ICS

团　　体　　标　　准

T/CNEA XXX-202X

核电厂概率安全分析同行评估规范及程序

第 1 部分：内部事件一级

Probabilistic Safety Assessment

Peer Review Specification and Procedure

For Nuclear Power Plant

Part 1: Level 1 for Internal Events

（征求意见稿）

XXXX-XX-XX 发布
XXXX-XX-XX 实施

中国核能行业协会 发布

中国核能行业协会（China Nuclear Energy Association，CNEA）是经国务院同意、民政部批准设立的全国性非营利社会团体，成立于 2007 年 4 月 18 日。协会的中心任务是做好政府与会员单位之间、会员单位之间、国内与国际之间的沟通与交流，维护全行业和会员的合法权益，向政府建言献策，为企业排忧解难，努力发挥桥梁和纽带作用。制定中国核能行业协会团体标准（以下简称：核协团标），以满足我国核能行业标准化发展市场需求为导向，为核能行业和相关社会事业提供行业领先的标准化服务，是中国核能行业协会的工作内容之一。中国境内的团体和个人，均可提出制、修订核协团标的建议并参与有关工作。

核协团标按《中国标准化协会标准管理办法》进行制定和管理。

核协团标草案经向社会公开征求意见，并得到参加审定会议的 3/4 以上的专家、成员的投票赞同，方可作为核协团标予以发布。

在本文件实施过程中，如发现需要修改或补充之处，请将意见和有关资料寄给中国核能行业协会，以便修订时参考。

中国核能行业协会地址：北京市海淀区西三环北路 72 号世纪经贸大厦 B 座 28 层。

固话：010-88305833　　传真：010-88305800

网址：http://www.china-nea.cn　　电子信箱：cnea_standard@vip.163.com

目　　次

前　言

《核电厂概率安全分析同行评估规范及程序》标准分为以下若干个部分：

——第1部分：内部事件一级

——第2部分：内部火灾一级；

——第3部分：内部水淹一级；

——第4部分：地震一级；

——第5部分：其他外部事件一级；

——第6部分：二级。

本文件为第1部分。

本文件依据GB/T1.1-2009的规则编写。

本文件起草单位：中国核能行业协会、苏州热工研究院有限公司、生态环境部核与辐射安全中心、上海核工程研究设计院有限公司、中国核电工程有限公司。

本文件起草人：赵成昆、郭建兵、依岩、张琴芳、赵博、奚树人、杨波、李春、黄志超、裴亮、陈捷飞、仇永萍、孙金龙、詹文辉、冯一斐。

考虑到本文件中的某些条款可能涉及专利，中国核能行业协会不负责对任何该类专利的鉴别。

本文件为首次发布。

引　言

随着我国核电技术的不断发展，概率安全分析（PSA） 越来越受到业界及核安全监管部门的认可与重视，应用也越来越广泛。而PSA的质量是PSA应用的关键因素之一。在国际上，保证PSA质量的一个通行做法是进行同行评估，我国核安全监管部门也逐渐对进行同行评估提出了相关要求。因此，在我国开展PSA同行评估将越来越迫切。为规范同行评估的过程，有必要制定相应的标准，以指导国内核能行业PSA同行评估的开展。

在国际上，美国核能研究所（Nuclear Energy Institute, NEI）于2000年出版了《概率风险评价同行评估程序导则》（Probabilistic Risk Assessment (PRA) Peer Review Process Guidance, NEI00-02），以指导业界进行PSA同行评估。国内已开展PSA模型开发工作三十余年，并逐级应用于核电厂的安全管理，积累了丰富的工程实践经验，对PSA领域的技术内涵具有深刻的理解，并相继出版了PSA质量要求的一系列行业标准。这些成果和经验为本标准的制定奠定了坚实的基础。

本标准与PSA质量要求的行业标准是相辅相成的。行业标准主要是阐述一个应用于核电厂设计、执照申请、运行或维修等活动的PSA在技术上应该要达到什么要求，但不太多涉及如何达到这些要求。本标准主要阐述如何评判一个PSA在技术上是否达到了要求以及如何组织该评判过程。

核电厂概率安全分析同行评估规范及程序 第1部分：内部事件一级

1 范围

本文件规定了核能行业实施概率安全分析（PSA）同行评估的方法，包括同行评估的流程、步骤、人员资质要求、评估队管理等活动及技术评定准则。本文件主要适用于压水堆核电厂，其他类型核电厂可参照执行。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

NB/T 20037.1 应用于核电厂的一级概率安全评价 第1部分：总体要求

NB/T 20037.2 应用于核电厂的一级概率安全评价 第2部分：低功率与停堆内部事件

NB/T 20037.11 应用于核电厂的一级概率安全评价 第11部分：功率运行内部事件。

HAF·J0088 核动力厂概率安全评价报告的标准格式和内容（一级、内部事件）

3 术语和定义

下列术语和定义适用于本文件。

3.1 事故序列 accident sequence

导致不希望后果状态（如堆芯损坏）的事件序列。

3.2 事故序列分析 accident sequence analysis

确定可能导致不希望后果状态（如堆芯损坏）的始发事件、安全功能以及系统失效和成功的组合的过程。

3.3 功率运行 at power

具有以下特征的电厂运行状态：反应堆处于临界且产生功率，关键安全系统的自动触发没有闭锁，而且重要的支持系统处于正常的运行配置状态。

3.4 共因失效（共因故障） common cause failure

由于某一共同原因而使两个或更多的部件在短时间内失效（故障）。

3.5 堆芯损坏（堆芯损伤） core damage

堆芯裸露和升温到预计会造成包括堆芯相当大的一部分区域长期氧化和严重的燃料损坏。

3.6 堆芯损坏频率（堆芯损伤频率） core damage frequency

单位时间内预计的堆芯损坏事件的次数。

3.7 相关性 dependency

某一物项实现其功能所依赖的外部要求，并且与相关事件有联系，这些相关事件由其他事件或偶发事件所确定、或受它们影响或与它们有相互关系。

3.8 **事件序列** event sequence

始发事件发生后，一系列事件（如系统、功能和操纵员响应）的成功或失败，并最终成功缓解或者导致不希望后果（如堆芯损坏）的事件情景。一个事件序列有一个明确的终态。

3.9 **事件树** event tree

一种逻辑图，该逻辑图以某一始发事件或状态开始，通过一系列描述预期系统或操纵员行为的成功或失败的分支说明事故的进程，并最终达到成功或失败的终态。

3.10 **故障树** fault tree

一种演绎逻辑图，描述特定的不希望事件（顶事件）是如何由其他不希望事件的逻辑组合所引发的。

3.11 **人员失误事件** human failure event

由于人员不动作或不适当地动作而引起的一个部件、系统或功能的失效或不可用的基本事件。

3.12 **人员可靠性分析** human reliability analysis

用于识别潜在的人员失误事件，并应用数据、模型或专家判断来系统地评估这些事件的概率的一种结构化方法。

3.13 **始发事件** initiating event

干扰电厂稳态运行并可导致出现不希望的电厂状态的事件。始发事件要求电厂缓解系统及人员作出响应，一旦响应失败则可能导致不希望的后果（如堆芯损坏）。

3.14 **内部事件** internal event

一类包含源于核电厂内部的、由随机机械失效、电气失效、结构失效或人员失误引起的事件的灾害组。该事件会直接或间接地引起始发事件，且可能导致安全系统失效或操纵员失误，从而可能导致堆芯损坏。按照惯例，丧失厂外电作为内部事件，内部水淹和内部火灾按独立的灾害组考虑而非内部事件。

3.15 **低功率** low power

反应堆功率低于正常运行功率的电厂运行状态。此时，功率水平可随着反应堆停堆或启动而变化。功率运行与低功率的功率水平的区别是低于该水平时，电厂会降低或提高功率水平，从而显著增加电厂紧急停堆的可能性（例如，手动控制给水量）。

3.16 **电厂运行状态** plant operational state

一种标准的电厂组态，其运行参数相对恒定（建模时看作是恒定的），并且在影响风险的方式上与其他组态有所不同，这些参数如：堆芯功率水平，一回路水位，一回路温度，一回路开口状态，安全壳状态和衰变热排出机制等。

3.17 **概率安全评价（分析）/概率风险评价** probabilistic safety assessment （analysis）/probabilistic risk assessment

一种全面的、结构化的处理方法，识别出核电厂失效的情景，并对工作人员和公众所承受的风险作出数值估计。PSA 通常分三个级别，其中一级 PSA 识别可能造成堆芯损坏的事故序列，估计堆芯损坏频率，对电厂的安全性和合理性进行评价，找出电厂薄弱环节，提出降低堆芯损坏频率的措施。

3.18 **PSA 维护** PSA maintenance

为反映诸如修改、规程变化或电厂性能（数据）变化而对 PSA 模型所作的适时更新。

3.19 **PSA 升级** PSA upgrade

将新的方法论或者范围的重大变化反映到PSA模型中，包括新的人员失误分析方法、新的数据更新方法、新的定量化或截断方法、或对新的共因失效处理方法等。

3.20 **停堆** shutdown

反应堆达到次临界深度的过程，也指反应堆达到规定次临界深度的状态。

3.21 成功准则 success criteria

建立在规定的时间内为保证满足安全功能而要求运行的系统或部件的最小数量或组合、或者每个部件运行的最低性能水平的准则。

4 同行评估范围

本文件的范围仅适用于内部事件一级PSA，涵盖了以下10项内容：

1.电厂运行状态分析（POS）

2.始发事件分析（IE）

3.事件序列分析（ES）

4.成功准则（SC）

5.系统分析（SA）

6.人员可靠性分析（HR）

7.数据分析（DA）

8.相关性分析（DF）

9.模型整合与定量化（MQ）

10.模型维护与升级（MU）

前9项为内部事件一级PSA的9个技术要素，其划分和代码与国家能源行业技术标准《应用于核电厂的概率安全评价第11部分：功率运行内部事件一级PSA》（NB/T20037.11）和《应用于核电厂的概率安全评价第2部分：低功率和停堆工况内部事件一级PSA》（NB/T20037.2）相一致，并以其技术要求为基础制定同行评估要求。最后一项是PSA的维护与升级的管理，目的是确保PSA能够随着电厂的实际情况而持续更新。

PSA同行评估过程是一个一次性评估过程，对现有PSA以及PSA维护和升级程序进行检查。根据本文件和技术导则，评估队人员以NB/T20037.11和NB/T20037.2为基础，对不同的PSA技术要素的技术质量和充分性进行检查。本文件还包括了对维护和升级PSA相关机制的检查，以便通过该机制在运行电厂中充分使用PSA技术支持风险指引型应用。

在核电厂内，确保PSA应用成功的因素包括：

－PSA组织，

－管理层的重视，

－PSA项目组和其他部门之间的交流，

－PSA技术充分性，

－活态PSA的实施，包括PSA的维护和升级。

前3项因素属于电厂的管理问题，需要由每个运营者考虑，以保证PSA技术在应用中的成功使用。最后两项是特定PSA的事项，是本文件所涉及的同行评估的重点。

5 同行评估流程

5.1 概述

PSA同行评估的流程框架见图1，它包括以下的必要活动：

－提出同行评估申请，

－筹备同行评估，

－开展同行评估，

以及以下两项可选活动：

－评估队的现场访问，

一举办方的内部审查。

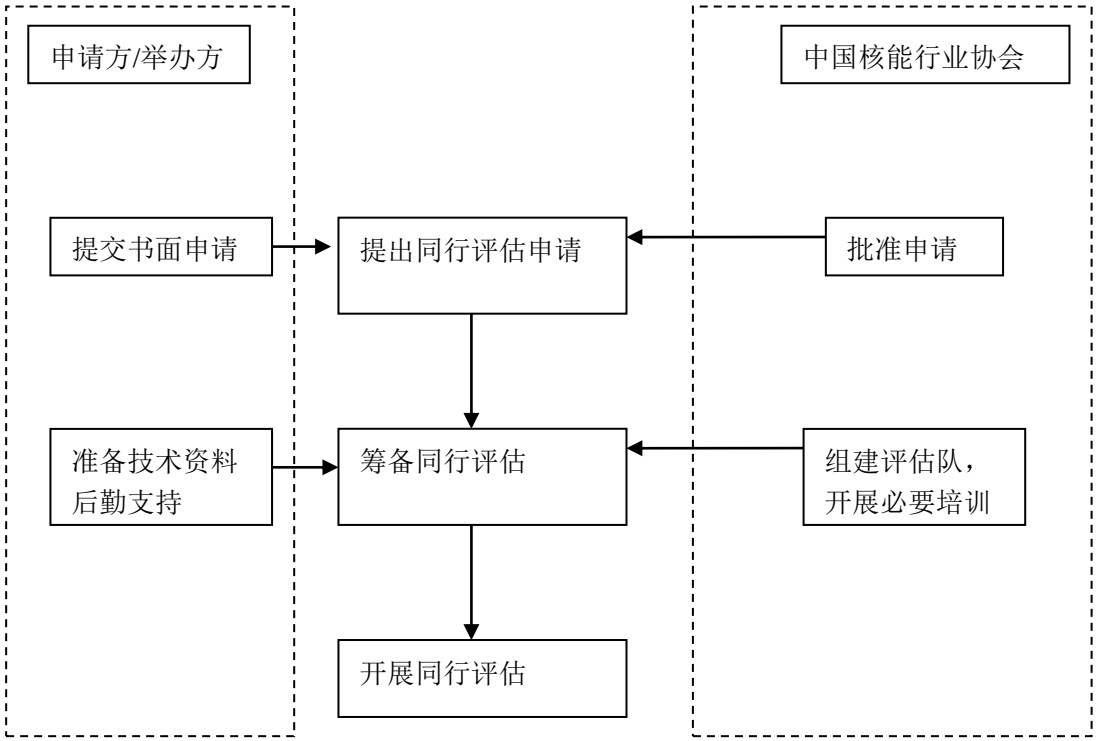

图1 PSA同行评估流程

5.2 必要活动

（1）提出同行评估申请

PSA同行评估由行业协会统一安排。申请方[1]应向核能行业协会提交正式的书面申请。提交申请的时间应在期望的同行评估开展之前至少4个月。申请书格式见表1。

（2）筹备同行评估

同行评估的筹备包括三方面工作。

首先，核能行业协会应选定同行评估专家，组成同行评估队。对同行评估专家的资质要求见本文件第7章。在组建同行评估队后，还需对首次参加评估队成员进行必要的培训，培训的内容包括熟悉本文件，了解技术标准的要求、同行评估的步骤和核能行业协会关于同行评估的一般规定等。

对于举办方，需要按本文件第8章的要求准备和提交相关的技术资料，还应为同行评估队进行评估时准备相应的办公地点和其他必要的后勤服务。

最后，同行评估队和举办方应共同确定评估计划。评估计划应由核能行业协会和举办方PSA主管共同批准。

（3）开展同行评估

同行评估的筹备工作完成后，按照评估计划开展评估工作，包括最后的评估文档的编制。具体内容和要求见本文件第9章、第10章、第11章、附录A和附录B。

[1]在本文件中，“申请方”是指向核能行业协会提出进行同行评估申请的单位，“举办方”是指承办同行评估的单位。在大多数情况下，申请方和举办方是相同的。然而，有些核电厂的 PSA 是通过开发合同，由承包商完成的。在这种情况下，申请和举办 PSA 同行评估可以由承包商进行，但也可以由核电厂提出申请，而由承包商举办。对于后一种做法，申请方和举办方是不同的。

