油气储运工控系统安全分析与管理策略探讨

兰　庆（中石油华东设计院有限公司吉林分院，吉林　吉林　132000）

摘　要：工业自动化和信息化系统是工业各行业、各企业的神经中枢，其中工控系统已经成为国家关键基础设施的重要组成部分。目前工控系统已广泛应用于油气储运等工业领域。近年来，随着油气储运信息化和工业化融合的不断深入，工控系统从单机走向互联，从封闭走向开放，从自动化走向智能化。在生产力显著提高的同时，工控系统面临着日益严峻的信息安全威胁。目前为止，油气储运行业工控网络缺少必要的安全防护措施，进而导致严峻的工控系统网络安全隐患，需要行业工作人员给予高度的重视，制定更加适合的控制和管理措施，在最大程度上避免造成严重的工控系统网络安全问题，规避工控系统运行瘫痪的情况。

关键词：油气储运；工业控制；系统网络安全；管理策略

在近些年中，油气储运行业的得到了充足发展，我国油气管网总长度已超过 16.5 万 km，如果油气管网受到“系统性”破坏，很可能会对国家安全造成严重危。工业控制系统作为油气储运行业关键组成，随着油气储运智能化水平的提升，工业控制系统突破信息孤岛，与传统信息网络之间数据交互愈发频繁。目前工控系统网络安全隐患越发严重，这就需要采用更多安全可靠的技术，依据实际需求采用行之有效的管理措施，从根本上确保油气储运行业工控系统在更为安全、稳定的环境中运行。相关工作人员需要具备前瞻性眼光，充分了解油气在存储、运输过程中工控网络安全隐患问题，并应用切实可行的管理方案，促进工控系统的有效运作。

1 油气储运工业控制系统概况

工业控制系统是一种广泛应用于油气储运行业的自动化控制系统，用于监控、管理和控制各种工业过程和装置。系统的主要任务是确保油气储运过程的高效性、可靠性和安全性。工业控制系统通常由硬件和软件组成，旨在自动执行任务，以减少人工干预并提高生产效率。这些系统通常包括传感器、执行器、控制器和监控界面。传感器用收检测油气储运过程中数据，如温度、压力、流量、液位、装置状态等，控制器根据这些数据采取相应措施，执行器则负责调整和控制各种设备，如阀门、电机和泵等。油化储运的工业控制系统主要包括数据采集和监控系统 SCADA、安全仪表系统 SIS、PLC（可编程逻辑控制器）等。这些系统通过定时任务、逻辑控制和反馈机制来确保工业过程的顺利运行。尽管工业控制系统在自动化控制、提高效率方面具有巨大潜力，但也面临一系列安全挑战 [1]。

2 油气储运工控系统中的网络安全隐患问题

2.1 安全区域边界问题

油气储运行业部分网络架构设计不合理，工控系统内部以及工业控制系统与企业其他系统之间没有独立的安全区域，涉及实时控制和数据传输的工业控制系统，没有使用独立的网络设备组网，在物理层面上没有实现与其他数据网及外部公共信息网的安全隔离，这意味着部分工控系统一旦发生网络攻击沦陷，容易导致横向渗透的风险。部分工作人员在工业主机上私自假设 VPN 或者安装远程访问软件，导致工控系统和互联网直接连接、通信。因此安全培训和意识教育是至关重要的 [2]。

2.2 拒绝服务攻击

工业控制系统中的网络安全隐患问题在拒绝服务攻击方面引发了严重的担忧。拒绝服务攻击是一种意图阻止合法用户访问或使用系统资源的攻击，它对工业控制系统的可用性和运行产生了严重威胁。工控系统通常依赖于实时性能，一旦遭受拒绝服务攻击，系统可能会变得不可用或失去对其控制的能力。这可能导致设备故障、输送中断和安全风险，甚至可能对环境产生负面影响。

此外，对工业控制网络的访问控制和监视通常较弱，使攻击者更容易找到和利用漏洞。为解决这一问题，首先需要加强油气储运企业对工业控制系统的网络安全意识和培训，组织应制定应急响应方案，以迅速应对拒绝服务攻击。此外，技术措施，如工业防火墙 / 工业网闸、入侵检测系统、工控流量检测系统，也可以降低拒绝服务攻击的风险。

2.3 遭受病毒攻击

所谓的病毒攻击指的是利用工控系统中存在的漏

洞，编写病毒代码后对系统中的某些驱动程序进行数字签名，对相关数据信息进行伪造处理，继而入侵到整个的工控制系统中，实现病毒的大面积传播。病毒攻击的隐患最大，伤害性最强，会产生极其恶劣的影响。病毒能够突破工控系统局域网的区域限制，对于系统的功能以及运行等都会造成极为严重的破坏。因此，在应对病毒攻击的时候需要给予重点关注，这是十分重要的工作环节，需要得到相关部门的重视，并且要依据实际情况采取积极有效的应对措施，切实降低病毒攻击的概率。

