国际原子能机构安全标准

保 护 人 类 与 环 境

研究堆安全重要仪器仪表和控制系统与软件

特定安全导则

第 SSG-37 (Rev.1) 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。

研究堆安全重要仪器
仪表和控制系统与软件

国际原子能机构成员国

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
布隆迪
佛得角
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
库克群岛
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
荷兰王国
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-37（Rev.1）号

研究堆安全重要仪器仪表和控制系统与软件

特定安全导则

国 际 原 子 能 机 构
2024 年 · 维也纳

版 权 说 明

国际原子能机构印刷
2024 年 9 月 • 奥地利

研究堆安全重要仪器仪表和控制系统与软件

国际原子能机构，奥地利，2024 年 9 月
STI/PUB/2051
ISBN 978-92-0-510924-4（简装书：碱性纸）
978-92-0-510724-0（pdf 格式）
EPUB 978-92-0-510824-7
ISSN 1020-5853

前　言

拉斐尔·马里亚诺·格罗西总干事

国际原子能机构（原子能机构）《规约》授权原子能机构“制定……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”。这些是原子能机构必须适用于其自身业务而且各国可以通过其国家法规来适用的标准。

原子能机构于 1958 年开始实施其安全标准计划，此后有了许多发展。作为总干事，我致力于确保原子能机构维护和改进这套具有综合性、全面性和一致性的、与时俱进的、用户友好的和适合目的的高质量安全标准。在利用核科学和技术的过程中正确地适用这些标准将为全世界的人和环境提供高水平的保护，并为持续利用核技术造福于所有人提供必要的信心。

安全是得到许多国际公约支持的一项国家责任。原子能机构的安全标准奠定了这些法律文书的基础，而且是有助于各方履行各自义务的全球基准。虽然安全标准对成员国没有法律约束力，但它们被广泛适用。对已在国家法规中采用这些标准以加强核能发电、研究堆和燃料循环设施中以及医学、工业、农业和研究领域核应用中的安全的绝大多数成员国而言，它们已成为不可或缺的基准点和共同标准。

原子能机构的安全标准以原子能机构成员国的实际经验为基础，并通过国际协商一致产生。各安全标准分委员会、核安保导则委员会和安全标准委员会成员的参与尤其重要，我向所有为这项工作贡献自己的知识和专长的人表示感谢。

原子能机构在通过评审工作组访问和咨询服务向成员国提供援助时，也使用这些安全标准。这有助于成员国适用这些标准，并使得能够共享宝贵经验和真知灼见。在安全标准的定期修订过程中，会考虑到这些工作组访问和服务的反馈，以及从使用和适用安全标准的事件和经历中汲取的教训。

我相信，原子能机构安全标准及其适用将为确保在使用核技术时实现高水平安全作出宝贵的贡献。我鼓励所有成员国宣传和适用这些安全标准，并与原子能机构合作，在现在和将来维护其质量。

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）。

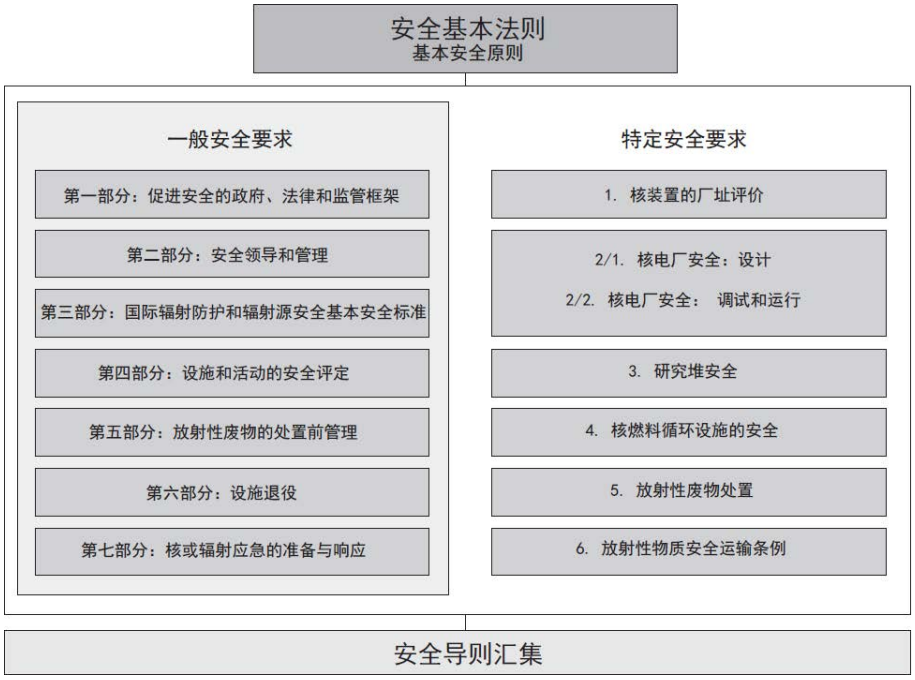

图 1. 国际原子能机构《安全标准丛书》的长期结构。

[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”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当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）、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。

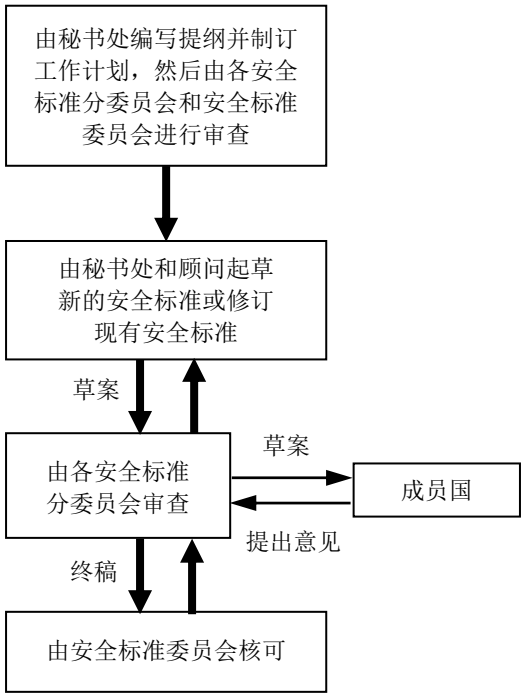

图 2. 制订新安全标准或修订现行标准的过程。

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

安全和核安保相关术语应理解为《国际原子能机构核安全和核安保术语》（见 https://www.iaea.org/resources/publications/iaea-nuclear-safety-and-security-glossary）中的术语。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. 原子能机构《安全标准丛书》第 SSR-3 号《研究堆的安全》[1]确立了研究堆的安全要求，特别强调其设计和运行。

1.2. 本“安全导则”提供了关于研究堆仪器仪表和控制系统设计和运行的建议。

1.3. 本“安全导则”是与其他七份关于研究堆安全的《安全导则》同时编写的，具体如下：

(a) 原子能机构《安全标准丛书》第 SSG-80 号《研究堆的调试》[2]；

(b) 原子能机构《安全标准丛书》第 SSG-81 号《研究堆的维护、定期试验和视察》[3]；

(c) 原子能机构《安全标准丛书》第 SSG-82 号《研究堆堆芯管理和燃料装卸》[4]；

(d) 原子能机构《安全标准丛书》第 SSG-83 号《研究堆的运行限值和条件及运行程序》[5]；

(e) 原子能机构《安全标准丛书》第 SSG-84 号号《研究堆营运组织和人员招聘、培训与资格》[6]；

(f) 原子能机构《安全标准丛书》第 SSG-85 号《研究堆设计和运行中的辐射防护和放射性废物管理》[7]；

(g) 原子能机构《安全标准丛书》第 SSG-10（Rev.1）号《研究堆老化管理》[8]；

1.4. 原子能机构《安全标准丛书》第 SSG-20（Rev.1）号《研究堆安全评定和安全分析报告的编写（Rev.1）》[9]和第 SSG-24（Rev.1）号《研究堆的利用和改造安全（Rev.1）》[10]提供了关于研究堆安全的其他建议。

1.5. 本“安全导则”使用的术语应当理解为原子能机构《核安全和安保术语》[11]定义和解释。

1.6. 本“安全导则”替代原子能机构《安全标准丛书》第 SSG-37 号《研究堆安全重要仪器仪表和控制系统及软件》[1]。

目的

1.7. 本“安全导则”的目的是提供对研究堆安全重要仪器仪表和控制系统及软件的建议，包括仪器仪表和控制系统结构及相关部件－从传感器到致动器、人机界面和辅助设备－以满足 SSR-3[1]相关要求，特别是要求 49、51 和 52。

1.8. 本“安全导则”提供的建议针对研究堆的营运组织、监管机构和参与研究堆物项的其他组织，包括仪器仪表和控制系统的供应商。

范围

1.9. 本“安全导则”主要适用于额定功率高达几十兆瓦的异质热谱研究堆。对于功率较高的研究堆、专用反应堆（如快谱反应堆）和具有专用设施（如热中子源或冷中子源、高压和高温回路）的反应堆，可能需要额外的指导。对于这种研究堆，原子能机构《安全标准丛书》第 SSG-39 号《核电厂仪器仪表和控制系统的设计》[12]提供的建议可能更合适。均相反应堆和加速器驱动系统不在本出版物的范围内。

1.10. 一些较低潜在危害的研究堆、临界组件和次临界组件可能不太需要全面的方法。虽然本“安全导则”的所有建议都应当予以考虑，但有些建议可能不适用于此类研究堆、临界组件和次临界组件（见 SSR-3[1]要求 12 和第 2.15－2.17 段，以及原子能机构《安全标准丛书》第 SSG-22（Rev.1）号《分级方法在适用研究堆安全要求中的使用》[13]）。

1.11. 在本“安全导则”，只有当特定建议与次临界组件无关或仅适用于次临界组件时，才会单独提及次临界组件。

1.12. 这些建议适用于新研究堆仪器仪表和控制系统及软件的设计和配置管理，以及现有研究堆仪器仪表和控制系统及软件的现代化。

---

[1] 国际原子能机构《研究堆安全重要仪器仪表和控制系统及软件》，国际原子能机构《安全标准丛书》第 SSG-37 号，维也纳（2015 年）。

1.13. 本“安全导则”还提供了关于仪器仪表和控制系统以及安全重要软件的人因工程和人机界面的建议。“安全导则”还提供了与研究堆仪器仪表和控制系统设计中安全和安保接口考虑相关的导则。

结构

1.14. 第 2 部分提供了仪器仪表和控制功能、系统和部件的安全分级建议；第 3 部分提供了如何将仪器仪表和控制系统排列成层级结构的建议；第 4 部分和第 5 部分提供了满足仪器仪表和控制系统设计要求的建议；第 6 部分提供了关于仪器仪表和控制系统运行方面的建议；第 7 部分扩展了第 4 部分在人机界面方面提供的建议；第 8 部分提供了关于基于计算机系统和软件的设计和其他方面的建议；第 9 部分提供了仪器仪表和控制系统配置管理的建议；第 10 部分提供了关于仪器仪表和控制系统的改造和现代化的建议。附件确定了可用于研究堆仪器仪表和控制系统。

2. 研究堆仪器仪表和控制系统的安全分级

2.1. 仪器仪表和控制功能、系统和部件可分为两类：安全重要和非安全重要（见图 1 和附件）。对非安全重要仪器仪表和控制系统是那些用于支持设施运行但对反应堆安全没有影响的系统。

2.2. 对安全重要的功能、系统和部件是指有助于以下主要安全功能的功能、系统和部件（见 SSR-3[1]要求 7）：

(a) 控制反应性，安全关闭反应堆，并在运行状态、事故工况和事故后工况下将其保持在安全关闭工况下；

(b) 在所有运行状态和事故工况下，从反应堆和燃料贮存库中排出热量；

(c) 密封放射性物质、屏蔽辐射、控制计划的放射性排放以及限制意外的放射性排放。

2.3. 根据原子能机构《核安全和安保术语》[11]，对安全重要系统和部件进一步分为安全系统、设计扩展工况下的安全特点和安全相关系统，特定如下：

(a) 安全系统：保护系统、安全驱动系统和安全系统支持功能；

(b) 设计扩展工况下的安全特点：设计用于执行设计扩展工况下的安全功能或在设计扩展工况下具有安全功能的物项；

(c) 安全相关系统：不属于安全系统的安全重要系统，如监控安全系统可用性的系统。

2.4. 研究堆安全要求的应用需要一种分级方法（见 SSR-3[1]要求 12）。对于安全重要仪器仪表和控制系统分级方法的程度是：

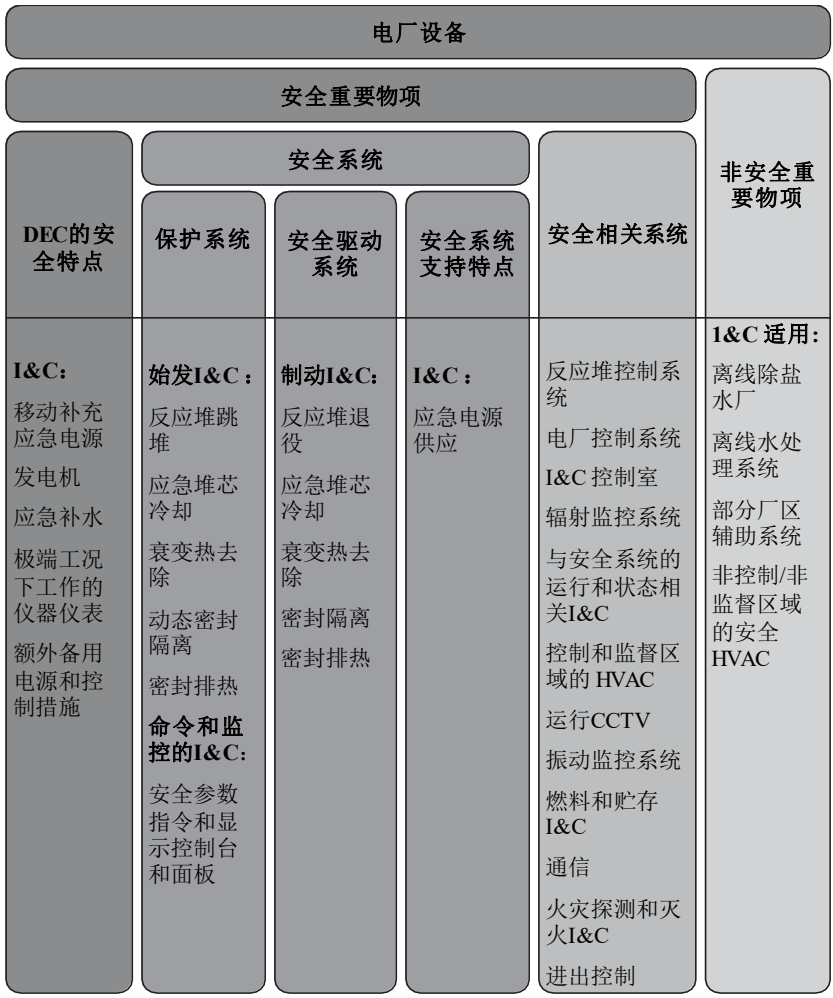

图 1. 根据对安全的重要性分类的研究堆仪器仪表和控制系统的示例。CCTV－闭路电视；DEC－设计扩展工况；HVAC－供暖、通风和空调；I & C－仪器仪表和控制。

应用应当在安全分析报告中明确说明（要考虑的因素见 SSR-3[1]第 2.17 段）。SSG-22[13]提供了关于分级方法应用的建议。

仪器仪表和控制系统的分级

2.5. SSR-3[1]第 6.29 段指出（脚注略）：

> “安全重要物项的安全重要性分类方法必须以确定性方法为主，在适当情况下通过概率方法（如有）进行补充，并适当考虑以下因素：
>
> (a) 物项将执行的安全功能；
> (b) 未能履行安全功能的后果；
> (c) 调用该物项执行安全功能的频率；
> (d) 在假想始发事件之后的时间，在此时间或期间，该物项将被要求执行安全功能。”

