国际原子能机构安全标准

保 护 人 类 与 环 境

核电厂电力系统的设计

特定安全导则

第 SSG-34 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。

核电厂电力系统的设计

国际原子能机构的成员国

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

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

国际原子能机构《安全标准丛书》第 SSG-34 号

核电厂电力系统的设计

特定安全导则

国 际 原 子 能 机 构
2024 年 · 维也纳

版 权 说 明

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

国际原子能机构印刷
2024 年 2 月 • 奥地利

核电厂电力系统的设计

国际原子能机构，奥地利，2024 年 2 月
STI/PUB/1673
ISBN 978-92-0-504223-7（简装书：碱性纸）
978-92-0-504123-0（pdf 格式）
ISSN 1020-5853

前　言

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

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

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

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

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

国际原子能机构安全标准

背景

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

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

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

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

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

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

原子能机构安全标准

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

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

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

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

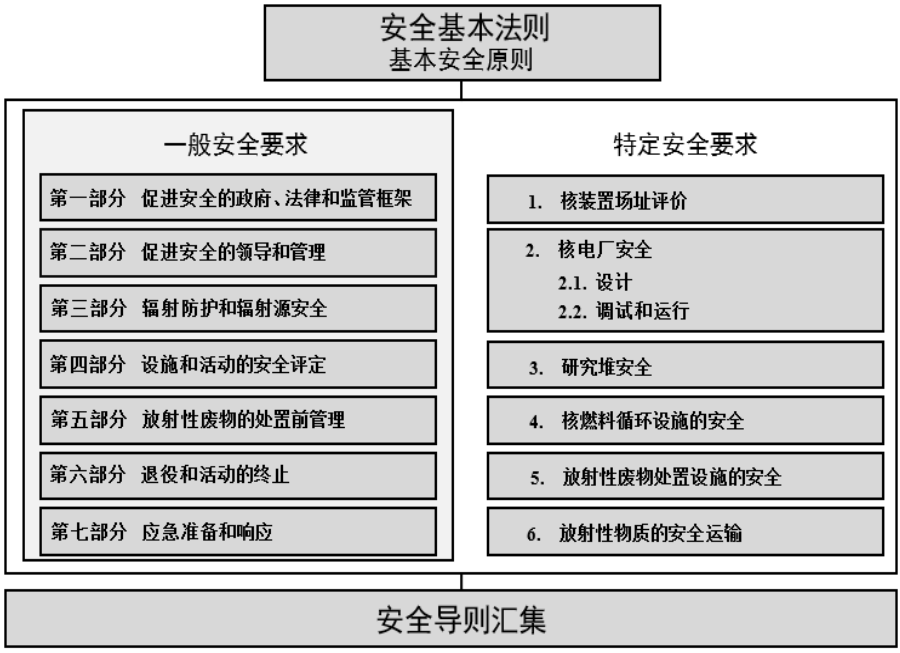


图 1. 国际原子能机构《安全标准丛书》的长期结构。

[1] 另见以原子能机构《核安保丛书》印发的出版物。

安全基本法则

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

安全要求

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

安全导则

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

原子能机构安全标准的适用

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

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

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

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

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

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

原子能机构安全标准的制定过程

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

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

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

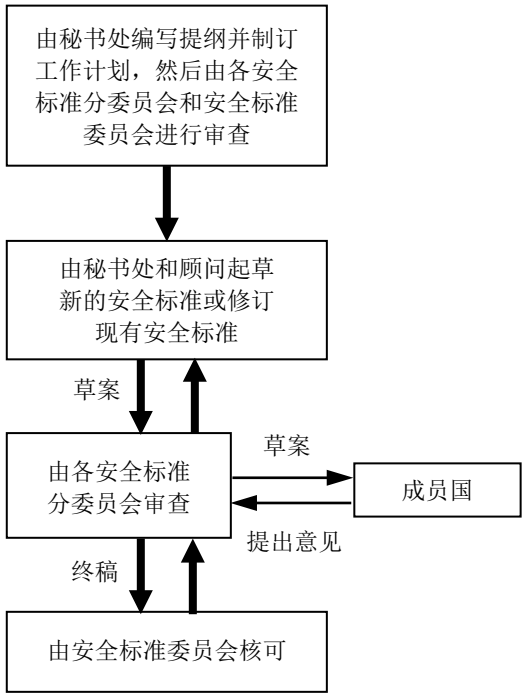


图 2. 制订新安全标准或修订现行标准的过程。

与其他国际组织的合作关系

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

文本的解释

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

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

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

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

目 录

1. 导言

背景

1.1. 本“安全导则”是“特定安全要求”出版物原子能机构《安全标准丛书》第 SSR-2/1（Rev.1）号《核电厂安全：设计》[1]支持性文件，对核电厂的设计提出了要求。

1.2. 本“安全导则”就核电厂电力系统所必备的特性以及如何设计这些系统提出了建议，以满足 SSR-2/1（Rev.1）[1]规定的安全要求。该导则体现了对 SSR-2/1 [1] 特别是对要求 68（译者注：能够经受丧失场外电源的设计）所做的修订。

1.3. 本“安全导则”是对 2004 年出版的原子能机构《安全标准丛书》第 NS-G-1.8 号《核电厂应急电力系统设计》的升版 [2]，同时旧版废止。本“安全导则”给出核电厂应急电力系统的设计要求，并且进一步提出所有为安全重要系统供电的电力系统的设计要求（见图 1 和图 2）。

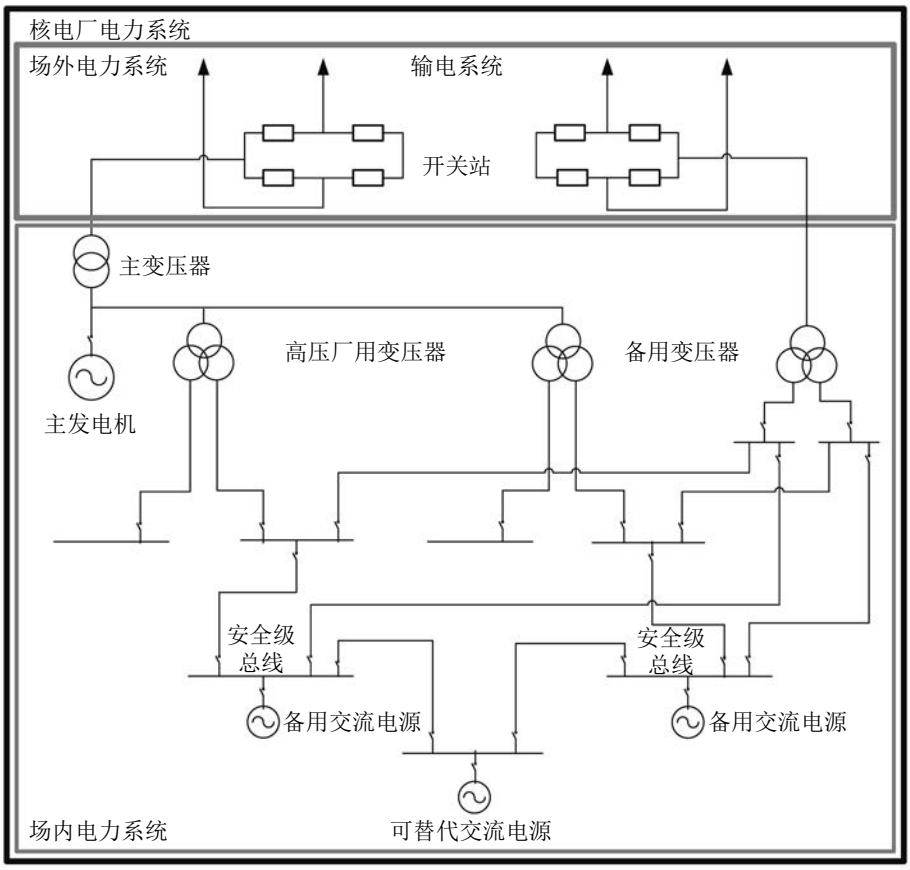
1.4. 已废止的标准 NS-G-1.8 还包含对非电力应急电力系统的相关要求，此部分内容将在新的核电厂辅助和支持系统安全导则中体现，目前该导则正在编写中。

1.5. 为安全重要系统供电的电力系统对核电厂的安全是非常关键的。这类电力系统包括相互配合的场内和场外电力系统，以确保核电厂在各种工况下都能提供维持安全状态所必需的电力。场外电力系统本身不属于核电厂设备，但对核电厂的安全和纵深防御至关重要。

---

[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 号，国际原子能机构，维也纳（2012 年）。

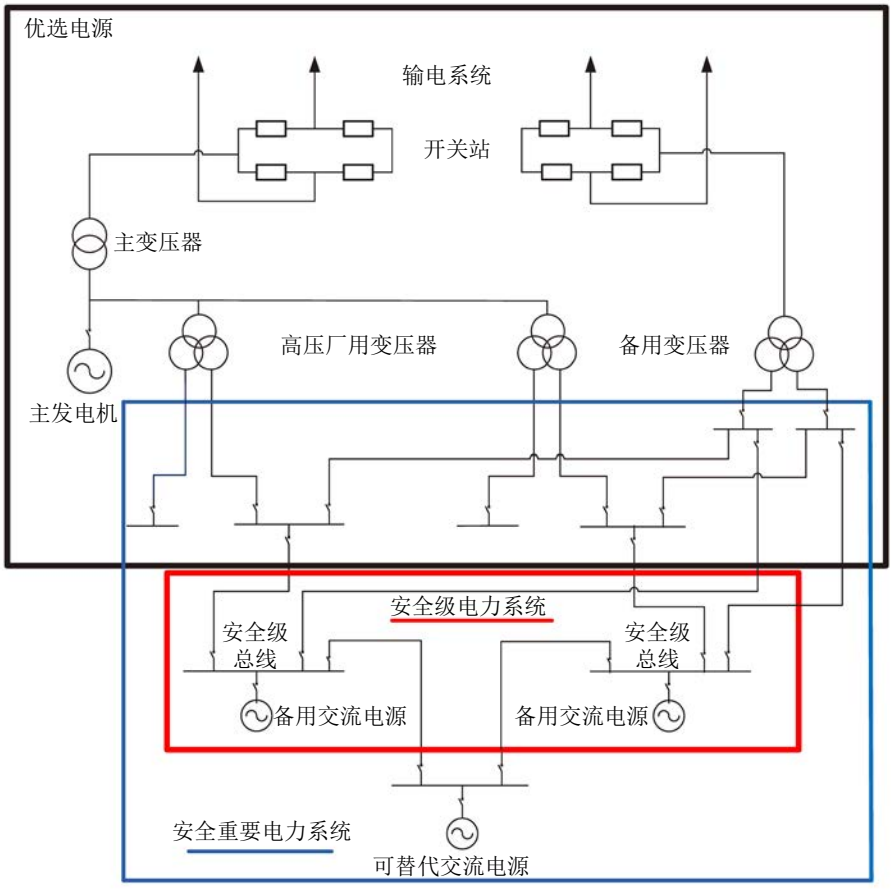
[2] 国际原子能机构《核电厂系统应急电源设计》，国际原子能机构《安全标准丛书》第 NS-G-1.8 号，国际原子能机构，维也纳（2004 年）。



注：满足 SSR-2/1（Rev.1）[1] 要求的系统接线有多种型式，本图仅为其中一种示例。此外，其他诸如非安全级总线或直流电力系统未在本图中体现。

图 1. 核电厂场外电力系统和场内电力系统的联系。

1.6. 本“安全导则”确定的优选电源是传输系统的电源，或从主发电机到安全级电力系统的电源。该电源由输电系统、开关站、主发电机和配电系统组成，直至安全级的电力系统。作为场外电力系统（如输电系统）一部分的优选电源部分不是电厂设备，因此不属于电厂安全分级的一部分（见图 2）。场外电源和场内电源之间的边界位置将由电厂特定决定。



注：满足 SSR-2/1（Rev.1）[1] 的要求的系统接线有多种型式，本图仅为其中一种示例。本图仅体现核电厂安全级电力系统和优选电源之间的联系，其他诸如非安全级总线或直流电力系统未在本图中体现。对不属于安全重要电力系统范围的优选电源设备，不需划为安全级。不同的国家因其电厂设计和分级方法不同，属于安全重要电力系统的范围也不同。有些电厂的设计不要求配备安全级备用电源，但所有的核电厂一般都应配置安全级直流电源。AC 表示交流。

图 2. 核电厂安全重要电力系统、安全级电力系统和优选电源间的联系。

1.7. 将本“安全导则”提出的所有建议都应用到在运和在建的核电厂可能不太实际。对于此类设计的安全分析，预计将与现行标准进行比较，例如作为电厂定期安全评审的一部分，以确定是否可以通过切实可行的安全改进来进一步加强电厂的安全运行。

目的

1.8. 本“安全导则”的目的是提出对核电厂电力系统设计的建议和指导，以满足 SSR-2/1（Rev.1）[1]要求 41、68 以及第 2－5 部分中的一般要求。本“安全导则”供从事核电厂设计、运行、维护、改造、评定和许可证申请工作的设计人员、评审人员、安全评定人员、监管机构、营运组织和运行人员参考使用。本“安全导则”没有对执行过程和使用的技术细节提出指导，但给出了相关解释。

范围

1.9. 本“安全导则”对新建和在运核电厂的电力系统提出建议和指导，本“安全导则”适用于核电厂所有安全重要电力系统和优选电源。

1.10. 本“安全导则”适用于所有类型的核电厂。电力系统的分级所给出的安全重要电力系统和安全电力系统的程度根据设计而不同。本“安全导则”概述了在不同电压水平下保持纵深防御和多样性所需电力系统的最低推荐设计要求。在任何情况下，本“安全导则”都应与电厂的安全分析报告一起使用，以确定不同电源的安全意义和重要性。例如，在具有非能动工程安全特性的电厂中，电力系统的分级可能与图 2 所示的分级有显著的不同。

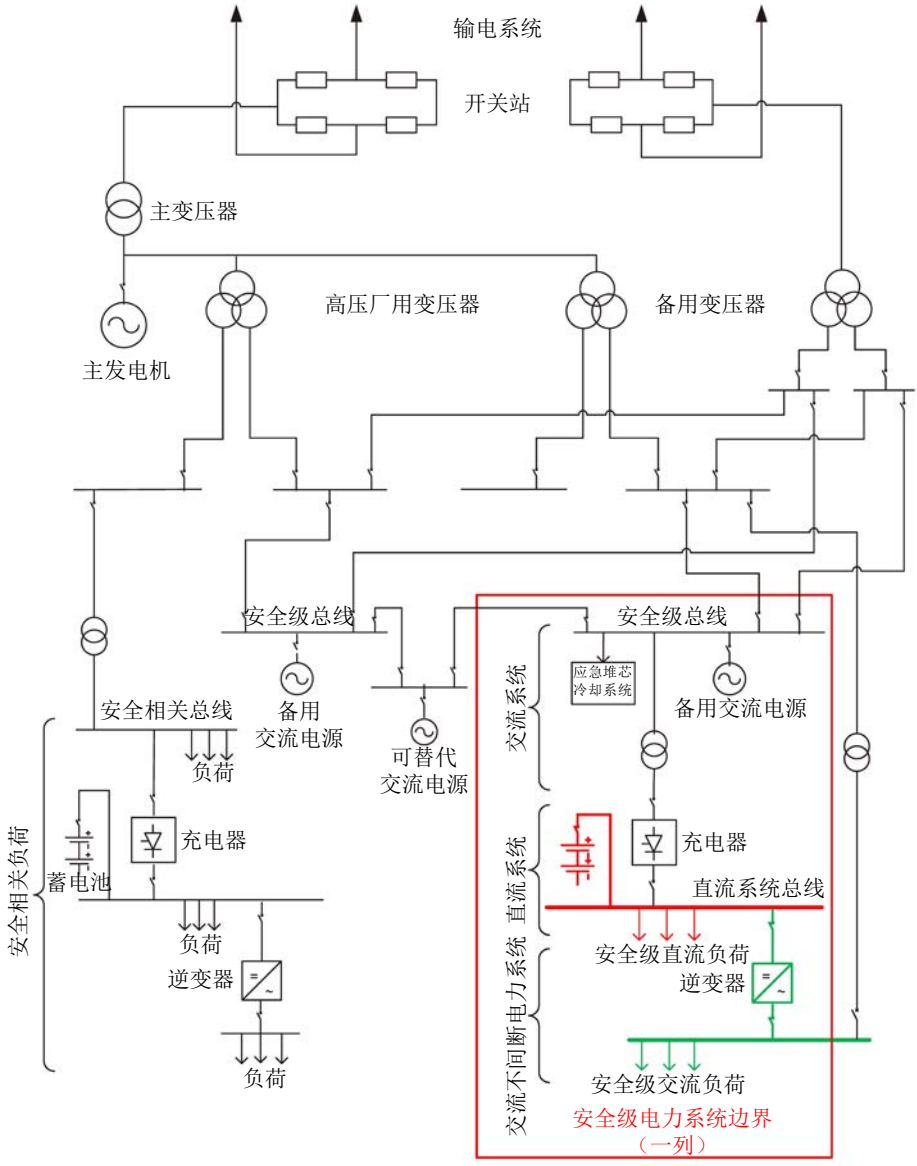
1.11. 相关核电厂电力系统控制和保护用电子设备的其他建议在原子能机构《安全标准丛书》第 SSG-39 号《核电厂仪器仪表和控制系统的设计》[2]提出。

1.12. 图 1－图 3 展示的几个核电厂电力系统设计示例说明了本“安全导则”的适用范围和使用的术语。相关术语的详细解释可见术语定义。

1.13. 本“安全导则”适用于核电厂电力系统，没有对用电负荷提出特定要求，但用电负荷的技术规范需与电力系统设计原则相适应。

1.14. 本“安全导则”不适用于核电厂安保系统（如围栏、监视系统和出入控制系统）的供电。

1.15. 本“安全导则”应与原子能机构《安全标准丛书》的其他相关安全标准结合使用。



注：AC — 交流电；DC — 直流电；ECCS — 应急堆芯冷却剂系统。

图 3. 安全导则所述核电厂供电电源各部分之间的关系原理图。

1.16. 相关电力系统和设备的设计及开发的其他导则可从标准制定国和制定机构获取。这些文件比原子能机构《安全标准丛书》更为具体，本“安全导则”应与这些特定的工业标准结合使用。

1.17. 电力系统设计时，应分析和管理核安保和安全之间一些潜在的接口。在原子能机构《核安保丛书》第 13 号（INFCIRC/225/Rev.5）《核材料和核设施实物保护的核安保建议》[3]）中对核设施的安保提出了要求。

结构

1.18. 第 2 部分主要介绍核电厂典型的电力系统所包含的主要系统，并提出每个系统所需达到的基本目标。

1.19. 第 3 部分介绍电力系统的安全分级。

1.20. 第 4 部分概述电力系统设计基准所应包含的内容。

1.21. 第 5 部分对所有交流和直流系统提出总体性要求，是需要满足的最低要求；第 6－9 部分对一些系统提出了特定要求，这些要求应与第 5 部分结合使用。

1.22. 第 6 部分对优选电源提出了建议。优选电源向电厂所有安全重要系统提供正常电源，且在其可用时，应作为电厂所有供电电源中的优先选择。

1.23. 第 7 部分介绍安全级电力系统设计的特定要求，包括安全级备用电源。

1.24. 第 8 部分介绍备用交流电源设计的特定要求，本部分是对第 5 部分所做的补充。备用交流电源通常是为应对场外交流电源和场内应急交流电源同时故障而设置的。

1.25. 第 9 部分对电力系统的设计确认和所提交的系统文件提出要求，这些文件用来支持电厂的安全分析与运行、维护、试验和核实。

1.26. 附录 I 论述电力系统设计和 SSR-2/1（Rev.1）[1]所述纵深防御概念之间的关系。

1.27. 附录 II 介绍一种为核实核电厂设计而开展的电力系统分析示例。

2. 核电厂电力系统

核电厂电力系统介绍

2.1. 图 1－图 3 所示为核电厂电力系统的主要框架。一个特定的电厂电力系统设计取决于电网、场内系统设计和工程设计方案（不在本“安全导则”范围内）。因此，图 1－图 3 不能作为任意特定电厂的推荐设计方案。

