核安全导则　HAD102/03-2025

核动力厂构筑物、系统和部件的安全分级

（国家核安全局2025年9月18日批准发布）

国家核安全局

核动力厂构筑物、系统和部件的安全分级

（2025 年 9 月 18 日国家核安全局批准发布）

本导则自 2025 年 9 月 18 日起实施

本导则由国家核安全局负责解释

本导则是指导性文件。在实际工作中可以采用不同于本导则的方法和方案，但必须证明所采用的方法和方案至少具有与本导则相同的安全水平。

目 录

1 引言

1.1 目的

1.1.1 本导则是对HAF102《核动力厂设计安全规定》（以下简称《规定》）中有关条款的说明和细化，其目的是为划分核动力厂安全重要的构筑物、系统和部件[1]的安全功能和安全等级提供指导。

1.1.2 本导则的附录A为参考性文件。

1.2 范围

1.2.1 本导则适用于核动力厂寿期内所有安全重要构筑物、系统和部件的设计，也可用于维修活动中的物项采购与更换的指导。

1.2.2 本导则提出的方法主要适用于为发电或其它供热应用（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。核动力厂也可采用其它分级方案，但必须论证满足《规定》的要求。对于其他类型的核动力厂，其物项安全分级可参考本导则。

1.2.3 核动力厂安保方面的分级不在本导则的范围之内。

2 安全功能

2.1 概述

2.1.1 《规定》确定了基本安全目标，即在核动力厂中建立并保持对放射性危害的有效防御，以保护人与环境免受放射性危

[1] 本导则中也采用“物项”代指构筑物、系统、部件或零件（包括耗材等）。

害。为了实现基本安全目标，《规定》要求必须采取以下措施：

（a）控制在运行状态下对人员的辐射照射和放射性物质向环境的释放；

（b）限制导致核动力厂反应堆堆芯、乏燃料、放射性废物或任何其他辐射源失控事件发生的可能性；

（c）如果上述事件发生，减轻这些事件产生的后果。

2.1.2 安全分级的目的在于根据物项在预防和缓解核动力厂正常运行、预计运行事件和事故工况下的放射性后果方面的作用，对实现基本安全目标所需的那些构筑物、系统和部件进行识别和分级。确定安全等级的依据是物项在以下三项基本安全功能中的作用：

（a）控制反应性；

（b）排出堆芯余热，导出乏燃料贮存设施所贮存燃料的热量；

（c）包容放射性物质、屏蔽辐射、控制放射性的计划排放，以及限制事故的放射性释放。

2.1.3 安全功能是为了保证设施或活动能够预防和缓解核动力厂正常运行、预计运行事件和事故工况下的放射性后果，保证安全而必须达到的特定目的。安全功能包括基本安全功能和任何预期用来确保完成基本安全功能的那些具体安全功能。

2.1.4 根据情况可以适当利用为正常运行而设置的构筑物、系统和部件，或为防止预计运行事件发展为事故工况或为减轻事故工况的后果而设置的构筑物、系统和部件来实现这些具体安全功能。

2.2 安全功能条目

2.2.1 基于典型的核动力厂设计，用于正常运行、预计运行事件和设计基准事故的典型安全功能[2]划分如下：

（a）防止发生不可接受的反应性瞬变；

（b）在所有停堆动作完成后，将反应堆保持在安全状态；

（c）按要求关停反应堆以防止预计运行事件发展为设计基准事故工况和减轻设计基准事故工况的后果；

（d）在所有运行工况期间和之后，保持足够的反应堆冷却剂装量用以冷却堆芯；

（e）在设计基准事故工况期间和之后，保持足够的反应堆冷却剂装量用以冷却堆芯；

（f）在反应堆冷却剂系统压力边界失效之后，从堆芯排出热量[3]以限制燃料损坏；

（g）在反应堆冷却剂系统压力边界完整的情况下，在预计运行事件或设计基准事故工况期间，从堆芯排出余热[3]；

（h）将其他安全系统的热量转移到最终热阱[4]；

（i）作为一种支持性功能，为安全系统提供必要的公用设施（如电、气、液压、润滑等）；

（j）保持堆芯内的燃料包壳可接受的完整性；

（k）保持反应堆冷却剂系统压力边界的完整性；

（l）在设计基准事故工况期间和之后，限制放射性物质从

[2] 4.2 给出了各典型安全功能的示例。另外，本导则中“安全功能（*）”的表述，即指按 2.2.1 和 2.2.2 编号的对应安全功能条目。

[3] 本条安全功能适用于排热系统的第一步（即从堆芯排出热量）。排热系统的其余各步（即从其它安全系统排出热量）均划归安全功能（h）。

[4] 当要求其它安全系统执行安全功能时，本条目可作为这些系统的支持功能。

反应堆安全壳内向环境释放；

（m）在反应堆安全壳以外发生放射性物质释放的设计基准事故工况期间和之后，使公众和厂区人员受到的辐射照射保持在可接受的限值以内；

（n）在所有运行状态下将放射性废物和气载放射性物质的排放或释放限制在规定限值以内；

（o）通过合理控制核动力厂厂区内的环境状况，保证各安全系统的运行和人员的可居留性，以便执行安全重要操作；

（p）在预计运行事件和设计基准事故[5]期间，对在反应堆冷却剂系统以外，但仍在厂区以内运输或贮存中的辐照过的燃料的放射性释放进行控制；

（q）在预计运行事件和设计基准事故期间从贮存在反应堆冷却剂系统以外，但仍在厂区以内的辐照过的燃料中排出衰变热；

（r）使贮存在反应堆冷却剂系统以外，但仍在厂区以内的燃料保持足够的次临界度；

（s）当某一部件或构筑物的损坏会损害某一安全功能时，防止该部件或构筑物发生损坏或限制其损坏所引起的后果；

（t）维持设计基准事故后关键参数的监测功能。

2.2.2 为了保证在核动力厂所有状态下实现三项基本安全功能，核动力厂的设计除了必须考虑正常运行、预计运行事件和设计基准事故工况下基本安全功能的实现，还必须考虑设计扩展工况下基本安全功能的实现。有些设计扩展工况对大部分核动力厂设计都是适用的，如未能紧急停堆的预计运行事件、全厂断电等，