2.6. 按需故障或虚假驱动可能导致始发事件或使假想始发事件的后果恶化的仪器仪表和控制系统应当被归类为高安全级别。反应性控制系统的仪器仪表和控制方面也应当采用类似的方法，其故障可能导致事故工况。

2.7. 应当确定研究堆所有设施状态的仪器仪表和控制功能。对于研究堆，缓解设计扩展工况后果所需的仪器仪表和控制功能可以被分配到比控制预计运行事件和设计基准事故以达到安全状态所需的功能更低安全级别。

仪器仪表和控制系统设计、建造、调试、运行和维护

2.8. 所有仪器仪表和控制系统及设备的设计、建造、调试、运行和维护应当确保其规范、核实和验证及其质量和可靠性与其安全级别相称。规范应当为其安全系统设计考虑足够的功能裕度。这些裕度应当通过试验和分析在部件级和系统级进行核实。

2.9. SSR-3[1]第 6.30 段指出：

> “设计必须确保防止安全重要物项之间的任何干扰，特别是在较低安全级别的系统中安全重要物项的任何故障不会传播到较高安全级别的系统。”

所有执行对安全重要功能的仪器仪表和控制系统都应当与不同安全级别的系统和设备有适当设计的接口（通过适当的实物或逻辑屏障），以满足上述要求。防止这种故障传播的设备应当被视为较高级别的设备。

2.10. 仪器仪表和控制系统的安全级别应当与其控制的系统或设备的最高安全级别相同。

3. 研究堆整体仪器仪表和控制系统结构

3.1. 仪器仪表和控制系统结构应当支持确保研究堆安全所需的所有仪器仪表和控制功能。SSR-3[1]要求 49 规定：

> **“必须为研究堆设施提供仪器仪表，以监控可能影响其安全和可靠运行所必需的主要安全功能和主要加工变量的所有主要变量的数值，确定设施在事故工况下的状态，并作出事故管理决定。设施必须提供适当和可靠的控制系统，以保持和限制相关加工变量在规定的运行范围内。”**

确保研究堆正常运行安全的仪器仪表和控制系统应当包括启动、功率运行、停堆、换料和维护。

3.2. SSR-3[1]第 6.168 段指出：“反应堆必须配备适当的手动和自动控制设备，以将参数保持在规定的运行范围内。”仪器仪表和控制系统应当能够自动启动反应堆停堆、堆芯应急冷却、余热排出和放射性物质密封，尽管如第 5.14 段所要求可能允许手动操作。仪器仪表和控制系统结构应当提供足够的涵盖所有预计运行事件、事故工况和事故后工况的能力。

3.3. 仪器仪表和控制系统结构（见第 3.15－3.18 段）应当提供仪器仪表和控制系统的高级定义，仪器仪表和控制功能分配给这些系统，以及仪器仪表和控制系统与反应堆运行人员和用户之间的通信（接口）。应当认真考虑高度一体化系统的结构，以确保纵深防御概念的适当实施（见第 3.4－3.6 段）。结构设计应当包括功能的合理分配，确保这些功能只分配给需要它们的系统。特定仪器仪表和控制系统可以包括在一个特定研究堆的整体系统结构中，这取决于反应堆的类型、用途和运行模式。附件描述了不同的仪器仪表和控制系统。

研究堆仪器仪表和控制系统中纵深防御的应用

3.4. SSR-3[1]第 2.11 段指出：

> “在整个设计和运行过程中应用纵深防御概念，可以防止预计运行事件和事故，包括设备故障或设施内不适当的人的行为造成事件和外部危害引起的事件。”

3.5. SSR-3[1]要求 10 规定：**“研究堆的设计必须应用纵深防御的概念，纵深防御级别必须尽可能独立。”**

3.6. 仪器仪表和控制系统系统结构的目标应当包括以下内容：

(a) 应用纵深防御概念。就仪器仪表和控制而言，纵深防御包括实施连续的仪器仪表和控制功能，旨在限制假想始发事件的后果，尽管设计用于首先做出反应的仪器仪表和控制系统出现故障。

(b) 不影响纵深防御概念在研究堆设计中的总体应用。

研究堆仪器仪表和控制系统的独立性

3.7. 独立性原则旨在防止故障从受故障影响的物项传播到其他冗余物项，或者从一个系统传播到另一个系统。

3.8. 仪器仪表和控制系统结构应当不损害不同纵深防御级别的独立性。

3.9. 安全系统应当独立于较低安全级别的系统，以防止故障从较低安全级别的系统传播，并确保安全系统能够在必要时执行其安全功能。

3.10. 安全系统支持特点的设计应当不损坏安全系统冗余部件之间或安全系统与较低安全级别系统之间的独立性。

研究堆仪器仪表和控制系统中对共因故障的考虑

3.11. 共因故障被定义为由于单一事件或原因导致的两个或多个结构、系统和部件的故障[11]。例如，由于以下原因，可能会发生共因故障：

(a) 运行或维护中的人为错误；

(b) 设计缺陷；

(c) 制造缺陷；

(d) 规范不足；

(e) 对内部或外部危害、人为事件、高电压、数据错误、数据通信错误或系统或部件之间故障传播的鉴定或保护不足。

3.12. SSR-3[1]要求 26 规定：

“研究堆设施的设备设计必须适当考虑到对安全重要物项共因故障的可能性，以确定如何必须用多样性、冗余、实物分隔和功能独立的概念来实现必要的可靠性。”

电气隔离用于防止一个系统中的电气故障影响连接系统或系统内的冗余元件，应当被视为实现必要可靠性的一种手段。

3.13. 应当识别潜在故障和可能导致冗余物项常见故障的常见故障模式。在宣布系统或单一部件之间的共因故障的来源不可信且无需进一步考虑之前应当提供正当性。例如，这种正当性可以基于指定的仪器仪表和控制功能纵深防御级别、部件的可靠性或所应用的技术。

3.14. 应对安全分析范围内的每个假想始发事件的后果进行分析，并结合会阻止保护系统执行必要安全功能的常见原因故障。

研究堆仪器仪表和控制系统的系统结构设计

3.15. 仪器仪表和控制系统结构应当包括以下规定：

(a) 它应当包括确保研究堆安全运行和管理预计运行事件和事故工况所需的所有仪器仪表和控制功能。

(b) 它应当包括支持研究堆纵深防御策略所需的系统。

(c) 它应当确保安全系统运行所需的行动优先于较低安全级别的系统运行所需的相反行动。

(d) 它应当确保系统和部件的适当布置，以便能够定期进行充分试验和维护，并能够根据 SSR-3[1]要求 51 进行适当的自检。

(e) 它应当根据需要将整个仪器仪表和控制系统划分为单独的系统，以实现以下目标：

(i) 满足纵深防御概念不同级别功能之间独立性的设计基准要求；

(ii) 充分分离不同安全级别的系统和功能；

(iii) 建立满足设计基准可靠性要求所需的冗余度；

(iv) 支持安全系统或安全系统组合符合单一故障标准和故障安全概念。

(f) 它应当定义人机界面以及各个仪器仪表和控制系统之间的界面。

(g) 它应当考虑研究堆的未来利用和改造，以及仪器仪表和控制系统配置的潜在变化，以便在反应堆的整个寿命期间进行配置管理。

(h) 它应当包括主控制室和辅助控制室（如适用）中的必要信息和运行人员控制，以及运行或事故管理需要信息的其他区域。

(i) 它应当包括必要的自动控制，以在规定的正常运行范围内维持和限制安全重要过程变量。

3.16. 仪器仪表和控制系统结构设计的输入应当参考研究堆的书面设计基准，该基准应当提供以下信息：

(a) 纵深防御概念在研究堆中的应用；

(b) 为应对假想始发事件而要实现的安全功能；

(c) 安全分级和安全重要物项的功能和性能要求；

(d) 将功能分配给手动手段和自动手段，以及自动化的作用和反应堆运行人员在管理预计运行事件和事故工况中的行动；

(e) 要提供给运行人员的信息 [2]；

(f) 自动启动和手动启动行动的优先级标准；

(g) 监管要求，包括仪器仪表和控制系统的授权要求；

(h) 安全重要系统的运行特点（例如，与人机界面相关的仪器仪表和控制系统的设计）。

[2] 运行人员包括反应堆经理、反应堆主管、值班主管、反应堆运行人员、维护人员和辐射防护人员。

3.17. 在仪器仪表和控制系统的结构中使用多样性、冗余性和独立性（即实物分隔、电气和功能隔离）应当符合每个仪器仪表和控制系统的安全分级，并符合纵深防御概念的应用，无论是对整个设施还是对仪器仪表和控制系统。关于冗余性应当考虑其他因素，如可靠性 [3] 以及仪器仪表和控制系统的可用性。

3.18. 仪器仪表和控制系统需要具有故障安全设计（参见 SSR-3[1]要求 28），以便仅由设计基准中详述范围内的条件变化引起的系统内任何故障都不会导致不安全工况或故障。

4. 仪器仪表和控制系统设计导则

4.1. 仪器仪表和控制系统必须符合其设计基准（见本“安全导则”第 4.3 段和第 4.4 段），根据 SSR-3[1]要求 17 建立。每个元件的起源和目标设计基准应当被指定和记录，以促进核实和可追溯性，并表明所有相关的设计要求都已得到满足。

4.2. 仪器仪表和控制系统的设计应当尽可能简单，同时仍确保其安全功能得以实现。设计的简单性导致更少的部件、更简单的界面、更容易的核实和验证，以及更容易的硬件和软件维护。应当仔细分析仪器仪表和控制系统的设计要求，以确保设计的简单性。

研究堆仪器仪表和控制系统设计基准

4.3. 研究堆每个安全重要仪器仪表和控制系统的设计基准应当规定如下：

(a) 要求系统运行的设施状态（运行状态和事故工况）；
(b) 仪器仪表和控制系统需要适应当研究堆的各种配置以及实验配置；
(c) 每个设施状态和运行模式下系统的功能要求，包括延长关闭时间；
(d) 履行安全功能的性能要求，包括保证的响应时间、延迟、精度和仪器仪表误差；
(e) 允许对每个手动保护行动进行手动控制的设施工况；

[3] 可靠性是指一个系统、一个部件或一个物项能够满足其要求的概率在规定的时间内和规定的运行工况下要求时的最低性能要求[11]。

(f) 所述系统需要响应的所述假想始发事件；

(g) 要监控的变量（或参数组合）、所需的控制行动，以及要自动、手动或两者同时执行行动的识别；

(h) 系统输入和输出信号的必要范围、变化率和精度；

(i) 在所有假想条件下对过程变量值的约束；

(j) 定期试验、自我诊断和维护的标准；

(k) 系统可靠性水平，可以使用确定性标准、概率标准或两者来指定；

(l) 系统可用性要求；

(m) 要求系统执行安全功能的瞬态和稳态环境条件的范围；

(n) 要求系统执行安全功能的环境条件范围，包括由自然现象引起的危害；

(o) 有可能降低安全重要系统功能性能的任何条件，以及保持其执行安全功能能力所必需的规定；

(p) 运行限值，例如需要与其他系统接口。

4.4. 在反应堆保护系统的设计基准应当规定如下：

(a) 安全系统的启动设置，应当从安全分析中得出；

(b) 要显示的变量，以便反应堆运行人员可以确认反应堆保护系统的运行或可以启动手动操作；

(c) 允许仪器仪表和控制安全功能旁路的工况（包括持续时间），以允许运行模式、试验或维护的改变。

研究堆仪器仪表和控制系统的可靠性设计

4.5. 如有必要，应当结合使用多种措施来实现和保持仪器仪表和控制系统所需的可靠性（见 SSR-3[1]要求 24）。

冗余和单一故障标准在研究堆仪器仪表和控制系统中的应用

4.6. 单一故障是指导致部件丧失执行其预期安全功能能力的故障，以及由这种能力丧失导致的任何间接故障[11]。单一故障可能发生在需要执行安全功能时或在此之前的任何时间。

4.7. 在研究堆的设计中，要求将单一故障标准应用于每个安全组（见SSR-3[1]要求 25），并涉及一种确定性方法来确定安全重要物项的必要冗余程度。对于安全系统，应用单一故障标准以便系统能够在出现任何单一故障的情况下执行其预期的安全功能。系统中的单一故障应当是与 (a) 由于假想始发事件导致的其他故障；和 (b) 系统中任何可信的未检测到的故障一起考虑。

4.8. 冗余是提高对安全重要系统的安全和可靠性的重要设计原则。冗余的概念应当通过适当提供替代（相同或不同）结构、系统或部件来应用，以便任何单一结构、系统或部件都能履行所需的功能，而不管任何其他结构、系统或部件的运行状态或故障。

4.9. SSR-3[1]第 6.79 段指出："采用的冗余程度必须反映可能降低可靠性的未检测故障的可能性。"对于安全重要仪器仪表和控制系统，应当在必要的程度上应用冗余（在系统级或部件级，或两个级别），以符合可靠性和可用性的设计基准。对于属于安全系统的仪器仪表和控制系统，当系统或部件因计划的监视或试验而停止使用时，冗余也应用到符合单一故障标准的必要程度。

4.10. 如果符合单一故障标准不足以满足可靠性要求，则应当提供额外的设计特点，或对设计进行修改。

研究堆仪器仪表和控制系统的常见故障原因

4.11. SSR-3[1]第 6.80 段指出："在考虑到运行、维护和试验多样化设备的复杂性可能带来的不利因素后，必须在可行的情况下采用多样化原则。"对安全重要仪器仪表和控制系统的设计必须通过应用独立性和多样性的标准，将共因故障的可能性降至最低。安全系统的设计必须能防止或缓解常见原因故障。

研究堆仪器仪表和控制系统的实物分隔和独立

4.12. SSR-3[1]要求 27 规定：

> **"研究堆设施的安全系统之间或系统的冗余元件之间的干扰，必须以下列方式防止实物分隔、电气隔离、功能独立和通信（数据传输）独立。"**

4.13. 独立性是一种设计特点，可降低共因故障和故障传播的风险。在可行的情况下，冗余安全系统应当相互实物分隔和电气隔离，并与较低安全级别的系统隔离。独立性的概念应当适用于整个安全系统，例如同一系统内的冗余通道之间，以及履行相同功能的不同系统之间，如第一和第二停堆系统。要求独立的安全功能应当由不同的模块、部件或系统执行，以避免其中任何一个物项的故障影响其他物项的性能。

4.14. 实物分隔应当被视为避免火灾、水淹或其他外部事件或事故工况导致的共因故障的一种手段。实物分隔也降低了人为疏忽错误的可能性。

4.15. 在设计研究堆的特定部分时，如密封贯穿件、电缆铺设室、设备室和控制室，应当考虑假想始发事件后可能丧失独立性的程度。

4.16. 安全系统内冗余部分之间的电气连接和数据连接的设计应当确保一个冗余部分的可信故障不会阻止其他冗余部分满足性能和可靠性的设计要求。

4.17. 安全系统和较低安全级别系统之间的电气连接和数据连接的设计应当确保较低安全级别系统中的可信故障不会阻碍安全系统满足性能和可靠性的设计要求。

4.18. 应当使用电气隔离来控制或防止由电磁干扰、静电拾取、短路、开路、接地和施加最大可信电压（交流或直流）等因素引起的设备和部件之间的不利相互作用。电气隔离规定的示例有电子隔离设备、光隔离设备（包括光纤）、继电器、电缆或部件的屏蔽、分隔和距离或这些的组合。

