煤矿安全与智能化融合背景下的电子信息安全防护措施

张芦定
榆林市榆阳区农垦榆卜界煤矿　陕西　榆林　719000

摘　要：随着煤矿产业智能化进程的不断加快，电子信息技术在煤矿生产、管理与安全监控等环节发挥着日益重要的作用。然而，信息系统的高度集成和网络化也使煤矿企业面临日益严峻的电子信息安全威胁。本文立足于煤矿安全与智能化融合发展的背景，分析煤矿智能系统的主要信息安全风险，包括数据泄露、非法入侵、设备控制失效等。针对这些风险，阐述了加强信息系统分层防护、完善身份认证机制、构建多元化的网络监控与预警体系、强化数据加密与备份措施以及提升员工信息安全意识等防护措施。研究指出，健全的电子信息安全防护体系不仅能有效防范网络攻击与信息泄露风险，还可保障煤矿智能化系统运行的稳定性和数据的完整性。因此，完善信息安全防护措施对于推动煤矿智能化与安全生产的深度融合、实现煤矿行业高质量发展具有重要意义。

关键词：煤矿智能化；电子信息安全；信息安全风险；防护措施；网络监控预警

引言

伴随第四次工业革命的影响，煤矿产业正处于智能化转型之中，普遍运用电子信息技术显著提高了煤矿的安全监管、生产调度及设备管理等环节的自动化与智能化水平。但伴随信息系统的高度集成和网络互联，煤矿信息安全风险日益增加，网络攻击等事件已经严峻危害到生产安全和人员安全。虽然已有面向工业控制系统和煤矿的信息安全研究，并且建立了包含物理防护、系统加固和网络隔离的多层次防护框架，但依然遭遇新兴威胁和发展新特征的挑战。文章探讨了智能化煤矿在信息安全方面遭遇的主要风险，并给出了相应的防护措施，意在助力煤矿行业智能化与安全生产的配合进步。

1 煤矿智能化与电子信息安全概述

1.1 煤矿智能化发展现状

信息技术与自动化技术的发展，推动了智能化成为煤矿行业迈向现代化的关键方向。智能化建设主要集中在三个不同领域，包括生产过程中的自动化操作控制、管理系统的信息数据整合，以及安全监测和预警系统的智能化技术升级。采用了自动化控制技术后，采煤设备的操作变得更加准确，生产过程效率大幅提升，安全保障也有了很大改善。安全监测完全依赖传感技术和数据分析工具，能够做到矿井环境的实时观察和突发情况的快速处理，大大提高了事故预警的准确度和反应速度。煤矿智能化推动了生产效率和安全标准的不断提高，通过技术革新引导煤矿产业走向绿色环保、安全可靠、长期可持续的发展道路。在这个过程中，智能化带来的信息安全问题开始显现出来，给煤矿产业的发展带来了一些潜在的威胁和隐患。

1.2 电子信息安全在煤矿智能化中的作用

电子信息安全在煤矿智能化中的作用极其关键，影响了智能系统的可靠性和生产的连续性。于煤矿智能化过程中，信息技术得到普遍使用于各检测、监控和管理系统中，给煤矿整体运营供应即时数据支持与决策依据。这种高集成度与网络化特性同样引发了崭新的安全挑战。信息安全充当智能化技术的核心支柱其一，维护了数据的准确性和有效性，避免信息在互联网传播过程中的丢失和篡改。借助尖端的加密和身份验证技术，能高效防范非法的访问及数据泄露风险，因此守护关键系统免于攻击。健全的信息安全体系有利于增强煤矿企业抵御潜在威胁的能力，保障生产运营的安全性，达成智能化与安全生产目标的协调进步。持久的安全防护机制不但增强了技术应用的可靠性，还为煤矿行业的智能化进程给予了稳固基础。

1.3 主要信息安全威胁分析

煤矿自动化技术发展的过程当中，信息安全问题逐渐暴露出来，涉及范围涵盖了数据泄露、非法入侵和设备控制失灵等多种风险隐患。如果发生数据泄露，煤矿重要的生产信息和商业机密就会被外人获知，从而引发无法弥补的经济损失和名誉受损的情况。非法入侵带来的威胁在于，攻击者会利用系统漏洞偷偷侵入内部，获取不被允许的访问权限，或者进行恶意毁坏行为造成重大损失。设备控制失灵的风险来源于网络攻击或者系统故障，引起生产设备运行出现异常或者直接中断运转，直接危害矿井的安全生产环境和工人的生命安全。这些安全隐患对煤矿企业自动化系统的平稳运行和安全保证形成了巨大的挑战，必须尽快采取保护措施来处理各种

