

# 电力系统二次安全防护策略研究

李进成

宁夏欣光泰电力技术有限公司 宁夏 银川 750000

**摘要:** 随着电力系统的智能化和数字化发展,二次安全防护成为保障电网稳定运行的关键环节。本文深入探讨了电力系统二次安全防护策略,分析了当前面临的主要威胁与挑战,并提出了包括加强防病毒系统有效性、引入多元化防护策略和技术手段、构建高效数据备份与恢复体系在内的多项措施。通过综合运用这些策略,旨在提升电力系统的整体安全防护能力,确保其在复杂多变的网络环境中能够稳定运行,为经济社会发展提供可靠的电力保障。

**关键词:** 电力系统;二次安全;防护策略

## 引言

电力系统作为国家基础设施的重要组成部分,其安全性和稳定性直接关系到国家能源安全和社会经济发展。随着信息技术的广泛应用和智能电网的加快建设,电力系统二次系统面临着日益严峻的安全挑战。黑客攻击、病毒入侵、数据泄露等安全事件频发,严重威胁到电力系统的正常运行。因此,加强电力系统二次安全防护策略研究,提升安全防护水平,成为当前电力行业亟待解决的问题。

## 1 电力二次系统网络信息安全防护的意义

电力二次系统网络信息安全防护的意义深远且重大,它不仅是确保电力信息化系统、电力实时闭环监控系统及调度数据网络稳定运行的关键所在,更是保障国家能源安全、社会经济稳定运行和民众日常生活不受影响的基石。第一,它能够有效抵御外部威胁,保障电力系统的稳定运行。通过采取一系列安全防护措施,如防火墙隔离、病毒防护、入侵检测系统等,可以及时发现并阻止潜在的攻击行为,确保电力二次系统的安全性和稳定性。这不仅有助于防范黑客和恶意代码的入侵,还能有效抵御自然灾害、设备故障等不可预见因素带来的风险。第二,电力二次系统网络信息安全防护能够保护电力数据的完整性和机密性,电力系统中包含了大量敏感数据,如调度数据、用户信息、设备状态等。这些数据一旦泄露或被篡改,将对电力系统的正常运行产生严重影响<sup>[1]</sup>。因此,加强电力二次系统网络信息安全防护,可以防止未经授权的访问和非法数据修改,确保电力数据的完整性和机密性。第三,电力二次系统网络信息安全防护还有助于提升电力系统的应急响应能力,通过建立健全的安全管理制度和应急预案,可以在电力系统遭受攻击或发生故障时迅速响应,及时恢复系统正常运行。这不仅能够减少停电时间,降低经济损失,还能提

高电力系统的可靠性和韧性。

## 2 电力系统安全防护中存在的问题

### 2.1 网络防护方法单一

在深入探讨电力系统安全防护所面临的挑战时,网络防护方法单一的问题尤为凸显,这不仅制约了电力系统抵御复杂网络威胁的能力,也直接威胁到电力二次系统乃至整个电网的安全稳定运行。具体而言,这一问题的核心在于当前电力防护系统过度依赖传统的防护手段,如防火墙和网闸等,这些措施虽然在一定程度上能够隔离潜在的网络攻击,但其局限性在大数据时代背景下愈发显著。防火墙作为电力系统网络安全的第一道防线,主要通过预设的安全规则对进出网络的数据包进行过滤,以阻止未经授权的访问和恶意流量。然而,随着黑客技术的不断演进,攻击手段日益复杂多变,传统的基于规则的防火墙往往难以应对零日攻击、高级持续性威胁(APT)等新型攻击方式。此外,防火墙对于内部威胁的防范能力也相对较弱,一旦内部人员或系统被恶意利用,防火墙的防护效果将大打折扣。另外,网闸则是一种更为严格的物理隔离设备,它通过物理断开网络连接的方式,确保内外网之间的数据交换只能通过特定的、可控的通道进行。尽管网闸在防止直接的网络攻击方面表现出色,但其应用也受到了诸多限制。首先,网闸的部署和维护成本较高,且对实时性要求较高的数据传输场景支持不佳;其次,网闸无法全面覆盖所有类型的网络威胁,特别是那些利用系统漏洞或供应链攻击等间接手段发起的攻击;最后,随着云计算、物联网等技术的广泛应用,电力系统内部网络结构日益复杂,传统的网闸隔离方式已难以满足现代电力系统安全防护的需求。更为严峻的是,电力系统作为关键基础设施,一直是网络黑客攻击的重点目标。一旦电力系统被外部入侵程序攻破,不仅可能导致电力供应中断、设备损坏等严

