附件

核安全导则

核动力厂安全分析用计算机软件开发与应用（试行）

国家核安全局

核动力厂安全分析用计算机软件开发与应用
（试行）

本导则自印发之日起施行

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。

本导则为试行导则，在试行期间需对导则的适用性和可操作性进行进一步的验证和改进。

目录

1 引言.....7
1.1 目的.....7
1.2 范围.....7
2 安全分析用计算机软件的范围及要求.....7
2.1 安全分析用计算机软件的范围.....7
2.2 评价模型的概念.....8
2.3 评价模型的类型.....8
3 评价模型开发与评估过程的方法.....10
3.1 方法概述.....10
3.2 评价模型开发基本原则.....12
3.3 建立评价模型能力需求.....13
3.4 开发评估基准.....16
3.5 开发评价模型.....18
3.6 评估评价模型的适宜性.....21
3.7 适宜性评定.....24
3.8 评价模型开发与评估过程的裁剪应用.....25
3.9 通用安全分析程序的特殊应用.....26
4 安全分析用计算机软件开发的验证与确认.....27
4.1 概述.....27
4.2 需求的验证和确认.....27
4.3 设计的验证和确认.....28
4.4 编码实现的验证和确认.....29
4.5 测试的验证和确认.....30
4.6 模型评估的验证和确认.....31
4.7 安装和检验的验证和确认.....31
4.8 运行的验证和确认.....32
4.9 维护的验证和确认.....32
5 安全分析用计算机软件开发的质量保证.....33

5.1 质量保证大纲的要求.....33
5.2 文件控制.....36
5.3 配置管理.....36
5.4 工具评定.....37
5.5 纠正措施.....37
5.6 第三方评定.....37
5.7 开发和评估过程的计划.....38
5.8 评价模型开发文件.....40
6 评价模型的应用.....44
6.1 概述.....44
6.2 保守评价模型.....44
6.3 最佳估算评价模型.....46
名词解释.....50
附件Ⅰ EMDAP 方法对 9 类安全分析程序的适用性说明.....54

1 引言

1.1 目的

1.1.1　本导则为我国自主研发的，用于国内核动力厂安全分析的计算机软件的开发及应用提供指导，以确保核动力厂安全分析的质量和可靠性，是对HAF102《核动力厂设计安全规定》中有关条款的说明和补充。

1.1.2　本导则论述了核动力厂安全分析所使用的计算机软件的开发与评估方法和应用原则，及验证与确认和质量保证的要求。

1.2 范围

1.2.1　本导则主要针对核动力厂安全分析中设计基准事故的确定论安全分析所使用的计算机软件体系（也称为“评价模型”）的开发与应用，核动力厂设计和运行中涉及到的其他计算机软件的开发和应用可参照本导则。

1.2.2　本导则的适用对象是我国自主研发的，用于国内核动力厂安全分析的计算机软件，包括全新开发的软件，或从已有计算机软件改造升级而来的软件。

2 安全分析用计算机软件的范围及要求

2.1 安全分析用计算机软件的范围

2.1.1　核动力厂安全分析用的计算机软件通常包括以下9类[1]：

（1）放射学分析程序：评估工作人员遭受的辐照剂量；

（2）中子物理程序：模拟反应堆堆芯的行为；

（3）燃料行为程序：模拟核动力厂正常运行期间及事故后燃料元件的行为；

（4）热工水力程序：模拟核动力厂正常运行及事故发生后反应堆堆芯及相关冷却剂系统的行为；

（5）安全壳热工水力程序：模拟冷却剂丧失或二回路管道破裂后安全壳压力和温度的行为；

（6）结构程序：模拟各部件和构筑物在载荷及载荷组合下的应力应变行为；

（7）严重事故分析程序：模拟自堆芯损坏至安全壳失效的事故序列进程；

注：[1]本部分内容来源于HAD102/17《核动力厂安全评价与验证》。

（8）放射性后果分析程序：模拟放射性物质在厂区内外的迁移，以确定其对工作人员及公众的影响；

（9）概率安全分析程序：构筑逻辑模型，以确定在假设始发事件后可能发生的事故序列并估计其发生频率。

2.1.2　对于上述中的非设计基准事故分析程序（如严重事故分析程序、概率安全分析程序等）的开发与应用，本导则仅作参考。

2.2 评价模型的概念

2.2.1　通常，将用于核动力厂安全分析的计算机软件体系称为“评价模型[2]”，用于评价核动力厂在瞬态或事故工况下是否满足核安全验收准则的计算体系。该计算体系可以包含一个或多个计算机程序、专用模型和计算某个特定事件所需要的所有其他信息，这些信息通常包括：

（1）处理输入输出信息（如核动力厂几何参数和瞬态或事故计算时假定的核动力厂初始状态参数等）的过程；

（2）未包含在计算机程序中的其他替代分析方法的说明；

（3）定义计算过程需要的所有其他信息。

2.2.2　评价模型的完整性决定了评价结果能否符合相关法规要求。因此，在开发、评估和审查过程中必须考虑评价模型的完整性。

2.2.3　核动力厂安全分析用评价模型需要进行模型评估，需用合适的数据（实验数据、国际标准题、核动力厂运行数据等）证明评价模型模拟核动力厂在假定的瞬态和事故期间行为的适宜性。

2.2.4　在本导则中，组成评价模型的每一个计算机程序、分析工具或计算步骤都称为“计算子块”。这里的计算机程序不仅仅局限于传统的编译语言的可执行文件，也包含在电子表格或其他数学分析工具中执行的计算处理。

2.3 评价模型的类型

2.3.1　表 1 中给出了确定论安全分析中常用的评价模型的不同类型，目前

注：[2]本导则也使用“物理模型”这个学术词汇，它与此处定义的评价模型应加以区分。“物理模型”是指在计算机软件或计算步骤中描述一个特定物理现象的表述方法。

通常采用前三种评价模型。

表 1 评价模型的类型[3]

类型	计算机程序	系统部件可用性假设	初始条件和边界条件
保守评价模型	保守程序	保守假设	保守数据
组合评价模型[4]	最佳估算程序	保守假设	保守数据
最佳估算评价模型	最佳估算程序+不确定性	保守假设	实际数据+不确定性
风险指引评价模型	最佳估算程序+不确定性	由概率安全分析得出	实际数据+不确定性

2.3.2　表 1 中的系统部件可用性假设针对的是安全系统和控制保护系统。

2.3.3　保守评价模型采用保守程序、保守的系统部件可用性假设以及保守的初始条件和边界条件（包括操作员动作的时间）。

2.3.4　组合评价模型采用最佳估算程序、保守的系统部件可用性假设，保守的初始条件和边界条件。保守的初始条件和边界条件应能包络程序模型和核动力厂参数的不确定性。

2.3.5　最佳估算评价模型采用最佳估算程序、保守的系统部件可用性假设，以及更加实际的初始条件和边界条件。最佳估算评价模型应进行不确定性分析，以评估计算结果的不确定性。应保证计算结果不超过验收准则的概率足够大。在进行不确定性分析时，应将计算程序、初始条件和边界条件等因素的不确定性通过统计学方法进行组合，并考虑各不确定性之间的关系。此外，需要确认参数的应用范围是真实合理的。同时，还应该进行敏感性分析，尤其是对那些具有“陡边效应”的问题。

2.3.6　虽然最佳估算评价模型与组合评价模型是两种不同的类型，但是，在实际应用中这两种类型通常混合使用。因为当数据充足时，倾向于采用真实的输入数据，当数据不足时，倾向于采用保守的输入数据。二者之间的差别在于不确定性分析的统计学方法不一样。

2.3.7　风险指引评价模型是在概率安全分析的基础上，对安全重要系统可

注：[3]本表格内容来源于国际原子能机构的 SSG-2《核动力厂确定论安全分析》。

[4]组合评价模型也被认为是一种保守分析方法。

用性和缓解措施的成功概率进行量化的真实分析。该类评价模型也与风险决策的开发相关，并可以作为验证确定论设计基准包络范围的一种方法，但是，不能再用于风险决策。

3 评价模型开发与评估过程的方法

3.1 方法概述

3.1.1　评价模型生存周期按照主要参与方的不同，可能包含获取、供应、开发、运行、维护等过程，以及相应的支持过程和组织过程。对核动力厂安全分析用评价模型而言，其开发过程应包含程序开发与模型评估两部分内容，本导则仅限于对评价模型开发过程中的活动进行规定。

3.1.2　本章推荐一种典型的评价模型开发与评估过程（EMDAP）的层次分析方法，如图 1 所示。该方法包括建立评价模型能力需求、开发评估数据基准、开发评价模型和评估评价模型的适宜性 4 个基本要素，23 项内容。

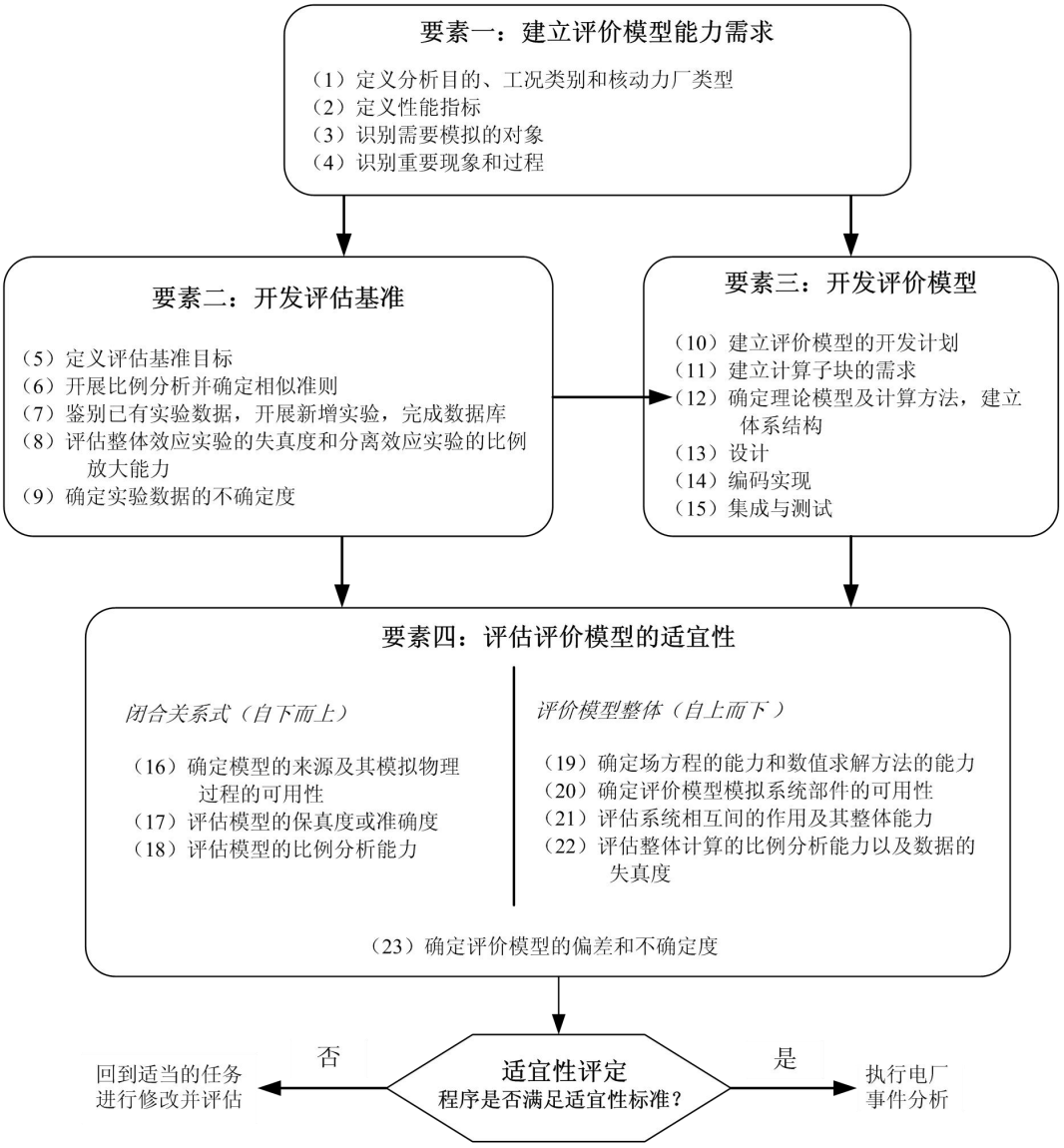

图 1 评价模型开发与评估过程分解

3.1.3　评价模型开发与评估过程方法可应用于复杂事件，尤其适用于全新的评价模型开发。该方法应用的详细程度取决于其所分析问题的复杂程度。如果所分析的问题比较简单，则该方法中的许多内容都可以简化。如果仅对一个已有的评价模型略作增加或修改，只要能保证能充分考虑到这些增加或修改引起的影响，则可以很大程度上简化该方法。

