文章类型：论文|刊号（ISSN）：2972-4112(P) / 2972-4120(O)

核电厂重要数字化控制保护信号回路可靠性提升研究

张朋　王博
中广核惠州核电有限公司
DOI:10.12238/pe.v3i3.13616

[摘　要] 数字化控制保护系统,对核电厂而言至关重要。重要控制保护信号回路尤其是跳机跳堆甩负荷信号回路,一旦出现失效将直接影响机组安全稳定运行。本文对核电厂重要数字化控制保护信号回路可靠性研究重要性进行论述,分析当前数字化控制保护信号回路典型的单点失效模式。在此基础上,提出数字化控制保护信号回路供电、通道、软件配置原则,最后提出可靠性提升的系统分析方法及管控措施落实的最优化考量建议。
[关键词] 数字化；控制保护信号；单点失效；可靠性
中图分类号：C935　文献标识码：A

Research on improving the reliability of important digital control and protection signal circuits in nuclear power plants

Peng Zhang　Bo Wang
CGN Huizhou Nuclear Power Co., LTD

[Abstract] Digital control and protection system is very important for nuclear power plant. Failure of the important control protection signal circuits, especially the turbine-trip,reactor jump or load rejection related signal circuits, will directly affect the safe and stable operation of the nuclear power plant. This paper discusses the importance of studying on improving the reliability of important digital control and protection signal circuits in nuclear power plants, and analyzes the typical single point failure modes of the digital control and protection signal circuits. On this basis, the principles of power supply, channel and software configuration of digital control protection signal circuits are put forward. Finally, the system analysis method to improve reliability and the optimal consideration for the implementation of control measures are put forward.
[Key words] Digitalization; Control protection signal; Single point failure; Reliability

引言

随着国内核电稳健有序发展,核电发电在全国的占比逐步提高。而核电厂控制保护系统的数字化水平,也随之不断迭代更新。核电站的安全稳定,直接关系经济民生乃至国家安全。加强对核电厂重要数字化控制保护信号回路可靠性提升具有重要意义,为核电站的安全运行提供坚实基础。

1 核电厂重要数字化控制保护信号回路可靠性提升的重要性

核电厂控制保护系统,通过实时监测及控制核电站运行参数(如温度、压力、中子通量)在要求的范围内,确保反应堆始终处于安全状态,并能够在异常工况下触发保护动作,防止堆芯熔毁或放射性泄漏,其作用至关重要。在核电站实际运维阶段,存在因数字化控制保护信号回路设备失效、异常导致跳机跳堆甩负荷或机组后撤情况。因此,数字化控制保护回路尤其是跳机跳堆甩负荷信号回路的可靠性,必须得到充分保证。其可靠性提升,有助于进一步提高核电厂安全性、延长设备寿命、降低运维成本等。而核电厂重要数字化控制保护信号回路单点失效的识别和管控,是提升可靠性的最关键、有效的方式。

单点失效:一个一旦失效便会造成无法挽回后果的关键点。

2 核电厂重要数字化控制保护信号回路典型单点失效模式

⑴冗余仪表设备共用取样管线,容易因共用取样管线堵塞、断裂、振动等共因故障同时导致冗余仪表测量信号异常。⑵触发跳机、跳堆、甩负荷等信号的重要单一仪表,由于设计不合理或本体故障率高易导致信号触发。⑶供电回路单一设备故障。冗余仪表设备,或多个控制保护执行机构存在单一供电薄弱点,如使用单一空开、供电模块、同一供电链路,从而导致供电故障同时影响冗余仪表及执行机构情况。⑷冗余仪表设备采用同一电缆,导致单一仪表故障后无法独立处理。⑸控制保护仪表信号分配不合理:①单一DI/AI卡采集多个存在控制保护逻辑关联的重

要信号或冗余信号；②多个重要存在控制保护逻辑关联的信号或冗余信号经过单一隔离设备；③单一DO/AO卡输出控制多个存在控制保护逻辑关联的执行设备。⑹如实现2/3、2/4等冗余控制保护信号前端冗余，而在信号传输及处理过程中间环节实际为假冗余设计，容易因中间薄弱环节导致控制保护异常或失效：①多个模拟量信号取中间值/次大值等用于控制，由单一卡件传输，卡件故障将导致控制保护异常；②多个冗余信号通过阈值或逻辑判断，由单一卡件传输，卡件故障将导致控制保护异常；③信号涉及柜间传输，采用单一网络或硬接线信号，网络或硬接线信号异常将导致控制保护异常。⑺逻辑设计不合理、软件缺省值/质量位设置不合理，导致单点故障引发控制保护异常。比如，单一仪表质量未参与重要阀门控制，引发系统控制异常等。

