石油天然气行业物流运输的通信网络安全加固研究

王新啸（国家管网集团西气东输公司南京计量研究中心，江苏　南京　210000）

摘　要：本文针对石油天然气行业物流运输体系中通信网络的网络安全问题进行了深入探讨。鉴于该行业在全球能源供应中的战略地位及其物流运输环节的特殊性和复杂性，文章强调通信网络的关键支撑作用，剖析现有通信网络架构、安全防护措施及存在的安全隐患。并提出针对不同运输方式和设施的网络安全加固策略，整合一系列通用的网络安全技术和管理措施以提升整体防护水平。最后，总结了构建全面、高效、智能的物流运输通信网络安全体系的必要性和可行性。

关键词：石油天然气行业；物流运输；通信网络；网络安全；加固策略

石油天然气行业的物流运输是连接勘探开采、加工、储存与消费市场的关键环节，其高效稳定的运行直接影响着全球经济秩序和社会能源供给安全。由于涉及大量敏感信息和关键基础设施，该体系具有高度复杂性、连续性和安全性要求极高的特点。现代石油天然气物流运输业已深度依赖于实时通信网络，实现从资源调度、设备监控到危机管理等全过程的信息化管控。通信网络的正常运作不仅有助于提升运输效率，更是在预防安全事故、抵御外部攻击和保护核心数据方面发挥着至关重要的作用。

1 石油天然气行业物流运输通信网络现状与问题

1.1 物流运输通信网络架构概述

当前的石油天然气行业物流运输通信网络是一个高度集成且复杂的体系，它融合了物联网 (IoT)、移动通信、卫星通信等多种先进通信技术，形成一个纵横交错的混合型网络架构。此网络贯穿从油气田井口的资源采集、经过炼制厂的加工处理，再到长距离的管道或陆海运输直至最终的分销终端用户全过程的数据传输与控制链条。

物联网技术通过嵌入式传感器和智能设备收集海量实时数据，包括但不限于温度、压力、流量等关键参数，用于监控和优化运输过程。移动通信技术则支持远程操作、实时跟踪和紧急响应，尤其在偏远地区或海上平台的作业中起着关键作用。卫星通信则因其覆盖范围广、不受地理限制的优势，保证了长途运输线路上通信的连续性和可靠性。

然而，这种多层互联的网络结构也带来巨大的安全挑战，尤其是在维护数据完整性、保护关键基础设施免受恶意攻击等方面，需要特别关注。

1.2 当前网络安全防护措施与存在的薄弱环节

尽管石油天然气行业在网络安全方面投入了大量资源，采用了诸如入侵检测系统（IDS）、防火墙、身份认证与访问控制等基础防护措施，但现实情况表明，该领域仍存在诸多亟待解决的安全隐患。

部分企业的信息系统可能存在老化问题，老旧的操作系统和应用程序如果没有得到及时的升级和补丁更新，就容易成为黑客攻击的突破口。特别是针对工业控制系统（ICS）和 SCADA 系统的安全漏洞，由于其固有的稳定性和长期在线运行特性，往往难以快速适应新的安全标准和修复方案。

物联网设备的安全性成为了明显的短板。许多物联网设备在设计之初并未充分考虑安全性，缺乏足够的安全防护功能，如弱密码策略、未加密的通信信道等，使得它们易于被恶意操控。此外，数据加密程度不足也是普遍存在的问题，无论是传输中的数据还是存储的数据，都可能因为加密强度不够而面临窃取和篡改的风险。

1.3 物流运输环节典型网络安全威胁

面对如此复杂的通信网络环境，石油天然气行业的物流运输环节面临的网络安全威胁呈现出多样化且严重的态势。以下是一些主要的网络安全威胁类型：

黑客攻击：高级持续性威胁 (Advanced Persistent Threats, APT) 和其他类型的黑客攻击可针对关键系统的弱点进行渗透，获取敏感信息，甚至直接控制运输和生产设施。

恶意软件植入：恶意软件可以通过电子邮件、网页链接、软件更新等方式潜入系统，一旦成功植入，可以破坏数据、瘫痪网络或悄悄搜集敏感信息。

中间人攻击：在网络通信过程中，黑客通过拦截并篡改传输数据，进行欺诈活动或窃取机密信息，尤其是在没有使用端到端加密的通信路径上尤为常见。

拒绝服务攻击（Denial of Service, DoS 或 Distributed

Denial of Service, DDoS）：此类攻击旨在让目标网络或系统无法正常提供服务，可能导致油气运输监控系统的中断，进而影响到整个供应链的正常运转。

这些攻击可能导致石油天然气运输过程中的生产中断，还会引发数据泄露事件，严重时甚至危及到物理设施的安全，对企业和国家经济造成重大损失。因此，对石油天然气行业物流运输通信网络进行全面有效的网络安全加固至关重要。

