浅析热电厂电力监控网络系统安全管理及防护措施

张　赫
国家能源集团廊坊热电厂　河北　廊坊　065000

摘　要：随着电力行业信息化深入，热电厂电力监控网络系统面临诸多安全挑战。本文聚焦于热电厂电力监控网络系统的安全管理及防护措施。首先概述热电厂电力监控网络系统，接着深入分析其安全现状，指出面临网络攻击威胁、设备故障风险、人为操作失误以及缺乏系统化管理等问题。随后，从安全管理和防护技术两个层面提出针对性措施，安全管理涵盖建立健全制度、明确职责分工、加强人员培训与管理以及强化安全评估与监督；防护技术包括网络安全、设备安全防护技术及应急响应与恢复技术，旨在提升热电厂电力监控网络系统的安全性与可靠性。

关键词：热电厂；电力监控网络系统；安全管理；防护措施

引言：在电力行业不断发展与智能化升级的背景下，热电厂作为重要的电力生产源头，其电力监控网络系统发挥着关键作用，承担着实时监测、控制与调度电力生产流程的重要任务。然而，随着网络技术的广泛应用，热电厂电力监控网络系统面临的安全挑战日益严峻。一旦该系统遭受攻击或出现故障，不仅会影响热电厂的正常生产运营，还可能引发大面积停电等严重后果，对社会的稳定与经济发展造成巨大冲击。因此，深入探讨热电厂电力监控网络系统的安全管理及防护措施具有重要的现实意义和紧迫性。

1 热电厂电力监控网络系统概述

热电厂电力监控网络系统是保障热电厂安全、稳定、高效运行的核心组成部分，它借助先进的计算机网络、通信及自动化技术，对热电厂的电力生产过程进行全面、实时的监测与控制。该系统具有多层次、分布式的架构特点。从硬件层面看，涵盖了各类传感器、控制器、服务器以及网络通信设备等。传感器负责采集电力生产中的各种参数，如电压、电流、功率、温度等；控制器依据采集的数据和预设逻辑，对设备进行精准控制；服务器则用于数据的存储、处理与分析；网络通信设备保障各部分之间数据的高速、稳定传输。在软件方面，具备强大的功能模块，包括数据采集与处理、实时监控、故障诊断、调度管理等。数据采集与处理模块能快速、准确地收集各类数据，并进行初步处理；实时监控模块以直观的界面展示电力生产的实时状态，让操作人员及时掌握运行情况；故障诊断模块可自动检测异常，分析故障原因；调度管理模块则根据电力需求和生产状况，合理调配资源，优化生产流程。热电厂电力监控网络系统的可靠运行，对于提高电力生产效率、降低运行成本、保障供电质量以及预防安全事故等方面都起着至关重要的作用[1]。

2 热电厂电力监控网络系统安全现状分析

2.1 网络攻击威胁

热电厂电力监控网络系统与外部网络存在一定连接，这使其成为网络攻击的潜在目标。黑客可能利用系统漏洞，如未及时修复的软件漏洞、弱口令等，发起攻击。常见的攻击手段有拒绝服务攻击，通过大量请求拥塞网络，使系统无法正常响应；还有恶意软件入侵，植入病毒、木马等，窃取或篡改系统数据，干扰电力监控指令的正常执行，严重时可导致系统瘫痪，影响热电厂的电力生产与供应，给社会用电带来极大影响。

2.2 设备故障风险

热电厂电力监控网络系统依赖众多硬件设备，如服务器、交换机、传感器等。这些设备长期运行在复杂恶劣的环境中，易出现老化、磨损等问题。例如，传感器可能因高温、强电磁干扰等，导致测量数据不准确；服务器可能因硬件故障，如硬盘损坏、内存故障等，造成数据丢失或系统崩溃。此外，设备兼容性问题也可能引发故障，不同厂商设备在协同工作时，若接口、协议不匹配，会影响系统的稳定运行。

2.3 人为操作失误

热电厂电力监控网络系统的操作人员专业水平参差不齐，部分人员可能对系统操作流程不熟悉，在执行操作时出现失误。比如，在进行参数设置时，误输入错误数值，导致设备运行异常；在执行紧急操作时，因紧张或操作不熟练，未能及时、准确地完成操作，延误故障处理时机。而且，一些人员安全意识淡薄，违规操作，如随意插拔设备、使用未经授权的软件等，都可能引发系统故障，威胁电力监控网络系统的安全稳定运行[2]。

