

ICS 27.120.20
F 69
备案号: 59599—2017

NB

中 华 人 民 共 和 国 能 源 行 业 标 准

NB/T 20429—2017

核电厂事故处理规程编写要求

**Requirements for preparation of emergency operating procedures for nuclear
power plants**

2017-04-01 发布

2017-10-01 实施

国家能源局 发布

目 次

前言.....	II
1 范围.....	1
2 规范性引用文件.....	1
3 术语和定义.....	1
4 事故处理规程的开发过程.....	3
5 事故处理导则.....	5
6 事故处理规程编写.....	7
7 事故处理规程验证.....	13
8 事故处理规程确认.....	14
9 事故处理规程文件体系.....	16
附录 A（资料性附录） 事故处理规程开发过程示例.....	17
附录 B（资料性附录） 流程图.....	19
附录 C（资料性附录） 条件语言和逻辑顺序.....	21
附录 D（资料性附录） 事故处理规程验证的检查清单示例.....	23

前 言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准由能源行业核电标准化技术委员会提出。

本标准由核工业标准化研究所归口。

本标准起草单位：中国核电工程有限公司。

本标准主要起草人：唐涛、杨庆明、刘勇、赵思桥、刘海宇、孙涛。

核电厂事故处理规程编写要求

1 范围

本标准规定了核电厂事故处理规程的编写要求，包括事故处理规程的开发、技术依据、编写规范、验证和确认等要求。

本标准适用于核电厂事故处理规程的开发和维护。

2 规范性引用文件

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

NB/T 20267—2014 核电厂计算机化运行规程系统设计准则

NB/T 20270—2014 人因工程在核电厂计算机化运行规程系统中的应用准则

3 术语和定义

下列术语和定义适用于本文件。

3.1

安全功能 safety function

维持核电厂在安全状态所需的功能，包括控制反应性，排出堆芯热量，包容放射性物质和控制运行排放、以及限制放射性释放。

3.2

正常运行 normal operation

核电厂在规定的运行限值和条件范围内的运行。

3.3

预计运行事件 anticipated operational occurrences

在核电厂运行寿期内预计至少发生一次的偏离正常运行的各种运行过程；由于设计中已采取相应措施，这类事件不至于引起安全重要物项的严重损坏，也不至于导致事故工况。

3.4

假设始发事件 postulated initiating event

设计期间确定的可能导致预计运行事件或事故工况的假设事件。

3.5

设计基准事故 design basis accident

导致核电厂事故工况的假设事故，这些事故的放射性物质释放在可接受限值以内，该核电厂是按确定的设计准则和保守的方法来设计的。

3.6

设计扩展工况 design extension conditions

不在设计基准事故考虑范围的事故工况，在设计过程中应该按最佳估算方法加以考虑，并且该事故工况的放射性物质释放在可接受限值以内。设计扩展工况包括没有造成堆芯明显损伤的工况和堆芯熔化（严重事故）工况。

3.7

事故工况 accident conditions

偏离正常运行，比预计运行事件发生频率低但更严重的工况。事故工况包括设计基准事故和设计扩展工况。

3.8

运行技术规格书 operating technical specification

在机组正常运行期间，确保公众和核电厂工作人员的安全而必需遵守的最低技术规则。这些规则的执行确保重要的安全系统在异常或事故工况下能够正确运行。

3.9

异常运行规程 abnormal operating procedure

用于应对异常运行工况的规程。使用异常运行规程意味着电厂状态已偏离正常运行工况，但尚未发展到事故处理规程覆盖范围。

3.10

事故处理导则 emergency operating guideline

确定了为缓解瞬态和事故造成的后果并恢复安全功能所必需操作的系统和设备，并且列出了应执行的操作的文件。

3.11

事故处理规程 emergency operating procedure (EOP)

用于指导操纵员执行缓解假设瞬态和事故后果所必需的操作的规程，这些瞬态和事故已经造成核电厂参数超出反应堆保护定值、专设安全设施定值或其他确定限值。

3.12

事件导向规程 event-oriented EOP

要求操纵员诊断并确认所发生的事件，根据其预先设定的操作措施对瞬态和事故进行缓解的规程。

3.13

功能导向规程 function-oriented EOP

指导操纵员如何检查安全功能是否正常，以及当这些功能降级时，如何进行维持和恢复的规程。功能导向的事故处理规程可将核电厂维持在安全状态而无需操纵员对具体事件进行诊断。功能导向规程有以下形式：征兆导向规程和状态导向规程。

