核安全导则　HAD 102/21-2021

核动力厂人因工程设计

（国家核安全局 2021 年 12 月 17 日批准发布）

国家核安全局

核动力厂人因工程设计

（2021 年 12 月 17 日国家核安全局批准发布）

本导则自 2021 年 12 月 17 日起实施

本导则由国家核安全局负责解释

本导则是指导性文件。在实际工作中可以采用不同于本导则的方法和方案，但必须证明所采用的方法和方案至少具有与本导则相同的安全水平。

目 录

1 引言

1.1 目的

1.1.1 本导则是对《核动力厂设计安全规定》（HAF102）有关条款的说明和细化。

1.1.2 本导则为人因工程应用于人机接口设计和改造提供一种结构化的方法和指导，以便最小化人员失误风险、优化人员效能，保证核动力厂的安全运行。

1.2 范围

1.2.1 本导则适用于人因工程在新建核动力厂的人机接口设计、运行和维护中的应用，也适用于现有核动力厂的人机接口改造。

1.2.2 本导则适用于核动力厂设计、建造、运行和退役阶段的分析、验证和审查，技术支持以及核安全监督。

1.2.3 本导则明确了设计和确认人机接口所必需的有关人的生理和认知过程的基本输入信息。

1.2.4 本导则不涉及核安保目的的人因工程应用。

2 人因工程管理

2.1 总则

2.1.1 应在核动力厂的设计、调试、运行和维护中运用人因工程，以确保充分考虑了人的特性与能力。

2.1.2 应对人因工程在设计中的结合进行规划和记录，并使其成为核动力厂项目的组成部分。

2.1.3 应制定人因工程大纲，并形成文件。

2.1.4 在人因工程大纲中，核动力厂应被视为由人、技术、组织构成的一个系统，应考虑所有相关因素内部和各因素之间的动态相互作用：

— 人的因素（如专业知识、认知、效能期望、动机、压力、人体的力量和尺寸）；

— 技术因素（如控制与显示、软件、硬件、工具、设备、核动力厂设计和核动力厂工艺）；

— 组织因素（如管理体系、组织结构、管治、资源、人员编制、管理者和其他核动力厂人员的角色与职责）。

2.1.5 在为所有核动力厂状态设计人机接口和分配资源的过程中，人、技术和组织以及它们之间的相互作用，应在人因工程大纲的规划和整个项目执行过程中统筹考虑。

2.1.6 在人因工程大纲中，在已有的设计方法和解决方案基础上，应考虑技术的发展，如新开发的信息技术、分析方法、知识和新技术的特点。

2.1.7 人因工程的实施应采取分等级应用的方法，以确定适当的严格程度、资源和应用细则。

2.1.8 人因工程大纲应概述人因工程活动及其输入与输出。人因工程活动包括管理、分析、设计、验证与确认、设计实现和人员效能监测。

2.1.9 人因工程大纲应详细说明人因工程是如何与核动力厂的设计或改造活动相结合的。

2.1.10 人因工程大纲应确定负责人因工程的人员与项目和

设计主管部门，以及与核动力厂其他组织单位人员之间的必要协调活动。

2.1.11 人因工程大纲应建立将分析结果传递至责任部门的流程，并要求记录存档，同时保证分析结果已被落实。

2.1.12 人因工程大纲应明确参与人因工程活动人员的组织要求和能力要求（如资质、技能、知识和培训）。

2.1.13 人因工程大纲应建立一个架构，用于记录并跟踪人因工程活动中识别出的相关问题。

2.1.14 人因工程大纲应规定设计团队有具备人因工程专业知识的成员。

2.1.15 在新建核动力厂的设计中，营运单位应确保预期的核动力厂设计满足适用的人因工程标准以及本导则的建议。

2.2 人因工程过程模型

完整的人因工程过程可分解为以下活动：

— 管理；

— 分析；

— 设计；

— 验证与确认；

— 设计实现；

— 人员效能监测。

2.3 工程项目中的人因工程活动

2.3.1 人因工程活动应结合到工程项目的各个阶段，具体见图 1。

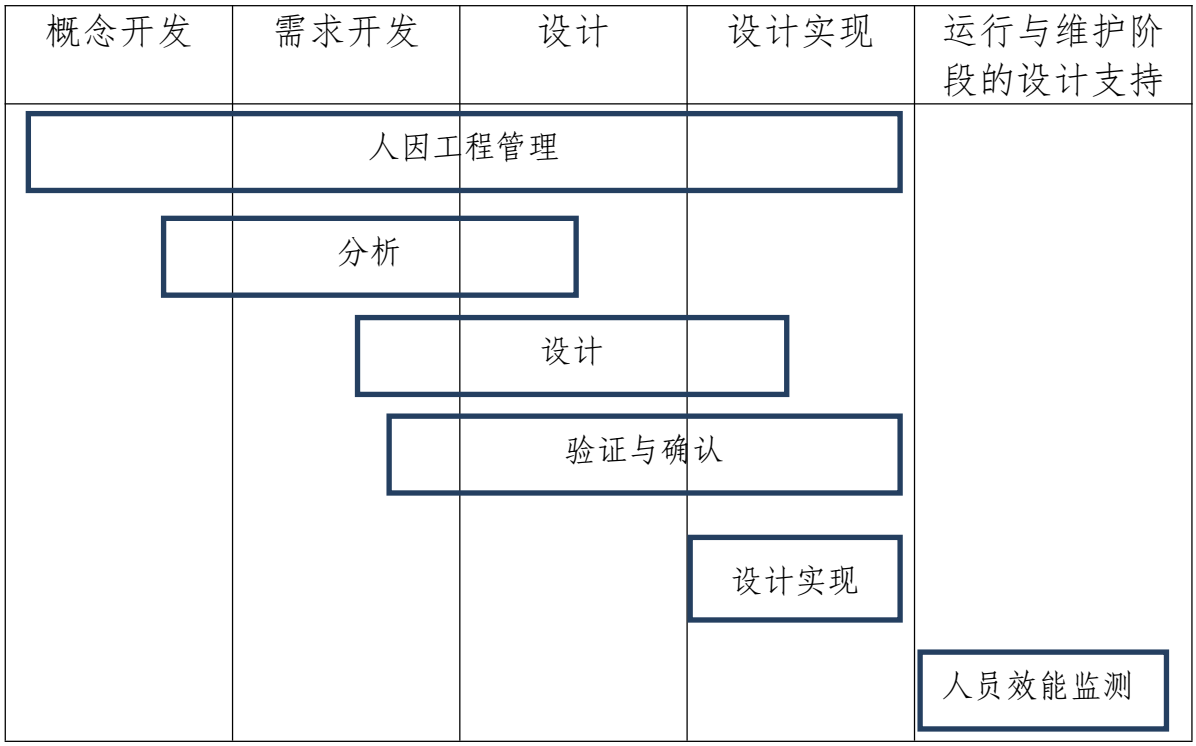

图 1 工程项目各阶段开展人因工程活动的示例

2.3.2 在概念开发阶段，人因工程应考虑给工程设计提供以下输入:

（1）人因工程大纲应确定一个系统的、完整的人因工程过程，应概述人因工程的职责，并描述人因工程过程的预期设计输入与输出;

（2）人因工程大纲应规定在所有层级建立一个有能力的组织来负责人因并被充分授权，以便实现必要的设计变更来满足人因工程期望;

（3）人因工程大纲应确定适用于工程项目的、人因工程相关的最新法规、标准、方法论、导则;

（4）人因工程分析应识别相关的经验反馈（包括正面的与负面的），重点关注人员效能问题以及潜在的人的失误及缓解措

施;

（5）人因工程分析应为制定与选择相关的设计方案提供必要的输入，如操纵员的需求与要求;

（6）应通过人因工程分析确定组织结构，形成人因工程大纲的使用框架，即识别用户以及他们的角色和职责、所需资质和监管要求，以支持运行和维护;

（7）人因工程分析应对功能分配以及人员监控的信息需求提供初步评价，在适用的情况下，还应提供对核动力厂系统功能的初步评价;

（8）人因工程分析应提供在控制系统及人机接口故障时，操纵员预计将如何应对的分析与考虑。

2.3.3 在需求开发阶段，人因工程应考虑给工程设计提供以下输入:

（1）确定构筑物、系统和部件功能需求的功能分析结果;

（2）提供以下内容的任务分析结果:

— 必要的报警、信息、规程、控制、系统反馈;

— 可能的任务序列;

— 潜在的人的失误与影响人员效能的因素，并提供减少错误和提高效能的设计要点;

— 对于安全重要的、复杂的任务，需要进行详细的技术分析和人因工程分析;

— 重要任务的时间限制;

— 人员完成其所分配任务并实现操作目标所需要的专业的知识、技能和能力;

— 完成任务所需的人或组织之间的协作。

（3）特定的人因工程设计原则和人机接口设计指南，用于制定对供应商的技术规范，并将其纳入供应商的人因工程规范。

2.3.4 在设计阶段，人因工程应考虑给工程设计提供以下输入:

（1）因设计发展和标准变化而更新的人因工程要求;

（2）特定的人因工程设计原则以及人机接口设计指南，用于规范核动力厂和工作场所的设计与布局、人机接口部件及结构;

（3）用于维护和试验的特定的人因工程设计原则和人机接口设计指南;

（4）关于人员效能的新设计或设计修改的潜在影响，以及规程和培训的开发;

（5）通过以可用性测试和对原型和概念的用户审查形式进行的早期人因工程分析，对用户反馈进行的收集和分析;

（6）对支持安全关键任务执行的运行规程的范围、内容和可用性的深入分析;

（7）对培训范围和内容的深入分析。

2.3.5 在设计实现阶段，人因工程应考虑给工程设计提供以下输入:

（1）根据先前确定的人因工程设计原则和适用的人因工程设计法规、标准和导则，验证设计实现;

（2）验证设计实现，以确保在设计中提供执行任务所必需的所有信息与控制;

（3）从人因的角度进行确认，以确定人机接口设计及其机

械设施在多大程度上有助于核动力厂安全运行;

（4）从人因的角度进行确认，证实在概率论和确定论安全分析中的重要人员任务的可行性;

（5）确认人因工程分析以及用于设计的人因工程输入符合人因工程大纲和监管预期。

2.3.6 在整个设计过程中，应考虑技术的约束条件（如可用性、可靠性、适用范围以及人员对技术的普遍的接受程度与熟悉程度）。例如：尽管人们在日常生活中已接受了数字技术，设计者仍需考虑采用虚拟现实或增强现实是否给人带来困难。

