中华人民共和国国家标准

核电厂控制室的设计

GB/T 13630—92

Design for control rooms of nuclear power plants

本标准等效采用国际电工委员会 IEC 964《核电厂控制室的设计》。

1 主题内容与适用范围

本标准规定了核电厂控制室的功能设计、人机接口要求、控制室人员配备操作规程和培训大纲的功能接口要求；还规定了检验与核准功能设计程序。

本标准适用于核电厂控制室的设计。

本标准不适用于特设的或通常无人管理的控制系统，如：控制室外的停堆系统、放射性废物处理控制系统、应急响应设施等。

2 引用标准

HAF 0200 核电厂设计安全规定

HAF 0202 核电厂防火

HAF 0204 核电厂内部飞射物及其二次效应的防护

GB 2951.19 电线电缆 燃烧试验方法

3 术语

3.1 报警 alarms

由光字牌或其他显示系统发出信号，向操纵员通告电厂和设备出现故障或电厂运行工况的变化超出允许范围，要求操纵员采取行动。

3.2 音响警报系统 audible warning systems

出现异常情况（例如：火灾、必须撤离安全壳或其他建筑物）时，发出音响警报的系统。

3.3 辅助控制（操作）系统 auxiliary control (operating) systems

安装在控制室外面的操作系统，例如：辅助控制点和就地停堆系统。

3.4 控制室系统 control room system

人机接口、控制室工作人员、操作规程、培训大纲和相关的设施或设备的总体，它们共同维持控制室功能的正确执行。

3.5 控制室工作人员 control room staff

定岗在控制室的一组电厂运行人员。他们通过人机接口按制电厂，对完成电厂的运行目标负责。通常，控制室工作人员由值班长和实际执行操作的操纵员组成。

3.6 控制器 control

操纵员用来向控制系统和电厂物项发送指令信号的设备。

3.7 通讯系统 communication system

国家技术监督局 1992-08-29 批准　　1993-04-01 实施

运行与管理人员、就地操纵员以及位于控制室设施之外的其他电厂人员之间交换信息的设施、设备和装置等。

3.8 显示器 displays

用于监督电厂工况和状态(例如:过程状态、设备状态等)的装置。

3.9 人类工效学 ergonomics

依据工作环境和由人力操作的设备,研究人的能力和心理的科学。

3.10 格式(显示格式) format(display format)

在屏幕显示器上显示信息的画面形式,例如:信息文字说明、数字表达、符号、模拟图、柱状图表、趋势图像和多角形显示。

3.11 功能 function

由人或自动系统所执行的一种行动或任务。

3.12 功能目标 runctional goal

为完成相应的功能,必须达到的性能指标。

3.13 功能分析 function analysis

根据可利用的人力、技术和其他手段,研究系统的各项功能目标,以便提供确定功能如何分配与执行的依据。

3.14 层次目标结构 hierarchical goal structure

将功能目标和子功能目标构成分层次的目标结构,表明功能目标和子功能目标之间的关系。

3.15 高级思维处理 high-level mental processing

为获得归纳与概括的信息,人对信息进行处理和(或)解释的活动。

3.16 人因工程 human factor engineering

就机器的设计、各种作业和人对实际环境的适应能力而言,有关人的能力和限度的知识领域。

3.17 不符人因工程原则 human factor engineering discrepancy

依据人因工程原则衡量,系统设计不符合操纵员的能力和职责。

3.18 仪表控制系统 instrumentation and control system

实现自动与手动控制的设备,它由仪表、控制和信息系统组成。

3.19 作业 job

操作上相关的一组任务。一项作业的任务所要求的技能、知识和责任应是一致的。

3.20 作业分析 job analysis

分析某一作业对控制室人员的配备、操作规程和培训大纲的基本要求。

3.21 就地控制点(或设施) local control points(or facilities)

设置在控制室外面的控制点(或设施),在那里就地操纵员进行控制活动。

3.22 就地操纵员 local operator

在控制室外面执行任务的操纵人员。

3.23 机器 machine

硬设备,即装置、设备和(或)仪表与控制系统。

3.24 人机接口 mau-machine interface

操纵人员与仪表控制系统和计算机系统之间的交接面。它包括显示、控制和操纵员支持系统的交接面。

3.25 运行人员 operating staff

为电厂运行轮班工作的电厂人员,包括控制室工作人员、维护人员等。

3.26 操作规程 operating procedures

规定为完成功能目标所需操作任务的一组文件。

3.27 人机交互作用 operator interaction

操纵员和仪表控制系统之间的相互关系，即：仪表控制系统显示的电厂状态和相应的操纵员活动之间的相互关系。

3.28 操纵员支持系统 operator support system (oss)

支持控制室工作人员的高级思维处理任务的一个或多个系统。

3.29 性能要求 performance requirements

确保功能目标实现，对规定的任务性能的定量要求。

3.30 广播系统 public address-system

呼叫电厂各个位置上的人员的扩音系统。

3.31 电厂运行目标 plani operational goal

电厂设计的最终目的，即按需要发电和限制向环境释放放射性。

3.32 公认惯例 population stereotype

一群人或全体人员中的大多数人，对某个特定的刺激源给出相同响应的趋势。公认惯例由抽样人口的传统和习惯决定。

3.33 任务 tasks

为实现某个功能目标，由人或机器所执行的一系列动作。

3.34 任务分析 task analysis

详细描述操纵员的任务。根据任务的组成，确定人活动的细节，以及这些活动的功能和时间的关系。

3.35 培训大纲 training programme

为培训控制室工作人员，使他们获得运行活动所必需的技能和知识所制定的大纲。

3.36 核准 validation

为确定某个问题的解决是否遵守了功能、性能和接口要求而进行的试验与评价。

3.37 检验 verification

确定控制室各组成部分是否满足规定要求的过程。在本标准中，检验是对照电厂工程准则、人因工程准则和操作与功能的要求，对控制室系统的各单个组成部分的核查。

3.38 屏幕显示 visual display unit (VDU)

用屏幕显现由计算机驱动的图像的显示设备，例如，CRT、等离子体显示器。

4 控制室的设计原则

4.1 控制室的主要目标

控制室的主要目标是实现核电厂在其所有运行和事故工况下安全与有效地运行。

控制室为控制室工作人员提供实现电厂运行目标所必需的人机接口和有关的信息和设备。

此外，控制室为控制室工作人员提供适宜的工作环境，以利于执行任务，而无不适之感和人身危险。

4.2 控制室的功能设计目标

控制室设计的基本目标是及时、准确和完整地向操纵员提供关于电厂设备和系统的功能状态的信息。

控制室设计必须考虑到所有运行状态下，包括换料和事故工况，使任务最佳化，并将监督与控制电厂所要求的工作量减到最小，控制室还必须向控制室外的其他设施提供必要的信息。

控制室设计必须提供各项功能的最佳分配，以便操纵员和系统能最大限度地发挥其能力。

控制室设计的另一个目标是使电厂能有效地进行试运行，并允许修改与维护。

4.3 安全原则

控制室必须使核电厂在所有运行状态下安全地运转。在设计中考虑的设计基准事件和事故工况发生之后，控制室仍能使电厂恢复到安全状态。

控制室内控制设备的设计应尽可能地阻止非安全手动指令的执行，例如应用取决于电厂状态的逻辑联锁。

在安全与非安全系统紧密相邻的地方，必须考虑功能的隔离和实体的分隔。

按制室必须采取适当的措施，保障控制室内人员的安全，免受可能的危险，例如，闯入未经批准的人，事故工况所产生的放射性，有毒气体，或火灾的后果等，这些事件都会危及操纵员必需的活动。

必须设有适当的通路，保证在紧急情况下，控制室工作人员能通过该通路撤离或抵达控制室，或去其他控制点。

4.4 可用性原则

为使电厂的容量因子最高，以保证核电厂建设投资及时回收，在控制室设计中必须考虑下列各项：

a. 便于电厂按计划运行；

b. 把因操纵员的错误判断与操作、或因仪表控制系统失灵与故障造成的局部扰动引起的意外功率降低或电厂停堆的几率减到最小。

提高可用性的技术措施必须不违背安全原则。

4.5 人因工程原则

为了提供各功能的最佳分配，保证人与机器能最大限度的发挥其能力，并使电厂的安全与可用性最好，设计必须特别注意人因原则和人的特性，例如：人体尺寸、人的感觉、思维、生理和运动机能的反应能力与限度。

4.6 营运管理原则

操纵员的配备与培训是控制室系统和运行管理的一部分，为了使核电厂最安全与最有效地运行，控制室必须配备数量足够并有专业技能的工作人员。

工作人员必须经过控制室运行方面的技术训练，受到有关核电厂运行与安全的工程原理的教育，具备电厂子系统和组成设备及其功能、性能和位置方面的详细知识。

由就地操纵员执行的任务，包括电厂设备的操作，必须受控制室行政上的管理与监督。

为确保核电厂的运行质量，在控制室的人员配备方面，营运单位应考虑以下因素：

a. 人员选择与资格的要求；

b. 正常、异常与事故工况下培训与进修的要求；

c. 操作技能的定期进修和扩充他们的工程原理知识的机会；

d. 在正常和紧急运行期间，控制室工作人员和每个人的职责。

4.7 与其他控制和管理中心的关系

为了帮助控制室工作人员对异常运行工况作出反应，在应急工况下，应急响应设施应能投入运行。

在控制室外还必须设置辅助控制点，以便在控制室不能执行其安全功能时，能使反应堆安全停堆，并将其保持在安全状态。

必须为这些控制点和设施提供信息交换设备。这些设备的运行必须不依赖控制室内的其他设备。

5 控制室的功能设计

必须使用一种系统化的方法来进行控制室的功能设计，并包括图 1 中所示的控制室和有关项目。这种设计方法必须包括图 2 所示的下列四个步骤：功能分析、功能分配、功能分配的检验与核准、作业分析。

