

**NB**

# 中华人民共和国能源行业标准

NB/T 20XXX—2016RK

代替 EJ/T 570—1999

## 压水堆安全重要流体系统单一故障准则

Single failure criteria for pressurized water reactor fluid systems important to safety

点击此处添加与国际标准一致性程度的标识

(报批稿)

(本稿完成日期：2016. 1. 10)

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 .....	II
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 单一故障准则及其应用规则 .....	2
5 不考虑单一故障的情况 .....	3
6 设计要求 .....	3
7 分析要求 .....	4

## 前 言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准代替EJ/T 570—1999《压水堆安全重要流体系统单一故障准则》，与EJ/T 570—1999相比，主要技术变化如下：

- 删除了范围中对其他类型轻水堆的适用规定（见第1章）；
- 增加了对“NB/T 20035”的规范性引用（见第2章）；
- 删除了对“GB/T 17569—1998”、“EJ/T 312—1988”、“ASME 第三卷”、“ASME 第XI卷”的规范性引用（见EJ/T 570—1999第2章）；
- 增加了术语“安全重要流体系统”、“假设始发事件”及其定义（见3.1、3.2）；
- 删除了术语“安全支持系统”、“安全功能”、“安全停堆”、“机组”、“始发事件”及其定义（见EJ/T 570—1999的3.1~3.3、3.9、3.10）；
- 修改了术语“单一故障”、“能动故障”、“非能动故障”、“短期”、“长期”、“操纵员差错”及其定义（见3.3~3.8，EJ/T 570—1999的3.4~3.8、3.11）；
- 增加了对“单一故障准则”的描述（见4.1）；
- 修改了应用规则中关于II类和III类、IV类工况始发事件的相关描述，并将执行的安全功能要求与HAD 102/17保持一致（见4.2.2，EJ/T 570—1999的4.2、4.3）；
- 删除了“设计者必须把操纵员一次差错视为一潜在单一能动故障”的要求（见EJ/T 570—1999的4.7）；
- 在“不考虑单一故障的情况”中增加了关于非能动的相关内容（见5.1）；
- 安全重要流体系统的运行方式中增加了“利用其他合适方式（如非能动）运行”（见6.1）；
- 删除了EJ/T 570—1999的附录A“关于ASME引用标准的说明”。

本标准参考ANSI/ANS-58.9-R2009《轻水堆安全重要流体系统单一故障准则》编制。

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：中国核动力研究设计院、中广核工程有限公司、上海核工程研究设计院、中国核电工程有限公司、核工业标准化研究所。

本标准主要起草人：陈宝文、黄代顺、关仲华、陈宏霞、隋海明、王建生、郭丹丹、张雪霜、董瑞林、杜建。

本标准所代替标准的历次版本发布情况为：EJ/T 570—1991，EJ/T 570—1999。

本标准2016年5月19日，经国家核安全局审查认可。

# 压水堆安全重要流体系统单一故障准则

## 1 范围

本标准规定了单一故障准则在压水堆安全重要流体系统中的应用规则。  
本标准适用于压水堆安全重要流体系统的设计及故障分析。

## 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，仅所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 20035 压水堆核电厂工况分类

## 3 术语和定义

下列术语和定义适用于本标准。

### 3.1

**安全重要流体系统** **fluid systems important to safety**

执行安全功能的流体系统，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工况的后果。

注：属于HAF 102中的安全系统范围。

### 3.2

**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事件。

### 3.3

**单一故障** **single failure**

导致某一部件不能执行其预定安全功能的一种故障，以及由此引起的各种继发故障。

### 3.4

**能动故障** **active failure**

依靠机械运动完成其预定功能的部件失效。

注1：例如，电动阀或止回阀不能动作到正确位置，或泵、风机或柴油发电机不能启动。

注2：应把由电动部件内自动启动系统或控制系统故障引起该部件误动作看作能动故障，防止这类误动作的方法是装有专门装置或操作限制装置（例如切断用于电动阀门的断路器）。误动作的例子是给电动阀误通电而将其打开或关闭。

### 3.5

**非能动故障** **passive failure**

一个部件不能保持其结构完整性或工艺流道被堵塞而不能完成其预期功能的故障。

注：例如，阀瓣从阀杆上脱落就会发生工艺流道堵塞。

### 3.6

**短期** **short term**

在始发事件之后较短（最多24小时）的运行时间，在这段时间内实行反应堆自动保护动作，证实系统的响应，鉴别事故的类型及规定出随后长期中应采取的步骤。

注：对于应急堆芯冷却系统和安全壳喷淋系统设计而言，应将这些系统切换到长期冷却模式之前均视为短期。对于具有再循环运行方式的应急堆芯冷却系统和安全壳喷淋系统，当应急堆芯冷却系统和安全壳喷淋系统转换到再循环运行方式时，即开始长期冷却。

### 3.7

#### 长期 long term

紧接着短期后的安全重要流体系统运行时间。在这段时间内需要系统继续发挥安全功能。

### 3.8

#### 操纵员差错 operator error

操纵员在试图执行安全相关操作时发生的误操作或漏操作。

## 4 单一故障准则及其应用规则

### 4.1 单一故障准则

单一故障准则是指某一安全重要流体系统应能在发生任何单一故障情况下执行其任务的准则（或要求）。

对某一假设始发事件，并同时存在下述情况时，安全重要流体系统应有能力完成全部要求的安全功能：

- a) 由单一故障引起的所有故障；
- b) 由假设始发事件引起的所有故障和误动作。

故障可能出现在要求安全重要流体系统动作的假设始发事件之前或假设始发事件期间的任何时间。

### 4.2 应用规则

4.2.1 按照 NB/T 20035 工况分类，应将反应堆设计成能承受 II 类、III 类、IV 类工况的始发事件并满足相应设计要求。

4.2.2 对于任何引起反应堆紧急停堆或汽轮机停机的 II 类工况始发事件，及任何导致 III 类或 IV 类工况的始发事件，假设除该始发事件之外有一个单一故障，应将反应堆设计成能在上述假定条件下执行下列安全功能：

