核安全导则　HAD 102/10-2021

核动力厂仪表和控制系统设计

(国家核安全局 2021 年 9 月 30 日批准发布)

国家核安全局

核动力厂仪表和控制系统设计

（2021 年 9 月 30 日国家核安全局批准发布）

本导则自 2021 年 9 月 30 日起实施

本导则由国家核安全局负责解释

本导则是指导性文件。在实际工作中可以采用不同于本导则的方法和方案，但必须证明所采用的方法和方案至少具有与本导则相同的安全水平。

目　录

1 引言

1.1 目的

本导则是对《核动力厂设计安全规定》（HAF102）有关条款的说明和细化，其目的是为新建核动力厂仪表和控制系统总体结构以及安全重要仪表和控制系统[1]的设计提供指导。本导则的主要内容可作为在役核动力厂设计修改和安全审查的参考。

1.2 范围

1.2.1 本导则适用于核动力厂安全重要仪控系统的设计、实现、鉴定及文档化。安全重要仪控系统指属于某一安全组合的一部分，或者其失效或故障可能导致对厂区人员或公众的辐射照射的仪控系统，例如：

（1）反应堆保护系统；

（2）反应堆控制系统、反应性控制系统及其监测系统；

（3）反应堆冷却控制与监测系统；

（4）应急供电控制与监测系统；

（5）安全壳隔离控制与监测系统；

（6）事故监测系统；

（7）流出物监测系统，等。

1.2.2 本导则适用于从传感器到驱动和控制工艺设备的装置的所有仪控设备，包括但不限于：

[1] “仪表和控制系统”简称“仪控系统”，在本导则中专指安全重要仪控系统。当某些条文对安全重要仪控系统和非安全重要仪控系统都适用时，将会特别说明。

（1）传感器、变送器；

（2）驱动控制装置；

（3）自动和手动控制设备；

（4）人机接口设备，等。

1.2.3 本导则适用于采用各种技术手段实现的仪控设备，例如：

（1）采用模拟技术的设备；

（2）计算机系统与相关通信系统；

（3）软件；

（4）使用硬件描述语言编程的设备（例如现场可编程门阵列）；

（5）限定功能的工业数字化设备，等。

1.2.4 本导则不包括仪控系统辅助设施（例如冷却、润滑以及供电）的设计。

1.2.5 由于与仪控系统相关，本导则涉及了人因工程以及网络安全方面的某些内容，但并不给出这些领域的详细指导。本导则旨在确定与人因工程和网络安全活动之间的主要接口，并对影响这些方面的仪控设计特性给出建议。

2 仪控设计管理

2.1 概述

2.1.1 设计必须保证核动力厂及其安全重要物项具有合适的

性能，以保证其能可靠地执行安全功能；在设计寿期内核动力厂能够在运行限值和条件范围内安全运行，并能够安全退役；对环境的影响最小。

2.1.2 必须制定和实施描述核动力厂设计的管理、执行和评价的总体安排的质量保证体系。该体系包括保证核动力厂每个构筑物、系统和部件以及总体设计的设计质量的措施，包括确定和纠正设计缺陷、检验设计的恰当性和控制设计变更的措施。

2.1.3 为确保安全性，仪控系统的设计基准文档及相关信息或记录应通过适当的流程进行控制，从而使它们可以在仪控系统的整个生命周期内保持完整、清晰、简明、正确并且一致。应确保设计基准文档及相关信息或记录是充分和适当的，并且能够得以长期维护以反映核动力厂的设计变化或变更状态。这其中包括可能源于设计基准文档的文件和信息，这些文件和信息可能会对安全性产生影响，例如仪控系统的运行、维护或修改相关的规程或手册。

2.1.4 参与仪控系统开发活动的各个组织都应建立质量保证体系，并与营运单位质量保证大纲总的要求相一致。

2.2 生命周期模型的使用

2.2.1 对于数字化仪控系统，要证明最终产品满足要求，在很大程度上（但不是唯一）依靠高质量的开发过程，以规范设计需求及其实现。同时，验证和确认活动也是不可或缺的。因此，较之纯硬件系统，对于数字化仪控系统正确性的信任更依赖于其

开发过程的规范性。

2.2.2 针对第 2.2.1 节，开发过程中普遍采用生命周期模型来描述数字化仪控系统的开发活动以及这些活动之间的关系。这些被广泛接受的实践已通过相关核工业标准被正式确定下来。这些标准对于仪控系统的开发过程给出了广泛的指导。通常，与同一个开发步骤相关的活动被归为生命周期的同一阶段。

2.2.3 应对开发过程进行完整记录，以提供证据，提升独立评审者和监管机构对最终产品的适用性的信心。

2.2.4 本章对生命周期的要求也适用于第 9 章中描述的生命周期活动。

2.2.5 仪控系统的开发可以用生命周期的三个基本层级描述：

（1）仪控总体结构的生命周期；

（2）一个或多个单独的仪控系统的生命周期；

（3）一个或多个部件的生命周期。部件生命周期通常置于平台开发框架中管理，并且独立于总体结构层级和各系统层级的生命周期。数字化系统的部件生命周期通常被划分为硬件生命周期和软件生命周期。

2.2.6 仪控系统开发之外的一些活动也会对仪控系统需求及设计产生重要影响，例如人因工程和网络安全，因此在设计阶段就应加以考虑。

2.2.7 图 1 给出了一个仪控系统生命周期的实例，以及来自人因工程与网络安全活动的主要输入。

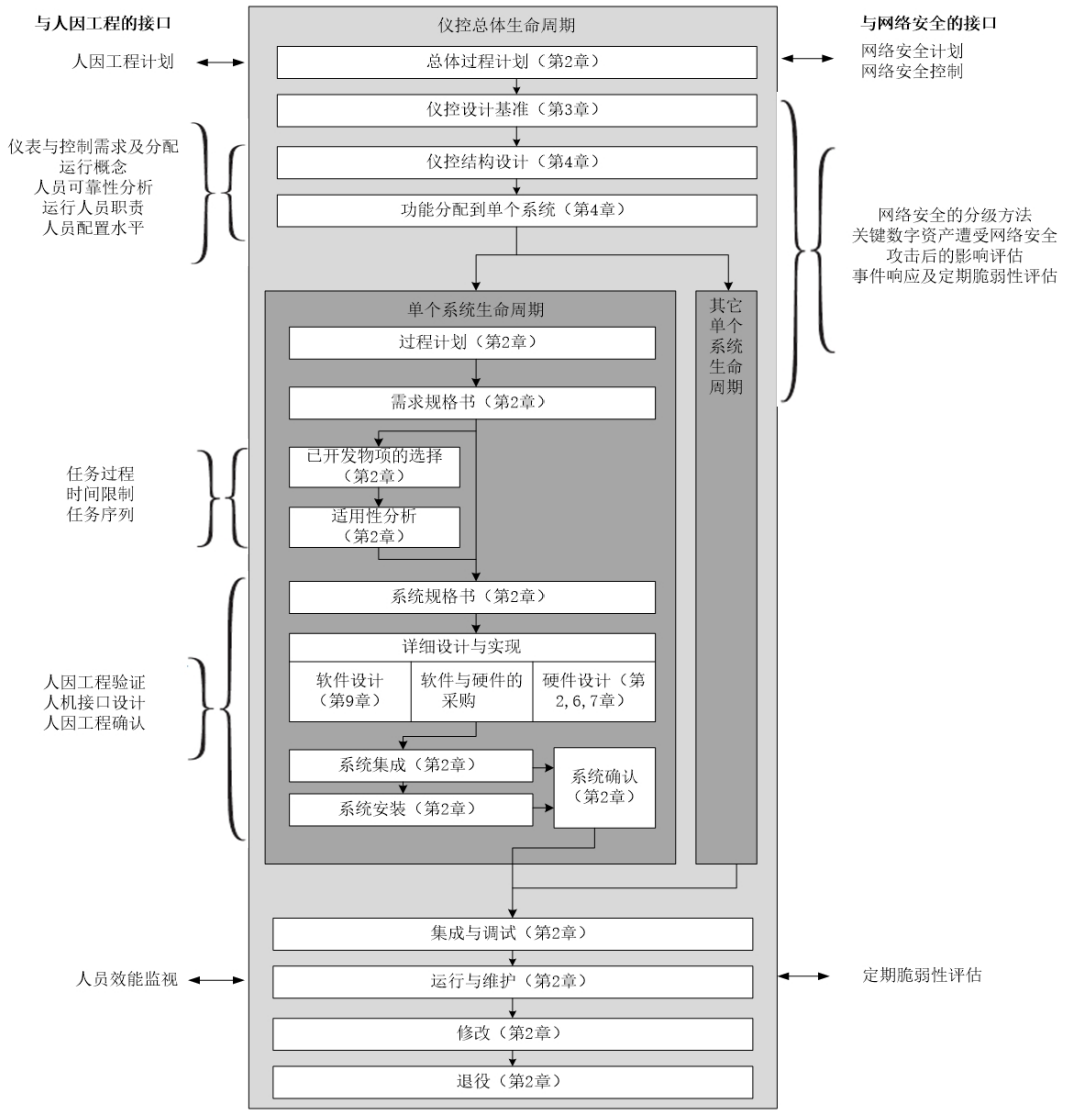

图 1 典型仪控系统生命周期活动以及与人因工程及网络安全活动的接口

2.2.8 图 2 的“V 模型”从另一个角度给出了仪控系统生命周期的样例。该模型说明了需求规格书、设计、集成和系统确认之间的关系，以及验证和确认活动是如何与开发活动相关联的。图 2 既适用于数字化系统，也适用于模拟系统。如果不包含软件，则无需考虑软件相关的活动。

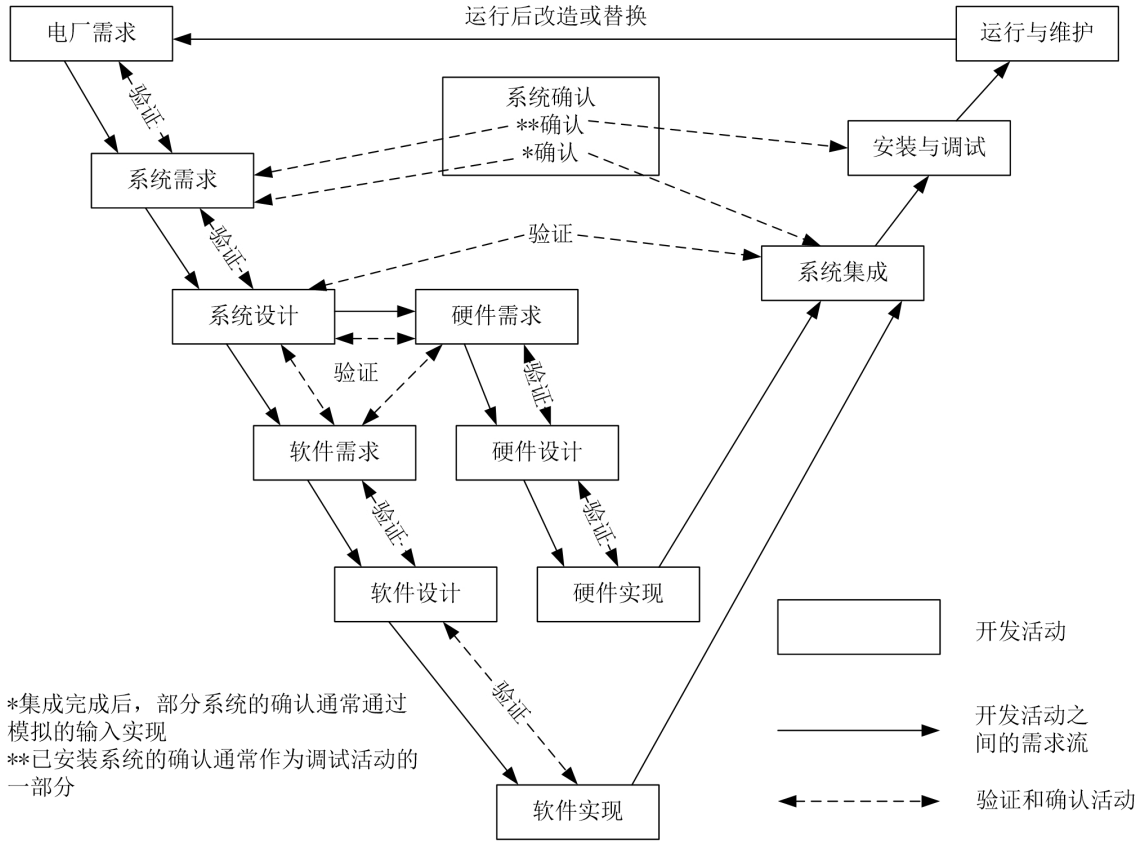

图 2 仪控系统生命周期过程与验证和确认活动之间的典型关系

2.2.9 在生命周期的任何一点都有可能需要修改之前阶段已完成的工作。这些修改将经过并影响到中间的各个阶段。为了简化起见，图 1 和图 2 没有表示出这类迭代路径。

2.2.10 所有与仪控总体结构、各个仪控系统和仪控部件（仪控部件包含硬件、软件，软件有应用软件、固件和硬件描述语言）的开发、实现和运行相关的所有活动均应在一个生命周期的框架内进行，并形成书面文档。

2.2.11 每个仪控系统和部件的生命周期均应从生成仪控系统和部件的需求开始，到仪控系统和部件不再被核动力厂安全所

需要结束。

2.2.12 过程计划

2.2.12.1 在任何技术活动开始之前，应根据质保要求准备计划，规定本活动必要的输入、成果和活动过程，以及本活动与其他活动之间的相互关系，并对计划进行批准。

2.2.12.2 仪控系统的开发计划应针对仪控特有的以及仪控开发需要特别应对的各个方面，包括：

（1）生命周期模型；

（2）配置管理；

（3）不符合项的识别、控制及解决；

（4）危害分析；

（5）验证和确认；

（6）概率安全评价结果的使用；

（7）针对仪控系统的安全分析；

（8）需求工程；

（9）结构设计；

（10）已开发物项的选择与接受；

（11）设计；

（12）实现（例如硬件制造，编程，或硬件描述语言的编码及综合）；

（13）集成；

（14）系统确认；

（15）安装；

（16）调试；

（17）设备鉴定；

（18）工具的鉴定与使用；

（19）维护；

（20）设备过时管理；

（21）运行；

（22）培训；

（23）软件维护。

2.2.12.3 仪控系统不同方面的开发计划可以合成一份。

2.2.12.4 仪控系统的开发还应依据那些并非专门针对仪控开发活动的计划，例如：

（1）质量保证；

（2）安全重要物项分级；

（3）采购；

（4）生产制造；

（5）文档的生成与维护，等。

2.2.12.5 所有仪控开发活动应依据适用的经批准的计划实施。

2.2.13 与人因工程活动和网络安全活动的协同

2.2.13.1 虽然本导则不包含人因工程和网络安全活动相关的生命周期模型，但是这类过程所提供的信息是仪控开发所需要

的。图 1 展示了与这些过程之间的关系与接口，包括：产生人因工程相关需求的活动；人因工程相关的验证和确认活动的输出；网络安全技术措施；网络安全需求。

2.2.13.2 仪控系统开发应与人因工程活动和网络安全活动相协调。

2.2.13.3 在仪控系统的开发过程中，应考虑人因工程大纲的需求，包括：

（1）运行人员的角色职责以及其他人员需求；

（2）人机接口相关的构筑物、系统与部件的安全分级；

（3）信息需求，包括确定应对事故和事故后工况所需的显示与控制集；

（4）控制需求，包括控制需求、自动与手动控制功能，以及将控制分配到合适的位置；

（5）由任务分析确定的任务执行过程、时间限制和信息流需求（任务分析见第 8.4.22.3 节）；

（6）基于情境的报警策略，以避免信息泛滥（例如在启堆阶段和瞬态期间）；

（7）仪控系统、设备或部件故障告警需求；

（8）支持仪控系统和设备可维护性的规定；

（9）安全分析中人员可靠性分析所给出的结论。

2.2.13.4 人因工程相关的验证和确认活动：

（1）应对人因工程相关建议的解决方案，以及人机接口设

计分析中所发现缺陷的解决方案进行验证；

（2）应验证仪控系统符合适用的人因工程设计导则；

（3）应验证设计提供的仪控系统、其他设备及操纵员辅助手段是充分的，能够支持运行人员执行分配给他们的任务；

（4）应验证人因设计能够使得操纵员对报警信息做出正确响应，包括允许充足的时间以保证可信的操纵员动作；

（5）应使用基于效能的测量方法，以确认在需要仪控系统起作用的核动力厂所有工况下，运行人员均可以通过该系统执行功能，包括当部分仪控系统或设备由于维护和试验等目的经授权处于旁通状态时。

2.2.13.5 人因工程需求的设计实现以及人因工程活动的验证和确认一般作为人因工程的一部分。除与仪控生命周期过程的接口外，人因工程在本导则中不做详细描述。

2.2.13.6 核动力厂的整个仪控系统应执行网络安全大纲中对其规定的安全措施。

2.2.13.7 应结合仪控系统总体结构和每个仪控系统的情况，对网络安全大纲及时更新。

2.2.13.8 仪控系统的开发应在满足网络安全大纲技术、程序和行政管理要求的开发环境中组织实施，统筹考虑核安全和网络安全。

2.3 生命周期各阶段的通用活动

2.3.1 配置管理

2.3.1.1 仪控系统生命周期内的配置管理目标包括：

（1）识别所有需要纳入配置管理的物项，例如文档、仪控产品及相关记录；

（2）规定配置项的安全存储和检索；

（3）识别配置项之间的从属或关系；

（4）识别配置项的所有变更；

（5）防止对配置项的误修改和未授权修改；

（6）保证与设计基准持续的一致性；

（7）规定配置基线，即规定每个配置层级的配置项内的相互兼容且一致的组成配置。建立配置基线的配置项可以包括单独部件、单个系统或整个仪控系统。配置项的基线需覆盖组成该物项的所有系统和部件；

（8）保证实体核动力厂与技术文档的一致性；

（9）说明配置项的最新状态(例如审查、批准或确认状态)。

2.3.1.2 配置管理应包括分析变更影响、批准变更、确认版本正确组合、发布设计文件和软件,以及建立和维护时间记录(例如设计中某个特定点使用了哪一版本的工具）的技术和程序。

2.3.1.3 所有仪控物项及其相关文档都应被指明、赋予唯一标识，并置于配置管理之下。

2.3.1.4 仪控物项包括交付的仪控系统、所有支持该系统的或该系统运行所需的单独安装的物项、定义所有这些物项的文档和记录，以及可能影响这些物项质量的软件工具。

2.3.1.5 仪控物项通常包括：

（1）采购物项、复用物项以及新开发物项；

（2）软件部件，例如源代码和可执行代码、硬件描述语言、现场可编程门阵列的配置数据，以及核动力厂设备中安装的软件，包括应用软件、操作系统和支持软件，等；

（3）硬件部件，以及硬件部件上的可更换元器件；

（4）固件；

（5）开发文档，例如需求规格书、设计文件、加工图纸及说明、安装图纸及说明、软件和硬件描述语言，等；

（6）设备、部件和关键元器件配置数据和配置文件（例如安全运行限值、警告与报警限值、整定值和标定常数，等）；

（7）用于生产、控制、配置、验证或确认仪控部件的实体工具和软件工具，包括使用这类工具时采用的参数设定。

2.3.1.6 应使用配置管理数据验证仪控物项是否正确地组装并安装在正确的物理和拓扑位置，是否正确安装预定版本的软件。

2.3.1.7 生命周期过程记录应置于配置管理之下。

2.3.1.8 用于生命周期记录的配置管理程序可以与用于仪控产品的配置管理程序不同。

2.3.1.9 置于配置管理之下的生命周期记录包括系统安全分析所依据的或者影响运行维护阶段安全的所有信息，例如：

（1）生命周期活动的计划和程序；

（2）安全论证计划；

（3）分析文件；

（4）记录安全论证及其支持性证据的媒介或记录，例如用于质保、验证（包括分析和测试）、确认（包括需求的确认）、过程评价和监查、真实性、完整性和可追溯性的媒介或记录；

（5）验证和确认活动的记录；

（6）测试规格书，程序，计划和结果；

（7）安全系统整定值及其设定方法；

（8）系统集成相关的程序、计划和结果；

（9）过程的审查与审核相关的文件；

（10）需求可追溯性矩阵；

（11）维护和运行程序；

（12）设备与备件采购规格书的技术部分；

（13）鉴定记录；

（14）仪控系统和部件的文档（见第 2.3.6.3 节），等。

2.3.1.10 置于配置管理下的物项标识应包含版本号。

2.3.1.11 仪控系统的初始开发阶段，开发过程中的变更以及运行之后的改造均应采取配置控制。

2.3.1.12 配置管理过程应维护每个配置项的相关信息。

2.3.1.13 记录的信息包括：物项初次完成时间；不同版本之间的变化，包括差异报告（如适用）；与其他配置项的从属关系；物项当前的批准状态；创建、审查和批准的责任人。

