第 2 卷◆第 4 期◆版本 1.0◆2024 年
文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

智能化煤矿工业控制系统的网络安全设计

刘淑中[1]　李国鑫[2]
1 山东新矿信息技术有限公司　2 新汶矿业集团孙村煤矿
DOI:10.12238/acair.v2i4.10302

[摘　要] 智能化煤矿工业控制系统的网络安全设计,已成为确保煤矿安全、高效、可持续运营的关键环节。本文基于人工智能技术提出煤炭行业工业互联网安全解决方案,旨在构建全面、智能的工业控制系统安全防护体系。方案针对煤炭企业的网络安全痛点,设计了威胁检测与免疫系统、IT+OT纵深防护体系、安全运营中心等多维度安全防护措施。引入自主AI算法引擎、全网资产可视化、仿生人体免疫机制等技术,实现对工业控制系统中已知和未知威胁的主动防御,提升煤炭企业的网络安全防护水平。
[关键词] 煤矿工业；控制系统；网络安全
中图分类号：X752　文献标识码：A

Network Security Design of Intelligent Coal Mine Industrial Control System

Shuzhong Liu[1]　Guoxin Li[2]
1 Shandong Xinkuang Information Technology Co., Ltd.　2 Sun Village Coal Mine of Xinwen Mining Group
[Abstract] The network security design of intelligent coal mine industrial control system has become a key link to ensure the safe, efficient and sustainable operation of coal mines. Based on artificial intelligence technology, this paper proposes a security solution for industrial Internet in coal industry, aiming to build a comprehensive and intelligent security protection system for industrial control system. The plan addresses the network security pain points of coal enterprises and designs multidimensional security protection measures such as threat detection and immune system, IT+OT deep protection system, and security operation center. Introducing autonomous AI algorithm engines, full network asset visualization, bionic human immune mechanisms and other technologies to achieve active defense against known and unknown threats in industrial control systems, and enhance the network security protection level of coal enterprises.
[Key words] coal mining industry; Control system; network security

煤矿工业控制系统面临内外多样的网络威胁,包括黑客攻击、病毒传播及数据泄露,这些均会威胁生产连续性及人员安全。煤矿工业控制系统因其复杂性高、设备多样及环境严苛,给网络安全设计带来挑战[1]。研究智能化煤矿工业控制系统的网络安全,构建安全网络环境,对保障煤矿生产安全、提升生产效率及煤炭行业可持续发展至关重要。强化网络安全设计能防御网络威胁,保障煤矿工业控制系统稳定运行,为煤矿智能化转型提供坚实支撑。

1 网络设计的关键问题

1.1信息融合与联动不足：煤矿监控的决策瓶颈

煤矿监控系统常面临信息融合、联动及决策融合不足的问题。各应用系统间缺乏有效的信息共享与协同机制,紧急状况下决策与响应速度迟缓,影响安全生产。系统独立运行,数据孤岛现象严重,关键信息无法及时传递。例如,瓦斯监测与人员定位系统因数据格式和通信协议不兼容,瓦斯超标时无法迅速关联井下人员位置,影响及时撤离和救援。网络设计需强化信息融合与联动,构建统一数据交换平台和通信协议,实现系统间实时信息共享。开发数据融合算法,整合分析不同系统数据,形成全面安全态势图。建立联动机制,监测到异常时迅速触发相关系统响应,如自动报警、启动应急预案,提高决策与响应速度[2]。

1.2感知网络覆盖不足：井下监测的盲区

煤矿监控系统面临地下无线覆盖感知网络空白区域多的挑战。井下环境复杂,遮挡物和电磁干扰多,无线信号难以全面覆盖,存在监测盲区。盲区可能隐藏瓦斯积聚、透水等安全隐患,后果严重。网络设计应着重扩展感知网络覆盖范围。采用5G、Wi-Fi6等先进无线通信技术,提高信号穿透力和抗干扰能力。部署更多无线接入点和感知元件,形成密集网络覆盖。利用有线网络作为补充,确保无线信号无法覆盖区域也能通过有线方式传输数据,实现全面监测。

1.3设备落后与单一性：系统适应性的局限

Copyright © This work is licensed under a Commons Attibution-Non Commercial 4.0 International License.

