ICS 27.120.20
F 65

中华人民共和国国家标准

GB/T 13630—2015
代替 GB/T 13630—1992

核电厂控制室设计

Design of control room of nuclear power plants

(IEC 60964:2009,Nuclear power plants—Control rooms—Design,MOD)

2015-10-09 发布　　2016-11-01 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

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GB/T 13630—1992《核电厂控制室的设计》，与 GB/T 13630—1992 相比，除编辑性修改外主要技术变化如下：

——增加了规范性引用文件(见第 2 章，1992 年版的第 2 章)；

——增加了术语“仪表和控制系统”及其定义(见 3.12)；

——删除了术语“音响报警系统”、“辅助控制系统”、“通讯系统”、“人类工效学”、“显示格式”、“人因工程”、“不符人因工程原则”、“机器”、“广播系统”及其定义(见 1992 年版的 3.2、3.3、3.7、3.9、3.10、3.16、3.17、3.23、3.30)；

——增加了“运行经验”(见 5.8)；

——删除了“计算机的利用”(见 1992 年版的 6.10.1)；

——增加了“命名方法”(见 7.6.2)；

——调整了附录 A 中的内容(见附录 A，1992 年版的附录 A)。

本标准使用重新起草法修改采用 IEC 60964:2009《核电厂　控制室　设计》。

本标准与 IEC 60964:2009 的技术性差异及其原因如下：

——关于规范性引用文件，本标准做了具有技术性差异的调整，以适应我国的技术条件，调整的情况集中反映在第 2 章“规范性引用文件”中，具体调整如下：

- 用修改采用国际标准的 GB/T 12727 代替 IEC 60780(见 7.10.2)；
- 用等同采用国际标准的 GB/T 13624 代替 IEC 60960(见 7.7.2.5)；
- 用等效采用国际标准的 GB/T 13625 代替 IEC 60980(见 7.10.2)；
- 用修改采用国际标准的 GB/T 13631 代替 IEC 60965(见 5.7)；
- 用修改采用国际标准的 GB/T 15474 代替 IEC 61226(见 7.7.2.1)；
- 用修改采用国际标准的 EJ/T 1118 代替 IEC 61771(见 8.1)；
- 用修改采用国际标准的 EJ/T 1143 代替 IEC 61839(见 6.2.1)；
- 用修改采用国际标准的 NB/T 20026 代替 IEC 61513(见 7.7.1)；
- 用等同采用国际标准的 NB/T 20027 代替 IEC 62241(见 7.7.2.4)；
- 用修改采用国际标准的 NB/T 20058 代替 IEC 61772(见 7.7.2.3)；
- 用修改采用国际标准的 NB/T 20059 代替 IEC 61227(见 7.7.3)；
- 用修改采用国际标准的 NB/T 20060 代替 IEC 60709(见 5.3)；
- 用非等效采用国际标准的 NB/T 20071 代替 IEC 61225(见 7.10.1)；
- 删除了 IEC 60964:2009 引用的 IAEA NS-G-1.3(见 IEC 60964:2009 的第 3 章)。

——第 4 章中仅保留对控制室设计和设计团队要求的内容。

本标准由中国核工业集团公司提出。

本标准由全国核仪器仪表标准化技术委员会(SAC/TC 30)归口。

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

本标准主要起草人：周玲、熊彦、刘艳阳、王远兵、周继翔、江国进、白涛、刘元、赵勇、焦丽玲、杜建、王根生。

本标准所代替标准的历次版本发布情况为：

——GB/T 13630—1992。

核电厂控制室设计

1 范围

本标准规定了核电厂主控制室设计原则、主控制室功能设计方法及功能设计和人员配备的要求等，还规定了验证与确认控制室功能设计的程序。

本标准适用于核电厂主控制室的设计。

本标准不适用于专用的或无人值守的控制点，如：主控制室外的停堆操作点、放射性废物处理设施、应急响应设施等，也不适用于详细的设备设计。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 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 13624 核电厂安全参数显示系统的功能设计准则(GB/T 13624—2008，IEC 60960：1988，IDT)

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 13631 核电厂辅助控制点设计准则(GB/T 13631—2015，IEC 60965：2009，MOD)

GB/T 15474 核电厂安全重要仪表和控制功能分类(GB/T 15474—2010，IEC 61226：2005，MOD)

EJ/T 1118 核电厂控制室设计验证和确认(EJ/T 1118—2000，IEC 61771：1995，MOD)

EJ/T 1143 核电厂控制室设计 功能分析与分配(EJ/T 1143—2002，IEC 61839：2000，MOD)

NB/T 20026 核电厂安全重要仪表和控制系统总体要求(NB/T 20026—2014，IEC 61513：2011，MOD)

NB/T 20027 核电厂主控制室的报警功能与显示(NB/T 20027—2010，IEC 62241：2004，IDT)

NB/T 20058 核电厂控制室屏幕显示的应用(NB/T 20058—2012，IEC 61772：2009，MOD)

NB/T 20059 核电厂控制室操纵员控制器(NB/T 20059—2012，IEC 61227：2008，MOD)

NB/T 20060 核电厂安全重要仪表和控制系统隔离准则(NB/T 20060—2012，IEC 60709：2004，MOD)

NB/T 20071 核电厂安全重要仪表和控制系统的供电要求(NB/T 20071—2012，IEC 61225：2005，NEQ)

ISO 11064(所有部分) 控制中心人因设计(Ergonomic design of control centres)

IAEA NS-G-1.9 核电厂反应堆冷却剂系统和辅助系统设计(Design of the reactor coolant system and associated systems in nuclear power plants)

IAEA NS-G-1.11 在核电厂设计中防止除火灾和爆炸以外的内部危害(Protection aginst internal hazards other than fires and explosions in the design of nuclear power plants)

3 术语和定义

下列术语和定义适用于本文件。

3.1

报警 alarms

用于警示操纵员关注过程变化或系统偏离的诊断、预报或指导信息。

注 1：报警所提供的特定信息包括：需要采取纠正措施的异常、异常原因和潜在后果、整个电厂的状态、针对异常所要求采取的纠正措施以及采取纠正措施后的反馈。

注 2：偏离可分成下述两类：

a) 非预期的偏离，即非预期的工艺偏离或设备故障；

b) 预期的偏离，工况或设备状态的偏离是对非正常电厂条件的预期响应。

3.2

控制室人员 control room staff

值守在控制室的一组电厂工作人员。他们通过人机接口控制电厂，负责完成电厂的运行目标。通常，控制室人员包括值班长和执行控制操作的操纵员，还可以包括在长期的事件期间经授权允许进入控制室内的其他人员和专家。

