

电力系统信息通信网络安全的防护研究

李智

国网四川射洪市供电有限责任公司

摘要：电力系统信息通信网络的安全性对于维护电力系统的稳定运行和数据的完整性至关重要。本文探讨了电力系统信息通信网络安全的各个方面，包括网络安全技术、数据安全技术和系统安全技术。并强调了制定明确的安全策略、定期安全演练与培训、以及建立完善的安全事件响应与恢复计划的重要性，这些对策不仅有助于预防潜在威胁，还能提高整个系统的抗攻击性和安全性。

关键词：电力系统；信息通信网络；安全

【DOI】10.12252/j.issn.2096-6288.2022.06.116

电力系统信息通信网络作为现代电力系统的核心组成部分，承载着大量的数据和控制信息。然而，随着网络威胁不断演化和增加，电力系统信息通信网络的安全性变得愈发重要。本文旨在探讨各种安全对策，以确保电力系统的稳定运行和数据的安全性。

一、电力系统信息通信网络概述

电力系统是国家经济的重要支柱，而其信息通信网络则充当着连接各个部分、确保系统协调运行的神经系统。随着科技的迅速发展，电力系统信息通信网络的角色变得愈发重要。电力系统通信网络包括了广泛的硬件和软件设备，用于监控、控制和优化电力系统的运行^[1]。这些网络连接了发电厂、输电线路、变电站以及终端用户，构建了一个复杂而庞大的系统。信息通信网络的作用不仅在于数据的传输，还在于实时监测电力系统的状态，支持远程操作和维护，以及提供数据用于系统的优化和改进。

电力系统信息通信网络的发展在很大程度上推动了电力系统的智能化和数字化。通过传感器、智能仪表和远程监控系统，电力系统能够更精确地感知电网状态、负荷变化和设备的健康状况。这为电力系统的运行提供了更多的数据支持，使得系统能够更灵活地应对各种挑战。然而，随着信息通信网络的不断扩展和深化，电力系统也面临着越来越多的安全威胁。网络攻击、恶意软件、数据泄漏等问题威胁着电力系统的稳定性和可靠性，因此有必要深入研究并采取有效的安全措施，以保障电力系统的正常运行^[2]。在这一背景下，本论文将着重探讨电力系统信息通信网络的安全性问题，并提出相应的防护策略。

二、电力系统信息通信网络的安全威胁

（一）外部威胁

①网络攻击

网络攻击是最为常见和直接的威胁之一，其中包括但不限于恶意入侵、拒绝服务攻击（DDoS）以及中间人

攻击。黑客可能试图获取未经授权的访问权限，篡改关键数据，或者干扰网络的正常运行。这类攻击不仅对电力系统的运行造成直接影响，还可能导致敏感信息泄露，危及系统的机密性。

②恶意软件

恶意软件是通过网络传播的病毒、木马、勒索软件等恶意代码的集合体。这些软件可能通过电力系统信息通信网络传播，感染关键设备或者控制节点。一旦感染，恶意软件可能导致设备故障、数据损坏，甚至使整个电力系统瘫痪。

③社会工程学攻击

社会工程学攻击是一种利用心理学原理欺骗人员，获取敏感信息或者趁虚而入的攻击手段。通过仿冒身份、伪装成可信实体，攻击者可能获得对电力系统的访问权限，从而执行恶意操作。这种类型的攻击通常利用人的弱点，使得防范相对更为困难。

（二）内部威胁

①内部人员

内部人员可能是故意的威胁源，也可能是由于疏忽或不当操作引起的意外威胁。这包括员工、供应商或其他有权访问电力系统信息通信网络的个体。内部人员的错误操作、故意破坏行为或者对安全政策的违反都可能导致系统崩溃或者数据泄露。

②设备故障

电力系统的硬件设备存在着各种各样的故障可能，其中包括但不限于设备失效、通信链路故障等^[3]。这些设备故障可能是由于自然灾害、设备老化或者恶意操作引起的。设备故障对电力系统的运行可能造成不可逆的损害，尤其是在紧急情况下。

③数据泄漏

数据泄漏是一种常见但危险的内部威胁。当敏感信息泄漏到未经授权的人员手中，可能导致隐私泄露、商业机密泄露等问题。这种威胁可能源自于恶意的内部人

员，也可能是由于网络漏洞或者不当的数据管理引起的。

三、电力系统信息通信网络安全的防护技术

（一）网络安全技术

电力系统信息通信网络的安全性直接关系到电力系统的稳定运行和数据的完整性。在面临不断演变的网络威胁时，采用先进的网络安全技术是确保电力系统信息通信网络安全性的关键步骤。