重后果,还可能引发连锁反应,影响其他关键基础设施的正常运行,进而威胁国家安全和社会稳定。因此,单纯依靠防火墙和网闸等传统防护手段已无法有效应对当前复杂的网络安全威胁。

## 2.2 数据安全和异地备份问题

在电力系统安全防护的广阔领域中,数据安全和异地备份问题无疑是一个亟待解决的关键议题,随着电力信息化进程的加速推进,海量数据在电力企业的运营中扮演着越来越重要的角色,它们不仅是电网调度、设备监控、用户管理等核心业务的基础,也是企业决策分析、战略规划的重要支撑。然而,当前绝大多数电力企业在处理不同地区的大面积数据备份时,仍面临着诸多挑战与不足。传统上,电力企业倾向于采用移动硬盘拷贝或CD-ROM录制等物理介质方式进行数据备份。这种方式虽然在一定程度上实现了数据的保存与转移,但其局限性也显而易见。一方面,物理介质备份需要耗费大量的人力物力,尤其是在面对大规模、跨区域的数据备份需求时,工作量急剧增加,效率低下。另一方面,物理介质易受环境因素影响,如损坏、丢失、被盗等风险,一旦发生,将给企业带来不可估量的损失。此外,数据恢复过程繁琐且耗时,难以满足紧急情况下快速恢复业务运行的需求。并且,这种分散的、非自动化的备份方式难以保证数据的一致性和完整性,在电力系统中,不同地区的数据往往相互关联、相互影响,一旦某个环节的数据出现问题,就可能引发连锁反应,影响整个系统的正常运行。所以,实现不同地区数据的同步备份,确保数据的实时性、一致性和安全性,对于电力系统的安全防护具有至关重要的意义。

## 2.3 防病毒系统缺乏有效性

电力二次系统作为电力系统的神经中枢,其稳定性和安全性要求极高。为了应对日益复杂的网络威胁,许多电力企业选择在二次系统中部署防病毒体系,旨在通过自动化管理手段,及时升级病毒代码和扫描引擎,以抵御各类病毒的侵袭。但是,由于电力二次系统的特殊性,它通常被设计为与互联网物理隔离,以确保其不受外部网络环境的干扰。这一设计初衷虽好,却也无形中给防病毒系统的升级与维护带来了难题。在没有互联网连接的情况下,防病毒中心的病毒代码无法及时更新,客户端的防病毒软件也无法获得最新的防护能力,这无疑削弱了防病毒系统的防御效果<sup>[1]</sup>。除此之外,一些供电单位的管理者和技术人员对病毒传播的危害性和多样性认识不足,忽视了在二次系统与办公系统之间建立科学安全隔离措施的重要性。在缺乏有效隔离的情况下,病

毒得以在两个系统之间自由穿梭,肆意传播和扩散,病毒以其极强的破坏性、隐蔽性和极快的传播速度,对电力二次系统构成了严重威胁。一旦病毒侵入二次系统,不仅可能导致系统瘫痪、数据丢失等严重后果,还可能引发连锁反应,影响整个电力系统的稳定运行,进而威胁到社会经济的正常运行和民众的正常生活。

## 3 加强电力系统二次安全防护的相关策略

### 3.1 引入多元化的防护策略和技术手段

(1) 聚焦于新兴技术的研发与应用是推动电力系统安全防护升级的关键,人工智能技术的引入,为电力系统提供了智能威胁识别与响应的能力。通过机器学习算法,系统能够自动分析网络流量、用户行为等数据,从中发现异常模式,并实时预警潜在的安全威胁。大数据分析则进一步增强了这种能力,通过对海量数据的深度挖掘,揭示隐藏在数据背后的安全风险和攻击趋势,为安全防护策略的制定提供科学依据。区块链技术以其去中心化、不可篡改的特性,为电力系统的数据安全和交易信任提供了全新解决方案,有效防止数据被恶意篡改或泄露。(2) 建立健全的网络安全管理体系是确保多元化防护策略有效实施的重要保障,这包括完善的安全管理制度、严格的访问控制策略、定期的安全审计以及高效的应急响应机制。管理制度的完善,明确了各级人员的安全职责和操作流程,规范了日常的安全管理行为<sup>[3]</sup>。访问控制策略的实施,确保只有经过授权的用户和设备才能访问系统资源,防止非法入侵和数据泄露,安全审计则是对系统安全性的全面检查与评估,帮助发现潜在的安全漏洞和隐患。(3) 电力系统安全防护工作的成功实施,离不开高素质的安全团队和全体员工的安全意识。通过定期举办安全知识讲座、开展安全技能竞赛、组织应急演练等活动,可以不断提升员工的安全防范意识和应急处理能力。(4) 加强多方合作与交流是推动电力系统安全防护持续发展的重要动力,政府、科研机构、安全厂商等各方在安全防护领域各具优势,通过加强合作与交流,可以实现资源共享、优势互补,共同应对电力系统安全防护面临的挑战。例如,政府可以制定相关政策法规,为安全防护工作提供法律保障;科研机构可以开展前沿技术研究,为安全防护提供技术支撑;安全厂商则可以提供先进的安全产品和服务,满足电力系统的实际需求。

