智能化煤矿工业控制系统网络安全分析及防护实践

王建华
平顶山中选自控系统有限公司　河南　平顶山　467000

摘　要：本文深度剖析了智能化煤矿工业控制系统的网络安全现状，揭示了系统建设、自身安全及新技术应用等维度的潜在风险。为应对这些挑战，本文提出构建多层次的纵深安全防御体系，并实施一系列关键防护措施，以增强系统的安全防护屏障。这些措施旨在显著提升煤矿工业控制系统的防御能力，确保煤炭生产在智能化进程中既安全又高效运行。

关键词：智能化煤矿；工业控制系统；网络安全；防护实践；纵深防御

引言：随着煤炭行业自动化、信息化、智能化的快速发展，煤矿工业控制系统在提升生产效率、保障生产安全方面发挥着越来越重要的作用。然而，与此同时，网络安全问题也日益凸显，成为制约煤矿智能化建设的重要因素。因此，对智能化煤矿工业控制系统的网络安全进行深入分析及防护实践具有重要意义。

1 智能化煤矿工业控制系统网络安全的重要性

1.1 保证生产稳定性

煤矿工业控制系统的安全性是确保生产连续性的基石。一旦系统遭受网络攻击，如病毒入侵、恶意软件植入或黑客控制等，可能导致系统瘫痪、指令错乱，进而引发生产中断。这种中断不仅会造成巨大的经济损失，还可能因设备停机而引发一系列安全隐患，如矿井通风不畅、瓦斯积聚等，严重威胁矿工的生命安全。因此，加强网络安全建设，防止外部威胁侵入，是保障生产稳定、避免灾难性后果的首要任务。

1.2 提升生产效率

智能化煤矿工业控制系统的网络安全同样至关重要。在智能化时代，系统通过实时数据采集、智能分析与优化调度，实现了生产过程的精细化管理和资源的高效利用[1]。然而这一切都建立在系统安全稳定运行的基础之上。如果系统频繁受到网络攻击或数据泄露的困扰，将严重影响其正常运行和数据分析的准确性，进而降低生产效率。因此，加强网络安全防护，确保系统稳定运行和数据安全传输，是提升煤炭生产效率、推动行业高质量发展的重要保障。

1.3 促进行业可持续发展

智能化煤矿工业控制系统的网络安全建设更是推动煤炭行业转型升级、实现可持续发展的关键一环。随着信息技术的飞速发展，煤炭行业正逐步向数字化、网络化、智能化方向迈进。然而，这一过程中也伴随着诸多网络安全挑战。只有不断加强网络安全建设，提升系统的安全防护能力，才能为煤炭行业的智能化转型提供坚实支撑，推动行业向更加安全、高效、绿色的方向发展。

2 智能化煤矿工业控制系统概述

智能化煤矿工业控制系统（如图1），作为现代煤炭开采技术的重要里程碑，正引领着煤炭行业向高效、安全、绿色的方向转型。这一系统集成了最尖端的自动化、信息化与智能化技术，不仅极大地提升了煤炭开采的效率与产量，还显著增强了作业安全性，降低了环境污染和能源消耗。

图1 智能化煤矿工业管理系统

2.1 数据采集与监控系统（SCADA）

SCADA系统作为智能化煤矿的“神经中枢”，负责实时采集煤矿生产现场的各种数据，包括但不限于矿井环境参数（如瓦斯浓度、温度、湿度、风速等）、设备运行状态（如皮带机、采煤机、提升机的电流、电压、转速等）以及生产进度信息。这些数据通过高精度传感器和智能终端设备采集后，经由通信网络传输至中央控制室，经过处理后以图形化、数值化或报警形式展示给操作人员和管理者。SCADA系统不仅能够实现对生产过程的远程监控，还能根据预设的算法自动调整生产参数，实现最优化的生产调度和安全管理。例如，在检测

到瓦斯浓度超标时，系统能立即触发报警并自动启动通风设备，有效预防安全事故的发生。

2.2 可编程逻辑控制器（PLC）

PLC作为智能化煤矿工业控制系统的“执行大脑”，扮演着控制设备动作、逻辑判断与决策执行的关键角色[2]。它接收来自SCADA系统的指令或根据预设的程序逻辑，直接控制煤矿生产中的各类机械设备。PLC具有强大的逻辑运算能力、丰富的输入输出接口以及高度的可靠性和稳定性，能够适应煤矿复杂多变的生产环境。通过编程，PLC可以实现复杂的控制策略，如根据煤层厚度自动调节采煤机的切割深度，根据运输需求优化皮带机的运行速度等，从而提高生产效率和资源利用率。此外，PLC还支持远程编程和维护，降低了现场维护难度和成本。

