ICS 27.120.20
F 83

# 中华人民共和国国家标准

GB/T 13284.1—2008
代替 GB 13284—1998

# 核电厂安全系统 第1部分：设计准则

The safety systems for nuclear power plants—Part 1: Design criteria

2008-03-24 发布　　2008-11-01 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

GB/T 13284《核电厂安全系统》的预计结构由七部分组成：

——第 1 部分：设计准则；

——第 2 部分：数字计算机的适用准则；

——第 3 部分：整定值；

——第 4 部分：定期试验与监测；

——第 5 部分：仪表通道响应时间试验；

——第 6 部分：仪表通道性能验证方法；

——第 7 部分：逻辑装置的特性和检验方法。

本部分为 GB/T 13284 的第 1 部分，对应于 IEEE Std 603:1998《核电厂安全系统准则》(英文版)。本部分与 IEEE Std 603:1998 的一致性程度为非等效，其主要差异如下：

——将 IEEE Std 603:1998 的图 2、图 3 和图 4 合并为图 2；

——将 IEEE Std 603:1998 中引用的美国标准改为我国相应的标准；

——增加了 4.4.2、4.4.3、4.4.4。

本部分代替 GB 13284—1998《核电厂安全系统准则》。

本部分与 GB 13284—1998 相比主要有以下变化：

——第 5 章中增加了“共因故障准则”；

——增加了附录 B(资料性附录)“电磁兼容性”。

本部分的附录 A、附录 B 和附录 C 都是资料性附录。

本部分由国防科学技术工业委员会提出。

本部分由核工业标准化研究所归口。

本部分起草单位：核工业标准化研究所。

本部分主要起草人：高丽艳、牛祝年、肖晨。

本部分于 1991 年 11 月首次发布，1998 年 11 月第一次修订。

# 核电厂安全系统
# 第1部分：设计准则

## 1 范围

GB/T 13284的本部分规定了核电厂安全系统动力源、仪表和控制部分最低限度的功能和设计要求。为了符合本部分的规定，也对安全系统其他部分(见图1)提出了接口要求。

本部分适用于为防止或减轻设计基准事件后果、保护公众健康和安全所需要的那些系统。对于保护整个核电厂安全所需的所有与安全有关的系统、构筑物和设备，亦可参照使用。

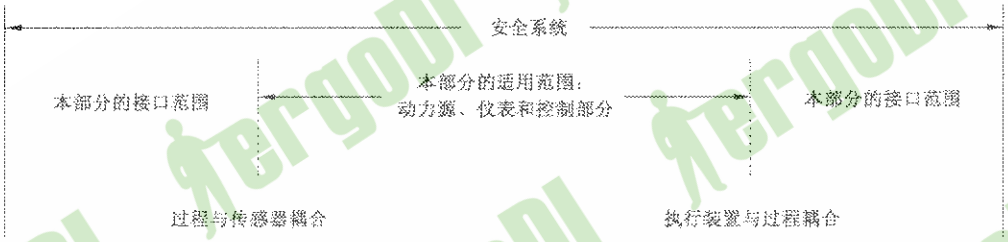



图1 本部分的适用范围和接口

图2用3×3矩阵的形式说明本部分的范围，矩阵顶部一行的名称说明安全系统可以分为监测指令设备、执行装置和动力源三个通用单元，它们代表一组设备为很多独立的安全功能提供类似的功能特性。矩阵左边一列的名称说明安全系统可分为反应堆停堆系统和专设安全设施、辅助支持设施及其他辅助设施三个工作单元。

| 安全系统工作单元 | 安全系统通用单元：监测指令设备 | 执行装置 | 动力源 |
|---|---|---|---|
| 反应堆停堆系统和专设安全设施 | • 过程传感器<br>• 过程控制器<br>• 信号处理<br>• 操纵员操作显示器<br>• 判断逻辑<br>• 行程开关<br>• 手动开关<br>• 控制电路 | • 反应堆停堆系统停堆断路器<br>• 专设安全设施电动机、启动器<br>• 专设安全设施断路器<br>• 专设安全设施电动阀门、电磁阀<br>• 专设安全设施泵 | (动力源属于辅助支持设施或其他辅助设施) |
| 辅助支持设施 | • 室温传感器<br>• 柴油机启动逻辑<br>• 设备温度传感器<br>• 柴油机加载程序<br>• 行程开关<br>• 压力开关和调节器<br>• 控制电路<br>• 电压互感器<br>• 欠电压继电器 | • 采暖、通风和空调风机、过滤器<br>• 润滑油泵<br>• 设备冷却泵<br>• 断路器、启动器、电动机<br>• 柴油机启动线圈 | • 空气压缩机和储气罐<br>• 蓄电池<br>• 柴油发电机组<br>• 逆变器<br>• 变压器<br>• 工作母线<br>• 配电盘 |
| 其他辅助设施 | • 自动检验设备和电路<br>• 行程开关<br>• 旁通和复位电路<br>• 柴油机过热和润滑缺油显示器<br>• 手动开关<br>• 电气保护继电器 | • 安全系统隔离装置<br>• 非重要负载断路器 | • 蓄电池充电器<br>• 变压器<br>• 工作母线<br>• 配电盘 |

图2 表示安全系统的3×3矩阵

图 2 同时给出了矩阵每一部分典型设备的例子，可以看出某些部件根据其用途可能分属于几个部分。

注 1：根据定义，动力源属于辅助支持设施或其他辅助设施，因此，在图 2 中没有作为反应堆停堆系统及专设安全设施的一部分。

注 2：从图 2 矩阵的一行可以看到，一个工作单元可组成一个系统，如厂用水系统；从一列可以看到，该列通用单元表示一组设备，为完成很多独立安全功能提供类似的功能特性（如传感器）。

注 3：每一个工作单元包括一个或几个通用单元，但不一定包括所有通用单元。

注 4：属于某一通用单元的设备不限于在一个工作单元中使用。

## 2 规范性引用文件

下列文件中的条款通过 GB/T 13284 的本部分的引用而成为本部分的条款。凡是注日期的引用文件，其随后所有的修改单（不包含勘误的内容）或修订版均不适用于本部分，然而，鼓励根据本部分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部分。

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 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 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 12727 核电厂 安全系统电气设备 质量鉴定（GB/T 12727—2002，IEC 60780：1998，MOD）

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

GB/T 12790 核电厂安全级电气设备和系统文件标识方法（GB/T 12790—1991，IEEE 494：1975，NEQ）

GB/T 13286 核电厂安全级电气设备和电路独立性准则

GB/T 13626 单一故障准则应用于核电厂安全系统

GB/T 13627.2 核电厂事故监测仪表准则 仪表准则

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

EJ/T 562 核安全有关的操纵员动作时间响应设计准则

EJ/T 574 核电厂安全级控制仪表盘（屏）和机架的设计与鉴定

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 799 核电厂安全系统仪表触发整定值的确定和保持

HAF 102 核动力厂设计安全规定

HAD003/01 核电厂质量保证大纲的制定

## 3 术语和定义

下列术语和定义适用于 GB/T 13284 的本部分。

3.1

**可接受的 acceptable**

通过核电厂安全分析证明是满足要求的。

3.2

**行政管理 administrative controls**

法律、法令、指示、程序、政策、习惯作法授予的权利与职责。

3.3

**分析限值 analytical limit**

根据安全分析确定的被测量或计算量的限值，以保证其不超过安全限值。

3.4

**相关电路 associated circuits**

非安全级(非1E级)电路，但是和安全级电路没有通过可接受的分隔距离、安全级构筑物、屏障或隔离器件进行实体分隔或电气隔离。

3.5

**辅助支持设施 auxiliary supporting features**

为安全系统完成其安全功能提供服务(如冷却、润滑和动力)的系统或设备。

3.6

**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所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的汇合处终止。

3.7

**安全级 class 1E**

核电厂电气设备和系统的一个安全级别。它们是完成反应堆紧急停堆、安全壳隔离、堆芯冷却以及从安全壳和反应堆排出热量所必需的，或者是防止放射性物质向环境大量排放所必需的。