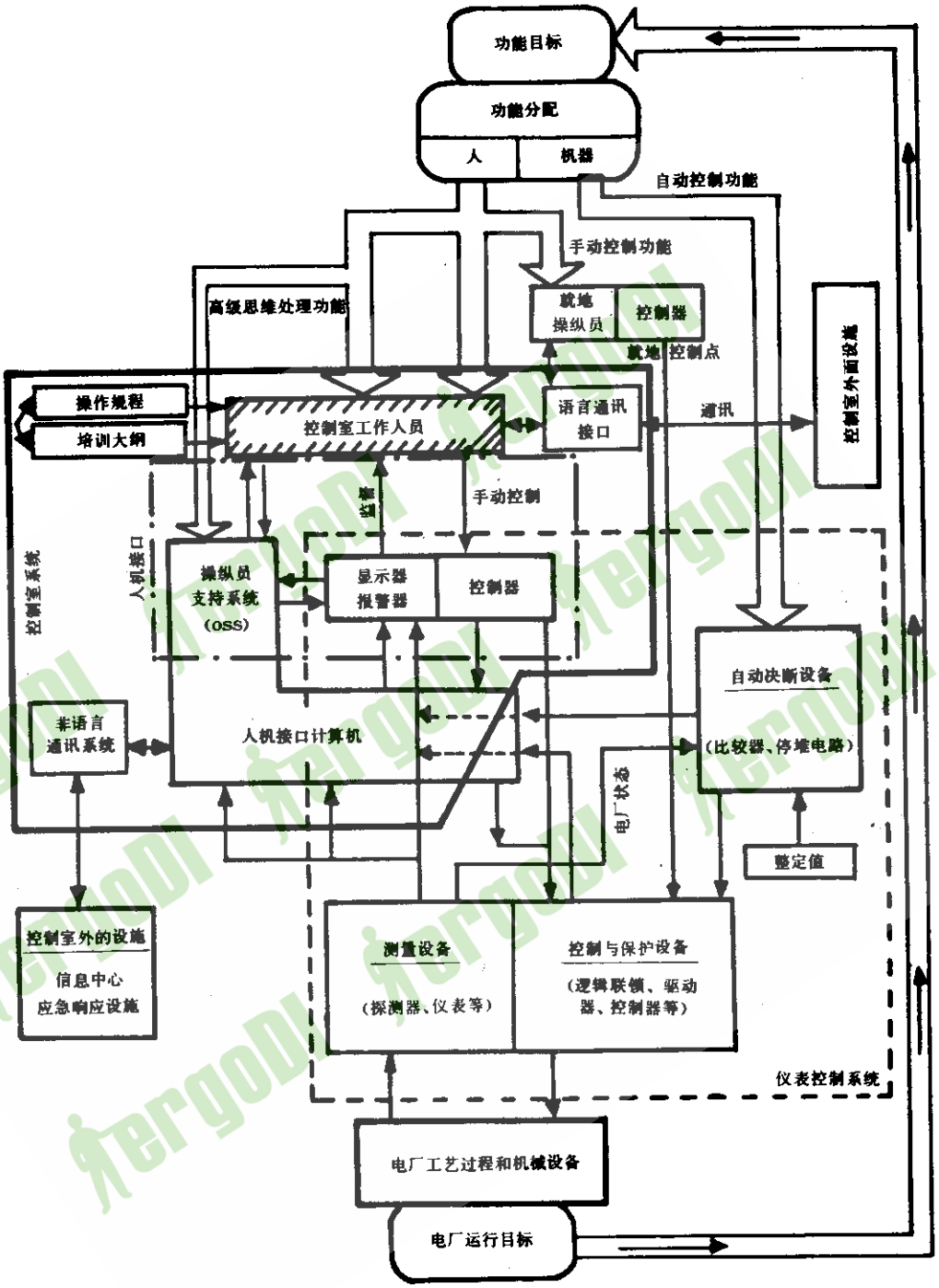

图 1　控制室系统的概貌

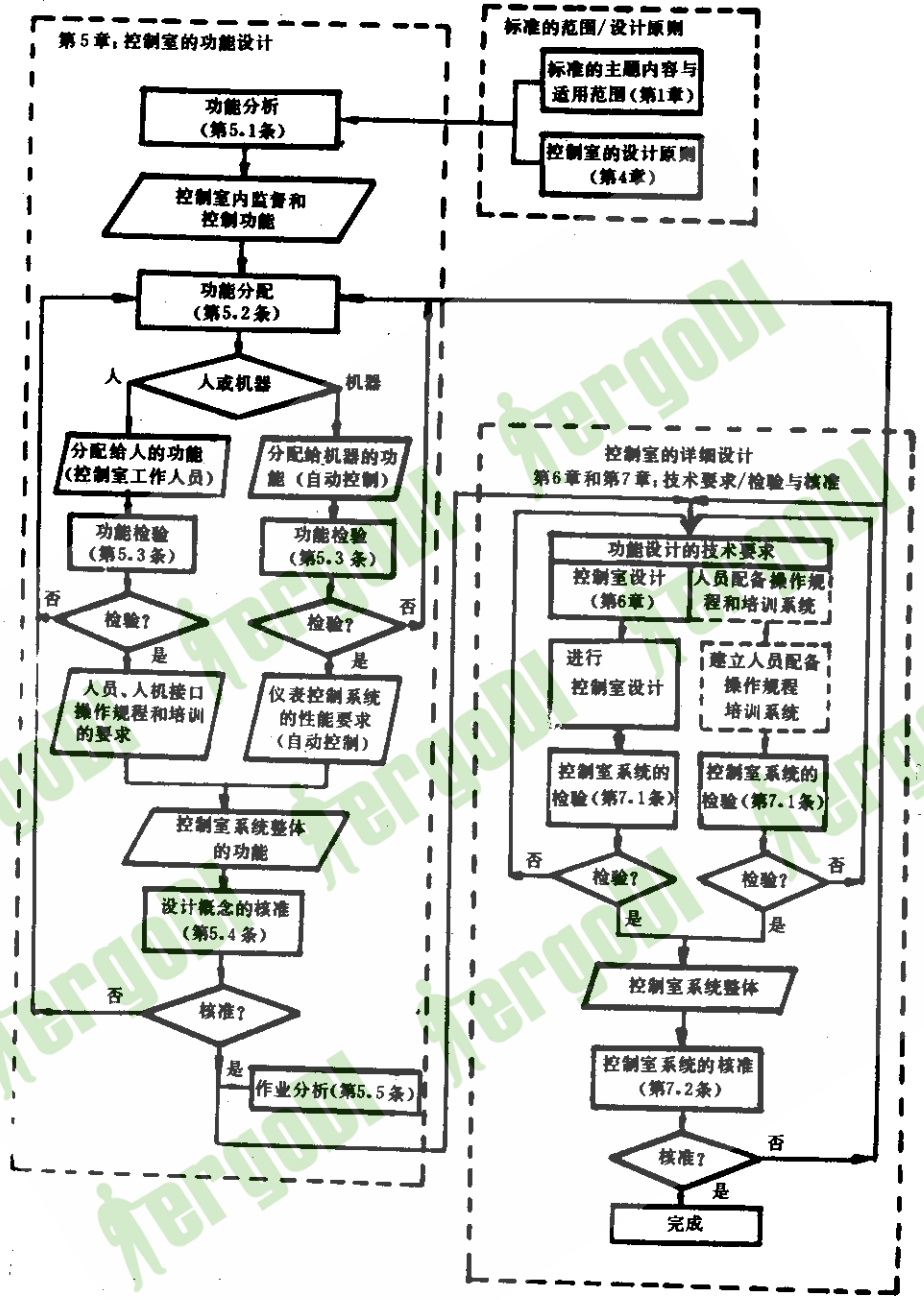

图 2　整个设计过程和标准各章条的关系

5.1 功能分析

为实现 4.1 条规定的目标，并符合 4.2～4.7 条规定的原则，必须对核电厂所执行的功能进行分析。

这一分析应就所有运行状态和事故工况确定控制室设计的目标层次。目标必须包括电力生产和把放射性释放减到最少这两项基本目标。每一目标可以进一步分解成子目标，并用于设计决策过程。

5.1.1 功能的确定

应按照层次目标结构确定与控制室目标有关的全部电厂的功能，并形成文件。附录 A 中的 A5.1.1 给出了确定这些目标的方法。在规定各项功能时，应进行综合性的分析，并考虑控制室和控制室外的设施及系统之间的相互影响。

5.1.2 信息流与处理要求

为了确定完成电厂功能(包括判断与操作)所要求的基本运行信息流与处理，必须进行分析(见附录 A 中的 A5.1.2)。

当确定信息与处理的要求时，设计者应考虑几种有代表性的设计基准事件以及全部正常运行工况，并应包括下列事件：

a. 鉴于数据的解释与控制的复杂性、控制速度等，操纵员难以就要求的操作作出主观判断的事件；

b. 要求操纵员确信无疑地作出正确反应的事件，例如某些事故工况；

c. 在概率风险评价中属重要的事件；

d. 除非及时采取纠正动作，否则很可能导致电厂停机的事件；

e. 出现的概率很高的事件。

考虑的事件数目必须足以覆盖已编入层次目标结构中的各项功能。

5.2 功能分配

设计者必须进行任务分析，以便决定哪些功能应分配给人，哪些功能应分配给机器。

分配给人的功能示于表 A1，它们是：

a. 手动控制，包括自动控制的后备控制；

b. 与手动控制和自动控制两者有关的监督；

c. 高级思维处理任务，例如：诊断异常的和意外的运行工况和事件的起因，并作出纠正动作的决定。

分配给机器的功能指由自动控制所完成的功能(见表 A1)。

在这种分析中，必须应用人因工程原则和设计准则。

用于分析的原则和准则必须形成文件，必须包括论述控制室工作人员和自动控制系统的能力和限度等因素(见附录 A 中的 A5.2.2 和 A5.2.3)。

5.2.1 操纵员的能力

分配给操纵员的功能应分解为：正在执行的控制任务，临视正在进行控制任务的自动系统；进行高级思维处理分析，如诊断。这种分析应导出为完成下述工作所需的信息：

a. 初步拟定的信息系统结构；

b. 为了作出每项决断和执行每项控制任务所需的信息资源的功能组织。

对操纵员可能行使的功能，必须根据工作负担、精确性、速率和时间等因素，按每项信息处理方式和控制动作，作出处理能力的估计。这些估计必须用于功能的初分配。这些估计应根据检验结果予以修改，用于考虑功能的重新分配，并提出对操纵员能力要求的更详细的规定。

这些要求连同显示、控制和通讯的要求，一定要与完成功能必须执行的任务一致。通常的任务应包括显示、控制和通讯的要求。分配的准则见附录 A 中的 A5.2.2。

操纵员可利用的各类数据，必须依据任务的需要编组，而不是依据数据的来源。其目的是按照每项任务组织不同来源的信息，在操纵员的使用能力范围内，为他提供一个综合的信息体系。

5.2.2 仪表控制系统的处理能力

仪表控制系统处理能力的分析，首先必须规定系统和设备的功能要求与限制；随后详述运行事件的顺序和每项任务的人机接口要求。目的是按照人机交互作用所规定的任务，组织机器的信息和能力。

这样组织将便于按每项判断与控制任务来估计自动控制与人工控制两者的能力。仪表控制系统的处理能力最终应包括各项技术指标，例如：系统或设备必须满足数量、响应速度和精度等要求，以及为每类设备而规定的人机接口的人因工程标准。

为减少操纵员出现差错的概率，控制系统应设计成：在电厂异常工况开始之后一个规定的时间内，无需操纵员的动作能保持电厂在安全极限之内。在自动控制系统的功能要求中，必须反映这种时间的要求。

5.3 功能分配的检验

必须检验控制室的功能是否正确地分配给人和机器。检验程序如图 2 所示。应证明所拟定的功能分配最大限度地发挥了人和机器的特长，又没有对人或机器强加不适当的要求。

5.3.1 工作程序

检验的工作程序必须包括准备、评价和判定三个阶段，见附录 A 中的 A5.3.1 和 A5.3.2.1。

5.3.2 检验的基本评价准则

着手检验所拟定的功能分配之前，应证明用于分配的准则自身是一致的。检验必须确认：

a. 完成电厂运行目标和安全目标所需的全部功能已经确定；

b. 所拟定的功能分配符合所建立的分配准则；

c. 每项功能的全部要求已经确定，它们包括性能的各方面（例如：时间限制、精度）。这些要求源自本标准规定的安全原则、可用性原则和电厂营运原则，以及其他标准、法规和导则；

d. 当较高级功能目标产生的要求体现在较低级功能之中时，在所有的运行方式下应没有矛盾。

检验和修改（纠正错误或重新分配）必须反复进行，直至所有准则得到满足。

5.4 功能分配的核准

所拟定的功能分配必须经过核准，以证明系统能完成所有的功能目标。特别在所有正常运行和几种有代表性的事件下，功能顺序的实现必须予以评定。

5.4.1 工作程序

核准的工作程序必须包括准备、评价和判定三个阶段，见附录 A 中的 A5.3.1 和 A5.3.2.2。

必须制定事件选择的准则，以便保证为评定所选择的事件是具有代表性的。除了 5.1.2 条中规定的所有正常运行和事件之外，为评价分配给人的功能，应考虑多重故障所产生的事件。

选出了有代表性的事件之后，确定每个事件所要求的功能，并按时间顺序予以综合。

5.4.2 核准的基本评价准则

必须按所有正常运行和有代表性的事件，评价各项功能的实施。必须满足核准的基本准则，包括：

a. 要求控制室工作人员承担的功能目标的数目和工作负担，必须不超过其能力；

b. 给控制室工作人员和就地操纵员分配的功能是适当的，尤其不应要求他们合作地、相互依赖地执行紧急的或对电厂安全与可用性具有重要功能的任务。

5.5 作业分析

为了进一步制定控制室人员配备结构、操作规程和培训大纲的基本要求，设计者应根据经过检验或核准的功能分配和功能要求进行作业分析。

分析应阐明：

a. 对操纵员的技能要求；

b. 操纵员的操作职责；

c. 操纵员的非操作任务（例如汇报）；

d. 操纵员之间的操作配合；

e. 操纵员与电厂之间的对话；

f. 操纵员与控制室之外的电厂人员的通讯。

以上各项连同功能分配的分析结果(例如初步拟定的信息结构)，应构成控制室工作人员配备结构、操作规程和培训大纲的基础。分析的步骤见附录 A 中的 A5.5。

6 功能设计的技术要求

本章规定控制室系统和监测与控制设备的功能设计要求。本章还规定人和控制室设备之间的接口。

设计必须基于完整的人机系统的工程方法。

6.1 人的能力和特性的基本数据

当实施控制室的详细设计时，必须提供人的能力和特性的基本数据，作为人因工程的基本设计资料。

基本数据应包括：

a. 人体尺度的考虑；

b. 公认惯例；

c. 听觉和视觉的能力与特性；

d. 人处理信息的能力；

e. 环境因素。

附录 A 中的 A6.1 论述如何提供以上数据和这些数据的一些实例。

6.2 控制室的位置，工作环境和防护措施

6.2.1 控制室的位置

控制室必须安排在便于电厂运行的地方，并应满足 4.3 条的安全要求。

6.2.2 工作环境

控制室内的工作环境必须保证操纵员有效地和舒适地执行他们的任务。

工作环境的技术要求必须包括如下项目：

a. 空气调节；

b. 音响环境；

c. 照明条件。

附录 A 中的 A6.2.2 论述工作环境的技术要求。

在工作环境设计中必须采取适当的措施，即使在电厂紧急工况下仍保持控制室的可操作性和监督电厂的能力。

6.2.3 防护措施

控制室的设计必须在设计基准事件范围内对下列事件提供防护措施：火灾、辐射、内部和外部的飞射物、地震和敌意活动。

附录 A 中的 A6.2.3 论述控制室的防护措施。

6.3 控制室的空间与布置

6.3.1 控制室的空间

控制室必须具有足够大的空间，允许控制室工作人员执行全部必需的活动，而且在异常工况下，使操纵员的移动范围最小。

在控制室设计中，必须注意提供工作场地、书写空间，和资料的存放空间，详见附录 A 中的 A6.3.1。

6.3.2 控制室的布置

在控制室的布置中，对下述事项必须给予应有的考虑：

a. 营运管理原则；

b. 分配给操纵员和仪表控制系统的功能；

c. 集中或就地控制的原则，由此决定控制室内有多少控制器；

d. 监视电厂的准则，由此决定控制仪表屏上有多少信息显示设备；

e. 电厂类型和工艺的选择〔不同序列之间的分割，自动控制顺序的使用，仪表与控制器的规格，自动化和(或)多路控制的程度〕；

f. 法定要求和营运单位的要求，例如：由运行方针或许可证发放当局所决定的控制室操纵员的人数。

控制室必须划分为若干操作区，在所有运行和事故工况下，每个操纵员在其操作区内，具有执行任务所需的全部控制器和信息。

操作区的布置和控制室设备(例如控制台、屏和盘)的布置必须符合人因工程原则。

操作区和控制室设备的编组和布置要求见附录 A 中的 A6.3.2.1 和 A6.3.2.2，设备的尺寸和外形要求见 A6.3.2.3。

信息显示设备和控制器的布置必须遵循统一的原则。这些原则应在设计过程中形成文件。

控制室的布置必须使系统与部件的识别，无论在正常运行、事故工况和紧急情况下都很简单，将人为差错引起的误操作几率减到最小。

以上准则可与其他设计要素结合使用。由此衍生的各种规则，所有的操作区都必须一致遵守。

6.4 屏的设计

6.4.1 优先性

属于某个系统的某一功能的报警器、显示器和控制器的布置与排列，以及在控制屏上布置的相似器件之间的优先次序，必须建立一些原则，并予以贯彻。对电厂中的所有控制屏，其规则必须一致。

