ICS 27.120.20
CCS F 83

中华人民共和国国家标准

GB/T 13284—2025
代替 GB/T 13284.1—2008

核电厂安全系统设计准则

Design criteria of safety systems in nuclear power plants

2025-04-25 发布　　2025-11-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替GB/T 13284.1—2008《核电厂安全系统　第1部分：设计准则》，与GB/T 13284.1—2008相比，除结构调整和编辑性改动外，主要技术变化如下：

——更改了术语的定义（见第3章，2008年版的第3章）；

——删除了整定值和安全状态限值的内容（见2008年版的4.4.4）；

——更改了安全系统的接口设备安全分级（见5.7.4.2，2008年版的5.6.3.1）；

——更改了共因故障的内容（见5.17，2008年版的5.16）；

——更改了手动控制方法（见6.3，2008年版的6.2）；

——增加了维修旁通的要求（见6.8）。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国核仪器仪表标准化技术委员会（SAC/TC 30）提出并归口。

本文件起草单位：核工业标准化研究所、北京广利核系统工程有限公司、中国核动力研究设计院。

本文件主要起草人：梁雪元、焦丽玲、王晓燕、杜建、裴红伟、武方杰、马建新、黄君龙、刘春明、刘宏春、陈鹏、何亮。

本文件及其所代替文件的历次版本发布情况为：

——1991年首次发布为GB 13284—1991，1998年第一次修订；

——2008年第二次修订时，将标准编号改为GB/T 13284.1—2008；

——本次为第三次修订。

核电厂安全系统设计准则

1 范围

本文件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。

本文件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的设计。对于保护整个核电厂安全所需的所有与安全有关的系统、构筑物和设备的设计参照使用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

GB/T 5204 核电厂安全系统定期试验与监测

GB/T 12727 核电厂安全重要电气设备鉴定

GB/T 12788 核电厂安全级电力系统准则

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 核电厂事故监测仪表准则

GB/T 13629 核电厂安全系统中可编程数字设备的适用准则

NB/T 20061 人因工程在核电厂系统、设备和设施中的应用

NB/T 20394 核电厂安全级控制盘、屏和机架的设计与鉴定

3 术语和定义

下列术语和定义适用于本文件。

3.1

安全功能 safety function

为了保证核设施或活动能够预防和缓解核电厂正常运行、预计运行瞬态和事故工况下的放射性后果，保证核安全而必须完成的特定功能。

[来源：GB/T 41143—2021，3.16，有修改]

3.2

安全系统 safety system

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件的后果的安全重要系统。

3.3

安全级 safety class

1E 级

核电厂电气设备和系统的一个安全级别。

注 1：这些设备和系统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 2：安全级（1E 级）是功能性的术语，完成注 1 中列举功能的设备和系统划归安全级。

[来源：GB/T 41143—2021，3.28]

3.4

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。

注：一个安全组包括一个或多个序列（见附录 A）。

3.5

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启动信号，或是操作装置内设备。

3.6

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。

3.7

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。

3.8

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。

3.9

多样性　diversity

为执行某一确定功能，设置两个或多个独立（或冗余）的、具有不同属性的系统或部件的一种设计原则。

注：多样性能够减少共因故障（包括共模故障）的可能性。

3.10

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部件和组件的一种配置。

注：一个通道在各单一保护动作信号汇合处终止。

3.11

共因故障　common cause failures

由特定的单一事件或起因导致两个或多个构筑物、系统或部件失效的故障。

3.12

可探测故障　detectable failures

能通过定期试验鉴别的故障，或通过报警或异常指示发现的故障。

注 1：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 2：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指示发现。

3.13

可接受的　acceptable

通过核电厂安全分析证明是满足要求的。

3.14

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。

注：设备范围是从被测过程变量开始，直到执行机构输入端为止。

3.15

相关电路　associated circuits

未与安全级电路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的非安全级电路。

注：电路包括互联的电缆和相连负载。

3.16

序列　division

与其他冗余系统或设备组在实体、电气和功能上建立并保持独立的某一给定系统或设备组的名称。

[来源：GB/T 41143—2021，4.1.19，有修改]

3.17

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。

注 1：一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，能作为一个单元被试验。

注 2：只要符合此定义，一个组件可以是一台大型装置的一块电路板卡、一个可抽出的断路器或其他子组件。

[来源：GB/T 41143—2021，4.2.2]

3.18

执行机构　execute feature

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执行装置组合。

注 1：执行机构由电气设备和机械设备及其连接件组成，其范围是从监测指令设备的输出端开始，直到并且包括执行与过程的耦合处。

注 2：在某些情况下，保护动作由直接对过程工况进行响应的执行机构（例如止回阀、自力式卸压阀）完成。

注 3：执行机构通常包括驱动设备、原动机及被驱动设备。

[来源：GB/T 41143—2021，4.2.6]

3.19

设计基准事件　design basis events

为确定构筑物、系统和部件的可接受的性能要求，在设计中采用的假设始发事件。

3.20

运行旁通　operating bypass

为避免安全功能在核电厂某些特定运行工况下动作而对执行安全功能的能力进行抑制。

注：运行旁通不同于维修旁通。在不同电厂运行模式下可能需要对某个特定安全功能进行自动或手动旁通。运行旁通用于运行模式的改变（如在冷停堆模式下阻止应急堆芯冷却的触发）。

