F 69

中华人民共和国国家标准

GB/T 4083—2005
代替 GB/T 4083—1983

核反应堆保护系统安全准则

General safety principles of nuclear reactor protection system

2005-08-16 发布　　2006-03-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准是对 GB/T 4083—1983《核反应堆保护系统安全准则》的修订，编写方法和格式符合 GB/T 1.1—2000的要求。

本标准与 GB/T 4083—1983 相比主要变化如下：

a) 增加了前言；

b) 原“1 名词术语”之前的文字说明，按新格式要求，经过修改和删节并调整至有关段落；

c) 增加了“1 范围”和“2 规范性引用文件”；

d) 原“1 名词术语”改为“3 术语和定义”，在内容上的主要修改有：

1) “安全停堆系统”改为“紧急停堆系统”，“专设安全系统”改为“专设安全设施驱动系统”，对定义的内容也进行了修改；

2) 修改“安全监测装置”、“保护动作整定值”的定义；

3) 删除原标准中“安全降功率系统”、“安全报警系统”、“冗余”和“符合”共 4 条术语定义；

4) 增加“系统安全生存周期”、“商品级物项”、“固件”、“验证”、“确认”、“软件工具”和“配置管理”共 7 条术语和定义。

e) “3 设计准则”改为“5 安全准则”；本准则作为完整的标准体系中的一个组成部分，在该章中指明了对第 2 章中规范性引用文件具体引用的内容；并对部分内容进行了修改：

1) 原“在役检验”改为“试验与校准能力”；

2) 原“设备质量”改为“设备质量和质量鉴定”；

3) 原“安全报警和信号显示”改为“安全报警和信息显示”；

4) 原“识别”改为“标识”；

5) 增加了“与其他系统的相互作用”、“接近控制”、“人因工程考虑”。

f) 增加了“6 基于计算机系统的补充要求”，该章是对基于计算机技术的反应堆保护系统的主要技术要求，其中也指明了对第 2 章中规范性引用文件的具体引用内容。

g) 增加了“参考文献”，列出资料性引用文件和在标准编制过程中参考过的文件。

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：中国核动力研究设计院。

本标准主要起草人：王远兵、周祖锰、李谢晋。

本标准所代替标准的历次版本发布情况为：GB/T 4083—1983。

核反应堆保护系统安全准则

1 范围

本标准规定了核反应堆保护系统应满足的基本安全要求。

本标准适用于各种类型的核反应堆保护系统。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 5204 核电厂安全系统定期试验与监测(GB/T 5204—1994，neq ANSI/IEEE 338:1987)

GB/T 5963 反应堆保护系统的隔离准则(GB/T 5963—1995，eqv IEC 60709:1981)

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

GB/T 8993 核仪器环境条件与试验方法

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

GB/T 11684 核仪器电磁环境条件与试验方法

GB/T 12505 计算机软件配置管理计划规范

GB/T 12727 核电厂安全系统电气设备质量鉴定

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

GB/T 13625 核电厂安全系统电气设备抗震鉴定(GB/T 13625—1992，eqv IEC 60980:1988)

GB/T 13629—1998 核电厂安全系统中数字计算机的适用准则(eqv IEEE Std 7-4.3.2:1993)

EJ/T 529—1990 用于核电厂安全重要系统数字计算机(eqv IEC 60987:1989)

EJ/T 797 人因工程原则在核电厂系统、设备和设施中的应用

EJ/T 1058—1998 核电厂安全系统计算机软件(eqv IEC 60880:1986)

HAD 102/10(1988) 核电厂保护系统及有关设施

3 术语和定义

下列术语和定义适用于本标准。

3.1

反应堆保护系统 reactor protection system

产生那些触发安全驱动器和安全系统支持(辅助)设施动作所必须的输出信号，防止反应堆状态超过规定的安全限值，或减轻超过安全限值后果的系统。它包括从敏感元件到安全驱动器输入端或到安全系统支持(辅助)设施输入端的所有设备(包括硬件及软件)。