3.1.4　对一个全新的问题或评价模型应用此方法会包含大量的迭代过程。但是，即使只是对已有的评价模型做些相对简单的修改，这些迭代过程也是必须的。

3.1.5　本章所推荐的 EMDAP 方法，并不全部适用于 9 类安全分析用计算

机软件，本导则附件 1 列出了该方法 23 个步骤对此 9 类程序的适用性说明。

3.2 评价模型开发基本原则

3.2.1　为开发出满足核安全要求的评价模型，在开发和评估过程中应遵循以下六个基本原则。

（1）确定评价模型需求。需对评价模型进行需求分析，以确定整个评价模型开发与评估过程的关注重点。通过需求分析，应识别计算特定事件行为所需的数学建模方法、计算对象（如部件、设备等）、现象、物理过程和重要参数，并识别重要度。这里的特定事件是指与核动力厂设计和安全评价所要求的性能指标相关的事件。

（2）建立与需求相一致的评估基准。由于评价模型仅能近似地模拟假想事件的物理行为，因此，需要使用合理的评估基准对计算子块进行确认。其中数据库应该由核动力厂运行数据和实验数据组成。实验数据的来源包括以下两类：一是已有的实验；二是根据模型评估需求而新增的实验。

（3）开发评价模型。需选择或开发与原则（1）所确定的需求相一致的计算子块。对特定核动力厂和事件的评价模型而言，还应选择合适的程序选项、边界条件、组成子块的时间和空间关系。

（4）评估评价模型的适宜性。基于原则（1）的应用，特别是重要现象的确定，应评估评价模型是否具有获得与性能指标相关的预期结果的固有能力。适宜性评估的关键特征是评价模型或其组成子块具有合理预测实验现象的能力，尤其应着重关注评价模型预测重要现象的能力。计算子块通常使用物理模型和经验关系式，应确保这些物理模型和经验关系式是在其已评定过的范围内使用。

（5）评价模型开发与评估过程需遵循质量保证规定。质量保证标准是评价模型开发与评估过程的关键因素，当包含复杂的计算程序时，还应组织项目组外该领域专家进行同行评审。所有影响质量的活动都必须进行严格管理。必须对评价模型开发与评估过程中的所有活动、步骤进行合理定义，以满足质量保证要求。评价模型开发与评估过程应逐步控制，应通过完整的结构给出正确性和适宜性的证据。应对开发与评估过程中的各项活动进行验证和确认。应在评价模型开发和评估过程的初期编制一个适当的质量保证大纲。质量保证大纲应覆盖开发与评估过程的质量要求。

（6）提供全面、准确、最新的文件。由于在评价模型开发与评估过程中可能会引入重要决策的变更，因此，及时编写并更新有关活动的文件是极其重要的。

3.3 建立评价模型能力需求

3.3.1 概述

3.3.1.1 评价模型开发与评估过程的要素一是建立评价模型的能力需求，共包含 4 项内容。其主要工作是确定评价模型的确切应用范围，对范围内的现象、过程和重要参数进行识别，并按重要度排序。

3.3.2 定义分析目的、工况类别和核动力厂类型

3.3.2.1 建立评价模型能力需求的第一步是定义分析目的、识别所需分析的工况类别和核动力厂类型。所定义的分析目的会影响整个评价模型开发、评估和分析过程。评价模型的可用性依赖于瞬态工况，原因在于主要进程、安全参数和验收准则都随工况的不同而不同。因此，瞬态工况就决定了必须要处理的过程。一个完整的瞬态工况定义取决于特定的核动力厂类型，有时甚至取决于特定的核动力厂，因为其主导现象及其相互作用会随着反应堆设计或某个特定核动力厂配置的不同而在一定程度上有所不同。

3.3.2.2 对于安全分析报告中所要求分析的事件而言，上述任务应该是明确的。然后，许可证持有人或申请者以及评价模型开发者应该定义其对核动力厂和核动力厂类型的可用性。例如燃料设计、堆芯装料、蒸汽发生器设计、冷却剂回路数目及其设计、安注系统设计以及控制系统设计等，不同的核动力厂可能会存在较大差异，而这将会显著地影响瞬态工况行为。

3.3.3 定义性能指标参数

3.3.3.1 性能指标是指用于定义安全分析结果可接受的量化标准。通常将核动力厂安全分析所用的验收准则直接作为性能指标，例如堆芯最小偏离泡核沸腾比、包壳峰值温度等。在评估现象和过程的重要度时，也可以采用“附加”性能指标，当然，在使用“附加”性能指标时，须提供合理的使用理由。例如在小破口失水事故评估中，压力容器水装量可作为“附加”性能指标。

3.3.3.2 与“附加”性能指标一样，还应考虑其他与主要目标相关的附加性能参数。由于程序中相互抵消的错误可能无意识地导致正确的结果，因此，附加性能参数可以充当物理追踪点和额外的准确性证明。例如，程序可能计算出了正

确的包壳峰值温度，但其他的计算结果却可能是错误的或出现物理上不可能的值。

3.3.4 识别需要模拟的对象

3.3.4.1 在复杂系统比例分析中采用的系统层次分解法，对识别评价模型的特征也非常有用。以反应堆热工水力分析为例，按照自上而下的顺序，各层次应识别的内容包括：

（1）系统：预期应用中必须分析的整个系统；

（2）子系统：分析中必须考虑的主要部件。可能包括一回路系统、二回路系统和安全壳系统等；

（3）构件：子系统中的物理部件（如反应堆压力容器、堆芯、燃料组件、蒸汽发生器、稳压器、管道等）；

（4）组分：物质的化学组成（如水、氮气、空气、硼等）；

（5）相：固态、液态和汽（气）态；

（6）形态（相拓扑或流型）：为一个给定的输运过程定义的几何形状（如池、液滴、气泡、膜等）；

（7）场：被输运量（如质量、动量和能量）；

（8）输运过程：表征各相在系统内的输运和相间相互作用的机理。

3.3.4.2 上述每一层次中的内容能够被分解为下一层次的内容，进一步表述为：

（1）每个系统都可以被分解为相互作用的子系统；

（2）每个子系统都可以被分解为相互作用的构件；

（3）每个构件都可以被分解为相互作用的组分；

（4）每个组分都可以被分解为相互作用的相；

（5）每个相都可以被归类为一个或多个形态（相拓扑或流型）；

（6）每个形态都可以由场方程来描述（例如质量、动量和能量守恒方程）；

（7）每个场的演变都可能会受到多个输运过程的影响。

3.3.4.3 经过详细定义每一层次每部分内容的数量和类型，才能够建立评价模型的基本特征。但要注意，在高层次存在的缺陷，通常不可能通过低层次内容的修复去处理它。

3.3.5 识别重要现象和过程

3.3.5.1 识别重要现象和过程是指导评价模型开发与评估的基础。它要求基于：（1）对事故序列分析的重要程度；（2）对计算性能指标的影响程度。

3.3.5.2 瞬态中发生的各种过程和现象对核动力厂行为的影响程度是不同的。为了限制候选现象的数量，最好的方法是按照现象对性能指标的影响程度对其进行识别和排序。应分别对瞬态工况的每个阶段和系统的每个部件进行研究。与每个部件相关的过程和现象都应进行检查，并区分因果关系。在完成过程和现象的识别后，应根据它们对性能指标的影响程度来决定其重要度。

3.3.5.3 重要度确定也可用于高层次的系统级过程中，因为如果仅关注部件，往往会忽略系统级过程。某些高层次的系统级过程，例如卸压和水装量减少，往往与性能指标紧密相关。关注这些过程也对识别单个部件行为的重要度有帮助。

3.3.5.4 正如 3.3.3 节所述，性能指标可能比验收准则更适合作为现象识别和排序的标准。对于识别与排序活动中所考虑的全部事故序列而言，只要能够证明待用的性能指标与核动力厂安全性是一致的，则该性能指标可以接受。

3.3.5.5 评价模型的开发与评估都应基于一个可靠且易于理解的现象及重要度识别文件，如现象识别与排序表（Phenomena Identification and Ranking Table, PIRT 表）。应将现象识别与排序表用于确定物理模型开发、比例分析能力、确认及敏感性分析的需求，最终还可用于指导不确定性分析或评估整个评价模型的适宜性。

3.3.5.6 评价模型需计算的过程和现象是通过对特定事故工况的实验数据、经验以及程序模拟结果的研究确定的。应采用相互独立的方法完成排序，包括专家意见、有选择的计算和决策方法（如层次分析法）等。

3.3.5.7 由于现象识别与排序过程的初始阶段主要依赖于专家的主观判断，因此，通过实验和理论分析来确认现象识别与排序表非常重要。由于经验是有限的，因此鼓励使用能够减少主观影响的其他重要度确定方法。

3.3.5.8 在开发现象识别与排序表的早期，敏感性分析有助于确定现象的相对影响。并且，当开展评价模型开发与评估过程的迭代时，敏感性分析对最终确认现象识别与排序表也有帮助。

3.3.5.9 过程和现象的识别步骤如下：

（1）将事故工况按发展进程划分成不同运行特征的时间阶段，各阶段上的

主导过程和现象基本保持不变；

（2）对于每个时间阶段，沿着系统中的一条闭合路线，对每个部件进行过程和现象的识别，以区分产生不同效应的原因；

（3）从第一个时间阶段开始，对部件逐个进行现象识别，直到识别出所有潜在的重要过程为止；

（4）按时间进程不断地重复这个过程，直到工况结束。

3.3.5.10　识别过程完成后，进入排序过程，通常采用数值排序的方法对过程和现象进行数值排序。

3.3.5.11　应为现象识别与排序表提供充足的文件资料，以充分地指导整个评价模型开发与评估过程。此方法中的开发和评估活动可以重复，也包括识别与排序活动的重复。然而，评价模型、现象识别与排序表以及所有的文件最终都应该被“冻结”，以作为正式评审的基础。

3.4 开发评估基准

3.4.1 概述

3.4.1.1 评价模型开发与评估过程的要素二是开发评估基准，共包含 5 项内容。

3.4.1.2 评估评价模型适宜性所采用的重要手段是将模型计算结果与实验数据和/或核动力厂运行数据进行比较。因此，必须根据 3.3.5 节所建立的现象识别与排序表，收集与重要过程和现象相一致的合适的实验数据和/或核动力厂运行数据，并通过比例分析确定实验台架和/或电厂系统对评价模型的可用性。对那些简单的瞬态或已进行了很好比例分析和评估的瞬态而言，本要素的实施也可以相应地简化。

3.4.2 定义评估基准目标

3.4.2.1 对于安全分析中的事件而言，对数据库的首要需求是用于评价模型的评估，如果需要，也可用于开发关系式。数据库的选择应根据要素一中所建立的需求来决定。评估数据库一般应包含以下内容：

（1）为开发和评估经验关系式及其他闭合模型所需要的分离效应实验数据；

（2）为评估各系统间的相互作用和模型的整体分析能力所需的整体效应实验数据；

（3）国际标准题；

（4）其他已经过充分评估并投入实际工程应用程序的标准算例（可选择）；

（5）核动力厂调试及运行瞬态数据（如果可用的话）；

（6）证明基本计算子块能力的简单测试问题。

3.4.2.2 应注意，不能刻意地仅用第 4 条和第 6 条的数据替代实验数据和/或核动力厂运行数据进行评价模型评估。

3.4.3 开展比例分析并确定相似准则

3.4.3.1 所有实验台架相对于全尺寸核动力厂系统而言都存在一定程度的缩小。即使名义上是全尺寸的实验台架也不会完全与核动力厂相同。因此，必须进行比例分析以确保实验数据、以及基于这些实验数据的模型能够适用于全尺寸核动力厂的安全分析。此处获得的比例分析结果最终将应用于第 3.6 节中的偏差和不确定性评估中。应证明实验数据库具有足够多样性，能够包络核动力厂各种预期的响应，且评价模型的计算结果与相应的实验数据在无量纲域上是一致的。还需通过对比计算结果和实验数据，进一步证明与程序能力相关的结论可扩展至特定核动力厂特定瞬态行为的预测。

3.4.3.2 比例分析采用自上而下（top-down）和自下而上（bottom-up）两种方法。自上而下的方法是通过代表特定核动力厂设计的整体效应实验台架来评估整个系统行为和系统间的相互作用。而自下而上的方法则要达到以下目的：

