ICS

附件 3

NB

中 华 人 民 共 和 国 能 源 行 业 标 准

NB/T 20037. 1—XXXX

应用于核电厂的一级概率安全评价 第 1 部分：总体要求

Level 1 Probabilistic safety assessment for nuclear power plant applications—

Part 1：General requirements

（报批稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家能源局　发 布

国 家 核 安 全 局　认 可

目　　次

前言 III
1 范围 1
2 术语和定义及缩略语 1
2.1 术语和定义 1
2.2 缩略语 13
3 一级 PSA 标准的框架和要求 14
3.1 标准框架 14
3.2 PSA 技术要求的组成结构 15
4 PSA 的应用过程 16
4.1 目的 16
4.2 识别应用案例和技术要求（A 阶段） 16
4.3 对 PSA 的必要范围、风险量和模型的评价（B 阶段） 17
4.4 应用过程的 SR 范围与详细程度的确定（C 阶段） 18
4.5 PSA 模型与标准的比较（D 阶段） 18
4.6 获得风险结论（E 阶段） 19
5 PSA 技术要求 21
5.1 目的 21
5.2 过程检查 21
5.3 专家判断的运用 22
5.4 PSA 要素的要求 22
6 PSA 状态控制 22
6.1 目的 22
6.2 PSA 状态控制程序 22
6.3 跟踪 PSA 输入并采集新信息 23
6.4 PSA 的维护和升级 23
6.5 待处理的变更 23
6.6 计算机程序的使用 23
6.7 文档 23
7 同行评估 23
7.1 概述 24
7.2 同行评估组的组成和人员资质 24
7.3 PSA 要素的评估 25
7.4 专家判断 25
7.5 PSA 状态控制 25

7.6 文档编制.....25
参考文献.....27

前　言

NB/T 20037《应用于核电厂的一级概率安全评价》分为以下12个部分:

——第1部分：总体要求；

——第2部分：功率运行内部事件；

——第3部分：功率运行内部水淹；

——第4部分：功率运行内部火灾；

——第5部分：功率运行地震；

——第6部分：功率运行其他外部事件的筛选和保守分析；

——第7部分：功率运行强风；

——第8部分：功率运行外部水淹；

——第9部分：功率运行其他外部灾害；

——第10部分：功率运行抗震裕度评价；

——第11部分：低功率和停堆工况内部事件；

——第12部分：低功率和停堆工况外部事件。

本部分为NB/T 20037的第1部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分主要参考ASME/ANS RA-Sa-2009和NUREG-2122进行编制。

本部分由能源行业核电标准化技术委员会提出。

本部分由核工业标准化研究所归口。

本部分起草单位:上海核工程研究设计院、苏州热工研究院有限公司、中国核电工程有限公司和中广核工程有限公司。

本部分主要起草人: 许以全、仇永萍、郭建兵、黄乾、孙金龙、喻新利、张冰、桑会娜。

本标准2016年8月30日，经国家核安全局审查认可。

应用于核电厂的一级概率安全评价
第1部分：总体要求

1 范围

本部分规定了一级概率安全评价（PSA）的总体要求，以保证针对压水堆核电厂开发满足质量要求的PSA模型。

本部分适用于压水堆核电厂设计、建造和运行阶段的一级PSA。其他堆型的核电厂可参照执行。

2 术语和定义及缩略语

2.1 术语和定义

下列术语和定义适用于本标准。

2.1.1

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。

2.1.2

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。

2.1.3

能动部件 active component

依靠触发、机械运动或动力源等外部输入而行使功能的部件。

2.1.4

随机不确定性 aleatory/random uncertainty

一种随机现象中固有的不确定性。该不确定性通过用概率模型模拟现象来反映。原则上，无法通过积累更多数据或附加信息来减小不确定性。

2.1.5

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。

2.1.6

基本事件 basic event

在故障树模型中，由于达到了合适的分解限度而不需要进一步展开的事件。

2.1.7

包络分析 bounding analysis

采用假设使评估结果等同或超过所有可能结果中最严重结果的分析。

2.1.8

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）。

2.1.9

同时热短路 concurrent hot short

两个或多个热短路在发生时间上是重迭的（如在前一个热短路自行缓解或由运行人员缓解前，第二个热短路已经发生）。

2.1.10

组态 configuration

电厂各种设备可用性状态的一种组合。

2.1.11

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。

2.1.12

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。

2.1.13

损坏准则 damage criteria

灾害对周围环境造成影响，判定导致目标物或目标物集合失效的条件。

2.1.14

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。

2.1.15

终态 end state

事件序列结束时的一组状态，它表征了事件序列对电厂或环境的影响。大多数一级PSA中，典型的终态包括：成功状态（即对电厂的影响可忽略的状态）和堆芯损坏状态。

2.1.16

认知不确定性 epistemic uncertainty

对现象认知不足的不确定性，从而影响现象的模化。认知不确定性反映在参数值的变动、实际模型的变化、模型详细程度、多种专家解释，以及统计学置信度。原则上，认知不确定性能够通过积累附加信息来减小。认知不确定性亦称为“建模不确定性”。

2.1.17

设备鉴定 equipment qualification

为证明设备在鉴定试验或试验与分析的条件下能够运行，形成数据和文件并维护。

2.1.18

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。

2.1.19

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表示事故的进程，并最终达到成功或失败的终态。

2.1.20

专家判断 expert judgment

由某一技术领域中的技术专家，根据经验判断或根据对推理（这种推理包括理论的、模型的或试验的评估）的合理解释所提供的信息。

2.1.21

外露的钢结构 exposed structural steel

没有用非能动的防火屏障（例如延缓火灾的外层）保护的钢结构单元。

2.1.22

外部事件 external event

发生在核电厂外部的事件，直接或间接地引起始发事件，并且造成安全系统失效或操纵员失误，进而可能导致不希望的后果（如堆芯损坏）。比如地震、强风、外部水淹、外部火灾等事件均可考虑为外部事件。通常丧失厂外电作为内部事件，内部水淹和内部火灾作为外部事件。

2.1.23

外部水淹 external flood

由外部水淹源， 比如降雨、溃坝、海啸、波浪、风暴潮等，造成的事件或灾害。

2.1.24

故障模式（失效模式） failure mode

设备不能实现某一具体功能的表现（即观察者可以据此判断故障（失效）已经发生）。一般表现为妨碍某一设备、某一部件或某一系统的成功运行（如不能启动、不能运行、泄漏）。

注：在火灾PSA中，通常考虑的电缆失效模式可能包括电缆内短路、电缆间短路和/或一个导体和外部接地装置之间的短路（参见“热短路”）；通常考虑的电路失效模式可能包括丧失动力电源、丧失控制、失去指示或指示错误、电路处于开路（如保险丝熔断或电路保护装置断开）以及误动作。

2.1.25

故障模式和影响分析 failure modes and effects analysis

识别特定部件的故障模式并评估它们对其他部件、子系统和系统的影响的一种方法流程。

2.1.26

故障（失效）概率 failure probability

构筑物、系统和部件不能投运或不能在规定的任务时间内持续运行的可能性。

2.1.27

故障（失效）率 failure rate

单位时间内，预期某物项发生一种给定模式故障（失效）的次数。虽然失效率与工作次数、可能出现的环境条件等有关，但故障率通常是时间的函数。

2.1.28

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。

2.1.29

火灾隔间 fire compartment

在火灾PSA中定义的建筑物或电厂的一个部分，是一个封闭空间，周边不要求有防火屏障。

注：一个火灾隔间通常在一个防火区内，四周有不可燃的屏障包围，很大程度上限制了该封闭区域内着火后产生的热量和燃烧产物。火灾隔间的边界处可以有打开的设备舱门、楼梯、通道，或未密封的贯穿件。基于消防系统的设计或运行上的考虑，由电厂根据可能的火灾损坏情况将电厂防火区和/或区间划分为火灾隔间。本标准中用“实体分析单元”代表火灾PSA中电厂所有的分区。实体分析单元包括了火灾隔间。

