核安全导则

# 核动力厂确定论安全分析

国家核安全局 2021 年 X 月 XX 日批准发布

国家核安全局

# 核动力厂确定论安全分析

（2021 年 X 月 XX 日国家核安全局批准发布）

本导则自 2021 年 X 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**

1.1 目的 1

1.2 范围 1

**2 总则 2**

2.1 确定论安全分析目的 2

2.2 确定论安全分析验收准则 3

2.3 确定论安全分析中的不确定性分析 4

2.4 确定论安全分析方法 4

2.5 放射性物质释放到环境中的源项 6

**3 假设始发事件和事故序列的识别、分类和分组 7**

3.1 概述 7

3.2 正常运行 8

3.3 假设始发事件 9

3.4 预计运行事件和设计基准事故假设始发事件的识别 12

3.5 识别设计扩展工况的总体考虑 17

3.6 没有造成堆芯明显损伤的设计扩展工况的识别 18

3.7 堆芯熔化设计扩展工况的识别 20

3.8 内部危险和外部危险导致的假设始发事件的识别 22

3.9 实际消除的事件序列和事故情景 22

**4 确定论安全分析验收准则 24**

4.1 基本原则 24

4.2 放射性验收准则 25

4.3 技术验收准则 26

4.4 其他 28

**5 确定论安全分析中保证安全裕量的通用方法 28**

5.1 总则 28

5.2 针对预计运行事件及设计基准事故的保守方法和组合方法的确定论安全分析 ..... 31
5.3 针对预计运行事件及设计基准事故的最佳估算加不确定性量化的确定论安全分析 ..... 34
**6 核动力厂不同状态的确定论分析方法 ..... 36**
6.1 总则 ..... 36
6.2 正常运行条件下的确定论安全分析 ..... 37
6.3 针对预计运行事件的现实性确定论安全分析 ..... 39
6.4 针对预计运行事件和设计基准事故的保守性确定论安全分析 ..... 41
6.5 没有造成堆芯明显损伤的设计扩展工况的确定论安全分析 ..... 46
6.6 堆芯熔化的设计扩展工况的确定论安全分析 ..... 49
6.7 支持“实际消除”的确定论安全分析 ..... 52
**7 确定论安全分析的归档、审查和更新 ..... 53**
7.1 概述 ..... 53
7.2 文件中的敏感信息 ..... 55
7.3 确定论安全分析的审查和更新 ..... 55
**名词解释 ..... 57**

# 1 引言

## 1.1 目的

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，其目的是给新建核动力厂确定论安全分析提供指导。本导则可作为在役核动力厂设计修改和安全审查的参考。

## 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，其他类型或采用革新技术的反应堆设计可参考本导则，但应经过细致的评价和判断。

1.2.2 本导则主要针对新建核动力厂，为确定论安全分析提供指导，以确认其符合安全相关的目标。确定论安全分析主要用于论证核动力厂设计上能够完全实现其安全功能，确保核动力厂在所有的状态下，能够防止放射性物质向环境的不可控释放，验证其运行限值和条件的合理性。确定论安全分析也用于根据不同核动力厂状态下的屏障状态，确定潜在的放射性物质释放（源项）特征。

1.2.3 本导则还可以应用于以下方面：

（1）核动力厂定期安全评价，确保核动力厂满足安全要求；

（2）核动力厂修改的安全分析；

（3）对实际运行事件，或这些事件与其他超出正常运行限值的假想故障组合的分析；

（4）开发和验证应急运行规程；

（5）开发严重事故管理指南；

（6）1 级和 2 级概率安全分析（PSA）中事故序列的开发和成功准则的验证。

1.2.4 本导则不包括核安保相关建议。

# 2 总则

## 2.1 确定论安全分析目的

2.1.1 核动力厂确定论安全分析的目的是确认：依靠安全功能的可靠执行（包括必要的构筑物、系统和设备，并结合操纵员动作），足够保证核动力厂放射性物质释放低于可接受限值，且具有合适的裕量。确定论安全分析需要证明核动力厂放射性屏障在所要求的范围内保持其完整性。确定论安全分析可被进一步的具体信息和分析（如与制造、测试、检验、运行经验评价有关的信息和分析）以及概率安全分析所补充，同时也有助于证明：

（1）在核动力厂不同状态下，源项和潜在的放射性后果是可接受的；

（2）导致早期放射性释放或大量放射性释放的事件序列可被认为实际消除。

2.1.2 核动力厂不同状态下确定论安全分析的目的是，通过论证分析结果满足既定的验收准则，来证明工程设计的适当性。

2.1.3 确定论安全分析可预测核动力厂对假设始发事件的响应。每个核动力厂状态应用一套特定的规则和验收准则。通常，采用合适的计算工具分析中子物理、热工水力、热工机械、结构和放射性等方面。针对已确定的运行模式和核动力厂状态，应开展具体的计算模拟。

2.1.4 计算结果是特定物理参数（如中子注量率，反应堆热功率，一回路冷却剂压力、温度、流量和流速，实体屏障的载荷，可燃气体浓度，放射性核素的物理和化学成份，堆芯损伤状态，安全壳压力，释放到环境中的源项等）随空间和/或时间的变化值。

## 2.2 确定论安全分析验收准则

2.2.1 确定论安全分析的验收准则用于判断分析结果的可接受性，以此作为核动力厂安全的证明。验收准则可以用总体性描述、定性术语或定量限值来表示，可以分为三类：

（1）安全准则：与运行状态或事故工况的放射性后果直接相关的准则，或与放射性屏障完整性相关的准则，应对这些准则进行适当考虑，以保证相关安全功能；

（2）设计准则：构筑物、系统和设备的设计限值，是设计基准的一部分，是满足安全准则的重要前提；

（3）运行准则：在正常运行和预计运行事件下操纵员必须遵守的规则，为满足设计准则和安全准则提供前提条件。

2.2.2 在本导则中，仅涉及安全验收准则。监管机构批准的验收准则相对于安全准则可以存在适当的裕量。

## 2.3 确定论安全分析中的不确定性分析

确定论安全分析中使用的不确定性分析方法包括：

（1）采用专家判断、统计学和敏感性计算相结合的方法；

（2）采用试验结果；

（3）采用包络分析计算。

## 2.4 确定论安全分析方法

2.4.1 表 1 列出了当前可用于确定论安全分析的不同选项，根据所采用的计算机程序、系统可用性假设和分析中采用的初始条件和边界条件，这些选项具有不同程度的保守性。

| 选项 | 方法 | 计算机程序 | 系统可用性假设 | 初始条件和边界条件 |
|---|---|---|---|---|
| 1 | 保守方法 | 保守 | 保守 | 保守 |
| 2 | 组合方法 | 最佳估算 | 保守 | 保守 |
| 3 | 最佳估算加不确定性分析 | 最佳估算 | 保守 | 最佳估算数据，部分最不利条件 |
| 4 | 现实方法[1] | 最佳估算 | 最佳估算 | 最佳估算 |

注 1：即最佳估算分析方法

表 1　确定论安全分析选项

2.4.2 选项 1 是一种保守方法，保守考虑核动力厂状态和物理模型。在保守方法中，参数取值应使针对特定验收准则的分析结果较为保守。采用保守方法来简化分析，并采用较大的保守性，来补偿对模型和物理现象认知上的不足。这种方法假设可包络多种相似的瞬态，使所有被包络的瞬态都能满足验收准则要求。

2.4.3 选项 2 是组合方法，采用最佳估算的模型和计算机程序替代保守的模型和计算机程序。将最佳估算计算机程序、保守

的初始条件和边界条件，与保守的系统可用性假设结合使用。该方法假设与计算机程序模型相关的所有不确定性都已确定，并且根据核动力厂运行经验使用保守的核动力厂参数。此方法需要进行敏感性研究，以证明选择的保守输入数据是正确的。选项 2 通常用于设计基准事故和预计运行事件的保守分析。

2.4.4 选项 3 是最佳估算加不确定性方法。允许使用最佳估算计算机程序和更现实的假设。考虑到所有参数同时处于最恶劣值的概率很低，因此可以使用最佳估算和部分不利（即部分保守）初始条件和边界条件相结合的方法。系统可用性通常采用保守的假设。为了确保设计基准事故分析所需的总体保守性，需要对不确定性进行识别、量化和统计组合。选项 3 包含一定程度的保守性，目前用于部分设计基准事故和预计运行事件的保守分析。

2.4.5 原则上选项 2 和 3 是截然不同的分析类型，然而在实践中通常采用选项 2 和选项 3 相结合。这是因为当有大量可用数据时，倾向于使用最佳估算输入数据，而当缺少数据时，倾向于使用保守的输入数据。选项之间的差异是不确定性的统计组合。

2.4.6 根据选项 1 至选项 3 进行的确定论安全分析是保守的，保守程度从选项 1 至选项 3 依次降低。

2.4.7 选项 4 允许使用最佳估算模型和计算机程序，以及最佳估算的系统可用性、初始条件和边界条件。选项 4 适用于旨在评价控制系统能力的预计运行事件的现实分析，通常也适用于设计扩展工况的最佳估算分析，同时也可用于确认规定的操纵员动作的现实分析，也可用于概率安全分析中的确定论安全分析。最

佳估算模型也可用于允许短期放宽监管要求的运行事件的确定论安全分析。

## 2.5 放射性物质释放到环境中的源项

2.5.1 确定论安全分析的一个重要方面是放射性物质释放源项的确定。该源项对于预测环境中放射性物质的扩散、核动力厂工作人员和公众的辐射剂量，以及对环境的放射性影响都十分重要。

2.5.2 为了评价核动力厂的源项，需要识别辐射源，确定产生的放射性核素的总量，了解放射性物质从核动力厂释放到环境的迁移机理。在事故工况下，需要采用计算机程序进行源项评价，要求计算机程序能够预测裂变产物从燃料元件的释放，裂变产物通过一回路系统、安全壳或乏燃料水池厂房的迁移，影响裂变产物迁移的相关化学现象，以及放射性物质释放的形态。