6.4.2 控制台和屏上的设备定位

在控制台和屏上，显示器、指示器和控制器的定位应依据下列准则：

a. 报警屏和指示器必须从控制室的操作区可以观察到；

b. 频繁使用的控制器必须位于便于触及的地方，有关的指示器和显示器必须从操作位置可以读数。

实例见附录 A 中的 A6.4.2。

6.4.3 镜像布置

为了防止左右混淆，各种屏、控制器和指示器必须避免采用镜像布置。

6.5 布置的辅助手段

6.5.1 显示信息和控制器的编组

显示信息和控制器逻辑地编组是重要的。附录 A 中的 A6.5.1 论述基本的编组方法。

编组必须与使用者的思维方式的规律一致。

必须特别注意避免编组出现矛盾现象，尤其当同时使用几种不同编组技术时，更要精心设计。

6.5.2 编码方法

在控制室设计的初期，必须建立编码原则。

在整个控制室内，编码体系必须是一致的。显示器和它们相关的控制器所使用的编码形式必须完全一致。这个原则适用于位置、信息、颜色和亮度编码。

鉴于各类编码方法的相对优点，在设计中必须确定一种实际应用的编码方法。各类编码方法及其导则见附录 A 中的 A6.5.2。

编码方法应与国内其他核电厂和培训模拟器的编码方法一致。

6.5.3 标记方法

在控制室内必须提供恰当的标记。标记方法必须与电厂中其他标记方法一致，并符合国家的标准和习惯。基本要求见附录 A 中的 A6.5.3。

6.6 信息系统

6.6.1 信息功能

为了向操纵员通告电厂状态以及与安全和可用性有关的重要变量，必须设置信息系统。

在事故工况下，系统必须向厂内和厂外的安全专家提供电厂状态的信息。

系统必须具有数据采集、显示和报警功能。为了分析和向营运机构与管理当局汇报，对安全和可用性重要的电厂过程变量，系统还必须具有记录与记忆功能。

系统还应具有信息处理功能，以支持操纵员的高级思想处理工作，其功能应包括下列各项：

a. 辅助决策；

b. 改善监测的性能和能力；

c. 改善信息的可用性和可靠性；

d. 为操作机构提供反馈信息；

e. 改善控制室工作人员之间的通讯；

f. 为分析目的改善动态过程与事故工况的记录；

g. 扩大现有信息的用途，揭示原隐含的数据。

对信息功能的要求见附录 A 中的 A6.6.1。

信息功能可以由单独的系统提供，也可以作为计算机化的电厂仪表、信息和控制系统的子功能。

6.6.2 数据采集与处理系统

数据采集与处理系统的主要功能要求如下：

a. 系统应设计成：在电厂运行中，系统的故障不引起任何不安全状态或不可承受的经济损失；

b. 输入数据的采样、预处理和分析速率必须适合于有关参数的变化速率的运行要求；

c. 数据更新的速率必须适合操纵员任务的需要；

d. 系统的设计必须考虑：显示系统和报警设备必须提供足够的、可利用的信息，使运行操纵人员能依据管理法规的要求实现安全停堆，并不限期地保持停堆状态；

e. 在系统的整个使用期限内，系统应能修改。

6.6.3 显示系统

鉴于人的能力和特性，显示系统必须作为信息系统的人机接口来设计。

6.6.3.1 对显示系统的主要功能要求

a. 控制室内的显示系统必须包括适当的变量。这些变量必须与安全分析的假设相符，并与正常运行和事故工况中操纵员所需的信息一致。显示器的精度和量程符合安全分析的假定；

b. 为了显示电厂和辅助设施的旁通或人为停运的工况，必须提供指示；

c. 与安全有关的信息显示器置于控制屏上适当位置，并加上特殊的标记；

d. 必须依据不同的显示目的选择显示器的合适类型。显示器的类型见附录 A 中的 A6.6.3。

6.6.3.2 对指示表和指示灯的显示要求

见附录 A 中的 A6.6.3.1。

6.6.3.3 对屏幕显示的主要功能要求：

a. 无论何时需要，都能提供必需的信息供操纵员使用；

b. 显示在屏幕上的信息，必须能被操纵员清楚地理解；

c. 显示必须向操纵员传递期望的和意义明确的信息；

d. 符号应标准化，符号尺寸的大小应受限制；

e. 图形显示中的工艺流向和事件时序的显示符合公认惯例，并与控制室各屏上的模拟图一致。

设计屏幕显示必须依据人因工程和 6.4 条与 6.5 条所述的设计准则，并参考附录 A 中的 A6.1、A6.4～A6.6 的适当要求；还必须与相关的控制仪表和操纵员的理解和认识的要求相容。见附录 A 中的 A6.6.3.2。

6.6.4 报警系统

6.6.4.1 报警系统的技术要求

控制室报警必须提供监视电厂偏离正常运行工况所需的全部信息。

报警系统必须具有：

a. 显示报警信息，使操纵员了解事故发展状态，又不因信息过多使操纵员负担过重；

b. 使操纵员能删去无关的信息，又保证有关的和重要的信息以操纵员易懂的方式显示出来；

c. 使操纵员能区分两种不同性质的报警：操纵员的纠正操作没有结束的报警，没有维修工作的介入不可能消除的报警；

e. 处理功能，向操纵员提供异常工况最有代表性的信息；

f. 显示功能，使得操纵员易于辨别某个报警及其严重性。

此外，为了向操纵员说明报警的可能原因和所需的纠正动作，必须为每个报警提供一份规程性文件，例如报警卡或电厂物项操作规程。

建议使用计算机来辅助操纵员，以便阐明报警信号各种特殊组合的重要性。

附加要求和报警处理见附录 A 中的 A6.6.4。

6.6.4.2 报警的显示

在报警屏或屏幕显示器上的报警显示应满足以下要求：

a. 报警必须显示在控制室中操纵员执行纠正动作的部位上；

b. 任何新出现的报警必须启动音响装置，并使报警指示器上的灯光或屏幕显示器上的标记闪动；

c. 操纵员确认某一报警后，可以手动停止报警灯的闪动；

d. 音响和报警灯的闪动停止后，仍必须有报警显示，以保证报警不被忘记；

e. 当引起报警的原因消除之后，报警显示必须手动或自动地恢复到正常状态。

6.6.5 操纵员支持系统

为提高电厂的安全性、可用性和可操作性，应提供各种操纵员支持功能，例如：安全参数显示与监视功能、电厂诊断功能、基于征兆与基于事件的操作指导功能、功率运行时的自动试验功能。这些功能应尽可能地贯彻到整个控制室设计之中。

6.7 控制器

本条涉及在正常与异常运行中手动操作与自动控制的后备操作所使用的控制器的技术要求和人因要求。电厂仪表控制系统所担负的控制功能的技术要求不属于本标准范围。

6.7.1 人类工效学的考虑

所选择的控制器应适合于操纵员在控制室环境中使用，并与预期的使用人员的人类工效学特征相适应。

控制器的设计必须保证操作简便，并使操纵员的差错最少。

控制器必须满足以下要求：

a. 控制器件的机械特性，例如：尺寸、操作力或操作压力、触觉反馈等，必须满足人体尺度基本数据所规定的人的能力与特性；

b. 为使操纵员差错最少，控制器的动作方式必须符合公认惯例；

c. 对于相同的控制功能，所选用的控制器的颜色、外形和尺寸的编码、控制动作方式都必须保持一致；

d. 控制器的分级必须与它们对安全的重要性相适应。

见附录 A 中的 A6.7.1。

6.7.2 误操作的防止

为防止人为事件，必须设法尽量减少控制器的误操作，措施如：将控制器置于正确位置上，使用固定的保护结构、可移动的盖或挡板、联锁控制器、应用驱动优先性、或以上措施的组合，以及应用人类工效

学原理。见附录 A 中的 A6.7.1 和 A6.7.2。

6.7.3 计算机辅助功能

若有可能，计算机辅助功能应引入控制器，通过顺序的或逻辑的驱动联锁，或以计算机辅助显示系统指导操纵员，帮助操纵员防止误操作。

6.8 控制与显示的组合

为了使控制室工作人员能保证电厂有效地运行，控制器和它们相关的显示器必须正确地组合。

控制与显示设备的组合必须符合按 5.1 条和 5.5 条进行分析后所提出的电厂运行方法。

控制与显示设备的组合必须满足以下基本要求：

a. 控制器应靠近相关的显示器。控制器的操作应在相关的显示器上产生相应的变化；

b. 所采用的控制器形式必须与相关的信息显示器形式一致；

c. 控制器与相关的显示器的编组，必须反映完成系统目标的需要，必须与使用者思维方式的规律一致；

d. 在使用顺序是关键因素的场合下，控制器与显示器的编排必须反映因果关系；

e. 控制器的编排必须体现使用者已经习惯的编组方法；

f. 显示器和相关的控制器所使用的编码形式必须完全一致。

基于计算机系统的显示与控制的组合见附录 A 中的 A6.8.1。

6.9 通讯系统

为促进电厂安全与有效运行，在控制室内必须提供通讯系统。在异常或事故工况下，与应急设施联络的通讯系统的设计，必须给予专门考虑。

为了改善电厂的可用性与安全，在控制室和其他信息中心之间，希望设置非语言的通讯系统，例如：电话传真、计算机之间的数据链。

6.9.1 语言通讯系统

6.9.1.1 厂内通讯

a. 正常运行工况下的一般联络，必须提供分机数目足够的电话系统，控制室电话系统的技术要求见附录 A 中的 A6.9.1.1；

b. 在事故工况下，为了与安全重要的操作设施和辅助控制点的联络，必须在适当的地方安装直通专线电话系统，直通专线电话系统的技术要求见附录 A 中的 A6.9.1；

c. 为了在任何电厂工况下寻找厂内人员，必须提供广播系统；

d. 在维护、试验或修理期间，如果其他通讯系统不能可靠到达的地点，必须提供便携式无线电对讲机，以无线电方式与控制室通讯。

在仪表控制系统的设计、电缆敷设、定位和试验中，必须考虑这种无线电频率干扰的问题。

为了尽量减少这种干扰，必须限制这些无线电设备的频率范围和最大输出功率。

凡不可使用无线电设备的场所，例如控制设备室，必须设置标志。

6.9.1.2 厂外通讯

a. 为了与厂外的营运单位、急救站、政府和公众机关通讯，必须设计一种专用的通讯系统。该系统的类型和规格应按当地的条件确定。某些电话分机的号码，尤其是控制室的分机号码必须保密；

b. 为了与必要的机构和人员能及时联络，必须提供最低数目的电话外线。附录 A 中的 A6.9.1.2 列出这些机构和人员清单。重要的联系必须具有冗余和多样的系统，可以由一个电话系统和一个无线电系统组成。

6.9.1.3 现场的配置

控制室还必须成为正常运行和事故初期的电厂通讯中心。

通讯系统必须依据它们使用期间现场环境的需要来设计。

6.9.2 非语言通讯系统

在控制室内，可以提供非语言通讯系统，例如：监督反应堆操作平台和汽轮发电机组状态的电视系统、电话传真系统和计算机的数据链（控制室和信息中心之间）。在紧急情况下，数据链还应能接通应急设施。见附录 A 中的 A6.9.2。

6.10 其他要求

6.10.1 计算机的利用

为提高人机接口能力而设置的计算机必须满足以下要求：

a. 计算机系统的故障必须不损害电厂安全功能；

b. 计算机系统必须设计成：不因计算机的单一故障引起或要求电厂停机。必须精心设计，将共因故障的后果减到最小；

c. 初次安装之后，应易于实现硬件与软件的修改，见 6.6.2 条；

d. 设计应考虑计算机硬件与软件都易于检验和核准；

e. 计算机系统应具有适宜的运算速度，足以执行必要的功能，在屏幕显示器上显示的信息应满足人因工程要求。

在控制室内，包含在仪表控制系统、显示系统和操作员支持系统的综合运行系统中的计算机部分，可以只由一个计算机系统组成，但在这种情况下，必须采取充分的措施，防止因计算机故障或运行错误产生共因故障。