2.3.1.14 仪控设备所安装软件的标识以及配置数据的数值

应可从所在设备上获取。

2.3.1.15 获取所安装物项的标识和配置数据数值的能力可以为设备配置正确性验证提供支持。安装自动检查措施或软件工具可以辅助该验证。

2.3.2 仪控系统的危害分析

2.3.2.1 应对仪控总体结构开展危害分析，以识别可能有损核动力厂设计的纵深防御或多样性策略的情况。

2.3.2.2 应对每个安全系统及其物项开展危害分析，识别可能导致其安全功能性能劣化的情况。

2.3.2.3 应考虑的危害包括：核动力厂内部危险和外部危险、核动力厂设备失效以及由硬件失效或软件错误导致的仪控失效或误动作。由非预期的相互作用所导致的危害也应予以考虑。

2.3.2.4 仪控系统的危害分析应考虑核动力厂所有状态及运行模式，包括不同运行模式之间的转换，劣化状态也应包含在内。

2.3.2.5 应在仪控总体设计基准完成之前形成仪控系统危害分析的初始结论。

2.3.2.6 危害分析应在生命周期的每个阶段不断更新，包括（但不限于）仪控总体结构设计，安全系统需求规格书及其设计、实现、安装和改造。危害分析更新的目的在于识别出可能由特定的安全仪控系统特性、安全仪控系统与核动力厂之间的相互作用以及安全仪控系统与其他仪控系统（无关其安全分级）之间的相互作用所引发的危害。

2.3.2.7 对于已经识别的可能导致系统功能劣化的危害，应采取措施消除、避免或缓解其后果。消除、避免或缓解危害后果的措施，可以是修改仪控系统的需求、设计或实现，或者修改核动力厂设计等。

2.3.2.8 危害分析所选取的方法应适用于被分析的系统和物项。

2.3.3 验证和确认

2.3.3.1 仪控系统生命周期的每个阶段均应使用此前阶段输出的信息，其结果作为此后阶段的输入。

2.3.3.2 生命周期每个阶段的结果应依据此前阶段设定的需求进行验证。

2.3.3.3 可使用需求追溯矩阵，书面确认生命周期每个阶段的需求均被满足，或在需求不满足时采取了适当的行动。

2.3.3.4 应对仪控总体、每个仪控系统以及每个仪控部件进行验证，以证实所有的需求（包括功能需求和非功能需求）均得以满足，并确定是否存在非预期的行为。应对仪控总体、每个仪控系统以及每个仪控部件的需求进行确认以证实这些需求得以正确实现。

2.3.3.5 验证和确认应由独立于设计者和开发者的个人、团队或组织实施。

2.3.3.6 验证和确认独立性的建立通常应保证执行验证和确认的团队、个人或组织符合下列要求：

（1）具备足够的技术能力与知识；

（2）能够确定自己的工作范围；

（3）不受来自开发者的压力；

（4）不受预算缩减或进度约束这些可能阻碍其完成全部审查的因素的影响；

（5）能够无障碍地向管理部门提交发现的问题。

2.3.3.7 验证和确认独立性的程度和类型应与相应系统或所含部件的安全等级相匹配。验证和确认可以在不同的独立性水平上并行开展（如验证和确认可以由来自原开发组织的独立于开发者的测试人员进行，同时由另一个独立的组织负责附加的独立验证和确认）。

2.3.3.8 验证和确认活动，包括已识别的异常及其处理，应形成正式文档。如果在验证和确认阶段发现了异常，那么对由此导致的设计修改及其实现也应执行与之前相同的验证和确认过程。

2.3.3.9 验证和确认团队、系统集成团队、调试团队，以及系统设计者和开发者之间的技术沟通应形成文档。

2.3.4 概率安全分析结果的使用

2.3.4.1 设计必须适当考虑核动力厂所有运行模式和所有状态（包括停堆工况）下的概率安全分析，特别是：

（1）论证整个设计是平衡的，没有任何一个设施或假设始发事件对于总的风险会有过大的或明显不确定的贡献，且纵深防

御的各层次应尽实际可能独立；

（2）确认核动力厂不存在陡边效应；

（3）将分析结果和已规定的风险准则进行比较。

2.3.4.2 在仪控系统设计中应考虑来自概率安全评价的结果。

2.3.5 安全评价

2.3.5.1 仪控系统的安全评价应符合确定论分析和概率论分析相关核安全导则的要求。

2.3.5.2 应实施设计分析、验证和确认活动，以证实仪控总体结构以及每个仪控系统的全部设计基准需求均得以满足。

2.3.5.3 第 3.2.7 节列出了在仪控总体结构和各仪控系统设计基准需求中需考虑的方面。第 3.2.8 节列出了在安全系统的设计基准需求中还需考虑的方面。

2.3.5.4 典型的设计分析、验证和确认技术包括：

（1）可追溯性分析：可追溯性分析通常用于证实需求的实现与确认。

（2）故障模式和影响分析：故障模式和影响分析常用于确认与单一故障准则的符合性，以及确认所有已知故障模式是可以自呈现或通过计划性试验发现的。

（3）纵深防御和多样性分析：纵深防御和多样性分析是审查安全系统共因故障薄弱点的手段之一。

（4）可靠性分析：可靠性分析采用统计学方法预测系统或部件的可靠性。通常采用的可靠性分析技术包括部件计数分析、

部件应力分析、寿期数据分析（例如威布尔分析）、可靠性框图以及故障树分析。

（5）确认：确认测试应使用确定性技术，也可能包括统计技术。

（6）网络安全测试：网络安全测试通常需要来自脆弱性评估的输入，用于证实在网络安全方面所采取的措施是有效的。

（7）证实物项可靠性设计的分析：此类分析用于证实设计中包含了那些公认可以提供高可靠性的措施，例如冗余、符合单一故障准则、可测试性、故障安全设计以及严格的鉴定，等。为验证仪控系统与可靠性要求的符合性，通常需要将定性分析、定量分析和测试相结合。

（8）证实仪控系统在各种运行模式下满足功能需求的分析：包括对电源中断期间和之后、重新启动、以及处于其他转换点（例如闰年等日历时间变换）时系统行为正确性的分析。

2.3.5.5 应列出分析中使用的每个假设，并证明使用该假设的合理性。

2.3.5.6 应对开展各种分析的方法进行详尽的规定，并与分析的输入、分析的结果以及分析过程本身一起形成文档。

2.3.5.7 对于符合当前技术水平，按照最高等级质量准则来规定和设计的单个系统，如考虑了与规格书、设计、制造、安装、运行环境和维护实践相关的所有潜在故障源（网络安全相关的故障源除外），则在概率安全分析中采用 10^{-4} 至 10^{-5} 失效/需求的总

体性限值是适宜的。这个指标包括系统冗余通道发生共因故障的风险，并且适用于从传感器，经过信号处理到输出，一直到被驱动设备的整个系统。也可以提出更高的可靠性指标，但需要结合上述所有因素进行专门的论证。

2.3.5.8 仪控系统的可靠性目标应是可证实的，并应在合理的范围内。

2.3.5.9 在设计与实现过程中，应对每个仪控系统与核动力厂之间的相互作用进行定期审查以满足相关安全要求。

2.3.5.10 当发现与这些要求有冲突时，应适当修正设计和实现。

2.3.6 文档

2.3.6.1 仪控文档

（1）应提供设计过程不同阶段之间，以及设计过程不同参与方之间的信息沟通的手段；

（2）应提供记录，表明需求已正确转化到设计中，并已在安装的系统中实现；

（3）应将运行所需的必要信息和安全设计相关信息传达给核动力厂运行人员；

（4）应为核动力厂及仪控系统的维护，以及未来可能的设计修改提供基础；

（5）应保证贯穿仪控系统生命周期各阶段的可追溯性；

（6）应处在配置管理系统的控制之下；

（7）应是清晰、完整、一致、结构完善、可读、对于使用者（例如领域专家、安全工程师以及软件设计者，等）是可理解的，并且是可验证和可维护的。

2.3.6.2 完善的文档有利于系统的运行、监督、故障排查、维护、未来改造或升级，以及核动力厂人员和技术支持人员的培训。

2.3.6.3 营运单位应建立或获得仪控系统及部件的相关文档，至少包含以下内容：

（1）设计要求；

（2）功能及功能性设计；

（3）运行原则；

（4）系统在全厂的作用；

（5）设计措施，包括安全重要设计措施的识别；

（6）竣工状态的设计及配置文档；

（7）竣工状态的系统及其主要部件（包括传感器和驱动器）的位置；

（8）与核动力厂其他系统之间的接口及从属关系；

（9）监督、试验、诊断、维护和运行相关的设施及要求；

（10）试验程序及结果；

（11）设备鉴定；

（12）设计和开发过程，以及设计中遵循的质量要求；

（13）各个阶段（包括调试）的试验策略；

（14）验证和确认方法的设计、开发以及结果；

（15）所有正常运行状态和模式的运行规程；

（16）覆盖假设事故工况和设计扩展工况的应急运行规程和严重事故管理指南；

（17）对备品备件的建议及采购规格书；

（18）网络安全设计特性及其应用。如果设计中假设营运单位采取了一定的网络安全相关政策和实践，则应与营运单位就此问题进行沟通。相关内容应通过单独的文档进行描述，该文档的分发限制相对于其他系统信息应更加严格。

2.3.6.4 采购、设计、制造、编程以及验证和确认等活动的过程及要求文档应可供营运单位、监管机构或代理这些机构职责的第三方用于评定（见第 9.8 节）。

2.4 生命周期具体活动

2.4.1 需求规格书

2.4.1.1 对于仪控总体、每个仪控系统以及仪控部件的需求应以适当的形式形成文档。

2.4.1.2 各仪控系统的需求的完整组合应满足仪控总体的设计基准。

2.4.1.3 对仪控总体以及每个仪控系统的需求应从仪控设计基准导出（仪控总体设计基准的导出及内容在第 3 章讨论）。

2.4.1.4 对于仪控系统及部件的需求应规定（如适用）：

（1）每个仪控系统或部件的作用；

（2）在每种核动力厂状态和运行模式下，每个功能的输入和输出关系；

（3）测量、控制功能和显示的最小精度和准确度，最大响应时间；

（4）系统接口（例如系统与操纵员，以及与其他系统之间的接口）；

（5）自监督特性，包括其时限特性需求（包括故障检测时间及修复时间）；

（6）通过自诊断方式发现故障后仪控系统需采取的动作；

（7）网络安全特性（例如有效性检查，专门的网络安全控制，以及系统在其所处环境下保持网络安全控制和访问权限的特性）；

（8）需要达到的可靠性与可用性水平，以及确保该目标能够达到所必需的支持性需求。可靠性与可用性水平可通过定量或定性的方式进行定义，例如从上述的支持性要求的角度，可以有具体可靠性策略的实现要求、开发过程特征的要求或者符合规定标准的要求等；

（9）维护所需设施和措施；

（10）设计限制，例如支持独立性或多样性要求的限制；

（11）对特定故障模式的安全响应；

（12）核动力厂正常工况、事故工况以及可预见的内外部危险相关的全部运行环境下的鲁棒性。

2.4.1.5 在考虑设计限制时，设计限制应是明确规定的、可论证的、可追溯的。

2.4.1.6 数字化系统的网络安全设计需求应考虑网络安全风险评估的结果并且应与营运单位的网络安全政策特性相一致。

2.4.1.7 应建立专门的过程来管理全生命周期的需求，确保所有的需求被完全满足、验证、确认并实现。

2.4.1.8 需求工程是一个专门的过程，用于确保仪控系统的安全目标通过设计来实现。

2.4.1.9 需求的建立和文档化应使用一套与系统的安全重要性相匹配的预先确定的技术方法。该技术包括使用具有明确定义的语法及语义的规范语言、建模、分析和审核。

2.4.1.10 需求应尽可能地反映需要达成的目标，而非该需求将如何被设计和实现。

2.4.1.11 需求的描述应便于各相关方（例如营运单位、供应商及设计者）明确理解。

2.4.1.12 需求文档应涉及、包括或补充额外信息，例如特定需求的背景信息、风险考虑、功能或安全措施的设计建议，以确保需求被其使用者充分理解。

2.4.1.13 尤其是那些对安全有潜在影响的需求，应在需求文档中明确。

2.4.1.14 应规定每个需求的来源和根据，以便于完成验证、确认及根据更高层次文档的追溯，并证明已考虑所有相关的设计

基准需求。

2.4.2 已开发物项的选择

2.4.2.1 已开发物项应按照第 6.3.1.1-6.3.4.21 节的要求进行适当的鉴定。

2.4.2.2 已开发物项包括硬件设备、已开发软件、由硬件和软件组成的数字化设备、使用硬件描述语言配置的硬件设备或可在硬件描述语言中使用的已开发功能模块等。

2.4.2.3 应证明已开发物项未在安全仪控系统中使用的功能不会妨碍系统的安全功能。在可行的情况下，应通过配置禁止已开发物项中未使用的功能，使其不起作用。

2.4.2.4 已开发物项应有相关文档，提供其在仪控系统中使用所需的信息。

2.4.3 设计与实现

2.4.3.1 仪控总体结构以及各仪控系统的设计应源自对所需的功能和其他需求进行的系统地、逐步地分解。

2.4.3.2 由仪控系统实现的系统需求应被分配到一组由硬件、硬件描述语言配置的可编程器件以及软件（若有）所构成的适当组合中。硬件可能包括专用于某种应用的集成电路。软件可能包括已开发软件及固件（例如操作系统）、待开发软件或用已开发软件组态生成的软件。

2.4.3.3 精确的需求还应考虑仪控系统之外的现场设备层面的设计选择，例如被驱动设备的类型及性能。

2.4.3.4 应证明非安全重要需求的实现不会妨碍安全重要功能。

2.4.3.5 应建立设计规则以确保每个仪控系统的内部逻辑均适合验证和确认。

2.4.3.6 设计中应考虑需要在运行期间可配置、验证和确认的仪控参数，并应提供实现手段（例如反应堆保护系统的停堆整定值、标定常数和软件配置设定）。

2.4.4 系统集成

2.4.4.1 系统集成的目标：

（1）应解决部件之间的所有接口问题，例如硬件与软件之间或软件模块之间；

（2）应确认系统不同部件之间的接口需求得以满足；

（3）应确认部件、子组件和子系统在集成后的系统中按设计运行，以使得系统满足规定的需求，包括超量程值、异常处理以及时限需求。

2.4.4.2 在开始系统集成之前，应保证已验证模块（硬件及软件）配置的一致性。

2.4.4.3 通常使用软件工具对下装到系统部件的软件模块的发布进行控制，以及对用于系统确认的软件的构建进行控制。软件工具还可在现场运行阶段使用，便于实施配置控制以及保证已安装部件与已确认部件之间的可追溯性。

2.4.4.4 应采用文档化的可追溯性分析，证明系统集成相对

于系统设计规格书而言是完整，并满足第 2.4.4.1 节的目标。

2.4.5 系统确认

2.4.5.1 对每个仪控系统以及集成的仪控系统都应进行系统确认。

2.4.5.2 通常，系统确认应在系统现场安装完成时结束。如果在现场安装结束后仍有一些系统确认的活动需要执行，那么这些工作可以包含在调试试验中，前提是测试结果将包含在确认试验记录中，而且保证了第 2.3.3.6 节和第 2.3.3.7 节中所规定的确认团队与设计团队之间的独立性。

2.4.5.3 用于确认试验的系统对于实际安装到现场的仪控系统的最终配置应具有代表性。用于系统确认的软件应与用于现场运行的软件完全相同。

2.4.5.4 系统确认应证明该系统在所有可能的接口条件以及所有可能的负荷条件下均满足各项需求。

2.4.5.5 不便在系统确认阶段进行测试的运行模式以及仪控系统与核动力厂之间的相互作用，应在调试阶段进行测试，或者通过补充性分析进行确认。

2.4.5.6 系统确认应覆盖：

（1）系统的所有部分；

（2）接口信号的全量程，包括超量程的值。接口信号包括与其他系统、传感器、驱动器和操纵员接口的输入和输出；

（3）异常处理；

（4）整定值的准确度与回差；

（5）核动力厂及系统的所有模式，以及不同模式之间的转换；

（6）失电之后的恢复；

（7）时限；

（8）鲁棒性和故障容错。

2.4.5.7 系统的确认测试应包括所有输入的变化，即应采用动态测试。

2.4.5.8 动态测试应使用可以代表核动力厂参数变化的现实情境，该情境是通过对各种可能的核动力厂情境的分析提出的，会要求仪控系统作出响应。

2.4.5.9 功能测试应能够覆盖功能需求所允许的所有行为。功能测试的覆盖率应根据功能需求论证其合理性。

2.4.5.10 确认测试可考虑采用统计技术。也可考虑使用模拟机进行系统确认。

2.4.5.11 在系统确认阶段应尽可能最大程度地对系统运行维护手册的适当部分进行确认。

2.4.5.12 文档化的可追溯性分析应证明系统确认相对于系统需求规格书是完整的，且满足第 2.4.5.4 节和第 2.4.5.6 节的要求。

2.4.5.13 完整的测试文档应足够充分，以确保测试过程是可重复的，并且确保任一重复的和先前的合规测试都会得到一致和

符合要求的结果。

2.4.6 安装、整体仪控系统集成和调试

2.4.6.1 仪控系统应按照经批准的设计方案在现场安装。

2.4.6.2 设备应进行到货检查，或通过调试试验，验证系统和部件没有在运输过程中损坏。

2.4.6.3 调试应逐步将仪控系统与其他部件及其他核动力厂物项进行整合，并验证其符合设计假设，满足功能准则和性能准则。

2.4.6.4 核动力厂环境中的测试是调试的一个重要组成部分。

2.4.6.5 调试应特别注意验证与外部系统之间的接口，证实接口设备正确执行功能。

2.4.6.6 在调试阶段，所有仪控系统均应在尽可能代表在役实际情况的运行、测试及维护工况下长时间运行。

2.4.6.7 应在调试结束之前完成对系统运行手册和维护手册相应部分的确认。

2.4.6.8 在宣布仪控系统可运行之前，应完成了生命周期中规划的相关活动，建立了从需求到已安装系统的可追溯性，系统构建和设计文档应是完整的且反映竣工配置。

2.4.7 运行与维护

2.4.7.1 仪控系统参数的修改应采用适当的手段进行。

2.4.7.2 应对仪控系统运行和维护的人员效能进行监测并形成运行经验记录，从中得到减少人因错误的改进需求。

2.4.7.3 在预计在役寿期的各个阶段，应有足够数量（例如基于仪控系统设计，部件的可靠性，替换部件未来的可获得性以及供应商的支持）的备品备件支持运行和维护。

2.4.8 修改

2.4.8.1 仪控系统的升级与修改设计应考虑：

（1）在役核动力厂的物理特性所造成的限制；

（2）维持替换设备与现有仪控设备设计一致性的潜在需要，例如降低操纵员接口以及核动力厂维护任务的复杂性；

（3）可用的商用设备或技术，以及制造厂商或第三方在设备安装寿期内为此类设备或技术提供稳定支持的前景；

（4）对原有设计文档更新的需要。旧系统的设计文档可能不完整或不准确，因此对系统的重大改动和替换可能需要一定程度的“逆向工程”以重新得到原始的设计基准和规格书。

2.4.8.2 如果仪控系统需要修改或者部分升级，应提前确定论证和执行该变更所适用的严格程度。

2.4.8.3 修改活动的严格程度取决于受影响系统在确保核动力厂安全方面的作用和功能，同时考虑修改之后还需继续运行的已有系统。这也适用于软件工具的修改。

2.4.8.4 仪控系统修改或升级的过程应遵循规定的生命周期。修改需要的生命周期过程的复杂程度与修改活动本身的复杂程度和安全重要性有关。

2.4.8.5 即使是对于最简单的变更，它的生命周期也至少应

包括图 2 中所示的单个系统生命周期的各个阶段，包括每个仪控系统修改后的验证和确认。

2.4.8.6 新老仪控设备过渡期人机接口的临时配置可能需要从人因工程的角度进行更加深入的分析，以便适应临时设备或规程的使用。对于人机接口的改进可能会导致改造后一段时间内运行人员和维护人员错误的增加。必要时应对培训进行修改。

2.4.8.7 如果考虑新老仪控系统的并行运行，应在带来的运行问题和复杂性上与获得置信度之间进行权衡，并评估风险。

2.4.9 从最初开发到修改之间的这段时间中，软件工具的升级或修改的后果可能是重大的，应对其影响进行评估（例如编译器的升级可能会使之前对于编译器适宜性的分析或验证结果失效）。

