国际原子能机构安全标准

保 护 人 类 与 环 境

核电厂设计中的人因工程

特定安全导则

第 SSG-51 号

IAEA
国 际 原 子 能 机 构

国际原子能机构安全标准和相关出版物

国际原子能机构安全标准

根据《国际原子能机构规约》第三条的规定，国际原子能机构受权制定或采取旨在保护健康及尽量减少对生命与财产之危险的安全标准，并规定适用这些标准。

国际原子能机构借以制定标准的出版物以**国际原子能机构《安全标准丛书》**的形式印发。该丛书涵盖核安全、辐射安全、运输安全和废物安全。该丛书出版物的分类是**安全基本法则**、**安全要求**和**安全导则**。

有关国际原子能机构安全标准计划的资料可访问以下国际原子能机构因特网网站：

www.iaea.org/zh/shu-ju-ku/an-quan-biao-zhun

该网站提供已出版安全标准和安全标准草案的英文文本。以阿拉伯文、中文、法文、俄文和西班牙文印发的安全标准文本；国际原子能机构安全术语以及正在制订中的安全标准状况报告也在该网站提供使用。欲求进一步的信息，请与国际原子能机构联系（Vienna International Centre, PO Box 100, 1400 Vienna, Austria）。

敬请国际原子能机构安全标准的所有用户将使用这些安全标准的经验（例如作为国家监管、安全评审和培训班课程的依据）通知国际原子能机构，以确保这些安全标准继续满足用户需求。资料可以通过国际原子能机构因特网网站提供或按上述地址邮寄或通过电子邮件发至 Official.Mail@iaea.org。

相关出版物

国际原子能机构规定适用这些标准，并按照《国际原子能机构规约》第三条和第八条 C 款之规定，提供和促进有关和平核活动的信息交流并为此目的充任成员国的居间人。

核活动的安全报告以**《安全报告》**的形式印发，《安全报告》提供能够用以支持安全标准的实例和详细方法。

国际原子能机构其他安全相关出版物以**《应急准备和响应》**出版物、**《放射学评定报告》**、国际核安全组的**《核安全组报告》**、**《技术报告》**和**《技术文件》**的形式印发。国际原子能机构还印发放射性事故报告、培训手册和实用手册以及其他特别安全相关出版物。

安保相关出版物以**国际原子能机构《核安保丛书》**的形式印发。

国际原子能机构《核能丛书》由旨在鼓励和援助和平利用原子能的研究、发展和实际应用的资料性出版物组成。它包括关于核电、核燃料循环、放射性废物管理和退役领域技术状况和进展以及经验、良好实践和实例的报告和导则。

核电厂设计中的人因工程

国际原子能机构的成员国

阿富汗
阿尔巴尼亚
阿尔及利亚
安哥拉
安提瓜和巴布达
阿根廷
亚美尼亚
澳大利亚
奥地利
阿塞拜疆
巴哈马
巴林
孟加拉国
巴巴多斯
白俄罗斯
比利时
伯利兹
贝宁
多民族玻利维亚国
波斯尼亚和黑塞哥维那
博茨瓦纳
巴西
文莱达鲁萨兰国
保加利亚
布基纳法索
佛得角
布隆迪
柬埔寨
喀麦隆
加拿大
中非共和国
乍得
智利
中国
哥伦比亚
科摩罗
刚果
哥斯达黎加
科特迪瓦
克罗地亚
古巴
塞浦路斯
捷克共和国
刚果民主共和国
丹麦
吉布提
多米尼克
多米尼加共和国
厄瓜多尔
埃及
萨尔瓦多
厄立特里亚
爱沙尼亚
斯威士兰
埃塞俄比亚
斐济
芬兰
法国
加蓬
冈比亚
格鲁吉亚
德国
加纳
希腊
格林纳达
危地马拉
几内亚
圭亚那
海地
教廷
洪都拉斯
匈牙利
冰岛
印度
印度尼西亚
伊朗伊斯兰共和国
伊拉克
爱尔兰
以色列
意大利
牙买加
日本
约旦
哈萨克斯坦
肯尼亚
大韩民国
科威特
吉尔吉斯斯坦
老挝人民民主共和国
拉脱维亚
黎巴嫩
莱索托
利比里亚
利比亚
列支敦士登
立陶宛
卢森堡
马达加斯加
马拉维
马来西亚
马里
马耳他
马绍尔群岛
毛里塔尼亚
毛里求斯
墨西哥
摩纳哥
蒙古
黑山
摩洛哥
莫桑比克
缅甸
纳米比亚
尼泊尔
荷兰
新西兰
尼加拉瓜
尼日尔
尼日利亚
北马其顿
挪威
阿曼
巴基斯坦
帕劳
巴拿马
巴布亚新几内亚
巴拉圭
秘鲁
菲律宾
波兰
葡萄牙
卡塔尔
摩尔多瓦共和国
罗马尼亚
俄罗斯联邦
卢旺达
圣基茨和尼维斯
圣卢西亚
圣文森特和格林纳丁斯
萨摩亚
圣马力诺
沙特阿拉伯
塞内加尔
塞尔维亚
塞舌尔
塞拉利昂
新加坡
斯洛伐克
斯洛文尼亚
南非
西班牙
斯里兰卡
苏丹
瑞典
瑞士
阿拉伯叙利亚共和国
塔吉克斯坦
泰国
多哥
汤加
特立尼达和多巴哥
突尼斯
土耳其
土库曼斯坦
乌干达
乌克兰
阿拉伯联合酋长国
大不列颠及北爱尔兰联合王国
坦桑尼亚联合共和国
美利坚合众国
乌拉圭
乌兹别克斯坦
瓦努阿图
委内瑞拉玻利瓦尔共和国
越南
也门
赞比亚
津巴布韦

国际原子能机构的《规约》于 1956 年 10 月 23 日经在纽约联合国总部举行的原子能机构《规约》会议核准，并于 1957 年 7 月 29 日生效。原子能机构总部设在维也纳，其主要目标是“加速和扩大原子能对全世界和平、健康及繁荣的贡献”。

国际原子能机构《安全标准丛书》第 SSG-51 号

核电厂设计中的人因工程

特定安全导则

国 际 原 子 能 机 构
2024 年 · 维也纳

版 权 说 明

Marketing and Sales Unit,
Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
传真：+43 1 2600 22529
电话：+43 1 2600 22417
电子信箱：sales.publications@iaea.org
https://www.iaea.org/zh/chu-ban-wu

国际原子能机构印刷
2024 年 2 月 • 奥地利

核电厂设计中的人因工程

国际原子能机构，奥地利，2024 年 2 月
STI/PUB/1843
ISBN 978-92-0-506423-9（简装书：碱性纸）
978-92-0-506323-2（pdf 格式）
ISSN 1020-5853

前　言

国际原子能机构（原子能机构）《规约》授权原子能机构“制定或采取旨在保护健康及尽量减少对生命与财产的危险的安全标准”。这些标准是原子能机构在其本身的工作中必须使用而且各国通过其对核安全和辐射安全的监管规定能够适用的标准。原子能机构与联合国主管机关及有关专门机构协商进行这一工作。定期得到审查的一整套高质量标准是稳定和可持续的全球安全制度的一个关键要素，而原子能机构在这些标准的适用方面提供的援助亦是如此。

原子能机构于1958年开始实施安全标准计划。对质量、目的适宜性和持续改进的强调导致原子能机构标准在世界范围内得到了广泛使用。《安全标准丛书》现包括统一的《基本安全原则》。《基本安全原则》代表着国际上对于高水平防护和安全必须由哪些要素构成所形成的共识。在安全标准委员会的大力支持下，原子能机构正在努力促进全球对其标准的认可和使用。

标准只有在实践中加以适当应用才能有效。原子能机构的安全服务涵盖设计安全、选址安全、工程安全、运行安全、辐射安全、放射性物质的安全运输和放射性废物的安全管理以及政府组织、监管事项和组织中的安全文化。这些安全服务有助于成员国适用这些标准，并有助于共享宝贵经验和真知灼见。

监管安全是一项国家责任。目前，许多国家已经决定采用原子能机构的标准，以便在其国家规章中使用。对各种国际安全公约缔约国而言，原子能机构的标准提供了确保有效履行这些公约所规定之义务的一致和可靠的手段。世界各地的监管机构和营运者也适用这些标准，以加强核电生产领域的安全以及医学、工业、农业和研究领域核应用的安全。

安全本身不是目的，而是当前和今后实现保护所有国家的人民和环境的目标的一个先决条件。必须评定和控制与电离辐射相关的危险，同时杜绝不当限制核能对公平和可持续发展的贡献。世界各国政府、监管机构和营运者都必须确保有益、安全和合乎道德地利用核材料和辐射源。原子能机构的安全标准即旨在促进实现这一要求，因此，我鼓励所有成员国都采用这些标准。

国际原子能机构安全标准

背景

放射性是一种自然现象，因而天然辐射源的存在是环境的特征。辐射和放射性物质具有许多有益的用途，从发电到医学、工业和农业应用不一而足。必须就这些应用可能对工作人员、公众和环境造成的辐射危险进行评定，并在必要时加以控制。

因此，辐射的医学应用、核装置的运行、放射性物质的生产、运输和使用以及放射性废物的管理等活动都必须服从安全标准的约束。

对安全实施监管是国家的一项责任。然而，辐射危险有可能超越国界，因此，国际合作的目的就是通过交流经验和提高控制危险、预防事故、应对紧急情况和减缓任何有害后果的能力来促进和加强全球安全。

各国负有勤勉管理义务和谨慎行事责任，而且理应履行其各自的国家和国际承诺与义务。

国际安全标准为各国履行一般国际法原则规定的义务例如与环境保护有关的义务提供支持。国际安全标准还促进和确保对安全建立信心，并为国际商业与贸易提供便利。

全球核安全制度已经建立，并且正在不断地加以改进。对实施有约束力的国际文书和国家安全基础结构提供支撑的原子能机构安全标准是这一全球性制度的一座基石。原子能机构安全标准是缔约国根据这些国际公约评价各缔约国遵约情况的一个有用工具。

原子能机构安全标准

原子能机构安全标准的地位源于原子能机构《规约》，其中授权原子能机构与联合国主管机关及有关专门机构协商并在适当领域与之合作，以制定或采取旨在保护健康及尽量减少对生命与财产之危险的安全标准，并对其适用作出规定。

为了确保保护人类和环境免受电离辐射的有害影响，原子能机构安全标准制定了基本安全原则、安全要求和安全措施，以控制对人类的辐射照射和放射性物质向环境的释放，限制可能导致核反应堆堆芯、核链式反应、辐射源或任何其他辐射源失控的事件发生的可能性，并在发生这类事件时减轻其后果。这些标准适用于引起辐射危险的设施和活动，其中包括核装置、辐射和辐射源利用、放射性物质运输和放射性废物管理。

安全措施和安保措施 [1] 具有保护生命和健康以及保护环境的共同目的。安全措施和安保措施的制订和执行必须统筹兼顾，以便安保措施不损害安全，以及安全措施不损害安保。

原子能机构安全标准反映了有关保护人类和环境免受电离辐射有害影响的高水平安全在构成要素方面的国际共识。这些安全标准以原子能机构《安全标准丛书》的形式印发，该丛书分以下三类（见图 1）。

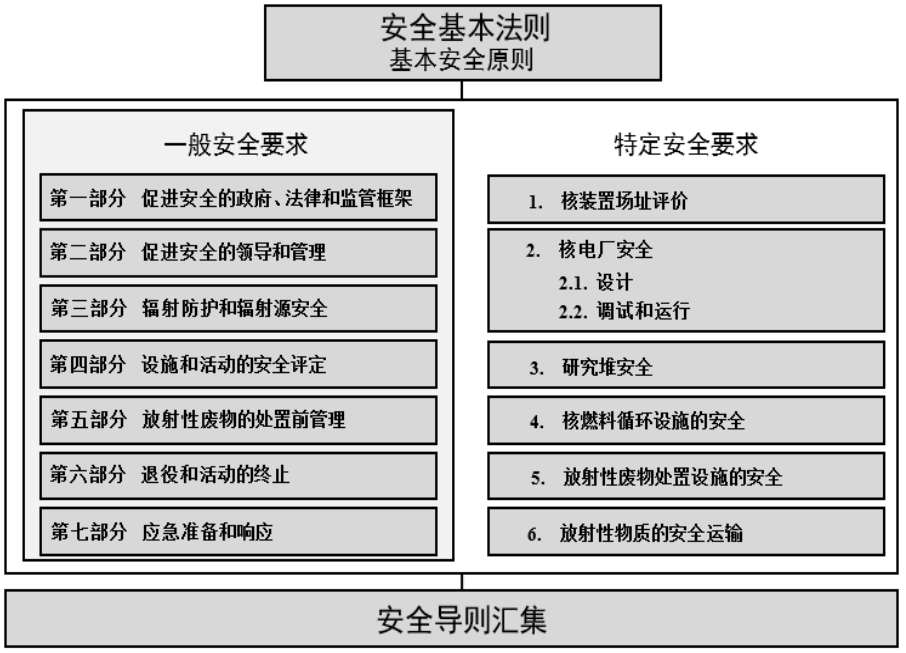

图 1. 国际原子能机构《安全标准丛书》的长期结构。

[1] 另见以原子能机构《核安保丛书》印发的出版物。

安全基本法则

“安全基本法则”阐述防护和安全的基本安全目标和原则，以及为安全要求提供依据。

安全要求

一套统筹兼顾和协调一致的“安全要求”确定为确保现在和将来保护人类与环境所必须满足的各项要求。这些要求遵循“安全基本法则”提出的目标和原则。如果不能满足这些要求，则必须采取措施以达到或恢复所要求的安全水平。这些要求的格式和类型便于其用于以协调一致的方式制定国家监管框架。这些要求包括带编号的“总体”要求用“必须”来表述。许多要求并不针对某一特定方，暗示的是相关各方负责履行这些要求。

安全导则

“安全导则”就如何遵守安全要求提出建议和指导性意见，并表明需要采取建议的措施（或等效的可替代措施）的国际共识。“安全导则”介绍国际良好实践并且不断反映最佳实践，以帮助用户努力实现高水平安全。“安全导则”中的建议用“应当”来表述。

原子能机构安全标准的适用

原子能机构成员国中安全标准的使用者是监管机构和其他相关国家当局。共同发起组织及设计、建造和运行核设施的许多组织以及涉及利用辐射源和放射源的组织也使用原子能机构安全标准。

原子能机构安全标准在相关情况下适用于为和平目的利用的一切现有和新的设施和活动的整个寿期，并适用于为减轻现有辐射危险而采取的防护行动。各国可以将这些安全标准作为制订有关设施和活动的国家法规的参考。

原子能机构《规约》规定这些安全标准在原子能机构实施本身的工作方面对其有约束力，并且在实施由原子能机构援助的工作方面对国家也具有约束力。

原子能机构安全标准还是原子能机构安全评审服务的依据，原子能机构利用这些标准支持开展能力建设，包括编写教程和开设培训班。

国际公约中载有与原子能机构安全标准中所载相类似的要求，从而使其对缔约国有约束力。由国际公约、行业标准和详细的国家要求作为补充的原子能机构安全标准为保护人类和环境奠定了一致的基础。还会出现一些需要在国家一级加以评定的特殊安全问题。例如，有许多原子能机构安全标准特别是那些涉及规划或设计中的安全问题的标准意在主要适用于新设施和新活动。原子能机构安全标准中所规定的要求在一些按照早期标准建造的现有设施中可能没有得到充分满足。对这类设施如何适用安全标准应由各国自己作出决定。

原子能机构安全标准所依据的科学考虑因素为有关安全的决策提供了客观依据，但决策者还须做出明智的判断，并确定如何才能最好地权衡一项行动或活动所带来的好处与其所产生的相关辐射危险和任何其他不利影响。

原子能机构安全标准的制定过程

编写和审查安全标准的工作涉及原子能机构秘书处及分别负责应急准备和响应（应急准备和响应标准委员会）（从 2016 年起）、核安全（核安全标准委员会）、辐射安全（辐射安全标准委员会）、放射性废物安全（废物安全标准委员会）和放射性物质安全运输（运输安全标准委员会）的五个安全标准分委员会以及一个负责监督原子能机构安全标准计划的安全标准委员会（安全标准委员会）（见图 2）。

