智能电网环境下关键基础设施信息安全防护体系研究

李 岳 江 长 林一方
国网浙江省电力有限公司青田县供电公司 浙江 丽水 323900

摘 要：本文聚焦智能电网环境下关键基础设施的信息安全防护问题。首先分析智能电网关键基础设施的范畴与信息安全面临的挑战，阐述构建信息安全防护体系的必要性；接着从技术、管理、人员三个维度探讨防护体系的核心要素；然后提出基于多维度融合的防护体系构建策略，并分析其运行机制与优势；最后通过实际案例验证防护体系的有效性，为智能电网关键基础设施的信息安全保障提供理论支持与实践参考。

关键词：智能电网；关键基础设施；信息安全防护体系；多维度融合

引言

智能电网作为现代能源体系的核心组成部分，融合了先进的传感测量、通信、信息技术，实现了电网的智能化运行与管理。然而，随着智能电网信息化、自动化程度的不断提高，其关键基础设施面临着日益严峻的信息安全威胁。关键基础设施一旦遭受攻击，可能导致电网瘫痪、能源供应中断，进而影响社会经济的正常运行和人民生活。因此，构建一套科学、有效的信息安全防护体系，保障智能电网关键基础设施的信息安全，已成为当前亟待解决的重要问题。

1 智能电网关键基础设施及其信息安全挑战

1.1 智能电网关键基础设施的范畴

智能电网关键基础设施贯穿于发电、输电、变电、配电、用电等电力生产与消费的各个环节，是一个由众多信息化设备与系统相互关联、协同工作构成的复杂系统。在发电环节，分布式能源接入系统是关键基础设施的重要组成部分。随着可再生能源的大规模开发利用，大量的分布式电源如太阳能光伏电站、风力发电场等接入电网。这些分布式能源接入系统通过智能控制设备和通信技术实现与电网的互联互通，能够根据电网的需求和自身发电状况进行灵活调节，提高能源利用效率和电网的稳定性。输电环节中，智能变电站起着核心作用。智能变电站采用先进的传感器、自动化设备和通信技术，实现了对变电站设备的实时监测、控制和保护。它能够自动采集设备的运行状态信息，通过数据分析及时发现设备故障隐患，并进行预警和处理。同时，智能变电站还支持与上级调度中心的实时通信，实现远程监控和操作，提高了电网的运行管理效率。变电环节涉及电力调度自动化系统。该系统是智能电网的“大脑”，负责对整个电网的运行进行实时监控、调度和控制。它通过采集电网的实时数据，运用先进的算法和模型进行分析和决策，实现电力资源的优化配置和电网的安全稳定运行。电力调度自动化系统的可靠性和安全性直接关系到电网的正常运行，一旦出现问题，可能导致大面积停电事故[1]。配电环节中，智能电表是重要的基础设施。智能电表不仅能够准确计量用户的用电量，还具备双向通信功能，可以实时将用户的用电信息上传至电网企业，同时接收电网企业的指令，实现用电的智能管理和控制。通过智能电表，电网企业可以更好地了解用户的用电需求，实施分时电价等政策，引导用户合理用电，提高电网的负荷调节能力。用电环节涵盖了各类用电设备和用户终端系统。随着智能家居、电动汽车等新兴用电设备的普及，用电环节的信息安全也变得越来越重要。这些设备通过互联网与电网进行连接，实现了能源的智能化管理和交互，但同时也面临着网络攻击的风险，可能导致用户信息泄露、设备被控制等问题。这些关键基础设施不仅承载着电力生产与传输的重要任务，还涉及大量的用户信息和电力市场交易数据。例如，智能电表记录了用户的用电习惯和消费信息，电力调度自动化系统掌握了电网的运行状态和电力交易数据等。这些信息一旦泄露或被篡改，将给用户和电网企业带来巨大的损失，因此其信息安全至关重要[2]。

1.2 信息安全面临的挑战

1.2.1 技术层面

智能电网广泛采用无线通信、物联网等技术，这些技术的开放性使得网络更容易受到攻击。无线通信技术在智能电网中用于实现设备之间的远程通信，如智能电表与采集终端之间的数据传输、分布式能源与电网之间的信息交互等。然而，无线信号在传播过程中容易受到干扰和窃听，攻击者可以通过截获无线信号获取敏感信息，或者干扰信号传输导致通信中断。物联网技术将各种智能设备连接到网络中，实现了设备的互联互通和智