注："安全级"(1E级)是功能性的术语。设备和系统只有完成本部分列举的功能才能划归安全级；不应根据其他功能将系统或设备定为安全级。

3.8

**共因故障 common-cause failure**

归因于一个共同原因的多个故障。

3.9

**部件 components**

组成一个系统的各个独立物项。例如：导线、晶体管、开关、电动机、继电器、电磁线圈、管路、配件、泵、罐、阀门等。

3.10

**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。

3.11

**可探测故障 detectable failures**

可以通过定期试验鉴别的故障，或通过报警或异常显示发现的故障。在通道级、序列级或系统级测出的部件故障都是可探测故障。

注：可判别但不可探测的故障是通过分析来判断的故障，这类故障不能通过定期试验发现，也不能通过报警或异常显示发现。

3.12

**序列 division**

某一给定系统或设备组的名称，它们能与其他冗余设备组在实体、电气和功能上保持独立。

3.13

**执行装置 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备的信号后，执行与安全功能直接或间接有关的某一功能。执行装置的范围是从监测指令设备的输出端开始，直到并且包括执行装置与过

程的耦合处。

注 1：在某些情况下，保护动作可由直接对过程工况进行响应的执行装置（例如止回阀、自力式卸压阀）完成。

注 2：执行装置通常包括驱动设备、原动机及被驱动设备。

3.14

**组件 module**

构成一个单独的装置、仪表或设备的互相连接的部件组合，一个组件能作为一个单元断开、拆卸和使用备件更换，它有固定的功能特性，可作为一个单元被试验。只要符合此定义，一个组件可以是一台大型装置的一块印制板、一个可抽出的断路器或其他子组件。

3.15

**动力源 power sources**

为产生或转换动力所必需的电气设备、机械设备及其连接件。

3.16

**保护动作 protective action**

为完成某一安全功能，在监测指令设备内产生一个信号，或是执行装置内设备的运行。

3.17

**冗余设备或系统 redundant equipment or system**

重复另一设备或系统必要功能达到如下程度的设备或系统，不管哪一个处于工作或故障状态，另一个均能完成要求的功能。实现冗余可采用相同设备、设备的多样性或功能的多样性。

3.18

**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状态（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反应堆停堆系统和辅助支持设施完成所有必需的保护动作，或者是专设安全设施和辅助支持设施完成所有必需的保护动作，或者由两者共同实现（参见附录 A）。

3.19

**安全组 safety group**

某一假设始发事件发生时，能完成其要求的安全功能的一组最少量的部件、组件和设备组合。一个安全组包括一个或多个序列（参见附录 A）。

3.20

**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、从堆芯排出热量或限制预计运行事件和事故工况的后果。安全系统执行安全功能，其电气部分属于安全级（1E 级）。

3.21

**监测指令设备 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，直到执行装置输入端为止。

## 4 安全系统的设计基准

对核电厂每个安全系统的设计都应规定具体的基准，根据需要，设计基准还可用于确定安全系统及其设计变更的正确性。设计基准应符合 HAF102 的规定，至少应按下列内容形成文件。

4.1 适用于核电厂每种运行方式的设计基准事件，以及对应每一事件的核电厂工况的初始条件和允许限值。

4.2 对应每个设计基准事件的安全功能和执行装置的相应保护动作。

4.3 对所提供的每种运行旁通能力的允许条件。

4.4 对 4.2 规定的每个保护动作应给出如下数据：

4.4.1 为确保保护动作的正确完成，需要监测的变量、变量组或两者之和（监测的目的是为了手动、自动或以两种方式控制每一保护动作）、与每个变量有关的分析限值和范围（包括正常、异常和事故工况）以及这些受控变量的变化率。

4.4.2 适用于每一被测变量或变量组的安全限值（见图 3 中曲线 *A*）。

4.4.3 对 4.7 和 4.8 所述情况适当组合时的最低性能要求：

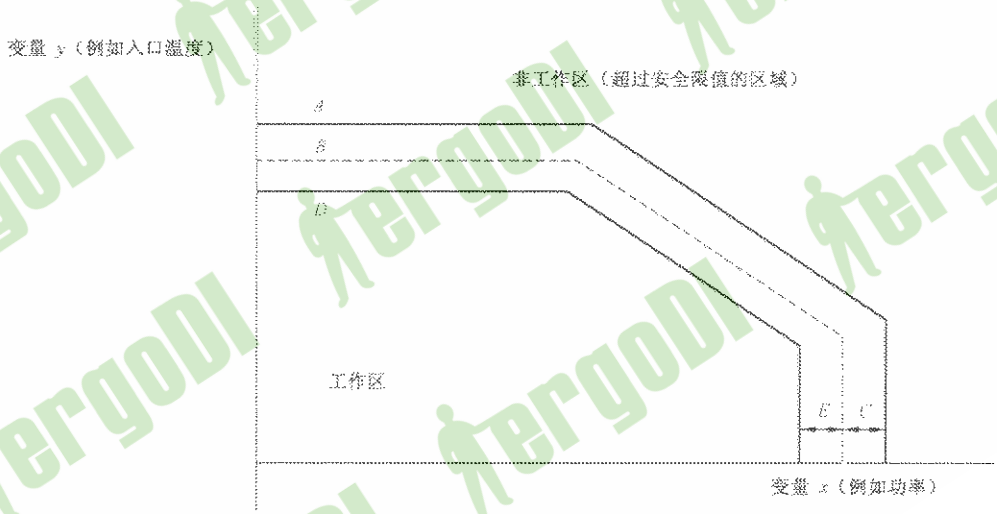
a) 每种变量或变量组的分析限值（见图 3 中曲线 *B*）；

b) 由于仪表的不准确度、校准的不确定度和误差而需给出的增量（见图 3 中增量 *C*）；

c) 在核电厂安全分析中确定分析限值所用的安全系统总响应时间。

应提供证据以证明由于仪表的不准确度、校准的不确定度、误差和时间响应所用的假定值是可以接受的和合理的。

4.4.4 为了考虑各次校准和验证试验的时间间隔之内的漂移，给出分析限值和保护动作整定值（见图 3 中曲线 *D*）之间的增量（见图 3 中增量 *E*）。应提供证据证明对仪表漂移所用的假定值是可以接受的和合理的。




*A*——安全限值，表示安全状态的限值；

*B*——分析限值，表示任何时候都可能存在的限制性最少的整定值；

*C*——考虑校准误差、仪表准确度和瞬态超调量的容差（它可能是变量 $x$ 或变量 $y$ 或两者的函数）；

*D*——保护动作整定值，设置在此值时可确保漂移不会使整定值超过整定点的允许值 *B*。

*E*——考虑仪器和整定值漂移的容差（它可能是变量 $x$ 或变量 $y$ 或两者的函数）。

图 3 安全系统整定值与安全状态限值的关系

4.5 对可以手动触发或触发后可以手动控制的 4.2 规定的保护动作应符合以下要求（详见 EJ/T 562）：

a) 允许手动控制的时刻与核电厂工况；

b) 允许只用手动触发或触发后只用手动控制的理由；

c) 操纵员应在正常、异常和事故工况期间进行手动操作时的环境条件范围；

d) 为了便于手动操作，应向操纵员显示的变量（见 4.4.1）。

4.6 对于 4.4.1 所述变量中的空间相关变量（即在某特定区域内变量是位置的函数），为保护目的所需要的传感器的最小数量和位置。

4.7 在安全系统应工作的正常、异常和事故工况期间，动力源、控制电源和环境条件（如电压、频率、辐射、温度、湿度、压力、振动和电磁干扰）的稳态及瞬态变化范围。对电磁干扰的有关信息参见附录 B。

4.8 可能引起安全系统功能劣化的情况(如飞射物、管道破裂、火灾、失去通风、消防系统误动作、操纵员差错、非安全有关系统中的故障),以及针对这些情况为保持安全系统完成安全功能的能力而应采取的预防措施。

4.9 为确定安全系统设计的可靠性适合于每个安全系统设计以及适合于对系统设计提出的任何定性或定量可靠性目标所采用的方法。

4.10 某一设计基准事件发生后的关键时刻或核电厂工况,包括:

a) 应触发安全系统保护动作的时刻或核电厂工况;

b) 确定安全功能正确完成的时刻或核电厂工况;

c) 需要自动控制保护动作的时刻或核电厂工况;

d) 允许安全系统恢复正常的时刻或核电厂工况。

4.11 阻止安全系统执行其安全功能的设备保护装置。

4.12 可能对安全系统设计提出的其他特殊的设计基准(例如多样性、联锁、管理规定)。

## 5 安全系统准则

安全系统应准确、可靠地把核电厂参数保持在可接受的限值之内,这些限值是按相应的设计基准事件规定的。每个安全系统的动力源、仪表和控制部分都应由一个以上的安全组组成,其中任何一个安全组都能完成该系统的安全功能(参见附录A)。

