一级概率

安全评定所用的如第 5 部分所述人的可靠性分析方法的任何偏差，都应当予以说明和记录。

7.39. 在将第 5 部分中所述的方法应用于人的可靠性分析时，应当考虑附加应力、可能存在矛盾信号、烟雾、丧失照明和进入或通过受影响区域的困难等特定火灾影响，来分析行为形成因子。

7.40. 若在内部始发事件一级概率安全评定模式中考虑人员修复行动，则应当检查执行修复行动的可行性。例如，可能难于在遭受火灾的房间实施特定的修复行动。还应当核实火灾可能对控制室的空气质量和人因故障概率产生的次生效应。

火灾对堆芯损坏频率贡献的量化筛选

7.41. 定量筛选时，应当根据第 7.5 段所给的一般公式，考虑到火灾假想方案的相应频率，对每个防火隔间的火灾对堆芯损坏频率的贡献进行评定。

7.42. 定量筛选应当基于堆芯损坏工况概率的保守估计或火灾对堆芯损坏频率的绝对贡献。可定义防火隔间定量筛选的以下两项标准：

(1) 所有被筛选掉的防火隔间的火灾对堆芯损坏频率的累积贡献应当在规定的阈值值之下。该阈值可以定义为一个特定的绝对值，或者以相对的术语给出（例如，内部始发事件对堆芯损坏频率的贡献）；

(2) 为允许做一定的筛选，应对单一防火隔间设定足够高的标准值；但为了保留所有风险重要的火灾假想方案，标准值应当足够低。

7.43. 根据火灾对堆芯损坏频率的贡献进行筛选时，对多个防火隔间的损坏频率被认为是在一个防火隔间的起火频率与火灾蔓延至其他防火隔间的条件概率之乘积。

7.44. 整个筛选过程（根据影响和频率）的结果将是一份与防火隔间相关联的火灾假想方案清单，其可能是风险的重要贡献者，需要做进一步考虑。对于此清单中的每一火灾假想方案，应当开发定量化的内部火灾一级概率安全评定模式以进行进一步分析。

火灾详细分析

火灾假想方案分析

7.45. 详细的火灾分析旨在降低在筛选过程中所识别的火灾假想方案的保守程度。应当考虑防火隔间内防火屏障及其他防火措施的影响、防火隔间内与安全和消防相关设备的位置以火灾的生长和蔓延等方面。应当考虑并评定火灾的所有影响，包括火焰、羽流、天花板射流、来自热气体热辐射，高能量电弧和烟雾。通常在开展内部火灾一级概率安全评定时应当进行专门的电厂巡视，为详细分析的核实收集支持性信息。

7.46. 应当采用更现实的模式来评定为降低设备损坏概率、阻止火灾的生长和蔓延及降低火灾对设备和电缆的影响等所采取的人员行动。

7.47. 应当评定火灾、烟雾和有毒气体的可能蔓延对人员行为的影响。还应当注意，火灾导致的超压可能导致进入恢复位置所需的门无法打开。

7.48. 对用于分析火灾生长和蔓延（例如火灾模拟计算机程序）所选择的特定建模工具的正当性应当予以说明，并记录在案。

7.49. 火灾假想方案应当描述在选定隔间始发火灾的时间相关过程以及任何后续的部件和电缆故障。火灾假想方案应当在内部火灾一级概率安全评定模式中予以表征，例如，通过火灾蔓延事件树（见附件 II 的示例），其对影响火灾发展的所有重要特点（防火屏障的设计和质量、火灾生长和蔓延模式，以及包括电缆、防火和灭火设施在内的遭受风险设备的损坏标准）进行建模。建立火灾蔓延事件树应当采用第 5 部分的相关建议。

7.50. 分析火灾假想方案时，应当使用与第 5 部分中所给的内部始发事件概率安全评定使用的相同方法来评定手动操作的人员可靠性及探测和消防系统的部件可靠性。

7.51. 火灾假想方案应当考虑可能与火灾传播相关的路径（例如通风或电缆槽，失效的防火屏障）。

7.52. 对于详细火灾分析中所考虑的防火隔间，应当补充完善相关火灾假想方案发生频率的数据，包括防火隔间特有的其他数据，如非永久性点火源、可燃性、可能存在的火灾负载等。

7.53. 对于特定火灾假想方案，应当确证火灾自动、手动探测和灭火能力的规定有效性和响应时间，以及规定的灭火失败概率。

主控制室火灾分析

7.54. 主控制室的内部火灾一级概率安全评定应当考虑与该位置相关的特定特征，如主控制室火灾对所有安全系统的大面积传播效应、可能的系统误动和主控制室火灾对运行人员行动的影响。后者应当包括以下方面：

(a) 火灾和烟雾对仪器仪表和相关设备可用性的影响；
(b) 火警探测和灭火设施的能力，包括洪水的潜在不利影响；
(c) 考虑到可达性和其他可能的限制方面，为安全停堆使用替代地点；
(d) 烟雾和有毒气体扩散的影响。

此外，还应当考虑机柜内火灾传播，包括存在的实物屏障以及冗余部件的空间分隔。

电气部件室火灾分析

7.55. 电气部件室、开关室、电缆室和其他包含控制设备的厂房往往自然成为设备和布线的聚合中心。它们所包含的电气设备和电缆可能属于多个安全系统通道。因此，火灾对安全停堆冗余设备和其他一级概率安全评定相关设备的潜在影响可能大于电厂其他位置火灾的影响，应当予以考虑。

7.56. 火灾发生在前述厂房导致电气短路时，单一或多个电气部件产生误动的概率较高。在分析电气部件误动时，应当识别特定的火灾所致电路故障并评定相关的条件概率。

多隔间火灾分析

7.57. 多隔间火灾分析旨在识别涉及多个防火隔间对风险重要的潜在火灾假想方案。应当假设火灾可能通过共用屏障或连接隔间的通风管道从一个隔间蔓延到另一个隔间。与筛选过程中所做的分析相比，多隔间火灾详细分析应当基于火灾成长模式、火灾蔓延分析模式和灭火模式。

7.58. 与单一防火隔间相比，对多隔间火灾的详细分析应当考虑火灾的传播深度、燃烧产物的扩散和/或热量向相邻（或相连）防火隔间的传递。

多重危害分析

7.59. 应当识别发生其他重要内部危害的可能性（如由于消防系统启动而排出大量水所引起的水淹、火灾引起的危害物质爆炸、爆炸引起的火灾），并在内部火灾一级概率安全评定中予以考虑。

7.60. 若未被纳入外部危害（如地震、闪电、外部火灾、飞机坠毁等）一级概率安全评定则应对其他危害导致内部火灾定性分析中予以特殊考虑，包括：其他危害和火灾对安全产生重要的联合影响的防火隔间、危害所致的点火源、消防系统的误动或效率退化、手动执行灭火行动的困难性等，（见第 8 部分所述的外部危害一级概率安全评定建议）。

7.61. 至少应当考虑其他危害引起的内部火灾对运行人员行为形成因子的以下影响：

(a) 发生火灾后，被关注防火隔间的可达性；
(b) 压力增加的程度；
(c) 指示故障或错误指示；
(d) 火灾对运行人员行为的其他影响。

内部火灾风险的量化

7.62. 完整的一级概率安全评定模式应当包括为内部火灾一级概率安全评定详细分析而开发的特定模式（例如主控制室火灾模式或用以评定火灾导致单一或多个部件误动的影响模式）。

7.63. 考虑到详细分析的结果，对筛选后剩余的防火隔间，应对内部火灾对堆芯损坏频率的贡献进行最终定量化。内部火灾一级概率安全评定应当包括用于根据频率定量筛选掉防火隔间的结果和模式。内部火灾的一级概率安全评定结果应当通过识别堆芯损坏频率的主要贡献者来解释（例如：防火隔间、火灾假想方案、人员行动）。在此最后阶段，应当评审筛选相关的假设，以考虑是否需要在详细模式中增加已被筛选掉的堆芯损坏频率的贡献者。

7.64. 内部火灾一级概率安全评定模式的量化、不确定性分析和敏感性分析应当遵循第 5 部分提出的建议。应当开展不确定性分析以识别不确定性的来源并对其进行评价。应当进行敏感性研究和重要度分析，以识别内部

火灾一级概率安全评定中对风险有重大影响的因素。对于重要的假设应当进行敏感性分析。应当确定对计算结果的各贡献者的相对重要度。

内部火灾的一级概率安全评定文档

7.65. 本段针对如何满足关于内部火灾一级概率安全评定文档的要求 20[3]提出了建议。内部火灾一级概率安全评定文档应当以便于评审、应用和更新。文档应当特别包括下列信息：

(a) 描述核电厂的特定防火设施，包括核电厂的非能动和能动缓解设施，以及核电厂防火隔间的划分；

(b) 描述用于评定火灾危害的特定方法和数据；

(c) 为考虑内部火灾的影响而对内部始发事件一级概率安全评定模式所做的修改；

(d) 防火隔间的表征；

(e) 分析中筛选特定防火隔间的正当性；

(f) 对详细的火灾假想方案、主控制室、电气部件室、多隔间火灾、多重危害等的特定分析结果；

(g) 根据堆芯损坏频率以及选定的中间结果，内部火灾一级概率安全评定的最终结果；

(h) 支持火灾分析的电厂巡视报告。

内部水淹分析

概述

7.66. 内部水淹一级概率安全评定是对发生在电厂厂房内的液体（通常为水）排放事件以及对安全的潜在影响进行的概率分析。内部水淹一级概率安全评定开发过程通常包括如图 4 所示并在第 7.67－7.92 段所述的任务。对于低功率和停堆模式的内部水淹一级概率安全评定，应当考虑与第 7.15 段所列的相同方面。

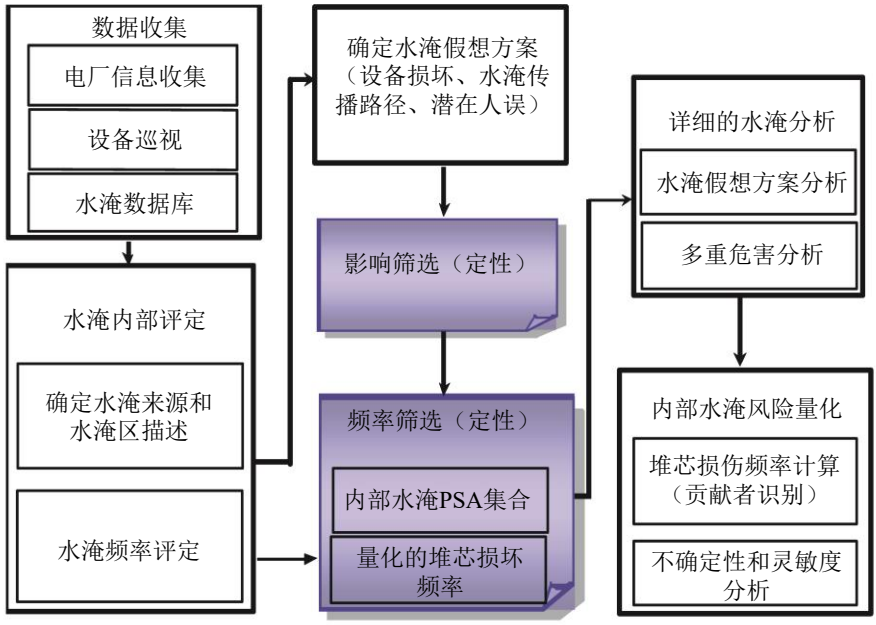

图 4. 内部水淹一级概率安全评定的开发过程

潜在内部水淹数据收集和评定

7.67. 对于在运核电厂，应当专门针对内部水淹评定开展电厂巡视，以核实从图纸和电厂其他信息来源所获得信息的准确性，并为分析每个潜在内部水淹来源的损坏影响获取相关空间上交互作用的必要信息。

7.68. 应当识别和描述可能发生的内部水淹事件和表征（关于核电厂设计中水淹的一般考虑见参考文献[10]）。在执行此项工作时，应当考虑到以下因素：

(a) 可能的水淹来源：管道、内部储罐、水池、阀门、热交换器、与开放源（如海、湖、河）的连接、多机组共享系统或结构等；

(b) 可能的水淹机制：喷淋系统（如安全壳喷淋系统或消防系统）的破裂、泄漏、断裂、错误或期望的启动，在运行或维护等相关活动中出现的人误（如阀门定位错误或误开）；

(c) 水淹特征：容量（取决于水淹的来源是封闭还是开放系统）、流速、温度和压力、存在或可能产生的蒸汽；

(d) 与水淹相关的警报、泄漏探测系统、排水系统容量和设备的水淹相关保护（如设备停堆信号）；

(e) 在水淹区域，与概率安全评定和房间尺寸相关的设备临界水淹高度。

7.69. 在识别潜在水淹事件时，应当特别考虑电厂停堆的情况，因为此种情况下，水通道经常被人工重构。

7.70. 应当识别可能受内部水淹影响的场区和水的可能扩散路径。识别时应当考虑到多机组的相关方面，并应当考虑到由于积水导致防水屏障故障的可能。

7.71. 电厂应当被划分为实物分隔的“水淹区”，这里，在内部水淹的潜在影响和水淹的可能扩散方面，一个水淹区通常被视为与其他区域相独立。

7.72. 应当按照第 5 部分的建议，对内部水淹事件的发生频率进行评价。在可行的情况下，应当使用电厂的自身数据。当电厂的自身数据不足时，可使用通用数据或有适当正当性的专家判断。

7.73. 评价内部水淹事件发生频率所使用的主要数据是管道故障概率和破裂频率以及相关的不确定性。应当针对代表内部水淹重要来源的管道系统选择数据。此外，应当在考虑到电厂自身的维护程序和经验的基础上，对由人因失误引起的水淹事件的频率和严重性进行评价。

水淹假想方案识别

7.74. 对于每个内部水淹事件，应当识别可能受到水淹影响的结构、系统和部件。根据分析范围的不同，水淹对设备的以下影响可能是相关的：由于高能量管道或阀门连接破裂导致的水淹、温度、压力、喷淋、蒸汽、管道甩动或喷射冲击。应当确保分析应尽可能完整。

7.75. 受内部水淹影响的部件时应当考虑到标高、屏障物、门和排水。应当考虑到排水堵塞的可能性。

7.76. 应当评定水淹从一个区域蔓延到另一个区域的可能性，包括考虑到屏障故障。

7.77. 所有可能的水淹蔓延路线都应当加以考虑，例如，部件排水和常闭门或舱口被打开。

7.78. 应当识别机柜、安全相关部件电缆接线盒及其他敏感设备的位置，包括标高。基于此，可识别部件是否易遭受特定厂房水淹的影响。

7.79. 应当评定水淹对电厂运行的潜在影响。分析水淹对电厂运行的潜在影响时，应当包括由于水淹影响造成的部件或系统的误动，这可能引发特定的事故序列。

通过影响进行筛选

7.80. 应当根据其影响对水淹假想方案进行筛选。基于对电厂安全的潜在影响是否可忽略，通过筛选掉电厂隔间来选择重要的水淹假想方案。基于以下定性标准，可将某一电厂隔间从分析中筛选掉，若：

(a) 以下两个条件均成立：
  (i) 该隔间不包含任何可导致始发事件的设备；和
  (ii) 电厂安全停堆所必需的系统及其支持系统均不位于水淹来源的隔间或水淹蔓延区域；或
(b) 该隔间不包含任何水淹来源，包括来自其他隔间的足以导致设备故障的漏入。

根据对堆芯损坏频率的贡献进行筛选

内部水淹与内部始发事件一级概率安全评定的整合

7.81. 应当根据其对堆芯损坏频率的贡献，对内部水淹事件做进一步筛选。因此，为考虑水淹现象应当修改内部始发事件一级概率安全评定（包括系统模式和运行人员行动）。

7.82. 应对内部始发事件一级概率安全评定中的人的可靠性分析进行全面评审。在将第 5 部分提出的方法用于人的可靠性分析时，应当分析行为形成因子，并考虑到水淹来源的特定情况。应当在考虑到缓解水淹的特定程序的基础上，对人因错误概率进行重新评定和调整。至少，应当考虑水淹对运行人员行为形成因素的以下影响：

(a) 在发生水淹及/或因水淹或有蒸汽或喷淋而导致的不利环境影响后，被关注隔间的可达性；
(b) 潜在的压力增加程度；

(c) 指示故障或错误指示；

(d) 水淹对运行人员行为的其他影响。

为筛选对水淹对堆芯损坏频率贡献的定量化

7.83. 应当采用保守方法进行定量筛选，即假设隔间内受水淹影响的所有部件都将发生故障。若该假设未对堆芯损坏频率造成实质性贡献（采用第7.5段所给的公式计算），则可将相应的内部水淹事件筛选掉。

7.84. 应当为内部水淹一级概率安全评定定义根据对堆芯损坏频率的贡献所进行筛选的定量标准，此类标准的示例可包括：

(a) 所有被筛选掉的水淹假想方案对堆芯损坏频率的累积贡献应当在规定的阈值以下；

(b) 单一水淹假想方案的筛选标准应当设定足够高的数值，以允许某些筛选；但其数值又应当足够低，以保留所有风险重要的水淹假想方案。

详细水淹分析

水淹假想方案分析

7.85. 定量、详细的水淹分析应当关注以下问题：

(a) 恢复时间的计算（水淹水位变化率）；

(b) 人的可靠性分析，为缓解水淹事件序列所需的人员额外行动；

(c) 为每个水淹假想方案开发事件树或故障树模式（基于内部始发事件一级概率安全评定（见第5部分或适当的新模式））；

(d) 对包含由于水淹所致设备故障的相应事件树或故障树进行量化，并对结果进行分析，包括敏感性研究和不确定性分析。

7.86. 应当根据其探测和控制手段，对所有潜在的有贡献的始发事件进行分析。在估计非探测和非隔离的概率时，应当考虑探测和控制手段。

7.87. 水淹假想方案应当描述源自选定场区水淹的时间相关过程以及随后的部件故障（详见第7.74段）。水淹假想方案可通过事件树表达，其中对所有影响水淹进展的重要特点（防水屏障设计、水淹探测和水淹来源隔离）和部件故障概率都进行建模。一般来说，在实施内部水淹一级概率安全评

定时应当开展专门的电厂巡视，旨在为核实详细的水淹分析收集支持性信息。

7.88. 应当识别为缓解水淹序列可能需要的人员额外行动，并就水淹探测和控制的成功或失败概率对其进行评定。这些额外行动包括诸如电源的隔离及后续的恢复。人的可靠性分析方法应当考虑可能由水淹引起的仪器仪表和控制设备的丧失及误指示。

多重危害分析

7.89. 关于因高能管道的破裂造成的水淹及对结构、系统或设备的损坏，若未作为内部始发事件一级概率安全评定模式的一部分被纳入，则应当在内部水淹一级概率安全评定中予以处理。

7.90. 由消防系统的启动排出的大量水所引发的水淹应当在内部火灾一级概率安全评定中予以处理（见第 7.59 段）。

内部水淹风险的量化

7.91. 在完整的一级概率安全评定模式中应当包括用于按频率定量筛选掉水淹假想方案的结果和模式及为内部水淹一级概率安全评定详细分析所开发的特定模式。其次，应对水淹对堆芯损坏频率的贡献进行最终量化，包括识别主要贡献者（如水淹来源、水淹假想方案）和评审与筛选、不确定性和敏感性分析相关的假设。本段所述量化应当遵循第 5 部分的建议。

内部水淹一级概率安全评定文档

7.92. 本段针对如何满足关于内部水淹一级概率安全评定文档的参考文献[3]要求 20 提供了建议。内部水淹一级概率安全评定文档应当以便于一级概率安全评定的评审、应用和更新。特别地，文档中应当包括下列信息：

(a) 描述用于评定内部水淹危害的特定方法和数据；
(b) 为考虑内部水淹的影响而对内部始发事件一级概率安全评定模式所作的特定修改；
(c) 从分析中筛选特定水淹假想方案的正当性；
(d) 水淹假想方案详细分析的结果，包括对假想方案的描述以及在分析中做出的重要假设；

(e) 内部水淹一级概率安全评定的最终结果，包括堆芯损坏频率、定性理解和建议等；

(f) 支持水淹分析的电厂巡视报告。

其他内部危害

重物坠落分析

7.93. 概率安全评定通常关注反应堆压力容器内或乏燃料水池贮存的堆芯冷却剂故障。但实际可能发生其他更直接的损坏，例如重物坠落至压力容器、乏燃料水池或执行关键安全功能所需的系统上。应当针对重物坠落对执行关键安全功能所需的结构、系统或部件的可能损坏或对燃料组件可能直接导致的机械损坏，分析可能的重物坠落（例如穹顶、反应堆压力容器盖、乏燃料桶和混凝土屏蔽块）。

7.94. 若重物的运输路径既不在燃料之上，也不在包含关键设备的区域之上，则可将相应的重物坠落风险源筛选掉。

7.95. 除装卸重物的反应堆换料平台外，概率分析还应当考虑位置。例如，部分电厂的汽轮机大厅的开放区域可能有余热排出系统，较容易受到重物坠落的影响（例如，试验设备或器具可能会坠落并破坏与容器相连的管道）。

7.96. 应当计算重物坠落对堆芯损坏频率的贡献，除非该事件可以在基于概率的基础上予以剔除。

7.97. 重物坠落一级概率安全评定应当与为低功率和停堆模式下内部始发事件一级概率安全评定开发的电厂响应模式相一致（见第 9.11 段）。

7.98. 应当考虑电厂内所有永久性起重设备。应当详细识别和检查重物坠落可能对安全相关部件产生不利影响的区域。为此目的，应当开展专门的电厂巡视。

7.99. 应当根据工作程序识别和分析停堆期间的起重操作。

7.100. 应当根据第 5 部分和第 9 部分的建议，计算始发事件的频率。计算时应当考虑机械设备故障、人误和自动保护功能的可能不可用。若在外部

危害一级概率安全评定中未予考虑，则应当在始发事件分析中处理诸如地震或飞机坠毁等外部现象。

7.101. 对于每一个重物坠落事件，都应当保守地假设最大重物坠落，或者，必要时应当分析坠落物的性质和坠落原因。应当阐明由重物坠落所产生的飞射物的可能方向、大小、形状和能量等表征，并评定其对厂房结构和电厂的影响。

