国际原子能机构安全标准

保 护 人 类 与 环 境

核电厂仪器仪表和控制系统的设计

特定安全导则

第 SSG-39 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。

核电厂仪器仪表和控制系统的设计

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-39 号

核电厂仪器仪表和控制系统的设计

特定安全导则

国 际 原 子 能 机 构
2023 年 · 维也纳

版 权 说 明

核电厂仪器仪表和控制系统的设计

国际原子能机构，奥地利，2023年12月
STI/PUB/1694
ISBN 978-92-0-500823-3（简装书：碱性纸）
978-92-0-500124-1（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）。

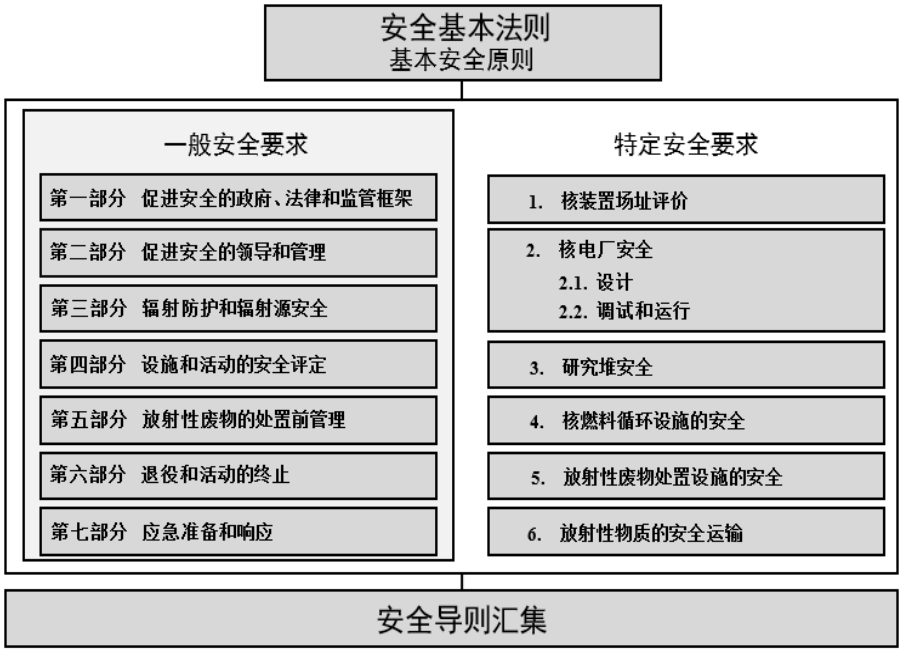

图 1. 国际原子能机构《安全标准丛书》的长期结构。

[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。

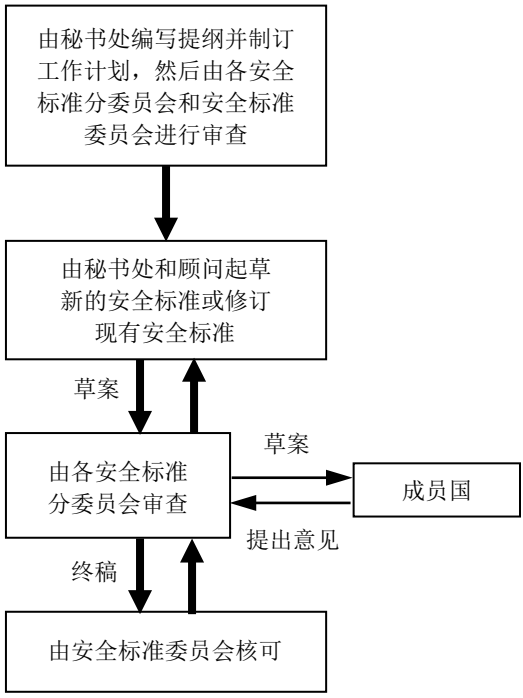

图 2. 制订新安全标准或修订现行标准的过程。

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 1

背景 (1.1-1.6) 1
目的 (1.7-1.8) 2
范围 (1.9-1.17) 3
结构 (1.18-1.27) 5

2. 仪器仪表和控制设计管理系统 6

概述 (2.1-2.9) 6
生命周期模式的使用 (2.10-2.37) 8
所有生命周期阶段的共同活动 (2.38-2.91) 15
生命周期活动 (2.92-2.167) 24

3. 仪器仪表和控制系统的设计基准 32

仪器仪表和控制功能的识别 (3.1-3.6) 32
仪器仪表和控制系统设计基准内容 (3.7-3.16) 33

4. 仪器仪表和控制系统架构 37

架构设计 (4.1-4.10) 37
仪器仪表和控制总体架构的内容 (4.11-4.12) 38
单一仪器仪表和控制系统的内容 (4.13) 39
独立性 (4.14-4.24) 40
共因故障的考虑 (4.25-4.40) 41

5. 仪器仪表和控制功能、系统和设备的安全分级 (5.1-5.13) 43

6. 对所有安全重要仪器仪表和控制系统的总体建议 44

概述 (6.1-6.5) 44
可靠性设计 (6.6-6.76) 45
设备鉴定 (6.77-6.134) 54
应对老化和技术老化的设计 (6.135-3.152) 60
接近安全重要系统的控制 (6.153-6.158) 62
运行期间的试验和可试验性 (6.159-6.191) 63
可维护性 (6.192-6.197) 68
用于因试验或维护而停用的措施 (6.198-6.204) 69
设定值 (6.205-6.212) 70
安全重要物项的标记和识别 (6.213-6.219) 71

7. 专用仪器仪表和控制系统和设备设计指导.....73

传感装置 (7.1-7.9).....73
控制系统 (7.10-7.14).....74
保护系统 (7.15-7.59).....74
电源 (7.60-7.65).....79
数字化系统 (7.66-7.147).....80
软件工具 (7.148-7.164).....89
安全应用中有限功能的工业数字化设备的鉴定 (7.165-7.175).....91

8. 有关人-机接口的考虑.....93

控制室 (8.1-8.18).....93
事故监控 (8.19-8.35).....96
运行人员通讯系统 (8.36-8.46).....98
仪器仪表和控制系统的人因工程的一般原则 (8.47-8.93).....99
历史数据的记录 (8.94).....104

9. 软件.....104

概述 (9.1-9.5).....104
软件需求 (9.6 -9.15) 105
软件设计 (9.16-9.43).....106
软件实现 (9.44-9.63).....108
软件核实与分析 (9.64-9.95).....110
预先开发软件 (9.96-9.98).....113
软件工具 (9.99).....114
第三方评定 (9.100-9.103).....114

参考文献.....115

附件 I 国际仪器仪表与控制标准参考文献目录.....119

附件 II 本“安全导则”原子能机构《安全标准丛书》第 NS-G-1.1 号和第 NS-G-1.3 号之间的相关性.....124

附件 III 成员国不同领域的实践.....128

定义.....133

参与起草和审订人员.....137

1. 导言

背景

1.1. 本“安全导则”就仪器仪表和控制系统的设计提出建议，以满足原子能机构《安全标准丛书》第 SSR-2/1（Rev.1）号[1]《核电厂安全：设计》的要求。

1.2. 本出版物是对原子能机构《安全标准丛书》第 NS-G-1.1 号 [1] 和第 NS-G-1.3 号 [2] 两个安全导则的修订与合并，并取代这两个导则。本版导则考虑了自 2000 年和 2002 年分别出版的这些较早的安全导则以来仪器仪表和控制系统的发展情况。主要的变化涉及计算机应用的持续发展以及对其安全、可靠和实际应用的必要方法的演变。此外，还考虑到人因工程的发展和对计算机安保的需要。本“安全导则”参考并考虑了原子能机构的其他安全标准和《核安保丛书》出版物，这些出版物提供了有关仪器仪表和控制系统设计的指导。其中最值得注意的是原子能机构出版的《安全标准丛书》中的第 GS-R-3 号《设施和活动管理系统》[2]、第 GS-G-3.1 号《设施和活动管理系统的适用》[3]、第 GS-G-3.5 号《核装置管理系统》[4]和第 GSR Part 4（Rev.1）号《设施和活动安全评定》[5]。

1.3. 本“安全导则”在以下主要相关主题领域新增或更新了导则：

— 为实现符合 GS-R-3[2]确定的要求，仪器仪表和控制所需要考虑的特定因素；
— 制定仪器仪表和控制系统的设计基准时考虑的设计输入；
— 仪器仪表和控制系统设计和实施阶段生命周期的相互依存性，特别是整个电厂总体仪器仪表和控制生命周期、单一仪器仪表和控制系统和软件的生命周期的依存性，以及将人因工程的输入和计算机安保的输入整合到这些生命周期中的需求；

---

[1] 国际原子能机构《核电厂基于计算机的安全重要系统的软件》,国际原子能机构《安全标准丛书》第 NS-G-1.1 号，国际原子能机构，维也纳（2000 年）。

[2] 国际原子能机构《核电厂安全重要仪器仪表和控制系统》,国际原子能机构《安全标准丛书》第 NS-G-1.3 号，国际原子能机构，维也纳（2002 年）。

— 计算机、用硬件描述语言编程的设备和有限功能的工业设备的使用，以及确保其正常运行的手段；
— 支持纵深防御概念的仪器仪表和控制总体架构（既包括核电厂系统设计中采用的纵深防御，也包括仪器仪表和控制系统本身用于防止共因故障的纵深防御）；
— 安全重要系统之间的数据传输，并专门考虑了接收数据系统的安全级别高于发送数据的系统的情况；
— 确保数字安全系统安保防范的措施；
— 与计算机软件开发有关的活动，包括根据本“安全导则”中提出的原则或以前的安全导则 NS-G-1.1 [3] 中隐含原则进行的设计、核实和验证。

1.4. 在本“安全导则”中，术语“仪器仪表和控制系统”指的是原子能机构《安全术语》[6]所定义的任何安全重要仪器仪表和控制系统。除了表示强调之外，“安全重要”不再重复。如果某一建议或解释即适用于安全重要仪器仪表和控制系统，也适用于非安全重要仪器仪表和控制系统，则会明确陈述。

1.5. 本“安全导则”与原子能机构《安全标准丛书》第 SSG-34 号《核电厂电力系统的设计》[7]密切相关，其中就电源、电缆系统、电磁干扰防护、设备和信号接地以及使仪器仪表和控制系统良好运行所必需的其他主题提出了建议。

1.6. 各成员国和制定标准的其他组织就仪器仪表和控制系统、设备和软件的设计和开发提供了进一步指导。这些出版物较原子能机构安全标准的要求更加详细。本“安全导则”可与专门的工业标准结合使用。

目的

1.7. 本“安全导则”的目的是就核电厂仪器仪表和控制总体架构和核电厂安全重要仪器仪表和控制系统提供指导，以满足核电厂的安全目标。

[3] 见脚注 1。

1.8. 本“安全导则”识别出仪器仪表和控制系统设计者在规定仪器仪表和控制系统设计基准所需的输入信息，这些输入信息来自于：核电厂的机械、电气、核和土建工程设计、电厂布置过程以及安全分析。例如，仪器仪表和控制系统设计基准将提供仪器仪表和控制系统所要完成的功能要求，设备要求运行的极端环境温度，仪器仪表和控制设备所需承受的外部事件以及需要自动停堆的工况等。

范围

1.9. 本“安全导则”为满足 SSR-2/1（Rev.1）[1]要求，对核电厂安全重要仪器仪表和控制系统的设计、实施、核实和文件编写提供了指导。本“安全导则”还描述了落实其他安全导则所建议的一些专门的仪器仪表和控制系统问题，这些问题涵盖了如管理系统、调试、安装、运行以及运行限值和条件。对此本“安全导则”会给出被应用的这些安全导则的相关章节。

1.10. 本“安全导则”适用于所有仪器仪表和控制设备，从传感器到驱动和控制机械设备的装置。它包括，例如：

— 传感器；
— 执行机构控制器；
— 对核电厂设备进行自动和手动控制的设备；
— 运行人员接口。

1.11. 本“安全导则”也适用于仪器仪表和控制设备实现的各种手段，例如：

— 计算机系统和相关的通信系统；
— 软件；
— 使用硬件描述语言编程的设备（例如现场可编程门阵列）；
— 有限功能的工业数字化设备。

1.12. 本“安全导则”不提供仪器仪表和控制系统辅助设施的建议，如冷却、润滑和能源。关于供电的建议见 SSG-34[7]。[4]

[4] 目前正在拟订关于辅助系统专题的安全导则草案，为其他支持功能提供建议。

1.13. 虽然本“安全导则”涵盖了与仪器仪表和控制相关的人因和计算机安保方面的内容，但未提供这些领域的全面指导。本“安全导则”旨在确定与人因和计算机安保活动的主要接口，并就影响这些主题的仪器仪表和控制系统设计特点提出建议。例如计算机化运行程序和信息技术安保都不包含在本导则的人因和计算机安保主题内。有关计算机安保的更多详细信息见附件 I[8]。

1.14. 本“安全导则”适用于新建核电厂仪器仪表和控制系统的设计、在役核电厂仪器仪表和控制系统的改造和现代化。原子能机构《安全标准丛书》第 NS-G-2.3 号《核电厂改造》[9]论述核电厂的改造，本“安全导则”也尽量避免与 NS-G-2.3[9]内容相重叠。

1.15. 原子能机构《安全术语》[6]将安全重要仪器仪表和控制系统定义为“作为某一安全组的组成部分和（或）其失效或故障可能导致现场人员或公民受到辐射照射的那些仪器仪表和控制系统/设备”。本“安全导则”第 5 部分进一步讨论了术语“安全重要”和与安全分级有关的其他术语。本“安全导则”适用的仪器仪表和控制系统示例包括：

— 反应堆保护系统；
— 反应堆控制系统和反应性控制系统及其监控系统；
— 用于监控和控制反应堆冷却的系统；
— 用于监控和控制应急电源的系统；
— 用于安全壳隔离监控和控制的系统；
— 用于事故监控的仪器仪表；
— 用于废水监控的系统；
— 用于燃料装卸的仪器仪表和控制系统。

1.16. 本“安全导则”为开发用于安全重要仪器仪表和控制系统的计算机软件以及数字化数据通信提供了建议。本“安全导则”还规定了使用硬件描述语言将仪器仪表和控制系统功能编程到集成电路中所需的措施。

1.17. 参考文献[10、11]概述了本“安全导则”所依据的概念，并举例说明了其中所涉及的系统。尽管这些参考文献没有提供原子能机构的导则，但它们可能为一些用户提供有用的背景材料。

结构

1.18. 第 2 部分提供了应用 GS-R-3[2]要求以及 GS-G-3.1[3]和 GS-G-3.5[4]建议给出了指导，这些要求和建议与仪器仪表和控制系统的开发尤为相关。同时它还涉及使用生命周期模式来描述仪器仪表和控制技术开发的过程管理系统，为仪器仪表和控制设计的一般过程以及进行特定的仪器仪表和控制技术开发活动提供指导。

1.19. 第 3 部分识别仪器仪表和控制必要的设计输入，为仪器仪表和控制系统的设计基准提供建议。

1.20. 第 4 部分为用于核电厂的仪器仪表和控制总体架构提供了指导。

1.21. 第 5 部分描述了安全分级方案，该方案用来根据物项的安全重要性依照本“安全导则”中的建议进行分级。

1.22. 第 6 部分提供了适用于所有安全重要仪器仪表和控制系统的一般导则。

1.23. 第 7 部分提供了专用于特定系统（例如反应堆保护系统）、特定类型的设备（例如传感器）以及特定技术（例如数字化系统和使用硬件描述语言配置的集成电路）的建议。第 2—6 部分和第 8—9 部分的建议也适用于第 7 部分中讨论的特定系统。

1.24. 第 8 部分提供人-机接口的建议。它包括人因原则在仪器仪表和控制应用的指导以及人-机接口应具有特性的指导。

1.25. 第 9 部分为基于计算机的安全重要仪器仪表和控制系统的软件开发提供了指导。

1.26. 本“安全导则”应作为一个整体应用，而不是独立章节的应用。例如，第 9 部分中提供的软件导则应与第 2 部分中提供的管理系统导则和生命周期导则结合使用。

1.27. 附件包括为本“安全导则”的主题领域提供更详细指导的工业标准清单、本“安全导则”中与被其取代的两份安全导则（NS-G-1.1[5] 和 NS-G-1.3[6]）相

[5] 见脚注 1。

关的信息、以及各国实际上存在差异领域的概要。还提供了本“安全导则”专用的名词解释清单。

2. 仪器仪表和控制设计管理系统

概述

2.1. SSR-2/1（Rev.1）[1]要求 6 规定：

> “核电厂的设计必须确保电厂和安全重要物项具有适当的特性，以确保安全功能可以必要的可靠性得到发挥，电厂可以在其整个设计寿期在运行限值和工况范围内安全运行并可以安全退役，并且将对环境的影响减少到最低程度。”

2.2. SSR-2/1（Rev.1）[1]要求 2 规定：

> “设计组织必须建立和实施管理系统，以确保在设计过程的所有阶段均考虑并实施为电厂设计所确定的所有安全要求，并确保在最后设计中达到这些要求。”

2.3. GS-R-3[2]建立了设施和活动管理系统的要求。

2.4. GS-R-3[2]第 2.1 段指出：

> “必须建立、实施、评定和不断改进管理系统。管理系统必须与有关组织的目标保持一致，并须促进实现这些目标。建立管理系统的主要目的必须是以下述方式实现和加强安全：
>
> — 以综合联贯的方式将实施组织管理的所有要求结合在一起；
> — 对提供满足所有这些要求的充分信心所需计划的和系统的活动作出说明；
> — 确保对健康、环境、安保、质量和经济等方面要求的考虑与安全要求不脱节，以有助于排除这些要求可能对安全造成的不利影响。”

---

[6] 见脚注 2。

GS-R-3[2]第 4.2 段还指出：“必须将该组织的信息和知识作为一种资源进行管理。”

2.5. 为了确保安全，应通过适当过程来控制设计基准和安全重要仪器仪表和控制系统有关的信息或记录的文件编写，以使它们在仪器仪表和控制系统的整个生命周期内保持完整、清晰、简明、正确和一致。管理系统应确保设计基准文件和相关或派生的信息或记录是足够的和充分的，并应长期维护，以反映核电厂的设计变更或变更状态。这包括可能来自设计基准文档的文件和信息，也包括可能对安全产生影响的文件和信息，例如与这些系统的运行、维护或改造相关的程序或手册。

2.6. 管理系统包括组织结构、组织文化、政策和流程，包括那些为开发满足安全要求的仪器仪表和控制系统的资源（如人员、设备、基础设施和工作环境）的识别和分配。

2.7. 参与仪器仪表和控制开发活动的每一个组织都应该有一个与营运组织管理系统期望相一致的管理系统。

2.8. GS-G-3.1[3]和 GS-G-3.5[4]就 GS-R-3[2]为设备和活动以及核设施确定要求的应用提供了指导。

2.9. 用于开发仪器仪表和控制系统的管理系统应符合 GS-R-3[2]要求，并符合 GS-G-3.1[3]和 GS-G-3.5[4]提出的建议，这些建议广泛适用于核电厂所有结构、系统和部件的开发。本“安全导则”涉及仪器仪表和控制系统所需的详细开发过程，应与上述出版物结合使用。

GS-R-3[2]对仪器仪表和控制系统的开发特别相关的主题是：

— 管理系统；
— 安全文化；
— 管理承诺；
— 遵守法律和监管要求；
— 组织政策；
— 计划；
— 职能和权力；
— 资源保障；

— 人力资源；
— 管理系统过程开发；
— 过程管理；
— 文件、产品（包括工具）和记录的控制；
— 采购；
— 通讯；
— 组织变更管理；
— 监控和衡量；
— 自评定；
— 独立评定；
— 不符情况以及纠正和预防措施；
— 改进。

生命周期模式的使用

2.10. GS-R-3[2]第 5.1 段指出：

> “必须确定管理系统中对于实现有关组织的目标、提供满足其所有要求的手段和交付其产品所必需的各个过程，而且必须对建立这些过程进行计划、实施、评定和不断改进。”

2.11. 现代的核电厂仪器仪表和控制系统是复杂的实体，必须采用不同的设计和核实方法，超出了老式系统中采用的典型方法。通常情况下，前几代仪器仪表和控制系统的功能特征和性能通常通过基于物理原理的模式和用于核实这些模式的试验来表征。

2.12. 现代的仪器仪表和控制系统，特别是其功能依赖于软件或硬件定义语言的数字化系统，其与旧系统的根本不同之处在于它们的行为由逻辑决定，而不是按照外部物理定律。因此，设计和实现中微小误差可能导致数字化系统出现非预期的行为。

2.13. 在数字化仪器仪表和控制系统中，证明最终产品是否满足其目标，在很大程度上（但不是唯一的）依赖于高质量的开发过程，该过程规定了设计需求的严格的规范和实施。为了确保最终产品适合使用，核实和验证

活动是必要的。然而通过采用与纯硬件系统相同的试验和物理模式相结合的方式，无法断定数字化仪器仪表和控制系统在所有工况下都能正确的执行。因此，与纯硬件系统相比，现代系统正确性的信心更多地来自于规范的开发过程。

2.14. 针对这种情况，在核电领域以及航空航天等其他安全重要领域，开发过程通常采用生命周期模式，该模式描述了电子系统的开发活动以及这些活动之间的关系。这些被普遍接受的实践已正式体现在核行业标准中，这些标准就仪器仪表和控制系统的开发过程提供了广泛的指导。通常情况下，与一个给定的开发步骤相关的活动被分组归入到生命周期的相同阶段。

2.15. 有完善文档记录的开发过程能提供证据，能增进独立的评审人员和监管机构对最终产品的目标适用性的信心。

2.16. 本部分中针对生命周期过程的建议也适用于第 9 部分描述的生命周期活动。本部分中针对生命周期过程的指导是针对 GS-R-3[2]要求以及 GS-G-3.1[3]和 GS-G-3.5[4]建议的补充，它们都适用于仪器仪表和控制系统的开发。

2.17. 为了描述仪器仪表和控制系统的开发，需要三个基本的生命周期层次：

(a) 仪器仪表和控制总体架构生命周期；
(b) 一个或多个单一仪器仪表和控制系统生命周期；
(c) 一个或多个单一部件生命周期：部件生命周期通常在平台开发的框架中进行管理，并且独立于总体架构层级和单一系统层次的生命周期期。数字化系统的部件生命周期通常分为独立的硬件开发生命周期和软件开发生命周期。

2.18. 有时仪器仪表和控制系统开发之外的其他活动会对仪器仪表和控制系统的要求和设计产生重要影响。人因工程和计算机安保就是这类活动的例子。与支持仪器仪表和控制系统设计相比，这些活动的目的更为广泛，并将对仪器仪表和控制的发展产生显著的影响。此外，在设计阶段考虑人因和安保防范特点更容易，成本效益也更高。如在设计阶段之后的再变更可能会非常困难，甚至于无法实现。

2.19. 图 1 给出了一个仪器仪表和控制开发生命周期的例子，以及来自于人因工程和计算机安保计划的主要输入。

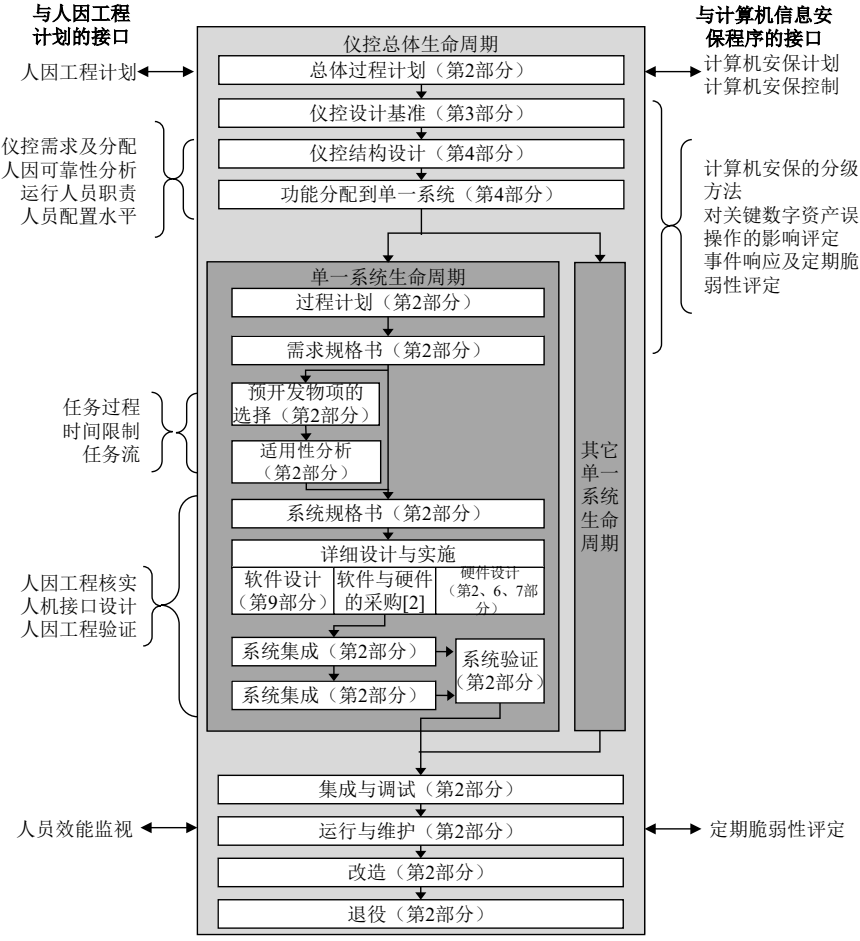

图 1. 典型的仪器仪表和控制开发生命周期活动以及与人因工程和计算机安保计划的接口。

2.20. 图 2 所示的“V 型”是另外一种角度开发生命周期的例子。该模式说明了需求规格书、设计、集成和系统核实之间的关系，以及核实和验证活动是如何与与开发活动之相关联的。图 2 既适用于数字系统，也适用于模拟系统。当然，如果系统中不存在软件，软件活动就没有必要了。

2.21. 根据获得的经验，在生命周期的任何一点都有可能需要修正前一阶段所做的工作。这些修正将流经并影响被修改阶段后所有工作。为简单起见，图 1 和图 2 没有给出此迭代路径。

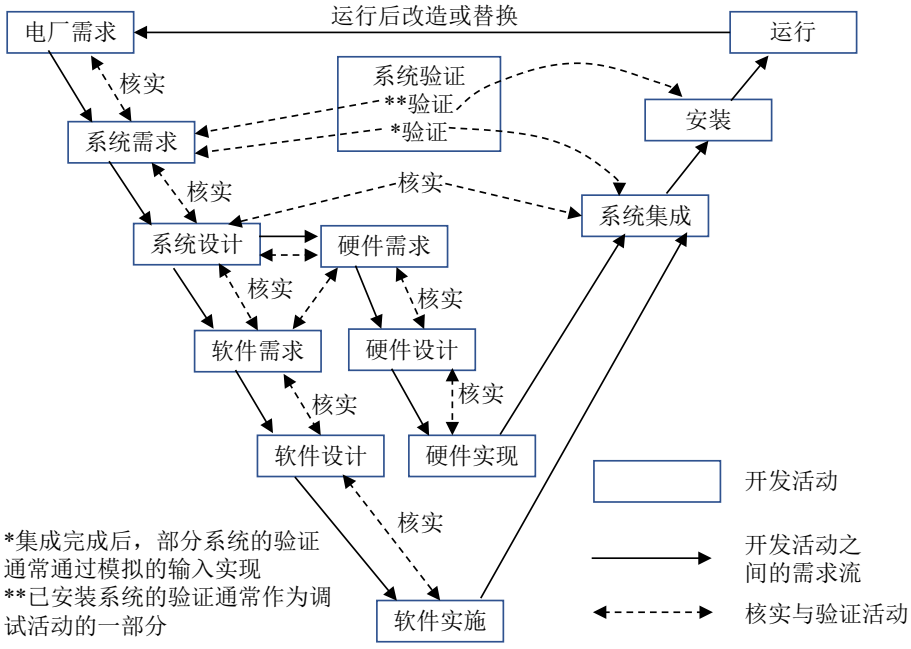

图 2. 仪器仪表和控制系统生命周期开发过程与核实和验证活动之间的典型关系。

2.22. 所有与仪器仪表和控制总体架构、单一仪器仪表和控制系统以及仪器仪表和控制部件的 [7] 开发、实现和运行有关的活动都应在编成文件的生命周期开发框架内进行。

2.23. 每个仪器仪表和控制系统和部件的生命周期都应涵盖从导出其需求开始，到核电厂安全不再需要该仪器仪表和控制系统或部件时终止的这段时间。

[7] 仪器仪表和控制部件包括硬件、软件（如应用软件和固件）以及硬件描述语言。

过程计划

2.24. 在开始任何技术活动之前，应根据管理系统的要求编写和批准一份计划，识别出该活动的必要投入、产品和过程，以及该活动与其他活动的关系。

2.25. 仪器仪表和控制系统的开发计划涉及仪器仪表和控制的特定主题以及需要专业化处理的仪器仪表和控制开发的主题。一般情况下，专门针对仪器仪表和控制开发的计划将涉及以下主题：