感知元件单一及设备落后,限制煤矿监控系统在复杂井下环境中的有效运作。传统感知设备只能监测单一参数,如瓦斯浓度,无法全面反映井下环境多维度信息。设备老化、性能下降,影响监测数据准确性和可靠性。网络设计需考虑升级和多样化感知设备。引入多参数传感器,同时监测瓦斯、温度、湿度、压力等多种参数,提高监测全面性。采用智能感知设备,具备自学习、自诊断功能,根据环境变化自动调整监测策略,提高系统适应性和可靠性[3]。

2 网络设计的建议

2.1建立统一标准与接口：打破数据孤岛的关键

在煤矿监控系统中,数据的顺畅交换是系统协同工作的基石。不同系统常因各自的数据传输标准和接口规范,形成数据孤岛,阻碍信息流通与共享。为破解此难题,制定统一的数据传输标准和接口规范至关重要。统一标准应覆盖数据采集、传输、处理、存储及共享各环节,包括统一的数据格式、通信协议和接口规范,以实现系统间数据的无缝对接与交换。例如,采用XML或JSON作为通用数据交换格式,TCP/IP或HTTP作为标准通信协议,促进数据顺畅传输。接口规范设计同样关键,需确保系统间接口能相互识别、理解和响应,涉及定义统一的接口调用方式、参数传递规则和数据返回格式,从而实现数据的实时共享与交换。随着技术和系统升级,数据传输标准和接口规范需不断调整和完善[4]。应设立专门机构负责标准的制定、发布和更新,以保持标准的时效性和适用性。

2.2构建数据共享平台：信息流通的加速器

为促进信息流通和共享,提高数据利用效率,构建集中的数据共享平台势在必行。平台设计需具备高可扩展性和灵活性,支持不同类型和格式的数据存储,并提供强大的数据处理和分析能力。通过引入大数据处理、云计算和人工智能等先进技术,快速处理和分析海量数据。

煤矿监控系统涉及井下人员位置、瓦斯浓度等大量敏感数据,必须采取数据加密、访问控制、安全审计等严格的安全措施保护数据安全和隐私,防止数据在传输、存储和处理过程中被泄露或篡改。为促进数据共享和利用,平台应提供丰富的数据接口和API,支持系统间数据调用和交换,实现数据无缝对接和共享。同时,平台应提供友好的用户界面和查询工具,方便用户快速查找和获取所需数据。

2.3强化信息融合与联动：提升决策与响应速度

信息融合指整合和分析来自不同系统的数据,形成全面的安全态势图。需开发先进的数据融合算法和技术,如多源数据融合、数据挖掘和机器学习等,对数据进行综合分析和处理,提取有价值的信息和规律,为决策提供支持。联动机制则指当某系统监测到异常时,迅速触发其他相关系统响应。例如,瓦斯监测系统检测到瓦斯浓度超标时,自动触发人员定位系统和报警系统,实现人员快速撤离和报警信息及时发布。为实现信息融合与联动,还需建立相应的监控和管理平台,实时监测各系统运行状态和数据变化,提供强大的数据分析和可视化功能。用户可通过此平台直观了解井下安全状况,及时发现潜在隐患,并采取措施处理[5]。

2.4扩展感知网络覆盖：消除监测盲区

采用5G、Wi-Fi6等先进的无线通信技术,提高信号穿透力和抗干扰能力,扩大无线网络覆盖范围。增加无线接入点和感知元件数量,形成更密集的网络覆盖,减少信号盲区。引入传感器、摄像头等多样化的感知元件,全方位监测井下环境,提高监测准确性和可靠性。此外,可利用有线网络作为补充,在无线信号无法覆盖的区域部署有线网络传输数据。有线网络传输稳定、抗干扰能力强,可靠传输和实时监测数据。