7.102. 若预期将进行二级概率安全评定，则应当考虑每一重物坠落事件以确定其潜在的放射性后果和对某一电厂损坏状态频率的贡献（如有）。

汽轮机飞射物分析

7.103. 应当计算汽轮机解体（例如汽轮机转子的故障）对堆芯损坏频率的贡献，除非该事件可以在基于概率的基础上予以剔除。在分析汽轮机飞射物影响时，应当考虑氢气点火或油燃烧引起的火灾对概率安全评定相关部件的影响。

7.104. 汽轮机解体的分析应当包括正常转速值和超速值。

7.105. 应当确定汽轮机解体后飞射物的分布，并根据汽轮机所在方向和位置，计算飞射物撞击厂房的概率。

7.106. 应当考虑到有足够动能穿透厂房的飞射物比例，确定所致的厂房内与安全相关设备的故障概率。

7.107. 在第一阶段，应当只考虑原先在一级概率安全评定中已识别出的事故序列所涉及的设备。

7.108. 计算导致堆芯损坏状态或大排放的故障频率时，应当使用飞射物撞击导致的故障概率，以及幸存安全相关设备的随机故障概率和汽轮机解体频率。

7.109. 应当开展电厂巡视，以确认分析中针对汽轮机飞射物而对结构、厂房和选定的设备所采取保护的假设。

内部爆炸分析

7.110. 考虑到核电厂的基本设计旨在尽量减少内部爆炸的可能性和影响，应当为内部爆炸一级概率安全评定内部危害一级概率安全评定一般流程做适应性修改。应当将由内部火灾所引发的或引发内部火灾的内部爆炸纳入内部火灾一级概率安全评定中予以考虑和分析。

7.111. 核电厂厂房设计基本上考虑了爆炸的预防和缓解（见参考文献[9]）。为此目的，对爆炸进行系统分析，以确定潜在的爆炸来源（爆炸材料的性质和数量、位置）、爆燃或爆炸对电厂的潜在影响（超压、冲击或拉力负载、火灾或热量）和预防设施等方面的表征。内部爆炸一级概率安全评定应当主要基于此类分析过程中收集的信息和数据，以允许定性筛选掉爆炸假想方案。

7.112. 应当开展电厂巡视以识别潜在的爆炸来源并进行核实。

7.113. 对于残留的爆炸假想方案，应当使用第 5 部分的建议来估计爆炸事件的频率。量化时应当考虑电厂内爆炸物质的数量、可能在爆炸来源处的人员活动以及预防手段（氢气探测设备、爆炸性液体或气体的泄漏探测器、通风等）的有效性。

7.114. 应当计算内部爆炸对堆芯损坏频率的贡献，除非该事件可以在基于概率基础上予以剔除。

8. 外部危害一级概率安全评定详述

概述

8.1. 本部分提供了如何满足参考文献[3]关于外部危害一级概率安全评定之要求 6－13 的规定。仅对大多数情况下不能被筛选掉的所选外部危害给出特定建议：

(a) 地震危害；
(b) 强风；
(c) 外部洪水；
(d) 人因导致的危害。

外部危害边界分析的概述

8.2. 边界分析旨在减少需详细分析的外部危害清单，以聚焦最重要的事故假想方案。开展边界分析时应当保证，与其他危害源相比，与特定外部危害相关的堆芯损坏是微不足道的。

8.3. 在边界分析中，应当考虑每一个未筛选掉的外部危害对核电厂的全部潜在影响。[25]

8.4. 应当计算纳入边界分析的外部危害的累积贡献，并保留在一级概率安全评定的最终结果中。

8.5. 应当开发特定危害的一整套假想方案，除非该危害对电厂的所有影响可限于单一假想方案，但通常情况并非如此。

8.6. 在边界分析中，还应当考虑外部危害组合。

8.7. 边界评定应当基于现实的或经证明系保守的模式和数据。此类模式和数据应当包括：

(a) 危害频率的评定（即超过特定强度概率的估计）；
(b) 分析危害对电厂的影响（即与危害相关的负载）；
(c) 电厂响应（即缺陷）分析；
(d) 电厂的一级概率安全评定模式和数据等。

地震危害

8.8. 由于在许多一级概率安全评定中地震呈现为堆芯损坏频率的重要贡献者，因此应当进行详细分析。但为了限制地震危害一级概率安全评定所需工作量，可以对一定范围的地震危害进行边界分析。在此阶段，还应当考虑地震危害的次生影响（例如地震引起的火灾和水淹）。除本“安全导则”

[25] 影响类别的示例（见参考文献[12]）如下：
(a) 场外电源丧失或全厂断电；
(b) 最终热阱的退化或丧失；
(c) 危害物质的爆炸或排放；
(d) 电厂通风的退化或被隔离（由于有毒性影响的风险）。

外，参考文献[13]还提供了对现有核装置地震评价的详细建议，包括概率安全评定方面的考虑。

强风

8.9. 取决于场址位置，应当考虑几种强风类型并进行边界分析或详细分析：

(a) 与龙卷风相关的风和其他影响；
(b) 与热带气旋相关的风（气旋、飓风、台风）；
(c) 温带强风（雷暴、飑线、锋面等）。

应当考虑强风和其他危害现象的组合，并考虑可能的相关性（例如强风和高水位）。

外部洪水

8.10. 在一级概率安全评定中应当考虑下列与水灾相关的危害：

(a) 河流或湖泊高水位；
(b) 高潮汐；
(c) 风暴；
(d) 极端降雨；
(e) 海啸；
(f) 假潮；
(g) 滑坡引起的洪水；
(h) 人因引发的洪水（如大坝、堤、堤坝垮塌或决堤）。

应当考虑到外部洪水和其他危害现象的组合，并考虑可能的相关性（例如高水位、随之发生的大坝垮塌）。

8.11. 大雨和其他洪水的后果例如屋顶和电厂低洼区域的积水，应当纳入分析范围。

其他自然灾害

8.12. 在边界分析中应当考虑潜在自然灾害（地震危害、强风和外部洪水除外）的综合清单。应当将附件 I 所列的自然灾害清单和电厂安全分析报告

中所考虑的自然灾害清单作为识别危害的基础，若适当时还应当考虑场址特定的自然灾害。

8.13. 应当考虑自然灾害与其他危害现象的组合，并考虑到可能的相关性（例如恶劣的天气条件、强风）。

人因引发危害

8.14. 最低限度应当考虑下列人因引发危害的来源：

(a) 自附近电厂机组或设施蔓延而来的火灾；
(b) 来自附近设施或由于运输或管道事故造成的固态物质、气体云爆炸；
(b) 来自附近设施或由于运输或管道事故造成的化学物质排放；
(c) 飞机坠毁；
(d) 船舶与进水构筑物的碰撞；

下列也可视为人因引发危害的来源：

(f) 来自场址中的其他电厂的飞射物；
(g) 在场区内外进行的挖掘工作；
(h) 电磁干扰（如雷达、无线电或移动电话产生的磁场或电场）。

外部危害的参数化

概述

8.15. 应当定义外部危害导致潜在损坏相关的最重要参数。当危害的潜在损坏不能用单一参数来表征时，应当定义多个参数。

地震危害

8.16. 地震危害由以下几个参数来表征：

(a) 烈度，衡量影响和损坏的描述性指标；
(b) 地面运动，例如加速度、速度、位移；
(c) 频率组成，通常用反应谱表征；
(d) 地震事件的全时间历程，包括加速度、速度、位移等方面。

当在一级概率安全评定中以简化方式使用单一参数来表征地震的潜在破坏（例如地面运动加速度峰值）时，还应当考虑以下其他参数以评定地震危害的特定影响：

(a) 概率组成对于考虑继电器颤振、确定结构和部件的响应和缺陷以及人因故障的应力因素均至关重要；

(b) 当地地质是针对土壤液化、沉降、边坡失稳、塌陷、地表断裂或压裂等次生影响应当考虑的重要因素。

8.17. 当有数据支持其估计时，应当使用选定频带上的谱加速度或平均谱加速度。[26]

8.18. 地震引起的地表振动应当不排除在考虑范围之外（即地震波可以到达地球表面的任何点）。

8.19. 地震地面运动应当不被筛选掉。

强风

8.20. 根据风力类型，应当考虑不同的参数：

(a) 阵风的动负载和在指定时间内（例如 10 分钟）的平均风负载，是表征连续移动风的基本参数；

(b) 龙卷风的旋转速度、压差和路径面积以及龙卷风携带飞射物的潜在影响（即大小和速度）是表征龙卷风等的基本参数。

外部洪水

8.21. 外部洪水的潜在危害可以通过排量、速度、水位、持续时间和波浪作用的贡献来表征。应对这些部分或全部参数进行估计以表征外部洪水。对于洪水，通常使用以下参数：

(a) 河流：水位、水排量/流速和洪水持续时间；

(b) 海/湖：水位、洪水持续时间和流速；

(c) 波浪：高度、长度、周期、风速和方向；

(d) 波浪爬高：高度、越浪的水量和每秒水量；

---

[26] 谱加速度比峰值地面加速度提供更全面的信息。

(e) 湖震 / 假潮：振荡频率和波高；

(f) 冰：厚度和流速。

8.22. 与洪水可能同时发生的风速、方向和持续时间，应当作为潜在的危害组合予以考虑。

其他自然灾害

8.23. 对特定场址可能有各种自然灾害。对于每种特定灾害，应当确定可限定与灾害相关的所有潜在影响参数。

8.24. 选择每种灾害的参数时，应当为分析危害组合影响提供可能。

人因引发危害

8.25. 对于每种人因引发危害，应当基于其特定的潜在损坏来确定参数，例如：

(a) 对许多与运输相关的危害，实际危害是爆炸或危害物质的排放。关键参数应当是所运载物料的数量或在事故中可能排放的最大量；

(b) 对于来自附近工业设施的排放，适当的参数是物料的性质和在事故中可能排放的最大量；

(c) 对于碰撞，关键参数应当与碰撞相关，即碰撞物的质量和速度（例如驳船与进水口的碰撞，飞机与构筑物的撞击）；

(d) 若人因引发危害是由直接撞击（例如飞机坠毁）后的爆炸所引起的，关键的参数应当涉及所载的燃料量和可能对构筑物造成损坏的重型发动机的质量的某种组合；

(e) 对于诸如管道事故的危害，适当的参数是可排放物料的装量及物料的性质和压力。

8.26. 每种人因危害导致的各种影响因素组合都应当予以考虑。例如，飞机坠毁可能造成直接损坏、爆炸、火灾和振动。类似地，管道事故可能导致爆炸（爆燃或爆炸引起的冲击负载）、火灾和振动。其还可能产生能够影响核电厂不同部分的飞射物。在对人因引发危害进行表征时，应当考虑到所有的一次和次生影响。无论其引发源如何，影响应当以下列参数来表达：

(a) 冲击负载；

(b) 热负载；

(c) 振动负载；

(d) 有毒气体的传播等。

8.27. 对于气体云的爆炸，应当考虑从其来源到电厂的潜在飘移。

8.28. 应当考虑人因引发危害与其他危害现象的组合，并考虑可能的相关性（例如化学排放、风速和风向）。

外部危害的详细分析

8.29. 应对经过初次筛选后的所有危害、边界分析由其产生结果的筛选、其结果对于特定应用，难以得出结论和建议，或难以判断危害或事故假想方案对风险的重要性等情形进行详细分析。

8.30. 当通过边界分析只能对一定规模的危害，而不能对整体危害得出有效结论时，应当将整个危害划分为子类，并对特定的子类或相关假想方案进行详细分析。内部始发事件一级概率安全评定模式的可用是开展外部危害详细分析的先决条件。

8.31. 详细分析应当以实际的模式和数据为基础，包括可对与所考虑的外部危害相关的所有现象进行建模的一级概率安全评定综合模式。

8.32. 在进行详细分析时，当外部危害具有共同的来源（例如强风、闪电）或其他相关性（例如由于降水造成的高水位、大坝损坏）时，应当考虑外部危害组合影响。

外部危害频率评定

概述

8.33. 外部危害频率评定旨在获得针对每个潜在相关外部危害的强度（由危害的某种参数表示）和发生频率之间的关系（‘危害曲线’）方面的场址相关详细信息。在频率评定中应当使用电厂及其环境的信息来源。

8.34. 外部危害的表征为多个输出参数，其中一些可能是概率相关的。为简单起见，危害曲线通常以有限个（通常是一个）参数来描述。在响应分析和缺陷评定中，通常会考虑对危害进行“完整”描述所需的其他参数。

8.35. 危害分析（对超过特定强度频率的估计）应当基于该场址特定的概率评价，其反映了最近的可用数据、场址特定信息以及电厂竣工或在运状态，如有相应的数据可用的情况下。在分析中应当使用历史数据或/和现象学模式。应当尽可能使用关于危害发生的最新数据和最先进的方法。通常，应当绘制危害曲线族以表达危害表征的不确定性。

8.36. 应对时间趋势进行分析，以确认不存在危害频率增加的趋势。除非明确地知道其是由具有非随机性质的过程所引起的，否则应当不考虑危害频率降低的最近短期趋势。[27]

8.37. 当危害频率是基于区域或通用基础上制定时，应当进行相关性分析，以了解这些数据对特定场址的适用程度且属最新数据。如有，应当将与使用区域和通用数据相关的不确定性反映在危害曲线族中（见第 8.35 段）。

8.38. 当使用专家启发或另一个基于专家的过程来开发危害曲线时，应当为该过程建立程序并得以遵循。该程序应当确保所建立的过程是正式、结构化和形成记录的，且至少应当满足以下条件：

(a) 选择为解释现有可用信息而能够对多个备选假设的相对置信度做出评价的合格专家；
(b) 保持专家意见的独立性；
(c) 专家判断的使用、基本原理和背景信息以可追溯和可重复的方式记录在案；
(d) 陈述专家判断中的不确定性和变化。评定这些不确定性和变化带来的影响；
(e) 基于过程结果得出的结论具有可靠的基础。

地震危害

8.39. 应当基于地震危害场址特定的概率分析得出场址地震频率。

---

[27] 例如，观察到的某河床中的差异性可用于支持相关运输事故频率的降低。

8.40. 应当建立反映目前知识状态的最新综合性数据库，包括：

(a) 地质、地震和地球物理数据；

(b) 场址地形；

(c) 场址的岩土工程和地球物理属性。

作为数据收集的一部分，应当编写一份历史报告、地质鉴定和/或仪器仪表记录的地震目录。

8.41. 应当考虑所有可能造成破坏性地震的可信来源。地震源表征为震源的位置和几何构型、地震的最大震级和重现概率。

地震源特征中还应当包括偶然不确定性和认知不确定性。[28]

8.42. 采用专家判断法来确定地震源表征的过程应当遵循第8.38段所提建议。

8.43. 用于表征地震危害的参数范围应当为准确估计地震风险而足够广泛和详细，且应当与物理数据及其解释相一致。

8.44. 对于危害分析使用的下限参数值，应当证明带任何比之较低的参数值的地震事件不会对结构和部件造成损坏，包括场外的结构和部件，如输电线和输送危害物质的管道。

8.45. 在评定地震危害发生的频率时，应当确保所考虑区域的大小和调查的范围足以表征对特定参数的估计发生频率有贡献的所有可信地震源。

强风

8.46. 用于计算强风频率和强度的模式应当基于可反映最近得到的区域和场址特定信息的场址特定数据。分析至少应当涵盖场址所经历的最恶劣天气条件。因此，最近的、短期的强风频率下降趋势应当不在强风频率评定中占主导地位。

8.47. 计算龙卷风的频率和强度时，应当采用龙卷风发生和强度等方面的最新方法和最新数据。计算应当包括下列因素：

(a) 龙卷风强度随发生频率的变化；

[28] 概率安全评定中建模事件的随机性导致偶然不确定性。知识状态的局限性导致认知不确定性。

(b) 损坏面积宽度与其长度的关系；

(c) 龙卷风面积与其强度的关系；

(d) 龙卷风强度随其路径长度的变化；

(e) 龙卷风强度随其路径宽度的变化；

(f) 龙卷风的压差随其路径宽度的变化。

8.48. 计算飓风的频率和强度时，应当采用飓风发生和强度等方面的最新方法和最新数据。计算应当包括下列因素：

(a) 中心压力分布；

(b) 最大风圈半径；

(c) 风暴在陆地上的衰减；

(d) 风场特征；

(e) 海岸线位置等。

8.49. 为评价温带风暴潮及其他涉及强直风的现象，应当使用适于场址的风速记录数据。在绘制大风危害曲线时，应当保守地考虑因缺乏气象站而产生的不确定性。

外部洪水

8.50. 在计算场址区域发生外部洪水频率和后果时，应当基于可反映最近、可用、场址特定信息的概率分析。当仅有场址的短期数据时，应当使用区域性的洪水数据，并确认这些数据的适用性（即可通过相关性分析来确认场址区域性数据对场址的适用性）。

8.51. 应当考虑模式和参数值的不确定性并充分传播，以获得危害曲线族，并以此得出平均危害曲线。极端河流洪水频率及后果分析应当包括由单一梯级大坝损坏引起的洪水。

8.52. 在计算极端海洋洪水的频率及后果时，应当基于可反映最近、可用、场址特定数据的概率分析。这些数据应当得到其他沿海地区较长时期数据的支持，并适当考虑该地区的地形，包括在调整后的沿海区域内和陆地上。应当始终考虑高波浪和大风的组合。

8.53. 在计算极端湖泊洪水的频率及后果时，应当基于可反映最近、可用、场址特定数据的概率分析。始终应当考虑风所致波浪的影响，包括任何潜在的由龙卷风所引起的水位移。

8.54. 在计算海啸的频率及后果时，应当基于由工程分析所支持的可靠的区域性数据。应当适当考虑与海啸的频率和后果相关的不确定性。

其他自然灾害

8.55. 应当建立综合数据库以用于支持特定自然灾害的频率评定。数据库应当包括为支持危害曲线的现实和验证估计所需的所有相关信息。尤其是关于场址附近及区域内发生灾害的历史信息应当为了使用阶段数据的可用而纳入数据库。

8.56. 应当使用场址特定的和区域性数据来估计特定自然灾害的频率。应当采用相关性分析来支持区域性数据的使用。

8.57. 在特定情况下，如既没有场址特定的数据也没有区域性数据时，可使用国际通用数据。在使用国际通用数据时，应当调查该数据对所分析场址的适用性，并应当记录分析中所用的所有假设。

人因引发危害

8.58. 应当收集适当的信息（最好以数据库的形式），并用于支持特定的人因引发危害的频率评定。为支持现实有效的危害频率评定之需，此类信息至少应当包括下列数据：

(a) 关于在核电厂预定半径的场内、场外存储的爆炸、危害或有毒物质组成的定性和定量信息：
   (i) 潜在危害来源（在核电厂预定半径内）：
      - 场外：
         — 储油站；
         — 气或油输送管道；
         — 车辆运输；
         — 铁路运输；
         — 河流运输；

— 其他设施。

- 场内：
  - — 仓库（酸、联氨等）。

(ii) 潜在危害源到核电厂的距离（以千米为单位）：

- 到构筑物的距离；
- 到装有安全重要设备厂房的距离；
- 到通风入口的距离。

(b) 其活动可能影响电厂的军事或训练设施的位置，并描述训练演习的频率。

(c) 可能的事故、频率及其潜在后果（爆炸能力）。

结构和部件的易损性分析

概述

8.59. 应当在电厂特定的信息可用时及在分析（边界分析或详细分析）所需的程度上，使用电厂特定的信息和可接受的工程方法对结构和部件的易损性 [29] 进行评价。在此类分析中，应当将电厂巡视的结果纳入考虑。

8.60. 易损性分析应当不局限于场址内的构筑物，还应当包括场外的构筑物，如电力线和输送危害物质的管道系统，因为涉及此类场外结构的故障可能导致始发事件，如场外电源丧失或爆炸。若易损性低，则此类故障可能会高度相关。

8.61. 易损性分析应当包括基础信息中的不确定性，特别是当使用非电厂场址特定数据（即通用数据）时。

地震危害

8.62. 地震易损性分析的结构和部件清单应当包括地震危害一级概率安全评定模式中所包括的所有结构和部件。初始部件集应当基于一级概率安全评定的部件清单。应当将清单范围扩大至包括所有结构和部件及其组合，如其故障可能对堆芯损坏频率或大排放频率产生贡献，后者对于二级概率安全评定很重要。

[29] 易损性是指在给定的输入危害程度下，系统、结构和部件故障的条件概率。

8.63. 应当通过评审电厂设计文件和电厂巡视，识别在地震期间和之后妨碍设备可运行性的结构和设备的所有现实故障模式。

8.64. 应当针对所发现的关键构筑物（如滑动、倾覆、易弯折、过度移位）、设备（如锚固故障、与相邻设备或构筑物的撞击、支撑故障、功能故障）和土壤（如液化、边坡失稳、过度差异沉降）的所有相关故障模式，开展易损性评价。

8.65. 通过电厂巡视为易损性分析提供支持。巡视应当集中在锚固、横向地震支护及其与结构、系统和部件的潜在相互作用。应当特别考虑非抗震鉴定的结构、系统或部件掉落至抗震鉴定设备的可能性。

8.66. 巡视的重点还应当包括潜在的地震引发火灾和洪水。

8.67. 在计算与地震易损性相关的参数（例如，构筑物的中位抗震能力及其变异性）时，应当基于电厂自身数据，并以实际地震数据、易损性试验数据和通用鉴定试验数据为补充。

8.68. 当基于通用数据欲将低易损性的结构和部件筛选掉时，应当证明通用数据是保守使用的，且未忽视相关的电厂和场址特定特点。

8.69. 对结构和部件在其故障程度上的地震反应的估计，应当基于给定场址地面运动参数（如平均谱加速度）的场址特定地震反应谱。

8.70. 在分析位于不同厂房中的结构和部件响应的联合概率分布时，应当考虑所输入的地面运动、结构和土壤性质的不确定性。

8.71. 对于出现在主导性事故序列中的所有结构和部件，应当确保相关的场址特定易损性参数是基于电厂自身信息排出的。这对于避免在一级概率安全评定地震危害贡献的失真是至关重要的。

