电力监控系统中安全防护技术及措施探析

李绪蛟
安能二局电力发展建设（厦门）有限公司，福建 厦门 361000

DOI:10.61369/EPTSM.2025010025

摘　　要： 数字化时代，电力监控系统自动化程度不断提高，智能化程度不断提高，电力监控系统与外部网络的交互不断增多，网络攻击风险逐步上升。电力作为关键基础设施，监控系统一旦出现安全问题不仅会影响电力供应，还很有可能使不良影响波及其他行业。许多电力企业开始在电力监控系统中应用安全防护技术，以确保电力监控系统的可行性和有效性。本文主要对电力监控系统中安全防控技术及措施详细分析。电力企业可基于现阶段电力系统规模庞大，结构复杂，设备比较多，不同厂家设备和系统间的兼容性和安全性参差不齐，会增加安全管理难度，积极探索电力监控系统中安全防护技术及有效方法，确保安全防护技术和有效措施能使电力监控系统持续且稳定运行。

关 键 词： 电力监控系统；安全防护技术；措施

Analysis of Safety Protection Techniques and Measures in the Electric Power Monitoring System

Li Xujiao
Anneng Second Bureau Electric Power Development and Construction (Xiamen) Co., Ltd. Xiamen, Fujian 361000

Abstract: In the digital era, the automation and intelligence levels of electric power monitoring systems are constantly improving, and the interaction between electric power monitoring systems and external networks is increasing, leading to a gradual increase in the risk of cyber attacks. As a critical infrastructure, any security issues in the power monitoring system will not only affect power supply but also potentially cause adverse impacts on other industries. Many power companies have begun to apply security protection techniques in their power monitoring systems to ensure their feasibility and effectiveness. This paper mainly provides a detailed analysis of the security prevention and control techniques and measures in the electric power monitoring system. Based on the current large-scale and complex power system structure, as well as the numerous devices and varying compatibility and security among different manufacturers' equipment and systems, which increase the difficulty of security management, power companies can actively explore security protection techniques and effective methods in the electric power monitoring system. This ensures that security protection techniques and effective measures enable the sustained and stable operation of the electric power monitoring system.

Keywords: electric power monitoring system; security protection techniques; measures

引言

电力企业在电力监控系统中落实有效的安全防护技术，把控要点，可保障电力监控系统安全，让电力持续稳定供应，避免因停电造成的社会秩序混乱。防止因系统故障或安全事件导致的经济损失。基于电力是国家关键基础设施的核心，让监控系统的安全防护成为维护国家安全和保障能源安全的重要组成部分，以便于有效抵御外部势力对电力系统的破坏和干扰。电力企业可通过在电力监控系统优化中有效落实安全防护技术，落实可靠措施，达成既定的目标。

一、电力监控系统对安全防护技术的应用所需

电力监控系统对安全防护技术的应用需求体现于多个方面，以下便开展了详细的分析。第一，网络隔离技术。电力监控系统直接关系电力生产的安全性和稳定性，需要与外部网络进行有效隔离，这样才能防止外部网络攻击和恶意软件入侵。许多电力企业在电力监控系统优化中，应用专用物理隔离装置，借助物理隔离装置的作用实现生产控制区和信息管理区之间的单向或者双向隔离，可以保障数据的安全传输。第二，身份认证和访问控制。电力监控系统在运行的过程中需要对系统内的用户和设备进行严

格身份认证，确保只有经过授权的人员和设备才能访问监控系统的资源。许多电力企业利用访问控制技术，根据用户角色和权限，精细划分对不同数据和功能模块的访问级别，防止越权操作。第三，数据加密技术。电力监控系统中的数据涉及电网运行的关键信息，电力企业需要对电力参数和设备状态等关键数据在传输和存储过程中进行加密处理，这样才能确保数据的保密性。许多电力企业应用先进加密算法，防止数据被窃取，防止数据被篡改，确保数据的机密性，确保数据的完整性。

二、电力监控系统中安全防护技术应用案例

电力监控系统中安全防护技术的优秀应用案例有许多，效果十分显著。某电力企业在电力监控系统优化工作中应用安全防护技术时，在火电厂DCS系统中部署工控监测审计系统，对网络流量、异常事件、操作行为和数据内容等进行安全审计，实时警报异常行为并追踪溯源。另外，企业部署工控入侵检测系统，及时发现网络入侵行为，分析潜在威胁并报警，协助解决安全威胁。此外，企业在工控系统工程师站和操作员站交换机上各部署1台USB安全隔离装置，防止病毒和木马通过USB接口进入系统，解决USB移动设备接入工控系统无管控、无记录的问题。企业还各机组DCS系统网络中部署运维审计系统，实现设备集中管控，限制远程登录地址，审计用户操作权限和行为，提供会话审计和回放功能。某电力企业在探索电力监控系统中安全防护技术应用方法时，提出全流量电力协议解析算法，研制网络行为动态感知装置，实现对网络空间内资产及行为的关键节点、关键路径监测。另外，企业提出基于漏洞价值和资产价值和利用影响业务范围的工控漏洞定级方法，建立工控安全状态脆弱性评价模型，研制专用漏洞定级及脆弱性评价电力网络空间装备。此外，企业还研发网络威胁智能诊断组件，全要素精准量化分析威胁特征、攻击轨迹及危害范围，全方位检测电力网络系统脆弱性，将60000余座变电站、新能源场站的网络空间纳入威胁评估范围，威胁诊断准确率达99.7%。相关电力企业在进行电力监控系统优化时，可通过以实际案例为鉴，丰富安全防护技术应用经验，有效落实安全防护技术，确保电力监控系统优化工作执行的效率和质量。

