# 中华人民共和国国家标准

GB/T 13626—2001

# 单一故障准则应用于核电厂安全系统

**Application of the single failure criterion to safety systems in nuclear power plant**

2001-10-24 发布　　2002-04-01 实施

中华人民共和国
国家质量监督检验检疫总局　发布

# 目　　次

# 前　言

1992 年等效采用美国 IEEE Std 379:1977《单一故障准则应用于核电厂　IE 级系统》制订了 GB/T 13626—1992《单一故障准则应用于核电厂安全级电气系统》,本标准等效采用 IEEE Std 379:1994,是对 GB/T 13626—1992 的修订。

本标准技术内容与 GB/T 13626—1992 相比较,作了如下修改:

1. 本标准名称改为《单一故障准则应用于核电厂安全系统》。

2. 在"1　范围"中增加了"本标准的应用必须与 GB 13284 的要求及其规定的单一故障准则一致"的内容。

3. 引用标准增加了 GB 13284—1998, GB/T 7163—1999

4. 在"3　定义"中对下列定义进行了修改:

a) "3.2　可探测故障"定义中增加了"注",解释了不可探测故障的含义;

b) "3.5　设计基准事件"定义中的"假想事件"改为"假设始发事件";

c) "3.8　安全系统辅助设施"改为"3.8　辅助支持设施";

d) "3.10　安全系统"定义中"注"的内容增加了"为完成安全功能的安全系统的电气部分属安全级(1E 级);

e) 取消了"保护功能"和"安全级"定义;

f) 增加了"3.11　执行设施"、"3.12　监测指令设施"、"3.13　安全组"和"3.18 共享系统"四条定义;

g) 修改了"3.15　保护动作"、"3.14　安全功能"。

5. 对"4　单一故障准则"内容增加了"单一故障可能出现时间的说明"。

6. 对"5.4　设计基准事件和单一故障"补充了"避免由设计基准事件引起的故障的措施"。

7. 对"5.5　共因故障"补充了防范共因故障的内容。

8. 增加了"5.6　共享系统",规定了单一故障准则应用于共享系统的要求。

9. 对有关独立性分析的 6.1.4 补充了"注",对 6.1.5 补充了故障例子。

10. 对"6.2.1　通道的相互联接"作了修改,将对仪表管路分析要求独立为"6.2.6 仪表管路"。

11. 对"6.3　其他考虑"作了修改。将原来的内容规定在"6.3.1 与安全系统耦合的其他系统"和"6.3.3　由单一故障引起系统驱动的可能性"内。增加了"6.3.2　概率评价特性"。

12. 根据 IEEE Std 379:1994"7. 文献目录",本标准增加了"附录 A(提示的附录)参考文献"。

此外,还作了格式与文字上的修改。

本标准从实施之日起,同时代替 GB/T 13626—1992。

本标准由中国核工业集团公司提出。

本标准由核工业标准化研究所归口。

本标准起草单位:核工业第二研究设计院。

本标准主要起草人:华爱媛,奚绍黄。

# IEEE 前言

（本前言不是 IEEE Std 379:1994《单一故障准则应用于核电站安全系统》的一部分。）

在许多文件（包括 IEEE 标准、美国核学会（ANS）标准以及联邦法规）中确定了核电站安全系统满足单一故障准则的要求。本标准的意图是：

——确切地符合 IEEE Std 603:1991《核电站安全系统准则》的要求。

——解释 IEEE Std 603:1991 陈述的单一故障准则；

——对应用 IEEE Std 603:1991 所述的单一故障准则提供指导。

单一故障准则适用于电气和机械系统的集合。但是，本标准制订的准则是用于电气系统的。在与机械系统不可避免的接口处（例如，仪表管线），与电气系统接口的机械部分要考虑为电气系统的一部分。应注意到“系统”是包括驱动系统、保护系统以及电源系统。