— 生命周期模式；
— 配置管理；
— 不符情况的识别、控制和解决；
— 危害分析；
— 核实和验证；
— 概率安全评定见解的运用；
— 仪器仪表和控制系统的专项安全分析；
— 需求工程；
— 架构设计；
— 预先开发物项的选择和验收；
— 设计；
— 实现（例如，硬件制造和软件编程或使用硬件描述语言的编码和整合）；
— 整合；
— 系统验证；
— 安装；
— 调试；
— 设备鉴定；
— 工具的鉴定和使用；
— 维护；
— 技术老化的管理；
— 运行；

— 培训；
— 软件维护。

2.26. 其中几个主题的计划可以合并为一个计划。

2.27. 仪器仪表和控制系统的开发还依赖于仪器仪表和控制系统开发以外的活动计划，例如：

— 质量保证；
— 安全重要物项的分级；
— 采购；
— 制造；
— 文件的编写和维护。

2.28. 所有仪器仪表和控制系统开发活动应根据适用经批准的计划进行。

与人因工程活动和计算机安全活动的协调

2.29. 虽然本“安全导则”未涵盖与人因工程和计算机安保有关的生命周期模式，但此类过程提供了仪器仪表和控制开发所需的信息。图 1 说明了这些过程之间的关系和接口。这些活动包括：产生特定于人因工程的需求的活动、与人因工程有关的核实和验证活动的输出、安保技术措施和计算机安保要求。

2.30. 仪器仪表和控制系统的开发应与人因工程活动和计算机安保活动协调一致。

2.31. 仪器仪表和控制系统开发中应考虑产生于人因工程程序的要求，包括：

— 运行人员的作用和职责以及其他人事需求的说明；
— 人-机接口的结构、系统和部件的安全分级；
— 信息要求说明，包括考虑明确一套处理事故工况和事故后工况所需的指示和控制器；
— 控制要求，自动和手动控制功能，以及将控制分配到合适场所的说明；

— 与通过分析识别的任务流程、时间限值、运行人员和信息交互所相关的要求（即任务分析，见第 8.78 段）；
— 基于工况背景的通知策略：基于工况背景的通知避免信息的“泛滥”，例如，在启动和瞬态期间；
— 报告仪器仪表和控制系统故障的要求；
— 支持仪器仪表和控制可维护性的措施；
— 在安全分析（即人的可靠性分析）中考虑人因错误的可能性所产生的见解。

2.32. 与人因工程有关的核实和验证活动：

— 应核实人因工程相关建议的处理情况以及在分析人-机接口设计过程中发现的不足之处；
— 应核实仪器仪表和控制系统是否符合适用的与人因工程相关的设计指引；
— 应核实设计是否提供了足以支持运行人员完成其指定任务的仪器仪表和控制系统、其他设备和运行人员辅助设备；
— 应核实人因设计是否能引导运行人员对告警信息的正确响应，包括允许为可信的运行人员动作留有足够的时间；
— 应使用基于效能的措施来验证运行人员是否可以在期望仪器仪表和控制系统运行的所有工况下使用系统完成其功能，包括当仪器仪表和控制系统的某些部分由于授权原因（例如，出于维护或试验目的）而停役。

2.33. 人因工程需求开发和人因工程活动的核实和验证通常作为人因工程程序的一部分执行。与仪器仪表和控制系统生命周期过程的接口除外，本“安全导则”中没有进一步详细描述人因工程程序。

2.34. 核电厂总体仪器仪表和控制应执行计算机安保计划指定的安保措施。

2.35. 计算机安保计划应考虑仪器仪表和控制总体架构以及单一仪器仪表和控制系统，如有必要应更新。

2.36. 仪器仪表和控制的开发应在符合计算机安保计划的技术、程序和行政要求的开发环境中，通过负责核安全和核保安的人员之间的意见交换或者核安全和核保安人员联合小组进行。

2.37. 关于在核设施计算机安保实施的补充资料见参考文献[8]。

所有生命周期阶段的共同活动

配置管理

2.38. GS-R-3[2]第 5.12 段、第 5.13 段、第 5.18 段和第 5.19 段指出：

> “5.12. 必须对文件进行管理……确保文件用户了解并使用适当和正确的文件。”
>
> “5.13. 必须评审和记录对文件所作的修改，这些修改须经与文件本身同样级别的批准。”
>
> ……
>
> “5.18. 必须通过控制来确保产品不绕过所要求的核实活动。”
>
> “5.19. 必须对产品进行标识，以确保其正确使用。在有可追溯性要求的场合，该组织须控制并记录产品的唯一性标识。”

2.39. 在 GS-R-3[2]，这些主题应在文件管理、产品控制和记录管理的标题下进行阐述。对于工程活动，文档和产品的控制通常归入到配置管理的标题下。GS-R-3[2]对记录管理的要求也适用于配置管理下的文档，尽管有些记录可以与配置管理系统分开控制（例如，通过一个独立的记录管理系统）。GS-G-3.1[3]和 GS-G-3.5[4]就第 2.38 段所述四个主题提出了补充建议。

2.40. 仪器仪表和控制系统的生命周期中配置管理的目标包括：

- 所有需要配置管理的物项的标识，即文档、仪器仪表和控制产品和相关记录；
- 配置物项的安全存储和检索措施；
- 配置管理下各物项之间的相关性和关系的识别；
- 配置管理下各物项所有变更的识别；

— 配置管理下对各物项无意的和未经授权修改的预防；
— 确保持续符合设计基准；
— 配置基线的规范说明，即在配置管理 [8] 下每个配置层级内用于物项的相互兼容和一致的部件的配置；
— 确保实际核电厂和技术文件之间的一致性；
— 配置管理下物项当前状态的说明（例如，审核、批准或验证状态）。

2.41. 配置管理应包括用于分析变更的影响、批准变更、确保版本正确组合、发布供使用的设计文档和软件以及建立和维护按时间顺序编排的记录（例如，在设计的特定点将使用工具的哪些版本）的技术和程序。

2.42. 应指定所有仪器仪表和控制系统物项及其相关文档，并给出唯一标识符并置于配置管理下。

2.43. 仪器仪表和控制物项包括交付的仪器仪表和控制系统、支持该系统或系统按预计运行所必需的任何单独安装的物项，定义所有这些物项的文档和文件，以及可能影响其质量的软件工具。

2.44. 仪器仪表和控制物项通常包括，例如：

— 采购物项、重复使用物项和新开发物项；
— 软件部件，如源代码和可执行代码、硬件描述语言、现场可编程门阵列的配置数据（称为“数据流”）和安装在核电厂设备中的软件，包括应用软件、操作系统和支持软件；
— 硬件部件和这些部件的可更换元件；
— 固件；
— 规范说明、设计文件、制造图纸及说明书、安装图纸及说明书、软件和硬件描述语言的开发文档；
— 设备配置数据和配置文件（如安全运行限值、警告或报警限值、设定值和标定常数）；
— 用于生产、控制、配置、核实或验证仪器仪表和控制部件的实体工具和软件工具，包括使用这些工具时使用的参数设定。

[8] 单一部件、系统或总体仪控系统等物项均可建立配置基线。任何物项的基线都将覆盖所有囊括该物项的的系统和部件。

2.45. 配置管理数据应用于核实仪器仪表和控制物项是否正确组装并安装在正确的物理和拓扑位置，以及预期的软件版本正确安装。

2.46. GS-R-3[2]第 5.21 段指出：“必须在过程文件中明确记载记录，并必须对记录进行管理。所有记录必须易读、完整、可识别和易检索。”

2.47. 生命周期过程记录应置于配置管理之下。

2.48. 生命周期记录的配置管理程序可能与用于仪器仪表和控制产品的配置管理程序不同。

2.49. 置于配置控制下的生命周期记录包括系统安全分析所依赖的或可能影响运行或维护期间安全的任何信息，例如：

— 生命周期活动的计划和程序；
— 安全证明计划；
— 分析文件；
— 记录安全证明及其支持证据的人工制品或记录，例如质保、核实（包括分析和试验）、验证（包括需求验证）、过程评定和监查、真实性、完整性和可追溯性的人工制品或记录；
— 核实和验证活动的记录；
— 试验说明、程序、计划和结果；
— 安全系统的限值和确定安全系统限值的方法；
— 与系统整合有关的程序、计划和结果；
— 与评审和监查过程有关的文件；
— 提供需求可追溯性的矩阵；
— 维护和运行程序；
— 设备和备件采购规格书的技术方面；
— 鉴定记录；
— 仪器仪表和控制系统及部件的文件（见第 2.90 段）。

2.50. 配置管理下物项的识别标识应包括版本号。

2.51. 应将配置控制应用于仪器仪表和控制系统的初始开发、开发过程中的更改以及投入使用后的变更。

2.52. 配置管理流程应维护配置管理下每个物项的相关信息。

2.53. 可记录的信息包括：该物项首次考虑的完成时间；酌情在各种版本中纳入了哪些改动，包括差异报告；配置管理中对其他项的依赖；物项的当前审批状态；以及负责制定、评审和批准该物项的责任人。

2.54. 宜通过仪器仪表和控制设备本身即可获知安装在仪器仪表和控制设备上的软件身份以及配置数据的值。

2.55. 可以获知已安装物项身份以及配置数据值的能力将支持核实设备是否正确配置。自动检查设施的安装或软件工具可能有助于此核实。

仪器仪表和控制系统的危害分析

2.56. 应对仪器仪表和控制总体架构执行危害分析，以识别可能危害核电厂设计的纵深防御或多样性策略的工况。

2.57. 应对每个安全系统执行危害分析，以识别可能降低其安全功能的性能的工况。

2.58. 应考虑的危害包括内部危害、外部危害、核电厂设备故障和由于硬件故障或软件错误导致的仪器仪表和控制故障或误操作。还应考虑由于不需要的相互作用而造成的危害。

2.59. 仪器仪表和控制系统的危害分析应考虑所有核电厂状态和运行模式，包括不同运行模式之间的转换。状态降低也应包括在内。

2.60. 在总体仪器仪表和控制设计基准完成之前，仪器仪表和控制系统危害分析的初始结果应可用。

2.61. 危害分析应在开发生命周期的每个阶段进行更新，包括（但不限于）仪器仪表和控制总体架构的设计，以及安全系统的要求和设计、实施、安装和改造的说明。

2.62. 更新危害分析的意图是识别可能由安全级仪器仪表和控制系统的具体特征、安全级仪器仪表和控制系统与核电厂之间的相互作用以及安全级仪器仪表和控制系统与其他仪器仪表和控制系统之间的相互作用引起的危害，而不论其安全分级如何。

2.63. 应采取措施消除、避免或缓解已识别的危害的后果，这些危害可降低系统功能的性能。

2.64. 为消除、避免或缓解危害后果的措施，例如，可以采取如改变仪器仪表和控制系统的要求、设计或实现，或修改核电厂设计等形式。

2.65. 为危害分析选择的方法应适用于被分析的物项。

核实和验证

2.66. 仪器仪表和控制系统生命周期的每个阶段都使用前期阶段开发的信息，并提供结果作为后继阶段的输入。

2.67. 生命周期期中每个阶段的结果都应对照前几个阶段设定的要求进行核实。

2.68. 可以使用需求可追溯性矩阵来记录验证在生命周期的每个阶段中令人满意地符合了需求，或者在没有令人满意地符合需求时采取了适当的措施。

2.69. 应核实总体仪器仪表和控制、每个仪器仪表和控制系统以及每个仪器仪表和控制部件，以确定所有需求（功能需求和非功能需求）均已满足，并确定是否存在任何不期望的行为（见第 2.128－2.142 段）。应验证对总体仪器仪表和控制、每个仪器仪表和控制系统和每个仪器仪表和控制系统部件的定义需求，以确定它们按预期履行。

2.70. 核实和验证应由独立于设计和开发人员的个人、团队或组织团体执行。

2.71. 独立核实和验证的建立通常涉及到确保进行核实和验证的团队、个人或组织团体：

— 具有足够的技术能力和知识；
— 可以设定自己的范围；
— 不会受到开发者的压力；
— 不受预算削减或进度表限制的影响，以免妨碍它们完成全范围评审；

— 允许向管理层提交其调查结果，而不受开发团队的不利压力。

2.72. 核实和验证的独立性程度和类型应适用于所涉及的系统或部件的安全级别。核实和验证可以在不同的独立性水平上同时进行（例如，由独立于原始开发组织中开发人员的试验人员所执行的核实和验证，以及由单一组织执行独立的核实和验证）。

2.73. 应记录核实和验证活动，包括探测到的异常及其处理的记录。如果在核实和验证阶段探测到异常，则由此产生的设计变更及其实现应遵循与先前执行的核实和验证过程相同的过程。

2.74. 核实和验证团队、系统整合团队、调试团队以及系统设计人员和开发人员之间的技术沟通应记录在案。

使用概率安全分析的见解

2.75. SSR-2/1（Rev.1）[1]第 5.76 段指出：

> “设计必须充分考虑电厂在所有运行工况和所有状态包括停堆状态下的概率安全分析，并特别涉及：
>
> (a) 确定已经实现平衡设计，使得任何特定特性或假想始发事件都不会对总体风险产生过大或明显不确定的贡献作用，而且纵深防御的各层级在实际的程度上具有独立性；
> (b) 提供关于将防止出现电厂参数微小偏差可能造成电厂工况很大变化（“陡边效应”）情况的保证；
> (c) 将分析结果与已规定的风险验收标准相比较。”

2.76. 在仪器仪表和控制系统的设计中应考虑从概率安全评定中获得的见解。

2.77. 原子能机构的相关安全标准[12、13]说明了设计期间概率安全评定的详细信息以及其评定结果的使用。

安全评定

2.78. 应根据 GSR Part 4（Rev.1）[5]要求以及原子能机构《安全标准丛书》第 SSG-3 号《制定和实施核电厂一级概率安全评定》[12]和第 SSG-2 号《核电厂确定性安全分析》[14]建议，对仪器仪表和控制系统进行安全评定。

2.79. 应进行设计分析、核实和验证，以确定满足仪器仪表和控制总体架构和每个单一仪器仪表和控制系统的所有设计基准的要求。

2.80. 第 3.14 段指出了在仪器仪表和控制总体架构以及所有仪器仪表和控制系统的设计基准要求中考虑的主题。第 3.15 段指出了在安全系统的设计基准要求中考虑其他主题。

2.81. 典型的设计分析、核实和验证技术包括：

— 可追溯性分析：可追溯性分析通常用于确定需求的实现和验证；
— 故障模式和影响分析：经常使用故障模式和影响分析来确定符合单一故障标准，并验证所有已知的故障模式要么是自揭示的，要么是通过计划的试验探测到的；
— 纵深防御和多样性分析：纵深防御和多样性分析是评审安全系统的共因故障脆弱性的手段之一（见参考文献[11]，其中提供了关于这一主题的补充资料）；
— 可靠性分析：可靠性分析使用统计方法来预测系统或部件的可靠性。常用的可靠性分析技术包括部件计数法分析、元件应力法分析、寿命数据分析（如威布尔分析）、可靠性框图和故障树分析；
— 验证：验证试验涉及确定性技术，可能包括统计技术；
— 安保防范试验：安保防范试验通常需要脆弱性评定的输入，并用于确定在安保防范方面使用了良好实践；
— 进行分析，以确定物项被设计成可靠的：此类分析用于确定设计包含已知的可促进高可靠性的特点，如冗余性、符合单一故障标准、可试验性、故障安全设计和严格的鉴定 [9]；

[9] 就仪器仪表和控制系统而言，通常需要结合定性分析、定量分析和试验来核实是否遵守了各项可靠性要求。

— 用于仪器仪表和控制系统各种不同运行模式的功能要求的确定：包括分析失电、重启或重新启动期间和之后正确的系统行为以及其他过渡点。日历时间更改（例如夏令时和闰年）是其他过渡点的示例。

2.82. 应陈述分析中使用的每个假设，并论证该假设的使用。

2.83. 进行的任何分析方法与分析的输入、分析的结果和分析本身一起都应完全规定并编写成文件。

2.84. 基于现有技术发生水平，单一系统按照最高质量标准进行规范和设计，当考虑与规范说明、设计、制造、安装、运行环境和维护实践相关联的所有潜在故障源（不包括信息安保相关的故障源）时，10^{-4}~10^{-5} 数量级的要求时风险失效概率可能是对概率安全分析中可能声称的可靠性适当的整体限值。该数值可能需要包括系统冗余通道中的共模故障风险，并适用于整个系统，从传感器、经过处理到输出，再到被驱动设备。不排除可靠性更高的宣称，但需要详细的论证，同时考虑上面所提到的所有因素。

2.85. 仪器仪表和控制系统的任何可靠性宣称都应有证据支撑，且应在可论证的限值内（附件 III 说明了一些国家接受的限度）。

2.86. 针对核电厂安全要求和 SSR-2/1（Rev.1）[1]要求，在设计和实施过程中应定期评审核电厂内每个仪器仪表和控制系统之间的相互作用。

2.87. 当发现与这些要求有任何冲突，则应适当纠正设计和实现。

文件

2.88. 仪器仪表和控制系统文件：

— 提供在设计过程中所涉及的各种不同阶段间及其不同部分之间传递信息的手段；
— 提供一个表明需求已正确地解释并在所安装的系统中正确实现的记录；
— 将运行极其重要的信息和安全设计有关的信息传递给核电厂运行人员；

— 为用于核电厂和仪器仪表和控制系统的维护和对可能的未来修改提供一个基础；
— 在仪器仪表和控制的生命周期各阶段都应具有可追溯性；
— 应被控制在配置管理系统下；
— 应该是明确的、完整的、一致的、良好结构化的、易读的、目标受众（如领域专家、安全工程师和软件设计人员）易于理解的，且便于可核实和可维护。

2.89. 完善的文件将有助于系统的运行、监视、故障排除、维护、后续变更或现代化改造，以及核电厂和技术支持人员的培训。

2.90. 营运组织应建立或提供用于仪器仪表和控制系统和部件的文档，这些文档至少应涵盖以下主题：

— 设计需求；
— 功能和功能设计；
— 运行原则；
— 系统在总的核电厂概念中的作用；
— 设计特点，包括安全重要设施的识别；
— 竣工的设计和配置文件；
— 系统及其主要部件（包括传感器和执行器）的竣工布置图；
— 与其他核电厂系统的接口和依赖关系；
— 监视、试验、诊断、维护和运行的设施和需求；
— 试验程序和结果；
— 设备鉴定；
— 设计和开发过程，以及设计中遵循的质量要求；
— 包括调试在内的所有试验阶段的策略；
— 核实和验证方法和结果的设计和开发；
— 所有正常运行状态和模式的运行程序；
— 应急运行程序及严重事故导则，以涵盖假设的事故假想方案及设计扩展工况；
— 备用件和部件供应的建议和采购说明；

— 安保防范设计特点及其应用。[10]

2.91. 采购和供应、设计、制造活动、软件代码以及核实和验证的需求和过程文件应可供营运组织、监管机构或代表这些组织行事的独立第三方评定之用（见第 9.100－9.103 段）。

生命周期活动

需求规范说明

2.92. 应以适当的形式记录对总体仪器仪表和控制、每个单一仪器仪表和控制系统和仪器仪表和控制部件的需求。

2.93. 全套单一仪器仪表和控制系统的需求组合，应符合为总体仪器仪表和控制建立的设计基准。

2.94. 应从仪器仪表和控制设计基准导出对总体仪器仪表和控制以及每个单一仪器仪表和控制系统的需求。

2.95. 第 3 部分论述了总体仪器仪表和控制设计基准的来源和内容。

2.96. 系统和部件需求应酌情规定以下内容：

— 每个单一的仪器仪表和控制系统或部件要做什么；
— 在每个核电厂状态和运行模式中，每个功能的输入和输出之间的关系；
— 测量、控制功能和显示器的最小精确度和准确度以及最大时间响应；
— 系统接口（例如系统与运行人员之间以及与其他系统的接口）；
— 自监督特点，包括所需的时限性能（包括故障探测时间和恢复时间）；

[10] 若在相关设计中假设了营运组织的运行安保政策和实践（包括与计算机安保防范有关的政策和实践），则需将这些假设告知用户。为了限制其分发范围（范围小于其他系统信息），用单一的文件来收录此类说明的要素或许比较。

— 仪器仪表和控制系统对基于自监督手段探测的故障所采取的行动；
— 安保防范特点（例如有效性检查、特定计算机安保控制和允许系统继承其环境中的安保防范控制并继承访问权限的特性）；
— 要达到的可靠性和可用性水平，以及确保达到这一水平所需的任何支持需求；[11]
— 维护所需的设备和设施；
— 设计限值；[12]
— 对特定故障模式的安全响应；
— 应对核电厂正常工况和事故工况相关的所有运行环境范围以及可预见的内外部危害的坚稳性。

2.97. 如果设计限值是必要的，则它们应加以规范说明和论证以及是可追溯的。

2.98. 数字化系统的安保防范设计需求应考虑安保防范风险评定的结果，并应符合营运组织安保策略的特点。

2.99. 应使用特定的流程来管理整个生命周期的需求，并确保所有需求都得到满足、核实、验证和实现。

2.100. 需求工程是用于确保仪器仪表和控制系统的安全目标通过设计得以实现的特定过程。

2.101. 应使用与系统安全的重要性相称的预定技术组合来建立和记录需求。

2.102. 用于建立和记录需求的技术可能包括使用定义良好的语法和语义、模式、分析和评审的规范语言。

---

[11] 可靠性和可用性水平可以从数量上或质量上定义，例如，根据上面提到的支持要求，如实施特定可靠性战略的要求、开发过程特性设定配置基线的项目可包括单一部件、系统或整个仪器仪表和控制系统。任何项目的基线将涵盖构成该项目的所有系统和组成部分的要求或符合特定标准的要求。

[12] 设计限值的例子包括支持独立性或多样性要求的限值。

2.103. 需求应该尽可能地根据需要实现的内容来编写，而不是根据需求的设计和实现方式来编写。

2.104. 应以所有相关各方（如被许可人、供应商和设计人）都能理解的术语描述需求。

2.105. 需求文档应参考，包括或补充其他信息，例如特定需求的背景信息、风险考虑、功能或安全特点设计的建议，以确保目标受众完全理解需求。

2.106. 应识别本身对安全有潜在影响的需求。

2.107. 应定义每项需求的来源和理由，以便于核实、验证、对更高层级文件的追溯，并证明所有相关的设计基准要求均已考虑在内。

预先开发物项的选择

2.108. 应根据第6.78－6.134段中的指导意见对预先开发物项进行适当的鉴定。

2.109. 预先开发物项包括硬件设备、预先开发的软件、商用现成设备、由硬件和软件组成的数字化设备、配置有硬件定义语言的硬件设备或可用于硬件描述语言的预先开发的功能块。

2.110. 参考文献[11]提供了关于商用现成设备使用的更多细节。

2.111. 不用于实施安全级仪器仪表和控制系统的预先开发物项的功能都应表明不会干扰系统的安全功能。

2.112. 在可行的情况下，应配置预先开发物项使得不使用的功能禁用。

2.113. 所选的预先开发物项通常是现成的商用设备。使用现成的商用设备可能会降低成本和设计工作量。此外，可能没有专门用于核电厂的装置，使用一种经过良好证实的商用产品可能比开发一个新物项更有效或更安全。

2.114. 商用现成设备往往更加复杂，可能具有不期望的功能，而且往往在更短的时间内就会过时。它们通常具有核电厂应用中不需要的功能。商用现成设备的鉴定可能更加困难，因为商用开发过程可能不如本“安全导则”中所述的过程那么透明和受控制。没有供应商的合作，鉴定一般是不可能

的。通常接受商用现成设备的相关困难之处可能在于质量和可靠性的证明信息不可用。

2.115. 许可证持有者在决定是否使用商业性现成设备时，应考虑在核电厂生命周期内质量鉴定的维护。

2.116. 例如，生产线可能经常发生设计修改，如子部件的修改、新的固件版本、新的制造流程或新的软件版本。这可能给供应商和核电厂的配置管理在正确识别此类修改方面（特别是仪器仪表和控制系统维护和备件管理方面相关的）带来挑战。在某些情况下，营运组织购买了特定版本备件的“全生命周期供应”，以避免出现特定部件或版本无法购买的可能性。

2.117. 预先开发物项应具有能提供在仪器仪表和控制系统中使用它们所需信息的文档。

仪器仪表和控制系统的设计与实现

2.118. 仪器仪表和控制总体架构和单一仪器仪表和控制系统的设计应源于所要求的功能加上其他要求系统性的和逐步的分解。

2.119. 应将仪器仪表和控制系统需满足的系统需求分配给硬件、由硬件描述语言配置的设备以及软件（如果存在）的适当组合。

2.120. 硬件可包括特定于某些应用的集成电路。软件可以包括现成的软件和固件，例如操作系统，要开发的软件或通过配置预先开发软件编写的软件。改进的要求可能还必须考虑到对仪器仪表和控制系统范围以外的部分所作的较低层次的设计决策，例如，被驱动设备的类型和性能。

2.121. 非安全重要需求的实现不应干扰安全重要功能。

2.122. 应制定设计规则，以确保每个仪器仪表和控制系统的内部逻辑经得起核实和验证的检验。

2.123. 设计应考虑需要在运行过程中配置仪器仪表和控制参数或对其核实和验证，并应提供这样做的手段（如反应堆保护系统的停堆设定值、标定常数和软件配置设定）。

系统整合

2.124. 系统整合：

— 应处理经整合的部件之间所有的接口，例如硬件和软件之间或软件模块之间的接口；
— 应确定满足用于系统不同部件内接口的要求；
— 应确定部件、配件和子系统按整合系统设计的那样运行，以使系统满足其特定要求，包括掩盖超范围值、异常处理和时限的要求。

2.125. 在开始系统整合之前，经过核实的模块（硬件和软件）的符合配置应可用。

2.126. 软件工具通常用来控制将模块集成到系统部件，并控制用于系统验证的软件构建。软件工具也可在现场使用以便于配置控制和已安装部件和已验证部件之间的可追溯性。

2.127. 应使用记录在案的可追溯性分析来证明系统整合相对于系统设计规范是完整的，并且第 2.124 段已得到满足。

系统验证

2.128. 应对每个单一仪器仪表和控制系统和仪器仪表和控制系统的整合进行系统验证。

2.129. 出于本“安全导则”的目的，当完成系统在核电厂的安装时，系统验证终止。如果在系统安装到电厂后需要进行系统验证的一些额外内容，这些内容可以包括在调试试验中，前提是验证试验记录中包括结果，并且设计团队和核实团队之间保持第 2.71 段和第 2.72 段中定义的独立性。

2.130. 用于验证目的而进行试验的系统应代表现场仪器仪表和控制系统的最终配置。

2.131. 经过系统验证的软件应与运行中使用的软件相同。

2.132. 系统验证应证明系统满足所有可能的接口条件和所有可能的负载条件下的所有要求。

2.133. 运行模式、仪器仪表和控制系统和核电厂之间的相互作用在系统验证期间不易试验，应在调试期间试验，或应通过补充分析进行验证。

2.134. 系统验证应包括：

— 系统的所有部分；
— 接口信号 [13] 的全部范围，包括超出范围的值；
— 异常处理；
— 设定值准确度和回差；
— 核电厂和系统运行的所有工况，包括工况之间的转换；
— 停电后的恢复；
— 时限；
— 坚固性和容错性。

2.135. 系统验证试验应涉及所有输入的变化，即应使用动态试验。

2.136. 动态试验应该使用，可以代表核电厂参数的变化的真实的假想方案，基于对可能的核电厂假想方案的分析，将会要求仪器仪表和控制系统响应。

2.137. 功能试验的设计应涵盖功能需求所允许的所有行为。功能试验的结构覆盖率进行论证时应该考虑功能需求。

2.138. 应考虑使用统计技术进行验证试验。

2.139. 应考虑使用模拟机进行系统验证。

2.140. 系统运行手册和维护手册的适当部分应在系统验证期间尽可能地进行验证。

2.141. 编写成文件的可追溯性分析应证明系统验证在系统要求的规范方面是完整的，并且第 2.132 段和第 2.134 段的目标已经实现。

2.142. 完整的验证文档应足以使验证过程得以重复，并确信对于任何重复的且先前令人满意的试验，将获得一致的令人满意的结果。

---

[13] 接口信号包括，例如，到达或来自其他系统、传感器、驱动设备和运行人员接口的输入和输出。

安装、总体仪器仪表和控制整合以及调试

2.143. 仪器仪表和控制系统应按照批准的设计安装在核电厂内。

2.144. 设备应在到货时进行视察，或进行调试试验，以核实系统和部件在运输过程中没有损坏。

2.145. 以下各段阐述了在执行原子能机构《安全标准丛书》第 SSG-28 号《核电厂调试》[15]导则时的考虑因素。

2.146. 调试应逐步将仪器仪表和控制系统与其他部件和其他核电厂物项整合，并应核实它们是否符合设计假设，是否符合功能标准和性能标准。

2.147. 核电厂环境试验是调试的一个重要部分。

2.148. 调试应特别注意核实与外部系统的接口，并验证与接口设备的正确性能。

2.149. 在调试期间，所有仪器仪表和控制系统应在尽可能能代表在役实际情况的运行、试验和维护条件下运行一段时间。

2.150. 调试完成前，应对运行手册和维护手册的适用部分进行验证。

2.151. 在宣布仪器仪表和控制系统可运行之前，应完成相关的生命周期计划的活动，应建立从需求到已安装系统的可追溯性，其建造和设计文档应完整，并反映竣工配置。

运行和维护

2.152. 应根据原子能机构《安全标准丛书》第 NS-G-2.6 号《核电厂的维护、监视和在役检查》[16]指导意见进行仪器仪表和控制系统的维护和监视，该指导意见就仪器仪表和控制系统的维护和监视（包括校准）的计划、组织方面和实施提供指导。