2 石油天然气行业物流运输通信网络安全加固策略

2.1 特定运输方式的通信网络安全加固

在石油天然气行业，由于其物流运输方式多样，涉及长途海运、陆地卡车运输和铁路运输等多种形式，不同运输方式对通信网络的安全需求有着显著差异。因此，在强化安全设计时，必须根据不同运输环境的具体条件和特点进行针对性的灵活优化。

针对海运运输方面，鉴于海洋环境的广阔覆盖范围和复杂的信号传输特性，通信系统的安全性能尤其关键。为了保障海上运输环节的信息安全，首要任务是对海事卫星通信系统实施高规格的加密升级。这一过程中，采用业界公认的安全级别较高的加密算法，如 AES-256 标准或者符合相关行业规定和国际标准的其他加密技术，有助于确保传输数据无法轻易被破解。同时，构建并维护一套高效的密钥管理系统至关重要，这套系统能在远距离无线通信过程中保证数据始终处于严密的加密状态，维持其私密性和完整性不受侵犯。

此外，严格执行接入控制策略是另一项重要的安全举措。这意味着只有预先经过授权的设备才能够成功接入通信网络，避免非授权设备带来的潜在安全风险。结合数据完整性校验机制，可以有效地阻止未经授权的访问行为，并及时发现并防止数据在传输过程中遭受非法篡改。

至于陆地运输，尤其是在卡车运输和铁路运输这两种主要陆上物流方式上，信息安全同样面临着严峻考验。解决之道在于部署虚拟专用网（VPN）技术，借助 VPN 技术能够在公共互联网环境中构建起一条安全隧道，利用隧道加密技术对私有数据进行封装和保护。在此基础上，实行多重身份认证机制，确保只有经过层层审核并持有有效权限的实体才能访问到敏感信息，或是参与到信息交换的过程中。通过这些精细化的访问控制策略，大幅降低了数据在公开网络上传输时被盗取或恶意篡改的风险，有力保障整个陆地运输链路上的信息安全。

2.2 油气储运、天然气管道输送网络安全加固

在油气储运和天然气管道输送这两个至关重要的环节中，网络安全加固工作要求强化物理设施的安全性，提升监控系统的智能化水平和数据安全等级。具体措施如下：

实时监测与智能预警：引入前沿的泄漏监测与定位技术是预防管道安全事故的重要手段。例如，分布式光纤传感技术能够通过感知温度、应力等细微变化来实时监测管道沿线的状态，一旦发生泄漏，系统能够立即发出警报并精确定位泄漏点，确保及时响应和处理。声波探测技术则通过捕捉和分析管道内流体流动产生的声学特征，辅助识别可能存在的异常情况。

数据完整性与可靠性：利用区块链技术搭建数据管理和共享平台，能极大地提升数据记录的透明度、可追溯性和不可篡改性。每一笔交易、每一次状态变更都会被记录在区块链上形成共识，这增强了数据的真实性和可靠性，还为上下游企业间的数据交换提供了安全可信的基础，有利于全产业链协同合作和风险管理。

工业控制系统安全强化：对于负责管道自动化监控和操作的 SCADA（Supervisory Control And Data Acquisition）等工业控制系统，安全加固尤为迫切。首先，要增强操作系统及其应用程序的安全配置，采用最新的安全补丁和最严格的访问控制策略；其次，部署专门适用于工业环境的防火墙设备，以抵御各类网络攻击和非法入侵。同时，建立定期的安全评估与漏洞扫描机制，对整个工业控制系统进行全面体检，及时发现并修复潜在的安全漏洞，防止恶意软件或黑客入侵。确保系统在面临内外部威胁时，仍能保持稳定运行，降低因网络攻击导致的生产中断或环境污染风险。

2.3 石油仓储、石油储罐网络安全加固

在强化石油仓储、石油储罐的网络安全方面，核心目标是对现场传感器网络进行全面安全保障，这些传感器肩负着实时采集与传输储罐内部诸如温度、压力、液位等关键运行指标的任务。为此，应采取多层次防御体系，首先通过物理隔离手段将关键生产设备与常规办公网络进行有效隔断，降低遭受横向攻击的风险，确保生产网络独立稳定且安全运行。其次，根据功能特性和安全级别要求，科学合理地将仓储区域划分为多个逻辑子网，实行精细化的分区分级管理模式，保证不同安全等级信息流的有序和受控传播。最

