第1章 概念原则

在核能开发与利用的过程中，核动力反应堆的安全性始终是最为关键的技术核心之一。核反应堆安全不仅关系到设备本身的可靠性与稳定性，更直接关联公众健康、环境保护与社会信任。为实现“安全第一”的原则，必须在设计、建造、运行、管理等各个环节中，贯彻系统性的安全理念与工程措施。本章主要讨论先进反应堆的类型、核动力反应堆安全的核心概念体系、设计运行原则、事故分析框架及监管要求。首先，说明了先进反应堆和核安全的基本范畴，包括先进反应堆的类型、风险性的定义与计算、安全总目标及其辅助目标的构成、固有安全性的内涵与价值，以及安全文化的起源、内涵与建设途径。其次，强调了确保核安全的关键设计原则，特别是纵深防御的多层次策略、单一故障准则、多样性原则、独立性原则、故障安全原则、合理可行尽量低原则，以及运行人员操作优化的人因工程考量。再次，说明了核电厂运行工况的明确定义与分类体系，分析了设计基准事故、超设计基准事故和严重事故的特征与区别，并列举了典型始发事故类型及其潜在后果与缓解措施。最后，通过介绍放射性核素的衰变类型、电离辐射机制及裂变与活化产物的释放过程，阐明了在不同事故条件下，放射性物质的释放路径与迁移特征，概述了其对人员、环境造成的潜在影响，以及国家在核安全法规、事故分级标准和许可制度等方面的监管措施。

1.1 基本概念

1.1.1 先进反应堆类型

1. 改进型

1）基本内容

对现有反应堆技术进行改进和优化，以提高其性能、安全性和经济性的反应堆类型。

2）概念示例

“华龙一号”是中国自主研发的第三代核电技术，其设计基于 CPR1000 和

ACP1000堆型，融合了全球先进的安全理念和技术。该反应堆采用177堆芯设计，具有双层安全壳、主动与非能动相结合的安全系统，以及更高的抗事故能力，符合国际最新核安全标准。“华龙一号”的成功研发和应用，不仅提升了中国核电的自主创新能力，也推动了核电技术的国际化发展，目前已在国内外多个项目中得到应用。目前我国正筹划进一步发展设计更先进的“华龙二号”。

2. 非能动型

1）基本内容

大量采用非能动的安全系统，同时简化系统，采用先进堆芯，延长寿期，以达到增强安全性和提高经济性的优化目的。

2）概念示例

美国西屋公司发展的AP1000；俄罗斯WWER1200；中国CAP1400(“国和一号”)等。

3. 革新型

1）基本内容

引入固有安全设计思想，根除严重事故产生的可能性。目前还处于概念设计阶段，有待发展和批准。

2）概念示例

瑞典ABB原子公司的PIUS(process inherent ultimate safety)型反应堆；还有安全整体式反应堆(safe integral reactor，SIR)。

4. 小微型

1）基本内容

小微型是一种先进核反应堆，具有建造速度快、成本低、占地面积小、灵活性强的特点。与传统发电厂相比，小型模块化反应堆(SMR)的换料周期更长，通常为3～7年，甚至可以达到30年。此外，SMR与数据中心和人工智能(AI)需求高度适配，因此受到了各国的青睐。

2）概念示例

中国ACP100先进压水堆；美国奥丁(Odin)微堆等。

1.1.2 风险性

1. 风险

表示人们在从事某项活动时，在一定时间内带给人类的危害。

2. 风险的计算

风险不仅取决于事件发生的概率，而且还与事件发生后所引起的后果大小

有关。

$$R\left[\frac{\text{损害}}{\text{单位时间}}\right]=P\left[\frac{\text{事件}}{\text{单位时间}}\right]\times C\left[\frac{\text{损害}}{\text{事件}}\right] \tag{1-1}$$

