 DOI: https://doi.org/10.12349/iser.v7i7.11413

Research on a Real-time Vulnerability Monitoring Platform for Equipment and Software Management Based on the Industrial Control Network of Oil and Gas Pipelines

Xuerui Teng[1] Chufan Zheng[2] Mingzhong Feng[3]

1. National Pipeline Network Group Tianjin Liquefied Natural Gas Co., Ltd., Tianjin, 300452, China
2. National Pipeline Network Group Northern Pipeline Co., Ltd. Beijing Oil and Gas Transmission Branch, Langfang, Hebei, 065000, China
3. Kate Intelligent Control Technology Co., Ltd., Weifang, Shandong, 261021, China

Abstract

Oil and gas pipeline networks constitute critical infrastructure within energy transmission systems, where their industrial control networks perform essential functions including station monitoring, valve room scheduling, pressure regulation, leakage detection, and remote coordination. With the continuous adoption of digital, networked, and intelligent technologies, the number of devices, software components, communication protocols, and remote maintenance interfaces within these control systems has surged, consequently expanding vulnerability exposure surfaces. Traditional vulnerability management primarily relies on manual records, periodic scans, and post-incident patch applications, failing to effectively track asset changes or evolve vulnerability risks. This study investigates management requirements for equipment and software in oil and gas pipeline industrial control networks, establishes a research framework for real-time vulnerability monitoring platforms, and analyzes core components such as asset discovery, dynamic topology analysis, vulnerability data synchronization, behavioral analysis, risk assessment, and closed-loop response mechanisms. It proposes technical implementation pathways and management safeguards for platform development, aiming to provide actionable insights for enhancing cybersecurity protection in oil and gas pipeline networks.

Keywords

oil and gas pipeline networks; industrial control networks; software management; real-time vulnerability monitoring; risk response

基于油气管网工业控制网络的设备与软件管理实时漏洞监控平台研究

滕学睿[1] 郑楚凡[2] 冯明忠[3]

1. 国家管网集团天津液化天然气有限责任公司，中国 · 天津 300452
2. 国家管网集团北方管道有限责任公司北京输油气分公司，中国 · 河北 廊坊 065000
3. 凯特智能控制技术有限公司，中国 · 山东 潍坊 261021

摘　要

油气管网属于能源输送模式内比较重要的基础设施，其工业控制网络肩负着站场监控、阀室调度、压力调节、泄漏监测、远程联动等关键工作。伴随数字化、网络化、智能化技术持续被应用，油气管网工业控制系统里的设备、软件、通信协议、远程运维接口数量日益增多，相应地漏洞暴露面也在不断扩大。传统的漏洞管理大多依靠人工台账、周期扫描、事后补丁修复，很难及时呈现资产变化、漏洞风险的演化情况。本文针对油气管网工业控制网络设备与软件管理需求展开研究，建立实时漏洞监控平台的研究框架，对资产发现、动态拓扑、漏洞数据同步、行为分析、风险评估、闭环响应等核心内容予以分析，提出平台建设的技术路径、管理保障措施，希望能够为油气管网网络安全防护提供一定的参考。

关键词

油气管网；工业控制网络；软件管理；实时漏洞监控；风险响应

1 绪论

1.1 研究背景

油气管网有着线路延伸距离长、站场数量众多、设备分布比较分散、连续运行有着较高要求这样的特性，是确保能源能够实现稳定供应的关键支撑。近些年来，工业控制网络于油气管网中的应用呈现出不断深入发展的趋势，SCADA 系统、PLC、RTU、DCS、HMI、工业交换机、边界安全设备、各类专业软件共同营造出了复杂的控制环境。这些设备、软件提高管网调度的效率，同时也让网络安全风