### 5.1 单一故障准则

安全系统在下列情况下应完成某一设计基准事件需要的全部安全功能:

a) 安全系统内存在单一可探测故障,同时存在可判别但不可探测的故障;

b) 由上述单一故障引起的所有故障;

c) 导致需要执行安全功能的设计基准事件或由这种事件引起的所有故障和系统误动作。

在要求安全系统执行安全功能的设计基准事件之前或期间的任何时间都可能发生单一故障。不管安全系统的控制是手动的还是自动的,单一故障准则都适用于安全系统,详见GB/T 13626。对于数字计算机的共因故障要求见GB/T 13629。

本部分并不要求在一个安全组内使用符合逻辑(或多通道),但根据其他标准要求,或者为使核电厂的可用性或可靠性达到最高也可以采用符合逻辑。在其他标准中已进行过评价并形成文件,证明某些流体系统中的故障可不遵守单一故障准则(参见附录C的C.3)。可以对安全系统进行概率评价,证明使用单一故障准则时不必考虑某些假想故障。概率评价的目的在于排除对不可信的事件和故障的考虑,但不能代替单一故障准则。可靠性分析的指导见GB/T 7163和GB/T 9225。

如果有合理的证据,表明一个安全系统的设计符合单一故障准则,但可能不满足4.9规定的所有可靠性要求时,就应对该系统进行概率评价,评价应不限于只考虑单一故障。如果评价表明不满足设计基准的要求,则应采取设计措施改进设计或校正修改,以保证该系统满足规定的可靠性要求。

### 5.2 保护动作的完成

安全系统应设计成一旦被自动或手动触发,执行装置就能按预定程序完成全部安全动作;只有操纵员有意识地操作才能使安全系统恢复到正常状态。这一要求不应妨碍使用设计基准4.11规定的设备保护措施或操纵员有意识的干预措施。对各个通道不要求自保持。

### 5.3 质量

部件和组件的质量应符合维修最少和故障率低的要求,优先选用可预计故障模式(拒动或误动)的设备。安全系统设备应按规定的质量保证大纲进行设计、制造、检查、安装、试验、运行和维修(见HAD003/01)。对于采用数字计算机和程序或固件的安全系统,应用这些准则的指导详见GB/T 13629。

5.4 设备质量鉴定

对安全系统设备应采用型式试验、以往的运行经验、分析或这三种方法的任意组合进行质量鉴定，证实它能满足设计基准规定的性能要求。安全级(1E 级)电气设备的质量鉴定应满足 GB/T 12727 的要求。对于采用数字计算机和程序或固件的安全系统，应用这些准则的指导详见 GB/T 13629。

5.5 系统的完整性

设计的安全系统应在设计基准中列举的所有适用工况下都能完成其安全功能。对于采用数字计算机和程序或固件的安全系统，应用这些准则的指导详见 GB/T 13629。

5.6 独立性

5.6.1 安全系统内部各冗余部分之间

对于提供某一安全功能的安全系统，其内部各冗余部分彼此之间应独立且实体分隔到必要程度，以便在需要这一安全功能的设计基准事件期间和事件后，能保持完成该安全功能的能力。

5.6.2 安全系统与设计基准事件影响之间

为缓解某一特定设计基准事件后果所需的安全系统设备，应与该设计基准事件的影响独立且实体分隔到必要程度，以保持满足本部分要求的能力。按 5.4 规定进行设备质量鉴定是满足这一要求的一种可用方法。

5.6.3 安全系统与其他系统之间

安全系统应设计成其他系统存在的可信故障或其他系统动作引起的可信故障(例如设计基准 4.8 所列的可信故障)不应妨碍安全系统满足本部分的要求。

5.6.3.1 接口设备

接口设备应：

a) 分级：用于安全和非安全两种功能的设备应属于安全系统，用于安全系统边界的隔离装置也应属于该安全系统；

b) 隔离：一个隔离装置非安全侧的任何可信故障，不得妨碍安全系统任何部分在需要执行安全功能的设计基准事件期间或事件后满足其最低性能要求。隔离装置的故障应与安全系统其他设备的故障一样进行评价。

5.6.3.2 邻近的设备

邻近的设备应：

a) 分隔：其他系统在实体上靠近安全系统设备，但不是相关电路也不是另一安全级电路的设备，应与安全系统的设备实体分隔到必要程度，以便在非安全级设备故障时安全系统仍能保持完成其安全功能的能力。实现实体分隔可以采用实体屏障或可以接受的分隔距离，或两者组合。安全级电气设备的分隔应符合 GB/T 13286 的规定；

b) 屏障：对某一安全系统起边界作用的实体屏障，应在设计基准 4.7 和 4.8 规定的使用条件下满足 5.3～5.5 的要求。

5.6.3.3 单一随机故障的影响

在非安全系统中的单一随机故障可能引起某一设计基准事件，同时又妨碍安全系统对该事件进行保护的那部分正确动作时，该安全系统的其余部分即使由于另外独立的单一故障引起性能劣化，也应具有完成这个安全功能的能力。对这一要求的应用指导详见 GB/T 13626。

5.6.4 详细准则

安全级(1E 级)电气设备和电路独立性准则详见 GB/T 13286。对于这些准则应用于互连计算机数据处理功能的分隔和隔离的指导详见 GB/T 13629。

5.7 试验和校准能力

在保持安全系统执行其安全功能能力的同时，应在功率运行期间提供对其设备进行试验和校准的能力，并且应尽可能接近实际地再现安全功能的特性。安全系统的试验应符合 GB/T 5204 的规定。在

不提供试验和校准能力对核电厂的安全或可用性也没有不利影响的情况下，允许在功率运行期间不进行试验和校准，在这种情况下：

a) 应提出合适的理由(例如证明不存在切实可行的设计方案)；

b) 应证明设备运行具有可接受的可靠性；

c) 应在核电厂停运期间提供试验和校准的能力。

5.8 信息显示

5.8.1 用于手动控制操作的显示

对于没有自动控制又是安全系统完成其安全功能所必需的手动控制操作，为其提供信息的显示仪表应是安全系统的一部分，并且应满足对核电厂事故监测仪表的要求，见 GB/T 13627.2。显示仪表的设计应使可能引起操纵员混淆的不明确显示减到最少。

5.8.2 系统状态显示

显示仪表应提供有关安全系统状态的准确、完整和及时的信息。这些信息应包括监测指令设备和执行装置保护动作的显示和识别。显示的设计应将不明确显示的可能性减到最少，以免操纵员混淆。为安全系统状态显示提供的仪表不必是安全系统的一部分。

5.8.3 旁通的显示

如果安全系统某个部分的保护动作因为运行旁通以外的目的而被旁通或处于不工作状态，就应在控制室连续显示每一个受影响的安全组的情况。

5.8.3.1 这种显示仪表不必是安全系统的一部分。

5.8.3.2 如果上述旁通和不工作状态预期每年出现一次以上，并且预期在要求受影响的系统工作时出现，那末这种显示应自动产生。

5.8.3.3 在控制室内应具备手动触发这种显示的能力。

5.8.4 位置

信息显示装置应位于操纵员能接近的地方。为手动控制保护动作提供的信息显示，应在进行相应操作的控制设备处能看得见。

5.9 接近控制

安全系统的设计应对接近安全系统设备能实施行政管理，行政控制应得到安全系统内部措施、核电厂设计措施或两者的支持。

5.10 维护

设计安全系统应易于对故障设备及时识别、定位、更换、修理和调整。

5.11 标识

为了保证本部分规定的要求能在核电厂的设计、建造、维修和运行期间应用，应满足下列要求：

a) 对安全系统的设备，应清楚地标识各个冗余部分，标识应符合 GB/T 13286 和 EJ/T 574 的规定；

b) 在已清楚标识的安全系统某一冗余部分安装的设备或组件，其内部的部件或组件本身不再要求标识；

c) 安全系统设备的标识应与设备上用于其他目的而设置的标志(如消防设备标志、动力电缆的相位标志)分辨开；

d) 安全系统设备及其序列划分的标识不得要求频繁引用参考资料；

e) 有关文件应按 GB/T 12790 的规定清晰标识；

f) 计算机程序和软件的版本应按 GB/T 13629 的规定清晰标识。

5.12 辅助设施

5.12.1 辅助支持设施应满足本部分的所有要求。

5.12.2 其他辅助设施执行的功能不是安全系统完成其安全功能所必需的，由于相关(即与安全系统没

有隔离)而成为安全系统的一部分,其设计应满足一些必要的准则,以保证这些系统的部件、设备和系统本身不会使安全系统的性能劣化到可接受的水平以下。其他辅助设施的例子见图 2。附录 A 给出应用本部分的一些说明。