3.14

征兆导向法 symptom-oriented approach

以某些安全相关参数偏离限值作为征兆,针对这些征兆制定有效措施将核电厂恢复至安全状态的事故处理方法。

3.15

状态导向法 state-oriented approach

用某些特定的物理参数表征核电厂状态,根据这些参数降级的程度使用合适的处理策略以恢复核电厂状态的方法。

3.16

验证和确认 verification and validation

验证是检验规程内容书写的正确性和技术要求的准确性的过程。

确认是指确定事故处理导则或规程的可用性和正确性的过程。

验证和确认是指为达到一系列目标而对规程所采用的评价过程。这些目标通常从技术角度和人因角度对规程的正确性和可用性等方面提出基本要求。

3.17

编者导则 writer's guide

事故处理规程编者导则给出了详细的方法,以确定如何编写规程的内容和相关支持图表,从而使规程是完整的、准确的、易读的和易使用的。

4 事故处理规程的开发过程

4.1 概述

事故处理规程的开发分为多个步骤,见图1。

若事故处理规程采用了其他技术形式(如计算机化),其开发的各个环节还应符合相关标准规范如NB/T20267—2014和NB/T20270—2014的规定。

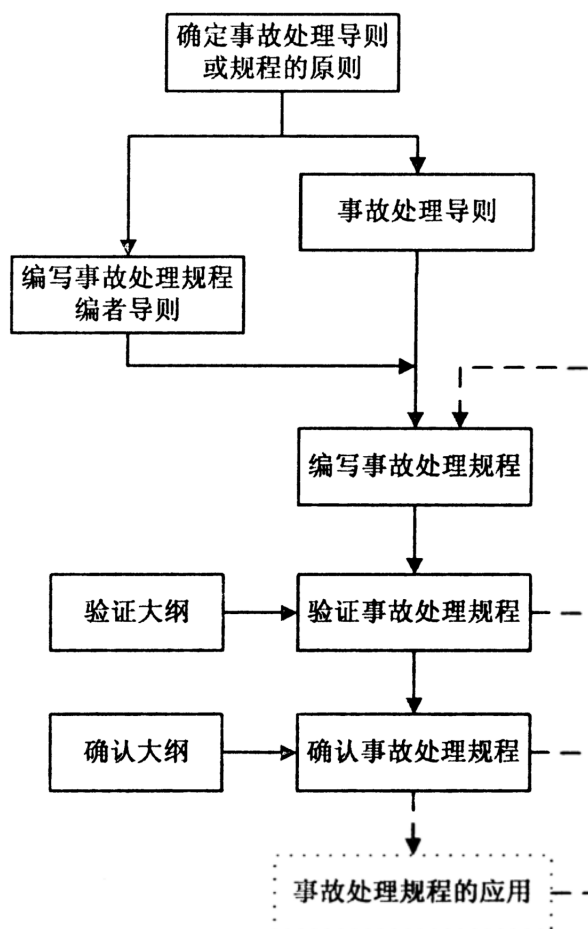


图1 事故处理规程开发过程

4.2 确定事故处理导则或规程的原则

事故处理导则或规程的原则涉及事故处理方法的确定、事故处理导则或规程在核电厂规程中的作用、导则或规程人因工程、运行组织等方面的内容。

事故处理规程和事故处理导则在导向方法上应保持一致。事故处理规程导向方法主体上分为事件导向法、状态导向法和征兆导向法三类。

4.3 事故处理导则

根据所确定的事故处理导则或规程的原则，进行事故处理导则开发。事故处理导则（见第5章）是事故处理规程的技术基础。

事故处理导则的开发一般有两种方法：革新法和参考法。革新的开发方法即开发一套新的、原创的事故处理导则，需要吸收以往实践经验，遵照有关标准，开展首创的研究、全面的分析，开发完善的事故处理导则各组成要素，并进行充分的论证和确认。参考法相对容易，可以借鉴已有的、成熟的事故处理导则或规程，只需开展较少的分析。

4.4 编写事故处理规程编者导则

编者导则用于规范并保证事故处理规程是完整的、准确的、易读的和易使用的。编者导则应包含将事故处理导则转化成事故处理规程的方法。

4.5 编写事故处理规程

4.5.1 概述

按照编者导则，基于事故处理导则，编写核电厂的事故处理规程。

4.5.2 事故处理规程编者

事故处理规程的编写需要多方面的信息和技能，宜采用团队的方式开展工作。整个团队应熟悉且不限于：技术文件的编写、人因工程、核电厂运行、操纵员培训和工程设计。

4.5.3 由导则转化成规程

事故处理规程中的操作步骤取决于转化所依据的事故处理导则的内容和方法。事故处理导则确定了核电厂所需达到的目标、要求可用的系统和子系统、需达到的性能水平、需要操纵员操作的情形及这些操作的执行顺序。

在事故处理导则的基础上，规程编者扩展相关信息，并且开展有关的技术分析、功能分析和任务分析。在规程的整个开发过程中，运行经验和编者导则有助于规范事故处理规程的形式以优化操纵员的执行表现。

对于事故处理规程中的操作步骤的顺序和关系，规程编者应始终遵照事故处理导则，以确保不违背事故处理导则的技术方法。通常从系统层次开始，然后在子系统层次和设备层次进行细化，最后将具体的操纵员任务确定并编写成操作步骤的形式。附录A给出了该过程的说明。

4.5.4 功能分析和任务分析

事故处理规程的开发应与人因工程的功能分析和任务分析相结合。

功能是指能使核电厂各个特定目标得到满足所依赖的手段。这个层次的分析与事故处理规程中的“功能导向”的功能相关联。功能是通过某些系统或多个系统的组合来实现的，其中这些系统或系统的组合由硬件、人员或两者结合组成。

功能和完成这些功能的系统的提炼（功能分析），通常是基于任务的方式进行分析。任务分析为定义操纵员所需信息提供基础。任务与功能一样，也可以进行多层次的分析，这取决于所需的应用。附录A给出了事故处理规程开发过程中信息提炼的示例。

4.6 验证和确认事故处理规程

在事故处理规程开发过程中，应必须对其进行验证（见第7章）和确认（见第8章）。验证和确认的目的是为了确定信息和指令的正确性，确定规程是否能被正确地、有效地执行，证明规程是否能恰当地缓解瞬态和事故。事故处理规程的技术和人因工程的充分性都应在验证和确认过程中得到检验。验证和确认与规程编写是交互的过程。

5 事故处理导则

5.1 概述

事故处理导则是从瞬态和事故分析得到的工程数据转化而来的，这些信息进而用于编写事故处理规程。

5.2 确定事故处理导则的原则

5.2.1 事故处理导则的基本原则

在编写事故处理导则之前，首先应确定与事故处理导则的原则有关的各个方面：

- a) 事故处理方法，宜采用征兆导向法或状态导向法；
- b) 事故处理导则应与核电厂的设计基准一致，包括与核电厂运行文件的关系；
- c) 事故处理导则应尽可能应对所有可能发生的事故状态，并对各种可能发生的设备失效和操纵员人因失误提供指导；
- d) 除了功率运行状态，事故处理导则应考虑停堆状态(包括余热排出系统连接及一回路开口状态)下的事故运行；
- e) 鉴于人因失误可能产生的严重后果，事故处理导则应考虑较优化的人因工程；
- f) 应考虑或确定事故工况下的运行组织和人员职责。

5.2.2 事故处理导则的开发方法

事故处理导则的开发应在分析的基础上至少确定以下事项：

- a) 事故处理的进入条件；
- b) 初始诊断；
- c) 事故后的电厂稳定策略；
- d) 基于事件或基于状态/征兆的恢复策略；
- e) 基于征兆或状态的持续监测；
- f) 安全功能的监测及恢复；
- g) 发生概率较高的多重事件的恢复策略，用于重建关键系统和支持系统；
- h) 事故状态下的仪表响应；
- i) 核电厂的危险工况，操纵员和现场人员可能面临的情况。

5.3 支持分析

支持分析是事故处理导则开发中至关重要的环节。典型的支持分析内容包括：

- a) 确定事故处理导则所应开展的事故分析；
- b) 分析事故工况响应的薄弱项；
- c) 开发和确认事故步骤策略。

在支持分析中，事故分析是确定事故处理策略所依赖的方法，尤其是扩展的事故分析。

在事故处理导则的开发过程中，应结合执照申请事故分析、工程判断、实践经验，确定事故处理导则所需的基于现实假设的扩展的事故分析。扩展的事故分析宜采用最佳估算分析方法。

由于事故处理导则涉及核电厂各系统的运行，因此支持分析应涵盖但不限于以下内容：

- a) 安全相关系统和设备的设计容量和限值；
- b) 安全功能相关的特定数值；
- c) 事故处理导则中使用的阈值与准则；
- d) 事故处理导则中使用的与时间相关的参数；
- e) 与材料热应力等方面有关的要求；
- f) 自然循环下的运行特性；
- g) 与次临界度裕量有关的特定数据；
- h) 所要求的支持系统及其恢复策略的分析；
- i) 多个策略或技术的优先级分析；

j) 设备与仪表的不确定度。

5.4 事故处理导则的确认

事故处理导则应进行确认,以保证事故处理导则在技术上是正确、合理的。确认可采用模拟机、审查、研讨会或专题讨论会等方式。根据需要,还可采用其他方法对所选用的确认方法进行补充。

