IAEA
国际原子能机构

国际原子能机构安全标准

第 SSG-3（Rev.1）号

保护人类与环境

制定和实施核电厂一级概率安全评定

特定安全导则

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。

制定和实施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
库克群岛
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（Rev.1）号

制定和实施核电厂一级概率安全评定

特定安全导则

国 际 原 子 能 机 构
2025 年 · 维也纳

版 权 说 明

国际原子能机构印刷
2025 年 2 月 • 奥地利

制定和实施核电厂一级概率安全评定

国际原子能机构，奥地利，2025 年 2 月
STI/PUB/2056
ISBN 978-92-0-524224-8（简装书：碱性纸）
978-92-0-524324-5（pdf 格式）
EPUB 978-92-0-524424-2
ISSN 1020-5853

前　言

拉斐尔·马里亚诺·格罗西总干事

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

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

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

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

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

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

国际原子能机构安全标准

背景

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

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

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

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

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

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

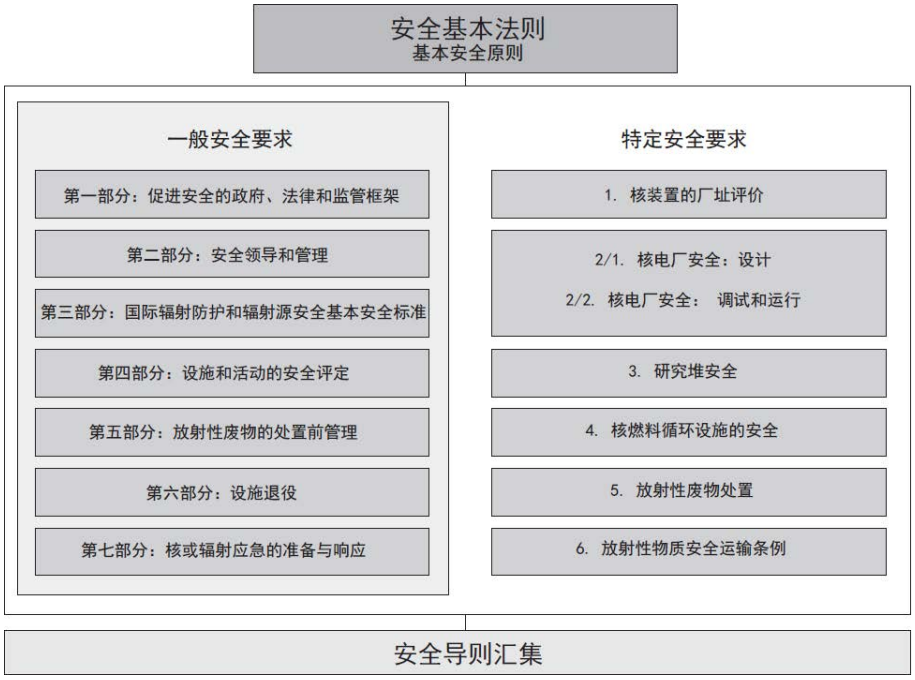

图 1. 国际原子能机构《安全标准丛书》的长期结构。

[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”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。

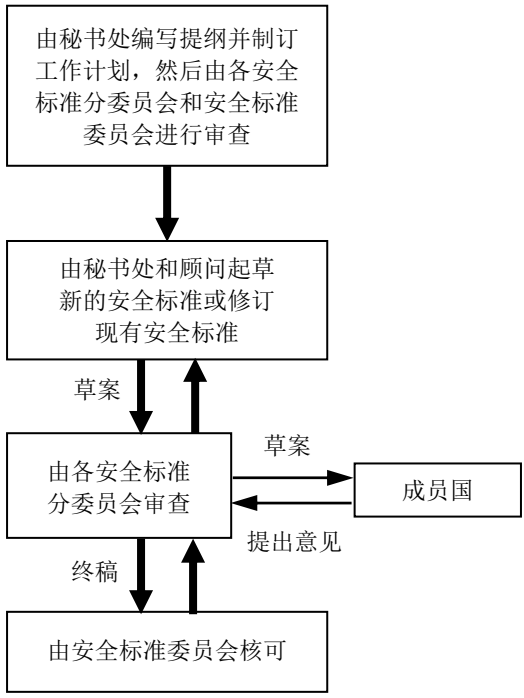

图 2. 制订新安全标准或修订现行标准的过程。

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

背景

1.1. 原子能机构《安全标准丛书》第 SF-1 号《基本安全原则》[1]确立了确保现在和将来保护工作人员、公众和环境免受电离辐射有害影响的原则。这些原则强调评定和控制固有风险的必要性。特别是 SF-1[1]第 3.22 段关于防护状态最优化的声明：

> “为了确定辐射风险是否在合理可达范围内，所有该类风险，无论是由正常运行或异常或事故工况导致，都必须优先地进行评定（使用分级方法），并在设施和活动的整个寿命期间定期再评定。”

1.2. 原子能机构的一些安全要求出版物对核电厂的风险评定提出了更特定要求。原子能机构《安全标准丛书》第 SSR-2/1（Rev.1）号《核电厂安全：设计》[2]要求 42 规定：

> **“核电厂设计的安全分析必须采用确定性分析和概率分析的方法，以便能够评价和评定各类电厂状态的安全挑战。”**

此外，SSR-2/1[2]第 5.76 段指出（脚注略）：

> “设计必须适当考虑到对电厂所有运行模式和包括关闭在内的所有电厂状态进行的概率安全分析，特别是：
>
> (a) 确定已经实现了平衡设计，因此没有任何特定特点或假想始发事件对总体风险造成不成比例的大的或显著不确定的影响，并且在可行的范围内，纵深防御级别是独立的；
> (b) 保证防止电厂参数的小偏差可能导致电厂工况大变化（陡边效应）的情况；
> (c) 将分析结果与已规定的风险验收标准进行比较。”

因此，概率安全评定（PSA）被认为是一种重要的分析工具，用于确保核电厂在可能由随机部件故障或人为错误以及内部和/或外部危害导致潜在始发事件方面的安全。

1.3. 原子能机构《安全标准丛书》第 GSR Part 4（Rev.1）号《设施和活动安全评定》[3]第 4.13 段指出：

> “安全评定必须包括安全分析，安全分析由一套不同的定量分析组成，用于通过确定性和概率方法评价和评定对安全的挑战。”

GSR Part 4[3]第 4.55 段指出：

> “概率安全分析的目的是确定导致某一设施或活动产生辐射风险的所有显著贡献因素，并评价总体设计在何种程度上是平衡的，符合已确定的概率安全标准。”

因此，需要一个全面的概率安全评定来彻底调查核电厂的安全。

1.4. 除了确定性分析提供的信息外，概率安全评定还能提供重要的安全信息。概率安全评定提供了一种方法学方法来识别各种始发事件可能导致事故序列，它包括对损坏和放射性排放及其频率的系统和现实的确定。在国际实践中，一般公认的概率安全评定分为三个级别：

(a) 在一级概率安全评定中，对电厂的设计和运行进行分析，以识别可能导致堆芯和/或燃料的事件序列估计损坏 [1] 和相应的堆芯和/或燃料损坏频率。一级概率安全评定提供了安全重要结构、系统和部件（SSC）的优势和劣势，以及防止堆芯和/或燃料损坏的现有或设想的程序。

(b) 在二级概率安全评定中，对一级概率安全评定中确定的堆芯和/或燃料损坏序列的时间序列进行评定，包括对反应堆燃料和/或乏燃料显著损坏导致现象进行定量评定。二级概率安全评定确定了燃料中放射性物质的相关排放可能导致向环境中排放的方式。它还估计放射性核素向环境排放的频率和其他相关特征。这一分析为事故预防和缓解措施的相对重要性以及放射性核素排放到环境中的实物屏障（如安全壳厂房）提供了额外的洞察。原子能机构《安全标准丛书》第 SSG-4 号《制定和实施核电厂二级概率安全评定》[4]提供了进一步的建议。

---

[1] 由于第 5 部分的重点是反应堆堆芯，除非特别提到燃料损坏，否则第 5 部分使用“堆芯损坏”术语；第 6—8 部分涉及内部和外部危害，这些危害不仅限于反应堆堆芯，还可能影响乏燃料水池中的燃料，因此适用术语“堆芯和/或燃料损坏”；第 9 部分阐述了反应堆堆芯和燃料装卸过程中燃料关闭状态的分析；最后，第 10 部分提供了燃料损坏的所有乏燃料水池特定考虑因素，而第 11 部分讨论了多机组风险指标计算的特定考虑因素。

(c) 在三级概率安全评定中，估计了公共健康和其他社会后果，如事故序列对土地或食物的污染导致放射性物质排放到环境中。

1.5. 一级概率安全评定、二级概率安全评定和三级概率安全评定是序列分析，每次评定的结果通常作为下一级概率安全评定的基础。一级概率安全评定提供了对设计弱点和防止导致堆芯和/或燃料损坏事故方法的洞察，堆芯和/或燃料损坏可能是导致放射性物质大量排放事故的前兆，对人类健康和环境有潜在的后果。二级概率安全评定提供了对导致堆芯和/或燃料损坏事故序列相对重要性的洞察，包括它们可能导致放射性物质排放的严重性，以及对密封功能和严重事故缓解和管理措施弱点的洞察，以及改进它们的方法，如 SSG-4[4]所述。三级概率安全评定提供了事故预防和缓解措施相对重要性的洞察，以对电厂工作人员和公众健康的不利后果，以及土地、空气、水和食物的污染来表示。此外，三级概率安全评定提供了与应急准备和响应相关的事故管理方面的相对有效性的洞察。

1.6. 本“安全导则”是在对相关出版物进行系统化评审的基础上编写的，包括原子能机构《安全法则》（SF-1）[1]、SSR-2/1[2]和 GSR Part 4[3]，其他安全导则的当前修订版，包括 SSG-4[4]、原子能机构《安全标准丛书》第 SSG-2（Rev.1）号《核电厂确定性安全分析》[5]、第 SSG-64 号《核电厂设计中内部危害防护》[6]和第 SSG-89 号《核装置地震安全评价》[7]，国际核安全咨询小组报告[8、9]和其他关于核电厂安全的出版物。

1.7. 本“安全导则”替代了原子能机构《安全标准丛书》第 SSG-3 号《制定和实施核电厂一级概率安全评定》[2]。

目标

1.8. 本“安全导则”的目的是为满足 GSR Part 4（Rev.1）[3]要求提供建议，这些要求与执行或管理核电厂的一级概率安全评定项目相关，并使用它来支持电厂的安全设计和运行。本“安全导则”适用于现有的和新的核电厂。本“安全导则”提供的建议旨在促进一级概率安全评定研究的技术一致性，以便为概率安全评定的应用和风险知情决策提供可靠的支持。本

[2] 国际原子能机构《制定和实施核电厂一级概率安全评定》，国际原子能机构《安全标准丛书》第 SSG-3 号，国际原子能机构，维也纳（2010 年）。

“安全导则”的另一个目的是推荐一个标准框架，以促进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。

1.9. 本“安全导则”还为确保有效履行《核安全公约》[10]第 14 条规定的义务提供了一致、可靠的手段。

1.10. 本“安全导则”提出的建议基于国际公认的良好实践。本“安全导则”并不是要先发制人地使用等效的新方法或替代方法，相反，它旨在鼓励使用任何实现一级概率安全评定目标的方法。然而，本“安全导则”概述的概率安全评定框架预计将在可预见的未来应用。

范围

1.11. 本“安全导则”以国际公认的良好实践为基础，阐述了一级概率安全评定的必要技术特点以及核电厂（现有和新的电厂）的应用。全球大多数核电厂都实施了一级概率安全评定。本“安全导则”所述的一级概率安全评定的范围包括电厂的所有运行状态（即功率运行和关闭）以及所有潜在始发事件和潜在危害，即 (i) 由随机部件故障和人为错误导致内部始发事件；(ii) 内部危害（如内部火灾、水淹、爆炸、汽轮机飞射物）；及 (iii) 自然（如地震、外部洪水、大风、其他气象灾害）及人为（如飞机坠毁、爆炸压力波、附近工业设施事故）的外部危害，以及各种危害的组合，如后果（后续）事件、相关事件及非相关（独立）事件。

1.12. 本“安全导则”侧重于评定核电厂的反应堆堆芯以及堆芯和乏燃料水池中的燃料。对场内其他放射性物质来源（如临时燃料贮存设施）的评定不在本“安全导则”范围内。然而，在影响整个场址的危害情况下，该类设施可能对反应堆和乏燃料水池产生的任何不利影响都将在安全评定中考虑，因此将在本“安全导则”进行说明。本“安全导则”还涵盖了多机组方面，在制定多机组一级概率安全评定以量化多机组风险指标时可能会考虑这些方面。

1.13. 考虑恶意行为导致危害超出了本“安全导则”的范围。[3]

[3] 尽管如此，一级概率安全评定被视为敏感信息，并得到相应处理（见原子能机构《核安保丛书》第 23-G 号《核信息安保》[11]）。

1.14. 一级概率安全评定最常见的实践是在一个综合模式中对各种危害和电厂运行状态进行分析，使用一级概率安全评定作为内部始发事件的功率运行基础。本“安全导则”概述了集成模式中包含的各种概率安全评定类型的信息。

1.15. 本“安全导则”的建议旨在尽可能保持技术中立，预计绝大多数建议将适用于各种类型的核电厂。

结构

1.16. 第 2 部分提供了关于概率安全评定性能和使用的一般问题的建议，包括概率安全评定的范围和验证以及“活的概率安全评定”的制定；第 3 部分提供了关于概率安全评定项目管理和组织的主要建议以及概率安全评定文件的一般方面；第 4 部分阐述了执行概率安全评定的团队熟悉核电厂的任务；第 5－8 部分提供了针对各种始发事件和危害的功率运行（包括低功率状态）的一级概率安全评定方法建议。特定来说，第 5 部分提供了关于内部始发事件的一级概率安全评定的建议；第 6 部分总结了关于内部和外部危害的一级概率安全评定概述的主要建议；第 7 部分和第 8 部分分别阐述了内部和外部危害的一级概率安全评定的特定方面；第 9 部分提供了关闭状态下一级概率安全评定的主要建议；第 10 部分阐述了乏燃料水池概率安全评定制定的特定方面；第 11 部分提供了旨在量化多机组风险指标的多机组一级概率安全评定建议，而第 5－10 部分从单机组一级概率安全评定的角度考虑多机组相互作用；第 12 部分列出了关于一级概率安全评定应用的主要建议。这三个附件提供了外部危害一般清单的示例、火灾事件树和地震事件树的示例，以及关于关闭状态概率安全评定的支持信息。

2. 关于概率安全评定性能和使用的一般考虑

2.1. 本部分描述了与概率安全评定性能相关的一些一般问题以及概率安全评定结果在实践中的使用。虽然本“安全导则”的范围仅限于考虑一级概率安全评定，但本部分从更广泛的角度描述了这些问题，以便对概率安全评定技术的能力及其结果提供一个完整的概述。本部分的一些陈述并不代表明确的建议，相反，它们提供了支持信息，有助于理解本“安全导则”其他部分提供的陈述和建议的上下文。

概率安全评定的范围

2.2. GSR Part 4（Rev.1）[3]要求 1 规定：

> **“在确定在某一特定阶段对任何特定设施或活动进行安全评定的范围和详细程度时，必须采用分级方法，与该设施或活动可能产生的辐射风险程度相一致。”**

此外，GSR Part 4（Rev.1）[3]要求 14 规定：**“设施或活动在所有运行状态下的性能，以及必要时在运行后阶段的性能，必须在安全分析中进行评定。”**

如果国家法规或导则中规定了概率安全目标或标准，则要进行的概率安全评定范围应当与概率安全目标或标准有关联。在高层次上，概率安全评定的定量结果通常用于核实是否符合概率安全目标或标准，这些目标或标准通常是根据 (i) 堆芯损坏频率或燃料损坏频率；(ii) 各种类型的放射性排放频率；或 (iii) 社会风险的定量估计来制定的，因此可能需要分别执行一级、二级或三级概率安全评定。概率安全目标或标准通常不会规定必须解决哪些危害和电厂运行状态。因此，为了使用概率安全评定结果来核实是否符合现有的概率安全目标或标准，应当执行包括始发事件和危害以及所有电厂运行状态全面清单的全范围概率安全评定，除非 (i) 概率安全目标或标准的制定是为了规定有限范围的概率安全评定；或 (ii) 替代方法是用于证明不在模式中的始发事件、危害和运行状态的风险不会威胁到对概率安全目标或标准的遵守。

2.3. 一级概率安全评定的范围应当包括考虑单机组反应堆堆芯中的燃料；第 5－9 部分提供了关于为单机组的反应堆堆芯制定一级概率安全评定的建议。一级概率安全评定还应当考虑乏燃料水池中的燃料；第 10 部分提供了建议。它可能还包括考虑多机组风险指标；第 11 部分提供了建议。

2.4. 概率安全评定的一个主要优势是它为风险估计中的不确定性分析提供了一个明确的框架。确定不确定性来源并理解其对概率安全评定模式及其结果的影响应当被视为任何概率安全评定的固有部分，以便在概率安全评定结果用于支持决策时，可以考虑不确定性的影响。

概率安全评定的验证和评审

2.5. GSR Part 4（Rev.1）[3]要求 18 规定：**“安全分析中使用的任何计算方法和计算机代码都必须经过核实和验证。”**概率安全评定涉及多种分析方法。根据分析的范围（一级、二级或三级概率安全评定），这些包括事故序列及其相关系统分析，通常通过制定事件树和故障树逻辑模式以及解决这些逻辑模式的方法，制定可能发生的现象的模式，例如，在堆芯损坏和/或燃料损坏后，在核电厂的安全壳和/或乏燃料厂房内可能发生的现象，以及制定放射性核素在环境中迁移的模式，以确定其对健康和环境的影响。在应用之前，应当证明这些分析方法充分代表了正在发生的过程。根据 GSR Part 4（Rev.1）[3]第 4.60 段，支持这些分析方法的计算机代码必须足以满足分析的目的和范围，控制物理和逻辑方程必须在计算机代码中正确编程。

2.6. GSR Part 4（Rev.1）[3]要求 21 规定：**“营运组织必须对安全进行独立核实，在营运组织使用或提交监管机构之前进行评定。”**一种被广泛接受的实践是，进行概率安全评定的组织委托外部机构（有时来自不同的国家）对概率安全评定进行独立的同行评审，以在一定程度上保证范围、建模和数据是充分的（例如，与提交给监管机构文件的范围一致），并确保它们符合当前国际公认的概率安全评定良好实践。参与概率安全评定评审的专家应当不参与任何与所考虑的概率安全评定绩效相关的活动，并应当代表独立于概率安全评定制定者的组织。

活的概率安全评定

2.7. GSR Part 4（Rev.1）[3]要求 24 规定：**“安全评定必须定期评审和更新。”**在核电厂的运行寿命期间，通常会对结构、系统和部件的设计或核电厂的运行方式进行修改。该类修改可能会对与电厂相关的风险水平产生影响。在电厂运行期间，将获得关于始发事件的频率和部件故障概率的额外统计数据。同样，可能会获得新的信息、更新的知识、新的运行经验和更复杂的方法和工具，这可能会改变分析中做出的一些假设，从而改变概率安全评定给出的风险估计。因此，概率安全评定应当在电厂的整个生命周期内保持最新，以确保其与决策过程相关。定期更新的概率安全评定被称为“活的概率安全评定”。在更新概率安全评定时，应当考虑电厂设计和运行的变化、新的技术信息、可用的更复杂的方法和工具，以及从电厂运

行中获得的新的电厂特定数据（例如，用于评定始发事件的频率或部件故障概率的数据）。概率安全评定的更新应当由特定流程启动，概率安全评定的状态应当定期评审，以确保其作为电厂的代表性模式保持不变并符合其预期目的。

2.8. 应当在核电厂的整个生命周期内收集数据，以检查或更新分析。这些数据应当包括关于运行经验的数据，特别是关于始发事件的数据，试验、维护和维修期间部件故障和不可用的数据，和人的表现数据。应当根据新数据定期再评定分析结果。来自其他电厂的新数据集相同类型或类似配置（如果可用）也应当用于改善活的概率安全评定。

2.9. 应当鼓励制定活的概率安全评定，以帮助电厂正常运行决策过程。许多决策，如评定与电厂变更或部件允许大修时间的临时变更相关的风险变化，都可以由概率安全评定得出的论据来支持。经验表明，这种活的概率安全评定可以给营运组织带来实质性的收益，其使用通常受到监管机构的欢迎。

概率安全目标或标准

2.10. GSR Part 4（Rev.1）[3]要求 4 规定：

> **“安全评定的主要目的必须是确定设施或活动是否达到了足够的安全水平，以及设计人员、营运组织和监管机构……是否达到了基本安全目标和安全标准。”**

当概率安全评定的目的是确定风险的显著因素或在各种设计方案和电厂配置之间进行选择时，参考值可能是不必要的。但是，当概率安全评定的目的是帮助判断 (i) 计算的风险是否可接受；(ii) 电厂的设计或运行的拟议变更是可接受的；(iii) 有必要进行变更以降低风险水平，则应当规定概率参考值，以便为设计人员、营运组织、监管机构和其他相关各方在提供核电安全规定履行各自职责时，就电厂期望或要求的安全水平提供指导。在一些国家，目前的实践是将参考值制定为概率安全目标，这意味着它们代表了旨在实现的方向值。在其他国家，参考值是规定必须遵守的严格限值的标准。

2.11. 概率安全评定将根据要评定的后果，产生与不同级别风险相关的数值。可针对以下任何或所有风险度量设定概率安全目标或标准：

(a) 执行安全功能所涉及的特定安全功能或系统的故障概率；

(b) 堆芯损坏 [4] 或燃料损坏的频率（一级概率安全评定）；

(c) 从电厂特定排放放射性物质的频率（例如，特定说明其数量、同位素或时间），或放射性物质的排放频率与其规模（二级概率安全评定）的函数关系；

(d) 对公众成员的特定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. 在国家中，概率参考值通常被确定为标准、对象、目标、目的或导则，或者被确定为方向的数值。此外，与容忍阈值和设计目标相对应的风险级别数值因国家而异。[5]

2.13. 对于安全功能或系统的故障概率，可以在安全功能或系统的级别设置概率目标。这种概率目标对于检查所提供的冗余性和多样性水平是否足够是有用的。该类目标将特定于电厂设计，因此本出版物中无法提供关于设定该类目标的建议。在安全评定中，应当检查是否达到了这些目标。如果没有，只要满足更高水平的标准，设计仍然可以接受。然而，应当特别考虑相关系统，看看是否可以做出任何合理可行的改进。

2.14. 根据目前核电厂的设计和运行经验，并根据可接受的风险，一些国家在国家层级界定了现有的和新的核电厂。参考文献[8]提供了一个示例 [6]。

---

[4] 如第 5 部分所述，需要为堆芯损坏规定概率安全目标或标准。对于不同的反应堆设计，这些安全目标或标准可能是不同的。

[5] 参考文献[12]提供了概率安全标准定义的可用框架和示例。

[6] 参考文献[8]的堆芯损坏频率目标为现有电厂每反应堆年 1×10^{-4} 次，未来电厂每反应堆年 1×10^{-5} 次。参考文献[8]没有明确规定数值适用于概率安全评定的哪个范围，假设是指全范围概率安全评定。

2.15. 堆芯损坏频率和燃料损坏频率[7]是一级概率安全评定中最常用的风险衡量标准。在许多国家，该类数值被正式或非正式地用作概率安全目标或标准。

概率安全评定在决策中的使用

2.16. GSR Part 4（Rev.1）[3]要求 23 规定：

> **“安全评定的结果必须用于特定说明维护、监视和视察计划，特定说明对安全具有重要意义的所有运行活动以及对预计运行事件和事故作出响应的程序，特定说明参与设施或活动的工作人员的必要能力，并以综合的、风险知情方法作出决定。”**

2.17. 概率安全评定应当在电厂寿命期间使用，结合确定性安全分析的结果和洞察以及纵深防御的考虑，为决策提供输入。

2.18. 概率安全评定可以为各种相关各方提供有用的洞察和输入，如营运组织（即管理、工程、运行和维护人员）、监管机构、技术支持组织、设计人员和供应商，以便就以下事项做出决策：

(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。

2.19. 如果将概率安全评定的结果用于支持决策过程，则应当为此建立一个正式的框架（见参考文献[9]）。决策过程的细节将取决于特定概率安全评定申请的目的、要做出决策的性质以及要使用的概率安全评定结果。如果要使用概率安全评定的数值结果，应当建立参考值以便与这些结果进行比较。

2.20. 概率安全评定应当说明电厂的实际设计或运行，或者－如果电厂正在建造中或正在进行改造－电厂的预计设计或运行，应当明确确定为分析的基础。为了给概率安全评定的完成提供一个明确的目标，电厂的状态可以固定

[7] 详情见第 10.2－10.6 段。

为特定日期（“冻结日期”）或商定的改造完成后的状态。如第 2.7－2.9 段所述，以后的变化可以在一个活的概率安全评定计划的框架内解决。

2.21. 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以评定安全水平。从概率安全评定中获得的洞察应当与从确定性分析中获得的洞察结合起来考虑，以做出关于电厂安全的决定。关于电厂安全的决定应当是一个迭代过程的结果，旨在确保满足国家要求和标准，设计是平衡的，风险尽可能低。

2.22. 此外，概率安全评定的结果应当与参考值进行比较，如概率安全目标或标准，如果这些已在国家法规或导则中规定。对于为电厂定义的所有概率目标或标准，包括涉及系统可靠性、堆芯损坏频率和/或燃料损坏频率、放射性物质排放频率、对工作人员健康的影响、对公众健康的影响以及场外后果（如土地污染和食品限制）的目标或标准都应当这样做。

2.23. 概率安全评定应当旨在识别对风险有不可忽略 [8] 影响的所有事故序列。[9] 如果分析没有解决对风险的所有显著影响（例如，如果它忽略了外部危害或关闭状态），那么从概率安全评定中得出的关于电厂风险水平的结论，即所提供的安全特点的平衡和/或对设计或运行进行修改以降低风险的需要可能是有偏见的。当使用概率安全评定支持决策时，应当认识到这些限制。因此，建议使用全范围概率安全评定模式。

2.24. 概率安全评定的结果应当用于识别电厂设计或运行弱点。这些弱点可以通过考虑始发事件组对风险的贡献，结构、系统和部件的重要性测量以及人为错误对整体风险的贡献来识别。如果概率安全评定的结果表明可以对电厂的设计或运行进行修改以降低风险，则应当在合理可行的情况下纳入该类修改（见参考文献[13]）。

2.25. 第 12 部分提供了关于概率安全评定特定应用的详细建议，供监管机构和营运组织或设计组织决策。

[8] 根据对最终结果和后续决策过程的评价潜在影响，对风险的贡献可被视为忽略不计。

[9] 这仅涉及不是由安保事件（如恶意行为）触发的假想方案。

3. 概率安全评定项目管理与组织

概率安全评定项目的目标和范围的定义

3.1. 确定概率安全评定的目标及其预期和潜在用途是开始概率安全评定之前的一个重要步骤。概率安全评定的范围由分析级别（即一级、二级或三级）、所考虑的始发事件和危害以及所处理的运行状态（即功率运行或关闭[10]）来定义。概率安全评定的范围应当符合分析的目标以及资源和信息的可获得性，如必要的程序和方法、人员、专门知识、资金和分析所需的时间。例如，如果概率安全评定的目的是根据指定的概率安全目标核实电厂运行产生的风险，从而意味着完整的风险评定，则应当执行包括始发事件和危害以及所有电厂运行状态的综合清单的全范围概率安全评定。应当为分析提供充足的资源。此外，可能需要分析其他辐射源（例如乏燃料水池中的燃料），这取决于概率安全目标的制定。

3.2. 概率安全评定的预期应用可能会对概率安全评定的范围、建模方法和详细程度产生影响。如果在概率安全评定项目的计划阶段考虑到这种影响，将有助于避免所获得的结果和洞察的不一致。例如，如果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。如果概率安全评定用于支持应急计划区的定义，还应当设想扩展到二级甚至三级。作为另一个示例，如果概率安全评定模式被用作风险监控器的基础，该模式在始发事件的建模中应当是“对称的”。[11] 第 12 部分提供了关于概率安全评定各种应用所必需特点的建议。

---

[10] 低功率和关闭状态的概率安全评定有时作为同一独立研究的一部分进行，然而，将低功率概率安全评定作为功率运行概率安全评定的一部分可能更实际（这就是本“安全导则”涵盖的各国家）。

[11] 如果一个概率安全评定模式明确地模拟了所有可能发生事件位置的始发事件，包括所有一回路、所有信用系统的通道以及正常运行系统的所有运行和备用通道，则该模式被认为是对称的（见第 5.83 段）。当在电厂配置中引入特定变化时，始发事件的非对称建模可能会对通过风险监控器获得现实的风险状况造成障碍。

概率安全评定项目管理

3.3. GSR Part 4（Rev.1）[3]要求 5 规定：**“进行安全评定的第一阶段必须确保确定并提供必要的资源、信息、数据、分析工具以及安全标准。”**

3.4. 此外，GSR Part 4（Rev.1）[3]要求 22 规定：**“必须计划、组织、应用、监查和评审产生安全评定的过程。”**

3.5. 概率安全评定的项目管理在很大程度上取决于一个国家的以下特定条件：

(a) 参与概率安全评定项目的组织；
(b) 参与组织的参与类型和程度；
(c) 概率安全评定项目的目标和范围。

在规定了概率安全评定的目标和范围后，应当制定概率安全评定项目的管理计划。这包括选择方法和建立程序，选择人员和组织将执行概率安全评定的团队，培训团队，编写概率安全评定项目时间表，预算和确保必要的资金，以及建立质量保证程序和同行评审程序。

3.6. 概率安全评定项目通常由以下机构之一委托：

(a) 电厂设计人员；
(b) 电厂营运组织；
(c) 监管机构。

概率安全评定可以由上述机构或顾问、研究机构、大学、技术支持组织或这些机构的组合来执行。营运组织应当始终作为运行知识的来源参与，并成为所获得的洞察的受益者。[12]

3.7. 希望在电厂的生命周期内尽早开始进行概率安全评定。早期发现的设计缺陷或程序缺陷可以比那些在电厂运行前仍然存在的缺陷更低代价地得到纠正或改进。虽然概率安全评定可以在电厂寿命的任何阶段启动，但

[12] 对于在设计阶段进行概率安全评定的情况，执行这项建议可能具有挑战性。如果对参考电厂进行一般概率安全评定，营运组织的运行经验可能会特别有益。

概率安全评定模式和文件应当在电厂的整个运行寿命中保持和定期更新，以提供持续的效益。

3.8. 概率安全评定项目应当考虑特定冻结日期，以模拟电厂的竣工和运行工况。如果在概率安全评定项目开始时就知道电厂设计和运行的某些变化将在近期实施，在概率安全评定完成之前，应当在概率安全评定的早期阶段决定这些变化是否将在概率安全评定中解决。如果决定应对未来的变化，应当相应确定冻结日期，概率安全评定应当考虑改造后电厂的状态。

3.9. 概率安全评定的文件应当以清晰、可追溯、系统和透明的方式制定，以便能够有效地支持概率安全评定的评审、概率安全评定的应用和未来的概率安全评定升级。

方法的选择和程序的建立

3.10. 应当在项目开始时建立适当的工作方法和程序，以便在项目期间尽量减少修改。方法和过程中不必要的迭代可能会导致概率安全评定项目的延迟。本出版物的以下章节给出了分析方法工具和途径的一般导则。一旦选定了工作方法，各种程序步骤应当与质量保证和团队培训任务相结合，以制定详细的任务计划，包括项目时间表。

3.11. 完成概率安全评定所需的资源，包括相关专家的专业知识、人力资源、计算机时间和日历时间，在很大程度上取决于概率安全评定的范围，而概率安全评定的范围又受总体目标和概率安全评定团队现有的专业知识的支配。应当根据既定的详细程序安排活动，并考虑到人员的可用性。

团队选择与组织

3.12. 执行概率安全评定的团队成员可以通过他们所代表的组织（如果涉及不同的组织）和他们提供的技术专长来表征。一旦选定了必要的人员，就应当建立沟通渠道，并分配特定任务。必要的培训应当根据概率安全评定的活动确定并随后组织。小组的组建和培训与第 3.15 段和第 3.16 段所述的质量保证任务密切相关。

3.13. 进行概率安全评定所需的专业知识应当包括两个基本要素：概率安全评定技术知识和电厂知识。根据概率安全评定的范围，这种专业知识的深度可能会有所不同，但应当预见到电厂设计人员和/或电厂营运组织的参与。更具体地说，应当提供与电厂知识相关的专门知识由非常熟悉电厂运行状态和事故工况下的设计和运行的人员进行。

3.14. 首次执行概率安全评定的团队应当接受培训，以获得成功完成分析所需的专业知识。

建立概率安全评定质量保证计划

3.15. 概率安全评定的质量保证[13]计划包括达到概率安全评定适当质量所必需的活动和核实达到适当质量所必需的活动。对于概率安全评定来说，适当的质量意味着最终产品是正确的和可用的，并且符合概率安全评定的目标和范围。质量保证计划应当为影响概率安全评定质量的所有活动提供严格的方法，包括在适当的情况下，核实每项任务是否已令人满意地执行，以及是否已实施必要的纠正措施。

3.16. 概率安全评定的质量保证应当被视为概率安全评定项目的一个组成部分，质量保证程序应当成为概率安全评定程序的一个组成部分。质量保证程序应当规定在组织、技术工作和文件领域对与概率安全评定相关的组成活动进行控制。在应当用于技术工作时，质量保证程序旨在确保目标、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件的控制和概率安全评定模式不同版本的控制。GSR Part 2[14]规定了文件控制的一般要求。

[13] 在其他原子能机构《安全标准丛书》出版物中，包括原子能机构《安全标准丛书》第 GSR Part 2 号《安全的领导和管理》[14]，使用了“管理系统”术语，而不是“质量保证计划”术语。然而，在本“安全导则”，保留了术语“质量保证”和“质量保证计划”，以反映概率安全评定领域广泛接受的当前实践和术语。

概率安全评定文件的一般方面

概率安全评定文件的目标和内容

3.17. GSR Part 4（Rev.1）[3]要求 20 规定：“**安全评定的结果和发现必须记录在案。**”概率安全评定文件的主要目标应当是满足用户的需求，并适合概率安全评定的特定应用。概率安全评定文件的可能用户包括：

(a) 核电厂的营运组织（即管理、工程、运行和维护人员）；
(b) 设计人员和供应商；
(c) 监管机构和向其提供技术支持的个人或组织；
(d) 其他政府机构；
(e) 公众。

其中一些用户（如公众）可能主要使用概率安全评定的总结报告，而其他人可能使用完整的概率安全评定文件，包括计算机模式。

3.18. 概率安全评定文件包括工作文件、带有解释的计算机输入和输出、信函、中期报告和概率安全评定的最终报告。文件应当完整、结构良好、清晰易懂，包括便于评审和更新。文件应当以可追溯和序列的方式呈现（即最终文件中分析的出现序列应当尽可能符合实际执行的序列）。对扩展和解释概率安全评定的假设、排除和限制的明确陈述对用户也特别重要。

3.19. 报告中包含的文件（和/或引用的材料）应当提供重建研究结果所需的所有信息。不在外部报告中公布的所有中间支持分析、计算和假设应当作为说明、工作文件或计算机输出保留。这对于将来重建和更新分析的每个细节非常重要。

文件的组织

3.20. 概率安全评定研究的最终报告应当分为三个主要部分：

(1) 总结报告；
(2) 主报告；
(3) 主报告的附录。

3.21. 总结报告的设计应当提供概率安全评定的动机、目标、范围、假设、结果和结论的概述，其水平应对反应堆安全专家的广大受众有用，并足以进行高水平评审。总结报告的设计应当实现以下目标：

(a) 支持概率安全评定的高水平评审；

(b) 向兴趣广泛受众传达研究的关键方面；

(c) 在查阅主报告之前，为用户提供清晰的框架和导则。

3.22. 总结报告应当包括一个关于主报告结构的小节，并简要说明主报告及其附录各部分的内容。概率安全评定各部分之间的关系也应当包括在总结报告的这一小节中。

3.23. 主报告应当清晰、可追溯地概述完整的概率安全评定研究，包括电厂描述、研究目标、使用的方法和数据、考虑的始发事件、电厂建模结果和结论，以及建议。主报告及其附录的设计应当实现以下目标：

(a) 支持概率安全评定的技术评审；

(b) 向兴趣用户传达关键的详细信息；

(c) 允许概率安全评定模式和结果的有效和多样的应用；

(d) 促进模式、数据和结果的更新，以支持电厂的持续安全管理。

3.24. 附录应当包含详细数据、工程计算记录和详细模式。附录的结构应当尽可能与主报告的各部分和分部分直接对应。

3.25. 除了本部分提供的关于文件的一般建议之外，关于各种始发事件、危害和关闭状态的概率安全评定的第 5－9 部分还提供了关于文件的特定建议。

4. 熟悉电厂和收集信息

4.1. 在准备一级概率安全评定时，概率安全评定团队成员应当熟悉电厂的设计和运行，包括应急程序以及试验和维护程序。可用于熟悉电厂的信息来源包括：

(a) 电厂的安全分析报告；

(b) 电厂的技术规范；

(c) 系统描述；

(d) 竣工（原样）系统图纸（如管道和仪器仪表图）；

(e) 电气线路图，包括电气总线保护系统的电路图和跳闸标准；

(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) 与系统成功标准相关的分析；

(i) 电厂或同一国家或其他国家类似电厂的运行经验，以及事故报告和分析；

(j) 运行人员日志；

(k) 与运行人员讨论；

(l) 电厂运行记录和关闭报告；

(m) 电厂数据库和/或用于维护的计算机化管理系统（如有）；

(n) 电厂布局图；

(o) 管道位置和布线图纸；

(p) 电缆位置和布线图纸；

(q) 电厂巡视报告；

(r) 监管要求；

(s) 其他相关电厂文件。

4.2. 应当收集包含分析所需信息的电厂文件，并提供给概率安全评定团队。取决于范围对于概率安全评定，可能需要更特定信息（例如，对于外部危害的概率安全评定，电厂布局和场址及周围的地形）。可能需要与不属于概率安全评定团队的运行人员进行互动，以获得澄清和额外信息。

4.3. 目前，在许多国家，概率安全评定的性能对于安全分析报告的一部分是必要的。在这种情况下，概率安全评定文件可能会参考安全分析报告的相应章节（如系统描述）。所有的信息都应当清楚地引用以便于找到。

4.4. 电厂熟悉度是概率安全评定应对外部和内部危害的关键要素。应当进行彻底的电厂巡视，以核实关于危害来源和易受危害损坏的电厂特点的信息。应当提供与外部和内部危害相关的电厂熟悉的特定导则。

5. 功率运行内部始发事件的一级概率安全评定

5.1. 本部分提供了在对内部始发事件执行一级概率安全评定时满足 GSR Part 4（Rev.1）[3]要求 6－13 的建议。特别是，它提供了对功率运行期间由随机部件故障和人为错误导致内部始发事件执行一级概率安全评定时需要解决的技术问题的建议。用于分析的一般框架在图 1 示出。

一级概率安全评定方法的一般方面

5.2. 第一步应当是定义用于一级概率安全评定的总体方针和方法。总体方针和方法应当提供从始发事件开始可能发生的故障序列建模，并确定可能导致堆芯损坏的人为错误和结构、系统和部件故障的组合。

5.3. 几种技术可用于执行概率安全评定。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大小（即复杂性）在很大程度上取决于偏好，还取决于所用软件的特点。

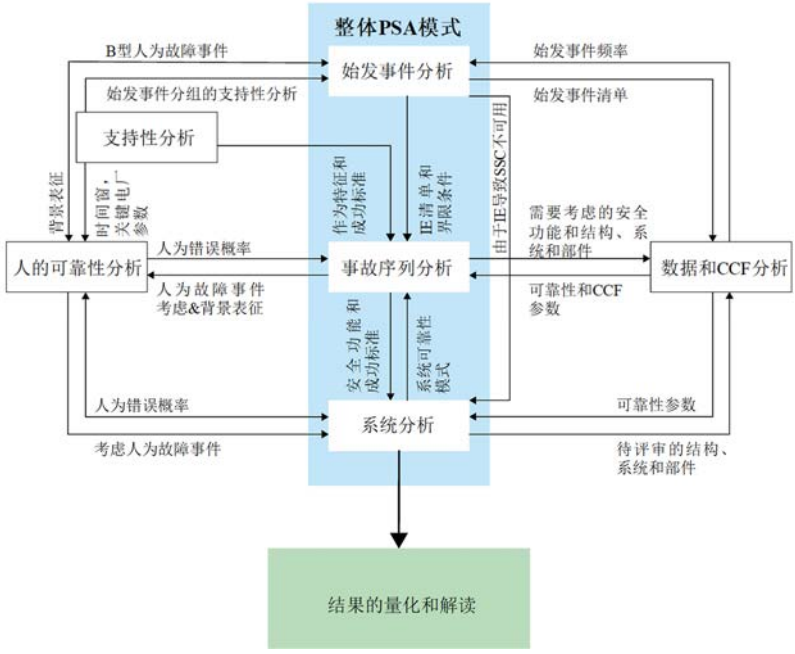

图 1. 内部始发事件一级概率安全评定的一般分析框架。IE－始发事件；AS－事故序列；CCF－共因故障。

5.4. 一种广泛实践的方法是使用小事件树和大故障树的组合，通常称为故障树链接方法。事件树概述了事故序列的广泛特征，这些特征从始发事件开始，根据信用系统 [14] 的成功或失败，导致成功的结果、堆芯损坏（见第 5.43 段和第 5.44 段）或一种电厂损坏状态（用于二级概率安全评定）。故障树用于模拟信用系统执行其安全功能的故障。这个依赖关系（不同信用系统之间或信用系统和始发事件之间）在故障树和事件树中建模。

5.5. 采用的另一种方法是使用大事件树和小故障树来执行分析。在这种方法中，安全功能、信用系统和支持系统的故障在事件树中建模。这种方法被称为大事件树方法、链接事件树方法或带边界条件的事件树方法。也可以仅使用事件树或仅使用故障树来执行分析。然而，在后一种情况下，高级故障树结构通常来自或基于事件树或事件树集。

5.6. 总体目标应当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度的保守性，因为这可能会使结果产生不适当的偏差。因此，一级概率安全评定应当基于最佳估计模式、假设和数据。然而，在高度不确定的情况下，一些保守可能是必要的，以避免不合理的乐观。使用保守的方法应当是正当的。如果无法获得核电厂对起始因子响应的最佳估计，则可使用以下一个或多个来源：

(a) 有界确定性分析；
(b) 设计分析；
(c) 调试试验；
(d) 在役试验；
(e) 专家判断。

[14] “信用系统”是在概率安全评定中可信的系统，包括运行和备用安全系统以及非安全系统，其在事故期间的运行有助于防止不希望的最终状态（例如堆芯损坏、燃料损坏）。此外，“可信的结构、系统和部件”是本出版物中使用的一个术语，用于指定概率安全评定中可信的特定结构或部件。

5.7. 对于具有多机组的电厂，机组之间的相互作用（从风险角度来看，包括积极和消极）应当在一级概率安全评定中从所考虑机组的角度进行考虑。第 11 部分 [15] 提供了为量化多机组风险指标而制定的多机组概率安全评定的建议

5.8. 应当可以将一级概率安全评定模式用于预期应用，并针对未来可能的应用进行更新。

5.9. 应当使用具有以下能力的适当计算机代码进行分析：

(a) 它应当能够处理核电厂非常大和复杂的逻辑模式。

(b) 它应当能够通过布尔逻辑约简来确定最小割集。

(c) 它应当能够在合理的短时间内量化概率安全评定模式。

(d) 它应当能够提供解释一级概率安全评定所需的信息，如堆芯损坏频率、主要最小割集、最小割集频率（即始发事件和故障的组合和/或导致堆芯损坏的人为错误）、重要性测量以及不确定性和敏感性分析的结果。

5.10. 一级概率安全评定模式的制定是一个迭代过程，应当持续到产生一个准确、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一组始发事件的识别。始发事件是挑战正常运行的事件，需要成功缓解以防止堆芯损坏或者可能直接导致堆芯损坏。

5.12. 本部分讨论在功率运行过程中可能出现的内部始发事件的识别；第 6 部分概述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 部分分别提供了详细建议；第 9 部分提供了关于识别关闭状态下可能出现的始发事件特定问题的建议；第 10 部分所述乏燃料水池中可能出现的始发事件；以及第 11 部分可能出现的与多机组概率安全评定相关的始发事件。

[15] 在导致影响整个场址的事件时，必须考虑对场址其他设施（如反应堆临时干式燃料贮存设施、乏燃料水池）的不利影响（见参考文献[15、16]）。

始发事件的识别

5.13. 应当使用一个系统化过程来确定一级概率安全评定中要处理的一组内部始发事件。这应当充分全面地结合各种不同的方法，包括：

(a) 评审确定性设计基准、事故分析和设计拓展工况分析以及安全分析报告；

(b) 根据被分析电厂和类似电厂的运行经验分析确定始发事件；

(c) 与为类似电厂的一级概率安全评定制定的始发事件清单以及现有的安全标准和导则进行比较；

(d) 分析方法，如危害和可运行性研究或故障模式和影响分析或电厂结构、系统和部件的其他相关方法，以确定其部分或全部故障是否会导致始发事件；

(e) 演绎分析，如主逻辑图，以确定可能挑战正常运行并导致始发事件的基本故障或基本故障组合。

5.14. 作为一级概率安全评定基础内部始发事件应当尽可能全面。使用第 5.13 段所列方法的充分综合组合使人相信，为电厂确定的一组始发事件尽可能完整。

5.15. 在确定始发事件时，应当特别考虑被分析电厂的任何新颖或特殊的设计特点，因为它们可能是新始发事件的潜在来源。这对于没有或很少运行经验的新的核电厂尤其重要，在这些核电厂中，应当特别努力确定特殊的始发事件、故障模式、事故序列和该设计特有的依赖性。第 5.13 (d) 段所述的分析方法，应当对所有运行系统和备用系统进行，以确定可能因运行故障、部分运行故障或意外运行而产生的可能始发事件（或可能构成始发事件的间接故障）。

