附件 2

核安全导则 HAD102/XX

核动力厂二级概率安全分析

国家核安全局 20XX 年 XX 月 XX 日批准发布

（征求意见稿）

国家核安全局

核动力厂二级概率安全分析

（201X 年 XX 月 XX 日国家核安全局批准发布）

本导则自 201X 年 XX 月 XX 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二级概率安全分析（PSA，Probabilistic Safety Analysis）工作的开展提供指导。

1.1.2 附录 I 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（例如，集中供热或海水淡化）而设计的陆上固定式水冷反应堆核动力厂。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，对在运核动力厂所开展的二级概率安全分析工作也可参照执行，但需要考虑在运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反应堆堆芯放射性物质的二级概率安全分析，不涉及核动力厂乏燃料水池、放射性废物等堆芯外放射源的二级概率安全分析。

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二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以核动力厂反应堆堆芯全范围一级 PSA 为起点，开展二级概率安全分析的基本技术要素及实施步骤，直到生成详细的源项清单，作为三级 PSA 的输入。最后给出了二级概率安全分析的应用建议。

1.2.6 本导则是对核安全导则《核动力厂一级概率安全分析》

的继承和发展，其中已经阐述的 PSA 通用技术要素和项目管理要求本导则不再赘述。

2 二级 PSA 的总体考虑

2.1 二级 PSA 的目标

2.1.1 在核动力厂开展二级 PSA 项目之前，应首先明确开展二级 PSA 的目标。二级 PSA 目标不同，二级 PSA 输入的要求和侧重点会有不同，技术要素和实施步骤也会有所差异。因此在开展二级 PSA 时，应首先明确二级 PSA 的所有预期目标。这些目标包括但不限于:

（1）获取严重事故进程和安全壳性能的见解;

（2）识别核动力厂在严重事故下受到的挑战和安全壳的薄弱环节;

（3）检验其是否符合我国核安全监管机构制定的风险准则，这些风险准则通常与大量释放频率和早期大量释放频率有关;

（4）确定安全壳主导失效模式和频率，评估相关的放射性释放频率和量级;

（5）评价现象、系统和模型假设等各种不确定性对核动力厂安全的影响;

（6）确定对严重事故是否已经采取足够的措施，以缓解事故的影响;

（7）为应急预案的编制提供输入;

（8）为核动力厂开发事故管理指南和制定事故应对策略提供输入;

（9）为核动力厂确定降低风险的特定措施提供输入;

（10）为确定相关研究活动的优先次序提供输入;

（11）为三级 PSA 提供输入;

（12）为核动力厂的环境影响评估提供输入。

2.1.2 应根据二级 PSA 分析目标建立模型。模型应尽可能反映现实情况，避免由于采用过于保守的假设，使结论与实际情况不符。

2.1.3 用于论证分析目标的二级 PSA 结论应考虑不确定性的影响，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。

2.2 二级 PSA 的范围

2.2.1 二级 PSA 的范围由其特定的目标和 PSA 的开展计划确定。通常，实施二级 PSA 有两种情况。第一种情况是作为全范围 PSA 的组成部分，二级 PSA 与一级 PSA 一起开展。此时应在一级 PSA 中纳入二级 PSA 的要求，以保证在一级 PSA 中尽可能考虑所有对安全壳响应及源项分析重要的核动力厂相关特性。第二种情况是二级 PSA 在已有一级 PSA 的基础上开展，此时应通过二级 PSA 增加一些安全壳及其安全系统状态的分析。一级 PSA 和二级 PSA 间的接口应通过核动力厂损伤状态（PDS，Plant Damage State）的定义和量化来实现。二级 PSA 应充分考虑一级 PSA 模型的初始状态和边界条件及其与一级 PSA 之间的相关性。确定二级 PSA 的范围时，还应考虑预期要开展的三级 PSA 的输入需求。二级 PSA 的输出应尽可能满足三级 PSA 的输入需求。

2.2.2 当 PSA 的范围包括了内部或外部危险（如：火灾，地震等），但它们对于放射性包容功能的潜在影响以及它们可能引起的相关性失效（如由于电缆着火所导致的安全壳隔离系统失

效、由于地震所导致的安全壳结构损伤等）没有在一级 PSA 中包含时，应在二级 PSA 中进行考虑。

2.3 风险准则

2.3.1 如果 PSA 的目标是为下列判断提供支撑，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:（1）评价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。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。

2.3.2 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。

2.3.3 核安全监管机构对二级 PSA 规定的风险准则通常采用放射性物质大量释放频率或大量早期释放频率进行表征。我国对新建核动力厂提出的核动力厂放射性物质大量释放目标值为 10^{-6}/堆·年。

2.4 二级 PSA 的维护和更新

2.4.1 应对 PSA 进行定期的维护和更新，以体现核动力厂设计和运行实践的变化以及经验和技术进步的反馈。

2.4.2 在分析和形成见解的过程中，应确保不同技术领域的分析者沟通顺畅，应用的方法协调一致，各项任务开展平衡合理。同时，还应保持 PSA 不同学科之间于技术上的独立性。

2.4.3 应使二级 PSA 分析中得到的相关见解正确地被核动力

厂的管理与运行人员及核安全监管人员或其他相关人员理解。

2.4.4 应依据二级 PSA 结果的含义及其潜在用途，建立适当的技术评估体系以满足独立验证要求。必要时，应预先建立独立评价和对比研究的程序或规定。二级 PSA 中所采纳的专家判断应通过文档记录的形式进行取证和管理。

2.5 团队选择与组织

2.5.1 二级PSA团队的专业技术水平可以因开展二级PSA时核动力厂所处的阶段、二级 PSA 分析范围和预期用途而有所差异，但应确保团队在如下方面具备足够的专业技术水平，并包含如下成员:

（1）核动力厂设计和运行方面:

核动力厂设计及运行专家、操纵员、安全壳相关系统专家、运行规程和严重事故管理指南专家;

（2）严重事故现象和安全壳完整性方面:

安全壳性能、严重事故现象、严重事故分析不确定性、主导事故进程的化学和物理过程、安全壳荷载、放射性释放和严重事故分析计算程序等方面的专家; 结构设计、安全壳承压能力和失效模式方面的专家;

（3）PSA 技术方面:

事件树分析、故障树分析、人因、不确定性分析、统计方法、专家启发和判断过程、PSA 软件和一级 PSA 方面的专家等。

2.6 质量保证要求

《核动力厂一级概率安全分析》提出的“PSA 质量保证要求”同样适用于二级 PSA，本导则不再赘述。

2.7 PSA 文档的规定

《核动力厂一级概率安全分析》提出的“PSA 文档的一般规定”同样适用于二级 PSA，本导则不再赘述。

3 二级 PSA 的核动力厂信息收集

3.1 确定与严重事故相关的重要设计

3.1.1 二级 PSA 团队应熟悉核动力厂，确定影响严重事故进程、安全壳响应和放射性物质在安全壳内迁移的核动力厂系统、构筑物（反应堆厂房和辅助厂房、二次安全壳或其他相关构筑物和厂房等）、设备和运行规程。

3.1.2 二级 PSA 团队应确定能够影响严重事故进程的核动力厂特性，必要时应开展进一步研究。对严重事故进程和缓解有重要意义的关键核动力厂设计特征包括:

（1）反应堆压力容器下部区域的特征。当堆芯熔融物从反应堆压力容器的底部流出时，这个区域的特征会影响到熔融物扩散的范围和熔融物的可冷却性。

（2）从反应堆压力容器下部区域到安全壳主空间的路径特征。流动的限制或者流道的其他几何影响可能降低下封头失效后的堆芯碎片的分布范围，这对于轻水堆中的高压熔融物喷射尤其重要。