[5] 燃料相关要求见HAD 102/15《核动力厂燃料装卸和贮存系统设计》。

此外，还需要根据核动力厂的设计确定其他可能的设计扩展工况。用于设计扩展工况的典型安全功能示例如下：

（t_1）为实施严重事故管理指南的核动力厂重要参数监测[6]；

（u）应对全厂断电；

（v）应对未能紧急停堆的预计运行事件；

（w）设计扩展工况下控制安全壳内温度和压力；

（x）堆芯熔融物的堆内或堆外滞留；

（y）防止高压堆芯熔融物的喷射；

（z）控制严重事故下安全壳内可燃气体浓度等。

2.3 安全功能的应用

2.3.1 在 2.2 中所列的安全功能条目可用来实现下述目的：

（a）提供一张参考的安全功能条目表，作为确定某一构筑物、系统和部件能否执行或有助于执行某一项或几项安全功能的基础；

（b）根据所考虑的特定安全功能的最终用途，先将每项功能按其对安全的重要性进行排序，然后按照这一排序对这些功能进行分组，每组称为一个“安全等级”。

2.3.2 有关安全分级的一般要求在第 3 章讨论。国际上实践较多的以确定论为主的安全分级方法在第 4 章讨论。划分安全等级的一个目的是确定物项的设计要求，第 5 章讨论了构筑物、系统和部件工程设计规则的选择。在确定论安全分级的基础上，核动力厂营运单位可以选用附录 A 的风险指引型安全分级方法对

[6] 设计基准事故的监测功能条目和设计扩展工况的监测功能条目编号都用字母 t，但设计扩展工况的监测功能条目设为 t_1 以示区分。

确定论安全分级的特殊处理要求[7]进行适当调整。

3 安全分级的要求

3.1 通用要求

3.1.1 安全分级过程由定义核动力厂假设始发事件开始，向下延伸到核动力厂中预防和缓解这些假设始发事件的安全功能，以及执行这些安全功能的构筑物、系统和部件，直至零件（包括耗材等），对这些安全功能和物项进行分级。

3.1.2 安全分级应在整个设计过程中进行反复迭代，并应在整个核动力厂寿期内得以保持。应在安全分级过程中考虑新的或变更的假设始发事件以及构筑物、系统和部件，并考虑其与可能受到影响的构筑物、系统和部件的现有安全功能和安全分级的接口。

3.1.3 安全分级宜考虑在纵深防御各个不同层次中执行的安全功能。

3.1.4 安全分级的依据和分级结果应形成可供审查的文件。构筑物、系统和部件的最终分级文件应是完整的，并可供审查。由于分级可能受到核动力厂后续（在核动力厂运行寿期内）设计变更影响，分级文件应作为核动力厂配置管理的一部分。

3.1.5 安全分级应规定并遵守不同构筑物、系统和部件之间接口的规则，并在分级文件中明确不同安全等级构筑物、系统和

[7] 特殊处理要求是指超出正常商业和工业实践的要求，以提供合理的保证确保核动力厂的构筑物、系统和部件能够在设计基准工况下执行其设计基准安全功能。这些特殊处理要求包括设计考虑、鉴定、变更控制、文档、报告、维护、测试、监察和质量保证等。

部件之间的接口。

3.2 安全等级划分的要求

3.2.1 物项在减少核动力厂总体风险方面的贡献或安全重要性是划分安全等级的重要因素。根据《规定》的要求，划分安全重要物项的安全重要性的方法，应主要基于确定论方法，酌情辅以概率论方法，并适当考虑以下因素：

（a）该物项要执行的安全功能；

（b）未能执行其安全功能的后果；

（c）需要该物项执行某一安全功能的可能性；

（d）假设始发事件发生后，需要该物项执行某一安全功能的时间点或时间段。

3.2.2 在 3.2.1 中所述的四项因素，因素（a）指在为实现三项基本安全功能所必需的那些功能中，该物项实际承担的功能；因素（b）考虑该安全功能失效时可能增加的辐射照射剂量的大小；因素（c）考虑要求执行该安全功能的可能性；因素（d）涉及到使核动力厂达到可控状态和安全状态的功能[8]。在排列安全功能的顺序时，应同时考虑安全功能失效的后果、要求执行该安全功能的可能性及核动力厂状态。

3.2.3 安全功能失效的后果只考虑该安全功能失效时可能增加的辐射照射剂量的大小。一般而言，当分析表明某一安全功能的失效后果很严重时，该安全功能即排到前列。例如，安全功能（k）失效的后果可能很大；相反，安全功能（n）失效的后果可能是小的，因此将安全功能（k）排列到安全功能（n）的前面。

[8] 可控状态和安全状态的定义见 HAF102 的名词解释。

3.2.4 对于要求执行该安全功能的可能性，比较安全功能（k）和（f）有助于说明这个问题。安全功能（k）失效的后果可能很大。同样，安全功能（f）失效的后果也可能很大。然而，只有在某种事故发生后才要求执行安全功能（f）。若不发生该种事故，安全功能（f）即使失效也不会导致辐射照射的增加，而安全功能（k）在核动力厂的任何状态下都需要保证。因此将安全功能（f）排列在安全功能（k）的后面。

3.2.5 核动力厂状态只考虑使核动力厂达到可控状态或安全状态的紧迫程度。对于事故发生后需要短时优先投入的功能，其安全等级要高于用于事故长期状态投入的功能。例如安全功能（f）和（h），安全功能（f）主要指事故发生后优先从堆芯排出热量，而安全功能（h）则主要指排出其它安全系统的热量，其紧迫程度没有排出堆芯热量那么高。因此，将安全功能（f）排列在安全功能（h）的前面。

