油气管道工控网络安全态势感知系统建设

冯云帆（国家石油天然气管网集团有限公司东北分公司，辽宁　沈阳　110170）

摘　要：油气管道工控系统属于能源运输关键基础设施的核心构成部分，它的安全稳定运行对于国家能源安全以及公共利益有着直接的关键关联。当下工控网络面临着如 APT 攻击、协议漏洞利用、数据篡改等多种类型的安全威胁，传统的防护体系在达成全生命周期安全管控方面存在险阻。本文基于油气管道工控网络的实时性、专用性等核心特性，从建设背景与需求出发，系统阐述态势感知系统的分层架构设计，深入剖析数据采集、分析及可视化等关键技术，明确系统实施与运维的核心要点，为构建全维度、智能化的油气管道工控网络安全防护体系提供技术支撑与实施指引。

关键词：油气管道工控网络；安全态势感知；系统架构；数据采集分析；可视化技术

中图分类号：TP393.08；TE973　　**文献标识码：**A　　**文章编号：**1674-5167（2026）002-0124-03

Construction of an Industrial Control Network Cybersecurity Situational Awareness System for Oil and Gas Pipelines

Feng Yunfan(Northeast Branch of National Petroleum and Natural Gas Pipeline Network Group Co., Ltd., Shenyang Liaoning 110170,China)

Abstract: The industrial control system of oil and gas pipelines is a core component of energy transportation critical infrastructure, and its safe and stable operation is directly related to national energy security and public interests. At present, industrial control networks are facing various types of security threats such as APT attacks, protocol vulnerability exploitation, and data tampering. Traditional protection systems have obstacles in achieving full lifecycle security control. This article is based on the core characteristics of real-time and specificity of oil and gas pipeline industrial control networks. Starting from the construction background and requirements, it systematically elaborates on the layered architecture design of the situational awareness system, deeply analyzes key technologies such as data acquisition, analysis, and visualization, clarifies the core points of system implementation and operation, and provides technical support and implementation guidance for building a comprehensive and intelligent oil and gas pipeline industrial control network security protection system.

Keywords: oil and gas pipeline industrial control network; Security situation awareness; System architecture; Data collection and analysis; Visualization technology

随着工业互联网与数字化转型推进，油气管道工控系统从传统封闭结构变为网络化、智能化结构，SCADA、DCS 等核心系统和公共网络联系增强，在提升运输效率和管控精度时，安全风险变大。油气管道是国家能源运输的重要通道，其工控网络安全影响能源供应、生态环境和社会稳定，受到攻击可能引发重大事故[1]。当前，对工控系统的攻击精准、隐蔽且持续，传统边界防护方式难以应对未知和内部风险。所以，构建有实时感知、精准判断、快速反应能力的安全态势感知系统，是提升油气管道工控网络安全防护水平的关键方法。

1　油气管道工控网络安全态势感知系统建设背景与需求

1.1　油气管道工控系统的重要性与特点

油气管道工控系统是达成油气全流程自动化管理控制的关键基础设备，承担着实时收集数据、进行控制、开展监控等任务，是保障能源供应的关键部分。和传统 IT 网络相比，它有明显的行业特殊之处：一是实时性要求高，SCADA 系统收集数据与控制响应的延迟要在毫秒级别，网络中断或者延迟可能引发事故；二是异构性突出，融合了多种网络架构和工业协议，不同厂商设备的协议有差别，增加了安全防护的难度；三是可用性比保密性更重要，部分老旧设备难以适配新型安全防护技术；四是地理分布范围大，沿线的工控设备分散部署，网络节点分散，物理防护困难，容易成为安全薄弱环节。这些特点决定了其安全防护要同时考虑实时性和可用性，不能直接使用传统 IT 网络防护方式[2]。

1.2　建设态势感知系统的必要性

当前，油气管道工控网络安全威胁增加，安全防护被动落后问题明显，建设态势感知系统十分必要。外部威胁方面，国际地缘政治冲突让能源基础设施成为攻击对象，攻击者利用漏洞修改指令、非法控制设备，隐蔽性高，传统边界防护设备难以预警。内部风险方面，运维操作不标准、权限管理无序、老旧设备漏洞未修复等会引发问题，传统管理模式难以追溯内部操作和预判风险。另外，系统互联互通使网络边界不清晰，安全风险传导途径增多，单一防护设备无法

掌控全网安全。态势感知系统通过实时收集与分析数据，能早期发现威胁、判断态势、准确预警，将防护从“被动应对”变为“主动防御”，为运维人员提供整体安全管控视角，是保障系统安全稳定运行的关键。