2.153. 以下第 2.154－2.156 段阐述了在执行 NS-G-2.6[16]关于仪器仪表和控制系统的指导意见时的考虑因素。

2.154. 应使用适当的手段对仪器仪表和控制系统参数进行更改。

2.155. 应监控仪器仪表和控制系统运行和维护中的人员效能，以记录可能产生为减少人为错误的修改需要的运行经验。

2.156. 在整个预计使用寿命内，应备有足够数量的备件可供运行和维护（例如，根据仪器仪表和控制系统设计、部件可靠性以及更换部件和供应商支持的未来可用性）。

改造

2.157. 以下各段阐述了在执行 NS-G-2.3[9]关于仪器仪表和控制系统的指导意见方面的考虑因素。

2.158. 仪器仪表和控制技术升级和改造的设计应考虑：

— 已建核电厂的物理特性造成的限制，有效地限制了仪器仪表和控制系统的设计选择；
— 设备更换的设计和现有的仪器仪表和控制设备之间可能需要保持一致，以便例如减少整个运行人员接口的复杂性和核电厂的维护任务；
— 关于商用设备或技术方面的实际考虑，以及获得制造商或第三方在设备安装生命周期内提供的设备和技术支持的期望；
— 需要更新现有的设计文件 [14]。

2.159. 当仪器仪表和控制系统被改造或升级时，应事先确定在证明和执行变更时所适用的严格程度。

2.160. 严格程度应以受影响系统在确保核电厂安全方面的作用和功能为基础，并与工作结束后将继续运行的现有系统相结合。这也适用于软件工具的变更。

2.161. 仪器仪表和控制系统的改造或升级应遵循规定的生命周期。

2.162. 改造所需的生命周期过程的复杂性与改造的复杂性和安全重要性有关。

[14] 旧系统的设计文档可能不完整或不准确。因此，对这类系统进行重大修改或更换可能需要某种程度的“逆向工程”,以重新创建原始设计基准和规范。

2.163. 即使是最简单的变更，其生命周期也应该至少包括图 2 所示的单一系统生命周期的各个阶段，包括每次仪器仪表和控制系统改造后的核实和验证。

2.164. 人-机接口的临时配置代表新的和现有的仪器仪表和控制系统之间的过渡，可能需要从人因工程的角度进一步分析，以适应临时设备或程序的使用。运行人员的接口的改进可能导致运行人员和维护人员在变更后一段时间内的错误增加。在某些情况下，可能有必要对培训进行修改。

2.165. 在更换新的输入及输出系统时，应考虑将新的输入及输出系统与旧系统同时运作一段试用期，直至对新系统足够有足够信心为止。通过一次只在一个序列安装新的冗余设备，可以实现等效的并行运行。

2.166. 在考虑仪器仪表和控制系统的并行运行时，应权衡运行问题和复杂性的缺点与可信度的增益，并对风险进行评价。

2.167. 在最初开发和变更期间，软件工具的更新或变更的后果可能影响很大，应评定其影响（例如，编译器升级可能会使以前关于编译器的充分性的分析或核实结果无效）。

3. 仪器仪表和控制系统的设计基准

仪器仪表和控制功能的识别

3.1. SSR-2/1（Rev.1）[1]要求 4 规定：

> “在所有电厂状态下均须确保实现核电厂的以下基本安全功能：(i) 反应性控制；(ii) 从反应堆和燃料库中移除热量；以及 (iii) 封闭放射性物质，屏蔽辐射和控制已计划的放射性释放，以及限制放射性的意外释放。”

3.2. SSR-2/1（Rev.1）[1]第 4.1 段指出：

> “必须采取系统性方案来确定实现基本安全功能所需的这些安全重要物项，以及确定正在促进实现或影响所有电厂状态下的基本安全功能的固有特征。”

3.3. SSR-2/1（Rev.1）[1]第 4.2 段指出：“必须提供对电厂状况进行监控的手段，以确保实现所要求的安全功能。”

3.4. 所需的安全功能来自核电厂的设计过程（见 SSR-2/1（Rev.1）[1]第 4 部分），需要采取系统的办法将这些功能分配给核电厂的结构、系统和部件。

3.5. 仪器仪表和控制系统所需功能的确定（如核安全、安保和时间限值等特性的非功能要求）应作为核电厂设计过程的一部分。

3.6. 分配给仪器仪表和控制系统的功能包括在各种运行状态和事故工况下提供与核电厂运行相关的信息和控制能力的功能。与纵深防御概念相对应的这些功能的目标是：

— 防止偏离正常运行；
— 探测故障并控制异常运行；
— 控制核电厂设计基准范围内的事故；
— 控制设计扩展工况的后果；
— 缓解事故的放射性后果。

仪器仪表和控制系统设计基准内容

3.7. SSR-2/1（Rev.1）[1]要求 14 规定：

> “安全重要物项的设计基准必须针对相关运行状态、事故工况以及内部和外部危害导致的工况规定必要的能力、可靠性和功能性，以满足核电厂寿期内的特定验收标准。”

3.8. SSR-2/1（Rev.1）[1]第 5.3 段指出：

> “必须系统地证明每个安全重要物项设计基准的合理性并将设计基准形成文件。这种文件必须提供营运组织安全运行电厂所需的资料。”

3.9. 仪器仪表和控制总体架构和每个仪器仪表和控制系统都应该有一个文档化的设计基准。

3.10. 仪器仪表和控制总体架构是核电厂仪器仪表和控制系统的组织结构。一个核电厂的仪器仪表和控制总体架构包括多个仪器仪表和控制系统，每个都发挥特定的作用。

3.11. 设计基准识别总体仪器仪表和控制以及每个单一仪器仪表和控制系统的功能、条件和需求。然后使用此信息对功能进行分类，并将其分配给安全级别适当的系统[17]。

3.12. 在某些情况下，仪器仪表和控制系统需求随着在建核电厂的设计和设计基准的发展才被识别出来。因此，在项目初期仪器仪表和控制设计基准的内容可能不完整。

3.13. 仪器仪表和控制系统设计基准的开发应来自核电厂安全设计基准文件，并应提供以下信息：

— 核电厂的纵深防御概念；
— 将提供的安全功能（见第 3.11 段）；
— 核电厂安全重要功能的安全分级、功能和性能需求；
— 关于自动和手动动作之间的优先级原则，以及当一个以上的系统可以驱动一个装置或功能时，自动动作之间的优先级原则；
— 国家对仪器仪表和控制系统许可证的要求；
— 国家对仪器仪表和控制系统安全分级的要求；
— 国家对关于运行需求的要求；
— 对核电厂安全和安保功能至关重要的数字化仪器仪表和控制系统的分析和确定；
— 计算机安保的风险评定与影响分析；
— 信息和控制需求及分配；
— 核电厂运行策略；
— 人员可靠性分析；
— 运行人员的作用；
— 人员配置水平。

3.14. 仪器仪表和控制系统的设计基准应规定总体仪器仪表和控制和每个单一仪器仪表和控制系统的必要能力、可靠性和功能性，包括：

— 所有功能需求，例如：
  - 每个仪器仪表和控制系统需要运行的核电厂所有电厂运行状态；
  - 每个仪器仪表和控制系统运行的各种配置；
  - 每个核电厂状态、每个核电厂运行模式和长期停堆的功能需求[15]；
  - 每个所需的仪器仪表和控制系统功能的安全重要性；
  - 系统需要响应的假想始发事件；
  - 每个单一仪器仪表和控制系统在仪器仪表和控制总体架构纵深防御概念中的作用；
  - 被监视的变量或变量组合；
  - 所需的控制和保护功能，包括规定自动、手动或两者同时执行的动作，以及控制装置的位置；
  - 每个仪器仪表和控制系统安全功能所需的量程、变化率、准确度、数字化表示的量化、计算精确度和响应时间。
— 为达到必要的可靠性和可用性水平而提出的所有需求，例如：
  - 安全功能独立性需求；
  - 定期试验、自诊断和维护的要求；
  - 定性或定量的可靠性和可用性目标[16]；
  - 工艺失效时的行为需求。
— 为达到必要的计算机安保水平而提出的所有需求，例如：
  - 设计中应遵守的计算机安保和运行限值；
  - 实施的计算机安保措施。
— 确保设备合理鉴定所需的所有要求，例如：
  - 设计基准，包括工业控制系统应符合的标准的说明；
  - 可能降低系统在履行其功能时的性能的核电厂工况，以及为保持必要的能力而应采取的措施；
  - 要求系统执行安全重要功能的内外部危害（包括自然现象）的范围；

[15] 例如，功能需求定义了输入到输出的转换和要采取的操作。

[16] 系统和部件的可靠性和可用性限制可以使用概率标准、确定性标准（例如，符合单一故障标准或软件的特定过程和核实方法）或两者来指定。

- 要求系统执行安全重要功能的核电厂环境条件 [17] 的范围；
- 对使用材料的限值；
- 核电厂实体设计和布置的限值和条件，包括设备位置、电缆敷设和电源的限值；
- 设备的物理位置和设备之间的接口。

3.15. 除第 3.14 段所提建议外，还应考虑到其他一些建议，安全系统的设计基准应规定：

— 驱动安全系统所需参数的限值（分析限值；见第 6.209 段和第 71 页图 3）。
— 需要显示的变量和状态，以便运行人员确定系统的保护功能的运行。
— 任何非自动触发安全动作的论证，包括：
  - 允许手动控制的时机、事件、持续时间和核电厂工况；
  - 允许仅通过手动触发，或触发后仅通过手动方式进行控制的论证；
  - 运行人员在运行状态和事故工况下预计采取手动动作的环境条件范围；
  - 验证运行人员在执行手动操作时要考虑的信息将显示在适当的位置，并具有支持运行人员操作所需的性能特征。
— 允许旁通仪器仪表和控制安全功能的工况；
— 被驱动的保护系统复位前必须满足的工况；
— 多样性功能的需求，以缓解共因故障的后果。

3.16. 上述条款可以在仪器仪表和控制总体架构设计基准中说明，也可以在单一系统的设计基准中说明。对于某些条款，在总体仪器仪表和控制设计基准中规定通用要求而在单一系统的设计基准中提供更多细节可能是适

[17] 关注的核电厂环境条件包括设计基准事故、内部事件或外部事件期间仪器仪表和控制系统设备可能经历的正常条件、异常条件和极端条件。如果不充分考虑到纵深防御的要求，跨仪器仪表和控制系统的任何相互作用，特别是在不同程度上合格的组件之间的相互作用，都可能损害纵深防御的要求。

当的。无论如何，仪器仪表和控制总体的设计基准与单一系统的设计基准应一致，而不同设计基准之间的关系和接口亦应易于理解。

4. 仪器仪表和控制系统架构

架构设计

4.1. 仪器仪表和控制总体架构设计确立：

- 构成总体架构的仪器仪表和控制系统；
- 这些系统的组织；
- 仪器仪表和控制功能在这些系统的分配；
- 仪器仪表和控制系统之间的互连，以及各个已分配和禁止的相互作用；
- 分配给总体架构的设计限值（包括禁止的相互作用和行为）；
- 仪器仪表和控制系统之间的边界的定义。

4.2. 单一仪器仪表和控制系统的架构设计确立：

- 从所有的整合层次下至到不可分割单一物项的合成—分解关系；
- 给每个整合层次上的每个物项分配仪器仪表和控制功能、行为、限值和（其对应的）质量要求；
- 可组合性和组合规则，以确保一个整合级别的行为组合满足下一个更高整合级别所需的行为，而不引入其他行为；
- 在每个整合层次上各物项之间和各整合层次之间的相互连接，以及各分配和禁止的交互；
- 分配给每个独立仪器仪表和控制系统的设计限值（包括禁止的交互和行为）。

4.3. 现代仪器仪表和控制系统相互联接更加紧密、更加难以分析（因此，相比前几代仪器仪表和控制系统安全更加难以保障）。一个设计良好的仪器仪表和控制系统架构将确保纵深防御和多样性，并将这些难以分析的特性局部化并包络在各系统中，以便这些特征不会使电厂安全的保证变得过于困难。

4.4. 仪器仪表和控制总体架构和单一仪器仪表和控制系统系统应满足核电厂的需求，包括对系统接口的需求以及对安全、安保、可核实性、可分析性和时间限值等特性的需求。

4.5. SSR-2/1（Rev.1）[7]要求 7 规定：“核电厂的设计必须体现纵深防御，各个层级必须尽实际可能相互独立。”

4.6. 参考文献[18、19]解释了纵深防御的概念，并说明了纵深防御的各个层次。

4.7. 仪器仪表和控制总体架构不应损害核电厂设计中的纵深防御概念和多样性策略。

4.8. 仪器仪表和控制总体架构应明确用于总体仪器仪表和控制纵深防御的概念和仪器仪表和控制多样性策略。

4.9. 仪器仪表和控制总体架构设计还应确定支持核电厂纵深防御和多样性不同层级的仪器仪表和控制系统间的独立性水平。

4.10. 在仪器仪表和控制总体架构中，纵深防御是通过防线独立的手段来达到的，因此，下一条防线将会弥补上一条防线的失效。

仪器仪表和控制总体架构的内容

4.11. 仪器仪表和控制总体架构：

- 应包括满足核电厂设计基准所需的所有仪器仪表和控制系统功能；
- 应识别要在所有仪器仪表和控制系统中一致处理的所有的主题；[18]
- 应识别将纳入仪器仪表和控制总体架构的各个仪器仪表和控制系统，以：
  - 支持在核电厂应用的纵深防御概念和多样性；
  - 支持总体仪器仪表和控制独立性的设计基准需求；

[18] 要在所有仪器仪表和控制系统中一致考虑的主题包括，例如，核电厂运行原则的应用、人机接口设计标准的应用、电缆敷设的限制、接地实践和报警管理的理念。

- 不同安全分级的系统和不同安全分级功能的充分隔离；

— 应定义各仪器仪表和控制系统之间的接口和通信方式；

— 应制定设计策略，用于满足分配给仪器仪表和控制总体架构的每个安全功能的可靠性要求；[19]

— 应支持安全组遵守单一故障标准；

— 应向主控室、辅助控制室及其他需要运行或事故处理信息的区域提供所需的信息；

— 应在主控制室、辅助控制室和运行或事故管理需要控制的其他区域提供必要的运行人员控制；

— 应提供必要的自动控制，以将过程变量保持和限制在规定的运行范围内，并限制故障和偏离正常运行工况的后果，使其不超过安全系统的能力。

4.12. 用于实现仪器仪表和控制系统的仪器仪表和控制平台的特征会影响仪器仪表和控制总体架构的设计，同时仪器仪表和控制总体架构会对仪器仪表和控制平台功能和鉴定提出需求。因此，总体建议将仪器仪表和控制总体架构的设计和仪控平台的选择结合起来考虑。安全系统的功能和鉴定需求通常不同于控制系统。正因如此，并且由于多样性的原因，总体仪器仪表和控制通常会涉及两个或两个以上的平台。

单一仪器仪表和控制系统的内容

4.13. 每个仪器仪表和控制系统的架构设计：

— 应提供所有必要的仪器仪表和控制功能，以完成在仪器仪表和控制总体架构设计中分配给它的职责；

— 应酌情将系统划分为冗余的序列，并应具体规定这些序列之间所要求的独立程度；[20]

---

[19] 确定可靠性要求的策略可能包括遵守单一故障标准、冗余、冗余功能之间的独立性、故障安全设计、多样性和可核实性（包括可分析性和可试验性）。第 6 部分描述了在达到可靠性的实施策略中的考虑。

[20] 典型的安全系统将由成冗余的序列组织而成，以符合单一故障标准。较低安全级别的系统出于安全原因可能不需要冗余元件，但为了改善其在正常运行时的可靠性实际上可能是冗余的。

— 应规定每个冗余序列应包括哪些仪器仪表和控制物项；
— 应描述仪器仪表和控制功能的分配和对每个仪器仪表和控制系统物项的其他系统要求；
— 应定义系统内仪器仪表和控制物项之间的接口和通信方式；
— 应定义应用于主要物项和数据链路的主要设计特点。

独立性

4.14. 仪器仪表和控制总体架构内的独立性旨在防止故障在系统之间的传播，并在实际可行的情况下避免多个系统暴露在相同的共因故障源。此类共因故障源的示例包括内部事件、外部事件和共同支持服务系统的故障。

4.15. 仪器仪表和控制总体架构既不应损害安全系统序列间的独立性，也不应损害核电厂不同纵深防御层次之间的独立性。

4.16. 应将要求完全独立的仪器仪表和控制功能分配给独立的硬件系统或物项。

4.17. 安全系统应独立于较低安全级别的系统。

4.18. 安全系统内的冗余序列应达到必要程度的相互独立，以确保在需要时能够完成所有安全功能。如果冗余序列之间的通信是必要的，例如为了表决或允许部分跳堆，则应采取足够的措施确保电气隔离和实体分隔以及通信的独立性。为了表决而进行的通信可以限制由随机故障引起的可能危及安全的误驱动。

4.19. 运行人员接口不应同时抑制一个以上冗余序列的安全功能。

4.20. 如果优选功能符合第 6.55 段要求，安全控制站可操作一个在其序列以外安全设备的物项。

4.21. 只有当来自安全系统的命令具有高优先权的情况下，来自较低安全级别系统的运行人员控制指令才可操作安全系统或部件。

4.22. 如果满足第 6.25－6.56 段的建议，安全系统提供的信息可用于较低安全级别的控制站。

4.23. 安全系统和部件在暴露于其必需响应的事故工况或因内外部危害产生的工况而受到影响时，仍应保持完成其安全功能的能力。

4.24. 安全仪器仪表和控制系统支持设施的故障或误操作不应损害安全系统的冗余部分之间、安全系统与较低安全级别系统之间、或应用于核电厂的纵深防御概念不同层次之间的独立性。

共因故障的考虑

4.25. SSR-2/1（Rev.1）[1]要求 24 规定：

> “设备的设计必须适当考虑安全重要物项发生共因故障的可能性，以确定必须如何应用多样性、冗余性、实体分隔和功能独立这些概念，从而实现所需的可靠性。”

4.26. 原子能机构《安全术语》[6]将“共因故障”定义为“由单一特定事件或原因引起的两个或多个结构、系统和部件的故障。”

4.27. 由于人为错误、开发或制造过程中的错误、维护中的错误、开发中软件工具使用的的错误、系统或部件之间的故障传播，或应对内外部危害的鉴定或防护说明不充分。

4.28. 仪器仪表和控制总体架构应该定义要使用的架构概念，为了使核电厂的纵深防御层次间尽可能独立。

4.29. 为了维持核电厂纵深防御层次之间的独立性，仪器仪表和控制系统的设计应考虑系统内和系统间共因故障的防护。为此，应充分考虑将功能分配给各种系统和系统元件，应在系统之间提供适当的独立性水平，并应说明应对安全系统内共因故障的策略。

4.30. 应评价总体仪器仪表和控制的共因故障危害一个或多个基本安全功能的可能性。

4.31. 对于本评价中不考虑的任何已确定的共因故障，应提供理由。

4.32. 对安全分析范围内每一假想始发事件，应分析其叠加妨碍保护系统发挥必要安全功能的共因故障所产生的后果。

4.33. 对纵深防御概念和多样性进行分析是执行第 4.32 段所述分析的一种方法。见第 2.81 段。

4.34. 如果第 4.32 段所述的分析结果确定假想始发事件叠加保护系统的共因故障导致的后果不可接受，应修改设计。

4.35. 完全消除仪器仪表和控制系统和架构的所有共因故障薄弱点是不可能的，但应对任何已识别的薄弱点是否可接受进行论证。

多样性

4.36. 原子能机构《安全术语》[6]将“多样性”定义为“两个或多个冗余系统或部件执行同一功能，这些不同系统或部件具有不同属性，从而减少包括共模故障在内的共因故障的可能性。”

4.37. 多样性是一种减少因需求、设计、制造或维护中的错误而导致的共因故障的脆弱性的方法，也是一个可用来补偿证明所规定的可靠性水平遇到困难时的保守方法。

4.38. 当利用多样性来缓解保护系统共因故障的影响时，则应提供论证，说明多样化的装置实际上能达到对所宣称的共因故障影响的缓解效果。

4.39. 当提供多样化的仪器仪表和控制系统时，多样化的系统在规范说明、设计、制造或维护方面不应存在相同的错误。

4.40. 概率分析 [21] 不应将安全重要仪器仪表和控制物项视为完全独立[22]，除非它们是多样的，并符合本“安全导则”中推荐的功能独立、电气隔离、通信独立、环境鉴定、抗震鉴定、电磁兼容鉴定、实体分隔和内部事件防护。

[21] 例如，概率分析包括可靠性分析和概率安全评定。

[22] 在概率分析中，系统通过简单地取其个别失效概率的乘积而被视为完全独立的。

5. 仪器仪表和控制功能、系统和设备的安全分级

5.1. SSR-2/1（Rev.1）[1]要求 18 规定：

> “核电厂安全重要物项的工程设计规则必须明确确定，并且必须符合相关国家或国际程序和标准以及成熟的工程实践，同时适当考虑到它们与核电技术的相关性。”

5.2. SSR-2/1（Rev.1）[1]要求 22 规定：“必须确定所有安全重要物项并根据其功能和安全重要性对其进行分类。”

5.3. SSR-2/1（Rev.1）[1]第 5.34 段指出：

> “划分安全重要物项的安全重要性必须主要基于确定性方法，并酌情辅以概率方法，同时适当考虑以下因素：
>
> (a) 该物项要执行的安全功能；
> (b) 不能执行安全功能的后果；
> (c) 需要该物项执行某一安全功能的频率；
> (d) 假想始发事件后需要该物项执行安全功能的时间或时间段。”

5.4. SSR-2/1（Rev.1）[1]第 5.36 段指出：“必须将执行多重功能的设备划入与该设备所执行的最重要功能相一致的安全级别。”

5.5. 原子能机构《安全标准丛书》第 SSG-30 号《核电厂结构、系统和部件的安全分级》[17]就如何满足 SSR-2/1（Rev.1）[1]和 GSR Part 4（Rev.1）[5]确定的要求提出了建议和指导意见，以确定安全重要结构、系统和部件，并根据其功能和安全重要性对其进行分类。

5.6. SSG-30[17]建议的安全分级过程与 SSR-2/1（Rev.1）[1]提出的纵深防御概念相一致。应考虑在纵深防御不同层次执行的功能。

5.7. 对于特定的核电厂，分级过程应主要考虑：

— 核电厂的设计基准和固有的安全特点；
— SSR-2/1（Rev.1）[1]要求的所有假想始发事件列表。应考虑核电厂设计基准中所考虑的假想始发事件的发生频率。

5.8. 在确定假想始发事件列表时，应考虑安全重要物项的故障或误操作可直接导致假想始发事件的可能性，或安全重要物项在需要时的故障可使假想始发事件的后果恶化的可能性。

5.9. 应识别为实现 SSR-2/1（Rev.1）[1]要求 4 中定义的用于不同核电厂状态（包括正常运行的所有模式）的主要安全功能必需的所有仪器仪表和控制系统功能和设计措施。

5.10. 然后应根据其安全重要性对所有仪器仪表和控制系统的功能进行分类，考虑以下三个因素：

(a) 不执行该功能的后果；

(b) 要求执行该功能的假想始发事件的发生频率；

(c) 一个假想始发事件发生后，要求该功能开始运行的那个时刻或时段。

5.11. 应识别执行每个分配了安全级功能的仪器仪表和控制系统和部件，并给它们进行安全分级。应该主要根据分配给它们所执行的功能的类别进行分级。

5.12. 在确定安全级别时，应考虑采取替代措施的及时性和可靠性，以及能探测和补救该仪器仪表和控制系统中任何故障的及时性和可靠性。

5.13. 在 SSG-30[17]，根据成员国的经验，建议将功能分为三个安全类别，结构、系统和部件分为三个安全级别。但也可使用更多或更少的类别和级别，只要它们与 SSG-30[17]第 2.12 段和第 2.15 段提供的指导相一致。

6. 对所有安全重要仪器仪表和控制系统的总体建议

概述

6.1. 仪器仪表和控制系统应完全满足其设计基准的要求。

6.2. 安全级仪器仪表和控制系统的设计应避免不必要的复杂性。

6.3. 仪器仪表和控制系统的所有特点都应有利于其安全功能。

6.4. 安全级仪器仪表和控制系统设计的复杂性不应导致违反其他设计原则（如独立性、冗余性或多样性）。

6.5. 避免复杂性的目的是使仪器仪表和控制系统尽可能简单，但仍然完全符合其安全要求。需要避免复杂性的例子包括：对仪器仪表和控制系统安全功能或对其可靠性没有贡献的功能；采用不易于进行充分分析或核实的设计和实现特点；以及使用过于复杂的平台从而不利于安全的充分论证。因此，所采用的架构应该具有简单的相互作用和简单的通信链路。仔细记录和审核每个需求的合理性是避免不必要复杂性的一个有效手段。

可靠性设计

6.6. SSR-2/1（Rev.1）[1]要求 23 规定："安全重要物项的可靠性必须与其安全重要性相称。"

6.7. SSR-2/1（Rev.1）[1]要求 62 规定：

> "核电厂重要安全物项的仪器仪表和控制系统必须设计得具有与拟执行的安全功能相称的高度功能可靠性和可定期可试验性。"

6.8. SSR-2/1（Rev.1）[1]第 6.34 段指出：

> "必须尽可能实际地使用必要时包括自检能力在内的可试验性、故障安全特性、功能多样性以及部件设计和运行概念方面的多样性等设计技术，以防止某个安全功能的丧失。"

6.9. 在仪器仪表和控制系统的设计中，用于提供功能可靠性的设计特点的例子包括：随机故障容限、设备和系统的独立性、冗余性、多样性、共因故障容限、可试验性和可维护性、故障安全设计和高质量设备的选择等能力。

单一故障标准

6.10. SSR-2/1（Rev.1）[1]要求 25 规定："必须对电厂设计中所考虑的每个安全组应用单一故障标准。"

6.11. SSR-2/1（Rev.1）[1]第 5.39 段指出：“必须把误动作视为将单一故障标准[脚注省略]用于某一安全组或安全系统时发生的一种故障模式。”

6.12. 通常情况下，采用冗余性、独立性、可试验性、连续监控、环境鉴定和可维护性等概念来满足单一故障标准。

6.13. 在安全系统中存在任何一个可探测故障并叠加以下情况，每个安全组应能够执行所有动作以响应假想始发事件：

— 任何不可探测的故障，即不能通过定期试验、报警或异常指示探测的故障；
— 由单一可探测故障和不可探测故障引起的所有故障；
— 所有故障和系统误动作导致的可能影响安全组的假想始发事件，或可能由影响安全组的假想始发事件导致的所有故障和系统误动作；
— 出于试验或维护目的停用或旁通安全系统的一部分，这是是核电厂运行限值和条件所允许的。

6.14. 设计、维护、运行或制造错误导致的故障不包括在单一故障标准符合性分析中。应通过管理系统适当处理已知错误。未知错误的影响是无法预测的，因此，单一故障标准不是理解此类错误对安全组影响的有用工具。在第 4 部分中讨论了评定由于此类错误而导致的共因故障潜在后果的分析。

6.15. 不符合单一故障标准应仅限于例外情况，并应在设计文件中加以明确，并在安全分析中进行清晰论证。

6.16. 在分析低频事件（如外部危害）时，必须非常谨慎论证不符合单一故障标准是合理的。应特别考虑确保安全系统的运行和监控所需的电气系统和其他支持系统的长期可用性。

6.17. 可靠性分析、概率评定、运行经验、工程判断或它们的组合可用于确立一个基准用于在应用单一故障标准时排除对特定故障的考虑。

6.18. 维护、维修和试验活动应符合核电厂的运行限值和条件，即使在不满足单一故障标准的情况下也是如此。

6.19. 当满足单一故障标准不足以满足可靠性要求时，应提供额外的设计措施或对设计进行修改，以确保系统满足可靠性要求。

冗余性

6.20. 仪器仪表和控制系统应冗余到必要的程度，以满足仪器仪表和控制系统可靠性要求和单一故障标准。

6.21. 冗余性通常用于仪器仪表和控制系统中，以实现系统的可靠性目标，包括符合单一故障标准。除非冗余的元件也是独立的，否则冗余性不完全有效。一般而言，冗余性增加了可靠性，但也增加了误操作的概率。冗余信号的符合（“表决逻辑”）或拒绝假信号的方案通常用于获得可靠性和排除误动作之间的适当平衡。

