天然气长输管道 SCADA 系统设计及网络安全性评估与强化

贾永强　范　刚　刘秦龙（国家管网集团西北公司西安输油气分公司，陕西　西安　710018）

摘　要：天然气长输管道作为国家能源运输的核心基础设施，其安全稳定运行直接关系到国计民生。SCADA 系统作为管道运行监控的神经中枢，承载着实时数据采集、远程设备控制和运行状态分析等关键功能。针对系统设计过程中的安全缺陷与防护薄弱环节，开展系统性网络安全评估并制定强化策略具有迫切现实意义。本文聚焦设计阶段的架构可靠性及运行阶段的安全防御机制，旨在构建全生命周期的防护体系，确保能源输送系统的持续安全运行。

关键词：天然气输送管道；SCADA 系统架构；工控系统安全评估

中图分类号：TE832　　**文献标识码：**A　　**文章编号：**1674-5167（2025）031-0141-03

Design and Network Security Assessment and Enhancement of SCADA System for Long-Distance Natural Gas Pipeline

Jia Yongqiang, Fan Gang, Liu Qinlong (Xi’an Oil & Gas Pipeline Sub-Company, Northwest Pipeline Company, PipeChina,Xi’an Shaanxi 710018, China)

Abstract: As a core infrastructure for national energy transportation, the safe and stable operation of long-distance natural gas pipelines is directly related to the national economy and people’s livelihood. The SCADA system, as the nerve center for pipeline operation monitoring, undertakes critical functions such as real-time data collection, remote equipment control, and operation status analysis. Conducting systematic network security assessment and formulating strengthening strategies for security flaws and weak points in the design process is of urgent practical significance. This paper focuses on the reliability of the architecture in the design stage and the security defense mechanism in the operation stage, aiming to build a full life-cycle protection system to ensure the continuous safe operation of the energy transportation system.

Keywords: Natural gas pipeline; SCADA system architecture; Industrial control system security assessment

工业控制系统安全已成为保障国家关键基础设施的核心要素。天然气长输管道 SCADA 系统因其分布范围广、结构层级多、通信环节复杂等特性，面临严峻的网络安全挑战。设备选型与拓扑设计奠定系统物理安全基础，通信协议与数据架构则决定信息传输的健壮性。当前威胁环境呈现攻击向量多元化、渗透手段隐蔽化趋势，传统边界防护模式难以应对高级持续性威胁。研究基于国际工业安全标准，从网络拓扑结构设计入手系统分析攻击路径，结合分层防护理念提出纵向加密与横向隔离协同防御机制。通过构建覆盖设备层、控制层及管理层的三位一体评估体系，形成可量化安全基线以指导防护策略优化。

1 天然气长输管道 SCADA 系统设计原则

1.1 可靠性原则

天然气长输管道跨越地理环境复杂区域，SCADA 系统必须维持全年无间断运行状态[1]。设备冗余配置在控制系统架构中扮演关键角色，主备通信信道采用物理隔离的光纤双环网结构，现场控制单元部署双 CPU 热备切换模块，当主处理器发生异常时可于毫秒级自动启用备用单元。工艺控制层设置独立的本地逻辑控制器，即使在控制中心通信中断情况下仍能维持压力调节、紧急截断等基础安全功能。远程终端单元（RTU）需通过 IEC 61508 SIL2 安全认证，电磁兼容性能满足 GB/T 17626 标准的 IV 级工业抗干扰要求。服务器集群采用故障自动检测机制，历史数据库实施分布式多节点实时同步存储策略。

1.2 开放性原则

系统设计必须兼容不同供应商的设备协议栈，通信架构采用国际通用 OPC UA 数据交换框架作为中间件层，支持 Modbus TCP/IP、DNP3.0 等工业协议的无缝接入。控制层应用程序接口（API）依据 IEC 61131-3 标准开发，组态软件提供标准 SQL 数据库访问通道满足第三方系统数据调用需求。网络拓扑保留标准 RJ45 和光纤接口扩展槽位，为后期新增压缩机站、分输站等节点预留即插即用接入能力。人机交互界面（HMI）需支持 SVG 矢量图形解析引擎，保障不同分辨率终端设备显示元素自适应缩放不丢失数据精度。