（3）安全壳内结构布置特征。高度分隔的安全壳结构将限制可燃气体的混合以及在安全壳气空间的扩散程度。

（4）可能导致安全壳旁路序列的特征。

（5）影响严重事故进程和缓解的核动力厂设计特征示例如表 1 所示。

关键设计特征	注释
反应堆	
反应堆堆型	PWR/VVER /其他
功率水平	稳态下总热功率
燃料类型/包壳类型	氧化物、混合氧化物/锆合金、不锈钢
堆芯	
燃料/包壳的质量	实际运行值
燃料组件几何形状	实际运行值
控制棒类型和数量	实际运行值
反应堆功率的空间分布	典型的轴向&径向功率峰值因子
衰变热	随时间变化的衰变热水平
放射性物质装量	堆芯内放射性物质总量
反应堆冷却剂系统（RCS）	
反应堆冷却剂和慢化剂类型	水、重水、氦气和其他
反应堆冷却剂/慢化剂体积	按照设计和制造的
安注箱容量和压力设定值	实际运行值
RCS降压装置/规程	具体设定点/规程
卸压能力	实际运行值
连接RCS的安全壳贯穿件的隔离	安全壳旁路的可能性
安全壳*	
安全壳几何结构	内部空间的形状和隔离
安全壳自由容积	考虑结构占位的建造值
安全壳设计压力/温度	极限承载力的现实评估值
安全壳材料组成	钢材、混凝土和其他
运行压力/温度	实际运行值
氢气控制设备	惰化措施、点火器、非能动复合器和其他
安全壳冷却剂能力和设定值	实际运行评估
混凝土成分	具体的化学成分

关键设计特征	注释
地坑、体积和位置	具体的几何形状
安全壳边界相邻部分	到反应堆压力容器和堆腔/基座的距离
安全壳通风规程和位置	通风管线位置和启动规程
外部危险响应	由地震，水淹事件引起的结构破坏
潜在的安全壳隔离失效	安全壳隔离的贯穿件排列和密封材料的可靠性

* 对没有承压能力的安全壳，所列的信息需要调整。

表 1 影响严重事故进程和缓解的核动力厂设计特征示例

3.1.3 除了核动力厂的设计特征外，还应考虑核动力厂相关运行规程和严重事故管理指南。对于在设计阶段暂时无法获取的信息，可以参考相似核动力厂的经验反馈。

3.2 收集严重事故的重要信息

3.2.1 PSA 团队应在全面理解影响严重事故行为和放射性物质释放的核动力厂设计特性的基础上，收集和整理开展特定核动力厂二级 PSA 所需要的数据。所需数据与 PSA 分析范围和计算工具相关，也受核动力厂严重事故进程的特定分析模型的影响。

3.2.2 应从合格的信息来源中获取数据。获取数据的参考文献应作为 PSA 文件的一部分。可用的信息来源主要包括:

（1）设计和/或核动力厂执照申请文件;

（2）施工图;

（3）核动力厂特有的运行、维修或试验程序;

（4）工程计算或分析报告;

（5）核动力厂巡访时的发现;

（6）建造标准;

（7）厂家技术资料;

（8）与运行人员的访谈;

（9）场区移动设施的布置图;

（10）应急预案和应急执行程序的规定等。

3.2.3 二级 PSA 使用参考核动力厂的数据时，应将两个核动力厂的数据进行比较，以确定两个核动力厂是否真的“相似”及因此是否有相似的薄弱环节。通过参考核动力厂的数据并比较得出二级 PSA 结论时，应给出对比的设计特征及可比性说明。可以对比的设计特性示例及比对说明如表 2 所示。

参数和设计特征	可比性说明
反应堆功率/RCS容积比	事故进程时间，恢复动作时间
反应堆功率/安全壳容积比	安全壳负载比例
锆质量/安全壳自由容积比	燃烧的可能性和安全壳负载比例
压力容器下部到安全壳的路径	熔融物可能的分布和高压熔融物喷射
混凝土成分	堆芯熔融物－混凝土相互作用时，不可凝气体的生成和放射性物质的释放

表 2 核动力厂设计特征对比及可比性示例

4 与一级 PSA 的接口

4.1 概述

4.1.1 一级 PSA 确定了大量导致堆芯损伤的事故序列。二级 PSA 与一级 PSA 接口是将一级 PSA 的信息有效地传递到二级 PSA，从而减少二级 PSA 中对这些事故序列评估事故进程、安全壳响应和放射性核素释放的工作量。在一级 PSA 和二级 PSA 模型之间传递信息时，应识别需要考虑的相关性。这些相关性包括始发事件和支持系统的相关性、已发生的设备失效引起的相关性失效、操纵员动作的相关性（包括可用时间及资源限制）、功能相关性（包括核动力厂状态的降级）和共因相关性等。应给出

处理一级 PSA 和二级 PSA 模型之间相关性的明确方法，例如：

（1）在二级 PSA 中考虑；

（2）扩展一级 PSA；

（3）构建桥树；

（4）通过 PDS 进行信息传递；

（5）上述方法的综合。

4.1.2 一级和二级 PSA 接口的典型方式是将一级 PSA 事故序列（或者单个割集）按照特征量属性进行归并得到 PDS，以减少二级 PSA 分析序列的数量，并保留二级 PSA 分析所需的初始和边界条件。PDS 代表了具有相似事故进程的一组事故序列，它们对安全壳施加了相似的负荷，进而导致相似的事件进展和放射性源项。PDS 的属性包括影响事故进程、安全壳响应或者放射性物质向环境释放等的各种因素，这些因素为开展严重事故分析提供了边界条件。

4.2 功率工况内部始发事件 PSA 的 PDS

4.2.1 当功率工况内部一级 PSA 没有描述安全壳系统或其他不会直接影响堆芯损坏的系统状态时，应扩展一级 PSA 以考虑在 PDS 定义中关注的特征及其属性。功率工况内部始发事件 PSA 的 PDS 定义需考虑的特征及其属性示例由表 3 给出。PSA 应用需要时，PDS 还应考虑其他属性。

特征	属性
始发事件	大破口失水事故； 小破口失水事故； 安全阀/泄压阀卡开导致的破口； 瞬态； 旁通类事件。

特征	属性
堆芯损坏时RCS系统的压力	高； 中； 低。
应急堆芯冷却和其他冷却系统的状态（堆芯损坏的时间）	所有安注早期丧失； 安注直接注入阶段成功，但是再循环阶段失效（随后堆芯损坏）； 堆芯损坏或反应堆压力容器损坏后，可提供紧急堆芯冷却功能； 蒸汽发生器冷却可用。
安全壳专设安全设施状态	喷淋（如果有）： 始终保持运行状态； 需求失效； 直接注入阶段成功，但是未成功切换至再循环冷却。
	氢气点火器/复合器（如果有）： 始终有效； 需求失效； 后期失效。
	通风/排放系统： 始终可用； 需求失效； 后期失效。
安全壳状态	完整且堆芯开始损坏时即隔离； 完整但堆芯开始损坏时未隔离； 结构失效或有较大泄漏（确定尺寸和泄漏位置）*。
二次安全壳状态（反应堆厂房或者包容构筑物）	完整且堆芯开始损坏时即隔离； 完整但堆芯开始损坏时未隔离； 结构失效或有较大泄漏。*

*包含了外部事件引起的结构损伤。

表 3 PDS 特征和属性示例

4.2.2 PDS 的定义应确保将一级 PSA 事故序列，特别是所有堆芯损伤序列都归入到相应的 PDS 中。给定的 PDS 代表性序列与该 PDS 中其他序列的差异不至于影响最终结果（如源项、影响应急准备行动的裂变产物屏障的丧失进程、释放类的条件概率）。

4.2.3 PDS 通常分为两大类：一类是安全壳具备包容和滞留能力，放射性物质从反应堆冷却剂系统释放到安全壳内；另一类是安全壳被旁通或者失效，放射性物质直接释放到环境中。当核动力厂内承担二次安全壳功能的反应堆厂房或包容构筑物可能

对源项有重要影响时，也应在 PDS 属性中考虑它们的状态。对于安全壳完整的 PDS，通常应进行安全壳事件树分析。对放射性物质直接释放到环境的 PDS，通常仅需要源项分析，必要时可开展安全壳事件树分析，评估减少源项的可能措施。