独立性

6.22. SSR-2/1（Rev.1）[1]要求 21 规定：

> “必须酌情通过实体分隔、电气隔离、功能独立和通讯（数据传输）独立等手段防止安全系统之间或系统冗余单元之间的相互干扰。”

6.23. SSR-2/1（Rev.1）[1]第 5.35 段指出：

> “就安全系统的每个冗余单元而言，场内的安全系统设备（包括电缆和线槽）必须易于识别。”

6.24. 原子能机构《安全术语》[6]将独立设备定义为：

> “具备以下两个特性的设备：
>
> (a) 该设备执行所要求功能的能力不受其他设备运行或故障的影响；
> (b) 该设备执行功能的能力不受需要其履行功能的假想始发事件所产生后果的影响。”

6.25. 建立独立性是为了防止故障、内部危害或外部危害影响安全系统的冗余部件，也是为了防止故障或危害影响为纵深防御不同层次的系统。应考虑的故障过程包括：设计基准事故引起的故障、暴露于相同危害、系统

之间或冗余序列之间的电气连接、系统之间或冗余序列之间的数据交换，以及设计、制造、运行和维护中的共有错误。

6.26. 提供独立性的手段包括以下特点：实体分隔、电气隔离、功能独立和不受通信错误影响的独立（见第 7 部分）。设备鉴定和多样性也可支持独立性。本部分稍后将讨论这些主题（第 6.77－6.134 段）。一般而言，这些特点的组合应该被用来实现独立性目标。

6.27. 在不同安全级别的系统之间使用确保隔离的装置时，它们应是较高安全级别系统的一部分。

6.28. 用于隔离各种物理效应、电气故障和通信错误的措施不一定需要包含在所保护的设备中。用于将系统与各种不同类型的威胁隔离的措施不需要并入到同一实体装置中，也不需要位于电路中的同一位置。单一效果的隔离功能也可能由多个装置共同完成。例如，缓冲存储器可以提供针对数据通信中的错误的隔离，以防止数据由一个序列直接写入另一个序列，有效性检查由不同设备中的处理器提供，以确保不从缓冲器读取数据，除非数据满足有效性、正确性和真实性标准。

6.29. 应论证为满足独立性要求而提供的设计措施的充分性。

实体分隔

6.30. 实体分隔的用途如下：

— 实体分隔可防止由于内部危害的影响而导致的共因故障。关注的内部危害包括火灾、飞射物、蒸汽喷射、管道甩动、化学爆炸、水淹和邻近设备的故障；

— 实体分隔可用于防止在正常、异常或事故工况下的共因故障、事故的影响（包括所有设计基准事故）或内外部危害的影响；[23]

— 实体分隔可减少因具有局部影响的外部事件（如飞机碰撞、龙卷风或海啸）造成共因故障的可能性；

[23] 实例包括衰减电磁干扰影响的空间，以及经过不同核实水平的系统和部件之间的隔离。环境验证、抗震验证和电磁验证也可单一使用，或与实体分隔一起使用，以防止事故、内部危害或外部危害的影响。

— 实体分隔可减少冗余设备在运行或维护过程中发生意外错误的可能性。

6.31. 属于安全系统的物项应与较低安全级别系统中的物项实体分隔。

6.32. 安全组的冗余部分相互之间应实体分隔。

6.33. 当传感器或执行机构紧密地布置在一起时，冗余物项之间完全的实体分隔可能是现实的，例如控制棒驱动器或容器内仪器仪表可能是此类情况。

6.34. 一些区域因为设备或布线的会聚可能出现分隔困难，例如：

— 安全壳贯穿件；
— 马达控制中心；
— 开关装置中心；
— 电缆分布间；
— 设备间；
— 主控制室及其他控制室；
— 核电厂过程计算机。

6.35. 如果无法进行适当的实体分隔，则应尽可能在可行范围内提供分隔，并应论证例外情况（见第 6.43 段）。

6.36. 实体分隔是通过距离、屏障或者它们的组合来实现的。

6.37. 原子能机构《安全标准丛书》第 NS-G-1.7 号《核电厂设计中的内部火灾和爆炸防护》[20]和第 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》[21]提供了关于火灾和其他内部危害防护的补充指导。

电气隔离

6.38. 电气隔离用于防止一个系统中的电气故障影响连接的系统或系统中的冗余元件。

6.39. 安全系统和部件应与较低安全级别的系统和部件电气隔离。

6.40. 安全组的冗余部分相互之间应电气隔离。

6.41. 提供电气隔离的装置应防止施加于装置一侧的最大可信电压或电流瞬变、接地、开路和短路导致相连的安全电路的运行不可接受的劣化。

6.42. 电气隔离措施的实例包括：不存在电气连接、提供隔离的电子装置、提供光隔离的装置（包括光纤）、继电器、隔离距离和内部机械结构，或这些措施的组合。

相关电路

6.43. 当在安全电路和较低安全级别的电路之间提供足够的实体分隔或电气隔离不可行时，较低安全级别的电路（此处称为“相关电路”）：

- 应进行分析或试验，以证明该关联并没有不可接受地降低与其相关的安全级别电路；[24]
- 应规定作为与之相关的安全序列的一部分；
- 应与其他部件实体分隔，分隔程度和与其相关的安全序列电路的分隔程度相同。

功能独立

6.44. 功能独立是指当一个系统所需功能的成功完成不依赖于另一个系统的任何行为（包括故障或正常运行）或来自另一个系统的任何信号、数据或信息时所存在的一种状态。功能独立是实现一个系统与另一个系统隔离的一种手段。功能独立也可用作冗余设备之间实现隔离的一种手段。

6.45. 功能独立由架构设计和对功能之间共享数据的谨慎处理来支持。架构考虑在第 4 部分中进行了描述。下面讨论共享数据的处理。

6.46. 来自较低安全级别的仪器仪表和控制系统的输入不应对安全系统执行其安全功能的能力产生不利影响。

6.47. 然而安全系统可以依赖于来自非安全级的维护系统的输入，例如，用于执行维护、软件更新、试验或用于设置配置数据的系统。此类输入通常在受上述活动影响的序列离线时进行，并在数据输入后对输入进行核实。

[24] 例如，与安全电路可容忍的电压相比，分析或试验可以考虑相关电路内的最大电压。

6.48. 较低安全级别的监控系统可连接到安全系统，前提是证明监控系统不会干扰安全系统。当安全系统要连接到较低安全级别的维护系统时，只有在受影响的序列或通道处于离线状态，维护系统数据的使用仅限于特定目的，以及维护系统的连接符合计算机安保计划时，才可进行连接。

6.49. 在允许进行通道级维护的情况下，应在共用一个序列的几个通道之间提供足够的隔离。

6.50. 应规定可连接维护系统的核电厂运行模式。

6.51. 安全系统与较低安全级别系统之间的数据传输应设计成，较低安全级别系统中的可信故障不会妨碍任何与之相连的安全系统完成其安全功能。

6.52. 安全组的冗余元件之间的数据通信应设计成使得发送部件中的可信故障不会妨碍与之连接的元件满足要求。

6.53. 在计算机系统中，当较高安全级别的基于计算机的系统向较低安全级别的系统提供数据，通常使用单向的，广播式数据通信。实施单向特点的硬件特性应被作为确保这种单向通信的手段，例如，使用仅连接到较高安全级别系统中的发射机且仅连接到较低安全级别系统中接收机的链路。

6.54. 在经认证的情况下，信号可通过单一模拟或二进制信号线路从较低安全级别的系统发送到较高安全级别的系统，前提是：

— 第 6.51 段的建议仍然满足；
— 对较低安全级别系统中可能导致安全级部件误驱动的潜在故障进行了评定，并表明是可以接受的。

6.55. 当安全系统执行机构根据来自其他系统的信息（包括较低安全级别的信息）执行操作时，应确保来自其他系统的不正确数据不会妨碍安全功能。通常通过使用优先级逻辑来实现，优先级逻辑给来自安全系统内的数据和命令以优先权。

6.56. 第 7.52—7.59 段就保护和控制系统使用公共信号输入的情况提出补充建议。

多样性

6.57. 在证明基于计算机的系统或使用复杂硬件功能、复杂硬件逻辑或复杂电子部件系统的可靠性方面可能会出现困难。如果不可能证明仪器仪表和控制系统执行的功能具有足够的可靠性，则可以使用多种不同的仪器仪表和控制设备来增加基本安全功能达到的置信度。期望的多样性类型在不同国家有很大的差异。

6.58. 是否在设计基准事故工况下使用多样性来完成基本安全功能的决策应进行论证。

6.59. 如果提供多样性是为了应对潜在的共因故障，应考虑使用一种以上的多样性。

6.60. 不同类型多样性的例子包括：

— 设计多样性：通过使用不同的设计方法来解决相同的或者类似的问题；
— 信号多样性：通过可以根据不同核电厂参数值触发安全动作的系统实现；
— 设备多样性：通过采用不同技术的硬件实现（例如，模拟设备对数字设备、固态设备对电磁设备、计算机设备对基于现场可编程门阵列的设备）；
— 功能多样性：通过采取不同动作以实现相同安全结果的系统来实现；
— 开发过程的多样性：通过使用不同的设计组织、不同的管理团队、不同的设计和开发团队以及不同的实施和试验团队来实现；
— 逻辑多样性：通过使用不同的软硬件描述语言、不同的算法、不同的逻辑功能时限和不同的逻辑功能排序来实现。

6.61. 在提供多样性的情况下，应证明选择的多样性类型达到了所宣称的共因故障缓解效果。

6.62. 并不总是需要在隔离的系统应用多样性。例如功能多样性和信号多样性可在一个系统内应用。

6.63. 多样性的措施还包括避免在多样性应用中存在潜在共性特征，例如类似的材料、类似的部件、类似的制造过程、类似的逻辑、运行原则的细微相似性或共同的辅助设施。例如，不同的制造商可能使用同样处理器或认可同样操作系统，从而潜在地引入一些共因故障模式。考虑这种可能性，对多样性的要求仅基于不同名称的制造商或型号的差异是不够充分的。

故障模式

6.64. SSR-2/1（Rev.1）[1]要求 26 规定："必须酌情将故障安全设计概念纳入安全重要系统和部件的设计中。"

6.65. 任何仪器仪表和控制部件的失电，或者任何一个故障（该故障模式是已知的和编写成文件）应将系统置于已证明安全可接受的预定状态。

6.66. 确保故障使系统处于安全状态的方法包括如下的设计：系统失电时进入安全状态，或者使用"监视定时器"探测到设备不再执行其设计功能时将系统置于安全状态。

6.67. 在应用这些实践时，应用第 6.65 段的指导意见时应考虑到故障安全设计装置本身的故障。

6.68. 仪器仪表和控制系统和部件的非系统性故障模式应是已知的并编写文件。

6.69. 了解部件的故障模式对于将故障安全概念应用于系统是非常重要的。确定控制系统故障不会导致超出安全分析范围的事件也很重要。

6.70. 软件错误可能导致的故障是很难预测的。然而，为了确定设备终端出现可能的故障状态，并不需要知道软件是如何发生故障的。一个选择是识别可能的故障模式并将其归为一组可管理的可能发生的事项（例如错误输出、延迟输出和冻结输出）。

6.71. 在硬件或软件设计中，最可能由系统性原因导致的故障模式基本上是不可预测的。因此，故障安全设计的概念对于处理由这些原因引起的故障是无效的。严格遵守的开发过程（见第 2 部分）、危害分析（第 2.56－2.65 段）、纵深防御概念的应用（见第 4 部分）和多样性的应用（见第 6.57－6.63 段）是更有效的减少这类原因的数量和处理剩余原因影响的工具。

6.72. 仪器仪表和控制部件的故障应通过定期试验或自诊断来探测，或通过报警或异常指示来自揭示。

6.73. 故障最好是自揭示的。故障自揭示的机制不应使系统处于不安全状态或导致安全系统的误启动。

6.74. 在评定与单一故障标准的一致性时，应假设不能通过定期试验、警报或异常指示探测到的任何已识别故障与单一故障同时存在。应探测并揭示自测功能、自诊断功能或自报警功能本身的故障。

6.75. 一个部件的故障应尽可能不导致任何安全系统的误驱动。

6.76. 重新启动或恢复安全仪器仪表和控制系统或部件的电源时，除响应有效的安全信号外，应将输出初始化在预定的安全工况。

设备鉴定

6.77. SSR-2/1（Rev.1）[1]要求 30 规定：

> “必须实施安全重要物项核实计划，以核实核电厂的安全重要物项在其设计寿命期间始终能够在必要时以及在当时发生的主要环境条件下执行预定功能，同时在维护和试验期间适当考虑到电厂工况。”

6.78. 仪器仪表和控制系统和部件应针对其使用寿命内预期的功能进行鉴定。

6.79. 仪器仪表和控制部件的鉴定应包括其软件、硬件描述语言和过程接口（如有）。

6.80. 鉴定应提供与系统或部件的安全重要性相称的可信度。

6.81. 鉴定程序应解决影响每一系统或部件是否适合其预定功能的所有主题，包括：

- 功能和性能的适用性和正确性；
- 环境鉴定；
- 对内外部危害影响的鉴定；
- 电磁兼容鉴定。

6.82. 设备鉴定应基于以下方法进行选择：

— 使用符合公认标准的工程和制造工艺；
— 可靠性证明；
— 以往类似应用方面的经验；
— 型式试验；
— 对所提供的设备进行试验；
— 根据有关工况下的试验数据或运行经验用合理工程外推法进行分析；
— 对制造商生产过程的评价；
— 制造过程中的部件视察。

6.83. 一般来说没有必要应用所有提到的方法。所选方法的特定组合将取决于所考虑的系统或部件。例如，在对先前存在的物项进行鉴定时，可以更多地强调过去的经验和分析，以弥补在工程和制造过程中完整记录的核实和验证的缺失。

6.84. 用于设备鉴定的方法或方法组合应是合理的。

6.85. 如果使用运行经验来支持设备鉴定，则应证明该经验与目标应用的建议用途和环境有相关性。

6.86. 对于安全系统，基于运行经验作为鉴定证明是不够充分的，因此应与所供设备的型式试验和试验以及制造商生产过程的评价或制造过程中部件的视察相结合。

6.87. 作为设备鉴定证据的一部分的分析应包括对所用方法、理论和假设的论证。

6.88. 例如，用于设备鉴定的数学模式的有效性可基于实验数据、试验数据或运行经验的基准来论证。

6.89. 应在每个已安装的安全重要系统和部件以及合理的鉴定证据之间建立可追溯性。

6.90. 这不仅包括部件本身的可追溯性，还包括鉴定配置和安装配置之间的可追溯性。

适宜性与正确性

6.91. 设备鉴定程序应证明仪器仪表和控制系统和部件的设计符合仪器仪表和控制系统和部件的设计基准和设备规范说明中包含的所有功能要求、性能要求和可靠性要求。

6.92. 功能需求的例子包括应用程序所需的功能、支持系统或设备可操作性所需的功能、对运行人员接口的要求以及与输入/输出量程相关的要求。

6.93. 性能要求示例包括准确度、分辨率、量程、采样速率和响应时间要求。

6.94. 可靠性要求的例子包括最小平均故障间隔时间要求（MTBF），以及对故障安全行为、独立性、故障探测、可试验性、可维护性和使用寿命的要求。

6.95. 设备鉴定程序应证明实际设计和竣工验收的系统及安装部件正确实施了合格的设计。

环境鉴定

6.96. 在本“安全导则”中，环境鉴定是指温度、压力、湿度、化学爆炸、辐照、水淹、电磁现象和老化机制的鉴定，这些因素影响部件在这些条件下的正确运行。

6.97. 系统和部件的设计应考虑到与正常运行相关的环境条件、预计运行事件和要求其运行假想事故的影响，并与之相适应。

6.98. 在规定的环境条件范围内，部件应明确能满足所有要求。

6.99. 设备鉴定要求、过程和方法详见参考文献[22]。

仅暴露在和缓环境的部件

6.100. 如果在事故期间任何时刻，仪器仪表和控制部件工作环境条件的严酷程度与正常运行期间没有显著差异（所谓的“和缓环境”），其环境鉴定可以基于一份清晰的规范说明了核电厂各个运行状态下特定环境条件的功能

需求规格书，并结合来自供应商的产品合格证或一份对部件能够在规定的环境条件下执行其要求功能的独立评价。

暴露在严酷环境的部件

6.101. 在事故期间任何时刻部件要求运行的工作环境条件比正常运行时的条件严峻得多（所谓的“严酷环境”），其环境鉴定应证明该部件在其合格寿命终止时能够在规定的全部工作环境条件范围内完成其安全功能。

6.102. 证明部件在其合格寿命终止时能够按要求运行，涉及显著老化效应（如辐照和热老化）的解决，以表明在合格寿命终止时仍能保持所需的功能性。通常情况下，这包括酌情采取进一步的保守实践，以允许不期望的老化机制。

6.103. 在设备鉴定程序的规格说明中，应解决工作环境条件最严酷的可信组合，包括工作环境条件之间的协同效应。

6.104. 如果有必要对不同的环境条件分别独立试验（例如，对辐照效应和温度效应独立进行试验），则应说明进行这些试验的顺序是正确的，能够合理模拟组合工作环境造成的退化。

6.105. 最严格的环境鉴定方法可能只需要应用于安全级部件。

6.106. 要求在严酷环境中运行的安全级部件的环境鉴定应包括型式试验。

6.107. 当提供保护屏障用于隔离设备使其免受可能的环境影响时，这些屏障本身应该通过质量鉴定程序以验证其充分性。

内外部危害

6.108. 核电厂的设计基准和安全分析将识别电厂为了运行或安全需要承受的内外部危害（如火灾、洪水和地震事件），且需要针对这些灾害进行防护或系统鉴定。电厂设计基准和安全分析还将识别由工程决策或缺陷等系统性原因造成的、可能导致安全功能退化的危害；应识别相应的系统限值，以防止安全功能退化。

6.109. 应根据 NS-G-1.7[20]指导，对仪器仪表和控制系统及其部件进行防火和防爆保护。

6.110. 应根据 NS-G-1.11[21]指导，保护仪器仪表和控制系统和部件免受其他内部危害的影响。

6.111. 应根据原子能机构《安全标准丛书》第 NS-G-1.6 号《核电厂的抗震设计和验证》[23]指导，仪器仪表和控制系统和部件应按能够承受地震危害进行设计和鉴定。

6.112. 应根据原子能机构《安全标准丛书》第 NS-G-1.5 号《核电厂设计中的非地震外部事件》[24]指导，保护仪器仪表和控制系统和部件应能防护它外部危害，或按能够承受其他外部危害进行设计和鉴定。

电磁鉴定

6.113. 电磁兼容性是指一个系统或部件在其电磁环境中令人满意地工作而不对该环境中的任何设备造成无法忍受的电磁干扰的能力。物项对电磁干扰的敏感度和电磁干扰对电磁环境（发射）的贡献都是电磁兼容性的一部分。

6.114. 电磁干扰包括射频干扰，本“安全导则”中使用的电磁干扰包括浪涌，例如由开关瞬变引起的电压尖峰。

6.115. 电气和电子系统和部件的不受干扰的运行取决于部件在其运行环境下的电磁兼容性，即部件承受由其周边或与其连接的部件引起的干扰的能力。

6.116. 电磁干扰的主要来源包括开关柜、断路器或熔断器分断时的故障间隙电流；无线电发射机引起的电场；自然源，如雷击或太阳风暴；以及核电厂内部或外部的其他人为引起的源。

6.117. 仪器仪表和控制系统和部件的电磁鉴定取决于系统和部件设计的组合，以最大限度地降低电磁噪声与仪器仪表和控制系统件的耦合，进行试验以证明部件能够承受预期的电磁辐射以及电磁发射在可容忍水平内。

6.118. 将电磁噪声的产生和耦合降至最低的技术包括：

— 抑制源处的电磁噪声；
— 将仪器仪表和控制系统信号电缆与电力电缆分隔和隔离；
— 保护设备和电缆不受外部磁场和电磁辐射的影响；

— 电磁噪声在耦合到敏感电子电路之前应先进行滤波；
— 电子设备与地电位差的清除或隔离；
— 电气和仪表及控制设备、电缆通道、机柜、部件和电缆屏蔽层的正确接地。

6.119. 适当的安装和维护实践对于这些规定的合理应用和持续有效性至关重要。

6.120. 应确定安全系统和部件的电磁兼容性的详细要求，并应证明其与要求的一致性。

6.121. 工业环境电磁兼容性国际标准可作为鉴定要求的基准，但必须在必要时加以补充，以覆盖可能要求更苛刻的核电厂所特有的电磁兼容性需要。电磁兼容性要求的确定需要考虑仪器仪表和控制部件暴露于重复性瞬变（如感性负载关断和继电器振铃）和高能浪涌（如电源故障和雷电）的可能性。

6.122. 通常需要对核电厂每台机组进行具体分析以建立各机组仪器仪表和控制部件的电磁环境。这些分析用于判断每个仪控部件电磁兼容能力的适当性。

6.123. 安全重要设备和系统，包括相关的电缆，其设计和安装应能保证其承受所处场所的电磁环境。

6.124. 在设计仪器仪表和控制系统和部件时，应考虑电磁干扰的方面包括：

— 电磁干扰的发射和抗扰度；
— 通过电缆的电磁发射干扰和传导干扰；
— 静电放电；
— 开关瞬态和浪涌；
— 核电厂使用的无线系统和设备[25]，以及那些维修、维护和测量设备的发射特征。

6.125. 在某些敏感设备附近设立禁区，限制无线设备和其他便携式电磁干扰源（如焊接设备）的操作。

[25] 无线系统和设备包括例如移动电话、无线电收发机和无线数据通信网络。

6.126. 设备鉴定程序应证明，安全级仪器仪表和控制部件有在暴露于电磁干扰和抗浪涌运行包络限值时能够完成其安全功能的能力。

6.127. 应对所有核电厂设备的电磁发射的辐射和传导确定限值。

6.128. 核电厂内的任何电气或电子设备都会对电磁环境产生影响。因此，限制电磁发射的需求应该应用于所有电厂设备，而不仅仅是安全重要设备。

6.129. 单一部件的发射限值应做到：在系统和设备的所有模式和状态下，包括模式或状态的切换以及劣化工况，在运行环境中产生的发射干扰在每个部件能够承受的电磁干扰的安全（无危害）包络限值之内。

6.130. 设备鉴定程序应证明所有核电厂设备的电磁发射都在规定的限值内。

6.131. 设备和系统，包括相关的电缆和电源，在设计和安装时应适当限制核电厂设备之间电磁干扰的扩展（通过发射和传导）。

6.132. 当多个仪器仪表和控制系统连接到同一电源时，电磁鉴定应评定电磁干扰的传输路径。

6.133. 仪表电缆应为双绞线并加以屏蔽，以最大限度地减少电磁干扰和静电干扰。

6.134. SSG-34[7]提供了接地、电缆选择和电缆敷设的建议，以减少电磁干扰的产生和扩展。

应对老化和技术老化的设计

6.135. SSR-2/1（Rev.1）[1]要求 31 规定：

> “必须确定核电厂安全重要物项的设计寿命。在设计中必须提供适当的裕度，以便适当考虑相关老化、中子脆化和磨损机理以及与年龄有关的降质可能性，从而确保安全重要物项在其整个设计寿命期间执行其必要安全功能的能力。”

6.136. SSR-2/1（Rev.1）[1]第 5.51 段指出：

“核电厂的设计必须适当考虑所有运行状态中归因于某一部件的老化和磨损效应，这些状态包括试验、维护、维护性停堆、假想始发事件期间的电厂状态和发生假想始发事件后的电厂状态。”

6.137. SSR-2/1（Rev.1）[1]第 5.52 段指出：

“必须对监控、试验、取样和视察做出规定，以便评定在设计阶段所预测的老化机理和帮助确定电厂的意外行为或使用过程中可能发生的降质。”

6.138. 电气和电子系统及部件的合格使用寿命可能大大低于核电厂的寿命。

6.139. 与老化相关的退化损害了部件在严酷环境条件下的运行能力，这种退化可能在正常工况下部件的功能能力受到明显影响之前就出现了。

6.140. 应在设计时识别可能对仪器仪表和控制部件产生重大影响的老化机制以及跟踪这些机制影响的手段。

6.141. 要确定老化的潜在影响，首先需要了解各种仪器仪表和控制部件的相关老化现象。

6.142. 仪器仪表和控制部件老化最常见的原因是暴露在高温或辐照下。然而在适用第 6.140 段的指导时，应考虑到与特定部件相关的其他现象（如微电路中的电迁移、“锡须”的形成、机械振动或化学降解）的可能性。

6.143. 维护程序应包括识别任何退化（老化）趋势的活动，包括探测可能导致设备无法完成其安全功能的前兆。

6.144. 监控技术的例子包括：

— 以合理的时间间隔，对因老化导致性能退化的核电厂的典型部件或典型单元进行试验；
— 目视检查；
— 运行经验分析。

6.145. 应对老化影响的手段包括：

— 在合格寿命终止前更换部件；

— 考虑老化的影响，调整功能特征（例如重新校准）；
— 有减缓老化过程效果的维护程序或环境条件的修改。

6.146. 应确定在严酷环境中执行安全功能所需的安全级部件的合格寿命。

6.147. 安全级部件应在其合格寿命终止前更换。

6.148. 在役鉴定可表明，一个部件的合格寿命是有效的，或表明与已通过试验、分析或经验确定的合格寿命不同。来在役鉴定的信息可用于增加或减少部件的合格寿命。

6.149. 应在设计过程中确定仪器仪表和控制系统及部件的预期使用寿命和预期的技术老化，并将其传达给营运组织。

6.150. 对仪器仪表和控制系统和部件的使用寿命的评价和预计技术老化日期的估计，为营运组织提供了与供应商订立长期协议、计划采购额外备件和计划及时更换过时物项所需的信息。

6.151. 估计某些仪器仪表和控制系统可能会因为老化或技术老化导致其使用寿命大大短于核电厂的使用寿命。因此，提供便于安装并切换到替换系统的设施可能是合理的。这类设施可能包括新设备的安装和相关电缆预留的空间。

6.152. 原子能机构《安全标准丛书》第 NS-G-2.12 号《核电厂的老化管理》[25]提供了关于老化管理和技术老化管理的补充指导。它包括设备鉴定方案和老化管理计划之间接口的说明。

接近安全重要系统的控制

6.153. SSR-2/1（Rev.1）[1]要求 39 规定：“必须防止擅自接触或干扰包括计算机硬件和软件在内安全重要物项的情况。”

6.154. 参考文献[26－28]就核电厂安保，和核安全与核安保的协调提供了指导。

6.155. 为防止未经授权的接近以减少发生错误的可能性，应限制对仪器仪表和控制系统中设备的接近。

6.156. 有效的方法包括行政措施和实体安保措施的适当结合（外壳加锁、房间加锁和外壳门上设报警装置）。

6.157. 特别值得关注的方面是对设定值调整和校准调整以及配置数据的访问，因为它们对防止运行和维护中的错误使系统的性能退化具有重要意义。

6.158. 第7.103－7.130段为数字化系统的电子式接近控制提供了补充指导。

运行期间的试验和可试验性

6.159. SSR-2/1（Rev.1）[1]要求29规定：

> “核电厂安全重要物项的设计必须使得能够对它们进行所需的校准、试验、维护、维修或更换、视察和监控，以确保它们执行其功能的能力及维持它们在设计基准中规定的所有工况中的完整性。”

6.160. SSR-2/1（Rev.1）[1]第6.35段指出：

> “安全系统的设计必须使得能够在电厂运行时定期试验安全系统的功能，包括有可能单独试验各个通道以探测故障和冗余性的丧失。设计必须允许对传感器、输入信号、最终启动器和显示器进行所有方面的功能试验。”

试验装置

6.161. 仪器仪表和控制系统应包括试验装置。

6.162. 永久连接到安全系统的试验装置本身就是安全系统，除非它们符合第6.25－6.56段中有关独立性的建议。

6.163. 安全系统设备的试验和校准应能在所有正常运行模式下进行，包括功率运行，同时保持安全系统完成其安全功能的能力。

6.164. 为了达到安全系统所要求的可靠性，核电厂运行期间通常需要进行定期试验；然而如果这样做会危及电厂的安全，需要避免在功率运行期间进行试验。功率运行期间的试验和校准的好处应与它们可能对电厂安全造成的不利影响相平衡。

