

电力系统信息通信网络安全及防护策略探究

卢军志 李 瑾

河南源网荷储电气研究院有限公司 河南 许昌 461000

摘要: 随着电力系统信息通信网络的不断发展,网络安全问题日益突出。本文对电力系统信息通信网络安全及防护策略进行了探究,重点分析了当前网络面临的主要威胁和挑战,并提出了针对性的防护策略。通过加强物理安全防护措施、建立身份认证与访问控制策略、建立安全监测与应急响应机制和提高网络安全技术防护能力等多方面的措施,可以有效保障电力系统的信息通信网络安全。

关键词: 电力系统;信息通信网络;安全防护;策略探究

1 电力系统信息通信网络概述

电力系统信息通信网络作为支撑整个电力系统运作的基础设施,其安全性与稳定性对电力系统的正常运行至关重要。该网络涵盖了发电、输电、配电等各个环节,为电力系统的调度、控制、运营等提供了必要的信息传输服务。随着科技的发展,电力系统信息通信网络正逐步向智能化、自动化、互动化的方向演进。例如,通过引入先进的信息技术和通信技术,电力系统能够实现远程监控、自动控制、智能调度等功能,极大地提高了电力系统的运行效率和安全性。从技术角度来看,电力系统信息通信网络采用了多种通信协议和设备,如光纤通信、微波通信、电力线通信等,形成了纵横交错的通信网络体系。这些技术和设备需要与电力系统业务需求相匹配,并且能够适应各种运行环境和条件。随着云计算、大数据等技术的广泛应用,电力系统信息通信网络的数据处理和存储能力也得到了显著提升。这为电力系统的实时监控、数据分析、决策支持等提供了强大的技术支持^[1]。未来应加大对新型防御手段的研发力度,通过更加智能化和自动化的方法应对复杂多变的网络安全威胁,提升整个电力系统信息通信网络的安全水平。

2 电力系统信息通信网络安全及防护的重要作用

在电力系统运作的各个环节中,信息通信网络的角色无可替代。它不仅是调度、控制和运营的重要载体,也是保障电力稳定供应、优化资源配置的关键环节。因此,确保信息通信网络的安全与稳定对于电力系统的正常运作至关重要。第一,网络安全是电力系统稳定运行的基础。电力作为国家基础设施,其信息通信网络的任何故障或安全事件都可能对整个电力系统造成严重影响,甚至导致大规模停电等严重后果。通过有效的防护措施,可以预防和减少各种潜在的网络攻击和故障,确保电力供应的稳定性和可靠性。第二,随着电力系统的

智能化发展,信息通信网络中存储和传输的数据日益丰富,涉及调度指令、控制参数、用户信息等敏感数据。这些数据一旦泄露或被篡改,不仅可能导致电力系统的正常运行受阻,还可能引发严重的隐私和安全问题。因此,加强网络安全防护对于保护数据安全和用户隐私也具有重要意义。第三,电力系统信息通信网络作为现代智能电网的重要组成部分,还承载着电力交易、远程控制、需求响应等多种智能服务。这些服务的正常运行需要高度可靠的网络安全环境作为支撑,以保障电力系统的整体效率和经济性^[2]。总之,维护电力系统信息通信网络安全是确保电力稳定供应、保障数据隐私及支持智能服务的核心要素。加强网络安全防护不仅能提高电力系统的稳定性,还能为电力行业的可持续发展提供有力保障。

3 电力系统信息通信网络安全的威胁因素

3.1 网络攻击与恶意软件

电力系统信息通信网络面临着多种威胁因素,这些因素可能源自内部或外部,既包括网络攻击和恶意软件,也涉及物理设备和人为操作失误。网络攻击是电力系统信息通信网络面临的主要威胁。攻击者可能利用各种手段,如拒绝服务攻击、病毒传播、特洛伊木马等,对网络发起攻击,旨在破坏网络正常运行、窃取敏感数据或实施其他恶意行为。这些攻击可能来自外部的黑客组织或敌对势力,也可能源自内部的违规操作或恶意员工。针对电力系统的网络攻击可能直接影响电力供应的稳定性,甚至威胁国家安全。恶意软件也是一类重要的安全威胁。例如,间谍软件会在用户不知情的情况下,在其电脑上安装后门、收集用户信息;蠕虫病毒则可能利用系统漏洞进行传播,导致网络拥堵甚至系统瘫痪。勒索软件可能会加密用户数据并索取赎金,对电力系统的正常运行造成严重干扰。