4.2.4 将事件序列归组到 PDS 时，应考虑一级 PSA 中系统与设备的失效对安全壳完整性或者放射性物质释放的可能影响，包括如下几方面:

（1）始发事件的类型。它影响到流体进入安全壳的流速，堆芯熔化和氢气生成的进程，放射性物质释放的时间进程;

（2）堆芯冷却功能的失效模式; 它影响堆芯熔化的时间进程;

（3）燃料损坏的程度;

（4）堆芯损伤开始时的反应堆冷却剂系统压力以及反应堆压力容器下封头失效前能够改变压力容器内压力的安全/释放阀或其他部件的状态; 堆芯损伤开始后的反应堆压力容器内的压力也会影响反应堆冷却系统超温超压的失效概率; 下封头失效时的反应堆压力容器内的压力能够影响堆芯熔融物到安全壳的蔓延和扩散模式; 始发事件和卸压系统的功能可能对压力产生影响。

4.2.5 将事件序列归组到 PDS 时，应考虑安全壳内安全设施的状态。安全壳内安全设施的状态影响安全壳冷却、放射性物质的迁移、可燃气体的混合等。

4.2.6 应将选定的 PDS 减少到可处理的数量。第一种方法是合并具有相似属性的 PDS，选择其中代表性的序列进行包络分析; 第二种方法是使用频率截断值筛选掉不太重要的 PDS。在引入频率截断值之前，要对放射性核素早期和大量释放到环境的 PDS 进行仔细筛选，以免遗漏。应考虑事故序列归并到 PDS 过

程中引入的变化和不确定性，并考虑其对 PSA 具体目标的影响。

4.3 其他 PSA 的 PDS

4.3.1 将二级 PSA 扩展到内部和外部危险时，需要考虑危险对严重事故缓解所需系统的影响，包括那些支持操纵员动作以及影响安全壳完整性的系统。例如，地震可能导致安全壳失效；在这种情况下还应考虑将新产生的PDS归入到已有PDS的可行性，例如，将安全壳失效归并到安全壳隔离失效中。

4.3.2 低功率和停堆工况和功率工况下二级 PSA 的差异主要在于始发事件发生时，一回路水装量、回路状态和安全壳状态不同。因此将功率工况二级 PSA 的范围扩展到低功率和停堆工况时，不能直接使用功率工况二级 PSA 定义的 PDS，应补充低功率和停堆工况的特有属性。核动力厂低功率和停堆工况存在影响严重事故行为的重大变化、或要对特定工况进行更精确的模拟时，则需定义新的 PDS。低功率和停堆二级 PSA 中，PDS 的定义应考虑包括安全壳的状态和冷却剂水位在内的更多属性，如一回路水装量低至半管运行、一回路开启（如：在开盖期间或换料期间）、安全壳未被隔离（如换料操作期间）等。

5 严重事故下的安全壳性能分析

5.1 分析对象

5.1.1 安全壳性能分析是对核动力厂设计中存在的，能够承受堆芯严重损坏导致的某些工况并滞留大部分放射性物质的非能动结构进行性能分析。这些非能动结构最常见的形式是安全壳构筑物，它包括安全壳相关系统。对没有这样结构的核动力厂，以下安全壳性能的分析可以参照执行。

5.2 分析目的

严重事故下的安全壳性能分析的目的是评估核动力厂安全壳极限承载能力，从而确定安全壳抵御严重事故进程中各种威胁安全壳完整性因素的能力。安全壳性能分析为安全壳失效模式、位置、大小和极限压力/温度承载能力提供工程基础数据。

5.3 分析方法

5.3.1 应收集安全壳结构设计和安全壳贯穿件的详细信息，并根据这些信息分析安全壳通过钢衬里或贯穿件泄漏的可能性，现实地评估安全壳性能极限。应收集的安全壳结构设计与安全壳贯穿件的重要特征示例如表 4 所示。

特征	特征属性
安全壳种类	钢结构； 混凝土结构： （1）预应力混凝土； （2）后张拉混凝土； （3）钢筋混凝土。
安全壳贯穿件	设备舱门； 人员舱门； 管道贯穿件； 电气贯穿件； 大气净化管线； 排气管线。
其他	安全壳的几何形状； 安全壳的几何不连续性，例如，从圆柱形壳过渡至穹顶和地基； 安全壳衬里锚固系统； 安全壳与周围其他构筑物的相互作用。

表 4 安全壳结构设计与安全壳贯穿件的重要特征示例

5.3.2 应识别安全壳失效机理，作为安全壳承载能力分析的输入。不能仅依据安全壳的设计准则来评估安全壳承载能力，因为安全壳设计时考虑了安全因素，安全壳实际能够达到的极限承载力常常超过设计值的 2-4 倍。当安全壳设计没有考虑严重事故

期间在安全壳内形成的恶劣环境条件时，通常需要考虑安全壳新的失效模型。

5.3.3 安全壳性能评估通常采用“阈值法”和“破前漏法”。“阈值法”定义了一个带有不确定性的压力阈值，安全壳一旦达到这个压力阈值就会失效并产生大的破裂，从而导致安全壳内气体可能大量和快速释放到环境。“破前漏法”假设安全壳在大破裂前会发生泄漏，随着压力逐步增加，达到极限承载压力时，安全壳将存在发生更大的失效可能性。当安全壳内气体的质量和能量增加速率小于或等于向外泄漏的速率时，则预计安全壳压力不会逐步增加，安全壳不会大规模失效。

5.3.4 安全壳性能分析所进行的核动力厂特定计算应基于验证过的结构模型，并有相应的数据和合理的失效准则。安全壳性能分析应考虑安全壳的不同负荷类型。

5.3.5 当内部压力负荷是安全壳失效的潜在主要决定因素时，二级 PSA 还应考虑温度对安全壳结构性能的影响。温度可能影响安全壳结构材料的强度特性，同时引起贯穿件密封材料的退化。

5.3.6 安全壳结构性能的评估应包括评估与其相关的安全壳极限承载压力/温度的不确定性。应考虑材料特性和建模的不确定性分析。泄漏、破裂等安全壳可信失效模式下的失效压力/温度分布可通过专家的分析判断来建立。

5.3.7 应评估安全壳由于长时间暴露并受堆芯熔融碎片冲击（堆芯熔融物-混凝土反应）而造成的混凝土结构大范围侵蚀的影响。

5.3.8 当严重事故进程分析表明侵蚀程度可能影响反应堆压

力容器支撑结构、安全壳壁或地板时，则应分析堆芯碎片是否会引起安全壳部分或完全熔穿。此时需确定和分析安全壳可能熔穿的位置（如，贯穿件、地坑汲水管线）。

5.3.9 安全壳性能评估可应用相似安全壳的计算结果，但应说明采用该计算结果的理由。

6 严重事故进程和现象分析

6.1 严重事故进程分析

6.1.1 开展特定的严重事故进程分析是评价核动力厂严重事故行为的首选方法。应对核动力厂堆芯损坏频率有明显贡献的PDS进行事故进程分析。对发生频率低、但是可能导致放射性物质大量或早期释放的PDS，如安全壳旁通或安全壳早期失效也要进行事故进程分析。对频率高和后果严重的 PDS 进行详细的事故进程分析，可以为其他没有详细分析的 PDS 事故序列发展提供评估信息。

6.1.2 核动力厂特定的严重事故进程分析可以用相似核动力厂和安全壳通用研究文献中的严重事故现象和安全壳响应进行补充，但应明确严重事故进程分析的不确定性可能超越核动力厂设计差异所带来的严重事故进程差异。可以通过对关键设计属性开展相应的比例分析来包络核动力厂设计特性的小差异，应用相似核动力厂的参考结果进行比例分析或适用性分析能够给特定核动力厂的严重事故进程分析提供更多有用的输入。

6.1.3 严重事故进程分析应使用经过验证的严重事故模拟程序。严重事故模拟程序和计算分析数量应基于二级 PSA 的目标确定，确定时应考虑:

（1）选定的程序能够模化事故过程中发生的绝大部分事件序列和现象。

（2）选定的程序能够正确考虑不同物理化学进程之间的相互影响;

（3） 选定的程序满足验证、对比分析和文档记录的要求;

（4）选定的程序所需计算时间和资源合理。

（5）选定程序的技术局限性和不足明确。

6.1.4 应了解选定程序中的各种建模选项对分析结果的影响。对模拟严重事故进程有潜在影响的不确定性因素（示例如表5）应进行敏感性分析。

不确定性因素	可能影响的相关现象
反应堆压力容器（RPV）内产生氢气	堆芯流道阻塞; 包壳氧化; 包壳肿胀; 再淹没与补水; 堆芯升温熔化; 熔融燃料迁移再定位。
反应堆冷却剂自然循环	RCS回路形成循环流动; RCS压力边界的升温和蠕变破裂; 主泵轴封降级或失效。
RPV内燃料-冷却剂的相互作用	可能导致RPV中燃料损坏; 重返临界; 爆炸导致RPV失效; 放射性物质释放。
RPV失效机理	下封头贯穿件的熔穿和冷却; 下封头局部失效; 整体蠕变失效。
熔融物高压喷射/安全壳直接加热	捕集向安全壳喷射的碎片; 锆氧化过程放热并产生氢气; 碎片迁移到堆腔外; 氢气燃烧; 放射性物质释放。
PRV外燃料-冷却剂相互作用	熔融物破碎和淬火; 安全壳缓慢升压; 蒸汽爆炸对安全壳的动态载荷; 放射性物质释放。

不确定性因素	可能影响的相关现象
堆芯-混凝土相互作用	熔融物碎片腐蚀安全壳结构； 生成不可凝气体； 熔融物碎片可能与安全壳压力边界接触； 放射性物质释放。
氢气燃烧	气空间的混合或分层； 蒸汽惰化； 点火传播与爆燃火焰； 火焰从爆燃变成爆炸； 向构筑物的传热； 隔间结构对燃烧压力波的响应导致门或防爆隔板打开、水池消失等。

表 5 事故进程的不确定性因素示例

6.1.5 应评估模型中用于事故进程定量化的重要计算变量，如压力和温度峰值、可燃气体产量、主要事件的发生时间等，并形成文档记录。应在 PSA 文档中给出这些变量在重要时间节点评估的结果并进行分析。

6.1.6 应考虑可能影响分析人员预判严重事故进程能力的因素，如所用计算程序的误差程度、合法性及供使用的反应堆试验数据等。

6.1.7 应考虑严重事故管理措施的影响，包括有利影响和潜在不利影响。包含在核动力厂的相关规程或严重事故管理指南中的人员响应通常都应在严重事故进程分析中考虑。

6.2 严重事故现象分析

6.2.1 应选取合适的模型、计算机程序和数据开展严重事故现象分析，并对所有相关的严重事故现象的概率进行了考虑。

6.2.2 应对评估严重事故现象过程中所用的经验数据或参考核动力厂数据的相关性和适用性进行说明。

6.2.3 严重事故现象分析作为严重事故进程分析的一部分，也应考虑严重事故管理措施的影响，包括有利影响和潜在不利影响。

6.2.4 应考虑并评估严重事故现象对二级 PSA 模型中的设备和系统可用性可能产生影响的环境条件。影响因素包括温度、压力、湿度和放射性以及来自能量释放事件的影响等。

6.3 严重事故现象分支条件概率定量化

6.3.1 应进行严重事故现象概率评价，给出用于量化严重事故现象的分支概率或支持性模型，以确定堆芯损坏后严重事故现象导致安全壳失效的概率。

6.3.2 通常采用阈值法或整体法确定严重事故现象分支条件概率。阈值法和整体法两种方法可以单独使用，也可以联合应用，还可以使用除了这两种方法以外的其他方法。

6.3.3 严重事故现象分支条件概率的确定应有分析和数据支持，并合理考虑其不确定性。概率值的确定可依据以下数据及信息:

（1）对严重事故现象进行的确定论分析成果;

（2）相关试验的测量或观测;

（3）相似核动力厂研究结果的分析和见解;

（4）专家意见和专家判断。

6.3.4 根据主导现象将其分解成一些子问题进行研究。子问题研究可以分别用于安全壳事件树节点概率的评估或作为其中一部分连接到安全壳事件树题头中。子问题概率值在安全壳事件树定量化中的应用原则应与顶事件和节点问题保持一致。

6.3.5 对二级 PSA 的重要事故序列，应使用现实的方式分析其中严重事故现象的分支概率；对二级 PSA 的其他事故序列，严重事故现象的分支概率可使用通用或保守的概率值，但要比较通用概率值与实际核动力厂的差异，评估其适用性。

6.3.6 应选择专家判断、参数分析等恰当的分析方法确定严重事故现象建模不确定性的概率值。

7 安全壳事件树分析

7.1 概述

7.1.1 安全壳事件树（CET ，Contaiment Event Tree）分析是系统评估核动力厂应对严重事故能力的一种结构化方法。二级PSA 通过建立安全壳事件树对堆芯损伤后的严重事故进程和现象、严重事故缓解系统响应以及人员动作进行评价，定性识别和定量评价可能导致早期或大量放射性释放的事故情景及发生可能性。安全壳事件树方法在二级 PSA 的应用过程见图 1。

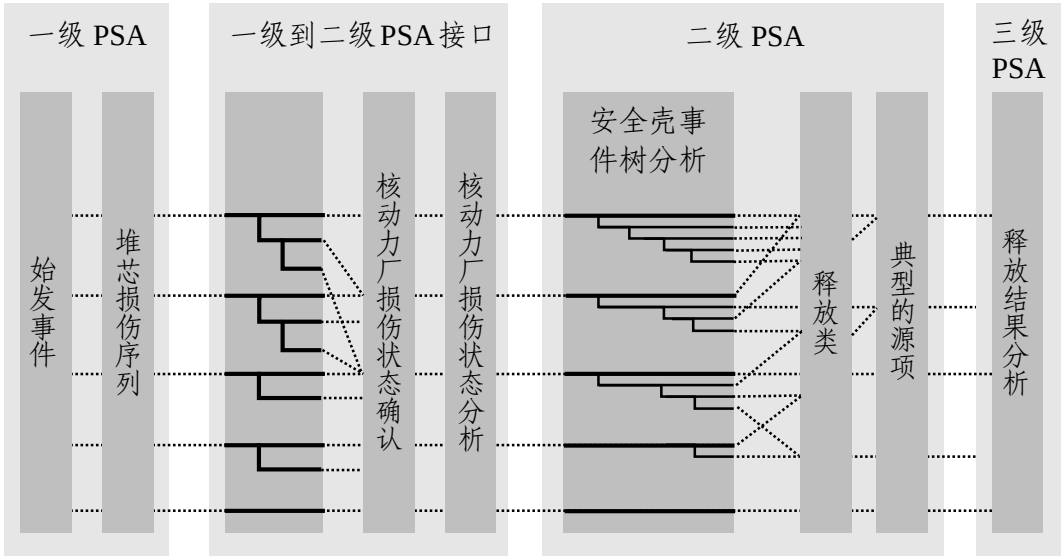

图 1 安全壳事件树分析的应用过程

7.1.2 安全壳事件树分析的目的是建立一个能够系统量化严重事故序列的逻辑框架。该逻辑框架至少应满足以下要求:

（1）以清晰的方式将一级PSA的信息充分传递至二级PSA;

（2）对可能会影响事故进程的人员动作、缓解系统响应和严重事故现象都进行了必要的描述与评价;

（3）在模型中恰当地反映了相关性;

（4）恰当反映并模化了严重事故现象;

（5）提供了支持系统/设备的成功准则、人员动作的时间窗口、人员动作的可达性要求以及其他恢复动作的分析;