2.2. 安全电力系统可以由优选电源或备用电源供电。备用交流电源也可以在设计扩展工况下为安全电力系统供电。

2.3. 本“安全导则”主要讨论核电厂电力系统的三个子系统：场外电力系统、场内电力系统和优选电力系统。下文将对本“安全导则”所使用的这几个术语进行解释。在本“安全导则”以外引用这几个术语时，可能会因核电厂采用的特定设计方案不同，而与本“安全导则”有不同的含义。

场外电力系统

2.4. 场外电力系统由输电系统（电网）和连接电厂与电网的开关站组成。场外电力系统通常在所有运行模式和所有电厂状态下向电厂提供交流电。它还为输出电力提供输电线路（见图 1）场内和场外电力系统之间的边界位于输电系统运营商所属设备与核电厂营运组织所属设备连接的位置。边界通常位于变压器电网侧的套管处，该套管与输电电压相连，或位于高压断路器最靠近电厂的电网侧。

2.5. 场外电力系统在安全方面发挥着重要作用，为场内电力系统提供来自多种电源的可靠电源：(i) 通过辅助变压器的主发电机；以及 (ii) 经由备用变压器的电网电力供应。场外电力系统是优选电源的一部分（见图 2）。

2.6. 固有健稳的电网系统提供了高度可靠的场外电源，因为它在正常运行中可以快速抑制电网扰动的影响，并最大限度地减少核电厂连接电力系统中的电压和频率波动。同样，具有快速汽轮机调速器和发电机励磁系统的大型核电机组也能对电网系统的健稳性产生相当大的影响。由于这种相互依赖性，在电网或核电厂发生重大运行变化期间，电网和核电厂营运组织之间通过设计实现的良好功能集成以及良好的运行协调是电网和核电厂安全可靠运行的重要需求。

场内电力系统

2.7. 场内电力系统（见图 1）由场内配电系统和电源组成。它包括必要的交流和直流电源，以便在预计运行事件或事故工况下使电厂进入受控状态，并将其保持在受控状态或安全状态，直到可以恢复场外电源。不包括独立电源，例如用于安保系统的独立电源。场内电力系统根据其安全重要性划分为安全重要系统（安全系统和安全相关系统）和非安全重要系统。

2.8. 场内电力系统的主要部件包括主发电机、发电机升压变压器、辅助变压器、备用变压器和配电系统馈电装置辅助设备、服务辅助设备、开关设备、电池、整流器、逆变器和/或不间断电源、电缆和备用交流电源（见图 1）。场内电力系统的部件是优选电源的一部分。

2.9. 根据负载的供电要求，场内电力系统通常可分为三类：

(a) 交流电力系统：指定交流负载的功能将允许出现一定的供电中断。通常，交流电力系统包括备用交流电源和可备用交流电源。保护继电器检测到电力系统的优选交流电源的丧失，并自动启动备用电源。在大多数情况下，电厂安全分析中假设备用交流电源将用于设计基准事故后的机组停堆，可备用交流电源多用于设计扩展工况。

(b) 直流电力系统：这样就可以不间断地从蓄电池向直流负载供电。直流电力系统包括连接到电力系统的交流电力系统的电池充电器。有时提供独立的直流电力系统来支持不同安全级的负载。

(c) 交流不间断电力系统：它从逆变器或电动发电机组供电，而逆变器或电动发电机组又由直流电源供电，如直流电力系统或带整流器的专用电池，并包括一个旁路电路，以便在维护和紧急情况下直接从安全级交流电力系统向安全级负载供电。

优选电源

2.10. 优选电源是电厂所有安全重要系统的正常供电电源。在其可用时，它始终作为安全级电力系统的首要供电电源。优选电源包括场内和场外电力系统部分（见图 2）。

规范和标准的作用

2.11. SSR-2/1[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规则和标准进行设计。”

2.12. 场外电力系统应满足国家和国际标准、电网规范和电力设计标准（国家电力规范规定）中规定的核安全标准。

2.13. 核电厂电力系统的设计和建造应符合国家和国际核标准以及国家安全规则，以确保核电厂所有运行模式的高可靠性和高可用性。

2.14. 国家安全规则为电力系统的安全可靠运行提供了可接受的设计要求导则。遵守这些安全规则通常为核电厂电力系统的能力提供合理的保证。

核安全要求的设计考虑

2.15. 核电厂的电力系统和部件从场内和场外电源向核电厂的辅助系统供电。

2.16. 核电厂的场外电源和系统应坚固耐用，在所有核电场状态和运行工况下都应高度可靠。场内电力系统的设计应考虑场外电力系统的能力有限性及其对核安全的影响。

2.17. 稳定可靠的电网（包括可靠的发电机组、输电系统和配电系统）是核电厂安全的基础。

2.18. 当核电厂运行时，电网扰动可能会对安全造成威胁：

- 正常并网发电；
- 通过电网倒送电来启动和停堆；
- 在特定事件和预计运行事件期间，作为电网的高优先级负载供电。

2.19. 健稳的系统应具备：

(a) 足够的裕度和固有的保守性，使达到预期目标所需的设备额定值、能力和容量不易受到威胁；

(b) 为适应场内和场外电力系统运行的预期变化而选择的设备保护整定值；

(c) 支持应急运行的能力，包括持续过载工况或过电压工况以及必要时启动的保护措施，以保持安全电力系统的功能。

2.20. 所有电压等级的电力系统都是大多数电厂设备的支持系统。可靠的电源对于在预计偏离正常运行期间保持控制，以及在设计基准事故和设计扩展工况下为相关电厂安全功能供电、控制和监控至关重要。

2.21. 在停堆期间，核电厂的部分电力系统可能因试验或维护而停运。当电厂关闭时，对电力系统的健稳性、可靠性和可用性的威胁将不同于在功率运行期间必须解决的威胁。

2.22. SSR-2/1（Rev.1）[1]要求 4 和第 4.1 段指出：

> “应确保所有核电厂状态都能实现核电厂的以下基本安全功能：(i) 反应性控制；(ii) 从所述反应堆和所述燃料库中排出热量；(iii) 密封放射性物质、屏蔽辐射和控制计划的放射性排放，以及限制意外的放射性排放。
>
> “4.1. 应采取系统化方法来识别那些安全重要物项，这些物项是实现基本安全功能所必需的，并识别有助于实现或影响所有电厂状态的基本安全功能的固有特性。”

2.23. 应采用系统化方法来确定必要的电力结构、系统和部件，以便实现基本安全功能所必需的物项可以由适当安全分级和可靠性的电源供电。

2.24. “可靠性”是指设计、试验、运行和维护的正确实施确保电力系统能够在最小干扰的情况下执行其功能。

2.25. 可以在场内外采取多种措施以实现所需的电力供应可靠性。这些措施可能涉及提高电厂的正常电源（优选电源）的可靠性，或者在正常电源可能不可用时向电力系统提供其他电源。这也可能包括为特别重要的安全级系统使用专用电源。

2.26. 防止共因故障的要素是对可能对电力系统造成威胁的事件并采取有效措施，明确定义设计基准并定期复核，适当地采用电源多样性配置。

2.27. 应特别关注安全级系统和安全级较低的系统之间的接口设计，需确保核电厂电力系统扰动时，非安全相关设备不会对安全级设备造成不利影响。

电力设计标准的设计注意事项

2.28. SSR-2/1（Rev.1）[1]要求 41 规定：

> “对核电厂安全重要物项的功能不应受到电网干扰的影响，包括电网电源电压和频率的预期变化。”

2.29. 设计时应考虑可能影响核电厂电力系统和部件的电压和频率的暂态和准稳态变化。

2.30. 电厂的保护方案和电厂部件的设计应确保优选电源中的干扰不会危及安全电力系统和连接负载的所需运行。

2.31. 在应急行动中，为了优先考虑安全行动，可以将设备保护减少到必要的一组。

核电厂作为发电设施接入电网要求

2.32. 根据国家法律、国家电网规则或每个输电系统运营商与每个发电设施之间的双边协议，发电设施的设计应支持电网系统的高度可靠运行。

2.33. 电网的高可靠性对于核电厂的安全可靠电力供应至关重要。输电系统运营商有责任确保核电厂有可靠的电力供应，并有责任将其电力输送给配电运营商。

2.34. 电网标准中应明确核电厂的特性和设计要求。

人员和设备安全

2.35. 电力系统的设计应尽量减少对人员的风险，并尽量减少因高温、弧光或额定电流、过电流或设备上的任何内部机械应力引起的机械应力而对设备造成的损坏。

2.36. 电力系统的设计和建造应确保其能够承受任何电厂状态或运行模式下可能出现的电压。

3. 电力系统的分级

3.1. SSR-2/1（Rev.1）[1]要求 18 规定：

> “应规定对核电厂安全重要物项的工程设计规则，并应符合相关国家或国际规则和标准以及经证实的工程实践，同时适当考虑其与核电技术的相关性。”

3.2. 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级。”

3.3. 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。”

3.4. 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。”

3.5. 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》[4]提出了建议和指导如何满足 SSR-2/1（Rev.1）[1]相关要求，用于识别安全重要的结构、系统和部件，并根据其功能和安全重要性对其进行分级。

3.6. SSG-30[4]推荐的安全分级流程符合 SSR-2/1（Rev.1）[1]提出的纵深防御概念，并考虑了不同纵深防御层次所执行的功能。

3.7. 对于一个核电厂，分级流程应主要涵盖：

— 电厂设计基准和电厂固有安全特性；
— SSR-2/1（Rev.1）[1]要求 16 规定的所有假想始发事件清单。作为电厂的设计基准应考虑假想始发事件的发生频率。

3.8. 在确定假想始发事件清单时，应考虑安全重要物项的故障或误动作可能直接导致假想始发事件或使假想始发事件的后果更严重的可能性。

3.9. 应明确在不同的电厂状态下，包括所有的正常运行模式，用以实现 SSR-2/1（Rev.1）[1]要求 4 所定义的基本安全功能的所有电力系统功能和设计规定。

3.10. 电力系统功能应能根据其安全重要性分类，主要考虑如下 3 个因素：

(a) 所执行功能故障的后果；
(b) 需要执行这个功能的假想始发事件的发生频率；
(c) 在发生假想始发事件后，需要该功能投入运行的时间或持续时间。

3.11. 应识别执行每种安全功能的电力系统和部件并对其分级，它们应主要根据分配给其执行的功能的类别进行分级。

3.12. 场外电力系统和主发电机系统在确保基本安全功能的性能方面也发挥着重要作用，但这些系统无需根据电厂的安全分级进行分级。

3.13. 在分配安全分级时，应考虑采取替代措施的及时性和可靠性，以及检测和补救电力系统中任何故障的及时性和可信度。

3.14. 根据各国经验，SSG-30[4]推荐将安全功能分为三类，将结构、系统和部件分为三个安全级。但也可以采用更多或更少的安全功能分类和安全级。

4. 电力系统设计基准

4.1. SSR-2/1（Rev.1）[1]要求 14 和第 5.3 段指出：

> “安全重要物项的设计基准应规定相关运行状态、事故工况以及内部和外部危害导致的工况所需的能力、可靠性和功能性，以满足核电厂寿期内的特定验收标准。
>
> “5.3. 必须系统地证明每个安全重要物项设计基准的正当性并将设计基准形成文件。文件应为营运组织安全运行电厂提供必要的信息。”

4.2. SSR-2/1（Rev.1）[1]要求 15－19 详细规定了制定系统设计基准时需要考虑的特殊问题。

4.3. 核电厂的所有电力系统均应明确其设计基准。

4.4. 设计基准应规定所需的功能任务、必要的特性、性能目标、运行工况和环境条件以及必要的可靠性。

4.5. 对核电厂的每一个电力系统，其带负荷连续运行时的电压和频率的变化范围应予以明确。

4.6. 电力系统带负荷连续运行时，暂态、准稳态电压和频率的允许变化范围应予以明确。

4.7. 电力系统应考虑的暂态包括内部事件和外部事件（包括第 4.10(d)(ii)段描述的电网故障）。

4.8. 设计基准应考虑所有的运行模式和各种可能会影响核电厂电力系统的事件，包括：

(a) 对称和非对称故障；
(b) 次同步谐振；
(c) 大型电动机启动；

(d) 电网的瞬时扰动，如操作冲击或雷电冲击；

(e) 电容器组的投切；

(f) 输电系统某一部分丧失，包括单相断相工况；

(g) 孤网运行及导致的频率和电压偏移。

4.9. 当（场内或场外）电力系统和负载发生变化或有更新时，或当开展定期安全评审时，应重新确认电力系统的设计基准。

4.10. 设计基准应描述核电厂电力系统的每个子系统：

(a) 电力系统应满足核电厂如下运行状态：

(i) 机组带最大厂用电负荷启动并达到最大允许运行功率；从满功率运行到停堆；发生设计基准事故或反应堆跳堆后安全停堆。

(b) 系统连续运行时电压和频率的变化范围：

(i) 该范围对电动机、泵、逆变器、蓄电池充电器和阀门执行机构等用电设备提出了运行要求。

(c) 容量要求：

(i) 电力设备的容量选择通常由事故分析决定，包括例如部件的同时启动或再加速；

(d) 系统在执行以下功能时，可能会经受稳态、短时运行和暂态工况：

(i) 稳态工况和条件包括：

— 重载和轻载工况下、所有电厂状态下以及厂用电运行（如适用）的电压范围和频率偏移；

— 电网电压和频率偏移；

— 直流系统浮充电压和充电电压。

(ii) 暂态工况包括：

— 运行过电压；

— 雷电过电压；

— 场内（外）电力故障引起的电压波动；

— 甩负荷、电动机启动和场内电力系统或外电网故障切除引起的电压波动；

— 电网（和主发电机）故障时出现的电压、频率的偏移和暂态；

— 运行冲击或旋转设备引起的谐波；
— 主保护或后备保护切除输电系统或场内电力系统（含各个电压等级）故障；
— 导致电厂和电网失步的事件；
— 单相故障或断相；
— 主发电机励磁系统（过励磁或欠励磁）故障；
— 断线；
— 太阳活动或地磁感应电流。

(e) 需监控主总线的参数，包括系统电压、电流和频率：
(i) 包括事故中和事故后需监控的参数。

(f) 触发备用电源投入的工况：
(i) 包括用于启动备用电源所需的参数。

(g) 电力部件和电缆所处的环境和电磁工况：
(i) 环境条件包括：
— 正常工况；
— 异常工况；
— 事故工况；
— 自然现象引发的衍生工况。

(h) 确定所有负载的安全分级和电力特性；
(i) 包括电动机惰转时的输入功率。

(i) 所有部件所需的性能特征。

(j) 维护和试验要求：
(i) 包括试验验收标准；

(k) 保护方案和保护配合：
(i) 保护方案需考虑对称和非对称故障，详见附件Ⅱ。

(l) 设计验收标准：
(i) 设计验收标准包括：
— 使用的标准；
— 设计特殊要求，如独立性、单一故障标准和多样性要求。

(m) 系统和关键部件的可靠性和可用性目标：

(i) 如，备用电源的可靠性：

— 通过概率、确定性或二者结合的方法来确定系统和部件的可靠性和不可用性限制。

(n) 适用于备用电源及其原动机的电压、速度、启动和加载时间以及其他限值。

(o) 备用电源启动和接受指定加载序列中负载的最长时间：

(i) 事故工况运行的设备一般会给定允许的启动时间。

(p) 备用电源所需的性能特征，包括空载、轻载、额定负载和启动负载的能力，以及在某些状态下所需时间段内的过载运行能力。

(q) 在整个负载范围内逐步加载备用电源的能力：

(i) 逐步带载能力规定了备用电源需维持的电压和频率，即使在投入和切除最大单台负载期间引起偏移时，电压和频率也不会低于最低限值。

(r) 允许关闭或断开安全级电源的情况：

(i) 包括保护设备免受严重故障损坏的需要。

(s) 场内电源必须能够独立于场外电源运行且没有从场外补充消耗的最短时间：

(i) 须考虑确定蓄电池的容量、应急柴油机燃油和润滑油的贮存量、需要贮存的其他耗材量（如空气过滤器）。

(t) 需监控的某些参数或参数组合。

(u) 所需的控制功能，以及明确自动、手动或两者兼有的动作，以及控制地点。

5. 电力系统总体设计

概述

5.1. 安全重要电力系统应充分满足其设计基准的要求。

预计电力事件

5.2. 核电厂电力系统应满足设计基准定义的稳态、短期和暂态运行工况的所有功能要求。

5.3. 引起场内电力系统对称或不对称扰动的始发事件如下：

(a) 输电系统中的电厂并网、解列或关闭，或由于预计故障或电压和频率变化超限导致发电厂与电网断开；

(b) 主发电机跳闸引起的场内电力系统连接至场外或其他场内电力系统；

(c) 场内电力系统中电动机启动、单相接地故障或开关操作冲击。

5.4. 应评价此类事件对所有场内电力系统（交流和直流）（见图 4）的影响，并应通过特定分析确认满足允许电压和频率的要求，同时应确认保护系统也满足要求。

5.5. 应通过电网暂态健稳性分析证明电厂能耐受这些扰动并保持与电网的连接，而不会导致发电机丧失和电网的同步（见图 5）。

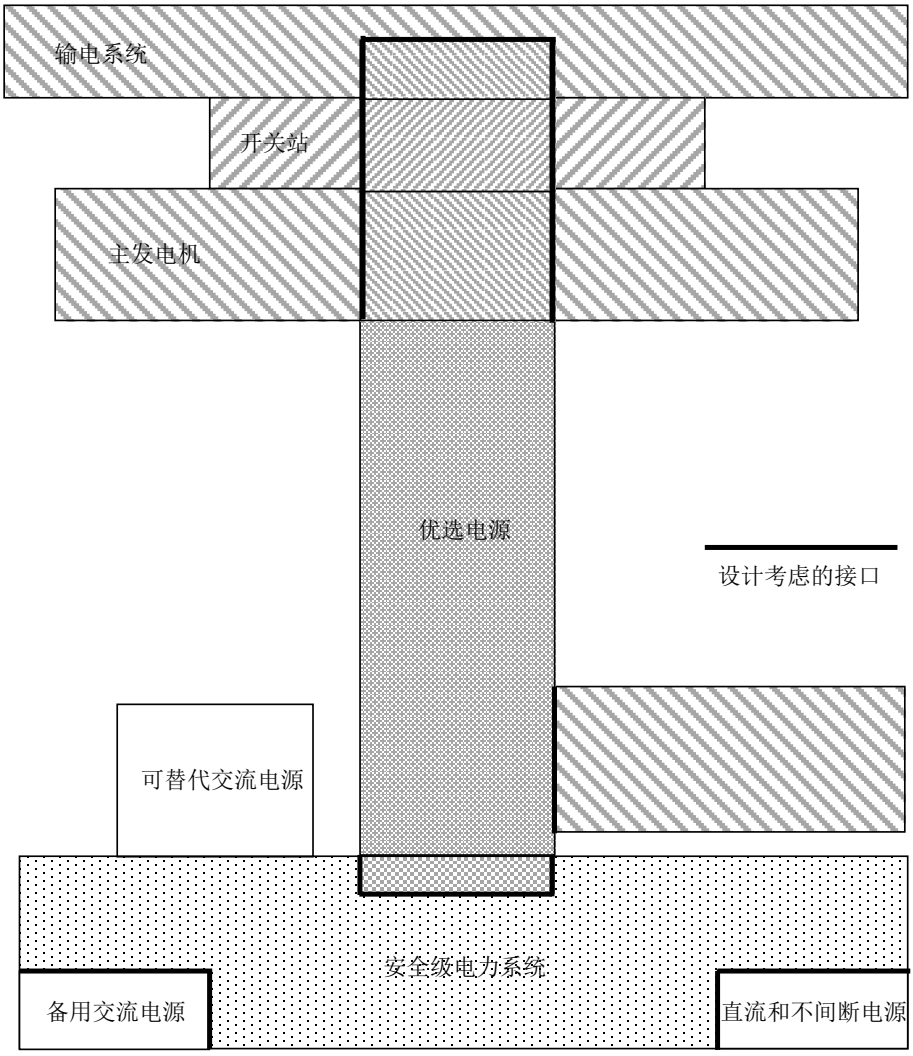
5.6. 电力故障清除时间应由电网营运商确定。

5.7. 预计的纵深防御能力保障了优选电源的可靠运行。

全厂断电

5.8. 国际运行经验表明，在汽轮机跳闸和所有备用交流电源不可用的情况下，优选电源的丧失是可信的。这样的事件可能会影响单台机组，甚至影响同一场址上的所有机组。这种事件被称为全厂断电，其发生频率应足够低，可以作为设计扩展工况事件进行考虑和分析。该术语不包括不间断交流电力系统或直流电源的同时故障，也不包括设计不同且不易受导致场内和场外电源丧失事件影响备用交流电源的故障。