3.3

控制室系统 control room system

人机接口、控制室人员、运行规程、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。

3.4

控制器 controls

操纵员用来向控制系统和电厂物项发送指令信号的设备。

3.5

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。

3.6

功能 function

可以详细说明和描述的所要完成的任务或目标，不涉及实现方法。

3.7

功能分析 functional analysis

根据可利用的人力、技术和其他资源，检查系统的各项功能目标，以提供确定功能如何分配与执行的依据。

3.8

功能目标 functional goal

为完成相应的功能，应达到的性能指标。

3.9

层次目标结构 hierarchical goal structure

以分层次的结构形式表明功能目标和子功能目标之间的关系。

3.10

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。

3.11

人机接口 human-machine interface；HMI

电厂中运行人员与仪控系统和计算机系统之间的交接面。人机接口包括：显示设备、控制器与运行支持系统等。

3.12

仪表和控制系统　instrumentation and control system;I&C system

基于电气和(或)电子和(或)可编程电子技术的系统,它执行仪表与控制的功能以及与系统自身运行有关的服务和监督。

注 1:本术语包含系统的所有部件,如:内部电源、传感器和其他的输入设备、数据总线和其他的通信路径、对驱动器和其他输出设备的接口等。系统内的不同功能可使用专用资源或共享资源。

注 2:特定的仪表和控制系统中包含的部件在系统的边界说明中规定。

注 3:按照仪表和控制系统典型的功能特性,IAEA 区分自动与控制系统、HMI 系统、联锁系统和保护系统。

注 4:改写 NB/T 20063—2012,定义 3.1.2。

3.13

作业　job

在操作上相关的一组任务。一项作业的各项任务在所需的技能、知识和责任方面是一致的。

3.14

作业分析　job analysis

为确定某一作业对控制室人员配备、运行规程和培训大纲的基本要求所做的分析。

3.15

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

设置在控制室外面由就地操作员进行控制活动的控制点(或设施)。

3.16

就地操作员　local operator

在控制室外面执行任务的操作人员。

3.17

运行规程　operating procedures

规定为实现功能目标所必需的运行任务的一系列文件。

[NB/T 20063—2012,定义 5.14]

3.18

运行人员　operating staff

电厂运行当班工作的电厂人员,包括控制室人员、维护人员等。

3.19

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,主要是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。

3.20

操纵员支持系统　operator support system;OSS

支持控制室人员进行高级思维处理任务的一个或多个系统。

3.21

性能要求　performance requirements

为确保功能目标的实现而对任务性能规定的定量要求。

3.22

电厂运行目标　plant operational goal

电厂设计的最终目的,即:按需要发电和限制释放到环境中的放射性。

3.23

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。

3.24

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。

3.25

任务分析　task analysis

根据任务的组成详细描述操纵员的任务，以确定人相关活动的细节，以及这些活动在功能上和时间上的关系。

3.26

培训大纲　training programme

为培训控制室人员，使他们获得运行活动所必要的技能和知识所制定的大纲。

3.27

验证　verification

确定一项产品或服务的质量或性能与规定、预期或要求是否符合的过程。

[IAEA Safety Glossary:2007]

3.28

确认　validation

确定一个产品或一项服务是否足以完成它的预期功能的过程。与验证相比，确认的范围更宽一些，包含了更多的评价元素。

[IAEA Safety Glossary:2007]

3.29

屏幕显示器　visual display unit;VDU

用屏幕显现由计算机驱动的图像的显示设备。

4　概述

控制室设计应由一个团队完成，控制室设计团队的目标是成功完成一个综合的控制室系统设计。

控制室系统应是一个集人机接口、控制室人员、运行规程、培训大纲和一些相关的设备与设施为一体的综合系统。图 1 是控制室系统总貌图，关于控制室系统概念的补充说明参见附录 A。

控制室设计应确立人机接口，建立一种用于开发员工需求、运行规程和培训大纲的方法。设计过程和标准各章条关系如图 2 所示。

控制室设计团队应由具有不同能力、从事不同专业的人组成。至少应包括如下的专业：

——核工程；

——建筑设计和土木工程；

——系统工程；

——仪表和控制系统；

——信息和计算机系统；

——人因工程；

——电厂运行；

——培训。

这些能力可以由专职的或临时的组员提供，甚至可以由顾问人员提供。

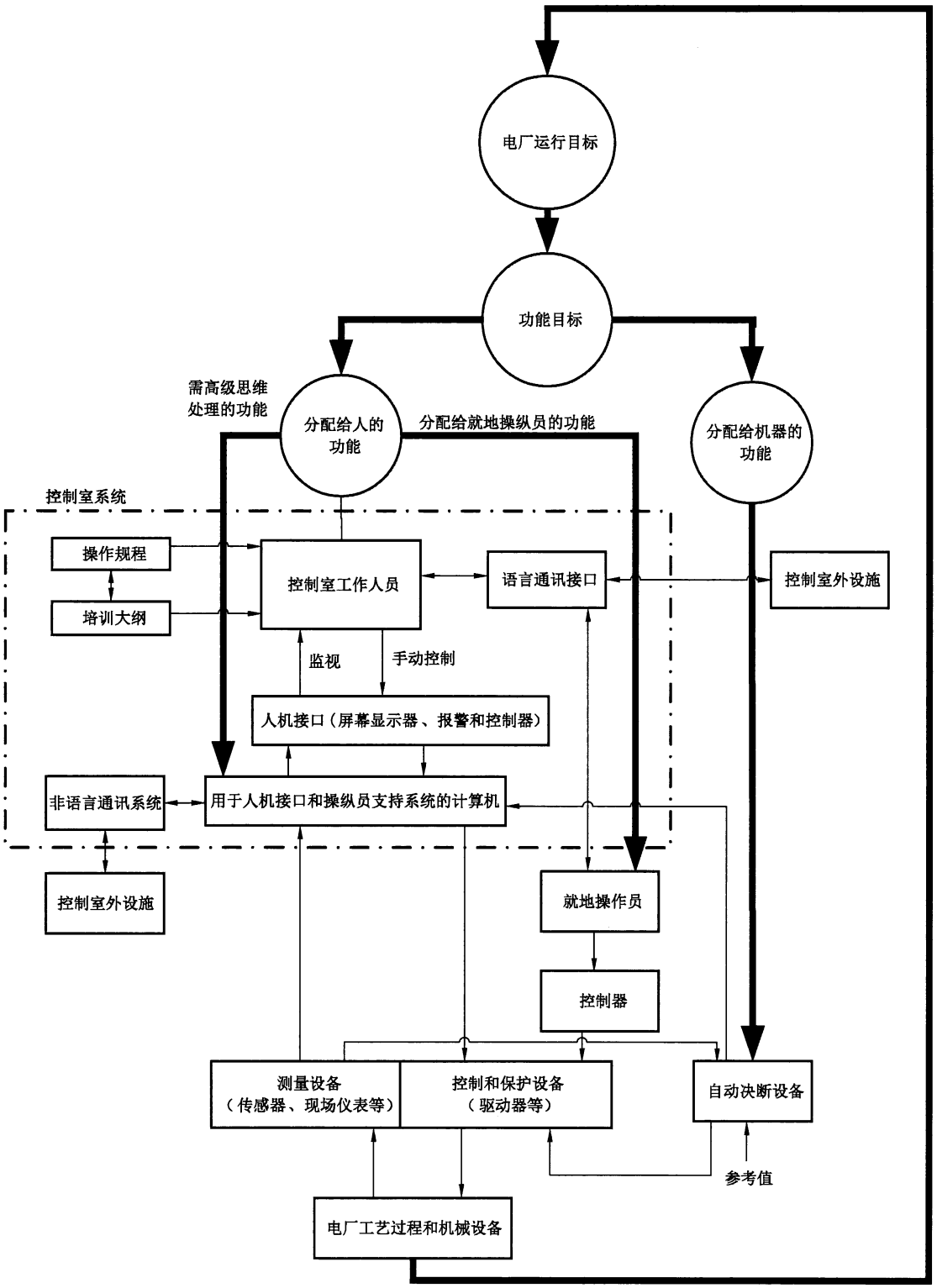
电厂运行目标
功能目标
需高级思维处理的功能
分配给人的功能
分配给就地操纵员的功能
分配给机器的功能
控制室系统
操作规程
培训大纲
控制室工作人员
语言通讯接口
控制室外设施
监视
手动控制
人机接口（屏幕显示器、报警和控制器）
非语言通讯系统
用于人机接口和操纵员支持系统的计算机
控制室外设施
就地操作员
控制器
测量设备（传感器、现场仪表等）
控制和保护设备（驱动器等）
自动决断设备
参考值
电厂工艺过程和机械设备