2.3.7 人员效能监测应在运行与维护阶段进行，以验证设计阶段的分析与假设在核动力厂的整个生命周期依然有效。

2.3.8 用于分析、设计、验证与确认的人因工程活动应在整个工程设计阶段迭代执行。

2.3.9 支持分析、设计、验证与确认的人因工程活动大多需要协作完成，应由一个具备人因工程专业知识的多学科团队来共同完成。人因工程分析、设计、验证与确认活动的结果应传递给参与设计的相关单位和部门，以便进行正确处理。

2.3.10 人机接口及其功能应作为统一整体的一部分进行处理，而不仅仅是控制器、指示器、系统的离散组合。

3 分析

3.1 运行经验评审

3.1.1 应对具有重要安全影响的事件进行调查，以查明其直接原因和根本原因，包括与设备设计、运行与维护、人员或组织

因素有关的原因。

3.1.2 从事件分析得到的数据与结论应作为新建核动力厂设计或现有核动力厂改造的人因工程输入。

3.1.3 运行经验评审应提供关于当前工作实践的信息，目的如下:

（1）评估计划变更的潜在影响;

（2）评估当前设计中的运行问题和困难，这些问题可能需要在核动力厂升级和设备改造过程中解决;

（3）评估与仪控系统和人机接口技术的设计选项相关的工业经验对提高核动力厂安全和效率的潜在作用。

3.1.4 运行经验评审过程中，效能和设计的正面和负面经验都应进行分析。

3.1.5 运行经验评审应考虑以下因素:

（1）核动力厂运行经验评审中识别出的适用于人因工程的相关问题;

（2）从核动力厂工作人员识别出的经验中所获得的技术分析;

（3）其他核动力厂及其他工业运行经验评审中识别出的问题。

3.1.6 应考虑以下运行经验数据:

（1）是更重大事件的前兆或促成因素的小问题，例如：未遂事件或低级别事件;

（2）能够表明可靠性下降的不利趋势;

（3）需要进行设计改进的根本原因数据;

（4）组织文化中可能会影响未来运行造成问题的证据;

（5）纠正措施与实施;

（6）重复发生的事件;

（7）维护实践的评审;

（8）行业良好实践。

3.2 功能分析

3.2.1 应针对所有核动力厂状态进行功能分析，以确保完成核动力厂安全运行所必需的功能得到明确的定义和充分的分析。

3.2.2 功能分析应提供说明，以便于理解人在核动力厂控制过程中的角色。

3.2.3 应通过功能分析确定人完成运行目标所需要的信息（例如：功能何时需要、何时可用、何时运行、何时达到目的或终止）与控制。

3.2.4 功能分析应提供执行功能所需的时间和性能要求及限制条件。

3.2.5 功能分析应考虑人、技术和组织因素。

3.2.6 应通过功能分析确定与维持核动力厂安全运行相关的高层次验收准则。

3.2.7 以下内容应作为功能分析的一部分进行分析并存档:

（1）确保核动力厂安全运行的高层次功能;

（2）高层次功能与执行这些功能的核动力厂系统之间的关系（例如：核动力厂配置或“成功路径”[1]);

1“成功路径”是所选构筑物、系统、设备的一个组合，该组合能高度确保核动力厂在事故发生后成功地达到安全状态。

（3）将高层次功能分解为可自动执行、手动执行或手/自动执行相结合的低层次功能;

（4）确定人与自动控制的角色与职责的框架。

3.2.8 实现高层次功能所需系统及过程和成功路径所需人员行为的组合应作为功能分析的一部分进行存档。

3.2.9 核动力厂功能、系统以及支持系统之间存在的相关性应作为功能分析的一部分进行存档。

3.3 功能分配

3.3.1 应针对所有核动力厂状态进行功能分配，以确保实现核动力厂安全运行所必需的功能得到充分明确的定义和恰当的分析。

3.3.2 进行人与自动控制的功能分配时，应考虑到人的能力（例如：改进能力、灵活性、判断与状态探查的能力）和机器的优势（例如：复杂操作的快速性与并行处理能力）。

3.3.3 进行功能分配时应考虑人、技术和组织因素。

3.3.4 设计团队应利用工艺过程知识、当前工业技术、运行经验以及人员效能的优势和弱点，将功能分配给人和自动控制（如硬件和软件等）。

3.3.5 功能分配应利用核动力厂控制系统的功能分析，建立控制过程的功能分配，可按以下方式分配:

（1）分配给人，如手动控制（无自动控制）;

（2）分配给自动控制系统，如全自动控制和非能动控制;

（3）分配给人与自动控制的组合，例如:

— 共同操作，即：一个功能的某些方面为自动执行，其他

方面则是手动操作;

— 经过批准或授权的操作，即：当得到人员许可且条件允许时，功能通过自动控制实现;

— 例外操作，即：功能通常通过自动控制实现，除非有特别预定义的情境或必须要手动操作的情况。

3.3.6 在功能分配时，除了考虑人的能力，还要考虑诸如技术是否可被人接受、系统响应的及时性、纵深防御等因素。

3.3.7 如果控制功能的实现需要将重叠和冗余的职责分配给人和自动控制（例如：将对于自动控制系统的监视并维持监督控制的责任分配给人），则应对该分配进行记录并存档。

3.3.8 对于所有功能，人员任务的性质和范围应进行记录并存档。

3.3.9 应分析不同运行状态和事故工况下的功能分配。

3.3.10 功能分析与分配应考虑严重事故管理指南实施的要求。

3.3.11 功能分配应可从功能追溯至相关系统或部件。

3.4 任务分析

3.4.1 任务分析的方法应考虑核动力厂状态和与此任务相关的运行和维修班组人员，如反应堆操纵员、汽机操纵员、值长、现场操作员、安工、运维人员。

3.4.2 任务分析应考虑人、技术和组织因素（如领导、管理和沟通）。

3.4.3 任务分析应对人员执行任务相关的身体活动与认知活动进行分析并存档。

3.4.4 任务分析应从任务执行者的角度来分析任务内容及其关系。

3.4.5 由于核动力厂个体的角色与活动的宽泛性，任务分析应确定分析的范围，一般包括以下内容:

（1）不同地点（例如：主控制室、辅助控制室、就地控制站、应急控制中心）需要执行的任务;

（2）取决于核动力厂状态的不同任务;

（3）需要个体完成的任务和/或需要在不同组织（运行、维修、规程编制、计算机系统工程）和相关方之间沟通协作的任务;

（4）必须要在时间压力或恶劣的环境条件和背景下执行的任务，或对安全至关重要但很少被执行的任务。

3.4.6 在确定需要进行分析的任务时应考虑风险与安全因素，包括以下任务:

（1）对人员造成职业风险的任务;

（2）安全分析中置信的任务;

（3）从运行经验中识别出的具有挑战性的或易于出现失误的任务;

（4）操纵员确定为高难度任务，且未制定自动实施计划;

（5）对于维持核动力厂处于安全状态或事件发生后将核动力厂恢复至安全状态具有关键意义的任务。

3.4.7 任务分析应分析对报警的响应，以及操纵员从控制室下达的监视和维护任务。

3.4.8 任务分析的结果应有助于识别以下内容:

（1）对安全有影响的预期人员任务和潜在的人员失误;

（2）关于如何执行每项任务的期望，预期的任务效果，任务的人员效能的可靠性评估;

（3）安全关键任务的防失误措施;

（4）各项任务的开始与终止条件以及受影响的安全功能;

（5）执行任务和子任务的顺序;

（6）人员需求（如组织方面、人员配置、资质与培训），设备需求（如人机接口、专用工具、防护服），文件需求（如程序、工艺流程和操作指南）;

（7）人员效能要求和限制（如时间、准确性和独立验证）;

（8）所需的通信系统及其使用。

3.4.9 任务分析时应考虑以下信息来源:

（1）文件（如供应商文件、技术规范、已有程序、手册和培训教材）;

（2）来自专家的信息，包括设计团队专家、有类似核动力厂运行经验的运行人员、相关方以及其他行业专家;

（3）通过排演、推演分析以往系统和相似核动力厂执行的任务，以及与正在开发的系统有关的任务;

（4）运行经验评审的数据（考虑与参考设计的差异）;

（5）用户需求数据;

（6）其他用做人因工程设计输入的数据（如功能分析与分配、重要人员任务处理）;

（7）来自模拟机研究的数据;

（8）国内外相关的人因工程标准。

3.4.10 应论证任务分析所使用的技术选项的适用性。

3.4.11 应评估任务执行需求对人员可靠性的影响。

3.4.12 对任务分析输入进行收集、列表和分析的一系列过程应存档。

3.4.13 任务分析是一项协作活动，应由具备人因工程专业知识和运行专业知识的多学科团队来共同完成。

3.4.14 任务分析结果应传递给参与设计的相关单位和部门。

3.4.15 任务分析结果可直接用于支持人的失误评估。

3.4.16 应特别针对重要的认知活动（如决策、问题解决、记忆、注意力和判断）进行任务分析。

3.4.17 当仅对文件（如规程）进行书面分析不足以确定任务可否执行时，可通过实物模型仿真、核动力厂实地考察、部分任务模拟机或全范围模拟机支持的模拟，来确定任务在真实场景中的可行性。

3.4.18 任务分析应包含对错误进行分类的方法，该方法至少能得出每项任务潜在的疏忽/遗漏错误和执行错误，包括决策错误、沟通错误。

3.5 人员配置、组织和资质的分析

3.5.1 应分析人员配置、组织架构、人员资质对重要人员任务的影响，以确定人员需求数量、组织交互和人员资质。

3.5.2 对于运行核动力厂的改造或新建核动力厂，应进行人员配置、组织和人员资质的分析，考虑相较参考核动力厂的所有变更，这些变更可能会影响:

（1）人员任务的安全执行;

（2）人的工作负荷;

（3）使每个团队成员的贡献与团队任务相一致的能力;

（4）负责检查任务进度（例如：检查操纵员在控制室和就地执行的行动）的个人的独立性与合作性;

（5）对任务及其作用的认识，以及人对任务的接受度。

3.5.3 人员配置、组织和资质分析应涵盖执行影响安全任务的所有团队（见 3.4）。这包括所有运行值、服务支持团队、应急准备与响应团队。分析应识别并评估这些团队在人员配置、组织、资质方面的需求。