2.5.3 需要分别针对运行状态和事故工况进行源项评估，用于：

（1）确认设计已达到最优化，使得在核动力厂所有状态下源项都被减小到可合理达到的尽量低的水平；

（2）支持论证导致早期放射性释放或大量放射性释放的事件序列可被实际消除；

（3）论证设计能够确保包含剂量约束在内的辐射防护要求得到满足；

（4）为应急计划提供基准，应急计划要求在核动力厂紧急状态下能够保护人类生命、健康以及环境；

（5）确定设备鉴定所需的环境条件；

（6）为应急计划相关的培训活动提供数据；

（7）支持严重事故缓解设施（如安全壳过滤排放系统）的设计。

2.5.4 本导则所阐述的关于确定论安全分析的准则也适用于源项的确定。

# 3 假设始发事件和事故序列的识别、分类和分组

## 3.1 概述

3.1.1 本导则确定论安全分析中考虑的核动力厂状态包括：

（1）正常运行；

（2）预计运行事件；

（3）设计基准事故；

（4）设计扩展工况，包括没有造成堆芯明显损伤的工况和堆芯熔化（严重事故）工况。

3.1.2 确定论安全分析应涵盖核动力厂所有假设始发事件，这些始发事件源于核动力厂的任何部分，由于事件本身或叠加其他可能的失效（如保护系统和控制系统以及相关安全功能），可能导致放射性物质释放到环境。这些始发事件导致的放射性物质释放可能源自反应堆堆芯，也可能是其他相关来源（如核动力厂内贮存的燃料元件、放射性物质处理系统等）。

3.1.3 对于给定厂址，如果有多个机组、乏燃料贮存单元或其他可能的放射性释放源，应考虑单一事件引起若干或所有机

组、乏燃料贮存单元或其他放射性释放源同时发生始发事件的可能性。

3.1.4 确定论安全分析应涵盖核动力厂所有正常运行模式下可能发生的假设始发事件。在始发事件发生前，初始条件应假设正常运行的设备处于稳定状态。

3.1.5 应考虑每个停堆模式（包括换料和维修）的电厂配置。对于这些模式，应考虑停堆期间可能发生的导致风险上升的故障或其他因素，例如：

（1）某些安全系统不能自动或手动启动；

（2）自动系统功能丧失；

（3）设备处于维修期间；

（4）一回路冷却剂装量较少（某些模式下二回路装量较少）；

（5）仪表关闭或不工作，导致无法测量；

（6）一回路处于开口状态；

（7）安全壳处于开口状态。

3.1.6 对于乏燃料水池相关的假设始发事件，应考虑与燃料操作和贮存相关的特定运行模式。

3.1.7 如果核动力厂运行模式的持续时间很短，且定量分析表明在此期间发生的假设始发事件对总风险（包括可能导致早期放射性释放或大量放射性释放的风险）的贡献可以忽略，则确定论安全分析中可以不考虑这些假设始发事件。然而，仍然需要根据具体情况通过合适的程序或措施来预防或缓解这些事件。

## 3.2 正常运行

3.2.1 确定论安全分析应包括正常运行分析。一般来说，正常运行包括如下运行工况：

（1）从停堆状态的正常启堆，达到临界和达到额定功率；

（2）功率运行，包括额定功率和低功率运行；

（3）反应堆功率变化，包括负荷跟踪模式，以及低功率运行一段时间后重返额定功率（如果适用）；

（4）功率运行时反应堆停堆；

（5）热停堆；

（6）冷却过程；

（7）冷停堆；

（8）停堆期间换料或不停堆换料（如果适用）；

（9）换料或维修停堆模式下，一回路或安全壳处于开口状态；

（10）乏燃料池正常运行模式；

（11）燃料贮存和操作。

3.2.2 在核动力厂正常运行期间，还应考虑由于运行模式或功率输出的变化导致的核动力厂主要参数的变化。对于正常运行期间发生的瞬态，分析的主要目的是论证核动力厂参数可以维持在规定的运行限值和条件范围内。

## 3.3 假设始发事件

3.3.1 应基于核动力厂特定的假设始发事件清单来预测非正常运行条件（包括：预计运行事件、设计基准事故和设计扩展工况）下的核动力厂行为，对于特定事故序列可能叠加额外的设备

故障或人员差错。

3.3.2 应提供一套全面的假设始发事件清单，确保对核动力厂行为分析尽可能完整，以在设计中考虑所有可预见的具有严重后果的事件和发生频率高的事件。

3.3.3 假设始发事件清单应考虑运行经验反馈，包括可利用的相关数据、实际核动力厂或类似核动力厂的运行经验。

3.3.4 假设始发事件应涵盖所有可信的失效，包括：

（1）核动力厂的构筑物、系统和设备失效（或部分失效），包括可能的误触发；

（2）操纵员失误导致的失效，包括有缺陷或不完整的维修操作，以及控制设备限值错误设置或操纵员错误操作；

3.3.5 对核动力厂响应进行分析时，应将继发效应视为假设始发事件的一部分。这些继发效应包括：

（1）如果电力系统故障是始发事件的继发效应，那么在预计运行事件、设计基准事故或设计扩展工况分析时应假设该电力系统供电的所有设备不可用；

（2）如果始发事件是一个释能事件，例如承压系统故障导致热水释放或管道甩击，那么在预计运行事件、设计基准事故和设计扩展工况分析时应考虑潜在的可能受该事件影响的设备失效；

（3）对于内部危险（如火灾或水淹）或外部危险（如地震）引起的故障，假设始发事件应包括所有相关设备失效。这些相关设备是指设计上既不具备抵御上述事件的影响，也没有采取保护措施免受上述事件影响的设备。

3.3.6 确定论安全分析中，除始发故障和继发故障外，还从保守角度（如设计基准事故中的单一故障准则）或纵深防御角度（如共因失效）假设其他故障。应区分上述故障与假设始发事件本身或继发的故障。此外，为了减少分析数量，分析时可增加一些故障来包络一组类似事件。

3.3.7 确定论安全分析中，假设始发事件只需包括直接挑战安全功能并最终威胁放射性屏障完整性的故障，包括始发的或继发的故障。因此，内部或外部危险（自然的或人为的）本身不作为确定论安全分析的假设始发事件。但是，应考虑这些危险的载荷的影响，包括这些危险引起的多重故障，它们是假设始发事件的潜在诱因。

3.3.8 如果由工程判断、确定论安全分析和概率论安全分析的结果表明事件组合将可能导致预计运行事件或事故工况，则必须主要根据其发生的可能性，将这些事件组合纳入设计基准事故或设计扩展工况。

3.3.9 必须在工程判断、确定论和概率论评价相结合的基础上系统性地识别假设始发事件。包括通过结构化的方法识别假设始发事件，例如：

（1）采用危险影响评估和系统可运行性影响分析、故障模式和影响分析、工程判断和主逻辑图等分析方法；

（2）与类似核动力厂安全分析中假设的始发事件清单进行比较；

（3）分析类似核动力厂的运行经验数据；

（4）采用概率安全分析的结果和见解。

3.3.10 某些极限故障在确定论安全分析中通常作为设计基准事故考虑（例如：大破口丧失冷却剂事故，主蒸汽或主给水管道破裂事故，压水堆弹棒事故）。它们是反应堆必须抵御的代表性事故。

3.3.11 如果支持系统发生的故障影响核动力厂正常运行，并最终要求触发反应堆保护系统或安全系统，也应考虑为假设始发事件。

3.3.12 在设计和安全评价过程中应审查假设始发事件清单，并且在设计和安全评价中进行迭代。在整个核动力厂寿期内也应定期审查假设始发事件（例如作为核动力厂定期安全评价的一部分），以确保它们仍然有效。

## 3.4 预计运行事件和设计基准事故假设始发事件的识别

3.4.1 结合事件后的物理进程，应将假设始发事件划分为若干具有代表性的事件序列组。每个组内的事件序列对安全功能和屏障带来相似的挑战，并且需要相似的缓解系统使核动力厂达到安全状态。因此，某个具有代表性的事件序列可以包络所有同类事件，在处理事件序列组时通常是指该代表性的事件序列。也可以根据发生频率对这些事件序列组进行分类。该方法允许组内所有假设始发事件采用相同的验收准则、初始条件、假设条件和分析方法。例如，一般情况下，“停运一台主给水泵”，“停运所有主给水泵”和“可隔离的主给水系统管道破裂”这些假设始发事件都被分组到“丧失主给水”这一代表性的事件序列。

3.4.2 代表性的事件序列也可以根据事件类型进行分类，比如：堆芯冷却恶化、反应堆冷却剂系统升压、安全壳升压、放射性后果或承压热冲击。例如，代表性的事件序列“丧失主给水”可以归类到“反应堆冷却剂系统排热减少”。

3.4.3 与预计运行事件和设计基准事故相关的假设始发事件应反映特定设计的特性。典型的始发事件和事件序列参见第 3.4.6 节和第 3.4.8 节。可按照下列典型的事件类型进行分类：

（1）反应堆冷却剂系统排热增加或减少；

（2）反应堆冷却剂系统流量增加或减少；

（3）堆芯反应性或功率分布异常，新燃料或乏燃料贮存时反应性异常；

（4）反应堆冷却剂系统装量增加或减少；

（5）潜在的旁通安全壳的反应堆冷却剂系统泄漏；

（6）向安全壳外的泄漏；

（7）乏燃料池水装量减少或丧失冷却；

（8）功率运行换料期间燃料丧失冷却（重水堆）；

（9）子系统或设备释放放射性物质（一般为放射性废物处理及贮存系统）。

3.4.4 对于源项分析，假设始发事件的特定分组可能足以说明放射性物质释放到环境的不同途径。需要特别关注可能旁通安全壳的放射性物质释放事故，因为即使堆芯的放射性物质释放量相对较小，仍然具有潜在严重后果。