3.21

维修旁通　maintenance bypass

由于更换、修理、试验或校准的需要，使通道、部件或设备部件丧失执行保护动作的能力。

4　安全系统设计基准

对核电厂每个安全系统的设计都应规定具体的基准，设计基准也应利于确定安全系统及其设计变更的充分性。设计基准至少应按下列内容形成文件。

a）　适用于核电厂每种运行模式的所有设计基准事件以及对应于每一事件的核电厂工况的初始条件和分析限值。

b）　对应每个设计基准事件的安全功能和执行机构的相应保护动作。

c) 所提供的每种运行旁通能力的允许条件。

d) 为控制每个保护动作而需要监测的变量，确定与每个变量有关的：

1) 分析限值；

2) 范围(正常、异常和事故工况)；

3) 在保护动作完成之前适应的变化率。

e) 对可手动触发或触发后可手动控制的 b)中确定的保护动作。对于每一个手动保护动作，应明确下列信息：

1) 允许手动控制的时刻与核电厂工况；

2) 允许只用手动触发或触发后只用手动控制的理由；

3) 在正常、异常和事故工况期间操作人员应执行手动操作时所经受的环境条件范围；

4) 在 d)确定的用于支持操作人员执行手动动作而应显示的变量，其要求应按照 GB/T 13627 执行。

f) 对于 d)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)，为达到保护目的所需要的传感器的最小数量和位置。

g) 在安全系统工作的正常、异常和事故工况期间，动力源、控制电源和环境参数(如电压、频率、辐射、温度、湿度、压力、振动和电磁干扰)所对应的瞬态和稳态条件。

h) 可能会引起安全系统功能降级或失效的情况(如飞射物、管道破裂、火灾、失去通风、消防系统误动作、操作人员失误、非安全有关系统中的故障)，以及为保持执行安全功能的能力而采取的对应措施。设计基准应包括分析、识别和应对系统的潜在危险的内容，能够指出哪些危害需要系统采取措施来保持执行安全功能的能力，或需要其他手段来维持核电厂安全。

i) 系统设计的可靠性目标。

j) 用于确定安全系统设计可靠性的方法适用于每个安全系统的设计。

k) 某一设计基准事件发生后的关键时刻或核电厂工况，包括：

1) 触发安全系统保护动作的时刻或核电厂工况；

2) 确定安全功能正确完成的时刻或核电厂工况；

3) 需要保护动作的自动控制的时刻或核电厂工况；

4) 允许安全系统恢复正常的时刻或核电厂工况。

l) 保护设备不受损坏但可能妨碍安全系统完成其安全功能的措施。

m) 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)。

5 安全系统准则

5.1 一般要求

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。核电厂安全系统中可编程数字设备的设计还应满足 GB/T 13629 的要求。

5.2 单一故障准则

安全系统在下列情况下应完成任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。有关应用单一故障准则的指

导应满足 GB/T 13626 的要求。

本文件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,或者为满足核电厂的可靠性目标或可用性目标也可采用符合逻辑。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考虑单一故障准则(见 NB/T 20402)。可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。概率评价的目的应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。

5.3 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,执行机构就能按预定程序完成全部安全动作。应只有操作人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第 4 章中 l)项规定的设备保护措施或操作人员有意识地干预措施。对各个通道不要求自保持。

5.4 质量

部件和组件的质量应符合最少量维修和故障率低的要求,为了提供高质量产品,需要制定设计、制造、质量控制、安装、校准和试验的具体操作规范。安全系统设备应按规定的质量保证大纲进行设计、制造、检验、安装、试验、运行和维修。

5.5 设备鉴定

对安全系统设备应采用型式试验、运行经验、分析或这三种方法的任意组合进行鉴定,证实它能满足设计基准规定的性能要求。安全级电气设备的设备鉴定应满足 GB/T 12727 的要求。

5.6 系统完整性

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,见第 4 章中 g)和 h)。

安全功能的设计应具有确定的(即可预测和可重复的)行为和时序。

5.7 独立性

5.7.1 通用要求

独立性应满足 GB/T 13286 的要求。

5.7.2 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之后,能保持完成该安全功能的能力。

5.7.3 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,以保持满足本文件要求的能力。按 5.5 规定进行设备鉴定是满足此要求的一种方法。

5.7.4 安全系统与其他系统之间

5.7.4.1 一般要求

安全系统设计应使设计基准第 4 章中 h)所规定的其他系统的可信故障和相应的行为不妨碍安全系统满足本文件的要求。

5.7.4.2 接口设备

与安全系统互联的属于其他系统的设备应符合以下准则。

a) 分级原则。

1) 执行安全功能的设备归为安全系统的一部分。

2) 未执行安全功能但连接到安全系统的设备要满足以下条件之一：

——归为相关电路；

——归为非安全级的设备，与安全系统电气隔离，对所有信号设备具有功能独立性。

3) 用于安全系统边界的隔离装置也要归于该安全系统。

b) 隔离原则：在需要安全功能的任何设计基准事件期间和之后，隔离装置的非安全方面的任何故障或事件都不需阻止安全系统的任何部分达到其最低性能要求。隔离装置要确保所有信号设备的电气隔离和功能独立性。隔离装置的故障要与安全系统中其他设备故障以相同的方式进行评估。

5.7.4.3 邻近设备

邻近设备满足下列要求。

a) 分隔，实体上靠近安全系统设备，但既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。实现实体分隔可采用实体屏障、可接受的分隔距离，或两者组合。

b) 屏障，对某一安全系统起边界作用的实体屏障，应在第 4 章中 g)和 h)规定的使用条件下满足 5.4～5.6 的要求。

5.7.4.4 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，这一要求的应用指导应按照 GB/T 13626 执行。

5.8 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，并且再现接近实际应用的安全功能特性。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，如下准则均应满足：

a) 提出合适的理由(例如，证明不存在切实可行的设计方案)；

b) 证明设备运行具有可接受的可靠性；

c) 在核电厂停运期间提供试验和校准能力。

5.9 信息显示

5.9.1 用于手动控制操作的显示

为完成安全功能所需的手动控制动作而提供的显示仪表应是安全系统的一部分，并应符合 GB/T 13627 的要求。

5.9.2 系统状态指示

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

执行机构保护动作的指示和识别。系统的设计避免模糊的指示，以免操作人员混淆。提供安全系统状态指示的仪表不必是安全系统的一部分。

5.9.3 旁通指示

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，就应在控制室连续指示每一个受影响的安全组的情况。如下准则均应满足：

a) 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，则这种指示自动产生；

b) 在控制室内具备手动触发这种指示的能力。

这种显示仪表不必是安全系统的一部分。

5.9.4 位置

信息显示装置应位于操作人员能接近的地方。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够看见。显示位置宜考虑包括功能任务分析结果和可接受的人因方面的考虑，可参考 NB/T 20061 和 GB/T 13627。

