厂站端调度自动化数据网络的安全防护

白云海，陈兴东
（国网河北省电力有限公司超高压分公司，河北省石家庄市，050000）

摘要　厂站端调度自动化系统及其数据网络是电力系统安全稳定运行的重要支撑，随着网络技术的迅速发展以及网络安全威胁的日益增加，构建全面的安全防护体系显得尤为重要。因此，本文旨在探讨厂站端调度自动化系统及数据网络的安全防护机制，提出有效的安全防护策略，以确保厂站端调度自动化系统及数据网络信息的安全可靠运行。

关键词　厂站端；调度自动化系统；数据网络；安全防护

中图分类号：TQ330.4+93　文献标识码：B
文章编号：1008-0899(2024)12-0053-03

从不同的视角审视厂站端调度自动化系统及其数据网络的安全防护，可以发现安全防护不仅仅是技术问题，更是一个涉及管理、制度以及文化的综合体。在这一理论视角下，安全防护被视为一个系统工程，其成功地实现依赖于多个因素的相互作用。技术层面的创新是基础，它要求不断地探索应用新技术来防御日益复杂的安全威胁。仅有技术创新是不够的，还必须建立一套完善的管理制度，包括安全政策的制定、人员的安全培训以及安全文化的培育。这些制度性措施能够确保技术应用的有效性，形成全员参与的安全防护氛围。此外，该理论还强调了跨界合作的重要性，即通过与其他行业的交流合作，借鉴其成功的经验，进一步强化电力系统的安全防护能力。通过这种综合性的理论视角，可以更全面地应对厂站端调度自动化系统及其数据网络面临的安全挑战。

1　自动化系统及数据网络安全防护的概述

厂站端调度自动化系统及其数据网络安全防护构成了现代电力系统中一个至关重要的领域。随着信息技术的广泛应用，这些系统不仅承载着电力调度以及管理的核心任务，也成了确保电力供应可靠性的关键。然而，随着技术的进步，这些系统面临的安全威胁也日益增多，包括恶意软件攻击、数据泄露、系统篡改等，这些威胁不仅可能导致数据丢失或泄露，还可能引发更严重的电力供应中断，甚至影响国家安全。

在构建安全防护体系时需要注意以下事项：①需要识别潜在的安全威胁，这包括对系统脆弱性的深入分析并对可能攻击路径的预测；②通过采取一系列技术措施来增强系统的防护能力，如使用先进的加密技术保护数据传输的安全，部署入侵检测的预防系统以识别潜在攻击，以及实施严格的访问控制策略，确保只有授权用户才能访问敏感信息；③定期的安全审计以及漏洞扫描也是不可或缺的，其能够及时发现并修复安全漏洞，降低被攻击的风险。

2　自动化系统及数据网络安全防护的应用

2.1　入侵检测系统的应用

在电力系统的安全防护体系中，入侵检测系统（IDS）与入侵防御系统（IPS）的融合应用扮演着至关重要的角色。通过对网络及系统活动进行连续的监控，这些系统能够实时识别各种潜在的恶意行为，例如未经授权的访问、病毒侵袭或不寻常的流量模式。IDS专注于监测安全威胁并进行报告，而IPS在此基础上进一步采取必要措施来阻止这些威胁，从而确保了系统的完整性与可用性得到保护。这一机制有效提升了电力系统面对外部攻击时的防御能力，是维护电力供应稳定性与可靠性不可或缺的一环。通过实现这样的安全措施，可以大幅度降低系统遭受破坏的风险，确保电力系统能够在各种威胁面前保持正常运作。

2.2　数据加密技术的应用

作者简介：白云海（1994~），男，汉族，河北石家庄人，硕士，工程师，研究方向：自动化。

数据加密技术在厂站端调度自动化系统的信息安全保护中发挥着核心作用，通过将传输存储过程中的数据转化为只有授权用户才能解读的密文，有效地避免了数据在被截获时的泄露风险。通过采用先进的加密算法以及实施严格的密钥管理策略，系统能够确保关键信息如控制命令、系统运行状态及用户个人信息的安全性。这种技术不仅提升了系统对抗外部威胁的能力，还保障了电力系统运行的安全，是电力系统安全防护措施中不可或缺的一环。