5.16. 一级概率安全评定中包含的始发事件的主要类别是威胁安全功能的事件，例如从反应堆堆芯中移除热量、控制一回路冷却剂库存、保持一回路的完整性以及控制堆芯的反应性。

5.17. 所识别的一组始发事件应当包括部分功能故障或部分系统故障（例如，蒸汽发生器供给量减少、一台蒸汽发生器供给量丧失）以及完全故障（例如，所有蒸汽发生器供给量完全丧失）。这一点很重要，因为涉及部分故障的始发事件仍然会对风险产生显著影响。

5.18. 所识别的一组始发事件应当包括在所有允许的运行状态下（例如，在一个冷却剂回路停止运行的情况下运行）可能发生的事件。

5.19. 所识别的一组始发事件应当包括具有潜在显著后果的频率极低事件（例如反应堆压力容器破裂、接口系统中冷却剂丧失事故）。如果一级概率安全评定打算用作二级概率安全评定（可能还有三级概率安全评定）的基础，那么在接口系统中包括冷却剂丧失事故尤为重要。

5.20. 对于拥有一个以上核电厂机组的场址，应当确定可能同时影响一个以上机组的一系列始发事件（例如场外电源丧失）。此外，应当识别可能在其中一个机组发生并导致在另一个机组始发事件的事件。例如，对于内部危害的一级概率安全评定，被分析机组中的始发事件可能是由相邻机组中汽轮机解体产生的飞射物撞击引起的。

5.21. 如第 5.13 (c) 段所述，应当将为该电厂确定的一组始发事件与类似电厂的始发事件进行比较，确保所有相关的始发事件都包括在内。如果发现差异，应当包括额外的始发事件，或提供正当性说明它们非相关的原因。

5.22. 应对核电厂（如果已经运行）和类似核电厂的运行经验进行评审，以确保实际发生的任何始发事件都包括在一级概率安全评定中处理的一系列始发事件中。在分析中应当确定并考虑该类始发事件的原因。

瞬变

5.23. 一级概率安全评定应当基于一组可能发生的瞬变。就对基本安全功能潜在退化的主要影响而言，瞬变分为以下几类：

(a) 反应堆排热增加（例如，由于次级安全阀打开或蒸汽管道破裂）；

(b) 反应堆排热减少（例如，由于主给水丧失或给水管道破裂）；

(c) 反应堆冷却剂系统流量降低（例如，由于反应堆冷却剂泵跳闸、泵卡住或轴断裂）；

(d) 反应性和功率分布异常（例如，由于控制棒不受控制抽出、控制棒弹射或硼稀释）；

(e) 反应堆冷却剂库存增加（例如，由于应急冷却剂注入系统的意外运行）；

(f) 导致反应堆跳堆或反应堆立即关闭的任何其他事件（冷却剂丧失事故除外）。

5.24. 这组瞬变应当包括作为内部始发事件的场外电源丧失。涉及场外电源丧失的始发事件应当根据发生频率和持续时间进行规定，并应当考虑场外电源恢复的可能性。该信息应当基于电厂设计的细节和与电厂电网连接相关的运行经验。

5.25. 当始发事件“场外电源丧失”是由于内部和外部危害而发生的，并且在各自的概率安全评定模式中明确建模（即内部和外部危害的概率安全评定），则内部始发事件概率安全评定的场外电源丧失的定义应当排除这些原因，以避免在一级概率安全评定中重复计算。

5.26. 应当特别注意，在事件序列中，当场外电源丧失后，所有现场交流电源都会丧失。概率安全评定研究表明，这种情况（称为电站断电）对许多电厂的风险造成了显著影响。

5.27. 一组始发事件还应当包括支持系统（例如电力系统、仪器仪表空气系统、冷却水系统、室内冷却系统）以及仪器仪表和控制系统的故障。当支持系统的故障可能导致始发事件时，这一点尤其重要并且支持系统还期望在始发事件之后提供安全功能。

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一整套始发事件。

5.29. 确定的一组冷却剂丧失事故应当包括所有可能导致一回路冷却剂丧失的不同大小和位置的断裂。应当根据电厂的实际设计和布局确定可能的断裂位置。冷却剂丧失事故还应当包括管道和阀门的故障，特别是安全阀。

5.30. 应当识别可能导致一回路冷却剂排放到安全壳外的冷却剂丧失事故。这些通常包括蒸汽发生器管的破裂和接口系统中冷却剂丧失事故，其中从破裂处泄漏的一回路冷却剂旁路安全壳，因此不能从安全壳集水坑再循环。

5.31. 应当根据需要操作以防止堆芯损坏的结构、系统和部件的成功标准，对确定的一组冷却剂丧失事故进行分类和分组。对于压水堆，冷却剂丧失事故通常分为大、中或小，主要基于冷却剂注入系统为缓解冷却剂丧失事

故所需的响应。根据电厂的设计，可能需要一套不同的设备来提供保护，防止非常小的冷却剂丧失事故，例如涉及反应堆冷却剂泵密封故障的事故。

始发事件的分组

5.32. 为了将一级概率安全评定所需的分析保持在可管理的规模，在进行事故序列分析之前，应对始发事件进行分组。

5.33. 如果为了进一步缩小概率安全评定模式的规模，对始发事件组进行筛选，并将一些事件排除在模式之外，则筛选标准应当与概率安全评定的目的一致，以便不排除风险的显著因素。如果进行了筛选，可能仍然需要针对特定概率安全评定应用进行重新检查。

5.34. 始发事件应当按组排列，其中始发事件的以下所有属性相同（或非常相似）：

(a) 始发事件后的事故进展；
(b) 信用系统的成功标准；
(c) 始发事件对信用系统的可用性和运行的影响，包括驱动保护动作或阻止系统驱动信号条件的存在；
(d) 运行人员的预计响应。

5.35. 用于特定始发事件组的信用系统成功标准应当是该组内所有单一事件的最严格标准。

5.36. 如果与信用系统的事故进展和/或成功标准略有不同的始发事件被分组在一起，事故序列分析应当提供所有潜在事故序列和这些始发事件后果的边界分析。

5.37. 始发事件应当以这样一种方式分组，即不在分析中引入不适当的保守主义。

5.38. 可能导致安全壳旁路的始发事件（如蒸汽发生器管道破裂、接口系统中的冷却剂丧失事故）应当不与安全壳保持有效的其他冷却剂丧失事故归为一组。这方面对于没有二级概率安全评定的应用可能特别重要，因为后果更严重。

5.39. 考虑到成组始发事件可能对多机组电厂产生不同的影响，应当避免将单机组和多机组始发事件分组（见第 11 部分）。

5.40. 一级概率安全评定文件应当包括为电厂确定的所有始发事件的清单，并应当提供每个始发事件的描述和用于识别该事件方法的充分信息（例如，危害和可运行性研究、故障模式和影响分析、主逻辑图、运行经验评审）。

事故序列分析

5.41. 分析的下一步是确定电厂运行人员对每组始发事件的响应，这些始发事件依赖于信用系统的运行来执行安全功能以防止堆芯损坏。这种安全功能通常包括关闭反应堆并将其保持在次临界状态，以及从反应堆堆芯散热（见第 5.47 段）。

5.42. 事故序列中确定的事件将与结构、系统和部件的成功与失败以及在执行始发事件组所需的安全功能时采取的人员行动相关。事故序列模式的最终状态将对应于安全稳定状态，其中所有必要的安全功能都已完成，或者对应于堆芯损坏状态，应当制定什么构成安全稳定状态的标准。[16]

堆芯损坏

5.43. 例如，对于轻水堆，通常认为，如果任何一个燃料参数（如包壳温度）超过其设计基准限值或更高的限值（如果正当的话），就会发生堆芯损坏。[17] 此外，还可以指定其他不良后果的标准，如反应堆容器冷超压、反应性瞬变或乏燃料水池沸腾。

5.44. 通常通过采用间接标准来确定什么构成堆芯损坏。例如，对于压水堆，堆芯损坏被认为是在长时间开放堆芯或超过最高规定包壳温度后发生的。如果在开放堆芯后需要相当长的时间间隔才能造成堆芯损坏，则在制定堆芯损坏的现实定义时应当考虑到这一点。

---

[16] 可以指定几种安全稳定状态（例如热备用、冷停堆）。

[17] 对于不同程度的损坏，可以指定几种堆芯损坏状态。例如，在通道型反应堆中，通常根据后果的严重程度来考虑对不同通道的损坏。（对于 CANDU 和 RBMK 型反应堆，严重堆芯损坏定义为由于过热导致多个燃料通道的广泛实物损坏，导致堆芯结构完整性丧失。）

安全功能和成功标准

5.45. 应对每组始发事件进行事故序列分析（见第 5.32－5.40 段）。

5.46. 对于需要长期措施以确保安全和稳定的最终状态序列，事故序列分析应当以能够分析长期措施效果的方式进行。这将使分析人员能够确保与长期措施的潜在故障相关的风险可以忽略不计，并适当捕捉可能的陡边效应。

5.47. 应当为每组始发事件确定防止堆芯损坏所需执行的安全功能。所需的安全功能将取决于反应堆类型和始发事件的性质，通常包括以下内容：

(a) 关闭反应堆并保持次临界状态；

(b) 从反应堆堆芯散热；

(c) 保持一回路的完整。

5.48. 应当确定执行这些安全功能所需的信用系统和运行人员的行动，以及相关的成功标准。

5.49. 运行人员为使设备达到安全稳定状态所需采取的行动应当在分析设备程序的基础上确定。在电厂运行人员、系统分析人员和人的可靠性分析人员之间合作确定这些行动是一种良好的实践。

5.50. 成功标准应当界定履行安全功能所需的每个信用系统（包括具有辅助功能的系统，如供水系统和供电系统）的最低性能水平，同时考虑到每个序列的特定特点。如果涉及信用系统的冗余通道，成功标准应当定义为保持运行所需的通道数量。如果涉及多个信用系统，成功标准应当考虑到每个系统所需的性能。这可能包括由安全分析支持的每个系统的部分运行，并提供足够的细节以提供可接受的正当性。

5.51. 运行人员每次行动的成功标准应当考虑从根据可用信息启动行动到首次行动无法实现安全功能之间的时间（考虑诊断和采取行动所需的时间）。

5.52. 在明确成功标准时，应当确定并考虑因缓解始发事件而受到影响但会因始发事件而故障的系统和部件。这种情况的示例是，始发事件涉及电力或冷却水系统等支持系统的故障，或者始发事件在被认为缓解事件的设备所在的区域产生恶劣环境。这两种情况都可能导致必要系统的故障。在

压水堆中发生大量或中度冷却剂丧失事故的情况下，如果连接到反应堆的任何管段发生断裂，则连接到该管段的应急堆芯冷却系统通道的流量将会丧失。

5.53. 成功标准应当规定信用系统的任务时间。在许多情况下，对于大多数始发事件，这被认为是 24 小时或 48 小时。应当充分界定任务时间，以捕捉可能的陡边效应，并确保任务时间过后产生的残留风险可以忽略不计。

5.54. 对于每个始发事件，一级概率安全评定文件应当包括使反应堆达到安全稳定状态所必需的安全功能、信用系统和运行人员行动的清单，以及相关的成功标准。

成功标准的支持规范分析

5.55. 信用系统的成功标准应当通过支持分析加以判断。支持分析包括瞬变和冷却剂丧失事故后衰变热去除的热力学分析，以及反应堆关闭和维持稳定的中子分析。支持分析应当尽可能基于电厂特定数据，并应当符合使用鉴定和验证计算机代码的最佳实践。

5.56. 在可能的情况下，应当在一级概率安全评定中定义和使用基于最佳估计支持分析的现实成功标准（见 SSG-2（Rev.1）[5]）。

5.57. 如果基于保守设计基准分析的保守成功标准已在任何事故序列中的一些信用系统的一级概率安全评定中使用，则应当注意这一点，并应当仔细评审整体分析的结果，以确保这种保守不会主导风险，从而模糊一级概率安全评定洞察。

5.58. 计算机代码只能在其既定的适用范围内使用，并且只能由合格的代码用户使用。

事故序列建模

5.59. 应当确定每组始发事件后可能发生的事故序列。这可以通过为每组始发事件构建事件树来实现，该事件树模拟信用系统、支持系统和人在执行安全功能时的行动的成功或失败。在构建事件树之前，绘制包含人交互的详细事件序列图被认为是一种良好的实践。

5.60. 始发事件组的事件树应当解决所有需要执行的安全功能和需要按照成功标准规定运行的信用系统。特定事件树的标题通常对应于始发事件组的前线信用系统的状态（即成功或失败）。标题还可以包括运行人员直接影响事故过程的任何行动，特别是根据应急运行程序采取的行动。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。

5.61. 事件树的结构应当考虑事件树标题中出现事件的时间序列，代表运行人员的行动或系统驱动。最自然的方式是按照对系统或运行人员提出要求的时间序列，按时间序列排列标题。然而，标题有时可以用另一种方式排序，以简化依赖关系的处理或减小模式大小。

5.62. 事件树的结构应当考虑到可能因始发事件、设备故障或人为错误而产生的功能和实物依赖性（见第 5.90 段）。

5.63. 事故序列分析应当涵盖响应一组始发事件的信用系统成功或失败的所有相关组合，并应当确定导致成功结果的所有事故序列，其中足够数量的信用系统已正确运行，以实现始发事件的所有必要安全功能，或导致堆芯损坏状态。

事故序列的最终状态与电厂损坏状态

5.64. 事故序列分析将确定 (i) 所有要求的安全功能都已实现从而不会发生堆芯损坏（或其他不良后果）的事故序列；以及 (ii) 一个或多个安全功能未实现从而假想发生堆芯损坏的事故序列。如果分析以一级概率安全评定结束，这种区别通常就足够了。但是，如果目的是使用一级概率安全评定的结果作为二级概率安全评定的输入，一般实践是将导致堆芯损坏的事故序列分组到电厂损坏状态中，这将是形成一级概率安全评定和二级概率安全评定之间接口的起点。电厂损坏状态是根据二级概率安全评定的需要规定的（见 SSG-4[4]），但可以有效地包括在一级概率安全评定建模中，然后在实施二级概率安全评定时进行相应的更新。

5.65. 如果正在进行二级概率安全评定，则应当定义一套核电厂损坏状态，其中应当考虑到导致堆芯损坏的每个事故序列的特征，这些堆芯损坏可能会影响安全壳响应或导致放射性物质向环境中排放。电厂损坏状态应当由

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共同确定（见SSG-4[4]）。[18]

5.66. 为电厂损坏状态指定的特征通常由分析人员确定，但特别包括以下内容：

(a) 已经发生的始发事件的类型（例如，一回路完好的始发事件或冷却剂丧失事故）；
(b) 信用系统（如反应堆保护系统、余热排出系统或应急堆芯冷却系统）发生故障，导致堆芯损坏；
(c) 堆芯损坏时一回路压力的状态（例如高或低）；
(d) 堆芯损坏发生的时间（例如，相对于反应堆跳堆时间的早或晚）；
(e) 安全壳的完整性（例如，完整、故障、隔离故障、由于蒸汽发生器管破裂或接口系统冷却剂丧失事故而被旁路）；
(f) 有或没有压力抑制能力的冷却剂丧失事故（例如沸水堆）；
(g) 发生堆芯损坏时（例如沸水堆）水池的状态（过冷或饱和）；
(h) 安全壳保护系统的可用性（例如安全壳喷淋、散热系统和氢气混合或重组器）；
(i) 交流和直流电源的可用性以及相关的恢复时间；
(j) 运行人员尝试过但失败的操作。

以上清单适用于功率运行概率安全评定。适用于关闭状态的额外特征在第9.34段提供。

5.67. 因此，导致堆芯损坏的事故序列（符合第5.43段规定的标准）应当根据每个事故序列导致核电厂的一般实物状态以及可能存在的可预防或缓解放射性物质泄漏的信用系统来表征。

5.68. 一级概率安全评定文件应当提供已绘制的事件树，以确定事故序列如何进展。应当给出事件树结构背后的逻辑描述来帮助理解，因为事件树图本身不提供推理，只提供推理的结果。还应当提供关于事件树标题的解释性信息（例如，标题是代表简单功能还是一个标题下包含多个功能的复

[18] 涉及严重堆芯损坏和安全壳子系统故障的一级概率安全评定最终状态的组合可以通过接口事件树产生（见SSG-4[4]）。

合事件）。在制定事件树和相应的标题定义时所做的假设应当清楚地提出并说明正当性。

5.69. 文件还应当描述电厂损坏状态并应当描述如何指定这些状态。

系统分析

5.70. 分析的下一步是对事故序列分析中确定的信用系统故障进行建模。如果这是通过故障树分析来完成的，那么故障树的顶部事件被作为由事件树分析识别的信用系统故障状态。故障树将分析扩展到单一基准事件的级别，这些事件通常包括部件故障（例如，泵、阀门或柴油发电机的故障）、维护或试验期间部件的不可用、冗余部件的共因故障以及代表人为错误影响的人因故障事件。

5.71. 需要绘制故障树的范围取决于事件树的大小和复杂程度，事件树越详细，故障树就越不复杂。[19]

故障树分析

5.72. 故障树可用于为由事件树分析识别的所有信用系统故障状态提供完整的逻辑故障模式。

5.73. 为每个安全功能提供故障树顶部事件的故障标准应当是第 5.50－5.58 段规定的事故序列成功标准的逆向逻辑。在某些情况下，根据系统需求之前的事件序列，同一信用系统可能需要一个以上的故障树模式来处理为不同的始发事件组或事件树的不同分支中指定的成功标准。这可以通过制定不同的故障树模式或使用逻辑开关（称为内部事件）来禁用或启用故障树模式的适当部分来实现，这取决于成功标准。

5.74. 故障树中建模的基准事件应当与部件故障的可用数据一致。故障树中建模的部件边界和部件故障模式应当与部件故障数据中定义的一致。这对于能动部件和非能动部件都同样有效。

[19] 其它技术是可能的，并且可用于概率安全评定的特定方面。然而，通常的方法是使用事件树和故障树的组合，这种方法被认为在本出版物中使用（见第 5.4－5.6 段）。

5.75. 故障树模式应当制定到单一部件（如泵、阀门、柴油发电机）的显著故障模式和单一人为错误的水平，并应当包括所有可能直接或与其他基准事件结合导致故障树顶部事件的基准事件。分析的详细程度通常由分析人员决定，但应当足以捕捉可能的相关性，并应当与部件故障的可用数据和一级概率安全评定的建议应用保持一致。

5.76. 要在故障树中建模的一组基准事件应当通过系统分析（例如，通过作为设计评定的一部分进行的故障模式和影响分析，以确定重要部件的故障模式）和通过在任务分析支持下对运行人员的行动进行评审，以确定潜在的人为错误。

5.77. 故障树模式应当包括信用系统中需要运行的所有部件，包括支持系统部件。它还应当包括其故障可能影响系统运行的非能动部件（如过滤器堵塞、管道泄漏）。故障树模式应当以确保明确考虑依赖性的方式制定。省略这些依赖性的显式建模可能会使结果产生显著偏差，并导致低估支持系统的相对重要性。

5.78. 故障树中部件的分辨率应当足以确保所有硬件依赖性都可以建模。例如，当同一系统向多个部件提供冷却水时，该冷却水系统应当明确建模。在确定分辨率时，还应当考虑部件可靠性的可用数据。例如，可靠性数据可能适用于整个泵，但不适用于其组成部分，如旋转轮、联轴器和轴承。此外，当定义故障树中部件的分辨率时，应当考虑概率安全评定在电厂设备或设备单一部件的风险重要性方面的洞察。

5.79. 当单一部件被组合在一起，并使用一个复合事件来模拟它们的故障时，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本身相同。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（即任何单一部件都应当不出现在一个以上的复合事件中，或者作为一个基准事件出现在其他地方）。

5.80. 故障树模式应当考虑到信用系统中的单一部件或设备组，这些部件或设备组可能会在电厂寿命期间因试验、维护或维修而停止使用。该类部件或设备通道应当在故障树分析中明确识别和建模。例如，这可以通过在故障树中包含基准事件来表示部件大修去实现。

5.81. 由于试验和维护而导致系统不可用应当以符合电厂技术规范[20]、电厂试验和维护实践以及运行经验（如有）的方式进行建模。

5.82. 应当制定一个系统，用于唯一地编码或标记故障树模式中的每个逻辑门和基准事件，并且该系统应当在为一级概率安全评定制定的整个逻辑模式中一致地使用。

5.83. 模式的制定应当与一级概率安全评定的拟议应用保持一致。例如，如果一级概率安全评定用于风险监控应用，模式应当是对称的，以便它明确地模拟所有可能发生事件位置的始发事件，包括所有一回路、信用系统的所有通道以及正常运行系统的所有运行和备用通道。对称模式的制定将允许以直接的方式使用由一级概率安全评定代码计算的重要性测量（重要性测量的示例见第 5.171 段）。

系统信息

5.84. 应当为一级概率安全评定中的每个系统提供功能描述，以确保正在制定的逻辑模式具有有效和可监查的基础。功能描述通常包括以下内容：

(a) 系统的功能及其运行模式；
(b) 系统边界；
(c) 与其他系统的接口；
(d) 系统的潜在故障模式；
(e) 正在建模的运行状态（对于具有一个以上状态的系统）；
(f) 需要运行或改变其状态和正常配置的部件；
(g) 部件运行是手动还是自动；
(h) 部件接收自动信号所需存在的条件。

5.85. 应当为每个信用系统提供一个简化的示意图，显示故障树中的系统模式，包括以下内容：

(a) 故障树中建模的所有系统部件；
(b) 部件在正常运行期间的配置；

[20] 在维护大修建模时，一般假设电厂在技术规范规定的运行限值和条件内运行。

(c) 连接所述部件的管段或布线段；

(d) 支持系统接口（如电源、仪器仪表和控制、冷却、通风）。

5.86. 为信用系统提供的功能描述和示意图应当为故障树的制定提供明确的基础。一级概率安全评定文件应当解释如何在故障树的制定中使用这些信息。

相关故障的分析

5.87. 应当特别考虑为一级概率安全评定制定的逻辑模式中依赖性的处理。在过去进行的概率安全评定中，相关故障经常被发现是堆芯损坏频率的主要贡献者之一。

5.88. 可能出现四种不同类型的依赖关系：

(a) 功能依赖性包括由电厂工况导致依赖性（例如，减压失败导致低压注入不可用）和由共享部件、公共驱动系统、公共隔离要求或公共支持系统（例如，电力、仪器仪表和控制、冷却、通风）导致依赖性。

(b) 实物依赖性（也称为空间交互依赖性），这是由于可能导致可信的结构、系统和部件故障的始发事件造成的。管道抖动、飞射物撞击、喷射冲击或环境影响都可能导致故障。

(c) 由于电厂人员所犯的错误而导致人与人之间的相互依赖关系，这些错误会促成或导致始发事件，或导致一个或多个可信的结构、系统和部件项目的不可用性或故障，以至于它们在始发事件后无法在需要时运行。

(d) 由于设计相似性、制造或安装错误或电厂人员在电厂运行期间犯下的错误而导致部件故障依赖性。通过共因故障分析解决了这些问题（见第 5.93－5.96 段）。

5.89. 应对电厂的设计和运行进行系统化评审，以确定可能出现的所有潜在依赖性，这些依赖性可能导致信用系统的部件不可用或其可靠性降低，以防止始发事件。

5.90. 所有功能和实物依赖都应当明确建模。还应对人工交互依赖和部件故障依赖进行建模，关于共因故障分析的第 5.93－5.96 段和关于人的可靠性分析的第 5.97－5.122 段将进一步讨论这些问题。

5.91. 在故障树模式中，应当考虑系统中可能出现的所有功能依赖。这些应当在概率安全评定模式中明确识别和建模。对于分析人员来说，将所有这些依赖关系清单在系统依赖关系矩阵中是一个很好的实践，这可以用作构建故障树的基础，并且在检查它们时对评审人员很有帮助。在系统的共因故障概率中，功能相关性应当不包括在部件故障相关性中。

5.92. 由于共享部件或支持系统而可能出现的系统间功能依赖关系应当在故障树分析中明确识别和建模。在链接事件树方法中（见第 5.5 段），系统间功能依赖可以使用边界条件方法来解决。这种依赖性可能出现在执行相同安全功能的独立信用系统或相关的支持系统中。这些需要明确地包含在故障树中。

常见故障原因的分析

5.93. 应当识别可能出现部件故障依赖性的冗余设备组，并将其纳入这些部件共因故障的一级概率安全评定模式中。有多种方法可用于模拟一级概率安全评定中的共因故障，所选择的方法应当尽可能得到数据收集的支持。解决系统内和系统间的共因故障事件被认为是一种良好实践。

5.94. 应当使用概率安全评定软件的适当功能识别和建模可能影响冗余部件组的共因故障，这通常在故障树中完成。分析应当确定所有相关部件组和故障模式。关于共因故障防御的任何假设应当在一级概率安全评定文件中说明。

5.95. 应当为一级概率安全评定中包含的每种部件故障模式使用的共因故障概率提供正当性。这一正当性应当考虑到系统的冗余程度，部件的设计方面，根据分离、隔离和设备鉴定水平的系统布局，以及系统的运行、试验和维护实践。

5.96. 在可能的情况下，共因故障概率应当基于电厂的特定数据，并应当考虑一般数据和类似电厂的运行数据。如果一般共因故障参数用于计算共因故障概率，应当分析并证明这些值的适用性。要使用的一般数据源中的

部件边界、故障模式和故障根本原因应当与概率安全评定中假想一致。如果使用专家判断来分配共因故障参数（当既没有电厂特定数据也没有一般数据时），应当为数据提供适当的正当性。指定的不确定性参数应当与指定共因故障参数过程中的不确定性相称。新的核电厂设计阶段的概率安全评定就是一个只有一般数据的示例。

人的可靠性分析

5.97. 应当识别可能导致安全功能故障或信用系统故障的人为错误，并将其纳入逻辑模式。应当采用结构化和系统化的方法来识别人因故障事件，将该型事件的影响纳入电厂逻辑模式（即事件树和故障树），并量化该型事件的概率（即人为错误概率）。结构化和系统化的方法将使人们相信，全面的分析已经进行了确定所有类型的人因故障事件对堆芯损坏频率的贡献。一个有用的起点是对照通常用于确保采取人的可靠性分析所有必要步骤的方法之一来检查所选方法。

5.98. 第5.99－5.121段提供的建议涉及一级概率安全评定中用于人的可靠性分析的最常用方法（见参考文献[17]）。人的可靠性分析过程应当包括以下四个迭代步骤：

(1) 概率安全评定中要考虑的人因故障事件的识别和定义；
(2) 人因故障事件的定性评定；
(3) 人因故障事件的定量评定；
(4) 整合到概率安全评定模式中。

5.99. 有各种各样的方法可用于人的可靠性分析，这一领域的技术水平仍在不断发展。所选择的方法应当得到一致和正确的应用和记录。当人的可靠性分析方法在其原始范围之外使用或被专家判断补充或取代时，该过程应当清楚地记录，并有足够的正当性支持适当的人的可靠性分析过程。

5.100. 人的可靠性分析中定量评定的目的应当是在一级概率安全评定的所有部分产生彼此一致的人为错误的概率。[21]

[21] 还需要讨论人为错误概率背后的建模不确定性，因为这种讨论为敏感性分析提供了基础，并增加了对人为错误概率值的信心。

5.101. 人的可靠性分析应当与电厂运行和维护人员密切合作进行，以确保分析反映电厂的设计特点及其运行状态和事故工况下的运行。如果这是不可能的（例如，如果在设计阶段对电厂进行分析），分析人员应当使用来自类似电厂的信息，或者应当清楚地说明他们分析所基于的假设。

人因故障事件的识别与定义

5.102. 对于包括在一级概率安全评定中的所有类型的人因故障事件的识别和定义，应当应用结构化和系统化的程序。

5.103. 人的可靠性分析应当包括在始发事件之前发生的人因故障事件，这些事件有可能导致信用系统的故障或不可用（即 A 型人因故障事件）。这些事件可能发生在视察、维护、试验、维修或校准任务期间。如果事件仍未被检测到，则在始发事件后需要时，受影响的部件或部件组将不可用。特别重要的是有可能导致多通道信用系统同时不可用的故障事件。这些不可用性的来源包括在部件、通道或系统级别的模式中。

5.104. 应对电厂程序进行系统化评审，以确定运行人员对信用系统进行视察、维护、试验、维修和校准任务期间可能发生的人因故障事件（A 型人因故障事件）。评审应当确定该型事件发生的可能性以及这些潜在事件对可信的结构、系统和部件不可用或故障的影响。

5.105. 应对电厂程序和运行经验进行系统化评审，以确定可能导致始发事件的潜在人因故障事件（B 型人因故障事件）。至少，应当检查在分析中使用的始发事件频率的评价中是否考虑了这些类型的人因故障事件。

5.106. 应对电厂程序进行系统化评审，以确定在始发事件发生后运行人员采取关键行动期间可能发生的人因故障事件（C 型人因故障事件）。评审应当确定人因故障事件发生的可能性，以及这些潜在错误对事故假想方案发展以及部件、系统或安全功能的不可用性或故障的影响。C 型人因故障事件通常对堆芯损坏频率有显著贡献。

5.107. 应考虑显著的调试错误（即错误地执行必要的任务或行动，或执行不必要的无关任务，这可能会加剧事故的进展或导致始发事件）。因此，可能会产生额外的事故序列。虽然对调试错误的系统建模尚未成为普遍实践，但它可以提供有用的洞察，以改善人机界面并减少调试错误的可能性（见参考文献[17]）。

5.108. 只有在有充分正当性证明其可行性的情况下，维修措施（如更换阀门上的电机，使其能够运行）才应当计入概率安全评定。人的可靠性分析技术不能总是用于维修行动，因为维修方法取决于具体情况。如果已知特定序列设备的特定故障模式，并且 (i) 可以快速诊断故障；(ii) 备件和维修人员可用；(iii) 执行维修所需的环境和工作条件到位或可以得到保证；以及 (iv) 时间窗口足够长，可以可信地假设维修的可能性，包括将备件和维修人员带到电厂所需的时间。在概率安全评定背景下，恢复被定义为通过克服或补偿结构、系统和部件故障来复原因结构、系统和部件故障而失去的功能。恢复可以由运行人员处理，而维修则不能。应当记录恢复和维修行动的适当性。

5.109. 可能被视为“英雄”的行动（例如，运行人员进入辐射水平极高的环境执行该行动）或在没有任何程序指导或培训的情况下执行的行动应当不作为正常实践纳入或计入分析，尽管可能有正当性的例外情况（例如，在长期事件的情况下）。

5.110. 在部署便携式设备的背景下，对人的可靠性评定应当遵守与整体人的可靠性分析过程相同的一般原则。如果所应用的人的可靠性分析方法没有解决与部署便携式设备相关的所有关键人的绩效因素，则应当对该方法进行调整和补充，以考虑这些绩效因素。

人因故障事件的定性评定

5.111. 人因故障事件的定性评定应当包括收集、分析和记录与分析人员理解正在进行人的可靠性分析的人因故障事件中涉及人员任务相关的信息。

5.112. 应当酌情从下列来源收集资料：

(a) 程序导则；
(b) 参观相关电厂位置；
(c) 评审运行经验；
(d) 与运行人员和教员的访谈、谈话和巡查；
(e) 关于运行人员在电厂模拟机中表现的信息；
(f) 热力学分析；
(g) 概率安全评定的其他部分，通常是系统分析笔记本和事故序列分析。

5.113. 定性评定应当导致人因故障事件的表征，以便能够充分进行量化和建模。通常通过以下主要活动实现这一表征：

(a) 任务分析，以详细洞察满足与人因故障事件相关的成功标准所需的活动；

(b) 背景表征，以表征定义人因故障事件所涵盖的人类行动的假想方案和绩效条件（例如，时间约束、程序指导、相关线索）；

(c) 错误识别，以识别导致人因故障事件的认知和人类行动；

(d) 错误表征描述，以确定、证明和表征从识别的错误中恢复的可能性和机制。

定性评定的这些活动对所有类型的人因故障事件（即 A 型、B 型和 C 型事件）和概率安全评定的所有领域都有效（见参考文献[17]）.

5.114. 对于新设计的核电厂，第 5.113 段列出的许多定性信息来源可能不可用。在这种情况下，应当使用类似电厂的信息。如果做不到这一点，应当对上述活动进行专家判断。在任何情况下，定性信息与实际电厂状态的对应关系应当在以后进行核实，概率安全评定应当在必要时进行更新。

人因故障事件的定量评定

5.115. 推导人为错误概率应当针对特定假想方案，并应当反映可能影响运行性能的因素人员，包括压力水平、执行任务的可用时间、运行程序的可用性、提供的培训水平和环境条件。还应当酌情考虑其他相关因素。这些因素（通常称为“绩效形成因素”）应当通过定性评定加以确定。[22]

5.116. 用于推导人为错误概率的方法应当与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使用是正当的。

5.117. 虽然不同类型的人因故障事件（即 A 型、B 型和 C 型事件）可能采用不同的量化方法，但应当使用相同的人的可靠性分析方法（即人的可靠性分析方法或方法组合）来评定类似类型的人因故障事件，以确保分析的一致性。如果对同一类型的人因故障事件使用不同的方法，应当记录选择它们的原因。

[22] 我们认识到，电厂的安全文化也会影响人为错误的概率。然而，目前在评定人为错误概率时，还没有公认的考虑安全文化的方法。

5.118. 应当评定人因故障事件的风险重要性 [23]，以确定应当进行更详细分析的事件。人因故障事件的量化通常分两个阶段进行：

(1) 筛选评定，其中应用了简单的量化模式；
(2) 详细评定，其中考虑了更多因素，并更详细地描述了背景，特别是运行人员采取的最具风险的重大行动。

在这种方法中，应当确保在筛选评定阶段之后准确描述人因故障事件的风险重要性，以便可以识别需要更详细评定的风险显著的人因故障事件。

5.119. 针对内部和外部危害的 C 型人因故障事件的评定应当包括以下内容：

(a) 包含在内部始发事件的一级概率安全评定中的人因故障事件，但也与内部或外部危害导致假想方案相关。在这种情况下，可能有必要修订对绩效影响因素的评定，因为运行人员实施行动可能比基本情况下更困难（例如，由于与危害环境相关的压力水平更高）。
(b) 仅与特定危害相关的人因故障事件（例如，使用便携式消防设备灭火）。用于评定特定危害的人因故障事件的方法通常可以遵守与用于分析其他类型的人因故障事件方法相同的原则。
(c) 运行人员对虚假警报和指示的不良响应。相关运行人员识别和评定不良行为的更多信息见参考文献[18]。

第 7 部分和第 8 部分提供了关于特定危害人的可靠性分析的进一步建议。

人因故障事件之间依赖关系的处理

5.120. 相关人因故障事件的分析应当嵌入到整个人的可靠性分析过程中（即识别、定性评定、定量评定、将人因故障事件整合到概率安全评定模式中）。逻辑模式中包含的单一人因故障事件之间的相互依赖性是可能的。这种相互依赖性可能源于共同线索或程序步骤的使用、电厂程序的结构或内容导致认知耦合、诊断和响应计划的驱动因素或采取响应行动条件的相似性。同一序列中人因故障事件之间的相关性（如有）会显著增加人为错误的概率。在分析中，应当识别和量化人因故障事件之间的相互依赖性。

[23] 术语“重要风险”和“显著风险”都是概率安全评定从业人员常用的术语，可以互换使用。

5.121. 应当识别涉及多个人因故障事件的所有最小割集或假想方案。[24] 应当评审相同的最小割集或假想方案，以确定它们之间的依赖程度，模式量化中使用的人为错误概率应当反映这种依赖程度。

概率安全评定模式中人因故障事件的集成

5.122. 人因故障事件应当作为基准事件纳入逻辑模式。根据人因故障事件的定义和影响，相应的基准事件可以出现在系统故障树中的适当级别，也可以表示事件树标题。恢复类型的人因故障事件也可以在量化的后处理阶段实施。整合步骤应当包括对最小割集的彻底检验，以核实人因故障事件是否已被正确整合。这一检验应当包括一个步骤，以确定可能需要进行依赖性评定的人因故障事件的组合（见第 5.120 段和第 5.121 段）。

其他建模问题

非能动系统

5.123. 概率安全评定中应当考虑评定非能动系统的功能可靠性，以令人满意地执行其安全功能（即评定其故障概率）。第 5.124－5.129 段涉及包含移动流体或膨胀固体结构、直接作用设备和贮存能源的非能动系统（即 B、C 和 D 类非能动系统，定义见参考文献[19]）。非能动系统功能（包括可靠性和可用性）的演示通常涉及一种或多种技术的使用，如热工水力计算、验证、专家判断、试验和性能监控。

5.124. 非能动系统的可靠性评定应当解决特定非能动特点，这些特点可能与能动运行系统和部件的特点有很大不同。能动安全和非能动安全概念的区别在于它们的工程结构、系统和部件是否依赖于外部机械和/或电力、信号或动力。在非能动系统中，不依赖外部输入意味着依赖自然法则、材料特性、内部贮存的能量或容量以及环境条件。当采用非能动安全时，能动系统故障的潜在原因，如缺乏人工操作或电源故障可以被消除。不仅要洞察个人所涉及的过程，以及它们如何相互结合。这些过程及其组合定义了系统的实际性能，可以根据系统内部件的状态条件、边界条件和故障或失效的变化而变化。

---

[24] 这可以通过将人为错误概率设置为高值（例如 0.9）并重新计算堆芯损坏频率来实现，涉及多个人因故障事件的最小割集将出现在最小割集清单的顶部。

5.125. 由于非能动安全系统（尤其是热工液压系统）通常比能动安全系统依赖更小的驱动力，它们对环境和边界条件更敏感。因此，非能动系统的可靠性评定应当涵盖可能影响环境和其他边界条件的故障机制和事件，如影响自然现象的条件，以有效缓解非能动系统特有的事故工况和机械或结构退化（包括老化效应）。例如，自然循环可能会因非凝性气体、堵塞、错误的阀门位置、杂质、腐蚀、储罐中的藻类、维护错误或系统中的异物而受损或受阻。非能动系统部件的潜在缺陷（例如，由于不适当的构造导致管道的非期望倾斜）也可能由于驱动力的低幅度而降低某些非能动系统的性能。

5.126. 非能动系统的可靠性评定还应当考虑定期试验和维护实践或计划程序，因为该类实践或程序可能对非能动系统的可靠性产生显著影响。例如，来自定期试验和维护的反馈（如果存在）可能揭示与老化相关的材料退化，或者可能证明需要修改试验或维护策略。

5.127. 非能动系统和部件可靠性评定的一般方法应当类似于概率安全评定中考虑的其他系统的方法。应当特别强调获得与概率安全评定相关的系统故障模式已被正确定义以及相关故障概率已以正当的方式进行评定的信心。因此，为了评定非能动系统的可靠性，可能需要制定一种基于模式的方法（见参考文献[20]）和/或其他技术，如试验和专家判断。

5.128. 非能动系统的可靠性评定应当包括以下几个阶段：

(a) 系统表征，以定义系统的任务、相关的事故假想方案、故障模式和成功或失败标准；
(b) 识别系统故障机制；
(c) 系统建模，以便能够考虑各种条件下的系统性能；
(d) 识别系统模式和输入数据中的相关参数和不确定性来源；
(e) 不确定性的量化（使用现有技术考虑偶然和认知不确定性）以产生系统的可靠性估计。

5.129. 共因故障是非能动系统最重要的故障模式之一，也是应当考虑的。通常，对于 C 类和 D 类非能动系统，使用冗余通道中类似部件的标准技术来评定运动部件或仪器仪表和控制部件的共因故障。然而，对于 B 类非能动系统，所有系统序列的系统故障原因可能是相同的。如果冗余通道的相

关故障可能与任何单一通道具有相同或接近相同的概率，这应当反映在非能动系统模式中。

基于软件的系统

5.130. 概率安全评定中应当考虑基于软件的系统的可靠性评定，这些系统被认为是确保安全功能的结构、系统和部件或可能导致始发事件的结构、系统和部件。在这种情况下，基于软件的系统被假定为包括具有可编程模块的各种仪器仪表和控制设备。

5.131. 从概率安全评定的角度来看，基于系统的风险重要性，应当使用分级方法来确定基于软件的系统的可靠性评定的范围和方法。例如，用于控制反应堆保护系统、反应堆控制系统或其他风险显著系统的基于计算机的系统预计需要比风险较低的显著仪器仪表和控制系统的可编程部件更详细的分析。考虑到系统的架构和安全分级，可以采用评定基于软件的系统可靠性的简化方法进行建模。

5.132. 运行人员界面系统的可靠性评定应当通过正常的概率安全评定故障树和事件树建模考虑其他仪器仪表和控制系统故障依赖性，其中事故序列中较早记录的系统故障通常是级联的。应当考虑不同仪器仪表和控制系统之间的运行人员和相关运行人员接口系统的相互依赖性。对于那些以简化方式建模的可编程运行人员界面系统，应当为分析中的局限性提供正当性。

5.133. 基于软件的系统可靠性评定应当涵盖硬件和软件部件以及这些系统的可编程逻辑设备的配置数据。对基于软件系统的可靠性建模是一个挑战，因为标准的统计方法对软件模块的适用性有限。

5.134. 对于任何系统分析，数字系统可靠性评定的首要任务应当是确定系统的范围及其概率安全评定相关任务。这里，还应当注意系统任务，如果虚假驱动，可能会对安全功能产生不利影响并导致始发事件，这也需要考虑。此外，应当分析仪器仪表和控制系统之间的相互作用，以确定所考虑的系统任务的系统依赖性。

5.135. 基于软件的系统分析应当足够详细，以捕捉系统的功能相关故障模式以及系统之间的依赖关系。故障模式“无法驱动某些仪器仪表和控制功能”和“虚假驱动”都应当考虑在内。所需的详细程度取决于仪器仪表和控制架构以及系统的容错特点，可能需要对故障（包括共因故障）进行详

细的功能分析，以帮助决定所需的详细程度。当使用更简化的模式时，它们至少应当在系统开发中使用的故障分析确定的主要故障模式（见参考文献[21]）。

5.136. 在可编程部件（如处理器、通信模块、传感器、驱动器）的分析中，起点应当是考虑部件（如模块、子部件）的硬件和软件部分，然后在必要和可行的情况下，以及在适用数据可用的情况下，进一步分别分析该硬件和软件。可编程部件的可靠性评定应当包括部件分析中所选详细程度的正当性。参考文献[21]提供了数字仪器仪表和控制系统故障模式分类的示例。

5.137. 硬件模块的可靠性应当使用标准技术进行评定，前提是这些技术能够模拟系统行为、故障模式和识别的依赖性。

5.138. 软件模块的可靠性评定应当包括对现有运行经验（包括来自其他核电厂或其他工业应用的经验）的评定和对制定过程（包括验证和核实过程）的评定，以获得对所提供的可靠性估计的尽可能多的信心。软件模块的可靠性评定仍然是一个挑战，公认的工业实践仍有待建立。[25] 相关更多信息见参考文献[22]。

5.139. 对自动功能（包括可编程系统功能）丧失所采取的恢复行动的处理应当与主控制室设计的人因故障事件模式、最低限度警报和控制库存相协调。如果恢复行动被记入备份自动功能的丧失（如数字系统功能），则应当考虑与仪器仪表丧失相关的可能依赖性。

5.140. 包括通信网络在内的可编程系统的可靠性评定应当包括系统间共因故障的评定。应当注意执行类似或相同功能的计算机系统。如果识别了两个计算机系统的硬件和软件的可信依赖性，则应当在一级概率安全评定中予以考虑。

5.141. 应当识别和解决数字系统和数据建模中的不确定性，至少是定性的不确定性。还应当解决数据不确定性问题。

---

[25] 评定方法的适用性取决于软件模块的类型（如操作系统、应用软件）和所考虑的故障模式，但在实践中，所有方法在产生正当的可靠性数字方面都有局限性，正如概率安全评定所期望的那样。已经注意到故障模式的识别以及动态相互作用和数据的建模存在很大的不确定性（见参考文献[22]）。在风险知情应用中使用概率安全评定时，需要考虑到这一点和软件故障。

5.142. 原子能机构《安全标准丛书》第 SSG-39 号《核电厂仪器仪表和控制系统的设计》[23]第 2.76 段指出：“在[仪器仪表和控制]系统的设计中，必须考虑从概率安全评定中获得的洞察。”仪器仪表和控制系统可靠性的推导应当得到证实，并基于国际公认的方法，假设应当记录在案并证明其正当性。在这方面，各国的实践各不相同。一些国家期望对硬件造成的仪器仪表和控制系统故障的概率进行定量估计对于其他状态，设计错误（包括软件错误）及其后果只能通过对架构和设计的定性分析来充分处理。一些将数字可靠性应当用于软件的国家已经为软件可靠性声明建立了数字限值。

一级概率安全评定数据

5.143. GSR Part 4（Rev.1）[3]要求 19 规定：**“必须收集和评定运行安全性能的数据。”**

5.144. 如果电厂的特定经验有限或缺乏，需要解决的一个主要问题是现有数据是否适用于所考虑的电厂设备设计和运行机制。

5.145. 应当尽可能使用电厂特定数据，如果可以证明这些数据是相关的，则由类似电厂的数据补充，从而提供更广泛的数据。然而，对于设计概率安全评定、新的电厂或仅运行相对较短时间的电厂，电厂特定数据不可用。在这种情况下，应当使用类似电厂的数据，如果没有这些数据，应当使用所有类型核电厂运行的一般数据。

5.146. 应当为用于一级概率安全评定数据提供正当性。在提供这种正当性时，良好的实践是比较各种来源的数据，并确定是否可以解释任何差异。一般来说，在选择最佳数据来源时需要做出判断。

5.147. 如果要使用不同来源的电厂特定数据和一般数据的组合，应当提供选择特定数据或合并来自一个以上来源的数据所用方法的正当性。这可以使用贝叶斯方法或通过工程判断来完成。

5.148. 对于一级概率安全评定中使用的参数，不仅要得出点估计值，还要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。

始发事件的频率

5.149. 应当为一级概率安全评定中模拟的每个始发事件或一组始发事件分配一个频率。组的频率应当是分配给该组的所有单一始发事件的频率之和。频率应当以每个反应堆年的发生次数来表示，以便频率说明核电厂处于适用的电厂运行状态的时间分数。

