核安全导则

核动力厂一级概率安全分析

国家核安全局 2021 年 5 月 19 日批准发布

国家核安全局

核动力厂一级概率安全分析

（2021 年 5 月 19 日国家核安全局批准发布）

本导则自 2021 年 5 月 19 日起实施

本导则由国家核安全局负责解释

本导则是指导性文件。在实际工作中可以采用不同于本导则的方法和方案，但必须证明所采用的方法和方案至少具有与本导则相同的安全水平。

目　录

1 引言

1.1 目的

1.1.1 本导则是对《核动力厂设计安全规定》（HAF102）有关条款的说明和细化，其目的是给核动力厂一级概率安全分析（PSA，Probabilistic Safety Analysis）工作的开展提供指导。

1.1.2 附录 I 和附录 II 为参考性文件。

1.2 范围

1.2.1 本导则主要适用于为发电或其他供热应用（诸如集中供热或海水淡化）而设计的，采用水冷反应堆的陆上固定式核动力厂。其他类型的或采用革新技术的反应堆设计可参照本导则，但应经过细致的评价和判断。

1.2.2 本导则所提供的建议主要针对新建核动力厂，对运行核动力厂所开展的一级概率安全分析工作也可参照执行，但需要考虑运行核动力厂概率安全分析中可能存在的特定要求。

1.2.3 本导则所分析的范围限于核动力厂的一级概率安全分析，以堆芯损坏频率（CDF, Core Damage Frequency）为关注目标。因此，本导则中概率安全分析工作的研究对象为核动力厂反应堆堆芯，不包括乏燃料水池、放射性废物等堆芯外放射源的概率安全分析。

1.2.4 本导则给出了核动力厂功率工况、低功率和停堆工况下开展内部事件一级概率安全分析工作的指导建议。

1.2.5 本导则给出了核动力厂内部危险和外部危险筛选的指导建议，并针对典型内部危险和外部危险的概率安全分析工作给

出了指导建议。

2 与 PSA 特性和应用相关的总体考虑

2.1 概述

本章给出一些在实践中与 PSA 开展和 PSA 结果应用相关的一般性问题和考虑。本导则的分析范围仅限于一级 PSA，但为呈现 PSA 技术能力及其分析结果的全貌，本章将从更为广泛的角度进行阐述。

2.2 PSA 的范围

2.2.1 PSA 的开展范围应与核动力厂安全目标或准则相匹配。PSA 的定量结果通常用于检验其是否符合我国核安全监管机构制定的风险准则，而风险准则通常是根据堆芯损坏频率、不同类型放射性的释放频率和社会风险的定量要求来制定的，为此可能需要分别开展一级、二级或三级 PSA。风险准则通常不会具体规定所需要考虑的危险类型和核动力厂运行模式，因此，为应用 PSA 结果来验证与规定的风险准则的符合性，应开展涵盖完整的始发事件清单、危险清单以及核动力厂所有运行模式的全范围 PSA，除非所规定的风险准则已明确限定 PSA 的范围，或已使用替代方法证明模型中未涵盖的那些始发事件、危险和运行模式所导致的风险并不影响对风险准则的符合性验证。

2.2.2 开展一级 PSA，通常将反应堆堆芯作为分析的重点；开展二级或三级 PSA，应重点评估放射性物质释放的影响，此时 PSA 的范围可能还需要包括厂址上其他放射性物质（例如，乏燃

料和放射性废物）对风险的贡献。当考虑核动力厂给厂址附近公众带来的总风险时，堆芯外的那些放射源也应纳入 PSA 分析范围。

2.2.3 PSA 可以为风险评估的不确定性提供一个明确的分析框架。识别不确定性的来源并理解其对 PSA 模型和结果的影响应作为 PSA 工作中必不可少的一个组成部分，以便在应用 PSA 结果来支持决策时考虑不确定性带来的影响。

2.3 PSA 的验证

2.3.1 应对 PSA 所使用的方法、模型和计算程序进行验证与确认。根据 PSA 的分析范围（一级、二级或三级），这些方法和模型包括用于事件序列分析的事件树和故障树逻辑模型、逻辑模型的求解方法、诸如堆芯损坏后核动力厂安全壳内现象的建模，以及用于确定放射性释放所导致的健康和经济影响的放射性核素环境输运模型等。在应用这些方法和模型之前，应证明其能够充分表征所发生的事故进程。用于支持这些分析方法和模型的计算机程序应与分析的目的和范围相匹配，并且它们对相关物理控制和逻辑方程的实现也应是正确的。

2.3.2 为保证 PSA 工作及分析结论的质量，常用的做法是在 PSA 开发过程中对 PSA 的关键技术要素进行独立的同行评审。其目的是从一定程度上保证 PSA 分析范围、建模和数据的充分性，并确保与当前国际公认的 PSA 良好实践相一致。参与 PSA 同行评审的专家应来自独立于该 PSA 开发机构的其他单位。

2.4 活态 PSA

2.4.1 应对 PSA 进行定期的评估和升版。在核动力厂运行寿

期内，通常会对安全系统的设计或核动力厂的运行方式进行改进，这些改进可能会对核动力厂相关的风险水平产生影响。此外，在核动力厂运行期间，还可以得到更多关于始发事件频率和设备故障参数的统计数据。同样，也可能会出现可用的新信息、新方法及分析工具，而它们可能会改变初始分析中所作的部分假设，进而改变 PSA 的风险分析结果。因此，应当在核动力厂的整个寿期中对 PSA 进行定期更新，以确保其可以紧密地支持相关决策过程，这种定期更新的 PSA 称为“活态 PSA”。在更新 PSA 时应考虑核动力厂设计和运行的变更、新的技术信息、可用的新方法和新工具，以及核动力厂运行中积累的新的特定数据（例如，用于评价始发事件频率或设备故障概率的相关数据）。PSA 的更新应按照规定的程序来实施，并定期评估 PSA 的状态，以确保其能够如实地表征核动力厂当前的实际状态，并与预期的使用目的相适应。

2.4.2 数据的收集工作应贯穿核动力厂的整个寿期，以核查或更新分析结论。数据的收集应涵盖与运行经验相关的数据，特别是与始发事件相关的数据，设备故障及其在试验、维护和维修期间不可用的相关数据，以及人员行为绩效的相关数据。应根据新的数据对分析结果进行定期的再评估。

2.4.3 应鼓励开发活态 PSA，以协助核动力厂在正常运行中的风险决策。此外，PSA 还可以支持很多问题的分析，例如，评价核动力厂变更或临时改变设备的允许后撤时间所引起的风险变化。

2.5 风险准则

2.5.1 如果 PSA 的目的是识别重要的风险贡献因素，或对不同设计方案和核动力厂配置进行选择，则不需要与核安全监管机构规定的风险准则进行比较。然而，如果 PSA 的目的是为下列判断提供支撑：（1）计算得到的风险结果是否可接受，（2）核动力厂设计和运行的变更申请是否可接受，（3）是否有必要进行某项设计变更以降低风险水平，则需要参考核安全监管机构制定的风险准则，从保证核动力厂满足规定的安全水平出发，指导设计单位、营运单位和核安全监管机构履行其各自应承担的职责。除了核安全监管机构规定的风险准则外，设计单位、营运单位也可以从管理的角度对核动力厂制定更高的安全水平目标和更严格的风险接受准则。

2.5.2 核动力厂设计的基本安全目标是建立并保持对放射性危害的有效防御，以保护人与环境免受放射性危害。风险准则是用于支持论证核动力厂基本安全目标的准则之一。

2.5.3 核安全监管机构对一级 PSA 规定的风险准则通常采用堆芯损坏频率[1]给出。我国对新建核动力厂制定的堆芯损坏频率目标值为 10^{-5}/堆年。

2.6 PSA 的应用

2.6.1 PSA 方法在加深对核安全问题的认识、识别核动力厂设计的薄弱环节以改进核动力厂的安全水平、平衡核动力厂的设计以优化核安全资源的利用、确认核动力厂不存在陡边效应以及定量评估核动力厂的安全水平等方面都可以起到非常重要的作

[1] 关于堆芯损坏的概念应规定具体的准则。不同的反应堆设计，其准则可能有所不同。

用。

2.6.2 在核动力厂设计阶段，PSA 可以支持但不限于如下工作:

（1）确认符合核动力厂的安全目标,包括规定的风险准则;

（2）支持核动力厂状态划分;

（3）支持对核动力厂设计中所考虑的超设计基准事故的重要事件序列的选取;

（4）支持事故源项的选取和确定;

（5）支持核动力厂纵深防御层次的设置;

（6）支持核动力厂技术规格书的制定;

（7）支持某些具体安全要求的建立或调整;

（8）支持安全重要物项的分级;

（9）支持核动力厂总体设计方案的论证、优化和确定。

2.6.3 在应用 PSA 时，应注意对下述问题的处理:

（1）确保 PSA 分析工作达到与其支持的工作相称的质量水平;

（2）合理处理 PSA 分析结果的不确定性，并进行必要的敏感性分析;

（3）由于确定论安全分析的保守性要求确实为某些未知因素带来一定的保守裕度，而在 PSA 的分析工作中使用保守模型还是现实模型，需要根据实际情况来斟酌，并注意识别风险见解中的保守性。

2.6.4 对于处于设计阶段的核动力厂，PSA 的结果应作为设计过程的一部分以，支持其安全水平的评估。核动力厂的安全决

策是一个迭代的过程，应综合考虑 PSA 分析与确定论分析的结论，以确保满足监管要求、准则和平衡设计。

2.7 PSA 质量保证要求

2.7.1 PSA 质量保证应涵盖保证 PSA 达到要求的质量所需的相关工作，以及验证 PSA 达到要求的质量所需的相关工作。PSA 达到要求的质量意味着分析的最终结果是正确的、可用的，并且可以满足 PSA 实施目的和范围的要求。应对所有影响 PSA 质量的工作设置一套科学规范的工作方法，包括在适当情况下核查每项任务是否圆满完成，并针对未完成的任务采取必要的纠正措施。

2.7.2 PSA 的质量保证应作为 PSA 项目管理的一个组成部分。质量保证应涵盖对 PSA 各项相关活动的控制，包括组织、技术工作及文档等方面。针对 PSA 技术工作，质量保证旨在确保目标、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。质量保证还应包括对 PSA 文档的管理。

2.8 PSA 文档的一般规定

2.8.1 PSA 文档的首要目标是满足使用方的需求，并与 PSA 的特定应用相适应。PSA 可能的使用方包括:

（1）核动力厂营运单位（管理人员及运行人员）;

（2）设计单位和供货商;

（3）核安全监管机构及为其提供技术支持的人员或机构;

（4）其他政府机构;

（5）公众。

2.8.2 PSA 文档包括 PSA 的工作文件、计算模型的输入和输出、阶段性成果报告和最终报告等。PSA 文档应内容完整，结构

合理、清晰，且易于理解、审查和升版。应采用可追溯的、有序的方式进行记录，即各部分应尽可能按照实际分析工作开展的顺序在最终文档中进行呈现。此外，还应为可能的扩展性分析提供方法说明，包括使用改进的模型、扩展 PSA 的范围以及其他应用等。清晰地描述在扩展与诠释 PSA 时所作的假设、例外和局限性对于 PSA 的使用方也非常重要。

2.8.3 应在报告（或参考文献）文档中给出用于复现研究结果的所有必要信息。所有的中间分析、计算、假设等信息应以文档记录、工作文件或计算机电子文件等形式予以保存，以保证将来可以对 PSA 分析的细节进行复现和更新。

2.8.4 PSA 研究工作最终应形成相应的 PSA 报告。报告应包括两个主要部分:

（1）主报告;

（2）主报告的附件。

2.8.5 主报告应采用清晰的、可追溯的方式阐述 PSA 工作的开展情况及研究结论，包括核动力厂描述、研究目标、使用的方法和数据、所考虑的始发事件、核动力厂建模结果及结论等。主报告及其附件应能够:

（1）支持 PSA 的技术审评;

（2）有助于相关使用方理解 PSA 分析的关键细节;

（3）支持运用 PSA 模型和结论进行高效、多样化的应用;

（4）便于模型、数据和结果的更新，以支持核动力厂进行持续的安全管理。

2.8.6 主报告的附件应包含开展 PSA 工作所涉及的详细数据、

工程计算的记录、详细模型等。附件的结构应尽可能直接对应主报告的相关章节。

2.8.7 本节对 PSA 文档给出了一般性的建议，本导则其他章节还将针对具体的分析对象给出具体的建议。

3 核动力厂信息收集

3.1 信息来源

3.1.1 PSA 团队应熟悉核动力厂设计和运行的相关信息，可用的信息来源主要包括:

（1）核动力厂的安全分析报告;

（2）核动力厂的技术规格书;

（3）系统说明书;

（4）竣工（现状）系统图（管道和仪表图);

（5）电气线路图，包括电路图及电气母线跳闸保护准则;

（6）控制和驱动电路图;

（7）正常运行规程、应急运行规程、试验规程和维修规程;

（8）系统任务成功准则的确定论分析;

（9）来自核动力厂或类似核动力厂的运行经验，以及事件报告和分析;

（10）操纵员日志（如果有);

（11）与运行人员的访谈（如果有);

（12）核动力厂运行记录和停堆报告（如果有);

（13）核动力厂数据库和/或计算机化的维修管理系统（如果有);

（14）核动力厂布置图;

（15）管道位置和布线图;

（16）电缆位置和敷设图;

（17）核动力厂巡访报告（如果有);

（18）监管要求;

（19）核动力厂其他相关文件。

3.1.2 PSA 团队应尽可能全面地收集包含分析所需信息的核动力厂文件。根据 PSA 分析的范围，可能还需要更为具体的信息，例如，外部危险 PSA 还需要核动力厂的布置图、厂址及周围的地形资料。必要时，还需要对 PSA 团队外的运行人员进行访谈，以澄清和获取更多可用信息。

3.2 现场巡访收集信息

熟悉核动力厂是开展内外部危险PSA分析的关键组成要素。应对核动力厂进行全面的巡访，以核实危险源及危险条件下核动力厂易损物项等的相关信息。应针对不同内外部危险的核动力厂巡访制定专门的实施程序。

4 功率工况内部事件一级 PSA

4.1 概述

本章为开展功率工况内部事件一级 PSA 所需考虑的技术内容提供相关建议，主要内容包括:

（1）一级 PSA 方法概述;

（2）始发事件分析;

（3）事件序列分析;

（4）系统分析;

（5）相关性分析;

（6）人员可靠性分析;

（7）数据分析;

（8）模型整合与定量化;

（9）重要度、敏感性和不确定性分析。

分析的总体框架如图 1 所示。

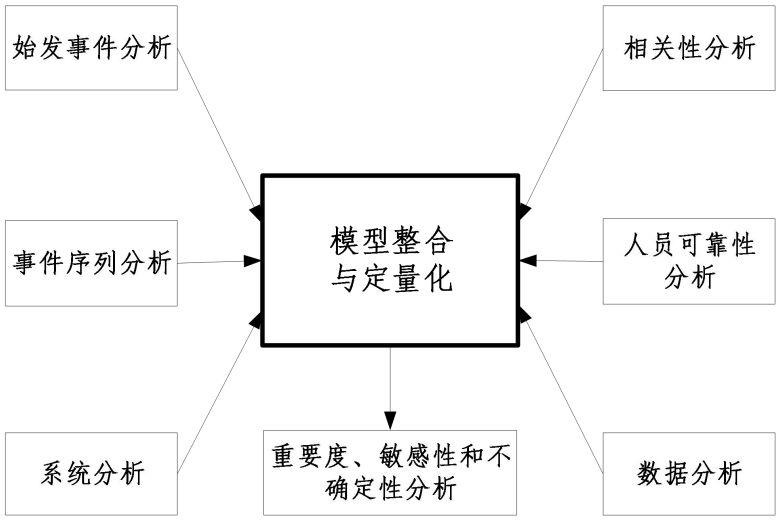

图 1 内部事件一级 PSA 的总体框架

4.2 内部事件一级 PSA 方法概述

4.2.1 本工作开展的第一步是确定功率工况内部事件一级 PSA 总的方法论。分析方法应从始发事件开始对可能发生的事件序列进行建模，识别会导致堆芯损坏的安全系统故障、支持系统故障和人员失误的组合。

4.2.2 PSA 的实施可以采用多种技术方法，一般通用的方法是组合使用事件树和故障树方法。事件树和故障树的规模（复杂性）在很大程度上取决于分析团队的选择（例如，相关性的处理方式），也取决于所用计算机软件的特性。

4.2.3 小事件树—大故障树方法是推荐的常用方法，一般称之为故障树联接法。事件树从始发事件开始，模化事件序列的总体特征，根据事故缓解措施和安全相关系统的成功或失败，确定各事件序列的终态（例如，成功或堆芯损坏）。故障树则用于模化执行安全功能的安全系统和支持系统的故障。

4.2.4 另一种方法是大事件树—小故障树方法，也称为大事件树法、联接事件树法或带边界条件的事件树法。此方法的特点是在事件树中直接模化功能、系统的相关性，即将安全功能、安全系统和支持系统的故障均在事件树模型中统一模化。

4.2.5 一级PSA分析的总体目标是给出堆芯损坏频率的最佳估算，同时尽可能避免引入过多的保守性，以免给结果带来不必要的偏差。因此，一级PSA应基于最佳估算模型、假设和数据。然而，在不确定性较大的情况下，有必要保留一定的保守性，以避免出现不合理的偏于乐观的评估结果。

4.2.6 一级PSA模型应当能够满足预期应用的需求，并且能够通过升级来支持未来可能的应用。

4.2.7 一级PSA分析所采用的计算机程序应具备以下能力:

（1）能够处理复杂的逻辑模型;

（2）能够在合理且较短的时间内完成定量分析;

（3）能够提供用于解释一级PSA分析结果的必要信息，例如，堆芯损坏频率、事故序列频率、最小割集、重要度分析、敏感性分析和不确定性分析结果。

4.2.8 一级PSA模型的开发应该是一个迭代过程，直至得到准确、足够详细的模型。

4.3 始发事件分析

4.3.1 一级 PSA 分析的起点是识别始发事件。始发事件是指任何干扰核动力厂稳定运行状态从而引起异常的事件，例如，导致瞬态或冷却剂丧失事故（LOCA, Loss of Coolant Accident）的核动力厂内部或外部事件。始发事件要求核动力厂缓解系统及人员作出正确响应，一旦响应失败则可能引起不希望发生的后果，例如堆芯损坏。

4.3.2 始发事件的识别

4.3.2.1 应系统化地识别一级 PSA 中需要分析的始发事件，通常建议组合应用下述方法对始发事件进行识别:

（1）工程分析，例如，危险和可运行性分析、故障模式及影响分析或其他相关方法，用于系统地分析核动力厂各系统和主要设备，以确定其故障（全部或部分）是否会引起始发事件;

（2）参考类似核动力厂的一级 PSA 分析、现有安全标准和导则所给出的始发事件清单，确定它们对所分析的核动力厂的适用性;

（3）以所分析的核动力厂（如果已运行）和类似核动力厂的运行经验为基础，识别可能的始发事件;

（4）审查基于确定论的事故分析和安全分析报告中考虑的始发事件是否包含在始发事件清单中;

（5）演绎分析，采用类似故障树的方法（例如，主逻辑图），以不希望发生的后果（例如，堆芯损坏）为顶事件，逐步分解成不同类别的可能导致该后果的事件，从最底层的各个事件中选出需要分析的始发事件。

4.3.2.2 作为一级 PSA 基础的内部始发事件清单应尽可能完整。虽然无法证明始发事件清单已包括所有可能的始发事件，但通过上述多种方法合理、必要的组合应用，有理由相信已尽可能全面地识别出了核动力厂的始发事件。

4.3.2.3 在识别始发事件时，应关注所分析核动力厂新的或独有的设计特点，它们可能是导致新始发事件的潜在来源。这对于缺乏或没有运行经验的新核动力厂尤为重要，需要特别注意识别特定设计所独有的始发事件、故障模式、事件序列和相关性。应利用工程分析法对所有的系统进行分析（详细分析前可进行适当的筛选），以识别它们可能因运行故障（全部或部分故障）或意外投运而引起的始发事件（或可能导致始发事件的继发性故障）。

4.3.2.4 始发事件清单应包括功能或系统的全部和部分故障，例如，多个蒸汽发生器的给水流量降低或单个蒸汽发生器的给水流量丧失，以及所有蒸汽发生器的给水流量完全丧失。因为部分故障导致的始发事件也可能会给风险带来显著贡献。

4.3.2.5 始发事件清单应包括核动力厂功率运行所有允许的模式下可能发生的始发事件。

4.3.2.6 始发事件清单应包括发生频率很低但潜在后果严重的事件，例如，反应堆压力容器破裂或界面 LOCA。若将一级 PSA 作为开发二级 PSA（也可能是三级 PSA）的基础，则将界面 LOCA 纳入始发事件清单就尤为重要。

4.3.2.7 应将识别出的核动力厂始发事件清单与类似核动力厂的始发事件清单进行比较，确保所有相关的始发事件都包括在

内。如果二者存在差异，应该将其补充到所分析的核动力厂的始发事件清单，或者论证它们不适用于所分析的核动力厂。

4.3.2.8 应对所分析的核动力厂（如果已运行）和类似核动力厂的运行经验进行审查，以确保所有发生过的始发事件都被纳入内部事件一级 PSA 始发事件清单中。

4.3.2.9 应确定始发事件的发生原因并在分析中加以考虑。对于有多个起因的始发事件以及由多个故障叠加导致的始发事件（例如，支持系统故障导致的始发事件），通常可以使用故障树方法对其进行模化。

4.3.2.10 一级 PSA 文档中始发事件分析部分应包括识别出的所有始发事件清单，并对每个始发事件进行描述，同时给出识别始发事件所采用的方法等详细信息，例如，危险和可运行性分析、故障模式和影响分析、主逻辑图或类似核动力厂运行经验等。

4.3.3 瞬态

4.3.3.1 一级 PSA 应以可能发生的完整的瞬态事件清单为分析基础。例如，瞬态类事件包括:

（1）反应堆排热增加，例如，二回路释放阀误开启或蒸汽管道破裂;

（2）反应堆排热减少，例如，主给水丧失或给水管道破裂;

（3）反应堆冷却剂系统流量降低，例如，反应堆冷却剂泵跳闸、卡轴或断轴;

（4）反应性和功率分布异常，例如，意外硼稀释;

（5）反应堆冷却剂装量增加，例如，安全注入系统的误投入;

（6）其他引起反应堆紧急停堆或快速停堆的事件。

4.3.3.2 内部始发事件瞬态清单中应包含丧失厂外电。应基于核动力厂厂外电网、厂内供电的相关设计和运行经验(如果有),确定丧失厂外电始发事件的发生频率、持续时间，并考虑厂外电源恢复的可能性。

4.3.3.3 丧失厂外电可能由内部危险（例如，厂内火灾）或外部危险（例如，极端环境条件或地震）导致。如果内外部危险PSA中已对丧失厂外电进行建模分析，则内部事件PSA对丧失厂外电的定义中应排除上述原因，以避免重复计算。

4.3.3.4 始发事件清单还应包括支持系统的故障，例如，电力系统、仪用压缩空气系统、冷却水系统、空调通风系统、仪表和控制系统等。特别是，当支持系统故障会引起反应堆紧急停堆，同时在停堆后该支持系统还要承担相关支持功能时，对此类始发事件的考虑更加重要。

4.3.4 冷却剂丧失事故

4.3.4.1 一级PSA中应尽可能全面地考虑会引起冷却剂丧失的始发事件。

4.3.4.2 冷却剂丧失始发事件应考虑会引起一回路冷却剂丧失的不同位置和不同尺寸的破口。应根据核动力厂的实际设计和布置情况确定可能出现破口的位置，包括管道和阀门的故障，特别是释放阀的故障。

4.3.4.3 应识别出会引起一回路冷却剂在安全壳外部排放的冷却剂丧失事故。此类典型的事故包括蒸汽发生器传热管破裂和界面LOCA。

4.3.4.4 应根据防止堆芯损坏的缓解措施中各安全系统的成功准则，对识别出的冷却剂丧失始发事件进行分类和归组。对于压水堆，通常基于对冷却剂丧失事故缓解的安全注入系统的性能要求，将冷却剂丧失始发事件分为大、中、小 LOCA 三类。根据核动力厂设计的不同，可能需要采取不同的措施应对极小 LOCA 的冷却剂丧失始发事件(例如，反应堆冷却剂泵轴封故障)。