1.3 安全性原则

纵深防御机制贯穿系统设计全生命周期，控制网络划分三层物理隔离域：现场传感器层采用 RS-485

屏蔽双绞线构建本安回路，场站控制层通过工业防火墙实施协议白名单过滤，调度中心层部署双向光闸实现与管理信息网的逻辑隔离。操作员站实行三因子身份认证，关键指令执行需经历权限复核与操作轨迹双录存证。数据存储采用 AES-256 算法分段加密，通信报文添加时间戳与序列号防重放攻击保护。控制器固件建立哈希值验证流程，任何未经签名的代码更新触发硬件级保护锁死机制。

2 天然气长输管道 SCADA 系统设计

2.1 系统总体架构设计

天然气长输管道 SCADA 系统采用分层分布式架构，由物理层、控制层与管理层构成纵向三级管控体系。物理层部署智能变送器和执行机构集群，通过本质安全型信号回路实时采集管道压力、温度及流量参数。控制层设置区域化冗余控制器组，每个场站配置双机热备的可编程逻辑控制器（PLC）系统，基于工艺单元划分独立控制域执行闭环调节 [2]。管理层搭建双活数据中心架构，历史服务器集群采用负载均衡技术分配实时数据写入任务，操作员工作站组态界面整合管道地理信息系统拓扑渲染引擎，三维可视化平台动态展示全线设备运行状态。控制指令传输采取逐级授权校验机制，任何远程操作命令需经控制层逻辑校验与设备层安全联锁双验证。

2.2 硬件设计

现场仪表选用符合 API 6A 标准的防爆型压力变送器，振动传感器满足 ISO 10816-III 级机械防护要求，电动执行机构配置扭力过载保护单元。通信节点采用工业级环网交换机组建光纤自愈环网，主干通信带宽预留 40% 余量承载突发数据流量。控制机柜配置双路独立供电模组，中央处理器模块支持在线热插拔维护功能。服务器集群采用刀片式架构，配置冗余电源与主动散热系统保障高温环境持续运行。工程师站配备 4K 多屏显示系统，操作台集成硬件急停按钮链与声光报警指示装置。场站控制室安装电磁屏蔽机柜，防雷接地系统符合 GB 50057 一级防护标准，机架空间预留 20% 扩展槽位支撑后期设备扩容。

2.3 软件设计

监控系统基于实时内核操作系统构建，多任务调度引擎保障数据采集周期稳定控制在 100 毫秒级。数据采集模块内置信号滤波算法消除现场干扰，控制模块集成 PID 参数自整定功能适应不同工况调节需求。人机界面采用矢量图形引擎开发，管线压力剖面图支持动态梯度着色预警显示。历史数据库采用时序数据分区存储策略，建立时间戳索引机制实现十年运行数据秒级检索。报警管理引擎实施多维关联分析，对温度骤降伴生压力异常等复合事件触发特别告警。数据备份系统执行差异增量同步策略，故障恢复时点精度达到交易级一致性要求。通讯驱动框架支持 DNP3.0 协议报文分片重组，异常断点续传功能保障网络波动期间数据完整性。

2.4 通信网络设计

主干通信采用环形光纤骨干网拓扑，关键节点设置物理层自愈切换装置实现 50ms 内链路重构。场站局域网划分三个逻辑隔离域：过程控制网部署工业级协议过滤网关限制非授权访问，视频监控网配置流量整形机制保障控制指令优先传输，管理信息网设置应用层代理防火墙进行深度报文检测。无线接入点采用 WAPI 认证协议加密传输，移动终端操作启动动态口令双因子校验。核心层交换机启用 MAC 地址绑定功能，边缘端口配置风暴抑制策略防范广播包泛洪攻击。通讯协议栈遵循 IEC 62351 安全规范，关键控制指令传输增加报文鉴别码（MAC）校验机制。卫星备份链路建立按需激活模式，主通道中断时自动切换载波频率维持最低带宽控制能力。

