电力通信网络安全防护与风险评估研究

姜久雪 320981198501176484

摘要

电力通信网络是保障电力系统稳定运行的关键基础设施，随着智能电网建设推进与物联网、云计算技术的广泛接入，电力通信网络的开放程度不断提升，同时也面临着日益复杂的网络安全威胁。本文梳理了当前电力通信网络面临的主要安全风险类型，分析了现有安全防护体系存在的不足，构建了基于层次分析法的电力通信网络风险评估模型，并提出了针对性的安全防护优化策略。研究结果表明，系统化的风险评估能够精准识别电力通信网络的薄弱环节，动态分层的防护体系能够有效提升电力通信网络的安全韧性，为电力系统的安全稳定运行提供支撑。

关键词：电力通信网络；安全防护；风险评估；层次分析法

一、引言

电力系统是国家关键信息基础设施的核心组成部分，电力通信网络作为电力系统的"神经中枢"，承担着电力调度控制、生产运营数据传输、业务管理信息交互等核心功能，其安全性直接关系到整个电力系统的稳定运行与国家能源安全。近年来，随着智能电网建设的不断深入，新能源并网、分布式能源、电动汽车充电网络等新业务快速发展，大量智能终端、物联网设备接入电力通信网络，使得原本相对封闭的电力通信网络逐渐向开放互联的方向转变。与此同时，全球范围内针对电力系统的网络攻击事件频发，攻击手段不断升级，从最初的病毒感染发展到定向勒索攻击、工控系统渗透等复杂攻击形式，给电力系统造成了巨大的经济损失与社会影响。在此背景下，深入研究电力通信网络的安全风险，构建科学的风险评估体系，完善安全防护策略，已经成为电力领域亟待解决的重要课题。

二、电力通信网络的安全风险分析

2.1 网络结构与设备层面风险

当前我国电力通信网络呈现出分层分区的结构特征，核心骨干网覆盖全国，区域接入网延伸到各类终端节点，网络结构复杂，节点数量庞大。一方面，部分老旧通信设备服役时间较长，存在硬件设计缺陷、固件漏洞无法及时更新等问题，

这些设备往往部署在偏远的变电站、发电站等区域，防护措施薄弱，容易成为网络攻击的突破口。另一方面，随着无线通信、电力载波等新型通信技术的应用，无线接入环节的加密机制不完善，容易被攻击者窃听、篡改数据，甚至发起中间人攻击，非法接入电力通信网络。此外，电力通信网络中不同业务系统之间的边界防护不足，部分跨区业务交互未设置严格的访问控制策略，一旦某一个区域被攻破，攻击者很容易横向移动，渗透到核心业务系统。

2.2 数据与应用层面风险

电力通信网络每天传输海量的生产数据与用户信息，包括电力调度指令、电网运行参数、用户用电信息等敏感数据，这些数据的完整性、保密性与可用性是电力系统正常运行的基础。当前数据层面存在的风险主要包括三个方面：一是数据传输过程中加密防护不到位，部分早期建设的业务系统未采用高强度加密算法，数据容易被截获篡改；二是数据存储环节存在漏洞，部分电力企业的数据存储系统访问控制不严，存在数据泄露的风险；三是恶意软件与勒索病毒的威胁，近年来针对电力企业的勒索攻击事件不断增加，攻击者通过加密电力系统核心数据索要赎金，严重影响电力系统的正常运行。应用层面，电力通信网络承载的各类业务应用，包括调度自动化系统、配电管理系统、营销管理系统等，部分应用存在代码漏洞、权限管理混乱等问题，容易被攻击者利用获取非法权限。

三、电力通信网络风险评估模型构建

科学的风险评估是开展安全防护的基础，只有精准识别风险、量化风险等级，才能针对性地配置防护资源，提升防护效果。本文采用层次分析法构建电力通信网络风险评估模型，将风险评估划分为目标层、准则层、指标层三个层级。