5.13 多机组核电厂

在多机组核电厂中,只要在所有机组中同时执行所需安全功能的能力不受损害,则允许机组之间共用构筑物、系统和设备。机组间共用电力系统的要求见 GB/T 12788,单一故障准则用于共用系统的指导见 GB/T 13626。

5.14 人因工程考虑

在设计的开始阶段和设计全过程中,应按 EJ/T 797 的规定考虑人因工程,以保证分配给操纵员和维护人员的整体功能和每部分功能都能成功地完成,实现安全系统的设计目标。

5.15 可靠性

对于已经定量或定性地规定了可靠性目标的安全系统,应进行适当的设计分析,以便证实已经实现了可靠性目标。对可靠性分析的指导见 GB/T 7163 和 GB/T 9225。采用数字计算机和程序或固件的安全系统设备,本部分的应用指导详见 GB/T 13629。

5.16 共因故障准则

对存在单一共因故障的每一个设计基准事件,电厂参数应维持在规定的可接受限值内(见 GB/T 13626)。应对软件,包括采用手动操作和非安全相关系统和(或)部件的共因故障进行工程评价,以便提供实现功能的手段,否则该功能将因共因故障而失效,对此 GB/T 13629 给出了指导。

## 6 监测指令设备的功能和设计要求

除了第 5 章规定的功能和设计要求以外,监测指令设备还应满足以下(6.1~6.8)要求。

6.1 自动控制

除了 4.5 判定的情况以外,对所有保护动作都应提供自动触发和控制的手段,安全系统的设计应在每一设计基准事件发生之后,在 4.5 规定的时刻与规定的核电厂工况出现之前,不需要操纵员采取任何操作。在选择安全系统设计方案时,对 4.5 所述保护动作也可以提供自动触发和控制的手段。

6.2 手动控制

6.2.1 应在控制室中对自动触发的序列级保护动作提供手动触发的方法,手动方法应使操纵员的随机操作次数减到最少,并且在符合 5.6.1 规定的前提下使用的设备最少。

6.2.2 应在控制室对 4.5 鉴别的并且没有按 6.1 选为自动控制的保护动作提供手动触发和控制的方法。为这些动作提供的显示应符合 5.8.1 的规定。

6.2.3 按 4.10 的规定完成保护动作以后,应提供保持安全状态所必需的手动操作方法。给操纵员提供的信息、要求操纵员采取的动作以及有关的显示与控制设备的数量和位置,应与要求完成这些动作的时间和能参与操作的合格操纵员的数目相适应。上述的显示和控制设备应安装在操纵员可以接近的地方和适于操纵员工作的环境中,其布置应适合操纵员的监视和操作。

6.3 监测指令设备与其他系统之间的相互作用

6.3.1 要求

单一可信事件及其直接后果和继发后果可能引起一个非安全系统动作,该动作又可能导致需要保护动作的某种工况,与此同时又可能妨碍对这种工况提供主要保护的那些监测指令设备通道中的保护动作,此时应满足下述任一要求。

6.3.1.1 应提供不会由该单一事件引起故障的备用通道,以便探测该事件并将其后果限制在设计基准规定的限值之内。备用通道应从下列通道中选择:

a) 监测的变量组与主通道不同的通道;

b) 监测同样变量但所用设备与主通道不同的通道;

c) 监测的变量组与主通道不同，所用设备与主通道也不同的通道；

d) 主通道和备用通道都应是监测指令设备的一部分。

6.3.1.2 应提供不会由该单一可信事件引起故障的设备，以便探测该事件并将其后果限制在设计基准规定的限值之内。应认为这样的设备是安全系统的一部分。6.3.1 的解释见图 4。


图 4 本部分 6.3.1 的图解

6.3.2 措施

如果某一通道处于维修旁通状态，则应采取措施以便能同时满足 6.3.1 和 6.2 的要求。采取的措施包括降低符合度的要求，使来自冗余通道的非安全系统信号无效，或者由被旁通的通道触发一个保护动作。

6.4 系统输入

只要实际可行，监测指令设备的输入应是变量的直接测量信号，这些变量是在设计基准中规定的。

6.5 试验和校准能力

6.5.1 检查运行的可用性

在反应堆运行期间应提供具有高置信度的方法，用于检查安全功能所需的监测指令设备的每个传感器的可用性。有多种方法可以实现这一要求，例如：

a) 扰动被测变量；

b) 在 6.6 限定的范围内，适用时向传感器引入一个与被测变量性质相同的替代信号并使其变化；

c) 通道间的交叉检查，但这些通道的相互关系要已经知道并且有合适的读出设备。

6.5.2 保证运行的可用性

对于事故后一段时间内需要工作的每个监测指令设备，都应提供下述方法之一来保证其运行可用性：

a) 采用 6.5.1 所述方法检查传感器的运行可用性；

b) 确定设备在事故后一段时间内是稳定的，并且确定保持其校准能力的时间段。

6.6 运行旁通

无论何时，只要不满足允许的应用条件，安全系统就应自动防止运行旁通，或触发适宜的安全功能。如果核电厂工况的变化使得已经实施的运行旁通不再是允许的，安全系统就应自动完成下述动作中的一个：

a) 撤销相应的现行运行旁通；

b) 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；

c) 触发适宜的安全功能。

6.7 维修旁通

在监测指令设备处于维修旁通状态时，安全系统应保持完成其安全功能的能力。在维修旁通期间，监测指令设备应继续满足 5.1 和 6.3 的要求。

注：在维修旁通期间，对于不能满足 5.1 和 6.3 要求的部分监测指令设备，应证明设备运行具有可接受的可靠性（例如，为了维修旁通而允许退出运行的时间足够短，或者采取附加措施，或者两者均备，从而对整个监测指令设备的可用性没有明显的有害影响）。

6.8 整定值

6.8.1 应采用形成文件的方法确定 4.4 中规定的过程分析限值和设备整定值之间不确定度的容差，见 EJ/T 799。

6.8.2 在需要对特定的一种运行方式或一组运行条件的充分保护提供多重整定值时，设计中应提供有效的方法，保证仅需要时采用限制性更多的整定值。防止误用限制性较少的整定值的装置，应是监测指令设备的一部分。

7 执行装置的功能和设计要求

除了第 5 章提出的功能和设计要求以外，执行装置还应满足 7.1～7.5 的要求。

7.1 自动控制

执行装置应能接受监测指令设备的自动控制信号，并且按信号完成符合设计基准 4.4 规定的动作。

7.2 手动控制

如果对执行装置中任一执行部件提供手动控制，那么为完成这种手动控制在执行装置中增加的设计措施不应违反 5.1 和 6.3 的要求。执行装置应能接受监测指令设备的手动控制信号，并且按信号完成符合设计基准规定的动作。

7.3 保护动作的完成

执行装置的设计应是一经触发，就应完成其保护动作。这一要求不应排除使用设计基准 4.11 规定的设备保护装置，也不应排除操纵员有意识干预的措施。当监测指令设备恢复正常时，执行装置不应自动恢复正常，需要操纵员有意识的独立操作才能恢复正常。在最初的保护动作完成以后，执行装置可以要求手动或自动（即周期性的）控制特定的设备，以继续完成安全功能。