5.5 记录和归档

应对事故处理导则开发过程进行详细归档,详细地记录所有从基础分析开始到用于事故处理导则开发之间的应用过程信息,从而使整个开发过程具有可追溯性。归档的内容应包括分析所采用的假设条件、分析结果的参考文件、事故处理导则实际开发过程的描述、确认过程的描述。

6 事故处理规程编写

6.1 总则

6.1.1 概述

应制定事故处理规程编者导则,保证规程编制过程及内容的标准化,保证事故处理规程的可用性、正确性、完整性、易读性和友好性。

事故处理规程的编写,应考虑核电厂的具体环境因素,通常包括工作压力(如心理、时间和工作量)和环境条件的变化(如照明亮度变化)。为了使规程的格式符合在应急工况下人因工程的需要(例如,能够从一定距离、一定角度阅读规程),应对规程的格式(如字体、字号和行距)进行优化。

6.1.2 一致性

事故处理规程应始终保持结构、格式、字体和内容的一致性。当需要进行规程间调用或规程内跳转时,规程的一致性对保证其易读性、流畅性和连续性等方面起到重要作用。

6.1.3 调用和跳转

如可能,实现同一目标的操作指令应保持一致。对于规程间调用和规程内跳转,所使用的方式应是快速的,以尽可能地减少规程执行的中断次数和产生错误的几率,同时应标明调用和跳转的原因以及是否返回。调用和跳转的设置应避免产生死循环或操作缺失。

6.1.4 辅助手段

辅助手段(如图、表、曲线、流程图和判断框)用于协助操纵员决策。辅助手段应能缩短决策时间并保证决策过程的准确。

6.2 可读性要求

事故处理规程中信息的表达方式决定了规程可读性的高低。可读性是指规程内容书面描述的特点,它反映了操作信息是否能够被简单、快速、准确地读取和理解,可读性包括易读性和易理解性。易读性是指文字符号的编印和排列特点;易理解性是指书写材料的呈现方式。

事故处理规程的易读和易理解应具备以下特点:

- a) 方便阅读;
- b) 能快速连续地阅读;
- c) 能正确地理解;

- d) 无需借助其他辅助资料;
- e) 内容易于接受;
- f) 内容简单易学;
- g) 内容便于记忆;
- h) 指令清晰;
- i) 内容简单、有序且贴切。

6.3 事故处理规程的结构

6.3.1 概述

事故处理规程的结构宜包括下述内容:

- a) 封面;
- b) 目录;
- c) 范围;
- d) 进入条件;
- e) 自动动作;
- f) 立即操作;
- g) 延迟操作;
- h) 定期监视;
- i) 支持材料(如附录)。

6.3.2 封面

事故处理规程应含有封面页。封面页应包含事故处理规程的特定标识:所适用的机组,执行人员,版本,日期,页数,审查、批准签字栏等信息。

如果事故处理规程没有封面页,则需在其首页中列出上述信息。

6.3.3 目录

事故处理规程目录应能避免操纵员产生混淆,并能在最短的时间内定位到规程的具体章节。

6.3.4 范围

事故处理规程应包含简要的说明,以描述规程所要实现的目标。通常,用简洁的标题来指明规程的使用范围。

6.3.5 进入条件

事故处理规程的进入条件极其重要,进入条件应能使操纵员确认所用规程是否正确。

6.3.6 自动动作

事故处理规程应设置相关指示用于提示操纵员核电厂的重要安全系统已自动动作。

6.3.7 立即操作

立即操作是指核电厂发生事故时,需操纵员立即执行的操作。在事故处理规程中,这些操作应能防止核电厂状态的恶化,并能缓解事故造成的后果,同时允许操纵员对核电厂的情形进行评估。

6.3.8 延迟操作

延迟操作用于在异常和事故工况下，将核电厂带入正常、稳定的工况或者安全的稳态工况，以使核电厂处于安全的状态。延迟操作构成了事故处理规程的主体。

6.3.9 定期监视

定期监视用于操纵员对重要参数和设备运行的定期检查和相关重要操作的执行。

6.3.10 支持材料（附录）

支持材料是不包含在规程正文中而作为附录的含有操作的内容。操纵员应能快速、方便地使用支持材料，且不同材料应易于区分。

6.4 事故处理规程的格式

6.4.1 概述

事故处理规程的格式应有助于操纵员理解其内容，并在最大程度上减少操纵员对规程的内容产生混淆和出现执行错误。规程的格式还应帮助操纵员快速、准确地定位并执行操作。

应对事故处理规程的整体布局和结构进行设计，包括信息布局、描述风格和信息详细程度等。信息布局是指操作步骤及其支持信息的排列方式。不同层次的操作可通过语句的缩进来区分。描述风格是指规程内容的表达方式，如可用完整的语句来描述，也可用简短的词组来描述，或者采取两者相结合的方式。信息详细程度是指规程内容表达的详细程度。章节标识和指令的详细程度应反映操纵员的经验和训练水平。

所采用的规程格式应能使得操纵员快速、准确地查找并理解基本信息。

6.4.2 信息标识

事故处理规程的每一页（包括封面），都应包含有充分的信息用于识别规程，包括所适用的机组、当前版本、页数。这些信息应统一位于容易读取的地方。

6.4.3 页面布局

为便于阅读，信息排列宜做到：不混乱、行距足够大、页边距足够大以便复制和装订。此外，装订应不遮盖信息，且易于手持。

信息排列应尽量避免出现连续信息的中断。每本规程（或子规程）应另起一页，而且每个操作步骤应完整地呈现在同一页内。

6.4.4 “警告”、“注意”和“说明”

应明确“警告”、“注意”和“说明”的不同含义。可选择其中一个或多个在整个规程中规范使用。它们用于对规程中重要或关键信息进行警示，以避免造成人员伤亡、工作人员健康损害或设备损坏；或者用于对重要补充信息进行强调，以助于规程的执行和操纵员训练。

设置“警告”、“注意”和“说明”应满足以下要求：

- a) 突出显示以吸引操纵员的注意力；
- b) 与相关步骤直接关联；
- c) 内容不应引起误解；
- d) 书写应考虑其阅读的完整性，不会因步骤或翻页而中断。

