团 体 标 准

T/CNEA XXX-202X

代替T/CNEA XXX-202X

核电厂反应堆保护系统信号故障处理技术导则

Technical guide for signal fault handling of reactor protection system in nuclear power plant

**（征求意见稿）**

XXXX-XX-XX发布 XXXX-XX-XX实施

**中国核能行业协会 发布**

中国核能行业协会（China Nuclear Energy Association，CNEA）是经国务院同意、民政部批准设立的全国性非营利社会团体，成立于2007年4月18日。协会的中心任务是做好政府与会员单位之间、会员单位之间、国内与国际之间的沟通与交流，维护全行业和会员的合法权益，向政府建言献策，为企业排忧解难，努力发挥桥梁和纽带作用。制定中国核能行业协会团体标准（以下简称：核协团标），以满足我国核能行业标准化发展市场需求为导向，为核能行业和相关社会事业提供行业领先的标准化服务，是中国核能行业协会的工作内容之一。中国境内的团体和个人，均可提出制、修订核协团标的建议并参与有关工作。

核协团标按《中国标准化协会标准管理办法》进行制定和管理。

核协团标草案经向社会公开征求意见，并得到参加审定会议的3/4以上的专家、成员的投票赞同，方可作为核协团标予以发布。

在本标准实施过程中，如发现需要修改或补充之处，请将意见和有关资料寄给中国核能行业协会，以便修订时参考。

本标准版权为中国核能行业协会所有。除了用于国家法律或事先得到中国核能行业协会文字上的许可外，不许以任何形式复制该标准。

中国核能行业协会地址：北京市海淀区西三环北路72号世纪经贸大厦B座28层。

固话：010-88305833 传真：010-88305800

网址：http://www.china-nea.cn 电子信箱：cnea\_standard@vip.163.com

目  次

[目次 II](#_Toc65680186)

[前言 III](#_Toc65680187)

[引言 IV](#_Toc65680188)

[1 范围 1](#_Toc65680189)

[2 规范性引用文件 1](#_Toc65680190)

[3 术语和定义 1](#_Toc65680191)

[4 总体原则 2](#_Toc65680192)

[5 技术规格书的编制 3](#_Toc65680193)

[6 设计与实现 3](#_Toc65680194)

[7 系统集成 6](#_Toc65680195)

[8 系统确认 7](#_Toc65680196)

[9 安装和调试 7](#_Toc65680197)

[10 运行和维护 7](#_Toc65680198)

[11 变更和修改 7](#_Toc65680199)

前  言

本标准依据GB/T 1.1-2020的规则编写。

本标准起草单位：江苏核电有限公司、生态环境部核与辐射安全中心等。

本标准起草人：李伟、张云波、管运全、乔宁、穆海洋、刘景宾、谢国宝、郑佳慷、管海飞、史东亮、支凤春、段鹏、刘敏、孟祥山等。

考虑到本标准中的某些条款可能涉及专利，中国核能行业协会不负责对任何该类专利的鉴别。

本标准为首次发布。

引  言

核电厂安全重要仪表和控制系统越来越计算机化后，其设计和故障模式也呈现出一定的复杂化趋势。根据IEC 61513-2011中相关的要求，执行安全功能的仪控系统检测到故障时，仍然需要通过逻辑降级、故障安全和闭锁输出的方式使安全系统保持在备用模式安全运行，为了规范安全相关系统信号故障后的处理原则，特制定本导则。

核电厂反应堆保护系统信号故障处理技术导则

1. 范围

本导则规定了核电厂执行A类安全功能的计算机化的反应堆保护系统应对信号故障的基本要求。

本导则适用于核电厂安全功能和反应堆保护系统的设计与改进。

1. 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20438 电气/电子/可编程电子安全相关系统的功能安全

IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related Systems

IEC 61513 Nuclear power plants – Instrumentation and control important to safety

1. 术语和定义

IEC 61508和IEC 61513界定的以及下列术语和定义适用于本文件。

**通道Train**

系统内相互连接的几个部件发出单一输出信号的配置，在单一输出信号与来自其他通道（例如监测通道或安全驱动通道）的信号结合在一起的地方，通道就告终止。

[GB/T 4960.6—2008，定义4.1.30]

**多样性Diversity**

为执行某一确定功能设置两个或多个独立（或冗余）的系统或部件，这些不同系统或部件具有不同属性，从而减少共因故障（包括共模故障）的可能性。

[HAF 102（2016）]