2.3 访问身份验证的应用

访问控制的身份验证在维护厂站端调度自动化系统的安全架构中扮演着关键角色。这些机制通过设定一系列严格的访问策略，确保只有经过授权的用户能够接触到系统的关键部分及敏感数据。采用如双因素认证、生物识别技术等先进的身份验证方法，能够大幅提升访问控制的安全水平，有效防止未经授权的访问或恶意操作，从而维护了系统及数据的安全。这些措施的应用不仅保护了系统免受外部攻击，同时也防止了内部威胁，确保了电力系统的稳定运行。

2.4 安全应急计划的制定

构建并执行有效的安全策略与应急响应计划是厂站端调度自动化系统安全管理的核心。这涉及全面的安全威胁评估，基于此评估结果制定针对性的防护措施，以减轻潜在的安全风险。安全策略为系统提供了一个预防框架，而应急响应计划则确保了一旦发生安全事件，能够迅速且有效地反应，从而最大程度地减少损失。这包括了详细的响应程序、系统恢复计划以及确保信息流通的通讯协议，旨在保证在紧急情况下，所有相关人员都能按照既定方案行动，保持响应的效率。通过这样的安全应急计划，不仅可以提升系统对抗安全威胁的能力，还能确保在遭遇攻击时，系统的关键功能能够得到快速恢复，保障电力系统的连续运行以及数据的完整性。

3 自动化系统及数据网络安全防护的创新建议

3.1 智能行为分析与异常检测技术融合

智能行为分析与异常检测技术的融合代表了厂站端调度自动化系统及数据网络安全防护领域中的一大创新方向。在日益复杂的网络环境中，传统的安全防护机制已经难以应对多样化的安全威胁，尤其是那些精心设计的、隐蔽性强的攻击。智能行为分析技术通过分析正常的网络以及系统行为模式，建立行为基准，能够实时识别出与这些基准有显著偏差的异常行为。当异常检测技术与之结合时，系统不仅能够依据预定义的规则识别已知威胁，还能利用智能算法发现未知，大大提高了安全防护的有效性。这种融合应用能够为厂站端调度自动化系统提供更加全面深入的安全保障，有效减少安全事件的发生。

通过部署在厂站端的传感器以及日志系统收集操作数据，利用机器学习算法分析这些数据，系统能够学习到电力调度自动化系统在正常运行状态下的行为模式。当检测到偏离这些正常模式的行为时，如非授权访问、数据流量异常增加或未知的系统命令执行等，系统即可立即触发警报，并启动预定的安全响应措施。这种方法的一个关键优势在于其自学习及其自适应的能力，使得安全系统能够持续进化，适应新的威胁环境。

3.2 基于区块链的数据传输安全的增强

基于区块链的数据传输安全增强方法在厂站端调度自动化系统中的应用，提供了一种创新的安全防护机制。区块链技术以其分布式账本、数据不可篡改以及高度加密的特性，为数据传输安全提供了新的解决方案。在厂站自动化网络安全领域，利用区块链技术可以确保数据在传输过程中的真实性，有效防止数据被篡改或伪造。此外，区块链的去中心化特性能够降低单点故障的风险，增强系统的抗攻击能力。通过将区块链技术与现有的网络安全措施相结合，可以构建一个更加安全可靠的厂站端调度自动化系统，为电力系统的稳定运行提供坚实的安全保障。

通过在厂站端调度自动化系统中部署区块链技术，每条数据在传输前都被加密并打包成一个区块链上的交易，所有交易记录被分布式存储在多个节点上，确保了数据传输的安全性。当数据从发送端传至接收端时，接收端可以通过验证区块链上的记录来确认数据的真实性。此外，任何试图篡改传输数据的行为都会被区块链网络识别并拒绝，因为篡改后的数据无法得到网络中大多数节点的验证。这种基于区块链的安全增强方法不仅提高了数据