5.150. 除了第 5.143－5.148 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，该故障树提供了所有设备故障和人为错误的逻辑模式，这些故障和人为错误可以结合起来并导致始发事件。应当检查故障树产生的预测是否与运行经验一致。如果从故障树分析中获得的结果与运行经验不一致，应当根据一级概率安全评定的预期应用重新考虑这些结果。

5.151. 为频繁始发事件分配的频率应当与所考虑电厂的运行经验一致，如果相关，也应当与类似电厂的运行经验一致。

5.152. 一级概率安全评定文件应当描述为电厂确定的每个始发事件或一组始发事件，以及始发事件频率的平均值、分配给它的数值的正当性和不确定性水平的指示。

部件故障概率

5.153. 故障概率应当分配给分析中包括的每个部件或部件类型。故障概率的确定应当符合部件的类型、运行状态、监控（即定期试验）、一级概率安全评定模式中为部件定义的边界及其故障模式。

5.154. 应当为一级概率安全评定量化中使用的部件故障概率数值提供正当性。

5.155. 对于需要运行一段时间的部件，如泵，应当规定任务时间。部件任务时间的确定应当基于通过事故序列分析确定的系统任务时间（见第 5.53 段）。

5.156. 一级概率安全评定文件应当提供一级概率安全评定量化中使用的所有部件故障数据。文件应当包括部件边界、故障模式、平均故障概率、与数据相关的不确定性、使用的数据来源和使用的数值的正当性描述。

部件大修频率和持续时间

5.157. 一级概率安全评定的量化应当考虑到由于试验、维护或维修而导致系统和部件的不可用性。用于部件大修频率和持续时间的数值应当是电厂正在使用或计划用于电厂实践的现实反映。

5.158. 在可能的情况下，部件大修频率和持续时间的确定应当基于从电厂维护记录和部件不可用记录或电厂技术规范分析中获得的电厂特定数据，并辅以来自类似电厂的数据。如果不可能，可以使用一般数据或制造商提供的数据，只要能够提供这些数据反映了电厂的运行实践的正当性。

5.159. 一级概率安全评定文件应当提供系统和部件不可用的数据，并应当提供所用数值的正当性。

分析的量化

5.160. 一级概率安全评定中制定的逻辑模式应当使用第 5.143－5.159 段指出的数据进行量化。然后，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、共因故障概率和人为错误概率的数据来计算事故序列频率。

5.161. 对于使用小事件树和大故障树组合的方法（故障树链接方法见第 5.4 和 5.5 段），需要对使用事件树和故障树为每组始发事件制定的逻辑模式进行布尔约简。由于相互的系统依赖性，在故障树集成过程中可能会产生逻辑回路，通常是在诸如服务水、仪器仪表空气和电力系统的支持系统之间。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回路。如果它们确实存在，打破回路是量化的先决条件。一级概率安全评定文件应当提供模式中任何逻辑回路是如何被打破的细节。

5.162. 根据 GSR Part 4（Rev.1）[3]要求 18，用于一级概率安全评定量化的任何计算机代码都需要经过核实和验证。许多可用于进行这种分析的复杂的一级概率安全评定计算机代码在商业上是可获得的，或者已经在不同的成员国中被制定。

5.163. 应用规则的分析人员应当有足够的经验，并且应当理解规则的适用性和局限性。

5.164. 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（点估计和不确定性边界或概率分布）；

(b) 每组始发事件对堆芯损坏频率的贡献；

(c) 最小割集和最小割集频率（对于故障树链接方法）或假想方案和假想方案频率（对于使用具有边界条件事件树的方法）；

(d) 敏感性研究和不确定性分析的结果；

(e) 用于解释一级概率安全评定的重要性测量（例如，风险实现价值、风险降低价值、基准事件的福塞尔－维斯利和伯恩鲍姆重要性）；

(f) 设备损坏状态的频率（如果定义），以提供一级概率安全评定和二级概率安全评定之间的接口。

5.165. 分析人员应当根据概率安全评定制定过程中所做的假设，检查由一级概率安全评定模式的解决方案确定的事故序列或最小割集是否确实导致堆芯损坏，应当检查序列的样品。此外，应当进行检查以确认代表预期会导致堆芯损坏的始发事件和部件故障组合的最小割集确实包括在生成的最小割集清单中。

5.166. 分析人员应当界定第 5.17 段所用的“对风险的显著贡献”的含义。这可以采取绝对标准或相对标准的形式（例如，相对于总堆芯损坏频率）。

5.167. 应当检查对最小割集执行的任何后处理，以删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，是否确实产生了正确的结果。后处理通常用于故障树链接方法。

5.168. 一级概率安全评定文件应当提供一级概率安全评定的定量结果，并应当描述最重要的序列和最小割集以及已执行的任何后处理。

5.169. 分析人员应当定义第 5.168 段所用的“显著序列”和“显著极小割集”的含义。这些标准可以采取绝对标准或相对标准的形式（例如，相对于总堆芯损坏频率）。

5.170. 对于一级概率安全评定的定量，需要指定临界值以限制分析所需的时间。通常的方法是设置一个频率截止值，以便频率较低的最小割集不包括在分析中。也可以指定一个阶数截止值，以便阶数大于指定水平的最小割集不包括在分析中。应当提供正当性，说明截止值已设置在足够低的水

平，以便一级概率安全评定的总体结果趋同，并且截止值不会导致严重低估堆芯损坏频率。截止值的选择可能因概率安全评定的应用而异。

重要性分析、敏感性研究和不确定性分析

重要性分析

5.171. 应当计算基准事件、基准事件组、信用系统和始发事件组的重要性测量，并用于解释概率安全评定的结果。以下重要性值通常用于一级概率安全评定：

(a) 福塞尔－维斯利（Fussell－Vesely）重要性 [26]；

(b) 风险降低价值 [27]；

(c) 风险实现价值 [28]；

(d) 伯恩鲍姆（Birnbaum）重要性 [29]。

各种重要性测量提供了一个视角，说明哪些基准事件对当前的风险估计贡献最大（福塞尔－维斯利重要性，风险降低价值），哪些基准事件对维持安全水平贡献最大（风险实现价值），以及哪些基准事件的结果最敏感（伯恩鲍姆重要性）。重要性值应当用于识别结构、系统和部件和运行人员的行为，这些行为对风险有显著影响，应当在设计阶段或电厂运行期间仔细考虑。重要性值应当用于确定电厂设计或运行中需要考虑改进的领域[9、13]。

---

[26] 对于特定基准事件，福塞尔－维斯利（Fussell－Vesely）重要性测量是包含待评定基准事件的所有事故序列对堆芯损坏总频率的贡献分数。

[27] 如果基准事件的概率被认为为零，风险降低价值是堆芯损坏频率的相对减少。风险降低价值是基准事件概率的直接函数，可用于评定基准事件对堆芯损坏频率的贡献。

[28] 如果基准事件的概率被认为是确定的，风险实现价值是堆芯损坏频率的相对增加。风险实现价值是对基准事件所代表的功能的重要性的测量。它确定了在安全方面起主要作用的基准事件，即使这些基准事件的潜在故障率非常低。

[29] 伯恩鲍姆（Birnbaum）重要性测量是一种测量当一个部件发生故障时，与该部件运行时相比，风险增加的测量。

不确定性的类型

5.172. GSR Part 4（Rev.1）[3]要求 17 规定：**“必须进行不确定性和敏感性分析，并在安全分析的结果和从中得出的结论中加以考虑。”**人们认识到，制定的模式和一级概率安全评定中使用的数据存在不确定性。当使用概率安全评定的结果来获得风险洞察或支持决策时，应当解决这些不确定性。这可以通过进行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一般分为以下三大类：

(1) 不完全不确定性。一级概率安全评定的总体目标是进行系统分析，以识别导致堆芯损坏频率的所有事故序列。然而，不能保证这一过程已经完成，所有可能的情况都已确定并进行适当的评定。这种潜在的不完整性给分析的结果和结论带来了难以评定或量化的不确定性。不可能明确解决这种不确定性。

(2) 建模不确定性。这是因为缺乏关于分析中使用的方法、模式、假设和近似值正当性的完整知识。使用敏感性研究来解决其中一些不确定性的重要性是可能的。

(3) 参数不确定性。这是由于一级概率安全评定量化所用参数的不确定性造成的。该类的不确定性通常通过不确定性分析来解决，通过指定所有参数的不确定性分布并在整个分析中传播它们。

5.173. 需要考虑如何在设计评定和决策过程中使用不确定性信息，记住堆芯损坏频率的概率安全目标和标准通常与点估计值 [30] 相关，而不是不确定性分布。一级概率安全评定用于识别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

5.174. 应当进行研究以确定一级概率安全评定结果对所做假设和所用数据的敏感性。

[30] 在这种情况下，点估计意味着要么由概率安全评定计算机代码计算，要么由概率分布的另一个参数或分位数计算，例如平均值或中位数。

5.175. 敏感性研究应当针对具有显著不确定性且可能对一级概率安全评定结果产生显著影响的假设和数据进行。敏感性研究应当通过使用替代假设重新量化分析或对反映不确定性水平的数据采用一系列数值来进行。

5.176. 分析人员应当定义第 5.175 段使用的“对一级概率安全评定结果的显著影响”的含义。这可以采取绝对或相对形式的数字标准（见第 5.166 段）、定性标准或定量和定性标准相结合的形式。

5.177. 敏感性研究的结果应当用于表明对从概率安全评定获得洞察的置信度（即，是否达到了堆芯损坏标准或目标，设计是否平衡，以及电厂的设计和运行中是否存在在与敏感性情况进行比较的基本情况一级概率安全评定中未强调的可能弱点）。

5.178. 敏感性研究通常一次针对一个假设或一个参数进行，敏感性研究的结果没有统计学意义。亦可分析相关假设组合的敏感度。

不确定性分析

5.179. 应当进行不确定性分析，以确定一级概率安全评定结果中的不确定性，该不确定性来自用于量化一级概率安全评定数据。

5.180. 作为数据分析的一部分，应当规定一级概率安全评定量化中使用的参数的不确定性分布。这些不确定性分布应当通过分析传播，以确定堆芯损坏频率的不确定性。这些不确定性应当用于提供对一级概率安全评定得出的任何洞察或结果的信心水平的指示。

5.181. 在不确定性分析中应当考虑故障率耦合，以解决来自同一来源数据的相关性。这可以通过参数采样来实现。

6. 内部和外部危害一级概率安全评定一般方法

概述

6.1. 除了可能导致内部始发事件的随机部件故障和人为错误（见第 5 部分）之外，故障序列可能是由其他危害造成的损坏导致。本部分提供以下

建议：符合 GSR Part 4（Rev.1）[3]与其他危害相关的一级概率安全评定要求 6－13，这些危害可分为以下几类：

(a) 内部危害。源自场址边界内并与营运组织控制下的设施和活动故障相关的危害。由位于同一场址的不同设施引起（或发生）的危害也被视为内部危害。内部危害的示例包括内部火灾、内部水淹、内部爆炸、内部飞射物（如汽轮机飞射物）、重物跌落、现场运输事故和源自场址边界内的危害物质排放。

(b) 外部危害。危害，包括自然和人为事件，源自场址边界之外和营运组织控制范围之外的活动，因此营运组织对这些活动几乎没有或根本没有控制。自然外部危害的示例有地震危害、外部洪水、大风和其他恶劣天气条件，人类引发危害的示例包括飞机坠毁、爆炸压力波（爆炸）、场外运输事故和源自场址边界外的危害物质排放。

6.2. 危害，也可以是危害组合，会损坏电厂结构、系统和部件，从而产生事故序列，可能导致堆芯和/或燃料损坏（或其他非期望最终状态，如果这些要在一级概率安全评定中考虑的话）。危害通常有可能同时影响许多结构、系统和部件，并对电厂人员产生不利影响。内部和外部危害（及其组合）都应当包括在一级概率安全评定中。[31]

6.3. 危害组合可以指两种或多种外部危害的组合、外部和内部危害的组合或两种或多种内部危害的组合。相关要考虑的组合类型的详细信息见 SSG-64[6]。危害组合对电厂安全的影响可能比分开考虑的每个单一危害大得多，危害组合的发生频率可能与单一危害相当（例如，一场严重的风暴可能导致强降水以及同时的大坝溃坝，导致电厂的高水位）。

分析过程

6.4. 应当采用一致的方法来识别内部和外部危害，并分析它们对堆芯和/或燃料损坏频率的影响。内部和外部危害分析的主要阶段通常如下：

(1) 内部和外部危害的初始信息的收集；

[31] 本“安全导则”不提供与战争或破坏行为或恐怖主义影响导致事件有关的建议。然而，考虑到军事设施或和平时期行动造成的附带危害（如军用飞机坠毁）。

(2) 危害识别，包括单一和组合危害；

(3) 定性和定量的危害筛选分析；

(4) 边界评定；

(5) 详细分析。

总体分析方法如图 2 所示。

6.5. 虽然内部和外部危害的危害识别和筛选阶段相似，但每种危害的边界评定和详细分析可能涉及该危害特有的任务（例如，在内部火灾的情况下，需要分析火势传播）。本部分阐述了识别和筛选危害的任务，这对于内部和外部危害是相似的，关于特定危害的边界评定和详细分析的特定建议在第 7 部分内部危害和第 8 部分外部危害中提供。

6.6. 要求考虑所有可能影响核电厂的潜在内部和外部危害，并应当酌情进行筛选分析、边界评定或详细分析（见原子能机构《安全标准丛书》第 SSR-1 号《核装置场址评价》[24]）。

初步资料的收集

6.7. 在内部和外部危害的一级概率安全评定的起点，应当收集所有与内部和外部危害特别相关的可用信息。至少应当收集以下信息：

(a) 安全分析报告中考虑的与内部和外部危害相关的设计信息；

(b) 厂房和结构、系统和部件的清单和布局；

(c) 电厂布局、场址及其周围的地理和地形；

(d) 环境条件，如气候带和气象特征，以及根据国家自然现象观测方案对核电厂所在地区的气象和水文过程和现象的详细观测；

(e) 关于管道、运输路线（即航空、铁路、公路、水路）以及危害（如可燃、有毒、窒息性、爆炸性、腐蚀性、放射性）材料的场内和场外贮存设施位置的当前信息；

(f) 场址附近工业和军事设施位置的当前信息；

(g) 场址和区域内任何内部和外部危害发生的历史信息；

(h) 危害风险的确定性分析（如果执行）。

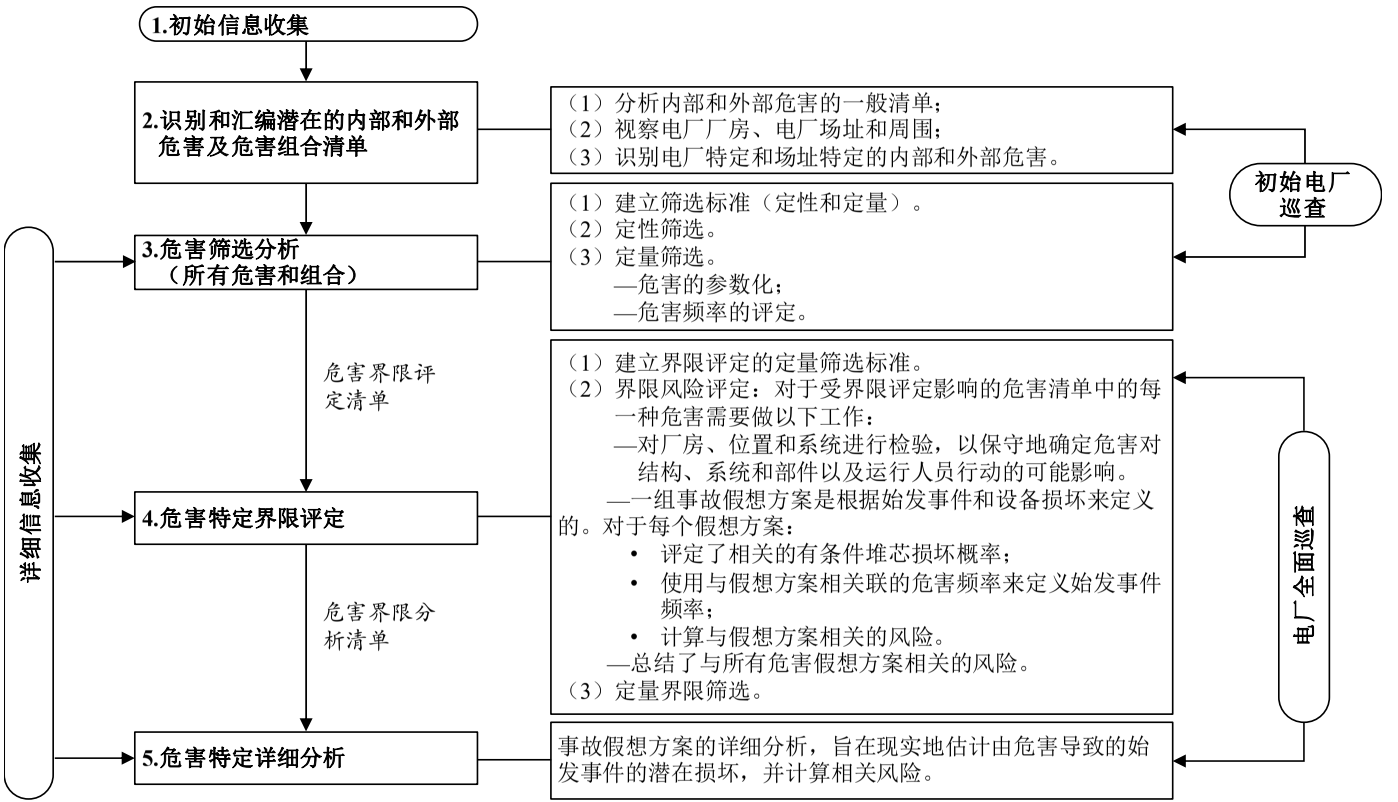

图2. 针对内部和外部危害的一级概率安全评定的总体分析方法。

6.8. 在内部和外部危害的一级概率安全评定过程中，应当根据筛选分析、边界评定或每种危害的详细分析的必要详细程度，更新和扩展初始信息。

危害的识别

6.9. 危害识别的任务应当旨在生成一份全面且可追踪的潜在内部和外部危害清单。特定危害和危害类别的示例如下：

(a) 内部危害：
  (i) 内部火灾；
  (ii) 内部爆炸；
  (iii) 内部飞射物；
  (iv) 管道断裂（包括管道甩鞭和喷射效应）；
  (v) 内部水淹；
  (vi) 重物跌落；
  (vii) 现场电磁干扰；
  (viii) 危害物质的现场排放；
  (ix) 高能电弧故障；
  (x) 现场运输事故；
  (xi) 现场静电（大涡流）；
  (xii) 涉及位于同一场址的其他反应堆装置或放射源的辐射事故。
(b) 外部自然灾害：
  (i) 地震危害；
  (ii) 水文灾害，包括外部洪水 [32]；
  (iii) 气象灾害，包括极端气象条件 [33] 和大风 [34]；
  (iv) 外星现象，如陨石和太阳耀斑；

---

[32] “外部洪水”术语包括多种危害，如大坝坍塌、海啸、流星、河流洪水和风暴潮。

[33] 根据原子能机构《安全标准丛书》第 SSG-68 号《核装置设计中的非地震外部事件》[25]，极端气象条件包括极端气温和湿度、极端水温、积雪、冰冻降水和霜冻相关现象以及闪电。其他危害可能与此有关，如冰雹和水内冰。

[34] “大风”术语涵盖多种灾害，如龙卷风、飓风、台风、下击暴流和直风。

(v) 生物现象 [35]；

(vi) 地质现象；

(vii) 天然火灾。

(c) 外部人类引发危害：

(i) （军用或民用飞机）意外坠毁；

(ii) 场外爆炸压力波（爆炸）（来自工业或军事设施）；

(iii) 场外运输事故（即航空、铁路、公路、水路）；

(iv) 场外工业贮存事故；

(v) 危害物质的意外场外排放；

(vi) 场外电磁干扰；

(vii) 场外人为火灾；

(viii) 其他军事事故；

(ix) 其他工业事故。

SSG-64[6]、SSG-89[7]提供了相关建议，原子能机构《安全标准丛书》第 SSG-79 号《核装置场址评价中与人为外部事件相关危害》[26]，第 SSG-9（Rev.1）号《核装置场址评价中地震危害》[27]，第 SSG-18 号《核装置场址评价中气象和水文危害》[28]和参考文献[29]提供了更多信息。

6.10. 首先，参考文献[30－32]提出的危害和过去概率安全评定研究中检验的危害应当包括在清单中，并根据其对场址的适用性进行系统化评审。附件 I 提供了一个潜在外部危害一般清单的示例。

6.11. 额外的场址或电厂特定危害应当添加到该一般清单中，该清单应当定期更新，以确保所有该类危害都包括在内。场址或电厂特定危害的识别应当以系统化、结构化的方式进行，以确保完整性。对于现有电厂，内部和外部危害识别过程的一组成部分应当是专门的场址调查和电厂/场址巡视。

[35] 生物现象的典型示例是冷却池中的异常鱼类种群，以及冷却水入口中的藻类、树叶或漂浮物（如动物）。

6.12. 应当制定一份可能对风险有显著影响的潜在危害组合清单。在这种情况下，SSG-64[6]推荐了三种类型的危害组合：后果性（后续）事件、相关事件和非相关（独立）事件。

6.13. 所有三种类型的危害组合都应当包括在危害识别和危害组合筛选过程中。[36]

6.14. 对于非相关危害组合，应当考虑组合中单一危害的影响持续时间（例如，长期干旱期间的地震事件、长期外部洪水期间的电厂内部火灾）。

6.15. 应当根据适用于场址单一内部和外部危害清单来识别潜在的危害组合。为此目的，在进行任何筛选分析之前，应当使用适用危害的完整清单。[37]

6.16. 应当排除相互排斥的危害组合。

单一危害源和组合危害源的筛选

6.17. 通常建立一个连续的筛选过程，以尽量减少对根据第 6.14－6.16 段确定的内部和外部单一危害和危害组合的强调，这些危害对风险的重要性较低，而是将分析重点放在风险显著的危害上。连续的筛选过程应当基于明确界定的筛选标准，并始终如一地应用，以确保不遗漏任何与电厂和现场相关的内部或外部单一危害或危害组合的显著风险因素。筛选标准和筛选过程应当与筛选过程的结果一起包含在一级概率安全评定的文件中。

6.18. 当对单一或组合危害单独或组合使用定性筛选标准时，应确认以下内容：

(a) 在给定的时间内，该危害既不会直接导致始发事件，也不会显著增加堆芯和/或燃料损坏的频率。对于外部危害，当危害不能发生在离电厂

[36] 对于后果性危害的事件组合，对组合危害后果的评定可以是对单一危害之一（最好是主要危害）评定的一部分。

[37] 通常，外部危害与其他外部危害的事件组合只涉及自然灾害（例如，大风和高海平面的组合）。然而，自然灾害和人类引发危害的组合也是可能的，不能先验地排除（例如，在恶劣天气条件下船舶事故的风险增加）。

足够近的地方而影响电厂时，或者当关键部件没有受到影响时，通常适用该标准。是否满足这一标准还取决于危害的程度。

(b) 危害发展缓慢，可以很有把握地证明有足够的时间消除危害源或提供可靠和充分的应对措施。

(c) 危害包含在另一种危害的定义中，或者危害组合包含在更严重的危害的定义中。

(d) 危害组合的影响并不比组合中最严重危害的影响更严重。

6.19. 适用于危害的定量筛选标准应当取决于一级概率安全评定的总体目标，并应当与总体堆芯和/或燃料损坏频率有关联（通常根据全范围概率安全评定获得）。详见参考文献[30、31]。就二级概率安全评定而言，应当考虑频率非常低但在放射性物质排放方面具有严重潜在后果的危害。

6.20. 应当规定与内部和外部危害的潜在损坏相关的最重要参数。如果危害的潜在损坏不能局限于考虑单一参数，则应当特定说明几个参数。应当采用为危害指定的所有参数在执行筛选分析时考虑（例如水位和水流压力）。

6.21. 应当特别强调对下列危害类别的分析，因为这些类别在许多场址最为重要：

(a) 地震危害；

(b) 水文灾害；

(c) 气象灾害；

(d) 人类引发危害。

6.22. 为了筛选出特定危害，应当证明电厂所在地的特定条件（如地形、地理、气象、生物）支持这些危害不足以损坏电厂的假设（如非沿海地区的飓风）。

6.23. 只有在证明超过特定强度的频率可以忽略不计的情况下，才应当排除具有一定潜在损坏的外部危害。

6.24. 对于每一个单独的危害，在对始发事件之后事件的悲观假想基础上，应当确定一个近似的最大影响，用于筛选过程。

6.25. 通常为由危害程度范围定义的子类提供危害频率。在某些情况下，筛选标准不能适用于整个危害，但可以适用于每个单独的子类（例如，空气中不同速度和粉尘浓度的沙尘暴）。这将允许分析人员避免筛选出频率低但高潜在损坏的危害。然而，在应用这种方法时，分析人员应当确保将危害划分为子类不会因此筛选出整个危害或显著低估由此产生的风险。

6.26. 电厂发生的始发事件可能是单一危害或两种或多种危害组合影响的结果。在使用筛选标准时，有理由认为，组合影响可能导致显著后果的危害不被排除在进一步考虑之外，即使单独考虑每一种危害对风险的影响可以忽略不计。

6.27. 在应用筛选标准时，应对电厂和周围环境的实际状态进行定期评审，以核实原始设计条件的变化不显著或在概率安全评定中得到考虑。特别是应当彻底调查有可能造成新的危害或导致某种程度危害频率增加的变化。[38]

7. 内部危害一级概率安全评定的特定方面

概述

7.1. 本部分提供了关于满足 GSR Part 4（Rev.1）[3]针对内部危害的一级概率安全评定要求 6－13 的建议（见第 6.9 段）典型内部危害清单）。为与核电厂某些内部危害（如火灾、水淹、汽轮机飞射物）相关的一级概率安全评定提供了特定建议。本“安全导则”未明确涵盖其他内部危害，但可以使用类似方法解决。

[38] 以下变更示例仅供说明之用：

(a) 场址半径 30 公里范围内的军事或工业设施发生变化，或附近运输路线（即铁路、飞机路线、公路和河流）发生变化，导致人为外部危害的范围和程度发生变化；

(b) 场区上游河流上大坝建造的变化导致外部洪水风险的潜在损坏增加；

(c) 环境条件的变化（如年平均和最大风速、水位、温度、本地降雨量），这可能导致具有更高损坏潜力的自然外部危害的频率发生变化。

7.2. 应当在边界评定和/或详细分析的框架内考虑内部危害（见第 6.1 (a) 段和第 6.9 段）。在考虑一级概率安全评定的内部危害时，应当采用一致的方法。这种方法通常包括以下任务：

(a) 在可行的情况下，通过电厂巡视支持场址和电厂信息的收集。

(b) 危害表征：危害的识别、危害频率的计算和危害影响的分析。

(c) 从内部始发事件的一级概率安全评定推导出内部危害的一级概率安全评定：

  (i) 确定由内部危害导致始发事件；

  (ii) 确定对内部始发事件的一级概率安全评定的现有事件树和故障树的必要修订；

  (iii) 特定依赖性和共因故障的分析；

  (iv) 特定数据的分析；

  (v) 特定人的可靠性分析方面。

(d) 定性和/或定量筛选。

(e) 量化内部危害对堆芯和/或燃料损坏频率的影响（例如，结果分析、敏感性研究以及不确定性和重要性分析）。

(f) 文件（特别考虑分析中使用的假设和参考文献，包括质量保证）。

一级概率安全评定内部危害边界评定

7.3. 大多数内部危害（如火灾、爆炸、水淹）可能发生在场址边界内（厂房内部或外部）的各种不同位置。因此，危害表征应当特定说明：

(1) 全面电厂分析边界，以便考虑所有可能导致危害风险的位置；

(2) 封闭的电厂区域，考虑电厂设计中现有的保护特点（如实物分隔、屏障、隔离设备），以将损坏控制在导致损坏的区域内。

7.4. 进行边界评定的目的是减少需要详细分析的内部危害（或内部危害假想方案）清单，从而专注于风险显著的事故假想方案。边界评定的执行方式应当确保与特定内部危害（或内部危害假想方案）相关的风险与其他危害相比忽略不计。

7.5. 筛选过程后残留的内部危害对堆芯和/或燃料损坏频率的影响应当使用这些危害的一级概率安全评定来确定。针对内部危害的一级概率安全评定应当依赖于针对内部始发事件的一级概率安全评定制定的电厂响应模式，包括功率运行和关闭状态。一级概率安全评定的可用性，内部始发事件应当是针对内部危害制定一级概率安全评定的先决条件。除了通过对内部始发事件执行一级概率安全评定发现的事件（例如，发生火灾时主控制室中的所有信息丢失）之外，危害分析的结果可能会产生进一步的始发事件。在这种情况下，应当制定新的事故序列并将其整合到一级概率安全评定中。

7.6. 出于对特定内部危害导致风险进行定量简化评定的目的或出于筛选目的，可以在没有内部危害的详细一级概率安全评定模式的情况下估计堆芯和/或燃料损坏频率。在这种情况下，计算特定内部危害对堆芯和/或燃料损坏频率的累积贡献的一般公式由公式 (1) 给出：

$$f_{\text{堆芯/燃料损坏危害}} = \Sigma f_{\text{厂区内危害}\,i} \times \mathrm{CCDP}_i \qquad (1)$$

式中

$f_{\text{堆芯/燃料损坏危害}}$ 是特定内部危害在场区至堆芯和/或燃料损坏频率；

$f_{\text{厂区内危害}\,i}$ 是指场区 i 特定内部危害的发生频率；

CCDP_i 是场区 i 的有条件的堆芯和/或燃料损坏概率，使用内部始发事件的一级概率安全评定进行估计，根据内部危害对场区的影响采用保守假设进行调整。

7.7. 影响分析应当考虑危害导致部件故障对内部危害概率安全评定中包含的始发事件以及相关安全功能的影响。应当进行基于物理研究的详细分析（如模拟火灾假想方案、水淹假想方案），以减少过度保守，从而高估危害造成的风险。

7.8. 屏障或实物分隔等保护功能的潜在故障可能导致损坏传播到其他区域，应当通过特定详细的分析来解决这一问题。

7.9. 基本的场址和电厂信息应当从图纸或数据库中获得。对于运行电厂，该类信息应当通过电厂巡视进行核实和完成。

7.10. 由于电厂巡视的信息可能会为内部危害的一级概率安全评定提供重要的输入，因此该类巡视应当得到良好的计划和实施，并彻底记录在案。

7.11. 电厂巡视最好在为内部危害制定一级概率安全评定的过程开始时进行，但特定任务（即对选定危害的详细分析）可能需要专门的电厂巡视。

7.12. 可信的结构、系统和部件内部危害导致故障的概率和一级概率安全评定模式中的独立故障组合将导致产生危害堆芯和/或燃料损坏频率。

7.13. 受边界评定影响的内部危害的累积贡献应当计算并保留在一级概率安全评定的最终结果中。

7.14. 应当为特定内部危害制定一套假想方案，除非危害对电厂的所有影响都可以由一个假想方案限定，但通常情况下并非如此。

内部火灾的分析

概述

7.15. 内部火灾的一级概率安全评定是对核电厂场址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因素[33]：

(a) 现场任何位置发生火灾的可能性；
(b) 火势传播到其他地方的可能性；
(c) 火灾探测、灭火和火灾密封；
(d) 由于驱动消防系统而损坏设备的可能性。例如，消防系统和设备导致喷淋和水淹可能会损坏原本可以在火灾中幸存的设备，或者这种设备的故障模式可能会改变；
(e) 火灾对结构、系统和部件及其相关电缆的影响，考虑的影响应当包括由“热短路”导致设备虚假驱动而导致新故障模式；
(f) 对结构、系统和部件和电厂构筑物特点（如墙壁、天花板、柱子、屋顶横梁）的完整性造成损坏的可能性；
(g) 火灾对部件故障概率的影响；
(h) 火灾对人类行为和人为错误概率的影响；

(i) 火灾对运行人员和可信的结构、系统和部件行动的直接影响（如需要疏散控制室）和间接影响（如虚假指示导致混淆信息）。

7.16. 安全重要冗余结构、系统和部件通道之间的实物分隔（即防火屏障）可以限制火灾损坏的程度。使用内部火灾的一级概率安全评定模式量化火灾对堆芯和/或燃料损坏频率的影响，应当包括未受火灾影响的设备随机故障的概率以及试验或维护大修的可能性。

7.17. 特别是在内部火灾的一级概率安全评定中，应当考虑到烟雾的影响，同时考虑到以下几点：

(a) 烟雾可能会导致电气和/或电子设备出现故障，尤其是在伴随高温的情况下。

(b) 由于烟雾（可能是有毒的，也可能是刺激性的）和高温，人为错误的概率可能会更高。

(c) 可能因烟雾的存在需要疏散主控制室。

7.18. 对于处于关闭状态内部火灾的一级概率安全评定，应当考虑以下特定方面：

(a) 第 9 部分陈述的关闭状态下内部始发事件的一级概率安全评定方法的特定物项；

(b) 可能较高的火灾负载、额外的火灾负载（例如瞬时可燃物）和额外的点火源，通常与在关闭状态期间执行的维护活动有关联；

(c) 消防手段的可用性；

(d) 火传播的其他路径的可能性（例如，在关闭状态下打开门）；

(e) 大修期间不同电厂位置的居留率增加，这可能会提高火灾探测能力，但也可能会产生额外的火源；

(f) 为控制可燃物而实施的与火灾相关的电厂运行和配置变更，以及为系统或部件大修提供补偿措施而实施的变更。

7.19. 在核电厂设计（见 SSG-64[6]）和运行（见原子能机构《安全标准丛书》第 SSG-77 号《核电厂运行中的内外部危害防护》[34]）期间进行的确定性火灾危害分析和火灾安全关闭分析，应当用于为内部火灾的一级概率安全评定提供重要输入。所提供的信息可能包括部件和电缆及其位置的清

单，以及根据专门为防火特点设计而执行的功能和详细火灾影响分析，将电厂划分为“防火隔间” [39] 的详细信息。

7.20. 内部火灾的一级概率安全评定的方法应当基于对电厂边界内所有位置的系统分析（见参考文献[33]）。为了便于这种分析，应当将电厂分成防火隔间，然后对其进行单独审查。在设计过程中进行的电厂划分可能有助于作为划分这些实物区域的起点。用于指定防火隔间的标准应当正当并记录在案。

7.21. 用于内部火灾的一级概率安全评定的制定过程通常包括图3 [40] 所示和第 7.22－7.71 段所示的任务。就本“安全导则”而言，火灾假想方案是根据火源和隔间内的火灾损坏程度来定义的。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点火频率和灭火概率。

数据收集和潜在内部火灾评定

7.22. 内部火灾一级概率安全评定中的数据收集和评定任务旨在准备必要的数据。这项任务应当集中在收集火灾风险建模所需的电厂和场址特定数据。然而，必须再评定一级概率安全评定中用于内部始发事件的一些数据，以考虑火灾导致工况。

[39] 在 SSG-64[6]，防火隔间被描述为“完全被防火屏障包围的厂房或厂房的一部分：所有墙壁、地板和天花板。”与此相反，在内部火灾概率安全评定的情况下，防火隔间可以简单地是一个封闭良好的房间，不一定被防火屏障包围。

[40] 图 3 所示的筛选过程需要适当考虑火势传播的可能性（另见第 7.38 段）。

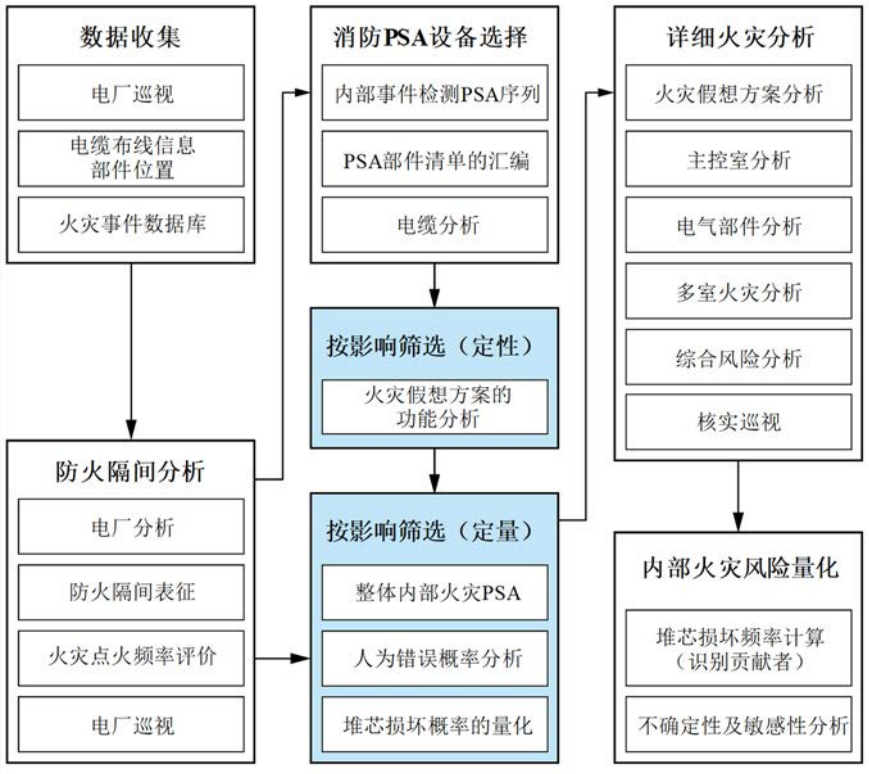

图 3. 用于内部火灾的一级概率安全评定的制定过程。

7.23. 针对内部火灾的一级概率安全评定的电厂特定数据应当包括以下内容：

(a) 电厂的电缆线路，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库存（见第 7.25 段）；

(c) 来自运行经验的数据涉及以下各项：

(i) 火灾事件；

(ii) 对消防功能故障和/或恶化的观察。

(d) 关于部件可能成为防火隔间特定信息（即可能导致火灾和瞬时可燃材料的部件故障）；

(e) 火灾探测和灭火手段可靠性的估计；

(f) 发生火灾时的人员行动；

(g) 消防队的可用性和能力；

(h) 消防系统和设备特征（例如，系统驱动的时间、可能导致设备损坏或阻止运行人员进入防火隔间的灭火剂）；

(i) 火灾导致设备故障模式和火灾损坏标准；

(j) 消防相关程序和技术规范。

7.24. 鉴于内部火灾一级概率安全评定需要收集和维护信息的数量和性质，应当考虑开发一个数据库作为支持工具。

防火隔间的分析

7.25. 出于内部火灾概率安全评定的目的，分析中包括的所有厂房和构筑物应当划分为不同的防火隔间并单独检查。防火隔间至少应当具备以下表征：

(a) 它们的实物边界（如墙、门、阻尼器、贯穿件、距离）；

(b) 消防功能到位（如火灾探测以及消防系统和设备）；

(c) 隔间周围屏障的耐火等级；

(d) 位于防火隔间内的部件和设备，包括电缆；

(e) 相邻的防火隔间和连接；

(f) 将待分析的防火隔间与不相邻的防火隔间连接起来的通风路径（管道）；

(g) 火灾负载（例如，类型、数量、是否受保护、位置、本地分布、是否永久或临时）；

(h) 潜在点火源（如类型、数量、位置）；

(i) 控制可燃材料的程序和其他行政规定；

(j) 居留水平（即人员探测火灾的可能性）；

(k) 位置的可达性（例如消防队）。

7.26. 从电厂文件中获得的信息，无论是用于数据收集还是用于防火隔间的规范，都应当在电厂巡视期间通过目视视察整个电厂的每个防火隔间来核实尽可能地确保数据代表电厂的实际和当前状况。

7.27. 对于防火隔间和火源，火灾点火频率的估计是内部火灾一级概率安全评定的重要组成部分，应当在筛选所有防火隔间之前进行，或在定量筛选过程开始时对通过定性筛选过程的最重要防火隔间进行。

7.28. 应当尽可能使用电厂特定数据评定与火灾点火源和/或防火隔间相关的点火频率。如果这些数据不足以估计火灾点火频率，一般数据应当与可用的电厂特定数据一起使用，并根据实际存在的火源（包括动火作业产生的来源）以及防火隔间内永久和临时可燃物和点火源的数量进行调整。

7.29. 火灾点火频率的估计应当考虑特定运行状态下引起火灾的潜在人为错误（例如，人类引发火灾，包括瞬时火灾和不同电厂运行状态下焊接、切割或其他动火作业导致火灾）。

7.30. 火灾频率应当估计为具有统计不确定性区间的平均值。

内部消防一级概率安全评定设备的选择

7.31. 在对一级概率安全评定中考虑的内部始发事件的设备部件进行检验的基础上，应当建立一级概率安全评定中用于内部火灾的建模设备清单。该清单应当包括其火灾导致故障可能导致下列一种或多种情况的设备：

(a) 该故障可能会导致始发事件。

(b) 故障可能会影响安全功能缓解始发事件的能力。

(c) 在火灾导致始发事件（C 型人因故障事件）发生后，故障可能会影响运行人员的行动。

(d) 故障可能导致功能的虚假驱动，从而在功率运行和电厂关闭期间对电厂造成其他不安全影响。

这种故障可能是由于动力或控制电源故障，或由于热短路导致虚假驱动或电厂监控仪器仪表和警报的错误输出。设备虚假驱动的分析深度应当适应概率安全评定的范围，并应当关注一级概率安全评定中尚未考虑的设备或故障模式。

7.32. 应当确定对内部火灾一级概率安全评定重要的内部始发事件概率安全评定模式的电厂部件和所有相关元素。应当系统地重新检验在概率安全评定模式中筛选或包括内部始发事件的部件故障模式的基本基础，以确定在火灾导致故障的背景下所做假想有效性，必要时，应当扩展内部始发事

件的模式。由于非能动部件也可能受到火灾的影响，因此在内部火灾的一级概率安全评定中应当考虑这些部件的易损部分。

7.33. 与第 7.31 段和第 7.32 段规定的部件相关的所有电缆和电路的识别以及电缆线路的分析应当是该检验的一个组成部分。此外，仪器仪表空气控制线等非电路应当考虑火灾的潜在损坏。

7.34. 应当为每个防火隔间制定一份一级概率安全评定相关设备清单。在详细分析的后期阶段，有必要更准确地确定防火隔间内部件的位置。

按影响筛选

7.35. 应当根据定性（以影响为导向）标准，使用影响筛选来消除不重要的火灾假想方案。筛选首先确定关键的防火隔间和区域，然后使用悲观假设确定潜在的单分区和多分区火灾假想方案。用于筛选特定火灾假想方案的影响导向标准应当考虑所考虑假想方案中涉及的防火隔间的特征。

7.36. 如果符合以下一项或两项条件，则可根据对电厂安全的潜在影响可忽略不计的情况，对防火隔间进行筛选：

(a) 火灾负载密度（防火隔间的每个地板面积）低于规定的可接受阈值，并且传播的可能性非常低。

(b) 以下所有条件均成立：

  (i) 隔间中不存在可能导致始发事件或需要手动关闭的设备；

  (ii) 安全相关系统（即电厂安全关闭所需的系统）及其电缆或支持系统均不位于隔间内；

  (iii) 火灾影响传播到含有安全重要结构、系统和部件的其他防火隔间的可能性非常低。

7.37. 出于筛选的目的，应当假设暴露在火灾中的所有部件和电缆都出现故障（即悲观假设火灾探测和灭火功能不起作用或不可用）。其他防护措施（如防火罩、保护涂层、不符合防火标准的外壳）通常不被考虑在内。

7.38. 根据影响进行筛选还应当涵盖在对火势传播的悲观假设下形成的多隔间火灾假想方案。对于每个单独防火隔间，通过将在任何方向上与其相邻的所有隔间以及通过通风与之相连但不一定相邻的所有隔间添加到该隔间来定义火可以在其中传播的隔间组合。然后，应当分析所有可能的防火

隔间组合，以确定火势传播到相邻或相连防火隔间的可能性。为了限制需要考虑的组合数量，可以根据相关的鉴定计划、行业和过去的设施性能数据，对防火屏障元件的可靠性和有效性做出总体悲观假设。

7.39. 在分析中应当考虑有可能从厂房外部传播到内部防火隔间的火灾（例如，火灾可能从变压器区传播到汽轮机大厅）。

7.40. 对于多机组场址和/或多源场址 [41]，在分析中应当考虑火势从一个反应堆机组或放射源传播到另一个反应堆机组或另一个放射源防火隔间的潜在可能性。还应当考虑公共区域（如机组共用的柴油发电机、开关站）发生火灾的可能性。

按频率筛选

7.41. 在定量标准的基础上，通过对堆芯和/或燃料损坏频率的贡献来筛选防火隔间，旨在进一步消除在通过影响进行定性筛选的第一步之后残留的防火隔间或多个防火隔间的组合。

内部始发事件一级概率安全评定中内部火灾的整合

7.42. 在这一步，火灾对堆芯和/或燃料损坏频率的影响应当使用在现有一级概率安全评定内部始发事件模式基础上制定的概率模式进行计算。这种模式通常用于计算特定火灾假想方案有条件的堆芯和/或燃料损坏概率。为了评定火灾假想方案发生的频率以及相关的因火灾而有条件的无法使用的必要安全功能，应当就以下方面作出悲观假设：

(a) 火的生长和传播；
(b) 火灾对设备的影响（例如，假设防火隔间内的所有设备都发生了故障）；
(c) 消防措施（例如，不计入探测和灭火手段）；
(d) 相关人因故障事件概率。

7.43. 根据这些假设，对于每个残留的防火隔间，应当修改内部始发事件的一级概率安全评定模式，以便绘制隔间内的火灾影响、火灾向其他隔间的传播以及相关的始发事件和设备故障模式。这将允许计算每个防火隔间

