IAEA
国际原子能机构
安全标准
丛书

核动力厂安全重要仪表控制系统

安全导则

No. NS-G-1.3

IAEA
国际原子能机构

该出版物已被第 SSG-39 号取代。

国际原子能机构安全相关出版物

国际原子能机构（原子能机构）安全标准

根据原子能机构《规约》第三条的规定，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的危险的安全标准，并规定适用这些标准。

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以及一般安全（即涉及上述所有安全领域）。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。

安全标准按照其涵盖范围编码：核安全（NS）、辐射安全（RS）、运输安全（TS）、废物安全（WS）和一般安全（GS）。

有关原子能机构安全标准计划的信息可访问以下原子能机构因特网网址：

http://www-ns.iaea.org/standards/

该网址提供已出版安全标准和安全标准草案的英文文本。也提供以阿拉伯文、中文、法文、俄文和西班牙文印发的安全标准文本、原子能机构安全术语表以及正在制订中的安全标准状况报告。欲求详细信息，请与原子能机构联系（P.O. Box 100, A-1400 Vienna, Austria）。

敬请原子能机构安全标准的所有用户将其使用方面的经验（例如作为国家监管、安全评审和培训班课程的基础）通知原子能机构，以确保原子能机构安全标准继续满足用户需求。资料可以通过原子能机构因特网网址提供或按上述地址邮寄或通过电子邮件发至 Official.Mail@iaea.org。

其他安全相关出版物

原子能机构规定适用这些标准，并按照原子能机构《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各成员国的居间人。

核活动的安全和防护报告以其他出版物丛书的形式特别是以**安全报告丛书**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。原子能机构其他安全相关出版物丛书是**安全标准丛书适用规定、放射学评定报告丛书**和**国际核安全咨询组丛书**。原子能机构还印发放射性事故报告和其他特别出版物。

安全相关出版物还以**技术报告丛书**、**国际原子能机构技术文件丛书**、**培训班丛书**、**国际原子能机构服务丛书**的形式以及作为**实用辐射安全手册**和**实用辐射技术手册**印发。保安相关出版物则以**国际原子能机构核保安丛书**的形式印发。

核动力厂安全重要仪表控制系统

该出版物已被第 SSG-39 号取代。

下述国家是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
阿根廷
亚美尼亚
澳大利亚
奥地利
阿塞拜疆
孟加拉国
白俄罗斯
比利时
贝宁
玻利维亚
波斯尼亚和黑塞哥维那
博茨瓦纳
巴西
保加利亚
布基纳法索
喀麦隆
加拿大
中非共和国
智利
中国
哥伦比亚
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
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
埃塞俄比亚
芬兰
法国
加蓬
格鲁吉亚
德国
加纳
希腊
危地马拉
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
拉脱维亚
黎巴嫩
利比里亚
阿拉伯利比亚民众国
列支敦士登
立陶宛
卢森堡
马达加斯加
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
摩洛哥
缅甸
纳米比亚
荷兰
新西兰
尼加拉瓜
尼日尔
尼日利亚
挪威
巴基斯坦
巴拿马
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
沙特阿拉伯
塞内加尔
塞尔维亚和黑山
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
前南斯拉夫马其顿共和国
突尼斯
土耳其
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
委内瑞拉
越南
也门
赞比亚
津巴布韦

原子能机构《规约》于 1956 年 10 月 23 日在纽约联合国总部召开的国际原子能机构规约会议上通过，于 1957 年 7 月 29 日生效。原子能机构总部设在维也纳。原子能机构的主要目标是“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 NS-G-1.3 号

核动力厂安全重要仪表控制系统

安 全 导 则

国 际 原 子 能 机 构
维也纳，2005 年

该出版物已被第 SSG-39 号取代。

版 权 说 明

Sales and Promotion Unit, Publishing Section
International Atomic Energy Agency
Wagramer Strasse 5
P.O. Box 100
A-1400 Vienna
Austria
传真：+43 1 2600 29302
电话：+43 1 2600 22417
网址：http://www.iaea.org/books

国际原子能机构印制
2005 年 8 月 • 奥地利

核动力厂安全重要仪表控制系统

国际原子能机构，奥地利，2005年8月
STI/PUB/1116
ISBN 92-0-513905-X
ISSN 1020-5853

序

总 干 事

穆罕默德·埃尔巴拉迪

国际原子能机构《规约》授权原子能机构制定旨在保护健康及尽量减少对生命与财产的危险的安全标准。原子能机构必须使这些标准适用于其本身的工作，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这些标准。原子能机构对这样的一整套安全标准定期进行审查并协助实施这些安全标准已经成为全球安全体制的一个关键要素。

在 20 世纪 90 年代中期，原子能机构开始对其安全标准计划进行大检查，包括修改监督委员会的结构和确定旨在更新整套标准的系统方案。已经形成的新标准具有高水准并且反映成员国的最佳实践。在安全标准委员会的协助下，原子能机构正在努力促进全球对其安全标准的认可和使用。

诚然，只有对这些安全标准在实践中加以适当应用，它们才会是有效的。原子能机构的安全服务——其范围包括工程安全、运行安全、辐射安全、运输安全和废物安全，直至监管事项和组织中的安全文化——协助成员国适用安全标准和评价其有效性。这些安全服务能够有助于共享真知灼见，因此，我继续促请所有成员国都能利用这些服务。

监管核安全和辐射安全是一项国家责任。目前，许多成员国已经决定采用原子能机构的安全标准，以便在其国家条例中使用。对于各种国际安全公约缔约国而言，原子能机构的安全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。世界各地的设计者、制造者和营运者也适用这些标准，以加强电力生产、医学、工业、农业、研究和教育领域的核安全和辐射安全。

原子能机构认真看待世界各地用户和监管者正在经历的挑战，这就是确保世界范围内的核材料和辐射源在使用中的高水平安全。必须以安全的方式管理核材料和辐射源的持续利用以造福于全人类，原子能机构安全标准的目的正是要促进实现这一目标。

编 者 按

如果列入附录，该附录可被视为标准的一个不可分割的组成部分并具有与主文本相同的地位。如果列入附件、脚注和文献目录，它们可被用来为用户提供可能是有用的补充信息或实例。

英文文本系权威性文本。

援引其他组织的标准不应被解释为国际原子能机构认可这些标准。

目 录

1. 引　言

背 景

1.1.　本安全导则是根据IAEA建立核动力厂安全标准的计划编写的。它对为确保核动力厂安全而制定的设计要求的安全标准丛书No.NS-R-1：《核动力厂安全：设计》[1]（设计要求）作了补充。本安全导则对安全重要仪表控制（I&C）系统应该何满足这些要求作了描述。

1.2.　本出版物是先前两个安全导则：安全丛书No.50-SG-D3和No.50-SG-D8的修订和结合，后两者由该新安全导则取代。

1.3.　修订中考虑了自这两个先前的安全导则分别于1980年和1984年出版以来，安全重要仪表控制系统方面的发展。修订中作出的主要变更，由以下诸项所引起：

— 在本安全导则中考虑了安全重要的基于计算机的仪表控制系统的应用中的发展。
— 在对安全丛书No.50-SG-D3和No.50-SG-D8的本次修订中，注重对安全重要的所有仪表控制系统问题的处理。导则是根据文献[1]中规定的要求和准则加以组织和介绍的。
— 对本安全导则的设想是，它要连同和根据设计要求[1]有关软件[2]和有关质量保证（参考文献[3]、安全导则Q3和Q10）的相关领域中的安全导则来读。
— 对安全重要的仪表控制系统的分级提出了指导意见，这些意见是从其他的一些国际标准中汲取的。

目 的

1.4.　制定本安全导则的目的是对核动力厂中的安全重要仪表控制系统的设计提供指导。这些系统包括，从配置给机械系统的传感器到驱动设备、操纵员接口和辅助设备的所有仪表控制部件。

1.5.　本安全导则主要涉及安全重要的那些仪表控制系统的设计要求。它充分地阐述参考文献[1]中有关安全重要仪表控制系统的那些章节。

1.6. 本出版物主要供核动力厂的设计单位使用，也可供核动力厂营运单位以及核安全监管部门使用。

范 围

1.7. 本安全导则提供广泛适用于多种核动力厂的、有关安全重要仪表控制系统的一般指导。因具体核动力厂类型而异的安全运行方面更详细的要求和限制，应该作为其设计程序的一部分加以确定。本安全导则提供的指导着重于值得特别注意的安全重要系统的设计原则，并且应被用于新的仪表控制系统的设计和现有系统的现代化。在按系统对安全重要性进行系统分级的方法的基础上，提供有关应该如何应用设计原则的指导。

1.8. 根据参考文献[1]中给出的定义，安全重要的仪表控制系统是作为一个安全组的组成部分的仪表控制系统和其失效或故障可能导致厂区人员或公众成员受到辐射照射的仪表控制系统。这样的系统的实例有：

— 反应堆保护系统，
— 反应堆控制系统，
— 用于监测和控制反应堆正常冷却的系统，
— 用于监测和控制应急电源的系统，
— 安全壳隔离系统。

1.9. IAEA的技术报告丛书No.387[4]给出本安全导则所讨论的系统的概念和实例的概述，并可为一些使用者提供有益的背景材料。

结 构

1.10. 本出版物按参考文献[1]的要求和准则加以组织并对有关安全重要仪表控制系统提供指导。

1.11. 第2章讨论本安全导则范围内仪表控制功能和系统的确定，以及如何进一步对它们进行安全和安全有关功能和系统的分级。第3章介绍安全重要仪表控制系统的设计基准的确定。第4章提供有关安全重要仪表控制系统的设计指导。它包括适用于所有安全重要仪表控制系统的指导，以及只适用于安全系统的指导。指导对这两类系统的适用性在正文中明确并已在表I中总结。第5章提供专门针对一定的仪表控制系统，即保护系统、电源和数字计算机系统的进一步的指导。有关这些系统的指导包括第4章中提供的一般指导和第5章中提供的具体指导。

第6章阐述第4章中给出的有关人机接口的指导。第7章阐述第4章给出的有关确保质量的设计程序的指导。

1.12. 第4、5、6和7章中的讨论，是为描述每个主题对安全和对设计要求的关系而特地安排的。提供了对每个主题的具体指导。

2. 安全重要的仪表控制系统

2.1. 设计要求规定，首先确定作为安全重要物项的所有仪表控制系统和部件（包括仪表控制系统所用的软件），然后依据它们在安全方面的功能和重要性加以分级（参考文献[1]，第5.1段）。

仪表控制系统的确定

2.2. 安全重要的仪表控制系统的确定是根据下述两个基础：必要的安全功能的确定和实施这些功能的某些组合的系统的确定。确定安全重要系统的典型过程在本章中讨论。

核动力厂安全重要功能

2.3. 有多种重要功能必须加以实施以确保一个核动力厂的安全和高效的运行以及它们可能涉及仪表控制系统的使用。为确保安全而需要完成的下述主要安全功能已在参考文献[1]第4.6段中确定：

— 反应性控制，
— 堆芯热量排出，和
— 放射性物质约束和运行排放控制，以及事故释放限制。

2.4. 为确定在一个假设始发事件（PIE）发生后完成这些安全功能所需要的系统、结构和部件，应该遵循一种系统化的方法。

2.5. 下面将展开和详细说明这些主要的安全功能，以便更充分地描述为确保安全需要完成的那些功能。这套扩大的功能包括，为避免或防止事故工况所需要完成的功能，以及为减轻事故工况的后果所需要完成的功能。完成这些功能，要酌情使用为正常运行提供的，为防止预计运行事件导致事故工况提供的，或为减轻事故工况后果提供的构筑物、系统和部件。

反应性控制的安全功能有：

— 保证正常反应性控制在安全限值范围内；
— 防止发生不可接受的反应性瞬态；
— 必须为防止预计运行事件导致设计基准事故工况停闭反应堆；
— 为减轻事故工况后果停闭反应堆；和
— 在一切停堆动作完成后，将反应堆保持在安全停堆工况。

从堆芯排出热量的安全功能有：

— 在功率运行时，排出堆芯产生的热；
— 在适当的运行状态和设计基准事故工况下，且反应堆冷却剂边界未受损伤时，排出余热；
— 在正常运行状态下和在任何预计始发事件发生后，为堆芯冷却保持足够的冷却剂装量；
— 在反应堆冷却剂压力边界故障发生后，从堆芯排出热量以限制燃料损伤；
— 把热量从用于堆芯排热的中间热阱转移到最终热阱。

放射性物质约束和运行排放控制以及事故释放限制的安全功能有：

— 保持反应堆堆芯中的燃料包壳的完整性；
— 保持反应堆冷却剂压力边界的完整性；
— 限制放射性物质的释放，并将公众和人员的辐射照射降到最低限度。

2.6. 以上所述安全上重要的功能应该由专设系统来完成，其中一些是仪表控制系统。就仪表控制系统而言，典型的主要的安全重要功能包括：

— 保护功能，
— 控制功能，
— 监测和显示功能，
— 试验功能。

2.7. 此外，还有一些安全重要的服务功能。应完成这些服务功能以支持主要功能。这种服务功能的实例，包括支持完成主要功能的系统的电力、气压动力或液压动力的供应；数据通信；以及监测和试验功能。

2.8. 安全重要的主要仪表控制功能可被表征如下：

保护功能

2.9. 保护功能提供一条对付核动力厂其他系统中故障的防线。从在发生严重故障时保护人员和公众的意义上说，保护功能属于安全功能中最重要者之列并且直接与核安全有关。

控制功能

2.10. 控制功能提供的保证是，核动力厂在正常和异常工况下得到控制，并保持在其运行包络线内。控制功能还能够减轻核动力厂瞬态或假设始发事件的效应，从而通过把对保护功能的需求降到最低限度对核安全作出贡献。

监测和显示功能

2.11. 监测和显示功能提供核动力厂与运行人员和维护人员之间的接口。这些功能在安全上是重要的，因为它们能够使核动力厂人员阻止瞬态，并且把核动力厂保持在安全运行的包络线内。

试验功能

2.12. 试验功能确保安全重要的其他功能的可用性和有效性，并确认它们尚未降低。

安全重要仪表控制系统的实例

2.13. 按照相关的核动力厂安全重要功能编制的下列清单，提供了安全重要仪表控制系统的实例。

2.14. 用来完成与反应性控制有关功能的仪表控制系统包括：

— 提供停堆（事故保护停堆）触发的系统；
— 用来监测核动力厂参数，或将其保持在下述范围的系统：
  - 安全上重要的运行限值（例如冷却剂温度控制系统）
  - 在安全分析中被假定为初始条件的限值(例如反应堆功率限值控制系统）；
— 其失常或故障可能要求某些系统提供保护功能的系统，例如反应性控制系统；

— 对维持安全停堆工况执行重要功能的系统，例如计算临界裕度的系统；
— 在防止、终止或缓解预计运行事件或设计基准事故工况方面完成重要功能的系统，例如反应堆降功率系统；
— 专门作为提供保护功能的系统的多样化后备而提供的系统，例如用来缓解未能紧急停堆的预期瞬态的系统，或考虑可能设计错误的系统。

2.15. 为完成与堆芯热量排出有关的功能而提供的仪表控制系统包括：

— 某些系统，例如反应堆保护系统和专设安全设施的驱动系统，这些系统能够自动地启动一些系统的运行，以确保作为预计运行事件的结果而规定的设计限值不被超过，监测设计基准事故工况和减轻其后果，或取消控制系统的不安全动作；和
— 用来监测或控制核动力厂环境条件的系统，该条件对安全和可居留性重要的核动力厂设备的正确运行是必不可少的。

2.16. 为完成放射性物质约束和运行排放控制以及事故释放限制诸项功能而提供的系统包括：

— 其失常或故障可能引起放射性物质向环境的释放，且未配备安全系统的系统，例如那些用来控制废物管理的乏燃料冷却的系统；
— 用来探测和测量反应堆冷却剂系统泄漏的系统；
— 用来监测或控制那些可能对安全有害影响的自然现象或人为现象的系统，例如地震监测器；和
— 用来事故监测和评定的系统，例如必要时监测和记录安全壳压力、安全壳放射性活度、反应堆堆芯冷却、放射性向环境的释放和气象数据的系统。

2.17. 为支持完成安全重要的其他功能而提供的仪表控制系统包括：

— 向安全重要的多重仪表控制系统提供支持性功能的系统，例如在系统之间和在系统的部件之间传递信号的数字数据通信系统；
— 用来监测安全系统状态的系统，例如用来监测安全通道故障和安全系统的管道、阀或泵中缺陷的系统；
— 在安全系统运行中可能使用的系统，例如用来试验保护系统的系统；
— 安全重要的其他特定的仪表控制系统，例如用于通信、火灾探测和灭火，以及出入口控制的系统。

安全重要的仪表控制系统的类型

2.18. 根据确定的要求执行的安全功能，建立了完成安全重要的功能的仪表控制系统。通常采用下列类型的系统。

保护系统

2.19. 保护系统是安全重要的仪表控制系统中的一种特别重要的类型。设计要求（参考文献[1]，第6.80段）规定：“保护系统必须被设计成这样：

(1) 自动地触发有关系统的动作，必要时包括自动触发反应堆停堆系统动作，以保证在发生预计运行事件时运行工况不超过规定的设计限值；
(2) 探测设计基准事故并且启动将这种事故后果限制在设计基准内所必需系统的运行；
(3) 能够抑制控制系统的不安全动作。”

2.20. 应该指出，“保护系统”这个术语在有些成员国中是不使用的，而且在完成这些保护功能的那个系统或那些系统的详细结构中存在某种可以接受的变化。例如，在一些成员国中使用一些独立的专用安全系统的仪表控制子系统，而不是一个通常的保护系统来完成监测和启动前面描述的安全系统。在这种场合，本安全导则的指导意见用于那些有关的仪表控制系统组。

联锁系统

2.21. 联锁系统用来防止不安全工况或不安全运行、保护人员和预防危险。联锁装置也用来防止发生可能导致或增加对核动力厂的危害或损害的动作，并且通常不触发旨在纠正工况的动作。联锁功能可以是能动功能，也可以是非能动功能。能动功能维持一种持续的行动，防止一种工况发展。非能动功能防止一种动作。

2.22. 联锁功能可以由机械手段或行政的或电的方法来提供。机械的和行政的联锁功能不属于本安全导则范围。

控制系统

2.23. 控制系统包含所有用于自动和手动控制核动力厂参数的设备和部件，从过程传感器的连接件到对改变被控参数值的实际工艺过程有直接影响的驱动设备。

2.24. 控制系统把过程变量维持在核动力厂安全分析中所假定的限值范围内。为使在安全分析中所作的那些假设有效，某些参数必须维持在预计运行事件或设计基准事故的初始条件规定的限值范围内。所论参数保持在这些规定限值范围内的概率，取决于维持这些参数的控制系统的可靠性，还取决于监测这些参数并且把任何偏差通知给操纵员以便其采取纠正措施的仪表系统的可靠性。

2.25. 控制系统的故障可能强加给保护系统一个要它动作的要求；就是说，一个控制系统的故障可能构成一个预计运行事件。自动控制系统中的任何故障，都将自动地触发一次向手动控制的转换。导致手动控制被自动触发的自动控制系统的故障应向操纵员发出注意控制状况改变的报警。

信息系统

2.26. 信息系统包含多种设备和部件，例如传感器；把传感器发出的信号转变为适合于显示或记录的信号设备；声音发送器；指示灯；测量仪表；可视装置；记录仪；打印机；以及固态显示装置。

2.27. 信息系统将系统或核动力厂的安全状况通知电厂操纵员。操纵员根据了解到的安全状态，可以确定维持核动力厂安全所需要的手动操作。在正常运行中，操纵员借助装备在主控制室中的显示器和报警器或可视显示装置，连续地监视核动力厂的安全状况。