图 1　控制室系统概貌图

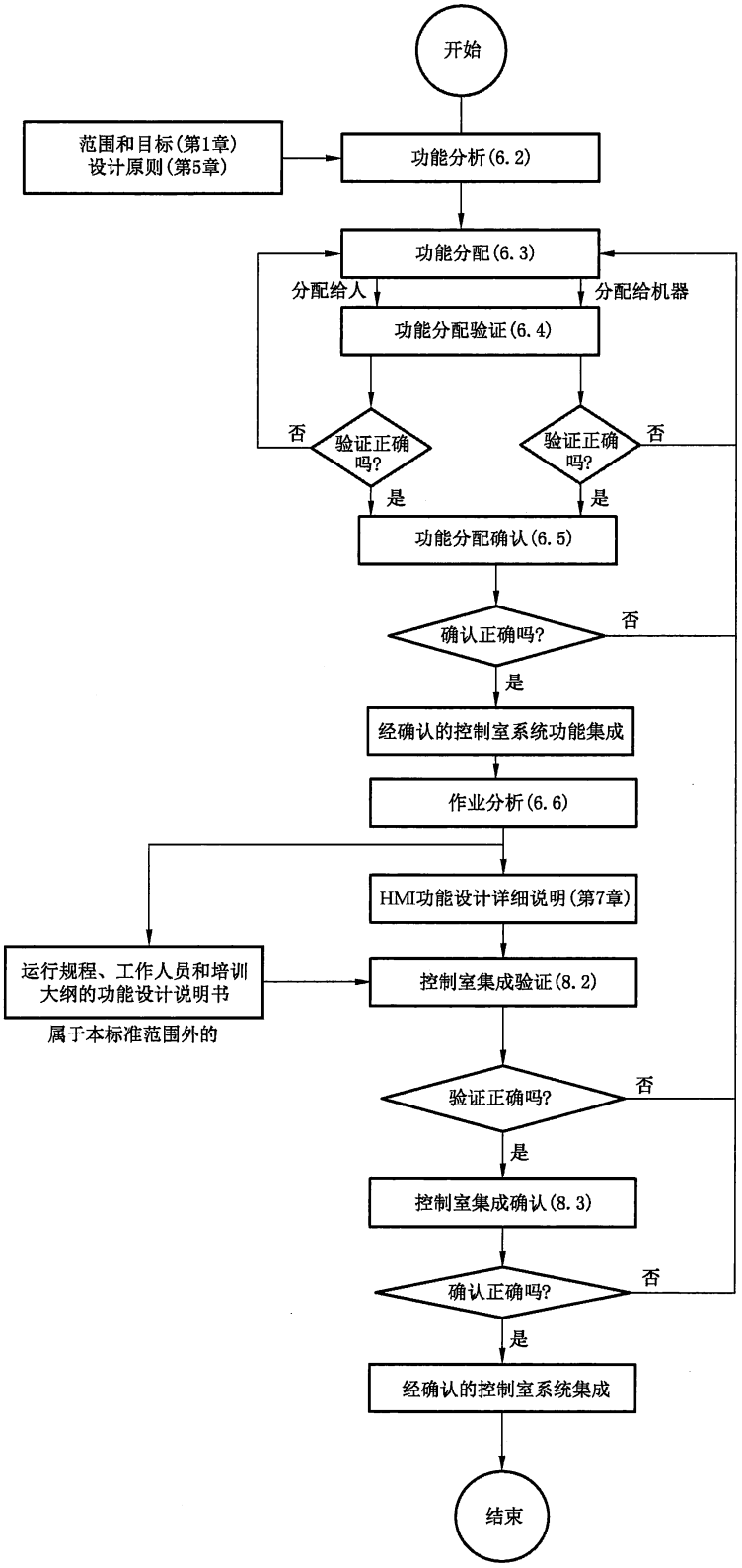

图 2　设计过程和标准各章条的关系

5 主控制室设计原则

5.1 主控制室的主要目标

核电厂的主要目标是其在所有运行状态和事故工况下可以从主控制室实现安全与有效地运行。主控制室为控制室人员提供实现电厂运行目标所必需的人机接口和相关的信息与设备(如,通信接口)。此外,控制室为控制室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。

5.2 主控制室的功能设计目标

控制室设计的基本目标是向操纵员提供关于电厂设备和系统运行状态的及时、准确、完整的信息。

控制室设计应满足所有运行状态(包括换料和事故工况)的要求,使任务执行最佳化,并将安全地监测和控制电厂所需的工作量减少到适当的水平,同时向控制室外的其他设施提供必要的信息。

控制室设计应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调试能有效地进行,并可以修改与维护。

5.3 安全原则

控制室设计应使核电厂可以在所有运行状态下安全地运行,并在事故工况发生后能使电厂恢复到安全状态。这样的事件在控制室设计时应加以考虑。

由控制室控制的设备应尽可能地设计成可阻止非安全手动指令的执行,例如:使用依赖于电厂状态的逻辑联锁。

在冗余的安全系统紧密相邻或者安全与非安全系统紧密相邻的地方,应考虑功能隔离和实体分隔要求。如果控制室和它的系统受到火灾的影响,应确保其安全,并且把发生火灾的可能性减至最小。详细要求见 NB/T 20060。

控制室应采取适当的措施,保障控制室内人员的安全,免受潜在危险的影响,例如,闯入未经批准的人、事故工况所产生的放射性、有毒气体或火灾影响等危及操纵员行动的事件。

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

5.4 可用性原则

为使电厂利用率最高,在控制室设计时应考虑以下各项:

a) 在负荷改变、启堆和停堆时便于按计划运行;
b) 把由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紧急停堆的几率减到最小;
c) 达到电厂的设计输出和性能指标。

与可用性相关的设计应不违反安全原则。

5.5 人因工程原则

为了提供最佳的功能分配,以保证人与机器能最大限度地发挥其能力,并使电厂的安全性与可用性最好,设计应特别关注人因原则和人的特性,例如:人体尺寸、人的感觉、认知、生理和运动机能反应的能力与限度。

5.6 营运管理原则

操纵员的配备与培训是控制室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

室应配备数量足够并有专业技能的工作人员。

控制室人员应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，具备电厂子系统和部件及其功能、性能和位置方面的详细知识。