本修订版的目的是：

——明确在设计基准事件前或在设计基准事件期间出现了单一故障的安全系统必须有能力执行其安全功能；

——修订定义以与 IEEE Std 603:1991 一致；

——更新文本中引用的参考文献。

已由本标准明确的，但没有全部制订的几个方面如下：

——与其他导则和标准的关系：为了生产一个可接受的和可靠的系统，任一好的设计均应包括其他的导则和标准。单一故障准则与其他导则、标准、文件要求、可靠性和概率研究、试验以及运行等的关系不属本标准范围。

——共享系统：现版本标准说明了单一故障准则应用于共享系统的方式。其目的是既不赞同也不禁止使用共享系统，但要提出最低要求以保证将和不使用共享系统同样严格地分析部件故障对共享系统的影响。

——单一的操作员错误：应考虑操纵员的操作，但这超出了本标准的范围。

——共因故障：不属于单一故障分析的共因故障包括那些可能由外部环境影响、设计缺陷、制造错误、维修错误和操纵员错误引起的故障。共因故障关系到评价电厂安全。共因故障应该用可靠性和概率工具来说明，并应考虑丧失安全功能的后果。共因故障已由 IAEA 50-p-1（单一故障准则应用）说明。

本标准由工作组 SC 6.3 制订。

中华人民共和国国家标准

# 单一故障准则应用于核电厂安全系统

GB/T 13626 - 2001

**Application of the single failure criterion to safety systems in nuclear power plant**

代替 GB/T 13626 1992

## 1 范围

本标准规定了单一故障准则应用于核电厂安全系统的电源、仪表和控制部分的一般原则和要求。

本标准阐明单一故障准则，探讨各类故障，指导安全系统如何应用单一故障准则并提出了一个可接受的单一故障分析方法。

本标准不规定哪些系统服从单一故障准则。

本标准适用于核电厂安全系统。

本标准的应用必须与 GB 13284—1998 的要求及其规定的单一故障准则一致。

## 2 引用标准

下列标准所包含的条文，通过在本标准中引用而构成为本标准的条文。本标准出版时，所示版本均为有效。所有标准都会被修订，使用本标准的各方应探讨使用下列标准最新版本的可能性。

GB/T 7163—1999 核电厂安全系统的可靠性分析要求(eqv IEEE Std 577:1976)

GB/T 9225—1999 核电厂安全系统可靠性分析一般原则(eqv ANSI/IEEE Std 352:1987)

GB/T 12788—2000 核电厂安全级电力系统准则(eqv IEEE Std 308:1991)

GB 13284—1998 核电厂安全系统准则(eqv IEEE Std 603:1991)

GB/T 13286—2001 核电厂安全级电气设备和电路独立性准则(eqv IEEE Std 384:1992)

