

电力网络安全管理现状及防御措施研究

王素宁 陈凯峰 童欣

国网上海市电力公司崇明供电公司

摘要: 阐述电力系统在现代社会中面临的网络安全威胁成因,对现有安全管理策略进行分析和未来趋势的预测,探索和提出适应当前环境的防御措施,为电力网络安全管理提供新的思路 and 方案。

关键词: 电力系统; 网络安全; 防御措施

【DOI】10.12252/j.issn.2096-627X.2022.11.068

引言

在当前的电力行业中,随着技术的进步和网络连接的增加,网络安全管理呈现出新的复杂性和紧迫性。电力系统作为国家基础设施的核心组成部分,其安全性直接关系到国家安全和人民生活,针对当前电力系统自动化设备面临的网络安全威胁和挑战,寻求有效的应对策略,对于确保电力网络安全、维护社会稳定具有重要意义。

一、现阶段电力网络防御措施的重要意义

在电力网络的网络安全管理领域内,不断地面临着网络安全挑战。这些挑战包括网络病毒侵袭、未经授权的访问和敏感信息泄漏等多个层面,每一个问题都可能对电力行业的安全带来严重威胁。在所有网络攻击手段中,网络劫持与数据篡改的发生尤为频繁,而分布式拒绝服务攻击以其特有的破坏性而著称。这种类型的攻击会中断电力系统的正常运作,不仅可能导致巨大的经济损失,还可能对社会稳定造成威胁。在构建电力监控系统时,建立一个坚固的安全防护体系是至关重要的核心基础。这一体系以所定义的安全分区为支撑。在现代电力产业中,以计算机和网络技术为基础的业务被明确划分为两个主要部分,即生产控制和管理信息系统。更进一步地区分,生产控制系统细分为控制区(也称为安全分区I)和非控制区(亦即安全分区II)。在这些安全分区的设计与部署过程中,必须遵循一系列安全防护的基本原则,并针对具体的业务系统需求,合理简化和调整安全分区的架构。特别需要注意的是,要尽可能避免或减少安全分区间的直接连接,此举对于防止可能的安全风险具有决定性的作用^[1]。

通过深入探究电力数据网络的特征结构,可以认识到这一网络作为连接电力生产控制中心的专用通信路径,展现出了其独特性。其主要职责是确保电力系统的实时监控及在线生产交易等关键操作的顺利进行。在该

网络架构中,发电环节的数据调度是通过特殊的通讯渠道执行的,且该网络采用专用的网络硬件设施构建。这种部署策略在物理层面为电力公司内部其他数据网络与外部的公共信息网络搭建了一座至关重要的安全防护墙,从而实现了信息安全的有效保障。电力系统的次级安全防护架构中,横向隔离原则是至关重要的组成部分。该原则通过构建一个类似“安全腰带”的结构,确保采用不同安全等级的措施来划分保护区域的界限。其中,在生产控制领域与管理信息领域的交界处,必须安装经官方鉴定认证,且专门针对电力系统定制的集成单向安全隔离设备,以实现接近物理分隔的隔离效果。在生产控制领域内部,不同安全领域之间则采用配备权限管理的网络组件、国内生产的专业硬件防火墙,或其他具有相同功能的技术解决方案实施逻辑隔离。这些隔离措施保证即便是在同一个较大的生产控制区域内部,各个安全领域也能维持必要的独立性,进而显著提升了整体网络安全防护的效率和效果。在对电力二次系统的安全结构进行系统性分析中,必须重视纵向认证技术所扮演的关键角色。纵向认证技术为电力系统的安全框架增添了至关重要的一环,塑造了一条结实的多层次防线,它象征性地守护着如同“城池”一般的系统要塞,保障了电力行业信息流通的安全。尤其在发电厂与数据调度网络的关键节点处,部署了经过国家级权威机构严格审查与认证的专为电力系统设计的纵向认证装置。这些装置的目的是确保通信各方身份的真实性,它们通过精确的验证流程,并结合先进加密技术和访问控制策略,为关键数据提供额外层次的保护。