4.19. 当在安全系统和较低安全级别的系统之间使用隔离设备时，隔离设备应当是具有较高安全级别系统的一部分。

4.20. 当在安全系统和较低安全级别的系统之间提供适当的实物分隔或电气隔离不可行时，应当执行以下建议：

(a) 较低安全级别的系统应当被识别为与其相关联的安全系统的一部分。

(b) 较低安全级别的系统应当独立于也在较低安全级别中的其他系统。

(c) 应对安全级别较低的系统进行分析或试验，以证明它不会不可接受地降低与其相关的安全系统。

4.21. 如果安全系统中要求独立的物项之间使用数据通信通道，其设计也应当应用独立性的概念（功能独立、电气隔离和实物分隔，视情况而定）。这包括不受沟通错误影响的独立性。

研究堆仪器仪表和控制系统的多样性

4.22. 多样性是指存在两个或多个冗余系统或部件来执行所识别的功能，其中不同的系统或部件具有不同的属性，以降低共因故障（包括共模故障）的可能性。因此，多样性增加了在必要时采取适当安全措施的可能性。这包括功能多样性和设备多样性（见第 4.25 段）。示例包括提供使用不同实物方法来提供实物多样性的设备类型、不同的工作原理、不同的硬件和/或软件设计、使用不同开发方法的不同设计团队以及使用不同设计的不同制造商。

4.23. 仪器仪表和控制系统的多样性应当通过使用不同的方法或技术、不同的逻辑或算法和/或不同的驱动手段来监控和处理参数，以便提供一种以上的方法来检测和响应特定事件。应当确保在设计中实现仪器仪表和控制系统的必要多样性，并在研究堆的整个寿命期间保持这种多样性。

4.24. 当声称两个系统（例如，一个具有主反应堆保护系统和一个不同的次级反应堆保护系统的研究堆，见第 5.11 段）之间的独立性时，通过在概率安全评定中乘以它们的故障概率，然后整个仪器仪表和控制链－从传感器、信号整备设备、信号处理器和计算器到执行器驱动器－都应当在证明多样性时使用。

4.25. 应用于仪器仪表和控制系统的多样性应当包括以下一种或两种手段：

(a) 功能多样性：这可以通过提供不同实物功能或实物手段的系统来实现，从而产生相同的安全效果。

(b) 设备多样性：这可以通过使用不同技术或由不同制造商设计和生产的传感器和系统来实现。

4.26. 在评定声称具有技术多样性的设备多样性时，应当注意设备的组成部分，以确保多样性确实存在。例如，不同的制造商可能使用相同的处理器或相同的运行系统，从而可能包含常见的故障模式。如果不考虑这些因素，仅仅基于制造商名称不同的技术多样性主张是不够的。

研究堆仪器仪表和控制系统的故障模式

4.27. 对安全重要仪器仪表和控制系统的可能故障模式应当在设计过程中确定。应当消除系统性故障模式。应当使用故障模式分析和因果分析方法正确记录非系统故障模式。更可能的非系统故障模式既不会使系统处于不安全状态，也不会引起安全系统的虚假驱动。

4.28. 对安全重要仪器仪表和控制系统故障模式的识别和分析应当考虑人因和人机界面。

4.29. 仪器仪表和控制系统部件的故障应当是自我指示的，或者应当通过定期试验或警报或其他指示来检测。

4.30. 安全重要仪器仪表和控制系统的设计应当包括通过自检检测系统中所有假设（识别）故障模式的规定，最好包括故障警报和试验读数可信度的组合。这通常是对定期试验的补充以展示系统性能。

研究堆仪器仪表和控制系统的故障安全设计

4.31. 要求在仪器仪表和控制系统的设计中考虑并酌情纳入故障安全设计（参见 SSR-3[1]要求 28）。设计应当确保在系统发生故障的情况下，系统进入安全状态，无需任何系统或反应堆运行人员采取任何行动。

研究堆仪器仪表和控制系统的老化设计考虑

4.32. 电气和电子系统和部件的使用寿命可能大大低于设施的使用寿命。影响经鉴定安全系统部件在恶劣服务条件下运行能力的老化效应，可能早在正常工况下对部件的功能能力产生任何可检测的影响之前就已经发生了。在设计过程中，应当确定可能影响仪器仪表和控制系统部件的退化机制以及检测由此产生的老化效应的方法。老化通常是由于高温和辐射照射，然而，应当考虑到其他现象（如机械振动、化学降解）可能与特定部件相关的可能性。

4.33. 在仪器仪表和控制系统的设计中需要考虑老化问题（见要求 37 和 SSR-3[1]第 6.112 段）。要考虑的因素包括计划和管理使用寿命的缩短、制造来源的减少和材料短缺。应当特别注意基于计算机设备的老化。

4.34. 设计中应当考虑潜在的重大老化影响（如热老化、辐射老化），以确保在运行状态和事故工况下保持必要的功能，直至系统或部件的使用寿命结束。在适当的情况下，应当采取进一步的保守措施，以考虑到意料之外的退化机制。

4.35. 应对老化影响的方法示例如下：

(a) 在部件的鉴定使用寿命结束前更换部件；
(b) 调整功能特征（如重新校准），以考虑到老化的影响；
(c) 对维护程序或环境条件的改变具有减缓老化过程的效果；
(d) 监控设备状况，包括自检老化特征。

4.36. SSG-10（Rev.1）[8]提供了关于老化管理和陈旧管理的进一步建议。

研究堆仪表和控制系统的设计中安全和安保接口的考虑

4.37. 适用于研究堆仪器仪表和控制系统的核安保（包括实物和计算机安保）的目的是防止、检测并在检测到时消除或减少可能从受保护设施现场区域内外被利用的漏洞，或与材料、设备、软件和数据相关的漏洞（另见第 8 部分）。研究堆仪器仪表和控制系统履行安全和核安保的功能。应当评定仪器仪表和控制系统在结构和功能上的脆弱性以及这些脆弱性对研究堆的安全和核安保的影响。

4.38. 从系统设计一开始，仪器仪表和控制系统就需要考虑安保措施。主要的安保考虑因素之一是由于外部或内部恶意行为而导致仪器仪表和控制系统故障或操纵的可能性。研究堆仪器仪表和控制系统的设计需要考虑并包括防止恶意行为或利用系统的措施。

4.39. 仪器仪表和控制系统总体结构中的许多设计概念和部件有助于加强安全和核安保，然而，为了满足 SSR-3[1]要求 90，应对系统结构进行评定，以确保安全措施和安保措施不会相互损害。如果潜在的冲突在设计过程中应当考虑已确定的补偿措施，以免削弱系统的安全或核安保。

4.40. 任何计算机安保功能的运行或故障都不应对仪器仪表和控制系统执行其安全功能的能力产生不利影响。同样，安全功能的执行应当不影响研究堆的核安保。

4.41. 如果在人机界面中包括计算机安保措施，其设计应当确保不会对运行人员维护研究堆安全的能力产生不利影响。

4.42. 在切实可行的情况下，在与仪器仪表和控制系统隔离的设备中，应当实施不具有安全效益的安保措施。

4.43. 营运组织为确保仪器仪表和控制系统设计中的安全而使用的计划和程序不应对安保系统产生不利影响。

4.44. 营运组织和设计人员应当在仪器仪表和控制系统寿期的所有阶段考虑安全和核安保，以及计算机安全和安保：设计要求规范，概念、初始和详细设计，以及仪器仪表和控制系统的采购、制造、集成、安装、调试、运行和维护以及退役。

4.45. 核设施的核安保建议见参考文献[14]，参考文献[15－17]提供了计算机安保导则。还需要考虑国家对信息技术安保的要求。

研究堆仪器仪表和控制系统的设备鉴定

4.46. 安全重要仪器仪表和控制系统以及部件必须符合其预期功能（见SSR-3[1]要求 29）。鉴定应当提供与系统或部件的安全级别相称的置信度，部件在使用范围内应当满足所有设计基准要求、设计基准要求的条件，鉴定的基准应当记录在案。原子能机构《安全标准丛书》第 SSG-69 号《核装置设备鉴定》[18]提供了关于设备鉴定的建议。

4.47. 鉴定计划应当涉及影响系统或部件是否适合履行预期安全功能的所有专题，包括以下各项：

(a) 系统和部件执行预期安全功能的适用性和正确性；
(b) 环境鉴定（包括抗辐射鉴定，如适用）；
(c) 抗震鉴定；
(d) 系统和部件电磁兼容性鉴定。

4.48. 鉴定应当以多种方法为基础，包括以下方法：

(a) 使用符合既定规范和标准的工程和制造流程；
(b) 可靠性的证明；

(c) 使用类似应用的运行经验；

(d) 设备试验；

(e) 分析以推断相关条件下的试验结果或运行经验；

(f) 老化分析（如适用）。

4.49. 应当在所有已安装安全重要结构、系统和部件与适用的鉴定证据之间建立可追溯性。这不仅包括部件本身的可追溯性，还包括试验配置和安装配置之间的可追溯性。

4.50. 设备鉴定计划应当证明竣工仪器仪表和控制系统以及安装的部件正确实施了鉴定的设计。

研究堆仪器仪表和控制系统的适用性和正确性

4.51. 对研究堆安全重要仪器仪表和控制系统及部件的设计应当满足设计基准和设备规范中包含的所有功能、性能和可靠性要求。功能需求的示例包括应用和支持系统的功能、设备可运行性和人机界面以及输入和输出范围。性能要求的示例包括准确性和响应时间。可靠性要求的示例包括故障安全行为、符合单一故障标准、独立性、故障检测、可维护性和使用寿命。

研究堆仪器仪表和控制系统的设计中对内部和外部危害的考虑

4.52. 仪器仪表和控制系统及部件应当针对内部和外部危害及其可信组合（包括地震危害）进行保护，或应当进行设计和鉴定，以承受设计基准和安全分析中包含的内部和外部危害及其可信组合（包括地震危害）。

研究堆仪器仪表和控制系统的环境鉴定

4.53. 鉴定计划要求包括设备鉴定的环境条件（见 SSR-3[1]第 6.82 段）。环境条件包括温度、压力、湿度、化学品和辐射，以及在这些条件下可能影响部件正常运行的退化机制。要求对安全重要仪器仪表和控制系统的设计能够承受与正常运行、预计运行事件和设计基准事故相关的环境条件的影响，并在这些环境条件下运行（见 SSR-3[1]第 6.83 段）。

电磁兼容研究堆仪器仪表和控制系统的鉴定

4.54. 电气和电子系统和部件的可靠运行取决于它们与附近或与之连接的部件的电磁兼容性。电磁干扰可能由设施内部或外部的来源引起。示例包

括故障电流通过开关设备、断路器或保险丝的操作来清除，无线电发射机引起的电磁场，和自然资源如雷击和地磁感应电流。仪器仪表和控制系统及部件，包括相关电缆，应当设计、安装和试验以承受其电磁环境条件。

4.55. 在仪器仪表和控制系统及部件的设计中需要考虑的电磁干扰类型包括：

(a) 通过电缆发射和传导电磁干扰；

(b) 静电放电。

4.56. 仪器仪表和控制系统及部件的电磁兼容性鉴定取决于系统和部件设计措施的组合，以最大限度地减少电磁噪声与电气部件的耦合。应当进行试验以证明系统和部件能够承受预期水平的电磁辐射，并证明其自身的电磁辐射在可容忍水平范围内。已经鉴定的仪器仪表和控制系统及部件应当附有相应的鉴定证书。

4.57. 研究堆使用的无线系统和设备的电磁辐射特征，以及用于维护、维护和测量设备的电磁辐射特征都应当予以考虑。这种无线系统和设备可以包括移动电话、无线电发射机和接收机以及无线数据通信网络。电磁辐射试验应当适用于对安全重要和非安全重要的系统和部件。

4.58. 设施中的任何电气或电子设备都会对电磁环境产生影响。应当评价所有设备－不仅仅是安全重要设备－电磁辐射的贡献，以及这种辐射对安全重要仪器仪表和控制系统性能的影响。

4.59. 包括相关电缆在内的设备和系统的设计、安装和鉴定应当适当限制电磁干扰向研究堆设备的传播（通过辐射和传导）。应当特别考虑设备汇聚的区域（如安全壳贯穿件、电机控制中心、开关设备区域、电缆传导室、控制室）。应当参考电磁辐射的国家和国际行业标准。

研究堆仪器仪表和控制系统的试验和可试验性

4.60. 研究堆仪器仪表和控制系统的试验安排包括与试验设备的接口、安装的试验设备以及内置的试验设施和程序。安全重要仪器仪表和控制系统的设计需要包括能够进行定期试验的规定（参见 SSR-3[1]要求 31 和 51）。理想情况下，试验应当可以在反应堆运行期间进行，或者，如果正当的话，

只能在关闭期间进行。许多研究堆的运行周期相对较短，因此，对于这种研究堆来说，运行期间的试验规定可能是不必要的。SSG-81[3]提供了关于研究堆定期试验的建议。

研究堆仪器仪表和控制系统的试验规定

4.61. 对安全具有重要意义的仪器仪表和控制系统及部件的试验规定应当包括以下内容：

(a) 试验规定应当有适当的试验接口和状态指示。试验接口应当包括引入模拟过程条件或电信号的能力。

(b) 试验规定的运行方式应当使设备中的任何故障都易于检测。

(c) 这些系统应当具有防止未经授权访问的功能。

(d) 系统的位置应当使试验设备和待试验部件易于接近。

(e) 系统的位置应当确保试验或进入试验场所不会使运行人员暴露在危害的环境条件下。如果要试验的设备位于危害区域，在设计中应当考虑从危害区域之外进行试验的规定。

(f) 这些系统应当有必要的通信设施来支持试验。

4.62. 在设计中应当确保系统不会不知不觉地留在试验配置中。控制室中应当指示安全系统部件或通道的不可运行性或旁路。对于经常绕过的物项，此类指示应当是自动通知的。

4.63. 在可行的情况下，要求使用安全重要仪器仪表和控制系统的自检功能（见 SSR-3[1]第 6.183 段）。为了满足这一要求，有必要在提供自检功能和简化设计的需要之间取得平衡（见第 4.2 段）。

4.64. 内置试验设备本身应当能够定期检查，以确保持续正确运行。

试验期间仪器仪表控制功能的保存

4.65. 研究堆仪器仪表和控制系统的试验应当不损害安全功能的性能，也应当不引入共因故障的可能性。在试验对运行过程中安全重要系统之前，应当考虑安全方面。

4.66. 永久连接到安全系统的试验设施应当被视为安全系统的一部分。已安装的试验设施应当定期对照另一个校准源进行独立试验。

研究堆仪器仪表和控制系统的试验考虑

4.67. 在研究堆试验仪器仪表和控制系统时应当考虑以下因素：

(a) 定位和安装传感器，使其试验和校准最好能在其所在地进行，包括在适用的情况下用于排水、干燥、去污、隔离和通风设备的传感器；

(b) 将试验设备和试验装备放置在有足够空间和方便被试验设备的地方；

(c) 确保试验期间运行人员的安全，包括采取措施切断设备电源并防止其意外使用；

(d) 确保部件状态指示和试验连接的便利性。

4.68. 通信设备是支持研究堆仪器仪表和控制系统试验所必需的。安全重要仪器仪表和控制系统的设计应当包括自动警报（例如通过使用警报器）运行人员通道或部件处于试验模式的规定。

4.69. 当试验安全系统的通道时，安全功能的性能应当不受到损坏。特别是仍应当满足单一故障标准。例如，考虑到系统中实施的保护逻辑，被试验的安全系统的通道应当在试验期间处于跳堆状态。