2.1.30

火灾情景 fire scenario

描述火灾事件的一组要素。

注：这些要素通常包括实体分析单元、火源位置和特性、所考虑的探测和灭火设施、受损目标物，以及其中的可燃物。

2.1.31

火灾情景选择 fire scenario selection

确定在火灾 PSA中要分析的火灾情景的过程，火灾情景代表了涉及一个或多个点火源的火灾的特征与结果。

注：火灾情景选择包括：确定一个点火源（或一组点火源）；二次可燃物和火灾蔓延的路径；火灾受损目标物，探测和灭火系统及可用的设施；以及影响火灾受损范围和时间的其他因素。

2.1.32

水淹区域 flood area

与其他区域之间有足以防止水淹危险的水淹屏障相隔离的建筑物或电厂的一部分。在同一水淹区域内，水淹对电厂有相似的影响。

2.1.33

水淹效应 flood effect

因水淹而对构筑物、系统和部件（SSC）产生的不利影响。

2.1.34

水淹情景 flood scenario

描述水淹事件的一组要素。

注：这些要素通常包括水淹时刻的电厂运行状态、水淹区域、水淹源和失效模式，水淹事件类型（比如喷淋、局部水淹、重大水淹等），还包括水淹漫延、水淹损坏的SSC和始发事件在内的水淹影响，以及操纵员动作和缓解系统的响应等。

2.1.35

易损度（脆弱性） fragility

在给定的灾害输入条件下，构筑物、系统或部件发生失效的条件概率。

注：灾害输入可以是地震运动、风速、或水淹水位。地震PSA的易损度模型是一个包含三个参数的双对数正态分布模型，这三个参数分别是：A_m，β_R 和 β_U，它们的意义分别是：抗震能力中值（中位数），抗震能力随机不确定性的对数标准差，以及抗震能力认知不确定性的对数标准差。

2.1.36

前沿系统 front-line system

PSA模型中用于直接实现任一种事故缓解功能（如堆芯或安全壳冷却、冷却剂补偿、反应性控制或反应堆压力容器压力控制等）的安全级或非安全级系统。

2.1.37

地面加速度 ground acceleration

由地震波造成的地面运动的加速度，通常用单位g表示，g表示地面重力加速度。

2.1.38

灾害 hazard

对电厂设施构成风险的事件或自然现象。内部灾害包括设备失效、人员失误、厂内水淹和火灾等事件。外部灾害包括厂外水淹和火灾、台风、地震和飞机撞击等事件。

2.1.39

危险性曲线 hazard curve

表示某自然现象的一些特征量（例如采用峰值地面加速度（PGA）描述地震动）超过各种水平的年超越概率的曲线。

2.1.40

高置信度低失效概率抗震能力 HCLPF capacity

具有高置信度（95%）、低失效概率（最多5%）的抗震能力。

注：通常用地震动水平表示，该能力用于衡量抗震裕度。

2.1.41

高能电弧失效 high-energy arcing fault

电弧导致了电能以热量、导体的汽化和机械力等方式快速释放。

2.1.42

强风 high winds

可能破坏或影响核电厂正常运行的一定强度的风现象。例如，热带（温带）气旋、龙卷风、雷暴、以及其他取决于厂址位置的风现象。

2.1.43

热短路 hot short

火灾情况下由于绝缘材料失效，相同的或不同的电缆内的独立导体之间相互接触，其中短路的导体中至少有一根通电进而导致所分析的电路上产生了外加电压或电流。

2.1.44

人员失误（人员差错） human error

超出某一可接受限制的任何人员动作，包括需要实施却没有实施的行为（动作），但不包括恶意的行为。

2.1.45

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。

2.1.46

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。

2.1.47

点火频率 ignition frequency

火灾发生的频率，通常表示为每堆年的点火次数。

2.1.48

点火源 ignition source

引起火灾的设备或活动。

2.1.49

始发事件 initiating event

干扰电厂稳定运行状态并可导致出现不希望的电厂状态的事件。始发事件发生后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）。

注：低功率工况始发事件基本包括与功率工况相同的始发事件类型。停堆工况典型的始发事件包括丧失衰变热排出和丧失水装量，即干扰停堆工况正常或计划运行状态的任何事件，包括维修导致的事件。特定始发事件定义及发生频率与电厂运行状态有关。

2.1.50

界面系统失水事故 interfacing system LOCA

在与冷却剂系统相连的系统上发生破口、且发生破口的系统和冷却剂系统之间的隔离失效时所产生的失水事故。界面系统失水事故的通常特征是低压系统在经受一回路压力时发生超压，且可能导致安全壳被旁路。

2.1.51

内部事件 internal event

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。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。

2.1.52

内部水淹 internal flood

由厂内水淹源，如管道、水箱、热交换器等引起的水淹。

2.1.53

关键安全功能 key safety function

为防止堆芯损坏所应维持的最小的一组安全功能，这些功能包括反应性控制、反应堆压力控制、反应堆冷却剂装量控制、衰变热排出和安全壳完整性。

2.1.54

低功率 low power

反应堆功率低于特定功率的电厂运行状态。

2.1.55

低温超压 low temperature over-pressurization

反应堆主系统在低温且处于水实体状态期间发生可能引起系统超压的瞬态过程。

2.1.56

主逻辑图 master logic diagram

为指导始发事件及其相关序列的识别和分组而建立的概括性的故障树，目的是保证始发事件的完整性。

2.1.57

中平面水位（半管）运行 midloop

反应堆压力容器水位低于热段顶部的电厂运行状态。

注：该状态的出现主要支持一回路系统维修，例如蒸汽发生器传热管检查，或者作为换料停堆的一个阶段。

2.1.58

任务时间 mission time

一个系统或部件为了成功实现其功能所需运行的时间。

2.1.59

多隔间火灾情景 multicompartment fire scenario

涉及除点火源所在火灾隔间外的其他房间或火灾隔间内的目标物火灾情景。

2.1.60

多重误动作 multiple spurious operations

两个或以上设备单元同时发生误动作。

2.1.61

运行模式 operation mode

由技术规格书规定的电厂运行工况，例如功率运行、热备用、热停堆、冷停堆和换料停堆等。

2.1.62

运行状态年 operating state year

假设一个反应堆一整年持续处于一个电厂运行状态。

2.1.63

停役 outage

反应堆或核电厂根据计划停止运行，进行换料、检修、试验或改进等工作的次临界状态。停役和停堆可相互转换。

2.1.64

停堆类型 outage type

用于描述电厂处于次临界的原因。由于维修和换料的不同需求，从而使其导致的不同停堆类型具有不同的低功率和停堆进程，并且产生不同的电厂运行状态。

注：例如，对于换料停堆类型，冷停堆时部分或全部燃料组件在压力容器外，然而在冷停堆下进行维修的停堆是另外一种不同的停堆类型。通常停堆类型包括：热停堆、冷停堆（二回路未排水）、冷停堆（二回路排水）和换料。停堆类型可进一步划分为周期换料大修停堆或定期维修停堆和非计划维修停堆。

