

数字新基建下的电力网络安全防护体系研究

苏宇

国网四川省电力公司资阳供电公司

摘要: 在数字化时代下, 电力网络逐渐成为国家基础设施的关键组成部分, 其安全性直接影响着社会经济的稳定与发展。在数字新基建的背景下, 电力网络安全防护体系的研究变得尤为重要, 这不仅涉及保护关键基础设施不受网络攻击和物理破坏的问题, 还包括确保电力系统的稳定运行和数据安全方面。随着技术的进步, 电力网络面临的安全威胁日益复杂多变, 深入研究并构建一个有效的安全防护体系, 对于预防和应对这些挑战至关重要, 这不仅有助于保障国家安全和公共安全, 也是推动经济持续健康发展的必要条件。

关键词: 数字新基建; 电力网络; 安全防护体系

【DOI】10.12252/j.issn.2096-6288.2022.10.117

电力网络安全现状受到数字化转型的深刻影响, 安全风险日益增加。随着物联网、云计算等技术的广泛应用, 电力网络变得更加复杂和互联, 这使得它易受到网络攻击和系统入侵。另外, 电力系统的自动化和智能化也带来了新的挑战, 比如数据泄漏和系统故障的风险增加。同时, 电力网络的物理设施也面临着自然灾害、恶意破坏等传统安全威胁, 这些风险不仅威胁到了电力供应的连续性和可靠性, 还可能导致重大的经济损失和社会不稳定。因此, 加强电力网络的安全防护, 应对数字化转型带来的挑战, 已成为确保能源安全和社会稳定的重要任务。

一、数字新基建在电力网络领域的应用

数字新基建主要涵盖云计算、大数据中心、物联网以及5G通信网络等技术, 这些技术在电力网络中的应用不仅提高了能源管理的效率和灵活性, 而且增强了电网的稳定性和可靠性。云计算为电力网络提供了强大的数据处理能力, 使得大规模数据的存储、分析和利用变得更加便捷高效。通过大数据技术, 电力公司能够实时监控电网运行状态, 预测和优化能源分配, 减少浪费, 同时提高对突发事件的响应能力。物联网技术在电力网络中的应用, 如智能电表和传感器的广泛部署, 使得电网能够实时收集终端用户的用电数据, 从而实现更精准的电能供需匹配和负荷管理。此外, 5G通信网络的高速度和低延迟特性对于实现电力系统的实时监控和控制至关重要, 尤其是在分布式能源和可再生能源日益增多的背景下。综上所述, 数字新基建的技术在电力网络中的应用, 不仅极大地提升了电网的智能化水平, 也为可持续能源发展和智慧城市建设提供了坚实的基础。

二、电力网络安全防护体系构建原则

(一) 综合性防护

构建电力网络安全防护体系的核心原则之一是实现综合性防护。这要求在技术、管理和策略层面采取多元化的措施, 形成一个全方位、多层次的安全保障体系。从技术角度来看, 应包括但不限于加强网络边界的防御、内部网络的隔离与监控, 以及对关键设备和系统的加固。特别是在网络边界防御方面, 需要利用防火墙、入侵检测系统和入侵预防系统等技术, 以防止未经授权的访问和攻击。同时, 内部网络监控和隔离是防止潜在威胁扩散和减少攻击面的关键, 通过实施网络分段和访问控制策略, 可以有效地隔绝和限制攻击者的活动空间。

此外, 对关键控制系统的加固也是至关重要的。这包括实施严格的物理安全措施, 如对关键设施的访问控制, 以及确保数据传输的加密和完整性。对于数据的安全存储和处理, 采用高级加密标准和持续的安全审计是必不可少的措施。在管理层面, 建立一套完善的安全管理体系是保障电力网络安全的关键。这包括制定全面的安全政策、程序和标准, 以及定期对员工进行安全意识培训。此外, 通过实施定期的安全审计和风险评估, 可以及时发现并纠正安全漏洞, 从而降低潜在的安全风险。策略层面的安全防护则涉及更为广泛的方面, 包括与政府、行业组织以及其他相关机构的协作。通过分享最佳实践、安全威胁信息以及应对策略, 可以提高整个行业的安全防护水平。同时, 配合政府制定的相关法规和标准, 对于提升电力网络的安全防护具有重要意义。

(二) 层次化管理

层次化管理是电力网络安全防护体系构建的另一个核心原则, 它强调在不同层面采取相应的管理和技术措施, 以形成有效的安全防护。在最基础的物理层面, 这涉及电力设施的物理安全, 包括但不限于对关键设施的