[41] 多源考虑意味着要考虑到涉及并置辐射源（如反应堆堆芯、乏燃料水池）的可能同时发生的事故假想方案。

的有条件的堆芯和/或燃料损坏概率，由此可以使用公式（1）计算火灾对堆芯和/或燃料损坏频率的整体贡献。

火灾环境中的人为错误概率分析

7.44. 应当修改与恢复和跳堆后人为错误相关的概率，以评定火灾对内部始发事件一级概率安全评定中模拟的信用恢复和人类行动影响。内部火灾一级概率安全评定中 C 型人因故障事件的评定应当包括以下内容（关于火灾环境中人的可靠性分析的一般规则，见参考文献[18]）：

(a) 包含在内部始发事件的一级概率安全评定模式中但也与火灾危害假想方案相关的人因故障事件。在这种情况下，应当检查是否需要修改表现形成因素的评定，因为运行人员实施行动可能比基本情况下更困难（例如，由于与火灾环境相关的压力水平更高）。

(b) 仅与火灾相关的人因故障事件，包括主控制室和/或辅助控制室的废弃。在这种情况下，用于评定火灾特定人因故障事件的方法通常可以遵守与用于分析其他类型人因故障事件的方法相同的原则。

(c) 运行人员对火灾导致虚假警报和指示的不良反应。

7.45. 当应用第 5 部分概述的人的可靠性分析方法时，应当分析表现形成因素，考虑特定火灾影响，如额外的应力、潜在的矛盾信号、烟雾、照明丧失以及进入或通过受火灾影响区域的困难。

7.46. 如果内部始发事件的一级概率安全评定模式中计入人员恢复行动，则应当检查采取这些行动的可行性。例如，在受火灾影响的房间中可能很难执行特定恢复运行。

量化内部火灾对堆芯和/或燃料损坏频率的影响以便进行筛选

7.47. 对于定量筛选，应当根据公式（1）和火灾传播的可能性，考虑火灾假想方案的相应频率，评定内部火灾对堆芯和/或燃料损坏频率的影响。

7.48. 定量筛选应当基于对有条件的堆芯和/或燃料损坏概率的悲观估计，或火灾到堆芯和/或燃料损坏频率的绝对贡献。防火隔间定量筛选的两个标准可定义如下：

(1) 对于筛选出的所有防火隔间，火灾对堆芯和/或燃料损坏频率的累积贡献应当不超过规定的阈值。这个阈值可以定义为一个特定绝对值，也可以用相对的术语给出（例如，内部始发事件对堆芯和/或燃料损坏频率的贡献）。

(2) 单一防火隔间中的火灾对堆芯和/或燃料损坏频率的贡献足够低，以保留所有风险显著的火灾假想方案。筛选阈值的定义方式与前面的标准相同，但至少应当低一个数量级。

7.49. 通过考虑火灾对堆芯和/或燃料损坏频率的贡献进行筛选，应当考虑多个防火隔间的损坏频率，作为一个防火隔间中点火频率和火灾传播到其他隔间的条件概率的乘积。

7.50. 整个筛选过程（即按影响和频率进行筛选）的结果应当如下：

(a) 不代表对风险有显著影响的火灾假想方案或防火隔间清单，可从详细分析中筛选出来。然而，与筛选出的火灾假想方案或防火隔间相关的估计风险应当保留在内部火灾一级概率安全评定的总体结果中。

(b) 与防火隔间相关的火灾假想方案清单，这些假想方案可能是风险的显著因素，需要进一步考虑。对于此清单中的每个火灾假想方案，应当制定内部火灾的定量一级概率安全评定模式，以供进一步分析。

火灾的详细分析

火灾假想方案的分析

7.51. 火灾的详细分析应当旨在降低筛选过程中迄今为止确定的火灾假想方案的保守程度。只要有可能，就应当有专门的巡视来支持它核实详细分析的支持信息。尤其应当考虑到以下几个方面：

(a) 隔间内的防火屏障、实物分隔和隔离措施以及其他防火措施；

(b) 可信的结构、系统和部件的位置；

(c) 消防措施（如消防系统）的位置和有效性；

(d) 防火隔间内火的生长和传播；

(e) 直接火灾效应，如火焰、羽流、天花板喷射、热气辐射热、烟雾和煤烟；

(f) 间接火灾效应，如灭火介质的效应，或随之而来的高能电弧。

7.52. 应当应用更现实的模式来评定旨在降低设备损坏、火灾增长和传播的可能性以及火灾对结构、系统和部件影响的人类行为。

7.53. 应当评定火灾和火灾副产品（如烟雾、有毒气体）对人员表现的影响。还应当注意的是，火灾造成的过压可能会阻止人员进入救援地点或消防队开展消防活动所需的门打开。

7.54. 应当判断并记录为分析火灾增长和传播而选择的特定建模工具（如火灾模拟代码）。

7.55. 火灾假想方案应当描述在选定隔间中导致火灾的时间相关过程，以及结构、系统和部件（包括电缆）的任何后续故障。火灾假想方案应当在内部火灾的一级概率安全评定模式中表示（例如，通过火灾事件树，示例见附件 II），其中对影响火灾发展的所有重要特点进行建模（即防火屏障的设计和质量、火灾增长和传播模式，以及风险设备损坏标准，包括电缆、防火和灭火特点）。第 5 部分的建议应当用于确定该类火灾事件树。

7.56. 对于要分析的火灾假想方案，应当使用第 5 部分针对内部始发事件的概率安全评定提出的相同方法评定人工操作的人的可靠性以及火灾探测和消防系统和设备的部件可靠性，并考虑第 7.44－7.46 段提到的方面。

7.57. 在火灾假想方案中，应当考虑可能与火灾传播相关的路径（如通风管道、电缆槽和通道、故障防火屏障）。

7.58. 对于详细火灾分析中考虑的防火隔间，火灾假想方案发生频率的数据应当辅以特定于防火隔间的额外数据，如临时火灾负载和点火源的存在及其可燃性。

7.59. 对于特定的火灾假想方案，应当证实火灾探测和灭火的自动和手动功能的指定有效性和响应时间，以及指定的无法灭火的概率。

主辅控制室火灾分析

7.60. 主控制室和辅助控制室内部火灾的一级概率安全评定模式应当考虑与这些位置相关的特定特点，例如控制室火灾对所有信用系统的广泛影响、系统虚假驱动的可能性以及控制室火灾对运行人员行动的影响。后者应当包括以下内容：

(a) 火灾和火灾副产品（如烟雾、煤烟）对仪器仪表和相关设备必要功能可用性的影响；

(b) 火灾探测和灭火功能的能力，包括间接火灾效应的潜在不利影响，通常是灭火的结果（如灭火介质）；

(c) 考虑到可达性、相互依赖性和其他可能的限制等方面，使用替代位置进行安全关闭；

(d) 同时影响主控制室和辅助控制室的潜在火灾导致故障模式（例如，辅助控制室火灾导致开关的虚假驱动，可能导致主控制室的控制失控）；

(e) 火灾副产品（如烟雾或有毒气体）传播的影响。

此外，应当考虑控制室内的火灾传播，包括面板之间存在实物分隔和分离装置，如经鉴定防火屏障，以及冗余通道部件的空间分隔。

7.61. 多隔间火灾分析旨在识别涉及多隔间的潜在火灾假想方案。应当假设火可能通过隔间之间的防火屏障从一个隔间传播到另一个隔间，特别是通过具有能动功能的防火屏障元件，如门或阻尼器，或通过屏障贯穿，如电缆槽或通风管道。多隔间火灾的详细分析应当基于火灾增长模式、火灾传播分析模式以及火灾探测和灭火模式。

7.62. 对于单一防火隔间，对多防火隔间火灾的详细分析应当考虑火的传播深度以及直接和间接火灾影响的传播，不仅包括防火隔间之间的热传递，还包括其他火灾副产品，如灭火介质。

电气部件房间火灾分析

7.63. 有电气部件的房间、开关设备室、电缆铺设室和其他包含电气仪器仪表和控制设备的房间往往成为设备和布线的自然集中中心。它们包含可能属于信用系统的一个以上通道的电气设备和电缆。因此，火灾对安全重要的冗余物项或其他一级概率安全评定相关设备的潜在影响可能高于其他电厂位置的火灾影响，这应当在分析中加以考虑。

7.64. 在这些位置，由于火灾导致电气故障（例如热短路），电气部件的单一或多个虚假驱动的可能性也更高。在分析电气部件的虚假驱动时，应当识别特定火灾导致电路故障，并评定相关的条件概率。

危害组合分析

7.65. 第 6.12 段提到的所有组合类型的火灾和其他危害组合发生的可能性（如 SSG-64[6]所定义）应当进行评定。对于这些危害，应当在一级概率安全评定中考虑其他危害导致火灾组合，而对于内部火灾，应当在一级概率安全评定中考虑火灾与其他间接危害的组合。对于因共因而与其他危害有关联的火灾组合，以及与未被排除的非相关危害（即同时但独立发生）的火灾组合，分析人员应当决定是否将这些危害组合纳入内部火灾或其他危害之一的一级概率安全评定中。

7.66. 对由其他危害（如地震、闪电、外部火灾、飞机坠毁）导致内部火灾进行定性分析，应当作为始发事件分析的一部分（见第 6 部分）。应当分析其他危害和火灾的组合影响对安全可能很重要的防火隔间。要考虑的影响示例包括由危害导致点火源、消防系统的虚假驱动或退化以及采取人工灭火行动的困难（关于外部危害的一级概率安全评定建议见第 8 部分）。

7.67. 应当考虑由其他危害导致内部火灾对运行人员的表现塑造因素（或其他因素，取决于人的可靠性分析方法）的以下影响：

(a) 火灾发生后，相关隔间的可达性；
(b) 压力水平增加；
(c) 指示失效或指示错误；
(d) 火灾对运行人员行为的组合影响。

内部火灾风险的量化

7.68. 为详细分析内部火灾的一级概率安全评定而制定的特定模式（例如，主控制室火灾的模式，评定火灾导致部件的单一或多个虚假驱动的影响的模式）应当包括在完整的一级概率安全评定模式中。

7.69. 考虑到详细分析的结果，应对筛选后残留的防火隔间进行内部火灾对堆芯和/或燃料损坏频率的影响的最终量化。用于按频率定量筛选防火隔间的结果和模式应当包含在内部火灾的一级概率安全评定中。内部火灾的一级概率安全评定结果应当通过确定堆芯和/或燃料损坏频率的主要因素来解释（例如，防火隔间、火灾假想方案、相关人类行动）。在最后阶段，应当评审与筛选相关的假设，以估计筛选对堆芯和/或燃料损坏频率的影响。

7.70. 内部火灾一级概率安全评定模式的量化、不确定性分析、重要性分析和敏感性分析第 5 部分提出的建议。应当进行不确定性分析，以确定不确定性的来源并对其进行评定。应当进行敏感性研究和重要性分析，以确定内部火灾的一级概率安全评定中对风险具有显著意义的要素。还应对重要的假设和数据进行敏感性研究。应当确定各种因素对计算结果的相对重要性。

内部火灾用一级概率安全评定文件

7.71. 根据 GSR Part 4（Rev.1）[3]要求 20，内部火灾的一级概率安全评定需要以便于其评审、应用和更新的方式进行记录。文件中应当包括以下信息：

(a) 对电厂特有的防火特点的描述，包括非能动和能动缓解特点，以及将电厂划分为防火隔间；
(b) 描述用于评定内部火灾危害的特定方法和数据；
(c) 描述对内部始发事件的一级概率安全评定模式所做的修改，以考虑内部火灾的影响；
(d) 防火隔间的表征；
(e) 从分析中筛选出特定防火隔间的正当性；
(f) 火灾假想方案的分析结果，包括详细分析（例如主控制室、多隔间火灾）；
(g) 内部火灾一级概率安全评定在堆芯和/或燃料损坏频率方面的最终结果；
(h) 支持火灾分析的电厂巡视报告。

内部水淹的分析

概述

7.72. 内部水淹的一级概率安全评定是对发生在核电厂场址或厂房内的液体（通常是水）泄漏相关事件的概率分析，以及该类泄漏对安全的潜在影

响。内部水淹一级概率安全评定的制定过程典型地包括在图 4 [42] 中示出并在第 7.73－7.107 段呈现的任务。对于关闭状态下内部水淹的一级概率安全评定，类似于第 7.15 段列出的内部火灾方面，应当予以考虑。

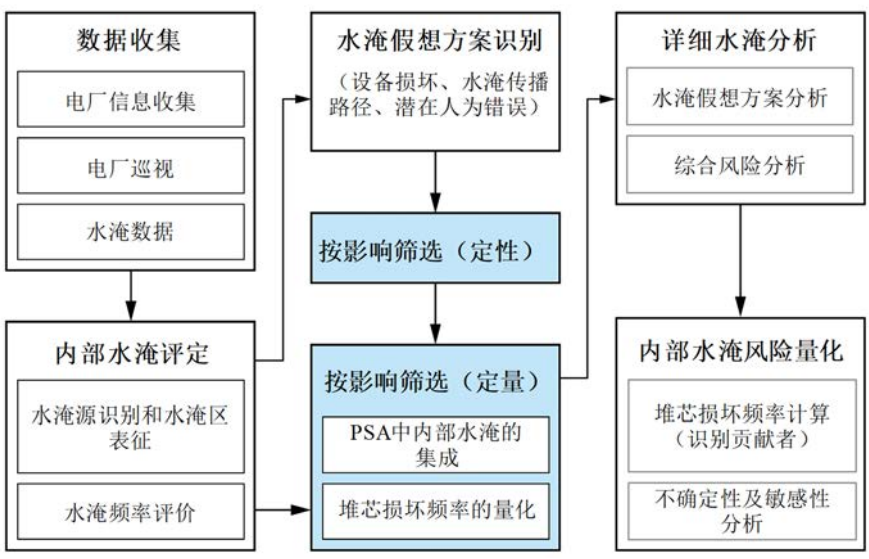

图 4. 用于内部水淹的一级概率安全评定的制定过程。

数据收集和内部水淹潜力评定

7.73. 对于运行核电厂，应当进行特别关注内部水淹的电厂巡视，以核实从图纸和其他电厂信息来源获得信息的准确性，并获得关于空间相互作用的必要信息，以分析每个潜在内部水淹来源的损坏影响。

7.74. 应当识别和描述可能的内部水淹事件（见 SSG-64[6]关于设计中核电厂的防水淹建议）。在执行这项任务时，应当考虑到以下几点：

(a) 可能的水淹源：管道、容器、储罐、水池、阀门、热交换器、与开放式水源（如海洋、湖泊、河流）的连接，以及由多机组或水源（如消防主环）共享的结构、系统和部件。

[42] 图 4 所示的筛选过程需要在适当考虑潜在水淹传播的情况下进行（见第 7.76 段、第 7.77 段和第 7.85 段）。

(b) 可能的水淹机制：破裂、泄漏、断裂、喷淋系统（如安全壳喷淋系统、消防系统）的虚假或预期驱动，以及运行或维护相关活动期间的人为错误（如阀门定位错误或意外打开）。

(c) 水淹的特征：容量（取决于水淹源是封闭系统还是开放系统）、流速、温度、压力以及蒸汽的存在或可能产生。

(d) 与水淹相关的警报、泄漏检测系统、排水系统的容量和部件的水淹相关保护（如设备跳闸信号），以及水淹隔离装置（如阀门）。

(e) 与概率安全评定相关的部件的临界水淹高度和水淹区域的房间尺寸。

7.75. 当识别潜在的水淹事件时，应当特别考虑电厂关闭状态，因为在关闭期间，水路径经常被手动重新配置。

7.76. 应当确定可能受内部水淹影响的电厂区域，并确定水的可能传播路径。在此过程中，应当考虑多机组和乏燃料水池方面，以及防水淹屏障失效的可能性。

7.77. 电厂应当被划分为实物上独立的“水淹区域”，每个区域在内部水淹的潜在影响和水淹传播的可能性方面通常被视为独立于其他区域。

7.78. 应当尽可能使用电厂特定数据来估计内部水淹事件的频率。当电厂的特定数据不充分时，可使用一般数据或专家判断，并提供适当的正当性。

7.79. 评定内部水淹事件频率的主要数据是管道故障率和破裂频率的估计值以及相关的不确定性。为管道系统选择的数据应当代表内部水淹的重要来源。

7.80. 考虑到电厂特定维护程序和经验以及水基消防系统的虚假驱动，还应当评定由人为错误导致水淹事件的频率和严重程度。

7.81. 水淹频率应当估计为具有统计不确定性区间的平均值。

内部水淹假想方案的识别

7.82. 对于每个水淹区域，应当确定可能受内部水淹影响的结构、系统和部件。以下水淹对设备的影响可能是相关的：水淹、温度、压力、喷淋、蒸汽、管道甩鞭或高能管道破裂或阀门结合导致喷射冲击。应当确保分析尽可能完整。

7.83. 考虑受内部水淹影响的结构、系统和部件应当包括高程、屏障、门和排水沟。还应当考虑下水道堵塞的可能性。

7.84. 应当评定水淹从一个区域传播到另一个区域的可能性，包括考虑屏障的破坏。

7.85. 应当考虑水淹传播的所有可能途径（例如，非防漏门、设备排水管、常闭门或舱口开着）。

7.86. 应当确定电气和/或电子元件（如机柜，安全重要结构、系统和部件，电缆接线盒）和其他对湿度敏感元件的位置，包括高度和任何保护功能。通过这种方式，可以识别部件在水淹方面的脆弱性。

7.87. 应当评定水淹对电厂运行的潜在影响。这一评定应当包括由于水淹效应造成的系统或部件的虚假驱动，这可能导致特定事故序列。

按影响筛选

7.88. 内部水淹假想方案应当根据其影响进行筛选。可以通过筛选那些可以忽略不计的水淹区域来选择关键的水淹区域对电厂安全的潜在影响。如果下列一种或两种情况都适用，则可以筛选出水淹区域：

(a) 以下两个条件均成立：
  (i) 水淹区域不包含可能导致始发事件的设备。
  (ii) 核电厂安全关闭所需的系统及其支持系统都不位于水淹发源区或水淹传播区。
(b) 水淹区域不包含任何足以导致设备故障的水淹源，包括来自其他水淹区域的水淹。

按频率筛选

7.89. 根据对堆芯和/或燃料损坏频率的贡献，在定量标准的基础上对水淹区域进行筛选，目的是进一步消除水淹区域或在按影响进行定性筛选的第一步之后残留的多个水淹区域。

针对内部始发事件的一级概率安全评定中内部水淹的集成

7.90. 在这一步，应当使用基于内部始发事件的现有一级概率安全评定模式制定的概率模式来计算水淹对堆芯和/或燃料损坏频率的影响。这种模式通常用于计算特定水淹情况下的有条件的堆芯和/或燃料损坏概率。为了评定水淹假想方案发生的频率以及水淹导致必要的安全功能有条件的不可用的相关情况，应当就以下方面作出悲观假设：

(a) 水淹动力学和传播；

(b) 水淹对设备的影响（例如，假设水淹区域内的所有设备都不可用）；

(c) 水淹控制措施；

(d) 相关人因故障事件概率。

7.91. 根据这些假设，对于每个残留的水淹区域，应当修改内部始发事件的一级概率安全评定模式，以便绘制该区域内的水淹影响、水淹向其他区域的传播以及相关的始发事件和设备故障模式。这将允许要计算的每个水淹区域的有条件的堆芯和/或燃料损坏概率，由此可以使用公式 (1) 计算水淹对堆芯和/或燃料损坏频率的总体贡献。

水淹环境中的人为错误概率分析

7.92. 应当修改与恢复和跳堆后人为错误相关的概率，以评定内部水淹对内部始发事件的一级概率安全评定中模拟的信用恢复和人类行动的影响。针对内部水淹的 C 型人因故障事件的评定应当包括以下内容：

(a) 包含在内部始发事件的一级概率安全评定中但也与水淹假想方案相关的人因故障事件。在这种情况下，可能有必要修改绩效形成因素的评定，因为运行人员实施行动可能比基本情况下更困难（例如，由于与水淹环境相关的压力水平更高）。

(b) 仅与水淹相关的人因故障事件（例如，与电力供应的隔离和随后恢复相关的事件）。在这种情况下，用于评定水淹特定人因故障事件的方法通常可以遵守与用于分析其他类型人因故障事件的方法相同的原则。概率安全评定模式中还应当考虑水淹特定作用对电厂结构、系统和部件的影响。

(c) 运行人员对水淹导致虚假警报和指示的不良反应。

7.93. 在应用第 5.97－5.122 段提出的人的可靠性分析方法时，应当分析表现形成因素，考虑特定水淹影响，如额外的压力、可能存在的矛盾信号、湿度、温度、失去照明以及进入或通过受水淹影响区域的困难。

7.94. 如果内部始发事件的一级概率安全评定模式中计入人为恢复行动，则应当检查采取这些行动的可行性。例如，在受水淹影响的房间中可能很难执行特别恢复操作。

量化内部水淹对堆芯和/或燃料损坏频率的影响以便进行筛选

7.95. 对于定量筛选，应当采取保守的方法，假设受水淹影响区域的所有部件都将失效。如果这种假设不会对堆芯和/或燃料损坏频率（使用公式(1)计算）产生显著影响。可以从详细分析中筛选出水淹区域。但是，这些结果应当计入内部水淹一级概率安全评定的总体结果中。

7.96. 对于内部水淹的一级概率安全评定，应当定义根据对堆芯和/或燃料损坏频率的影响进行筛选的定量标准。这类标准的示例如下：

(a) 对于筛选出的所有水淹区域，水淹对堆芯和/或燃料损坏频率的累积贡献应当不超过规定的阈值。这个阈值可以定义为一个特定绝对值，也可以用相对的术语给出（例如，内部始发事件对堆芯和/或燃料损坏频率的贡献）。

(b) 对于单一水淹区域，水淹对堆芯和/或燃料损坏频率的贡献足够低，以保留所有风险显著的水淹假想方案。

7.97. 整个筛选过程（即按影响和频率进行筛选）的结果应当如下：

(a) 不代表显著风险因素的水淹假想方案或水淹区域清单，可从详细分析中筛选出来。然而，与筛选出的水淹假想方案或水淹区域相关的估计风险应当保留在内部水淹一级概率安全评定的总体结果中。

(b) 与水淹区域相关的水淹假想方案清单，这些水淹可能是风险的显著因素，因此需要进一步考虑。对于该清单中的每种水淹假想方案，应当制定一个针对内部水淹的定量一级概率安全评定模式，以供进一步分析。

水淹详细分析

水淹假想方案分析

7.98. 对水淹的详细分析应当旨在降低筛选过程中迄今确定的水淹假想方案的保守程度。只要有可能，它应当得到专门的巡视支持，以收集支持信息来核实详细的分析。尤其应当考虑到以下几个方面：

(a) 水淹区域内的防水淹屏障、实物分隔和隔离措施以及其他防水淹手段；
(b) 可信的结构、系统和部件的位置；
(c) 防水淹屏障的位置和有效性；
(d) 水淹假想方案的动态（例如水淹水位的变化率）；
(e) 水淹效应，如水淹、湿度、温度、压力、喷淋、蒸汽、管道甩鞭或喷射冲击。

7.99. 所有可能造成水淹的事件都应当从探测和控制手段的角度进行分析。然后，在估计未检测和未隔离的概率时，应当考虑检测和控制手段。

7.100. 应当应用更现实的模式来评定旨在减少设备损坏和水淹传播可能性的人员行动，以及水淹对结构、系统和部件的影响。

7.101. 应当评定水灾对人类行为的影响，特别是以下方面：

(a) 水淹开始后，需要运行人员采取行动以确保所需安全功能的电厂位置的可达性；
(b) 压力水平增加；
(c) 指示失效或指示错误；
(d) 水淹对运行人员行为的其他影响。

危害组合分析

7.102. 第 6.12 段提到的所有三种组合类型的内部水淹和其他危害组合发生的可能性（如 SSG-64[6]所定义）应当进行评定。涉及内部水淹的组合。因此，对于这些危害，应当在一级概率安全评定中考虑其他危害，而对于内部水淹，应当在一级概率安全评定中考虑涉及内部水淹和其他间接危害的组合。对于因共因与其他危害相关的内部水淹组合，以及内部水淹与未筛选出的非相关危害（同时发生但独立发生）的组合，分析人员应当决定这

些危害组合是否应当在内部水淹或其他危害之一的一级概率安全评定中考虑。

7.103. 应对其他危害（如地震活动、外部洪水、飞机坠毁、内部火灾）导致内部水淹进行定性分析，作为始发事件分析的一部分（见第 6 部分）。应当分析其他危害和水淹的组合影响对安全可能很重要的水淹区域。要考虑的影响示例包括由危害导致水淹来源和采取人工防水淹措施的困难（见第 8 部分，洞察针对外部危害的一级概率安全评定建议）。此外，因启动消防系统排放大量水而导致水淹应当在内部火灾的一级概率安全评定范围内处理（见第 7.62 段）。

内部水淹风险的量化

7.104. 为详细分析内部水淹的一级概率安全评定而制定的特定模式（例如，评定水淹导致部件虚假驱动影响的模式）应当包括在完整的一级概率安全评定模式中。

7.105. 考虑到详细分析的结果，应对筛选后残留的水淹区域进行内部水淹对堆芯和/或燃料损坏频率的影响的最终量化。用于按频率定量筛选水淹区域的结果和模式应当包含在内部水淹的一级概率安全评定中。应当通过确定堆芯和/或燃料损坏频率的主要因素（如水淹区域、水淹假想方案、相关人类行动）来解释内部水淹的一级概率安全评定结果。在最后阶段，应当评审与筛选相关的假设，以估计筛选对堆芯和/或燃料损坏频率的影响。

7.106. 内部水淹一级概率安全评定模式的量化、不确定性分析、重要性分析和敏感性分析都应当遵守第 5 部分提出的建议。不确定性分析应当执行以识别不确定性的来源并对其进行评定。应当进行敏感性研究和重要性分析，以确定一级概率安全评定中对风险有显著影响的内部水淹要素。还应对重要的假设和数据进行敏感性研究。应当确定各种因素对计算结果的相对重要性。

内部水淹一级概率安全评定文件

7.107. 根据 GSR Part 4（Rev.1）[3]要求 20，内部水淹的一级概率安全评定需要以便于其评审、应用和更新的方式进行记录。文件中应当包括以下信息：

(a) 对电厂特有的防水淹功能的描述，包括非能动和能动缓解功能，以及将电厂划分为水淹区域；

(b) 描述用于评定内部水淹危害的特定方法和数据；

(c) 描述对内部始发事件的一级概率安全评定模式所做的修改，以考虑内部水淹的影响；

(d) 从分析中筛选出特定水淹假想方案和水淹区域的正当性；

(e) 水淹假想方案分析结果，包括详细分析；

(f) 水淹分析中假想描述；

(g) 内部水淹一级概率安全评定的最终结果，包括堆芯和/或燃料损坏频率、定性洞察和建议；

(h) 支持水淹分析的电厂巡视报告。

其他内部危害因素的分析

构筑物倒塌与重物跌落分析

7.108. 概率安全评定通常集中在未能冷却反应堆容器内的堆芯或贮存在乏燃料水池中的燃料。然而，也可能发生其他更直接的损坏，例如由于重物跌落到容器、乏燃料水池或执行临界安全功能的系统上。构筑物倒塌和物体坠落的可能性，特别是重物（例如，密封圆顶、反应堆压力容器顶盖、乏燃料容器、混凝土屏蔽块），应当分析其损坏安全重要结构、系统和部件的可能性，或其直接导致燃料组件机械损坏的可能性。

7.109. 如果运输负载的路径既不在燃料上方，也不在含有安全重要结构、系统和部件的区域上方，则可以筛选出某些导致构筑物倒塌或重物跌落的单独起始因子导致。

7.110. 概率分析应当包括除反应堆换料层之外装卸重物的位置。例如，一些电厂在汽轮机大厅中有开放区域，衰变热去除系统位于这些区域，这些区域容易受到重物跌落的影响（例如，试验设备可能会跌落并损坏连接到容器的管道）。

7.111. 构筑物倒塌或重物跌落的一级概率安全评定应当与为内部始发事件的一级概率安全评定制定的电厂响应模式一致（例如，见第 9.12 段）。

7.112. 应当考虑电厂中的所有永久性吊装设备。应当详细识别和检查构筑物倒塌或重物跌落可能对安全重要的结构、系统和部件产生不利影响的区域。为此，应当进行电厂巡视。

7.113. 在关闭期间，应当根据工作程序识别和分析装载运行。

7.114. 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。计算应当考虑机械设备故障、人为错误和自动保护功能可能不可用。

7.115. 对于构筑物倒塌或重物跌落与其他危害的组合，应当考虑以下对运行人员表现塑造因素的影响：

(a) 倒塌或重物跌落后，需要人员采取行动以确保所需安全功能的电厂位置的可达性；
(b) 压力水平增加；
(c) 指示失效或指示错误；
(d) 安全重要结构、系统和部件的虚假驱动；
(e) 构筑物倒塌或重物跌落对运行人员行为的组合影响。

7.116. 对于每一次重物跌落事件，应当保守地假设最大重物跌落，如有必要，应当分析重物跌落的性质及其跌落的原因。应当确定任何一枚或多枚飞射物的可能方向、大小、形状和能量，并评定其对厂房结构和电厂的影响。

7.117. 如果预见到二级概率安全评定，应当考虑每个构筑物倒塌或重物跌落事件，以确定潜在的放射性后果和对电厂损坏状态频率的影响（如果有）。

汽轮机飞射物分析

7.118. 汽轮机飞射物在汽轮机解体后的潜力应当从其潜在风险方面进行分析。对汽轮机解体的考虑应当包括汽轮机飞射物对可信的结构、系统和部件造成的损坏以及与汽轮机飞射物造成的次级效应相关的影响。汽轮机飞射物导致次要影响可能包括潜在的火灾（例如，由于氢气的点燃，由于石油燃烧）或水淹（例如，由于管道损坏）。

7.119. 汽轮机解体分析应当包括正常转速值和超速值。

7.120. 应当确定和描述潜在的汽轮机解体情况（例如，鉴于汽轮机的方向和位置，汽轮机解体后飞射物的分布）。对于每一种汽轮机解体情况，应当保守地假设飞射物生成方面的最坏配置和工况已经到位。应当确定飞射物的可能方向、大小、形状和能量，并评定对厂房结构和电厂的影响。

7.121. 应当考虑到具有足够动能穿透厂房的飞射物比例，确定对厂房内安全至关重要的结构、系统和部件的最终故障概率。

7.122. 在第一阶段，应当考虑之前在一级概率安全评定中确定的事故序列中计入的设备。

7.123. 飞射物撞击导致故障概率，以及安全重要幸存结构、系统和部件的随机故障概率和汽轮机解体频率，应当用于计算导致堆芯和/或燃料损坏的故障频率。

7.124. 应当进行电厂巡视，以确认分析中关于保护结构、系统和部件免受汽轮机飞射物撞击的假设。

7.125. 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。

7.126. 对于汽轮机解体后飞射物与其他危害的组合，应当考虑到对运行人员绩效影响因素的以下影响：

(a) 汽轮机解体开始后，需要人员采取行动以确保所需安全功能的电厂位置的可达性；
(b) 压力水平增加；
(c) 指示失效或指示错误；
(d) 安全重要结构、系统和部件的虚假驱动；
(e) 汽轮机解体后飞射物对运行人员行为的组合影响。

7.127. 如果预见到二级概率安全评定，应当考虑每个汽轮机解体事件，以确定潜在的放射性后果和对电厂损坏状态频率的影响（如果有）。

内部爆炸的分析

7.128. 考虑到核电厂的设计是为了最大限度地减少内部爆炸的可能性和影响，针对内部危害进行一级概率安全评定的一般流程应当适用于针对内部爆炸的一级概率安全评定。内部爆炸的概率安全评定应当考虑爆炸的潜在

原因或来源，如储氢和高能电弧故障。在内部火灾的一级概率安全评定中，应当考虑由内部火灾引起或导致内部火灾的内部爆炸分析。

7.129. 厂房的设计提供了预防和缓解爆炸的措施（见 SSG-64[6]）。出于设计目的，爆炸的系统化分析用于描述潜在爆炸源的表征（例如，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（例如，超压、脉冲或阻力负载、火灾、热量）以及预防特点。内部爆炸的一级概率安全评定应当主要依赖于这些分析过程中收集的信息和数据，以便对爆炸假想方案进行定性筛选。

7.130. 应当进行电厂巡视，以识别潜在的爆炸源并进行核实。

7.131. 应当按照第 5 部分的建议评定爆炸事件的频率。量化应当考虑电厂内爆炸性材料的数量、可能导致爆炸的人类行动以及预防手段的有效性（如氢气检测设备、爆炸性液体或气体探测器的泄漏、通风）。

其他可信内部隐患分析

7.132. 对内部危害进行一级概率安全评定的一般流程应当适用于筛选单一或危害组合后残留的所有其他内部危害的一级概率安全评定。

7.133. 应当进行电厂巡视，以识别其他可信内部危害的潜在来源并进行核实。

8. 外部危害一级概率安全评定的特定方面

概述

8.1. 本部分提供了满足 GSR Part 4（Rev.1）[3]针对外部危害的一级概率安全评定要求 6－13 的建议。特定建议仅针对以下清单中无法针对某一特定核电厂场址进行筛选的选定外部危害：

(a) 外部自然灾害：
    (i) 地震危害；
    (ii) 水文灾害（如外部洪水）；
    (iii) 气象灾害（如大风、降水）；

(iv) 地外灾害（如陨石、太阳耀斑）；

(v) 生物危害；

(vi) 地质灾害；

(vii) 天然火灾。

(b) 外部人类引发危害：

(i) （军用或民用飞机）意外坠毁；

(ii) 场外爆炸压力波（爆炸）（来自工业或军事设施）；

(iii) 场外运输事故（航空、铁路、公路、水上）；

(iv) 场外工业贮存事故；

(v) 危害物质的意外场外排放；

(vi) 场外电磁干扰；

(vii) 场外人为火灾；

(viii) 其他军事事故；

(ix) 其他工业事故。

8.2. 外部危害（见第 6.1 (b) 段、第 6.9 段和附件 I）应当在边界评定和/或详细分析的框架内加以考虑。在考虑一级概率安全评定中的外部危害时，应当采用一致的方法。它通常包括以下任务：

(a) 在可行的情况下，通过电厂巡视支持场址和电厂信息的收集。

(b) 危害表征：识别外部危害，计算危害频率，分析外部危害的影响。

(c) 从内部始发事件的一级概率安全评定推导出外部危害的一级概率安全评定：

(i) 确定由外部危害导致始发事件；

(ii) 确定对内部始发事件的一级概率安全评定的现有事件树和故障树的必要修订；

(iii) 特定依赖性和共因故障的分析；

(iv) 特定数据的分析；

(v) 特定人的可靠性方面的分析。

(d) 定性和/或定量筛选。

(e) 量化外部危害对堆芯和/或燃料损坏频率的影响（即结果分析、敏感性研究以及不确定性和重要性分析）。

(f) 文件（特别考虑分析中使用的假设和参考，包括质量保证）。

一级概率安全评定外部危害边界评定

概述

8.3. 进行边界评定的目的是减少需要详细分析的外部危害清单，从而关注风险显著的事故假想方案。边界评定应当确保与特定外部危害相关的风险与其他危害相比忽略不计。

8.4. 筛选过程后残留的外部危害对堆芯和/或燃料损坏频率的影响应当使用这些危害的一级概率安全评定来确定。针对外部危害的一级概率安全评定应当依赖于针对内部始发事件的一级概率安全评定制定的电厂响应模式，包括功率运行和关闭状态。针对内部始发事件的一级概率安全评定的可用性应当是针对外部危害制定一级概率安全评定的先决条件。除了通过对内部始发事件（例如，由于极端外部危害导致汽轮机厂房损坏）执行一级概率安全评定发现的事件之外，危害分析的结果可能会产生进一步的始发事件。在这种情况下，应当制定新的事故序列并将其整合到一级概率安全评定中。

8.5. 影响分析应当考虑危害导致部件故障对概率安全评定中包含的始发事件以及相关缓解安全功能的影响。

8.6. 基本的场址和电厂信息应当从图纸或数据库中获得。对于运行电厂，该类信息应当通过电厂巡视进行核实和完成。

8.7. 由于电厂巡视的信息可能会为外部危害的一级概率安全评定提供重要的输入，因此该类巡视应当得到良好的计划、组织和完整的记录。

8.8. 在边界评定中，应当考虑到未排除的每种外部危害对核电厂的所有潜在影响。[43]

[43] 影响分类的示例包括场外断电或电站断电，最终散热器的退化或丧失，危害物质的爆炸或排放，以及电厂通风退化或隔离（由于有毒影响的风险）。

8.9. 受边界评定影响的外部危害的累积贡献应当计算并保留在一级概率安全评定的最终结果中。

8.10. 应当为特定外部危害制定一套假想方案，除非危害对电厂的所有影响都可以由单一假想方案限定，但通常情况下并非如此。

8.11. 在边界评定中，还应当考虑第 6 部分描述的外部危害的适用组合。

8.12. 边界估计应当基于现实但明显保守的模式和数据。这些模式和数据包括：

(a) 评定危害发生频率（即估计超过特定强度的频率）；
(b) 分析危害对电厂的影响（即与危害相关的负载）；
(c) 电厂响应分析（即脆弱性）；
(d) 电厂的一级概率安全评定模式和数据。

8.13. 应当评定是否需要在一级概率安全评定中考虑以下气象灾害：

(a) 温度导致危害：
    (i) 低温现象的危害；
    (ii) 高温现象的危害。
(b) 大风危害：
    (i) 温带大风（如温带气旋、雷暴、飑线、天气锋面）；
    (ii) 龙卷风或水龙卷；
    (iii) 下击暴流或下沉风；
    (iv) 热带气旋、飓风或台风；
    (v) 盐暴或沙尘暴；
    (vi) 盐雾风；
    (vii) 风致飞射物。
(c) 积雪危害。
(d) 空气湿度危害。
(e) 闪电。
(f) 冰雹。
(g) 气压危害。

(h) 雾和薄雾。

8.14. 应当评定是否需要在一级概率安全评定中考虑以下水文危害：

(a) 高水位（洪水）危害：

(i) 快速发展：

— 极端局部降水导致山洪爆发；

— 海啸；

— 冰洪；

— 上游挡水构筑物失效导致河流洪水；

— 下游河流堵塞造成的河道洪水；

— 滑坡、雪崩或火山活动导致波浪；

— 湖震；

— 火山导致冰和雪融化导致洪水。

(ii) 缓慢发展：

— 风暴潮；

— 电厂边界外的极端降水（如雨、雪）导致河流洪水；

— 下游河道变化导致洪水；

— 由潮汐或大潮导致洪水。

(b) 低水位危害：

(i) 快速发展：

— 下游挡水构筑物失效导致河流洪水；

— 冰凌；

— 上游河流堵塞导致洪水。

(ii) 缓慢发展：

— 干旱；

— 上游河道变化导致河流洪水；

— 海平面低。

(c) 本地降水（如雨、雪）：

(i) 局部降水导致屋顶负载增加；

(ii) 局部降水导致局部洪水。

(d) 地下水位：

(i) 地下水位高；

(ii) 地下水位低。

(e) 非生物漂浮物。

自然灾害

地震危害

8.15. 在许多一级概率安全评定中，地震危害是堆芯和/或燃料损坏频率的显著因素，因此，应当进行详细的分析。然而，为了限制地震危害的一级概率安全评定所需的努力，可以对一定范围的地震危害进行边界评定（例如，带有悲观假想简化分析）。在这一阶段还应当考虑地震危害的次生影响（如地震导致火灾和水淹）。SSG-89[7]和 SSG-68[25]提供了额外建议，参考文献[29、35]提供了更多信息。

外部洪水

8.16. 第 8.14 段列出的与洪水相关的灾害类型应当予以考虑，并根据场址特征进行边界评定或详细分析。外部洪水灾害与其他危害的适用组合，如第 6.3 段所述也应当予以考虑，同时考虑到可能的依赖关系（例如高水位、随之而来的溃坝）。

8.17. 大雨和其他洪水的后果，如屋顶和低洼场区积水，应当包括在分析范围内。

大风

8.18. 第 8.13 段列出的大风类型应当予以考虑，并根据场址特征进行边界评定或详细分析。如第 6.3 段所述，大风与其他危害的适用组合也应当考虑到可能的依赖性（如大风和高水位）。

其他自然灾害

8.19. 在边界评定中，应当考虑除地震危害、水文灾害和气象灾害之外的潜在自然灾害的组合清单。附件 I 列出的自然灾害清单和电厂安全分析报告中考虑的自然灾害清单应当作为确定危害的基础。如果适用，还应当考虑场址特定自然灾害。

8.20. 如第 6.3 段所述，自然灾害与其他灾害的适用组合应当考虑到可能的依赖性（例如恶劣天气条件、运输事故、内部火灾）。

人类引发危害

8.21. 应当评定是否需要在一级概率安全评定中考虑下列人类引发危害：

(a) 机械撞击：
  (i) 来自民用和军用运输事故，包括飞机坠毁以及航空、铁路、公路和水运；
  (ii) 来自工业事故；
  (iii) 来自军事事故。
(b) 人类引发火灾：
  (i) 来自交通事故；
  (ii) 来自工业事故；
  (iii) 来自军事事故。
(c) 爆炸（冲击波）：
  (i) 来自交通事故；
  (ii) 来自工业事故；
  (iii) 来自军事事故。
(d) 危害物质（如窒息性、可燃性、腐蚀性、爆炸性、毒性或放射性物质）的排放：
  (i) 来自交通事故；
  (ii) 来自工业事故；
  (iii) 来自军事事故；
  (iv) 来自管道事故。
(e) 其他危害：
  (i) 电厂边界外的挖掘或厂房工程；
  (ii) 电网不稳定；
  (iii) 高压绝缘的工业杂质；
  (iv) 电磁干扰；
  (v) 人类引发地面沉降。

8.22. 至少应当考虑下列人类引发危害来源：

(a) 火灾从附近设施传播，或由于运输或管道事故；
(b) 附近设施或运输或管道事故造成的固态物质或气体云爆炸；
(c) 从附近设施或由于运输或管道事故而排放化学物质；
(d) 飞机坠毁；
(e) 船舶与进水口构筑物的碰撞。

以下来源也可被视为人类引发危害：

(a) 场外来源（如无线电发射机、军用雷达站、粒子加速器、高压输电线路、电话网络）导致电磁干扰；
(b) 场址边界外的挖掘工作。

外部危害的参数化

概述

8.23. 应当界定与外部危害的潜在损坏相关的最重要参数。如果危害的潜在损坏不能用一个参数来描述，则应当定义几个参数。

自然灾害

地震危害

8.24. 地震危害的表征是以下主要参数（见 SSG-89[7]和参考文献[29]）：

(a) 峰值地面运动（如加速度、速度、位移）；
(b) 频率和/或能量含量，通常由与地面响应谱相关的谱加速度表示，但也可能包括其他强度测量。

8.25. 地震导致地面振动应当不被排除在考虑范围之外，因为地震波可以到达地球表面的任何一点。

8.26. 地震地面运动应当不被筛选掉。

外部洪水

8.27. 外部洪水的潜在破坏可以用流量、速度、水位、持续时间和波浪作用的贡献来表征。对于外部洪水的表征，应当估计这些参数中的部分或全部（见 SSG-18[28]）。对于洪水，通常使用以下参数：

(a) 河流：水位、排水量/流速和洪水持续时间；

(b) 海洋或湖泊：水位、洪水持续时间和流速；

(c) 波浪：高度、长度、周期、风速和风向；

(d) 波浪上升：高度、溢出水量和每秒水量；

(e) 湖震：振荡频率和波高；

(f) 冰：厚度和流速。

8.28. 风的速度、方向和持续时间可能与洪水同时发生，应当作为一种潜在的危害组合加以考虑。

大风

8.29. 应当根据风的类型考虑不同的参数，如下所示：

(a) 阵风的动态负载和特定时间段（例如 10 分钟）内平均的风的负载是表征连续平移风的基本参数。

(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）是表征龙卷风的基本参数。

其他自然灾害

8.30. 各种各样的自然灾害可能适用于特定场址。对于每一种特定危害，应当规定与危害相关的所有潜在影响的参数。

8.31. 选择每种危害的参数时，应当能够对危害的组合影响进行分析。

人类引发危害

8.32. 对于每一人类引发危害，应当根据其对安全具有重要意义的结构、系统和部件的特定挑战来确定参数，示例如下：

(a) 对于许多与运输相关的危害，实际危害来自爆炸或危害物质的排放。关键参数是运输的物质量或事故中可能排放的最大数量。

(b) 对于附近工业设施的排放，危害物质的性质和事故中可能排放的最大量是合适的参数。

(c) 对于碰撞（例如驳船与进水口碰撞、飞机与厂房碰撞），关键参数应当与撞击相关（即撞击物体的质量和速度）。

(d) 如果人类引发危害是由直接撞击后的爆炸导致（如飞机坠毁），关键参数应当包括机载燃料量和可能损坏构筑物的重型物项（如发动机）质量的某种组合。

(e) 对于管道事故等危害，可能排放的物质库存以及物质的性质和压力是适当的参数。

8.33. 每种人类引发危害都可能导致需要考虑的各种影响因素的组合。例如，飞机坠毁可能会导致直接损坏、爆炸、火灾和振动。同样，管道事故可能导致爆炸（爆燃或爆炸产生的脉冲负载）、火灾和振动。它还可能生产影响电厂不同部分的飞射物。在确定人类引发危害的表征时，所有主要和次要影响应当考虑到。无论导致的起始因子如何，其效果都应用以下参数表示：

(a) 冲击负载；

(b) 热负载；

(c) 振动负载；

(d) 有毒气体的传播。

8.34. 对于气体云的爆炸，应当考虑从其起源点到电厂的潜在漂移。

8.35. 如第 6.3 段所述，人类引发危害与其他危害的适用组合应当考虑到可能的依赖关系（如化学品排放、风速和风向）。

外部危害的详细分析

8.36. 应对所有（单一和组合）危害进行详细分析，对于这些危害，带有悲观假想界限或简化分析已证明危害的风险不可忽略。

8.37. 内部始发事件的一级概率安全评定模式是对外部危害进行详细分析的先决条件。

8.38. 详细分析应当基于现实的模式和数据，包括一个全面的一级概率安全评定模式，该模式提供了对与所考虑的外部危害相关的所有现象进行建模的可能性。

外部危害频率评定

概述

8.39. SSR-1[24]第 4.20 段指出：

> “核装置的场址评价必须考虑可能影响核装置安全的自然和人类引发外部事件的频率和严重程度，以及这些事件的潜在组合。”