6.165. 如果不具备在功率运行期间试验安全系统或部件的能力，则应确保：

— 应明确受影响功能的可靠性在两次试验之间的时间间隔内是可接受的；
— 应证明未经试验的部件的准确度和稳定性在试验间隔期间满足要求；
— 应考虑提供手段，将未经试验的仪器通道的测量结果与其他装置进行比较（例如，将中子功率与热功率进行比较）；
— 应提供在停堆期间试验未经试验的系统或部件的能力。

自动试验、自监督和监控

6.166. 仪器仪表和控制系统应具有自监督或监控的功能，以便定期验证其是否连续正确运行。

6.167. 这些特点应包括检查输入合理性的手段。

6.168. 数字化安全系统应包括“安全状态”特点，如“监视定时器”。

6.169. 通过系统或部件设计来自揭示这些系统或部件的故障，是实现本“安全导则”第 6.166 段指出的一个手段。

6.170. 试验设施包括为执行试验和相关试验顺序而提供的硬件和软件，无论它们是手动触发还是自动触发。

6.171. 应设置警报以提示安全系统冗余性的丧失。

6.172. 当通过自监督探测到系统或设备故障时，应采取预定动作。

在试验期间保留仪器仪表和控制功能

6.173. SSR-2/1（Rev.1）[1]第 5.46 段指出：

> “在计划在功率运行期间对安全重要物项进行校准、试验或维护的情况下，各系统的设计必须使得能够在不显著减少安全功能的性能可靠性的情况下执行这些任务。必须在设计中纳入有关在停堆期间进行安全重要物项校准、试验、维护、维修、更换或视察的规定，以便能够在不显著减少安全功能的性能可靠性的情况下执行这些任务。”

6.174. 仪器仪表和控制系统的试验装置（手动装置和自动装置）应确保试验不会对仪器仪表和控制系统完成其安全功能的能力产生不利影响，并将误触发安全动作的可能性和试验对核电厂可用性的其他不利影响降至最低。

6.175. 试验安排既不应该损害安全系统的独立性，也不应该引入共因故障。

6.176. 试验安排包括程序、试验接口、已安装的试验设备和内置试验设施。

试验接口

6.177. SSR-2/1（Rev.1）[1]第 5.45 段指出：

> “电厂布置必须做到便于进行校准、试验、维护、维修或更换、视察和监控活动，而且这些活动能够根据相关国家和国际程序和标准进行。这类活动必须与将执行的安全功能的重要性相适应，必须在不对工作人员造成不适当的过量照射的情况下进行。”

6.178. 用于试验仪器仪表和控制系统和部件的措施应具有以下特征：

— 应具有适当的试验接口[26]和状态指示手段；
— 运行时应使设备的故障易于探测；
— 应具备防止未经授权接近的设施；
— 试验人员及试验设备应易于接近这些装置；
— 应具备必要的通讯设施，以支持试验；
— 它们的位置应使试验或接近试验地点都不会使运行人员暴露在危害环境[27]。

---

[26] 比如能够引入模拟过程工况或电信号的试验接口。

[27] 在确定试验装置的位置时，要考虑到的因素包括：
- 将各传感器放在能就地试验和校准这些传感器的位置；
- 将各种试验装置和试验设备放在便于试验这些设备的位置；
- 由于电厂或管理的因素可能会使试验设备难以进入被试验部件所处位置，例如需要将设备沿着狭窄的路径运输或进出受污染的区域；
- 部件和试验连接件状态显示的便利性。

6.179. 如果被试验设备位于危害区，应提供设备以便允许从危害区之外进行试验。

试验程序

6.180. 仪器仪表和控制系统的设计应包括试验和校准程序的详细说明，以支持原子能机构有关安全导则[16、29－31]提出建议的应用。

6.181. 仪器仪表和控制系统试验程序通常包括：

- 程序目的的描述；
- 被试验的系统和通道的详细说明；
- 单一试验的频率及顺序；
- 进行试验以及试验间隔的理由及论证，；
- 所需文档和报告的描述；
- 试验通过或失败的标准，以及处理不符合这些标准的过程；
- 规定定期审核试验计划有效性的需求；
- 用于控制试验进行的各项试验程序的详细说明。

6.182. 应论证试验和校准的范围和频率符合功能要求和可用性要求。

6.183. 试验程序应验证在试验期间和完成之后满足以下条件：

- 系统总体功能能力没有退化；
- 安全级仪器仪表和控制系统继续满足其功能和性能要求。

6.184. 在试验程序中，试验应按顺序排列，以便能够立即评定正在试验的系统或部件的总体状况，而无需对其他部件或系统进行进一步试验。

6.185. 试验程序的实施不应该引起任何核电厂部件发生超出设计规定的退化。

6.186. 在执行试验程序和确定何时达到部件合格寿命末期，可能有必要考虑例如试验造成的磨损和老化。

6.187. 试验程序应提供：

- 系统或部件状态的客观信息；

— 部件退化评定；
— 协助探测退化的趋势数据；
— 系统内早期故障的指示；
— 对失败的试验做回归试验前，要求对试验的失败进行的评价是可信的，以建立系统或部件的可运行性。[28]

6.188. 试验程序应定义定期试验和校准的过程：

— 要求从传感器到执行机构的安全功能的全面检查；
— 能在现场完成；
— 确定满足设备的功能要求和性能要求；
— 进行必要程度的输入和输出功能试验，（如报警、指示器、控制动作和驱动装置的运行），以满足系统可靠性和功能的要求；
— 规定每项试验的预期结果；
— 确保试验期间核电厂的安全；
— 尽量减少误触发任何安全动作的可能性以及试验对核电厂可用性的其他任何不利影响的可能性；
— 禁止使用暂时替代的试验装置、临时跨拉线或临时修改计算机代码；[29]
— 禁止修改核电厂部件的配置参数，除非这些参数以前已被确定为服务参数；
— 尽量缩短设备停用的时间间隔；
— 在实际可行的范围内，对每个传感器进行单独试验。

[28] 在使用重复试验的结果来证明所涉及的系统或部件的可操作性之前，通常需要对试验失败的原因、根本原因和试验失败后采取的措施进行评价和记录。纠正措施可能包括部件的维护或维修，或对试验程序的修改。如果确定不需要纠正措施，则应记录原因。

[29] 试验的核电厂设备配备有为与试验设备连接而专门设计的装置，可以使用与试验设备的临时连接。若因定期试验或校准的缘故需要临时连接，则要为此类设备的连接和使用受到适当的行政控制。

6.189. 除第 6.188 段外。定义安全系统定期试验和校准过程：

— 应为单一在线试验 [30]；
— 应独立确定传感、指令、执行和支持功能的每个通道的功能要求和性能要求；
— 在不危及核电厂持续正常运行的前提下，在试验时应包括尽可能多的功能（包括传感器和驱动机构）；
— 尽可能在实际的或模拟的运行工况下完成，包括操作顺序；
— 在变量组合用于为保护系统产生一个特定信号的情况下，应试验和校准所使用的所有变量
— 应能探测冗余设备的故障 [31]。

6.190. 当单一在线试验实际不可行时，试验程序可以结合交叠试验来实现试验目的。如果没有为安全系统通道提供单一在线试验，则应提供使用交叠试验的书面论证。

6.191. 通常情况下书面论证将证明交叠试验提供完全覆盖，设备的可靠性在较长的试验间隔下是可接受的，并且任何不进行在线试验的部件将在核电厂停堆期间试验。

可维护性

6.192. 仪器仪表和控制系统的设计应包括所有系统和部件的维护计划。

6.193. 仪器仪表和控制系统和部件的设计、定位和安装应尽量减少对运行人员的风险，和便于必要的预防性维护、故障排除和及时维修。

6.194. 便于维护、故障排除和维修的设计包括：

— 避免将设备放置于在核电厂正常运行期间预计温度或湿度过高的区域；

[30] 这种在线试验将能够在触发时直接识别特定缺陷，而不需要进行试验连接或干扰在线设备或其运行超过有限的时间。

[31] 冗余设备可以是冗余序列中的设备，也可以是单一序列中的冗余设备。

— 避免将设备放置于存在高辐射水平风险的区域（见原子能机构《安全标准丛书》第 NS-G-1.13 号《核电厂辐射防护设计》[32]）；
— 应考虑完成维护活动的人员能力和限值；
— 在设备周围应该留出足够的空间，以确保维护工作人员能够在正常工作条件下完成其任务。

6.195. 如果部件位于不可接近区域，其他应对故障的策略示例包括：

— 安装备用多重装置；
— 为远程维护提供便利；
— 设备发生故障并且不可能被迅速和易于修理或更换的情况下降低功率运行的计划。

6.196. 为安全重要表控制系统维护提供的手段应该被设计成，对核电厂安全的任何影响都是可接受的。

6.197. 这类手段的典型实例有断开多重冗余序列系统中的一个序列，以及执行代替手动操作的措施。

用于因试验或维护而停用的措施

6.198. 如果进行试验或维护设施的使用会损害仪器仪表和控制系统功能，接口应该受硬件联锁，以确保在没有谨慎的手动干预的情况下，与试验系统或维护系统的相互作用是不可能的。

6.199. 设计应确保该系统不可能被粗心地留在试验或维护配置中。

6.200. 安全系统的任何单一部件或任何冗余序列的停用，不应丧失所要求的最小冗余度，除非能充分证明系统运行可靠性是可接受的。

6.201. SSR-2/1（Rev.1）[1]第 6.36 段指出：

> “在必须使安全系统或安全系统的一部分停止运行以便进行试验时，必须对在整个试验或维护活动期间所需的任何保护系统旁通作出适当的规定并予以明示。”

6.202. 应在控制室中指示安全系统或序列的部件不可操作或旁通。

6.203. 如果经常旁通或经常有意使物项不能工作，则这些指示应该是自动的。

6.204. NS-G-2.6[16]为试验和维护之后系统和设备的重返工作提供了指导。

设定值

6.205. SSR-2/1（Rev.1）[1]第 5.44(b)段指出：“核电厂设计中确定的要求及运行限值和条件必须包括……限制安全系统设定值……”。

6.206. 安全运行的运行限值和条件包括安全系统的仪器仪表和控制设定值。

6.207. 安全系统的仪器仪表和控制设定值的确定通常考虑以下几个数值：

— 安全限值：某些运行参数的限值，已经证明核电厂在这些限值内运行是安全的 [32]；
— 分析限值（设定值的）：通过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 [33]；
— 触发设定值：驱动最终设定值装置以触发保护动作的预定值；
— 允许值：定期试验时设定值可能的限值，超过该限值需要采取适当的动作。找到超过其允许值的设定值可能意味着通道没有在设定值分析的假设内执行。在这种情况下，有必要确定是否违反了运行限值和条件，如果有，需要采取什么行动来恢复通道的可运行性；
— 安全系统的设定值：为防止出现超过安全限值 [34] 的状态，在发生预计运行事件或事故工况时自动驱动保护装置的若干触发点。

---

[32] 有时给定安全限值的参数并不由仪器仪表和控制系统直接测量。

[33] 分析限值和安全限值之间的裕度考虑了仪器仪表通道的响应时间和被考虑事故引起的瞬态范围。

[34] “安全系统的设定值”在某些国家属于法律术语，可用触发设定值或允许值来表达（亦可同时用两者来表达）。原子能机构《安全标准丛书》第 NS-G-2.2 号《核电厂运行限值、条件及运行程序》[29]就确立和实现安全系统设定值作了进一步的指导。

6.208. 应评价定期试验期间测量的设定值，以验证其与先前设定的偏差与不确定度分析中使用的预期是一致的。即使没有超过允许值（例如，保守方向的偏差），但过度的偏差可能仍然表征该通道的行为不符合预期，并且设备需要维修或分析需要修改。

6.209. 图 3 说明了这些术语与测量不确定度和偏差类型之间的关系，这些测量不确定度和偏差通常在建立触发设定值和允许值的基准时考虑。

6.210. 设定值可以是一个固定值，也可以是一个取决于核电厂其他某个参数或工况变量。

6.211. 应选择用于触发安全动作的跳堆设定值，以确保在被监控变量达到其分析限值之前采取所需的缓解措施。

6.212. 安全系统的设定值应使用书面方法进行计算，该方法应在跳闸设定值和分析限值之间提供足够的裕度，以考虑测量偏差、通道偏差、不确定性以及随时间发生的这些值的任何变化。

安全重要物项的标记和识别

6.213. 在核电厂的整个生命周期的设计、安装和运行阶段都应遵循和遵守一致的、连贯的和易于理解的命名和识别所有仪器仪表和控制部件的方法，以及人-机接口名称描述的方法。

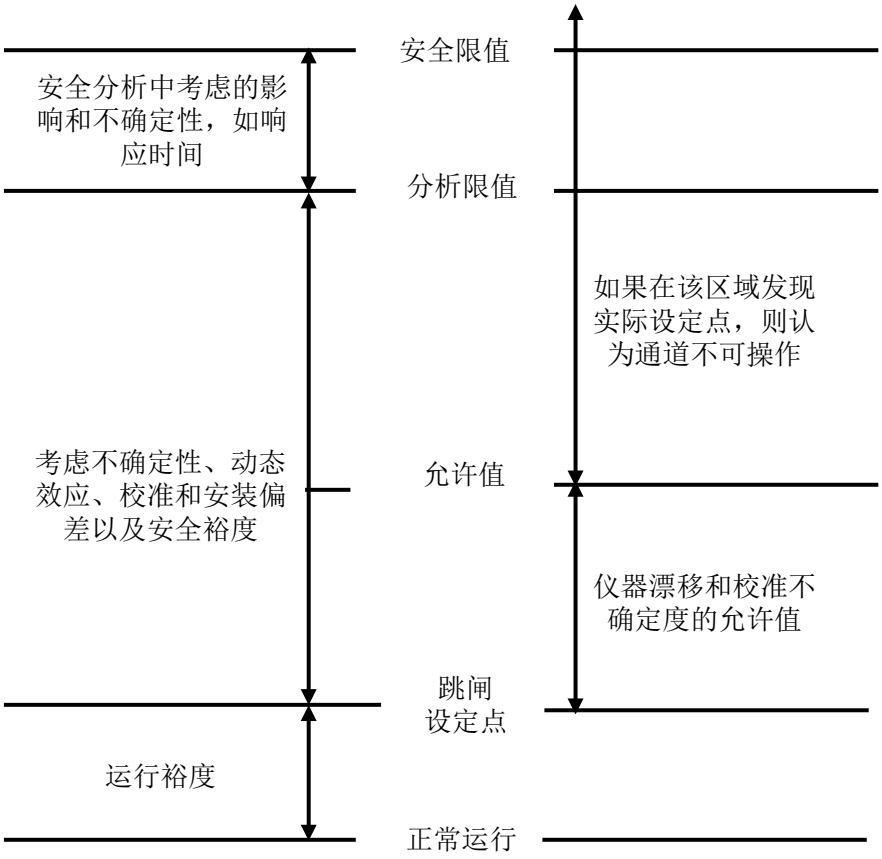

图 3. 设定点术语和在确定设定点时要考虑的偏差。

6.214. 适当的识别方案不应要求频繁参考图纸、手册或其他材料。

6.215. 一致的、易于理解的系统和部件命名和识别对工程人员、维护人员和施工人员以及标签控制、显示和指示是非常重要的。

6.216. 核电厂内的仪器仪表和控制部件一般应标明其标识信息。安装在设备或部件中的部件或模块不需要自身的标识。通常通过配置管理足以维护这些部件、模块和计算机软件的标识。

6.217. 不同安全级别的部件应易于相互区分，并易于与较低安全级别的部件区分。

6.218. 清晰标识的部件可降低由于疏忽在错误通道上中执行维护、试验、维修或校准的可能性。

6.219. 标识可以采取标签或颜色编码的形式。

7. 专用仪器仪表和控制系统和设备设计指导

传感装置

7.1. 核电厂变量的测量应符合仪器仪表和控制系统和电厂设计基准的要求。

7.2. 核电厂变量的测量即包括在某个量程范围内变量的当前值的测量，也包括离散状态的测量，如由限位开关、辅助继电器触点和温度、压力、流量或液位开关进行探测。

7.3. 核电厂变量的测量可以通过直接测量或间接测量来进行，例如基于多个测量的计算，或者基于与期望变量具有已知关系的其他数据的测量来确定变量的值。

7.4. 在实际可行的范围内，应通过直接测量来监控核电厂工况，而不应从别的更为间接的测量中推导出来。

7.5. 对每个监控变量的传感器及其量程的选择，应基于需要传感器提供测量信息的所有核电厂状态下监控变量的准确度、响应时间、运行环境和量程。在传感器和执行机构的设计中，应考虑设计裕度。

7.6. 第 4.30－4.34 段所描述的分析应包括传感器共因故障的后果。

7.7. 已识别的传感装置的共因故障薄弱点不应存在拒绝向运行人员提供控制事故和减轻其后果所需的信息和参数的可能性。

7.8. 如果使用一个以上的传感器来充分覆盖监控变量的整个范围，则应该在每个过渡点上提供从一个传感器到另一个传感器合理的重叠度，以便确保信号饱和效应或重叠效应不妨碍所需功能的完成。

7.9. 如果变量测量中的空间相关性（即，变量的测量值取决于传感器的位置）对仪器仪表和控制功能很重要，则应确定传感器的最低限度数目和位置。

控制系统

7.10. SSR-2/1（Rev.1）[1]要求 60 规定：“必须在核电厂提供适当而可靠的控制系统，以便将相关过程变量维持和限制在规定的运行范围之内。”

7.11. 将主要过程变量维持在运行限值内的自动控制是核电厂纵深防御的一部分，因此有关的控制系统通常是安全重要。

7.12. 控制系统应提供自动控制模式和手动控制模式之间的无扰切换，以及在自动模式下在线处理器和备用处理器之间的切换。

7.13. 控制功能失电时，应无扰地切换到备用设备或冻结执行机构并发出警报，然后切换到运行人员手动控制。

7.14. 自动控制系统故障的影响不应造成超出设计基准事故的验收标准或假设的工况。对于指定的系统设计，如果存在发生此类故障的可能性，如控制系统的多个误动作，则还应考虑这种故障模式。适当的设计措施（如功能分割）可用作消除控制系统看似合理的多个误动作或将其发生的可能性降低到可接受水平的手段。

保护系统

7.15. SSR-2/1（Rev.1）[1]要求 61 规定：

> “必须在核电厂提供能够探测电厂不安全工况和自动触发安全动作的保护系统，以启动实现和维持电厂安全工况所需的安全系统。”

7.16. 保护系统应监控核电厂变量并探测偏离其规定限值，以便保护系统将电厂参数维持在每个设计基准事故规定的限值内。

7.17. 整个保护系统可包括多个系统。

自动安全动作和手动安全动作

7.18. SSR-2/1（Rev.1）[1]第 6.33 (b) 段指出：

> “[保护系统]……的设计必须使用于启动安全系统的各种安全动作自动化，以便在预计运行事件或事故工况开始后的合理时间范围内无需运行人员采取行动。”

7.19. 应为保护系统所有安全动作提供自动触发和控制的手段，但那些论证过仅需手动动作的手段除外。

7.20. 通常对保护系统的绝大多数功能提供自动触发。

7.21. 可论证仅需手动动作的情况包括，例如：

- 自动程序完成后触发某些安全任务；
- 事故后将已停堆的核电厂带至长期处于安全状态；
- 假想始发事件之后很长段时间内才要求触发的某些安全动作。

7.22. 为了论证仅手动动作是可接受的，应用下列要求并应证明已满足这些要求：

- 安全系统应向运行人员提供清楚和充分的信息以便它们做出合理判断和触发所要求的安全动作；
- 运行人员备有用于安全任务的书面程序并受过培训；
- 运行人员备有足以完成要求动作的核电厂控制手段；
- 执行动作的运行人员之间的通讯线路足以保证这些行动的正确完成；
- 应进行适当的人因工程分析，以确保核电厂工况能够维持在每个假想始发事件的推荐验收标准内；
- 允许运行人员有足够的时间估计核电厂的状况和并完成所要求的动作。[35] 相关的时限分析应考虑到可用的时间和每个运行人员

[35] 对于新的设计或重大改造，建议将核电厂设计为在设计基准事故的前 30 分钟内，不需要运行人员采取行动将电厂参数保持在规定的限值内。

必要的动作所需的时间。时限分析确定安全裕度，随着安全裕度的降低，应适当考虑估计这些时间之间差异的不确定性。

7.23. 对触发和控制安全功能执行所必须的机械安全系统和单一部件，应提供手动触发手段。

7.24. 触发机械安全系统的安全功能的手动信号应尽可能在接近最终驱动装置处注入。

7.25. 安全动作的手动触发为预计运行事件和事故工况提供了一种纵深防御形式，并支持长期的事故后核电厂运行。

7.26. 机械安全系统是指例如控制杆驱动机构、应急给水、紧急堆芯冷却或安全壳隔离之类系统。

信息显示

7.27. SSR-2/1（Rev.1）[1]第 6.33(c)段指出：“[保护系统的]设计……必须向运行人员提供相关信息，供用于监控自动动作的效果。”

7.28. 保护系统应向核电厂运行人员提供保护系统功能中使用的各输入参数的测量值、各序列中各停堆功能和驱动功能的状态以及各系统的触发状态。

保护系统的传感器和设置

7.29. 向保护系统提供信号的传感器应仅通过适当的缓冲和隔离装置向其他系统提供信号。

7.30. 在实际可行的范围内使用功能多样化、冗余和信号多样化等设计技术，以防止丧失保护系统功能。

7.31. 当保护系统功能需要多个设定值时（例如，用于允许功率增加或减少），设计应确保当核电厂工况不再适合使用较低限制性的设定值时，自动使用较强限制性的设定值，或通过行政手段强制使用较强限制性的设定值。

7.32. 有时需要提供多个设定值，以实现对特定运行模式或一组运行工况的充分保护。

7.33. 如果设计提供可变设定值或在要求保护系统运行时提供改变设定值的能力，则用于改变或修改设定值的装置应当是保护系统的一部分。

7.34. 保护系统应提供一种手段，用于确定保护系统的每个通道的设定值。

运行旁通

7.35. 运行旁通或停堆闭锁逻辑可能是必要的，以便在特定核电厂工况下禁止保护系统功能的驱动动作。例如，在启动时间限制反应堆功率的停堆触发在某一点被旁通以允许功率上升，通过低功率停堆的设定值是必要的操作。

7.36. 在需要运行旁通的情况下，当核电厂接近需要运行旁通的状态时，应向运行人员提供适当的警告或警报。

7.37. 应在控制室中提供运行旁通状态的指示。

7.38. 如果不满足激活运行旁通的条件，则保护系统应自动完成以下一项动作：

— 退出已启动的运行旁通；
— 将核电厂置于运行旁通是允许的工况；或
— 触发相应的保护动作。

保护系统功能自保持

7.39. SSR-2/1（Rev.1）[1]第 6.33 (a) 段指出：

> “[保护系统]……的设计必须防止运行人员在运行状态和事故工况中采取可能损害保护系统有效性的动作，但不得阻碍运行人员在事故工况中采取正确行动。”

7.40. 应自保持保护系统触发的动作。动作一旦开始，便将一直持续，即使触发状态可能已不存在。

7.41. 通常在核电厂设备的驱动信号层级上实现保护系统触发的动作的自保持。单独测量通道的“自保持”不是必要的。

7.42. 一旦触发保护系统功能，该功能执行的所有动作都应完成。

7.43. 第 7.42 段的指导并不是用来限制由保护系统驱动的安全设备的电气保护。SSG-34[7]就安全重要物项的电气保护提出了建议。

7.44. 当保护系统功能复位时，驱动的设备不应返回正常状态，除非通过特定的、慎重的运行人员动作。

7.45. 复位安全功能的设施应是安全系统的一部分。

误触发

7.46. 保护系统的设计应在实际可行的范围内尽量减少保护系统产生误触发或误动作的可能性。

7.47. 保护系统功能的误触发可能导致：

— 设备承受不必要的应力，缩短核电厂的寿命；
— 对其他安全动作的需要；
— 运行人员对设备的信心受损，可能随后导致对正确信号的轻视；
— 核电厂生产能力丧失。

7.48. 保护系统的误触发不应使核电厂处于不安全状态。

7.49. 如果保护系统的误触发或误驱动可能导致需要保护功能的核电厂状态，那么应通过由保护系统不响应误驱动且未受误驱动影响的部分或其他安全系统触发和执行的动作来维持安全工况。

保护系统与其他系统之间的相互作用

7.50. SSR-2/1（Rev.1）[1]要求 64 规定：“必须以通过分隔、避免互连或实施适当的功能独立性来防止核电厂保护系统和控制系统之间的相互干扰。”

7.51. SSR-2/1（Rev.1）[1]第 6.38 段指出：

> “如果信号由保护系统和控制系统共用，则必须确保其分隔（如通过适当的去耦合），并须将信号系统作为保护系统的一部分进行分类。”

7.52. 当保护系统和控制系统共同使用的任何部件或信号出现故障时，保护系统应满足可靠性、冗余性和独立性全部要求。

7.53. SSR-2/1（Rev.1）[1]第 6.32(a)段指出：“保护系统的设计应……能够能够推翻控制系统的不安全动作……”

7.54. 如果假想始发事件能引起一个导致要求安全动作触发的核电厂工况的控制系统动作，那么这同一个假想始发事件不应妨碍提供必要保护系统功能的安全系统的正确动作。

7.55. 不应忽视保护系统故障本身可能是触发控制系统动作的一个假想始发事件的可能性，保护系统是控制系统所必需的。

7.56. 避免由于控制系统和保护系统之间的相互干扰导致核电厂能不正确运行的措施的示例包括：

— 为保护和控制提供独立的仪器通道；
— 在安全组中增加额外的设备，以应对潜在的干扰；
— 在核电场内设置屏蔽或替代安排，以限制假想始发事件所造成的损害；或
— 这些要素的组合，使安全组和核电厂设计足以将核电厂工况维持在可接受的限度内。

7.57. 第 7.52 段、第 7.54 段和第 7.55 段中提出的建议旨在确保在发生此类故障时，保护系统仍能完全满足其要求。满足的可靠性要求包括符合单一故障标准。

7.58. 当一个装置可由保护系统或较低安全级别的系统驱动时，用于触发保护功能的保护系统的要求具有驱动装置的优先权。

7.59. 例如，可以从控制系统发送驱动信号用于正常运行，或者如果任何来自保护系统要求超驰来自控制系统的，则允许运行人员控制来自同一驱动信息接口的所有系统元件的正常运行。

电源

7.60. 无论仪器仪表和控制系统的电源类型（如电源、气源和液压动力源）如何，都应具有符合其所服务的仪器仪表和控制系统可靠性要求的安全级别、可靠性措施、鉴定、隔离性、可试验性、可维护性和停用指示。

7.61. 要求在运行状态或设计基准事故工况下随时可用的仪器仪表和控制系统应连接到不间断电源，以便在仪器仪表和控制系统的设计基准规定的容差范围内为系统供电。

7.62. 如果运行环境需要，仪器仪表和控制系统可以通过手动操作或自动切换操作从正常电源切换至备用电源，前提是仪器仪表和控制系统的功能能够容忍相关的电源中断。通常情况下，供电系统应视为电源系统的一部分，并与其所支持的仪器仪表和控制系统具有相同的安全级别。

7.63. 一些现代仪器仪表和控制系统可以直接由直流电源供电。这对于需要不间断电力的系统是有利的，因为它消除了对电力系统中的逆变器、电动发电机或电力传输装置的需要。

7.64. 电源可以为电磁干扰提供传输路径，这些电磁干扰可能源自仪器仪表和控制系统外部，也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（见第 6.132 段）。

7.65. SSG-34[7]提供了电源和相关配电系统的建议。原子能机构《安全标准丛书》第 NS-G-1.8 号《核电厂应急电源系统的设计》[33] [36] 对其他形式的电源（如气源、液压动力源和机械动力源）提出了建议。

数字化系统

7.66. 数字化系统包括例如基于计算机的系统和用硬件描述语言编程的系统。

7.67. SSR-2/1（Rev.1）[1]要求 63 规定：

> “如果核电厂的安全重要系统依赖于基于计算机的设备，则必须制订开发和试验计算机硬件和软件的适当标准和实践并在该系统的整个使用期内特别是软件的整个开发周期执行这些标准和实践。必须将整个开发工作纳入质量管理系统的管理。”

[36] 还在编写一份关于核电厂辅助和支持系统设计的安全导则。

数字化系统功能

7.68. 使用数字化系统实现仪器仪表和控制系统功能的优势包括提供复杂功能的灵活性、改进的核电厂监控和运行人员的接口、自试验和自诊断能力、更好的便于基于强大数据记录能力的运行经验反馈环境、更低的物理尺寸和布线需求。数字化系统具有试验和自检功能，可以提高系统可靠性。

7.69. 仪器仪表和控制系统功能在数字化系统中的实现方式与在模拟系统中的实现方式不同。在数字技术中，功能组合在一个或多个处理单元中。处理单元中的组合功能可能导致非常难以分析的情况，并且处理单元的故障将导致多个功能的同时故障。另外一个功能可能通过不需要的交互降低另一个功能的性能（没有任何可识别的“失效”）。