3.4.5 每个假设始发事件组内，代表性的事件序列应根据该

组内假设始发事件最大发生频率进行分类。在确定假设始发事件频率范围时，应采用合适的方法进行核实。

3.4.6 根据事件类型，预计运行事件应包括下列典型的假设始发事件（下列事件主要用于示例，实际清单与反应堆类型和实际设计有关）：

（1）反应堆冷却剂系统排热增加：蒸汽释放阀误开启，压力控制故障导致蒸汽流量增加，给水系统故障导致排热能力增加，余热排出系统误投入；

（2）反应堆冷却剂系统排热减少：给水泵停运，各种原因（控制故障、主蒸汽阀关闭、汽机停机、丧失外电负荷和其他外电网扰动、失电、丧失冷凝器真空）引起的蒸汽流量下降；

（3）反应堆冷却剂系统流量增加：一台停运的冷却剂泵启动；

（4）反应堆冷却剂系统流量减少：一台或多台冷却剂泵停运，一条主冷却剂环路误隔离（如果适用）；

（5）堆芯反应性和功率分布异常：控制棒组失控提升，化学和容积控制系统故障导致的硼稀释（压水堆），燃料组件装错位置；

（6）新燃料或乏燃料贮存时反应性异常：乏燃料池硼稀释；

（7）丧失慢化剂循环，慢化剂热阱能力下降或丧失（重水堆）；

（8）反应堆冷却剂系统装量增加：化学和容积控制系统故障，应急堆芯冷却系统误运行；

（9）反应堆冷却剂系统装量减少：仪表管线故障导致的非常小的丧失冷却剂事故；

（10）乏燃料池燃料冷却能力下降或丧失：丧失场外电源，衰变热排出系统故障，乏燃料池水泄漏；

（11）反应堆冷却剂系统泄漏并可能旁通安全壳，从而导致放射性物质释放；

（12）子系统或设备泄漏导致的放射性物质释放：放射性废物处理系统或污水系统小泄漏。

3.4.7 应识别可能导致设计基准事故的假设始发事件。识别为预计运行事件的所有假设始发事件也应采用设计基准事故规则进行分析，即证明“通过安全系统的自动响应并结合所规定的操纵员动作”能够管理预计运行事件和设计基准事故。虽然假设始发事件通常不包含发生频率很低的事件，但是确定频率下限时应考虑特定反应堆的安全目标。

3.4.8 根据事故类型，设计基准事故应包括下列典型假设始发事件（下列事件主要用于示例，实际清单与反应堆类型和实际设计有关）：

（1）反应堆冷却剂系统排热增加，如蒸汽管道破裂；

（2）反应堆冷却剂系统排热减少，如给水管道破裂；

（3）反应堆冷却剂系统流量减少，如反应堆冷却剂泵卡转子或断轴，所有反应堆冷却剂泵停运；

（4）反应性和功率分布异常，如单束控制棒失控提升，弹棒（压水堆），非运行环路启动导致的硼稀释（压水堆）；

（5）反应堆冷却剂系统装量减少，如各种破口谱的丧失冷却剂事故，一回路系统卸压阀误开启，一回路向二回路泄漏；

（6）乏燃料池燃料冷却能力下降或丧失，如与水池相连的管道破裂；

（7）功率运行换料期间燃料丧失冷却（重水堆）；

（8）丧失慢化剂循环，慢化剂热阱能力下降或丧失（重水堆）；

（9）反应堆冷却剂系统、子系统、设备的泄漏并可能旁通安全壳，从而导致放射性物质释放，如在运输过程中或贮存时，乏燃料过热或损坏，废气或废液处理系统破口；

（10）端屏蔽冷却失效（重水堆）。

3.4.9 为证明根据事件发生频率对假设始发事件进行分类的合理性，应采用概率论分析方法支持确定论安全分析。频率计算应考虑可能发生假设始发事件的核动力厂运行状态（例如额定功率运行或者热停堆）的时间份额。应特别注意，有可能降低屏障完整性的瞬态的分类应与该瞬态对屏障可能的影响相一致。

3.4.10 每个事件类别应选取一些极限工况（即包络情景）。选取的极限工况应最可能挑战相关的验收准则，并且使得安全相关设备的性能参数达到极限。为包络该组内所有可能的假设始发事件，在包络情景范围内，多个假设始发事件可以组合，以使得它们的后果更恶劣。安全分析需确认始发事件的分组和选取的包络情景可接受。

3.4.11 针对不同的验收准则，单个事件可以从不同角度开展分析（如压水堆核动力厂丧失冷却剂事故，该事故应针对堆芯冷

却恶化、安全壳升压、放射性物质迁移并释放到环境等多个方面开展分析)。

3.4.12 应评价新燃料和辐照后的燃料操作期间的事故。该类事故可能发生在安全壳内和安全壳外。

3.4.13 还有其他一些假设始发事件可能导致放射性物质释放到安全壳外，这类事件包括：

（1）位于安全壳外的乏燃料水池中的燃料冷却能力降低或丧失；

（2）新燃料或乏燃料反应性增加；

（3）任何处理固体、液体或气体放射性物质的辅助系统意外排放；

（4）正常运行时，用于过滤或缓解放射性物质释放的系统或设备（如过滤器或衰变箱）失效；

（5）换料或维修期间反应堆或安全壳开口状态下发生的事故。

3.4.14 预计运行事件或设计基准事故的包络工况的频率取值应包络该组内所有假设始发事件的发生频率。

## 3.5 识别设计扩展工况的总体考虑

3.5.1 必须在工程判断、确定论和概率论安全评价的基础上得出一套设计扩展工况，目的是增强核动力厂应对比设计基准事故更严重的或包含多重故障的事故的承受能力，避免不可接受的放射性后果，以进一步改进核动力厂的安全性。设计必须考虑这些设计扩展工况来确定额外的事故情景，并针对这类事故制定切

实可行的预防和缓解措施。

3.5.2 应识别两类设计扩展工况：

（1）没有造成堆芯明显损伤的设计扩展工况；

（2）堆芯熔化的设计扩展工况，即严重事故。

这两类设计扩展工况的确定论安全分析可采用不同的接受准则和方法。

## 3.6 没有造成堆芯明显损伤的设计扩展工况的识别

3.6.1 在初步选取没有造成堆芯明显损伤的设计扩展工况时，需考虑发生频率很低的单一始发事件或多重故障，这些工况需满足防止堆芯损伤的接受准则。

3.6.2 应得出一套确定的没有造成堆芯明显损伤的设计扩展工况清单。相关的设计扩展工况应包括：

（1）始发事件导致的工况可能超出用来缓解设计基准事故的安全系统的能力（如压水堆核动力厂蒸汽发生器多根传热管破裂）。

（2）预计运行事件或设计基准事故叠加多重故障（如共因失效），这些故障导致安全系统不能执行其预期功能（如丧失冷却剂事故叠加安注失效）。支持系统失效也是导致安全系统失效的起因之一。应通过分析任一安全系统完全失效对核动力厂的影响来系统性识别这些序列，这些安全系统在预计运行事件或设计基准事故（尤其是较可能发生的预计运行事件和设计基准事故）安全分析时认为有效。

（3）可信的假设始发事件包含多重故障导致的执行一部分正常运行功能的某个安全系统丧失。该情况适用于某些设计（如在事故期间或停堆期间使用相同的排热系统）。应通过分析正常运行所需的任一安全系统完全失效对核动力厂的影响来系统性识别这些序列。

3.6.3 设计扩展工况在很大程度上取决于具体的技术和设计，但是，没有造成堆芯明显损伤的设计扩展工况可初步参考下列清单，并应根据核动力厂的类型和设计进行选取：

（1）通常不作为设计基准事故的发生频率很低的始发事件：

— 蒸汽发生器多根传热管破裂（压水堆，重水堆）；

— 主蒸汽管道破裂和继发的蒸汽发生器传热管破裂（压水堆，重水堆）。

（2）预计运行事件或设计基准事故叠加安全系统多重故障：

— 未能紧急停堆的预期瞬态：预计运行事件叠加控制棒插入堆芯失效；

— 全厂断电：丧失场外电源叠加应急柴油发电机或备用应急电源失效；

— 丧失全部给水：丧失主给水叠加丧失全部应急给水；

— 丧失冷却剂事故叠加完全丧失一类应急堆芯冷却设施（高压或低压应急堆芯冷却系统）；

— 假设始发事件后维持长期稳定阶段丧失所需的安全系

统。

（3）包含多重故障的假设始发事件：

— 完全丧失设备冷却水系统或重要厂用水系统；

— 冷停堆或换料期间丧失余热排出系统；

— 丧失用于乏燃料池正常冷却和设计基准事故缓解的冷却系统；

— 丧失最终热阱的正常途径。

3.6.4 为了识别没有造成堆芯明显损伤的设计扩展工况，应特别关注辅助和支持系统（例如：通风系统，冷却系统和供电系统），因为这些系统可能导致运行系统和安全系统立即或随后发生多重故障。

3.6.5 对于没有造成堆芯明显损伤的设计扩展工况的不同序列，如果它们对安全的挑战相似，则应将它们归为一组。每组应对包络情景开展分析，该包络情景对相关接受准则具有最大的挑战。

3.6.6 应单独列出在每个没有造成堆芯明显损伤的设计扩展工况序列中考虑的多重故障。

## 3.7 堆芯熔化设计扩展工况的识别

3.7.1 根据核动力厂安全目标，应选取一系列堆芯熔化的序列（严重事故）开展分析，以建立用于缓解该类事故后果的安全设施的设计基准。这些序列可代表所有堆芯熔化序列的主要物理现象（例如：一回路压力、堆芯衰变热或安全壳状态）。

3.7.2 应假设防止堆芯熔化的系统失效或无法充分发挥作

用，从而使得事故发展至严重事故。应在设计基准事故、设计扩展工况以及概率安全分析中识别出的主导事故序列的基础上，考虑额外的故障或操纵员错误响应，从而选取具有代表性的序列。