2.28. 在事故工况下，信息系统还向厂区和厂外的安全专家通知核动力厂的安全状态。在正常运行、预计运行事件、设计基准事故和严重事故中，主控室对操纵员而言，是核动力厂的信息和驱动中心。在紧急情况下，主控室还可以用做初始阶段指导厂外活动活动的主要中心。

2.29. 在紧急情况下，很多专家可能被召到厂区。这些专家要进入不同的区域场所（技术支持中心；应急运行中心；或应急响应中心），这些区域场所应该配备信息系统（可视装置；运行程序；系统手册），以便使这些专家能够执行其使命。信息系统可以包括与被允许进入主控室中的那些专家进行直接通信的线路。

2.30. 信息系统记录或打印安全重要的过程变量的短期和长期趋势，供立即或随后的分析中使用，或作为运行组织内的报告和向外部主管部门的报告。对模拟过程变量和二进制信号，记录或打印输出要保存在主控室中（并且可能贮存在计算机硬盘中以便查询），使有关核动力厂的实绩和性能的信息按时间顺序编排供人们使用。这种信息是必要的：(1)值班操纵员备用信息（给出短期和长

期趋势），(2)向核动力厂管理者提供总的运行信息，(3)运行和事故的长期分析所需要的信息。

限制系统

2.31. 限制系统包含专门为降低预计运行事件的频率而配备的所有设备和部件，如果被证明是正确的则限制系统在核动力厂安全分析中是可信的。例如联锁控制棒和降低反应堆功率有时便是由限制系统完成的。

2.32. 一些成员国在其条例和设计中明确地承认限制系统。在另一些成员国中，限制功能可能被指定给正常的控制系统。

降低风险系统

2.33. 降低风险系统包括专门为降低多故障序列事件中堆芯损坏概率，以及为阻止初因事件（例如通过驱动一个另外的专用停堆系统或启动另一个应急给水系统），而不是减轻这种事件的后果（例如供在核动力厂断电时使用的各种发电机）而提供的所有设备和部件。

2.34. 在一些成员国中，风险降低系统在条例和设计中被明确地承认。在另一些成员国中，风险降低功能可能被指定给正常的控制系统。

2.35. 应该指出，在一个系统中，典型的仪表控制功能很少是互不相容的；例如，控制系统往往是信息系统所用数据的来源，而联锁系统很少包含几个独立系统。

仪表控制系统的分级

2.36. 在第2.13段到第2.35段中，安全重要的仪表控制系统是与设计要求[1]中确定的那些主要安全功能相关的。不过，这样并不意味着按安全重要性对这些仪表控制系统进行分级；一个特定的仪表控制系统可能涉及一种或多种主要安全功能的完成。但是，这些仪表控制系统的安全重要性的分级是必要的，并且是通过安全重要的仪表控制系统的分级完成的。这种分级是参考文献[2]第5.1段所要求的。

2.37. 具体地说，设计要求（参考文献[1]，第5.2段）规定，构筑物、系统或部件的安全重要性的分级方法主要基于确定论方法，并酌情由概率论方法和工程判断加以补充；且要考虑下列诸因素：

— 要完成的安全功能；
— 仪表控制系统故障的后果；
— 要求该仪表控制系统完成一种安全功能的概率；和
— 一个预计运行事件发生后，要求该仪表控制系统开始运行的那个时刻或时段。

2.38. 采用这种分级方法，除如参考文献[1]所规定的那样考虑上述因素外，在确定仪表控制系统的级别时还应考虑下述因素。在下述因素中提出了一些应选择的判据，以便为正被分级的仪表控制系统在安全上的相对重要性，提供一个定量的和（或）定性的指标：

— 预计运行事件的概率，以及在所提供的这个仪表控制系统发生故障的情况下，这些事件的后果的潜在严重性（例如高、中或低概率，以及高、中或低后果（例如放射性后果））；
— 仪表控制系统本身引起一个预计运行事件的可能性（即该仪表控制系统的故障模式），在安全系统或在本安全导则涵盖的其他仪表控制系统中为这样一个预计运行事件所采取的措施（即探测仪表控制系统故障的措施），以及这样一个预计运行事件的概率和后果（即故障频率和放射性后果）的综合影响；
— 一旦安全功能被触发，该仪表控制系统要求保持运行状态的时段长度（例如长达12小时，超过12小时）；
— 能采取替代措施的及时性和可靠性（例如立即采取/低可靠性，超过30分钟采取/高可靠性）；
— 能探测和补救该仪表控制系统中任何故障的及时性（例如长达12小时，超过12小时）和可靠性。

2.39. 一旦仪表控制系统中每个系统考虑了这些因素中的每个因素，则应该就所述的这个仪表控制系统的级别做出决定。

2.40. 仪表控制系统大致分为两类：一类用于完成安全重要的功能，另一类用于完成安全不重要的功能（见图1）。安全重要的仪表控制系统，正如本章前面部分所讨论的，是用于完成安全重要的主要功能的系统。在“安全重要仪表控制系统”的类别中，再分成如下的两个主要部分：

— “安全级仪表控制系统”（可简称安全系统）是这样的安全重要的仪表控制系统：它们完成设计要求中确定的那些主要安全功能；即它们保证反应堆的安全停堆或从堆芯排除余热，或限制预计运行事件和设计基准事故的后果；

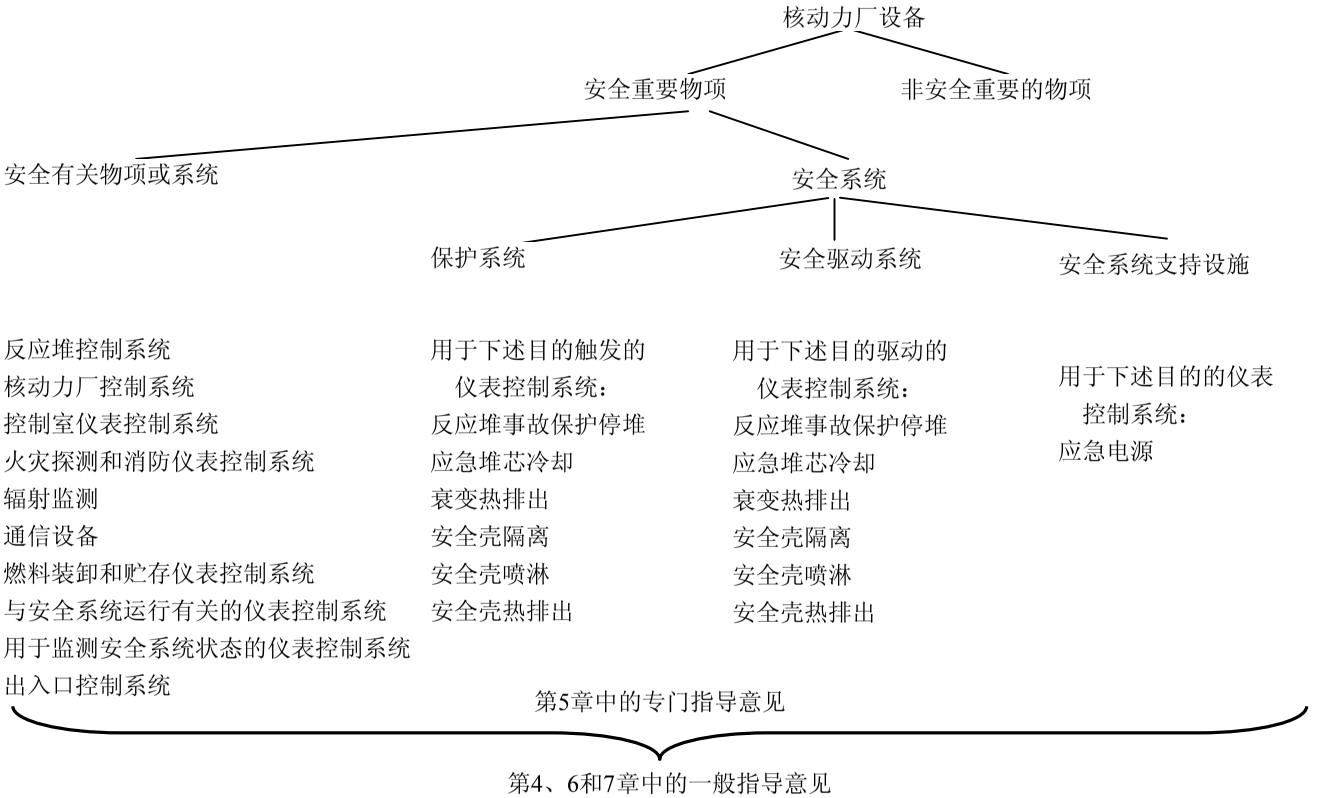

图1. 安全重要的仪表控制系统实例。（给出的说明实例。一些系统被列入某一栏，但它们也可能属于另一栏，例如控制室仪表控制系统。）

— “安全有关仪表控制系统”是这样的安全重要仪表控制系统：它们完成不是由安全级仪表控制系统完成的安全重要的其他功能。

2.41. 安全级仪表控制系统包括用来提供保护功能的那些系统。这些功能一般由一个被称为反应堆保护系统的系统完成，或由反应堆停堆系统、应急堆芯冷却系统和安全壳隔离系统等专用安全系统的仪表控制分系统完成。安全级仪表控制系统还可完成事故后监测功能和支持功能（例如，为保护系统或专用安全系统提供支持和重要的数据通信系统）。

2.42. 安全有关仪表控制系统的典型实例包括控制系统、监测和显示系统，以及不分级为安全系统、限制系统或风险降低系统的那些系统。

2.43. 应保证，必要的服务系统（电的、气动的或液压的动力供应系统，以及润滑系统）的分级与它们所支持的那些安全功能的分级相适应。

2.44. 用来完成安全重要功能的所有仪表控制系统和设备，都应该与不同级别的系统和设备有适当的设计接口，以确保在一个较低级别的系统的任何故障不扩大到在一个较高级别的系统。防止故障扩大的功能和设备属于那个较高级别的系统。

2.45. 所有仪表控制系统和设备都应该这样设计、建造和维护：它们的技术要求、验证与确认、质量保证、质量控制和可靠性是与它们的级别相适应的。

3. 设计基准

3.1. 一个核动力厂的设计基准按所规定的辐射防护要求，规定该核动力厂应付特定范围的运行状态和设计基准事故工况所需要的能力。设计基准一般包括：正常运行技术规格；由假设始发事件引起的那些工况；重要假定；以及在某些场合的具体分析方法。

3.2. 核动力厂的性能也应针对该核动力厂未设计到的一些事件，即超出设计基准的（或严重的）事故工况。安全重要的仪表控制系统在这种事件中起重要作用，这是因为可能要求这种系统提供有关核动力厂状态的重要信息，或在有关的机械设备系统的设计范围以外运行。

3.3. 设计要求确定影响安全重要的仪表控制系统设计基准的若干种活动。这些活动将在下面讨论。（有关对仪表控制系统的这些要求的指导意见，将在本安全导则的第4、5和6章中提供。）

核动力厂状态类别

3.4. ‘设计要求’规定，要确定核动力厂状态，并按其发生的概率把这些状态分组归入数目有限的类别中（参考文献[1]，第5.7段）。这些类别一般涵盖正常运行、预计运行事件、设计基准事故、以及严重事故。

运行状态

3.5. ‘设计要求’规定（参考文献[1]，第5.25段），在设计中要考虑反应堆处在起动、换料和维护等低功率和停堆状态（此时一些仪表控制安全系统的可用性可能降低）时发生的事故的可能性，并确定对安全级仪表控制系统的不可用性的适当限制（见第4章和第5章）。

3.6. 意在涵盖所有正常运行模式的一个核动力厂的安全的正常运行，应该在设计程序中得到考虑。在设计过程中，应该对核动力厂安全运行所需的仪表控制系统的正常运行规定一套要求和限制。这些要求应该涵盖（参考文献[1]，第5.26段）以下内容：

— 为安全系统确定整定值所需的信息；
— 施加在过程变量和其他重要参数上的控制系统限制和程序限制；
— 为确保构筑物、系统和部件能够如预定的那样完成功能的核动力厂维护、试验和检查；和
— 明确规定包括安全系统停役事件时的运行限制在内的运行配置。

3.7. 这些要求和限制是确定批准核动力厂运行的运行限值和工况的基础。

假设始发事件

3.8. ‘设计要求’规定，对纵深防御的所有层次可能发生的那些挑战要在核动力厂设计中得到考虑；并且要提供确保所要求的安全功能能够完成和安全目标能够达到的设计措施（参考文献[1]，第5.8段）。仪表控制系统要具备根据一个假设始发事件感知一个挑战的发生，并且在必要时触发一些动作以完成所要求的安全功能，以确保不超过设计基准中规定的限值。

3.9. 为确定仪表控制系统完成安全功能所需的那些探测能力、处理能力和驱动能力，应该在核动力厂设计基准中规定假设始发事件的明确清单。在这个清单中，应该考虑核动力厂的位置，假设始发事件发生的预计频率，以及不发生保护动作时导致的后果。

3.10. 在核动力厂的安全分析中，这些假设始发事件要逐一地加以考虑。此外，还要考虑一个始发事件可能导致的一系列事件或故障。在核动力厂安全分析中要考虑的所有这种随之发生的事件或故障，都应该在设计基准中加以规定。应该规定可接受的假设始发事件后果的限值。

3.11. 这些假设始发事件及其后果可接受的限值构成安全分析的输入基础。这些输入基础随后以定量的形式给出完成安全任务所需系统总的功能性能要求。

3.12. 然后这些功能性能要求被指定给安全重要的适当仪表控制系统。本安全导则不专门讨论这些安全分析，也不提供评定所导出性能要求的适当性的手段。不过，本安全导则规定指导保护系统随后设计所需要的输入信息。下面介绍的是，随着设计展开可能要重复若干次的这些安全分析的一个典型的序列：

— 确定适用于核动力厂运行的每种模式的假设始发事件，并且估计它们的发生频率；
— 确定每种这样的事件的可接受限值；
— 确定核动力厂工况的限值，以便通过适当的裕度防止超过假设始发事件后果的可接受限值（见参考文献[1]第5章）；
— 确定将核动力厂工况维持在这些可接受限值范围内所需要的安全任务，并确定这些任务的实施所要求的完整性；和
— 在核动力厂的实际配置的基础上，确定保护系统的部件必须在其工作的环境条件的范围，包括有可能使保护系统的部件功能降级的条件，以及为保持保护系统的部件完成其安全任务的能力需要提供如实体屏障等措施的条件。

设计基准事故的设计基准

3.13. ‘设计要求’规定：在需要迅速和可靠动作响应一个假设始发事件的场合，要采取自动触发必要的安全系统动作的措施，以便防止可能向威胁下一个屏障的更严重的工况发展。有关保护系统的自动响应的设计指导在第5章中提供。

3.14. ‘设计要求’规定，在不需要迅速动作的场合，允许系统的手动启动或其他的操纵员操作，条件是这些操作需要足够长的时间展示，并确定能够确保这些操作可靠性的适当程序。有关人-机接口设计的，旨在确保操纵员能够得到适当和可靠的信息的指导，在第6章中提供。

超设计基准事故的设计基准

3.15. 在安全分析中，要考虑发生这样的严重事故的可能性，其中，一些很不可能的事件可能威胁放射性物质释放屏障中的许多屏障或全部屏障的完整性。安全分析要确定严重序列，并能确定这些序列的合理可行的预防措施和缓解措施。这些情况下的事故管理战略和程序，要根据参考文献[1]的第5章制定。

仪表控制系统设计要求

3.16. 安全重要的仪表控制系统的设计基准，应该根据为相应系统和特性提供文件的核动力厂设计基准来确定。仪表控制系统的设计基准，应该按照本安全导则第7章中给出的指导写成文件。其性能要求、系统可用性的要求，以及仪表控制系统工作的环境条件（包括事故期间和事故后的环境条件），应该在仪表控制系统的设计中得到考虑。

3.17. 仪表控制系统的功能和性能要求，应该根据核动力厂营运单位的要求、核动力厂人员的能力、核动力厂的安全要求和安全分析作详细规定。应确定被测变量的量程、准确度、响应时间、带宽和输出信号水平等性能要求。在安全有关仪表控制系统设计中，应该考虑动力供应特性中的瞬态和正常变化，例如电压波动、频率变化和仪表空气压力变化的影响，以确保仪表控制系统充分完成其安全功能必需的程度。

3.18. ‘设计要求’规定，对于运行状态和设计基准事故，要为每个构筑物、系统或部件详细规定一套与其关键物理参数相一致的设计限值。对于安全重要的仪表控制系统，这套限值应该包括针对运行状态的和针对设计基准事故工况的，对该系统将被要求经受住的那些环境条件的详细说明，以及对在这些条件下的预期运行持续时间的详细说明。应考虑下列环境条件：最高和最低的温度、压力、湿度、电离辐射强度、电磁干扰、动力源变化、振动、腐蚀、疲劳和应力等。

4. 一般设计导则

4.1. 安全重要的仪表控制系统的若干关键属性或重要方面已经确定。有关这些属性的一般指导将在下面的篇幅中提及。对每种属性，将提出支持导则的论证。这种论证及时地提醒设计者，注意随确定属性提出的那些问题或关注。在有关论证的每次讨论之后，根据安全重要性的分级（见第2章），按两个层次来

安排和介绍导则。第一个层次包含为安全重要的所有系统提出的导则。这些导则同样适用于所有安全系统和安全有关系统。第二个层次导则特定地适用于安全系统，并且补充第一个层次。虽然对于每种属性存在两个导则层次，但在一些场合下，这些导则并不确定为是适用于安全系统，或适用于安全有关系统。导则对这两级系统的适用性，将在正文中介绍，并总结于表I中。

4.2. 为某些个别系统的设计特定的详细的进一步的指导，将在第5章中提供。第4章中提供的指导与第5章中给出的特定指导一起构成对这些个别系统的全面指导。

性能要求

4.3. 性能要求规定要完成的仪表控制动作和关键的技术特性。这些要求包括提供的被测变量的量程、精确度、响应时间、带宽和输出信号水平。

4.4. 安全重要的仪表控制系统及其支持设施的这些必要的性能要求和可靠性目标，要通过对一个具体的核动力厂的安全分析加以确定，并在该核动力厂的设计基准中得到阐述。

4.5. 安全重要的仪表控制系统应完成核动力厂安全分析中认为可信的那些功能，并且其技术特性应与安全分析中所做的假定以及设计其准要求相一致。

4.6. 当要求一个安全重要的仪表控制系统在环境条件的某一范围内运行时（见第4.62段至第4.65段），当它经受那个范围的环境条件时，其设计应能够满足所有对它提出的要求。

4.7. 当一个系统内的设备用于完成不同功能时，对该设备的性能要求（例如精确度和响应时间）应满足所有这些功能的要求。

可靠性设计

4.8. 可靠性是安全重要系统的一个重要属性。‘设计要求’规定，所有安全重要物项的构筑物、系统和部件都要设计成，它们的质量和可靠性是与它们的级别相适应的。具体地说，可靠的安全重要仪表控制系统必须防止对实体屏障完整性的过分的要求，并且确保所设计的保护系统的可靠性。对于保护系统，参考文献[1]第6.81段特别要求满足功能的高可靠性的设计。