由控制室外的操作员执行的涉及电厂设备操作的任务，应受控制室行政上的管理与监督。

为确保核电厂的运行质量，电厂营运单位应对控制室的人员配备考虑以下因素：

a) 人员选择与资质的要求；
b) 针对正常、异常与事故工况的初始培训和复训要求；
c) 操作技能的定期复训以及获得拓展工程原理知识的机会；
d) 在正常和紧急运行期间，控制室人员和每个人的职责；
e) 人员的身体要求，如视听能力、身高及身体缺陷等；
f) 管理方式、监督体系与人员职责；
g) 换班的模式与工作强度。

5.7 与其他控制和管理中心的关系

为了辅助控制室人员对异常运行工况做出反应，在应急工况下，应急响应设施应能投入运行。

在主控制室外应设置辅助控制点，以便在主控制室受损或不可用时，足以保证反应堆的安全。辅助控制点的设计要求见 GB/T 13631。

应配置切换设备，用以将监控功能从主控制室切换到辅助控制点。切换设备的操作应不依赖于主控制室内的其他设备。

5.8 运行经验

宜对在役核电厂可用的运行经验进行收集和分析，将适用的经验反馈到新的核电厂设计中。

这些经验可能建议采用已经证明的方案或对其进行优化，甚至会影响到以下方面原则的考虑：

a) 人员配备；
b) 运行团队组织机构与作业安排；
c) 控制室与就地控制点之间功能分配；
d) 自动化水平。

信息处理、信息显示与控制器的设计。

6 主控制室功能设计

6.1 一般要求

应使用一种系统化的方法来进行控制室的功能设计，包括图 1 中所示的控制室和有关项目。这种设计方法应包括图 2 所示的下列 5 个步骤：

a) 功能分析；
b) 功能分配；
c) 功能分配的验证；
d) 功能分配的确认；
e) 作业分析。

6.2 功能分析

6.2.1 一般要求

为了实现 5.1 和 5.2 的目标，并符合 5.3～5.8 的原则，应对核电厂所执行的功能进行分析。

这种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。目标应包括电力生产和把放射性释放减到最少这两项基本目标。每一目标可进一步分解成子目标，并用于设计决策过程。

功能分析过程的详细要求见 EJ/T 1143。

6.2.2 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。确定这些目标的方法见 EJ/T 1143。在定义各项功能时，应考虑控制室与控制室外的设施和系统之间的相互影响。

6.2.3 信息流与处理要求

应进行分析，以确定为实现电厂功能（包括判断与操作）所需要的基本运行信息流和处理过程，分析过程详见标准 EJ/T 1143。

在确定信息流与处理要求时，设计者除了考虑所有正常运行工况外，还应考虑几种有代表性的设计基准事件。应包括下列事件：

a) 需要操作，但由于数据的解释或控制的复杂性、控制速度等原因导致操纵员难以主观判断的事件；

b) 要求操纵员确定无疑地做出正确反应的事件，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) 出现频度高的事件。

考虑的事件数目应足以覆盖层次目标结构中的各项功能。

6.3 功能分配

6.3.1 一般要求

应进行任务分析，以决定哪些功能分配给人，哪些功能分配给机器。

分配给人的功能参见表 A.1，它们是：

a) 手动控制，包括自动化的后备控制；

b) 与自动控制和手动控制有关的监视；

c) 高级思维处理任务，例如：诊断异常的、意外的运行工况和事件的起因，并做出纠正动作的决定。

分配给机器的功能指由自动控制所完成的功能（参见表 A.1）。

在分析中，应采用人因工程原则和设计准则，详见 ISO 11064。

分析中所采用的原则和准则应形成文件，文件的内容应包括控制室人员和自动控制系统的能力和限度等因素。

功能分配的详细要求见 EJ/T 1143。

6.3.2 操纵员的能力

分配给操纵员的功能应区分为：

a) 由操纵员实际执行的控制任务；

b) 监视正在执行控制任务的自动系统；

c) 执行高级思维处理任务，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) 为了做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。

对操纵员可能执行的功能，应根据工作负担、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，做出处理能力的估计。应将这些估计用于初始的功能分配。这些估计应根据验证结果予以修改，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、控制和通信的要求，应与完成功能所要执行的任务一致。通常的任务应包括显示、控制和通信的要求。

操纵员可利用的各类数据，宜依据任务的需要而不是依据数据的来源进行编组。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。

6.3.3 仪表和控制系统处理能力

仪表和控制系统处理能力的分析应首先确定系统和设备的功能要求及约束条件，随后详细描述运行事件序列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，组织仪表和控制系统的信息和能力。

这样组织将便于按每项决策与控制任务来估计自动控制与人工控制两者的能力。仪表和控制系统的处理能力最终应包括系统或设备应满足的各项技术指标，例如：数量、响应时间和精度等要求，以及每类设备人机接口的人因工程要求。

为减少操纵员出现差错的概率，控制系统宜设计成在电厂异常工况开始之后一个规定的时间段内，无需操纵员任何动作即可以保持电厂在安全限制范围内。对这个时段的要求应反映在自动控制系统的功能要求中。

6.4 功能分配的验证

6.4.1 一般要求

应验证控制室的功能是否正确地分配给人和机器。验证程序如图 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，又没有对人或机器提出不适当的要求。

功能分配的验证见 EJ/T 1118。

6.4.2 验证过程

验证的工作程序应包括准备、评价和总结三个阶段。

在进行功能分配的验证之前，应证明用于功能分配的准则自身是一致的。验证应确认：

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) 所拟定的功能分配与所建立的分配准则一致；

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：时间常数、准确度)。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) 当高层功能目标产生的要求融入低层功能之中时，在所有的运行模式下应没有矛盾。

修改(纠正错误或重新分配)和验证应反复进行，直至所有准则得到满足。

6.5 功能分配的确认

6.5.1 一般要求

所拟定的功能分配应经过确认，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，应对 6.2 所确定的功能予以评价。更详细的描述参见 EJ/T 1118。

6.5.2 确认过程

确认的工作程序应包括准备、评价和总结三个阶段。

应制定事件选择的准则，以保证为评定所选择的事件是具有代表性的。在评价分配给人的功能时，除了6.2.3中规定的所有正常运行和事件之外，宜考虑多重故障所产生的事件。

选出了有代表性的事件之后，应确定每个事件所要求的功能，并按时间顺序予以整合。

6.5.3 用于确认的基本评价准则

应在所有正常运行和有代表性的事件中，评价各项功能的执行情况。应满足确认的基本准则，包括以下内容：

a) 要求控制室人员承担的功能目标的数目和工作负荷率，应在其能力范围之内；

b) 分配给控制室人员和就地操纵员的功能是可接受的；

c) 分配给自动控制系统的功能是适宜的和切实可行的。

6.6 作业分析

为了进一步制定控制室人员结构、运行规程和培训大纲的基本要求，设计者应根据经过验证或确认的功能分配和功能要求进行作业分析。

作业分析的第一步是确定分配给人的任务特点和数量。在此基础上，设计者可以根据法规所要求的控制室人员结构框架和电厂的通常习惯，确定操纵员的构成和数量。

分配给操纵员的任务宜与控制室人员结构中确定的职责一致，且不宜对操纵员造成过重的负担。设计者应进一步确定为完成任务所必须的通信，包括控制室操纵员与其他操作员之间的通信，以及控制室内操纵员之间的通信。