2.4 缺乏系统化管理

热电厂电力监控网络系统在管理方面存在诸多不足，缺乏系统性的规划与统筹。一方面，安全管理制度不完善，对于系统访问权限、数据备份恢复等关键环节没有明确规定，导致管理混乱。另一方面，各部门之间缺乏有效的沟通与协作，在系统维护、故障处理等工作上存在职责不清、推诿扯皮现象。此外，对系统的安全评估与监测不够全面、及时，不能及时发现潜在的安全隐患，使得系统长期处于风险之中，影响热电厂电力生产的可靠性。

3 热电厂电力监控网络系统安全管理措施

3.1 建立健全安全管理制度

建立健全安全管理制度是热电厂电力监控网络系统安全管理的基石。(1)要制定全面且细致的访问控制制度。明确不同人员对系统各模块的访问权限，依据工作性质和职责划分权限等级，例如，普通操作人员仅能进行常规数据查看与简单操作，而系统管理员则拥有最高级别的管理权限。同时，严格规范用户身份认证方式，采用多因素认证，如密码、指纹、动态令牌等结合，防止非法用户入侵。(2)完善数据备份与恢复制度。定期对系统中的重要数据进行备份，备份方式可采用本地备份与异地备份相结合，确保数据的安全性和完整性。制定详细的数据恢复流程，在系统出现故障或数据丢失时，能够迅速、准确地恢复数据，减少对电力监控工作的影响。(3)建立安全审计与监督制度。对系统的操作行为进行实时审计记录，包括操作时间、操作人员、操作内容等，以便在出现问题时能够追溯源头。定期对安全管理制度的执行情况进行监督检查，及时发现制度执行过程中的漏洞和问题，并进行整改完善，确保安全管理制度能够有效落实，保障热电厂电力监控网络系统的安全稳定运行[3]。

3.2 明确职责分工

明确职责分工对于热电厂电力监控网络系统的安全管理至关重要，它能确保各项工作有序开展，避免出现管理盲区与推诿现象。(1)要划分系统管理层级职责。高层管理者应承担整体安全战略规划与决策职责，制定系统安全管理的总体目标与方向，协调各方资源，为安全管理工作提供支持与保障。中层管理者负责将高层战略转化为具体可执行的管理措施，组织制定安全管理制度与流程，监督基层执行情况，并及时反馈问题。基层操作人员则需严格按照操作规范，执行日常的系统监控、数据记录与简单故障处理等工作。(2)明确不同部门职责。技术部门要负责系统的技术维护与升级，及时修复系统漏洞，保障系统硬件与软件的稳定运行；安全部门专注于安全防护体系的构建与维护，监测网络攻击行为，制定应急预案；运维部门承担系统的日常运行维护，包括设备巡检、数据备份等。(3)细化岗位个人职责。为每个岗位制定详细的职责说明书，明确其在系统安全管理中的具体任务与要求，使员工清楚知晓自己的工作内容与责任边界，做到各司其职、各负其责，共同维护热电厂电力监控网络系统的安全稳定。

3.3 加强人员培训与管理

加强人员培训与管理对于热电厂电力监控网络系统的安全稳定运行意义重大，可从多方面着手提升人员素质与安全保障能力。(1)构建多元化培训体系。依据不同岗位需求与人员技能水平，制定分层分类的培训计划。针对新入职员工，开展基础理论与操作规范培训，使其快速熟悉系统基本架构与操作流程；对于有一定经验的员工，提供进阶技术培训，如网络安全防护技术、系统深度维护技巧等，助力其提升专业能力。同时，定期邀请行业专家进行讲座，分享前沿技术与安全理念，拓宽员工视野。(2)强化培训效果评估。建立科学合理的考核机制，不仅关注理论知识考核，更注重实际操作能力评估。通过模拟故障场景、实际操作演练等方式，检验员工应对突发情况的能力。根据考核结果，为员工提供针对性的反馈与指导，帮助其查漏补缺，不断提升技能水平。(3)完善人员日常管理制度。明确人员岗位职责与操作权限，严格规范人员操作行为，杜绝违规操作。加强人员安全意识教育，通过定期安全会议、安全宣传活动等形式，强化员工安全责任感，营造良好的安全文化氛围，确保热电厂电力监控网络系统安全可靠运行。