表I. 第4章各节对安全有关系统或安全系统的适用性

段落	题 目	适用于	
		安全有关系统	安全系统
4.1—4.2	一般设计导则	是	是
4.3—4.7	性能要求	是	是
4.8—4.13	可靠性设计	是	是
4.14	可靠性设计	否	是
4.15	单一故障准则	是	是
4.16	单一故障准则	是	是
4.17—4.21	单一故障准则用于安全重要仪表控制系统	是	是
4.22	多重性	是	是
4.23—4.30	多样性	是	是
4.31	多样性	否	是
4.32—4.34	可靠性评定	是	是
4.35	软件可靠性	是	是
4.36—4.48	独立性	是	是
4.49—4.50	故障模式	是	是
4.51—4.53	接近设备控制	是	是
4.54—4.60	整定值	是	是
4.61	人机接口	是	是
4.62—4.65	设备质量鉴定	是	是
4.66—4.69	设备质量鉴定程序	是	是
4.70	设备质量鉴定程序	否	是
4.71—4.73	质量鉴定方法	是	是
4.74—4.76	质量	是	是
4.77—4.78	电磁兼容性设计	是	是
4.79—4.80	试验和可试验性	是	是
4.81—4.83	试验程序	是	是
4.84—4.85	试验设备	是	是
4.86—4.87	试验设备	否	是
4.88—4.89	故障探测	是	是
4.90	故障探测	否	是
4.91—4.92	系统性能证实	否	是
4.93	停用	是	是
4.94—4.95	停用	否	是
4.96	试验的控制和进行	否	是
4.97—4.103	可维修性	是	是
4.104—4.106	文件	是	是
4.107—4.108	安全重要物项的确定	是	是

4.9. 为确保能满足安全重要仪表控制系统设计基准的可靠性要求，一般应采用概率论设计准则和确定论设计准则的适当结合。对与系统的硬件有关的故障，一般应提供定量的可靠性数值。在安全重要仪表控制系统的设计中，应适当考虑随机故障容限、共因故障容限、故障安全设计、设备和系统的独立性、高质量设备的选择、可试验性和可维修性等设计特点。

4.10. 实际上，这些因素中的一些因素的适当的折衷可能是必要的，以便使尽量缩短修理所需的停役时间和降低试验频率之类的目标得到最优化。不论一个仪表控制系统是如何被优化的，它仍应满足其可靠性要求。

4.11. 一个仪表控制系统内部的各个部件的可靠性愈高，则整体系统的可靠性愈高。但是，对于各个部件的可靠性水平，存在一些实际限制。更高的可靠性要通过使用多重性或多样性来实现。例如，也许能用多个通道，或用测量中子通量或温度和流体流量或压力之类的多样手段来监测反应堆功率。多重性的使用提供免受随机故障影响的保护。多样性的使用提供免受某些共因故障影响的保护。

4.12. 要求每个系统达到的可靠性，取决这一系统的功能在安全上的重要性，一般应在设计基准中作明确规定。一个仪表控制系统在安全上愈重要，它的可靠性就应该愈高。规定所需要的可靠性的一种方法是，为第2章所介绍的每个级别指定一个可靠性数值。另一种方法是，通过在工程经验的基础上进行的判断，为各级别规定确定论的设计准则，把系统指定到所定的那些级别，然后确定适用于每个级别的一组要求。然后，将同一级别的所有系统与典型系统作比较。在大多数情况下，要结合使用确定论准则和概率论准则。

4.13. 一些成员国使用明确的可靠性要求。在另一些成员国中，可靠性只是对安全系统和设备所要求的性能的论证的一个方面。除单一故障准则外，不同的国家实践还为保护系统的性能制订了一套目标。这一附加可靠性，有时是通过在保护系统的部件中使用双故障保护和（或）通过使用带有更宽的设计裕度的设备实现的。

4.14. 安全系统应符合单一故障准则，而且应该考虑发生共因故障的可能性。在某些情况下，可以采用可能允许运行的最低限度多重性要求。在安全系统的设计中，应该仔细地确定和考虑故障的潜在原因，以便确定何处适合使用多样性原则。

单一故障准则

4.15. 单一故障准则是用于确保得到一个系统或一组设备物项的最低限度多重性的确定论方法。它是根据下述的一般经验：即使是按照高质量标准制造出来的部件和设备，有时也会以一种随机的和不可预测的方式，在一个随机的和不可预测的时间不能工作。如果一个系统被设计成，尽管经历这样一个随机的部件故障，它的安全有关功能也得到保证的话，那么它的可靠性水平将得到改善。

单一故障准则

4.16. ‘设计要求’规定：当已证明每个安全组能够在下述条件下完成其安全功能时，必须认为已符合单一故障准则（参考文献[1]，第5.37段）：

— 假定对安全组发生一个假设始发事件的任何潜在的有害后果；
— 从维护、试验、检查、修理以及从允许的设备停役时间上考虑，采用了完成必要安全功能的安全系统的最差可容许配置。

当应用单一故障准则时，误动作应该被认为是一种故障模式。在任何时候不假设发生1个以上的故障。

单一故障准则应用于安全重要仪表控制系统

4.17. 为了解释‘设计要求’中定义的单一故障准则，这个准则必须应用于核动力厂设计所包括的每个安全组。定义为设备组合的‘安全组’（常被称为‘系列’）要完成一个假设始发事件发生后所要求的所有动作，以便不超过设计基准中为这种事件规定的那些限值（参考文献[1]，第5.34段）。

4.18. 对那些适用单一故障准则的仪表控制系统，首先要确定要求系统完成的安全功能，以及完成这些安全功能所需要的安全组。还应该确定包括与仪表控制系统有关的、其故障可能影响该系统被规定安全功能的所有其他系统。当有关的安全组已确定时，应完成以下分析：

— 应确定设计基准中的那些对所要求的安全功能有关的假设始发事件。应确定这些假设始发事件的发生概率。如果概率是可信的，则应该确定这些假设始发事件随之发生的影响。
— 应确定为对付这些假设始发事件所需要的那些安全功能、安全系统和支持设施（例如插入控制棒或关闭安全壳隔离阀）。还应包括可完成安全功能的其他“成功途径”。
— 应假设在系统中发生了单一故障，并应确定这个单一故障的后果。

— 应该证明安全功能仍然能完成。
— 在确定单一故障后果时，应证实在安全组内符合独立性要求（参考文献[1]，第II.11段）。这个过程应包括，尽可能地核实安全组没有共享设备或易损点。
— 如果已确定所要求各系统独立的多重性和独立系列是为抗单一故障的，则这些系统不需要依据单一故障准则对潜在的故障进行进一步的详细分析。
— 如果在一些特殊场合单一故障准则得不到满足，则要变更设计以满足这个准则，或者，如果证明设计是合理的，可以不变更设计。然后应该确保通过适当的在役检查、维护和运行程序，将其可靠性保持在很高的水平，致使在系统工作时发生故障变得不可信。
— 如果一个单一故障足以损害一个安全系统的可靠性，则应该确保，可利用其他系统防止不可接受的后果。
— 在应用单一故障准则时，隐含地假定了故障的可探测性。但是，可能存在一些不能通过试验探测出的，或以报警或异常指示所揭示的故障。应该就这样一些不可探测的故障对系统进行分析。可取的方法是重新设计系统或试验方法，使故障容易被探测。如果这是不可能的，便应该假定这样一些不可探测的故障已经发生，然后还应该假定一个单一故障已经发生。应确保在这样的情况下能够完成安全功能。
— 应该确定针对重要的事件序列规定的操纵员操作。应该分析操纵员的不正确操作或忽略的单一随机规定动作的后果影响。应确保在这样一些情况下能完成安全功能。
— 在一些成员国中，当多重系列之一由于试验或维护停役而不适用单一故障准则时，在这样一些情况下应该确定能够确保所要求的可靠性的可容许停役时间。
— 共因故障一般不包括在这种分析中。应该分别地评定一些可信的共因故障。评估时可以使用确定论方法或概率安全分析，或两者的结合。应该引入充分的独立性和多样性，以便提供合理的保证，即在发生共因故障的情况下，安全功能是能够完成的。

4.19. 虽然仪表控制系统的某些组成部分（电缆、印刷电路板或机柜）可被认为是非能动的，但是很少需要或可能有效地使用这种措施去使单一故障分析变得轻松。

4.20. 对下述情况不符合单一故障准则可能是合理的：

— 一些极少见的假设始发事件；

— 假设始发事件的一些极不可能的后果；
— 在限定时间间隔内，为维护、修理或定期试验目的某些部件退出运行；
— 用于防止或缓解严重事故的设施；和
— 其发生故障的可能性能被证明足够小以致于可被忽略的部件。

4.21. 关于单一故障准则应用和实现符合性策略的进一步指导，可参阅文献[5]。

多重性

4.22. 多重性通常被用于安全重要仪表控制系统中以达到系统的可靠性目标和（或）符合单一故障准则。为使多重性充分有效，应该有独立性（见第4.36段至第4.48段）。虽然单独来看，多重性能够提高安全动作或安全有关动作的可靠性，但是它可能增大误动作的概率。设备多重信号的符合或基于多重信号相互比较拒绝假信号的方案通常用来获得可靠性和排除误动作之间的适当平衡。

多样性

4.23. 仪表控制系统中的多样性是这样一种原则，即使用不同的技术、不同的逻辑法或计算法，或不同的驱动手段来监测不同的参数，以便提供几个方法去探测和响应一个值得注意的事件。多样性提供对共因故障的防御，是对纵深防御原则的补充，并且必要时增大完成安全任务的机会。不同深度层次的防御也可以是彼此互异的。可考虑的多样性类型包括人员多样性、设计多样性、软件多样性、功能多样化、性能多样性、设备多样性和系统多样性。

4.24. 在不能进行系统可靠性必要论证的场合，例如在一个多重系统的可靠性将受限于共因故障或设计中的若干不确定性等因素的场合，应该提供额外的保守性。例如，在以计算机为基础的系统的可靠性论证中，可能出现一些特殊的困难。多样性是一个可用来包含保守性的方法，以便补偿论证所需可靠性水平时遇到的困难。

4.25. 应该论证根据上述准则提供的多样性的适当性。应该考虑多样性的范围和级别。达到所希望的保守水平，也许不需要扩大多样性的范围去涵盖一些极不可能的假设始发事件或低后果假设始发事件，这是因为这类事件的风险也许是可接受的，尽管存在发生共因故障的可能性。

4.26. 一般应有几类多样性。功能多样性（提供具有重叠安全效果的不同物理功能的系统）和信号多样性（使用不同的监测参数触发保护动作）也可能是特别有效的。

4.27. 在任何应用中都应该谨慎，以确保多样性在所执行的设计中实际上得到实现，并且在核动力厂的整个寿期内一直被保持。设计者应积极地审查设计，以避免在多样性应用中存在潜在的共性，例如类似的材料、类似的部件、类似的制造过程、类似的软件、运行原则中的细微相似性或共同的辅助设施。

4.28. 对设备多样性或为有关仪表控制系统（如实时操作系统）软件多样性所进行的论证，应该扩展到这些设备的部件，以确保存在实际的多样性。例如，不同的制造厂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同故障模式。不考虑这种可能性，对多样性的要求仅基于不同名称的制造厂的是不够的。

4.29. 在软件的多样性方面，经验表明，如果软件的多个版本是根据同一个软件需求规格说明开发的，故障模式的独立性可能是达不到的。具体地说，一些独立开发的程序版本可能发生共因故障。对这种限制的处理，采用功能多样性和信号多样性之类的多样性可能是非常有效的。

4.30. 为使额外增加的可靠性高于仅满足单一故障准则所达到的水平，额外增加的可靠性要通过多重性、多样性、经过考验的设备的使用、可试验性、连续监测和可维修性等概念的扩大使用来实现。

4.31. 在一些成员国中，除单一故障准则外，还对保护系统提出可靠性要求。这种附加的可靠性，有时是通过在保护系统部件中使用双故障保护，和（或）使用带有较大设计裕度的设备实现的。在一些成员国中，一个用数字表示的总的可靠性目标已经建立，为验证保护系统是否达到这个目标，采用了一些分析方法和试验方法。

可靠性评定

4.32. 对于所有的安全重要系统，应该证明其多重性、多样性、可试验性和坚固性足以达到要由系统完成其安全功能所要求的可靠性。证明可以基于确定论准则和定量可靠性分析或两者的结合。

4.33. 在数字仪表控制系统的可靠性评定中，应考虑可能的硬件和软件故障的影响，也应该考虑为防止或限制这些影响而提供的设计性能。要考虑的硬件故

障应该包括计算机本身各个部分的故障，以及通信系统的各个部分的故障。持久故障和短暂故障这两者都应该考虑。

4.34. 应确定部件故障对一个仪表控制系统不可用性贡献的适当可信度，例如当使用概率方法时，通过规定的置信水平达到这个目的。

软件可靠性

4.35. 软件故障是由设计错误引起的系统性故障，所以没有硬件可靠性分析中所假定的随机故障性质。因此，评定由硬件和软件引入的不可靠性，可能需要使用不同的方法。例如，以计算机为基础的系统的可靠性可能要在定性评价的基础上加以论证，同时要考虑设计的复杂性，在一个宽的输入条件范围内对软件开发过程验证、确认和试验的质量，以及运行经验的反馈。

独立性

4.36. 独立性防止：(1) 故障从一个系统扩展到另一个系统或 (2) 故障在系统内的多重部件之间扩展，以及 (3) 由核动力厂内共同危险引起的共因故障。为保证安全重要的系统的高可靠性而提供的多重性和多样性有效，独立性对确保这一点也是重要的。

4.37. 应该考虑独立性，以防止故障：

— 作为假设始发事件的后果，在系统部件之间扩展；
— 在有相同安全重要性的一些系统之间扩展；和
— 从安全重要性较低的系统向安全重要性较高的系统扩展。

4.38. 安全系统应该与安全有关系统和非安全系统独立。安全重要性较低的系统可以与一个安全系统相联系，条件是，保持这些系统之间的独立性，以及不降低多重安全组的独立性。

4.39. 安全重要仪表控制系统内的多重安全组应该是彼此独立的。

4.40. 在安全有关系统的多重部件之间，应具备独立性。

4.41. 在多样功能之间，应具备适当的独立性。应证明所提供独立性的适当性。

4.42. 独立性是以系统间的电气隔离、实体分隔和通信独立性的方式实现的。

4.43. 要求电气隔离，以控制或防止由下述因素引起的设备与部件之间有害的相互作用：电磁干扰；静电积累；短路；断路；接地；最大可信电压的引入（交流电压或直流电压），以及机械相互作用等。电气隔离措施的实例有电的和光的隔离装置、电缆屏蔽、内部机械结构或类似的装置。当隔离装置用于不同安全重要性的系统之间时，隔离装置应与那个重要性更高的系统相联系。

4.44. 在任何一个要求完成功能的假设始发事件持续期间和假设始发事件后，隔离装置的非安全侧发生的任何可信故障都不应该防碍安全系统的任何部分满足其最低限度的性能要求。

4.45. 系统相互间的实体分隔是通过距离、屏障或这两者的结合实现的，并且可用来降低作为一些假设始发事件（例如火灾、飞射物、水淹或高能管道破裂）的继发故障导致共因故障发生的可能性。此外，这种实体分隔还能降低在运行或维护期间，这些系统的一个以上的部件中发生不小心的调试错误的可能性。

4.46. 在核动力厂中的不同部位，选择用距离、屏障或它们的结合来实现实体分隔可以有所不同。选择取决于：提供应付设计基准中考虑的所有假设始发事件，包括火灾、化学爆炸、飞行器撞击和飞射物的效应所需要的保证。参考文献[6—9]提供进一步的指导。

4.47. 核动力厂中的某些区域往往会成为多重设备或线路的自然会聚中心。在这些区域中，在某些假设始发事件发生后独立性丧失的程度应仔细地加以确定，以便作为建立一个达到可靠性要求和目标的总设计的依据。这种会聚中心的实例包括安全壳贯穿件、马达控制中心、开关装置中心、电缆分布间、设备间、控制室和核动力厂过程计算机。

4.48. 通信独立性仅与那些包括有数据通信的设计有关。通信独立性要通过选择系统结构和数据通信协议方法实现，使一个系统中发生的逻辑故障或软件故障不可能对与之相联接的系统产生不利影响。通信独立性要通过对数据的缓冲做出适当安排（包括用于支持数据换接、传输错误探测和纠正、信息流控制或传输控制，或通信协议处理的任何硬件逻辑和（或）软件逻辑）的方法实现，使发送和接收处理模块发生的任何故障都不会影响处理模块的功能。

故障模式

4.49. 故障导出已知故障模式的设计方法，是适应系统或部件的预期故障的一种方法。故障不仅应该产生可预测的故障模式，而且所产生的故障模式应该将

系统置于安全状态。‘设计要求’规定，要考虑故障安全设计原则，并酌情纳入核动力厂安全重要系统和部件的设计中（参考文献[1]，第5.40段）。

4.50. 为方便安全系统的总体设计，设备应该尽实际可能呈现可预测和可指示的故障模式。安全重要系统中的可能性较大的那些故障模式，应该尽可能地将系统置于安全状态。应该考虑将‘断电脱扣’或‘监视定时器’之类的故障安全措施纳入仪表控制系统的设计中（参考文献[1]，第5.40段），但是，在适用这种作法的场合，不排除这样的必要性，即满足故障安全设计装置本身可能发生故障而提出的安全要求。

接近设备的控制

4.51. 为了防止发生未授权的接近和人员发生错误的可能性，应该适当地限制对安全重要系统中设备的接近。有效的方法是，根据设备所在区域中的监督程度采取实体保安措施（外壳加锁、房间加锁、盘门上设报警装置）和行政措施的适当结合。

4.52. 接近控制的两个值得关注的部位是整定值调整和校准调整，因为它们对防止由于运行或维护中的一些可能的错误使系统的性能降低方面具有重要意义。

4.53. 对于以数字计算机为基础的系统的接近控制而言，应使用限制对软件和数据的电子接近的手段。这些限制应适用于通过网络联接和维修设备进行的接近。

整定值

4.54. 核动力厂必须设计成，它能安全地在规定的参数范围内运行，对公众和环境的放射性危害保持在法规限制范围内（参考文献[1]，第5.24段）。虽然核动力厂状态应该改变以响应始发事件，但核动力厂可能接近处于安全运行包络线以外的一个状态。某些安全重要系统会启动，以引起必要的动作使核动力厂恢复到安全状态。当一个被监测变量达到预定的整定值时，这些系统便会启动。

4.55. 对一个给定的被监测变量（例如一回路压力、安全壳压力）或计算变量（例如反应堆功率、临界热流密度比），要在安全准则的基础上确定一个安全限值。这个限值应是该变量这样的值：超过它时，预计要发生不可接受的安全后果（见图2）。

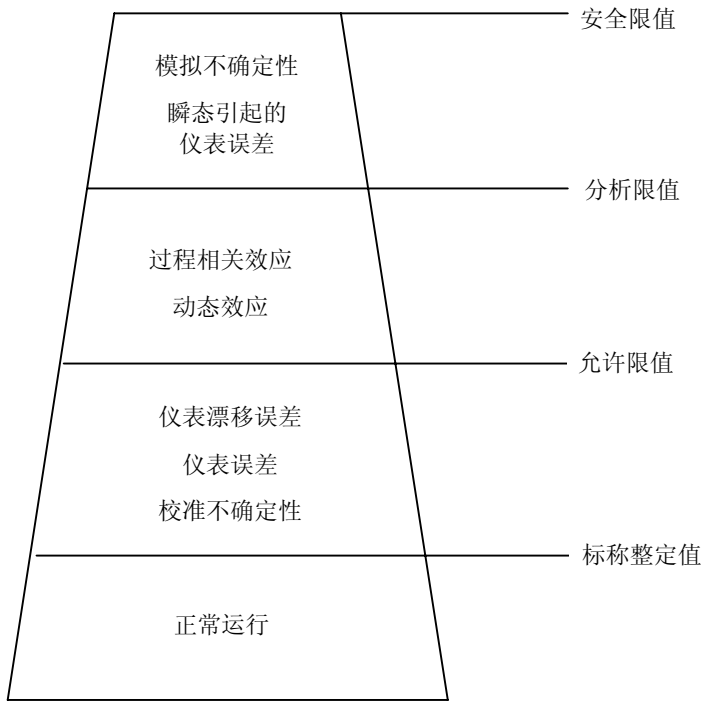

图2. 整定值和限值之间关系的实例。

4.56. 分析限值[1]是从安全分析中导出的一个理论值。安全分析应该论证，在一个始发事件发生后，如果在分析限值达到时开始缓解动作的话，将不会达到安全限值。在分析中，要假定系统和设备的“正如所设计的”配置是可用的，以及适当假设的故障是的确会发生的。因此，在计算安全限值和分析限值之间的差值时，要考虑模拟的不确定性和由瞬态引起的仪表性能中可能的误差。