三、电力监控系统中安全防护技术应用问题

（一）兼容性问题

电力监控系统包含众多不同厂商和不同时期的设备和软件，不同厂商和不同时期的设备和软件，通信协议和接口标准很有可能存在差异，会导致安全防护技术难以统一应用，影响安全防护技术的作用。举例而论，部分电力企业老旧设备不支持新的加密算法和安全协议，导致电力监控系统在运行的过程中，很难实现医治的安全防护策略。

（二）漏洞检测问题

电力监控系统规模大，结构复杂，存在许多潜在的安全漏洞，虽然部分电力企业在社会发展现阶段未紧随时代潮流应用漏洞扫描工具对漏洞进行检查，但由于系统特殊性和复杂性，很难确保所有漏洞都能被及时和准确的检测到。举例而论，部分电力企业在进行漏洞检测的过程中，针对一些涉及底层硬件或特定业务逻辑的漏洞要用常规扫描工具，并不能对潜在的问题及时发现，并不能对问题进行有效解决[1]。

（三）技术更新不及时

网络攻击技术不断发展，电力企业需要在电力监控系统优化工作中应用安全防护技术时，对技术不断更新，这样才能使技术具有现代化和智能化的特性，让技术发挥良好作用。但是，部分电力企业监控系统中的安全防护技术往往比较滞后，主要原因在于系统稳定性要求高，电力企业不敢轻易进行技术更新，或者电力企业因资金和技术人员等方面的限制，无法及时采用最新的安全防护技术[2]。

四、电力监控系统中安全防护技术的应用方法

（一）合理应用网络隔离技术

电力企业在监控系统优化工作中应用网络隔离技术时，可通过明确隔离区域划分和选择合适的物理隔离设备等达成既定的目标。电力企业在进行明确隔离区域划分的过程中，可清晰界定电力监控系统的安全区域，如生产控制大区和信息管理大区，基于控制区域涉及电力生产的直接控制安全要求比较高，非控制区相对低些，信息管理大区主要处理管理信息，实施不同强度的隔离措施，确保隔离措施与不同区域安全等级和功能所需相匹配，确保关键控制区的安全。电力企业在选择合适的物理隔离设备的过程中，可针对生产控制大区和信息管理大区之间应用物理隔离装置，提高工作效果。电力企业可给予正向隔离装置，允许数据从生产控制大区单向流向信息管理大区，可用于传输实时监测数据，反向隔离装置可在严格的安全控制下允许特定非实时数据从信息管理大区流向生产控制大区，如调度指令，有针对性选择隔离设备，让隔离设备有效防止网络攻击从信息管理大区渗透到生产控制大区中。电力企业为进一步提高网络隔离技术的应用效果，也可通过合理部署网络防火墙，利用网络防火墙进行逻辑隔离，确保工作成效。电力企业可在生产控制大区内部的不同子网之间，以及信息管理大学内不同部门网络之间，合理部署网络防火墙，让网络防火墙发挥良好作用。该过程中，电力企业可通过配置防火墙规则。依据源地址和目标地址以及端口号等条件，对网络流量进行过滤，对网络流量进行控制，限制非法访问和数据传输，以便于实现逻辑层的隔离[3]。

（二）合理应用身份认证和访问控制技术

电力企业在应用身份认证和访问控制技术的过程中，可通过选择合适身份认证方法和严格用户账号管理等达成既定的目标。电力企业在选择身份认证方式的过程中，可应用用户名和密码以及数字证书等多种方式，进行方式结合。具体实践中，电力企业可在输入正确用户名和密码之后，插入数字证书或通过生物特征验证，以便于提高身份认证的准确性，提高身份认证的安全性，防止身份被冒用。这一企业也可应用动态口令牌或者手机验证码