3 仪控系统的设计基准

3.1 仪表和控制功能识别

3.1.1 识别和确定仪控系统功能（以及相应的非功能需求，例如安全特性、网络安全特性和时间限制等）应是核动力厂设计过程的一部分。

3.1.2 分配给仪控系统的功能包括为核动力厂在不同运行工况以及事故工况下提供相关信息和控制。这些功能的目标是：

（1）防止偏离正常运行；

（2）检测故障并控制异常运行；

（3）控制核动力厂设计基准以内的事故；

（4）控制设计扩展工况的后果；

（5）缓解事故的放射性后果。

3.2 设计基准的内容

3.2.1 仪控系统总体结构以及每个仪控系统均应有文档化的设计基准。

3.2.2 仪控系统总体结构即核动力厂仪控系统的配置架构。核动力厂仪控系统总体结构下包括多个仪控系统，每个仪控系统具有特定作用。

3.2.3 设计基准确定仪控总体以及每个仪控系统的功能、工况和具体需求。这些信息用于将功能分类并分配到具有适当安全分级的系统。

3.2.4 在某些情况下，仪控系统的需求需要在核动力厂的设计和设计基准的开发过程中确定。因此，在项目初期可能无法获得仪控设计基准的完整内容。

3.2.5 仪控设计基准的开发应源自核动力厂安全设计基准。

3.2.6 仪控设计基准的开发应考虑但不限于以下信息：

（1）核动力厂的纵深防御概念；

（2）要提供的安全功能（见第 3.2.3 节）；

（3）核动力厂安全重要功能的安全分类、功能以及性能需求；

（4）自动与手动控制之间的优先原则，以及一个以上系统

可驱动同一个设备或功能时各个自动动作之间的优先原则；

（5）仪控系统执照监管要求；

（6）仪控系统安全分级要求；

（7）运营监管要求；

（8）对核动力厂安全和网络安全功能有关键影响的数字化仪控系统的分析与识别；

（9）网络安全的风险评估及影响分析；

（10）信息和控制需求及分配；

（11）核动力厂运行策略；

（12）人员可靠性分析；

（13）运行人员的职责；

（14）人员配备水平。

3.2.7 仪控系统的设计基准应确定仪控总体以及每个仪控系统必需的能力、可靠性与功能性，具体如 3.2.7.1-3.2.7.4 所述。

3.2.7.1 所有的功能需求，例如：

（1）需要使用各仪控系统的核动力厂运行状态；

（2）各仪控系统运行所处的不同核动力厂配置；

（3）针对每种核动力厂状态、运行模式以及长期停堆的功能性要求，例如定义输入和输出的转换关系和需执行的动作；

（4）每个所需的仪控功能的安全重要性；

（5）系统需要响应的假设始发事件；

（6）每个仪控系统在仪控总体结构的纵深防御策略中所起

的作用；

（7）被监测的变量或变量的组合；

（8）所需的控制和保护功能，包括对采用自动或手动控制（或两者兼而有之）动作以及控制位置的规定；

（9）每个仪控安全功能所需的量程、变化率、准确度、数值量化、计算精确度，以及响应时间，等。

3.2.7.2 为达到必要的可靠性与可用性水平而提出的所有要求，例如：

（1）安全功能的独立性要求；

（2）定期试验、自诊断和维护的要求；

（3）定性的或定量的可靠性与可用性目标，可通过概率论方法、确定论方法或同时使用两种方法来确定；

（4）对故障行为的要求。

3.2.7.3 为达到必要的网络安全水平而提出的所有要求，例如：

（1）设计中需要遵守的网络安全及运行限制；

（2）将要实施的网络安全手段。

3.2.7.4 保证设备鉴定适当性的要求，例如：

（1）设计准则，包括对仪控系统应遵守的标准的规定；

（2）可能会使系统在执行其功能时出现性能劣化的核动力厂工况，以及为维持系统必要能力所需采取的措施；

（3）系统执行安全重要功能的内外部危险（包括自然现象）的范围；

（4）系统执行安全重要功能的核动力厂环境条件的范围，包括仪控设备在设计基准事故、内部事件或外部事件中可能经受的正常、异常和极限环境条件。需要充分地考虑仪控系统之间，特别是不同鉴定等级的部件之间的相互影响，避免违背纵深防御的要求；

（5）材料使用的限制；

（6）核动力厂实体设计及布置的限制，包括对设备位置、电缆路径以及电源的限制；

（7）设备的物理位置以及设备之间的接口。

3.2.8 此外，安全系统的设计基准还应确定 3.2.8.1-3.2.8.6 所述内容。

3.2.8.1 驱动安全系统的参数的限值（分析限值；见第 6.9.5 节及图 3）。

3.2.8.2 需要显示的变量和状态，从而使操纵员能够确认系统保护功能的执行。

3.2.8.3 论证所有非自动触发的安全动作的合理性，包括：

（1）允许手动控制的时机、事件、时长和核动力厂工况；

（2）允许仅通过手动方式触发或触发后仅通过手动进行控制；

（3）在核动力厂运行状态及事故工况下，需要手动操作时操纵员所处的环境条件范围；

（4）确认操纵员在进行手动操作时所需要考虑的信息将在

适当的位置显示并且必须具备支持操纵员操作的性能特点。

3.2.8.4 允许执行仪控安全功能旁通的条件。

3.2.8.5 保护系统动作后复位所必须满足的条件。

3.2.8.6 用于缓解共因故障后果的多样化功能需求。

3.2.9 上述各项需求可在仪控总体设计基准或各仪控系统设计基准中规定。对于某些项目，可在仪控总体设计基准中规定总的需求，然后在各仪控系统设计基准中规定更加具体的需求。无论何种情况，仪控总体设计基准与各仪控系统的设计基准应相互一致，不同的设计基准之间的关系和接口也应便于理解。

4 仪控系统结构

4.1 结构设计概述

4.1.1 仪控总体结构设计将确定：

（1）构成总体结构的仪控系统；

（2）仪控系统的组织架构；

（3）仪控功能在系统间的分配；

（4）仪控系统间的互联，以及其中分配和禁止的交互；

（5）对总体结构的设计限制（包括禁止的交互和行为）；

（6）仪控系统间边界的确定。

4.1.2 单个仪控系统的结构设计将确定：

（1）各个集成层级的组合-分解关系，直至不可拆分的单个物项；

（2）各集成层级的每个物项的仪控功能分配、行为、限制条件及其对应的质量要求；

（3）可组合性和组合的规则，以保证当前层级的行为组合可满足其上一层级的行为要求，同时不会引入其他的行为；

（4）各层级内部和层级间设备和部件的互联，以及各种互联所允许和禁止的交互；

（5）对各系统的设计限制条件（包括禁止的交互和行为）。

4.1.3 数字化仪控系统之间具有更多互联且更加难以分析(因此相较于模拟仪控系统更难保证其安全性）。合理设计的仪控系统结构可以保证纵深防御和多样性的建立，并将这些难以分析的特性局部化并包络在各系统中，避免由于这些特性使得对于核动力厂安全的保证过于困难。

4.1.4 仪控系统的总体结构和各仪控系统的结构应满足核动力厂要求，包括系统接口要求，以及对例如安全、网络安全、可验证性、可分析性、时间限制等特性的要求。

4.1.5 设计必须体现纵深防御。纵深防御的各层次之间应尽实际可能地相互独立，避免一个层次防御的失效降低其他层次的有效性。

4.1.6 仪控系统的总体结构不应违背核动力厂设计的纵深防御概念和多样性策略。

4.1.7 仪控系统的总体结构应明确自身的纵深防御概念和多样性策略。

4.1.8 在仪控总体结构设计中，还应确定支持核动力厂纵深防御和多样性不同层级的仪控系统间的独立性水平。

4.1.9 仪控总体结构内的纵深防御通过各条独立的防御线来实现，一条防御线的失效可以由下一条防御线弥补。

4.2 总体结构设计内容

4.2.1 仪控总体结构

4.2.1.1 仪控总体结构应包含满足核动力厂设计基准所需的所有仪控功能。

4.2.1.2 应明确需在所有仪控系统设计中保持一致性的技术内容，例如，核动力厂运行概念，人机接口设计标准，电缆路径限制，接地方法以及报警管理原则。

4.2.1.3 应明确纳入仪控总体结构的系统，用于：

（1）支持核动力厂的纵深防御概念和多样性策略；

（2）支持仪控总体的独立性设计基准；

（3）在不同安全分级系统和安全分类功能之间进行适当的隔离。

4.2.1.4 应确定仪控系统间的接口和通信方式。

4.2.1.5 对于仪控总体结构中的每项安全功能，应建立实现其可靠性要求的设计策略，包括符合单一故障准则、冗余、独立性、故障安全设计、多样性和可验证性（含可分析性和可测试性）等。如何实施这些策略以实现可靠性要求见第 6 章。

4.2.1.6 应支持安全组合满足单一故障准则。

4.2.1.7 应向主控制室、辅助控制室和其他运行或事故处理需要获取信息的场所提供必要的信息。

4.2.1.8 应为主控制室、辅助控制室和其他运行或事故处理需要执行控制的场所提供必要的操纵员控制手段。

4.2.1.9 应提供必要的自动控制手段，将工艺参数维持和限制在规定的运行范围内，并限制故障和偏离正常运行的后果，使其不超过安全系统的能力。

4.2.2 仪控平台的特性会影响仪控总体结构设计，同时仪控总体结构会对仪控平台提出功能和鉴定要求。因此建议将仪控平台的选择与仪控系统总体结构的设计结合起来考虑。安全系统的功能和鉴定要求通常不同于控制系统的功能和鉴定要求，考虑到这一点以及多样性的因素，仪控系统总体结构通常包含两个或两个以上仪控平台。

4.3 系统结构设计内容

每个仪控系统的结构设计：

（1）应提供所有必要的仪控功能，以满足其在仪控总体结构设计中承担的任务；

（2）适用时，应将系统划分成冗余序列并规定序列间的独立性程度。通常情况下，安全系统设置有冗余的序列以满足单一故障准则。较低安全等级的系统可能不需要因安全考虑而采用冗余配置，但也可以采用冗余设计以提高其在正常运行时的可靠性。可靠性实现策略上应有的考虑见第 6 章；

（3）应规定每个冗余序列中所包含的仪控物项；

（4）应描述分配给每个仪控物项的功能和其他系统需求；

（5）应规定系统内仪控物项间的接口和通信方式；

（6）应规定主要物项和数据链的主要设计特性。

4.4 独立性

4.4.1 仪控系统总体结构中的独立性用来防止系统间故障的传播，在可行的范围内避免同一共因故障源对多个系统产生影响。共因故障源包括内部事件、外部事件、共用支持系统故障等。

4.4.2 仪控系统的总体结构既不能损害安全系统序列间的独立性，也应尽实际可能地不损害核动力厂不同纵深防御层级间的独立性。

4.4.3 需要完全独立的仪控系统功能应分配给独立的硬件系统或物项。

4.4.4 安全系统应独立于低安全等级的系统。

4.4.5 安全系统内的冗余序列间应保持充分的独立，以保证所有安全功能在需要时能够完成。在冗余序列间必须进行通信时（例如用于表决或局部触发），应采取适当措施保证电气隔离、实体隔离和通信的独立性。用于表决目的的通信能够限制由随机故障引起的误动作，避免其影响安全。

4.4.6 操纵员接口不应同时闭锁一个以上的冗余序列的安全功能。

4.4.7 安全系统的控制站可通过优选功能操作其所属序列之

外的安全设备，优选功能应符合第 6.2.4.9.12 节要求。

4.4.8 只有当安全系统具有对设备操作的优先权时，安全系统或部件才可接受来自低安全等级系统的操纵员手动控制。

4.4.9 若满足第 6.2.4.1-6.2.4.9 节要求，安全系统的信息可在低安全等级的控制站上显示。

4.4.10 当发生需要安全系统响应的事故工况或由于内外部危险导致的工况时，安全系统和部件应能承受这些工况的影响，有能力执行其安全功能。

4.4.11 安全仪控系统支持设施的故障或误动作不应影响安全系统冗余部分之间、安全系统和低安全等级系统之间、核动力厂纵深防御不同层次之间的独立性。

4.5 共因故障

4.5.1 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，以确定如何应用多样性、多重性、独立性原则来实现所需的可靠性。

4.5.2 产生共因故障的原因包括人因失误、开发和制造过程中的错误、维护中的错误、软件开发工具的错误、系统或部件间故障的传播、对于内外部危险不充分的规范说明、鉴定或防护等。

4.5.3 仪控系统的总体结构应明确所采用的结构化理念，使得核动力厂纵深防御层次间尽实际可能地相互独立。

4.5.4 为保持核动力厂不同纵深防御层次间的独立性，仪控系统的设计应防范系统内部或系统间出现共因故障。为实现这一

目标，应充分考虑功能在不同系统及系统各部分的分配，系统间应保持适当水平的独立性，同时应详细说明防范安全系统共因故障的策略。

4.5.5 应评估仪控系统总体结构中共因故障影响一个或多个基本安全功能的可能性。

4.5.6 在评估中对某项已经识别的共因故障不予考虑时，需要论证其合理性。

4.5.7 应分析安全分析范围内要求保护系统执行必要安全功能的每个假设始发事件叠加妨碍保护系统执行上述功能的共因故障所产生的后果。

4.5.8 纵深防御和多样性分析是实现第 4.5.7 节所述分析的一种方法。详见第 2.3.5.4 节。

4.5.9 如果第 4.5.7 节所述分析表明某假设始发事件叠加保护系统共因故障会导致不可接受的后果，则应修改相关设计。

4.5.10 彻底排除仪控系统和结构的所有共因故障薄弱点是不可能的，但应对所有已经识别的薄弱点是否可接受进行论证。

4.5.11 多样性

4.5.11.1 多样性是减少共因故障（来源于需求、设计、制造、维护中的错误）薄弱点的一种手段，同时也是在难以证明仪控总体或系统能否达到要求的可靠性水平时的一种保守的补偿方法。

4.5.11.2 当利用多样性缓解保护系统共因故障的影响时，应对该多样性措施达到了预期的缓解效果进行论证。

4.5.11.3 如果采用多样化的仪控系统，多样化系统和保护系统不应在规格书、设计、制造或维护方面出现相同的错误。

4.5.11.4 概率分析，包括可靠性分析和概率安全评价（PSA）等，不应将安全重要的仪控物项视为完全独立的（在概率分析中，完全独立的系统，其失效概率可以直接相乘），除非这些物项具备多样性并满足本导则中功能独立性、电气隔离、通信独立性、环境鉴定、抗震鉴定、电磁兼容鉴定、实体隔离和内外部事件防护方面的要求。

5 仪控功能、系统和部件的安全分级

5.1 应对在不同的核动力厂状态（包括正常运行的不同模式）下实现基本安全功能所需的所有仪控系统功能与设计措施加以识别。

5.2 安全重要仪控系统和部件的识别，以及根据其功能和安全重要性进行安全分级的相关要求应参考物项安全分级相关导则。

5.3 对于所有仪控系统功能，应根据它们的安全重要性进行分类。考虑以下三个因素：

（1） 未能执行该功能的后果；

（2） 需要该功能执行的假设始发事件发生的频率；

（3） 假设始发事件发生后，需要该功能执行的时刻或持续时间。

5.4 应确定执行安全分类中每个功能的仪控系统和部件并对其进行分级。分级主要依据其所执行功能的安全分类。

5.5 在确定安全分级时，应考虑可采取的替代动作的时效性和可靠性，以及检测和纠正仪控系统故障的时效性和可靠性。

5.6 对执行多个功能的物项，必须按照其执行的最重要功能划分其安全等级。

6 安全重要仪控系统的通用要求

6.1 概述

6.1.1 仪控系统应完全满足其设计基准。

6.1.2 安全仪控系统的所有特性都应有利于其安全功能。

6.1.3 安全仪控系统设计应避免不必要的复杂性，不应由于复杂性导致其违反其他设计原则(例如独立性、冗余性或多样性)。避免复杂性的目的是使仪控系统在完全满足其安全要求的基础上，尽可能简单。需要避免的复杂性列举如下：对仪控系统安全功能或其可靠性没有贡献的功能；采用未经过充分分析或验证的设计和实现措施；采用过于复杂而难以充分证明其安全性的实现平台。因此，仪控总体结构应采用简单的交互方式和通信连接。仔细记录和审查每条需求的合理性是一种避免不必要的复杂性的有效手段。

6.2 可靠性设计

6.2.1 安全重要仪控系统必须具有与所执行的安全功能相适

应的高可靠性和定期可试验性。必须在实际可行的范围内采用各种设计技术，以防止安全功能的丧失。在仪控系统中能够提高功能可靠性的特性列举如下：随机故障容错能力、设备和系统的独立性、冗余性、多样性、共因故障容错能力、可试验性（必要时包括自检能力）、可维护性、故障安全设计和选择高质量设备。

6.2.2 单一故障准则

6.2.2.1 必须对核动力厂设计中所包括的每个安全组合都应用单一故障准则。当把单一故障准则应用于一个安全组合或安全系统时，必须将误动作视为故障的一种模式。可采用冗余、独立性、可试验性、连续监测、环境鉴定和可维护性等方面的措施来满足单一故障准则。

6.2.2.2 安全系统在下列情况下应完成（导致预计运行事件或设计基准事故的）某一假设始发事件需要的全部安全功能：

（1）在安全系统内存在单一可探测故障，并同时存在可判别但不可探测的故障（不可探测的故障即不能通过定期试验、报警、异常指示来揭示的故障）；

（2）由上述单一故障引起的所有故障；

（3）导致需要安全系统执行安全功能的假设始发事件的所有故障和系统误动作，或由上述假设始发事件引起的所有故障和系统误动作。

6.2.2.3 在对单一故障准则的符合性分析中，由设计、维护、运行或制造等方面的错误导致的故障不包括在内。此类错误中，

对于已知的错误，应通过质保活动妥善处理；对于未知的错误，其影响是无法预知的。因此，单一故障准则并不是一种分析理解这类错误对安全组合影响的有效工具。如何分析评估此类错误导致的共因故障的潜在后果在第 4 章讨论。

6.2.2.4 只允许在某些特殊情况下可以不符合单一故障准则，且应在设计文件中加以标识，并在安全分析中进行清晰的论证。

6.2.2.5 论证低频率事件（例如外部危险）不必符合单一故障准则时必须非常谨慎。尤其应考虑保证安全系统运行和监测所必需的电气系统和其他支持系统的长期可用。

6.2.2.6 可以采用可靠性分析、概率评估、运行经验、工程判断或这些方法的组合，来论证在运用单一故障准则时不必考虑某一特定故障的合理性。

6.2.2.7 当符合单一故障准则仍不足以满足可靠性要求时，应提供补充的设计措施，或对设计进行修改，以确保系统满足可靠性要求。

6.2.3 冗余

6.2.3.1 仪控系统冗余度应满足其可靠性要求和单一故障准则。

6.2.3.2 冗余是仪控系统中常用的实现系统可靠性目标，以及符合单一故障准则的方法。冗余部件应相互独立，否则冗余就不能完全有效。冗余提高了可靠性，但也增加了误动作的概率。通常采用冗余信号符合（表决逻辑）或虚假信号剔除的方法在可

靠性和避免误动作之间取得适当平衡。

6.2.4 实现独立性的措施

6.2.4.1 独立性用于防止某个故障、内部危险或外部危险影响安全系统的冗余部件，也用于防止某个故障或危险影响纵深防御不同层次的系统。应考虑的故障包括：设计基准事故引起的故障、暴露于同一危险引起的故障、系统之间或冗余序列之间的电气连接引起的故障、系统之间或冗余序列之间的数据交换引起的故障，以及设计、制造、运行或维护中的共性错误。

6.2.4.2 实现独立性的措施包括：实体隔离、电气隔离、功能独立和通信独立（见第 7 章）。设备鉴定和多样性也可支持独立性，见第 6.3 节。应采用这些措施的组合来实现独立性目标。

6.2.4.3 当不同安全等级的系统之间使用了隔离装置，这些隔离装置应属于较高安全等级系统的一部分。

6.2.4.4 用于隔离各种物理影响、电气故障和通信错误的措施并非一定要集成到受保护设备中。系统隔离不同类型威胁的措施，可属于不同物理设备，或位于电路中的不同位置。对单一效应的隔离功能也可由多个设备共同完成。例如，对数据通信错误的隔离可以采用下列方式实现：由一个缓存存储器防止数据直接由其他冗余序列写入本序列，同时由另一个装置上的处理器实现有效性检查，以确保只有在数据满足有效性、正确性和真实性准则时才会从缓存存储器中读取。

6.2.4.5 应对为满足独立性要求所采用的设计措施的充分性

进行论证。

6.2.4.6 实体隔离

6.2.4.6.1实体隔离的应用列举如下：

（1）实体隔离可以防范由于内部危险而导致的共因故障。需要考虑的内部危险包括火灾、飞射物、蒸汽喷射、管道甩击、化学爆炸、水淹和邻近设备故障等。

（2）实体隔离可以防范在正常、异常或事故工况下的共因故障、事故（包括所有设计基准事故）的影响，或内部和外部危险的影响。例如，通过距离减弱电磁干扰影响，或在不同鉴定等级的系统和部件之间进行隔离。也可通过环境鉴定、抗震鉴定、电磁兼容鉴定，或连同实体分隔一起，防止事故、内部危险或外部危险的影响。

（3）实体隔离可以降低具有局部效应的外部事件（例如飞机坠毁、龙卷风或海啸）导致共因故障的可能性。

（4）实体隔离可以降低在冗余设备的运行或维护过程中由于疏忽导致其同时出现差错的可能性。

6.2.4.6.2 安全系统物项应与低安全等级系统物项进行实体隔离。

6.2.4.6.3 安全组合的各冗余部分之间应进行实体隔离。

6.2.4.6.4 一些情况下冗余设备间充分的实体隔离是不现实的，如冗余的传感器或驱动器必须紧凑布置时（例如控制棒驱动机构或堆内仪表），或在某些设备或线缆汇集的区域（例如安全

壳贯穿件区域、电机控制中心、开关设备区域、线缆分布间、设备间、主控室和其他控制室、核动力厂过程计算机），此时应在实际可行的范围内尽可能进行隔离，并应对不满足隔离要求的情况进行合理性论证。