能化管理。但在物联网环境下，设备数量众多、分布广泛，且部分设备的安全防护能力较弱，容易成为攻击者的入侵目标。攻击者可以利用物联网设备的漏洞，窃取设备中的数据，或者控制设备发起攻击，如通过控制大量的智能电表发起拒绝服务攻击，导致电网通信系统瘫痪。同时，智能电网系统的复杂性也增加了安全漏洞的发现与修复难度。智能电网涉及多个领域的技术和设备，系统架构复杂，不同设备和系统之间的接口众多[3]。这使得安全漏洞可能隐藏在系统的各个层面，难以全面发现和及时修复。而且，随着新技术的不断应用和系统的升级改造，新的安全漏洞也可能不断出现，给信息安全带来持续的挑战。

1.2.2 管理层面

现有的安全管理制度可能无法适应智能电网快速发展的需求。智能电网是一个新兴的领域，其技术和管理模式都在不断变化和创新。然而，部分企业的安全管理制度更新不及时，存在安全策略不完善、安全审计不严格等问题。例如，安全策略可能没有明确规定不同用户和设备的访问权限，导致一些非授权用户能够访问敏感信息；安全审计可能只是形式上的检查，没有真正发现和解决安全管理中存在的问题。此外，智能电网涉及多个部门和单位，如发电企业、电网企业、用户等，各部门之间的信息共享和协同管理存在困难。在信息安全事件发生时，可能由于信息传递不及时、协调不力等原因，导致事件得不到及时有效的处理，扩大事件的影响范围[4]。

1.2.3 人员层面

部分工作人员信息安全意识淡薄，操作不规范，可能导致内部信息泄露或系统被恶意攻击。在日常工作中，一些工作人员可能为了方便操作，使用简单的密码或者不设置密码，容易被他人猜解和破解。还有些工作人员可能会随意将含有敏感信息的文件通过公共网络传输，或者在公共场所谈论工作相关的信息安全内容，增加了信息泄露的风险。同时，部分工作人员对信息安全技术和知识了解不足，在面对网络攻击时缺乏应对能力。例如，当收到可疑的邮件或链接时，不能正确识别其中的风险，轻易点击导致系统感染病毒或遭受攻击。此外，随着智能电网与互联网的深度融合，外部网络攻击手段不断升级。黑客组织越来越专业化，他们利用先进的技术和工具，针对智能电网的关键基础设施发起攻击。例如，通过网络钓鱼、恶意软件感染、零日漏洞攻击等手段，窃取电网的敏感信息，破坏电网的正常运行。这些外部攻击手段的不断升级，使得关键基础设施的信息安全形势更加严峻。

2 信息安全防护体系的核心要素

2.1 技术要素

技术是保障信息安全的基础。在智能电网环境下，应采用多层次的安全防护技术。加密技术可对传输和存储的数据进行加密处理，防止数据被窃取或篡改。访问控制技术能够限制用户对系统和资源的访问权限，确保只有授权用户才能进行操作。入侵检测与防御系统可以实时监测网络流量，及时发现并阻止异常行为。此外，还应加强智能电网系统的安全漏洞扫描与修复，定期对系统进行安全评估，及时发现并消除潜在的安全隐患。

2.2 管理要素

有效的管理是信息安全防护的关键。建立健全信息安全管理制度，明确各部门和人员的安全职责，制定详细的安全操作规程。加强安全审计与监督，定期对系统的安全状况进行检查和评估，及时发现并纠正安全管理中存在的问题。同时，应建立应急响应机制，制定应急预案，在发生安全事件时能够迅速响应，采取有效的措施进行处置，降低安全事件对智能电网的影响。

2.3 人员要素

人员是信息安全防护的主体。提高工作人员的信息安全意识至关重要。通过开展信息安全培训与教育活动，使工作人员了解信息安全的重要性，掌握基本的安全知识和技能，规范操作行为。同时，应加强对工作人员的安全管理，建立人员安全档案，对关键岗位人员进行背景审查和安全考核，确保人员素质符合信息安全要求。

3 基于多维度融合的防护体系构建策略

3.1 体系架构设计

基于多维度融合的防护体系应采用分层架构设计，包括物理层、网络层、系统层、应用层和管理层，各层次相互协作，共同保障智能电网关键基础设施的信息安全。物理层主要保障智能电网基础设施的物理安全，如设备的防盗、防破坏等。通过采用物理防护设备，如防护栏、监控摄像头、门禁系统等，对变电站、配电室等重要场所进行防护，防止设备被非法访问和破坏。同时，对设备进行定期巡检和维护，确保设备的正常运行。网络层负责网络通信的安全，采用防火墙、入侵检测等技术防止网络攻击。防火墙可以设置访问控制策略，阻止外部非法网络流量进入智能电网内部网络；入侵检测系统可以实时监测网络流量，发现并阻止异常行为。此外，还可以采用虚拟专用网络（VPN）技术，为远程访问智能电网系统的用户提供安全的通信通道，保障数据传输的安全性。系统层确保操作系统和数据库