【作者简介】滕学睿（1998–），男，中国黑龙江大庆人，硕士，助理工程师，从事安全环保管理研究。

险从传统的信息系统扩展到了生产控制现场。一旦工业控制设备或者管理软件存在着尚未修复的漏洞，那么攻击者便有可能借助远程访问、弱口令、协议缺陷、补丁滞后或者供应链方面的问题进入到控制网络，进而对数据采集、阀门控制、报警联动、调度决策产生影响。油气管网要实现安全运行，这就要求漏洞管理从静态备案转变为实时监测，从单点处置转变为平台化协同。

1.2 研究目的

本文致力于建立一个适用于油气管网工业控制网络的设备与软件管理实时漏洞监控平台理论架构。此平台把资产识别当作基础，凭借漏洞数据同步给予支持，将风险评估与闭环处置作为核心部分，去处理工业控制网络里资产信息不全、软件版本不明、漏洞更新迟缓、补丁适配麻烦、处置过程无法追溯等一系列问题。研究的重点涵盖自动化资产发现机制、动态拓扑管理办法、漏洞库与厂商通告同步形式、风险分级模型、异常流量识别、补丁响应流程。借助对这些方面的系统设计，可以提高油气管网工业控制网络针对设备和软件漏洞的感知水平，促使漏洞监控从人工经验判断朝着数据驱动、连续管控的方向转变。

1.3 研究意义

油气管网的工业控制网络和一般办公网络不一样，其设备运行所处的环境比较复杂，而且停机窗口时间有限，部分控制设备的生命周期比较长，在进行补丁安装的时候要同时考虑安全性、稳定性、生产连续性这几个方面。建立实时漏洞监控平台，能够帮助形成完整的资产画像，能够及时了解设备类型、软件版本、通信关系、暴露端口等情况，防止因为资产信息不明确而致使风险失去控制。借助标准化的漏洞描述、动态数据同步，该平台可以把 CVE、CWE、CVSS、厂商安全通告和本地资产信息联系起来，让漏洞风险判断变得更加具体。对这个平台展开研究，也有助于完善工业控制网络安全管理办法，为油气管网、电力、交通、水务等关键基础设施的漏洞监控提供有参考价值的思路。

2 理论基础与研究现状

2.1 工业控制网络资产管理理论

工业控制网络资产包括现场控制设备、上位监控系统、工程师站、历史数据库服务器、通信设备、安全设备、工控协议服务、专用软件等。资产管理不能仅停留在名称登记方面，还需要掌握物理位置、逻辑位置、系统版本、开放端口、通信关系、业务功能、责任主体。在油气管网场景里，资产分布于调控中心、站场、阀室、边缘监测点，设备型号多样、协议复杂、运行周期长，人工台账难、时体现设备更换、软件升级、临时接入状况。实时漏洞监控平台应以自动化发现作为基础，结合被动流量识别、主动安全探测、人工校核，形成动态资产库，为漏洞匹配和风险判断给予支撑。

2.2 漏洞监控与风险评估理论

漏洞监控的关键要点在于识别出资产里有可能被利用的安全缺陷，然后依据风险程度来确定处置的优先级。仅仅凭借漏洞评分是很难反映出油气管网的真实风险状况的，这是因为同一个漏洞要是出现在办公终端、站场控制设备上，其产生的影响范围、处置要求是不一样的。平台需要在标准化的漏洞描述基础之上，把业务重要性、网络分区、访问路径、补丁可用性、运行负荷、安全冗余等诸多因素加以综合考虑，从而建立起适合工业控制环境的风险评估模型。像调度主站、远程终端单元、阀门控制设备、实时数据库、边界通信设备等关键资产，应该设定更高的风险权重，这样一来评估结果就能为告警排序、整改决策、补偿防护提供支持与服务。