6.2.4.6.5 实体隔离可通过距离、屏障或这两者的结合来实现。

6.2.4.6.6 防范火灾和其他内部危险的具体要求见防火与防爆设计相关以及其他内部危险防护设计相关的核安全导则。

6.2.4.7 电气隔离

6.2.4.7.1 电气隔离用于防止一个系统内的电气故障对与之连接的系统或同一系统内的冗余设备造成影响。

6.2.4.7.2 安全系统和部件应与低安全等级的系统和部件进行电气隔离。

6.2.4.7.3 安全组合的各冗余部分之间应彼此电气隔离。

6.2.4.7.4 提供电气隔离的装置应防止在装置一侧的最大可信电压或电流瞬变、接地、开路和短路导致与之相连的安全电路出现不可接受的运行劣化。

6.2.4.7.5 电气隔离措施列举如下：无电气连接，提供隔离能力的电子装置，光电隔离装置（包括光纤）、继电器、通过距离和内部机械结构分隔，或这些措施的组合。

6.2.4.8 相关电路

当在安全电路和较低安全等级的电路之间不能提供充分的实体隔离或电气隔离时，较低安全等级的电路（称为“相关电路”）

应满足下列要求：

（1）应进行分析或测试，以证明该关联不会导致相连的安全电路出现不可接受的降级。例如，分析或测试可考虑相关电路中的最大电压，与安全级电路可以承受的电压值进行比较；

（2）应规定为与其相关联的安全序列的一部分；

（3）与其他部件的实体隔离，其程度应与它相关联的安全序列电路相同。

6.2.4.9 功能独立

6.2.4.9.1 功能独立性是指一个系统所需功能的实现不依赖于其他系统的任何行为（包括故障或正常运行），或者来自其他系统的任何信号、数据或信息。功能独立性是实现系统与其他系统隔离的一种手段，也可用作实现冗余设备之间隔离的手段。

6.2.4.9.2 功能独立性取决于结构设计和对不同功能之间的共用数据的处理（结构设计的考虑见第 4 章。共用数据的处理见第 6.2.4.9.3-6.2.4.9.13 节）。

6.2.4.9.3 来自较低安全等级仪控系统的输入不应对安全系统执行其安全功能的能力产生不利影响。

6.2.4.9.4 较低安全等级的监测系统可与安全系统连接，但必须证明该监测系统不会干扰安全系统的运行。

6.2.4.9.5 某些情况下安全系统会需要非安全级的维护系统（例如用于执行维护、软件更新、测试或设置配置数据的系统）的输入。当安全系统要与低安全等级的维护系统连接，只有在受

影响的序列或通道处于离线状态，来自维护系统的数据仅用于某一特定目的，且和维护系统的连接符合网络安全程序的情况下，才能进行连接，并应在数据输入后进行验证。

6.2.4.9.6 如果要允许进行通道级维护，应在属于同一序列内的多个通道之间提供充分的隔离。

6.2.4.9.7 应明确规定维护系统可以连接到安全系统时的核动力厂运行模式。

6.2.4.9.8 安全系统与低安全等级系统之间的数据传输应设计成低安全等级系统中的可信故障不会妨碍与之相连的安全系统完成其安全功能。

6.2.4.9.9 一个安全组合的冗余设备之间的数据通信应设计成发送设备的可信故障不会妨碍与之连接设备满足其要求。

6.2.4.9.10 在计算机系统中，当高安全等级系统向低安全等级系统提供数据时，通常采用单向、广播式数据通信。应考虑采用硬件层面的单向性特性作为一种确保单向通信的手段，例如，通信链路在高安全等级系统一侧仅连接发射器，在低安全等级系统一侧仅连接接收器。

6.2.4.9.11 如果经过论证满足下列条件，则可以将模拟量或开关量信号以硬接线方式从低安全等级系统发送到高安全等级系统：

（1）低安全等级系统中的可信故障不会妨碍相连的安全系统完成其安全功能；

（2）低安全等级系统的故障导致安全系统部件误动作的可能性及其后果是可接受的。

6.2.4.9.12 如果安全系统驱动器根据来自其他系统（包括低安全等级系统）的信息动作时，应采取措施确保来自其他系统的错误数据不会阻止安全功能的执行。通常，这是通过使用优选逻辑来实现的，优选逻辑保证来自安全系统的数据和命令优先。

6.2.4.9.13 第7.3.10.3-7.3.10.9节为保护系统和控制系统共用信号输入的情况提供了补充指导。

6.2.5 多样性

6.2.5.1 很难证明计算机系统或使用复杂硬件功能、复杂硬件逻辑、复杂电子器件的系统的可靠性。如果无法证明仪控系统执行的功能具有足够的可靠性，那么可以使用多样化的仪控设备来提高实现基本安全功能的置信度。

6.2.5.2 对于是否采用多样性来实现设计基准事故条件下的基本安全功能，应进行合理性论证。

6.2.5.3 当采用多样性以应对潜在共因故障时，应考虑使用多种类型的多样性。不同的多样性类型列举如下：

（1）设计多样性：使用不同的设计方案来解决相同的问题或类似的问题。

（2）信号多样性：系统根据不同的核动力厂参数来启动安全动作。

（3）设备多样性：采用不同技术的硬件（例如，模拟设备

与数字设备，固态设备与电磁设备，基于计算机的设备与基于现场可编程门阵列的设备）。

（4）功能多样性：系统采用不同的保护动作来达到相同的安全目标。

（5）开发过程的多样性：使用不同的设计组织，不同的管理团队，不同的设计和开发团队以及不同的实现和测试团队。

（6）逻辑多样性：使用不同的软件或硬件描述语言，不同的算法，逻辑功能的不同时序或顺序。

6.2.5.4 在采用多样性时，应证明所选择的多样性类型达到了预期的共因故障缓解目标。

6.2.5.5 在同一系统中可应用不同的多样性，例如功能多样性和信号多样性可以在同一个系统中应用。

6.2.5.6 应避免多样性应用中潜在的共性，例如类似的材料，类似的部件，类似的制造工艺，类似的逻辑，类似的运行原理或共同的支持设施。如不同的制造商可能会使用相同的处理器或相同的操作系统授权，从而会有可能引入共同的失效模式。如果不考虑这种可能性，仅根据制造商名称或型号的差异就宣称具备多样性是不充分的。

6.2.6 故障模式

6.2.6.1 必须恰当地考虑故障安全设计原则，并贯彻到核动力厂安全重要系统和部件的设计中。在适用时，应将安全重要系统和部件设计为故障安全，使其自身的故障或支持设施的故障不妨

碍预定安全功能的执行。

6.2.6.2 当某个仪控部件失电或出现故障（该故障模式是已知并且有记录的）时，系统应被置于一个预定状态下，这个状态应已被证明对于安全是可接受的。

6.2.6.3 确保故障时使系统处于安全状态的方法包括将系统设计成在失电时进入安全状态，或使用“看门狗定时器”来检测设备不再执行其设计功能的情况并将系统置于安全状态等。

6.2.6.4 在应用第 6.2.6.2 节要求时，故障安全设计措施自身的失效也应予以考虑。

6.2.6.5 仪控部件和系统的非系统性故障模式应是已知的并形成书面记录。

6.2.6.6 在将故障安全概念应用于系统设计时，了解部件的故障模式非常重要。同时，了解部件的故障模式对于确认控制系统故障不会导致某些超出了安全分析范围的事件也是很重要的。

6.2.6.7 软件错误可能导致的故障很难预测。然而，可能不需要了解软件的失效机理，也可以通过装置端口所见来判断可能的故障状态。一种方法是对可能的故障模式进行识别和分类，形成易于处理的一组可能性(例如错误输出、延迟输出和冻结输出)。

6.2.6.8 主要由硬件或软件设计中的系统性原因导致的故障模式本质上是不可预测的。因此，故障安全设计的概念无法处理由这类原因导致的故障。规范的开发过程（见第 2 章），危害分析（见第 2.3.2 节），纵深防御概念的应用（见第 4 章）和多样

性的应用（见第 6.2.5 节）是减少此类系统故障原因以及应对此类原因影响的更为有效的手段。

6.2.6.9 仪控部件的故障应可以通过定期试验或自诊断检测出来，或通过报警或异常指示自呈现。

6.2.6.10 宜采用故障自呈现的方式。故障自呈现的机制不应将系统置于不安全状态或导致安全系统的误动作。

6.2.6.11 在评估与单一故障准则的符合性时，应假定任何已识别但不能通过定期试验、报警或异常指示检测到的故障是与单一故障同时存在的。自检设施、自诊断设施或自报警设施本身的故障也应被检测和显示。

6.2.6.12 在实际可行的范围内，部件的故障不应引起安全系统的误动作。

6.2.6.13 在安全仪控系统或部件重启或恢复供电时，除非是响应有效的安全信号，否则输出应初始化为预定的安全状态。

6.3 设备鉴定

6.3.1 总的鉴定要求

6.3.1.1 仪控系统和部件应针对其在役寿期内的预期功能进行鉴定。

6.3.1.2 仪控部件的鉴定应包括其软件、硬件描述语言和工艺接口（如果有）。

6.3.1.3 鉴定应提供与系统或部件的安全重要程度相称的置信度水平。

6.3.1.4 鉴定大纲应涵盖对各个系统或部件执行其预期功能的适用性有影响的所有方面，包括：

（1）功能和性能的适用性和正确性；

（2）环境鉴定；

（3）内部和外部危险影响鉴定；

（4）电磁兼容鉴定。

6.3.1.5 设备鉴定应在以下方法的基础上选择：

（1）使用符合标准的工程设计和制造过程；

（2）可靠性证明；

（3）运行经验；

（4）型式试验；

（5）供货设备的测试；

（6）对测试结果或相关条件下运行经验的推论分析；

（7）对制造商生产过程的评估；

（8）制造过程中的部件检查。

6.3.1.6 通常情况下没有必要应用第 6.3.1.5 节提到的所有方法。所选方法的具体组合取决于需鉴定系统或部件的情况。例如，对已开发物项的鉴定，可能更多地将重点放在以往经验和分析上，以弥补其缺少工程设计制造期间完整验证和确认文档的不足。

6.3.1.7 设备鉴定所采用的方法或方法组合应经过合理性论证。

6.3.1.8 在使用运行经验来支持设备鉴定时，应证明运行经

验与目标应用的用途和使用环境的相关性。

6.3.1.9 对于安全系统而言，仅以运行经验作为鉴定的证据是不充分的，因此应结合采用型式试验和供货设备的测试，以及制造商生产过程评估或制造过程中对部件的检查。

6.3.1.10 分析可作为设备鉴定证据的一部分，此时应包括对所用方法、理论和假设的合理性论证。例如，根据试验数据、测试数据或运行经验来论证用于设备鉴定的数学模型的正确性。

6.3.1.11 应在每个所安装的安全重要系统和部件与适用的鉴定证据之间建立可追溯性。这不仅包括部件本身的可追溯性，还包括鉴定配置与实际安装配置之间的可追溯性。

6.3.2 适用性和正确性

6.3.2.1 设备鉴定大纲应证明仪控系统和部件的设计符合它们的设计基准和设备规格书中包含的所有功能需求、性能需求和可靠性要求。

6.3.2.2 功能需求包括应用所需的功能、支持系统或设备工作所需的功能、操纵员接口的要求以及与输入/输出范围有关的需求等。

6.3.2.3 性能需求包括对精度、分辨率、量程、采样速率和响应时间的需求等。

6.3.2.4 可靠性要求包括最小平均无故障时间、故障安全特性、独立性、故障检测、可试验性、可维护性和在役寿命的要求等。

6.3.2.5 设备鉴定大纲应论证实际设计、最终的仪控系统和所安装的部件与已经通过鉴定的设计是一致的。

6.3.3 环境鉴定

6.3.3.1 环境鉴定是指在部件所处的影响其正确执行功能的环境条件下的鉴定，包括温度、压力、湿度、化学暴露、辐照、浸没、电磁现象和老化机理。

6.3.3.2 系统和部件应设计成能够承受要求其执行功能的正常运行、预计运行事件和假设事故工况下的相关环境条件影响，与上述环境相适应，并应对此进行证明。

6.3.3.3 和缓环境

对于仪控部件始终（包括在事故期间）工作在和缓环境的情况，仪控部件的环境鉴定可以基于规定了核动力厂各个运行状态下具体环境条件的功能需求规格书，以及供应商证明文件或对部件能够在规定的环境条件下执行其要求功能的评估。

6.3.3.4 严酷环境

6.3.3.4.1 对于仪控部件在事故期间的某一时段需要在严酷环境下工作的情况，仪控部件的环境鉴定应证明在其鉴定寿期末，仍能够在所有规定的工作环境条件范围内执行其安全功能。

6.3.3.4.2 对部件在其鉴定寿期内能够按要求执行功能的证明，涉及对显著老化效应（例如辐射和热老化）的处理，以证明所需的功能在鉴定寿期末仍能够保持。通常应包括适量的保守裕度，以能够包络非预期的老化机理。

6.3.3.5 在设备鉴定大纲的技术说明中，应考虑工作环境条件的最严酷的可信组合，包括工作环境条件之间的协同效应。

6.3.3.6 如果需要针对不同的环境条件分别进行试验（例如分别对辐射效应和温度效应进行单独测试），则应对这些试验的顺序进行合理性论证，以说明能够恰当的模拟组合环境条件所引起的部件劣化。

6.3.3.7 可只对最高安全等级的部件采用最严格的环境鉴定方法。

6.3.3.8 对于要求在严酷环境下运行的安全系统部件，环境鉴定应包括型式试验。

6.3.3.9 如果使用防护屏障作为防止环境影响的隔离设备，屏障本身也应通过鉴定程序确认其有效性。

6.3.3.10 内外部危险

6.3.3.10.1 核动力厂设计基准和安全分析将识别内部和外部危险，例如火灾、水淹和地震事件，核动力厂需要承受这些危险并保持运行或维持安全，为此需要针对这些危险采取防护措施或进行设备鉴定。核动力厂设计基准和安全分析也将识别由于系统性原因（例如工程设计决策或设计缺陷）导致的会引起安全功能劣化的危险，应确定相应的系统限制以防止安全功能的劣化。

6.3.3.10.2 仪控系统和部件的防护设计应参考核动力厂内、外部危险防护相关的核安全导则。

6.3.3.10.3 仪控系统和部件还应对核动力厂设计基准中规定

的其他外部危险进行防护，或者按能够承受这些外部危险进行设计和鉴定。

6.3.4 电磁兼容鉴定

6.3.4.1 电磁兼容性是指系统或部件在其电磁环境中能够可靠地执行功能而不会对该环境中的任何设备引入不能容忍的电磁干扰的能力。电磁兼容性包括两个部分：物项对电磁干扰的敏感度以及对电磁环境中电磁干扰的贡献（发射）。

6.3.4.2 在本导则中，电磁干扰包括射频干扰，也包括浪涌，如由开关瞬态造成的电压尖峰。

6.3.4.3 电气电子系统和部件的运行能否不受干扰影响取决于部件与其运行环境的电磁兼容性，即部件承受由其周围或与其连接的部件引起的干扰的能力。

6.3.4.4 电磁干扰的重要来源包括开关设备、断路器或熔断器的分断故障电流；无线电发射装置产生的电场；自然干扰源如雷击或太阳风暴；和其他人为导致的核动力厂内外部干扰源。

6.3.4.5 仪控系统和部件的电磁兼容鉴定取决于以下三者的组合：通过系统和部件设计最大限度地减少电磁噪声与仪控部件的耦合，通过测试证明部件可以承受预期的电磁辐射水平，以及通过测试证明电磁发射处于可接受的水平。

6.3.4.6 用于减小电磁噪声的产生和耦合的措施包括：

（1）抑制源处的电磁噪声；

（2）仪控信号电缆与动力电缆分隔和隔离；

（3）将设备和电缆同外部磁场和电磁辐射源屏蔽；

（4）在耦合到敏感电子设备之前过滤掉电磁噪声；

（5）电子设备对地电位差的消除或浮空；

（6）电气和仪控设备、电缆通道、机柜、部件和电缆屏蔽层的正确接地。

6.3.4.7 适当的安装和维护对于保证上述措施的正确应用和持续有效至关重要。

6.3.4.8 应确定对安全系统和部件电磁兼容性的具体需求，并证明其符合这些需求。

6.3.4.9 一般工业环境的电磁兼容性国际和国家标准可以作为鉴定需求的基础，并应对其进行必要补充以满足核动力厂特有的电磁兼容性需求，这些需求可能更加严苛。确定电磁兼容性需求时应考虑到仪控部件暴露于重复性瞬变（例如感性负载分闸和继电器振铃现象）和高能浪涌（例如电源故障和闪电）的可能性。

6.3.4.10 通常需要对每个核动力厂机组进行具体分析以确定机组内仪控部件的电磁环境。这些分析用于判断每个仪控部件的电磁兼容能力是否适当。

6.3.4.11 安全重要的设备和系统（包括相关电缆）的设计和安装应确保能够承受其所处位置的电磁环境。

6.3.4.12 在仪控系统和部件的设计中要考虑的电磁干扰包括以下方面：

（1）电磁干扰的发射，和对电磁干扰的抗扰度；

（2）通过电缆的电磁发射干扰和传导干扰；

（3）静电放电；

（4）开关瞬态和浪涌；

（5）核动力厂中使用的无线系统和设备，以及维修、维护和测量设备的发射特性，例如移动电话、无线电收发器和无线数据通信网络。

6.3.4.13 在某些敏感设备附近应建立禁区，以限制无线设备和其他便携式电磁干扰源（例如焊接设备）的使用。

6.3.4.14 设备鉴定大纲应证明，当安全仪控系统部件暴露于电磁干扰和浪涌运行包络限值之内时，能够执行其安全功能。

6.3.4.15 核动力厂中的任何电气或电子设备都会对电磁环境有影响。因此，不仅要限制安全重要设备的电磁辐射发射和传导发射，也要限制非安全重要设备的电磁辐射发射和传导发射。

6.3.4.16 在设计中应识别那些对安全重要仪控设备和系统所处电磁环境有显著贡献的电气或电子设备，在实际可行的前提下为此类设备建立电磁辐射发射和传导发射限值，或了解其发射水平，相应地采取各种减少电磁噪声耦合的措施，确保安全重要仪控设备和系统在可承受的电磁干扰水平之内运行。

6.3.4.17 单个部件的发射限制应做到：在系统和部件的所有模式和状态下，包括模式或状态的切换以及劣化工况，在运行环境中产生的发射干扰在每个部件能够承受的电磁干扰的安全（无危害）包络限值之内。应证明第 6.3.4.16 节所述的要建立限值的

设备，其电磁发射都在规定的限值内。

6.3.4.18 设备和系统（包括相关电缆和电源）的设计和安装应适当限制核动力厂设备之间电磁干扰的传播（通过发射和传导方式）。

6.3.4.19 如果多个仪控系统连接到同一电源，电磁兼容鉴定应评估电磁干扰的传播路径。

6.3.4.20 应根据传输信号的特性和应用环境，采用绞合、屏蔽等型式的信号电缆，减少电磁干扰和静电干扰。

6.3.4.21 核动力厂电力系统设计相关的核安全导则提供了接地、电缆选择和电缆敷设的指导，以减少电磁干扰的产生和传播。

6.4 应对设备老化和过时的设计考虑

6.4.1 必须确定核动力厂安全重要物项的设计寿命。设计必须提供适当的裕度，以考虑有关老化、中子辐照脆化和磨损机理，以及与服役年限有关的性能劣化的可能性，从而保证安全重要物项在其整个设计寿期内执行所必需的安全功能的能力。

6.4.2 必须考虑到在所有正常运行状态，包括试验、维修和维修停役，以及在假设始发事件中及其后的核动力厂状态下的老化和磨损效应。

6.4.3 必须采取监测、试验、取样和检查措施，以评价设计阶段预计的老化机理，以及识别在使用中可能发生的未预期到的行为或性能劣化。

6.4.4 电气和电子系统和部件的鉴定在役寿命可能显著短于

核动力厂的寿期。

6.4.5 由老化导致的降级会影响部件在严酷环境条件下执行功能的能力，这种降级可能在正常条件下部件的功能性受到明显影响之前就出现了。

6.4.6 在设计过程中应识别能够显著影响仪控部件的老化机理并确定跟踪这些机理影响的手段。

6.4.7 确定老化的潜在影响首先要了解各种仪控部件的相关老化现象。最常见的仪控部件老化原因是暴露于高温或辐射环境中。但是，在按第 6.4.6 节要求识别老化机理时，还应考虑到具体设备可能还有其他老化现象（例如微电路中的电子迁移，“锡须”的形成，机械振动或化学降解）。