5.9. 应在电厂处于全厂断电状态期间分析电厂维持安全功能和排出乏燃料衰变热的能力。设计中应采取足够的措施，以防止电厂处于全场断电状态期间的任何显著燃料破损。



注：UPS — 不间断电源。

图 4. 优选电源与电力系统其他组成部分之间的关系。

5.10. 提高电力系统应对全厂断电能力的措施包括：增加为安全级仪器仪表、控制设备以及其他重要设备供电的蓄电池容量；运用机组间的互相连接；配置多样化的备用交流电源来应对正常电源和备用电源故障。

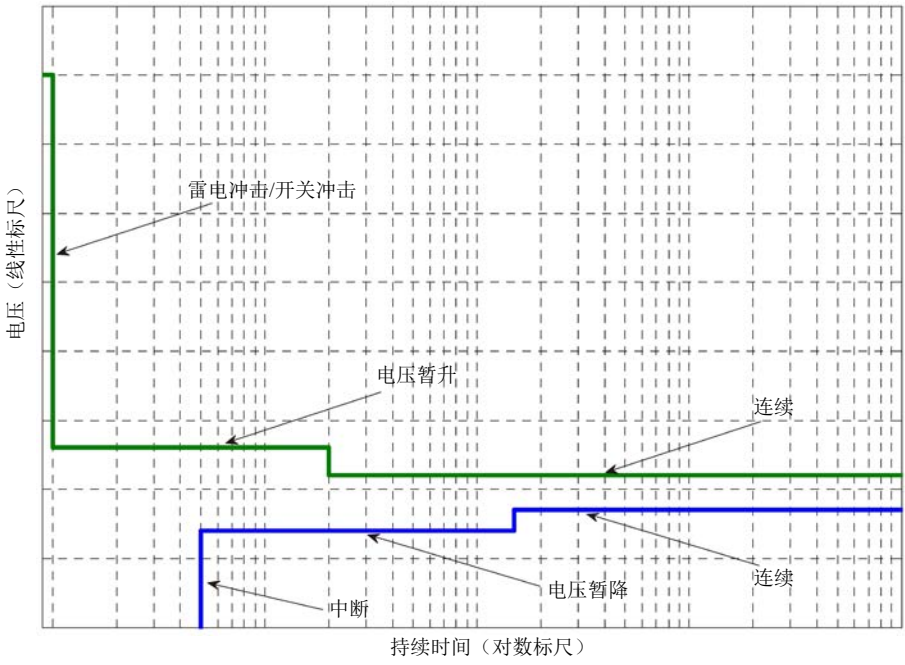


图 5. 电压暂升与暂降（注：始发条件可为规定电压范围内的任意数值）。

可靠性设计

概述

5.11. 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匹配。”

5.12. 在设计安全重要电力系统时，通常采用诸如冗余性、多样性、随机故障耐受能力、设备和系统独立性、共因故障耐受能力，可试验性和可维护性、故障安全设计以及高质量设备的选择等设计特性来保证指定的安全功能可靠性。

冗余性

5.13. 安全重要电力系统应冗余配置以满足设计基准可靠性的要求。

5.14. 为达到可靠性目标或符合单一故障标准[3]，安全重要电力系统通常冗余配置为了充分发挥冗余作用，独立性也是必要的。冗余会提高安全功能执行的可靠性，但同时也增加了误操作的可能性。

5.15. 运行经验表明，同列系统内的冗余配置可提供运行的灵活性并提高可用性。

独立性

5.16. 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。”

5.17. SSR-2/1（Rev.1）[1]要求 21 规定：

> “必须酌情通过实体分隔、电力隔离、功能独立和通信（数据传输）独立等手段防止安全级系统之间或系统冗余单元之间的互相干扰。”

5.18. SSR-2/1（Rev.1）[1]第 5.35 段指出：

> “设计必须做到确保防止安全重要物项之间的任何互相干扰，特别是确保较低安全级系统中的安全重要物项的任何故障都不会蔓延到较高安全级的系统。”

5.19. 独立性是为了防止故障或内外部危害影响安全级电力系统的冗余部件，以及防止故障或内外部危害影响提供纵深防御水平的系统。需要考虑的故障过程包括：

— 设计基准事件造成的故障；

---

[3] 单一故障是指导致系统或部件丧失执行其预计安全功能的能力以及由此产生的任何后果性故障。单一故障标准是应用于系统的标准（或要求），即系统必须能够在出现任何单一故障时执行其任务（见第 7.25 段）。

— 受相同的内外部危害影响；
— 公共支持系统的故障；
— 系统或分列之间的电力连接；
— 系统或分列之间的数据交换；
— 设计、制造、运行、维护中的共性错误。

5.20. 安全级物项不应受到它们需要应对事故的影响。

5.21. 必要时，安全级系统应独立于较低安全级的系统，以确保安全级系统能够在需要执行这些功能的任何事件期间和之后执行其安全功能。

5.22. 安全组的冗余部分应相互独立，以确保安全组能够在需要执行这些功能的任何事件期间和之后执行其安全功能。

5.23. 电力结构、系统及部件的局部故障不应造成剩余部分不可用。

5.24. 安全级系统支持功能的故障不应破坏安全级系统冗余部件之间或安全级系统与安全级较低的系统之间的独立性。例如，将房间通风划分为与其支持的安全级系统相同的列，可防止一列安全级电力系统的机械功能丧失，导致另一列同时丧失安全功能。

5.25. 应将安全重要性不同的系统之间的隔离设备应看作更重要性更高系统的一部分。

5.26. 应证明为满足独立性要求而提出的设计特性的正当性。

实体分隔

5.27. 实体分隔：

(a) 可防止因内部危害造成的共因故障。涉及的内部危害包括：
— 直接和间接水淹，例如水通过屋顶、墙壁、沟道或管道发生喷射和渗漏；
— 火灾；
— 飞射物；
— 蒸汽喷射；
— 管道甩动；

— 化学爆炸；
— 水淹；
— 相邻设备的故障。

(b) 可防止由于正常、异常或事故工况、设计基准事故、内部和外部危害导致的共因故障。采用环境、地震以及电磁鉴定，或结合实体分隔，可用来防止事故和内外部危害的影响；

(c) 可减少如小型飞机坠毁等局部事件造成共因故障的可能性；

(d) 可减少冗余设备运行或维护期间人为失误的可能性。

5.28. 实体分隔是通过屏障、距离或两者的组合来实现的。

5.29. 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》[5]，以及原子能机构《安全标准丛书》第 NS-G-1.11 号《核电厂设计中除火灾和爆炸外的内部危害防护》[6]，提供了防止火灾和其他内部危害的指导。

5.30. 由于设备或布线的交叉汇集造成实体分隔困难的区域包括：

— 安全壳贯穿件；
— 电动机控制中心；
— 开关设备区域；
— 电缆室；
— 设备间；
— 主控室和其他控制室；
— 电厂程控计算机。

电力隔离

5.31. 电力隔离用于防止一个系统中的电力故障影响与其连接的其他系统。电力隔离可控制或防止由于电磁干扰、静电感应、短路、开路、接地或交流、直流过电压等因素导致的设备和部件之间产生不利的相互作用。

5.32. 一般情况下，安全级电力系统不应向非安全级负荷供电。

5.33. 由安全级电力系统供电的非安全级负荷应使用安全级隔离设备进行隔离。

5.34. 安全级断路器可作为优先选用的隔离设备，该断路器通过在与隔离设备相同的安全分区内产生的事故或失压信号启动自动跳闸。

5.35. 不应互相连接安全级电力系统的冗余列。

5.36. 如果安全评定确认电源的可靠性显著提高，并且确保了冗余分区的足够独立性，则可以在运行期间在冗余分区之间进行临时连接。

5.37. 如果安全评定确认以下内容，则可在停堆期间进行冗余分区之间的临时连接：

(a) 具有不能通过简单的开关操作解除交叉互联闭锁的措施；
(b) 临时连接对电厂安全功能可靠性的影响和对诱发共因故障的影响是可接受的。

5.38. 这些交叉互联可用于应对全厂断电。

5.39. 电力隔离措施包括断路器、继电器、电子隔离器件、光隔离设备（包括光纤）、电缆或屏蔽层、隔离间距、内部机械构件或以上的组合。

5.40. 防止电磁干扰和静电感应的电磁兼容性认证可作为电力隔离措施的补充。

相关电路

5.41. 如果在安全级电路和安全级较低的电路之间提供足够的电力故障分隔和隔离是不切实际的，则安全级较低的相关电路应该：

(a) 通过分析或试验证明不会对与之相关的安全级电路造成不可接受的影响；
(b) 确定为与其相关联的安全组的一部分；
(c) 采取与其相关联的安全组电路相同的电力分隔方式。

多样性

5.42. 安全级电力系统应配置多样化的电源。

5.43. 电源的多样性通常是电力系统接线设计应具备的重要特性。

5.44. 通常情况下，安全级电力系统的电源来自：

(a) 通过优选电源供电的场外电力系统；
(b) 作为正常电源或带厂用电负荷运行的主发电机；
(c) 在丧失场外电源时为安全级电力系统供电的备用电源；
(d) 全厂断电时的备用交流电源。

5.45. 直流负荷可由蓄电池或上述交流电源通过整流器供电。

5.46. 不间断交流电力系统的电源来自蓄电池、蓄电池充电器（通过逆变器）或使用旁路开关的安全级系统交流总线。

5.47. 电力设备软件多样性设计应遵循安全导则 SSG-39[2]。

5.48. 针对特定负载的电源多样性通常会提高整个系统的可用性，如仪器仪表和控制系统。

5.49. 如果将非电力动力系统作为多样化手段来完成特定安全功能，则其相关的电源、仪器仪表和控制系统应独立于其他系统。

5.50. 非电力动力系统（如蒸汽或发动机驱动的泵）提供了除电力系统以外的多样化方案，本“安全导则”相关多样性的建议适用于多种形式的非电力动力系统。

5.51. 除了实体分隔和电力隔离之外，多样化配置的动力源或不间断电源可提高冗余系统或不同纵深防御层次系统之间的独立性。

共因故障

5.52. 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。”

5.53. 在安全级电力系统及其支持系统的设计、维护、试验和运行中，应考虑导致安全级电力系统无法在其需要时执行安全功能共因故障的可能性。

5.54. 应采用多样性和独立性原则（实体分隔和功能隔离）来防止源于安全级系统设备自身所可能产生的共因故障，或源于相连系统或人为操作和维护引起的开关冲击、电压和频率偏移的可信共因故障。

5.55. 采用独立性和多样性设计有助于在最大程度上避免 — 但不能完全保证 — 共因故障成为系统不可用的主要原因。

5.56. 由于核电厂通常只接入一个输电系统，因此电网事故可能同时影响安全级电力系统的冗余部分。如果核电厂有两台汽轮机和两台发电机，则发生共因故障的可能性将降低。如果冗余的安全级电力系统分别单独接入电网，则发生共因故障的可能性也会降低。

5.57. 场内和场外电源的电压暂态事件及相关运行经验表明，需更加关注电力系统的设计，以便将其发生共因故障的风险降至最低。应采用降低系统暂态影响的设计措施来实现预期“不间断运行”的要求（见图 5）。

5.58. 由于发电设施可能出现电压偏移、频率偏移和相位偏移，当查找源于优选电源的共因故障的薄弱环节时，来自工业应用领域运行经验的参考价值是有限的。

5.59. 针对源自电网共因故障的主要保护措施包括：

(a) 建立全面的设计基准和安全导则，以确定可能对安全级电力系统构成威胁的所有可能事件；
(b) 通过内置功能或继电保护，核实安全级电力系统应对这些事件的能力；
(c) 核实电网的电压/频率偏移不会传递至由整流器和逆变器供电的总线。

5.60. 当某事件导致场外电源丧失后，如果安全级电力系统不由主发电机供电，则备用电源将启动并将为安全级电力系统供电。即使安全级电力系统分为不同的列，由于所有列具有相同的启动特性，因此备用电源的加载启动仍然有发生共因故障可能性。

5.61. 备用电源共因故障的主要保护功能包括：

(a) 建立全面的设计基准和安全导则，以确定所有可能对备用电源的控制、启动和运行所构成威胁的事件；

(b) 通过内置功能或继电保护，核实备用电源具备应对这些事件的能力（包括备用电源加载期间的暂态性能）；

(c) 控制电路和设备的适当冗余可保证启动的可靠性和运行的连续性，并避免误跳闸。

5.62. 为了最大限度地降低基于软件设备共因故障的风险，应使用 SSG-39 [2]建议的仪器仪表和控制设备的适当设计功能。

故障模式

5.63. 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。”

5.64. 应了解安全重要电力部件的故障模式，并应记录在文件中。

5.65. 为建立故障安全的概念，必须了解部件的故障模式。

5.66. 安全重要电力部件的故障应通过定期试验进行检测，或通过警报或异常指示进行提示。

5.67. 设计应确保故障是自动显示的，除非这种设计可能导致不安全状态或可能导致安全系统的误动作。

保护配合

5.68. 电力保护方案应防止故障使安全功能故障，并达到可接受的水平。

5.69. 每个负载组的保护动作应独立于冗余负载组提供的保护动作。

5.70. 当出现异常工况导致运行设备可能退化或发生故障时，应使用保护继电器迅速将电力系统的相应部件从服务中移除。

5.71. 为尽量减小故障的影响范围，断路器应选择性跳闸。

5.72. 保护方案应该具备以下功能：

(a) 在检测到不可接受的状态时，保护应动作于必要的设备，以减轻电力系统扰动的严重程度和影响范围、设备损坏以及对人员和财产的潜在危害。

(b) 应监控所连接的优选电源，并能自动或手动切换至替代电源。在这种情况下，替代电源可以是其他的场外电源或场内备用交流电源。采用先进的快速切换技术和充分的闭锁方案可减少对运行设备的冲击。

(c) 提供保护运行的指示和标识。

(d) 监控保护系统控制电源的可用性。

(e) 确保只切除电力系统中的故障设备。

5.73. 通常，仅切除故障设备的保护方案通常具备如下特征：

(a) 在所有设计的电力系统运行方式下，当发生短路和过载时，保护设备的动作应具备选择性。

(b) 保护设备应动作于断路器并快速切断故障电流，以避免对系统内的设备造成危害并最大限度地减少扰动。

(c) 电厂的开关设备应具有可靠的弧光保护或其他适当的保护措施，以尽量减少潜在的燃弧故障对开关设备造成的损坏，确保电厂安全和运行和维护人员人身安全。

(d) 列出并设计了在试验期间为保护部件而安装的单一保护设备，使其运行不会危及系统在实际事件中的运行能力。

5.74. 保护方案应考虑电压跌落、中断及总线切换后的冲击电流。

5.75. 保护设备的设计应考虑系统的对称和不对称故障。

5.76. 需考虑所有可能的短路和断线故障类型，包括诸如不接地系统中的断相和接地故障等，保护配合还应考虑测量方式的影响。

5.77. 为支持对保护配合的分析和核实，需要具备捕捉事件暂态的方法。

5.78. 数字型保护设备应按其执行的安全功能进行核实。

5.79. 核电厂电力系统和部件保护设备的设计还应符合适用于电力设备和电力装置安全的国家标准及其他相关规定。

可靠性确认

5.80. 应对所有安全重要系统进行系统化评定，以确认设计基准中可靠性的要求已在系统设计中落实。

5.81. 由于软件和复杂多部件逻辑模块的应用，使得确认在共因故障模式下系统设备的可靠性和灵敏性变得困难。因此，可靠性的确认依赖于在设计和实施过程中不发生错误。关于此问题的建议和指导见 SSG-39[2]。

5.82. 在确定系统的可用性时，试验设备应作为安全级系统的一部分来考虑。

额定值

5.83. 电厂电力系统中使用的所有设备的运行参数与其标称额定值相比应具有足够的裕度。

5.84. 应在保守假设和可信方法的基础上进行分析和模拟，以确认设计裕度。

5.85. 应定期确认设备额定值裕度的充分性，至少应与主要部件的更换、电厂改造和定期安全评审一起确认。

5.86. 电力设备应具有足够的设计裕度，以确保在不超过设备额定值的情况下，可以实施未来的电厂升级和改造。

电动机

概述

5.87. 根据电力系统设计基准的规定，用于安全重要物项的电机应设计出足够高的输出转矩，以允许在最小允许设计电压下启动。

5.88. 由电力系统供电的，用于安全重要物项的电动机和其他设备应能够承受设计基准定义的稳态、短时和暂态运行工况所导致的过电压、欠电压和高频、低频状态。

5.89. 电动机的额定功率、安全级电力部件的容量和过载保护设备的整定值应与电动机实际负载以及输出转矩相匹配。

5.90. 阀门的驱动设备应在低压和低频时能提供足够的扭矩来打开或关闭阀门，且在高电压和高频率时不超过最大允许转矩。

5.91. 电机驱动机构的保护设备与力矩开关的定值之间应互相配合，以避免在运行过程中误跳闸。

过载保护设计

5.92. 电力设备和电缆应可在不超过其额定耐受值的情况下过载运行。

5.93. 在某些情况下，设备可能需要短时间过载运行。通常情况下，大型水泵在启动时可能会导致短时过载运行。例如，电路保护设备的整定值可以高于设备免受损坏的持续过载值。

5.94. 应依据电缆的持续载流量来配置其过载保护。

5.95. 当设备过载运行时，不应对其他回路或相关设备产生不利的影响。

5.96. 安全系统设备在过载工况下的持续运行及其造成的损坏风险不应被视为在事故工况下运行的安全正当性。

5.97. 高于额定值的持续过载应在主控室中预警。

5.98. 正常运行工况下，如果保护设备的整定值较高，将无法检测到系统中的过载，这种情况下可能会导致设备加速故障。

电力设备、电缆及通道

概述

5.99. 此处论述的电力设备包括开关设备、电动机控制中心、变压器和电缆。

5.100. 电力设备的选择和鉴定应符合其使用条件和环境条件。

5.101. 电力设备应具有足够的阻燃性以防止火灾蔓延。

5.102. 消防安全方面的考虑见 NS-G-1.7[5]。

额定值和选型

5.103. 电力设备的额定电压应大于系统标称电压（通常为系统额定电压的110%），脉冲额定值应大于设备可能承受的任何暂态电压。

5.104. 电力设备应按如下条件选型：

(a) 在允许的系统电压波动范围内，可承载主回路和分支回路的电流；
(b) 满足负载运行要求而不超过温度限值；
(c) 可承受系统短路电流（例如在规定切除时间内的故障电流）；
(d) 可承受短路峰值电流而不超过其机械强度。

5.105. 在计算导体温度时，需考虑的因素包括：

(a) 最高环境温度；
(b) 正常电流和故障电流；
(c) 负载率；
(d) 在同一或附近通道中其他电缆的布置情况；
(e) 电缆桥架、穿墙、穿楼板、消防堵料和阻燃涂层对电缆发热的影响。

安装

5.106. 总线、电缆管道（即电缆桥架或电缆保护管）及其支架的设计应能够承受电缆及其附件的机械负载，并留适当的裕度。

5.107. 为避免因假想始发事件造成的损害，安全级系统的总线、隔室和电缆应得到充分的保护。

5.108. 可能影响总线、隔室和电缆的危害包括：火灾、流系统统、机械或结构部件的故障或失灵。

5.109. 一般情况下，为使因火灾、旋转机械设备故障或支撑系统故障等外部事件损坏的电缆不超过安全分析报告中论证过的可接受的最小范围（通常是任一安全组的一列），应对安全级系统电缆的敷设和防护采取适当设计。机械设备故障包括管道甩动、喷射冲击、旋转设备或其他高能系统故障产生的飞射物及其可能造成的后果。防止机械设备故障的建议和指导见NS-G-1.7[5]。