2.3 国内外相关研究现状

如今工业控制网络安全研究已经从边界防护逐渐朝着资产可视、漏洞治理、异常检测、持续监测的方向转变。自动化资产发现工具能够识别 IP 地址、端口、协议、设备指纹，漏洞扫描工具可以将软件版本与漏洞库进行比对，流量分析和行为建模技术则能够帮助发现异常访问、异常命令、潜在攻击行为。油气管网场景对这些相关技术提出了更高的要求，主动扫描有可能会影响老旧工控设备的稳定性，补丁安装也有可能引发控制软件的兼容问题，异常检测还需要理解工艺流程、通信周期。现有研究在通用漏洞管理方面比较成熟，然而面向油气管网的设备与软件一体化实时监控仍有待进一步深入。

3 平台总体设计思路与架构

3.1 平台设计原则

设计油气管网工业控制网络实时漏洞监控平台时，需要遵循安全可控、低扰动运行、分区分级、持续更新、闭环管理的原则。对于安全可控原则而言，平台在采集、分析、响应过程中，不能对生产控制稳定性造成影响，所有扫描策略、插件加载、补丁建议都要经过适配验证。在低扰动运行方面，平台要依据资产类型来选择不同的监测方式，对于核心控制设备，更多地运用被动识别和日志分析，对于非实时业务设备，可适度采用主动探测。分区分级原则要求平台依照调控中心、站场控制区、生产管理区、边界接入区、办公区来实施差异化管理。持续更新原则意味着漏洞库、资产库、软件清单和补丁信息要保持动态同步。闭环管理原则要求告警、派单、处置、复核、归档形成完整的链条，以此避免漏洞长期停留在发现方面。

3.2 平台总体架构

平台能够被划分成资产感知层、数据治理层、漏洞分析层、风险决策层、闭环响应层这几个部分。资产感知层的职责在于针对网络资产、软件版本、通信关系、端口服务、日志信息、流量特征展开采集工作。数据治理层需要达成数据清洗、格式转换、资产去重、字段标准化、拓扑关系整理等各项任务。漏洞分析层会把资产信息同漏洞库、厂商通告、补丁信息、威胁情报进行关联匹配。风险决策层依据漏洞评

分、资产重要性、网络暴露面、利用迹象形成风险等级。闭环响应层负责告警推送、工单派发、补丁建议、隔离措施、复核确认、报告输出等相关事宜。各层之间不但维持着功能边界，还借助统一数据模型达成联动，从而使得平台能够从资产识别一直延伸到风险治理的整个过程。

3.3 数据流与业务流程

平台的运行流程主要包括资产入库、状态更新、漏洞匹配、风险研判、响应处置、结果复核这几个环节。在资产入库阶段的时候，平台借助自动发现、人工校验的方式来形成初始资产清单。进入状态更新阶段，系统会持续地采集设备变更、软件版本的变化、通信关系的变化情况。到了漏洞匹配阶段，平台依据设备型号、操作系统、软件组件还有固件版本等来比对漏洞数据。在风险研判阶段，会结合控制系统分区、资产业务影响、攻击路径从而形成风险等级。响应处置阶段，系统会向责任部门推送整改工单，同时还会提供补丁、配置加固、访问控制或者隔离等方面的建议。而结果复核阶段，则是通过复测、日志验证、人工确认来判断风险是否已经消除。此流程能够有效减少漏洞管理过程当中的信息断点，并提高处置的可追溯性。

4 核心技术分析

4.1 自动化资产发现与动态拓扑整理

实时漏洞监控得以进行的前提在于精准把握资产状况。平台需要综合运用主动探测、被动流量识别、设备指纹库、人工确认机制，针对工业控制网络里的设备与软件实施分层识别。对于一般服务器、工程师站、边界设备而言，能够借助低频、低强度扫描来获取端口、服务、版本信息，而对于 PLC、RTU、老旧工控终端，则应以被动监听、日志接入和配置导入作为主要方式，防止扫描干扰。动态拓扑整理要留意设备之间的通信方向、协议类型、访问频率、业务关系，建立起从调控中心到站场、从服务器到控制终端、从边界设备到远程维护接口的关系图谱。当资产出现新增、下线或者通信关系发生变化时，平台会自动标记变更并触发复核，避免未知设备长时间存在于控制网络之中。