为了提高系统的可靠性和可维护性，对于重要功能，希望使用一种具有分级和局部冗余结构的分布式系统。

6.10.2 电源

控制室的电源装置必须具有与仪表控制系统、安全系统以及安全有关的系统同等的可靠性与可用性。在控制室内，对安全重要的系统必须由不间断电源供电，因为正常运行和事故工况下，要求这些系统任何时候都是可用的。

6.10.3 质量鉴定

为了证实控制室中与安全有关的设备和系统，在需要它们运行时可能出现的特殊环境下能连续地满足设计基本性能要求（例如：量程范围、精度、响应），必须制定一个鉴定大纲，并按此大纲进行鉴定。该大纲必须包括保证设备适合于规定的使用寿期的计划，如必要的话，还应提出及时再检验或更换的要求。

6.10.4 可维修性

设备必须设计成便于监视与维修，在出现故障的情况下，易于诊断和修复，或易于更换。

在设计阶段必须估计修复时间对可用性的影响。在每个具体系统的设计依据中必须规定修复的平均时间和检查的频率。探查已发故障的方法，例如功率运行时的系统检查（试验），应是这种估计的一部分。

系统维护的方法对电厂安全的任何影响必须是可接受的。

6.10.5 修理

控制室的设计要考虑控制屏的布置和设备的外形，必须使其里面的系统和设备易于修理。设计还必须考虑修理设施和备品备件。

6.10.6 可试验性

控制室必须设计成：在需要的时间间隔内，每项必需的功能允许无困难地进行试验与校验。

7 控制室系统的检验与核准

在整个控制室系统（包括控制室工作人员的配备、人机接口、操作规程和培训大纲）的初步设计完成之后，必须检验与核准控制室系统的设计是否适当。本章规定控制室人机接口检验与核准的工作程序和基本评价准则。有关控制室人员配备结构、操作规程和培训大纲的评价，其工作程序和准则应参照有关

标准和导则另行规定。

7.1 控制室系统的检验

在控制室系统设计的这个阶段，检验是一项通常的设计评审，是质量保证程序的一部分。这种设计评审的目的是保证功能要求和其他技术数据正确地体现在控制室系统初步设计之中。

7.1.1 工作程序

检验的工作程序必须包括准备、评价和判定三个阶段。

在这个阶段所进行的评价，必须包括已分别提供的操作规程和培训大纲，如图 2 所示。

参见附录 A 中的 A5.3.1 和 A5.3.3.1。

7.1.2 控制室系统检验的基本评价准则

控制室系统整体必须正确地贯彻全部功能要求和所有其他技术要求。

设计必须满足下列准则：

a. 人机接口的功能技术要求必须满足设计准则及有关的管理条例、标准和导则，必须正确地贯彻在控制、显示和其他控制室设备与设施的设计之中；

b. 培训必须使操纵员能获得对人机接口的功能和操作规程的正确了解；

c. 培训大纲必须正确地体现操作规程。

7.2 控制室系统的核准

在控制室系统的详细设计之前和之中，控制室系统整体必须经过核准，以证明能完成期望的性能，必须特别注意控制室系统整体随时间变化的动态性能。

7.2.1 工作程序

核准的工作程序必须包括准备、评价和判定三个阶段。详见附录 A 中的 A5.3.1 和 A5.3.3.2。

核准的准备工作用类似于功能分配核准的方式(见 5.4 条)进行。在此阶段中，运行经验是特别重要的。

为了评价控制室系统随时间变化的动态性能，应制作一个适当的控制室模型。对于其设计原理与已有的常规系统有明显差异的系统，最好用动态模拟器进行核准。当与现有系统的差异甚小或局部核准就能验证时，可以采取其他方法，例如全尺寸的模型。

为了便于多重评价，应设置多重的性能测量。相互有关的性能测量，必须检查定性与定量两者的一致性，以便确认评价的结果。

在估价各种环境因素的影响方面，必须考虑单个因素和多种因素的切合实际的组合。

为了尽量减少设计缺陷，核准大纲应包括调试实验的要点。

评价的准则必须与所有有关的管理条例、标准和导则等一致。

7.2.2 控制室系统核准的基本评价准则

为了评价人机接口与控制室其他组成部分(控制室人员配备、操作规程和培训大纲)之间以及人机接口自身的相互影响，必须制定准则。详细的相互关系见图 1。

评价准则如下：

a. 分配给控制室工作人员和自动装置的各项功能，其组成的功能顺序必须是彼此一致的和完整的；

b. 在功能要求中所陈述的操作原理必须一致地用于所有的控制功能，使得具有相似操作特性的各子系统，能相似地操作；

c. 分配给控制室工作人员的任务，必须在人的能力限度之内。要求快速、缓慢或复杂的控制与信息处理任务，不应交付给操纵员；

d. 为适应人的本能差异，必须给操纵员留有足够的裕度(例如时间限制)；

e. 在视觉、听觉、触觉和振动等方面，操纵员的敏感能力必须在公认的限度内；

f. 对操纵员在操作中的移动、伸展、操作、体力和耐力等方面的活动能力的要求必须在公认的限

度以内；

g. 操作员的思维处理负担必须在他们的能力变化限度内。在信息处理、感觉、信息记忆的持久力(短期和长期)和记忆的容量(短期和长期)等方面，由于警觉与疲劳程度不同，其能力亦随之变化；

h. 在异常的温度、湿度和压力、异常的照明(照度、对比度、眩光等)、控制室内异常的噪音和声学特性、有毒物和辐射等条件所表征的实际工作环境下，操纵员的工作负担必须在他们的工作能力内；

i. 分配给每个操纵员的任务必须是能完成的，工作负担不超过公认的正常操纵员的能力限度；

j. 在各种运行状态和状态变化过程中，操纵员执行其任务所需的全部信息必须容易观察到，并必须提供所需的控制设备。在手动控制情况下，必须向操纵员提供有关真实系统行为的适当反馈信息；

k. 如果规定使用屏幕显示，信息必须易于搜索。同一时刻所需的不同变量的信息，只要可能，必须同时显示在同一个屏幕显示器上。显示系统应具有足够大的显示面积和分辨率，便于稳定而清晰成象。键盘和其他操作设备应使信息系统简单而可靠地操作。显示格式应符合公认的标准。显示给操纵员的信息必须清晰易懂；

l. 操作规程必须与人机接口和预期的电厂响应的要求相容，必须包括控制室所执行的全部预期的任务和功能序列。操作规程的陈述必须是正确的、完整的和一致的，并易于解释；

m. 人机接口系统必须能向控制室外的设施提供所要求的信息；

n. 培训大纲必须与操作规程和人机接口的要求相容，必须为操纵员提供电厂安全与可靠运行所需的技能与知识，包括处理非预期事件；

o. 控制室人员配备必须与安全和可靠运行的要求一致，并与操作规程和培训大纲两者相容；

p. 控制室工作人员和就地操纵员以及位于控制室之外的电厂人员之间的通讯必须方便；

q. 必须证明操纵员支持系统能提高操纵员的能力，不会产生可能干扰操纵员进行决断(例如监察和高级思维活动)的副作用。

附 录 A
核电厂控制室设计导则
（补充件）

A1 附录的范围与目的

A1.1 范围

本附录是一份导则，它提供控制室设计中所需要的、标准正文中没有包括的补充资料。

A1.2 目的

控制室设计标准规定了控制室设计的主要依据，但仅限于设计的基本要求。本附录的目的是提供补充资料，包括控制室设计的原理与方法的要点、详细的建议和技术要求。

A2 应用

核电厂控制室设计标准适用于标准公布之后开始设计的新控制室。如果希望本文用于现有的电厂或设计，必须特别慎重考虑本标准所假定的因素，例如自动化水平。

A3 标准中所使用的概念和术语

A3.1 控制室系统

人机接口、控制室工作人员、操作规程、培训大纲和有关的设备与设施的总体称之为控制室系统，图1中粗实线包围的部分。

控制室系统各组成部分的功能和相互关系详细说明如下：

电厂有两个基本的运行目标：发电和防止向环境释放放射性物质。为达到电厂的运行目标，必须实现许多功能目标。为此要有控制地利用电厂设备（例如机械系统）来控制（“控制”指控制与保护）电厂的工艺过程。

本质上，控制电厂系统有两种方法：自动控制和手动控制（远距离和就地手动控制）。实现自动控制和远距离手动控制的硬件系统称为电厂控制与安全系统（仪表控制系统的一部分），它们包括驱动器、探测器和其他硬件设备。

自动控制的运行要求控制室工作人员通过显示器监督其执行情况。必要时采取手动控制，包括自动控制的后备控制、复原等。

远距离手动控制的运行要求控制室工作人员通过安装在控制室内的控制与显示设备进行干预。

控制和显示设备（也属仪表控制系统的一部分）与控制室工作人员具有一种实体交接面，如图1所示，所以它们被称为人机接口。

就地手动控制是在控制室工作人员要求下，由就地操纵员通过就地的控制设施来执行的控制。控制室工作人员的指令通过通讯系统下达。

除了自动控制、手动控制和相应的监督（指简单的任务如水位检查、状态检查）之外，要求控制室工作人员进行信息的高级思维处理，例如：多重读数的解释，基于知识形成对策。

为了帮助高级思维处理，开发基于计算机的操纵员支持系统。有各种类型的操纵员支持系统可以利用，例如：诊断系统、运行咨询系统、规程综合装置。

控制室工作人员可以按各种各样的方法同这些系统联系——从通过显示器进行简单的单向信息检索，到通过适当的装置进行高水平的双向通讯。操纵员支持系统被归类为人机接口。

与控制室外的电厂人员和管理工作人员的通讯，可以通过通讯接口实现。

A3.2 人和机器

给机器分配的功能指用自动方法完成的功能。因此，在功能范畴中的“机器”代表自动化。而在功能范畴中的“人”代表控制室工作人员。给人分配的功能指由手动控制、监督、高级思维处理或它们的各种组合所完成的功能(见表 A1)。

“机器”指的是硬件实体，它包括仪表控制系统和操纵员支持系统。应该注意，属于仪表控制系统部分的手动控制系统、控制器和显示器，使控制室工作人员能完成分配给他们的功能。

在标准中规定的项目表示在表 A2 中。

表 A1　功能范畴和实体范畴中的人和机器

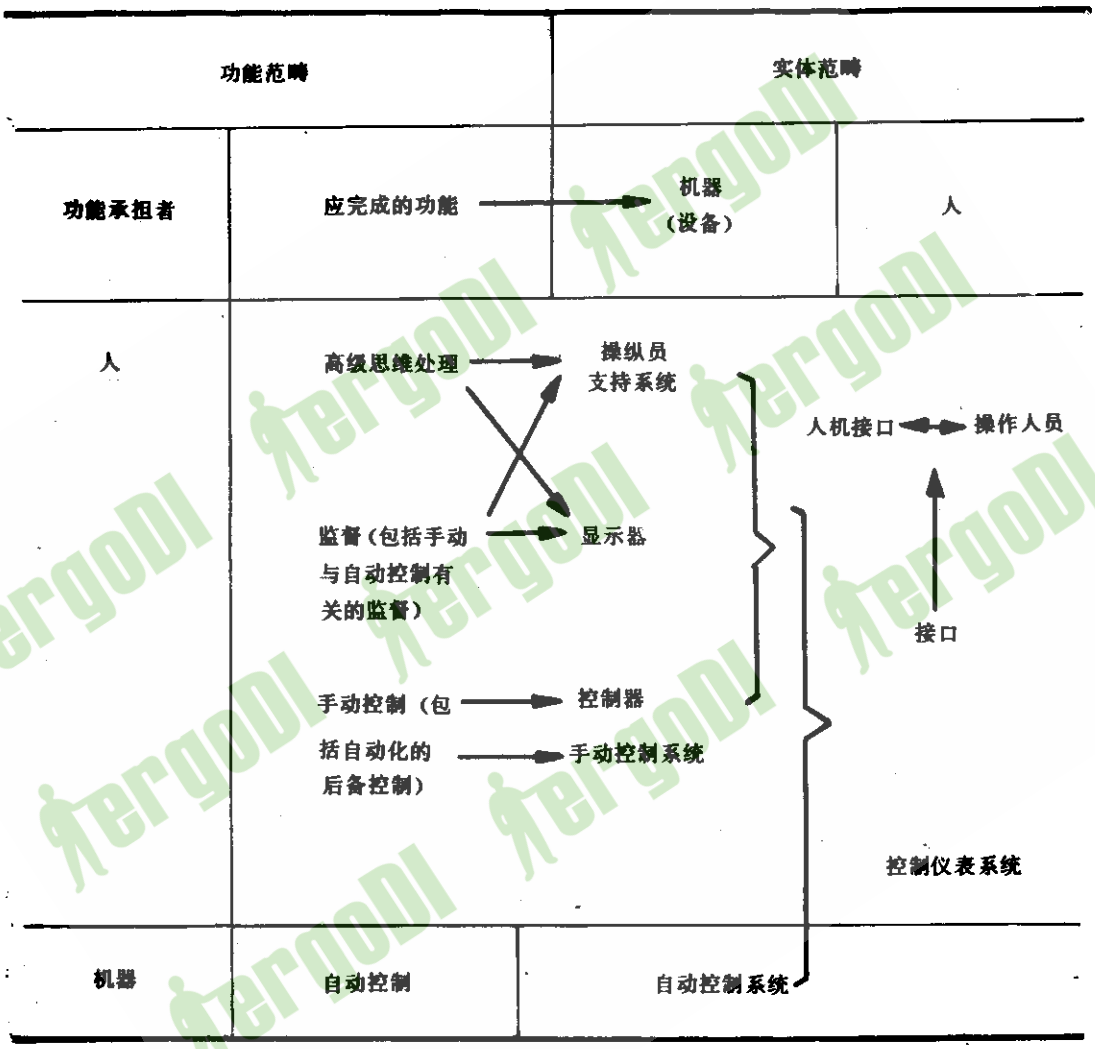

表 A2 标准中规定的项目

项　　目	标准中的要求	标准的检验与核准的准则
功能范畴		
(1)人和机械	5.1 和 5.2 条	5.3 和 5.4 条
(2)远距离控制和就地控制	5.1 和 5.2 条	5.3 和 5.4 条
(3)操纵员支持系统支持的功能或任务	5.1 和 5.2 条	5.3 和 5.4 条
(4)操作规程、培训大纲和控制室工作人员结构准则	仅接口要求	仅接口要求
实体范畴		
(1)仪表控制系统的功能设计	不属本标准范围	不属本标准范围
(2)人机接口的功能设计	第 6 章	7.1 和 7.2 条
(3)操作规程、培训大纲,控制室工作人员结构	不属于本标准范围	7.1 和 7.2 条中的控制室系统