表 1 中国核能行业协会概率安全分析同行评估申请表

<table>
<tr><td>申请单位名称</td><td colspan="5"></td></tr>
<tr><td rowspan="5">举办方联系人</td><td>姓名</td><td></td><td>手机</td><td colspan="2"></td></tr>
<tr><td>办公电话</td><td></td><td>传真</td><td colspan="2"></td></tr>
<tr><td>电子邮箱</td><td colspan="4"></td></tr>
<tr><td>通讯地址</td><td colspan="4"></td></tr>
<tr><td>邮编</td><td colspan="4"></td></tr>
<tr><td rowspan="5">PSA 项目
基本情况</td><td>完成单位</td><td colspan="4"></td></tr>
<tr><td rowspan="3">项目经理</td><td>姓名</td><td colspan="3"></td></tr>
<tr><td>电话/手机</td><td colspan="3"></td></tr>
<tr><td>电子邮箱</td><td colspan="3"></td></tr>
<tr><td>完成时间</td><td colspan="4"></td></tr>
<tr><td>同行评估时间</td><td colspan="5"></td></tr>
<tr><td>同行评估地点</td><td colspan="5"></td></tr>
<tr><td colspan="6">申请单位意见

申请单位（公章）
年 月 日</td></tr>
<tr><td colspan="6">中国核能行业协会审批意见

中国核能行业协会（公章）
年 月 日</td></tr>
</table>

备注：申请单位请将本表填写完整后发至中国核能行业协会。

5.3 可选活动

除了上述必要的活动以外，还有两项建议的活动，分别为评估队的现场访问和举办方的内部审查活动。

现场访问在正式的同行评估工作开展前4-8周左右进行，目的是评估队与举办方针对现场评估期间的准备工作进行面对面的交流和讨论。如果双方已经达成一致，则该项活动可以不必进行。

内部审查是举办方对PSA质量进行的内部检查。该活动应在开展正式的评估工作之前完成。对于该项活动，本文件不作为必要的一环节，但建议举办方开展，因为该项活动可以提高同行评估的质量和效率。需说明的是，内部审查也可以邀请举办方以外的外部专家参加，但为了保证同行评估的独立性，原则上参加内部审查的外部专家不能作为同行评估队成员。

6 同行评估过程与步骤

6.1 概述

PSA同行评估程序的流程图见图2。该图描述了在同行评估活动中对特定电厂PSA采用的一般方法和程序步骤。在整个评估过程中，同行评估队成员和举办方之间的开放和坦率的交流是很有必要的。

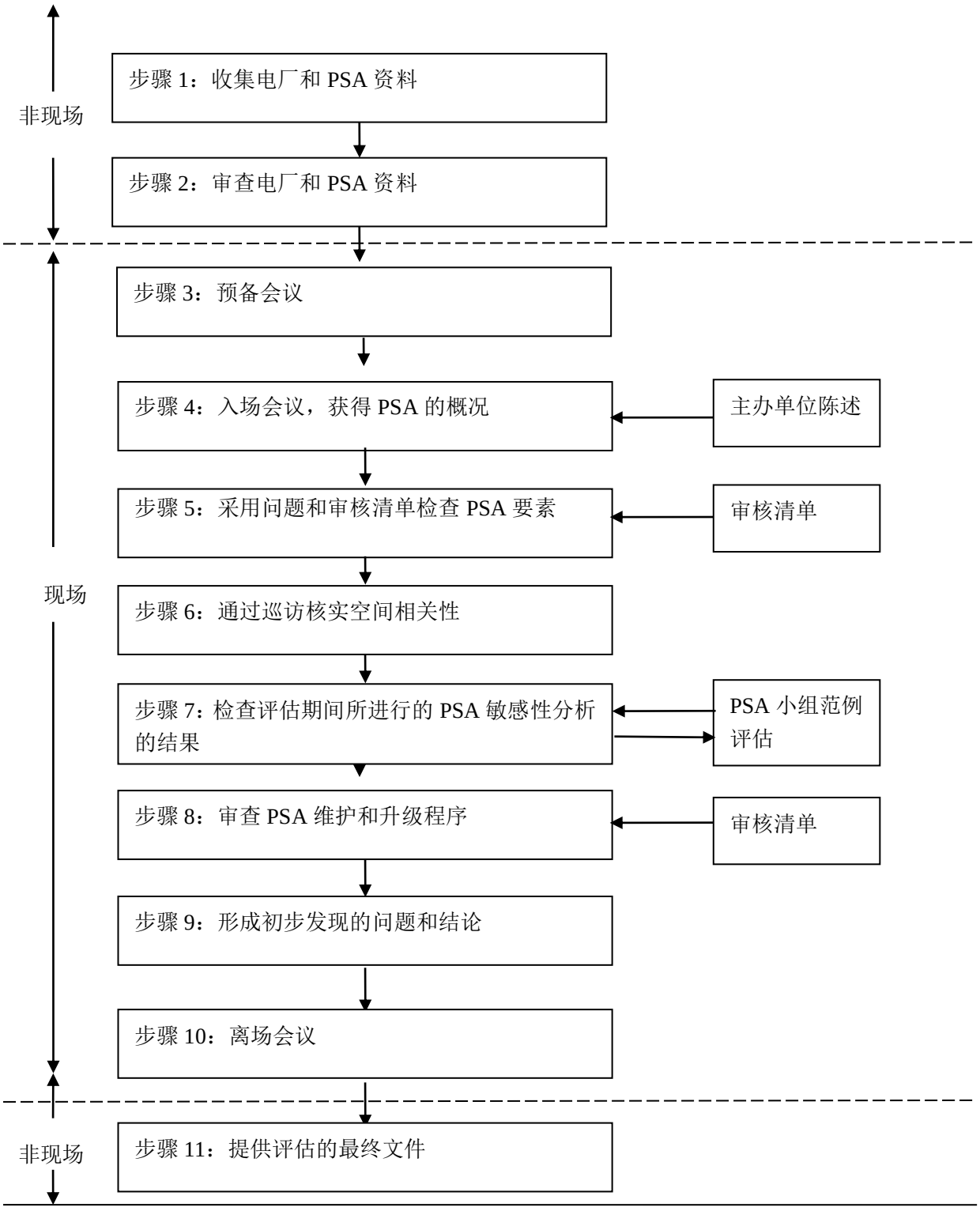

图2 PSA同行评估流程图

同行评估活动中的各步骤描述如下，评估人员应特别关注与同行评估队相关的信息。

6.2 步骤 1：收集电厂和 PSA 信息

至少在现场评估会议之前一个月，举办方应将有关资料提交给核能行业协会。本文件第8章提供了对所需资料类型的指导。

6.3 步骤 2：审查电厂和 PSA 资料

评估队应准备审查PSA的细节。形成完整的审查文档，在评估会议前分发。但是，对于单个的团队成员来说，他们的注意力应该集中到分配给他们的领域。

6.4 步骤 3：预备会议

同行评估队达到同行评估现场后，应召开内部的预备会议。会议内容主要是成员汇报对已提交资料的审查情况，交流需重点关注的要素和问题，并对评估程序、分工和时间安排进行讨论和最终确定。

6.5 步骤 4：入场会议，获得 PSA 的概况

举办方的PSA团队应准备一个关于PSA关键要素的详细介绍材料，包括电厂重要设计特征的概述、PSA项目的总体情况和主要结果。为了同行评估活动有效执行，举办方应准备好给评估队的材料。

6.6 步骤 5：采用问题和审核清单检查 PSA 要素

评估时，应首先开始进行高层次要求审查，然后延伸到详细技术问题的检查。这涉及PSA要素的广度和深度的检查。关于该步骤的详细方法和要求在附录A和附录B中加以规定。

为得到关于不同技术要素和PSA总体的相对质量的结论，评估人员应以国家能源行业技术标准为基础，有重点地审查PSA，并对发现的问题进行分级。每个评估人员应向整个评估队介绍他们的观点，评估队应对每一个PSA要素是否满足技术要求达成共识，并集中审查PSA的特定结论，以保证该评估直接针对计划中的电厂PSA应用。

6.7 步骤 6：通过巡访核实空间相关性

PSA审查的一个重要要素是对可能有空间相关性的电厂区域进行现场巡访，这些相关性可能产生新的事故序列或者增加先前已识别的序列的频率或改变序列进程。巡访可以在评估的前几天确定特定问题后，由同行评估队的部分成员来执行。但对于新建核电厂，可能现场巡访的条件并不具备，该步骤可不进行。

6.8 步骤 7：检查评估期间所进行的 PSA 敏感性分析的结果

在审查期间，很可能会产生与PSA结果有关的疑虑或问题。此时，应使用所审查的PSA计算机模型执行若干个敏感性分析案例计算来确认。

6.9 步骤 8：审查 PSA 维护和升级程序

应审查PSA维护的过程，确保所审查的PSA能够真实反映电厂、电厂规程和工作人员培训状态，以保证PSA能够有效地应用。

6.10 步骤 9：形成初步发现的问题和结论

这一步包括初步发现的问题和同行评估结果的形成，以及编制报告草稿。报告草稿为此评估的离场会议提供了依据（见步骤11 提供评估的最终文件）。

6.11 步骤 10：离场会议

此会议旨在向举办方PSA项目组和管理层陈述初步发现的问题和评估队报告并提交报告的初稿，会议将在现场评估的最后一天召开。

6.12 步骤 11：提供评估的最终文件

最终报告由评估队长利用在现场审查期间准备的信息和评估队提供的其它任何概括性注解来编写，并应由每一位同行评估队成员签署认可。该报告将确定评估队对每个技术要素的质量评定（并给出恰当的理由），以及指出需要改进的地方。

7 同行评估队

7.1 总体要求

同行评估队的组建和成员选择是同行评估程序最重要的一个方面。同行评估队应由在PSA的开发和应用中具有丰富经验的人员组成。该同行评估队成员包括对所评估电厂的同类电厂PSA有丰富知识的同行。同行评估队由核能行业协会负责组建。

同行评估队一般由10－12名 PSA专业人员（其中一人担任评估队队长）和一名协调员组成，每个PSA技术要素应配备主审和副审人员。

同行评估队总体上应具备以下特征：

—与审查的PSA有充分的独立性，

—在PSA的各个方面具有足够的专业性，

—在PSA的执行方面具有丰富经验，

—具有一定的代表性，可能的话，包括了工业界相关单位的代表（同行评估过程一个有用的副产品是将技术传递给作为审查者参与的其他单位工作人员）。

以下是上述特征的具体要求：

7.2 独立性

充分的独立性应满足以下要求：

评估队成员不应是负责开发该PSA的项目组成员，也不应是该PSA所针对的核电厂运营单位成员；

原则上，评估队成员不应曾经作为外部专家参与过该PSA的内部审查；

队长应来自于PSA项目组所在单位和该PSA所针对的核电厂运营单位以外的专家。

7.3 专业性

同行评估队应具有丰富的经验来执行同行评估程序，且从总体上覆盖本文件第4章所描述的所有技术要素。评估队成员从专业素养和经验上应满足以下要求：

（a）队长

－具有10年以上核领域工作经验，并且

－作为项目负责人组织过至少一次完整的PSA开发过程；

（b）一般成员

－具有8年以上核领域工作经验（工业界其他相关单位代表可放宽到5年），并且

－在PSA某个关键技术领域至少具有5年工作经验（工业界其他相关单位代表可放宽到3年），这些关键技术领域包括：

- PSA建模和定量化，
- 人员可靠性分析，
- 数据分析，

- 系统分析。

7.4 丰富的经验

每一个成员应都参加过至少一次PSA的执行、管理。

7.5 代表性

同行评估队应有一定数量的来自各相关单位的参与者。

本文件涉及的同行评估程序要求评估人员遵循一个比较紧凑的时间安排，如果同行评估队主要由无足够经验的人员组成，那么该程序难以有效完成。在每次评估开始前，应进行必要的培训，以保证所有的评估人员对该程序、审核清单和技术评定准则有一致理解。

协调员由核能行业协会指派人员担任，其职责是负责评估的组织、协调和联系工作；参与评估的前期的策划，负责内外联系和前期的准备工作；协助队长在评估的过程中组织和协调；协助队长培训评估员和评估报告的编制。

8 同行评估资料的准备

8.1 概述

同行评估所需要的资料包括两部分：

－同行评估开始前提交给评估队的资料

－现场评估期间所需的资料

以下对这两部分资料的准备要求分别进行描述。

8.2 同行评估前所需提交资料

表2中给出了举办方应在评估前向评估队提交的资料的详细清单。这些资料是同行评估需要用到的资料的一部分，其目的是为了让评估队成员在评估开始之前对所评估的PSA概况、电厂设计和厂址特征、主要方法、重要的事件序列和系统分析模型、主要结果（含敏感性分析）有一个初步的了解，以提高评估效率，保证评估效果。列出的资料应在评估前至少一个月提交到评估人员手中，以保证评估人员有足够的时间查阅。其中，有些资料应提供给每个评估人员审阅，而其他资料则可能只需要提交给那些负责特定领域评估的评估队成员即可。这些有限分发的文件可能包括人员可靠性分析方法描述和计算案例，数据分析和共因失效分析方法及数据处理案例，选定的敏感性案例。分发范围和要求应由评估队队长与举办方评估协调员讨论后决定。

表2 评估前向评估队提交的资料清单

文件名称2	备注
PSA 报告第 1 章 研究概况	
PSA 报告第 2 章 方法综述	

[2]此处的 PSA 报告是指按照 HAF •J0088 标准格式编写的报告。如果未按照此格式要求编写，则可参照表 1，提供相同内容的章节。

文件名称2	备注
PSA 报告第 3 章 电厂运行状态分析	
PSA 报告第 4 章 始发事件确定和分组	
PSA 报告第 5 章 事件序列分析	可选取部分内容，一般应包括LOCA中的一个、丧失厂外电、丧失余热排出系统。应包括相应的事件树图。
PSA 报告第 7 章 人员可靠性分析	可简化，但至少应包括分析方法论述、主要结果。
PSA 报告第 8 章 数据分析	可简化，但至少应包括数据选取原则、收集和处理方法论述、主要结果。
PSA 报告第 9 章 事件序列定量化	
PSA 报告第 12 章 敏感性分析	
PSA 报告附录 A 系统分析	可选取部分内容，一般应至少包括一个流体系统、一个电气系统。应包括相应的系统简化流程图、故障树图和顶事件最小割集。
PSA 报告附录 D 热工水力学及其他确定论分析	可简化，但至少应包括计算案例的目的、计算机程序、假设、案例清单、结果的汇总。
PSA 报告附录 F 编码规定	

8.3 现场评估所需资料

表3中给出了现场评估通常需要使用的或便于查阅而需要准备好的资料清单。这些资料应妥善保存在同行评估队工作区域。然而，资料的准备不仅仅是把所需的资料收集齐全，还应保证这些资料的时效性和相关性。表2清单以外的资料并不是同行评估队首要关注的，但

可能是需要备查的，应另行保存。需要重点注意的是，尽管本文件所涉及的PSA同行评估并不是文件的鉴定过程，但文件不足是影响PSA质量的一个因素，并导致评估人员不能恰当的评估PSA质量，也会影响最后的技术评定结果。

表3 现场评估所需资料清单

资料名称		备注
完整的 PSA 报告		
PSA 模型的电子文档		
PSA 各技术要素开发导则或实施程序		
电厂运行状态分析支持性材料	电厂运行状态划分的技术方法	
	电厂运行状态划分报告	
	各电厂运行状态的持续时间计算报告	
始发事件分析支持性资料	始发事件通用数据	
	始发事件特定电厂数据	对于在建核电厂，可不包括。
	始发事件数据处理报告	
	特定始发事件（如 ISLOCA、用故障树方法计算发生频率的丧失支持系统始发事件）分析报告	
数据分析支持性资料	设备分类和边界划分报告	
	设备可靠性参数通用数据	
	设备可靠性参数特定电厂数据采集与处理报告	对于在建核电厂，可不包括。

