工程与管理科学
Engineering and Management Science
第 7 卷◆第 2 期◆版本 1.0◆2025 年
文章类型：论文|刊号（ISSN）：2705-0637(P) / 2705-0645(O)

电力调度自动化二次系统安全防护技术的应用研究

丁翔　原哲　林瑞峰　王若惠　王玲
国网焦作供电公司　河南省焦作市　454100

DOI：10.12238/ems.v7i2.11677

[摘　要] 在电力系统运行的过程中，保障其智能化与自动化水平得以不断提高是非常重要的一项举措。而电力调度自动化二次系统的安全防护，便逐渐成为保障电网安全稳定运行的关键所在，同时也是从根本上实现电力系统运行质量得以全面提高的必由之路。因此，通过对电力调度二次安全防护系统及电力调度数据网展开深度研究，并探讨防护网的相关内容，以构建多层次安全防护体系，从根本上确保电力系统在长期运行的过程中处于相对安全的状态，以避免出现窃电问题或电能损耗过大等诸多因素的存在而带来的深刻影响，进而为日后更好的实现用户用电需求得以高质量实现的目标奠定坚实的基础。基于此，本文通过电力调度自动化二次系统安全防护技术的应用策略展开深度分析，希望可以为进一步提高电力系统运行工作的整体效率带来切实有效的帮助，并在这一基础之上实现电力企业综合效益得以全面提升的目标。

[关键词] 电力调度；自动化；二次系统；安全防护技术

引言：

电力调度自动化二次系统作为电力系统的核心组成部分，其负责监控控制及保护电网的运行。然而，随着电力系统的自动化与自动化技术的不断提升，二次系统在运行的过程所面临的安全威胁也日益严峻，黑客攻击、病毒入侵与代码传播的安全事件的发生时有发生，给电网安全运行带来了十分严重的威胁与挑战。因此，为了能够更好地实现电力系统稳定运行的目标，并构建多层次的安全防护体系，就应当被视为保障电网安全引进问题的关键所在。基于这一点，工作人员就需要对以往所开展的电力调度工作予以深度重视，并通过构建电力调度自动化的安全防护体系作为开展电力企业日常工作中需要重点关注的一项内容，并以此实现保障电网安全运行的最终目标。而这也正是在未来开展电力调度自动化工作的过程中，需要引起工作人员高度关注的一项重要内容。

一、防护系统的核心算法研究

（一）密码学技术在数据加密与身份认证中的应用

密码学技术是保障电力调度自动化二次系统数据安全的关键手段。基于密码学技术的数据加密与身份认证算法，并通过对敏感数据进行加密处理的方式，以确保数据在传输和组织的过程中，具有机密性和完整性的优势。此外工作人员还可以采用设备认证技术对访问系统用户进行设备验证，以避免因未经授权的访问和操作所带来任何影响。通过采用最为先进的加密算法和身份认证协议，以确保数据的安全性和可靠性，进入从根本上确保电力调度自动化二次系统安全防护技术在应用的过程中，不会出现各类信息泄露的问题，进而从根本上实现电力系统得以稳定运行的预期目标。

（二）入侵检测系统的设计与实现

入侵检测系统是及时发现并防范网络攻击的重要工具。机器学习与深度学习的入侵检测算法是通过对网络流量进行实时监测与分析的方式，识别并阻止潜在的恶意攻击及其所在的影响。入侵检测系统的应用，能够自动学习正常网络流量的特征，并建立与之相对应的行为模型，对异常流量进行报警与拦截。一般而言可以采用支持向量机、随机森林、神经网络等先进的机器学习算法，以全面提升入侵检测工作的准确性和效率，使得电力系统在长期运行的过程中能够避免因恶意侵袭的存在所带来的深刻影响，确保民众的用力安全得到满足。

（三）安全隔离装置的研发与应用

安全隔离装置是防止恶意代码的传播和攻击扩散的重要途径。基于物理隔离和逻辑隔离的安全隔离装置，并通过在网络边界设置安全隔离装置，以实现内外网络的物理隔离、逻辑隔离。安全隔离装置则可以对网络的数据进行严格的过滤检查，以防止恶意代码和病毒的入侵，阻断对自身的影响。同时，安全隔离装置还可以支持数据单向传输与签名认证，以确保数据具有安全性与完整性的优势。由此可见，安全隔离装置的应用，对于电力调度自动化二次系统安全防护技术这一广泛应用的目标将会产生十分深刻地影响，并在这一基础之上使得该项技术的使用效率得到进一步提高，并避免出现因恶意窃取的问题给电力系统的运行所带来的深刻影响。