强风

8.72. 评定强风的影响时，应当考虑包围安全相关构筑物的外部屏障（如墙和屋顶）、任何暴露在相应天气的结构、系统或部件或其组合、因风载飞射物撞击（其可能导致始发事件）造成的损坏后果等方面的特定特点。应对电厂厂房及其周围环境进行调查，以评定被强风刮起并可能成为飞射物的数量和类型。还应当基于现有技术方法，评定飞射物撞击的概率。

8.73. 应当针对强风下其故障可导致始发事件的结构、系统或部件或其组合，对电厂特定的、现实的易损性进行评价。

8.74. 应当使用电厂自身数据评定结构和部件与强风相关的易损性。评定中，应当考虑可能落入或落到与安全相关结构上并造成损坏的非安全结构。该评定中，电厂巡视的调查结果应当用作重要的信息来源。

8.75. 应当针对每个结构或部件，建立与某一特定故障模式相对应的易损性曲线族，并采用中值风速容量和不确定性特征（如对数标准差）表示，表示结构或部件的容量的随机性和中值容量的不确定性。

外部洪水

8.76. 应对在河流高洪水水位条件下坝体故障进行分析，并确定相应的频率。[30]

8.77. 在评价结构和部件在外部洪水方面的易损性时，应当使用电厂自身数据。在评定中，应当考虑可能落入或落到与安全相关结构上而造成损坏的非安全结构。评定中，电厂巡视所得的结果应当用作重要的信息来源。所有位于低标高的构筑物，特别是吸入口和最终热阱，都应当纳入考虑范围。

8.78. 易损性分析应当包括浸没、波浪对结构和部件的动负载以及地基破坏（土壤侵蚀）。

其他自然灾害

8.79. 对于其他自然灾害，应当遵循地震危害、强风和外部洪水易损性分析方面适用的概述和建议。

人因引发危害

8.80. 对于人因引发危害，应当遵循地震危害、强风和外部洪水易损性分析方面适用的概述和建议。

[30] 应当针对河流的不同水位计算大坝故障概率。通常假想当河流水位高于大坝失效的设计水位时则大坝失效。

外部危害与一级概率安全评定模式的整合

概述

8.81. 实际上，内部始发事件一级概率安全评定模式总是被用作外部危害一级概率安全评定模式的基础。一级概率安全评定模式应对内部始发事件一级概率安全评定模式进行修改，以便纳入因外部危害影响引起的不同方面。在从内部始发事件概率安全评定模式选择合适的事件树时，应当评定可能导致不同等级的内部始发事件（如大破口冷却剂丧失事故、小破口冷却剂丧失事故、瞬态）或可能直接导致堆芯损坏的危害的主要影响（例如，使用危害事件树）。附件 II 为地震危害提供地震事件树的示例。重要结构、系统和部件适当的危害曲线和易损性应当纳入外部危害一级概率安全评定模式予以考虑。与特定危害相关的所有重要相关性、关联性和不确定性都应当在外部危害一级概率安全评定模式中予以考虑。应当修正与恢复和紧急停堆后的人因故障相关的概率，以评定外部危害对内部始发事件一级概率安全评定模式中所纳入的恢复和人员行动的影响。

8.82. 外部危害一级概率安全评定模式应当反映电厂竣工和在运状态。

地震危害

8.83. 应对内部始发事件一级概率安全评定模式加以修正，以将不同于内部始发事件一级概率安全评定模式的相应方面的地震特定内容纳入模式中。

8.84. 对于超过一定震级（如 50%设计基准地震）的地震危害，许多电厂都强制要求手动停堆。地震危害的一级概率安全评定模式应当反映此项要求，即使对动力转换系统具有高抗震能力及可避免反应堆自动紧急停堆的情形也应当如此。

8.85. 地震危害一级概率安全评定模式应当包括所有可能导致堆芯损坏的地震引发的重要始发事件。尤其应对导致以下类型假想方案的始发事件进行建模：

(a) 大型部件（如反应堆压力容器、蒸汽发生器、稳压器）的故障；

(b) 各种尺寸和位置的冷却剂丧失事故。因地震导致小管线（如波动管）的破裂，进而引发的极小破口冷却剂丧失事故，也应当作为额外故障模式在地震危害一级概率安全评定模式中予以考虑；

(c) 丧失场外电源；

(d) 瞬态（不论是否有动力转换系统故障），包括各种支持系统的丧失。

8.86. 当地震导致的内部始发事件特定事故假想方案未在一级概率安全评定模式中进行考虑时，应当将特定事故序列模式增加到内部始发事件的一级概率安全评定模式中。应当将内部始发事件一级概率安全评定模式加以扩展，以将地震危害纳入一级概率安全评定模式中，从而涵盖更广范围的设备或设备故障模式，如非能动部件的故障（结构、厂房、配电系统、电缆槽、继电器震颤等）。应当考虑对堆内构件的影响，特别是由于地震事件对反应堆堆芯的影响而导致的控制棒卡棒。

8.87. 在内部始发事件一级概率安全评定中已建模的所有结构、系统和部件，以及由于地震造成的损坏可能会影响到事故序列的那些结构、系统和部件，均应当纳入地震危害一级概率安全评定模式中。

8.88. 地震危害一级概率安全评定模式应当包括所有对堆芯损坏频率有贡献的非地震相关故障、不可用性和人因故障。

8.89. 地震引起的结构、系统和设备的损坏模式中应当充分考虑因地震事件引发厂房损坏后位于该厂房内设备的所有相关故障。如欲从模式中消除该类相关性或者降低其在模式中的重要性，应当予以解释论证。

8.90. 地震危害评定、地震易损性、结构、系统和部件间的相关性、非地震引发的故障、不可用性和人因故障应当适当地纳入地震危害一级概率安全评定模式中。

8.91. 应当针对恢复行动和人因故障概率进行全面检查和相关调整。应当从一级概率安全评定模式中删除由于特定震级地震事件的影响导致的不能执行的恢复行动，或者增加执行该恢复行动时的故障概率。应当根据特定的地震条件，对内部始发事件一级概率安全评定模式中的始发事件做出的响应中可能发生的所有后始发事件人因故障进行修正和调整。至少，应当考虑地震对运行人员行为形成因子的以下影响：

(a) 地震事件后，至特定结构、系统和部件路径的可用性；

(b) 压力水平的增加；

(c) 指示故障或错误指示；

(d) 通信系统故障；

(e) 含随之而来的火灾和洪水的假想方案；

(f) 影响运行人员行为的其他适当因素。

8.92. 地震引发的火灾和洪水应当包括在地震危害一级概率安全评定模式中，除非有正当性证明其他地震损坏涵盖地震引起的火灾和洪水的额外影响。

8.93. 在堆芯损坏频率量化时，除了综合结果外，作为模式量化的结果，还应当获得每个事故序列和最小割集的关键信息。

8.94. 应对地震危害一级概率安全评定模式进行整合和量化，以使来自每个一级概率安全评定（即地震危害的频率、地震易损性、相关性及与系统分析相关的方面）不确定性在模式中得以适当传播，以获得堆芯损坏频率正确的不确定性特征。

强风

8.95. 一级概率安全评定模式应当包括所有由强风引起的始发事件，并应当尽可能完整，以模拟所有与风相关的损坏。

8.96. 对由强风导致的事故序列的考虑应当包括场址特定的危害曲线以及对其损坏可能导致一级概率安全评定模式中设备故障的所有结构的易损性。需要考虑的其他因素应当包括设备不可用或故障以及与强风无关的人因故障。应当调整人因故障的概率，以考虑风对人员行为形成因子的影响。

外部洪水

8.97. 对由外部洪水引发的事故序列的考虑应当包括场址特定的危害曲线以及对其损坏可能导致一级概率安全评定模式在设备故障的所有结构、系统和部件的易损性。需要考虑的其他因素应当包括设备不可用或故障以及与外部洪水无关的人因故障。应当调整人因故障的概率，以考虑洪水对人员行为形成因子（特别是设备的可达性）的影响。

8.98. 在开发外部洪水所致始发事件的事故序列模式时，应当充分考虑不确定性、相关性和关联性。

其他自然灾害

8.99. 应当遵循地震危害、强风和外部洪水模式整合的一般方面和建议。

人因引发危害

8.100. 应当遵循地震危害、强风和外部洪水模式整合的一般方面和建议。

文档记录和结果描述

概述

8.101. 为满足参考文献[3]关于外部危害一级概率安全评定文档要求 20 第8.101－8.111 段提供了建议。对外部危害一级概率安全评定的筛选分析、边界分析和详细分析应当按以下便于同行评审及一级概率安全评定的未来升级和应用的方式形成文档记录：

(a) 筛选每种特定外部危害时，应当描述所使用的程序、提供所用方法、所做的假设及其依据等方面细节，并形成文档记录；

(b) 应当描述用于确定每个外部危害的危害曲线的方法，包括：
  (i) 用于确定危害曲线的数据；
  (ii) 为输入和结果提供依据的技术解释；
  (iii) 基本假设和相关不确定性。

(c) 应当提供需进行易损性分析的结构、系统和部件的详细清单，以及：
  (i) 每个结构、系统或部件的位置；
  (ii) 用于易损性分析的关键假设和方法；
  (iii) 每个结构、系统或部件的主导性故障模式；
  (iv) 分析的信息来源。

(d) 还应当讨论不进行缺陷分析的那些结构、系统和部件，并提供从一级概率安全评定模式中将其筛选掉的依据；

(e) 对内部始发事件一级概率安全评定模式所做的特定调整应当进行完整记录，并说明每处调整的正当性；

(f) 应对边界分析和详细分析的最终结果形成文档记录，包括与外部危害相关的每个假想方案的堆芯损坏频率、重要最小割集和重要事故序列。同时应当遵循本“安全导则”第 3.15－3.22 段提出的关于文档记录的一般性建议。

8.102. 应当提供外部危害一级概率安全评定的如下主要输出结果：

(a) 堆芯损坏频率及其不确定性分布；
(b) 敏感性研究的结果；
(c) 重要事故序列和重要最小割集的清单；
(d) 讨论重要序列和重要最小割集的技术基准；
(e) 描述不确定性的主要贡献者。应当讨论认知和偶然不确定性的贡献者。

地震危害

8.103. 应当描述对震源表征所用的特定方法和所选的参数。特别应当详细记录作为输入和结果建模基础的特定解释。

8.104. 地震危害一级概率安全评定模式文档中应当包括以下信息：

(a) 地震危害一级概率安全评定中考虑的结构、系统和部件清单；
(b) 每个结构、系统和部件的易损性表征及其技术基准；
(c) 一级概率安全评定所模拟的地震危害范围内的定量化损坏概率；
(d) 结构、系统和部件的重要故障模式及每个结构、系统和部件的位置；
(e) 为考虑地震事件的影响而对内部始发事件一级概率安全评定模式所做的特定调整；
(f) 在地震危害一级概率安全评定中建模的相关性（特别是空间相互作用）的全面信息，以及用于消除或降低相关性影响的任何假设。

8.105. 应当充分描述筛选掉任何结构、系统或部件的依据。

8.106. 对地震易损性量化所使用的方法和程序，应当形成文档记录。此应当包括地震易损性分析的以下不同方面：

(a) 地震反应分析；
(b) 筛选所涉及的步骤；

(c) 电厂巡视；

(d) 设计文件评审；

(e) 每个结构、系统和部件关键故障模式的识别；

(f) 每个结构、系统和部件易损性的计算。

8.107. 应当详细记录电厂巡视的程序、人员组成及由其所得的观察和结论。

强风

8.108. 强风一级概率安全评定应当以便于一级概率安全评定评审、应用和更新的方式形成文档记录。文档中应当特别包括以下信息：

(a) 对确定强风危害曲线所用的特定方法和数据的描述；

(b) 为考虑与强风相关的影响而对一级概率安全评定模式所做的特定修改；

(c) 分析中所考虑的所有结构、系统和部件的清单，以及从分析中被筛选掉的结构、系统和部件的正当性；

(d) 推导一级概率安全评定模式中所有结构、系统和部件的强风易损性所使用的方法和数据；

(e) 一级概率安全评定在堆芯损坏方面的最终结果以及有用的中间结果。

外部洪水

8.109. 外部洪水一级概率安全评定应当以便于一级概率安全评定评审、应用和更新的方式形成文档记录。文档中应当特别包括以下信息：

(a) 对确定外部洪水危害曲线所用的的特定方法和数据的描述；

(b) 为考虑与外部洪水相关的影响而对一级概率安全评定模式所做的特定修改；

(c) 分析中所考虑的所有结构、系统和部件的清单，以及从分析中被筛选掉的结构、系统和部件的正当性；

(d) 推导一级概率安全评定模式中所有结构、系统和部件的水灾易损性所使用的方法和数据；

(e) 一级概率安全评定在堆芯损坏方面的最终结果以及有用的中间结果。

其他自然灾害

8.110. 应当遵循地震危害、大风和外部洪水分析的文档方面的概述和建议。

人因引发危害

8.111. 应当遵循地震危害、大风和外部洪水分析的文档方面的概述和建议。

9. 低功率和停堆模式一级概率安全评定

低功率和停堆模式一级概率安全评定的概述

9.1. 针对如何满足参考文献[3]相关低功率和停堆模式一级概率安全评定的要求 6－13，本部分提供了建议。原则上，因内部始发事件致低功率和停堆状态的一级概率安全评定是基于与第 5 部分所述的满功率状态一级概率安全评定相同的方法。因此，除非对低功率和停堆模式有其他特定规定，本部分的结构与第 5 部分的结构和图 1 所示的总体分析框架基本一致。除非低功率和停堆模式的方法和条件需要特定的描述，避免了重复而只提及本“安全导则”前述内容。然而，值得注意的是，分析目标不一定是确定堆芯损坏频率，因为燃料损坏频率和意外临界也可能是关心的风险指标。

9.2. 正如对满功率状态，内部和外部危害对低功率和停堆状态也是重要的。本“安全导则”第 6－8 部分中讨论的方法适用，但应当根据低功率和停堆模式的特定情况进行修改调整。始发事件的范围原则上是相同的，但是对事件的筛选可能导致不同的模式。这对低功率和停堆状态的持续时间比满功率状态的持续时间短得多的情形尤其如此。这个比例在许多情况下是 1 : 10 或更少。显然，在低功率和停堆状态下，外部危害的发生概率更小。另一方面，对低功率和停堆状态的后果也大不相同。例如在处理重型设备时，可能需要仔细考虑地震事件或外部爆炸，外部洪水也可能导致核电厂不同的事故序列。

9.3. 在低功率和停堆状态期间，通常在轻水堆容器式电厂开展以下活动：

(a) 从满功率达到停堆状态；
(b) 运行余热排出系统；
(c) 开启反应堆压力容器，堆腔内浸水；

(d) 换料；

(e) 维护和试验；

(f) 关闭余热排出系统并恢复至满功率运行。

对于其他类型的反应堆，活动清单可能有不同，例如，打开反应堆压力容器和堆腔内浸水与通道式反应堆无关。附件 III 提供了压水堆和沸水堆停运概况示例和电厂运行状态示例。

停堆类型和设备运行状态的规范

9.4. 与满功率运行相比，在低功率和停堆模式下，电厂的运行配置和运行工况发生了显著变化。通常（对于离线换料的电厂），有三种不同类型的停堆：

(1) 定期换料停堆，在此期间也进行主要的维护活动；

(2) 计划停堆，在此期间仅进行特定的维护活动；

(3) 在满功率运行过程期间因故发生的计划外但可预见的停堆。

应当在电厂的技术规范中反映上述内容，通常根据运行模式分类，每一类对电厂设备的可运行性都有其要求。

9.5. 对第 9.4 段提及的各种类型停堆进行分析是良好实践。应当全面评定与换料停堆相关的风险。应当根据一级概率安全评定的目标，决定是否需对其他两种停堆类型进行全面分析。必须对干扰后的序列进行分析，直至达到安全稳定的状态。在固定的任务时间终止分析可能会妨碍获得有意义的结果。在许多情况下，第一步是分析典型的停堆。对于运行中的反应堆，此种停堆应当从最近的一次停堆开始，并增加从最近停堆记录文件和与负责规划此类停堆相关人员的讨论得出的相关因素。如必要，应当单独评价预计会对风险有贡献的特定停堆因素。例如，在专门为某些维护活动计划的停堆情况下，将与计划停堆相关的风险和与持续运行相关的风险进行比较，可为决策提供重要输入。

9.6. 若概率安全评定的目标之一是评价与未来运行相关的风险，则应当在分析中纳入对停堆程序的预期修改。

9.7. 在低功率和停堆期间，存在大量和各类电厂状态，若单独处理，将导致需要分析的假想方案数量过多。为了处理低功率和停堆期间的各种电

厂状态，应当确定有限数量的电厂运行状态，其电厂状态和配置足够稳定且具代表性。

9.8. 为将电厂运行状态的组合数限制在可处理的范围内，需要对类似的状态进行分组。分组时应当考虑电厂状态的下列物理和技术方面：

(a) 反应堆临界（和/或停堆裕度）；
(b) 衰变热的水平；
(c) 反应堆冷却剂系统的温度和压力；
(d) 一回路系统的水位；
(e) 反应堆冷却剂系统打开或关闭状态；
(f) 反应堆冷却剂系统回路的可运行状态；
(g) 燃料位置；
(h) 安全系统和支持系统的可用性，包括考虑其是自动或手动控制；
(i) 系统校准；
(j) 安全壳完整性的状态。

9.9. 对于低功率和停堆状态的一级概率安全评定，应当基于实际运行经验并根据现行实践和程序来确定电厂的运行状态。根据前述步骤中执行的停堆类型的选择（第 9.5 段），应对适当数量的停堆进行详细分析，以确定停堆期间所相关注参数在全时间内的实际状态。可用于此目的的相关信息来源包括：

(a) 停堆和启动程序；
(b) 特定停堆的停堆计划；
(c) 停堆的通用电厂实践；
(d) 停堆技术规范；
(e) 技术状态控制导则；
(f) 可提供停堆信息的其他文件（如详细记录硼浓度的日志簿）；
(g) 维护记录（指明特定部件的维护时限）；
(h) 与运行人员和值班主管的面谈；
(i) 与停堆计划人员的面谈。

应当从此类信息来源中提取并记录与电厂运行状态表征相关的所有信息，特别是安全功能和其他相关功能的可用性。附件 III 包含有选择电厂运行状态的示例，其中区分了 11 种不同的电厂运行状态。然而，需要特别强调的是，对于低功率和停堆一级概率安全评定，分析应当基于大量的电厂运行状态并有赖于概率安全评定的特定应用，例如用于风险监控应用。

9.10. 为避免遗漏某些电厂运行状态（例如，中间电厂功率水平）的风险贡献因素，确保覆盖全运行周期，或为避免重复计算，应当根据每个电厂运行状态（包括满功率）下的持续时间、功率水平和系统配置、以及进入每个电厂运行状态的频率（每日历年）和始发事件（例如，同一事件的频率可针对满功率和低功率分析进行估计），明确规定每个电厂运行状态之间的接口点。为此目的应当使用运行历史数据。

始发事件分析

9.11. 原则上，始发事件的识别遵循第 5.11－5.39 段描述的方法。因此，应当处理冷却剂丧失事故和瞬态，以及在内部和外部危害分析中识别的始发事件。作为起点，可以从满功率分析编写通用清单。该清单应当根据第 9.12－9.22 段描述的步骤进行修改和扩展。

9.12. 第 5.11 段将始发事件定义为可直接导致堆芯损坏或威胁正常运行的事件，并需要使用安全或非安全系统进行成功缓解以防止堆芯损坏。如第 9.4－9.8 段指出，在不同的低功率和停堆状态下，堆芯配置状态可能大不相同，例如堆芯在压力容器内与其卸载到安全壳内的燃料水池（贮存在反应堆厂房外部乏燃料水池中的燃料，不包含在本“安全导则”）。因此，停堆工况下有许多特有的始发事件，其不同于满功率运行一级概率安全评定中所识别出的事件（见附件 III 的示例）。此外，许多始发事件可能是由维护活动或运行程序相关的人因造成的。对于低功率和停堆状态一级概率安全评定而言，所关心的主要始发事件类别是威胁关键安全功能的事件，如排出热量、一回路装量或完整性和反应性控制。这意味着，不仅如满功率模式的堆芯损坏可能是低功率和停堆模式一级概率安全评定中事故序列的终态，还涉及反应堆压力容器外燃料损坏的状态，此类状态通常称为燃料损坏状态和临界事件。有必要决定哪些状态应当包含在分析当中。该决定应当以国家风险目标为基础。此类状态的特征高度专属于反应堆类型，因此

不能在此进行深入讨论。在大多数情况下，低功率和停堆状态一级概率安全评定处理以下事件：

(a) 在装卸过程中的燃料损坏；
(b) 重物坠落对燃料造成的损坏；
(c) 由于燃料配置（在燃料水池或压力容器内）的变化而引起的临界；
(d) 丧失对燃料水池的冷却。

9.13. 应当审慎并清晰度地识别所关注的终态。为补充根据第 9.11 段获得的通用清单，应当采用系统化技术识别终态。识别时可采用下列方法（详见第 5.13－5.23 段）：

(a) 系统的分析方法，如主逻辑图、故障模式和影响分析、故障树等；
(b) 对改变反应堆冷却剂系统配置的电厂程序、设备试验和维护程序进行系统性评审。

序列的终点可能不同于堆芯损坏状态。

9.14. 识别执行此类电厂正常程序中潜在的人因故障是该过程的关键目标之一，应当结合电厂巡视，使概率安全评定专家熟悉电厂的工作实际。

9.15. 为了确保低功率和停堆状态一级概率安全评定始发事件清单的足够完整性，除从满功率状态概率安全评定所得清单外，还应当评审以下信息来源：

(a) 其他类似电厂的低功率和停堆状态一级概率安全评定；
(b) 电厂运行历史；
(c) 类似电厂的经验；
(d) 低功率状态运行和停堆下的通用数据。

这些信息的公开来源包括：

(a) 通用研究（例如因不慎将未加硼酸的水注入堆芯而导致的硼稀释事件的资料）；
(b) 许可证事件报告；
(c) 来自国际组织和电厂业主团体的事件报告。

9.16. 应对始发事件进行适当分组（见第 5.32－5.39 段）。始发事件组应当包括可以使用相同的事件树和故障树模式进行分析的始发事件。即同样的事故序列适用于组中所有的始发事件。一般而言，下列标准构成始发事件分组的基础：