资料名称		备注
	共因失效通用数据	
	共因失效特定电厂数据采集与处理报告	如果只使用通用共因数据，可不包括。
	试验维修不可用度数据收集和处理报告	对于在建核电厂，可不包括。
	完整的基本事件清单（包括参数）	
	完整的共因失效事件组清单（包括参数）	
人员可靠性分析支持性资料	电厂工作人员访谈记录	对于在建核电厂，可不包括。
	人员可靠性分析详细计算过程	
成功准则分析支持性资料	详细的热工水力计算分析报告	
定量化分析支持性资料	各敏感性分析案例计算报告	
	各敏感性分析案例计算结果	应包括支配性最小割集
电厂一般性资料	系统手册	对于这些资料尚未完成编制的在建核电厂，可用参考核电厂的资料代替。
	停堆操作规程	
	事故规程	
	技术规格书	
	大修总结报告	

资料名称		备注
	详细的系统图册	
	最终安全分析报告	对于尚未编制最终安全分析报告的在建核电厂，可用初步安全分析报告代替。
	评估队认为需要的其他资料	

9 同行评估日程

从提交申请到完成最终评估报告，整个同行评估的持续时间一般为24周，进度安排见表4。

表4 概率安全分析同行评估日程

事件：

第 0 周：举办方提交同行评估申请

第 1 周：行业协会批准同行评估申请

第 4 周：组建同行评估队，完成培训

第 6 周：同行评估计划书发送到举办方

第 8-12 周：同行评估前现场访问（如果需要的话），为同行评估入场会议作准备（内部审查在此之前完成）

第 10 周：举办方将 PSA 评估资料送达同行评估队成员

第 16 周： 同行评估队的集中评估审查，编制同行评估报告初稿

第 24 周：编制同行评估最终报告

10 同行评估技术要素

核电厂PSA是一个对复杂系统和不确定物理过程所进行的广泛而详细的工程和统计分析。评估程序的目的是通过核实PSA的准确性、分析的真实性、完整性和文档质量，以提升PSA的质量水平。

如同本文件第4章所述，对于完整的内部事件一级PSA，PSA的质量由10项内容来保证，如5表所示。

表5 概率安全分析同行评估要素

代码	PSA 要素
POS	电厂运行状态分析
IE	始发事件分析
ES	事件序列分析
SC	成功准则
SY	系统分析
HR	人员可靠性分析
DA	数据分析
DF	相关性分析
MQ	模型整合与定量化
MU	模型维护与升级

在附录A和附录B给出的同行评估技术导则中，针对每项内容制定了同行评估的技术评定准则，为整个同行评估程序的完成和记录提供了依据。评估队应根据技术导则有序开展评估行动，对于发现的弱项或良好实践进行记录，填写事实观察表（格式见表C2）。

需要特别强调的是，遵循本文件进行的同行评估应针对每一个要素的技术特征给出是否满足的评定意见，在此基础之上，给出每一个技术要素是否满足要求的大概结论，并填写技术评定表（格式见附表A1至A9）。根据每一个技术要素的评定结论，对所评PSA的总体质量应给出一个整体性结论。

11 同行评估结果和文档

同行评估的输出结果是一份书面报告，记录了评估的细节和总结果。附录C给出了该报告和相关附件的建议格式。在评估现场准备的审核清单、事实和审查以及其他表格占本报告很大一部分。在现场评估结束时，同行评估队应就主要成果、结论和建议与举办方进行交流，并应将此包含在报告中。

同行评估报告应明确陈述以下方面的内容：

－每个PSA要素是否满足技术要求的大概结论；

－评估队的审查结果；

－改进建议

形成的正式评估报告应由中国核能行业协会报送举办方，同时报送核安全监管部门。

同行评估报告应作为举办方的PSA文档文件的一部分，以作为今后内部改进和其他外部评审的参考。

12 回访

12.1 回访人员组成

回访是同行评估的一部分，其目的是对举办方PSA在同行评估后的改进行动进行评估。

回访人员应从同行评估队中抽取，人数为4－5人，应包括：

－同行评估队队长；

－同行评估队协调员；

－部分技术要素主审。

至少应包括一名对PSA各技术要素都熟悉和了解的专家。

12.2 回访的组织与步骤

回访由同行评估主办方向中国核能行业协会提出申请，协会负责组建回访人员队伍，以及回访行动的实施。

根据A类和B类发现项数目以及改进行动完成情况，回访的持续时间为1－2天，包括以下步骤：

1)举办方的改进行动汇报

回访活动的第一天上午应举行入场会，举办方应就同行评估后的改进行动进行汇报，汇报内容应包括：

a)同行评估主要结论；

b)A类和B类发现项及改进行动，应针对发现项逐个介绍；

c)主要结果和风险见解。

2)针对A类和B类发现项的改进行动进行评估

针对A类和B类发现项的改进行动，回访人员应按照技术导则，逐个进行评估。需注意，回访人员的组成中不包括所有技术要素的主审，但是在回访的评估时应包括所有的A类和B类发现项。因此，在回访人员中应包括一名对PSA各技术要素都熟悉和了解的专家，以便对其他要素的发现项进行评估。

针对每一个A类和B类发现项，回访人员应填写回访事实观察表。

3)现场巡访（可选）

如果A类和B类发现项中涉及空间相关性，则针对其改进行动，必要时还应进行现场巡访，以核实改进的适当性。如不涉及空间相关性，该步骤可不进行。

4)形成同行评估回访报告

回访期间，回访人员应对每一个技术要素进行技术评定，在此基础上形成同行评估回访报告初稿，并在离场前向举办方介绍报告的主要结论。在回访结束2周内，应形成同行评估回访报告终稿，并由评估队队长签字确认。

13 附录 A（资料性附录）概率安全分析同行评估技术导则（功率工况内部事件一级）

A1. 目的

本附录属于同行评估中的功率工况内部事件一级PSA技术导则，主要目的是提供确定功率工况内部事件一级PSA的技术质量和充分性的方法，对评估PSA是否满足技术要求的准则进行规范。

A2. 范围

本附录的适用范围是功率工况内部事件一级PSA，涵盖了以下9项内容：

1)始发事件分析（IE）
2)事件序列分析（ES）
3)成功准则（SC）
4)系统分析（SY）
5)人员可靠性分析（HR）
6)数据分析（DA）
7)相关性分析（DF）
8)模型整合与定量化（MQ）
9)模型维护与升级（MU）

前8项为功率工况内部事件一级PSA的8个技术要素，其划分和代码与国家能源行业技术标准《应用于核电厂的概率安全评价第11部分：功率运行内部事件一级PSA》（NB/T20037.11）相一致，并以其技术要求为基础制定同行评估要求。最后一项是PSA的维护与升级的管理，目的是评估核电厂PSA是否能够随着电厂的实际情况而持续更新。

A3. 同行评估技术导则与技术标准的关系

国家能源行业技术标准《应用于核电厂的概率安全评价第11部分：功率运行内部事件一级PSA》（NB/T20037.11）主要参考ASME《应用于核电厂的概率风险评价标准》（ASME RA-S-2002，ASME RA-Sa-2003，ASME RA-Sb-2005，以ASME RA-Sb-2005作为参考的基准版本，以下统称为ASME标准），并结合IAEA的技术文件IAEA-TECDOC-1511中对PSA质量的要求以及NRC的管理导则RG1.200中对ASME标准的修改与补充，特别是结合我国在开发核电厂PSA模型中的经验，以及当前国内外PSA各技术要素的技术水平，借鉴IAEA及各国PSA同行评估中对PSA的技术要求，确定该标准的技术要素后，制定出的适用于核电厂功率运行工况内部事件一级PSA模型的技术标准。

本导则的技术评定准则基于NB/T20037.11，但两者还是有区别的。

技术标准主要是阐述一个应用于核电厂设计、执照申请、运行或维修等活动的PSA在技术上应该要达到什么要求，但不太多涉及如何达到这些要求。

同行评估技术导则主要阐述如何评判一个PSA在技术上是否达到了要求。

A4. 同行评估技术评定准则

附表A1－A9给出了针对技术标准，同行评估小组如何判断所评估的PSA是否满足要求。

在评定准则中，针对每一个技术要素，先总结出该要素应该具备的技术特征。随后根据技术要求，提炼出同行评估的管理行动，该管理行动提出了同行评估小组成员在对该技术要素需审查的重点内容。最后是该技术要素是否满足技术要求的评估标准。

附表 A1 始发事件分析

技术特征	同行评估行动	技术评定准则
实施程序（IE1）	审查始发事件分析实施程序。	始发事件分析实施程序对分析过程的描述应足够详细，以作为后续更新和修订的指导文件。该实施程序应该为进行始发事件分析提供合理基础，并且应与经验证的方法保持一致。实施程序的详细程度应足以支持获得等同的结果。
识别始发事件（IE2）	检查始发事件识别的方法，确保所采用的方法能够满足尽可能完整地找出始发事件清单的需要，并符合业界的良好实践。	应结合不同的堆型和不同的阶段合理选用分析方法，尽可能全面地综合使用多种方法，并应对分析的完整性进行论证。
	审查始发事件清单，并与类似机组 PSA 或 NUREG/CR-5750 中确认的始发事件进行比较。	始发事件清单至少包括了技术标准 SR-IE-A2 所列出的始发事件和类似机组 PSA 或 NUREG/CR-5750 中确认的始发事件，如果排除，则应记录其根据。
	审查是否考虑了受评核电厂或者类似核电厂的运行经验。	对受评核电厂或者类似核电厂的运行进行了收集、筛选和分析，并有分析记录文件。
	检查可能由某列失效或某个系统失效引发的始发事件，并确认是否采用了结构化的方法。	FMEA 分析是满足要求的一种方法，如果采用，应有分析记录文件。
对始发事件进行归并和分组（IE3）	审查始发事件归并分组文件。	应详细说明各始发事件是如何归并成为最终的始发事件类别。
	确认分组不会影响重要事故序列。	为了避免过度保守，作为包络条件的最严重事件的频率在所属始发事件组内不

技术特征	同行评估行动	技术评定准则
		能忽略，应避免将严重得多的事件与其他事件归并在一组。 应避免进行非保守性分组，即把某些始发事件归并到一组而不以最严重事故作为包络条件。
	审查可能导致更严重的放射性核素释放的事件的分组。	这些事件应分别单独作为一个事件组，这些事件包括压力容器破裂、界面系统 LOCA 和蒸汽发生器传热管破裂等。
估算每个始发事件或始发事件组的年发生频率（IE4）	审查始发事件发生频率确定原则。	对于由于系统故障导致的始发事件（例如界面系统 LOCA、支持系统故障导致的始发事件），可采用故障树方法进行分析； 与厂址条件密切相关的始发事件，应进行专项分析； 瞬态等比较常发的始发事件，应采集电厂特定数据。
	审查电厂运行经验数据的收集和处理报告。	如果有足够可用的数据，始发事件频率可根据电厂特定数据计算，否则采用贝叶斯方法或等价的统计方法。始发事件的频率应该使用最新的可用数据。可剔除商业运行后第 1 年的数据，但应有合理的论证。
	如果对于支持系统故障导致的始发事件建立了故障树进行分析，审查始发事件故障树方法，检查始发事件故障树和定量化过程与结果。	每一个最小割集是由一个部件的年故障频率事件与其他部件的不可用概率事件组成（单阶割集除外），其他部件的不可用概率事件应使用合理的任务时间，例如采用技术规格书的 AOT、第一个部件故障的平均修复时间。应考虑重要部件的共因故障。

技术特征	同行评估行动	技术评定准则
	将各始发事件发生频率与类似机组或国际上公认的通用数据进行比较。	如果与类似机组或者通用数据的发生频率有较大差异，则需有合理的解释。
文档记录（IE5）	审查始发事件分析的文档。	始发事件分析的文档应保证其分析是可追溯的，包括： 1) 始发事件清单的确定过程； 2) 电厂始发事件数据的收集与甄别； 3) 始发事件分组的基础； 4) 始发事件发生频率的分析过程。

附表 A2 事件序列分析

技术特征	同行评估行动	技术评定准则
实施程序（ES1）	审查事件序列分析实施程序或导则。	实施程序或导则对事件序列分析过程的描述足以为后续升版和修订提供指导；应与业界认可的方法保持一致，并为事件序列分析提供合理的依据；导则的详细程度应支持足以获得等同的结果。
事件序列评估（ES2）	审查事件树是否反映了始发事件分组。	事件树应反映始发事件组及其对电厂响应的潜在影响，不同始发事件的电厂响应都应模化，包括时间、系统成功准则和操纵员动作。
	审查事件序列分析及模型是否与电厂实际状态相一致。	证实模型与分析与电厂实际状态是一致的，系统分析和相关性评估将在建模过程中提供相应输入。
	审查典型的事件序列模化是否正确。	模型应包含所必需的关键安全功能，并完成定量化模型，如有例外情况需加以说明。每个功能中所有相关的系统均应在模型中考虑。 事件树结构应恰当描绘规程中关键的操纵员动作及对关键安全功能的影响。 对于所模化的可能引起堆芯损坏的每个始发事件，应建立一套合理完整的事件序列。 应正确定义并现实地处理成功路径。
	审查事件树之间的分支转移是否正确。	事件树之间的转移应明确定义并作相应的定量或定性处理。 事件树之间的转移应保留相关性，包括功能、系统、始发事件、操纵员、以及

技术特征	同行评估行动	技术评定准则
		空间或环境的相关性。 为避免在转移过程中遗漏信息，定量化模型中应单独处理事件树之间的转移并编制文档。
	审查事件树题头之间的相关性。	应识别和处理题头之间的相关性，包括功能、系统内及系统间、人因、空间/环境的相关性。 相关性处理方法应编制文档，并与题头之间相关性处理相一致；应现实地处理相关性。 定量化模型中应合理定义明显具有时间相关特征的失效模式及可能的恢复，例如，SBO 情景下电池容量及交流电源恢复。
	审查是否合理模化主泵轴封 LOCA 事件。	PSA 模型应模化主泵轴封 LOCA（如果不模化则需说明理由）。
	审查是否正确模化系统/设备的维修和恢复。	PSA 模型中包含的维修和恢复应基于适用的数据或可接受的模型，并考虑事件序列的相关性，例如，可用时间，不利环境，及缺少通道、照明或房间冷却。
与运行规程的接口（ES3）	审查事件树功能和结构是否反映异常和事故规程。	事件树功能和结构应与异常和事故规程相一致。规程引导的操纵员动作，如果显著影响事件序列进程或失效概率，则应在相应的事件序列结构或故障树分析中加以考虑。
事件序列终态（ES4）	审查事件序列终态。	一级 PSA 终态应明确定义为堆芯损坏或安全稳定状态。堆芯损坏的定义与成功

技术特征	同行评估行动	技术评定准则
		准则中的考虑要一致，堆芯损坏基于 24 小时或其它证明是适当的任务时间。
文档（ES5）	审查建立事件树结构的依据文档。	对于特定电厂的或通用的分析应是可追溯的。建立的文档应包括事件树图，文字描述。 要求文档能提供满足上述准则的依据，反映建树过程。