## 3 定义

本标准采用下列定义。

3.1 故障(失效) failure

某物项丧失规定的功能。

3.2 可探测故障 detectable failure

通过定期试验发现的故障或由报警、异常指示揭示的故障。在通道、序列或系统级探测到的部件故障是可探测故障。

注：可判明的但不可探测的故障是那些不能通过定期试验发现或不能由报警、异常指示揭示的，但由分析判明的故障。

3.3 定期试验 periodic test

按计划的时间间隔，为探测故障和证实可运行性所进行的试验。

3.4 共因故障 common cause failure

由一个公共原因引起的多重故障。

3.5 设计基准事件 design basis events

为确定构筑物、系统和部件可接受的性能要求，在设计中采用的假设始发事件。

中华人民共和国国家质量监督检验检疫总局 2001 - 10 - 24 批准　　2002 - 04 - 01 实施

3.6 驱动器 actuation device, actuator

直接控制执行装置原动力(电力、压缩空气、液体流等)的部件或一些部件的集合,例如电路断路器、继电器和先导阀等。

3.7 执行装置 actuated equipment

用来完成一个安全动作的原动机和被驱动设备的组合。

注:原动机的例子有汽轮机、电动机和电磁线圈。被驱动设备的例子有控制棒、泵和阀门。

3.8 辅助支持设施 auxiliary supporting features

为安全系统完成其安全功能提供诸如冷却、润滑和动力等服务的系统或设备。

3.9 安全执行系统 safety actuation system

安全系统的一部分,当受到保护系统信号触发时,为完成要求的某个安全动作所必需的设备集合。

3.10 安全系统 safety system

与安全有重要关系的系统,用于在任何工况下保证反应堆安全停堆、从堆芯排出热量和(或)限制预计运行事件和事故工况的后果。

注:安全系统包括保护系统、安全执行系统和辅助支持设施。为完成安全功能的安全系统的电气部分属安全级(1E级)。

3.11 执行设施 execute features

由电气设备和机械设备及其连接件组成。接到来自监测指令设施的信号后,执行与安全功能直接或间接有关的某一功能。执行设施的范围从监测指令设施的输出端开始直到并且包括执行装置与过程的耦合处。

3.12 监测指令设施 sense and command features

产生与安全功能直接或间接有关的信号的电气和机械设备及其连接件。其范围是从被测过程变量开始直到执行设施输入端为止。

3.13 安全组 safety group

能完成某一安全功能的一组最少量部件、组件和设备的组合。

3.14 安全功能 safety function

为了把核电厂参数保持在按设计基准事件确定的可接受的限值内所必需的一种过程或条件(例如应急负反应性引入、事故后热量排出、应急堆芯冷却、事故后放射性物质清除和安全壳隔离)。

注:完成某一安全功能是由反应堆停堆系统和辅助支持设施、或者是由专设安全设施和辅助支持设施、或者是由两者完成所有必需的保护动作来实现的。

3.15 保护动作 protection action

为完成某一安全功能在监测指令设施内产生一个信号或触发执行设施内设备的运行。

3.16 通道 channel

在核电厂工况需要时,为产生一个单一保护动作信号需要的元器件和组件的一种配置。一个通道在各单一保护动作信号汇合处就丧失其特征。

3.17 冗余设备或系统 redundant equipment or system

功能相同的两个或两个以上的设备或系统,其中任何一个都可以完成要求的功能,而与其他设备或系统是否处于正常状态无关。

注:可通过采用相同的设备,设备多样性或功能多样性来实现冗余。

3.18 共享系统 shared systems

在多机组电厂内,能为一个以上机组完成功能的构筑物、系统和部件。

共享包括下述含意:

a) 系统同时由两个机组共享;

b) 时间序列共享,或者说,按照事件序列在不同时间由两个机组共享;

c) 系统在某一给定时间仅由一个机组使用，但它可按指令从该机组断开并由另一机组使用。

3.19 系统逻辑 system logic

监测两个或两个以上通道的输出并按预定的组合规则(如三取二、四取二等)给出输出信号。

## 4 单一故障准则

对某一设计基准事件，并同时存在下述情况时，安全系统应有能力完成全部必需的安全功能：

a) 在安全系统内存在任何单一可探测故障，并同时存在所有可判别的但不可探测的故障；

b) 由上述单一故障引起的所有故障；

c) 引起要求安全功能的设计基准事件或由设计基准事件引起的所有故障和系统误动作。

单一故障可能出现在要求安全系统动作的设计基准事件之前或设计基准事件期间的任何时间。

## 5 要求

在单一故障准则应用于安全系统设计时，应考虑满足 5.1～5.6 的有关要求，其中有些条件是隐含的。

### 5.1 独立性和冗余性

独立性原则是有效应用单一故障准则的基础。安全系统的设计应使某一部件的单一故障不影响任一独立的与其冗余的部件或系统的正确运行。

### 5.2 不可探测的故障

单一故障准则应用隐含了故障的可探测性。可探测性是系统设计和规定试验的功能之一。不能由定期试验发现或不能由报警、异常指示揭示的故障是不可探测的故障。安全系统分析目的之一是判别不可探测故障。当判别了不可探测的故障，应采取下列措施：