原子能机构所有成员国均可指定专家参加四个安全标准分委员会的工作，并可就标准草案提出意见。安全标准委员会的成员由总干事任命，并包括负责制订国家标准的政府高级官员。

已经为原子能机构安全标准的规划、制订、审查、修订和最终确立过程确定了一套管理系统。该系统阐明了原子能机构的任务；今后适用安全标准、政策和战略的思路以及相应的职责。

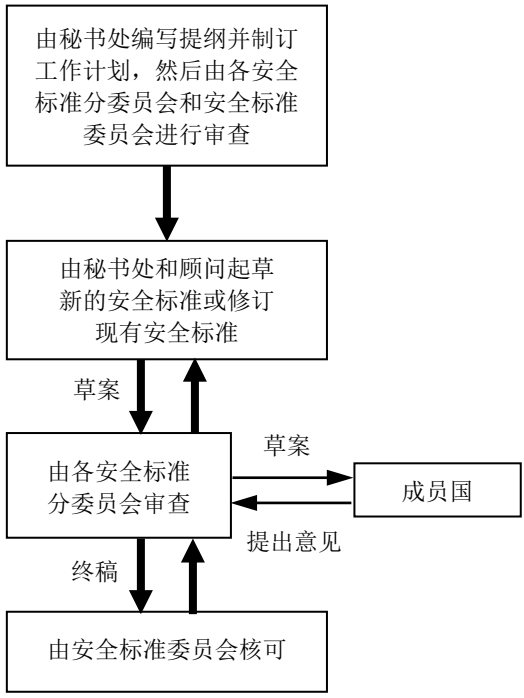

图 2. 制订新安全标准或修订现行标准的过程。

与其他国际组织的合作关系

在制定原子能机构安全标准的过程中考虑了联合国原子辐射效应科学委员会的结论和国际专家机构特别是国际放射防护委员会的建议。一些标准的制定是在联合国系统的其他机构或其他专门机构的合作下进行的，这些机构包括联合国粮食及农业组织、联合国环境规划署、国际劳工组织、经合组织核能机构、泛美卫生组织和世界卫生组织。

文本的解释

安全相关术语应按照《国际原子能机构安全术语》（见 http://www-ns.iaea.org/standards/safety-glossary.htm）中的定义进行解释。否则，则采用具有最新版《简明牛津词典》所赋予之拼写和含义的词语。就“安全导则”而言，英文文本系权威性文本。

原子能机构《安全标准丛书》中每一标准的背景和范畴及其目的、范围和结构均在每一出版物第一章“导言”中加以说明。

在正文中没有适当位置的资料（例如对正文起辅助作用或独立于正文的资料；为支持正文中的陈述而列入的资料；或叙述计算方法、程序或限值和条件的资料）以附录或附件的形式列出。

如列有附录，该附录被视为安全标准的一个不可分割的组成部分。附录中所列资料具有与正文相同的地位，而且原子能机构承认其作者身份。正文中如列有附件和脚注，这些附件和脚注则被用来提供实例或补充资料或解释。附件和脚注不是正文不可分割的组成部分。原子能机构发表的附件资料并不一定以作者身份印发；列于其他作者名下的资料可以安全标准附件的形式列出。必要时将摘录和改编附件中所列外来资料，以使其更具通用性。

目 录

1. 导言

背景

1.1. 本“安全导则”就人因工程（HFE）[1] 的实施提出建议，以满足原子能机构《安全标准丛书》第 SSR-2/1（Rev.1）号《核电厂安全：设计》[1]、SSR-2/2（Rev.1）《核电厂安全：调试和运行》[2]和 GSR Part 4（Rev.1）《设施和活动的安全评定》[3]要求。

1.2. 本“安全导则”已经考虑了把人因工程的形成、经验和实践，融入到核电厂全寿期设计中。它参照并把原子能机构其他有关和相关的将人因工程融进设计的《安全标准丛书》出版物也考虑在内。包括原子能机构《安全标准丛书》第 GSR Part 2 号《安全的领导和管理》[4]，及其对安全导则给予的支持，原子能机构《安全标准丛书》第 GS-G-3.1 号《设施和活动管理系统的适用》[5]和第 GS-G-3.5 号《核装置管理系统》[6]。

1.3. 本“安全导则”为重要的领域提供了指导：

- 为了达到符合 SSR-2/1（Rev.1）[1]要求，在对电厂所有状态的人因界面（HMI）设计中使用人因工程流程；
- 为了达到符合 GSR Part 2[4]要求，将人因工程融入到对核电厂全寿期的设计中；
- 核电厂全寿期的人的绩效监控和评价；
- 将人因工程整合到安全流程、实施以及安全产品的选择范围。

1.4. 本“安全导则”考虑了与设计相关联的多个重要流程的人因工程，如：

- 安全分析报告的形成和评审；
- 为达到符合 SSR-2/2（Rev.1）[2]要求而进行的电厂改造；
- 定期安全评审。

[1] “人因工程”是指理解和考虑可能影响人的绩效和可能影响安全因素的工程，特别是在设施的设计和运行中。

1.5. 本“安全导则”考虑了针对设计的相关人因工程以及计算机程序的使用。

1.6. 本“安全导则”考虑了在现有电厂系统中，对各自产品的选择、采购、集成和使用的相关人因工程方面，如：

— 个人防护设备（例如，在维护活动、视察、事故监控，以及缓解严重事故的设备运行期间所使用的个人防护设备）；
— 工业用的现成产品；
— 移动设备（例如手持、便携式和可穿戴设备）。

1.7. 关于人因工程在人因界面的设计和形成中的补充导则，可从形成工业标准的机构得到（见附件）。这种标准比原子能机构的安全标准更为详细。要求本“安全导则”与此类详细的行业标准一起使用。

目的

1.8. 本“安全导则”的目的，是为人因工程在人因界面的设计和改造中的实施，提供一种结构化的方法与指导，以最大限度地减少人因失误的风险，优化人的绩效来确保核电厂的安全运行。

1.9. 鉴于人因界面是人的切身感受与认知过程的基础，本“安全导则”对设计并认可的人因界面所需的输入信息进行确认。

范围

1.10. 本“安全导则”主要适用于陆上、固定式、商用的核电厂。它也可以适用于其他类型的反应堆（例如小型模块化反应堆），这需要采取相应的判断，来决定在设计中必须要考虑的导则。

1.11. GSR Part 2[4]所述的分级方法，将适用于推荐给本“安全导则”。

1.12. 本“安全导则”适用于对新电厂在设计、运行和维护的人因界面中的人因工程实施，同样也适用于现有电厂人因界面的改造。

1.13. 本“安全导则”旨在针对核电厂的设计、制造、建造、改造、维护、运行和退役的相关组织和监管机构，用来进行分析、核实、验证、实施和监控，以及对技术支持进行的准备。

1.14. 本“安全导则”不针对核安保用途的人因工程实施。

结构

1.15. 第 2 部分为人因工程计划的管理提供指导；第 3 部分为运行经验、用途分析；功能分配；任务分析；人员的配置分析、组织与资质的评审提供建议，以及对重要的人的任务探讨；第 4 部分对人因工程在设计中的应用给出了建议；第 5 部分对设计过程中就相关对人因的核实和验证提供了指导；第 6 部分就人因界面的设计实施给出了建议；第 7 部分就电厂运行期间，人员对系统性能进行监控的绩效给出了建议；第 8 部分就人因工程在计算机程序设计中的实施给出了建议；第 9 部分给出了将人因工程整合到安全管理流程中的建议；第 10 部分就人因工程在分包采购的技术规范和产品选择中的实施给出了建议。附件提供了国际上仪器仪表和控制的行业标准清单，以及与本“安全导则”当前重要领域有密切关系的人因工程清单。

2. 人因工程计划管理

概述

2.1. GSR Part 2[4]对管理系统的所有设施和活动的类型确立了要求。

2.2. GSR Part 2[4]要求 6 规定：**“管理系统应将包括其安全、健康、环境、安保、质量、人与组织因素、社会和经济等要素融为一体，以使安全不受到损害。”**

2.3. GSR Part 4[4]第 4.24 段指出：

> “支撑组织内部机构的能力应包括：对所有管理层级的领导能力；对强有力的安全文化的培养与持续保持的能力；以及为确保安全，对与设施或活动相关的技术理解、人与组织方面的专业知识。”

2.4. 应确保人因工程能做到把人的特征与能力，融入到核电厂的设计、调试、运行和维护中。

2.5. 应对人因工程融入设计进行计划并提供文件，并应是任何核电厂项目不可缺少的一部分。

2.6. 应形成人因工程的计划并提供文件。

2.7. 在人因工程计划中，应把核电厂看作是一个由人、技术和组织组成的系统，并应考虑到所有相关因素和其中的一个因素产生的动态相互作用：

— 人的因素（如知识和专业技能、认知、表现要求、积极性、精神压力、体力和体型大小）；
— 技术因素（如包括控制和显示、软件、硬件、工具、设备、电厂设计和电厂流程等技术）；
— 组织因素（如管理系统、组织机构、治理、资源、为各层级配置人员，以及负责人和电厂其他人员的作用和责任）。

2.8. 在人因界面设计和对电厂所有的状态进行资源分配期间，在人因工程计划的制定与执行中，始终以融为一体的方式来考虑人、技术和组织，以及它们之间的相互作用。

2.9. 在人因工程计划中，应以新形成的信息、分析方法、知识，以及所考虑的新技术特点，对通用的设计方法和解决方案采取质疑和学习的态度。

2.10. 为了确认所用人因工程计划对应的严谨程度、资源及细节，应采用GSR Part 2[4]所述的分级方法。

2.11. 人因工程计划应对人因工程活动，以及对这些活动流程的输入和输出进行概述。人因工程活动包括对人因界面的分析与设计，对人的绩效进行核实与验证的评价与监控（见第 2.19 段）。

2.12. 人因工程计划应具体说明人因工程如何与电厂的其他设计或改造活动进行融合。

2.13. 人因工程计划应对负责人因工程计划、任务与设计授权的人员，以及来自电厂其他部门人员之间必需协调的工作进行确认。

2.14. 为了对负责工程设计的部门表达分析的结果，并确保该结果已得到了处理，应建立相应的流程并提供证明文件。

2.15. 人因工程计划应对相关组织上的要求，以及对执行人因工程活动人的能力要求（如资质、技能、知识和培训）进行确认。

2.16. 人因工程计划应对由人因工程流程确认出的相关人因工程的问题，提供一个用来进行记录与跟踪的框架。

2.17. 人因工程计划应对设计团队中需具备人因工程专业知识的一名或多名成员给予规定。

2.18. 对于新电厂的设计，营运组织应确保其想要的电厂设计符合人因工程相应的标准和本“安全导则”给出的建议。

人因工程流程模式

2.19. 总体的人因工程流程可分为以下人因工程活动：

— 计划管理；
— 分析；
— 设计；
— 核实和验证；
— 设计实施；
— 对人的绩效进行的监控。

工程项目中的人因工程活动

2.20. 应将人因工程的活动融入到工程设计项目的初始阶段，如图 1 中所示。

2.21. 应将以下内容看作是对概念形成阶段的人因工程输入：

— 人因工程计划的管理部门应确认一个系统的、整体的人因工程流程，应对人因工程流程的责任进行概述，并应提出对人因工程流程所要求的设计输入和输出。

— 人因工程计划的管理部门应确立一个组织上能对人因负责的部门，并在所有等级水平上有充分的授权，来实施符合人因工程要求所需的设计变更。

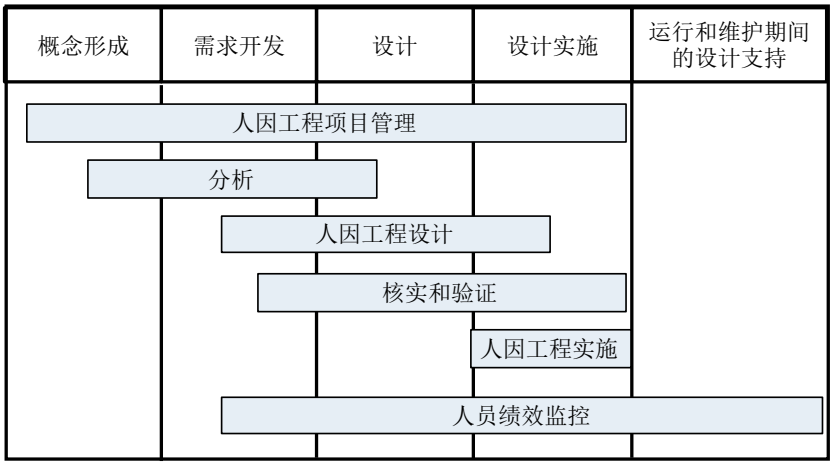

图 1. 一般工程设计项目的示例，表明开展人因工程活动的时间。

— 人因工程计划的管理部门应对适用于工程设计项目的最新相关人因工程规范、标准、方法和导则进行确认。

— 人因工程分析部门应对相关的运行经验（正面和负面）予以确认，重点是人的绩效问题和可能的人因失误及其缓解措施。

— 人因工程分析部门应对相关设计选择范围的定义与筛选提供有用的输入（如运行人员的需求和要求）。

— 人因工程分析部门应被用来对人因工程计划中使用的组织机构框架进行确认（即对用户的鉴定，用户的作用和责任，所需资质和监管要求），并对运行和维护部门给予帮助。

— 人因工程分析部门应对电厂中适用的系统功能，给出功能分配的初始解释，以及对人进行监控与控制的信息要求。

— 在出现控制系统和人因界面故障时要求运行人员如何回应，应由人因工程分析部门给出深刻见解与考虑。

2.22. 应将以下内容视为需求形成阶段的人因工程输入：

— 功能分析是用来对结构、系统和部件的功能需求进行确认的。
— 任务分析是用来深入了解：
  - 需要什么类型的警报、信息、程序、控制和系统反馈；
  - 可能的任务顺序；
  - 可能的人为失误和需要考虑的对人的绩效影响因素，并给出减少失误并提高绩效的设计之处；
  - 以详细的技术和人因工程分析来作为保证的重要安全且复杂的任务；
  - 重大任务的时限；
  - 为完成所分配的任务并满足业务目标，人所需的特定知识、技能与能力；
  - 为支持任务所必要的个人或团体间的合作与协调。
— 为了形成针对供应商的技术规范，而对人因工程设计原则和人因界面设计导则进行具体说明，并将其纳入到供应商的人因工程的技术规范中。

2.23. 应将以下内容视为在设计阶段的人因工程输入：

— 因设计的改进或标准的变化而更新了对人因工程的要求；
— 对电厂的技术规范和工作区的设计与布置，以及人因界面部件及其系统结构的人因工程设计原则和人因界面设计导则给予特定说明；
— 对维护和试验的人因工程设计原则和人因界面设计导则给予具体说明；
— 新的或修改的设计可能对人的绩效，以及程序的形成与培训造成的影响；
— 通过初期的以用户友好性试验的形式进行的人因工程分析，以及用户对原型和概念的评审来收集并分析用户的反馈；
— 通过对使用的运行程序范围、内容及用户友好性的深刻了解来帮助安全关键任务的执行；
— 对培训的范围和内容的深刻了解。

2.24. 应将以下内容视为设计实施阶段的人因工程输入：

— 对照先前确认的人因工程设计原则和适用的人因工程设计规范、标准和导则来核实设计实施；
— 确保执行了设计中已规定任务所需要的全部信息与控制来验证设计实施；
— 对确定关于人因界面的人因设计深度，以及帮助电厂促进对安全运行实现方法的认可；
— 在概率和确定性安全分析中通过对关于人因的认可，来对重要的人的任务可行性进行验证；
— 根据人因工程计划和监管的要求，来对人因工程分析的结束以及人因工程对设计的输入进行确认。

2.25. 在整个设计阶段，应把被视为是技术限制（如对技术的可用性、可靠性、使用频率，以及人员的普遍接受与熟悉程度）的因素考虑进去。例如，虽然工作人员接受在日常生活中使用数字技术，但设计者可能需要考虑到使用虚拟现实或增强现实是否会给工作人员带来麻烦。

2.26. 为了核实设计阶段对电厂全寿期一直有效的分析与假设，应在运行和维护阶段对设计的支持中安排对人的绩效的监控。

2.27. 对人因工程的分析、设计、核实和验证等支持活动，应以与总体的设计计划相符的迭代方式来进行安排。

2.28. 对人因工程的分析、设计、核实和验证等支持活动，经常是相互合作的，并应有人因工程专门知识的多学科团队的参与。为了让人因工程的分析、设计以及核实和验证活动的结果具有充分的针对性，应将其传达给参与设计的其他组织单位。