3.2 物理安全风险

除了网络层面的威胁外,电力系统信息通信网络还面临着物理层面的安全风险。这些风险主要源于网络设备、设施及环境的可靠性、物理安全保护措施不足等方面。首先,关键设备和设施的损坏或失效是导致电力系统通信网络安全事故的重要原因之一。例如,网络设备(如路由器、交换机、服务器等)因环境条件、物理损坏或其他原因而失效,可能导致数据丢失、服务中断或安全漏洞。其次,物理安全保护措施不足也是一大隐患^[3]。例如,未设置足够的安全控制措施来保护关键的通信设备和设施,可能导致未经授权的访问、篡改或破坏。此外,缺乏对物理访问和出入口的控制,可能使恶意人员有机可乘,对网络设备进行破坏或窃取敏感信息。自然灾害和环境因素也是不可忽视的物理安全风险。例如,地震、雷击、火灾或其他自然灾害可能对电力系统的通信设备及设施造成直接损坏,影响网络的正常运行和数据的安全性。同时,极端天气或气候变化也可能对设备的稳定运行构成威胁。

3.3 身份认证与访问控制风险

在电力系统信息通信网络中,身份认证与访问控制是确保网络安全的关键环节。身份认证风险主要集中在用户账号和密码的安全管理上。如果用户账号和密码设置过于简单或长期未更换,攻击者可能通过猜测、暴力破解等方式获取账号密码,进而非法访问网络资源。如果用户账号在不同系统间未实现统一认证,可能增加管理难度并引发安全漏洞。访问控制风险主要指对网络资源的非法访问或越权访问。如果网络未实施严格的访问控制策略,攻击者可能利用漏洞或恶意软件渗透到网络内部,窃取、篡改或破坏敏感数据。此外,内部人员也可能因权限管理不善而进行违规操作,对电力系统造成重大安全隐患。

4 电力系统信息通信网络安全防护策略

4.1 建立完善的网络安全管理体系

为应对电力系统信息通信网络所面临的各种威胁,建立一个完善的网络安全管理体系至关重要。这一体系应涵盖技术、人员和制度等多个方面,确保网络的安全稳定运行。首先,技术防护是网络安全管理体系的基础。应采取多层次、多手段的防护措施,包括防火墙、入侵检测系统(IDS)、数据加密等,以增强网络的安全性。定期对网络设备进行安全漏洞扫描和修复,防止潜在的攻击。其次,人员管理在网络安全体系中占据重要地位。应加强员工的安全意识培训,提高员工对网络安全的重视程度。实施严格的访问控制策略,对员工的网络行为进行监控和管理,防止未经授权的访问和违规操

作。制度建设是网络安全管理体系的重要支撑。应制定全面的网络安全管理制度和规范,明确各部门和员工在网络安全方面的职责和操作流程^[4]。建立完善的应急响应机制,以便在发生安全事件时迅速响应,降低损失。持续的监测和维护对于网络安全管理体系的长期有效运行至关重要。应定期对网络进行安全检查和评估,及时发现并解决潜在的安全问题。同时,与专业的网络安全服务机构合作,引入外部的专家意见和先进技术,不断提升网络安全防护能力。

4.2 加强物理安全防护措施

为了确保电力系统信息通信网络的安全稳定,除了加强技术和管理层面的防护外,还需要重视物理安全层面的防护。(1)物理访问控制:对所有进入网络设施的人员进行身份验证和授权管理,确保只有授权人员能够访问关键设备和区域。应采用多因素认证方式,如门禁卡、密码和生物识别技术等。(2)物理安全监控:安装视频监控和报警系统,对重要设备和区域进行实时监控。一旦发现异常行为或未授权访问,立即触发报警并采取相应措施。(3)设备冗余与容灾恢复:为关键设备配置冗余备份,确保在设备故障或损坏时能够迅速切换到备用设备,保障网络的连续性。同时,建立容灾恢复计划,确保在严重灾害或事故发生后能够迅速恢复数据和系统的正常运行。(4)环境安全:确保网络设备运行的环境安全稳定。这包括提供适当的电源和电力保障、保持适宜的温度和湿度、定期对设备进行维护和检查等。(5)物理安全审计:定期对物理安全防护措施进行审计和评估,及时发现并修复潜在的安全漏洞。审计范围应包括设备设施、人员访问、监控系统等各个方面。(6)灾难恢复计划:制定详细的灾难恢复计划,明确在发生自然灾害、事故或其他紧急情况时的应对措施。该计划应包括数据备份、设备替换、人员协调等多个方面。