4.2 设备与软件清单精细化管理

油气管网漏洞监控时，不能仅仅局限于识别设备的 IP 地址，还需要建立设备与软件的精细化清单。设备清单所涵盖的内容有资产编号、设备类型、厂商所生产的型号、设备的安装位置、所属的站场、所在的网络区域、责任单位、重要等级。软件清单包括操作系统、数据库、中间件、监控软件、组态软件、防病毒软件、固件版本、驱动组件、第三方库。对于工控设备而言，固件版本、工程配置同样具备安全方面的意义。平台可通过自动采集、配置导入、人工维护相结合的方式，形成设备与软件之间的对应关系。清单的精细化能够提高漏洞匹配的准确度，降低同一漏洞出现误报、漏报、重复告警的情况。对于那些无法自动识别的软件组件，应当设置人工确认流程，并且在后续维护过程中完善指纹库。

4.3 漏洞数据统一描述与同步机制

漏洞数据的来源比较多样，包括标准化漏洞库、厂商安全通告、补丁发布说明、威胁情报、内部安全测试结果等。平台需要运用统一字段去描述漏洞编号、漏洞名称、影响产品、受影响版本、利用条件、严重程度、修复建议、补丁链接、替代缓解措施等方面。CVE 能够用作漏洞的唯一标识，CWE 可以进行弱点类型的归类，CVSS 用于基础严重度评价，不过平台还得结合油气管网业务场景来展开二次评估工作。漏洞数据同步机制应当对定时更新、增量更新、人工审核给予支持，防止漏洞信息长时间处于滞后状态。针对厂商尚未发布补丁的漏洞，平台要记录临时缓解措施，例如关闭非必要服务、调整访问控制、强化边界隔离、加强日志监测等，以此确保风险处置能够持续连贯。

4.4 流量行为分析与异常检测

油气管网工业控制网络通信具备一定的周期性、业务规律，流量行为分析能够填补已知漏洞匹配方面存在的不足。该平台能够借助深度包检测、协议解析、流量基线建模、异常行为识别，找出异常访问、异常命令、横向扫描、暴力认证、远程控制尝试还有非授权配置变更等情况。在正常生产周期当中，SCADA 主站与现场设备之间的访问关系、通信频率、指令类型相对稳定，要是出现非常规地址访问、异常端口连接或者控制命令频繁变动的状况，那么就应当纳入风险告警范围。行为分析不能脱离工艺实际情况，需要和调度计划、检修作业、远程维护申请、设备调试记录进行关联，防止把正常运维误判为攻击行为。通过将已知漏洞数据与未知异常行为相结合，该平台能够提高风险发现的完整性。

5 漏洞响应与闭环管理机制

5.1 风险分级与处置优先级

当平台察觉到漏洞之后，需要依据漏洞的严重程度、资产的重要性、网络的暴露程度、利用的迹象、业务所受到的影响来展开综合分级操作。针对处于边界接入区域、远程运维通道或者核心控制链路之上的高危漏洞，应当优先予以处理，针对已经被公开利用并且对关键资产产生影响的漏洞，要立刻启动应急响应举措，对于低风险、无法远程利用或者具备边界隔离保护的漏洞，可以纳入到计划整改范围内。风险分级工作不能仅仅凭借分数的高低来判断，还得体现出油气管网运行的特点。有一些设备尽管漏洞评分并非很高，但是倘若处于阀门控制、压力调节或者站场通信的关键位置，依旧需要提高处置的优先级。借助分级管理的方式，平台能够帮助企业把有限的安全资源运用到最为关键的风险上，防止因为告警大量堆积而致使管理失效。