2.29. 应从以下角度来对待人因界面及其实用性，即人因界面是一个一体化整体的组成部分，且不只是对不相关联的控制、指示器和系统进行的装配。

3. 分析

运行经验评审

3.1. SSR-2/2（Rev.1）[2]第 5.28 段指出：“对安全可能产生重大后果的事件应进行调查以确认其直接和根本原因，包括与设备设计、运行和维护相关的原因，或与人和组织因素相关的原因。”

3.2. 事件分析的数据和结论应用作对新电厂或对现有电厂改造的人因工程设计的输入。

3.3. 运行经验评审应就相关当前的工作实践提供如下用途的信息：(i) 对已安排变更可能产生的影响进行评定；(ii) 对电厂设备进行现代化升级和改造期间，对运行问题和当前设计中需要解决的困难进行评价；(iii) 为了提高对电厂效率和安全的可能性，对仪器仪表和控制系统和人因界面技术进行设计选择的行业经验进行评价。

3.4. 在评审运行经验时，应从正反两个方面对工作绩效和设计进行分析。

3.5. 运行经验评审应把以下内容考虑在内：

— 在对核电厂的运行经验评审中，确认相关人因工程的问题；
— 从电厂人员的经验中确认的见解；
— 在运行经验评审中，在其他核电厂和其他行业所确认的问题。

3.6. 应将下列任何一项的运行经验数据考虑在内：

— 小问题（如未遂事件或低级别事件），这些小问题往往是更重大事件的前兆或促成因素；
— 能表明可靠性降低的负面趋势；
— 能表明需要改进设计的根本原因的数据；
— 能证明组织文化对今后运行造成困难的影响与趋势的证据；
— 纠正行动及其落实；
— 反复发生的事件；
— 对维护实践的评审；
— 最佳实践的行业交流。

3.7. 原子能机构《安全标准丛书》第 SSG-50 号《核装置运行经验反馈》[7]，对确立、执行、评定和持续改进核设施运行经验管理计划给出了建议，通过对在设施上或其他地方已经发生的事件中吸取教训，防止或尽量减少今后发生事件的风险。

功能分析

3.8. 应对核电厂的所有状态安排一次功能分析，对完成核电厂安全运行所必需的功能，都确保得到了充分完整的界定与正确的分析。

3.9. 功能分析应提供一个对控制电厂的人员职责进行熟悉的框架。

3.10. 功能分析应用来对功能信息进行识别（例如，在什么时候需要、可得到、起作用的功能，在什么时候完成或终止该功能意图的信息），并对需要由人来完成运行目标的控制进行确认。

3.11. 功能分析应给出时间与性能上的要求，以及在执行功能时的约束条件。

3.12. 在进行功能分析时应考虑人、技术和组织的因素。

3.13. 功能分析应用来对保持电厂安全运行相关的高水平验收标准进行确认。

3.14. 作为功能分析的一部分，应分析并提供以下内容的文件：

— 确保电厂安全运行的高级别功能；
— 高级别功能和负责执行这些功能的电厂系统之间的关系（例如电厂配置或成功动作路径 [2]）；
— 对由电厂自动化设备或人执行的任务，或由人和自动化设备共同执行的任务，能在图上标出高级别功能到低级别功能的分解图；
— 对人和自动化设备的作用与责任进行确定的系统。

[2] “成功动作路径”是指在核电厂发生某一事故后，有很大把握使核电厂顺利达到安全状态的一整套选定结构、系统和部件。

3.15. 利用系统和流程的组合来完成某一高级别的功能以及成功实践需要人的行动，都应作为功能分析的一部分而记录在案。

3.16. 电厂功能、电厂系统及其支持系统间可能存在的依赖关系，应作为功能分析的一部分而提供证据文件。

功能分配

3.17. 应为核电厂所有的状态安排功能分配，对完成核电厂安全运行所必需的功能都确保得到了充分完整的界定与正确的分析。

3.18. 对人和自动化设备的功能分配，应把人的能力（如临时应变的能力、灵活性、判断力与模仿监控力）和机器的优势（如对复杂操作可迅速并同时进行处理）考虑在内。

3.19. 在进行功能分配时应考虑人、技术和组织的因素。

3.20. 设计团队应利用对实际流程、当前行业的技术、运行经验，以及人的绩效的强弱程度与薄弱环节的了解，来对人和自动化设备（如硬件和软件）进行功能分配。

3.21. 功能分配利用对电厂控制系统的功能分析，建立了可按以下实践对控制流程的分配进行布置：

- 对人（如没有自动化设备的手动控制）。
- 对自动系统（如全自动控制和非能动的、自我管理的情况）。
- 对人和自动化设备的组合动作，例如：
  - 共有的动作（即，某些功能是自动动作，而其他方面是手动执行的）；
  - 经许可或授权的动作（即，当人给予许可且情况允许时，自动化设备对功能执行的控制）；
  - 特殊的动作（即，功能的自动动作，除非存在专门说明的预先规定情况或必须要手动控制的客观情况）。

3.22. 除了考虑人的能力外，设计人员在对功能进行分配时还应把这样的因素考虑在内：技术对人是否是可接受的、与系统响应相关的时长性能，以及对纵深防御要考虑的因素等。

3.23. 如果控制功能的实现，需要对人和自动化设备的作用（例如，指派人负责对自动系统进行的监控与监督）的重叠部分和多余的部分进行分配，这种分配应被记录在案。

3.24. 对所有功能中属于由人来完成的任务，以及任务的范围提供证明文件。

3.25. 应针对不同的运行状态和事故工况来对功能分配进行分析。

3.26. 功能分析和功能分配应考虑到严重事故管理标准的相关要求。

3.27. 功能分配应是从功能一直可追溯到相关的系统或部件。

任务分析

3.28. 任务分析的方法应把电厂状态以及与所分析任务相关的运行人员团队（如反应堆操纵员、汽轮机操纵员、值长、现场操纵员、安全工程师以及运行和维护的全部人员）考虑进去。

3.29. 在进行任务分析时，应考虑到人、技术和组织的因素（如领导力、管理部门和交流）。

3.30. 对分配到人的任务应安排任务分析，对执行任务时的体力与认知活动进行分析和记录。

3.31. 任务分析应从用户完成任务的角度把任务的背景也包含进去。

3.32. 在核电厂中的个人责任和活动范围很广，因此，应合理制定分析范围，通常包括：

— 在不同地点执行的任务（例如控制室、应急控制室、就地控制站、应急响应设施）；
— 任务的差别随电厂状态的变化；

— 需要单独工作的任务，和（或）需要不同的内部部门（例如运行、维护、程序编写和计算机系统设计）和相关各方间配合或互动的任务；
— 有时在时间压力下，或者在艰苦的环境条件和背景下不得不执行的任务，或者是安全临界且很少被执行的任务。

3.33. 在任务分析中对所包含的任务进行确认时，还应考虑任务的风险和安全，应包括：

— 对人员构成职业风险的任务；
— 被算作是安全分析中的任务；
— 从运行经验中确认的被当作考验能力的或容易失误的任务；
— 由运行人员确认的被当作困难的任务，且为此尚没有计划让任务通过自动化设备来执行；
— 保持电厂始终处于临界安全状态的任务，或者事件后使电厂重新恢复到安全状态的任务。

3.34. 还应对运行人员对警报的响应，以及从主控室对监视和维护发出指令的任务进行分析。

3.35. 任务分析的结果应可用来确认：

— 要求由人来完成的任务，以及可能影响安全的人为失误；
— 关于如何执行每项任务的要求、所要求的任务结果，以及任务的人的绩效准确性的评定；
— 对安全临界任务在现场的失误预防方法；
— 受影响的安全功能，以及每项任务的开始条件和终止状态；
— 执行任务和子任务的顺序；
— 人的需求（如组织上的、人的配置、资质和培训）、设备需求（如人因界面的基本组成、专用工具和防护服）和文件需求（如程序、流程和工作说明）；
— 人的绩效的要求与限值（例如时间、精度和独立核实）；
— 所需的通信系统和对这些系统的使用。

3.36. 为了进行任务分析，应考虑源自以下的信息：

— 文件（供应商文件、技术规范、现有程序、手册和培训材料）；
— 设计团队中知识丰富的人员、在类似电厂获得运行经验的运行人员、相关各方和其他行业的专家；
— 通过在相似电厂上对原有系统和任务的任务分析，包括对正在开发的相关系统任务来进行推演并“说透”；
— 对运行经验评审的数据（考虑到与参考设计的差异）；
— 客户需求的数据；
— 作为人因工程设计流程输入的其他分析数据（例如，功能分析和分配，以及重要的人的任务处理）；
— 模拟机的研究数据；
— 国际上的人因工程标准（另见附件）。

3.37. 进行任务分析所采用的技术的选择应具有正当性。

3.38. 评价人的可靠性对任务绩效要求的影响。

3.39. 应对任务分析的输入数据收集、列表和分析的流程提供证明文件。

3.40. 任务分析是一项合作的活动，且应需要一个具有人因工程和运行方面专业知识的多专业学科的团队参与。

3.41. 任务分析的结果应传达给参与设计的其他组织单位供其考虑。

3.42. 任务分析的结果可以直接用于支持对人因失误的评定。

3.43. 任务分析应专门针对任务的认知流程进行分析，如重要的决策、问题解决、记忆力、注意力和判断等。

3.44. 仅对文件（如程序）进行台面上的分析可能不足以确定是否可以执行一项或多项任务。可以通过仿制、电厂巡检、可执行的部分任务模拟机或全范围模拟机的帮助，从模拟的输入来对任务在实际假想方案中的可行性进行证实。

3.45. 任务分析应包括对失误分类的方法，它至少可以对可能遗漏的失误和正在犯的失误进行准确记录，包括与每项任务相关的决策失误和传达失误。

人员配置、组织和资质分析

3.46. 为了确定完成的重要任务所需人数、组织上的交流以及人的资质，应分析人的配备、组织机构和人的资质对其造成的影响。

3.47. 如果对已有电厂或新电厂进行改造，对人的配备、组织及资质进行的分析，与参考电厂相比的任何改造都应考虑在内，其可能会影响到：

— 任务安全完成；
— 工作负荷；
— 团队每个成员的作用与团队任务的匹配能力；
— 负责检查任务进展的个人的自立与协作（如运行人员在主控室和就地采取的检查行动）；
— 人对任务的看法及其津贴，以及对任务的认同。

3.48. 人的配备、组织和资质分析应包括执行对安全有影响的任务的所有团队（关于任务分析见第 3.28—3.45 段）。这包括所有的运行人员团队、电厂技术支持团队，以及应急准备和响应团队。分析应从这些团队对人的配备、组织和资质需求的角度，来进行确认与评价。

3.49. 人的配备、组织和资质分析，应就参考电厂的组织及技术差异产生的影响进行评价。

3.50. 对人的配备、组织和资质分析的输入应包括：

— 在运行状态和事故工况中的运行概念；
— 设计要求；
— 任务要求；
— 监管要求；
— 运行经验；
— 对由人来完成的重要任务的处理（如，为了确保某些任务的准确完成，对由人来完成的重要任务的处理可能对必须实行两个人的规则进行确定）。

3.51. 任务分析应用来帮助对团队的作用、要求及职责，以及所需的工作成果进行界定。

3.52. 当给团队成员指派单独的任务时，应确保：

— 指派给每个成员的任务应被明确说明；
— 任务分配的依据应被确定并说明正当性；
— 在所有的运行状态和事故工况中，团队每个成员的工作量都应是合理的；
— 在白班团队和夜班团队之间分配任务时，应把对人的绩效影响考虑进去；
— 对团队成员指派的任务是以多种运行职位要求具备的任务时，要以确保责任的连续性方式来进行，并保持个人及团队的职位意识。

3.53. 应通过模式设计、分析或全范围模拟机的试验，对可能影响安全的人的配备的任何缩减进行评价。

重要人工任务的处理

3.54. 由人来完成的重要任务和行动应该从概率安全分析或确定性安全分析中进行确认。

3.55. 对由人来完成的重要任务进行裁定的基本方法，是把运行的状态以及在事故工况下的响应考虑进去。

3.56. 分析可以采取定性和/或定量分析的形式，来对人因工程在设计中的实施提供帮助。

3.57. 至少应对属于安全分析中的由人来完成的重要任务和行动，包括影响绩效的相关因素进行分析，并应对设计解决计划是否满足相关人的绩效这样的安全要求进行核实。

3.58. 无论采取何种方法来对重要的人的任务，设计、程序、培训、人的配备水平和运行概念进行确认，都应对重要的人的决定与行动的执行给予帮助。

3.59. 对电厂的改造，可能会按照执行由人来完成的重要任务的方式而变样。对于电厂的所有改造，对是否仍能可靠地执行相关的由人来完成的重要任务应进行评定。

4. 设计

概述

4.1. SSR-2/1（Rev.1）[1]要求 32 规定：**“在核电厂设计过程的早期阶段就应包含对人因，包括人因接口的系统性考虑，并在整个设计过程中应自始至终都是延续进行的。”**

4.2. SSR-2/1（Rev.1）[1]第 5.55 段指出：

> “设计应支持运行人员履行职责和执行任务，并应限制由于操作失误而对安全可能和已产生的影响。设计过程应对电厂布置和设备布置，以及包括维护和视察程序进行妥善考虑，以便在电厂所有工况下让运行人员与电厂之间的互动更为容易。”

4.3. SSR-2/1（Rev.1）[1]第 5.56 段指出：

> “人因界面的设计应根据必要的决策次数和行动次数，为运行人员提供不但易于管理而且是综合的信息。运行人员对行动决策的必要信息应是表达简明且不含糊的信息。”

4.4. 应通过一种结构化的方法来设计人与机器间的相互作用，从概念设计开始，到人因界面候选计划的确认与选择，以及到详细设计的界定都采取许可方式，并在必要时对人因界面试验的性能与评价也采取许可的方式。

4.5. 在人因界面的设计中应采用纵深防御的概念，以确保一旦发生故障，将通过相应的手段来察觉到故障并抵消故障影响，或直接给予纠正。

4.6. 设计应以从履行相关职责和任务人员的视角，采用以人为核心的方法去考虑设备和系统。

4.7. 在设计过程的所有阶段都应考虑到人的方面、技术（硬件和软件）、工作环境以及将要实施的控制、运行和管理策略（按照综合、系统的方法）。

4.8. 设计人员应考虑经由人因界面转达的信息，将如何被不同的工作组（例如，主控室和应急响应设施中的工作人员）来进行传递、交换和使用。

4.9. 设计人员应考虑到必要的约束条件，并确保设计中具有灵活性，以便针对不同的电厂状态和电厂运行模式采取不同的控制和运行策略。

4.10. 设计需要考虑为运行人员及其组织对事件的恢复能力做如下试验上的准备：

— 对假想始发事件的响应是否正确分配了自动动作；
— 对意外事件的预计与响应人因界面是否能够给予支持；
— 在对意外崩溃或故障状态的预计中人因界面是否提供递增变化的信息（如使用预测性显示）；
— 对补充的工具及设备是否预备并选定好可用的存放位置；
— 在营运组织就电厂系统对严重事故的响应进行“压力试验”时，是否为运行人员如何能够将设备用于原设计意图以外的目的以保护裂变产物边界提供了建议；
— 是否必须采取不同的运行策略以便在事件发生时达到安全状态；
— 设备是否可以超出设计意图而使用，以支持采用不同的策略（例如，利用消防系统进行排热）。

人因界面设计输入

4.11. 人因界面设计中要考虑的要求，应通过在设计过程早期阶段进行的以下分析来确认（见第 3 部分）：

— 运行经验评审；
— 功能分析与功能分配；
— 任务分析；
— 对人的配备、组织和资质的分析；
— 对由人来完成的重要任务的处理。

4.12. 人因界面设计中需要考虑的重要输入包括：

— 由整个仪器仪表和控制系统强加的限制（例如，由于传感器数据的可用性而对可以呈现信息的限制）；
— 在所部署的人因界面中的切身操作环境；
— 用户的认知局限性和认知优势；

— 人的知识、技能和能力，包括来自不同职业群体的人；
— 相应的监管要求。

4.13. 人因界面设计应对电厂运行人员的职责起到帮助，并应把在功能分析和功能分配流程中确认的自动化程度考虑进去。

4.14. 任务分析的结果应为人因界面设计提供以下输入：

— 在从正常运行到事故工况的一系列电厂状态中，控制电厂所必需的任务；
— 仪器仪表和控制的详细技术要求（例如，显示范围、精确度、准确度和测量单位的要求）；
— 与支持任务方面相关的要求，包括可居留性（例如照明和通风要求）。