4.3.5 始发事件归组

4.3.5.1 为了合理地减少一级 PSA 的工作量，在进行事件序列分析前应对始发事件进行归组。

4.3.5.2 若要将 PSA 模型进一步限制在可控制的规模，可将部分始发事件组从模型中筛除，但应注意，所采用的筛选准则应与开展 PSA 的目的相一致，以保证不会筛除对风险有显著贡献的始发事件组。需要注意，如果对 PSA 模型进行了这种筛除处理，则针对 PSA 的特定应用，仍可能需要重新检查模型的合理性以及筛选处理对结果的影响。

4.3.5.3 归为同一组的始发事件应具有相同（或极为相似）的特征，包括:

（1）始发事件发生后的事故进程;

（2）缓解系统的成功准则;

（3）始发事件对安全系统和支持系统的可用性和运行状态的影响，包括触发保护动作或闭锁系统启动的信号;

（4）预期的核动力厂操纵员响应。

4.3.5.4 在给定始发事件组中，缓解系统的成功准则，应采用该组内最为严格的始发事件的成功准则。

4.3.5.5 若将事故进程和/或缓解系统成功准则有细微差别的始发事件归为同一组，则事件序列分析应能包络这些始发事件所有可能出现的序列和后果。

4.3.5.6 对始发事件进行归组时，不应引入不合理的保守性。

4.3.5.7 可能引起安全壳旁通的始发事件（例如，蒸汽发生器传热管破裂、界面 LOCA）不应与事故后安全壳系统仍然有效的其他冷却剂丧失始发事件归为同一组。

4.3.5.8 一级 PSA 文档中始发事件归组部分应包括始发事件筛选、分组及合并的依据。

4.3.6 始发事件频率

4.3.6.1 应对一级 PSA 中模化的每个始发事件组确定其发生频率。在确定发生频率时，应考虑识别出的导致始发事件的全部因素。

4.3.6.2 应尽可能使用核动力厂特定的始发事件统计数据（如果有），并适当地辅以类似核动力厂的相关数据；若新建核动力厂或运行时间较短的核动力厂缺乏特定数据时，可以参考使用类似核动力厂的数据；若无法获得类似核动力厂的数据，则可以使用其他类型的运行核动力厂的通用统计数据。

4.3.6.3 对于发生频率较低的始发事件，即使采用通用数据，也会存在数据稀少或缺失的情况。可以通过基于知识和经验的判断来确定始发事件发生频率的取值，同时应对判断的依据进行阐述。

4.3.6.4 如果需组合使用核动力厂特定数据和不同来源的通用数据，应说明特定数据选取或多个数据源融合的方法，通常可

以采用贝叶斯估计或专家判断的方法。

4.3.6.5 除采用统计数据的方法外，还可以采用故障树方法来估计始发事件的发生频率。故障树可以对导致始发事件的所有设备故障和人员失误进行逻辑建模。如果采用这种方法，应检查故障树的分析结果是否与类似核动力厂的运行经验相一致。

4.3.6.6 经常发生的始发事件的频率取值应与所分析的核动力厂（如果已运行）和类似核动力厂的运行经验相一致。

4.3.6.7 始发事件组的发生频率应为组内所有始发事件发生频率的总和。

4.3.6.8 一级 PSA 文档中始发事件分析部分应给出所有始发事件的描述、频率均值、取值依据以及不确定性等相关信息。

4.4 事件序列分析

4.4.1 确定始发事件后，需要针对每个始发事件组确定核动力厂的事故缓解响应，即要求相关安全系统执行安全功能以防止堆芯损坏。安全功能通常包括反应堆停堆并使其保持次临界状态、堆芯余热的导出、放射性包容等。

4.4.2 事件序列中包含的功能事件用于表征安全功能执行所需的安全系统或人员动作的成功或失败。事件序列的终态为安全稳定状态（所有要求的安全功能都成功实现）或堆芯损坏。

4.4.3 堆芯损坏

4.4.3.1 应制定堆芯损坏或特定程度的堆芯损坏[2]的判断准则。通常可以假设燃料参数（例如，包壳温度）超过其设计基准限值

[2] 根据堆芯损坏程度，可规定堆芯损坏的若干状态。确定堆芯损坏程度的另一个因素是时间，例如晚期的堆芯损坏。

或更高限值（需论证），则会发生堆芯损坏。

4.4.3.2 堆芯损坏的判断还可以采用间接准则。例如，对于压水堆，当堆芯顶部长时间裸露或包壳温度超过规定的最大值时，即认为发生堆芯损坏。如果堆芯顶部裸露后需要经过相当长的时间才会造成堆芯损坏，在堆芯损坏的实际定义中应予以考虑。

4.4.3.3 在某些压水堆的 PSA 中，所采用的堆芯损坏判断准则举例如下:

（1）坍塌水位在一段较长的时间内持续在堆芯活性区的顶部以下；或者

（2）采用具有详细堆芯模型的程序预计的堆芯燃料包壳表面峰值节点温度高于 1204℃；或者

（3）采用具有简化堆芯模型（例如，单节点堆芯模型，集总参数）的程序预计的堆芯燃料包壳表面峰值节点温度高于 982℃；或者

（4）采用具有简化堆芯模型的程序预计的堆芯出口温度持续 30 分钟高于 650℃。

在实际的工程分析中，经常采取间接的判别准则。例如某个维持堆芯安全所必需的功能预计会发生不可恢复或者长时间的失效，也可以作为堆芯损坏的判断依据。

4.4.4 安全功能、安全系统和成功准则

4.4.4.1 应对每个始发事件组进行事件序列分析。

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

（1）始发事件的探测和紧急停堆;

（2）停堆并保持次临界;

（3）堆芯余热载出;

（4）反应堆冷却剂系统压力边界和安全壳的完整性保持。

4.4.4.3 应确定执行每个安全功能所需的安全系统和操纵员动作，包括各安全系统的成功准则。

4.4.4.4 安全系统的成功准则应根据每个序列对其安全功能性能水平的最低要求来确定。当安全系统有多个冗余列时，成功准则应确定为所需运行列的数量; 若安全功能涉及到多样化设置的多个安全系统，则成功准则应分别考虑每个系统所需的性能要求，此时可以基于最佳估算分析结果考虑每个系统的部分运行。

4.4.4.5 应识别出始发事件发生会导致其故障的安全系统，或始发事件发生导致安全相关设备处于严酷的环境条件，并在确定成功准则时予以考虑。例如，支持系统（如电源和冷却水系统）故障导致的始发事件; 再例如，在压水堆大 LOCA 或中 LOCA 事故情况下，若破口出现在冷段，则与该管段相连的一列应急堆芯冷却系统将无法向堆芯进行冷却剂的补充，在确定成功准则时，应对这种情况予以充分考虑。

4.4.4.6 成功准则中应规定安全系统的任务时间，即需要安全系统运行的时间，以使反应堆达到安全、稳定的停堆状态，并可以采取长期措施以保持该状态。对于大多数始发事件，任务时间通常可以设为 24 小时; 对于具有延迟堆芯损坏措施的新设计，可能需要考虑更长的任务时间。

4.4.4.7 应根据执行安全功能的前沿系统的成功准则，确定

相关支持系统的成功准则要求。

4.4.4.8 成功准则应明确为了使核动力厂达到安全、稳定的停堆状态，操纵员根据核动力厂规程所需采取的动作及允许的时间窗口。良好的实践是由核动力厂操纵员、系统分析人员、人员可靠性分析人员合作来确定操纵员应采取的动作。

4.4.4.9 一级 PSA 文档中始发事件分析部分应包括每个始发事件组中为将反应堆带入安全、稳定的停堆状态所需的安全功能、安全系统、支持系统和操纵员动作的清单。

4.4.5 成功准则的支持性分析

4.4.5.1 应通过支持性分析对安全系统和支持系统的成功准则进行验证。支持性分析包括瞬态和冷却剂丧失事故后衰变热导出的热工水力分析、反应堆停堆与保持次临界的中子物理学分析等。

4.4.5.2 如果有可能，应在一级 PSA 中使用基于最佳估算的、现实的成功准则。

4.4.5.3 如果采用基于设计基准分析的保守的成功准则，则应对整体分析结果进行仔细的审查，以确保这种保守性不会曲解一级 PSA 的风险见解。

4.4.5.4 用于验证成功准则的计算机程序应具备能够正确模化事故及需要分析的事故序列的能力，并能够给出最佳估算结果。计算机程序只能在其适用的范围内由合格的分析人员使用。如果有可能，应使用最佳估算的输入数据和假设，以避免不必要的保守性。

4.4.6 事件序列建模

4.4.6.1 应确定每个始发事件组后续发生的事件序列。通常采用事件树方法进行构模，在事件序列构模中综合考虑安全系统、支持系统和人员动作在执行安全功能时的成功或失败。

4.4.6.2 事件树应涵盖所有需要执行的安全功能和安全系统。通常将前沿系统的状态（成功或失败）作为事件树的题头，有时也称为“事件树顶事件”。此外，事件树题头还可以包括任何直接影响事故过程的操纵员动作，特别是应急运行规程所规定的应采取的动作。对事件序列有直接和显著影响的其他事件也可以作为题头。

4.4.6.3 事件树结构中应考虑表征操纵员动作和系统动作的题头事件的先后顺序。通常做法是尽量按照对系统或操纵员要求的时间先后进行顺序建模。

4.4.6.4 事件树结构中还应考虑由设备故障或人员失误所引起的功能上或实体上的相关性。

4.4.6.5 事件序列分析应分析事件树中各安全系统成功或失败的所有相关组合，以对后果为成功或堆芯损坏的所有序列进行建模。

4.4.6.6 一级 PSA 文档事件序列分析部分应给出事件树图，以清晰地表征事件序列的进展，并对事件树结构内含的逻辑进行阐述。

4.4.6.7 一级 PSA 文档事件序列分析部分应对各事件树题头进行阐述。例如，事件树题头可以表示简单的功能，也可以表示事件组合（在一个题头下包含多个功能）。应清楚地给出并解释在事件树构建过程中所作的假设和相应题头定义。

4.4.7 事件序列终态

4.4.7.1 事件序列终态的定义和划分应体现核动力厂的设计特性。通常可以分为两类：第一类完全执行所有必需的安全功能，从而避免堆芯损坏，即成功缓解；第二类因一个或多个安全功能未能执行而假定会发生堆芯损坏。

4.4.7.2 应明确导致堆芯损坏的事故序列的特征，以用于支持后续二级 PSA 的开发。例如，每个事故序列所导致的核动力厂的物理状态，以及用于防止或减少放射性物质泄漏的安全系统的可用性等。

4.5 系统分析

4.5.1 应对事件序列分析中所涉及的系统故障进行建模，一般可以采用故障树方法来分析，故障树的顶事件即为事件树分析中确定的系统故障状态。故障树从顶事件开始逐级向下分解到单个底事件，通常包括设备故障（例如，泵、阀、柴油发电机等的故障）、维修或试验导致的设备不可用、冗余设备的共因失效以及人员失误事件等。

4.5.2 需要分析的故障树范围取决于事件树的大小和复杂程度。

4.5.3 故障树分析

4.5.3.1 故障树建模的目的是为事件序列分析中涉及的安全系统的故障状态进行逻辑建模。

4.5.3.2 每个安全系统的故障树顶事件的故障准则应与事件序列中要求的成功准则在逻辑上互反。某些情况下，一个安全系统可能需要建立多个故障树模型，以处理不同始发事件组对应的

不同成功准则，或在事件树的不同分支中根据该系统前序事件的状态来处理不同的成功准则。具体实践中，可以针对不同的故障准则建立不同的故障树模型，或根据成功准则的要求使用逻辑开关（所谓的“房形事件”）来禁用或启用故障树模型的相关部分。

4.5.3.3 故障树中模化的基本事件应与可获得的设备故障数据相匹配。在故障树中模化的设备边界和故障模式应与设备故障数据中的定义相一致。

4.5.3.4 故障树模型的详细程度应达到单个设备（泵、阀门、柴油发电机等）的重要故障模式及单个人员失误事件的层次，并且应包含所有可以直接导致或与其他基本事件组合导致故障树顶事件发生的基本事件。分析层次通常由分析人员自行确定，但它应与可获得的设备故障数据和所预期的一级PSA应用相匹配。

4.5.3.5 应通过系统化的分析（例如，故障模式和影响分析）来确定故障树中需要模化的基本事件，并根据任务分析对操纵员动作进行审查，以识别潜在人员失误基本事件。

4.5.3.6 故障树模型应包括安全系统和支持系统运行所需要的所有重要设备，还应该包括其故障可能引起系统故障的非能动设备，例如，过滤器堵塞等。故障树模型中应明确考虑功能相关性和设备故障的相关性，否则可能会使分析结论产生严重偏差，低估支持系统的相对重要性。

4.5.3.7 故障树中设备分析的层次应能够保证模型对所有的硬件相关性都可以进行考虑。例如，在同一系统向多个设备提供冷却水的情况下，应对该冷却水系统进行明确建模，以考虑不同设备间因共用该冷却水系统而产生的相关性。设备可靠性数据的

可用性也是确定设备分析层次中需考虑的一个因素（例如，可以得到整台泵的可靠性数据，但无法得到其各零部件的可靠性数据，如转轮、联轴器、轴承）。此外，在确定故障树中设备分析的层次时，还应适当考虑希望得到的关于设备或零部件风险重要程度等 PSA 见解的需要。

4.5.3.8 将多个设备组合在一起采用超级设备进行故障建模时，应可以证明超级设备中每个设备的故障模式对系统的影响与超级设备整体对系统的影响是相同的。此外，模型中包含的所有超级设备在功能上都应是独立的，即同一个设备不应出现在多个超级设备中，或作为基本事件出现在别处。

4.5.3.9 故障树模型应识别安全系统中单个设备或设备列因试验、维护或维修而退出运行的情况，如果存在这种情况，则应进行明确的建模。例如，可以在故障树中添加表示设备不可用的基本事件来实现。

4.5.3.10 对系统因维修不可用的建模应与核动力厂的技术规格书[3]和维修活动相一致。建模中系统或设备的维修不可用时间应优先采用核动力厂基于维修经验得到的实际不可用时间；若核动力厂处于设计或施工阶段，则可以参考类似核动力厂的维修经验或参照技术规格书中规定的允许后撤时间。

4.5.3.11 应制定专门的编码体系，以统一规定每个逻辑门和基本事件对应唯一的编码。

4.5.3.12 故障树模型的开发应与预期的应用相匹配。例如，若将一级 PSA 用于风险监测器，则应建立对称的模型，对可能

[3] 在模化维修不可用时，通常假设核动力厂在技术规格书规定的运行限制条件下运行。

发生在所有位置的始发事件分别进行建模，包括一回路所有环路、安全系统的所有列、正常运行系统的所有运行列和备用列。

4.5.4 所需系统信息

4.5.4.1 应对一级 PSA 所模化的每个系统进行功能描述，为逻辑模型的开发提供有效和可审查的基础依据。通常包括以下内容:

（1）系统功能;

（2）系统故障模式;

（3）系统边界;

（4）与其他系统的接口;

（5）需要模化的运行模式（适用于具有多个模式的系统);

（6）需要运行或需要改变状态的设备及其正常配置状态;

（7）设备运行需要手动投入还是自动投入;

（8）设备接收自动信号须具备的条件。

4.5.4.2 应为故障树模化的每个系统提供简化流程图，图中应包括:

（1）故障树中模化的所有设备;

（2）设备的正常配置状态;

（3）连接各设备的管段或连接段;

（4）与支持系统的接口（动力、电气、冷却等)。

4.5.4.3 安全系统的功能描述和简化流程图应作为故障树建模的基础依据，一级 PSA 文档中系统分析部分应阐述如何在故障树建模中使用这些基础信息。

4.5.5 非能动系统

4.5.5.1 新型核动力厂的设计趋势是利用非能动系统来实现相关的安全功能（例如，余热载出、应急堆芯冷却）。

4.5.5.2 非能动系统运行边界条件的建立应基于热工水力分析、实验和测试的结果，这些边界条件包括系统的温度、压力、装量等。若边界条件满足，则认为非能动系统可运行；反之，则认为无法执行其设计功能。

4.5.5.3 应对非能动系统的故障进行建模分析，并评估其故障概率。非能动系统的建模可以使用标准的故障树建模方法来模化设备故障（止回阀或释放阀开启失败、管道堵塞等）、系统启动准备中的人员失误以及启动失败（若需要外部启动）等，在建模分析中应考虑上述分析中可能存在的不确定性。此外还应结合当前业内探索使用的方法对无法达到系统运行边界条件的可能性（例如，物理过程失效）进行适当地讨论。

4.5.6 基于计算机的系统

4.5.6.1 基于计算机的系统已广泛应用于新建核动力厂的控制和保护系统中，一些已运行的核动力厂也正在或即将进行相应的技术改造。基于计算机的系统，其功能的执行既依赖于系统硬件，也依赖于其内置的软件。硬件的可靠性在现阶段可以用常规的可靠性分析技术来评估，软件的可靠性在一定程度上可以通过软件的 V&V 程序加以分析。

4.5.6.2 基于计算机系统的故障概率可能主要取决于软件的故障，然而目前无法给出一个行业公认的用于评价软件故障的概率模型[4]，所以，首先需要保证软件编程的质量，即软件编程过

[4] “软件故障概率模型”是指始发事件后，虽然输入计算机系统的参数值均是正确的，但因软

程中是否遵循了恰当的流程以降低编程中出现错误的可能性，是否进行了恰当的检查以发现软件中的错误（静态测试），是否对已完成的软件进行了恰当的测试（动态测试）；其次，还应结合当前业内探索使用的方法对测试后的软件发生随机失效的可能性进行适当地讨论。

4.5.6.3 当控制和保护系统或执行相同安全功能的两个不同的系统都是基于计算机的系统时，应考虑这两个系统的硬件和软件是否存在相关性，如果有，则应在一级 PSA 模型中予以考虑。

4.6 相关性分析

4.6.1 相关性故障是堆芯损坏频率的主要贡献之一，因此，故障树分析中应对相关性进行建模处理。

4.6.2 可能的相关性包括以下四种：

（1）功能相关性：包括由核动力厂工况导致的相关性（例如，反应堆一回路冷却剂系统卸压失败造成低压安注不可用），以及由于共用设备、共用触发系统、相同隔离要求或共用支持系统（动力、冷却、仪控、通风等）而导致的相关性。

（2）实体相关性：也称为空间相关性，由可能引起安全系统设备故障的始发事件导致。这类相关性可能是由于管道甩击、飞射物撞击或环境影响所形成的。

（3）人员相关性：由核动力厂人员失误导致，这些人员失误将作为因素之一或直接导致始发事件，或造成一个或多个安全系统设备的不可用或故障而使它们在始发事件后无法执行其规定功能。

件错误而未得到正确输出的概率，以及软件错误所导致的后果。

（4）设备故障相关性：由于设计、制造或安装方面的错误或人员失误导致，此类相关性可以通过共因失效分析来处理。

4.6.3 应对核动力厂的设计和运行进行系统化的审查，以识别可能存在的相关性，它们会引起安全系统设备在应对始发事件时不可用或可靠性降低。

4.6.4 应在事件树或故障树模型中对所有功能相关性、实体相关性和设备故障相关性进行明确的建模。同时，也应对人员相关性进行建模，在人员可靠性分析（HRA，Human Reliability Analysis）部分将作进一步描述。

4.6.5 系统间的功能相关性应在事件树或故障树分析中进行明确的建模。分析人员可以利用相关性矩阵来对其进行识别，并作为支持事件树或故障树构建的基础信息。功能相关性不同于设备故障相关性，它可以采用事件树或故障树方法进行直接建模。对于无法直接处理的设备故障相关性则通常采用共因失效的方式来进行处理。

4.6.6 故障树分析中应识别并明确地模化由于共用设备或共用支持系统导致的系统间的功能相关性。这种相关性可能出现在执行相同安全功能的不同安全系统中，也可能出现在相关的支持系统中，无论哪种情况都应在故障树中进行明确的模化。

4.6.7 共因失效分析是相关性分析中的一个重要组成部分，用于模化设备故障相关性。应采用系统化的方法对其进行识别、建模和定量分析。

（1）对于可能出现设备故障相关性的情形，应识别出冗余设备清单并将其纳入设备共因失效模型。目前有多种方法可以对

共因失效进行建模分析，在同一个 PSA 模型中，若有足够的共因失效数据作为基础，应尽量采用同一种方法对共因失效进行建模。在共因失效建模中，应尽可能全面地考虑系统内存在的共因失效事件，并适当考虑系统间存在的共因失效事件。

（2）应识别可能会影响冗余设备组的共因失效，并利用 PSA 软件在故障树中进行恰当的建模。分析中应识别所有相关的设备组和重要的故障模式。在一级 PSA 文档中应阐明有关防范共因失效的相关假设。

（3）应论证各设备故障模式的共因失效概率的合理性，可以从下述方面进行考虑：系统的冗余度、设备的设计特性、系统布局（分隔、隔离、设备鉴定等），以及系统的运行、试验和维护情况。

（4）共因失效概率的计算，应尽可能基于核动力厂的特定数据，并综合考虑类似核动力厂的运行数据和通用数据；若使用通用的共因失效参数，则应论证这些参数的适用性，且通用数据源中的设备边界、故障模式和故障根原因应与 PSA 中的假设相一致；若采用专家判断的方法为共因失效参数赋值（当核动力厂特定数据和通用数据均不可用时），应对共因失效参数的赋值进行合理的论证，并保证所赋值的误差因子与共因失效参数确定过程中的不确定性相匹配。

4.7 人员可靠性分析

4.7.1 应采用结构化、系统化的方法来识别可能影响核动力厂安全的人员失误，并定义相应的人员失误事件，定量化其发生概率（即人员失误概率），以将其恰当地纳入核动力厂的 PSA 模

型中。应采用结构化、系统化的方法对各类人员失误对堆芯损坏频率的贡献进行全面分析，以使结论更具可信度。由于现有核动力厂设计中安全系统通常具有高度的冗余性、多样性和可靠性，因而使得包含导致始发事件或导致始发事件缓解失败的人员失误的事故序列对堆芯损坏频率的贡献往往会更加显著。

4.7.2 一级 PSA 通常采用经典的 HRA 方法对人员行为可靠性进行建模和定量化。如果条件具备，可以采用更先进的方法，以考虑人员行为与工作环境在动态交互中认知层面的因素。

4.7.3 尽管人员可靠性分析技术在近些年有所改进，但存在的方法众多，并且该领域的技术水平仍在不断提高。因此，应正确、自洽地应用所选用的方法。

4.7.4 人员可靠性分析的目的是得到体系人员失误概率。得到的各人员失误事件的概率之间应是自洽的，并且应与一级 PSA 的其他要素相匹配。

4.7.5 在开展人员可靠性分析时，应与核动力厂运行和维修人员密切合作，以确保分析过程和结论可以正确地反映核动力厂的设计特征及正常和事故工况下的运行情况。若无法开展此项工作（例如，处于设计阶段的核动力厂），则分析人员应参考其他或类似核动力厂的相关信息，或者应清楚地说明分析人员在分析中所依据的假设。

4.7.6 人员动作的识别

4.7.6.1 应采用结构化、系统化的步骤来识别需要在一级 PSA 中考虑的人员动作，应包含其失误可能会对堆芯损坏频率产生贡献的所有类型的人员动作。

4.7.6.2 人员可靠性分析应包括在始发事件发生前可能已经存在的会导致事故缓解所需设备或系统故障或不可用的人员失误（通常称为 A 类人员失误事件），这类人员失误通常发生在维修、维护、试验或校准任务活动中。若这类人员失误在始发事件发生前一直未被发现，则受其影响的设备或设备组在始发事件发生后对其需求时将不可用。特别是，此类人员失误有可能会同时引起多列安全系统的不可用。这类不可用通常会模化在设备、列或系统级的逻辑模型中。