6.4.5 标记

应设计标记手段，用于操纵员执行指定操作时跟踪当前步骤。

6.4.6 分割、标题和编号

应采用一种适当的标题和编号方法，对规程内容进行清晰地组织和分割。该方法应具有逻辑性质，以让操纵员知道其在整体文件中的位置。该方法还应使操纵员能识别规程的各步骤。

6.4.7 强调

规程中存在某些信息需操纵员给予关注的，应在整套事故处理规程中采用统一的强调方法。

6.4.8 定位

需提供一定的手段用于快速地识别规程或子规程的具体章节，以便操纵员快速定位。

6.4.9 图和表

规程中的图和表应有助于操纵员决策和信息查找。为有效达到该目的，图和表应符合以下要求：

- a) 标题和含义明确，便于规程正文的引用及方便查找；
- b) 仅包含用于澄清或达成规程正文有关目的的相关信息；
- c) 用标准的专业图文来绘制；
- d) 设置在便于查找和使用的位置。

6.4.10 流程图

流程图可作为事故处理规程的一种形式或一种辅助手段，描述事故诊断、操作步骤和逻辑顺序，以及用于辅助训练，附录B给出了两种可用于事故处理规程的流程图的示例。

6.5 表达和描述

6.5.1 概述

事故处理规程的编写应采用简洁、通俗、清晰、明确的表达和描述方式。

6.5.2 词汇

应使用最为简洁、通俗和清晰的词汇来准确地表达规程的内容。规程中的词汇应使用符合以下规范的标准语言，并且易于操纵员理解：

- a) 使用简短的词汇和常用词汇；
- b) 使用培训过程中所采用的语句和行业内标准术语；
- c) 使用详细、清晰的词汇来精确描述操纵员需执行和遵守的信息；
- d) 整套规程采用的词汇和含义应统一；
- e) 避免使用难以界定的副词（如频繁地、缓慢地）。

6.5.3 缩写、缩略语和符号

应使用操纵员熟悉的缩写、缩略语和符号，使得操纵员无需去查询缩略语表。当缩写、缩略语和符号用于描述标签或设备时，操纵员应能立即识别出标签或设备的名称和位置。

6.5.4 语句结构

句子、从句和短语应简洁，并且使用标准的语言语法。对于要求操纵员执行或遵守的句子应使用祈使句。

6.5.5 标点符号

应遵守所使用语言的标点符号的标准用法。标点符号的使用应有助于让操纵员清楚地理解规程编者的思想和意图。恰当地使用标点可以降低操纵员误解规程编者本意的可能性。

6.5.6 字体

中文应使用常用字体和格式，强调词语或句子时可以使用其他格式。英文应遵守标准用法，包括字母大写。

6.5.7 单位

规程中所使用的单位应是操纵员所熟知的，应与电厂仪表所用的单位保持一致，而无需进行中间的转化、换算和运算。

6.5.8 数字

规程中数字的书写方式应是操纵员所熟悉的。数字应和设备上标识的数字尽量保持一致，以便操纵员迅速地识别和查找。数字用于表达仪表读数时，应和仪表所显示的数字保持一致，而无需进行中间的转化、换算和处理。

6.5.9 偏差

应使用偏差范围来限定数值范围，以避免估算。表达偏差范围的单位应和对应的画面或控制器上的单位一致。

6.5.10 公式和计算

在事故处理规程中，应尽量减少让操纵员使用公式和进行计算，因为使用公式和计算不仅会耗费时间，还有可能增加操纵员出错的可能性。对于必需须计算的情况，计算过程应尽可能简单，并预留出空间。

6.5.11 条件语言和逻辑

条件语言和逻辑广泛应用于事故处理规程，用以描述一系列条件和操作顺序。应对条件语言和逻辑建立规范的原则以保证逻辑正确、清晰和完整。所使用的条件语言和逻辑术语应保持一致性。逻辑术语和顺序宜突出显示或强调，以便操纵员可以清楚地识别所有条件和给定逻辑顺序的范围。

附录C中给出了适用于事故处理规程的条件语言和逻辑顺序。

6.6 事故处理规程的内容

6.6.1 排序

应根据技术必要性对操作任务和操作步骤进行排序。任务的排序应考虑主控室的布置和结构，以优化操纵员执行规程时的移动和监视。对于顺序操作步骤，应考虑让操纵员明白其目的和完成结果。规程中应说明操作步骤在给定顺序中何时不必执行。

6.6.2 验证性步骤

验证性步骤用于检查某操作任务或操作序列的目标是否达到，有以下三种验证方法：

- a) 检查操作已产生设备命令信号；操纵员不应依赖这种检查，而应使用确定的指示；
- b) 检查某步操作已得到确定的指示，表明设备已根据命令正确响应；
- c) 检查操纵员已正确执行某步操作或一系列操作步骤。

应该在规程中恰当使用以上三种验证性步骤，以保证设备正确响应、操纵员操作得到执行且执行正确。

6.6.3 非顺序步骤

规程中可能存在其执行时间不确定的步骤（如“当换料水箱水位低时将安注泵吸入口从换料水箱切换至从地坑取水”），应说明何时、何地、何种条件下、采用何种时间顺序来执行这类非顺序步骤。

6.6.4 等效步骤

等效步骤是指其中多个操作手段或操作顺序均可实现其功能目标的步骤。对于这种情况，规程应指定优先方法（步骤或顺序）和替代方法，优先方法不可用时则使用替代方法。

6.6.5 周期性步骤

周期性步骤指需要操纵员重复执行的操作，典型的例子是监视或控制某些电厂参数（如“每30 min 检查冷凝水箱的水位”）。对于这些操作步骤，应向操纵员说明执行的时间或多经常执行，对操纵员提供提醒，并告知操作终止条件。

6.6.6 限时步骤

限时步骤是指需要操纵员在规定的時間间隔或在某步操作之后的某段时间内执行的操作。应提供一定的手段来辅助操纵员在规定的時間窗口执行这些步骤。

6.6.7 并行步骤

并行步骤是指需要在同一时间执行的操作。规程中应明确指明并行步骤，以使操纵员能够容易地关注到相并行的所有步骤。并行的步骤数量不应超过主控室人员能力。

6.6.8 诊断步骤

诊断步骤是指在事故处理规程中用以引导操纵员进入恰当步骤的步骤。诊断步骤应为操纵员提供清晰和明确的诊断信息，用于诊断决策，并正确地引导操纵员进入恰当步骤。诊断步骤可采用流程图、图表或其他辅助方式。

6.6.9 “警告”、“注意”和“说明”