5.110. 电缆和通道应采用永久标牌来标识列别。

5.111. 工程中通常的实践是在通道和电缆的两端和固定间隔处做永久的标识（封闭通道内的电缆除外），通道的标识通常还包括电缆电压等级。

5.112. 每根电缆应有适当的标识以确保其敷设在正确的通道中。

5.113. 一般情况下禁止在桥架内使用电缆接头。

5.114. 经鉴定合格的电缆接头可以用于现场电缆和设备之间的连接。安全壳内的安全级电缆和设备应采用鉴定合格的端接技术，以防止在事故工况下产生过大的泄漏电流。

电缆隔离

5.115. 应采用适当的方法（如距离或物理屏障）对以下对象进行实体分隔：

(a) 安全级与非安全级电缆；
(b) 属于不同安全组的电缆；
(c) 不同电压等级的电缆。

5.116. 按安全级进行分离是为了避免由于系统故障或未进行安全分级的电缆而对安全级电缆造成损坏。不同安全组电缆之间的隔离旨在防止单一危害影响安全级系统中的多个冗余物项。按电压等级进行分离旨在防止高能量电路中预期的电磁干扰对低能量电路不可接受地影响。

5.117. 以下电压等级的电缆之间应进行实体分隔：

(a) 仪器仪表和控制电缆；
(b) 低压电力电缆（1 千伏及以下）；
(c) 中压电力电缆（大于 1 千伏至 35 千伏）；
(d) 高压电力电缆（大于 35 千伏）。

5.118. 高压电力电缆通常不用于核电厂场内电力系统。

5.119. 应将相同电压等级的电缆放置于同一通道中（如梯架、托盘或保护管）。

5.120. 不同电压等级的电缆和电缆管道应根据等级进行分隔，可以通过空间分隔，也可以通过防止一个等级对另一个等级产生有害影响的屏障进行分隔。

5.121. 有效接地的金属保护管可作为隔离屏障。

接地

概述

5.122. 接地用于确保电力系统、仪器仪表和控制系统的电力安全和功能。国家和国际标准中提供了详细的接地设计导则。

5.123. 在任何发电厂中，通常有四个概念上可识别但不一定物理上不同的接地系统：安全（保护）接地、防雷接地、电力与仪器仪表和控制系统接地，以及信号接地。

5.124. 所有接地系统应连接到一个接地网。

5.125. 接地电阻值会影响：

(a) 设备的故障电流耐受能力；
(b) 电力安全（即假定接地放电或故障电流允许的跨步电压和接触电压）。

5.126. 国际技术标准描述了许多仪表和控制系统接地的解决方案。通常，发电厂使用两种方法中的一种来接地仪器仪表和控制系统：单点接地或多点接地。特定方案在工程设计中确定。

5.127. 应正当使用接地方法，并与电磁兼容的总体设计要求相协调。

电力安全

5.128. 为保护人员、设备和厂房免受损害，应有效地设计、安装和维护全厂接地网络。

5.129. 除非会妨碍设备的功能，否则所有设备和装置的金属框架均应接地。

5.130. 如果设备和装置的金属框架不接地，则应采取额外的措施来确保安全。

5.131. 电力系统的接地设计应进行整体考虑，因为即使是系统中一部分接地不恰当，也可能影响整个系统。

系统接地方式

5.132. 中压交流电力系统应优先考虑采用高阻抗接地方式。

5.133. 高阻抗接地可以限制故障电流，并且允许受影响的设备持续运行。

5.134. 当可证明正当时，也可选用其他系统接地方式，例如直接接地或不接地。

5.135. 若采用高阻抗接地方式，应对电力系统的接地故障进行监控，且监控系统应易于识别故障地点。

5.136. 对地低阻抗的检测应仅发出警报，并且仍应允许设备执行其功能。

5.137. 保护方案应可切除多种类型的故障。

防雷及电涌保护

5.138. 应采取有效措施防止雷击影响电力和仪器仪表和控制系统执行其安全功能。

5.139. 系统的防雷可采用外部或内部防护措施。通常，有必要采用内外部防护措施相结合的方式。

5.140. 外部防护措施通常采用接闪器或由厂房金属部分构成的法拉第笼，以保护厂房及其设备免受雷击影响。为创造一个免受电磁危害的环境，内部防护措施包括房间内采用特定的电磁防护设备。

5.141. 为防止雷电流引起的感应过电压和传递过电压的危害，内部雷击防护通常采用屏蔽和避雷器。传递过电压由外部防雷保护系统及其接地线与地电位间的电势差所引起。

5.142. 为防止雷击感应电压影响安全级电力系统，不应将安全级的电缆通道和电缆靠近厂房外墙布置。

5.143. 外部防雷装置应就近接地，并使雷电电流在厂房外入地。

5.144. 内部接地保护设备应与防雷接地系统连接，同时应避免人员和设备遭受传递过电压的伤害。

5.145. 防雷保护系统与大地之间连接线的敷设应使雷电放电效应既不危及安全级电力系统的安全功能，也不危及防雷保护接地系统本身的功能。

5.146. 电厂的接地还可以辅以其他特定的接地体。

5.147. 维护和支持人员用的仓库、办公室和车间等临时设施一般不应从电厂用电力系统进行供电。

5.148. 当厂用总线给辅助厂房供电时，应采取适当的措施以确保辅助厂房内电力设备所产生的电力干扰和电压扰动不会对厂用电系统产生不利影响。

5.149. 控制和监控系统不应由电厂外部线路直接供电，以降低由于感应或其他影响产生的干扰风险。

5.150. 如果电缆线路具备对雷电引起的感应电压和接地电位上升的有效防护，那么可将其与具备类似有效防护措施（如采用接地的钢结构墙体）的厂房连接。

5.151. 为防止过电压超过设备或其绝缘的允许电压限值，应在系统中正确配置浪涌保护器或避雷器。

5.152. 过电压浪涌可能由雷击、电力故障或开关现象引起，在不同电压等级下可能需要抑制器。

5.153. 开关操作、整流器、逆变器和旋转设备都可能产生谐波和干扰，这可能对电力设备的正常运行带来危害。在电力系统中，为了确保对电力干扰敏感设备的可靠运行，有必要装设额外的设备来过滤和抑制电力干扰。

设备鉴定

概述

5.154. SSR-2/1（Rev.1）[1]要求 30 规定：

> “必须实施安全重要物项鉴定计划，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。”

5.155. 对于安全重要的电力系统及部件，应鉴定在其使用寿期内的设计功能。

5.156. 鉴定应确保设备或部件具有与其安全分级相对应的可信度。

5.157. 鉴定计划应考虑影响系统或部件预计安全功能适用性的所有方面，包括：

(a) 功能及性能的适用性和正确性；
(b) 部件的环境鉴定；
(c) 部件的抗震鉴定；
(d) 电磁场相关的鉴定。

5.158. 鉴定活动应基于某一适当的方法组合，比如：

(a) 使用符合现行有效标准的工程和制造流程；
(b) 可靠性论证；
(c) 类似应用的运行经验；
(d) 型式试验；
(e) 已供货设备的试验；
(f) 根据已有试验结果或相应工况下获得的运行经验来外推。

5.159. 鉴定方法的组合应根据被鉴定的特定系统或部件而定，通常不需要采用上述所有的鉴定方法。例如，对已存在物项的鉴定，可更加关注其运行经验和分析，并作为工程和制造的记录和核实完整性的有效补充。

5.160. 用于设备鉴定的方法或方法组合应正当并有形成文件。

5.161. 当采用运行经验作为支持设备鉴定时，则应证明运行经验与拟议用途和目标应用的环境条件相关。

5.162. 作为设备鉴定支撑性文件的分析报告，应论证其方法、理论和假定条件的正当性。

5.163. 例如，用于设备鉴定的数学模式的有效性可根据实验数据、试验数据或运行经验予以证明。

5.164. 应保证每个已安装的安全重要系统和部件及其鉴定相关的依据可被追溯。

5.165. 不仅部件本身可追溯，部件在通过鉴定时的构造和实际安装的构造之间的差别和变化也应可追溯。

适用性和正确性

5.166. 设备鉴定计划应证明电力结构、系统、部件以及软件的设计满足所有要求，包括在相关设计基准和设备技术规范书中要求的安全重要的性能、容量和可靠性。

5.167. 例如，设备可靠性包括故障安全的运行方式、单一故障标准、独立性、故障监控、可维护性和运行寿期的要求。

5.168. 设备鉴定程序应证明已竣工的电力系统和已安装的部件可正确执行设计功能。

环境鉴定

5.169. 在本“安全导则”中，“环境鉴定”是指因温度、压力、湿度、化学制剂接触、辐照、气象条件、水淹、机械老化等可能影响部件正常功能而进行的鉴定。

5.170. 在电厂各种状态下，安全重要的结构、系统和部件的设计应能适应相应运行的所有电厂状态相关环境的影响，并应与之兼容。

5.171. 当受到设计基准规定的环境条件范围影响时，安全重要部件应符合设计基准的所有要求。

5.172. 有时即使不要求某一部件所有功能完全可用，但仍需要其能执行安全功能。比如，在特定模式下对于维持机械完整性而不允许故障的部件。

和缓环境条件下的部件

5.173. 如果对于安全重要电力系统的部件在事故运行中的环境条件不比正常运行的环境条件更严苛（即和缓环境条件），则可以基于供应商的鉴定文件证明该部件是适应规定的运行工况的。

恶劣环境条件下的部件

5.174. 如果对于安全重要电力系统的部件在事故运行中的环境鉴定比正常运行的环境条件更严苛（即恶劣环境条件），则应证明该部件在鉴定寿命末期仍能执行规定运行工况范围内的安全功能。

5.175. 为证实部件在其鉴定寿命末期仍能执行预期功能，设备鉴定需表明部件在考虑重要老化效应后（例如辐照老化和温度老化），在其鉴定寿命末期仍能执行预期功能。老化鉴定一般更加保守，以应对无法预计到的老化机理。

5.176. 在制定设备鉴定计划时，应考虑可信的最恶劣环境条件组合，包括与运行工况之间的叠加效应。

5.177. 如果需要将被鉴定的物项在不同环境条件下分别试验（例如分别进行辐照和温度效应试验），应证明试验实施的顺序恰当地模拟了被鉴定物项在组合环境条件下的退化。

5.178. 最严格的环境鉴定方法可以仅用于安全级部件。

5.179. 预期在恶劣环境条件下运行的安全级部件的环境鉴定应包括型式试验。

5.180. 当提供防护屏障将设备与潜在环境影响隔离时，屏障本身应接受鉴定程序，以验证其有效性。

内外部危害

5.181. 电厂设计基准和安全分析将识别电厂运行所需承受或安全承受的内部和外部危险，如火灾、水淹和地震事件，以及需要保护或系统鉴定的危害。

5.182. 根据 NS-G-1.7[5]建议，应保护电力系统和部件免受火灾和爆炸的影响。

5.183. 根据 NS-G-1.11[6]建议，应保护电力系统和部件免受其他内部危害的影响。

5.184. 根据原子能机构《安全标准丛书》第 NS-G-1.6 号《核电厂的抗震设计与鉴定》[7]建议，电力系统和部件应能承受地震危害，并通过抗震鉴定。

5.185. 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》[8]建议，应保护电力系统和部件免受其他外部危害，或将其设计成能承受其他外部危害并通过鉴定。

电磁鉴定

5.186. 电力、电子系统和部件的抗干扰运行能力取决于部件在其运行环境中的电磁兼容性；部件应具有承受周围空间或电力连接的部件引起的电磁干扰的能力。

5.187. 安全重要设备和系统及其相关电缆的设计和安装应能承受安装环境中的电磁工况。

5.188. 例如，重要的电磁干扰源包括：

(a) 开关、断路器或熔丝动作开断短路电流；
(b) 无线电发射器的电场；
(c) 其他人为的电厂内外部电磁干扰源；
(d) 自然界的电磁干扰源，如雷击。

5.189. 电力系统和部件的电磁鉴定依据：

(a) 通过系统集成设计和部件设计使电磁噪声与电力部件耦合最小化；
(b) 通过试验证明部件能承受预期的电磁噪声水平；
(c) 通过试验证明电磁发射在可接受的水平以内。

5.190. 降低电磁噪声产生和耦合的技术包括：

(a) 在干扰源抑制电磁噪声；
(b) 在仪器仪表和控制系统的信号电缆与电力电缆之间的分离和隔离；
(c) 设备和电缆屏蔽外部磁场源和电磁场源；
(d) 在与敏感电子电路耦合前过滤电磁噪音；
(e) 消除或隔离电子设备的地电位差；
(f) 电力设备、电缆通道、机柜、部件和电缆屏蔽正确接地。

5.191. 应明确所有电力系统和部件电磁兼容性能的详细要求，并证明这些系统和部件符合要求。

5.192. 适当开展安装和维护活动以确保相关电磁兼容的规定被正确实施和持续有效。

5.193. 工业环境条件下的电磁兼容国际标准可作为核电厂对电磁兼容的基本要求，必要时，应对这些标准进行补充，以涵盖核电厂部件对电磁兼容性能的更高要求。电磁兼容性能要求取决于部件可能遭受的重复浪涌（例如开断感性负载和振铃继电器）和高能浪涌（例如电源故障和雷击）。

5.194. 需通过对整个核电厂的特定分析，来确定其电力系统和部件的电磁兼容性能。每个电力部件的电磁兼容性要求的充分性是在这些机组特定分析的基础上进行评价的。

5.195. 电力系统和部件设计中应考虑的电磁干扰类型包括：

(a) 辐射电磁干扰的发射及抗扰度；
(b) 通过电缆发射和传导的电磁干扰；
(c) 静电放电；
(d) 开关暂态和浪涌；
(e) 在电厂中使用的无线系统和设备的发射特性，其中也包括维护、维修和测量设备的发射特性。无线系统和设备包括移动电话、无线电收发器和无线数据通信网络等。

5.196. 应考虑是否有必要在某些敏感设备附近设立禁区，在这些设备内不允许使用无线设备和其他便携式电磁干扰源的操作（如电焊）。

5.197. 应为电厂所有设备设定辐射电磁和传导电磁发射限值。

5.198. 电厂中任何电力或电子设备都会对电磁条件产生影响。因此，电磁辐射的限值应适用于所有电厂设备，而不仅适用于安全重要设备。

5.199. 应将单一部件的运行电磁发射值限制在一定数量范围内，以保证任何单一部件都不会产生导致显著危害的电磁干扰。

5.200. 设备鉴定计划应表明电厂所有设备所有物项的电磁辐射都在规定的限值内。

5.201. 设备和系统（包括相关电缆）的设计和安装应适当限制电磁干扰在电厂设备间的传播（通过辐射和传导）。

5.202. 仪器仪表电缆应通过充分绞合和屏蔽以最大限度地减少电磁干扰和静电干扰。

5.203. SSG-39[2]为电力系统的电子设备电磁兼容性提供了更多的建议和指导。

老化设计

5.204. 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老化相关的退化可能性，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。”

5.205. 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。”

5.206. 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退化。”

5.207. SSR-2/1（Rev.1）[1]要求 31 和第 5.51 段、第 5.52 段的目的是为了保证在恶劣环境条件下，老化效应不会影响安全部件的功能。在功能被显著影响之前，部件在正常工况下运行时的退化是必然发生的。

5.208. 设计过程中应确定电力部件的显著老化机理及应对此机理影响的措施。

5.209. 识别潜在的老化影响首先包含对相关老化现象的理解，这是设计流程的组成部分。

5.210. 最常见的老化效应是由热和辐照造成的，但其他现象对于某些部件也可能是重要的老化机理（例如机械振动和化学反应导致的退化）。

5.211. 维护计划、监视计划和老化管理计划应识别可能导致设备不能执行其安全功能的退化（老化）趋势。

5.212. 老化的监控方法包括：

(a) 进行部件试验或从部件中抽样进行老化试验；
(b) 目视视察；
(c) 运行经验分析。

5.213. 应对和处理老化影响的措施包括：

(a) 在鉴定寿命结束前更换部件；
(b) 调整功能性参数以说明老化影响；
(c) 改变维护程序或环境条件以减缓老化进程。

5.214. 应确定安全级部件的鉴定寿命，以使其在恶劣环境条件下能执行安全功能。

5.215. 应在鉴定寿命内更换安全级部件。

5.216. 部件的在役质量鉴定可以表明该部件的鉴定寿命是经验证的，或表明寿命与预期不符。部件的在役质量鉴定信息可以用于增加或减少该部件的鉴定寿命。

5.217. 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》[9]提供了更多关于老化管理的建议和指导，包括设备鉴定和老化管理计划之间的接口。

访问控制

5.218. 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的安全重要物项的情况。”

5.219. 应限制对安全重要系统中设备的访问，以防止未经授权的访问并减少出错的可能性。

5.220. 有效的方法包括一系列实物安保防护的组合，例如上锁的外壳、上锁的房间、外壳门上的警报器和行政措施等。

5.221. 应特别关注对定值调整和校对操作的准入控制，因为这些操作对防止因运维错误引起的系统性能退化有着重要作用。

5.222. 关于访问控制和电力系统中关于计算机应用安全的更多要求见 SSG-39[2]。

监视试验及可试验性

试验规定

5.223. 所有安全重要系统应包括试验规定，包括适当的自检能力。

5.224. 为满足系统和部件的可用性要求，试验规定应与运行试验程序相协调。包括在确定试验频率时考虑部件试验的故障率，以及某些试验只能在换料大修期间执行。

5.225. 试验准备的内容包括程序、试验设备接口、试验设备的安装和自检设备。

5.226. 在包括功率运行的所有正常运行模式下，应能对安全级系统设备进行试验和校准，同时应保持安全级系统执行其安全功能的能力。

5.227. 通常，为保证安全级系统的可靠性，有必要在电厂运行期间进行定期试验；然而，如果试验会影响电厂的安全运行，则有时需避免进行试验。

5.228. 如果对电厂的安全或运行产生不利影响，则无需在功率运行期间进行试验和校准。

5.229. 如果在功率运行期间不具备试验的条件，那么安全级设备应满足以下要求：

(a) 正当性可能受到影响功能的可靠性是可接受的；
(b) 停堆期间试验的可能性。

试验程序

5.230. 安全重要系统的设计应包括制定相应试验程序，以满足以下安全导则的要求：

(a) 原子能机构《安全标准丛书》第 NS-G-2.2 号《核电厂运行限值和条件及运行程序》[10]；
(b) 原子能机构《安全标准丛书》第 NS-G-2.4 号《核电厂营运组织》[11]；
(c) 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》[12]；
(d) 原子能机构《安全标准丛书》第 NS-G-2.14 号《核电厂的运行行为》[13]。

5.231. 试验程序一般包括：

(a) 试验目的；
(b) 试验的系统和部件；
(c) 主要试验计划；
(d) 进行试验的依据和正当性以及试验间隔；
(e) 验收标准；
(f) 所需文件和报告；
(g) 程序有效性的定期评审；
(h) 用于管理试验实施的独立程序。

5.232. 试验的范围和频率应符合功能需求和可用性要求。

5.233. 试验程序的实施应提供：

(a) 系统和部件的客观状态；
(b) 对部件退化的评定；
(c) 协助检测部件退化的趋势数据；
(d) 系统内出现早期故障的迹象；
(e) 在重做失败的试验之前，为确定试验可操作性而应进行评价的要求。

5.234. 在重做试验的结果可以用来证明所涉及的系统或部件的可用性之前，必须对试验失败的原因及采取的补救措施进行评价和记录。纠正措施可包括校准、维护或维修部件，或修改试验程序。

5.235. 对电力系统中电子元器件的试验程序，包括含电子元器件的保护设备，还应满足安全导则 SSG-39[2]相应要求。

5.236. 试验程序应确定定期试验方法，并满足以下要求：

(a) 在试验期间确保电厂的安全；
(b) 定期试验既不影响安全级系统的独立性，也不提高发生共因故障的可能性；
(c) 不应超出设计使用条件而使电厂的任何部件退化（例如，在空载或频繁快速启动时，柴油机的可运行性或可靠性可能会降低）；
(d) 为快速评定系统或部件的总体状态，应对各试验项目的实施顺序进行排序；
(e) 确认系统和部件满足设计基准的功能和性能要求；
(f) 包括验收标准；
(g) 应试验所有安全重要功能的输入和输出，如警报、指示、控制动作和驱动设备的操作；
(h) 尽量减少任何安全动作误启动的可能性，尽量减少试验对电厂可用性造成的其他不利影响；
(i) 尽可能减少设备退出运行的时间；
(j) 尽可能在系统执行其预期功能的实际或模拟运行工况下完成试验；
(k) 完成试验后，需核实任何因定期试验而受到影响的物项都已正确地回归到原来的正常运行状态；