4.7.6.3 应对核动力厂运行规程、维修大纲等进行系统性的审查，以识别与一级 PSA 中模化的系统相关的维修、维护、试验和校准等运行人员及维修人员活动，从而识别相应的 A 类人员失误事件。应通过系统性审查确定发生此类人员失误的可能性以及这类失误对相关系统、设备的可用性或故障的潜在影响。

4.7.6.4 应通过系统性的审查来识别可能引起始发事件的潜在人员失误（通常称为 B 类人员失误事件）。功率运行阶段 PSA 中，此类人员失误通常可以包含在相应始发事件中。

4.7.6.5 应对核动力厂应急规程进行系统性的审查，以识别在始发事件发生后核动力厂操纵员需要采取的关键动作，从而确定潜在的人员失误事件（通常称为 C 类人员失误事件）。通过审查应确定发生此类人员失误的可能性，以及这类人员失误对设备或系统的可用性或故障的潜在影响。C 类人员失误事件通常对堆芯损坏频率有较为显著的贡献，因此是一级 PSA 中需要识别的最重要的人员失误。

4.7.6.6 应将人员失误事件作为基本事件纳入故障树模型，

或作为题头事件纳入事件树模型，以反映人员失误对事故情景的影响。

4.7.7 人员失误概率的确定

4.7.7.1 人员失误概率的确定应基于特定的情境，并反映可能影响操纵员绩效的各种因素，包括压力水平、任务执行的可用时间、运行规程的可用性、培训程度、环境条件等。可以通过任务分析来识别这些影响因素（通常称为“绩效形成因子”）。

4.7.7.2 用于确定人员失误概率的方法应与一级 PSA 中常用的 HRA 方法保持一致，否则应论证所采用的方法的适用性。

4.7.7.3 应对每个关键的人员动作进行描述，详细说明与运行人员动作相关的所有重要事项，一般应包含以下内容:

（1）人员动作的时间;

（2）相关的核动力厂规程;

（3）动作执行时所处的环境;

（4）实际运作情况，例如，运行人员班组的结构及其职责;

（5）先前动作对当前动作的影响;

（6）操纵员可用的信息及培训情况等。

4.7.7.4 应采用恰当的方法对人员可靠性分析模型的正确性进行核查，例如，核动力厂巡访或操纵员访谈。此外，模拟机演练中对操纵员绩效和人机交互行为的观察也可为人员可靠性分析提供有用的支持信息。

4.7.7.5 核动力厂的安全文化也会影响人员失误概率，但目前还没有一个公认的方法能将安全文化合理地考虑在人员失误概率评估之中。

4.7.8 HRA 相关性分析

4.7.8.1 逻辑模型中包含的人员失误事件之间可能存在相关性，这种相关性通常由于使用共同的指示信息或程序步骤、错误的规程、错误的诊断或响应等导致。若同一个事件序列中的人员失误事件之间存在相关性，则可能会显著增加人员失误的概率，因此，应正确地识别人员失误事件之间的相关性并进行定量化。

4.7.8.2 应识别出包含多重人员失误的重要最小割集。具体实践中，可以将人员失误概率设置为一个较高的数值（例如，0.9），重新计算堆芯损坏频率，这样可以使包含多重人员失误事件的最小割集突显出来。应审查在同一最小割集中出现的人员失误事件，以确定它们之间的相关性水平，并在人误概率的定量化中体现这种相关性。

4.8 数据分析

4.8.1 本节对设备故障参数、设备退出运行的频率及持续时间等可靠性数据提出建议。始发事件频率和人员失误概率的相关建议在其他相应章节中讨论。

4.8.2 数据分析需要解决的主要问题之一是，当核动力厂特定运行经验有限或缺乏时，是否具备适用于所分析核动力厂设备设计和运行状态的可用数据。

4.8.3 应尽可能使用核动力厂的特定数据（如果有），并适当地辅以类似核动力厂的相关数据，以提供更为广泛的数据来源；若新建核动力厂或运行时间较短的核动力厂缺乏特定数据，可以参考使用适用于类似核动力厂的通用数据；若无法获得适用于类似核动力厂的通用数据，则可以使用其他类型的运行核动力厂的

通用数据。

4.8.4 若可用的运行数据未统计到设备故障，则应对设备故障概率的取值进行合理的论证。

4.8.5 应对用于一级 PSA 的可靠性数据进行论证。通常的做法是对多个不同来源的数据进行比较并解释其差异性。一般而言，在确定最优数据源的同时应提供相应的判断依据。

4.8.6 如果需组合使用核动力厂的特定数据和不同来源的通用数据，则应说明特定数据选取或多个数据来源融合所采用的方法，通常可以采用贝叶斯估计或专家判断的方法。

4.8.7 对于低故障概率的设备，即使采用通用数据，也可能存在数据稀少或缺失的情况，这种情况下可以采用专家判断的方式对其进行赋值，但应采取审慎的态度，并对取值的判断依据进行阐述。

4.8.8 设备可靠性参数

4.8.8.1 应对分析中包含的每个设备或每类设备的可靠性参数（失效概率或失效率）进行赋值。可靠性参数的确定应与设备的类型、运行状态、PSA 模型中确定的设备边界及故障模式相一致。

4.8.8.2 应对一级 PSA 模型定量化中所采用的设备可靠性参数的合理性进行论证。

4.8.8.3 对于停堆后还需运行一定时间的设备（例如，泵），应明确其任务时间。任务时间的确定需要考虑达到安全稳定的长期停堆状态和建立长期恢复行动所需的时间。在某些始发事件（例如，冷却剂丧失事故）下，这类设备的任务时间可能会非常

长。

4.8.8.4 一级PSA文档中数据分析部分应给出一级PSA定量化所采用的所有设备可靠性参数。应涵盖设备边界、故障模式、可靠性参数及其不确定性、数据来源等，并论证所用数据的合理性。

4.8.9 设备退出运行的频率和持续时间

4.8.9.1 一级PSA的定量化应包含设备和系统因试验、维护或维修所导致的不可用度。设备退出运行的频率和持续时间所采用的数值应真实地反映核动力厂运行的实际情况或计划的情况。

4.8.9.2 如果有可能，应基于核动力厂维修记录和设备不可用记录等特定数据，确定设备退出运行的频率和持续时间，也可以结合类似核动力厂的相关数据；若无法做到，则可以参考类似核动力厂的维修经验或参照技术规格书中规定的允许后撤时间。

4.8.9.3 一级PSA报告中数据分析部分应给出设备或列的不可用度数据，并应对所采用的数值进行论证。

4.9 模型整合与定量化

4.9.1 一级PSA模型中对事件序列频率的定量化需要始发事件发生频率、设备故障参数、设备退出运行频率和持续时间、共因失效概率和人员失误概率等数据的支持。

4.9.2 使用小事件树—大故障树方法时，应对每个始发事件组的逻辑模型（事件树和故障树）进行布尔逻辑运算。在对一级PSA模型进行定量化计算前，应确保模型中不存在逻辑环；如果存在逻辑环，则应在定量化前先进行解环，并应确保原有的相关性能够尽可能地保留。一级PSA报告应给出模型中所有逻辑环

的解环方式和细节。

4.9.3 一级PSA的定量化应使用经过充分验证和认可的计算机程序来进行。

4.9.4 定量化所用计算机程序的使用者应具备充足的经验，并且理解计算机程序的使用条件和限制条件。

4.9.5 一级PSA模型的定量化结果应包括以下内容:

（1）堆芯损坏频率（均值、点估计值和不确定性区间或概率分布);

（2）每个始发事件组对堆芯损坏频率的贡献;

（3）重要最小割集及其发生频率、事件序列及其发生频率;

（4）敏感性分析和不确定性分析结果;

（5）重要度分析结果。

4.9.6 分析人员应根据一级PSA开发过程中所作的相关假设，核查PSA模型分析得到的事故序列或最小割集的正确性，以保证他们确实会导致堆芯损坏的发生。这种核查可以采用抽样的方式进行，重点关注对风险有显著贡献的事故序列。此外，还应保证预计会导致堆芯损坏的最小割集也确实已包含在分析得到的最小割集中。

4.9.7 分析人员应合理地定义“风险贡献显著”的标准，可以采用绝对准则或相对准则（例如，相对于总堆芯损坏频率）的形式。

4.9.8 应验证对最小割集进行后处理（剔除互斥事件或添加一级PSA模型中未明确包含的恢复性操作）后，确实能够得到正确的结果。

4.9.9 一级 PSA 文档应给出 PSA 的定量化结果，并描述最重要的事件序列和最小割集及所进行的后处理。

4.9.10 分析人员应合理地定义“重要事件序列”和“重要最小割集”的标准，可采用绝对准则或相对准则（例如，相对于总堆芯损坏频率）的形式。

4.9.11 一级PSA定量化中通常需要规定截断值以控制定量化分析所需的时间。常用的方法是设置一个频率截断值，将低于此频率的最小割集进行筛除，从而节约分析时间（也可以采用阶数截断的方式，即筛除阶数大于规定数值的最小割集）。应当论证所设定的截断值水平足够低，既保证一级 PSA 的整体结果稳定收敛，又不会严重低估堆芯损坏频率结果。此外，可以根据 PSA 不同应用的需求来设定不同的截断值。

4.10 重要度、敏感性和不确定性分析

4.10.1 重要度分析

应对基本事件、基本事件组、安全系统、始发事件组等进行重要度计算，以用于支持 PSA 结果的解释。通常使用的重要度包括:

（1）Fussell-Vesely（FV）重要度[5];

（2）Risk Reduce Worth（RRW）重要度[6];

（3）Risk Achievement Worth（RAW）重要度[7]。

[5] Fussell-Vesely 重要度，对于特定的基本事件，FV 重要度是指包括该特定基本事件的所有最小割集的发生频率之和占全部堆芯损坏频率的份额（百分比）。

[6] Risk Reduce Worth 重要度，是指某特定故障模式的发生概率为零时（即该故障模式不会发生），堆芯损坏频率降低的倍数，它是设备可靠性的函数。

[7] Risk Achievement Worth 重要度，是指某特定设备确定发生故障时，堆芯损坏频率增加的倍数。它可以衡量设备所执行功能的重要性，可以识别对安全起主要作用的设备，即使该设备的故障率非常低。

4.10.2 不确定性分析

4.10.2.1 一级 PSA 模型及其所使用的数据均存在一定程度的不确定性，因此，在使用 PSA 结果进行风险分析或决策支持时，应考虑这些不确定性可能带来的影响。通常可以通过敏感性分析或不确定性分析来对它们进行评估。一级 PSA 的不确定性通常包括以下三类:

（1）分析不完备导致的不确定性：一级 PSA 的总体目标是通过系统化的分析，识别对堆芯损坏频率有贡献的所有事故序列，但在实际分析中无法保证此过程的绝对完整以及可以识别出所有可能的情景并进行恰当的评估。这种分析的不完备性导致的分析结果和结论的不确定性很难进行评估和定量化，甚至无法准确地处理这种不确定性。

（2）建模过程的不确定性：这种不确定性是由于不能完全把握分析中所用方法、模型、假设和近似处理的适当性而导致的不确定性。通常可以采用敏感性分析来评价其中某些因素的不确定性。

（3）参数的不确定性：这是由一级 PSA 定量化中所用参数的不确定性而导致的。此类不确定性通常可以利用不确定性分析来进行处理，给出所有参数的不确定性分布并考虑其在分析中的传递过程。

4.10.2.2 一级 PSA 定量化过程中用到的所有参数都应确定其不确定性分布，这项工作可以作为数据分析的一个组成部分。这些不确定性分布应能在分析中正确的传递，从而确定始发事件组发生频率、堆芯损坏频率等的不确定性。

4.10.2.3 在设计评估和决策过程中需要考虑存在的不确定性信息。

4.10.3 敏感性分析

4.10.3.1 应开展敏感性分析以确定一级 PSA 分析结果对所作假设和所用数据的敏感性。

4.10.3.2 应针对不确定性水平较高、可能会对一级 PSA 分析结果产生显著影响的假设和数据进行敏感性分析。敏感性分析可以应用其他假设或反映不确定性水平的数据区间对一级 PSA 结果重新进行定量化分析来开展。

4.10.3.3 分析人员应合理地定义“对一级 PSA 结果有显著影响”的标准，可以采用绝对的或相对的定量准则或定性准则（例如，引入新的事故序列）或二者的结合。

4.10.3.4 敏感性分析的结果可以支持 PSA 分析结论的置信水平，即可以为下述结论的论证提供置信度，包括：是否满足堆芯损坏的风险准则、核动力厂设计是否平衡、核动力厂在设计和运行方面是否存在基准分析情况下（与敏感性分析相比）未突显出来的薄弱环节等。

4.10.3.5 敏感性分析通常每次只针对一个假设或一个参数进行，必要时，也可以对相关假设的组合进行敏感性分析。

5 低功率和停堆工况内部事件一级 PSA

5.1 概述

5.1.1 本章给出适用于低功率和停堆工况内部事件一级 PSA 的相关建议。低功率和停堆工况内部事件一级 PSA 采用的方法

与功率工况内部事件一级 PSA 的方法基本相同，因此，除了低功率和停堆工况特有的要素外，本章的结构基本对应于第 4 章的结构。

5.1.2 低功率和停堆工况下，内外部危险的分析方法参考本导则第 6-8 章的说明，相关内容在必要时可根据低功率和停堆工况的需要进行适当调整。

5.1.3 低功率和停堆工况下，压水堆核动力厂通常开展以下主要活动：

（1）从功率工况切换到停堆工况；

（2）余热排出系统投入；

（3）开启反应堆压力容器，向换料水池注水；

（4）换料；

（5）维修和试验；

（6）余热排出系统停运并重返功率工况。

不同类型的反应堆，上述对应的活动可能会存在差异。例如，对于管式反应堆，第（3）条不适用。

5.2 停堆类型和核动力厂运行状态的定义

5.2.1 与功率运行工况相比，低功率和停堆工况下核动力厂的运行配置和工况有显著的不同。对于离线换料的核动力厂通常有三种不同的停堆类型：

（1）计划换料停堆，在此期间会同时开展大部分的维修活动；

（2）计划停堆，在此期间只开展特定的维修活动；

（3）功率运行期间可预计的非计划停堆。

核动力厂的技术规格书中将上述停堆类型划分为几个不同的运行模式，每种模式设置不同的设备运行要求。必要时，还应适当考虑长期临停的工况。

5.2.2 通常应对上述三种类型的停堆都进行分析，特别应对换料停堆的风险进行充分的评价，而另外两种停堆类型的风险是否需要进行全面的分析可以根据一级 PSA 的目的来确定。对事件序列的分析应从发生扰动开始，直至核动力厂达到安全稳定状态为止，因为若对分析预先设定一个固定的任务时间（例如，24 小时），则可能会因为任务时间终点时核动力厂尚未达到安全稳定状态而导致分析结果不能正确反映风险的实际水平。

5.2.3 若 PSA 的目的之一是评估核动力厂未来运行的风险，则在分析中应涵盖停堆规程可能预期的变更。

5.2.4 在低功率和停堆工况下，核动力厂可能存在多种不同的系统配置状态。如果对每一个配置状态都进行单独分析，则需要分析大量的配置情景，因此在能够体现低功率和停堆过程中核动力厂不同状态差异性的前提下，可以定义有限数量的核动力厂运行状态以减少不必要的分析工作量，即选取核动力厂的状况与配置均相对稳定且具有代表性的状态。

5.2.5 为将核动力厂运行状态组合的数量控制在便于分析的规模上，可以对相似的运行状态进行必要的归组。核动力厂运行状态归组时可以考虑以下特征：

（1）反应堆的临界水平（和/或停堆深度）；

（2）衰变热水平；

（3）反应堆冷却剂系统的温度和压力；

（4）一回路系统的水位;

（5）反应堆冷却剂系统状态（是否开启）;

（6）反应堆冷却剂回路的可运行性;

（7）燃料的位置;

（8）前沿系统和支持系统的可用性，包括自动投入还是手动投入;

（9）系统组态/系统配置;

（10）安全壳完整性。

5.2.6 对于低功率和停堆工况一级 PSA，核动力厂运行状态的确定应基于实际的或类似核动力厂的运行经验和现行的实践与规程。应根据需要分析的停堆类型，选取合理数量的具有代表性的停堆状态进行详细分析，以确定所关注参数在整个状态进程中的实际状态。此分析可用的信息来源包括:

（1）停堆和启堆规程;

（2）针对某个特定停堆状态的停堆计划;

（3）核动力厂通常的停堆操作;

（4）停堆的技术规格书;

（5）配置管理文件;

（6）停堆相关信息的其他文件（例如，操纵员值班日志）;

（7）维修记录（如果有，可以用于确定特定设备的维修周期）;

（8）对操纵员和值长的访谈（如果有）;

（9）与停堆计划编制人员的访谈。

从以上信息来源中提炼与核动力厂运行状态特征相关的所

有信息，特别是安全功能和其他相关功能的可用性信息。

5.2.7 为确保分析能够覆盖整个运行周期，避免遗漏或重复计算某些核动力厂运行状态的风险贡献，应明确定义核动力厂各运行状态（包括功率运行状态）的分界点。分界点的确定可以参考下述特征：每个核动力厂运行状态的持续时间、功率水平和系统配置，以及进入每个运行状态的频率（每日历年）。这个过程中可以参考历史运行数据（如果有）或类似核动力厂的历史运行数据。

5.2.8 应审查可用的特定核动力厂记录（如果有，例如运行历史、跳机跳堆记录），或根据参考核动力厂或设计最相似的核动力厂的记录信息，确定低功率和停堆工况中各核动力厂状态的平均持续时间和停堆后进入该状态的开始时刻。

5.3 始发事件分析

5.3.1 原则上，低功率和停堆工况始发事件的识别应遵循与功率工况内部事件一级 PSA 同样的方法。始发事件应包含冷却剂丧失事故、瞬态以及内外部危险分析所识别的始发事件。

5.3.2 与功率工况内部事件一级 PSA 类似，低功率和停堆工况下的始发事件分析同样关注会对核动力厂稳定状态产生干扰的事件。始发事件要求核动力厂的缓解系统及操作人员作出正确的响应，如果响应失败则可能导致不希望的后果（例如，堆芯损坏）。如前所述，低功率和停堆工况中不同的状态下，堆芯的配置也大不相同，因此可能会产生一些与功率工况一级 PSA 不同的特有的始发事件。此外，低功率和停堆工况下，人员维修活动或操作规程涉及的人员动作会更多，这也可能会引入很多由于人

误导致的始发事件。

5.3.3 低功率和停堆工况一级PSA所关注的主要始发事件为威胁关键安全功能或导致关键安全功能丧失的事件。所关注的事件序列终态（堆芯损坏）与功率工况一级PSA相同，压力容器外的燃料损坏不在本导则中考虑。

5.3.4 可以采用与功率工况一级PSA相同的方法来识别低功率停堆工况的始发事件，具体分析可以参考第4.3.2节。此外，还应系统地检查反应堆冷却剂系统配置变更规程及设备的试验与维修规程，这有助于对低功率和停堆工况特有始发事件的识别。

5.3.5 识别核动力厂操作规程执行过程中潜在的人员失误是低功率和停堆工况始发事件分析的关键之一。PSA分析人员应通过核动力厂的现场巡访来熟悉核动力厂的实际操作过程。

5.3.6 为确保低功率和停堆工况一级PSA始发事件清单尽可能完整，还应审查以下信息以识别需要补充的始发事件:

（1）其他类似核动力厂的低功率和停堆工况一级PSA始发事件清单;

（2）核动力厂运行历史（如果有）;

（3）类似核动力厂的经验;

（4）低功率和停堆工况的通用信息。

但需要注意，在审查核动力厂运行历史及类似核动力厂的经验时，应审查所有运行状态的运行历史和经验，并分析其对低功率与停堆工况的适用性。

5.3.7 应对始发事件进行恰当的归组。始发事件组包含的始发事件应可以用相同的事件树和故障树进行模化，即组内所有的

始发事件适用于相同的事件序列。通常可以参照下述准则对始发事件进行归组:

（1）组内所有始发事件对安全系统和支持系统的可用性和运行状态有相似的影响;

（2）组内所有始发事件对事故缓解所需的安全系统、支持系统及其他相关系统有相似的成功准则要求;

（3）组内所有始发事件对操纵员动作的需求相似;

（4）操纵员对组内所有始发事件的预期响应相似;

（5）组内所有始发事件的序列终态对应相同的核动力厂损伤状态。

虽然不同的核动力厂运行状态下可能会发生相同或类似的始发事件，但由于不同运行状态下系统的可用性和成功准则通常不同，因而在大多数情况下，一般不考虑跨核动力厂运行状态的始发事件归组。

5.3.8 在某些情况下，始发事件组中可能包含不完全满足第5.3.7节所述准则的始发事件，此时，始发事件组的特征应依据组内限制条件最为严格的事件来确定。

5.3.9 低功率和停堆工况始发事件频率的确定应采用与功率工况一级PSA相同的标准做法，但应注意对核动力厂某些特定因素的考虑，例如，设备配置状态及可用性、技术规格书和停堆管理等。

5.3.10 在低功率和停堆工况一级PSA中，始发事件频率可以用核动力厂在特定运行状态下的发生频率（可以以小时计）来表示。但是如果某个始发事件是由于进入某个核动力厂运行状态

而导致的，而不是核动力厂运行状态持续过程中发生的（例如，某些始发事件与试验活动或过渡活动相关，并且此类事件的频率不会随着核动力厂运行状态持续时间的增加而增加），则不应采用这种方式来确定始发事件频率。一种可以考虑的方法是，采用进入该运行状态的频率与此过程中发生该始发事件的条件概率的乘积来进行处理。

5.3.11 在低功率和停堆工况一级 PSA 模型定量化中，应以始发事件每小时发生频率为基础确定以“堆年”为基准的始发事件发生频率。对于每个核动力厂运行状态，应考虑核动力厂在每个运行状态的时间份额，从而使始发事件频率可以用核动力厂处在该运行状态中的时间份额进行加权。

5.3.12 对给定核动力厂运行状态下始发事件频率的定量化方法通常有三种（详细可参见第 4.3.6 节）:

（1）直接根据运行经验（所分析的核动力厂、其他有类似设计的核动力厂或通用堆型）进行评估;

（2）以功率工况一级 PSA 中始发事件频率为基础，通过补充分析来进行评估;

（3）利用逻辑模型对导致始发事件的所有因素进行建模分析。

对于利用逻辑模型评估始发事件发生频率的情况，通常可以用故障树方法或人员可靠性分析方法（导致始发事件的 B 类人误事件）来确定。这类始发事件（通常是支持系统故障导致的始发事件）的发生频率在很大程度上取决于核动力厂特定的设计特征。需要注意，在使用故障树方法或人员可靠性分析方法时，定量化

的目标应为始发事件的发生频率，而不是在一个特定时间区间内始发事件的发生概率。此外，为了正确地考虑导致始发事件的故障（例如，导致衰变热导出功能丧失的故障）与该事件缓解响应时相关功能的故障（例如，未能恢复衰变热导出功能）之间的相关性，也需要对导致始发事件的故障进行明确建模。

5.3.13 可以采用表格等方式概括地给出始发事件与各核动力厂运行状态的对应情况。

5.4 事件序列分析

5.4.1 安全功能、安全系统和成功准则

5.4.1.1 事件序列分析的一般方法可以参见功率工况事件序列分析的相关建议。虽然停堆期间的衰变热水平通常远低于功率运行立即停堆时的水平，但此工况下核动力厂的配置状态仍有可能引起威胁安全功能的事件。分析中应考虑以下方面:

（1）在停堆状态下，由于安全系统的自动触发多数不可用，会增加安全设备投入对操纵员动作的依赖程度;

（2）在停堆状态下，系统和设备进行的预防性维修和试验会导致系统和设备的可用性降低;

（3）反应堆冷却剂系统压力边界和安全壳的完整性可能降低;

（4）事故缓解对前沿系统功能的要求通常与特定的始发事件、核动力厂运行状态特征和衰变热水平密切相关。

5.4.1.2 应针对系统功能的性能要求定义系统不同的成功准则，它们可能会与功率工况一级 PSA 定义的成功准则不同。

5.4.2 成功准则定义的支持性分析

5.4.2.1 应酌情对功率工况一级 PSA 构建的系统故障树模型进行修改，因为即便在低功率和停堆工况下系统的响应逻辑与功率工况下的情况基本相同，但仍应考虑到设备或系统在停堆工况下的可用性可能会发生变化。