(a) 同组的所有始发事件对安全系统和支持系统的可用性和运行都有类似的影响；

(b) 同组的所有始发事件对于安全系统、支持系统和缓解事件所需的其他系统都有类似的成功标准；

(c) 同组的所有始发事件对运行人员都有类似的要求；

(d) 同组的所有始发事件，运行人员的预期响应是类似的；

(e) 同组的所有始发事件，序列终点所对的电厂损坏状态是相同的。

显然，始发事件可能发生在不同的电厂运行状态下（见附件 III (1)），但由于系统的可用性和成功标准对不同的电厂运行状态一般来说是不相同的，因此多数情况下，对跨电厂运行状态进行分组是不可行的。

9.17. 在某些情况下，始发事件组可能包括不完全满足第 9.16 段所列标准的事件。此种情况下，应当根据组内限制最严格的事件确定该组特征（详见第 5.35 段）。

9.18. 针对满功率状态的概率安全评定，始发事件频率的量化应当遵循第 5.128－5.132 段所描述的一级概率安全评定标准实践。然而，对低功率和停堆状态下始发事件频率的量化应当考虑到电厂的特定物项，如设备配置和可用性、技术规范和停堆管理（包括换料操作）。

9.19. 在停堆状态的一级概率安全评定中，始发事件频率可以用特定电厂运行状态下的每小时发生率来表示。但若始发事件是由于与电厂运行状态的发生而非其持续时间相关的事件所导致的（例如一些始发事件可能与试验或瞬态活动相关，其频率不以电厂运行状态的持续时间来衡量），则不能用前述方法来表示始发事件频率。

9.20. 可以通过以下三种方法量化发生在特定电厂运行状态下始发事件的频率（详见第 5.128－5.132 段）：

(1) 根据运行经验直接评估（正被分析的电厂、其他有类似设计的电厂或通用反应堆类型）；

(2) 根据满功率状态一级概率安全评定中确定的频率进行估计，并加以补充分析；

(3) 使用逻辑模式，包括导致始发事件的所有预期输入。

为了正确考虑导致始发事件的失误（例如，导致衰变热排出功能丧失的失误）与响应事件中的失误（如未能恢复衰变热排出功能）间的相关性，应对导致始发事件的失误进行明确建模。

9.21. 始发事件与电厂运行状态之间指配的总体结果应当以表格或其他总览的形式给出。如附件 III 所示。

事故序列分析

安全功能、安全系统和成功标准

9.22. 关于事故序列分析应当使用的一般方法第 5.40－5.68 段提供了建议。虽然停堆期间的衰变热水平通常远低于刚自满功率停堆后的水平，但可能的电厂配置特征仍可能引发威胁安全功能的事件。分析时应当考虑以下方面：

(a) 由于在停堆状态下安全系统的自动驱动被禁用，可能降低安全设备的可用性并增加对运行人员行动的依赖性；

(b) 一回路冷却系统和安全壳的完整性可能受到危害；

(c) 前沿系统的性能一般取决于特定的始发事件、电厂运行状态的特征和衰变热水平。

9.23. 应当采用功能性性能标准为各种系统制定成功标准，其可能与为满功率运行状态一级概率安全评定所制定的成功标准不同。

分析以支持成功标准规范

9.24. 为适用于满功率运行工况下的一级概率安全评定构建的故障树模式应当酌情进行修改。即使系统的逻辑和响应与满功率基本相同，也应当考虑部件或系统条件可用性的可能变化。

9.25. 为了确保堆芯冷却的假设正确，应当进行热工水力计算以确定实际的成功标准。热工水力分析的详细程度应当与系统分析和一回路系统配置要求相适应。对于过渡运行模式（在停堆和启动期间）和在热停堆工况下，一回路系统的配置和条件在某些情形下与自满功率引发瞬态的相似，同时用于满功率状态的热工水力计算模式也是适用的（例如 RELAP、TRAC、MAAP、MELCOR）。在其他情况下，必须证明其适用性。对于电厂的其他运行状态，应对一回路系统特点和模式能力进行比较，以评定特定计算机程序的适用性。例如，对于轻水堆，为支持成功标准规范，热工水力分析至少应当考虑以下因素：

(a) 一回路压力边界状态；

(b) 压力容器顶盖移除或松开；

(c) 拆除安全阀或打开一回路系统通风口；

(d) 隔离的回路或安装的喷嘴坝；

(e) 蒸汽发生器水位；

(f) 一回路参数（温度、压力、不可凝气体的存在、停堆裕度）；

(g) 一回路系统水位；

(h) 余热水平；

(i) 安全壳的隔离状态。

事故序列建模

9.26. 应当使用事件树（见第 5.57－5.61 段）或类似方法以模拟电厂和电厂运行人员对始发事件的响应。在对事故序列建模前，通常的良好实践是绘制详细的事件序列图（包括人员交互）。

9.27. 事故序列建模应当由多学科的团队完成，该团队从分析过程之初就应当包括人的可靠性分析方面的专家。

事故序列终点和电厂损坏状态

9.28. 对于满功率模式，应当将事故序列分组至电厂损坏状态，以为进一步分析（二级概率安全评定或三级概率安全评定）和简洁表达研究结果而将一级概率安全评定可能的不同后果减至可控的数量。预计事故进展（堆芯损坏以外），包括对安全壳完整性和放射性核素输运的损坏，对于被分组

于某一特定电厂损坏状态下的所有事故序列而言，都应当是定性相似的。另一方面，现代分析工具为模拟事故序列直至排放类别提供了可能。这些分析方法不要求为一级概率安全评定对电厂损坏状态进行分组。考虑到所发生过程的特定特征和时间，应当为安全系统规定适当的任务时间（见第5.49 段）。

9.29. 在为低功率和停堆状态一级概率安全评定选择电厂损坏状态的过程中，应当考虑为满功率运行工况一级概率安全评定所确定的电厂损坏状态。然而，对于低功率和停堆状态的一级概率安全评定，应当识别与满功率运行工况一级概率安全评定电厂损坏状态不同的额外电厂损坏状态。例如，对于特定停堆电厂运行状态所特有的状态（如拆除反应堆压力容器盖或打开安全壳设备舱口的状态），可能需有额外的电厂损坏状态。在确定电厂损坏状态时，应当考虑以下额外的事故序列特征：

(a) 电厂运行状态的衰变热水平（自满功率运行下停堆以来的时间）；
(b) 安全壳状态－特别是对于安全壳有开口的电厂运行状态；
(c) 决定恢复安全壳隔离时间的相关条件，以及在此时间内安全壳有效性（密封性）的可能降低；
(d) 在压力容器盖拆除、喷嘴坝安装、安全阀拆除、一回路系统通风口开启的情况下，一回路系统压力边界的完整性；
(e) 一回路中水装量。

9.30. 对电厂损坏状态进行适当规范将对结果及其解释起决定性作用。

系统分析

9.31. 正如满功率工况下的一级概率安全评定，低功率和停堆模式下的一级概率安全评定系统分析的目标是对事故序列量化所需的系统故障进行详细建模。故障树分析是系统建模中应用最广泛的方法。应当尽量使用或修正为满功率工况所构建的故障树模式（见第 5.69－5.91 段）。然而，必要时应对现有模式进行修改，或者尤其是在下列情况下，可能需要开发新模式：

(a) 现有的系统模式不适用于描述在电厂不同运行状态下的特定系统行为，例如，维护时系统的不同配置；
(b) 一个特定系统在满功率运行期间处于备用而在停堆期间运行；

(c) 在停堆期间系统驱动由手动进行，而在满功率运行时自动驱动系统；

(d) 系统所需的任务时间差异大；

(e) 对不同的电厂运行工况，成功标准有变化；

(f) 对每个电厂运行状态，初始可用的通道数不同；

(g) 时间“窗口”和电厂工况有显著差异，这可能影响恢复行动的成功概率；

(h) 因对于满功率工况不必要而未对特定系统予以建模；

(i) 为建立一种仅在低功率和停堆状态下使用的安全功能配置，特定系统的互连是必要的。例如，将乏燃料冷却系统用于堆芯冷却；应当考虑这种连接的程序；

(j) 因仅对满功率工况二级概率安全评定必要而未对特定系统予以建模。

系统建模的特定要求示例详见附件 III。

相关故障分析

9.32. 如第 5.86－5.91 段对满功率状态所描述的，相关故障分析工作的目标是识别可能影响事故序列和系统模式的逻辑和量化的相关性。在这方面，相关性的主要类型为对供应系统和支持系统的功能相关性，系统之间的硬件共享或过程耦合，包括物理上相关性的由始发事件直接或间接引起的相关性，对人员交互和共因故障的相关性。分析中应当包含这些相关性。

9.33. 以满功率状态为出发点，应当评审和检查不同的支持和前沿系统及其之间的相互关联，特别是针对其对特定电厂运行状态的适合性。分析团队应当意识到，试验和维护活动可能会产生新的相关性来源，如冗余部件的同时维修或维护，示例详见附件 III。

9.34. 必要时应对满功率运行工况的相关性模式进行修订，特别是当低功率和停堆模式的成功标准不同或者支持系统的条件不同时，例如对通风系统和供电系统的要求。还应当评审系统校准和部件大修的情况。

9.35. 分析人员应当了解各种共因故障的机理以及停堆工况下的特定维护和其他活动对共因故障的发生可能产生的影响。

人的可靠性分析

9.36. 在第 5.96－5.113 段解释了人的可靠性分析的关键方面。这些方面也基本适用于低功率和停堆工况。分析停堆期间的人员交互相当复杂。因此，应当采用结构化和逻辑方式进行人的可靠性分析。与其他分析一样，人的可靠性分析的过程应当以可追溯的方式进行完整记录、存档。人的可靠性分析旨在得出既其相互间一致也与一级概率安全评定其他部分所做分析相一致的故障概率。

9.37. 根据第 5.107 段，低功率和停堆工况的典型方面均应当在分析中予以充分考虑，如广泛使用来自外部组织的外部维护人员、频繁加班和控制室工作需求的增加。还应当考虑到由于进度紧迫导致的工作监督方面的困难和压力。

9.38. 对于人的可靠性分析，应当与电厂运行和维护人员开展紧密互动，以确保低功率和停堆工况的电厂设计和运行特征在分析中得到恰当的反映。如果这不可行，例如对尚处于设计阶段或建造阶段的电厂，分析人员应当努力获取来自其他类似运行电厂的实践经验和知识。

A 类交互－始发事件前的人员行动

9.39. A 类交互（第 5.102 段）包括与试验、维护、维修和校准相关的行动，若行动不当，可能导致设备不可用。A 类交互的识别和量化过程类似于满功率状态一级概率安全评定过程，但应当特别考虑到以下低功率和停堆的特定特点：

(a) 在接近停堆结束时开展的功能试验可能会受到严格的时间约束，因此人误的可能性较高；

(b) 自动重校功能可用性的降低（例如，阀门无自动关闭信号，其可能在试验后保持开启状态）。

B 类交互－可导致始发事件的人员行动

9.40. 由于各种不同的维护措施、试验和配置的变化，不能期望在低功率和停堆状态特定始发事件（例如由于阀门不当校准所致的排放）频率相关的运行经验中观察到所有可能的人误。因此，应当明确评定人因故障导致始发事件的可能。这对于处理针对响应行动（C 类行动）的相关性也很重

要（如第 9.45 段所讨论）。此评定可以识别直接导致部件不可用的人因故障，或导致在始发事件的故障树中所建模的潜在的需求故障。分析时可以使用以下信息来源：

(a) 运行启动和停堆的书面程序；

(b) 运行经验；

(c) 相关停堆计划的文件，包括技术规范、试验和维护程序。

可能需要为 B 类交互分析进行筛选，以基于定性评价决定哪些故障可被筛选掉，并确定哪些需要进行定量评价甚至详细分析。附件 III 概述了一种可能的方法。人误概率的推导可按照第 5.107－5.111 段规定进行。

C 类交互—始发事件后的人员行动

9.41. 由于电厂自动化程度降低，C 类人员交互（详见第 5.105 段）在停堆期间尤为重要。在许多低功率和停堆状态一级概率安全评定研究中，C 类交互是堆芯损坏频率的重要贡献者。因此，应当仔细考虑对该类交互的故障概率进行现实性评定。

9.42. 选择方法时，应当系统地考虑在低功率和停堆状态下一级概率安全评定框架下对 C 类交互进行建模和量化相关的特定方面。某些方面可能与满功率情况不同，例如：

(a) 更频繁地启动警报和持续警报；

(b) 程序性指导文件的质量；

(c) 运行人员培训情况；

(d) 响应时间窗口的持续时间；

(e) 在低功率和停堆状态下，有利于人员行动的接口质量。

9.43. 值得注意的是，由于在停堆状态下的时间窗口可能远超出时间可靠性关系式的适用范围，因此使用特定于满功率运行的时间可靠性关系式所产生的数值不能不加批评地予以接受。

9.44. 特别是在使用基于事件的程序时，应当考虑始发事件原因诊断时可能出现的错误。

9.45. 与满功率运行工况一级概率安全评定一致，应当考虑同一事故序列中人员交互之间的相关性（见第 5.112 段和第 5.113 段）。但是，在低功率和停堆状态概率安全评定模式中，考虑 B 类和 C 类交互之间的相关性尤为重要。若始发事件（如衰变热排出丧失）是由人误所引起的，导致运行人员犯错误的环境可能使衰变热排出功能的恢复复杂化并导致比由机械故障导致功能丧失情形更高的故障概率。

数据评定

9.46. 低功率和停堆状态一级概率安全评定量化所需数据包括：

(a) 始发事件频率；
(b) 与人因故障概率相关的数据；
(c) 电厂运行状态的持续时间；
(d) 允许停堆时间；
(e) 部件可靠性数据；
(f) 维护不可用性，包括基于运行历史的重叠维护；
(g) 共因故障评定；
(h) 其他数据需求。

第 5 部分中所描述的数据采集基本要求和方法，同样适用于低功率和停堆状态。本部分已经提供了关于数据评定的建议－特别是关于相关故障分析、人员可靠性和始发事件频率的建议，以及相关的方法概要。

9.47. 与满功率状态相比，更难获得用于停堆状态下部件可靠性参数量化的数据。因此，一个广泛使用的方法是对来自满功率运行的数据进行修正。如无合适正当性表明这些数据的适用性时，则应当不采用此实践。

9.48. 计划停堆期间的试验主要是为了验证以前正在进行维护部件的功能，即是对设备重新投入运行之前的功能试验。不可用性的确定应当与平均试验持续时间以及其间设备受试的电厂运行状态的持续时间相关。

9.49. 应当评定可能的人员交互作用以及由于试验和维护活动导致的重要校准中的人误概率。

9.50. 应当考虑维护的可能性，因为修复可以显著提高在低功率停堆状态下安全系统的可用性。在许多情况下，不考虑维护可能导致风险的高估，特别是在始发事件后的假想方案中，分析中应当计入辨别可提升现实性考虑的某一特定维护选项可能性的概率。这里的“维护”包括短期恢复的情形，其足以满足被考虑事故序列的需求。但其应当限于根据电厂经验表明有高的修复可能性的情形，或成功概率受工程判断所支持和／或在事故序列条件下所建立的维护程序属有效等情形。

9.51. 应当考虑维护时间与电厂运行状态的相关性。这种相关性可能是由于系统和设备的可达性、承担维护的人员的可用性、备件的可用性以及对某些事故序列而言待维护设备周围的辐射水平。

9.52. 低功率和停堆状态一级概率安全评定分析团队应当认识到，在功率运行期间处于备用状态的部件可能在停堆期间处于运行状态。若停堆的操作策略是循环使用冗余部件或通道，则应当选择合适的可靠性模式。

9.53. 在计算始发事件后用于维持或达到稳定状态的在运设备不能继续运行概率的模式中，应当使用任务时间。任务时间可对系统故障概率的计算有重大影响。任务时间的假设应当与事故序列建模一致。

9.54. 若要在分析中加入可预见的停堆程序变更，则可能对数据采集产生影响。这些变更可能使可获得的运行经验相关信息无法提供必要的数据，或者只能在通过分析或工程判断进行修正后提供必要数据。

9.55. 对一级概率安全评定中所使用的参数，不仅应当得出其点估计值，还应当得出完整的不确定性分布，因为这些是不确定性分析所必需的。

事故序列的量化

9.56. 对于低功率和停堆状态一级概率安全评定，其事故序列量化方法与满功率状态的基本相同。但是应当注意的是，对于停堆状态一级概率安全评定，由于其任务时间或恢复时间通常较长，使用马尔可夫技术而不是标准故障树和事件树评价方法，可能会得到更真实的结果。然而，对于复杂系统来说，使用前述方法则较为麻烦。马尔可夫技术对核电厂概率安全评定目前还处于开发阶段。

9.57. 在评审量化结果时，如同满功率运行工况一级概率安全评定的情形，应当仔细评审所得到的最小割集。在低功率和停堆状态一级概率安全评定中，系统模式可能需要修改，以表达电厂不同运行状态。若系统模式被修改，应对不同电厂运行状态下针对类似事故序列或系统所得到的最小割集进行交叉检查，以确保这其中的任何差异能真实反映不同的电厂运行状态或序列特征，而不是源于建模方面的差错。

重要度分析、敏感性研究和不确定性分析

9.58. 对于不确定性分析，应当使用与满功率状态一级概率安全评定所用的相同技术（详见第 5.159 段和第 5.160 段）。

9.59. 重要度分析和敏感性研究应当使用与满功率状态一级概率安全评定所用的相同技术（见第 5.154－5.158 段和第 10.19 段）。

9.60. 敏感性研究是低功率和停堆状态一级概率安全评定分析的重要组成部分；其目的是分析低功率和停堆状态概率安全评定诸多特定因素的潜在影响。例如，被选择用于表征电厂运行状态的特定工况可表示比电厂运行状态中实际发生的更为广泛的工况。与满功率状态概率安全评定相比，可能存在不同的不可用系统组合；有些组合可能由更保守的分析所致，有些则源于不太保守的分析。电厂运行状态的持续时间可能更长或更短。人员行动的可用时间依电厂运行状态相对于电厂停堆的时间而可能大不相同。成功标准也依衰变热水平而可能有差异。应对此类差异进行调查，尤其是对用于对电厂运行状态进行建模的假设会对风险产生主导性贡献的情形。

文档记录和结果描述

9.61. 为满足参考文献[3]关于低功率和停堆状态一级概率安全评定文档要求 20，第 9.61－9.71 段提供了相应建议。一级概率安全评定报告的结构应当包括满功率运行工况一级概率安全评定的程序，此外，报告中应当增加描述低功率和停堆状态一级概率安全评定特殊内容的章节，如详细描述用于识别停堆类型、电厂运行状态和始发事件的过程的章节。

9.62. 如前面章节所讨论，分析的每个主要步骤所获得的结果都应当予以整合和呈现，包括从分析中得到的重要工程见解。报告中应当包括对总体结果和发现的评定以及对不确定性的讨论。

9.63. 作为对初始分析结果的响应，通常对书面的维护或运行程序进行修改或引入。对此也应当在报告中体现。

9.64. 最后，应当提出普遍性结论和建议并加以讨论。在决策所需的程度上，报告中应当包括以下专题：

(a) 堆芯损坏频率－综合所有电厂运行状态的重要贡献：
    (i) 主导序列的贡献；
    (ii) 电厂运行状态的贡献；
    (iii) 始发事件组的贡献；
    (iv) 堆芯损坏频率不确定性分析的结果；
    (v) 堆芯损坏频率重要度分析和敏感性研究的结果。
(b) 提供每个电厂运行状态的结果：
    (i) 主导序列的贡献；
    (ii) 始发事件组的贡献。
(c) 提供与二级概率安全评定的接口（如必要），包括电厂损坏状态的特征和频率。
(d) 定性见解和结论：
    (i) 结果解释及工程见解；
    (ii) 结论和建议。

9.65. 工程见解和建议的提出应当使其为决策过程提供明确的输入。

9.66. 为典型的停堆计划，尤其是换料停堆计划，构建风险剖面图是有裨益的。例如，此类剖面图可以显示电厂不同运行状态下的堆芯损坏频率，其作为停堆时间或开始降功率后的时间的函数。附件 III 提供了一个示例。

9.67. 报告中应当包括来自低功率和停堆状态一级概率安全评定的以下详细信息：

(a) 对总堆芯损坏频率有贡献的重要最小割集；

(b) 每个电厂运行状态下，对堆芯损坏频率有贡献的重要最小割集。

应当根据概率安全评定的目标来确定最小割集的重要程度。

9.68. 报告应当包括下列内容：

(a) 人误和相关故障对堆芯损坏频率的贡献；
(b) 独立故障对堆芯损坏频率的贡献；
(c) 在事件树中建模的各种安全功能对堆芯损坏频率的影响。

9.69. 除堆芯损坏频率外，还应当评定例如涉及临界或燃料水池损坏及其频率的其他终态，并记录其结果（详见第 9.12 段、第 9.13 段和第 9.19 段）。

9.70. 应当通过数据库和计算机文件充分记录和配置电厂模式和数据，以便于结果的重现和模式的应用。

9.71. 文档的编写应当符合法规评审要求。

10. 概率安全评定的使用和应用

适合应用的概率安全评定范围

10.1. “安全要求”出版物《设施和活动安全评定》（见参考文献[3]）指出，安全评定需要包括一个全范围的概率安全评定，用于估计和评定在各种运行状态、预计运行事件和事故工况下的安全威胁。概率安全评定的完整性（其包括一组全面的内部始发事件、内部危害、自然和人因引发外部危害，涵盖电厂所有运行模式包括启动、功率运行、低功率以及电厂停堆和换料期间的所有模式）将确保概率安全评定针对事故序列、结构、系统和部件、人因错误、共因故障等的风险重要度方面的见解，均是由综合集成的电厂模式所推演得出的。为满足参考文献[3]关于一级概率安全评定使用的要求 23，本部分提供了建议。应当使用一级概率安全评定来支持应用。应当认识到，在许多情况下应当将二级概率安全评定的结果和见解纳入考虑范围。[31]