4.57. 标称整定值是设定在事故保护停堆功能的值。标称整定值与分析限值之间的裕度应该是，在分析限值达到之前缓解动作已经完成。

[1] 分析限值是从安全分析中导出的一个理论值，如果在一个始发事件发生后，缓解动作在达到分析限值时开始，安全限值将达不到。

4.58. “允许限值”用于需要定期试验和监视的仪表。允许限值和标称整定值之间的裕度包含仪表校准中的随机不确定性、仪表随机误差和仪表漂移引起的误差。如果发现一个整定值超过允许限值，应该立即采取纠正措施。

4.59. 应该编制文件和论证在确定标称整定值和允许限值确定时使用的依据。

4.60. 在某些场合，被监测的变量与确定安全限值使用的变量不一样。这种场合的实例有：

— 不监测冷却剂丧失事故后燃料包壳的峰值温度。代之监测反应堆冷却剂的压力，因为不断下降的压力可能是威胁燃料完整性事故的指示信号。
— 在压水堆中，被监测的是轴向中子通量、热腿和冷腿的温度以及一回路压力，因为它们合在一起能够提供偏离泡核沸腾的信号，而这种偏离是不可能直接测量的。

人-机接口

4.61. 安全重要系统需要有效的人-机接口，以便向操纵员提供有关核动力厂状态的准确的、完整的和及时的信息，并且使由仪表控制系统控制的那些系统能够正常运行。‘设计要求’规定，在设计过程中，要包括对人的因素和人-机接口的系统化的考虑（参考文献[1]，第5.5段）。安全重要的仪表控制系统的人-机接口，应该符合本安全导则第6章给出的指导。

设备鉴定

4.62. 应确保安全重要系统在正常运行、外部事件和预计运行工况中，以及在设计基准事故工况中和其后，能够完成其所要求的安全功能。这对于防止放射性物质的释放，以及在释放发生的情况下防止或减轻释放给人体健康和环境带来的放射性后果是十分重要的。

4.63. 从设计基准事故工况中产生的能够引起设备故障的危险环境条件的实例有，与管道破裂（包括反应堆冷却剂系统的破裂）相关的放射性条件和蒸汽条件。潜在危险的过程条件实例包括，高速两相流、高水平振动或充满碎片的工艺过程流。除有潜在危险的工艺过程事件外，还应该考虑那些可能引起共因故障的效应，例如过热、电磁干扰、静电放电和动力源中的各种变化。

4.64. ‘设计要求’规定，要制订一个质量鉴定程序，以证实所述设备在其整个设计工作寿期中，当其处在要求其完成安全功能时可能出现的环境条件（振

动、温度、压力、喷气式飞机撞击、电磁干扰、辐射、湿度或其任何可能的组合）下，能够满足完成安全功能的要求（参考文献[1]，第5.45段）。质量鉴定的过程是，识别设备可能在其中运行的环境中的危险和实施一个试验和（或）分析程序，以确定和用文件证明设备在所规定的工作条件下是否能够令人满意地完成其安全功能。质量鉴定是用来将引起该设备共因故障的环境事件或影响的可能性降至最低限度的一种方法。

4.65. 设备质量鉴定应该证明，设备在要求的环境和运行条件下能够完成功能。下述建议虽然是针对安全重要系统的设计特别提出的，也应该结合关于质量鉴定问题提供的其他指导（例如参考文献[10]。）予以应用。

设备鉴定程序

4.66. 应该完成质量鉴定程序，以证实安全重要设备在要求完成安全功能时，在可能需要承受的环境条件（例如温度、压力、辐射、湿度或苛性喷淋）下，直至其设计寿期末，均能够满足指定安全任务的设计基准性能要求（例如范围、准确度和响应）。

4.67. 环境条件应该包括，正常运行期间与预计运行事件期间以及设计基准事故期间的和设计基准事故后的各种环境条件的那些预计的组合。在设备质量鉴定程序中不要求考虑严重事故工况。但是，应该以合理可信度和尽可能高的程度证明用于响应严重事故的可信设备能够在预计的严重事故工况下完成安全功能（参考文献[1]，第5.46段）。

4.68. 在设备承受自然现象或其他外部影响等外部事件，并且要求在事件期间或之后完成其安全任务的场合，质量鉴定程序应该包括外部事件强加在该设备上的那些条件。此外，质量鉴定程序中还应该包括任何能够合理预计的，以及例如在安全壳泄漏率定期试验时可能由特定工况产生的那些异常环境条件。

4.69. 质量鉴定程序应该包括一个计划，旨在确保设备在预定的使用期内都是合格的，以及必要时进行及时的再质量鉴定或更换。应考虑各种环境因素的联合效应，以及在设备整个安装寿期内周围正常环境因素的综合效应。对没预计到的老化机制，应该酌情提供进一步的保守性。应该为核动力厂设备的监测、试验和检查作出安排，以便识别未预计到的行为或退化（参考文献[1]，第5.47段）。

4.70. 在安全系统设备质量鉴定中，最可取的作法应该是质量鉴定整个设备，而不是只质量鉴定与所考虑的安全任务直接相关的那些部分。

鉴定方法

4.71. 为达到上述目标，应该使用下述质量鉴定方法的适当组合：

— 对提供的设备类别进行性能试验；
— 对已供应的实际设备进行试验；
— 考虑以往类似应用方面的有关经验；和（或）
— 根据有关工况下取得的试验数据或运行经验用合理工程外推法进行分析。

4.72. 所选定的质量鉴定方法应该如第2章中所介绍的那样，提供的置信度应与设备在系统的安全重要性相适应。为设备质量鉴定应该进行试验。在一切实际可行的场合，也应该对安全设备进行试验。

4.73. 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，这些屏障本身应该经受一个质量鉴定程序以确认其适当性。

质 量

4.74. 为确保安全重要系统能证明满足其安全要求，设计和制造的高质量是必要的。根据适当的质量水平进行的设计和制造是在实现参考文献[1]，第5.1段规定要求的重要因素。

4.75. 安全重要系统的部件和模件应该具有与将维护需要和故障率降至最低限度的目的相一致的质量。

4.76. 为安全重要系统选择的设备，只要可能就应是成熟的设计，应该与可靠性目标相一致，并且应便于满足对校准、试验、维护和修理提出的那些要求。在设备选择时，应该考虑误动作和非安全故障模式，例如当要求时不能进行保护停堆的故障模式。

电磁兼容性设计

4.77. 仪表控制设备和系统，包括相关电缆，应设计和安装成能承受核动力厂的电磁环境。

4.78. 在设计中，应对干扰的接地、屏蔽和去耦采取适当措施。用于安装和维护的方法应足以确保这些措施在安装和维护时得到适当实施。参考文献[4]给出有关接地的进一步指导。参考文献[4]就接地与屏蔽提供了典型实践的例子。

试验和可试验性

4.79. 在役试验能够提供这样的保证，即所考虑的这些安全重要系统仍是可运行的并能够完成其安全任务。应该根据系统的可用性和可靠性要求确定试验频度。可试验性——系统被试验的能力——应该作为设计的一部分。在可试验系统的设计中，应该考虑：(1) 设备的位置是否适当，(2) 接近是否得到适当控制，(3) 该设备中的故障是否易于探测，和 (4) 继续保持功能能力的证明是否要以运行中的核动力厂的安全不受损害的方式进行。

4.80. 对‘设计要求’第5.32段至第5.42段中所描述的系统可靠性，以及‘设计要求’第5.43段至第5.44段中所要求的在役试验、检查和监测而言，可试验性都是设计的一个必要部分。此外，保护系统还应该满足‘设计要求’第6.81段至第6.84段所描述的对可靠性和可试验性的特殊要求。

试验程序

4.81. 安全重要仪表控制系统的设计应该包括确定与其可用性要求一致的试验和校准程序。

4.82. 这个试验程序应该确保安全重要系统和部件的功能能力得到保持。这应该包括定期证实设计基准要求，例如对精确度、响应时间和整定值等有关的那些要求是否满足。

4.83. 尽实际可能，对安全重要的仪表控制系统的试验应该是全面的检验（从传感器到执行机构），应该是能在现场以最低限度的努力完成的。由几个合在一起可试验整个通道的交叠试验组成的试验程序是可接受的。所有安全重要的输出功能，例如报警驱动装置的控制操作和运行都应该试验。

试验装置

4.84. 一切安全重要系统都应该包括允许完成所要求的试验的试验装置，合适时包括内装式试验装置。这些装置本身应能定期检验，以确保连续正确运行。在要试验的设备不能安装在非危险区的情况下，应该提供一些装备，以便允许从危险区外远距离进行试验。

4.85. 在提供试验设施的情况下，设计应确保该系统不可能被粗心地留在试验配置中。在已为定期试验提供固定式试验设备的场合，接口应该受硬件联锁，以确保在没有慎重的手动干预的情况下，与试验系统的相互作用是不可能的。

4.86. 就安全系统而言，每一种功能的试验方法理论上都应该涉及包括从传感器到执行机构的所有部件的单一在线试验。不过，这样一些试验不总是实际可行的。在这种情况下，试验程序应该将在线（要求或可能要求安全功能的运行状态）和离线（不要求安全功能的运行状态）试验组合成一系列交叠试验步骤，并使这种组合达到实现试验目标所需要的程度。应该论证使用交叠试验步骤的适当性。

4.87. 安全系统及其试验设备的设计应该确保核动力厂在实际试验中的安全，并且在理论上应该尽量减少任何安全动作的误触发和试验对核动力厂可用性的任何其他不利影响。试验程序的实施不应该引起任何核动力厂部件发生超出设计规定的退化。

故障探测

4.88. 用于定期试验的设备应该提供有关系统状态的客观信息，并且应该酌情提供有关趋势的数据，以便有助于探测系统的退化和能够显示系统内早期故障的那些工况。尽实际可能，安全重要系统的设计应使用自检设施。不过，自检设施的提供应与对简单性的需要加以平衡。

4.89. 在实际可行的范围内，每个被测变量的传感器都应该单独试验，其方法有多种，例如：

— 扰动被测变量；
— 酌情向传感器引入一个与被测变量性质相同的替代输入，并且改变这个输入；或
— 对相互间存在已知关系而且其读出信号可使用的变量进行交叉检查。

4.90. 所要求的试验应该探测安全系统（从传感器到执行机构）中的故障。试验应该能够探测系统的每个多重部分中的故障。在一个通道中提供有多重设备的场合，试验应该验证每个多重部件的可运行性。

系统性能证实

4.91. 选定的定期试验和校准措施应该是，能证实设计基准中为保护系统、安全驱动系统和安全系统支持设施多重通道规定的那些性能特性。试验和校准一般应该以不同的时间间隔进行。

4.92. 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。

停 用

4.93. 在对定期试验充分的需要与安全组的可靠性发生冲突的情况下（例如在一个通道因试验已停用并仍必须正确地恢复以便为安全服务的场合），所选的试验方法应该确保能满意地达到两个目标。例如，当一个传感器为进行定期试验已停用时，与多重传感器的目视相互校核法（或别的相当方法）应该用来验证它随后使用的恢复。此外，应该验证那些为适应定期试验曾被扰动的物项的状态（例如仪表根阀的位置、维修旁通），以确保它们返回本来的运行状态。在这方面，应充分注意可能的人为错误。

4.94. 在安全系统的设计中，应该确保的是，当进行定期试验时，那些仍然在役的部分能够完成所要求的安全任务。对安全系统而言，任何单个部件或通道停用，不应导致丧失所要求的多重性，除非能充分证明系统运行可靠性是可接受的（见参考文献[1]，第6.81段）。所选定的试验方法应该在实际可行的范围内，尽量缩短设备停用的时间间隔。优先选用的将设备停用的方法是，将停用的通道输出置于规定的安全状态。

4.95. 安全级仪表控制系统定期试验所用的试验程序既不应要求，也不应允许使用暂时替代的试验装置、使用临时跨接线、取出保险丝或打开断路器。在试验的安全系统设备配备有为与试验设备连接而专门设计的装置的场合，可以使用与试验设备的临时连接。这些装置应视作这个安全系统的一部分，并应该符合本安全导则的全部有关建议，而不论所用的便携式试验设备是否要被拆接或仍然被连接到这些装置上。

试验的控制和实施

4.96. 为试验所作的那些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。

可维护性

4.97. 核动力厂用的一些仪表控制系统中的若干固有因素，使人们有必要把这些系统设计成允许可靠的和高效的维护。这些因素包括：

— 与仪表控制系统的各种硬件部件的典型使用寿命相比，核动力厂的长使用寿命；
— 仪表的不可避免的漂移、退化或劣化；和

— 仪表控制硬件的磨损（也就是使部件在核动力厂使用寿命内不可避免地至少更换一次的那些部件故障率）。

4.98. 对安全重要系统而言，应特别注意如何方便进行这样一些维修活动：它们能够维持系统必须在其中运行的环境的合格性。尽量减少进行修理所需的时间，有助于提高总的可靠性和可用性。在参考文献[1]第2.9段至第2.11段中规定的纵深防御原则的实施中，可维修性是一个重要因素。

4.99. 安全重要的仪表控制系统应该设计和定位成便于进行监测和维护，允许人员及时接近，并在发生故障或错误的情况下，人员易于诊断和修复。

4.100. 安全重要仪表控制系统的设计，应考虑完成所要求的维护活动的人员能力和限制。在实际可行的场合，仪表控制系统应放置在对维护人员的风险最小并便于设备维护的地方。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。在实际可行的场合，设备不应该置于存在高辐射水平风险（见参考文献[12]）或通常温度或湿度过高的场所。

4.101. 应仔细研究其装置放在不可接近区域中的系统，以便决定其他对付故障的策略将是否适当。这类策略的实例包括安装备用多重装置、为远距离安装提供便利的措施，以及设备发生故障并且不可能被迅速修理或更换的情况下降低功率运行的计划。在功率运行期间，某些部件的位置可能使这些部件不能被定期校准。在这种场合，应该特别强调所选用装置的长期准确性和稳定性，并且应该提供与其他装置进行比较（例如将中子功率与热功率进行比较）的手段。

4.102. 在应用单一故障准则的那些系统中，如果在核动力厂运行期间，一个通道出于维护、试验、修理或校准的目的而被旁路，则系统的其他那些仍然可运行的通道应该继续满足单一故障准则，除非如本安全导则第4.15段至第4.21段中所讨论的那样，已经另有论证。

4.103. 为安全重要仪表控制系统维护提供的手段应该被设计成，对核动力厂的安全的任何影响都是可接受的。这类手段的典型实例有断开多重通道系统中的一个通道，以及代替手动操作的措施。

文 件

4.104. 对安全重要系统设计的信心，在很大程度上基于所用设计过程的正确性。在建立设计信心和将信心的根据传达给别人方面，文件起重要作用。在安全重要系统的设计和实现中产生的文件，应该是清楚的和严谨的。

4.105. 应该产生和保存一套文件，以便确保设计所有理论基础的可追溯性。在设计过程中的每个阶段应产生相应的文件。一套系统文件应该在交付时与系统一起提供。文件的范围、类型和内容的细节，将在第7章进一步讨论。对与安全重要系统有关的所有文件而言，应该具有下述特征：

— 文件应该能被涉及设备的设计、建造、调试、运行、维护和审批，具有不同背景和经验的人清楚地理解；
— 所用的语言应该是清楚的，有一套明确定义的的术语；和
— 在整个文件中应该以统一的方式使用符号、术语、正文和图表。

4.106. 文件编写应注意可适用性，即文件编写应该考虑其使用者的下述需要：

— 设计的那些要求、规格书和描述，应该对每一单个要求、规格书或描述只允许有一种解释；
— 应能从较高层次文件追溯到设计文件以检查文件的完整性；
— 应能从设计文件反向追溯到较高层次文件以检查文件的不必要项；
— 文件应该不含任何矛盾的或不一致的陈述；
— 每条信息在文件中应该有一个单一的、可识别的位置，并且不应重复或分解；
— 每个要求或设计要素都应该有一个唯一的标志符（它也有助于提高可追溯性）；
— 应说明要求和设计信息，以便有可能验证安全重要系统满足那些要求并且是按照设计建造的；
— 文件的结构和风格应能容易地、完整地和一致地做出任何必要的更改；和
— 文件应该是预期的使用者可以理解的。

安全重要物项的标识

4.107. 应确定安全重要物项，以确保有关安全重要系统的要求应用于核动力厂的设计、建造、维护和运行。应该完成标识，以便满足参考文献[1]第5.1段至第5.3段为安全分级的要求。

4.108. 安全系统及其部件应专门地，例如用标签或颜色编码的方法加以标识。此外，在安全系统内，应该适当地标识多重通道，以便降低因粗心在不正确的通道上进行维护、试验、修理或校准的可能性。这种标识不应该依赖于查阅图纸、手册或别的参考材料。这种标识应该区别于用于其他目的的标识记号。对于安全有关系统，也应该采用这种作法。被清楚标识的设备或装置中的部件或

模件本身不需要标识。对保持这类部件、模件和嵌入的计算机软件的标识而言，配置管理一般是足够的。

5. 系统特定设计导则

5.1. 除第4章介绍的一般导则外，本章介绍的特定导则也适用。

安全系统

5.2. 保护系统是安全系统的一部分：它探测与核动力厂可接受工况的偏离，并触发用以防止一种不安全的或潜在不安全的工况的动作。为达到该目的使用各种不同的系统配置，因而‘保护系统’这个术语在有些成员国是不通用的。本章介绍的有关保护系统的指导，适用于完成这些功能的任何系统。

保护系统

5.3. 在控制系统不能将核动力厂变量维持在规定限值内的情况下保护系统用来维持安全。这种情况的出现可能是因为控制系统内已经发生了故障，也可能因为已经发生的事件引起过程变量变化太快而控制系统不能适当地反应，或者因为一个安全重要物项发生了故障。在这种情况下，需要迅速的动作以便防止这种情况发展成为可能的事故。

5.4. 一般来讲，一个特定情况所需要的动作，即为处理这种情况所要完成的安全任务，涉及核动力厂多个物项以一种协调的方式的运行。保护系统提供与安全驱动系统和安全系统支持设施一起完成所有规定的安全任务。

5.5. 保护系统监测核动力厂的有关变量。这些变量可能是过程变量，如中子注量率[2]（通量）或冷却剂温度和压力，或可能是与预计运行事件或设计基准事故工况特别有关的变量，如过程变量的变化率、湿度水平、设备位置的变化或辐射水平。被测量的这些核动力厂变量，不论是单个地或作为选定组合的被测变量，都应该允许探测完成一个安全任务的所有情况。

[2] 注量率（⊥）为适当小时间间隔内的中子增量dΦ除以这个时间间隔dt：⊥=dΦ/dt。

保护系统的目的

5.6. ‘设计要求’规定（参考文献[1]，第6.80段），保护系统要设计成：

— 能够自动地触发合适系统动作，必要时包括自动触发停堆系统动作，以保证在发生预计运行事件时不超过规定的设计限值；
— 能够探测设计基准事故并触发必须将这类事故的后果限制在设计基准内所需系统的运行；和
— 能够抑制控制系统的不安全动作。

5.7. 一般要求保护系统：

— 探测核动力厂的一个变量已达到整定值；
— 识别需要保护的情况；
— 在保护系统本身、安全驱动系统和安全系统支持设施内，以正确顺序触发相应安全任务所需要的所有安全动作；
— 在某些成员国中，监测核动力厂变量并向操纵员显示变量值，供采取手动保护动作使用。