3.7.3 应分析每条接受准则相对应的堆芯熔化设计扩展工况的代表性序列，以确定极限工况（尤其是可能挑战安全壳完整性的序列），为安全壳和缓解事故后果所需的安全设施的设计提供输入。

3.7.4 设计扩展工况在很大程度上取决于具体的技术和设计，但是，堆芯熔化的设计扩展工况（严重事故）可初步参考下列事故，并且应该根据核动力厂的类型和设计进行选取：

（1）丧失堆芯冷却能力，比如丧失场外电叠加部分或全部丧失厂内交流电源和/或丧失最终热阱的正常途径（具体序列与设计有关）；

（2）丧失反应堆冷却剂系统的完整性，比如丧失冷却剂事故叠加应急堆芯冷却系统失效或者超出应急堆芯冷却系统能力。

3.7.5 不论设计中是否提供保护，都应在分析中假设堆芯熔化的发生。为了防止安全壳失效，分析应论证在堆芯熔化事故工况下不会发生高能现象（即认为该现象发生的可能性已被实际消除）。

3.7.6 应选取堆芯熔化设计扩展工况的代表性序列，以识别严重事故现象导致的极限的核动力厂参数。这些参数用于核动力厂构筑物、系统和设备的确定论安全分析，以论证该严重事故序列下放射性后果的接受值。上述序列分析应考虑环境条件，以评

价严重事故中使用的设备是否能够在需要时执行其功能。

## 3.8 内部危险和外部危险导致的假设始发事件的识别

3.8.1 确定假设始发事件时需考虑相关的厂址特定内部危险和外部危险的影响（单独或组合）。内部危险和外部危险分析与假设始发事件（由核动力厂系统单一故障或多重故障导致，或由对实现基本安全功能存在直接影响的操纵员失误导致）分析不同。危险本身不作为假设始发事件，但危险产生的载荷可能会导致这些事件。

3.8.2 对于多机组厂址，为确定厂址特定危险导致的假设始发事件，应考虑该危险同时影响若干或所有机组的可能性。尤其应考虑丧失电网、丧失最终热阱的正常途径和共用设备失效的影响。

3.8.3 应采用概率论方法或工程判断方法对危险进行分析，以论证对于每个危险符合下列条件之一：

（1）由于对风险贡献可忽略，该危险可以筛除；

（2）核动力厂设计足够稳健，可预防危险产生的载荷导致始发事件；

（3）危险导致的始发事件已经在设计中考虑。

3.8.4 如果危险导致了始发事件，始发事件分析时应只考虑经鉴定的或被保护不受该危险影响的构筑物、系统和设备可用。

## 3.9 实际消除的事件序列和事故情景

3.9.1 纵深防御第四层次的安全目标是，在严重事故下仅需要在区域和时间上采取有限的防护行动，且避免场外放射性污染

或将其减至最小。这要求可能导致早期放射性释放或者大量放射性释放的事件序列被实际消除。

3.9.2 需实际消除的事件序列可根据具体的堆型设计来确定，通常可包含以下几类：

（1）导致堆芯快速损伤并进而引起安全壳早期失效的事件，如：

— 反应堆冷却剂系统的大型承压部件失效；

— 不可控的反应性事故。

（2）导致安全壳早期失效的严重事故序列，例如：

— 安全壳直接加热；

— 大规模蒸汽爆炸；

— 大空间可燃气体（包括氢气和一氧化碳）的爆炸。

（3）导致安全壳晚期失效的严重事故序列，例如：

— 堆芯熔融物与混凝土相互作用导致的底板熔穿或安全壳旁通；

— 长期丧失安全壳排热；

— 大空间可燃气体（包括氢气和一氧化碳）的爆炸。

（4）安全壳旁通的严重事故；

（5）燃料贮存池中的燃料明显损伤和不可控释放。

3.9.3 实际消除的事件序列不作为确定论安全分析的一部分，但确定论安全分析能够支持论证设计和运行特征可有效实际消除这些事件序列。

# 4 确定论安全分析验收准则

## 4.1 基本原则

4.1.1 全面负责设计过程的部门必须保证核动力厂设计满足安全性、可靠性和质量方面的验收准则。这些准则符合相关的法律法规和标准规范。

4.1.2 确定论安全分析方法必须包括将分析结果与验收准则、设计限值、剂量限值以及可接受限值进行比较，以满足辐射防护要求。应通过确定论安全分析证明满足相应的验收准则。

4.1.3 应为运行状态和事故工况的整个范围建立验收准则。这些准则的目的是防止相关屏障损坏而导致放射性物质释放，从而防止放射性释放（和后果）超出可接受限值。准则的选取应确保准则与丧失屏障完整性的物理限值之间有合适的裕量。

4.1.4 验收准则应与工况的发生频率有关。发生频率较高的工况（如正常运行或预计运行事件）的验收准则应比发生频率较低的工况(如设计基准事故或设计扩展工况)的验收准则更严格。

4.1.5 验收准则应在如下两个层次内确定：

（1）放射性验收准则，该准则与核动力厂的运行状态或事故工况的放射性后果相关。这些准则一般由法律和监管要求规定，通常表述为活度水平或剂量；

（2）技术验收准则，该准则与防止放射性物质释放的屏障（如燃料芯块、燃料包壳、反应堆冷却剂系统压力边界和安全壳）

完整性相关。该准则是由监管要求规定，或者是由设计方提出并被监管机构认可、以在安全论证中使用的。

## 4.2 放射性验收准则

4.2.1 放射性验收准则应表述为核动力厂工作人员、公众或环境（如适用，应包括非人类生物）的有效剂量、当量剂量或剂量率。与剂量相关的放射性验收准则应根据现行的安全要求确定。

4.2.2 为了将核动力厂设计特征与环境特性解耦，表述为剂量的放射性验收准则可转换为不同放射性核素的可接受活度水平。

4.2.3 正常运行条件下的放射性验收准则一般应表述为核动力厂工作人员和核动力厂邻近公众的有效剂量约束值，或表述为核动力厂排放的放射性活度控制值。

4.2.4 为预计运行事件制定的放射性验收准则应比设计基准事故的验收准则严格。

4.2.5 设计基准事故的放射性验收准则应确保在厂内、外没有或仅有微小的放射性后果，并且无须采取任何场外防护行动。

4.2.6 设计扩展工况的放射性验收准则应确保：

（1）安全壳及其安全设施必须能够承受包括堆芯熔化在内的极端事故情景；

（2）设计必须做到实际消除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发生的可能性；

（3）保护公众所采取的防护行动在持续时间和范围上必须

是有限的，并必须有足够的时间来采取这些防护行动。

## 4.3 技术验收准则

4.3.1 为了保证满足验收准则或接受准则，可确定一系列技术验收准则。应根据挑战屏障完整性物理过程的主导参数来设置技术验收准则。工程实践中一般采用与屏障完整性相关的替代参数来建立验收准则或者验收准则的组合，以确保屏障的完整性。在确定这些验收准则时，应包含足够的保守性，以确保距离丧失屏障完整性仍有合适的裕量。

4.3.2 在规定技术验收准则时，应根据特定的设计方案考虑下列合适的准则：

（1）燃料芯块完整性相关的准则：最高燃料温度和最大径向平均燃料焓（考虑燃耗，燃料成份和添加物，如可燃毒物）；

（2）燃料包壳完整性相关的准则：最小偏离泡核沸腾比，最高包壳温度，包壳最大局部氧化量；

（3）反应堆堆芯整体完整性相关的准则：足够的次临界度，包壳氧化最大产氢量，堆芯燃料元件最大损坏量，燃料组件最大变形量（冷却、控制棒插入和移出的要求），排管式压力容器完整性（适用于重水堆）；

（4）堆外燃料完整性相关的准则：足够的次临界度，有足够的水位淹没燃料组件且有足够的热量排出能力；

（5）反应堆冷却剂系统完整性相关的准则：反应堆冷却剂系统最高压力，最高温度、压力和温度变化导致的反应堆冷却剂

系统压力边界应力和应变，假想的压力容器缺陷不会导致脆性断裂或延展性失效；

（6）二回路完整性相关的准则（如果相关）：冷却剂最高压力，二回路设备所承受的最大温度、压力和温度变化；

（7）安全壳完整性和限制放射性释放到环境相关的准则：最大和最小压力值及其持续时间，安全壳内外最大压差，最大释放率，可燃或可爆气体最大浓度，运行系统可接受的工作环境，安全壳内最高温度；

（8）限制放射性扩散的其他设备（如重水堆中的端屏蔽）完整性相关的准则：最大压力、温度和升温速率。

4.3.3 在停堆模式或任一屏障完整性丧失或降级情况下的假设始发事件，在可能的情况下应采用更严格的准则（如防止在开盖的压力容器和乏燃料水池内的冷却剂沸腾，或防止燃料组件裸露）。

4.3.4 通常，对于发生频率较高的始发事件，屏障完整性相关的技术验收准则更加严格。对于预计运行事件，不应导致物理屏障继发失效（燃料芯块、燃料包壳、反应堆冷却剂系统压力边界和安全壳）或燃料损坏（如果正常运行时允许在运行限值内有少量燃料泄漏，则不允许有更多燃料损坏）。对于设计基准事故和不会导致堆芯明显损伤的设计扩展工况，应维持防止核动力厂放射性物质释放的屏障完整性（4.2.5 和 4.2.6 节）。对于堆芯熔化的设计扩展工况，应保证安全壳的完整性，同时防止安全壳被旁通，以确保防止早期放射性释放或大量放射性释放。

## 4.4 其他

4.4.1 应明确给出每个准则的适用范围和条件。比如，燃料熔化温度或燃料焓升应与燃耗和可燃毒物成份相关。为了限制放射性释放，应给出放射性物质释放的持续时间。根据条件不同，验收准则可能变化很大。因此，在安全分析中使用验收准则时，应给出足够详细的条件和假设。