附表 A3 成功准则分析

技术特征	同行评估行动	技术评定准则
实施程序（SC1）	审查成功准则及热工水力计算分析的实施程序。	应详细描述成功准则分析过程，使其可作为后续升版和更新工作的指南，所采用的分析方法应符合行业标准相应的要求。
成功准则定义（SC2）	审查关键安全功能成功准则的定义。	应识别关键安全功能的成功准则并编制文档，关键安全功能应有相应的技术依据以支持 PSA。
	审查堆芯损坏的判据。	一级 PSA 终态应明确定义为堆芯损坏或安全稳定状态。堆芯损坏判据应与 NB/T 20037.1 一致。对于压水堆核电厂堆芯损坏判据如下： 1) 堆芯塌陷水位长期低于燃料活性区顶部；或 2) 详细堆芯模型分析堆芯燃料包壳表面峰值节点温度>1204℃；或 3) 简化堆芯模型分析堆芯燃料包壳表面峰值节点温度>982℃；或 4) 简化堆芯模型分析堆芯出口热电偶温度>650℃。
	审查成功准则对应任务时间。	对于已经达到稳定状态的序列，一般可采用最短 24 小时的任务时间；如果 24 小时仍不能达到稳定状态，则应认定该序列为电厂损伤状态或采用适当方法加以评估。
	审查构筑物、系统、部件及人员动作的成功准则。	应按照事件序列分析要求对每个模化的始发事件给出为防止堆芯损坏所需要的构筑物、系统、部件及人员动作的成功准则，并且这些成功准则应与电厂竣工

技术特征	同行评估行动	技术评定准则
		和实际运行的特征、规程和运行原则相一致。
成功准则确定与依据（SC3）	审查成功准则的依据，包括 审查确定系统/部件、事件序列及人员动作的成功准则的依据等。	成功准则可基于现实的热工水力分析，或确定论安全分析结果以及参考电厂的分析结果。用于不同始发事件组和相应事件树中的成功准则应体现始发事件及事件序列发展对系统失效的影响。如果采用保守的包络分析，应对最终结果不产生明显影响。
		采用合理现实的、通用的或特定电厂的热工水力计算分析来确定系统、事件序列及人员动作可用时间的成功准则。支持成功准则的依据应足以进行模型定量化，即运用热工水力或其它适用的分析/评估应考虑到与始发事件（组）和事件序列模化相一致的详细程度。
	审查热工水力计算程序模型的适用性和结果的合理性。	热工水力分析模型和计算机程序应有能力建模确定出所考虑工况的成功准则，可使用类似电厂中使用过的热工水力程序、模型或分析来进行定性评价。 当条件允许时，应与类似电厂分析结果进行比较并考虑电厂特征的差异，或与其它电厂特有程序的相似分析的结果进行比较，如果与类似机组情况有较大差异，则需有合理的解释。
	审查建立成功准则过程中的关键假设和不确定性的来源，以及一些专家判断的合理性。	应与 PSA 标准及业界的作法相一致；只有在缺乏关于所模化的 SSC 状态或响应的可用信息，或者缺乏作为预计 SSC 状态或响应依据的分析方法情况下才使

技术特征	同行评估行动	技术评定准则
		用专家判断，其他情况不使用专家判断。使用专家判断时应给出相应的使用原则，并且满足 NB/T 20037.1 相应要求。
文档（SC4）	审查支持成功准则的依据的文档。	文档应包括特定电厂的、或通用的热工水力分析，要求足以支持成功准则的确定，并且是经过有丰富经验人员独立审查过的。 文档应当给出满足上述成功准则定义和成功准则依据的技术准则要求，文档描述的结果与过程相一致。 文档应包括成功准则确定过程中用到的保守的、简化的假设条件和特定的判断。

附表 A4 系统分析

技术特征	同行评估行动	技术评定准则
实施程序（SY1）	审查系统分析实施程序。	实施程序应对系统分析的输入、分析方法和步骤、简化原则和基本假设的确定、设备失效的考虑、相关性的处理、共因失效的处理、人员失误的处理、试验维修不可用的处理、建造故障树的原则和步骤、定性和定量分析的要求和文档的编制等做出规定。 实施程序的详细程度应能够指导系统分析人员进行并规范系统分析工作。
系统分析模型（SY2）	审查系统分析模型，确保事件序列分析中与安全功能相关的所有系统建立系统分析模型。	应对所有的前沿系统和支持系统建立详细的系统分析模型，以下情形可以不建立详细的系统分析模型： 1) 在不具备建立详细模型的情况下可以采用系统级的数据，但要说明对系统分析结果的影响； 2) 系统失效的主要贡献是操纵员动作，并且省略建模不会掩盖对支持系统或其他相关性失效模式的贡献。
	审查系统成功运行所需设备的清单。	对系统成功运行有重要影响的设备应包含在清单内，应与系统分析的简化原则和基本假设保持一致，须绘制系统分析简化流程图。

技术特征	同行评估行动	技术评定准则
	审查系统模型是否反映所有不同成功准则的系统构成。	应根据不同的成功准则建立系统分析模型，或通过设置边界条件使得系统分析模型能够在不同的边界条件取值下反映不同的成功准则。 应反映如下情况带来的成功准则的不同：不同的事故情景、与其他部件的相关性、两个机组共用情况。
	审查系统模型中包含的影响系统可运行性（由系统成功准则确定）的设备。	应包括能动部件（例如，泵、阀门和空气压缩机）、非能动部件（例如，热交换器和水箱）和系统特定设备。只有满足 NB/T 20037.1 中 SY-A13 的准则时，才可不包含这一设备。 设备的边界应与建立设备失效数据所用的定义相一致。
	审查设备失效包含的失效模式。	应考虑对设备失效有重要影响的失效模式。 应考虑设备的状态，避免考虑在某种状态下不可能发生的失效模式。 应与采用的数据和模型的详细程度相一致，只有满足 NB/T 20037.1 中 SY-A13 的准则时，才可不包括该设备的这些失效模式。
	审查人员失误事件。	应包含会导致系统或设备在需求时不可用的人员失误事件（始发事件前人员失误事件）；应包含在系统或设备的运行中预期出现的人员失误事件或在事故序列的最终定量化时考虑的人员失误事件（始发事件后人员失误事件），除非在事故序列模型中已经明确包含了这些人员失误事件。

技术特征	同行评估行动	技术评定准则
	审查互斥事件组。	应对互斥事件组进行处理，避免同时考虑互斥事件组中的事件，如开关的拒开和拒关。
	审查设备退出服务的不可用事件，并确保对不可用事件的影响进行了合理的处理。	应包括：当一个设备或系统系列因试验造成设备不可用无法执行其安全功能；当规程要求隔离整个系列进行维修时的系统级维修事件；在规程指导下的子系列级（即，在作标记的边界之间，例如一个功能设备组）的维修事件。 一般来说，冗余系统的不同系列的维修是互斥的，应合理处理。
共因失效和系统相关性（SY3）	抽查系统内共因失效，确保对系统内共因失效进行了完整地处理。	应对系统内的共因失效进行建模；应采用一种逻辑化、系统化的方法建立共因失效组；应合理的选择共因失效组；共因失效的候选设备应包括 SY-B3 规定的设备；共因失效模型应与数据分析的共因模型相一致。
	抽查与支持系统或接口系统的相关性。	应考虑系统与支持系统或接口系统的相关性，可通过故障树连接或事件树连接的方法。 应考虑要求的任务时间内系统成功运行所需的所有支持系统。 应考虑启动和触发一个系统所要求的系统。
系统分析定量化（SY4）	以足够低的截断值定量化系统分析模型。	选取的截断值应足够低，以避免将对系统失效有较大贡献的割集截断。

技术特征	同行评估行动	技术评定准则
	对用于支持不同成功准则的系统分析模型进行顶事件失效概率计算，并确定支配性最小割集。	应对所有的顶事件或用于支持相关系统的接口顶事件进行失效概率计算，并确定导致这些顶事件发生的支配性最小割集。
	对系统分析模型进行重要度分析。	应对系统分析模型进行重要度分析，并确定对系统失效具有重要贡献的事件、设备、人员动作等。
文档记录（SY5）	审查系统分析文档的内容。	文档应提供系统建模的依据，保证其分析是可追溯的。 1) 应包含对系统功能和边界、相关的成功准则、模化的设备和包括人员动作在内的失效模式以及包括支持系统和共因失效在内的相关性模型的描述； 2) 应包括对系统分析有关的假设产生的模型不确性来源的描述； 3) 应包括对系统定量化分析结果的描述，包括顶事件失效概率、支配性最小割集、不确定性分析结果、重要度列表、敏感性分析结果等。

附表 A5 人员可靠性分析

技术特征	同行评估行动	技术评定准则
实施程序（HR1）	审查人员可靠性分析实施程序。	实施程序应对人员可靠性分析过程有详细的描述，便于作为今后更新和升版的指导；实施程序应为开展 HRA 给出合理的技术基础，并与公认的方法保持一致。实施程序内容应足够详细，以支持获得等同的分析结果。
事故前人员动作（HR2）	确认在 PSA 中考虑了事故前人员动作。	应在 PSA 中明确包含事故前人员失误事件，特别是会导致多个冗余部件失效的潜在失误。 应包括对基准 CDF 可能存在不利影响的事故前人员动作，例如： 1) 未能恢复设备至所期望的备用或运行状态； 2) 未能恢复使设备启动或重新接入的启动信号或设定值； 3) 未能恢复自动重新接入或供电。
	审查事故前人员失误的识别方法。	应采用系统化的方法来识别 PSA 中包含的事故前人员失误，应包括对电厂规程和培训的审查以识别可能导致多个冗余部件失效的潜在失误。
	审查在对事故前人员动作的 HEP 定量化过程。	下列情况下可筛选掉事故前 HEP 而不必作进一步考虑： 1) 有设备位置监视； 2) 设备能自动复位； 3) 要求经常检查设备的状态（每个运行值至少一次）；

技术特征	同行评估行动	技术评定准则
		4) 执行维修后功能试验。 在对有支配性贡献的事故前 HEP 定量化时应采用最佳估算 HEP，包括恢复因子的考虑。其余的事故前 HEP 可采用筛选值。
事故后人员动作（HR3）	审查事故后人员动作的识别方法。	应包含预防和缓解系统的触发、控制、隔离和投入相关人员动作的 HEP。应采用系统化的方法识别 PSA 中包含的事故后人员失误，该方法应考虑人员动作的复杂性、完成动作的可用时间和所需时间、由事故情景导致的紧张程度影响等各方面因素。
	审查 HRA 中对电厂规程和特定运行经验的评价。	在人员动作的识别和定量化时应明确包含对电厂规程和特定运行经验的评价。在评价时应包含对操纵员、培训人员或值长的访谈，并形成访谈记录。
	审查事故后人员动作的 HEP 定量化过程。	HEP 值应为 PSA 提供相对准确的失误概率，应尽量减少筛选 HEP 的使用。特别在对 CDF 的主要贡献因素进行定量化时不应采用筛选 HEP，而应采用最佳估算 HEP。
	审查运行人员对操纵员动作的反馈。	运行人员应至少对支配性操纵员动作进行审查，并且其输入已包含在 HRA 评价中。 并且，HRA 的假设和判断应与操纵员培训和规程相一致。应让运行人员对 HRA 计算内容进行审查，特别是分析中所作的假设。

技术特征	同行评估行动	技术评定准则
	审查人员动作是否正确结合到模型中，及其模化的合理性。	在计算 HEP 时应正确体现所模化的事件序列的规程、培训和模拟机响应。在模型中应包含 HEP 来表示那些特定序列的动作。
	审查定量化中相关的绩效形成因子的模化。	定量化时应模化表示特定事件序列和相关 HEP 的绩效形成因子，包括可用时间、执行时间、紧张程度、复杂度、可用的指示、资源限制等。 总的 HEP 应包含诊断、操作等贡献因素的评价。
	审查动作的可用时间获取的合理性。	动作的可用时间应基于电厂特定的热工水力分析或考虑了电厂特性的通用分析。 应识别提示操纵员动作的信号发出时间。
	审查完成动作所需的时间来源和依据。	完成动作所需的时间应基于观测或运行人员的访谈。
	审查恢复动作模化的合理性。	如果考虑恢复动作，则应满足以下条件： 1) 有可用的规程，并且已在所有操纵员的培训中针对这类动作进行过培训； 2) 有提醒操纵员采取恢复动作的“提示”，例如警报； 3) 有充足的人力来执行该动作。 应考虑恢复动作与动作所涉及的序列、情景或最小割集中其他 HFE 之间的相关性。
人员动作间的相关性	审查人员动作之间的相关性和模型的充分	在 PSA 中应评价人员动作之间的相关性。相关性的分析应考虑：

技术特征	同行评估行动	技术评定准则
（HR4）	性。	1) 完成所有动作所需的时间与执行这些动作的可用时间的关系； 2) 可能引起相关性的因素，例如公共的仪表、公用的规程、紧张程度加大等等； 3) 资源的可用性，如人员。 在检验模型的充分性时，除了恢复动作中很低的人员失误概率，应当对可能成为堆芯损坏频率支配性贡献的序列进行识别。
文档记录（HR5）	审查人员可靠性分析文档。	将识别、表征、量化始发事件前/始发事件后人员失误事件以及恢复动作的过程形成文档，包括输入、方法和结果，确保分析的可追溯性。例如，该文档通常包括： 1) 用于确定始发事件前/后人员失误概率的 HRA 方法和过程； 2) 定性筛选规则和筛选结果； 3) 用于量化人员动作的因素，以及如何将其考虑到量化过程中； 4) 人员失误概率的定量化，包括： a） 筛选值及其依据； b） 详细的人员失误概率分析； c） 始发事件后人员动作的相关性的分析方法及处理；

技术特征	同行评估行动	技术评定准则
		d） 模型、系统、始发事件和功能评价中的始发事件前和始发事件后的人员动作列表； e） 恢复动作的人员失误概率及其与其他 HEP 的相关性。

附表 A6 数据分析

技术特征	同行评估行动	技术评定准则
实施程序（DA1）	审查数据分析实施程序。	数据分析实施程序对分析过程的描述应足够详细，以作为后续更新和修订的指导文件。该实施程序应该为进行始发事件分析提供合理基础，并且应与经验证的方法保持一致。
通用数据源（DA2）	检查所选取的通用数据源，包括公开的通用数据源和设备生产厂家专用数据源。	应使用业界所公认的通用数据源，例如： 1) 设备失效数据：NUREG/CR-4550、NUREG/CR-6928； 2) 共因失效参数：NUREG/CR-5497。 对于通用数据源未包括的设备，可采用厂家专用数据作为通用数据。 对数据的选取应该做出分析与评价。
设备边界划分和归类（DA3）	检查设备边界划分。	设备边界划分应与所选用的通用数据或厂家专用数据以及与“系统分析”要素中对设备失效模式的模化相一致。 应有设备边界划分的详细记录。
	检查设备分类文件和设备清单。	在对设备进行归类时，考虑了以下因素： 1) 任务类型 2) 工作条件 设备样本空间应涵盖 PSA 所模化的所有设备。