5.10 访问控制

安全系统的设计应允许对安全系统设备的访问实施管理控制。管理控制应通过安全系统内部措施、核电厂设计措施或两者结合实现。

5.11 维修

安全系统的设计应易于对故障设备及时识别、定位、更换、维修和调整。

5.12 标识

在核电厂的设计、建造、维修和运行期间，安全系统的标识满足下列要求：

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 NB/T 20394 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应要求频繁引用参考资料；

e) 有关文件应明确标识。

5.13 辅助设施

安全系统的辅助设施应满足本文件的所有要求。

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，由于没有与安全系统隔离而成为安全系统的一部分，必要时其设计应满足本文件的要求，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 1。附录 A 给出了应用本文件的一些说明。

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

注 1：3×3 矩阵顶部安全系统分为监测指令设备、执行机构和动力源 3 个通用单元；矩阵左边一列安全系统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 3 个工作单元。

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

注 3：从图 1 矩阵的一行看到，一个工作单元能够组成一个系统，如厂用水系统；从一列看到，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 4：每一个工作单元包括一个或几个通用单元；属于某一通用单元的设备不限于在一个工作单元中使用。

图 1　安全系统的 3×3 矩阵示例

5.14　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的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应满足 GB/T 12788，单一故障准则用于共用系统应满足 GB/T 13626 的要求。

5.15　人因工程考虑

在设计的开始阶段和设计全过程中，应按 NB/T 20061 的规定考虑人因工程，以保证分配给操作人员和维修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。

5.16　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。

5.17　共因故障

安全系统的设计和开发应应对可能导致安全系统功能降级或失效的共因故障。应对共因故障的方法宜包括确定以下内容。

a）　发生共因故障的可能性足够低。可接受的减少某些共因故障来源发生可能性的方法包括本文

件所规定的要求。质量（见5.4）、设备鉴定（见5.5）和设计属性（例如5.6和5.7）提供了防止设计和制造缺陷、外部环境影响和内部故障的保护。人因工程（见5.15）对操作人员差错提供保护。此外，人员培训和电厂规程（即运行、维护和监督）提供了防止人为差错的保护。其他考虑的因素包括可测试性、适用的运行经验和安全系统设计的多样性。

b) 共因故障与任何设计基准事件一起发生所造成的安全影响低，因而公共健康和安全得以维持。确定安全系统共因故障影响的一种可接受方法是，将安全功能的丧失或降级与适用的设计基准事件一起进行电厂级分析。

如果共因故障的后果很轻微，即使不能证明发生共因故障的可能性低，或者如果共因故障的后果是严重的，确定共因故障发生的可能性低，其包含共因故障源的安全系统设计均可能是合理的。每个已识别的共因故障来源宜逐一评估。

6 监测指令设备的功能和设计要求

6.1 一般要求

除第5章规定的功能和设计要求外，以下（见6.2～6.9）要求也适用于监测指令设备。

6.2 自动控制

除第4章中e）所述的情况以外，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，在第4章中e）规定的时刻与规定的核电厂工况出现之前，不需要操作人员采取任何操作。在选择安全系统设计方案时，对第4章中e）所述保护动作也可提供自动触发和控制的手段。

6.3 手动控制

手动控制包括以下方法。

a) 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。所提供的方法应包括：
   1) 将操作人员的分散操作次数减到最少；
   2) 将执行操作的时间减到最少；
   3) 将操作人员进行操作所需的分散位置的数量减到最少；
   4) 在符合5.7.1规定的前提下使用的设备最少。

b) 在控制室中对第4章中e）鉴别的并且没有按6.2的要求选为自动控制的保护动作提供手动触发和控制的方法，为这些动作提供的指示应符合5.9.1的规定。

c) 按第4章中k）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。

要求操作人员采取的动作以及有关的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作人员的数目相适应。上述的控制设备应安装在操作人员可接近的地方和适于操作人员工作的环境中，其布置应适合操作人员的监视和操作。

6.4 监测指令设备与其他系统之间的相互作用

6.4.1 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，而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。对6.4.1的解释见图2。

a) 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。主通道和备用通道均应为监测指令设备的一部分。备用通道应从下列通道中选择：