4.4.2 虽然对安全重要的工程评价在安全分析中可能没有明确说明，但是它是安全评价的相关组成部分。构筑物、系统和设备设计时采用的安全裕量应与它们可能必须承受的载荷不确定性及其失效后果相当。

4.4.3 应力和应变评估除了考虑所有相关的物理量外，还应考虑由每个载荷或载荷组合造成的环境条件和适用的边界条件。验收准则应足以表明与假定载荷相关的事件发生后，缓解其后果必需的构筑物、系统和设备不会产生继发失效。

# 5 确定论安全分析中保证安全裕量的通用方法

## 5.1 总则

5.1.1 确定论安全分析应论证满足相关安全要求，而且重要参数实际值与放射性屏障的失效阈值之间有合适的裕量（取决于核动力厂状态）。应在许多方面考虑保守性，如验收准则或者物理模型、初始条件及边界条件。

5.1.2 计算机程序预测的不确定性可采用一些适当的方法隐性地反映，也可采用包含量化不确定性的最佳估算方法来显性地

反映。对于最极限情况（与验收准则相比裕量最小的情况）来说，这是极为重要的。

5.1.3 为了证明预计运行事件能够满足验收准则，分析时可考虑两套互补的方法，应根据分析目的来选取相应的分析方法，即考虑核动力厂控制及限制系统的现实方法与仅考虑安全系统的更为保守的方法。

5.1.4 必须用保守的方法来分析设计基准事故。该方法包括在分析中假定安全系统的某些故障模式，规定设计准则，采用保守的假设、模型和输入参数等。

5.1.5 必须对核动力厂开展设计扩展工况分析。必须保证核动力厂能进入可控状态并维持安全壳功能，从而能实际消除导致早期放射性释放或大量放射性释放的核动力厂状态发生的可能性。相关的分析可采用最佳估算方法。

5.1.6 当采用最佳估算分析时，仍然需要保证距离丧失屏障完整性有合适的裕量。应通过敏感性分析来论证可避免潜在的可能造成早期放射性释放及大量放射性释放的陡边效应。该论证结论在采用最佳估算方法分析设计扩展工况时特别重要，特别是对于严重事故，其导致屏障降级从而造成早期放射性释放或大量放射性释放的可能性较高。

5.1.7 应识别对分析结果最为敏感的参数。通过对关键输入参数系统性变化进行敏感性分析，以确定该类参数对分析结果的影响。这些敏感性分析不但用于确定可能对系统安全带来最大挑战的重要参数值，也用于论证实际情况下参数可预见的变化不会

带来陡边效应。应注意的是，当每次改变一个参数进行敏感性分析时，由于不一定能体现多个参数同时变化时可能的补偿或累积效应，可能会得到误导性的结果。

5.1.8 基于现实原因，只能考虑对有限数量的被识别为对结果有重要影响的参数进行敏感性分析。在给定范围内改变参数的取值，以确定针对选定验收准则造成最小安全裕量的参数值。这些选值将会用于安全分析，并且参数的重要性可能会随着瞬态变化而变化。需要特别注意，不能对所选的相关的参数进行随意改变，否则有可能会带来数据矛盾的问题（比如质量不守恒）。

5.1.9 确定论安全分析中，应基于安全分析目的及核动力厂状态，考虑与之相称的保守性。针对预计运行事件及设计基准事故，可考虑以下两种选项中的一种，或者两者结合的方式，由此来代替完全保守的分析方式（表 1 中的选项 1）：

（1）采用最佳估算计算机程序与保守输入数据（表 1 中的选项 2）；

（2）采用最佳估算计算机程序与最佳估算输入数据（表 1 中的选项 3）。

在前一种情况下，结果由一系列计算得到的保守参数来表示，这些参数是由验收准则所限定的。在后一种情况下，结果由计算参数的百分比或概率分布的形式来表示。

5.1.10 应认真遵守规范、程序记录及用户指南，以限制使用确定论安全分析方法时的人因影响（用户效应）。

5.1.11 初始与边界条件的选取应考虑核动力厂的几何边界变化、燃料燃耗变化及与运行年限相关的变化（如锅炉或蒸汽发

生器的结垢）。

## 5.2 针对预计运行事件及设计基准事故的保守方法和组合方法的确定论安全分析

5.2.1 在采用保守方法或组合方法时，须在核动力厂运行限值及条件所规定的参数范围内，选择保守的初始条件和边界条件。初始条件包括堆芯功率水平、功率分布、压力、温度和一回路流量等；边界条件包括触发整定值、核动力厂系统（如泵与电源）的性能、质量和能量的外部源项和损失项，以及其他在瞬态进程中变化的参数等。系统可用性及操纵员动作的保守假设在第6章核动力厂不同状态的确定论分析方法中讨论。

5.2.2 应选取的输入数据和模型假设，不仅考虑预计运行事件及设计基准事故中的中子物理和热工水力方面，还考虑辐射方面。特别是在向环境释放的源项分析中，须考虑下述因素：

（1）燃料（堆芯或乏燃料水池）内的裂变产物与其他同位素的总量；

（2）反应堆冷却剂系统内的放射性，包括了事件发生前及事件过程中挥发性裂变产物的释放（峰值）；

（3）燃料损伤（包壳泄漏）的时间进程与范围；

（4）燃料释放的放射性核素的份额；

（5）反应堆冷却剂系统与安全壳泄漏途径内的放射性核素的滞留；

（6）裂变产物在冷却剂汽液相间的份额分布；

（7）安全壳系统的性能（喷淋、通风、过滤、沉积及再悬浮）；

（8）安全壳的泄漏率及泄漏点；

（9）释放的时间及过程；

（10）释放的放射性物质的化学及物理形态，特别关注碘的形态；

（11）向环境释放的有效高度，该高度的确定需要考虑释放的能量。

5.2.3 当采用最佳估算计算机程序与保守输入及假设结合时，需要确保最佳估算计算机程序有关的不确定性被保守的输入充分补偿。分析必须包含计算机程序的确认、保守输入的采用以及敏感性研究，以评估及考虑计算机程序模型相关不确定性。这些研究可能随瞬态类别而变化，因此应在每次确定论安全分析中开展。

5.2.4 采用保守或组合方法时，初始与边界条件应设置为使安全相关参数结果更保守的值。初始与边界条件单组保守值未必能够导致每一个安全相关参数或验收准则的结果保守。因此，应基于特定的瞬态及验收准则来分别选择合适的保守初始与边界条件。

5.2.5 在选择分析所需保守的输入参数时，需要考虑以下因素：

（1）有意的保守假设可能未必导致预期的保守结果，比如不同的假设可能出现补偿效应并消除保守性；

（2）保守程度可能在事故进程中发生变化，一个假设可能无法在整个瞬态中都保持保守；

（3）某些保守假设可能导致对事件序列与时间表的预测存在误导或不真实；

（4）如果根据工程判断选择保守参数，则存在用户效应显著的风险，即用户没有采用合理的选择，从而导致无法获得保守的结果。

因此，针对每一条验收准则，都需要进行敏感性分析来支持输入的保守选择。建议至少选出那些对结果特别重要的序列，进行最佳估算结合不确定性量化分析。

5.2.6 由于保守计算机程序的运用可能会掩盖某些现象的影响或者显著改变现象出现的前后顺序，因此，针对该类现象，必须进行充分的敏感性分析以论证重要的事故现象没有被保守计算机程序所掩盖。

5.2.7 在保守方法中，应采用基于敏感性分析获得的核动力厂运行寿期中最为极限的初始条件。始发事件应在与反应堆初始条件（如核动力厂功率运行或停堆状态、功率水平、衰变热水平、裂变产物储量、反应性条件、反应堆冷却剂系统温度、压力和水装量）相关的最为不利的时刻发生。

5.2.8 初始条件的选取应包含可能出现的最不利状态的组合，但无需考虑不可能同时发生的初始条件。例如，极限衰变热功率与极限峰值因子物理上不可能同时在燃料瞬态中出现。

5.2.9 在保守初始条件的选择中可以不用考虑出现频率极低

及出现时间极短的运行状态。

## 5.3 针对预计运行事件及设计基准事故的最佳估算加不确定性量化的确定论安全分析

5.3.1 采用最佳估算计算机程序并结合模型、初始条件、边界条件及其他输入参数的不确定性，可以获得确定论安全分析中的不确定性（尤其是预计运行事件与设计基准事故的不确定性）。为了能够获得安全分析的保守结果，应识别和评价这些不确定性对结果的影响，以确认计算得到的上限值和下限值能够包络核动力厂参数的真实值，并具有合适的置信度水平。

5.3.2 在对不确定性进行量化之前，需要确保：分析采用的最佳估算计算机程序经过充分确认；用户效应（比如可能选择不恰当的值）经过合适考虑；计算平台（硬件和软件）对于结果的影响最小化；评价不确定性的方法经过鉴定。

5.3.3 为了进行稳健的“最佳估算加不确定性量化”分析，有必要对不确定性进行可靠的评价，尤其是识别并区分随机不确定性和认知不确定性的来源。在进行不确定性分析时，应区别对待不同来源的不确定性。最好采用计算机程序与真实数据对比的方式来量化已知的不确定性。当然，敏感性研究、计算机程序之间的对比以及专家判断等方式相结合也可以用于不确定性评价。搜集与所分析事件相关的核动力厂初始及边界条件数据是评价随机不确定性的首选方法。

5.3.4 不确定性的量化应基于核动力厂状态不确定性与程序模型不确定性的统计组合，以确保在指定的概率下，有足够多的

计算结果满足验收准则。对于核动力厂预计运行事件及设计基准事故，应特别要求在95%置信度水平或更高水平下，至少95%的结果满足验收准则。

5.3.5 在考虑不确定性评估方法时，应选择采用输入的不确定性传递方法或者输出的不确定性外推方法来评估不确定性。在前一种方法中，输出参数总的不确定性是通过改变不确定性输入参数的值来开展足够数量的计算进行评价；在后一种方法中，输出参数总的不确定性应基于输出值（计算值）与试验数据的对比进行评价。