设计者还宜依据适当的文件，确定在一些任务中存在的非操作的行为(如：向上级报告)。

作业分析完成时应阐明：

a) 操纵员的组织和数量；

b) 操纵员的能力要求；

c) 操纵员的运行职责；

d) 操纵员的行政职责(例如报告)；

e) 操纵员之间的操作配合；

f) 操纵员与电厂之间的交互；

g) 操纵员与控制室之外的电厂人员的通信；

h) 与管理和监督部门之间的通信。

以上各项连同功能分配的分析结果(例如初步的信息结构)，应构成控制室配备人员结构、制定运行规程和培训大纲的基础。

7 功能设计的技术要求

7.1 一般要求

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。

设计应基于完整的人机系统的工程方法。

7.2 人的能力和特性的基本数据

在进行控制室详细设计时，应提供人的能力和特性的基本数据，作为基本的人因工程设计资料。

基本数据应包括：

a) 人体尺寸的考虑；

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。

这些基本数据针对不同的用户可以是不一样的。

7.3 控制室的位置，工作环境和防护措施

7.3.1 位置

控制室应安排在便于电厂运行的地方，并应满足 5.3 的安全原则。

7.3.2 工作环境

主控制室内的工作环境应使操纵员能高效且舒适地执行他们的任务。

控制室的环境设计应包括对空气调节、照明条件及音响环境的要求。具体要求如下：

a) 空气调节：主控制室应能进行空气调节。空调系统的设计应包括应对核电厂事故工况的措施，例如：使用过滤器或隔离功能；
b) 照明：照明系统设计应确保照度均匀，防眩光、反光和阴影；
c) 声响环境：声响环境设计应确保运行班组内通信便利，尽量不受环境噪声干扰，同时确保对语音信息、报警和紧急信号的可靠感知。

正常工况下对工作环境的技术要求导则见 ISO 11064。

在环境技术要求中考虑控制室尺寸和形状要求以及初步布置、电缆敷设要求、抗震要求、房间和盘台颜色以及其他完工细节要求，有助于满足土建需求和后续详细的设计确认需求。

在工作环境设计中应采取适当的措施，即使在电厂紧急工况下仍保持控制室的可用性。

7.3.3 防护措施

控制室的设计应在设计基准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。控制室设备应按设计基准条件进行鉴定。

控制室设计应确保上述事件不会同时危害主控制室和辅助控制点。

具体要求如下：

a) 防火：应注意只使用非燃性材料。控制室区域应安装火警探测系统和灭火系统。控制室内的电气设备应在合理可行的范围内设计成既不引燃，也不助燃。与控制室有关联的电缆和开关柜应有防火保护。电缆绝缘和护套材料应满足低烟、无卤、阻燃要求。
b) 放射性防护：控制室人员应受保护，免受任何事故情况下的直接照射。空气引入风管应安装辐射监测系统。如果情况需要，控制室通风系统应具有自身隔离的能力，应为工作人员配备呼吸面具。
c) 飞射物防护：控制室的设计应对控制室外部与内部飞射物做出评估，并采取预防措施。飞射物防护应符合 IAEA NS-G-1.11 的要求。
d) 地震防护：与安全功能有关的控制室设备、空调系统和应急照明系统(即：为地震后保持功能而设的照明)，应按相同的地震基准来设计。详细设计要求见 GB/T 13625。
e) 保安措施：应采取措施阻止无关人员进入控制室，并防止敌意行动。保安计划应遵守国家法规的要求。

7.4 控制室的空间与布置

7.4.1 控制室的空间

控制室应具有足够大的空间，使控制室人员可以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，应注意提供工作场地、书写空间和资料的存放空间，详细要求如下：

a) 操纵人员持续工作的区域将设计成坐姿操作，并提供舒适的座位，但也可以站姿操作；

b) 当书写与阅读文件成为操纵员任务中的经常工作时，应有适当的书写空间；

c) 在靠近操作位置的地方，还应提供文件存放空间，以避免文件堆放在控制台或办公桌上；

d) 可以提供一定的空间满足未来扩展的需要（例如：在设计阶段或控制室的生存周期内）。

7.4.2 控制室的布置

在控制室的布置中，应考虑下述事项：

a) 营运管理原则；

b) 给操纵员和仪表控制系统的功能分配；

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，由此决定概貌显示图的使用，以及控制仪表盘上使用的屏幕显示器、指示仪表、记录仪、报警器和指示灯的数量；

e) 技术的选择，如：相对于软控制和屏幕显示器（包括大屏幕显示）的使用程度而言，专用硬接线控制器和指示器的使用程度；不同序列之间的分区；自动控制顺序的使用；自动化和（或）多路控制的程度；

f) 营运主管当局要求和法定要求，例如：由运行策略或安全当局所要求的控制室操纵员的人数；

g) 不需要操纵的系统（如：火灾报警与消防系统，及其他与就地相关的功能系统）的安装；

h) 为行政管理提供的空间。

控制室应划分为若干操作区，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、控制盘和盘）的布置应符合人因工程原则。控制室的布置应让每一位操纵员对控制室设备按照其相应功能实现方便操纵和快速辨识，并且应让每一位操纵员能够和通常在场的其他操纵员直接对视并交流，而没有彼此间视线的不当干扰。

具体的技术要求见 ISO 11064（所有部分）。

信息显示设备和控制器的布置应遵循统一的原则。这些原则宜在设计过程中形成文件。

控制室的布置应是结构化的，尤其在控制室大量使用专用硬接线控制器和指示器的情况下，以利于在正常运行、事故工况和紧急情况下系统与部件的识别，并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，所有的操作区都应一致遵守。

7.5 台盘设计

7.5.1 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，以及在控制盘上布置的相似器件之间的优先次序，应建立一些原则，并予以贯彻。对电厂中的所有控制盘，其规则应一致。

7.5.2 台盘上的设备布置

在控制台盘上，显示器、指示器和控制器的布置应依据下列准则：

a) 报警屏和报警牌应从控制室的操作区可以观察到，并且从操纵员的可视性和辨识性角度考虑应布置在合适的高度上；

b) 频繁使用的控制器应位于便于触及的地方，有关的指示器和显示器应从操作位置可以读数。

详细的技术要求见 ISO 11064（所有部分）。

7.5.3 镜像布置

为了防止左右混淆，各种控制盘、控制器和指示器应避免采用镜像布置。

7.6 布置的辅助手段

7.6.1 显示信息和控制器的编组

显示信息和控制器按逻辑关系编组是重要的。

下列技术可用于显示信息和控制器的编组：

a) 按功能编组：信息和控制宜按功能或在系统内的相互关系来编组。应注意根据信息在完成系统目标中所起的作用，而不是根据信息的来源或测量的方法来确定其功能。

b) 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。在显示上宜反映因果关系。可以使用符合使用者公认惯例的自然编组法，例如：1、2、3 或 a、b、c 等。由于同一理由，显示宜按相应方法来组织，例如，从左至右、从上至下。

c) 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，放在显示的上部，较少使用的放在显示的下部，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。

d) 按优先级编组：按信息或控制对系统正确执行功能的重要性编组，最高优先级物项宜置于一组之内的主要位置上。

e) 按运行规程编组：信息显示和控制器宜根据运行规程编组，在紧急工况下所要使用的显示器与控制器等专用设备，宜与正常运行的显示与控制设备分别编组。

f) 模拟图式的编组：如果使用模拟图，应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工艺流程或仪表与控制器的话，一定要注意保持相同的模拟原则。