4.70. 应当考虑仪器仪表和控制系统试验可能对安全分析中假设产生的任何影响。

4.71. 在对安全系统进行在线试验之前，应当考虑行政控制。

研究堆仪器仪表和控制系统试验计划

4.72. 仪器仪表和控制系统的设计应当包括试验和校准程序的规范。试验和校准的范围和频率应当符合功能要求和可用性要求（另见 SSR-3[1]第 7.72 段）。在确定试验频率时，应当考虑所选仪器仪表的必要精度和稳定性。具有低漂移的稳定仪器仪表可能需要较少的试验频率。

4.73. 试验计划应当包括以下内容：

(a) 计划目标说明；

(b) 待试验系统和通道的标识；

(c) 主试验时间表；

(d) 进行试验的原因和正当性以及试验间隔；

(e) 试验文件和报告的描述；

(f) 定期评审计划有效性的安排；

(g) 在进行试验时使用的单一试验程序的规范。

4.74. 试验计划中规定的试验应当通过明确的程序确保在试验期间和试验完成后证明以下各项：

(a) 系统的整体功能能力没有退化。

(b) 仪器仪表和控制系统继续满足其性能和可靠性的设计基准要求。

(c) 仪器仪表和控制系统正确恢复运行。

4.75. 试验程序应当将试验安排成一个顺序，以便可以评定被试验系统或部件的整体状况，而尽可能不进一步试验其他部件或系统。

4.76. 试验计划应当规定仪器仪表和控制系统的定期试验和校准过程，其目标如下：

(a) 规定对从传感器到致动器的所有特定功能的检查，这些功能能够在现场以最少的努力进行；

(b) 通过记录显示符合公差要求的试验结果，确认满足设计基准的功能要求和性能要求 [4]；

(c) 试验所有输入和输出功能，如警报、指示器、控制行动和驱动设备的操作；

(d) 提供维护后试验，以确保系统正确恢复运行；

(e) 确保研究堆在试验期间的安全；

(f) 最大限度地减少虚假启动任何安全行动的可能性，并最大限度地减少试验对研究堆的安全和可用性的任何其他不利影响。

4.77. 试验计划的实施应当不导致任何系统或部件的任何损坏。

4.78. 如果设备的临时连接是定期试验或校准所必需的，则应当通过警报和/或警告灯提醒反应堆运行人员存在临时连接，并且此类设备的使用应当受到适当的行政控制。

---

[4] 试验响应时间的要求必须严格基于安全分析报告中的假设，并必须限于涉及试验响应时间的特殊考虑的参数，因为这些参数的及时响应对设施的安全很重要。

4.79. 不允许为试验目的临时修改仪器仪表和控制系统中的计算机程序。

4.80. 设备停止使用的时间间隔应当最小化，每个传感器应当尽可能单独试验。

4.81. 安全系统通道的试验最好是单一的在线试验。当单一的在线试验不可行时，试验程序可以将重叠的试验组合起来以达到试验目标。对于安全系统通道的试验，应当提供使用重叠试验的文件正当性。

4.82. 安全系统的试验应当独立确认 (a) 传感设备的每个通道；和 (b) 指挥、执行和支持功能的功能要求和性能要求。

4.83. 安全系统的试验应当包括尽可能多的被试验功能（包括传感器和致动器），并适当考虑过度试验时致动器的磨损。

4.84. 只要有可能，安全系统的试验应当在实际或模拟的服务条件下完成，包括运行顺序。在试验特别敏感的安全系统时应当采取预防措施。

4.85. 试验失败后，在重新试验的结果可用于证明系统或相关部件的可运行性之前，应当评价并记录失败的原因、根本原因以及随后采取的措施。

4.86. 纠正措施可能包括，例如，部件的维护或维修，或试验程序的修订。如果确定纠正措施是不必要的，应当记录原因。

研究堆仪器仪表和控制系统的可维护性

4.87. 设计中需要考虑仪器仪表和控制系统的维护规定（见 SSR-3[1]要求 31）。这个仪器仪表和控制系统的设计应当包括所有系统和部件的维护计划。

4.88. 仪器仪表和控制系统及部件的设计应当避免维护人员的不当照射（见 SSR-3[1]第 6.88 段）。营运组织还需要确保与非辐射相关的风险尽可能低（见 SSR-3[1]要求 80）。该设计还应当便于预防性维护、故障排除和及时维护。

4.89. 为便利仪器仪表和控制系统的维护、故障排除和维修而采取的设计措施包括：

(a) 避免将设备放置在极端温度、极端湿度或高水平放射性的区域；

(b) 在执行维护活动时考虑人因；

(c) 在设备周围留出足够的空间，以确保维护人员能够使用必要的工具执行任务；

(d) 提供试验面板、仪器仪表隔离和试验连接。

4.90. 为如果部件必须位于难以接近的区域，则应当考虑其他设计措施，例如：

(a) 在冷或热备用状态下安装备用冗余设备；

(b) 提供远程更换、维护和恢复服务的设施。

研究堆仪器仪表和控制系统的安全评定

4.91. 需要安全分析来支持新仪器仪表和控制系统的设计或现有系统的改造（见 SSR-3[1]要求 41）。应当进行下列活动，以确认仪器仪表和控制系统符合其设计基准：

(a) 确认所有已知和可预测的故障模式都是自我显示的或可通过计划试验检测到的，并且系统是故障安全的，视情况而定。

(b) 核实整个仪器仪表和控制系统支持在研究堆应用纵深防御概念。

(c) 核实对安全重要仪器仪表和控制系统共因故障的脆弱性是已知的，并已得到充分解决。共因故障的漏洞可以通过消除漏洞、通过提供实现共因故障安全功能的不同方法或通过证明接受漏洞来处理。

(d) 核实是否满足设计基准可靠性要求。这种核实可以基于确定性标准和定量可靠性分析，其中考虑了设计特点，如冗余和可试验性、故障模式、平均故障间隔时间和鉴定的严格性。对于复杂的系统，通常需要结合定性分析、定量分析和试验来核实是否符合设计基准可靠性要求。

(e) 核实仪器仪表和控制系统的设计包括足够的试验规定。

(f) 确定系统可用性，并确保作为安全系统一部分的试验设施被视为永久安装的试验设备。

(g) 仪器仪表和控制系统各种运行模式功能要求的确认。这种确认将包括在调试期间、当设施不在正常工况下运行时的第一次启动期间（例如，由于新堆芯的低通量而跳堆之后）以及在正常运行期间（包括在执行

试验之后的电源中断和再接通（或重启）之后）对正确系统行为的分析。

(h) 核实自动控制系统故障的影响不会超过为预计运行事件建立的验收标准。

4.92. 进行的任何安全分析的方法都应当详细说明，并应当记录在案，同时记录分析的输入、结果和分析本身的细节。应当使用可追溯性分析来确认实施和核实要求。为分析所做的每一个假设都应当是正当的，并且这种正当性应当被记录下来。

4.93. SSG-20（Rev.1）[9]提供了关于研究堆安全评定的进一步建议。

研究堆仪器仪表和控制系统安全系统设置

4.94. 研究堆设计中确定的运行限值和条件应当包括仪器仪表和控制系统的安全系统设置。SSG-83[5]提供了关于研究堆运行限值和条件的建议。

4.95. 在确定作为安全系统的仪器仪表和控制系统的设置时，通常会考虑以下因素：

(a) 安全限值：对某些运行参数的限值，在此范围内研究堆的运行被证明是安全的。

(b) （安全系统设置的）分析限值：由安全分析确定的测量或计算变量的限值，以确保不超过安全限值。

(c) 允许值：安全系统设置的限值，超过该值需要采取适当的措施。特定安全系统设置的允许值是在定期试验相应通道时发生跳堆是可接受的值。如果发现启动保护措施的点超出了允许值，应当采取纠正措施。

图 2 说明了这些术语与建立安全系统设置时通常考虑的测量不确定性类型之间的关系。

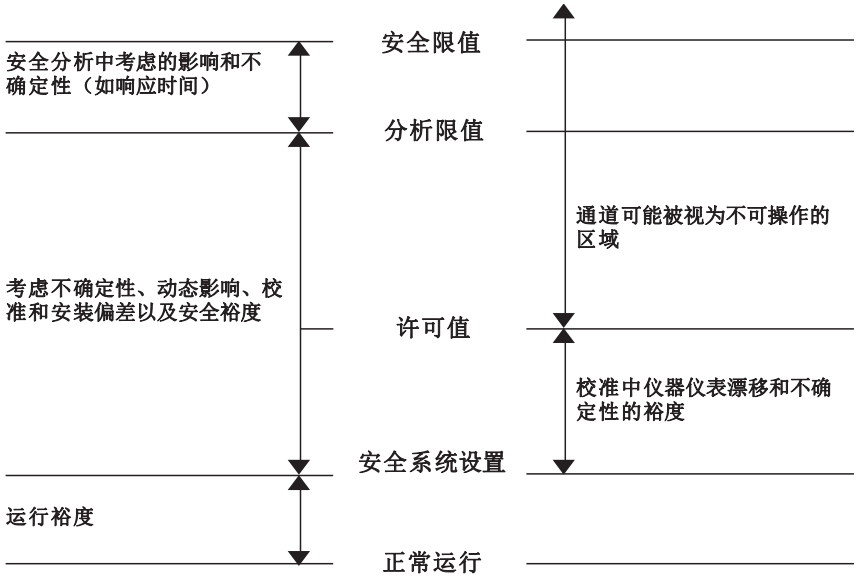

图 2. 确定安全系统设置时要考虑的安全系统设置术语和不确定性。

研究堆安全重要仪器仪表和控制系统的识别和核实

4.96. 仪器仪表和控制系统的安全分级要求主要基于确定性安全分析，并酌情辅以概率安全评定（见 SSR-3[1]第 6.29 段）。这应当得到专家提供的工程判断的支持，包括来自研究堆设计组织和营运组织知识渊博的人员。

4.97. 在研究堆寿命的整个设计、建造、安装、调试和运行阶段，以及控制、显示和指示的标识过程中，应当确定并遵循一致和连贯的命名和识别所有仪器仪表和控制部件的方法。应当明确标识部件，以降低无意中安装、改造、维护、试验、维修或校准不正确部件的可能性。安装在设备或部件中的部件或模块本身可能不需要标识。

研究堆设计扩展工况下仪器仪表和控制系统的设计

4.98. SSR-3[1]第 6.65 段指出：

> “设计扩展工况必须用于界定安全特点的设计规范和安全重要所有其他物项的设计规范，这些设计规范是防止此类工况发生或在发生时控制此类工况并缓解其后果所必需的。”

4.99. 作为设计扩展工况下的额外安全功能而提供的仪器仪表和控制系统及设备应当满足可靠性、可试验性、可维护性、可视察性、老化管理和（在可行的范围内）设备鉴定的设计要求。这种系统被认为是安全重要物项。

5. 研究堆专用仪器仪表和控制系统设计导则

研究堆仪器仪表和控制系统传感设备

5.1. 研究堆变量的测量应当符合设计基准的要求。这些测量包括检测范围内变量的现值和检测离散状态，例如由限位开关或开关（例如温度、压力、流量或液位限位开关、主电源可用性开关或控制系统运行开关、联锁开关）检测的离散状态。

5.2. 可以直接或间接地进行变量的测量，例如通过执行多次测量或通过测量与所需变量具有已知关系的其他数据来计算值。在可行的范围内，应当通过直接测量来监控反应堆工况，而不是通过间接测量来推断。

5.3. 每个被监控变量的传感器及其范围应当根据正常运行和事故工况下监控变量所需的精度、响应时间和范围来选择。

5.4. 应当确定传感设备易受共因故障（如辐射监控器饱和）影响的脆弱性，因为它们有可能使反应堆运行人员无法获得控制和缓解事故状况所需的信息和参数。

5.5. 如果需要一个以上的传感器来覆盖被监控反应堆参数的整个值范围，则一个传感器之间的合理重叠量应当提供给另一个传感器。例如包括中子通量监控器的源范围、中间范围和功率范围。

5.6. 如果监控变量具有空间相关性（即，如果参数的测量值取决于传感器的位置），则应当在设计中确定传感器（如流量测量元件）的最小数量和位置并加以证明。还需要对最终位置进行试验，以核实设计假设，并确定是否应当重新评定相关的设定点、限值条件和允许值。

反应堆保护系统

5.7. SSR-3[1]要求 50 规定：“**必须为研究堆提供一个保护系统，以启动自动动作，启动实现和维持安全状态所需的安全系统。**”该系统的设计需要包括实现和维持安全状态的规定，即使主反应堆保护系统遭受可信的共因故障，例如硬件故障、人因故障（见 SSR-3[1]第 6.177 段）。

5.8. 在适用的情况下，反应堆保护系统应当符合本仪器仪表和控制系统设计安全导则第 4 部分提供的建议。

5.9. 反应堆保护系统至少应当包括启动反应堆停堆的功能。对于次临界组件，停堆可以通过撤出中子源来实现。反应堆保护系统还可以提供其他安全功能，例如启动应急堆芯冷却和密封（反应堆保护系统的特点因此充当仪器仪表和控制系统的扩展工程安全特点）。

5.10. 要求反应堆保护系统能够在短时间内对所有假想始发事件进行自动响应，而无需手动操作（见 SSR-3[1]第 6.173 段和第 6.174 段）。

5.11. 作为纵深防御的一部分，为了应对主反应堆保护系统的潜在共模故障，应当评价和评定是否需要具有主反应堆保护系统的全部或部分功能的第二反应堆保护系统。如果提供两个反应堆保护系统，这两个系统应当相互独立和不同。

5.12. 反应堆保护系统启动动作应当闭锁，以便一旦启动，即使启动状态终止，该动作也将持续到完成（见 SSR-3[1]第 6.174 段）。由保护系统启动动作的闭锁通常在反应堆设备的致动信号水平上实施，并且这种动作应当不将系统的可靠性降低到可接受的水平以下。

5.13. 在某些情况下，如果诊断简单且动作明确，例如如下所述，启动保护动作的手动动作可能就足够了：

(a) 反应堆运行人员有足够和清晰的信息来对启动必要安全措施的必要性做出有效的判断。
(b) 反应堆运行人员有足够的时间评价研究堆的状态并完成必要的行动。
(b) 反应堆运行人员被提供足够的反应堆控制手段来执行必要的行动。

5.14. 除了自动动作外，还应当提供手动启动反应堆跳堆和反应堆保护系统的任何其他安全动作的手段。这种手动动作应当尽可能接近最终致动设备（如反应堆跳堆断路器），而不是反应堆保护系统逻辑的输入。

5.15. 抑制反应堆保护系统跳堆的系统功能，包括启动和停用这些功能的设备，应当是反应堆保护系统的一部分。有时，有必要抑制反应堆保护系统的作用，以改变反应堆工况。例如，在启动期间限制反应堆功率的跳堆必须在某个点被抑制，以提升功率。另一个示例是，在研究堆脉冲运行工况下，必须抑制某些行动。在本“安全导则”，反应堆保护系统的这种抑制功能被称为运行联锁，并被归类为安全系统的部件和/或功能。当不满足适用的启用条件时，反应堆保护系统应当防止启用运行联锁。如果运行被禁止并且工况改变使得这不再是允许的，反应堆保护系统应当自动禁用运行联锁或启动适当的保护运行（另见 SSR-3[1]第 6.175 段）。

5.16. 如果为了定期试验或校准反应堆保护系统而需要临时连接设备，则应当通过以下方式提醒运行人员临时连接存在的警报和/或警示灯，以及此类设备的使用应当受到适当的联锁或行政控制，以确保在使用后将其拆除。

5.17. 设计应当确保安全系统设置可以在启动点和安全限值之间建立一个裕度，在该裕度中，反应堆保护系统启动的行动将能够在达到安全限值之前控制过程。此外，在选择这种差值时应当考虑到以下因素：