“警告”、“注意”和“说明”应准确简明，其内容应仅与警告、注意和说明有关，不应包含需要执行的操作。

6.6.10 位置信息

事故处理规程应向操纵员提供使用率低、较偏僻或者难以找到的设备、控制器或画面的位置信息。

6.7 主控室人员和职责

6.7.1 概述

事故处理规程编写应结合主控室人员配置和职责分工。

6.7.2 人员和规程的一致性

为保证事故处理规程的执行，规程的编写应考虑最小运行值人数能够满足执行特殊操作、并行步骤以及其他方面的要求。

6.7.3 职责分工

规程编写应考虑主控室内人员的职责分工和组织关系，以便主控室人员高效和准确地完成规程的各种操作和各方面要求。

6.7.4 主控室人员

主控室的人员数量和资质决定了可以执行的顺序操作、并行步骤和其他任务的总数以及规程的执行效率。

规程的编写应考虑以下目标：

- a) 人员站位重叠、冲突的最小化（在同一时间、同一地点执行操作，交叉路径）；
- b) 避免操纵员重复不必要的任务；
- c) 确保主控室值长能及时监控操纵员操作和电厂状态。

7 事故处理规程验证

7.1 验证的目的

事故处理规程验证的主要目的在于检验内容书写的正确性和技术要求的准确性。

7.2 验证的方式和要求

事故处理规程验证包括对规程与其开发过程中所使用的输入文件进行比较。这些文件包括编者导则、事故处理规程参考文件、核电厂设计文件、运行技术规格书、最终安全分析报告等。

应根据验证大纲开展验证活动，包括验证准备、评价、问题解决、归档等方面：

- a) 验证准备包括确定信息需求，指导如何应用评价准则，确定验证人员及评价计划。其中，验证人员应为规程编者之外的具备资质的人员。因验证在确认之前，验证准备应采用对确认影响最小的方式进行；
- b) 评价包含书写正确性和技术准确性两个方面，这两方面验证所要求的专业技术是不同的。这一阶段应识别出规程与上游输入文件之间的所有偏差；
- c) 在问题解决阶段应处理所有规程与上游输入文件之间的所有偏差，应注意不是所有的偏差问题都需要修改规程；
- d) 归档过程是对验证过程所有活动的细节都进行记录，以保证可追溯性和完整性。

书写的正确性是指检查规程与编者导则的一致性，包括对内容的易读性、格式、信息描述和规程调用与跳转信息等方面进行检查。

技术的准确性是指检查规程与上游输入文件的一致性。其评价内容包括规程的进入条件、操作顺序、步骤、警告/注意/说明、数值和设备信息，以及处理策略。

事故处理规程验证的检查清单示例参见附录D。

若事故处理规程采用了新技术，验证时应考虑其特殊验证要求。

8 事故处理规程确认

8.1 确认的目的

事故处理规程确认的目的是保证操纵员可以使用事故处理规程应对应急工况,即保证规程是可用的和正确的。

8.2 确认的方法

事故处理规程确认一般有以下五种确认方法:

- a) 实景试验法:在观察者或审查者见证下,在保证电厂安全运行的前提下,使用电厂系统和设备进行实际情景操作;
- b) 模拟机法:在观察者或审查者见证下,操纵员在模拟机上对特定情景进行控制功能操作;
- c) 排练法:在观察者或审查者见证下,操纵员在应对特定情景过程中对规程的操作步骤进行一步一步地演练;
- d) 推演法:在观察者或审查者见证下,操纵员对特定情景响应过程的操作步骤进行解释和/或讨论;
- e) 参考法:采用通用事故处理规程时,使用相似核电厂规程确认过程中所得到的数据。

应制定确认大纲,由规程编者之外的具备资质的人员作为确认人员来开展确认活动,对确认过程进行详细归档,并宜编写确认报告。这些文件为规程修改提供依据。

若事故处理规程采用了新技术,确认时应考虑其特殊确认要求。

8.3 确认的要求

8.3.1 规程可用性确认

事故处理规程可用性确认包含两个方面的检查:内容详细程度和易理解程度。

内容详细程度是指规程内容应充分且适度,在提供所有可能信息与最少必备信息之间达到平衡。执行规程的确认时,操纵员与观察者应对内容详细程度进行评价,包括以下方面:

- a) 信息对于执行每一步骤或进行决策是否充分?
- b) 操纵员所使用的设备位号、缩写、位置等信息是否给出?
- c) 操纵员是否使用了标题和编号来查找引用或跳转信息?

易理解程度是指规程中的信息是否表述恰当,操纵员在应急工况下是否可以理解该信息。执行规程的确认时,对易理解程度的评价包括易于阅读、标准术语、格式恰当、重点突出。典型的问题包括以下方面:

- a) 规程是否易于阅读?
- b) 数值是否准确、正确?
- c) “警告”、“注意”和“说明”是否可辨识和可理解?
- d) 操纵员是否能正确执行规程调用和跳转?
- e) 操纵员是否能遵守规程?
- f) 操纵员是否能找到恰当的步骤?
- g) 操纵员在规程引用或跳转时是否遗漏步骤?
- h) 操纵员跳转时进入位置是否正确?
- i) 操纵员跳转时退出位置是否正确?

8.3.2 规程正确性确认

事故处理规程的正确性确认包含两个方面的检查：与设计的一致性和与操纵员的相容性。

与设计的一致性的确认可保证操纵员能够使用电厂所设计的系统和设备完成所要求的操作，并且能在应急工况下安全地执行。典型的问题包括以下方面：

- a) 操作能否按顺序执行？
- b) 规程中是否缺漏其他替代成功路径？
- c) 电厂仪表是否提供了所要求的信息？
- d) 所列出的征兆/状态是否足够用于选择所要求的规程？
- e) 电厂征兆/状态相应的进入条件对操纵员是否可见？
- f) 操纵员是否需要用到规程未提供或指定的设备或信息？
- g) 技术依据是否与电厂响应一致？
- h) 仪表读数（就地或远传）及其误差是否与规程一致？
- i) 规程（文本或流程图）是否与工作情形相协调？

与操纵员的相容性的确认，是为了检验运行值人力是否充足以执行规程所规定的操作，操纵员职责分工是否与规程所规定的操作相冲突。该评价还包括以下检查：时间相关步骤能否由运行值在分配的时间内完成，人员所承担的操作是否与规程相协调，运行值全员能否有序地执行操作。在操纵员和观察者开展确认过程中，典型的问题如下：