技术特征	同行评估行动	技术评定准则
		每一个 PSA 所模化的设备应归类到一个设备类中。 应有设备样本空间选取和归类的详细记录。
电厂特定数据的采集（DA4）	抽查电厂数据采集报告。	应采集自商运以来的电厂特定数据。对于新建核电厂，可采用类似设计核电厂的数据，或者使用通用数据。 如果对某一时间段的数据进行筛选，则应有合理的筛选理由，经论证后的电厂设计改造、运行实践变化导致原有数据不适用是可接受的理由。 设备需求次数和运行时间应来自电厂实际的试验、维修、运行记录。对于记录不完整的情况，可根据电厂试验、维修、运行等规程估计需求次数和运行时间。 设备失效数据应尽可能完整地收集来自电厂的实际记录。 如果设备降级在所考虑的任务时间内不影响 PSA 模化的安全功能，则不应计为失效，否则应计入。对不计为失效的设备降级，应有筛除记录。
	抽查不可用度采集和处理报告。	系统、列、设备不可用度的采集应基于电厂特定数据。对于新建核电厂，可采用类似设计核电厂的数据，或者采用设计文件数据。 不可用时间应来自电厂实际的试验、维修等记录。 对于定期试验，如果试验期间有自动信号恢复其可用，则不应计入试验维修不可用。

技术特征	同行评估行动	技术评定准则
		支持系统的不可用应单独计入到支持系统的不可用度。 能够导致冗余设备不可用的事件应单独统计和处理。
电厂特定的参数估计（DA5）	检查电厂特定数据处理过程报告。	如果有足够的电厂特定数据，根据电厂特定数据来计算重要基本事件的参数值和不确定性参数。 如果没有足够的电厂特定数据，则在相关通用的和电厂特定的统计证据基础上计算它们的参数估计值，贝叶斯更新方法是一种可接受的处理方法。 可以只对重要的基本事件来估计电厂特定的参数，其余事件可采用通用数据。 应给出参数估计值的不确定性分布参数。 对于新建核电厂，可采用参考核电厂数据或其他核电厂同类型设备的数据。对于独特设备，可采用设计文件数据或者通用数据。
共因失效参数（DA6）	检查共因失效参数报告。	对共因失效参数的确定方法做出说明与评价。 共因失效参数应与模型中采用的共因失效模型相一致。 可以采用工业界公认的共因失效通用数据。
文档记录（DA7）	审查数据分析文档。	数据分析的文档应保证其分析是可追溯的，包括： 1) 通用数据源的确定过程； 2) 设备边界划分和归类；

技术特征	同行评估行动	技术评定准则
		3) 电厂特定数据的采集，包括维修和失效事件的甄别、需求和运行时间、不可用时间等； 4) 电厂特定参数的估计方法、过程与结果； 5) 共因失效参数的选取。

附表 A7 相关性分析

技术特征	同行评估行动	技术评定准则
实施程序（DF1）	审查相关性分析实施程序。	实施程序对相关性分析有定义清晰，识别出重要的相关性，描述了这些相关性的分析方法。
功能和实体相关性(DF2)	检查事件序列和系统故障树分析模型，安全功能的定义和划分结果。	全面考虑设计方面的相关性。 事件序列分析中体现功能之间的相关性，安全功能的定义应清晰明确，符合业界的良好实践；且在事件序列中正确反映。功能相关性的特殊假设和限制条件应记录于分析文件之中。 应模化支持系统，并通过适当的转移门链接至系统模型中。 系统范围有明确的定义，对于不同系统间的共用部件的同一失效模式，应有确定且唯一的编码，并在故障树中分别给予模化。 使用系统相关性矩阵记录功能相关性。
人员可靠性相关性（DF3）	审查始发事件前人员失误相关性的考虑。	始发事件前人员失误事件之间的相关性应该体现在系统模型中，包括维修、试验、标定情况导致的相关性。
	审查系统局部失效的情况下（如丧失一列设备冷却水系统，由于切换失败导致失效）人员失误相关性。	操纵员实施应急操作规程可能出现的相关性应在系统建模中处理。

技术特征	同行评估行动	技术评定准则
	审查安全功能和人员失误相关性的考虑。	功能或系统对操纵员干预的相关性应在事件序列和系统模型中模化。
	审查事件序列和系统建模中考虑的人员失误事件相关性。	同一个最小割集中的多个人员失误事件之间应该考虑相关性，相关人员失误事件的赋值应做适当调整。
设备环境恶化导致的相关性(DF4)	审查有关管道破裂，可能导致二次效应以及可能导致相关安全设备失效的场景的考虑，确认设备环境恶化导致的相关性。	考虑管道破裂或容器破裂等情况导致的管道甩动、飞射物、水/蒸汽喷射冲击。
		考虑湿度或温度上升导致的一些后果。
		考虑保温层材料脱落阻塞再循环流动（LOCA 事故后）。
共因始发事件(DF5)	审查对共因始发事件的模化，共因始发事件（CCI）是指导致瞬态（或者需要手动停堆）的事件，且事件发生后所需的一个或者多个安全功能同时降级。	应识别出由于共因导致的始发事件，如控制和保护系统、电源系统、重要厂用水系统或者其他支持系统的失效，并在模型中正确模化。在模化中应考虑始发事件导致的安全功能降级或失效。
部件共因故障分析(DF6)	审查事件序列和故障分析中对部件共因失效的考虑。	共因故障的定义清晰。 正确识别了共因故障，确定共因事件组。 共因失效分析方法是国际上通用并符合业界的良好实践。 在模型中体现共因故障。 采用国际上比较通用的共因数据源，共因故障的分析应达到共因失效数据所能支持的程度。

技术特征	同行评估行动	技术评定准则
文档记录(DF7)	审查相关性分析的文档记录。	文档记录应清晰、准确，可追溯。

附表 A8 模型整合与定量化（MQ）

技术特征	同行评估行动	技术评定准则
实施程序（MQ1）	审查模型整合及定量化分析的实施程序。	实施程序应对定量化所采用的分析软件版本及特性、模型整合流程、定量化计算过程中软件参数的设置、边界条件的设置、逻辑环路的处理等给出说明，并说明最小割集计算、不确定性、重要度、敏感性分析的原理及分析步骤。 实施程序的详细程度应能够使从业人员进行并规范模型整合与定量化工作。
PSA 模型整合（MQ2）	审查所有的系统模型和事件序列分析模型到 PSA 模型中的整合。	在整合的PSA模型中应包含PSA分析中所考虑的所有始发事件及对应的事件树和故障树模型，并包括所考虑的转移事件树模型。
	结合模型及报告中的事件树题头及成功准则表，审查事件树题头与对应输入链接的正确性。	应确保故障树的逻辑等输入满足对应事件树题头的成功准则要求。
	审查 PSA 中包含定量化计算过程所需的边界条件的设置。	应在 PSA 模型中正确设置边界条件，并有文档记录。
	审查逻辑环路的合理处理。	模型中如果存在逻辑环路，则应通过合适的、可解释的，且不会对定量化结果产生重要影响的方式进行处理（断开逻辑循环的方法可参见 NUREG/CR-2728）。应有文档记录。

技术特征	同行评估行动	技术评定准则
堆芯损坏频率的定量计算（MQ3）	审查每一个始发事件组的定量化，检查得到的事件序列频率。	对于导致堆芯损坏（CD）总的 CDF 及各始发事件类导致堆芯损坏的 CDF 进行计算，并给出其对应的评价结果。
	审查模型的正确性和评价结果的合理性。	对支配性序列的结果进行检查，可以参考国内外同类型电厂的分析结果以确认整合的 PSA 模型的正确性和结果的合理性。
	审查恢复动作的处理。	为了避免不必要的过分保守，在模型中可考虑适当的恢复动作。在报告中对于所考虑的恢复动作给予说明，并且以适当的形式给出恢复概率的计算过程与相关支持材料。
定量化软件及其使用（MQ4）	审查定量化软件的合法性。	申请者提交的模型所采用的 PSA 分析软件应是本行业被国内外广泛认可的专业分析软件；如果是有具备软件开发资格的单位开发的专业软件，则需要提交软件认证材料，及软件分析验证支持材料，以证明软件分析结果的正确性。
	审查截断值的选取。	应综合考虑 CDF 计算结果的准确性及计算机运算速度，在分析中选取合适的截断值，以免忽略重要的最小割集或事故序列。
	审查系统成功的处理。	应当说明如何在 PSA 软件中对系统成功处理的设置，以实现对成功逻辑和概率的模化。

技术特征	同行评估行动	技术评定准则
	审查互斥事件的处理。	应在分析中说明互斥事件的具体处理方法，一般来说可以通过下列两种方式之一进行修正： 1) 用逻辑模型消除互斥的情况； 2) 在结果中删除含有互斥事件的最小割集。
计算结果审查（MQ5）	抽样审查重要的（或支配性的）最小割集和序列。	支配性最小割集和序列的逻辑应合理，反映电厂的实际情况。有条件的情况下，可与相同类型的核电厂 PSA 分析结果对比，如果差异较大，则应给出合理解释。
	审查对 CDF 有重要贡献的事项。	定量化结果中应当分别论述对 CDF 产生重要贡献的项目，包括始发事件、事故序列、设备失效、共因故障及人误事件等
不确定性分析（MQ6）	审查定量化结果的不确定性分析结果和不确定性的主要来源。	应说明不确定性的来源和定量计算的方法，并给出评价结果。
重要度分析（MQ7）	审查重要度分析方法及其分析结果。	应针对始发事件、设备失效基本事件、人误事件、共因失效等进行重要度分析，列表给出重要度较高的分析结果（至少给出 FV 及 RIF 重要度，或等价的重要度），并且应对重要度分析结果给出讨论与分析，解释其合理性，应保证重要度分析与敏感性分析在定性上是一致的。

技术特征	同行评估行动	技术评定准则
敏感性分析（MQ8）	审查敏感性分析方法及其分析结果。	应针对始发事件、设备失效基本事件、人误事件、可靠性参数、共因事件等进行敏感性分析，说明敏感因子的取值，并列表给出敏感性分析结果，并且应对敏感性分析结果给出讨论与分析，解释其合理性，应保证重要度分析与敏感性分析在定性上是一致的。 对模型中重要假设进行敏感性分析。
	对重要度高，敏感性强的问题开展专题敏感性分析的审查，可进行实例校验。	应针对某些特定构模假设、特定数据等开展专题敏感性分析，以便进一步解释其合理性，并给出有益见解。
文档记录（MQ9）	审查模型定量化的文档记录。	文档记录应清晰、准确，可追溯。

附表 A9 模型维护和升级

技术特征	同行评估行动	技术评定准则
模型维护和升级程序（MU1）	审查有关模型维护和升级的实施程序。	模型使用者应提供模型维护和升级的管理程序。 应详细描述采用的模型维护和升级的程序，且与业界的普遍实践一致。
电厂运行经验、设计变更和改造信息的收集（MU2）	审查信息收集的过程和结果。	应建立了运行经验、设计变更和改造信息的收集渠道和程序。 收集信息的来源应包含以下几个方面： 运行经验、设计变更、新的维修策略、操作员培训程序、技术规格书、升版的工程计算结果、应急和异常处理规程、运行规程、应急计划，事故管理程序以及业界的研究成果。
	审查电厂特定数据的收集情况。	应建立了相应的组织机构进行数据收集，并编制了数据采集导则，建立了电厂特定数据库。应定期收集和处理电厂数据，并按模型升级的周期更新数据。
模型版本控制（MU3）	审查 PSA 模型的版本控制情况。	PSA 模型应以有效地方式进行管理并处于受控状态，包括存储地点以及管理权限等。
计算机程序控制（MU4）	审查与模型相关的计算机程序的控制与管理。	计算机程序已经定型，PSA 模型的变更对于程序的影响已经得到充分的理解并适当的。
模型的升级（MU5）	审查模型的升级管理。	应制定模型升级的固定计划，间隔时间原则上不应超过 4 年。 应按计划定期对模型进行升级，对于需要升级的要求制定了合理的判断准则。

技术特征	同行评估行动	技术评定准则
		由于电厂设计或技术标准的重大变更造成的重要更新应及时升级
	审查模型升级相关的过程和结果，PSA 模型需尽可能的与电厂的实际情况保持一致。	模型的升级过程应包括下列要素： 1) 识别出影响模型的各个 PSA 要素； 2) 修改 PSA 模型，评估结果； 3) 针对 PSA 的各个要素已经建立了适当的实施程序。 模型升级过程应有详细的文档记录。
结果的评估（MU6）	审查对于升版后的模型进行评估的结果。	升级后的模型应由有经验的人进行内部审查和验证，使得升级后 PSA 模型的计算结果可靠。
文档记录（MU7）	审查对模型维护和升级过程的文档。	文档记录应清晰、准确、及时，可追溯。

14 附录 B（资料性附录）概率安全分析同行评估技术导则（低功率和停堆工况内部事件一级）

B1. 目的

本附录属于低功率和停堆工况内部事件一级概率安全分析同行评估中的技术导则，主要目的是提供确定低功率和停堆工况内部事件一级PSA的技术质量和充分性的方法，对评估低功率和停堆工况内部事件一级PSA是否满足技术要求的准则进行规范。

B2. 范围

适用范围是低功率和停堆工况内部事件一级PSA（所分析的放射源为反应堆堆芯，所关注的是堆芯损坏（CD）风险，乏燃料水池风险不在评价范围之内），涵盖了以下10项内容：

1)电厂运行状态分析（POS）
2)始发事件分析（IE）
3)事件序列分析（ES）
4)成功准则（SC）
5)系统分析（SA）
6)人员可靠性分析（HR）
7)数据分析（DA）
8)相关性分析（DF）
9)模型整合与定量化（MQ）
10)模型维护与升级（MU）

前9项为低功率和停堆工况内部事件一级PSA的9个技术要素，其划分和代码与国家能源行业技术标准《应用于核电厂的概率安全评价第2部分:低功率和停堆工况内部事件一级PSA》（NB/T20037.2）相一致，并以其技术要求为基础制定同行评估要求。最后一项是PSA的维护与升级的管理，目的是评估核电厂PSA是否能够随着电厂的实际情况而持续更新。

B3. 同行评估技术导则与技术标准的关系

国家能源行业技术标准《应用于核电厂的概率安全评价第2部分：低功率和停堆工况内部事件一级PSA》（NB/T20037.2）主要参考美国核学会（ANS）制定的低功率和停堆(LPSD)概率风险评价(PRA)方法标准草案(Low-Power and Shutdown PRA Methodology Standard draft#8c)，并结合IAEA的技术文件IAEA-TECDOC-1511中对PSA质量的要求，特别是结合我国在开发核电厂PSA模型中的经验，以及当前国内外低功率和停堆工况内部事件一级PSA各技术要素的技术水平，借鉴IAEA及各国低功率和停堆工况内部事件一级PSA同行评估中对PSA的技术要求，确定该标准的技术要素后，制定出的适用于核电厂低功率和停堆工况内部事件一级PSA模型的技术标准。

本导则的技术评定准则是基于NB/T20037.2，但两者还是有区别的。

技术标准主要是阐述一个应用于核电厂设计、执照申请、运行或维修等活动的PSA在技术上应该要达到什么要求，但不太多涉及如何达到这些要求。

同行评估技术导则主要是阐述如何评判一个PSA在技术上是否达到了要求。

B4. 同行评估技术评定准则

附表B1－B10给出了针对技术标准，同行评估小组如何判断所评估的PSA是否满足要求。

在评定准则中，针对每一个技术要素，先总结出该要素应该具备的技术特征。随后根据技术要求，提炼出同行评估的管理行动，该管理行动提出了同行评估小组成员在对该技术要素需审查的重点内容。最后是该技术要素是否满足技术要求的评估标准。