（1）推导出台架间的主要相似无量纲数组；

（2）证明这些无量纲数组可以比例模拟不同实验台架的结果；

（3）确定由不同实验组合给出的这些无量纲数组的取值范围是否能覆盖特定核动力厂和特定瞬态的取值范围。

3.4.3.3 在大部分应用中，特别是具有大量过程和参数的应用中，很难设计一个能够与特定核动力厂完全相同的实验台架。因此，基于 3.3.5 节中识别的重要现象和过程，以及上述的比例分析，应该能确定最佳的相似准则和用于选择已有数据或设计并运行新增实验台架的比例分析原理。

3.4.4 鉴别已有实验数据，开展新增实验，完成数据库

3.4.4.1 应基于要素二的前几个任务的结果选择数据，并根据需要开展新增实验，确保完成数据库的建设。为了完成评估矩阵，应基于 3.3.5 节中开发的现象识别与排序表，选择与重要现象和过程最有关系的实验和数据。在选择实验时，

应选择一系列的实验以证明计算子块或现象学模型不只是针对某个单一实验的。可以在评价模型中使用通过特定数据集推导出的关系式，但在此情况下，还应获取额外的数据用于评估该关系式。最理想的方法是，在开发关系式之前，区分用于开发和评估关系式的实验数据，这可以确保关系式不是针对于某一具体数据集，并保证那些用于评估该关系式的实验数据不是为了使关系式看起来更准确而刻意选择的。用于开发和评估的实验数据应该覆盖关系式将会用到的全部工况。对于整体行为评估，应选择不同比例尺的实验台架开展的对比实验（具有相似事故序列和瞬态条件）。

3.4.5 评估整体效应实验的失真度和分离效应实验的比例放大能力

3.4.5.1 整体效应实验的失真度：整体效应实验数据的失真可能是由于实验台架的比例缩小或台架初始条件和边界条件的不适宜造成的。在 3.4.2 节所确定的实验目的内容中就应该评估实验的失真度。如果失真度非常严重，则可能需要回到 3.4.4 节中去重新选择实验数据或根据需要开展新的实验。

3.4.5.2 分离效应实验的比例放大：如 3.4.4 节所述，关系式应基于不同比例尺的分离效应实验。如果分离效应实验的比例放大能力很差，则可能需要回到 3.4.4 中重新选择实验数据或根据需要开展新的实验。

3.4.6 确定实验数据的不确定性

3.4.6.1 实验数据的不确定性可能来自于测量误差、实验失真以及实验的其他方面。如果相对于评价模型的评估要求，实验数据的不确定性太大，则不能使用这些数据或关系式。

3.5 开发评价模型

3.5.1 概述

3.5.1.1 评价模型开发与评估过程的要素三是开发评价模型，共包含 6 项内容。本要素的目的是为满足要素一所建立的需求而开发一系列计算子块（包括计算机程序和计算步骤）。

3.5.2 建立评价模型开发计划

3.5.2.1 根据要素一建立的需求，应制定一个评价模型的开发计划，该计划内容一般包含在第 5.7 节的开发计划内。

3.5.3 建立计算子块的需求

3.5.3.1 需要建立评价模型各计算子块的需求，这些需求可通过编码实现成为计算子块。需要明确给出整个评价模型的需求与各计算子块的需求之间的对应关系。

3.5.3.2 计算子块的需求建立与设计是紧密联系的。要保证计算子块的需求是可以通过设计和编码实现的，这些需求有可能在设计和编码实现过程中得到更新和完善。

3.5.3.3 计算子块的需求应当足够详细且具有可测试性。应确保开发者和那些未参与需求建立的人或组织可以通过需求文件追溯到这些计算子块需求的起源，并验证这些计算子块的需求。

3.5.4 确定理论模型及计算方法，建立体系结构

3.5.4.1 评价模型的体系结构包括各计算子块的结构，以及集成计算子块的整体结构。该体系结构应该基于 3.3 节中的需求，以及 3.5.3 节中所建立的需求。以反应堆热工水力分析为例，一个独立的计算子块或计算机程序的体系结构可能包括以下几个组成部分：（1）系统和部件，（2）组分和相，（3）场方程，（4）闭合关系式，（5）数值求解，（6）其他特征。最终程序如果要满足 3.5.2 节中所确定的目标，需要成功整合和优化上述几个组成部分。

3.5.4.2 描述某个特定过程的模型或闭合关系式通常是通过分离效应实验数据开发出来的，包括单独使用的模型或包含在计算子块中的关系式。只有在极少数情况下，也有可能从整体效应实验中开发出关系式。在开发或选择这些关系式时，其比例分析能力及应用范围也许是不知道的，因此，为保证关系式的可用性，往往要重复 3.4.5 节中的比例分析评估和要素四的适宜性评估。关系式可能直接从已有的数据库中选出。

3.5.4.3 此处确定的物理模型对于成功开发评价模型而言至关重要。物理模型中的现象学模型的依据、应用范围和准确度应已知且可追溯。超出任何物理模型的原始依据、应用范围和精度/准确度的扩展应用都需要提供正当理由。

3.5.4.4 应当阐述说明将计算子块在空间和时间上耦合起来的方法，它们耦合的紧密程度不仅取决于 3.3.4 节中分析的结果，同时也取决于各计算子块间传递过程的规模和方向。层次分解法可应用于分析计算子块间的传递过程。此外，由于许多计算子块包含用户选项，因此，需要证明所有的选项对评价模型都是合

适的。

3.5.5 设计

3.5.5.1 评价模型的设计包含系统功能设计（体系结构设计）和模块设计（详细设计）。设计需要满足 3.5.3 节和 3.5.4 节的要求。

3.5.5.2 体系结构设计使用 3.5.4 节的方法将需求转变为体系结构，该体系结构描述评价模型的顶层结构，并标识计算子块中的各个模块，应确保所有需求都被分配到模块，以便进行详细设计。

3.5.5.3 应对每一模块进行详细设计。应细化到更低层次的能被编码、编译、测试的单元。应确保来自这些模块的所有需求都被分配到单元。

3.5.5.4 应进行评价模型的外部接口，模块之间接口的详细设计。模块之间的接口说明应当完整、简明、接口两侧应当匹配，尽可能具有一致的顺序并在模块的输入输出接口间使用相同的变量名。

3.5.5.5 设计应当避免不必要的复杂性。应当证明评价模型在系统功能设计及其编码实现方面均已避免不必要的复杂性，遵循规范化设计、编程规范和编码规则的证据应是上述证明的一部分。评价模型模块化和接口定义的逻辑结构应尽可能简单。在设计中，应优选简单算法而不选用复杂算法。不应为实现不需要的性能而增加复杂性。

3.5.5.6 设计中不应当包含矛盾和模糊的内容。详细设计应使编码实现时不需要更多信息。

3.5.6 编码实现

3.5.6.1 编码实现一般包括软件的编码和单元测试。应测试每一个软件单元，以确保满足需求。

3.5.6.2 编码实现应依据模块说明手册，且其生成的代码应是可验证、可测试的。如果验证工作包含人工检查部分，这些代码应是可读的、充分注释的和方便理解的。为了便于验证代码，编码实现应使用已确认的工具。

3.5.6.3 应仔细控制编码实现过程中的变更，并应保持各个版本之间的协调一致。编码实现可以发现模块说明手册或需求文件中的遗漏或不一致问题，使各模块不同版本之间协调一致，并对变更进行全范围的测试。

3.5.6.4 应使用已经确认的软件工具，减少人为差错的产生。如果使用没有充分测试过的工具，应通过额外的分析和验证、人工检查或使用其他工具来证明

该工具是正确的。编码实现阶段使用的工具与其他开发阶段使用的工具应是兼容的。

3.5.6.5 在模块开始编码实现以前，应保证模块说明手册中的功能说明和接口说明是完整的和可用的。

3.5.7 集成与测试

3.5.7.1 应将软件单元和部件作为开发的集合体进行集成和测试；确保每一集合体满足相应软件需求并且在集成活动终了时相应软件项已经集成。应确保已集成的软件可用于软件系统测试。系统测试应对每一项系统需求进行测试，应考虑简化回归测试，保证测试是可重复的。尽量使用自动化测试工具简化测试。

3.5.7.2 在测试用例的设计过程中应覆盖评价模型的所有功能。测试范围应是明确的，并包括对相应功能需求的每项测试的可追溯性信息。应测试输入变量的所有范围。应考虑等效类别划分和边界值分析等方法技术，减少所需测试用例的数量，同时能够保证覆盖足够的测试范围，提高测试效率。必须考虑执行异常状态的测试方法。

3.5.7.3 进行测试的程序应特别注意接口测试（如模块间以及外部接口）。通过测试应能证明所有接口均实现了预期功能。

3.5.7.4 应分析输出与预期结果的偏差，应保存测试记录。

3.5.7.5 如果确定在已经基线化的模块中存在错误，则应在经批准的变更规程控制下进行必要的修改。应分析错误的原因以及研究开发过程未能尽早发现错误的原因，并进行相应的回归测试。

3.6 评估评价模型的适宜性

3.6.1 概述

3.6.1.1 评价模型开发与评估过程的要素四是评估评价模型的适宜性，共包含 8 项内容（见图 1）。

3.6.1.2 在已实施了前面各项任务，并建立了评价模型的能力文件之后，可以对评价模型的适宜性进行评估。

3.6.1.3 评价模型的评估分成两部分。第一部分（3.6.2 节至 3.6.4 节）属于自下而上的评估，针对的是每个计算机程序的闭合关系式。第一部分对重要的闭合模型和关系式进行检查，包括其来源、可用性和对相应的基本原理或分离效应实

验数据的保真度，以及比例分析能力等。使用“自下而上”这个概念是因为该部分评估的重点是那些组成评价模型的基本模块。

3.6.1.4 第二部分（3.6.5 节至 3.6.8 节）属于自上而下的评估，针对的是计算机程序的控制方程、数值求解、每个程序的综合性能，以及整个评价模型的综合性能。通过检查场方程、数值求解、部件或整体效应实验数据的保真度、可用性以及比例分析能力等手段对评价模型进行评估。这部分之所以被称为“自上而下”，是因为其关注点在于评价模型的能力和性能。对自上而下的评估而言，尽管计算真实的核动力厂瞬态或事故工况在确定单个模型的适宜性时往往不够详细，但它在支持评价模型评估时被证实是有用的。只要能证明其具有足够的精度，核动力厂数据也可以用来进行程序评估。

3.6.1.5 对评价模型的任何变更应至少包含与该变更相关的评估，以确保评价模型不会因该变更而引起非预期的结果。

3.6.2 确定模型的来源及其模拟物理过程的可用性

3.6.2.1 模型的来源评估涉及的是闭合模型的物理基础、模型的假定和限制条件，以及模型在被开发出来时的适宜性。可用性评估涉及到程序中所应用的模型是否与其来源相一致，或其应用范围是否合理。

3.6.3 评估模型的保真度或准确度

3.6.3.1 保真度评估主要是确保是否开展了确认工作（通过与数据比较）、基准题工作（通过与其他基准解的比较）或上述工作的组合，并评估这些工作开展的完整度。

3.6.3.2 在模型评估（通常是计算机程序）时，为各组成子块准备的分离效应实验的输入文件，应能描述所要模拟的现象和实验装置，以及核动力厂设计特征。网格划分和选项的选择应该与实验台架和核动力厂中的类似部件相一致。还应该开展网格收敛性分析，直到在实验装置和核动力厂模型中都可用为止。由于有些模型是集总参数模型，不能对其进行网格收敛性分析，所以应注意保证这些模型对实验台架和核动力厂都适用。当完成分离效应实验的计算后，应量化重要现象的计算结果与实验数据之间的偏差和误差。

3.6.4 评估模型的比例分析能力

3.6.4.1 比例分析能力评估仅用于判断特定模型或关系式是否适用于所模拟的核动力厂和瞬态条件。

3.6.5 确定场方程的能力和数值求解方法的能力

3.6.5.1 场方程评估应考虑每个组成程序中控制方程的可接受性。该评估的目标是确定方程与目标应用之间的相关性。为此，该评估应该考虑每个组成程序所求解的方程组的来源、关键概念和过程。

3.6.5.2 当应用于要素一定义的目标应用时，对数值求解方法的评估应考虑程序计算求解原始方程的收敛性、守恒性和稳定性。本评估的目标是要得到与数值方法的应用范围和用户选项相关的信息，这些用户选项可能影响每个组成程序的准确性、稳定性和收敛性。