5.8. 设计基准中确定的下述共同安全功能由保护系统触发：

— 反应堆安全停堆；
— 在所有运行工况下维持状反应堆冷却剂压力边界在设计限值以内；
— 在预计运行事件和事故工况期间排出余热；
— 在设计基准事故工况期间和之后的堆芯应急冷却；
— 在设计基准事故工况期间和之后的反应堆安全壳隔离；
— 事故后反应堆安全壳中压力和温度的降低；
— 安全壳内大气的净化；
— 排出流放射性废物的隔离；和
— 气载放射性物质的控制，包括它进入任何作业区域和向环境的外逸的控制。

5.9. 当核动力厂的一个变量达到预定值，即标称整定值时，保护动作便被触发。

保护系统的范围

5.10. 保护系统包括从过程变量测量到产生保护动作信号涉及的所有电气和机械装置以及所有电路。图3表示保护系统与下述诸项的接口：

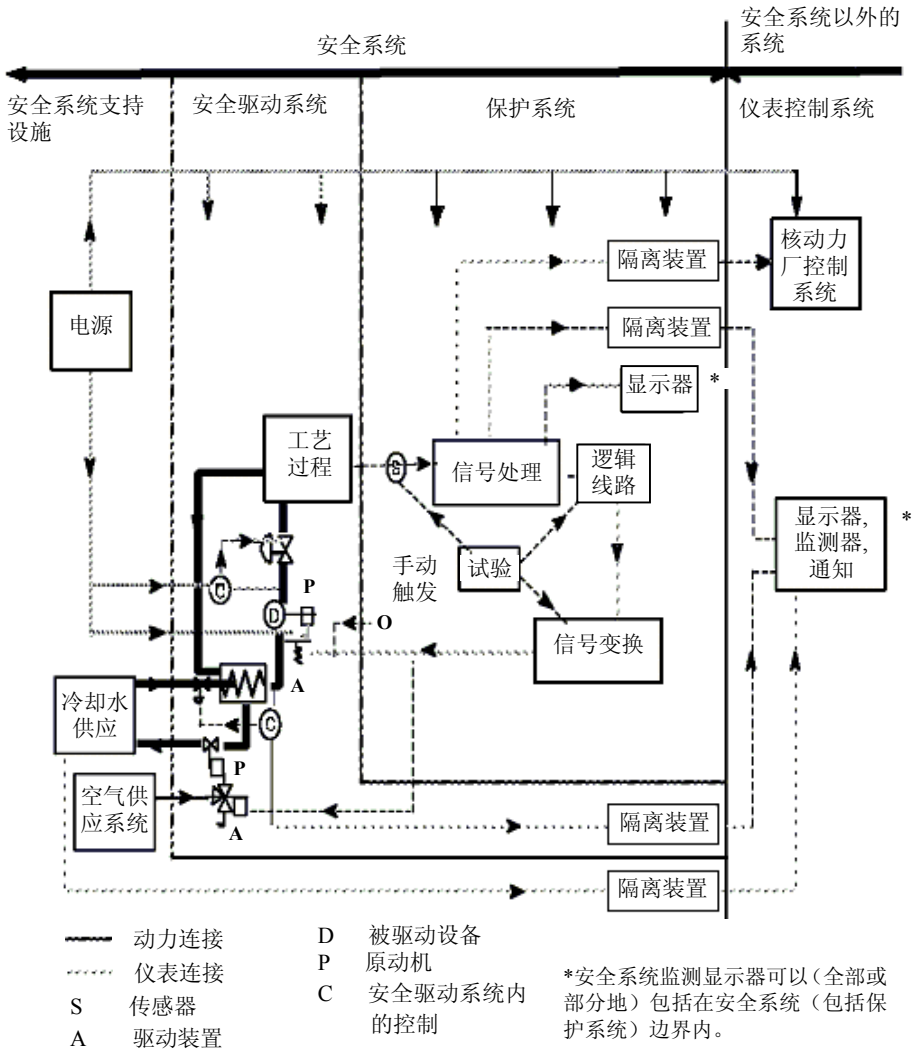

图3. 保护系统及其与其他系统相互连接典型示意图。

— 被保护的核动力厂工艺过程（通过保护系统内的传感器）；
— 安全驱动系统（通过安全驱动系统内的驱动装置）；
— 不包括在保护系统中，但通过装在保护系统中的隔离装置从保护系统中取出信号的任何操纵员信息显示器；和

— 控制系统（通过保护系统中的隔离装置）。

5.11. 为了清晰起见，图3没有表示出保护系统与其他系统（例如监测信息系统、安全系统支持设施，以及现场盘面上控制点之间的所有可能的接口点。

5.12. 保护系统由下述物项组成：

— 传感器，它们可以是：
  - 从工艺过程直到并包括输入变换器的仪表传感线（例如压力、流量和位置传感线）；和
  - 用于测量核动力厂变量的一次传感装置（例如热电偶和电离室）；
— 一次传感装置用的信号处理设备，包括脱扣比较器和模数信号变换器；
— 用于每个被测变量的表决逻辑线路；
— 作为保护动作向驱动装置提供输出的信号变换设备；
— 为手动触发保护动作所需的显示器；
— 与操纵员信息显示器和不同安全级别系统接口的隔离装置；
— 装有保护系统设备的盘、机架和机柜；
— 连接电缆和电缆管道；
— 电气电缆和仪表电缆的安全壳贯穿件；
— 介于工艺过程连接器和驱动装置输入端之间的任何其他设备。

5.13. 本章提供的指导也适用于为确保完成保护系统的功能必须运行的其他安全系统设备。这样的其他安全系统设备包括：

— 接收保护系统输出信号的驱动装置；
— 由驱动装置操作的原动机设备；和
— 由原动机设备操作的被驱动设备。

传感装置

5.14. 保护系统应被用来监测核动力厂变量和探测与这些变量的规定限值的偏离，以便能够完成规定的安全功能。核动力厂变量的测量应该符合设计基准中规定的性能要求。在实际可行的范围内，对所关心的核动力厂工况应通过直接测量加以监测，而不应从别的更为间接的测量中推导出来。

5.15. 对每个监测变量测量范围的选择，应考虑特定的功能所需的精确度、响应速度和超量程，以及任何必要的事故后监测能力。如果必须使用一个以上的传感器来充分覆盖监测变量的整个范围，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的合理的重叠度，以便确保饱和效应或重叠效应不妨碍保护功能的完成。

5.16. 整定值可以是固定的，也可以随核动力厂的某个参数或工况而变化的。当使用可变的整定值时，则用于调整整定值的装置应作为保护系统的一部分并应满足保护系统的要求。系统设计应该向操纵员提供为每个保护系统通道确定整定值的手段。

保护系统‘自保持’

5.17. 保护系统触发的动作应该是自保持的[3]。自保持应该是不能解除的，除非安全动作完成后操纵员手动切除，或为防止超过设计基准中规定的限值通过保护系统动作切除。一旦一个动作被自保持，既定的序列便应该继续，直到已完成安全任务。动作自保持后，保护系统应该自动地监测核动力厂工况，使核动力厂工况所要求的安全动作能够完成，并提供信息以支持任何允许的操纵员操作。一个安全功能的完成不应妨碍保护系统触发随后的核动力厂工况可能要求的其他保护动作。

5.18. 为自保持功能而添加的部件不应该把安全动作的可靠性降低到可接受水平以下。

手动安全动作

5.19. 操纵员操作包括：

— 安全动作的手动后备；
— 某些安全动作的直接触发或终止；和
— 保护系统动作后的复位。

5.20. 手动设备的设计应该灵活到足以允许在异常状况下启动安全动作，以及允许长期的事故后运行。

5.21. 对大多数保护动作要求自动触发是必要的。此外，应该提供反应堆停堆的手动触发能力以及如安全壳隔离之类的系统级动作的手动触发能力。这不排

[3] ‘自保持’是部件的特性：它引起部件的输出信号呈现新的状态，并且在触发新状态的那个或那些输入信号已恢复到初始值后继续保持在那个状态。

除操纵员以一种更细的方式进行的干预。在提供手动驱动设备的情况下，手动驱动设备应在实际可行的范围内独立于自动保护系统的驱动设备。

5.22. 即使一个安全动作因疏忽而被手动触发，保护系统应该通过自动动作来保护核动力厂。可以只使用手动触发或终止安全动作，条件是能证明不超过可接受的限值。这种手动动作的实例有：

— 自动序列完成后触发某些安全任务；
— 事故后将已停堆的核电厂长期置于其最佳状态；
— 假设始发事件过后很长时间才要求触发的某些安全动作。

5.23. 为证实只用手动动作是可接受的，应该证明：

— 操纵员已充分和清楚地获取安全级信息以便做出合理判断和触发所要求的安全动作；
— 操纵员备有帮助操作的书面程序并受过培训；
— 操纵员备足以完成要求动作的手段；
— 允许该操纵员有足够的时间估计核动力厂的状况和完成所要求的动作；和
— 执行动作的操作员之间的通信线路足以保证这些动作的正确完成。

5.24. 从一个预计运行事件或设计基准事故工况之初算起，可用于计划内的操纵员操作的时间在成员国间是不同的，其范围为10 min～30 min。这个时间长短取决于决策的复杂性、可用的显示、区分不同的假设始发事件的需要和错误决定的后果等因素。

5.25. 控制室的设计和布置应使手动安全操作便于实现。安全运行、反应堆停堆和从反应堆中排出余热，以及安全壳系统功能所需要的所有控制器、显示器和报警器，都应该方便可用，并且应该以清晰的方式向操纵员提供信息。

5.26. 有关主控室以外的运行人员实施的安全重要操作的信息，应能在主控室中立即得到，主控室已损坏或放弃的情况除外。在这种情况下，所需信息应能在一个辅助控制室中得到。

5.27. ‘设计要求’规定（参考文献[1]，第6.84段）：设计应该是这样的，虽然要尽量减小操纵员操作使保护系统在正常运行和预计运行事件中丧失有效性的可能性，但是采取的在设计基准事故工况下不要取消正确的操纵员操作。

误驱动

5.28. 误触发可能有多种原因，尤其是设备中的故障、与正常运行中发生的种种变化有关的某些参数的不适当的停堆裕度，或干预中的人为错误。这些原因可能源于下述因素：

— 没有充分考虑核动力厂对运行扰动的响应和被监测参数中的随后变化；
— 没有对仪表不准确性、校准中的不确定性和漂移，或停堆整定值确定中的误差留有充分的裕度；
— 没有充分处理信号噪声；和
— 这些因素的组合。

5.29. 对保护系统的主要要求应该是充分地完成其规定的保护任务。但是，误触发的数目应尽量减小到实际可行的程度，因为误触发能够导致下述问题：

— 设备承受不必要的应力；
— 对其他安全动作的需要；
— 操纵员对设备的信心受损，可能随后导致对正确信号的轻视；和
— 核动力厂生产能力丧失。

5.30. 因此，保护系统应该被设计成，既能够满足有关的要求，又能够将误触发的数目减小到最低限度。来自保护系统的误输出，应该不触发一个涉及安全意义的事件。如果保护系统内的误触发可能导致核动力厂要求处于保护的状态，那么应该通过由保护系统、安全驱动系统和安全系统支持设施未受影响的部分去触发和执行的动作来维持安全工况。

5.31. 减小误触发次数的有效措施包括信号在线滤波、参数确认、多重信号“表决”和给能驱动等。

保护系统和其他系统的相互作用

5.32. 应评估保护系统和各种控制系统之间的可能的相互作用。‘设计要求’规定，保护系统和各种控制系统之间的相互作用要通过避免相互联接，或提供适当的功能隔离加以防止（参考文献[1]，第6.86段）如果信号被保护系统和任何控制系统共用，则必须保证有适当的隔离（例如用适当的去耦方法加以隔离）。

5.33. 如果一个控制系统中发生的故障能够引起一种要求安全动作的核动力厂工况，并同时又使保护核动力厂工况的安全组内的一个通道不能工作，那么在假定这个安全组内任何地方与上述故障同时发生单一故障的情况下，仍应继续

满足安全要求。如果在一个保护通道出于试验或维修的目的被旁通或停用情况下运行是允许的，那么在分析中应假定该通道旁通或停用。

5.34. 如果一个假设始发事件能引起一个导致要求安全动作的核动力厂工况的控制系统动作，那么这同一个假设始发事件不应该妨碍为针对那种核动力厂工况的保护而提供的该安全组的正确动作。用来防止这类相互作用的有效措施包括：

— 安全组中用于处理这类潜在相互作用的附加设备；
— 提供用于限制假设始发事件引起的损害的屏障和（或）另一种核动力厂的布置；或
— 上述两项的结合，以便安全组和（或）核动力厂设计足以将核动力厂工况维持在可接受的限值内。

5.35. 在个别驱动装置（如泵电机或阀驱动器）受核动力厂的控制系统控制，并且又受保护系统控制的场合，保护系统动作应能优先于控制系统所要求的那个动作。例如，如果控制系统要求一台泵以半速运转，而保护系统要求这台泵以全速运转，那么保护系统的要求应该有优先权，这台泵应该全速运转。类似地，如果控制系统要求一个阀关闭，而保护系统要求这个阀打开，那么保护系统的要求应该有优先权，这个阀应该打开。

运行旁通

5.36. 在一种正常运行模式下的保护停堆可能妨碍反应堆转换到另一种运行工况。例如，反应堆在低功率水平的保护停堆将妨碍反应堆升到满功率。为允许这种转换，应该用运行旁通（有时称停堆闭锁）的方法禁止一个不必要的和不希望有的保护动作的触发。这种闭锁停堆信号的逻辑应纳入保护系统。

5.37. 每当允许旁通的条件未满足时，安全系统都应该自动防止一个运行旁通的启动并且应该完成下述任务之一：

— 退出已启动的运行旁通，
— 将核动力厂置于运行旁通是许可的工况，或
— 触发相应的保护动作。

5.38. 不论以何种方法启动运行旁通，用来启动运行旁通的手段认为是保护系统的一部分，并应符合本安全导则的要求。

动力源

5.39. 动力源（所需要的电的、气压的或液压动力源）应与仪表控制系统相适应。用于安全重要仪表控制系统的动力源应该具有与其服务的那些仪表控制系统的可靠性要求相一致的级别、质量鉴定、隔离、可试验性、可维修性和停用指示。

5.40. 动力源一般为可能起因于该仪表控制系统外的，或可能来自直接或间接与同一动力源相接的其他仪表控制系统的电干扰效应提供一个传输途径。动力源和仪表控制系统的设计应保证，这种干扰影响不应大到足以损害仪表控制系统功能的程度。这一点应该通过试验、分析或用以评定与整体安全重要仪表控制系统及其相关的一个或多个动力源系统等其他适当手段(见第4章)加以证实。

5.41. 那些要求在各种运行状态或设计基准事故工况下的所有时间都可供使用的安全重要的仪表控制系统，应该被连接到一个不间断动力源上。不间断动力源的性能要求应该满足由该动力源提供动力的那个系统的要求。

5.42. 当运行情况证明，如果安全重要仪表控制系统功能能够容许动力供应中的相应中断，则这些仪表控制系统可由核动力厂运行人员或自动切换动作连接到代替正常动力源的备用动力源。在大多数场合，这里涉及的切换系统应被认为是那个或那些动力供应系统的延伸部分。

数字计算机系统

5.43. 数字计算机系统用于安全重要仪表控制系统，以完成保护、数据采集、计算、控制、监测和显示功能。如果设计适当，这种系统能够具有比模拟系统更好的可靠性、精确性和功能度。计算机系统可采取多种形式，从支持多种功能的大型信息处理机到由专用于特定应用的小型处理器构成的高度分布式网络。

5.44. 应用计算机系统有助于探测和监测核动力厂中安全重要系统和设备的内部和外部发生的故障。

5.45. 计算机系统的硬件和软件应该如此配置，使形成的系统在硬件和软件可信故障的条件下能以一种预先规定的安全方式运行。

5.46. 借助于计算机，有可能使一套设备完成几个系统功能。计算机系统的缺点是，如果一个部件发生故障，几种功能可能同时不能完成。因此，在计算机系统的设计和分析中应该考虑这个因素。

5.47. 当一台计算机的使用涉及属于不同安全级的两个或更多功能时，这个计算机系统应该满足较高安全级的要求。

5.48. 数字系统的启动和复位（例如在电源暂时丧失后）应该将这个系统初始化到预先规定的，能够确保继续安全运行的状态。

5.49. 应将数字系统所用的软件很好地编成文件，并且应该通过一种受控制的工程程序来开发。

5.50. IAEA安全导则[2]提供有关数字计算机系统应用的进一步指导。

维 护

5.51. 在核动力厂整个寿期内应该保持有关硬件和软件的原始技术的充分技术经验。与核动力厂其他系统的典型情况相反，计算机系统的维护不是例行性的。维护工作人员应该对计算机化系统的需求和数字系统改型开发过程的需求有深入了解。

数字系统升级

5.52. 应该认识到，新的核动力厂中的那些计算机化的仪表控制系统也将老化，变得过时并且最终需要更换。鉴于数字设备的供应商经常改变其生产线，维持供核动力厂的整个寿期使用的备件贮存量变得困难。用户不得不贮存相当多的数量的数字部件，并且在这样做的过程中应该考虑到长期贮存的电子产品可能发生的退化。

数据通信

5.53. 为本安全导则的目的定义的数据通信，是指通过使用分时、分频、脉冲编码技术或类似的技术，在单个数据通道内把两个或更多信号或信息从一个位置传输到另一个位置。数据通信包括多种技术解决方法，从简单的仅硬件多路传输到由软件控制的、复杂的自动校正和多层通信协议。

5.54. 安全重要数据通信通道应该满足第4章，尤其是第4.36段至第4.48段中给出的有关独立性的建议。

5.55. 数据通信系统的设计应该保证错误的探测，并在实际可行的范围内保证错误的校正，以及保证所传输信息中数据的状态。

5.56. 数据通信的检查可以作为一种自动的自检工能定期进行。对数据的使用和需要由系统完成安全功能的频度，所选自检频度应是合适的。用于错误探测和校正的设备能够用于改善信号传输的可靠性，以便达到可靠性目标。

5.57. 应该选择通信技术和进行适当配置，以便确保在所有可能的数据装载条件下，通信技术都能够满足对时间响应的要求。

5.58. 在数据和数据传输装置的可靠性非常重要的场合，应选择适当的通信技术。选择和应用较复杂的技术虽然可能带来一些功能优点，但是也可能引入更多的故障模式和确认困难。对在数据传输装置中采用多重性、对一般数据传输装置依赖的适当程度以及对发送和接收系统承受所有故障模式的能力，应该给予适当的考虑。数据通信技术的应用，不应该使系统结构内的处理部件或逻辑元件的实体的或功能的通道化失效。

5.59. 一般应尽实际可能避免从较低安全级系统到较高安全级系统的数据流。在这样的数据流是必要的场合，应该采取措施（例如数据确认或数据范围检验）以确保来自较低级系统的数据不能损害安全重要功能。

6. 人-机接口

6.1. 对安全重要系统的监视和控制，涉及自动测量和控制功能与由运行人员进行的监视和控制的某种组合。虽然安全系统的自动控制和自动驱动广泛地用于现代核动力厂中，但核动力厂操纵员仍然总体上指挥着核动力厂。

6.2. 一个基本目标应该是，有一个与运行人员的实力和局限性相适应的设计。在人-机接口的设计中应该注意核动力厂运行人员的任务和责任，以便实现运行人员与核动力厂间的有效接口。不仅应注意这些操纵员，还应注意维修人员、检查人员，以及在核动力厂的行政人员和应急人员。

6.3. 为有助于确定信息显示和控制的设计原则，应该注意到操纵员的双重作用：既是包括事故管理的系统管理者，又是设备操作者。

6.4. ‘设计要求’规定（参考文献[1]，第5.54段），承当系统管理者角色的操纵员，要得到使其能完成下述工作的信息：

— 在核动力厂所处的无论哪种工况（正常运行、预计运行事件或事故工况）下，迅速评定核动力厂的总体状态，并迅速确认所设计的自动安全动作正在完成；和
— 确定要采取的操纵员触发的合适的安全动作。