[31] 注意，本部分的重点是一级概率安全评定。但应当指出，对许多应用而言，期望由二级概率安全评定甚至三级概率安全评定得出的见解也是必要的。

10.2. 在许多情况下，支持特定应用所需的概率安全评定范围可能与上述全范围不同。在任何情况下，当从其范围小于应用所需的实际范围的概率安全评定中推导得出风险见解时，在应用这些见解时应对此予以明确。

10.3. 用于任何应用的概率安全评定应当保持为“动态概率安全评定”，即应当定期更新，以反映当前电厂的设计和运行及瞬态分析，并进行完整记录，以使分析可以追溯到设计和支持性分析的细节。

10.4. 当从概率安全评定中推得风险见解时，分析人员应当注意理解各种类型的事故源（内部始发事件、内部火灾、内部水淹、地震等）对概率安全评定结果贡献的相对意义。分析人员尤其应当认识到，即使将不同类型事故源的概率安全评定模式合并为一个大的概率安全评定模式，实施各类分析时其方法也会不同，这将导致不同的详细程度和保守程度。例如，在分析由火灾引起的风险时，通常使用连续的边界和筛选方法，因此特定火灾区域分析的详细程度取决于根据筛选标准判断其对堆芯损坏频率的贡献是否足够低。这样做是为了避免将不必要的资源花费在详细的火灾建模或电缆追踪上。这种不同的详细程度可能导致得出误导性的见解。这是依赖于重要度评价的概率安全评定应用以及风险监控类应用尤为关注之点。

10.5. 若欲将某个概率安全评定用作同一场址多个类似机组的代表性概率安全评定，则应当识别特定单一机组与代表性模式之间任何差异的影响，并评定其对概率安全评定结果的影响。

风险指引法

10.6. 在下面描述的任何概率安全评定应用中，从概率安全评定所得见解应当用作风险指引决策的组成部分，并考虑以下方面：

(a) 与概率安全评定应用相关的任何强制性要求（通常包括应当遵守的任何法律或法规要求）；

(b) 由确定性安全分析所得的见解（如是否满足纵深防御的要求，是否有足够的安全裕度以及是否满足较低程度的要求，例如执行安全功能的安全系统是否有足够的冗余度和多样性水平以满足相关规定的要求，以及电厂设备是否通过了足够水平的鉴定，以使其能承受始发事件后的严酷环境）；

(c) 其他任何适用的见解和信息（可能包括成本－效益分析和关于电厂剩余寿命的详细信息、视察结果、运行经验、对电厂硬件做必要改进中工作人员所受的剂量）。

10.7. 应用风险指引法的目的是确保在任何概率安全评定应用中，在考虑到所有相关因素下，做出任何决策都应当采取一种平衡的方法。本部分其余部分中所讨论的概率安全评定应用不涵盖所有可能的概率安全评定应用。[32]

概率安全评定用于设计评价

概率安全评定在电厂全寿期中的运用

10.8. 概率安全评定应当在电厂全寿期内用于为设计评价提供部分输入。概率安全评定应当：

(a) 在概念阶段，用于为所提出的安全系统、支持系统及电厂布局设计是否适当提供见解；

(b) 在详细设计和施工阶段进行更新，以考虑到设计和安全分析获得的新信息；

(c) 被保持为在运电厂的“动态概率安全评定”，用作解决与电厂运行、定期安全评审和延寿相关问题的输入之一，并为提议的设计修改和运行改进是否适当提供见解。

10.9. 在电厂全寿期内应当使用同一概率安全评定，且概率安全评定的范围、详细程度和精确性随着设计进展、支持概率安全评定建模假设所做的更多分析以及从电厂运行经验可获得数据而不断增加。应当将概率安全评定的结果用于识别设计和运行中的薄弱环节，并对改进设计或运行的选项进行评定和排序。

10.10. 概率安全评定的结果应当被用来针对预防堆芯损坏，为安全系统和安全相关系统的设计和运行提供见解。使用概率安全评定结果时应当包括与所制定的总体风险标准和目标的比较。

---

[32] 提供概率安全评定应用更多信息的出版物示例包括《概率安全评定在核电厂的应用》[14]（IAEA-TECDOC-1200）和《概率安全评定在核电厂应用质量的确定》[15]（IAEA-TECDOC-1511）。

电厂易损性识别

10.11. 为了获得最大的效益，用于设计评价的概率安全评定应当是上文（第 10.1 段）所述的全范围概率安全评定。这将确保能够使用概率安全评定解决电厂设计和运行方面的广泛问题。概率安全评定的范围主要涉及概率安全评定中包含的始发事件和内部和外部危害的范围，以及概率安全评定中所涉及的电厂运行模式的范围。

10.12. 应当使用从概率安全评定中获得的详细定量信息（例如始发事件组的频率和割集频率，基本事件的重要度值）和定性信息为设计评价提供更详细的见解，即识别与堆芯损坏相关的特定易损性。

与风险标准和目标的比较

10.13. 一级概率安全评定的总体结果（通常是堆芯损坏频率）应当与风险标准（若对其已做了定义）进行比较，以确定所提出的电厂设计和运行是否能确保足够低的风险水平。目标应当是确定是否满足风险标准和/或目标，并提供电厂是否已达到足够的安全水平的宽泛指示，即，为防止堆芯损坏，是否已将足够的安全系统和应急程序融入到电厂设计和运行中。原则上，同样的考虑也适用于二级概率安全评定和三级概率安全评定的结果。

10.14. 对概念设计，应当将一级概率安全评定的结果与风险标准和/或目标进行比较，以检查其是否适当，并在设计阶段、建造阶段和运行阶段的各个节点检查设计是否适当。

10.15. 在进行比较时，应当考虑已进行的敏感性研究和不确定性分析的结果。这将表明满足标准和/或目标的置信度，以及其被超越的可能性。

割集的使用

10.16. 应当使用自一级概率安全评定模式得到的割集清单来确定电厂设计和运行中存在的相对薄弱环节。应当对堆芯损坏频率有重要贡献的割集进行评审（见第 5.146 段和第 5.149 段），以识别对堆芯损坏频率贡献最大的始发事件组和安全功能。对于含重要度高的基本事件的割集也应当如此。

10.17. 应当使用各组始发事件对堆芯损坏频率的贡献及其割集来确定电厂的设计是否平衡，即无特定的始发事件组和特定的事故序列会给堆芯损坏

频率带来过大的贡献。原则上，前述考量同样也适用于二级概率安全评定和三级概率安全评定的结果。

10.18. 应当使用割集清单来确定是否存在单阶割集，其表明对任何安全系统不符合单一故障要求。

重要度数值的使用

10.19. 应当计算基本事件、基本事件组、安全系统、始发事件组等的重要度，并利用其解释概率安全评定结果。在一级概率安全评定中使用的重要度数值通常包括：

(a) F-V 重要度；[33]

(b) 风险成就值（又称风险增加率）和风险降低值（又称风险降低率）；

(c) 伯恩鲍姆（Birnbaum）重要度。

10.20. 应当使用重要度数值来识别对风险有重大贡献的部件和系统，并且应当在设计层面或电厂运行期间予以仔细考虑。应当使用重要度数值来识别电厂设计或运行需考虑改进的方面。

10.21. 独立故障事件的高 F-V 重要度数值或高伯恩鲍姆（Birnbaum）重要度数值可能表明在某些电厂运行模式中系统的冗余度不足，因此需要改进。此种情况下，如有可能，应当增加系统冗余度，或者对于特定的电厂运行模式，应当使系统运行限值和条件更加严格。独立故障事件的高风险成就值可能表明应当仔细维持设备的可靠性水平，以避免风险增加。通常，F-V 重要度数值或风险降低值和风险成就值所提供的两个方面应当一同使用。

10.22. 对于共因故障，高 F-V 重要度数值可能表明在特定的安全功能方面安全系统的多样性不足。在这种情况下，可能需要对设计基准进行较大的修改。

10.23. 一级概率安全评定的结果应用于提供一种方法以确定是否：

(a) 安全系统具有足够的多样性和冗余度；

[33] 对于各种重要度的解释，请参见脚注 13－16。

(b) 对经历事故工况下严酷条件的结构、系统和部件，有足够的设备鉴定水准；

(c) 对火灾和水淹等危害，有充分的区域分隔和隔离；

(d) 人机接口设计是合适的以确保将人因故障的可能性降低到足够低的水平。

一级概率安全评定的结果还应用于确定设计是否平衡或是否需要采取额外措施以降低风险。

10.24. 在识别电厂易损性时，应当考虑到一级概率安全评定结果中的不确定性以及敏感性研究提供的见解。

设计选项的比较

10.25. 在考虑对核电厂进行改造时，通常有多种选项。应当使用一级概率安全评定来为选项的比较提供输入。其特定实践取决于所考虑改造的复杂程度，但可涵盖从对一级概率安全评定模式进行修改以纳入建议的新安全系统至对割集进行后处理以考虑更简单的更改。一级概率安全评定为综合和风险指引决策过程提供输入，以决定选择哪个选项。

一级概率安全评定在设计评价中的局限性

10.26. 若一级概率安全评定的范围小于本“安全导则”描述的完整范围—例如，若概率安全评定不包括所有可能对堆芯损坏频率有贡献的始发事件和危害—此种情况应当在一级概率安全评定的使用时予以考虑。

10.27. 此外，应当指出的是，存在某些方面，其模式和数据开发尚不完善。例如，在设计阶段，数据、模式和电厂运行实践中可能存在重大的不确定性，特别是对于新概念和设备，或对于老化效应和/或安全文化进行建模时。在使用一级概率安全评定结果时应对此予以明确。

风险指引的技术规范

10.28. 电厂的技术规范规定了电厂运行、维护和试验的限值和条件，为安全的并与安全分析中所做假设相一致的电厂运行提供了一个包络。传统上，技术规范的要求基于确定性要求和工程判断。

10.29. 运行限值和条件就诸如设备的可运行性、允许的大修时间和需求的行动（如冗余设备的试验）做出了要求。特定系统或部件的允许大修时间是指在其间应当完成任何维护或维修活动的时间周期。若超过允许的大修时间，技术规范规定电厂运行人员应当采取的行动。例如，如果在功率运行期间超过允许的停堆时间，可能要求运行人员降低功率或将电厂停堆。此外，对设备可运行性的要求通常包括对为了进行维护可能同时被解除的设备组合的限制（通常称为配置控制）。概率安全评定得出的见解可以用作论证运行限值和条件和允许大修时间正当性的输入之一。

10.30. 监视试验间隔给出了安全相关系统的试验要求，并规定试验频率，有时会规定必须遵循的试验策略。若超过了监视试验间隔，则技术规范将要求将受影响的设备认为是不可运行的。概率安全评定的这种应用涉及到风险指引法的使用，其使用概率安全评定的见解来优化允许的停堆时间、监视试验间隔和试验策略。

10.31. 应当使用风险指引法为技术规范提供依据。目标应当是提供一个与受影响电厂特点的风险重要性相关的一致性依据。

10.32. 一级概率安全评定提供的见解应当包括对用于支持技术规范风险指引的决策标准或导则进行比较所需的信息。这些信息可能包括，例如，当电厂物项正处于维护中时，堆芯损坏工况频率，递增的堆芯损坏工况概率，全年中累积的、递增的、带条件的堆芯损坏概率以及变更对年均堆芯损坏频率的影响。

10.33. 若建议将某个特定的维护活动从功率运行移到停堆模式期间（反之亦然），则应当使用概率安全评定来确定满功率和停堆模式下风险的相应变化。

10.34. 在为监视试验间隔的优化提供来自一级概率安全评定的输入时，应当为用于监视试验间隔与部件故障概率之间的关系提供正当性。

10.35. 当对试验策略进行调整时（例如引入交错试验）时，应当使用一级概率安全评定来确定此将导致的堆芯损坏频率变化。应当考虑间接影响，例如对共因故障概率的改变和对调试中人因故障可能性的改变。[34]

[34] 虽然概率安全评定模式中未明确包含调试错误，但应当就变更会如何影响调试错误的可能性进行讨论，此将为支持变更的可接受性决策提供有用的额外信息。

风险监控器

10.36. 风险监控器是一个实时分析工具，可根据实际电厂配置的多种因素生成风险信息，通常包括：电厂运行状态（功率运行或停堆模式之一）、解除在役部件以及正常运行系统运行通道和备用通道的选择。风险监控器生成的信息可用于日常维护计划，以确保维护活动的安排尽可能避免风险的高峰值，并且电厂累积的、递增的、带工况的堆芯损坏概率低。

10.37. 风险监控器在应对美国核管会维护规则方面发挥了相当作用，其要求营运组织评定和管理与维护活动相关的风险。在核电厂中通常使用大量的风险监控器以支持运行决策。因此这可视为概率安全评定的一种非常成熟的应用。

风险监控器的概率安全评定模式

10.38. 尽管风险监控器是动态概率安全评定的一种特定应用，但需要认识到，风险监控器所需的概率安全评定模式与动态概率安全评定的不同，通常需要如下所述对其进行修改。

10.39. 应对一级概率安全评定模式进行修改，使其能够计算输入的每个电厂配置的“时间点风险”，而不是概率安全评定通常计算的平均风险。这要求识别所有与平均风险（例如始发事件的频率、由于维护而导致的部件不可用性）计算相关的建模假设和数据，并代之以用于估计时间点风险的等效假设和数据。

10.40. 应对概率安全评定模式进行修正，以消除为减少概率安全评定所需分析量而做的任何简化，因为这些简化可能导致风险监控器对可能出现的某些电厂配置给出错误的结果。应当消除的概率安全评定模式中的简化一般包括：

(a) 将概率安全评定中模化为带集总频率的始发事件替换为单一始发事件（例如，将模化为一条环路上一个事件的冷却剂丧失事故替换为每条冷却剂环路上的各单一事件）；

(b) 对系统校准和正常运行系统的运行通道和备用通道的选择进行明确建模；

(c) 删除概率安全评定中为对维护进行建模所包含的基本事件，或将其概率设置为零。

10.41. 应当提升概率安全评定模式，以提供与实际电厂配置更密切相关的风险计算。概率安全评定模式的提升通常包括：

(a) 规定一种方法，用于当部件因维护而解除在役时，确定适当的共因故障概率；

(b) 使用的人员可靠性模式应当考虑到实际电厂配置中可能发生的人因故障；

(c) 引入动态事件以模拟由于电厂环境的变化而引起的始发事件频率的变化以及基本事件概率的变化。

10.42. 所开发的概率安全评定模式应当与风险监控器所用的软件相兼容。必要的改进可能包括将概率安全评定中开发的事件树和故障树模式更改为逻辑上等效的大故障树模式（通常称为“顶逻辑模式”）或改变模式中逻辑“非”和逻辑开关的使用方式。

10.43. 风险监控器的运行需要大量数据库的支持。例如，需要下述数据库，在电厂运行人员熟悉的电厂部件常规术语和概率安全评定建模的基本事件间建立链接，这些基本事件与这些电厂部件的故障或不可用性相关联。支持风险监控器应用所需的所有数据库都应当核实。

10.44. 为风险监控器开发的概率安全评定模式的逻辑结构和相关的数据库可能与原始概率安全评定的有显著差异，因此应当予以确认。确认过程旨在提供高的置信度，即风险监控器给出的定量结果是准确的，并与原始概率安全评定对所有可能的电厂配置给出的结果是相同的或等效的。

10.45. 在将动态概率安全评定进行转换用于风险监控器应用方面有大量的经验，以使其可计算时间点风险，消除不适合风险监控器的简化，改善、提高概率安全评定模式的精度并确认所生成的概率安全评定模式[16]。

风险监控器软件

10.46. 用于风险监控器的软件与用于开发和求解概率安全评定的软件有显著不同。其本质区别是风险监控器的设计目的在于供给所有核电厂人员使用，而不仅限于概率安全评定专家，用户不需要拥有概率安全评定的专业技术知识。用户仅限于对电厂配置进行更改，例如指定电厂运行状态并识别因维护而解除在役的部件。这对所选择设备使用正常电厂识别器即可完

成。因此，用户不需要直接与概率安全评定模式交互，通常无需对其进行概率安全评定技术培训。

10.47. 目前已经开发了许多高质量的软件程序，支持包括定量和定性的风险度量等多种功能。计算机允许采用通常方法，风险监控器包括一个完整范围的概率安全评定模式，用于计算每一个实际或所提出的电厂配置下的堆芯损坏频率的时间点风险，因为这可允许建模的更大灵活性并为计算所有电厂配置下的风险水平提供更高的精度。已被使用的另一种方法是为大量配置创建预先求解的评定目录。

10.48. 为风险监控器应用所选择的（或开发的）软件应当经过确认，应当提供广泛的功能，并且能为电厂广大人员所使用。软件应当能够提供实时结果。对基于对概率安全评定模式实时求解的风险监控器，软件相关的计算速度应当相当高。

风险监控器的信息表达

10.49. 风险监控器提供定量风险信息（计算时间点堆芯损坏频率值、允许的配置时间和累积递增带条件的堆芯损坏频率）和定性风险信息（安全功能和系统状态）。定性信息与确定性要求相关，并提供与定量结果所提供的见解形成补充的见解。这些见解对停堆模式的风险管理特别有用。

10.50. 风险监控器应当能够被承担各种职责的广大电厂人员所用。因此，风险监控器的信息表达应当以广大潜在用户能理解的方式进行。通常以彩色显示的形式实现，使用户能清楚地看到风险水平或安全功能和系统状态。

风险监控器的使用

10.51. 控制室运行人员和其他人使用的风险监控器应当进行及时更新，以确保当前电厂配置和环境因素的信息准确无误。良好实践是尽快进行更新，以便风险监控器能实时使用并显示当前的电厂风险。

10.52. 风险监控器可用于计划未来的维护大修、长期的风险剖面、累积递增带条件的堆芯损坏概率分析以及如设备故障等意外事件的评价。

10.53. 风险监控器产生的定量和定性风险信息应当作为综合性风险指引决策过程的一部分，其同时也考虑到强制性要求（如电厂的技术规范）和确定性要求（如保持纵深防御）。

风险监控器的局限性

10.54. 动态概率安全评定的范围或详细程度可能存在局限，因此由风险监控器提供的风险信息也会有局限。例如，一级概率安全评定模式可能不包括所有的内部和外部危害、未涵盖所有的电厂运行状态以及未对所有的运行通道和备用通道以及电厂互联进行建模。风险监控器的用户应当意识到此类局限性，并在将信息用于支持运行决策时予以考虑。

风险指引的在役检查

10.55. 核电厂管道在役检查计划的总体目标是识别在发生故障前可修复的退化领域。所执行的视察计划通常是基于传统的确定性方法和工程判断。

10.56. 风险指引法的目的是利用概率安全评定提供的见解修改视察计划（视察频率、所用方法、样本大小等），并将其集中在具有最高风险重要度的管段，减少对低风险重要度管段的视察。预计这样可降低实施管道视察的数量、降低成本并降低对运行人员的相关剂量负担，而又不会增加电厂的风险。

10.57. 目前已经开发了几种方法来进行风险指引的在役检查。[35]

概率安全评定用于风险指引在役检查

10.58. 从一级概率安全评定得出的见解应当作为确定下列事项的输入之一：

(a) 将由风险指引在役检查项目予以评定的管段；
(b) 待评定管段的风险重要度；
(c) 待视察管段的目标故障概率；
(d) 由在役检查计划的变更所引起的风险变化。

10.59. 对于分析中所包含的各管段，应当通过以下方式之一确定该段故障的后果：

(a) 作为一个始发事件，考虑可能发生的次生故障（例如，由于水或蒸汽的排放、管道甩动）；

[35] 示例包括由其开发并得名的电力研究所方法和西屋业主集团方法，两者都已被广泛使用。

(b) 作为一个备用系统中的一个故障，其可能导致该系统（或整个系统）的一个通道在执行其安全功能时不可用；

(c) 作为一个系统（或整个系统）一个通道的一个故障，当该通道因加于该管段的负载而按需求运行时发生故障。

10.60. 全范围一级概率安全评定通常已包含了直接导致始发事件的管道故障。应对此予以检查是否属实。然而，概率安全评定模式通常不包括导致安全系统在需求时不可用或故障的管道故障，原因是与能动部件故障对安全系统故障概率的贡献相比，管道故障的贡献可以忽略。

10.61. 对导致始发事件的管道故障，应当使用概率安全评定来确定堆芯损坏工况概率。对导致备用系统故障或需求时系统故障的管道故障，应当使用概率安全评定来计算堆芯损坏工况频率。

10.62. 确定风险指引在役检查项目所包括的所有管段的风险重要度的严格方法是修改概率安全评定模式以明确包括这些管段，从而直接确定相关的堆芯损坏频率和堆芯损坏工况概率。这种方法已应用在各成员国所开展的部分风险指引在役检查项目中。

10.63. 另一种通常采取的可选方法是采用替代法将概率安全评定模式中未明确包含的管段故障与概率安全评定模式中已经包括的基本事件（或基本事件组）关联起来，其故障后果是相同的。在此过程中，需确保管道故障的次生影响在概率安全评定模式中得以考虑。

10.64. 在确定了修订的在役检查计划后，应当使用概率安全评定来确定风险见解，其对与决策标准或导则的对比是必要的，用于评定对在役检查计划所做变更的可接受性。这可通过估算始发事件频率或部件故障概率的特定变化来实现，这些变化可由在役检查计划的变更而引起，或者通过采用这些修正值对概率安全评定重新量化来实现，或者通过开展敏感性研究来实现。在此过程中，应当识别并考虑对概率安全评定在建模细节、范围等方面的相关限制。

风险指引的在役试验

10.65. 当前的在役试验方法要求其实施需遵循法规或标准，这种法规或标准可能包含也可能不包含在规定的管理系统中[36]，该管理系统使用确定性方法来决定需对电厂部件实施的在役试验计划。

10.66. 将风险指引法应用于在役试验的目的是使用概率安全评定提供的风险信息来帮助优化在役试验计划，使其关注于具有最高风险重要度的部件。从电厂运行人员的角度来看，在役试验的风险指引法有可能降低总体维护成本，同时仍保持高水平的安全。

10.67. 将风险指引方法应用于在役试验时，应当使用概率安全评定的结果以及确定性与工程方面的考虑一起来确定待处理部件的风险重要度。概率安全评定的风险信息应当使用 F-V 重要度和伯恩鲍姆（Birnbaum）重要度（或风险成就值）来推得，因为这两种重要度都能提供部件风险重要度方面的见解。