5.4.2.2 为确保相关假设的正确性，应通过热工水力计算来确定现实的成功准则。热工水力分析的详细程度应与系统分析和一回路系统配置状态相匹配。对于过渡工况（停堆及启堆期间）和热停堆工况，在有些情况下一回路系统的配置状态和条件与功率工况的瞬态事件类似，此时可以采用功率工况下的热工水力模型进行计算；其他情况下，必须要论证所使用的热工水力模型的适用性。对于其他核动力厂运行状态，应将一回路系统的特征与模型的分析能力进行对比，以评估特定计算程序的适用性。以轻水反应堆为例，基于热工水力分析确定成功准则时至少需要考虑以下因素：

（1）一回路压力边界状态；

（2）压力容器顶盖开启；

（3）一回路系统排气口开启；

（4）环路隔离或管嘴密封板的安装；

（5）蒸汽发生器的水位；

（6）一回路参数（温度、压力、不可凝气体、停堆深度）；

（7）一回路系统水位；

（8）反应堆余热水平；

（9）安全壳隔离状态。

5.4.3 事件序列建模

5.4.3.1 应使用事件树或者类似方法对核动力厂系统和操纵员对始发事件的响应进行建模。

5.4.3.2 事件序列建模应由具备多种专业知识背景的成员构成的团队来完成，特别应包含人员可靠性分析的专家。

5.4.4 事件序列终态

低功率和停堆工况事件序列分析终态的定义和划分可参考功率工况 PSA 事件序列终态的定义。

5.5 系统分析

低功率和停堆工况一级 PSA 系统分析的目的与功率工况一级 PSA 系统分析相同，都是为支持事件序列定量化对所需的缓解系统建立故障逻辑模型。系统建模最常用的方法是故障树，应尽量采用或调整功率工况一级 PSA 所建立的故障树模型。必要时，需要修改已有模型，或建立新的模型，特别是对于如下情形:

（1）现有模型不适用于模化不同核动力厂运行状态下特定系统的状态，例如，系统因维修而改变配置状态;

（2）功率工况下处于备用状态但在停堆时需要投入运行的系统;

（3）功率工况下系统为自动启动，而在停堆时需手动启动;

（4）系统在不同工况下的任务时间存在明显不同;

（5）不同的核动力厂运行状态的成功准则不同;

（6）不同的核动力厂运行状态下，系统初始可用列的数量不同;

（7）核动力厂工况与时间窗口存在明显不同，可能影响恢复动作的成功概率;

（8）功率工况一级 PSA 中无建模必要的系统;

（9）为实现低功率和停堆工况下特定安全功能的要求，将相关系统关联在一起的情况，例如，利用乏燃料冷却系统进行堆芯冷却。

5.6 相关性分析

5.6.1 与功率工况相同，相关性分析的目的是识别可能影响事件序列与系统模型逻辑结构和定量化结果的相关性，主要涉及前沿系统和支持系统的功能相关性、系统间的硬件共享或过程耦合、物理相关性（包括由始发事件直接或间接引起的相关性）、人员操作间的相关性和共因失效等方面。

5.6.2 参照功率工况一级 PSA 中的相关性分析，评估与检查低功率和停堆工况下应用的前沿系统和支持系统及其相关性，以考查它们对特定核动力厂运行状态的适用性。此外，还应关注试验和维修活动可能导致的新的相关性，例如，冗余设备同时维修或维护导致的相关性。

5.6.3 相关性分析的建模中需要关注低功率和停堆工况不同模式下成功准则不同或支持系统（例如，通风系统和供电系统）不同的情况。还应审查系统和设备退出运行的情况。

5.6.4 分析人员应熟悉和理解各种共因失效的机理以及停堆工况下的维修及其他活动对共因失效的潜在影响。

5.7 人员可靠性分析

5.7.1 功率工况内部事件一级 PSA 中对人员可靠性分析的主要内容对低功率和停堆工况同样适用。由于低功率和停堆工况下的人员行为分析更为复杂，因此需要有步骤、有逻辑地进行人员

可靠性分析。人员可靠性分析的目的是得到人员失误概率，不同人误事件概率的定量化应是自洽的，且应与其他要素的分析需求相匹配。

5.7.2 分析中应充分考虑低功率和停堆工况的典型特征，例如，大量雇用外部维修人员、频繁的加班工作以及对主控室工作要求的增加等，还应考虑工作监督方面的困难以及由于工期紧迫产生的压力。

5.7.3 应与核动力厂运行人员和维修人员密切沟通，以确保人员可靠性分析中能够正确地体现低功率和停堆工况下核动力厂的设计和运行特征。对处于设计阶段或施工阶段的核动力厂，分析人员应尝试从类似运行核动力厂的实践经验中获取相关信息。

5.7.4 A 类人员失误事件——始发事件前的人员失误

A 类人员失误事件是指始发事件发生前进行的试验、维护、维修和校准等人员行为未能正确执行从而导致设备不可用的事件。低功率和停堆工况下 A 类人员失误事件的识别和定量化过程与功率工况一级 PSA 类似，但还需要考虑低功率停堆工况的特点:

（1）临近停堆末期的功能性试验可能会面临更紧迫的时间限制，从而导致人员失误出现的概率增大;

（2）自动复位功能的可用性降低（例如，由于阀门自动关闭信号被隔离，试验后可能会由于维修人员遗忘导致未恢复关闭）。

5.7.5 B 类人员失误事件——可能引起始发事件的人员失误

由于在低功率和停堆工况下存在多种不同的维修策略、试验方案和配置变更，不可能从始发事件频率统计相关的运行经验中发现所有可能的人员失误事件，因此应系统化地评估人员失误引起始发事件的可能性。通过评估可以识别出会导致始发事件故障树中所需设备不可用（直接的或潜在的）的人员失误。分析时可以参考以下信息来源:

（1）启动规程和停堆规程;

（2）类似核动力厂的运行经验;

（3）停堆计划相关文件，包括技术规格书、试验和维修规程等。

应对 B 类人员失误事件进行定性筛选以确定需要进行定量评估或详细分析的人误事件。

5.7.6 C 类人员失误事件——始发事件后的人员失误

5.7.6.1 停堆期间，由于核动力厂自动化水平降低，始发事件的缓解会更依赖于人员操作，因此 C 类人员失误事件在低功率和停堆工况一级 PSA 中往往会成为堆芯损坏频率的显著贡献因素。因此，应对 C 类人员失误事件的概率进行仔细的考虑和尽量现实的评估。

5.7.6.2 所采用的分析方法应系统地考虑低功率和停堆工况一级 PSA 中对 C 类人员失误事件建模和定量化的特定需求，因为低功率和停堆工况与功率工况在很多方面存在明显差异。例如:

（1）更频繁的报警和持续的报警;

（2）规程指导文件的质量;

（3）操纵员的培训情况;

（4）响应时间窗口的长度;

（5）低功率和停堆工况下人机界面的质量。

5.7.6.3 需要注意，对于基于功率工况下人误概率与时间函数关系得到的人误概率值，应谨慎地审查其是否可以应用于低功率和停堆工况，因为低功率和停堆工况下的时间窗口可能远超该函数的适用范围。

5.7.6.4 应考虑始发事件诊断中可能发生的人员失误，特别当始发事件的诊断有规程可以遵循时。

5.7.6.5 与功率工况一级 PSA 相同，应考虑同一事件序列中人员动作之间的相关性。在低功率和停堆工况一级 PSA 模型中，对 B 类和 C 类人员失误事件之间相关性的考虑尤为重要。若始发事件（例如，衰变热导出功能丧失）是由人员失误所引起的，则导致操纵员失误的环境可能会使恢复衰变热导出功能的操作更加复杂，并可能会使人员失误导致该功能故障的概率要高于设备机械故障导致功能故障的概率。

5.8 数据分析

5.8.1 低功率和停堆工况一级PSA定量化所需要的数据包括:

（1）始发事件频率;

（2）人员失误概率;

（3）核动力厂运行状态的持续时间;

（4）技术规格书规定的后撤时间;

（5）设备可靠性数据;

（6）试验、维修不可用度;

（7）共因失效分析的相关参数;

（8）其他所需数据。

第 4 章功率工况内部事件一级 PSA 中给出的数据需求及获取相关数据的方法同样适用于低功率和停堆工况。

5.8.2 对于低功率和停堆工况，可用的设备可靠性参数不像功率工况那么充分，因此通常的方法是利用功率工况下的相关数据来支持低功率和停堆工况的定量化分析，但需要论证功率工况下相关数据的适用性。

5.8.3 计划停堆期间的大部分试验主要是为了验证设备在维修后的功能，即对设备重新投入运行前进行的功能试验。这类维修试验不可用度的确定应以试验的平均时长以及设备试验时核动力厂运行状态的持续时间为基础。

5.8.4 应评估试验和维修活动中涉及的与重要仪表校准活动相关的人员失误概率。

5.8.5 如果有可能，应考虑对设备或系统故障进行修复的可能性，因为修复动作可以显著提高安全系统在低功率和停堆工况下的可用性。若不考虑修复，在很多情况下可能会导致对风险的高估，特别是对于始发事件发生后的情景，在分析中考虑特定修复方案的可能性及其成功概率可使分析结果更加符合实际情况。这里的“修复”包含可以满足事故序列缓解需求的短期恢复动作，但仅限于实践经验证明其恢复可能性较大的情况，或者根据工程判断和/或在当前事故情景下可以建立有效的维修规程来保证恢复动作成功概率的情况。

5.8.6 在考虑修复的情况下，应考虑修复时间与核动力厂运行状态的相关性，包括系统和设备的可达性、维修人员的时间安

排、备品备件的可用性，以及某些事件序列下待维修设备周围的辐射水平等导致的相关性。

5.8.7 分析中应注意，在功率运行期间处于备用状态的设备在低功率和停堆工况中可能处于运行状态。若停堆工况下采用冗余设备或冗余列交替循环使用的运行策略，则应针对此类设备或系统列应选择恰当的可靠性模型。

5.8.8 计算始发事件发生后达到或维持稳定状态所需运行的设备的故障概率时，计算模型中应设置相应的任务时间，且任务时间的假设应与事件序列建模相匹配。

5.8.9 若要在分析中考虑预期要进行的停堆规程的变更，可能会对数据的采集产生影响。因为，这些变更可能使运行经验中已获得信息无法用于所需数据的分析，或必须经过分析或工程判断修正后才能提供所需数据。

5.8.10 对定量化中所使用的参数，不仅应给出其均值（或点估计值），还应给出其完整的不确定性分布以支持后续的不确定性分析。

5.9 事件序列定量化

5.9.1 低功率和停堆工况一级PSA事件序列定量化方法与功率工况下的方法相同。

5.9.2 审查定量化结果时应仔细评估所得到的最小割集。在低功率和停堆工况一级PSA中，可能需要对系统模型进行修改以体现不同核动力厂运行状态下的需求，因此应对不同核动力厂运行状态下类似事故序列或系统分析得到的最小割集进行交叉检验，以确保它们存在的任何差异都是真实地反映了不同核动力

厂运行状态或序列特征，而不是由于建模错误所导致的。

5.10 重要度、敏感性和不确定性分析

5.10.1 低功率和停堆工况一级 PSA 的重要度、敏感性和不确定性分析的方法与功率工况一级 PSA 的相同。

5.10.2 敏感性分析是低功率和停堆工况一级 PSA 的重要组成部分，旨在分析各个因素对低功率和停堆工况 PSA 的潜在影响。例如，选定的用于代表核动力厂运行状态的特定工况可能会涵盖核动力厂运行状态期间实际发生的更广的工况范围；与功率工况相比，低功率和停堆工况中存在多种不同的系统不可用组合，其中，某些组合的分析假设可能较为保守，而有些组合分析假设的保守性则可能较小；核动力厂运行状态的持续时间可能长短不一；人员动作的可用时间会根据核动力厂运行状态的不同而存在很大差异；成功准则也可能根据衰变热水平的不同而不同。应对上述这些差异进行研究，特别是对风险有显著贡献的核动力厂运行状态的建模假设等。

5.11 文档记录和结果呈现

5.11.1 本节对低功率和停堆工况一级 PSA 的文档记录和结果呈现给出建议。报告的结构可以参考功率工况一级 PSA 实施过程中各要素的结构，并添加用于描述低功率和停堆工况一级 PSA 特有内容的章节，例如，停堆类型识别、核动力厂运行状态定义等。

5.11.2 应该对各项研究内容的每个主要步骤所得到的结果进行整合与呈现，包括分析中得到的重要工程见解。总的结果评估、风险见解以及对不确定性的讨论也应包含在文档中。

5.11.3 根据初步分析结果对维修规程或操作规程进行的完善，或引入了新的维修规程或操作规程，通常也应在文档中进行概述。

5.11.4 应对总体性结论进行探讨并适当提出合理的建议。为支持风险决策，报告中应包括以下内容:

（1）堆芯损坏频率，整合所有核动力厂运行状态后得到的重要贡献因素:

— 支配性事故序列的贡献;

— 各核动力厂运行状态的贡献;

— 各始发事件组的贡献;

— 堆芯损坏频率不确定性分析结果;

— 堆芯损坏频率重要度和敏感性分析结果。

（2）每个核动力厂运行状态结果的呈现:

— 支配性事故序列的贡献;

— 各始发事件组的贡献。

（3）定性的结论和见解:

— 结果诠释和技术见解;

— 结论和建议。

5.11.5 工程技术见解和建议的阐述应明确清晰，能够为风险决策提供有益的支持。

5.11.6 为典型的停堆计划（尤其是换料停堆）构建一个风险剖面图，这非常有助于对该停堆计划总体风险的把握。例如，风险剖面图可以给出核动力厂不同运行状态的堆芯损坏频率与停堆时间或功率开始降低后的时间之间的关系。但需要注意正确考

虑时间份额对核动力厂不同运行状态风险的影响。

5.11.7 报告中应包含低功率和停堆工况一级 PSA 的详细信息:

（1）对总堆芯损坏频率有显著贡献的最小割集;

（2）每个核动力厂运行状态中对堆芯损坏频率有显著贡献的最小割集。

最小割集“贡献显著”的标准应根据 PSA 的目标来确定。

5.11.8 文档中还应包含以下内容:

（1）人员失误和相关性故障对堆芯损坏频率的贡献;

（2）独立失效对于堆芯损坏频率的贡献;

（3）事件树所模化的各种安全功能对堆芯损坏频率的影响。

5.11.9 应在数据库和计算机文件中对核动力厂模型和数据进行详细地记录和正确地设置，以保证结果可以复现，模型易于应用。

5.11.10 应以一种可追溯的，便于专家审查、升级和应用的方式对分析过程进行记录。

6 内外部危险一级 PSA 的一般方法

6.1 概述

除了由于设备随机故障和人员失误引起的内部始发事件外，还需要考虑核动力厂外部事件导致的风险。核动力厂的外部事件通常可以分为以下两类:

（1）核动力厂厂址范围内（包括厂房内和厂房外）的内部危险。例如，内部火灾、内部水淹、汽轮机飞射物、厂址内的运

输事故和厂址贮存设施有毒物质的释放;

（2）核动力厂厂址范围外的外部危险。例如，地震、外部火灾（例如，影响到厂址区域的森林火灾）、外部水淹、强风及其导致的飞射物、厂址外运输事故、厂址外贮存设施有毒物质的释放和极端气象条件。

上述危险可能会损坏核动力厂的设备，从而可能导致核动力厂发生堆芯损坏。这些危险通常会同时影响多个不同的设备，并对核动力厂运行人员造成不利影响。因此，内外部危险都应纳入一级 PSA 的分析范围[8]。

6.2 分析过程

6.2.1 应采用自洽的方法来识别核动力厂的内外部危险，并评估它们对堆芯损坏频率的贡献。内外部危险分析的主要步骤通常包括:

（1）收集内外部危险的基础信息;

（2）危险的识别，包括单一危险和危险组合;

（3）危险的筛选分析，包括定性和定量的筛选分析;

（4）包络分析;

（5）详细分析。

总体分析方法如图 2 所示。

6.2.2 虽然内外部危险识别和筛选的步骤类似，但针对每一种危险的包络分析和详细分析也可能会有其特有的任务，例如，对于内部火灾，需要对火灾的蔓延进行分析。

[8] 本导则不涉及由战争、恶意破坏或恐怖袭击行为等所引起的事件，但要考虑军事设施或和平时期军事活动的偶发性危险（例如，军机的坠落）。

6.2.3 应考虑对核动力厂具有潜在影响的所有内外部危险，并恰当地开展筛选分析、包络分析或详细分析。

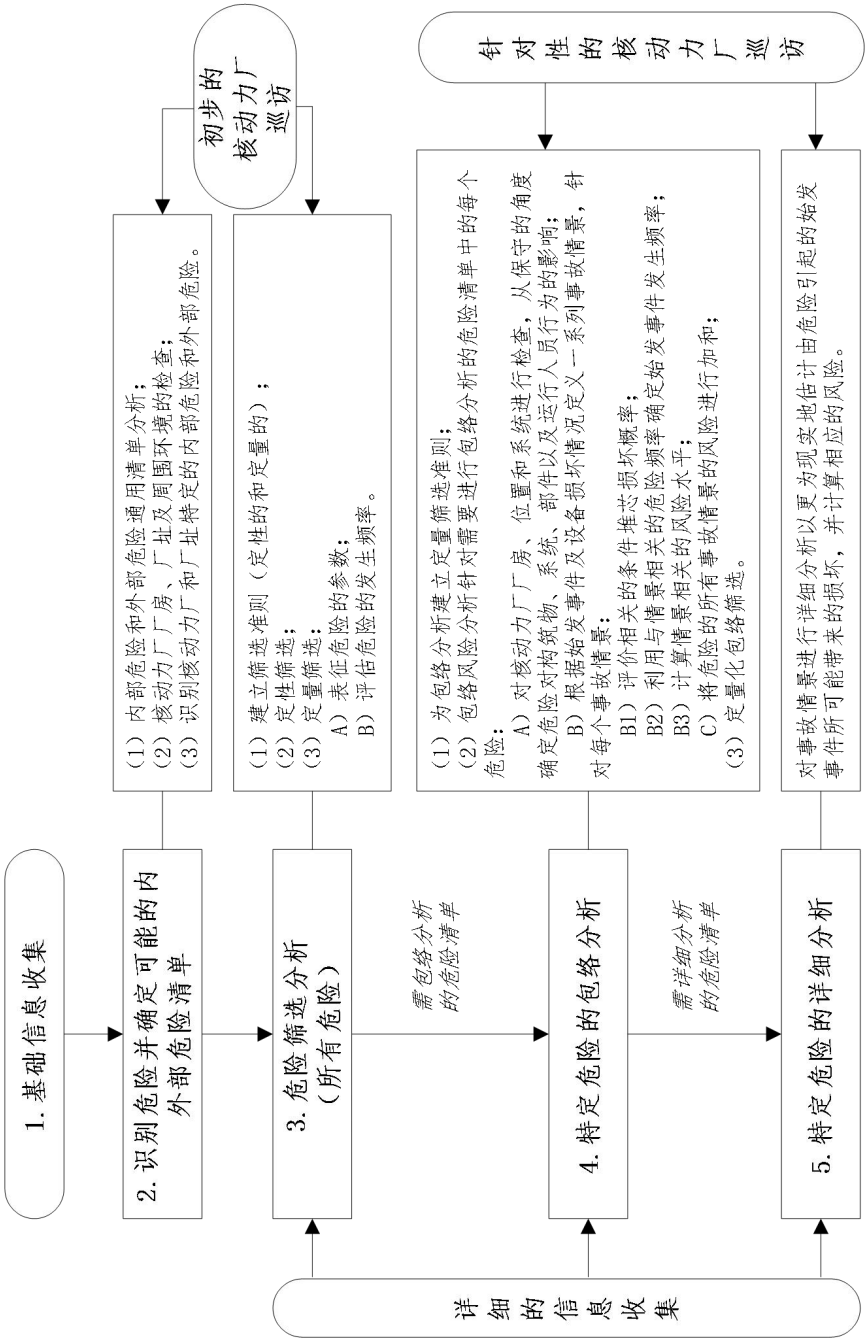

图 2 一级 PSA 内外部危险评价方法概述

6.2.4 在内部事件的一级 PSA 中，为消除逻辑环，在确保原有的相关性尽可能地保留的前提下，通常可以通过移除设备随机故障的子模型来简化故障树模型。这种情况下，这类设备（其随

机故障已从逻辑模型中删除）由于内外部危险引起的相关性故障，仍应纳入到内外部危险的一级 PSA 模型中。

6.3 基础信息的收集

6.3.1 开展内外部危险一级 PSA 时，应首先收集与内外部危险相关的所有可用信息。这些信息至少包括:

（1）安全分析报告所考虑的与内外部危险相关的设计信息;

（2）核动力厂厂房、构筑物、系统和部件的清单及布置图;

（3）厂区布局、厂址及周边的地形;

（4）管道位置、运输路线以及厂址内外有害物质贮存设施的相关信息;

（5）厂址周边工业设施的位置;

（6）厂址及该区域内发生过的内外部危险的历史信息等。

6.3.2 在内外部危险一级 PSA 的开展过程中，应根据每个危险所需的筛选分析、包络分析或详细分析的详细程度，对基础信息进行更新和补充。

6.4 危险的识别

6.4.1 危险识别的目的是形成一份潜在的内外部危险的完整清单。例如:

厂房内的内部危险:

（1）内部火灾;

（2）内部水淹;

（3）内部飞射物;

（4）内部爆炸;

（5）重物坠落;

外部自然灾害:

（1）地震;

（2）外部火灾;

（3）外部水淹;

（4）强风;

（5）生物现象（例如，厂用水进出口鱼类数量异常);

（6）极端气象条件[9];

外部人为事件:

（1）厂外爆炸;

（2）厂外有毒物质释放;

（3）飞机撞击。

6.4.2 为确保危险识别过程的全面性和可追溯性，应采用以下步骤对可能的危险进行识别:

（1）采用国际上已有的内外部危险分析方法。以已有相关文件包含的危险清单和已有研究关注的危险清单作为分析的起点。附录I给出了一份通用的内外部危险清单示例;

（2）采用结构化的方法识别厂址和核动力厂特定的内外部危险，保证可以对识别结果进行全面的核查。

6.4.3 对于已建核动力厂，应通过厂址调查和核动力厂巡访来识别内外部危险; 对于处于设计阶段的核动力厂，在识别中可以参考核动力厂厂址分析及厂区布置图等信息。

6.4.4 应列出潜在的危险组合清单，识别可能对风险有显著

[9] 极端气象条件包括极端温度、极端湿度、极端降雪（或暴雪）及浮冰、雷暴，其他的一些危险也可与之相关，例如，冰凌、霜冻和冰雹。

贡献的所有危险组合。危险组合对核动力厂安全所造成的影响显著高于单个危险各自作用所造成的影响，而且危险组合的发生频率可与单个危险的发生频率相当，例如，由暴风雨引起的高水位与由暴风雨引起的大坝溃坝等。

6.4.5 潜在的危险组合的识别应以单一内外部危险的清单为基础，且该清单应是未经筛选的完整的危险清单。尽管危险组合通常主要涉及自然灾害（例如，强风和高海水水位的组合），但自然灾害和人为事件的组合也有可能出现（例如，极端气候条件会增加船舶事故的风险），不能仅凭经验就将其排除。

6.4.6 通常可以通过对所有内外部危险之间的相关性进行系统性的检查，来较为现实地识别可能的危险组合。识别过程中应考虑以下可能产生危险组合的因素：

（1）危险有在相同条件下同时发生的可能（例如，强风和降雪）；

（2）一种外部危险可能引起其他危险（例如，地震引起的外部水淹并伴随溃坝）；

（3）外部危险可能引起内部危险（例如，地震引起的内部火灾或水淹）；

（4）一种内部危险可能引起其他的内部危险（例如，内部飞射物引起的内部水淹）。

应重新评估危险组合对安全功能的影响，因为它们可能会对不同安全功能或同一安全功能产生以比单一危险更为严重的影响[10]。

[10] 以下为潜在外部危险组合的示例：（1）干旱（由于高温）和强风及森林火灾引起的烟雾；

6.5 危险的筛选

6.5.1 对内外部危险进行筛选的目的在于尽量减少对风险贡献较低的内外部危险的关注，而将重点放在对风险有显著贡献的内外部危险上。筛选过程应是自洽的，同时所建立的筛选准则应确保不会遗漏任何与核动力厂和厂址有关的且对风险有显著贡献的内外部危险。内外部危险一级 PSA 报告中应明确给出内外部危险的筛选结果。