6.5. ‘设计要求’规定（参考文献[1]，第5.55段），承担设备操作者角色的操纵员，要得到足够的与核动力厂各系统和设备相关的参数信息，以便确认能有效完成必要的安全动作。

6.6. 概括地说，因为在现代核动力厂中典型地配备给仪表和管理的参数和设备很多，应仔细注意人-机接口的设计，以确保操纵员需要时能够得到全部所需要的信息。同时，操纵员不应由于人的感知、认识和记忆等人为能力上的局限性可能难以消化的大量数据而被压倒。同样，在涉及操纵员触发的控制动作的系统设计中，应该仔细地注意减少人为错误发生的可能性，以及确保所设计的系统应对可能发生的错误是坚固的。

6.7. ‘设计要求’规定（参考文献[1]，第5.50段），对人为因素和人-机接口的系统化考虑，要在设计开发早期阶段就纳入设计过程，并且在整个设计过程中继续考虑，以确保适当的和明确的区分运行人员与所提供自动系统之间的功能。

6.8. 应该确保向核动力厂操纵员和维修人员提供了解核动力厂状所必需的信息，以便使他们能够完成他们的任务。在设计最早阶段开始实施人因素工程计划，是实现该目标的有效方法（见第7.6段至第7.10段）。

6.9. 与仪表控制系统有关的设计、培训、运行程序和小组组织应以一种综合的设计循环的方式（例如，以这样一种方式，即能分析计算机化的人-机接口的使用对操纵员行为的影响方式）考虑。有关这些考虑的详细讨论超出本安全导则的范围。其他的安全标准将提供有关总的人因工程设计过程的指导。

6.10. 操纵员与核动力厂的接口主要设在主控制室、技术支持中心、辅助控制室和应急控制中心。这些设施装备有安全有关显示器、安全有关控制器、事故监测系统、报警器和历史数据系统。有关这些设施和系统的设计指导在本章提供。

主控室

6.11. 完成安全有关控制操作的主要场所是主控制室。‘设计要求’规定（参考文献[1]，第6.71段），要提供这样一个控制室，在其所有运行状态下都能从这里安全地运行核动力厂并将核动力厂保持在安全状态，或在预计运行事件、设计基准事故和严重事故发生后能在这里采取措施使其返回安全状态。此外，能够从主控制室中采取一些用于缓解严重事故后果的措施。

6.12. ‘设计要求’规定（参考文献[1]，第6.73段），仪表的配置和显示信息的方式能向运行人员提供有关核动力厂的状况和性能的充分全面的图画。在控制室设计中，要考虑人因工程因素。

6.13. 控制室功能设计的主要目标是，向操纵员提供所有运行状态和设计基准事故工况下有关核动力厂设备和系统的状态的准确的、完整的和及时的信息，以及优化操纵员在核动力厂监测和控制中进行的活动。在主控室的设计中，应该考虑有关功能隔离、实体分隔和人因工程原则的要求。主控室是安全系统、安全有关系统和非安全重要系统仪表控制单元会聚的中心。

6.14. 在控制室设计中，应该考虑如工作负荷、人为错误的可能性、操纵员响应时间以及操纵员的体力和脑力工作减到最低限度等人因工程因素，以便在所有运行状态和设计基准事故工况之后为保证安全而规定的运行程序的执行。应该采取必要措施，以确保有令人满意的工作环境条件，包括照明条件、温度和湿度条件，并且避免危险的条件，例如不可接受的辐射水平，或控制室空气中的烟雾或有毒物质。因为一般在所有核动力厂运行工况中都使用安全有关的显示器、报警器和控制器，所以控制室的设计应该包所有假定条件的平衡的考虑。应在多数场合使用安全有关控制器的自动动作，以便在完成安全功能方面不对操纵员造成不合理的负担。人因考虑已导出某些设计目标的规格说明，其中更为重要的如下：

— 借助于显示器和仪表的信息显示应统一为协调的布置，使操纵员能最佳地了解核动力厂的状态和优化控制核动力厂所需要的活动；
— 当正被控制的过程涉及多重的或多样的显示器作为确定信息的手段时，应尽可能安装和配置其他的信息源，使操纵员能不费力气地使用这两类源得出结论，同时不损害这些信息源要求的独立性；
— 主控制室显示器的布置应该使操纵员能够容易地观察这些显示器，并确定任何系统的状态；
— 控制装置及其功能相关的显示器，应尽可能地放在便于操纵员操作的地方；
— 应该注意，有必要使操纵员对核动力厂状态有一个全面的了解，并应注意对控制室内各种人员显示信息的一致性；
— 一些显示器可能显示源于不同合格水平（即可信性）的仪表参数；在这些情况下，应该使操纵员易从显示器上看到合格水平的差别。

辅助控制室

6.15. 除主控室外，还要使用各种类型的辅助控制室和控制场所。虽然在名称细节和功能分配上成员国间有差别，这些其他的控制室和控制场所包括：

— 应急控制室，
— 次要（二级）控制区，
— 安全停堆盘，
— 辅助控制室，和
— 其他就地控制站。

进一步的信息可在参考文献[4]中找到。下面提供有关设计的指导。

6.16. ‘设计要求’规定（参考文献[1]，第6.75段），最好是在实体上和电气上与主控室分隔的单一场所有足够的仪表控制设备可供使用，以便在主控室已经丧失完成这些重要安全功能能力的情况下，能使反应堆置于和维持在停堆状态，排出余热，以及能监测重要的核动力厂变量。

6.17. 核动力厂的设计基准应该界定这样的一些条件，由于敌方接管、火灾或其他可能要求放弃主控室的原因，不再可能从主控室完成控制功能。

6.18. 应采取适当措施，使主控制室一被放弃便将优先控制转移到一个新的场所，并且隔离主控制室中的设备。

6.19. 核动力厂的设计基准通常是这样的，一个假设始发事件引起的主控室可用性的丧失是极少发生的。因此，当主控室不可用，而必要的安全功能正在辅助控制室中完成时，不必假设会出现第二个假设始发事件。

6.20. 如果设计基准规定要考虑对主控室中设备的损伤，那么独立性要求应该适用于这些区域馈电的电路，以便以一个区域中的假设始发事件引起的那些故障，例如短路、断路和高电位，不妨碍另一个区域中所要求安全任务的完成。根据事件的性质和核动力厂的设计，也许有必要为每个区域安装多重的仪表通道、逻辑通道和其他安全设备。在使用共同安全驱动设备的场合，在设计基准中应该规定控制点信号的优先级。

6.21. 辅助控制室的设计应该提供措施防止未经授权的接近和使用。

6.22. 来自辅助控制室的手动控制通常应该由操作一个开关或按一个按钮之类的简单操作完成。在实际可行的范围内，显示器和控制器应该与主控室中的相类似。

6.23. 主控室和辅助控制室的设计应该是这样的，不能使任何一个假设始发事件同时影响主控室和辅助控制室达到使其不能完成所要求的安全功能的程度。

6.24. 应该确保，不是主控室就是辅助控制室能够得到触发一个特定安全功能所需要的优先权。

6.25. 在辅助控制室设计中，应该考虑本安全导则其他章节的适用部分。应该适当地考虑辅助控制室和主控室在目的和使用方面的差异。

6.26. 应该根据假设始发事件的性质，考虑提供与主控室中仪表通道独立的仪表通道。在必要的场合，还应该考虑对安全系统的支持设施的特定需要。

6.27. 设计中还应该考虑如何确保提供一个相当合格的出入途径，以便允许放弃主控室的那些操纵员能够安全地和方便地转移到辅助控制室。

6.28. 沿着从主控室到辅助控制室的这条合格的出入途径，应该提供潜在危险（例如烟雾）的适当指示和相应的对策（例如呼吸面具）。

6.29. 辅助控制室的定位和配置应该使操纵员能够在一个可接受的时间范围内在新的场所开始执行其任务。

6.30. 如果安全分析表明长期逗留将是必要的，则应该利用例如通风手段来确保可居留性。还应该提供足够的座椅、书写和接触文件的手段，以及用于放置文件的地面空间。

应急响应设施

6.31. 对核动力厂运行状态和设计基准事故工况，主控室是操纵员的信息和驱动中心。在应急时，它也可能用做初始阶段指挥厂外活动的主要中心。不过，厂外应急响应运作不应该损害主控室工作人员实施事故管理程序的能力。因此，应该做出安排，以便尽可能快地将小组指挥或厂外通知和协调之类应急响应的非运行方面从主控制室转移出去，并且在发生紧急事件时，限制出入主控制室。

6.32. ‘设计要求’规定（参考文献[1]，第6.87段），要提供一个与核动力厂控制室相分隔的厂内应急控制中心，作为紧急情况发生时应急工作人员的会议场所，他们将从那里进行运作。这个中心应提供有关核动力厂重要参数和核动力厂及其附近地区环境中重要放射性状况的信息。这个中心也应该提供与主控室、辅助控制室和核动力厂内其他重要场所，以及与厂内和厂外应急响应组织的通信手段。应该要求采取适当的措施，以保护应急控制中心的控制人员在长时间内免受严重事故造成的危害。

6.33. 除为管理事故所做的就地安排外，一些成员国还发现，建立一个远离厂区的协调专家所提建议的应急支持中心，是一种有效的办法。同样，应该为这样的设施提供适当的信息和通信系统。

6.34. 有关应急响应设施的进一步的信息，可在参考文献[4，13]中找到。

控制设施

6.35. 如果安全重要设备能够从主控制室和主控室以外的场所进行控制，那么实际的控制源应该在每个控制场所以可视手段（光字牌、可试验指示灯、手开关位置）进行自动指示。

6.36. 控制室应该包括处理那些有下述性质的事故工况所需的一切控制器：

— 性能可能受事故工况限制的设在主控制室外的必要的控制器，和
— 对处理事故工况的时间限制可能使操纵员不能离开控制室去操作其他场所中的控制器。

6.37. 应该提供照明、通信设施和消防设施之类的适当服务功能，以便使核动力厂的运行工作人员能够在任何假设始发事件后解释监测显示结果并采取正确的安全动作。

6.38. 在控制设施的设计中，应该基于为核动力厂规定的起因于外部和内部的假设始发事件，考虑诸多非仪表控制的方面，例如放射防护[12]、可居留性[8]、针对闪电的防护、消防措施[6]、可达性和接近控制、飞射物防护[7，8]和抗震能力[14]。

6.39. 对安全，尤其是对预计运行事件或设计基准事故工况下的安全而言，主控室、辅助控制室、核动力厂的其他适当的场所和厂外应急响应机构之间的口头通信是重要的。一般应该为这种通信提供两条最好是种类不同的通信线路。这种通信设备应该是与仪表控制系统在电磁上兼容的（带自备能源的电话、用电池作电源的电话、手持无线电话）。这些通信线路应该这样敷设，即火灾、电气系统的故障或别的可适用的假设始发事件不可能同时使这两个系统失去能力。

显示器

6.40. 显示器向核动力厂操纵员提供有关核动力厂状态以及电厂所要求系统和设备状态的信息，以便监测、维修和运行安全重要系统并将核动力厂保持在其设计基准包络线内。显示器用来完成下述功能中一种或多种：

— 向核动力厂操纵员通报各系统的状态和核动力厂的安全状态；
— 向厂内和厂外安全专家通报处于事故工况中的核动力厂的安全状态；和
— 提供有关安全重要的过程变量随时间变化的行为信息，以便用于立即的或随后的分析，并用于向运行组织内部和向外部主管部门的报告。

6.41. 应该通告安全系统状态的变化，并且应该在主控室显示这种状态。

6.42. 在正常运行中，操纵员利用主控制室中配备的一套显示器和光字牌或可视装置持续不断地监视核动力厂的状态。报警器或其他装置用来指示与正常运行的偏离。当偏离发生时，应该向操纵员提供必要的信息，以便其：

— 识别正由自动系统完成的动作；
— 分析发生扰动的原因；
— 跟踪核动力厂行为的发展趋势；和
— 完成任何必要的手动操作。

6.43. 显示设施应该覆盖相应的变量，即与安全分析的那些假设并与操纵员所需要的有关运行状态和设计基准事故工况的信息相一致的变量。显示的精确度和范围应与安全分析的假设相一致。

6.44. 在多重显示器用来满足可靠性要求的场合，这些显示器在功能上应是隔离的，在实体上应是分隔的，例如通过使用多画面显示装置的两个键盘，确保这个系统中发生的单一故障将不导致被监测变量的信息的完全丧失。

6.45. 在单一信息显示通道发生的故障可能导致信息变得模棱两可的情况下（例如引起一对多重显示器不一致的单一故障），这个故障有可能使操纵员受挫折或不能完成所要求的安全功能。为避免发生这种情况，应该提供一些使操纵员能够解决信息中这种冲突的额外手段。做到这一点有多种方法可用，例如通过提供信息的第三个通道，或通过显示与那一对有问题的显示通道有已知关系并能判定故障通道的另一个变量。在探测和修复故障显示通道或探测和更换故障显示通道所需要的平均时间比容许停用时间短的场合，带有可明确判定故障模式的单一显示信道是适当的。

6.46. 在了解一个变量的趋势对确定操纵员的相应操作是十分重要的情况下，应该提供显示这种趋势的手段。

6.47. 如果有意使一个安全重要系统的一部分不能工作，而所使用的是设计中专门为此目的提供的设施，则这种情况应自动在主控室中显示。如果一个安全重要系统的一部分已通过行政上可以控制的手段使其不能工作，这一点也应明确在主控室中显示。

事故工况监测

6.48. 应该提供有关核动力厂状态和核动力厂关键参数的变化趋势的可靠的、易看到的和可理解的信息显示，以便确保操纵员能够有效地处理事故工况，以及被要求提供帮助的支持人员充分地了解情况。有关事故监测系统和设施的设计建议，在下述诸段中提供。

6.49. 在主控室以及必要时在辅助控制室中应安装用于监测核动力厂事故工况的信息显示器。

6.50. 在决定要显示哪个信息时，应该考虑操纵员的下述需要：

— 识别与正常工况的偏离；
— 确定发生的特定事故，并在可能时识别其始发事件；
— 核实所要求的安全功能正在执行；
— 跟踪事件或事故进程；
— 确定什么时候工况发展到有必要由厂外有关主管部门采取应急措施；
— 解决可能从多重显示通道中产生的信息冲突。

6.51. 为了能确定所要求的安全功能是否正在执行，监测事故工况的设备应设计成使操纵员能够确认：

— 反应堆已停堆并且将保持在停堆状态；
— 堆芯和其他安全重要物项的余热正在排除并且将继续排入最终热阱；和
— 用来防止放射性向环境释放而设计的任何屏障处于适当位置并将继续留在该位置。

6.52. 为这种确认而监测的核动力厂参数，应该是与反应堆的设计和选址相称的那些参数。

6.53. 需要时和在需要的时间间隔内，监测事故工况的设备应能够在事故后的环境中运行。所选关键参数的测量范围应扩展到事件可能威胁屏障时可达到的数值，这些事件将导致放射性物质从燃料、主系统或安全壳，或者从一个或多个屏障物中释放出来。

6.54. 用于事故后监测的显示器应该与其他显示器不同。

6.55. 在事故分析或应急措施需要使用历史资料时，应该提供相关数据记录和检索的能力。

6.56. 在核动力厂中应该提供这样一些设备：它们将足够的数据传递到参考文献[13]中所规定的那些应急设施，同时不对在紧急情况发生时主控室活动产生不适当的干扰。

报警系统

6.57. 使用可视和音响报警系统，使运行人员注意需要对电厂运行进行干预，例如通过手动触发安全功能或启动核动力厂控制或维修动作，以确保核动力厂的状态维持在其设计基准包络线内。下述各条导则适用于与安全重要系统相关的报警应用。

6.58. 应该以及时的，与操纵员操作的根本要求相一致的方式，在适宜的场所提供适当的可视和音响警报。

6.59. 在报警系统设计中，应该适当注意确保最重要的信息能够有效地被操纵员判别出来，尤其是在可能涉及大量报警的预计运行事件和事故工况期间。可用多种技术来实现这个目的，包括报警的分组、优先次序排列和调整，以及利用音响的或图象的差异以区分不同类型和优先次序的报警。

6.60. 不应以导致删除确定故障位置和潜在后果所需信息的方式而使用为防止报警信息加重操纵员负担的技术。

6.61. 应该提供使操纵员能及时地确认单个或成组报警的手段。

6.62. 音响报警信号一般被用来引起操纵员对新的报警状态的注意，应该提供用于抑止这些听觉信号的手段，以避免听觉过载和有利于识别出可能随后发生的新报警。如果一些报警被抑制，这些报警状态的可视显示应该持续到潜在的故障状态已被排除，以确保这些状态不被忘记。应该使用一些可视手段（颜色的变化或从闪烁到不闪烁的变化），将已确认的报警状态与尚未确认的报警状态区分开。当核动力厂状态恢复到正常状态时，报警显示应该持续到被操纵员复原为止，以便保持有关报警的信息。

历史数据记录系统

6.63. 应该提供记录来自核动力厂重要工艺过程中的核动力厂实绩和行为历史数据的记录、存储和检索能力。这样的历史数据系统一般提供下述支持：

— 供值班操纵员使用的备用信息（给出短期和长期趋势）；
— 供核动力厂管理者使用的总的运行信息；和
— 对运行和事故的短期和长期诊断和分析。

6.64. 传统上，硬拷贝系统（数据的纸打印输出）一直被用于这些功能。不过，应考虑使用一些以计算机为基础的系统，因为这样的系统将使一般涉及大量数据的存储、检索和处理变得效率更高。通常，在使用以计算机为基础的系统的场合，应该合适地设置打印机，以便使用者能够打印出硬拷贝。

6.65. 应该酌情在主控室内及其周围设置一些用于存取历史信息的终端。为供工程支持人员使用而合适地设置远距终端设备是有益的，也是应该考虑的。在就终端位置和历史数据存取的人-机接口设计做决定的过程中，应该考虑使用者的需要、职责和能力。

7. 安全重要的仪表控制系统设计程序

7.1. 核电工程是涉及许多技术学科的复杂活动。为确保设计按要求交付，对每个学科而言，在一个项目的适当时间提供正确的信息是必要的。对于安全重要系统，应该使用包括若干保守的设计措施和合理的工程设计实践的结构化开发程序，以确保‘设计要求’[1]被正确应用。因为使用一种组织得不好或管理不善的程序就作不到这样，就可能损害核安全。

质量保证

7.2. 为达到所要求的质量标准，重要的是确保安全重要的仪表控制系统，是根据一份由设计者、制造者或安装者编写并被相关的主管部门认可的质量保证大纲进行设计、制造、质量鉴定、检验、安装、运行、试验和维修的。这份大纲应该符合相关的法规和安全导则（参考文献[3]，安全导则Q3和Q10）。

7.3. 质量保证大纲应该包括下述所需的全部活动：（1）验证安全系统设计的适当性和（2）确保安全系统符合所有适用的标准和要求。

项目计划

7.4. 为了保证设计所需的元件及时和商业上可行地交付，应使用项目管理和项目规划技术。在推动完成一个项目的计划活动中，应该考虑被设计系统的安全要求。在项目进度表中，应为向监管部门提交安全重要系统设计的文件留有足够的时间。

变更控制和配置管理

7.5. 在整个设计过程中，从构思到进行，在任何迭代中，都应该对任何变更实施控制，以便设计的配置得到管理。有关做出设计更改的程序应该写成文件，应该寻求书面认可，以便确保所建议的变更得到适当的考虑，而能由独立于设计者的人员对其影响加以评定。在设计的早期阶段，为确定所要求的设计，多次重复可能是必要的，因而，往往用于管理变更的方法变得不大正规。在这些情况下，应该进行定期的设计审查，以确保能使设计小组以外的适当人员了解设计进展，并证实安全要求是否继续得到满足。不过，一旦决定支持一个特定的设计，就应该有控制设计变更的正式程序。