**安全系统safety system**

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

[HAF 102（2016）]

**保护系统Protection system**

监测反应堆的运行，并根据接收到的异常工况信号，自动触发动作以防止发生不安全或潜在的不安全工况的系统。

[HAF 102（2016）]

**仪控（I&C）功能I&C function**

对工艺过程指定部分实施控制、操作和（或）监督的功能。

**仪控系统I&C system**

基于电气和（或）电子和（或）可编程电子技术的系统，它执行仪控功能以及与系统自身运行有关的服务和监督功能。

**冗余redundance**

除本身外，设置另外一个或多个（相同的或不同的）构筑物、系统或部件，以便其中一个都能执行所要求的功能，不管任何其他的是处于运行状态还是故障状态。

[GB/T 4960.6—2008，定义4.1.10]

**故障failure**

使功能单元执行要求的功能的能力降低或失去其能力的异常状况。

**单一故障single failure**

导致某一系统或部件不能执行其预定安全功能的一种故障，以及由此引起的各种继发故障。

[HAF 102（2016）]

**单一故障准则single failure criterion**

要求系统或设备组合在其任何部件发生可信的单一随机故障时仍能执行其正常功能的设计准则。

[GB/T 4960.6—2008，定义4.1.4]

**质量位quality**

表征信号品质优劣或信号是否故障的开关量信号。

**安全生命周期Safety Lifecycle**

安全相关系统实现过程中所必需的生命活动，这些活动发生在从一项工程的概念阶段开始，直至所有的安全相关系统停止使用为止的一段时间内。

1. 总体原则

通用原则

* + 1. 应对A类安全功能信号故障的功能应满足与A类安全功能一致的安全等级要求，实现该功能的系统软件和硬件平台应与A类安全功能相同。
    2. 为了保证信号故障功能满足电厂安全要求得以确定、实现和保持，应采用系统性的方法。应把与信号故障功能的设计、实现和运行相关的活动置于仪控系统的安全生命周期的框架内。

典型的仪控系统生命周期包括下列阶段：

1）系统技术规格书；

2）系统设计和实现；

3）系统集成；

4）系统确认；

5）系统安装和调试；

6）系统运行和维护；

7）系统设计修改。

1. 技术规格书的编制

安全要求应清晰、准确、可验证、可测试以及可维护，应切实可行，生命周期任一阶段应能方便理解。

针对所有安全功能的描述，应提供充分的、可理解的详细要求。

对于系统及其部件的失效模式（包括应对失效的响应，应对失效的措施等）应当明确要求。

对于系统信号故障后的系统提示要求（报警等）应当详细说明。

1. 设计与实现

故障假设

* + 1. 研究和设计核电厂安全重要仪表和控制系统时，应对可能发生的信号故障进行假设，并根据其假设采取具体的防护措施。
    2. 故障假设的基础应是对安全级信号回路已发生的故障的总结和正确估计。例如：

a)信号源故障，比如取样管线故障、变送器故障等；

b)信号回路故障，比如供电保险、信号保险熔断或者线路故障等；

c)通道间信号交换故障，比如信号分配通道错误、通道间通讯故障等；

d) 系统软件故障，比如堆内核测系统、堆外核测系统、辐射仪表系统等智能化仪表系统的软件故障；

e) 系统硬件故障，比如控制机柜供电模件、信号模件、通讯模件、逻辑处理模件等硬件故障等。

* + 1. 组成安全相关信号回路的元器件性能和环境条件应根据产品标准或生产厂家的规定，结合信号回路的安全要求正确选用，并应考虑故障后果，例如：

a）超量程；

b) 板卡故障；

c) 通道故障；

d) CPU故障等。

故障监测

* + 1. 安全级信号回路应具备必要的自诊断功能及必要的检(监)测设备。检(监)测设备工作或故障时，不能影响其他安全功能的正常工作。

比如部分核电厂安全重要仪表信号可分为模拟量信号和开关量信号两类。其中，模拟量信号输入为4~20mA电流，开关量信号输入为0或24V电压，这两类信号故障监测采用如下手段：

a) 模拟量信号当输入的电流数值偏差超过设计量程的偏差百分比时则判定信号为故障状态；

b) 开关量信号通过设置常开（常闭）双反馈回路的监视，当双反馈回路的电压数值不在设计范围内则判定信号为故障状态。

* + 1. 假设故障一般应以很高的概率发现，发现故障不应引起危险状态或导致运行的危险状态。
    2. 当信号被识别为发生故障后，反应堆保护系统应有效标识故障的信号，使其与正常信号区别开来。
    3. 信号的故障状态在系统的传输流程中应是能被识别且可以被提取出来，用于信号后续传输流程中该信号的隔离、标识、逻辑降级以及触发默认值输出等作用。
    4. 信号发生故障时，应能向核电厂运行人员及时发出警报或报警，以利于及时采取相应的行动。