3.6.5.3 整体评估只有在完成了充分的基础评估分析后才能进行。

3.6.6 确定评价模型模拟系统部件的可用性

3.6.6.1 可用性评估应考虑整个程序是否有能力模拟核动力厂的系统和部件。在进行整体分析之前，应确定评价模型的各种选项、专用模型和输入参数，以保证其具有模拟特定应用所要求的主要系统和子系统的固有能力。

3.6.7 评估系统相互间的作用及其整体能力

3.6.7.1 保真度评估应考虑评价模型的计算结果与部件或整体效应实验台架获得的实验数据，以及核动力厂瞬态数据（可能的话）的比较。对于这些计算，应该将整个评价模型或者其主要计算子块与要素二中选定的整体效应实验数据进行计算比较。

3.6.7.2 与 3.6.3 节的分离效应实验评估一样，整体效应实验的评价模型输入应能最佳地反映实验台架和核动力厂设计的特征。核动力厂的网格划分和计算选项应与实验计算时相一致。此外，在切实可行的范围内，应该对实验台架和核动力厂模型进行网格收敛性分析。对于集总参数模型，不能进行网格收敛性分析，此时应注意保证这些模型既能应用于实验台架，也能应用于核动力厂。一旦完成整体效应实验的模拟计算，可以量化重要过程和现象的计算结果与实验数据间的偏差和误差。在这一步也应该评估评价模型模拟系统相互作用的能力，而且还应准备好目标应用的核动力厂输入卡。为确定在核动力厂中预期会出现的参数范围，需要做充分的分析研究。另外，输入卡也为 3.6.9 节中进行的分析提供基础。

3.6.8 评估整体计算的比例分析能力以及数据的失真度

3.6.8.1 比例分析能力评估仅用于确认评估计算和实验是否显示出了台架间无法解释的差异，或同一台架的计算值与测量值的差异，这种差异可能会给出实

验或程序的比例失真度。

3.6.9 确定评价模型的偏差和不确定性

3.6.9.1 第 3.3.2 节中建立的分析目的和瞬态的复杂程度决定了本节的内容。在使用最佳估算时，不确定性分析的最终目的是为不确定性提供一个定量的值。而这个不确定性量值需在每个不确定性因素的贡献都被确定之后才能得到。

3.6.9.2 对于失水事故的最佳估算分析方法，要求进行完整的不确定性分析，而对于安全分析报告中的其他事故不要求进行完整的不确定性分析，但通常需要采用“适当保守的”输入参数。这些参数保守程度的确定可能需要对偏差和不确定性进行有限的评估，且与 3.6.5 节中的分析紧密相关，因为构成“适当保守的”的输入参数依赖于评价模型所选择的场方程组。基于 3.3.5 节的结果，单个计算模型可以从 3.4.6 节的结果中选择。每一个关键贡献因子的不确定性（范围和分布）由实验数据、核动力厂模型的输入，以及对性能指标的影响等确定。性能指标和计算子块的选择应该保持一致。在大多数情况下，应该包含对整个评价模型的分析。本节的最后部分是确定整体的保守程度或所分析的不确定性对整个评价模型是否合适，以满足 3.3.2 节中所建立的分析目的和监管的要求。

3.7 适宜性评定

3.7.1 应该在整个评价模型开发与评估过程中始终考虑与评价模型适宜性相关的问题。在评价模型开发与评估过程的最后，应该再次考虑评价模型的适宜性，以确保前面提出的所有问题都已得到满意的答案，而且要保证整个过程中的干预活动没有使前面已经被接受的响应受到影响。如果评定结果不能接受，且评价模型有明显的缺陷，则需要对程序的缺陷进行修正，而且要重复评价模型开发与评估过程的相应步骤以对这些修正进行评估。该过程将一直持续到关于评价模型适宜性的问题最终得到确切的答案为止。

3.7.2 在第 5.8 节的“评价模型开发文件”中的文件应该随着计算机程序的改进与评估活动的完成而更新。后期的分析、评估和敏感性分析工作可能会导致现象识别与排序表需要重新评定，因此，也应该酌情修订相应的文件。在评价模型开发与评估过程中，最好的方法是列出一份问题清单并在整个开发与评估过程中持续质询，并在最后再次审查这些问题。为了回答这些问题，应制定用于评估评价模型及其组成程序和模型能力的标准。

3.8 评价模型开发与评估过程的裁剪应用

3.8.1 概述

3.8.1.1 对于只是在此前开发的或获得的评价模型上做一些相对较小修改的评价模型而言，不必完整地应用本导则所描述的评价模型开发与评估的全部过程，即评价模型开发与评估过程的应用范围和深度是可以裁剪的。但是，在决定应用评价模型开发与评估过程的简化程度时，需要考虑所开发的评价模型的以下四个属性：

（1）改进的评价模型相对于已接受模型的改进点；

（2）所分析事件的复杂度；

（3）评价模型的保守度；

（4）需重新分析的核动力厂设计或运行变更的范围。

3.8.2 改进的评价模型相对于已接受模型的改进点

3.8.2.1 评价模型开发与评估过程的裁剪应用程度与评价模型的变更范围相一致。对一个可靠的、经过长期应用的评价模型做些细微的变更，可不必应用整个评价模型开发与评估过程。在此情况下，如果该模型是从缩比实验开发出来的，在考虑其是否具有模拟真实核动力厂能力时只需要考虑比例问题。对于模拟全尺寸核动力厂的评价模型而言，要考虑评估算例的合理程度。应开展测试工作以证明新模型是正确地应用到评价模型中。对某些模型而言，只需完成评估矩阵的一部分工作就足以测试受模型修订影响的现象。另外，还需要进行一些额外的程序测试，以保证程序的变更没有对模型的其他部分造成意外的影响。应评估由错误改正造成的变更对当前的许可证申请分析的影响。而对一个模型进行大的变更，则需要较大程度地应用评价模型开发与评估过程。

3.8.3 分析事件的复杂度

3.8.3.1 评价模型开发与评估过程的应用程度应该与评价模型的复杂程度相一致。对一个简单事件应用该过程是非常复杂的，因此，对于简单事件而言，该过程的应用会自然而然地得到简化。在简单事件中，关键物理现象的数量会相应的少，即使通用瞬态分析程序可能会包含有应用范围比较大的模型，程序评估也仅要求覆盖重要现象即可。另外一种极端情况是用于大破口失水事故分析的评价模型，其物理现象和数值方法都非常复杂，且覆盖范围较广，需要完整地应用评价模型开发与评估过程。

3.8.4 评价模型的保守度

3.8.4.1 通过程序输入和模型假设的综合考虑可以使预期分析结果变得保守。如果可以证明保守程度非常大，或新模型能够给出一个比原有模型更加保守的结果，则对于这种评价模型的变更所需要进行的评估工作量会显著减少。然而，只是在评价模型的某一方面保守并不能证明整个评价模型是保守的，因为评价模型的其他方面可能是不保守的，进而导致整个评价模型不保守。为了减少评估工作量，应该量化并记录整个评价模型的保守度。即使这个评价模型所使用的计算机程序是一个大型多用途的程序，也可以通过相对简单的不确定性分析来获得评价模型分析简单瞬态的保守度。简化不确定性分析的关键是识别决定事故行为的少量重要参数和物理现象。

3.8.5 需重新分析的核动力厂设计或运行变更的范围

3.8.5.1 评价模型开发与评估过程的应用程度应该与核动力厂设计和运行变更程度相一致。许多核动力厂设备或运行的变更不会导致核动力厂超出评价模型的有效范围，则不需要开展开发和评估工作。

3.9 通用安全分析程序的特殊应用

3.9.1 通用安全分析程序（如系统安全分析程序）可应用于分析多种核动力厂的不同事件。可对这类程序进行通用性评审，以减少特定核动力厂和事故工况要求的评审工作量。这些通用性评审可能仅局限于所考虑的应用范围和参数范围，以为证明计算机程序能适用于许可证持有者开展的特定核动力厂和事件分析建立技术基础。当判断某个已有的通用安全分析程序是否适合作为评价模型的基础时，应用评价模型开发与评估过程中的部分内容是非常有用的，并能帮助识别出模型的缺陷和在将程序提交给监管机构审查之前需要做的评估工作。

3.9.2 事实上，为通用程序评审开展的安全评估往往包含大量的程序使用限制条件。为了避免这类问题，确定通用安全分析程序（包括其模型和关系式）的预期应用范围非常重要。通用性评估必须能支持程序在其预期应用范围内的可用性。在通用安全分析程序提交评审之前应使用评价模型开发与评估过程方法，以保证程序的模型和评估可支撑程序适用于整个预期应用范围。在提交一个可用于不同核动力厂和事件分析的通用安全分析程序评审之前，应将评价模型开发与评估过程的应用作为一个先决条件。

4 安全分析用计算机软件开发的验证与确认

4.1 概述

4.1.1　验证和确认（Verification &Validation，简称 V&V）过程属于评价模型生存周期中的支持过程，支持所有的生存周期过程，本章主要针对评价模型的开发和评估过程提出 V&V 的基本要求。

4.1.2　开发过程包含与评价模型有关的需求分析、设计、编码、集成、测试、评估、运行和维护等活动。V&V 活动被划分为需求 V&V、设计 V&V、编码实现 V&V、测试 V&V、评估 V&V、运行 V&V 和维护 V&V 等。评价模型开发与评估过程的 23 个步骤和适宜性评定整体上也构成了一个验证和确认的过程。

4.2 需求的验证和确认

4.2.1　需求 V&V 活动确定功能性和性能需求、评价模型外部接口、合格性需求、安全性和安全保密性需求、人因工程、数据定义、用户文档、安装和验收需求、用户操作和执行需求、用户维护需求。需求 V&V 的目标是确保需求的正确性、完备性、准确性、可测试性和一致性。

4.2.2　需求 V&V 的最低限度任务包括可追踪性分析、评价模型需求评价、接口分析、系统 V&V 测试计划生成和验证、验收 V&V 测试计划生成和验证、配置管理评估，具体要求如下：

（1）可追踪性分析：追踪模块需求（软件需求规格说明（SRS））到系统需求，系统需求到评价模型需求。分析标识出正确性、一致性、完备性和准确性的关系。

（2）评价模型需求评估：评估 SRS 需求（例如功能性、能力、接口、合格性、安全性、安全保密性、人为因素、数据定义、用户文档等）的正确性、一致性、完备性、准确性、可读性和可测试性。

（3）接口分析：验证和确认评价模型与用户、操作人员、及其他系统接口的需求是正确、一致、精确和可测试的。

（4）系统 V&V 测试计划生成和验证：策划系统 V&V 测试以确认需求。策划系统需求对测试设计、用例、规程、和结果的追踪。策划测试设计、用例、规程和结果的文档编制。

（5）验收 V&V 测试计划生成和验证：策划验收 V&V 测试以确认模块在运行环境下正确地实现了系统和评价模型需求。策划验收测试需求对测试设计、用例、规程和执行结果的追踪。策划测试任务和结果文档。验证验收 V&V 测试计划是否满足项目定义的测试文档目的、格式和内容的要求。

（6）配置管理评估：验证配置管理过程是完整和充分的。

4.3 设计的验证和确认

4.3.1　在设计 V&V 活动中，评价模型需求被转化为每个评价模型的体系结构和详细设计。设计 V&V 活动涉及评价模型体系结构设计和评价模型详细设计。V&V 的目标是表明设计是正确、准确和完备地转化了评价模型的需求，而且没有引入非预期的特征。

4.3.2　设计 V&V 的最低限度任务包括可追踪性分析、软件设计评价、接口分析、模块 V&V 测试计划生成和验证、集成 V&V 测试计划生成和验证、V&V 测试设计生成和验证，具体要求如下：

（1）可追踪性分析：追踪设计要素（软件设计描述（SDD）和接口设计文档（IDD））到需求（SRS），及需求到设计要素。分析正确性、一致性和完备性的关系。

（2）软件设计评估：评估设计要素（SDD 和 IDD）的正确性、一致性、完备性、准确性、可读性和可测性。

（3）接口分析：验证和确认评价模型设计与用户、操作人员、评价模型和其他系统的接口的正确性、一致性、完备性、准确性和可测试性。

（4）模块 V&V 测试计划生成和验证：策划模块 V&V 测试以确认评价模型模块（例如，单元、源代码模块）正确实现了模块需求。策划设计需求的追踪以测试设计、用例、规程和结果，策划测试任务和结果的文档，验证模块 V&V 测试计划是否满足项目定义的测试文档目的、格式和内容的要求。

