电力系统信息通信网络安全及防护措施分析

张腾
国网河北省电力有限公司新乐市供电分公司

摘　要：信息通信技术与电力系统的深度融合，为电力行业的发展带来了革命性的变化。但同时，信息通信网络的安全问题也逐渐成为制约电力系统稳定发展的关键因素。本文通过深入分析电力系统信息通信网络的特性，指出了网络安全面临的主要威胁，如外部攻击、内部泄漏及技术漏洞等。文章还探讨了现有防护措施的不足，并基于此，提出了一系列创新的防护策略。这些策略包括强化安全教育、运用新技术进行风险预测和响应、严格审查外部接入设备等。目的在于提升电力系统信息网络的整体安全水平，确保电力供应的稳定性和可靠性。

关键词：电力系统；信息通信网络；网络安全；防护措施
【DOI】10.12252/j.issn.2096-627X.2023.08.082

一、引言

在当今社会，电力系统不仅仅是一个单纯的能源供应系统，它已经成为国家基础设施的核心部分，其稳定运行对社会的影响深远。信息技术的引入使得电力系统运行更加高效，但也带来了新的挑战。信息通信网络作为电力系统的神经中枢，其安全问题牵一发而动全身。本文旨在探讨电力系统信息通信网络面临的安全威胁，分析现有防护措施的不足，并提出相应的改进措施。文章的核心在于如何在确保电力系统高效运行的同时，也保障其信息安全，避免因网络安全问题导致的严重后果。

二、网络安全的重要性

1.网络安全的核心地位

电力系统的信息网络承担着极其重要的职责，它不仅仅是数据传输的渠道，更是整个电力系统稳定运行的基石。如同人体的神经系统一样，信息网络负责着控制指令的传达和监测数据的回流，这些数据和指令对于电力系统的每一个运行环节都至关重要。一旦这个系统受到破坏或干扰，其后果是不可估量的。数据的错乱可能导致控制系统的失灵，进而使得电力设备无法正常工作，严重时甚至可能触发大规模的停电事件，对社会造成巨大的影响。

2.网络攻击的日益严峻

近年来，随着技术的发展，网络攻击手段变得更加多样和隐蔽，它们对电力系统信息网络的威胁日益增加。黑客利用各种手段进行网络入侵，这些攻击可能源自国内外的不同主体，包括黑客、竞争对手甚至是国家机构。他们可能出于不同的目的，如窃取重要数据、破坏系统运行或是进行恶意的政治和经济干预。这些网络攻击的复杂性和隐蔽性使得防御工作变得更加艰巨。

3.安全防护的紧迫性

鉴于网络攻击的日益严重，加强电力系统信息网络的安全防护显得尤为迫切。电力系统作为国家基础设施的重要组成部分，其安全直接关系到国家安全和社会稳定。信息网络的安全防护不仅仅是技术层面的问题，它还涉及政策制定、法规监管、员工培训等多个方面。有效的安全防护措施能够减少网络攻击带来的风险，保障电力系统的平稳运行，从而确保社会的正常运转和人民的生活安宁。

4.安全策略的多维构建

要提高电力系统信息网络的安全性，就需要从多个维度出发，构建一个全面的安全防护体系。第一，技术防护是基础，包括加强网络的物理隔离、使用防火墙和入侵检测系统等。第二，需要加强员工的安全意识培训，因为很多安全事故都是由内部操作不当引起的。第三，与政府、行业组织以及其他电力企业进行信息共享和合作，可以有效提高对新型攻击手段的识别和防范能力。第四，建立应急响应机制，一旦发生安全事故，能够迅速采取行动，减少损失。

三、面临的主要威胁

1.网络威胁的多样性

电力系统信息网络面临的安全威胁呈现出多样化的特点。外部网络攻击日益猖獗，这些攻击可能来自黑客、竞争对手，甚至是国家级的网络战行动。他们运用各种手段，包括病毒、木马、DDoS攻击等，对电力系统进行破坏。除了外部威胁，内部数据泄漏也是一个严重问题。员工操作失误或内部人员的恶意泄漏，都可能导致敏感信息的外泄，从而危及整个系统的安全。

2.技术缺陷与系统漏洞

技术层面的缺陷是导致电力系统信息网络易受攻击

的重要原因之一。系统漏洞，如软件漏洞、硬件缺陷等，为攻击者提供了可乘之机。随着新技术的不断应用，如云计算、物联网等，电力系统的网络架构变得更加复杂，相应的安全防护措施也需要同步更新，以应对新出现的安全挑战。