2.1.65

非能动部件 passive component

不依靠触发、机械运动或动力源等外部输入而行使功能的部件。

2.1.66

峰值地面加速度 peak ground acceleration

地震在厂址产生的最大地面加速度。

2.1.67

行为形成因子（绩效形成因子） performance shaping factor

在人员可靠性分析中影响人员失误概率的一个因子，包括培训程度、程序化导则的质量/可用性、执行一个动作的可用时间等。

2.1.68

实体分析单元 physical analysis units

作为火灾 PSA分析基础的电厂空间划分。

注：在电厂区域划分技术要素中，实体分析单元通常以火灾隔间域和/或火灾隔间来定义。

2.1.69

电厂损伤状态 plant damage state

具有相似事故进程和安全壳或专设安全设施状态的事故序列终态组。

2.1.70

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。

注：一个电厂运行状态可以是一个稳定的状态也可以代表两个稳定状态之间的过渡状态。例如，满功率和由于余热排出系统冷却的冷停堆是两个稳定态的电厂运行状态。在这个例子中，可能有一、两个过渡状态的电厂运行状态覆盖电厂从功率停至冷停堆过程中的温度和压力范围。例如，热停堆的温度范围为284℃至294.4℃，可模化为一个温度为294.4℃电厂运行状态。系统或设备的试验或维修不可用的影响可包括在电厂运行状态定义中，或者在电厂运行状态定义外作为定量化过程的一部分。

2.1.71

特定电厂数据 plant-specific data

由所分析电厂的观察样本数据组成的数据。

2.1.72

点估计 point estimate

对一个参数以单个数值的形式给出的估计。

2.1.73

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。

2.1.74

超越概率 probability of exceedance

危险性分析中，在厂址或一个区域，在指定的时间内，至少有一次灾害超过给定水平的概率。

2.1.75

未能扑灭的概率 probability of nonsuppression

在目标物损坏前，灭火失败的概率。

2.1.76

PSA应用 PSA application

一种基于部分或全部的特定电厂PSA的分析，并备有相关文件，用于帮助有关核电厂的设计、执照申请、采购、建造、运行或维修等作决策。

2.1.77

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。

2.1.78

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。

2.1.79

恢复 recovery

通过克服或补偿某一失效的SSC,使得由其导致的某个功能丧失得以恢复。通常采用HRA技术来模化。

2.1.80

换料停堆 refueling shutdown

技术规格书规定的一个（或一组）电厂模式，此时，反应堆压力容器顶盖打开以使燃料组件移出。

2.1.81

反应谱 response spectrum

通过地震加速度时程计算出来的曲线，以有阻尼的单自由度振子（定阻尼比）的峰值反应(加速度、速度或位移)作为它的固有周期（或频率）的函数。

2.1.82

安全停堆地震 safe shutdown earthquake

在核电厂抗震设计中，针对安全相关、抗震 I 类的某些特定构筑物、系统和部件（SSC）设计的、可维持其安全功能的地震动。安全停堆地震（SSE）通常以 PGA 标定的标准加速度反应谱来描述。

2.1.83

安全稳定状态 safe stable state

始发事件发生后的一种电厂状况。在这种状态下，反应堆冷却剂系统的状态是可控的，并处于或接近期望值。

2.1.84

安全系统 safety system

安全上重要的系统，用于保证反应堆安全停堆、从堆芯排出余热或限制预计运行事件和设计基准事故的后果。

2.1.85

筛选 screening

基于对某一事故的概率或其后果的贡献可忽略而不对该事件作进一步考虑的过程。

2.1.86

筛选准则 screening criteria

用于确定某一物项对事故序列的概率或其后果的贡献是否可忽略的数值或条件。

2.1.87

地震设备清单 seismic equipment list

地震 PSA 的地震易损度任务中需要评价的所有 SSC，或抗震裕度评价中需要开展抗震能力评价的所有 SSC。

2.1.88

抗震裕度 seismic margin

高于设计基准而实际具备的抗震能力。

注：通常用危及核电厂安全（特别是导致堆芯损坏）的地震动水平来表示。裕度的概念可以延伸到任何特定SSC，对它们而言，“危及安全”指的是单独的或与其他失效组合的对堆芯损坏有影响的安全功能丧失。

2.1.89

抗震裕度评价 seismic margin assessment

为评价核电厂的抗震裕度，并识别核电厂抗震薄弱环节而进行的过程或活动。

2.1.90

抗震裕度地震 seismic margin earthquake

抗震裕度评价中所选择的用于抗震能力初步筛选的地震动，该地震动应大于电厂安全停堆设计基准地震动。

注：一般情况下，抗震裕度地震由峰值加速度和反应谱来定义，在实际应用中有时也称之为审查级地震。

2.1.91

震源 seismic source

潜在震源区和能动构造的统称。

注：潜在震源区是地球的一部分，具有统一的地震潜能（同样的预期最大地震和复发频率），地震活动有别于周边的地区。能动构造既可以产生地表振荡运动，又可以产生地表变形，如达到或接近地表的断裂或褶皱。在概率地震危险性分析中(PSHA)，需要考虑所有厂址区域内对地面运动概率有潜在影响的震源。

2.1.92

地震空间相互作用 seismic spatial interaction

由地震引起的构筑物、管道、分布系统或其他物项与邻近的安全相关设备间的相对运动，可能会导致安全相关设备不执行其安全功能。

注：此类相互作用包括临近效应、结构失效和功能降级、附线和电缆的弯曲等。

2.1.93

严重性因子 severity factor

点火后火灾具有某些特性的概率，这些特性反映了燃烧发展的速率，释放的能量水平，以及达到目标物受损对应的火灾持续时间（自灭的时间）。

2.1.94

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。

2.1.95

谱加速度 spectral acceleration

一般情况下作为一个周期或频率和阻尼比函数给出（通常是 5%），等于地面上的线性频率谐振子的峰值相对位移乘以$(2\pi f)^2$。单位是 g 或cm/s^2。

2.1.96

喷溅 spray

液体直接喷射或飞溅到设备上，尤其是电气设备上，可能影响设备的绝缘或因液体渗入设备后导致内部电路短路，从而导致设备失效的一种水淹效应。

2.1.97

误动作 spurious operation

由于火灾导致设备的不期望动作，从而影响到实现和维持安全停堆的能力。

2.1.98

淹浸 submergence

SSC所在区域的水位超过SSC底部，导致SSC被水淹浸的一种水淹效应。

注：在水淹PSA中一般假定部件淹浸将导致设备（一般指电气设备）失效。当SSC底部（例如底座之上）被淹浸时，通常认为SSC可能失效，除非有详细的评估证明，部件部分淹浸时仍然可用。但这一假设一般不适用于非能动部件，比如热交换器、止回阀、手动阀，也不适用于其他在事故工况下不需要改变其状态位置或不需要外部动力改变其状态位置或操作的部件。

2.1.99

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。

2.1.100

支持系统 support system

为一个或多个其他系统提供支持功能（如动力电源、控制电源或冷却）的系统。

2.1.101

目标物 target

火灾受损目标物，或点火源目标物。

注：火灾受损目标物是任何模化的火灾可能导致其功能受到不利影响的实物。典型的火灾受损目标物是火灾PSA设备或电缆清单中所列出的设备或电缆，且这些设备和电缆包括在火灾风险评价的事件树和故障树中。点火源目标物是指任何易燃或可燃的物质，且其燃烧可以蔓延开来。