3.5.4 人员配置、组织和资质分析应评估与参考核动力厂的组织和技术差异的影响。

3.5.5 人员配置、组织和资质分析的输入应包括:

（1）运行状态和事故工况下的运行概念方案;

（2）设计需求;

（3）任务需求;

（4）监管要求;

（5）运行经验;

（6）重要人员任务的处理（例如：对重要人员任务的处理可能确定需要启用两人规则，以确保可靠地完成某些任务）。

3.5.6 任务分析应用于支持对团队角色、需求、责任及必要输出的定义。

3.5.7 在给团队成员分配个体任务时应考虑以下几点:

（1）分配给每个成员的任务清晰明了;

（2）任务分配的依据是确定的、合理的;

（3）在所有运行工况和事故工况下，每个成员的工作负荷

是合适的;

（4）在白班和夜班团队间分配任务时，应考虑对人员效能的影响;

（5）不同运行工况下的任务应以某种方式分配给团队成员，这种方式要确保职责的连续性，并保持个人与团队的情境意识。

3.5.8 任何人员配置的减少都应通过建模、分析以及全范围仿真试验评估其对安全的潜在影响。

3.6 重要人员任务处理

3.6.1 重要人员任务和动作应通过概率论或确定论的安全分析来识别。

3.6.2 确定重要人员任务的基本方法应同时考虑运行状态和事故工况下的响应。

3.6.3 支持人因工程在设计中应用的分析可采用定性或定量分析的形式。

3.6.4 至少应对安全分析中置信的操纵员任务与动作进行分析，包括影响效能的相关因素。应确认设计方案能满足与人员效能相关的安全要求。

3.6.5 无论采取什么方法识别重要人员任务，设计、规程、培训、人员配置水平和运行概念应支持重要的人员决策与动作。

3.6.6 核动力厂改造可能会改变重要人员任务的执行方式。所有核动力厂改造都应评估相关的重要人员任务是否仍然能够可靠地执行。

4 设计

4.1 总则

4.1.1 必须在核动力厂设计过程初期就系统地考虑人因（包括人机接口），并贯彻于设计全过程。

4.1.2 设计必须支持运行人员履行职责和执行任务，并必须限制操作差错的可能性及其对安全造成的影响。设计过程必须适当考虑核动力厂布置、设备布置、以及包括维修程序和检查程序在内的有关程序，以便于在核动力厂各种状态下运行人员和核动力厂之间的互动。

4.1.3 人机接口的设计必须能按照决策所需时间和行动所需时间给操纵员提供全面且易于管理的信息。向操纵员提供的用于决策和行动所需的信息必须简洁明了且无歧义。

4.1.4 应采用结构化方法开展人机交互设计，可进行概念设计、备选人机接口方法的识别和选择、详细设计，以及必要时开展人机接口测试和评估。

4.1.5 应将纵深防御的理念应用于人机接口设计，以保证故障一旦发生可以被探查到，并可以通过采取适当措施进行弥补或纠正。

4.1.6 设计应采用以人为中心的方法，从执行相关功能和任务的人员的角度来考虑设备和系统。

4.1.7 人员、技术（包括硬件和软件）、工作环境以及使用的控制、运行和管理策略，应在设计全周期的所有阶段予以考虑（按照集成的和系统的方法）。

4.1.8 设计应考虑人机接口信息如何在不同组织人员（例如：主控制室人员和其他应急响应设施人员）之间进行传递、交换和使用。

4.1.9 设计应考虑必要的约束，并确保设计的灵活性，以便采用不同的控制和运行策略来应对不同的核动力厂状态和运行模式。

4.1.10 应通过如下检查，为运行人员和组织弹性[2]提供设计考虑：

（1）是否恰当地为假设始发事件的响应分配了自动动作；

（2）人机接口是否能够支持预测并响应一个非预期事件；

（3）人机接口是否提供预期突发中断或故障条件下渐进式变化的有关信息（例如：使用预测性显示）；

（4）是否提供额外的工具和设备及其放置场所；

（5）营运单位通过核动力厂系统对严重事故的响应而实施的“压力测试”，是否为操作人员如何将设备用于不同于最初目的而是为了保护裂变产物边界提供了分析；

（6）当一个事件发展后，是否必须采用不同运行策略以达到安全状态；

（7）设备能否超越设计意图，以支持其他不同的策略（例如：使用消防系统带出余热）。

4.1.11 人机接口设计输入

4.1.11.1 应从设计早期阶段（见第 3 章）的以下分析中识别

2 指组织应对逆境的能力，在面对异常、令人担忧的或意想不到的威胁之后，能够恢复和回到常态。

出人机接口设计中需考虑的要求:

（1）运行经验评审;

（2）功能分析和功能分配;

（3）任务分析;

（4）人员配置、组织和资质的分析;

（5）重要人员任务处理。

4.1.11.2 人机接口设计中需要考虑的重要输入包括:

（1）总体仪控系统的限制（例如: 传感器数据的可用性对可提供信息的限制）;

（2）配置人机接口的物理环境;

（3）用户的认知局限和能力;

（4）不同专业组人员的知识、技能和能力;

（5）适用的监管要求。

4.1.11.3 人机接口设计应支持核动力厂运行人员完成任务，应考虑在功能分析和功能分配中所确定的自动化水平。

4.1.11.4 任务分析结果应为人机接口设计提供以下输入:

（1）在各种状态下（从正常运行到事故工况）控制核动力厂的必要任务;

（2）详细的仪表与控制要求（如显示范围、精度、准确度、测量单位等的要求）;

（3）有关任务支持方面的要求，包括可居留性（如照明和通风要求）。

4.1.11.5 人员和资质分析结果应为人机接口设计提供输入，以确定控制室总体布置方案以及每个控制台、盘和工作站上的控

制和显示的分配。

4.1.11.6 在设计中应用人因工程的特定指南应记录存档，并用于设计人机接口特性、人机接口布局及其部署环境。

4.1.11.7 上述特定指南应规定人机接口要素的详细设计准则。如果运行核动力厂的人机接口要进行升级改造，则应根据人机接口升级改造和运行概念，对特定指南的任何必要修订进行评价。

4.1.11.8 应基于通用的人因工程指南和与人机接口设计相关的分析来开发人因工程特定指南，并明确地反映出在处理人机接口设计的某些具体方面的设计考虑。

4.1.12 人机接口的详细设计及其与核动力厂总体设计的结合

4.1.12.1 人机接口应给操纵员提供必要的信息以便探查核动力厂状态的改变、诊断状态、采取行动以及确认手动或自动动作。

4.1.12.2 人机接口设计应在各种环境条件下（如丧失照明、烟尘、高放水平、水淹、蒸汽进入和有限通风的情况）支持人员效能。

4.1.12.3 人机接口各个方面（包括控制、显示布置、编码方法）应与操纵员的心智模型和固有习惯保持一致。

4.1.12.4 信息的呈现方式应使操纵员对核动力厂状态的理解以及控制核动力厂的必要活动最优化。

4.1.12.5 不同信息和不同场所仪控设备的人机接口的操作方式和呈现形式应保持一致。

4.1.12.6 人机接口的设计应尽可能地防止并探查操纵员失误，特别是可能在错误条件或不恰当的核动力厂配置情况下采取行动时。设计要保证能够对控制系统、监测系统、保护系统的定值改变进行确认。

4.1.12.7 当出现错误信息时，人机接口设计应给操纵员提供足够的信息来支持他们做出决策。

4.1.12.8 信息流程图和控制动作应尽可能地与信息处理能力及操纵员效能匹配。

4.1.12.9 人机接口设计:

（1）应尽实际可能地适应与核动力厂有交互的各种运行人员的不同岗位和职责;

（2）应重点关注负责设备安全运行的操作人员的角色;

（3）应支持控制室人员建立共同的状况认知，例如：通过大屏幕显示核动力厂状态;

（4）应提供一个有效的核动力厂状态总貌;

（5）应尽实际可能地从使用者角度，采用满足功能和任务要求的最简单设计;

（6）应以能使操纵员快速识别并理解的方式呈现信息（例如：考虑人的信息处理能力以及视觉注意力）;

（7）应适应模拟和数字显示的故障，不导致重大的控制动作的中断;

（8）应反映出对人员认知、生理特征、人体运动控制特征和人体尺寸的考虑。

4.1.12.10 人机接口应对探查到的操纵员失误提供简单且易

于理解的提示，并能够提供简单有效的恢复手段。

4.1.12.11 应设计和比较人机接口程序和培训大纲，以确保彼此的一致性。

4.1.12.12 所有的描述性的标识和标签应考虑使用同一种语言和协调一致的描述。

4.1.12.13 人机接口设计应考虑对其进行检查、维护、测试和维修而不影响其他的核动力厂控制活动。

4.1.12.14 人机接口设计应支持在最小、典型或优化人员配置条件下完成任务。

4.1.12.15 如果要进行人机接口改造，则新的人机接口应:

（1）与已有人机接口的设计指南保持一致，这样新旧设备对于操纵员来说接口相似;

（2）尽可能与任务分析中用户现有的收集和处理信息、执行动作的策略保持一致。

4.1.12.16 如果修改人机接口，减少任何显示信息都应经过设计工程师、人因工程师和操纵员的论证、评审和一致同意。

4.1.12.17 就地控制站的人机接口设计应与控制室的人机接口设计保持一致。

4.1.12.18 监控安全系统的人机接口设计应采用纵深防御的理念。

4.1.12.19 应说明人机接口是如何进行控制、显示和报警的，以保证正确可靠地执行识别出来的重要人员任务。

4.1.12.20 人机接口设计应考虑必要的补偿动作和支持程序，以保证人员能够有效地应对仪控功能和人机接口的降级，并提供

后备系统切换。

4.1.13 人机接口的测试和评估

4.1.13.1 在人机接口的开发过程中应对概念设计和详细设计的特性进行可用性测试。

4.1.13.2 权衡评价是基于对成功完成任务重要的人员效能的各个方面和其他设计考量，对设计选项进行比较。权衡评价应考虑:

（1）人员任务的要求;

（2）人员能力和限制;

（3）人机接口的性能要求;

（4）检查和测试所需;

（5）维护要求;