- a) 操纵员的问题：
 - 1) 识别恰当的规程是否有困难？
 - 2) 规程是否包含不易理解的步骤？
 - 3) 不同操作过程中是否有顺序问题？
 - 4) 对流程图中的恰当跳转的决定是否有困难？
 - 5) 规程的导向（路径）是否需要支持？
 - 6) 规程是否包含不必要的信息？
 - 7) 规程所使用的术语是否与通用术语不一致？
 - 8) 图和表是否不易理解？
 - 9) 规程所用的仪表、设备是否不存在？
 - 10) 主控室的仪表读数准确性是否与规程要求不同？
 - 11) 规程中的参数数值是否不能由现有仪表确定？
 - 12) 规程是否包含不清楚或错误的指令？
 - 13) 是否需要在规程中补充其他信息？
 - 14) 阅读和使用指令是否有困难？
 - 15) 处理应急工况时是否感到不适？
 - 16) 是否感觉电厂始终可控？
- b) 观察者的问题：
 - 1) 规程进入条件的情形是否不可认知？
 - 2) 对进入条件诊断后，操纵员是否无法进入恰当的规程？
 - 3) 规程中是否存在冗长的步骤？
 - 4) 顺序执行步骤时是否出现错误？
 - 5) 操纵员操作是否有错误？
 - 6) 操纵员决策是否有问题？
 - 7) 操纵员对指令的理解是否有问题？
 - 8) 操纵员执行流程图的路径是否有问题？
 - 9) 操纵员阅读或使用规程是否有问题？

- 10) 规程中是否有操纵员无法执行的步骤?
- 11) 在特定情景下操纵员是否需要更细节的指令?
- 12) 不同规程的相同指令是否有偏差?
- 13) 规程所用的仪表、设备是否不存在?
- 14) 规程中的参数数值是否不能由现有仪表确定?
- 15) 指令的执行是否用到未注明位置或操纵员不知道的特殊设备?
- 16) 特定情景是否导致了操纵员无法稳定参数的情形?

应确定规程编者之外的具备资质的人员作为确认人员,根据确认大纲开展确认活动,对确认过程进行详细归档,并宜编写确认报告。这些文件为规程修改提供依据。

若事故处理规程采用了新技术,确认时应考虑其特殊确认要求。

9 事故处理规程文件体系

9.1 概述

事故处理规程文件体系包括以下两类:技术文件和管理文件。

9.2 技术文件

9.2.1 事故处理规程

事故处理规程是一套完整的文件(包括主控室使用的文件和现场使用的文件),可以是纸质的,可能还包括数字化的。

9.2.2 技术基准和背景文件

这些文件对事故处理规程的组织、目的、各规程结构及与其他规程的关系提供详细说明,还对各规程中的操作步骤、指令和元素提供细节。这些文件的特点如下:

- a) 技术基准文件为整套事故处理规程的各个元素提供依据;
- b) 背景文件对各个事故处理规程的各个元素的历史和原因进行跟踪记录。

9.2.3 其他相关文件

事故处理规程相关的其他文件包括:

- a) 安全分析报告;
- a) 运行限值和条件/运行技术规格书;
- b) 系统设计手册;
- c) 运行规程;
- d) 设备规格书和运行维修手册;
- e) 事故处理方法的分析和审查资料。

9.3 管理文件

下列文件是支持事故处理规程编写所需的主要的管理文件:

- a) 事故处理规程编者导则:制定了一般性原则和一系列准则,以规范规程编写的一致性;
- b) 事故处理规程用户指南:规定了事故处理规程使用时需遵循的原则和准则,是对事故处理规程编者导则的补充;
- c) 事故处理规程的验证大纲和验证报告;

- d) 事故处理规程的确认大纲和确认报告；
- e) 监管要求：监管部门规定相关的管理和技术标准；
- f) 质量保证要求。

附 录 A
(资料性附录)
事故处理规程开发过程示例

本附录说明了电厂信息的提炼过程，以用于从事故处理导则开发事故处理规程。该示例的目的是阐明一种过程，而不是为了说明一种方法。

在以下示例（表A.1）中，每个层次的分析都会确定若干元素，如安全壳完整性功能分析的结果会包含有若干系统。其中每个系统可再进行功能和任务层次的分析，用于为事故处理规程中的步骤提供技术依据。为简化起见，示例中只给出了一个路径：从确定电厂目标（安全），到规程的某个特定步骤。

表 A.1 信息提炼示例

分析的层次	元素示例
电厂目标	<u>安全</u> 发电
功能（高层次）	<u>反应性控制</u> 安全壳完整性
系统	<u>控制棒驱动系统</u> 反应堆保护系统 硼水控制系统
功能（低层次）	<u>快速引入负反应性</u> <u>缓慢引入负反应性</u>
任务	<u>快速插入控制棒</u> 投运硼水控制系统
功能分配	机器——自动停堆（反应堆保护系统紧急停堆信号） <u>人员——ATWS 时手动停堆</u> 手动停堆/操纵员判断
操纵员任务	识别工况 <u>手动停堆</u>
任务描述	手动停堆 a) 按下手动停堆按钮 b) 确认控制棒插入 1) 控制棒插入灯亮（绿色） 2) 监视各控制棒棒位在 0 步 c) 确认反应堆功率下降 1) 功率量程通道（PRC）位于低限 2) 中间量程通道（IRC）通电 3) 监视通量降低
规程步骤（按照编者导则）	4 操纵员操作 4.1 紧急停堆 4.1.1 按下手动停堆按钮（RPA300T0、RPB300T0） 4.1.2 确认控制棒插入（RGL061KS） 4.1.3 确认反应堆功率下降（IRC）
注：表中下划线标识内容是该特定路径提炼中相应层次分析的结果。	

