电网新一代集控系统中的网络安全问题研究

刘书占　张晓伟　杨红永
国网天津市电力公司高压公司

摘　要：本文深入探讨了电网新一代集控系统的核心技术、面临的网络安全问题，及其解决方案。新一代集控系统强调高度的自动化与智能化，运用了实时数据处理、人工智能、物联网等先进技术，以提升电网运行的效率和安全性。然而，随着系统对网络技术的依赖加深，多种网络安全挑战随之浮现，包括系统架构与设计的安全隐患、数据保护与隐私问题以及远程访问控制的风险。为应对这些安全问题，文中提出了包括安全加固与系统升级、数据加密与安全传输、访问控制与权限管理、安全检测与防范以及培训与教育等一系列综合性的解决方案。

关键词：电网；新一代集控系统；网络安全

1 电网新一代集控系统简介

随着技术的持续进步，电网新一代集控系统在未来的发展中将更加注重系统的集成性和开放性。通过与其他智能系统的融合，如智能建筑和电动汽车充电网络，集控系统的功能将更加多样化，更好地满足智能电网和城市化发展的需求。此外，系统安全性的提升也将是未来发展的重点，以保护电网免受网络攻击和物理破坏的威胁。电网新一代集控系统是以高度的自动化和智能化为特征，结合了最新的信息技术和通信技术，致力于提升电网运行的效率和安全性。这一系统的构成涵盖了多个关键组成部分，包括集中监控中心、数据采集与分析平台、高级决策支持系统以及远程自动化设备。

电网新一代集控系统技术的核心在于实现更高的自动化和智能化水平，以应对日益复杂的电网运行环境。这些技术主要包括实时数据处理、人工智能和物联网技术。实时数据处理技术能够快速处理和分析从电网各个部门传来的数据，确保信息的及时性和准确性。这对于预测和防止电网故障，优化电网运行至关重要。人工智能技术则在数据分析和决策支持方面发挥着重要作用，它通过学习历史数据和实时情况，可以提供更准确的负荷预测、故障诊断和维护建议。此外，物联网技术通过在电网各个节点部署传感器和智能设备，实现了对电网的全面感知和控制，极大地提高了电网的监控范围和效率。

2 电网新一代集控系统中存在的网络安全问题

2.1 系统架构与设计安全问题

系统架构方面，新一代集控系统通常采用高度集成和复杂的网络结构，以支持广泛的数据收集和处理需求。然而，这种复杂性本身就带来了多个安全隐患。首先，系统的集成性使得任何一个安全漏洞都可能影响到整个电网的安全。一旦黑客攻击或技术故障发生在系统的某个节点，便有可能迅速扩散至整个网络，导致广泛的数据泄露或操作失误。其次，电网集控系统的多依赖性也增加了其脆弱性。系统往往依赖于多种通信技术和网络设备，一旦这些基础设施受到攻击，整个系统的稳定性和安全性都将受到威胁。

设计安全问题则表现在系统设计初期可能未能充分考虑到所有潜在的安全威胁。例如，设计时可能过分侧重于系统功能的实现，而忽视了安全性的构建。这导致了系统在面对日益复杂的网络安全环境时，缺乏足够的防御措施。此外，随着技术的快速发展，原有设计中的安全措施可能无法有效应对新型的网络攻击手段，如零日攻击和先进的持续威胁（APT），使得系统容易受到攻击。

2.2 数据保护与隐私问题

电网新一代集控系统中的数据保护与隐私问题是随着技术发展逐渐显现的关键挑战。这些问题主要表现在数据泄露、未经授权的数据访问以及数据滥用等方面。

首先，数据泄露问题频发，尤其是在电网系统中，大量的用户数据和敏感的运行数据存储在集控系统中。这些数据若被泄露，不仅可能导致经济损失，还可能影响到电网的安全运行。泄露的原因多种多样，包括黑客攻击、系统安全漏洞以及人为的操作错误。由于电网系统的复杂性和规模庞大，一旦数据管理不当，就容易成为攻击的目标。其次，未经授权的数据访问问题也十分严重。在一些情况下，电网系统内部的访问控制和权限管理不够严格，导致未授权的人员能够访问敏感数据。这种情况可能因为权限设置错误、系

统设计缺陷或是监管不足等原因引发。此外，随着远程操作和监控技术的普及，如不采取足够的安全措施，外部攻击者可能通过网络侵入系统，获取或篡改关键数据。最后，数据滥用问题也不容忽视。在没有明确的法律法规和行业标准的指导下，即便是内部员工或合作伙伴也可能因缺乏足够的数据保护意识，而对收集到的数据进行不当使用。这不仅侵犯了用户的隐私权，还可能引起法律纠纷和社会信任危机。