3.2.6 对系统内的多样性和多重性[9]，例如某些安全功能可能由多个系统来完成，当采用以确定论为主的安全分级方法时，不考虑可能由多个系统来完成某一特定安全功能的情况，只有被专门规定用来完成该特定安全功能的系统内的部件，其设计才必须满足该指定系统的安全分级要求。一般来说，在分级时不再考虑某个特定的系统内部设计的多重性（即在规定须完成某一安全功能的系统以内，多重部件一律划入为该安全功能指定的那一安全等级）。

[9] 多样性的定义见 HAF102 的名词解释。多重性指为完成一项特定安全功能而采用多于最少套数的设备，它是达到安全重要系统高可靠性和满足单一故障准则的重要设计原则。

3.2.7 任一系统在完成其指定的安全功能时，必定有一些部件起主要作用，该系统内的其他有关部件则用于试验、维修、运行人员培训或与该系统的安全功能无直接关系的目的。只有为执行系统指定的安全功能所必需的部件（即主要部件）划分为该特定的安全等级，系统内的其它非主要部件（如用于试验、维修、运行人员培训或其它用途的那些部件）可能对安全各有其不同的重要性，因而必须根据其各自不同的重要性来进行分级。同样，在一个复杂部件内，各部分所执行的安全功能也不一定相同，因而也可以划分为不同的安全等级。

3.2.8 对执行多项安全功能的部件，其安全等级一般按等级最高的安全功能划分。

3.2.9 若安全等级较低的系统或部件失效时会妨碍安全等级较高的安全功能的完成，则必须在相连的两系统或两部件之间设置合适的接口。接口部件的安全等级必须和较高安全等级的部件一致。

3.2.10 部件失效的可能性受到该部件设计要求的影响。理论上，设计要求越严格，部件失效的可能性就越小。因此，对排列在最前列的各安全功能及其所属安全等级的设计要求最严格；安全等级较低时，设计要求也较低。

3.3 安全等级的数目

3.3.1 建立安全等级的目的是为制订一套分级的设计要求提供基础。对于 2.2 中列举的每条安全功能，理论上都能规定不同的设计要求，但这对确定部件的设计要求来说并不实用，而切实可行的办法是将这些安全功能组合为若干个安全等级，每个安全

等级中的诸安全功能被视为对安全均具有同等的重要性；然后再将各安全等级按其对安全的重要性顺序排列，并对每一安全等级规定不同的要求。核动力厂应根据其设计特点设置合适数目的安全等级。安全等级过多，会给设计和工程带来不必要的复杂性；安全等级过少，可能会导致对安全重要性低的物项提出过严的要求。

3.3.2 不同专业领域的物项，安全等级数目可能不同。如不同堆型大量实践的结果表明，为确定流体包容部件边界的设计要求将安全等级分为四级是行之有效的。安全一级对安全的重要性最大，应采用最严格的标准和规范。安全二、三、四级的重要性依次递减。

4 安全分级方法

4.1 概述

4.1.1 本章所述安全分级方法主要基于确定论，通过关注事故类型、放射性物质的释放和后果来对物项进行分级。该安全分级方法在排列安全功能顺序时所作的判断反映了对大量假设事故进行分析的结果，涵盖了压水堆核动力厂绝大部分构筑物、系统和部件。

4.1.2 核动力厂的构筑物、系统和部件分为安全级和非安全级两大类。在正常运行、预计运行事件和设计基准事故期间及之后，为实现三项基本安全功能中的任一功能所必需的构筑物、系统和部件为安全级，用 SC（Safety Class）表示；其余构筑物、系统和部件为非安全级，用 NC（Non-Safety Class）表示。

在非安全级中应识别出有附加要求的安全有关物项，即对安全重要但不属于安全级的物项，用 NC（S）（Non-Safety Class with Special Requirement）表示。安全有关物项的附加要求应在设备规格书中说明，4.2~4.5 给出不同类别 NC（S）部件的定义和示例，其中包含了对可能的附加要求的考虑。

安全级物项和安全有关物项共同组成安全重要物项，其余为非安全重要物项。

4.1.3 核动力厂不同类别构筑物、系统和部件的安全等级划分及其代号见表 1。

表 1 不同类别构筑物、系统和部件的安全等级及其代号

<table>
<tr><th>物项类别</th><th colspan="5">安全等级及其代号</th></tr>
<tr><td rowspan="2">所有物项</td><td colspan="4">安全重要物项</td><td>非安全重要物项</td></tr>
<tr><td colspan="3">安全级　SC</td><td colspan="2">非安全级　NC</td></tr>
<tr><td>流体包容部件</td><td>安全1级
SC-1</td><td>安全2级
SC-2</td><td>安全3级
SC-3</td><td>安全有关
NC（S）</td><td>NC</td></tr>
<tr><td>非流体包容部件</td><td colspan="3">安全级　SC</td><td>NC（S）</td><td>NC</td></tr>
<tr><td>电气仪控部件</td><td colspan="3">安全级　SC（1E）</td><td>NC（S）</td><td>NC</td></tr>
<tr><td>构筑物</td><td colspan="3">安全级　SC</td><td>NC（S）</td><td>NC</td></tr>
</table>

4.1.4 本章给出的分级规则主要基于确定论方法，随着概率安全评价技术在核动力厂中的应用日益广泛，形成基于概率风险视角的风险指引型安全分级方法（见附录 A）。核动力厂营运单位可以选用风险指引型安全分级方法对确定论安全分级的特殊处理要求进行适当调整。

4.2 流体包容部件的安全分级

4.2.1 在 4.2 中所述内容适用于包容流体的压力容器、热交换器、管道、泵、阀门、管道附件，包括低压和常压贮罐。对流体包容部件，传统上安全分级主要考虑包容放射性的大小，一回

路压力边界包容放射性最大（最接近堆芯），为安全 1 级（SC-1）；设计基准事故条件下包容放射性物质的专设安全设施以及紧邻一回路的二回路部分，为安全 2 级（SC-2）；除 SC-1 和 SC-2 物项外，其他在预计运行事件和设计基准事故工况下执行安全功能的物项为安全 3 级（SC-3）。