功能独立性和隔离

不同安全等级的系统和功能之间应相互独立。主要体现在相互间的数据通信隔离和屏障要求。高等级系统相对较低等级系统的单向通信设计。安全级系统内部不同安全组或系列之间也应充分的独立性。

故障失效应对

* + 1. 信号故障应对策略应涵盖冗余信号故障的全部组合

A类安全功能的设计者应明确反应堆保护系统应对信号故障的策略，策略应涵盖冗余信号故障的全部组合：单个冗余信号故障、多个冗余信号故障、所有冗余信号故障。

* + 1. 信号故障应对的常用策略

通常，信号故障应对策略包括：

a)降级运行：当冗余的信号中有数量较少（通常是1个或者2个）的信号发生故障时，剔除发生故障的信号、剩余冗余信号参与下一步功能计算；

例如，四个冗余通道的降级运行方案：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 信号故障情况 | 模拟量降级运行方案 | 开关量降级运行方案 |
| 1 | 无冗余信号故障 | 4取次大（小） | 4取2 |
| 2 | 单个冗余信号故障 | 3取次大（小） | 3取2 |
| 3\* | 两个冗余信号故障 | 2取次大（小）或触发 | 2取1或触发 |
| 4 | 三个冗余信号故障 | 触发 | 触发 |
| 5 | 四个冗余信号故障 | 默认值或最后有效值 | 触发 |
| \*根据安全功能设计者对功能的要求选择2取1或触发 | | | |

三个冗余通道的降级运行方案：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 信号故障情况 | 模拟量降级运行方案 | 开关量降级运行方案 |
| 1 | 无冗余信号故障 | 3取次大（小） | 3取2 |
| 2\* | 一个冗余信号故障 | 2取次大（小） | 2取2或2取1 |
| 3 | 两个冗余信号故障 | 触发 | 触发 |
| 4 | 三个冗余信号故障 | 触发 | 触发 |
| \*根据安全功能设计者对功能的要求选择2取1或触发 | | | |

b)输出默认值，根据安全分析的要求，当冗余信号中有多个或者全部（通常超过3个）发生故障时，输出事先设定的默认值；

例如：

信号故障状态值

表决（4取3）

信号值

默认值

切换

输出

c)闭锁输出，当参与一个功能的冗余信号中有多个或者全部发生故障时，闭锁该功能的输出。

功能完整性

故障状态逻辑设置的闭锁/排除的总体要求是当出现内外部信号故障或条件劣化且可能会造成安全功能失效的情况下，系统仍有能力完成其规定的安全功能。其他辅助性功能、支持性功能都不能对系统执行安全功能的产生有害影响，也不应使安全系统产生误动作。

应考虑工艺状态对核电厂安全重要仪表和控制系统信号的影响

对工艺状态影响了反应堆保护识别信号故障功能的情况，可结合安全功能设计者对于参数监测的要求，根据工艺参数条件排除受影响信号的部分或全部故障应对策略。当机组不在功率运行、处于检修或者检修前的冷却或者检修后的加热状态时，部分就地仪表或传感器可能受到工艺状态的影响，导致反应堆保护系统错误地识别信号出现故障，从而错误地根据信号故障应对策略响应或触发安全功能。应考虑这种可能性，并考虑设置闭锁条件。

其他一般要求

* + 1. 核电厂安全重要仪表和控制系统中的信号传输（包括硬件和软件），应具有必要的安全性和可靠性。

核电厂安全重要仪表和控制系统的所有硬件和软件应满足所有核级设备鉴定、设计、测试等标准。

核电厂安全重要仪表和控制系统信号故障的应对策略应贯穿系统的整个生命周期，并按照系统的安全功能级别执行各阶段的质量控制。

* + 1. 对故障安全的要求，应是从技术上能够实现的，研究和设计各种安全级信号回路，均应满足故障安全的原则。
    2. 信号故障功能应根据冗余信号故障的程度，涵盖全部组合：单个冗余信号故障、多个冗余信号故障、所有冗余信号故障。