附录 B
(资料性附录)
流程图

以下流程图示例1（图B.1）和流程图示例2（图B.2）的形式可用于事故处理规程。

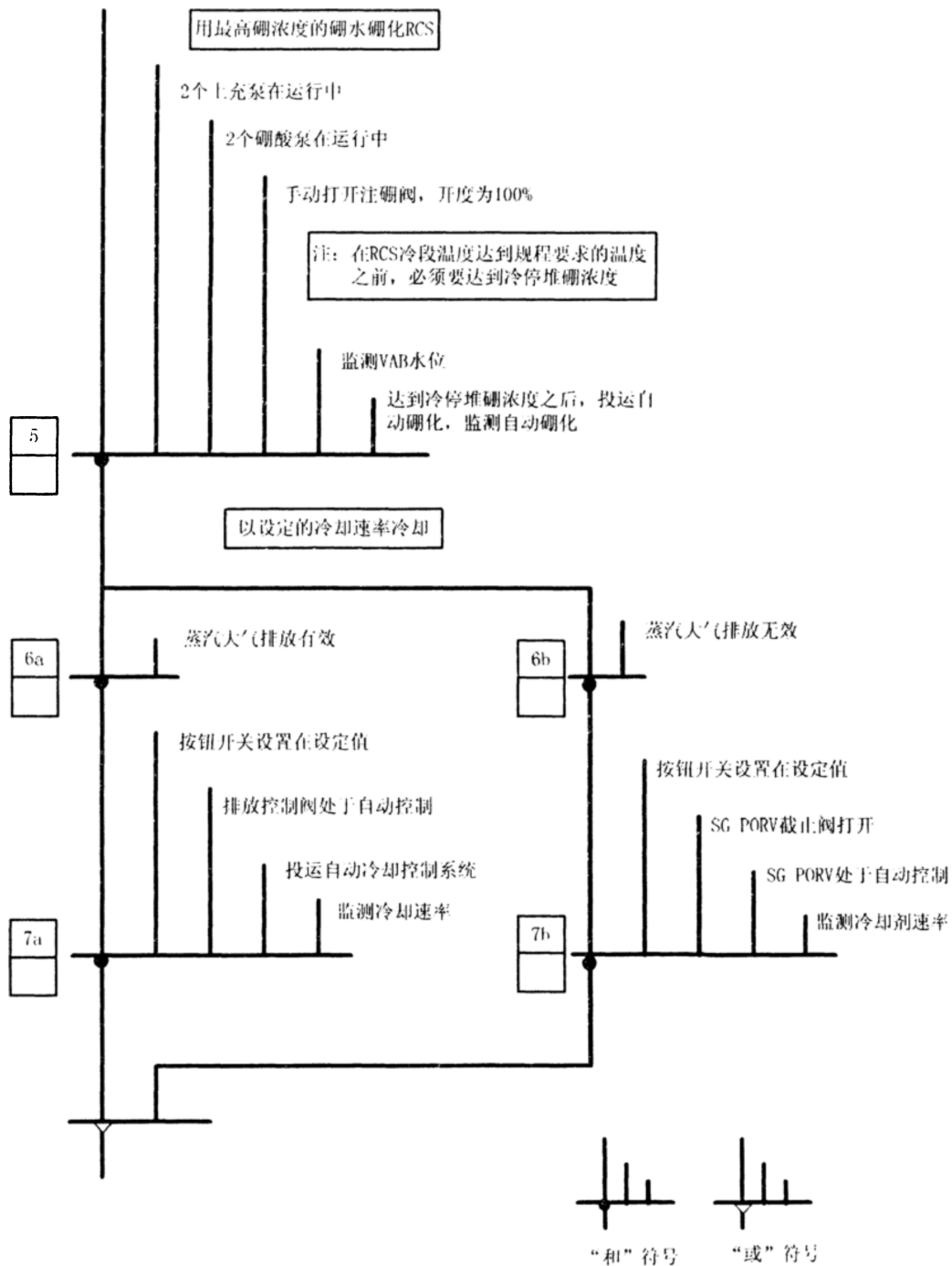


图 B.1 流程图示例 1

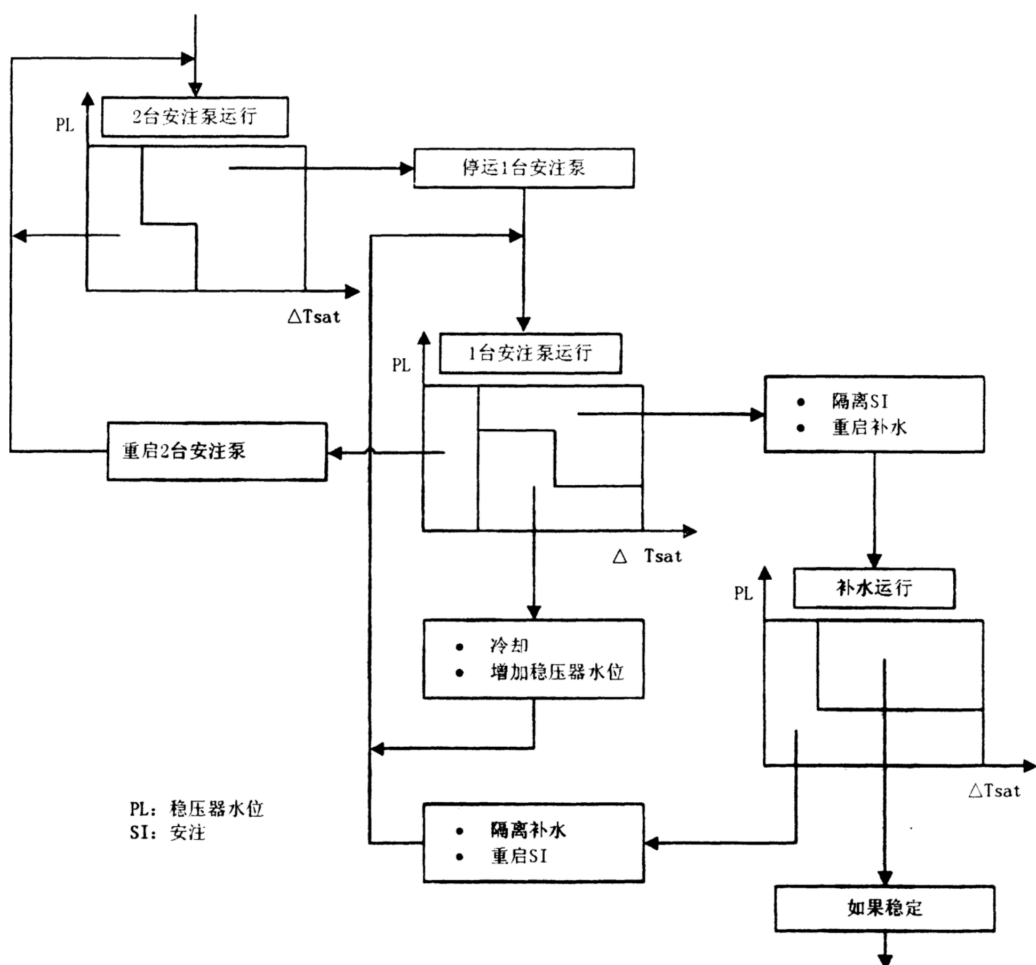


图 B.2 流程图示例 2

附录 C

(资料性附录)

条件语言和逻辑顺序

C.1 概述

事故处理规程中常用的逻辑术语包括“且”、“或”、“如果”、“如果不是”、“则”和“当”，其作用是描述一系列条件以对操作步骤按条件进行排序，或描述复杂的条件组合、其他前置条件、操作。每个逻辑术语对应特定的功能，应在事故处理规程中统一一致并符合惯例。另外，当使用逻辑术语组合时应特别注意，以避免模糊和难以理解。以下示例说明了如何正确地使用逻辑术语和逻辑术语组合。

C.2 “如果”、“如果不是”、“当”和“则”的用法

当步骤需按照特定条件或条件组合执行时，这些步骤应以“如果”、“如果不是”或“当”开头，并对这些条件（前提条件）进行描述，接下来，以“则”开头并对需采取的操作进行描述。例如：

- a) “如果 RPS 紧急停堆未触发，
则投运硼水控制系统，并隔离反应堆冷却剂净化。”
- b) “当稳压器水位达到 50%，
则停运上充泵。”