4.2.2 SC-1 指构成反应堆冷却剂压力边界、其失效会导致反应堆冷却剂丧失事故且无法通过正常补水功能补偿泄漏的机械部件及其主支承件。

安全功能（k）所对应的物项应定为 SC-1，但以下情况除外，即属于反应堆冷却剂压力边界但其失效导致的反应堆冷却剂丧失可以通过正常的补给系统进行补偿的物项，这部分物项应定为 SC-2。

4.2.3 SC-2 包括以下安全功能。

（a）为减轻某一设计基准事故后果所必需的安全功能，如果没有这些安全功能的作用，该设计基准事故可能导致大部分堆芯裂变产物释放到环境中。只有在另一安全功能初始失效后才有必要考虑这些属于 SC-2 安全功能失效的后果。

（b）为防止预计运行事件发展为设计基准事故工况所必需的那些安全功能，但是不包括只对另一安全功能起支持作用的那些安全功能，如 2.2.1 中的安全功能（h）、（i）和（o）。

（c）其失效的后果与要求执行这些安全功能的可能性的乘积可能很大的安全功能，如反应堆余热的排出。

安全功能（k）（反应堆冷却剂系统边界组成部分内不属于

SC-1 的那些部件）、（c）、（e）、（f）、（g）、（l）[10]对应的机械物项的流体包容部分及其主支承件应定为 SC-2。

4.2.4 SC-3 包括以下安全功能。

（a）对 SC-1、SC-2、SC-3 中的安全功能起支持作用的所有安全功能，即 2.2.1 中的安全功能（h）、（i）和（o）。由于认识到这些支持功能的失效不会直接引起辐射照射增大的后果，所以将它们划入 SC-3 而不划入 SC-1 或 SC-2。

（b）为防止反应堆冷却剂系统以外的放射源对公众和厂区人员产生超过可接受限值的辐射照射所必需的安全功能。

（c）设计基准事故工况下与反应性控制相关的安全功能，其时间尺度比 SC-1、SC-2 中的反应性控制功能慢。

（d）这样一些安全功能，它们的作用是使贮存在反应堆冷却剂系统以外的燃料保持在次临界状态或是排出贮存在反应堆冷却剂系统以外的辐照过的燃料所发出的衰变热。

安全功能（a）、（b）、（d）、（h）、（i）、（m）、（o）、（p）、（q）、（r），以及（n）（该功能所对应的包容放射性物质的部件，其失效会导致放射性物质释放超过规定限值）对应的机械物项的流体包容部分及其主支承件应定为 SC-3。

4.2.5 未列入 SC-1、SC-2、SC-3 的流体包容部件为 NC。在 NC 中，由安全功能（n）、（s）等功能所对应的包容放射性物质（其失效不会导致放射性物质释放超过规定限值）的部件、其失

[10] 安全功能（l）可通过综合利用安全壳壳体和这样一些部件来实现，这些部件能执行下列一种或几种功能：

（ⅰ）能限制从安全壳内向外泄漏；

（ⅱ）在事故工况期间和之后，降低安全壳壳体内环境的温度和压力；

（ⅲ）在事故工况期间和之后，排除安全壳内的放射性物质和控制其氢浓度。

效可能影响安全级物项功能的部件，以及属于某个特殊事件（如未能紧急停堆的预计运行事件、全厂断电和火灾）所依赖的部件应定为 NC（S）。用于设计扩展工况的安全功能〔如（t_1）到（z）〕所对应的流体包容部件定为 NC（S）。

4.2.6 表 2 提供了压水堆流体包容部件分级的示例。

表 2 压水堆流体包容部件分级示例

安全等级	安全功能	功能描述	部件示例
SC-1	k	保持反应堆冷却剂系统压力边界的完整性	· 反应堆冷却剂系统部件，包括：反应堆压力容器，主管道和延伸到并包括第二道隔离阀的连接管线，控制棒驱动机构的壳体，主泵压力边界，稳压器和波动管，反应堆冷却剂系统安全阀、卸压阀及其与稳压器相连的管道，蒸汽发生器一次侧； · 非能动安全系统压水堆核动力厂的应急堆芯补水箱、非能动余热排出热交换器。
SC-2	k	保持反应堆冷却剂系统压力边界的完整性	· 反应堆冷却剂压力边界部件中不属于 SC-1 的部件，即其失效导致的反应堆冷却剂丧失可以通过正常的补给系统进行补偿的物项，如连接到反应堆冷却剂系统上的仪表管线和取样管线（直至并包括作为反应堆冷却剂系统压力边界的隔离阀）。
SC-2	c	按要求关停反应堆以防止预计运行事件发展为设计基准事故工况和减轻设计基准事故工况的后果	· 事故后将硼酸注入反应堆冷却剂系统或应急堆芯冷却系统所必需的部件。
SC-2	e	在设计基准事故工况期间和之后，保持足够的反应堆冷却剂装量用以冷却堆芯	· 提供应急堆芯冷却的部件，如安注系统的部件。
SC-2	f	在反应堆冷却剂系统压力边界失	· 提供应急堆芯冷却的部件，如安注系统的部件。