因此，危害评定的结果应当包括危害的频率和严重程度，并应当适当考虑不确定性。

8.40. 外部危害的表征是多个输出参数，其中一些可能是概率相关的。为简单起见，危害曲线通常用有限数量的参数（通常是一个）来描述。在响应分析和脆弱性评价中，通常会考虑更完整地描述危害所需的其他参数。

8.41. 超过特定强度频率的估计应基于特定场址的概率评价。

8.42. 应当进行时间趋势分析（例如，由于气候变化，水文或气象参数随时间的变化），以确认不存在危害频率增加的趋势。如果确认频率显著增加的趋势，则应当界定危害频率，以便在兴趣时间段内考虑到气候变化。应当不考虑最近危害频率下降的短期趋势，除非很好地理解这些趋势是由具有非随机性质的过程导致。[44]

8.43. 当危害频率是在区域或一般基础上确定的时，应当进行评定，目的是洞察这些数据在多大程度上适用于特定场址以及是最新的。与使用区域和一般数据相关的不确定性应当反映在危害曲线族中（如有）。

8.44. 当专家启发或其他基于专家的过程被用于制定危害曲线时，应当建立并遵守该过程的程序。SSG-79[26]、SSG-9（Rev.1）[27]、SSG-18[28]和

[44] 例如，在河床中观察到的多样性可以用来证明相关运输事故的频率降低的正当性。

原子能机构《安全标准丛书》第 SSG-21 号《核装置场址评价中火山灾害》[36]提供了关于危害评定方法的建议。

自然灾害

地震危害

8.45. 场址地震地面运动的发生频率应当基于场址特定概率地震风险评定（见 SSG-89[7]和参考文献[29、35]）。

8.46. 概率地震危害评定应当根据 SSG-9（Rev.1）[27]提供的建议进行。

8.47. 用于表征地震危害的参数范围应当涵盖兴趣加速度范围（例如，从“无故障“到“筛选限值”），以便准确估计地震风险。

8.48. 对于危害分析中使用的下限参数值，应当证明任何较低参数值的地震事件只会对结构、系统和部件造成忽略不计的损坏，包括场外的结构、系统和部件，如输送危害物质的电线和管道。

外部洪水

8.49. 外部洪水的频率和后果的计算应当基于概率分析，该分析反映了最近可用的场址特定信息。如果该场址的数据仅在短期内可用，则应当使用区域洪水数据，并确认这些数据的适用性（即可使用相关性分析来确认区域数据对该场址的适用性）。

8.50. 外部洪水危害评定应当根据 SSG-18[28]提供的建议进行。

8.51. 应当适当考虑模式和参数值中的不确定性，并充分传播这些不确定性，以便获得一系列危害曲线，从中可以导出平均危害曲线。对极端河流洪水的频率和后果的分析应当包括单坝或级联坝溃坝造成的洪水。

8.52. 极端海洋洪水的频率和后果的计算应当基于概率分析，该分析应当反映最近的、可用的、特定场址的信息。这些数据应当有更长时期的数据支持对于其他沿海地区，适当考虑该地区的地形，包括调整后的沿海地区内和陆地上的地形。应当始终考虑大浪和大风的组合。

8.53. 极端湖泊洪水的频率和后果的计算应当基于概率分析，该分析反映了最近的、可用的、特定场址的信息。应当始终考虑风浪的影响，包括任何潜在的龙卷风导致排水量。

8.54. 海啸频率和后果的计算应当基于由工程分析支持的可靠区域数据。应当考虑到与海啸的频率和后果相关的不确定性。

8.55. 外部洪水危害评定应当考虑相关的时间趋势（如气候变化）。

大风

8.56. 用于计算大风频率和强度的模式应当基于反映最近、可用、区域和特定场址信息的特定场址数据。分析至少应当包括场址经历的最恶劣天气条件。因此，大风频率降低的近期短期趋势应当不在风频率评定中占主导地位。

8.57. 应当根据 SSG-18[28]提供的建议进行大风危害评定。

8.58. 用于描述风危害的参数范围应当涵盖兴趣范围（例如，从“无故障”到“筛选限值”），以便准确估计风风险。

8.59. 大风危害评定应当考虑一段时间内的相关趋势（例如，由于气候变化）。

8.60. 对于温带风暴和其他涉及高直风现象的评价，应当使用适合场址的记录风速数据。在绘制大风危害曲线时，应当保守地考虑因缺少气象站而产生的不确定性。

其他自然灾害

8.61. 应当制定一个全面的数据库，用于支持特定自然灾害的频率评定。该数据库应当包括所有必要的相关信息，以支持对危害曲线的现实和有效估计。特别是关于场址附近和该区域发生灾害的历史信息应当纳入现有数据期的数据库。

8.62. 应当使用特定场址和区域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数据的使用。

8.63. 在特定情况下，当既没有特定场址的数据也没有区域数据时，可以使用全球数据。在使用全球数据时，应当调查这些数据对所考虑场址的适用性，并记录用于分析的所有假设。

人类引发危害

8.64. 应当根据 SSG-79[26]提供的建议对人类引发外部危害进行评定。

8.65. 应当收集适当的信息（最好以数据库的形式），并用于支持特定人类引发危害的频率评定。这一信息至少应当包括以下必要数据，以支持对危害频率的现实和有效估计：

(a) 关于贮存在核电厂预定半径内场址边界以外的危害（例如可燃、爆炸性、窒息性、毒性、腐蚀性）材料成分的定性和定量信息如下：
   (i) 潜在危害源（在核电厂的预定半径内）如下：
      — 石油或天然气贮存设施；
      — 石油或天然气运输线路；
      — 危害物质的空运；
      — 危害物质的铁路运输；
      — 危害物质的公路运输；
      — 危害物质的水上运输；
      — 其他设施。
   (ii) 潜在危害源到核电厂下列区域的距离（公里）：
      — 构筑物；
      — 存放安全重要物项的厂房；
      — 通风进气口。

(b) 其活动可能影响电厂的军事或其他训练设施的位置，以及训练演习频率的说明。

(c) 事故的可能性和频率及其潜在后果（如爆炸能力）。

结构、系统和部件脆弱性分析

概述

8.66. 结构、系统和部件的脆弱性[45]应当使用可用的电厂特定信息进行评定，以达到分析（即边界评定或详细分析）和公认工程方法的必要程度。分析中应当考虑电厂巡视的结果。

8.67. 脆弱性分析应当不局限于场内构筑物，而应当包括场外构筑物，如输电线和运载危害物质的管道，因为涉及该类场外结构的故障可能会导致场外断电或爆炸等事件。如果脆弱性较低，这种故障可能高度相关。

8.68. 脆弱性应当表示为危害参数的函数。脆弱性分析应当包括基础信息中的不确定性，特别是当使用电厂特定数据以外的数据（即一般数据）时。

8.69. 当考虑危害组合时，导致结构、系统和部件故障模式的所有特定危害故障机制都应当包括在一级概率安全评定模式中。如果危害组合具有不同的故障机制，则故障应当由单一危害脆弱性来表示。如果危害组合具有相似的破坏机制，则应当考虑复合脆弱性。

自然灾害

地震危害

8.70. 用于地震脆弱性分析的结构、系统和部件的初始清单应当基于包含在内部始发事件的一级概率安全评定模式中的结构、系统和部件。该清单应当扩大到包括所有结构、系统和部件及其组合，如果失效，可能导致堆芯和/或燃料损坏频率或大排放频率，后者对于二级概率安全评定考虑很重要。

8.71. 抗震设备清单应当补充与第 6.12 段指出的任何危害组合相关的任何结构、系统和部件，并在分析中保留。根据保留的危害组合，这可能包括系统识别的大坝、海啸墙、内部水淹源或内部火源。参考文献[35]提供了抗震设备清单制定的详细信息。

---

[45] 在这种情况下，脆弱性是指在给定的危害输入水平下，结构、系统和部件发生故障的条件概率。

8.72. 应当通过评审电厂设计文件和电厂巡视来确定地震期间和地震后干扰设备可运行性的结构、系统和部件的所有实际故障模式。巡视将启用以下功能：

(a) 确定相关考虑因素（例如，在同一厂房的同一楼层上具有相同配置、方向或锚固的相同设备）；
(b) 检验运行人员对潜在地震导致干扰的响应路径；
(c) 确定未列入抗震设备清单，但其结构故障可能影响清单上附近物项的设备或结构（即地震相互作用问题）；
(d) 考虑与地震导致火灾和地震导致水淹相关的问题。

8.73. 应当评价结构（如滑动、倾覆、屈服、过度漂移）、设备（如锚固故障、与相邻设备或结构的撞击、支撑故障、功能故障、水淹和喷淋考虑的压力边界突破）和土壤（如液化、边坡失稳、超差沉降）的所有相关故障模式的脆弱性。地震脆弱性分析的细节见参考文献[29、35]。

8.74. 部件的极限脆弱性应当作为与点火故障模式相关脆弱性的替代物。应当使用条件点火概率将功能故障与火灾点火联系起来。参考文献[37]提供了示例。

8.75. 脆弱性分析应当得到电厂巡视的支持。巡视应当集中在锚固和横向抗震支撑上。

8.76. 地震相互作用的可能性（例如，结构、系统和部件可能落入抗震设备清单物项的可能性），包括与火灾和水淹的额外相互作用的可能性，也应当是巡视的重点。

8.77. 与地震脆弱性相关的参数（如结构的中值抗震能力及其可变性）的计算应当基于电厂特定数据，并辅以实际地震数据、脆弱性试验数据和一般鉴定试验数据。

8.78. 当根据一般数据筛选出低脆弱性的结构、系统和部件时，应当证明一般数据是以保守的方式使用的，并且没有忽略相关的电厂和场址特异性特点。

8.79. 应当根据锚定在地面运动参数（如平均谱加速度）上的场址特定地震响应谱来估计结构、系统和部件在其破坏水平下的地震响应。

8.80. 在制定位于不同厂房中的结构、系统和部件响应的联合概率分布时，应当考虑输入地面运动以及结构和土壤特性的不确定性。

8.81. 对于出现在主要事故序列中的所有结构、系统和部件，应确保相关的场址特定脆弱性参数是基于电厂特定信息得出的。这对于避免一级概率安全评定的结果和洞察中地震危害的贡献被扭曲至关重要。

8.82. 对于不是建立在岩石地基上的电厂结构，需要进行土壤－结构相互作用分析，包括嵌入效应和地面运动非相干函数。即使对于建立在岩石地基上的结构，考虑地面运动非相干性的土壤－结构相互作用分析的性能将有利于计算真实的地震响应，并可能降低高频范围内的响应谱峰值，由于统一危害响应谱的高频含量，预计会出现这种情况。

外部洪水

8.83. 应当针对与河流高洪水水位相对应的条件进行大坝破坏分析，并确定相关频率。应当计算河流中不同水位的大坝溃坝概率。[46]

8.84. 在评定结构、系统和部件在外部洪水方面的脆弱性时，应当使用电厂特定数据。电厂巡视的结果应当作为评定中的重要信息来源。所有位于低水平的构筑物，尤其是进气口和最终散热器都应当考虑在内。

8.85. 脆弱性分析应当包括浸没、波浪对结构、系统和部件的动态负载和地基破坏（土壤侵蚀）。关于外部洪水脆弱性分析的更多细节见参考文献[32]。

大风

8.86. 在评定大风的影响时，应当考虑对安全重要的结构、系统和部件周围外部屏障（即墙壁和屋顶）的特定特点、任何暴露于天气的结构、系统和部件或其组合，以及风载飞射物撞击或其他影响（如结构损坏、通风管道倒塌）造成的损坏后果，这些后果可能导致始发事件或系统故障。应对电厂厂房及其周围环境进行调查，以评定可能被大风卷起并可能成为飞射物物体的数量和类型。飞射物撞击的概率也应当在最先进方法的基础上制定。

[46] 对于高于溃坝设计水位的河流水位，通常假设溃坝。

8.87. 应当进行评价，以估计那些结构、系统和部件或其组合在大风方面电厂特定、现实的脆弱性，其故障可能导致始发事件。

8.88. 在评价结构、系统和部件与风相关的脆弱性时，应当使用电厂特定数据（例如，防风设备的锚固、防风飞射物屏障的安装）。评定中应考虑任何可能落入或落在对安全重要的结构上从而造成损坏。在此评定中，电厂巡视的结果应当被用作重要的信息来源（例如，为脆弱性分析的任何建模参数提供依据）。

8.89. 应当构建对应于每个结构、系统和部件的特定故障模式的脆弱性曲线族，并用中值风速容量和不确定性特征（如对数标准偏差）表示，代表结构、系统和部件容量的随机性和中值容量的不确定性。关于大风脆弱性分析的更多细节见参考文献[32]。

其他自然灾害

8.90. 对于其他适用的自然灾害，应当符合地震、水文和气象灾害脆弱性分析的一般方面和建议。

人类引发危害

8.91. 对于适用的人类引发危害，应当遵守与自然灾害相关的结构、系统和部件脆弱性分析的概述和建议。关于飞机撞击、爆炸和危害物质排放的脆弱性分析和容量分析的更多细节见参考文献[32]。

将外部危害纳入一级概率安全评定模式

概述

8.92. 内部始发事件的一级概率安全评定模式几乎总是用作外部危害的一级概率安全评定模式的基础。外部危害的一级概率安全评定模式应当改编自内部始发事件的一级概率安全评定模式，以纳入因外部危害的影响而不同的方面。在从概率安全评定模式中为内部始发事件选择适当的事件树时，应当评定可能导致不同分级内部始发事件（例如，大量冷却剂丧失事故、少量冷却剂丧失事故、瞬变事故）或可能直接导致堆芯和/或燃料损坏的危害的主要影响（例如，通过使用危害事件树）。附件 II 提供了一个地震危害的地震事件树的示例。安全重要结构、系统和部件的适当危害曲线和脆弱

性应当纳入外部危害的一级概率安全评定模式。与特定危害相关的所有重要依赖性、相关性和不确定性都应当在外部危害的一级概率安全评定模式中考虑。

8.93. 应当修订与恢复和行程后人为错误相关的概率，以评定外部危害对内部始发事件的一级概率安全评定中模拟的信用恢复和人类行动的影响。

8.94. 针对外部危害的 C 型人因故障事件的评定应当包括以下内容：

(a) 包含在内部始发事件的一级概率安全评定中但也与外部危害假想方案相关的人因故障事件 [47]。在这种情况下，可能有必要修订对绩效影响因素的评定，因为运行人员实施行动可能比基本情况下更困难（例如，由于与危害环境相关的压力水平更高）。

(b) 仅与特定外部危害相关的人因故障事件（例如，与地震事件后继电器复位相关的事件）。在这种情况下，用于评定外部危害特定人因故障事件的方法通常可以遵守与用于分析其他类型人因故障事件的方法相同的原则。

(c) 运行人员对虚假警报和指示的不当响应。

8.95. 外部危害的一级概率安全评定模式应当反映电厂的竣工和运行工况。

自然灾害

地震危害

8.96. 内部始发事件的一级概率安全评定模式应当适当纳入地震的特定方面，不同于相应的内部始发事件的一级概率安全评定模式的各个方面。SSG-68[25]提供了关于概率安全评定模式中地震事件整合的建议，参考文献[35]给出了更多信息。

8.97. 在许多电厂，对于超过一定震级的地震危害（例如，设计基准地震的 50%），电厂会启动手动关闭。地震危害的一级概率安全评定模式应当反

[47] 在外部危害的情况下，与部署便携式设备有关的人因故障事件可能特别重要，如第 5.110 段所述，目前人的可靠性分析方法可能需要调整和补充，以处理与部署便携式设备有关的特定情况。有关便携式设备人的可靠性分析的更多信息见参考文献[17]。

映这一点，即使在电力转换系统具有高抗震能力和可以避免自动反应堆停堆的情况下。

8.98. 地震危害的一级概率安全评定模式应当包括所有可能导致堆芯和/或燃料损坏的重要地震导致始发事件。特别是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）的故障和现场构筑物（如堤坝）的损坏。

(b) 各种规模和位置的冷却剂丧失事故。地震导致的由小管线（如脉冲管线）破裂导致非常小的冷却剂丧失事故也应当在地震危害的一级概率安全评定模式中作为额外故障模式考虑。

(c) 场外断电。

(d) 瞬变（有或没有电力转换系统故障），包括各种支持系统的损耗。

(e) 重物跌落（如环吊）。

8.99. 地震导致的始发事件导致内部始发事件的一级概率安全评定模式中未考虑的特定事故假想方案时，应当将特定事故序列的模式添加到内部始发事件的一级概率安全评定模式中。内部始发事件的一级概率安全评定模式应当进行扩展，以便将地震危害纳入一级概率安全评定，从而纳入更广泛的部件故障或部件故障模式，如非能动部件故障（如结构、厂房、配电系统、电缆槽、继电器颤动）。应当考虑对反应堆内部构件的影响，特别是由于反应堆堆芯上的地震事件而导致控制棒卡住。

8.100. 针对内部始发事件在一级概率安全评定中建模的所有结构、系统和部件以及地震导致的损坏可能对事故序列产生影响的结构、系统和部件应当纳入针对地震危害的一级概率安全评定模式。

8.101. 地震危害的一级概率安全评定模式应当包括所有非地震相关的故障、结构、系统和部件的不可用性以及可能对堆芯和/或燃料损坏频率产生显著影响的人为错误。

8.102. 结构、系统和部件的地震导致损坏模式应当充分考虑厂房因地震事件而损坏后位于厂房内设备的所有相关故障。如果要从模式中消除该类的依赖，或者如果要降低它们在模式中的重要性，这应当是正当的。

8.103. 地震危害评定，地震脆弱性，结构、系统和部件之间的依赖性和地震相关性，非地震导致故障，结构、系统和部件的不可用性和人为错误应当适当整合到地震危害的一级概率安全评定模式中。

8.104. 应当针对恢复措施和人为错误的可能性进行彻底检查和相关调整。由于一定震级地震事件的影响而无法执行的恢复行动应当从一级概率安全评定模式中删除，或者，应当增加执行操作时失败的概率。响应始发事件时可能发生的所有后起始因子人为错误，如内部始发事件的一级概率安全评定中所模拟的，应当针对特定地震条件进行修订和调整。至少应当考虑到以下地震导致对运行人员绩效影响因素的影响：

(a) 需要人员采取行动以确保所需安全功能或救援人员电厂位置的可达性；
(b) 压力水平增加；
(c) 指示失效或指示错误；
(d) 通信系统故障；
(e) 影响运行人员行为的其他适用因素。

8.105. 在量化堆芯和/或燃料损坏频率时，除了组合结果之外，关于每个事故序列和最小割集的关键信息应当作为模式量化的结果可用。

8.106. 应对地震危害的一级概率安全评定模式进行整合和量化，以便从每个地震输入到一级概率安全评定的不确定性（即地震危害的频率、地震脆弱性、依赖性和与系统分析相关的方面）通过用于获得堆芯和/或燃料损坏频率的正确不确定性特征的模式。

外部洪水

8.107. 外部洪水导致事故序列的考虑应当包括场址特定危害曲线和所有结构、系统和部件的脆弱性，其损坏可能导致一级概率安全评定中模拟的设备故障。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为错误。应当调整人为错误的概率，以考虑洪水对表现形成因素（特别是设备的可达性）的影响，如第 8.94 段所述。

8.108. 在制定由外部洪水导致始发事件的事故序列模式时，应当充分考虑不确定性、依赖性和相关性 [48]。

大风

8.109. 一级概率安全评定模式应当包括所有由大风导致始发事件，并应当尽可能完整，以模拟所有与风相关的影响。

8.110. 对大风导致事故序列的考虑应当包括场址特定危害曲线和所有结构的脆弱性，这些结构的损坏可能导致一级概率安全评定中模拟的设备故障。要考虑的其他因素应当包括设备不可用或故障以及与大风无关的人为错误。应当调整人为错误的概率，以考虑风对表现形成因素的影响，如第 8.94 段所述。

其他自然灾害

8.111. 对于其他自然灾害，应当遵守地震、水文和气象灾害模式整合的概述和建议。

人类引发危害

8.112. 应当遵守自然外部危害模式整合的概述和建议。

成果的文件和表述

概述

8.113. 为了满足 GSR Part 4（Rev.1）[3]要求 20，应当以便于同行评审的方式记录针对外部危害的一级概率安全评定的筛选分析、边界分析和详细分析，以及一级概率安全评定的未来更新和应用，如下所示：

(a) 每种特定外部危害的筛选应当以描述所使用的过程和方法、所做的假设及其依据的方式记录在案。

[48] 例如，相关性与外部洪水假想方案有关，在外部洪水假想方案中，多列通道可能通过不同的洪水路径受到影响，这可能意味着水积聚和传播方面的不同动态。在这种情况下，对于不同通道的外部洪水导致故障，可能并不总是假设完全相关。

(b) 应当说明用于确定每种外部危害的危害曲线的方法，包括以下内容：

(i) 用于确定危害曲线的数据；

(ii) 作为输入和结果基础的技术解释；

(iii) 基本假设及相关不明朗因素。

(c) 应当提供接受脆弱性分析的结构、系统和部件的详细清单，以及以下内容：

(i) 每个结构、系统和部件的位置；

(ii) 用于脆弱性分析的关键假设和方法；

(iii) 每个结构、系统和部件的主要故障模式；

(iv) 分析的信息来源。

(d) 还应当讨论那些未进行脆弱性分析的结构、系统和部件，并提供从一级概率安全评定模式中筛选出它们的基础。

(e) 针对内部始发事件对一级概率安全评定模式所做的特定调整进行彻底记录，并注明每次调整的动机。

(f) 边界评定和详细分析的最终结果应当记录在与外部危害相关的每种情况下的堆芯和/或燃料损坏频率、显著最小割集和显著事故序列方面。还应当遵守第 3.17－3.25 段提出的关于文件的一般性建议。

8.114. 应当概述针对外部危害的一级概率安全评定的以下主要输出：

(a) 堆芯和/或燃料损坏频率及其不确定性分布。

(b) 敏感性研究的结果。

(c) 显著事故序列和显著最小割集清单。

(d) 讨论显著序列和显著极小割集的技术基础。

(e) 描述不确定性的主要因素。应当讨论认知不确定性和偶然不确定性的促成因素。

自然灾害

地震危害

8.115. 应当提供用于表征震源和所选参数的特定方法的描述。特别是作为建模输入和结果基础的特定解释应当彻底记录在案。

8.116. 地震危害的一级概率安全评定应当以便于其评审、应用和更新的方式记录。特别是以下信息应当列入文件：

(a) 一级概率安全评定中考虑的地震危害结构、系统和部件清单；
(b) 每种结构、系统和部件的脆弱性表征及其技术基础；
(c) 一级概率安全评定中模拟的地震危害范围的量化损坏概率；
(d) 结构、系统和部件的重要故障模式和每个结构、系统和部件的位置；
(e) 对内部始发事件的一级概率安全评定模式进行了特定调整，以考虑地震事件的影响；
(f) 关于地震危害一级概率安全评定中模拟的相关性（特别是空间相互作用）的全面信息，以及用于消除或减少相关性影响的任何假设。

8.117. 应当充分描述筛选任何结构、系统和部件的基础。

8.118. 应当记录用于量化地震脆弱性的方法和程序。这应当包括地震脆弱性分析的以下不同方面：

(a) 地震响应分析；
(b) 筛选涉及的步骤；
(c) 电厂巡视；
(d) 设计文件的评审；
(e) 识别每个结构、系统和部件的关键故障模式；
(f) 每个结构、系统和部件的脆弱性计算。

8.119. 电厂巡视的程序、巡视团队的组成以及从巡视中得出的观察和结论都应当完整记录。

外部洪水

8.120. 外部洪水的一级概率安全评定应当以便于其评审、应用和更新的方式进行记录。特别是，以下信息应当列入文件：

(a) 说明用于确定外部洪水危害曲线的特定方法和数据；
(b) 描述一级概率安全评定模式中为考虑外部洪水相关影响而进行的修改；

(c) 分析中考虑的所有结构、系统和部件的清单，以及从分析中筛选出的结构、系统和部件的正当性；

(d) 用于推导一级概率安全评定中模拟的所有结构、系统和部件洪水脆弱性的方法和数据；

(e) 一级概率安全评定在堆芯和/或燃料损坏方面的最终结果，以及选定的有用结果。

大风

8.121. 针对大风的一级概率安全评定应当以便于其评审、应用和更新的方式进行记录。特别是以下信息应当列入文件：

(a) 描述用于确定大风危害曲线的特定方法和数据；

(b) 描述一级概率安全评定模式的变化，以考虑与大风相关的影响；

(c) 分析中考虑的所有结构、系统和部件的清单，以及从分析中筛选出的结构、系统和部件的正当性；

(d) 用于推导一级概率安全评定中模拟的所有结构、系统和部件的风脆弱性的方法和数据；

(e) 一级概率安全评定在堆芯和/或燃料损坏方面的最终结果以及有用的中间结果。

其他自然灾害

8.122. 应当酌情遵守第 8.115－8.121 段提供的记录和呈现结果的建议。

人类引发危害

8.123. 应当酌情遵守第 8.115－8.121 段提供的记录和呈现结果的建议。

9. 关闭状态一级概率安全评定

关闭状态下一级概率安全评定的一般方面

9.1. 本部分提供了满足 GSR Part 4（Rev.1）[3]要求 6－13 的建议，该要求适用于反应堆堆芯和燃料装卸期间关闭状态 [49] 的一级概率安全评定。乏燃料水池中燃料的一级概率安全评定见第 10 部分。原则上，内部始发事件关闭状态一级概率安全评定基于与第 5 部分概述的功率运行状态的一级概率安全评定相同的方法。因此，因此，除非关闭状态的特定情况另有要求，否则本部分的结构在很大程度上与第 5 部分和图 1 所示的一般分析框架相对应，避免了内容的重复，而是参考了本“安全导则”的前面章节，除非关闭状态的方法和条件需要特定的描述。然而，应该指出的是，分析的目的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兴趣风险指标。

9.2. 内部和外部危害对于关闭状态和功率运行状态同样重要。本“安全导则”第 6－8 部分讨论的方法适用，但必须根据关闭状态的特定特点进行修改。原则上，始发事件的范围是相同的，但是事件的筛选可能导致不同的模式。这主要是在关闭状态的持续时间比功率运行的持续时间短得多的情况。显然，在关闭状态下，外部危害发生的概率要小得多。另一方面，对于关闭状态，后果可能非常不同。例如，在搬运重型设备时，可能需要仔细考虑地震事件，外部爆炸和外部洪水也可能导致电厂发生不同的事故。

9.3. 在关闭期间，轻水堆通常进行以下主要活动：

(a) 实现功率运行关闭；
(b) 余热排出系统的运行；
(c) 打开反应堆压力容器，水淹空腔；
(d) 换料；
(e) 维护和试验；
(f) 关闭余热排出系统并恢复功率运行。

[49] 对于低功率运行，第 2－8 部分提供的所有建议都是适用的，并适当考虑到潜在的降低功率水平以及与功率运行相比不同的联锁和系统配置。

对于其他类型的反应堆活动清单可以不同。例如，反应堆压力容器的打开和空腔的水淹与通道型反应堆无关。附件 III 提供了压水堆和沸水堆大修情况的示例以及核电厂运行状态的示例。CANDU 型反应堆典型运行状态的示例见参考文献[38]。

大修类型和电厂运行状态规范

9.4. 与功率运行相反，在关闭状态下，电厂的运行配置和电厂工况会发生显著变化。一般而言（对于离线进行换料的电厂），有三种不同类型的大修，如下所示：

(a) 定期大修换料，部分或全部从反应堆重新放置燃料 [50]，在此期间还进行重大维护活动；

(b) 计划大修，在此期间只进行特定维护活动；[51]

(c) 在有或没有反应堆容器排水和装料的情况下，功率运行期间发生干扰后的计划外大修。

这些都反映在电厂的技术规范中，这些技术规范通常根据电厂的各种运行状态进行划分，每个状态对电厂设备都有自己的可运行性要求。

9.5. 分析第 9.4 段提到的所有类型的大修被认为是良好的实践。应当全面评定与换料大修相关的风险。必须继续分析扰动后的序列，直到达到安全稳定状态。在预定义的序列任务时间终止分析可能会阻止获得有意义的结果。在许多情况下，作为第一步，对典型的大修进行分析。对于运行反应堆，这种大修应当从最近的大修开始，并添加从最近额外大修的记录以及与负责计划大修的人员讨论中获得的因素。如有必要，应当单独评定预计会增加风险的某些大修因素。例如，在专门为维护活动计划大修的情况下，与计划大修相关的风险与与持续运行相关的风险的比较可以是决策的重要输入。

[50] 对于燃料完全重新放置到乏燃料水池中的换料大修的电厂运行状态，第 10 部分的建议适用。

[51] 所有标准的计划关闭和启动条件通常在不同的电厂配置中考虑。

9.6. 如果概率安全评定的目标之一是评定与未来运行相关的风险，则应当将大修程序的可预见变化纳入分析。

9.7. 在关闭期间，存在大量和各种各样的电厂配置，如果分开处理，将导致需要分析的假想方案过多。为了处理关闭期间的各种设备配置，应当指定有限数量的电厂运行状态，对于这些状态和配置，设备状态和配置足够稳定和具有代表性。

9.8. 为了将电厂运行状态的组合数量限制在一个可管理的规模，一些相似状态的分组将是必要的。分组应当考虑到电厂的下列实物和技术方面：

(a) 反应堆临界程度（和/或关闭裕度）；
(b) 衰变热水平；
(c) 反应堆冷却剂系统中的温度和压力；
(d) 其他相关的功率相关参数（如稳压器水位、一回路系统水位、蒸汽发生器水位）；
(e) 开放式或封闭式反应堆冷却剂系统；
(f) 反应堆冷却剂系统回路的可运行性状态；
(g) 燃料的位置；
(h) 信用系统的可用性，包括支持系统，并考虑它们是自动控制还是人工控制；
(i) 系统校准；
(j) 安全壳完整性的状态。

9.9. 对于关闭状态一级概率安全评定，应当根据实际运行经验并根据当前实践和程序规定电厂运行状态。根据上一步中选择的大修类型（见第 9.5 段），应当详细分析适当的大修次数，以确定大修期间所有相关参数的实际状态。为此目的使用的信息来源一般包括：

(a) 关闭和启动程序；
(b) 特定大修或大修的大修计划；
(c) 大修的一般电厂实践；
(d) 大修的技术规范；
(e) 配置控制导则；

(f) 提供大修信息的其他文件（如详细说明硼浓度的日志）；

(g) 维护记录（例如，指定特定部件的维护持续时间）；

(h) 与运行人员和值长面谈；

(i) 大修计划人员面谈。

所有与描述电厂运行状态相关的信息都应当从这些来源中提取并记录在案，尤其是关于安全功能和其他相关功能可用性的信息。附件 III 有一个示例，显示了电厂运行状态的选择，其中区分了 11 种电厂运行状态。然而，对于关闭状态一级概率安全评定，分析应当基于大量的电厂运行状态，这取决于概率安全评定的特定应用（例如，风险监控应用）。

9.10. 对于处于设计阶段的核电厂，应当尽可能使用类似或参考电厂的信息。对于全新的设计，应对不同类型大修的不同运行所需的时间进行全面评定。该信息应当在调试阶段和电厂运行的第一年进行核实和更新。

9.11. 为确保涵盖整个运行周期，并避免遗漏某些电厂运行状态的风险因素，或避免重复计算，应当根据每个电厂运行状态的持续时间、功率水平和系统配置、进入每个电厂运行状态的频率（每个日历年）和始发事件，明确规定电厂运行状态（包括功率运行）之间的接口点。运行历史数据应当用于此目的。

始发事件分析

9.12. 原则上，确定始发事件的方法与第 5.13－5.22 段所述的方法相同。因此，应当解决冷却剂丧失事故和瞬变，以及内部和外部危害分析中确定的始发事件。作为起点，可以从功率运行的分析中编写一个一般清单。需要按照第 9.13－9.24 段所述步骤对该清单进行修改和扩充。

9.13. 在第 5.11 段，始发事件是参照堆芯损坏来定义的。如第 9.4－9.8 段所述，在不同的关闭状态下，堆芯可能处于非常不同的配置。贮存在反应堆厂房内部或外部乏燃料水池中的燃料作为乏燃料水池概率安全评定的一部分在本“安全导则”单独说明（见第 10 部分）。因此，许多始发事件是关闭工况所特有的，这些事件将不同于功率运行的一级概率安全评定中确定的事件（示例见附录 III）。此外，许多与维护活动或运行程序相关的始发事件可能是人类引发。对于关闭状态一级概率安全评定而言，始发事件的主

要类别是威胁安全功能的事件，如散热、一回路库存或完整性和反应性控制。这意味着，除了堆芯损坏之外，反应堆压力容器外燃料的损坏可能是关闭状态下一级概率安全评定事故序列的最终状态，这种最终状态通常被称为燃料损坏状态或临界事件。参考文献[38]提供了 CANDU 型反应堆关闭状态下概率安全评定中始发事件的示例。应当决定这些最终状态中的哪一个需要包括在分析中。如果国家法规或导则中有规定，该决定应当与要核实的概率安全目标或标准有关联。这种最终状态的特征是高度特定于反应堆类型的，因此不能在这里深入讨论。在大多数情况下，关闭状态一级概率安全评定考虑了可能导致以下最终状态的事件：

(a) 由于燃料丧失冷却而造成的燃料损坏；
(b) 装卸过程中燃料损坏；
(c) 重物跌落造成的燃料损坏；
(d) 由于燃料配置的变化（部分燃料可能是乏燃料）而在临界事件中对燃料造成的损坏。

9.14. 应当注意清楚地识别兴趣始发事件，补充根据第 9.12 段获得的一般清单。应当使用系统的技术来识别始发事件。除第 5.13－5.22 段建议的方法外，还应对改变反应堆冷却剂系统配置的电厂程序以及设备试验和维护程序进行系统检验。关闭状态下始发事件的事故序列的最终状态可能不同于堆芯损坏状态。

9.15. 在针对不同类型的关闭状态执行电厂程序期间，识别潜在的人为错误是该过程的关键目标之一，该过程应当包含电厂的知识程序和电厂巡视，使得概率安全评定专家熟悉电厂的工作实践。

9.16. 为确保关闭状态下一级概率安全评定始发事件清单的充分完整性，除功率运行概率安全评定清单外，还应当评审以下信息来源：

(a) 其他类似电厂关闭状态的一级概率安全评定
(b) 电厂运行历史；
(c) 类似电厂的经验；
(d) 关闭状态下运行的一般数据。

该类信息的公开来源包括一般性研究（例如，关于意外中通过堆芯泵入未硼化水造成硼稀释事件的信息）、许可证持有人的事件报告以及国际组织和电厂业主团体的事件报告。

9.17. 始发事件应当以这样一种方式分组，即该组中的所有始发事件都可以使用相同的事件树和故障树模式进行分析（见第 5.32－5.40 段）。除第 5.32－5.40 段所列的标准外，以下标准构成了对关闭状态下的始发事件进行分组的基础：

(a) 一组中的所有始发事件对可信的结构、系统和部件的可用性和运行具有相似的影响。

(b) 一组中的所有始发事件对于信用系统都具有相似的成功标准。

(c) 一组中的所有始发事件都需要类似的运行人员操作。

类似的始发事件可能发生在不同的电厂运行状态（见附件 III），但由于这些不同状态的系统可用性和成功标准通常不同，因此在大多数情况下，对电厂运行状态进行分组是不可行的。

9.18. 该组的特征应当根据该组内最具限制性的事件来定义（见第 5.35 段）。

9.19. 与功率运行的概率安全评定情况一样，始发事件频率的量化应当遵守第 5.149－5.152 段所述的标准一级概率安全评定实践。然而，关闭状态下的始发事件频率的量化应当考虑到人因故障事件导致始发事件的可能性较高，因此人的可靠性分析方法应当考虑到人因故障事件导致始发事件的可能性较大也可在适用时使用。此外，还应当考虑到设备配置和可用性、技术规范和包括换料操作在内的大修管理等电厂特定物项。

9.20. 在关闭状态一级概率安全评定中，始发事件的频率可以首先根据特定电厂运行状态下的预期每小时发生率来定义，然后考虑实际状态持续时间来重新计算。然而，如果始发事件是由于与电厂运行状态的发生相关的事件而不是其持续时间导致，则应当不以这种方式定义频率。例如，一些始发事件可能与试验或过渡活动相关，该型事件的频率不会根据电厂运行状态的持续时间而变化。

9.21. 如果由于相关电厂运行状态持续时间较短，导致发生频率较低，一些始发事件被排除在进一步分析之外，那么第 9.20 段提到的假设。如果一级概率安全评定用于风险监控应用，则应当重新审视并证明其正当性。

9.22. 在给定的电厂运行状态下，基本上有三种方法可以量化始发事件的频率（见第 5.149－5.152 段），特定如下：

(a) 根据运行经验（即根据被分析的电厂、类似设计的其他电厂或一般类型的反应堆）进行的直接估算；
(b) 根据功率运行的一级概率安全评定中确定的频率进行估计，并进行补充分析（即再评定减压或开启反应堆的冷却剂丧失事故频率）；
(c) 逻辑模式的使用，包括导致始发事件的所有可预见的输入。

9.23. 为了正确解释导致始发事件的错误之间的依赖关系（例如，导致衰变热去除功能丧失的错误）以及在响应该事件时出现的错误（例如，未能恢复衰变热去除功能），应当明确地对导致始发事件的错误进行建模。

9.24. 将始发事件分配给电厂运行状态的总体结果应当以表格或其他类型概述的形式呈现。附件 III 提供了一个示例。

事故序列分析

安全功能和成功标准

9.25. 第 5.41－5.69 段提供了关于事故序列分析一般方法的建议。尽管关闭期间的衰变热水平通常比功率运行关闭后马上低很多，但可能的电厂配置的特征仍可能导致挑战安全功能实现的事件。分析应当考虑到以下方面：

(a) 由于在关闭时禁用信用系统的自动驱动，安全设备的可用性可能会降低，并且对运行人员操作的依赖性可能会增加。
(b) 一回路冷却系统的完整性可能会受到损坏，并且可能会额外旁路安全壳。
(c) 前线系统的性能通常取决于特定始发事件、电厂运行状态的特征和衰变热水平。
(d) 在确定某一安全功能的可用冗余通道或部件的数量时，应当考虑运行限值和条件的最低要求以及运行经验。

9.26. 应当使用功能性能标准来指定各种系统的成功标准，这些标准可能不同于为功率运行的一级概率安全评定指定的成功标准。

成功标准的支持规范分析

9.27. 为功率运行的一级概率安全评定构建的故障树模式应当进行适当的修改。即使系统的逻辑和响应与功率运行时基本相同，也应当考虑系统或部件的工况可用性的可能变化。

9.28. 为了确保分析人员做出的假设是正确的（例如，与堆芯冷却相关的假设），应当进行热工水力计算，以确定现实的成功标准。热工水力分析的详细程度应当符合系统分析和一回路系统配置的要求。对于过渡电厂运行状态（在关闭和启动期间）和热关闭工况下，一回路系统的配置和工况在某些情况下与瞬变系统的配置和工况相似。从功率运行开始，因此为功率运行的热工水力计算设计的模式将是适用的。在其他情况下，必须证明适用性。对于其他电厂运行状态，应当进行一回路系统特点和模式能力的比较，以评定特定规范的适用性。例如，对于轻水堆，支持成功标准规范的热工水力分析至少应当考虑到以下因素：

(a) 一回路压力边界的状态；
(b) 移除或解除容器上盖张力；
(c) 安全阀拆除或一回路系统排气口打开；
(d) 隔离回路或安装喷嘴坝；
(e) 蒸汽发生器中的水位；
(f) 一回路参数（如温度、压力、非凝气体的存在、关闭裕度）；
(g) 一回路系统中的水位；
(h) 余热水平；
(i) 安全壳的隔离状态；
(j) 安全功能驱动保护系统的可用性。

9.29. 在进行热工水力计算时，应当评定是否违反了特定燃料损坏状态的标准。这些标准和损坏时间可能会有很大的不同，取决于反应堆是关闭还是打开。

事故序列的建模

9.30. 应当使用事件树（见第 5.59－5.63 段）或等效演示来模拟电厂和运行人员对始发事件的响应。在对事故序列建模之前，绘制详细的事件序列图，包括人与人之间的相互作用，被认为是一种良好的实践。

9.31. 在事故序列分析中，运行人员旨在恢复冷却功能以及从替代来源向反应堆供水行动的可能性至少应当被视为缓解行动。

9.32. 事故序列建模应当由一个多学科团队完成，该团队应当包括人的可靠性分析专家，从分析过程开始。

事故序列最终状态与设备损坏状态

9.33. 对于关闭状态以及功率运行，事故序列应当分为电厂损坏状态，以便将一级概率安全评定的可能不同结果的数量减少到可管理的数量，以便进一步分析（二级概率安全评定或三级概率安全评定）和简明概述研究结果。对于归入特定电厂损坏状态的所有事故序列，预期的事故进展，包括对安全壳完整性和放射性核素运输的挑战，应当定性相似。另一方面，现代分析工具提供了模拟事故序列和相应排放类别的可能性。这种方法不涉及上述一级概率安全评定的电厂损坏状态分组。应当指定适当的序列任务时间（见第 5.53 段），同时考虑到所发生过程的特定特点和时间安排。

9.34. 为关闭状态一级概率安全评定选择电厂损坏状态的过程应当考虑为功率运行的一级概率安全评定规定的电厂损坏状态（见第 5.66 段），然而，对于关闭状态一级概率安全评定，应当确定不同于功率运行的一级概率安全评定的额外电厂损坏状态。例如，对于某些关闭状态所特有的条件，例如反应堆容器上盖被移开或安全壳设备舱口打开的情况，额外的电厂损坏状态可能是必要的。

在指定设备损坏状态时，应当考虑以下额外事故序列特征：

(a) 衰变热水平（基于从功率运行关闭以来的时间）；
(b) 安全壳状态，尤其是当安全壳打开时；
(c) 确定恢复安全壳隔离所需时间以及在此期间安全壳有效性（即渗漏性）可能降低的条件；

(d) 拆除容器上盖、安装喷嘴坝、拆除安全阀和打开一回路系统排气口时，一回路系统压力边界的完整性；

(e) 一回路中的水库存。

9.35. 电厂损坏状态的适当说明将对结果及其解释具有决定性作用。

系统分析

9.36. 对于功率运行的一级概率安全评定，关闭状态一级概率安全评定系统分析的目标是对量化事故序列所需的系统故障进行详细建模。故障树分析是最广泛使用的系统建模方法。可以尽可能利用和调整为功率运行构建的故障树模式（见第 5.72－5.83 段）。然而，如有必要，应对现有模式进行修订，或可能需要制定新的模式，特别是在下列情况下：

(a) 现有的系统模式不适合描述不同电厂运行状态下的特定系统行为。例如，系统可能被不同地配置以适应维护，或者系统的特定对准可能改变系统成功标准（例如，当一列安全通道处于计划维护中时）。

(b) 在功率运行期间处于待机状态的特定系统在关闭期间运行。

(c) 在关闭期间，系统驱动是手动执行的，而在功率运行中，驱动是自动的。

(d) 不同系统所需的任务时间明显不同。

(e) 不同电厂运行状态的成功标准会有所不同。

(f) 对于每个电厂运行状态，初始可用的通道数量是不同的。

(g) 时间窗口和电厂工况存在显著差异，这可能会影响恢复行动的成功概率，并允许将维修活动记入。

(h) 没有对特定系统进行建模，因为它不是功率运行所必需的。

(i) 特定系统的互连对于建立仅在关闭状态下使用的安全功能配置是必要的（例如，使用乏燃料冷却系统进行堆芯冷却）。应当考虑这种互连应当遵守的程序。

(j) 没有对特定系统进行建模，因为这仅适用于功率运行的二级概率安全评定。

附件 III 给出了特定系统建模要求的示例。

相关故障的分析

9.37. 如第 5.87－5.92 段关于功率运行的描述，本分析的目的是确定可能影响事故序列和系统模式的逻辑和量化的相关性。这方面的主要依赖类型是对供应和支助系统的功能依赖；系统间硬件共享或进程耦合；实物依赖性，包括由始发事件直接或间接导致依赖性；对人类互动的依赖；和共因故障。这些依赖关系都应当包含在分析中。

9.38. 作为功率运行期间条件的出发点，应当评审和检查不同的支持和前线系统及其相互依赖性，以确定其对特定电厂运行状态的适用性。试验和维护活动可能会产生新的依赖源，例如应当考虑的冗余部件的同时维修或维护。示例见附件 III。

9.39. 应当根据需要对功率运行的依赖性模式进行修订，特别是如果关闭状态的成功标准不同，或者支持系统（如通风系统、供电系统）的条件不同。

9.40. 还应当评审系统和部件大修的一致性。

9.41. 应当确定各种共因故障机制以及维护和其他特定于关闭状态的活动对这些故障机制发生的潜在影响。

人的可靠性分析

9.42. 在第 5.97－5.122 段解释了人的可靠性分析的关键方面，这些方面也适用于关闭。关闭期间人因故障事件的分析是复杂的。因此，人的可靠性分析应当以结构化和逻辑化的方式进行。与其他分析任务一样，人的可靠性分析的过程应当以一种可追溯的方式被彻底地记录下来。人的可靠性分析应当旨在产生彼此一致的故障概率，以及与一级概率安全评定其他部分进行的分析一致的故障概率。

9.43. 在分析中应当充分考虑关闭期间的典型方面，如大量使用外部组织的维护人员、频繁加班和控制室工作增加。还应当考虑到工作监督方面的困难和紧张的时间表带来的压力。

9.44. 对于人的可靠性分析，人的可靠性分析人员与电厂运行人员和维护人员之间应当进行密切互动，以确保关闭期间的电厂设计和运行特点在分析中得到适当反映。如果这是不可能的（例如，对于处于设计阶段或建造阶段的电厂），分析人员应当尝试在类似电厂运行的实际经验的基础上获得知识。