A4 控制室的设计原则

标准正文第 4 章中规定了控制室设计原则。在安全方面还需符合核安全法规 HAF0200 的规定。

A5 控制室的功能设计

A5.1 功能分析

A5.1.1 功能的确定

如 5.1 条中规定,功能分析从制定层次目标结构开始。

由于电厂的最终目的是按需发电(可用性目标)和防止向环境释放放射性(安全目标)。以上两项是放在所制定的层次目标结构顶端的目标。

A5.1.1.1 设计者应首先将这些目标中的每一项分解为若干子目标。

可用性目标有四项子目标:

a. 使电厂达到功率运行状态(启动操作,最初的功率提升);

b. 在各种正常运行方式下,控制核蒸汽供给(例如,稳定功率运行,负荷跟踪运行等);

c. 把蒸汽能转换为电能,使电厂具有最高可能的效率和可用性;

d. 停堆与换料。

A5.1.1.2 设计者还必须确定每一项子目标的基本功能。这些功能通常叫做重要的可用性功能,因为,这些功能的丧失将改变功率运行的持续性,从而影响电厂的可用性。

例如,上述 b 项子目标(核蒸汽供给的控制)可以分解为以下各项基本功能:

a. 控制核功率;

b. 控制中子注量率分布;

c. 控制主冷却剂装载量;

d. 控制堆芯热量排出;

e. 控制热阱;

f. 控制汽轮发电机系统;

g. 保持反应堆冷却剂系统性能。

A5.1.1.3 为了安全目标，实现防止放射性释放，一般设置三道屏障：燃料包壳、反应堆冷却系统的边界和安全壳。操作规程的目的是保持这些屏障的完整性，以便达到事故工况下的安全目标。然后，设计者确定那些保持屏障完整性的基本功能。

最基本的重要安全功能如下：

a. 控制反应性在临界以下(维持次临界)；

b. 维持主冷却剂装载量；

c. 维持堆芯热量排出；

d. 维持热阱；

e. 维持反应堆冷却剂系统的完整性；

f. 维持安全壳的完整性。

在事故工况中，这些功能的丧失可以导致电厂状态严重恶化，危及电厂安全。

注：虽然甩负荷不是正常运行工况，但在 A5.1.1.1b 项子项目标(核蒸汽供给的控制)之下应予以考虑。

在确定重要的功能(即重要的安全功能和重要的可用性功能)之后，设计者可以开始分解每项重要功能。

例如：对于压水堆，A5.1.1.3a 项确定的重要功能，可以分为如下子功能：

a. 保持所有控制棒完全插入堆芯；

b. 维持足够的化学毒物控制液的浓度。

设计者应继续分解，直到不能再分解为止。但是，在已获得详细的子功能和已确定系统的重要组成部分的情况下，分解也可以终止。

最终的层次目标结构应该是：概括的高级功能在顶部，系统级的功能在中间，具体设备或部件级功能在底部。

A5.1.2 信息流和处理要求

A5.1.2.1 功能分析的下一步是为前一步中所确定的每项功能确定所需的信息和信息处理要求。

对每项功能，设计者应确定下述各项：

a. 指示功能状态的可观察参数；

b. 完成功能所要求的控制过程和性能测量；

c. 如何确定功能在正确执行；

d. 如果功能不能正确执行，可用哪些替代功能，如何选择替代功能。

替代功能指能够替代被分析的功能、支持高一级功能的功能。例如，依据电厂的工况，应有几种冗余的热量排出的途径可供选择。

在这个阶段，上述方法应是通用的，不涉及特殊的措施或人员干预的水平。

A5.1.2.2 为了保证功能实现所进行的性能测量，有时需要利用设计基准事件下的信息。直接的物理方法是开展性能测量的理想方法。例如，堆芯热量排出的性能测量中的一个值，可以由燃料包壳所使用材料的知识(熔化温度)来决定。但是，不是所有的性能测量都可以用这种方法来决定。有时性能测量不得不依赖于事故分析所获得的信息。选择事件的导则在 5.1.2 条中已作了规定。

虽然每个设计者应根据他的设计目的确定一组有代表性的事件，但如下事件可作为一种典型的选择：

a. 与安全有关的：失水事故、主蒸汽管道破裂、给水管道破裂(压水堆)、蒸汽发生器换热管断裂(压水堆)和全部交流电源丧失；

b. 与可用性有关的：控制系统的传感器故障(例如，压水堆的给水控制系统)。

设计者应该选择能够覆盖被分析的各种功能的事件。设计者应知道某个功能的丧失相当于某一事件的发生，并能看到它如何沿着层次结构从底部向顶部扩散，影响较高一级功能。

A5.2 功能分配

功能分配由三个阶段组成:任务分析、制定分配的准则和分配。

A5.2.1 任务分析

设计者使用功能分析(信息流和处理要求)中制定的基本数据进行任务分析。这种任务分析的目的是为了确定任务的详细内容和它的特性要素。

A5.2.1.1 设计者应将密切相关的各子功能组合为一体,以便将它们作为一个单元来处理。它们也可以具有层次结构。这样的单元可以分成两类:

a. 功能单元的共同实现是完成较高一级功能的基本条件;

b. 功能单元是较高一级功能的替换的支持功能,它们的实现不一定是较高一级功能的必要条件。

A5.2.1.2 对于组合体中的每一项子功能,设计者应确定以下内容(即任务的内容):

a. 要求它实现的逻辑(为什么要求它实现?);

b. 实现它所需的控制动作(怎样才能实现?);

c. 控制动作所需的参数;

d. 评价控制动作结果的准则;

e. 评价所需的参数;

f. 评价准则;

g. 选择替代功能的准则。

应该注意,以上被确定的参数组形成参数编组的依据,它也构成显示和控制设备布置编组的依据。

A5.2.1.3 设计者应该确定各项特性要素,并为每项要素规定几个等级。特性要素应是客观的(例如:时间,速率),但可以包括主观评估的值,还应包括某些为作出决断所需要的定性要素。设计者应考虑以下特性:

a. 工作负担;

b. 准确性;

c. 时间因素(例如:速率、时间裕度和限制);

d. 动作逻辑的复杂性;

e. 作判断的类型和复杂性(例如,模式识别);

f. 由于功能丧失和相关的时间因素所产生的后果。

为确定有关的特性要素,设计者可请教心理学专家以及系统设计者。然后,设计者参照全部特性要素将每项任务进行分级。

A5.2.2 分配准则的制定

与任务分析并行,为了在人和机器、远距离手动控制和就地手动控制、操纵员支持系统之间进行功能分配,设计者应为功能分配的决策制定分配准则。

准则的基准与特性要素的基准必须是一致的。

A5.2.2.1 人和机器功能分配的准则

给人和机器分配功能的准则应主要依据下列特性因素:

a. 工作负担;

b. 准确性;

c. 时间因素;

d. 操作逻辑的复杂性;

e. 作决断的类型和复杂性。

准则的基本结构表示在表 A3 中。

表 A3 人和机器的功能分配基本结构

特性因素	分配	
	人	机器
工作负担	中等	高,很低
时间裕度	大	小,很大
速率	中等	高,很低
控制逻辑的复杂性	简单的	复杂的
进行决断的类型和复杂性	不良	良好

A5.2.2.2 远距离和就地手动控制功能分配的准则

给远距离手动控制和就地手动控制分配功能的准则应主要依据下列特性要素:

a. 时间因素;

b. 由于功能丧失和相关的时间因素所产生的后果。

要求很快完成或时间上要求较严和后果严重的功能应不用就地控制。

A5.2.2.3 操纵员支持系统功能分配的准则

给操纵员支持系统分配功能的准则应主要依据下列特性测量:

a. 在限定的时间裕度下,决断的复杂性;

b. 对电厂安全和可用性来说,决断的重要性;

c. 在决断活动(例如,诊断、监督和高级思维处理)中,提高操纵员能力的必要性。

A5.2.3 分配

设计者可以通过分级的特性要素与分配准则的比较,进行功能分配。如标准正文规定,功能分配一直持续到在检验与核准中证明无设计缺陷为止。

A5.3 功能分配和控制室系统的检验与核准

A5.3.1 检验与核准的共用条款

给人和机器分配的控制室功能和控制室系统的整个设计都按图 2 所示进行检验和核准。

A5.3.1.1 工作程序

检验和核准的工作程序应包括以下几个阶段:

A5.3.1.1.1 准备

准备应包括鉴定原始文件,制定评价准则,组建评价工作组和拟定评价计划。对于文件的完整性和评价工作组的独立性应予以特别注意。

准备工作还应包括为核准选择典型事件和综合功能顺序。在控制室系统的核准中,运行经验是特别重要的。此外,评价工作组应该具有必要程度的多学科性。

A5.3.1.1.2 评价

评价必须是系统的,它的工作程序必须按便于追溯的方式形成文件。分配给人的功能和分配给机器的功能评价应按图 2 所示进行。

A5.3.1.1.3 判定

在评价中鉴别出来的任何错误必须分别地反复地加以纠正,直至功能要求满足全部评价准则。如果在检验或核准中发现了任何不适当之处,必须进行分配准则的修改或功能的重新分配,按图 2 中所示的

反复路线进行。

如果发现了重大缺陷，判定工作应细致地进行并作记录，使得那些在先前的评价中已认为是适当的设计概念不受有害的影响。在任何情况下，如果控制室系统总体做了修改，核准工作必须重复进行。

A5.3.1.2 评价工作组

对于评价工作组，主要有两项建议：

A5.3.1.2.1 工作组应与从事初始功能分配或控制室系统总体设计的设计者无关。但无需阻止同这些设计者的联系；相反，他们应可以参与讨论和说明。

A5.3.1.2.2 工作组应包括相关的学科，下列专家应包括在内：

a. 核工程；
b. 建筑设计与土木工程；
c. 系统分析；
d. 仪表控制系统；
e. 信息与计算机系统；
f. 人因工程；
g. 运行经验与培训。

为保证提出的要求都是实际的，需要运行经验。为保证有效的工作，工作组成员的数量应该少。问题涉及到评价工作组没有包括的技术范畴时，必须通过求教于工作组以外的专家来解决。

A5.3.2 功能分配的检验与核准

A5.3.2.1 功能分配的检验

如标准正文规定，设计者必须验证功能分配的完整性。应该注意，只有在核准工作中（而不是检验工作中），设计者才能对功能分配的正确性作出评估，判断它能否保证人和机器的最佳效能。

A5.3.2.2 功能分配的核准

在功能分析中所制定的层次目标结构，本质上是以静态的数据为基础的。根据为各功能所规定的性能测量，设计者能知道每项功能怎样才能实现或不能实现。但是，在某特定事件期间一系列功能如何动态地实现还不很清楚。丧失某项功能引起的事件的影响沿层次结构以多快的速度传播，是否影响较高一级功能，取决于事件的类型和它的规模。核准的主要目的是分析层次体系随时间变化的特性，以保证功能分配的适当性。

A5.3.3 控制室系统的检验与核准

控制室系统检验与核准的前提是：依据标准正文第5章制定的、经过检验与核准的功能要求已作为设计的输入，并贯彻在控制室制造和建造的详细技术条件中；在设计工作中已考虑了标准正文第6章中给出的准则与建议。

在这个阶段，控制室作为一个设计存在，它体现为详细的图纸和技术条件。至少在原则上，检验与核准工作的目标是：在制造过程开始之前，检查技术要求。事实上，因为工程项目的不同部分之间的进度不同，检验与核准过程可能延续一段时间。