（5）集成 V&V 测试计划生成和验证：策划集成测试以确认评价模型正确地实现了评价模型需求和设计，而每个评价模型模块（例如：单元或模块）相互渐增地集成。设计需求追踪以测试设计、用例、规程和结果，设计测试任务和结果的文档。验证集成 V&V 测试计划是否满足项目定义的测试文档目的、格式和内容的要求。

（6）V&V 测试设计生成和验证：设计模块、集成、系统和验收测试。继续 V&V 测试计划要求的追踪。验证 V&V 测试设计是否满足项目定义的测试文档目的、格式和内容的要求。确认 V&V 测试设计满足 V&V 任务中有关模块、集成、系统和验收测试的各自的准则。

4.4 编码实现的验证和确认

4.4.1　编码实现一般包括软件的编码和单元测试。编码实现 V&V 活动将设计转化为代码、数据库结构和相关的可执行机器表示，编码实现 V&V 活动涉及软件编码和单元测试。V&V 的目的是验证和确认这些转化是正确、准确和完备的。

4.4.2　实现 V&V 的最低限度任务包括可追踪性分析、源代码和源代码文档（如源代码注释、结构说明等）评价、接口分析、V&V 测试用例生成和验证、V&V 测试规程生成和验证、模块 V&V 测试执行和验证，具体要求如下：

（1）可追踪性分析：追踪源代码模块到相应设计规格说明、设计规格说明到源代码模块。分析标识的正确性、一致性和完备性的关系。

（2）源代码和源代码文档评价：评价源代码模块（源代码文档）的正确性、一致性、完备性、准确性、可读性和可测试性。

（3）接口分析：验证和确认软件源代码与用户、操作人员、评价模型和其他系统的接口的正确性、一致性、完备性、准确性和可测试性。

（4）V&V测试用例生成和验证：开发模块测试、集成测试、系统测试及验收测试的V&V测试用例，继续V&V测试计划要求的追踪。验证V&V测试用例是否满足项目定义的测试文档目的、格式和内容的要求。确认V&V测试设计满足V&V任务中有关模块、集成、系统和验收测试的各自的准则。

（5）V&V测试规程生成和验证：开发模块测试、集成测试、系统测试及验收测试的V&V测试规程，继续V&V测试计划要求的追踪。验证V&V测试规程是否满足项目定义的测试文档目的、格式和内容的要求。确认V&V测试规程满足V&V任务中有关模块、集成和系统测试的各自的准则。

（6）模块V&V测试执行和验证：执行模块V&V测试。分析测试结果以确认代码正确实现了设计。确认测试结果可追踪到在测试计划文档中由测试可追踪性建立的测试准则。按模块V&V测试计划的要求记录结果。使用V&V模块测试结

果来确认评价模型满足了V&V测试验收准则。记录真实的和预期的测试结果间的差异。

4.5 测试的验证和确认

4.5.1　测试一般包括集成测试和系统测试。测试 V&V 活动覆盖软件测试、软件集成、软件合格性测试、系统集成和系统合格性测试。V&V 的目标是确保通过执行集成测试、系统测试和验收测试，使计算子块需求和分配给模块的系统需求得到满足。

4.5.2　V&V 工作应生成自己的 V&V 评价模型和系统测试产品（例如，计划、设计、用例、规程），执行并记录自己的测试，并对照评价模型需求验证开发过程的测试计划、设计、用例、规程和结果。

4.5.3　测试 V&V 的最低限度任务包括可追踪性分析、验收 V&V 测试规程生成和验证、集成 V&V 测试执行和验证、系统 V&V 测试执行和验证、验收 V&V 测试执行和验证，具体要求如下：

（1）可追踪性分析：分析在V&V测试计划、设计、用例和规程中的正确性和完备性的关系。对于正确性，验证在V&V测试计划、设计、用例和规程间是否具有有效的关系。对于完备性，验证所有V&V测试规程可追踪到V&V测试计划。

（2）验收V&V测试规程生成和验证：制定验收V&V测试规程。继续验收V&V测试计划要求的追踪。验证V&V测试规程是否满足项目定义的测试文档目的、格式和内容的要求。确认验收V&V测试规程满足V&V任务中“验收V&V测试计划生成和验证”的准则。

（3）集成V&V测试执行和验证：执行V&V集成测试。分析测试结果以验证评价模型模块是否正确地集成。确认测试结果可追踪到在测试计划文档中由测试可追踪性建立的测试准则。按集成V&V测试计划的要求记录结果。使用V&V集成测试结果来确认评价模型是否满足V&V测试验收准则。记录实际的和预期的测试结果的差异。

（4）系统V&V测试执行和验证：执行V&V系统测试。分析测试结果以确认评价模型是否满足了系统需求。确认测试结果可追踪到在测试计划文档中由测试可追踪性建立的测试准则。按系统V&V测试计划的要求记录结果。使用V&V系

统测试结果来确认评价模型是否满足了V&V测试验收准则。记录实际的和预期的测试结果间的差异。

（5）验收V&V测试执行和验证：执行验收V&V测试。分析测试结果以确认评价模型是否满足了系统需求。确认测试结果可追踪到在测试计划文档中由测试可追踪性建立的测试准则。按验收V&V测试计划的要求记录结果。使用验收V&V测试结果来确认评价模型是否满足了V&V测试验收准则。记录实际的和预期的测试结果间的差异。

4.6 模型评估的验证和确认

4.6.1　模型评估的 V&V 工作应覆盖评价模型评估整个过程的所有活动。V&V 的目标是确保通过执行实验/电厂数据的确认与不确定性评估（仅针对最佳估算评价模型）工作，使评价模型的计算结果符合最初建立的评价模型能力需求。

4.6.2　模型评估的 V&V 工作应生成模型评估 V&V 产品（例如：计划、用例等），执行并记录自己的评估，并对照评价模型能力需求验证评估过程的计划用例和结果。

4.6.3　模型评估的 V&V 应确保评价模型的不确定性或保守度分析过程符合 EMDAP 方法步骤，且其确认的范围要符合评价模型的能力需求所定义的范围。

4.6.4　对于保守评价模型，V&V 工作要确保评价模型的计算结果应该总是比真实值更接近验收准则。

4.6.5　对于最佳估算评价模型，V&V 工作要确保模型评估是包络了实验数据和那些与物理模型相关的不确定性的。实验数据本身的不确定性（包括测量误差、实验失真度等）需要在实验文件中明确报告，且其不确定度要合适。

4.7 安装和检验的验证和确认

4.7.1　安装和检验 V&V 活动是指在目标环境下对软件产品的安装、以及需方对软件产品的验收评审和测试。安装和检验 V&V 活动涉及软件安装和软件验收支持。V&V 的目标是验证和确认在目标环境下软件安装的正确性。

4.7.2　安装和检验 V&V 的最低限度 V&V 任务包括安装配置审核、安装检验及 V&V 最终报告生成，具体要求如下：

（1）　安装配置审核：验证正确地安装和运行软件需要的所有软件产品是

否都在安装包内。确认所提供的与场所有关的参数和条件是否正确。

（2） 安装检验：进行分析或测试以验证已安装的软件与经受 V&V 的软件是否一致。验证软件代码和数据库按规定进行初始化、执行和终止。在软件从一个版本到下一个版本的转换中，V&V 工作应确认软件能在不影响剩余系统模块的性能的情况下从系统删除。V&V 工作应验证在包括用户通知的转换过程中连续地运行和服务的需求。

（3） V&V 最终报告生成：在 V&V 最终报告中总结 V&V 活动、任务和结果，包括异常的状态和处理。提供对于软件质量的全面评估和建议。

4.8 运行的验证和确认

4.8.1 运行过程包括软件的运行和对用户的运行支持。运行 V&V 活动是最终用户在运行环境下对软件的使用的评价。运行 V&V 活动涉及运行测试、系统运行和对用户的支持。V&V 的目标是评价系统的新的约束条件，评估建议的更改和它们对软件的影响，并评价操作规程的正确性和可用性。

4.8.2 运行 V&V 的最低限度 V&V 任务包括对新约束条件的评价、评估建议的更改及操作规程评价，具体要求如下：

（1） 对新约束条件的评价：评价关于软件需求的新约束条件（例如，运行需求、平台特性、运行环境）以验证软件验证和确认计划（SVVP）的适应性。软件更改视为维护活动。

（2） 评估建议的更改：评估建议的更改（例如，修改、增强或附加）以确定这些变化对系统的影响。确定 V&V 任务重复的程度。

（3） 操作规程评价：验证操作规程是否与用户文档一致并且遵循系统需求。

4.9 维护的验证和确认

4.9.1 由于问题的出现、需要改进或适应新的需求而导致对软件的代码和相关文档进行修改时，维护过程即被激活。维护 V&V 活动覆盖软件的修改（例如，增强、添加、删除）、迁移或退役。维护 V&V 活动涉及问题和修改分析、修改的实施、维护评审/验收、迁移和软件退役。V&V 的目标是评估所建议的更改和它们对软件的影响，评价运行期间发现的异常，评估迁移需求，评估退役需求并重新执行 V&V 任务。

4.9.2　维护 V&V 的最低限度 V&V 任务包括 SVVP 修改、评估建议的更改、异常评价、迁移评估、退役评估及任务重复，具体要求如下：

（1）　SVVP 修改：修订 SVVP 以遵循批准的更改。当没有开发文档集可用时，生成一个新的 SVVP 来导出要求的开发文档集。

（2）　评估建议的更改：评估建议的更改（例如，修改、增强或附加）以确定这些变化对系统的影响。确定 V&V 任务重复的程度。

（3）　异常评价：评价软件运行异常的影响。

（4）　迁移评估：评估软件需求和实现是否指出：特定迁移需求、迁移工具、软件产品和数据转换、软件归档、先前的环境支持及用户通知。

（5）　退役评估：对于软件退役，评估安装包是否指出：软件支持、对现存系统和数据库的影响、软件归档、转换为一个新的软件及用户通知。

（6）　任务重复：按需执行 V&V 任务以确保计划的更改被正确实现、文档完整且通用以及更改没有导致不可接受的或不可预期的系统行为。

5 安全分析用计算机软件开发的质量保证

5.1 质量保证大纲的要求

5.1.1 概述

5.1.1.1 质量保证大纲应涵盖评价模型开发与评估过程中使用的设计控制、文件管理，以及错误识别和纠正措施等程序。并应覆盖评价模型开发过程的配置管理和交付后更改控制。对安全相关计算机软件开发，至少应以支持独立监查的方式覆盖独立验证、确认和测试。应在质量保证大纲或软件质量保证计划中描述评价模型质量要求。大纲还应包括为代码开发、评估和维护提供合格人员，并为相关人员提供足够的培训。代码维护必须满足质量保证大纲关于设计控制的要求。为保证用户能正确理解和使用评价模型的各项功能，在程序移交给用户时应为用户提供必要的相关培训。

5.1.1.2 评价模型开发与评估应置于质量保证大纲的程序控制之下，应保证所有影响项目质量的相关人员执行质量保证大纲和程序，发现错误时应遵循纠正措施程序。

5.1.1.3 应对使用说明（用户指南）、纠正措施、文件管理和记录保存等方

面提出要求。

5.1.1.4 评价模型开发与评估的质量验证人员应独立于评价模型开发与评估人员。需要对评价模型开发与评估过程进行审查。同样地，用户也需要对评价模型开发与评估过程进行审查，以确保评价模型是被正确地使用。

5.1.1.5 评价模型在应用时需要经过第三方评定。应在质量保证大纲中规定评定的范围和程度。

5.1.2 人员要求

5.1.2.1 应制订评价模型的开发、评价和维护等人员的职责和资格要求，并保证仅由有资格和有经验的人员执行这些职责。为了将软件开发中人为错误降到最低，应由具有合适资格的人员参与软件开发、验证和确认，所以应对实施开发、评估和维护，包括在执行质量保证大纲内的每项任务的人员进行资格鉴定。

5.1.2.2 从事评价模型开发与评估的工作人员，应包括热工、物理等专业应用领域专家和计算机软件专家，以及独立的评审专家。应保证所有人员理解他们的工作如何关系到安全要求的实现，同时应能妥善开展处理核安全分析的研究活动。

5.1.2.3 对评价模型实施独立测试的人员，应给予相关测试工具、程序和技术使用的适当培训。这些人员应与开发团队相互独立。

5.1.3 开发与评估过程的控制

5.1.3.1 评价模型的设计过程应由文件规定，并应由责任设计单位批准和控制。应确定评价模型的设计要求并形成文件，形成的设计要求文件应予以审查和批准。

5.1.3.2 在评价模型的设计过程的每一活动完成时，应设立评价模型的基线。其后产生的并得到批准的基线变更加入到该基线中。基线应确定最新批准的软件配置。

5.1.3.3 应建立识别和控制设计接口的措施，以及建立参与其他的开发组织之间协调的措施。这些措施应包括建立参与开发组织管理程序，这些程序用于审查、批准、发布、分发和涉及设计接口文件的修改。