通过衡量上述方法各自的特性，宜将合适的方法筛选出来单独或组合使用。每个组的规模应适当，以便可以迅速与准确地寻找。此外，应充分考虑人的执行能力。

编组宜与操纵员对于核电厂的认知模型相一致。

应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。

7.6.2 命名方法

核电厂内的每一个物项（还应考虑核电厂其他冗余物项）的名称和标识应精心设计并在项目范围内统一使用。

宜统一规定并使用专用的简称或缩写（例如：CVCS 代表化容控制系统）。按照人因工程原则对这些核电厂标识进行审核是十分有益的。

7.6.3 编码方法

控制器和显示信息的编码用于区分不同类型的控制器或不同种类的显示信息，例如：安全功能、安全重要的其他功能、非安全重要功能。

编码规则应建立于控制室设计的早期阶段，而且应符合要求和工程实践。

在整个控制室内，编码体系应是一致的。显示器和它们相关的控制器所使用的位置、信息、颜色和亮度的编码形式应完全一致。

实际采用的编码方法应通过衡量各类编码方法的相对优势来确定：

a) 物理编码(尺寸编码、形状编码、颜色编码、音响编码、亮度编码等);

b) 信息编码;

c) 位置编码。

各类编码方法及其导则见 ISO 11064(所有部分)。

考虑到潜在的人员因素(例如:色弱型人员)和设备因素(如:褪色,仪表和控制系统设备的部分失效),颜色不应作为区别安全重要信息的唯一编码手段。同样的,在其他应用场合也宜避免颜色成为唯一编码手段。

7.6.4 标识

在控制室内应提供恰当的标识。标记方法应与电厂中其他标记方法一致,并符合相关标准要求和工程实践。详细要求见 ISO 11064(所有部分)。

控制室中所有的标记、标识符和所有显示所使用的语言和字符样式都应统一。

7.7 信息和控制系统

7.7.1 一般要求

按照 NB/T 20026 规定的设计过程和要求,仪表和控制系统总体结构设计将会产生信息和控制系统,实现主控制室对核电厂监测控制功能的人机接口。

系统结构取决于:

a) 安全分级;

b) 失效准则;

c) 纵深防御策略;

d) 鉴定和可靠性要求;

e) 维护要求;

f) 可用技术的选择。

信息和控制系统由一个或几个子系统实现。这些子系统分别完成不同的人机接口功能和操纵员支持功能。典型的信息和控制系统包括带屏幕显示器和软控制的计算机系统以及专用模拟指示表和控制器。

7.7.2 信息功能

7.7.2.1 一般要求

应设置信息系统,向操纵员提供对安全和可用性重要的电厂状态及变量的显示,使控制室操纵员可以随时全面了解核电厂状态。

应提供足够的信息,使运行人员能依据法规要求实现并长期保持在安全停堆状态。

在事故工况下,系统还应向技术专家和厂内、厂外的安全专家提供电厂状态的信息。

系统应具有数据采集、显示和报警功能。系统还应具有对安全和可用性重要的电厂过程变量的记录与记忆功能,以便分析和向营运机构与管理当局报告。

系统还应具有信息处理功能,以作为支持操纵员的高级思维处理工作的手段,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。

以上功能宜通过如下方法实现:

a) 确保信息的高可用性和可靠性;

b) 为规范化操作提供有用信息；
c) 方便控制室人员之间信息交流；
d) 为分析提供瞬态过程与事故工况的记录，包括提供对记录数据的获取；
e) 如果可行，记录操纵员控制操纵动作；
f) 将提供的信息范围扩大到包括隐含的数据。

信息系统功能分级应符合 GB/T 15474 的规定。

详细技术要求如下：

a) 提供给操纵员的信息。操纵员应能通过信息系统随时全面了解核电厂状态。信息系统（包括其测量设备）的设计基准应考虑到它们对安全的重要性。每个系统所预期的安全功能和它在预计运行事件和事故工况下使操纵员采取正确操纵行为中的重要性应体现在该系统的设计准则里，并且应作为选择仪表和控制系统分类方法的依据。信息系统可帮助操纵员完成如下功能：
   1) 辨识任何已出现的或潜在的核电厂安全或可用性方面的危害；
   2) 了解自动化系统正在执行的操作；
   3) 分析所有扰动的原因，并跟踪其发展过程；
   4) 执行任何必需的手动操作。
b) 提供给非值班专家的信息。虽然控制室是正常运行和事故工况下电厂操纵员的信息和控制中心，但在事故初期阶段，根据国家和营运单位的应急运行支援的原则，它还可作为主要中心指导厂外活动。相关内容参见 IAEA NS-G-1.9。最好在一个单独的房间接待来访专家而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，信息系统可以扩展。
c) 记录和打印。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，应为过程变量模拟量和二进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：
   1) 为值班操纵员提供短期和长期趋势的备份信息；
   2) 为电厂管理提供总的运行信息；
   3) 为运行和事故的短期和长期分析提供信息。

   宜考虑自动记录控制器的动作，以便分析操纵员的操作。

7.7.2.2 数据采集和处理

数据采集与处理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。

在确定数据采集与处理系统时，基本工作是综合分析（例如：任务分析）。这种分析还应将控制室人员能力因素考虑在内。这样的分析将明确对数据的要求，包括必要的数据可用性和正确性。

数据采集和处理应满足下列要求：

a) 数据采集与处理的主要功能要求：
   1) 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；
   2) 输入数据的采样、预处理和分析速率应适合于有关参数的变化速率的运行要求；
   3) 数据更新的速率应适合操纵员任务的需要；
   4) 即使在数据峰值负荷时刻，对电厂数据或操纵员请求的处理，应没有大的延迟；
   5) 在系统的整个使用期限内，系统应能修改；
   6) 应采取相关措施，便于操纵员辨识无效显示信息。
b) 确定数据采集与处理系统总体上应考虑的事项：
   1) 数据采样频率和冗余度；
   2) 预处理和一致性检查；
   3) 异常工况所需的分析；

4) 输出要求和输出形式，例如：打印或屏幕显示等。

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处理时间。类似的，任务分析、数据输出和显示也要消耗数据处理器处理时间。因此，在数据采集和处理系统正式投入使用前，宜估计出正常和数据高峰情况下系统计算机的负荷情况。估计的正确性宜通过在全面安装好的系统上进行适当的测试得到验证，从而表明该系统在核电厂可预期的运行范围内对运行人员的可用性。即使在数据峰值负荷时刻，处理和显示电厂数据或操纵员请求方面，应没有大的延迟。经验表明，当计算机化信息系统的任一项功能有超过 1 s 的系统延迟时，操纵员会失去耐心。在某些情况下，较长的响应时间是可以接受的，例如：访问历史或存档数据，此时应有信息反馈的提示表明此操作正在进行。