其中，P 为事件发生的概率；C 为事件后果的幅值。

3. 风险与安全关系

有活动就有风险，风险无处不在，关键是用科学的态度和标准来正确衡量收益和风险。以合理可行的手段来尽可能降低活动带来的风险，就构成各项活动的安全目标。

4. 核电风险来源与危害

1）来源

主要是事故工况下，不可控放射性核素的释放。

2）危害

根据上述 1)的来源，对工作人员、居民和环境带来的危害。

5. 核电厂的安全特征

高危险性、低风险率。

6. 核电安全问题

1）辐射安全问题

要求在任何条件下，确保工作人员和环境处于正常的辐射水平之下。

2）技术安全问题

要求反应堆设计和运行中，必须考虑并采取相应措施，以排除不可控制的链式裂变反应的偶然发生和发展的可能性。

1.1.3 安全总目标

1. 最终安全目标

1）内容

保证工作人员、社会及环境免遭放射性危害。

2）方法

在核电厂里建立并维持一套有效的防护措施。

2. 辅助安全目标

1）内容

保证最终安全目标的实现。

2）类型

辐射防护目标和技术安全目标。

3. 辐射防护目标

1）内容

缓解对工作人员、居民及环境的危害。

2）方式

确保在正常运行时，核电厂及从核电厂释放出的放射性照射保持在合理可行尽量低的水平，并且低于规定的限值，确保由事故引起的辐射照射程度得到缓解。

3）要求

(1) 辐射预防。

在正常情况下，有一套完整的辐射防护措施。

(2) 事故缓解。

在事故工况下，有一套减轻事故后果的措施，包括厂内和厂外的对策。

4. 技术安全目标

1）内容

为防止事故的发生，并进一步制止事故的发展，在必要时缓解事故后果。

2）方式

(1) 预防核电厂发生事故。

有很大把握预防核电厂事故的发生。

(2) 确保放射性后果低。

对于核电厂的所有事故，甚至对于那些发生概率极小的事故，都要确保其放射性后果(如果有)是小的。

(3) 确保发生严重事故的概率非常低。

对于那些会带来严重放射性后果的严重事故，确保其发生的概率非常低。

3）要求

(1) 事故预防。

从设计到运行都需要贯彻一系列的安全原则，例如采用合理的设计、可靠的设备、完善的各种规程，运行人员具有良好的安全文化等。这是设计人员和安全人员应尽的安全职责。

(2) 事故缓解。

由于事故预防不能完全避免事故的发生，在设计中就需要考虑到特定范围内某些可能产生严重后果的事故，这就需要设置若干专设安全设施(engineered safety feature，ESF)。

1.1.4 安全性

1. 安全性概述

1）第一原则

在反应堆与核电厂的设计、建造和运行过程中，必须坚持安全第一的原则。

2）正常的工况

反应堆正常运行时，裂变产物几乎全部被包容在燃料元件内，从燃料元件泄漏的少量气态裂变产物以及活化产物，几乎都被包容在封闭的一回路系统内。

3）可能的问题

一旦发生严重的堆芯损坏事故，同时又发生一回路边界和安全壳破损的情况，将有大量的放射性物质释放到环境中，造成严重污染。

2. 安全性要素

1）自然安全性

反应堆内在的负反应性温度系数、燃料的多普勒效应和控制棒借助重力落入堆芯等自然法则的安全性，事故时能控制反应堆反应性或自动终止裂变，确保堆芯不熔化。

2）非能动安全性

建立在惯性原理（如泵的惰转）、重力法则（如位差）、热传递法则等基础上的非能动设备（无源设备）的安全性，即安全功能的实现无需依赖外来的动力。

3）能动的安全性

必须依靠能动设备（有源设备），即需由外部条件加以保证的安全性。

4）后备的安全性

由冗余系统的可靠度，或阻止放射性物质逸出的多道屏障，提供安全保证。

3. 固有安全性

当反应堆出现异常工况时，不依靠人为操作或外部设备的强制性干预，通过自然的安全性和非能动的安全性，控制反应性或移出堆芯热量，使反应堆正常运行或安全停闭。

4. 固有安全性堆

1）定义

主要依靠自然安全性、非能动安全性和后备反应性的反应堆体系，即具备固有安全性能力的堆。

2）价值

考虑到核电厂系统的复杂性，以固有安全性概念贯穿反应堆、核电厂设计的安

全新论点，来保证解决设计上的薄弱环节，大力推进核电的安全性。

3）特点

以固有安全概念贯穿反应堆的整个设计。而过程固有最终安全反应堆（process inherent ultimate safety reactor）的设计，则进一步发挥了这一个概念。