5.1.3.4 应采取设计控制措施验证或检查设计的适宜性，如采用设计评审、使用替代的或简单化的计算方法，以及执行一个适合的测试程序等对原设计进行验证。对于一个复杂的评价模型开发与评估，需要实施独立的同行评审。设计变

更也应采用适当的设计控制措施。

5.1.3.5 设计验证或检查过程应由与原设计无关的个人或小组执行，但他们可能从属于同一个组织。设计控制措施适用于评价模型的开发与评估的每项活动。

5.1.3.6 设计变更应由原设计单位负责作正式的评审和批准，除非其他的组织已得到管理当局的授权作此变更的批准。对软件基线只能在授权之下作变更。变更应进行合适性的验证。应采用文件反映这种变更，并保持对软件设计要求的变更的可追溯性。对变更应恰当的验收测试。

5.1.3.7 应对需求分析、设计、编码实现等活动建立正式变更申请和变更控制的机制，应保持这些变更记录并可以供管理人员使用。

5.1.3.8 在开发与评价过程的各阶段中所产生的文件应具有可审查性、可追溯性、与标准的符合性，开发的评价模型应具有可证明的可信性、可测试性和可维护性，并且须经过验证和确认。

5.1.3.9 在开发与评估过程的所有阶段应产生正确而容易审查的文件。用于证明开发与评估过程是恰当的文件，应当与评价模型开发与评估过程中实际使用的文件相同。

5.1.3.10 需求对设计应是可追溯的，设计对编码应是可追溯的，需求、设计和编码对测试应是可追溯的。当实施更改时，应保持其可追溯性。反向也应是可追溯的，以保证不产生非预期的功能。

5.1.3.11 应确定安全质量要求和用于开发过程的技术标准。

5.1.3.12 评价模型不仅本身是可信的，还应能向管理人员证明它是可信的，本导则推荐采用改善追溯性的设计方法和质量鉴定方法以及产生足够的文件来实现可信性证明。

5.1.3.13 每项需求和设计特性应能通过测试确定其是否正确实现。所有功能和非功能的需求均应是可测试的。测试结果对相应的需求应能反向可追溯。

5.1.3.14 评价模型的设计应便于错误的发现、定位和诊断，以便能有效修正。

5.1.4 同行评审

5.1.4.1 应在评价模型开发与评估过程中的每一重要步骤都实施独立的同行评审。推荐在评价模型开发的早期成立一个评审小组，评审评价模型能力需求。

同行评审也应该在评价模型开发与评估过程的适宜性评定阶段做出重要决策前进行。除了开发人员和最终用户以外，同行评审小组应包括那些具有相关科学与工程学科，数值计算和计算机编程等领域的专家。同行评审小组成员不直接参与评价模型的开发和评估活动，这样可以提高评价模型的可靠性。同时，这也对识别出大型系统计算程序中常见的缺陷非常有用。

5.2 文件控制

5.2.1　在开发和评估过程的每一步应产生适当的文件用于记录开发和评估过程。文件应随开发不断更新，包括调试过程和维护过程。管理人员应能得到与设计人员所使用的相同的文件。在项目早期应向设计人员明确上述这些要求。

5.2.2　需求、设计、编码、测试和评估的文件应清晰和严谨，以便设计人员、编程人员和独立审查人员能充分了解每个开发阶段并能验证文件的完整性和正确性。

5.2.3　文件应能被具有不同背景和经验的人理解。所使用的语言应明确，如果采用形式语言（例如图形格式）时，应明确定义语法和语义。

5.2.4　整套文件应保证设计决策的可追溯性，追溯的目的是证明对评价模型的需求和设计的实现是完整的，且有助于检测实现过程中的非预期功能。应对需求文件中的每项要求给予唯一的标识。

5.2.5　应建立追溯矩阵图，以清晰显示评价模型的需求与需求分析、设计和实现之间的链接。这个矩阵应证明在编码实现、测试、评估和维护包含了评价模型的整个需求范围。

5.2.6　文件不应包含矛盾的或不一致的语句。文件中每条信息应分为单一的、可确定的段，并且不应在两段或多段之间重复或分割。每项需求、设计或模块应有唯一标识（这也有助于可追溯性）。在整个文件中，符号（标记）、术语、注释和技术方法应是唯一的。

5.2.7　文件应具有可修改性，即文件的结构和风格应能够方便、完整和保持一致地进行任何必要的更改，并且容易确定。

5.3 配置管理

5.3.1　在评价模型的整个开发和评估过程中，应实施配置管理来保证程序的完整性，并追踪程序版本以及用于模拟核动力厂或设施的核动力厂输入模块的

开发。评价模型的各个计算子块（如代码版本和核动力厂输入模块）的配置管理是可以相互独立的，但又都与评价模型开发要素相关，因此对质量保证有同样高的要求，应明确这些不同计算子块的功能。

5.4 工具评定

5.4.1　在评价模型开发和评估过程中所使用的软件工具在被正式使用前，应对所使用的开发、管理或验证的工具的功能进行适当的质量审核，应对前述的任何一类工具都明确规定其功能和适用范围。

5.5 纠正措施

5.5.1　应制定措施，当出现故障、错误、缺陷和偏差，以及不合格品等不符合项时，能及时发现并纠正。在重大不符合质量的情况下，这些措施应保证找到产生不符合的原因，并采取纠正措施和预防措施，以避免重复。识别的重要条件不利的质量，条件的原因，并进行记录，报告给相关的管理层。

5.5.2　错误是指程序或文件与设计需求不符合。应向代码开发者报告所有的故障、错误、缺陷和偏差，并且由程序开发者进行修改。

5.5.3　对故障、错误、缺陷和偏差的追踪和修正状态的报告应该是一个持续的过程，并且是程序代码维护工作的组成部分。对于已经完成并作为核动力厂安全评价组成部分的分析结果，需要评估该故障、错误、缺陷和偏差造成的影响。

5.6 第三方评定

5.6.1　应对评价模型进行独立第三方评定，以确认关键现象的重要度，并评估这些关键现象的不确定性对电厂计算的性能指标的影响。第三方评定也可用来对不确定性分析进行确认。

5.6.2　第三方评定的目的是提供关于评价模型适宜性的评定，该评定是独立于开发机构和用户（许可证持有者）的。第三方评定应得到参与各方（国家核安全监管部门、许可证持有者和开发机构）的认可，以便在期望的时间能得到合适的资源。为得到必要的置信度，应仔细考虑第三方评定必需的关于项目评价的策略、资格和知识。另外，最终评价模型评定应尽可能在最终的版本上进行，但也可能包括开发过程中的中间评价模型的第三方判定。

5.7 开发和评估过程的计划

5.7.1 开发计划

5.7.1.1 开发计划需要按照贯穿于整个开发活动的开发标准和规程来制定，并应规定一系列开发和开发管理活动以及每项活动的基本特性。开发计划应当提供清晰的证据证明整个开发活动遵循了软件开发过程控制的要求。开发计划还应涉及以下几个特定的重要方面：

（1） 计算子块的设计规格说明书；

（2） 文件需求；

（3） 编程标准和流程；

（4） 可移植性需求；

（5） 质量保证要求；

（6） 配置管理要求。

5.7.1.2 在开发计划中应确定开发所使用的工具。工具的选择应便于正确使用所选择的方法、标准和程序。

5.7.1.3 在开发计划中应确定每个步骤产生的文件，并规定其主要内容。应指明用于整个项目的验收准则。

5.7.1.4 开发计划应包含项目相关培训计划，保证那些涉及开发活动的人员有能力使用相关的标准、程序和方法，使用设计、编程、分析工具和方法以及实施配置管理和变更控制。

5.7.2 质量保证计划

5.7.2.1 在项目一开始，开发者应根据质量保证大纲的要求编制评价模型开发与评估的质量保证计划。整个计划应覆盖外部开发承包商，并至少包括下述内容：

（1） 确定适用于质量保证大纲说明的物项以及在该项目中使用的管理标准、程序和工具；

（2） 指明形成的每份文件应由谁审查和批准；

（3） 项目组织机构的描述，该描述应保证其质量保证监督员的独立性；

（4） 对参与项目人员的能力和培训要求的说明；

（5） 对不符合项的标识、报告和纠正的机制；

（6） 确定所有必要的质量控制计划；

（7） 提出对由外部开发承包商提供的计算子块进行质量检查的机制。

5.7.3 测试计划

5.7.3.1 应在项目初期制订总的测试计划，并且每个阶段的测试计划可在上一阶段结束时就开始制定，并可根据需要更新之前制定的测试计划。测试计划应包含测试工作职责的说明。测试计划应是全面的、可理解的并且是完全切合实际的。

5.7.3.2 总体测试计划中应规定计算子块准备使用的技术，应标明所使用的技术规程，和将使用的多种技术，包括文件的静态检查和编码实现的动态测试。并规定将要编写的测试记录、报告和文件。

5.7.3.3 测试计划中应当规定证明测试全部功能范围的方法。应当测试由计算子块完成的所有非功能需求。测试计划应当包含用于证明满足非功能需求的测试方法。

5.7.3.4 应当定义和论证测试的结构范围的度量指标。与计划中规定的指标之间的偏差应证明是合理的并形成记录文件。

5.7.4 评估计划

5.7.4.1 评价模型的评估计划应对第 3 章描述的要素二和要素四的内容进行细化。应明确针对要素四关于评价模型适宜性的评估制定计划。

5.7.4.2 应在评估计划中明确实施评价模型评估的工作人员的组成。实施评估工作的人员应独立于评价模型开发人员。

5.7.5 配置管理计划

5.7.5.1 配置管理计划应当明确要求将软件开发和评估过程中涉及到的所有重要物项都置于配置管理控制之下。所有可识别的物项都应当给予包括版本号在内的唯一标识。这些物项应当包括正在开发的物项和已经开发的现有物项。

5.7.5.2 配置管理计划应当明确要求有配置库或贮存区域用于存放所有处于配置控制下的项目，以便可能在任何现行版本中找到和检索任何标识的项目。

5.7.5.3 应建立配置管理程序，将开发或获取的项目置于配置控制之下。应有一种机制能在时间表的特定点确定一组代表后续工作“基线”的配置控制项。

5.8 评价模型开发文件

5.8.1 概述

5.8.1.1 适当的文件能为评估评价模型应用于安全分析提供支持。评价模型的文件应该覆盖评价模型开发与评估过程的所有要素，一般应包含以下内容：

（1） 评价模型需求说明；

（2） 评价模型方法说明；

（3） 计算子块说明手册；

（4） 验证和分析相关文件；

（5） 用户手册和用户指南；

（6） 比例分析报告；

（7） 评估报告；

（8） 不确定性分析报告。

5.8.2 需求说明文件

5.8.2.1 应该将要素一中所确定的评价模型的需求编写成文件，以此指导评价模型的开发和评估。最重要的是要建立一个成文的、最新版的现象识别表，这对决定一个特定的评价模型应用前是否需要做修改非常重要。

5.8.2.2 需求文件应遵照相关标准，采用清晰可读的格式编写。需求文件应是可验证的和可维护的。

5.8.3 评价模型方法说明文件

5.8.3.1 评价模型方法说明文件应该阐述评价模型中所包含的所有计算子块之间的相互关系，包括外部输入输出接口的描述、体系结构设计的描述等。也可能包括对那些未包含在计算机程序中的评价模型部分进行描述和定义，同时也应对定义一个计算程序的所有其他必要的信息进行描述。

5.8.4 计算子块说明手册

5.8.4.1 需要对评价模型中包含的每一个计算子块建立相应的说明手册，包括理论模型信息，详细设计信息，还应当规定相关的编码实现限制和接口描述。

5.8.4.2 这些手册由多个重要部分组成，其中一部分是对建模理论、数值方法和求解器的描述，包含了对程序体系结构、流体力学、热构件、传热模型、保护系统、控制系统、反应堆中子动力学模型和燃料行为模型等的描述。