附表 B1 电厂运行状态分析

技术特征	同行评估行动	技术评定准则
实施程序（POS1）	审查电厂运行状态分析对应的实施程序。	应采用业界通用的方法指导电厂运行状态分析，包括 POS 划分的原则、方法、实施过程；可用于后续的升版和更新。
电厂运行状态确定（POS2）	审查 LPSD 进程确定的方法和依据，确保 LPSD 进程的确定是合理的。	应确定一组典型的、要模化的 LPSD 进程（低功率和停堆进程或停堆类型，包括换料停堆、排水的维修停堆、不排水的维修停堆、热停堆）。LPSD 进程的确定应参考特定电厂文档和记录，如技术规格书、停堆、换料和启动的各种规程、近期停堆计划、大修总结报告或大修里程碑划分资料和记录等，LPSD 进程应代表满功率 PSA 所没有覆盖的所有电厂状态。 对于设计阶段或在建阶段核电厂，在条件不具备时，可根据其参考电厂或设计上最接近的核电厂的运行信息，确定其 LPSD 进程。
	审查 POS 划分依据。	POS 划分应参考 LPSD 进程的结果，结合技术规格书、反应堆冷却剂系统组态、反应堆冷却剂系统参数等来确定。
	审查 POS 划分结果。	POS 划分应包含电厂已遇到和可能遇到的运行状态，所有 POS 的组合应覆盖停堆或特定停堆进程。可通过与电厂合适人员访谈的方式确定是否有潜在的 POS 被遗漏。反应堆水池满水时，堆芯损坏的风险很小，可不做定量分析。
电厂运行状态分组（POS3）	审查 POS 分组依据和结果是否满足要求的准则。	LPSD 归并过程和 POS 的最终定义应确保归并成的组选择了最不利或最有约束性的特征（对堆芯损坏或大量放射性释放而言）。 该过程应考虑始发事件的类型和频率。对 POS 分组应同时满足以下两条准则： 1） 这些 POS 在电厂响应、成功准则、对操作的影响以及对操纵员行为和相关缓解系统的影响等方面是相似的； 2） POS 归并为一组且该 POS 组被“新”组内的最不利的 POS 所包络，此时，应保证不会由于 POS 归并而影响组内各 POS 对 CDF 的重要贡献项。
	审查不同成功准则或更严重后果的 POS 分组。	具有不同电厂响应或更严重后果的 POS 通常应独立分组，如 MID-LOOP 工况。如不独立分组，则应采用最不利的特征进行包络分析，但不应对总体结果有明显的影响。

确定每个 POS 组的持续时间及参数特征（POS4）	审查 POS 组持续时间的统计。	各 POS 持续时间统计应参考特定电厂记录，如停堆计划、主控室日志或大修总结报告等。应选取一系列典型的、连续的停堆进程时间记录来统计各 POS 持续时间。 将组内各 POS 的持续时间之和作为该 POS 组的持续时间，如果某 POS 在一年内多次进入，则持续时间需累计。 对于设计阶段或在建阶段核电厂，在条件不具备时，可根据参考核电厂或设计最相似核电厂的记录信息进行分析。
	审查各 POS 组的参数特征。	每个 POS 组的特征应包含对安全功能的实现有不同影响的参数，可包括一回路温度、压力、水位、开口状况等。
文档记录（POS5）	审查电厂运行状态分析的文档。	电厂运行状态分析的文档应保证其分析是可追溯的。 至少应包括技术标准 SR-POS-D2 所包含的内容，主要包括 POS 清单的确定过程、POS 分组的过程和准则、POS 组持续时间的统计等。

附表 B2 始发事件分析

技术特征	同行评估行动	技术评定准则
实施程序（IE1）	审查始发事件分析实施程序。	始发事件分析实施程序对分析过程的描述应足够详细，以作为后续更新和修订的指导文件。该实施程序应该为进行始发事件分析提供合理基础，并且应与经验证的方法保持一致。实施程序的详细程度应足以支持获得等同的结果。
识别始发事件（IE2）	检查始发事件识别的方法，确保所采用的方法能够满足尽可能完整地找出始发事件清单的需要，并符合工业界的良好实践。	应结合不同的堆型和不同的阶段合理选用分析方法，尽可能全面地综合使用多种方法，并应对分析的完整性进行论证。
	审查始发事件清单，并与类似机组 PSA 中确认的始发事件进行比较。	始发事件清单至少包括了下列通用的始发事件： 1） 瞬态：在瞬态这一类别中包含由设备和人员导致的扰乱电厂正常运行、但一回路系统压力边界不发生变化的事件（即完整或开口）； 2） LOCA：在 LOCA 这一类别中包含由设备和人员导致的使反应堆冷却剂装量损失从而扰乱电厂正常运行的事件。采用事先定义的基本原则区分 LOCA 始发事件，LOCA 的实例包括： a) 小 LOCA：例如反应堆冷却剂泵轴封 LOCA，管道的小破裂； b) 中 LOCA：例如管道的较大破裂； c) 大 LOCA：例如主回路管道双端剪切断裂； d) 过大的 LOCA（由任意组合的专设安全设施都不能缓解的 LOCA）：例如反应堆压力容器破裂； e) 安全壳外 LOCA； f) 流量转移过程中引起的 LOCA； g) 典型连接系统上的 LOCA； h) 维修引起的 LOCA。 3） 界面 LOCA：包括与反应堆冷却剂系统接口的系统中因能动设备（即需要改变状态的设备）失效或者以某种方式运行而导致反应堆冷却剂失控流失到安全壳

技术特征	同行评估行动	技术评定准则
		外的假想事件； 4） SGTR； 5） 特殊始发事件：例如一回路低温超压等； 6） 反应性事件：例如，引入非硼水，误装燃料组件； 7） 其他始发事件：例如支持系统故障，仪表管破裂。 还应包括类似机组 PSA 中确认的始发事件，如果排除，则应记录其根据。
	审查是否考虑了受评核电厂或者类似核电厂的运行经验。	对受评核电厂或者类似核电厂的运行进行了收集、筛选和分析，并有分析记录文件。
	在各 POS 下，检查可能由某列失效或某个系统失效引发的始发事件，并确认是否采用了结构化的方法。审查每个系统及其支持系统的接入状态，这会因其故障导致的始发事件的可能性和严重程度。	FMEA 分析是满足要求的一种方法，如果采用，应有分析记录文件。
	审查是否考虑各 POS 下人因导致的始发事件。	应通过分析运行规程和实践识别人因导致的始发事件。
	审查是否考虑低功率和停堆工况下特定的始发事件。	应结合低功率和停堆工况特点，识别特定的始发事件，如一回路低温超压事件等。
对始发事件进行归并和分组（IE3）	审查始发事件归分组文件。	应详细说明各始发事件是如何归并成为最终的始发事件类别。
	确认始发事件分组是否与 POS 分组相协调。	不同 POS 下，相同的始发事件组在电厂响应、成功准则、时间进程、和对操纵员和相关缓解系统的可运行性及性能存在差异，应确保始发事件分组与 POS 分组相协调。
	确认分组不会影响重要事故序列。	为了避免过度保守，应避免将后果严重得多但发生频率小很多的事件与其他事件归并在一组。 应避免进行非保守性分组，即把某些始发事件归并到一组而不以最严重事故作为包

技术特征	同行评估行动	技术评定准则
		络条件。
	审查可能导致更严重的放射性核素释放的事件的分组。	这些事件应分别单独作为一个事件组，这些事件包括压力容器破裂、界面系统 LOCA 和蒸汽发生器传热管破裂等。
估算每个始发事件或始发事件组的年发生频率（IE4）	审查始发事件发生频率确定原则。	对于由于系统故障导致的始发事件（例如界面系统 LOCA、支持系统故障导致的始发事件），可采用故障树方法进行分析； 与厂址条件密切相关的始发事件，应进行专项分析； 瞬态等比较常发的始发事件，应采集电厂特定数据； 某些始发事件发生的可能性在不同 POS 下存在较大的差异，若采用按照时间份额推算频率的方法，应证明其合理性。
	审查电厂运行经验数据的收集和处理报告。	如果有足够可用的数据，始发事件频率可根据电厂特定数据计算，否则采用贝叶斯方法或等价的统计方法。始发事件的频率应该使用最新的可用数据。可剔除商业运行后第 1 年的数据，但应有合理的论证。
	如果对于支持系统故障导致的始发事件建立了故障树进行分析，审查始发事件故障树方法，检查始发事件故障树和定量化过程与结果。	每一个最小割集都是由一个部件的年故障频率事件与其他部件的不可用概率事件组成（单阶割集除外），其他部件的不可用概率事件应使用合理的任务时间，例如采用技术规格书的 AOT、第一个部件故障的平均修复时间。应考虑重要部件的共因故障。
	审查是否以堆年为基准计算始发事件频率。	对于每个 POS，应考虑电厂在每个 POS 的时间份额，使始发事件频率用电厂处在该 POS 的时间份额进行加权。
	将各始发事件发生频率与类似机组或国际上公认的通用数据进行比较。	如果与类似机组或者通用数据的发生频率有较大差异，则需有合理的解释。
文档记录（IE5）	审查始发事件分析的文档。	始发事件分析的文档应保证其分析是可追溯的，包括： 1） 始发事件清单的确定过程； 2） 电厂始发事件数据的收集与甄别； 3） 始发事件分组的依据； **4）** 始发事件发生频率的分析过程。

附表 B3 事件序列分析

技术特征	同行评估行动	技术评定准则
实施程序（ES1）	审查事件序列分析实施程序或导则。	实施程序或导则对事件序列分析过程的描述足够为以后的升版和修订提供指导；应与业界认可的方法保持一致，并为事件序列分析提供合理的依据；导则的详细程度应足够获得等同的结果。
事件序列评估（ES2）	审查事件树是否反映了始发事件分组。	事件树应反映始发事件组及其对电厂响应的潜在影响，不同始发事件的电厂响应都应模化，包括时间、系统成功准则和操纵员动作，特别是 LPSD 时，人因导致的始发事件与恢复事件间的相关性的影响。
	审查事件序列分析及模型是否与电厂实际状态相一致。	证实模型与分析与电厂实际状态是一致的，系统分析和相关性评估将在建模过程中提供相应输入。
	审查典型的事件序列模化是否正确。	模型应包含所必需的关键安全功能，并完成定量化模型，如有例外情况需加以说明。每个功能中所有相关的系统均应在模型中考虑。 事件树结构应恰当描绘规程中关键的操纵员动作及对关键安全功能的影响。 对于所模化的可能引起堆芯损坏的每个始发事件，应建立一套合理完整的事件序列。 应正确定义并现实地处理成功路径。
	审查事件树之间的分支转移是否正确。	事件树之间的转移应明确定义并作相应的定量或定性处理。 事件树之间的转移应保留相关性，包括功能、系统、始发事件、操纵员、以及空间或环境的相关性。 为避免在转移过程中遗漏信息，定量化模型中应单独处理事件树之间的转移并编制文档。
	审查事件树题头之间的相关性。	应识别和处理题头之间的相关性，包括功能、系统内及系统间、操纵员动作、空间/环境、始发事件和后续的恢复事件之间的相关性。 相关性处理方法应编制文档，并与题头之间相关性处理相一致；应现实地处理相关性。 定量化模型中应合理定义明显具有时间相关特征的失效模式及可能的恢复，例如，

技术特征	同行评估行动	技术评定准则
		SBO 情景下电池容量及交流电源恢复。
	审查是否正确模化系统/设备的维修和恢复。	PSA 模型中包含的维修和恢复应基于适用的数据或可接受的模型，并考虑事件序列的相关性，例如，可用时间，不利环境，及缺少通道、照明或房间冷却。
与运行规程的接口（ES3）	审查事件树功能和结构是否反映异常和事故规程。	事件树功能和结构应与异常和事故规程相一致。规程引导的操纵员动作，如果显著影响事件序列进程或失效概率，则应在相应的事件序列结构或故障树分析中加以考虑。
事件序列终态（ES4）	审查事件序列终态。	一级 PSA 终态应明确定义为堆芯损坏或安全稳定状态。堆芯损坏的定义与成功准则中的考虑要一致，堆芯损坏基于 24 小时或其它证明是适当的任务时间。
文档（ES5）	审查建立事件树结构的依据文档。	对于特定电厂的或通用的分析应是可追溯的。建立的文档应包括事件树图，文字描述，相关性矩阵。 要求文档能提供满足上述准则的依据，反映建树过程。

附表 B4 成功准则分析

技术特征	同行评估行动	技术评定准则
实施程序（SC1）	审查成功准则及热工水力计算分析的实施程序。	应详细描述成功准则分析过程，使其可作为后续升版和更新工作的指南，所采用的分析方法应符合行业标准相应的要求。
成功准则定义（SC2）	审查关键安全功能成功准则的定义。	应识别关键安全功能的成功准则并编制文档，关键安全功能应有相应的技术依据以支持 PSA。
	审查堆芯损坏的定义。	一级 PSA 终态应明确定义为堆芯损坏或安全稳定状态。堆芯损坏定义应与 NB/T 20037.2 中的定义相一致。对于压水堆核电厂堆芯损坏定义如下： 1） 堆芯塌陷水位长期低于燃料活性区顶部；或 2） 详细堆芯模型分析堆芯燃料包壳表面峰值节点温度>1204℃；或 3） 简化堆芯模型分析堆芯燃料包壳表面峰值节点温度>982℃；或 4） 简化堆芯模型分析堆芯出口热电偶温度>650℃。
	审查成功准则对应任务时间。	对于已经达到稳定状态的序列，一般可采用最短 24 小时的任务时间；如果 24 小时仍不能达到稳定状态，则应认定该序列为电厂损伤状态或采用适当方法加以评估。
	审查构筑物、系统、部件及人员动作的成功准则。	应按照事件序列分析要求对每个模化的始发事件给出为防止堆芯损坏所需要的构筑物、系统、部件及人员动作的成功准则，对于 LPSD 特别要注意这些成功准则是否适用于相应 POS 定义和特征，并且这些成功准则应与电厂竣工和实际运行的特征、规程和运行原则相一致以及考虑正在减少的衰变热影响。
成功准则确定与依据（SC3）	审查成功准则的依据，包括 审查确定系统/部件、事件序列及人员动作的成功准则的依据等。	成功准则可基于 POS 的定义和特征以及现实的热工水力分析，或确定论安全分析结果以及参考电厂的分析结果。用于不同始发事件组和相应事件树中的成功准则应体现始发事件及事件序列发展对系统失效的影响。如果采用保守的包络分析，应对最终结果不产生明显影响。
		采用合理现实的、通用的或特定电厂的热工水力计算分析来确定系统、事件序列及人员动作可用时间的成功准则。支持成功准则的依据应足以进行模型定量化，即运用热工水力或其它适用的分析/评估应考虑到与始发事件（组）和事件序列模

技术特征	同行评估行动	技术评定准则
		化相一致的详细程度。
	审查热工水力计算程序模型的适用性和结果的合理性。	热工水力分析模型和计算机程序应有能力建模确定出所考虑工况的成功准则，可使用类似电厂中使用过的热工水力程序、模型或分析来进行定性评价。 当条件允许时，应与类似电厂分析结果进行比较并考虑电厂特征的差异，或与其它电厂特有程序的相似分析的结果进行比较，如果与类似机组情况有较大差异，则需有合理的解释。
	审查建立成功准则过程中的关键假设和不确定性的来源，以及一些专家判断的合理性。	应与 PSA 标准及业界的作法相一致；只有在缺乏关于所模化的 SSC 状态或响应的可用信息，或者缺乏作为预计 SSC 状态或响应依据的分析方法情况下才使用专家判断，其他情况不使用专家判断。使用专家判断时应给出相应的使用原则，并且满足 NB/T 20037.2 相应要求。
文档（SC4）	审查支持成功准则的依据的文档。	文档应包括特定电厂的、或通用的热工水力分析，要求足以支持成功准则的确定，并且是经过有丰富经验人员独立审查过的。 文档应当给出满足上述成功准则定义和成功准则依据的技术准则要求，文档描述的结果与过程相一致。 文档应包括成功准则确定过程中用到的保守的、简化的假设条件和特定的判断。

