自控系统冗余设计在天然气关键节点中的逻辑配置原则

王海鹏　周敬桢
国家管网集团北京管道有限公司河北输油气分公司永清作业区　河北　廊坊　065600

摘　要：随着我国能源结构的持续优化和“双碳”战略目标的深入推进，天然气作为清洁高效的化石能源，在国家能源体系中的地位日益凸显。其长距离、高压、大管径的输送特性，对管道系统的安全、稳定、连续运行提出了极高要求。自控系统（SCADA/DCS）作为天然气管网的“神经中枢”，其可靠性直接决定了整个输气网络的安全边界。本文聚焦于天然气关键节点（如首站、压气站、分输站、末站及阀室等）的自控系统冗余设计，深入剖析了硬件冗余、软件冗余、通信冗余及供电冗余等多维度冗余架构，并在此基础上，系统性地提出了适用于天然气行业的冗余逻辑配置核心原则，包括“故障安全优先”、“无缝切换无扰动”、“独立性与隔离性”、“可诊断与可维护性”以及“全生命周期成本最优”。研究表明，科学、严谨的逻辑配置是实现冗余系统从“形式冗余”到“实质可靠”跃升的关键，对于保障国家能源动脉安全、提升企业运营效率具有重要的理论与实践价值。

关键词：天然气；关键节点；自控系统；冗余设计；逻辑配置；功能安全

引言

天然气是能源转型及“双碳”目标实现的重要桥梁，我国已建成庞大天然气骨干管网，总里程超数十万公里。其核心在于首站、压气站等关键节点，这些节点非计划性中断会引发连锁反应，造成巨大损失、社会影响及公共安全风险。自控系统（SCADA/DCS）是保障关键节点安全高效智能运行的核心支撑，负责采集参数、执行逻辑、实现保护并上传数据。但电子元器件老化等因素使单一设备可能失效，若自控系统核心组件故障且无有效应对机制，后果严重。冗余设计是提升系统可靠性的根本策略，在天然气关键节点应用中，它是提高可用性及满足功能安全法规要求的基石[1]。不过，冗余并非简单硬件堆砌，其效能依赖底层逻辑配置的科学性，错误配置会引发安全事故。所以，深入研究并确立一套清晰、普适、可操作的冗余逻辑配置原则，对指导工程实践、筑牢安全防线意义迫切。

1 天然气关键节点自控系统冗余架构概述

在深入逻辑配置之前，有必要先厘清自控系统冗余的基本架构层次。一个典型的天然气关键节点自控系统冗余设计通常涵盖以下四个层面：

1.1 硬件冗余

这是最直观的冗余形式，指对物理设备进行备份。（1）控制器冗余：采用主/备（1oo1D, One out of One with Diagnostics）或三重化（TMR）配置。主/备模式下，一台控制器处于工作状态（Active），另一台处于热备状态（Hot Standby），实时同步数据和状态。当主控制器故障时，备用控制器在毫秒级时间内接管控制权。（2）I/O模块冗余：对于关键信号（如ESD按钮、关键压力变送器），可采用冗余I/O卡件。信号可以同时接入两个独立的I/O通道，由控制器逻辑进行处理（如2oo2表决）。（3）现场设备冗余：虽然成本高昂，但对于极端关键的执行机构（如干线截断阀），有时会考虑双电磁阀、双执行机构等设计，但这更多属于SIS范畴。

1.2 软件冗余

软件冗余主要体现在控制逻辑和数据处理层面。（1）表决逻辑（Voting Logic）：在多重化系统中（如2oo2, 2oo3），通过软件算法对多个通道的输出结果进行比较和表决，只有满足预设条件（如两个通道一致）才输出有效指令，有效屏蔽单点故障。（2）故障检测与诊断（FDD）：嵌入在控制逻辑中的自诊断程序，能够实时监测硬件状态、通信质量、逻辑执行周期等，及时发现潜在故障并触发报警或切换。（3）数据同步机制：主备控制器之间通过高速同步链路（Sync Link）交换内存数据、程序状态、I/O映像等，确保切换时上下文的一致性。

1.3 通信冗余

通信网络是自控系统的“血管”，其可靠性至关重要。（1）网络拓扑冗余：普遍采用环形（Ring）或双星型（Dual Star）拓扑。主流工业以太网协议如PRP（Parallel Redundancy Protocol）、HSR（High-availability Seamless Redundancy）或厂商私有协议（如西门子的MRP）能够在链路或交换机故障时实现＜50ms的无缝切换，远优于传统STP/RSTP协议。（2）多路径路由：对于广域网（WAN）连接调度中心，通常采用双运营商、双物理路由的专线，结合动态路由协议（如OSPF）实现路径冗余。