4）示例

在池式快堆（也叫整合式快中子增殖反应堆（integral fast reactor，IFR））中，其堆芯泡在一个极大的水池内，堆芯产生的热量永远小于水池的冷却能力，堆芯的安全保证依靠重力和热工水力学定律。

1.1.5 安全功能

1. 安全功能类型

安全功能类型如图 1-1 所示。

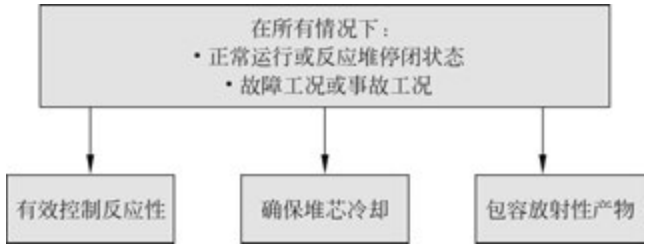


图 1-1 安全功能类型

从图 1-1 可以看出，设置反应堆控制系统、反应堆保护系统和专设安全措施，以确保反应堆在所有情况下，具备有效地控制堆芯反应性、确保堆芯有效冷却和确保包容放射核素不向外释放等 3 项功能。

2. 反应性的控制

1）目的

初始较多装料使堆芯在寿命初期具有足够多的剩余反应性，使其能够在反应堆运行过程中，补偿反应性的损失。

2）初始装料特点

在反应堆运行过程中，由于燃料的不断消耗和裂变产物的不断生成，反应堆初始装料比维持临界所需量要多。堆芯寿期的长短通常取决于反应堆初始装料量。当然，反应堆的燃料量也部分取决于其控制元件所能补偿的剩余反应性量。

3）剩余反应性补偿途径

通过在堆芯内引入适量的可随意调节的负反应性而实现。

4）可控负反应性的功能

（1）补偿堆芯长期运行所需剩余反应性。

（2）调节反应堆功率水平。

（3）停堆的手段。

3. 确保堆芯冷却

1）目的

为了避免过热引起燃料元件的损坏，任何情况下都必须确保对堆芯的冷却，导出核燃料所释放的能量。

2）反应堆堆芯冷却工况

反应堆堆芯冷却的工况如表 1-1 所示。

表 1-1 反应堆堆芯冷却的工况

工况	系统或设备	热 阱
正常运行	蒸汽发生器	正常给水 辅助给水及蒸汽旁路系统
机组停运	第 1 阶段：蒸汽发生器	辅助给水及蒸汽旁路系统
	第 2 阶段：余热排出系统	设备冷却水系统、重要厂用水系统
事故工况	蒸汽发生器	辅助给水及蒸汽旁路系统
	余热排出系统	设备冷却水系统、重要厂用水系统
	安全注射系统	换料水箱
	安全壳喷淋系统	换料水箱、设备冷却水系统、重要厂用水系统
乏燃料组件的冷却	反应堆换料水池及乏燃料水池冷却净化系统	设备冷却水系统、重要厂用水系统

4. 包容放射性产物

1）目的

为避免放射性产物扩散到环境中去，在核燃料和环境之间，设置了多道屏障，从而包容放射性产物。

2）设置的多道屏障

多道屏障一般指燃料包壳、反应堆压力壳、安全壳这 3 道屏障；或者加上燃料棒自身这 4 道屏障。在核燃料和环境之间，设置的多道屏障如图 1-2 所示。

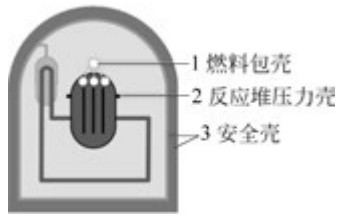


图 1-2 核燃料与环境之间的多重屏障

从图 1-2 可以看出，运行时，必须严密监视这些屏障的密封性，确保公众与环境免受放射性危害。

1.1.6 数学物理模型

1. 中子输运方程(neutron transport equation)