3 重要数字化控制保护信号回路的配置要求

3.1供电配置

可靠的电源是保证数字化控制系统正常运行的基础，不可靠的电源会导致冗余设备同时故障或者导致通讯网络的失去，进而导致跳机、跳堆、甩负荷。①控制系统必须有可靠的两路独立的供电电源，互为备用，切换时间应满足机组要求。应具有电源诊断和报警功能，无论是外部供电故障或内部电源故障，均能够发出报警提示。②所有控制系统电源必须专用，不得用于其他用途。严禁非控制系统用电设备连接到控制系统的电源装置。比如：电加热器、风扇、照明灯泡、检修插座等不直接接入控制系统供电回路，并采用有效隔离，辅助设备故障不能导致电源越级动作。保护电源采用厂用直流电源时，应有发生系统接地故障时不造成保护误动的措施。③保护系统应采用不间断电源或蓄电池直流电源，并应设置双回路供电。保护系统电源中断或恢复时不会误发动作指令。④重要的仪控系统双路供电回路，应取消人工切换开关。直流电源宜采用二极管进行冗余配置。⑤所有装置和系统的内部电源切换可靠，回路环路连接，任一接线松动不会导致电源异常影响装置和系统的正常运行。⑥各级电源开关容量和熔断器熔丝应匹配，熔断器的连接方式可靠、容量/特性满足要求，防止故障越级。⑦交、直流电源开关和接线端子应分开布置，交、直流电源开关和接线端子应有明显的标识。⑧多路电源冗余并列运行，应定期检查各电源装置的输出电流均衡，防止因电源负载不均衡造成个别电源负载加重而降低电源可靠性。⑨IO板件单个通道电源故障(接地、短路)的影响范围不应超过其所在的卡件。⑩卡件、服务器、网关、交换机等重要设备的电源故障(接地、短路)不引起系统电源故障。

3.2信号通道配置原则

①重要仪控模拟量控制项目的变送器宜冗余配置(至少二重冗余)。冗余配置的测量信号应分别使用不同电缆进行信号传输。②严禁涉及重要保护的变送器、开关与其他测量元件共用取样口及取样管路。③控制器模块应采用冗余配置[1]，重要参数测点、参与机组或设备保护的测点应冗余配置，冗余I/O测点应分配在不同模件[2]上，任一测点采集故障不应影响其它冗余测点采集。冗余信号相关修正计算信号或参与重要信号计算的也不能放置在同一卡件且不能交叉放置，防止一块卡件故障后导致冗余信号同时失去。④单一跳机跳堆信号应通过硬接线传输。重要信号不宜采用通讯的方式进行传输[3](尤其是不能使用与第三方的通讯方式来传输)，否则信号处理逻辑中应该有防止通讯故障的处理措施。⑤冗余信号从采集信号传感器开始至运算输出全链路，包括中间传输环节(电缆、隔离分配及隔离分配电源)在物理上应是独立的，任一信号链路故障不会影响其他信号。不同控制器之间通过硬接线传输的单一信号，可使用通讯信号作为备用信号，在硬接线故障时切换至通讯信号。⑥在控制系统中非冗余电源最后一级空开、熔断器、开关所带设备中不能配置冗余信号，防止最后一级空开、保险动作后冗余信号同时失去。⑦信号负极共地端子排的总接地线应冗余配置，防止一根总接地线脱落后该端子排所有信号丢失。控制系统接地必须严格遵守相关技术要求，接地电阻满足标准要求，并保证控制系统一点接地；所有进入控制系统的控制信号电缆必须采用质量合格的屏蔽电缆，且可靠单端接地；分散控制系统与电气系统共用一个接地网时，分散控制系统接地线与电气接地网只允许有一个连接点。⑧重要的模拟量输出控制信号要保证IO卡件有足够的带载余度。⑨在仪表和控制设备的信号电缆的敷设过程中应与动力和控制电缆保持一定的距离以降低来自动力和控制电缆的电气噪声。仪表和控制设备的信号和控制电缆的敷设应避开电动机、发电机、射频设备、电弧或工业电焊设备等强电磁场区域。⑩所有就地涉及仪控重要保护的启停或开关操作按钮、就地远方切换按钮、就地操作显示面板均应有防护措施，防止因无意磕碰、踩踏造成重要设备误动。