2.5升级与多样化感知设备：提高系统适应性

升级感知设备包括更新传感器、摄像头等硬件设备,提高其性能和精度。例如,采用高精度的瓦斯传感器实时监测瓦斯浓度变化,采用高分辨率的摄像头捕捉井下细节信息。这些升级可提高监测数据的准确性和可靠性,为决策提供更可靠依据。多样化感知设备引入不同类型的感知元件监测井下的多种参数,除瓦斯浓度外,还可监测温度、湿度、压力等参数,全面了解井下安全状况。通过引入多参数传感器和智能感知设备,实现对井下环境的全方位、多维度监测,提高系统的感知能力和适应性。

3 安全防护体系设计

3.1威胁检测与免疫系统

智能化煤矿工业控制系统作为现代矿业安全高效运行的核心支撑,深度融合先进信息技术与传统采矿工艺,智能监控与管理煤矿生产全过程。系统多渠道全面收集网络设备日志、工控系统(如PLC、SCADA系统)日志、安全设备(如防火墙、入侵检测系统)警报、流量分析数据及用户行为数据,为煤矿安全运营奠定坚实数据基础。在网络资产可视化方面,系统采用WebGL、SVG等前沿图形化技术,构建直观网络拓扑图、设备分布图及资产属性表,清晰展示煤矿网络架构、设备布局及资产状态,实时监控网络流量、连接状态、会话信息等关键指标,动态生成拓扑图,一旦检测到异常流量、未授权访问尝试或恶意代码传播等安全威胁,立即在拓扑图上高亮或闪烁标注具体位置,迅速引导安全管理人员定位并处理[6]。

为增强安全管理能力,系统集成柱状图、折线图、饼图等,按威胁类型、来源、目标、时间等维度统计分析威胁检测与免疫结果,直观展现威胁分布态势和趋势变化。系统运用机器学习算法(如随机森林、深度学习神经网络)深度挖掘海量数据,自动识别并分类正常与异常行为,不断优化模型,提升威胁检测准确性和效率。系统还支持基于规则的威胁检测,安全管理人员可根据煤矿实际安全需求定制规则库和阈值条件,触发规则即自动报警。面对DDoS攻击,系统自动启动流量清洗与过滤机制,运用BGP Flowspec或专门DDoS防护设备,有效隔离并清除恶意流量,保障网络通畅。针对SQL注入等应用层攻击,系统实时监测并阻断攻击者连接,立即通知安全团队进行后续处理,如封锁攻击源IP、修复漏洞。

3.2 IT+OT纵深防护体系

Copyright © This work is licensed under a Commons Attibution-Non Commercial 4.0 International License.

在现场控制层,作为工业控制系统的基础关键,部署专用的工业防火墙和安全网关至关重要。启用深度包检测技术(DPI)对防火墙的每一个数据包逐包检查,识别并阻断潜在的恶意代码和攻击行为。定期更新防火墙的规则库和特征库,防御最新的安全威胁。IDS系统实时监控网络流量,利用模式匹配、异常检测等技术分析数据包特征和行为模式,识别潜在的入侵和攻击。检测到异常,IDS系统立即触发警报,并将信息推送至安全运营中心。安全审计系统记录和分析网络中的所有操作,包括登录、访问、修改等,实现操作的可追溯和可审计。定期对审计日志分析,发现潜在的安全风险和漏洞。

生产管理层是煤炭企业工业互联网的核心,涉及大量业务数据和管理信息。部署高级威胁防护系统(ATP)系统利用机器学习和人工智能技术深度分析和挖掘流量,识别并阻断高级持续性威胁(APT)、零日攻击等复杂攻击。加强身份认证和访问控制,采用多因素认证、基于角色的访问控制(RBAC)等策略,限制敏感数据和业务系统的访问。部署数据加密系统,对敏感数据加密处理,保障数据传输和存储的安全。采用安全传输协议(如TLS/SSL)保护数据传输。对企业资源层的访问严格审计和监控,防止未经授权的访问和数据泄露。

为强化网络安全监测预警体系,引入态势感知平台。平台整合网络中的安全设备和日志信息,利用大数据分析和机器学习技术深度挖掘和分析安全日志,识别潜在的网络安全风险和威胁。态势感知平台实时展示网络安全态势,发现异常行为或攻击迹象立即触发警报,生成详细报告和分析结果,为安全管理人员提供决策支持。利用应急响应工具和技术,对受影响的系统和数据隔离、恢复和加固,防止事态扩大。定期组织应急演练和培训,提高安全管理人员的应急响应能力。与专业的网络安全服务机构建立合作,发生重大网络安全事件时及时获得专业支持。