5.8.4.3 计算子块说明书应包含详细的设计信息。设计信息中可使用图表和

流程图，或采用用于描述设计的其他常用方法，如数据流程图、结构图等。

5.8.4.4 设计信息应完整地定义与其他计算子块的接口，并应完整地定义模块功能及其在整个评价模型中的作用。

5.8.4.5 设计信息应描述计算错误处理的方法，证明当检测到计算异常时，应提供错误信息的描述、出错位置和性质。

5.8.4.6 该文件的另一部分是关于“模型和关系式的质量评估（MC/QE）”报告，该报告提供模型来源追踪和闭合关系的详细信息。模型和关系式的来源、数据库、精度、比例分析能力以及对特定核动力厂瞬态条件的可用性等信息都应该包含在质量评估报告中。模型和关系式的质量评估报告应包含以下内容：

（1） 提供闭合关系式（指模型、关系式或其他所用的准则）的来源和质量信息；

（2） 描述这些闭合关系式是如何在计算子块的编码中实现的，并保证手册中的描述与编码是一致的，而编码与闭合关系式的来源也是保持一致的；

（3） 为使用这些闭合关系式提供技术原理和证明。换言之，确认模型和关系式中的主导参数（如压力、温度等）能反映核动力厂和所关注的瞬态的预期范围。

5.8.4.7 因此，对于模型、关系式及所用的准则，该质量评估报告应达到以下目的：

（1） 应提供关于初始来源、支撑数据库、精度和应用到特定核动力厂瞬态条件的能力等信息；

（2） 应评估出在支撑模型评价的数据库之外使用这些模型、关系式和准则的影响，描述其外推方法并提供其证明；对某些应用，质量评估报告可能推荐使用可选项而不是默认项，但应提供了证据，证明这些非标选项已经过充分确认；

（3） 应描述计算子块的编码实现；

（4） 应描述为解决计算上的难点进行的任何修改；

（5） 应评估由编码实现和修改引起的对程序的整体应用能力和精度的影响。

5.8.5 测试验证和分析相关文件

5.8.5.1 单元测试应形成单元测试规程、数据等相关文件。测试结果也应形成文件。

5.8.5.2 应制订测试计划，该计划应包括测试需求、规程、数据、职责和进度安排，并形成文件。集成测试结果应形成文件。

5.8.5.3 应编写用于实施软件系统测试的测试矩阵、测试用例（输入、输出、测试准则）和测试规程，并形成文件。

5.8.5.4 应分析输出与预期结果的偏差，分析结果形成文件。应保存测试相关记录。

5.8.6 用户手册和用户指南

5.8.6.1 用户手册应该完整地描述如何准备所有必需的和可选的输入，而用户指南应提供关于准备输入的某些最佳实践方法或例子。为了将不恰当使用程序的风险降到最低，用户指南应该包含以下内容：

（1） 对于所考虑的特定核动力厂瞬态和事故，正确使用程序的方法；

（2） 对所分析的瞬态和事故的适用范围；

（3） 程序对这些瞬态和事故的局限性；

（4） 对所考虑的瞬态分析推荐的模型选项，设备要求，以及节点划分方案的选择。

5.8.7 比例分析报告

5.8.7.1 比例分析报告需要描述对模型评价的所有比例分析，提供对实验数据库的可用性、模型与关系式的比例分析能力以及整个评价模型的比例分析能力的支持。

5.8.8 评估报告

5.8.8.1 评估报告通常有三类：

（1） 开发评估；

（2） 部件评估；

（3） 整体效应实验评估。

5.8.8.2 大多数开发评估报告应包含一系列集中于现象识别与排序表中有限的几个重要现象的程序分析。包括对各种分离效应实验或核动力厂数据的模型评估结果，以证明评价模型有能力计算对特定核动力厂和事故序列类型重要的分离现象和过程。

5.8.8.3 某些程序或计算子块可能以某种特殊的方法来模拟某些设备，应对这些方法进行评估。

5.8.8.4 整体效应实验评估是通过与相关的整体效应实验或核动力厂数据比较来展示评价模型的整体能力，应为这些整体效应实验评估给出评估报告。

5.8.8.5 对于某些核动力厂或某些瞬态，程序与程序的比对是有帮助的。特别是当一个新程序或计算子块只是进行很有限地应用时，其结果可以与一个以前的程序计算的结果相比较，并在评估报告中给出对比结果。但是，新程序所考虑的核动力厂类型和瞬态，必须保证以前的程序已经使用整体效应实验数据或核动力厂数据进行过很好的评估。在评估报告中应该对关键的输入数据（例如系统节点划分）上的差异解释清楚，以保证好的比较结果是合理的。但这样的标准题计算并不能替代对新程序的评估。

5.8.8.6 在进行特定核动力厂安全分析之前，可能需要预先完成大量的评价模型评估工作。在某些情况下，评估工作的范围可能会超出评价模型所定义的核动力厂类型和瞬态。在某些情况下，评估活动不是由负责核动力厂分析的人员组织完成的。因此，为了确保这些评估结果对所考虑的核动力厂和瞬态的可信度，需要谨慎地对这些评估结果的适用性进行充分评估，并整理成文。

5.8.8.7 为了在评价模型应用于特定核动力厂事件时对其预测能力有信心，评估报告必须包括以下内容：

（1） 应评估出计算子块计算各种重要参数（尤其在现象识别与排序表中现象相关的参数）的能力和精确度；

（2） 应通过适当的比例分析和敏感性分析判定出计算结果是否受益于相互抵消的错误；

（3） 应评估出计算结果是否自洽，且描述的相关联的信息是否是合理且可接受的；

（4） 应评估出评价模型计算的事故序列是否与实验数据的趋势保持一致；

（5） 应评估出评价模型比例放大到典型的核动力厂的能力（这些评估都必须基于用于开发和确认评价模型的实验数据）；

（6） 应对任何意料外的或看似奇怪的计算结果给出解释。（尤其当实验测量值和计算结果不相符时非常重要。在这种情况下，合理的技术解释应能很好地支持评价模型的可信性）。

5.8.8.8 当计算结果和实验数据不一致时，评估报告也必须要包括以下内容：

（1） 应找出引起不一致的原因，并进行解释，即识别并讨论了计算子块的缺陷（必要时，应讨论实验测量的不准确）；

（2） 应说明这些缺陷对整体结果有多大影响；

（3） 当认为缺陷可能不会对特定的事故序列产生重大影响时，应该给予合理的解释。

5.8.8.9 对于一个计算子块的输入模型和相关的敏感性分析，评估报告必须包括以下内容：

（1） 应提供节点划分图，并讨论节点划分的原理；

（2） 应指定并讨论边界条件和初始条件，以及计算的运行条件；

（3） 应提供并讨论对闭合关系式和其他参数的敏感性分析结果；

（4） 应由敏感性分析结果讨论对输入模型（节点划分，边界、初始和运行条件）的修改；

（5） 应记录数值求解收敛性的研究内容，包含使用的时间步长和选定的收敛准则；

（6） 需要为相似性分析提供指南。

5.8.9 不确定性分析报告

5.8.9.1 应为评价模型开发与评估过程中进行的任何不确定性分析提供文件。

6 评价模型的应用

6.1 概述

6.1.1 目前核动力厂安全分析应用的评价模型包括保守评价模型（表 1 中的组合评价模型也认为是保守分析方法）和最佳估算评价模型。

6.1.2 本章的应用要求适用于新开发的评价模型，也适用于在成熟评价模型的基础上改进的评价模型。

6.2 保守评价模型

6.2.1 保守方法与保守程序

6.2.1.1 保守方法是指对验收准则产生不利影响的参数设置或计算方法。

6.2.1.2 保守程序是指基于保守方法开发的程序。

6.2.1.3 应证明对于任何情况，基于保守方法得到的计算结果都是保守的。应考虑控制系统和安全系统动作的相互影响，以确保计算结果是保守的。

6.2.2 初始条件和边界条件

6.2.2.1 基于保守计算的目的，初始条件和边界条件的设置应能产生保守的结果。一系列的初始条件和边界条件的保守设置不一定会对每一个安全参数都产生保守的结果。因此，需要对每一个初始条件和边界条件，依据特定的事故序列和相应的验收准则来选择合适的保守度。

6.2.3 系统和部件可用性

6.2.3.1 安全分析中，在确定系统和部件可用性时应采用单一故障准则，本准则规定当发生任何单一故障时，安全系统应能够执行其特定功能。

6.2.3.2 应对系统和部件假定一个对计算安全参数产生最大负面效果的失效。

6.2.3.3 除了遵循单一故障准则，应考虑相同原因引起的故障及其后果。而且，还应考虑在电厂运行操作规程范围内的在线维修引起的失效。

6.2.3.4 应采用最保守的假设合理地考虑事故过程中失去厂外电的情况。对于未经特定事故下测试认证的设备，除非其长期运行将会产生更不利的影响，否则应假定其失效。应考虑到控制系统失效和保护系统及安全系统动作的延迟，对于这些系统，应考虑其持续动作是否会比其失效能导致更加保守的条件。

6.2.4 操作员动作

6.2.4.1 在特定的时间范围内，一般不考虑操作员动作对设计基准事故进程的影响。如需考虑早期的操作员动作，则操作员动作的时间应该是保守的并经过充分证明的。应根据动作时间的不同，采用不同的保守假设。对于大多数工况，应假定操作员应能实施事故后恢复动作。

6.2.5 核动力厂网格划分与建模

6.2.5.1 核动力厂的建模网格划分可能对计算结果产生很大影响。应严格遵循模型文件、程序文件、用户指南的要求，以减小用户效应。模型文件应包括输入数据设置说明和模型选择说明。

6.3 最佳估算评价模型

6.3.1 最佳估算方法与最佳估算程序

6.3.1.1 最佳估算方法是指真实地描述核动力厂物理现象的模型方法。

6.3.1.2 最佳估算程序是指对于核动力厂重要的现象采用真实的物理模型的计算程序。

6.3.1.3 最佳估算评价模型是指采用最佳估算方法计算，对计算结果与验收准则进行比较，并评估其不确定性。最佳估算方法能提供核动力厂的更真实的信息，能识别与安全最相关的问题，并且能提供计算结果与接收准则之间的裕量的信息。

6.3.1.4 采用最佳估算程序，或其他能真实描述物理现象的工具，应证明考虑了所有重要现象或者包络了所有重要现象的影响。应采用足够多的数据证明已考虑了所有重要现象，或者已包络了这些现象的效应。

6.3.1.5 最佳估算程序的计算结果不保证能包络试验数据，也不保证保守，应采用试验数据量化计算结果的不确定性，特别是那些与验收准则相关的参数的不确定性，量化其不确定性是重要的。

6.3.1.6 量化不确定性的方法应是成熟的。

6.3.1.7 应采用现象识别与排序表（PIRT 表）帮助确定参数的不确定性。应根据可用的试验数据，识别出最重要的现象。这些重要的参数应根据概率分布而变化，以确定总的不确定性。

6.3.1.8 应针对特定的事件、特定的程序或方法，建立特定的 PIRT 表。

6.3.1.9 由于可用的实验数据和核动力厂运行数据的层次不同，且这些数据独立评估的程度不同，所以最佳估算程序的认证资质也是不同的。应建立包含足够多实验数据的数据库，将程序的计算结果与数据库的数据进行比较，以改进最佳估算程序的质量，并分析基于最佳估算程序得到的计算结果的不确定性。

6.3.2 初始条件和边界条件

6.3.2.1 应考虑初始条件和边界条件相关参数的不确定性。若不考虑参数的不确定性，则应将初始条件和边界条件的参数范围限制在保守范围内。

6.3.2.2 应采用核电站寿期内最极限的初始条件，该初始条件通常是通过敏感性分析得到的。

6.3.2.3 当采用现实初始条件时，不可能同时发生的初始工况无需考虑。

6.3.3 系统和部件可用性

6.3.3.1 该部分内容与保守评价模型的系统和部件可用性假设相同。

6.3.4 核动力厂网格划分与建模

6.3.4.1 网格划分应保证计算机程序模拟的事故过程包括事故序列中的所有重要现象，以及核动力厂所有重要的设计特征。只有经过实验数据确认的网格划分才能用于实际核动力厂相应事故序列的计算。当使用缩比实验数据评估评价模型时，对实验和全尺寸核动力厂进行分析时需使用与之相一致的网格划分，且需要进行充分的网格敏感性分析以确保计算结果稳定。

6.3.5 时间步长划分

6.3.5.1 应对时间步长大小的影响进行敏感性分析，并对时间步长大小引起的不确定性进行评估。

6.3.6 不确定性分析与敏感性分析

6.3.6.1 敏感性分析指确定程序输入变量、模型参数的变化对计算结果的影响。

6.3.6.2 不确定性分析指在分析特定事件时，对于程序模型、电厂模型、电厂数据的不确定性的处理，包括测量的不确定性与标定的不确定性。计算的总的不确定性应是各个输入的不确定性的综合，此外，应考虑试验台架与电厂的尺寸的差别。