3 天然气长输管道 SCADA 系统网络安全性评估

3.1 网络安全威胁分析

天然气长输管道 SCADA 系统的分布式特性导致攻击面扩大，外部威胁主要源于互联网暴露接口的协议漏洞探测与恶意代码注入，攻击者利用工业控制协议缺乏加密认证机制实施中间人劫持。内部风险集中在操作权限越界行为，维护人员误触关键参数可能引发联锁反应失效，未授权设备接入控制网络形成横向渗透跳板。物理层脆弱性体现为恶劣环境中通信光缆意外中断，电磁干扰造成传感器数据失真，极端天气导致的基站供电中断威胁监控连续性。攻击者可能结合工控协议弱点与 IT 系统漏洞，设计针对压力调节阀的特定时序攻击序列 [3]。

3.2 评估指标体系构建

网络安全评估维度架构建立在保密性、完整性、可用性三重防护目标基础上，可用性维度重点追踪控制指令端到端传输延迟与冗余控制器切换时效。完整性监控关注组态工程版本哈希值异常变动，审计控制逻辑下装过程的操作时间戳合规性，检测配置库文件非授权篡改行为。保密性度量聚焦密钥轮换周期合理性及访问控制策略颗粒度，特别核查远程维护会话的加密协议强度等级。核心量化指标涵盖工业协议签名验证覆盖率、安全事件审计完整率、控制器固件校验成功率，设置动态基线阈值驱动分级预警机制运行。

3.3 评估方法选择

威胁建模采用 ATT&CK 框架绘制攻击路径图谱，分析压缩机组控制单元遭受勒索软件加密的操作序列可能性。定性评估组织跨领域专家德尔菲法三轮评议，

开发包含工业防火墙规则验证、用户权限矩阵核查的专项检查表。定量方法应用改进型模糊层次分析法（IFAHP），构建判断矩阵计算协议缺陷、物理防护薄弱、身份认证失效的复合风险权重。网络渗透测试激活工业协议模糊测试工具，模拟 Modbus TCP 异常功能码报文冲击控制站协议栈健壮性。主机层部署安全探针采集进程调用链数据，时间序列分析模型识别与正常操作模式偏离度超过预设阈值的异常指令组合。

3.4 评估流程与实施

评估范围明确定义为从场站 RTU 至调度中心的控制数据流完整路径，边界划分兼顾与站场消防系统的数据交互接口安全验证需求。现场勘察阶段配置工业流量镜像设备捕获 OPC DA 通信会话建立过程的安全协商细节，使用频谱分析仪扫描控制柜周边电磁环境识别异常辐射信号。数据采集环节同步启动安全信息事件管理平台，汇聚操作行为日志、网络流特征及 PLC 运行状态多源数据流，部署轻量级数据探针采集老旧 PLC 的串口通信报文。分析过程执行基于杀伤链模型的攻击仿真推演，验证控制系统遭遇拒绝服务攻击时的本地控制回路维持能力，推演场景包含主备通信链路交替中断的极限工况测试。报告生成阶段关联漏洞扫描结果与资产关键值映射矩阵，划分需 48h 内处置的紧急风险项与允许周期性整改的中低风险问题，输出涵盖控制层加固措施与管理规程优化的处置路线图，特别标注涉及压力调节阀安全联锁的参数修改强制复核流程 [4]。建立评估结果回溯验证机制，三个月内复查高风险项整改实效并测量攻击面收敛程度。