a) 优先采取的措施是重新设计系统或重新制订试验方案以使故障成为可探测的；

b) 另一可采取的措施是假定已出现了所有已判定的不可探测故障，分析每个单一故障的影响。

### 5.3 级联故障

当有理由认为系统中的一些附加故障是由于任一来源的(机械的、电气的或环境的)单一故障引起时，则应把这些级联故障统一考虑为单一故障。

### 5.4 设计基准事件和单一故障

导致需要安全功能的设计基准事件可能引起系统部件、组件或通道故障。为了预防由设计基准事件引起的故障，设备的设计、质量鉴定和安装应避免这类预期故障。当分析表明设计基准事件将导致安全系统的部件、组件或通道故障时，则应把这些故障考虑为该设计基准事件的后果。对要满足单一故障准则的系统，应证明在存在这些由设计基准事件引起的故障、存在所有已判别的不可探测故障和任一别的单一故障时，系统能完成所要求的安全功能。

### 5.5 共因故障

当进行单一故障分析时，应把某些共因故障考虑为单一故障。这些故障可能存在于不同的部件，并有不同的故障模式。5.3 和 5.4 已分别讨论了来自级联故障和设计基准事件的故障。它们必须包括在单一故障分析中。

不属于单一故障分析范围的共因故障包括：可能来自外部环境影响、设计缺陷、制造错误、维修错误和运行错误的故障。

设计鉴定和质量保证程序是为了防范外部环境影响、设计缺陷和制造错误。人员培训、正确的控制室设计和运行、维护、监督规程是用来防范维修和运行人员错误的。

### 5.6 共享系统

应用于有共享系统的机组的单一故障准则如下：

a) 假设在共享系统或在与共享系统接口的辅助支持设施内存在一个单一故障，则所有机组的安全

系统都应有能力完成其所要求的安全功能。

b) 在每一机组未共享的系统内同时存在一个单一故障时，每一机组的安全系统都应有能力完成其所要求的功能。

设计应保证在一个机组内的单一故障不影响(不扩展到)另一机组，从而不妨碍共享系统完成其要求的安全功能。

在单一故障分析时，不必同时考虑 a)和 b)的故障，即对电厂进行单一故障分析，论证满足准则 a)，然后重复单一故障分析论证满足准则 b)。

## 6 单一故障的设计分析

应系统地对应用单一故障准则的安全系统的设计进行分析，以确定是否存在违反单一故障准则的情况。本章将对进行单一故障分析给予指导。本章所建议的方法是一种可接受的分析系统的方法，但不是唯一的方法。进行单一故障分析的其他步骤见 GB/T 9225—1999 第 5 章。

### 6.1 步骤

按下述步骤对每个设计基准事件进行系统的分析。

6.1.1 应确定要进行分析的安全功能(例如降功率、安全壳隔离、堆芯冷却等)。

6.1.2 应确定用以完成安全功能的安全动作(例如快速插入控制棒、关闭安全壳隔离阀、安全注入、堆芯喷淋等)。

6.1.3 应确定足以满足所要求安全功能的安全组。例如两个堆芯喷淋子系统或一个堆芯喷淋子系统和两个低压冷却剂注入子系统都足以冷却堆芯。

6.1.4 应验证在 6.1.3 所确定的安全组的设计独立性，即通过检查至少有两个安全组，这些安全组没有共享设备或易损点(例如其位置和配置低于可接受实体分隔要求的继电器、开关装置、母线、电源等)来验证独立性。一旦确立了独立性，就证明了存在完成安全功能的冗余能力，就不需要为满足单一故障准则去进一步考虑存在于冗余部分内的潜在故障。

注：在某些情况下不能很容易地确立独立性(如冗余通道或冗余序列汇集在一起的三取二结构的系统)，而在另一些情况下较容易地确立独立性(如冗余通道或冗余序列不汇集在一起的二取一结构的系统)，对此，进一步的指导见 6.2.1 和 6.2.2。

6.1.5 对独立性不易被证明的系统或系统的某些部分，应进行潜在故障的系统性研究以确保不违反单一故障准则。故障例子有短路、开路、接地、高阻抗短接到地、热短路、交流或直流电压以及那些由引入的可信最大交流或直流电势引起的或其后果的故障。