2.1.102

目标物集合 target set

在给定的火灾情景下，根据同样的损坏准则和受损阈值所确定的一组火灾受损的目标物。

注：某个火灾情景的目标物集合经常是火灾隔间受损目标物的一个子组，但也可能包括一个实体分析单元中所有与风险有关的受损目标物，或者包括多个实体分析单元中的受损目标物。这样的定义意味着：当目标物集合中出现第一个目标物质失效时，那么就假定了该组目标物中的其他所有目标物都失效了（即“组内目标物基于同样的损坏准则和受损阈值”）。通过为单一火灾情景定义多个目标物集合（如在管沟内直接位于火源上面的电缆，和远离火源的电缆），可以进行描述火灾受损进程或随时间的变化。与目标物集合定义详细程度通常是与火灾情景选择和分析（例如筛选水平对应分析详细程度）的详细程度对等。

2.1.103

顶事件 top event

在故障树模型中位于故障树起始点（顶点）的不希望发生的系统状态（例如，系统不能完成其功能）。

2.1.104

不确定性 uncertainty

对构建PSA中用到的参数值和模型的知识水平的可信度的一种表示。

注：在地震易损度分析中，该术语表示由于用于计算中值能力的模型和模型参数的认知不完善所产生的中值抗震能力变化性。

2.1.105

一致危险性反应谱 uniform hazard response spectrum

一种在不同频率下具有相同超越可能性的地面响应参数（如谱加速度或谱速度）图谱。

2.1.106

现场巡访 walkdown

对核电厂系统和部件所在现场区域的检查以及与电厂人员的访谈，以确保规程、图纸、设备位置和运行状态的正确性，并确定在事故工况下环境对设备的影响或系统对设备的影响。

2.2 缩略语

下列缩略语适用于本文件。

ACC：安注箱
AOT：允许停役时间
ASEP：事故序列评价程序
ATWS：未能紧急停堆的预期瞬态
BOP：核电厂配套设施
CCCG：共因部件组
CCDP：条件堆芯损坏概率
CCF：共因失效（共因故障）
CCI：共因始发事件
CCW：设备冷却水
CDF：堆芯损坏频率（堆芯损伤频率）
CDFM：确定性失效裕度方法
DHR：衰变热排出
ECCS：应急堆芯冷却系统
EOP：应急运行规程
EDG：应急柴油发电机
FA：易损度分析方法
FHA：火灾危害性分析
FIVE：火灾引起的缺陷分析
FMEA：故障模式和影响分析
FRSS：火灾风险范围研究
FSAR：最终安全分析报告
HEP：人员失误概率（人员差错概率）

HFE：人员失误事件
HLR：高层次要求
HRA：人员可靠性分析
HVAC：加热、通风和空调
IE：始发事件
IF：内部水淹
ISI：在役检查
ISLOCA：界面系统失水事故
LOCA：丧失冷却剂事故（简称失水事故）
LOOP：丧失厂外电
LPSD：低功率和停堆工况
MOV：电动阀
NPSH：净正吸入压头
PCS：非能动安全壳冷却系统
PDS：电厂损伤状态
PGA：峰值地面加速度
PMF：可能最大水淹
POS：电厂运行状态
PSA或PRA：概率安全评价（分析）/概率风险评价
PSF：行为形成因子（绩效形成因子）
PSHA：概率地震危险性分析
RCS：反应堆冷却剂系统
RHR：余热排出
SAR：安全分析报告
SBO：全厂断电
SEL：地震设备清单
SGTR：蒸汽发生器传热管破裂
SMA：抗震裕度评价
SME：抗震裕度地震
SR：支持性要求
SSA：安全停堆分析
SSC：构筑物、系统和部件
SSE：安全停堆地震
THERP：人员失误率预测技术
TS：技术规格书
UHS：一致危险性反应谱

3 一级 PSA 标准的框架和要求

3.1 标准框架

《应用于核电厂的一级概率安全评价》建立了适用于所有电厂运行模式（包括功率运行、低功率和停堆工况）的内部和外部事件的一级概率安全评价（PSA）要求。本标准适用于支持风险指引型决策的PSA，这些决策与设计、执照申请、采购、建造、运行和维修相关。

本标准给出了以下事件的要求：

（a） 内部事件

（b） 内部水淹

（c） 内部火灾

（d） 地震

（e） 强风

（f） 外部水淹

（g） 其他外部灾害

本标准还规定了其他外部事件的筛选和保守分析的要求。这些要求分别对应本标准的第2至第12部分。

第2部分给出了电厂响应一系列完整的始发事件的基本认识，为模化其他各种事件对电厂的影响提供基础。虽然第2部分的标题只与内部事件有关，然而，其许多要求也是进行其他事件PSA的基本要求，故认为该部分的要求适用于本标准范围内的所有事件，即第3至9部分和第11至12部分中的电厂响应相关要求可参考第2部分的要求。

3.2 PSA 技术要求的组成结构

3.2.1 PSA 要素

PSA的技术要求由各个PSA技术要素组成。PSA要素定义了本标准各部分的分析范围。

功率运行内部事件PSA要素主要包括：始发事件分析（IE）、事件序列分析（ES）、成功准则（SC）、系统分析（SY）、人员可靠性分析（HR）、数据分析（DA）、相关性分析（DF）和模型整合与定量化（MQ）。

功率运行内部水淹PSA要素主要包括：内部水淹电厂分区（IFPP）、内部水淹源的确定（IFSO）、内部水淹情景的建立（IFSN）、内部水淹导致的始发事件分析（IFEV）和内部水淹事件序列和定量化（IFQU）。

功率运行内部火灾PSA要素主要包括：电厂区域划分（PP）、设备选择（EQS）、电缆选择和定位（CS）、定性筛选（QLS）、火灾PSA电厂响应模型（PRM）、火灾情景选择和分析（FSS）、点火频率（IGN）、定量筛选（QNS）、电路失效（CF）、人员可靠性分析（HRA）、火灾风险定量化（FQ）和不确定性和敏感性分析（UNC）。

功率运行地震PSA要素主要包括：地震危险性分析（SHA）、地震次生灾害分析（SSH）、地震易损度评估（SFR）、地震电厂响应分析（SPR）。

功率运行强风PSA要素主要包括：强风危险性分析（WHA）、强风易损度评估（WFR）和强风电厂响应模型（WPR）。

功率运行外部水淹PSA要素主要包括：外部水淹危险性分析（XFHA）、外部水淹易损度评估（XFFR）和外部水淹电厂响应模型和量化（XFPR）

功率运行其他外部灾害PSA要素主要包括：外部灾害危险性分析（XHA）、外部灾害易损度评估（XFR）和外部灾害电厂响应模型（XPR）。

对于低功率和停堆工况，PSA要素除了包括上述功率运行PSA要素外，主要还包括：电厂运行状态（POS）。

3.2.2 高层次要求

本标准各部分的技术要求为每个PSA要素给出了一组目标和高层次要求（HLR）。HLR确定了技术上可接受的基准PSA（与具体应用无关）的最低要求。HLR定义了通用要求，并给出高层次逻辑，以引出更详细的支持性要求（SR）。HLR不仅反映了现有PSA开发时所用方法的多样性，而且反映了适应未来技术革新的需求。

3.2.3 支持性要求

本标准各部分的技术要求为每个PSA要素的每个HLR给出了一组SR。SR规定了满足HLR所需的最低要求。当给定HLR下的所有SR均满足时，则PSA将满足该HLR。

SR规定了“做什么”，而非“如何做”，即对满足要求的具体方法不作规定。然而，制定标准要求时，考虑了某种方法。如果其他方法的结果表明等价于或优于满足本标准推荐的常用方法，则可使用该方法。应记录该方法，并进行同行评估。