		效之后，从堆芯排出热量以限制燃料损坏	
SC-2	g	在反应堆冷却剂系统压力边界完整的情况下，在预计运行事件或设计基准事故工况期间，从堆芯排出余热	· 余热排出系统的部件； · 蒸汽和给水系统的这一部分：始于并包括蒸汽发生器二次侧，直至并包括最外的安全壳隔离阀；以及与之相连接的支管，直至并包括反应堆运行状态下常闭的或能够自动关闭的第一道阀门（如一个安全阀或释放阀）； · 为反应堆冷却剂系统提供自然循环冷却所必需的部件。
SC-2	l	在设计基准事故工况期间和之后，限制放射性物质从反应堆安全壳内向环境释放	· 安全壳及其隔离系统的部件； · 事故后安全壳排热系统（如安全壳喷淋系统）的部件； · 事故后排除安全壳内空气中放射性物质和控制氢浓度的部件。
SC-3	a	防止发生不可接受的反应性瞬变	· 为补偿堆芯反应性和在预计运行偶发事件期间和之后，向反应堆冷却剂系统注入或从中排出硼酸所必需的反应堆辅助系统的部件。
SC-3	b	在所有停堆动作完成后，将反应堆保持在安全状态	· 应急硼注入系统的部件。
SC-3	d	在所有运行工况期间和之后，保持足够的反应堆冷却剂装量用以冷却堆芯	· 正常运行工况期间和之后，为维持足够的反应堆冷却剂或应急给水装量以进行堆芯冷却所必需的反应堆辅助系统的部件，如化学和容积控制系统。
SC-3	h	将其他安全系统的热量转移到最终热阱	· 冷却系统的部件，包括：中间冷却系统，厂用水系统，应急冷却水池，冷却塔或空气热交换器等。
SC-3	i	作为一种支持性功能，为安全系统提供必要的公用设施（如电、气、液压、润滑等）	· 为提供厂内应急电源所必需的部件，如柴油机燃料贮罐和输油泵； · 安全重要部件和系统（例如反应堆冷却剂泵、应急柴油发电机以及控制室）运行所需的安全重要冷却水和密封水系统及其部件。
SC-3	m	在反应堆安全壳以外发生放射性物质释放的设计基准事故工况期间和之后，使公众	· 用于控制和去除放射性物质的空气过滤系统，如屏蔽建筑物、乏燃料厂房或双层安全壳环形空间空气过滤系统中为事故后控制和排除放射性物质的部件。

		和厂区人员受到的辐射照射保持在可接受的限值以内	
SC-3	o	通过合理控制核动力厂厂区内的环境状况，保证各安全系统的运行和人员的可居留性，以便执行安全重要操作	· 为安全系统安全操作和运行人员居留所必需的空调和净化系统的部件，如控制室通风系统和应急柴油发电机房的空调系统的部件，电气厂房冷冻水系统等。
SC-3	p	在预计运行事件和设计基准事故期间，对在反应堆冷却剂系统以外，但仍在厂区以内运输或贮存中的辐照过的燃料的放射性释放进行控制	· 预计运行事件和设计基准事故期间为排除辐照过燃料贮存厂房空气中的放射性物质所必需的部件。
SC-3	q	在预计运行事件和设计基准事故期间从贮存在反应堆冷却剂系统以外，但仍在厂区以内的辐照过的燃料中排出衰变热	· 冷却辐照过的燃料所必需的部件，如乏燃料池冷却系统的部件。
SC-3	r	使贮存在反应堆冷却剂系统以外，但仍在厂区以内的燃料保持足够的次临界度	· 为将硼酸注入乏燃料池所必需的辅助系统的部件。
SC-3	n	在所有运行状态下将放射性废物和气载放射性物质的排放或释放限制在规定的限值以内而设置的那些部件。如果这些部件失效将使公众或厂区人员的辐射照射超过规定的限值	· 放射性废物管理系统的部件，如废气处理系统。

NC（S）	n	在所有运行状态下将放射性废物和气载放射性物质的排放或释放限制在规定限值以内而设置的那些部件。如果这些部件失效，不会使公众或厂区人员的辐射照射超过规定的限值	· 放射性废物管理系统的部件，如废气处理系统； · 从乏燃料贮存池冷却系统清除放射性物质的部件； · 已辐照的中子吸收材料（如硼化合物）的再利用所需的贮存、运输和工艺处理部件。
NC（S）	s	当某一部件或构筑物的损坏会损害某一安全功能时，防止该部件或构筑物发生损坏或限制其损坏所引起的后果	· 与安全系统部件邻近的蒸汽管线和水管部件。
NC（S）	u	应对全厂断电	· 应对全厂断电的柴油发电机的流体包容部件； · 电气厂房冷冻水系统的风冷系列部件。
NC（S）	v	应对未能紧急停堆的预计运行事件	· 应急硼注入系统的部件； · 提供触发停堆和专设安全设施动作功能的多样化驱动。
NC（S）	w	设计扩展工况下控制安全壳内温度和压力	· 非能动安全壳热量导出系统部件。
NC（S）	x	堆芯熔融物的堆内或堆外滞留	· 堆腔注水冷却系统部件。
NC（S）	y	防止高压堆芯熔融物喷射	· 快速卸压管线。

4.3 非流体包容部件的安全分级

4.3.1 非流体包容部件包括反应性控制、应急通风、正常通风、核空气和气体净化、燃料操作等系统的部件。本节也适用于包容水和（或）蒸汽的热交换器、泵和阀门的内部功能构件或动力传动部件。

4.3.2 非流体包容部件中执行安全功能的物项应定为安全级，

如安全功能（j）对应的机械物项等。这类物项的示例如下：

（a）堆内构件；

（b）控制棒驱动机构（耐压壳除外，见4.2.3）；

（c）为保证控制室运行人员居留和安全系统运行所需要的暖通空调、空气净化系统的部件，包括主控室、应急柴油发电机厂房等场所的空气调节、通风系统的主要部件；

（d）安全级部件的主支承件（在4.2中已分级的除外）；

（e）主泵的转轴、叶轮和飞轮；

（f）蒸汽发生器的抗振条。

4.3.3 未列入安全级的部件为NC。在NC中应识别出NC（S）部件。用于设计扩展工况的安全功能〔如（t_1）到（z）〕所对应的非流体包容部件定为NC（S）。

4.3.4 NC（S）部件的示例：

（a）未列入安全级，用于为厂区人员或为安全级部件提供保护、屏蔽的部件；

（b）其失效可能导致安全级物项失效的部件；

（c）新燃料贮存格架；

（d）内部危险发生时保护安全级物项（以确保能够停堆和维持安全状态）的部件。

4.4 电气仪控部件的安全分级

4.4.1 在4.4中所述内容适用于电气部件、仪控部件。

4.4.2 电气仪控部件的安全分级是一种功能性的分级，这种分级只是对冗余度、丧失厂外电源时的操作、电磁兼容、安全级软件以及在使用环境和地震情况下的质量鉴定规定了要求。