7.4 运行旁通

无论何时，只要不满足允许的应用条件，安全系统就应自动防止运行旁通，或触发适宜的安全功能。如果核电厂工况的变化使得已经实施的运行旁通不再是允许的，安全系统就应自动完成下述动作之一：

a) 撤销相应的现行运行旁通；

b) 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；

c) 触发适宜的安全功能。

7.5 维修旁通

当执行装置的设备处于维修旁通状态时，安全系统应保持完成其安全功能的能力。执行装置中冗余度为一（即二取一、三取二或四取三等）的那部分应设计成，其中一部分处于维修旁通时（即将其冗余

度暂时降为零，使其成为一取一、二取二或三取三等），其余部分应能提供可接受的可靠性。

## 8 对动力源的要求

### 8.1 电源

为安全系统供电的那部分电源（属于安全级）应符合本部分的规定，并且是安全系统的一部分。其具体要求见 GB/T 12788。

### 8.2 非电气动力源

为安全系统提供动力的非电气动力源，例如控制用空气系统、瓶装压缩气系统和液压系统，是安全系统的一部分，应按本部分的规定提供动力，但是其设计准则不属于本部分的范围。

### 8.3 维修旁通

当动力源处于维修旁通状态时，安全系统应保持完成其安全功能的能力。动力源中冗余度为一的那部分应设计成，其中一部分处于维修旁通时（即暂时将其冗余度降为零），其余部分应能提供可接受的可靠性。

# 附 录 A
（资料性附录）
安全系统范围演变过程的一些基本概念的图解

## A.1 目的

本附录的目的是利用安全系统范围演变过程中的一些基本概念，更好地理解和应用本部分。

## A.2 安全功能

安全系统范围演变过程的最基本和最明显的起点就是鉴别一项安全功能的范围。

从任一典型事故分析中都可看到，为了缓解某些设计基准事件的后果，可能需要一个以上的安全功能。图 A.1 以非常简单的形式解释了失水事故(LOCA)这一特定设计基准事件所需的安全功能，这些安全功能包括(但不限于)：

a) 应急负反应性引入；
b) 应急堆芯冷却；
c) 事故后放射性清除；
d) 安全壳隔离；
e) 事故后热量排出。

## A.3 典型安全系统范围的阐述

根据定义，一个安全系统应包括实现某个安全功能所需的全部设备。

用应急堆芯冷却功能来图解一个典型的安全系统。图 A.2 是一个典型的安全系统方框图，图 A.3 是这个方框图转变成提供应急堆芯冷却所需具体设备的图。

图 A.4 至图 A.8 是对安全系统的一个序列，用流程图和单线格式，以逐个增加设备的方式组成应急堆芯冷却系统。从图 A.4 的裸堆开始，图 A.5 加上了应急堆芯冷却系统(ECCS)的监测指令设备；图 A.6 加上了应急堆芯冷却系统的执行装置，即应急堆芯冷却系统的泵、热交换器、贮水箱、阀门、管线、仪表和控制器，从而构成这个安全系统的专设安全设施部分；图 A.7 增加了一部分辅助支持设施，具体是厂用水、设备冷却水(CLCW)和采暖通风及空调系统；图 A.8 增加了其余的辅助支持设施，即安全级(1E 级)电源而构成了该安全系统的一个完整序列。

## A.4 安全组

安全组是能够完成某一安全功能的一组数量最少的互相连接的部件、组件和设备。在每个序列都能完成安全功能的设计中，一个序列就是一个安全组，如图 A.9 所示。但是在一个安全系统的设计有 3 个能力为 50%的序列时，就有三个安全组，为了完成某一安全功能，每个安全组要求三个序列中有任两个序列(三取二)工作，这时安全组按图 A.10 中的逻辑来分开。根据 5.8 的要求，为了识别安全组的状态，显示系统中应包括这种逻辑的显示。

## A.5 其他辅助设施

绝大多数安全系统的设计都包括一些部件、设备和系统，它们的主要作用不是直接执行安全功能而是增加安全系统的可用性或可靠性。这些部件、设备和系统包括(但不限于)设备保护装置、内装式检验设备、隔离装置等，如图 A.2 所示。正如 5.12 所述，安全系统中的这些部分只需满足本部分的部分要求，即保证它们不会使安全系统的性能降低到可接受的水平以下，它们可不必满足的安全系统准则的例

子如运行旁通、维修旁通和旁通显示。

为了解释这些准则的应用，以安全级(1E 级)电力系统继电保护为例。继电保护的一个功能是增加安全级电力系统的可用性和可靠性，但是从安全系统的观点出发，关键的功能是在需要安全系统工作时不引起误脱扣，所以实现这个关键功能就是本部分规定的准则。增加安全级电力系统可靠性和可用性的功能要求见 GB/T 12788。