- a) 快速停堆；
- b) 排出堆芯余热；
- c) 应急堆芯冷却；
- d) 安全壳隔离；
- e) 安全壳的排热；
- f) 安全壳的大气控制净化。

4.2.3 在事故的短期阶段，单一故障可只考虑能动故障。

4.2.4 在事故的长期阶段，需考虑的单故障可以是能动故障或非能动故障。

4.2.5 若某非能动故障为泄漏的情况，应在适当考虑运行工况和可能的故障或泄漏模式的同时，通过系统中现实的非能动故障机理的分析来规定发生非能动故障时的设计泄漏流量。

4.2.6 若为单一故障的探测、诊断和纠正提供了合适的时间和办法，则应允许操纵员为减轻单一故障后果而采取行动。

## 5 不考虑单一故障的情况

5.1 若能够证明某一具有能动功能的部件在发生可信工况下能执行正确的能动功能，则可不考虑该部件会发生能动故障（如按规范设计的安全阀和某些止回阀的开启）。若认为可免除单一故障分析，则应在单一故障分析里用文件资料来说明免除的根据和合理性。

非能动部件的设计、制造、在役检查和维修均达到很高的质量水平，并且保持不受到假设始发事件的影响，则在单一故障分析中可不假设它会发生故障。假定某一非能动部件不发生故障时，应从该部件所受的载荷、所处的环境以及始发事件发生后要求该部件执行其功能的全时程的角度来论证这种分析方法的合理性。

5.2 不必考虑安全壳边界和安全壳隔离系统发生非能动故障或超过安全分析中规定限值的泄漏。

5.3 若按照技术规格书要求，允许安全重要流体系统冗余设置的多个系列中的一个系列在短期维修期间暂时不可用，则在此期间不必假设在其他系列中有单一故障。

5.4 若某非能动故障引起的泄漏未超过 4.2.5 中的设计泄漏流量，且该故障不会导致反应堆丧失所需的安全功能，则单一故障分析中不必考虑这种有限的泄漏。

5.5 若假设始发事件是具有双重目的的安全重要流体系统（即该系统既是 I 类工况运行所需，又是反应堆停堆和减轻始发事件的后果所需）的两个或多个系列中的一个系列的故障，则在系统其余的一个系列或双重系列中不必假设单一故障。其条件是该系统按抗震 I 类要求进行设计，能从厂内和厂外获得电源，按安全分级相应的质量保证、试验、在役检查标准进行建造、运行和检查。在这种情况下，可按照技术规格书要求，反应堆继续运行。

5.6 始发事件是 I 类工况期间不要求运行的安全重要流体系统的两个或多个系列中的一个系列的故障，若此始发事件不要求自动保护动作去减轻其后果，则不必假设单一故障。在这种情况下，可按照技术规格书要求，反应堆继续运行。

5.7 若始发事件是在 I 类工况期间不要求运行的安全重要流体系统的两个或多个系列的一个系列中的假设故障，但此始发事件要求自动保护动作去减轻其后果，则应假设该系统的另一个系列中有单一故障。然而，若假定在该系统的另一个系列中有单一故障，则所有可利用的系统（包括非安全相关的系统和由操纵员来操纵的系统）皆可用来减轻上述始发事件叠加单一故障的后果。在判断这些系统的可用性时，若该始发事件直接导致反应堆紧急停堆或汽轮机停机，则应评价电源是否可继续使用。判断实现操纵员行动的可行性应根据是否有足够的显示、是否有足够的时间执行被建议动作和可利用设备的可达性来进行。

## 6 设计要求

6.1 安全重要流体系统应能够利用厂内应急电源或其他合适方式（如非能动）运行。

6.2 安全重要流体系统应能够利用在役检查和试验技术对现存的或可能的故障进行探测。

6.3 反应堆应设计为能使得安全重要流体系统的能动部件能通过定期试验来证明这些系统的可运行性。

6.4 对恢复期可能较长的事（如反应堆冷却剂丧失事故），应采取保证可以接近和修理事故后恢复期内可能损坏的设备。这些措施包括诸如冗余部件的适当屏蔽、清洗隔间的能力、排空和清洗隔间内需要接近的放射性管道的能力以及通向设备的安全通道。在制定这些措施时，需假定设计的源项。进行论证时，可假定厂外电源、非安全相关的设备和厂外设备可用。

6.5 对事故后安全壳放射性排放的设计应保守考虑在有效隔离之前由于假想的单一故障所排放的放射性物质的种类和排放量，并包括隔离后的排放。应根据泄漏的探测、定位和隔离措施保守地确定排放的持续时间。

## 7 分析要求

7.1 应对安全重要流体系统的设计进行单一故障分析以论证符合本标准的要求。

7.2 对每一个始发事件，单一故障分析的范围应包括要满足 4.2.2 相应要求的安全重要流体系统。

在这些安全重要流体系统中，除去所分析的单一故障或始发事件的后果引起的故障，不必再考虑其他故障。