(l) 禁止使用临时试验设备、临时“跳线”或临时修改电厂设备中的计算机代码或数据。

如果设计上有考虑连接试验设备的接口，那么待试验的安全重要设备可以临时接入试验设备。

可维护性

5.237. 电力系统的设计内容应包括所有系统和部件的维护计划。

5.238. 安全重要电力系统的设计和安装应便于监视和维护，便于维护人员和工具及时进入，并在故障的情况下容易诊断和维修，以尽量降低维护人员的人身伤害风险。

5.239. 便于维护、故障排除和维修的设计原则包括：

(a) 设备不应布置在通常处于极端温度或极端湿度的区域；
(b) 设备不应布置在可能有高放射性水平的区域；
(c) 在执行所需的维护活动时，需考虑到人因的影响（能力和局限性）；
(d) 应在设备周围留有足够的空间，以确保维护人员能够在正常工作工况下完成维护任务。

5.240. 对安全重要电力系统的维护方法应不会对电厂的安全造成任何不利影响。

试验或维护期间电力设备退出运行规定

5.241. 当电力设备退出运行时，应确保其被正确隔离，以保护人员人身安全和避免误操作。

5.242. 如果使用设施进行试验或维护会损害系统功能，则外接设备的接口应具备硬件联锁，以确保在没有人工干预的情况下，待试验或维护系统不能与试验或维护设备进行交互操作。

5.243. 电力系统应具备提示其满足投用条件的设计功能。

5.244. 除非可以充分证明系统的运行可靠性是可接受的，否则安全级系统中任何单一设备退出运行都不应导致系统丧失最低的冗余要求。

5.245. 符合第 5.244 段设计要求的安全级系统应允许对其一部分进行定期试验，而其余运行部分可继续执行要求的安全功能。

5.246. 应在主控室中显示安全级系统设备的不可运行或旁通状态。

5.247. 对于频繁处于旁通或不可运行状态的部件，其状态应在主控室中自动显示。

5.248. NS-G-2.6[12]为系统及设备在试验和维护后恢复运行提供指导。

群堆电厂的共用结构、系统和部件

5.249. SSR-2/1（Rev.1）[1]要求 33 规定：

> “多机组核电厂的每台机组都必须具备自身的安全系统，并必须具备自身的设计扩展工况安全特性。”

5.250. 拥有多机组核电厂的每个机组都应该有相互隔离和独立的安全重要电力系统。

5.251. 安全重要电力系统和部件不应在反应堆机组之间共用，除非可以证明在所有机组同时发生事故时，共用的安全重要电力系统或部件执行安全功能的能力没有被显著削弱。

5.252. 应证明在机组之间共用的系统或部件不会增加事故及共因故障发生的可能性或后果的严重性，也不会增加在维护共用系统的共用部件时导致一个或多机组停堆的可能性。

5.253. 分析具有共用系统机组的单一故障标准符合性时，应满足以下条件：

(a) 当共用系统或部件或与其有接口的支持系统出现单一故障时，所有机组的安全级系统仍可执行其安全功能。

(b) 当各机组的非共用系统同时发生单一故障时，每个机组的安全级系统仍可执行其安全功能。

5.254. 本“安全导则”第 5.253 (a) 和 (b) 段不需要同时满足。

标记与识别

5.255. SSR-2/1（Rev.1）[1]第 5.33 段指出：

> “就安全系统的每个冗余元素而言，电厂内的安全系统设备（包括电缆和线槽）必须易于识别。”

5.256. 在电厂设计、建造和运行的各阶段，应使用协调一致的方法来命名和标识所有电力部件。

5.257. 标识应易于识别而不需要经常查阅图纸、手册或其他资料。

5.258. 不同安全组或不同安全级的部件应易于区分。

5.259. 标记可以采取标签或颜色编码的形式。

5.260. 连贯且易于理解的系统和部件命名和标记方式可降低运行、维护、试验、改造、维修或校准错误对象的可能性。

5.261. 安装在已有明确标识的设备和装置内的部件或模块不需要标识。设备或装置的配置管理通常足以支持这些部件、模块以及计算机软件的标识。

电力贯穿件

5.262. 电力贯穿件是实现安全壳安全功能的设备，应当满足相应的安全分级要求。

5.263. 电力贯穿件的结构完整性功能包括能够耐受额定电流和故障电流，且泄漏率不会超过规定的水平。对于不影响贯穿件结构完整性的电力功能的安全分级，应和与其连接的安全壳内部物项保持一致。

5.264. 电力贯穿件应作为负载与开关之间连接电缆的一部分。

5.265. 电力贯穿件额定值的选择应当满足：

(a) 贯穿件的额定持续工作电压不小于所在系统的标称电压；
(b) 贯穿件的额定冲击耐受电压不小于所在系统最大预计的暂态过电压；
(c) 贯穿件应能持续承载各种电厂状态下的预计负载电流，而不超过导体允许的温升限值或导致压力边界的退化；

(d) 在预计的电压波动工况下，贯穿件应能够安全地承受从短路发生至保护设备切除故障期间的短路电流；

(e) 当过流保护设备因单一随机故障故障后，贯穿件应能够承受最大的预计过电流，且不应丧失结构完整性。

5.266. 在整定保护设备时，应考虑电力贯穿件持续额定电流值和短时耐受电流值。

5.267. 安全壳贯穿件应配置冗余的安全保护设备，应且动作于断开不同的开关设备。

5.268. 若通过单一故障标准分析表明，非能动保护设备（例如熔断器）不会故障且假想始发事件不会影响其功能为高置信度事件，则可以选用单一的非能动保护设备（例如熔断器）来保护贯穿件。

5.269. 若贯穿件能长期承受安全壳内部故障导致的最大预计电流，则不需要配置冗余的保护措施。

5.270. 贯穿件应满足与其连接的电缆相同的隔离标准要求。

配电系统

性能

5.271. 每个配电系统应有足够的容量和性能，以满足下列要求：

(a) 在所有设计要求的工况下给所需的负载供电；

(b) 在电力故障情况下承受最大的过电流；

(c) 在暂态工况下不会损害配电系统的任何部件或对部件造成不利影响；

(d) 按要求给负载供电。

主回路、分支回路及其负载的保护设备

5.272. 所有主回路和分支回路应有过载和短路保护，并应对接地故障进行监控并在适当情况下给予保护。

5.273. 保护设备应具有适当的尺寸、设置和协调，以防止配电系统主回路和分支回路的设备、总线和电缆在过载和故障工况下损坏。

5.274. 安全级系统的保护设备应是安全级系统的一部分。

5.275. 为免受环境条件影响、限制电磁辐射和保护人员，保护设备应安装在盘柜外壳内。

5.276. 保护设备的功能是尽量减少对设备的损坏，以及由于机械故障、电力故障或其他不可接受的工况而造成的不必要的供电中断。保护的对象包括支持安全级电力系统执行其安全功能所需的设备，以及提高安全级设备可用性和可靠性的部件。

5.277. 保护设备的协调配合应保证只有电力系统中故障部分被隔离，其余电力回路应不受影响。

控制和监控

5.278. 为监控和控制场内和场外电力系统，主控室应配备适当的仪器仪表和控制设备。

5.279. 电力系统的人机接口需符合 SSG-39[2]相关要求。

5.280. 应提供足够的监控信息以评定安全级电力系统的可运行性。这些信息包括：

(a) 断路器位置（安全级电力系统、电源和大型负载）；
(b) 总线电压和电流；
(c) 备用电源的电压、电流和频率。

5.281. 应提供旁通状态和设备退出运行的指示。

5.282. 应为电厂所有状态及电力系统所有重要事件制定相应的运行程序。

5.283. 为监视和控制安全级电力系统执行其安全功能，应在辅助控制室内配置足够的仪器仪表和控制设备。

5.284. 为使运行人员准确有效地实施检测、诊断和操作，应设计电力系统相关的警报和信号系统。

5.285. 安全级电力系统不可用状态的警报应由断电逻辑实现。

5.286. 所有安全运行应可自动启动和控制。

5.287. 当满足下列要求时，安全操作可以只采用手动模式：

(a) 运行人员能从安全级系统的传感器和设备获得足够而明晰的信息，对需要采取安全措施的必要性作出合理的判断。
(b) 为运行人员提供执行安全任务的书面程序和培训。
(c) 运行人员有足够的时间评价电厂的状况和完成所需的操作。
(d) 运行人员有足够控制电厂的手段来执行所需的操作。
(e) 执行操作的运行人员之间的通信系统足以确保这些操作的正确执行。

5.288. 应在系统级和设备级提供手动启动安全操作的手段。

5.289. 手动启动安全操作为防止异常运行提供了一种纵深防御的方法，同时可支持长期的事故后运行。

5.290. 场内电力系统的控制应包括以下功能：

(a) 当正常场外电源不可用时，应自动选择场外备用电源；
(b) 应采用手动或自动方式切换到场外备用电源；
(c) 当优选电源退化且未恢复时，安全级电力系统应自动切除一部分负载（按设计基准规定）和所有其他电源；
(d) 安全级电力系统应按照规定顺序自动启动和接入备用交流电源和负载；
(e) 备用交流电源应采用手动方式；
(f) 当正常电源恢复供电时，安全级供配电系统应通过同步恢复到正常电源供电；
(g) 在正常运行或停堆模式下，应易于手动切换至试验、维护和维修状态。

5.291. 无论实际需求的顺序如何，自动加载程序都应正确工作。丧失场外电源和事故信号可能以任何顺序出现。

安全相关备用交流电源

5.292. 有些设计方案配置了不执行安全系统支持功能的备用交流电源，安全级备用交流电源的通用设计导则应同样适用，安全相关备用交流电源的设备鉴定等级、设计确认和文档记录级别应与安全相关部件的原则保持一致。

5.293. 对于不要求备用交流电源执行安全功能的核电厂，为满足纵深防御的功能需求，应配置可靠的安全相关的备用交流电源作为安全级系统的补充电源，以降低安全级系统失电的风险。

5.294. 备用电源应包括一台发电机组及其配套的全部辅助设备，以及用于原动机启动和持续运行的专用独立储能部件。

5.295. 备用电源应具有足够的容量和能力来启动和带载设计基准所要求的全部负载。

6. 优选电源设计

概述

6.1. SSR-2/1（Rev.1）[1]要求 41 规定：

> “不得让电网的干扰因素包括预期的电网供电电压和电频变化损害核电厂安全重要物项的功能。”

6.2. 在核电厂启动、停堆和应急工况下，输电系统均应向核电厂稳定、持续地供电。

6.3. 安全级电力系统的优选电源来自电网。当功率运行时，安全级电力系统的电源来自主发电机，并接入电网。发电机可抵御电网的电压波动，并在机组孤岛运行时向场内电力系统供电。

6.4. 输电系统应将核电厂产生的电能稳定、连续地送出。

6.5. 当电网发生预计事件后但仍与核电厂连接时，第 6.4 段的要求同样适用。

6.6. 优选电源可来自电网相对独立的不同部分，为减少电网、开关站或主发电机发生事故引发的共因故障风险，可考虑将核电厂电力系统的不同列接至不同的优选电源，同时不会显著增加意外跳闸和其他扰动的风险。

保护设备和高压设备的可靠性

6.7. 接入系统、控制回路和继电保护的设计应有利于提高优选电源的可靠性。

6.8. 接入系统和继电保护设计时需考虑的事件包括：

(a) 电网甩负荷及失步振荡；
(b) 停堆期间发生的预计电力事件；
(c) 户外电力设备被污染；
(d) 地磁风暴；
(e) 变压器绕组匝间故障和接入系统线路断相事件等。

6.9. 在高污染风险地区，可通过增加绝缘子长度来保证绝缘子的污染不会引发场外电源共因故障。

场外电源

6.10. 在电厂的所有运行模式下，场外电源均应具备足够的容量和能力向场内负载供电。

6.11. 当核电机组停堆时，应注意电网电压变化对核电厂场内电力系统的影响。

6.12. 输电系统是场内电力系统的供电电源，对电厂安全设计中的纵深防御起着非常重要的作用。当场外电源可用时，核电厂可以更加灵活可靠地正常停堆或在暂态和事故时安全停堆。因此，场外电源需具备足够的供电容量和能力。

6.13. 场外电源应包括两路或多路实体独立的回路，这样可将场外电源同时故障的可能性减少至实际可行的程度。

6.14. 电厂与电网间的输电回路数量取决于整个电网的容量和电厂的设计。

6.15. 如果经安全分析报告论证且满足 SSR-2/1（Rev.1）[1]提出的技术安全目标时，核电厂的每个场外电源可只设一回输电线路。例如，采用非能动工程安全特性的反应堆设计，单一场外电源是可接受的。

6.16. 只有单回输电线路的电厂因线路跳闸而被迫大修的概率可能会更高，尤其应特别考虑线路雷击频率较高的地区。丧失场外电源的情况下，核电厂可能会过早达到设计的热力循环状态，除非电厂的设计使其可承受丧失场外电源带来的影响，或采取了额外的措施来降低输电线路被迫大修的次数，如增加输电线路回路数量或提高线路保护水平。

6.17. 至少，每路场外电源应有足够的容量和能力为所有用于缓解设计基准事故和预计运行事件影响的电力负载供电。

6.18. 除满足电厂正常运行、启动和停堆的基本用电需求以外，每路场外电源应有额外的能力向电厂所有正常电力负载供电。

6.19. 对于群堆场址，每台机组应接入两路场外电源，从而使所有机组都能同时满足 SSR-2/1（Rev.1）[1]规定的技术安全目标。

6.20. 为满足第 6.19 段的建议，两个或多个核电场址或机组可共用场外电源，也可以配置互相独立的专用场外电源回路。

6.21. 对于群堆场址，若安全分析报告表明一回场外电源足够时，则该反应堆采用单回路场外电源设计也是可接受的。

6.22. 当群堆场址的多机组共用场外电源时，任何一台机组跳闸都不应影响场外电源对其他机组的场外电源可用性。

可用性

6.23. 为满足事故分析的要求，当发生设计基准事故后，至少应有一回场外电源可以在几秒钟之内自动切换至向安全总线列供电。

6.24. 在发生设计基准事故后，第二回路场外电源也应在短时间内可用。

6.25. 在发生设计基准事故后，第二回路也应在几秒内可用。

6.26. 应针对设计安全要求对厂用负载的切换系统进行评价。

6.27. 无论采用手动或自动方式切换厂用电源，均应易于完成。

6.28. 应只在必要的时候进行电源切换，因为两个带电回路之间的切换存在风险。

6.29. 当主回路失电时，优先切换至第二回路供电。两个回路的断路器之间宜设置闭锁，以防止两个回路并联运行而导致危害性电压或电流。

6.30. 设计切换时序时，应考虑切换过程中出现的电压波动和电流冲击。

6.31. 在核电厂正常运行时，应采用最可靠的电源作为正常电源。

6.32. 将最可靠的电源作为核电厂正常运行的电源，可最大限度降低对配电设备电源切换的需求。

6.33. 与电网断开连接后，核电厂开始甩负荷，随后反应堆和发电机输出功率降低至维持孤岛运行状态的厂用电负荷水平，此时蒸汽轮机未脱扣，且发电机未跳开。此切换过程会导致机组在达到稳定运行前出现频率和电压偏移。

6.34. 对于具备孤岛运行模式的电厂，场内电力系统的设计应能适应机组从正常运行切换至孤岛运行时出现的电压和频率偏移及暂态过程。

6.35. 主发电机跳闸后，可立即跳开发电机出口断路器，实现由场外电源向场内电力系统立即供电。发电机负载开关也可实现该目标，但切换过程无法立即完成。

独立性

6.36. 两回场外电源的设计和位置应尽可能减少其在所有电厂工况下和设计基准环境条件下同时发生故障的可能性。

6.37. 可导致两回场外电源同时故障的事件示例包括：

(a) 两回场外电源线路同塔架设；
(b) 导致两回场外电源同时故障的单台断路器故障、开关站总线故障或控制电源故障。

开关站

6.38. 开关站的实体设计应使单台设备故障导致向安全级负载供电的场外电源回路故障的可能性降到最低。

6.39. 两个或以上场外电源回路不应共用控制电源。

6.40. 开关站的控制电源应为开关站专用，不应引自核电厂其他电力系统。

6.41. 户外开关站的控制回路应在进入厂房处设置过电压保护，且应与场内控制回路隔离。

6.42. 开关站设备设计应可承受最严重故障时的破坏力。

6.43. 保护系统应将提供安全负载供电的场外电源回路同时故障的可能性降至最低。

6.44. 保护系统的设计特性建议包括：

(a) 主保护和后备保护；
(b) 断路器失灵保护；
(c) 双蓄电池系统；
(d) 断路器设双跳闸线圈。

电网健稳性和可靠性

6.45. 电网应向核电厂提供稳定的场外电源，当核电厂负载变化时，电网的电压和频率应维持在规定限值之内。

6.46. 电网的惯性应足以保证一台大型发电机组退出，一台核电机组跳开，或电网的总线故障时不会危及电网的健稳性。

6.47. 具备足够的容量（即电压和频率）且能对核电厂不间断地供电是电网可靠性的指标。

输电系统运营商和核电厂营运组织之间的接口和通信

6.48. 核电厂营运组织和输电系统运营商应确定设备接口和通信接口并提出要求，包括：

(a) 通信渠道；
(b) 运行程序；
(c) 核电厂停堆或事故工况下优先选择的供电通道；
(d) 运行经验反馈；
(e) 维护和停堆计划协调；
(f) 维护要求；
(g) 当出现核电厂电压持续下降，需要营运组织手动切除场外电源的情况时，双方的沟通协调机制。

6.49. 在许多国家的电力市场，电力系统正在进行分割，并建立独立的发电、输电和配电公司。

6.50. 为保证核电厂的安全运行和安全停堆，输电系统运营商和核电厂营运组织需建立特别的沟通配合机制。这种机制基于以下共同目标：保证核安全，保证核电厂电力系统供电安全性。可由一个或多个输电系统运营商向核电厂供电。

6.51. 经验表明，核电厂营运组织和输电系统运营商就计划协调机制（包括明确的责任）签署正式协议是有益的。

6.52. 核电厂营运组织计划进行以下活动时应告知输电系统运营商，如停堆、改造和维护活动，以及对电厂设计、配置、运行、限值、电力保护系统或性能的修改，这些活动可能会影响输电系统运营商向核电厂供电的能力。

6.53. 输电系统运营商计划进行以下活动时应告知核电厂营运组织，如电网的停电、改造和维护等可能影响核电厂场外电源可用性和可靠性的活动。该类活动的示例如通往核电厂输电线路的服务变电站维护工作。

6.54. 核电厂营运组织应与输电系统运营商就电力保护方案进行配合，在电网发生故障时，可最大限度地保证核电厂和电网供电的可用性。

6.55. 上述协调配合机制也适用于核电厂和电网改造可能会影响到双方接口的情况。

6.56. 核电厂营运组织应与输电系统运营商进行配合，并验证电网在线分析工具预测的低电压穿越的精确度和保守性是有效的。

6.57. 核电厂营运组织应确保核电厂的运行许可证要求和设计要求能得到输电系统运营商的充分理解，从而确保输电系统在受到扰动、暂态和营运组织影响时不会对核安全造成威胁。

6.58. 出于确保核电厂接入电网安全的需要，核电厂营运组织有必要与输电系统运营商协商并达成一致，以使核电厂开关站内的涉网设备（包括控制设备和保护设备）及与之相连的输电回路采用比其他电网设备更高的标准，或者提高试验和视察的频率。