控制室的检验是对照适用的功能要求和设计要求与准则，来评价所提出的设计技术要求。

控制室系统的核准是评价控制室、操纵员、操作规程和培训大纲之间的互相作用，以便保障电厂的安全与可靠运行。

A5.3.3.1 控制室系统检验

当正式制定检验准则时，使用两个主要的资料来源：依据第5章所制定的实际控制室的功能要求和第6章中给出的控制室设计所应用的规则和准则。

根据这两个来源所制定的准则，应包括技术方面以及人因工程方面。

这些准则用于证明正确的人因工程原则以及所需的技术能力都已贯彻在控制室设计中。

检验准则的典型实例是：

a. 在控制室内提供的仪表与显示设备必须表达有关的过程参数；

b. 控制与显示设备必须按一致的和有序的模式排列；

c. 出了故障的仪表和显示设备必须易于识别；

d. 操作区的布置应使到达控制屏的通路不受阻碍；

e. 必须提供适当的温度、湿度和通风控制设备；

f. 控制设备的布置应使有关的显示器能提供反馈信息。

A5.3.3.2 控制室系统核准

控制室系统核准的目标是：评价控制室系统各部分之间的相互作用能否使控制室系统以电厂安全与可靠的运行所要求的方式运转。在本标准中，核准的范围限于三种可能的相互作用即：控制室与操纵员、控制室与操作规程、控制室与培训大纲。

A5.3.3.2.1 核准的范围

鉴于在设计的这个阶段，控制室以及操作规程和培训大纲是以图纸和技术条件的形式存在，因此核准的范围一定会受到限制。

A5.3.3.2.2 核准用的脚本

脚本是一份说明书，它描述适合于核准方法所选择的运行工况。这种脚本必须真实地反映电厂的情况，必须包括正常运行、多重故障事件加上干扰的混合工况，以及应急工况。脚本必须描述初始条件，电厂响应的正确顺序和可应用的征兆。必须给出电厂运行预期的发展途径，以便编写需要使用的评价准则。

A5.3.3.2.3 核准方法的选择

核准控制室系统可利用的方法是：

a. “圆桌”法：包括对所提交的脚本，按其程序的步骤，逐步进行深入的讨论；

b. 排演法：按照所提供的脚本，以人当作操纵员，为评论组进行一步接一步的程序操作表演，而不实现真的控制功能。排演要准备一个模型。最简单的模型是一个房间，在房间的墙上悬挂控制屏的图纸；

c. 模拟器法，在所提供的脚本指导下，以人当作操纵员，当着评论组面，在模拟设备上执行真实的控制功能。

这些核准方法可以按核准范围使用不同组合。例如，用“圆桌”法和排演法核准时，对于包含有随时间变化的参数的场景，可以用专项功能模拟机或其功能局限于某一方面的模拟机来演示。

A5.3.3.2.4 评价准则

在核准控制室系统总体时，设计者必须制定具体的评价准则。

A5.3.3.2.4.1 控制室与操纵员的评价准则

a. 规定的光字牌、仪表或电厂显示器作为提示信号，能否足以提醒操纵员执行所需的操作；

b. 控制器是否便于接近，显示设备是否易于读数；

c. 仪表和控制器的铭牌是否足够详细，允许操纵员不借助于其他文件能找到所需要的屏和控制器；

d. 是否提供了指示，允许操纵员确定某个工序已经完成或某个工况已实现。这种指示是否能提供满意的信息；

e. 当基本的提示信息、控制器和指示器不可用时，为完成规定工序，是否还有其他手段；

f. 如果操纵员希望当某个过程参数达到某个数值时采取某项操作，该参数的测量仪表能否清晰地读出该数值；

g. 按刻度与时间分辨能力，全部仪表的刻度与量程是否适合所要求的读数精度。

A5.3.3.2.4.2 控制室与操作规程的评价准则

a. 能否按规定的顺序执行规程中规定的操作；

b. 是否有替代的有效途径没包含在被评审的规程中；

c. 在控制室内和规定的时间内，能否完成规程中规定的动作；

d. 从控制室内所指定的仪表中，操纵员能否获得规程中所要求的必需信息；

e. 为了操纵员选择适用的规程，指定的仪表与显示设备能否提供足够的信息；

f. 操纵员为完成他的任务，是否必需使用规程中没有规定的信息或设备；

g. 控制室中显示的电厂工况是否与规程中描述的同一工况一致；

h. 操纵员能否按提供的标记、缩写、符号和地址信息找到正确的设备；

i. 仪表的量程是否与规程中说明的测量数值一致；

j. 规程的使用是否把过重的负担加在操纵员的记忆上；

k. 应急操作规程是否容易与控制室内的其他规程区分出来(颜色、外形、位置)；

l. 规程与控制室是否实体上一致；

m. 控制室的不同部位是否有可供放置规程的地方，订成册的规程是否允许将它们打开平放在工作位置上；

n. 为方便使用，装订成册的规程是否太大或太重。

A5.3.3.2.4.3 控制室与培训大纲的评价准则

a. 借助可利用的控制与仪表设备，是否能安全与正确地运行电厂所有的系统和设备；

b. 是否会由于对任一电厂系统或设备缺乏了解而产生不正确的操作；

c. 根据光字牌的指示，能否采取应有的操作；

d. 从控制器和仪表来的信息是否会被误解；

e. 控制器和仪表能否引出错误的结论；

f. 培训是否用来弥补控制室或规程的设计缺陷。

A5.4 仪表控制系统的检验

虽然仪表控制系统的验证与核准不属本标准范围。但给出如下评价准则作为参考：

A5.4.1 总的方面的检验

以下各点应予检验：

a. 仪表控制系统各方面的技术要求，最终必须是相互一致的，并符合有关安全、可靠和自动化水平的设计基本原则；

b. 对系统试验和试运行所需设施的要求必须包括在功能要求之中；

c. 可维修性的要求必须形成文件，并与可用性的要求一致；

d. 所拟定的仪表与控制功能的灵活性与适应性的要求，必须能满足使用者设想到的今后的变化；

e. 分配给仪表控制系统的功能必须与工作环境相容。操纵员必须不遭受过高的温度、噪音、有害物质、放射性等侵害，必须避免应用冗长的工作顺序或过重的体力强度。

A5.4.2 自动化方面的检验

必须检验下列各项是否适当地实现了。

A5.4.2.1 给仪表控制系统分配的功能应与一定的自动化水平一致。自动化水平(包括控制、保护、联锁、显示、记录、数据管理、通讯以及不同的运行方式和方式的转换)必须符合避免操纵人员负担过重工作的目标。

自动化水平必须依据人的能力限度来选择。例如，人没有能力控制很快的、很慢的或很复杂的过程。人受记忆力的限制，在不可接近和(或)距离较远的情况下，必须检验系统远距离操作的可能性。

A5.4.2.2 对于每个子过程、子过程之间的相互作用、运行状态和状态的转换，若其运行速度和(或)精度方面的功能要求要人来满足是困难的，则必须选择自动控制的方法。

A5.4.2.3 为改善可用性和生产力，提高发电质量与发电能力而采用自动控制的方法，应证明是正确的。而且，对测量的速度、精度与数量、工艺过程与装备设计以及操纵员的任务不得强加不可能的要求。这些要求不得迫使违背设计所依据的原则。

A5.4.2.4 必须尽可能提供足够的仪表和控制设备，以便允许操纵员安全地处理那些自动功能既不可指望也无能力处理的事件。

A5.4.2.5 在有关安全的自动化设备的要求方面，可用性的技术要求必须完全满足审批当局和营运单位的安全管理规则，并是可行的。

A5.5 作业分析

如 5.5 条规定，作业分析的目的是确定控制室工作人员结构，操作规程和培训大纲的基本要求。

作业分析的第一步是确定分配给人的任务的特性和数量；然后，设计者可以在管理条例和(或)营运单位的正常实践经验所要求的控制室工作人员结构体制内，规定操纵员的数目和结构。

可能使操纵员的工作负担过重或超出人员结构所规定的职责与范围的任务，必须不分配给操纵员。接着，设计者可以确定操纵员之间的通讯和(或)控制室操纵员与就地操纵员之间的通讯。

设计者还可依据相应文件给操纵员确定为完成某些任务而需要完成的非操作活动(例如，向主管当局作报告)。这些因素形成操作规程和培训大纲的部分依据。

A6 功能设计的技术要求

本章为第 6 章提供补充资料，包括详细的推荐意见和某些数据，帮助进行人机接口和设备的设计，并提供控制室系统的详细技术要求。

A6.1 人因工程主要的设计数据

A6.1.1 人体尺度的考虑

在人机接口设计中，人体尺度的考虑占有中心地位。在设计中，这种考虑的失误，可能损害系统的性能、操纵员的安全、或机器的可用性。

a. 为控制仪表屏、盘和设备的设计，必须建立人体尺度的基本数据。可以采用现有的基本数据，但在应用之前，必须针对人员的具体情况检查数据的适用性；

b. 人体尺度的基本数据必须构成控制与相关设备的尺寸和形式的具体要求的基础；

c. 以上设计参数的大小和最终的伸展半径、观察距离、观察范围和观察角的大小，必须在 90%的使用人员可接受的范围内；

d. 为制定设备尺寸的限定值，表 A4 列出了人体尺度的数据。

表 A4 人体尺度数据(站立和坐着)的实例

	数值极限 cm	
	最低限制值 成年女性	最高限制值 成年男性
站着(不穿鞋)		
身高	152	179
眼至地面高	141	168
肩高	123	146
肘高	95.0	110
指尖至地面高	61.5	70.7

续表 A4

	数值极限 cm	
	最低限制值 成年女性	最高限制值 成年男性
功能伸屏范围	64.0	83.1
人体轴线至台边的距离	12.7	12.3
人体中心轴至眼的距离	7.6	8.2
坐着		
腿弯曲部位的高度(膝下方)	38.1	45.4
椅面以上的身高(伸直)	79.0	96.3
椅面以上的身高(放松)	77.5	94.3
椅面以上的眼高(伸直坐着)	67.6	85.1
椅面以上的肩高	49.8	64.1
椅面以上的肘高	16.3	29.7
功能伸展范围	64.0	83.1
大腿的净高度	10.4	14.9
臀部至膝弯内侧的距离	43.4	49.4
膝的高度	47.0	53.5
人体轴线至台边的距离	12.7	12.3
人体中心轴至眼的距离	7.6	8.2

A6.1.2 公认惯例

控制室接口的设计必须恰当考虑公认惯例。

必须对下列各项建立公认惯例的基准：

a. 控制器的动作方向；

b. 显示指针和等效物的位移方向；

c. 各种颜色的意义。

控制器的习惯响应的实例示于图 A1。

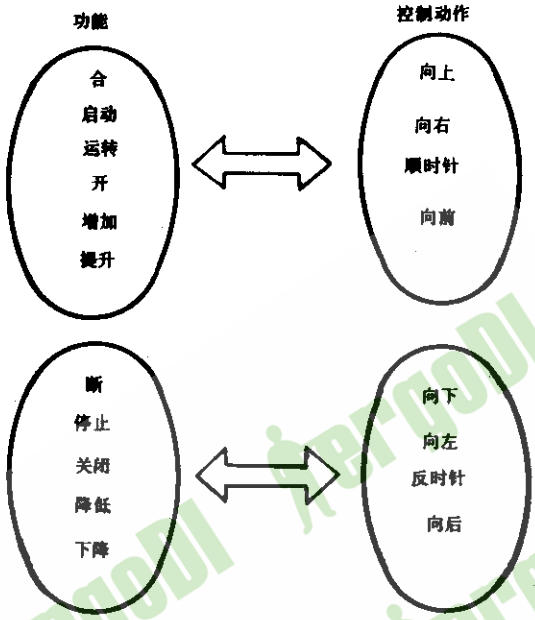

图 A1　控制设备习惯响应的实例

A6.1.3　听觉和视觉的能力与特性

必须提供听觉和视觉的能力与特性方面的设计数据，包括下面这些项目。

A6.1.3.1　听力：

a.　频率范围：200～5 000Hz；

b.　最佳频率范围：500～3 000Hz；

c.　音响强度：在 60dB 和 90dB 之间；

d.　最大环境噪声：45dB；

e.　音响强度对环境噪声的最小差值：10dB；

f.　应急信号的音响强度：90～100dB。

A6.1.3.2　视力：

a.　照明照度：最大 750lx，最小 200lx；

b.　照度均匀度：不小于 0.5；

c.　对荧光屏的事故照度：最大 100lx，最小 50lx；

d.　文字和符号的最小视角：15′；

e.　视线与显示的正面之间的最小观察角度：45°；

f.　最低应急照明照度：200lx。

A6.1.4　人处理信息的能力

还必须提供人在信息处理方面的能力与特性的设计基准，例如：工作负担、速度、时间迟延和判断的方式（例如：图形的识别、文字说明的寻找）。

这些数据的实例陈述如下：

a.　屏幕显示或等效物的平均调出时间应小于 2s，理想的是小于 1s。显示数据的更新时间应小于 2s，但应与人的能力和测量的时间间隔相匹配，显示时间应取决于信息的数量和格式；

b.　在关系到确定限值、变化速率或方向变化、数据比较的地方，为检查读数，采用模拟式的表达方

式比较好。当引入时间标尺作趋势和预示性显示时，模拟式表达较好。数码式显示适宜于数值比较；

c. 在要求数值或数值对比的场合，数字式的表达比模拟量的表达快 4 倍，而且有关的差错率大约是 1∶20。

还应提供信息表达型式(用模拟量还是数字量)的选择准则。

A6.1.5 环境因素

对电厂的正常与异常的两种工况，应提供控制室内操纵员的工作环境要求的数据。应使用的数据见 6.2.2。

A6.2 控制室的位置、工作环境与防护措施

A6.2.1 控制室的位置

作为安全要求，控制室必须安排在不受电厂内部危险后果(如：飞射物、放射性、火灾等)影响的位置，而且在所有电厂工况下，当控制室不宜居留时，操纵员能易于获得撤离控制室的通路。