“如果不是”的使用应限于操纵员需要应对两个可能条件中的第二个条件的情况。“如果”此时应用于指定第一个条件。例如：

“如果压力升高，则停止安注泵，如果不是，则启动第二台安注泵。”

“则”不应用于操作步骤地末尾，去指导操纵员执行同一步骤的另一个操作，因为这样就同时操作了。例如：

“检查所有安注箱隔离，则用辅助喷淋冷却稳压器。”

此时操作将嵌套了，这样会导致以下问题：没注意到，没被执行；当使用检查框或签字框时，会难以检查每个步骤的表现；逻辑混乱。

C.3 “且”的用法

通常操作步骤应按顺序执行，各操作步骤之间不需要用“且”进行衔接。但对于多个条件组合的情况，应在每个条件的描述前使用“且”。例如：

“如果 RCS 压力升高，
且稳压器水位升高，
且 RCS 温度升高，
则执行规程第 6.1。”

为简化较长的条件顺序，用“且”衔接的条件通常不应超过三个。如果操作执行的条件超过三个，则应使用项目符号。例如：

“如果所有下列条件得到满足，

- a) 条件1；
- b) 条件2；

c) 条件3;

d) 条件4;

.....

则（操作）。”

当作为简单连词使用时，“且”字无需强调（如“停止低压安注泵且置为备用”）。

C.4 “或”的用法

“或”用于多个条件选其一的情况。“或”用于多个条件时，具有全部包含的意思，即任何一个或全部条件都有可能出现。例如：

“如果RCS压力低于或等于破口蒸汽发生器的压力；

或

如果稳压器水位高于20%；

则停止对RCS进行降压。”

对于替代操作情况，应减少“或”的使用，并且尽可能确定优先关系。如果不能确定优先级，而且替代操作是等同，则有必要使用与以下示例类似的方法来规定“或”的排他性：

“启动1号柴油机或3号柴油机，但不都启动。”

C.5 逻辑术语组合

应避免在同一步骤中使用“如果”和“则”的同时，使用“且”和“或”。当同时使用“且”和“或”时，会造成逻辑混乱和含糊不清误解。例如：

“如果条件A且条件B或条件C出现，

则执行步骤5.3.6。”

以上逻辑具有两种含义：

a) “如果条件A且条件B出现，

则执行步骤5.3.6。”

b) “如果条件A且条件B出现，

则执行步骤5.3.6。

或

如果条件A且条件C出现，

则执行步骤5.3.6。”

如果在同一步骤中不能避免使用“且”和“或”，则应使用更加显式的用法（见a）和b））。

附 录 D
(资料性附录)

事故处理规程验证的检查清单示例

表D.1给出了事故处理规程验证应检查的项目清单。

表 D.1 验证检查的项目清单

检查项目	是	否	不适用
1. 规程编号是否准确地标识出使用人员?			
2. 规程的标题是否准确地描述规程的主题?			
3. 规程中由其他使用人员执行的步骤是否恰当标识?			
4. 规程的“目的”是否准确地概述了规程的目标?			
5. 规程的格式是否与编者导则中所规定的格式相一致?			
6. 是否对规程中的术语和缩写进行了定义或描述?			
7. 参考文件中是否包含了所有与制定具体技术条款、实现规程目的的文件?			
8. 是否给出了充分的预防措施和限制条件,以防止系统与设备发生未预期的动作?			
9. 是否给出了充分的预防措施和限制条件,以防止设备损坏或人员损伤?			
10. 核电厂响应是否与规程中的指示一致?			
11. 规程中是否标识了与化学控制相关的特殊处理或危害?			
12. 是否列出了所有必要的设备或人员的保护措施?			
13. 规程中是否标明了执行任务所需要的工具或保护设备?			
14. 仪表是否满足规程中所要求的精度要求?			
15. 规程是否提供了一种机制,要求操纵员在从协调员(机组长)或其他人员获得许可后才能开始执行规程?			
16. 整套规程所使用的缩写、术语和单位是否一致?			
17. 规程中所使用的数据表、图和实例是否标识恰当?对其引用是否标识恰当?			
18. 当某些步骤可以同时执行或不按照顺序执行时,规程中是否给出了明确的指导?			
19. 规程中所有的警告、注意、说明是否位于恰当的位置(在适用步骤之前)、且易于理解?			
20. 所有步骤的描述是否简短、简洁?			
21. 所有步骤或任务是否以要求执行行动的方式进行描述?			
22. 每一步骤是否包含不超过三个操作?(每一步骤只有一个操作是最理想的,如果步骤中的操作之间联系紧密且逻辑严谨则可以在一个步骤中最多设置三个操作)			
23. 规程中的步骤顺序是否是最有效的,是否与当前的方法和实践经验相一致?			
24. 规程中内容的详细程度是否与最缺乏经验的合格操纵员相容?			
25. 规程中词汇的复杂程度、语句的长短和语法结构对最缺乏经验的合格操纵员是否是合适的?			
26. 是否避免了不必要的回忆要求?			
27. 规程中的限值和数值的表达方式是否尽可能不需要操纵员进行心算或换算?			

表 D.1 验证检查的项目清单（续）

检查项目	是	否	不适用
28. 要求进行数据处理、转换时，是否提供了充分的辅助手段，如转换因子、图表等？			
29. 规程是否自成一体的，尽可能减少了规程调用和跳转？			
30. 规程调用和跳转时，其指令是否完整且准确，以防止遗漏重要的信息，并保证规程执行的连贯性而不会出现死循环的情况？			
31. 是否所有的量程、量和数值与所使用的单位相一致？			
32. 对较长的前提条件或计算是否提供了检查清单或数据表？			
33. 独立验证的要求是否与编者导则和相关规定一致？			
34. 将系统或设备恢复正常的步骤是否是必要的？			
35. 对于需要重点强调的内容，是否采用了一定方法进行标识，如大写、下划线、字体（黑体、斜体、颜色、字号等），并且清楚过度使用强调格式反而会降低效率？			
36. 如果可能，是否使用了图表来代替冗长的描述？			
37. 图表是否有明确的标题，易于理解并适合于规程任务？			
38. 图表是否位于可以让操纵员在执行相关内容时直接引用的位置？			
39. 规程中的公式与等式是否是从现有规程或参考文件中直接引用，而无修改？			
40. 补充背景信息是否独立于规程主体？			

中 华 人 民 共 和 国
能 源 行 业 标 准
核电厂事故处理规程编写要求
NB/T 20429—2017

*

核工业标准化研究所出版发行
北京海淀区骚子营1号院
邮政编码：100091
电 话：010-62863505
原子能出版社印刷
版权专有 不得翻印

*

2017年10月第1版 2017年10月第1次印刷
印数 1—50 定价 51.00 元