人因整合

7.6. 因为操纵员和核动力厂其他人员在安全重要的仪表控制系统（以及整个核动力厂）的运行和使用中起着广泛和重要的作用，因此人因过程应该被整合到总的设计过程中。

7.7. 适用的人因技术包括功能分析、任务分析和工作负荷分析。这些技术被用于人－机之间的功能分配和人-机接口设计中。有关人因工程学的指导，尤其是有关人体测量学、人为错误、用户接口的设计，以及各种其他相关问题的指导，现已可供使用。为利用这种知识，应该对人因给予系统化的注意（见第6章）。

7.8. 应该遵守有关人因的适用的设计原则或要求，以确保所设计的人-机接口与使用者的相容性、易理解性和有效性。系统设计过程应该包括用户小组反馈和对人-机接口验证及确认的适当措施。有关人因的工程计划（如第6章中所述的）应该包括在总的项目计划中。在工程设计过程中，应该遵循适用的工程设计导则和有关人因的参考文献，与人因有关的分析和结论应系统化地提供佐证文件。

7.9. 在设计的最初阶段开始时需要促进对人-机接口设计选择的评价工作，起初，应该用实体模型和计算机形象化辅助手段。在设计的后期阶段，应该使用一个全规模控制室模拟器来确认主控室的设计。

7.10. 设计应该考虑系统用户方面发生人为错误——因疏忽错误和命令错误的可能性。为将用户错误引起严重不利后果的可能性降到最低，在可能的范围内，设计中应该这样安排人-机接口，即操纵员方面的单一错误是无关紧要的，并且是可探测的和可纠正的。其中，人为错误有较高发生可能性和较大不利后果的那些情况，应该借助于适宜的系统结构或用户接口的设计、或用自动装置加以避免。

设计过程描述

7.11. 安全重要系统的开发应该是一个循序渐进的控制过程。在这种方法下，开发过程形成一套有序的性质不同的阶段。每个阶段使用在较早一些阶段中产生的信息，并且提供作为以后阶段输入使用的输出信息。请注意，安全重要系统的开发就其本质而言，是一种重复过程。随着设计的进行，在较早一些阶段中发生的错误和疏忽将变得明显，因而将使若干重复成为必要。这种方法的一个重要特点是，每个开发阶段的产物都应该对照前阶段的要求加以验证，以确定设计是正确的。在开发的某些阶段，应该进行确认活动以便证实输出（特定阶段的产物）满足所有的功能的和其他的要求，并且不存在任何不希望的特性。验证及确认的活动应该由独立于设计者和开发者的小组来进行。

7.12. 图4是一个系统化的开发过程的典型阶段和本安全导则中描述的那个过程的示意图。各方框所示为应该被完成的开发活动，而箭头所示为预计的顺序和主要信息流。图5表示验证和确认活动与要求以及设计和实施的各个阶段的关系。图5和本安全导则中对特定开发活动及其顺序所作的这种选择，并不打算规定一种特殊的开发方法；其他有所变更的方法可能同样能够满足本安全导则就有关原则和属性提出的建议。

7.13. 一座核动力厂的全部设计，一般从该核动力厂的机械系统和工艺过程系统以及部件的设计开始。接着，应该在所选定的设计基准事件（见第3章）安全分析（确定论和（或）概率论）的基础上，开展仪表控制系统的设计工作。设计程序应该包括为拟订所选定的设计基准事件清单开展的一个系统化的过程，这是由于一些疏忽可能导致安全设备不正确要求的技术规格书，因而导致一个不安全系统的形成。

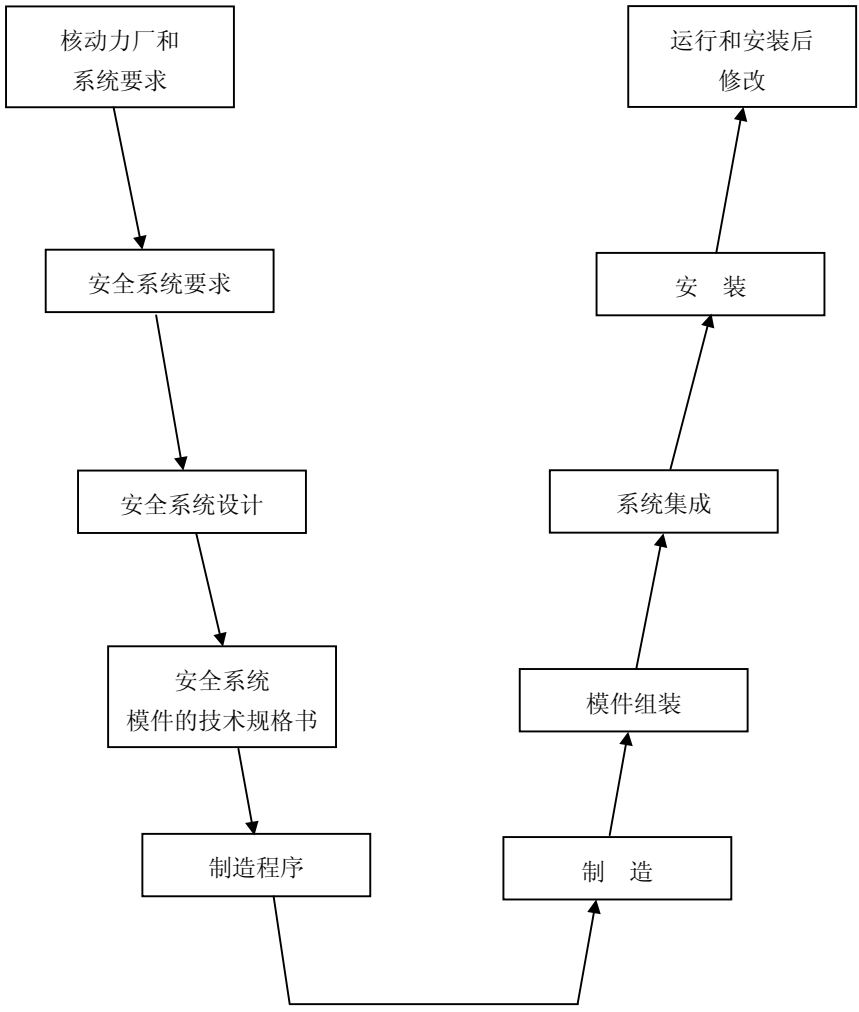

图4.　安全重要仪表控制系统的开发。

7.14.　应该在这些分析结果的基础上得出对安全系统的要求。在适当的情况下，核安全和其他工程学科的专家应该对确定安全系统的要求做出贡献。通常，对初始设计作一些变更是必要的，于是一个新的设计产生，接着又要进行安全分析。在完成几次重复之后，便得到其中所有现行核安全要求都满足的机械、工艺过程系统和仪表控制系统的配置。

7.15.　一旦设计已开发到人们知道将如何满足要求，核动力厂主要的系统和部件将如何配置的阶段，设计文件通常便作为采购用技术规格书发出。在商订核

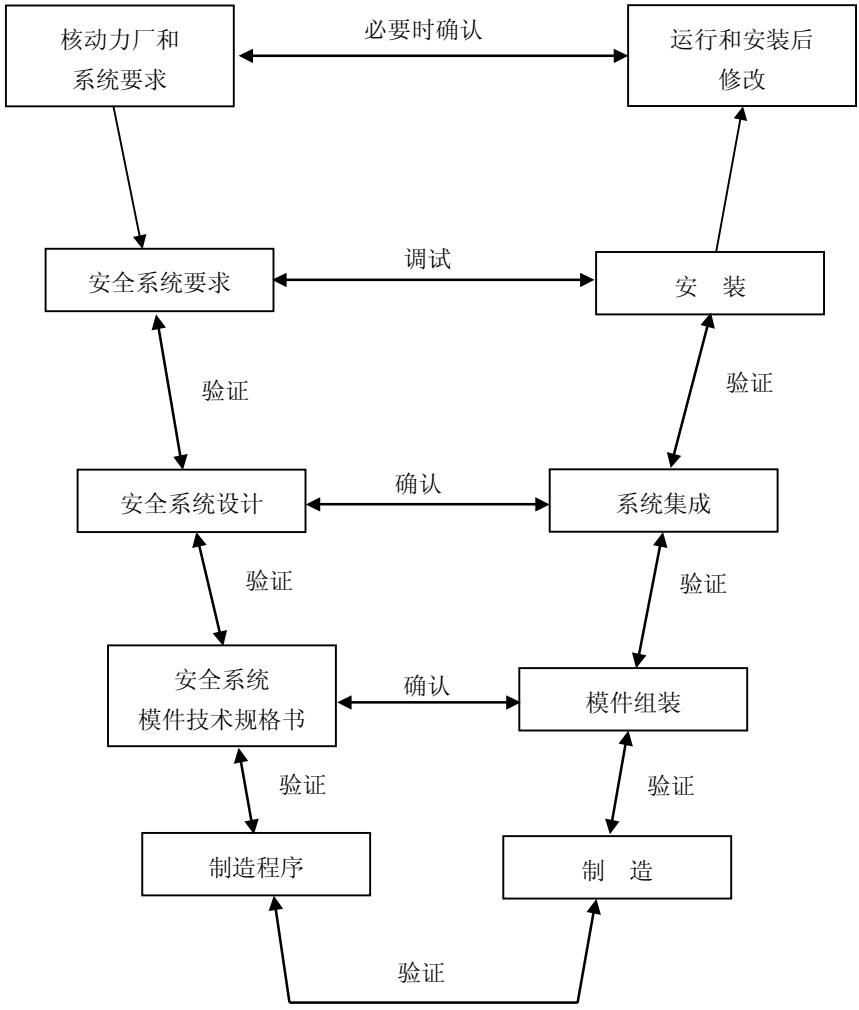

图5.　验证、确认和调试过程。

动力厂系统和设备的采购合同的过程中，设计者应该建立一种通信手段，它将确保供应商提出的实施方案能证明满足系统的要求。设计者和供应商应该确定有效的验证和确认活动。

7.16.　一旦确定了安全级仪表控制系统的要求，该仪表控制设计者便将通过为安全级仪表控制系统编写设计要求来陈述将如何满足每一项要求。如果提出的

是一个以计算机为基础的系统，那么设计者应该编写这个计算机系统要求，并且应该确定系统结构和要完成的功能。同样地，还应该确定人的和（或）机器的功能分配。在这个设计阶段，对设计的哪些部分，能依靠容易取得的技术，以及哪些部分需要用特定的精力去开发，将变得很清楚。在需要开发工作和制造样机的场合，设计过程的其他模式（例如螺旋型模式）可能更有效。

7.17. 当实现仪表控制设计和设备的模件（模块）变得可供使用时，这些模件（模块）应该进行一系列检查和试验，以便证明各模件或子装置能像所要求的那样进行工作。这被示于图5中。通常在这个阶段，设备鉴定试验从模件或子装置这一级开始，而一般试验或型式试验在用于多种用途的设备上进行。然后各单个模件集成为用于完成设计者所要求功能的分系统。应该进行针对具体设备配置的进一步的试验，以便证明这些模件在其被要求的分系统中是一起发挥作用的。接着，组合或集成这些分系统，以允许在供应商的设施上对系统进行一系列“工厂验收试验”。这些试验应该证明，设计者所要求的系统功能已正确实现。

7.18. 一旦设计者对系统在供应商的设施上完成所要求的功能表示满意，设备便运输到核动力厂并进行安装。运输或安装本身可能影响设备的性能，因此安装后应该对设备进行全面试验。这些安装试验和‘竣工试验’，除重复最后的工厂验收试验外，还应该确保整个系统是在其实际运行条件下进行试验；例如，多个多重系统应该在其一起工作时试验，而不应利用一些模拟信号进行试验。对于一个需要长电缆敷设的系统，要求在进行性能竣工试验前完成电缆敷设往往不是实际可行的。在这些情况下，为慎重起见，一旦完成对系统所有不同类型连接件的有代表性的选择，便应该完成各种试验。这样，将容易确定接口的任何一般问题，并能有效地解决。对完全装好电缆的系统，应该进行最后试验。这时，能够调试和证明系统如所要求的那样完成功能。在可能的范围内，仪表控制系统应该在要求该仪表控制系统运行的其他调试活动开展之前调试和运行。

升级和改进

7.19. 为确保核动力厂持续提供可靠的动力并且满足现行的安全标准，应该对仪表控制系统定期实施现代化。核工业在为其在20—30年以前设计和生产的硬件模拟仪表控制系统寻找备件方面已经遇到问题。设备的实体老化加上缺少备件，已经使故障率上升并使运行和维护成本增加。此外，许多供货厂商已经减少其对模拟系统的支持——并且可能存在一些原来供应商不再营业的情况。由

于数字电子设备的可靠性在近几年中已有很大改善，许多核电公司已经决定用计算机化的系统代替老的模拟仪表控制系统。

7.20. 数字技术中的进步为升级提供下述额外激励：

— 能够完成更复杂的功能；
— 能够达到更高的精确度；
— 能够编辑和应用更大量和更多样的信息；
— 用户接口能做得适应性更强；
— 系统能够更容易地探测和处理预计内部故障；
— 在无实体改变或甚至无实体接近的情况下能够完成功能改变；
— 一些已知可靠性的标准处理机能够用于多种应用。

7.21. 当一个计算机化仪表控制系统是一项改进或一项升级的一部分时，应该考虑它在确保核动力厂的安全方面的功能。这个仪表控制系统的安全级别，应该根据第2章中介绍的准则加以确定。有关系统可靠性、质量鉴定和质量保证的要求，以及其他要求，将根据安全级别加以确定。

7.22. 出于实用上的考虑，作为第一步，应该完成现有系统的技术规格书和新的或更改了的系统需求的技术规格书。现有模拟系统的设计文件可能缺少完整性和准确性。可能需要完成某种程度的‘反向的工程设计’以便根据设计实现重新形成设计技术规格书和要求。

7.23. 应该权衡更改操纵员接口和（或）控制策略带来的好处与可能的成本。加强操纵员接口可能需要对盘面进行广泛的修改，并且需要对操纵员和维修人员的再培训。此外，在选择一个操纵员接口之前，应该咨询控制室操纵员。他们也应该在开发过程的不同阶段，向设计小组提供反馈意见。

7.24. 关于仪表控制升级的详细信息，可从参考文献[15,16]获取。

安全系统要求的分析

故障分析

7.25. 在安全系统设计过程的适当阶段应该完成一些分析，以便验证重要分系统（保护系统、安全驱动系统和安全系统支持设施）的组合能够持续地满足本安全导则有关单一故障（见第4章）和共因故障的建议，以及对安全系统的可靠性的任何其他要求。这应该包括为证实故障安全设计所要求的故障模式分析。这些分析应编制文件。

试验措施评定

7.26. 应该完成对最终设计的评定，以便验证对保护系统、安全驱动系统和安全系统支持设施的试验措施的适宜性。评定的结果应编制文件，最终设计那些对系统试验和设备试验的任何方面发生的设备故障或人为错误敏感的领域，应该在该文件中明确。

可靠性分析

7.27. 在一个已决定在安全系统或其部件的可靠性方面使用数值要求的成员国中，应该使用可证明的合适的部件故障率和平均修复时间，完成适当的定量可靠性分析，以便：

— 考虑设备随机故障；
— 考虑共因故障，包括人为错误；
— 确定安全系统部件可靠性的相对重要性；
— 确定与适用的部件故障率和系统可靠性要求相一致的初始试验时间间隔；
— 在核动力厂运行过程中证实故障暴露率与假设的数值一致，可靠性目标正在达到；
— 如果实际故障率超过或达不到假设的设计故障率，则确定要采取的行动，例如缩短或延长试验的时间间隔，或更换妨碍达到可靠性目标的那些部件。

7.28. 这个分析结果，以及定期试验结果，在役可靠性评定结果和完成的任何补救行动，均应编制文件。

概率安全评价

7.29. 在设计中应该考虑从概率安全评价（PSAs）中得到的知识，以便确保没有具体的设施会对总风险产生不成比例地大的或不确定的影响。有关概率风险评价的详细信息，可从参考文献[17—20]中获得。

分析中所做的假设

7.30. 设计验证要求进行的任何分析中所做的假设，应该包括在分析文件中。应该陈述每个假设，并证明它是正确的。

仪表控制系统的文件编制

7.31. 编制仪表控制系统文件的目的是：(1) 提供在设计过程中所涉及不同阶段及其不同方之间传递信息的手段；(2) 提供一个表明要求已正确地解释并在所安装的系统中正确实现的记录；(3) 将运行上极其重要的设计相关信息传递给核动力厂操纵员；(4) 为核动力厂维修和对设计可能的未来修改提供一个基础。

7.32. 对一个安全重要仪表控制系统而言，将在与设计过程相关的诸多活动中产生大量文件。为确保人们对这些文件的意义的认识，它们应该按其在设计过程所起的作用加以分组。

7.33. 一次文件是这样一些文件：它们对设计过程是完整的，并构成每个阶段的输入文件和输出文件。这些文件中的一个错误能够直接导致相应系统本身发生一个故障。一次文件一般包括为核动力厂安全分析编写的设计基准文件、安全系统要求文件、逻辑框图和竣工图。

7.34. 二次文件是这样一些文件：它们随着设计过程的进行而产生，并且被设计者用来编写输入文件和输出文件。虽然这些文件的一个错误将不直接导致相应系统发生一个故障，但是它们有可能通过信息的不正确报告而掩盖一个错误的存在。另一方面，按照文件中的错误建议行事有可能将一个故障引入相应的系统中。一般，二次文件规定和记录与设计过程有关的活动，例如不同阶段之间的验证和确认活动。验证和确认记录在发现故障的情况下，用于决定是否有必要更改其相关阶段的文件。

7.35. 在质量保证大纲、项目计划和设备鉴定中产生的其他文件支持设计过程。这些支持性文件有助于做出有关设计过程组织的、逻辑的和战略的决定，这些决定能够对设计产生间接影响。

7.36. 安全重要的仪表控制系统的设计，应该在其完成期间被充分地写成文件。这份文件应该是全面的、完整的、可追溯的和可验证的，以便证明系统所要求的功能度和可信度。合适的文件将使系统的未来更改或现代化变得容易。

7.37. 当仪表控制系统的设计完成时，最终设计文件应该包括一份设计、设计验证和设计确认的相关文件的清单，并且应该包含有关这些文件的特定参考文献。

7.38. 应该随时更新仪表控制系统的文件，系统所经历的任何修改都应该在文件中得到反映。仪表控制系统的所有文件都应该保持在配置管理下。

法规和标准

7.39. 一份适用于安全重要的仪表控制系统设计的导则、法规和标准以及相关的遵从指令的清单，应该在项目开始之时商定一致，应该写成文件，并且在项目实施过程中传递给项目监管部门。

设计基准文件

7.40. 最终设计基准应写成文件。它最低限度应该包括对下述诸项的标识和文件：

— 系统在其中可运行的那些核动力厂运行状态；
— 预计运行事件，对仪表控制系统的相应的安全和保护任务的识别，以及初始预计运行事件工况和为每个这样的事件规定的核动力厂工况的允许限值；
— 为手动或自动(或以两种方式)控制每种保护动作而被监测的那些变量，或变量的组合；
— 应由安全重要仪表控制系统调节的那些变量或变量组合的量程和变化率；
— 在每一种适用的核动力厂运行模式下，这些变量中的每一个与安全系统驱动相应的限值；
— 在涉及过程变量和其他重要参数的允许值方面对控制系统施加的限制。