严格访问控制、监控摄像头的部署以及对重要区域的环境监控。这样的物理层面措施能够防止未授权的物理访问和潜在的破坏行为。网络层面的安全管理则聚焦于保护电力网络免受网络攻击和未授权访问。这包括使用先进的防火墙技术、入侵检测系统以及网络分割技术。网络分割，尤其是将关键的控制系统与其他网络隔离，可以有效减少网络攻击的范围和影响。同时，实施严格的网络访问控制和身份验证机制，确保只有授权人员可以访问敏感和关键的网络资源。

在应用层面，关注点在于确保所有运行在电力网络中的应用程序和服务的安全性。这涉及对应用程序的持续安全测试、漏洞扫描以及定期的更新和打补丁。此外，对数据的安全处理和存储也是应用层面管理的重要组成部分，比如实施数据加密和采用安全的数据备份策略。从组织管理的角度来看，层次化管理还包括制定和实施一系列安全政策和程序，确保整个组织在安全防护方面的一致性和有效性。这包括但不限于对员工进行定期的安全培训、建立应急响应和事故处理机制，以及实施定期的安全审计和风险评估。

（三）动态性和适应性

在电力网络安全防护体系的构建中，动态性和适应性原则扮演着至关重要的角色，这意味着安全体系需要能够灵活地应对不断变化的威胁景观和技术环境。动态性体现在安全体系能够实时监测网络状态和安全威胁，并根据检测到的信息做出快速响应。此外，安全系统应具备自学习能力，能够根据历史数据和新出现的威胁模式不断调整其检测和响应策略。

适应性则要求安全体系能够适应技术发展和业务需求的变化。随着电力网络技术的不断进步，如分布式能源、智能电网和可再生能源技术的融入，安全体系需要能够适应这些新技术的特点和要求。例如，安全策略和措施需要适应分布式能源系统的分散性和可再生能源的不确定性。同时，随着电力网络越来越多地依赖于远程控制 and 自动化，安全体系也需要更新以保护这些新的通信和控制系统。

此外，适应性还体现在对法规和标准变化的响应能力。随着国家和国际对电力网络安全的关注度提高，相关法规和标准也在不断更新。电力网络的安全体系需要能够及时适应这些新的法规要求，确保合规性。在实践中，动态性和适应性原则要求安全团队保持持续的学习

和改进态度，定期评估和更新安全策略和技术，确保安全措施与当前的威胁和技术环境保持一致。这不仅包括对安全技术的升级，也涉及安全管理流程和人员培训的更新，确保整个组织能够有效地应对不断变化的安全挑战。

三、电力网络安全防护技术探究

（一）物理层面的安全措施

电力网络的物理层面安全措施是保护关键基础设施不受物理威胁的基础。这些措施主要包括增强电力设施的物理防护、提升监控能力以及实现环境安全。加强电力设施的物理防护包括构建围栏、安装防爆门窗以及实施严格的出入口控制，以防止未经授权人员进入重要设施。例如，电力变电站和控制中心等关键区域可以通过设置生物识别门禁系统，如指纹或虹膜扫描，来控制人员访问。监控能力的提升则涉及安装高清摄像头、感应器以及报警系统，以便实时监控设施状态和周围环境，及时发现和响应任何异常情况。例如，通过部署红外线和运动检测器可以在未经授权的入侵发生时立即触发警报。此外，监控系统通常与本地公安部门或安全中心联网，确保在紧急情况下能够快速响应。

环境安全的确保也是物理层面安全措施的重要组成部分，它包括对电力设施的环境条件进行实时监测，如温度、湿度和水位等，以预防由环境因素引起的设备故障或损坏。例如，通过安装温湿度传感器和水位报警器，可以及时发现变电站内部的异常环境条件，并采取措​​施防止设备损坏。除了上述措施，电力网络的物理层面安全还包括确保关键设备的冗余和备份。这意味着对关键组件，如变压器和控制系统，进行冗余设计，以保证在一部分设备失效时，电力网络仍能继续运行。此外，对电力网络中的关键数据和配置进行定期备份，确保在数据丢失或系统损坏的情况下能够快速恢复。

（二）网络层面的安全技术

在电力网络的网络层面，安全技术的重点在于防止网络攻击和保障数据传输的安全性。这包括实施强大的网络边界防御、内部网络安全监控，以及数据传输的加密和完整性保护。网络边界防御通常依赖于防火墙和入侵检测系统（IDS），这些系统能够有效识别和阻止来自外部的恶意流量和攻击尝试。例如，现代防火墙不仅能够基于端口和IP地址过滤流量，还能进行深度包检查（DPI），从而识别并阻止复杂的网络攻击，如拒绝服