威胁，保证整个系统能够安全运行下去，避免更大的损失发生。

2 煤矿智能化系统中的信息安全风险

2.1 数据泄露风险

煤矿智能化发展的大环境下，数据外泄的风险已经变成了信息安全防护的一个关键问题。智能化技术如今煤矿行业中得到广泛使用，各种数据比如生产数据、监控视频、人员信息以及设备运行状态，系统内都会被大量收集、传递和保存。一旦这些数据被外泄或者遭到更改，就会带来巨大的财务损失，甚至还会引发安全生产事故。数据外泄问题通常是由于系统存在缺陷、网络遭到侵袭或者人为失误造成的，智能化系统中信息流动的复杂性和开放性更是让数据外泄的风险变得更大。来自外界的侵袭者和内部人员的不当行为都有可能导致数据外泄，这充分说明数据安全防护的重要性，必须高度重视并且采取有效措施来应对潜在威胁，确保整个行业能够安全稳定地发展。数据泄露会带来很多风险，煤矿企业一定要建立一套完备的保护系统。这个系统要包含数据加密技术、访问权限的严格控制，还有系统运行时的实时监控等多种方式，确保信息不被外泄，不被恶意修改，同时还能顺畅运行。需要认真研究数据泄露可能引发的各种危害，制定出详细的保护方案，并且认真执行这些方案，只有这样才能真正维护煤矿智能化系统的稳定运行和安全保障。数据安全是信息保护中非常重要的一部分，也是帮助煤矿产业实现智能化发展的基础和支柱，更是让整个行业能够长久稳定发展的关键因素，必须高度关注，绝不能忽视。

2.2 非法入侵风险

煤矿智能化系统在运作的时候，如果未经许可擅自进入，就会给企业的安全运营带来很大的威胁。系统的集成程度逐渐提高，网络连接看起来更加复杂难懂，黑客会抓住网络漏洞、防护措施的不足之处，或者工作人员粗心犯下的错误，用各种方法进行非法入侵。这种情况会造成重要数据被泄露或者被恶意修改，还会导致系统设备运行出现问题，比如设备经常死机或者指令不灵敏，最后影响到生产流程的稳定和可靠。未经许可进入的危险一般会通过漏洞扫描、钓鱼攻击这些具体方法钻进信息系统，甚至会用恶意软件悄悄隐藏，等到合适的时候突然发动攻击。为了处理好这些危险，煤矿企业需要改进防火墙和入侵检测系统的性能，认真落实权限管理和身份认证的政策，防止任何人未经批准就进入系统或者操作设备，比如不让无关人员靠近核心设备，确保生产和管理工作稳定可靠，确保整个系统运行顺畅没有问题，尽量降低隐藏的危险给企业带来的各种损失。

2.3 设备控制失效风险

信息系统遭遇网络攻击、软件漏洞或内部操作失误的干扰时，设备控制系统就会出现故障。遇到这种情况，生产流程会被迫停止，煤矿工人的生命安全可能会陷入严峻的危险境地。对于自动化操作的设备，例如矿井提升机、通风系统、排水设备等，控制系统一旦失灵，就会诱发严重的安全事故。设备控制失灵还可能因为恶意软件的入侵。

3 电子信息安全防护措施

3.1 分层信息系统防护

煤矿智能化管理系统安全设计采用分级防护措施，实用可靠，值得推广。该方法将信息系统分多个层级管理保护，抵御内外安全威胁。具体操作是分开管理数据存储、网络连接和功能应用模块，各模块采用独特防护手段，提高数据加密水平，确保存储传输安全。同时安装防火墙、入侵检测设备，设置多层次访问权限，杜绝非法访问和网络攻击。还需按时检查代码安全，修复漏洞，减少安全隐患。周期性安全审计与评估可评估防护效果，形成防护屏障，提高煤矿企业信息安全抵御能力，为智能化系统长期发展提供稳固支持。

3.2 完善的身份认证机制

煤矿智能化系统运作中，优化身份认证机制对电子信息安全防护至关重要。传统密码认证方式在复杂信息安全威胁前无力防范风险。多因素认证技术融合密码与生物特征识别，如指纹、人脸识别及智能卡等，显著提升安全性能，降低未授权进入风险。动态认证技术通过分析用户操作习惯，增强实时防护，减少安全漏洞。访问控制策略需严谨改进，遵循最小权限原则，防止信息外泄。这些措施减缓了隐秘入侵者攻击进程，提升防御能力，为煤矿企业信息安全管理提供坚实保障，减少重大损失风险。