(a) 仪器仪表不准确；
(b) 校准的不确定性；
(a) 仪器仪表漂移；
(a) 仪器仪表和系统响应时间；

5.18. 如果基于计算机系统拟用于反应堆保护系统，则需要系统地记录系统的寿期（见 SSR-3[1]第 6.180 (b) 段），并应当应用独立的核实和验证过程。

5.19. 应当考虑确保实施保护行动的各种手段。可通过以下方式提供多样性：

(a) 在反应堆保护系统本身内或通过一个单独和独立的系统，但须符合设计基准；
(b) 通过使用不同技术的不同系统，该系统可以是硬连线的或基于计算机的，只要足够的多样性是正当的。

5.20. SSR-3[1]第 6.180 (c) 段指出：

> “为了确认基于计算机系统可靠性，必须由独立于设计人员和供应商的专家进行系统的、完整记录的和经过评审的评定。”

5.21. 对于基于计算机的反应堆保护系统和部件，设计需要包括计算机安保特点（见 SSR-3[1]第 6.180 (d) 段和本“安全导则”的第 4.37－4.45 段）。

研究堆的安全重要其他仪器仪表和控制系统

5.22. 应当为反应堆运行人员提供足够的仪器仪表，用于在正常运行（包括停堆、换料和维护）和事故工况下监控反应堆系统的运行，包括记录安全重要所有参数。

5.23. 在设计中应当考虑到需要合适的启动中子源和专用的启动仪器仪表。

5.24. 营运组织应当为研究堆安全运行所必需的仪器仪表和控制系统的正常运行制定一套设计要求和限值。这些设计要求和限值应当解决以下问题：

(a) 建立安全限值和安全系统设置所需的信息；
(b) 对过程变量和其他重要参数的控制系统约束和过程约束；
(c) 维护、试验和视察研究堆，以确保系统、结构和部件按预计运行；
(d) 明确定义的运行配置，包括安全系统关闭时的运行限值；
(e) 研究相关任务的考虑。

这些设计要求和限值是建立研究堆授权运行的运行限值和条件的基础。

研究堆控制室的设计

5.25. 在研究堆的主控制室中，需要采取措施保护居留人员免受危害工况的影响（见 SSR-3[1]第 6.185 段）。对于辅助控制室（见 SSR-3[1]要求 54）和运行人员需要监控和控制研究堆系统的其他区域，也应当做出类似的规定。在所有这些地点，目标应当是确保工作环境条件令人满意。

5.26. 控制室的设计需要考虑人机工程学原则和人因（见 SSR-3[1]第 6.104 段）。在控制室的设计中也应当考虑任务分析的结果。

5.27. 为了满足 SSR-3[1]要求 39，控制室的设计应当包括防止未经授权的进入和使用的充分规定。

5.28. 主控制室的设计和建造必须能够抵御可能影响其持续运行的内部和外部危害，特别是火灾（见 SSR-3[1]第 6.185 段和第 6.186 段）。至少应当设计和建造一个控制室（主控制室或辅助控制室），以抵御设计基准地震。

研究堆主控制室

5.29. 安全行动和安全相关控制行动的主要地点是主控制室。SSR-3[1]要求 53 规定：

> **“研究堆设施必须设置控制室，使该设施能够在所有运行状态下自动或手动安全运行，并可采取措施使研究堆保持在安全状态，或在预计运行事件和事故工况发生后使其恢复到安全状态。”**

研究堆辅助控制室

5.30. 如果安全分析确定了可能抑制反应堆运行人员从主控制室关闭反应堆并将其保持在安全工况下能力的事件，则应当提供反应堆停堆的远程能力。如果反应堆运行人员需要执行安全措施，并且安全分析确定了主控制室可能不可用或主控制室的操作可能被禁止的事件，则应当提供辅助控制室或应急控制台。可能抑制反应堆运行人员从控制室关闭反应堆能力的事件包括，例如，控制室中的火灾或影响控制室和研究堆中其他地方的设备之间连接位置中的火灾。

5.31. 辅助控制室的仪器仪表和控制系统必须适本地独立于主控制室（见 SSR-3[1]要求 54），以避免降低辅助控制室系统可运行性的共因故障。例如，控制系统网络的设计应当确保无法从两个控制室中的任何一个使用系统的可能性极低。另一个示例是控制室电源的分离。

5.32. 应当考虑在主控制室外设置适当的设施，以便将反应堆的优先控制权转移到新的地点，并在主控制室中的设备被废弃时进行隔离。

研究堆辐照设备和实验设备控制系统

5.33 在许多研究堆中，有用于辐照设施和实验设备的专用控制台，它们可能位于主控制室或其他房间。实验设备的运行人员应当与反应堆运行人员保持通信联系，以分享关于实验和反应堆状态的信息，并使彼此了解预期的行动（例如需要关闭反应堆的情况）。

5.34. 如果安全分析确定的事件表明，辐照设施和实验设备需要独立的仪器仪表和控制系统，以确保在功能上与研究堆的其他活动隔离，则辐照设施和实验设备的控制台应当专门用于这些辐照设施和实验设备。

5.35. 警报系统应当涵盖对反应堆运行重要的参数。不涉及反应堆安全问题的实验设备的警报器应当与反应堆警报器功能隔离。

研究堆语音通信系统

5.36. 要求在主控制室和辅助控制室（如适用）与急救中心之间提供通信系统（见 SSR-3[1]第 6.185 段和第 6.91 段）。还应当提供与设施内其他地点的安全通信手段，包括与实验设备和相关设施的运行人员以及与场外响应组织的通信。

5.37. 主控制室和辅助控制室都应当具有至少两条不同的通信线路，其中包括：

(a) 在预计运行事件和事故工况下需要通信的现场位置；
(b) 场外应急响应组织；
(c) 可能受研究堆运行影响的其他设施。

这些通信线路的路由应当确保它们不会受到丧失主通信线路的影响，无论这种丧失的原因是什么（包括外部事件），并且它们应当能够独立于研究堆电源和场外电源运行。

5.38. SSR-3[1]第 6.189 段要求从控制室向相关应急响应设施提供相关信息和通信手段。还要求向应急设施提供来自研究堆外部来源的环境监控信息。要求信息和通信线路设计为在事故工况下运行（见 SSR-3[1]第 7.93 段）。

研究堆火灾探测系统和消防系统

5.39. SSR-3[1]要求 61 规定：

> **“研究堆设施的消防系统，包括火灾探测系统和消防系统……必须在整个研究堆设施中提供，并适当考虑到火灾危害分析的结果。”**

火灾警报系统的性质、布局、必要的响应时间及其探测器的特征应当在火灾危害分析的基础上确定。火灾探测系统应当在火灾特定位置的控制室中通过声音和视觉火警发出警告。

5.40. 适当时，还应当在设施中通常有人居住的区域提供本地的声音和视觉火警。火警应当与众不同，以避免与设施中的任何其他警报混淆。

5.41. 火灾探测和警报系统必须随时运行（见 SSR-3[1]第 6.207 段），并应当提供不间断应急电源，包括必要时的防火电缆。

5.42. 火灾探测器的位置应当确保污染控制所需的通风或压差导致的气流不会导致烟雾或热能从探测器中流出，从而过度延迟探测器警报的启动。

5.43. 如果环境不允许在受保护的区域放置探测器（例如，由于放射性水平增加或温度过高），则应当考虑其他方法，例如通过自动操作的远程探测器对气体大气进行采样。

5.44. 当消防泵、喷淋系统、通风设备、防火阀和相应的电源等物项由火灾探测系统控制或使用时，以及当虚假驱动会对研究堆和现场人员造成损害时，操作应当由串联运行两种不同的火灾探测手段控制。如果证实是虚假的，设计应当允许系统停止运行。还应当考虑系统的虚假驱动对研究堆的潜在影响，例如，对于包含电力系统、仪器仪表和控制系统的房间，气体抑制系统可能是喷淋消防系统的良好替代方案。

5.45. 火灾探测系统、警报系统和驱动系统的接线应当采取以下措施：

(a) 应当通过选择适当的电缆类型、适当的布线或其他方式来保护布线免受火灾的影响。
(b) 应当保护线路免受机械损坏。
(c) 应当持续监控布线的完整性和功能性。

5.46. 应当定期试验火灾探测系统和消防系统。

5.47. 国家消防要求也应当被用作火灾探测系统和消防系统设计的输入。

研究堆仪器仪表和控制系统的电力供应

5.48. 仪器仪表和控制系统的电源（见 SSR-3[1]要求 56）应当进行分类和鉴定，并应当包括可靠性、隔离性、可试验性、可维护性和停止使用指示的规定，这些规定应当与它们所服务的仪器仪表和控制系统的设计基准一致。此外，应当考虑这些电源的故障模式。

5.49. 需要在运行状态和/或事故工况下随时可用的仪器仪表和控制系统需要连接到不间断电源（见 SSR-3[1]第 6.191 段）。这种电源应当在系统设计基准规定的公差范围内为仪器仪表和控制系统提供电力。应当为仪器仪表和控制系统规定这些公差，以确保系统能够承受正常电源故障以及由外部事件引起的设施停电。

5.50. 电源可以为电磁干扰提供传输路径，电磁干扰可能来自仪器仪表和控制系统外部，或者可能来自直接或间接连接到同一电源的其他仪器仪表和控制系统。这种干扰的来源包括与同一电源上的其他设备相关的电气故障清除。应当分析并尽可能避免这些干扰。

6. 研究堆的仪器仪表及控制系统的运行

研究堆仪器仪表和控制系统及运行限值和条件

6.1. SSR-3[1]要求 71 规定：**“研究堆设施的营运组织应当确保研究堆按照运行限值和条件运行。”**

6.2. 研究堆仪器仪表和控制系统有助于确保反应堆的运行参数保持在运行限值和条件内。SSG-83[5]提供了关于研究堆运行限值和条件的建议。

研究堆安全限值

6.3. 研究堆仪器仪表和控制系统应当能够防止在运行状态、设计基准事故和设计扩展工况下超过安全限值。

研究堆安全系统设置

6.4. 每个参数都需要一个分析限值（见第 4.95 段）来启动安全系统，任何其他安全重要相关参数都应当由仪器仪表和控制系统监控。在适当的情况下，系统应当提供一个可用于自动防止该参数超过设定限值的信号。

研究堆安全运行限值和条件

6.5. 正常运行值和安全系统设置之间的可接受裕度应当应用于仪器仪表和控制系统，以确保反应堆的安全运行，同时避免安全系统的频繁启动。可接受的裕度应当考虑仪器仪表精度、系统响应时间、测量信号的预期漂移和允许误差裕度，以及正常运行中的所有预期变化。

研究堆安全重要仪器仪表和控制系统进入的控制

6.6. SSR-3[1]要求 39 规定：**“必须防止未经授权接触或干扰对研究堆设施安全重要的物项，包括计算机硬件和软件。”**应当采取所有合理的预防措施，防止人员在进入仪器仪表和控制系统或在仪器仪表和控制系统上执行任务时执行可能危及安全的未经授权的操作。

6.7. 应当控制安全重要仪器仪表和控制系统的进入。访问控制方法应当包括实物的限制或障碍、特殊嵌入式设备，以及通过硬件或软件访问键、访问警报和行政控制对安全重要功能的访问限制。

6.8. 在任何配置安全系统设置的地方，只有经过授权的人员才能更改这些设置，并且应当检查这些设置的完整性。应当通过实物和行政手段限制对安全系统设置和校准调整的访问。

6.9. 仪器仪表和控制系统中基于计算机部件的保护需要在考虑到国家要求的适当安保程序中解决。参考文献[15－17]提供了计算机安保导则。

6.10. 应当使用安全的存储安排和程序控制，以确保只有授权的软件版本才能上传到研究堆仪器仪表和控制系统及设备中。软件版本的记录应当保存在研究堆的管理系统中。基于计算机系统在重新投入使用之前，应当证明其正确的性能。

6.11. 应当禁止从反应堆外部通过网络连接以电子方式访问对安全重要计算机系统的软件和数据。

6.12. 应当使用访问控制方法来确保用户只能访问他们已被授权的数据和命令。

6.13. 应当实施适当的措施来防止未经授权访问软件、使用或损坏软件或数据、引入恶意代码、未经授权连接外部网络或其他基于计算机的攻击。

研究堆仪器仪表和控制系统维护、定期试验和视察

6.14. 需要安全重要仪器仪表和控制系统进行维护、定期试验和视察，以确保其所有部件的功能符合设计要求和意图并符合运行限值和条件（见SSR-3[1]第 7.68 段）。此类活动的频率必须符合此类系统或部件的可靠性要求（见 SSR-3[1]第 7.72 段）。SSG-81[3]提供了进一步的建议。

6.15. 研究堆仪器仪表和控制系统应当便于定期试验，并在适用的情况下包括在线试验功能，以减少连接器的插入和拔出次数，从而提高系统的可靠性。

仪表和控制系统用于试验或维护停止使用的规定

6.16. 除非能够充分证明系统可接受的可靠运行，否则任何单一安全系统、部件或通道的停止使用应当不导致所需的最小冗余损失。

6.17. 如果使用设备进行试验或维护会损坏仪器仪表和控制功能，接口应当进行硬件互锁，以确保在没有故意手动干预的情况下不可能与试验或维护系统进行交互。

6.18. 对于安全系统，设计特点应当确保在安全系统部分的定期试验期间，那些仍在使用的部分能够继续执行所需的安全功能。例如，在试验“三选两”逻辑时跳堆冗余会使系统处于“二选一”逻辑安排中。对安全系统可用性的行政控制应当使得这些系统在设计基准内运行。

研究堆的仪器仪表和控制系统在长期关闭期间

6.19. 营运组织应当评定和定义在长期关闭期间需要保持运行的安全重要最小仪器仪表和控制系统。

7. 研究堆人因工程和人机界面

7.1. 对于设计的每个方面，都需要将有效的人因工程流程嵌入到整体设计流程中（参见 SSR-3[1]要求 35）。应当确定适当的设计标准和导则，并在整个设计过程中使用。参考文献[19]提供了人因工程方面的导则。

7.2. 与人因工程相关的核实和验证活动应当在研究堆仪器仪表和控制系统的整个设计过程中进行，以确认设计充分适应当运行人员的所有必要行动和营运组织的所有相关行政安排。这种核实和验证可以包括任务分析和对诸如时间、人类认知和感知、运行人员过度疲劳和运行人员响应的可用指示等因素的考虑。

7.3. 如果仪器仪表和控制系统的一部分被改造，应当仔细考虑系统现代化部分的设计及其与现有系统的人员互动的兼容性。

研究堆人因工程和人机界面设计标准

7.4. 人机界面的设计应当考虑运行经验，以保留有用的功能并避免人因工程的问题。在新物项和改造物项的系统结构中，应当考虑这些设计因素。人机界面的设计应当强调人因和机器特点的重要性，并将两者都考虑在内。

7.5. 应当确定实现研究堆安全目标所需的仪器仪表和控制功能，履行这些功能所需的人力资源和系统资源应当按照规定的方法进行分配，并应当在设计阶段的系统结构中予以考虑。

7.6. 所有人机界面都应当按照人体工程学标准进行设计。营运组织应当确定使用常规显示器（如面板仪器仪表、警报器）最有效地显示哪些信息，使用视频屏幕最有效地显示哪些信息。在信息显示和控制的设计标准中，应当考虑运行人员的不同角色和授权访问级别，如反应堆运行人员、维护人员、系统管理员和在紧急情况下负责的人员。

7.7. 人机界面的设计要求应当根据界面支持的所有任务来规定，包括在正常运行期间以及在预计运行事件和事故工况下。所考虑的任务应当包括反应堆运行人员、维护人员、实验人员和在紧急情况下负有责任的人员所承担的任务。