6.59. 需要注意优选电源（如开关站或电网）的结构、系统和部件不受核电厂营运组织的直接管辖，且核监管机构与特定场址相关。

6.60. 对电厂安全重要的供电电源首要特征应在安全分析中予以记录，且许可证持有人应确保供电电源已具备这些特性。

电网接入可靠性评定

6.61. 应通过定期开展分析论证，来确保电网有符合要求的电力（以合适的电压和频率）向核电厂供电，并对电网接入的可靠性进行评定。

6.62. 上述分析所考虑的因素包括丧失核电机组，丧失其他重要的发电机组，丧失输电系统的重要部件，以及保护设备和输电系统中断路器和其他设备的故障率。

6.63. 原子能机构《核能丛书》第 NG-T-3.8 号《电网可靠性及与核电厂接口》[14]就核电厂与电网的连接提供了更多的背景信息。

7. 安全级电力系统设计

概述

7.1. 在核电厂任一运行模式下，均应保证电力系统的电压和频率波动不能降低任何安全系统设备的性能。

预计电力事件

7.2. 应采用系统化方法识别由优选电源或场内电源故障引起的安全级总线电压和频率的波动和暂态，并确认保护方案的充分性。

7.3. 需考虑的预计电力事件已在第 5 部分中给出。

7.4. 作为场内电力系统的备用电源，其电压和频率在负载加载期间会产生波动。

7.5. 这些电压和频率波动幅度不应影响正在启动、已加载或运行中的设备。

7.6. 应分析所有的运行模式以及对称性和非对称性事件，因其电压上升时间、故障持续时间、振幅或不对称性等特点的不同，会对电力系统中的不同部件造成不同程度的损害。

总线监控与切换

7.7. 应检测安全级交流电力系统总线优选电源的退化情况（例如过电压、低电压、超频或低频）。

7.8. 当优选电源的退化程度超出设计要求的规定限值，应自动断开其电源。

7.9. 当安全级总线断开退化的优选电源后，其应按照下述顺序自动投入备用电源：

(a) 其他可用的场外备用电源；
(b) 属于同一安全组的场内备用电源。

7.10. 通过延时投入备用电源的设计，可使安全级电力系统经受较小的扰动。

7.11. 事故分析中的假设应支持延时。

7.12. 向安全级总线供电的优选电源回路推荐采用双断路器接线方式（例如第 1 部分图 3）。

7.13. 若未采用可替代优选电源自动投入的方案，则应表明此方案符合电厂的设计标准。

7.14. 应确定电厂各种运行状态和设计基准事故工况下安全级电力系统的运行参数，包括设计分析中确定的可用率，并据此定义核电厂运行工况及运行限值。

7.15. 每列电源应配置独立的检测、保护方案，以断开安全级总线与优选电源的连接并进行甩负荷，并在电压下降、频率退化或失压的情况下启动备用电源。

7.16. 以下建议适用于安全级总线电压和频率监控及保护方案配置，用于防止电压和频率退化及失压。

(a) 应直接监控接有备用电源的安全级总线电压和频率。

(b) 安全级总线电压和频率退化的警报信号应送至主控室。

(c) 当向安全级总线供电的电源电压和频率退化超出可接受的限值时，应自动将其与安全级总线断开。

  (i) 有必要在安全级总线上设置两级不同延时的电压保护：第一级用来检测安全级总线是否丧失场外电源，第二级用来检测安全级总线电压的退化程度。

(d) 当检测到优选电源出现不可接受的过电压时，应自动将其与安全级总线断开；

  (i) 过电压保护的整定值和延时与连接设备的过电压能力相配合；

  (ii) 过电压监测设备的复位值应低于备用电源的最低预期运行电压值。

(e) 应监控交流电力系统全部三相电力参数。

(f) 测量回路应该避免谐波对精度造成的影响。

(g) 应设计冗余的电力保护系统。

(h) 测量回路故障不应导致误操作或监控和保护拒动。

(i) 设计上应考虑降低优选电源意外断开的风险。

  (i) 采用一致性判别逻辑和延时来躲过系统暂态，是降低优选电源意外断开风险的方法之一；

(j) 监控和保护系统应具备在线试验和校准的能力。

(k) 主控室应能监控任一旁路回路的运行状态。

7.17. 仅用于警报的电压监控无需遵守第 7.16 段的建议。

7.18. 安全级电力系统的低电压和延时整定值应根据各级场内配电系统供电的安全级用电负荷的电压来确定。

7.19. 不恰当的电压保护逻辑会对安全级系统和设备造成不利影响，例如：将安全级负载从备用电力系统中误卸载，或由于电动机正常起动暂态导致安全级电力系统从场外电源中误切除。

设计可靠性

单一故障标准

7.20. 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。”

7.21. 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用于某一安全组或安全系统时发生的一种故障模式。”

7.22. SSR-2/1（Rev.1）[1]第 5.40 段指出：

> “设计必须适当考虑非能动部件的故障，除非已在单一故障分析中以非常高的置信度证明该部件的可靠性，即该部件发生故障的可能性非常小并且其功能仍将不受假想始发事件的影响。”

7.23. 尽管在 SSR-2/1（Rev.1）[1]定义的单一故障标准仅适用于安全级系统，然而在任何系统中应用单一故障标准的概念都是确保其功能具备高可靠性的有效方法。

7.24. 通常采用冗余性、独立性、可试验性、连续监控、环境鉴定以及可维护性等概念以达到满足单一故障标准的要求。

7.25. 每个安全组应能在假想始发事件叠加下述情况时执行所有要求的功能：

(a) 安全级系统内任何单一可检测到的故障；
(b) 任何无法检测的故障（例如不能通过定期试验、警报或异常指示等方法检测到的故障）；
(c) 所有由单一故障引起的故障；
(d) 由执行安全功能的设计基准事件引起或由其引起的系统所有故障和误动作；
(e) 在满足核电厂运行限值和条件的情况下，安全级系统相关部件因试验或维护退出运行或旁路运行。

7.26. 在证明不符合单一故障标准的情况是否可接受时，可特别关注发生低频外部危害的可能性以及电力系统运行所必需的支持系统的长期可用性。

7.27. 不符合单一故障标准的情况应属于特例，且应在安全分析中充分说明。

7.28. 可接受的不符合单一故障标准的理由如下：

(a) 假想始发事件非常罕见；
(b) 假想始发事件所导致的后果极不可能发生；
(c) 由于维护、维修或定期试验，特定部件在有限时间内退出运行；
(d) 只针对设计扩展工况的功能；
(e) 证明假设故障发生的可能性足够小以至于可忽略不计。

7.29. 在应用单一故障标准时，可靠性分析、概率评定、运行经验、工程判断或这些方法的组合可作为是否排除特定故障的基础。

7.30. 如果在试验或维护期间无法满足单一故障标准，应从其重要性及其对堆芯熔化频率的潜在影响评价其退出运行的时间。

7.31. 在维护、维修或试验期间无法满足单一故障标准时，至少应符合核电厂运行限值及条件。

7.32. 当遵守单一故障标准不足以满足可靠性要求时，应提供附加的设计功能或对设计进行修改以确保系统满足可靠性要求。

保护动作

7.33. 安全级电力系统及其保护设备和自动功能应设计为一旦经自动或手动触发将按照预期序列连续完成保护动作。

7.34. 运行人员应慎重采取将安全级电力系统恢复到正常备用工况的操作。

安全级备用交流电源

概述

7.35. SSR-2/1（Rev.1）[1]要求 68 规定：

> “核电厂的设计必须包括能够在发生预计运行事件和设计基准事故时一旦丧失场外电源的情况下提供必要电力的应急电源。设计必须包括在设计扩展工况下提供必要电力的备用电源。”

7.36. 备用交流电源应由发电机及其辅助设备、用于原动机启动及运行的专用独立储能电源组成。

7.37. 优选方法是每列宜配置一台备用电源，以避免多电机并列运行的必要性。

7.38. 如果每列采用多个电源，应证明该配置计划是安全可靠的。

7.39. 备用电源应具备足够的容量和能力，能够在各种条件下启动并持续供应其分区内的全部负载，并允许以下工况的裕度：

(a) 负载处于偏心振摆运行状态；

(b) 负载过载运行；

(c) 发电机处于允许的电压和频率范围下限或上限运行时导致负载特性的改变；

(d) 环境条件或者燃油温度变化导致发动机降容运行，例如吸入口空气温度较高；

(e) 未来负载的增加。

7.40. 在应急运行模式下，柴油发电机应在设计规定的电压和频率范围内运行。通常情况下，发电机的稳态运行电压和频率保持在定义值的±2%之内。当电动机运行电压低于额定电压时，电动机的某些性能特征将轻微改变并且功耗将增加。

7.41. 备用电源的原动机宜具备在额定出力下连续运行 3000－4000 小时且无需大修的能力。原动机一般具备在 24 小时内以 10%－15%的过载率持续运行 2 小时的能力。这种设计可保证应急电源在以下事故初始阶段满足短期的过负载需求，包括：安全系统正在实施安全注入、冷却剂系统运行但水泵处于偏心振摆的运行工况、冷却剂系统实际流量高于热工水力分析的给定值。这种工况下热工水力分析通常是趋于保守的，以至于低估了电动机的预期功耗。

7.42. 发电机运行在频率范围下限时，应当评价电动机是否满足被驱动泵的流量要求。

7.43. 发电机的频率波动影响电动机提供的转矩值。

7.44. 备用电源应能在设计基准要求的时间周期内持续运行且不会因维护活动而停止。

7.45. 当应急总线丧失优选电源时，备用电源应能自动启动。

7.46. 即使安全级总线未失电，备用交流电源也可由应急信号触发而自动启动。

7.47. 备用交流电源的实际启动和接入时间应与安全分析中提出的启动时间相匹配。

7.48. 场内燃油及其他消耗品（如润滑油）应足够支持备用电源运行至场外电源恢复。

7.49. 场外燃油及其他消耗品的供应取决于场内备用电源的消耗品是否需要补充，以及补充供应所需的时间是否满足要求。大多数国家规定，场内备用电源可在无外部补充消耗的情况下持续运行 1－2 周。

7.50. 备用电源的运行不应依赖与其不属于同列的电力系统电源和仪其仪表和控制系统电源。

7.51. 用于备用电源启动、接入、运行以及保护的仪器仪表和控制系统应由同列的蓄电池供电。

7.52. 与备用电源同列的直流电源故障会导致其不可用。

7.53. 当备用电源使用专用蓄电池时，应充分监视这些电池的状态，并检测其退化及故障状态，使其与其他安全级蓄电池具有相同的状态。

7.54. 只有当稳定可靠的优选电源或其他备用电源不可用时，场内备用电源才能投入。

7.55. 不得使用备用电源来维持主发电机满功率运行。

7.56. 只有满足本“安全导则”的独立性要求时，安全级电力系统才能向低安全级或非安全重要的负载供电。

7.57. 事故状态下，应自动断开由安全级总线供电的非安全级负载。

7.58. 安全级电力系统与低安全级设备之间的隔离设备应作为安全级电力系统的一部分。

7.59. 应急电源的加卸载程序应能自动甩掉所有非安全负载，并且非安全负载不应自动启动。

7.60. 在应急电源的加卸载程序中，应明确非安全负载仅在安全负载启动后才允许启动，并且取决于应急电源是否有足够容量来启动和运行非安全负载。

7.61. 将安全级电力系统总线由备用交流电源切回优选电源供电时，应采用手动操作方式。

7.62. 多列安全级总线同时从备用电源切回优选电源供电时，一次只能切回一列。

7.63. 当某一列安全级总线切回优选电源供电后，应确认对应的备用交流电源已恢复至正常备用工况后，才能允许其他列总线切回优选电源。

试验

7.64. 应给出电厂运行期间备用电源的定期试验方法。

7.65. 试验标准应确保备用电源在试验期间仍能够执行安全功能。

7.66. 试验安排不应破坏安全级系统的独立性，也不应引入产生共因故障的可能性。

7.67. 试验活动破坏安全级系统的独立性或引入产生共因故障可能性的示例包括在空载工况下试验柴油机烟尘的成分、试验完成后恢复到正常备用工况过程中的不当措施或冗余设备试验时引入的人为失误。

暂态及动态性能标准

7.68. 应显示备用交流电源的电压和频率波动范围在所供电的负载和原动机的设计基准之内。

7.69. 备用交流电源的预期持续运行电压和频率波动须维持在一定范围内。在备用交流电源的加载期间，允许出现电压和频率的短时偏差超出范围，但需确保电压和频率在下一个负载带载前恢复至正常范围，并且电动机端电压足够启动每一个步序中的负载。

7.70. 对于仅在事故工况中才会出现的连续加载需求，备用电源在顺序加载期间的性能通常是由试验方法与分析方法共同确定。

备用电源的继电保护

7.71. 在备用电源的任何运行模式下，对于保护系统免受瞬时严重故障而损坏的跳闸装置均应保持在线。

7.72. 这类保护设备示例如下：

(a) 保护备用电源免受严重故障的影响，例如超速保护和发电机差动保护；

(b) 保护安全级电力系统免受严重故障的影响，例如后备过电流保护以及低阻抗接地故障保护。

7.73. 在备用电源为安全负载供电的应急运行期间，应关闭保护设备的非严重故障的跳闸功能，但应在备用电源正常运行和试验期间保持可用。

7.74. 设计上应考虑每一个跳闸功能和旁路功能的独立试验方法。

7.75. 备用电源的所有保护跳闸警报信号均应在主控室显示。

备用交流电源的支持系统

7.76. 为了保证冗余性和独立性，冗余的备用电源的支持系统（如通风系统、冷却水泵及润滑系统）应由本列电源供电。

7.77. 备用交流电源的辅助及支持系统的容量应满足应急电源多次启动的需求。

7.78. 通常，启动系统有能力支持应急电源至少启动 5 次，为实现该目标，通常需要在指定时间后中止任何启动尝试以保留资源。

备用电力系统的燃料

7.79. 应保证备用交流电源的燃料可长期存储。

7.80. 核电厂的燃油存储时间较长，某些类型的燃油长时间存储时化学性不稳定。燃油老化及氧化会导致高含酸量、高粘稠、胶体化以及沉淀物的形成，从而阻塞过滤器。燃油质量的退化可能导致备用电源的共因故障。

7.81. 每批燃料的交付都应经过试验，以核实其符合技术规范书要求。

7.82. 通常在电厂内进行燃料的抽样试验。

直流系统

概述

7.83. 每列直流安全电力系统应至少包含一组蓄电池、一套充电器和一套配电盘。

7.84. 为便于维护，每列直流系统宜配置两套充电器以及两组并联的蓄电池组。

7.85. 直流系统的负载应能适应浮充电压和均充电压。

7.86. 为保证蓄电池的可用容量，直流系统总线浮充电压应高于总线标称电压，放电终止电压应低于总线标称电压。

蓄电池

7.87. 在蓄电池充电器不投用的情况下，每套电池组应能满足所有设计基准工况条件（包括工作周期和电力暂态）下的负载要求，并考虑诸如设计裕度、温度效应、近期放电情况和老化效应等因素。

7.88. 一般情况下，蓄电池容量选择的限值和条件是全厂断电工况。

7.89. 蓄电池间应配置通风设施，以保持可燃气体浓度低于限值。

7.90. 如需配置强制通风：

(a) 蓄电池室的通风系统应由与蓄电池相同列的电源供电。
(b) 应考虑将氢气监测作为一种预防措施。

7.91. 为证明蓄电池的可用性并检测其退化情况，蓄电池应进行定期试验。

7.92. 蓄电池定期试验通常按照该型号蓄电池推荐的方法进行，依据蓄电池状况，蓄电池容量的试验周期一般为 1－5 年，并且需要进行以下经常证实：

(a) 涓流充电电流；
(b) 每个蓄电池的电解液液位；
(c) 电解液密度抽检；

(d) 单电池电压抽样；

(e) 电池温度抽检。

7.93. 应监控蓄电池室的环境温度。

7.94. 蓄电池室的环境温度会影响电池容量和寿命。

7.95. 应监控蓄电池熔丝的状态。

充电器

7.96. 每组蓄电池都应配置专用充电器。

7.97. 每台充电器应具有足够的容量以满足以下要求：

(a) 在正常运行中保持蓄电池处于充满状态；

(b) 在可接受的时间内将蓄电池从完全放电状态恢复到最基本的充电状态，同时在丧失正常电源后可满足各种稳态和事故负载组合的供电需求。

7.98. 当整流器作为逆变器的电源时，应具有自我保护功能。

7.99. 充电回路保护包括：反向电流保护、限流功能或过载保护，以及输出欠压、超压保护。

7.100. 蓄电池充电器应能避免直流侧与交流侧的暂态互相影响。

7.101. 蓄电池充电器应能够在以下情况下保持直流电压运行在允许的范围内：

(a) 当交流电源侧故障期间产生低电压，故障清除后又恢复高电压：

(i) 当电厂近区输电线路发生故障时，典型的故障持续时间为 100－250 毫秒，当场内电力系统发生故障时，典型的故障持续时间可达 100 毫秒。当电网故障清除后，电源电压的恢复取决于发电机出口的电压水平（见图 6）。这种短时间的电压突变可能造成直流系统充电器输出严重过压；

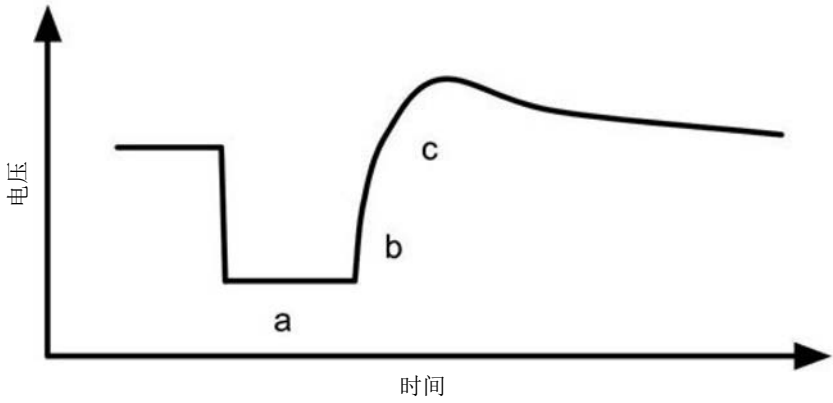
(ii) 当充电器交流侧出现低电压时瞬时关闭蓄电池充电器，当电源恢复正常后再自动重启充电器，可有效将蓄电池充电器输出电压维持在正常范围内，同时可避免直流电力系统（以及交流不间断电力系统）遭受电网故障引起的电压瞬变影响。

(b) 在输入电压升高时的甩负荷情况下：

(i) 充电器的输入电压上升幅度由发电机甩负荷前的有功、无功功率决定，此时，过电压通常为 130－150%（见图 7）。

7.102. 充电器应能够在不连接蓄电池的情况下直接为负载供电。

7.103. 直接由蓄电池充电器为负载供电的能力是体现直流电力系统电源多样性的一部分，通常不宜在这种模式下长期运行。



注：(a) 故障期间电压；(b) 电压快速上升；(c) 由于发电机励磁造成的电压上升，随后恢复正常电压。

图 6. 输电线路故障清除期间典型的场内电源电压曲线。

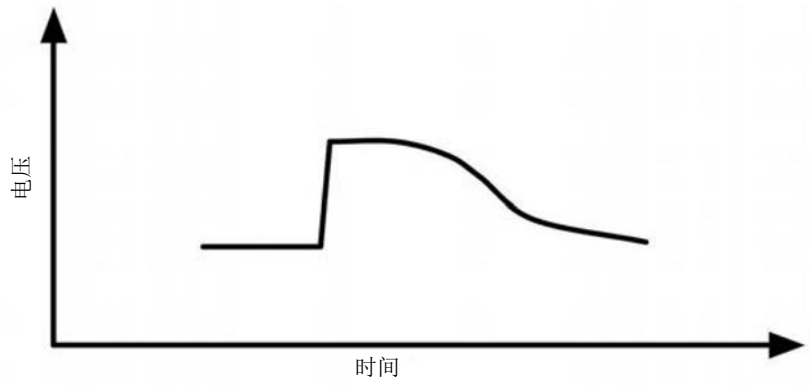


图 7. 发电机甩负荷后（孤岛运行）典型的场内电源电压曲线。

7.104. 每台充电器的交流和直流侧都应设置开关部件以隔离充电器。

交流不间断电力系统

7.105. 安全级交流不间断电力系统应向需要不间断供电的安全重要负载提供电源。

7.106. 某些电站设计不需要交流不间断电源。对于新型仪器仪表和控制系统，用直流电力系统为需要持续供电的负载供电也是可行的，这种方案可减少故障来源。

7.107. 每列安全级交流不间断电力系统应由安全级直流电力系统供电的逆变电源、同一安全组的交流总线的电源以及用于这两个电源之间自动切换的设备组成。

7.108. 交流不间断安全电力系统也可由专用的充电器、蓄电池和逆变器组成。

7.109. 交流不间断电力系统的充电器、蓄电池也应满足本“安全导则”的相关要求。

7.110. 交流不间断电力系统的电力特性和供电连续性应满足负载要求。

7.111. 一般情况下，交流不间断电力系统容量选择的限值和条件是全厂断电工况。

7.112. 交流不间断电力系统可接受其输出侧的扰动，如电压跌落或中断，但这种扰动不能导致负载功能故障或导致任何设备误动作。

7.113. 交流不间断电源的设计应满足负载以及负载间相互作用的特性和设计要求。

7.114. 例如，静态逆变器的设计应确保逆变器本身以及任何负载所产生的谐波电压不会导致所供电的系统功能退化。

直流电力系统和交流不间断电力系统的保护

7.115. 蓄电池充电器、逆变器和电动机－发电机组会限制系统短路电流值，这将影响保护设备的灵敏度。

7.116. 蓄电池充电器、逆变器和电动发电机组的保护配置应与备用电源、逆变器、静态开关、蓄电池充电器、配电盘、仪器仪表盘和机架以及它们供电的其他设备相协调。

7.117. 直流电力系统和交流不间断电力系统应配置欠压保护和过压保护。

7.118. 应为隔离（未接地）直流电力系统应配置接地检测监控。

7.119. 接地检测应在系统对地阻抗值降低至可能发生故障之前发出警报。

7.120. 直流配电系统应满足保护配合要求。

7.121. 直流电力系统回路的保护配合包括：主总线和分支回路、断路器控制回路、继电器控制回路、过程控制设备回路、电池充电器回路之间的保护配合。

7.122. 在进行直流系统保护配合分析时，应使用适当的修正系数或采用直流保护设备的跳闸特性曲线。

7.123. 安全级交流不间断电力系统应满足保护配合要求。

7.124. 交流不间断电力系统逆变器的直流侧不宜配置过压保护。

7.125. 交流不间断电力系统的主总线保护和分支电路的保护之间应配合。

7.126. 蓄电池充电器、蓄电池和逆变器（或电动发电机组）组成一个独特的功能系统，并且它们之间存在密切的相互作用，因此，正确的保护配合设置可保证系统的安全功能。例如，如果蓄电池充电器的交流电源出现过电压，蓄电池充电器可将传输至直流侧的干扰限制在不会导致安全级负载（包括不间断电源本身）跳闸的水平。