4.15. 人的配置和资质分析的结果应为人因界面设计提供输入，以便决定控制室的总体布置，并将控制和显示器分配给各个控制台、面板和工作站。

4.16. 应对在人因工程设计中实施人因工程的特定导则提供证明文件，并将该导则用于对人因界面的特性、布置和部署人因界面环境的设计中。

4.17. 本“安全导则”应规定人因界面环境的详细设计标准。如果现有电厂的人因界面进行了更新改造，应按照人因接口的技术更新和运行理念两方面对导则进行评价以便进行必要的修订。

4.18. 本“安全导则”的形成源自人因界面设计相关的通用人因工程导则及分析。它应是对各种特定人因界面设计所采用设计结论的特定反映。

人因界面的详细设计及与电厂总体设计的融合

4.19. 为了察觉电厂状态的改变、诊断的状况、所采取的措施，并核实对手动或自动的动作，人因界面应向运行人员提供必要的信息。

4.20. 人因界面的设计应支持人在各种环境条件下的工作执行情况，如丧失照明、烟雾、高放射性水平、水淹、蒸汽进入和有限的通风。

4.21. 人因界面的所有特性（包括控制、显示布置和编码技术）都应符合运行人员使用的心智模式和既定惯例。

4.22. 以运行人员掌握电厂状态最有效的方式，和控制电厂必要行动来显示信息。

4.23. 人因界面的操作和外观在不同的信息显示和仪器仪表和控制位置上都应是一致的。

4.24. 设计的人因界面应尽最大可能来防止并发现运行人员的失误，特别是在错误的事件背景或按照不正确的电厂配置情况下而可能采取的行动。这包括对确保控制系统、监控系统和保护系统的整定值变更生效的设计。

4.25. 人因界面的设计应为运行人员提供足够的信息，以便在出现错误信息的情况下支持其做出决策。

4.26. 信息流程图和控制操作应尽可能弥补运行人员对信息的处理能力及执行。

4.27. 人因界面的设计：

— 应尽可能考虑到与电厂进行相互影响的各类运行人员的不同作用与职责；
— 设计时应首先关注负责设备安全运行的运行人员作用；
— 应在控制室的部分人员中共同形成对电厂的状况意识（例如，通过大型壁挂式状态显示器）；
— 应提供有效的电厂状态概览；
— 应尽可能从用户的角度采用符合功能和任务要求的最简单的设计；
— 应提供便于运行人员能够快速识别和理解的信息（例如，考虑关于人对信息处理和视觉注意的知识）；
— 在控制动作没有受到明显干扰的情况下，应考虑到模拟和数字显示的故障；
— 应考虑到人的认知、生理特点、人的运动神经控制的特点和人的体型。

4.28. 人因界面应对可察觉的运行人员错误提供简单、易懂的通知，并应给出简单、有效的恢复方法。

4.29. 应对人因界面程序和培训计划进行构思与比较，以确保其相互的一致性。

4.30. 对所有描述性的确认书与标签使用同一语言和兼容的书写字母。

4.31. 在与电厂其他控制行动不产生冲突的情况下，人因界面设计应允许对人因界面的视察、维护、试验和维修。

4.32. 人因界面设计应支持人员在最低限、特殊和最佳人的配备条件下来执行任务。

4.33. 如果要对人因界面进行修改，则修改后的人因界面和新的人因界面皆应设计成：

— 与现有人因界面使用的设计导则保持一致，使人员在新旧设备之间具有类似的界面；
— 尽可能与用户现有的收集与处理信息的方法，以及在任务分析中确认的执行动作保持一致。

4.34. 如果修改了人因界面，任何减少的显示信息都应得到设计工程师、人因工程师和运行人员的证明理由、评审和同意。

4.35. 就地控制设备的人因界面设计应与控制室的人因界面设计一致。

4.36. 安全系统监督控制所需的人因界面设计应采用纵深防御概念。

4.37. 应就人因界面如何进行控制、显示和警报给出说明，以确保所确认的由人完成的重要任务能正确并可靠地执行。

4.38. 人因界面的设计应把必要的补救措施和支持性程序考虑进去，以确保工作人员对任何仪器仪表和控制功能及人因界面的退化工况进行有效控制，并为向备用系统过渡做好准备。

人因界面的试验与评价

4.39. 在形成人因界面的过程中，应对概念设计和详细设计的特性进行可用性试验。

4.40. 对比不同的设计选择要经过“权衡”评价，它是以人能够顺利执行任务，以及其他设计上的考虑为基础的。这样的权衡性评价应考虑到：

— 由人来完成的任务要求；
— 人的执行能力和局限性；
— 人因界面的性能要求；
— 视察和试验需要；
— 维护需求；
— 使用先前设计的经过证实的技术和运行经验。

4.41. 为了对设计选择和设计可接受性进行评定，可用性和性能试验要求对人因界面的性能进行评价，包括用户意见。

人因界面的操控设备设计

4.42. 如果一个操控设备可以从多个位置进行读取，例如从控制室、应急控制室或位于电厂内的设备，则应采取保护措施，以确保多个运行人员之间的协调使用。

4.43. 对于多路复用控制设备或专用控制设备，或对于上述设备的组合，人因界面操控设备可当作“软”控制来执行（见第 4.50－4.61 段）。

4.44. 模拟控制设备（例如按钮、旋转开关、滑块、拨动开关和摇杆开关）适合于经常使用的控制（例如电力输出）和其即时可访问性和可靠性至关重要的控制（例如应急停堆按钮）。

4.45. 操控设备在满足要求的时间内，为表明系统已经接收到某一控制输入，应给出视觉和/或听觉上的反馈。

4.46. 通过使用控制设备所附带的反馈，向运行人员表明数据输入的过程（如对整定限值的调整），并告知数据输入已经完成。

4.47. 对可能产生负面后果的执行动作，需要利用慎重的行动措施（如确认按钮和开关罩上塑料盖），人因界面应确保将意外触发的可能性降到最低。

4.48. 为了防止模拟操控设备的错误动作，措施应包括：

— 把操控设备设置在正确的位置上；
— 使用保护性的结构；
— 请求再次确认动作；
— 使用具有相应优先顺序分配的联锁或许可信号；
— 选择适合切身感受特征的设备，如尺寸、进行操作时的按压或用力，以及对触觉、视觉和/或听觉的反馈。

4.49. 为了最大限度地减少运行人员的失误，操控设备的机构应该符合常规操作（例如，其应该符合使用者的预料），并且应该与受控变量的特性相兼容。

对软操控设备的设计考虑

4.50. 使用与指示设备（如鼠标、轨迹球、光笔或触摸功能）连在一起的视频显示设备，或者带有一套用于操控设备的视频显示的组合设备，为软操控设备提供手段。

4.51. 对运行人员执行工作的重要信息显示，使用的软操控设备应包括对受控部件进行选择的方式，以及输入数据的显示区域和所用的输入格式。

4.52. 应使用软操控设备进行交互，如挑选电厂的某个可变量或受操控的部件，提供控制输入并对系统的响应进行监控。

4.53. 软操控设备应提供以下显示设备：

— 必要时，允许对单独部件件进行读取；
— 允许读取每个部件的相关状态信息；
— 控制与其他部件的关联。

4.54. “挑选重点的显示屏”显示的是一整套受操控的部件或变量。在重要事项显示屏中的部件和变量，为了有助于做出正确的选择，应是在视觉上清晰可见，布置简明并进行单独地用标签进行标识。

4.55. 软操控设备的设计应使运行人员能够一目了然地通过上下文、视觉上不同的格式、分隔、输入字段和可选部件等特性来区分选项。

4.56. 软操控设备通常使用的输入格式是分开的控件接口、软滑块和箭头按钮。输入数据的输入格式应在软操控设备中提供。

4.57. 光标应具有独特的外观，其移动应具有与所需任务和运行人员技能相适合的敏感程度。光标移动应符合运行人员的触觉、视觉和舒适性的相关特性，允许快速移动和准确放置。

4.58. 人因界面内操控导航的动作应与操控电厂的动作区分开来，例如在计算机屏幕上对泵进行的停止或开启。

4.59. 任何特定动作的操控指令应只向运行人员提供可供选择的选项和控制。这些选项应在工作显示器的补充菜单中列出，而无需运行人员记住他们或对单独的菜单显示进行读取。

4.60. 软操控设备菜单的设计应保持一致，其选项列表在整个人因界面中的表达风格也应保持一致。

4.61. 为了避免在执行命令时出错，操控的顺序应该包括对操控的选择、指令的选择和指令的核对。

在对工作站设计中的人因工程实施

4.62. 工作站的设计应把与运行人员的触觉、视觉和舒适性相关的特性考虑在内，例如：

— 工作站高度；
— 台面倾斜度、控制台的角度和深度，以及可调节坐立的工作站；
— 控制设备的位置；
— 显示设备的位置；
— 控制台或工作站上控制和显示设备的布置；
— 文本和图形的大小和易读性；
— 腿和脚的空间。

4.63. 控制台的高度应允许运行人员通过其顶部查看（例如，查看共享显示器和其他运行人员）。

4.64. 警报面板的位置应使其可从主控室的运行区域可见，并处于便于运行人员可见和易读的高度。

4.65. 频繁使用的操控设备应在运行人员可触及的范围内，相关指示器和显示器应便于从运行人员的位置读取。

4.66. 功能和流程操作应根据其特点分为不同的功能组。

4.67. 功能组应按功能、使用顺序、使用频率、优先级、操作规程或具有模拟显示 [3] 布置的系统来进行安排。

4.68. 相关的功能性操控设备和显示应与其他功能组的操控设备和显示区分开来。

4.69. 为了防止部分运行人员出现“左－右”混乱，应避免面板、操控设备和指示器的反射成影布置。

4.70. 工作站上的控制设备、显示器和其他设备应适当和清楚地贴上标签，以便于迅速和准确地进行人工操作。

4.71. 应该使用按等级进行标记的计划来减少混淆、检索时间和重复。主标签用于对主系统或工作站的确认，子标签用于对子系统或功能组的确认，部件标签用于对每个工作站元件的确认。

4.72. 标签应对设备物项的功能进行说明，所使用的符号应是唯一的并与其他物项可区分。

4.73. 标签在使用单词、首字母缩写词、缩写词以及系统和设备编号时，应在面板内部和面板之间保持一致，并且在程序中使用的命名法和标签上打印的命名法之间不应发生不匹配。

4.74. 工作站的设计应考虑到可能必须在工作站上执行的试验和维护操作。其应包括：

— 为了维修、拆卸或更换，对面板上的部件进行读取；
— 为了试验和维护，把运行使用的这些操控设备和仅用于显示的部分进行区分；
— 针对专用试验设备或进行维修的应急空间。

[3] “mimic display”模拟显示是在显示面板上，对电厂实物布置进行模拟的一种布置。

人因工程在可达性和工作环境设计中的应用

4.75. SSR-2/1（Rev.1）[1]第 5.60 段指出：

> “设计应确保在影响电厂运行的事件后，在控制室或应急控制室，以及在通往应急控制室的路线上的环境条件，不会危害到对运行人员的防护和安全。”

4.76. SSR-2/1（Rev.1）[1]第 5.61 段指出：“运行人员的工作场所和工作环境的设计应符合人体工学概念。”

4.77. 在需要运行人员监控和控制电厂系统的区域，应作出必要的规定，以确保适宜的工作环境和工作条件，并防止危害情况。

4.78. 工作环境应考虑的方面包括照明、温度、湿度、噪声和振动。

4.79. 应考虑的危害包括放射性、烟雾和大气中的有毒物质。

4.80. 确保出入适宜的一种方法是给出限定路线，来防止在应急控制地点和其他现场位置，对采取规定行动时的运行人员可能造成的内外部危害。

主控室

4.81. SSR-2/1（Rev.1）[1]要求 65 规定：

> **“核电厂应设有控制室，不论是自动还是手动状态，在所有运行状态下均可安全运行，并在发生预计运行事件和事故工况后，可采取措施使核电厂保持在安全状态或恢复到安全状态。”**

4.82. SSR-2/1（Rev.1）[1]第 5.57 段指出：

> “应向运行人员提供必要的信息：
>
> (a) 评价电厂在任何情况下的总体状况；
> (b) 在与电厂系统和设备相关的特定参数（运行限值和条件）限值内运行电厂；

(c) 确认启动安全系统的安全动作在需要时可自动触发，相关系统按预期运行；

(d) 确定手动启动特定安全措施的必要性和时间。”

4.83. SSR-2/1（Rev.1）[1]第 6.39 段指出：

“应采取适当措施，包括在核电厂控制室与外部环境之间设置隔离墙，并应向长期居留在控制室的运行人员提供足够的保护信息，使其免受事故工况造成的高放射性水平、放射性物质的排放、火灾或爆炸性气体或有毒气体等危害。”

主控室的人因界面设计

4.84. 主控室的设计应符合运行概念，该概念体现了电厂在所有电厂状态下的运行方式。

4.85. 主控室人因界面的设计应充分考虑：

— 运行的目的和特定目标，包括安全运行；
— 将人因界面变成工作站的系统（例如控制台和面板）；
— 主控室的工作站布置及配套设备。

4.86. 显示器的人因界面应使运行人员能够：

— 认识反应堆保护系统和其他自动系统正在采取的行动；
— 分析扰动的原因，跟踪扰动的发展过程；
— 执行必要的手动应对操作。

4.87. 主控室的设计应考虑显示选项，这些选项应提供电厂状态的高级摘要，并支持运行人员在执行共享任务时的合作以及对彼此活动的了解。

4.88. 主控室内应设置显示设备，以便运行人员和监督人员能够监控所有安全功能，包括电厂的状态、安全状态和电厂关键参数的趋势。

4.89. 每个特定任务的人因界面元素和代码（例如颜色、形状、线条、标签、首字母缩略字和缩写）在最低环境照明条件下，在最大限度的观看距离内，应是可确认且字迹清晰可见。

4.90. 显示系统应传达给运行人员想要的信息，而不是含糊或没有意义的信息，并且都没有不必要的时间耽搁或等待。

4.91. 显示功能应允许运行人员快速评定单独的人因界面元件的状态及其与其他人因界面元件的关系。

4.92. 数值应仅显示运行需要的重要数据级别，即使有更精确的个别输入数据可用。

4.93. 显示系统的响应时间应符合运行要求。

4.94. 当要求多名运行人员同时与系统交互时，一名运行人员的控制输入项不应干扰优先级更高的其他控制输入项。

4.95. 人因界面设计应考虑到运行人员要采取的共同或协调行动。

4.96. 来自人因界面的信息应允许运行人员立即评定整个电厂状态，并检测需要注意的条件，而不需要执行额外的复杂任务。

4.97. 在任何运行工况下，视频显示单元上显示的信息都应清晰易懂。

4.98. 显示系统中使用的符号应该标准化。

4.99. 应向运行人员提供指示系统正常运行（或发生了系统故障）的显示功能。

4.100. 当显示系统的过载或其他系统条件可能导致处理延迟时，系统应识别数据输入，并应向运行人员提供延迟和处理完成的指示。

4.101. 对于需要运行人员快速响应的实时任务，人因界面应该只需要运行人员的有限操作。例如，应限制光标在显示页之间的移动距离、扫描时间和显示器上的窗口数。

4.102. 视频显示单元系统应提供用户协助。必要时，这种协助应包括咨询信息、错误消息、确认消息和验证系统。

4.103. 运行人员应能够索取相关输入命令要求的指导（例如，所需的语法、参数和选项）。

4.104. 视频显示网络系统应对建立在任务要求基础上的明显逻辑做出反应，并且应当易于被运行人员理解。

4.105. 应将各种标准化显示的人因界面功能（例如，数据显示区、控制区和消息区）的显示屏位置安排有序。

4.106. 人因界面显示系统应清楚地指明哪些项目可供选择。当运行人员对选定的显示项执行操作时，应突出显示该选项，以避免错误。

4.107. 人因界面应该是用户友好的，不应要求运行人员在执行操作时记住特殊代码或顺序。

4.108. 大屏幕显示可采用通过访问电厂公共汇集信息或共享信息的手段来提高运行人员的效率。

主控室布置

4.109. 主控室应具备足够的空间以允许主控室工作人员执行所有必要的操作，同时尽量减少运行人员在异常和事故工况下的不必要走动。

4.110. 主控室的人的配置和任务分配，应保证在所有运行模式下的控制、显示和其他必要设备都能充分、迅速地投入。

4.111. 主控室工作站和控制台的布置：

- 应提供所有控制和显示面板（包括警报显示）的全视图；
- 应便于工作站运行人员与主运行区域内的任何地点进行口头上的交流；
- 应允许无需克服障碍进入工作站；
- 应允许有效、畅通无阻的行动和交流。