①防火墙技术

防火墙被认为是网络安全的第一道防线。它通过检查进出网络的数据流量，根据预定义的规则和策略来允许或拒绝数据的传输。在电力系统信息通信网络中，防火墙可以防止未经授权的访问、减缓拒绝服务攻击（DDoS）以及监控网络流量。防火墙的配置和管理需要根据电力系统的特定需求进行定制，以确保防护力度和性能的平衡。

②入侵检测与防御系统

入侵检测系统（IDS）和入侵防御系统（IPS）在电力系统信息通信网络中扮演着重要角色。IDS通过分析网络流量和系统日志，检测异常行为和潜在攻击。一旦检测到异常，系统可以触发警报或采取预定的防御措施。IPS更进一步，不仅能检测潜在威胁，还能主动采取措施进行防御，如自动阻止攻击源。

③虚拟专用网络（VPN）技术

在电力系统信息通信网络中，数据的加密和安全传输尤为重要。VPN技术通过在公共网络上建立安全的通道，使用加密协议对通信数据进行保护。这有效地防止了数据在传输过程中被窃取或篡改的风险。电力系统中采用VPN技术的通信通道可以确保敏感数据的机密性，尤其是在通过公共互联网进行数据传输时。

（二）数据安全技术

数据在电力系统信息通信网络中是至关重要的资源，因此确保数据的机密性、完整性和可用性是系统安全的基石。在应对日益复杂的威胁环境时，采用高效的数据安全技术成为维护电力系统信息通信网络安全性的不可或缺的一部分。

①加密技术

加密技术是保护数据机密性的关键工具。通过对数据进行加密，即对数据进行转换，使其在未经授权的情况下难以理解。在电力系统中，采用强大的对称加密和非对称加密算法，确保敏感数据在传输和存储过程中不被窃取或篡改。此外，定期更新加密算法和密钥管理策略对于维持加密的有效性至关重要^[4]。

②数字签名技术

数字签名技术用于验证数据的完整性和真实性。通

过在数据上应用数字签名，发送者可以确保接收者能够验证数据在传输过程中是否被篡改。在电力系统信息通信网络中，数字签名技术可以防止中间人攻击和数据篡改，保障关键数据的可信性。

③安全存储技术

安全存储技术涉及对存储在电力系统中的数据进行安全的管理和保护。这包括在存储介质上采用加密、访问控制和备份等措施。定期备份关键数据，并将备份存储在安全的离线介质上，以防止数据丢失。同时，强化对数据存储区域的访问控制，确保只有经过授权的人员能够访问敏感数据。

（三）系统安全技术

系统安全技术 in 电力系统信息通信网络中扮演着至关重要的角色，涉及对整个系统的监控、审计、认证和访问控制等方面。通过综合应用系统安全技术，能够有效应对内外部的潜在威胁，确保电力系统的运行不受干扰，数据不受损害。

①安全审计与监控

安全审计与监控系统对电力系统信息通信网络的实时活动进行记录、分析和审计。通过监控网络流量、系统日志和关键事件，可以及时发现潜在的安全威胁和异常行为。安全审计的记录对于事后的调查和分析提供了重要的依据，而实时监控则使系统管理员能够迅速做出反应，采取必要的安全措施，从而提高整个系统的安全性。

②认证与访问控制

认证与访问控制是确保只有经过授权的用户能够访问系统和数据的重要手段。强大的认证机制，如多因素认证和生物识别技术，可以有效防止未经授权的访问。同时，采用灵活的访问控制策略，确保不同用户有不同的权限，最小化潜在的内部威胁。这包括在网络设备、服务器和数据库上实施细粒度的访问控制，以限制对关键资源的访问。

在电力系统信息通信网络中，系统安全技术的应用需要根据系统的特性和运行环境进行调整。建议采用最新的认证标准和访问控制技术，以适应不断演变的威胁环境。此外，定期对系统进行安全审计，评估系统的整体安全性，并根据评估结果调整安全策略，以持续提升系统的安全性水平。