1.4 供电冗余

稳定的电力供应是所有电子设备工作的前提。（1）双路市电输入：来自不同变电站的两路独立市电。（2）UPS不间断电源：在市电中断后提供分钟级的后备电力，保证系统有足够时间安全停机或等待发电机启动[2]。（3）冗余电源模块：控制器、交换机等关键设备内部通常配备N+1冗余的电源模块，单个模块故障不影响整机运行。

这四个层面的冗余相互交织、共同作用，构成了一个立体的防护网。而将这张网编织得牢固、高效的“针线”，正是我们接下来要探讨的逻辑配置原则。

2 自控系统冗余逻辑配置的核心原则

冗余逻辑配置是冗余设计的灵魂。它决定了在何种条件下触发切换、如何进行状态同步、如何处理故障信号等一系列关键问题。针对天然气关键节点的特殊性，我们提出以下五大核心原则。

2.1 故障安全优先原则

这是所有安全相关系统设计的首要铁律。在天然气领域，“故障安全”意味着当系统发生任何可检测的故障（包括自控系统自身故障）时，最终的安全状态必须是趋向于“关闭”或“隔离”，即触发ESD（Emergency Shutdown）动作，关闭相关区域的进出站阀门，停止压缩机运行，以防止事故扩大。逻辑配置体现在：（1）输出失效模式设定：所有关键安全输出（DO）点，在控制器失电、程序跑飞、通信中断等故障状态下，必须默认进入“安全状态”（通常是失电关闭，即Fail-Safe to De-energize）。这需要在硬件选型（选用故障安全型继电器）和逻辑组态中双重确认。（2）冗余表决逻辑选择：对于安全联锁回路，应优先选用能导向安全侧的表决逻辑。例如，2oo3（三取二）架构中，只要有两个通道检测到危险状态，就触发ESD。即使一个通道故障（给出错误的安全信号），另外两个正确的危险信号仍能驱动系统进入安全状态。相比之下，2oo2（二取二）虽然可用性更高，但若一个通道故障给出危险信号，会导致误停车，需谨慎使用。（3）通信故障处理：当关键设备（如远程I/O站、安全栅）与主控制器的通信中断时，相关的安全输入信号应被置为“最坏情况”（如压力高高报），并参与联锁逻辑计算，确保在通信丢失的情况下也能导向安全。

2.2 无缝切换无扰动原则

冗余切换的目标是在用户和工艺过程完全无感知的情况下完成。任何切换过程中的数据丢失、控制指令跳跃或短暂失控，都可能对高压天然气管道造成冲击，甚至引发喘振、水击等次生灾害[3]。逻辑配置体现在：（1）精确的数据同步：主备控制器间的同步链路必须保证关键数据（如PID控制器的积分项、累加器值、设备状态位）的实时、一致同步。逻辑组态时，应明确区分哪些变量需要同步，哪些可以不同步（如调试用的临时变量）。（2）输出保持（Output Hold）：在切换瞬间，备用控制器的输出值必须与主控制器切换前的最后一刻完全一致。这要求控制器硬件支持“输出冻结”或“最后状态保持”功能，并在逻辑中正确启用。（3）避免重复动作：逻辑中需设置防抖和去重机制。例如，一个启泵命令在主控制器发出后，即使切换到备用控制器，也不应再次发送该命令，除非收到明确的停止指令。这通常通过在命令信号上附加唯一的序列号或时间戳来实现。（4）切换条件精细化：不应仅凭简单的“心跳丢失”就触发切换。应综合判断，如连续N个扫描周期无响应、关键任务超时、硬件自检报错等，以避免因瞬时网络抖动导致的频繁、不必要的切换。

2.3 独立性与隔离性原则

冗余单元之间的独立性是冗余有效的前提。如果主备单元共享同一个故障源（Common Cause Failure, CCF），那么冗余就失去了意义。逻辑配置体现在：（1）物理隔离：主备控制器、电源、网络交换机应安装在不同的机柜，甚至不同的房间，以规避火灾、洪水等区域性风险。（2）电气隔离：主备系统的供电回路、I/O回路应完全独立，使用独立的端子排、保险丝和电缆。逻辑上，应禁止主备控制器通过非同步链路进行任何形式的数据交互，以防故障蔓延。（3）软件隔离：主备控制器应运行完全相同的程序镜像，但其内部的执行环境（如内存地址空间）是相互隔离的。逻辑组态工具应能确保程序下载和更新的原子性，避免主备程序版本不一致。（4）共因故障分析（CCF Analysis）：在逻辑设计阶段，应进行CCF分析，识别并消除潜在的共因，如使用同一品牌的同批次元器件、受同一电磁干扰源影响等，并在逻辑中增加多样性设计（如对关键信号采用不同算法处理）。