（6）用经过验证的技术和先前设计的运行经验。

4.1.13.3 可用性和性能测试包括对人机接口性能的评价（其中包含用户意见），以评估设计选项和设计可接受性。

4.1.14 人机接口控制的设计

4.1.14.1 如果一个控制可以从多个地点实施，例如：分别从主控制室、辅助控制点和就地都可进行控制，则应采取保护措施以保证多个运行人员之间的协调控制。

4.1.14.2 人机接口控制可以通过“软”控制（见 4.1.15）来实现，适用于多路复用控制设备、专用控制设备或两者结合的控制设备。

4.1.14.3 模拟控制设备（如按钮、旋转开关、滑动/拨动开关、摇臂开关）适用于经常使用的控制（如电气输出），以及注重立

即可达和可靠性的控制（如紧急停堆按钮）。

4.1.14.4 控制应及时提供视觉的和/或听觉的反馈，以表明系统已收到了控制输入。

4.1.14.5 控制应与反馈相伴，以展示数据输入过程（例如：调整设定值）并确认数据输入完成。

4.1.14.6 人机接口应保证在执行会产生负面结果的动作时要求采取一些谨慎的操作（如确认按钮、开关上的保护罩），从而使误触发的可能性最小。

4.1.14.7 防止模拟控制误触发的措施包括：

（1）控制器布置在合适的位置；

（2）使用保护结构；

（3）要求二次确认动作；

（4）通过优先级的合理分配，使用联锁或允许信号；

（5）正确选择控制器的物理特性，例如：尺寸大小、操作用力以及触觉、视觉、听觉反馈。

4.1.14.8 为将操纵员失误减到最少，控制动作应符合常规（例如：应符合用户期望），而且应适合控制变量的属性。

4.1.15 软控制的设计考虑

4.1.15.1 软控制是通过视频显示单元与一个定位设备（如鼠标、跟踪球、光笔、触摸屏）共同来实现的，或者是一个视频显示单元与一套专用控制器的集成。

4.1.15.2 以下信息显示方式会极大地影响操纵员使用软控制的效能：选择被控部件的方式、输入的显示区域、输入数据的格式。

4.1.15.3 软控制宜用于交互，例如：选择一个变量或被控部件，提供控制输入并监测系统响应。

4.1.15.4 软控制通过显示设备应做到:

（1）必要时能够访问单个部件;

（2）能够访问每个部件的状态信息;

（3）控制与其他部件的关系。

4.1.15.5 “选择显示”显示一组要控制的部件或变量，它们应有明显的视觉差异，布局清晰，标识唯一，以便能够正确选择。

4.1.15.6 软控制应设计成操纵员能够通过诸如前后关联、视觉上独特的格式、分隔、输入区域、可选部件等特性，一眼就能辨别出选项。

4.1.15.7 常与软控制共用的输入格式包括离散型控制界面、滚动条、箭头按钮。软控制中必须为输入数据提供输入格式。

4.1.15.8 光标应有独特的标识，其移动应灵敏，适合所要求的任务和操纵员技能。光标移动应符合操纵员的捕捉、视觉、舒适度等特性，应能够快速移动并准确定位。

4.1.15.9 人机界面中控制导航的操作应与控制核动力厂的操作（例如：从计算机屏幕启/停泵）区分开来。

4.1.15.10 对于任何特定动作的控制输入，应只向操纵员提供可选项和控件。选项应列在附加于工作显示区的一个菜单中，而不需要操纵员记忆它们或访问一个不同的菜单显示。

4.1.15.11 软控制菜单设计应保持一致，其选项列表的文字和排序在整个人机界面也应一致。

4.1.15.12 为避免执行命令时出现失误，控制顺序应包含:

控制选择、命令选择、命令确认。

4.1.16 人因工程在工作站设计中的应用

4.1.16.1 工作站设计应考虑操纵员的可达性、视野和舒适度等相关特性，如:

（1）工作站的高度;

（2）工作台的倾斜度、控制台的角度和深度，以及可以根据坐姿和立姿调整的工作站;

（3）控制设备的位置;

（4）显示设备的位置;

（5）控制和显示设备在控制台或工作站上的布局;

（6）文本和图形的尺寸和易读性;

（7）容腿和容足空间。

4.1.16.2 控制台的高度应允许操纵员越过它的顶部观看，例如：看到共享显示和其他操纵员。

4.1.16.3 报警面板的位置应可以在主控制室的操作区域看到，并且处在便于操纵员可见和易读的高度。

4.1.16.4 频繁使用的控制器应布置在操纵员的伸展范围内，与之相关的指示和显示设备在操纵员位置即可观察到。

4.1.16.5 应根据功能和工艺运行的特点将其组合成功能组。

4.1.16.6 应根据功能、使用顺序、使用频率、优先级、操作规程或模拟显示[3]布置的系统划分功能组。

4.1.16.7 功能上相关的控制和显示，应与其他功能组的控制和显示区分开来。

3 模拟显示是指在显示盘上模拟核动力厂的实际布置情况。

4.1.16.8 为防止操纵员左右混淆，应避免控制盘、控制和显示设备的镜像布置。

4.1.16.9 应为工作站上的控制、显示和其他设备设置恰当、清晰的标识，以使人员迅速准确地识别相关信息。

4.1.16.10 应采用分层级的标识体系，以减少混淆、缩短查找时间和避免重复。主要标识应用于识别主要的系统或工作站，次要标识应用于识别子系统或功能组，设备标识应用于识别每个部件。

4.1.16.11 标识应描述设备物项的功能，所使用的符号应是唯一的、易于互相区分的。

4.1.16.12 控制盘上标识使用的词语、缩略语、缩写词以及系统和设备编号应保持一致。此外，程序文件和印刻在铭牌上的名词术语之间应保持一致。

4.1.16.13 工作站的设计应考虑必须在工作站进行的测试和维护活动，这种考虑包括:

（1）对盘上部件进行维修、移除或更换的通道;

（2）将仅用于测试和维护的显示和控制设备与用于运行的显示和控制设备分开;

（3）用于特殊测试设备或维修通道的应急空间。

4.1.17 人因工程在可达性及工作环境设计中的应用

4.1.17.1 在需要运行人员监视和控制核动力厂系统的区域，应采取必要的措施确保适宜的工作环境，保护人员免受有害影响。

4.1.17.2 工作环境设计中应考虑的因素包括照明、温度、湿度、噪声和振动。

4.1.17.3 应考虑的危害包括放射性、烟尘以及环境中的有毒物质。

4.1.17.4 确保可达的一种恰当方法是提供受到保护、不受潜在内部和外部危险影响的合格路径，通向辅助控制点和预计操纵员采取行动的其他现场地点。

4.2 主控制室

4.2.1 总体要求

4.2.1.1 核动力厂必须设置主控制室，以进行下述活动：在各种运行状态下以自动或手动方式安全地运行核动力厂；出现预计运行事件和事故工况后，采取相应措施，以使核动力厂保持在安全状态或回到安全状态。

4.2.1.2 必须向操纵员提供能够进行下列工作的必要信息：

（1）评估核动力厂在任何工况下的总体状态；

（2）在系统和设备规定的参数限值（运行限值和条件）内运行核动力厂；

（3）确认启动安全系统所需的安全动作在需要时自动触发，且相关系统按预期要求执行功能；

（4）确定手动启动特定安全动作的必要性和时间。

4.2.1.3 必须采取适当的措施（包括在核动力厂主控制室和外部环境之间设置屏障），并向主控制室人员提供足够的信息，以在较长时间内保护控制室人员免于受到事故工况下形成的高辐照水平、放射性物质释放、火灾、易爆或有毒气体的危害。

4.2.2 主控制室人机接口设计

4.2.2.1 主控制室设计应符合运行概念，运行概念描述了在

所有核动力厂状态下如何运行核动力厂。

4.2.2.2 主控制室的人机接口设计应考虑以下内容:

（1）运行目标和目的，包括安全运行;

（2）工作站人机接口的组织（如控制台和盘);

（3）主控制室中工作站和支持设备的布置。

4.2.2.3 人机接口显示信息应能帮助操纵员:

（1）识别出反应堆保护系统和其他自动系统所执行的动作;

（2）分析产生扰动的原因并跟踪过程;

（3）完成必要的手动干预。

4.2.2.4 主控制室设计应提供高层次的核动力厂状态的综合信息，并支持操纵员在共同任务上的合作，以及他们对彼此活动的了解。

4.2.2.5 在主控制室内应提供显示设备，使操纵员和监督人员能够监视所有安全功能，包括核动力厂状态、安全状态以及重要核动力厂参数的趋势。

4.2.2.6 对于每一特定的任务，应保证人机接口要素和编码（如颜色、形状、线条、标识、缩略语和缩写词）在最低环境照明条件下可从最大可视距离处识别和读出。

4.2.2.7 显示系统应清晰、明确、及时地向操纵员提供所需信息。

4.2.2.8 显示能力应允许操纵员快速评估单个人机接口要素的状态以及它们与其他人机接口要素之间的关系。

4.2.2.9 即使单个输入数据有更高的精度，但数值也应仅显示到运行所需数据的精确程度。

4.2.2.10 显示系统响应时间应符合运行需求。

4.2.2.11 当需要多个操纵员同时干预系统时，一个操纵员的控制输入不能妨碍具有更高优先权的其他控制输入。

4.2.2.12 人机接口设计应考虑到操纵员的共同或协调行动。

4.2.2.13 人机接口的信息应允许操纵员立即评估全厂状态，发现需要给予关注的工况，而不需要完成额外的复杂任务。

4.2.2.14 显示器上的信息应在任何运行工况下都能被充分理解。

4.2.2.15 显示系统使用的符号应标准化。

4.2.2.16 应提供显示功能，向操纵员表明系统运行正常或系统出现故障。

4.2.2.17 当出现显示系统过载或可能导致处理延迟的其他系统情况时，系统应确认数据输入，并应向操纵员提供延迟和处理完成的指示。

4.2.2.18 要求操纵员快速响应的实时任务所需的人机接口应只要求有限的操纵员动作。例如：光标在画面上和画面间的移动距离、扫描时间以及一幅画面上的窗口数量都应是有限的。