注：反应堆保护系统包括紧急停堆系统和专设安全设施驱动系统。

3.2

紧急停堆系统 reactor trip system

反应堆保护系统的一部分。它触发安全驱动器动作，使反应堆快速停闭。

3.3

专设安全设施驱动系统 engineering safety feature actuation system

反应堆保护系统的一部分。它触发专设安全设施动作，以缓解事故后果，防止放射性物质外泄。

3.4

安全联锁 safety interlock

仅当规定条件存在时，它才允许进行某些影响反应堆安全的操作。

3.5

安全监测装置 safety monitoring assembly

用于反应堆安全的监测装置。一般它包括敏感元件、信号调理和(或)处理部件。

3.6

安全逻辑装置 safety logic assembly

它与安全监测装置相连，用来完成预定的逻辑功能，并将其输出信号送给一个或多个安全驱动器。

3.7

安全驱动器 safety actuator

根据一个或多个安全逻辑装置的指令，直接控制执行机构动作的装置。例如紧急停堆断路器、阀门和泵的控制器等。

3.8

安全故障 safe failure

保护系统内一种增加安全动作概率的故障。

3.9

非安全故障 unsafe failure

保护系统内一种减少安全动作概率的故障。

3.10

误停堆 spurious shutdown

反应堆正常运行时，由于保护系统中的一个或多个安全故障引起的自动停堆。

3.11

保护动作整定值 protective setpoint

根据安全分析预先确定的值，当被监测的变量达到此值时，保护系统触发安全驱动器动作。

3.12

运行旁通 operational by-pass

根据运行的需要，抑制保护系统中一部分特定功能的行为和措施。

3.13

维修旁通 maintenance by-pass

为了设备更换、检修、检验或校准，人为地取消保护系统中一个或多个设备功能的行为和措施。

3.14

系统安全生存周期 system safety life cycle

与保护系统实现有关的必要活动，它发生的时间段从系统需求详细定义的概念阶段开始，直到该系统不再可用时结束。

注：典型的系统安全生存周期包括系统需求说明、系统规格说明、系统详细设计和实施、系统集成、系统确认、系统安装和调试、系统运行和维护以及设计修改(如果有)等阶段。

3.15

商品级物项 commercial grade item

满足下列条件的物项：

a) 不是为核设施专门设计或不以核设施特有技术要求为条件；

b) 已用于非核设施；

c) 按制造厂说明(例如样本)中规定的技术条件从制造厂或供货商处采购。

例如商品级计算机。

3.16

固件 firmware

具有软件功能的硬件，如驻留在只读存储器中的软件和数据的组合。

3.17

验证 verification

在系统研制过程中，为确定其每个阶段的产品是否满足由前一阶段为其规定的所有要求的一个过程。

3.18

确认 validation

对系统进行的测试与评价，以保证系统满足功能、性能和接口等方面的要求。

3.19

软件工具 software tools

用来开发、测试、分析或维护其他程序或其文件的计算机程序。

3.20

配置管理 configuration management(control)