6.5.2 应保证用于内外部危险筛选的初始清单尽可能完整，不应出于对危险的大小或特征（强度或概率）已有的主观认识而预先将其筛除，即无论内外部危险对核动力厂造成损坏的可能性有多大，都应将其纳入初始清单。在随后的筛选过程中，可根据定性和定量的筛选准则针对具体的危险进行恰当地筛除。

6.5.3 通常可以单独或组合使用下列定性筛选准则，筛除满足条件的内外部危险:

（1）根据定性判断不会引起始发事件的危险，例如，在能够对核动力厂产生影响的足够近的位置范围内不可能发生的外部危险。需要注意，能否满足此项准则还取决于危险的强度等级，例如，危险事件不会引起停堆操作、触发前沿系统投入或安全系统丧失。

（2）危险的发展进程缓慢，并且可以证明有足够的时间可以消除危险源或能够进行恰当的响应。

（3）已包含在另一危险中的危险。

（2）强风与闪电；（3）高气温与高水温；（4）降雪与强风；（5）低吹雪与强风；（6）低吹雪与强风和冰凌。

（4）危险的发生频率均值明显低于其他危险（具有相似的不确定性分布），且不会引起更严重的后果。以这种方式筛除的危险可以认为其对总体风险没有显著贡献。

6.5.4 应针对核动力厂的安全目标，制定与核动力厂风险水平相匹配的定量筛选准则。危险筛选的定量准则取决于一级 PSA 的总体目标，并应与内部始发事件及内外部危险导致的堆芯损坏频率相关联。

6.5.5 第 6.5.3 节给出的定性准则不适用于源自厂房内部的危险的筛选。不能将厂房内部的危险作为一个危险类别进行整类筛除，通常需要进行包络分析或详细分析。

6.5.6 应确定用于表征内外部危险引起损坏程度的最重要的参数。若某一危险可能引起的损坏程度不能用单个参数表征，则应确定多个相关的参数。在筛选分析中应考虑被评估危险的所有特定参数（例如，水位和水压）。

6.5.7 下列外部危险不能被整类筛除:

（1）地震;

（2）人为事件;

（3）风类危险。

6.5.8 若要排除强风类危险中的某种特定危险（例如，非沿海地区的台风），应证明核动力厂所处位置的气候条件不足以使这一危险对核动力厂造成损坏。若能证明超过某一特定风速的强风的发生频率可以忽略不计，也可以将具有特定破坏力的风类危险筛除。应适当考虑风类危险与其他危险的组合（例如，降雨或水淹）。在进行筛选时，还应考虑被风卷起的物体（主要是在龙

卷风和台风的情况下）变成飞射物的可能性。

6.5.9 对于外部水淹危险的筛选，应考虑下列因素：

（1）核动力厂位置与河流、海洋或湖泊的距离，以及水淹浸入厂址的可能性；

（2）预警时间[11]：

— 对于滨河核动力厂，预警时间一般足以保证实现核动力厂的停运（例如，可以提前一天以上）；

— 对于沿海地区的核动力厂，预警时间通常较短，特别是在厂址附近发生海啸时，预警时间可能只有几个小时，甚至几分钟；

— 除了预警时间，还应考虑成功收到预警以及成功采取预防措施所需要的时间；

（3）核动力厂适当位置的挡水构筑物的类型；

（4）当发生水淹时，其他邻近地区有可能被淹没，且水淹水位可能高于预期值。地处狭窄洪泛区边缘的核动力厂比位于广阔三角洲地区的核动力厂更容易被水淹。

6.5.10 对于每种外部危险和源自厂房外部的内部危险，应在事故发生后的事件情景分析中通过保守性假设来估计其可能产生的最大影响，并将其应用于筛选过程。

6.5.11 当筛选准则只适用于某类危险中的部分危险（例如，一定强度的危险）时，应将这类危险拆分成若干个子类，并分别应用筛选准则，以避免将频率低但很可能会引起损坏的危险筛除。

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

6.5.12 核动力厂发生的始发事件可能是单个危险或多个危险组合的结果。应用筛选准则时，应保证不会筛除那些会引起严重后果的危险组合，即使其中的每个危险单独对风险的贡献都可以忽略不计[12]。

6.5.13 在应用筛选准则时，还应审查核动力厂及其周围环境的实际状况，以确定初始设计条件的变更不会影响分析结果或这种影响已经在 PSA 模型中予以考虑。特别应重点核查那些可能引起新危险源的变更，或可能导致某一强度等级的危险发生频率增加的变更[13]。

7 内部危险一级 PSA 的具体要求

7.1 概述

本章针对内部危险一级 PSA 的相关要求给出建议，涉及的内部危险包括（本导则未明确涵盖的其他内部危险，也可采用类似的方法加以评价）:

（1）内部火灾;

（2）内部水淹;

（3）重物坠落;

（4）汽轮机飞射物;

（5）内部爆炸。

---

[12] 这种危险组合例如强风与外部水淹。即使每一危险都可被筛除，但危险的组合可能给核动力厂带来大得多的风险。例如，外部水淹伴随强风，甚至是由强风所引起的。

[13] 此类变更举例如下：

（1）厂址 30 公里半径范围内的军事和工业设施的变更或附近运输线路（即铁路、航空线路、公路、河流等）的变更，这些变更将人为地引起外部危险的范围和量级的变化；

（2）厂址上游所建河坝的变更，将增加外部水淹危险引起损坏的可能性；

（3）环境条件（年平均风速及年最大风速、水位、温度、当地的降雨量等）的变更，将增加具有更严重破坏潜力的危险的发生频率。

7.2 内部危险一级 PSA 的包络分析和详细分析

7.2.1 对于厂房内可能发生的危险，很多研究表明这类内部危险的风险贡献通常较为显著，一般不能通过保守性的筛选将其筛除，因此应考虑对其开展包络分析或详细分析。内部危险一级 PSA 的包络分析和详细分析应采用自洽的方法开展，通常包括以下任务:

（1）如果可行，应通过核动力厂巡访来收集厂址和核动力厂的相关信息;

（2）危险特征的表述：危险的识别、危险发生频率的计算、危险影响的分析;

（3）与内部事件一级 PSA 模型整合形成内部危险一级 PSA 模型:

— 确定内部危险引起的始发事件;

— 识别内部事件一级 PSA 事件树和故障树模型中需要修改的内容;

— 分析特定的相关性和共因失效;

— 分析特定的数据（如果有）;

— 进行特定的人员可靠性分析;

（4）定性筛选和/或定量筛选;

（5）内部危险引起的堆芯损坏频率的定量化分析，包括结果分析，敏感性、不确定性和重要度分析;

（6）文档记录，特别应包含分析中所作的假设和参考的信息，以及质量保证等。

7.2.2 某些内部危险（内部爆炸、火灾和水淹等）可能会在

核动力厂的不同位置（房间、构筑物或厂址的其他地方）发生，对这些危险特征的描述应明确以下内容:

（1）整个核动力厂的分析边界，以涵盖所有可能对危险风险有贡献的区域;

（2）核动力厂中划分的若干封闭的分析区域。假设核动力厂设计中的保护措施（物理隔离、屏障和设备隔离等）能够有效地将危险的影响限制在这些区域内。

7.2.3 不能被筛除的内部危险应使用内部危险一级PSA确定其对堆芯损坏频率的贡献。内部危险一级PSA模型应基于内部事件一级PSA的核动力厂响应模型（包括功率运行工况以及低功率和停堆工况）来构建，并对内部危险可能引起的新的始发事件（例如，火灾事件中主控室丧失所有信息显示）建立新的事件树，将其整合到内部危险一级PSA模型中。

7.2.4 为支持对特定内部危险进行简化的定量风险评价，或支持对第7.2.2节中定义的核动力厂若干封闭区域的筛选分析，在没有详细的内部危险一级PSA模型时，仍可以利用公式（1）来估计特定内部危险引起的累计堆芯损坏频率（CDF）。

$$f_{H_i} = \sum f_j \times CCDP_j \qquad (1)$$

其中，f_{H_i} 为特定内部危险 H_i 导致的堆芯损坏频率；f_j 为核动力厂区域 j 内特定内部危险的发生频率；$CCDP_j$ 为核动力厂区域 j 导致堆芯损坏的条件概率，可以利用内部事件一级PSA进行估算，并根据核动力厂区域 j 中内部危险的影响进行保守性修正。

7.2.5 对于内部危险的影响分析，应该考虑危险导致的设备故障对PSA中始发事件及相关缓解安全功能的影响，对其影响

机理进行详细研究（例如，火灾情景和水淹漫延情景的模拟），以避免因过度保守而过高地估计危险带来的风险。

7.2.6 应对特定危险开展详细分析，以考查屏障和物理隔离等保护措施可能发生的失效，因为这类失效可能会使危险引起的损坏蔓延至核动力厂的其他区域。

7.2.7 可以从图纸或数据库中获取厂址和核动力厂的基本信息。对于运行机组，还可以通过核动力厂巡访对这些信息进行确认和完善。

7.2.8 通过核动力厂巡访所获取的信息是内部危险一级 PSA 的重要输入，因此如果有条件开展核动力厂巡访，应做好巡访的规划和组织，并进行全程记录。

7.2.9 如果有条件开展核动力厂巡访，最好在开展内部危险一级 PSA 之初进行。此外，某些任务（例如，所选危险的详细分析）还可能需要进一步开展有针对性的专门的核动力厂巡访。

7.2.10 危险导致堆芯损坏频率的定量化中既要考虑安全相关设备因该危险发生的故障，还应考虑设备的随机独立故障。

7.3 内部火灾分析

7.3.1 一般规定

7.3.1.1 内部火灾一级 PSA 是对发生在核动力厂厂址内的火灾事件及其对安全的潜在影响所开展的概率安全分析工作。内部火灾一级 PSA 模型应考虑:

（1）核动力厂内任何位置发生火灾的可能性;

（2）火灾蔓延至其他区域的可能性;

（3）火灾探测、灭火系统和火灾隔离;

（4）如果有必要，应合理地考虑因灭火系统投入而导致设备损坏的可能性（例如，灭火系统引起的喷溅和淹浸可能会损坏那些原本未被火灾损坏的设备，或者改变它们的故障模式）；

（5）火灾对设备及其相关仪控和动力电缆的影响，还应包括因“热短路”导致设备误动作而引起的新的故障模式；

（6）火灾情形下设备损坏的可能性，并适当考虑严重火灾对核动力厂构筑物（墙壁、顶棚、柱子、屋顶梁等）完整性产生威胁的可能性；

（7）设备随机故障及人员失误的影响；

（8）火灾对操纵员行为的直接影响（例如，需要从控制室撤离）或间接影响（例如，误指示引起的信息混淆）。

7.3.1.2 安全相关设备冗余列之间的物理隔离（防火屏障）可以限制火灾引起损坏的范围，因此，在利用内部火灾一级 PSA 模型来评估火灾对堆芯损坏频率的贡献时，通常都要包含不受火灾影响的设备的随机故障概率，以及设备由于试验或维修而退出运行的不可用概率。

7.3.1.3 应特别考虑以下由于烟雾而产生的影响：

（1）烟雾可能导致电子设备故障；

（2）火灾引起的异常环境条件（有毒或刺激性烟雾、高温）会增加人员动作的失误概率；

（3）烟雾可能会迫使操纵员从主控制室撤离。

7.3.1.4 针对低功率和停堆工况的内部火灾一级 PSA，应特别考虑以下方面：

（1）低功率和停堆工况内部事件一级 PSA 方法的特定需求；

（2）对低功率和停堆工况下的火灾危险应单独进行筛选，以考虑此工况下可能出现的更大的火灾荷载和更多的潜在点火源，尤其是低功率和停堆工况下维修操作可能产生的临时性可燃物；

（3）可用的消防设施；

（4）潜在的火灾蔓延路径（例如，低功率和停堆工况下，某些房门可能处于打开状态）；

（5）停堆期间人员在核动力厂不同区域内停留增多，可能会提高火灾探测的可能性；

（6）为控制可燃物对火灾相关的核动力厂运行和配置所进行的变更，以及为系统或设备不可用所采取的补偿措施。

7.3.1.5 在核动力厂设计和运行阶段所开展的确定论火灾危险性分析应作为内部火灾一级 PSA 的重要输入。例如，设备和电缆的清单及位置信息、核动力厂划分防火分区时为支持消防设施设计所开展的详细火灾影响分析。

7.3.1.6 内部火灾一级 PSA 应对核动力厂边界内的所有区域进行系统化的分析。为便于检查，应将核动力厂细分为不同的物理单元（火灾隔间[14]），并对其进行单独的检查。防火分区可以作为火灾隔间划分的起点，并应对火灾隔间划分的准则进行论证与记录。分析人员在划分火灾隔间时可以有一定的灵活性，例如，为便于进行筛选分析，分析人员可以将几个火灾隔间合并为一个火灾隔间来考虑。在火灾 PSA 的早期阶段，没有必要将核动力厂过细地划分为大量的小隔间。

[14] 在内部火灾 PSA 中，火灾隔间可以是一个封闭性良好的空间，不一定必须是被防火屏障（例如，墙、地板、顶棚等）包围的区域。

7.3.1.7 内部火灾一级 PSA 的开展过程通常包括如图 3 所示所述的各项任务。火灾事故情景应根据点火源和火灾隔间内火灾导致损坏的程度来确定，而特定火灾情景的发生频率取决于点火频率和灭火概率。

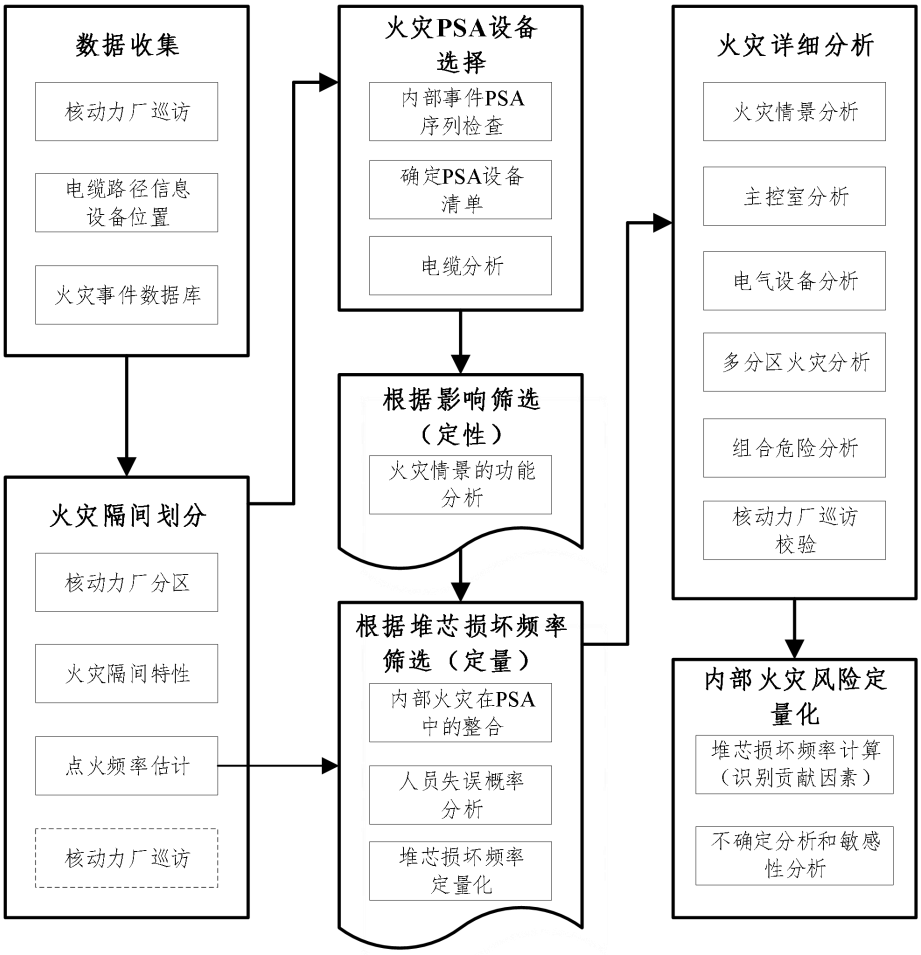

图 3 内部火灾一级 PSA 的开展流程

7.3.2 数据收集

7.3.2.1 内部火灾一级 PSA 数据收集和评估的任务是准备分析所需的相关数据。数据收集的重点是收集火灾风险建模所需的核动力厂特定数据，同时也需要对内部事件一级 PSA 中的部分数据从火灾影响的角度进行重新评估。

7.3.2.2 内部火灾一级 PSA 所需的核动力厂特定数据包括:

（1）核动力厂的电缆路径，包括电缆槽、导管、桥架和屏

障;

（2)火灾隔间的物理特性及其内部设施(参见第 7.3.3.1 节);

（3）火灾事件数据;

（4）火灾隔间内可能成为点火源的设备（即设备故障可能引起火灾，成为临时性可燃物）的特定信息;

（5）火灾探测及消防设施的可靠性;

（6）火灾时人员动作及人员失误概率;

（7）消防队的可用性及其能力;

（8）消防系统的特点（系统启动时间、可能引起设备损坏或阻碍操纵员进入火灾隔间的灭火剂等);

（9）火灾引起的设备故障模式以及火灾导致损坏的准则。

7.3.2.3 考虑到内部火灾一级 PSA 需要收集和维护的信息的数量及特点，可以开发相关的数据库作为支持工具。

7.3.3 火灾隔间划分

7.3.3.1 针对内部火灾 PSA，分析范围内包含的所有厂房和构筑物都应被划分到不同的火灾隔间，并分别对其进行单独检查（参见第 7.3.1.6 节)。对火灾隔间的检查至少应包括以下方面:

（1）物理边界（墙壁、门、挡板、贯穿件等);

（2）消防设施;

（3）火灾隔间边界的耐火性（耐火等级);

（4）火灾隔间内的设备和电缆;

（5）相邻的火灾隔间及其连接方式;

（6）火灾隔间与其非相邻火灾隔间连通的通风路径（通风管);

（7）火灾荷载（例如，类型、数量、是否有保护、位置、分布、长期存放或临时存放）;

（8）潜在点火源（例如，类型、数量和位置）;

（9）控制可燃物的管理规程;

（10）人员在区域内停留的情况（即人员发现火灾的可能性）;

（11）火灾隔间的可达性（例如，对于消防队而言）。

7.3.3.2 无论是对数据的收集还是对火灾隔间的确定，在核动力厂巡访期间，都应尽可能地对核动力厂的每个火灾隔间进行目视检查，以验证从核动力厂文件中所获得资料的准确性，以确保这些数据和信息能够反映核动力厂当前的实际情况。

7.3.3.3 火灾隔间内点火频率的估算是内部火灾一级 PSA 工作的重要组成部分，此项工作应在对所有火灾隔间进行定性筛选前，或对最重要的火灾隔间（定性筛选后保留下来的）进行定量筛选前开展（参见第 7.3.6.3 节）。应尽可能根据核动力厂的特定数据来估计点火源的点火频率；当核动力厂特定数据不足时，应使用通用数据以及可用的核动力厂特定数据来估计点火频率，并根据实际点火源（包括动火作业产生的火源）以及火灾隔间中长期和临时存放可燃物的数量对其进行调整。

7.3.4 内部火灾一级 PSA 的设备选择

7.3.4.1 应基于内部事件一级 PSA 所考虑的设备，确定内部火灾一级 PSA 中需要模化的设备清单。清单中所包含的设备，其因火灾发生故障后会产生如下后果:

（1）可能引起一个始发事件;

（2）可能影响安全功能的事故缓解能力（前沿系统和支持

系统);

（3）可能影响火灾引起始发事件后的操纵员动作;

（4）功率运行或停堆期间可能会导致某些功能的误动作，对核动力厂产生其他的不安全影响。

此类故障可能是由于动力或控制电源故障、热短路引起误动作或核动力厂监测仪表和报警错误而导致的。设备误动作分析的详细程度应与 PSA 的范围相匹配，并应关注内部事件一级 PSA 中未包含的设备或故障模式。

7.3.4.2 应识别对内部火灾一级 PSA 分析有重要影响的设备及建模相关的要素。应重新系统化地检查内部事件一级 PSA 模型中对设备故障模式进行筛选或归并的准则，以确定在火灾引起故障的背景下所作假设的有效性，并在必要时对内部事件一级 PSA 模型进行扩充。

7.3.4.3 还应梳理与第 7.3.4.1-7.3.4.2 节中列举的设备相关的所有电缆和电路，并进行电缆路径分析。此外，还应考虑非电管路（例如，仪用空气控制管路）因火灾而可能发生的损坏。

7.3.4.4 应为每个火灾隔间编制一份设备清单，有助于在详细分析中更为准确地确定各设备在火灾隔间内的位置。

7.3.5 基于影响的定性筛选

7.3.5.1 应依据定性的筛选准则（基于影响），按照影响程度筛除不重要的火灾情景。筛选过程应从识别关键的火灾隔间和区域开始，然后采用保守性假设明确潜在的单隔间和多隔间火灾情景。在利用基于影响的定性筛选准则筛除某特定火灾情景时应考虑火灾情景所涉及的火灾隔间的特征。

7.3.5.2 利用基于影响的方法对火灾隔间进行筛选时，若火灾隔间至少满足下列条件中的一条，则该火灾隔间对核动力厂安全的潜在影响可以忽略，从而可以将其筛除。

（1）火灾荷载密度低于规定的可接受阈值;

（2）以下所有条件均满足:

— 隔间内没有可能引起始发事件或需要手动停堆的设备;

— 安全相关系统（即核动力厂安全停堆所需要的系统）及其电缆或支持系统均不在隔间内;

— 火灾蔓延至其他设有安全相关设备的火灾隔间的可能性很低。

7.3.5.3 在进行筛选时，应假设所有暴露在火灾中的设备和电缆都会发生故障，即通常保守地假设火灾探测和灭火功能均无效或不可用。通常也不考虑其他的保护措施，例如，防火罩、保护涂层或外壳等。

7.3.5.4 进行筛选时，还应涵盖对火灾蔓延采用保守性假设条件下得到的多隔间火灾情景。对于每个火灾隔间，可以对该隔间添加其所有相邻的隔间（所有方向）和所有与该隔间不相邻但通过共用通风系统相连通的隔间来确定可能发生火灾蔓延的隔间组合。然后根据火灾蔓延至相邻（或相连）火灾隔间的可能性，分析所有可能的火灾隔间组合。为控制需要考虑的隔间组合的数量，在防火屏障可靠性和有效性的分析中可以设定相关的通用假设，例如，可以认为多道独立屏障同时发生独立失效的可能性非常小。

7.3.5.5 分析中应考虑可能从厂房外部蔓延到厂房内部火灾

隔间的火灾（例如，火灾从变压器厂房蔓延至汽轮机厂房的可能性）。

7.3.5.6 对于多机组厂址，应考虑公共区域（例如，机组间共用的柴油机和开关站）发生火灾对所分析机组产生影响的可能性。

7.3.6 基于对堆芯损坏频率（CDF）贡献的定量筛选

7.3.6.1 内部火灾与内部事件一级 PSA 的整合

（1）基于对 CDF 的贡献，利用定量准则对火灾隔间进行筛选，旨在进一步筛除根据“影响”进行定性筛选后保留下来的火灾隔间或包含多个火灾隔间的隔间组合。

（2）火灾对 CDF 的贡献应基于已有内部事件一级 PSA 的概率模型来估算特定火灾情景下的条件堆芯损坏概率。在这项工作中，评估火灾情景的发生频率以及火灾导致安全功能的条件不可用度时，应对火灾的发展和蔓延、火灾对设备造成的影响以及对相关的人员动作的影响采用保守性假设，即保守地假设火灾时火灾隔间内的所有设备不可用且探测和灭火手段均失效。