数学物理模型是用于理解和预测核反应堆的行为,确保其安全性和效率的关键工具。中子输运方程描述了中子在核反应堆内的行为,包括它们的生成、散射、吸收和逃逸。它是一个六维(空间、方向、能量、时间)方程,描述了不同能量和方向的中子通量的分布。该方程考虑了中子源、散射源、吸收,以及中子的逃逸,用于计算反应堆内的中子通量分布,从而预测反应堆的功率分布和反应性。

当中子角通量密度变化不大时,玻尔兹曼输运方程可以近似为扩散方程:

$$\phi(r)=-\nabla D(r)\nabla f(r)+\Sigma_{a}(r)f(r) \tag{1-2}$$

其中,D 是扩散系数,cm^2/s;ϕ 是中子通量密度,中子/($cm^2\cdot s$);Σ_a 是吸收截面,cm^2。

2. 点堆动力学方程(point kinetics equation)

核反应堆的点堆动力学方程是描述中子动力学的基本方程,用于研究反应堆功率随时间的变化行为。该方程通过考虑瞬发中子与缓发中子的耦合作用,描述反应堆功率随时间的变化过程,是研究反应堆动态行为、设计控制系统,以及进行瞬态分析的核心工具。点堆动力学方程如下:

$$\frac{dP(t)}{dt}=\frac{[\rho(t)-\bar{\beta}(t)]}{\Lambda}P(t)+\sum_{i=1}^{6}\lambda_i C_i(t)+\tilde{S}_{e}(t) \tag{1-3}$$

$$\frac{dC_i(t)}{dt}=\frac{\bar{\beta}(t)}{\Lambda}P(t)-\lambda_i C_i(t),\quad i=1,2,\cdots,6 \tag{1-4}$$

其中,$P(t)$是瞬时中子密度或反应堆功率(与中子密度成正比),W;$\rho(t)$是反应性,表示系统的中子倍增因子的变化,$\Delta k/k$;β 是总缓发中子分数,表示缓发中子占中子总数的比例;Λ 是中子寿命,表示从中子生成到下一次裂变所需的平均时间,s;$C_i(t)$是缓发中子前驱物浓度,1/m;λ_i 是缓发中子前驱物的衰变常数,1/s;S_e 是外中子源项,中子数/($m^3\cdot s$)。

3. 热工水力学模型(thermal-hydraulics models)

热工水力学模型通过纳维-斯托克斯方程和质能守恒方程,描述了冷却剂在反应堆中的流动和热传递过程。它包括流体力学和热力学方程,考虑了冷却剂的流动、压力、温度、相变等物理现象,以及湍流、热对流、导热和多相流动等复杂现象。该模型用于评估冷却剂的温度分布、压力降,以及在事故条件下的冷却能力。流动换热模型表达式如下:

$$q=hA(T_s-T_f) \tag{1-5}$$

其中,q 为对流换热量,W;h 为对流换热系数,W/($m^2\cdot K$);A 为换热表面积,m^2;T_s 为固体表面的温度,K;T_f 为流体温度,K。

4. 燃料行为模型(fuel behavior models)

燃料行为模型描述了燃料元件在反应堆内的热、机械和化学行为,包括燃料芯块的膨胀、裂变气体释放、燃料包壳的蠕变和失效等。这些行为影响燃料的温度分布和机械完整性。用于评估燃料元件的完整性和寿命,预测燃料芯块的温度分布和可能的故障模式。

5. 辐射屏蔽与防护模型(radiation shielding and protection models)

辐射屏蔽与防护模型用于评估和设计防护屏蔽物,以减少辐射暴露。模型考虑了不同类型辐射(中子、γ射线等)的衰减和散射过程,以及屏蔽物材料的吸收和反散射效应。该模型涉及辐射传输方程和蒙特卡罗(Monte Carlo)方法,计算辐射在不同材料中的衰减。