二、现阶段电力网络安全问题的成因

1. 电力网络自身结构复杂

电力网络构建了一张错综复杂的结构图谱,精密展现了整个系统的基础骨架及其交织的网络关系。在这一庞大体系中,各个单元宛若精确配合的齿轮,相互依

靠，共同确保电力系统的高效运作。但这种紧紧相连的特性同样暗示着，任何单一环节的失效都会迅速传导，形成连锁反应，潜在地影响到整个电网。鉴于电力网络的复杂性及其内在的互联性，系统安全防护面对重大挑战，要求从业人员必须不断警觉，以确保网络各环节的安全可靠。信息基础设施在电力行业中扮演着极其关键的角色，其覆盖范围广泛，涵盖了行业的各个管理层次和业务流程。信息系统巨大的规模宛若信息技术界的高峰，然而，庞大体系的维护同样伴随着若干挑战。组织协同合作、信息共享以及权限管理都需经过周密策划与严格操控。更为关键的是，复杂的信息架构成为黑客攻击的焦点，一旦遭受黑客侵袭，电力基础设施可能遭受空前风险，甚至危机到整体社会的正常运行。因而，加固信息安全防护屏障，保障电力行业的稳固与安全势在必行。部分设备由于长期使用，已难以满足现代网络安全的要求，技术水平日渐滞后。这导致这些装备在防护能力上显现出明显的脆弱性，经常成为网络攻击者的首选目标。为确保电力系统的安全与稳定，亟须关注此问题并实施有效措施。定期进行设施的更新与维护，可以有效提高其性能并增强对网络攻击的防护能力。这一过程是一个漫长且复杂的挑战，需我们投入大量的资源与努力。然而，唯有持续的投入与维护，才能够保障电力系统的安全运行，为社会稳定运作提供可靠的支持^[2]。

2. 现有框架难以适应

在电力系统中，网络通信规则及标准对于确保系统的顺畅运行至关重要。但是，随着网络技术的快速发展，现有的规则 and 标准可能存在不足，成为网络攻击者潜在的攻击目标，这对电力系统的稳定性和可靠性构成了实质性的威胁。因此，必须持续保持高度警觉，加强对通信规约和安全标准的持续研究和更新，以确保电力系统的网络安全。通过不断的努力，我们可以为社会稳定与发展保驾护航。同时，加大与其他行业及机构的合作与交流，是推动电力网络安全进步和发展的关键途径。不容忽视的是，在数据安全防护的实施过程中，电力产业存在的某些做法暴露出明显的不足。尤其是对备份数据重要性的认识不充分会导致在不期而遇的数据损坏事件下，企业受到重大冲击。为此，若缺乏必要的先进数据备份技术投入和管理流程，风险将日益增加，而数据安全难以得到有效维护。由于网络安全投入与管理的不匹配，在网络安全领域，部分电力企业的高层领导

未能给予足够重视。这种状况反映在对网络安全的财务预算分配、硬件设备采购，以及规章制度构建等方面。随着网络威胁不断增加，这些企业的网络安全防护措施显然不足，难以有效地防范潜在威胁，从而可能难于应对网络安全挑战。

3. 网络管理效应不足

在当今电力行业中，信息网络管理的不一致性问题尤为显著，这主要是由于缺乏全面且统一的信息网络管理框架，导致在安全防护及规程建设方面存在显著短板，成为限制行业发展的关键问题。这一缺陷不仅妨碍了电力网络安全防护效应的协同增强，也使整个网络在抵御网络安全威胁时显得捉襟见肘，其防御能力受到严重削弱。这种管理体系的不协调性不仅干扰了电力行业的正常运作，还增大了信息泄漏和系统崩溃的风险，对电力行业的稳健运营和安全防护构成了潜在的威胁。伴随科技的迅猛进步，电力通信网络所面临的外部安全威胁日益增多。这些威胁源头多元，其手段日益复杂化，涵盖了网络病毒传播、非法侵入的恶意攻击，以及黑客的精准定向打击等多种形式。这些安全威胁不仅可能导致电力数据的泄漏，还可能引起电力系统运行故障，乃至触发电网全局性的瘫痪。因此，电力通信网络安全正面临着前所未有的考验。为有效应对这些挑战，电力企业亟须加强安全防护体系构建，提高网络安全防护的整体能力，以确保电力通信网络的稳定性。这不仅是电力行业持续发展的必然要求，更是维护国家能源安全与社会稳定的关键措施。

三、电力网络安全的不同防御措施

1. 传统防御措施

在电力网络的安全体系结构中，防火墙承担着至关重要的基础防御角色。作为内部网络与开放性公共网络间的屏障，防火墙设定了严格的数据传输安全标准。利用先进的防护技术，防火墙对穿越边界的数据流进行精细的审查，确保评估数据内容的安全性，并坚决拦截包含潜在风险的信息及应用。这样的防御措施有效保护内部网络不受外界干扰，确保信息系统的完整安全。此外，防火墙还能有效抑制网络内的潜在威胁传播，增强网络的安全防护层级。在构建计算机网络防护体系的过程中，杀毒软件是不可或缺的关键元素。该软件机制专注于在源头识别和清除恶意代码，与防火墙共同形成防御联盟。杀毒软件彻底排查任何意图入侵系统的程序，