的安全，通过安全配置、漏洞修复等措施提高系统的安全性。对操作系统和数据库进行定期安全更新，安装最新的安全补丁，修复已知的安全漏洞。同时，对系统进行安全配置，关闭不必要的服务和端口，限制用户的权限，防止系统被非法入侵和利用。应用层针对智能电网的各类应用系统进行安全防护，如电力调度自动化系统、智能电表管理系统等。对应用系统进行安全评估和测试，发现并修复系统中存在的安全漏洞。采用身份认证、授权、加密等技术，保障应用系统的访问安全和数据安全。例如，在电力调度自动化系统中，采用多因素身份认证技术，确保只有合法的调度员能够登录系统进行操作。管理层则统筹协调各个层次的安全工作，制定安全策略、进行安全审计和应急响应等。管理层负责制定智能电网信息安全总体策略和规划，指导各个层次的安全工作。同时，对各层次的安全状况进行实时监控和审计，及时发现和处理安全问题。在发生安全事件时，管理层负责组织协调应急响应工作，确保事件得到及时有效的处理。

3.2 多维度协同防护机制

各维度之间应建立协同防护机制，实现信息共享与联动响应。当网络层检测到异常流量时，应及时将信息传递给系统层和应用层，系统层和应用层根据网络层提供的信息进行进一步的检测和防范。例如，网络层检测到有大量异常的请求访问电力调度自动化系统，立即将该信息传递给系统层，系统层对系统的运行状态进行检查，发现是否有异常进程或文件；同时，应用层对用户的访问行为进行分析，判断是否存在非法访问。同时，管理层应实时监控各维度的安全状况，根据安全事件的发展态势及时调整安全策略，协调各维度的资源进行应急处置。管理层通过安全信息管理平台，收集各维度的安全信息，进行综合分析和评估。当发生重大安全事件时，管理层根据事件的性质和影响范围，及时调整安全策略，如增加防火墙的访问控制规则、限制部分用户的访问权限等。同时，协调物理层、网络层、系统层和应用层的资源，共同开展应急处置工作，如调动技术人员对受攻击的设备进行修复、对网络进行隔离等。通过多维度协同防护，提高防护体系的整体效能。各维度之间相互配合、相互支持，形成一个有机的整体，能够更加有效地应对各种信息安全威胁，保障智能电网关键基础设施的信息安全。

3.3 持续优化与更新

智能电网技术不断发展，信息安全威胁也在不断变化。因此，防护体系应具备持续优化与更新的能力。定期对防护体系进行评估和改进，根据新的安全威胁和技术发展调整防护策略和技术手段。例如，随着量子计算技术的发展，传统的加密算法可能面临被破解的风险，防护体系应及时调整加密策略，采用抗量子计算的加密算法。同时，加强与行业内的交流与合作，及时了解最新的安全动态和解决方案，不断提升防护体系的水平。参加行业内的信息安全研讨会、交流会等活动，与其他企业和专家分享信息安全经验和技术。与安全厂商、科研机构等建立合作关系，共同开展信息安全研究和开发工作，引入先进的安全技术和产品，提高防护体系的性能和可靠性。

结束语

智能电网关键基础设施的信息安全面临着技术、管理和人员等多方面的挑战。为了保障智能电网的安全稳定运行，需要构建一个基于多维度融合的信息安全防护体系。该防护体系应涵盖技术、管理和人员等核心要素，采用分层架构设计，建立多维度协同防护机制，并具备持续优化与更新的能力。通过某地区智能电网的案例分析可以看出，基于多维度融合的信息安全防护体系能够有效提高智能电网关键基础设施的信息安全水平，降低信息安全风险。未来的研究中，应进一步关注智能电网新技术的发展带来的信息安全问题，不断完善防护体系，为智能电网的健康发展提供有力保障。

参考文献

[1]裴庆祺,沈玉龙,马建峰.无线传感器网络安全技术综述[J].通信学报,2017.8(8):96-97

[2]杨义先,李洋.智能电网的信息安全技术[J].中兴通讯技术,2016.8(8):84-85

[3]陶士全,刘永生,冯文龙.智能电网信息安全及其防护技术[J].信息安全,2015.6(5):84-86

[4]高翔.数字化变电站应用技术[M].中国电力出版社.2015.8:78