1） 与主通道变量组不同的监测通道；

2） 同样变量但所用设备与主通道不同的监测通道；

3） 与主通道变量组不同，且与主通道所用设备也不同的监测通道。

b） 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。这样的设备是安全系统的一部分。

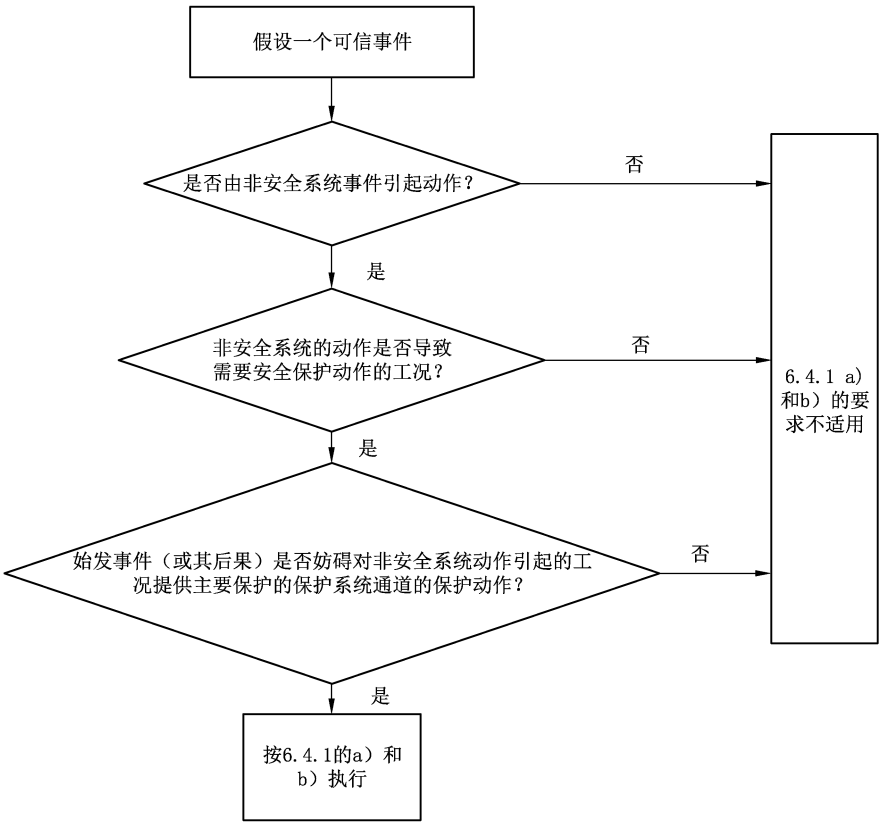


图 2 单一可信事件对监测指令设备及其相关系统的影响示意图

6.4.2 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 6.4.1 和 6.8 的要求。采取的措施包括降低符合度的要求，使取自受影响的冗余通道的非安全系统信号无效，或者将受影响的通道置于触发状态。

6.5 系统输入

只要实际可行，监测指令设备的输入来源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。

6.6 试验和校准能力

6.6.1 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。有多种方法可实现这一要求，例如：

a） 扰动被测变量；

b） 在 6.8 的约束下，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） 在相互之间具有已知关系且具有可用读数的通道之间进行交叉检查。

6.6.2 保证事故后运行的可用性

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以保证其运行可用性：

a） 采用 6.6.1 所述的方法检查传感器的运行可用性；

b） 在事故后一段时间内，确定设备是稳定的，并且确定其校准周期。

6.7 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。

6.8 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，系统的每一部分应满足以下要求之一。

a） 监测指令设备满足 5.2 和 6.4 的要求。

b） 在维修旁通期间，对于因冗余度限制不能满足 5.2 和 6.4 要求的部分监测指令设备，采取补充措施确保整体监测指令设备的可靠性没有受到明显的有害影响。例如，可进行评估，为维修旁通而允许退出运行的时间足够短，以确保满足整个监测指令设备的可靠性指标。

6.9 整定值

应采用形成文件的方法确定第 4 章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 NB/T 20072。

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，保证在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 执行机构的功能和设计要求

7.1 一般要求

除第 5 章提出的功能和设计要求以外，执行机构还应满足 7.2～7.6 的要求。

7.2 自动控制

执行机构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安全系统设计基准规定的动作。

7.3 手动控制

如果对执行机构中任一执行部件提供手动控制，则为完成这种手动控制在执行机构中增加的设计措施不应违反 5.2 和 6.3 的要求。执行机构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。

7.4 保护动作的完成

执行机构的设计应是一经触发，就完成其保护动作。这一要求不应排除使用第 4 章中 l)规定的设备保护装置，也不应排除操作人员有意识干预的措施。

当监测指令设备恢复正常时，执行机构不应自动恢复正常，应需要操作人员有意识地独立操作才能恢复正常。在最初的保护动作完成以后，执行机构可要求手动或自动(即周期性的)控制特定的设备，以继续完成安全功能。

7.5 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。

7.6 维修旁通

当执行机构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。执行机构中冗余度为一(即二取一、三取二等)的那部分应设计成，当机构的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、二取二等)，机构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 电力动力源

为安全系统供电的安全级电源系统应符合本文件和 GB/T 12788 的规定。符合本文件规定的安全系统供电的那部分是安全级电源系统，并且是安全系统的一部分。

8.2 非电力动力源

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，应提供符合本文件要求的动力，但其特定的设计准则不属于本文件的范围。

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，当动力源的一部分处于维修旁通时(即暂时将其冗余度降为零)，动力源其余部分应能提供可接受的可靠性。