4.112. 应在主控室内提供一个存放程序文件和其他文件的空间。该存储空间应便于查阅和提取文件。

4.113. 在事故期间，应为控制室工作人员提供可能需要应急设备的存储空间。该存储空间应便于使用。

对可居留性的考虑

4.114. 主控室的环境应该是在没有感到不适、过度压力或身体危害的情况下，让主控室工作人员能够执行它们的任务。

4.115. 在主控室内对工作空间的设计，应考虑能对人的绩效具有重要影响的环境因素，如温度舒适性、包括应急事件在内的满足要求的照明、改善清晰口头交流的听觉环境以及适当的布置。

4.116. 控制室应配置足够的设施和用品，以确保在应对事故期间长期居留的舒适性。

4.117. 控制室的设计应包括对来自控制室外部的飞射物撞击的评定和防护。原子能机构《安全标准丛书》第 NS-G-1.11 号《核电厂设计中除火灾和爆炸外的内部危害防护》[8]提供了关于控制室免受飞射物攻击的指导。

安全参数显示系统的设计

4.118. 应提供安全参数显示系统，以便在事故期间协助主控室工作人员确定核电厂安全状况，并评价是否需要运行人员采取纠正行动，以避免反应堆堆芯性能退化或放射性物质排放。

4.119. 在安全参数显示系统的设计中应采用人因工程技术，以提高主控室工作人员职责的有效性。

4.120. 安全参数显示系统应提供与电厂关键安全功能的信息。

4.121. 安全参数显示系统应放置在主控室工作人员方便查看的位置，并应提供连续的显示信息，以便随时可靠地评定电厂状态。

4.122. 在设计安全参数显示系统时，应汇集一组最少的电厂参数，运行人员无需调阅主控室中显示的所有信息即可评价电厂状态。

4.123. 用于安全参数显示系统的显示设备可以包括模拟设备和计算机辅助设备。模拟显示设备可以包括仪器仪表、指示灯、数字显示器和绘图仪。计算机辅助显示设备可以包括平板设备和大屏幕设备。

4.124. 用于安全参数显示系统的显示设备应符合主控室人因界面的通用设计导则。

4.125. 安全参数显示系统应在显示和编码信息方面与人因界面的其他显示器和设备保持一致与兼容。

应急控制室

4.126. SSR-2/1（Rev.1）[1]要求 66 规定：

> **“仪器仪表和控制设备应始终随时可用，最好是在一处单独的地点（应急控制室），与核电厂主控制室在实体、电气和作用上是相互隔开的。如果主控制室丧失了执行重要安全功能的能力，则应急控制室应同样具有能让反应堆实现停堆并保持在关闭状态、能排出余热，以及能够监控重要电厂参数的能力。”**

4.127. 应急控制室的人因界面设计过程应与主控室的设计过程并行开展，要使用类似的程序、标准和方法。

4.128. 应急控制室的人因界面设计应考虑人因工程原理和运行人员在应急情况下的人类特性，并应特别考虑需要立即采取的行动。

4.129. 应提供确保应急控制室可居留性的手段，包括在应急控制室需要长期占用的情况下（例如，为通风系统配备备用电源和碘过滤器等）。

4.130. 应急控制室工作空间的设计应考虑可能对人的表现产生重要影响的环境因素，如热舒适性、充足的照明（包括应急情况下的照明）、有助于清晰语言交流的听觉环境以及适当的布置。

4.131. 应急控制室中使用的计算机辅助信息或控制，应在功能上与主控制室中的类似控制和显示严格匹配，或最好完全相同。

4.132. 应急控制室显示和控制的人因界面应与主控室相似，以便于运行人员轻松转换；并应根据其功能进行布置，最大限度地减少人为错误的可能性。

4.133. 应建立将指挥、控制和通信从主控室转移到应急控制室的程序。

4.134. 应提供应急控制室与就地控制地点之间，以及与电厂管理层、临界管理的外部团队和技术支持中心之间的通讯手段。

现场的应急响应设施

4.135. 现场应急响应设施 [4] 的设计应采用人因工程。设计应提供个人工作场所的最优布置，以及在执行事故管理策略时采取行动所需的数据和信息。

4.136. 应急设施中支持态势感知的显示器应采用公认的人因工程方法和原则进行设计。要考虑的因素包括照明、尺寸、几何构型、显示和控制布置、内容的可用性、格式的适用性和显示的标准化。应从根本上考虑用显示器提供信息去执行的任务。

4.137. 对包括应急演练在内的运行经验的评审，连同功能分析和任务分析，应作为在缓解严重事故后果的情况下确认事故监控和设备运行与人的表现相关要求的基础。

4.138. 应考虑资源分配策略（如人的配置）、电厂的物质条件（如供电、可达性、以及环境和辐射工况）、天气条件（极热、极寒或降水）等退化因素，以及应急情况下与人的表现相关的技术选择。

4.139. 当要求运行人员运行严重事故管理安全分析中使用的非永久性设备时，应考虑人因工程方面的规定。这包括安全进入就地控制并能够安全使用非永久性设备。就地控制的典型示例包括：就地控制面板、连接点、开关和端子，以便 (i) 能够连接非永久性设备；或 (ii) 能够使用非永久性设备供电来运行设备（例如泵）。

4.140. 应考虑在应急情况下，各级人员和相关方面与场内和场外应急响应组织的内部和外部互动范围。

4.141. 应考虑在应急行动期间可能存在的压力和工作量水平。

4.142. 为支持实施严重事故管理标准，技术支援中心工作人员应接受工具确认和使用的培训。原子能机构《安全标准丛书》第 SSG-54 号《核电厂的事故管理计划》[10]为制定和执行严重事故管理标准提供了更详细的建议。

---

[4] 应急响应设施见原子能机构《安全标准丛书》第 GSR Part 7 号《核或辐射应急的准备与响应》[9]。对于核电厂，应急响应设施（与控制室和辅助控制室分设）包括技术支援中心、运行支援中心和应急中心。

警报管理

4.143. SSR-2/1（Rev.1）[1]第 5.66 段指出：“应提供适当的警报系统和通信手段，以便在核电厂和现场的所有人员在运行状态和事故工况下都能得到警告和指示。”

4.144. 警报器或其他设备指示与正常运行工况的偏差。发生这种情况时，应向运行人员提供必要的信息，以便：

— 对自动系统正在采取的行动进行确认；
— 执行必要的手动应对措施；
— 跟踪电厂的运行状况或响应过程。

4.145. 警报应提供异常工况的相关信息，如：

— 偏离了控制或保护整定值的参数或变化速率；
— 设备故障、异常或差异；
— 不完整或故障的自动动作。

4.146. 无需运行人员执行任何操作的情况不应导致警报。对并非表明异常，而是从某个系统要求响应的消息中得到的计划情况数据，作为状态信息，也应包括在内。

4.147. 对所有警报都应提供证明文件，并在配置控制的范围内。

4.148. 警报系统应具有足够的覆盖范围，以便能够在运行状态和事故工况下生成警报。

4.149. SSR-2/2（Rev.1）[2]第 7.9 段指出，对于经过分析的电厂运行状态、停堆或事故工况，应尽量减少警报数量以防止不必要或无意义的警报可能导致警报过多。

警报产生

4.150. 警报系统应能够从以下来源产生警报：

— 数字信号；
— 模拟信号；
— 直接输入或从其他系统得到的计算、合成或分组信号。

4.151. 基于模拟和数字信号的警报应该是可配置的。警报状态可以在信号的不同状态中选择（例如，ON/OFF，OPEN/COLSED 和 TRIPPED/UNTRIPPED）。

4.152. 生成的警报应支持与电厂中的结构、系统和部件的分类系统相一致的警报层级。

4.153. 警报应知道产生警报的前后关系（例如，泵低流量警报应在实际低流量条件下生成，而不是在泵启动期间生成）。

警报验证

4.154. 应对用于产生警报的传感器和输入信号进行生效验证，防止产生不必要的瞬时或无休止警报。

4.155. 警报系统应能在任何时候自动减少警报的数量。

4.156. 通常在对相关设备的试验、维护或维修期间，禁止警报通过消除警报生成能力，让闲置的警报停止工作。警报系统应支持禁止警报的功能，以避免发生警报滋扰或变成长时间的警报。

4.157. 应采用人因工程分析和验证来确定是否存在某一个警报掩盖另一个警报或其他警报的情形发生。

4.158. 警报系统应支持对警报进行优先排序，以确定警报的相对重要性。

警报处理

4.159. 警报系统应支持生成用户定义的警报。运行人员应能够为模拟变量选择一个高警报限值或一个低警报限值，或在离散变量可能的警报状态中选择一个状态。

4.160. 警报系统应能够以事件为起点来使用警报，以及以重要性为起点，在以下不同警报等级水平上，来实施对警报解除的技巧：

— 以事件为起点对警报进行简化的技巧，对支持系统或设备物项故障的结果，或由于电厂事件的结果而产生的警报进行过滤或解除；
— 以重要性为起点对警报进行简化的技巧，在警报过载的状态下，对较低级别的警报进行解除。

4.161. 无论是自动还是由运行人员启动的，应使用对警报的过滤或解除，来避免运行人员负担过重，但不应解除必要的信息。

警报的预报信号与控制

4.162. 当出现警报工况或准许警报时，警报系统应提供视觉指示。视觉指示可包括：

— 闪烁，在出现警报工况或准许警报时触发，识别或复位后终止。当一个新的子警报在另一个子警报已经触发并被识别之后出现时，分组警报应该闪烁。
— 颜色编码：根据警报优先级和警报状态，警报可以点亮不同的颜色。也可以使用其他显示编码方法。

4.163. 当出现任何警报工况或准许警报时，警报系统应提供听觉上的指示。

4.164. 应提供使音频信号静音的手段以避免听觉过量，并便于识别随后可能出现的新警报。

4.165. 应提供允许运行人员单独或成组地及时收到警报的方式。

警报显示

4.166. “暗屏”标准是指在不影响电厂安全工况下，最大限度地减少正常运行期间出现的警报数量。

4.167. 在满功率和正常运行的其他工况下，警报处理应遵循暗屏标准。

4.168. 警报显示应基于以下不同类型的显示：

— 专用地点、连续可视的显示设备（例如，使用了连续可视类似墙体嵌板的显示设备或装饰，或集成了警报功能的连续可视的模拟显示器）；
— 警报信息的排列显示（例如，在可视显示单元屏幕上展示的文本消息）；
— 集成到图形显示器中的警报（例如，模拟显示器或软控制显示器）；
— 单独的警报信息显示；
— 混合显示（即其他类型显示的组合）。

4.169. 相关警报状态变化和新警报的信息应单独显示和管理。

4.170. 警报信息应简单、明确和标准化。

4.171. 警报消息应包含运行人员有效响应警报所需的所有信息，如警报来源、优先等级、描述、设定值和参数值，以及对警报响应过程和相关显示的索引。

4.172. 运行人员应该能够根据需要对警报消息进行排序。警报系统可按如下分类原则，对警报清单进行组织：

— 按时间先后排列的顺序；
— 优先级；
— 警报状态；
— 警报信息；
— 其他的逻辑顺序。

4.173. 特别是当警报对相关系统、功能、设备或部件之间关系有帮助时，警报应融入到图形显示中。

4.174. 应使用单独的警报信息显示来提供与警报相关的专门信息，如：

— 警报衍生的变量趋势；
— 统计数字，例如平均多久发生一次警报；
— 与其他警报或变量的关系；
— 与警报相关的当前或历史的工单或报告数量。

警报响应程序

4.175. SSR-2/2（Rev.1）[2]第 7.9 段指出：针对控制室中的所有警报，需要运行人员使用程序，对经核实的警报响应进行管理。

4.176. 警报响应程序应向运行人员提供以下信息：

— 警报所属的系统或功能组；
— 与警报相关的准确信息；
— 警报的响应排序；
— 自动动作，以及快速行动和其他运行人员的行动；
— 可能造成警报或造成警报原因的清单；
— 参考文献。

程序的形成

4.177. 本部分就程序形成中的人为因素内容给出建议，并应结合原子能机构《安全标准丛书》第 NS-G-2.2 号《核电厂运行限值和条件及运行程序》[11]和 SSG-54[10]提出的建议来阅读。

4.178. 通过安全分析确认的由人来完成的重要任务应在程序中得到阐述。

4.179. 对经安全分析确认的由人来完成的重要任务进行整体说明的程序，应进行定期的生效批准，以核实：

— 对顺利完成每个程序所需设备的可用性及其状态；
— 就相关由人来执行的安全相关任务，在安全分析中作出任何假设或要求的有效性。

4.180. 为确保程序能按规定执行，且执行结果或输出满足要求，应对程序生效进行批准。

4.181. 针对以下目的，形成的程序还应把任务分析的结果考虑进去。

— 有必要在程序中对突出强调的可能失误进行确认；
— 对顺利完成任务所需的信息流、行动和反馈进行说明；
— 对任务与人员之间的关系进行确认；

— 就程序中各项行动的时间安排给出初始信息；
— 方便程序间的过渡；
— 确定对终止程序的格式与内容，包括提前的技术通知、先决条件（始发条件）和要求。

4.182. 程序中要求所确认行动（或一系列行动）的结果应是明确的、可理解的和可核实的。

4.183. 在人因工程实施于电厂程序的形成中，应把程序类别相关的格式和内容（如应急运行程序、维护程序和试验程序）考虑进去。

4.184. 对安全临界任务、复杂任务和极少执行的任务的程序，应以详细、逐步地方式开始。

4.185. 如果规定的操作无法执行，则应向每个程序提供安全替代操作的指导，或者提供安全终止程序的指导。

培训计划的形成

4.186. 在确定所设计系统的培训要求时，任务分析应给出一个标准（如对知识、技能和能力的确认要求）。

4.187. 就显示内容与想要表示的电厂状态间关系，应对运行人员进行培训，包括故障模式及其影响，以及在显示设备上的现象。

4.188. 对在显示设备内和相互间的导航，屏幕上的操作特征（如 Windows），以及在人因界面中使用的其他功能，对运行人员进行培训。

4.189. 应根据设计的进步，定期对培训计划进行评审与修改。

4.190. 培训应及时进行，与电厂改造相关的培训应在改造实施前完成。

4.191. 培训计划的制订应遵循原子能机构《安全标准丛书》第 NS-G-2.8 号《核电厂人员的招聘、资格和培训》[12]提供的指导。

5. 对人因的核实和验证

概述

5.1. 对人因界面系统中的人为因素的核实和验证，是对人因界面系统是否整体上符合特定的人因工程设计要求的决定因素，并且为了确保电厂安全运行，也是对人员是否能顺利并安全地履行其预期作用的决定因素。

5.2. 核实和验证的实施应贯穿于人因工程设计过程，它随着项目进展是以变得越来越逼近真实情况的模式和模拟为基础的。

5.3. 核实和验证应该提供客观的证据，证明设计者正确地遵守了设计原则和可用性要求，包括人员、技术和组织方面，以及它们之间的相互影响。

5.4. 核实活动通常包括：

- 确认人因工程标准和导则；
- 人因界面的核实，包括硬件（如控制台、面板和模拟接口，包括警报显示）和软件，以及相关文档（如程序、说明和警报表）；
- 评审设计要求、图纸和手册；
- 任务支持手段的核实，包括提供工具、工作辅助工具、个人防护设备、与任务相关的设备和培训、运行人员的资格以及在需要时提供无障碍和可用的程序。

5.5. 核实活动可能需要与系统用户的互动。

5.6. 核实和验证活动必须由原先从事设计工作的个人或团体以外的个人或团体进行[1]。

5.7. 特别是为了评价应进行的核实：

- 控制室人员在运行状态和事故工况下完成所需行动的能力；
- 对支持任务执行的程序描述和编写；
- 人因界面对运行人员的职责支持能力；
- 工作空间布置是否适合对任务和系统性能起到帮助的作用；
- 临界管理以及事故管理团队成员之间的资源协调，包括外部组织。

5.8. 控制室设计在人因方面的验证应包括：

— 支持运行人员任务的主控制室和应急控制室的布置；
— 对监控、控制和维护（控制室内外）的系统有效性；
— 与整个电厂相连的控制室中的监控系统，在运行状态和事故工况下的使用工况。