有效检测和隔离携带病毒的文件。用户得以手动或通过自动化方式激活该软件，开展全面系统扫描，消除来自木马、蠕虫等数字威胁的不安全因素，并为网络安全立下坚实的防线。访问控制策略是电力网络安全管理的必不可少组成部分，尤其在预防非法入侵方面效果显著。许多安全事件源于非法获取访问权限，无论是由于恶意软件还是黑客攻击所致。鉴于此，建立严格的进出请求监管机制变得尤为重要。遵循这一原则，我国的电网安全管理普遍采用多元化访问控制策略，如基于属性的访问控制、权限分配以及详细的目录权限管理方案。通过配置可视化访问控制目录，并使用白名单机制记录授权IP和端口，建立起有效阻遏未经授权访问活动的手段。这样的策略强化了对电力网络数据的保护，避免了关键信息遭非法访问或篡改的风险^[3]。

2. 新型防御措施

随着数据中心在电力行业互联网化构建中扮演核心枢纽的角色，大量的数据传输和复杂的技术设施正日益增加。以厦门电网网络安全架构为例，其中一个不可或缺的要害便是DDOS攻击监控系统，以及其他多种关键性系统。这类监控系统致力于实时流量监测与分析，运用数据挖掘技术侦察潜在的安全风险。在复杂多变的网络安全领域内，及时发现并监控潜在缺陷显得尤为迫切。进一步应用数据挖掘，对于提升工业控制系统、企业网络、移动应用以及权限管理的安全性起到了积极的增强作用。未来电力网络安全的基石之一，深度包过滤技术，承担着检查通信数据包的责任，其在恶意软件检测方面的性能已经超越传统方法。例如，厦门某电力公司采取了深度包过滤技术与嵌入式软件的结合之策，旨在提高数据分析和防御响应的速度。此技术能精准地解析数据包的路径和网络协议，并以此为基础执行信息过滤和保护工作。作为一种新颖的电力网络防御策略，免疫网络通过巧妙设计的网络拓扑结构及高效的安全资源管理，实施了有效的数据过滤与病毒隔离。在厦门某电力公司的案例中，技术团队采用免疫网络技术和路由器特性，提升了系统的自我防护能力，构建了层级与深度兼备的网络安全防线。该技术还通过强化鉴权流程，提高了网络的机密性及自动化病毒分析的能力，确保电力网络在受到攻击时能够迅速且有效地应对。

3. 系统免疫及恢复

在制定电力网络系统安全保护的框架时，面对

多变的安全风险以及应对已发生安全事故的快速应急机制，制订一系列综合策略成为必要举措。其中，加快数据与系统恢复的速度显得尤为关键，意味着在遭受病毒侵袭或外部攻击后，快速采取行动以最小化损害，并恢复电力系统常规运行功能的策略，应引起高度关注。我国众多电力网络系统参考生物免疫系统的原理，构建了具有多层次应变及系统恢复能力的架构，其中云安全技术发挥了核心作用。在安全性管理与保障实践过程中，云安全技术通过对大量客户端软件操作与数据交换进行实时监控，有效地识别和分析网络中的恶意软件特征及行为模式，从而及时传递分析结果和解决方案至客户端以供实施。该技术展现出了自动化分析及防范安全风险的能力，允许我们在恶意软件发展的早期阶段介入，为电力网络的安全防护提供了强有力的策略。关于数据与系统恢复的议题，云备份技术在其中扮演关键角色，它使得关键电力网络数据能够加密后通过网络传输至云端存储，进而确保数据的安全性。在遭受数据损害时，可以便捷地从云端恢复数据，实现系统的迅速回复。该方法不仅大幅度降低了电力网络故障带来的潜在影响，而且确保业务能迅速恢复运行。为进一步防范未经授权的数据盗取风险，可采用自我销毁的加密技术。该技术能够在检测到非法解密尝试时自动触发警报并销毁数据，依托云备份技术实现数据的迅速恢复，从而增强了电力网络数据的安全防护。通过持续地研究与强化这些关键技术，我们不仅构建了针对安全威胁的防护体系，也确保了面对挑战时电力网络能够迅速恢复至稳定运行状态^[4]。

结语

电力网络安全是电力系统稳定运行的重要保障，需要持续关注 and 加强。未来，我们应继续加强技术防范、完善管理制度、提升人员安全意识，共同构建安全可靠的电力网络环境。

参考文献

- [1] 王磊. 浅谈电力网络安全管理及防御措施[J]. 网络安全技术与应用, 2020, (12): 137-138.
- [2] 蔡昶. 电力网络安全管理现状及防御措施研究[J]. 网络安全技术与应用, 2019, (02): 80+84.
- [3] 张仕海. 配电网安全运行管理的研究[J]. 科技资讯, 2017, 15 (13): 36-37.
- [4] 李智勇. 电力调度自动化网络安全防护系统的研究[J]. 中国新技术新产品, 2016, (15): 180-181.