6.4.8 维护程序应包括识别劣化（老化）趋势的活动，包括对可能导致设备无法执行其安全功能的前兆的探测。具体技术有：

（1）以适当的时间间隔对会受到老化影响导致性能劣化的有代表性的部件或单元进行试验；

（2）目视检查；

（3）运行经验分析。

6.4.9 应对老化影响的手段包括：

（1）在鉴定寿命结束之前更换部件；

（2）考虑老化的影响，调整功能特性（例如重新标定）；

（3）改变维护程序或环境条件，延缓老化过程。

6.4.10 应确定需要在严酷环境下执行安全功能的安全系统

部件的鉴定寿命。

6.4.11 安全系统部件应在鉴定寿命结束之前更换。

6.4.12 在役鉴定的结果可能使部件的鉴定寿命得到确认，也可能显示与原来通过测试、分析或经验确定的鉴定寿命不同。在役鉴定的信息可用于延长或缩短部件的鉴定寿命。

6.4.13 应在设计时确定仪控系统和部件的预期在役寿命和预期报废时间，并将其通报给营运单位。对仪控系统和部件在役寿命和预期报废时间的估算，可以为营运单位提供必要的信息，以便其与供应商签订长期协议，制定备品备件采购计划，以及过时物项更换计划。

6.4.14 老化或过时可能会导致一些仪控系统的在役寿命显著短于核动力厂的寿期。因此，应适当考虑便于安装和切换到替代系统的技术措施，例如预留用于安装新设备和相关电缆的空间。

6.4.15 核动力厂老化管理相关核安全导则就老化管理和过时管理提供了进一步指导，并包括了对设备鉴定大纲与老化管理大纲之间接口的描述。

6.5 仪控系统的访问控制

6.5.1 应对仪控系统设备的访问进行限制，以防止未经授权的访问，并减少发生错误的可能性。行政管理措施和物理防护措施（例如，机柜上锁，房间上锁和机柜开门报警）的适当结合是一种行之有效的方法。

6.5.2 应特别关注对整定值调整手段、标定调整手段和配置

数据的访问控制，这对于防止由于操作或维护中的错误而导致系统性能劣化至关重要。

6.5.3 第 7.5.6.2.1-7.5.6.5.4 节为数字化系统的访问控制提供了补充指导。

6.6 运行期间的试验和可试验性

6.6.1 设计应保证能够对安全重要物项进行标定、试验、维护、修理或更换、检查和监测，以在设计基准规定的所有条件下保证其执行功能的能力并保持功能的完整性。

6.6.2 安全系统必须具有可在核动力厂运行时对其功能进行定期试验的条件，包括各通道分别进行试验的可能性，以查明可能发生的故障和多重性的丧失。设计必须允许对包括从传感器到最终的触发驱动器和显示单元所有环节的定期试验。

6.6.3 试验措施

6.6.3.1 仪控系统应包括试验措施。

6.6.3.2 与安全系统永久连接的试验措施应被视为安全系统的一部分，除非它们符合第 6.2.4.1-6.2.4.9 节中提出的独立性相关要求。

6.6.3.3 安全系统设备的试验和标定应可在所有正常运行（包括功率运行）模式下进行，同时应保持安全系统执行其安全功能的能力。

6.6.3.4 为了达到安全系统要求的可靠性，核动力厂运行期间的定期试验通常是必要的。然而，有些情况下，如果在核动力

厂运行期间进行试验会给其安全带来风险，就需要避免进行这种试验。在功率运行过程中进行试验和标定的好处，应与其可能对核动力厂安全造成的不利影响进行平衡。

6.6.3.5 如果不能在核动力厂功率运行期间对安全系统或部件进行试验，应保证：

（1）证明在两次试验的间隔时间内所影响的功能的可靠性是可接受的；

（2）证明在两次试验的间隔时间内未试验部件的准确度和稳定性是满足要求的；

（3）提供将未试验仪表通道的测量结果与其他设备进行比较的手段（例如比较核功率和热功率）；

（4）对未试验的系统或部件提供在停堆期间进行试验的能力。

6.6.3.6 自动试验、自监督和自监视

6.6.3.6.1 仪控系统应具有自监督或自监视措施，以便能定期确认其连续正确运行。

6.6.3.6.2 仪控系统的自监督或自监视措施应包括检查输入信号合理性的手段。

6.6.3.6.3 数字化安全系统应具有达到安全状态的措施，例如看门狗定时器。

6.6.3.6.4 系统或部件的设计应使故障自呈现，这是实现第6.6.3.6.1节要求的一种手段。

6.6.3.6.5 试验设施包括执行试验和相关试验序列的硬件和软件，试验可以是手动启动也可以是自动启动的。

6.6.3.6.6 应提供报警以指示安全系统冗余性的丧失。

6.6.3.6.7 自监督发现系统或设备故障时应采取预先规定的动作。

6.6.3.7 在试验期间仪控功能的保持

6.6.3.7.1 仪控系统试验措施（包括手动措施和自动措施）的设计应确保试验不会影响仪控系统执行其安全功能的能力，并将误触发安全动作的可能性和对核动力厂可用性的其他不利影响降至最低。

6.6.3.7.2 试验准备措施不应损害安全系统的独立性，也不应引入潜在的共因故障。

6.6.3.7.3 试验准备措施包括试验程序、试验接口、需安装的试验设备和内置的试验设施。

6.6.3.8 试验接口

6.6.3.8.1 仪控系统和部件的试验措施应具有以下特性：

（1）应具有适当的试验接口和状态指示手段；

（2）应能使仪控设备故障易于探测；

（3）应具有防止未授权访问的能力；

（4）应便于试验人员和试验设备接近；

（5）应有必要的通信设施来支持测试；

（6）试验地点的选择应确保试验和到达试验场地期间都不

会使操作人员暴露于危害环境中。在确定试验地点时需要考虑的因素有：传感器的位置应便于在该位置完成试验和标定；测试设备和装置应放置在便于对受试设备进行测试的区域；由于核动力厂条件或管理的因素可能会使测试设备难以到达受试设备所处位置（例如需要将设备沿着狭窄的路径运输或进出受污染的区域）；便于设备的状态指示和试验连接。

6.6.3.8.2 如果受试设备位于危险区域时，应提供措施以允许从危险区域之外控制试验。

6.6.4 试验大纲

6.6.4.1 仪控系统的设计应包括对试验和标定程序的说明。

6.6.4.2 仪控试验大纲通常应包括：

（1）对试验大纲目的的描述；

（2）待试验的系统和通道的描述；

（3）各项试验的频度和顺序；

（4）确定试验项目以及试验间隔的理由和合理性论证；

（5）对要求的文档和报告的描述；

（6）通过或未通过试验的准则，以及不符合项的处理流程；

（7）试验大纲有效性的定期审查要求；

（8）用于控制试验实施的各个试验程序的描述。

6.6.4.3 应对试验和标定的范围和频度进行论证，以说明其符合功能需求和可用性要求。

6.6.4.4 试验大纲应确认在试验期间和试验完成之后始终满

足下列条件：

（1）系统整体执行功能的能力不会劣化；

（2）安全仪控系统始终满足其功能需求和性能需求。

6.6.4.5 在试验大纲中，应将各项试验按适当顺序进行排列，以便可以对正在进行测试的系统或部件的总体状况立即进行评估，而无须进一步试验其他部件或系统。

6.6.4.6 试验大纲的执行不应导致任何核动力厂部件发生超出设计规定的劣化。

6.6.4.7 在执行试验大纲和确定部件是否达到鉴定寿期末时，可能需要考虑由于试验导致的损耗和老化。

6.6.4.8 试验大纲应提供：

（1）有关系统或部件状态的客观信息；

（2）对部件劣化的评估；

（3）用于探测劣化的趋势数据；

（4）系统早期失效的表征；

（5）对于失败过的试验，对重复试验可信性的评估要求。在试验失败之后，通常需要评估和记录导致试验失败的直接原因、根本原因和应采取的纠正措施，才可以进行重复试验并用其结果证明相关系统或部件的可运行性。纠正措施可能包括部件的维护或修理或对测试程序的更改。如果确认不需要采取纠正措施，其理由应予以记录。

6.6.4.9 试验大纲应对定期试验和标定的过程作出规定，使

其满足下列要求：

（1）规定从传感器到驱动器对安全功能的全面检查；

（2）试验能够在现场完成；

（3）确认设备的功能和性能满足需求；

（4）试验输入和输出功能，例如报警、指示、控制动作和驱动装置的运行，满足系统可靠性要求和功能需求；

（5）规定每个试验的预期结果；

（6）在试验过程中确保核动力厂的安全；

（7）减少误触发安全动作，以及对核动力厂可用性造成其他负面影响的可能性；

（8）禁止使用临时搭建的测试装置、临时跳线或临时修改计算机代码。测试设备临时连接到受试设备是允许的，但受试设备必须有为连接该测试设备而专门设计的接口。如果定期试验或标定需要临时连接，则应将此类试验设备的连接和使用纳入适当的管控；

（9）禁止修改核动力厂部件的配置参数，除非这些参数先前已被定义为可维护参数；

（10）尽可能缩短设备停用时间；

（11）在实际可行的前提下对每个传感器通道单独测试。

6.6.4.10 除第 6.6.4.9 节的要求外，安全系统定期试验和标定的过程还应满足下列要求：

（1）应采用一次性完成的在线试验，该试验能够在启动后

直接识别具体缺陷，而无须进行试验连接或不会妨碍在线设备及其运行超过一定的时间限制；

（2）应独立确认每个通道（包括信号检测、触发逻辑、驱动和支持功能）的功能需求和性能需求；

（3）测试应覆盖尽实际可能多的功能（包括传感器和驱动器），同时不会影响核动力厂连续正常运行；

（4）定期试验和标定应尽可能在安全系统实际或模拟运行条件（包括操作顺序）下进行；

（5）对于生成安全系统特定信号的变量组合，应试验和标定所使用到的所有变量；

（6）应能够检测冗余设备中的故障。冗余设备可能是不同冗余序列的设备，也可能是同一序列内的冗余设备。

6.6.4.11 如果一次性完成在线试验不可行，可采用几个试验搭接的方式来实现试验目标。若安全系统通道未采用一次性在线试验，应为使用搭接试验的合理性提供书面的论证。通常，要通过合理性论证来证明搭接试验提供了完整的覆盖范围、更长的试验间隔对于设备的可靠性是可接受的、任何未在线试验的部件都会在停堆期间进行试验。

6.7 可维护性

6.7.1 仪控系统的设计应包括所有系统和部件的维护计划。

6.7.2 仪控系统和部件的设计、布置和安装应尽可能减少对操作人员的风险，并便于进行必要的预防性维修、故障排除和及

时维修。为此，设计应考虑：

（1）避免将设备布置在核动力厂正常运行期间预计会出现极端温度或湿度条件的区域；

（2）避免将设备布置在有高辐射风险的区域；

（3）应考虑到人员执行维护活动的能力和局限性；

（4）在设备周围留出足够的空间以确保维护人员能够在正常工作条件下执行任务。

6.7.3 如果部件位于不可达区域，应采用其他策略应对部件失效，包括：

（1）安装备用冗余设备；

（2）远程维护设施；

（3）如果设备发生故障并且无法及时方便的维修或更换，核动力厂降功率运行的预案。

6.7.4 仪控系统维护措施的设计应确保其对核动力厂安全的影响是可接受的。这种措施的典型例子是将系统中的一个序列与其他几个冗余序列断开，或者提供替代的手动操作。

6.8 为试验或维护目的退出运行的规定

6.8.1 安全系统由于试验或维护原因，任一部件或冗余序列退出运行或旁通时，仍应满足单一故障准则，不应导致要求的最小冗余度的丧失，除非可以充分证明系统运行的可靠性仍是可接受的。即使不满足单一故障准则，试验、维护和修理活动也应符合核动力厂的运行限制和条件。

6.8.2 如果试验或维护设施的使用可能影响仪控功能，则应对仪控接口进行硬件联锁，以确保在没有谨慎的人工干预情况下不能与试验或维护系统进行交互。

6.8.3 设计应确保系统不会处于试验或维护模式或配置下而不被察觉。安全系统部件或安全序列的不可操作或旁通应在控制室内指示，对于经常被旁通或经常被置于不可操作的设备，这些指示应是自动的。

6.8.4 核动力厂维修、监督和在役检查相关的核安全导则为试验和维护后系统和设备重新投入运行提供了指导。

6.9 整定值

6.9.1 安全系统仪控整定值的确定通常要考虑以下几个值：

（1）安全限值：对某些运行参数规定的限值，核动力厂在此限值内运行是安全的。

（2）（整定值的）分析限值：为了保证不超过安全限值，通过安全分析确定的一个可测的或导出的变量限值。分析限值与安全限值之间的裕度应考虑：仪表通道的响应时间和所考虑事故的瞬态范围。

（3）触发整定值：为了触发保护动作，用于驱动最终整定值装置动作的预设值。

（4）允许值：定期试验时触发整定值可采用的一个限值，超出此限值需要采取适当的措施。整定值超出其允许值可能意味着该通道未在整定值分析的假设范围内执行功能。在这种情况下，

必须确定是否违反了运行限值和条件，并且需要采取哪些措施恢复通道的可运行性。

（5）安全系统整定值：为防止出现超过安全限值的状态，在发生预计运行事件或设计基准事故时启动有关自动保护装置的触发点。安全系统整定值也可以表示为触发整定值或允许值。

6.9.2 应对定期试验期间测量出的整定值进行评估，以确认其与原定的整定值的偏差与不确定度分析的预期一致。即使没有超过允许值，但过度的偏差可能仍然表征该通道的行为不符合预期，该设备需要维修或分析需要修改。

6.9.3 图 3 说明了这些术语与测量不确定度和误差的类型之间的关系，这些测量不确定度和误差通常是确定触发整定值和允许值的基础。

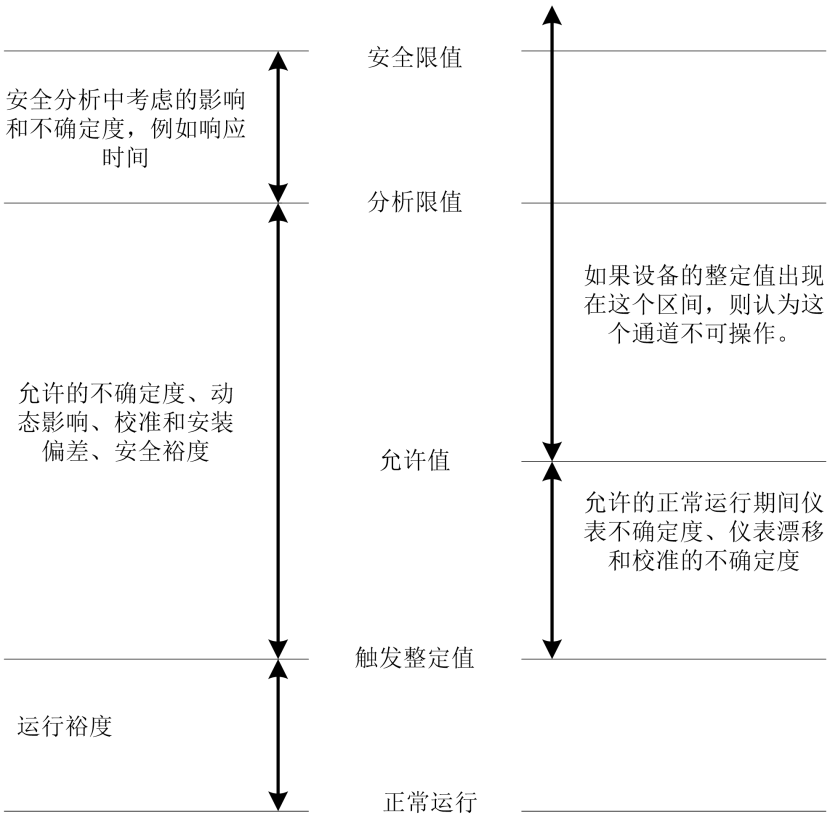

图 3 整定值术语和确定整定值时要考虑的误差

6.9.4 整定值可以是固定值，也可以是随其他核动力厂参数或工况而变的变化量。

6.9.5 用于触发安全动作的触发整定值的选择应确保在被监测变量达到其分析限值之前启动所需的缓解动作。

6.9.6 安全系统整定值的计算方法应有书面说明，证明该方法在触发整定值和分析限值之间提供了足够的裕度，以考虑测量误差、通道误差、不确定度以及这些值随时间的变化。

6.10 安全重要物项的标记和标识

6.10.1 应对所有仪控部件确定一个一致、连贯、且易于理解的命名和标识方法，并用于人机接口的描述性标题，此种命名和标识方法应在核动力厂生命周期的设计、安装和运行的各阶段遵

循。

6.10.2 一个合适的标识方案应不需要人员频繁地查阅图纸、手册或其他材料即可使用或识别。

6.10.3 系统和部件的命名和标识具有一致性且易于理解对于工程设计人员、维护人员和施工人员是非常重要的，也有助于控制、显示和指示的标签设计。

6.10.4 核动力厂中的仪控部件通常应标记其标识信息。安装在设备或组件中的部件或模块不需要再单独标识。通常通过配置管理维护这些部件、模块和计算机软件的标识。

6.10.5 不同安全序列的部件彼此之间应易于区分，并且应易于与安全等级较低的部件区分。

6.10.6 部件的清晰标识可以减少因疏忽大意在不正确的通道上执行维护、测试、修理或标定的可能性。

6.10.7 标识可以采取标签或颜色编码的形式。

7 特定仪表、控制系统和设备的设计

7.1 传感器

7.1.1 核动力厂变量的测量应符合仪控系统和核动力厂设计基准的要求。

7.1.2 核动力厂变量的测量既包括某个量程范围内变化量当前值的测量，也包括通过限位开关、辅助继电器触点及温度、压力、流量或液位开关等对离散状态的检测。

7.1.3 核动力厂变量可以直接测量，也可以间接测量，例如基于多个测量值的计算，或通过测量其他与所需变量有已知关系的数据来确定该变量的值。

7.1.4 在实际可行的前提下，核动力厂工况应尽量通过直接测量来监测，而不是通过间接测量来推断。

7.1.5 每个监测变量的传感器及其量程应根据需要该传感器信息的所有核动力厂状态下该变量监测的准确度要求、响应时间要求、运行环境和变量变化范围来选择。在传感器和驱动器的设计中，应考虑设计裕度。

7.1.6 传感器共因故障的后果应在第 4.5.5-4.5.9 节规定的分析活动中予以考虑。

7.1.7 对于所识别出的传感设备共因故障薄弱点，应采取措施使其不会妨碍操纵员获取为控制事故并减轻其后果所需的信息和参数。

7.1.8 如果需要多个传感器来覆盖被测变量的整个测量范围，则应在两个传感器的过渡点处提供一个合理的重叠量，以确保信号响应曲线中的信号饱和或折叠效应不会妨碍所需功能的执行。

7.1.9 对于某个仪控功能，如果变量测量的空间位置非常重要（即变量的测量值取决于传感器的位置），则应确定传感器的最小数量和位置。

7.2 控制系统

7.2.1 必须设置适当且可靠的控制系统，使得相关的工艺变

量保持在规定的运行范围内。

7.2.2 将主要工艺变量保持在运行限值范围内的自动控制是核动力厂纵深防御的一部分，因此，相关的控制系统通常是安全重要的。

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

7.2.4 应对执行控制功能的输入信号和设备的故障进行监测，根据可能的故障模式，采用适当的缓解手段，例如采用冗余信号，无扰切换到备用设备，或使得驱动器保持原位、发出报警并切换到操纵员手动控制模式。

7.2.5 自动控制系统故障的影响不应导致超出设计基准事故验收准则或为此假设的工况。对于一个具体的系统设计，如果存在某类故障的可能性，如控制系统的多重误动作，则在设计中应加以考虑。采用适当的设计措施，例如分段，可以消除控制系统多重误动作的可能性或将其发生的可能性降低至可接受水平。

7.3 保护系统

7.3.1 必须设置能够探测不安全状态并自动触发安全动作的保护系统，以启动必要的安全系统来实现和维持核动力厂安全状态。

7.3.2 保护系统应监控核动力厂变量并检测其与规定限值的偏差，使得核动力厂参数不超出每个设计基准事故确定的限值范

围。

7.3.3 保护系统可以由多个系统组成。

7.3.4 自动安全动作和手动安全动作

7.3.4.1 应为保护系统的所有安全动作提供自动的触发和控制手段，除非经过论证可以只采用手动动作。

7.3.4.2 通常情况下，保护系统的大部分功能都应自动启动。在下列情况下，才可能会允许仅采用手动动作：

（1）自动序列完成后某些安全任务的启动；

（2）在事故后将核动力厂带入长期安全状态的控制动作；

（3）发生假设始发事件相当长的时间后才需要启动的安全动作。

7.3.4.3 要论证仅采用手动动作是可以接受的，应证明满足下列要求：

（1）安全系统应为操纵员提供清晰且充分的信息，使得他们对于是否需要启动安全动作能够作出合理的判断；

（2）应向操纵员提供关于该安全任务的书面规程和培训；

（3）应为操纵员提供足够的控制手段以执行所需的动作；

（4）执行动作的操纵员之间应有充分的通信手段，以确保这些动作的正确完成；

（5）应进行适当的人因工程分析，以确保对于每个假设始发事件，能够将核动力厂工况维持在验收准则之内；

（6）应允许操纵员有充足的时间评估核动力厂状态并完成

必要的操作。相关的时限分析应考虑每个操纵员动作的可用时间和所需时间。时限分析决定了安全裕度，随着安全裕度减少，应适当考虑上述时间差值估算的不确定性。对于新建核动力厂，应将核动力厂设计成在设计基准事故发生后的30分钟内，不需要操纵员动作便能将核动力厂参数保持在设定的限值范围内。