2.4 存在非法连接

油气储运行业工控系统中的网络安全问题涉及多个方面，其中存在非法连接是一项严峻的隐患。因为许多恶意行为试图通过非法连接来渗透、破坏或控制这些系统。工业控制系统网络通常设计用于实时控制和监视油气储运装置的运行过程，因此安全性可能不是首要关注点。这使得网络通信协议通常缺乏足够的加密和认证机制，使得攻击者可以更容易地建立恶意连接并窃取敏感数据或注入恶意命令。工业控制系统网络中的设备和控制系统通常长时间运行，且不经常更新，这导致系统容易受到已知漏洞的攻击。攻击者可以利用这些漏洞建立非法连接，然后控制或干扰运行过程。此外，由于制造商可能不再提供支持或更新，这使得工业控制系统难以升级，从而使网络更容易受到攻击。另一方面，人为因素也是恶意连接的隐患。内部或外部的不慎行为，如员工的疏忽大意、密码泄露或社会工程攻击，都可能导致攻击者成功建立恶意连接。这强调了培训和教育的重要性，以提高员工的网络安全意识。

2.5 安全运维风险

目前油气储运行业有大量的日常运维工作，涉及到生产调度，设备维护等日常工作，目前生产调度方面的运维监控主要依托生产系统自身的操作审计，对运维工程、运维记录缺乏有效的监测，事后无法进行运维过程追溯。缺乏运维审计技术措施，容易造成管理不到位和越权滥用的风险，一旦发生安全事件，无法追踪定位。

3 工业控制系统网络安全与管理策略

3.1 使用分区分层管理模式

对于油气储运行业工控系统网络实施全面性管理的时候，不仅要界定好互联网、企业办公网、工控网络，还要做好相对应分层、分区，严格依照功能的不同进行分区，继而可以使用不同的网络安全和管理技术实现多样化的安全防护。另外，工控系统中不同装置之间也要设置好访问权限，这样可以在最大程度上避免一套装置受到外来攻击后所有的装置因此沦陷，减少工控系统之间数据交互范围，能够将网络安全问题限定在可控的范围内，对于筛查安全问题也起到了极为重要的作用，实现对成本资金的有效控制和管理，管理工作的效率也能够因此提升。比如，油工控系统之间可以建立逻辑隔离区域、层次，确保工控系统与办公网络进行逻辑隔离，防止潜在的网络攻击与恶意程序的扩散。在工控系统内部，通过部署工业防火墙等措施进行区域划分，以限制通信范围，减少横向传播风险。还可以通过部署工业防火墙或相关技术手段进行工控系统分层。通过技术手段加强人员、设备的权限管理，只有经过授权的操作员站才能访问控制器，而操作员只能访问必要的界面。这种分级访问控制确保了只有有权限的人员才能执行关键操作，减少了潜在的内部威胁。通过技术手段实时检测工控系统流量，及时发现工控系统中存在的恶意流量以及非法操作，并定期进行漏洞扫描，以及实施紧急补丁和更新。这种分区分层分域的管理模式能够帮助维持工控系统安全，降低风险，确保了油气储运的稳定运行。

3.2 合理采用主动防御技术

由于现代科学技术不断发展创新，工作人员不仅要重视其所带来的便利性，更为重要的是关注其中潜在的安全问题，主动防御技术也因此应运而生，得到了良好的发展前景，并且可以在油气储运行业工控系统网络中实现了广泛应用。其中，白名单主动防御技术在日常工作中是最为常见的，此技术的应用原理是根据提前拟定好的协议规则来限制不同网络间的信息交互，并且能够实现对约定协议的分析，了解到端口限制方式，可以在根源上限制未知来源软件的安全和使用，继而加强了对于工业控制系统网络安全防护工作质量。如工程师 / 操作员在工作的时候应该使用注册后的 U 盘以及其他的存储设备，在使用工业主机的时候也要确定管理人身份信息，没有获得任何授权的行为都会被白名单防御系统所拒绝。比如，可以在油气储运企业程师站、操作员站上部署工业主机卫士，阻止非授权程序的运行、阻止非授权存储设备的接入，阻止存储设备数据的写入，加强主业主机的基线管理。