2.3 远程访问控制问题

电网新一代集控系统中的远程访问控制技术，虽然带来了操作的便捷性和效率提升，但同时也引入了一系列安全风险和管理问题。这些问题主要表现在未经授权的访问、数据泄露以及操作失误等方面。

首先，未经授权的访问是远程访问控制中最严重的安全隐患之一。由于远程访问允许用户在网络的任何地点连接到电网控制系统，恶意攻击者可能利用网络安全漏洞侵入系统。一旦入侵成功，攻击者可以控制电网设备，甚至造成供电中断等严重后果。此外，远程访问的数据传输过程中如果没有得到充分加密保护，也可能导致敏感信息如用户认证数据、操作指令等被截获和泄露。

其次，远程操作的另一大问题是操作失误。远程访问通常依赖于复杂的界面和控制命令，操作人员如果对系统不够熟悉，或者在网络延迟等技术问题影响下，可能会发生误操作。这种误操作在电网系统中可能导致不可预见的负面影响，比如错误的数据输入或不当的设备控制命令，进一步影响电网的稳定运行。

造成这些问题的原因多种多样，技术原因包括系统设计的安全措施不足、加密技术应用不广泛或者技术本身的缺陷。此外，人为因素也不容忽视，如操作人员对远程控制系统的不熟悉、缺乏足够的安全意识或者培训不充分等。

2.4 网络攻击与防范问题

网络攻击已经成为当今数字化社会中一个严峻的问题，其影响范围从个人隐私泄露到影响国家安全的重大事件。这些攻击的表现形式多种多样，包括但不限于病毒感染、钓鱼攻击、拒绝服务攻击（DDoS）以及勒索软件的侵害等。例如，钓鱼攻击通过伪装成可信网站或通信，诱使用户透露敏感信息，如登录凭据和财务信息。DDoS攻击则通过向目标服务器发送大量请求，超出其处理能力，从而使网站或服务瘫痪。

网络攻击的原因可以从技术和人文两个层面进行分析。从技术层面看，许多网络系统和软件存在设计上的缺陷和漏洞，攻击者可以利用这些漏洞执行恶意操作。随着技术的快速发展，新的技术和工具的出现也为攻击者提供了新的攻击手段，使得防御措施不断面临新的挑战。此外，随着物联网和移动设备的普及，越来越多的设备连接到互联网，也为网络攻击提供了更多的入口。

从人文层面分析，网络安全意识的不足是导致网络攻击频发的另一个重要原因。许多用户和企业对网络安全的重视程度不够，缺乏有效的安全防护措施和应急响应计划。此外，随着网络攻击手法的多样化和复杂化，普通用户往往难以识别和防范新型攻击，使得网络攻击更易成功。

3 网络安全问题的解决方案

3.1 安全加固与系统升级

在网络安全问题的处理中，安全加固与系统升级是两个关键的方面。安全加固主要是指采取措施加强现有系统的安全性，避免潜在的安全风险和攻击。这通常包括安装防火墙和入侵检测系统来监控和阻止未授权的访问，使用加密技术来保护数据传输的安全，以及实施严格的访问控制，确保只有授权用户才能访问敏感数据或系统。

系统升级则涉及定期更新软件和系统，修补已知的漏洞。软件供应商经常发布更新来修复在软件中发现的安全漏洞。通过及时应用这些更新，可以有效防止攻击者利用这些已知漏洞进行攻击。此外，升级也可能包括替换过时的技术和系统，以采用更安全、更高效的解决方案。

为了有效实施安全加固和系统升级，企业需要进行持续的安全评估和风险管理，以识别和解决安全薄弱环节。同时，应当建立一个固定的维护窗口和程序，确保所有的安全更新和补丁能够在不影响业务连续性的前提下，迅速而有效地部署。通过这些措施，可以大幅提高系统的安全性，减少潜在的安全威胁。

3.2 数据加密与安全传输

数据加密与安全传输是网络安全的核心组成部分，旨在保护数据在存储和传输过程中的安全和隐私。加密技术通过将数据转换为只有持有正确密钥的用户才能解读的形式，有效阻止了未授权访问和数据泄露。

在实际应用中，对于数据的安全存储，常用的方法包括使用对称加密算法（如 AES）和非对称加密算法（如 RSA）。对称加密算法以同一个密钥进行数据的加密和解密，适用于加密大量数据，因其加解密速度快；而非对称加密则使用一对密钥，即公钥和私钥，其中公钥可公开，私钥需保密，这种方式常用于加密传输中的密钥

本身或小量数据。数据在传输过程中的安全性，通常通过实时传输层安全协议（如 TLS）来保证。TLS 协议通过在数据传输前建立安全连接，并在此过程中使用数字证书确保通信双方的身份，然后对传输的数据进行加密，有效保障了数据在 Internet 上的传输安全。

