 DOI: https://doi.org/10.12345/dlynyqy.v2i12.22662

Construction and Upgrading of the Power Communication Network Security Protection System

Hongyu Sheng

State Grid Northeast Branch Yunfeng Power Plant, Tonghua, Jilin, 134000, China

Abstract

As an important part of the power system, the security of the power communication network is crucial to the stable operation of the power grid and the energy supply. With the rapid development of information technology and the increasingly complex network attack means, the power communication network is facing an increasingly severe security threat. Based on the characteristics of power communication network, this paper systematically analyzes the key requirements and main challenges of security protection, puts forward a set of targeted and advanced security protection system construction scheme, and discusses its upgrade path. By adopting multi-layer protection, active monitoring and dynamic response mechanism, the anti-risk ability of the power communication network can be effectively improved to provide technical support for the safe operation of the power grid.

Keywords

power communication network; network security; protection system; security upgrade; dynamic response

电力通信网络安全防护体系构建与升级

盛红玉

国网东北分部云峰发电厂，中国 · 吉林 通化 134000

摘　要

电力通信网络作为电力系统的重要组成部分，其安全性对电网的稳定运行和能源供应至关重要。随着信息技术的快速发展和网络攻击手段的日益复杂，电力通信网络面临着愈加严峻的安全威胁。论文结合电力通信网络的特点，系统分析其安全防护的关键需求和面临的主要挑战，提出一套针对性强、技术先进的安全防护体系构建方案，并对其升级路径进行了探讨。通过采用多层防护、主动监测和动态响应机制，可以有效提升电力通信网络的抗风险能力，为保障电网安全运行提供技术支持。

关键词

电力通信网络；网络安全；防护体系；安全升级；动态响应

1 引言

随着智能电网和信息化技术的深度融合，电力通信网络已经成为现代电网的重要支撑平台，为电力调度、运行管理和远程控制提供了关键通信保障。然而，这一网络也成为潜在网络攻击的重要目标。一方面，电力通信网络的开放性和互联性使其容易受到外部攻击，例如恶意软件传播、分布式拒绝服务攻击（DDoS）等。另一方面，内部的管理疏漏或设备漏洞也可能成为威胁的切入点。近年来，全球范围内多起针对电力系统的网络攻击事件表明，网络安全问题已经成为威胁电力系统安全的重要因素 [1]。

传统的安全防护措施往往以静态防御为主，缺乏对复杂威胁的快速感知和动态响应能力，难以满足当前网络安全防护的需求。因此，构建一套以主动防御为核心的电力通信网络安全防护体系，已经成为行业发展的关键任务。论文从电力通信网络的实际需求出发，系统分析其安全防护的现状与问题，提出基于多层次安全架构的防护体系，并探讨其在技术手段和管理机制上的升级策略，为电力通信网络的安全保障提供科学参考。

2 电力通信网络安全现状分析

2.1 电力通信网络的特点与安全需求

电力通信网络具有高可靠性、高实时性和多样性等显著特点，支撑着现代电网的核心功能，包括电网调度、远程数据采集与控制、设备状态监测等。这些功能的高效运行要求通信网络具备高带宽、低延迟和强抗干扰素力，以满足电力系统对数据传输的高精度和高可靠性的需求。然而，随着网络规模的不断扩大和接入设备种类的多样化，电力通信网络的安全需求也随之变得更加复杂和多样化。例如，在智能

【作者简介】盛红玉（1975–），女，满族，中国辽宁丹东人，本科，工程师，从事电力通信研究。

电网场景中，物联网设备的大量接入使得网络边界模糊化，进一步增加了攻击面和管理难度，如何确保物联网终端的安全接入成为关键挑战之一。同时，随着 5G 通信和边缘计算的引入，电力通信网络的拓扑结构更加复杂，边缘节点和数据中心的安全性直接影响整个网络的稳定性和运行效率 [2]。