附表 B5 系统分析

技术特征	同行评估行动	技术评定准则
实施程序（SY1）	审查系统分析实施程序。	实施程序应对系统分析的输入、分析方法和步骤、简化原则和基本假设的确定、设备失效的考虑、相关性的处理、共因失效的处理、人员失误的处理、试验维修不可用的处理、建造故障树的原则和步骤、定性和定量分析的要求和文档的编制等做出规定。 实施程序的详细程度应能够指导系统分析人员进行并规范系统分析工作。
系统分析模型（SY2）	审查系统分析模型，确保事件序列分析中与安全功能相关的所有系统建立系统分析模型。	应对所有的前沿系统和支持系统建立详细的系统分析模型，以下情形可以不建立详细的系统分析模型： 1) 在不具备建立详细模型的情况下可以采用系统级的数据，但要说明对系统分析结果的影响； 2) 系统失效的主要贡献是操纵员动作，并且省略建模不会掩盖对支持系统或其他相关性失效模式的贡献。
	审查系统成功运行所需设备的清单。	对系统成功运行有重要影响的设备应包含在清单内，应与系统分析的简化原则和基本假设保持一致，须绘制系统分析简化流程图。
	审查系统模型是否反映所有不同成功准则的系统构成。	应根据不同的成功准则建立系统分析模型，或通过设置边界条件使得系统分析模型能够在不同的边界条件取值下反映不同的成功准则。 应反映如下情况带来的成功准则的不同：不同的事故情景、与其他部件的相关性、两个机组共用情况。
	审查系统模型中包含的影响系统可运行性（由系统成功准则确定）的设备。	应包括能动部件（例如，泵、阀门和空气压缩机）、非能动部件（例如，热交换器和水箱）和系统特定设备。只有满足 NB/T 20037.2 中 SY-A13 的准则时，才可不包含这一设备。 设备的边界应与建立设备失效数据所用的定义相一致。

技术特征	同行评估行动	技术评定准则
	审查设备失效包含的失效模式。	应考虑对设备失效有重要影响的失效模式。 应考虑设备的状态，避免考虑在某种状态下不可能发生的失效模式。 应与采用的数据和模型的详细程度相一致，只有满足 NB/T 20037.2 中 SY-A13 的准则时，才可不包括该设备的这些失效模式。 应考虑系统或设备在不同 POS 的可用性。系统或设备在不同 POS 下，启动信号、空气、冷却或其他设施可能不同。
	审查人员失误事件。	应包含会导致系统或设备在需求时不可用的人员失误事件（始发事件前人员失误事件）；应包含在系统或设备的运行中预期出现的人员失误事件或在事故序列的最终定量化时考虑的人员失误事件（始发事件后人员失误事件），除非在事故序列模型中已经明确包含了这些人员失误事件。
	审查互斥事件组。	应对互斥事件组进行处理，避免同时考虑互斥事件组中的事件，如开关的拒开和拒关。
	审查设备退出服务的不可用事件，并确保对不可用事件的影响进行了合理的处理。	应包括：当一个设备或系统系列因试验造成设备不可用无法执行其安全功能；当规程要求隔离整个系列进行维修时的系统级维修事件；在规程指导下的子系列级（即，在作标记的边界之间，例如一个功能设备组）的维修事件。 一般来说，冗余系统的不同系列的维修是互斥的，应合理处理。
共因失效和系统相关性（SY3）	抽查系统内共因失效，确保对系统内共因失效进行了完整地处理。	应对系统内的共因失效进行建模；应采用一种逻辑化、系统化的方法建立共因失效组；应合理的选择共因失效组；共因失效的候选设备应包括 SY-B3 规定的设备；共因失效模型应与数据分析的共因模型相一致。
	抽查与支持系统或接口系统的相关性。	应考虑系统与支持系统或接口系统的相关性，可通过故障树连接或事件树连接的方法。 应考虑要求的任务时间内系统成功运行所需的所有支持系统。 应考虑启动和触发一个系统所要求的系统。
系统分析定量化（SY4）	以足够低的截断值定量化系统分析模型。	选取的截断值应足够低，以避免将对系统失效有较大贡献的割集截断。

技术特征	同行评估行动	技术评定准则
	对用于支持不同成功准则的系统分析模型进行顶事件失效概率计算，并确定支配性最小割集。	应对所有的顶事件或用于支持相关系统的接口顶事件进行失效概率计算，并确定导致这些顶事件发生的支配性最小割集。
	对系统分析模型进行重要度分析。	应对系统分析模型进行重要度分析，并确定对系统失效具有重要贡献的事件、设备、人员动作等。
文档记录（SY5）	审查系统分析文档的内容。	文档应提供系统建模的依据，保证其分析是可追溯的。 1）应包含对系统功能和边界、相关的成功准则、模化的设备和包括人员动作在内的失效模式以及包括支持系统和共因失效在内的相关性模型的描述； 2）应包括对系统分析有关的假设产生的模型不确性来源的描述； 3）应包括对系统定量化分析结果的描述，包括顶事件失效概率、支配性最小割集、不确定性分析结果、重要度列表、敏感性分析结果等。

附表 B6 人员可靠性分析

技术特征	同行评估行动	技术评定准则
实施程序（HR1）	审查人员可靠性分析实施程序。	实施程序应对人员可靠性分析过程有详细的描述，便于作为今后更新和升版的指导；实施程序应为开展 HRA 给出合理的技术基础，并与公认的方法保持一致。 实施程序内容应足够详细，以获得等同的分析结果。
事故前人员动作（HR2）	确认在 PSA 中考虑了事故前人员动作。	应在 PSA 中明确包含事故前人员失误事件，特别是会导致多个冗余部件失效的潜在失误。 应包括对基准 CDF 可能存在不利影响的事故前人员动作，例如： 1） 未能恢复设备至所期望的备用或运行状态； 2） 未能恢复使设备启动或重新接入的启动信号或设定值； 3） 未能恢复自动重新接入或供电。
	审查事故前人员失误的识别方法。	应采用系统化的方法来识别 PSA 中包含的事故前人员失误，应包括对电厂规程、培训和 LPSD 运行事件的审查以识别可能导致多个冗余部件失效的潜在失误。
	审查在对事故前人员动作的 HEP 定量化过程。	下列情况下可筛选掉事故前 HEP 而不必作进一步考虑： 1） 有设备状态监视； 2） 设备能自动复位； 3） 要求经常检查设备的状态（每个运行值至少一次）； 4） 执行维修后功能试验； 5） 存在有效的行政隔离手段确保设备状态。 在对有支配性贡献的事故前 HEP 定量化时应采用最佳估算 HEP，包括恢复因子的考虑。其余的事故前 HEP 可采用筛选值。
事故后人员动作（HR3）	审查事故后人员动作的识别方法。	应包含预防和缓解系统的触发、控制、隔离和投入相关人员动作的 HEP。应采用系统化的方法识别 PSA 中包含的事故后人员失误，该方法应考虑人员动作的复杂性、完成动作的可用时间和所需时间、由事故情景导致的紧张程度影响等各方面因素。
	确认事故后人员动作分析是否与 POS 分	不同 POS 下，相同的人员动作在完成动作的可用时间和所需时间、由事故情景导

技术特征	同行评估行动	技术评定准则
	组相协调。	致的紧张程度等方面存在差异。
	审查 HRA 中对电厂规程和特定运行经验的评价。	在人员动作的识别和定量化时应明确包含对电厂规程和特定运行经验的评价。在评价时应包含对操纵员、培训人员或值长的访谈，并形成访谈记录。
	审查事故后人员动作详细评价方法的适用性。	应采用业界通用的适用于低功率和停堆工况下的人员动作详细评价方法。
	审查事故后人员动作的 HEP 定量化过程。	HEP 值应为 PSA 提供相对准确的失误概率，应尽量减少筛选 HEP 的使用。特别在对 CDF 的主要贡献因素进行定量化时不应采用筛选 HEP，而应采用最佳估算 HEP。
	审查运行人员对操纵员动作的反馈。	运行人员应至少对支配性操纵员动作进行审查，并且其输入已包含在 HRA 评价中。并且，HRA 的假设和判断应与操纵员培训和规程相一致。应让运行人员对 HRA 计算内容进行审查，特别是分析中所作的假设。
	审查人员动作是否正确结合到模型中，及其模化的合理性。	在计算 HEP 时应正确体现所模化的事件序列的规程、培训和模拟机响应。在模型中应包含 HEP 来表示那些特定序列的动作。
	审查定量化中相关的绩效形成因子的模化。	定量化时应模化表示特定事件序列和相关 HEP 的绩效形成因子，包括可用时间、执行时间、紧张程度、复杂度、可用的指示、资源限制等。 总的 HEP 应包含诊断、操作等贡献因素的评价。
	审查动作的可用时间获取的合理性。	动作的可用时间应基于电厂特定的热工水力分析或考虑了电厂特性的通用分析。应识别提示操纵员动作的信号发出时间。
	审查完成动作所需的时间来源和依据。	完成动作所需的时间应基于观测或运行人员的访谈。
	审查恢复动作模化的合理性。	如果考虑恢复动作，则应满足以下条件： a) 有可用的规程，并且已在所有操纵员的培训中针对这类动作进行过培训； b) 有提醒操纵员采取恢复动作的“提示”，例如警报； c) 有充足的人力来执行该动作。 应考虑恢复动作与动作所涉及的序列、情景或最小割集中其他 HFE 之间的相关性。
人员动作间的相关性（HR4）	审查人员动作之间的相关性和模型的充分性。	在 PSA 中应评价人员动作之间的相关性。相关性的分析应考虑： 1) 完成所有动作所需的时间与执行这些动作的可用时间的关系；

技术特征	同行评估行动	技术评定准则
		2) 可能引起相关性的因素，例如，公共的仪表，公用的规程，紧张程度加大，等等； 3) 资源的可用性，例如，人员。 在检验模型的充分性时，除了恢复动作中很低的人员失误概率，应当对可能成为堆芯损坏频率支配性贡献的序列进行识别。
文档记录（HR5）	审查人员可靠性分析文档。	将识别、表征、量化始发事件前/始发事件后人员失误事件以及恢复动作的过程形成文档，包括输入、方法和结果，确保分析的可追溯性。例如，该文档通常包括： 1） 用于确定始发事件前/后人员失误概率的 HRA 方法和过程； 2） 定性筛选规则和筛选结果； 3） 用于量化人员动作的因素，以及如何将其考虑到量化过程中； 4） 人员失误概率的定量化，包括： a） 筛选值及其依据； b） 详细的人员失误概率分析； c） 始发事件后人员动作的相关性的分析方法及处理； d） 模型、系统、始发事件和功能评价中的始发事件前和始发事件后的人员动作列表； e） 恢复动作的人员失误概率及其与其他 HEP 的相关性。

附表 B7 数据分析

技术特征	同行评估行动	技术评定准则
实施程序（DA1）	审查数据分析实施程序。	数据分析实施程序对分析过程的描述应足够详细，以作为后续更新和修订的指导文件。该实施程序应该为进行始发事件分析提供合理基础，并且应与经验证的方法保持一致。
通用数据源（DA2）	检查所选取的通用数据源，包括公开的通用数据源和设备生产厂家专用数据源。	应使用业界所公认的通用数据源，例如： **1)** 设备失效数据：NUREG/CR-4550、NUREG/CR-6928； 2) 共因失效参数：NUREG/CR-5497。 对于通用数据源未包括的设备，可采用厂家专用数据作为通用数据。 对数据的选取应该做出分析与评价。
设备边界划分和归类（DA3）	检查设备边界划分。	设备边界划分应与所选用的通用数据或厂家专用数据以及与“系统分析”要素中对设备失效模式的模化相一致。 应有设备边界划分的详细记录。
	检查设备分类文件和设备清单。	在对设备进行归类时，考虑了以下因素： 1) 任务类型 2) 工作条件 设备样本空间应涵盖 PSA 所模化的所有设备。 每一个 PSA 所模化的设备应归类到一个设备类中。 应有设备样本空间选取和归类的详细记录。
电厂特定数据的采集（DA4）	抽查电厂数据采集报告。	应采集自商运以来的电厂特定数据。对于新建核电厂，可采用类似设计核电厂的数据，或者使用通用数据。 如果对某一时间段的数据进行筛选，则应有合理的筛选理由，经论证后的电厂设计改造、运行实践变化导致原有数据不适用是可接受的理由。 设备需求次数和运行时间应来自电厂实际的试验、维修、运行记录。对于记录不完整的情况，可根据电厂试验、维修、运行等规程估计需求次数和运行时间。 设备失效数据应尽可能完整地收集来自电厂的实际记录。

技术特征	同行评估行动	技术评定准则
		如果设备降级在所考虑的任务时间内不影响 PSA 模化的安全功能，则不应计为失效，否则应计入。对不计为失效的设备降级，应有筛除记录。
	抽查不可用度采集和处理报告。	系统、列、设备不可用度的采集应基于电厂特定数据。对于新建核电厂，可采用类似设计核电厂的数据，或者采用设计文件数据。 不可用时间应来自电厂实际的试验、维修等记录。 对于定期试验，如果试验期间有自动信号恢复其可用，则不应计入试验维修不可用。 支持系统的不可用应单独计入到支持系统的不可用度。 能够导致冗余设备不可用的事件应单独统计和处理。 应考虑 LPSD POS 和特殊的维修活动的影响。
电厂特定的参数估计（DA5）	检查电厂特定数据处理过程报告。	如果有充分的电厂特定数据，根据电厂特定数据来计算重要基本事件的参数值和不确定性参数。 如果没有足够的电厂特定数据，则在相关通用的和电厂特定的统计证据基础上计算它们的参数估计值，贝叶斯更新方法是一种可接受的处理方法。 可以只对重要的基本事件来估计电厂特定的参数，其余事件可采用通用数据。 应给出参数估计值的不确定性分布参数。 对于新建核电厂，可采用参考核电厂数据或其他核电厂同类型设备的数据。对于独特设备，可采用设计文件数据或者通用数据。
共因失效参数（DA6）	检查共因失效参数报告。	对共因失效参数的确定方法做出说明与评价。 共因失效参数应与模型中采用的共因失效模型相一致。 可以采用工业界公认的共因失效通用数据。
文档记录（DA7）	审查数据分析文档。	数据分析的文档应保证其分析是可追溯的，包括： 1) 通用数据源的确定过程； 2) 设备边界划分和归类； 3) 电厂特定数据的采集，包括维修和失效事件的甄别、需求和运行时间、不可用