4 PSA 的应用过程

4.1 目的

本章说明为了确定支持某项特定的风险指引型应用所要求的PSA质量而需进行的活动。应用过程应采用已完成同行评估或安全评审的PSA，该同行评估应满足各部分对应的同行评估要求。

图1给出了应用过程的逻辑顺序。虽然要求开展规定的活动，但可改变其实施顺序。如图中虚线框所示，这一过程有5个阶段：

a) A 阶段：按照受变更影响的构筑物、系统和部件（SSC）及活动，来定义某项应用。对于该项应用，确定受电厂变更影响的 PSA 的各部分，并识别该项应用所需涉及的事件、该项应用相应的 PSA 范围和支持该项应用所需的风险量。通过对应用与 PSA 模型中对变更特别敏感的各部分之间因果关系的了解，确定为支持应用所必需的 PSA 各部分的技术要求；

b) B 阶段：对 PSA 进行检查，以确定其范围和详细程度对该项应用而言是否足够。如果发现该 PSA 在一个或多个方面还有不足，则其可能需要升级，或需要由其他分析加以补充（E 阶段）；

c) C 阶段：进行评估以确定对于 PSA 各个部分，本标准各部分中相应的 SR 是否足以支持该项应用。如果不足以支持该项应用，则可用 E 阶段所述的补充要求来增补 SR；

d) D 阶段：按 A 阶段中所确定的支持该项应用所需的技术要求，将 PSA 的各个部分与本标准各部分中相应的 SR 进行比较。确定该 PSA 是否具有足够的质量，是否需要升级以满足相应的 SR，或者是否需要开展 E 阶段所述的补充分析；

e) E 阶段：将 PSA 用于支持该项应用，如有必要，对该 PSA 增加补充分析。

图1中的活动范围确定了如何评估PSA在应用中的作用。为满足所需的技术要求，进行补充分析来替代PSA升级，判定补充分析质量的准则超出了本标准各部分的范围。因此，满足本标准各部分意味着在该项应用中所用到的PSA的各个部分都满足一组与规定的技术要求相应的HLR和SR。应根据具体案例来确定在该项应用中如何使用PSA。

4.2 识别应用案例和技术要求（A 阶段）

4.2.1 应用案例的识别

通过下述各项内容来定义应用案例：

a) 对要作评价的电厂设计变更或运行变更进行评估（见图 1 中的框 1）；

b) 识别受变更影响的SSC和电厂活动，包括电厂设计或运行的变更与PSA模型之间的因果关系（见图 1 中的框 2）；

c) 识别为评价变更所需的事件、PSA 范围和 PSA 风险量（见图 1 中的框 3）。

示例1：非能动安全壳冷却系统（PCS）设计了两条PCS水箱出口管线，每条管线上设置一台常关气动阀和一台常开电动阀。为考虑多样性，提出设计变更，拟增加第三条PCS水箱出口管线，在该管线上设置一台常关电动阀和一台常开电动阀。

为评价所提出设计变更的影响，需要识别那些受变更影响的SSC。PCS新增的第三条出口管线与原先的出口管线相互冗余，三条管线中的任一条开启就可满足PCS带出热负荷的需求。

所提出的设计变更增加了一条出口管线以实现系统功能，从而降低电厂风险。这一变更是通过考虑对系统不可用度的影响和对电厂风险量的影响来评价的。

示例2：对技术规格书（TS）提出变更，重新定义对可运行的厂用水系统的要求。这一变更取消了TS中关于每条厂用水回路中的三台泵中的任一台泵的允许停役时间（AOT）的要求。此外，增加了不可运行部件的其他选定组合的AOT。需要详细识别所涉及的在TS和（或）规程中的有关变更。

为了评价所提出的TS变更的影响，需要识别那些受变更影响的SSC，如厂用水系统。电厂的厂用水系统有两条冗余回路，每条回路有两台全容量的厂用水泵，它们以海水作为最终热阱，另外有第三台泵采用的是冷却塔冷却，以大气作为热阱。厂用水系统设计成在发生LOCA并同时发生丧失厂外电的情况下，单台厂用水泵（由其相应的EDG供电）就有足够的能力带走热负荷。现行TS要求有二条可运行的厂用水回路，每条回路有三台可运行的泵。这一要求超出了单一故障准则的要求，因为在正常工况与设计基准事故下均不要求投入第二台厂用水泵，并且冷却塔冷却的厂用水泵为设计基准LOCA提供了冗余。所提出的变更把一条可运行的厂用水回路重新定义为有一台可运行的厂用水泵和一台可运行的冷却塔冷却的厂用水泵，取消了两台厂用水泵的AOT要求，延长了厂用水泵的AOT要求，并且根据备用的冷却塔冷却的厂用水泵的风险重要度较低而延长其AOT。

所提出的AOT变更增加了一台厂用水泵因计划性或非计划性维修而不可用的可能性，从而影响了堆芯损坏频率（CDF）。这一变更是通过考虑对系统不可用度的影响和对涉及单列厂用水不可用度的序列频率的影响来评价的。

4.2.2 技术要求

针对应用，确定支持该项应用所需各事件的PSA各部分的技术要求（见图1中的框4）。这一决定规定了要采用哪些SR来评估支持该项应用的PSA各部分的质量。为确定这些技术要求，需对该项应用进行评估，以评价PSA在支持该项应用中的作用。当进行这一评估时，需考虑应用的下述特征：

a) PSA 在该项应用中的作用和决策对 PSA 结果的依赖程度；
b) 用于支持该项应用的风险量和有关的决策准则；
c) 风险贡献对决策的重要程度；
d) PSA 或 PSA 的某一给定部分所采用方法的包络或保守程度，从而对应用所做的决策以及在决策过程中所采用的方式产生不适当的影响；
e) 所要求的 PSA 结果的精确度、不确定性评估和敏感性评估；
f) 用于支持决策的结果的置信度；
g) 在应用中所做的决策对电厂设计基准的影响程度。

技术要求及确定技术要求的依据应编制成文档。

4.3 对 PSA 的必要范围、风险量和模型的评价（B 阶段）

4.3.1 必要范围和风险量

确定PSA能否提供评价电厂或运行变更所需的结果（见图1中的框5）。如果PSA的某些方面不足以评价该变更，则按本标准各部分技术要求相应的SR对PSA的这些方面进行升级（见图1中的框6a），或者进行补充分析（见4.6节）。如果断定PSA是足够的，则应将这一判断的依据编制成文档。任何PSA升级应按第6章的要求进行并编制成文档。

示例1：继续4.2.1的示例1，所提出的PCS水箱出口管线设计变更会影响系统不可用度。PCS作为事故缓解系统，在安全壳高温、高压的情况下提供最终热阱，其设计变更主要影响PSA技术要素如下：

a) 成功准则要素：确认成功准则与电厂特征相一致，即需要考虑3列出口管线；
b) 系统分析要素：新增部件失效模式相关的模化。

这些影响应结合到电厂模型中，以计算系统不可用度和电厂CDF的变化量。

示例2：继续4.2.1的示例2，所提出的厂用水系统AOT的变更会影响厂用水的不可用度。对所讨论的电厂，厂用水向ECCS泵、柴油发电机、给水泵、CCW系统和放射性废物系统提供冷却。因此，PSA的始发事件分析要素应包括：

a) LOCA始发事件，因为厂用水系统不可用度的变化将会影响再循环阶段ECCS泵的冷却；

b) 丧失厂外电始发事件，因为厂用水的变化将会影响柴油发电机；

c) 丧失给水始发事件，因为给水泵是由厂用水冷却的。

虽然采用厂用水冷却CCW系统，但CCW系统具有足够的热惯性，使它在丧失厂用水后数小时内仍能起作用，从而能使电厂处于安全稳定状态，因此对这一应用案例，不需要考虑丧失CCW这一始发事件。同样，由于放射性废物系统与确定CDF无关，因此也不需要考虑。经确认，维修不可用度的变化很小，不用考虑其对厂用水泵的可靠性（它会影响很多序列，包括丧失厂用水始发事件和厂用水泵失效的序列）会造成显著影响。这些影响都应结合到电厂模型中，以计算CDF的变化量。由于只需要ΔCDF（CDF的变化量），因此只需要TS变更前与变更后的CDF值。