3.3软件配置原则

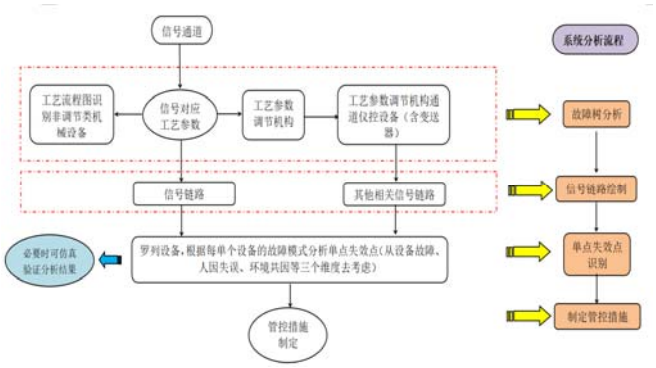

图1　可靠性提升的系统性分析方法示意图

①重要模拟量信号应该设置可靠性判断逻辑(偏差大、开路、短路、接地、超量程)，当判断出信号不可靠时应该剔除。②单个信号判断不可靠后应触发相应的报警。③应设置重要信号故障后的处理逻辑：A、单个信号故障后应该设置有缺省值或者自保持最后一个有效值，缺省值的设置的大小应结合实际控制回路综合分析后给出，考虑的因素包括对设备监视的影响、对机组瞬态的影响、机组技术规范要求等。缺省值的设置要考虑IO卡件故障后存储器清除后的影响，建议在控制器中来存储缺省

值。B、多个冗余信号故障后,由于此时信号已不可信,应分析是否该将控制回路切手动控制及报警情况。

4 可靠性提升的系统分析方法

可靠性提升系统性方法如图1所示,分为故障树分析、信号链路绘制、单点失效点识别、制定管控措施几个步骤。

4.1故障树分析

将信号通道触发作为顶事件,使用故障树自上而下的分析方式,逐级梳理可能的故障原因。比如,典型的压水堆核电厂汽水分离再热器壳体液位,四块液位计测量液位,2/4液位高触发跳机保护。一是从工艺流程图识别导致跳机信号触发的非调节类机械设备,比如某安全阀外漏导致再热器内部压力降低,引起虚假高水位,则该设备为单点失效设备。二是识别液位信号采集至最终跳机输出的全链路上是否可能存在单点失效点；三是壳体液位工艺上实际由正常/应急疏水阀门控制。因此识别正常/应急疏水阀门控制全链路上是否可能存在单点失效点从而可能导致跳机。

4.2信号链路绘制

以信号流为逻辑关系,将信号链路的所有设备绘制在一张图上,图上需要标注关键信号,包括电缆编码、端子号、卡件通道号等信息。

4.3单点失效点识别

罗列出设备,从设备故障、人因失误、环境共因等三个维度去考虑分析是否存在单点失效。设备角度,故障模式应考虑合理,比如,模拟量传感器考虑上漂、下漂故障模式,仪控继电器应同时考虑拒动和误动模式。识别单点失效主要参照前文【重要数字化控制保护信号回路的配置要求】进行对比分析。人因失误主要考虑误碰、引入异物。环境共因可考虑温湿度、粉尘、电磁干扰、水淹等情况。

4.4制定管控措施

①通过改造优化彻底消除；②缓解：A、增加或优化预防性维修项目,根据失效风险、故障模式及发生概率、老化/环境等因素的影响进行综合评估；B、状态监测,明确监测方式、关键点及关键参数、监测周期等；C、增加防误碰或放异物管控措施,如使用警示标识、布置重要敏感区域、增加实体防护等；D、加强相关作业管控；E、提高及完善失效点设备相关的工作文件质量,增加提醒等。

5 可靠性提升措施落实的最优化考量

从提高核电厂重要数字化控制保护信号回路可靠性角度而言,通过改造优化彻底消除理论上是最好的处理方式。实际上,上述单点失效分析更多为定性分析,其对机组的潜在风险跟设备故障率有较大关系,不可一概而论。另外,改造通常在重要敏感设备上实施,其潜在技术风险也非常高,成本投入较多。因此在考虑消除单点失效的改造方案确定上,需要结合失效点风险、故障发生概率、改造的必要性和可行性分析进行综合考量其经济性,即投入与产出的关系。如经济性差,而通过缓解措施也可以进行有效管控,那采取合适的缓解措施则为最优化方案。

6 总结

综上所述,本文提出核电厂重要数字化控制保护信号回路典型单点失效模式,在此基础上提出了供电、通道、软件配置原则,并给出一种可靠性提升的系统分析方法,开展单点失效系统性排查及管控,进一步提升数字化控制保护系统的运行稳定性。

[参考文献]

[1]郑伟智.集散控制系统在核电站保护系统中的应用[J].核电子学与探测技术,2012,32(04):438-441+452.

[2]公民,黄鹏,肖林,等.核电站安全级DCS系统IO分配原则浅析[J].仪器仪表用户,2018,25(11):40-42+46.

[3]陆炜伟,彭沛星,连鑫炜.提升“华龙一号”核电机组DCS可靠性的研究[J].电子技术应用,2023,(S1):79-83.

作者简介：

张朋(1988--),男,汉族,广东韶关人,中广核惠州核电有限公司,工程师,大学本科,研究方向：仪表控制。