附 录 A
（资料性）
安全系统范围开发过程的一些基本概念的图解

A.1 目的

使用安全系统全范围开发中的一些基本概念，本附录描述了如何应用本文件。

A.2 讨论

最基本和最明显的起点就是识别一项安全功能的概念。

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

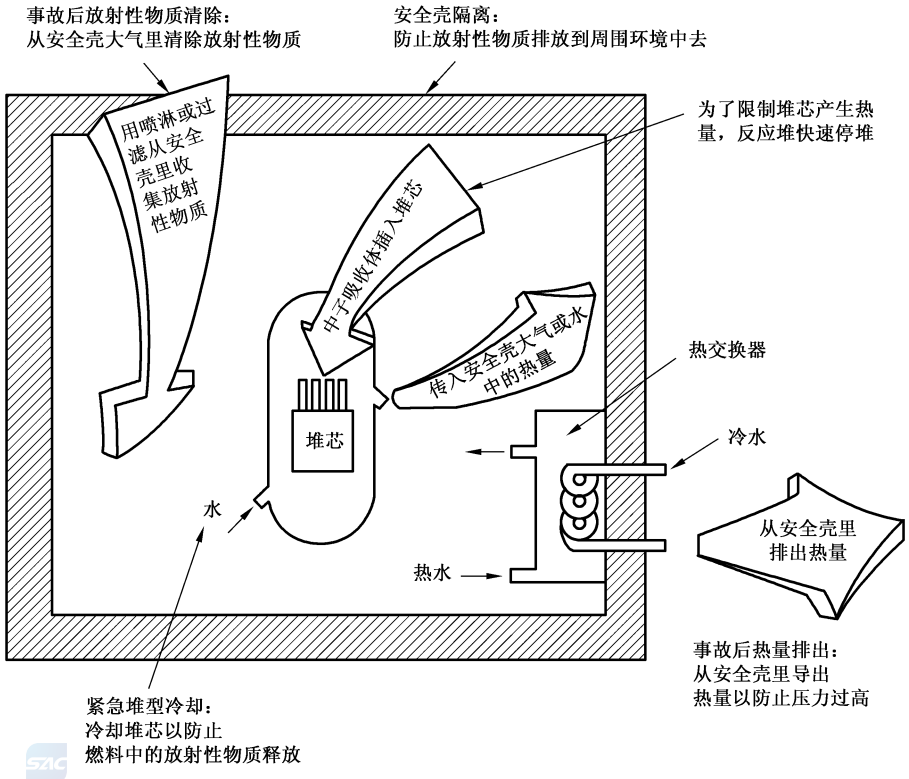


图 A.1 压水堆失水事故（LOCA）安全功能

A.3 典型安全系统范围的阐述

根据定义，一个安全系统包括实现某个安全功能所需的全部设备。

图 A.2 是一个典型的安全系统方框图，用紧急堆芯冷却功能来图解一个典型的安全系统。图 A.3 说明了从一个通用的安全系统到提供紧急堆芯冷却所需具体元素的转变。

图 A.4～图 A.8 说明了安全系统的一个序列，用流程图和单线格式，以逐个增加元素的方式组成紧急堆芯冷却系统。从图 A.4 的裸堆开始，图 A.5 加上了紧急堆芯冷却系统(ECCS)的监测指令设备；图 A.6 加上了紧急堆芯冷却系统的执行机构，即紧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，即安全级电源而构成了该安全系统的一个完整序列。