6.3.6.3 不确定性包括认知的不确定性与偶然的不确定性。

6.3.6.4 认知的不确定性来源于信息的不完整、认识的不充分。通过直接对计算结果进行不确定性分析与敏感性分析，从而对认知的不确定性进行处理。

6.3.6.5 偶然的不确定性来源于不可预计的系统、部件及其参数的任意行为，包括操作员的行为。通过概率论的方法，量化发生概率，从而处理偶然的不确定性。

6.3.6.6 应考虑的不确定性包括：

（1） 程序的不确定性：主要是指计算模型及其数值方法带来的不确定性。

（2） 初始条件、边界条件以及设备的可用性：应考虑核动力厂边界条件与初始条件、设备的特征和行为的不确定性。当然，如若将这些参数的值设置成保守的也是可以接受的。

（3） 燃料行为：应考虑燃料行为参数的不确定性，这些参数包括：燃料

导热率、间隙宽度、间隙导热率、功率峰值因子等。

（4） 其他参数：某些计算模型的不确定性不能通过与整体效应实验数据比较得到，例如在大多数整体效应实验中使用电加热棒来模拟真实燃料棒，因此实验忽略了堆芯衰变热、包壳金属与水反应产热的影响。应对这些参数的不确定性进行量化。

6.3.6.7 安全分析通常牵涉大量的参数，导致结果具有不确定性。大多数量化不确定性的方法需要识别具有不确定性的输入参数。应通过确定这些参数的范围以及取值的概率分布，量化其不确定性。若这种方法不可行，应采用保守的方法。

6.3.6.8 应给出评估计算结果在可接受的置信度下的总不确定性的评估方法并给予证明。如果假设各参数线性不相关，则需要给出其合理的证明。应通过与实验数据比较，确定各个参数对程序不确定性的影响。并要为各个参数假定的分布和所考虑的范围提供依据。

6.3.6.9 每一个关键参数的真实统计分布实际上是无法得到的，需要应用工程数据和信息对每一个统计分布都进行验证。可通过合理的数据和工程分析结果来预估各个关键参数合理的统计分布，并应对上述过程提供相关的支持性文件。

6.3.6.10 应通过与相关的整体效应实验及不同比例的分离效应实验数据进行对比得出程序的不确定性。通过这种方法，可以得到在不同比例范围和不同现象中，程序各个模型和关系式组合的不确定性。需要足够多的来自不同比例实验台架的实验数据，以保证合理地评估程序的不确定性。若有必要，应通过分离效应实验评估特定现象的不确定性，同时，还应考虑测量误差及校准误差等的影响。

6.3.6.11 应对所有重要参数进行实验数据对比计算，以证明整个程序的最佳估算能力。例如在大破口失水事故中，最重要的参数是燃料包壳峰值温度，该参数是验收准则之一，并对其他验收准则产生重要影响。此外，还应评估其他重要参数产生的补偿误差。例如在小破口失水事故中，除了评估燃料包壳峰值温度外，还要评估程序预测系统冷却剂质量和压力容器冷却剂装量的能力。

6.3.6.12 事故进程中，不同时间段的现象或物理过程是不同的，所以，应明确程序对于不同时间段的预测能力，并提供评估程序计算各时间段的不确定性及总的不确定性的方法，并需要证明该方法是合理的。

6.3.6.13　如果将从小比例实验台架得到的实验结果用于分析大比例对象的不确定性，应证明这种方法是合理的。实验台架比例的影响可以通过大比例的分离效应实验的比较以及整体效应实验的比较来确定。如果存在比例的影响，特别是这种影响如果会导致计算不保守，则在程序计算大比例对象时，应对该程序予以改进。不具备计算不同比例对象能力的程序，若其计算结果是不保守的，则不可接受。

名词解释

比例分析能力（Scalability 或 scaling）

评价从缩比实验台架得到的结果或一个计算子块的建模特征应用于描述真实核动力厂的合适程度的过程。

闭合关系式（Closure relations）

为处理得到预期结果，对场方程进行补充的那些方程和关系式。包括物性定义和描述输运现象的关系式。

编码实现（Coding）

编码实现即软件编码和单元测试。编码是用编程语言表示计算机程序的过程，将逻辑和数据从设计规格说明（设计描述）转换为编程语言。单元测试（包括部件测试）是指对独立的软件单元（部件）或相关单元（部件）的测试。编码实现主要包括：开发软件单元（部件）或数据库；编写用于测试软件单元（部件）的测试算例、规程和数据；测试独立软件单元（部件），以确保对设计的正确实现；评价软件编码和测试结果。

不确定性（Uncertainty）

此概念有以下三个独立却又有一定关联的定义：（1）由测量系统从实验中采集到的数据的不准确度；（2）计算主要安全限制或与性能指标相关的不准确度，这些不准确度的典型来源是试验数据或用于开发分析工具的假定条件；（3）与近似值和不确定性相关的分析不准确度。

场方程（Field equations）

用于求解所感兴趣的物理量（通常是质量、能量和动量）的输运。

层次分析法（Analytical hierarchical process）

一种软件基础分析方法，该方法以一种前后一致且可追踪的方式，基于现象和过程，并结合实验数据和专家判断，对核动力厂事故或瞬态响应的重要程度进行有效排序的方法。

冻结（Frozen）

在整个安全分析过程中保持分析工具的条件和相关台架的输入卡保持不变（且处于配置管理之下），从而保证最终结果的可追溯性和一致性。

分离效应实验（Separate effects test）

将主要关注点放在单个物理现象或过程上的实验。

集成与测试（Integration and testing）

集成是指将软件单元和软件部件、硬件部件或两者合成为一个完整系统的过程。测试是一种活动。在此活动中，在一定的条件下执行系统或部件执行代码，观察或记录其结果，对系统或部件的某些方面进行评价。其目的是为了证明开发的产品是符合需求和设计要求。测试主要包括集成测试和系统测试。集成测试是指把软件部件、硬件部件或两者组合起来进行的测试，并测试评价它们之间的交互。系统测试是在完整的、集成的系统上的测试行为，它用以评价系统与规定的需求的遵从性。

几何形态（Geometrical configurations）

为输入过程而定义的几何形状（如池、液滴、气泡和膜等）。

基线（Baseline）

基线是项目储存库中每个工件版本在特定时期的一个“快照”。它为此后的工作提供一个正式的标准，此后的工作基于此标准，并且只有经过授权后才能变更这个标准。

目标应用（Target application）

针对某个已确定的应用目的、瞬态类型和核动力厂类型的安全分析。

模型（Model）

在计算子块中用于描述一个特定物理现象的方程或方程组。

评估（Assessment）

用整个评价模型或其中的单个计算子块执行计算，将计算结果与实验数据、电厂运行参数（如果可获得的话）、国际基准题、解析解等相比较，以确认其是否能满足目标应用的过程。

设计（Design）

设计活动是进行软件体系结构、组成部分、接口和数据的设计，为设计编制文件，并对其进行验证，以满足评价模型能力需求的过程。

通用安全分析程序（General purpose computer programs）

可应用于分析不同目的、不同核动力厂在不同事故工况下的安全分析程序。

现象识别与排序表（Phenomena identification and ranking table）

根据上下语义，可以指表格或过程。是指确定某现象（或物理过程）对核动力厂在某事故或瞬态条件下行为影响的相对重要性的过程。

相（Phase）

输运过程中涉及到的物质状态，通常是液相和气相。

需求分析（Requirements analysis）

需求分析活动是研究用户需要以得到软件需求的定义过程，或者研究和重新定义软件需求的过程。需要确定评价模型确切的应用范围，并要对范围内的现象、过程和重要参数进行识别并按重要度排序。

验证与确认(Verification and validation)

验证是评价系统或部件，以确定软件开发周期中的一个给定阶段的产品是否满足在各阶段的开始确立的需求的过程。

确认是在开发过程期间或结束时对系统或部件进行评价，通过检查和提供客观证据，以确定它是否满足特定预期用途的需求的过程。

验证与确认是确定系统或部件的需求是否完成和正确，每一开发阶段的产品是否实现在上一阶段规定的需求或条件，以及最后的系统或部件是否依从规定的需求的过程。

整体效应实验（Integral effects test）

与分离效应实验相对应，将主要关注点放在整个系统行为以及参数和过程间的相互作用上的实验。

自上而下（Top-down）

与安全分析相关的一种逐步确定方法，其逐步确定过程涉及的内容如下：（1）分析的准确目标（监管活动、许可证活动和期望成果等）；（2）分析范围（台

架或核动力厂、瞬态、分析程序、台架几何尺寸和运行边界条件等）；（3）所有可能的对台架或核动力厂行为有影响的现象或过程；（4）现象识别与排序过程；（5）分析工具的应用能力和比例分析能力；（6）引入分析中的各种不确定性对最终产品的影响。自上而下分析方法的一个主要特征是，当处理与第（5）和（6）条相关的安全分析时，采用一种基于第（4）条所确定的相对重要度的分级处理方法。条目（1）到（4）的分析工具是相互独立的，而条目（5）和（6）在选择分析工具时却是相关的。

自下而上（Bottom-up）

是一种与安全分析相关的方法，与下一条“自上而下”类似，但其主要特征是处理所有的现象和过程，包括与建模分析工具相关的那些现象和过程。

组分（Constituents）

任何可被传输的物质的化学形式（如水、空气和硼等）。

附件Ⅰ EMDAP 方法对 9 类安全分析程序的适用性说明

本导则第 3 章所推荐的 EMDAP 方法，并不适用于全部 9 类安全分析用计算机软件（详见 2.1.1 节），下表列出了 EMDAP 方法 23 个步骤对此 9 类程序的适用性说明。

EMDAP 方法的要素与步骤		放射学分析程序	中子物理程序	燃料行为程序	热工水力程序	安全壳热工水力程序	结构程序	严重事故分析程序	放射性后果分析程序	概率安全分析程序
要素一：建立评价模型能力需求	步骤 1：定义分析目的、工况类别和核动力厂类型	√	√	√	√	√	√	√	√	×
	步骤 2：定义性能指标	√	√	√	√	√	√	√	√	×
	步骤 3：识别需要模拟的对象	√	√	√	√	√	√	√	√	×
	步骤 4：识别重要现象和过程	○	×	○	√	√	○	√	√	×
要素二：开发评估基准	步骤 5：定义评估基准目标	√	√	√	√	√	√	√	√	×
	步骤 6：开展比例分析并确定相似准则	×	×	×	√	√	×	×	×	×
	步骤 7：鉴别已有实验数据，开展新增实验，完成数据库	○	○	○	√	√	○	√	○	×
	步骤 8：评估整体效应实验的失真度和分离效应实验的比例放大能力	×	×	×	√	√	×	○	×	×
	步骤 9：确定实验数据的不确定性	○	○	○	√	√	○	√	×	×
要素三：开发评价模型	步骤 10：建立评价模型开发计划	√	√	√	√	√	√	√	√	×
	步骤 11：建立计算子块的需求	√	√	√	√	√	√	√	√	×
	步骤 12：确定理论模型及计算方法，建立体系结构	√	√	√	√	√	√	√	√	×
	步骤 13：设计	√	√	√	√	√	√	√	√	×
	步骤 14：编码实现	√	√	√	√	√	√	√	√	×
	步骤 15：集成与测试	√	√	√	√	√	√	√	√	×

EMDAP 方法的要素与步骤		放射学分析程序	中子物理程序	燃料行为程序	热工水力程序	安全壳热工水力程序	结构程序	严重事故分析程序	放射性后果分析程序	概率安全分析程序
要素四：评价模型的适宜性	步骤 16：确定模型的来源及其模拟物理过程的可用性	√	√	√	√	√	√	√	√	×
	步骤 17：评估模型的保真度或准确度	√	○	×	√	√	√	×	√	×
	步骤 18：评估模型的比例分析能力	×	×	×	√	√	○	×	×	×
	步骤 19：确定场方程的能力和数值求解方法的能力	×	○	√	√	√	√	√	√	×
	步骤 20：确定评价模型模拟系统部件的可用性	×	×	×	√	√	√	√	×	×
	步骤 21：评估系统相互间的作用及其整体能力	×	×	×	√	√	√	√	√	×
	步骤 22：评估整体计算的比例分析能力以及数据的失真度	×	×	×	√	√	○	×	×	×
	步骤 23：确定评价模型的偏差和不确定性	√	√	√	√	√	√	×	√	×
符号说明：“√”表示本步骤适用于该类程序；“○”表示本步骤可能适用于该类程序；“×”表示本步骤不适用于该类程序。										