7.70. 如果设计不正确，对这种复杂部件进行全面核实和验证可能非常困难，甚至实际上是不可能的。可能存在无法识别的错误，这些错误可能会复制到所有冗余部件中，或者扩展到基于同一平台的其他系统中，因为软件模块、编程设备或库可能对所有人都是共用的。

7.71. 在数字化系统中，输入在离散时间点采样。信号在系统部件之间周期性地传输，并且输出也周期性地产生。因此，如果数字化系统设计不正确，那么处理负载或通信负载的改变可能影响传输速度和响应时间。处理负载或通信负载的变化可能是由于核电厂参数的变化、不同的系统或电厂运行状态或设备故障造成的。

7.72. 参考文献[11]提供了关于数字化系统特性的进一步详细信息。

7.73. 数字化仪器仪表和控制系统的设计应确保系统在所有规定的运行工况和所有可能的数据负载条件下，按照要求的响应时间和准确度完成其安全功能。

7.74. 安全仪器仪表和控制系统应设计为确定性行为，因为在物项规范说明范围内的任何给定输入顺序将始终产生相同的输出和响应时间，即激励和响应之间的时间延迟具有确定的最大值和最小值。

7.75. 确保确定性响应时间可能涉及：

— 避免与过程有关的中断，使核电厂工况不会直接影响仪器仪表和控制系统必须处理的中断率；

— 在设计时静态分配资源；
— 归并由预定义限值设置的循环迭代。

7.76. 数字化系统的响应时间和准确度在本质上取决于采样速率和处理周期。在未正确设计的系统中，这些参数也可能取决于处理器的速度。

7.77. 数字化系统的设计和分析应使单一部件（例如计算机处理器）故障导致系统行为在可预测的接受范围内。

7.78. 数字化系统断电或重新启动不应导致不希望的配置数据或软件修改。

数字化数据通信

7.79. 安全化系统的数据通信应设计成具有确定的传输时间。

7.80. 确保确定性传输时间的方法可能包括：

— 预设的、基于时间的行为，即数据通信系统的动作不是由其客户端节点确定的，而是根据时间表通过设计预设的；
— 预设的数据通信负载，即通过设计预设在任何给定时间要发送的消息的大小，使得通信负载始终与数据通信系统的传输容量一致；
— 预设的数据通信模式，即在任何给定时间要传输信息的发送方和接收方是预先设计好的。

7.81. 数字化数据通信应符合第 6.25－6.56 段的建议。

7.82. 应自动检查通过数字化数据通信发送和接收的每条信息，并能自动检查出错误对其进行标记。

7.83. 错误可能包括损坏的数据、无效的数据（非计划信息）或不真实的信息（来自非预期来源的信息）。

7.84. 如果通信系统加密数据或使用专有协议，则这些设施不应阻止对错误的探测。

7.85. 应预先定义在数据通信中探测到错误时应采取的动作。

7.86. 探测到错误时可能采取的动作包括自动拒绝无效或不真实的数据、在可能的情况下更正或拒绝损坏的数据。

7.87. 设计应确保探测到数据传输和数据通信设备的故障，向运行人员提供适当的报警，并进行记录以用于性能分析。

7.88. 在数字化数据通信中存在某些类型的错误本身并不构成系统故障，因为这种错误是预期的，并且通信协议被设计成处理这些类型的错误和一定范围内的错误发生率。因此，应考虑如何适用第 7.87 段中的指导意见，规范说明哪些错误会构成数据传输失效。例如，可以规定成功传输之间的最大允许时间间隔或最大错误率的判定标准。

7.89. 用于探测和纠正错误的设施提高了信号传输的可靠性。

7.90. 错误处理和通信故障探测方法的使用范围应适用于数据的使用，适合于需要使用数据的功能的频率，并与所引入的复杂性相平衡。

安全系统中的通信功能

7.91. 如果安全相关数据的通信出现任何故障，安全系统应继续完成其安全功能或进入安全状态。

7.92. 此建议通常是通过使用两个处理器来实现的，这两个处理器通过对共享内存的仔细控制访问来共享数据。一个处理器专用于执行安全功能，另一个专用于数据通信任务。将计算和逻辑功能与通信和中断功能隔离，可防止后两种功能中的错误干扰安全计算或逻辑功能的确定性行为和时限。这种隔离（有时称为缓冲）旨在防止本序列外的通信故障和失效扩展到实现安全功能的处理器。

7.93. 安全系统接收机只应处理预定义的信息。

7.94. 要预定义的信息的要素包括信息协议、信息格式和一组有效信息。

数据通信的独立性

7.95. 本部分具体针对数字系统中的数据通信对第 6.25－6.56 段的指导意见补充。

避免共因故障

7.96. 设计和实现数据通信网络拓扑结构和对介质的访问控制，避免安全系统的常见故障。

安全序列之间的通信

7.97. 安全序列间的通信，包括通信错误或故障，不应妨碍相连的安全序列完成其安全功能。

7.98. 第 7.97 段中建议的目的是为了防止故障在序列之间扩展。通常采用数据核实（见第 7.82－7.94 段）和设置缓冲区相结合的方法。

7.99. 不应使用中央集线器或路由器的架构。在该架构中，多个安全序列的通信通过单一链路传输。

不同安全级别系统之间的通信

7.100. 不同安全级别的数字化系统和设备之间的数据通信应符合第 6.25－6.56 段的指导。触发保护系统功能的要求应具有驱动设备的优先权。

计算机安保

7.101. 参考文献[8]就在核设施实施计算机安保计划的关注点、要求和策略提供了指导，本部分作出补充。

安全与安保之间的互动

7.102. SSR-2/1（Rev.1）[1]要求 8 规定：

> “必须以统筹兼顾的方式设计和实施核电厂的安全措施、核安保措施和国家核材料衡算和控制安排，以免其相互掣肘。”

7.103. 任何计算机安保措施的运行或故障都不应对系统执行其安全功能的能力产生不利影响。如果计算机安全与安保之间存在冲突，则设计应考虑在寻求解决计算机安保计划的过程中确保安全。不应该简单的接受计算机安保解决方案的缺失，这种情况只能作为个案处理，并且只有在得到全面的论证和计算机安保风险分析的支持的情况下才可考虑接受。

7.104. 计算机安保措施的故障模式以及这些故障模式对仪器仪表和控制系统功能的影响应通过系统危害分析了解、记录和考虑。

7.105. 如果在人-机接口中实现计算机安保措施，则这些设施不应对运行人员维持核电厂安全的能力产生不利影响。

7.106. 在可行的情况下，不提供安全收益的计算机安保措施应在独立于仪器仪表和控制系统的设备中实施。

7.107. 在仪器仪表和控制系统中加入计算机安保功能会增加该系统的复杂性，并可能会使系统引入潜在的故障模式，从而挑战其可靠执行安全功能的能力，或增加误操作的可能性。

7.108. 应根据本“安全导则”第 2 部分中的建议开发包含在仪器仪表和控制系统中的计算机安保功能，并应具有与功能所在系统相同的设备鉴定水平。

7.109. 数字化系统或部件的开发过程、运行和维护应根据计算机安保计划进行，该计划应具体规定和详细说明实现计算机安保的手段。

7.110. 计算机安保计划应包括在开发仪器仪表和控制系统期间实施的适当的物理、逻辑和行政控制。

7.111. 数字化系统的开发环境和随后的数字化系统的安装、运行和维护应具备适当的措施，以防止软件或数据被蓄意或无意的入侵或损坏、恶意代码的引入、与外部网络的不正确连接和黑客攻击。

为安全重要数字化系统的控制访问

7.112. 系统和部件的所有数据连接都应置于机柜内，对机柜的访问和对机柜内部的访问都应根据第 6.156 段进行控制。

7.113. 数据连接包括网络连接、外部存储器连接以及对存储棒、闪存卡和数据磁盘等便携式介质的访问。

7.114. 应禁用未使用的数据连接。

7.115. 临时使用所需的连接，例如维护计算机的连接，在不使用时应禁用。

7.116. 禁用未使用连接的形式包括移除、物理措施或逻辑措施。

7.117. 如果使用逻辑措施作为禁用数据连接的手段，则应提供附加措施以确保连接保持禁用状态，或者探测和评价连接配置或状态的任何更改对系统可运行性的影响。

7.118. 对允许更改软件或配置数据的访问功能以及更改本身应进行监控和记录。

7.119. 监控和日志记录可以通过管理程序自动或手动执行。

7.120. 所使用的方法应被认为在不妨碍履行安保功能的情况下提供必要的安全。

7.121. 第 7.118－7.120 段不适用于控制室运行人员根据设计可对配置数据进行的更改。

与应急设施通信的安保

7.122. 来自核电厂仪器仪表和控制系统的数据可以传输到电厂场内的其他位置（例如，技术支持中心）和场外的位置（例如，应急响应组织）以支持应急响应，前提是仪器仪表和控制系统不受这些连接的不利影响。

7.123. 核电厂与技术支持中心之间以及电厂与应急组织之间的通信链接，包括用于人与人之间通信的链接，应是专用的，并应防止篡改。

7.124. 数据通信可包括关于基本安全功能状态的信息和支持应急管理的其他信息。

运行安保设施

7.125. 应考虑使用能动的计算机安保措施来探测计算机安保威胁并缓解其影响。

7.126. 仪器仪表和控制系统的能动计算机安保功能不应对安全重要功能产生不利影响。

7.127. 能动的计算机安保措施可能会增加系统的复杂性、争夺系统资源、增加误操作的可能性或引入新的故障模式。任何时候都应考虑非能动计算机安保措施的应用。

7.128. 建议仅在系统离线时使用能动计算机安保措施。对于仪器仪表和控制系统，最好离线执行扫描功能。

7.129. 计算机系统应包括定期核实和维护后核实的措施，以确保计算机安保措施配置正确和运行正常。

7.130. 应制定程序，评监查算机安保监视的结果并采取行动。

使用硬件描述语言配置的设备

7.131. 硬件描述语言配置的设备是提逻辑结构的可编程电子模块（例如，逻辑门和开关阵列），由仪器仪表和控制系统开发者定制以提供特定功能。如现场可编程门阵列。

7.132. 这种定制涉及到专门的软件工具，对实现这些功能的需求进行形式化的描述。

7.133. 本部分有关硬件描述语言配置的器件的导则应与第 2 部分的生命周期导则、本部分提供的数字化系统导则和第 9 部分提供的软件导则一起使用。适用于直接实现安全功能的设备。

7.134. 使用硬件编程设备进行应用开发应遵循满足第 2 部分建议的预定义的生命周期。

7.135. 开发计划应要求以第三方可以理解的方式对每项技术决定的合理性进行论证。

7.136. 硬件可编程设备的实施计划应规定确保每个生产出的器件符合设计要求的手段。

7.137. 硬件可编程设备的设计要求应包括时限要求，如门延时和启动时间的要求。

7.138. 硬件可编程设备和相关物项（如库、最终产品中包含的知识产权核（半导体 IP 核）和硬件定义语言）的选择应遵照已规定的和文档化的流程，以确保其适用性。

7.139. 只有在满足以下条件的情况下，才应使用知识产权：

— 使用的知识产权核应从合格的供应商处获得，这些供应商应遵照高质量的知识产权核开发流程，包括严格的工程流程、明确定义的和有用的文档，且易于整合；
— 进行评价以确保不引入危害。

7.140. 如果有必要对预先开发物项进行修改才能验收，则应在验收评审前对其进行规范说明、设计、实现和核实。

7.141. 如果所选硬件可编程设备包括辅助措施（例如，内置的自测），则应通过对包括其开发过程（以及核实过程）和其设计在内的各种元件的评价来确定此类对安全功能有贡献的设备的适用性。

7.142. 应选择鉴定过的和兼容的软件工具的标准化硬件描述语言对硬件可编程设备进行编程。

7.143. 硬件可编程设备的设计：

— 应确保硬件可编程设备的行为是确定性的。例如通过使用内部同步设计可实现确定性设计。同步设计有利于正确性（避免亚稳态问题）和可试验性，并允许充分利用软件工具的能力进行设计和核实；
— 应仅使用具有良好定义的实现和行为属性的硬件可编程设备结构。实现良好定义的实现和行为的方法包括对开发设备的形式化描述，例如寄存器传输级的描述、使用严格的语义和语法规则、使用硬件描述语言的“安全”子集以及使用预定义的语言和编码规则；
— 应在可行的范围内，支持使用基于数学定理证明的核实技术；
— 应明确处理硬件可编程设备的所有可能的逻辑用例和所有运行模式，如复位、上电和正常工作；

— 应对电源电压、温度和微电子工艺中的边界变化引起的所有可能的时限情况进行校正；
— 应确保硬件可编程设备中实现的每个功能都是可试验的。

7.144. “布线后分析”应用于证明设备的设计和实现是否符合设计供应商所定义的技术规则，以及是否符合用于实现的软件工具。

7.145. 硬件可编程设备的设计过程应整合到仪器仪表和控制系统的总体开发过程中。

7.146. 核实和验证：

— 用于验证没有对任何未规定功能进行编程，这些功能可能影响到硬件可编程设备的运行；
— 包括对硬件可编程设备中的所有信号路径的试验；
— 应对硬件可编辑设备所特有的系统特性；
— 应包括时限分析和仿真。

7.147. 应使用环境鉴定和分析来证明，使用预先开发物项或辅助措施不会降低安全重要系统完成其安全功能的能力。

软件工具

7.148. 通过使用软件工具可以获得好处，并且这些软件工具是可用的，应使用软件工具来支持仪器仪表和控制开发生命周期的所有方面。

7.149. 使用适当的软件工具可以降低在仪器仪表和控制系统开发过程中引入故障的风险，并可以提高在检查、核实和验证过程中发现故障的概率。因此，使用软件工具可以提高仪器仪表和控制系统开发过程的完整性，从而提高部件的可靠性。使用软件工具也可以带来经济效益，因为它们可以减少生产系统、部件和软件所需的时间和人力。软件工具可以用来自动检查对构建规则和标准的遵守情况，以标准格式生成适当的记录和一致性文档，并支持变更控制。软件工具还可以减少试验所需的工作量，并可以维护自动化的日志。一些特定的开发方法需要使用软件工具。

7.150. 用于开发仪器仪表和控制系统的软件工具包括：

— 提供基础设施和开发支持系统的软件工具，例如需求管理系统或整合开发环境；
— 自动电路和布线计划软件；
— 转换软件工具，如软件生成器、编译器、逻辑分析仪和将一个文本或图表从一个抽象级别转换为另一个抽象级别（通常是较低级别）的工具；
— 自动化电子设计软件工具；
— 用于核实和验证的软件工具，如静态软件分析器、自动电路试验器、试验覆盖率监视器、定理证明辅助软件、电子电路模拟器和核电厂系统模拟机；
— 编写系统配置数据的软件工具；
— 配置管理和控制软件工具；
— 用于检测已知和未知漏洞的计算机安保试验的软件工具。

7.151. 整合项目支持环境的一个关键要素是确保适当的控制和一致性。如果没有可用的软件工具，应考虑开发新的软件工具。

7.152. 使用软件工具的收益和风险应与不使用软件工具的收益和风险进行权衡。

7.153. 选择能限制出错和引入故障的机会的软件工具，但最大限度地避免或检测故障，是一个重要的方法。软件工具的使用可能以几种方式对系统开发产生不利影响。例如，用于设计的软件工具可能通过产生损坏的输出来引入故障，或者核实工具可能无法发现某些故障或故障类型。

7.154. 软件工具应选择在系统的整个使用生命周期保持可用，并应与系统开发期间使用的其他软件工具兼容。

7.155. 应确定并记录所有软件工具的功能和应用限值。

7.156. 软件工具及其输出不应在其声明的功能或应用限值之外使用，除非事先经过论证。

7.157. 例如，当需要判断时软件工具不能代替人。某些情况使用软件工具提供支持比完全自动化的流程更合适。

7.158. 应基于对软件工具的可靠性要求、软件工具的类型、软件工具引入故障或未能使用户发现现有故障的可能性以及软件工具可能对一个系统或多样性系统的冗余元件的影响程度，对软件工具进行核实和评定。

7.159. 可能影响核实和评定的必要程度的情况举例如下：

— 具有引入故障能力的软件工具应比不具有该能力的软件工具进行更加严格的核实；
— 不能使用户发现现有故障的软件工具应比不具备该功能的软件工具得到更加严格的核实；
— 当软件工具的输出得到系统性的和独立的核实时，软件工具不需要核实；
— 软件工具核实严格程度降低可能是可以接受的，如已制定措施以缓减任何潜在的软件工具故障的后果（例如，流程多样化或系统设计）。

7.160. 软件工具的核实和评定应考虑以前使用的经验，包括开发人员的经验和从软件工具使用的过程中获得的经验。

7.161. 软件工具的选择、核实和评定应该经过论证并形成文档。

7.162. 所有软件工具都应置于适当的配置管理之下。

7.163. 在基线设备、软件和硬件描述语言配置设备的开发、核实或验证过程中使用的软件工具设置应记录在开发记录中。

7.164. 这种文档不仅有助于确保最终软件的一致性，它还有助于评价错误的源头，这些错误可能存在于源代码、软件工具或软件工具设置中。有关使用的工具设置的信息对于评定由于软件工具而导致的共因故障的可能性可能至关重要。

安全应用中有限功能的工业数字化设备的鉴定

7.165. 本部分提供核电厂安全系统中使用的有限功能但尚未专门针对此类应用开发的工业数字化设备的核实导则。本导则描述了满足第 6.78－6.134 段中对此类器件的鉴定建议的方法。

7.166. 有限功能的设备具有以下特性：

— 含有预先开发的软件或可编程逻辑；
— 自主的，只执行一个概念上简单的主要功能，由制造商定义，用户不可修改；
— 被设计成不可重新编程；
— 如果是可重新配置的，则可配置性仅限于与所监控或控制的过程的兼容性有关的参数，或与所连接的设备的接口。

7.167. 所有不是“有限功能的工业数字化设备”的其他设备具有以下特性：

— 使用商用计算机（例如个人计算机、工业计算机或可编程逻辑控制器）；
— 它们是为仪器仪表和控制平台开发的；或
— 它们是专门为核工业开发的。

7.168. 验证有限功能的工业数字化设备对其预期功能的适用性和正确性应提供以下证据：

— 设备的主要功能满足应用的功能要求；
— 除主要功能 [37] 以外的其他功能的运行或故障都不能导致主要功能的不安全运行；
— 设备不应存在可以可信地导致安装在冗余或多样化的仪器仪表和控制系统中的相似元件几乎同时共因故障的系统性故障；
— 开发过程是系统的，遵循本“安全导则”第 2 部分概述的一般原则；
— 制造的质量保证足以为以后制造的相同设备或相似型号的接受提供基准。

7.169. 在其他工业领域为安全目的进行认证期间开发的信息可用作支持设备鉴定的证据。仅有认证证书是不够充分的；相反，认证过程中产生的信息可能提供价值。

[37] 除主要功能之外的功能包括，例如用于维护或配置设备的功能和预期应用不需要的功能。

7.170. 如果上述一项或多项建议未得到满足，应提供补充证据，直接应对设备适当性和正确性证据上的薄弱点。

7.171. 此类补充证据：

— 应直接应对其需要证实的要求；
— 应表明适用于被质疑的设备。

7.172. 提供补充证据的技术示例包括：

— 专用于设备（适用于预期应用）的补充任务，以及其正确性证据的其他要素；
— 适用和可信的运行经验的评价；
— 设计输出的核实；
— 统计试验。

7.173. 用户可以配置设备以使它们适合于预期的应用。此类修改应符合本“安全导则”中关于设计正确性和文档的标准，且不应使先前鉴定中可信的运行经验或试验无效。

7.174. 为安全使用该装置，应确定在预期应用中应遵守的限值。

7.175. 这些限值包括，例如：

— 已鉴定设备应用的限值；
— 要启用或禁用的特定选项和不使用的功能；
— 运行环境和运行寿命的限值；
— 在运行、试验和维护期间应遵守的措施。

8. 有关人-机接口的考虑

控制室

主控室

8.1. SSR-2/1 [1]要求 65 规定：

“必须在核电厂设立一个主控室，以便能够在所有运行状态下从主控室以自动或手动方式安全运行电厂，以及能够从主控室采取措施使电厂保持安全状态或在发生预计运行事件和事故工况后使之返回到安全状态。”

8.2. SSR-2/1（Rev.1）[1]要求 59 规定：

“必须提供用于以下目的的仪器仪表：确定可能影响核电厂裂变过程、反应堆堆芯完整性、反应堆冷却剂系统完整性和安全壳完整性的一切主要变量；获得安全和可靠运行电厂所需的电厂重要信息；以及为事故管理的目的作出决定。”

8.3. SSR-2/1（Rev.1）[1]第 5.57 段指出：

“必须向运行人员提供必要资料：以便：

(a) 评定电厂在任何工况下的总体状态；
(b) 在与电厂系统和设备相关的规定参数限值（运行限值和条件）范围内运行电厂；
(c) 验证启动安全系统所需的安全动作能够在需要时自动启动，并且相关系统能够发挥预定作用；
(d) 确定手动启动规定安全动作的必要性和时间。”

8.4. 仪器仪表和控制应允许控制室的运行人员对控制核电厂和维持安全所需的每个功能进行触发或手动控制。

8.5. 控制室应有足够的显示器，以监控所有安全重要功能，包括核电厂状态、其安全状态和电厂关键参数的趋势。

8.6. 应提供安全级别指示和控制，以实施应急运行程序和严重事故管理导则。

8.7. 第 8.6 段的指导并不排除使用其他适当手段来满足应急运行程序和严重事故管理导则目标的选项。

8.8. 如果控制核电厂和维持安全所需的系统或系统的一部分发生故障或有意使其不可用，则应在控制室以及需要将此信息传达给运行人员的场所显示此状态。

8.9. 应通告安全系统状态的变化，并在运行人员需要此信息的地方指明。

8.10. 需要报警的系统状态变化可能包括偏离正常运行限值、安全系统可用性丧失或由于故障、维护或试验导致的备用设备不可用。

8.11. 先进的报警系统功能性能够实现期望的功能，例如报警处理、报警优先级以及报警控制和管理，这有助于运行人员有效地监控和响应核电厂事件。

8.12. 主控制室和辅助控制室的设计应使任何火灾、内部危害或假想始发事件都不能妨碍运行人员履行基本的安全功能。

辅助控制室

8.13. SSR-2/1（Rev.1）[1]要求 66 规定：

> “必须配有仪器仪表和控制设备供随时使用，最好是在一个在实体、电气和功能上与核电厂主控室相分离的单独场所（辅控室）。辅控室的设备配备必须能够在主控室丧失执行这些关键安全功能的能力时将反应堆置于或维持在停堆状态，能够排出余热，并能够监控关键的电厂变量”。

8.14. 有些核电厂可能设计了一个以上的辅助控制室，或者可能有不在辅助控制室中的辅助控制点。

8.15. 辅助控制室应包含必要的信息显示器，用于监控核电厂工况，以支持对可能由需要撤离主控制室的情况导致的事件的响应。

8.16. 辅助控制室应包含的控制器、指示、报警和显示器，足以让运行人员将核电厂带到安全状态，确定已达到并维持在安全状态，以及监控电厂的状态和电厂关键参数的趋势。

8.17. 如果在辅助控制室提供为执行第 8.16 段建议所需的所有控制是不切实际的，可使用就地控制点的控制器。

8.18. 应在主控制室外采取适当措施，使主控制室一被放弃便将优先控制转移到一个新的控制场所。

事故监控

8.19. SSR-2/1（Rev.1）[1]第 6.31 段指出：

> “必须提供仪器仪表和记录设备，以确保获得必不可少的信息，供用于监控基本设备的状况和事故过程、预测可能从设计中预定的部位释放的放射性物质的释放位置和数量以及进行事故后分析。”

8.20. 应根据运行人员的作用和职责，酌情（即在主控制室和辅助控制室）提供和显示用于监控核电厂事故工况的信息显示。

8.21. 监控事故工况的一组显示通常称为“事故监控系统“或“事故后监控系统”。这种显示可以作为其他系统的一部分提供，或者可以是单一仪表通道的集合。

8.22. 事故监控系统应标明事故工况下核电厂运行人员所需的变量值，以使它们能够：

(a) 采取预先计划好的手动动作，把核电厂带到安全状态；
(b) 确定基本安全功能是否已经完成；
(c) 确定是否有可能突破或实际突破防止裂变产物释放的屏障（例如燃料包壳、反应堆冷却剂压力边界和安全壳）；
(d) 确定缓减设计基准事故和设计扩展工况后果所需核电厂系统的状态和性能，并将电厂带到安全状态；
(e) 确定是否有必要采取行动保护公众不受放射性物质释放的影响；
(f) 实施核电厂严重事故管理导则。

8.23. 执行第 8.22 段(a)—(d)项所列指示功能的仪器仪表，应定为安全级，并应由能够在设计基准、事故工况和设计扩展工况下运行的仪器仪表和控制设备提供。

8.24. 定级为“安全系统”则需要充分应用第 6 部分的导则，包括符合用于安全组的单一故障标准。

8.25. 严重事故监控仪表的设计和鉴定应符合预期环境条件的全部范围。

8.26. 在可能遇到的最严酷的可信状况下，对严重事故监控仪表进行全面的型式试验并不总是可行的。在这种情况下，可以用其他方法作为试验的补充，包括但不限于第 6.82 段所述的方法。

8.27. 支持严重事故管理导则执行的事故监控功能：

(a) 不能因不属于严重事故监控仪器仪表的设备运行、故障或误操作而导致不可用；

(b) 不应依赖外部电力，或应设计成具有从核电厂电力系统以外的其他来源获得电力的能力。

8.28. 如果仪器仪表的单一显示通道无法执行第 8.22(a)－(c)和(f)段中所列的功能，可能导致模棱两可的指示，应提供允许运行人员解决这种模棱两可情况的手段。

8.29. 单一显示通道发生的故障可能导致一对冗余显示器不一致。解决此模棱两可的情况的手段包括：提供额外的仪器仪表通道，或者将模棱两可的读数和另一个不同变量（与问题计数有已知的关系）进行比较的程序。

8.30. 为事故监控提供的仪器仪表应涵盖事故工况下可能达到的全部参数值。

8.31. 事故监控变量的显示应清晰可识。

8.32. 应为运行人员提供电子辅助（如“安全参数显示系统”），以协助运行人员快速确定核电厂的状态，验证事故监控通道的运行，验证其读数，并从直接测量中确定间接测量变量的值。

8.33. 计算机化的导航可以提高安全性，以及提供采取正确行动的更大确定性。

8.34. 在先进控制室的设计中，安全参数显示系统和事故监控系统的功能常常整合到正常的运行人员人-机接口中。建议可能仅限用于特定运行或事故假想方案，也可涵盖所有操作，包括启堆和正常功率运行情况。

8.35. 对于执行第 8.22(a)－(c)和(f)段指示功能的仪器仪表，还应提供不依赖于电源的运行人员辅助。

运行人员通讯系统

8.36. SSR-2/1（Rev.1）[1]要求 37 规定：

> “必须在整个核电厂范围内提供有效的通讯手段，以有助于在所有正常运行模式下进行安全运行，以及供发生所有假想始发事件后和在事故工况下使用。”

8.37. SSR-2/1（Rev.1）[1]第 5.66 段指出：

> “必须提供适当的警报系统和通讯手段，以便在核电厂现场和场区中的所有人员在运行状态下和事故工况下都能得到警报和指令。”

8.38. SSR-2/1（Rev.1）[1]第 5.67 段指出：

> “必须在核电厂范围内和毗邻区域提供确保安全所需的适当而多样化的通讯手段以及与相关场外机构进行通讯所需的这类通讯手段。”

8.39. 应为运行人员提供通讯系统，使它们能够安全地与核电厂内外部场所联系，而不必离开需要它们监控和控制的仪器仪表和控制系统。

8.40. 提供给运行人员之间以及与和场外应急设施的通讯系统不应因任何个人防护设备、假想始发事件或单一恶意行为而失效。

8.41. 仪器仪表和控制设备的特性不应妨碍运行人员之间的通讯。

8.42. 例如，如果仪器仪表和控制系统设备干扰无线电通讯，无线电通讯干扰仪器仪表和控制设备，或者个人防护设备妨碍电话使用，则可能需要其他的通讯形式。

8.43. 主控制室、辅助控制室和技术支持中心应至少有两种多样化的方法与以下进行通讯：

(a) 在预计运行事件或事故工况下需要通讯的区域；
(b) 应急响应设施，如技术支持中心和应急响应机构；
(c) 相关设施。[38]

[38] 相关设施包括可能受到核电厂机组运行影响的其他设施（例如同一场址的其他机组）。

8.44. 各种通讯方法的示例包括电子邮件、数据传输、传真、视频连接、固定电话线路、卫星和移动电话以及便携式无线电。

8.45. 第 8.43 段和第 8.44 段中确定的各种通讯链路：

(a) 其设计应使它们不会受到同样的故障、内部危害、外部危害或假想始发事件的影响；

(b) 应能独立于核电厂电力系统和场外电力系统运行。

8.46. 应提供现场和核电厂的所有人员都能听到广播的通讯系统。

仪器仪表和控制系统的人因工程的一般原则

8.47. SSR-2/1（Rev.1）[1]要求 32 规定：

> “必须在核电厂设计过程初期就对人为因素包括人-机接口进行系统性考虑，并须在整个设计过程中持续进行这种考虑。”