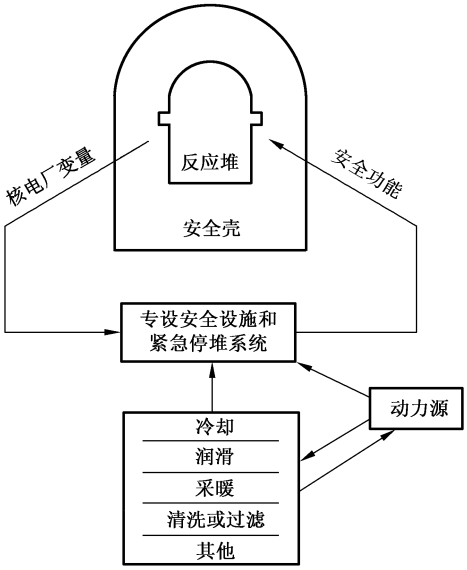


图 A.2 典型的安全系统方框图

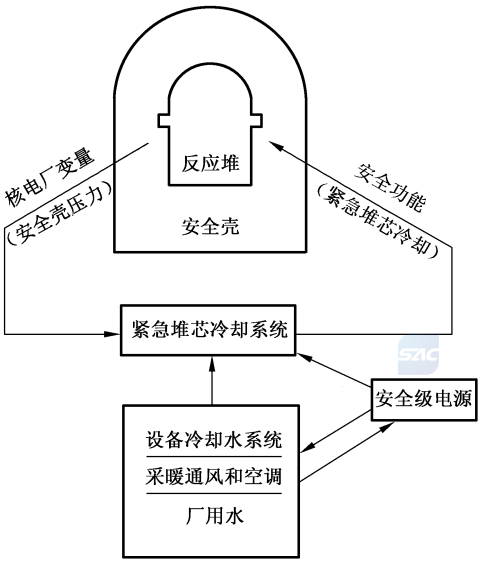


图 A.3 紧急堆芯冷却设备

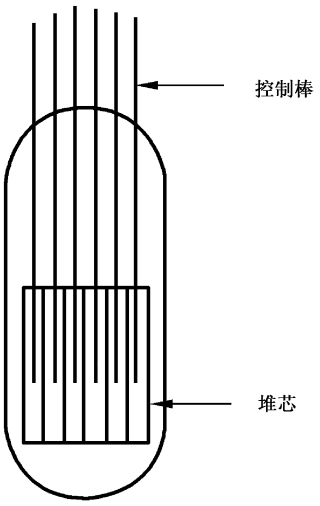


图 A.4　紧急堆芯冷却部件:反应堆

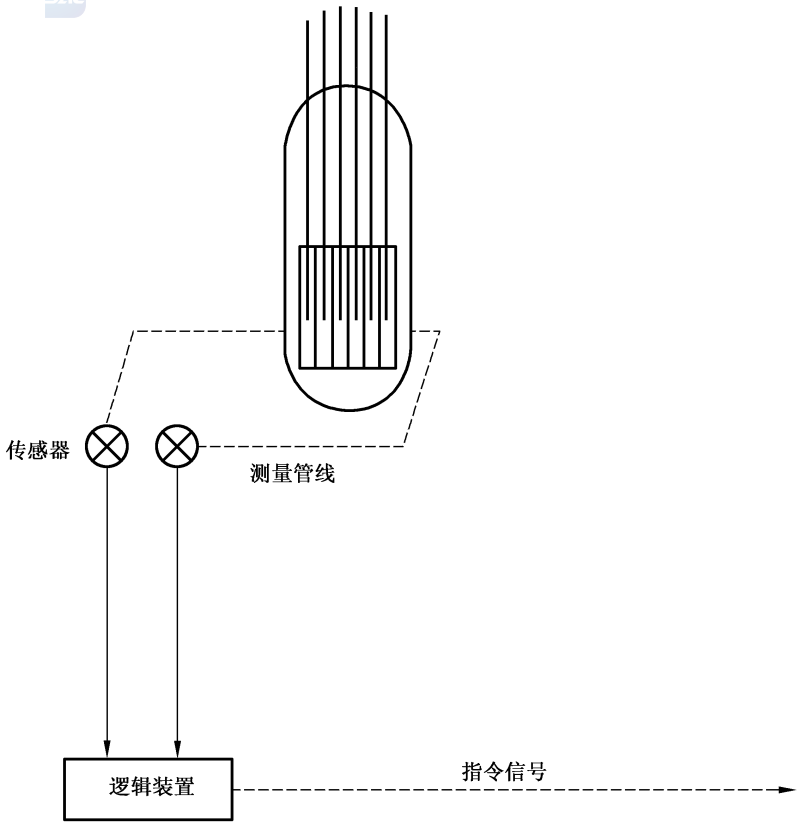