（6）事件序列终态的定义应包括释放时间、安全壳失效模式、放射性核素的分布以及释放量等特征。

（7）计算了导致所定义终态的严重事故序列的频率。

7.2 安全壳事件树的顶事件和节点问题

7.2.1 安全壳事件树中的顶事件和节点问题应表明对事故进程、严重事故响应、放射性物质屏障的挑战和放射性物质释放到环境的缓解起决定作用的事件和物理过程，包括严重事故现象、严重事故缓解系统响应、严重事故相关管理措施和人员响应行动等。安全壳事件树顶事件和节点问题与核动力厂类型密切相关，对某类反应堆/安全壳系统重要的严重事故响应对于其他类型来说可能并不重要。

7.2.2 安全壳事件树建模的详细程度和实际规模应与二级 PSA 目标相匹配。当二级 PSA 的目的仅仅是确定放射性早期大量释放频率，而不需要量化评估全范围严重事故源项和晚期大量释放频率时，可以开发结构较小的安全壳事件树，此时主要关注适当时间范围内后果严重的严重事故序列。

7.2.3 安全壳事件树应正确描述时序，合理考虑事件/现象之间的相互影响。处理时序问题的一种方法是以事故进程中的主导因素发生重要改变为依据，将安全壳事件树划分成多个连续时间段，如：阶段 1 为压力容器内堆芯损伤早期，核动力厂立即响应由始发事件导致的 PDS; 阶段 2 为压力容器内堆芯损伤后期到反

应堆压力容器失效；阶段 3 为长期核动力厂响应。阶段 3 有时进一步细分为三个子阶段:

（1）阶段 3a，RPV 即将失效时刻，考虑由于 RPV 失效而带来的挑战，如安全壳直接加热;

（2）阶段 3b，反应堆压力容器失效后的几小时内，考虑堆芯熔融物在压力容器外的即刻行为，如：堆芯熔融物在压力容器外的稳定或者开始与混凝土发生反应;

（3）阶段 3c，反应堆压力容器失效几小时之后，考虑由堆外熔融物行为带来的挑战，如熔融物-混凝土相互作用生成的不可凝气体引起的压力上升，燃烧现象或蒸汽的不断生成导致的压力上升。

7.3 安全壳事件树分支概率确定

7.3.1 需对安全壳事件树题头事件进行评估分析，以确定安全壳事件树分支概率。

7.3.2 安全壳事件树分支条件概率包括量化严重事故现象的分支概率、量化二级 PSA 模型中系统/设备可靠性的分支概率和量化二级 PSA 模型中人员动作可靠性的分支概率。严重事故现象分支概率计算参见 7.3 节。此外，还应给出用于量化二级 PSA 模型中系统/设备可靠性和人员可靠性的分支概率或支持性模型。

7.3.3 应进行系统评价，确定堆芯损坏后严重事故缓解系统的可靠性，给出用于量化二级 PSA 模型中系统/设备可靠性的分支概率或支持性模型。系统评价需要合理考虑并评估严重事故导致的环境条件对二级 PSA 模型中的设备和系统的可用性影响。对于时间窗口比较长的事故序列，可考虑系统或设备的恢复操作，比如恢复电源。

7.3.4 应进行人员可靠性分析，以确定堆芯损坏后严重事故缓解操作的可靠性，给出用于量化二级 PSA 模型中人员动作可靠性的分支概率或支持性模型。在一级 PSA 模型中采用的人员动作状态（成功或失败）可直接或者间接通过 PDS 属性传递到二级 PSA 中。在一级 PSA 模型中没有体现的严重事故管理行为对严重事故进程和严重事故现象的影响应在安全壳事件树中考虑。对二级 PSA 中模化的人员动作，应评估其与一级 PSA 事故序列中人员动作可能存在的相关性。人员动作的概率处理方法要与一级 PSA 相协调。人员动作概率的处理要考虑严重事故进程带来影响。对于时间窗口比较长的事故序列，可考虑人员操作的恢复。

7.3.5 安全壳事件树定量化可以使用连接事件树、故障树、用户自定义的功能或其他方法。所使用的二级 PSA 软件应满足将评估结果整合到安全壳事件树定量化结果中的需求。

7.3.6 应对安全壳事件模型及分支概率的确定进行管理和审查，确保整个模型构建和定量化过程是可追溯的。

8 严重事故源项

8.1 源项分析的范围

8.1.1 二级 PSA 应针对安全壳事件树终态进行源项分析，从而确定从核动力厂释放到环境中的放射性物质数量。源项分析的范围取决于二级 PSA 的目标和预期应用。在二级 PSA 研究开始时就应根据其目标和预期应用，定义安全壳事件树终态的相关属性。当二级 PSA 要应用于三级 PSA 时，应对 CDF 有贡献的所有事故序列进行放射性物质源项分析，给出其与 CDF 相关的释放

特性。当二级 PSA 仅需给出导致“早期大量释放”序列频率时，则可针对选定的事故序列进行典型放射性物质的源项分析。通常选择碘和铯作为典型放射性物质开展源项分析。

8.1.2 二级 PSA 源项分析的内容通常包括:

（1）根据放射性源项的属性定义释放类;

（2）将安全壳事件树终态归并成释放类;

（3）对每个释放类进行源项分析。

8.2 释放类的定义

8.2.1 将安全壳事件树序列的终态进行分组，将具有相同或相似向环境释放特定属性的安全壳事故序列终态归并为一组，定义为释放类。然后对每个释放类进行源项分析，以减少需要开展确定论源项分析的事故序列数量。定义的释放类数量过多时，应进一步归并成适中的组，以用于源项分析。

8.2.2 安全壳事件树的事件序列代表了堆芯损伤后的一系列事件组合，其中很多事件对放射性物质从安全壳的释放有显著影响，这些事件的特性包括:

（1）反应堆冷却系统的失效模式;

（2）安全壳失效的模式和时间;

（3）熔化堆芯材料的冷却机理;

（4）放射性物质的滞留机理。

8.2.3 二级 PSA 源项分析中的释放类定义需要明确与放射性物质迁移和安全壳失效机理相关的一系列属性，这些属性也与放射性物质释放到环境的特性相关。应对每个释放类选出一个典型事故序列进行核动力厂特定计算评估严重事故源项。

8.3 安全壳事件树终态归并成释放类

8.3.1 应采用系统性方法将安全壳事件树终态归并成所定义的释放类。安全壳事件树定量化使用的软件会影响安全壳事件树终态的归并过程。软件中包含的安全壳事件树终态（割集）的后处理过程或安全壳事件树模型中的相关属性，可以用于释放类的归并。

8.3.2 安全壳事件树终态的归并应考虑影响放射性物质释放的各种因素。归并依据的属性应体现二级 PSA 结果的特性，必要时还需考虑扩展到三级 PSA 的需求。根据归并的属性不同，安全壳事件树终态的归并可以分为多个阶段分别进行。如，首先可以依据主导放射性释放的规模和时间因素进行归并，后续再依据影响放射性物质在场外大气中的弥散和影响场外人员健康评估的重要属性来归并。

8.3.3 归并后同一释放类中的每个安全壳事件树终态应有相似的放射性释放特性和场外后果，从而使该释放类的源项分析能够代表该类中所有终态的特性。

8.4 源项分析

8.4.1 源项分析应识别和考虑核动力厂设计特征和严重事故现象对源项大小和特性的影响。核动力厂固有的设计特征对于所有安全壳事件树终态的源项的影响是一致的，如：燃料和控制棒组件的配置以及材料组成、堆芯功率密度及分布、燃耗和混凝土成分等。严重事故现象对源项大小和特性的影响会因事故序列不同而发生变化，如：

（1）堆芯损伤和 RPV 破裂时的 RCS 压力；

（2）冷却水的可用性（压力容器内和外）；

（3）压力容器外的堆芯碎片的厚度和成分;

（4）安全壳专设安全设施的运行;

（5）安全壳破口的尺寸;

（6）安全壳失效的位置和导致的向环境迁移路径。

8.4.2 源项分析应模拟影响安全壳和相连厂房中放射性物质的释放和迁移的所有过程，包括:

（1）放射性物质在压力容器内阶段从燃料的释放;

（2）放射性物质在反应堆冷却系统中的滞留;

（3）放射性物质在压力容器外阶段的释放;

（4）放射性物质在安全壳和相连厂房中的滞留。

8.4.3 源项分析应评估各类放射性核素在反应堆冷却回路和安全壳内的空间分布以及到环境中的释放量。

8.4.4 应在每个释放类中选择一个或几个具有代表性的事故序列开展源项分析，确保源项分析能准确地表征释放类所包含的所有安全壳事件序列终态。典型事故序列的选择应根据序列的频率和后果对释放类的贡献来确定。当释放类包含的事故序列中主导释放现象的不确定性相对较低时，可选取其中相对较少的代表性事故序列进行源项分析。当缺少可用的可信模型评价由潜在的不确定机理（如，蒸汽爆炸，安全壳直接加热）造成的释放类时，可以采用简化分析、专家判断、参照相似其他 PSA 结果等方法进行评估。

8.4.5 当释放类的源项分析对核动力厂的某个设计特性或者放射性物质的某个具体迁移机理特别敏感时，可使用更详细的模型程序进行补充分析。

8.4.6 可使用核动力厂特定的源项分析确定释放类源项的大

小和特性。在新建核动力厂的初期设计阶段或二级 PSA 开展的初期阶段、或需要快速获取结果时，也可以使用参考核动力厂的源项分析结果得到初步的或包络的源项估计结果。

8.4.7 当使用参考核动力厂的源项分析结果进行源项估计时，应满足以下条件:

（1）所研究核动力厂与拟参考核动力厂在设计上足够相似。

（2）所研究核动力厂进行源项评估的事故序列与拟参考核动力厂中开展源项分析的事故序列足够相似。

（3）所参考的源项分析结果是基于当时最新的严重事故建模水平。

8.4.8 源项分析中使用的计算机仿真程序应能够模拟严重事故现象的综合行为，包括：反应堆热工水力响应、堆芯升温、燃料损伤和燃料材料的再定位、安全壳响应、放射性物质从燃料中的释放以及放射性气溶胶和蒸汽在 RCS 和安全壳中的迁移等。

8.4.9 源项的大小通常以一个或多个放射性核素组占初始堆芯装量份额的形式来表示。使用一体化严重事故分析程序时，通常基于物理化学属性的相似性和迁移过程中与其他元素和物质发生化学反应的相似性，将反应堆燃料中生成的放射性物质和放射性同位素归组成放射性核素组。应在源项分析中给出使用的放射性核素组及结构组成。

8.4.10 源项评估应尽可能借助理论研究、试验研究、专家判断或不确定性分析等方式确定放射性核素组离开堆芯区域后以各种可能化学形态存在的份额。放射性核素组离开堆芯区域后的化学形态决定了它们迁移到环境的效率。

8.5 源项分析结果及其不确定性

8.5.1 源项分析应给出放射性核素释放的定量结果及定量结果的敏感性或不确定性分析结果。应给出每个放射性核素组超过给定释放量的频率。应给出每个互补累积分布函数的统计重要度，如均值、中值和95%分位值等。

8.5.2 释放类的频率是该类中所有安全壳事件树终态频率的加和。通过释放类来确定大量释放频率（LRF）或早期大量释放频率（LERF）并与所定义的风险准则进行比较时，需要定义“大量”和“早期”两个概念，并建立与释放类的对应关系。

8.5.3 源项分析尽可能考虑不确定性对结果的影响。除了严重事故现象模拟中的不确定性之外，放射性物质从燃料释放、在反应堆内部表面的沉积和滞留以及安全壳安全系统洗涤的物理和化学过程也存在很多不确定性，源项分析中不确定性的主要包括:

（1）堆芯损坏过程和安全壳行为中的不确定性（示例如表5）;

（2）燃料裸露（烧毁）对放射性物质从燃料释放率的影响;

（3）挥发和半挥发核素的化学构成;

（4）在堆芯降级的过程中，燃料、中子吸收体和结构性材料的化学相互作用;

（5）放射性物质和气溶胶在反应堆冷却剂回路表面的沉积速率;

（6）安全壳旁路事故序列中放射性物质在管道和其他设备上的沉积;

（7）堆芯熔融物与混凝土相互作用（MCCI）过程中放射性

物质和气溶胶的释放;

（8）堆芯熔融物与混凝土相互作用（MCCI）中的化学反应过程;

（9）氢气燃烧/火焰前沿自由基与气载放射性物质的相互作用;

（10）气溶胶与水蒸气被洗涤的效率;

（11）水池中所俘获放射性物质的水化学特性;

（12）表层放射性物质的再汽化和再悬浮;

（13）放射性气溶胶的化学分解。

8.5.4 应对源项分析模型及其定量化结果的确定进行管理和审查，确保整个模型构建和定量化过程是可追溯的。

9 二级 PSA 结果和评价

9.1 二级 PSA 的结果

9.1.1 应给出安全壳事件树定量化结果。安全壳事件树终态通常用释放类表示。

9.1.2 应以清晰的方式给出二级 PSA 终态及其重要贡献项的分析结果，包括但不限于:

（1）应确定每种释放类的频率和不确定性。应确定总释放频率的主要贡献者，并列表给出每个释放类对总释放频率的贡献。

（2）对重要的释放类，识别其贡献项（如始发事件、一级 PSA 事故序列、设备失效、共因失效、操纵员失误、PDS、二级 PSA 事故序列、严重事故现象、安全壳威胁、安全壳失效模式和释放类）及相对贡献份额、安全壳的可能响应、放射性物质向环境的释放及相关频率、释放物质的总量、物理和化学特性、释放

的时间、能量、时长和地点等信息。

（3）应确定和说明安全壳早期失效的主要贡献项。应确定和说明不同 PDS 的安全壳早期失效条件概率不同的根本原因。

（4）应按照相应分析的具体要求对不确定性进行描述和处理，给出用于处理二级 PSA 不确定性的具体方法，以及对不确定性的定量评价结果。

9.1.3 应按照分析的具体要求对敏感性进行描述和处理，给出基于分析结果的重要风险见解。

9.1.4 应识别分析中可能会影响二级 PSA 结果应用的局限性，包括但不限于:

（1）识别二级 PSA 分析中所考虑的一级 PSA 堆芯损坏频率的比例，识别在二级 PSA 分析中所考虑堆芯损坏频率的比例低于 100%的原因（如有）;

（2）识别分析详细程度可能会影响二级 PSA 应用的局限性;

（3）识别分析中的建模假设和未考虑的过程、现象、人员操作所导致的局限性。

9.1.5 应描述和评价不确定分析的结果以完善二级 PSA 结论。

9.1.6 对于目前不能在二级 PSA 定量化中明确考虑的不确定性，可以通过针对影响二级 PSA 结果的不确定性的主要来源进行敏感性分析，识别出源项定量化的不确定性，或通过已完成及正在进行的研究项目减少严重事故源项分析的不确定性。

9.1.7 二级 PSA 分析过程和结果应形成文档报告，使用便于审查、应用、升级和同行评估的方式进行二级 PSA 模型结果的展示；应说明二级 PSA 分析的具体内容，所使用的方法、PSA

处理过程以及通过逻辑演绎得出的定量化结果、风险见解和结论，同时也要便于支持性资料的查阅。

9.2 二级 PSA 结果的不确定性

9.2.1 二级 PSA 的不确定性来源非常多，应确定二级 PSA 的不确定性主要来源，并评价不确定性对评价结果的影响。二级 PSA 分析中产生不确定性的因素主要包括:

（1）分析不完备导致的不确定性。二级PSA模型的主要目标是评估能够导致放射性物质释放的所有可能情景(事件序列),这些情景许多来自一级PSA的结果。然而，无论是一级PSA还是二级PSA都无法保证已识别出所有可能出现的放射性物质释放情形并进行了合理的评估。同时，将一级PSA事故序列或割集归组为PDS作为二级PSA的输入时，会因为丢失一些模型细节而引入不确定性。安全壳事件树归并时，也会因为事故进程归组所使用的属性不完整而引入不确定性。分析的不完备给分析结果和结论带来不确定性很难明确地评估和量化，通常可通过增加计算量、减少归组开展广泛的同行评审等方式降低这类不确定性。