4.3.2 SSC 和电厂活动的模化

确定受电厂设计或运行变更影响的SSC或电厂活动是否已在PSA中作了模化（见图1中的框5）。如果没有模化受影响的SSC或电厂活动，则按本标准各部分技术要求相应的SR对PSA进行升级以包括这些SSC（见图1中的框6a），或者进行补充分析（见4.6节）。如果断定PSA是足够的，则应将这一判断的依据编制成文档。任何PSA升级应按第6章的要求进行并编制成文档。

示例1：继续4.3.1的示例1，PSA需要模化受PCS设计变更影响的、并对电厂风险量的变化有贡献的SSC及电厂活动。例如，PCS系统成功准则由出口管线二取一成功变更为三取一成功，并需要考虑新增SSC的不可用度，或者电厂技术规格书根据该设计变更进行变更，从而降低反应堆行政停堆频率，则该PSA需要升级以考虑该影响，或者进行补充分析。

示例2：继续4.3.1的示例2，在PSA中需要模化与受到所提出的厂用水变更影响的系统有关的、并对CDF的变化有贡献（即：ECCS、柴油发电机、给水和CCW）的SSC及电厂活动。例如，如果丧失给水始发事件被模化为一个全局性的始发事件（这是很可能的），则该PSA需要升级以包括厂用水与给水之间的关系，或者必须补充分析来找出厂用水对给水的影响。

4.3.3 同行评估的确认

对应用所需的PSA各部分内容都应已按照本标准各部分相应的同行评估要求进行过评价。

4.4 应用过程的 SR 范围与详细程度的确定（C 阶段）

针对4.2.2所确定的技术要求，确定本标准各部分技术要求所述的SR的覆盖范围和详细程度是否足以充分评价所考虑的应用（见图1中的框8）。

如果断定本标准各部分没有给出专门要求，则应评价这些所缺的要求对应用的相关性（见图1中的框9）。如果所缺的要求不相关，则本标准各部分的要求足以满足该项应用的需要。应将确定本标准各部分充分性的依据编制成文档。如果所缺的要求是相关的，则可使用补充的要求（见图1中的框7）。

4.5 PSA 模型与标准的比较（D 阶段）

确定PSA的各个部分是否满足为支持该项应用所需的SR（见图1中的框10）。可利用同行评估的结果。如果PSA满足该项应用所必需的SR，则该PSA对所考虑的应用是可接受的（见图1中的框11）。应将这一确定的依据编制成文档。

如果PSA不满足相应的SR，则应确定其原因是否相关或重要（见图1中的框12）。确定这种相关性或重要性的可接受要求包括：

a) 如果不满足相应 SR 的原因不适用，或不会影响因应用而受影响的定量化，则该原因并不相关（例如，如果处理人员可靠性的有关 SR 没有满足，其原因是未采用详细的 HRA 方法评估一些

在基准模型中是重要的人员失误事件的失效概率，但这些人员失误事件对应用所需的结果不产生作用，由此，不满足技术要求对决策是不相关的）；

b) 如果模型中至少占所评价事件的 CDF 的 90%（若适用）的事故序列不会受相应的敏感性研究或包络性评估的影响，则该差异不重要。这些研究或评估应估量本标准各部分的技术要求用于该项应用时由于例外情况所造成的总影响。当需要确定该差异对应用的重要性，可单独或合并评估相关事件。

上述确定的情况取决于所考虑的具体应用，并且还可能涉及专家组所作的决定。

如果差异不相关且不重要，则 PSA 对该项应用是可接受的。如果差异是相关的或重要的，则根据本标准各部分技术要求所述的相应的 SR 对 PSA 进行升级（见图 1 中的框 6b），或者进行补充分析（见 4.6 节）。任何 PSA 升级应按第 6 章的要求进行并编制成文档。

4.6 获得风险结论（E 阶段）

4.6.1 补充分析的采用

如果 PSA 的范围或本标准各部分的范围并不足够，则可采用补充分析或补充要求（见图 1 中的框 7）。这些补充分析取决于所考虑的具体应用，但可能涉及确定论方法（如包络分析或筛选分析）以及专家组所作的决定。这些内容应编制成文档。

示例 1：对于按风险指引型分级方法确定为低安全重要性的电动阀，希望对其试验频率进行变更。若该项目中所关注的所有电动阀或电动阀的故障模式没有都反映在 PSA 中，则可对 PSA 进行补充。通过采用总的风险信息来支持把电动阀置于适当的风险类别中，这一例子说明了处理 SSC 模型恰当性的过程。

补充要求应从其他公认的规范或标准中获取，这类规范或标准的范围是对本标准各部分作了补充且适用于该项应用的。但若没有这类公认的规范或标准，则补充要求可由专家组确定。

示例 2：进行对某电厂在役检查（ISI）大纲的风险排序/分类。现有的 PSA 模型满足在本标准各部分中所规定的要求。然而，对管路或管段的模化，本标准各部分并没有给出恰当的支持详细定量排序的相关要求。对此，可由一个专家组确定各管段的安全重要性来补充本标准各部分的要求。可用确定论和其他传统工程分析、纵深防御理念或维持安全裕量方面的考虑来对管段进行分类。也可用已发布的工业界或国家核安全局关于风险指引型 ISI 的指导性文件对本标准各部分加以补充。还可用 PSA 模型估算各管段故障对风险的影响（不修改 PSA 的逻辑）来补充本标准各部分的要求。通过识别在 PSA 中已模化的始发事件、基本事件或事件组来完成此估算，在这些事件和事件组中包括了管段故障的影响。

示例 3：为了得到一个阻尼器试验的分级方法，要求根据其风险重要度对阻尼器进行分级。除了主系统的大型部件上的阻尼器外，其他阻尼器对 CDF 的影响很小，因此本标准各部分并不要求在确定 CDF 时考虑其失效。然而，阻尼器是安全相关部件，要求通过试验程序来证实其能够执行动力支撑功能。如 ASME 规范案例 OMN-10 中所示，失效机理的评价可能表明，在阻尼器起安全重要作用的事件中，阻尼器的安全重要度可用其所支撑的部件的安全重要度来近似。这个补充准则可用于划分阻尼器的安全重要度等级。

示例 4：当采购新的阀门时，希望用商用级电动阀来替换某些当前的安全级电动阀。内部事件 PSA 表明，这些阀门在重要事故序列中起的作用较小，其主要故障模式只有“需求时打不开”。通过可靠性数据了解到，对这一故障模式，商用级阀门的失效率与安全级阀门的失效率相同。然而问题是：在大地震期间和发生大地震以后，商用级阀门是否能像安全级阀门一样执行其功能。为处理这一问题，可以采用补充要求，评价商用级阀门的抗震能力，并与即将被其替换的安全级阀门的抗震能力进行比较。