传输的安全性，还提升了整个电力调度系统的抗干扰能力，从而为自动化网络安全防护树立了新的标杆。

3.3　深度学习技术在网络安全中的应用

深度学习技术依托其强大的数据处理以及模式识别能力，能够有效地识别网络流量和用户行为中的复杂模式，包括那些传统方法难以察觉的细微异常。通过对正常与异常行为的深入学习，深度学习模型能够预别出恶意软件、钓鱼攻击以及内部威胁等潜在的安全威胁，从而为网络安全防护提供了一种更为动态的防御手段。

深度学习技术在网络安全中的应用不仅限于威胁识别，还包括威胁情报的生成、安全事件的预测以及安全策略的自动化调整等方面。例如，通过训练深度神经网络模型分析历史安全事件以及当前网络活动，可以有效地预测未来可能发生的安全事件，从而提前采取预防措施。此外，深度学习还可以辅助开发出更为精准的安全策略，通过不断地学习网络环境的变化，动态地调整防护措施，以实现更加灵活有效的安全防护。在厂站自动化网络安全方面的具体应用中，深度学习技术可以帮助识别复杂的攻击模式，如针对工控系统的定制化恶意软件，以及通过正常通讯协议进行的隐蔽攻击等，极大提高了安全防护的效率。

3.4　多因素身份认证机制的创新性设计

传统的单一认证方式，已无法满足当前网络安全的需求，容易受到各种攻击的威胁，如钓鱼攻击、密码破解等。多因素身份认证（MFA）通过要求两个或更多验证因素，显著提高了安全性。这些验证因素通常包括用户知道的信息（如密码）、用户拥有的东西（如手机或安全令牌）以及用户本身的特征（如指纹或面部识别）。这种方法的核心优势在于即使其中一个因素被破解，攻击者也难以获得系统的完全访问权限，从而大大增加了安全防护的深度。

深入探讨多因素身份认证机制的创新性设计，可以从以下进行理论论证。①创新设计需要考虑用户体验以及安全性之间的平衡。例如，虽然增加验证因素可以提高安全性，但也可能导致用户操作变得繁琐。因此，设计时可以引入智能化元素，如基于用户行为及其访问地点的风险评估，动态调整认证强度；②考虑到不同厂站自动化系统的特定需求，多因素身份认证机制应支持生物识别、基于移动设备的认证，以及基于物理令牌的认证等多样化的认证方式，以适应不同的操作环境；③为了增强系统的抗攻击能力，可以结合区块链等技术，利用其分布式的特性，安全存储认证信息，保证认证过程的透明性。通过这些创新设计，不仅可以提高厂站端调度自动化系统的安全防护能力，还可以为用户提供便捷、灵活的操作体验，从而在提升系统安全性的同时，也保证了系统的高效运行。

4　结论与展望

综上所述，随着信息技术的飞速发展和电力系统自动化程度的不断提高，厂站端调度自动化系统及数据网络面临的安全威胁日益增多，安全防护的重要性日益凸显。从智能行为分析与异常检测技术的融合应用，到基于区块链的数据传输安全增强，再到多因素身份认证机制的创新设计，以及深度学习技术在网络安全中的应用，这些创新建议不仅展示了当前电力系统安全防护领域的研究动态，也指明了提升系统安全性的有效途径。这些技术的应用能够显著提高电力系统的安全防护能力。

参考文献

[1]　乌兰.电网系统调度自动化数据网络的安全防护措施探究[J].电子世界,2020,(10):179-180.

[2]　蒋斌.电网调度自动化系统设计及其数据网络安全防护[J].电子元器件与信息技术,2020,4(02):43-44.

[3]　杨天丽.调度自动化系统及数据网络安全防护技术[J].通讯世界,2019,26(12):266-267.