尽管某些系统可能仅使用一台计算机来处理数据和提供信息，数据采集和处理系统还是宜配置冗余的计算机或模块，以确保单一故障（频繁发生的是单一故障）发生时系统能够继续提供服务。

7.7.2.3 显示系统

显示系统应作为信息系统的人机接口来设计，设计时应考虑人的能力和特性。显示系统应满足下列要求：

a) 显示系统设计

1) 应使操纵员了解反应堆保护系统和其他自动化系统正在执行的动作，以便可以验证系统状态并执行必要的支持动作；
2) 应使操纵员能分析扰动原因并跟踪其发展过程；
3) 应使操纵员能执行任何必要的手动操作。

显示系统应使操纵员能够判明潜在的安全或可用性方面的危险。

b) 显示系统的主要功能要求

1) 控制室内的显示系统应包括适当的变量。这些变量应与安全分析的假设相符，并与操纵员在正常运行和事故工况下的信息要求一致；
2) 显示器的精度、量程和刻度应符合安全分析的假设和所支持的操纵员任务；
3) 应提供电厂和辅助设施的旁通或人为停运的工况的显示；
4) 与安全重要的信息显示器应置于控制盘上适当位置，并加上特殊的标识；
5) 应依据不同的显示目的选择显示器的合适类型；
6) 显示系统应既提供信息显示又提供报警显示，以综合的方法显示核电厂工况。

c) 显示系统一般采用基于屏幕显示器的方法提供显示和信息。但专用显示器，例如：模拟仪表、数字指示器、指示灯以及趋势记录仪在如下场合也可能被采用：

1) 基于设备鉴定或多样性考虑的事故后工况；
2) 如果要求必须配备专用显示器的场合。

宜配置足够数量的打印机以输出硬拷贝给值班人员，作为团队内部讨论和分析的材料以及用于满足规定的存档需求。

基于屏幕显示器的显示系统的要求见 NB/T 20058；专用显示器的要求见 ISO 11064（所有部分）。

7.7.2.4 报警系统

主控制室报警应提供监视电厂偏离正常运行工况所需的全部信息。

报警系统应能够：

a) 显示报警信息，使操纵员了解事故发展状态。
b) 使操纵员能略去无关的信息，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：

1) 操纵员的纠正操作没有结束的报警；

2） 没有维修工作的介入不可能消除的报警。

d） 避免信息过多使操纵员负担过重。

报警系统还应具有：

a） 处理功能，向操纵员提供异常工况最有代表性的信息；

b） 显示功能，使得操纵员易于辨别某个报警及其严重性。

此外，应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指令，向操纵员说明报警的可能原因和所需的纠正动作。

详细要求见 NB/T 20027。

7.7.2.5 操纵员支持功能

为提高电厂的安全性、可用性和可操作性，宜提供如下操纵员支持功能：

a） 安全参数显示与监视功能(详细内容见 GB/T 13624)；

b） 电厂诊断功能；

c） 正常运行和事故后工况下的操作指导功能，例如：基于状态的运行规程与基于事件的运行规程；

d） 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。

7.7.3 控制功能

本条涉及在正常与异常运行中手动操作及自动化的后备操作所使用的控制器与人因相关的功能性要求，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：

a） 总体思路：控制器的设计应保证操作简便，并使操纵员的差错最少。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特征相适应。控制器应满足以下要求：

1） 为使操纵员差错最少，控制器的动作方式应符合公认惯例并且应与被控变量匹配；

2） 控制器应包含被选功能项的反馈信息和被控组件状态的核对信息显示；

3） 控制功能的分类应与它们对安全的重要性相适应，满足 GB/T 15474 的要求。

b） 错误操作的防止：为防止人为的事件，控制器的错误操作应用下列方法减到最少：

1） 将控制器安置于适宜的位置，防止在任何操作过程中意外地被触动；

2） 使用保护结构，例如：使用实物屏障、隐藏式安装法或使用可移动的盖板或挡板；

3） 提供二次确认动作，例如：使用释放按钮或附加的软控制命令；

4） 使用联锁或允许信号，并对信号进行适宜的优先级分配；

5） 选择适宜的控制器件的机械特性，例如：尺寸、操作压力或操作力、触觉反馈、光学和(或)声学反馈等；

6） 以上措施的组合。

c） 技术：控制功能可通过软控制器、多用途控制器、专用控制器，或者它们的混合方式实现。宜根据如下原则做出选择：

1） 鉴定和独立性考虑；

2） 所需的访问速度和使用频率；

3） 可行的技术。

详细要求见 NB/T 20059。

7.8 控制与显示的组合

控制器和它们相关的显示器应正确地组合，以使控制室人员能保证电厂有效地运行。

控制与显示设备的组合应符合按 6.2 和 6.6 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应满足以下基本要求：

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) 控制器与相关的显示器的编组应反映完成系统目标的需要，并宜与使用者头脑中的核电厂模型一致；

c) 控制器与显示器的编排应反映因果关系；

d) 控制器的编排应体现使用者的习惯；

e) 显示器和相关的控制器所使用的编码形式应完全一致。

7.9 通信系统

7.9.1 一般要求

在控制室内应提供通信系统以便于电厂安全与有效运行。对于在异常或事故工况下用于与应急设施联络的通信系统的设计，应给予专门考虑。

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，有必要设置非语言的通信系统，例如：电话传真、计算机之间的数据链。

7.9.2 语言通信系统

7.9.2.1 厂内通信

应提供分机数目足够的电话系统，用于正常运行工况下的一般联络。至少有一台电话分机应安装在控制室内。每台电话分机可以与公用电话系统连接。在控制室内应额外提供一台专用的应急电话分机，公用电话系统不能与它接通。这台电话分机的号码应为人熟知，并标记在所有电话分机上，只用于向控制室人员传送异常和事故报告。

应在适当地方安装一个独立的、直通的电话系统，以便在事故或紧急工况下与安全重要的辅助操作设施和控制点通信。系统应使控制室人员能进行一对一的通信或同时与选定的数台电话分机并行通信。系统还应使控制室人员能与同一厂址内具有独立控制室的任一其他机组的控制室通信。系统应由不间断电源系统供电。应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入。该系统也可以在运行中使用。

应提供广播系统，以便在任何电厂工况下寻找厂内人员。

在维护、试验或维修期间，其他通信系统不能可靠到达的地点，应提供便携式无线电对讲机，以无线电方式与控制室通信。在仪表控制系统的设计、电缆敷设、设备布置和试验中，应考虑无线电频率干扰的问题。为了尽量减少这种干扰，应限制并规定这些无线电设备的频率范围和最大输出功率。应确定不可以使用无线电设备的场所，例如控制设备室。

7.9.2.2 厂外通信

为了与厂外的营运单位、急救站、政府和公众机关通信，应提供专用的通信系统。某些电话分机的号码，尤其是控制室的分机号码应不对外公开。

为了与必要的机构和人员及时联络，应提供最低数目的电话外线。重要的联系应具有冗余和多样的系统，例如包含一个电话系统和一个无线电系统。这种通信联系应按照国家标准进行设计，典型的通信联系包括：