四、电力系统信息通信网络安全的防护措施

（一）安全策略制定与实施

电力系统信息通信网络的安全策略是确保系统长期稳定运行和数据完整性的关键组成部分。安全策略的制定与实施需要全面考虑系统的特点、威胁状况以及合规性要求。

首先，建立一个全面的风险评估是安全策略制定的第一步。该评估应该涵盖外部和内部威胁，包括网络攻击、数据泄漏、设备故障等。了解潜在威胁的性质和来源，有助于制定有针对性的安全对策。其次，在制定安全策略时，需确保策略的可理解性和可执行性。明确定义用户权限、数据分类和加密要求，以及对关键设备和系统的访问控制。同时，制定应急计划，明确安全事件的应对流程，包括通报、隔离、调查和恢复等步骤。制定的安全策略需要适应不断变化的威胁环境。定期的策略评估和更新是必不可少的。在这个过程中，要充分利用最新的威胁情报和安全技术，确保安全策略始终能够适应最新的威胁。再次，实施安全策略需要广泛的合作和协调。系统管理员、网络工程师、安全专家以及其他相关人员都需要参与实施的全过程。定期的培训和意识提升活动对于确保所有相关人员都理解并遵循安全策略至关重要。最后，在实施安全策略的过程中，要注重监测和反馈。建立监控机制，及时发现潜在威胁并采取相应措施。同时，通过事件的回顾和分析，不断优化安全策略，提高系统的整体安全性。

（二）定期安全演练与培训

①安全演练

安全演练是一种模拟安全事件的实践活动，旨在检验安全策略和应急响应计划的有效性。这些演练可以模拟各种威胁情境，包括网络攻击、数据泄漏、设备故障等。通过参与者模拟实际情况下的行动，演练能够评估团队的响应速度、协作效果以及对安全事件的处理能力。定期进行安全演练有助于发现并纠正安全策略和应急计划中的不足。同时，演练还可以提高团队成员对安全威胁的敏感性，使其更具备发现和应对潜在威胁的能力。最终，通过不断的演练，团队能够在真正发生安全事件时做出更迅速、更有效的响应。

②安全培训

安全培训是提高团队成员的安全意识和技能的重要途径。培训内容应该涵盖最新的威胁情报、攻击技术、安全最佳实践等方面。培训不仅要面向系统管理员和安全团队，还要包括所有与电力系统信息通信网络有关的人员，以确保整个组织的安全水平。培训课程可以包括网络安全基础知识、密码学、社会工程学攻击防范、安全意识等方面的内容。通过与实际案例的结合和实际操作的演示，培训能够使人员更深入地理解安全原理，并学到实际应对威胁的技能。

（三）安全事件响应与恢复

①安全事件响应计划的建立

安全事件响应计划应该明确规定在发生安全事件时需要采取的步骤和措施。首先，计划要明确识别潜在威

胁的方法和工具，以迅速发现并确认安全事件。其次，要建立隔离受影响系统的措施，以防止威胁扩散到整个网络。然后，计划中应包括清除威胁的详细步骤，确保系统得以从潜在的威胁中完全恢复。最后，追溯攻击者的步骤有助于将事件的责任人绳之以法，同时为未来防范提供有力的依据。

②迅速响应与损失减小

在发生安全事件时，时间是至关重要的因素。迅速响应可以减小潜在的损失，避免威胁扩散。团队应具备快速的决策和执行能力，以便迅速实施响应计划中的措施。这可能包括暂时关闭受影响的系统、切断网络连接、还原备份数据等。通过最小化安全事件的影响，可以降低损失并迅速恢复正常运行。

③模拟演练与计划评估

定期进行模拟演练是验证安全事件响应计划有效性的重要手段。通过模拟真实的安全事件场景，团队可以发现计划中可能存在的不足之处，进而进行改进。演练不仅包括技术层面的操作，还应该考虑到与相关利益相关方的沟通协调，以确保在真实事件发生时，团队能够协调一致地应对。同时，定期评估安全事件响应计划的有效性也是保持响应能力的敏捷性的关键。这可以通过定期审查计划、参与者的反馈、模拟演练的结果以及最新的威胁情报等手段来实现。根据评估结果，不断优化和更新计划，以确保其在不断变化的威胁环境中仍然具有高度的适应性。

结语

电力系统信息通信网络的安全是电力系统运行的基石。在当前威胁不断升级的环境下，必须不断提高警惕，采取多层次的安全措施，以应对各种威胁。制定明确的安全策略、定期进行安全演练与培训，以及建立完善的安全事件响应与恢复计划是确保电力系统信息通信网络安全的关键步骤。只有通过不懈的努力和持续的改进，才能保护电力系统的稳定性和数据的完整性，确保其为社会供电提供可靠的支持。

参考文献

- [1] 王桂彬. 电力系统信息通信网络安全及防护安全探究[J]. 信息通信, 2019(12): 168-169.
- [2] 吕旭明, 郑善奇, 曹丽娜等. 图数据库技术在电力系统信息通信资产管理中的应用[J]. 东北电力技术, 2017, 38(11): 27-30.
- [3] 张鸿毓. 电力系统中网络信息通信技术的应用分析[J]. 数字通信世界, 2017(08): 190.
- [4] 何湘君. 信息通信融合在电力系统中的应用[J]. 电子技术与软件工程, 2017(14): 26.