7.3.4.4 对启动和控制安全功能执行所必需的机械安全系统和单个设备，应提供手动启动手段。机械安全系统是指例如控制棒组，应急给水，应急堆芯冷却或安全壳隔离此类的系统。

7.3.4.5 启动机械安全系统安全功能的手动信号应尽可能在接近最终驱动装置处注入。

7.3.4.6 手动启动安全动作为预计运行事件和事故工况提供了一种纵深防御的形式，并支持事故发生后核动力厂的长期运行。

7.3.5 信息显示

保护系统应向操纵员提供保护系统功能中使用的每个输入参数的测量值，每个序列中每个停堆和驱动功能的状态，以及每个被驱动系统的启动状态。

7.3.6 保护系统的传感器和整定值

7.3.6.1 向保护系统提供信号的传感器，如需同时向其他系统提供信号，必须通过适当的缓冲和隔离装置。

7.3.6.2 在实际可行的前提下，应使用例如功能多样性、冗余和信号多样性等设计技术，以防止保护系统功能丧失。

7.3.6.3 有时可能需要提供多个整定值，以实现对特定运行

模式或一组运行工况的充分保护。

7.3.6.4 如果同一个保护系统功能需要多个整定值（例如，提升或降低功率时使用的定值），设计上应确保在核动力厂工况不再适合使用限制性低的整定值时，会自动使用或通过行政管理手段使用限制性高的整定值。

7.3.6.5 如果设计上提供了可变整定值或在保护系统运行时在线更改整定值的手段，则使得整定值变化或更改整定值的装置应属于保护系统的一部分。

7.3.6.6 保护系统应为其每个通道提供确定整定值的手段。

7.3.7 运行旁通

7.3.7.1 在特定的核动力厂工况下，可能需要运行旁通或停堆条件逻辑来禁止保护系统功能启动。例如，在反应堆启动过程中，需要旁通用于限制反应堆功率的停堆保护，以允许功率提升通过该低功率停堆整定值。

7.3.7.2 如果需要运行旁通，在核动力厂接近进行运行旁通操作的状态时，应向操纵员提供适当的警示或报警。

7.3.7.3 应在控制室提供有关运行旁通状态的指示。

7.3.7.4 如果已激活的运行旁通的条件不再满足时，保护系统应自动完成以下任一动作：

（1）取消已激活的运行旁通；

（2）将核动力厂置于允许运行旁通的工况下；

（3）触发适当的保护动作。

7.3.8 保护系统功能的保持

7.3.8.1 保护系统设计必须防止操纵员在运行状态和事故工况下采取可能损害保护系统有效性的动作，但不得阻碍操纵员在事故工况下采取正确行动。

7.3.8.2 保护系统触发的动作应保持，以便保护动作一旦启动，即使触发条件可能已不再存在，保护动作仍将持续。

7.3.8.3 保护系统触发动作的保持通常在核动力厂设备的驱动信号级实现。不必对单个测量通道进行“保持”。

7.3.8.4 某个保护系统功能一经触发，应完成该功能执行的所有动作。

7.3.8.5 第 7.3.8.4 节的要求并不限制保护系统驱动的安全设备的电气保护装置动作。核动力厂电力系统设计相关的核安全导则就安全重要物项的电气保护给出了指导。

7.3.8.6 保护系统功能复位后，只有再经过一个特定的操纵员动作，被驱动设备才能返回到正常状态。

7.3.8.7 复位安全功能的设施应是安全系统的一部分。

7.3.9 误触发

7.3.9.1 保护系统的设计应尽可能使保护系统误触发或误动作的可能性降至最低。

7.3.9.2 保护系统功能的误触发可能导致：

（1）对设备施加不必要的应力，缩短核动力厂的寿命；

（2）需要其他安全动作；

（3）削弱操纵员对设备的信心，可能导致他们忽视后面的有效信号；

（4）核动力厂失去生产能力。

7.3.9.3 保护系统的误触发不应使得核动力厂处于不安全状态。

7.3.9.4 当保护系统的误触发或误动作导致的核动力厂状态仍需要保护功能时，应通过没有造成该误动作，并且也不受该误动作影响的保护系统其余部分或其他安全系统来触发和执行的安全动作，将核动力厂保持在安全状态。

7.3.10 保护系统与其他系统之间的相互作用

7.3.10.1 必须通过分隔、避免相互连接或采用适当的功能独立来防止核动力厂保护系统和控制系统之间的相互干扰。

7.3.10.2 如果保护系统和控制系统共用信号，必须保证适当的分隔措施，且信号系统必须按照属于保护系统的一部分来分级。

7.3.10.3 当保护系统和控制系统共用的部件或信号出现故障时，保护系统仍应满足可靠性、冗余性和独立性的所有要求。

7.3.10.4 保护系统必须设计成能够超越控制系统的不安全动作。

7.3.10.5 如果某个假设始发事件引起控制系统动作，进而导致需要启动保护系统功能的工况，则同一假设始发事件不应妨碍提供必要保护系统功能的安全系统的正确动作。

7.3.10.6 不应忽视一种可能性，即保护系统故障本身即是一

个假设始发事件，它触发控制系统动作，进而需要启动保护系统功能。

7.3.10.7 避免由于控制系统和保护系统之间相互干扰导致核动力厂不能正常运行的措施，例如：

（1）为保护和控制提供单独的仪表通道；

（2）安全组合中增加额外的设备来应对潜在的干扰；

（3）在核动力厂内提供屏障或替代的布置方案，以限制假设始发事件造成的损害；

（4）以上这些要素的组合，使得安全组合和核动力厂设计足以将核动力厂工况维持在可接受的限度内。

7.3.10.8 第 7.3.10.3 节、第 7.3.10.5 节和第 7.3.10.6 节的要求旨在确保在发生此类故障时保护系统仍能完全满足要求。要满足的可靠性要求包括符合单一故障准则。

7.3.10.9 如果一个设备既可以被保护系统，也可以被其他较低安全等级的系统驱动，则来自保护系统的保护功能触发指令应优先驱动设备。例如，驱动信号可以来自控制系统，用于正常运行，或使运行人员可以从同一人机接口控制所有系统设备的正常运行，前提是保护系统的任何指令优先级高于控制系统的指令。

7.4 动力源

7.4.1 不论其类型（例如电源、气动动力源和液压动力源）如何，仪控系统动力源的安全等级、可靠性规定、鉴定、隔离、可试验性、可维护性和退出运行时指示的要求应与他们所服务的

仪控系统的可靠性要求相一致。

7.4.2 要求在正常运行状态和设计基准事故工况下始终可用的仪控系统，应连接到不间断电源，以便在仪控系统设计基准规定的允许范围内为其供电。

7.4.3 如果运行环境需要，仪控系统可以通过手动操作或通过自动切换操作从正常电源切换到备用电源，前提是仪控系统功能可以承受相应的电源中断。通常，切换系统应视为供电系统的一部分，并与其所供电的仪控系统具有相同的安全等级。

7.4.4 一些仪控系统可以直接由直流电源供电。

7.4.5 电源可以为电磁干扰提供传输路径，这些电磁干扰可能源自仪控系统之外，或由直接或间接连接到同一电源的其他仪控系统引起（见第 6.3.4.19 节）。

7.4.6 核动力厂电力系统设计相关的核安全导则提供了关于电力供应和相关配电系统的指导。

7.5 数字化系统

7.5.1 数字化系统包括基于计算机的系统和使用硬件描述语言的可编程系统等。

7.5.2 当安全重要系统设计成依赖于基于计算机的设备时，必须确定或制定用于开发和测试/验证计算机软、硬件的适当的标准和规范，并在整个寿期内执行，特别是在软件开发过程中应执行这些标准和规范。整个开发过程必须遵循质量保证大纲。

7.5.3 数字化系统功能

7.5.3.1 仪控功能采用数字化系统的优势在于实现复杂功能的灵活性、核动力厂监测的改进、人机接口的改进，自测试和自诊断的能力、便于运行经验反馈的强大的数据记录能力、更低的物理空间和布线需求。数字化系统具有试验和自检功能，可提高系统可靠性。

7.5.3.2 数字化系统中仪控功能的实现方式与模拟系统不同。在数字化技术中，多个功能被组合在一个或多个处理单元中。处理单元中多个功能的组合可能导致非常难以分析的情况，并且一个处理单元的故障会导致多个功能同时失效。一个功能还可能会通过非预期的相互影响降低另一个功能的性能（没有任何可识别的“故障”）。

7.5.3.3 如果设计不合理，对如此复杂部件的全面验证和确认可能非常困难，甚至几乎不可能。可能存在未识别的错误，并且这些错误可能会被复制到所有冗余部件中，或传播到基于同一平台的其他系统，因为软件模块、可编程器件或库可能是共用的。

7.5.3.4 在数字化系统中，输入是在离散的时间点采样的。信号周期性地在系统部件之间传输，并且周期性地产生输出。因此，如果设计不合理，数字化系统的处理负荷或通信负荷的变化可能会影响传输速度和响应时间。核动力厂参数的变化、在不同的系统状态或核动力厂状态下运行或设备故障都可能引起处理负荷或通信负荷的变化。

7.5.3.5 数字化仪控系统的设计应确保系统在所有规定的运

行工况和所有可能的数据负荷条件下，按照要求的响应时间和准确度执行其安全功能。

7.5.3.6 安全仪控系统应设计为具有确定性行为，对该物项规格书范围内的任一给定输入序列总是会产生相同的输出和相同的响应时间，即激励与响应之间的时间延迟具有确定的最大值和最小值。

7.5.3.7 确保确定性响应时间的方法包括：

（1）避免过程相关的中断，以免核动力厂工况直接影响仪控系统需处理的中断率；

（2）在设计时静态分配资源；

（3）按预先规定对循环迭代进行限制。

7.5.3.8 数字化系统的响应时间和准确度取决于采样速率和处理周期时间。若系统设计不合理，这些参数也可能取决于处理器的速度，这种情况应避免。

7.5.3.9 数字化系统的设计和分析应做到，单个部件（例如计算机处理器）故障导致的系统行为在一个预期的可接受范围之内。

7.5.3.10 数字化系统失电或重新启动不应导致配置数据或软件修改。

7.5.4 数字化数据通信

7.5.4.1 安全系统的数据通信应设计成具有确定性的传输时间。

7.5.4.2 确保确定性传输时间的方法包括：

（1）预定的基于时间的行为，即数据通信系统的行为不是由其客户端节点确定的，而是基于时间调度，由设计预先确定的；

（2）预定的数据通信负荷，即在任何给定时间要传输信息的大小是由设计预先确定的，使得通信负荷总是与数据通信系统的传输能力相匹配的；

（3）预定的数据通信模式，即在任何给定时间点所传输信息的发送者和接收者是由设计预先确定的。

7.5.4.3 数字化数据通信应符合第 6.2.4.1-6.2.4.9 节的要求。

7.5.4.4 通过数字化数据通信发送和接收的每条信息应经自动检查，例如识别出错误应自动加以标记。错误可能包括数据损坏、无效数据（非计划信息）或不可靠信息（来自非预期来源）。

7.5.4.5 如果通信系统对数据加密或使用专有协议，这些措施不应妨碍对错误的检测。

7.5.4.6 在数据通信中检测到错误时要采取的行动应预先规定。可能采取的行动包括自动丢弃无效或不可靠的数据、纠正损坏的数据（如可能）、或丢弃损坏的数据。

7.5.4.7 设计应确保数据传输故障和数据通信设备的故障能够被检测，向操纵员提供适当的报警，并形成记录用于性能分析。

7.5.4.8 数字化数据通信中存在的某些类型的错误本身并不构成系统中的一个故障，因为这些错误是设计中预先考虑到的，并且通信协议被设计为能够处理这些特定类型的错误和一定范

围内的错误发生率。因此，应用第 7.5.4.7 节指导原则时要对哪些错误算作数据传输故障做出规定。例如，可以规定两次成功传输之间的最大允许时间间隔或最大错误发生率等判定准则。

7.5.4.9 错误检测和纠正特性可以提高信号传输的可靠性。采用的检测通信故障和处理错误的方法应适合数据的应用，适合使用数据的功能的需求频率，并与引入的复杂性相平衡。

7.5.4.10 安全系统中的通信特性

7.5.4.10.1 如果安全相关数据的通信出现任何故障，则安全系统应继续执行其安全功能或进入安全状态。通常，这需要使用两个处理器来实现，两个处理器通过受控访问共享内存进行数据共享，一个处理器专用于执行安全功能，另一个专用于数据通信任务。将计算和逻辑功能与通信和中断功能隔离，防止后一功能中的错误影响安全计算或逻辑功能的确定性行为和时序。这种隔离，有时称为缓冲，旨在防止本序列以外的通信故障和失效传播到实现安全功能的处理器。

7.5.4.10.2 安全系统接收方只处理预先规定的报文。

7.5.4.10.3 预先规定的报文要素包括报文协议，报文格式和一组有效报文。

7.5.5 数据通信的独立性

7.5.5.1 避免共因故障

数据通信网络拓扑结构和介质访问控制的设计和实现应避免导致安全系统的共因故障。

7.5.5.2 安全序列之间的通信

7.5.5.2.1 一个安全序列的通信，包括通信错误或故障，不应妨碍与之相连的安全序列执行其安全功能。

7.5.5.2.2 为防止各序列之间的故障传播，通常采用数据验证（见第 7.5.4.4-7.5.4.10 节）和数据缓冲两种方式的组合。

7.5.5.2.3 不应使用基于中央集线器或路由器，使多个安全序列的通信通过一个链路传输的架构。

7.5.5.3 不同安全分级系统之间的通信

不同安全分级的数字化系统和设备之间的数据通信应符合第 6.2.4.1-6.2.4.9 节的要求。启动保护系统功能的指令应优先驱动设备。

7.5.6 网络安全

7.5.6.1 网络安全相关要求和策略应遵守国家相关法规，应对仪控系统和设备进行网络安全等级划分，针对不同网络安全等级采取相应程度的防护措施。此外，还应满足第 7.5.6.2-7.5.6.5 节提出的具体技术要求。

7.5.6.2 核安全和网络安全之间的关系

7.5.6.2.1 任何网络安全措施的运行和故障都不应对系统执行其安全功能的能力产生不利影响。如果核安全与网络安全之间存在冲突，那么在寻求网络安全风险解决方案过程中，设计考虑应确保核安全。不应简单地接受网络安全解决方案的缺失，这种情况只能作为个案处理，并且必须经过全面的合理性论证和网络

安全风险分析。

7.5.6.2.2 网络安全措施的故障模式以及这些故障模式对仪控功能的影响应在系统危害分析中得以了解、记录和考虑。

7.5.6.2.3 如果在人机接口中采取网络安全措施，不应对操纵员维持核动力厂安全的能力产生不利影响。

7.5.6.2.4 如果网络安全措施不能同时为仪控系统带来核安全功能方面的好处，则应尽量在仪控系统之外的单独设备中实施。

7.5.6.2.5 在仪控系统中增加网络安全功能增加了系统的复杂性，并可能会向系统引入潜在的故障模式，这可能会影响其执行安全功能的可靠性，或增加误动作的可能性。

7.5.6.2.6 在仪控系统中实施的网络安全措施应根据本导则第 2 章中的要求进行开发，并应按照与所在系统相同的鉴定等级进行鉴定。

7.5.6.2.7 数字化系统或部件的开发过程、运行和维护应根据网络安全大纲进行，该大纲规定并详细说明实现网络安全的手段。

7.5.6.2.8 网络安全大纲应包括在开发仪控系统期间实施的适当的物理、逻辑和行政管理控制。

7.5.6.2.9 数字化系统的开发环境以及后续数字化系统的安装、运行和维护应有配套的措施，以防止软件或数据被蓄意或无意入侵或破坏、引入恶意代码、与外部网络错误连接和遭受黑客攻击。

7.5.6.3 对安全重要数字化系统的访问控制

7.5.6.3.1 系统和部件的所有数据连接都应置于盘柜内，应按照第 6.5.1 节的指导对接近盘柜和进入盘柜内部进行控制。

7.5.6.3.2 数据连接包括网络连接、外部存储器连接以及访问便携式介质（例如记忆棒、闪存卡和数据磁盘）。

7.5.6.3.3 未使用的数据连接应禁用。临时使用的连接，例如与维护计算机的连接，应在不使用时禁用。禁用未使用连接的形式包括移除、物理措施或逻辑措施。

7.5.6.3.4 如果使用逻辑措施作为禁用数据连接的方法，则应提供附加措施以确保连接保持禁用状态，或者连接配置或状态的任何变化都将被检测并评估其对系统运行的影响。

7.5.6.3.5 对于允许更改软件或配置数据的访问功能，以及更改本身应被监视和记录。监视和记录可以自动或根据行政管理程序手动执行。应对所使用的方法进行论证，说明其提供了必要的网络安全性，且不会影响安全功能的执行。

7.5.6.3.6 第 7.5.6.3.5 节的要求不适用于专门设计的，由控制室操纵员进行的配置数据更改。

7.5.6.4 与应急设施通信的安全

7.5.6.4.1 核动力厂仪控系统的数据可以传输到核动力厂厂址的其他地点（例如技术支持中心）和厂址以外的地点（例如地方应急组织）支持应急响应，前提是这些连接不会对仪控系统造成不利影响。

7.5.6.4.2 核动力厂与技术支持中心之间以及核动力厂与应

急响应机构之间的通信连接，包括用于人员通信的连接，应是专用的，并且应防止被篡改。

7.5.6.4.3 数据通信包括有关基本安全功能状态的信息以及支持应急管理的其他信息。

7.5.6.5 运行期间的安全措施

7.5.6.5.1 应综合考虑被动和主动网络安全措施。应优先采用被动网络安全措施。在此基础上，考虑使用主动网络安全措施来探测网络安全威胁并减轻其影响。

7.5.6.5.2 主动网络安全措施不应对安全重要功能产生不利影响。如主动网络安全措施可能会增加系统的复杂性，占用系统资源，增加误动作的可能性或引入新的故障模式。尽量只在系统离线时应用主动安全措施。仪控系统最好离线执行扫描功能。

7.5.6.5.3 对于计算机系统应有定期验证和维护后验证的规定，以确保网络安全措施的正确配置和正确运行。

7.5.6.5.4 应建立程序用于规定对网络安全监控所获结果的审查和响应。

7.5.7 硬件描述语言可编程器件

7.5.7.1 硬件描述语言可编程器件是指提供逻辑结构（例如门和开关阵列）、可由仪控开发者定制以实现特定功能的可编程电子模块，例如现场可编程门阵列。这种定制需要采用专门的软件工具，以对实现这些功能的需求进行形式化的描述。

7.5.7.2 与硬件描述语言可编程器件有关的要求应与第 2 章

关于生命周期的要求，第 7.5 节关于数字化系统的要求，以及第 9 章中关于软件的要求一起使用。它适用于直接执行安全功能的器件。

7.5.7.3 使用硬件描述语言可编程器件进行应用开发应遵循满足第 2 章要求的预先定义的生命周期。

7.5.7.4 开发计划中应要求以第三方可以理解的方式对每个技术决策进行论证。

7.5.7.5 硬件描述语言可编程器件的实现计划应规定确保每个生产出的部件符合设计的方法。

7.5.7.6 硬件描述语言可编程器件的设计要求应包括时序要求，例如门延迟和建立时间的要求。

7.5.7.7 硬件描述语言可编程器件和相关物项（例如最终产品和硬件描述语言中包含的库和知识产权核）的选择应遵循预先定义的、文档化的流程，以确保其适用性。

7.5.7.8 仅当下列条件满足时，才应使用知识产权核：

（1）应从合格供应商处获得所使用的知识产权核，其知识产权核遵循了高质量的开发过程，包括严格的工程设计过程，形成了明确且有用的文档，并且易于集成。

（2）应进行评估以确保没有引入危害。

7.5.7.9 如果需要对已开发物项进行修改才能予以接受，则应在开展接受审查之前完成对修改的说明、设计、实现和验证。

7.5.7.10 如果所选择的硬件描述语言可编程器件还包含其

他辅助功能（例如内置的自检功能），则应通过对各种要素进行评估来确定此类设备执行安全功能的适用性，包括对其开发过程（也包括验证过程）及设计的评估。

7.5.7.11 对硬件描述语言可编程器件，应选择有合格的、兼容性好的软件工具支持的标准化硬件描述语言来进行编程。

7.5.7.12 硬件描述语言可编程器件的设计：

（1）应确保器件的行为是确定性的。例如，通过使用内部同步设计可以实现确定性设计。同步设计有利于正确性（避免亚稳态问题）和可测试性，并且可以充分利用软件工具进行设计和验证。

（2）器件结构应具有明确的实现特性和行为特性。可采用的方法包括对设备的形式化描述，使用严格的语义和语法规则，使用硬件描述语言的“安全”子集，以及使用预定义的语言和编码规则。