务攻击（DoS）和分布式拒绝服务攻击（DDoS）。

内部网络的安全监控则更多侧重于网络行为的分析和异常检测。通过部署网络行为分析工具（NBA）和安全信息与事件管理系统（SIEM），可以实时监控网络中的活动，如数据流量模式和用户行为，以便及时发现内部威胁或已经发生的入侵。例如，通过分析网络流量的异常模式，如突然的流量增加或不寻常的访问尝试，可以及时发现并响应内部网络的安全事件。数据传输的安全性是另一个关键领域，尤其是在电力网络中，数据的准确性和完整性对于系统运行至关重要。为此，采用端到端的加密技术，如传输层安全协议（TLS）和安全套接层（SSL），可以确保数据在传输过程中的保密性和完整性。此外，对关键数据的数字签名也是常见的做法，它可以验证数据的来源和完整性，防止数据被篡改。

除了上述措施，网络层面的安全还涉及对网络设备和系统的持续管理和维护。这包括定期更新网络设备的固件和软件，以修补已知的安全漏洞，以及对网络配置的定期检查，确保符合最佳安全实践。例如，对路由器和交换机等网络设备进行定期的漏洞扫描和配置审计，可以确保这些设备不成为网络攻击的薄弱环节。电力网络的网络安全层面安全技术需要综合考虑边界防御、内部监控和数据传输保护等多个方面，通过这些措施构建一个全面且强大的网络安全防护体系。

（三）数据层面的安全策略

数据层面的安全策略在电力网络中至关重要，其核心在于确保数据的保密性、完整性和可用性。数据加密是保护数据保密性的首要手段，特别是在存储和传输过程中。采用强加密算法，如AES（高级加密标准）和RSA，可以有效防止敏感数据，比如用户信息和电力使用数据，在存储或传输过程中被未经授权访问或窃取。此外，对数据进行分类和分级管理，确保只有授权用户才能访问特定级别的数据，也是保障数据保密性的重要策略。保障数据完整性则涉及确保数据在存储、处理和传输过程中不被篡改。实现这一目标的方法包括使用数据校验和数字签名。数据校验和可以在数据传输结束后验证数据的完整性，而数字签名则提供了一种验证数据来源和完整性的机制，确保数据在传输过程中未被篡改。例如，对电力监测数据实施数字签名，可以在数据到达控制中心时验证其真实性和完整性。

确保数据可用性是数据层面安全策略的另一个关键

方面。这通常通过实现数据备份和灾难恢复计划来实现。定期备份关键数据，并在安全的地理位置存储多个副本，可以确保在发生数据丢失或系统故障时，关键数据能够迅速恢复。此外，实施灾难恢复计划和维护备用系统，确保在主系统出现故障时能够迅速切换，从而保证电力网络的连续运行。除了上述措施，数据层面的安全还涉及对数据访问的严格控制和审计。实施细粒度的访问控制，比如基于角色的访问控制（RBAC），可以确保用户只能访问其角色所需的数据。同时，对所有数据访问活动进行记录和审计，可以在发生安全事件时提供关键的信息，帮助追踪和响应安全威胁。

结语

展望未来，电力网络的安全防护将面临更加复杂多变的挑战，但同时也将得益于技术的不断进步。随着物联网、云计算等先进技术的进一步发展和应用，电力网络的管理和运行将变得更加智能和高效。然而，这也意味着安全威胁将更为隐蔽和多样化，对安全防护体系提出了更高的要求。因此，持续地创新和改进，以及对新兴技术的深入理解和适应，将是确保电力网络安全的关键。同时，跨领域合作，如与网络安全、人工智能和数据科学等领域的融合，也将为电力网络安全带来新的视角和解决方案。面对未来的挑战和机遇，电力网络的安全防护需要不断地进化和升级，以保护这一至关重要的基础设施，支撑社会的持续发展和繁荣。

参考文献

- [1] 余明阳, 查志勇, 詹伟, 梁航函, 吴耿. 电力监控系统网络安全防护方案的研究与设计[J]. 电子世界, 2021, (05): 142-143.
- [2] 刘超, 张鹏, 强仁, 赵毓鹏, 鞠伟, 夏永欣, 袁琳琳. 数字新基建下的电力网络安全防护体系研究[J]. 华电技术, 2021, (02): 60-65.
- [3] 孙静. 电力监控系统网络安全防护体系建设[J]. 数字通信世界, 2020, (10): 160-161.
- [4] 胡倩云. 电力监控系统网络安全防护体系建设[J]. 技术与市场, 2020, (04): 93-94.
- [5] 姜再能, 郭翔, 郭丰. 电力监控系统网络安全防护体系建设研究[J]. 数字通信世界, 2020, (02): 265.
- [6] 陈正. 电力监控系统网络安全防护体系建设[J]. 电工技术, 2019, (03): 106-107.