5.9. 包括硬件、软件、程序和人员在内的集成系统的验证应在设计定稿之前进行，以便有足够的时间在电厂投入运行之前对设计进行更改。

5.10. 对核实和验证的输入信息，应来源于已经实施的人因工程流程，特别是：

— 所有运行状态和事故工况下的运行观念；
— 尤其是与安全临界任务相关的技术要求和用户要求；
— 控制方式和自动化等级的作用和详细技术规格；
— 功能分析的输入；
— 监管要求；
— 运行经验评审的输入信息；
— 由人完成的重要任务；
— 安全分析数据；
— 人员可靠性分析的数据；
— 人的配备、组织和资格分析的数据；
— 以往人因工程评审和分析的数据；
— 模拟输入（如部分任务模拟）。

核实和验证的计划制定

5.11. 在人因核实和验证计划中，应对核实和验证提供证明文件。该计划应具有独立性的地位并对资源、评价方法，以及适用的标准和监管进行安排。

5.12. 核实和验证的计划制定是一项迭代性活动，以便根据设计的进展来对项目的变更进行支持，例如：

— 当有更多的接口可用时；
— 随着程序变得更加详细；
— 当运行人员经过了培训；
— 随着模拟变得更加逼真。

5.13. 核实和验证计划应特定规定：

— 评定的范围；
— 必要的数据收集和分析；
— 有效性措施；
— 评定和验收标准；
— 在评定中需要的参与者；
— 评定小组的必要培训，包括作为用户代表参加的培训；
— 试验环境；
— 日程表。

5.14. 此外，核实和验证计划还应具体规定：

— 假想方案的选择；
— 评定小组使用的材料 [5] 和工具。

5.15. 核实和验证计划也应对人因界面设计承诺的目标和要求的结果进行说明，来证明：

— 使用了计划规定的人因工程要求（如人类工效学要求和计划特定要求）；
— 使用了电厂的运行验收标准；
— 使用了对运行人员响应的监管要求。

[5] “材料”包括录音、录像、计算机录音和调查表。

5.16. 核实和验证计划还应描述以下流程：

— 任何人因工程相关问题的分析和评价；
— 人因工程相关问题的跟踪情况；
— 解决设计缺陷的方法。

5.17. 验证应由具备多种专业知识的多学科验证小组（例如，电厂运行专家、教员、事故和偶然事件工况下的运行专家和人因工程专家）来进行界定与安排。

5.18. 进行验证试验的参与者应按照电厂后续运行的组织机构进行组织。

5.19. 验证试验的参与者应该是电厂今后使用人因界面的人员代表（例如，有执照的运行人员，而不是培训或工程人员）。

5.20. 验证小组应接受数据收集技术方面的培训。

试验方法

5.21. 正常工况下，对人因的核实和验证应包括以下全部或其中的一个部分；

— 静态试验（例如，核实系统是否符合设计规范）；
— 动态试验（例如，试验系统响应的时间和准确性）；
— 假想方案试验和部分任务模拟或全范围模拟（例如，试验运行人员在时间和准确性方面的反应）；
— 监控；
— 独立报告（例如问卷和组织访谈）；
— 核对表（例如在静态或动态试验中）；
— 任务演练。

5.22. 试验人员在进行试验前应熟悉相关系统。

5.23. 核实和验证试验中使用的试验台、模式和模拟器的相似性和代表性范围，应得到合理证明。

绩效指标

5.24. 对人为因素的核实和验证，应适用于实际工作环境的相关人的绩效指标。这些指标可包括：

— 要执行的任务的复杂性；
— 工作量（个人和团队）；
— 相关设计所要求的知识、技能和能力；
— 排序和响应时间；
— 对工作觉悟的要求（个人和团队）；
— 使用程序的要求；
— 对不利状态进行察觉并响应的要求；
— 用户之间以及与其他团队之间的协作和沟通的要求。

5.25. 可能与人的绩效相关的定性和定量指标可包括：

— 时间；
— 准确性；
— 沟通次数和内容；
— 发现失误和失误补救率；
— 与工作觉悟相关的特征（如线索确认、理解和预测）；
— 集体决策方法的运用；
— 注视时间和思索时间（例如，用眼睛跟踪）；
— 疲劳；
— 任务执行的成功概率。

核实标准

5.26. 用于核实的标准应包括设计中使用的人因工程标准和导则。用于核实的人因工程标准和标准的选择，取决于评定范围所包含的人因界面部件的特性。

5.27. 对于已经满足人因工程任务分析中核实的任务（例如，与时间限制、顺序和精度相关的要求），为了对该任务的要求进行确认，还应对人因界面的设计进行确认。

验证试验

5.28. 为了对人为因素的相关设计进行验证，所选择的试验计划应尽可能切合实际，包括：

- 模拟和试验台应符合电厂的设计和实体布置。
- 试验计划应是典型反映了电厂所有状态中的运行工况，并应包括事件（如故障）及其初始条件。
- 运行任务应是电厂常用的这些典型任务（例如，监控、检测、诊断、预计的参数变化、监视、自动控制系统的控制与手动恢复）。
- 参与试验者应接受培训，并应在试验计划中担任与其资质等级和责任相对应的职位。
- 所采用的程序应与相关运行工况中使用的程序相匹配。
- 在计划试验期间，要求人的互动范围。

5.29. 试验情况的可信性及其代表性应当被证明是正当的。

数据收集

5.30. 收集数据的方式应记录在人因核实和验证计划中。该计划应规定试验的持续时间或试验的试验次数、要试验的系统和子系统，以及要从中收集数据对象的数目。

5.31. 为了评价，应在对模式、部分任务模拟器和全范围模拟器进行试验的过程中收集数据，例如：

- 通过试验参与者采取的行动（例如，在每次试验期间由监控者手工收集数据）；
- 控制室内的试验参与者之间的沟通，以及控制室与参与电厂运行的其他团队和临界管理部门的之间的沟通。

5.32. 就相关由设计预先考虑到的缺陷（即由试验参与者察觉到的困难和错误），以及工具易用性的数据都应进行收集。因此，出于安全的目的，应利用验证试验，来对运行人员的行动起到支持作用的资源，以及对这些资源所必须的改进进行确认，例如：

— 促进对核电厂的监视，并强化状况意识；
— 优化人的工作量；
— 鼓励人员之间的合作与交流。

5.33. 在验证试验中收集数据的方法，应能进行客观测量（例如，测量采取行动所花费的时间）和主观测量（例如，人员对工作量的感受使用主观调查表进行测量）。

5.34. 收集的数据应考虑到对每个试验情况的全面分析及涵盖范围，例如：

— 所采取行动的时间顺序；
— 对一贯执行良好和没有问题的任务确认；
— 在计划执行中对异常工况的确认和分析（例如人员遇到的任何困难、对如何开始的犹豫，以及控制室团队成员间对系统或设备状态的误解）。

5.35. 试验期间和之后收集的数据应可用于分析。

数据分析

5.36. 验证试验的分析应包括对所收集数据的全面检查。分析应涵盖两部分，试验参与者所犯的错误，以及顺利完成由人来执行的活动。此外，在所有试验的运行状况中，分析应强调：

— 试验参与者顺利使用并满足其需要的系统；
— 难以使用的系统；
— 试验结果所包含的安全意义；
— 改进设计的建议（由分析人员和用户提出）。

5.37. 收集数据的分析应对人员可利用的系统效率，以及组织准备上的效率进行证明，并应证明在没有过多工作量的情况下，试验参与者能够：

— 对状况的理解；
— 在考虑相应的要求时，采取的必要行动；
— 在控制室内相互合作，并与控制室工作人员必须互动的人（如维护人员、自动控制系统人员和临界管理小组）合作。

5.38. 应对试验活动中产生的人因工程相关问题提供系统性的证明文件，并进行跟踪。

5.39. 应对用来缓解人因工程相关问题的解决计划，以及这些解决计划的有效性提供证明文件，并进行评价和监控。

5.40. 应对每个试验活动中收集的数据及其分析提供证明文件。

结果

5.41. 应对每次核实和验证试验活动的结果提供证明文件。

5.42. 应就所进行的核实和验证形成报告，对试验计划、试验结果、改进建议和结论进行总结。

5.43. 应对人因工程的标准和安全目标之间的任何差距进行调查，并加以解决和提供证明文件。

5.44. 在核实和验证试验中无法解决的，且在电厂投入运行后必须在现场进行验证的任何事项，都应予以具体说明。

6. 人因工程的设计实施

6.1. 对人因设计实施是由人因设计流程的形成、部署及其结果评价构成的。

6.2. 设计实施应正式作为建造和调试计划、许可证审批计划或电厂改造流程的一个部分。

6.3. 人因工程设计实施应对竣工设计是否遵守了已核实和验证的设计要求进行评价，并对设计在电厂和工作环境的实际实施中，是否出现任何不可预见的问题进行评价。

6.4. 人因工程设计实施应证明如下内容：

— 实施的设计流程，要与其技术规范在标准、设计功能和安全性能的相一致；
— 实施的设计没有对相关的人员、管理系统或结构、系统或部件（例如与现有系统或接口不一致）产生任何的问题或冲突（例如，安全、可运行性或文化方面）。

6.5. 人因工程设计实施的范围应把设计对以下内容造成的影响考虑进去：

— 组织因素；
— 人因；
— 工作岗位设计；
— 安全分析；
— 概率安全评定与人的可靠性分析
— 人因界面；
— 设备；
— 程序；
— 培训；
— 电厂参考文件；
— 工作环境。

6.6. 在人因工程设计实施阶段，应适当考虑以下方面内容：

— 为缓解人因工程设计实施的任何不良后果，对竣工设计的结果考虑到的可能需要采取的行动进行的评定。
— 在开始实施之前就需要准备好的基本工作（例如，对实施团队就模拟器或试验台的使用进行的必要培训，以确保它们达到所要求的任务执行水平）。

— 对顺利实施的标准进行规定。这可与人的绩效监控系统相连，以确保检测并衡量到准确的人的绩效。
— 在人因工程设计实施阶段，就要对人因工程相关问题进行关注、评定和解决的方法予以确认。
— 万一发生人因工程设计实施未能达到其性能目标时，要有可行的应急策略。

6.7. 应对人因工程设计实施的结果提供证明文件，并应对以下事项的证据进行汇总：

— 设计计划的结果，包括对准备工作的支持（如人因界面、程序和培训），以及在计划开始时所规定要满足的相关标准、性能和成功标准；
— 在人、技术和组织上任何可容忍或可进行适当改善的任何负面影响；
— 反映在电厂图纸和材料中的对竣工设计进行的任何变更（如培训材料、程序、图纸、模拟器、组织机构和辅助设备）；
— 在人因工程设计实施进行适当处理之前，所有人因工程的相关问题都必须得到确认；
— 已经对人因工程相关的任何新的问题进行了记录与评定，并已确定了配套的解决计划；
— 任何遗留的不符合项已经过评定，且被认为在安全理由上是可接受的。

7. 人的绩效的监控

7.1. 为了对设计的持续有效性进行评价，在对人的安全并有效地执行其工作任务的适当支持中，对人的绩效的监控应是一个能动和持续的过程。对人的绩效监控有助于深入了解：

— 人因界面设计是否符合（并将一直符合）初始的安全性、可运行性和性能假设；
— 运行人员能否有效利用人因界面设计，在主控室、应急控制室、就地控制站和应急设施中完成其任务；

— 对人因界面的设计、程序和培训做出的变更，是否对运行人员执行其工作任务产生了不利影响；
— 是否能根据响应时间标准和绩效标准来实现由人来完成的任务；
— 在系统生效阶段确定的绩效水平，是否在电厂的整个寿期内保持不变；
— 对准备工作的支持，例如监督、培训、人员编制、程序、个人防护装备、工具及工作辅助工具，是否对人员执行其任务中起到了相应且足够的帮助作用。

7.2. 人的绩效监控应考虑以下几点：

— 负责人的绩效监控的个人，及其监控结果的使用者，都应经过充分的培训。
— 负责人的绩效监控的个人应在人与组织、系统计划和根本原因分析方法等领域符合条件与经历要求。
— 应当全面理解人的绩效缺陷的原因与重要性，并对改进绩效的手段予以确认。
— 为了确保系统用户对问题调查报告的有效利用，应建立一种公开且诚实的对问题进行调查的文化。
— 个人和团队绩效受组织内各级人的绩效的影响；因此，对人的绩效的监控应来自对所有层级的数据记录。
— 为了确保在相应时间范围内作出响应，应对退化的人的绩效进行回应，并对予以解决的进展情况进行监控。

7.3. 在电厂所有状态中，为了全面收集电厂在人的绩效方面的回应信息，为此对电厂进行练习与训练提供了一个重要的时机。在切实可行的地方，应面向实际存在的事件状态，最大程度去接近真实情况。

7.4. 对于营运组织内没有对新建计划的设计授权时，在设计阶段对人的绩效所做出的假设，应确保其在调试和运行阶段得到关注并经过验证。

8. 人因工程在计算机程序设计中的实施

概述

8.1. 可以通过将纸面程序转换为数字形式，使用计算机程序，来对运行人员提供在监控与发现、状态评定、响应措施的计划制定与响应实施任务等方面的帮助，以便给出包括不同自动化程度的不同层次的实用性。

8.2. 当对一个现有电厂实施计算机程序时，为了确保正确的设计功能，以及与运行人员的要求与经验保持一致，人因工程计划应对如何实施这些计算机程序进行考虑。

8.3. 计算机程序应包括在电厂的配置管理计划中。

8.4. 计算机程序的设计应考虑对程序的编写、质量保证、评审、核实、验证、控制和更新的切实可行性。

8.5. 计算机程序系统有三种类型：

- I 类系统相当于和纸质程序一样的复印件，且不接受任何的流程处理或实时的信息。
- II 类系统使用动态嵌入的流程数据来对程序进行增加。
- III 类系统提供了 II 类系统的能力，并且还包括了用于操控运行电厂设备的嵌入式软件控制。III 类系统可以包含程序中规定的自动执行动作步骤次序的能力。

计算机程序系统的人因界面

8.6. 对新电厂和现有厂的计算机程序设计中，应实施人因工程。

8.7. 人因工程原则应适用于以下计算机程序：

- 在合理可行的范围内，只显示并执行任务相关的信息；
- 对每个程序持续提供可辨别性的信息（如标题、版本号、日期、电厂名称和机组）；

— 在计算机程序系统中，对保持连贯性的信息显示与位置、导航帮助、控制，以及对每个显示屏的其他应用的菜单；
— 在将使用的系统上，对适应任何设备电子化的程序系统（包括例如其结构、格式、导航菜单和控制）进行布置。

8.8. 为了正确地执行程序，应使用足够数量的显示设备向运行人员提供所有必要的信息。

8.9. 计算机程序的人因界面应支持多个显示设备间的方便导航。

计算机程序系统的互动

8.10. 除特殊说明外，第 8.11－8.20 段文字中的互动功能的建议，适用于 I 类、II 类和 III 类计算机程序。

8.11. 应显示程序步骤中提到的预警和警告，以便：

— 当步骤在显示器上显示时才出现；
— 在步骤中的详细动作执行之前，由运行人员进行读取；
— 每个警告或预警都以一种容易与其他警告或预告区分开的方式呈现。

8.12. 每组相关的程序条款应以列表格式呈现，该格式应：

— 使运行人员易于处理信息；
— 每组条款与其他组条款都能清晰进行辨别；
— 包括指定列表内容的标题。

8.13. 应说明程序步骤的状态（例如，该步骤是否已完成、正在进行、在必要时是否已检查和授权，或是否已失败）。对于 I 类系统，应提供手动跟踪步骤状态的功能。必要时还应说明其他行动。