10.68. 应当将风险信息用于识别具有相对高安全重要度的部件，这些部件需要进行严格的在役试验，而具有相对低安全重要度的部件则是不需严格试验的备选。考虑到部件的安全重要度，则可对在役试验计划进行修订。

10.69. 在修改在役试验间隔时，应当使用一级概率安全评定来计算新试验间隔下的堆芯损坏频率，以确定其是否可接受。

分级质量保证[37]

10.70. 适用于核电厂的结构、系统和部件的质量保证计划旨在提供高的置信度，即它们将在正常运行期间及事故后所遇到的工况范围内可靠地执行其安全功能。通常的方法是应用确定性方法和工程判断来识别与安全相关的结构、系统和部件，并对其施以高水平的质量保证。历史上的方法是对电厂内所有与安全相关的结构、系统和部件施以同样高水平的质量保证。

---

[36] 一个示例是参考文献[17]第 OM 节。

[37] 在美国，风险指引质量保证已被风险指引的“特殊处理”要求所取代，该等“特殊处理”要求包括质量保证，但也包括诸如环境鉴定方面的条款。其理由在于，即使变更质量保证要求被证明是可行的，其他特殊处理要求也不允许实施变更。因此，特殊处理要求须作为一个整体来对待。该应用是通过自愿性法规 10 CFR 50.69[18]来说明的。

10.71. 然而，目前已开展的许多概率安全评定的结果表明，某些被归类为安全相关的结构、系统和部件具有相对低的风险重要度，而另一些被归类为非安全相关的结构、系统和部件具有相对高的风险重要度。

10.72. 将分级方法应用于质量保证的目的是考虑是否可以对对某些结构、系统和部件的传统质量保证要求进行修改，使这些要求与结构、系统和部件的风险重要度更加一致。从电厂运行人员的角度来看，这可能会减少实施质量保证计划所需的资源，并且从监管机构的角度来看，它将消除电厂运行人员不必要的负担。

10.73. 应当使用一级概率安全评定来确定结构、系统和部件的风险重要度。风险重要度应当使用 F-V 重要度和伯恩鲍姆（Birnbaum）重要度（或风险成就值）来推得，因为这两种重要度都能提供部件风险重要度方面的见解。此外，风险重要度的推导应当主要在安全功能和安全系统级别上进行，而不是在单一结构、系统或部件级别上（因为对于执行相同安全功能或属于同一安全系统的部件集，质量保证要求应当是相同的）。然而，也可能需要考虑单一部件的重要度。

10.74. 应当将安全分类（由确定性分析和工程判断得到）和风险重要度（由概率安全评定得到）一起用于决定是否应对现有电厂的现行质量保证方面的安排或对新电厂基于传统方法提出的质量保证方面的安排进行变更。

10.75. 应当考虑是否可以对被归类为安全相关但风险重要度相对低的结构、系统和部件减少质量保证方面的安排，以及是否需要对被归类为非安全相关但风险重要度相对高的结构、系统和部件增加质量保证方面的安排。现有的质量保证方面的安排将继续适用于其他结构、系统和部件。

基于概率安全评定的安全能指标

10.76. 基于概率安全评定的安全能指标可用于提供追溯性或当前的电厂安全能指标。这类指标通常包括电厂以往运行的风险剖面、当前风险以及维护大修带来的累积堆芯损坏概率等。许多前述指标可以直接使用风险监控器获得。其他安全能指标也可以通过基于概率安全评定的事件分析得到。

10.77. 应当为电厂开发一套直接使用一级概率安全评定信息的安全能指标，并对其进行监控。

基于概率安全评定的事件分析

10.78. 可使用概率安全评定模式分析运行事件。这在许多国家成为越来越普遍的实践，并形成了运行反馈的常规部分，以补充为确定根本原因等而进行的传统确定性分析。事件分析的目的通常是为了确定可能事件的风险重要度和风险的贡献者，以根据风险重要度对事件做出响应。

10.79. 应对在电厂发生的事件（称“直接事件”）或在其他电厂发生的事件（称“转移事件”）进行基于概率安全评定的事件分析。基于概率安全评定的事件分析应当包括对始发事件（始发事件实际发生的情形以及故障发生的情形，除通过运行人员的快速干预而阻止始发事件的情形）和工况事件（始发事件的可能性增加或响应始发事件所需的安全系统的可用性降低的情形）的分析。

10.80. 应对具有高潜在安全重要度的事件进行基于概率安全评定的事件分析。这需要制定筛选标准，以使用其将具有低安全重要度的事件筛选掉，并根据事件重要度对其进行排序。

10.81. 应当确定电厂的状况、已经发生的故障及在事件期间运行人员的行动并且精确地反映到概率安全评定模式中。应对概率安全评定模式进行重新量化并产生与第 10.80 段所讨论的标准进行比较所需的结果。为进行比较所需的结果通常是始发事件的堆芯损坏工况概率和工况事件的即时堆芯损坏频率。事件分析应当辅以敏感性研究，以提供“如果……会怎样”问题的答案。例如，“如果运行人员未能正确响应事件，那么堆芯损坏工况概率会是多少？”对这些问题的回答应当辅以定性的见解，以了解对事件风险的主要贡献者。

10.82. 应当进行基于概率安全评定的事件分析，以补充确定性分析，允许使用集成模式处理多重故障，并提供运行事件风险重要度的定量指标。基于概率安全评定的事件分析还应用于为可做出哪些改变以减少此类运行事件再次发生的可能性方面的考虑提供输入。

10.83. 应当谨慎使用基于概率安全评定的事件分析结果来确定一座核电厂或核电厂群场址在一段时间内的性能趋势。除非始终使用相同的模式、方法和假设，否则对基于概率安全评定的事件分析此种应用得到的结果可能会是误导性的。

风险指引的规定

10.84. 监管机构可以使概率安全评定提供的见解来决定它们开展活动的方式。这是对监管机构在就核电厂安全问题以及本部分前述概率安全评定应用做出决策时使用概率安全评定的补充。

10.85. 概率安全评定的见解应当用作一个综合的、基于风险指引决策过程的一部分。其目的应当是对监管活动进行排序和优化，以将监管活动的重点放在具有最高风险重要度的方面。还应当通过取消不必要的规定和要求来减少对电厂运行人员的监管负担。

法规的风险指引制定和更新

10.86. 在制定和更新法规和监管导则时，监管机构应当采用风险指引法以考虑到一级概率安全评定提供的风险信息和见解。

10.87. 目的是使用从一级概率安全评定得出的见解，以：

(a) 识别现有法规未涵盖的风险重要领域，以便进一步制定法规；
(b) 确定现有法规或要求的相对风险重要度，以便根据其风险重要度对其进行修订；
(c) 识别法规或要求中不必要或无效的部分，以便予以删除。

监管活动的风险指引排序和优化

10.88. 监管机构开展的活动包括：发放、修改、暂停或撤销授权或许可证，开展监管视察和监督，确保纠正措施得以实施并在必要时采取强制措施。

10.89. 应当将一级概率安全评定提供的风险信息用于对监管机构的活动进行排序和优化。例如，一级概率安全评定提供的风险信息可用于确定开展拟出的下阶段监管视察的优先顺序。目的是确保将视察集中在具有高风险重要度的电厂设计和运行方面，并在具有低风险重要度的方面减少或不进行视察。

参 考 文 献

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

[2] 国际原子能机构《核电厂安全：设计》，国际原子能机构《安全标准丛书》第 NS-R-1 号，国际原子能机构，维也纳（2000 年）。

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

[4] 国际核安全咨询组《核电厂基本安全原理》第 75-INSAG-3（Rev.1）号,《国际核安全咨询组丛书》第 12 号，国际原子能机构，维也纳（1999 年）。

[5] 国际原子能机构《核安全公约》，《法律丛书》第 16 号，国际原子能机构，维也纳（1994 年）。

[6] 国际原子能机构《概率安全评定和概率安全标准在核电厂安全中的作用》，《安全丛书》第 106 号，国际原子能机构，维也纳（1992 年）。

[7] 国际原子能机构《设施和活动管理系统》，国际原子能机构《安全标准丛书》第 GS-R-3 号，国际原子能机构，维也纳（2006 年）。

[8] 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）。

[9] 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）。

[10] 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）。

[11] 国际原子能机构《核电厂运行中的消防安全》，国际原子能机构《安全标准丛书》第 NS-G-2.1 号，国际原子能机构，维也纳（2000 年）。

[12] 美国核管制委员会《美国核电厂外部危害评价》，第 NUREG/CR-5042 号报告附录 2，核管制委员会，华盛顿特区（1989 年）。

[13] 国际原子能机构《现有核装置地震安全评价》，国际原子能机构《安全标准丛书》第 NS-G-2.13 号，国际原子能机构，维也纳（2009 年）。

[14] 国际原子能机构《核电厂概率安全评定（PSA）的应用》，国际原子能机构《技术文件》第 1200 号，国际原子能机构，维也纳（2001 年）。

[15] 国际原子能机构《核电厂应用概率安全评定（PSA）质量的确定》，国际原子能机构《技术文件》第 1511 号，国际原子能机构，维也纳（2006 年）。

[16] 国际原子能机构、经济合作与发展组织核能机构《WGGRisk 风险评定工具：最先进的技术在核电厂的制定和实施情况》,NEA/CSNI/R（2004）20，经济合作与发展组织，巴黎（2004 年）。

[17] 美国机械工程师学会《锅炉和压力容器规范》（2007 年版），美国机械工程师学会，纽约（2007 年）。

[18] 美国核管制委员会《核反应堆结构和部件的风险信息分类和处理》，联邦法规第 10 篇第 50.69 部分，美国政府出版办公室，华盛顿特区（2004 年）。

附件 I

内部和外部危害的通用清单示例

序号	危害	危害的定义与影响	接口和备注
基于大气的自然灾害			
A1	强风	危害是根据强风对电厂造成的损坏来定义的。它包括由风压所致的直接损坏和风载飞射物所致的间接损坏。	由于其独特特征，此危害不包括龙卷风（A2）。其也不包括雪暴（包括在 A7 中），盐暴（A12）或沙暴（A13）的差异化影响。但是，包括这些危害中风的影响。风暴潮的影响由高水位危害（W3）涵盖。
A2	龙卷风	危害是根据龙卷风对电厂造成的损坏来定义的。由于该危害在持续时间、风速和发生频率方面的特殊特征，将其与其他强风区分开。	
A3	高气温	危害是根据高气温对电厂的损坏来定义的。	高水温对电厂影响被单独处理（W4）。
A4	低气温	危害是根据低气温对电厂的损坏来定义的	低水温（W4）或冰（W7、W8、W9）对电厂的影响被单独处理。
A5	极端气压（高/低梯度）	危害是根据高压或低气压或快速压力变化对电厂的损坏来定义的。	
A6	极端降雨	危害是根据极端降雨对电厂造成的损坏来定义的。	它包括由于结构上的降雨负载和由于降雨引起的水灾所造成的损坏。
A7	极端降雪（包括暴风雪）	危害是根据极端降雪（包括暴风雪）对电厂造成的损坏来定义的。	暴风雪引起的风力影响由强风危害（A1）涵盖。由于雪的融化导致的水灾效应被认为由极端降雨引起的水灾效应（A6）涵盖。

序号	危害	危害的定义与影响	接口和备注
A8	极端冰雹	危害是根据极端冰雹对电厂造成的损坏来定义的。它包括由构筑物上的冰雹负载所致的损坏。	由冰雹融化引起的水灾效应受极端降雨引起的水灾效应（A6）涵盖。对最终热阱的任何可能影响都被认为由冰害（W7、W8、W9）涵盖。
A9	雾	危害是根据雾对电厂造成的损坏来定义的。	
A10	白霜	危害是根据白霜对电厂的损坏来定义的。	
A11	干旱	危害被定义为一个延续性干旱期，其使得湖泊、河流和开放水域的水位下降。	由高气温（A3）或高水温（W4）引起的对电厂的可能影响是通过对这些事件的分析来涵盖的。认为其对水位（热阱）没有影响。
A12	盐暴	危害被定义为涉及对电厂结构盐覆盖的风暴。	来自盐暴的风力影响由强风危害（A1）涵盖。
A13	沙暴	危害是根据沙暴所载的沙对电厂造成的影响来定义的。	来自沙暴的风力影响由强风危害（A1）涵盖。
A14	闪电	危害是根据闪电对电厂造成的损坏来定义的，影响可能是直接的，导致结构损坏或与场外电源丧失相关的危害，或间接的，通过闪电引发的电磁馈电火灾。	闪电引发的火灾由外部火灾（G7）和内部火灾分析涵盖。
A15	陨石	危害是根据陨石撞击对电厂造成的损坏来定义的。	
地面自然灾害			
G1	地壳上升	危害是根据地壳上升对电厂造成的损坏来定义的。	
G2	土壤霜冻	危害根据土壤霜冻对电厂造成的损坏来定义的。	
G3	动物	危害是根据动物对电厂造成的损坏来定义的。	W10 涵盖了鱼类、贻贝等对进水口水的影响。

序号	危害	危害的定义与影响	接口和备注
G4	火山现象	危害是根据火山爆发对电厂造成的损坏来定义的。	
G5	雪崩	危害是根据雪崩对电厂造成的损坏来定义的。	
G6	水上滑坡	危害是根据水上滑坡对电厂造成的损坏来定义的。	
G7	外部火灾	危害是根据来自场外、场取内部或外部的火灾对电厂造成的影响来定义的。	从场址另一电厂蔓延来的内部火灾将单独处理（M15）。作为其他外部危害的次生影响而产生的火灾被视为这些危害的一部分（M2、M11、M20）。内部火灾作为内部危害概率安全评定的一部分进行分析。
G8	地震危害	危害是根据地震对电厂造成的影响来定义的。	
G9	岩溶	危害是根据由于侵蚀引起的裂缝，落水洞，地下伏流和洞穴对电厂造成的损坏来定义的。	
基于水的自然灾害			
W1	强水流（水下侵蚀）	危害是根据强水流对电厂结构造成的损坏来定义的。	水下滑坡的影响单独处理（W6）。
W2	低水位	危害是根据低水位对电厂造成的损坏来定义的。	由于地面上升导致的水位下降由 G1 涵盖。
W3	高水位	危害根据高水位对电厂造成的损坏来定义的。高水位可能是由于风暴潮、波浪或假潮。高水位也受潮汐变化的影响。	
W4	高水温	危害是根据高水温对电厂造成的影响来定义的。	高气温对电厂带来的影响单独处理（A3）。
W5	低水温	危害是根据低水温对电厂造成的影响来定义的。	低气温（A4）或冰的影响（W7、W8、W9）对电厂带来的影响单独处理。

序号	危害	危害的定义与影响	接口和备注
W6	水下滑坡	危害是根据水下滑坡对电厂造成的影响来定义的。	水下滑坡可能是由于水面上的原因造成的，例如长时间的强降水。水下侵蚀对电厂的影响被视为强水流危害（W1）的一部分。
W7	表面冰	危害是根据表面厚冰对电厂造成的影响来定义的。	危害不包括由冰层（W8）和冰障（W9）造成的影响。
W8	水内冰	危害是根据冷却水进水口中的冰对电厂的影响来定义的。	
W9	冰障	危害是根据冰障对电厂造成的影响来定义的。	
W10	水中的有机物	危害是根据指进水口水中的有机物对电厂造成的影响来定义的。有机物可能是藻类、海藻、鱼类、贻贝、海蜇等。	
W11	腐蚀（来自盐水）	危害是根据腐蚀对电厂造成的影响来定义的。	
W12	来自船舶排放的固态或液态（非气态）杂质	危害根据从船上排放到水中的固态或液态（非气态）杂质对电厂造成的影响来定义的。	
W13	化学物质排放到水中	危害是根据化学物质向水中的排放对电厂造成的影响来定义的。重点是降低水质。这些排放可能是由于船舶事故造成的，但也可能源自陆地。	危害不包括排放的固态或液态（非气态）杂质（W12）而产生的影响。
W14	海啸	危害是根据高水位和波浪的压力对电厂造成的损坏来定义的。	
场外事故			
M1	船舶碰撞造成的直接影响	危害是根据船舶的直接影响来定义的。	危害不包括与船舶事故（爆炸、污染、进口堵塞或有毒气体排放）相关的排放后

序号	危害	危害的定义与影响	接口和备注
			果，因为这些危害（M2、M3、W12、W13）是单独处理的。
M2	运输事故后的爆炸	危害是根据场外地面运输事故或海上、湖泊或河流运输事故之后引起的爆炸对电厂造成的损坏来定义的。损坏可能是由于压力冲击或来自飞射物撞击。	危害不包括由飞机坠毁（M20）或源于管道事故（M5）造成的损坏。M3 涵盖了化学排放产生的毒性损坏。
M3	运输事故后化学品排放	危害是根据场外地面运输事故或由于海上、湖泊或河流运输事故后引起的化学物质排放对电厂造成的毒性损坏来定义的。	运输事故的爆炸效应由 M2 涵盖。
M4	场外爆炸	危害是根据由于场外固态物质或气体云的爆炸（爆燃或爆炸）对电厂造成的损坏来定义的。 损坏可能是由于压力冲击或飞射物撞击。	危害不包括与场外的运输事故（M2）或源自管道（M5）相关的爆炸。M6 涵盖了化学排放产生的毒性损坏。
M5	管道事故后的爆炸	危害是根据管道事故后爆炸（爆燃或爆炸）对电厂造成的的损坏来定义的。损坏可能是由于压力冲击或飞射物撞击。	M7 涵盖了化学排放产生的毒性损坏。M4 和 M11 涵盖了在场外或场址内的爆炸效应。在 M3 和 M7 中分析了运输或管道事故后的毒性损坏。
M6	场外的化学排放	危害是根据场外的化学排放对电厂的毒性损坏来定义的。这些排放可能源自电厂外的工业过程事故或源自电厂外贮存物质的泄漏。	
M7	管道事故后的化学排放	危害是根据管道事故后化学排放对电厂的毒性损坏来定义的。	管道事故的爆炸效应由 M5 涵盖。
M8	来自军事活动的飞射物	危害是根据来自军事活动的飞射物对电厂造成的影响来定义的。	对供电和热阱的影响假设由其他危害所涵盖。

序号	危害	危害的定义与影响	接口和备注
M9	挖掘工作	危害是根据在场址区域内、外的挖掘工作对电厂造成的影响来定义的。	
现场事故			
M10	在场址内的重型运输的直接影响	危害是根据场址内但在厂房外的重型运输对电厂造成的直接影响来定义的。这也包括安全壳外部维护平台的运输。	电厂厂房内的重型运输作为内部危害概率安全评定的一部分进行分析。
M11	场内爆炸	危害是根据场内但在厂房外的固态物质或气体云爆炸（爆燃或爆炸）对电厂造成的损坏来定义的，损坏可能是由于压力冲击或飞射物撞击。	电厂厂房内的爆炸作为内部危害概率安全评定的一部分进行分析。
M12	场址内管道事故后的爆炸	危害是根据现场管道破裂后爆炸（爆燃或爆炸）对电厂造成的损坏来定义的。损坏可能是由于压力冲击或飞射物撞击。	
M13	电厂内的化学排放	危害是根据场内化学排放对电厂造成的毒性损坏来定义的。	这些排放可能源自电厂内的工业过程事故，也可能源自贮存在电厂内但在厂房外的物质的泄漏。贮存在厂房内物质的化学排放作为内部危害概率安全评定的一部分进行分析。
M14	场内管道事故后的化学排放	危害根据场内管道事故后的化学排放对电厂造成的毒性损坏来定义的。	
M15	蔓延自厂场址其他机组的内部火灾	危害是根据源自现场另一机组的火灾对电厂造成的影响来定义的。	外部火灾单独处理（G7）。作为其他外部危害的次生效应而产生的火灾被视为这些危害（M2、M11、M20）的一部分。
M16	来自场址其他机组	危害是根据另一机组产生的飞射物对电厂造成的损	

序号	危害	危害的定义与影响	接口和备注
	的飞射物	坏来定义的。	
M17	蔓延自场址其他机组的水灾和恶劣环境	危害是根据来自它机组的水灾蔓延对电厂造成的损坏来定义的。	
M18	场址区域内的挖掘工作	危害是根据电厂区域内的挖掘工作对电厂造成的影响来定义的。	
飞行器坠毁			
M19	卫星坠毁	危害是根据卫星坠毁对电厂造成的损坏来定义的。	
M20	飞机坠毁	危害是根据场址区域内的飞机坠毁对电厂结构造成的损坏来定义的。飞机可能是商用的、私人的或军用的。	
其他人因引发危害			
M21	磁干扰	危害是根据人因引发的磁场或电场对电厂造成的影响来定义的。此类场的主要归因示例包括雷达、无线电和移动电话。	
M22	电厂上游的大坝决堤	危害是根据高水位和水波对电厂厂房、系统和部件造成的损坏来定义的。	

备注：该危害清单是基于脚注参考文献 [1] 中给出的危害清单。源自电厂厂房内的内部危害不包括在表中。

[1] KNOCHENHAUER, M., LOUKO,P., “外部事件分析导则”，第 SKI-R-02/27-SE 号报告，SKI，斯德哥尔摩，2003 年 2 月。

附件 II

火灾传播事件树和地震事件树示例

事件树方法在火灾缓解和传播分析中的应用

II-1. 图 II-1 所示的火灾传播事件树的示例包括从火灾始发开始的相关特点。因与火灾控制和扑灭的概率不同相关，火灾探测的早和晚是有区别的。火灾的传播则与房间是否关闭以及关闭的程度相关。深入建模时应当考虑可用的消防设备，也应当考虑到消防手段对安全相关的物项造成的可能损坏。图 II-1 提供了如何使用事件树方法来分析火灾的缓解和传播的说明。