A 型人因故障事件－前起始因子人因故障事件

9.45. A 型人因故障事件（见第 5.103 段）包括与试验、维护、维修和校准相关的行动，如果执行不当，可能导致设备不可用。A 型人因故障事件的识别和量化过程与功率运行的一级概率安全评定相似，但应当考虑特别关闭特点，尤其是以下特点：

(a) 在接近大修结束时执行的功能试验可能会受到时间限制，导致人为错误的可能性很高。

(b) 自动调整功能的可用性可能会降低（例如，试验后保持开启的阀门没有自动关闭信号）。

B 型人因故障事件－可能导致始发事件的人因故障事件

9.46. 由于各种不同的维护措施、试验和配置变化，不能期望观察到所有可能的人为错误，这些错误与特定于关闭的始发事件的频率相关（例如，由于不利的阀门对准而导致排放）。因此，应当明确评定人为未能始发事件的可能性。这对于解决响应动作（C 型人因故障事件）的依赖性也很重要。此评定可能识别导致部件不可用的人因故障，或者在起始因子的故障树中建模需求的情况下，立即或作为潜在故障。为了进行分析，可以使用以下信息来源：

(a) 启动和关闭运行的书面程序；

(b) 运行经验；

(c) 关于大修计划的文件，包括技术规范、试验和维护程序。

对于 B 型人因故障事件的分析，筛选可能是必要的，以决定哪些故障可以在定性评定的基础上筛选出来，哪些故障需要定量估计甚至详细分析。附件 III 概述了一种可能的实践。人为错误概率的推导可按照第 5.115－5.119 段所述进行。

C 型人因故障事件－后起始因子人因故障事件

9.47. C 型人因故障事件（见第 5.106 段）在关闭期间特别重要，因为电厂自动化水平降低。在关闭状态的许多一级概率安全评定研究中，它们往往是重要的风险贡献者。因此，应当彻底考虑对该型事件的失败概率进行现实评定。

9.48. 所选择的方法应当考虑到在关闭状态一级概率安全评定框架内以系统的方式对 C 型人因故障事件进行建模和量化的相关特定方面。以下方面可能与功率运行的一级概率安全评定不同：

(a) 警报和持续警报的驱动频率；
(b) 程序指导的质量；
(c) 运行人员的培训状况；
(d) 响应时间窗口的持续时间；
(e) 在关闭状态下促进人工操作的界面质量。

9.49. 应当谨慎使用特定于功率运行的时间可靠性相关产生的值，因为关闭状态下的时间窗口可能远远超出该类相关性的适用范围。

9.50. 应当解决始发事件的原因诊断中可能出现错误的问题，尤其是在使用基于事件的程序时。

9.51. 与功率运行的一级概率安全评定一样，应当考虑同一事故序列中人因故障事件之间的相关性（见第 5.120 段和第 5.121 段）。然而，在关闭状态的概率安全评定模式中，解决 B 型和 C 型人因故障事件之间的依赖性尤为重要。如果诸如衰变热去除丧失的始发事件是由人为错误导致，则导致个人犯错误的环境可能会使衰变热去除功能的恢复变得复杂。与机械故障导致功能丧失的情况相比，这可能导致故障概率增加。

数据评定

9.52. 对关闭状态一级概率安全评定进行量化所需的数据包括：

(a) 始发事件的频率；
(b) 与人为错误概率相关的数据；

(c) 电厂运行状态的持续时间；

(d) 允许的大修时间；

(e) 部件可靠性数据；

(f) 因维护而无法使用，包括根据运行历史进行的重叠维护；

(g) 共因故障的评定。

第 5 部分（见第 5.143－5.159 段）描述的数据采集的基本需求和方法也适用于关闭状态。由于用于量化特定于关闭的部件可靠性参数的数据不如功率运行的数据广泛可用，因此广泛使用的方法是调整来自功率运行的数据。如果不明确说明这些数据的正当性，就应当不这样做。

9.53. 对于不同的配置，应当评审与维护和试验活动相关的数据评定，虽然某些活动可能在整个大修期间进行，但其他活动可能仅在某些配置中进行。此外，维护和试验频率可能会因配置而异。

9.54. 计划大修期间试验的一个主要目的是在设备重新输入运行之前，核实经过维护设备的正确运行。该设备的不可用性应当根据平均试验持续时间和部件试验期间电厂运行状态持续时间的基础。

9.55. 应当评定维护和试验活动导致覆盖比对中可能的人为交互和人为错误的概率。

9.56. 应当考虑维修的可能性，因为它可以显著增加电厂运行状态下的信用系统在关闭工况下的可用性。在许多情况下，忽视维修可能会导致高估风险，尤其是在后起始因子的假想方案下。在分析中计入维修动作将增强概率安全评定模式的真实性。这里的“维修”包括足以满足所考虑的事故序列要求的短期恢复情况。然而，维修应当限于电厂经验显示良好的恢复可能性或成功概率可由工程判断和/或在事故序列条件下有效的既定维修程序支持的情况。

9.57. 应当考虑维修时间对电厂运行状态的依赖性。这种依赖性可能与系统和设备的可达性、进行维修人员的可获得性、备件的可获得性相关，对于某些事故序列，还可能与待维修部件周围的辐射水平相关。

9.58. 在关闭状态下，应当选择合适的可靠性模式，以考虑功率运行期间待机的部件可能在大修期间仍运行。

9.59. 在模式中使用部件任务时间来计算用于确保某些安全功能以在始发事件后达到和/或保持稳定关闭状态的运行设备无法继续运行的概率。部件任务时间会对计算出的系统故障概率产生显著影响。关于部件任务时间的假设应当与事故序列建模（即序列任务时间和系统任务时间）以及可靠性数据相一致，因为这些数据可能显示出对运行时间的敏感性。

9.60. 如果要在分析中纳入大修程序的可预见变化，这可能会对数据采集产生影响。这些变化可能是这样的，即关于运行经验的现有信息要么不能提供必要的数据，要么只能在通过分析或工程判断进行调整后提供必要的数据。

事故序列的量化

9.61. 对于关闭状态一级概率安全评定，事故序列的量化应当使用与功率运行的一级概率安全评定相同的技术。使用其他技术，如马尔可夫技术，而不是标准的故障树和事件树评定方法，对于长序列任务时间使恢复行动成为可能的关闭状态，可能会产生更现实的结果。

9.62. 当评审量化结果时，如在功率运行的一级概率安全评定的情况下，应当仔细评审获得的最小割集。在关闭状态一级概率安全评定中，可能必须修改系统模式以反映不同电厂运行状态的条件。如果修改系统模式，应当交叉检查在不同电厂运行状态下为类似事故序列或系统获得的最小割集，以确保它们中的任何差异确实反映了不同的电厂运行状态或序列特征，并且不是由建模错误导致。

不确定性分析、重要性分析和敏感性研究

9.63. 对于关闭状态的不确定性分析，应当使用与功率运行的一级概率安全评定相同的技术（见第 5.179－5.181 段）。

9.64. 重要性分析和敏感性研究也应当使用与功率运行一级概率安全评定相同的技术进行（见第 5.171 段和第 5.174－5.178 段）。

9.65. 敏感性研究是关闭状态一级概率安全评定分析的重要组成部分，它们旨在分析许多特定于概率安全评定的因素对关闭状态的潜在影响。例如，

被选择来表征电厂运行状态的特定条件可能代表在电厂运行状态期间实际可能发生的更广泛的条件。与用于功率运行的概率安全评定相比，可能存在不可用的不同系统组合，一些组合可能来自更保守的分析，而一些来自不太保守的分析。电厂运行状态可能有更长或更短的持续时间。根据电厂运行状态相对于电厂关闭的时间，可用于人的行动时间可以变化很大。成功标准也可能因衰变热水平而异。应对这些变化进行调查，特别是对于用于模拟电厂运行状态的假设导致风险占主导地位的情况。

成果的文件和表述

9.66. 为了满足 GSR Part 4（Rev.1）[3]要求 20，一级概率安全评定文件应当包括执行功率运行一级概率安全评定的程序，以及关闭状态一级概率安全评定特有方面的章节，例如详细描述用于识别大修类型、电厂运行状态和始发事件过程的章节。

9.67. 如前几部分所述，在研究的每个主要步骤中获得的结果应当与从分析中获得的重要工程洞察一起整合和展示。文件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。

9.68. 通常，书面维护或运行程序会响应初步分析结果进行改进或引入。任何该类变更也应当在文件中概述。

9.69. 最后，应当提出并讨论更一般性的结论和建议。在决策所必需的范围内，文件中应当包括下列专题：

(a) 代表堆芯和/或燃料损坏的最终状态的频率－综合所有电厂运行状态的重要贡献：
    (i) 显性序列的贡献；
    (ii) 电厂运行状态的贡献；
    (iii) 始发事件组的贡献；
    (iv) 堆芯和/或燃料损坏频率的不确定性分析结果；
    (v) 堆芯和/或燃料损坏频率的重要性分析和敏感性研究结果。
(b) 每个电厂运行状态的结果呈现：
    (i) 显性序列的贡献；

(ii) 始发事件组的贡献。

(c) 概述二级概率安全评定的界面（如有必要），包括电厂损坏状态的特征和频率。

(d) 定性洞察和结论：

(i) 结果和工程洞察的解释；

(ii) 结论和建议。

9.70. 工程洞察和建议的展示应当为决策过程提供清晰的输入。

9.71. 为典型的大修计划，尤其是换料大修，构建一个风险概况可能会有所帮助。这种曲线可以例如显示不同电厂运行状态的堆芯和/或燃料损坏频率，作为大修时间或功率降低开始后时间的函数。附件 III 提供了一个风险简介的示例。

9.72. 以下来自关闭状态一级概率安全评定的详细信息应当包括在报告中：

(a) 对总堆芯和/或燃料损坏频率有贡献的显著最小割集；

(b) 每个电厂运行状态下导致堆芯和/或燃料损坏频率的显著最小割集。

最小割集的显著水平应当根据概率安全评定的目标来确定。

9.73. 文件中应当包括以下内容：

(a) 人为错误和相关故障对堆芯和/或燃料损坏的影响；

(b) 独立故障对堆芯和/或燃料损坏频率的影响；

(c) 事件树中模拟的各种安全功能对堆芯和/或燃料损坏频率的影响。

9.74. 除堆芯和/或燃料损坏频率外，还应当评定其他非期望最终状态（例如，涉及燃料水池的临界状态或损坏）及其频率，并记录结果。

9.75. 电厂模式和数据应当在数据库和计算机文件中充分记录和配置，以便能够复制结果，并使模式易于应用。

9.76. 应当根据监管评审要求起草文件。

10. 乏燃料水池一级概率安全评定的特定方面

10.1. 原则上，乏燃料水池的一级概率安全评定基于与第 5－9 部分概述的反应堆堆芯的一级概率安全评定相同的方法。因此，考虑到本部分所述的一般方面，对反应堆堆芯进行一级概率安全评定的一般过程应当适用于乏燃料水池。本部分讨论的一些专题与反应堆堆芯的概率安全评定和乏燃料水池的概率安全评定都相关。

非期望最终状态

10.2. 应当明确界定乏燃料水池一级概率安全评定的不良最终状态。如果在国家法规或导则中规定了这些目标或标准，则适用于乏燃料水池的国家概率安全目标或标准应当作为指定非期望最终状态的基础。

10.3. 应当制定一个标准（或多个标准，如果合适）来表征指定的非期望最终状态。关于堆芯（见第 5.43 段和第 5.44 段），通常认为，如果超过燃料的设计基准限值就会发生燃料损坏。在没有详细的热力学分析的情况下，燃料发现（即当乏燃料水池中的水位由于沸腾或排空而下降到乏燃料水池中贮存或装卸的燃料组件的活性部分的顶部以下时）也可用作假设燃料损坏的标准。

10.4. 除了燃料损坏之外，燃料暴露和池水沸腾（例如，对于位于安全壳之外的乏燃料水池）也应当在识别过程中被视为潜在的非期望最终状态。

10.5. 如有必要进行风险评定，应当考虑燃料组件达到预定程度的损坏情况，以确定主要的关注终点。有限数量的燃料棒或单一燃料组件的机械损坏，如果能够判断这些事件不会导致大量放射性物质排放，则可以从进一步评定中筛选出来。

10.6. 由于重物跌落或物体坠落（包括危害导致结构故障的结果）或危害组合等内部危害造成的总机械性燃料损坏也应当被视为非期望最终状态，因为该型事件可能会挑战燃料的设计基准限值。

电厂运行状态

10.7. 所有与风险相关的电厂运行状态的建模可能需要涵盖各种各样的乏燃料水池配置，以及相关的定期维护活动和余热水平的变化。相似的电厂运行状态应当组合在一起，以将状态的数量限制在可管理的大小。

10.8. 这种分组应当考虑到以下物理和技术方面以及电厂运行状态下燃料装载模式的差异：

(a) 乏燃料水池的水库存；
(b) 贮存在乏燃料水池中的燃料组件的余热；
(c) 乏燃料水池系统配置（即乏燃料水池是否与反应堆隔离或连接）；
(d) 燃料组件在乏燃料水池中的贮存位置（例如，根据设计，在下架或上架）；
(e) 执行装卸活动；
(f) 信用系统的可用性和定期维护；
(g) 潜在的恢复措施和维修；
(h) 必要时，不同燃料贮存配置和相关燃料操作中潜在始发事件的差异。

始发事件

10.9. 乏燃料水池一级概率安全评定应当考虑的始发事件类型示例如下：

(a) 冷却丧失（即乏燃料水池散热系统故障、场外电源丧失）；
(b) 冷却剂库存丧失（例如乏燃料水池排热回路中的管道破裂，由于错误的人为干预而导致意外排放）；
(c) 反应性事故（如硼稀释、燃料装载错误）；
(d) 由内部危害导致始发事件，可能导致乏燃料水池的排热系统故障（包括管道破裂，作为除排热回路以外系统内部水淹的来源）、乏燃料水池库存损失或物体因提升活动而跌落到乏燃料水池中的燃料组件上；
(e) 由外部危害导致始发事件，可能导致乏燃料水池排热系统故障、乏燃料水池库存损失或物体因危害导致结构故障而落到乏燃料水池中的燃料组件上；
(f) 可能导致上文 (d) 和 (e) 所述后果的危害组合导致事件。

事故序列分析

10.10. 在事故序列分析中，运行人员旨在回收乏燃料水池排热系统以及从替代来源向乏燃料水池供水行动的可能性至少应当被视为缓解行动。如果适用，还应当考虑自动驱动。

10.11. 事故序列分析应当考虑到乏燃料水池冷却系统恢复、管道破裂恢复和场外电源丧失恢复（例如维修故障部件）所涉及的特定活动。在估算恢复时间时，应当考虑乏燃料水池中的初始水库存、乏燃料水池中贮存的燃料组件的余热以及可用于缓解系统的能力。

10.12. 应当考虑反应堆堆芯和乏燃料水池之间的潜在依赖关系，涉及信用系统的共享部件或资源（包括水库存），以及在共同始发事件的情况下共享人力资源。还应当考虑乏燃料水池和反应堆堆芯之间的相互作用（例如，水淹效应、外部危害或其他现象造成的结构负载、乏燃料水池和反应堆连接时的排空事件）。

10.13. 在模拟乏燃料水池中冷却剂丧失事故时，应当将水淹视为一种间接危害。可隔离管道的及时隔离可被认为避免了水淹影响（例如乏燃料水池排热系统的长期故障）。在冷却剂丧失始发事件的事故序列分析中，也应当考虑虹吸管的故障（包括破裂）。

10.14. 事故序列分析应当考虑到沸腾会导致泵气蚀，这可能会妨碍冷却系统的成功重启和/或由于乏燃料水池附近的环境条件（包括气温和辐射水平）恶化而使局部行动无法进行。

10.15. 对于涉及大量水库存和低功率水平的乏燃料水池事故序列，在确定序列任务时间时应当考虑缓慢的事故进展，该序列任务时间可能相对较长，以便进行可靠的恢复行动和维护。在预定的序列任务时间终止分析可能会阻止获得有意义的结果。

人的可靠性分析

10.16. 在乏燃料水池冷却丧失事件的情况下，事故进展缓慢，这使得多方参与者能够参与诊断和决策过程以及恢复行动和维护的执行。在这些情况

下，当定义主要影响恢复运行故障概率的表现形成因素[52]时，应当考虑到这一点。

10.17. 对于乏燃料水池事故，应急运行程序的详细程度可能与反应堆堆芯事故不同。这种差异可能会影响应对事故时的人的可靠性，在对乏燃料水池的一级概率安全评定进行人的可靠性分析时应当予以考虑。

10.18. 应当考虑到与乏燃料水池的本地人员行动可及性相关的问题。特别是这些问题对于沸腾的情况来说是很重要的。

10.19. 应当考虑防止乏燃料水池和反应堆堆芯出现不良最终状态的人员行动之间的潜在依赖性。此外，在评定相关人为错误概率时，应考虑工作量增加对运行人员同时缓解并发事故的加重影响。

分析的量化

10.20. 第 5.160－5.170 段提出的所有建议均适用于乏燃料水池的一级概率安全评定。此外，应当整合反应堆堆芯和乏燃料水池中燃料的概率安全评定模式，以便正确模拟任何共享系统的依赖性。这对于导致同时影响反应堆堆芯和乏燃料水池的事件以及随后的二级概率安全评定（特别是对于安全壳内有乏燃料水池的电厂）尤为重要。

结果的解读

10.21. 对乏燃料水池和反应堆堆芯事故风险的组合或单独解释应当符合国家法规或规则中规定的概率安全目标或标准。

10.22. 对于是否将乏燃料水池的一级概率安全评定结果与反应堆的结果合并，国际上没有达成共识（见参考文献[15]）。[53]

---

[52] 只有在事故进展缓慢的情况下，才能记入恢复行动，并为运行人员提供足够的时间窗口和信息来实施这些行动。

[53] 反应堆和乏燃料水池的风险结果可在二级和三级概率安全评定中适当汇总。

10.23. 如果将两个风险测量估计值进行汇总，以生成一个总体风险测量估计值，定量描述核电厂对严重事故的脆弱性，则应当考虑乏燃料水池事故序列和反应堆事故序列之间的相关性，而不是简单地将这些估计值相加（即类似于用于汇总多机组或现场堆芯损坏频率的方法，见第 11 部分）（见参考文献[15、16]）。

11. 多机组一级概率安全评定

11.1. 第 5－10 部分从单机组一级概率安全评定的角度考虑了多机组相互作用（例如，见第 5.7 段、第 5.20 段、第 7.40 段和第 7.76 段）。本部分提供的建议与多机组一级概率安全评定的制定相关，旨在量化多机组风险指标。关于成员国经验、实际案例研究和多机组概率安全评定导则的更多信息见参考文献[16]。

11.2. 多机组概率安全评定模式通常是在单机组概率安全评定模式的基础上制定的，并考虑了所考虑的每个机组的特定方面。

多机组概率安全评定的范围

11.3. 如第 2.2 段所述，对于一般的概率安全评定，多机组概率安全评定的范围和需要也应当与概率安全目标或标准有关联，如果这些目标或标准已在国家法规或导则中规定的话。

11.4. 多机组概率安全评定的范围应当包括所有风险显著的多机组始发事件[54]和危害，以及所有电厂运行状态，这些都可以通过对单机组概率安全评定结果的评审来确定。为了确定多机组概率安全评定的范围，必要时可根据对单机组概率安全评定结果的评审进行筛选。[55]

[54] 多机组始发事件是指挑战两个或更多机组正常运行（或最终导致跳堆或挑战正常运行的退化状态）的始发事件，需要成功缓解以防止受影响机组的堆芯损坏，或可能直接导致堆芯和/或燃料损坏。

[55] 视概率安全评定的范围而定，就风险汇总而言，概率安全评定还可能考虑多机组方面以及场址上并置的其他辐射源（如临时燃料贮存设施、核废料处理设施）的潜在影响。

多机组概率安全评定的风险测量

11.5. 除了单机组概率安全评定中额外使用的风险指标（如堆芯损坏频率）之外，还应当制定其他风险指标，以表达多机组核电厂的风险状况用于相关决策目的。为例如，以下风险测量可用于多机组一级概率安全评定（见参考文献[15、16]）：

(a) 单机组堆芯损坏频率：多机组场址仅涉及一个反应堆堆芯损坏的事故频率；

(b) 多机组堆芯损坏频率：涉及多机组场址两个或多个反应堆堆芯损坏的事故频率；

(c) 场址堆芯损坏频率：涉及多机组场址一个或多个反应堆堆芯损坏的事故频率；

(d) 多源燃料损坏频率：多机组场址上涉及两个或更多源（如反应堆堆芯、乏燃料水池）燃料损坏事故的频率。

应当定义多机组概率安全评定的风险指标，以捕捉场址反应堆堆芯和乏燃料水池之间的不同组合，并便于将多机组概率安全评定的结果用于决策。

电厂运行状态

11.6. 对于多机组概率安全评定，应当为每个机组选择一组具有代表性的电厂运行状态组合，以便考虑风险显著的组合。

11.7. 所选择的组合应当考虑到处于功率运行和关闭状态的所有反应堆的不同配置，以及处于不同电厂运行状态的乏燃料水池。根据电厂运行实践，一些组合可能会被取消（例如，不同时给两个装置换料）。电厂运行状态组合的简化应当根据风险重要性进行论证。

11.8. 如第 9.8 段和第 10.7 段所建议的，应对各种电厂运行状态进行分组。从多机组风险的角度来看，这种分组的方式应当不掩盖潜在的显著风险始发事件。

11.9. 对于多机组概率安全评定，应当估计每个反应堆机组在每个模拟的电厂运行状态组合中花费的概率或时间分数。

始发事件分析

11.10. 在多机组概率安全评定中，应当筛选多机组始发事件，考虑其风险重要性。如果详细的现实分析不会对选定的多机组概率安全评定风险指标做出显著贡献，则可以筛选出事件。

11.11. 考虑到分组始发事件可能对多机组电厂产生不同的影响，如有必要，应当检查和修改单机组始发事件的分组。

11.12. 对于多机组概率安全评定，应当计算取决于电厂运行状态组合的事件频率，同时考虑组合的概率（另见第 11.9 段）。

系统分析

11.13. 机组间共享的结构、系统和部件和资源应当在多机组概率安全评定中明确建模。

11.14. 在涉及多机组的事故中，应当考虑每个机组共享结构、系统和部件或资源的可用性。

11.15. 应当尽可能现实地考虑和模拟共享结构、系统和部件和资源的不同机组的使用优先级。

11.16. 在多机组概率安全评定系统分析中，应当考虑场址不同机组的结构、系统和部件之间的功能和空间依赖性。

人的可靠性分析

11.17. 对于多机组始发事件和/或事故序列，应当考虑与管理多个反应堆机组的需要相关的人类活动。

11.18. 多机组概率安全评定中使用人的可靠性分析方法应当考虑多机组的环境特征，例如由于现场事故工况、共享人力资源、在共享控制室工作（如适用）以及机组与公共技术支持中心的相互作用而增加的压力。

11.19. 应当考虑不同机组运行人员行动之间的潜在依赖性。应当评定依赖程度，考虑影响因素，如共享资源、与共同技术支持中心或协调现场活动的另一组织的互动，以及内部和外部危害的影响。

11.20. 在单个或多机组同时发生事故的情况下，应当考虑对其他机组的控制和事故管理的不利影响，同时考虑与现场其他机组的严重事故相关的因素（如放射性排放、氢气爆炸）。

共因故障与危害脆弱性相关性

11.21. 应当确定相关结构、系统和部件的机组间共因故障并对其进行建模。

11.22. 应当确定机组间危害脆弱性相关性并对其进行建模。

多机组概率安全评定风险概况量化

11.23. 多机组概率安全评定风险概况量化应当考虑场址机组的所有非期望最终状态组合。为洞察决多个并置装置和/或乏燃料水池的所有影响和相互依赖性，对场址使用整体概率安全评定模式是可行的，该模式包括所有考虑的始发事件、事故序列和信用系统功能。

11.24. 多机组概率安全评定风险概况应当作为与场址相关的各种风险因素（如内部和外部危害、来自场址反应堆堆芯和乏燃料水池的风险）汇总的结果得出。当汇总这些要素时，重要的是要考虑它们之间的潜在异质性，并在利用多机组概率安全评定风险概况进行风险知情决策时使用这些信息（见第 12.7 段）和参考文献[15、16]）。

11.25. 应当评审最小割集，以确保模式正确考虑了多机组电厂的各个方面，如共享结构、系统和部件、同时发生的事故工况和对多个机组的损坏。

11.26. 从多机组概率安全评定获得的结果应用作风险知情决策的输入。

12. 一级概率安全评定的使用和应用

概率安全评定应用的一般方面

12.1. 本部分讨论了各国根据其国家安全政策和法规实施的一些概率安全评定应用，并就满足以下要求提出了建议：

— GSR Part 4（Rev.1）[3]关于概率安全评定一般用途的要求 23；
— SSR-2/1（Rev.1）[2]关于在核电厂设计中使用概率安全评定的要求 6、10、16 和 42；
— SSR-2/1（Rev.1）[2]关于使用概率安全评定进行安全分级的要求 22；
— 原子能机构《安全标准丛书》第 SSR-2/2（Rev.1）号《核电厂安全：调试和运行》[39]要求 31，与使用概率安全评定进行试验和维护优化相关；
— SSR-2/2（Rev.1）[39]关于使用一级概率安全评定进行定期安全评审的要求 12；
— SSR-2/2（Rev.1）[39]关于使用一级概率安全评定支持安全相关活动的要求 8。

12.2. 概率安全评定应当在电厂的整个设计和运行过程中使用，以协助与电厂安全相关的决策过程，从而优先考虑和优化设计和安全相关活动，使其专注于风险重要性最高的区域。

12.3. 概率安全评定的结果应当用于深入了解结构、系统和部件的设计和运行，这对防止反应堆堆芯或乏燃料水池中的燃料损坏非常重要。概率安全评定结果的这种使用应当包括与总体概率安全目标或标准的比较。

12.4. 用于任何应用的概率安全评定应当保持为“活的概率安全评定”，定期更新以反映当前的设计和运行电厂及其瞬变电流分析。应当将其完全记录在案，以便整个概率安全评定分析可以追溯到设计和辅助分析的细节。[56]

[56] 对于特定概率安全评定应用至关重要的一级概率安全评定模式的质量属性在参考文献[40]提供。

12.5. 概率安全评定应当在电厂的整个生命周期内更新，概率安全评定的范围、详细程度和准确性应当随着设计的发展、为支持概率安全评定中的建模假设而进行的更多分析以及从电厂运行经验中获得的数据而增加。概率安全评定的结果应当用于确定设计和运行弱点，并对改进设计或运行的选项进行评定和排序。

12.6. 概率安全评定模式以及（如有必要）概率安全评定应用程序应当在电厂的整个生命周期内定期更新，以考虑设计、运行实践、运行经验和其他影响概率安全评定建模参数问题的归属变化。

12.7. 在从概率安全评定中获得风险洞察时，应当注意理解各种类型的事故起始因子（即内部始发事件、内部和外部危害）和电厂运行状态对概率安全评定结果贡献的相对重要性。特别是，应当认识到，各种风险因素（如危害、电厂运行状态、设施）的汇总意味着单一因素在详细程度、分辨率、固有的保守性和不确定性方面存在一定程度的异质性。这种异质性可能会导致概率安全评定的误导性洞察，因此在决策过程中应当予以考虑（见参考文献[16]） [57] 这对于依赖重要性测量评价的概率安全评定应用和风险监控类型的应用尤为重要。因此，强烈建议为每个风险贡献者分别计算各种结构、系统和部件的风险重要性。例如，地震事件和内部事件的风险重要性测量应当分别计算。

12.8. 在从概率安全评定获得风险洞察时，应当注意考虑不确定性的主要来源，并且可能需要对主要假设进行敏感性分析。

12.9. 对于运行电厂的一级概率安全评定应用，所涉及的技术和概率安全评定的含义应当充分传达给电厂管理层，以便其对相关管理职责有一个完整的理解。

12.10. 在这些应用中，需要一级概率安全评定结果，以及结果的详细定性总结和所有建模结构、系统和部件和事件的相关风险洞察和风险重要性，

[57] 例如，在分析火灾风险时，通常采用连续划界和筛选方法，以便根据所采用的筛选标准，分析某一特定火灾区域的详细程度取决于其对堆芯或燃料损坏频率的影响是否足够低。这样做是为了优化用于详细火灾建模或电缆追踪的资源。外部洪水是另一个示例，其中与灾害相关的不确定性可能远远大于与内部事件相关的不确定性。

以将风险洞察添加到安全文化中。此外，电厂管理层积极参与所有风险知情应用程序将建立如何管理风险的意识。

12.11. 概率安全评定模式如何很好地反映建成和运行的电厂，以便电厂管理层对概率安全评定结果有信心，这是许多概率安全评定应用的最重要属性之一（见参考文献[40、41]）。

12.12. SSR-2/2[39]第 4.32 段指出：

> “如果风险的概率评定用于决策目的，营运组织必须确保风险分析具有用于决策目的的适当质量和范围。风险分析必须由具有适当技能的分析人员进行，并必须按照适用的法规和电厂许可证条件，以补充决策的确定性方法的方式使用。”

风险的概率评定应当伴随着对概率安全评定概念和方法的基本理解，以便能够正确解释结果。

一级概率安全评定应用的范围

12.13. 为了满足 GSR Part 4（Rev.1）[3]要求 4，根据规定的概率安全目标或标准，安全评定应当包括全范围概率安全评定，用于评定正常运行、预计运行事件和事故工况下的安全挑战。概率安全评定的完整性（包括一套全面的内部始发事件、内部危害以及自然和人类引发外部危害）并解决所有电厂运行状态，包括启动、功率运行、停堆和换料）将确保概率安全评定中与事故序列、结构、系统和部件、人为错误和共因故障的风险重要性相关的洞察来自电厂的全面、集成模式。然而，对于一些概率安全评定应用，预计可能需要洞察电厂特异性或一般二级甚至三级概率安全评定。

12.14. 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部范围不同。如果风险洞察来自概率安全评定，而概率安全评定的范围小于本“安全导则”描述的全部范围（例如，没有考虑所有始发事件和危害），则在应用概率安全评定洞察时应当认识到这一点。[58]

[58] 例如，如果一级概率安全评定不包含内部火灾的分析，则将概率安全评定洞察用于电缆布线是不可行的。

12.15. 如果概率安全评定旨在用作一个场址多个类似装置的代表性概率安全评定，则应当确定特定装置和代表性模式之间的任何差异的影响，并评定对概率安全评定结果的影响。

12.16. 对于多机组核电厂，国家安全政策或法规可能要求在风险知情决策中使用与多机组相关的风险。在这种情况下，应当使用来自多机组概率安全评定洞察（如果可用）或来自概率安全评定洞察，从单机组的角度适当考虑多机组的相互作用（例如，考虑同时影响多机组的始发事件、机组之间的共享系统、对人员绩效和资源的影响、机组间依赖性的评定、考虑级联或并发排放）。

风险知情方法

12.17. 在本部分所述的任何概率安全评定应用中，概率安全评定洞察应当被用作风险知情决策过程的一部分，该过程应当考虑以下因素（见参考文献[9、13]）：

(a) 与正在考虑的概率安全评定申请相关的任何强制性要求（例如法律要求或法规）；

(b) 来自确定性安全分析的洞察（例如，是否满足纵深防御要求的规定，是否有足够的安全裕度，是否满足较低水平的要求，如在执行安全功能的结构、系统和部件中提供足够水平的冗余性和多样性，电厂中的设备是否鉴定，足以承受始发事件后的恶劣环境）；

(c) 任何其他适用的洞察或信息（例如，成本效益分析、电厂剩余寿命的详细信息、检查结果、运行经验、工作人员对电厂进行改造的剂量）。

12.18. 当在风险知情方法中应用概率安全评定时，任何决策都应当以平衡的方式做出，并考虑所有相关因素。本部分的其余部分没有涵盖所有可能的概率安全评定应用，下文只概述个别国家最常用的应用程序。[59]

[59] 参考文献[40、41]是提供关于概率安全评定应用的额外信息出版物的示例。

概率安全评定在设计评价中的使用

12.19. 概率安全评定应当用于在设备的整个寿命期间为设计评定提供输入，如下所示：

(a) 概率安全评定应当在概念阶段使用，以提供对信用系统的拟议设计和电厂布局是否充分的洞察。

(b) 概率安全评定应当在概念阶段使用，以确定需要考虑作为电厂设计基准和许可基础的始发事件的范围。为了满足 SSR-2/1（Rev.1）[2]要求 20，在适用的情况下，内部始发事件的一级概率安全评定模式应当用于确认一组没有显著燃料退化的设计扩展工况，该条件应当根据 SSG-2（Rev.1）[5]第 3.40 段确定得出。

(c) 概率安全评定应当在整个设计和建造阶段进行更新，以考虑与设计、安全分析和选址相关的新信息。

(d) 概率安全评定应当作为运行电厂的活的概率安全评定进行维护，并作为解决与运行相关问题的输入之一，定期安全评审和寿命延长，以及提供关于拟议设计修改和运行变更是否充分的洞察。

(e) 概率安全评定应当用于核电厂的退役阶段，以确保与退役过程和贮存在现场的残留放射性物质相关的风险可以忽略不计（见原子能机构《安全标准丛书》第 WS-G-5.2 号《使用放射性物质设施的退役安全评定》[42]第 4.28 段和第 4.29 段）。

概率安全评定在核电厂设计决策中的使用

12.20. 为了获得最大的利益，用于设计评定的概率安全评定应当是第 12.13 段规定的全范围概率安全评定。这将确保电厂的设计和运行的广泛问题可以使用概率安全评定来解决。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、内部和外部危害的范围，以及概率安全评定中涉及的电厂运行状态的范围。

12.21. 根据 SSR-2/1[2]第 5.76 段。设计必须适当考虑概率安全评定，以确定已实现平衡设计，防止陡边效应，并将分析结果与风险验收标准进行比较。陡边效应应当以敏感性研究的形式在分析结果中进行试验，方法是改变一组可能具有显著风险的分析输入数据。

12.22. 来自概率安全评定洞察允许新的电厂设计在风险指标和成本方面得到优化。概率安全评定的结果应当用于提供一种确定以下各项的方法：

(a) 信用系统是否具有足够的多样性和冗余性；
(b) 对于在事故工况下经历恶劣环境的结构、系统和部件，是否有足够的设备认证水平；
(c) 对于火灾和水淹等危害，是否有足够的隔离和隔离区域；
(d) 人机界面的设计是否足以确保人为错误的可能性已经降低到足够低的水平。

概率安全评定的结果还应当用于确定是否需要纳入额外措施来降低风险。

12.23. 概率安全评定包括对变体和探索性设计方案的调查，以及系统冗余和多样性的充分性，并在一定程度上反映了应急安排和事故管理措施。概率安全评定的结果应当用于提供信息，以加强应急安排 [60] 和事故管理措施。概率安全评定结果还应当用于分配结构、系统和部件的可靠性和可用性目标，以满足概率安全目标或标准，从而构成设计规范的一部分。此外，概率安全评定应当作为选择或修改设计基准事故和设计扩展工况以及定义一般设计标准的支持工具。概率安全评定也可用于为成本效益分析提供输入。

12.24. 当将概率安全评定应用于核电厂的设计时，应当特别努力正确反映以前的概率安全评定中可能没有涉及的新设计特点（例如，特殊的始发事件、故障模式、共因故障、特定事件序列、依赖性）。

12.25. 在早期设计阶段进行的概率安全评定中，应当记录由于缺乏设计和运行细节而需要额外假想事实，并应当在设计的后期阶段（如建造或调试阶段）检查这些假想有效性。

12.26. 应当使用不确定性分析和敏感性研究来评定输入信息、数据和由此产生的风险估计的不确定性。应当证明用于设计优化和安全评定的风险洞察不依赖于主要假设和关键不确定性。

---

[60] 可以理解的是，概率安全评定可能无法处理与应急安排效力有关的所有方面。概率安全评定的预期输入与事故序列的时间和动态、风险显著的假想方案以及假想方案期间背景的详细信息（如现场破坏、排放细节）等方面相关。

12.27. 一级概率安全评定模式中的最小割集清单应当用于确定电厂设计和运行相对弱点。应当针对对堆芯和/或燃料损坏频率有显著贡献的最小割集进行此运行，以便识别对堆芯和/或燃料损坏频率有最大贡献的始发事件、部件故障和人因故障事件组。对于包含重要性值很高的基准事件的最小割集也应当这样做。

12.28. 应当利用单组始发事件对堆芯和/或燃料损坏频率的贡献，以及单组始发事件的最小割集对堆芯和/或燃料损坏频率的贡献，来确定核电厂的设计是否平衡（即确保没有特定组始发事件和组内没有特定事故序列对堆芯和/或燃料损坏频率的贡献过大）。[61]

12.29. 概率安全评定应当用于核实给定设计的单一故障标准。这可以使用最小割集清单来完成，以确定是否存在仅包含始发事件和单一故障事件或单一人因故障事件（不包括用于在特定电厂运行模式下控制系统配置的配置基准事件）的任何最小割集，这可能指示设计没有满足单一故障要求。

12.30. 应当评审主要最小割集清单，以确定如果发现缺陷，是否有机会加强纵深防御。

12.31. 应当计算基准事件、基准事件组、信用系统和始发事件组的重要性测量，并用于解释概率安全评定的结果。[62] 独立故障事件的高福塞尔－维斯利重要性值或伯恩鲍姆重要性值可能表明系统在某些电厂运行状态下冗余性不足，或可靠性低，因此需要改进。独立故障事件的高风险实现价值可能表明应当小心维护设备的可靠性水平，以避免风险增加。共因故障的高福塞尔－维斯利重要性值可能表明信用系统在特定安全功能方面的多样性不足。在这种情况下，可能需要对设计基准进行相当大的修改。在电厂设计过程中，应当以互补的方式使用几个重要措施来支持决策。

12.32. 当多机组和/或源并置在一个场址时，应当在风险知情设计优化过程中考虑其中一个机组对其他机组的影响，以支持降低该类影响的风险重要性。

---

[61] 国际实践表明，对于外部危害，特别是对于新设计很难实现这一目标，因为对于内部始发事件，堆芯和/或燃料损坏频率值可能相对较低。

[62] 关于各种重要措施的解释，见第 5.171 段。

概率安全评定在许可证发放过程中的使用

12.33. 对电厂整体安全的评定对于获得运行许可证是必要的，通常涉及全面的一级概率安全评定[63]作为许可证申请的一部分，概率安全评定的结果应当与概率安全目标或标准（如果已定义）进行比较。申请建造前许可证的安全评定可能涉及有限范围的概率安全评定（例如，使用类似电厂的数据）。

12.34. 一级概率安全评定的总体结果（通常是堆芯和/或燃料损坏频率）应当与概率安全目标或标准（如果已定义）进行比较，以确定电厂的拟议设计和运行是否将确保足够低的风险水平。其目的应当是确定是否达到了目标和标准，并提供一个广泛的指示，表明电厂是否达到了足够的安全水平（即，电厂设计中是否纳入了足够的信用系统，以及是否有足够的应急、运行、维护和试验程序来防止运行期间的堆芯或燃料损坏）。

12.35. 一级概率安全评定的结果与概率安全目标或标准的比较应当从概念设计开始，并在设计、建造和运行阶段的不同阶段重复进行，以帮助安全、技术和组织决策，并检查设计是否足够。

12.36. 在进行第 12.35 段所述的比较时。应当考虑敏感性研究和不确定性分析的结果。这些结果将表明实现目标和/或标准的信心程度以及实现目标和/或标准的可能性。

12.37. 该概率安全评定申请应当包括在旨在获得公众对核电厂建设和运行的认可的预许可过程中提供的信息。

设计方案的比较

12.38. 当考虑对核电厂进行改造时，通常有许多选择。概率安全评定应当用于为这些选项的比较提供输入。完成此运行的方式取决于所考虑的改造的复杂性，但范围可以从修改概率安全评定模式以纳入拟议新信用系统（对于复杂的改造）到对最小割集进行后处理（对于简单的改造）。概率安全评定应当为组合风险知情决策过程提供输入，以确定选择哪一个选项（见参考文献[9、13]）。

---

[63] 不同的国家根据所考虑的危害和始发事件以及燃料的位置（如反应堆、乏燃料水池、新鲜燃料或辐照燃料贮存设施），对用于许可证目的的概率安全评定范围有不同的要求。

12.39. 与新设计电厂的概率安全评定相比，运行电厂的概率安全评定中假设和简化的使用应当受到限制，因为电厂特定信息的使用总是更可取的。

概率安全评定在定期安全评审中的使用

12.40. SSR-2/2（Rev.1）[39]第 4.46 段指出：“概率安全评定……可用于[定期]安全评审的输入，以深入了解电厂不同安全相关各方面对安全的贡献。”应当按照原子能机构《安全标准丛书》第 SSG-25 号《核电厂定期安全评审》[43]提供的安全要素 6：概率安全评定的建议对一级概率安全评定进行评审。

12.41. 该应用的安全评定过程应当包括识别安全问题、评定其安全重要性以及就纠正措施的必要性做出决定。

12.42. 在定期安全评审中，概率安全评定应当用于创建整个核电厂的最新概览，并帮助确定具有成本效益的安全改进措施。[64] 因此，概率安全评定应当使用电厂特定数据、建造和运行时的电厂工况模式，并解决老化现象和部件寿命考虑因素对整体风险指标的可能影响。可进行敏感度计算以评定老化对通常得不到维护或更换的非能动部件的潜在影响。[65]

12.43. 应当利用积累的运行经验或知识的发展来核实为本部分所述概率安全评定应用提供的概率安全评定洞察的充分性（例如，核实设计扩展工况规定的充分性，以防止燃料显著退化）。

内外部危害防护的最优化

12.44. 内部和外部危害的概率安全评定应当从设计制定一开始就进行，以便针对内部和外部危害始发事件对设计进行早期优化。

12.45. 支持针对内部和外部危害的设计优化的概率安全评定应当用于为以下方面提供输入：

(a) 检查结构、系统和部件对内部和外部危害的稳健性，包括遏制（基于内部和外部危害的概率安全评定结果）；

---

[64] 作为定期安全评审的一部分，概率安全评定可用于支持延长电厂的寿命，支持对可能的回流进行成本效益分析，以降低严重事故的风险，并评定安全相关问题（如偏离法规）的风险重要性。

[65] 目前，概率安全评定背景下的结构、系统和部件老化建模处于探索阶段，老化效应通常是定性解决的。

(b) 制定设备隔离、电缆追踪和电厂布局的标准（例如，根据火灾和水淹概率安全评定的结果）；

(c) 洞察危害发生因素（如高能管线的关键位置、关键火源）并设计保护功能（如火灾探测、火灾缓解、水淹或防火屏障、外部洪水防护措施）；

(d) 建立防火隔间、排水、水淹探测和隔离的分隔和/或隔离标准；

(e) 识别并减少可能导致火灾或水淹事件的维护活动。

12.46. 在设计阶段，应当考虑与内部和外部危害的概率安全评定重要方面相关的不确定性（例如，详细的电缆布线，防火和防水淹屏障，结构、系统和部件的锚固，部件的位置和方向）。

概率安全评定在视察、试验和维护最优化的使用

12.47. 第 12.48－12.79 段提供建议在满足 SSR-2/2[39]要求 31，其中相关段落规定：

> “8.5.个别结构、系统和部件的维护、试验、监视和视察频率必须根据下列各项确定：
>
> (a) 结构、系统和部件对安全的重要性，考虑概率安全评定洞察；
>
> (b) 它们运行可靠性和可用性；
>
> (c) 评定其运行中退化的可能性及其老化特征；
>
> (d) 运行经验；
>
> (e) 供应商的建议。
>
> “8.6. 必须采取全面和有条理的办法识别故障情况，以确保适当管理维护活动，酌情使用概率安全分析方法。
>
> ……
>
> “8.13. 营运组织必须确保在功率运行期间进行维护工作时有足够的纵深防御。必须酌情使用概率安全评定，以证明风险不会显著增加。”

风险知情技术规范

12.48. 概率安全评定应当用于为风险知情技术规范提供一致的基础，这些技术规范规定了与受影响的电厂特征的风险重要性相关的电厂运行和维护的限值和条件。[66]

12.49. 概率安全评定应当用于制定技术规范，并确定技术规范中包含的设备。这样，在没有为其运行指定限值和条件的情况下，具有高度安全意义的设备不会被排除在技术规范之外 [67]。

12.50. 如果发生不导致反应堆立即停堆的异常事件，概率安全评定洞察应当作为建立或核实应当实施措施的输入使用如下：

(a) 在设计阶段，一级概率安全评定有助于量化与不同允许大修时间（或其他相应措施）以及为应对同一异常事件而采取的任何额外措施相关的风险。应对这些风险进行比较，并提出风险方面的最佳选择，以纳入技术规范。在量化该类风险时，应当同时考虑在允许时间内继续运行的风险和措施实施后的风险。

(b) 对于已经有技术规范和运行限值和条件的运行电厂，应当使用一级概率安全评定来证明其正当性，并在正当性不充分的情况下建议修改允许大修时间（或其他相应措施）。

在这两种情况下，应当使用全范围一级概率安全评定并酌情修改，以考虑与特定异常事件或电厂配置相关的所有方面。如果一级概率安全评定的范围有限，则只有当异常事件或电厂配置对概率安全评定缺失部分相关风险的影响被证明可以忽略不计时，才能使用一级概率安全评定。

12.51. 当建议将特定维护活动从功率运行状态转移到关闭状态（反之亦然）时，概率安全评定应当用于评定与修改后的电厂配置相关的风险。

---

[66] 技术规范确定了在发生不导致反应堆立即停堆的异常事件时应当采取的措施，以及在实施这些措施之前允许的大修时间（或其他相应措施），以及任何必要的额外行动（例如，对冗余设备的额外试验要求、降低功率水平、断开受影响设备、立即维修故障部件）。如果超过允许的大修时间（或其他相应措施），技术规范规定了运行人员应当采取的进一步措施。技术规范通常基于确定性要求和工程判断。