目标层为电力通信网络整体安全风险等级，准则层分为四个维度：设备层风险、网络层风险、数据层风险、管理层风险，每个准则层下设置具体的评估指标，具体指标体系如下：设备层风险包括设备老旧程度、漏洞覆盖率、物理防护强度；网络层风险包括边界防护强度、访问控制完善性、入侵检测覆盖率；数据层风险包括数据加密强度、数据备份完整性、访问权限合理性；管理层风险包括安全制度完善性、人员安全意识、应急响应能力。

通过邀请电力安全领域专家对各指标的重要性进行打分，构建判断矩阵，计算各指标的权重，并进行一致性检验，最终得到各指标的权重值，其中数据层风

险权重为 0.35，网络层风险权重为 0.28，设备层风险权重为 0.20，管理层风险权重为 0.17，说明数据与网络层面的风险对电力通信网络整体安全的影响最大。通过对具体电力通信网络的各指标进行打分，结合权重计算得到整体风险得分，将风险划分为低风险、中风险、高风险三个等级，为安全防护决策提供依据。该模型能够将定性分析与定量计算结合，有效解决了电力通信网络风险难以量化的问题 。

四、电力通信网络安全防护优化策略

4.1 构建动态分层的安全防护体系

针对电力通信网络分层分区的结构特征，构建分层纵深防护体系，在物理层、网络层、应用层、数据层分别部署针对性的防护措施。物理层面，加强核心通信节点、重要变电站的物理防护，完善门禁、监控、防雷、防断电措施，保障硬件设备的物理安全。网络层面，严格落实区域边界防护，采用虚拟局域网划分、防火墙、入侵检测系统构建边界安全防线，实现不同安全区域之间的逻辑隔离，严格控制跨区域访问行为。应用层面，定期开展应用漏洞扫描与渗透测试，及时修复已知漏洞，完善身份认证与权限管理机制，采用多因素认证方式提升身份认证的安全性。数据层面，对敏感数据进行全生命周期保护，传输环节采用国密算法进行加密，存储环节完善备份机制，采用异地多活备份方式保障数据的可恢复性。

4.2 完善风险评估与应急响应机制

建立常态化的风险评估机制，定期对电力通信网络开展全面风险评估，针对新接入的系统与设备开展专项风险评估，及时发现新增风险，动态调整防护策略。构建风险预警机制，依托大数据分析技术对网络攻击特征进行分析，提前识别潜在的攻击威胁，发布风险预警。完善应急响应体系，制定分级分类的应急预案，针对不同类型的网络安全事件明确处置流程与责任分工，定期开展应急演练，提升应急处置能力。建立攻击事件复盘机制，对发生的安全事件进行深入分析，总结经验教训，不断完善防护体系与应急预案。

五、结论

电力通信网络的安全是电力系统稳定运行的基础，在当前网络威胁日益复杂的背景下，传统的安全防护模式已经难以适应电力通信网络发展的需求。本文通过对电力通信网络面临的安全风险进行系统梳理，构建了基于层次分析法的风险评估模型，能够实现风险的量化评估与精准识别，在此基础上提出的动态分层防护体系与常态化风险管控策略，能够有效提升电力通信网络的安全防护能力。未来随着电力系统数字化转型的不断推进，电力通信网络还将面临更多新型安全威胁，需要持续深化风险评估技术研究，不断完善安全防护体系，保障电力系统的安全稳定运行。

参考文献

[1] 张涛, 赵东艳, 王磊. 智能电网环境下电力通信网络安全防护体系研究[J]. 中国电力, 2020, 53(8): 121-128.

[2] 刘玉磊, 刘常坤, 刘树田. 电力通信网络风险评估方法与防护策略研究[J]. 电力信息与通信技术, 2019, 17(5): 45-50.

[3] 陈星豪, 李涛. 基于层次分析法的电力通信网安全风险评估[J]. 计算机工程与应用, 2018, 54(12): 221-226.