5.2 补丁管理与替代性防护

工业控制网络的补丁管理存在特殊性，无法直接套用办公网络那种快速更新的方式。油气管网的控制设备、专业

软件对稳定性有着较高要求，在安装补丁之前，必须完成兼容性验证、备份恢复相关工作、制定回退方案、安排好窗口期。平台需要记录补丁的来源、适用版本、影响范围、测试结果、实施状态，以此形成能够进行追溯的管理。对于当下暂时无法打补丁的设备，应当提供一些替代性的防护措施，像是关闭不必要的端口、限制访问来源、强化防火墙策略、部署虚拟补丁、增强身份认证、提高日志审计的频率。补丁管理与生产运维之间要建立协同流程，安全部门提出风险方面的要求，生产部门对实施窗口进行评估，运维部门执行变更操作，平台负责跟踪并实现闭环。

5.3 告警派单与整改复核

实时漏洞监控平台需要把告警转变成为能够执行的任务。系统能够依据资产责任的归属、风险的等级自动生成整改工单，清晰地明确漏洞信息、受到影响的资产、处置建议、责任单位、完成的时限、复核的方式。责任人员完成处置工作之后，要上传补丁安装的记录、配置的截图、复测的结果或者风险接受的说明。复核的环节要通过平台自动验证与人工确认相结合的方式来完成，以此保证漏洞状态有真实的变化。对于那些没有按照期限进行处置的高风险漏洞，要自动升级提醒并且纳入到安全考核之中。对于反复出现的同一类漏洞，要展开原因的分析，判断是不是存在版本管理混乱、补丁流程不通畅或者资产台账不真实等管理方面的问题。闭环管理可以推动漏洞治理从“发现风险”朝着“消除风险”的方向发展。

6 平台运行保障与优化建议

6.1 完善组织协同机制

油气管网工业控制网络漏洞治理牵涉到信息安全、生产调度、自动化、设备管理、通信运维、软件厂商、现场站队等多个方面的主体。平台建立完成之后，各部门在资产维护、漏洞确认、补丁测试、整改实施、应急响应等方面的职责需要予以明确。安全部门的任务是负责漏洞监控规则制定、风险评估工作，自动化部门承担控制系统技术确认的职责，生产部门要做好停运窗口协调的事宜，设备管理部门负责现场处置的配合工作，厂商负责补丁、兼容性支持方面的事务。多个部门协同合作能够降低漏洞整改过程中的推诿现象、等待时间。针对关键漏洞，应当建立会商机制，全面判断风险、生产影响、处置路径，确保安全防护与连续运行之间维持平衡状态。

6.2 强化数据质量和安全防护

平台自身需处理众多资产信息、漏洞数据、拓扑关系、安全告警，故而必须拥有严格的数据治理、安全防护能力。在数据质量方面，应当统一资产编码、软件命名、漏洞字段、网络区域、风险等级标准，以此来减少因名称不一致而导致的误匹配情况发生。在数据安全方面，平台要实施最小权限、强身份认证、日志审计、备份恢复、加密传输等措施，从而防止监控平台自身成为新的攻击入口。对于采集探针、扫描节点和管理接口需进行安全加固操作，并且限制其访问范围。在平台运行过程中，还应当定期评估误报率、漏报率、处置时效、工单关闭质量，通过调整识别规则和业务流程来实现更好的运行效果。

6.3 推动平台持续迭代

油气管网工业控制网络环境一直处于不断变化的状态，新增加的设备、软件进行升级、网络进行改造、远程运维需求等，这些情况都会对漏洞风险状态造成改变。平台开发不应该追求一次性就完成，而是要建立起持续迭代的机制。在早期建设的时候，可以着重去解决资产清单、漏洞匹配、工单闭环等方面的问题，当运行稳定之后，再循序渐进地增强行为分析、攻击路径推演、风险预测、智能化处置建议等方面的能力。平台还能够结合历史漏洞数据、设备故障数据、安全事件记录，去训练出更加契合油气管网场景的风险模型。持续迭代能够让平台更好地适应业务变化，防止系统上线之后因为规则陈旧、数据失真、使用复杂等情况而使得价值降低。