4.2.2.19 视频显示器系统应提供用户协助。必要时，此类协助应包括：建议信息、错误提示、确认信息和确认系统。

4.2.2.20 操纵员应能够请求有关命令输入的指导（如语法、参数和可选项）。

4.2.2.21 画面体系组织应反映出基于任务需求的清晰的逻辑关系，并易于被操纵员充分理解。

4.2.2.22 显示界面的组织应使各种人机接口功能（如数据显

示区、控制区和消息区）的位置是统一的。

4.2.2.23 人机接口显示系统应清楚地显示哪些项是可选的。当操纵员在选定项上进行操作时，选定项应突出显示以避免出现差错。

4.2.2.24 人机接口应是用户友好的，不应要求操纵员记忆特殊的代码或序列来执行操作。

4.2.2.25 大屏幕显示器可用于提高操纵员的效能，使其能够获得核动力厂信息的共同视图或共享信息。

4.2.3 主控制室布局

4.2.3.1 主控制室应具有足够的空间，使主控制室人员可以执行全部必须的活动，而且在异常和事故工况下，使操纵员的移动最小。

4.2.3.2 主控制室的人员配置和任务分配应确保所有运行模式下均能充分、迅速地访问控制器、显示器和其他必要的设备。

4.2.3.3 主控制室内工作站和控制台的布局应:

（1）允许看到所有控制和显示盘（包括报警显示）的全貌;

（2）便于工作站操纵员与主要操作区域内任何地点人员的口头交流;

（3）使主控制室人员不需要绕过障碍就可以接近工作站;

（4）使主控制室人员进行有效的、无障碍的活动和交流。

4.2.3.4 主控制室内应为运行规程和其他文件提供存放空间。该存放空间应便于人员接近和取放文件。

4.2.3.5 应为事故期间主控制室人员可能需要使用的应急设备提供存放空间。该存放空间应便于人员接近和取放应急设备。

4.2.4 可居留性设计

4.2.4.1 主控制室应为控制室人员提供适宜的工作环境，以利于任务的执行，而不会感到不适、过度的压力或受到身体伤害。

4.2.4.2 主控制室中的工作区设计应考虑对人员效能可能有重要影响的环境因素，包括热舒适度、紧急情况下的充足照明，利于清晰口头交流的听觉环境，以及合适的布局。

4.2.4.3 主控制室应配置足够的设施和供给，以保证事故响应期间舒适的长期居留。

4.2.4.4 主控制室设计应对来自外部的飞射物进行评价并采取相应的保护措施。

4.2.5 安全参数显示系统设计

4.2.5.1 应提供安全参数显示系统，以帮助主控制室人员在事故中确定核动力厂安全状态，并评估该工况是否需要操纵员采取纠正动作以避免堆芯恶化或放射性物质释放。

4.2.5.2 安全参数显示系统设计应利用人因工程以提高主控制室人员的效能。

4.2.5.3 安全参数显示系统应提供与核动力厂重要安全功能相关的信息。

4.2.5.4 安全参数显示系统应布置在便于主控制室人员使用的位置，并提供信息的连续显示，主控制室人员从这里可以方便、可靠地评估核动力厂状态。

4.2.5.5 安全参数显示系统的设计应将最小的一组核动力厂参数集合在一起，操纵员可以据此评估核动力厂状态，而不需要查看主控制室内的全部显示信息。

4.2.5.6 可使用模拟设备和计算机设备来显示安全参数。模拟显示设备可包括表计、指示灯、数显表和记录仪。计算机显示设备可包括平板显示器和大屏幕。

4.2.5.7 安全参数显示系统所使用的显示设备应遵守主控制室人机接口通用设计准则。

4.2.5.8 在信息的呈现和编码方面，安全参数显示系统应与显示器及其他人机接口装置一致和兼容。

4.3 辅助控制室

4.3.1 必须在核动力厂内与主控制室实体分隔、电气隔离和功能隔离的一个独立地点设置辅助控制室，并配置仪表和控制设备。辅助控制室应能在主控制室丧失执行重要安全功能时完成下述任务：使反应堆进入并保持在停堆状态，排出余热以及监测核动力厂的重要参数。

4.3.2 辅助控制室的人机接口设计过程应与主控制室的人机接口设计过程同步进行，使用相似的程序、准则和方法。

4.3.3 辅助控制室的人机接口设计应考虑人因工程原则和紧急工况下的人员特点，尤其是采取立即行动的需要。

4.3.4 应采取措施确保辅助控制室的可居留性，4.2.4 中的相关要求如果适当也可用于辅助控制室。

4.3.5 辅助控制室中的工作区设计应考虑对人员效能可能有重要影响的环境因素，包括热舒适度、紧急情况下的充足照明，利于清晰口头交流的听觉环境，以及合适的布局。

4.3.6 辅助控制室中使用的基于计算机信息或控制应以与主控制室中类似的控制和指示密切匹配或最好是相同的方式发挥

作用。

4.3.7 辅助控制室中用于显示和控制的人机接口应与主控制室中的人机接口相类似，以便操纵员快速适应。应根据所需完成的功能布置人机接口，将可能的人员失误降至最低。

4.3.8 应制定相应的规程，以便将命令、控制和通信从主控制室切换到辅助控制室。

4.3.9 辅助控制室应提供通信手段，实现与就地控制点、核动力厂管理部门、外部应急管理团队以及技术支持中心之间的通信。

4.4 其他场内应急设施

4.4.1 其他场内应急设施[4]的设计应采用人因工程。设计应提供每一处工作场所的最佳布局，以及执行事故管理策略活动所需的数据和信息。

4.4.2 应急设施中支持情境意识的显示应使用公认的人因工程方法和原则来设计。需要考虑的因素包括照明、大小、几何结构、显示和控制布局、内容的可用性、格式的适合性和显示的标准化。应从根本上考虑通过显示信息来执行的任务。

4.4.3 运行经验评审，包括应急演习，结合功能分析和任务分析，应为确定缓解严重事故后果的事故监测和设备操作方面与人员效能有关的要求提供基础。

4.4.4 应考虑资源分配策略（如人员配置）、核动力厂实际情况（如电源、可达性、环境及放射性情况）、恶劣因素（如高温、

4其他场内应急设施独立于主控制室和辅助控制室，包括应急控制中心、技术支持中心和运行支持中心。

严寒、冰雹等极端天气情况）以及应急状态下与人员效能相关的技术选择。

4.4.5 当要求人员操作严重事故管理确认的非永久性设备时，应考虑人因工程。包括安全接近就地控制装置以确保非永久性设备的安全使用。典型就地控制装置的例子包括就地控制盘、连接点、开关和端子，这些就地控制装置用于:

（1）连接非永久性设备;

（2）对由非永久性设备供电的设备（如泵）进行操作。

4.4.6 应考虑到在各种应急情况下，个人和相关各方与场内和场外应急组织的内部和外部互动的范围。

4.4.7 应考虑应急响应期间的压力和工作负荷水平。

4.4.8 应培训技术支持中心人员识别和使用支持严重事故管理指南执行所需的仪表。

4.5 报警管理

4.5.1 报警或其他装置指示与正常运行的工况偏差。当发生时，应向操纵员提供必要的信息，以便:

（1）识别自动系统动作;

（2）实施必要的手动缓解动作;

（3）跟踪核动力厂的运行状况或响应过程。

4.5.2 报警应提供以下异常状态信息:

（1）控制或保护定值的参数偏离或变化率偏离;

（2）设备故障、异常或偏差;

（3）不完全或失效的自动动作。

4.5.3 不需要任何操纵员动作的工况不应产生报警。来源于

计划工况的数据，如果并非异常指示，而仅仅是预期系统响应信息，则这些数据应属于状态信息而不是报警。

4.5.4 所有报警都应记录存档，并置于配置管理之下。

4.5.5 报警系统应有足够的覆盖范围，能够对运行状态和事故工况发出警报。

4.5.6 对于核动力厂任何被分析的运行状态、停运或事故工况，报警的数量应减到最小，以防止可能导致报警过量的不必要或无意义的报警。

4.5.7 报警产生

4.5.7.1 报警系统应可以从如下信息源产生报警:

（1）数字信号;

（2）模拟信号;

（3）直接或间接来源于其他系统的经过计算、综合或分组的信号。

4.5.7.2 基于模拟和数字信号的报警应是可以配置的。报警状态可以根据信号不同状态（如通、断，开、关，跳闸、连接）来选择。

4.5.7.3 所产生的报警应支持与核动力厂构筑物、系统和部件的体系结构一致的报警层次结构。

4.5.7.4 报警应是情境感知的（例如：泵低流量报警应在实际低流量的情况下产生，而不是在泵启动时产生）。

4.5.8 报警确认

4.5.8.1 用于报警产生的传感器和输入信号应是确认有效的，以防止产生不必要的瞬时或抖动报警。

4.5.8.2 报警系统应具备可以自动减少任意时刻产生的报警数量的能力。

4.5.8.3 在测试、维护或维修相关设备期间，报警禁止可禁用非活动的报警。报警系统应支持该功能，以避免成为干扰报警或持续报警。

4.5.8.4 应经过人因工程分析和确认以确定一个报警是否遮蔽了另一个或其他报警的发生。

4.5.8.5 报警系统应支持报警优先级管理以确定报警之间的相对重要性。

4.5.9 报警处理

4.5.9.1 报警系统应支持用户定义的报警生成。操纵员应能够为模拟变量选择一个高或低的报警限值，或为离散变量在可能的报警状态中选择一种状态。

4.5.9.2 报警系统应能够在不同层级上使用基于事件或重要性的报警抑制技术:

（1）基于事件的精简技术过滤或抑制由于支持系统或设备故障，或由核动力厂事件而产生的报警;

（2）基于重要性的精简技术在报警过载的情况下抑制低优先级的报警。

4.5.9.3 无论自动或手动触发，报警过滤或抑制应用来防止操纵员的超负荷，但不能抑制必要的信息。

4.5.10 报警指示和控制

4.5.10.1 当任一报警条件出现或消失时，报警系统应提供视觉显示。视觉显示应包含:

（1）闪烁。当报警条件出现或消失时启动，确认或复位后终止。对于已有子报警出现并被确认的组报警，当任一新的子报警出现时，应重闪;

（2）颜色编码。报警应根据报警优先级和报警状态用不同颜色来编码。也可以使用其他显示编码方式。

4.5.10.2 当任一报警条件出现或消失时，报警系统应提供听觉指示。

4.5.10.3 应提供报警消声手段以避免听觉疲劳并且便于识别可能随后出现的新报警。

4.5.10.4 应为操纵员提供及时确认单个或成组报警的手段。

4.5.11 报警呈现

4.5.11.1 “暗盘”原则，包括在不影响核动力厂安全的情况下，将正常运行期间出现的报警数量减到最小。

4.5.11.2 在满功率运行及其他正常运行工况下报警处理应遵守“暗盘”原则。

4.5.11.3 报警有下列不同的显示方式:

（1）专用空间的持续显示（例如: 模拟盘上的光字牌，视频显示单元上的报警窗，以及集成了报警的模拟流程画面）;

（2）报警信息列表显示（例如: 视频显示单元屏幕上的文本信息显示）;

（3）显示画面中的报警（例如: 模拟流程画面和软控制器画面）;

（4）单一报警显示;

（5）混合显示，例如: 不同类型显示的组合。

4.5.11.4 报警状态变化和新报警应分别显示和管理。

4.5.11.5 报警信息应简单、清晰并标准化。

4.5.11.6 报警信息应包含操纵员有效应对报警所需的所有信息，如报警源、优先级、描述、设定值、参数值及报警响应规程和相关显示。

4.5.11.7 操纵员应能够根据需要分类排序报警信息。报警系统可以根据如下方式提供报警列表:

（1）时间排序;

（2）优先级水平;

（3）报警状态;

（4）报警信息;

（5）其他逻辑顺序。

4.5.11.8 报警应集成到图形显示中，尤其是当其有利于显示报警与相关系统、功能、设备或部件关系时。

4.5.11.9 应使用单个报警信息显示来提供报警相关的专门信息，如:

（1）报警源参数的趋势;

（2）统计数据，例如：报警出现的平均频率;

（3）与其他报警或变量的关系;

（4）报警相关的当前或历史工作单或报告。

4.5.12 报警响应规程

4.5.12.1 应为操纵员提供控制室内所有报警的响应规程。

4.5.12.2 报警响应规程应为操纵员提供如下信息:

（1）报警所属系统或功能组;

（2）与报警相关联的准确信息;

（3）报警响应优先级;

（4）自动动作、立即动作和其他操纵员动作;

（5）报警（潜在）原因列表;

（6）参考信息。

4.6 规程开发

4.6.1 规程中应处理安全分析所确定的重要人员任务。

4.6.2 应定期确认那些包含了安全分析所确定的重要人员任务的规程，以证实:

（1）成功完成每步规程所需设备的可用性和状态;

（2）安全分析中做出的对安全相关人员任务的任何假设或要求的有效性。

4.6.3 规程应得到确认，以保证它们可以按照规定执行且结果或输出与期望一致。

4.6.4 规程开发还应考虑来自任务分析的输入，以达到下述目的:

（1）识别需要在规程中强调的潜在失误;

（2）描述成功完成一项任务所必需的信息流、动作和反馈;

（3）识别任务和人员之间的联系;

（4）在规程内提供独立动作时间的初步信息;

（5）方便规程之间的切换;

（6）建立技术警告的格式和内容、前提条件（初始条件）和规程终止需求。

4.6.5 规程中某一动作（或一系列动作）的期望结果应清晰、

易懂并可以验证。

4.6.6 在核动力厂规程开发过程中应用人因工程时，应考虑不同规程类型（如事故规程、维修规程和试验规程）相关的格式和内容。

4.6.7 对于安全关键任务、复杂任务和很少执行的任务，规程应以详细、一步一步的方式陈述。

4.6.8 规程应提供规定动作无法实现时的安全替代动作或安全终止该规程的指导。

4.7 培训计划开发

4.7.1 任务分析应为确定所设计系统的培训需求提供基础（如所需的知识、技能和能力）。

4.7.2 应对运行人员培训显示格式与所表达的核动力厂状态之间的关系，包括故障模式及其对显示的影响和表现。

4.7.3 应对运行人员培训画面内和画面间的导航、屏幕属性管理（如窗口）和人机接口其他功能的使用。

4.7.4 培训计划应随设计进展定期进行审查和修改。

4.7.5 应及时进行培训，与核动力厂变更有关的培训应在变更生效前完成。

5 人因验证和确认

5.1 总则

5.1.1 人机接口系统的人因验证和确认，应全面地确定人机接口系统是否符合规定的人因工程设计要求，及其是否能使人员成功且安全地执行预期功能，以确保核动力厂的安全运行。

5.1.2 验证和确认的实施应贯穿整个人因工程设计过程。随着项目进展，验证和确认可基于逼真度不断提高的模型和仿真。

5.1.3 验证和确认应提供客观证据，表明设计者正确遵守了可用性的设计原则和要求，这些原则和要求考虑了人、技术和组织，以及彼此间的交互。

5.1.4 验证活动通常包括:

（1）确定适用的人因工程标准和导则;

（2）验证人机接口，包括硬件（如盘台、模拟接口，包括报警指示）和软件，以及相应的文件（如规程、手册、报警卡);

（3）评审设计要求、图纸和手册;

（4）验证任务支持手段，包括工具、任务辅助、人员防护设备、任务相关设备和培训、操纵员资质，以及规程的可获取性和可用性。

5.1.5 验证活动可包括与系统用户的交互。

5.1.6 验证和确认活动应由未承担原设计的人员或组织实施。

5.1.7 确认尤其应评价:

（1）在运行状态和事故工况中，控制室人员完成所要求的动作的能力;

（2）规程的呈现和组织能支持任务执行;

（3）人机接口支持操纵员任务的能力;

（4）为支持任务执行和系统运行，工作场所布置的合理性。

5.1.8 控制室设计的人因确认应覆盖:

（1）主控制室和辅助控制室布局对操纵员任务的支持性;

（2）系统监视、控制和维护（在主控制室内/外）的有效性;

（3）与全厂的运行状态和事故工况相关的控制室监控系统。

5.1.9 覆盖硬件、软件、规程和人员的集成系统确认应在设计最终固化前实施，以便为核动力厂运行前开展设计变更提供充裕的时间。

5.1.10 验证和确认的输入，应源于已实施的人因活动，特别是:

（1）所有运行状态和事故工况的运行概念;

（2）与任务（特别是安全关键任务）相关的技术和用户要求;

（3）控制方式和自动化水平的功能要求和详细说明;

（4）来自功能分析的输入;

（5）监管要求;

（6）来自运行经验评审的输入;

（7）重要人员任务;

（8）来自安全分析的数据;

（9）来自人员可靠性分析的数据;

（10）来自人员配备、组织和资质分析的数据;

（11）来自以往人因评审和分析的数据;

（12）来自仿真的输入，如部分任务仿真（若有）。

5.2 验证和确认计划

5.2.1 应编制验证和确认计划。计划应对资源、独立性水平、评价方法、采用的标准和法规进行规划。

5.2.2 验证和确认活动的策划是迭代的，它支持随着设计推进而进行的项目变更，例如:

（1）可用人机接口的增加;

（2）规程详细程度的提高;

（3）操纵员培训水平的提升;

（4）模拟逼真度的提高。

5.2.3 验证和确认计划应明确:

（1）评价的范围;

（2）必要的数据收集和分析;

（3）有效性的测量;

（4）评价和接受准则;

（5）参与评价的人员;

（6）评价团队（包括作为参试者的用户代表）的培训需求;

（7）试验环境;

（8）日程安排。

5.2.4 验证和确认计划还应明确:

（1）场景选择;

（2）评价团队使用的资料和工具。

5.2.5 验证和确认计划应描述相关的目标和预期的输出，以论证人机接口设计与下述几方面的符合性:

（1）项目人因工程要求（例如: 人体工效学要求和项目特定的要求）;

（2）核动力厂运行接受准则;

（3）与操纵员响应有关的监管要求。

5.2.6 验证和确认计划应阐述下列过程:

（1）对任何人因相关问题的分析和评估;

（2）人因问题的跟踪;

（3）解决设计偏差的方法。

5.2.7 确认应由具备不同技能和经验的多学科确认团队（例如：核动力厂运行专家、教员、事件和事故处理专家以及人因工程专家）来定义和实施。

5.2.8 应根据核动力厂未来运行的组织结构来组织确认试验的参试者。

5.2.9 确认试验的参试者应代表后续使用人机接口的核动力厂人员，例如：持照操纵员，而非培训人员或者工程设计人员。

5.2.10 确认团队应接受数据收集技术的培训。

5.3 试验方法

5.3.1 人因验证和确认通常应包括以下所有或部分内容:

（1）静态试验（例如：验证系统满足设计规范）;

（2）动态试验（例如：按照时间和准确度测试系统响应）;

（3）场景试验，以及部分任务模拟或全范围模拟（例如：按照时间和准确度测试操纵员的响应）;

（4）观察;

（5）独立报告（例如：调查问卷和结构化访谈）;

（6）检查表（例如：用在静态或动态试验中）;

（7）任务排演。

5.3.2 参试者在进行试验前应熟悉相关系统。

5.3.3 验证和确认试验中使用的试验平台、模型和模拟机，其代表性的符合程度和限制应得到论证。

5.4 效能测量

5.4.1 人因验证和确认应采用真实工作环境中的人员效能测量指标。测量指标可包括:

（1）所执行任务的复杂性;

（2）工作负荷（个人和团队）;

（3）设计所要求的相关的知识和技能;

（4）任务序列和响应时间;

（5）情境意识的要求（个人和团队）;

（6）使用规程的要求;

（7）发现和响应不利工况的要求;

（8）用户间以及和其他团队协作和沟通的要求。

5.4.2 与人员效能相关的定性、定量测量指标可包括:

（1）时间;

（2）准确性;

（3）沟通频率和内容;

（4）错误识别和失误恢复率;

（5）与情境意识相关的参数（例如：状态识别、理解和预测）;

（6）团队决策方法的使用;

（7）凝视时间和停留时间（例如：来自眼动仪）;

（8）疲劳;

（9）任务成功执行的概率。

5.5 验证准则

5.5.1 验证准则应包括设计中使用的人因工程标准和导则。

验证活动使用的人因标准和导则的选取，取决于评价范围内人机接口资源的特点。

5.5.2 人机接口设计验证还应识别任务分析所确定的任务要求（例如：与时间限制、操作顺序和精确度相关的要求）是否得到了满足。

5.6 确认试验

5.6.1 所选择的从人因角度用于确认设计的试验场景，应尽可能的真实，包括:

（1）仿真和试验平台应与核动力厂设计和物理布置相一致;

（2）试验场景应代表核动力厂所有状态下的运行工况，且应包含事件（例如：失效）及其初始条件;

（3）确认任务应具有核动力厂运行任务的代表性（例如：监视、检测、诊断、参数变化预测、监督、控制，以及自动控制系统的手动恢复);

（4）参试者应经过培训，在试验中的岗位应与其资质和职责水平相一致;