鉴别和确定系统中的配置项、管理整个系统安全生存周期中这些配置项的释放和变更、记录和报告配置项的状态和变更请求的过程。

4 设计基准

对于每个反应堆保护系统，应当给出设计基准，用以进行保护系统的设计并判断其功能是否满足要求。

设计基准至少应给出以下资料：

a) 需要保护的反应堆状态及保护动作；

b) 为了产生保护动作而要求的监测变量(如：中子注量率、冷却剂流量、压力、温度等)，监测变量所需敏感元件的最少数目及其布置；

c) 监测变量的运行限值和保护动作整定值；

d) 在正常工况、异常工况和事故工况下，动力源特性与环境条件(如：电压、频率、湿度、温度、压力、振动、辐射场等)的稳态及动态变化范围；

e) 引起保护系统中元件损坏或引起保护系统性能下降的误动作、事故或其他随机事件(如：火灾、爆炸、飞射物、雷击、洪水、地震、台风及生物危害等)；

f) 保护系统最低性能要求：

1) 系统准确度；

2) 系统响应时间；

3) 系统可靠性；

4) 在正常工况、异常工况和事故工况下，系统应适应被测变量的变化范围和变化率范围。

5 安全准则

5.1 单一故障准则

保护系统内单一故障或单次事件及其继发故障不应有损于系统的保护功能。

5.2 冗余

为了使保护系统满足单一故障准则，提高反应堆的安全性，设计中应使用冗余技术 一般包括安全监测装置的冗余，安全逻辑装置的冗余和(或)整个系统的冗余。

5.3 独立性

为满足单一故障准则、实现在役检验和维修，保护系统应保持独立性，包括：

a) 结构上的独立性，要求假设始发事件不影响保护功能；

b) 在保护系统内部，要求各冗余装置之间在电气上和实体上相互独立；

c) 在保护系统与控制系统和其他系统之间，要求在电气上和实体上相互独立。

电气上的独立性至少要求隔离设备输出端的任何可能故障(开路、短路、接地、出现最大可能的电压等)都不影响隔离设备输入端及其所连设备的正常工作。隔离设备应作为保护系统的一部分。

有关系统的隔离应符合 GB/T 5963 的规定。有关系统的独立性还宜符合 GB/T 13629—1998 中 5.6 的规定。

5.4 多样性

包括功能的多样性及设备的多样性。对每个规定的反应堆假设始发事件尽量用不同的物理效应或不同的变量来监测，在某些条件下可用不同类型的设备来测量同一物理变量，以便克服共因故障。

5.5 电缆隔离与屏蔽

为了减轻火灾、飞射物或其他原因引起的机械损伤和随机故障所造成的后果，保护系统与其他系统的电缆和电线之间，保护系统内部各冗余部分的电缆和电线之间，都应进行实体隔离。为了减少噪声和干扰，保护系统的电缆和电线还应根据需要采取屏蔽等措施加以保护。

5.6 变量的直接连续测量

用于反应堆保护的变量应连续测量，尽量从直接测量中获得，并且尽可能单独使用，如与其他系统共用，应采取隔离措施。

5.7 故障安全准则

保护系统的设计应当尽量保证当部件故障或失去动力源时都使系统趋于保护动作。为避免误动作造成系统可用性降低，安全故障率要限制在最低水平。

5.8 符合

为了减少保护动作误动概率，设计时应尽量采用符合技术。根据实际情况可选用整体符合或局部符合。

5.9 试验与校准

保护系统应具有可定期试验的能力。如设备要求的试验时间间隔短于反应堆正常运行间隔，则此设备应能在功率运行期间进行在役试验。试验应尽量包括从敏感元件到安全驱动器输入端(可扩展到输出端)的所有部分。试验的时间要尽量短。进行在役试验时，不应引起误动作。如需将被试验部分旁通，则剩余部分应尽可能满足单一故障准则。

有关系统定期试验的要求宜符合 GB/T 5204 的规定。

保护系统还应具有可校准的能力，有关要求宜符合 GB 13284—1998 中 5.7 的规定。

5.10 设备质量和质量鉴定

保护系统的元件、部件(包括软件单元)应当是合格的和高质量的，应在规定的条件下进行检验。在正常工况、异常工况和事故工况下，保护系统的设备都能满足系统性能的设计要求。仪表要稳定，使其在例行校验的间隔期间不用调整。设备要既可靠又简单，并按相应的质量鉴定等级进行必要的鉴定。

有关质量鉴定的要求宜符合 HAD 102/10(1988)的 7.9 的规定。有关环境条件和电磁干扰特性的要求应符合 GB/T 8993 和 GB/T 11684 的规定。有关电气设备质量鉴定宜符合 GB/T 12727 的规定。有关抗震鉴定的要求宜符合 GB/T 13625 的规定。