7.127. 安全级交流不间断电源应提供低频和超频保护。

8. 可备用交流电源

8.1. 如果核电厂的设计依赖于交流电源，以使核电厂在失去场外电源和安全备用电源后处于受控状态，则应在核电厂场内或附近提供可备用交流电源。

8.2. 为防止核电厂电力系统同时丧失场外电源及场内应急交流电源，应配置可备用交流电源及配套的连接设备。可备用交流电源应采用多样化设计，且不应受到场内和场外电源丧失的影响。

8.3. 附带辅助设备的可备用交流电源应鉴定符合其预期用途。

8.4. 为应对全厂断电工况，可备用交流电源应具备足够的容量为相关系统运行提供必要的电力供应，并在规定时间内将核电厂带入并维持在可控状态。

8.5. 应确保可备用交流电源能够应对全厂断电工况，包括确保反应堆衰变热量排出、维持一回路完整性、维持反应堆次临界状态以及乏燃料余热排出，并为其他电源可靠恢复提供足够的时间窗口。

8.6. 若机组配备的备用交流电源数量超过冗余性需求，可将这些电源中的一个作为可备用交流电源来使用，该交流电源不应受其他场内电源或场外电源故障的影响，并满足本部分其他建议。

8.7. 在安全备用交流电源为多机组共享的场址内，若多台机组共用同一可备用交流电源供电，当发生全厂断电时，则该可备用交流电源应具备足够的容量为所有机组的系统运行提供必要的电力供应，并在规定时间内将核电厂带入并维持在可控状态。

8.8. 在正常情况下，为某一机组配置的可备用交流电源不应该与该机组的场内电力系统相连。

8.9. 对维持可备用交流电源处于热备用状态的支持系统，可由一台或多台机组供电，并确保其电源配置不会影响可备用交流电源的可用性。

8.10. 应确保任一安全级交流备用电源与可备用交流电源之间具有最小的潜在共因故障可能性。

8.11. 不应存在因恶劣天气、外部事件或单一故障引发的单一缺陷，从而导致某一机组的安全交流备用电源故障，并同时造成所有场外电源及可备用交流电源故障。

8.12. 可备用交流电源应可接入任一或全部安全级电力系统总线。

8.13. 只有在安全级电力系统与其他电源断开连接后，才能由交流电源供电。

8.14. 可备用交流电源应能够在电厂安全分析和全厂断电分析中规定的时间内为相应负载供电。

8.15. 发生全厂失电后，应尽快使可备用交流电源可用并为负载供电。尽快恢复交流电源，可恢复电力系统的纵深防御层级，也可恢复由交流电力系统供电的安全级系统运行，同时还可以恢复能显著提升运行人员对事故响应能力的支持系统（例如照明系统及可居留系统）运行。

8.16. 可备用交流电源应具备为设计扩展工况下所必须的负载供电的能力。

8.17. 设计上应考虑采用移动电源及相关措施，用于恢复必需的电力供应。

8.18. 用于缓解堆芯融化事故后果所必需的设备应能够由任何电源供电。

9. 设计确认及文件

管理系统

9.1. 对安全级电力系统的设计策划和管理应按照原子能机构《安全标准丛书》第 GS-R-3 号《设施和活动的管理系统》[15]规定进行，并遵循原子能机构《安全标准丛书》第 GS-G-3.1 号《设施和活动管理系统的适用》[16]以及原子能机构《安全标准丛书》第 GS-G-3.5 号《核装置管理系统》[17]要求。

核实

9.2. 电力系统的容量和能力应由分析确定并由试验核实（见附录 II）。

9.3. 作为设计和设计核实的一部分，应进行如下论证且每项论证的过程应形成便于评审的文件：

(a) 论证电力系统能够完成设计基准中设定的安全功能。

(b) 论证电力系统满足设计要求。

(c) 论证安全级电力系统满足单一故障标准。

(d) 论证电力系统可靠性满足设计要求。

(e) 论证保护设备的动作经过充分配合。

(f) 论证已充分实施应对全厂断电的措施。

(g) 论证场外电源回路的可靠性满足要求，并在输电系统和发电设施规划变更后仍然满足为安全级负载供电的可用性要求。

(h) 在发生如下事件后，论证场外电源回路的容量和能力可为安全级负载连续供电：整个核电厂与电网失去连接；系统中容量最大的一台发电机脱扣；系统中负载最重的一回输电线路或联络线跳闸；或丧失系统中最大的负载。

(i) 论证每个场外电源回路都有足够的容量及能力为缓解预计运行事件及设计基准事件后果的所有负载供电。

9.4. 论证应涵盖核电厂所有的运行模式。

9.5. 核电厂营运组织应和输电系统运营商共同完成场外电源回路的可靠性及可用性论证（见第 6 部分）。

9.6. 应对安全重要系统开展系统化评定，以确认设计方案满足设计基准中关于可靠性的要求。

9.7. 对于安全重要系统的设计特性的系统化评定，可综合采用确定性标准和定量可靠性分析的方法，例如冗余性试验、故障模式及鉴定严格的鉴定。

9.8. 软件或复杂多元逻辑模块的应用会导致对共因故障可靠性和敏感性的确认产生困难。此时，可依靠消除设计及实施过程中的偏差来保证可靠性。SSG-39[2]提供了这方面的建议及指导。

9.9. 在确定安全级系统可用性时，应将其试验设备作为系统的一部分来考虑。

9.10. 应鉴定电力系统设计及分析工作中使用的工具，且应基于实验数据或运行经验论证数学模式的有效性。

9.11. 本“安全导则”第 9.2－9.10 段提出的分析内容仅是电厂安全评定的一部分。原子能机构《安全标准丛书》第 GSR Part 4（Rev.1）号《设施和活动安全评定》[18]对安全评定制定了完整的要求。

试验

9.12. 设计阶段应制定相应条款，以保证电厂在实施下述试验程序时处于安全状态：

(a) 运行前试验计划。用于证明所有系统模式（如运行状态和紧急情况）的可运行程度，证明满足设计要求，确认互为冗余的各列安全级系统之间互相独立；

(b) 运行期间的试验计划。为系统按需运行的就绪状态提供充分保证；

(c) 定期试验程序。用于证明系统的连续运行能力，并检测和识别系统或系统中部件的退化情况。

9.13. GS-G-3.5[17]第 5.114－5.134 段提供了关于核实设计充分性方法的总体要求。

9.14. 核电厂电力系统在投入运行前和进行重大改造之后的运行前试验计划的一个主要考虑因素是确认安全电力系统各序列的独立性。通常，这包括试验，以验证所有场内电力系统及其负载组能够成功运行，且不会受其他列电源的部分或全部功能故障所影响。

设计文件

9.15. 电力系统的文件应包括下列文件：

(a) 设计基准。

(b) 对整个电力系统的描述，包括：

  (i) 核电厂如何与电网连接的详细说明；

  (ii) 安全级电力系统冗余度的说明；

  (iii) 识别与辅助系统的接口。

(c) 对用于设备安装、电缆和电缆通道（包括配电盘内部的接线和部件）的隔离标准的说明。

(d) 单线图、功能控制图、原理图、连接图、端接图和系统描述。

(e) 包含电力设备及其辅助系统布置的场内电力系统布置图。

(f) 整个装置的电缆敷设图，包括电缆桥架、场内电缆沟槽和电缆管道、冗余分区、电缆及其路径的标识。

(g) 电缆桥架一览表，用于显示每段电缆桥架所包含的电缆以及桥架容积率。

(h) 电缆路径清单，用于标识每个区域电缆的连接点、电缆类型及其路径所穿越的电缆管道系统。

(i) 电力负载分析显示了电力负载的详细清单，同时对于安全级电力系统而言，可根据负载加载时序分析对电力系统中的部件容量进行计算。

(j) 电力系统和设备的运行程序和维护手册。

(k) 电力系统和设备的定期试验和维护要求。

(l) 电力系统和设备的验收试验和调试试验报告文件。

(m) 质量管理记录。

(n) 电压和频率暂态分析、短路电流和电压降计算：

  (i) 机组功率运行期间电网侧相关分析计算；

(ii) 场内配电系统分析计算；

(iii) 机组停堆期间电网侧相关分析计算；

(iv) 主发电机分析计算。

(o) 核电厂在不同运行模式下，包括发生设计基准事件、正常运行工况和在电压降低时，应对电力系统的稳态负载和电压变化情况进行分析。

(p) 在核电厂的不同运行模式下，进行暂态负载和电压分析，以描述按顺序加载到优选电源和备用电源的负载情况。

(q) 开展总线切换分析，包括电压、相角、频率以及电机再启动的影响分析，以及在总线自动切换之前、切换期间和切换之后的瞬间，对连接在总线上电机的影响。

(r) 短路电流分析计算，用以确定核电厂不同运行模式下（包括设计基准事件）电力系统的最大和最小故障电流，以此分析电力设备切除故障的能力。

(s) 保护设备的配合研究和保护设备的研究表明，在所有保护方案中都选择了正确的整定值。

(t) 备用电源的燃料储备分析。

(u) 部分或全部丧失电源的后果分析。

(v) 设备鉴定计划和分析试验报告。

(w) 电力部件技术规范书。

参 考 文 献

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

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

[3] 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）。

[4] 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）。

[5] 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）。

[6] 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）。

[7] 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）。

[8] 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）。

[9] 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）。

[10] 国际原子能机构《核电厂运行限值和条件及运行规程》，国际原子能机构《安全标准丛书》第 NS-G-2.2 号，国际原子能机构，维也纳（2000 年）。

[11] 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）。

[12] 国际原子能机构《核电厂维护、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）。

[13] 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）。

[14] 国际原子能机构《电网可靠性和与核电厂的接口》，国际原子能机构《核能丛书》第 NG-T-3.8 号，国际原子能机构，维也纳（2012 年）。

[15] 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）。

[16] 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）。

[17] 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）。

[18] 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）。

附录 I

电力系统的纵深防御

I-1. 核电厂依赖电力系统实现各种安全功能，供电可靠性对于核电厂的安全至关重要。不论每个部分的安全分级是否一样，整个电力系统都应作为一个整体来设计。

I-2. 核电厂电力系统对所有纵深防御层级都是必不可少的支持系统。在各种威胁放射性物质包容和设计扩展工况下，可靠的电力供应对控制核电厂预计运行偏差，以及对核电厂保持供电、控制和监控是十分有必要的。

I-3. 应及时处理电力系统中发生的任何故电力事件或干扰，以保证核电厂的安全功能不受影响。

I-4. 运行经验表明，丧失外部电源或者场内电力系统故障都会威胁到核电厂的安全，例如参考文献[I-1]所述的情况。

I-5. 为形成不同层次的纵深防御系统，电力系统需具备保持可靠和健稳的多重系统特征，这些特征应覆盖外部电网和场内电力系统，包括安全级电力系统和非安全级电力系统。尽管安全级电力系统需要采用更加严格的标准并实施更多的设计核实，但场内、场外电力系统对实现一个稳定可靠的安全级电力系统都有着重要意义。

I-6. 控制和监控是电力系统的支持功能，这也是主控室和辅助控制室整体功能中的一部分，同时也是各种电厂状态和电力事件发生时，电力系统运行程序中的一部分。

I-7. 表 I-1 总结了电力系统对纵深防御等级的支持特征，正如原子能机构《安全标准丛书》第 SSR-2/1（Rev.1）号《核电厂安全：设计》[I-2]所述的那样。纵深防御的等级目标必要措施涉及电厂电力系统时在安全导则中的指导条目（节）。

表 I-1. 为核电厂纵深防御提供电力供应的支持

纵深防御	目标[I-2]	基本手段[I-2]	应用于电厂电力系统	本“安全导则”中的导则（章节）
1	防止异常运行和故障	设计保守，施工操作质量高	全面的设计基础，健稳可靠的电网，健稳可靠的现场电力系统	4. 设计基准 5. 一般设计导则 6. 优选电源设计导则
2	异常运行控制及故障检测	控制系统、限制系统、保护系统和其他监视功能	强大可靠的故障排除系统，保护、电源传输能力、厂用电运行可能性的协调	5.1. 可靠性设计 6. 优选电源设计导则
3	设计基准范围内的事故控制	专设安全设施和事故程序	健稳可靠的安全电力系统，健稳可靠的现场备用交流电源	7. 电力安全系统设计导则
4	控制严重的核电厂工况，包括防止事故发展和减轻设计扩展工况的后果	补充措施与事故管理	耐用可靠的交流备用电源	7. 电力安全系统设计导则 8. 交流备用电源
5	缓解重大放射性排放的放射性后果	场外应急响应	（本“安全导则”未涵盖）	

第一级纵深防御

设计基准

I-8. 场内电力系统的设计基准是实现可靠性和健稳性的基础。设计基准说明了电压和频率的持续运行范围，所有可能导致电压和频率暂态、动态或持续变化的事件和危及电力系统可靠性的内外部危害。由于核电厂本身就是一个产生电力的场所，因此其由于各种事件所引起的电压和频率与正常值的偏离，会不同于一般工业系统事件所引起的电压和频率的偏离。

I-9. 不完整的设计基准将导致设备无法满足预期功能，而且无法通过增加冗余度或多样性得到纠正。

电网

I-10. 对于核电厂和安全级电力系统而言，电网是优选电源的组成部分。在功率运行期间，场内电力供应通常来源于发电机，它可以降低电网波动的影响。

I-11. 电网必须能提供稳定的场外电源，也就是说，它应该能够承受负载的变化和没有超出电网电压和频率允许限值范围的预计运行事件。图 I-1 展示了某个核电机组在预计运行事件期间，电压和频率波动对场内电力系统的影响。原子能机构《核能丛书》第 NG-T-3.8 号《电网可靠性及与核电厂接口》[I-3]提供了更多关于核电厂并网运行的信息。

场内电力系统

I-12. 场内电力系统是互相连接的，因此在非安全级总线上发生的电力事件将很可能会影响安全级电力系统。对于电力负载和其他设备而言，一个可靠的场内电力系统故障率应该足够低。场内电力系统的很多要求由国家电力规范所规定，但是设备鉴定（包括环境和电力）和基于电厂设计基准的设备技术规范书也是场内电力系统设计的组成部分。对场内供电系统良好的维护将减少发生故障的风险，同时对负载特性的正确判断能够减少旋转设备的过载风险。

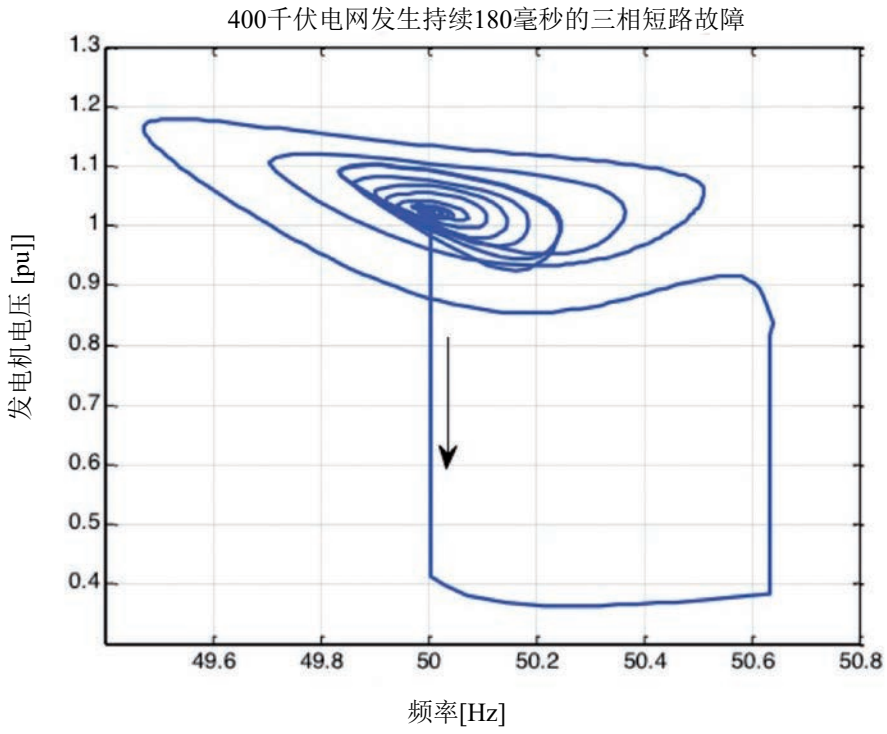


图 I-1. 基于某个电网切除故障的示例（纵坐标为场内发电机电压，横坐标为频率）。

I-13. 用于设计和核实场内系统可靠性与健稳性的确定性分析，是核电厂安全论证的一部分。

I-14. 为实现场内电力系统的健稳性和可靠性，需要对电厂的整体配置计划进行分析，包括因某些原因，如换料大修，而退出运行的电力系统。

I-15. 不能排除共因故障的可能性，由于正常工况时安全级电力系统的冗余列是连接到同一优选电源的。因此采取一些预防性措施，例如实现供电系统的多样性（在设计中已嵌入该内置功能）是十分有必要的。

I-16. 维护计划和程序应按最高标准要求，这不仅指安全级系统还包括所有的场内电力系统。监视性试验和性能试验是跟踪设备老化的一种方法。

I-17. 电厂的改造通常也会对电力系统产生影响，因此应该评定负载及其特性变化所带来的影响，这其中也包含控制系统的变化，因为这类变化可能会影响蓄电池的负载。

I-18. 在处理运行的干扰和事件中，为照明和通信供电的电力系统十分重要，尽管它们通常不会被归类于安全重要相关的系统。

第二级纵深防御

保护系统和保护配合

I-19. 为了使电力系统发生故障时所带来的影响最小化，所提供的保护配合和故障切除系统将只会切除故障设备。为了防止主保护或者故障切除设备故障，应设置后备保护。

I-20. 由于蓄电池充电器、逆变器和电动发电机通常都会在短路时贡献短路电流，因此要特别关注保护设备的配合以及可能会出现的故障电流。

I-21. 保护配合应设计为在功率运行期间和停堆期间均能正常工作。

电源切换能力

I-22. 场外电源通常采用至少两个在供电回路和位置上互相独立的电源，以尽可能减少它们同时发生故障的可能性。对于有些反应堆设计（通常指具有非能动安全特性的设计），可能会在安全分析报告中显示一个场外电源就足够了。

I-23. 在发生冷却剂丧失事故的几个周期内，其中一个场外电源应能正常供电，以维持堆芯冷却、安全壳完整性和其他重要的安全功能可用。

I-24. 通常场外电源的切换都是自动进行的，但应具备手动切换和自动切换两种方式。应研究总线切换之前、切换期间和切换之后的瞬间，对总线和电机的电压、相角和频率的影响。电机再启动也应包括在研究中。