2.3 通信网络

通信网络是智能化煤矿工业控制系统的“血脉”，它负责各系统之间、设备之间以及人与系统之间的信息传输与交互。煤矿通信网络通常采用工业以太网、光纤通信、无线通讯等多种技术手段相结合，确保数据的实时性、准确性和安全性。随着5G、物联网（IoT）等先进技术的引入，煤矿通信网络正向着更高速率、更大容量、更低时延的方向发展。这不仅使得数据采集与监控更加全面和精细，还为实现设备间的无缝协同、远程故障诊断与维护等高级功能提供了可能。同时，通信网络的安全防护也日益受到重视，通过加密传输、身份认证等手段保障系统免受网络攻击和数据泄露的风险。

3 智能化煤矿工业控制系统网络安全分析

在智能化煤矿工业控制系统的网络安全领域，随着技术的飞速发展与广泛应用，其面临的威胁也日益复杂和多样化。

3.1 系统建设松散导致的安全防护能力不足

3.1.1 系统整合度低

煤矿企业往往拥有多个业务信息系统，这些系统建设时间不同，技术架构各异，导致系统间存在大量老旧系统、僵尸系统，难以实现高效整合。这种松散的系统建设模式不仅增加了管理难度，还使得整体安全防护能力大打折扣。例如，各系统间缺乏有效的信息共享和联动机制，当某一系统遭受攻击时，难以迅速在其他系统中采取防御措施，从而扩大了攻击范围。

3.1.2 防护手段单一

目前，许多煤矿企业在网络安全防护上采取的是“打补丁”的方式，缺乏系统性和前瞻性的规划。虽然部分系统安装了网络安全防护工具，但这些工具往往各自为战，缺乏统一的协调和管理。一旦发生网络安全事件，各防护工具难以形成合力，导致响应速度慢、处理效率低。

3.2 系统自身在设计、开发、部署等环节中的安全隐患

3.2.1 设计缺陷

在系统设计阶段，如果未能充分考虑网络安全因素，就可能留下安全隐患。例如，系统架构设计不合理，导致关键数据泄露风险增加；权限管理不严格，使得低权限用户能够访问高权限资源；缺乏必要的审计和监控机制，无法及时发现和应对安全事件。

3.2.2 开发漏洞

在软件开发过程中，由于编码不规范、测试不充分等原因，可能引入各种安全漏洞。这些漏洞一旦被攻击者利用，就可能对系统造成严重损害[3]。例如缓冲区溢出漏洞、SQL注入漏洞等是常见的软件开发漏洞，它们允许攻击者执行恶意代码、窃取数据或破坏系统。

3.2.3 部署问题

系统部署时，如果未能遵循最佳安全实践，也可能导致安全隐患。例如，将系统部署在公共网络上而未进行必要的隔离和防护；未对系统进行充分的安全配置和优化；未及时更新系统补丁和升级安全软件等。这些问题都可能使系统面临外部攻击的风险。

3.3 新技术应用带来的未知风险

3.3.1 新技术成熟度不足

随着物联网、云计算、大数据等新技术在煤矿工业控制系统中的广泛应用，这些新技术本身的成熟度不足也可能带来安全隐患。例如物联网设备的安全防护能力相对较弱，容易受到网络攻击；云计算平台可能存在数据泄露风险；大数据技术可能因处理不当而泄露敏感信息。

3.3.2 技术融合挑战

新技术与传统工业控制系统的融合过程中，可能因技术不兼容、协议不匹配等问题而引入新的安全隐患。例如工业控制系统广泛使用的SCADA、DCS、PLC等设备在与新技术融合时，可能因通信协议不统一、安全防护措施不到位等原因而遭受攻击。

3.3.3 未知漏洞和威胁

新技术的快速发展也带来了未知漏洞和威胁。由于新技术应用广泛且更新迅速，攻击者可能利用新技术中的未知漏洞进行攻击。此外，新技术还可能带来新的攻击方式和手段，使得传统安全防护措施难以应对。