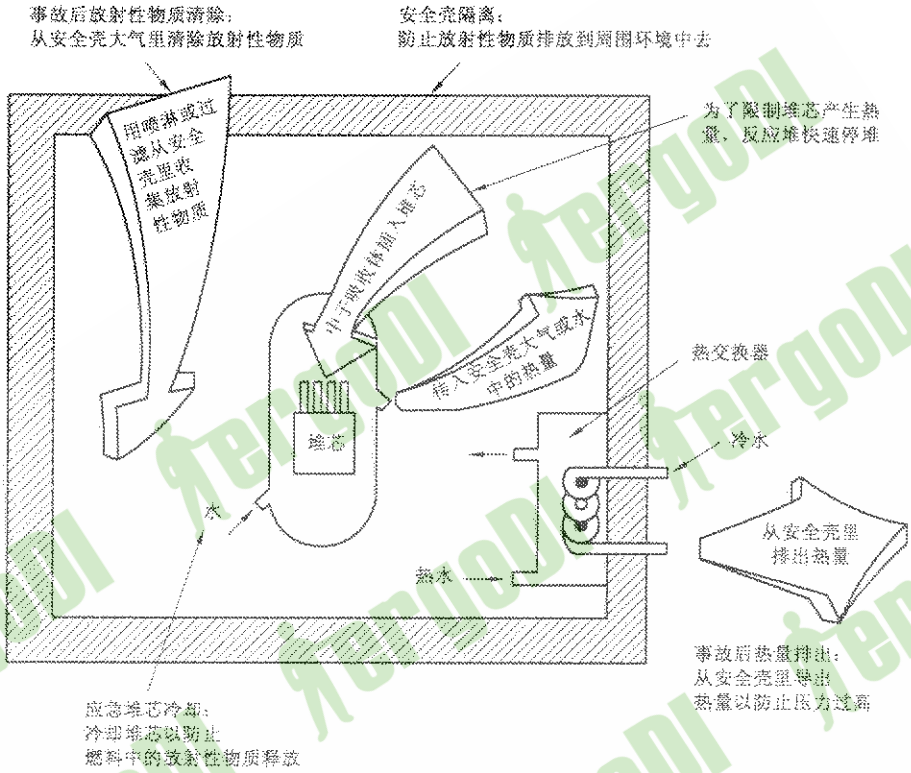



图 A.1 压水堆失水事故(LOCA)安全功能

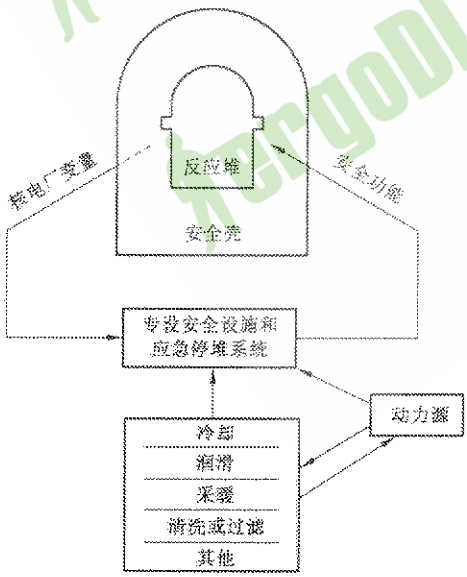



图 A.2 典型的安全系统方框图

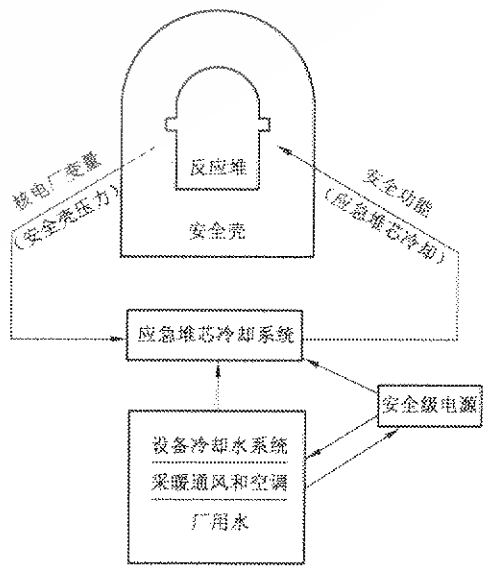



图 A.3 应急堆芯冷却设备

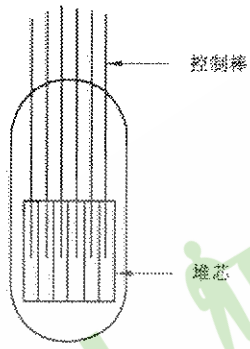



图 A.4 应急堆芯冷却部件:反应堆

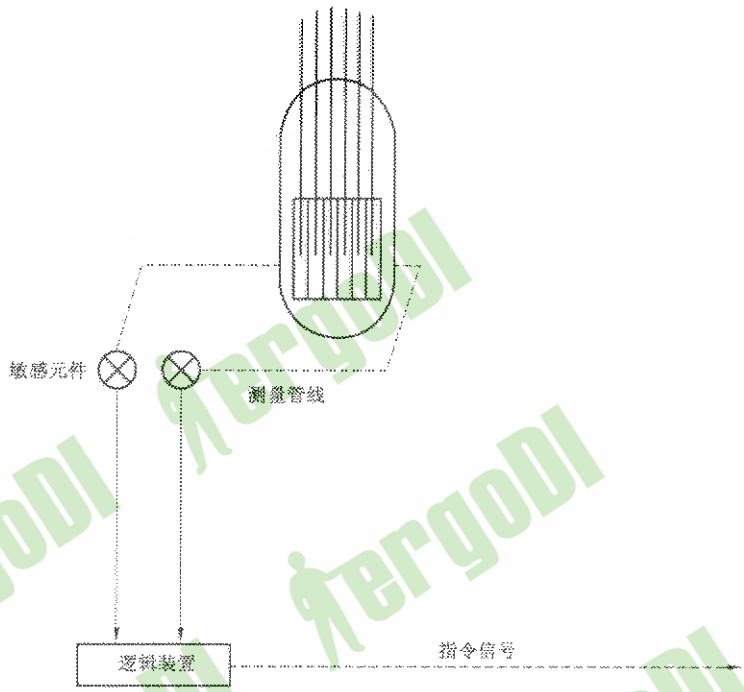