4.4.3 电气仪控部件可分为安全级（1E）和非安全级（NC）。预防、缓解设计基准事故以及事故期间保护公众所需的电气仪控部件应定为1E。1E电气仪控部件用于保证紧急停堆、安全壳隔离、应急堆芯冷却、排出堆芯和安全壳热量、防止和限制放射性物质向环境释放、主蒸汽管道隔离、乏燃料水池安全以及安全系统的支持功能。

1E 电气仪控部件完成的主要功能示例如下：

——反应堆紧急停堆：安全功能（c）；

——安全壳隔离：安全功能（l）；

——应急堆芯冷却：安全功能（a）、（e）、（f）、（j）、（k）；

——反应堆余热排出：安全功能（b）、（d）、（g）；

——反应堆厂房热量的排出：安全功能（o）；

——防止和限制放射性物质向环境释放：安全功能（l）、（m）、（n）；

——主蒸汽管道隔离：安全功能（b）、（l）；

——乏燃料水池安全：安全功能（p）、（q）、（r）；

——安全系统的支持功能：安全功能（i）、（h）、（t）。

4.4.4 1E电气仪控部件的示例：

（a）能动安全系统压水堆核动力厂厂内交流电源系统中执行安全功能的各种部件；应急柴油发电机；安注泵、余热排出泵、辅助给水泵等设备所用的电动机；应急电力系统蓄电池及其充电设备；

（b）非能动安全系统压水堆核动力厂中为安全级物项（用于紧急停堆、事故后监测和通风）提供可靠电力的直流电源和不

间断电源部件；主交流电源系统中反应堆冷却剂泵断路器；

（c）安全级的阀门电动装置，如安全壳隔离阀电动装置；

（d）反应堆保护系统，包括监测工艺系统的传感器、变送器、信号处理及表决机柜、供电机柜等；

（e）用于设计基准事故后所必需的监测装置，例如事故后安全壳辐射监测装置，事故后稳压器液位、压力监测装置；

（f）安全壳电气贯穿件。

4.4.5 未列入1E的电气仪控部件为NC。NC中应识别出NC（S）部件。用于设计扩展工况的安全功能〔如（t_1）到（z)〕所对应的电气仪控部件也定为NC（S)。

4.4.6 NC（S）部件示例：

（a）使过程变量保持在安全限值以内的控制部件；

（b）在核动力厂设计基准范围内预防、减轻较小的放射性释放（不超过限值）的部件；

（c）监测安全级系统或部件状态的部件；

（d）为安全级部件和运行人员提供可接受环境所需的且未列入安全级的电气仪控部件；

（e）监测可控排放的部件；

（f）非能动安全系统压水堆核动力厂的备用柴油发电机；

（g）用于维持设计扩展工况下关键参数监测的电气仪控部件。

4.5 构筑物的安全分级

4.5.1 在4.5中所述内容适用于钢结构、混凝土结构、水（土）工构筑物以及各类厂房。

4.5.2 以下物项应定为安全级：容纳或贮存放射性物质，其失效可能使公众或厂区人员所受照射超过规定限值的构筑物；对安全级物项起保护作用的某些构筑物。

4.5.3 安全级构筑物的示例：

（a）安全壳；

（b）主控制室、辅助控制室、安全级电气厂房；

（c）最终热阱构筑物；

（d）乏燃料贮存池；

（e）能动安全系统压水堆核动力厂的核辅助厂房、应急柴油发电机厂房；

（f）非能动安全系统压水堆核动力厂的屏蔽厂房及安全级的部分辅助厂房；

（g）安全级的预埋件。

4.5.4 未列入安全级的构筑物为NC。NC中应识别出NC（S）构筑物。

4.5.5 NC（S）构筑物的示例：容纳、贮存、处理放射性废物的贮存池、厂房等（其失效不会使公众或厂区人员所受照射超过规定限值），如核岛废液贮存罐厂房。

5 构筑物、系统和部件工程设计规则的选择

5.1 工程设计规则的总体要求

5.1.1 工程设计规则为国家或国际上的相关规范、标准和被证明的工程经验。工程设计规则应被合理地应用于构筑物、系统和部件的设计以达到相应的设计要求。

5.1.2 构筑物、系统和部件的安全分级一旦建立，就应确定和应用相应的工程设计规则。工程设计规则的选择应使得核动力厂设计满足发生可能性高的事件对公众产生很少或无不利后果，同时极端事件（具有潜在严重后果）的发生可能性极低。

5.1.3 工程设计规则与构筑物、系统和部件的下述功能性、可靠性和稳健性相关，应对这些特性进行界定，并考虑不确定性。

（a）功能性是指构筑物、系统和部件执行其所要求功能的能力。

（b）可靠性是指构筑物、系统和部件以和安全分析相符的足够低的失效可能性执行其所要求功能的能力。

（c）稳健性是指确保运行负载或假设始发事件引起的负载不会对构筑物、系统和部件执行其功能造成不利影响的能力。

5.1.4 针对已安全分级的构筑物、系统和部件，应制定一套完整的工程设计规则，以确保构筑物、系统和部件的设计、制造、建造、安装、在役、运行、试验、检查和维修等都符合适当的质量标准。为达到以上目标，设计规则应确定适当水平的功能性、可靠性和稳健性。设计规则应考虑监管机构对安全级构筑物、系统和部件制定的附加要求。