[67] 运行限值和条件规定了对设备可运行性的要求，通常限制可同时拆除进行维护的设备组合（称为配置控制）。

12.52. 概率安全评定提供的洞察应当包括与用于支持技术规范风险知情的决策标准或导则进行比较所需的信息。这种信息的示例包括维护和维修期间的有条件的堆芯损坏或燃料损坏频率，增量有条件的堆芯和/或燃料损坏概率，每年累积的、递增的、有条件的堆芯和/或燃料损坏概率，以及变化对平均每年堆芯和/或燃料损坏频率的影响。

监视试验间隔时间的确定与评价

12.53. 监视试验间隔决定了试验的频率，有时还决定了安全重要结构、系统和部件的试验策略。基于概率安全评定的监视试验间隔评定考虑了因未检测到的故障而导致不可用风险，以及因试验和试验导致故障而导致不可用风险。

12.54. 该应用程序的目标是优化监视试验策略和间隔对设备可靠性和整体风险估计的影响。在优化试验间隔时，通常会考虑监视试验期间可能发生的潜在人为错误，这些错误可能会对安全产生不利影响（例如，导致电厂跳堆和始发事件）。

12.55. 在设计阶段，应当考虑概率安全评定模式中包含的所有结构、系统和部件，以量化与不同在役试验间隔策略相关的风险，并选择将确保以下各项的策略：

(a) 实现了设计的总体概率安全目标或标准。

(b) 对安全具有高度重要性的部件有更严格的试验要求。

(c) 降低了试验期间和之后可能导致设备不可用或始发事件的人因故障事件的概率。

(d) 在役试验间隔不会因试验部件可能过度磨损而导致设备过度不可用。

12.56. 对于已经有在役试验策略的运行电厂，概率安全评定应当用于证明其正当性，并建议具有最高风险贡献和高风险重要性值部件的在役试验间隔的变化。

12.57. 在量化该类风险时，应当考虑到数学模式和试验部件数据的不确定性。

12.58. 在为监视试验间隔策略的最优化或正当性提供概率安全评定的输入时，应当调查并考虑以下因素：

(a) 在役试验间隔与部件故障概率（如频繁试验造成的磨损）之间的相关性；

(b) 适当考虑试验类型（即交错或非交错）的共因故障；

(c) 潜在的人因故障事件，包括试验期间和之后的调试错误，导致部件不可用和/或始发事件。

12.59. 对于新建和运行核电厂，应当使用全范围概率安全评定来考虑不同在役试验间隔策略的影响。只有在证明在役试验间隔策略的变化对概率安全评定缺失部分相关风险的影响可以忽略不计的情况下，才应当使用有限范围的概率安全评定。

12.60. 概率安全评定模式应当明确地对由于结构、系统和部件试验而导致不可用性进行建模，并使预测在役试验间隔的变化对每个受影响的结构、系统和部件的影响成为可能。

12.61. 应当使用风险重要性测量来对在役试验间隔变更的候选结构、系统和部件进行优先级排序。风险测量的变更应当用于评定拟议变更的风险重要性和可接受性，增量风险测量应当用于评定新拟议在役试验间隔的可接受性。

12.62. 为了平衡监视试验的积极和消极方面，需要洞察试验过程中的人为错误如何导致事件频率和部件故障的发生。应当考虑到由于试验后人为未能正确恢复正常排列而导致设备不可用。如果已知试验可能导致更高概率的始发事件（始发事件的频率与试验频率相关），那么如果试验频率发生变化则应当考虑这一点。

风险知情在役试验

12.63. 目前定期在役试验的方法是根据规范或标准进行试验，该规范或标准可能包含也可能不包含在规定条例中，该法规使用确定性方法来决定需要为电厂的结构、系统和部件进行的在役试验计划。

12.64. 将风险知情方法应当用于在役试验的目的是利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，以便将重点放在具有最高风险重要性的部件上。风险知情在役试验方法可以让运行人员对具有各种风险重要性的部件进行优先排序，并有可能防止试验对部件产生不适当的不利影响，提高部件的可用性，同时仍然保持非常高的安全。

12.65. 在将风险知情方法应当用于在役试验时，概率安全评定的结果应当与确定性和工程性考虑因素一起使用，以确定待处理部件的风险重要性。

12.66. 概率安全评定中的风险信息应当使用福塞尔－维斯利重要性和伯恩鲍姆重要性（或风险实现价值）得出，因为这两种重要性测量都提供了对部件风险重要性的洞察，并应当包括共因故障考虑因素。

12.67. 如果多机组概率安全评定模式可用，应当使用它来支持与共享系统相关部件的风险知情试验。就多机组核电厂的风险指标而言，多机组概率安全评定模式的使用可以提供关于共享系统和部件的风险重要性的额外洞察。

12.68. 风险信息应当用于识别安全重要性相对显著的部件，需要进行严格的使用试验，以及安全重要性相对较低的部件，可以进行不太严格的试验。考虑到部件的安全重要性，可以修改在役试验计划。

12.69. 当修改了在役试验间隔时，应当使用一级概率安全评定来计算新试验间隔的堆芯和/或燃料损坏频率，以确定这些变化是否可接受。

风险知情役前和在役检查

12.70. 核电厂管道系统使用前和使用中视察计划的总体目标是在故障发生前确定可以维修的退化区域。通常实施的视察计划基于传统的确定性方法和工程判断。在风险知情的役前和在役检查方法中，假设管道工程的各个部分的风险重要性是通过定性或定量退化潜力评定和管道工程的各个部分故障的潜在后果评定（如有条件的堆芯损坏概率）的组合来确定的，这可能以风险矩阵的形式呈现。

12.71. 应当使用风险知情方法提供概率安全评定洞察，以修订视察计划（在视察频率、使用的方法和样品量方面），重点关注风险重要性最高的管道工程的各个部分，并减少对风险重要性较低的管道工程的各个部分进行的视

察。预计这将导致进行的管道视察总数减少，并减少相关的职业照射，而不会增加风险估计。[68]

12.72. 在设计阶段，应当使用风险知情方法来支持视察计划的制定，以防止风险显著的管道系统故障。对于运行电厂，该计划应当根据运行经验的反馈进行维护和更新。

12.73. 来自概率安全评定洞察应当作为确定以下内容的输入：

(a) 通过风险知情的役前和在役检查评定管道工程的各个部分；
(b) 待评定管道工程的各个部分的风险重要性；
(c) 待视察管道工程的各个部分的目标故障概率；
(d) 因役前和在役检查计划的变化而导致风险变化。

12.74. 对于概率安全评定研究中包括的每一管道工程的各个部分，该管道部分故障的后果应当以下列方法之一确定：

(a) 作为始发事件，考虑可能发生的任何次生故障（例如，由于水或蒸汽排放、管道抖动）；
(b) 作为备用系统中的故障，可能导致系统通道（或整个系统）无法执行其安全功能；
(c) 当系统通道（或整个系统）按需运行时，由于施加在管道管段上的负载而出现故障。

12.75. 直接导致始发事件的管道故障通常已经包含在全范围概率安全评定中。应当检查情况是否如此，并对管道故障导致所有始发事件评定有条件的堆芯或燃料损坏概率。这些概率的排列应当用于识别风险最显著的管道。

12.76. 对于导致信用系统不可用或信用系统按需故障的管道故障，概率安全评定应当用于计算有条件的堆芯和/或燃料损坏频率。该类故障并不总是包括在概率安全评定模式[69]中，因此该模式应当针对概率安全评定应用进

[68] 已经制定了几种进行风险知情在役检查的方法（见参考文献[44]）。示例包括电力研究所、压水堆业主团体和欧洲检验和鉴定网络推荐的方法。

[69] 有时，如果管道系统的故障对信用系统的故障概率的贡献与能动部件的故障相比可以忽略不计，则会筛选出该类故障。

行相应的修改。通常采用替代方法，其中未明确包括在概率安全评定中管道管段的故障与已经包括在概率安全评定中的基准事件（或基准事件组）有关联，并且故障的后果是相同的。在此过程中，应当考虑确保在概率安全评定模式中考虑管道故障的任何次要影响。

12.77. 确定风险知情役前和在役检查计划中所有管道管段的风险重要性的更严格方法是修改概率安全评定模式，明确包括这些管道管段，从而直接确定相关的有条件的堆芯和/或燃料损坏频率。这种方法已在多个成员国实施的许多风险知情役前和在役检查计划中使用[44]。

12.78. 当修订后的役前和在役检查计划确定后，概率安全评定应当用于确定与决策标准或用于评定计划变更可接受性的导则进行比较所需的风险洞察。这应当通过估计因役前和在役检查计划的变化而导致始发事件的频率或部件故障概率的特定变化，并通过用这些修订值重新量化概率安全评定，或通过进行敏感性研究来实现。在这一过程中，应当认识到并考虑到概率安全评定在建模细节和范围方面的相关限制。

12.79. 如果多机组概率安全评定模式可用，应当使用它来支持与共享系统相关的管道系统的风险知情视察。应当额外考虑共享系统管道系统故障的影响，以确定如何使用风险知情方法调整视察策略。

结构、系统和部件的风险知情分类

12.80. 提供以下建议以支持 SSR-2/1（Rev.1）[2]要求 22 的应用，该要求根据其功能和安全重要性对所有安全重要物项进行识别和分类。SSR-2/1[2]第 5.34 段指出：

> “安全重要物项的安全重要性分类方法必须主要以确定性方法为基础，并酌情以概率方法为补充，同时适当考虑到以下因素：
>
> (a) 物项将执行的安全功能；
> (b) 未能履行安全功能的后果；
> (c) 调用该物项执行安全功能的频率；
> (d) 在假想始发事件之后的时间，在此时间或期间，该物项将被要求执行安全功能。”

12.81. 此外，原子能机构《安全标准丛书》第 SSG-30 号《核电厂结构、系统和部件的安全分级》[45]就使用概率安全评定进行安全分级提出了以下建议（脚注略）：

> “2.3. 安全分级是一个反复的过程，必须在整个设计过程中定期进行，并在电厂的整个寿命期间保持。将结构、系统和部件分配到特定安全等分级必须使用确定性安全分析，辅之以概率安全评定洞察力，并以工程判断为依据。
>
> ……
>
> “2.14. 这一进程的下一步是确定所有安全重要结构、系统和部件的安全分级。通常必须采用确定性方法，并酌情辅以概率安全评定和工程判断，以获得适当的风险概况，即在电厂设计中，后果严重程度高的事件预计发生频率非常低。
>
> ……
>
> “3.27. 必须利用确定性安全分析来核实安全分级的充分性，并辅之以概率安全评定洞察和/或工程判断的支持。
>
> “3.28. 结构、系统和部件对降低电厂总体风险的贡献是确定其安全级别的一个显著因素。确定性和概率方法之间的一致性将使人们确信安全分级是正确的。”

12.82. 应用风险知情分类的目的是为根据以下标准向结构、系统和部件分配安全级别的过程提供输入它们的风险重要性。[70] 概率安全评定应当用于考虑是否可以对某些结构、系统和部件的传统规范性监管要求进行修改，以使要求更加符合结构、系统和部件的安全重要性。由一组具有各种相关专门知识（如概率安全评定、确定性安全分析、运行、维护、技术或许可）的专家进行的分析，可能会产生一项提升或降低被调查项目分类的最终建议。在由此产生的升级的情况下，以前隐藏的影响核安全的设计不平衡可

[70] 安全分级的历史方法是对所有被确定为对安全重要的结构、系统和部件应用高水平的质量保证。然而，迄今为止进行的许多概率安全评定的结果表明，一些安全分级的结构、系统和部件显示出相对较低的安全显著性，而一些非安全分级的结构、系统和部件显示出相对较高的安全显著性。

能会被消除。在由此导致退化的情况下，运行人员实施监督计划所需的资源可能会减少，不必要的监管负担可能会消除而不会增加风险。

12.83. 一级概率安全评定应当用于确定用于防止堆芯或燃料损坏的结构、系统和部件的风险重要性。应当使用福塞尔－维斯利重要性（或提供等效信息的测量，如风险降低价值或部分贡献）和伯恩鲍姆重要性（或风险实现价值）来推导风险重要性，因为这两种重要性测量都提供了对结构、系统和部件风险重要性的洞察。假设结构、系统和部件发生故障，有条件的堆芯或燃料损坏频率也应用作风险重要性的衡量标准。然后，应当将风险重要性参数与定义为与传统（即确定性）分类方法一致的阈值进行比较。

12.84. 当将系统分类为具有低或高安全重要性时，风险重要性应当与其他重要信息（如纵深防御）一起用作风险知情决策过程的输入之一。

12.85. 应当考虑是否可以降低被归类为对安全重要但安全重要性相对较低的结构、系统和部件的要求，以及是否应当提高被归类为对安全不重要但在概率安全评定中具有不可忽略的重要性的结构、系统和部件的要求。

12.86. 当大量结构、系统和部件被重新分类并根据风险重要性调整其处理（如试验和维护）时，概率安全评定中模拟的大量结构、系统和部件的估计故障概率可能会发生变化。

因此，应当评定风险的累积影响，以确保任何累积的潜在风险增加都是可接受的。

监控和管理风险配置

12.87. 风险监控器是一种实时分析工具，应当用于根据实际电厂配置（通过许多因素，通常包括电厂运行状态、已停止运行的部件以及正常运行系统的运行通道和备用通道的选择）和当前环境运行工况（例如，夏季高降雪或极低温度的影响应当不出现在风险简介中）生成风险信息。

12.88. 风险监控器可用于计划未来的维护大修、风险的长期分析、累积增量有条件的堆芯和/或燃料损坏概率的分析以及与异常电厂运行（即设备故障等意外事件）相关的风险评定。

12.89. 风险监控器生成的信息可用于日常维护计划，以确保维护活动的计划方式尽可能避免风险高峰，并且电厂的累积、增量、有条件的堆芯和/或燃料损坏概率较低。

12.90. 风险监控器为运行电厂提供的定量和定性风险信息应当作为综合的、风险知情的决策过程的一部分，该过程还应当考虑其他方面（如电厂的技术规范、纵深防御）。尽管风险监控器仅用于运行电厂，但一旦电厂的设计已经最终确定，在设计阶段就开始制定风险监控器是一种良好的实践。

12.91. 风险监控器应当提供定量风险信息（例如，计算时间点堆芯或燃料损坏频率、允许的配置时间以及累积、增量、有条件的堆芯和/或燃料损坏概率）和定性风险信息（例如，安全功能和系统的状态）。

风险监控器的概率安全评定模式及软件

12.92. 应当修改风险监控器的概率安全评定模式，使其计算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。

12.93. 应当修改概率安全评定模式，以消除为减少概率安全评定所需分析量而进行的任何简化（例如，建模不对称），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不正确的结果。

12.94. 为了制定风险监控器，概率安全评定模式应当得到增强，以便它提供与实际电厂配置更密切相关的风险计算。例如，它必须是对称的，以考虑所有可能的配置（例如运行系统的配置），并且必须能够将基准事件的状态设置为真或假，以显示由于试验或维护而导致部件不可用，从而反映当前的部件配置。所制定的概率安全评定模式还应当与用于风险监控的软件兼容。[71]

12.95. 风险监控器的设计应当供洞察核电厂设计和运行的核电厂人员使用，而不仅仅供概率安全评定专家使用。

12.96. 概率安全评定从业者或风险监控器用户可能做出的改变应当与这些个人的专业水平相称，并应当记录在案。

---

[71] 可能需要将概率安全评定中制定的事件树和故障树模式改变为一个逻辑等价的大型故障树模式（通常称为“顶级逻辑模式”），或者改变模式中使用非逻辑和逻辑开关的方式。

12.97. 为风险监控应用程序选择（或制定）的软件应当经过验证，应当提供广泛的功能，并应当可供广泛的电厂人员使用。

12.98. 软件应当能够在满足其主要用户（如工作计划人员、控制室运行人员）的需求的时限内提供结果，以履行其预期功能（如评定和管理计划或紧急情况下的配置风险）。

12.99. 风险监控器应当以潜在用户容易理解的方式呈现信息。这通常以彩色显示器的形式进行，给用户一个清晰的视觉指示，说明风险水平或安全功能和系统的状态。

12.100.风险监控器验证过程应当旨在提供高度的可信度，即风险监控器产生的定量结果是准确的，并且与所有可能的电厂配置的基本情况概率安全评定给出的结果相同或相当。

风险监控器的局限性

12.101.风险监控器的用户应当意识到风险监控器模式的范围和详细程度的重要限制，以及风险监控器提供的风险信息的相应限制。例如，如果模式不包括内部和外部危害，它可能无法捕捉到致力于缓解这些危害造成事件的信用系统的重要性。因此，如果没正当证明所考虑的决策不受模式缺失部分的影响，就应当不将风险监控模式用于决策。

基于风险安全绩效指标

12.102.概率安全评定结果应当用于确定一组适当的绩效指标，以提供电厂安全绩效的回顾性或当前指示。

12.103.基于风险安全绩效指标侧重于过去的电厂行为，考虑到已经发生的事件以及结构、系统和部件的故障和不可用性，应当用于确定趋势，并在预期和计算的风险值之间进行比较，以便决策人员能够确定结构、系统和部件的老化影响。

12.104.基于风险安全绩效指标还应当提供与计划活动相关的风险变化信息。这些指标应当基于对风险的即时评定。

12.105.一旦基于风险安全绩效指标在监管机构和营运组织之间建立并达成一致，就应当使用这些指标来提高视察效率。

12.106.基于风险安全绩效指标应当使用基于电厂特定数据和实际运行经验的风险监控器或概率安全评定得出。

基于概率安全评定事件分析（前兆分析）

12.107.可以使用概率安全评定模式（前兆分析）对可能导致电厂跳堆和/或降低或禁用结构、系统和部件的运行事件进行分析和排序。这种实践现在在许多国家越来越普遍，并成为运行反馈的一个常规部分，以补充为确定根本原因而进行的传统确定性分析。

12.108.事件分析的目的是确定运行事件如何恶化为具有更严重后果的事故，并得出事件的风险重要性，以便对事件的响应符合其风险重要性 [72]。

12.109.应当对电厂的事件（也称为直接事件）和其他电厂的相关事件（也称为转置事件）进行基于概率安全评定事件分析。基于概率安全评定事件分析应当包括对始发事件和有条件事件的分析（其中始发事件的可能性增加或响应始发事件所需的信用系统的可用性降低）。

12.110.如果所讨论的事件是一个始发事件，应当使用活的一级概率安全评定模式来估计有条件的堆芯或燃料损坏概率。

12.111.如果所讨论的事件影响了一个或多个结构、系统和部件的可用性和/或运行人员的行动，但不是始发事件，概率安全评定模式用于计算有条件的堆芯或燃料损坏概率，同时考虑受影响结构、系统和部件的不可用性和事件的持续时间（例如，使用风险监视器）。

12.112.概率安全评定模式应当能够评价适用于事件的潜在影响。

12.113.对于具有显著潜在安全意义的事件，应当进行基于概率安全评定事件分析。为此，应当制定筛选标准，筛选出安全显著性较低的事件，并根据其安全显著性对事件进行排序。

---

[72] 通过对轻微运行事件进行基于风险的外推，得出具有严重后果的事故假想方案，可以在没有任何实际后果的情况下获得对事故的宝贵洞察。

12.114.电厂的状况、已经发生的故障和运行人员在事件中采取的行动应当被确定并准确地映射到概率安全评定模式中。概率安全评定模式应当重新量化，以产生与第 12.113 段提到的筛选标准进行比较所需的结果。比较所需的结果通常是有条件的堆芯或燃料损坏概率。

12.115.当进行基于概率安全评定事件分析（如显著性确定过程）时，应对已知的不利事件进行建模，将相关的基准事件设置为真，而对已知的成功事件进行建模，将相关的基准事件保持在其名义概率。

12.116.对事件的分析应当辅以敏感性研究，以提供“如果（what if ？）”问题的答案（例如，如果运行人员未能正确应对事件，有条件的堆芯和/或燃料损坏概率是多少？）。对这些问题的回答应当辅以定性的洞察，以提供对事件风险的主要贡献者的理解。

12.117.应当执行基于概率安全评定事件分析，以补充确定性分析，允许使用综合模式解决多个故障，并提供运行事件风险重要性的定量指示。它还应当用于为考虑可以做出哪些改变以降低该类运行事件再次发生的可能性提供输入。

12.118.在使用基于概率安全评定事件分析的结果来确定一个或一组核电厂在一段时间内的性能趋势时应当小心谨慎。这种基于概率安全评定事件分析应用的结果可能会产生误导，除非分析始终使用相同的模式、方法和假设。

12.119.如果多机组概率安全评定模式可用，则应当使用该模式来支持基于概率安全评定事件分析，方法是考虑共享系统的退化以及在多机组可能受到影响的情况下，始发事件对运行人员和共享资源行为的影响。

风险知情法规

12.120.概率安全评定应当用于识别电厂特定或一般的风险洞察，以及可以提高安全的设计或运行变更。概率安全评定洞察还应当用于指导监管目标和要求以及相关安全研究的长期优先级。风险指标的变化用于评定实施风险管理策略所需的监管要求的可能变化。

12.121.监管机构应当考虑利用概率安全评定洞察颁布风险知情法规，以加强公共安全或根据国家安全政策和法规发布电厂特定命令。

12.122.在某些情况下，概率安全评定洞察可能表明，法规给营运组织带来了显著的负担，而安全效益却可以忽略不计。在这种情况下，监管机构应当考虑颁布现有法规的风险知情替代方案或根据国家安全政策和监管要求取消该类法规是否合适。

12.123.在制定和更新法规和监管导则时，监管机构应当采用风险知情方法，考虑概率安全评定提供的风险信息和洞察，如下所示：

(a) 利用概率安全评定洞察来识别现有法规未涵盖的具有显著风险的领域，以便建立额外的法规；
(b) 确定现有法规或要求的相对风险重要性，以便根据其风险重要性进行修订；
(c) 识别法规或要求中不必要或无效的部分，以便撤销。

12.124.概率安全评定的范围和详细程度应当与调查中的问题相称，概率安全评定应当能够考虑到处理问题的所有方面。

风险知情监督和执行

12.125.监管机构就运行电厂进行的活动包括发出、修订、暂停或撤销授权或许可证，执行监管监督，确保采取纠正措施，并在必要时采取执法行动。从概率安全评定中获得的定性或定量风险洞察应当用于确定监管机构监督活动的优先次序并优化其活动，例如：

(a) 定义电厂设计和运行方面，以确保视察集中在具有高风险重要性的电厂设计和运行区域，并减少或不在具有低风险重要性的区域进行视察。
(b) 用于计划监管行动，以应对电厂特定事件或运行经验揭示的电厂特定潜在退化条件，监管机构在确定后续活动的规模时应当考虑风险重要性（例如，后续监管行动和执法的必要性）。
(c) 用于评定营运组织未能满足监管期望和遵守执法行动的重要性。

(d) 用于评定与视察结果相关的风险措施的变化。风险指标和条件风险指标的变化可用于评价视察期间发现的退化或问题的风险影响，并评价可能的纠正措施。

(e) 针对监督过程中发现的安全问题制定和评价纠正措施，包括对不同变量进行探索性调查，以解决特定问题，当风险指标的变化用于根据风险表征确定建议措施的风险重要性和风险可接受性时。风险指标的变化应当用于根据风险表征确定建议措施的风险重要性和风险可接受性。

12.126.概率安全评定应当用于评定和排列一般和新发现的电厂特定安全问题。应当使用风险贡献者和风险重要性测量来识别和排列安全问题。在概率安全评定之外发现的安全问题可以作为概率安全评定的一部分进行评定，以确定其风险重要性，一旦对问题进行了风险表征评定（即确定受影响的始发事件、事故序列、结构、系统和部件和运行人员的行动）。

12.127.在评定长期解决方案时，概率安全评定还可用于做出临时决策，以缓解监管问题。可能需要临时决定的问题示例如下：

(a) 针对某一电厂的某一事件采取监管行动的必要性；

(b) 技术规范或其他许可要求的一次性豁免；

(c) 对硬件配置或程序的临时修改。

12.128.所使用的概率安全评定的范围应当足以提供有价值的信息，并取决于监管关注的领域和视察结果。简化的一般概率安全评定模式最初可用于进行保守的筛选评定，如果结果显著，可进行更现实和详细的评定。必要时，应当针对特定关切领域扩大评价范围。

概率安全评定洞察制定或加强应急运行程序的使用

12.129.电厂脆弱性的系统评定和从一级概率安全评定中获得的洞察应当用于确定任何进一步制定（即完善或扩大范围）应急运行程序的潜在需求，确保以现实、适当详细和一致的方式解决广泛范围的脆弱性。

12.130.在设计阶段，一级概率安全评定使用参考电厂的应急运行程序进行事故序列建模和人的可靠性分析。概率安全评定过程允许识别没有完全考虑特定设计特点的程序。在设计阶段，应当使用风险洞察来识别参考电厂中不可用且应当制定的程序，或需要进一步阐述的程序。风险洞察还应当提供关于应急运行程序中应当包括的特定人工运行和应当明确描述条件的信息，以允许运行人员正确执行运行。

12.131.对于运行电厂，使用现有应急运行程序执行的一级概率安全评定事故序列分析中的信息，以及相关人员互动的评定，应当用于根据概率安全评定洞察确定需要改进的应急运行程序。

12.132.应当评审一级概率安全评定结果，以确定造成过度风险的电厂事件序列，以及信用系统仍然可用，但由于缺乏足够的应急运行程序而无法信任的电厂事件序列。对于该类电厂事件序列，应当进一步制定应急运行程序。

12.133.从一级概率安全评定中获得的洞察应当用于识别和评定现有、替代或额外系统、设备和措施的风险收益，这些系统、设备和措施可被拟议纳入应急运行程序，以恢复信用系统的功能并防止事件发展为严重事故。概率安全评定方法中使用的电厂响应的整体观点应当用于确定某些措施的潜在负面影响。

12.134.受影响或拟议行动和相关事故序列的风险重要性测量[73]应当用于帮助确定程序中可能变更的优先级。堆芯和/或燃料损坏频率的变化应当用于证明可接受的风险影响并确定风险重要性。

12.135.对运行人员行动的一级概率安全评定评审应当支持加强旨在防止严重堆芯或燃料损坏行动的应急运行程序。

12.136.如果现有的一级概率安全评定没有明确表示事故序列和运行人员的行动，特别是调用相关的应急运行程序，则应当提高一级概率安全评定模式在受涉及事故序列的程序变更影响区域的详细程度。

12.137.一级概率安全评定中使用人的可靠性分析方法应当能够预测程序变更的影响以支持该应用，否则应当重新考虑。

---

[73] 通常，福塞尔－维斯利重要性与伯恩鲍姆重要性（或风险成就价值）一起。

12.138.一级概率安全评定还应当就向严重事故管理导则过渡的指定决策点的潜在修订提供反馈。

使用概率安全评定洞察对电厂人员进行风险知情培训

改进运行人员培训计划

12.139.一级概率安全评定的结果应当用于确定运行人员显著风险行动的子集，并制定（针对电厂）通过提供关于事故过程、主要事故序列的相对可能性以及防止或缓解堆芯或燃料损坏所必需的相关行动的信息，改进（对于运行电厂）运行人员的培训计划。

12.140.应当描述堆芯或燃料损坏频率的主要事故序列，其中人因故障事件起重要作用，人因故障事件和相关结构、系统和部件的风险重要性测量，恢复措施和具有高风险重要性的事故管理措施，以加强运行人员的培训计划。这些还应当用于缓解人因故障事件的后果，概率安全评定结果应当用于选择强化培训有益的行动[74]。

12.141.概率安全评定中使用人的可靠性分析方法应当能够测量受影响的变化。风险测量的变化应当允许分析人员评定拟议变化的重要性和可接受性。

12.142.核电厂的运行人员花很大一部分时间接受电厂程序培训，因此，风险洞察应当用于风险信息培训，并确保运行人员有足够的时间了解风险显著行动。

12.143.培训应当至少告知运行人员相关显著风险行动的信息。可以通过调整某些假想方案的模拟机培训频率、运行人员的资格认证计划中增加风险显著假想方案以及在演习中使用风险显著假想方案来进一步增强这一点。

---

[74] 人因故障事件的风险实现值代表了如果个人未能采取行动，燃料损坏将增加的比率。相反，福塞尔－维斯利重要性参数代表了如果个人成功，燃料损坏频率可以降低的分数。因此，这两个重要性参数都应用作运行人员风险知情培训的输入。

改进维护人员培训计划

12.144.应当根据概率安全评定提供的洞察和信息，加强对维护人员的培训，重点关注维护活动的潜在风险显著影响，如多系统通道的共因故障和维护导致故障。

12.145.风险洞察提供了关于风险显著的结构、系统和部件，风险显著的功能和故障模式的信息，这些信息应当在维护计划中解决，并提供了优化对风险管理不显著的维护任务的机会。

12.146.与第 12.134 段建议的风险重要性措施相同。应当用于识别风险显著的结构、系统和部件，事故前人因故障事件以及与维护和共因故障相关的基准事件，并对其进行排序，以识别潜在的维护计划修订。

12.147.风险指标的变化（如燃料损坏频率）应当用于评价维护培训计划拟议修订的显著性和可接受性。

概率安全评定解决新出现问题的使用

12.148.随着运行经验的积累，可能会出现在电厂设计、建造和早期运行过程中未知的各种问题（例如，非能动结构、系统和部件与老化相关的故障机制）。

12.149.　概率安全评定中的定性和/或定量洞察应当用于评定新出现问题的风险重要性。

12.150.出现的许多问题可能与非能动结构、系统和部件的老化相关，退化和陈旧部件的更换相关，这在概率安全评定中无法明确建模。因此，应当仔细考虑如何使用概率安全评定模式对问题进行准确建模（例如，没有过于保守的假设），（例如，控制棒分组的退化状况应当不为未能插入控制棒建模）。由于新出现的问题通常提供有限的信息，应当使用敏感性分析来收集概率安全评定洞察。

12.151.营运组织应当利用概率安全评定洞察，在国家安全政策和法规的背景下确定解决新问题的优先级。

12.152.监管机构应当利用概率安全评定洞察，在国家安全政策和法规的背景下，为营运组织设定适当的时间表来解决新出现的问题。

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），https://doi.org/10.61092/iaea.hmxn-vw0a.

[2] 国际原子能机构《核电厂安全：设计》，国际原子能机构《安全标准丛书》第 SSR-2/1（Rev.1）号，国际原子能机构，维也纳（2016 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（Rev.1）号，国际原子能机构，维也纳（2016 年）。

[4] 国际原子能机构《制定和实施核电厂二级概率安全评定》，国际原子能机构《安全标准丛书》第 SSG-4 号，国际原子能机构，维也纳（2010 年）。（修订版准备中）

[5] 国际原子能机构《核电厂确定性安全分析》，国际原子能机构《安全标准丛书》第 SSG-2（Rev.1）号，国际原子能机构，维也纳（2019 年）。

[6] 国际原子能机构《核电厂设计中内部危害防护》，国际原子能机构《安全标准丛书》第 SSG-64 号，国际原子能机构，维也纳（2021 年）。

[7] 国际原子能机构《核装置地震安全的评价》，国际原子能机构《安全标准丛书》第 SSG-89 号，国际原子能机构，维也纳（2024 年）。

[8] 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）。

[9] 国际核安全咨询组《综合风险知情决策过程框架》，《国际核安全咨询组丛书》第 25 号，国际原子能机构，维也纳（2011 年）。

[10] 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）。

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

[12] 国际原子能机构《核装置安全目标的层次结构》，国际原子能机构《技术文件》第 1874 号，国际原子能机构，维也纳（2019 年）。

[13] 国际原子能机构《执行综合风险知情决策的考虑因素》，国际原子能机构《技术文件》第 1909 号，国际原子能机构，维也纳（2020 年）。

[14] 国际原子能机构《安全的领导和管理》，国际原子能机构《安全标准丛书》第 GSR Part 2 号，国际原子能机构，维也纳（2016 年），https://doi.org/10.61092/iaea.cq1k-j5z3.

[15] 国际原子能机构《核装置风险汇总》，国际原子能机构《技术文件》第 1983 号，国际原子能机构，维也纳（2021 年）。

[16] 国际原子能机构《多机组概率安全评定》，《技术报告丛书》第 110 号，国际原子能机构，维也纳（2023 年）。

[17] 国际原子能机构《核装置人的可靠性分析》，国际原子能机构，维也纳（准备中）。

[18] 美国核管制委员会《EPRI/NRC RES 火灾人的可靠性分析导则－最终报告》，第 NUREG-1921 号报告，电力研究所，加利福尼亚州帕洛阿尔托（2012 年）。

[19] 国际原子能机构《先进核电厂的安全相关术语》，国际原子能机构《技术文件》第 626 号，国际原子能机构，维也纳（1991 年）。

[20] 国际原子能机构《先进反应堆非能动安全系统可靠性评定方法进展》，国际原子能机构《技术文件》第 1752 号，国际原子能机构，维也纳（2014 年）。

[21] 经济合作与发展组织核能机构《用于概率风险分析的数字仪器仪表和控制系统可靠性评定的故障模式分类》，第 NEA/CSNI/R（2014）16 号报告，经济合作与发展组织/核能机构，巴黎（2015 年）。

[22] 国际原子能机构《核电厂安全仪器仪表和控制系统软件可靠性评定》，国际原子能组织《核能丛书》第 NP-T-3.27 号，国际原子能机构，维也纳（2018 年）。

[23] 国际原子能机构《核电厂仪器仪表和控制系统的设计》，国际原子能机构《安全标准丛书》第 SSG-39 号，国际原子能机构，维也纳（2016 年）。

[24] 国际原子能机构《放射性废物钻孔处置设施》，国际原子能机构《安全标准丛书》第 SSG-1 号，国际原子能机构，维也纳（2009 年）。

[25] 国际原子能机构《核设施非地震的外部事件设计》，国际原子能机构《安全标准丛书》第 SSG-68 号，国际原子能机构，维也纳（2021 年）。

[26] 国际原子能机构《核装置场址评价中与人为外部事件相关危害》，国际原子能机构《安全标准丛书》第 SSG-79 号，国际原子能机构，维也纳（2019 年）。

[27] 国际原子能机构《核装置场址评价中地震危害》，国际原子能机构《安全标准丛书》第 SSG-9（Rev.1）号，国际原子能机构，维也纳（2022 年）。

[28] 国际原子能机构《核装置场址评价中气象和水文危害》，国际原子能机构《安全标准丛书》第 SSG-18 号，国际原子能机构，维也纳（2011 年）。

[29] 国际原子能机构《现有核装置抗震安全评定方法》，《安全报告丛书》第 103 号，国际原子能机构，维也纳（2020 年）。

[30] 电力研究所《概率风险评定中用于分析的外部危害的识别：报告 1022997 的更新》，电力研究所，技术报告 3002005287，加利福尼亚州帕洛阿尔托（2015 年）。

[31] DECKER, K.，BRINKMAN, H.，“ASAMPSA_E 中考虑的外部危害清单”，ASAMP SA_E/WP21/D21.2/2017-41 技术报告，维也纳大学，维也纳（2016 年）。

[32] 国际原子能机构《运行中的核电对极端外部事件的脆弱性评定》，国际原子能机构《技术文件》第 1834 号，国际原子能机构，维也纳（2017 年）。

[33] 美国核管制委员会《EPRI/NRC-RES 核电设施火灾 PRA 方法 — 最终报告》，第 NUREG/CR 6850 号报告，（EPRI 1011989），电力研究所，加利福尼亚州帕洛阿尔托（2005 年）。

[34] 国际原子能机构、联合国环境规划署，《核电厂运行中的内外部危害防护》，国际原子能机构《安全标准丛书》第 SSG-77 号，国际原子能机构，维也纳（2022 年）。

[35] 国际原子能机构《地震事件的概率安全评定》，国际原子能机构《技术文件》第 1937 号，国际原子能机构，维也纳（2020 年）。

[36] 国际原子能机构《核装置场址评价中火山危害》，国际原子能机构《安全标准丛书》第 SSG-21 号，国际原子能机构，维也纳（2012 年）。

[37] 电力研究所《地震引发的内部火灾和水淹概率风险评定方法》，电力研究所，技术报告 3002012980，电力研究所，加利福尼亚州帕洛阿尔托（2018 年）。

[38] 国际原子能机构《CANDU 型反应堆核电站一级概率安全评定实践》，国际原子能机构《技术文件》第 1977 号，国际原子能机构，维也纳（2021 年）。

[39] 国际原子能机构《核电厂安全：调试和运行》，国际原子能机构《安全标准丛书》第 SSR-2/2（Rev.1）号，国际原子能机构，维也纳（2016 年）。

[40] 国际原子能机构《核电厂应用的全范围一级概率安全评定（PSA）的属性》，国际原子能机构《技术文件》第 1804 号，国际原子能机构，维也纳（2016 年）。

[41] 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）。

[42] 国际原子能机构《使用放射性物质设施退役的安全评定》，国际原子能机构《安全标准丛书》第 WS-G-5.2 号，国际原子能机构，维也纳（2008 年）。

[43] 国际原子能机构《核电厂定期安全评审》，国际原子能机构《安全标准丛书》第 SSG-25 号，国际原子能机构，维也纳（2013 年）。

[44] 国际原子能机构《核电厂管道系统在役风险知情视察：过程、现状、问题和发展》，国际原子能机构《核能丛书》第 NP-T-3.1 号，国际原子能机构，维也纳（2010 年）。

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

附件 I

外部危害的一般清单的示例

表 I-1 提供了潜在外部危害的一般清单的示例。它以 ASAMPSA_E 报告[I-1]为基础，其中包括核电厂概率安全评定（PSA）中要考虑的外部危害的详尽清单。更多细节见参考文献[I-1]。

表 I-1. 外部危害的一般清单的示例

代码	危害	危害定义和危害影响	接口和注释
		外部自然灾害	
		地震危害	
N1	振动地面运动	该危害的定义是振动地面运动对电厂及其周围所有土木构筑物和结构、系统和部件的同时影响。	需要考虑长周期地面运动和余震的影响。
N2	人类活动（石油、天然气或地下水开采、采石、矿井坍塌）引起或触发的地面振动	该危害的定义是振动地面运动对电厂及其周围所有土木构筑物和结构、系统和部件的同时影响。	
N3	地表断层（断层能力）	该危害的定义是同震断层破裂和地表位移对电厂的影响。它包括次级断层处的地表破裂。	
N4	液化，侧向扩散	该危害的定义是地基土抗剪强度的丧失及其对土木结构和地下设施（如管道或电缆槽）的影响。	
N5	强夯（地震导致土壤沉降）	该危害的定义是土壤沉降对土木结构和地下设施（如管道或电缆槽）的影响。它包括地震导致表面裂缝的影响。	

表 I-1. 外部危害的一般清单的示例（续）

代码	危害	危害定义和危害影响	接口和注释
N6	地震后地面永久性位移	该危害的定义是地震后应变排放导致永久性地面沉降或地面隆起对电厂的影响。	由其他地质过程导致地面沉降（N63）和地面隆起（N64）分别处理。
		水文灾害	
N7	海啸（地震、火山、水下滑坡、陨石撞击）	该危害的定义是由一系列水波导致洪水和波谷期间的水位下降。	地震（N1）、滑坡（N60、N61）和火山灾害（N68、N69）分别处理。
N8	山洪爆发：本地极端降雨导致洪水	该危害的定义是极端降雨造成的洪水对电厂造成的损坏。	雨水负载对构筑物造成的损坏分开处理（N25）。
N9	积雪融化导致洪水	该危害的定义是由季节性或快速融雪导致洪水造成的。	火山现象导致快速融雪分开处理（N68）。
N10	因场外降水导致洪水，以及流入现场的水（包括河流洪水）	该危害的定义是流向场址的洪水对电厂造成的损坏。	
N11	高地下水	该危害的定义是高地下水洪水对电厂造成的损坏。	
N12	由于滑坡、冰、原木或碎片造成的堵塞或火山活动阻塞河道（下游或上游）而导致洪水或低水位	该危害的定义是由下游河流蓄水或上游河流筑坝决堤产生洪水，以及上游筑坝造成的低水位。	
N13	河道因侵蚀或淤积、河流改道而导致洪水或低水位	该危害的定义是指由于河道变化或这种现象产生低水位而导致洪水。	侵蚀造成的沿海地区不稳定性分开处理（N23）。
N14	由火山、滑坡、雪崩或飞机坠毁产生内陆水域大浪导致洪水	该危害的定义是由内陆水域的大浪导致洪水。	由风力产生的波浪导致洪水分开处理（N19）。

表 I-1. 外部危害的一般清单的示例（续）

代码	危害	危害定义和危害影响	接口和注释
N15	水控制构筑物失效和河道围堵故障导致的洪水和波浪（水坝、堤坝或防洪堤失效）。	该危害的定义是由于水坝、堤坝或其他水容器的破坏（例如，由于水文或地震影响）导致洪水。	
N16	湖震	该危害的定义是封闭或部分封闭水体中的驻波导致水位波动造成的洪水。	湖震的影响可能会加剧其他灾害现象，如海啸或潮汐。
N17	孔	该危害的定义是由钻孔导致洪水（由涨潮或水管理导致波浪沿河流而上）。	
N18	海水水位：高潮、大潮	该危害的定义是由涨潮或大潮导致洪水。	
N19	海水水位、湖泊水位或河流水位：风生浪	该危害的定义是由风力产生的波浪导致洪水定义的，包括长周期、短周期和巨浪（反常波浪）。	
N20	海水水位：风暴潮	该危害的定义是风暴潮导致洪水。	
N21	海水水位、湖泊水位或河流水位：波浪/潮汐中断和码头等人造构筑物的影响	该危害的定义是由人造构筑物的水文效应引起或放大的洪水造成的。	
N22	盐水腐蚀	该危害的定义是盐水腐蚀对电厂的影响。	
N23	由于强水流侵蚀或沉积（海洋和河流）造成的沿海地区的不稳定性	该危害的定义是强水流侵蚀或沉积对电厂构筑物造成的损坏。	
N24	水下碎片	该危害的定义是影响终极散热器可用性的冷却水入口或出口的损坏或堵塞。这可能是由于水冲入的泥沙量造成的。	冰对取水构筑物的影响分开处理（N48）。

表 I-1. 外部危害的一般清单的示例（续）

代码	危害	危害定义和危害影响	接口和注释
		气象灾害	
N25	降水（雨或雪）、积雪	该危害的定义是极端雨雪对电厂造成的损坏，它包括由于雨雪负载对构筑物造成的损坏。	极端降雨（N8）或融雪（N9）造成的洪水分开处理。
N26	极端气温（高和低）	该危害的定义是极高温度（如通风功能停止）和低温（如管道冻结）对电厂的影响。	高或低水温（N28）或冰的影响分开处理。
N27	极端地面温度（高和低）	该危害的定义是高或低地面温度对电厂的影响（例如管道冻结）。	极端土壤霜冻的影响分开处理（N38）。
N28	冷却水（海、湖或河）温度（高和低）的极端值	该危害的定义是冷却水温度高或低对设备的影响。	冻结（表面冰：N48 冰障：N50）和冰冻（N49）分别处理。
N29	湿度（高和低），极端大气湿度	该危害的定义是湿气对安全相关设备和电子设备（仪器仪表和控制设备）功能的影响（例如，通过电气和电子设备中的液滴冷凝）。	
N30	极端气压	该危害的定义是高气压或低气压对设备的影响或可能影响压力表（如安全壳内）的快速压力变化，从而导致意外运行。	
N31	极端干旱：河流或湖泊水位低	该危害的定义是长期干旱，降低湖泊、河流和开放水域的水位，挑战冷却水或服务水的可用性。	高气温（N26）和高水温（N28）分别处理。地下水位的极端情况分开处理（N32）。
N32	地下水位低	该危害的定义是地下水位低对冷却水或供水的可用性构成挑战。	
N33	海水水位低	该危害的定义是根据低海水水位对电厂冷却功能的影响。	该危害包括低潮、海上风、高气压和海流异常变化的影响。

表 I-1. 外部危害的一般清单的示例（续）

代码	危害	危害定义和危害影响	接口和注释
N34	结冰、冰冻雾	该危害的定义是冻雨或雾对冰盖的影响。它包括结构（电线和开关站）的负载和冰对进气口的堵塞。	
N35	白霜、硬雾凇、软雾凇	该危害的定义是白霜的影响，包括对电线和开关站的影响，以及雾凇对进气口的堵塞。	
N36	冰雹	该危害的定义是极端冰雹对电厂造成的损坏。它包括冰雹撞击和冰雹负载造成的损坏。	冰雹融化导致洪水被雨雪融化导致洪水相结合（N8、N9）。对终极散热器的可能影响被认为受到地表冰灾的限制（N48）。
N37	永久冻土	该危害的定义是永久冻土融化和再冻结的影响。	
N38	反复发生的土壤霜冻	该危害的定义是土壤霜冻的影响（例如，对水管等浅层地下设施的影响）。	
N39	闪电（包括电磁干扰）	该危害的定义是闪电对电厂造成的损坏。这种影响可能是直接的，导致结构损坏或场外电源丧失，也可能是间接的，通过闪电导致电磁馈线火灾。	由闪电导致火灾受外部火灾（N73、M24）和内部火灾分析的限制。
N40	大风、风暴（包括飓风、热带气旋、台风）	该危害的定义是强风和风压的直接影响对电厂造成的损坏。	由于龙卷风（N41）的特殊特征，该危害不包括龙卷风。该危害不包括暴风雪、盐雾或沙尘暴的不同影响。然而，这些危害的风的影响也包括在内。风暴潮导致洪水分开处理（N20）。风吹飞射物造成的危害分开处理（N46）。