图 A.5 应急堆芯冷却部件:增加了监测指令设备

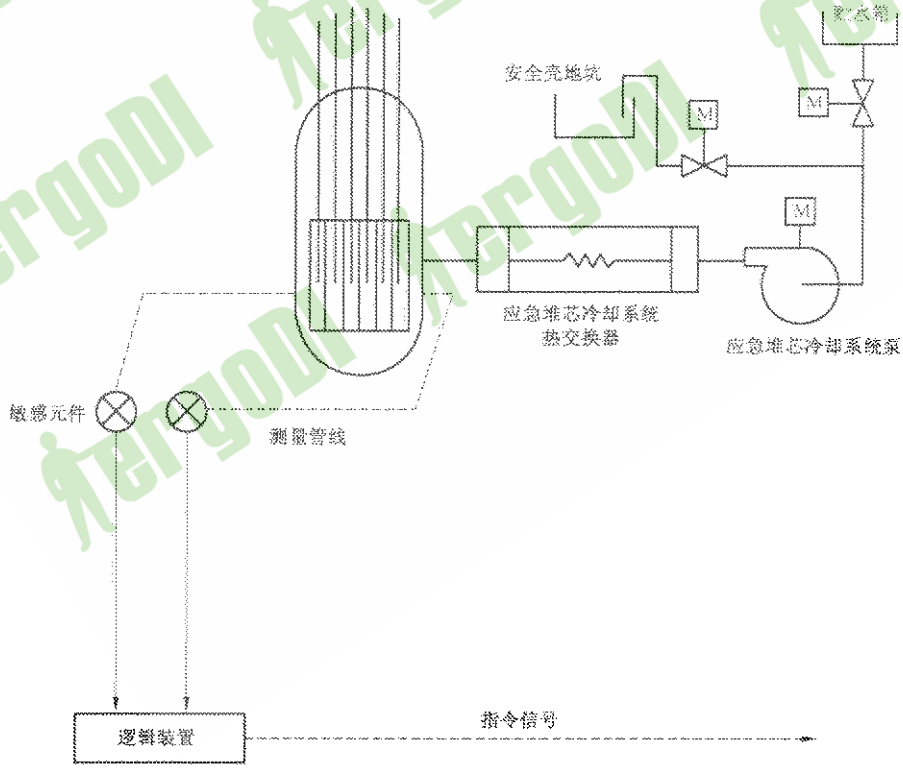



图 A.6 应急堆芯冷却部件:增加了执行装置

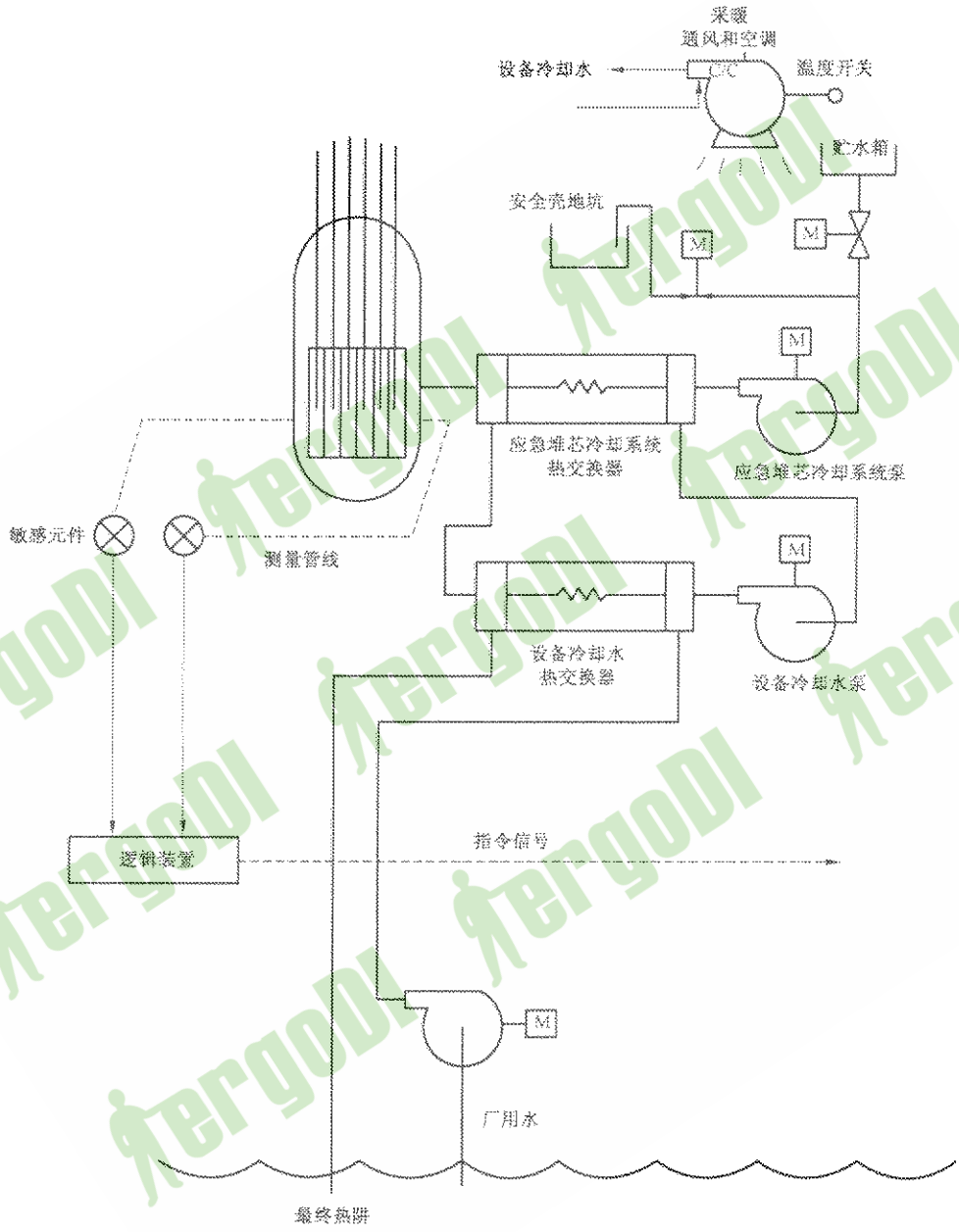



图 A.7 应急堆芯冷却部件:增加了一些辅助支持设施

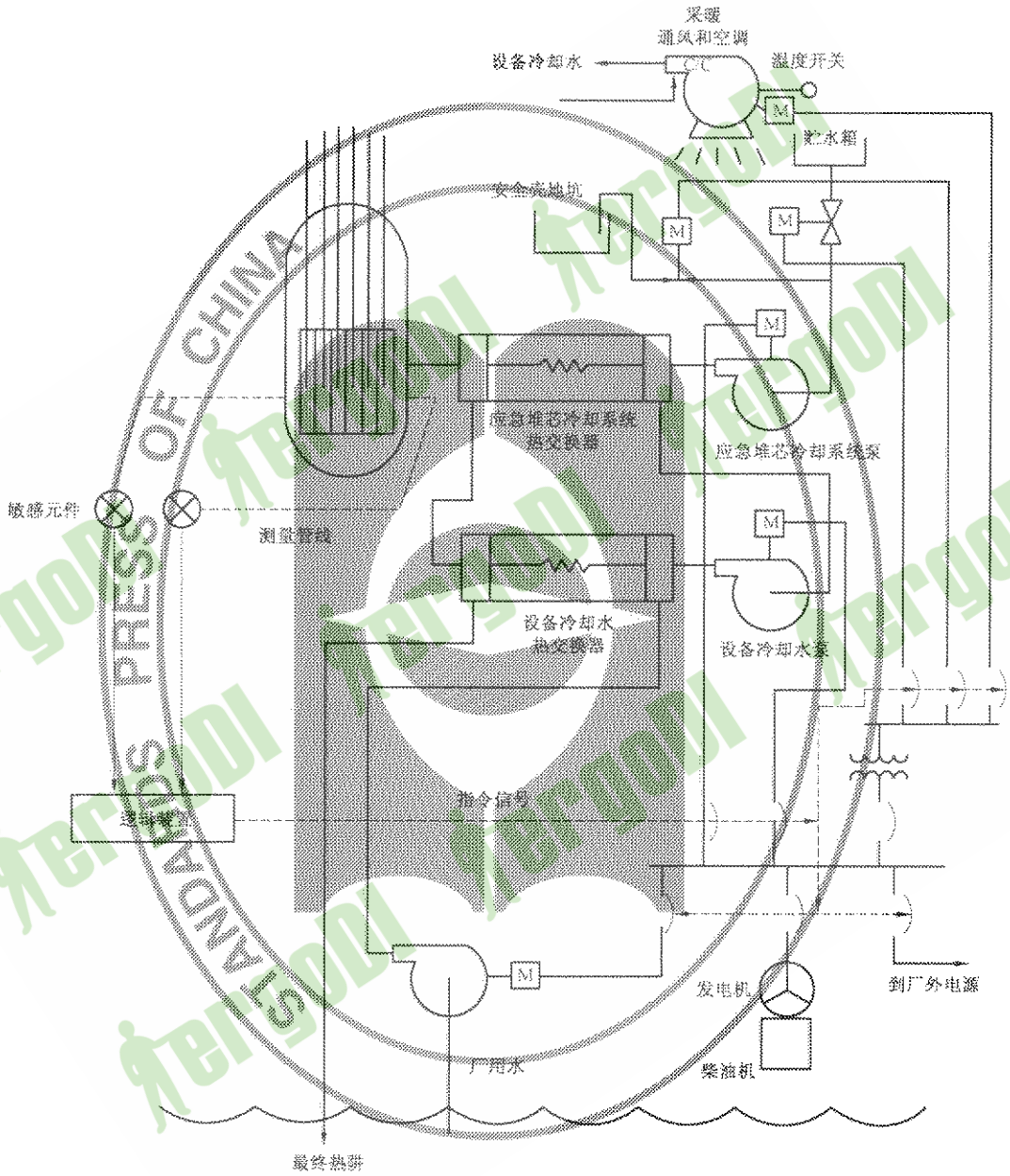
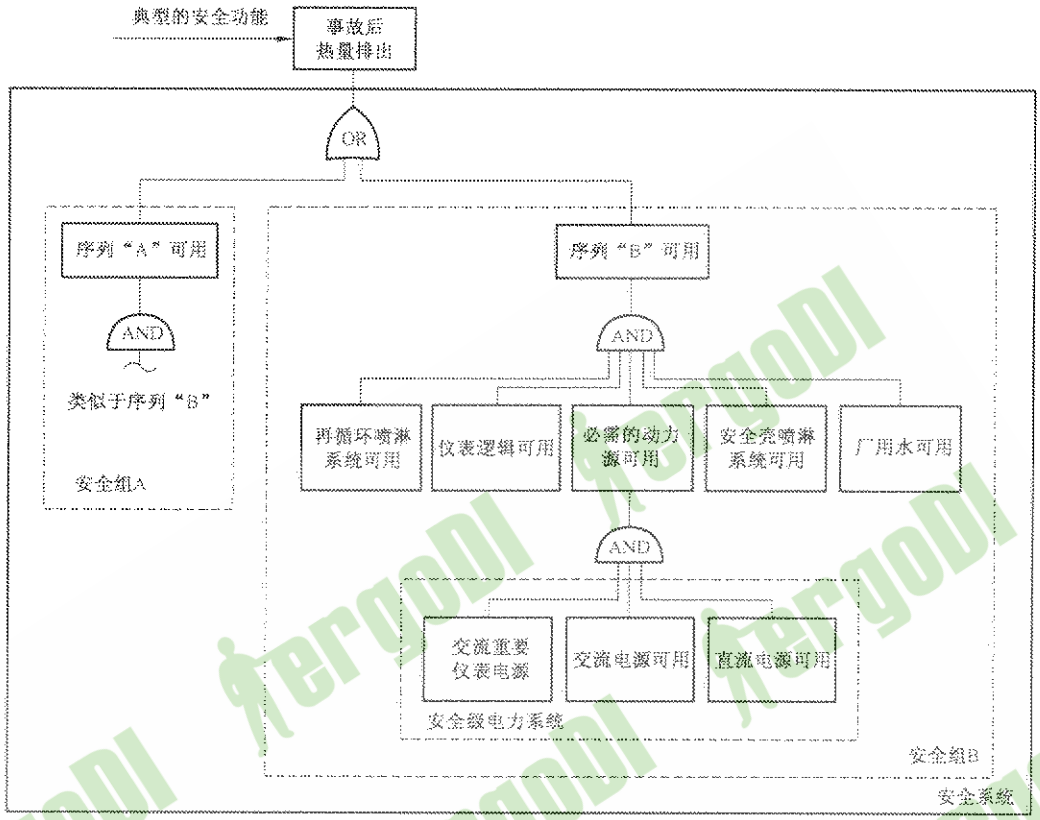
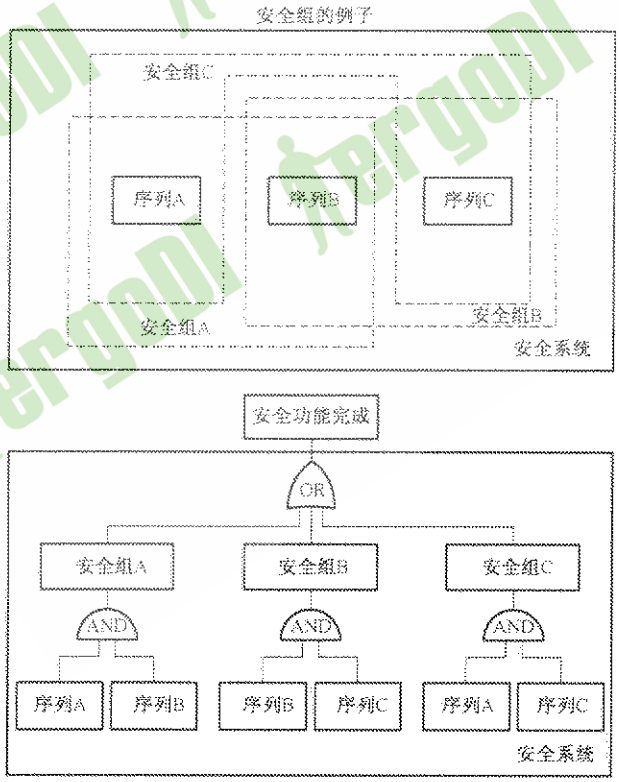