5.3.6 对于“输入不确定性传递”的方法，不确定性输入参数应至少包含最为重要的参数。需要确定输入参数的范围和在该范围内的概率分布（概率分布应基于相关试验数据、测量参数、核动力厂运行参数记录或者其他合适的数据源确定）。如果该方法不可行，则应采用参数范围内保守的值。所选输入参数要么是独立的，要么输入参数之间的关联性被识别和量化。后者应对分析结果进行特定的处理。

5.3.7 不确定性输入参数的选取、范围以及概率分布对于结果的可靠性是极为重要的。这是由于对工程应用具有重要意义的结果不确定带的宽度受到它们的极大影响。

5.3.8 对于“输入不确定性传递”的不确定性评价方法，允许对输入参数组和相应的输出值采用回归或关系式拟合技术，也允许根据对输出不确定性的贡献对不确定性输入参数进行排序。此类排序指出哪些参数需要被重点关注。然而，需要注意的是，回

归或拟合技术也可能给出不清晰或者误导性的结果，尤其当响应并非线性或者相关效应非常重要的时候。

5.3.9 对于每个分析的事件，与计算机程序结果有关的参数不确定性也可以基于专家判断来估算，该过程需要使用现象识别和分级表（PIRT）。每个 PIRT 表都应识别最重要的现象，而模拟这些现象的计算机程序模型适用性需要根据可用的数据进行确认。重要的参数需要基于它们各自的概率分布进行随机的变化，以估算总的不确定性。该流程也可以用于评估计算机程序或者模拟某选定事件的计算工具的适用性。

# 6 核动力厂不同状态的确定论分析方法

## 6.1 总则

6.1.1 应对核动力厂不同状态下的假设始发事件与事故序列进行确定论安全分析，并应在验收准则选择、计算机程序使用、不确定性的处理和保证安全裕量方面遵循本导则所述的通用规则。

6.1.2 在确定论安全分析中，只能采信那些满足与电厂状态相关的要求并进行了适当的安全分级的构筑物、系统和设备，以及完成了设计扩展工况下可用性论证的构筑物、系统和设备。

6.1.3 确定论安全分析时，作出保守水平的决定时，应考虑以下输入数据或假设：

（1） 计算机程序的模型；

（2） 核动力厂运行参数；

（3） 控制及限制系统；

（4） 能动安全系统；

（5） 非能动安全系统；

（6） 设计扩展工况的安全设施；

（7） 操纵员动作。

6.1.4 不同类型的失效下，影响源项的现象可能不同，因此需要针对每种失效类型进行各自的源项分析。典型的事故类型包括：导致冷却剂与裂变产物由堆芯释放到安全壳的丧失冷却剂事故；旁通安全壳或者发生在安全壳外（如乏燃料水池）的事故；维修带有放射性燃料时发生的事故；处理及贮存气相或液相放射性废物系统的事故释放。

6.1.5 对于某些假想事故，放射性核素的释放是由堆芯进入反应堆冷却剂系统，再逐步进入安全壳内，直至放射性核素最终释放至环境。因此，源项分析应包含预测经过该路径的放射性核素的行为。

## 6.2 正常运行条件下的确定论安全分析

6.2.1 分析的特定目标

6.2.1.1 正常运行条件下的确定论安全分析应采用迭代过程，以支持运行限值和条件的开发，并确认其适当性。这些运行限制条件以过程变量数值、系统要求、监督要求或试验要求等表示。

6.2.1.2 正常运行条件下的确定论安全分析所用的限值与条件（如反应堆功率及冷却剂装量），应包含所有重要的初始和边界条件，并将在预计运行事件、设计基准事故及设计扩展工况的

分析中被使用。

6.2.1.3 应分析运行限值和条件范围内的所有正常运行模式及相应核动力厂配置，需特别关注相关瞬态（如堆芯功率变化、功率运行状态下的停堆、启堆、反应堆冷却、半管运行等），以及新燃料和已辐照燃料的操作（包括已辐照燃料卸料至乏燃料水池及堆芯装料等）。

6.2.1.4 正常运行条件下的确定论安全分析应包括核动力厂辐射状态的分析及对放射性物质向环境扩散的估算。这是确定核动力厂员工以及核动力厂周边公众与动植物受辐射剂量所需的输入参数。本导则中不包含与此相关的指导。

6.2.2 验收准则

6.2.2.1 确定论安全分析应提供核动力厂在其参数不超过运行限值和条件的情况下能否正常运行的评价。正常运行的设计评价必须验证在所有运行模式的瞬态下，不会触发反应堆紧急停堆及安全系统动作。还应考虑运行规程内可预计的运行状态之间的转换。

6.2.2.2 正常运行条件下的安全分析应包含核动力厂总体设计与运行的分析：

（1）预测员工及公众可能受到的辐射剂量；

（2）评价这些剂量低于限值；

（3）确保这些剂量满足可合理达到的尽量低原则。

与放射性验收准则保持一致并不在本导则涵盖的范围之内。

6.2.3 系统可用性

正常运行条件下的确定论安全分析中采信的系统应局限于

正常运行系统，包括核动力厂控制系统。在正常运行模式有关的瞬态中，不应触发核动力厂的其他系统。

6.2.4 操纵员动作

正常运行规程中设定的操纵员动作在分析中应采信。

6.2.5 分析假设与不确定性处理

6.2.5.1 正常运行条件下的分析应提供核动力厂现实的行为表征。尽管如此，应考虑系统（包括仪表、控制与机械系统）性能的不确定性，以评价可用设备的适当性。

6.2.5.2 考虑的初始条件应可以代表所有预期及批准的核动力厂运行模式，并与运行限值和条件保持一致。使用的参数包络值应考虑参数全部可接受的范围。

6.2.5.3 当预测剂量存在不确定性时，应进行保守假设。本导则不包括此方面的详细指导。

## 6.3 针对预计运行事件的现实性确定论安全分析

6.3.1 分析的特定目标

6.3.1.1 对预计运行事件现实分析的主要目的是验证核动力厂的运行系统（特别是控制及限制系统）可以防止预计运行事件发展到事故状态，且核动力厂能够在预计运行事件发生后恢复到正常运行状态。现实分析应给出核动力厂对始发事件现实的响应。

6.3.1.2 分析考虑的假设始发事件中的预计运行事件，应包括所有在核动力厂寿期内预计会发生的事件。对于很多假设始发事件，利用控制及限制系统结合核动力厂固有特性和操纵员动作，

能够消除事件影响，从而不会出现反应堆紧急停堆或者安全系统投入。在这些情况下，核动力厂可以在纠正错误后恢复运行。

6.3.1.3 通常，预计运行事件不应对缓解设计基准事故的安全设施产生任何不必要的挑战。因此，分析应证明，在核动力厂控制及限制系统能够依照设计运行的情况下，不需要触发安全系统。然而，某些预计运行事件本身就需要触发安全系统。

6.3.2 验收准则

6.3.2.1 对预计运行事件的现实分析应旨在论证实体屏障（燃料芯块、燃料包壳、反应堆冷却剂系统压力边界和安全壳）或者重要的安全系统不会出现损坏。另外，还应尽可能地验证，不会出现反应堆紧急停堆及安全系统触发。

6.3.2.2 现实分析也可用来论证在控制及限制系统可用的情况下，设计能满足特定的设计准则（比如安全阀不开启）。该设计准则比针对预计运行事件保守分析的验收准则更严格。

6.3.2.3 为了保证实体屏障不失效，通常需要在 95%置信度水平的 95%概率下确保（轻水堆）：堆芯任何区域不发生沸腾危机或干涸，堆芯任何区域的燃料芯块中心部分不熔化，反应堆冷却剂系统与主蒸汽系统的压力不会明显超过设计值。

6.3.2.4 任何预计运行事件都不应导致核动力厂紧邻区域以外的放射性影响。预计运行事件相关的放射性释放验收准则应与正常运行下的年放射性限制准则相当，而应比设计基准事故的放射性剂量限制更严格。可接受的有效剂量限值应与正常运行的有效剂量限值相当。

6.3.3 系统可用性

在预计运行事件现实分析中，任何不受假设始发事件影响的系统都应被假设为可用。分析应主要依靠控制及限制系统，以及核动力厂固有特性。

6.3.4 操纵员动作

分析中应考虑正常与异常运行下操作规程所设定的操纵员动作。通常，当假设控制及限制系统正常运行时，在相应瞬态中便不再需要操纵员动作，否则应使用现实估算的操纵员动作时间。

6.3.5 分析假设与不确定性处理

针对预计运行事件的现实分析应采用最佳估算方法，并涵盖确定假设始发事件时考虑的核动力厂预期初始条件。通常，针对预计运行事件的现实分析不考虑不确定性。对于可运行性考虑（比如核动力厂可靠性分析），可对控制及限制系统应用不确定性处理。

## 6.4 针对预计运行事件和设计基准事故的保守性确定论安全分析

6.4.1 分析的特定目标

6.4.1.1 必须用保守的方法来分析设计基准事故，即应采用表1选项1至选项3中的一种。现实分析不应被运用至设计基准事故分析中。针对预计运行事件和设计基准事故的保守分析应能够证明短期内仅依靠安全系统的自动动作，长期叠加操纵员动作，可以使核动力厂达到安全状态，并满足以下安全条件：

（1）在预计运行事件或者设计基准事故后反应堆停堆并达到次临界状态；

（2）在预计运行事件或者设计基准事故后能够从堆芯导出停堆后产生的衰变热；

（3）在预计运行事件或者设计基准事故中减少放射性物质释放的可能性并确保释放量在可接受限值以下。

6.4.1.2 安全分析应论证可以满足与事件相关的验收准则。特别是，需要论证防止放射性物质释放的部分或全部屏障在一定程度内保持完整性。

6.4.1.3 安全分析用于建立安全系统的运行特性及整定值，并建立运行规程，以保证维持基本安全功能。安全分析也为反应性控制系统、反应堆冷却剂系统与专设安全设施（如应急堆芯冷却系统与安全壳热量导出系统）的设计提供基础。