5.1.5 应用于系统的设计要求和应用于单个构筑物及部件的设计要求是不同的，应合理区分：

— 应用于系统的设计要求包括单一故障准则、冗余系列之间的独立性、多样性、可试验性等。

— 应用于单个构筑物和部件的设计要求包括环境和抗震鉴定、质量保证等。它们通常通过明确适用的规范或标准来规定。

5.1.6 核动力厂营运单位应提供和证明安全分级与工程设计规则和制造规则之间的一致性，包括应用于每一个构筑物、系统和部件的规范或标准。

5.1.7 一旦明确了构筑物、系统和部件的工程设计要求，则应验证系统执行其功能的可靠性与安全分析中假设的可靠性是一致的。

5.1.8 本章给出第 4 章所述安全分级方法的工程设计规则选择要求。

5.2 系统设计要求

系统设计要求用于确保安全重要系统在所有预期运行工况下均有适宜的功能性和可靠性，系统典型设计要求见表3，内容包括：

— 单一故障准则；

— 实体隔离和电气隔离；

— 应急供电；

— 定期试验；

— 环境鉴定；

— 内外部危险防护（包括抗震）。

表 3 系统典型设计要求

系统安全等级	单一故障准则	实体/电气隔离	应急供电	定期试验	环境鉴定	内外部危险防护（包括抗震）
SC	是	是	是	是	是	是
NC（S）	否	否[a]	逐个分析	是[b]	逐个分析[c]	逐个分析

[a] 当 NC（S）系统作为应急备用时，如果该系统可能会受到相同始发事件或事件后果的影响，则该系统应与其所备用的系统相隔离；当 NC（S）系统用于缓解内外部危险时，该系统不应受到此危险影响。

[b] 要求持续运行的情况除外。

[c] 应根据具体功能分析中所需部件运行环境确定鉴定要求。

5.3 构筑物和部件规范要求

5.3.1 对于分级为SC-1、SC-2、SC-3和SC的构筑物和部件，应采用与其安全等级相适应的核相关的设计建造规范。

5.3.2 对于分级为NC（S）的构筑物和部件，可选用合适的核相关规范或相适应的相关行业规范。

5.3.3 下面给出一些推荐的物项工程设计规则选择示例。构筑物根据安全等级采用适用的规范和标准，表4提供了构筑物安全分级和工程设计规则之间的相互对照关系。表5提供了流体包容部件安全分级和工程设计规则之间的相互对照关系。表6提供了非流体包容部件安全分级和工程设计规则之间的相互对照关系。非流体包容部件包括堆内构件、部件支承件、通风系统部件、装卸设备等可采用适用的规范和标准。表7提供了电气仪控系统和部件的安全等级与工程设计规则之间的关系。构筑物、系统和部件的抗震要求遵守核安全导则《核动力厂抗震设计与鉴定》（HAD 102/02）的规定。

表 4 构筑物安全分级和工程设计规则之间的关系

安全分级	抗震要求
SC	抗震Ⅰ类
NC（S）	逐个分析
NC	非核抗震类

表 5 流体包容部件安全分级和工程设计规则之间的关系

安全分级	规范等级	抗震要求
SC-1	规范 1 级	抗震Ⅰ类

SC-2	规范 2 级	抗震Ⅰ类
SC-3	规范 3 级	抗震Ⅰ类
NC（S）	适用标准[a]	逐个分析
NC	常规工业	非核抗震类
注 a： NC（S）流体包容部件的设计要求应与常规动力厂中最高的规范和标准一致，同时还应增加与安全重要性相适应的补充设计要求。		

表 6 非流体包容部件安全分级和工程设计规则之间的关系

安全分级	抗震要求
SC	抗震Ⅰ类
NC（S）	逐个分析
NC	非核抗震类

表 7 电气仪控系统和部件的安全等级与工程设计规则之间的关系

功能物项分级	抗震要求
1E	抗震Ⅰ类
NC（S）	逐个分析
NC	非核抗震类

附录 A 风险指引型安全分级方法

A.1 概述

A.1.1 风险指引型安全分级方法（Risk Informed Safety Classifications，RISC）主要建立在概率论方法的基础上，将概率安全分析的见解与其他工程见解相结合，根据物项对核动力厂的安全重要度，在传统的确定论分级的基础上将安全级和非安全级分别再细分为高安全重要（HSS）和低安全重要（LSS）两类（见图 A.1），并基于此对物项提出相应的要求，A.1.2~A.1.5 给出不同级别的定义。

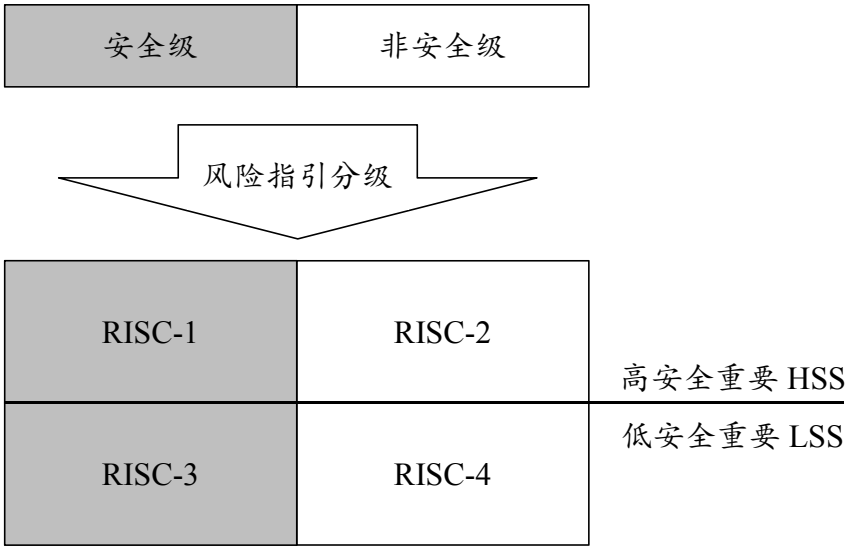

图 A.1 风险指引型安全分级示意图

A.1.2 RISC-1 是指安全级，且高安全重要的构筑物、系统和部件。在确定论安全分级中这类物项属于安全级，相关的各项特殊处理要求都很高，在风险指引型安全分级中仍然认为其具有高安全重要性，因此，其特殊处理要求不可降低。

A.1.3 RISC-2 是指非安全级，但高安全重要的构筑物、系统

和部件。在确定论安全分级中这类物项属于非安全级，对应的特殊处理要求相对较低，但它们对降低核动力厂的风险水平有着重要的贡献，因此，需加强对这类物项的特殊处理要求，以确保其能够更好地执行相关功能，提高核动力厂的安全性。