3.人为因素的影响

在电力系统信息网络的安全问题中，人为因素不容忽视。员工的安全意识不足，操作不规范，是引发安全事件的常见原因。内部人员的故意破坏行为也时有发生，这些行为可能由个人的不满、报复心理或其他私人原因驱动。因此，提高员工的安全意识，加强内部管理，对防止内部数据泄漏具有重要意义。

4.管理漏洞的危害

管理层面的漏洞也是导致电力系统信息网络安全问题的一个重要方面。这包括安全政策的缺乏或执行不力，安全培训的不到位，以及对安全事件反应不够迅速或有效。管理层需要充分认识到信息安全的重要性，将其作为企业战略的一部分，建立健全的安全管理体系。

四、当前防护措施的局限性

1.安全防护的现状

电力系统在安全防护方面已经做了大量工作，包括建立起防火墙、入侵检测系统等基础安全设施。这些措施在一定程度上保障了网络的安全，阻挡了一些常规的网络攻击，为电力系统的稳定运行提供了基本保障。但随着网络环境的不断变化和攻击技术的不断进步，现有的安全防护措施开始显露出局限性。

2.传统防御手段的不足

目前的安全防护措施主要针对传统的网络攻击方式设计，如针对病毒、木马等恶意软件的防护。但在面对更加复杂、隐蔽的攻击时，如零日攻击、高级持续性威胁（APT）等，这些传统的防御手段往往力不从心。这类攻击方式往往具有高度的隐蔽性和针对性，能够绕过传统的安全防护措施，给电力系统带来严重威胁。

3.新型威胁的挑战

随着网络攻击技术的不断演进，新型的网络威胁层出不穷。例如，利用人工智能技术的网络攻击可以实时学习和适应防御策略，更加难以预防和检测。物联网设备的普及也为攻击者提供了新的入口，增加了网络防护的难度。这些新型威胁要求我们不断更新和升级安全防护策略，以应对更加复杂的安全挑战。

4.忽视内部安全的风险

在现有的安全防护措施中，往往过分强调对外部威胁的防护，而忽视了内部安全的重要性。内部员工的操作失误、权限滥用或故意的破坏行为，都可能导致严重的安全事件。对内部系统的安全审计和监控往往不够，这使得内部威胁成为电力系统安全的一个薄弱环节。

五、创新安全防护策略

1.全面提升安全意识

电力系统信息网络安全的根本在于深植于每位员工心中的安全意识。安全，不仅是技术问题，更是文化问题。在电力行业这样一个特殊且重要的领域，每个员工的行动和决策都与整个系统的安全息息相关。因此，深化员工安全意识的教育和培训显得尤为关键。这种培训不应仅停留在理论知识的灌输上，更应关注如何将这些理论知识应用到日常工作中去。在实际操作过程中，员工能够识别潜在的网络威胁，并采取有效的预防措施，这对于防范网络攻击和数据泄漏至关重要。

为了更好地培养员工的实战能力，组织模拟演练和安全演习成了提高安全意识的有效手段。通过这样的活动，员工可以在模拟的网络攻击环境中学习如何应对，这不仅提升了他们识别和处理网络安全威胁的能力，也增强了他们在紧急情况下的应变能力。更重要的是，这种亲身体验的过程使员工能够更加深刻地理解网络安全的重要性，从而在日常工作中自然而然地发挥出高度的安全意识。

安全意识的培养也是一个持续的过程，它需要在企业文化中扎根。电力系统应当将安全教育融入日常工作的每一个环节，不断地提醒员工注意安全。例如，通过定期的安全讲座、更新安全操作手册、在工作场所设置安全提醒标识等方式，不断地强化安全意识的重要性。同时，还可以通过表彰在安全方面表现突出的个人或团队，激励所有员工更加注重网络安全。

在安全意识的提升过程中，管理层的态度和行为同样起到了关键作用。领导的示范行为和对安全重视的态度能够极大地影响员工。如果管理层能够亲自参与安全培训，不仅展示了对安全问题的重视，也会激励员工更加认真对待安全培训。这种自上而下的重视将在整个组织中形成强有力的安全文化氛围。