3.4 强化安全评估与监督

强化安全评估与监督是保障热电厂电力监控网络系统安全的重要举措，能够及时发现系统潜在风险并加以整改，确保系统长期稳定运行。(1)建立科学全面的安全评估体系。定期对电力监控网络系统开展全方位评估，涵盖网络安全、设备安全、数据安全等多个维度。制定详细的评估指标与标准，从系统架构的合理性、安全防护措施的有效性到人员操作的规范性等方面进行量化评估。通过专业评估工具与人工分析相结合的方式，深入挖掘系统存在的安全隐患，为后续整改提供准确依据。(2)加强日常安全监督检查。成立专门的安全监督小组，制定监督检查计划，定期对系统运行情况进行巡查。检查内容包括设备运行状态、安全制度执行情况、人员操作规范等。对发现的问题及时记录并反馈，要求相关部门限期整改，并对整改情况进行跟踪复查，确保问题得到彻底解决。(3)引入第三方安全评估与审计。借助外部

专业机构的力量，对电力监控网络系统进行独立、客观的安全评估与审计。第三方机构凭借其丰富的经验和先进的技术，能够发现内部监督难以察觉的问题，提供更具针对性的改进建议，进一步提升系统的安全防护水平[4]。

4 热电厂电力监控网络系统防护技术措施

4.1 网络安全防护技术

热电厂电力监控网络系统面临着诸多网络安全威胁，需采取多层次防护技术。部署防火墙是基础防线，它能依据预设规则，对进出网络的数据流进行监控与过滤，阻止非法访问和恶意攻击，将外部不安全因素隔绝在外。入侵检测系统（IDS）与入侵防御系统（IPS）可实时监测网络流量，及时发现异常行为和潜在攻击，IDS负责检测并报警，IPS则能主动阻断攻击行为。采用加密技术对重要数据进行加密处理，无论是数据传输过程还是存储状态，都能防止数据被窃取或篡改。同时，实施访问控制策略，根据用户身份和权限，严格限制其对系统资源的访问，确保只有授权人员能够操作关键设备和数据。定期进行网络安全漏洞扫描，及时发现并修复系统存在的安全漏洞，提升系统整体安全性。

4.2 设备安全防护技术

设备安全是热电厂电力监控网络系统稳定运行的关键。对于硬件设备，要选择质量可靠、经过严格认证的产品，确保其在恶劣的工业环境下能长期稳定运行。为设备提供良好的物理防护，如安装防尘、防潮、防电磁干扰的外壳，设置专门的设备机房并控制机房的温度、湿度等环境参数。对设备进行定期巡检与维护，及时发现设备老化、损坏等问题并更换部件。软件方面，及时为设备操作系统和应用程序打补丁，修复已知漏洞。采用设备冗余设计，关键设备配备备用设备，当主设备出现故障时能迅速切换至备用设备，保障系统不间断运行。此外，对设备进行身份认证和访问控制，防止非法设备接入网络，干扰系统正常运行。

4.3 应急响应与恢复技术

建立完善的应急响应机制是应对热电厂电力监控网络系统突发安全事件的重要保障。制定详细的应急预案，明确在不同安全事件发生时的应急流程、责任分工和处置措施。组建专业的应急响应团队，定期进行应急演练，提高团队成员的应急处理能力和协同配合能力。当安全事件发生时，能够迅速响应，按照预案进行处置，如隔离受攻击的设备、停止受影响的服务等，防止事件进一步扩大。同时，做好数据备份与恢复工作，定期对系统中的重要数据进行备份，并将备份数据存储在异地安全场所。在系统遭受破坏后，能够利用备份数据快速恢复系统运行，将损失降到最低。事后对应急事件进行总结分析，吸取经验教训，不断完善应急预案和防护措施[5]。

结束语

热电厂电力监控网络系统的安全管理与防护，是保障电力稳定供应、维护社会正常运转的关键环节。通过建立健全安全管理制度、明确职责分工、强化人员培训与管理以及加强安全评估与监督等管理举措，为系统安全筑牢制度与人员防线。同时，运用网络安全、设备安全和应急响应恢复等防护技术，有效抵御各类内外部威胁。未来，随着技术发展，热电厂电力监控网络系统安全管理及防护需持续创新升级，以更先进理念、更完善体系、更强大技术，确保系统安全稳定，为电力行业高质量发展提供坚实支撑。

参考文献

[1]潘峰.水电厂电力监控系统安全防护策略浅析[J].中国新通信,2020,22(17):149-150.

[2]邓志平.水电厂电力监控系统的安全防护措施研究[J].大众标准化,2020(10):182-183.

[3]刘中坚.水电厂电力监控系统安全防护策略研究[J].电子制作,2020(Z2):87-88+12.

[4]宗和刚,张朝粤.水电厂网络安全态势感知系统的实现[J].水电站机电技术,2022,42(09):13-16+70.

[5]林茂.古田溪梯级水电厂智能化系统设计与应用[J].福建水力发电,2021(01):29-33.