8.14. 对于 II 类和 III 类计算机程序，系统应记录并存储整个程序的进度。可能需要同时执行计算机程序系统内的多个程序。

8.15. 在这种情况下应适当分配人力资源，并协调多种程序的执行。例如，当同时执行多个过程时，该程序和该程序中的步骤状态应显示在所有设备上。

8.16. 计算机程序系统应包括导航支持功能，允许运行人员在程序内（步骤之间或同一程序的其他部分）移动，并从一个程序移动到另一个程序（例如通过活动链接）。

8.17. 对于所有类型的计算机程序，运行人员都应能够获得注释、警告和预告。

8.18. 计算机程序系统所使用的数据和逻辑规则应提供给运行人员。

8.19. 计算机程序系统应为运行人员提供一种手段，记录他们对程序执行情况的注释和评论。这些说明应予以保存和存档，以便以后查阅。

8.20. 电子化的程序系统可以建议使用哪种程序，但这一决定应由运行人员负责，运行人员应根据电厂状况作出这一决定。这适用于 II 类和 III 类计算机程序。

计算机程序系统的实用性功能

8.21. 当电厂状态需要进入程序、退出程序或从一个程序转变到另一个程序时，计算机程序系统应通知运行人员。

8.22. 相关参数和设备状况的准确信息应由计算机程序系统自动提供。

8.23. 计算机程序系统提供的信息和运行人员辅助工具应具有易读性，以便运行人员不会收到不适当的信息。

8.24. 计算机程序系统可以自动处理程序中的某些步骤。应向运行人员突出显示自动处理步骤的结果。计算机程序系统应指明那些需要运行人员持续监控的步骤（例如，与时间相关的步骤和与过程相关的步骤）。当达到这些步骤中所要求的条件时，计算机程序系统应向运行人员发出警报。此外，计算机程序系统应指明对参数的监控是已经停止还是仍在进行。

8.25. 计算机程序系统，包括操纵电厂设备的软操控（III 类程序），应向运行人员提供必要的信息，以支持有效使用这些控制。

计算机程序系统的退化和故障

8.26. 应对备用程序（例如纸质程序、备份硬件面板）形成调换的导则，并在适当的时候，把计算机程序的备用程序调换回来。

8.27. 对由于计算机程序系统的退化状态及故障，而必须转变到备用程序的状态应有所认识并给出指示。

8.28. 作为备用程序的纸质程序应可供运行人员使用。

8.29. 计算机程序中的信息结构和格式应与备用程序中的信息结构和格式兼容。

8.30. 当有必要转变到基于纸质的备用程序时，应提供以下信息：

— 目前正在执行的程序；
— 已完成程序步骤，以及尚未完成的部分，包括暂停程序执行中的步骤；
— 当发生备用程序的转变时，对步骤或状态的信息进行监控；
— 在程序暂停的地方，为了继续程序执行，避免对已完成步骤的重复所需的信息。

8.31. 向备用程序的转换导则，应考虑计算机程序系统相关的故障模式，以及在计算机程序系统故障期间，和计算机程序系统恢复之后，应对要求运行人员采取的行动进行明确规定。这些行动应站在运行人员的角度来进行描述。

8.32. 应对向备用程序转变所需的执行时间进行验证，要满足计算机程序的功能要求。

8.33. 计算机程序的培训应包括向纸质程序转变所需的特定步骤。

计算机程序中步骤次序的自动排序

8.34. 计算机程序的最高程度是自动化（即对程序中规定的动作执行自动的步骤顺序）。程序步骤次序的自动化仅适用于 III 类程序。

8.35. 在计算机程序中步骤次序的自动执行，应得到负责电厂安全运行的运行人员的授权与监督。

8.36. 运行人员应能够对手动执行计算机程序的步骤还是触发自动进行选择。

8.37. 运行人员应负责对所使用的程序进行选择。

8.38. 自动的步骤次序应该包含在一份程序中（即每个次序应在一份程序中开始和结束）。

8.39. 应通过计算机程序系统，向运行人员提供关于详细和特定步骤顺序的信息。

8.40. 还应向运行人员提供关于自动步骤次序的进展信息（即已完成、正在执行和将要执行步骤的信息）。

8.41. 应提供自动故障的信息以及故障发生时的次序位置信息。

8.42. 应通过计算机程序系统，向运行人员提供关于在开始执行一系列自动步骤之前必须满足初始条件的信息。

自动步骤次序中的停工待检点

8.43. 一个自动的步骤次序可以包括一个控制点，该控制点是程序中的一个预先规定点，在此处程序执行将暂停，并要求得到运行人员对自动次序状态的认可，以及程序继续执行的授权。

8.44. 应将停工待检点包含在自动的步骤次序中，以便：

— 协助运行人员对自动的进展状态，以及对继续执行程序所做出的任何相关和必要的决定或调整进行辨别；
— 保持运行人员对正在执行的步骤次序中，对电厂设备状态所要求的责任意识；
— 使运行人员能够授权程序的继续执行。

8.45. 计算机程序系统应允许运行人员在开始自动的步骤次序之前，把追加的临时停工待检点加到步骤中。

8.46. 计算机程序系统不允许运行人员删除预先规定好的控制点。

8.47. 程序中定义的控制点应使程序处于稳定状态，在这种状态下，运行人员能够正确评价程序的执行状态，并为程序的继续执行做出必要的决定。

自动步骤次序的暂停

8.48. 当自动步骤次序暂停时，计算机程序系统应允许运行人员安全地从自动执行转变到手动执行，或恢复自动执行。

8.49. 就暂停的信息，如被暂停次序的原因、已经完成了的步骤以及仍有待执行的步骤，应由计算机程序系统来给出。

8.50. 计算机程序系统在不满足完成步骤必要条件的情况下，或由于任何其他原因不能保证安全完成当前步骤的情况下，应能够对自动步骤次序进行自动暂停。

8.51. 计算机程序系统应对任何暂停的自动次序向运行人员进行提醒。

9. 将人因工程融入安全管理流程

安全分析报告的形成与评审

9.1. 安全分析报告中的人因工程章节内容，应对人因工程计划及其在电厂具体设计中的实施内容进行说明。

9.2. 安全分析报告中应涵盖对人因工程要考虑的因素，至少包括：

- 人因工程计划的管理，包括对人因工程在设计过程中的授权与监管；
- 使用的人因分析方法；
- 对考虑了人因工程的人因界面设计所选择的假设；
- 人为因素的核实和验证，包括在设计规划期间及对做出的假设进行的分析期间，对人因工程相关问题的确认与解决；
- 针对整个电厂对已经实施了人因界面的设计进行的说明；
- 针对安全临界任务的人的绩效监控策略说明。

9.3. 为了对可接受的人因工程实践进行核实，应安排进行评审，并将该标准纳入设计和安全分析报告。

9.4. 当安全分析中将手动操作归为自动操作的备用时，应在设计分析中把包括人因工程分析的多样性内容考虑进去。

9.5. 在安全分析报告中，应提供与人因相关电厂改造的证明文件。

9.6. 关于安全分析报告的格式和内容的建议见原子能机构《安全标准丛书》第 SSG-61 号《核电厂安全分析报告的格式和内容》[13]。

电厂改造

9.7. SSR-2/2（Rev.1）[2]第 4.40 段指出："改造必然会对由人完成的任务及执行造成影响应进行系统分析。对于电厂的所有改造应充分考虑人和组织上的因素。"

9.8. 当对由人来完成任务的改变是由于对电厂的改造而引起，为了对这种风险可能产生的影响进行确认，应对人因工程的某些内容进行评审。这种评审对大小规模的改造都适用。

9.9. 对属于安全分析中的程序，只要对这个程序做出变更（如次序、时间和工作量），就应进行人因工程方面的评审。

9.10. 针对电厂改造的人因工程计划应采用分级方法。

9.11. 任何涉及人因工程解决计划的改造，在实施改造前都应被合并到电厂的控制中（如文件、程序、配置、行政控制和培训）。

9.12. 原子能机构《安全标准丛书》第 NS-G-2.3 号《核电厂改造》[14]提出了对核电厂改造的相关控制活动的建议。

定期安全评审

9.13. 本部分就人因工程活动提出建议，以支持原子能机构《安全标准丛书》第 SSG-25 号《核电厂的定期安全评审》[15]提出的建议。

9.14. 定期安全评审应验证对下列情况所作的假设是否还继续有效：

— 对于每种运行模式或电厂状态，最可行的资源集约状态；
— 通过功能分配、任务分析及工作量分析，以资源最集约的状态，来对工作的分工与协调的可行性进行评定。

9.15. 针对满意的人的绩效结果是否恰当，以及对最集约的资源状态是否充分，定期安全评审应对人的配备、组织、系统设计、培训、程序、工具、设备和其他必要资源进行考虑。

9.16. 定期安全评审应考虑是否使用了第 5 部分所规定的、对人因工程核实和验证活动的假设和要求，来对安全分析中验证的由人来完成的任务进行确认，让这个假设和要求持续有效。

9.17. 定期安全评审应考虑到对工作人员称职能力所做的假设，其是否对人的局限性及能力，以及任务要求和监管要求相一致。

9.18. 应利用定期安全评审，也包括通过对人因工程计划的评审，对人为的及组织的因素所进行的管理中，确认出合理可行的改进以确保取得满意的人的绩效结果。

10. 人因工程在产品选择与采购中的实施

10.1. 本部分就相关几种人因工程产品的选择、采购、集成与使用给出了建议，例如个人防护设备（例如用于维护、视察、事故监控和运行用于缓解严重事故的设备）、商用现成产品和移动设备（例如手持式、便携式和可穿戴设备）。

个人防护装备

10.2. 个人防护装备及其特性的选择应与使用者的体型、佩戴时要执行的任务以及预期使用者工作的环境范围相适应。与使用个人防护设备相关的人因工程设计标准应被用在预先准备好的设备和工具上使用，并允许辅助工作佩戴该设备时使用。

10.3. 个人防护装备不应对任务执行的可靠性有重大的影响。

10.4. 应进行人因工程分析，以确定是否可以在执行任务时使用个人防护设备，这可能会影响使用者的视力、听力、灵敏性、机动性或在极端温度下工作的能力。

10.5. 应根据个人防护设备在电厂各种工况下的预想用途（例如通过演习和应急演习）对其进行核实和验证。这种核实和验证应考虑使用者的身材的大小。

现成商业产品

10.6. 当现成商业产品融入到现有系统中时，在选择与电厂的设计、运行和维护策略一致的产品时应考虑到人为因素。

10.7. 当一个现成商业产品或多种现成商业产品融入到新的或现有的系统中时，应考虑选择那些能够确保人因界面特性一致的产品：

— 在每个系统内使用的；
— 运行人员已经在类似系统之间用过的；
— 与电厂现有人因界面特点一致的。

10.8. 如果将现成商业产品纳入现有系统，则应评定对人的绩效的影响。

10.9. 人因工程应用于确保现成商业产品的安装，不会导致工作环境或任务执行方式的不良变化。

10.10. 人因工程应用于确定现成商业产品的安装是否需要额外培训、修改或新程序、维护或试验，或技能和资格要求的变化。

移动设备

10.11. 评审移动设备的范围应包括手持设备、便携式设备和可穿戴设备。

10.12. 移动设备的选择应当以分析为基础，显示出移动设备是否适合于该任务，以及使用者是否能长时间握住它，与设备进行长时间交互，以及运送或佩戴设备。如果使用者佩戴个人防护设备则移动设备也应适合该任务。

10.13. 移动设备及其特性应与使用者的体型、环境条件和人因工程以及设计标准（例如照明、抓紧方式、尺寸、重量和人对信息处理的特征）是相互符合的。

10.14. 移动设备不使用时不应干扰其他任务的完成。

10.15. 在适当的情况下，使用者应了解极端环境中移动设备的要求（例如，坚固设备的使用）。

10.16. 在人因工程分析中应考虑移动设备的存放。

10.17. 应考虑移动设备的同步或校准要求。

10.18. 对于移动计算设备，由于对使用设备的潜在限制，错误管理对于安全非常重要。人因工程应确定是否需要：

— 纠错功能（例如，纠正错误输入和纠正个别错误而不需要重新输入正确输入的命令或数据的简单方法）；
— 用户和软件在输入后但进入系统之前及早发现和纠正错误的功能；
— 以不干扰用户的方式（例如，在数据字段的末尾而不是逐个字符地）进行错误检查；
— 当从移动设备控制设备时，用户对过程的控制（例如，由于指示的错误而在指令次序中的任何位置停止控制过程的能力）。

10.19. 应考虑来自高强度辐射场地干扰的可能性，因为这种辐射场地可能构成了对设计的限制。

参 考 文 献

[1] 国际原子能机构《核电厂安全：设计》，国际原子能机构《安全标准丛书》第 SSR-2/1（Rev.1）号，国际原子能机构，维也纳（2016 年）。

[2] 国际原子能机构《核电厂安全：调试和运行》，国际原子能机构《安全标准丛书》第 SSR-2/2（Rev.1）号，国际原子能机构，维也纳（2016 年）。

[3] 国际原子能机构《设施和活动安全评定》，国际原子能机构《安全标准丛书》第 GSR Part 4（Rev.1）号，国际原子能机构，维也纳（2016 年）。

[4] 国际原子能机构《安全的领导和管理》，国际原子能机构《安全标准丛书》第 GSR Part 2 号，国际原子能机构，维也纳（2016 年）。

[5] 国际原子能机构《设施和活动管理系统的适用》，国际原子能机构《安全标准丛书》第 GS-G-3.1 号，国际原子能机构，维也纳（2006 年）。

[6] 国际原子能机构《核装置管理系统》，国际原子能机构《安全标准丛书》第 GS-G-3.5 号，国际原子能机构，维也纳（2009 年）。

[7] 国际原子能机构《核装置运行经验反馈》，国际原子能机构《安全标准丛书》第 SSG-50 号，国际原子能机构，维也纳（2018 年）。

[8] 国际原子能机构《核电厂设计中除火灾和爆炸外的内部危害防护》，国际原子能机构《安全标准丛书》第 NS-G-1.11 号，国际原子能机构，维也纳（2004 年）（本“安全导则”正在修订中）。

[9] 联合国粮食及农业组织、国际原子能机构、国际民用航空组织、国际劳工组织、国际海事组织、国际刑警组织、经济合作与发展组织核能机构、泛美卫生组织、全面禁止核试验条约组织筹备委员会、联合国环境规划署、联合国人道主义事务协调厅、世界卫生组织、世界气象组织，《核或辐射应急准备与响应》，国际原子能机构《安全标准丛书》第 GSR Part 7 号，国际原子能机构，维也纳（2015 年）。

[10] 国际原子能机构《核电厂事故管理计划》，国际原子能机构《安全标准丛书》第 SSG-54 号，国际原子能机构，维也纳（2019 年）。

[11] 国际原子能机构《核电厂运行限值和条件及运行规程》，国际原子能机构《安全标准丛书》第 NS-G-2.2 号，国际原子能机构，维也纳（2000 年）（本“安全导则”正在修订中）。

[12] 国际原子能机构《核电厂员工的招聘、资格和培训》，国际原子能机构《安全标准丛书》第 NS-G-2.8 号，国际原子能机构，维也纳（2002 年）（本“安全导则”正在修订中）。

[13] 国际原子能机构《核电厂安全分析报告的格式和内容》，国际原子能机构《安全标准丛书》第 SSG-61 号，国际原子能机构，维也纳（修订版编写中）。

[14] 国际原子能机构《核电厂改造》，国际原子能机构《安全标准丛书》第 NS-G-2.3 号，国际原子能机构，维也纳（2001 年）。

[15] 国际原子能机构《核电厂定期安全评审》，国际原子能机构《安全标准丛书》第 NS-G-2.10 号，国际原子能机构，维也纳（2003 年）。

附　件

仪器仪表与控制及人因工程的国际标准参考书目

A-1.　原子能机构《安全标准丛书》第 SSR-2/1（Rev.1）号《核电厂安全：设计》[A-1]要求 9 规定：**“对核电厂安全重要物项的设计应按照相关的国家和国际的规范和标准。”**

A-2.　本“安全导则”提出了原子能机构成员国广泛接受的高级别建议。除了原子能机构提供的导则外，还有大量的国家和国际标准化组织，给出了更为详细的建议，来帮助接受 SSR-2/1（Rev.1）[A-1]设计方法论和系统特性。为此，将要求设计人员、营运组织和监管机构要利用这些标准中的信息。

A-3.　国际电工委员会（IEC；第 45 分委员会）和电气和电子工程师学会（IEEE；核电工程设计委员会）是负责核电厂使用的大多数仪器仪表和控制系统国际标准的两个标准制定组织。每个组织都形成了大量的标准。这两个组织制订的标准，是对构成 SSR-2/1（Rev.1）[A-1]要求的基础与本“安全导则”建议的共同原则的回答。因此，这两套标准都可以用来进一步解释本“安全导则”的建议。

A-4.　本附件旨在帮助读者理解本“安全导则”与国际电工委员会和核电工程设计委员会标准之间的关系。表 A-1 列出了与本“安全导则”的建议有密切关系的国际电工委员会和核电工程设计委员会标准。表 A-1 并不是这两套标准的完整清单，而是对加入国际电工委员会和核电工程设计委员会标准的方向进行确认。