后，借助智能监控系统的部署，实时监控并深入分析各类设备的运行状态，一旦检测到异常状况，即刻触发报警系统并联动自动化响应机制，以期在第一时间预防由网络安全事件可能引发的物理安全隐患，确保整个石油仓储设施的运行安全。

2.4 输送管道网络安全加固

对于输送管道沿线的通信设备，强化设备的管理和维护工作至关重要，应定期进行安全审计和性能测试，确保所有通信节点的软件版本保持最新，及时消除已知的安全漏洞。采用最先进的管道安全监控系统，不仅能实时监测管道的各项运行参数，如压力、温度等，还能有效检测网络通信链路的安全状态，自动识别并报告异常流量和潜在的网络攻击行为。此外，还应确保数据采集设备、传输通道和数据处理中心均达到必要的安全防护标准，采用可靠的加密技术对从管道采集的数据进行实时加密传输，确保数据从产生至目的地全程安全。同时，建立健全网络安全事件应急响应机制，确保在遭遇安全事件时能够迅速、高效应对，最大限度降低安全事件对管道运输安全的影响。

3 通用网络安全加固措施与技术应用

3.1 建立健全物流运输通信网络安全管理体系

为了确保石油天然气行业物流运输通信网络的安全，首要任务是建立一套健全且行之有效的网络安全管理体系。这包括从顶层规划开始，明确网络安全战略目标，制定详细的网络安全政策和操作流程，并将其贯彻执行。具体而言，企业需要构建涵盖网络规划、建设、运行、维护和退役全生命周期的网络安全管理框架，明确各个阶段的安全责任，落实责任人制度，确保每一环节都有相应的安全管理措施予以保障。

3.2 强化边界防护与访问控制

强化边界防护是网络安全的核心要素之一，企业应通过部署现代化的防火墙、入侵防御系统（IPS）以及其他先进的网络边防技术，形成严密的防护屏障。在此基础上，实施细粒度的身份验证和授权管理机制，确保只有合法的用户和设备才能获得网络访问权限。对外部访问，应设立严格的访问控制列表，对内部访问，则应按照最小权限原则分配访问权限，严防非法侵入和越权操作。

3.3 加强数据保护与隐私保护

数据安全是石油天然气行业物流运输通信网络的命脉，为此，应采用国际公认的 SSL/TLS 协议进行加密通信，确保数据在传输过程中不会被窃听或篡改。同时，推行数据脱敏技术，对敏感信息进行去标识化处理，降低数据泄露带来的潜在风险。此外，制定全面的数据备份与恢复策略，定期进行数据备份并确保备份数据的可用性，在发生意外事故时能快速恢复业务运行，保持数据的完整性。

3.4 提升网络设备与系统的安全防护能力

持续提高网络设备与系统的安全防护水平是必不可少的步骤。企业应定期检查并及时更新各类软硬件的补丁，修补已知的安全漏洞，防止攻击者利用旧版软件的弱点发起攻击。采用零信任模型，即使在内部网络环境中，也不默认任何设备或用户为可信，而是通过对每一次请求进行动态验证来保障安全性。此外，部署反病毒软件和反恶意软件系统，实时监控和阻止各类恶意代码的传播，有效防范系统级别的安全风险。

3.5 构建全面的监测、预警与应急响应体系

构建一体化的态势感知平台，整合各类安全日志和威胁情报，实时监测网络中的异常行为和潜在威胁。基于历史数据和威胁情报库，预先设定一系列有针对性的预警规则，当检测到可疑活动时，能即时发出警告。与此同时，建立一套完整的网络安全应急响应预案，包括详尽的应急处置流程、团队组织架构、技术支持资源调配等内容，并定期组织实战演练，确保在实际遭受网络攻击时，能够迅速、准确、高效地做出反应，最大程度地减轻攻击所带来的损害。

4 结论

石油天然气行业物流运输通信网络的网络安全加固是一项系统工程，需要整合技术、管理和政策层面的多种手段，通过持续改进和完善，方能在日益严峻的网络环境下保障这一关键基础设施的安全运行。随着新兴技术的发展，未来还应积极探索和实践人工智能、机器学习等先进技术在网络安全防护领域的创新应用。

参考文献：

[1] 戴绘 . 燃气企业信息化网络的安全加固实践 [J]. 天津科技 ,2023,50(02):20-23+30.

[2] 杨维 . 浅析局域网系统的网络安全加固策略 [J]. 西部广播电视 ,2021,42(S1):221-226.

作者简介：

王新啸（1989.08— ），男，汉族，江苏盐城人，身份证号：320982198908236713，学历：大专，职称：助理工程师，研究方向：天然气。