应同时考虑电气故障和机械故障。

一个部件可能有不同的故障模式，应对每一种模式进行单独的分析。

应分析安全设备的所在位置和配置以确定共因故障的影响。

### 6.2 系统某些特定部分的分析

当进行单一故障分析时，安全系统的某些部分可能要求一些特殊考虑。6.2.1～6.2.6 列出这些部分应用单一故障准则时可能关注的几个方面和要求。

#### 6.2.1 通道，相互联接

若通过数据记录仪、试验电路等装置使冗余通道间相互联接，其联接部分是可能丧失独立性的区域。应分析这些相互联接部分以保证单一故障不会导致丧失安全功能。对那些可能导致丧失安全功能的单一故障，应分析冗余部分的隔离措施。

#### 6.2.2 系统逻辑

在单一故障分析中，系统逻辑的分析特别重要，因为冗余通道和冗余的驱动电路在这里汇集。分析应证明在系统逻辑中的单一故障不会引起可能导致丧失安全功能的通道故障或驱动电路故障。

#### 6.2.3 驱动器

为了确保不存在可能引起丧失安全功能的单一故障，应分析按失电时以最可能的模式失效所设计的驱动器，例如应分析使驱动器端误保持电源的故障或引起妨碍移动到优先位置的机械粘结故障。

应分析那些在要求安全动作时接入动力源的驱动器，以确保单一的开路、短路或失去动力源不会导致丧失安全功能。

应从可能影响系统能力的故障出发，对整个驱动器系统（包括气动、机械、电气和液压部件在内）进行分析，以满足单一故障准则。应特别注意要保证驱动器机械部分的故障不引起冗余设备的电气故障，电气故障也不引起冗余设备的机械故障。

6.2.4 电源

电源有可能以几种方式引起丧失安全功能，例如电源故障引起的高压可能导致冗余通道的故障（如晶体管故障），低压可能导致丧失冗余通道，电源的频率和波形变化可能引起冗余通道整定值的漂移。单一故障分析应包括整个电源系统，包括可以甩去非主要负荷的装置。有关这方面的进一步指导见GB/T 12788。

6.2.5 辅助支持设施

任何为应用单一故障准则的安全系统的正常运行所需要的辅助支持设施，应作为它支持的系统的一部分被包括在单一故障分析中。例如当安全系统的一部分和保持受控环境相关时，除非能证明环境系统故障不会导致丧失所要求的安全功能，否则环境系统的故障就可能成为违反单一故障准则的潜在原因。

如果辅助支持设施的设计不满足单一故障准则，则不管是否丧失辅助支持设施，均应确保完成所要求安全功能的能力。

6.2.6 仪表管路

联接传感器和工艺系统的管路（例如，包括参考小室、平衡阀和隔离阀等）应包括在单一故障分析内。

6.3 其他考虑

6.3.1 与安全系统耦合的其他系统

应检查以某种方式与应用单一故障准则的安全系统耦合的所有其他系统（如非安全级的试验电路），以确定在这些系统内的任何故障是否能使安全系统劣化。如果它们能使安全系统的某部分失效，则应假定存在那些故障作为初始条件，进行安全系统的单一故障分析。有关这方面的进一步指导见GB/T 13286。

6.3.2 概率评价特性

不应该用概率评价取代单一故障分析。但是，安全系统的概率评价特性可用于论证某些假设故障不可信，从而不需要在单一故障分析里考虑。有关这方面的进一步指导见GB/T 7163和GB/T 9225。

6.3.3 由单一故障引起系统驱动的可能性

应检查由单一故障引起的系统驱动的可能性，以判定这样的驱动是否会构成一个具有不可接受的安全后果的事件。对任何被判定为不可接受的驱动，应满足单一故障准则，也就是，在系统中存在所有不可探测的故障外，还存在任一单个可探测故障时，不准引起安全系统驱动。

# 附 录 A
（提示的附录）
## 参 考 文 献

下列文件在应用本标准时可能提供有用的信息：

1) CFR Publication 10 CFR 50.49(Jan. 1994)

2) CFR Publication 10 CFR 100 (Jan. 1994)

3) IAEA Safety Series NO. 50-P-1(1990), Application of the single Failure Criterion