图 A.8 应急堆芯冷却部件:增加了安全级电源




注：每个序列由一个能力为100%的系统组成，因此，为完成这个安全功能的每个安全组只需要一个序列。

图 A.9 典型的安全功能




注：每个序列由一个能力为50%的系统组成，因此，为完成这个安全功能的每个安全组需要两个序列。

图 A.10 安全组的例子

# 附 录 B
（资料性附录）
电磁兼容性

## B.1 概述

由于部件(模拟的和数字式的)对电磁干扰(以下简称 EMI)的敏感性和易损性，所以需要考虑电磁环境。电磁干扰可能导致部件的运行异常或损坏。

4.7 要求在确定安全系统设计基准工况时考虑电磁环境。5.5 要求安全系统应设计成在所有可能产生危害的内部或外部条件下(包括 EMI)都能完成其安全功能。本附录为这些考虑提供指导，并且给出了有关定义和性能的其他参考文件。

## B.2 讨论

EMI 来源于几种耦合机理。在确定电磁环境、进行设备的 EMI 试验、设计仪表和控制系统时，应考虑这些耦合机理。

### B.2.1 电磁环境的确定

可以通过测量和(或)分析确定电磁环境。下述标准和导则可对电磁环境的确定提供指导：

IEEE Std 473,1985(1997 年重新确认)，电磁现场监测的 IEEE 推荐方法(10 kHz～10 GHz)；

MIL-STD-462，INT Notice 3，电磁干扰特性的测量。

### B.2.2 电磁环境的评定

安全系统设备必须设计成在承受核电厂的电磁环境时能完成其安全功能。这就要求考虑传导耦合、辐射耦合、感应耦合和电容耦合这 4 类耦合机理以及静电放电(ESD)。

#### B.2.2.1 传导耦合

绝大多数噪声是传导性耦合，传导性耦合具有下述特性：

a) 需要金属接触；

b) 噪声不受人线电缆移动的影响；

c) 噪声波形具有非零平均值(直流信号部分)；

d) 传导性耦合可以通过切断或分开金属接触，或者通过对噪声滤波消除。

#### B.2.2.2 辐射耦合

辐射耦合被称为电磁辐射或射频耦合，它在 1/6 波长以上的距离发生。通常只关心耦合的高频部分，此时波长很短，足以在短距离发生耦合，如电缆或任何天线类设备。电磁场强度与离辐射源的距离成反比，与发射功率的平方根成正比。阻止辐射耦合噪声的唯一方法是采用屏蔽技术，用以吸收或反射扩散的波。为实现有效屏蔽，屏蔽要完全地包围导体以屏蔽任何扩散的波。

#### B.2.2.3 感应耦合

当噪声和信号电路或导体经受电流变化并存在相互感应时，便发生感应或电磁耦合。此电磁场产生的能量(感应电压)与电流随时间的变化率、导体的长度和轴向位移成正比。

a) 感应耦合噪声某些可识别特性如下：

1) 噪声频率高或电流强(动力电缆)；

2) 具有很大的布线电感；

3) 不受非导电材料的影响；

4) 其磁场可探测。

b) 消除感应耦合噪声的方法包括：

1) 降低噪声频率或电流源；
2) 降低互感(环形线面积和导体的距离)；
3) 对噪声的滤波或屏蔽。

B.2.2.4 电容耦合

电容耦合由信号和噪声电路中金属表面之间的电场(电压改变)引起的。因此，电容耦合与金属的表面积、间距、阻抗和介质有关。

a) 某些可识别特性如下：
1) 相对于信号电压有较高的噪声电压；
2) 金属表面形成电容；
3) 高阻抗信号回路；
4) 噪声受电缆或人员移动影响。

b) 消除电容耦合噪声的方法如下：
1) 降低电压或减小噪声源频率；
2) 降低耦合电容(表面积)；
3) 降低线路阻抗；
4) 使用屏蔽。

可通过试验、分析或类似环境中有文件证明的运行经验等的组合来证明系统的抗电磁干扰能力，这些活动需考虑总的系统设计，包括某些降低设备敏感性的设计措施，例如采用绞合电缆、屏蔽电缆、光纤通信电缆等。试验规模应足以覆盖预期的环境，并且对异常工况和事件具有足够的裕度。

下述文件可对试验提供指导：

EPRI TR-102323:1994 动力厂中电磁干扰试验导则

IEC 60255-3:1989 继电器 第3部分：与时间相关或不相关的输入单一激励量的测量继电器

GB/T 17626.1 电磁兼容 试验和测量技术 抗扰度试验总论

GB/T 17626.2 电磁兼容 试验和测量技术 静电放电抗扰度试验

GB/T 17626.3 电磁兼容 试验和测量技术 射频电磁场辐射抗扰度试验

GB/T 17626.4 电磁兼容 试验和测量技术 电快速瞬变/脉冲抗扰度试验

GB/T 17626.5 电磁兼容 试验和测量技术 浪涌抗扰度试验

GB/T 17626.6 电磁兼容 试验和测量技术 射频场感应的传导骚扰抗扰度

GB/T 17626.7 电磁兼容 试验和测量技术 供电系统及所连设备谐波、谐间波的测量和测量仪器导则

GB/T 17626.8 电磁兼容 试验和测量技术 工频磁场抗扰度试验

GB/T 17626.9 电磁兼容 试验和测量技术 脉冲磁场抗扰度试验

GB/T 17626.10 电磁兼容 试验和测量技术 阻尼振荡磁场抗扰度试验

GB/T 17626.11 电磁兼容 试验和测量技术 电压暂降、短时中断和电压变化抗扰度试验

GB/T 17626.12 电磁兼容 试验和测量技术 振荡波抗扰度试验

IEEE Std C62.45:1997 对连接到低压交流电路的设备进行浪涌试验的导则

MIL-STD-461C Notice 2 对于电磁干扰控制的电磁发射和敏感性要求

B.2.3 系统设计中对电磁干扰的考虑

为防止电磁干扰，系统设计需要采用适当的设计技术。这些技术包括：

a) 屏蔽；
b) 地线选择；
c) 布线路径；
d) 抑制；

e) 滤波；

f) 数据品质检查；

g) 软件处理(如软件带通滤波)。

下述标准可提供设计指导：

IEEE Std 1050:1996 电厂中仪表和控制设备接地的 IEEE 导则

IEEE Std 518:1982(1996 年确认) 为尽量降低外部源对控制器的电噪声输入而采用的对电气设备安装的 IEEE 导则

# 附 录 C
（资料性附录）
提供附加信息的其他标准

这些标准在应用本部分时可能有作用：

GB/T 13285—1990 核电厂安全重要系统和部件的实体防护

EJ/T 562—2005 核安全有关的操纵员动作时间响应设计准则

EJ/T 570—2001 压水堆安全重要流体系统单一故障准则

ANSI/ANS 59.3—1992 控制用空气系统的安全准则

ANSI/ANS 59.51—1997 备用柴油发电机组的燃油系统

Code of Federal Regulations,CFR Publication 10CFR50.49(Jan.1994)

中华人民共和国
国家标准
核电厂安全系统
第1部分：设计准则
GB/T 13284.1—2008

*

中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码：100045

网址 www.spc.net.cn
电话：68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

*

开本 880×1230 1/16 印张 1.75 字数 42千字
2008年6月第一版 2008年6月第一次印刷

*

书号：155066·1-31576 定价 22.00元



GB/T 13284.1-2008