2 油气管道工控网络安全态势感知系统架构设计

2.1 系统总体架构概述

油气管道工控网络安全态势感知系统用分层结构来设计，依照“数据驱动、协同合作、精准助力”原则，建立“采集 – 处理 – 分析 – 展示 – 应对”全流程闭合体系，达成对工控网络安全态势的全方面感知与全周期管理。系统整体结构从上到下分为数据采集层、数据处理与分析层、态势展示与预警层三个主要层级，各层级通过标准接口相互连接、协同工作。同时使用边云协同结构，把部分对实时性要求高的分析任务放在边缘节点，核心数据与深度分析任务放在云端，兼顾实时反应与整体判断。这种结构适合油气管道工控网络分布式布置与实时性要求，能整合安全资源，准确识别并快速应对网络攻击、设备异常、操作违规等安全风险 [3]。

2.2 数据采集层设计

数据采集层是态势感知系统的基础部分，承担全网安全相关数据的收集与汇总任务。其设计重点在于确保数据收集的全面、实时与安全，且不干扰工控系统正常工作。收集范围涵盖油气管道工控网络全方面数据，包含核心工控系统业务数据、网络设备网络数据、终端设备数据、运维人员操作数据。收集采用“无源收集为主、有源收集为辅”的方式，网络流量等数据使用无源收集设备以避免干扰，终端设备状态等数据在取得厂商许可后用有源方式收集，同时保证数据安全。另外，数据采集层具备数据预处理能力，对不同结构的数据进行标准化等处理，为后续数据工作提供高质量支持。

2.3 数据处理与分析层设计

数据处理与分析层是态势感知系统的关键部分，承担对采集数据进行深度挖掘和安全态势判断的任务，核心目标是实现异构数据的融合分析以及安全威胁的精准识别。该层级采用“边缘计算 + 云端分析”的合作架构。边缘节点对实时性要求高的数据流进行本地分析，例如网络流量异常检测等，部署轻量级模型以快速应对紧急威胁；云端平台汇聚并深度分析全网上报的大量数据，构建多维度模型以全面判断态势和预测趋势。数据处理使用分布式框架，以分布式方式存储和并行处理大量异构数据，确保效率和可扩展性；运用数据融合技术整合不同数据源的数据，消除数据孤岛以提升数据价值。数据分析融合多种技术，构建多维度安全态势分析模型，包括基于异常检测、威胁情报、攻击链的模型。通过多模型合作分析，精准识别威胁、评估威胁等级和判断态势。

3 油气管道工控网络安全态势感知系统关键技术

3.1 数据采集技术

数据收集技术是态势感知系统正常工作的基础。针对油气管道工控网络具有异构性和实时性的特点，采用多种技术结合的收集方法，准确收集全方面数据。工业协议分析技术是数据收集的核心技术之一，针对主流工业协议，通过逆向分析和深度分析算法，准确分析协议字段，提取关键信息，识别异常字段和违规操作，为安全分析提供基础数据。网络流量收集技术使用高精度流量探测工具和网络镜像技术，全面收集工控网络链路流量，支持协议流量识别统计，捕捉异常数据包等关键信息，使用流量过滤和采样技术减少数据处理压力。终端设备数据收集技术结合轻量级代理和标准化 API，在终端部署轻量级收集代理，实时收集设备信息，对老旧设备通过工业协议网关收集，使用数据加密传输技术保证数据传输安全。此外，数据同步技术使用时间戳同步方法，统一不同数据源收集数据的时间，确保后续数据分析准确 [4]。

3.2 数据分析技术

数据分析技术是实现安全态势准确判断的核心。针对油气管道工控网络安全威胁特征，结合机器学习、深度学习、关联分析等技术，建立多维度、智能化分析模型。机器学习技术在异常检测中普遍使用，通过监督、无监督学习算法，对工控网络正常运行数据进行训练，建立正常行为基线模型，当实时数据偏离基线时识别异常。其中，无监督学习算法不需要人工标注样本，能够识别未知异常，适用于复杂多变的安全威胁。深度学习技术通过建立循环神经网络（RNN）、卷积神经网络（CNN）等深度神经网络模型，深入挖掘海量工控数据，自动提取深层特征，提高对隐蔽性攻击的识别能力，例如，基于 RNN 模型的时序数据分析可以识别基于时间序列的攻击行为。关联分析技术建立攻击链关联模型，关联匹配不同数据源信息，例如，关联分析网络流量、设备日志、运维操作等数据，还原攻击路径，预测攻击意图，识别协同攻击行为，提高对复杂攻击的识别能力。

3.3 安全态势可视化技术

安全态势可视化技术把复杂安全数据和态势信息变成图形来展示，帮助运维人员快速了解全网安全情况，提高决策速度。拓扑可视化技术根据工控网络拓扑结构制作动态拓扑图，实时呈现设备和链路状态，出现异常时高亮显示，帮助运维人员快速找到故障。

态势仪表盘技术用多维度指标展示方式，通过仪表盘、柱状图等展示核心指标，帮助运维人员掌握整体安全态势。热力图可视化技术基于地理信息系统（GIS）展示油气管道沿线节点安全状态，用不同颜色区分风险等级，帮助运维人员了解风险地理分布。事件追溯可视化技术通过时间轴等展示安全事件全过程和结果，帮助运维人员还原事件全貌、总结经验。