此外，电力通信网络中的数据种类繁多，从实时运行数据到预测性分析数据，再到远程监控数据，均对数据传输的保密性、完整性和可用性提出了更高的要求。

2.2 面临的主要安全威胁

当前，电力通信网络面临的安全威胁主要包括以下几个方面：

①外部攻击：如恶意软件攻击、网络钓鱼、DDoS 攻击等，这些攻击可能导致通信中断或关键数据泄露。

②内部威胁：由于管理疏漏或权限控制不当，内部人员可能无意或故意引发安全事件。

③设备漏洞：嵌入式设备固件中的漏洞可能被黑客利用，成为攻击的突破口。

④数据篡改与泄露：在数据传输过程中，攻击者可能通过中间人攻击篡改或窃取关键信息，威胁电网运行的可靠性。

2.3 现有防护措施的不足

尽管电力通信网络已经部署了防火墙、入侵检测系统（IDS）等安全设施，但这些传统手段往往存在以下不足：

①被动性：多数防护措施以静态规则为主，难以应对新型攻击手段。

②孤立性：各防护模块之间缺乏协同，难以实现全面的威胁感知。

③响应滞后：对于复杂攻击场景，现有系统的威胁检测和响应速度较慢，容易导致严重后果。

3 电力通信网络安全防护体系的构建

3.1 多层次安全架构设计

为应对复杂的安全威胁，电力通信网络安全防护体系应采用多层次的架构设计，包括网络层、设备层、数据层和应用层的协同防护：

①网络层防护：部署分布式防火墙、虚拟专用网（VPN）和加密技术，确保网络传输的安全性。

②设备层防护：加强终端设备的安全认证和固件升级管理，避免因设备漏洞导致的安全风险。

③数据层防护：引入数据完整性校验机制和分布式存储技术，确保数据的真实性和可用性。

④应用层防护：针对电力调度、远程控制等关键应用，采用访问控制和操作日志记录等手段，防止非法操作。

3.2 主动监测与动态响应机制

传统的静态防护手段在面对动态变化的安全威胁时显得力不从心，因此需要构建以主动监测和动态响应为核心的防护机制：

①实时监测：部署网络流量监控和异常行为检测系统，实时捕捉潜在威胁。

②智能分析：基于人工智能算法，对安全事件进行关联分析，快速识别攻击模式。

③动态响应：结合威胁等级和攻击类型，自动触发安全策略调整，如封禁可疑 IP、隔离受感染节点等。

4 电力通信网络安全防护的升级策略

4.1 基于人工智能的智能化防护

人工智能技术在网络安全中的应用日益广泛，为提升电力通信网络的安全防护能力提供了重要契机。深度学习模型能够通过训练大规模的历史数据来识别异常流量，尤其在应对复杂的多态攻击模式时表现出色。传统规则驱动的检测方式难以适应动态变化的攻击行为，而人工智能模型可以通过自适应算法进行实时学习，识别潜在威胁。此外，基于机器学习的分类算法能够在高维数据中快速定位恶意活动，从而减少误报和漏报的情况 [3]。

人工智能还可以帮助构建全面的态势感知系统，通过整合来自网络、主机和终端设备的数据，实现跨域威胁的综合分析。例如，异常检测算法不仅能够发现单点攻击，还能够识别跨系统或分布式攻击的关联行为。此外，通过应用强化学习，网络可以根据实时威胁动态调整自身配置，从而提升防御能力。与传统防护措施相比，人工智能驱动的智能化防护不仅更高效，还能在攻击发生前提前预测并采取预防措施。未来，随着 AI 技术的进一步发展，深度神经网络、联邦学习等新兴技术将为电力通信网络的安全防护注入更多创新动能。

4.2 强化安全管理机制

除了技术手段的升级，加强电力通信网络的安全管理机制同样至关重要。

首先，权限管理体系需要更加精细化。通过基于角色的访问控制（RBAC）和基于属性的访问控制（ABAC）模型，可以实现不同用户和角色的分级授权，从而避免权限滥用和越权操作。对于关键岗位和敏感操作，还应引入双因素认证、行为审计等多重验证手段，进一步提升安全性。

其次，安全意识培训是网络安全管理的重要组成部分。员工往往是防护体系中的薄弱环节，攻击者常通过社会工程学等方式对其进行攻击。定期组织网络安全培训和模拟攻击演练，可以提高员工识别威胁的能力和应对突发事件的水平。此外，通过设立奖励机制，鼓励员工发现并上报潜在的安全隐患，有助于构建全员参与的安全文化。

最后，建立统一的安全事件管理平台对于提升事件响应效率至关重要。通过将事件检测、分类、溯源和响应集成到一个平台中，可以实现全网的安全事件集中管理。配合自动化安全编排与响应（SOAR）技术，该平台能够在发现威

胁后快速协调多方资源进行处理，减少人为干预可能带来的延迟和失误。这种集中化的管理模式不仅提升了事件处理的效率，还能为管理者提供全面的安全态势视图，支持更科学的决策。