（3）在合理可行的程度上，尽可能支持基于数学定理证明的验证技术的使用。

（4）应明确地处理器件所有可能的逻辑情况和所有运行模式，例如复位、开机和正常运行。

（5）电源电压、温度和微电子工艺在设计边界范围内的变化所引起的所有可能的时序情况都应是正确的。

（6）应确保在器件中实现的每个功能均可测试。

7.5.7.13 应使用布线后分析来证明设备的设计和实现与供

应商预定技术规则以及用于实现的软件工具的符合性。

7.5.7.14 硬件描述语言可编程器件的设计过程应集成到仪控系统的整体开发过程中。

7.5.7.15 验证和确认：

（1）应确认没有未规定的，且会影响硬件描述语言可编程器件正常工作的功能；

（2）应达到预期的测试覆盖率。应对测试覆盖率进行分析并文档化，保证对于确认需求规格书和设计实现的特征是足够的，同时测试工具能够提供足够的可观测性确定每个被测试覆盖的单元是否通过；

（3）应注意对基于硬件描述语言可编程器件的系统所特有方面的验证和确认；

（4）应包括时序分析和仿真。

7.5.7.16 应使用环境鉴定和分析来证明，已开发物项或辅助特性不会降低安全重要系统执行其安全功能的能力。

7.6 软件工具

7.6.1 如果有可用的工具并且能够从中获益，应使用软件工具来支持仪控生命周期的各个方面。

7.6.2 使用适当的软件工具可以降低在仪控开发期间引入故障的风险，并且可以提高在检查、验证和确认过程中发现故障的可能性。因此，使用软件工具可以提高仪控开发过程的完整性，从而提高设备的可靠性。使用软件工具也可以带来经济效益，因

为它们可以减少制造或开发系统、设备和软件所需的时间和人力。软件工具可用于自动检查是否遵守构建规则和标准，以标准格式生成正确的记录和一致性文档，并支持变更控制。软件工具还可以减少测试所需的工作量，并且可以维护自动化的日志。一些特定的开发方法需要使用软件工具。用于开发仪控系统的软件工具包括：

（1）提供开发基础和开发支持系统的软件工具，例如需求管理系统或集成开发环境；

（2）电路和布线自动规划软件；

（3）转换软件工具，例如代码生成器、编译器、逻辑综合器以及可将文本或图表从一个抽象层次转换为另一个通常更低的抽象层次的工具；

（4）电子设计自动化软件工具；

（5）用于验证和确认的软件工具，例如静态代码分析器，自动电路测试器，测试覆盖率监视器，定理证明辅助软件，电子电路模拟器和核动力厂系统模拟机；

（6）用于准备系统组态数据的软件工具；

（7）用于配置管理和控制的软件工具；

（8）用于检测已知和未知漏洞的网络安全测试软件工具。

7.6.3 要实现完整一体的项目支持环境，一个关键要素是确保适当的控制和一致性。如果没有可用的软件工具，可考虑开发新的软件工具。

7.6.4 应对使用软件工具的好处和风险，以及不使用软件工具的好处和风险进行权衡。

7.6.5 应选择软件工具来限制出错和引入故障的机会，同时最大限度地提供避免或检测故障的机会。软件工具的使用也可能对系统开发造成不利影响。例如，设计软件工具可能会通过生成有缺陷的输出来引入故障，验证工具可能无法揭示某些故障或故障类型。

7.6.6 选择的软件工具应在整个系统使用寿期内保持可用状态，并且应与系统开发期间使用的其他软件工具兼容。

7.6.7 应确定和记录所有软件工具的功能和适用范围。

7.6.8 如果没有事先论证，软件工具及其输出不应在其声明的功能或应用范围之外使用。

7.6.9 软件工具不能完全取代人的判断。在某些情况下，通过软件工具提供支持比完全的自动化过程更为合适。

7.6.10 应根据对软件工具的可靠性要求、软件工具的类型、软件工具引入故障或无法使用户发现已有故障的可能性，以及软件工具对系统冗余部分或多样化系统的影响程度，对软件工具进行验证和评估。下面列举了影响验证和评估必要性程度的几种情况：

（1）与被证明不具备引入故障能力的软件工具相比，应对具有这种能力的软件进行更严格的验证。

（2）与能够使用户发现故障的软件工具相比，应对无法使

用户发现已有故障的软件工具进行更严格的验证。

（3）如果软件工具的输出经过系统和独立的验证，则软件工具无须验证。

（4）如果已经采取了措施缓解任何潜在软件工具故障所产生的后果（例如通过过程多样性或系统设计），那么对软件工具的验证的严格程度可以降低。

7.6.11 软件工具的验证和评估应考虑到以前使用的经验，包括开发人员的经验和使用软件工具的过程中获得的经验。

7.6.12 软件工具的选择、验证和评估应经过论证并形成文档。

7.6.13 所有的软件工具应置于适当的配置管理之下。

7.6.14 在对基线设备、软件和基于硬件描述语言的器件进行开发、验证或确认期间所使用的软件工具，其设置应在开发记录中形成文档。这样的文档不仅有助于确保最终软件的一致性，它还有助于对故障源头进行评估，这些故障可能出现在源代码、软件工具或软件工具设置中。在评估由于软件工具导致的潜在共因故障时，相关工具设置的信息可能是至关重要的。

7.7 对安全应用中使用的限定功能工业数字化装置的鉴定

7.7.1 用于核动力厂安全重要系统的限定功能工业数字化装置的鉴定应满足第6.3.1.1-6.3.4.21节基本要求，以及第7.7.2-7.7.8节要求。

7.7.2 限定功能的工业数字化装置具有以下特征：

（1）包含已开发软件或编程逻辑；

（2）该装置是自治的，只执行一个简单的基本功能，该基本功能由制造商规定，不能由用户修改；

（3）不可重新编程；

（4）如果是可重新配置的，则仅限于可以配置与被监视或被控制过程的匹配性相关的参数，或与所连接设备的接口。

7.7.3 所有其他装置都不是“限定功能的工业数字化装置”，它们具有下列一项或多项特征：

（1）使用商用计算机（例如个人计算机、工业计算机或可编程逻辑控制器）；

（2）为仪控平台开发的；

（3）专门为核行业开发的。

7.7.4 确认限定功能的工业数字化装置对于其预期功能的适用性和正确性，应提供如下证据：

（1）装置的主要功能符合应用的功能需求。

（2）主要功能之外的其他功能的运行或故障都不会导致主要功能的不安全运行。主要功能之外的其他功能包括用于维护或配置该装置的功能以及预期应用不需要的功能等。

（3）该装置不存在此类系统故障，即这种故障可能会导致安装在仪控系统冗余或多样化部分的相似装置几乎同时发生共因失效。

（4）有系统性的开发过程，并遵循本导则第 2 章的一般原则。

（5）制造的质量保证是充分的，足以为后续制造的相同或相似型号的设备的接受提供基础。

7.7.5 在其他行业安全认证过程中的信息可以作为支持该装置鉴定的证据。但是仅凭认证证书是不够的，认证过程中产生的信息可能更有价值。

7.7.6 如果第 7.7.4 节的一项或多项要求未得到满足，应提供补充证据。补充证据应直接针对适用性和正确性证据上的薄弱点，应直接针对需要被证实的要求，并且应可证明适用于相关的装置。提供补充证据的技术方法，例如：

（1）为确认装置适用于预期应用的针对性的补充工作，以及其他正确性证据；

（2）适用且可信的运行经验的评估；

（3）设计输出的验证；

（4）统计测试。

7.7.7 用户可以对装置进行配置以使其适用于预期的应用。此类修改应符合本导则中关于设计正确性和文档化的准则，并且不应违背鉴定中采信的以往运行经验或测试。

7.7.8 应确定该装置在预期应用中安全使用所需遵守的限制条件。这些限制包括：

（1）已鉴定装置的应用限制；

（2）启用或禁用的特定选项和未使用的功能的限制；

（3）运行环境和运行寿命的限制；

（4）在运行、测试和维护期间要遵守的措施等。

8 人机接口所需考虑的因素

8.1 控制室

8.1.1 主控制室

8.1.1.1 必须设置主控制室，以进行下述活动：在各种运行状态下以自动或手动方式安全地运行核动力厂；出现预计运行事件和事故工况后，采取相应措施，以使核动力厂保持在安全状态或回到安全状态。

8.1.1.2 仪控系统应使操纵员可以在主控制室内完成控制核动力厂运行和维持核动力厂安全所需的各项功能的启动和手动操作。

8.1.1.3 主控制室应为所有核动力厂安全重要功能的监视提供充分的显示信息，包括核动力厂的运行状态、安全状态和关键参数趋势。

8.1.1.4 应为应急运行规程和严重事故管理指南的执行提供安全重要级别的显示和控制。

8.1.1.5 第 8.1.1.4 节的要求并不排除使用其他适用的手段实现应急操作规程和严重事故管理指南的目标。

8.1.1.6 用于控制核动力厂和维持核动力厂安全的系统或部分系统失效或退出运行时，相关状态应在主控制室和需要通知操纵员的其他地方予以显示。

8.1.1.7 应将安全系统的状态变化告知操纵员，其状态应在操纵员需要的地方显示。

8.1.1.8 重要的系统状态变化应触发报警，包括偏离正常运行限值，安全系统可用性丧失，或由于故障、维护或测试使得原处于待命状态的设备不可用等。先进的报警系统可以实现进一步的功能，例如报警处理、报警优先级、报警控制和管理等功能，有助于操纵员有效监视核动力厂事件并作出及时响应。

8.1.1.9 必须采取适当的措施（包括在核动力厂主控制室和外部环境之间设置屏障），并向主控制室人员提供足够的信息，以在较长时间内保护主控制室人员免于受到事故工况下形成的高辐照水平、放射性物质的释放、火灾、易爆或有毒气体的危害。

8.1.1.10 必须特别关注对可能危及主控制室连续运行的（主控制室）内、外部事件的识别。设计中必须采取合理可行的措施，将这些事件的后果减至最小。

8.1.1.11 主控制室设计必须提供恰当的裕度，以应对比设计中考虑的自然灾害水平（由厂址危险性评价确定的）更为严重的自然灾害。设计应保证设计基准规定的内外部事件不会使得主控制室和辅助控制室同时不可用或同时失效。

8.1.2 辅助控制室

8.1.2.1 必须在核动力厂内与主控制室实体分隔、电气隔离和功能隔离的一个独立地点设置辅助控制室，并配置仪表和控制设备。辅助控制室应能在主控制室丧失执行重要安全功能时完成下

述任务：使反应堆进入并保持在停堆状态，排出余热以及监测核动力厂的重要参数。

8.1.2.2 核动力厂可设计多个辅助控制室，或在辅助控制室外设置辅助控制点。

8.1.2.3 为支持操纵员对导致主控制室撤离的工况所引发的事件作出正确响应，辅助控制室应配有必要的用于核动力厂状态监视的信息显示。

8.1.2.4 辅助控制室应提供控制、指示、报警和显示，足以支持操纵员将核动力厂带入安全状态、确认核动力厂达到并维持在安全状态，以及监视核动力厂状态和关键参数的趋势。

8.1.2.5 如辅助控制室内无法提供第 8.1.2.4 节中的所有控制，可以在就地控制点提供相关控制。

8.1.2.6 应在主控制室外提供适当措施，以便从主控制室撤离后，可以将控制权限转移至新的控制点。

8.1.2.7 第 8.1.1.9 节相关要求，如果适当也可用于核动力厂辅助控制室。

8.2 事故监测

8.2.1 应在核动力厂适当位置（例如主控制室和辅助控制室）显示与运行人员角色和职责相匹配的事故工况信息。

8.2.2 用于事故工况监测的信息显示一般称为“事故监测系统”或“事故后监测系统”。这些显示可以是其他系统的一部分或是单个仪表通道的组合。

8.2.3 事故监测系统应提供事故工况下核动力厂操纵员所需的变量值，使其可以：

（1）通过预先计划的手动动作将核动力厂带入安全状态；

（2）确认基本的安全功能是否已经完成；

（3）确认防止裂变产物释放的屏障（例如燃料包壳、反应堆冷却剂压力边界和安全壳）是否可能发生破损或者已经破损；

（4）确认用于缓解设计基准事故和设计扩展工况后果，并将核动力厂带入安全状态的系统的状态和性能；

（5）确定是否需要启动保护公众免受放射性物质释放影响的行动；

（6）实施核动力厂严重事故管理指南。

8.2.4 事故监测系统应根据第 5 章的指导原则进行功能分类和设备分级，并遵守第 6 章中相应的通用设计要求。

8.2.5 用于执行第 8.2.3 节显示功能的相关仪控设备应能在对应的设计基准事故和（或）设计扩展工况下执行功能，严重事故监测仪表的设计和鉴定应考虑预期运行环境的整个变化范围。

8.2.6 对于严重事故监测仪表，根据其将承受的最恶劣的可信工况进行型式试验并不总是可行的。这时可以采用其他方法作为试验的补充，包括但不限于第 6.3.1.5 节中的方法。

8.2.7 支持严重事故管理指南的事故监测功能：

（1）不能由于严重事故监测仪表通道外其他仪控设备的运行、故障或误操作而失效；

（2）或者不依赖外部电源，或者具备通过核动力厂电源系统之外的其他电源供电的能力。

8.2.8 若执行第 8.2.3 节中（1）-（3）和（6）项功能仪表的单个显示通道失效会导致显示上的分歧时，应为操纵员提供消除这种分歧的手段。单个显示通道的失效可能会导致一对冗余显示存在分歧，解决这种分歧的手段包括提供额外的通道或提供程序将有分歧的仪表读数与和它有已知关系的其他变量读数进行对比。

8.2.9 用于事故监测的仪表应覆盖事故工况下参数值可能达到的整个量程范围。

8.2.10 事故监测变量的显示应清晰可读。

8.2.11 应提供电子化的操纵员辅助功能（例如安全参数显示系统）以帮助操纵员快速确定核动力厂状态、确认事故监测通道运行、确认它们的读数以及从直接测量确定间接测量变量的值。

8.2.12 计算机化的指导可以提高安全性和采取正确动作的确定性。

8.2.13 在新的控制室设计中，安全参数显示系统和事故监测系统的功能经常集成到用于正常运行的操纵员人机接口系统中。对于操纵员的辅助或指导功能可以仅用于特定的工况或事故情境，也可以用于所有的工况，包括启堆和正常功率运行。

8.3 运行人员通信系统

8.3.1 应为运行人员提供与厂内外可靠联系的通信系统，并

且不必离开需要监控的仪控系统。

8.3.2 用于运行人员之间以及与厂外应急设施通信的系统不应因任何个人防护设备、假设始发事件或单一的恶意行为而失效。

8.3.3 仪控设备的特性不应妨碍运行人员之间进行通信。

8.3.4 如果仪控设备干扰了无线电通信、或无线电通信干扰了仪控设备、或人员防护设备妨碍了电话的使用，则需要使用其他通信形式。

8.3.5 主控制室、辅助控制室和技术支持中心应与以下地点具有至少两种多样化的通信手段：

（1）在预计运行事件或事故工况下需要通信的场所；

（2）应急响应设施（例如技术支持中心）和应急响应机构；

（3）相关设施，包括受当前机组运行影响的其他设施，例如同一厂址的其他机组。

8.3.6 多样化的通信手段包括：邮件、数据传输、传真、视频连接、固定电话、卫星和移动电话以及便携式无线电。

8.3.7 第 8.3.5 节和第 8.3.6 节中定义的多样化通信连接：

（1） 应设计为不受相同的故障、内部危险、外部危险或假设始发事件的影响。

（2）应不依赖于厂内电源系统和厂外电源系统运行。

8.3.8 应设置使得厂区和厂内所有人员均能听到通知的通信系统。

8.4 仪控系统人因工程相关的总体原则

8.4.1 必须在核动力厂设计过程初期就系统地考虑人因（包括人机接口），并贯彻于设计全过程。

8.4.2 应尽实际可能地促使有类似核动力厂运行经验的运行人员积极参与设计过程，以保证在设计过程中尽早考虑未来的运行和设备维护的需求。

8.4.3 人机接口的设计必须能按照决策所需时间和行动所需时间给操纵员提供全面且易于管理的信息。向操纵员提供的用于决策和行动所需的信息必须简洁明了且无歧义。

8.4.4 人机接口设计应保持参考设计的正面特性并应避免其已经导致不良运行经验的问题。

8.4.5 用于安全系统监督控制的人机接口设计应采用纵深防御原则。

8.4.6 仪控系统应为操纵员提供发现系统状态变化、工况诊断、系统操作（在必要时）及核实手动和自动动作所需要的信息。

8.4.7 设计上应考虑操纵员的认知处理能力和过程相关的时间限制。

8.4.8 设计应保证从执行一项控制操作到控制系统确认收到控制输入所需的最长时间对操纵员是可以接受的。

8.4.9 仪控系统设计应保证操纵员任务可以在系统需求所规定的时间内完成。

8.4.10 信息流传输速率和控制执行的过快或过慢都会降低操纵员效能。

8.4.11 仪控系统应尽量设计成可以防止和发现操纵员的错误，例如在错误的情境或不适宜的核动力厂配置下采取的动作。这包括对控制系统、监视系统和保护系统的整定值修改的确认。

8.4.12 仪控系统应提供简单易懂的操纵员错误提示，并提供简单有效的恢复手段。

8.4.13 操纵员的单一错误不应导致反应堆失控。

8.4.14 人机接口应设计为：

（1）尽可能适用于与系统交互的多种类型运行人员的不同角色和职责；

（2）首先要考虑负责设备安全运行的操纵员的角色需求；

（3）支持一部分控制室成员获得共同的状况认知，例如利用墙装全厂状态显示器；

（4）提供有效的核动力厂状态总览；

（5）尽量使用符合功能和任务需求的最简化设计；

（6）对操纵员培训的依赖降至最低；

（7）提供的信息能够被操纵员快速识别和理解，以降低操纵员认知的工作负荷；

（8）在模拟和视频显示失效时不会对控制动作产生重大干扰；

（9）考虑人员生理特性、人员运动控制特性和人体测量学特性。人的生理学特性包括视觉、听觉感知和生物力学（触及和运动）等。

8.4.15 人机接口、规程、培训系统和培训应彼此之间保持一致。

8.4.16 信息显示的集成应协调布局，从而有利于操纵员对核动力厂状态的理解，优化核动力厂控制所必需的活动。

8.4.17 人机接口的操作和外观应在不同监控点和平台之间保持一致并高度标准化。

8.4.18 所有描述性标识和标签应考虑使用同一种语言和协调一致的字体。

8.4.19 仪控系统的所有特性（包括控制和显示布置）应与操纵员心智模型相一致并符合传统习惯。心智模型包含了操纵员对于系统行为的理解和预期，通过培训、规程的使用和经验获得。

8.4.20 设计时应确定各类控制和显示类型的风格，并且在控制和核动力厂状态显示的标识、布局和布置上遵循。

8.4.21 人员和自动动作交互的考虑

8.4.21.1 应使用系统化的、一致的方法，确定人和仪控系统之间适当的功能分配。

8.4.21.2 影响人机之间功能分配的因素包括：

（1）所有运行模式下潜在的人员负荷；

（2）准确度和重复性的需求；

（3）时间因素；

（4）决策和所需动作逻辑的类型和复杂程度；

（5）环境因素；

（6）人体生理学和人体测量学。

8.4.21.3 必须把对操纵员在短时间内进行干预的需求降至最低，并必须证明操纵员有足够的时间作出决策和采取行动。

8.4.21.4 如果操纵员无法可靠并及时地完成手动动作，或依靠手动控制将导致操纵员负荷过重，仪控系统应提供自动动作。

8.4.21.5 仪控系统应为操纵员提供监视所有自动功能所需的信息。

8.4.21.6 仪控系统应为操纵员提供多种手段来确认自动动作。

8.4.21.7 用于自动功能监视的信息显示的速率和详细程度（例如用于确定目标或验证）应使得操纵员能够有效实施监视。

8.4.21.8 仪控系统应允许操纵员手动启动或控制用于控制核动力厂和维持安全所需的每个功能。

8.4.22 仪控系统中任务设计所需考虑的因素

8.4.22.1 操纵员的职能应由有明确目标和意义的任务组成，使操纵员保持对核动力厂的熟悉并维持合理的工作负荷，从而既不会影响操纵员效能，又能使其保持充分的警惕性。

8.4.22.2 仪控系统应包含任务分析确定的所有必要的特性。

8.4.22.3 任务分析应考虑所有核动力厂状态、运行模式和运行人员，例如反应堆操纵员、汽轮机操纵员、机组长、现场操纵员、安全工程师和运维人员。任务分析应为仪控系统提供设计输入信息，例如显示信息的准确度和精度要求、系统响应时间、物

理布局、控制显示和报警类型以及软控制与信息显示的集成。

8.4.22.4 人机接口显示单元上的控制和显示信息应按照最便于任务执行的方式进行配置，从而有利于提高任务效能。

8.4.22.5 人机接口的各个方面（格式、术语、排序、分组和操纵员决策支持辅助）均应体现出基于任务需求或其他合理依据的清楚的逻辑性。

8.4.22.6 所有显示、控制和数据处理与相关功能和任务的关系应清晰明确。

8.4.22.7 人机接口为操纵员提供信息的格式和形式应符合任务分析结果。

8.4.22.8 仪控系统为操纵员提供的控制选择应覆盖任务分析所确定的各种可能的操纵员动作。

8.4.22.9 仪控系统应为操纵员提供执行动作的多种手段。

8.4.22.10 仪控系统应允许操纵员执行最少的动作就可以完成任务。

8.4.23 可达性和工作环境所需考虑的因素

8.4.23.1 运行人员的工作场所和工作环境的设计必须符合工效学概念。

8.4.23.2 对于预计运行人员执行核动力厂系统监控所处的区域，应采取必要措施确保合适的工作环境并使其免受危害影响。工作环境通常要考虑照明、温度、湿度、噪声、振动等，当需要持续监视时还应考虑休息区域和卫生间。要考虑的危害包括辐射、