6.4.2 验收准则

6.4.2.1 针对预计运行事件的保守分析，技术验收准则（与燃料完整性相关）和放射性验收准则原则上应与现实分析所采用的验收准则相同。

6.4.2.2 设计基准事故的结果应满足规定的验收准则，没有或仅有少量向核动力厂紧邻区域以外的放射性影响。

6.4.2.3 应定义特定的技术验收准则，使得只要满足上述验收准则就能够在任何情况下保证核动力厂三项基本安全功能（即反应性控制、余热排出、放射性物质包容），以及在预计运行事件或设计基准事故下，部分或者全部屏障能够限制放射性物质向环境释放。

6.4.2.4 技术验收准则通常应包含以下几点：

（1）在不发生进一步的独立失效（除了为满足单一故障准则而提出的任何单一失效假设）情况下，单个事件不应导致更为严重的核动力厂状态。因此，预计运行事件不应发展为设计基准事故，而设计基准事故不应发展为设计扩展工况。

（2）用于缓解事故后果的安全系统不应丧失全部功能，尽管某个安全系统可能因为假设始发事件而受到部分影响。

（3）用于事故缓解的系统应能够承受该事故所带来的最大载荷、应力及环境条件。这应通过逐个分析加以论证，分析需涵盖环境条件、老化效应（如温度、湿度、放射性及化学环境）以及核动力厂结构与部件所承受的热工与机械载荷。设计中考虑所受载荷考虑的裕量应与载荷的概率相称。

（4）反应堆冷却剂系统及主蒸汽系统的压力不应超过对应核动力厂状态相应的设计限值，应与超压保护规定保持一致。可能需要额外的超压分析来研究核动力厂状态对安全阀及卸压阀的影响。

（5）针对每类假设始发事件都应限制燃料包壳失效数量，以满足总的放射性准则，并限制放射性水平低于设备鉴定采用的值。

（6）在涉及燃料裸露及升温的设计基准事故中，应保持燃料组件（轻水反应堆）的可冷却几何形状及结构完整性。

（7）任何事故都不能造成安全壳的温度、压力及安全壳隔间压差超过安全壳设计基准使用的限值。

（8）停堆后的反应堆中、新燃料贮存区域和乏燃料水池中的核燃料应维持次临界状态。只要满足燃料持续充分冷却的准则，在特定事件及核动力厂运行模式下，可以接受暂时的重返临界（如压水堆蒸汽管线破裂）。

（9）在核动力厂设计寿期内，对于任何设计基准事故，压力容器都不能出现由假想的缺陷发展为脆性断裂或延展性失效的情况。

（10）堆内构件应能够承受设计基准事故下的动态载荷，以保证反应堆安全停堆、次临界以及堆芯充分冷却。

6.4.2.5 对于假定的不能保持屏障完整性或完整性降级的情况下（如反应堆打开、安全壳打开或者乏燃料水池发生事故），应采用更严格的验收准则（如避免冷却剂沸腾或燃料裸露）。

6.4.3 系统可用性

6.4.3.1 在分析中，与核动力厂系统可用性相关的保守假设一般包括：

（1）如果没有受到假设始发事件本身或始发事件结果的影响，则在假设始发事件发生时，正常运行系统继续运行。

（2）只有在使得始发事件的影响更为恶劣的情况下，才考虑控制或限制系统运行。在缓解始发事件影响时，不能考虑控制系统的投入运行。

（3）依照安全级设计与维护（符合质量保证与定期试验规定，使用已接受的设计程序与设备鉴定）的安全系统以保守能力运行。

（4）根据单一故障准则，在始发失效及任何继发失效之外，还应对缓解始发事件所需运行的安全系统假设单一部件故障。根据所选的验收准则，应假设可导致对安全系统造成最大挑战的系统或部件单一故障。

（5）分析中，不能考虑专门为设计扩展工况设计的安全设施。

6.4.3.2 除非是运行限值或条件允许的维修，则应考虑相关的一列安全系统不可用。

6.4.4 操纵员动作

6.4.4.1 针对保守安全分析，直到在保守的规定时间后，才能考虑操纵员开始必要的操作。针对特定的反应堆设计，分析中假设的时间应予以论证和确认，比如最短的主控室操作时间可能是30 分钟，就地操作时间可能是 60 分钟。

6.4.4.2 只有在事件序列及核动力厂特定边界条件允许采取假设操作时，在分析中才能考虑核动力厂工作人员为了预防事故或缓解事故后果而进行的正确操作。考虑到的条件包括事件序列发生的整体背景、控制室的工作环境、撰写的规程、相关员工培训情况及必要信息的获取能力等内容。

6.4.4.3 可考虑在执行恢复操作过程中一项操纵员失误(未执行规定动作)作为单一故障。

6.4.5 分析假设与不确定性处理

6.4.5.1 针对预计运行事件及设计基准事故分析使用的保守假设应考虑不确定性，包括初始条件及边界条件，核动力厂系统

及操纵员操作可用性。目的是以高置信度证明分析结果与安全限值之间具有足够的裕量。

6.4.5.2 预计运行事件的保守分析应与设计基准事故确定论安全分析使用相同的保守假设，特别是与那些在假设始发事件下维持安全功能的系统有关的假设。

6.4.5.3 如果采用保守或者组合方法，则应保守假设安全系统运行在最低或者最高性能水平，这具体取决于给定的验收准则。对于反应堆停堆与安全系统触发系统，应假设开始动作发生在可能条件范围内最不利的情况。如果采用最佳估算加不确定性分析方法，安全系统性能的不确定性应包含在总体的不确定性分析中。

6.4.5.4 除了假定的始发事件自身，还应考虑将丧失场外电作为额外的保守假设。此时丧失场外电应为始发事件一个潜在的事故后果，其发生时刻可根据实际情况合理考虑，并且事故验收准则不变。

6.4.5.5 与确定论安全分析的一般规定保持一致，针对预计运行事件及设计基准事故的源项评价应考虑事故过程中发生的全部重要物理过程，并采用核动力厂特定基准下的初始数据及系数的保守值。

## 6.5 没有造成堆芯明显损伤的设计扩展工况的确定论安全分析

### 6.5.1 分析的特定目标

针对没有造成堆芯明显损伤的设计扩展工况的安全分析，目的是证明在合适的置信度下燃料不会熔化且保持合适的裕量，以

避免任何陡边效应。

6.5.2 接受准则

对于设计扩展工况，保护公众所采取的防护行动在持续时间和范围上必须是有限的，并必须有足够的时间来采取这些防护行动。没有造成堆芯明显损伤的设计扩展工况可以采用与设计基准事故相同或近似的技术及放射性后果准则。放射性释放应被减少到可合理达到的尽量低水平。

6.5.3 系统可用性

6.5.3.1 通常，分析中只考虑在设计扩展工况中仍能运行的系统。

6.5.3.2 在没有造成堆芯明显损伤的设计扩展工况分析中，可采信不受到假设失效影响的安全系统。当评价与假设失效（如内部水淹）相关的安全系统独立性时，应特别注意其他可能导致安全系统（如地坑滤网堵塞）与支持系统（电力、通风及冷却系统）受到影响的因素。

6.5.3.3 对没有造成堆芯明显损伤的设计扩展工况，无须应用单一故障准则，无须考虑由于维修造成安全设施不可用的情况。

6.5.3.4 为保证纵深防御不同层级之间的独立性，考虑到以下原因，没有造成堆芯明显损伤的设计扩展工况分析中通常不应考虑包括控制及限制系统在内的正常运行系统，但是应考虑正常运行系统可能给事件带来的不利影响。

（1）一个给定事件序列可能涵盖了多种假设始发事件，考虑到假设始发事件的起因及多重失效，可能很难论证运行系统总是可用的；

（2）事故序列通常造成运行环境的恶化，分析中所有采信的系统都应针对此环境条件进行充分的可用性论证。

6.5.3.5 在论证核动力厂设计的适当性时，通常不考虑移动设备。这些设备通常用于事件发生后的长期阶段，并且依据应急运行规程或者事故管理指南假设可用。应证明移动设备投入时间的合理性。

6.5.4 操纵员动作

设计扩展工况分析中，操纵员动作可采用最佳估算假设。然而，在一定程度上也可以采用设计基准事故中的一些保守假设。

6.5.5 分析假设与不确定性处理

6.5.5.1 针对没有造成堆芯明显损伤的设计扩展工况，原则上可以使用适用于设计基准事故计算机程序的选择、确认及使用的要求。

6.5.5.2 针对没有造成堆芯明显损伤的设计扩展工况，原则上可以使用适用于设计基准事故的组合方法或者加不确定性量化的最佳估算方法（最佳估算加不确定性）。但是，在满足 6.5.5.3 和 6.6.5.2 的情况下，也可以使用没有不确定性量化的最佳估算分析，这与设计扩展工况分析的通用准则是一致的。

6.5.5.3 当进行最佳估算分析时，必须证明用于避免陡边效应的裕量是合适的。例如可由敏感性分析来论证，即在可操作范围内，即使针对重要参数进行更为保守的假设，距离丧失实体屏障

完整性依然有合适的裕量。

## 6.6 堆芯熔化的设计扩展工况的确定论安全分析

6.6.1 分析的特定目标

6.6.1.1 严重事故的分析应识别由假想堆芯熔化事故所产生的核动力厂包络参数，并且论证如下几点：

（1）核动力厂可进入能够长期维持必要的安全壳功能的状态；

（2）核动力厂构筑物、系统和设备（如安全壳）及规程能够防止包含安全壳旁通在内的早期放射性释放或大量放射性释放；

（3）控制区域（例如主控室、备用控制室及其他应急响应设施与区域）应保持人员可居留性以便工作人员进行操作；

（4）计划的严重事故管理措施有效。

6.6.1.2 严重事故安全分析应论证设计采用的设施与执行事故管理规程或事故管理指南相结合能够满足接受准则。

6.6.2 接受准则

6.6.2.1 严重事故分析中使用的针对公众剂量（或环境释放剂量）的放射性接受准则，应只需进行有限时间及有限区域的场外保护措施，并且尽早采取这些措施以保证有充足的时间使其发挥作用。