技术特征	同行评估行动	技术评定准则
		时间等； 4) 电厂特定参数的估计方法、过程与结果； 5) 共因失效参数的选取。

附表 B8 相关性分析

技术特征	同行评估行动	技术评定准则
实施程序（DF1）	审查相关性分析实施程序。	实施程序对相关性分析有定义清晰，识别出重要的相关性，描述了这些相关性的分析方法。
功能和实体相关性(DF2)	检查事件序列和系统故障树分析模型，安全功能的定义和划分结果。	全面考虑设计方面的相关性。 事件序列分析中体现功能之间的相关性，安全功能的定义应清晰明确，符合工业界的良好实践；且在事件序列中正确反映。功能相关性的特殊假设和限制条件应记录于分析文件之中 应模化支持系统，并通过适当的转移门链接至系统模型中。 系统范围有明确的定义，对于不同系统间的共用部件的同一失效模式，应有确定且唯一的编码，并在故障树中分别给予模化。 使用系统相关性矩阵记录功能相关性。
人员可靠性相关性（DF3）	审查始发事件前人员失误相关性的考虑。	始发事件前人员失误事件之间的相关性应该体现在系统模型中，包括维修、试验、标定情况导致的相关性。
	审查系统局部失效的情况下（如丧失一列设备冷却水系统，由于切换失败导致失效）人员失误相关性。	操纵员实施应急操作规程可能出现的相关性应在系统建模中处理。
	审查安全功能和人员失误相关性的考虑。	功能或系统对操纵员干预的相关性应在事件序列和系统模型中模化。
	审查事件序列和系统建模中考虑的人员失误事件相关性。	同一个最小割集中的多个人员失误事件之间应该考虑相关性，相关人员失误事件的赋值应做适当调整。
设备环境恶化导致的相关性(DF4)	审查有关管道破裂，可能导致二次效应以及可能导致相关安全设备失效的场景的考虑，确认设备环境恶化导致的相关性。	考虑管道破裂或容器破裂等情况导致的管道甩动、飞射物、水/蒸汽喷射冲击。
		考虑湿度或温度上升导致的一些后果。
		考虑保温层材料脱落阻塞再循环流动（LOCA 事故后）。
共因始发事件(DF5)	审查对共因始发事件的模化，共因始发	应识别出由于共因导致的始发事件，如控制和保护系统、电源系统、重要厂用水

技术特征	同行评估行动	技术评定准则
	事件（CCI）是指导致瞬态（或者需要手动停堆）的事件，且事件发生后所需的一个或者多个安全功能同时降级。	系统或者其他支持系统的失效，并在模型中正确模化。在模化中应考虑始发事件导致的安全功能降级或失效。
部件共因故障分析(DF6)	审查事件序列和故障分析中对部件共因失效的考虑。	共因故障的定义清晰。 正确识别了共因故障，确定共因事件组。 共因失效分析方法是国际上通用并符合工业界的良好实践。 在模型中体现共因故障。 采用国际上比较通用的共因数据源，共因故障的分析应达到共因失效数据所能支持的程度。
文档记录(DF7)	审查相关性分析的文档记录。	文档记录应清晰、准确，可追溯。

附表 B9 模型整合与定量化（MQ）

技术特征	同行评估行动	技术评定准则
实施程序（MQ1）	审查模型整合及定量化分析的实施程序。	实施程序应对定量化所采用的分析软件版本及特性、模型整合流程、定量化计算过程中软件参数的设置、边界条件的设置、逻辑环路的处理等给出说明，并说明最小割集计算、不确定性、重要度、敏感性分析的原理及分析步骤。 实施程序的详细程度应能够使从业人员进行并规范模型整合与定量化工作。
PSA 模型整合（MQ2）	审查所有的系统模型和事件序列分析模型到 PSA 模型中的整合。	在整合的 PSA 模型中应包含 PSA 分析中所考虑的所有始发事件及对应的事件树和故障树模型，并包括所考虑的转移事件树模型。
	结合模型及报告中的事件树题头及成功准则表，审查事件树题头与对应故障树的输入链接的正确性。	应确保故障树的逻辑满足对应事件树题头的成功准则要求。
	审查 PSA 中包含定量化计算过程所需的边界条件的设置。	应在 PSA 模型中正确设置边界条件，并有文档记录。
	审查逻辑环路的合理处理。	模型中如果存在逻辑环路，则应通过合适的、可解释的，且不会对定量化结果产生重要影响的方式进行处理（断开逻辑循环的方法可参见 NUREG/CR-2728）。应有文档记录。
堆芯损坏频率的定量计算（MQ3）	审查每一个始发事件组的定量化，检查得到的事件序列频率。	对于导致堆芯损坏（CD）总的 CDF 及各始发事件类导致堆芯损坏的 CDF 进行计算，并给出其对应的评价结果。
	审查模型的正确性和评价结果的合理性。	对支配性序列的结果进行检查，可以参考国内外同类型电厂的分析结果以确认整合的 PSA 模型的正确性和结果的合理性。
	审查恢复动作的处理。	为了避免不必要的过分保守，在模型中可考虑适当的恢复动作。在报告中对于所考虑的恢复动作给予说明，并且以适当的形式给出恢复概率的计算过程与相关支持材料。
定量化软件及其使用（MQ4）	审查定量化软件的适用性。	申请者提交的模型所采用的 PSA 分析软件应是本行业被国内外广泛认可的专业分析软件；如果是有具备软件开发资格的单位开发的专业软件，则需要提交软件认证材料，及软件分析验证支持材料，以证明软件分析结果的正确性。

技术特征	同行评估行动	技术评定准则
	审查截断值的选取。	应综合考虑 CDF 计算结果的准确性及计算机运算速度，在分析中选取合适的截断值，以免忽略重要的最小割集或事故序列。
	审查系统成功的处理。	应当说明如何在 PSA 软件中对系统成功处理的设置，以实现对成功逻辑和概率的模化。
	审查互斥事件的处理。	应在分析中说明互斥事件的具体处理方法，一般来说可以通过下列两种方式之一进行修正： 1） 用逻辑模型消除互斥的情况； 2） 在结果中删除含有互斥事件的最小割集。
计算结果审查（MQ5）	抽样审查重要的（或支配性的）最小割集和序列。	支配性最小割集和序列的逻辑应合理，反映电厂的实际情况。有条件的情况下，可与相同类型的核电厂 PSA 分析结果对比，如果差异较大，则应给出合理解释。
	审查对 CDF 有重要贡献的事项。	定量化结果中应当分别论述对 CDF 产生重要贡献的项目，包括始发事件、事故序列、设备失效、共因故障及人误事件等。
不确定性分析（MQ6）	审查定量化结果的不确定性分析结果和不确定性的主要来源。	应说明不确定性的来源和定量计算的方法，并给出评价结果。
重要度分析（MQ7）	审查重要度分析方法及其分析结果。	应针对始发事件、设备失效基本事件、人误事件、共因失效等进行重要度分析，列表给出重要度较高的分析结果（至少给出 FV 及 RIF 重要度，或等价的重要度），并且应对重要度分析结果给出讨论与分析，解释其合理性，应保证重要度分析与敏感性分析在定性上是一致的。
敏感性分析（MQ8）	审查敏感性分析方法及其分析结果。	应针对始发事件、设备失效基本事件、人误事件、可靠性参数、共因事件等进行敏感性分析，说明敏感因子的取值，并列表给出敏感性分析结果，并且应对敏感性分析结果给出讨论与分析，解释其合理性，应保证重要度分析与敏感性分析在定性上是一致的。 对模型中重要假设进行敏感性分析。
	对重要度高，敏感性强的问题开展专题敏感性分析的审查，可进行实例校验。	应针对某些特定构模假设、特定数据等开展专题敏感性分析，以便进一步解释其合理性，并给出有益见解。

技术特征	同行评估行动	技术评定准则
文档记录（MQ9）	审查模型定量化的文档记录。	文档记录应清晰、准确，可追溯。

附表 B10 模型维护和升级

技术特征	同行评估行动	技术评定准则
模型维护和升级程序（MU1）	审查有关模型维护和升级的实施程序。	模型使用者应提供模型维护和升级的管理程序。 应详细描述采用的模型维护和升级的程序，且与工业界的普遍实践一致。
电厂运行经验、设计变更和改造信息的收集（MU2）	审查信息收集的过程和结果。	应建立了运行经验、设计变更和改造信息的收集渠道和程序。 收集信息的来源应包含以下几个方面： 运行经验、设计变更、新的维修策略、操作员培训程序、技术规格书、升版的工程计算结果、应急和异常处理规程、运行规程、应急计划，事故管理程序以及工业界的研究成果。
	审查电厂特定数据的收集情况。	应建立了相应的组织机构进行数据收集，并编制了数据采集导则，建立了电厂特定数据库。应定期收集和处理电厂数据，并按模型升级的周期更新数据。
模型版本控制（MU3）	审查 PSA 模型的版本控制情况。	PSA 模型应以有效地方式进行管理并处于受控状态，包括存储地点以及管理权限等。
计算机程序控制（MU4）	审查与模型相关的计算机程序的控制与管理。	计算机程序已经定型，PSA 模型的变更对于程序的影响已经得到充分的理解并适当的。
模型的升级（MU5）	审查模型的升级管理。	应制定模型升级的固定计划，间隔时间原则上不应超过 4 年。 应按计划定期对模型进行升级，对于需要升级的要求制定了合理的判断准则。 由于电厂设计或技术标准的重大变更造成的重要更新应及时升级。
	审查模型升级相关的过程和结果，PSA 模型需尽可能的与电厂的实际情况保持一致。	模型的升级过程应包括下列要素： 1）识别出影响模型的各个 PSA 要素； 2）修改 PSA 模型，评估结果； 3）针对 PSA 的各个要素已经建立了适当的实施程序。 模型升级过程应有详细的文档记录。
结果的评估（MU6）	审查对于升版后的模型进行评估的结果。	升级后的模型应由有经验的人进行内部审查和验证，使得升级后 PSA 模型的计算结果可靠。
文档记录（MU7）	检查对模型维护和升级过程的文档。	文档记录应清晰、准确、及时，可追溯。

15 附录 C 同行评估报告格式

1. 概率安全分析同行评估活动概述

1.1 目的和方法

1.2 范围

1.3 评估过程简介

1.4 同行评估对概率安全分析质量的技术评定

1.5 同行评估队资质要求

2. ×××电厂概率安全分析同行评估及回访概述（同行评估报告不包括“及回访”，同行评估回访时增加）

2.1 自评情况（若没有开展，可不包括）

2.2 电厂概述

2.3 评估前的准备

2.4 现场评估活动

2.5 评估回访（同行评估报告不包括本节，同行评估回访时增加）

3. PSA 要素评估意见

3.1 电厂运行状态分析

3.2 始发事件分析

3.3 事件序列分析

3.4 成功准则分析

3.5 系统分析

3.6 人员可靠性分析

3.7 数据分析

3.8 相关性分析

3.9 模型整合与定量化

3.10 模型维护与升级

4. 同行评估结论

4.1 技术评定结论

4.2 优势和创新

4.3 主要的发现

4.4 改进建议

5 评估回访结论（同行评估报告不包括本节，同行评估回访时增加）

5.1 评估回访总体结论

5.2 同行评估改进建议落实情况

附件 1 同行评估队成员简历（表 C1）

附件 2 事实观察表汇总（表 C2）

附件 3 各要素技术评定表（表 C3-1 至 C3-10）

表 C1 同行评估队简历

姓　　名		毕业院校	
所学专业		学位	
单位及部门		职务/职称	
核领域 工作经历			
PSA 工作 经历			
PSA 关键 领域专长			

表 C2 事实观察表

编号：	要素编码：	要素编号：
描述		
重要等级（注）：		
建议		
电厂反馈		
评估方签字：	受评方签字：	

注：重要等级划分原则为：

A：该问题非常重要，对 PSA 结果和风险见解会有重要影响，需要尽快解决，会影响 PSA 同行评估技术评定结论。

B：该问题比较重要，对 PSA 结果和风险见解会有比较重要影响，但可在下次更新或升级时解决。可能会影响 PSA 同行评估技术评定结论。

C：该问题基本不重要，对 PSA 结果和风险见解可能无影响或影响不重要。少量的问题不会影响同行评估技术评定结论。

S：超出预期期望和技术要求的高质量实践。

表 C3-1 技术要素评定表

要素名称：电厂运行状态划分（POS）
实施程序
电厂运行状态确定
电厂运行状态分组
确定每个 POS 组的持续时间及参数特征
文档/记录
改进建议
总体评价
评定结论 ☐满足技术要求　　☐基本满足技术要求 ☐部分满足技术要求　☐基本不满足技术要求 签字：

表 C3-2 技术要素评定表

要素名称：始发事件（IE）
实施程序
识别始发事件
对始发事件进行归并和分组
估算每个始发事件或始发事件组的年发生频率
文档记录
改进建议
总体评价
评定结论 ☐满足技术要求　　☐基本满足技术要求 ☐部分满足技术要求　☐基本不满足技术要求 评估员：

表 C3-3 技术要素评定表

要素名称：事件序列分析（ES）
实施程序
事件序列评估
与事故规程的接口
事件序列终态
文档
改进建议
总体评价
评定结论 ☐满足技术要求　　☐基本满足技术要求 ☐部分满足技术要求　☐基本不满足技术要求 评估员：

表 C3-4 技术要素评定表

要素名称：成功准则分析（SC）
实施程序
成功准则定义
成功准则确定与依据
文档
改进建议
总体评价
评定结论 ☐满足技术要求　　☐基本满足技术要求 ☐部分满足技术要求　☐基本不满足技术要求 评估员：

表 C3-5 技术要素评定表

要素名称：系统分析（SY）
实施程序
系统分析模型
共因失效和系统相关性
系统分析定量化
文档记录
改进建议
总体评价
评定结论 ☐满足技术要求　　☐基本满足技术要求 ☐部分满足技术要求　☐基本不满足技术要求 评估员：

表 C3-6 技术要素评定表

要素名称：人员可靠性分析（HR）
实施程序
事故前人员动作
事故后人员动作
人员动作间的相关性
文档记录
改进建议
总体评价
评定结论 ☐满足技术要求　　☐基本满足技术要求 ☐部分满足技术要求　☐基本不满足技术要求 评估员：

表 C3-7 技术要素评定表

要素名称：数据分析（DA）
实施程序
通用数据源
设备边界划分和归类
电厂特定数据的采集
电厂特定的参数估计
共因失效参数
文档记录
改进建议
总体评价
评定结论 ☐满足技术要求　　☐基本满足技术要求 ☐部分满足技术要求　☐基本不满足技术要求 评估员：

表 C3-8 技术要素评定表

要素名称：相关性分析（DF）
实施程序
功能和实体相关性
人员可靠性相关性
设备环境恶化导致的相关性
共因始发事件
部件共因故障分析
文档/记录
改进建议
总体评价
评定结论 ☐满足技术要求　　☐基本满足技术要求 ☐部分满足技术要求　☐基本不满足技术要求 评估员：

表 C3-9 技术要素评定表

要素名称：模型整合与定量化分析（MQ）
实施程序
PSA 模型整合
堆芯损坏频率的定量计算
定量化软件及其使用
计算结果审查
不确定性分析
重要度分析
敏感性分析
文档记录
改进建议
总体评价
评定结论 ☐满足技术要求　　☐基本满足技术要求 ☐部分满足技术要求　☐基本不满足技术要求 评估员：

表 C3-10 技术要素评定表

要素名称：模型维护与升级（MU）
模型维护和升级程序
电厂运行经验、设计变更和改造信息的收集
模型版本控制
计算机程序控制
模型的升级
结果的评估
文档记录
改进建议
总体评价
评定结论 ☐满足技术要求　　☐基本满足技术要求 ☐部分满足技术要求　☐基本不满足技术要求 评估员：

备注：

评定结论准则：

满足技术要求：没有 A 类的发现项, 且 B 类发现项不多于 2 个。可以有少量的 C 类发现项。

基本满足技术要求：没有 A 类的发现项，且 B 类发现项不多于 5 个。可以有少量的 C 类发现项。

部分满足技术要求：A 类发现项不多于 2 个，A、B 类发现项数量之和不超过 10 个。可以有部分 C 类发现项。

基本不满足技术要求：超过上述发现项数量。