（3）对于每个筛选后保留下来的火灾隔间，应对内部事件一级 PSA 模型进行修改，以考虑火灾对火灾隔间的影响，模化相关的始发事件和设备故障模式。由此，可计算得到每个火灾隔间的条件堆芯损坏概率，再由第 7.2.4 节所给出的通用公式（1）计算得到火灾对 CDF 的贡献。

7.3.6.2 人员失误概率分析

（1）在确定火灾对 CDF 的贡献或计算条件堆芯损坏概率时，因为应急运行规程与专门的火灾消防程序之间会存在差异，因此

应重新审查内部事件一级PSA中采用的人员失误概率的适用性。如果采用的分析方法与内部事件一级PSA所采用的人员可靠性分析方法存在差异，则应论证差异的合理性并加以记录。

（2）在应用内部事件一级PSA所采用的人员可靠性分析方法时，绩效形成因子的分析应考虑特定火灾可能产生的影响。例如，额外的压力、可能存在的信号冲突、烟雾、失去照明以及进入或穿过受火灾影响区域的困难等。

（3）如果在内部事件一级PSA模型中考虑了人员恢复行动，则应检查其在火灾情境下相应恢复行动的可行性，例如，在受火灾影响的房间内执行特定的恢复动作可能很困难。还应检查火灾对主控室空气质量和人员失误概率产生的继发影响。

7.3.6.3 通过定量化火灾对CDF的贡献进行筛选

（1）对于定量筛选过程，应根据第7.2.4节给出的通用公式（1），结合火灾情景的发生频率，评估每个火灾隔间的火灾对CDF的贡献。

（2）定量筛选应基于保守估计的条件堆芯损坏概率或火灾对CDF的贡献来开展。火灾隔间的定量筛选可以参考以下两条准则：

— 所有筛除掉的火灾隔间对CDF的累积贡献应低于规定的阈值。该阈值可以是一个确定的绝对数值，也可以是相对数值；

— 单个火灾隔间的筛选准则应高到足以进行筛选，但也应低到足以保留所有风险重要的火灾情景。

（3）根据火灾对CDF的贡献进行定量筛选时，应考虑多个火灾隔间发生损坏的频率，它是一个火灾隔间的点火频率与火灾

蔓延至其他火灾隔间的条件概率的乘积。

（4）筛选过程（按影响和频率）的最终结果是确定一个火灾隔间相关的可能对风险有显著贡献的火灾情景列表。对于列表中包含的每个火灾情景，都应在内部火灾一级 PSA 中作进一步的分析。

7.3.7 火灾的详细分析

7.3.7.1 火灾情景分析

（1）详细的火灾情景分析旨在降低火灾情景筛选过程中所引入的保守性。应考虑火灾隔间内的防火屏障及其他消防措施、隔间内安全相关设备和火灾相关设备的位置，以及火灾发展和蔓延等多种因素。应考虑并评估火灾可能产生的所有影响，包括火焰、火羽、顶棚射流、辐射热、高能电弧和烟雾等。一般而言，在开展内部火灾一级 PSA 时，应进行专门的核动力厂巡访，以收集与验证进行详细分析所需要的支持信息。

（2）在评估用于降低设备损坏可能性的人员动作、火灾的发展和蔓延、火灾对设备和电缆造成的影响等方面时，应采用更现实的模型。

（3）应评估火灾、烟雾以及有毒气体蔓延对人员行为的影响。还应注意，火灾产生的过高压力也可能会妨碍人员开启房门进入执行恢复动作的相关区域。

（4）对选用的用于火灾发展和蔓延分析的建模工具（例如，火灾模拟程序）应提供合理的说明并加以记录。

（5）火灾情景应描述在所分析隔间内始发的火灾随时间变化的进程以及随后引起的设备和电缆的故障。火灾情景应在内部

火灾一级 PSA 模型中进行明确的呈现，例如采用火灾蔓延事件树（见附录 II 中的示例）的方式，以模化影响火灾发展进程的所有重要特征（防火屏障的设计和质量，火灾的发展和蔓延模型，火灾导致设备损坏的准则，包括电缆、消防和灭火设施）。

（6）对于需要详细分析的火灾情景，应采用与内部事件一级 PSA 相同的方法来评估手动操作的人员可靠性以及火灾探测与灭火设施相关设备的可靠性。

（7）火灾情景分析中应考虑可能的火灾蔓延路径（例如，通风系统或电缆沟槽以及失效的防火屏障）。

（8）对于需要进行详细火灾分析的火灾隔间，应采用所分析火灾隔间的特定数据（如果有）对相关火灾情景发生频率的数据进行补充和修正。例如，火灾隔间中的临时性点火源、可燃物和可能的火灾荷载等。

（9）对于特定的火灾情景，应论证火灾探测和灭火措施（自动和手动）能力的有效性和响应时间，以及灭火措施的失败概率。

7.3.7.2 主控室火灾分析

内部火灾一级 PSA 模型对主控室进行模化时应充分考虑其所处区域的具体特征。例如，主控室火灾对所有安全系统产生的广泛影响，可能导致的系统误动作以及火灾对主控室操纵员产生的影响，对后者的影响主要包括如下方面：

（1）火灾和烟雾对仪表及相关设备可用性的影响；

（2）火灾探测设施和灭火设施的能力；

（3）备用停堆点的可用性要考虑可达性及其他可能的限制条件；

（4）烟雾和有毒气体扩散的影响。

此外，还应考虑机柜内部的火灾蔓延，包括物理屏障以及冗余设备之间的空间隔离等因素。

7.3.7.3 电气设备间火灾分析

（1）电气设备间、开关设备间、电缆间和其他装有控制设备的房间往往是设备和线缆汇聚的中心，这类房间可能装有分属多个安全系统列的电气设备和电缆。因此，这类房间的火灾对安全停堆所需的冗余设备和其他相关设备的影响可能大于核动力厂其他区域火灾的影响，在内部火灾一级 PSA 中应对其进行考虑。

（2）这些房间中由于火灾导致电气短路而引起电气设备单次或多次误动作的概率也更高。在分析电气设备的误动作时，应识别需要分析的由火灾导致的电路失效，并对其条件概率进行评估。

7.3.7.4 多隔间火灾分析

（1）多隔间火灾分析旨在确定涉及多个火灾隔间的风险重要的火灾情景。分析中应假设火灾可能会通过共用屏障或连通隔间的通风管道从一个火灾隔间蔓延至另一个火灾隔间。多隔间火灾的详细分析应以合理的火灾发展模型、火灾蔓延模型和灭火模型为基础。

（2）相比单隔间火灾的详细分析，多隔间火灾的详细分析应考虑火灾蔓延的程度、燃烧产物的扩散和/或与相邻（或相连）火灾隔间的热量传递。

7.3.7.5 危险组合分析

（1）必要时，应在内部火灾一级 PSA 中适当考虑火灾引起次生内部危险的可能性（例如，灭火系统投入导致的大量排水引起的水淹、火灾引起的危险品爆炸、爆炸引起的火灾等）。

（2）如果外部危险（例如，地震、闪电、外部火灾、飞机撞击）一级 PSA 中未对如下方面进行分析，则在定性分析其他危险导致的内部火灾时应对它们给予适当的考虑，包括：火灾隔间可能同时遭受内部火灾和其他危险的叠加影响、其他危险导致的点火源、灭火系统的误动作或功能降级、手动灭火存在困难等。

（3）必要时，应适当考虑其他危险引起的内部火灾对操纵员绩效形成因子的影响。例如：

— 火灾发生后某隔间的可达性；

— 压力水平的升高；

— 无指示或误指示；

— 火灾对操纵员行为的其他影响。

7.3.8 内部火灾风险的定量化

7.3.8.1 用于内部火灾一级 PSA 详细分析所建立的特定分析模型（例如，主控室火灾模型、用于评估火灾导致单个或多个设备误动作影响的模型）应包含在完整的内部火灾一级 PSA 模型中。

7.3.8.2 应对筛选后剩余火灾隔间对 CDF 的贡献进行定量化，以支持详细的火灾分析。用于火灾隔间定量筛选的模型和结果都应纳入到内部火灾一级 PSA 中。应根据内部火灾 CDF 的主要贡献因素（例如，火灾隔间、火灾情景、人员动作）对内部火灾一级 PSA 的结果进行解释。在最后阶段，应该重新审查筛选过程

的相关假设，以考虑是否需要将已筛除但对 CDF 有一定贡献的因素重新添加到详细分析模型中。

7.3.8.3 内部火灾一级 PSA 模型的定量化中，应对结果进行不确定性分析，以确定不确定性的来源并对其进行评估；应进行敏感性分析和重要度分析，以确定内部火灾一级 PSA 中的风险重要因素。应对重要的假设进行敏感性分析，并确定各贡献因素对最终结果的相对重要性。

7.3.9 内部火灾一级 PSA 的文档

应作好内部火灾一级 PSA 的文档记录，以便于内部火灾一级 PSA 的审查、应用和更新。文档记录中应包含以下信息:

（1）对核动力厂特定消防设施的描述，包括核动力厂的非能动和能动缓解设施，以及对核动力厂火灾隔间的划分;

（2）对用于评估火灾危险的具体方法和数据的说明;

（3）为考虑内部火灾影响而对内部事件一级 PSA 模型所进行的具体修改;

（4）火灾隔间的特征;

（5）筛选分析中筛除特定火灾隔间的理由;

（6）火灾情景详细分析、主控制室火灾、电气设备间火灾、多隔间火灾、危险组合等的具体分析结果;

（7）内部火灾一级 PSA 最终的 CDF 结果及需要的中间结果;

（8）支持火灾分析的核动力厂巡访报告。

7.4 内部水淹分析

7.4.1 一般规定

内部水淹一级 PSA 是对厂房内发生的流体（通常是水）排放事件以及此类排放对安全的潜在影响所开展的概率安全分析工作。针对内部水淹建立一级 PSA 模型的过程通常包括如图 4 所示的各项任务。对于低功率和停堆工况的内部水淹一级 PSA，应参照第 7.3.1.4 节对与内部水淹适用的相关内容进行适当考虑。

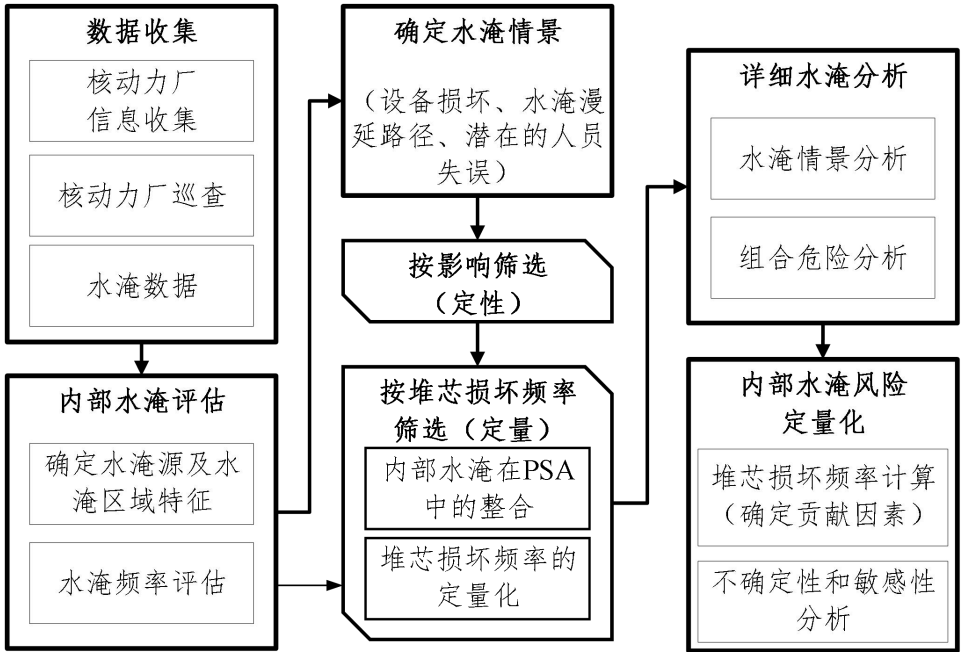

图 4 内部水淹一级 PSA 分析的开展过程

7.4.2 内部水淹可能性评估及数据收集

7.4.2.1 对于运行核动力厂，应针对内部水淹进行专门的核动力厂巡访，以验证从图纸和其他信息来源所获信息的准确性，并收集空间相互影响的相关信息，以合理地分析各内部水淹源引起损坏的影响。

7.4.2.2 应识别和描述可能发生的内部水淹事件，主要考虑以下方面：

（1）可能存在的水淹源：管道、内部水箱、水池、阀门、热交换器、与开放水源（例如，海、湖、河）的连接；对于多机

组厂址，还应将可能影响所分析机组的共用系统或构筑物考虑在内；

（2）可能存在的水淹机理：喷淋系统（例如，安全壳喷淋系统或灭火系统）的断裂、泄漏、破裂以及系统误投入或计划的正常投入，运行期间或维修相关活动中的人员失误（例如，阀门定位错误或被意外打开）；

（3）水淹特征：水量（取决于水源是封闭系统还是开放系统）、流速、温度和压力、存在蒸汽或可能产生蒸汽；

（4）与水淹相关的报警、泄漏检测、排水系统能力及水淹相关的设备保护（例如，设备跳闸信号）；

（5）PSA 相关设备的临界水淹高度和水淹区域内房间的尺寸。

7.4.2.3 在识别可能的水淹事件时，应特别关注核动力厂的停堆状态，因为在停堆状态下，经常需要进行手动疏排水，这可能会导致水淹事件。

7.4.2.4 应确定可能受内部水淹影响的厂房区域，识别可能的水淹漫延路径，并考虑因积水而导致防水屏障失效的可能性。

7.4.2.5 应将核动力厂划分为多个实体独立的水淹区域，即一个特定的水淹区域在内部水淹的潜在影响和可能的水淹漫延方面都独立于其他区域。

7.4.2.6 在评估内部水淹事件的发生频率时，应尽可能使用核动力厂的特定数据；当核动力厂特定数据不足时，经过论证后，可以使用通用数据。

7.4.2.7 用于评估内部水淹事件发生频率的数据主要包括管

道失效率、破裂频率及其不确定性分布，应对内部水淹重要来源的管道系统进行此类数据的收集和估计。此外，如果条件具备，应根据核动力厂特定的维修规程和经验，评估人员失误导致的水淹事件的发生频率及其严重程度。

7.4.3 确定水淹情景

7.4.3.1 对于每个内部水淹事件，应确定那些可能会受水淹影响的构筑物、系统和部件。根据分析的范围，水淹可能会对设备产生如下影响：淹浸、温度、压力、喷溅、蒸汽、高能管道破裂或阀门汽蚀引起的甩管或射流冲击等，应确保分析尽可能完整。

7.4.3.2 对于受内部水淹影响的设备，应考虑与其相关的标高、屏障、门和地漏等因素，且应考虑地漏发生堵塞的可能性。

7.4.3.3 应评估水流从一个区域漫延到另一个区域的可能性，包括对屏障失效的考虑。

7.4.3.4 应考虑所有可能的水淹漫延路径，例如，经过设备排水管、被开启的常闭门或闸门发生的漫延。

7.4.3.5 应确定安全相关设备和其他易受影响设备的机柜、电缆接线盒的位置（包括标高），以识别所分析房间在水淹情景下的薄弱环节。

7.4.3.6 应评估水淹对核动力厂运行的潜在影响，包括由于水淹引起的设备或系统的误动作。

7.4.4 基于影响的定性筛选

应根据水淹的影响对水淹情景进行定性筛选，筛除那些对核动力厂安全影响可以忽略的核动力厂隔间。若满足以下任一条准则，即可以将核动力厂隔间筛除：

（1）以下两个条件均成立:

— 该隔间内没有可以引起始发事件的设备;

— 水淹源所在隔间或水淹蔓延区域内没有反应堆安全停堆所需的系统及其支持系统。

（2）隔间内不包含任何足以导致设备故障的水源，包括来自其他隔间的水源渗漏。

7.4.5 基于对堆芯损坏频率（CDF）贡献的定量筛选

7.4.5.1 内部水淹与内部事件一级 PSA 的整合

（1）应根据对 CDF 的贡献进一步筛选内部水淹事件，因此，应对内部事件一级 PSA 模型进行修改以考虑水淹情景（包括系统模型和操纵员动作）。

（2）应对内部事件一级 PSA 中的人员可靠性分析进行全面审查。在应用功率工况内部事件一级 PSA 所采用的人员可靠性分析方法时，应基于水淹始发事件的特征对绩效形成因子进行评估。还应根据水淹事故缓解的具体规程，对人员失误概率进行重新评估和调整。水淹对操纵员绩效形成因子的影响至少需要考虑以下方面:

— 所分析隔间在水淹后的可达性，以及由于水淹、蒸汽或喷溅等不利环境条件带来的影响;

— 压力水平的升高;

— 无指示或误指示;

— 水淹对操纵员行为的其他影响。

7.4.5.2 通过定量化水淹对 CDF 的贡献进行筛选

（1）对于定量筛选过程，应保守的假设受水淹影响的隔间

内的所有设备都发生故障。如果这种保守性假设不会对 CDF 结果产生显著影响（使用第 7.2.4 节的通用公式（1）计算），则该水淹事件可以被筛除。

（2）内部水淹一级 PSA 的定量筛选准则应以水淹情景对 CDF 的贡献为基础。例如:

— 所有筛除的水淹情景对 CDF 的累计贡献应低于规定的阈值;

— 单一水淹情景的筛选准则应高到足以进行筛选，但也应低到足以保留所有风险重要的水淹情景。

7.4.6 水淹的详细分析

7.4.6.1 水淹情景的分析

（1）详细的水淹定量分析应考虑以下问题:

— 恢复时间的计算（水淹水位变化率）;

— 水淹事件缓解序列所需要的人员动作的可靠性分析;

— 为每个水淹情景建立事件树或故障树模型（适当时也可采用新的建模方法）;

— 对水淹事件树和相关故障树的定量化及分析结果，包括敏感性、重要度和不确定性分析。

（2）应根据探测和控制水淹事件的方法，分析所有对风险有潜在贡献的始发事件并评估这些探测和控制措施的失败概率。

（3）水淹情景应描述所选厂房区域内始发的水淹事件的发展进程和后续的设备故障。可以用水淹事件树来模化影响水淹情景发展进程的所有重要特征（水淹屏障设计、水淹探测和水源隔离）和设备故障的概率。在开展内部水淹一级 PSA 时，通常需

要进行专门的核动力厂巡访，以收集进行详细分析的支持信息。

（4）应对水淹事件序列缓解所需的额外的人员动作进行识别和评估，以确定水淹探测和控制措施的成功或失败概率，例如，电源的隔离和后续的电源再恢复。人员可靠性分析应考虑仪控设备可能出现的损坏以及水淹可能引起的误指示。

7.4.6.2 危险组合分析

（1）如果在内部事件一级 PSA 中未模化高能管道破裂引起的水淹及其造成的构筑物、系统和部件损坏，则在内部水淹一级 PSA 中应对其进行适当地考虑。

（2）如果有必要，因灭火系统投入导致的大量排水引起的水淹应在内部火灾一级 PSA 中进行适当地考虑。

7.4.7 内部水淹风险的定量化

用于水淹情景定量筛选的模型和结果，以及内部水淹一级 PSA 详细分析所建立的特定模型，都应纳入到完整的内部水淹一级 PSA 模型中。应对水淹导致的 CDF 进行定量化，包括识别支配性贡献因素（例如，水源、水淹情景）、审查筛选分析相关假设的合理性、开展不确定性分析和敏感性分析等。

7.4.8 内部水淹一级 PSA 的文档记录

应作好内部水淹一级 PSA 的文档记录，以便于内部水淹一级 PSA 的审查、应用和更新。文档记录中应包含以下信息:

（1）对评估内部水淹所用的具体方法和数据的描述;

（2）为考虑内部水淹影响而对内部事件一级 PSA 模型所作的具体修改;

（3）筛选分析中筛除特定水淹情景的理由;

（4）水淹情景详细分析的结果，包括情景的描述以及所作的重要假设;

（5）内部水淹一级 PSA 的最终结果，包括内部水淹导致的 CDF、定性的技术见解和建议等;

（6）支持水淹分析的核动力厂巡访报告。

7.5 其他内部危险

7.5.1 重物坠落分析

7.5.1.1 一级 PSA 通常主要关注反应堆压力容器内堆芯丧失冷却的情况，但核动力厂还可能会发生其他导致直接损坏的事件，例如，重物坠落在压力容器或执行关键安全功能的系统上。应考虑重物（例如，安全壳穹顶、反应堆压力容器顶盖等）可能发生的坠落事件，并评估其对执行关键安全功能所需构筑物、系统和部件造成损坏的可能性，或直接导致燃料组件机械损坏的可能性。

7.5.1.2 如果重物的运输路径不经过关键设备布置区域的上方，则可以筛除该重物坠落事件。

7.5.1.3 除堆芯外，还应考虑其他进行重物操作的区域。例如，一些核动力厂在汽轮机厂房大厅内布置余热排出系统，而它们很容易会受到重物坠落的影响（例如，试验设备可能掉落并损坏与压力容器相连的管道）。

7.5.1.4 应计算重物坠落事件对 CDF 的贡献，除非该事件在概率意义上可以忽略不计。

7.5.1.5 重物坠落一级 PSA 中核动力厂响应模型的详细程度应与预期的评价目的相匹配。

7.5.1.6 应针对核动力厂内所有的永久性起重设备，仔细识

别和检查可能发生重物坠落并对安全相关设备产生不利影响的区域。必要时，可以开展专门的核动力厂巡访。

7.5.1.7 应基于停堆期间的工作流程识别可能发生的起重作业并进行分析。

7.5.1.8 在计算重物坠落始发事件发生频率时，应考虑机械设备故障、人员失误和自动保护功能不可用等因素。如果在外部危险一级 PSA 中未考虑地震、飞机撞击等外部事件，则应在始发事件分析中对此类事件导致的重物坠落进行适当地考虑。

7.5.1.9 对于每个重物坠落事件，应保守假设以最大载荷发生坠落，或深入分析坠落物的特性及坠落原因（必要时）。应描述坠落物或重物坠落所产生的飞射物可能的方向、尺寸、形状和能量，并评估其对厂房构筑物及核动力厂的影响。

7.5.2 汽轮机飞射物分析

7.5.2.1 应评估汽轮机解体（例如，汽轮机转子故障）对 CDF 的贡献，除非该事件在概率意义上可以忽略不计。在分析汽轮机飞射物的影响时，应适当考虑氢气火灾和油类火灾对 PSA 相关设备的影响。

7.5.2.2 汽轮机解体的分析应涵盖汽轮机在正常转速值和超转速值下发生解体的情况。

7.5.2.3 应确定汽轮机解体后飞射物的散布状态，进而根据汽轮机的方向和位置，评估此类飞射物撞击厂房的概率。

7.5.2.4 应基于具有穿透厂房能力的飞射物的占比，确定导致厂房内安全相关设备发生故障的概率。

7.5.2.5 在分析的第一阶段，应只考虑一级 PSA 事件序列中

采信的设备。

7.5.2.6 飞射物导致的堆芯损坏频率可以通过飞射物撞击导致设备故障的概率及未因飞射物撞击发生故障的安全相关设备的随机故障概率与汽轮机解体频率进行叠加计算得到。

7.5.2.7 应进行核动力厂巡访，以确定构筑物、厂房及所选设备对汽轮机飞射物防护的相关假设。

7.5.3 内部爆炸分析

7.5.3.1 核动力厂的基本设计已经尽量降低和限制了内部爆炸发生的可能性及其影响，基于这种前提，可以对内部危险一级PSA的开展步骤进行适当调整以用于内部爆炸一级PSA的分析。由内部火灾引起的内部爆炸或由内部爆炸引起的内部火灾可以在内部火灾一级PSA中进行适当地考虑。

7.5.3.2 核动力厂厂房的设计基本上都会考虑对爆炸的预防和缓解。应对爆炸事件进行系统性的分析，描述潜在的爆炸源（爆炸材料的性质、数量和位置）、爆燃和爆炸对核动力厂的潜在影响（超压、冲击或拉力载荷、火灾或高温）及预防措施。内部爆炸一级PSA应依据上述分析过程中收集的信息和数据，对爆炸情景进行定性的筛选。