A6.2.2 工作环境

为了保持控制室的工作环境适宜于操纵员执行他们的任务，至少必须满足下列要求：

A6.2.2.1 空气调节

控制室必须实现空调。通风系统的设计必须包括对付电厂事故工况的措施。

A6.2.2.2 照明

在控制室照明系统的设计中，应特别注意照明的均匀性、阴影、眩光、反光和强照度。某些数据提供在 A6.1.3 中。

在正常照明系统发生故障时，应急照明系统必须连续地提供为进行工作所必需的照度。

A6.2.2.3 音响环境

控制室音响环境依据 A6.1.3 所陈述的人的听觉能力和特性的数据设计。

控制室的本底噪声应降至最低，应不超过 45dB。

A6.2.3 防护措施

A6.2.3.1 防火

应注意只使用非燃性材料。控制室区域必须安装火警探测系统和灭火系统，并符合 HAF 0202 规定的要求。

控制室内的电气设备必须设计成：即不引起着火，也不助长着火，在这些方面尽可能达到合理。

与控制室有关联的电缆电路和配电箱必须防护火灾的后果。电缆绝缘和护套材料应是阻燃的，并满足 GB 2951.19 规定的阻燃级别要求。

A6.2.3.2 放射性防护

控制室工作人员应受保护，免受任何事故情况下的直接照射。空气引入风管必须安装辐射监督系统。如果情况需要，控制室通风系统必须具有自身隔离的能力，必须为工作人员准备好可用的防护器具。

A6.2.3.3 飞射物防护

控制室的设计必须包括对控制室外部与内部产生的飞射物作出估计，并采取预防措施。飞射物防护应符合 HAF 0204 规定的要求。

A6.2.3.4 地震防护

有关安全功能的控制室设备、空调系统和应急照明系统，必须按电厂重要的安全仪表与控制设备相同的地震基准来设计。

A6.2.3.5 保安措施

为阻止无关人员进入控制室，并防止故意行动，应采取措施。保安计划必须遵守国家管理法规的要求。

A6.3 控制室的空间与布置

A6.3.1 控制室的空间

如 6.3.1 条所述，应为工作场地、书写空间和文件的存放空间提供必要的场所，如：

a. 给持续的工作人员配备的工作场所，必须设计成坐着操作，并提供舒适的座位，也应允许站着操作；

b. 当书写与接触文件成为操纵员任务中的经常工作时，必须有适当的书写空间；

c. 在紧靠操作位置的地方，还必须提供文件存放空间，以避免文件堆放在控制台或办公桌上；

d. 为将来可能进行的修改，可以提供一定的空间。

A6.3.2 控制室内的布置

A6.3.2.1 操作区的分组

a. 控制室区域必须理想地分成几个操作区，在各种运行工况下，每个操纵员具有执行其分配的任务所要求的全部控制与指示设备。运行工况包括启动、正常运行、停机和应急处理等；

b. 控制室的布置应使操纵员任务之间的干扰最少。

A6.3.2.2 控制屏与布置

控制室内的控制屏、台和盘的布置必须是：

a. 允许每个操纵员在它们之中占有足够的空间，能立即和直接接近与他的任务有关的信息与控制设备；

b. 将不同操纵员的通路冲突减到最小；

c. 方便操纵员之间的联络与协调；

d. 反射眩光最小。

如果控制屏或盘多于一横排，不在操纵员正面屏上的指示和控制设备，必须是不要求立即或连续操作的指示和控制设备。

A6.3.2.3 尺寸与外形

控制室设备(例如：控制台、屏、盘和椅等)的尺寸和外形必须根据人体尺度的要求来决定，并满足其他各项人因工程需考虑的事项。

A6.4 屏的设计

A6.4.1 优先性

在控制台、屏和盘上的报警器、显示器和控制器的布置与排列，应考虑重要性和人类工效学的因素，在屏和盘上的优先次序必须与电厂中的优先次序一致。

A6.4.2 控制台和屏的设备定位

在控制台和屏上的显示器、指示器和控制器的布置，从上至下常用的排列是：

a. 报警板；

b. 指示仪表；

c. 不常用的控制器；

d. 常用的控制器。

A6.5 布置的辅助手段

A6.5.1 显示器和控制器的编组技术

被显示的信息和控制器，按逻辑关系编组是重要的。六种主要技术可以利用。这些技术是：

a. 按功能或相互关系编组；

b. 按使用顺序编组；

c. 按使用频率编组；

d. 按优先性编组；

e. 按操作程序(正常或应急)编组；

f. 模仿工艺过程的模拟编组。

编组方法应与使用者思维方式的规律一致。

以下技术可以用于显示信息和控制器的编组。

A6.5.1.1 按功能编组

信息和控制应按它们在一个系统内的功能或相互关系来编组。必须细心地依据信息在完成系统目标中扮演怎样的角色来鉴定其功能，而不是根据信息的来源或测量的方法。

A6.5.1.2 按使用的顺序编组

信息和控制器可以依据使用顺序编组。既可把显示当作一个整体，也可把显示分为几个部分。这两种情况都可以按顺序组织。在显示上应反映因果关系。

在一组或一个显示内，历史的信息应置于较新的信息之上。

使用自然的编组法是符合使用者的公认惯例。例如：1，2，3 或 a，b，c 等。由于同一理由，显示应按相应方法来组织，例如，从左至右、从上至下。

A6.5.1.3 按使用的频率编组

在这种编组形式中，将最常用的信息集中在一起，也就是：最常使用的在显示的上部，较少使用的在下部，使用最多的控制器最靠近操纵员。

确定使用频率最通用的方法是链分析法，以便决定信息或控制设备和操作顺序之间的联系。

由于这种类型的编组方法在显示上有明显不合逻辑的风险，应用是有限制的。

A6.5.1.4 按优先性编组

信息或控制依据对系统完成功能的重要性编组，重要物项应置于一组之内的主要位置上。

A6.5.1.5 按操作顺序编组

信息显示和控制器应根据操作顺序编组，在紧急工况下被使用的显示器与控制器等专用设备，应与正常运行的显示与控制设备分别编组。

A6.5.1.6 模拟图式的编组

如果使用模拟图，一定要注意避免跟所用的其他准则相矛盾；如果将来需要变更或增加流程或仪表与控制器的话，一定要注意保持相同的模拟原理。

在斟酌选用上述编组技术时，应排除那些不适用的编组技术，并从改善信息传递出发权衡剩下的各种编组技术的相对重要性。在所有情况下，每个组的规模必须适当，以便允许迅速与准确的寻查。此外，人的性能要求始终放在优先地位。

A6.5.2 编码方法

6.5.2 条的编码方法和导则分述如下：

A6.5.2.1 物理编码法

A6.5.2.1.1 尺寸编码

用绝对尺寸作区分，被使用的尺寸必须不多于三种。

A6.5.2.1.2 外形编码

用设备的外形作区分，外形的数目应受到限制。

A6.5.2.1.3 颜色编码

用于编码的颜色数目必须保持最少，以便提供必需的信息。颜色数目少于 8 种是较好的，但必须不多于 12 种，包括黑色和白色。

为了保证颜色编码的正确使用，下列规则应予应用：

a. 应以冗余的方式使用颜色，以适应照明条件的变化；

b. 颜色的选择应允许所有使用者在各种使用条件下能区分开每种颜色；

c. 使用的颜色必须与显示的底色有适当的对比度。此外，相邻的颜色彼此必须具有适当的对比度；

d. 最基本的要求是给每种颜色规定的含意应始终如一。这个要求不仅必须应用于全部显示仪表，还必须应用于电厂的屏幕显示和其他仪表、控制与报警显示。颜色编码用于符号时，也必须保持一

致；

e. 对于屏幕显示器，背景颜色应是纯正的，而且没有噪声干扰；

f. 屏幕显示格式中的固定部分所使用的颜色数目必须限于从规定的八种颜色中取四种；

g. 白色只用于正常范围内的变量数据；

h. 对于增强编码有四种颜色就够了，而且必须一致地使用这四种颜色。

在选择颜色编码中，应考虑颜色含义方面的公认惯例以及现有的工业标准和控制室设备已经制造的事实。

A6.5.2.1.4 音响编码

以音响的频率编码是许可的，但使用的不同频率信号应不多于三种。

A6.5.2.1.5 强度编码

强度编码应不用于音响编码中，也不用于目视显示器上。

A6.5.2.2 信息编码法

显示器的编码通过促进使用者的理解和消化来改善信息的可用性，所应用的编码必须有助于信息从工艺过程向使用者传递。也不应要求使用者为了使用它而转译信息。

编码的最重要因素是增加识别能力。

必须避免纯粹抽象的编码，例如物项与数据的随意结合，因为难于记忆和使用。

A6.5.2.3 位置编码(结构编码)法

除了用指针、字母、字母组或符号传输信息之外，信息置于不变的相对位置能增强所期望的寓意。

A6.5.2.4 数据编码法

数据编码的主要用途是形成缩写。用在标牌、显示器和屏幕显示中的缩写应遵守一套满足使用者需要的标准缩写格式。

严格地订出一种简写词和缩写词的词汇表是最重要的。

A6.5.2.5 增强编码法

增强编码法可用来加强被传输的数据，可利用的技术包括：屏幕显示器上的翻转显象和 3～5Hz 闪烁，以及所有各类显示器上的符号大小与字体亮度。

A6.5.3 标记方法

控制室内的标记方法必须与电厂内的其他标记方法一致，并符合我国的习惯。

标记方法的准则如下：

a. 标牌上的书写方式必须同我国读物的阅读方式是相同的；

b. 标记方法中的分级制应以尺寸大小来实现，而不是以不同的颜色、外形或排字方法来实现；

c. 词汇(例如：简写词或缩写词)必须在所有系统中都是一致的，并易于联系其全称；

d. 铭牌必须提供功能描述和维修目的的识别标志，并与电厂正式的文件中所使用的相同；

e. 功能描述的重要性与物项所使用的编组方法有关。

A6.6 信息系统

A6.6.1 信息功能

信息系统为操纵员和非值班专家提供数据采集、数据处理、显示和报警功能。这个系统还具有记录和打印功能。

A6.6.1.1 为操纵员提供的信息

整个电厂的状态必须由操纵员使用一组显示器、光字牌或屏幕显示器进行监督。

从控制室所表达的信息，操纵员必须在任何时候都能获得对电厂的完整了解。

必须用报警或其他设施指示偏离正常运行。当这些情况出现时，信息系统必须能够使操纵员做到：

a. 判明任何已出现的或潜在的安全或可用性方面的危险；

b. 知道自动系统正在进行的动作；

c. 分析扰动的原因，并跟踪其发展过程；

d. 执行任何必需的手动操作。

信息系统(包括它们的测量设备)的设计依据必须考虑它们对安全的重要性，每个系统所期望的安全功能和它在假想运行事件和事故工况下使操纵员采取正确的操作中的重要性。以上各项都必须在它的设计依据中予以确定，并必须作为选择与控制仪表分类方法的依据。

A6.6.1.2 为非值班专家提供的信息

虽然，控制室是正常运行和事故工况下操纵员的电厂信息和控制中心。但是，在事故初期阶段，它还当作根据国家和(或)营运单位的应急运行支援的原则指导厂外活动的主要中心。

为适应来访的专家，必须在邻近控制室的地方另设一个接待室，不让他们进入控制室。

为了向独立的外部支援设施提供信息，信息系统必须可以扩展。

A6.6.1.3 记录与打印

为了获得关于电厂的性能与行为按时序的信息记录。在控制室内或附近，必须为模拟的过程变量和二位制信号提供足够数量的记录仪或打印机，以便为下述目的提供信息。

a. 为值班操纵员提供短期和长期趋势的备份信息；

b. 为电厂管理提供总的运行信息；

c. 为运行和事故的短期和长期分析提供信息。

应考虑自动记录控制器的操作，以便分析操纵员的操作。

A6.6.2 数据采集系统

数据采集与处理系统应考虑可操作性和可靠性、将来电厂的修改以及可维修性等所有方面的要求。

这就要求：在确定数据采集与处理系统时，基本工作是综合的任务分析。这个分析不仅涉及电厂系统控制的要求，而且涉及控制室工作人员对正常与异常工况的操作要求。这样的分析将明确对数据的要求，包括必需数据的可用性和正确性。