7 理论意义与未来展望

7.1 理论意义

本文聚焦于油气管网工业控制网络设备、软件管理的需求，建立了实时漏洞监控平台的研究框架，具备一定的理论意义。该框架把资产发现、软件清单、漏洞同步、风险评估、行为分析、闭环处置整合至同一逻辑脉络之中，解决了传统漏洞管理里资产、漏洞、整改相互分离的问题。研究着重关注工业控制网络的低扰动监测、业务影响评估、替代性防护，展现出了油气管网连续生产环境下安全治理的特性。借助设备与软件一体化管理，平台能够把抽象的漏洞转变为具体的资产风险，将静态台账转变为动态拓扑，把单次扫描转变为持续监控，为关键基础设施工业控制网络的漏洞治理提供了一套系统的思路。

7.2 未来展望

未来油气管网工业控制网络漏洞监控会朝着智能化、自动化、协同化的方向去发展。伴随人工智能、知识图谱、威胁情报技术趋于成熟，平台能够进一步达成漏洞影响路径的推演、攻击行为的预测、整改方案的智能推荐。针对那些无法频繁打补丁的工控设备，可以去探索虚拟补丁、零信任访问控制、自适应隔离策略，以此来提高风险缓解能力。平台还能够与安全运营中心、应急指挥系统、生产调度系统进行联动，达成安全告警、生产影响、应急处置之间的信息贯通。技术升级不应削弱人工审核与现场验证，油气管网安全治理依旧要依靠制度、人员、流程、平台共同发挥作用。经由不断完善实时漏洞监控模式，油气管网工业控制网络的安全韧性、运行可靠性将会进一步得到提高。

参考文献

[1] 牛煜荣,孙铁良,李立,等.油气管网控制系统网络动态检测技术研

究与实现[J].信息安全与通信保密,2025,(8):73-81.

[2] 邓勇,李旺,陈小华,等.油气管网工业控制系统多维安全测试平台建设[J].仪器仪表标准化与计量,2026,(3):4-6.

[3] 李亚锋,闫峰,王云鹏,等.油气管网工业控制系统网络安全[C]//中国网络空间安全协会人工智能安全治理专委会.2024世界智能产业博览会人工智能安全治理主题论坛论文集.[出版者不详],2024:126-129.

[4] 李晓鹏,耿汉轩,吕坤朋.极端工况下油气管网瞬态压力化工控制技术研究[J].化学工程与装备,2026,(6):81-83+90.

[5] 王泽煜,张根才,赵振飞,等.智慧管网下输气管道分输控制技术发展的认识与思考[J].石油化工自动化,2024,60(5):1-10.

[6] R. M Y S D ,A. A F A ,Lucas S , et al.Computer Vision Based Path Following for Autonomous Unammed Aerial Systems in Unburied Pipeline Onshore Inspection[J].Drones,2022,6(12):410-410.

[7] Basha N S ,Watit B ,Rao S P , et al.Recurrent neural network-based model for estimating the life condition of a dry gas pipeline[J].Process Safety and Environmental Protection,2022,164639-650.

[8] Hui Q ,Liu B ,Fan J , et al.Knowledge graph construction for pipeline standards: Enhancing efficiency in the oil and gas industry[J].Journal of Pipeline Science and Engineering,2026,6(4):100445-100445.

[9] Chibani B E M ,Bouyaya L ,Zellagui R , et al.Pipephase 9.6 Simulation-Based Assessment of an LPG Transport Network's Resilience in the Event of an Unexpected Pumping Station Shutdown[J].Materials Circular Economy,2026,8(1):30-30.

[10] Safran A E ,Shaaban O .Prediction of slug length distribution in horizontal large-diameter gas/liquid pipeline systems[J].Geoenergy Science and Engineering,2024,240212985-.