A-5.　表 A-2 列出了与本“安全导则”重要专题领域相关标准的进入方法。

A-6.　合力避免本“安全导则”的建议与国际电工委员会和核电工程设计委员会的标准发生冲突。在本“安全导则”的形成中，国际电工委员会和核电工程设计委员会两个标准委员会的成员都需参与制定，并且两个标准组织都需对文件初稿进行评审，有助于确认并消除冲突。

A-7. 尽管如此，用户一定要认识到国际电工委员会和核电工程设计委员会标准之间存在着重大的差异，并把这一事实考虑进去。国际电工委员会标准采用了原子能机构的安全要求出版物，并将原子能机构的安全导则作为其发展的根本输入。因此，国际电工委员会标准对安全重要物项的处理，以及对仪器仪表和控制系统采用的导则，都是通过源自原子能机构的整体性建议给出的。

A-8. 核电工程设计委员会标准主要侧重于对安全重要物项，因此核电工程设计委员会导则与本“安全导则”相比，恰好适用于更小的功能、系统和设备装置。尽管如此，核电工程设计委员会导则仍可通过分级方法适用于安全相关的物项（是安全重要物项，但并没有用在安全系统上）。

A-9. 其他指导文件（如 NUREG 系列出版物）包括相关的监管决定、研究结果、事故调查结果，以及其他技术和管理上的说明报告或小册子。表 A-2 列出了与本“安全导则”重要专题领域相关的其他指导性文件。

表 A-1. 与本“安全导则”密切相关的国际标准

国际标准	标 题
IEC 60960 : 1988[A-2]	核电站安全参数显示器系统的功能设计标准
IEC 60964 : 2018 RLV[A-3]	核电厂 — 控制室 — 设计
IEC 60965 : 2016[A-4]	核电厂 — 控制室 — 用于反应堆停堆不进入主控室的辅助控制室
IEC 61227 : 2008[A-5]	核电厂 — 控制室 — 运行人员控制
IEC 61771 : 1995[A-6]	核电厂 — 主控制室 — 设计核实和验证
IEC 61772 : 2009[A-7]	核电厂 — 控制室 — 可视化显示单元（VDUS）的应用
IEC 61839 : 2000[A-8]	核电厂 — 控制室的设计 — 功能分析和分配
IEC 62241 : 2004[A-9]	核电厂 — 主控室 — 警报功能和显示
IEEE 845-1999[A-10]	核发电站人类系统绩效评价的 IEEE 导则
IEEE 1023-2004[A-11]	核发电站人因工程系统、设备和设施应用的 IEEE 实践建议
IEEE 1082-2017[A-12]	核发电站和其他核设施概率安全评定纳入人的可靠性分析的 IEEE 导则
IEEE 1289-1998[A-13]	核发电站计算机监控和控制显示器设计人因工程应用的 IEEE 导则
IEEE 1707-2015[A-14]	核设施事件调查的 IEEE 实践建议
IEEE 1786-2011[A-15]	核发电站和其他核设施的计算机化运行程序系统（COPS）人因应用的 IEEE 导则

注：IEC：国际电工委员会；IEEE：电气和电子工程师协会。

表 A-2. 国际标准、相关导则与本“安全导则”专题领域之间的关系

本“安全导则”章节	国际通用仪器仪表和控制标准
1. 导言	
2. 人因工程计划管理	IEC 61513:2011[A-16]，IEEE 1023-2004[A-11]，IEEE 1074-2006[A-17]，ISO/IEC/IEEE 15288:2015[A-18]，NUREG-0711（Rev.3）[A-19]，INL/CON-12-25117[A-20]，ISO 11064-1-7[A-21－A-27]
3. 分析	IEC 61839:2000[A-8]，IEEE 845-1999[A-10]，IEEE 1082-2017[A-12]，NUREG-0711（Rev.3）[A-19]，IEEE 1707-2015[A-14]，NUREG/CR-6400[A-28]
4. 设计：	
— 控制室	IEC 60964:2018 RLV[A-3]，IEC 61227:2008[A-5]，IEC 61771:1995[A-6]，IEC 61772:2009[A-7]，IEC 61839:2000[A-8]，IEC 62241:2004[A-9]，IEEE 576-2000[A-29]、IEEE 1289-1998[A-13]、NUREG-0700（Rev.2）[A-30]，EPRI — 控制室设计和数字人因界面设计与修改的人因导则（2015 年）[A-31]
— 辅助控制室	IEC 60965:2016 [A-4]， NUREG-0700（Rev.2）[A-30]
— 安全参数显示系统	IEC 60960:1988 [A-2]，IEEE 497-2016[A-32]，NUREG-0700（Rev.2）[A-30]，NUREG-0696 [A-33]
— 仪器仪表和控制系统人因工程的一般原则	IEEE 1023-2004 [A-11]，IEEE 1082-2017[A-12]，IEEE 1289-1998 [A-13]
5. 对人因的核实和验证	NUREG-0711（Rev. 3）[A-19]

表 A-2. 国际标准、相关导则与本“安全导则”专题领域之间的关系（续）

本“安全导则”章节	国际通用仪器仪表和控制标准
6. 人因工程设计实施	IEC 61839:2000 [A-8]，IEEE 845-1999 [A-10]，IEEE 1082-2017 [A-12]，NUREG-0711（Rev.3）[A-19]
7. 人的业绩监控	IEEE 845-1999 [A-10]，NUREG-0711（Rev.3）[A-19]
8. 人因工程在计算机程序设计中的应用	IEC 62646:2016[A-34]，IEEE 1786-2011[A-15]
9. 将人因工程纳入安全过程：	IEC 61772:2009[A-7]，IEC 62241: 004[A-9]，IEEE 1289-1998[A-13]，NUREG-0711（Rev.3）[A-19]
— 仪器仪表和控制系统的人因工程的一般原则	IEC 61513:2011[A-16]，IEEE 1023-2004 [A-11]，IEEE 1082-2017[A-12]，IEEE 1289-1998 [A-13]

附件 参考文献

[A-1] 国际原子能机构《核电厂安全：设计》，国际原子能机构《安全标准丛书》第 SSR-2/1（Rev.1）号，国际原子能机构，维也纳（2016 年）。

[A-2] 国际电工委员会《核电厂安全参数显示系统的功能设计标准》（IEC 60960:1988），国际电工委员会，日内瓦（1988 年）。

[A-3] 国际电工委员会《核电厂 — 控制室 — 设计》（IEC 60964:2018 RLV），国际电工委员会，日内瓦（2018 年）。

[A-4] 国际电工委员会《核电厂 — 控制室 — 主控制室不可达时的备用停堆控制室》（IEC 60965:2016），国际电工委员会，日内瓦（2016 年）。

[A-5] 国际电工委员会《核电厂 — 控制室 — 操纵员控制办法》（IEC 61227:2008），国际电工委员会，日内瓦（2008 年）。

[A-6] 国际电工委员会《核电厂 — 主控制室 — 设计的核实和验证》(IEC 61771:1995)，国际电工委员会，日内瓦（1995 年）。

[A-7] 国际电工委员会《核电厂 — 控制室 — 视觉显示设备（VDU）应用装置》（IEC 61772 : 2009)，国际电工委员会，日内瓦（2009 年）。

[A-8] 国际电工委员会《核电厂 — 控制室的设计 — 功能分析和分配》（IEC 61839 : 2000)，国际电工委员会，日内瓦（2000 年）。

[A-9] 国际电工委员会《核电厂 — 主控制室 — 警报功能和显示》（IEC 62241 : 2004)，国际电工委员会，日内瓦（2004 年）。

[A-10] 电气和电子工程师协会《IEEE 导则 — 关于核电厂人类系统性能评价》（IEEE 845-1999)，电气和电子工程师协会，新泽西州皮斯卡特维（1999 年）。

[A-11] 电气和电子工程师协会《IEEE 推荐实践 — 核电厂和其他核设施系统、设备和设施人因工程学应用》（IEEE 1023-2004)，电气和电子工程师协会，新泽西州皮斯卡特维（2004 年）。

[A-12] 电气和电子工程师协会《IEEE 导则 — 核电厂和其他核设施将人因可靠性分析纳入概率风险评定》（IEEE 1082-2017)，电气和电子工程师协会，新泽西州皮斯卡特维（2017 年）。

[A-13] 电气和电子工程师协会《IEEE 导则 — 核电厂基于计算机的监控显示设计中人因工程学应用》（IEEE 1289-1998)，电气和电子工程师协会，新泽西州皮斯卡特维（1998 年）。

[A-14] 电气和电子工程师协会《IEEE 推荐实践 — 核设施事件调查》(IEEE 1707-2015)，电气和电子工程师协会，新泽西州皮斯卡特维（2015 年）。

[A-15] 电气和电子工程师协会《IEEE 导则 — 核电厂和其他核设施计算机操作程序系统（COPS）的人因》（IEEE 1786-2011)，电气和电子工程师协会，新泽西州皮斯卡特维（2011 年）。

[A-16] 国际电工委员会《核电厂 — 安全重要仪器仪表和控制 — 一般系统要求》（IEC 61513 : 2011)，国际电工委员会，日内瓦（2011 年）。

[A-17] 电气和电子工程师协会《电气和电子工程师协会标准 — 开发软件项目寿期过程》（IEEE 1074-2006），电气和电子工程师协会，新泽西州皮斯卡特维（2006 年）。

[A-18] 国际标准化组织、国际电工委员会、电气和电子工程师协会，《系统和软件工程 — 系统寿期过程》（ISO/IEC/IEEE 15288:2015），国际标准化组织，日内瓦（2015 年）。

[A-19] 美国核管制委员会《人因工程项目审查模式》，第 NUREG-0711（Rev.3）号报告，美国核管制委员会，华盛顿特区（2012 年）。

[A-20] HUGO, J.，“为核工业建立统一的 HFE 程序”，第 INL/CON-12-25117 号报告，爱达荷州爱达荷瀑布城爱达荷国家工程与环境实验室（2012 年）。

[A-21] 国际标准化组织《控制中心人因工程学设计 — 第一部分：控制中心的设计原则》（ISO 11064-1 : 2000），国际标准化组织，日内瓦（2000 年）。

[A-22] 国际标准化组织《控制中心的人体工学设计 — 第二部分：控制设备的布置原则》（ISO 11064-2 : 2000），国际标准化组织，日内瓦（2000 年）。

[A-23] 国际标准化组织《控制中心的人体工学设计 — 第三部分：控制室布局》（ISO 11064-3 : 1999），国际标准化组织，日内瓦（1999 年）。

[A-24] 国际标准化组织《控制中心的人体工学设计 — 第四部分：工作站的布局和尺寸》（ISO 11064-4 : 2013），国际标准化组织，日内瓦（2013 年）。

[A-25] 国际标准化组织《控制中心的人体工学设计 — 第五部分：显示和控制》（ISO 11064-5 : 2008），国际标准化组织，日内瓦（2008 年）。

[A-26] 国际标准化组织《控制中心的人体工学设计 — 第六部分：控制中心环境要求》（ISO 11064-6 : 2005），国际标准化组织，日内瓦（2005 年）。

[A-27] 国际标准化组织《控制中心的人体工学设计 — 第七部分：控制中心评价原则》（ISO 11064-7:2006），国际标准化组织，日内瓦（2006 年）。

[A-28] 美国核管制委员会《基于运行经验的先进反应堆人因工程学（HFE）见解》，第 NUREG/CR-6400 号报告，美国核管制委员会，华盛顿特区（1997 年）。

[A-29] 电气和电子工程师协会《IEEE 推荐实践 — 工业和商业应用中使用绝缘电力电缆安装、终止和试验》（IEEE 576-2000），电气和电子工程师协会，新泽西州皮斯卡特维（2000 年）。

[A-30] 美国核管制委员会《人因界面设计审查导则》，第 NUREG-0700（Rev.2）号报告，美国核管制委员会，华盛顿特区（2002 年）。

[A-31] 电力研究院《控制室设计和数字人系统统界面设计和修改人因导则》，电力研究院，加利福尼亚州帕罗奥多（2015 年）。

[A-32] 电气和电子工程师协会《电气和电子工程师协会标准 — 核电厂事故监控仪器仪表》（IEEE 497-2016），电气和电子工程师协会，新泽西州皮斯卡特维（2016 年）。

[A-33] 美国核管制委员会《应急响应设施的功能标准》，第 NUREG-0696 号报告，美国核管制委员会，华盛顿特区（1981 年）。

[A-34] 国际电工委员会《核电厂 — 控制室 — 基于计算机的程序》（IEC 62646 : 2016），国际电工委员会，日内瓦（2016 年）。

定　义

以下定义是本出版物特有的，不在《国际原子能机构安全词汇：核安全和辐射防护使用系列（2018 年版）》中提供，或与该词汇不同。

符号“*”表示的定义与原子能机构安全词汇表中提供的定义不同。

计算机程序系统。以计算机电子化而不是以纸质格式的方式呈现电厂程序的系统。

运行的概念。* 运行的概念是为了执行设计想要的功能，对如何让其运转起来进行描述，其包括人员的多样化作用，以及如何组织、管理并帮助他们。运行的概念对电厂如何运行（“运行理念”）进行了描述，包括运行人员的数量与构成，以及他们在正常和异常工况下如何运行电厂。

错误管理。是建立在监控力、认知倾向和人体测量学的理论基础上的，其包括了在系统和技术分界面中，对人为失误的可能性进行的识别。人因系统工程先对失误进行预言，然后再为了阻止失误，或阻止这些失误对电厂安全运行造成的影响而做出设计。

人因界面。人因界面是系统的一个组成部分，通过人因界面使人员与系统进行交互来执行人因界面的功能和任务。人因界面构成了人和电厂系统之间的分界面，其包括程序、通讯系统显示、警报和控制。

人的运动控制。人的运动控制是指人的肌肉系统对动作进行控制的生理能力，包括对力量活动和细小活动的控制。

由人完成的重要任务。由安全分析决定的、能对安全产生负面或正面效果的由人来完成的任务。

状况意识。是为了帮助个人和团队对系统后续工况的预计能力，对电厂实际工况进行监控并理解的动态过程。它是对状况及后续计划行动的智力原型的一种构想方式。状况意识的多少，相当于是对电厂工况与真实工况之间，在给定规定时间上的理解差异。人因系统工程的目标之一，就是为了帮助运行人员形成状况意识。

验证。* 通过检查并借助于客观证据，把人因界面系统，包括用户当作一个整体，对成功地执行其想要的功能进行的确定，并在所想到的不得不进行操作的运行环境范围内，符合其目的与目标。

核实。* 通过检查并借助客观证据，把人因界面系统当作一个整体，来确定其符合设计规范和要求，并对完成想要完成的任务提供必要的帮助。

参与起草和审订人员

Duchac, A.	国际原子能机构
Gertman, D.	爱达荷国家工程与环境实验室
Hata, T.	日本核监管局
Humbel, C.	瑞士联邦核安全监察局
Illobre, F.	西班牙泰纳通有限公司
Ito, K. MHI	日本核系统与解决方案工程公司
Johansson, Y.	瑞典辐射安全局
Laarni, J.	芬兰技术研究中心
Ngo, C.	加拿大坎杜公司
Obenius Mowitz, A.	瑞典辐射安全局
O'Hara, J.	美国布鲁克海文国家实验室
Rycraft, H.	国际原子能机构
Screeton, R.	英国核监管办公室
Selmer, S.	瑞典辐射安全局
Tasset, D.	法国辐射防护与核安全研究所
Yllera, J.	国际原子能机构

IAEA
国 际 原 子 能 机 构

No. 27

当 地 订 购

国际原子能机构的定价出版物可从我们的主要经销商或当地主要书商处购买。
未定价出版物应直接向国际原子能机构发订单。

定价出版物订单

请联系您当地的首选供应商或我们的主要经销商：

Eurospan
1 Bedford Row
London WC1R 4BU
United Kingdom

交易订单和查询：
电话：+44 (0) 1235 465576
电子信箱：trade.orders@marston.co.uk

个人订单：
电话：+44 (0) 1235 465577
电子信箱：direct.orders@marston.co.uk
网址：www.eurospanbookstore.com/iaea

欲了解更多信息：
电话：+44 (0) 207 240 0856
电子信箱：info@eurospan.co.uk
网址：www.eurospan.co.uk

定价和未定价出版物的订单均可直接发送至：

Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
电话：+43 1 2600 22529 或 22530
电子信箱：sales.publications@iaea.org
网址：https://www.iaea.org/zh/chu-ban-wu

通 过 国 际 标 准 促 进 安 全

国际原子能机构
维也纳