7.8. 根据 SSR-3[1]要求 49，仪器仪表和控制系统需要提供必要的信息，以检测系统状态的变化，并为事故管理做出决策。人机界面必须包括必要的仪器仪表和控制系统，以评定研究堆在任何工况下的总体状态，确认自动安全行动按预期实施，并确定手动安全行动的必要性和时间（见 SSR-3[1]第 6.105 段）。

7.9. 在研究堆运行期间，当设施接近应当启用或禁用运行联锁的状态时，应当向反应堆运行人员提供适当的警告或警报。

7.10. 应当为反应堆运行人员提供足够的指示器和记录仪器仪表，以便能够在预计运行事件和事故工况期间和之后监控相关的反应堆参数。

7.11. 如果运行工况的变化可能影响安全，应当使用声音和视觉警报系统提供反应堆运行工况变化的早期指示。

7.12. 在设计人机界面时应当认真注意，以确保反应堆运行人员不会被大量数据淹没，这些数据可能因其固有的局限性而难以吸收人员的感知、认知和记忆。这对于设计警报器尤为重要。

7.13. 在仪器仪表和控制系统的设计中，应当适当考虑反应堆运行人员执行其预期任务所需的时间。

7.14. 仪器仪表和控制系统应当通过实施范围限制、联锁或跳堆来防止人为错误，以保护研究堆免受不安全运行的影响。

7.15. 在自动执行安全功能的情况下，仪器仪表和控制系统应当向反应堆运行人员提供必要的信息，以监控功能的性能。信息应当以反应堆运行人员能够有效监控的速度和详细程度提供。

7.16. 仪器仪表和控制系统应当提醒反应堆运行人员自动控制系统的故障。

7.17. 信息的介绍应当协调一致，以便于了解研究堆的状况和确保安全所必需的活动。

7.18. 研究堆内不同位置的人机界面的操作和外观应当一致，应当反映高度标准化，并应当与运行程序和向运行人员提供的培训相一致。

7.19. 人机界面应当包括显示记录信息的能力，这些信息将有助于反应堆运行人员识别模式和趋势，了解系统的过去或现在状态，或预测其未来进展。显示屏的设计应当确保冻结的显示屏易于识别。

研究堆控制室人因工程

7.20. 研究堆控制室的设计需要考虑人机工程学原则（见 SSR-3[1]第 6.104 段）。人因考虑因素，如工作量、人为错误的可能性，运行人员的响应时间并应当考虑尽量减少反应堆运行人员的体力和脑力劳动，以促进必要运行程序的执行，从而确保所有运行状态和事故工况下的安全。

7.21. 应当确保控制室中可接受的工作环境－就放射性水平、照明、温度、湿度、噪音、灰尘和振动而言－用于正常运行、预计运行事件和事故工况。主控制室的设计需要考虑内部危害（如火灾、烟雾、大气中的有毒物质）和外部危害（如地震、洪水、极端气象条件、人为错误造成的危害）导致的工况（见 SSR-3[1]第 6.185 段和第 6.186 段）。如果适用，也应当为辅助控制室提供类似的设施。

7.22. 在设计中应当考虑仪器仪表的布局和向运行人员提供信息的方式，包括研究堆状态和性能的充分总体概述，以及必要时关于特定系统或设备状态和性能的详细信息。

7.23. 主控制室中显示的信息应当允许反应堆运行人员实现以下目标：

(a) 采取没有自动控制的特定手动控制行动；
(b) 确认安全功能的可用性和自动安全行动的性能；
(c) 确定裂变产物屏障被破坏的可能性或探测这种破坏；
(d) 确认缓解事故状况或实现和保持安全状态所需的安全系统、辅助支持功能和其他系统的性能；
(e) 确定任何放射性排放的数量，并不断评定这种排放。

7.24. 如果辅助控制室不需要用于响应与主控制室相同范围的预计运行事件和事故工况，则辅助控制室中显示的参数可以不同于主控制室中显示的

参数。对于辅助控制室，需要有足够的仪器仪表和控制设备，以便在丧失执行能力的情况下主要控制室的基本安全功能，研究堆可以放置并保持在安全状态，余热可以排出，密封功能可以执行，基本设施参数可以监控（见SSR-3[1]第 6.188 段）。辅助控制室中的仪器仪表和控制设备应当与主控制室中的设备在实物和电气隔离。

8. 研究堆计算机系统和软件

8.1. SSR-3[1]要求 52 规定：

“如果对研究堆的安全重要系统依赖于基于计算机的设备，则必须在系统的整个寿命期间，特别是在整个软件开发周期内，为计算机硬件和软件的开发和试验制定和实施适当的标准和实践。”

8.2. 基于计算机系统对研究堆的安全越来越重要，因为它们在新旧设施中的使用越来越多。这种系统既用于安全相关的应用，例如过程控制系统和监控系统，也用于安全应用，例如反应堆保护系统。

8.3. SSR-3[1]第 6.184 段指出：

“对于安全系统和安全重要系统中基于计算机的设备：

……

(c) 设备的评定应当由独立于设计团队和供应商团队的专家进行，以保证其高可靠性。

(d) 当不能以高度的可信度证明设备必要的高可靠性时，应当提供确保履行安全功能的各种手段”。

基于计算机系统的可靠性应当根据系统的、完整记录的和评审的工程过程进行评价。这个过程应当包括对新软件和已有软件的评价。相关运行经验可用于评价现有软件。

8.4. 设计故障，包括软件故障，本质上是系统性的而不是随机的，因此需要考虑潜在的共因故障（见 SSR-3[1]第 6.184 (e) 段）。特别是应当系统地考虑采用冗余子系统的安全系统，这些子系统使用硬件和软件的相同副本。

8.5. 根据研究堆中实验设备的复杂程度，应当考虑为反应堆和实验配备独立的基于计算机的仪器仪表和控制系统。在这种情况下可以为每个系统提供自己的一套设计要求和目标。

8.6. 在基于计算机系统的设计和运行中应当考虑老化管理，以计划和管理使用寿命的缩短、制造来源的减少和材料短缺。

研究堆计算机系统和软件设计考虑

8.7. 对于基于计算机的安全系统，应当通过使用遵循正式软件开发寿期的结构化设计来避免系统功能和实现的复杂性。诸如“自上而下”分解、抽象层次和模块化结构等概念对于应对复杂性非常重要。系统模块化背后的逻辑和接口的定义应当尽可能简单。对于系统及其相关软件，应当采用“自上而下”的设计流程（即分解系统以深入了解其子系统），以便于评定是否实现了设计目标。

8.8. 关于研究堆的安全系统，计算机系统所满足的功能要求对于安全功能的实现都是必不可少的。应当隔离对非安全重要的功能，以避免对安全功能产生任何影响。

8.9. 当一个计算机系统包含两个或多个不同安全级别的部件时，该计算机系统应当满足更高安全级别的要求。

8.10. 在基于计算机系统设计的不同级别，应当考虑使用不同的功能和系统部件。

8.11. 系统故障安全功能、自我监视和容错机制应当纳入软件，但仅限于设计基准功能要求和性能要求证明额外复杂性正当的程度。故障检测和自我监视功能不应对计算机系统执行其安全功能的能力产生不利影响，也不会导致虚假操作。

8.12. SSR-3[1]第 6.184 (f) 段指出：

> “对于安全系统中基于计算机的设备和安全重要系统：……必须提供保护，防止系统运行受到意外干扰或故意干扰（安全重要基于计算机系统、通信和网络系统，包括反应堆保护系统，必须充分防止网络攻击，达到并包括设计基准威胁……）。

应当证明已经采取措施在基于计算机系统的整个寿期中保护其免受实物和计算机攻击、未经授权的访问、欺诈、计算机病毒和其他恶意威胁。安全系统应当不连接到外部网络。外部存储设备的连接应当被锁定，以防止未经授权的使用。

8.13. 研究堆中基于计算机系统应当设计为可维护性，以便于检测、定位和诊断潜在或实际故障，从而有效地修复或更换系统。具有模块化结构的软件可能更容易修复、评审和分析，因为设计可能更容易理解。软件的可维护性还包括对功能进行更改的概念。基于计算机系统的设计应当尽可能允许将更改限制在软件的一小部分。

8.14. 执行安全功能的基于计算机系统应当在功能和时间方面具有确定性行为，这意味着任何给定的输入序列在系统的规范范围内，总是在相同的响应时间内产生相同的输出。

8.15. 采样速率和处理速度应当符合精度和时序要求。

8.16. 安全重要数据通信通道应当满足第 4.21 段关于独立性的建议。设计应当确保检测到传输设备和数据通信设备的错误和故障，为运行人员提供适当的警报，并为性能分析做记录。

8.17. 研究堆的通信技术的选择和配置应当确保它能够在所有可能的数据加载条件下做出及时响应。

8.18. 应当适当考虑在数据通信中使用冗余。

8.19. 数据通信网络的拓扑和网络接口应当从电气和通信协议的角度来设计和实现，以避免独立系统或子系统的共因故障。

8.20. 除非安装了解耦设备并使用了解耦协议，否则应当避免数据从较低级别的安全系统流向较高级别的安全系统。

8.21. 在研究堆的计算机系统中选择预先开发的物项应当遵循一个明确和记录的过程，以确保其适用性。

8.22. 软件工具可用于支持仪器仪表和控制系统的寿期。应当根据可靠性要求、工具类型以及软件工具引入错误或无法检测现有错误的可能性来核实和评定这些工具。

研究堆计算机系统和软件项目计划

8.23. 研究堆中基于计算机系统和软件的项目开发过程应当详细计划，并应当提供明确的证据，证明该过程已被遵循，以促进安全重要系统的独立评定。开发计划应当确定和定义将用于特定项目的过程。应当考虑和计划的项目的其他方面是质量管理、核实和验证、配置管理、安装和调试。

8.24. 应当确定研究堆中基于计算机系统和软件开发过程的所有阶段。前几个阶段的设计活动应当为下一个阶段提供输入。应当在开发过程的每个阶段执行核实。

8.25. 应当确定开发过程中要使用的方法。方法的选择应当符合建立过程和程序的质量管理计划。质量管理计划应当在项目开始前准备和实施。软件质量管理计划应当在项目开始时可用。

研究堆计算机系统和软件的核实和验证

8.26. SSR-3[1]第 6.184 (g) 段指出：“对于安全系统和安全重要系统中基于计算机的设备：……应当对软件系统进行适当的核实、确认和试验。”应当执行核实和验证活动，以证明计算机系统实现了其总体安全目标和功能要求。特定技术和核实程序应当包括在核实和验证计划中。

8.27. 核实和验证计划应当包括列出和收集指导核实过程的适用规范和标准、程序和实践。

8.28. 执行核实和验证的团队应当独立于开发团队。独立性通常是通过对核实和验证团队以及开发团队进行不同的直线管理来确保的团队。执行核实和验证的人员应当不参与同一物项的设计。可以使用不同的组织来完成核实和验证活动。

8.29. 核实和验证计划应当包括一种机制，用于记录在分析过程中发现的所有不遵守情况，并确保通过经批准的变更控制过程妥善解决这些情况。

研究堆计算机系统和软件的配置管理

8.30. 与软件开发相关的所有物项，如编译器、开发工具、配置文件和操作系统，都应当接受配置管理。所有可识别的物项，如文档、软件部件或

数据结构，都应当有一个唯一的标识，包括版本号。这些物项应当包括开发的物项和正在重用或重新应用的现有物项。

8.31. 应当建立变更控制程序。本程序应当规定保存在研制过程中或研究堆运行过程中发现的需要对基于计算机系统或软件进行修改的任何问题的记录。该程序还应当包括以下文件：问题及其分析，受影响的物项，为解决问题而做出的变更，以及结果产生了哪些版本（例如软件的版本号、软件的部件）以及仪器仪表和控制系统的系统和部件的哪个基准数据库。变更控制程序应当规定批准变更的责任。

研究堆计算机系统和软件的配置管理

8.32. 研究堆计算机系统和软件的安装和调试计划应当包括以下内容：

(a) 将该系统适当并入研究堆的步骤顺序，以及安全引入新的或已改变的系统所需的相应设施状态；
(b) 在系统投入运行之前，与监管机构进行必要的互动，包括批准、待检点和报告；
(c) 调试试验案例和顺序以及确认系统在研究堆环境条件下正常运行所需的相应设施状态；
(d) 描述调试结果所需的记录和报告的描述。

研究堆计算机系统要求的规范

8.33. 研究堆计算机系统的规范至少应当包括计算机系统的必要功能特性和非功能特性。在规定功能要求时，应当使用安全分析（例如，基于假想始发事件和安全标准的设施安全分析、瞬态分析和事故分析）。与安全没有直接关系的其他要求，如可用性或安全要求，应当包括在设计的这一阶段。

8.34. 应对安全系统和安全相关系统进行安全分析，以确定这些系统的功能要求。

8.35. 非功能性需求的规范说明应当包括以下内容：

(a) 相关的可靠性属性，如系统的可靠性、可用性和安全性能；
(b) 基于计算机系统的安保要求，包括安保程序；

(c) 性能要求（例如，执行安全功能的响应时间）；

(d) 环境鉴定要求，如温度和辐射；

(e) 是否以及在何处需要进行实物分隔（例如，安全功能和控制功能之间的隔离）；

(f) 确认与非安全直接相关的要求（如可用性或安保要求）不会对执行安全功能的能力产生不利影响。

在开始项目的下一阶段之前，应当对这些要求进行准确和清晰的描述，并且这种描述应当接受独立的评审。

研究堆软件要求

8.36. 软件需求的规范应当定义每个单独的软件物项的功能，以及它将如何与系统的其他物项交互。研究堆软件要求应当完整、明确、一致、清晰，目标受众（如领域专家、安全工程师、软件设计人员）可以理解，并且可以核实和追踪。每个软件需求的来源都应当被充分地记录下来，以便于核实、确认和追溯到更高级别的文档，并证明所有的软件需求都已经得到满足。

8.37. 软件要求应当包括对软件的系统要求分配的说明，同时考虑到潜在的故障条件、每种运行模式的功能要求、性能标准、时间和限值、故障检测、事件记录、自我监视、安全监控以及与核安保的接口。

研究堆软件设计

8.38. 在研究堆安全重要系统软件中，应当在设计的各个层面避免不必要的复杂性。设计越简单就越容易实现和展示所有其他属性。拥有一个更简单的设计也给了软件被完全理解的更大信心。

8.39. 为了便于在整个设计过程中跟踪软件需求的符合性，每个设计元件－如软件模块、程序、子程序或文件－都应当有一个唯一的标识符。

8.40. 研究堆软件设计应当不包含矛盾和歧义。模块之间接口的描述应当是完整的。除了软件模块之间的内部接口之外，设计还应当明确指定软件的外部接口，例如硬件接口和库。设计及其描述应当证明每个软件设计要求都已得到满足，并应当能够核实实现相对于详细设计是正确的。

8.41. 软件设计的文档应当提供关于软件系统结构和所有软件模块的详细设计的技术信息，以及它们之间的交互，以证明它们的整体行为符合规定在所有可能的情况下。这些信息应当包括非功能性方面，如时间安排和资源使用情况。还应当具体说明实施方面的相关约束。

8.42. 软件结构中确定的每个软件模块都应当在详细设计中进行描述。可以使用图表和流程图，只要图表元素的含义定义明确。描述设计的常用技术包括数据流图和结构图或图形。