（5）用于试验的规程应与将在相关运行工况下使用的规程相匹配;

（6）试验应覆盖场景中预期的人员交互范围。

5.6.2 试验场景的合理性和代表性应得到论证。

5.7 数据收集

5.7.1 人因验证和确认计划应规定数据收集方法。计划应明确试验持续时间和试验次数、测试的系统和子系统，以及需要收集的数据项目。

5.7.2 为进行评价，应从实体模型、部分范围模拟机、全范围培训模拟机试验中开展数据收集，例如:

（1）参试者所采取的动作（例如：每次试验中由观察员手动收集数据);

（2）控制室内参试者间的沟通，以及控制室和参与核动力厂运行和应急管理的其他团队之间的沟通。

5.7.3 数据收集应涵盖偏差（例如：参试者遇到的困难和发生的错误）以及设计中预期所用工具的易于使用性。因此，确认试验应识别出为操纵员安全运行提供支持的资源，以及必要的设计改进，例如:

（1）有利于核动力厂监督并加强情境意识;

（2）优化人员工作负荷;

（3）鼓励合作和沟通。

5.7.4 确认试验数据收集方法应支持客观测量（例如：动作完成所需时间）和主观测量（例如：采用主观问卷评价人员工作负荷)。

5.7.5 收集的数据应允许对每个试验场景进行深入分析，覆盖例如:

（1）动作时间序列;

（2）识别始终被成功完成没有问题的任务;

（3）识别和分析场景执行过程中出现的异常情况（例如：人员遇到的任何困难，对过程进展的犹豫，以及控制室班组成员之间对系统或设备状态存在不一致的意见)。

5.7.6 试验中和试验之后收集的数据应可用于分析。

5.8 数据分析

5.8.1 确认试验的分析应包括对所收集数据的深入检查。分析应同时覆盖试验参试者的错误以及成功实施的人员活动。此外，在试验覆盖的所有运行情况中，应重点分析:

（1）参试者使用成功且满足其需求的系统;

（2）难以使用的系统;

（3）试验结果对安全的意义;

（4）关于设计改进的建议（由分析人员和用户提出）。

5.8.2 对收集数据的分析应证明提供给人员和组织的系统的有效性，并应证明在没有过度工作负荷的情况下，参试者能够:

（1）理解情境;

（2）执行所需动作，同时考虑相应的要求;

（3）在控制室成员之间，以及与控制室人员有交互的人员之间相互配合（例如：维修人员、自动控制系统人员和风险管理团队）。

5.8.3 应对试验中识别的人因相关问题进行系统性地存档和跟踪。

5.8.4 对用于处理人因工程相关问题的解决方案以及解决方案的有效性，应进行记录存档、评估和监测。

5.8.5 每次试验收集的数据及其分析应存档。

5.9 结果

5.9.1 每项验证和确认试验的结果应存档。

5.9.2 验证和确认完成后应形成报告，对试验计划、试验发现、改进建议和结论进行总结。

5.9.3 任何与人因标准和安全目标之间的差距都应进行研究、解决和存档。

5.9.4 应明确未被验证和确认试验所覆盖，但核动力厂投运后将在现场确认的事项。

6 人因工程设计实现

6.1 人因工程设计实现的一般原则

6.1.1 人因工程设计实现包括对人因工程设计输出的开发、部署和评估。

6.1.2 设计实现应作为正式建造和调试、取证或核动力厂改造过程的一部分来实施。

6.1.3 人因工程设计实现应评估最终设计是否符合经过验证和确认的设计，并且在实际核动力厂和工作环境中实现设计时是否出现非预期的问题。

6.1.4 人因工程设计实现应证明:

（1）设计过程的实施符合其在标准、功能和安全性能方面的技术规范;

（2）已实施的设计未产生与人员、管理系统、构筑物、系统或部件相关的任何问题(例如:与当前系统或人机接口不一致）或矛盾（例如：安全性、可运行性或文化方面）。

6.1.5 人因工程设计实现的范围应考虑设计对下列要素的影响:

（1）组织因素;

（2）人员因素;

（3）工作设计;

（4）安全分析;

（5）概率安全评价和人员可靠性分析;

（6）人机接口;

（7）设备;

（8）规程;

（9）培训;

（10）核动力厂参考文件;

（11）工作环境。

6.1.6 在人因工程设计实现阶段，应适当地考虑如下事宜:

（1）评估最终设计对设计实现的影响，可能有必要采取减轻人因工程设计实现非预期后果的行动;

（2）在开始设计实现之前需要准备就绪的要素，例如：对执行团队进行必要的关于使用模拟机或测试平台的培训，以确保他们达到预期的任务执行水平;

（3）设计实现成功准则的定义，这可以与人员效能监测系统相关联，以确保对人员效能的相关方面进行测试或测量;

（4）开发一种方法，用于识别、评估和解决在人因工程设计实现阶段发现的人因相关问题;

（5）若可行，在人因工程设计实现无法实现其效能目标时的应对措施。

6.2 人因工程设计实现的输出

人因工程设计实现的输出应存档，并总结下列事宜:

（1）证明包括支持性要素（如人机接口、规程和培训）的

设计输出满足项目之初所确定的相关标准、人员效能和成功准则;

（2）对于人、技术和组织的任何负面影响，是可接受的，或得到恰当地改善;

（3）任何针对最终设计的变更已体现到核动力厂的图纸和资料中，如培训资料、规程、图纸、模拟机、组织结构和辅助设备;

（4）在设计实现之前，所有识别到的人因问题已得到妥善处理;

（5）所有新的人因相关问题得到识别和评估，形成了解决问题的合适的计划;

（6）任何遗留的不符合项已被评估，并且从安全角度被认为是可接受的。

7 人员效能监测

7.1 人员效能监测的目的

人员效能监测应是一个主动和持续的过程，以评估设计能否持续有效地支持核动力厂人员安全、有效地完成其工作。人员效能监测提供以下分析结果:

（1）人机接口设计是否满足并将持续满足初始的安全、运行和效能假设;

（2）在主控制室、辅助控制室、就地控制站和其他应急设施中，人机接口设计能否支持运行人员有效完成其任务;

（3）人机接口设计、规程和培训的变更，是否给操纵员执行任务带来负面影响;

（4）人员任务能否按照响应时间准则和效能准则得以完成;

（5）能否在核动力厂全寿期维持在系统确认阶段建立的效能水平;

（6）所提供的支持，如监督、培训、人员配备、规程、个人防护设备、工具和工作辅助，对人员任务的支持是否恰当和充分。

7.2 人员效能监测的实施

7.2.1 人员效能监测应考虑:

（1）应对人员效能监测的负责人和结果使用者开展充分培训;

（2）人员效能监测负责人应具有合适的资质，并具有人和组织因素、系统方法和根本原因分析方法的经验;

（3）应全面理解人员效能水平不足的原因和重要度，应提出改善效能的措施;

（4）应建立一种开放和诚实的报告文化，以确保系统用户所发布报告的有效使用;

（5）个人和团队的效能受组织内各层级人员效能的影响，因此有效的人员效能监测应从所有层级获取数据;

（6）应监测人员效能降级的响应和解决过程，以确保响应在合理时间范围内。

7.2.2 核动力厂演习和演练提供了一个重要的机会，以收集人员效能在所有核动力厂状态下大范围核动力厂响应期间的信息。在可行的情况下，应使用高水平的逼真度来接近真实事件中所面临的情况。

7.2.3 在营运单位不是设计责任方的新建项目中，在调试和运行阶段中，应确保设计阶段关于人员效能的假设得到识别和确认。

8 人因工程应用于计算机化规程设计

8.1 总则

8.1.1 通过将纸质规程转换为数字形式，计算机化规程可以在监视和检测、情境评估、响应计划和响应执行的任务中为运行人员提供支持，以便提供不同层次的功能，包括各种不同的自动化水平。

8.1.2 当在核动力厂实施计算机化规程时，人因工程大纲应考虑如何引入这些规程，以确保正确的功能，并与运行人员的期望和经验保持一致。

8.1.3 计算机化规程应包括在核动力厂的配置管理大纲中。

8.1.4 计算机化规程的设计应考虑编写、质量保证、审查、验证、确认、控制和更新程序的实际可行性。

8.1.5 计算机化规程系统有三种类型:

（1）I 类系统相当于纸质规程的等价复制，不接收任何经过处理的或实时的信息;

（2）II 类系统通过动态嵌入的过程数据来增强规程;

（3）III类系统提供 II 类系统的能力，并包括了可操作核动力厂设备的嵌入式软控制。III类系统可以包括自动化步骤序列的能力，即可自动执行规程中所描述的动作。

8.2 计算机化规程系统的人机接口

8.2.1 应将人因工程应用在新建核动力厂和运行核动力厂的计算机化规程的设计中。

8.2.2 以下人因工程原则适用于计算机化规程:

（1）在合理可行的范围内，仅显示与执行任务相关的信息;

（2）每个规程应持续提供可辨认的信息，如标题、版本号、日期、核动力厂名称和机组;

（3）对于计算机化规程系统的每个显示画面，保持信息、导航辅助、控制和其他应用菜单的显示和位置的一致性;

（4）调整计算机化规程系统（包括结构、格式、导航菜单和控制等），以适应任何将要使用该规程系统的设备。

8.2.3 应使用适当数量的显示向操纵员提供正确执行规程所需的所有信息。

8.2.4 计算机化规程的人机界面应支持在显示画面间的便捷导航。

8.3 与计算机化规程系统的交互

8.3.1 除非另有规定，8.3.2-8.3.11 所列有关交互能力的要求适用于 I、II 和 III 类的计算机化规程。

8.3.2 规程步骤中提到的报警和警告，应以下述方式显示:

（1）当画面呈现步骤时，显示对应的报警和警告;

（2）操纵员需要在执行步骤规定的详细操作之前，读取这些信息;

（3）每个报警或警告的呈现方式可使之易于与其他报警或警告进行区分。

8.3.3 每组相关的物项应以列表的形式呈现，以满足下述要求:

（1）使操纵员可以容易地处理信息;

（2）该组物项可以清晰地与其他组物项区分开;

（3）在呈现列表时包括标题，用以明确列表的内容。

8.3.4 应指示规程步骤的状态（例如：步骤是否完成、进行中、必要处的检查和授权，或者失败）。对于I类系统，应提供手动跟踪步骤状态的能力。还应在必要时指示替代措施。