5.11 系统可靠性

保护系统的安全故障率和非安全故障率是度量系统可靠性的重要指标。设计系统时对可靠性应进行定性分析和相应的定量计算。动力堆紧急停堆系统可参考下述指标：

a) 每个变量的系统安全故障率(误停堆率)不大于每年一次；

b) 每个变量在要求保护动作时，系统因随机故障而不动作的概率不大于 10^{-5}。

其他反应堆亦可根据实际情况参考上述指标。有关可靠性的要求宜符合 GB/T 13629—1998 中 5.15的规定。可靠性分析要求和一般原则宜符合 GB/T 7163、GB/T 9225 的规定。

5.12 保护动作信号

每个变量只要达到保护动作整定值，安全监测装置就应给出一个保护动作信号。该信号可以被延迟，但不能被抑制。变量的保护动作信号来源要尽量与设备故障的保护动作信号来源相区别。

5.13 保护动作的完成

保护动作一旦被触发就应完成到底，仅当保护变量恢复到允许的整定值范围内时，系统才能手动复原。

5.14 整定值调整

应简化整定步骤，尽量减少调整整定值的设备数量和调整次数，但要保证准确度。整定值调整不应引起误动作。

为适应运行状态的变化，出于安全的考虑，可设置过余量保护或整定值的自动调整。

5.15 运行旁通

在一定条件下才能使用运行旁通。条件不满足时，保护系统应具有以下功能：

a) 防止运行旁通的启动；

b) 若运行旁通原已启动，则应撤销相应的现行运行旁通，使核电厂恢复原来的工况，以便再次出现允许运行旁通的条件，或触发适宜的安全功能。

实现上述功能的设备应作为保护系统的一部分。

5.16 手动触发

保护系统除自动触发外还应设置手动触发。自动触发电路中的故障不应阻碍手动触发。手动触发应操作简单，采用设备数量最少。手动触发与自动触发的共用设备也应尽可能少。操作部件应置于醒目且可靠的位置。

5.17 辅助(应急)控制点

除主控室外，应在适当的地方设置辅助(应急)控制点，以便在主控制室不可用时，手动停堆或启动相应的设备使反应堆保持在停堆状态。

5.18 安全报警和信息显示

当反应堆状态参数值超过安全报警整定值或保护系统装置发生故障时，保护系统要触发准确的视听报警信号，并用不同的颜色和声调与其他报警信号相区别。事故原因、动作状态、旁通状态以及安全联锁状态等都应有信息显示。重要安全参数显示应置于操纵员便于观察的位置。其他要求宜符合 GB 13284—1998中 5.8 的规定。

5.19 系统维修

保护系统的设计应使设备故障易于识别、定位，设备应易于更换、修理和调整。维修周期应与系统可靠性要求相适应。

5.20 维修旁通

正确使用维修旁通时，反应堆应受到充分保护；不正确使用维修旁通时，应导致自动保护动作。

5.21 标识

保护系统的部件、设备及连接电缆等应设置清晰和永久的标识，宜符合 GB 13284—1998 中 5.11 的规定。

5.22 电源监督

保护系统应接不间断电源，并应监督其正常供电条件。供电不正常时应发出报警。

5.23 与其他系统的相互作用

应尽量避免保护系统与其他安全级别较低的系统的连接，当存在相互连接的情况时，应采用隔离措施。

5.24 接近控制

应能对接近保护系统设备实施行政控制，此类控制应得到保护系统内部措施设计、核设施总体设计或两者的支持。

5.25 人因工程考虑

在设计全过程中，尤其是在设计开始阶段，宜按 EJ/T 797 的规定考虑人因工程，以保证分配给操纵员和维修人员的整体功能和各部分功能都能成功地完成，以实现保护系统的设计目标。