3.3 多元化网络监控与预警系统

多方面网络监控预警系统成为维护煤矿智能化系统平稳运行的关键中心组成部分。使用顶尖的网络流量分析工具和入侵检测设备，能够不间断地观察不正常的流量和疑似异常活动，提前预防可能发生的网络侵害行为，避免造成重大经济损失。应用人工智能技术，能够大幅提升预警系统的自动化分析和未来风险预判能力，使得应对复杂网络侵害时反应更加及时有效。整合大数据分析技术，能够完善应对突发情况的处理方案，提高对风险管理的全面效率和可靠性，确保煤矿智能化系统的安全保护能力得到全面加强，维护作业环境和信息资

料的安全，降低突发事件导致损害的可能性，保护重要设备和设施。

4 防护效果与未来展望

4.1 防护效果评估

判断防护效果好坏对搭建电子信息安全防护体系来说十分关键。深入检查和分析煤矿智能化系统的运行情况，可以准确分辨信息安全防护措施有没有起到作用。开展判断工作需要从多个不同方面入手，像是仔细查看系统防御网络攻击的本领、确认数据是否能免于被随意改动的能力，还有维持系统运行平稳不出现故障的状态。使用分层防护的办法能够明显减少信息泄露和网络攻击发生的次数，这样就能增强整个信息系统的安全程度，维护核心数据不被破坏的完好状态。建立健全的身份认证机制可以有效管理谁能进入系统的权限，降低未经许可擅自闯入系统的风险。设置多元化的网络监控和预警系统能在察觉安全隐患和快速处理紧急状况时表现得很优秀，减少安全事件造成的隐性损失，确保整个系统运行顺畅无阻。审查还表明，通过安全培训的员工可以提升对信息安全威胁的辨别与应对能力，塑造有用的安全防护文化。所执行的防护措施有用维护了煤矿自动化系统的安全性与稳定性，但伴随科技发展与攻击方式的演变，必须不断审查和改进安全策略，以对抗未来更为繁琐的信息安全难题。

4.2 提升员工信息安全意识

提高员工的信息安全意识是为保障煤矿智能化系统安全防护的关键环节。员工是信息系统的直观使用者，其安全意识直观影响到信息安全措施的成效。定时实施专项的安全培训，有利于协助员工领会信息安全的重要性，并熟悉辨别和处理隐性安全威胁的方法。通过真实案例分析，强化员工的风险感知能力，增进对社会工程攻击、钓鱼攻击等普遍威胁的警觉性。设立激励机制，激励员工积极反馈信息安全事件，巩固平常工作的规范性。企业还需将信息安全意识的提高融入绩效考核体系，以规范化的方式保证培训的持久性和成效。有效的信息安全意识提高可以塑造一个坚韧的安全文化氛围，因此增进整体的安全防护水平，为煤矿智能生产的持久发展给予稳固保障。

4.3 未来发展趋势及建议

未来煤矿智能化与电子信息安全防护的趋势首要聚焦在技术的创新与制度的完善上。伴随人工智能、大数据分析、区块链等技术的提升，这些技术会在煤矿安全领域获得普遍运用，供应更加精确和机械化的安全管理和监控。面对持续转变的安全威胁，煤矿企业必需增强与网络安全领域的合作，迅速取得前沿的安全防护工具和策略。监管机构应当更深入巩固信息安全法规，并促进行业标准的确立，以顺应智能化发展的要求，保障煤矿行业在高质量发展的电子信息安全防护措施可以不断改进。

结束语

目前煤矿智能系统被运用在数据存储、传输和控制等多个关键环节，但也显现出一些重大且棘手的安全问题。煤矿工作环境具有独特性且充满不确定因素，技术本身也存在繁琐和难点问题，有些安全隐患暂时无法得到解决。未来需要重点关注如何提升防护体系的智能化和自动化水平，打造更高效先进的安全保护机制，确保煤矿智能化发展能够稳步向前推进，降低安全事故出现的概率，保护生产环境和工作人员的生命安全。

参考文献

[1]韩倩.医院电子档案管理与电子信息安全防护分析[J].长江信息通信,2021,(02):178-180.

[2]魏琛.煤矿安全监控系统智能化现状分析[J].内蒙古煤炭经济,2022,(08):97-99.

[3]张文宏张鸿基.煤矿智能化系统的雷电安全防护策略研究[J].进展：科学视界,2021,(19):71-72.

[4]李鑫.煤矿智能化系统网络安全整体防护[J].中国科技投资,2021,(35):52-55.

[5]张志愿.网络环境下办公室电子信息安全防护分析[J].数码世界,2020,(07):206-206.