8.3.5 对于II类和III类计算机化规程，系统应记录并存储规程执行的进展。计算机化规程系统中的多个规程可能需要同时被执行。

8.3.6 在这类情况下，应适当分配人力资源，并协调多个规程的执行。例如：当多个规程同时执行时，该规程和规程中步骤的状态应显示在相应的设备上。

8.3.7 计算机化规程系统应包括导航支持功能，允许操纵员在规程内部（在步骤之间或转到同一规程的其他部分）以及从一个规程到另一个规程（例如：通过动态链接）进行跳转。

8.3.8 对于所有类型的计算机化规程，注释、报警和警告应能够被操纵员所访问。

8.3.9 操纵员应能够查看计算机规程系统使用的数据和逻辑规则。

8.3.10 通过计算机化规程系统，操纵员应能记录其关于规程执行的注释和评论。这些记录应被保存并存档，以备之后查阅。

8.3.11 计算机化规程系统可对规程的选用提出建议，但操纵

员应承担决策责任，并应基于核动力厂状态做出决策。这适用于II类和III类计算机化规程。

8.4 计算机化规程系统的功能（适用于II类、III类）

8.4.1 当核动力厂的状态需要进入规程、退出规程或者从一个规程切换到另一个规程时，计算机化规程系统应通知操纵员。

8.4.2 计算机化规程系统应能自动提供有关参数状态和设备状态的准确信息。

8.4.3 计算机化规程系统提供的信息和操纵员支持功能应是基于情境的，以免操纵员收到不适当的信息。

8.4.4 计算机化规程系统可以自动处理一个规程内的某些步骤。应将步骤自动处理的结果突出显示给操纵员。计算机化规程系统应指明需要操纵员连续监视的步骤（例如：时间相关和过程相关步骤）。当这些步骤中的预期条件达到时，计算机化规程系统应向操纵员发出警报。此外，计算机化规程系统应指示出对参数的监视是否已停止或仍在进行中。

8.4.5 包括了可操作核动力厂设备的软控制的计算机化规程系统（III类规程），应向操纵员提供必要的信息，以支持对这些控制的有效使用。

8.5 计算机化规程系统的降级和失效

8.5.1 应为切换到后备规程（如纸质规程）以及在适当时从后备规程切回到计算机化规程的活动制定指南。

8.5.2 计算机化规程系统应识别和指示需要过渡到后备规程的降级条件和故障。

8.5.3 对于操纵员，作为后备规程的纸质规程应可用且易获

取。

8.5.4 计算机化规程中信息的结构和格式应与后备规程中信息的结构和格式相兼容。

8.5.5 当需要过渡到纸质的后备规程时，应提供以下信息:

（1）目前正在执行的规程;

（2）已完成和未完成的规程步骤，包括规程执行中断时所处的步骤;

（3）在过渡到后备规程时，正在监视的步骤或条件的有关信息;

（4）从中断处继续执行规程所需的信息，避免重复已完成的步骤。

8.5.6 到后备规程的过渡指南应考虑与计算机化规程系统相关的故障模式，并应规定在计算机化规程系统故障期间和恢复之后所需的操纵员动作。这些动作应从操纵员的角度进行描述。

8.5.7 应确认过渡到后备规程所需的时间能满足计算机化规程的功能要求。

8.5.8 针对计算机化规程的培训应包括过渡到纸质规程所需的具体步骤。

8.6 计算机化规程的自动步骤序列

8.6.1 计算机化规程的最高水平是自动化，即将规程所述的操作步骤的序列进行自动化处理。规程步骤序列的自动化仅适用于 III 类规程系统。

8.6.2 应由负责核动力厂安全运行的操纵员授权和监视计算机化规程中自动化序列的执行。

8.6.3 操纵员应能够选择手动执行计算机化规程的步骤或者激活自动执行。

8.6.4 操纵员应负责选择需要使用的规程。

8.6.5 自动化的步骤序列应包含在单个规程中（即每一个序列的开始和结束都在同一个规程中）。

8.6.6 计算机化规程系统应向操纵员提供详细而具体的步骤序列的信息。

8.6.7 应向操纵员提供有关自动序列执行进展情况的信息（即关于已完成、目前正执行和有待执行的步骤的信息）。

8.6.8 应提供有关自动化失效的信息，同时提供序列中发生失效的点。

8.6.9 计算机化规程系统应向操纵员提供在开始执行自动化步骤序列之前需要满足的初始条件的信息。

8.6.10 自动化步骤序列中的确认点

8.6.10.1 自动化步骤序列可以包括确认点，它是规程中预先设定的点，在该点上规程将停止其进程并要求操纵员确认自动化序列的状态并授权规程继续执行。

8.6.10.2 自动化步骤序列中的确认点应：

（1）协助操纵员识别自动化的进程，并做出任何相关和必要的决策或调整，以使规程继续进行；

（2）对于正在执行的步骤序列中涉及到的核动力厂设备，保持操纵员对其状态的掌握；

（3）允许操纵员授权规程继续进行。

8.6.10.3 计算机化规程系统应允许操纵员在自动化步骤序

列开始之前，添加额外的临时确认点。

8.6.10.4 应不允许操纵员移除预先设定的确认点。

8.6.10.5 规程中定义的确认点应使规程处于稳定状态，在此状态下，操纵员能够正确评估规程的状态，并做出必要的决策使规程继续进行。

8.6.11 自动化步骤序列的中断

8.6.11.1 当自动化步骤序列中断时，计算机化规程系统应允许操纵员安全地从自动执行过渡到手动执行，或恢复自动执行。

8.6.11.2 计算机化规程系统应提供有关中断的信息，如序列中断的原因、已完成的步骤和有待执行的步骤。

8.6.11.3 计算机化规程系统应能够在步骤完成的必要条件不满足时，或因任何其他原因无法保证当前步骤的安全完成时，自动中断自动化序列。

8.6.11.4 当自动化序列发生任一中断时，计算机化规程系统应向操纵员发出告警。

9 人因工程应用于产品选择

9.1 人员防护设备的使用

9.1.1 人员防护设备及其特性选择应适合用户的身体尺寸、穿戴后执行的任务和用户的工作环境。与人员防护设备的使用相关的人因工程设计准则应适用于穿戴后使用这些设备、工具和辅助作业措施的预期应用。

9.1.2 人员防护设备不能显著影响任务执行的可靠性。

9.1.3 应进行人因工程分析，以确定是否可以在使用个人防

护设备的情况下执行任务，这可能影响用户的视觉、听觉、灵活性、移动性及在极端温度下工作的能力。

9.1.4 人员防护设备应根据其在不同核动力厂工况下的预期用途进行验证与确认（例如：通过演习和应急演练）。验证与确认应考虑用户人体尺寸。

9.2 商业现货产品

9.2.1 把商业现货产品集成到已有系统中时，应考虑人因问题，选择与核动力厂设计、运行和维修策略相一致的产品。

9.2.2 当把一件或多件商业现货产品集成到一个新的或现有系统中时，产品选择应考虑下列人机接口特性的一致性：

（1）系统内部的一致性；

（2）与操纵员已使用过的类似系统之间的一致性；

（3）与核动力厂人机接口现有特征的一致性。

9.2.3 把商业现货产品集成到已有系统中时，应评估其对人员效能的影响。

9.2.4 应考虑人因工程应用以保证商业现货设备不会导致工作环境或任务执行方式发生不良变化。

9.2.5 需应用人因工程以确定商业现货产品的使用是否需要额外的培训、修改或新增规程、维护或试验，以及在技能和资质要求方面的变化。

9.3 移动设备

9.3.1 移动设备的审查范围应包含手持、便携和可穿戴设备。

9.3.2 移动设备选择应基于分析以证明移动设备适用于任务和时长（人员持有、利用设备交互、运输或穿戴设备）。当人员

穿戴了防护设备时，移动设备应适用于任务。

9.3.3 移动设备及其特性选择应符合用户的人体尺寸、环境条件和人因工程设计准则（如照明、握力、尺寸、重量和人员信息处理特性）。

9.3.4 移动设备在不使用时不应影响其他任务的执行。

9.3.5 在适当的情况下，用户应了解极端环境下移动设备的要求（例如：使用加固设备）。

9.3.6 在人因工程分析中应考虑移动设备的存放。

9.3.7 应考虑移动设备的时间同步或校准需求。

9.3.8 对移动计算设备，由于设备使用的潜在限制，失误管理对安全至关重要。人因工程应确定以下需求：

（1）纠错功能（例如：更正错误输入及更正个别错误的一种简易方法，而无须重新正确输入命令或数据）；

（2）在键入后但没有输入到系统前，通过用户和软件早期探测和纠正错误的特性；

（3）以不干扰用户的方式进行错误检查（例如：在数据字段的末尾而不是逐个字符地进行错误检查）；

（4）设备被移动设备控制时，用户对过程的控制（例如：当指示有错误存在时，可以在序列中的任何点停止过程的能力）。

9.3.9 由于高强度辐射场可能会造成设计上的限制，应考虑其潜在干扰。

名词解释

计算机化规程系统

通过计算机而非纸质形式体现的核动力厂规程系统。

运行概念

运行概念描述预想设计方案将如何执行设计功能，包括各种人员角色以及如何组织、管理和支持他们。运行概念描述核动力厂的运行方式(运行原理),包括运行人员的数量和组成以及正常和异常工况下运行人员如何操作核动力厂等方面。

失误管理

基于知觉、认知偏差、人体测量学理论，确定人在人机接口中失误的可能性。人因工程预测失误并设计防止失误或避免失误影响核动力厂安全运行。

人机接口

人机接口是一个系统的一部分，用于人与系统交互完成它们的功能和任务。人机接口建立了人与核动力厂系统的接口，包括规程、通讯系统显示、报警和控制。

人体运动控制

人体运动控制是人体肌肉系统的生理能力，能够控制力量运动和精细运动。

重要人员任务

根据安全分析确定的、对安全有消极或积极影响的人员任务。

情境意识

对核动力厂真实状况的动态感知过程和理解，以帮助个人和团队预测系统的未来状况。这是一种建立情境和未来行动计划的心智模型的方法。情境意识程度对应于对核动力厂状态的理解与实际状态的差异。人因工程目的之一是支持操纵员形成情境意识。

验证

通过检查和客观证据确认整个人机接口系统满足设计规范、要求并为按计划完成任务提供必要的支持。

确认

通过检查和客观证据确认整个人机接口系统（包括用户）能成功执行预期功能，并在预期运行的工况下实现其目标。