3.3 访问控制与权限管理

网络安全的核心组成之一是有效的访问控制与权限管理，这关系到如何确保数据和资源的安全使用。访问控制主要是限制用户对系统资源的访问权限，确保只有授权的用户才能访问敏感数据或操作关键系统。这通常涉及用户身份的认证和授权两个步骤。身份认证是确认用户身份的过程，常见的方法包括密码、生物识别技术及多因素认证等。一旦身份得到验证，系统将根据预设的策略授予相应的权限。

权限管理则是制定和维护用户权限的过程，其目标是确保每位用户只能访问其完成工作所必需的资源。实施最小权限原则是权限管理的关键策略，即用户只能获取完成当前任务所必需的最低级别权限。此外，定期审计用户权限和访问记录也非常重要，这有助于发现不当权限设置或滥用权限的行为，及时进行调整或处理。

3.4 安全检测与防范

在网络安全领域，进行有效的安全检测与防范是确保信息系统安全不可或缺的措施。首要步骤是实施全面的安全审计和风险评估，这涉及对现有信息系统的硬件、软件、数据处理和存储过程进行详尽的检查，以识别潜在的安全漏洞和威胁。基于这一评估，可以制订具体的安全策略和防护措施。

接下来，部署入侵检测系统（IDS）和入侵防御系统（IPS）至关重要。这些系统能够监控网络流量和系统活动，实时检测和响应异常行为或已知的攻击模式。同时，定期更新防病毒软件和应用程序补丁是基本的安全维护工作，可以有效防止恶意软件感染和利用已知漏洞发起攻击。

此外，加强用户认证和访问控制机制也是防范网络安全问题的重要手段。采用多因素认证和最小权限原则可以大大减少未授权访问和数据泄露的风险。最后，加强网络安全意识培训，使每位员工都能意识到网络安全的重要性，掌握基本的安全防护知识和技能，这是提高整体网络安全防御能力的关键。通过这些综合措施的实施，可以为企业和组织构建一道坚固的网络安全防线。

3.5 培训与教育

网络安全培训与教育是提高组织和个人抵御网络威胁能力的关键措施。有效的培训和教育项目应包含几个核心组成部分。首先，基础教育是必需的，它涉及对所有员工进行关于常见网络威胁、如钓鱼攻击、恶意软件等基本知识的普及。这种基础教育有助于提高员工的安全意识，使他们能够识别和防范基本的安全威胁。进一步地，针对具有特定职责的员工，如 IT 支持团队和网络安全人员，进行更深入的技术培训。这种培训包括高级安全协议、加密技术、入侵检测系统的使用等，旨在使这些员工能够管理复杂的网络安全任务和应对更高级的网络攻击。最后，培训和教育应该是持续的，而不是一次性的活动。网络安全环境不断变化，新的威胁和技术陆续出现。因此，定期更新培训内容和教育材料，以及定期进行安全演习和测试，是确保持续有效性的关键。通过这些综合措施，可以大大提高组织和个人对抗网络安全威胁的能力。

4 结束语

通过详细分析电网新一代集控系统的技术特点和面临的网络安全挑战，本文强调了在现代电力系统中，安全性和技术创新同等重要。随着技术的进步，电网系统不仅需要不断优化其性能，更要加强安全防护措施，以防范和应对日益复杂的网络威胁。同时，持续的员工培训和教育也是保障网络安全的关键，它确保每位员工都能够在变化的安全环境中作出正确的判断和应对。综合这些策略，我们能够为电网的安全和稳定运行提供坚实的保障，支持电力行业在未来发展中的持续创新与进步。

参考文献：

[1]新一代变电站集中监控系统通过实用化验收[J].大众用电，2023，38（07）：37.

[2]杨骏，王劲林，倪宏，等.基于 KG-DBN-SVM 的工控网络安全态势感知算法[J].网络新媒体技术，2023，12（03）：10-19.

[3]徐文，郭伟伟，胡睿聪.电网新一代集控系统中的网络安全问题研究[C]//上海筱虞文化传播有限公司.河南许昌国网河南省电力公司禹州市供电公司；河南许昌国网河南省电力公司许昌供电公司；，2023：2.

[4]贾志强.基于工控网络数据的网络安全态势分析研究[D].华北电力大学（北京），2023.

[5]刘彬.新能源集控中心接入电网系统若干问题的探讨[J].红水河，2023，42（01）：80-83+104.

[6]张宁，俞尧，贾栋栋，等.新能源集控中心的计算机网络安全措施分析[J].集成电路应用，2022，39（08）：230-231.