信号故障的识别

* + 1. 从参与A类安全功能的工艺信号的生成，到仪控系统安全功能的触发，整个信号链路发生的信号故障均应被有效识别。
    2. 模拟量信号发生的就地仪表、传感器故障和信号传输路径故障，通常可在仪控系统逻辑单元中根据信号电流是否处于正常工作区间判断。此方法需要充分考虑仪表特性，在特定工况下存在误判的可能性。
    3. 模拟量信号如传感器故障和信号传输路径故障可通过单独的质量位信号判断。
    4. 开关量信号的信号触点故障和信号传输路径故障，通常应配置双触点，在仪控系统逻辑单元中通过双触点信号互异的特点判断。
    5. 系统数据传输故障、系统软件故障、系统硬件故障产生的信号故障是由仪控系统本身引起，可通过系统自检有效监视和识别故障。

信号故障的标识

* + 1. 信号在仪控系统逻辑单元的处理中，应包含信号值和质量位两个方面的信息。质量位表征该信号是否故障的状态。
    2. 当信号被识别为故障时，该信号的质量位应标识此状态。
    3. 质量位信号应能被仪控系统逻辑单元提取，以便用于信号后续传输流程中该信号的隔离、标识、逻辑降级以及触发默认值输出等作用。
    4. 在仪控系统的人机接口或可视化界面中，应通过有效的标识方法使工程师、管理员、运行人员能够辨识信号是否处于故障状态。
    5. 对于信号故障的标识，应防止多个通道同时故障后，因为标识对系统多个通道产生影响，导致安全功能不可用。

信号故障的报警

* + 1. 信号发生故障时，应能向核电厂运行人员及时发出警报或报警，以利于及时采取相应的行动。
    2. 信号故障的报警应根据信号冗余故障程度和信号类别分等级设置，既充分引起运行人员注意，又不会不必要地分散运行人员注意力。

1. 系统集成

通用要求

* + 1. 信号故障功能的集成应与仪控系统的集成同步进行。
    2. 如有可能，应集成系统设计中所有的功能模块，以验证这些模块在测试过程中的相互影响和作用。

一般要求

* + 1. 测试前应选择测试用例，测试用例应考虑：

1)覆盖信号故障功能相关的所有信号；

2)覆盖故障假设中设定的所有故障类型；

3)对同一类别的信号，应覆盖此类信号涉及的所有应对策略；

4)应验证信号故障功能不会引起A类安全功能的执行。

* + 1. 通过静态和动态模拟输入信号，应测试验证信号故障功能在正常运行工况、预期运行事件、事故工况的响应。
    2. 测试中应关注信号故障时，仪控系统的响应。
    3. 在集成测试中，应对集成系统的任何修改或改变进行影响分析，以确定是否需要对修改或改变涉及到的模块进行重复测试；
    4. 集成测试应形成文档报告，记录测试结果是否满足测试目的和准则；如测试失败或故障影响仪控系统功能失效的情况，应记录失败原因，并评估是否需要进行修改和重复验证。

1. 系统确认

本阶段的目标是对集成的系统进行试验以证明其符合功能、性能和接口的技术规范。

系统确认应在最终配置（包含最终版本的软件）的系统上进行。

应对每个保护系统信号故障及其相关组合进行测试。

1. 安装和调试

在完成现场安装后，信号故障功能应通过调试试验得到验证。

结合现场信号源相关的故障，应通过现场实际的案例测试验证各种类别的故障的响应与预期一致。

应通过现场实际的案例测试验证其它各种类别的典型故障的响应与预期一致。

结合工艺系统在各种工况的工作情况，评估对仪控系统测量的影响以及是否会导致信号故障。

1. 运行和维护

制定规程规定为满足安全功能日常需采取的活动，如风扇、电池、滤网等。

为防范不安全状态或降低不安全因素，应制定日常、机组停机期间的定期测试规程。

针对可预见的故障、干扰或失效，应制定应急方案或者预案。

1. 变更和修改

应当为每次修改建立文档，文档应包括：

1）变更或修改的详细描述；

2）变更或修改对整个系统的相互作用进行影响分析；

3）变更或修改带来的改进或提升；

4）变更或修改验证的方案；

5）系统规程及相关文档的变更；

变更或修改的设计、实施和测试应与系统开发时的水平保持一致。

变更或修改完成后，应对系统功能及相互影响重新进行验证。

变更或修改应获得批准后才能执行。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_