6 基于计算机系统的补充要求

6.1 系统安全生存周期活动

为保证所有反应堆安全要求的获取、执行和维持，与保护系统研制、实现和运行有关的所有活动均应置于系统安全生存周期的框架中来完成。安全生存周期中一个阶段可再划分成若干个基本任务，每个任务均规定有明确的活动，一个阶段可在前一阶段活动完成之前开始，但该阶段只有在前面的各阶段已经完成并且它的输出与这些阶段活动所提供的输入相一致时才能结束。

6.2 系统确定性特征

基于计算机的系统设计应保证系统内部具有与执行功能要求相一致的预先确定性行为特征，具有承受某些不能预料运行情况的能力。如保证激励和响应之间的时间延迟存在最大和最小值；满足所有预期电厂瞬态数据负荷下的性能要求；软件的确定性宜采用 EJ/T 1058—1998 附录 B 推荐的方法等。

6.3 系统完整性

基于计算机的保护系统应设计成在所有可能造成保护功能失效的内外部条件下完成其保护功能，试验和校准功能不得对计算机完成其保护功能的能力产生不利影响。系统完整性宜符合 GB/T 13629—1998的 5.5 的规定。

6.4 验证和确认

应编制保护系统的验证和确认计划，以确认设计的正确性和完整性。软件研制和修改过程中执行验证和确认宜符合 EJ/T 1058—1998 第 7、10 章以及 GB/T 13629—1998 附录 I 中 I3 的规定，硬件验证要求宜符合 EJ/T 529—1990 第 7 章的规定，系统的综合验证和确认宜符合 EJ/T 1058—1998 中 8.5 和第 9 章的规定。

6.5 数据通讯

保护系统通讯结构应提供冗余的通讯连接并保证本系统与其他系统以及冗余子系统之间的独立性，安全级别较低的系统数据通讯不能危及本系统的通讯和运行。应对通讯设备运行和所传输的数据进行正确性检查。应选择适当的通讯技术和通讯容量以满足在所有预期瞬态数据负荷下的执行能力要求。

6.6 商品级计算机质量鉴定

在将商品级计算机应用于保护系统时，应进行质量鉴定。对支持完成保护功能所需的计算机硬件、软件和固件进行质量鉴定的要求宜符合 GB/T 13629—1998 中 5.3.2 和附录 D 的规定，应有充分证据确认包括上述部件和接口在内的现有商品级计算机能够完成其预期的保护功能。

6.7 软件共因故障的防御

软件缺陷会造成系统出现共因故障，应在整个研制过程和评估中采用适当的对策防御由软件引起的共因故障的可能结果。

6.8 **软件工具**

应选择用于保护系统软件研制的适当的软件工具，以降低在软件研制过程中引入缺陷的风险，增强该过程的正确性和软件产品的可靠性。软件工具应经过认可、进行标识并置于配置管理之下。

6.9 **安全性**

只有经批准的人和系统才能访问保护系统计算机。但对信息和数据未经许可的访问、修改、泄露以及恶意破坏，要求有安全性措施保护。

6.10 **硬接线手动后备**

应提供少量必要的硬接线手动操作功能，作为基于计算机系统的功能后备。

6.11 **软件配置管理**

应编制软件配置管理计划(计划指导符合 GB/T 12505)，软件配置管理宜符合 GB/T 13629—1998 附录 I 中 I 4 的要求。

6.12 **文档**

在系统安全生存周期每个阶段应生成适当的文档并构成相互一致的文件体系，以确保对整个生存周期过程的可追溯性。文档应完整，包含各阶段文档所要求的充分的信息，同时应尽可能做到清晰、准确以使其能被各种相关技术人员和评审人员所理解。有关文档宜符合 EJ/T 529—1990 的 5.4、第 14 章和 EJ/T 1058—1998 附录 F 的具体要求，并宜符合 HAD 102/10(1988)第 11 章的规定。

参 考 文 献

[1] IEC 61513:2001, Nuclear power plants—Instrumentation and control for systems important to safety—General requirements for systems

[2] IEC 60880-2:2000, Software for computers important to safety for nuclear power plants-Part 2: software aspects of defence against common cause failures, use of software tools of pre-developed software