4 油气管道工控网络安全态势感知系统实施与运维

4.1 实施流程规范化

系统实施流程标准化是保证态势感知系统成功部署与正常运行的关键，要按照“需求调查 – 方案制定 – 部署操作 – 测试检查 – 投入使用”全流程标准进行。需求调查阶段要仔细调查油气管道工控网络核心信息，联合各方力量确定系统需求，形成需求规格说明文件。方案制定阶段根据调查结果，结合行业经验制定各类方案，关注兼容性、安全性等关键问题，保证方案可行合理。部署操作阶段采用“分步部署、先试点后推广”策略，先在非核心区域或试点站点部署验证，再推广到全网，严格遵守安全规范。测试检查阶段搭建全面测试环境，对系统进行全面测试，邀请第三方评估，及时改进问题。投入使用阶段制定投入使用方案，明确流程、分工和应急预案，完成系统部署配置，培训运维人员[5]。

4.2 部署策略精准化

部署策略精确化需依据油气管道工控网络分布式特征与业务需求，运用“边云协同、分区部署”方式，保证系统运行效率与防护成效。云端平台设置在企业核心数据中心，承担全网数据汇聚整合、分析、态势判断与趋势预测任务，运用分布式集群架构确保高可用性与可扩展性，同时设置数据备份与恢复系统保障核心数据安全完整。边缘节点设置在油气管道沿线加压站、阀室等站点，承担本地数据采集、分析与预警任务，运用轻量化方案适配有限算力与带宽，快速应对本地威胁并上报关键数据与结果。针对核心工控系统，如 SCADA 控制中心、DCS 系统等，单独设置采集设备与分析节点，保证数据采集安全可靠，防止干扰核心业务。

4.3 运维体系常态化

构建长期稳定运维体系是保证态势感知系统持续运行的关键，要建立“日常监测 – 故障处理 – 策略改进 – 紧急应对”完整运维流程。日常监测由专业运维人员负责，持续监测系统运行情况等，建立每日检查制度、形成记录，及时处理数据采集中断等问题。故障处理建立标准响应流程，明确故障级别、响应时间等，制定处理方案，出现故障后及时启动，找到原因、采取行动，记录过程并形成记录。策略改进根据日常监测、故障处理、威胁信息更新等情况，定期改进采集策略、分析模型等，提高系统识别准确性与响应速度，如更新威胁信息库。紧急应对建立联合机制，重大安全事件出现时，系统预警，运维人员启动方案，协调多方力量处理事件，及时报告进展，减少损失。

4.4 安全管理体系化

体系化安全管理是保障态势感知系统自身和数据安全的重要方法，要从人员管理、制度建设、技术保障三个方向构建完整体系。在人员管理方面，建立严格的准入和权限管理机制，按照最小权限原则分配操作权限，并定期审核清理，防止出现滥用情况；加强安全培训，定期开展演练，提高人员安全意识、操作技能和应急处理能力。在制度建设方面，制定完善的安全管理制度，明确操作规范和责任追究机制，保证运维工作规范、标准；建立安全审计制度，全面审计操作行为、运行日志和访问记录，及时纠正违规行为。在技术保障方面，采用多种安全技术，例如用加密技术处理采集和传输的数据、用访问控制技术限制非法访问、用入侵检测与防御技术防范攻击、用漏洞扫描技术定期检测并修复漏洞，保证系统安全稳定。

5 结语

建设油气管道工控网络安全态势感知系统，是应对当下复杂多变安全威胁、保障能源运输“大动脉”稳定运行的必然举措。借助分层架构设计、突破关键技术以及构建实施运维体系，达成了从数据采集到态势研判、从实时预警到快速响应的全流程闭环管控，此系统提升了工控网络的安全防护能力，推动了安全防护模式从被动响应转变为主动防御，为油气管道行业的数字化转型与智能化发展奠定了坚实安全基础，有深远的行业示范意义与战略价值。

参考文献：

[1] 黄伟，汪佳慧，唐宁泽 . 油气管道工控系统网络安全风险与三道防线构建 [J]. 中国石油和化工 ,2025(08):65-67.

[2] 张贺 . 油气管道工控网络数据安全防护 [J]. 数字技术与应用 ,2025,43(03):77-79.

[3] 王荡 . 局域网信息安全技术在油气管道企业中的应用分析 [J]. 中国石油和化工标准与质量 ,2025,45(03):189-191.

[4] 李欣嵘，郭亮，朱同，等 . 油气管道工控系统网络性能提升与隔离防护 [J]. 油气田地面工程 ,2022,41(10):51-58.

[5] 油气管道工业控制系统网络安全防护方案 [J]. 自动化博览 ,2022,39(01):104-105.