7.5.3.3 应进行核动力厂巡访，以识别和核查潜在的爆炸源。

7.5.3.4 对于筛选后保留下来的爆炸事件情景，应评估相关爆炸事件的发生频率。在发生频率的定量化中应考虑核动力厂内爆炸性材料的数量、爆炸地点的人员活动以及预防措施（氢气探测、爆炸性液体或气体泄漏的探测、通风等）的有效性。

7.5.3.5 如果有可能，应计算内部爆炸对CDF的贡献，除非

该事件在概率意义上可以忽略不计。

8 外部危险一级 PSA 的具体要求

8.1 概述

本章重点对大多数情况下不能筛除的外部危险给出具体的分析建议，包括:

（1）地震;

（2）强风;

（3）外部水淹;

（4）外部人为事件。

8.2 外部危险包络分析的一般规定

8.2.1 包络分析旨在减少需要详细分析的外部危险清单，以关注最重要的事故情景。需要通过包络分析来证明某特定外部危险导致的堆芯损坏频率相比于其他危险而言是不显著的。

8.2.2 在包络分析中，每个未被筛除的外部危险对核动力厂的全部潜在影响都应予以考虑[15]。

8.2.3 应对包络分析的外部危险的累积贡献进行计算，并将其保留在外部危险一级 PSA 的最终结果之中。

8.2.4 应对特定危险构建其相应的事故情景组，除非该危险对核动力厂的所有影响均可以被一个事故情景所包络，但这种情况通常不会出现。

---

[15] 影响类别的示例：
（1）丧失厂外电或全厂断电；
（2）最终热阱的降级或丧失；
（3）有害物质的爆炸或释放；
（4）核动力厂通风系统的降级或隔离（由于毒性影响的风险）。

8.2.5 在包络分析中，还应适当考虑外部危险的组合。

8.2.6 包络性估计应基于现实的或经论证偏于保守的模型和数据，包括:

（1）危险发生频率评估（即超越频率估计);

（2）危险对核动力厂的影响分析（即危险相关的荷载);

（3）核动力厂响应分析（即易损度);

（4）核动力厂外部危险一级 PSA 模型和数据等。

8.2.7 地震

根据经验，地震对堆芯损坏频率有显著贡献，因此应对地震进行详细分析。为了控制地震一级 PSA 的工作量，可以对一定范围内的地震进行包络分析。如果有必要，还应适当考虑地震引起的次生危险（例如，地震引起的火灾和水淹)。

8.2.8 强风

根据厂址位置的不同，应考虑以下几种强风事件并进行包络分析或详细分析:

（1）龙卷风及其伴随的其他影响;

（2）热带气旋（气旋、台风);

（3）温带强风（雷暴、飑线、锋面等)。

如果有必要，应适当考虑强风和其他危险现象的组合，并考虑可能存在的相关性（例如，强风和高水位)。

8.2.9 外部水淹

8.2.9.1 外部水淹一级 PSA 中所考虑的水淹相关危险主要包括:

（1）河流或湖泊的高水位;

（2）高潮;

（3）风暴;

（4）极端降雨;

（5）海啸;

（6）湖震;

（7）滑坡引起的水淹;

（8）人因引起的水淹（例如，大坝、堤、堤坝的垮塌或决堤）。

如果有必要，应适当考虑外部水淹和其他危险现象的组合，并考虑可能存在的相关性（例如，高水位和随之发生的大坝垮塌）。

8.2.9.2 强降雨及其他水淹导致的后果（例如，屋顶和核动力厂低洼区域的积水）也应纳入分析范围。

8.2.10 其他自然灾害

8.2.10.1 包络分析应参考尽可能完整的自然灾害清单（不只是地震、强风和外部水淹），应将附录I所列的自然灾害清单和核动力厂安全分析报告中所考虑的自然灾害作为识别外部危险的基础，同时还应考虑厂址特定的自然灾害（如果有）。

8.2.10.2 如果有必要，应适当考虑自然灾害与其他外部危险的组合，并考虑可能存在的相关性（例如，恶劣天气条件和强风）。

8.2.11 外部人为事件

外部人为事件的来源至少应考虑下列方面:

（1）从附近的核动力厂机组或设施蔓延而来的火灾;

（2）来自附近设施或由于运输或管道事故造成的固体物质或气体云的爆炸;

（3）来自附近设施或由于运输或管道事故造成的化学物质排放;

（4）飞机撞击;

（5）船舶对核动力厂进水构筑物的撞击;

除上述的外部人为事件外，下列危险也可以作为人为事件的来源:

（6）厂址上其他核动力厂的飞射物;

（7）厂址区域内外所进行的挖掘工作;

（8）电磁干扰（例如，雷达、无线电或移动电话产生的磁场或电场）。

8.3 外部危险的参数

8.3.1 一般规定

应定义用于表征外部危险引起损坏程度的最重要的参数，如果可能的损坏程度不能用一个单一参数进行表征，则应定义相关的多个参数。

8.3.2 地震

8.3.2.1 地震可以通过以下几个参数进行表征:

（1）烈度，用于衡量地震所产生的影响和可能引起的损坏程度的描述性指标;

（2）地面运动，例如，加速度、速度、位移;

（3）频率成分，通常采用响应谱给出;

（4）地震的完整时程，包括加速度、速度、位移等。

若在地震一级 PSA 中简化地使用单一参数（例如，峰值地面运动加速度）来表征地震可能导致的损坏程度，则在评估地震

产生的影响时还应考虑以下相关参数:

（1）在考虑继电器震颤、构筑物及设备的响应和易损度、人员失误的压力因子等问题时，地震的频率成分是必需的;

（2）在分析土壤液化、沉降、边坡失稳、塌陷、地表断裂或破裂等次生影响时，局部地质是一个需要考虑的重要因素。

8.3.2.2 当有可用数据支撑时，应使用谱加速度或选定频段上的均值谱加速度[16]。

8.3.2.3 分析中还应考虑地震引起的地表振动所带来的影响（即地震波可以到达地表的任意一处）。

8.3.2.4 地震引起的地面运动不应被筛除。

8.3.3 强风

应根据强风的类型考虑以下参数:

（1）阵风的动荷载和在给定时间段内（例如，10 分钟）的平均风荷载，是表征连续平移风的基本参数;

（2）龙卷风的旋转速度、压差和途经区域以及龙卷风携带飞射物的潜在影响（即大小和速度）是表征龙卷风的主要参数。

8.3.4 外部水淹

8.3.4.1 外部水淹可能导致的损坏可以通过流量、流速、水位、持续时间和波浪作用等因素进行表征。应采用上述参数的部分或全部以用于表征外部水淹的影响，不同外部水淹可能产生的影响通常可以采用如下参数进行表征:

（1）河流：水位、流量/流速和水淹持续时间;

（2）海/湖：水位、水淹持续时间和流速;

[16] 谱加速度可以比峰值地面加速度提供更全面的信息。

（3）波浪：高度、长度、周期、风速和方向;

（4）波浪爬高：高度、越浪量和每秒水量;

（5）湖震：振荡频率和浪高;

（6）冰：厚度和流速。

8.3.4.2 可能与水淹同时发生的风的速度、方向和持续时间，以用于必要时对潜在危险组合的考虑。

8.3.5 其他自然灾害

8.3.5.1 一个特定厂址上可能会有多种不同的自然灾害，应对每种自然灾害确定可包络其所有潜在影响的参数。

8.3.5.2 选取每种自然灾害的表征参数时，如果有必要，应适当考虑与其他危险进行组合影响分析的情况。

8.3.6 外部人为事件

8.3.6.1 对于每种外部人为事件，应根据其可能导致的损坏的具体特征来确定相关参数。例如:

（1）对于与运输相关的危险，其引起的实际危险往往是危险物质的爆炸或释放，因此应采用运输材料的数量或事故中可能产生的最大释放量作为其关键参数;

（2）对于来自附近工业设施的释放，材料的特性及事故中可能产生的最大释放量是较为合理的参数;

（3）对于撞击类的危险，应采用与撞击有关的参数作为关键参数，即撞击物的质量和速度（例如，运输船对进水口的撞击、飞机对构筑物的撞击）;

（4）若外部人为事件是由直接撞击（例如，飞机坠毁）后的爆炸所引起的，则关键参数应是会对构筑物造成损坏的所载燃

料量和重型发动机质量的组合;

（5）对于管道事故相关的危险，适用的参数是释放物质的装量及其性质和压力。

8.3.6.2 每种外部人为事件应适当考虑其可能产生的多种影响后果的组合。例如，飞机坠毁可能造成直接损坏、爆炸、火灾和振动；类似地，管道事故可能引起冲击波（爆燃或爆炸引起的冲击载荷）、火灾和振动，还可能会产生能够影响核动力厂不同区域的飞射物。在对外部人为事件进行参数化表征时，应尽可能全面地考虑所有直接影响和次生影响。无论事故的引发源是什么，应包括以下可以表征事故影响的参数:

（1）冲击载荷;

（2）热载荷;

（3）振动载荷;

（4）有毒气体的传播等。

8.3.6.3 对于气体云爆炸事故，应考虑其从源点向核动力厂的飘移过程。

8.3.6.4 必要时，还应适当考虑外部人为事件与其他危险的组合，并考虑可能存在的相关性（例如，化学物质释放、风速和风向）。

8.4 外部危险的详细分析

8.4.1 应对初步筛选后保留下来的所有外部危险进行详细分析。此外，如果针对特定的应用目标，仅根据包络分析的结果很难给出结论和建议，或很难判断危险或某事故情景对风险贡献的显著程度，也应进行详细分析。

8.4.2 若包络分析不能对整类危险而只能对其中一定强度等级的危险给出有意义的见解和结果，则应将该危险划分为多个子类，并对特定的子类或相关情景开展详细分析。

8.4.3 详细分析应基于现实的模型和数据，并建立可以模化所考虑外部危险的所有相关现象的详尽的一级 PSA 模型。

8.4.4 在进行详细分析时，若外部危险有共同的初始来源（例如，强风和闪电）或其他相关性（例如，降水造成的高水位和溃坝），则应适当考虑外部危险的组合影响。

8.5 外部危险发生频率评估

8.5.1 一般规定

8.5.1.1 外部危险发生频率评估旨在针对特定厂址的每个相关的外部危险，给出能够反映强度（由危险的某个参数表征）和危险发生频率之间关系（“危险性曲线”）的详细信息。外部危险频率的评估应以核动力厂及其周边环境的相关信息作为基础。

8.5.1.2 对于利用多个参数进行表征的外部危险，其中的部分参数可能在概率上存在相关性，因此，为简单起见，危险性曲线通常采用少数几个（通常是一个）参数来进行描述，而在响应分析和易损度评价中来考虑其他用于“完整”表征危险的参数。

8.5.1.3 危险性分析（特定强度危险的超越频率估计）应基于厂址特定的概率性评价，这种评价应能够反映近期的可用数据、厂址特定信息以及核动力厂实际的建造和运行情况（如果有相应的可用数据支持）。危险性分析中应包含历史数据和/或现象模型，并且应尽可能使用危险相关的最新数据和当前最先进的方法（如果有）。危险性分析中通常采用危险性曲线族来表征危险的不确

定性分布。

8.5.1.4 应进行时间趋势分析，以确认危险发生频率不存在持续增加的趋势。不应考虑危险发生频率近期内的短期下降趋势，除非能够明确和理解这种下降趋势是由非随机过程因素所引起的[17]。

8.5.1.5 若危险的发生频率是以局部区域数据或通用数据为依据来确定的，则需要进行关联分析，以确定这些数据对特定厂址的适用程度以及是否为最新的数据。局部区域数据和通用数据所带来的不确定性应体现在危险性曲线族的分布中。

8.5.1.6 如果采用专家参与的方式来开发所分析危险的危险性曲线，需要建立和遵循一套规范的专家参与程序。该程序应确保专家参与的流程是正式的、高度结构化和程序化的。

8.5.2 地震

8.5.2.1 地震的发生频率应基于厂址特定的多方案概率地震危险性分析。

8.5.2.2 应建立反映当前最新认知状态的综合数据库，包含以下内容:

（1）地质、地震和地球物理数据;

（2）厂址区域地形;

（3）厂址的地质特性和地球物理属性。

作为数据收集的一部分，应编制一份涵盖历史记录、地质鉴定和/或仪器记录的地震事件的目录。

8.5.2.3 应考虑所有可信的潜在破坏性地震源。地震源特征

[17] 例如，河床发生的可观测的变化可以用于论证相关运输事故发生频率的降低。

包括震源的位置和分布、最大震级和重现频率，此外，还应包括随机不确定性和认知不确定性[18]。

8.5.2.4 采用专家判断法确定震源特征的过程同样应遵循前述采用专家参与方式开发危险性曲线的质量保证要求。

8.5.2.5 表征地震的参数取值范围应足够大和足够详细，从而可以准确地评估地震风险，并应与物理数据及其解释相匹配。

8.5.2.6 对于危险性分析中所使用的参数值的下限，需要论证所有低于下限值的地震都不会对构筑物和设备造成损坏，包括厂址外的构筑物和设备（例如，输电线和输运有害物质的管道）。

8.5.2.7 在评估地震发生频率时，应确保所分析区域的大小和调查的范围足以涵盖所有可信的地震源。

8.5.3 强风

8.5.3.1 强风发生频率和强度的计算模型，应以能够反映近期可用的区域信息和特定厂址信息的特定数据为基础。分析应至少涵盖厂址发生过的最恶劣的天气条件，因而，在近期发生的强风频率短期下降的趋势不应在强风频率评估中占主导地位。

8.5.3.2 计算龙卷风的频率和强度时，应采用体现龙卷风发生情况、强度等的最新数据和当前最新的方法。具体应包括以下因素：

（1）龙卷风强度随发生频率的变化；

（2）受灾面积宽度与其长度的关系；

（3）龙卷风影响面积与其强度的关系；

[18] 随机不确定性是因外部危险的随机性或统计特征而引起的，认知不确定性是因当前知识状态的局限性而引起的。

（4）龙卷风强度沿其路径长度的变化;

（5）龙卷风强度沿其路径宽度的变化;

（6）龙卷风的压差沿其路径宽度的变化。

8.5.3.3 计算台风的频率和强度时，应采用体现台风发生情况、强度等的最新数据和当前最新的方法。具体应包括以下因素:

（1）中心压力分布;

（2）最大风圈半径;

（3）陆地上的衰减;

（4）风场特征;

（5）登陆位置等。

8.5.3.4 在评估温带风暴和其他涉及强直风的自然现象时，应采用适用于厂址的风速记录数据。在构建强风危险性曲线时，应采用保守的方式来考虑由于气象数据缺乏而带来的不确定性。

8.5.4 外部水淹

8.5.4.1 在评估厂址外部水淹的发生频率和后果时，应基于可反映近期的、可用的厂址特定信息的概率性分析。若厂址仅有短期的数据可用，应采用厂址区域的水淹数据，并论证这些数据的适用性(即通过关联性分析来确认厂址区域数据对厂址的适用性)。

8.5.4.2 应正确处理模型及参数取值中的不确定性，并通过不确定性传播得到危险性曲线族，从而可以得到均值危险性曲线。极端河流水淹频率及其后果分析应包括由单坝或梯级大坝失效引起的水淹。

8.5.4.3 在评估极端海洋水淹的发生频率和后果时，应基于

可反映近期的、可用的厂址特定数据的概率分析。这些数据应有其他沿海地区较长时期的统计数据作为支撑，并适当考虑该区域的地形（包括调整后的沿海区域和陆地地形）。必要时，还需要适当考虑高海浪和强风的组合。

8.5.4.4 在评估极端湖泊水淹的频率及后果时，应基于可反映近期的、可用的厂址特定数据的概率分析。分析中通常需要考虑风的作用而引起的波浪的影响，包括可能由龙卷风引起的排水等。

8.5.4.5 在评估海啸的频率及后果时，应基于有工程分析支持的、可靠的厂址区域数据，并应恰当地考虑海啸的频率和后果相关的不确定性。

8.5.5 其他自然灾害

8.5.5.1 应建立综合数据库以支持特定自然灾害的频率评估。数据库应包括对危险性曲线进行现实、有效的评估所需要的全部相关信息，特别是厂址附近及周边区域内发生过的历史灾害信息应在可用数据期内纳入数据库。

8.5.5.2 特定自然灾害发生频率的估计应使用厂址特定数据和区域数据，且在使用区域数据时应进行关联性分析。

8.5.5.3 在某些情况下，如果既没有厂址特定数据也没有区域数据，则可以使用通用数据。在使用通用数据时，应论证该数据对所分析厂址的适用性，并记录分析中采用的所有假设。

8.5.6 外部人为事件

应对相关的信息进行恰当的收集（最好以数据库的形式），以支持特定外部人为事件的频率评估。为了能够现实、有效地评

估外部人为事件的发生频率，至少应包括下列数据信息:

（1）核动力厂厂址半径范围内厂址内与厂址外储存的爆炸物、有毒有害物质的定性信息和定量信息:

1）潜在危险源（核动力厂厂址半径范围内):

— 厂址外，包括储油站、输油（气）管道、车辆运输、铁路运输、河流运输等;

— 厂址内，包括仓库（酸、联氨等）等。

2）潜在危险源与核动力厂的距离（以千米为单位):

— 与构筑物的距离;

— 与安全重要设备构筑物的距离;

— 与通风系统入口的距离。

（2）可能对核动力厂产生影响的军事设施或训练设施的位置，包括训练活动的频率;

（3）可能发生的事故、频率及其潜在后果（如，爆炸威力）。

8.6 构筑物和设备的易损度分析

8.6.1 一般规定

8.6.1.1 应尽可能采用核动力厂的特定信息（如果有）对构筑物和设备的易损度[19]进行评价。评价的详细程度应与分析的目的（包络分析或详细分析）相匹配，且应采用公认可接受的工程方法进行评价。评价中还应考虑核动力厂巡访中的发现项。

8.6.1.2 易损度分析不应仅局限于厂址内的构筑物，还应包括厂址外的构筑物。例如，电力输送线和有害物质的管道系统，因为它们的失效可能会引起核动力厂的始发事件（例如，丧失厂

[19] 易损度是指在给定的危险输入程度下，结构、系统或部件的条件失效概率。

外电或爆炸)。若这类构筑物的易损度较低，则它们失效的关联度可能会很高。

8.6.1.3 易损度分析中应体现基础信息的不确定性，特别是当使用的数据不是核动力厂的特定数据时（即采用通用数据)。

8.6.2 地震

8.6.2.1 地震易损度分析的构筑物、设备清单应涵盖地震一级 PSA 中模化的所有构筑物和设备。初始的设备清单应基于内部事件一级 PSA 模型给出，然后将清单范围扩大至涵盖因地震发生故障后对堆芯损坏频率有贡献的所有构筑物和设备及其组合。

8.6.2.2 应通过审查核动力厂设计文件和核动力厂巡访，识别在地震期间和地震后影响设备可运行性的构筑物和设备的所有现实的故障模式。

8.6.2.3 应对构筑物、设备和土壤相关的所有关键失效模式进行易损度分析。构筑物的失效模式，例如，滑移、倾覆、屈曲、超限位移；设备的故障模式，例如，锚固失效、与相邻设备或构筑物的碰撞、支承失效、功能故障；土壤的失效模式，例如，液化、边坡失稳、过度沉降。

8.6.2.4 应进行核动力厂巡访以支持易损度分析的开展。核动力厂巡访应关注锚固、侧向抗震支承及其与构筑物、系统和部件的潜在相互作用。特别需要关注无抗震要求的构筑物、系统和部件坠落至或撞击有抗震要求的设备的可能性。

8.6.2.5 如果有必要，核动力厂巡访还应适当关注地震可能引起的火灾和水淹。

8.6.2.6 地震易损度相关参数的计算（例如，构筑物抗震能力的中值及其不确定性）应尽可能以核动力厂的特定数据为基础，并利用实际地震中获取的相关数据、易损度试验数据和通用鉴定试验数据加以补充。

8.6.2.7 当利用通用数据将抗震能力较高的构筑物和设备筛除时，应论证所采用的通用数据是保守的，并且没有忽略核动力厂和厂址相关的真实特征。

8.6.2.8 构筑物和设备的地震响应评估，应以由地震动参数（例如，均值谱加速度）表征的厂址特定的地震反应谱为基础。

8.6.2.9 在分析构筑物和设备响应的联合概率分布时，应考虑所输入的地面运动、构筑物响应和土壤特性的不确定性。

8.6.2.10 对于出现在主导事故序列中的构筑物和设备，应确保相关的易损度参数是以核动力厂的特定信息为基础的，这对于正确评价地震在一级 PSA 中的贡献是非常重要的。

8.6.3 强风

8.6.3.1 在评估强风的影响时，应考虑安全相关构筑物周围的外部屏障（例如，墙和屋顶）、露天构筑物、系统或部件或其组合的具体特征，以及可能引起始发事件的强风飞射物所造成损坏的特征。应对核动力厂厂房及其周围环境进行调查，评估可能被强风刮起而成为飞射物的物体的类型和数量，并采用当前先进的技术方法估计飞射物撞击的概率。

8.6.3.2 应对强风下其故障可能引起始发事件的构筑物、系统或部件或其组合，进行核动力厂特定的、现实的易损度评价。

8.6.3.3 在评估构筑物和设备在强风下的易损度时，应尽可

能采用核动力厂的特定数据。评估中应考虑可能落入或落到安全相关构筑物上并对其造成损坏的非安全相关的构筑物。核动力厂巡访中的发现项是识别此类问题的重要信息来源。

8.6.3.4 应尽可能针对每个构筑物或设备的特定故障模式，构建相应的易损度曲线族，包含风速能力中值和不确定性（例如，对数标准差），以及构筑物或设备能力的不确定性。

8.6.4 外部水淹

8.6.4.1 应对河流高洪水水位情况下的水坝失效进行分析，并确定相应的发生频率[20]。

8.6.4.2 在评估构筑物和设备在外部水淹下的易损度时，应尽可能采用核动力厂的特定数据。评估中应考虑可能落入或落到安全相关构筑物上并造成损坏的非安全相关的构筑物。核动力厂巡访中的发现项是识别此类问题的重要信息来源。所有标高较低的构筑物（特别是入水口和最终热阱）都应纳入考虑范围内。

8.6.4.3 易损度分析中应包括浸没、波浪对构筑物和设备的动态载荷以及地基损坏（土壤侵蚀）。

8.6.5 其他自然灾害

对于其他自然灾害，可以参照地震、强风和外部水淹易损度分析的一般规定和建议，并选取适用的要求。

8.6.6 外部人为事件

对于外部人为事件，可以参照地震、强风和外部水淹易损度分析的一般规定和建议，并选取适用的要求。

[20] 水坝失效概率应针对不同的河流水位进行计算。通常假定河流水位高于水坝设计水位时水坝会发生失效。

8.7 外部危险与一级 PSA 模型的整合

8.7.1 一般规定

8.7.1.1 内部事件一级 PSA 模型是外部危险一级 PSA 模型的基础，可以对内部事件一级 PSA 模型进行修改，以考虑外部危险带来的差异。外部危险可能会引起不同类型的内部始发事件（例如，大 LOCA、小 LOCA、瞬态等），甚至可能直接导致堆芯损坏，这都需要通过内部事件一级 PSA 中相应的事件树进行评价。外部危险一级 PSA 模型应能够反映重要构筑物、系统和部件的危险性曲线和易损度分析结果，并考虑特定危险条件下所有可能的相关性、关联性和不确定性。还需要对恢复行动和紧急停堆后的人误事件概率进行修正，以体现外部危险对内部事件一级 PSA 模型所模化的恢复行动和人员动作的影响。

8.7.1.2 外部危险一级 PSA 模型应能够真实地反映核动力厂的实际建造和运行状态。

8.7.2 地震

8.7.2.1 通过对内部事件一级 PSA 模型的修改，将各分析要素中由地震引起的与内部事件一级 PSA 不同的方面反映到模型中。

8.7.2.2 对于超过一定震级（例如，设计基准地震的 50%）的地震，很多核动力厂都规定要求进行行政停堆，因此即使汽轮机发电系统具有很高的抗震能力，可以避免触发反应堆的自动紧急停堆，但地震一级 PSA 模型中仍需要考虑这种情况下核动力厂行政停堆的相关要求。