空气中的烟雾和有毒物质。

8.4.23.3 设计必须能够保证当某一影响核动力厂的事件发生后，控制室或辅助控制室以及通往辅助控制室的通道的环境条件不会损害运行人员的防护和安全。

8.4.23.4 如果人机接口控制站分散配置，运行人员应可以安全、及时地进入不同场所。分散配置的人机接口控制站包括辅助控制室和其他需要操纵员动作的就地场所。

8.4.23.5 为了使运行人员可以有效进入辅助控制室或其他需要人员动作的就地场所，应为其提供适当的路径以防止潜在的内部危险和外部危险。

8.5 历史数据记录

人机接口应提供记录、存储和显示历史数据的功能，帮助运行人员判断模式和趋势、理解系统过去和当前状态、执行事件后分析或预测未来发展。

9 软件

9.1 概述

9.1.1 本章的要求适用于仪控系统安全重要设备中使用的所有软件类型，例如操作系统、已开发软件或固件、针对项目专门开发的软件以及在现有的已开发系列软硬件模块的基础上开发的软件。

9.1.2 相对于模拟系统，数字化系统需要采用不同的可靠性

分析方法。数字化系统的可靠性可从对生产活动质量及验证和确认结果的评估来推断。软件的固有特点使其比硬件（电气或机械设备）具有更大的设计空间。如果不加以系统性的约束，将容易产生缺陷且无法验证。软件实现的复杂度会在设计中产生额外的故障、增加发现和纠正故障的难度、引入在简单设计中不存在的失效模式和影响、降低与安全系统设计准则（例如独立性、可测试性和可靠性）符合性相关论证的可信度。

9.1.3 第 2 章对质量保证和全生命周期过程的要求与软件特别相关，因为其所覆盖的活动对于有效的软件开发是不可或缺的。

9.1.4 基于计算机的安全重要系统必须确定或制定用于开发和测试/验证计算机软、硬件的适当的标准和规范，并在整个寿期内执行，特别是在软件开发过程中应执行这些标准和规范。整个开发过程必须遵循质量保证体系。

9.1.5 系统的软件开发应按照预定的生命周期进行，应充分的规划并形成文档，同时应包括全面的验证和确认（详见第 2 章）。

9.2 软件需求

9.2.1 为满足仪控系统需求所必需的全部软件，包括复用软件或自动生成的代码，其需求均应以适当的形式文档化，满足第 9.2.2-9.2.7 节下述要求。

9.2.2 建立软件需求所采用的技术组合应预先确定，且与系统的安全重要程度相匹配。建立软件需求的技术包括使用有明确定义的语法和语义的规范语言、建模、分析和审查。

9.2.3 软件需求的开发者应对第 3 章中所述的系统设计基准有着充分的理解。理解系统的设计基准对于确保软件需求能够正确的满足系统的基本属性来说是必要的。需要考虑的设计基准包括：

（1）潜在的故障状态；

（2）运行模式；

（3）用于安全目的的监视；

（4）自监督；

（5）故障探测；

（6）在出现可探测但不可恢复的故障时应达到的安全状态；

（7）其他故障安全特性；

（8）安全相关的输入输出关系。

9.2.4 软件需求规格书：

（1）应定义每个软件需要做什么及其与系统内其他软件如何交互；

（2）软件需求应来自仪控系统生命周期的相关过程（包括对在先前分析中识别出的系统危害的考虑），以及与仪控系统生命周期接口的过程，例如人因工程和网络安全活动（见图 1）；

（3）应尽量描述所需实现的目标，而不是描述这些目标如何设计和如何实现；

（4）其内容应完整、无歧义、前后一致、便于阅读、易于使用者（例如该领域的专家、安全工程师和软件设计者）理解，

并且可验证、可追溯；

（5）应满足分配给软件的系统需求，包括质量要求；

（6）必要时，应详细说明要求的最小精度、数值准确度、接口描述（例如软件和操纵员之间的接口、与传感器和驱动器之间的接口、计算机硬件和其他软件之间的接口、系统之间的接口）、执行线程的独立性、自监督、时限性能（包括故障探测和恢复时间）和网络安全要求（例如有效性校验和权限控制）；

（7）应包含需达到的必要的可靠性和可用性水平。可靠性和可用性的水平可定性确定或定量确定，例如与本节(1)-(6)项软件需求的符合性，以及开发过程与标准的符合性；

（8）应考虑计算机、软件工具和现有相似系统的能力以保证软件需求的可行性；

（9）应适当引用、包含或补充适用于使用者的额外信息，例如特定需求的背景信息、对风险的考虑、对功能或安全特性的设计建议，以使要求能够被使用者理解；

（10）应规定需要特别强调不能由软件实现的功能、行为或交互。

9.2.5 当需要设置设计限制条件时，限制条件应明确、合理、可追溯。

9.2.6 所有软件需求的来源应充分的文档化，以便于验证、确认、追溯至高层级文档，并证明相关需求均已得以考虑。

9.2.7 应使用需求追溯系统以使在开发项目的设计、实现、

集成和验证阶段均可对软件需求进行追溯。

9.3 软件设计

9.3.1 完整的软件设计应做到能够无歧义的、正确的和完整的体现软件需求、前后一致、结构合理、便于阅读、易于使用者（例如该领域的专家、安全工程师和软件设计者）理解、可验证、可确认、可追溯、可维护和文档化。

9.3.2 应采用预先确定的、与系统的安全重要程度相匹配的技术组合来进行软件设计并保持更新。此类技术可包括文字描述、定义了明确语法语义的逻辑图和图形化表达、建模、分析和审查。

9.3.3 软件设计应在理解安全需求来源的情况下进行。

9.3.4 应充分区分软件设计的各个部分，以便于保持软件需求的可追溯性。

9.3.5 安全系统的软件设计应在各个层次上尽可能地简单，包括总体结构、外部接口、模块间的内部接口以及详细设计。

9.3.6 简单化设计是实现和证明安全性的关键手段，但通常需要进行折中考虑（例如功能性、灵活性和成本之间的取舍）。虽然简单化设计要求仅适用于安全系统，但简单化设计对低安全等级系统也是可取的。对于低安全等级的系统，安全性和复杂性之间的取舍关系是不同的，更高复杂度的设计也是可以接受的。

9.3.7 软件的设计架构应是结构化的，以便于未来的修改、维护和升级。

9.3.8 软件架构应是层次化的，提供抽象化的层次分级。

9.3.9 在可行的情况下可使用“信息隐藏”技术（指一个模块内包含的信息，对于不需要这些信息的其他模块来说是不可访问的），以便于分段审查和验证并便于修改。

9.3.10 软件设计应包含软件与外部环境的接口。

9.3.11 软件设计应包含所有软件模块的详细设计。

9.3.12 软件模块的描述应完整地定义其功能、与其他模块的接口以及其功能与整个软件的关系。

9.3.13 具有相似功能的软件模块在结构上应一致。

9.3.14 模块的接口应一致。

9.3.15 模块之间每个接口的两侧应匹配，输入侧和输出侧变量的命名应一致，同时应尽可能地避免模块的递归调用。安全系统不应使用递归调用。

9.3.16 如果系统包含多个处理器且软件分布在不同的处理器上执行，软件设计应规定每个进程在哪个处理器上运行，并规定数据和显示的所在位置。

9.3.17 软件设计应支持安全系统的确定性行为和确定性时限。

9.3.18 通信协议应满足第 7.5.4 节的要求。

9.3.19 在设计细化时，应考虑故障探测和自监督特性的附加功能需求，并包括在软件设计中（见第 6.6.3.6 节）。

9.3.20 在检测到故障时，应采用适当措施满足恢复或停止进程，错误信息和日志等方面的软件需求，保证系统处于安全状态。

9.3.21 软件设计文档应包含设计阶段需关注的对于实现的限制。此类对于实现的限制可能包括确保多样性的要求，以及程序设计语言、编译程序、子程序库和其他支持软件工具的特定属性要求等。

9.3.22 对于实现的限制应进行合理性论证或可追溯到更高层次的需求或限制。对于安全系统以外的系统，若使用专有系统，其实现限制追溯到该系统供应商的标准文档即可。

9.3.23 软件的结构设计应考虑由于采用多样性所产生的对模块和接口的限制条件。

9.3.24 软件设计应尽可能地考虑在网络安全上的良好实践，以避免在设计阶段引入漏洞。此类漏洞会使得软件容易被恶意软件感染或黑客攻破，且难以修复。

9.3.25 在可行的情况下，软件设计应进行同行审查。

9.4 软件实现

9.4.1 软件实现应满足：

（1）应正确和完整地体现软件需求，完整地体现软件设计，结构合理，具备可读性、可验证性、可追溯性、可维护性，适当地文档化；

（2）应采用预先确定的、与系统的安全重要程度相匹配的技术组合，包括编程语言、软件工具、代码编写规范、分析、审查、测试等；

（3）应可证明已落实所有软件需求和软件设计；

（4）应简单并易于理解，相对于易于编程，应优先保证可读性和可维护性；

（5）应包括可读形式的源代码和可执行代码、单元接口测试和模块接口测试的结果及充分的上下文信息，以验证代码相对于其规格书的正确性。

9.4.2 代码应充分的文档化。

9.4.3 对于安全系统，所有代码（包括运行时支持代码和故障监督功能）应有对应的描述文档，以满足本导则中测试相关的要求。

9.4.4 应在开始编写代码前制定代码编写规则，并验证规则的执行情况。

9.4.5 应采用一致的数据结构和命名规则。

9.4.6 软件实现应满足下列要求：

（1）执行规定的变更控制程序（包括影响分析）；

（2）执行配置管理；

（3）对于所有变更结果保证适当的测试覆盖率。

9.4.7 所用的编程语言（或语言子集）应能满足表达力、避免不安全表述、抽象层级、对模块化和信息隐藏的支持、编译检查和运行时检查、错误处理方面的要求。

9.4.8 安全系统所用编程语言应支持简明化的软件实现。

9.4.9 编程语言的选择和采用的功能定义方式（例如逻辑图或图形化表达）应基于对功能性和过程完整性需求的系统评估。

9.4.10 对于安全系统，应对编程语言的选择进行合理性论证并形成文件。

9.4.11 对于安全系统，编程语言的语法和语义应完整、有效并有严格的定义。

9.4.12 软件函数是执行特定功能的编程元素。这些函数可能是编程语言固有的、包含在库文件中的或以其他形式预先开发的。

9.4.13 软件函数的使用目的是最大程度上提升软件的简单性，使用的软件函数应是事先确定的，有明确定义的接口，其调用应遵循相关的使用限制条件。

9.4.14 如果使用操作系统，则应对其进行（或已进行过）深入全面的测试，并论证其对于目标应用的适用性。

9.4.15 对于安全系统，所有的操作系统软件应符合本导则的全部要求。

9.4.16 应以错误最小化为目标选用合适的软件实现工具。相关要求见第 7.6 节。

9.4.17 第 9.4 节的要求适用于使用代码生成和传统软件开发方式的所有可能的组合。

9.4.18 软件多样性（即采用独立的开发团队和/或不同的方法、语言、时序、函数或算法顺序）可以作为降低软件共因故障可能性和影响的手段。然而软件多样性会引入设计限制，这些限制本身可能会导致新的故障。

9.4.19 应采取预防措施以避免因使用相同的软件（例如操作

系统、网络通信软件或其他运行支持软件）导致各层纵深防御所需系统之间的独立性被破坏。

9.4.20 软件实现团队应接受过安全开发技术培训。

9.5 软件验证和分析

9.5.1 软件的需求、设计和实现应根据仪控系统需求规格书进行验证。

9.5.2 可追溯性的验证应是一个持续的活动，以确保尽早发现不足并进行必要的修改。

9.5.3 软件生命周期内每个阶段的成果均应按照上一阶段的需求进行验证。

9.5.4 应生成软件验证计划以记录：

（1）所采用的验证技术；

（2）每种技术对应的验证程序的细节或参考资料，包括程序的范围和深度；

（3）如何证实非功能需求和限制条件已得到满足；

（4）判断验证是否充分的准则，包括对于前一阶段设计输出的验证完整性目标和功能测试的覆盖率目标，以及如何证实已经实现了这些目标；

（5）验证结果的记录方式；

（6）不符合项和缺陷的记录和解决方式；

（7）执行验证的团队以及该团队与软件设计者之间的独立性；

（8）验证所用的软件工具的功能，预期的使用方法（例如适用范围、语言和流程）和使用限制；

（9）确定上述（1）-（8）项的依据，以及对所实施的软件验证充分性的论证（相对于软件所属系统的安全等级）。

9.5.5 验证应包含以下技术：

（1）人工检查，例如审查、走查、检验或审核；

（2）对源代码的静态分析；

（3）动态分析。

9.5.6 静态分析应在软件的最终版本上进行。

9.5.7 静态分析所采用的技术因系统的安全重要程度而异。静态分析技术包括与设计和代码编写标准的符合性验证、控制流分析、数据和信息流分析、符号执行、形式化代码验证等。

9.5.8 应对软件中实现的所有非功能需求进行验证。

9.5.9 应根据相关运行经验来识别软件异常，并予以纠正，以进一步提高对于软件可靠性的置信度。相关运行经验可作为其他验证技术的补充，但不能代替其他验证技术。

9.5.10 第 7.6 节给出了使用软件验证和分析工具的相关要求。

9.5.11 应为软件实现的验证和确认确定测试的策略（例如自下向上的策略或自上向下的策略）。

9.5.12 测试用例规格书应确保以下项目得到充分测试：

（1）接口（例如模块间的接口、软硬件间的接口、系统边界接口）；

（2）数据传输机制和接口协议；

（3）异常状态；

（4）每个输入变量的全范围（采用等效类别划分和边界值分析等技术）；

（5）系统的所有运行模式。

9.5.13 测试计划应确保测试是可重复的且测试结果得到记录，以便于开展回归测试。

9.5.14 应尽量减少重复性测试中所需的人工干预。

9.5.15 所有测试工具的选择、标识、使用方法、标定要求和标定间隔应予以规定。应明确对测试工具进行管控的责任。

9.5.16 应审查测试用例规格书及其有效性，对相对于验证计划目标的任何不足，均应予以解决或进行合理性论证。

9.5.17 验证工作应由独立于设计者和开发者的团队、个人或工作组执行。

9.5.18 应审查源代码以检查软件安全漏洞，审查中应使用自动的软件工具，并辅以关键代码（例如输入输出处理和异常处理）的人工审查。

9.5.19 验证过程中应监视仪控系统的所有输出，同时分析和记录所有与预期结果的偏差。

9.5.20 验证结果相对于验证计划的不足（例如实际达到的测试覆盖率）应得以解决或论证。

9.5.21 对于任何检测到的错误，应分析其原因、按照批准的

变更程序改正并进行适当的回归测试，并对此是否适用于仪控系统其他部分进行评估。

9.5.22 发现的异常数量和类型的记录应予以保持，通过对记录的审查可以对开发过程有深入的认识，通过使用这些记录可以适当地改进开发过程，为当前项目和未来项目带来好处。

9.5.23 验证和分析文档应提供一套条理清晰的证据，证明开发过程的结果是完整的、正确的和协调一致的。

9.5.24 验证结果（包括测试记录）应形成文档，保存并可随时供质保监查和第三方评定所用。

9.5.25 设计文档的可追溯性应包含生命周期每个阶段的文档和功能需求之间的有序链接。

9.5.26 测试结果文档应可追溯至（或自）测试用例规格书，同时应指出哪些测试结果不符合预期以及这些问题是如何解决的。

9.5.27 测试范围应清晰的记录在文档中。

9.5.28 对于安全系统，应能够通过追溯矩阵来追溯每个测试用例，追溯矩阵显示了软件需求、设计、实现和测试之间的链接关系。

9.5.29 对于安全系统，生成的应用程序应进行网络安全测试（例如渗透测试），以确认难以检测到一般的网络安全漏洞，并支持软件设计和实现的持续改进。

9.5.30 测试文档应足以保证测试过程可以重复进行并能够

得到相同的结果。

9.6 已开发软件

9.6.1 安全系统中使用的已开发软件应和为该应用专门开发的软件具有相同的鉴定等级。

9.6.2 已开发软件的功能应符合第 2.4.2 节的要求。

9.6.3 对于安全系统以外的安全重要系统，已开发软件应具备用户文档，描述：

（1）所提供的功能；

（2）接口，包括输入、输出、异常信号、参数和配置数据的作用、类型、格式、范围和限制；

（3）不同的行为模式及其对应的转换条件（如适用）；

（4）使用已开发软件需满足的限制条件；

（5）对于已开发软件符合用户文档（1）-（4）项的论证；

（6）对其功能适用于仪控系统的论证。

9.7 软件工具

第 7.6 节提供了软件工具的要求。

9.8 第三方评定

9.8.1 安全系统软件的第三方评定应和软件开发过程同步进行。

9.8.2 第三方评定的目的是提供关于系统及其软件适当性的评定，该评定独立于系统和（或）软件的供应商和运行机构。这样的评定可以由监管机构或监管机构认可的组织承担。

9.8.3 与软件开发者进行适当的约定和妥善的安排以便于开展第三方评定。

9.8.4 评定应包含以下内容的检查：

（1）开发过程（例如通过质保监查和技术检验，包括检查生命周期文档，例如计划、软件规格书和全范围测试活动的文档）；

（2）终版软件（例如通过静态分析、检验、审核和测试）和后续变更。

名词解释

在本导则中下列名词术语的含义为：

部件。组成系统的一个部分。一个部件可以是硬件或软件，并可以再细分为其他的部件。

非功能需求（也称质量需求）。除功能和行为需求之外，规定物项的固有属性或特性的需求。例如可分析性、可用性、可维护性、可靠性、安全性、可验证性、准确性和响应时间，等。

固件。装载到一类存储器（例如只读存储器 ROM）、在处理过程中不能由计算机动态修改的计算机程序和数据。

功能需求。规定物项需具备的功能和行为的要求。

和缓环境。严酷性不超过在核动力厂正常运行和预计运行事件期间的环境。

校准。在规定的条件下，确定测量仪表或测量系统的指示值、实物量具、参考物质所表示的值与相应标准规定值之间关系的一组操作。

结构。核动力厂安全重要仪控系统的组织架构。

静态分析。基于系统或物项的组成、结构、内容或文档对其进行分析。

可靠性。在给定状态下和给定时间间隔内某物项（或系统）完成所要求使命的概率。

可用性。反映某物项（或系统）按命令工作的概率。包括稳态可用性，即某物项（或系统）长期运行时预期满意工作的时间

份额；和瞬态可用性，即在某一特定瞬时，某物项（或系统）将正常工作的概率。

配置基线。在物项生命周期中的特定时间点上正式指定和固化的一系列物项配置。

确定性时限。系统或部件从激励到响应之间的延时保证在一定范围内的特性。

确定性行为。系统或部件在规格范围内任意输入序列总是产生相同输出的特性。

确认。通过检查或提供其他证据，证实该系统完全满足预期的需求规格书要求。

人机接口。运行人员与连接到核动力厂的仪控系统之间的接口，包括显示、控制以及与操纵员辅助系统之间的接口。

生命周期模型。一个框架，它包括从需求定义到使用终止，贯穿整个生命期的系统开发、操作和维护中所需实施的过程、活动和任务。

危害。潜在的损害。

危害分析。对系统全生命周期的检查过程，以识别其固有危害和危害因素，以及消除、预防、控制危害的要求和限制。

危害因素。导致潜在损害的因素。

现场可编程门阵列（FPGA）。可由仪控制造商进行现场编程的集成电路，包含了可编程的逻辑模块（组合或顺序使用）、逻辑模块间可编程的连接关系及可编程的输入输出模块。其功能

由仪控设计者定义，而不是由电路制造商定义。

型式试验。对代表产品的一个或多个物项进行的符合性试验。

序列。构成冗余系统或安全组合的一个冗余度的一系列物项及其连接。一个序列可以包含多个通道。

需求工程。包含了对一系列需求开发、记录和维护活动的工程过程。

严酷环境。由反应堆冷却剂丧失、主蒸汽管道破裂和其他高能管道破裂导致的环境。

验证。通过检查和提供客观证据，证实一项活动的结果符合为此活动规定的目标和需求。

硬件描述语言（HDL）。为形成文档、仿真或综合，用来正式描述电子部件的功能和（或）结构的语言。

硬件描述语言可编程器件。使用硬件描述语言及相关软件工具配置的集成电路器件（对核动力厂 I&C 系统）。

已开发模块。可用于硬件描述语言的已开发功能模块，包括库、宏或知识产权核。在开发硬件编程设备之前，可能需要对已开发模块进行大量的工作。

已开发物项。已存在的可用于仪控系统的商用或专用产品。已开发物项包括硬件设备、已开发软件、包含硬件和软件的数字化装置或通过硬件描述语言或已开发模块配置的硬件设备等。

知识产权核。集成电路设计中，功能明确、接口规范、易于验证、便于重用、具有开发者自主知识产权的电路功能模块。