4.6.2 补充分析的结果

如果已确认PSA具有足够的质量，则其结果可用于支持该项应用（见图1中的框13）。否则，补充分析的结果（其中有些分析可按补充要求进行）也可用来支持该项应用（见图1中的框7）。

对各事件，应确定风险贡献者及其不确定性的特性（见图1中的框14）。当已经确定所有相关事件的特性时，则向决策制定者提供风险输入信息（见图1中的框15）。根据支持应用的需要，相关事件的特性可以单独确定或合并后确定。

对于风险指引型的应用，术语“重要”可从不同角度进行评估。“重要”的序列、贡献项和割集等可由其对某一特定事件（如内部火灾）的贡献或者对整个电厂风险的贡献进行衡量。当使用本标准进行基准PSA分析时，需要对给定事件进行评价并描述风险贡献项的相对贡献，以确定“重要”项。

为满足本标准要求，先针对基准PSA模型评估或确定“重要”的程度，执行相关支持性要求，该基准PSA模型是用于量化所有事件的平均年风险量。在本标准的应用过程中，对“重要”项的评估或确定（见图1中的框12），先针对风险指引型应用所涉及的变更范围，再针对每个事件，对所有风险贡献项进行评估，以确定是否需要进行补充分析。

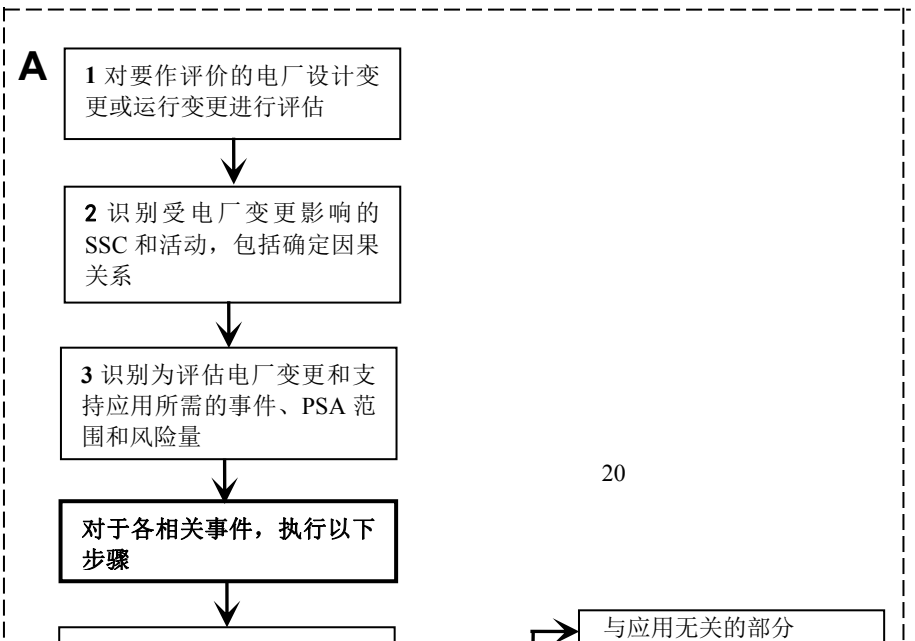

图 1　应用过程流程图

5　PSA 技术要求

5.1　目的

本章的目的是为PSA能够用于支持核电厂风险指引型决策提供技术要求。本章还包括分析计算的过程检查及运用专家判断的通用要求。

5.2　过程检查

对于PSA中直接使用的分析计算（例如，人员可靠性分析和数据分析）或用于支持PSA的分析计算（例如，支持界定任务成功的热工水力计算），应由未参与分析计算的资深人员进行评估。评估文件应进行归档，确保过程可追溯性。

5.3 专家判断的运用

PSA分析组应明确而清楚地说明应用外部专家判断所寻求信息的目的，并应向专家解释这一目的和这些信息的预期用处，清楚地说明需由专家处理的具体技术问题。

PSA分析组应判断问题的重要程度和复杂程度，并确定一个或多个专家组成专家评估组。PSA分析组可选择利用自己的专家判断或其组织内的其他人员的判断来解决技术问题。在必要时， PSA分析组应寻求外部专家帮助。如果由于下述任何原因或相关原因而需要获得更广泛的意见时，即使在内部能够得到专家意见，PSA分析组也应利用外部专家：

a) 分析者知道存在复杂的实验数据，而不同的外部专家对此给出了不同的解释；

b) 对于技术问题的解释存在一个以上的概念模型，并需要对不同模型的适用性做出判断；

c) 需要由判断来评价包络假设或计算是否适当保守；

d) 不确定性大而且重要，而外部技术专家的判断有利于阐明这一具体问题。

若有需要，PSA分析组还应确定其他技术问题专家，例如：

a) 提倡特定假设或技术见解的专家，如评估数据并提出特定假设来解释数据的个人；

b) 具有与问题有关的特定技术领域方面知识的技术专家。

PSA分析组应规定专家组对最终判断的责任。专家组应对来自文献和来自建议者及资深专家的所有可能假设和输入依据进行评价，并应提供他们自己的输入和他们自己对业界研究状态和成果的判断。每个专家都应对其所作的判断和解释承担责任。

PSA分析组负责对专家评估组的判断加以综合，以获得基于可靠信息的最终判断。

5.4 PSA 要素的要求

对于每个PSA技术要求，规定了相应的目标。目标总结了PSA发展和使用过程中积累的经验，并为建立HLR提供基础。

在建立HLR时，基于目标，形成一组不可缩减的要求，适用于所有PSA应用层次。HLR通常给出PSA要素的以下特征：

（a） 范围和详细程度；

（b） 模型精确性和现实性；

（c） 输出或定量化结果；

（d） 文件编制。

SR确定了为支持HLR而需要采取的行动要求。

对于每个PSA技术要素，给出了相应的HLR和SR的表格。通过对SR进行编号和标识，与所支持的HLR保持一致。当给定HLR下的所有SR均满足时，则PSA将满足该HLR。

6 PSA 状态控制

6.1 目的

本章给出了对与本标准各部分一起用于支持核电厂风险指引型决策的PSA状态控制的要求。

6.2 PSA 状态控制程序

应制定PSA状态控制程序。该程序应包含下列关键要素：

a) 跟踪 PSA 输入和采集新信息的过程；
b) 维护和升级 PSA 使之与电厂状态保持一致的过程；
c) 确保在应用 PSA 时考虑了待处理变更的累积影响的过程；
d) 维护用于支持 PSA 定量化的计算机程序的状态控制的过程；
e) 程序的文档。

6.3 跟踪 PSA 输入并采集新信息

PSA 状态控制程序应包括跟踪可能影响 PSA 的设计、运行、维修和业界运行记录的变更的过程。这些变更应包括影响运行规程、设计状态、始发事件频率、系统或子系统的不可用度以及部件故障率的输入信息。该程序还应跟踪可能改变 PSA 模型结果的 PSA 技术和业界经验的变更。

6.4 PSA 的维护和升级

应维护和升级PSA，使之能充分支持对电厂的PSA应用。

应评估按照6.3确定的PSA输入中的变更或新发现的信息，以确定是否需要对PSA进行维护或升级（PSA维护与PSA升级的区别见第3章）。对会影响风险指引型决策的变更应进行排序，以确保尽可能切合实际地把最重要的变更整合进去。与具体应用有关的变更应满足按4.5中所述的过程确定的、与该应用有关的支持性要求。

因PSA维护和升级而引起的PSA变更应满足本标准各部分的技术要求。PSA的升级应按本标准各部分同行评估章节所规定的要求进行同行评估，但只限于PSA中已升级的那部分内容。