8.7.2.3 地震一级 PSA 模型应包括地震引起的所有可能导致

堆芯损坏的重要始发事件。尤其应对引起以下事故情景的始发事件进行建模:

（1）大型设备（例如，反应堆压力容器、蒸汽发生器、稳压器）的失效;

（2）不同尺寸和位置的冷却剂丧失事故。地震引起的小管线破裂导致的极小 LOCA 也应在地震一级 PSA 模型中予以考虑;

（3）丧失厂外电;

（4）瞬态（无论电力转换系统是否故障），包括各种支持系统的丧失。

8.7.2.4 如果地震引起的始发事件所导致的事故情景未包含在内部事件一级 PSA 模型中，则应添加相应的事件序列模型。应对内部事件一级 PSA 模型进行扩展以将地震的影响纳入一级 PSA 模型，从而涵盖更大范围的设备或故障模式，例如，非能动设备（构筑物、厂房、配电系统、电缆桥架、继电器震颤等）的故障。此外，还应考虑地震对堆内构件的影响，特别是地震导致的控制棒卡棒。

8.7.2.5 地震一级 PSA 模型应包含内部事件一级 PSA 模化的所有构筑物、系统和部件，以及因地震损坏可能会对事件序列进程产生影响的那些构筑物、系统和部件。

8.7.2.6 地震一级 PSA 模型应包括所有对堆芯损坏频率有贡献的非地震失效、设备/系统不可用和人员失误。

8.7.2.7 在地震引起的构筑物、系统和部件的失效模型中，应充分考虑厂房因地震失效而导致厂房内多个设备故障的相关失效。模型中如果不考虑这种相关性或降低这种相关性的重要程

度，需要对其合理性进行充分的论证。

8.7.2.8 地震一级 PSA 模型应恰当地将地震危险性评价、易损度、构筑物系统和部件间的相关性、非地震引起的故障、系统/设备的不可用和人员失误等问题融合到一起。

8.7.2.9 应针对恢复动作和人员失误概率进行全面的检查和必要的修正。地震一级 PSA 模型中应该删除在给定地震动水平下不能执行的恢复动作，或提高该恢复动作的失误概率。应根据特定的地震条件，对始发事件后续响应中可能发生的所有事故后人员失误事件进行修正和调整。地震对人员绩效形成因子的影响应至少考虑以下方面:

（1）地震后特定构筑物、系统和部件可达性;

（2）压力水平的升高;

（3）无指示或误指示;

（4）通讯系统故障;

（5）诱发的火灾和水淹的场景（如果有必要）;

（6）影响操纵员行为的其他因素。

8.7.2.10 在地震一级 PSA 模型中，应适当考虑地震引起火灾和水淹的情况。若可以证明地震引起的其他损坏可以包络地震引起的火灾和水淹的额外影响，则可以在模型中忽略这种叠加影响。

8.7.2.11 在定量化堆芯损坏频率时，除了给出最终的定量化结果外，还应给出每个事故序列和最小割集的重要信息。

8.7.2.12 地震一级 PSA 模型的整合和定量化过程，应保证各要素（即地震频率、地震易损度、相关性以及与系统分析等）的不确定性可以在模型中正确地传递，从而能够正确地表征堆芯损

坏频率的不确定性。

8.7.3 强风

8.7.3.1 强风一级 PSA 模型应包括强风引起的所有始发事件，并尽可能全面地模化强风导致的影响。

8.7.3.2 强风引起的事件序列分析中应包括厂址特定的危险性曲线和所有其失效会导致强风一级 PSA 中模化的设备发生故障的构筑物、系统和部件的易损度。还需要考虑不是由强风导致的设备不可用或故障以及人员失误。还应对人员失误概率进行调整，以考虑强风对人员绩效形成因子的影响。

8.7.4 外部水淹

8.7.4.1 外部水淹引起的事件序列分析中应包括厂址特定的危险性曲线和所有其失效可能导致外部水淹一级 PSA 中模化的设备发生故障的构筑物、系统和部件的易损度。还需要考虑不是由外部水淹导致的设备不可用或故障以及人员失误。还应对人员失误概率进行调整，以考虑外部水淹对人员绩效形成因子（特别是设备的可达性）的影响。

8.7.4.2 外部水淹引起的始发事件的事件序列建模中，应充分考虑不确定性、相关性和关联性。

8.7.5 其他自然灾害

应遵循地震、强风和外部水淹一级 PSA 模型整合的一般规定和建议。

8.7.6 外部人为事件

应遵循地震、强风和外部水淹一级 PSA 模型整合的一般规定和建议。

8.8 文档记录

8.8.1 一般规定

8.8.1.1 外部危险一级 PSA 的筛选分析、包络分析和详细分析的文档记录应便于同行评审，以及外部危险一级 PSA 的升级和应用。

（1）对特定外部危险一级 PSA 筛选分析的文档记录，应涵盖整个流程，包括所用方法、所作假设及其依据等方面的细节内容;

（2）阐述用于确定各外部危险的危险性曲线的方法，包括:

— 用于确定危险性曲线的数据;

— 输入条件和分析结果的技术解释;

— 采用的基本假设及相关的不确定性。

（3）给出需要进行易损度分析的构筑物、系统和部件的详细清单及其他相关信息，包括:

— 每个构筑物、系统和部件的位置;

— 用于易损度分析的关键假设和方法;

— 每个构筑物、系统和部件的关键故障模式;

— 分析所用信息的来源。

（4）应对不需要进行易损度分析的构筑物、系统和部件进行讨论，并给出将其从外部危险一级 PSA 模型中筛除的依据;

（5）完整清晰地记录对内部事件一级 PSA 模型所作的具体修改，并说明每处修改的理由;

（6）对包络分析和详细分析最终结果的文档记录，应包括外部危险相关的每个场景的堆芯损坏频率、重要最小割集和重要

事故序列。

8.8.1.2 应给出外部危险一级 PSA 的主要输出结果，包括:

（1）堆芯损坏频率及其不确定性分布;

（2）敏感性分析的结果;

（3）重要事故序列和重要最小割集的清单;

（4）对重要事故序列和重要最小割集的技术讨论;

（5）描述不确定性的主要贡献因素，包括认知不确定性和随机不确定性的贡献因素。

8.8.2 地震

8.8.2.1 描述表征地震源特征所用的具体方法，并给出相关参数。应详细记录对模型输入条件和分析结果的具体解释。

8.8.2.2 地震一级 PSA 的文档记录中应包括以下信息:

（1）地震一级 PSA 中所考虑的构筑物、系统和部件清单;

（2）各构筑物、系统和部件的易损度特征及其分析基础;

（3）在地震一级 PSA 中所模化的地震范围引起的损坏的概率;

（4）各构筑物、系统和部件的位置及其重要故障模式;

（5）为反映地震影响对内部事件一级 PSA 模型所作的具体修改;

（6）地震一级 PSA 中模化的相关性（特别是空间相互作用）的全面信息，以及用于排除或降低相关性影响的所有假设。

8.8.2.3 应详细阐述筛除任一构筑物、系统和部件的依据。

8.8.2.4 记录地震易损度分析所采用的方法和程序，应包括如下内容:

（1）地震响应分析;

（2）筛选的步骤;

（3）核动力厂巡访;

（4）设计文件审查;

（5）构筑物、系统和部件关键故障模式的识别;

（6）构筑物、系统和部件易损度的计算。

8.8.2.5 应详细记录核动力厂巡访的程序、人员组成及巡访结果和结论。

8.8.3 强风

强风一级 PSA 的文档记录应便于强风一级 PSA 审查、应用和更新，应包括以下内容:

（1）阐述确定强风危险性曲线所用的方法和数据;

（2）为反映强风相关影响对内部事件一级 PSA 模型所作的具体修改;

（3）分析中考虑的所有构筑物、系统和部件的清单，并给出筛除某一构筑物、系统和部件的依据;

（4）强风一级 PSA 模型中构筑物、系统和部件的强风易损度分析所采用的方法和数据;

（5）强风一级 PSA 堆芯损坏评价的最终结果及有用的中间结果。

8.8.4 外部水淹

外部水淹一级 PSA 的文档记录应便于外部水淹一级 PSA 审查、应用和更新，应包括以下信息:

（1）阐述确定外部水淹危险性曲线所用的方法和数据;

（2）为反映外部水淹相关影响对内部事件一级 PSA 模型所作的具体修改;

（3）分析中所考虑的构筑物、系统和部件的清单，并给出筛除某一构筑物、系统和部件的依据;

（4）外部水淹一级 PSA 模型中构筑物、系统和部件的水淹易损度分析所采用的方法和数据;

（5）外部水淹一级 PSA 堆芯损坏评价的最终结果及有用的中间结果。

8.8.5 其他自然灾害

应遵循地震、强风和外部水淹一级 PSA 对文档记录方面的一般规定和建议。

8.8.6 外部人为事件

应遵循地震、强风和外部水淹一级 PSA 对文档记录方面的一般规定和建议。

附录 I 内外部危险通用清单示例

表 I.1　内外部危险通用清单示例

序号	危险	定义与影响	备注
气象自然灾害			
A1	强风	根据强风对核动力厂造成的损坏来定义。包括由风压引起的直接损坏和风载飞射物引起的间接损坏。	不包括龙卷风（A2），也不包括雪暴（含在 A7 中）、盐暴（A12）或沙暴（A13）中的非风力影响，但需要考虑这些危险中风的影响。风暴潮的影响由高水位危险（W3）包络。
A2	龙卷风	根据龙卷风对核动力厂造成的损坏来定义。由于该危险在持续时间、风速和发生频率方面的特殊性，应将其与其他强风事件进行区分。	
A3	高气温	根据高气温对核动力厂造成的损坏来定义。	高水温对核动力厂的影响在（W4）中单独处理。
A4	低气温	根据低气温对核动力厂造成的损坏来定义。	低水温（W5）或冰灾（W7，W8，W9）对核动力厂的影响单独处理。
A5	极端气压（高/低/梯度）	根据高气压、低气压或快速压力变化对核动力厂造成的损坏来定义。	
A6	极端降雨	根据极端降雨对核动力厂造成的损坏来定义。	包括降雨对构筑物产生的载荷和降雨引起的水淹造成的损坏。

序号	危险	定义与影响	备注
A7	极端降雪（包括暴风雪）	根据极端降雪（包括暴风雪）对核动力厂造成的损坏来定义。	暴风雪引起的风力影响由强风（A1）包络。雪的融化引起的水淹效应由极端降雨引起的水淹效应（A6）包络。
A8	极端冰雹	根据极端冰雹对核动力厂造成的损坏来定义，包括冰雹引起的构筑物载荷所造成的损坏。	由冰雹融化引起的水淹效应由极端降雨（A6）涵盖。所有对最终热阱可能产生的影响都由冰灾（W7，W8，W9）包络。
A9	雾	根据雾对核动力厂造成的损坏来定义。	
A10	霜	根据霜对核动力厂造成的损坏来定义。	
A11	干旱	定义为一个连续性干旱期，使湖泊、河流和开放水域的水位下降。	高气温（A3）或高水温（W4）对核动力厂的影响在这些事件中进行分析。其对水位（热阱）没有影响。
A12	盐暴	对核动力厂构筑物形成盐覆盖的风暴。	来自盐暴的风力影响由强风（A1）包络。
A13	沙暴	根据沙暴所载沙量对核动力厂造成的影响来定义。	来自沙暴的风力影响由强风（A1）包络。
A14	闪电	根据闪电对核动力厂造成的损坏来定义。包括导致的直接影响（例如，引起构筑物损坏或引起丧失厂外电等）和间接影响（例如，闪电引起的电磁馈电火灾）。	闪电引起的火灾由外部火灾（G7）和内部火灾分析包络。

序号	危险	定义与影响	备注
A15	陨石	根据陨石撞击对核动力厂造成的损坏来定义。	
地表自然灾害			
G1	地壳上升	根据地壳上升对核动力厂造成的损坏来定义。	
G2	土壤霜冻	根据土壤霜冻对核动力厂造成的损坏来定义。	
G3	动物	根据动物对核动力厂造成的损坏来定义。	鱼类、贻贝等对进水口的影响由水中有机物（W10）包络。
G4	火山爆发	根据火山爆发对核动力厂造成的损坏来定义。	
G5	雪崩	根据雪崩对核动力厂造成的损坏来定义。	
G6	水面以上滑坡	根据水面以上滑坡对核动力厂造成的损坏来定义。	
G7	外部火灾	根据来自厂外、厂址区域内部或外部的火灾对核动力厂造成的影响来定义。	从厂址另一核动力厂蔓延而来的内部火灾（M15）将单独处理。其他外部危险（M2，M11，M20）引起的火灾作为相应外部危险的一部分进行分析。内部火灾作为内部危险 PSA 的一部分进行分析。
G8	地震	根据地震对核动力厂造成的影响来定义。	
G9	岩溶	根据侵蚀引起的裂缝、落水洞、	

序号	危险	定义与影响	备注
		地下暗流和洞穴对核动力厂造成的损坏来定义。	
水文自然灾害			
W1	强水流（水下侵蚀）	根据强水流对核动力厂构筑物造成的损坏来定义。	水面以下滑坡（W6）的影响单独处理。
W2	低水位	根据低水位对核动力厂造成的损坏来定义。	由于地壳上升引起的水位下降由地壳上升（G1）包络。
W3	高水位	根据高水位对核动力厂造成的损坏来定义。高水位可能是由风暴潮、波浪或湖震引起的，也受潮汐变化的影响。	
W4	高水温	根据高水温对核动力厂造成的影响来定义。	高气温（A3）对核动力厂的影响单独处理。
W5	低水温	根据低水温对核动力厂造成的影响来定义。	低气温（A4）或冰灾（W7，W8，W9）对核动力厂的影响单独处理。
W6	水面以下滑坡	根据水面以下滑坡对核动力厂造成的影响来定义。	水面以下滑坡可能是由于水面以上的原因造成的，例如长时间的强降水。水下侵蚀对核动力厂的影响被视为强水流危险（W1）的一部分。
W7	冰盖	根据冰盖对核动力厂造成的影响来定义。	不包括由冰层（W8）和冰障（W9）造成的影响。
W8	冰片	根据冷却水进水口中的冰片对核动力厂的影响来定义。	
W9	冰障	根据冰障对核动力厂造成的影	

序号	危险	定义与影响	备注
		响来定义。	
W10	水中有机物	根据进水口有机物对核动力厂造成的影响来定义，包括藻类、海藻、鱼类、贻贝、海蜇等。	
W11	腐蚀（来自盐水）	根据腐蚀对核动力厂造成的影响来定义。	
W12	船舶排放的固态或液态（非气态）杂质	根据从船上排放到水中的固态或液态（非气态）杂质对核动力厂造成的影响来定义。	
W13	化学物质的水中排放	根据化学物质向水中的排放对核动力厂造成的影响来定义，关注水质的污染。排放可能由于船舶事故造成，也可能源自陆地。	不包括排放的固态或液态（非气态）杂质（W12）产生的影响。
W14	海啸	根据高水位和波浪作用对核动力厂造成的损坏来定义。	
厂址外事故			
M1	船舶撞击的直接影响	根据船舶撞击的直接影响来定义。	不包括与船舶事故（爆炸、污染、进口堵塞或有毒气体释放）有关的释放后果，这些危险在（M2，M3，W12，W13）中单独处理。
M2	运输事故引起的爆炸	根据厂外地面运输或海上、湖泊、河流运输事故引起的爆炸对核动力厂造成的损坏来定义。损坏可能由压力冲击或飞射物撞击导致。	不包括由飞机坠毁（M20）或管道事故引起的爆炸（M5）造成的损坏。运输事故引起的化学品释放（M3）包络分析

序号	危险	定义与影响	备注
			化学释放产生的毒性损害。
M3	运输事故引起的化学品释放	根据厂外地面运输或海上、湖泊、河流运输事故引起的化学物质释放对核动力厂造成的毒性损害来定义。	运输事故的爆炸效应由运输事故引起的爆炸（M2）包络。
M4	厂外爆炸	根据厂址外固体物质或气体云的爆炸（爆燃或爆炸）对核动力厂造成的损坏来定义。损坏可能由压力冲击或飞射物撞击导致。	不包括运输事故引起的爆炸（M2）或管道事故引起的爆炸（M5）。化学释放产生的毒性损害在厂址外的化学释放（M6）中包络。
M5	管道事故引起的爆炸	根据管道事故后爆炸（爆燃或爆炸）对核动力厂造成的损坏来定义。损坏可能由压力冲击或飞射物撞击导致。	化学释放产生的毒性损害在管道事故后的化学释放（M7）中包络。在厂址外或厂址内的爆炸效应分别由厂外爆炸（M4）和厂内爆炸（M11）包络。运输或管道事故后的毒性损害在运输事故引起的化学品释放（M3）和管道事故后的化学释放（M7）中包络。
M6	厂址外的化学释放	根据厂址外的化学释放对核动力厂的毒性损害来定义的。这些释放可能源自核动力厂外的工业过程事故或源自核动力厂外贮存物质的泄漏。	

序号	危险	定义与影响	备注
M7	管道事故后的化学释放	根据管道事故后化学释放对核动力厂的毒性损害来定义。	管道事故的爆炸效应由管道事故引起的爆炸（M5）包络。
M8	军事活动的飞射物	根据来自军事活动的飞射物对核动力厂造成的影响来定义。	对供电和热阱的影响由其他危险所包络。
M9	挖掘工作	根据在厂址区域内外的挖掘工作对核动力厂造成的影响来定义。	
厂址内事故			
M10	厂址内重型运输的直接影响	根据厂址内但在厂房外的重型运输对核动力厂造成的直接影响来定义，也包括安全壳外部维护平台的运输。	核动力厂厂房内的重型运输作为内部危险 PSA 的内容进行分析。
M11	厂内爆炸	根据厂址内但在厂房外的固体物质或气体云爆炸（爆燃或爆炸）对核动力厂造成的损坏来定义。损坏可能由压力冲击或飞射物撞击导致。	核动力厂厂房内的爆炸作为内部危险 PSA 的内容进行分析。
M12	厂内管道事故引起的爆炸	根据厂址上管道破裂后爆炸（爆燃或爆炸）对核动力厂造成的损坏来定义。损坏可能由压力冲击或飞射物撞击导致。	
M13	厂内的化学释放	根据厂址内化学释放对核动力厂造成的毒性损害来定义。	释放可能源自核动力厂内的工业过程事故，也可能源自贮存在厂址内但在厂房外的物质的泄漏。贮存在厂房内物质的化学释放作为内部危险

序号	危险	定义与影响	备注
			PSA 的内容进行分析。
M14	厂内管道事故引起的化学释放	根据厂址内管道事故后的化学释放对核动力厂造成的毒性损害来定义。	
M15	由厂址其他机组蔓延而来的内部火灾	根据源自厂址另一机组的火灾对核动力厂造成的影响来定义。	外部火灾（G7）单独处理。其他外部危险（M2、M11、M20）引起的火灾可以作为相应外部危险的一部分进行分析。
M16	厂址其他机组的飞射物	根据另一机组产生的飞射物对核动力厂造成的损坏来定义。	
M17	厂址其他机组的漫延水淹和恶劣环境	根据来自其他机组的水淹漫延对核动力厂造成的损坏来定义。	
M18	厂址内的挖掘工作	根据厂址内挖掘工作对核动力厂造成的影响来定义。	
飞行器坠毁			
M19	卫星坠毁	根据卫星坠毁对核动力厂造成的损坏来定义。	
M20	飞机坠毁	根据厂址区域内的飞机坠毁对核动力厂构筑物造成的损坏来定义，包括商用、私人或军用飞机。	
其他外部人为事件			
M21	磁干扰	根据人因所致的磁场或电场对核动力厂造成的影响来定义。主要包括雷达、无线电和移动电话	

序号	危险	定义与影响	备注
		等。	
M22	核动力厂上游大坝决堤	根据高水位和波浪对核动力厂厂房、系统和部件造成的损坏来定义。	

备注：列表清单中不包括源自核动力厂厂房内的内部危险。

附录 II 火灾蔓延事件树示例

图 II.1 给出了如何利用事件树方法分析火灾事故缓解和火灾蔓延的示例。图 II.1 中的火灾蔓延事件树包含了从火灾发生开始的各相关现象。事件树中对早期火灾探测和晚期火灾探测进行了区分，因为这关系到控制或扑灭火灾成功概率的分析。火灾蔓延场景与房间关闭与否及关闭程度直接相关。在进一步建模过程中还应考虑消防设施的可用性，同时还要适当考虑消防设施的投入对安全有关物项可能造成的损坏。

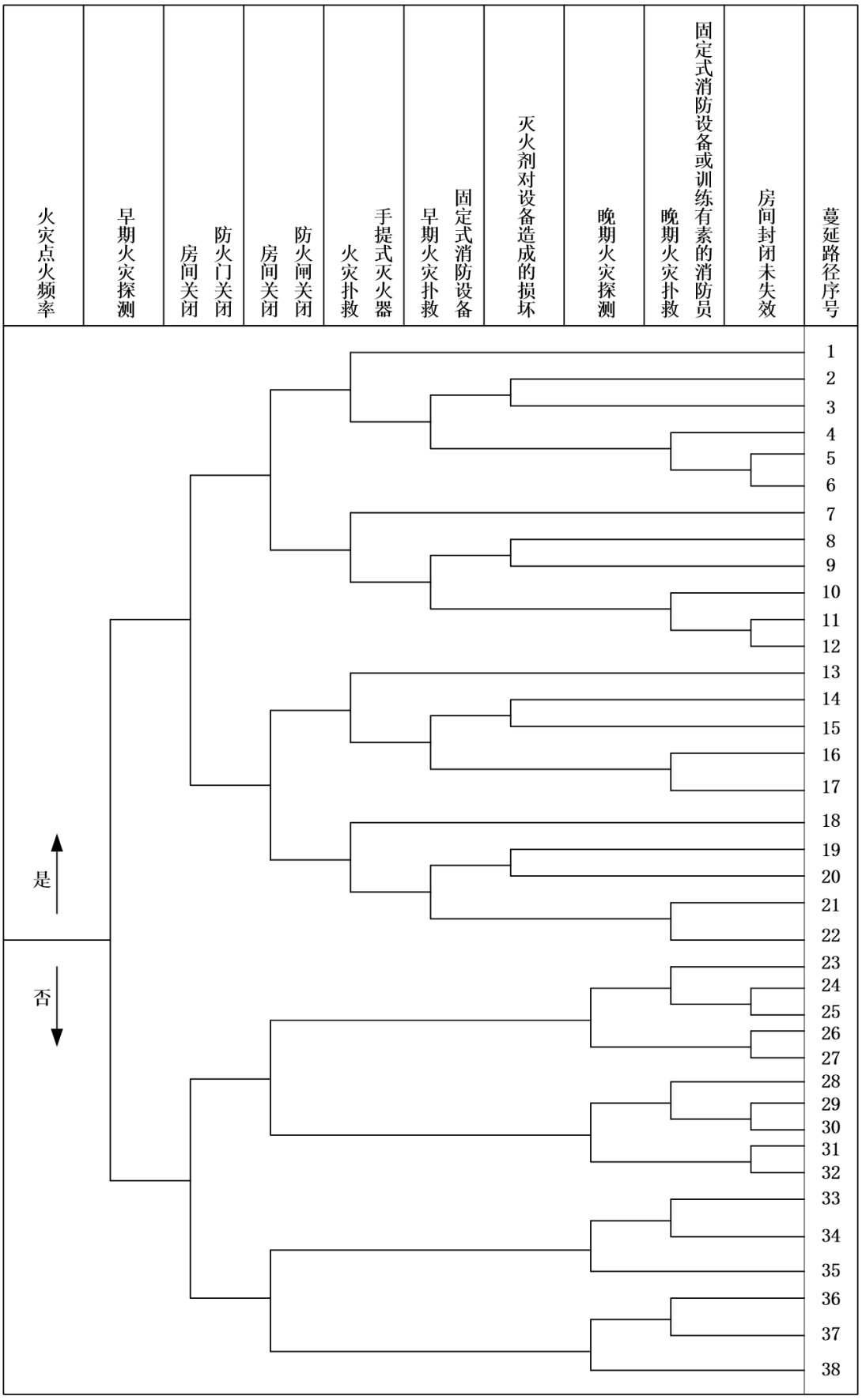

图 II.1　火灾蔓延事件树示例