

ICS 27.120.20  
F 83



# 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 .....	I
IEEE 前言 .....	II
1 范围 .....	1
2 引用标准 .....	1
3 定义 .....	1
4 单一故障准则 .....	3
5 要求 .....	3
6 单一故障的设计分析 .....	4
附录 A(提示的附录) 参考文献 .....	6

## 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(IE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。