图 A.5　紧急堆芯冷却部件:增加了监测指令设备

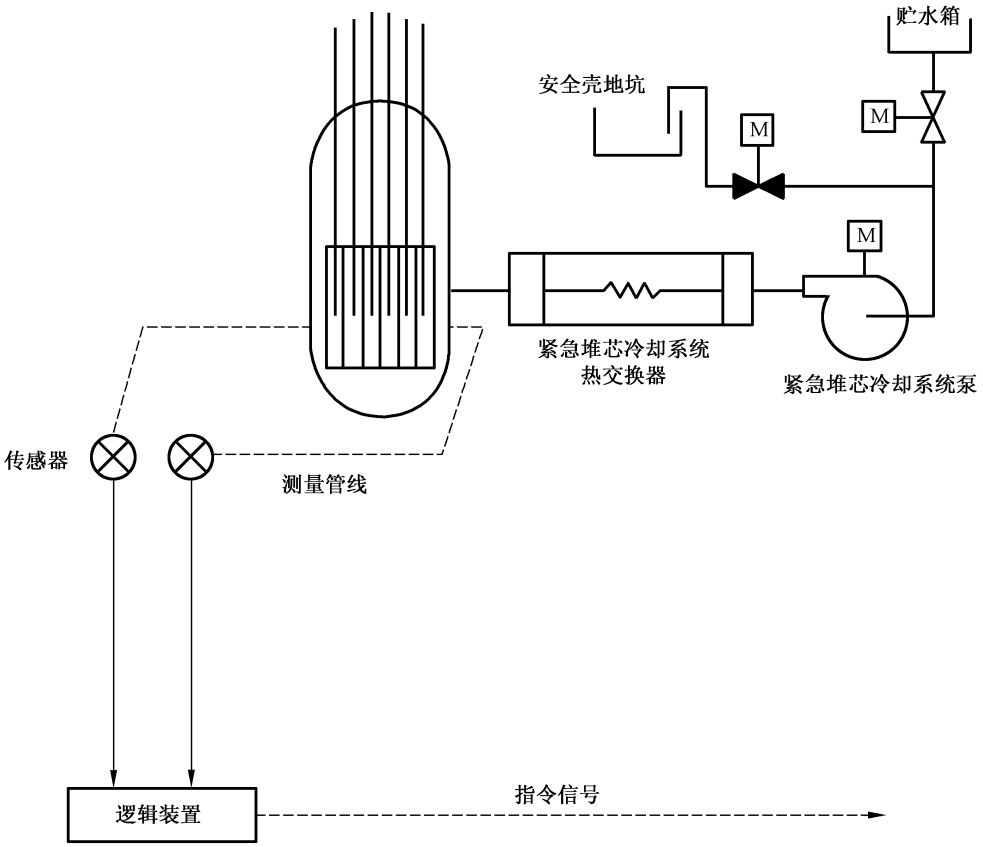


图 A.6　紧急堆芯冷却部件:增加了执行机构

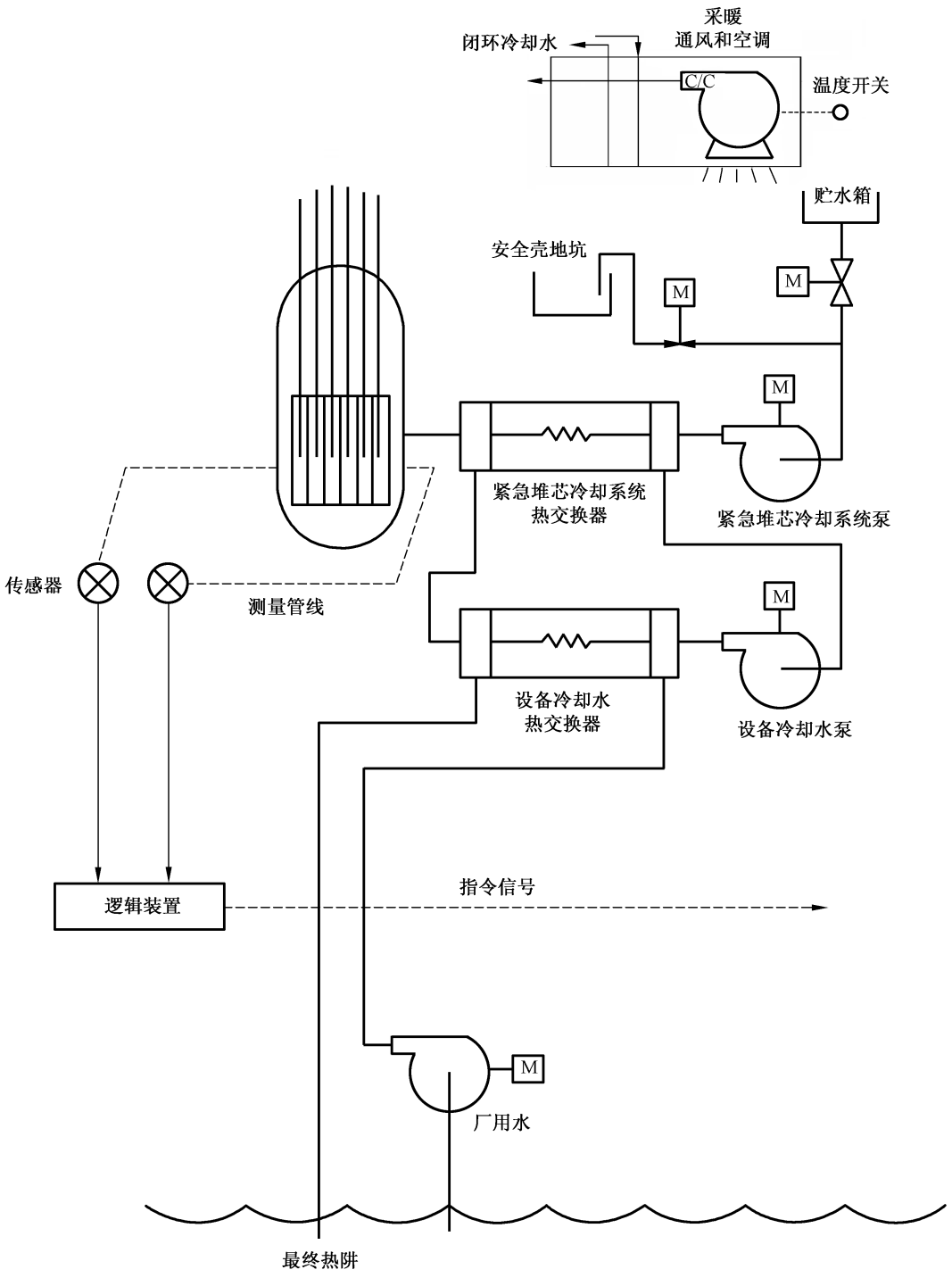


图 A.7　紧急堆芯冷却部件:增加了一些辅助支持设施

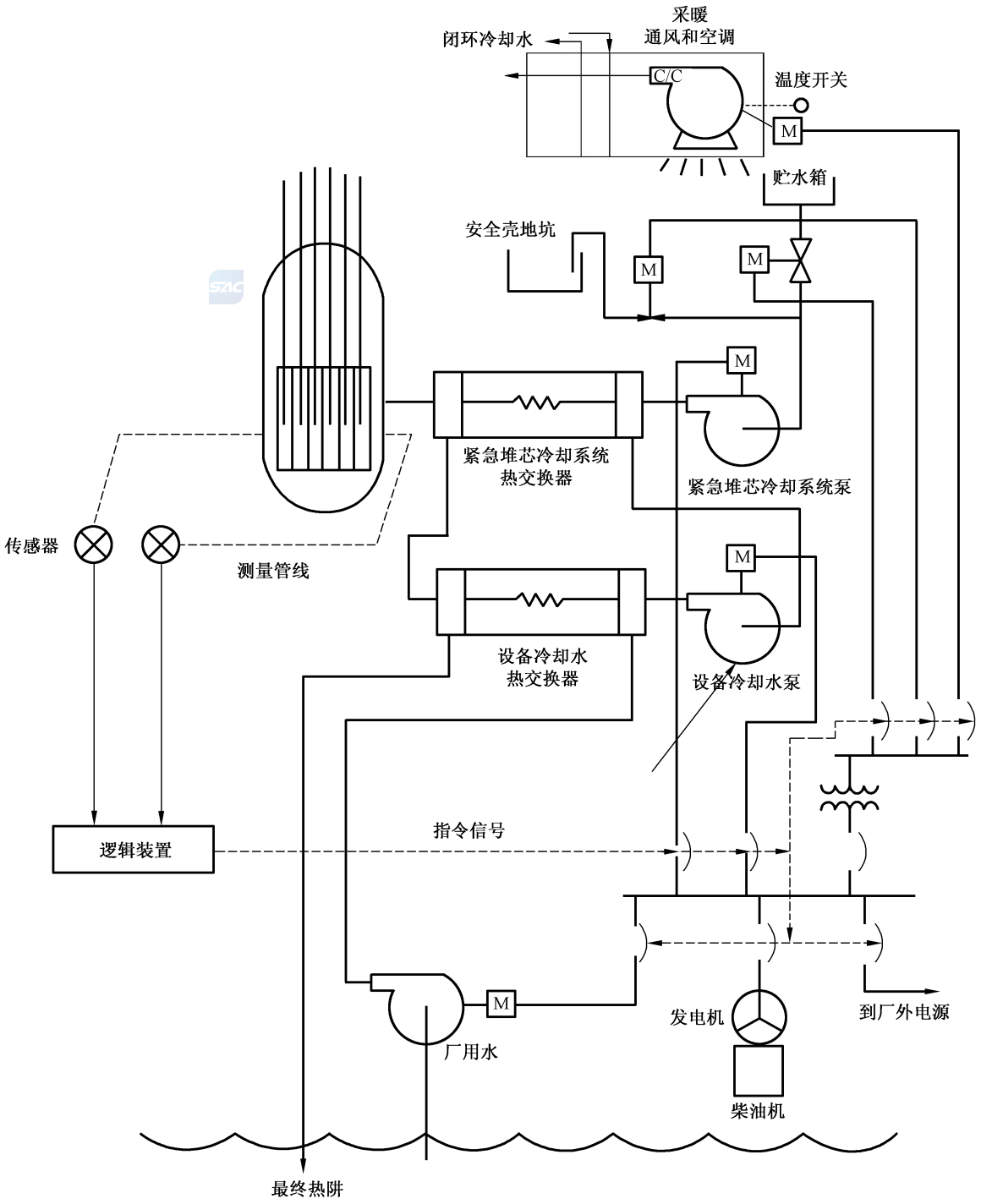
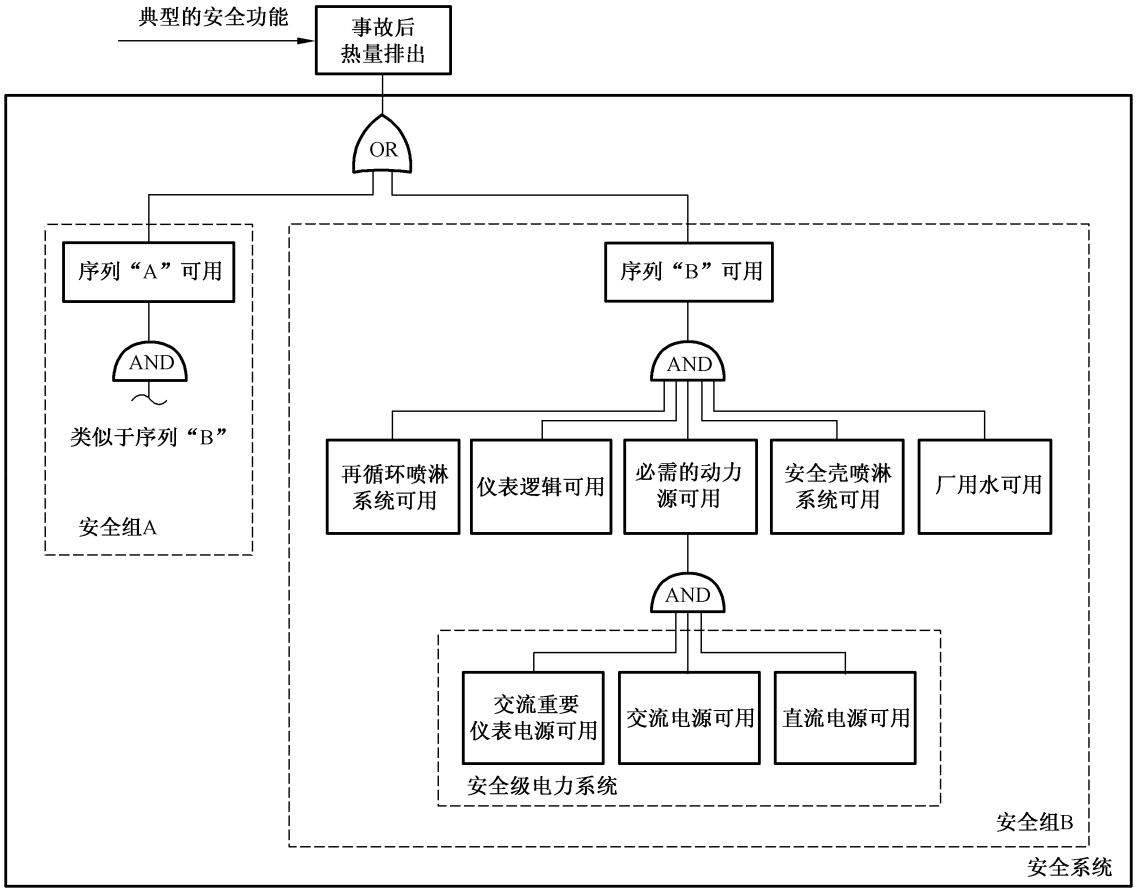