等方式，确保每次登录的口令不同，保障信息安全。让动态口令基于时间和事件等因素生成，抵御口令猜测和窃取攻击，有效增加攻击者的破解难度。电力企业在严格用户账号管理的过程中，可通过对用户账号创建和修改以及禁用进行严格管理，做好账号生命周期管理，提高管理水平。电力企业可让新用户经过审批流程创建账号，让离职和调岗人员及时禁用或删除账号，防止账号被非法应用。电力企业可根据用户工作职责和业务需求有针对性分配权限，如让普通操作人员只能进行数据查看和简单操作，让系统管理人员有配置和高级管理权限，管理好权责。电力企业为进一步提高身份认证和访问控制技术的应用效果，也可通过细化访问控制策略，让相关工作开展得更有意义和价值。电力企业通过将用户划分不同角色，划分成系统管理员和操作员以及工程师等，让每个角色都拥有相应的权限。让不同角色对数据和功能模块等系统资源有不同访问级别，方便管理和维护权限。电力企业也要注重做好基于属性的访问控制，除角色之外，考虑用户部门和工作地点以及时间等其他属性，制定访问控制策略，让访问控制得到良好管理[4]。

（三）合理应用数据加密技术

电力企业在应用数据加密技术的过程中，可通过选择合适加密算法和确保数据真实性和确保数据的完整性等达成既定的目标。电力企业在选择加密算法的过程中，可对大量数据的快速加密和解密需求，有针对性应用对称加密算法，确保加密算法的可行性和有效性。电力企业可应用高级加密标准，基于高级加密标准加密速度快和效率高，比较适用于电力监控系统中实时数据的加密，借助高级加密标准，对电力参数和设备状态信息等在传输过程中进行加密保护。电力企业也可在需要保证数据来源可靠性和不可抵触性的场景中，合理应用非对称加密算法，确保加密算法得到有效落实。该过程中，电力企业可在用户认证和数字签名等环节合理利用非对称加密算法对关键信息进行加密处理，确保数据的真实性，确保数据的完整性。此外，电力企业可依据实际情况应用哈希算法，即 SHA-256，对数据进行摘要处理，生成固定长度的哈希值，确保哈希算法在验证数据在传输或存储过程中是否被篡改时，发挥良好作用。电力企业为进一步提高数据加密技术应用的有效性，也可通过确定加密范围进一步提高技术应用效果。电力企业可对电力监控系统中不同设备之间和系统与外部通信的数据进行加密传输，如果在变电站与调度中心之间的数据通信链路中，合理应用加密隧道技术，对，数据进行加密处理，防止数据在传输的过程中被窃取，被篡改。电力企业针对存储在数据库和服务器硬盘等存储介质中的数据，也要注重做好加密存储。电力企业可通过应用数据库自带的加密功能或者第三方加密工具对敏感数据字段进行加密处理，确保用户账号信息和电力设备配置参数等信息得到良好保护[5]。

五、电力监控系统中安全防护技术的应用原则

电力企业在电力监控系统优化工作中探索安全防护技术应用方法时，要注重遵循安全分析原则和网络专用原则等，把控原则，提高工作效果。以遵循安全分区原则为例，电力企业要注重根据电力监控系统的功能和实时性以及重要性等因素合理划分安全区域，如果合理划分生产控制大区和信息管理大区，将生产控制大区细分为控制区和非控制区，确保不同安全区域实施不同等级的安全防护策略，确保关键控制区域的安全性。以遵循网络专用原则为例，电力企业要确保电力监控系统使用专用网络设备和通信线路，确保电力监控系统与外部公共网络物理隔离，通过避免使用公用网络进行电力监控数据传输，防止外部网络攻击，防止外部网络干扰让电力监控系统在实际运行的过程中，网络具有独立性和安全性的特点。以遵循安全审计原则为例，电力企业也要注重建立完善的安全审计机制，利用安全审计机制对电力监控系统的操作和访问进行全面记录和审计。如对审计日志进行分析，以便于及时发现潜在的安全问题和违规行为，以便于采取有效措施对问题进行处理，为安全事件追溯和调查提供相应的依据。

六、结语

结合以上论述的相关内容可具体总结为，电力企业基于电力系统是国家重要基础设施，电力系统稳定性是社会经济良性发展的重要保障，对电力监控系统进行优化提升，既可以提升企业综合发展实力，还可以促进社会发展。电力企业可通过积极引入并合理应用安全防护技术，促使电力监控系统强化功能。电力企业可通过合理应用网络隔离技术、合理应用身份认证和访问控制技术、合理应用数据加密技术等。借助可行性较强和有效性较强的安全防护技术，提高电力系统安全性，提高电力系统的稳定性。

参考文献

[1] 汤超 . 浅析电力监控系统网络安全监视体系建设 [J]. 机电信息 ,2020(32):142-143.

[2] 蒋涛 , 董贵山 , 杨乐怡 , 黄妮娜 . 新形势下电力监控系统网络安全风险分析与防护对策 [J]. 信息安全与通信保密 ,2022(04):79-84.

[3] 赵兴荣 . 如何提高水电厂电力监控系统网络安全防护水平 [J]. 云南水力发电 ,2021,37(09):162-164.

[4] 杨浩 , 陈宝靖 , 李燕 . 电力监控系统网络安全防护技术应用研究 [J]. 电子世界 ,2021(01):128-129.

[5] 郭丰 . 电力监控系统网络安全加固技术探讨 [J]. 网络安全技术与应用 ,2020(11):132-134.