辐射传输方程描述了辐射(如γ射线、X射线等)在通过物质时的衰减过程。这个方程通常采用指数衰减的形式,称为朗伯-比尔定律(Lambert-Beer law),其表达式如下:

$$I(I_0,x)=I_0\mathrm{e}^{-\mu x} \tag{1-6}$$

其中,I 是经过距离 x 后的辐射强度,mSv/h;I_0 是辐射的初始强度,即在 $x=0$ 处的强度,mSv/h;μ 是线性衰减系数(也称为线性吸收系数),是一个与辐射类型和介质性质有关的常数,1/cm;x 是辐射在介质中传播的距离,cm。

蒙特卡罗方法用于模拟辐射,在复杂几何体内的传输和散射。通过统计方法,估计辐射的剂量分布。

6. 严重事故分析模型(severe accident analysis models)

严重事故分析模型用于模拟极端工况下,核反应堆的事故进程,如堆芯熔化、压力容器破损等。模型考虑了多相流动、化学反应、热力学平衡等复杂过程,用于评估事故后果,设计事故管理措施和应急响应策略。

7. 概率安全评价(probabilistic safety assessment,PSA)模型

概率安全评价模型(PSA模型)用于评估核电站在各种事故情况下的安全性。它通过分析可能的事故序列、故障树和事件树,评估事故发生的概率及其后果。这种分析帮助识别和量化系统中的潜在风险,优化安全设计和应急策略。

1.1.7 安全文化

1. 源起与价值

1) 源起

1986年,国际原子能机构(International Atomic Energy Agency,IAEA)之国际安全咨询组(International Nuclear Safety Advisory Group,INSAG)在《切尔诺贝利核事故后评审会议总结报告》中,首次引出“安全文化”一词。1988年,国际安全咨询组在《核电安全的基本原则》中把安全文化概念作为一种管理原则,要求“实

现安全目标必须渗透到为核电厂所进行的一切活动中去”。1991 年，国际安全咨询组出版《安全文化》一书，深入概括了安全文化的概念。

2）价值

三哩岛事故、切尔诺贝利事故加上福岛第一核电站事故的教训，促使人们反复认识到，无论如何先进的系统（严格审批、纵深防御、多道实体屏障和多安全系统），一旦人犯了直接或间接错误，都会引起某些设备失效，从而引发严重的核事故。同时，人的才智在查出和消除潜在的问题方面是十分有效的，这一点对安全有着积极的影响。安全文化的提出，为解决人因问题提供了一条可能的途径。

2. 内涵与要求

1）内涵

存在于单位和个人的种种特征和态度的综合，它建立超出一切之上的观念，即核电厂安全问题由于它的重要性而得到应有重视。是指从事任何与核电厂核安全相关活动的全体工作人员的献身精神和责任心。

2）要求

（1）核安全文化把每个人的工作态度和思维习惯以及单位的工作作风联系在一起。安全文化既是体制（与单位有关）问题，又是态度（与个人有关）问题，同时涉及所有核安全问题时，所应该具有的正确理解能力和应该采取的正确行动。

（2）要寻找具体办法，来检验每个人的工作态度和思维习惯等个人品质的具体表现。对现在正在拓展的人工智能也要如此，人工智能也需要正确的核安全文化理念。

（3）必须以高度的警惕性、实时的见解、丰富的知识、准确无误的判断能力和高度的责任感，来履行所有安全重要职责。

3. 层级和表征

1）核安全文化层级

核安全文化的层级构成如图 1-3 所示。

从图 1-3 中可以看出，核安全文化的具体组成部分，即所有从事与核安全相关工作人员的参与结果，它包括核电厂员工、核电厂管理人员及政府决策层。一是单位内部必要体制和管理部门的逐级责任制；二是各级人员响应上述体制并从中受益所持的态度。

2）优良核安全文化表征

（1）核安全文化应该表现为一整套科学而严密的规章制度，加上全体员工的自觉性和良好的工作习惯，从而在整个核电厂内形成人人自觉关注安全的氛围。

（2）工作人员不仅要具备良好的工作方法，而且要具有高度的警惕性、实时的