8.48. SSR-2/1（Rev.1）[1]第 5.55 段指出：

> “设计必须有助于运行人员履行职责和执行任务，而且必须限制操作失误的可能性和对安全造成的影响。设计过程必须适当考虑电厂布置和设备布置以及包括维护程序和视察程序在内的有关程序，以有利于运行人员和电厂之间在电厂所有状态下的相互作用。”

8.49. SSR-2/1（Rev.1）[1]第 5.56 段指出：

> “人-机接口的设计必须做到能够根据需要作出决定和采取行动的时间为运行人员提供全面而易于管理的信息。必须以简洁明了的方式向运行人员提供其作出行动决定所需的资料。”

8.50. 人-机接口的设计应保留与参考设计相关的好的特性，并应避免导致不良运行经验的负面问题。

8.51. 安全系统的监督控制所需的人-机接口设计应采用纵深防御原则。

8.52. 仪器仪表和控制系统应向运行人员提供必要信息以便探测系统状态的变化，并用于诊断运行系统（必要时）和核实手动或自动操作的的执行。

8.53. 一个令人满意的设计将考虑到运行人员的认知处理能力以及与过程相关的时间限值。

8.54. 设计应确保从操作控制一直到此输入被控制系统验证所需的最长时间能被运行人员所接受。

8.55. 仪器仪表和控制系统设计应确保运行人员的任务能在规定的系统要求时间内完成。

8.56. 过快或过慢的信息流速率和控制器性能会降低运行人员的效能。

8.57. 当在不适当的假想方案下或核电厂配置不适当的情况下采取行动时，仪器仪表和控制系统应尽量设计成能预防和探测运行人员的错误。这包括控制系统、监控系统和保护系统的设定值修改的验证。

8.58. 仪器仪表和控制系统应提供简单的，易懂的被探测到的运行人员错误的指示，并应提供可用的简单且有效的恢复方法。

8.59. 任何一个运行人员的错误都不应导致反应堆控制的丧失。

8.60. 人-机接口：

(a) 应尽可能适应预订与系统交互的多种运行人员的不同作用和职责；
(b) 设计时应首先重点考虑负责设备安全运行的运行人员的作用；
(c) 应支持部分控制室工作人员的共同态势感知的获得，例如通过大型壁挂式设备状态显示器；
(d) 应提供有效的核电厂状态总概；
(e) 应尽可能采用与功能和任务要求一致的最简化设计；
(f) 通过设计将对运行人员培训的依赖最小化；
(g) 应显示能够被运行人员迅速识别和理解的信息；[39]
(h) 应能容许模拟指针式和视频显示的故障，而不会严重干扰控制动作；
(i) 应反映对人体生理特征[40]、人体运动控制和人体测量学特征的考虑。

---

[39] 以易于理解的形式显示信息可减少运行人员的认知工作量。例如，符合本导则的人机界面设计将最大限度地减少运行人员进行脑力计算和转换以及使用回忆记忆的需求。

[40] 人类的生理特征包括，例如，视觉/听觉感知和生物力学（伸展和运动）。

8.61. 人-机接口、程序、培训系统和培训应相互一致。

8.62. 信息显示应整合到协调布置，从而有利于运行人员对核电厂状态的理解以及对核电厂的控制。

8.63. 人-机接口的操作和外观应在不同的监控场所及平台之间保持一致，并应体现出高度的标准化。

8.64. 应考虑对所有描述性标识和标签使用同一语言和协调的字体。

8.65. 仪器仪表和控制系统的所有方面（包括控制器和显示器排列）都应与运行人员使用的心理模式相一致并符合传统习惯。

8.66. 心理模式结合了运行人员和对系统行为的理解和期望。这些模式是通过培训、程序使用和经验开发的。

8.67. 在设计中确定每类控制和显示的规定，然后在控制核电厂状态显示的标识、布局和布置中完全遵循这些规定。

人与自动动作相互作用的考虑

8.68. 应当使用系统化的，和一致的方法，确保仪器仪表和控制功能合理分配给人和仪器仪表和控制系统。

8.69. 可能影响人机功能分配的因素包括：

— 所有运行工况下的潜在的人员工作负荷；
— 准确度和重复性要求；
— 时间因素；
— 决策和所需动作逻辑的类型和复杂性；
— 环境因素；
— 人体生理学和人体测量学。

8.70. SSR-2/1（Rev.1）[1]第 5.59 段指出：

> “运行人员在短时间内进行干预的必要性必须保持最低程度，并且必须证明运行人员有充分的时间作出行动决定和采取行动。”

8.71. 当运行人员不能可靠和及时地完成手动动作，或依赖手动控制会给运行人员带来不合理的负担时，仪器仪表和控制应提供自动动作。

8.72. 仪器仪表和控制系统应给运行人员提供监控每个自动功能必需的信息。

8.73. 仪器仪表和控制系统应提供给运行人员多重手段核实自动行动。

8.74. 提供用于监控自动功能的信息的显示速率和详尽程度（例如，目标或目的的标识，或核实时机）应使运行人员能够有效的监控。

8.75. 仪器仪表和控制系统应允许运行人员手动触发或控制每个用于控制和维持核电厂安全的必要功能。

仪器仪表和控制系统中任务设计的考虑

8.76. 运行人员的职能应由有目的和有意义的任务组成，使工作人员能够保持对核电厂的熟悉，并保持不高的工作负荷，以免对性能产生不利影响，但足以维持警惕。

8.77. 仪器仪表和控制应该具有被任务分析识别出所有必要的特性。

8.78. 任务分析应考虑所有核电厂状态、所有电厂运行模式和所有运行小组，如反应堆运行人员、汽轮机运行人员、值长、现场运行人员、安全工程师和运行维护人员。任务分析应为仪器仪表和控制的特性提供设计输入，如显示信息的准确度和精确度、系统响应时间、实体布置、控制器、显示器和报警类型，以及在信息显示中软控制的整合。

8.79. 人-机接口应允许按照对任务最方便的配置对视频显示单元上的显示器和控制器进行配置，从而有利于任务执行。

8.80. 这种可配置性的好处，例如，包括不同的配置可能更好地适应不同经验水平的运行人员，或者不同的配置在不同的运行模式中可能更有效。

8.81. 人-机接口的所有方面（格式、术语、排序、分组和运行人员的决策支持辅助工具）都应反映出基于任务要求或其他有目的的明显的逻辑性。

8.82. 所有显示、控制和数据处理辅助与相关任务和功能的关系都应清晰。

8.83. 人-机接口应以与任务分析结果一致的形式和样式向运行人员显示信息。

8.84. 仪器仪表和控制应提供控制选项，以涵盖通过任务分析所识别的潜在运行人员采取动作的范围。

8.85. 仪器仪表和控制应向运行人员提供用于完成行动的多重手段。

8.86. 仪器仪表和控制应允许运行人员以最少的动作次数完成任务。

可达性和工作环境方面的考虑

8.87. SSR-2/1（Rev.1）[1]第 5.61 段指出：“运行人员工作场所和工作环境的设计必须符合人机工程学概念。”

8.88. 在期望运行人员监控和控制核电厂系统的区域，应制定必要的措施，以确保合适的工作环境条件和防止危害工况。

8.89. 正常的工作环境方面要考虑的包括照明、温度、湿度、噪音、振动，如果需要持续监控，则包括休息区和洗手间等设施。

8.90. 要考虑的危害包括辐射、烟雾和大气中的有毒物质。

8.91. SSR-2/1（Rev.1）[1]第 5.60 段指出：

> “设计必须能够确保在发生影响电厂的事件后，控制室或辅助控制室内以及通往辅助控制室的通道上的沿途场所的环境状况不损害运行人员的防护和安全。”

8.92. 当人-机接口站 [41] 分散时，运行人员应具有安全地和及时地接近这些不同场所的手段。

8.93. 为了使运行人员可以有效进入辅助控制点或其他需要人员操作的就地场所，应为其提供适当的路径以防止潜在的内部危害和外部危害。

[41] 分散式人-机接口站的示例包括辅助控制室和预计运行人员操作的其他现场位置。

历史数据的记录

8.94. 人-机接口应提供记录、存储和显示历史信息的功能，这些显示器将帮助运行人员识别形势和趋势、理解系统过去的或当前的状态、执行事故后分析或预测未来发展。

9. 软件

概述

9.1. 本部分中的建议适用于应用在安全重要仪器仪表和控制设备中所有类型的软件，例如操作系统、预先开发的软件或固件、为物项专门开发的软件，或针对预先开发的现成的硬件或软件模块家族开发的软件。

9.2. 数字系统需要采用与模拟系统不同的可靠性评定方法。可靠性是从对生产活动质量的评定以及核实和验证的结果中推断出来的。软件，就其性质和应用目的而言，允许比（电气或机械）硬件大得多的设计空间。如果没有系统性的限值，软件可能变得容易出现缺陷并且无法核实。软件实现的复杂性会在设计中产生额外的故障，增加探测和纠正故障的难度，引入在更简单的设计中不存在的故障模式和影响，并降低安全系统设计标准（如独立性、可试验性和可靠性）一致性证明的信心。

9.3. 第 2 部分中提供的管理系统和生命周期过程导则与软件特别相关，因为所涵盖的活动是软件有效开发的组成部分。

9.4. SSR-2/1（Rev.1）[1]要求 63 规定：

> “如果核电厂的安全重要系统依赖于基于计算机的设备，则必须制订开发和试验计算机硬件和软件的适当标准和实践并在该系统的整个使用期内特别是软件的整个开发周期执行这些标准和实践。必须将整个开发工作纳入质量管理系统的管理。”

9.5. 系统软件的开发应遵循预定义的生命周期，进行适当的计划并编写成文件，包括彻底的核实和验证（见第 2 部分）。

软件需求

9.6. 满足仪器仪表和控制系统要求所需的所有软件，包括重复使用或自动生成的软件，都应具有符合本部分建议的适当形式的文档化要求。

9.7. 应使用与系统安全重要性相称的预定技术组合来建立软件需求。

9.8. 建立需求的技术可能包括使用定义良好的语法和语义、模式、分析和评审的规范语言。

9.9. 软件需求的开发人员应该对系统的底层设计基准有适当的理解，如第 3 部分所述。

9.10. 理解系统设计的基准是必要的，以确保软件需求正确地满足系统的必要属性。相关问题包括：

— 潜在失效条件；
— 运行模式；
— 为安全目的进行监控；
— 自监督；
— 故障探测；
— 当发生探测到故障但无法恢复的事件时达到安全工况；
— 其他故障安全行为；
— 与安全有关的输入和输出关系。

9.11. 软件需求说明：

(a) 应该定义每个单一软件物项需要做什么，以及它将如何与系统的其他物项交互；

(b) 应源自仪器仪表和控制生命周期的相关流程（包括考虑以前分析中确定的系统危害），以及与仪器仪表和控制生命周期相衔接的流程，如人因工程和计算机安保活动（见第 11 页图 2）；

(c) 应尽可能按需要实现的目标而不是按设计和执行这些目标的方式来编写；

(d) 应是完整的、明确的、一致的、可读性强的、目标受众（如领域专家、安全工程师和软件设计人员）可理解的、可核实和可追溯的；

(e) 应满足分配给软件物项的系统要求，包括质量要求；

(f) 必要时，应详细说明所需的最低精确度、数值准确度、接口说明[42]、执行线程的独立性、自监督、时限性能[43]和安保性[44]；

(g) 应包括达到的可靠性[45]和可用性的必要水平；

(h) 应考虑到计算机、软件工具和类似现有系统的能力，以确保软件要求是可行的；

(i) 应参考、包括或补充适用于目标受众的其他信息，例如，必要程度的定要求的背景信息、风险考虑、功能或安全特点设计建议，以确保目标受众能够理解所必需的程度；

(j) 应规定软件并未规定的特别重要的任何功能、行为或相互作用。

9.12. 如果设计限值是必要的，这些限值应该是明确的、合理的和可追溯的。

9.13. 每个软件需求的来源都应该有足够的文档记录，以便于核实、验证、追溯更层级的文档，并证明所有相关需求都已得到满足。

9.14. 应使用需求跟踪系统，以便通过开发项目的设计、实现、整合和验证阶段跟踪软件需求。

9.15. 安全重要软件的需求同样应该被识别出来。

软件设计

9.16. 已完成的软件设计应是明确的、正确的，可证明相关软件需求是完整的、一致的、良好结构化的、可读的、目标受众（如领域专家、安全工程师和软件设计人员）可理解的、可核实的、可验证的、可追溯的、可维护的和文档化的。

---

[42] 接口示例包括软件和运行人员之间、传感器和致动器之间、计算机硬件和其他软件之间以及系统之间的接口示例。

[43] 时限性能包括故障探测时间和恢复时间。

[44] 安保性的示例包括有效性检查和访问权限。

[45] 可靠性和可获得性的水平可以从数量上或质量上加以界定，例如，根据第 9.11(a)-(f)段所述的辅助软件要求加以界定，和开发过程（如遵守标准）。

9.17. 应建立软件设计，并保持采用与系统安全重要性相称的预定技术组合。

9.18. 这类技术可能包括描述、逻辑图和图形表示，以及良好定义的语法和语义、模式、分析和评审。

9.19. 在开发软件设计时，应了解安全要求的来源。

9.20. 应充分分辨软件设计的各个部分，以便在整个设计中实现对需求的有效跟踪。

9.21. 安全系统软件的设计应在所有层次最大限度地简化，包括总体架构、外部接口、模块之间的内部接口和详细设计。

9.22. 设计的简单化是实现和证明安全的关键手段，但总是涉及权衡，例如功能、灵活性和成本。而第 9.21 段指出仅适用于安全系统，对于安全级别较低的系统软件来说，简单是一个值得追求的目标。对于较低安全级别的系统，安全和复杂性之间的平衡是不同的，可接受更高的复杂程度。

9.23. 软件设计架构应设计成允许将来的修改、维护和升级。

9.24. 软件架构应该是分层的，以提供抽象的分级层次。

9.25. 应鼓励尽可能的使用信息隐藏，以使分段评审和核实成为可能，并便于修改。

9.26. 软件设计应包括软件与外部环境的接口。

9.27. 软件设计应包括所有软件模块的详细设计。

9.28. 软件模块的描述应完整地规定其功能、与其他模块的接口及其在整个软件中的功能背景。

9.29. 执行类似功能的软件模块应具有一致的结构。

9.30. 模块接口应该是一致的。

9.31. 每个模块间接口的两端应该匹配，模块输入和输出接口之间应该使用一致的变量名，并且应该尽可能避免递归调用。

9.32. 如果系统包括多个处理器，且软件分布在这些处理器之间，那么软件设计应当规定哪些软件进程在哪个处理器上运行，以及数据和显示器又放在哪里。

9.33. 软件设计应支持安全系统的确定的行为和时限。

9.34. 通信协议应符合第 7.79－7.94 段的建议。

9.35. 随着设计的改进，应考虑是否需要增加故障探测和自监督功能，并将其纳入软件设计（见第 6.166－6.172 段）。

9.36. 在探测到故障时，应采取适当的行动以满足恢复、停止过程、错误信息和日志方面的软件要求，以确保系统保持在安全状态。

9.37. 软件设计文档应该包括在那些需要在设计阶段遵守的实现限值。

9.38. 这种实现限值可包括确保编程设计语言、编译程序、子程序库和其他支持软件工具的多样性和所需属性的任何需要。

9.39. 应当证明限值是合理的，或者是可追溯到较高层次的要求或限制的。

9.40. 对于安全系统以外的系统，对私有系统的实施限值可足以追溯到供应商提供的标准文档。

9.41. 软件设计架构应该考虑到模块和接口上的限值，这些限值可能来自于应用多样性的决定。

9.42. 软件设计应考虑到信息安保方面的最佳实践，以避免容易被恶意软件或黑客利用而难以修复的某些设计薄弱点。

9.43. 酌情对软件设计进行同行评审。

软件实现

9.44. 软件实现：

— 应正确和完整地体现软件需求且完整地体现软件设计、结构合理、具备可读性、可核实性、可追溯性、可维护性且适当的文档化；

— 应使用与系统安全重要性相称的预定技术组合，包括语言、软件工具、编程实践、分析、评审和试验；
— 应明确说明所有软件要求和软件设计；
— 应简单易懂，可读性和可维护性优先于编程的易用性；
— 应包括源代码和可执行代码的可读形式、单元接口试验和模块接口试验的结果，以及足够的上下文背景信息，以核实代码相对于其规范说明的正确性。

9.45. 所有代码都应该有充分的文档记录。

9.46. 对于安全系统，代码所有部分的文档（包括运行时支持代码和故障监督功能）的可用性将使本“安全导则”的试验导则得以满足。

9.47. 编程开始前应先制定编程规则，并核实规则的遵守情况。

9.48. 应该一致地应用数据结构和命名约定。

9.49. 软件的实施应经受：

— 规定的变更控制程序（包括影响分析）；
— 配置管理；
— 确保对所有更改的结果进行适当的试验覆盖。

9.50. 所使用的程序设计语言（或子集）在表达能力、避免不安保因素、抽象层次、对模块化和信息隐藏的支持、编译和运行时检查以及错误处理方面应该是充分的。

9.51. 用于安全系统的程序设计语言应该支持简单实现。

9.52. 所使用的程序设计语言和功能定义方法（如逻辑图或图形表示）的选择应基于对所涉及进程的功能性和完整性要求的系统性评定。

9.53. 对于安全系统，程序设计语言选择应该是论证的并有文档记录。

9.54. 安全系统语言语法和语义应该是完整的、可用的和严格定义的。

9.55. 软件功能是执行特定任务的编程元。它们可能是程序设计语言固有的，包含在库中或者是预先开发的。

9.56. 软件功能的使用应以最大限度地简化为目标，并应加以识别，具有定义良好的接口，而且始终应根据对其使用的相关限值进行调用。

9.57. 如果使用了操作系统，则应该或已经对其进行了彻底和令人满意的试验，并且应该论证其适合于目标应用程序。

9.58. 对于安全系统，任何操作系统软件都应符合本“安全导则”的所有建议。

9.59. 应选择一套适当的软件工具来执行，以尽量减少错误。有关建议见第 7.148－7.164 段。

9.60. 本部分中的建议适用于软件生成和经典软件开发的所有可能组合。

9.61. 软件多样性（即使用独立程序设计组和/或不同的方法、语言、时限、功能顺序或算法）可被考虑为降低软件中共因故障的可能性和影响的一种手段。但软件的多样性可能会引入设计限值，而这些限值本身可能会导致新的故障。

9.62. 应当采取预防措施，以确保支持纵深防御不同层次的系统之间的独立性不因使用相同的软件（如操作系统、网络通信或其他运行中的支持软件）而受到损害。

9.63. 实现软件的设计组应该接受安全开发技术的培训。

软件核实与分析

9.64. 软件需求、设计和实现应根据仪器仪表和控制系统需求的规范说明进行核实。

9.65. 核实可追溯性应是一项持续的活动，以确保尽可能早的解决不足之处，因此，必要的改变仍然切实可行。

9.66. 软件生命周期中每个阶段的结果都应该对照前面阶段设置的需求进行核实。

9.67. 应制定软件核实计划，以证明：

(a) 使用的核实技术；

(b) 应用于每种技术的程序的细节或参考，包括其范围和深度；

(c) 如何证明非功能要求和限值得到满足；

(d) 确定何时进行了充分核实的标准，包括前一阶段输出的完整性和功能试验的结构覆盖面的目标，以及如何证明这些目标；

(e) 记录结果的手段；

(f) 记录和解决不符合情况和故障的手段；

(g) 执行核实的一个或多个小组及其与软件设计者的独立性；

(h) 用于核实的任何软件工具的功能，包括对其如何使用的期望和限值（如领域、语言和流程）；

(i) 上文(a)－(h)项所列每一要素的理由，以及核实对所适用的安全类别系统中的软件而言足够的理由。

9.68. 核实应包括下列技术：

— 人工检测，如评审、预排、视察或监查；
— 源代码的静态分析；
— 动态分析。

9.69. 应该对软件的最终版本执行静态分析。

9.70. 所使用的静态分析技术将根据系统安全的重要性而有所不同。静态分析包括核实是否符合设计和编码标准、控制流分析、数据和信息流、符号执行和正式代码核实等技术。

9.71. 应核实软件中实现的所有非功能要求。

9.72. 应使用相关的运行经验来识别异常以进行纠正，并对软件的可信性提供进一步的信心。

9.73. 有关的运行经验可以补充但不能取代其他核实技术。

9.74. 第 7.148－7.164 段提供了有关使用软件核实和分析工具的指导。

9.75. 应确定试验策略（例如，自下而上策略或自上而下策略）以核实和验证软件实现。

9.76. 试验案例的规范说明应确保充分试验：

— 接口（如模块-模块接口、软件-硬件接口、系统边界接口）；
— 数据传递机制和接口协议；
— 例外情况；
— 每个输入变量的整个范围（使用等价类划分和边界值分析等技术）；
— 所有的系统运行模式。

9.77. 试验计划应确保试验是可复验的以便于回归试验，并记录试验结果。

9.78. 还希望最大限度地减少重复试验所需的人工干预。

9.79. GS-G-3.1[3]为确保用于试验的测量和试验设备的适用性提供了指导。

9.80. 应评审试验案例的规范说明及其有效性，相较于核实计划目标的任何不足之处都应得到解决或论证。

9.81. 核实应由独立于设计人员和开发人员的团队、个人或组织团体进行。

9.82. 应使用自动化软件工具评审软件以检查软件安保漏洞，并辅之以代码关键字段的手动评审（例如，输入/输出处理和异常处理）。

9.83. 应在核实期间对被测系统的所有输出进行监控，应当调查对预期结果的任何偏离，并将调查结果并记录在案。

9.84. 相较于核实计划的核实结果中的任何不足（例如，在所实现的试验覆盖范围）都应得到解决或论证。

9.85. 应分析任何探测到的错误的原因，通过早先商定的修改程序加以纠正，并实施相应的回归试验。

9.86. 错误分析应包括对仪器仪表和控制系统其他部分适用性的评价。

9.87. 应当保存有关异常之处的的数量和类型的记录，应对这些记录进行评审以增加对开发过程的了解，并使用这些记录来采取相应的措施改进设计过程，以有益于当前和未来的系统开发项目。（见 GS-G-3.1[3]第 6.50－6.77 段和 GS-G-3.5[4]第 6.42－6.69 段。）

9.88. 核实和分析文档应提供一套连贯的证据，证明开发过程的产品是完整、正确和一致的。

9.89. 应记录包括试验记录在内的核实结果，并维护和保持这些核实结果可供质量保证监查和第三方评定使用。

9.90. 设计文档的可追溯性应包括每个生命周期阶段的文档与功能需求之间的有序连接。

9.91. 试验结果文档应可追溯到试验案例的规范说明，并应指出哪些结果未能满足预期，以及如何解决这些问题。

9.92. 应该清楚地记录试验覆盖范围。

9.93. 对于安全系统使用可追溯矩阵追踪每个试验案例应该是可能的，该矩阵体现软件需求、设计、实现和试验之间的联系。

9.94. 对于安全系统，应将生成的应用程序提交试验，以确保计算机安保（如渗透试验），以确定不容易探测的共用安保漏洞，并允许软件设计和实现的不断改进。

9.95. 试验文档应足以使试验过程能够重复进行且有信心得到相同结果。

预先开发软件

9.96. 对于安全系统，安全级仪器仪表和控制系统中使用的预先开发软件应具有与专门为应用程序编写的软件相同的质量鉴定。

9.97. 预先开发的软件功能应符合第 2.108－2.117 段的建议。

9.98. 对于非安全级系统的安全重要系统，预先开发的软件应具有描述以下内容的用户文档：

(a) 提供的功能；

(b) 接口，包括输入、输出、异常信号、参数和配置数据的作用、类型、格式、范围和施加的限值；

(c) 不同的行为模式和相应的瞬态工况（如适用）；

(d) 使用预先开发的软件时要满足的任何限值；

(e) 说明预先开发的软件在用户文件对上文(a)－(d)项的说明是正确的；

(f) 论证这些功能适用于仪器仪表和控制系统。

软件工具

9.99. 关于软件工具的建议见第 7.148－7.164 段。

第三方评定

9.100. 安全系统软件的第三方评定应与软件开发过程同时进行。

9.101. 独立于系统和/或软件的供应商和营运组织的第三方评定的目的是提供对系统及其软件适用性的看法。此类评定可以由监管实体或监管者认可的实体进行。

9.102. 有必要与软件发起人作出适当安排，允许第三方评定。

9.103. 评定应包括对以下方面的检测：

— 开发过程（例如通过质量保证监查和技术视察，包括生命周期文件检测，如计划、软件规格说明和试验活动的全部范围）；

— 最终软件（例如通过静态分析、视察、监查和试验），包括任何后续修改。

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《设施和活动管理系统》，国际原子能机构《安全标准丛书》第 GS-R-3 号，国际原子能机构，维也纳（2006 年）（准备修订中，将作为 GSR Part 2 发布）。

[3] 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）。

[4] 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）。

[5] 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）。

[6] 国际原子能机构《国际原子能机构核安全和辐射防护安全术语》（2007 年版），国际原子能机构，维也纳（2007 年）。

[7] 国际原子能机构《核电厂电力系统的设计》，国际原子能机构《安全标准丛书》第 SSG-34 号，国际原子能机构，维也纳（2016 年）。

[8] 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 号，国际原子能机构，维也纳（2011 年）。

[9] 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）。

[10] 国际原子能机构《核电厂现代仪器仪表与控制导则》，《技术报告丛书》第 387 号，国际原子能机构，维也纳（1999 年）。

[11] 国际原子能机构《核电厂仪器仪表和控制系统堆芯知识》，国际原子能机构《核能丛书》第 NP-T-3.12 号，国际原子能机构，维也纳（2011 年）。

[12] 国际原子能机构《制定和实施核电厂一级概率安全评定》，国际原子能机构《安全标准丛书》第 SSG-3 号，国际原子能机构，维也纳（2010 年）。

[13] 国际原子能机构《制定和实施核电厂二级概率安全评定》，国际原子能机构《安全标准丛书》第 SSG-4 号，国际原子能机构，维也纳（2010 年）。

[14] 国际原子能机构《核电厂确定性安全分析》，国际原子能机构《安全标准丛书》第 SSG-2 号，国际原子能机构，维也纳（2009 年）。

[15] 国际原子能机构《核电厂调试》，国际原子能机构《安全标准丛书》第 SSG-28 号，国际原子能机构，维也纳（2014 年）。

[16] 国际原子能机构《核电厂的维护、监视和在役检查》，国际原子能机构《安全标准丛书》第 NS-G-2.6 号，国际原子能机构，维也纳（2002 年）。

[17] 国际原子能机构《核电厂结构、系统和部件的安全分级》，国际原子能机构《安全标准丛书》第 SSG-30 号，国际原子能机构，维也纳（2014 年）。

[18] 国际核安全咨询组《核安全的纵深防御》，《国际核安全咨询组丛书》第 10 号，国际原子能机构，维也纳（1996 年）。

[19] 国际核安全咨询组《核电厂基本安全原理》第 75-INSAG-3（Rev.1）号，《国际核安全咨询组丛书》第 12 号，国际原子能机构，维也纳（1999 年）。

[20] 国际原子能机构《核电厂设计中的内部火灾和爆炸防护》，国际原子能机构《安全标准丛书》第 NS-G-1.7 号，国际原子能机构，维也纳（2004 年）。

[21] 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）。

[22] 国际原子能机构《在运核电厂设备鉴定：升级、维护和审查》，《安全报告丛书》第 3 号，国际原子能机构，维也纳（1998 年）。

[23] 国际原子能机构《核电厂抗震设计和鉴定》，国际原子能机构《安全标准丛书》第 NS-G-1.6 号，国际原子能机构，维也纳（2003 年）。

[24] 国际原子能机构《核电厂设计中的非地震外部事件》，国际原子能机构《安全标准丛书》第 NS-G-1.5 号，国际原子能机构，维也纳（2003 年）。

[25] 国际原子能机构《核电厂老化管理》，国际原子能机构《安全标准丛书》第 NS-G-2.12 号，国际原子能机构，维也纳（2009 年）。

[26] 国际原子能机构《保护核电厂免受破坏的工程安保问题》，国际原子能机构《核安保丛书》第 4 号，国际原子能机构，维也纳（2007 年）。

[27] 国际原子能机构《内部威胁的预防和保护措施》，国际原子能机构《核安保丛书》第 8 号，国际原子能机构，维也纳（2008 年）。

[28] 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）。

[29] 国际原子能机构《核电厂运行限值、条件及运行程序》，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）。