表 I-1. 外部危害的一般清单的示例（续）

代码	危害	危害定义和危害影响	接口和注释
N41	龙卷风	该危害的定义是龙卷风对电厂造成的损坏。它包括压差和旋转风的影响。	由于龙卷风在持续时间、风速和发生频率方面的特殊特征，该危害与其他强风（N40）不同。 风吹飞射物造成的损坏分开处理（N46）。
N42	水龙卷（龙卷风）	该危害的定义是旋转能量。水龙卷含有水蒸气（即不是液态形状）。	
N43	暴风雪	该危害的定义是风吹雪对电厂的影响。它包括电线和开关站外部高压绝缘的污染，以及进气口的堵塞。	暴风雪风压的影响被危害的大风（N40）所掩盖。雪负载分开处理（N25）。
N44	沙暴、尘暴	该危害的定义是风暴带来的沙子或灰尘对电厂的影响及其研磨作用。它包括电线和开关站外部高压绝缘的污染以及进气口的堵塞。	沙尘暴风压的影响被危害的大风（N40）所掩盖。
N45	盐雾、盐风暴	该危害的定义是一场风暴，涉及电厂结构的盐覆盖和大气中盐导致腐蚀。它包括电线和开关站外部高压绝缘的污染，以及盐颗粒导致电介质击穿。	沙尘暴风压的影响被危害的大风（N40）所掩盖。
N46	风吹碎片（外部飞射物）	该危害的定义是大风和龙卷风造成的风吹碎片的冲击造成的损坏。	典型的飞射物包括包层板、绝缘和非绝缘铝、脚手架板、脚手架杆、树木和汽车。
N47	雪崩	该危害的定义是雪崩对电厂的影响。	雪崩可能由大雪或融雪导致。
N48	河、湖、海表面冰	该危害的定义是影响终极散热器可用性的漂流冰或厚表面冰对冷却水入口或出口的损坏或堵塞。	冰冻（N49）和冰障（N50）分别处理。

表 I-1. 外部危害的一般清单的示例（续）

代码	危害	危害定义和危害影响	接口和注释
N49	水内冰	该危害的定义是冰对冷却水入口或河流筑坝的影响。	
N50	冰障	该危害的定义是冰障对电厂的影响（例如，堵塞取水口）。	下游冰障导致洪水分开处理（N12）。
N51	雾	该危害的定义是薄雾对电厂、电线和开关站的影响。它包括降低场址的可见性。	
		地外灾害	
N52	太阳耀斑、太阳风暴（空间天气）：地磁风暴	该危害的定义是电磁干扰和地面电网故障造成的电气和电子设备故障和损坏。	
N72	陨石坠落	该危害的定义是陨石撞击（直接撞击、冲击波、撞击导致振动、火灾）对电厂造成的损坏。	陨石撞击导致海啸、导致洪水分开处理（N7）。
		生物危害	
N53	海洋/河流/湖泊生长（海藻、藻类）、生物污染	该危害的定义是藻类、海藻或细菌的过度生长影响了终极散热器冷却水的可用性。	
N54	甲壳类或软体动物生长（虾、蛤、贻贝、贝壳）	该危害的定义是结壳生物堵塞了进水口或出水口，影响了终极散热器冷却水的供应。	
N55	鱼、水母	该危害的定义是由于冷却池中异常数量的鱼/水母或异常鱼类数量堵塞了取水口，导致终极散热器不可用。	海藻堵塞（N53）和生物漂浮物（N58）分别处理。
N56	蜂群（昆虫、鸟）或树叶	该危害的定义是由于鸟类堵塞进气口或过滤器中的树叶或昆虫堵塞通风系统而对电厂造成的损坏。它包括堵塞应急柴油发电机的进气口。	
N57	啮齿动物和其他动物侵扰	该危害的定义是啮齿动物（大鼠、小鼠）对电缆或电线的损坏以及穴居哺乳动物对结构的破坏。	

表 I-1. 外部危害的一般清单的示例（续）

代码	危害	危害定义和危害影响	接口和注释
N58	生物漂浮物（如木头、树叶、草）	危害的定义是由于大量漂浮物的积累而损坏或堵塞冷却水入口或出口，影响终极散热器的可用性。	
N59	微生物腐蚀	该危害的定义是微生物腐蚀对电厂的损坏。	
		地质灾害	
N60	陆上斜坡不稳定（滑坡、落石，包括气象和地震导致事件）	该危害的定义是滑坡或落石对电厂的影响，包括冷却水入口或出口可能堵塞，影响终极散热器的可用性。	因溪流堵塞（N12）或在海洋或湖泊中引发海啸（N7）而导致洪水的大规模运动的影响分开处理。
N61	水下滑坡、重力流（包括地震导致事件）	该危害的定义是水下滑坡对电厂的影响。	水下滑坡可能是由水面上的原因造成的，如长时间的强降水。水下侵蚀（N23）和滑坡导致海啸（N7）分别处理。
N62	泥石流、泥石流（包括地震导致事件）	该危害的定义是泥石流或泥流对电厂的影响。影响可能包括冷却水入口或出口构筑物堵塞。	火山泥流灾害在火山灾害（N68）中处理。
N63	地面沉降（采矿、地下水开采、石油/天然气生产造成的自然或人为沉降）	该危害的定义是地面沉降对电厂的影响。	
N64	地面隆起	该危害的定义是地面隆起对设备的影响。	
N65	岩溶，可溶岩石（石灰石、石膏、硬石膏、石盐）的渗出	该危害的定义是化学侵蚀导致裂缝、天坑、地下溪流和洞穴对电厂的影响。	
N66	天坑（天然洞穴和人造洞穴的坍塌）	该危害的定义是地下坍塌造成的天坑对电厂的影响。	

表 I-1. 外部危害的一般清单的示例（续）

代码	危害	危害定义和危害影响	接口和注释
N67	不稳定土壤（如快速粘土）	该危害的定义是不稳定土壤对电厂的影响。	
N68	火山灾害：火山中心附近发生的现象	该危害的定义是根据对以下设备的影响： 火山口开口；飞射物发射；余波；火山碎屑物质，如灰烬、火山灰、火山砾或浮石；火山碎屑流；熔岩流；泥石流、滑坡和边坡破坏；融雪引起的火山泥流、射气岩浆和洪水；空气冲击和闪电；气体排放（包括“发光雪崩”）；地面变形；地热和地下水异常；火山活动导致的森林大火。	火山现象种类繁多，需要对这些现象进行分开处理。地震（N1）和火山活动导致海啸（N7）分开处理。
N69	火山灾害：影响延伸到远离火山中心的地区	该危害的定义是火山现象（如火山灰沉降物）对电厂的影响。	由火山活动导致地震（N1）和海啸（N7）被分开处理。
N70	甲烷渗出	该危害的定义是从土壤或岩石中渗出的甲烷对电厂的影响。	
N71	天然辐射	该危害的定义是天然辐射对电厂的影响。	
		天然火灾	
N73	森林火灾、野火、燃烧的草皮或泥炭	该危害的定义是由于火灾或受烟雾和有毒气体排放影响的运行人员行为对电厂造成的损坏或场外电源丧失。它包括由于火花点燃其他火灾和燃烧气体导致危害。	该危害可能是极端气象条件（高温、干旱或风暴）的影响。人类行动导致火灾分开处理（M24）。

表 I-1. 外部危害的一般清单的示例（续）

代码	危害	危害定义和危害影响	接口和注释
		人为外部危害	
		工业事故	
M1	工业事故：爆炸	该危害的定义是固态物质、液体或气体爆炸（爆燃或爆震）对电厂造成的损坏，导致电厂损坏、场外电源丧失或影响运行人员行动。损坏可能是由于压力撞击或飞射物撞击造成的。	该危害与化学品或燃料贮存设施（炼油厂、化电厂、贮存仓库、其他核设施）最为相关。 与运输相关的爆炸（M11）和管道事故（M13）分开处理。 工业事故导致火灾分开处理（M24）。
M2	工业事故：化学品排放（爆炸性、易燃性、窒息性、毒性、腐蚀性或放射性物质）	该危害的定义是工业电厂排放物的影响，这些排放物会对电厂造成损坏，或者运行人员的行为会受到爆炸性、易燃性、窒息性、毒性、腐蚀性或放射性物质排放的影响。该危害还涉及向水中排放化学物质对电厂的影响（例如水质下降）。	该危害与化学品或燃料贮存设施（炼油厂、化工厂、贮存仓库、其他核设施）最为相关。 运输事故（M12）或管道事故（M14）造成的危害分开处理。
M3	高能旋转设备飞射物	该危害的定义是高能旋转设备产生的飞射物的影响。	
		军事事故	
M4	军事设施（永久和临时）:爆炸、射弹、导弹和火灾	该危害的定义是军事设施中事故的影响，如爆炸、射弹产生（弹片）或导弹。	军事设施排放的化学品分开处理（M5）。 来自军事设施的火灾按人为/技术活动导致火灾危害处理（M24）。

表 I-1. 外部危害的一般清单的示例（续）

代码	危害	危害定义和危害影响	接口和注释
M5	军事设施（永久性和临时性）：化学物质排放（爆炸性、易燃性、窒息性、毒性、腐蚀性或放射性物质）	该危害的定义是军事设施排放的影响，导致受爆炸性、易燃性、窒息性、毒性、腐蚀性或放射性物质排放影响的电厂或运行人员行动受损。	
M6	军事行动	该危害的定义是军事行动对电厂造成的损坏。	军事行动导致爆炸和火灾应当被视为最低限度。
		交通事故	
M7	船舶事故：直接撞击	该危害的定义是船舶的直接撞击。	与终极散热器的进水口构筑物和部件的碰撞分开处理（M8）。危害不包括与船舶事故相关的排放后果（爆炸、污染、进气口堵塞或有毒气体排放）。这些危害分别处理（M9、M11）。
M8	与进水口和最终散热部件（船舶、浮桥、渔网）的碰撞	该危害的定义是碰撞（如与船舶、浮桥、渔网的碰撞）对取水口和终极散热器结构的损坏或堵塞。	危害不包括与船舶事故相关的排放后果（爆炸、污染、进气口堵塞或有毒气体排放）。这些危害分别处理（M9、M11）。
M9	船舶事故：固体或流体（非气体）排放	该危害的定义是船舶排放到水中的杂质（如溢油或腐蚀性液体）对进水口和终极散热器结构的损坏或堵塞，这些杂质可能影响冷却水的可用性或质量及其热交换能力。	
M10	地面运输事故：直接影响	该危害的定义是场外火车、货车和道路车辆的直接影响。	危害不包括与运输事故相关的排放后果（爆炸、污染、进气口堵塞或有毒气体排放）。这些危害分别处理（M11、M12）。

表 I-1. 外部危害的一般清单的示例（续）

代码	危害	危害定义和危害影响	接口和注释
M11	交通事故：爆炸、火灾	该危害的定义是地面运输事故后爆炸或海洋、湖泊或河流运输事故对电厂造成的损坏。损坏可能是由于压力撞击或飞射物撞击造成的。	其他危害的后果（不同的主要原因）。飞机坠毁（M15、M16）或管道事故（M13）造成的危害分开处理。化学品排放的毒性效应分开处理（M12）。
M12	运输事故：化学品泄漏（爆炸性、易燃性、窒息性、毒性、腐蚀性或放射性物质）	该危害的定义是地面运输事故后或由于海洋、湖泊或河流运输事故导致化学品排放的影响，这些事故从外部和内部影响电厂，破坏或削弱安全相关系统和运行人员行动。排放可能源于运输事故、运输物质的溢出或泄漏。	
		管道事故	
M13	场外管道事故：爆炸、火灾	该危害的定义是场外管道事故（包括泵站）后爆炸（爆燃或爆炸）对电厂造成的损坏。损坏可能是由于压力撞击或飞射物撞击造成的。	化学品排放的影响分开处理（M14）。
M14	场外管道事故：化学品排放	该危害的定义是管道事故（包括泵站）后化学物质排放的影响，这些事故从外部和内部影响电厂，破坏或削弱安全相关系统和运行人员行动。	管道事故的爆炸影响分开处理（M13）。
		飞机事故	
M15	飞机坠毁：机场区域	该危害的定义是异常飞行导致坠毁对电厂的损坏。 直接撞击、爆炸、飞射物、火灾（煤油）、烟雾（有毒物质）和导致振动都可能造成损坏。	危害取决于飞行频率、跑道特征以及飞机的类型和特征。飞机可以是商用的、私人的或军用的。

表 I-1. 外部危害的一般清单的示例（续）

代码	危害	危害定义和危害影响	接口和注释
M16	飞机坠毁：空中交通走廊和飞行区域（军事/民用/农业）	该危害的定义是异常飞行导致坠毁对电厂的损坏。直接撞击、爆炸、飞射物、火灾（煤油）、烟雾（有毒物质）和导致振动都可能造成损坏。	危害取决于飞行频率、空中交通走廊的特点以及飞机的类型和特点。飞机可以是商用的、私人的或军用的。
M17	卫星坠毁	该危害的定义是卫星撞击对电厂造成的损坏。直接撞击、导致振动或冲击波都可能导致损坏。	
		其他人为外部危害	
M18	挖掘及厂房工程	该危害的定义是场址区域外的挖掘和建造工作对电厂的影响，包括对埋在地下的电缆和管道的破坏性工作，这可能导致地下供应的中断或爆炸性、易燃性、窒息性、毒性或腐蚀性物质的排放。	
M19	场外电网的不稳定性	该危害的定义是场外对电网和开关站的运行造成的干扰影响。它包括导致电压浪涌的外部电网干扰。	
M20	户外开关设备和电力线路高压绝缘的工业污染	该危害的定义是工业污染物（如灰尘或化学物质排放物）对室外开关设备中高压绝缘的影响。	
M21	场外来源的电磁干扰、射频干扰或干扰	该危害的定义是人类感应磁场或电场的影响以及可能导致安全相关设备或仪器仪表故障或损坏的放射性磁干扰。	这类领域的主要示例是雷达、无线电和移动电话系统，或高压电气开关装设备的启动。
M22	高压涡流入地（场外源）	该危害的定义是地下金属接地部件的腐蚀和接地问题。	

表 I-1. 外部危害的一般清单的示例（续）

代码	危害	危害定义和危害影响	接口和注释
M23	洪水：水闸事件或水坝的失效或管理不善	该危害的定义是由人为损坏、故障或控水构筑物管理不善导致高水位和水波对电厂造成的损坏。	由于自然事件（N15）导致控水构筑物故障（大坝失效），灾害可能被洪水灾害所包围。
M24	人为/技术行动导致火灾	该危害的定义是人类引发森林、荒地或草原火灾或城市地区火灾对电厂造成的损坏或场外电源丧失。它包括由点燃其他火灾的火花、烟雾、火的燃烧气体和热量（热流）导致危害。	火灾可能由工业事故或业余活动导致。
M25	场内重型运输的直接影响	该危害的定义是场内但厂房外重型运输的直接影响对电厂造成的损坏。这也包括安全壳外部维护平台的运输。	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。
M26	场内爆炸	该危害的定义是场内但厂房外固态物质或气体云爆炸（爆燃或爆炸）对电厂造成的损坏。包括现场管道破裂后的爆炸。损坏可能是由于压力撞击或飞射物撞击造成的。	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。
M27	场内火灾	该危害的定义是由于影响场址的火灾、源自场外的火灾或地震等其他自然事件的影响而对电厂造成的损坏。	
M28	场内化学物质排放：爆炸性、易燃性、窒息性	该危害的定义是影响电厂外部和内部、破坏或削弱安全相关系统和运行人员行动的化学物质排放的效果。	这些排放可能源于电厂内部的加工事故或贮存在现场但在电厂厂房外部的物质泄漏。作为内部危害概率安全评定的一部分，对贮存在厂房内的物质排放的化学物质进行分析。

表 I-1. 外部危害的一般清单的示例（续）

代码	危害	危害定义和危害影响	接口和注释
M29	场内管道事故：爆炸火灾	该危害的定义是场内管道事故后爆炸（爆燃或爆炸）或火灾对电厂造成的损坏。损坏可能是由于压力撞击或飞射物撞击造成的。	场内管道事故后化学品排放的影响分开处理。场外排放的爆炸效应分开处理。
M30	场内管道事故：化学物质排放（爆炸性、易燃性、窒息性、毒性、腐蚀性或放射性物质）	该危害的定义是场内管道事故后化学物质排放的影响，这些事故从外部和内部影响电厂，破坏或削弱安全相关系统和运行人员行动。	其他危害的后果（不同的主要原因）。管道事故的爆炸影响分开处理。
M31	场内开挖及厂房工程	该危害的定义是场址区域内挖掘工程和民用厂房对电厂的影响，包括对埋在地下的电缆和管道的破坏性工程。	
M32	场内电网的稳定性	该危害的定义是从电厂内部操纵开关站或电网产生的电流波动的影响。	
M33	来自现场源的电磁干扰、射频干扰或干扰	该危害的定义是人类感应磁场或电场对电厂的影响，以及可能导致安全相关设备或仪器故障或损坏的放射性磁干扰。	这些领域的主要示例是无线电通信和移动电话系统领域。
M34	高压涡流入地（现场源）	该危害的定义是地下金属接地部件的腐蚀和接地问题。	
M35	场内储罐水淹	该危害的定义是场内储罐故障导致水淹影响。	
M36	来自场内其他机组的飞射物	该危害的定义是场内另一个装置或机组的高能旋转设备产生的飞射物对电厂造成的损坏。	
M37	内部火势从场内其他机组传播	该危害的定义是源自场内另一个机组的火灾对电厂的影响。	外部火灾分开处理。由其他外部危害的次要影响导致火灾被视为这些危害的一部分。

表 I-1. 外部危害的一般清单的示例（续）

代码	危害	危害定义和危害影响	接口和注释
M38	内部水淹和恶劣环境从场内其他机组传播	该危害的定义是其机组的水扩散效应对电厂造成的损坏。	
M39	场内其他机组事故的影响	该危害的定义是爆炸（如氢气）或场内其他机组的放射性排放对电厂造成的损坏。	

注： 危害清单改编自参考文献[I-1]。危害的编号保留了参考文献[I-1]内容，并根据本“安全导则”使用的自然和人类引发危害类别进行了调整。源自厂房内部的内部危害不包括在表中。I&C－仪器仪表和控制。SSC－结构、系统和部件。UHS－终极散热器。

附件 I 参考文献

[I-1] DECKER, K.，BRINKMAN, H.，“ASAMPSA_E 中考虑的外部危害清单”，ASAMP SA_E/WP21/D21.2/2017-41 技术报告，维也纳大学，维也纳（2016 年）。

附件 II

火灾事件树和地震事件树的示例

使用事件树技术分析火灾缓解和传播的说明

II-1. 图 II-1 所示的火灾事件树示例包括从火灾开始的相关特点。火灾的早期和晚期探测是有区别的，因为这些情况与控制和扑灭火灾的不同概率有关联。对于火的传播，房间是否关闭以及关闭到什么程度是相关的。进一步的建模解决了可用的消防设备，考虑了灭火手段对安全相关物项可能造成的损坏。图 II-1 说明了如何使用事件树技术来分析火灾缓解和传播。

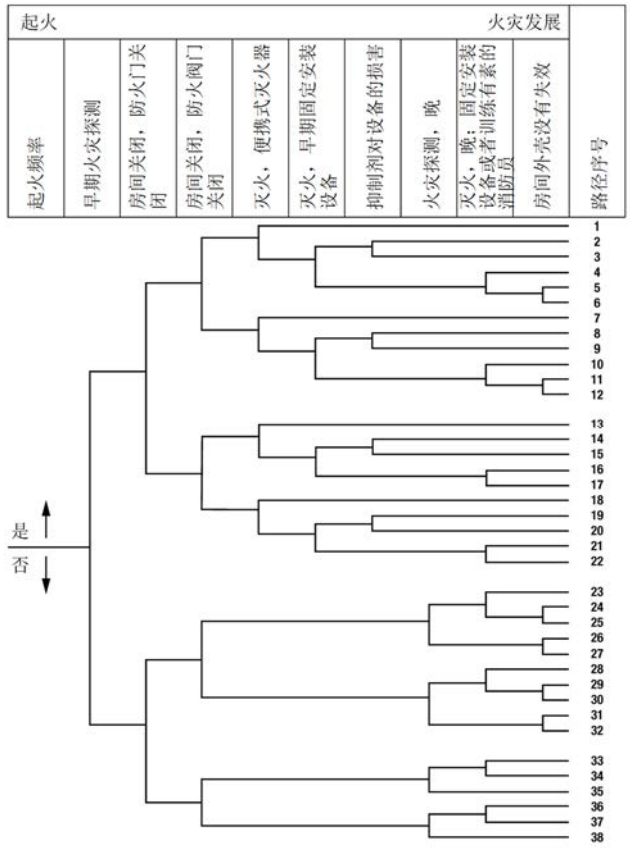

图 II-1. 一般火灾事件树的示例。

使用事件树技术识别地震导致始发事件的说明

II-2.　图 II-2 说明了如何使用事件树技术来模拟地震导致始发事件的不同后果。

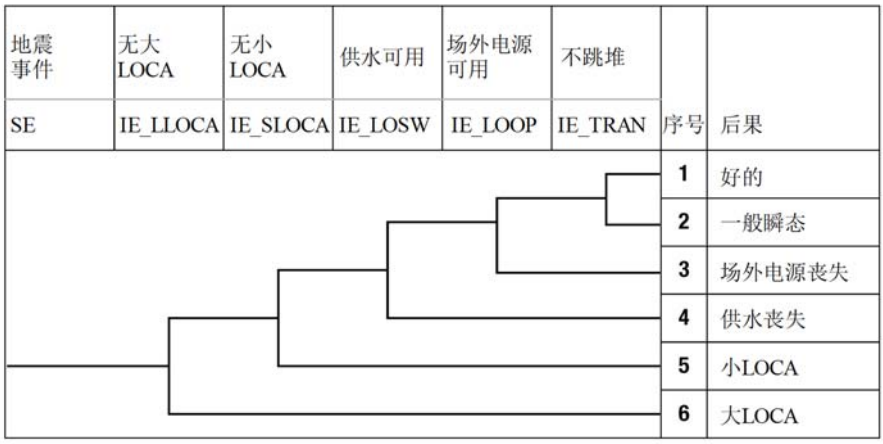

图 II-2.　地震导致始发事件建模的事件树示例。LOCA－冷却剂丧失事故。IE－始发事件。

附件 III

关闭状态下概率安全评定支持信息

电厂运行状态和相关始发事件示例

III-1. 在德国 SWR 69 型沸水堆[III-1]概率安全评定框架内对关闭状态进行了概率评定。参考文献[III-2]提供了压水堆电厂的类似示例。

III-2. 在参考文献[III-1]基础上，本附件提供的信息说明了如何指定电厂运行状态，以及如何将始发事件与各种电厂运行状态联系起来。为了描述系统相关状态和实物状态的变化，大修被分为不同的状态（见图 III-1 和表 III-1）。以这样的方式选择状态，即系统可用性和实物状态尽可能恒定。通常，在大修期间（状态 3-1－3-7），应急电源的两个电气冗余中的一个、余热排出系统的 4 个通道中的两个和应急备用系统的两个通道中的一个是可用的。在状态 3－4 中，大部分维护工作都在进行，反应堆厂房集水坑中的泄漏回流系统需要可用。

III-3. 对德国的运行经验进行了详细评定，以确定可能导致始发事件或可能影响关闭状态下事故控制的事件。除了评定德国的运行经验外，还评定了国际关闭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也被用作识别始发事件的基础[III-5、III-6]。

III-5. 始发事件的识别及其对可能发生的电厂运行状态的分配导致了表 III-2 所示的矩阵。表 III-2 标有“X”的机组格内表示始发事件可能发生在该电厂运行状态下。正如第 9.13 段所指出的，根据国家概率安全目标或标准，决定列入哪些最终状态。

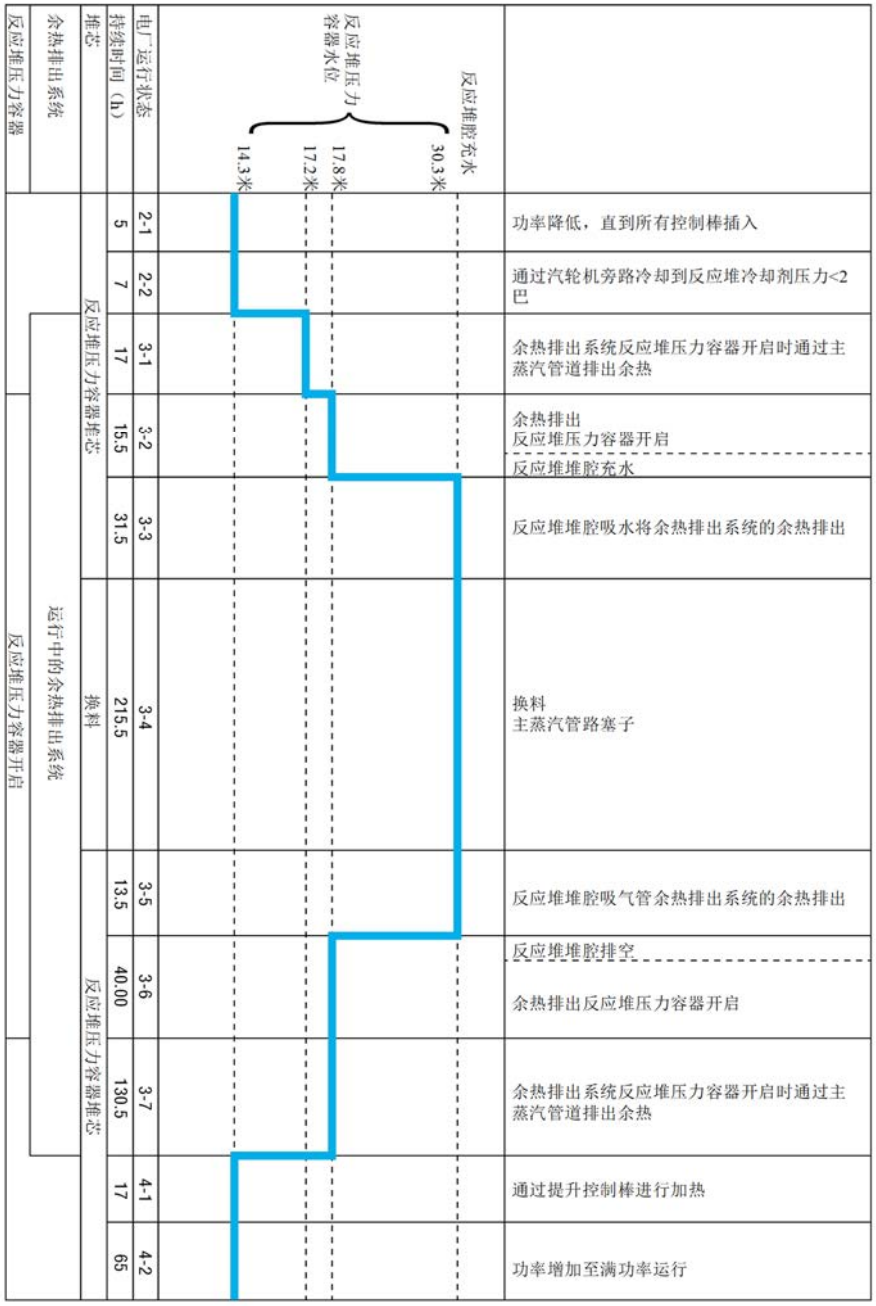

图 III-1.　关闭期间的反应堆冷却剂液位。

表 III-1. 压水堆电厂大修期间电厂运行状态

电厂运行状态		电厂运行状态的表征
关闭	2-1	功率降低，直到所有控制棒插入
	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，通过余热排出系统注入提高主蒸汽管道以上反应堆水位
大修	3-1	通过带有余热排出系统的主蒸汽管道排出余热，反应堆压力容器关闭，反应堆冷却剂温度130－150℃
	3-2	通过带有余热排出系统的主蒸汽管道排出余热，反应堆压力容器开启，反应堆冷却剂温度<40℃，反应堆腔密封衬里的安装，反应堆堆腔水淹
	3-3	反应堆腔水淹，余热排出系统通过反应堆堆腔吸入管线将余热排出，打开换料口，在主蒸汽管路中插入封堵
	3-4	换料，余热排出系统通过反应堆堆腔吸入管线将余热排出
	3-5	拆除主蒸汽管道中的封堵，关闭换料口，余热排出系统通过反应堆堆腔吸入管线将余热排出
	3-6	排空反应堆堆腔，余热排出系统通过反应堆堆腔吸入管线将余热排出，拆除反应堆堆腔密封衬板
	3-7	反应堆压力容器关闭，通过余热排出系统的主蒸汽管道排出余热
重新启动	4-1	关闭余热排出系统，在主蒸汽管道以下的反应堆中降低液位，抽出控制棒进行加热
	4-2	汽轮机旁路运行，运行汽轮发电机，同步，功率增加至满功率运行

表 III-2. 压水堆电厂大修期间始发事件（分别显示临界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	关闭		大修							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
		瞬变										
T1	主散热器丧失	X	X									X
T2	优选功率丧失	X	X	X	X	X	X	X	X	X	X	X
T3	主给水丧失	X	X									X
T4	主给水和主散热器丧失	X	X									X
T5	安全阀未关闭	X	X								X	X
T6	抑制池泄漏		X		X							
T7	主给水系统反应堆压力容器的超给水	X	X									X
T8	带有余热排出系统的反应堆压力容器的超给水		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	无紧急停堆的预期瞬变	X									X	X

表 III-2. 压水堆电厂大修期间始发事件（分别显示临界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										
		关闭		大修							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
	冷却剂丧失事故											
S1	安全壳内反应堆压力容器泄漏：											
S1.1	由于管道破裂：											
S1.1.1	上堆芯（A喷嘴）					X	X	X				
S1.1.2	下堆芯（L型喷嘴）					X	X	X				
S1.2	由于以下期间的人为错误：											
S1.2.1	主蒸汽管道阀门的视察						X					
S1.2.2	堆芯喷淋和一回路补给系统中阀门的视察						X					
S1.2.3	循环泵轴的拉动						X					
S1.2.4	控制棒驱动设备的视察						X					
S1.2.5	堆芯中子通量探测器的变化						X					
S2	余热排出系统泄漏			X	X	X	X	X	X	X		

表 III-2. 压水堆电厂大修期间始发事件（分别显示临界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	关闭		大修							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
S3	反应堆堆腔密封衬里泄漏				X	X	X	X	X			
S4	泄漏到连接的系统中：											
S4.1	反应堆压力容器液位控制失效			X	X				X	X		
S4.2	余热排出过程中安全阀的开启			X	X	X		X	X	X		
S4.3	余热排出换热器泄漏			X	X	X	X	X	X	X		
S5	乏燃料水池泄漏			X	X	X	X	X	X	X		
		火灾和内部水淹										
B1	安全壳内火灾	X	X	X	X	X	X	X	X	X	X	X
B2	安全壳外火灾	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	控制棒的错误抽出						X					
K2	控制棒错误移除						X					
K3	燃料装载错误						X					
		重物跌落										
H1	燃料元件跌落						X					
H2	重物跌落			X	X	X	X	X	X	X		

III-6. 压水堆电厂的相应信息见参考文献[III-2]并在表 III-3 和表 III-4 进行了总结。表 III-3 显示了需要区分的电厂运行状态。表 III-4 显示了在不同电厂运行状态下要考虑的始发事件。这份清单是基于对国家和国际运行经验的分析。

表 III-3. 压水堆电厂大修两周电厂运行状态

序号	实物工况/系统特点的变化
(1)A0	降低功率以调部分次临界热/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	通过蒸汽发生器关闭至一回路系统压力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	一回路系统冷却至减压冷/余热排出系统在120℃时启动，蓄能器和高压泵断开
(1)B2	液位降低到中回路，中回路运行/堆芯在反应堆压力容器内，一回路系统压力紧密关闭
(1)C	打开反应堆压力容器上盖，反应堆压力容器内的中回路运行/堆芯，一回路系统不是压力密封关闭的，冷却水池和燃料水池之间的换料舱口关闭
(1)D	反应堆堆腔注水，反应堆压力容器内燃料元件/堆芯全部或部分卸载，换料舱口打开
E	反应堆堆腔排空，反应堆压力容器/堆芯完全卸载，换料舱口关闭，工作在下边缘回路水平进行
(2)D	反应堆堆腔的再充水，燃料元件/堆芯全部或部分装入反应堆压力容器，换料舱口打开
(2)C	液位降至中回路，反应堆压力容器内的反应堆压力容器上盖/堆芯关闭，一回路系统未密封关闭，换料舱口关闭
(2)B2	反应堆压力容器内一回路系统/堆芯的排空和再填水，一回路系统压力密闭
(2)B1	一回路冷却剂泵/所有反应堆保护系统可用的一回路系统加热
(2)A1	冷却剂的减硼和使反应堆达到临界状态/撤回控制棒和/或减硼
(2)A0	功率增加到规定水平/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) 表示关闭期间的电厂运行状态；(2) 表示重启期间的电厂运行状态。

表 III-4. 压水堆电厂在关闭状态期间始发事件（分别显示临界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												
	A0	A1	B1	B2	C	D	E	D	C	B2	B1	A1	A0
	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			
	瞬变												
优选电源丧失—外部	X	X	X	X	X	X	X	X	X	X	X	X	X
优选电源丧失—内部						X	X	X					
在不损失主供热的情况下丧失主给水	X	X										X	X
在不损失主给水的情况下丧失主散热器	X	X										X	X
主给水和主散热器丧失	X	X										X	X
安全壳外主蒸汽管道泄漏	X	X										X	X
安全壳内主蒸汽管道泄漏	X	X										X	X
汽轮机厂房给水管道泄漏	X	X										X	X
安全壳内给水管道泄漏，不可隔离	X	X										X	X
余热排出丧失，原因是：													
— 液位降低错误				X					X				
— 余热排出通道运行故障			X	X	X	X		X	X	X			
意外激活应急堆芯冷却系统信号				X									

表 III-4. 压水堆电厂在关闭状态期间始发事件**（分别显示临界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												
	A0	A1	B1	B2	C	D	E	D	C	B2	B1	A1	A0
	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			
冷却剂丧失事故													
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
稳压器安全阀意外开启	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
维护故障导致P-bdV意外开路		X	X	X						X	X	X	
非场内电力丧失时意外打开P-bdV	X	X	X								X	X	X
汽轮机跳机后意外开启P-bdV	X	X	X								X	X	X
蒸汽发生器管泄漏	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			
环形余热排出系统泄漏			X	X	X	X	X	X	X	X			

表 III-4. 压水堆电厂在关闭状态期间始发事件（分别显示临界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												
	A0	A1	B1	B2	C	D	E	D	C	B2	B1	A1	A0
	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			
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					
泄漏到附属系统			X	X	X	X	X	X	X	X			
	意外减硼												
从含有未硼化水系统泄漏：													
— 蒸汽发生器管泄漏			X	X	X	X	X	X	X	X	X		
— 余热排出热交换器泄漏			X	X	X	X	X	X	X	X	X		
— 轴承密封泄漏			X	X	X	X	X	X	X	X	X		
— 一回路系统意外注入			X	X	X	X	X	X	X	X	X		
余热排出系统中的意外未硼化水		X	X	X	X	X	X	X	X	X			
去污工作中硼的稀释									X				
提高液位过程中硼的稀释										X			
关闭时硼化失效		X											
所有一回路冷却剂泵丧失后关闭时意外硼稀释												X	

注：P-bdV－稳压器排污阀。

特定系统建模需求示例

III-7. 参考文献[III-7]第 III-8－III-10 段所述示例的主要和几乎唯一来源。

III-8. 特定系统可能需要对关闭状态进行特定建模。例如，燃料水池冷却系统可能不包括在分析中功率运行，但在关闭状态下可能很重要。可能还需要考虑仅在大修期间使用的余热排出系统的某些运行状态。系统模式必须反映运行状态和特定系统排列。成功标准，例如所需的特定系统的 n 通道中的 k 列，对于关闭状态可能不太严格，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。为了防止意外启动，在关闭状态下可以旁路系统的自动启动功能。例如，安全注入系统可能在自动启动模式下被阻塞，以防止在关闭期间驱动。因此，需要改变这些系统的故障树中的控制逻辑，以反映必要时必须手动启动系统的事实。还需要制定相关人类互动的模式。

III-9. 在大修期间，由于大修后正在进行活动，计入功率运行分析的手动恢复运行可能是不可能的。例如，虽然低压系统的交叉连接可能是功率运行期间的适当运行，但这可能会被锁定，或者系统通道可能会在大修期间完全禁用。因此，如果该类的动作包含在功率运行的故障树中，则需要对其进行修改以进行关闭评价。总之，需要针对每个电厂运行状态评审来自功率运行概率安全评定的适合于关闭状态概率安全评定的每个故障树，以确定该电厂运行状态是否存在可能对故障树结构的逻辑产生影响的任何特点。

III-10. 大修期间各种系统可用性的变化使系统建模任务变得复杂。在某些电厂运行状态下，某些系统或部分系统可能不可用。此外，由基准事件表示的部件故障的概率可能会改变。大多数概率安全评定软件包都基于“快速割集算法”，该算法生成并存储最小割集的方程。最小割集的分析可以在几个级别上进行：特定故障树门、单一事件树序列或特定后果（每个事件树序列可以被分配一个或多个后果（例如，电厂损坏状态））。分析案例可以指定一个“边界条件集”，其中包括需要应当用于模式的值规范或修改的清单。边界条件集可以包括逻辑开关的真/假设置、基准事件和故障树门的概率设置、基准事件和故障树门的真/假状态设置以及参数值的设置。这对于根据电厂运行状态对具有不同变化的相同基本模式进行分析非常有用。当然，也可以在不使用逻辑开关的情况下执行分析，但是对于每个边界条

件集，不同的单一故障树模式被添加到关闭状态的完整概率安全评定模式中，如果必须进行修改，这将使建模和评审所需的工作变得复杂，因为要考虑不同故障树模式的数量。

关闭状态下与概率安全评定相关的前起始因子人因故障事件和人为引发起始因子识别方法

III-11. 由于对人员在关闭期间可能采取的所有措施进行详细分析是不可行的，因此前起始因子行动的有效筛选步骤是必不可少的。这一步骤的结果将是一份行动清单，其中列明哪些行动需要进行定性评价，哪些行动需要进行估计，哪些行动需要进行详细的定量分析。第 III-12－III-18 段所述方法见参考文献[III-6]。

III-12. 筛选方法的基础是标准大修计划的主要步骤和任务的电厂特定清单。显然，该清单与为关闭状态的概率安全评定选择的电厂运行状态之间存在密切关系。对于沸水堆，该清单通常包括 30 个步骤或任务。参考文献[III-6]列举了以下主要步骤和任务：

— 实施降功率；
— 开始与电厂关闭和系统隔离相关的试验；
— 发电机与电网解列；
— 继续降功率，直到开始去除余热；
— 为燃料转移的打开安全壳；
— 打开反应堆压力容器；
— 安装补偿器，用于反应堆堆腔充水；
— 开始注水；
— 开展反应堆压力容器活动；
— 拆下蒸汽干燥机；
— 设置插头和面板；
— 在冗余通道上工作；
— 系统和部件方面的工作；
— 进行啜吸试验；
— 更换燃料元件；

— 拆卸并重新安装给水喷淋器；
— 拆下封堵和板；
— 安装蒸汽干燥机；
— 排空堆腔水；
— 拆下补偿器；
— 关闭反应堆压力容器；
— 关闭安全壳；
— 进行与启动相关的试验；
— 升功率；
— 发电机并网；
— 提升至功率运行。

III-13. 对于此清单中的元素，对工作环境和执行的任务进行评定，以识别潜在的人为错误和后果。然后判断每个潜在误差的显著性。在确定可能的后果时，要区分部件或系统部件的不可用性和始发事件。

III-14. 在第一种情况下，评定如何检测故障，在哪个时间间隔会导致不可用或潜在故障，以及在哪个始发事件中不可用或潜在故障会变得明显。最后，描述了可能的对策和后果。

III-15. 在第二种情况下，始发事件被分类（例如冷却剂丧失事故）。再次描述了可能的对策和后果。

III-16. 这种筛选分析的一个重要目标是以透明和系统的方法准备一份包含全部筛选结果的表格，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的分析，可以使用第 5 部分描述的人的可靠性分析方法进行。

III-18. 作为中间情况，对于性质相似的始发事件组（例如泄漏位置在堆芯上方的冷却剂丧失事故），对整体故障概率的粗略估计就足够了。

作为沸水堆电厂关闭状态概率安全评定结果的大修风险概况示例

III-19. 在参考文献[III-8]，概述了沸水堆电厂关闭状态的概率安全评定结果。规定了 6 种电厂运行状态：

(1) 电厂运行状态 1：功率运行和启动，压力从额定工况（71 千克/平方厘米）到 35 千克/平方厘米，热功率不大于 15%。

(2) 电厂运行状态 2：压力从 35 千克/平方厘米到 10 千克/平方厘米的启动和热停堆。

(3) 电厂运行状态 3：压力低于 10 公斤/平方厘米、温度高于 93℃的热停堆。

(4) 电厂运行状态 4：温度低于 93℃的冷停堆，直到容器上盖被移除。

(5) 电厂运行状态 5：移除容器上盖并将水位升至蒸汽管道的情况下进行换料。

(6) 电厂运行状态 6：在移除容器上盖、水位升至乏燃料水池且换料输送管打开的情况下进行换料。

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显示为 Laguna Verde 核电厂的沸水堆时间函数。在图 III-3，对于同一电厂的电厂运行状态 1－4 显示出了风险概况。显然，与其他电厂运行状态中的风险相比，电厂运行状态 4 中的风险是最高的。这个示例强调了风险概况提供的洞察，从而有助于分配安全改进的努力。

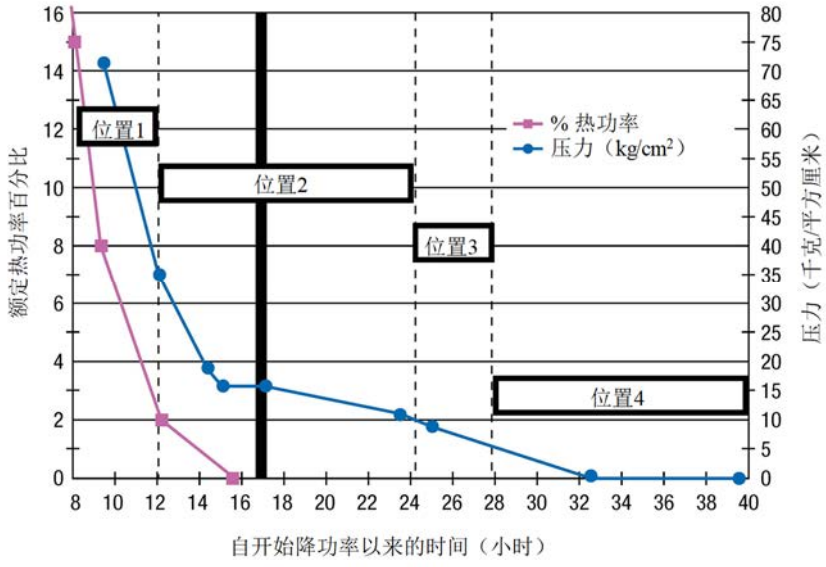

图 III-2. Laguna Verde 核电厂关闭状态概率安全评定中的电厂运行状态。POS－电厂运行状态。

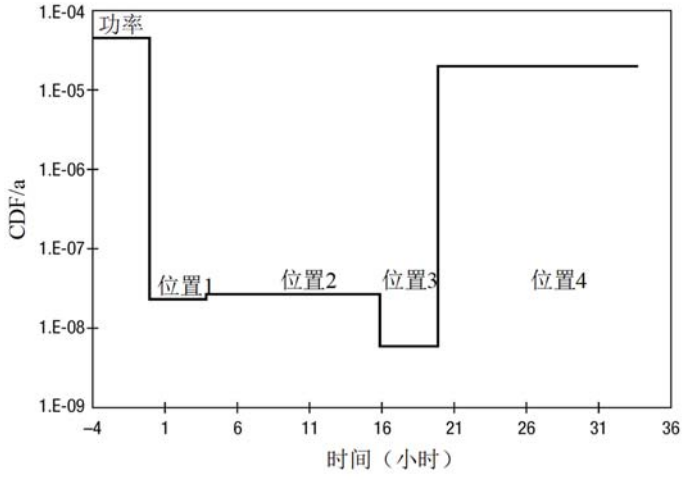

图 III-3. 功率运行和关闭状态下概率安全评定年堆芯损坏频率（CDF）的比较。POS－电厂运行状态。

附件 III 参考文献

[III-1] BABST, S.，等，“德国 SWR 69 型反应堆关闭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.，GASMANN, D.，“低功率和停堆工况下现代 1300 兆瓦压水堆的概率安全分析”，概率安全评定和管理（波多黎各圣胡安国际会议第 6 届会议论文集，2002 年），爱思唯尔科学，牛津（2002 年）。

[III-3] 合作概率风险评定计划（COOPRA），“合作概率风险分析，低功率停堆工作组，状态报告，2001 年 10 月”，爱达荷州国家工程与环境实验室，爱达荷瀑布，爱达荷州（2001 年）。

[III-4] 合作概率风险评定计划（COOPRA），“合作概率风险分析，低功率停堆工作组，始发事件－总结，2004 年 7 月”，爱达荷州国家工程与环境实验室，爱达荷瀑布，爱达荷州（2004 年）。

[III-5] 联邦环境、自然保护和反应堆安全部《宣布自 2005 年 8 月 30 日起对德意志联邦共和国核电站实施“根据原子法第 19a 条进行的安全评审，概率安全分析指南”》，联邦公报 207a（2005 年）。

[III-6] 特性的概率安全分析《核电概率安全分析的方法和数据》，2015 年 5 月，BfS-SCHR-61/16，德意志联邦施特拉伦舒茨，萨尔茨基特（2016 年）。

[III-7] 国际原子能机构《核电厂低功率和关闭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-8] ESQUIVELTORRES, J.L.，LÓPEZMORONES, R.，“墨西哥拉克纳维尔德核电厂低功率和关闭状态概率安全评定”，《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

Bedrossian, S.	加拿大安大略省发电公司
Bukhari, W.	国际原子能机构
Choi, G.	国际原子能机构
Holmberg, J.-E.	芬兰辐射与核安全局
Jang, D.	韩国核安全研究所
Jeon, H.	大韩民国韩国水电和核电有限公司
Kim, D.	韩国核安全研究所
Laroche, S.	法国电力公司
Liubarskii, A.	俄罗斯联邦原子能工程公司
Maioli, A.	美国西屋电气公司
McLean, R.	加拿大布鲁斯电力公司
Minibaev, R.	俄罗斯联邦原子能工程公司
Poghosyan, S.	国际原子能机构
Röwekamp, M.	德国电厂和反应堆安全学会（GRS）
Siklóssy, T.	匈牙利核安全研究机构
Weerakkody, S.	美国核管制委员会

通 过 国 际 标 准 促 进 安 全

国际原子能机构
维也纳 • 2025 年
www.iaea.org

ISBN 978-92-0-524224-8