4 智能化煤矿工业控制系统网络安全防护实践

在智能化煤矿工业控制系统的网络安全防护实践中，构建一个全面、高效且灵活的安全防护体系是至关

重要的。

4.1 构建纵深安全防御体系

智能化煤矿工业控制系统的网络安全防护需从全局出发，构建多层次、多维度的纵深安全防御体系。这一体系应涵盖计算环境安全、区域边界安全、通信网络安全以及安全管理中心等多个层面。（1）计算环境安全：首先，确保煤矿工业控制系统中的计算设备（如服务器、工作站、PLC等）具备基本的安全防护能力，如安装最新的操作系统补丁、配置合理的安全策略、启用访问控制等。同时对关键业务数据进行加密存储和传输，防止数据泄露。（2）区域边界安全：在煤矿工业控制系统的不同区域（如生产区、办公区、网络核心区等）之间设置清晰的边界，并通过防火墙、网闸等安全设备进行隔离。这些设备能够严格控制跨区域的流量，阻止未授权访问和恶意攻击。（3）通信网络安全：加强煤矿工业控制系统通信网络的安全防护，采用加密技术保障数据传输的机密性和完整性。同时对网络流量进行实时监控和审计，及时发现并处理异常行为。（4）安全管理中心：建立集中的安全管理中心，对整个煤矿工业控制系统的网络安全状况进行实时监控和综合分析。安全管理中心应具备日志收集、分析、报警和响应等功能，为管理人员提供全面的安全视图和决策支持。

4.2 部署关键防护措施

为了进一步提升煤矿工业控制系统的安全防护能力，需要部署一系列关键防护措施。（1）工控防火墙：在煤矿工业控制系统的关键区域边界部署工控防火墙，对进出网络的流量进行严格的过滤和控制[4]。工控防火墙应具备针对工业协议深度解析的能力，以有效应对针对工业控制系统的特定攻击。（2）安全监测审计系统：部署安全监测审计系统，对煤矿工业控制系统的网络流量、系统日志、用户行为等进行全面监测和记录。通过大数据分析和机器学习技术，及时发现并预警潜在的安全威胁。（3）入侵检测与防御系统：部署入侵检测与防御系统（IDS/IPS），对网络中的恶意流量进行实时检测和拦截。IDS/IPS能够识别并阻止各种已知和未知的攻击手段，为煤矿工业控制系统提供实时的安全防护。（4）终端防护与行为管控系统：在煤矿工业控制系统的终端设备上部署终端防护软件，如防病毒软件、主机入侵防御系统等。同时建立行为管控机制，对用户的操作行为进行实时监控和审计，防止内部人员误操作或恶意破坏。（5）数据库审计与安全管理平台：针对煤矿工业控制系统中存储的关键业务数据，部署数据库审计与安全管理平台。该平台能够记录数据库的所有访问和操作行为，提供详细的审计日志和报告，帮助管理人员及时发现并处理潜在的安全风险。

4.3 建立应急响应机制

在构建纵深安全防御体系和部署关键防护措施的基础上，还需要建立完善的应急响应机制，以应对可能发生的网络安全事件。（1）制定应急响应预案：根据煤矿工业控制系统的实际情况和业务需求，制定详细的应急响应预案。预案应明确各级响应组织的职责、应急处理流程、资源调配方案等内容，确保在发生安全事件时能够迅速启动应急响应机制。（2）开展应急演练：定期组织应急演练活动，检验应急响应预案的可行性和有效性。通过模拟真实的安全事件场景，提高各级响应组织的协同作战能力和应急处置能力。（3）建立快速恢复机制：在发生安全事件后，应迅速启动快速恢复机制，对受损的系统和设备进行修复和恢复。对事件原因进行深入分析，总结经验教训，完善安全防护措施和应急响应机制。

结语

智能化煤矿工业控制系统的网络安全是煤炭行业高质量发展的重要保障。通过深入分析系统存在的安全风险点并采取有效的防护实践措施，可以显著提升煤矿工业控制系统的安全防护能力，为煤炭生产的安全与高效提供有力支撑。未来，随着技术的不断进步和应用的深入拓展，智能化煤矿工业控制系统的网络安全防护工作将面临更多挑战和机遇。因此，我们需要持续关注和研究相关领域的最新动态和技术进展，不断完善和优化网络安全防护体系，为煤炭行业的可持续发展贡献力量。

参考文献

[1]王明钦,王力,张苗苗.主井煤流系统保护功能的创新与应用[J].山东煤炭科技,2019(11):211-213.

[2]谭成.某煤矿主煤流运输自动化系统改造[J].矿山机械,2019,47(11):31-35.

[3]奂光润,张豪,时培源.煤矿主煤流运输智能化控制技术研究[J].能源与环保,2019,41(10):140-142+146.