2.运用先进技术防护

在当今这个数字化日益加深的时代，大数据和人工智能技术成了电力系统网络安全防护的强大武器。随着这些技术的不断发展和成熟，它们在识别和预防网络安

全威胁方面发挥着越来越关键的作用。这些技术的应用不仅仅是增加了一个防护层面，更是在电力系统网络安全管理中开辟了新的领域。

利用大数据分析技术，可以对电力系统产生的海量数据进行深入挖掘和分析。在这个过程中，通过复杂的算法和模型，可以有效地识别出网络行为中的异常模式。这种识别不仅局限于已知的攻击手段，更重要的是能够发现新型和复杂的网络攻击模式。大数据的应用使网络安全防护不再是简单地应对，而是能够预测并主动防御，这对于电力系统这种关键基础设施尤为重要。

人工智能技术的引入，更是为网络安全防护带来了革命性的变革。人工智能系统能够学习和适应不断变化的网络环境和攻击模式，提高了对新型威胁的识别能力。特别是在自动化响应网络安全事件方面，人工智能展现出了无与伦比的优势。通过自动化处理安全事件，不仅大幅提高了应对速度，更重要的是提高了处理这些事件的准确性。在网络安全事件发生时，快速而准确的响应对于最小化损失至关重要。

大数据和人工智能技术的结合还为电力系统的网络安全管理提供了前所未有的视角和深度。这些技术能够帮助安全专家深入了解网络攻击的本质，发现潜在的安全漏洞，并制定出更为有效的防护策略。随着这些技术的进一步发展，未来的网络安全防护将更加智能化、精准化。

3.强化网络边界安全

电力系统信息网络的安全，从其边界开始，这一层是防御体系中至关重要的部分。网络边界像是一座坚固的城墙，守护着系统的安全，防止外部威胁的侵入。在这个前线，所有接入系统的外部设备和服务都承担着重要的角色，因此，对它们实施严格的安全审查变得尤为必要。这些设备和服务涵盖了供应商提供的硬件、云计算资源、远程访问工具等，它们可能成为潜在的安全漏洞。

为了强化这些边界点的安全性，持续的监控和管理是不可或缺的。这不仅涉及对设备和服务的初步审查，更包括对其运行状态的持续监视，确保它们在任何时候都不会成为网络攻击的突破口。在这个过程中，高效的监控系统和专业的安全团队发挥着核心作用，他们通过不断的观察和分析，能够及时发现异常行为，防止安全威胁的发生。

4.建立应急响应机制

面对网络安全事件，快速和有效的响应机制是减轻损失的关键。电力系统应建立一套完善的应急响应流程，包括事件的立即识别、评估、隔离和恢复等。同时，需要建立一个跨部门的应急响应团队，这个团队应该包括网络安全专家、系统工程师、法律顾问等，确保在安全事件发生时能够从多个角度迅速做出反应。

5.不断创新和改进

电力系统信息网络的安全防护是一个持续的过程，需要不断的创新和改进。随着网络环境的变化和攻击手段的升级，安全策略也需要相应地进行调整和更新。电力企业应该持续关注最新的网络安全趋势，积极参与行业内的交流和合作，学习和引入最新的安全技术和管理方法。通过不断的学习和创新，可以确保电力系统信息网络的安全防护始终处于最佳状态。

六、结论

电力系统信息通信网络的安全是一个多维度、动态变化的问题，它不仅关系到技术层面，更涉及管理、政策和人文等多个方面。本文通过对现有安全威胁的分析和对防护措施的审视，提出了结合教育、技术和管理的综合性解决策略。这些策略的实施旨在构建一个更为安全、稳定的电力系统信息通信网络。展望未来，随着技术的不断进步和安全威胁的日新月异，电力系统的信息安全将是一个持续的挑战，需要我们不断学习、探索和创新。只有这样，我们才能确保电力系统的稳健运行，支撑社会的持续发展。

参考文献

[1]欧阳宇宏，康文倩，车向北.电力监控系统信息通信网络安全及防护问题研究[J].信息系统工程，2020，33（12）：60-61.

[2]安子畅，杨硕，郑景.电力系统信息通信的网络安全及防护研究[J].通信电源技术，2020，37（5）：216-217.

[3]候正煜.电力系统信息通信的网络安全及防护研究[J].网络安全技术与应用，2020（2）：132-133.

[4]叶磊，刘立亮，张科健.电力系统信息通信的网络安全及防护研究[J].通讯世界，2019，26（9）：319-320.

[5]张在琛.泛在电力物联网关键支撑技术[J].电力工程技术，2019，38（6）：1-1.

[6]安子畅，杨硕，郑景.电力系统信息通信的网络安全及防护研究[J].通信电源技术，2020，37（5）：216-217.