3.3 科学利用隔离技术

隔离技术（如工业网闸、光闸）是最早应用于油

气储运工控系统与办公网络间数据传输安全问题的技术，此技术的发明时间节点较早，在实际应用的时候具备较多的经验，相关工作人员在实际使用时候也较为熟练，在运用到实际工作中可以发挥出极大的作用。无论是在油气储运的调度中心、场站、油库，物理隔离技术都能够发挥出不可替代的作用，在多个部门中起到了关键性价值，具备较为优质的安全防护作用。物理隔离技术在工业控制系统网络中会采用“2+1”的模块结构，经过隔离单元实现对两个主机系统的联系，切实建立起安全的数据传输通道。

3.4 制定个性化工业防火墙软件

工业控制系统网络的使用可以通过防火墙软件制定不同形式的安全防护规则，实现对不同系统以及控制设备之间的数据控制。工业防火墙软件在使用的时候一定要充分建立在网络连通的前提下，经过对规则的更改和协议的分析，了解到管理过程中一些较为敏感和关键的信息，并对这些进行实现主动过滤或者限制，对于未经授权的内容应该设置好访问权限。工业控制系统而网络在建设期间如果需要使用多个防火墙，则应该使用不同品牌的防火墙软件，这是因为不同的软件设计思路 也存在较大的差异性，在进行联合运用的时候具备更强的安全性，对于外部攻击工作起到了较好的防护作用。比如，可以采用了多层防御策略，包括基于签名和行为分析的威胁检测，以及实时更新的病毒库，这保证了工业控制系统在不断演进的网络威胁面前具有强大的防护能力。

3.5 构造入侵预防网络系统

入侵预防系统简称为 IPS，这是一种较为先进的计算机网络安全防护系统，也能够对防火墙和白名单进行效用上的补充，起到更好的辅助作用。这项系统的使用可以对网络或者是相关设备中传输资料进行实时监视，对于传输期间出现的异常情况可以及时捕捉，如若发现存在攻击性的行为，网络资料传输过程会立即暂停，并做好中断和隔离工作，以此减少出现网络安全事故的几率。相较于工业防火墙以及白名单软件，入侵预防系统的功用更加侧重于做好前期预警工作，不需要网络管理者对其实施定期的维护处理，也不用随时进行更新，是一种相对有效的应对系统。比如，在设备层面采用工控设备固件的定期更新和漏洞修复策略，以防范已知的安全漏洞。另外，通过强化访问控制，确保只有授权人员可以访问关键设备，而且还实施了多因素身份验证，提高了系统的安全性。

3.6 建立统一安全管理中心

通过部署统一安全管理平台，作为工控系统网络安全管理中心。统一安全管理平台是针对工控系统网络的安全状态的感知，将安全防护设备（如网闸 / 工业防火墙、入侵监测、入侵防御、主机卫士等）发现的问题，实时传输给统一安全管理平台，有安全平台进行进一步分析，从而快速定位、通过对安全防护设备的策略调整，及时将恶行程序引发的问题控制在最小范围内。同时通过可视化技术，将威胁告警、异常行为告警、资产管理等数据结构化，实现集中可视化管理。

4 工业控制系统网络安全趋势展望

油气储运行业工控系统网络安全在未来呈现出一些重要的趋势和展望，工业设备更加互联和智能化。然而，这也将增加网络攻击的风险，因此工业控制系统的安全将更加关键。

其次，油气储运企业智能化不断提升。这将提供更大的灵活性和效率，但也需要更强大的网络安全措施，以保护工业控制系统。人工智能和机器学习将成为网络安全的强大工具。这些技术可以用于检测异常行为、实时威胁分析和自动化响应，有助于更快地应对威胁。

综上所述，油气储运行业工控系统网络安全的重要性愈发凸显，这一领域的分析与管理策略至关重要。随着信息技术的不断发展，工业控制系统面临着更多潜在的网络威胁和漏洞。本研究的目的在于深入探讨油气储运行业工控系统网络安全，为油气储运提供保护工控系统的有效策略，有效应对工控系统网络安全威胁。这就需要建立多层次的安全措施，并确保工作人员具备应对威胁的知识和技能。此外，持续监测和漏洞修复也是确保工业控制系统网络安全的不可或缺的一部分。工业控制系统网络安全需要全面的管理策略，包括风险评估、政策制定、技术部署和应急响应。这样可以建立健壮的工业控制系统网络安全体系，确保生产和运营的连续性，保护工控系统免受网络威胁的侵害。

参考文献：

[1] 牛书宁，梁佳伟 . 工业信息控制网络信息安全的防护措施 [J]. 价值工程 ,2022,41(31):48-51.

[2] 蒲永杰 . 工业控制系统网络安全防护措施的研究 [J]. 设备管理与维修 ,2022(21):114-115.