I-25. 电源切换方案中还应包含交流不间断电源。

孤岛运行的可能性

I-26. 某些核电厂具备在甩负荷后，反应堆不用停堆或者汽轮发电机不需要停堆，具备可以孤岛运行的能力。

I-27. 孤岛运行的切换之所以复杂，原因在于反应性的反馈和降功率时的控制。经验表明，如果能够承受初始的暂态效应，运行工况能够持续数小时；这为核电厂的电源设置增加了多样性。

I-28. 为成功实现孤岛运行，在电网和核电厂之间设置断路器是非常必要的。除了发生断路器两侧同时故障或者核电厂发电机与电网同时故障的情况外，上述措施将使得我们可以从汽轮发电机或电网任一侧获得持续的电源。

第三级纵深防御

场内备用交流电源

I-29. 核电厂的安全级系统通常从优选电源（也即是电网或主发电机）或者从场内备用交流电源获得电源。

I-30. 备用交流电源的可操作性应定期进行核实。对备用交流电源启动能力的试验应不会对其长期正常运行造成负面的影响。

I-31. 对备用交流电源的启动能力和负载能力的核实通常被作为一个整体的试验和分析，以用于匹配设计基准事件。

I-32. 安全级系统负载以外的其他负载的电力供应也可能来自于安全级电力系统。这些负载在丧失场外电源以后不会自动启动，因为它们会影响安全负载的可用性。只有在确保拥有足够的容量和能力来保证非安全负载的启动和运转的时候，它们才可能会被启动。

I-33. 当发生威胁电力系统（如：与电网的连接和孤岛运行）的第一级和第二级纵深防御的外部危害时，场内的备用交流电源应能应对这类危害事件。应基于原子能机构《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》[I-4]以及原子能机构《安全标准丛书》第 NS-G-1.6 号《核电厂的抗震设计和鉴定》[I-5]来制定适当的预防措施。

安全级电力系统

I-34. 由安全级电力系统供电的各类负载对于核电厂抵御各种威胁放射性物质排放的始发事件时有着非常重要的作用。

I-35. 源于优选电源的事件会导致在所有配电系统中发生共因故障。因此在设计、建造和运行环节中准备充分的应对措施是十分有必要的。在丧失优选电源之后，如果备用交流电源分别只对一个供电列供电时，可以忽略由于电力事件所导致的共因故障，原因在于此时不存在共同的部分（尽管备用交流电源的启动顺序对共因故障比较敏感）。经验表明，设计基准的不完整性是导致共因故障的罪魁祸首，即使通过增加部件的多样性也不能降低这种风险。

I-36. 以下情况可以排除相同部件发生共因故障：

(a) 这些设备部件执行不同的功能（在一个系统中一个断路器需要闭合，而另一个断路器则需要打开）。

(b) 这些设备部件拥有不同的运行模式（两个处于并联的整流器，其中一个处于运行状态而另一个处于关闭状态）。

共因故障发生的原因通常不考虑非能动的设备例如总线、电缆和变压器上发生的电力事件。

I-37. 直流电力系统对于安全级电力系统和其他场内外电力系统的健稳性都至关重要。优选电源的一个设计原则是源于场外或发电机所导致的场外干扰不应传导到直流电力系统，因此也不能传导至不间断交流电力系统。上述原则应作为设计基准的一部分，并且可以通过设计或保护设备来实现。

I-38. 为了应对电子保护设备共因故障的风险，应对仪器仪表和控制设备使用相同的设计标准[I-6]。

I-39. 有些电力负载的设备技术规范书中会规定电力系统的电压和频率运行范围，此外认识和了解电力暂态过程及其对负载的影响也是很有必要的。同样对认识和了解机械负载也是需要的，以此决定负载的范围和不同运行模式下功率的消耗情况。这将有助于确定备用电源的容量和选择适当的保护配置。

第四级纵深防御

可备用交流电源

I-40. 为实现核电厂中执行安全功能的电源的独立性，应将全厂断电的情况也考虑在内。应考虑全厂断电情况下核电厂允许的丧失所有交流电源的持续时间，并应能在此时间内连接到一个可备用交流电源。

I-41. 有必要采取预防措施来保证可备用交流电源在发生外部危害时是可用的，并能在发生地震、海啸、洪水或者风暴的情况下期间内接入核电厂。

I-42. 可备用交流电源应该尽可能独立于其他为安全级电力系统供电的电源。

附录 I 参考文献

[I-1] 经济合作与发展组织核能机构《DIDELSYS 任务组最终报告：电力系统和电网相互作用的纵深防御》，第 NEA/CSNI/R（2009）10 号报告，经济合作与发展组织，巴黎（2009 年）。

[I-2] 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-3] 国际原子能机构《电网可靠性和与核电厂的接口》，国际原子能机构《核能丛书》第 NG-T-3.8 号，国际原子能机构，维也纳（2012 年）。

[I-4] 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）。

[I-5] 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）。

[I-6] 国际原子能机构《核电厂仪器仪表和控制系统的设计》，国际原子能机构《安全标准丛书》第 SSG-39 号，国际原子能机构，维也纳（2016 年）。

附录 II

用于设计核实的电力系统分析

II-1. 应开展分析性研究，以证明核电厂电力系统的设计裕度及健稳性。这些分析和设计能力必须通过试验或运行经验进行核实和验证。在附件 II 中描述了电力系统设计中一些正常要开展的关键的电力系统分析要素。对分析的需求适用于交流和直流电力系统，但提及的许多特殊专题仅适用于交流电力系统。

潮流分析

II-2. 潮流分析是电力系统分析的重要组成部分，因为它评价电网在正常运行工况和应急运行工况下的情况并建立边界限值。使用模拟电力系统实际稳态运行工况的计算机软件进行潮流分析，从而能够评价总线电压幅值和负载角、有功和无功潮流以及损耗。采用多种假想方案进行潮流分析有助于确保电力系统的设计充分满足性能标准。具体而言，潮流分析通常用于分析以下内容：

(a) 部件或回路加载；
(b) 总线电压幅值和负载角；
(c) 有功潮流和无功潮流；
(d) 电力系统损耗；
(e) 适宜的变压器分接头设置；
(f) 系统运行的边界限值；
(g) 总线切换方案；
(h) 回路配置优化；
(i) 假想工况下的实际电压波动；
(j) 设备技术规范书导则。

II-3. 在潮流分析中，通常采用如下总体性设计标准：

(a) 在所有考虑的运行工况下，所有总线的稳态压降在±5%额定电压范围内。

(b) 在负载加载工况下，暂态电压波动可允许>5%。

(c) 在任何假想运行工况下，电力回路不能过载。

(d) 在所有的运行工况下，无功潮流（生产、吸收和发出）均在特定的限值之内：

(i) 在特定的偶发性工况下，电能质量不下降；

(ii) 谐波含量在限值范围之内。

II-4. 在潮流分析中应特别考虑如下情况：

(a) 最大及最小负载的极端运行工况，以检查场内电源和场外电源在正常运行工况及停堆工况下的适当性。

(b) 偶发性工况。比如场外电源线路停运，场外电源的变压器和发电机停运，同时场内辅助系统（包括事故后用以缓解放射性后果的设备）处于最大或最小负载。

(c) 电厂运行参数的优化。比如变压器分接头，发电机励磁限值，无功补偿及电缆选型。

(d) 大型电动机启动。在额定电压直接启动时，大部分交流电动机的启动电流比正常满载电流大数倍。过大的启动电流会导致端电压的降落，并可能由于过低启动转矩导致电动机启动失败，导致低电压继电器的非必要动作或连接在系统中的其他投运电动机的停运。电动机启动分析有助于选择最佳的启动方式，适当的电动机设计及适当的系统设计，使电动机启动的影响降低至最小。在更换电动机后，基于电动机的特性，此项分析可能要进行再评价。

短路电流分析

II-5. 短路电流计算提供了电力系统在故障状态下的电流和电压。这些信息都是以下设计所需要的：设计一个充分的继电保护系统、确定每个电压级的断路器在最大故障电流水平下的开断要求、有足够的故障电流使保护继电器动作以核实保护设备清除故障的及时性。为核电厂电力系统的稳定

运行，应把故障的及时隔离与保护配合相结合。在任意给定时刻应考虑所有在运电源的故障贡献。核电厂中有可以为电厂电力系统的故障电流提供重要贡献的大型电机。当场内或场外电力系统有重大变化或重大改造时，应重新验证短路电流计算，并且应周期性的开展累计评价。

II-6. 故障状态可以为平衡或非平衡的并联故障或串联（导体断开）故障。故障可由对地、相间短路，或一相、多相断相引起。

II-7. 当场内或场外电力系统有重大变化或重大改造时，应更新故障分析，并且应周期性的开展累计评价（例如作为周期性安全评审的一部分）。

电力保护配合分析

II-8. 一份短路分析和/或一份保护配合分析确定了在故障发生后各时间间隔内流过电力系统的电流幅值，并且评价了系统保护设备的选型及设置，比如继电器、熔断器和断路器，以及它们保护的回路。目标是为电力变压器、开关柜、电动机控制中心、配电盘和其他电力设备提供必要的保护。这项分析在设备选择和配置工作中同样是有用的，这些是为了保证回路在过载工况或短路工况下有选择性的快速断开，从而将有必要隔离的设备范围最小化。

II-9. 保护继电器是用来快速驱动用于隔离系统故障部分的设备，防止设备的损坏，以对系统扰动最小的方式，保证电力系统不受影响部分的连续供电。当用来保护特殊设备，如安全壳贯穿件的继电器故障时，或者主保护区域内的主保护不能动作以清除故障，则在为主保护继电器的动作提供足够的时间后，后备继电器应隔离故障。保护继电器应能区分故障工况、正常运行工况和异常运行工况，并为它们提供设计所需的特定保护功能。继电保护配合计算应考虑继电器的运行特性、电厂设备的正常运行及耐受特性，并为达到电力系统的高可靠性设置最优的继电器定值。

II-10. 适用于不同的电厂部件及运行状况，保护系统应提供耐热限值、电动机堵转、负序及直流耐受限值保护、频率异常保护和不平衡运行工况保护。保护配合同样应考虑测量方式。

II-11. 保护继电器的典型分析包括：

(a) 过载保护；
(b) 过流保护；
(c) 接地故障保护；
(d) 最大负载电流下的配合；
(e) 熔断器特性的配合；
(f) 最大电动机启动电流及时间的配合；
(g) 变压器励磁涌流配合；
(h) 再加速电流的配合；
(i) 主后备的配合；
(j) 耐热能力的配合；
(k) 电动机安全堵转限值的配合。

II-12. 应特殊考虑接地故障保护，因故障电流的幅值决定于系统的接地方式：直接接地系统或低阻接地系统可能会有高水平的接地故障电流。这些高水平电流通常会要求快速的脱扣以将故障从系统中清除。接地过流及方向过流继电器是这些系统中接地故障保护的典型解决方案。高阻接地故障的检测是困难的，因为专用继电器需要测量伴有不平衡电流的接地故障电流，不平衡电流由线路相位及配置、负载不平衡引起。

电压丧失及电压退化分析

II-13. 作为上述讨论的保护方案的补充，核电厂的安全设备应配置保护，以应对在完全丧失优选电源（失压继电器）对安全总线的供电以及优选电源持续电压退化的工况，这些工况可能导致故障或导致安全重要设备的损坏。

II-14. 被认为对安全重要的设备应设置两种低电压事件的保护：

(1) 安全重要设备应配置保护以应对电压丧失事件，该事件意味着电网系统中突然大幅的电压降落。如果电压不能恢复到正常运行范围，典型的方案是允许一个正常延时动作将场内总线从电网中隔离。电压丧失将同时会触发场内备用电源的自动启动信号。

(2) 安全重要设备同时应配置保护以应对持续低电压工况达数秒并随后恢复至正常运行范围的电压退化。如果场外电源不能恢复至正常运行工况，将优先隔离此电源。

丧失发电机组、非预期系统负载、输电部件丧失或系统故障导致的发电不足，导致输电系统过载。这个保护方案对特定电厂需要额外的考虑。总体方法概述如下：

(a) 为评价场外电源及场内电力系统接口而做的电压降或负载流分析中，使用在厂一网接口节点处的最小预期电压，以证明电厂部件在正常运行、预计运行事件和事故工况下的启动和运行有足够的电压。

(b) 电压和时间延迟定值由对所有场内系统配电级中安全重要负载的运行电压要求分析确定。

(c) 基于下述情况选择延迟时间：

(i) 允许的延迟时间包括裕度，不超过在事故分析中假定的最大延迟时间；

(ii) 延迟时间应躲过短时电网扰动的影响，维持场外电源的可用性；

(iii) 所有配电系统级中的电压退化状态的持续时间不应导致安全级系统或部件的故障。

II-15. 一个典型的电压退化保护方案包含两个单独的延时继电器来应对如下工况：

(a) 第一个延迟时间应有效建立持续的电压退化状态（例如比由电动机启动引起的暂态时间）。在这个延迟之后，控制室的警报提示控制室的运行人员电压退化状态。随后事故信号将安全配电系统立即从场外电力系统中隔离。

(b) 第二个延迟时间应比可能会损坏永久连接的安全负载的电压退化维持时间短。在这个延迟之后，如果没有恢复足够的电压，将自动或手动（运行人员操作）地把安全配电系统从场外电力系统中隔离。

暂态稳定分析

II-16. 由于自身特性，电力系统将持续的经历扰动。这些扰动可能包括生产的损失、雷击导致的短路或其他故障状态、大负载的突然变化、或这些事件的组合。这些扰动可能导致电力系统配置的改变。为确定在这样大的扰动之后系统能否保持稳定，电力系统的暂态稳定分析是必要的。一个既定的场外电力系统在不同故障状态下的临界故障清除时间是不同的。这个临界故障清除时间 [1] 可在核电厂安全分析报告中确定和描述。电力系统在经受一个严重的大扰动之后的恢复对电厂的可靠及安全运行是重要的。典型的实践是，系统应设计并运行在这样的一个方式，在此方式下，特定数量的可信偶发事件不会导致负载供电质量和连续性的丧失。这要求对系统动态特性的精确计算，包括旋转机械的机电动态特性、发电机控制、无功补偿器、负载、保护系统和其他控制。系统健稳性程度是核电厂周边电网系统运行特性的一个重要因素。需要尽快地将导致电力系统丧失同步的电网扰动隔离，以避免设备的损害或系统的失稳。

II-17. 影响暂态稳定的参数包括：

(a) 同步电机的参数；
(b) 主变压器的阻抗；
(c) 汽轮发电机的转动惯量；
(d) 输电线路的参数；
(e) 断路器和继电器特性；
(f) 系统布置；
(g) 励磁系统、电力系统稳定器和发电机调速器特性；
(h) 系统接地方式；
(i) 系统控制，比如断路器的自动重合闸、单极开关、甩负荷和系统惯量。

II-18. 典型的暂态稳定分析包括：

(a) 根据发电机稳态、暂态及次暂态参数的发电机建模；
(b) 三相故障或线路接地故障的暂态仿真；

[1] “临界故障清除时间”是系统保持稳定的最大故障持续时间。

(c) 电动机及电动机负载转矩、滑差、电流及加速曲线的建模；

(d) 模拟发电机启动和电动机启动；

(e) 断路器脱扣和闭合、开关的打开和闭合、和基于设定值的继电器动作的建模；

(f) 在假定扰动后，发电机和电动机速度、电流、电压和功率曲线的绘制。

II-19. 利用计算机开展暂态稳定分析，可以优化断路器动作特性、同步机械特性和系统连接。

雷电防护系统和系统接地分析

II-20. 雷电防护系统是一个用来保护结构不因雷击损坏的系统，它通过截获这些雷击并将它们极高的电压电流安全地散入大地。雷击引起的电压会非常快速地上升，通常在百万分之几秒内就会达到峰值。为了防止设备损坏和人员伤害，雷击能量应通过一低阻抗路径快速返回大地。

II-21. 雷电防护系统的大部分外部系统包括接闪器、引下导体和接地端子，包括与电厂接地网相连接的避雷针，金属导体和接地极网络，为雷击提供一个低阻抗路径。雷电防护的内部系统包括雷电等电位联接、外部系统的电力绝缘和浪涌保护器。

II-22. 在任何电力生产电厂中，总体上有四种概念上可区分的不同接地系统，但没必要在物理上区分：为人身安全、雷电接地、电力系统和仪器仪表和控制系统，包括信号的接地系统。所有的接地系统均接至同一接地网络。

II-23. 国际技术标准通常建议大型电厂的接地电阻应小于或等于 1Ω。

II-24. 影响雷电防护的因素包括：

(a) 电厂接地网设计；

(b) 土壤电阻率；

(c) 接地极设计（如是否铜包裹、镀其他贵金属材料和规范及深度）。

II-25. 设计完善的电厂接地系统对电厂设备防护接地故障和雷击至关重要。

电磁兼容分析

II-26. 工业环境条件下的电磁兼容性有国际技术标准。这些国际技术标准可以作为核电厂电磁兼容性要求的基础。必要时，必须补充这些标准，以涵盖在运核电厂部件环境条件下的电磁兼容要求，这可能会有更严苛的要求。这种分析的结果将包括带频谱的包络发射水平和带频谱的包络磁化率水平。

定义

以下定义适用于本“安全导则”。原子能机构安全术语中提供了进一步的定义：核安全和辐射防护用术语（2007 年版），国际原子能机构，维也纳（2007 年）：
http://www-pub.iaea.org/books/iaea books/7648/iaea-safety-glossary

符号“ⓘ”表示信息注释。

备用交流电源。在安全电力系统（电厂停电）和其他设计扩展工况下，在完全丧失所有非电池电源的情况下，为电厂供电而保留的电源。

受控状态。在预计运行事件或事故工况下的电厂状态，可确保基本安全功能，并可维持足够的时间以达到安全状态。

优选电源。从传输系统到安全级电力系统的电源。

ⓘ 部分优选电源不属于安全级。（见图 2）

电厂状态。在预计运行事件或事故工况下，反应堆处于次临界状态，基本安全功能可以得到保证并长期保持稳定。[1]

电厂停电。电厂条件下，场外电源、主发电机和备用交流电源的所有交流电完全丧失，这些交流电源对重要和非重要开关设备总线的安全至关重要。只要电池能为负载供电，直流电源和不间断交流电源就可以使用。提供备用交流电源。

[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）。

参与起草和审订人员

Auvinen, K.	瑞典福什马克核电厂
Diaz, E.	阿根廷国家原子能委员会
Dubois, A.	法国辐射防护与核安全研究所
Duchac, A.	国际原子能机构
Fredlund, L.	瑞典 Ringhals AB
Frey, W.	德国装置与反应堆安全公司
Giannelli, I.-A.	意大利国家电力公司工程和研究处
Givaudan, B.	法国电力公司
Goodney, D.	美国联合能源公司
Johnson, G.	国际原子能机构
Jordan, R.	美国西屋电力公司
Kiger, C.	美国分析测量服务公司
Kim, B.-Y.	韩国核安全研究所
Knutsson, M.	瑞典 Ringhals AB
Krastev, E.	保加利亚科兹洛杜伊核电厂
Lamell, P.	瑞典福什马克核电厂
Lindner, L.	德国高等科学技术与经济商业学院
Lochthofen, A.	德国装置与反应堆安全公司
Matharu, G.	美国核管制委员会
Mathew, R.	美国核管制委员会
Mauhin, B.	比利时特克贝尔工程公司、法国天然气苏伊士集团
Meiss, S.	德国联邦辐射防护办公室

Padin, C.	阿根廷国家原子能委员会
Rogers, A.	顾问（加拿大）
Sarwar, T.	巴基斯坦原子能委员会
Schnuerer, G.	德国高等科学技术与经济商业学院
Sobott, O.	德国阿海珐
Yonezawa, T.	日本能源公司
Zhu, O.-P.	韩国核安全研究所

IAEA
国 际 原 子 能 机 构

No. 27

当 地 订 购

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

定价出版物订单

请联系您当地的首选供应商或我们的主要经销商：

Eurospan
1 Bedford Row
London WC1R 4BU
United Kingdom

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

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

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

定价和未定价出版物的订单均可直接发送至：

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

通 过 国 际 标 准 促 进 安 全

国际原子能机构
维也纳