（2）建模过程的不确定性。建模过程的不确定性来源于二级PSA相关的支持性分析中对所用方法、模型及假设和近似处理的适当性缺乏完善的认识。通常可通过敏感性分析来评估建模过程的不确定性。

（3）参数的不确定性。参数的不确定性来源于二级PSA定量化过程中基本参数取值的不确定性。通常可通过定义所有参数的不确定性分布并考虑分析过程中的传播来处理参数的不确定性。

9.2.2 二级 PSA 应定义不确定性分析范围。通常可选择支配

性不确定性来源，并对它们进行详细处理，以估计二级 PSA 结果的总体不确定性。

9.2.3 不确定性分析包括定量化评估和不确定性传播。不确定性分析定量化评估通常采用敏感性分析和不确定性分析两种方法。敏感性分析用于度量选择不同的模型选项、假设或输入参数值时，结果的变化程度，这是对一个问题或者在同一时间内一组相关问题的不确定性分析。敏感性分析结果可用于指导支配性不确定性来源的选取。不确定性分析是根据可选的模型或者参数值的范围，生成表示结果可信度的概率分布。在确定不确定性分析范围后，再确定不确定性参数值的分布。不确定性分析范围内的每个参数都有一个概率密度方程或分布。确定参数分布的依据应有出版文献中的数据、分析和相关考虑支持。没有在不确定性分析范围内的其他参数也可用平均值来描述或评估等。不确定性分布应作为 PSA 研究的一部分进行同行评审。

9.2.4 二级 PSA 应根据不同的不确定性分析目标，通过不同的方法对不确定性的传播进行分析。可用的分析技术包括:

（1）使用离散概率分布;

（2）基于简单（蒙特卡洛）随机抽样或分层（拉丁超立方）抽样的直接模拟方法。

9.2.5 重要度评价可以参考不确定性问题或现象中关联变量的关联系数。也可以应用回归分析技术评估 PSA 中具体不确定性因素的重要度。如果使用敏感性分析代替全面的不确定性分析，则应建立敏感性指标表征模型选项或参数值对二级 PSA 的影响。

9.2.6 对于目前不能在二级 PSA 的定量化中明确考虑的不确

定性，可以通过对影响二级 PSA 结果不确定性的主要来源进行敏感性分析，识别出源项定量化的不确定性，或通过已完成及正在进行的研究项目减少严重事故源项分析的不确定性。

9.3 二级 PSA 结果的评价

9.3.1 二级 PSA 结果评价的目的是:

（1）通过一致的方法及相应文档，说明一级 PSA 事故序列被恰当地传递到二级 PSA 模型中并定量化;

（2）确保二级 PSA 分析结果与相似核动力厂的分析以及当前对严重事故现象的认知水平相一致;

（3）识别能够合理解释分析结果的因素;

（4）提供二级 PSA 所有相关内容的可追溯性，以便于解释分析结果;

（5）在考虑涉及三级 PSA 方面的应用时，确保二级 PSA 结果与三级 PSA 的应用要求一致。

10 二级 PSA 的应用

10.1 概述

10.1.1 二级 PSA 的结果可单独应用，也可以与一级 PSA、三级 PSA 的结果联合使用。《核动力厂一级概率安全分析》中关于“PSA 的应用”的要求同样适用于二级 PSA，二级 PSA 与一级 PSA 结果的联合应用相较于单独应用一级 PSA 结果可以得到更多的见解。二级 PSA 在设计方面的应用主要包括论证核动力厂设计是否满足已规定的风险准则、论证核动力厂与严重事故缓解相关设计是否平衡，以及为纵深防御第 4、第 5 层次的设置提供输入等。

10.1.2 二级 PSA 的范围和详细程度应与其应用目标相匹配。二级 PSA 的范围和详细程度会因应用目标不同而有所差异。为适用于更多潜在用途，二级 PSA 应尽可能建立在全范围一级 PSA 基础上。当二级 PSA 基于范围或详细程度有限的一级 PSA 时，则应在二级 PSA 应用时应考虑这些局限性。

10.1.3 所应用的二级 PSA 模型应体现核动力厂的设计现状和严重事故分析的最新研究成果。

10.2 论证核动力厂设计是否满足规定的风险准则

10.2.1 二级 PSA 的结果应与规定的风险准则相比较。确定核动力厂的设计是否满足风险准则时，应确保二级 PSA 定量结果与其所比较的风险准则具有相同的含义。

10.2.2 二级 PSA 的结果支持论证“实际消除”的判断时，应考虑核动力厂设计措施的可用性和可达性。二级 PSA 中可能导致早期放射性释放或大量放射性释放的核动力厂工况或事故序列可用于论证其被“实际消除”。

10.2.3 论证时应考虑二级 PSA 敏感性分析结果和不确定性，用敏感性分析和不确定性分析表明二级 PSA 结果满足风险准则的可信度以及超出目标的可能性。

10.3 论证核动力厂与严重事故缓解相关的设计是否平衡

10.3.1 二级 PSA 可用于评估堆芯损伤后采取的严重事故缓解措施是否适当。

10.3.2 二级 PSA 可用于识别出各种严重事故现象之间的相关性，并在开发严重事故管理指南时，用来识别或改进严重事故管理措施。

10.3.3 二级 PSA 可用于评价和确定严重事故管理指南或规

程中严重事故管理措施的有效性。二级 PSA 应用于严重事故管理指南的过程应采用迭代、更新的方式，以促进严重事故管理指南的优化。

10.3.4 二级 PSA 可用于识别核动力厂严重事故预防与缓解措施的薄弱环节，为是否需要改进设计提供输入。包括:

（1）应用二级 PSA 给出的大量释放频率和大量早期释放频率识别导致安全壳（早期或晚期）失效的支配性现象;

（2）应用二级 PSA 给出的各释放类频率和源项识别一回路和安全壳的主要失效模式;

（3）应用二级 PSA 给出的每个释放类割集和系统、设备和其他基本事件的重要度分析结果识别对每个释放类重要的结构、系统和部件。

10.3.5 二级 PSA 可用于评价严重事故预防与缓解措施薄弱环节改进措施的有效性。二级 PSA 所考虑的改进措施包括纳入到核动力厂的设计或设计改进中的额外保护系统或设施。改进措施应能够有效地降低最高的风险贡献项占整体风险的份额。

10.3.6 二级 PSA 可用于为严重事故管理有关的设计或设计变更提供方案比选依据。二级 PSA 可从降低风险的角度比较设计选项所带来的收益。方案比选依据应包括对设计选项正反两方面的认识和影响。

10.3.7 二级 PSA 可用于支持核动力厂设计扩展工况的划分与评价。

10.4 为纵深防御第 4、5 层次的设置提供输入

10.4.1 二级 PSA 可用于确定核动力厂的纵深防御设计是否足够充分。

10.4.2 二级 PSA 可用于选取后果最严重的严重事故源项和代表性的严重事故源项，也可用于确定发生频率极低的严重事故序列。

10.4.3 二级 PSA 可为核动力厂应急计划区大小的测算提供事故进程和源项分析输入。

10.4.4 二级 PSA 可为应急设施可居留性评价提供事故进程和源项分析输入。

10.4.5 二级 PSA 可为识别和开展严重事故现象相关的研究活动及其优先次序提供依据，以优先关注风险最重要领域。

10.5 其他应用

10.5.1 二级 PSA 可用于向三级 PSA 扩展。此时，二级 PSA 应能够向三级 PSA 提供不同释放类的发生频率和源项特征。需要输入三级 PSA 的源项特征通常包括放射性物质的组成、释放起始时间和持续时间、释放量、释放高度等。