3.3安全运营中心

在智能化煤矿工业控制系统的安全运营中心建设中,功能定位与架构设计至关重要,奠定了煤矿安全高效运行的基础。安全运营中心集成了用户身份管理、策略调试、远程运维监控、资产与漏洞管理等多个核心模块,旨在实现全方位的安全运维管控。架构设计严格遵循高可用性、可扩展性和易用性原则,以灵活应对煤矿未来业务的动态发展。在用户身份管理方面,系统融合了多因素认证和生物特征识别技术,如指纹识别、面部识别,严格把控访问权限,仅限于授权用户访问系统。系统还根据用户角色和权限精细划分访问权限,有效阻止未经授权的访问和操作。此外,系统详尽记录用户的登录行为、操作记录,为后续安全审计和追溯提供可靠依据。

策略调试作为安全运营中心的关键功能,为安全管理人员提供灵活的策略配置和调试工具,轻松配置和调整防火墙规则、入侵检测规则、访问控制策略等各类安全策略。系统还具备策略模拟和测试能力,使安全管理人员能够在不影响业务运行的前提下,全面测试和优化策略。在远程运维监控方面,安全运营中心实时监控远程运维操作的动态,一旦发现任何未经授权的远程运维行为,立即触发警报并采取断开连接、封锁IP等安全措施。系统还详细记录远程运维操作的操作时间、操作人员、操作内容等。系统集成了资产管理和漏洞扫描工具,能够全面监控和管理煤矿内的各类资产,如网络设备、工控系统、服务器等。资产管理模块自动发现、识别网络中的资产,并进行分类和标记,确保资产管理的清晰性和可控性。漏洞扫描模块则定期对资产进行漏洞扫描和风险评估,及时发现潜在的安全漏洞和弱点,并提供针对性的漏洞修复建议和整改方案,助力安全管理人员及时修复漏洞,全面提升系统的安全性。系统运用大数据分析和机器学习算法,深入分析和挖掘海量安全日志和事件,揭示潜在的安全风险和威胁。例如,当系统检测到某个IP地址频繁尝试访问敏感资源时,会自动触发警报,并建议采取封禁或限制访问等措施。同时,系统还能根据历史数据和趋势分析,预测未来的安全风险和威胁,为安全管理人员提供前瞻性的安全决策支持。

4 结语

本文引入自主AI算法引擎、全网资产可视化和仿生人体免疫机制等关键技术,实现网络威胁的主动防御和智能响应。在安全防护体系设计中,着重构建威胁检测与免疫系统、IT+OT纵深防护体系及安全运营中心,覆盖从现场控制层到企业资源层的全方位防护。实践此方案,煤炭企业能有效防御网络威胁,保障生产安全,提升生产效率,实现可持续发展。

[参考文献]

[1]闫光杰.智能化煤矿工业控制系统网络安全分析及防护实践[J].软件,2023,44(01):144-146.

[2]陈晅.浅析煤矿提升机制动系统电控装置设计[J].中国设备工程,2021,(14):88-89.

[3]王大为,贾芳云,刘志勇.PLC控制在矿用电气设备中的应用——评《煤矿电气控制系统运行与维护》[J].有色金属(冶炼部分),2020,(10):118.

[4]李雅卓.选煤厂装车站液压管路改造与质量控制对策[J].企业科技与发展,2020,(06):116-117.

[5]陈团团.电气自动化技术在煤矿通风系统中的应用[J].现代矿业,2019,35(09):273-274.

[6]丁剑明.煤矿工业控制系统安全现状和解决方案[J].信息安全研究,2019,5(08):656-662.

作者简介：

刘淑中(1988--),男,汉族,山东省泰安市新泰市人,大学本科,工程师,职务,研究方向：煤炭信息化智能化。

Copyright © This work is licensed under a Commons Attibution-Non Commercial 4.0 International License.