8.43. 评审应当在软件设计阶段进行，以避免潜在的错误并评定软件质量。

研究堆软件实施

8.44. 软件代码的产生应当可以根据软件设计需求进行核实。代码应当是可读的，充分的注释和可理解的。经过核实的软件工具可用于简化代码核实过程。

8.45. 在实施阶段，应当使用一个正式的系统来请求改变和控制对研究堆软件的修改，以处理遗漏和不一致。应当保留最新的修改记录，以备评审和监查。

8.46. 每个计算机程序的代码应当保持简单易懂，无论是一般结构还是细节。数据结构及其命名约定应当在整个基于计算机系统中统一使用。

研究堆软件的核实与分析

8.47. 核实与分析技术应用于提供软件质量保证以及符合仪器仪表和控制系统要求。

8.48. 软件核实计划应当记录以下内容：

(a) 将使用的核实技术；
(b) 应用每种技术所用程序的细节或参考文献，包括其范围和深度；
(c) 如何证明非功能性要求和约束得到满足；
(d) 确定何时进行了充分核实的标准，包括前一阶段产出的完整性目标和功能试验的结构覆盖率目标，以及如何证明这些目标；

(e) 记录结果的方法；

(f) 记录和解决不符合和错误的方法；

(g) 进行核实的小组及其与软件设计人员的独立性（见第 8.50 段）；

(h) 用于核实的任何软件工具的功能，包括对如何使用它的期望和限制（例如，领域、语言、过程）；

(i) 上述物项 (a) — (h) 中列出的每个要素的基本原理，以及核实对于所应用的安全级别系统中的软件来说有足够的正当性。

8.49. 应当制定一个软件试验计划，涵盖所有要做的试验，包括单元级试验、集成试验、工厂验收试验和装置试验。

8.50. 核实应当由独立于设计人员和开发人员的团队、个人或组织团体来执行。

8.51. 应当使用自动化软件工具对软件代码进行评审，以检查安全漏洞，并辅以对代码关键部分的人工评审（如输入输出处理、异常处理）。

8.52. 在软件代码核实期间，应当监控仪器仪表和控制系统的所有输出，并对任何偏离预期结果的情况进行调查和记录。

8.53. 核实结果相对于核实计划的任何不足之处（例如，就实现的试验覆盖率而言）都应当被记录并解决或证明。

8.54. 检测到的任何错误都应当进行原因分析，并应当通过商定的修改程序和回归试验进行纠正，以确保以前开发和试验的软件在修改后仍能正确运行。误差分析应当包括对仪器仪表和控制系统其他部分适用性的评价。

8.55. 应当保留异常数量和类型的记录。应当评审这些记录，以确定是否可以吸取任何教训，以及是否应当进行适当的流程改进。

8.56. 评审、视察或监查等技术应用于基于计算机系统和软件寿期所有阶段的核实。应当在核实计划中说明记录评审、视察或监查结果的方法，并说明所用方法的正当性。

8.57. 应当评审关于软件设计和软件实施的文档。软件试验案例应当只在功能的基础上设计（即不知道被测软件的结构），以保持试验活动的独立性，并能够分析设计后执行试验的结构覆盖。试验案例规范应当被充分记录和评审。

8.58. 试验计划的设计应当通过确保试验是可重复的并且涉及最少的人工干预来促进回归试验。

8.59. 应当评审试验性能中的任何异常工况，如果确定需要修改试验程序，应当应用适当的修改控制程序。

8.60. 软件试验性能中的任何异常都应当记录在一份报告中，该报告包括问题的性质、确定的纠正措施、重新试验安排和令人满意的重新试验确认。此外，还应当保持软件更正和软件构建的相互参照记录，以便对已安装软件进行配置管理。

研究堆软件的第三方评定

8.61. 研究堆安全系统软件的第三方评定应当与软件开发过程同时进行。

8.62. 这种第三方评定的目的是提供独立于系统和软件供应商以及营运组织的关于系统及其软件充分性的观点。此类评定可由监管机构或监管机构认可的机构进行。

8.63. 与软件创建者进行适当的安排以允许第三方评定是很重要的。

8.64. 评定应当包括对下列各项的评审：

(a) 开发过程（例如，通过质量保证监查和技术视察，包括检验寿期文件，如计划、软件设计要求和试验活动的全部范围）；
(b) 最终软件（例如，通过静态分析、视察、监查和试验），包括任何后续改造。

研究堆计算机系统集成

8.65. 集成到研究堆计算机系统中的软件版本应当是经过核实和验证的最新版本。

8.66. 计算机系统集成阶段应当包括至少三个连续的活动：软件试验，硬件试验和集成，以及软硬件集成。软硬件集成应当包括三个部分：将所有软件加载到硬件系统中，试验是否满足软硬件接口要求，以及试验所有软件是否能在软硬件集成环境下运行。

8.67. 在计算机系统的核实过程中，应当生成证据来证明系统集成已经过适当的检查和核实。作为核实的一部分，应当进行可追溯性分析并记录在案，以证明系统集成要求相对于计算机系统的设计规范是完整的。

研究堆综合计算机系统试验

8.68. 综合计算机系统试验应当在系统转移到研究堆并安装之前进行。最终的集成计算机系统试验通常与工厂验收试验相结合，形成一个单一的试验活动。

8.69. 在构建试验案例时，应当特别考虑以下内容：

(a) 涵盖硬件和软件的所有设计要求（包括健稳性试验和功能）；
(b) 覆盖输入信号的全部值范围；
(c) 异常处理（例如，当输入故障发生时可接受行为的演示）；
(d) 定时相关要求（如响应时间、输入信号扫描、同步）；
(e) 准确性；
(f) 所有接口（例如，系统集成中的硬件－软件接口、核实期间的外部接口）；
(g) 压力试验和负载试验；
(h) 安保要求（如记录用户活动）；
(i) 计算机系统的所有操作模式，包括模式之间的转换和电源故障后的恢复。

8.70. 应当进行可追溯性分析，以证明试验和评价的核实过程已经完成。

缓解与电厂内危害物质排放相关危害的后果

8.71. 应当进行核实和调试试验，以核实计算机系统已在研究堆正确连接，并确认系统的正确运行。

8.72. 核实和调试试验通常应当与现场验收试验相结合，现场验收试验包括对设备运行的核实。

8.73. 在调试过程中，应当保持对计算机系统（硬件和软件）的严格配置控制。所做的任何修改都应当遵循正式记录的修改流程。

8.74. 应当提供足够的文件来证明已安装的基于计算机系统和软件调试计划的充分性。

研究堆计算机系统和软件的运行、维护和改造

8.75. 关于研究堆计算机系统和软件的运行、维护和改造，应当考虑下列活动：

(a) 定期试验，以核实系统没有退化；
(b) 因为为增强或改变功能或纠正错误而进行的改造而进行的回归试验；
(c) 运行参数的变化；
(d) 诊断活动，例如执行特别诊断计划；
(e) 因故障更换硬件部件。

8.76. 软件开发、试验、安装、集成、运行和维护中使用的所有软件工具都应当鉴定。

8.77. 系统的寿期应当包括实施改造的过程。这个寿期应当包括开发的主要阶段，包括核实和验证。这些活动加上影响分析和回归试验将是必要的，以确保改造得到正确实施，没有引入新的错误。

8.78. 硬件部件出现故障后，纠正措施应当限于逐个更换硬件部件和重新加载现有软件模块。这些操作应当不包括任何改造，除非对故障部件的分析显示需要改造。

9. 研究堆仪器仪表和控制系统的配置管理

9.1. 在设施调试之前，应当提供反映研究堆仪器仪表和控制系统配置和状态的全套文件。在研究堆的整个寿命期间文件应当保持最新。

9.2. 应当建立一个关于仪器仪表和控制系统的系统和部件的基准数据库，并应当包括下列信息：

(a) 一般信息（如系统标识、序列号、制造商、供应商支持、位置、安全级别）；

(b) 系统摘要（例如，功能、配置、系统对安全的影响、当前性能、系统不可用时运行可用性的损失、接口、文档）；

(c) 物理特征（如机柜数量、详细的部件库存、运行限值）；

(d) 边界（例如，环境条件、电源、接地、机柜和房间所需的电源裕度、与其他系统交换的信息量）；

(e) 系统约束（如许可证条件、技术规范、设计约束、运行特征）；

(f) 老化问题（如维护成本、更换零件、性能下降）；

(g) 改进措施（如功能、配置、性能、维护）；

(h) 支持参考。

9.3. 反应堆营运者和维护人员应当协作完善和更新仪器仪表和控制系统配置管理的文件。第 9.1 段和第 9.2 段所述文件和数据库应视为敏感资料，应当按国家信息安全要求进行保护。

10. 研究堆仪器仪表和控制系统的改造和现代化

10.1. 研究堆仪器仪表和控制系统现代化的主要原因是现有系统老化（例如，由于没有备件）或系统故障率增加。这些发展可能导致频繁的反应堆关闭和长时间的维护，导致研究堆越来越不可用。SSG-10（Rev.1）[8]提供了关于研究堆老化管理的建议。

10.2. 现代化的另一个原因是仪器仪表和控制系统的技术进步，它可以提供更高的可靠性、改进的人机界面以及更广泛和更快速的数据收集和数据处理能力。其他因素（如新的监管要求）也可能影响研究堆仪器仪表和控制系统现代化的最终决定。

10.3. 在仪器仪表和控制系统现代化之前，应当利用现有系统的经验收集关于当前限制和未来需求的信息。这包括来自过去故障和事故的信息，这些信息应当由研究堆使用的事件记录系统记录下来。其他弱点可以从运行绩效的自评定中发现，包括分析即使是与正常运行的微小偏差。此外，还应当考虑今后可能出现的问题，并评定这些问题的潜在影响。

10.4. 仪器仪表和控制系统的改造和现代化应当按照 SSG-24（Rev.1）[10]关于研究堆改造的计划、组织方面、安全评定、实施和实施后方面、培训和文件的建议进行。对于与研究堆仪器仪表和控制系统的改造和现代化相关的每一项改造，都应当进行严格的独立核实和验证。

10.5. 对仪器仪表和控制系统的改造可能包括系统部件的完全更换。对现有安全系统的改造需要遵循与原始设备相同的设计、建造和调试程序（见 SSR-3[1]第 7.101 段）。本“安全导则”第 4 部分提供了关于仪器仪表和控制系统设计的建议。

10.6. 仪器仪表和控制设备的改造预计将在研究堆的寿命期间进行。在每种情况下，都应当考虑到正在改造设备的功能以及从一种技术转换到另一种技术可能产生的影响。这可能包括从模拟系统改为数字系统，或因缺少备件（即老化）而更换仪器仪表和控制系统。

10.7. 当决定对安全重要仪器仪表和控制系统进行改造时，需要考虑和评定对研究堆安全的可能影响（见 SSR-3[1]第 7.101 段）。

10.8. 营运组织应当核实对仪器仪表和控制系统的每一次改造都已就其对安全的潜在影响进行了适当的评定、记录和报告，并应当确保在改造完成后，反应堆不会在未经正式批准的情况下重新启动。

10.9. 旧仪器仪表和控制系统的设计文件可能不完整或不准确。因此，对此类系统的重大改造或替换可能涉及某种程度的“逆向工程”，以重新创建原始设计基准和规范。应当提供反映研究堆仪器仪表和控制系统目前配置的全套文件。

10.10. 根据 SSR-3[1]第 7.99 (e) 段核实和更新现有文件的过程，应当在研究堆仪器仪表和控制系统开始任何现代化之前进行。反应堆运行人员和维护人员应当合作更新该文件，以确保所有现代化活动都包含在系统配置管理文件中（见第 9 部分）。第 9.2 段中描述的仪器仪表和控制系统的基准数据库也应当更新。

10.11. 现有文件的核实和更新应当从仪器仪表和控制系统结构的高级功能描述开始，最好是以图示的形式，并附有所有仪器仪表和控制系统的列表。

10.12. 营运组织应当指定一名设计人员负责仪器仪表和控制系统改造的设计、集成、记录和维护，并负责培训运行人员使用新系统。参考文献[20]提供了指定设计人员应当承担责任的细节。

10.13. 对于仪器仪表和控制系统的改造，应当考虑运行人员和在紧急情况下负有责任人员的职责和责任。应当考虑改造对这些人员与系统交互的影响，以实现有效的人机界面。第 7 部分提供了关于人因工程和人机界面的建议。

10.14. 应当考虑新设备或改造设备的可靠性，以及改造对整个系统可靠性的影响。定性分析的执行（例如，故障模式及其影响的分析）可能有助于确定仪器仪表和控制系统的哪些部分可能会受到改造的影响，以及系统执行其安全功能能力的影响。

10.15. 在改造仪器仪表和控制系统时，应当考虑对实施纵深防御和独立性概念的影响。要求安全系统尽可能独立于其他反应堆系统（见 SSR-3[1]要求 27）。在改造仪器仪表和控制系统时，应当考虑设计导则的制定。

10.16. 对仪器仪表和控制系统进行复杂改造的影响将更加难以分析。应当认真考虑增加任何新功能以及今后扩大现有系统能力的能力。

10.17. 应当考虑系统预期环境条件下的改造鉴定。改造应当符合相关的使用条件（包括运行环境），鉴定计划应当基于对拟议改造的安全分析。

10.18. 应当制定研究堆仪器仪表和控制系统改造控制程序，包括适当的程序和评审和批准修改的安全方面的组织机构。

10.19. 在设计仪器仪表和控制系统的升级和改造时，应当考虑以下因素：

(a) 由于研究堆的物理特征而可能限制仪器仪表和控制系统设计选择的任何限制；

(b) 需要在替换设备的设计与现有仪器仪表和控制系统的设计之间保持一致（例如，降低整个人机界面和系统维护的复杂性）；

(c) 设备或技术的商业可用性，以及制造商或第三方在设备使用寿命期间技术支持的未来可用性。

10.20. 改造的好处应当与潜在的安全负面后果进行权衡，这种评定应当作为改造正当性的一部分记录下来。应当实施补偿措施以预测和防止负面安全后果。

10.21. 应当向相关人员提供关于改造仪器仪表和控制系统的适当培训，以最大限度地减少或消除潜在的错误。

10.22. 更新或更改软件工具的后果可能很严重，应当进行影响评定（例如，编译器的升级可能会使先前关于编译器是否足够的分析或核实结果失效）。

10.23. 研究堆仪器仪表和控制系统的改造需要由合格人员进行（见SSR-3[1]第 7.99 (d) 段）。工作应当在设计人员的监督和反应堆经理的授权下进行。

10.24. 一旦完成，在研究堆启动之前，应当根据 SSG-10（Rev.1）[8]提供的建议对设备进行功能试验。

10.25. 当仪器仪表和控制系统被改造或者是升级的一部分时，在证明和执行变更时所做的努力应当是与该系统在确保研究堆安全方面的作用和功能

相称，同时考虑到现有系统和在改造或升级后将继续运行的任何系统。这也适用于基于软件的系统。

10.26. 当更换仪器仪表和控制系统时，新的仪器仪表和控制系统可以在适当的情况下与旧系统并行运行一段试用期，直到对新系统的充分性获得足够的信心。在这种配置中，只有旧的仪器仪表系统能够控制反应堆。在试用期内，新仪器仪表和控制系统驾驶员的响应应当记录在独立的采集系统中，以评定和比较他们的响应与旧系统的响应。