6.6.2.2 技术接受准则应体现维持安全壳完整性的条件。设计扩展工况分析的接受准则可包括安全壳压力、水位、温度、可燃气体浓度等限值及堆芯熔融物稳定性。

6.6.2.3 厂内放射性接受准则应保证控制区域及用于在区域之间转移场所内的人员可居留性。核动力厂控制区域的辐射水平（如空气中剂量率与空气中的放射性物质浓度）应能够保证这些区域内人员（例如应急工作人员）有适当的保护。

6.6.3 系统可用性

6.6.3.1 只有以合理的置信度表明满足以下条件，严重事故分析中才可考虑安全系统：

（1）该系统的失效不属于严重事故序列要包含的任何场景；

（2）该设备在需要执行其预定功能的时间段内能够在现实的严重事故条件下可用。

6.6.3.2 对于假设在严重事故下运行的设备，其可用性应考虑：

（1）适用的始发事件状况，包括外部危险（例如全厂断电及地震）造成的状况；

（2）需要该设备运行的环境（例如压力、温度及辐射剂量）与时间段。

6.6.3.3 对于堆芯熔化的设计扩展工况，不需要应用单一故障准则。此外，确定论安全分析中不需要考虑由于维修造成的系统或者部件的不可用。应为设计扩展工况下必需的系统或者部件的试验及维修制定合适的规定，以保证其可用性。

6.6.3.4 在论证核动力厂设计的适当性时，不应考虑移动设备。针对某些设计扩展工况，这些设备通常用于事件的长期阶段，并且依据应急运行规程或者事故管理指南假设可用。应证明移动

设备可用时间的合理性。

6.6.4 操纵员动作

堆芯熔化的设计扩展工况与没有造成堆芯明显损伤的设计扩展工况采用同样的操纵员动作假设。

6.6.5 分析假设与不确定性处理

6.6.5.1 严重事故分析应模拟（堆芯未熔化时发生的中子物理及热工水力现象除外）堆芯损伤后可能发生的及可能导致放射性物质向环境释放的大范围物理过程。如果适用，应包括以下现象：

（1）堆芯损伤过程及燃料熔化；

（2）燃料-冷却剂相互作用（包括蒸汽爆炸）；

（3）熔融物堆内滞留；

（4）压力容器熔穿；

（5）安全壳直接加热；

（6）一回路内热源分布；

（7）氢气的产生、控制与燃烧；

（8）安全壳的失效或旁通；

（9）熔融物与混凝土相互作用；

（10）裂变产物的释放与迁移，包括为防止超压而进行的安全壳卸压排放；

（11）对压力容器内和压力容器外的堆芯熔融物进行冷却的能力。

6.6.5.2 严重事故分析应使用在可行范围内的现实方法（表 1 的第 4 选项）。由于现象的复杂性与试验数据的不充分性，可能

无法实现对不确定性的定量分析，因此需要进行敏感性分析以论证严重事故分析结果与结论的稳健性。

## 6.7 支持“实际消除”的确定论安全分析

6.7.1 设计必须做到实际消除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发生的可能性。监管机构可建立更为详细的规定来描述论证“实际消除”的可接受的方法。

6.7.2 论证可能导致早期放射性释放或大量放射性释放的工况可实际消除，包括确定论安全分析，工程评价（如：构筑物、系统和设备的设计、建造、试验和检查）及运行经验评估，并由概率论安全分析进行补充，以考虑某些物理现象认知局限性引起的不确定性。

6.7.3 论证可能导致早期放射性释放或大量放射性释放的工况可实际消除，应包括以下步骤（如果适用）：

（1）识别潜在的威胁安全壳完整性或者导致安全壳旁通的工况，这些工况可能导致早期放射性释放或者大量放射性释放；

（2）实施用于实际消除这些工况的设计及运行措施。这些措施的设计应考虑足够裕量以应对不确定性；

（3）通过确定论安全分析辅以概率安全评价和工程判断来最终确认措施的适当性。

6.7.4 尽管可以设定概率目标，但对实际消除可能导致早期放射性释放或大量放射性释放工况的论证，不应仅基于较低的概率值。应由确定论定义事件序列，并基于安全设施性能使之极不可能发生来论证将其实际消除。

6.7.5 如果宣称某些工况在物理上不可能导致早期放射性释放或者大量放射性释放，则有必要审查系统固有安全特性并且通过自然法则论证其不会发生，并且可以实现基本安全功能——控制反应性、排出余热、包容放射性物质，包括限制事故的放射性释放。实际上该方法仅限于非常特殊的工况。可能用到的一个例子是不可控的反应性事故，对此主要的保护是在堆芯功率、冷却剂压力与温度的所有可能组合下维持负反应性系数。

# 7 确定论安全分析的归档、审查和更新

## 7.1 概述

7.1.1 确定论安全分析的结果和结论一般以安全分析报告的形式记录下来。安全分析报告的内容应恰当地反映设施或活动的复杂性及其辐射风险。

7.1.2 尽管安全分析报告本身应足以支持独立验证和监管审查，但通常还有可能包括确定论安全分析描述和结果的其他文件用于支持独立验证和监管审查。对安全分析报告的要求适用于提交给监管机构的所有确定论安全分析文件。

7.1.3 安全分析报告应给出在确定论安全分析中考虑的所有核动力厂状态清单，并根据它们的频率和对防止放射性物质释放的实体屏障完整性产生的挑战进行合理分组。应在每组中选择包络的序列。对于可能导致早期放射性释放或大量放射性释放的工况，应论证实际消除其发生的可能性。

7.1.4 应以安全分析报告独立章节或者通过独立的文件提供

一系列重要的核动力厂数据。这些数据用于核动力厂模型（即确定论安全分析数据库）开发，以及开展确定论安全分析独立验证或评估。这些数据应包括几何信息、热工水力参数、材料物性、控制系统特征和整定值、核动力厂设备仪表装置的不确定性范围，以及相关图纸和图形文件。如果安全分析报告本身并未充分记录和证明这些数据，则应明确地标注并引用其他用于准备核动力厂模型的可信数据源。

7.1.5 应提供在确定论安全分析中所使用的计算机程序的简要描述。除了引用特定的计算机程序文档之外，描述应包括计算机程序对指定用途适用性的说明，以及用户验证和确认的说明。

7.1.6 根据每个分析序列模拟的现象和其他特征，应为每个序列选择一条或一系列相应的准则，但应说明这种选择的依据或合理性。针对选取的验收准则，给出相应的安全分析结果。

7.1.7 应描述用于论证符合每条特定验收准则分析所使用的模型、模型经验证的范围、主要假设。应描述对于每种核动力厂状态可能使用的不同方法。

7.1.8 如果确定论安全分析依次使用了不同的计算机程序，则应清晰地描述事故分析不同阶段和/或使用的不同计算机程序之间的数据传递，以便于追溯并作为独立验证、理解和接受分析结果的必要条件。

7.1.9 事故序列分析的时间跨度应延伸到核动力厂达到稳定的安全状态的时刻。安全分析报告中应提供稳定的安全状态的定义。通常认为，核动力厂在发生预计运行事件或事故工况后，反应堆处于次临界，并能够保证基本安全功能且长期保持稳定的状

态，则已达到稳定的安全状态。

7.1.10 确定论安全分析的结果文件应以合适的格式提供，以便对事故的过程提供清晰地描述和解释。类似的分析可以采用标准化的格式，以便于结果的阐述和相互对比。

7.1.11 一般地，确定论安全分析的结果文件应包含以下信息：

（1）按照时间顺序描述计算的主要事件；

（2）基于选取的参数，描述和评价事故；

（3）图形展示主要参数的计算结果；

（4）对于所达到安全水平可接受性的结论，以及与所有相关验收准则的符合性的说明，包括是否有足够的裕量；

（5）视情况提供敏感性分析结果。

7.1.12 确定论安全分析应遵守相关的质量保证规范和质量控制要求。

## 7.2 文件中的敏感信息

如果未经授权的信息披露可能威胁到核安保，那么应识别和适当保护确定论安全分析报告中的敏感信息。这些信息可能包括但不限于假设始发事件的识别和分类，以及确定论安全分析的结果。这些信息应按照有关规定进行保护。

## 7.3 确定论安全分析的审查和更新

7.3.1 在执照申请过程中使用的确定论安全分析应定期更新，以考虑在核动力厂配置、系统和部件的特性、运行参数、规

程、研究发现、对知识和物理现象认识的进步以及计算机程序等方面的变化，这些变化可能对计算结果产生重要影响。

7.3.2 除了定期更新以外，还应在发现任何可能导致危害的信息后对安全分析进行更新。与之前假设相比，这些危害可能在性质上不同、概率更大或者幅度更大。

7.3.3 在上述情况下，应重新进行安全分析评价，以确保安全分析仍然有效并满足分析目标。结果的评价应参照确定论安全分析相关的最新要求、适用的试验数据、专家判断，并与类似分析进行对比。

7.3.4 如果需要，应将新的确定论安全分析以及重新评价的结果反映在更新的安全分析报告中，文件深度应与变化的程度和相关影响相符。

# 名词解释

本安全导则中下述名词术语的含义为：

## 确定论安全分析

确定论安全分析方法是以纵深防御概念为基础，以保障反应性控制、余热排出和放射性包容三项基本安全功能为目标，针对确定的工况，采用相应的假设和分析方法，并满足特定验收准则的一套方法。

## 随机不确定性

现象的内在不确定性，它与随机发生的事件或者现象相关。

## 认知不确定性

由于对现象认识不充分所导致的不确定性，它会导致无法精确模拟该现象。

## 源项

从设施释放（或假定释放）的放射性物质的数量和组份。用于模拟放射性核素向环境的释放或者处置库中放射性废物的释放。