4.3 身份认证与访问控制策略

为了确保网络的安全稳定运行,应制定并实施严格的身份认证与访问控制策略。应实施多层次的账号密码策略,要求用户设置复杂度高的密码,并定期更换密码。为了提高安全性,可以引入加盐值的方法来存储用户密码,以防止密码被轻易破解。采用多因素认证机制,除了传统的账号密码认证外,引入其他身份验证方法,如动态口令、短信验证、生物识别等。这样可以增加攻击者破解认证的难度,提高网络的安全性。实施基于角色的访问控制(RBAC)策略,根据用户角色和权限分配相应的资源访问权限。这样可以确保用户只能访问其权限范围内的资源,有效防止越权访问和数据泄露。

为了进一步强化身份认证与访问控制，可以引入单点登录（SSO）系统。通过单点登录，用户只需在单一平台上进行身份验证，即可访问网络中的多个应用系统。这样可以简化用户登录过程，降低管理复杂度，并提高网络的安全性。

4.4 建立安全监测与应急响应机制

为了应对潜在的网络威胁和安全事件，电力系统信息通信网络需要建立一套完善的安全监测与应急响应机制。通过实时监测网络状态、及时发现并处置安全问题，确保网络的安全稳定运行。首先，应部署全面的安全监测系统，对网络进行实时监控和威胁检测。该系统应具备入侵检测、恶意软件防范、漏洞扫描等功能，以便及时发现异常行为和潜在的安全威胁。定期对网络进行安全漏洞扫描，确保所有设备和系统均已更新到最新版本，且不存在已知的安全漏洞。其次，建立快速应急响应机制，以确保在网络遭受攻击或出现故障时能够迅速作出反应。该机制应明确应急响应流程、责任分工和处置措施，确保相关人员能够迅速启动应急响应计划，并采取有效的应对措施。定期进行应急演练和模拟攻击测试，提高应急响应团队的实战能力和协作水平。与专业的网络安全服务机构保持密切合作，共同应对安全事件和威胁。机构可以利用其专业知识和经验提供外部的专家意见和技术支持，帮助企业完善安全防护策略和提高应急响应能力。通过建立合作与共享机制，及时分享网络安全信息、情报和威胁态势，共同抵御网络安全威胁。最重要的是，建立一支专业的网络安全团队，负责监测网络状态、分析安全事件、执行应急响应计划等任务。团队成员应具备丰富的网络安全知识和实战经验，能够应对各种复杂的安全挑战。定期对团队成员进行培训和技能提升，确保他们始终保持最新的网络安全知识和技术水平^[5]。

4.5 提高网络安全技术防护能力

通过引入先进的技术手段和防护措施，可以有效应对不断变化的网络安全威胁。首先，加强防火墙配置。防火墙是网络安全的第一道防线，应合理配置防火墙规

则，严格控制网络访问。对于不必要的端口和服务，应予以关闭或限制访问。同时，定期对防火墙日志进行分析，及时发现潜在的威胁和攻击行为。其次，部署入侵检测系统（IDS）。IDS能够实时监测网络流量和系统状态，发现异常行为或入侵行为。通过配置合理的IDS规则，能够及时报警并采取相应的处置措施，防止网络被进一步渗透或攻击。数据加密是保障数据传输和存储安全的重要手段。应采用对称加密或非对称加密算法对敏感数据进行加密处理，确保即使数据在传输过程中被截获，攻击者也无法轻易解密。加强数据备份和恢复机制，确保在数据遭受损坏或丢失时能够迅速恢复。针对云计算和物联网等新技术应用，应建立相应的安全防护措施。例如，使用虚拟专用网络（VPN）技术来保护数据的传输安全，采用身份验证和访问控制机制来确保只有授权用户能够访问相关资源。

结束语

通过综合运用多种手段和方法，可以有效应对当前电力系统信息通信网络面临的主要威胁和挑战，保障电力系统的安全稳定运行。同时，需要不断加强网络安全管理和技术防范措施，提高网络安全意识，以应对不断变化的网络安全威胁。在未来的发展中，应继续关注网络安全领域的最新动态和技术趋势，不断完善和更新防护策略，确保电力系统的信息通信网络安全得到有效保障。

参考文献

- [1]丁嘉祺.电力信息通信机房的智能巡检技术[J].科技视界,2019(10):71-72.
- [2]张青.谢坤.徐洋.信息通信网络在电力系统安全中的应用研究[J].电力系统及其自动化学报.2021.43(8):1-8.
- [3]王亮.张伟.杨锐.电力系统信息通信网络安全保护策略研究[J].电力系统保护与控制.2021.49(10):24-31.
- [4]邓培.王鹏.杜云霄.基于大数据分析的电力系统信息通信网络安全防护[J].电力电子技术.2021.45(6):1-5.
- [5]刘瑞.高峰.王伟.电力系统信息通信网络安全漏洞与防护策略研究[J].电力工程技术学报.2021.41(6):1-7.