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。

7.9.2.3 布置

满足运行通信需要和操纵员间通信需要的通信设备应安装在操纵员工作台上。

控制室还应设计成为正常运行和事故初期的电厂通信中心。在这些阶段使用的通信系统的职责和需求应在任务分析中确定，通信设备应按照分析结果相应布置。与厂外通信的绝大多数设备，最好安放在一个专门的通信桌上，或安装在主控制台和控制盘的延伸面板上。

7.9.3 非语言通信系统

在控制室内，可以提供非语言通信系统，例如：

a) 在事故工况下可能用到的监督反应堆操作平台和汽轮发电机状态的电视系统；

b) 为了紧急状态下传送电厂状态和运行建议，与应急响应设施连接的电话传真系统。

7.10 其他要求

7.10.1 电源

控制室的电源装置的可靠性与可用性应符合与仪表控制系统、安全系统以及安全重要系统的要求。控制室内的安全重要系统需要在正常运行和事故工况下全时可用，应由不间断电源供电。

控制室的供电要求见 NB/T 20071。

7.10.2 鉴定

应制定一个与整个核电厂设备一致的鉴定大纲，以证实控制室中的安全重要设备和系统，在需要它们运行时可能出现的环境条件下能连续地满足设计基准性能要求（例如：量程、精度、响应时间）。该大纲应包括保证设备预期的使用寿期的鉴定计划，如必要的话，还应提出及时复检或更换的要求。

鉴定的技术要求见 GB/T 12727 和 GB/T 13625。

7.10.3 可维护性

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

在设计阶段应估计修复时间对可用性的影响。在每个特定系统的设计基准中应规定平均修复时间和检查频度。探查发生故障的方法，例如电源系统检查（试验），应是这种估计的一部分。

系统维护的手段应设计成对电厂安全的任何影响应是可接受的。

7.10.4 维修

控制室的设计应考虑控制盘的布置和设备配置，应使其里面的系统和设备易于维修。设计还应考虑维修设施和备品备件。

7.10.5 可试验性

控制室应设计成在必要的时间段内，可以对每项必需的功能方便地进行试验与校验。

8 控制室系统的验证与确认

8.1 一般要求

在整个控制室系统（包括控制室人员的配备、人机接口、运行规程和培训大纲）的初步设计完成之

后，应对控制室系统的设计是否适当进行验证与确认。本章规定控制室人机接口验证与确认的工作过程和基本评价准则。有关控制室系统其他组成部分，如：人员结构、运行规程和培训大纲的评价，其工作过程和准则宜参照有关标准和导则（参考 IAEA 安全导则）另行规定。

详细技术要求见 EJ/T 1118。

8.2 控制室系统的验证

8.2.1 一般要求

在控制室系统的详细设计之前和之中，应对控制室系统的功能技术要求进行验证，以证明它能满足相关准则和功能要求。

8.2.2 验证过程

验证的工作过程应包括准备、评价和总结三个阶段。在这个阶段应对集成的控制系统进行评价，其中包括运行规程和培训大纲（已分别提供）的评价，如图 2 所示。

8.2.3 验证的基本评价准则

控制室系统整体应正确地体现了全部功能要求和所有其他技术要求。

8.3 控制室系统的确认

8.3.1 一般要求

在控制室系统的详细设计之前和之中，整个控制室系统综合体应经过确认，以证明能达到预期的性能，应特别关注控制室系统综合体与时间相关的动态特性。

8.3.2 确认过程

确认的工作程序应包括准备、评价和总结三个阶段。

确认的准备工作用类似于功能分配确认的方式（见 6.5）进行。在此阶段中，运行经验是特别重要的。

宜制作一个适当的控制室模型，便于评价控制室系统与时间相关的动态特性。对于设计概念与常规系统有明显差异的系统，有必要采用动态模拟器进行确认。如果与现有系统的差异较小或局部确认可以完成时，可以采取其他方法，例如全尺寸的模型。

宜设置多种性能度量，便于多方面评价。相互有关的性能度量，应检查定性与定量两者的一致性，以便确认评价的结果。

宜考虑建立接近真实的试验环境，例如：实体布局、环境条件（温度，湿度，照明，音响）等。

部分确认工作可以利用现场调试来实施。例如，在早期设计阶段无法进行试验的确认项目（例如控制室撤离）和需要进一步评估才能确认的项目，可以利用现场调试来进行。

8.3.3 确认的基本评价准则

评价的准则应与所有有关的管理条例、标准和导则等一致。

详细的技术要求见 EJ/T 1118。

附 录 A
（资料性附录）
概 念 解 释

A.1 控制室系统

人机接口、控制室人员、运行规程、培训大纲和有关的设备与设施的综合体称之为控制室系统（参见图 1）。

核电厂有两个基本的运行目标：按需要发电和防止放射性物质向环境释放。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来控制电厂的工艺过程。电厂系统的控制主要有两种方式：自动控制和手动控制（包括远程手动控制和就地手动控制）。

实现自动控制和远程手动控制的硬件系统包括电厂控制和安全系统（仪表控制系统的一部分），还包括驱动器、传感器和其他硬件设备。

自动控制的运行需要控制室人员通过显示器监督其执行情况，并在必要时采取手动控制，包括自动控制的后备控制、复原等。远程手动控制的运行需要控制室人员通过安装在控制室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）与控制室人员具有一种实体交接面，所以它们被称为人机接口。

就地手动控制是在控制室人员要求下，由就地操作员在控制室以外任意区域通过就地的控制设施来执行的控制。控制室人员的指令通过通信系统下达。

除了自动控制、手动控制和相应的监督之外，控制室人员需要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。

有各种类型的操纵员支持系统可用于支持高级思维处理，例如：诊断系统，运行专家系统，计算机化的规程系统。控制室人员可以以多种方式与这些系统交互——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信。操纵员支持系统也归入人机接口。

与控制室外的电厂人员和管理工作人员的通信，可以通过通信接口实现。

A.2 “人”和“机器”

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。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“人”代表控制室人员，机器则代表自动化。（参见表 A.1）

术语“机器”涉及许多硬件实体，它包括仪表控制系统和操纵员支持系统。应该注意的是，属于仪表控制系统一部分的手动控制系统、控制器和显示器，使控制室人员能完成分配给他们的功能。

表 A.1　功能范畴和实体范畴中的人和机器

<table>
<tr><th colspan="2">功能范畴</th><th colspan="2">实体范畴</th></tr>
<tr><th>功能承担者</th><th>应完成的功能</th><th>机器（硬件）</th><th>人</th></tr>
<tr><td>人</td><td>高级思维处理
监督（包括手动与自动控制有关的监督）
手动控制（包括自动化的后备控制）</td><td>操纵员支持系统
显示器
控制器
手动控制系统
人机接口
仪表控制系统</td><td>操纵人员</td></tr>
<tr><td>机器</td><td>自动控制</td><td>自动控制系统</td><td></td></tr>
</table>

中华人民共和国
国家标准
核电厂控制室设计
GB/T 13630—2015
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
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 48 千字
2015年11月第一版 2015年11月第一次印刷
*
书号:155066·1-52866 定价 27.00元

GB/T 13630-2015

书印日期 2016年1月12日 F009B