7.41. 在一个设计基准事件发生后，那些支配系统动作的时间关键点或核动力厂工况关键点应该写成文件，其中包括：

— 要求触发安全功能的时间或核动力厂工况；
— 要求自动控制的安全功能被启动的时间或核动力厂工况；
— 确定正确完成安全功的时间或核动力厂工况；
— 允许安全系统恢复到其正常备用状态的时间或核动力厂工况。

7.42. 用来确定安全系统设计的可靠性对每一种安全系统功能都是适当的方法，以及可能纳入该系统设计的任何定性的或定量的可靠性目标，都应该写成文件。

7.43. 对系统设计有影响的任何与限制有关的特定带宽（例如所要求的采样速率和数据传输率）都应该写入文件。

7.44. 对所识别的、其运行从开始或触发之后可能由手动方式控制的每种保护任务，下述诸项应编制文件：

— 允许手动控制的时间和核动力厂工况；
— 允许只用手动方式触发，或触发后进行控制的理由；
— 在其中要求执行手动操作的核动力厂运行状态和事故工况期间，施加于操纵员的环境条件的范围；
— 正如前面所述，为使操纵员在完成手动动作中能够加以考虑的那些要求显示的变量。

7.45. 应为要求安全重要系统完成功能的那些核动力厂运行状态和事故工况，确定安全系统支持设施的瞬态和稳态条件（例如电压和频率）的范围，并将其写成文件。

7.46. 对核动力厂运行状态、事故工况，以及外部事件，应将要求安全重要系统完成动作的系统所处的瞬态和稳态环境条件（例如辐射、温度、湿度、压和振动条件）写成文件。

7.47. 应将在功能上有可能降低安全系统性能的条件及其为保持完成安全功能的能力已采取的应付措施（例如飞射物撞击、管道破裂、火灾、通风丧失、消防系统误动作、操纵员错误、不同安全等级系统中的故障）写成文件。

7.48. 应该确定那些允许旁通安全任务的核动力厂工况，还应描述使这些被认可的旁通能够实现的手段以及重要的旁通指示器。

7.49. 应将系统和部件要遵循的工程设计程序和编制技术规格书的过程写成文件。

仪表控制系统设计文件

7.50. 应将安全重要仪表控制系统的设计写成文件。这份文件应该至少包括以下信息。

功 能

7.51. 每个仪表控制系统都应该如第2章所规定的那样分级。

7.52. 应该将每个系统的设计基准写成文件，包括其安全有关任务、与其他系统的接口以及安全有关任务适用的那些假设始发事件和核动力厂工况。

7.53. 应该将每个仪表控制通道提供的功能写成文件。这包括指示、报警和控制特性的文件，以及适用时稳定性裕度的文件。

7.54. 对保护任务而言，应将有关核动力厂工况和这些工况的一些指标准确和清晰地说明写入文件。

性 能

7.55. 应该提供一个对整个系统和对每个通道要求的范围、准确度和响应时间的描述。

7.56. 应该提供一份论证系统及其部件的质量鉴定、功能特性和其他任何特殊要求的文件。

7.57. 应该成为仪表控制系统设计文件一部分的是，安全重要仪表控制系统中这样一些设备的清单：其性能在核动力厂总的使用寿期可能不满足该系统的功能要求，包括判定设备寿命终止和期望寿命的准则要求。

7.58. 对安全系统（即保护系统、安全驱动系统和安全系统支持设施），应该提供完成要求的安全功能所允许最长时间和所需要期望时间的信息。

7.59. 应该描述第7.25段至第7.28段中明确的那些安全系统分析，并且提及与设计文件有关的参考文献。

质量鉴定

7.60. 应该提供有关每个部件必须在其中工作的那些环境条件的描述，包括正常工况、预计运行事件和设计基准事故工况。

7.61. 应该明确这样一个或多个动力源：在正常工况、预计运行事件和设计基准事故工况下，每个系统都将靠其提供的动力进行工作。

7.62. 应该对每个部件或系统质量鉴定的要求提供验证文件。

试验和维护

7.63. 应该规定一个旨在确保设备所要求可用性的试验、检查和定期维护的时间表。

7.64. 应该详细规定有关试验、维护和检查的要求，以及这类活动可能引起的任何潜在的损害、危险或劣化。

运 行

7.65. 应该描述系统在所有运行状态下的运行原则。描述应详细说明相关的信号和所要求的自动动作或要由操纵员完成的操作。

7.66. 应该提供运行规程和维修规程。

规 程

7.67. 应该提供与系统有关的运行、调试和维修规程。

备用部件

7.68. 对每种部件应该备有采购技术规格书。

7.69. 为了将设计基准维持到未来，应该将备用部件选择的标准和基本理由写成文件。

7.70. 应该满足IAEA质量保证安全标准中为质量保证规定的那些文件编制要求。（欲得进一步指导，请阅参考文献[3]安全导则Q3和Q10。）

文件的组织

7.71. 文件应组成如下的结构：

- 由系统提供的功能及其功能设计；
- 系统的设计特点；
- 系统的试验、诊断和维护设施及其运行；
- 试验结果的文件；
- 设备鉴定；
- 设计程序和设计中所遵守的质量要求；
- 维护策略；

— 试验策略；
— 设计验证和确认方法；
— 系统运行；
— 维修、监督和定期试验大纲；
— 备用件和（或）部件的供应。

安全级仪表控制系统的文件

7.72. 当安全级仪表控制系统的设计完成时，应该将系统的预期功能性能和可靠性写成文件。该文件至少应该包含下述信息：

— 对设计基准、包括来自运行经验审查的输入在内的设计变更的基本理由（如果适用的话）、系统的功能设计和构成设计的具体选择的基本观点的概括描述。
— 对系统的全面描述，描述应该包括有关该系统在所有运行模式下，一切被测变量（过程变量、操纵员信号）和被控变量（向驱动器和显示器的输出）的信息。描述还应该包括数据表示方法（例如硬件实现的方法或以计算机为基础的方法）。
— 对任何接口系统，安全驱动系统、其他的安全有关系统或包括动力源在内的安全系统支持设施的运行特性的任何相关性的细节。
— 为实现保护动作的目的而要监测的那些变量或变量的组合，以及所用的组合方法。要提供的信息应该包括，为恰当监测包括有空间关系（即其测量值作为一特定区域内的位置函数而变化的变量，例如中子注量率）的变量在内的所有安全重要变量所需要的传感器的最低限度数目和位置。应该详细说明上述那些变量或变量组合的计算的范围和变化率。
— 仪表控制通道的数目，它们的功能和输入-输出逻辑，以及有关显示器、报警器和控制器特性的信息，包括安全性、产生信号能力和稳定性的余量。
— 系统的描述应该包括传感器、机箱、机柜、控制盘、操纵员控制器和操纵员显示器以及手动调节和系统试验设施的位置（例如核动力厂网格坐标和高度、房间编号或区域编号）。
— 假设始发事件，及其相应的保护任务和安全任务。
— 为每个设计基准事件提供保护动作监测的那些变量或变量组合。
— 在每种适用的核动力厂运行方式下，包括所有运行的和维修旁通工况下，为每个列出的变量设定的安全系统极限整定值，以及为考虑仪表校

准中的误差所确定的任何修正量。应该确定安全系统整定值与考虑用来标志不安全工况开始的水平之间的裕度，同时为解释提供适当的信息。

— 安全系统完成所有保护任务和安全任务所需要的最大允许响应时间。
— 每种保护任务的可靠性准则。
— 其实现规定完成保护任务的条件。
— 安全系统每个变量或变量组合的标称整定值。
— 安全系统设备的每个物项的范围、寿期和期望准确度。
— 第7.25段至第7.28段中明确的那些设计分析。
— 用以验证对安全系统设备鉴定和功能性能要求，以及任何其他特定要求的文件。
— 安全系统中其性能在核动力厂总的使用寿期中可能不满足该系统的功能要求的设备清单。应该说明用以判断设备寿命终止和期望寿期的准则。
— 安全系统设计适用法规和标准的清单。
— 其中允许确定的安全任务旁通的核动力厂工况（适用的允许的工况，见第5.36段至第5.38段）。

参考文献

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Software for Computer Based Systems Important to Safety in Nuclear Power Plants, Safety Standards Series No. NSG-1.1, IAEA, Vienna (2000).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Quality Assurance for Safety in Nuclear Power Plants and Other Nuclear Installations, Code and Safety Guides Q1–Q14, Safety Series No. 50-C/SG-Q, IAEA, Vienna (1996).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Modern Instrumentation and Control for Nuclear Power Plants: A Guidebook, Technical Reports Series No. 387, IAEA, Vienna (1999).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of the Single Failure Criterion, Safety Series No. 50-P-1, IAEA, Vienna (1990).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Fire Protection in Nuclear Power Plants, Safety Series No. 50-SG-D2 (Rev. 1), IAEA, Vienna (1992).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection Against Internally Generated Events and their Secondary Effects in Nuclear Power Plant Design, Safety Series No. 50-SG-D4, IAEA, Vienna (1980).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, External Man-induced Events in Relation to Nuclear Power Plant Design, Safety Series No. 50-SG-D5 (Rev. 1), IAEA, Vienna (1996).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Ultimate Heat Sink and Directly Associated Heat Transport Systems for Nuclear Power Plants, Safety Series No. 50-SGD6, IAEA, Vienna (1981).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Equipment Qualification in Operational Nuclear Power Plants: Upgrading, Preserving and Reviewing, Safety Reports Series No. 3, IAEA, Vienna (1998).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Emergency Power Systems at Nuclear Power Plants, Safety Series No. 50-SG-D7 (Rev. 1), IAEA, Vienna (1991).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Design Aspects of Radiation Protection for Nuclear Power Plants, Safety Series No. 50-SG-D9, IAEA, Vienna (1985).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Preparedness and Response for a Nuclear or Radiological Emergency, Safety Standards Series No. GS-R-2, IAEA,Vienna (in preparation).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Design and Qualification for Nuclear Power Plants, Safety Series No. 50-SG-D15, IAEA, Vienna (1992).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Modernization of Instrumentation and Control in Nuclear Power Plants, IAEA-TECDOC-1016, IAEA, Vienna (1998).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Specifications of Requirements for Upgrades Using Digital Instrumentation and Control Systems, IAEA-TECDOC-1066, IAEA, Vienna (1999).

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Treatment of External Hazards in Probabilistic Safety Assessment for Nuclear Power Plants, Safety Series No. 50-P-7, IAEA, Vienna (1995).

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 2): Accident Progression, Containment Analysis and Estimation of Accident Source Terms, Safety Series No. 50-P-8, IAEA, Vienna (1995).

[19] INTERNATIONAL ATOMIC ENERGY AGENCY, Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants, Safety Series No. 50-P-10, IAEA, Vienna (1995).

[20] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 3): Off-Site Consequences and Estimation of Risks to the Public, Safety Series No. 50-P-12, IAEA, Vienna (1996).

术 语 表

下列定义适用于本出版物。

事故工况 对正常运行的偏离，比预计运行事件严重，包括设计基准事故和严重事故。

执行装置 用来完成一个或多个安全任务的原动机和被驱动设备的组合。

驱动设备 直接控制执行装置动作能源的设备。例如对电源的配置和使用进行控制的断路器和继电器，控制液体流或气体流的先导阀。

预计运行事件 在核设施运行寿期内预计至少出现一次的偏离正常运行的各种运行过程，由于设计中已采取相应措施，这类事件不致于引起安全重要物项的严重损坏，或导致事故工况。

可用性（利用率） 系统在该期间能完成预定任务的时间份额。

旁通（旁路） 一种装置，例如使继电器的接点短路，有意地但是暂时地，使一个回路或系统停止起作用。

维修旁通（旁路） 安全系统设备在维护、试验和修理期间的旁路。

运行旁通（旁路） 在一个特定的核动力厂运行方式期间某些不需要的保护动作的旁路。[4]

通道 在系统内相互连接部件构成的启动单一输出的一种配置。在单一输出信号与来自别的通道，例如来自一个监测通道或一个安全驱动通道的信号汇合处，一个通道就失去其特征。

符合 保护系统的一个设计特点，为了使逻辑线路产生一个保护动作信号，需要来自若干个通道的两个或更多个重叠的或同时输出的信号。

共因故障 由单一特定事件或原因引起的，两个或多个构筑物、系统或部件的故障。

---

4 当保护动作阻止或可能阻止以所要求的方式可靠运行时，可以使用运行旁路。

部件 系统的一个分离的元件。例如导线、晶体管，集成电路，马达，继电器，线圈，管子，配件，泵，罐和阀。

可信性 用以描述一个系统的总的值得信赖的一般术语；也就是能够合理地信赖这个系统的程度。可靠性、可用性和安全性是可信性的属性。

设计基准事故 核动力厂按确定的设计准则在设计中采取了针对性措施的那些事故工况。发生这样的事故时，燃料损伤和放射性物质的释放保持在允许的限值内。

多样性 存在两个或多个多重的系统或部件完成一个确定的功能，这些不同的系统或部件有不同的属性，以便降低发生共因故障的可能性。

被驱动设备 被原动机操作的如泵或阀之类的部件。

功能隔离 防止一个回路或系统的运行或故障模式对另一个回路或系统产生影响的措施。

安全重要物项 这样的物项：它是一个安全组的组成部分和（或）它的失效或故障可能导致厂区人员或公众成员受到辐射照射。

逻辑 按照预先确定的规则，从多个二进制输入信号产生1个要求的二进制输出信号，或逻辑电路用于产生上述信号的设备。

多路通信 使用如分时、分频或脉冲编码技术，在一个单一数据通道上发送和接收两个或多个信号或信息。

正常运行 在规定的运行限值和条件内的运行。

核安全 完成正确的运行工况，防止事故或缓解事故后果，导致保护工作人员、公众和环境免受不适当的辐射危害。

运行状态 符合正常运行和预期运行事件的状态。

实体分隔 用几何条件（距离、方位等）、适当的屏障或这两者的结合的分隔。

假设始发事件 在设计过程中确定能导致预计运行事件或事故工况的事件。

原动机 当得到驱动装置命令时，能将能量转变为动作的部件，例如马达、电磁控制器或气动控制器。

保护系统 这样一个系统，它监测反应堆运行，当监测到异常工况时，自动启动一些动作，以防止不安全和或潜在不安全的工况。

保护动作 使某个特定的安全驱动装置动作的保护系统动作。

保护任务 为保证完成某一给定假设始发事件所要求的安全任务，所需最少数量的保护动作。

质量保证 为对某一物项、过程或服务满足规定的质量要求提供足够置信度所必需的有计划的和系统化的活动，例如许可证中规定的那些活动。

质量控制 质量保证的组成部分，旨在验证构筑物、系统和部件符合预先确定的要求。

多重性 设置另外的（相同的或不同的）构筑物、系统或部件，以便任何一个都能完成所要求的功能，不管任何其他者是处于运行状态还是故障状态。

可靠性 当要求一个系统满足其最低限度性能要求时，它将满足这些要求的概率。

响应时间 从部件收到要求呈现输出状态的信号到部件达到规定的输出状态所需的时间间隔。

安全动作 安全驱动系统的一次性动作[5]。

安全驱动系统 由保护系统触发用以完成要求的安全动作所必需的设备集合。

安全功能 为实现安全必须达到的一个特定目的。

安全组 完成某一特定假设始发事件所必需的全部动作指定设备的组合，以确保不超过设计基准中为预计运行事件和设计基准事故规定的限值。

安全限值 运行参数的限值，一个被批准的设施在这些限值范围内运行已证明是安全的。

安全有关仪表控制（I&C）系统 不作为安全系统组成部分的安全重要仪表控制（I&C）系统。

安全系统 安全上重要的系统，用于保证反应堆安全停堆或从堆芯中排出余热，或限制预计运行事件和事故工况的后果。

---

5 例如插入控制棒；关闭安全壳隔离阀门或运行安全注射泵。

安全系统支持设施 为保护系统和安全执行系统提供所需冷却、润滑和能源等服务的设备集合[6]。

安全任务 探测表示某一特定假设始发事件的一个或多个变量，处理信号，启动和完成的需要的安全动作以防止超过设计基准中规定的限值，启动和完成安全系统支持设施的某些服务。

单一故障 导致某一部件不能执行其预定安全功能的一种故障，以及由其引起的任何继发故障。

系统生存周期 一个系统所经过的从概念设计到最终处置的所有阶段。

确认 确定一个产品或服务是否足以令人满意地完成其预期功能的过程。例如，对仪表控制系统而言，确认便是证实整个系统（硬件和软件）满足其所有的功能要求和其他要求，并且没有非预期行为的过程。

验证 确定一个产品或服务的质量或性能是否如所指明、所预期或所要求的过程。例如，对一个开发过程而言，验证便是保证该开发过程中的一个特定阶段满足前一个阶段对其要求的过程。

6 在假设始发事件发生后，一些要求的安全系统支持设施可能被保护系统启动，另一些要求的安全系统支持设施可被它们服务的那些安全驱动系统启动；其他一些要求的安全系统支持设施可能不需要被启动，如果在假设始发事件发生时它们正在运行的话。

参与起草和审订的人员

Anani, N.	加拿大原子能管理委员会
Bock, H.W.	德国西门子公司
Duong, M.	国际原子能机构
Faya, A.	加拿大原子能管理委员会
Hughes, P.J.	英国皇家核设施检查机构
Johnson, G.L.	美国劳伦斯·利弗莫尔国家实验室
MacBeth, M.	加拿大原子能有限公司
Pachner, J.	国际原子能机构
Pauksens, J.	加拿大原子能有限公司
Rollinger, F.	法国核防护和安全研究所

该出版物已被第 SSG-39 号取代。

认可安全标准的机构

核安全标准委员会

阿根廷:Sajaroff, P.; 比利时: Govaerts, P. (主席); 巴西: Salati de Almeida, I.P.; 加拿大: Malek, I.; 中国: Zhao, Y.; 法国: Saint Raymond, P.; 德国:Wendling, R.D.; 印度: Venkat Raj, V.; 意大利:Del Nero, G.; 日本:Hirano, M.; 大韩民国: Lee, J.-I.; 墨西哥: Delgado Guardado, J.L.; 荷兰: de Munk, P.; 巴基斯坦: Hashimi, J.A.; 俄罗斯联邦:Baklushin, R.P.; 西班牙:Mellado, I.; 瑞典: Jende, E.; 瑞士: Aberli, W.; 乌克兰:Mikolaichuk, O.; 英国:Hall, A.; 美利坚合众国:Murphy, J.; 国际原子能机构: Hughes, P. (协调员); 欧洲委员会: Gómez-Gómez, J.A.;国际标准化组织:d'Ardenne, W.; 经济合作与发展组织核能机构: Royen, J.

安全标准委员会

阿根廷: D'Amato, E.; 巴西: Caubit da Silva, A.; 加拿大: Bishop, A., Duncan, .M.; 中国: Zhao, C.; 法国: Lacoste, A.-C., Gauvain, J.; 德国: Renneberg, W., Wendling, R.D.; 印度: Sukhatme, S.P.; 日本: Suda, N.; 大韩民国: Kim, S.-J.; 俄罗斯联邦: Vishnevskij, Y.G.; 西班牙: Martin Marquínez, A.; 瑞典: Holm, L.-E.; 瑞士: Jeschki, W.; 乌克兰: Smyshlayaev, O.Y.; 英国: Williams，L.G. (主席), Pape, R.; 美利坚合众国: Travers，W.D.; 国际原子能机构: Karbassioun， A. (协调员)； 国际辐射防护委员会: Clarke, R.H.; 经济合作与发展组织核能机构: Shimomura, K.

通过国际标准实现安全

“国际原子能机构的标准已经成为促进有益利用核和辐射相关技术全球安全机制中的一项重要内容。

“国际原子能机构安全标准正在适用于核电生产以及医学、工业、农业、研究和教育，以确保对人类和环境的适当保护。”

国际原子能机构
总干事
穆罕默德·埃尔巴拉迪

国际原子能机构
维也纳
ISBN 92-0-513905-X
ISSN 1020-5853