在总体上确定数据采集与处理系统时，必须考虑下列各项：

a. 数据采样的频率与冗余度；

b. 预处理与一致性检查；

c. 偏离正常状态所要求的分析。

对于单一的计算机系统，原始数据的处理可能占用数据处理器很大一部分运算时间。在这种情况下，数据采集、处理和显示应限制在经营运单位认可的最低数量。这就要求：数据采集的技术要求应包括适当的数据表达和所需的输出。即使在高峰负担的时刻，在处理电厂数据或操纵员请求方面，必须没有大的迟延。

用分散功能和计算机结构配置变化的方法来降低计算机的处理负担，在系统设计中采取的措施一定要考虑操纵人员对信息完整性与易于理解的要求。

A6.6.3 显示系统

可利用的显示器有许多类型，例如：

a. 模拟式或数字式指示仪表；

b. 模拟式记录仪；

c. 二位式信号的灯光指示器；

d. 屏幕显示器；

e. 数字和图形打印机；

f. XY 绘图仪。

应依据显示的目的选择显示器的适当类型。

A6.6.3.1 用指示器与指示灯的显示

用模拟式或数字式指示表、模拟式记录仪、指示灯等信息显示的布置，必须依据人的特性和人类工

效学的要求，见 6.1 和 6.4 条。

指示表、指示灯、记录仪等必须应用 6.5 条和 A6.5 所述的布置的辅助手段(例如：颜色、外形等的编码)的原则。模拟式指示表的刻度盘和指针的动作方式必须与相关的过程变量的变化和公认惯例一致。

A6.6.3.2 屏幕显示器的显示

屏幕显示器必须运用 6.1、6.4 与 6.5 条和 A6.1 与 A6.5 所述的准则进行设计，必须既与相关的控制器和仪表一致，又与操纵员的感觉和理解的需求相容。

A6.6.3.2.1 设计

对一个显示或一组显示的要求，必须根据正确而系统地分析被显示数据的用途来确定。对每个信息项目，设计者必须弄清楚下列属性：

a. 所要求的数据是为谁的。为满足操纵员的需要，信息应构成或修订成什么样的格式；

b. 数据是为何目的要求的，例如维修数据应与运行数据分开；

c. 是否要求与屏幕显示上的其他数据或其他显示器进行比较；

d. 数据在什么时候需要，例如，与操纵员动作的关系；

e. 必须读出的数据所具有的精度；

f. 在变化速率、噪声等方面的数据特性；

g. 如果会有解释错误，那么什么样的解释错误是可接受的；

h. 要求详细与抽象的程度；

i. 在引起一个重要的瞬态过程的某个事件发生时，随之出现的报警只应该是瞬态过程的种类(包括起始事件)和自动动作期间各种故障。

数据显示设备的位置应考虑运行人员的配备、运行责任和功能的分配以及与每个操作站上人员配备的情况相一致的显示数量的最佳化。后一个考虑事项必须取决于人体尺度因素，例如：观察角度、观察距离，靠近相关的控制器与指示设备等(A6.1 所述)，此外还要考虑有关数据的数量。

A6.6.3.2.2 屏幕显示设计的总要求

显示应尽可能简单、明确和易于理解。在需要复杂的或高度详细的显示的地方，应有良好的组织与结构。

除了处理过的信息之外，安全准则要求原始的、未作处理的数据也要表达出来的地方，显示的组织与标识必须区分这两类信息。

A6.6.3.2.2.1 可用性

无论什么时候要求，需要的信息必须显示给操纵员。

A6.6.3.2.2.2 清晰性

表达在屏幕上的信息，必须在任何运行工况下被清楚地理解。为获得屏幕显示必需的清晰性，信息格式的技术要求必须符合 A6.1 所述的人因基本数据。

A6.6.3.2.2.3 精度

显示必须向操纵员传送预期的信息，而不能含糊或丧失意义。

图形和柱状图表的标尺必须使操纵员能恰当地分辨指示；最大值或当前值应以数字值注明。对于数字显示，被显示的小数点后的位数，必须与要求的测量精度相符。

A6.6.3.2.2.4 一致性

显示画面的标准化是有益的，但它必须不优先于标准正文规定的重要的准则。

在一组显示画面内表达同一个信息，所有项目应相同地命名。

在不同的显示画面上使用同一个项目时，它们应在每个显示画面相同位置上。编组技术应一致地运用标准化的标题和字体。

A6.6.3.2.3 表达的形式

如前所述，最重要的设计原则是使显示尽可能简单与明确；但另一方面，既不损失重要的细节，又不丧失重要的原则和关系。

在选择显示的形式时，必须根据被显示信息恰当地考虑具体表达方式的优点。对于数字显示，在稳定的工况下，显示器上需要更新变化的数字分额，应低于总数的1%。

A6.6.3.2.3.1 符号与图形的使用

符号应标准化。符号尺寸的大小应限于一种系列，使不同尺寸易于识别。

A6.6.3.2.3.2 原理图显示

使用一种适当简化的图形，按照电厂相关物项的相互关系将其组织起来，以避免显示的混乱。

工艺流程和顺序事件，按公认惯例通常应从左至右、从上至下展开。

A6.6.3.2.3.3 信息的格式

语句和信息的造句应有良好的措辞，如有可能，应使用一种标准化的层次信息结构。

如果信息被使用时有一定的顺序，则信息显示应反映这种顺序。

表格式信息的横行，通常不多于五组。

表达方式应与在同一位置内其他有关信息显示的形式相容。

为增强对被显示信息的感觉，使用编组与编码技术是重要的。这些编组与编码准则见6.5条和A6.5条。

A6.6.4 报警系统

A6.6.4.1 报警的功能

报警系统是一种告诫操纵员电厂工况出现不希望或不安全变化的手段。这些工况包括：

a. 以超过物理参数阈值(例如过程超出允许极限)表示的或以电厂异常状态表示的故障；

b. 操纵员未觉察的事故而产生的自动动作；

c. 自动动作未实现，或未完全实现；

d. 电厂指令状态与电厂的真实情况不符合。

A6.6.4.2 系统的技术要求

控制室报警提供监视电厂偏离正常工况所必需的全部信息。

由报警功能所监督的电厂参数和这些参数的报警整定点必须符合技术规格书的规定，必须使操纵员能监督电厂的状态，并对不希望的和不安全的工况作出有效的反应。

整定点的数值应这样确定：使操纵员具有适当的时间，在发展成电厂的严重问题之前，对告诫的工况作出反应。

在下列情形下，必须考虑具体技术措施：

a. 报警要求迅速动作；

b. 性质不同的信息也可向操纵员发出报警，例如监督滑动的模拟信息；

c. 报警来自自动系统的监视部分。

A6.6.4.3 报警处理

为提高报警系统的功能，应提供报警处理。

为了给出每个事件的最有代表性的报警，报警处理应完成下列功能：

a. 如果逻辑数据仅代表某些状态下的某个故障，那么必须只在这些状态下才报警；

b. 必须显示报警的被抑制和被旁通的状态；

c. 确认后的报警状态，在请求后必须是可利用的；

d. 如果某个单一事件有规则地导致一系列伴随故障，而伴随故障是该事件的结果，若有可能，应只发出主事件的报警；

e. 如果某个事态的发展导致通报该事态发展的信息接连出现时，重要性较高的信息应抑制重要性较低的信息。

为了事后分析的目的，所有对安全重要的报警必须记录或打印。在引起重大暂态过程的某个事件发生的时刻，尽可能只通告起始事件或自动动作期间各种失灵的报警。

必须使操纵员能够区分下述两种报警：他的纠正操作没有结束的报警和没有维修工作介入不可能消除的报警。

报警应按照事故的重要性、或操纵员不干预对电厂的影响以及对操纵员操作的需要来分类。

A6.7 控制器

A6.7.1 人类工效学的考虑

为了保证易于操作和操纵员的差错最少，控制器必须依据人类工效学来设计。

A6.7.1.1 机械的性能

控制器件的机械特性，例如：尺寸、操作压力和力，触觉反馈等，必须满足人体尺度基本数据中规定的人的能力和特性。

A6.7.1.2 一致性

a. 为了使操纵员差错最少，控制器动作方式应遵守 A6.1 陈述的公认惯例；

b. 为了区别功能上不同的或相似的控制器，所使用的颜色方案和编码方法必须是一致的；

c. 相似功能的控制器的选择，必须彼此一致；

d. 外表相似的控制器件或布置，必须以相同的方法操作。

A6.7.1.3 控制器的编码

a. 编码技术必须应用于控制器的设计。尺寸编码、外形编码和颜色编码，为此目标都是有效的。编码准则见 6.5 条和 A6.5；

b. 控制器编码必须与所有相关的系统和设备一致。

A6.7.1.4 控制器的布置

a. 控制器必须按照本标准 6.5 条和 A6.5 陈述的布置辅助手段在控制屏上布置；

b. 控制器应靠近相关的显示器；

c. 控制器的操作应在相关的显示器上产生相应的变化。

A6.7.1.5 分类与安全的关系

控制器的分类必须与它们对安全的重要性相称。

A6.7.2 误操作的防止

为防止人为的事件，控制器的误操作必须用下列方法减到最少。

A6.7.2.1 适宜的位置

控制器必须正确定位与定向，使操纵员不会无意地触动它们，在任何操作顺序的过程中，不会意外地被触动。

A6.7.2.2 固定的保护结构

控制器可以安装在凹外、加装屏障物、或用实物屏障包围。

A6.7.2.3 可移动的盖板或挡板

控制器可以用能移动的屏障物盖住或挡住，例如：控制盖、带铰链的屏障物。

A6.7.2.4 联锁控制器

可以为控制器提供联锁。例如：双重操作、许可逻辑、使用两个独立的按钮。如果某一个按钮为几个目标共用，例如总断开按钮，那么该按钮的触点动作不应是持续式的，而应是脉冲式的，从而防止越权操作。

A6.7.2.5 驱动的优先性

安全系统动作信号必须优先于手动控制信号。例外情况必须明确规定。

A6.8 控制与显示设备的组合

A6.8.1 基于计算机的控制与显示组合的使用

为电厂控制目的而增加使用基于计算机的系统，对提高控制显示的协调性提供了新的可能。这种发展需要以操纵员行为分析为依据精心制定设计准则，没有广泛而实际的试验不得采用。

A6.9 通讯系统

A6.9.1 语言通讯系统

A6.9.1.1 厂内通讯

A6.9.1.1.1 控制室的电话系统

至少有一台电话分机必须安装在控制室内。每台电话分机可以与公用电话系统连接，但在控制室内必须提供一台额外的专用电话分机，公用电话系统不能与它接通。这台电话机具有一个为人熟知的应急电话号码，该号码标记在所有电话分机上。这台电话分机必须只用于向控制室人员传送异常和事故报告。

A6.9.1.1.2 至辅助操作设施的电话系统

按6.9.1.1条的要求，为了在事故或紧急工况下与重要的安全辅助操作设施和控制点通讯，应安装一个独立的、直通的电话系统。

a. 系统必须使控制室人员能与选定的数台电话分机，在同一时间进行单一或并行通讯；

b. 系统还必须使控制室人员能与本厂的、具有独立控制室的任一其他机组的控制室通讯；

c. 系统必须由不间断电源系统供电；

d. 必须在控制室外需要的地方提供电话机的插孔。这些插孔在事故工况下应仍能接近；

e. 为运行使用，系统也能扩展。

A6.9.1.2 厂外通讯

最低限度的电话外线必须是：

a. 机组工作人员中的待命和随叫随到的人员，在紧急或事故工况中支援的专家；

b. 在厂址外面执行有关安全工作的辐射监测工作队；

c. 有关的消防站；

d. 当地公安局；

e. 政府、公众或代理机关。

A6.9.1.3 现场的布置

a. 控制室可以当作正常运行和事故初期的电厂通讯中心；

b. 与厂外通讯的绝大多数设备，最好安放在一个专门的通讯桌上，也可以安装在主控制台和控制屏中带有电话分机的屏或台上；

c. 在设有技术支援中心或应急控制设施的地方，设备必须设计成允许按照这些岗位特有的任务来传输信息；

d. 系统必须依据它们在使用期间现场环境的需要来设计；

e. 必须进行预先试验、试运行和服役试验，并记录其结果，现场的要求必须予以考虑。

A6.9.2 非语言通讯系统

A6.9.2.1 电视系统

为连续地监督反应堆操作平台和汽轮发电机的状态，希望在控制室内提供闭路电视。也可以为紧急工况提供电视装置。

A6.9.2.2 电话传真系统

在控制室内或附近，希望提供电站传真系统。为了紧急状态下传送电厂状态和运行建议，系统应与应急响应设施连接。

A6.9.2.3 计算机的数据链

为了改进电厂的可用性与安全，希望在控制室和信息中心的计算机之间提供数据通讯链。在紧急工况下，这个链应能与应急设施连接。

A7 控制室系统的检验与核准

控制室系统的检验与核准的程序与要求见 A5.3、A5.3.1、A5.3.3 和 A5.4。

附加说明：

本标准由中国核工业总公司提出。

本标准经国家核安全局审定并认可。

本标准由核工业第一研究设计院负责起草。

本标准主要起草人彭经文、赵善德、杨岐。