### 3.2 构建数据备份与恢复体系

面对自然灾害、人为误操作、网络攻击等潜在威胁,构建一套高效、可靠、自动化的数据备份与恢复体系,已成为电力企业保障业务连续性、降低数据风险的

关键举措。一方面,通过建立基于云的数据备份中心,电力企业能够实现跨地区、跨平台的数据集中存储与统一管理,这不仅极大地扩展了数据存储容量,还提升了数据管理的灵活性和可扩展性。云备份服务以其按需付费、弹性扩展、高可用性等优势,有效降低了企业的备份成本,同时利用云平台的强大计算能力和分布式存储技术,实现了数据的快速备份与高效恢复。在灾难发生时,云备份中心能够迅速提供数据恢复服务,确保电力业务在最短时间内恢复正常运行。另一方面,电力企业应采用先进的加密技术,对备份数据进行加密处理,确保数据在传输和存储过程中的机密性和完整性。同时,通过实施严格的访问控制策略,限制对备份数据的非法访问和篡改。安全审计机制则用于记录备份数据的操作日志,及时发现并处理潜在的安全威胁。此外,电力企业还应定期对备份数据进行安全评估与漏洞扫描,确保数据备份环境的安全性。此外,在构建数据备份与恢复体系的过程中,建立健全的数据备份管理制度和应急预案同样至关重要。制度方面,企业应明确备份策略、备份周期、备份验证等关键要素,确保备份工作的规范化和标准化。并且,建立备份数据的定期验证机制,确保备份数据的可用性和准确性。应急预案则包括数据丢失、损坏等突发事件的应急响应流程、恢复策略、资源调配等内容,确保在发生数据灾难时,企业能够迅速启动应急预案,有序开展数据恢复工作。

### 3.3 提升防病毒系统的有效性

电力企业应高度重视对防病毒系统的投入与管理,这不仅仅体现在硬件设备的采购和部署上,更重要的是对软件维护与更新的持续关注。防病毒软件的核心在于其病毒代码库和扫描引擎的时效性,只有保持这些组件的及时更新,才能有效识别和抵御最新出现的病毒威胁。因此,电力企业应建立规范的软件更新流程,确保防病毒软件能够定期从官方渠道获取最新的病毒定义和扫描算法,从而不断提升其防护能力<sup>[4]</sup>。同时,考虑到

电力二次系统的特殊性和敏感性,电力企业还应积极探索适用于该领域的离线升级方案。电力二次系统往往承载着控制、监测等关键任务,对实时性和稳定性要求极高。在某些情况下,由于网络隔离或安全策略的限制,这些系统可能无法直接连接互联网进行在线升级。为此,电力企业可以与防病毒软件供应商合作,定制离线升级包,通过安全可靠的渠道传输至电力二次系统,实现防病毒软件的离线更新。这种方式既保证了系统的安全隔离性,又确保了防病毒系统的时效性。另外,提升防病毒系统的有效性还需要加强与其他安全措施的协同作战,防病毒系统只是信息安全防护体系中的一环,它需要与防火墙、入侵检测系统、安全审计系统等共同协作,形成多层次的防御体系。电力企业应优化这些安全组件之间的联动机制,确保在发现病毒入侵时能够迅速响应、协同处置,最大限度地降低病毒对系统的影响。

### 结束语

综上所述,电力系统二次安全防护策略的研究与实施对于保障电网稳定运行具有重要意义。通过加强防病毒系统有效性、引入多元化防护策略和技术手段、构建高效数据备份与恢复体系等措施的综合运用,可以显著提升电力系统的安全防护能力。未来,随着技术的不断进步和威胁形势的不断变化,电力系统二次安全防护工作仍需不断创新和完善,以适应新的安全挑战和需求。

### 参考文献

- [1]姜松.电力系统二次安全防护策略研究[J].通信电源技术,2019,36(06):263-264.
- [2]饶巨为.电力监控系统二次安全防护探讨[J].通信电源技术,2019,36(06):285-286.
- [3]刘家鑫.电力系统及其自动化技术的安全控制问题和对策[J].家庭生活指南,2019(06):178.
- [4]杨钊.电力监控系统二次安全防护策略研究[J].电工技术,2019(13):118-119+122.