事件树方法在识别地震诱发始发事件中的应用

II-2. 图 II-2 展示了如何使用事件树方法对地震诱发始发事件的不同后果进行建模，在这个示例中，假设地震始发事件总是导致场外电源的丧失。

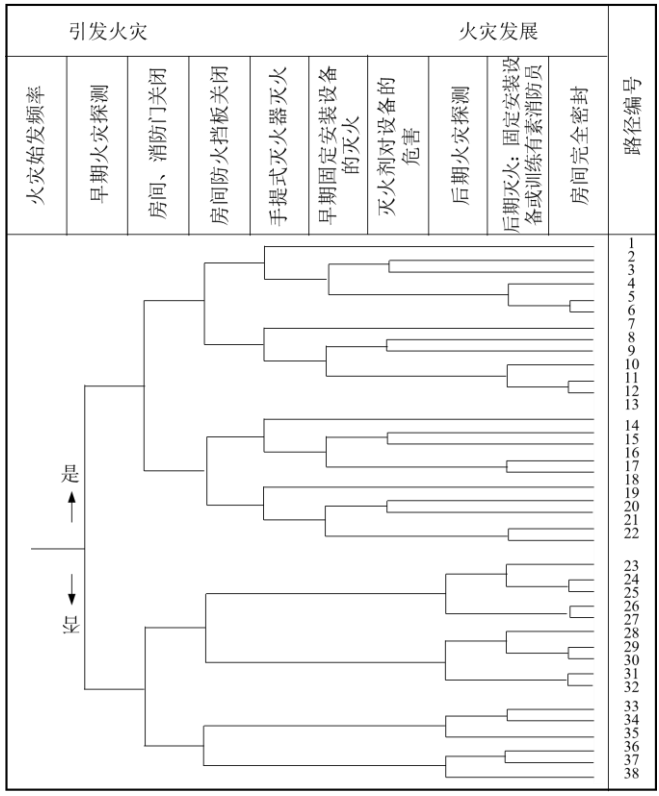

图 II-1. 火灾传播事件树示例

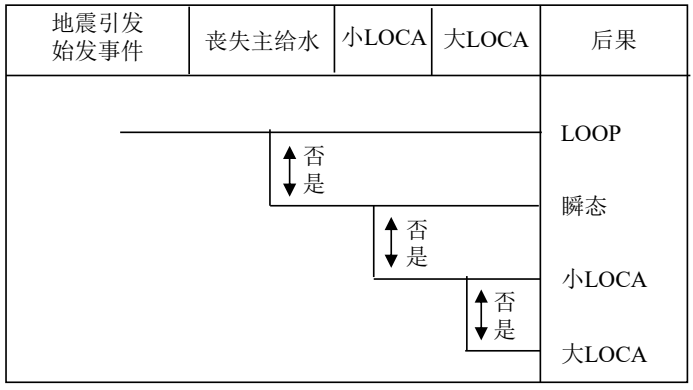

图 II-2. 用于地震诱发始发事件建模的事件树示例

LOCA：冷却剂丧失事故

附件 III

低功率和停堆模式概率安全评定的支持信息

电厂运行状态和相关始发事件示例

III-1. 在德国沸水堆型 SWR69 的概率安全评定框架中，对低功率和停堆模式进行了概率评价[III-1]。参考文献[III-2]提供了压水堆的示例。

III-2. 在参考文献[III-1]的基础上，提供了如何规定电厂运行状态以及如何将始发事件与电厂运行状态相关联的信息。为了描述系统相关状态和物理状态的变化，将停堆纳入电厂运行状态（见图 III-1 和表 III-1）。设备运行状态的选择应当使得系统可用性和物理状态尽可能恒定。通常，在停堆期间（状态 III-1－III-7），应急电源的两个电气冗余之一、余热排出系统的四个通道中的两个以及应急备用系统的两个通道之一是可用的。在状态 III-4 中，需执行其大部分的维护工作，反应堆厂房地坑的泄漏返回系统也应当是可用的。

III-3. 对德国的运行经验进行了详细评价，以发现在低功率和停堆模式下，可能导致始发事件或影响事故控制的事件。除了评价德国的运行经验外，还评价了国际上低功率和停堆模式概率安全评定的结果[III-3、III-4]。

III-4. 提供概率安全评定指导的德国文件，被用作识别始发事件（III-5－III-7）的基础。

III-5. 识别始发事件并将事件匹配到相应的电厂运行状态就得到表 III-2 所示的矩阵，在此电厂运行状态中，该事件可能发生。在表 III-2 标记有“X”，表明始发事件可以发生在该电厂运行状态。正如在第 9.11 段指出的，被纳入的终态须根据国家风险标准来决定。

III-6. 作为一个示例，参考文献[III-2]提供了压水堆型电厂的相应信息，并在表 III-3 和表 III-4 进行了总结。表 III-3 给出了需区分的电厂运行状态。基于对国家和国际运行经验的分析，表 III-4 呈现了不同电厂运行状态中应当考虑的始发事件。

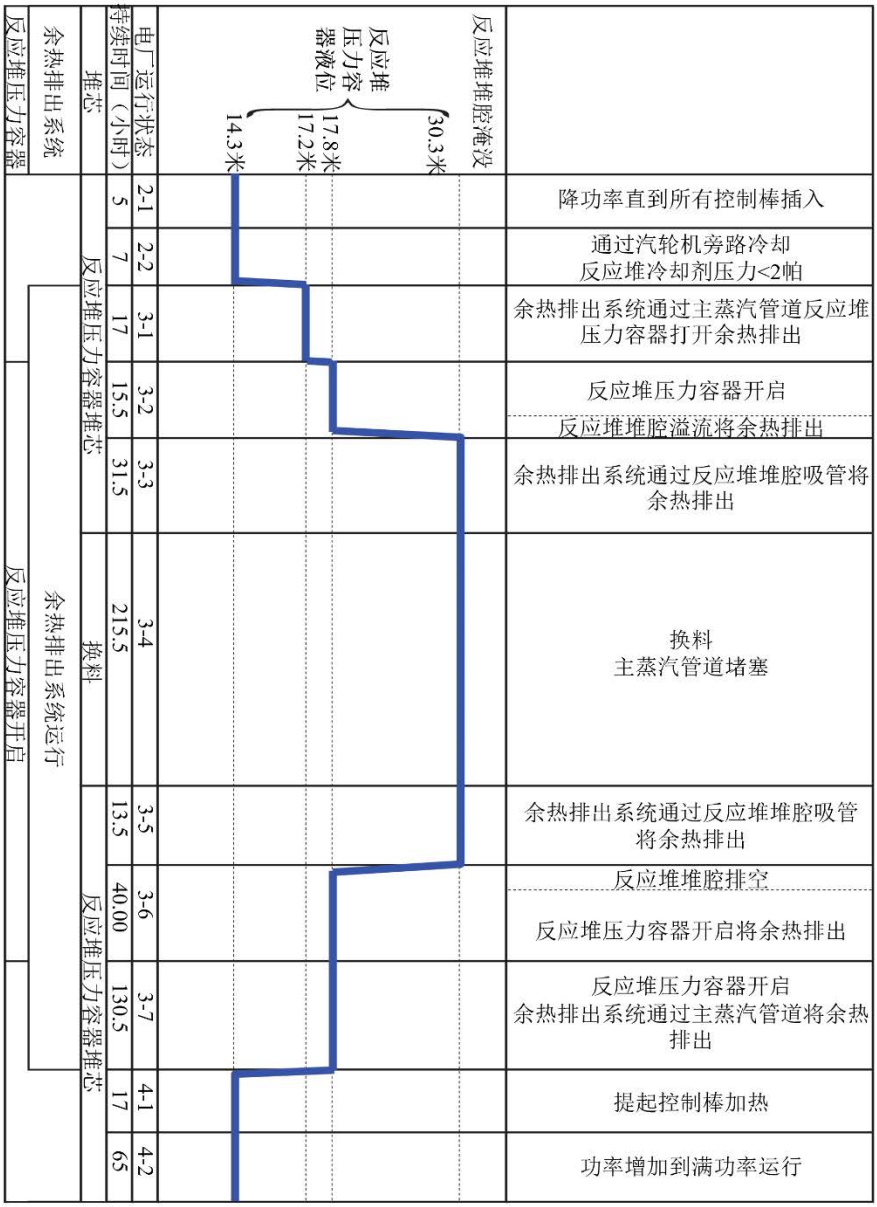

图 III-1.　大修期间反应堆冷却水平。

表 III-1. 参考电厂停堆期间的电厂运行状态

	电厂运行状态	电厂运行状态的表征
停堆	2-1	降功率，直到插入所有控制棒。
	2-2	通过汽轮机旁路冷却到反应堆冷却剂压力<2 巴，关闭主蒸汽隔离阀，通过从余热排出系统注入提高反应堆水位至主蒸汽管线以上。
大修	3-1	带余热排出系统、通过主蒸汽管线的余热排出，反应堆压力容器关闭，反应堆冷却剂温度 130－50℃。
	3-2	带余热排出系统、通过主蒸汽管线的余热排出，反应堆压力容器打开，反应堆冷却剂温度<40℃，反应堆堆腔密封衬垫的安装，反应堆堆腔的淹没。
	3-3	反应堆堆腔淹没，通过反应堆堆腔吸入管线利用余热排出系统进行余热排出，打开换料舱口，在主蒸汽管线中插入塞子。
	3-4	装料，通过反应堆堆腔吸入管线利用余热排出系统进行余热排出。
	3-5	主蒸汽管线中塞子的去除，换料舱口的关闭，通过反应堆堆腔吸入管线利用余热排出系统排出余热。
	3-6	排空反应堆堆腔，带余热排出系统、通过主蒸汽管线的余热排出，拆除反应堆堆腔密封衬垫。
	3-7	反应堆压力容器关闭，带余热排出系统、通过主蒸汽管线的余热排出。
重新启动	4-1	余热排出系统的关闭，反应堆液位下降至主蒸汽管线以下，控制棒提棒以加热。
	4-2	汽轮机旁路运行，汽轮发电机运行，并网，功率增加至满功率运行。

表 III-2. 参考电厂停堆期间的始发事件（分别指关键安全功能的丧失或触发始发事件的机制）

始发事件		电厂运行状态										
		触发停堆		停堆							重新启动	
		2-1	2-2	3-1	3-2	3-3	3-4	3-5	3-6	3-7	4-1	4-2
瞬态												
T1	主热阱丧失	X	X									X
T2	优先电源丧失	X	X	X	X	X	X	X	X	X	X	X
T3	主给水丧失	X	X									X
T4	主给水和主热阱丧失	X	X									X
T5	关闭一台安全阀失败	X	X								X	X
T6	抑制池泄漏		X		X							
T7	通过主给水系统的反应堆压力容器给水过多	X	X									X
T8	通过余热排出系统的反应堆压力容器给水过多		X									
T9	余热排出丧失			X	X	X	X	X	X	X		
T10	乏燃料水池冷却丧失	X	X	X	X	X	X	X	X	X	X	X
TA	预计无停堆瞬态	X									X	X

表 III-2. 参考电厂停堆期间的始发事件（分别指关键安全功能的丧失或触发始发事件的机制）（续）

始发事件		电厂运行状态										
		触发停堆		停堆							重新启动	
		2-1	II-2	3-1	3-2	3-3	3-4	3-5	3-6	3-7	4-1	4-2
冷却剂丧失事故												
S1	反应堆压力容器安全壳内泄漏											
S1.1	由于管道破裂：											
S1.1.1	堆芯之上（A 管嘴）					X	X	X				
S1.1.2	堆芯之下（L 管嘴）					X	X	X				
S1.2	在以下过程中的人因错误:											
S1.2.1	主蒸汽管线阀门检验						X					
S1.2.2	堆芯喷雾和主补水系统中阀门的检验						X					
S1.2.3	抽拔循环泵泵轴						X					
S1.2.4	控制棒驱动的检验						X					
S1.2.5	更换堆芯中子通量探测器						X					
S2	余热排出系统的泄漏			X	X	X	X	X	X	X		
S3	反应堆腔密封衬套泄漏				X	X	X	X	X			

表 III-2. 参考电厂停堆期间的始发事件（分别指关键安全功能的丧失或触发始发事件的机制）（续）

始发事件		电厂运行状态										
		触发停堆		停堆							重新启动	
		2-1	2-2	3-1	3-2	3-3	3-4	3-5	3-6	3-7	4-1	4-2
S4	泄漏入相连系统											
S4.1	反应堆压力容器水位控制失效			X	X				X	X		
S4.2	在余热排出过程中安全阀的开启			X	X	X		X	X	X		
S4.3	余热排出热交换器的泄漏			X	X	X	X	X	X	X		
S5	乏燃料水池泄漏			X	X	X	X	X	X	X		
火灾与内部水淹												
B1	安全壳内的火灾	X	X	X	X	X	X	X	X	X	X	X
B2	安全壳外的火灾	X	X	X	X	X	X	X	X	X	X	X
IF	内部水淹			X	X	X	X	X	X	X		
临界事故												
K1	控制棒的错误提棒						X					
K2	控制棒的错误去除						X					
K3	燃料装载错误						X					
重物坠落												
H1	燃料元件的跌落						X					
H2	重物坠落			X	X	X	X	X	X	X		

表 III-3. 参考压水堆核电厂停堆两周的电厂运行状态

编号	物理状态/系统特点的变化
(1)A0	降功率至次临界热态/反应堆保护信号和安全系统的可用性与功率运行期间相同。
(1)A1	通过蒸汽发生器停运至一回路系统压力 3.1 兆帕和一回路系统温度 120℃/所有反应堆保护系统仍然可用。
(1)B1	一回路系统冷却至卸压冷态/在 120℃时启动余热排出系统，安注水箱和高压泵断开。
(1)B2	水位降至中间环路，中间环路运行/堆芯在反应堆压力容器内，一回路系统压力密闭。
(1)C	打开反应堆压力容器顶盖，半管水位运行/堆芯在反应堆压力容器内，一回路系统处于卸压状态，在乏燃料转运舱与和换料水池之间的通道处于关闭状态。
(1)D	反应堆堆腔淹没，卸出燃料元件/堆芯全部或部分在反应堆压力容器内，换料舱口打开。
E	反应堆堆腔和反应堆压力容器排空/堆芯完全卸载，换料舱口关闭，在下边缘环路水位开展工作。
(2)D	反应堆堆腔再充水，燃料元件装载/堆芯全部或部分在反应堆压力容器内，换料舱口打开。
(2)C	液位下降到中间环路，关闭反应堆压力容器盖/堆芯在反应堆压力容器内，一回路系统非压力密闭，换料舱口关闭。
(2)B2	一回路系统排气和再充水/堆芯在反应堆压力容器内，一回路系统压力密闭。
(2)B1	利用主泵加热一回路系统/所有反应堆保护系统可用。
(2)A1	冷却剂硼稀释并使反应堆达到临界状态/控制棒提棒和/或硼稀释。
(2)A0	功率增加到指定水平/反应堆保护信号和安全系统的可用性与功率运行期间相同。

注：(1) 表示停堆期间的电厂运行状态；(2) 表示重新启动期间的电厂运行状态。

表 III-4. 压水堆低功率和停堆模式期间的始发事件（分别指关键安全功能的丧失或触发始发事件的机制）

	电厂运行状态												
始发事件	A0	A1	B1	B2	C	D	E	D	C	B2	B1	A1	A0
瞬态	反应堆压力容器关闭				反应堆压力容器开启					反应堆压力容器关闭			
优先级电源的丧失－外部	X	X	X	X	X	X	X	X	X	X	X	X	X
优先级电源的丧失－内部						X	X	X					
主给水丧失但主供热未丧失	X	X										X	X
主热阱丧失但主给水未丧失	X	X										X	X
主给水和主热阱丧失	X	X										X	X
安全壳外主蒸汽管线泄漏	X	X										X	X
安全壳内主蒸汽管线泄漏	X	X										X	X
汽轮机厂房内主给水管线泄漏	X	X										X	X
安全壳内给水管线泄漏，不可隔离	X	X										X	X
由于以下原因导致的余热排出的丧失：													
— 降低水位的故障				X					X				
— 余热排出通道的运行故障			X	X	X	X		X	X	X			
应急堆芯冷却系统信号的意外激活				X									

表 III-4. 压水堆低功率和停堆模式期间的始发事件（分别指关键安全功能的丧失或触发始发事件的机制）（续）

	电厂运行状态												
始发事件	A0	A1	B1	B2	C	D	E	D	C	B2	B1	A1	A0
冷却剂丧失事故	反应堆压力容器关闭				反应堆压力容器开启					反应堆压力容器关闭			
一回路系统小泄漏 A＜25 平方厘米	X	X	X								X	X	X
一回路系统小泄漏 25 平方厘米 ＜A＜200 平方厘米	X	X	X								X	X	X
意外开启稳压器安全阀	X	X	X								X	X	X
一回路系统中泄漏 200 平方厘米＜A＜500 平方厘米	X	X	X								X	X	X
一回路系统大泄漏 A＞500 平方厘米	X	X	X								X	X	X
由于维护故障使 P－bdV[a] 打开		X	X	X						X	X	X	
丧失场外电源情况下不小心打开 P－bdV	X	X	X								X	X	X
汽轮机停堆后不小心打开 P－bdV	X	X	X								X	X	X
蒸汽发生器传热管泄漏	X	X	X								X	X	X
安全壳内余热排出系统泄漏			X	X	X	X	X	X	X	X			
环堆腔内余热排出系统的泄漏			X	X	X	X	X	X	X	X			
容积控制系统泄漏	X	X	X	X	X	X	X	X	X	X	X	X	X
反应堆堆腔/沉降池泄漏						X		X					
泄漏入相连系统			X	X	X	X	X	X	X	X			

表 III-4. 压水堆低功率和停堆模式期间的始发事件（分别指关键安全功能的丧失或触发始发事件的机制）（续）

	电厂运行状态												
始发事件	A0	A1	B1	B2	C	D	E	D	C	B2	B1	A1	A0
意外硼稀释	反应堆压力容器关闭				反应堆压力容器开启					反应堆压力容器关闭			
来自非含硼水系统的泄漏													
—蒸汽发生器传热管泄漏			X	X	X	X	X	X	X	X	X		
—余热排出热交换器的泄漏			X	X	X	X	X	X	X	X	X		
—轴承密封泄漏			X	X	X	X	X	X	X	X	X		
—因疏忽的一回路系统注入			X	X	X	X	X	X	X	X	X		
因疏忽的余热排出系统中的非含硼水			X	X	X	X	X	X	X	X	X		
去污工作期间的硼稀释									X				
提升水位过程中的硼稀释										X			
停堆加硼故障		X											
在所有主冷却剂泵丧失后停堆因疏忽而致的硼稀释												X	

[a] P－bdV 表示稳压器排污阀。

特定系统建模要求的示例

III-7. 参考文献[III-8]是下述 III-8－III-10 中所给示例的主要和几乎是唯一来源。

III-8. 特定系统可能需要针对低功率和停堆工况进行专门建模。例如，燃料水池冷却系统可能不包括在满功率运行工况的分析中，但在停堆工况中则可能是重要的。余热排出系统的某些运行模式也可能仅在停堆期间使用，因此需要考虑这些模式。系统模式须反映运行模式和特定的系统配置。成功标准，例如，要求特定系统通道的 n 中取 k，对于低功率或停堆工况可能不那么严格，因为衰变热水平较低。需要进行详细的热工水力计算来确定这些标准。系统的自动启动特征可在低功率或停堆工况下被旁路以防止意外启动。例如，可解除安全注入系统的自动启动模式以防止停堆期间的驱动。因此，需改变这些系统故障树中的控制逻辑，以反映如果需要须手动启动系统的事实。也需要为相关的人机交互开发模式。

III-9. 在停堆期间，由于作为停堆的一部分正在进行的活动，可能无法进行满功率运行工况分析中所考虑的手动恢复操作。例如，在满功率运行期间，低压系统的交叉连接可能是适当的行动。然而，在停堆期间，交叉连接可能被锁定关闭，或者一个系统通道可能被完全禁用。因此，如果在满功率运行的故障树中包括这种类型的行动，则需要对它们进行修改，以便进行低功率和停堆评价。总而言之，对于从满功率运行工况概率安全评定中修改而得的停堆模式概率安全评定的每个故障树，需针对每一电厂运行状态进行评审，以确定是否有该电厂运行状态的任何特点可能对故障树结构的逻辑产生影响。

III-10. 停堆期间各种系统的可用性变化增加了系统建模任务的复杂性。某些系统或部分系统在某些电厂运行状态下可能不可用。此外，由基本事件表示的部件故障的概率可能改变。大多数概率安全评定软件包是基于“快速割集算法”的，它生成并存储最小割集的方程。最小割集的分析可以在多个级别上进行：一个特定故障树门、单一事件树序列或某一特定后果（每个事件树序列可以被指派一个或多个后果，例如，一个电厂损坏状态）。分析案例可以规定一个“边界条件集”，其中包括一个需要应用到模式的数值规范或变化的清单。边界条件集可包括逻辑开关的真/假设置、基本事件和故障树门的概率设置、基本事件和故障树门的真/假状态的设置以及参数值的设置。这对于根据电厂运行状态具有不同变化的相同基本模式进行分析非常有用。当然，也可以不使用逻辑开关来进行分析，但是对于每个边界条件集，就需将不同的单一故障树模式添加到停堆模式的完整的概率安全评定模式中，这使得建模和评审所需的工作复杂化，因为需要考虑的不同故障树模式的个数如果需要做修改时尤其如此。

用于识别与低功率和停堆模式概率安全评定相关的始发事件前人员行动的方法

III-11. 由于详细分析人员在低功率和停堆期间可能采取的所有措施根本是不可行的，因此对预启动器行动进行有效筛选的步骤是必不可少的。这一步骤的结果将是一个行动清单，其指明哪些行动定性评价就已足够，哪些行动需要作出估计以及哪些行动需要进行详细的定量分析。参考文献[III-6]概述了第 III-12－III-18 段所描述的方法。

III-12. 筛选方法的基础是关于标准停堆计划的主要步骤和任务的电厂特定清单。显然，该清单与低功率和停堆模式概率安全评定所选择的电厂运行状态之间存在密切关系。对于沸水堆，它通常包括 30 个步骤或任务。在参考文献[III-6]，给出了以下主要步骤和任务清单的示例：

— 实施降功率；
— 启动与电厂停堆和系统隔离相关的试验；
— 发电机与电网解列；
— 继续降功率直至余热排出启动；
— 为燃料转运打开安全壳；
— 打开反应堆压力容器；
— 为反应堆堆腔的淹没安装补偿器；
— 开始淹没；
— 开展反应堆压力容器活动；
— 除去蒸汽干燥器；
— 布置插头和插板；
— 在冗余通道方面的工作；
— 在部件和系统方面的工作；
— 开展啜漏试验；
— 更换燃料元件；
— 拆卸和重新安装给水分配器；
— 拆卸插头和插板；
— 安装蒸汽干燥器；