2.4 可诊断与可维护性原则

一个优秀的冗余系统不仅要在故障时能用，还要能让运维人员快速、准确地知道“哪里坏了”、“为什么坏”以及“如何修”。逻辑配置体现在：（1）分级报警体系：建立完善的报警逻辑，区分“冗余单元故障”、“同步链路异常”、“即将切换预警”等不同级别的报警，并将信息清晰地推送给操作员和维护工程师。（2）内置自诊断（BIST）：在控制逻辑中嵌入周期性的自检程序，如内存校验、CPU负载监控、I/O通道回路测试等。诊断结果应形成详细的日志，便于事后分析[4]。（3）在线维护支持：逻辑应支持在系统运行期间对备用单元进行软件升级、硬件更换

等维护操作，而无需停机。这要求逻辑能识别维护模式，并暂时屏蔽相关的切换条件。（4）仿真与测试接口：在逻辑中预留测试点和仿真接口，允许在离线或在线状态下对冗余切换逻辑进行充分验证，确保其在真实故障场景下的正确性。

2.5 全生命周期成本最优原则

冗余设计需要投入额外的成本（CAPEX）和维护费用（OPEX）。过度冗余会造成资源浪费，冗余不足则会带来安全风险和潜在的停产损失。因此，冗余配置必须基于风险评估，追求全生命周期成本的最优平衡。逻辑配置体现在：（1）基于SIL定级的差异化配置：依据IEC 61511标准，对每个安全仪表功能（SIF）进行SIL（Safety Integrity Level）定级。SIL等级越高（如SIL3），对冗余的要求就越严格（如必须采用TMR或2oo3）。对于非安全相关的常规控制回路（如温度调节），可采用成本更低的1oo1D主备冗余。逻辑配置必须与SIL定级结果严格对应。（2）可用性与安全性权衡：在满足安全底线的前提下，通过逻辑设计优化可用性。例如，在2oo3系统中，当一个通道故障后，系统可降级为1oo2模式继续运行（此时安全性降低，但可用性得以维持），并发出高级别报警，提示尽快维修。这种“降级运行”逻辑需要精心设计，明确其适用边界和退出条件。（3）标准化与模块化：在逻辑组态中采用标准化的冗余功能块（Function Block）和模板，可以大幅降低工程设计、测试和后期维护的成本，减少人为错误。

3 结语

自控系统冗余设计是保障天然气关键节点安全的生命线，而科学、严谨的逻辑配置则是这条生命线能否真正发挥作用的决定性因素。本文系统性地提出的“故障安全优先”、“无缝切换无扰动”、“独立性与隔离性”、“可诊断与可维护性”以及“全生命周期成本最优”五大逻辑配置原则，为工程实践提供了清晰的指引。这些原则并非孤立存在，而是相互关联、相互制约的有机整体，需要在具体项目中根据风险评估结果进行综合权衡与应用。未来，随着数字化、智能化技术的发展，自控系统冗余逻辑配置将面临新的机遇与挑战。一方面，基于大数据和人工智能的预测性维护技术，可以提前预判硬件故障趋势，使冗余切换从“被动响应”走向“主动预防”。另一方面，云边协同、虚拟化等新技术的引入，对传统物理隔离的冗余模式提出了挑战，如何在虚拟化环境中保证逻辑的独立性和确定性，将是未来研究的重要方向。无论如何演进，坚守功能安全的底线，以科学的逻辑配置为核心，始终是确保国家能源大动脉安全、稳定、高效运行的根本之道。

参考文献

[1]黎燕.PLC在天然气输送自控系统中的应用研究[J].化工管理,2020,(12):123-124.

[2]贾继灿.天然气长输管线自控系统设计与应用[J].化工管理,2020,(27):172-173.

[3]缪全诚.PLC在天然气输送自控系统中的应用[J].中国高新科技,2022,(13):54-55.

[4]王克琼,张鹏,赖鑫,等.天然气场站自控信息化设备可靠性分析及优化措施研究[J].中国石油和化工标准与质量,2025,45(18):135-136+139.