4 天然气长输管道 SCADA 系统网络安全性强化策略

4.1 技术层面强化策略

工业防火墙在网络边界部署七层深度包检测引擎，配置基于 Modbus 功能码的白名单过滤机制阻断异常寄存器访问请求。控制网内部实施微隔离策略，按照压缩机控制单元与调压单元划分逻辑安全域，域间通信启用工业协议深度解析网关验证消息来源可靠性。操作员站登录采用生物特征与物理密钥双因子认证，关键指令执行前触发操作复核流程并由数字签名系统记录操作轨迹。通信会话建立阶段强制激活国密 SM4 算法加密信道，控制报文添加序列号与时间戳双重防重放保护。安全审计探针部署在核心交换机镜像端口，采集控制器 CPU 异常负载率与进程非法调用行为，威胁分析模型实时比对 ISA/IEC 62443 异常行为特征库生成告警事件。

4.2 管理层面强化策略

设备全生命周期管理要求新接入控制器提交安全评估报告，运维终端启用临时账户自动回收机制限定两小时有效操作时长。人员权限遵循最小化授予原则，工程师站账户划分 16 级操作权限树，阀门调试操作需要值班长权限与区域控制权限双重解锁。现场设备维护期间激活电子工牌近场感应功能，工具软件安装启动代码签名证书验证流程防止未授权程序注入。安全培训体系设置年度八课时强制性课程模块，包含社会工程学攻击识别实景演练与控制器灾备恢复操作考核。供应商管理制度明确现场服务监管条款，外部人员设备接入控制网前必须通过专用沙箱设备完成恶意代码扫描认证。

4.3 应急响应机制建设

应急预案基于攻击杀伤链模型划分四级响应场景，勒索病毒激活事件触发隔离被感染控制站立即步骤，同步启用本地控制单元紧急接管流程。应急演练设置压力变送器信号欺骗实战科目，攻击组利用协议漏洞注入虚假超压信号，防御组需在 5min 内定位欺诈节点并切除通信链路。恢复阶段部署具有自签名能力的控制器固件恢复盘，逻辑控制器在固件刷新过程保持本地 PID 调节功能不间断运行。取证分析系统配置只读镜像存储设备，完整留存攻击过程审计日志用于追溯入侵路径。灾难恢复预案每季度执行无预警压力测试，模拟主调度中心瘫痪状况下，备用中心可于十五分钟内部署应急指挥平台接管全网络负荷 [5]。

5 结语

科学合理的 SCADA 系统架构设计为管道安全运行奠定技术基础，分层解耦的系统结构保障各功能模块既独立运作又协同响应。网络安全防御体系应贯穿控制系统全生命周期，技术层面深度整合协议级防护与加密认证机制，管理层严格规范设备准入流程与操作权限控制。持续开展覆盖设备层、网络层、应用层的安全评估能够动态识别系统脆弱性，应急响应机制建设有效降低突发事件处置延迟。将可扩展性原则融入系统设计蓝图为技术升级预留空间，使监控系统既能适应当前管道运行需求，又能兼容未来智能化升级趋势，最终构建具备弹性防御能力的工业控制系统生态。

参考文献：

[1] 刘涛 . 天然气长输管道 SCADA 系统设计及网络安全性评估与强化 [J]. 仪器仪表用户 ,2024,31(01):8-10.

[2] 高楠 , 陈彦合 , 李景雪 , 等 . 天然气长输管道站控系统网络架构分析 [J]. 化工管理 ,2025,(18):89-91.

[3] 刘华秋 . 天然气长输管道施工技术研究 [J]. 现代盐化工 ,2025,52(01):82-84.

[4] 周万悦 . 天然气长输管道施工关键技术分析 [J]. 石化技术 ,2024,31(10):154-155+112.

[5] 王亚栋 . 长输天然气管道 SCADA 系统信息安全现状分析及优化措施 [J]. 网络安全和信息化 ,2024,(10):147-149.