10.5.2 二级 PSA 并不仅局限于上述应用领域，还会随着工业实践和技术发展而不断拓展。

附录 I 严重事故仿真程序

I.1 简介

I.1.1 严重事故现象的复杂性及其之间的相关性能够通过大型计算机软件进行现实的分析。本附录给出二级 PSA 中常用的严重事故仿真程序类型，并简要介绍其应用范围。

I.2 程序分类及应用

I.2.1 程序类型

I.2.1.1 根据程序的模拟能力和用途，可将严重事故仿真程序分为三类:

（1）机理程序。机理程序的模型主要基于基本原理，用于计算严重事故进程中的主导现象，涉及从燃料损坏行为到放射性物质释放和迁移，再到氢气混合和燃烧过程等的广泛技术学科。在严重事故研究中通常使用这类程序来设计和分析严重事故试验。程序一旦被合适的试验工况所验证，就可作为一体化程序的比较基准。机理程序分析的详细程度一般都会超过大多数二级 PSA 所必需的要求程度。

（2）一体化程序。一体化程序通常采用简化的现象模型，也可能会采用简化模型和综合模型相结合来处理相同的过程，以便于能够相对快速地模拟整个核动力厂对假想的严重事故从始发事件到放射性物质释放到环境的响应过程。通过将一体化程序结果与试验数据以及机理程序的并行计算结果进行对比可以确定简化程度，简化的程度应正确地反映严重事故进程实际主导现象的主要特性。一体化程序可模拟的现象和过程包括:

— 反应堆冷却剂系统、安全壳结构和/或封闭厂房的热工水力过程;

— 堆芯冷却的降级、燃料升温、包壳氧化、燃料降级（燃料几何变形）、及堆芯材料的熔化和再分布;

— 燃料材料的再分布引起的RPV下封头的升温、RPV下封头的热工及机械载荷和失效;

— 堆芯材料从RPV到堆腔的迁移;

— 熔融堆芯碎片和安全壳底板上的混凝土间的热-化学相互作用以及引发气溶胶的生成;

— 压力容器内外的氢气生成、传输和燃烧;

— 放射性物质（气溶胶和蒸汽）释放、迁移和沉积;

— 放射性气溶胶在反应堆安全壳厂房中的行为，如气溶胶颗粒在水池中的水洗、在气空间的凝聚和重力沉降等;

— 专设安全设施对热工水力和放射性核素行为的影响。

一体化程序是二级PSA常用的程序。可用于评估核动力厂在不同事故序列下的响应，或者通过对同一个事故序列进行多次计算以支持不确定性分析。

（3）参数化程序。参数化程序基于简单参数的模型对复杂程序的计算结果进行差值计算，以建立初步的技术基础。参数化程序可为特定 PSA 应用提供粗略估计的参数，如估算放射性源项或高压熔融物喷射的安全壳荷载等。参数化程序可以得到不确定性分析结果，但参数化程序使用的参数以及它们生成的结果必须被更详细的计算或实验数据所校核。

I.2.2 程序的验证

I.2.2.1程序的验证是增强应用信心的关键。严重事故程序要

通过合理验证是很困难的。严重事故中发生的极端情况和真实的物理尺度难以通过实验实现。通常，验证过程由含有众多模拟的验证矩阵组成。应谨慎地验证这些程序，通过改变用户提供的参数值去验证程序，直到对实验数据的合理符合。最好这是参数值的非直接试验测量，并且不是程序的独立验证。

I.2.3 程序的使用

I.2.3.1 严重事故仿真程序应便于二级PSA分析人员使用。使用者不需要具备严重事故专业特定领域的详细知识。为了能够将程序的计算与二级PSA的工作框架有效地配合，分析者必须具备以下合理的知识:

（1）程序中描述的现象及其模化方法和局限性;

（2）输入变量的含义;

（3）输出变量的含义。

I.2.3.2 程序使用者应全面了解程序的优点和局限性，不应在其设计工况和条件的范围以外使用程序。

I.2.3.3 在二级 PSA 中应用的一体化程序应能够处理图 I-1 所示的大部分或者全部现象。

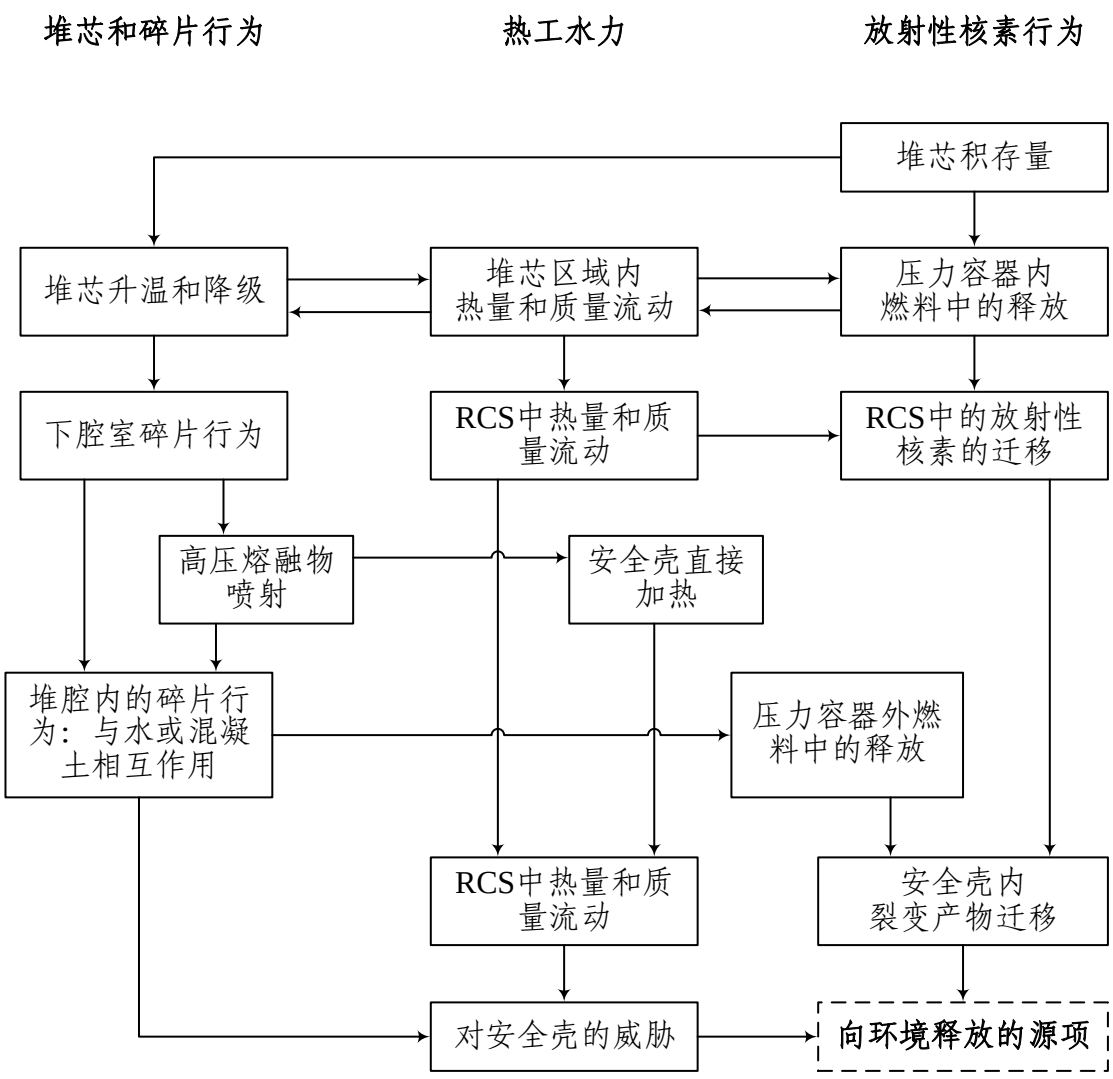

图 I-1 应用于二级 PSA 的一体化程序涉及的严重事故现象