参 考 文 献

[1] 国际原子能机构《研究堆的安全》，国际原子能机构《安全标准丛书》第 SSR-3 号，国际原子能机构，维也纳（2016 年）。

[2] 国际原子能机构《研究堆的调试》，国际原子能机构《安全标准丛书》第 SSG-80 号，国际原子能机构，维也纳（2023 年）。

[3] 国际原子能机构《研究堆的维护、定期试验和视察》，国际原子能机构《安全标准丛书》第 SSG-81 号，国际原子能机构，维也纳（2023 年）。

[4] 国际原子能机构《研究堆堆芯管理和燃料装卸》，国际原子能机构《安全标准丛书》第 SSG-82 号，国际原子能机构，维也纳（2023 年）。

[5] 国际原子能机构《研究堆运行限值和条件及运行程序》，国际原子能机构《安全标准丛书》第 SSG-83 号，国际原子能机构，维也纳（2023 年）。

[6] 国际原子能机构《研究堆的营运组织和人员招聘、培训与授权》，国际原子能机构《安全标准丛书》第 SSG-84 号，国际原子能机构，维也纳（2023 年）。

[7] 国际原子能机构《研究堆设计与运行中的辐射防护与放射性废物管理》，国际原子能机构《安全标准丛书》第 SSG-85 号，国际原子能机构，维也纳（2023 年）。

[8] 国际原子能机构《研究堆的老化管理》，国际原子能机构《安全标准丛书》第 SSG-10（Rev.1）号，国际原子能机构，维也纳（2023 年）。

[9] 国际原子能机构《研究堆安全评定和安全分析报告的编写》，国际原子能机构《安全标准丛书》第 SSG-20（Rev.1）号，国际原子能机构，维也纳（2022 年）。

[10] 国际原子能机构《研究堆的利用和改造安全》，国际原子能机构《安全标准丛书》第 SSG-24（Rev.1）号，国际原子能机构，维也纳（2022 年）。

[11] 国际原子能机构《核安全与安保术语：用于核安全、核安保、辐射防护、应急准备与响应》（2022 年暂定版），国际原子能机构，维也纳（2022 年）

[12] 国际原子能机构《核电厂仪器仪表和控制系统的设计》，国际原子能机构《安全标准丛书》第 SSG-39 号，国际原子能机构，维也纳（2016 年）。

[13] 国际原子能机构《分级方法在适用研究堆安全要求中的使用》，国际原子能机构《安全标准丛书》第 SSG-22（Rev.1）号，国际原子能机构，维也纳（2023 年）。

[14] 国际原子能机构《关于核材料和核设施实物保护的核安保建议》（《情况通报》第 INFCIRC/225/Revision 5）号，国际原子能机构《核安保丛书》第 13 号，国际原子能机构，维也纳（2011 年）。

[15] 国际原子能机构《计算机核安保》，国际原子能机构《核安保丛书》第 42-G 号，国际原子能机构，维也纳（2021 年）。

[16] 国际原子能机构《核设施计算机的安保》，国际原子能机构《核安保丛书》第 17-T（Rev.1）号，国际原子能机构，维也纳（2021 年）。

[17] 国际原子能机构《核设施仪器仪表和控制的计算机安保》，国际原子能机构《核安保丛书》第 33-T 号，国际原子能机构，维也纳（2018 年）。

[18] 国际原子能机构《核装置设备鉴定》，国际原子能机构《安全标准丛书》第 SSG-69 号，国际原子能机构，维也纳（2021 年）。

[19] 国际原子能机构《仪器仪表和控制设计中的人因工程方面》，国际原子能机构《核能丛书》第 NR-T-2.12 号，国际原子能机构，维也纳（2021 年）。

[20] 国际核安全咨询组《维持核装置在整个运行寿期内的设计完整性》，《国际核安全咨询组丛书》第 19 号，国际原子能机构，维也纳（2003 年）。

[21] 国际原子能机构《核信息的安保》，国际原子能机构《核安保丛书》第 23-G 号，国际原子能机构，维也纳（2015 年）。

附　件

可用于研究堆仪器仪表和控制系统

A-1.　研究堆仪器仪表和控制系统涉及许多系统，这些系统可能因反应堆的类型、用途和运行模式而异（见第 2 部分）。本附件确定了可用于研究堆仪器仪表和控制系统以及相关结构。如果特定类型的设施不需要这些仪器仪表和控制系统，它们中的一些可能不会用于特定的研究堆。

A-2.　仪器仪表和控制系统可以设计成“自上而下”的系统结构（见图 A-1），具有不同级别的监控和处理以及传感器和执行器。不同系统结构级别的设计可用于降低每个级别上相关故障的可能性。在这种结构中，监控功能通常位于监督级别，计算、算法、安全和过程功能位于控制级别，传感器和致动器位于现场。

A-3.　典型的仪器仪表和控制系统及其相互关系如图 A-2 所示。

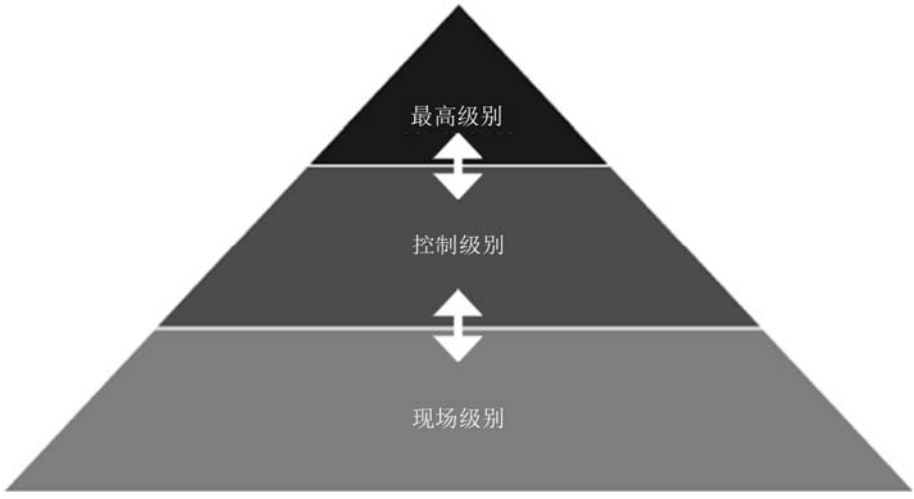

图 A-1.　仪器仪表和控制系统的“自顶向下”系统结构。

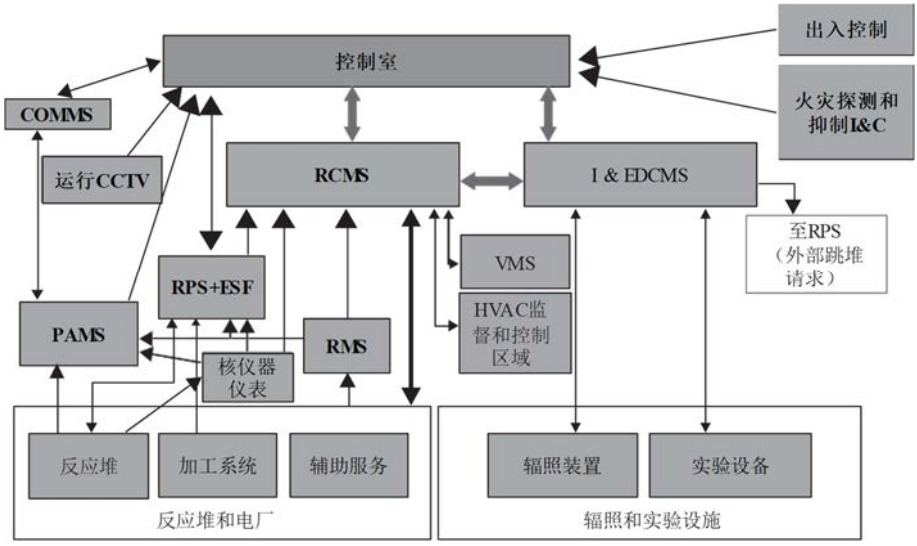

图 A-2. 研究堆仪器仪表和控制系统。CCTV－闭路电视； COMMS－通信系统；ESF－用于启动其他工程安全特点的仪器仪表和控制系统；HVAC－控制和监督区域的供暖、通风和空调；I&C－仪器仪表和控制；I&EDCMS－辐照设施和实验设备的控制和监控系统；Instr.－仪器仪表；PAMS－事故后监控系统；RCMS－反应堆控制和监控系统；RMS－均方根辐射监控系统；RPS－反应堆保护系统；VMS－振动监控系统。

反应堆保护系统

A-4. 反应堆保护系统是一组设计用于监控反应堆运行参数（如中子功率和周期、冷却剂流速、入口和出口温度、反应堆堆芯压降）的部件，以将它们与安全系统设置进行比较，并在参数达到或超过安全系统设置时自动启动反应堆停堆系统的动作。每个参数可以由两个或多个独立的通道测量。基于用于启动保护动作的逻辑布置符合单一故障标准来启动自动动作。当有三个独立的通道可用时，可以使用三个通道中两个通道的逻辑布置来防止由寄生信号启动保护动作。反应堆保护系统也可以由反应堆运行人员、实验者或辐射和实验设备的控制和监控系统手动启动。反应堆保护系统的跳堆导致反应堆停堆。

用于启动其他工程安全特点的研究堆仪器仪表和控制系统

A-5. 用于启动工程安全设施的仪器仪表和控制系统是一套部件，设计用于根据要求启动应急堆芯冷却系统、衰变热排出系统、隔离系统和隔离热排出系统的行动。该系统也可以由运行人员手动启动。工程安全功能的跳堆导致上述一个或多个动作的启动。工程安全特点的功能可以包括在反应堆保护系统中。

研究堆事故后监控系统

A-6. 事故后监控系统是研究堆的一个重要特点。其目的是为反应堆运行人员及其后备团队提供事故管理所需的信息，并确保这些信息是可靠的。在事故工况下，反应堆运行人员可能需要用于以下目的的信息：

(a) 执行预先计划的手动控制行动，这些行动没有提供自动控制系统，并且是预防或缓解事故后果所必需的。安全分析报告中规定的此类行动在事故管理程序中有所描述。

(b) 确定与反应性控制、堆芯冷却、反应堆冷却剂系统完整性、散热器、安全壳完整性和放射性监控相关的重要安全功能是否受到挑战，以及这些功能是否由反应堆保护系统、工程安全功能及其基本支持系统来实现。

(c) 向现场的应急响应设施传递信息，并与之有效沟通。

研究堆中核仪器仪表

A-7. 核仪器仪表跟踪反应堆在其所有运行状态下中子通量的值和演变，因为该参数与确保反应堆的安全运行最为相关。核仪器仪表还提供了建立合适控制策略的方法，用于启动反应堆并使其在不同功率水平下保持稳定运行。

反应堆控制和监控系统

A-8. 反应堆控制和监控系统旨在可靠地监控反应堆的性能和安全运行。反应堆控制和监控系统提供启动和功率自动调节，补偿燃料燃耗，并为安

全运行提供联锁。反应堆控制和监控系统是使用故障安全和冗余设备构建的，以接收和处理来自大量传感器的信号，启动相应的控制驱动器，并在研究堆的主控制台（主人机界面）为反应堆运行人员提供关于反应堆状态的信息。

A-9. 测量过程参数和致动器实际状态（位置）并连接到反应堆控制和监控系统的过程仪器仪表（如探测器、传感器、开关）位于仪器仪表和控制系统的现场级。

研究堆辐射监控系统

A-10. 辐射监控系统设计用于对研究堆及其周围地区进行连续辐射监控，以检测放射性物质的可能排放。这种排放可能是由于技术设备故障、保护屏障完整性丧失、水净化系统有效性丧失、隔离丧失或过滤器和通风系统故障造成的。

研究堆供暖、通风和空调系统

A-11. 供暖、通风和空调系统通过提供温度控制和空气质量控制，确保和维持人员和设备的适当环境条件。通风系统也有助于保持辐射条件，例如通过压力梯度和使用适当的过滤器。现代电子设备产生的热量比旧设备少得多，然而，温度过高仍然会降低性能。空调作为从作为安全系统的仪器仪表和控制系统中排出多余热量的一种手段，需要满足安全系统支持功能的设计要求。在热带气候或高湿度地区，通风系统的适当设计（实物分隔、冗余和密封循环）可能是消除仪器仪表和控制系统中潜在共模故障来源的唯一方法。在一些设施中，反应堆控制和监控系统具有向供暖、通风和空调系统远程发送命令的能力（即应急通风系统远程跳堆的命令）。

研究堆振动监控系统

A-12. 振动监控系统提供了一种监控和检测反应堆主旋转设备异常振动的手段。反应堆控制和监控系统用于将信息从振动监控系统传输到控制室。

研究堆控制室

A-13. 在主控制室中提供足够的控制、指示、警报和显示器，以启动、监督和监控正常的反应堆运行和反应堆停堆到安全状态，并提供已经达到并保持安全状态的保证。

A-14. 主控制室的最低限度规定，包括人机界面，必须考虑到反应堆运行人员需要做以下工作：

(a) 在反应堆的所有运行状态下安全运行反应堆；
(b) 监控反应堆的安全运行；
(c) 监控警报的出现；
(d) 执行并确认受控停堆；
(e) 启动安全相关系统；
(f) 执行并确认反应堆跳堆；
(g) 执行并确认工程安全功能的启动；
(h) 监控裂变产物屏障的状态；
(i) 保持反应堆处于安全关闭模式；
(j) 实施应急运行程序。

A-15. 警报器显示系统的状态。安全系统在反应堆运行人员的控制台或控制面板上有声音和视觉警报，以提供任何违反运行限值和条件的警告。反应堆运行人员可以通过反应堆控制和监控系统的主控制台访问所有信号。辐照设施和实验设备的控制台和显示器通常位于主控制室。

A-16. 如果主控制室不能远程关闭反应堆，辅助控制室在适用的情况下提供了远程关闭反应堆的可能性。在辅助控制室中提供足够的控制、指示、警报和显示器，以便能够启动、监视和监控反应堆停堆至安全状态，并保证已经达到并保持安全状态。

研究堆辐照设备和实验设备的控制与监控系统

A-17. 研究堆的主要用途是为研究目的和材料的中子辐照产生中子。辐照设施包括用于放置、移动和排列样品的设备。设计了专用和定制的仪器仪

表和控制系统来控制和监控这些操作。辐照设施和实验设备可能会影响研究堆的安全运行。影响反应堆安全的实验设备参数显示在主控制室。如安全分析所示，还可以提供从辐照设施和实验设备的控制和监控系统到反应堆保护系统的跳堆信号。

研究堆中的通信系统

A-18. 通信系统是主控制室和辅助控制室、反应堆大厅和加工区的运行人员、使用辐照设施和实验设备的人员以及设施内其他内部位置（如警报站）之间的链接，也是与场外应急响应组织的链接。采用语音公告系统，使现场所有人都能听到公告人员或报告需要立即响应的紧急情况或不可预见的情况。

研究堆的闭路电视系统

A-19. 闭路电视是一种有用的辅助设备，允许反应堆运行人员监控和监视运行人员正在执行的相关运行或维护任务或活动，也可用于监控设施的安全状态。

用于探测和灭火的仪器仪表和控制系统

A-20. 用于探测和灭火的仪器仪表和控制系统是一个独立的系统，有能力探测研究堆的火灾，然后在受影响的区域启动自动消防系统。火灾探测面板位于控制室，为反应堆运行人员提供相关信息。

研究堆进出控制系统

A-21. 主控制室的最低限度规定，包括人机界面，必须考虑到反应堆运行人员需要做以下工作：进出控制系统是研究堆实物保护系统的一部分，有能力监督和管理设施内人员的行动。进出控制面板可以位于控制室和/或中央警报站中，以向反应堆运行人员提供相关信息。

参与起草和审订人员

D’ Arcy, A.	顾问（南非）
Hargitai, T.	顾问（匈牙利）
McIvor, A.	国际原子能机构
Morris, C.	顾问（奥地利）
Rao, D.V.H.	国际原子能机构
Sears, D.F.	国际原子能机构
Shaw, P.	国际原子能机构
Shokr, A.M.	国际原子能机构
Sumanth, P.S.	印度巴巴原子研究中心
Sun, K.	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