6.5 待处理的变更

只要电厂发生了变更（例如工程改造、规程变更、电厂性能（数据）），或一旦识别出模型的某一方面需改进（例如新的人员失误分析方法、新的数据更新方法），则只有在这种变更整合进PSA之后，该PSA才能真实地反映电厂的情况。因此，PSA的状态控制过程应考虑待处理电厂变更或模型改进对所实施的应用的累积影响。这些电厂变更或模型改进对PSA结果和应用所考虑的决策的影响应按照与第4章中所采用的方法相类似的方式进行评估。

6.6 计算机程序的使用

对用于支持和进行PSA分析的计算机程序应加以控制，以确保得到一致的、可复现的结果。

6.7 文档

状态控制程序的文档和处理上述各要素的文档应足以证明PSA是按照与电厂状态相一致的要求来维护的。

文档一般包括：

a) 跟踪 PSA 输入并采集新信息的过程的描述；
b) 证明上述过程有效的证据；
c) 所提议的变更的描述；
d) 每次 PSA 升级或 PSA 维护引起的 PSA 变更的描述；
e) PSA 评估执行情况及其结果的记录（与 7.6 的要求一致）；
f) 处理待定变更的累积影响的过程和结果的记录；
g) 软件技术状态控制过程的描述。

7 同行评估

7.1 概述

7.1.1 一般要求

本章给出了对风险指引型决策的PSA进行同行评估的要求。拟应用的PSA部分应进行同行评估。

7.1.2 目的

同行评估的目的之一是确定PSA所采用的方法及其实施情况是否满足本标准各部分的要求。同行评估的另一个目的是确定该PSA的强项和弱项。同行评估虽然不必按本标准各部分技术要求的所有要求评价PSA的所有方面，但对评估人员来说，应对PSA足够多的方面进行评估，以便对各PSA要素所采用的方法及其实施情况的合适性达成共识。

7.1.3 频度

在PSA应用之前，需进行一次完整的同行评估。此外，第6章要求对PSA的升级进行同行评估。当对PSA升级进行同行评估时，应考虑对最近一次评估记录的评估。附加的同行评估的范围可仅限于自上次评估以来所作的PSA的变更。

7.1.4 方法

评估应采用书面的方法进行，该方法评价本标准各部分的技术要求并要实施本标准各部分同行评估的要求。

同行评估方法应包括下列要素：

a) 选择同行评估组的过程；
b) 同行评估过程中的培训；
c) 同行评估组用来评价该 PSA 是否满足本标准各部分技术要求的支持性要求的一种方法；
d) 处理和解决不同专业意见的过程；
e) 评估 PSA 状态控制的方法；
f) 编制评估结果文件的方法。

7.2 同行评估组的组成和人员资质

7.2.1 综合素质的队伍

同行评估组的组成人员应具备如下综合资质：

a) 具有评价本标准各部分技术要求的所有 PSA 要素（适用时）及这些要素之间接口的能力；
b) 具有电厂核蒸汽供应系统设计、安全壳设计和电厂运行的综合知识。

7.2.2 队伍成员

同行评估组成员个人应具备下列条件：

a) 深刻了解本标准各部分对其所评估领域的要求；
b) 对于指派其评估的 PSA 要素，该评估人员应具有进行这方面工作的丰富经验。

为避免出现技术利益冲突的情况，同行评估组成员原则上不应参与或直接指导受评估PSA的任何工作。

7.2.3 PSA 升级的同行评估组成员

当对PSA升级进行同行评估时，评估人员应具有所评估的特定PSA要素方面的充分知识和经验。另一方面，还应符合本章的其他要求。

7.2.4 人员要求

同行评估人员应充分了解（通过直接的经验）指定评估的PSA要素中使用的具体方法论、程序、工具或方法。评估人员应证明其对所指派领域有深入了解并可以胜任有关该领域的评估工作，这通过其在指定领域中从事的各种不同的独立工作以及这些工作的不同复杂程度中的个人经验丰富程度来证明。

a) 同行评估组中应有一名成员（负责技术综合）熟悉本标准各部分认定的所有 PSA 要素，并具有综合这些 PSA 要素的能力。当评估内容超过一个部分时，可对每个部分配置一名独立的技术综合者；
b) 同行评估组应有一名组长来领导评估组开展评估工作；
c) 同行评估应由至少五位成员组成的评估组来进行，而且应该至少进行为期一周的评估。如果评估集中在某个特定的 PSA 要素上，诸如对某个 PSA 要素的升级的评估，则同行评估应由至少 2 位成员组成的评估组来进行，评估时间由处理该特定 PSA 要素所需时间而定；
d) 根据可获得的组建同行评估组的合适人选，本条的要求可有例外。只有当评估涉及的是某个要素的升级，而且对升级中所涉及的技术，评估者的资质合格时，由单个成员开展的同行评估才被认为是正当合理的。所有这些例外情况都应依照 7.6 编制成文件。

7.3 PSA 要素的评估

同行评估组应采用本节中关于所评估的PSA要素的要求，确定每个PSA要素的分析方法及其实施情况是否满足本标准各部分的要求。根据所获得的结果，可能要评估关于这些要素的其他附加材料。这些建议并不打算列出最低或全面的要求清单。而应由评估人员的判断来确定对每个PSA要素评估的具体范围和深度。

同行评估组应评估整个PSA（包括模型和假设）的结果以及每个PSA要素的结果，以确定它们对于给定的电厂设计和运行情况的合理性（如研究割集或序列组合的合理性）。

同行评估组应采用本标准各部分技术要求中的高层次要求和综合的支持性要求，来评价某个PSA要素的完备性。

7.4 专家判断

应用5.3中所考虑的内容对为实施本标准各部分的要求而采用的专家判断进行评估。

7.5 PSA 状态控制

同行评估组应按第6章的状态控制要求对维护或升级PSA的过程（包括实施情况）进行评估。

7.6 文档编制

7.6.1 同行评估组的文档

同行评估组的文档应证明评估过程充分贯彻了评估要求。

同行评估文档应明确包括以下内容：

a) 对所评估 PSA 的版本的确认；
b) 同行评估组成员的姓名；
c) 评估组每名成员的简历，说明各人的受雇单位、学历、所受的 PSA 培训以及在 PSA 和 PSA 要素方面的经验和专长；
d) 每名成员所评估的 PSA 要素；
e) 对每一 PSA 要素的评估范围的讨论；

f) 评估结果，该评估结果说明本标准各部分技术要求和第 6 章的要求与所采用的方法之间的各项差异，并详细到便于将来解决这些差异的程度；
g) 对于支持性要求的例外情况和不足之处的识别，以及这些例外与不足的重要性，包括评估人员已经确定相关的 PSA 假设的评价；
h) 同行评估人员内部的不同观点和反对意见（当任何评估人员要求列出这些内容时）；
i) 处理各种不同观点的建议方案；
j) 对该 PSA 的强项和弱项的认定。

7.6.2 对同行评估组意见的答复

对同行评估组意见的答复应编制成文件。对同行评估组的建议方案有异议时应证明异议的合理性。

参 考 文 献

[1] ASME/ANS RA-Sa-2009，Addenda to ASME/ANS RA-S-2008 Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications，ASME，2009.

[2] ASME/ANS RA-Sb-2013，Addenda to ASME/ANS RA-S-2008 Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications，ASME，2013.

[3] NUREG-2122, Glossary of Risk-Related Terms in Support of Risk-Informed Decisionmaking, U.S. Nuclear Regulatory Commission, 2013.

[4] HAF 102-2004，核动力厂设计安全规定，国家核安全局，2004年。