A.1.4 RISC-3 是指安全级，但低安全重要的构筑物、系统和部件。在确定论安全分级中这类物项属于安全级，具有较高的特殊处理要求，但在风险指引型安全分级中认为其安全重要性较低，较高的特殊处理要求并不能明显提高核动力厂运行的安全性，反而会增加核动力厂的成本和负担。因此，可依据相关规定豁免或降低不必要的特殊处理要求。

A.1.5 RISC-4 是指非安全级，且低安全重要的构筑物、系统和部件。在确定论安全分级中这类物项属于非安全级，其特殊处理要求相对较低，且在风险指引型安全分级中仍然认为其安全重要性较低，所以对其特殊处理要求维持原来水平即可满足其安全重要性的要求。

A.1.6 风险指引型安全分级方法包含了概率安全分析、纵深防御评价、敏感性分析和综合决策。上述各项评价应依次进行。

A.2 概率安全分析

A.2.1 开展概率安全分析之前，需要对系统开展相关评价，主要工作是鉴别和确定开展风险指引型安全分级所必需的基本信息。

A.2.2 构筑物、系统和部件的安全重要度应分别通过内部事件风险、内部水淹风险、内部火灾风险、地震风险和其它外部危险等方面进行评估。

A.2.3 如果所要分析的构筑物、系统和部件用于预防和缓解严重事故，则首先需要通过内部事件概率安全分析模型分析其风险贡献。重要度评估是从风险的角度来评价选定构筑物、系统和部件的安全重要性，若物项的重要度满足下面准则中的任一条，则该物项应定为高安全重要等级：

（a）单个构筑物、系统和部件的FV重要度[11]>0.005，取其所有基本事件（包括共因失效）FV重要度的总和；

（b）单个构筑物、系统和部件的RAW重要度[12]>2.0，取除共因失效（CCF）外基本事件（CCF基本事件单独考虑）最大的RAW；

（c）构筑物、系统和部件的共因组RAW重要度>20.0，取其所有CCF基本事件中最大的RAW。

A.2.4 对于内、外部危险（如外部水淹、强风等）的风险，如果其堆芯损坏频率（CDF）低于内部事件 CDF 的 1%，可以将其概率安全分析中考虑的构筑物、系统和部件的安全重要度视为LSS；否则，采用类似于内部事件概率安全分析的评估过程。

A.3 纵深防御评价

A.3.1 纵深防御评价通过堆芯损坏缓解、早期安全壳失效/旁通和安全壳长期完整性三个方面评估构筑物、系统和部件功能，如果任一方面判定为对纵深防御为高安全重要，则该构筑物、系统和部件即认定为 HSS。

[11] FV 重要度，就是包含基本事件 i 的最小割集的发生频率之和与全部 CDF/LERF 的比值。CDF 指堆芯损坏频率，LERF 指早期大量释放频率。

[12] RAW 重要度，就是基本事件 i 肯定发生（概率为 1）时导致 CDF/LERF 与原始 CDF/LERF 的比值。

A.3.2 除了堆芯损坏，还需要评估构筑物、系统和部件在防止大量放射性释放中的纵深防御程度。

A.3.3 对于每一个被确定为 LSS 的构筑物、系统和部件，如果对于下述问题任何一个的答案为是，则该构筑物、系统和部件应为 HSS。

（a）安全壳旁通。是否会引发界面破口导致的一回路冷却剂丧失事故？是否能够为界面破口导致的一回路冷却剂丧失事故提供重要缓解能力？能否在蒸汽发生器传热管破裂事故后隔离该蒸汽发生器？

（b）安全壳隔离。是否用于支持特定安全壳贯穿件的隔离?

（c）早期氢气燃烧。是否用于安全壳内氢气风险的缓解?

（d）安全壳长期完整性。是否为堆芯损坏后保持安全壳长期完整性的唯一方式?

A.4 敏感性分析

A.4.1 经过概率安全分析和纵深防御评价后仍划分为 LSS 的构筑物、系统和部件，还需进行敏感性分析。敏感性分析主要针对人员失误、共因失效和不可用度进行，以确保概率安全分析模型的假设不会弱化构筑物、系统和部件的重要度。

A.4.2 建议采用下述方法对构筑物、系统和部件进行敏感性分析，对以下 5 项内容，分别执行安全重要度评估，如果任一操作导致该构筑物、系统和部件变为 HSS，则该构筑物、系统和部件应为 HSS：

（a）将所有人员失误基本事件值增加到其 95%分位值；

（b）将所有人员失误基本事件值降低到其 5%分位值；

（c）将所有共因失效概率值增加到其95%分位值；

（d）将所有共因失效概率值降低到其5%分位值；

（e）将所有维修不可用度设为0。

A.5 累积敏感性分析

将所有LSS的构筑物、系统和部件的不可靠度增加3~5倍，计算其对CDF和LERF的潜在影响。如果相应结果表明不允许变更，则需调整方案重新进行分级。

A.6 综合决策

A.6.1 通常由来自设计、安全分析、概率安全分析、运行和维修等多个专业的有经验的人员组成专家组，审核上述步骤的分级结果，充分考虑核动力厂设计、运行实践和经验进行综合决策，确定最终的分级方案。这个审查过程贯穿于整个分级过程的始终。

A.6.2 综合决策基于下述方面开展：（a）概率安全分析和敏感性分析；（b）纵深防御评价；（c）其他风险指引项目（如维修规则、风险指引在役检查等）的见解；（d）运行和维修经验。

A.7 基于风险指引方法对安全分级特殊处理要求的调整

在开发完成反映核动力厂当前状态的概率安全分析工作后，可以选择采用风险指引型安全分级方法对基于确定论安全分级的物项的特殊处理要求进行优化。需注意的是，对属于LSS（即RISC-3和RISC-4）的构筑物、系统和部件，虽然可降低某些特殊处理要求，但仍必须要确保这些构筑物、系统和部件能完成它们的设计基准功能。