4.3 推进标准化与协同防护

电力通信网络的复杂性和多样性决定了其安全防护需要标准化与协同化的支持。

首先，行业内需加快制定统一的安全标准，包括设备接口、数据格式和通信协议等，以确保不同系统和设备之间能够无缝对接。这种标准化建设可以有效减少因兼容性问题导致的安全隐患，同时提升全行业的防护水平。

其次，协同防护是应对大规模攻击的重要手段。在区域性或国家级电力通信网络中，攻击往往具有连锁效应，仅靠单一机构的力量难以应对。通过建立跨机构的威胁情报共享机制，各方可以及时共享攻击信息、漏洞情报和防护策略，从而实现快速联动。例如，某地发生大规模 DDoS 攻击时，各相关机构可以通过协同平台共享实时流量数据，联合实施流量清洗和源头封堵，减少攻击影响范围。

最后，国际合作也具有重要意义。近年来，跨国界的网络攻击事件频发，单一国家或地区的应对能力有限。通过参与国际标准化组织、建立全球性的威胁情报网络，国内电力企业可以借鉴国际先进经验，同时贡献自身的安全防护技术，共同提升全球电力通信网络的安全水平。

5 应用案例与效果评估

5.1 某省电力公司网络安全体系实践

某省电力公司通过引入多层次防护架构和主动监测技术，显著提升了电力通信网络的安全性。其安全体系的核心包括实时流量监测、终端设备加固以及分布式威胁响应模块。通过部署基于 AI 的流量监控系统，该公司能够在大量网络数据中迅速识别异常行为。数据显示，该系统上线后，攻击检测率提高了 40% 以上，误报率降低了 20%。

设备层的安全升级也取得了显著成效。例如，该公司实施了设备固件的自动升级管理，同时引入定期漏洞扫描机制，有效防止了因设备老化或固件缺陷导致的安全问题。在管理方面，该公司建立了统一的安全事件响应中心，整合了入侵检测、日志分析和应急响应等多项功能。在一次针对某变电站的攻击中，响应中心通过自动化分析迅速定位了攻击源，并在 5 分钟内采取了隔离措施，避免了更大范围的影响。这一案例充分证明了多层次防护架构和主动监测技术的实用性与可靠性。

5.2 国际电网企业的经验借鉴

国外一些电网企业在网络安全防护中取得了显著成果，尤其是在零信任架构的应用方面表现突出。零信任架构的核心理念是“不信任任何人，无论内部还是外部”，通过细粒度的权限控制和动态身份认证，最大程度降低内部威胁的风险。例如，美国某大型电网企业在其通信网络中部署了零信任解决方案，严格限制每个用户和设备的访问权限。其系统还集成了行为分析模块，能够实时监测用户活动，并在发现异常行为时自动触发响应 [4]。

这一实践经验表明，零信任架构不仅适用于企业内部网络，也对复杂的电力通信网络具有重要的参考价值。国内电力企业可以结合实际需求，逐步引入零信任模型，同时完善身份认证和访问控制机制，从而显著提升整体安全水平。

6 结语

电力通信网络的安全防护不仅是技术问题，更是管理与协作的综合考验。随着网络威胁的不断演变，传统的静态防护手段已难以满足需求。论文提出了一套以智能化、多层次架构和协同防护为核心的防护体系，结合实际案例分析了其应用效果和实施路径。这些策略不仅能够有效提升电力通信网络的抗攻击能力，还能为其他关键基础设施的安全保障提供参考。

未来，随着人工智能、大数据、区块链等新技术的持续发展，电力通信网络的安全防护将进入新的阶段。在这一过程中，加强行业标准化建设、推动多方协同合作、借鉴国际先进经验，将为保障电网稳定运行和能源供应安全奠定坚实基础。

参考文献

[1] 陈雪,林奕夫.基于边缘计算的电力网络安全威胁等级评估研究[J/OL].自动化技术与应用,1-7[2024-12-12].http://kns.cnki.net/kcms/detail/23.1474.TP.20241203.1559.101.html.

[2] 朱曙,冉月,赵慧明.基于IEC 61850标准的配电站网络攻击模型研究[J/OL].自动化技术与应用,1-6[2024-12-12].http://kns.cnki.net/kcms/detail/23.1474.TP.20241203.1431.040.html.

[3] 何嫱君.等级保护2.0标准下职业院校安全通信网络研究与设计[J].网络安全技术与应用,2024(12):91-93.

[4] 蒋小莉,刘茂彬,吴家奇.电力系统信息通信网络安全问题及措施分析[J].光源与照明,2024(11):228-230.