[30] 国际原子能机构《核电厂营运组织》，国际原子能机构《安全标准丛书》第 NS-G-2.4 号，国际原子能机构，维也纳（2001 年）。

[31] 国际原子能机构《核电厂运行的实施》，国际原子能机构《安全标准丛书》第 NS-G-2.14 号，国际原子能机构，维也纳（2008 年）。

[32] 国际原子能机构《核电厂的辐射防护设计》，国际原子能机构《安全标准丛书》第 NS-G-1.13 号，国际原子能机构，维也纳（2005 年）。

[33] 国际原子能机构《核电厂应急电源系统的设计》，国际原子能机构《安全标准丛书》第 NS-G-1.8 号，国际原子能机构，维也纳（2004 年）。

附 件 I

国际仪器仪表与控制标准参考文献目录

I-1. SSR-2/1（Rev.1）[I-1]要求 9 规定：“核电厂的安全重要物项必须按照相关国家和国际程序和标准进行设计。”

I-2. 本“安全导则”提出了原子能机构成员国广泛接受的高层次的建议。除了原子能机构提供的指导外，还有大量的国家和国际标准，就支持遵守 SSR-2/1（Rev.1）[I-1]设计方法和系统特征提出更详细的建议。预期设计人员、用户和监管机构将利用这些标准中的信息。

I-3. 两个标准开发组织负责大多数国际上使用的核电厂仪器仪表和控制标准：(a) 国际电工委员会（IEC）第 45 小组分委员会；(b) 电气和电子工程师协会（IEEE）核工程委员会。每个组织都制定了大量的标准。这两个组织都制定了符合 SSR-2/1（Rev.1）[I-1]要求和本“安全导则”建议共同原则的标准。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。

I-4. 本附录旨在帮助读者理解本“安全导则”与国际电工委员会和电气和电子工程师协会标准之间的关系。表 I-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电气和电子工程师协会标准。表 I-1 不是这两套标准的完整列表，但它确定了国际电工委员会和电气和电子工程师协会标准集的切入点。

I-5. 表 I-2 显示了这些切入标准与本“安全导则”主要主题领域的关系。

表 I-1. 与本“安全导则”有密切关系的国际标准

IEC 60515	核电厂安全重要仪器仪表辐射探测器特性和试验方法
IEC 60568	核电厂安全重要仪器仪表动力堆中子注量率（通量）测量用堆芯仪器仪表
IEC 60671	核电厂安全重要仪器仪表和控制系统监督试验
IEC 60709	核电厂安全重要仪器仪表和控制系统分离
IEC 60737	核电厂安全重要仪器仪表温度传感器（堆芯和主冷却剂回路中）特性和试验方法

表 I-1. 与本“安全导则”有密切关系的国际标准（续）

IEC 60780	核设施安全重要电气设备鉴定
IEC 60880	核电厂安全重要仪器仪表和控制系统执行 A 级功能计算机系统软件方面
IEC 60964	核电厂控制室设计
IEC 60980	核电厂安全系统电气设备抗震鉴定推荐程序
IEC 61226	核电厂安全重要仪器仪表和控制功能的分类
IEC 61468	核电厂堆芯仪器仪表自供电中子探测器的特性和试验方法
IEC 61500	核电厂安全重要仪器仪表和控制执行 A 级功能系统中的数据通信
IEC 61501	核反应堆仪器仪表宽量程中子注量率计均方电压法
IEC 61513	核电厂安全重要仪器仪表和控制系统的一般要求
IEC 61772	核电厂控制室视觉显示装置（VDU）的应用
IEC 61839	核电厂控制室的设计、功能分析和分配
IEC 61888	核电厂安全重要仪表跳闸设定值的测定和维护
IEC 62003	核电厂安全重要仪器仪表和控制电磁兼容性试验要求
IEC 62138	核电厂安全重要仪器仪表和控制执行 B 或 C 类功能计算机系统的软件方面
IEC 62241	核电厂主控制室报警功能和显示
IEC 62340	核电厂安全重要仪器仪表和控制系统处理共同原因故障（CCF）的要求
IEC 62397	核电厂安全重要仪器仪表和控制耐温探测器
IEC 62566	核电厂安全重要仪器仪表和控制执行 A 级功能的系统用 HDL 编程集成电路的开发
IEC 62671	核电厂安全重要仪器仪表和控制功能有限的工业数字装置的选择和使用
IEEE Std. 1023	人机工程在核电厂和其他核设施的系统、设备和设施中应用的电气和电子工程师协会推荐程序
IEEE Std. 308	核电厂 1E 级电力系统的电气和电子工程师协会标准
IEEE Std. 323	核电厂 1E 级设备鉴定的电气和电子工程师协会标准
IEEE Std. 338	核电厂安全系统定期监督试验标准
IEEE Std. 344	核电厂设备抗震鉴定电气和电子工程师协会标准

表 I-1. 与本“安全导则”有密切关系的国际标准（续）

IEEE Std. 379	核电厂安全系统单一故障标准应用的电气和电子工程师协会标准
IEEE Std. 384	IEEE 1E 级设备和电路独立性标准
IEEE Std. 497	核电厂事故监控仪器仪表的电气和电子工程师协会标准
IEEE Std. 603	核电厂安全系统的电气和电子工程师协会标准
IEEE Std. 7-4.3.2	核电厂安全系统中数字计算机的电气和电子工程师协会标准
IEEE Std. 1012	软件核实和验证的电气和电子工程师协会标准
IEEE Std. 1074	开发软件生命周期过程的电气和电子工程师协会标准
ISO/IEC 15288	系统和软件工程系统生命周期过程
ISO/IEC 12207	系统和软件工程软件生命周期过程

注：ISO：国际标准化组织。

表 I-2. 本“安全导则”主题领域与国际标准的关系

本“安全导则”	国际通用仪器仪表和控制标准
1.说明	
2.仪控设计管理系统：生命周期模式的应用	IEC 61513、IEEE 7-4.3.2 IEC 61513、IEEE 7-4.3.2, ISO/IEC 15288
3.仪控系统设计基准：	IEC 61513、IEEE 603
—仪控功能识别	IEC 61226
—仪控系统设计基准内容	IEC 61513
4.仪控架构	IEC 61513、IEC 6 2340
5.仪控功能、系统和设备的安全分类	IEC 61226
6.所有安全重要仪控系统的总体建议：	IEC 61513、IEC 60709、IEEE 379、IEEE 384
—总则	IEC 60780、IEC 980、IEC 62342、IEEE 344、IEEE 323、IEC 2003
—可靠性设计	IEC 61513
—设备鉴定	IEC 60671、IEEE 338
—应对老化和过时的设计	IEC 61513
—对安全重要系统的访问控制	IEC 61513
—运行期间的试验和可试验性	

表 I-2. 本“安全导则”主题领域与国际标准的关系（续）

本“安全导则”	国际通用仪器仪表和控制标准
—可维护性 —为试验或维护而停止使用的规定 —设定值 —安全重要物项的标记和识别	IEC 61888
7.特定仪控系统和设备的设计导则：	IEC 60515、IEC 61501、IEC 60568，
—传感装置	IEC 61468、IEC 60737
—控制系统	IEEE 603
—保护系统	IEC 61225、IEEE 308
—电源	IEC 61513、IEEE 7-4.3.2,
—数字系统	IEC 61500、IEC 62671
—使用硬件描述语言配置的设备	IEC 62566
—软件工具	IEC 60880、IEC 62138
8.人机界面注意事项： —控制室 —辅助控制室 —事故监控 —营运者通信系统 —仪控系统人因工程通则 —历史数据的记录	IEC 60964、IEC 61772、IEC 62241， IEEE 576 IEC 60965 IEEE 497 IEC 61839、IEC 61772、IEEE 1023 IEEE 1082
9.软件	IEC 60880、IEC 62138， IEEE 7-4.3.2、IEEE 1012， IEEE Std. 1074、ISO/IEC 12207

I-6. 齐心协力以避免本“安全导则”的建议与国际电工委员会和电气和电子工程师协会的标准发生冲突。国际电工委员会和电气和电子工程师协会标准委员会的成员都参与了本“安全导则”的开发，两个标准组织都评审了草案，以帮助识别和消除冲突。

I-7. 然而，用户需要认识并考虑到国际电工委员会与电气和电子工程师协会标准之间存在重要差异这一事实。

I-8. 国际电工委员会标准将原子能机构的安全要求和安全导则作为制定其标准的基本输入。因此，国际电工委员会标准应对安全重要物项，并将原子能机构提供的仪器仪表和控制系统的导则作为总体建议的来源。

I-9. 电气和电子工程师协会标准主要侧重于安全物项，因此，与本“安全导则”相比，其导则直接适用于较小的功能、系统和设备集。然而，电气和电子工程师协会的导则可以应用于安全相关物项（不是安全系统的安全重要物项）。

I-10. 电气和电子工程师协会标准未将本“安全导则”作为参考。在电气和电子工程师协会标准框架中 IEEE 603（见表 I-1）等同于本“安全导则”。然而，本“安全导则”和电气和电子工程师协会标准响应相同的一套仪器仪表和控制系统设计原则。应当指出，电气和电子工程师协会标准经常使用术语“安全”、“安全相关的”和“1E”作为原子能机构术语“安全”的等效词。电气和电子工程师协会没有一个术语等同于原子能机构所使用的“安全相关的”。

I-11. 参考文献[I-2]包含了更广泛的仪器仪表和控制系统设计标准参考书目。

附件 I 参考文献

[I-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）。

[I-2] 国际原子能机构《核电厂仪器仪表和控制系统堆芯知识》，国际原子能机构《核能丛书》第 NP-T-3.12 号，国际原子能机构，维也纳（2011 年）。

附 件 II

本“安全导则”原子能机构《安全标准丛书》第 NS-G-1.1 号和第 NS-G-1.3 号之间的相关性

II-1. 本附件提供的表格显示了本“安全导则”的两个前身 NS-G-1.1 [1] 和 NS-G-1.3 [2] 所涵盖的主题在本“安全导则”中的位置。

表 II-1. 原子能机构《安全标准丛书》第 NS-G-1.1 号与本“安全导则”的对应关系

国际原子能机构《安全标准丛书》第 NS-G-1.1 号	本“安全导则”
1.说明	1.说明
2.计算机系统的技术考虑	2.仪控设计管理系统 9.软件：概述
3.安全管理要求在计算机系统中的应用	2.仪控设计管理系统 9.软件：第三方评定
4.项目计划	2.仪控设计管理系统
5.计算机系统要求	2.仪控设计管理系统
6.计算机系统设计	2.仪控设计管理系统 6.所有安全重要仪控系统的总体建议 7.特定仪控系统和设备的设计导则 8.关于人机界面的考虑
7.软件需求	9.软件：软件需求
8.软件设计	9.软件：软件设计
9.软件实现	9.软件：软件实现
10.核实与分析	9.软件：软件核实与分析

[1] 国际原子能机构《核电厂基于计算机安全重要系统的软件》,国际原子能机构《安全标准丛书》第 NS-G-1.1 号，国际原子能机构，维也纳（2000 年）。

[2] 国际原子能机构《核电厂安全重要仪器仪表和控制系统》,国际原子能机构《安全标准丛书》第 NS-G-1.3 号，国际原子能机构，维也纳（2002 年）。

表 II-1. 原子能机构《安全标准丛书》第 NS-G-1.1 号与本“安全导则”的对应关系（续）

国际原子能机构《安全标准丛书》第 NS-G-1.1 号	本“安全导则”
11.计算机系统集成	2.仪控设计管理系统
12.计算机系统的核实	2.仪控设计管理系统
13.安装调试	2.仪控设计管理系统
14.运行	2.仪控设计管理系统
15.交付后修改	2.仪控设计管理系统
附件：预先存在软件的使用和核实	2.仪控设计管理系统 9.软件：预先开发的软件

注：仪控：仪器仪表和控制。

表 II-2. 原子能机构《安全标准丛书》第 NS-G-1.3 号与本“安全导则”的对应关系

国际原子能机构《安全标准丛书》第 NS-G-1.3 号	本“安全导则”
1.介绍	1.介绍
2.安全重要仪控系统：	见参考文献[II-1]
—仪控系统的识别	3.仪控系统设计基准
—仪控系统分类	5.仪控功能、系统和设备的安全分类
3.设计基准	3.仪控系统设计基准

表 II-2. 原子能机构《安全标准丛书》第 NS-G-1.3 号与本“安全导则”的对应关系（续）

国际原子能机构《安全标准丛书》第 NS-G-1.3 号	本“安全导则”
4.总体设计导则：	
—性能要求	2.仪控设计管理系统：生命周期活动：规范要求
—可靠性设计	6.所有安全重要仪控系统的总体建议：设计的可靠性
—独立性	4.仪控架构：独立性 6.所有安全重要仪控系统的总体建议：设计的可靠性：独立性
—失效模式	6.所有安全重要仪控系统的总体建议：设计可靠性：故障模式
—设备使用控制	6.所有安全重要仪控系统的总体建议：控制进入安全重要系统 7.特定仪控设计导则：系统和设备：数字系统：计算机安全
—设定值	6.所有安全重要仪控系统的总体建议：设定值
—人机界面	8.关于人机界面的考虑
—设备鉴定	6.所有安全重要仪控系统的总体建议：设备鉴定
—质量	2.仪控设计管理系统
—电磁兼容设计	6.所有安全重要仪控系统的总体建议：设备鉴定：内部和外部危害：电磁鉴定
—试验和可试验性	6.所有安全重要仪控系统的总体建议：运行期间的试验和可试验性
—可维护性	6.所有安全重要仪控系统的总体建议：可维护性
—文档	2.仪控设计管理系统：所有生命周期阶段共同的活动：文件
—安全重要项目的识别	6.所有安全重要仪控系统的总体建议：对安全重要项目的标记和识别

表 II-2. 原子能机构《安全标准丛书》第 NS-G-1.3 号与本“安全导则”的对应关系（续）

国际原子能机构《安全标准丛书》第 NS-G-1.3 号	本“安全导则”
5.系统特定设计导则：	
—安全系统	7.特定仪控系统和设备的设计导则：保护系统
—保护系统	
—电源	7.特定仪控系统和设备的设计导则：电源
—数字计算机系统	7.特定仪控系统和设备的设计导则：数字系统
6.人机界面	8.关于人机界面的考虑
7.安全重要仪控系统设计过程	2.仪控设计管理系统：生命周期活动：修改

附件 II 参考文献

[II-1] 国际原子能机构《核电厂仪器仪表和控制系统的核心知识》，国际原子能机构《核能丛书》第 NP-T-3.12 号，国际原子能机构，维也纳（2011 年）。

附 件 III

成员国不同领域的实践

导言

III-1. 在一些领域，支持仪器仪表和控制（仪控）安全设计标准的学术基础或工程实践并没有得到所有成员国的广泛接受。本附件讨论在制定本“安全导则”过程中识别的存在差异的领域。可以预期成员国的实践将随着时间的推移而改进。

数字化系统可靠性的确定

III-2. 如果在多个冗余的数字化系统中使用相同的软件，则软件错误可能导致冗余数字系统中的共因故障。因此，为了估计数字化系统的可靠性，有必要估计由于硬件故障而导致系统故障的概率，以及对于一些成员国而言，估计软件错误的概率。对其他成员国来说，设计错误（包括软件错误）及其后果只有通过对结构和设计的定性分析才能得到充分处理。

III-3. 一些成员国在制定仪器仪表和控制设计基准时，确保仪器仪表和控制系统的可靠性要求与概率安全分析之间的一致性，为每一个安全重要仪器仪表和控制系统保持明确的可靠性目标数值。因此，这些成员国认为，数字化系统可靠性的数值评估是证明可靠性的一个必要因素。

III-4. 对于将可靠性数值应用于软件的成员国来说，目前无法证明软件可靠性高的说法。因此，需要谨慎对待要求单个计算机系统实现软件按 PFD 低于 10^{-4} 的设计。

III-5. 一些对数字化系统使用可靠性数值评估的监管机构已经对对仪器仪表和控制系统设定了它们认为合理的可靠性水平限值。例如，对任何无论使用何种技术，基于公共平台的仪器仪表和控制系统都被限值为 10^{-5} PFD，并且对于基于公共计算机平台的任何单一仪器仪表和控制系统的可靠性要求都被限值为 10^{-4} PFD，无论在多大程度上采用了本“安全导则”中描述的策略（例如，冗余）。

III-6. 一些成员国使用定性方法来确定软件的可靠性。这种定性方法通常基于对软件确定性行为的严格要求，以允许充分的核实和验证。这种强大的设计需求组合，允许充分的核实和验证，使人们对软件的可靠性有很高的信心。

安全系统中共因脆弱性的评定

III-7. 本“安全导则”第 4.32 段指出：

> “对安全分析范围内每一假想始发事件，应分析其叠加妨碍保护系统发挥必要安全功能的共因故障所产生的后果。”

在这一点上，人们普遍同意，但对于分析的范围、在假想始发事件叠加安全系统共因故障时可接受的放射性后果，或在确定放射性后果时所使用的分析方法的类型，并没有达到普遍的一致意见。

分析范围

III-8. 监管机构对第 4.32 段所述分析的预期范围。包括以下示例：

— 安全系统共因故障叠加被认为是预计运行事件的假想始发事件和设计基准事故工况的分析；
— 发生频率大于 10^{-3}/年的假想始发事件叠加安全系统同原因故障的分析。

可接受的后果

III-9. 如果假想始发事件与安全系统中的共同原因故障同时发生，监管机构可能接受的后果示例包括：

— 与反应堆保护系统中的共因故障同时发生的预计运行事件的后果，但不会导致：
  • 在裂变产物释放开始后在禁区边界的任何一点停留 2 小时，或在裂变产物释放的整个期间停留在低人口区边界，接受碘对甲状腺的全身剂量超过 25 毫希沃特或剂量超过 300 毫希沃特的任何个人；或

- 超过一次冷却剂系统的设计限值。

— 与反应堆保护系统中的共因故障同时发生的设计基准事故的后果，该事故不导致：
  - 裂变产物释放开始后在禁区边界的任何一点停留 2 小时，或在整个裂变产物释放期间停留在低人口区边界，接受碘对甲状腺的全身剂量超过 0.25 毫希沃特或超过 3 毫希沃特；或
  - 超过一次侧冷却剂系统或安全壳的设计限值。
— 同时发生设计基准事故和反应堆保护系统共因故障后，其余安全系统应能够：
  - 确保达到监管机构与许可证持有者所约定的剂量限值；
  - 防止一次侧传热系统因超压而失效；
  - 防止燃料超温；
  - 防止燃料破裂；
  - 在不危及安全壳完整性的情况下，限制核功率上升速度和核功率总量；
  - 将反应堆保持在次临界状态的时间足够长，以提供确保次临界状态的替代方法。
— 为防止或缓解共因故障后果而提供的多样性和其他手段确保系统功能具有足够高的可靠性；
— 如果安全系统发生故障，设计基准事故的后果不超过可接受的剂量限值。

分析方法

III-10. 在确定后果时，作为第 4.32 段所述分析的一部分。一些监管机构期望使用保守的方法；另一些则允许使用最佳估计方法。原子能机构《安全标准丛书》第 SSG-2 号《核电厂确定性安全分析》[III-1]讨论了保守方法和最佳估计分析方法。

多样化驱动系统

III-11. 当使用数字化系统来实现保护系统功能时，第 4.32 段所述的分析经常用于找出可能产生不可接受后果的某些数字化保护系统共因故障和假想始发事件的组合。当遇到这种情况时，通常提供不同的驱动系统用于保护系统的后备。

III-12. 人们普遍认同一个多样化的驱动系统可以有效地缓解特定假想始发事件叠加保护系统同时发生假设共因故障的后果。然而，也有不同的安全分级方法，可使用多样化的数字化驱动系统用作数字化保护系统的后备，以及使用手动驱动来缓解保护系统共因故障的后果。

安全分级

III-13. 一些监管机构期望将多样化的驱动系统归为安全系统。一些监管机构允许它们是安全级别较低的系统。一些监管机构基于对多样化驱动系统的可靠性要求来确定所期望的安全等级。

多样化驱动系统技术

III-14. 一些监管机构期望多样化驱动系统将是硬接线系统。有些管理机构不鼓励，但不禁止数字化系统的使用。一些监管机构允许使用数字化系统，如果证明有足够的多样性。

用于多样化驱动的手动动作的使用

III-15. 通常接受手动驱动作为为保护系统的后备，但是采用手动驱动的条件则千变万化。可接受的实践包括：

- 如果在 30 分钟内不需要手动动作，并且人因分析已验证在该时间内可以做出并执行适当的决定，则手动动作是可信的；
- 如果在 20 分钟内不需要手动动作，则手动动作是可信的；
- 用于驱动专设安全设施手动动作是可信的，但不用于反应堆跳闸；
- 手动动作是可信的，不受任何约束。

III-16. 虽然上文说明了监管机构的各种实践，但监管机构可以根据拟议的具体情况采取不同的实践。

附件 III　参考文献

[III-1] 国际原子能机构《核电厂确定性安全分析》，国际原子能机构《安全标准丛书》第 SSG-2 号，国际原子能机构，维也纳（2009 年）。

定　义

下列定义特定于此出版物，不是《国际原子能机构安全术语》中所规定的或不同于《国际原子能机构安全术语》中规定的：

核安全和辐射防护术语（2007 年版），

原子能机构，维也纳（2007 年）：

http://www-pub.iaea.org/books/iaeabooks/7648/iaea-safety-glossary

符号“*”表示的定义不同于原子能机构安全术语中的定义。

架构。核电厂安全重要仪器仪表和控制系统的组织结构。

可用性*。在给定的条件下，在给定的时间瞬间或给定的时间间隔内，一件物品处于某种状态以执行所需功能的能力，前提是提供了必要的外部资源。

校准*。在规定的条件下建定测量仪器仪表或测量系统所指示的量值或实物量具或参考实物所代表的值与根据标准所实现的相应值之间关系的一组操作。

组件*。组成系统的一部分。一个部件可以是硬件或软件，并可以再细分为其他的部件。

注意：术语“设备”、“组件”和“模块”通常可以互换使用。这些术语的关系尚未标准化。

配置基线。在物项生命周期的特定时间正式指定和固定的一组配置物项。

确定性行为。系统或部件的特性，使得在该物项的规格说明范围内的任何给定输入序列总是产生相同的输出。

确定性时序。系统或部件的特性，使得刺激和响应之间的时间延迟具有保证的最大值和最小值。

多样性*。两个或多个冗余系统或部件执行同一功能，这些不同系统或部件具有不同属性，从而减少包括共模故障在内共因故障的可能性。

注 1：当“多样性”一词带有附加属性时，“多样性”一词表示“存在两种或两种以上实现特定目标的不同方式或手段”的一般含义，

而属性表示所采用的不同方式的特征，如功能多样性、设备多样性、信号多样性。

注 2：另见原子能机构《安全术语》中“功能多样性”一栏。

序列。一个冗余系统或安全组的一个冗余物项的集合，包括它们的互连。序列可以包括多个通道。

现场可编程门阵列。一种可由仪器仪表和控制制造商在现场编程的集成电路。它包括可编程逻辑模块（组合和时序）、它们之间的可编程互连以及用于输入和/或输出的可编程模块。然后功能由仪器仪表和控制设计人员定义，而不是由电路制造商定义。

固件。与所安装的硬件特性紧密耦合的软件。

功能需求。指定物项所需功能或行为的要求。

硬件描述语言。一种语言，允许人们正式描述电子元件的功能和/或结构，用于文档、模拟或合成。

硬件编程设备硬件编程设备。可以是配置的集成电路（用于核电厂仪器仪表和控制系统），具有硬件描述语言和相关软件工具。

危害。造成损害的可能性。

危害因素。对潜在危害有贡献的因素。

危害分析。在一个系统的整个生命周期中对其进行检测的过程，以确定其固有的危害和促成的危害，以及消除、预防或控制这些危害的要求和限值。

注：危害分析的范围超出了电厂的设计基准事故，包括异常事件和电厂退化的设备和系统的电厂运行。

人机界面。运行人员与仪器仪表和控制系统之间的接口，以及与电厂相连的计算机系统。界面包括显示、控制和与操作员支持系统的界面。

非功能性需求（也称为质量需求）。规定物项除所要求的功能和行为之外的的固有属性或特征的要求。示例特征包括可分析性、可保证性、可监

查性、可用性、兼容性、文档化、完整性、可维护性、可靠性、安全、安保、可用性和可核实性。

预开发块。可用于硬件描述语言的预开发功能块。例如，预先开发的块包括库、宏或知识产权核心。在并入硬件编程设备之前，预先开发的块可能需要大量工作。

预先开发的物项。已存在的项目，作为商业或专有产品提供，并正在考虑在仪器仪表和控制系统中使用。预开发的项目包括硬件设备、预开发的软件、商用现成设备、由硬件和软件组成的数字设备、或配置有硬件定义语言或预开发块的硬件设备。

需求工程。一种工程过程，包括开发、记录和维护一组需求所涉及的活动。

静态分析。基于系统或组件的形式、结构、内容或文档的分析。

型式试验。对代表产品的一个或多个项目进行的一致性试验。

验证*。通过检测和提供其他证据来验证系统完全满足预期的需求规范。

核实*。通过检测和提供客观证据，验证一项活动的结果符合为该活动确定的目标和要求。

参与起草和审订人员

Alpeev, A.	俄罗斯联邦核与辐射安全科学与工程中心
Alvarado, R.	美国核管制委员会
Asikainen, S.	芬兰工业部
Babcock, B.	加拿大安大略电力公司
Benitez-Read, J.	墨西哥国家核研究所
Bicer, C.	土耳其原子能机构
Boeva, T.	保加利亚科兹洛杜伊核电厂
Bouard, J.-P.	法国电力公司
Bowell, M.	英国核监管办公室
Curtis, D.	顾问
Debor, J.	顾问
Duchac, A.	国际原子能机构
Edvinsson, H.	瑞典万滕福尔电力公司
Eriksson, K.-E.	瑞典奥斯卡港核电厂
Faya, A.	阿拉伯联合酋长国联邦核管制机构
Fichman, R.	加拿大安大略电力公司
Furieri, E.-B.	巴西国家核能委员会
Gassino, J.	法国辐射防护与核安全研究所
Gonchukov, V.	俄罗斯联邦环境、工业与核监督服务局
Göring, M.	德国 Vattenfall 公司
Harber, J.	加拿大原子能有限公司
Hohendorf, R.	加拿大安大略电力公司
Johnson, G.	国际原子能机构

Karasek, A.	捷克电力公司
Kawaguchi, K.	日本核监管局
Kim, B.-Y.	韩国核安全研究所
Klopkov, V.	俄罗斯联邦环境、工业与核监督服务局
Lee, J.-S.	韩国原子能研究所
Li, H.	美国核管制委员会
Lindskog, U.	瑞典奥斯卡港核电厂
Mangi, A.	巴基斯坦核监管机构
Ngo, C.	加拿大坎杜公司
Odess-Gillett, W.	美国西屋电力公司
Park, H.-S.	韩国核安全研究所
Parsons, A.	英国艾铭集团公司
Piljugin, E.	德国装置与反应堆安全公司
Poulat, B.	国际原子能机构
Régnier, P.	法国辐射防护与核安全研究所
Santos, D.	美国核管制委员会
Seidel, F.	德国联邦辐射防护办公室
Shumov, S.	俄罗斯联邦仪器工程专业科学研究所
Sjövall, H.	芬兰工业部
Stattel, R.	美国核管制委员会
Svensson, C.	瑞典奥斯卡港核电厂
Takala, H.	芬兰辐射与核安全局
Takita, M.	日本核监管局
Tate, R.	英国核监管办公室

Thuy, N.	法国电力公司
Welbourne, D.	顾问
Yastrebenetsky, M.	乌克兰国家核与辐射安全科学技术中心
Yates, R.	英国核监管办公室
Zeng, Z.-C.	加拿大核安全委员会

IAEA
国 际 原 子 能 机 构

No. 26

当 地 订 购

国际原子能机构的定价出版物可从下列来源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。联系方式见本列表末尾。

北美

Bernan / Rowman & Littlefield
15250 NBN Way, Blue Ridge Summit, PA 17214, USA
电话：+1 800 462 6420 • 传真：+1 800 338 4550
电子信箱：orders@rowman.com • 网址：www.rowman.com/bernan

世界其他地区

请联系您当地的首选供应商或我们的主要经销商：

Eurospan Group
Gray's Inn House
127 Clerkenwell Road
London EC1R 5DB
United Kingdom

交易订单和查询：
电话：+44 (0) 176 760 4972 • 传真：+44 (0) 176 760 1640
电子信箱：eurospan@turpin-distribution.com

单个订单：
www.eurospanbookstore.com/iaea

欲了解更多信息：
电话：+44 (0) 207 240 0856 • 传真：+44 (0) 207 379 0609
电子信箱：info@eurospangroup.com • 网址：www.eurospangroup.com

定价和未定价出版物的订单均可直接发送至：

Marketing and Sales Unit
International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
电话：+43 1 2600 22529 或 22530 • 传真：+43 1 26007 22529
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