图 A.8　紧急堆芯冷却部件:增加了安全级电源

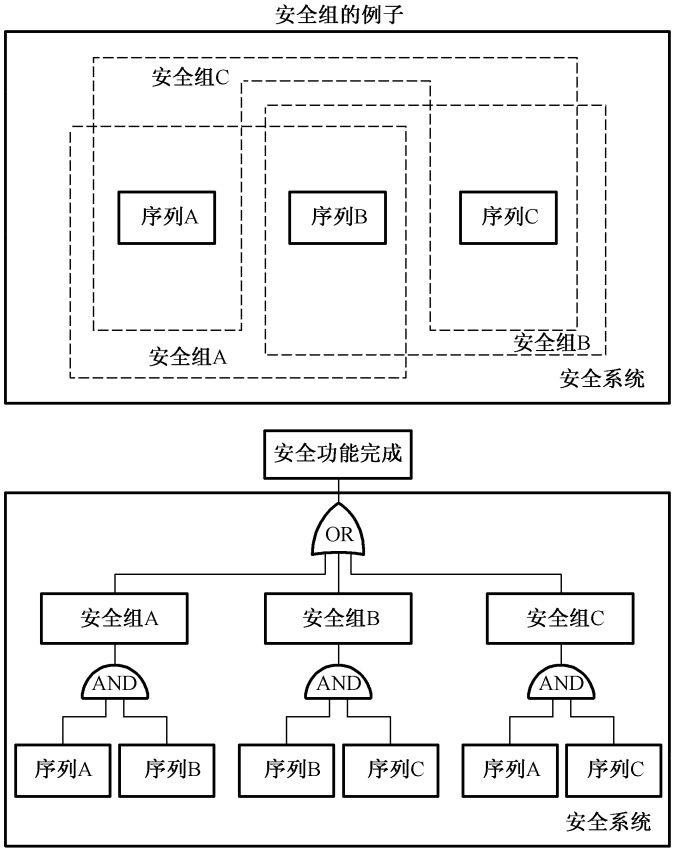
A.4　安全组

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 3 个安全组,为了完成某一安全功能,每个安全组要求 3 个序列中有任两个序列(三取二)工作,这时安全组按图 A.10 中的逻辑来区分。



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只需要两个序列。

图 A.10　安全组的例子

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1所示。正如5.13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，允许不满足安全系统准则的例子如运行旁通、维修旁通和旁通显示。

为了说明这些准则的应用，以安全级母线继电保护为例。继电保护的一个功能是提高安全级电力系统的可用性和可靠性，但是从安全系统角度来看，其基本功能是防止在安全系统运行时出现误脱扣。这一基本功能符合本文件的要求；提高安全级电力系统可靠性和可用性的功能要求见GB/T 12788。

参 考 文 献

[1] GB/T 7163 核电厂安全系统可靠性分析要求
[2] GB/T 9225 核电厂系统与其他核设施可靠性分析应用指南
[3] GB/T 41143—2021 核电厂仪表和控制术语
[4] NB/T 20402 压水堆安全重要流体系统单一故障准则
[5] NB/T 20072 核电厂安全系统仪表触发整定值的确定和保持