— 排空被水淹没的堆腔；
— 拆除补偿器；
— 关闭反应堆压力容器；
— 关闭安全壳；
— 进行与启动相关的试验；
— 提升功率；
— 同步发电机到电网的连接；
— 提升至满功率。

III-13. 对于该清单的各组成部分，开展对工作环境和任务的经验评价，包括电厂巡视，以识别潜在的人因错误和后果。从而判断每个潜在错误的重要度。在确定可能的后果时，一方面区分部件或系统部分的不可用性，另一方面区分始发事件。

III-14. 在第一种情况下，应当评定如何探测故障，对于哪些时间间隔期间将导致不可用或潜在故障，以及对于哪些始发事件这些不可用或潜在故障会变明显。最后，描述可能的应对措施和后果。

III-15. 在第二种情况下，应对始发事件进行分类（例如冷却剂丧失事故）。再次，描述可能的应对措施和后果。

III-16. 筛选分析的重要目的之一是以透明和系统的方式，制定一个包括全部筛选结果的表格。其中包括与潜在错误或后果相关的运行经验。

III-17. 如果认为有必要进行详细分析，则可使用第 5 部分中描述的人的可靠性分析方法进行。

III-18. 作为中间情况，对于类似性质的始发事件组（例如，泄漏位置在堆芯上方的冷却剂丧失事故），对整体故障概率进行粗略估计可能就已足够。

作为沸水堆核电厂低功率和停堆模式概率安全评定结果的停堆风险剖面的示例

III-19. 在参考文献[III-9]，针对沸水堆电厂给出了低功率和停堆模式概率安全评定的结果。规定了 6 种电厂运行状态（图 III-2 和 III-3 中的“POS”）：

(1) 电厂运行状态 1：功率运行和启动（压力从额定工况（71 公斤/平方厘米）到 35 公斤/平方厘米，热功率不大于 15%）；

(2) 电厂运行状态 2：启动和热停堆（压力从 35 公斤/平方厘米到 10 公斤/平方厘米）；

(3) 电厂运行状态 3：热停堆（压力低于 10 公斤/平方厘米，温度高于 93℃）；

(4) 电厂运行状态 4：冷停堆（温度低于 93℃），直到容器盖被移除；

(5) 电厂运行状态 5：换料（容器盖被移除且水位升高至蒸汽管线）；

(6) 电厂运行状态 6：换料（容器盖被移除、水位升高至乏燃料水池且换料传输管打开。

III-20. 在图 III-2 中，对于电厂运行状态 1—4，一回路中的热功率和压力将作为时间的函数予以显示。在图 III-3 中，对于电厂运行状态 1—4，显示了风险剖面。显然，与其他电厂运行状态的风险相比，在电厂运行状态 4 的风险最高。该示例强调了风险剖面所提供的见解，从而有助于分配安全改进的努力方向。

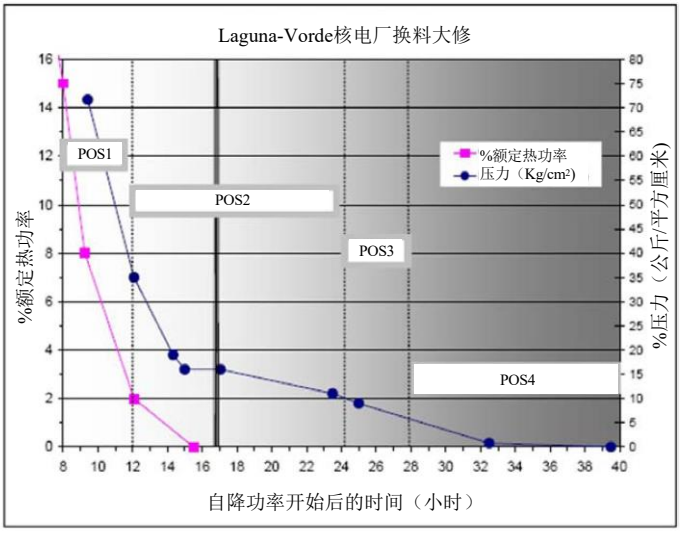

图 III-2. Laguna-Vorde 核电厂低功率和停堆模式电厂运行状态的概率安全评定。
POS：电厂运行状态。

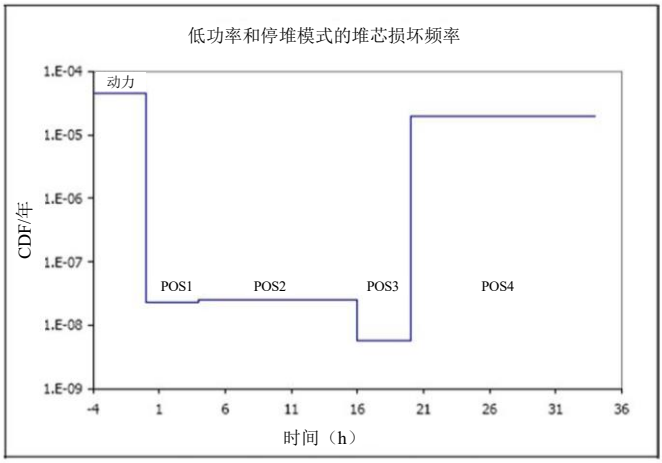

图 III-3. 每年对满功率状态与低功率和停堆模式的堆芯损坏频率概率安全评定的比较。POS：电厂运行状态。

附录 III 参考文献

[III-1] BABST, S.，等，“德国 SWR 69 型反应堆停堆概率安全评定的观察与结果”，（概率安全评定和管理第 8 届国际会议论文集，新奥尔良，2006 年），美国机械工程师学会，纽约（2006 年）。

[III-2] MÜLLER-ECKER, D., MAYER, G., GASSMANN, D.，“现代 1300 兆瓦压水反应堆低功率和停堆工况下的概率安全分析”，概率安全评定和管理”（圣胡安第 6 届国际会议论文集，波多黎各，2002 年），爱思唯尔科学，牛津（2002 年）。

[III-3] 概率风险评定协作项目组（COOPRA）《低功率停堆工作组状态报告：概率风险分析协作项目》，2001 年 10 月，爱达荷国家工程与环境实验室瀑布城（2001 年）。

[III-4] 概率风险评定协作项目组（COOPRA）《低功率停堆工作组始发事件总结：概率风险分析协作项目》，2004 年 7 月，爱达荷国家工程与环境实验室瀑布城（2004 年）。

[III-5] 联邦环境、自然保护和核安全部《根据原子能法第 19a 条进行核安全评审的实施导则－联邦德国核电厂概率安全分析导则》，2005 年 8 月 30 日，联邦 207a（2005 年 11 月 3 日）。

[III-6] 《核电概率安全分析－核电厂概率安全分析数据》，BfS-SCHR-37/05，联邦辐射防护办公室，萨尔茨吉特（2005 年）。

[III-7] 《核电概率安全分析－核电厂概率安全分析数据》，BfS-SCHR-38/05，联邦辐射防护办公室，萨尔茨吉特（2005 年）。

[III-8] 国际原子能机构《核电厂低功率和停堆模式的概率安全评定》，国际原子能机构《技术文件》第 1144 号，国际原子能机构，维也纳（2000 年）。

[III-9] ESQUIVELTORRES, J.L., LÓPEZMORONES, R.，“墨西哥拉克纳维尔德核电厂低功率和停堆状态概率安全评定”，《概率安全评定和管理》（第 8 届国际会议论文集，新奥尔良，2006 年），美国机械工程师学会，纽约（2006 年）。

参与起草和审订人员

Alzbutas, R.	立陶宛能源研究所
Bagdonas, A.	立陶宛伊格纳利纳核电厂
Berg, P.	德国联邦辐射防护办公室
Bryant, R.	英国罗尔斯-罗伊斯公司
Burgazzi, L.	意大利欧洲核能机构
Bykov, M.	俄罗斯联邦原子能公司
El-Shanawany, M.	国际原子能机构
Elter, J.	匈牙利帕克斯核电厂
Fujimoto, H.	日本核能安全组织
Goertz, R.	德国联邦辐射防护办公室
Hari, V.	印度核电公司
Hessel, P.	加拿大核安全委员会
Hlavac, P.	斯洛伐克 Relko 有限公司
Husarcek, J.	斯洛伐克核监管局
Hustak, S.	捷克核研究所
Kajimoto, M.	日本核能安全组织
Kirchsteiger, C.	欧洲委员会
Kivirinta, T.	芬兰富腾电力与热力公司
Kompella, D.	瑞士联邦核安全监察局
Kouzmina, I.	国际原子能机构
Kovacs, Z.	斯洛伐克 Relko 有限公司
Loeffler, H.	德国装置与反应堆安全公司

Lopez, A.	墨西哥国家核安全与保障委员会
Lyubarskiy, A.	俄罗斯联邦核与辐射安全科学与工程中心
Mancheva, K.	保加利亚风险工程有限公司
Niemelä, I.	芬兰辐射与核安全局
Palmaerts, S.	比利时特克贝尔工程公司
Papazov, V.	保加利亚科兹洛杜伊核电厂
Parry, G.	美国核管制委员会
Rogers, P.	英国罗尔斯-罗伊斯公司
Röwekamp, M.	德国装置与反应堆安全公司
Shepherd, C.	英国企业风险联合会
Sorel, V.	法国电力公司
Taglioni, A.	意大利欧洲核能机构
Tokmachev, G.	俄罗斯联邦原子能工程公司
Tronea, M.	罗马尼亚国家核活动管制委员会
Tudor, C.	罗马尼亚切尔纳沃德核电厂
Varde, P.	印度巴巴原子研究中心
Yang, J.	韩国原子能研究所
Yang, Zhichao	中国核动力技术研究院
Yli-Kauhaluoma, M.	芬兰洛维萨核电厂
Yllera, J.	国际原子能机构
Youngchuay, U.	泰国核技术研究所
Zeng, Yi	加拿大核安全委员会
Zhao, Bo	中国北京核工程研究所

国际原子能机构安全标准核可机构

星号表示通讯成员。通讯成员收到征求意见稿和其他文件，他们一般不参加会议。两个星号表示候补者。

安全标准委员会

阿根廷：González, A.J.；澳大利亚：Loy, J.；比利时：Samain, J.-P.；巴西：Vinhas, L.A.；加拿大：Jammal, R.；中国：刘华（Liu Hua）；埃及：Barakat, M.；芬兰：Laaksonen, J.；法国：Lacoste, A.-C.（主席）；德国 y：Majer, D.；印度：Sharma, S.K.；以色列：Levanon, I.；日本：Fukushima, A.；韩国：Choul-Ho Yun；立陶宛：Maksimovas, G.；巴基斯坦：Rahman, M.S.；俄罗斯：Adamchik, S.；南非：Magugumela, M.T.；西班牙：Barceló Vernet, J.；瑞典：Larsson, C.M.；乌克兰：Mykolaichuk, O.；英国：Weightman, M.；美国：Virgilio, M.；越南：Le-chi Dung；原子能机构：Delattre, D.（协调员）；核安全咨询小组：Hashmi, J.A.；欧盟：Faross, P.；国际核安全小组：Meserve, R.；国际放射防护委员会：Holm, L.-E；经济合作与发展组织核能署：Yoshimura, U.；安全标准委员会主席：Brach, E.W.（运输安全标准委员会）；Magnusson, S.（辐射安全标准委员会）；Pather, T.（废物安全标准委员会）；Vaughan, G.J.（核安全标准委员会）。

核安全标准委员会

阿尔及利亚：Merrouche, D.；阿根廷：Waldman, R.；澳大利亚：Le Cann, G.；奥地利：Sholly, S.；比利时：De Boeck, B.；巴西：Gromann, A.；*保加利亚：Gledachev, Y.；加拿大：Rzentkowski, G.；中国：李京喜（Jingxi Li）；克罗地亚：Valčić, I.；*塞浦路斯：Demetriades, P.；捷克：Šváb, M.；埃及：Ibrahim, M.；芬兰：Järvinen, M.-L.；法国：Feron, F.；德国：Wassilew, C.；加纳：Emi-Reynolds, G.；*希腊：Camarinopoulos, L.；匈牙利：Adorján, F.；印度：Vaze, K.；印度尼西亚：Antariksawan, A.；伊朗：Asgharizadeh, F.；以色列：Hirshfeld, H.；意大利：Bava, G.；日本：Kanda, T.；韩国：Hyun-Koon Kim；利比亚：Abuzid, O.；立陶宛：Demčenko, M.；马来西亚：Azlina Mohammed Jais；墨西哥：Carrera, A.；摩洛哥：Soufi, I.；荷兰：van der Wiel, L.；巴基斯坦：Habib, M.A.；波兰：Jurkowski, M.；罗马尼亚：Biro, L.；俄

罗斯：Baranaev, Y.；斯洛伐克：Uhrik, P.；斯洛文尼亚：Vojnovič, D.；南非：Leotwane, W；西班牙：Zarzuela, J.；瑞典：Hallman, A.；瑞士： Flury, P.；突尼斯：Baccouche, S.；土耳其：Bezdegumeli, U.；乌克兰：Shumkova, N.；英国：Vaughan, G.J.（主席）；美国：Mayfield, M.；乌拉圭：Nader, A.；欧盟：Vigne, S.；欧洲原子能公司：Fourest, B.；原子能机构：Feige, G.（协调员）；国际电力委员会：Bouard, J.-P.；国际标准化组织：Sevestre, B.；经济合作与发展组织核能署：Reig, J.；*世界核能协会：Borysova, I。

辐射安全标准委员会

*阿尔及利亚：Chelbani, S.；阿根廷：Massera, G.；澳大利亚：Melbourne, A.；*奥地利：Karg, V.；比利时：van Bladel, L.；巴西：Rodriguez Rochedo, E.R.；*保加利亚：Katzarska, L.；加拿大：Clement, C.；中国：杨华庭（Huating Yang）；克罗地亚：Kralik, I.；*古巴：Betancourt Hernandez, L.；*塞浦路斯：Demetriades, P.；捷克：Petrova, K.；丹麦：Øhlenschlæger, M.；埃及：Hassib, G.M.；爱沙尼亚：Lust, M.；芬兰：Markkanen, M.；法国：Godet, J.-L.；德国：Helming, M.；加纳：Amoako, J.：*希腊：Kamenopoulou, V.；匈牙利：Koblinger, L.；冰岛：Magnusson, S.（主席）；印度：Sharma, D.N.；印度尼西亚：Widodo, S.；伊朗：Kardan, M.R.；爱尔兰：Colgan, T.；以色列：Koch, J.；意大利：Bologna, L.；日本：Kiryu, Y.；韩国：Byung-Soo Lee；*拉脱维亚：Salmins, A.；利比亚：Busitta, M.；立陶宛：Mastauskas, A.；马来西亚：Hamrah, M.A.；墨西哥：Delgado Guardado, J.；摩洛哥：Tazi, S.；荷兰：Zuur, C.；挪威：Saxebol, G.；巴基斯坦：Ali, M.；巴拉圭：Romero de Gonzalez, V.；菲律宾：Valdezco, E.；波兰：Merta, A.；葡萄牙：Dias de Oliveira, A.M.；罗马尼亚：Rodna, A.；俄罗斯：Savkin, M.；斯洛伐克：Jurina, V.；斯洛文尼亚：Sutej, T.；南非：Olivier, J.H.I.；西班牙：Amor Calvo, I.；瑞典：Almen, A.；瑞士：Piller, G.；*泰国：Suntarapai, P.；突尼斯：Chékir, Z.；土耳其：Okyar, H.B.；乌克兰：Pavlenko, T.；英国：Robinson, I.；美国：Lewis, R.；*乌拉圭：Nader, A.；欧盟：Janssens, A.；联合国粮食及农业组织：Byron, D.；原子能机构：Boal, T.（协调员）；国际放射防护委员会：Valentin, J.；国际电力委员会：Thompson, I.；国际劳工处：Niu, S.；国际标准化组织：Rannou, A.；国际源供应商和生产者协会：Fasten, W.；经济合作与发展组织核能署：Lazo, T.E.；泛美卫生组织：Jiménez, P.；联合国原子辐射影响科学委员会：Crick, M.；世界卫生组织：Carr, Z.；世界核能协会：Saint-Pierre, S。

运输安全标准委员会

阿根廷：López Vietri, J.；**Capadona, N.M.；澳大利亚：Sarkar, S.；奥地利：Kirchnawy, F.；比利时：Cottens, E.；巴西：Xavier, A.M.；保加利亚：Bakalova, A.；加拿大：Régimbald, A.；中国：李晓清（Xiaoqing Li）；克罗地亚：Belamarić, N.；*古巴：Quevedo Garcia, J.R.；*塞浦路斯：Demetriades, P.；捷克：Duchaček, V.；丹麦：Breddam, K.；埃及：El-Shinawy, R.M.K.；芬兰：Lahkola, A.；法国：Landier, D.；德国：Rein, H.；*Nitsche, F.；**Alter, U.；加纳：Emi-Reynolds, G.；*希腊：Vogiatzi, S.；匈牙利：Sáfár, J.；印度：Agarwal, S.P.；印度尼西亚：Wisnubroto, D.；伊朗：Eshraghi, A.；*Emamjomeh, A.；爱尔兰：Duffy, J.；以色列：Koch, J.；意大利：Trivelloni, S.；**Orsini, A.；日本：Hanaki, I.；韩国：Dae-Hyung Cho；利比亚：Kekli, A.T.；立陶宛：Statkus, V.；马来西亚：Sobari, M.P.M.；**Husain, Z.A.；墨西哥：Bautista Arteaga, D.M.；**Delgado Guardado, J.L.；*摩洛哥：Allach, A.；荷兰：Ter Morshuizen, M.；*新西兰：Ardouin, C.；挪威：Hornkjøl, S.；巴基斯坦：Rashid, M.；*巴拉圭：More Torres, L.E.；波兰：Dziubiak, T.；葡萄牙：Buxo da Trindade, R.；俄罗斯：Buchelnikov, A.E.；南非：Hinrichsen, P.；西班牙：Zamora Martin, F.瑞典：Häggblom, E.；**Svahn, B.；瑞士：Krietsch, T.；泰国：Jerachanchai, S.；土耳其：Ertürk, K.；乌克兰： Lopatin, S.；英国： Sallit, G.；美国：Boyle, R.W.；Brach, E.W.（主席）；乌拉圭：Nader, A.；*Cabral, W.；欧盟：Binet, J.；原子能机构：Stewart, J.T.（协调员）；国际航空协会：Brennan, D.；国际民用航空组织：Rooney, K.；国际航空飞行员协会联合会：Tisdall, A.；**Gessl, M.；国际海事组织：Rahim, I.；国际标准化组织：Malesys, P.；国际源供应和生产者协会：Miller, J.J.；**Roughan, K.；联合国欧洲经济委员会：Kervella, O.；万国邮政联盟：Bowers, D.G.；世界核能协会：Gorlin, S.；世界核运输研究所：Green, L。

废物安全标准委员会

阿尔及利亚：Abdenacer, G.；阿根廷：Biaggio, A.；澳大利亚：Williams, G.；*奥地利：Fischer, H.；比利时：Blommaert, W.；巴西：Tostes, M.；*保加利亚：Simeonov, G.；加拿大：Howard, D.；中国：曲志敏（Zhimin Qu）：克罗地亚：Trifunovic, D.；古巴：Fernandez, A.塞浦路斯 Demetriades, P.；捷克：Lietava, P.；丹麦：Nielsen, C.；埃及：Mohamed, Y.；爱沙尼亚：Lust, M.芬兰：Hutri, K.；法国：Rieu, J.德国：Götz, C.；加纳：Faanu, A.；希腊：Tzika, F.；匈牙利：Czoch, I.；印度：Rana, D.；印度尼西亚：Wisnubroto, D.；

伊朗：Assadi, M.；*Zarghami, R.；伊拉克：Abbas, H.；以色列：Dody, A.；意大利：Dionisi, M.；日本：Matsuo, H.；韩国：Won-Jae Park；*拉脱维亚：Salmins, A.；利比亚：Elfawares, A.；立陶宛：Paulikas, V.；马来西亚：Sudin, M.；墨西哥；Aguirre Gómez, J.；*摩洛哥：Barkouch, R.；芬兰：van der Shaaf, M.；巴基斯坦：Mannan, A.；*巴拉圭：Idoyaga Navarro, M.；波兰：Wlodarski, J.；葡萄牙：Flausino de Paiva, M.；斯洛伐克：Homola, J.；斯洛文尼亚：Mele, I.；南非：Pather, T.（主席）；西班牙：Sanz Aludan, M.；瑞典：Frise, L.；瑞士：Wanner, H.；*泰国：Supaokit, P.；突尼斯：Bousselmi, M.；土耳其：Özdemir, T.；乌克兰：Makarovska, O.；英国：Chandler, S.；美国：Camper, L.；*乌拉圭：Nader, A.；欧盟：Necheva, C.；欧洲核设施安全标准：Lorenz, B.；*欧洲核设施安全标准：Zaiss, W.；原子能机构：Siraky, G.（协调员）；国际标准化组织：Hutson, G.；国际源供应商和生产者协会：Fasten, W.；经济合作与发展组织核能署：Riotte, H.；世界核能协会：Saint-Pierre, S。

IAEA
国 际 原 子 能 机 构

No. 27

当 地 订 购

国际原子能机构的定价出版物可从我们的主要经销商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。

定价出版物订单

请联系您当地的首选供应商或我们的主要经销商：

Eurospan
1 Bedford Row
London WC1R 4BU
United Kingdom

交易订单和查询：
电话：+44 (0) 1235 465576
电子信箱：trade.orders@marston.co.uk

个人订单：
电话：+44 (0) 1235 465577
电子信箱：direct.orders@marston.co.uk
网址：www.eurospanbookstore.com/iaea

欲了解更多信息：
电话：+44 (0) 207 240 0856
电子信箱：info@eurospan.co.uk
网址：www.eurospan.co.uk

定价和未定价出版物的订单均可直接发送至：

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

通 过 国 际 标 准 促 进 安 全

国际原子能机构
维也纳