二、网络边界防护与安全配置研究

（一）网络边界防护策略的实施与制定

网络边界是电力调度自动化系统安全防护工作的第一道防线。基于防火墙，入侵防御系统等技术的网络边界防护策略。具体而言，通过在网络边界设置防火墙或入侵防护系统等方式，对进出网络的数据进行严格的过滤和检查，进而避免因恶意攻击和病毒侵袭所带来的影响。基于访问控制列表的细粒度访问控制策略，通过限制用户对系统资源的访问权限，以防止因未经授权的访问和操作给电力企业的运行所带来的深刻影响，并在这一基础之上是由网络资源能够充分的发挥自己应有的作用，进而实现对各类资源进行优化与配置的目标，电力调度工作也能够按部就班地开展[1]。

（二）安全配置的优化与加固

安全背景是保障电力调度自动化二次系统得以安全稳定运行的前提和基础,基于最佳实践的安全配置优化交互方法，通过对系统配置进行定级审查与加固方式，从根本上保障配置符合安全标准进行管理规范。通过对网络设备的配置，操作系统的配置与应用系统配置等诸多方面的内容予以重点关注，并关闭不必要的服务，采取限制远程访问、加强密码策略等方式。使得电力系统在运行的过程中具有安全性与稳定性的目标，同时也可以借此为实现电力调度自动化二次系统安全保护技术的高效应用带来切实有效地意义。因此，在未来开展电力系统运行与维护工作的过程中，都需要对电力调度工作采取高度谨慎的状态，以避免出现不稳定因素而带来的深刻影响[2]。

（三）安全审计与日志管理

管理工作是有效发现和防范安全事件的重要手段，基于安全审计和日志管理工作的安全保护策略，并通过定期对系统日进行时代与分析方式及时发现潜在人群风险与异常行为。此外，基于集中制管理的安全防护措施，通过将各类设备的日志集中储存与管理，实现对各个系统进行全面监控与产业的目标，使得日记分析工作的总体效率和准确性达到较

高的水准。因此，在未来开展电力调度自动化二次系统安全防护工作的过程中，工作人员就需要做好安全检查与日常管理工作，以减少在开展电力调度工作的过程中出现的各类问题，并在这一基础之上使得安全审计与日志管理工作能够更为真实地反应电力调度工作的真实情况，为之后更好地实现其全面发展任务奠定坚实的基础[3]。

三、安全分层分区的具体策略

在利用电力调度自动化二次系统安全防护技术工作的过程中，工作人员也需要根据不同的用电区域，对其制定与之相对应的安全防护策略，以避免因策略不当导致各电力系统在运行的过程中面临研究安全问题的情况，同时也使得用户的体验得到进一步改善。因此，在未来开展电力调度工作的过程中，工作人员就应当采取行之有效的策略，积极开展安全分层分区工作，要结合不同的区域选择合适的技术手段展开电力调度工作，从根本上保证电力调度工作效率得到进一步提高。具体而言，目前安全分层分区的策略主要体现在以下几个方面。

（一）安全分层分区策略的制定

安全分区分层是保障电力调度自动化二次系统安全防护的重要措施。基于安全分层分区策略的安全防护体系，将系统划分为不同的安全区域城市，以实现不同区域和层次的安全防护与管理。而依据系统的功能与安全需求，工作人员一般将系统划分为生产控制大区，信息管理大区等不同的安全区域。并在各个区域内设置不同的安全层次，如网络层、应用层、数据层等。通过实施安全分层分区策略，全面提高社区的安全性与可靠性，从根本上避免出现各类问题，同时也可以便于集中管理减少因此类问题的存在所带来的能源浪费问题，进而为更好地实现节约能源，保护环境的目标贡献自己的力量。

（二）逻辑隔离与访问控制策略的实施

逻辑隔离是防止恶意代码传播与攻击扩散的重要途径，基于防火墙，安全隔离装置等技术的逻辑隔离策略。通过在网络边境设置逻辑隔离装置，以实现代表网络之间的逻辑隔离。此外，该项目还研究了基于访问控制列表的犀利度访问控制策略。并借助于限制用户对系统资源访问权限的方式，以避免出现未经授权进行访问与操作的问题。而通过实施逻辑隔离与访问控制策略，则可以切实有效的是系统安全基于稳定性得到进一步提高，同时也可以避免因异常状况的存在所带来的深刻影响。因此，在未来开展电力调度工作的过程中，工作人员就应当采取切实有效的措施，以保证工作安全及稳定性。作为开展日常工作的中心原则，

（三）安全监测与应急响应机制的建立

安全监测与应急响应机制的构建，是有效防范安全事件的重要手段，通过基于安全监测与应急响应机制，安全防护机制通过定期在系统中加入安全监测与防护评估机制，找到了潜在的安全风险影响行为。此外，该法通过教育项目较为完善的应急响应机制，其中包括应急预案的制定与应急研究的开展、应急资源调配等方面。而通过实施安全监测与应急响应机制后，可以使得系统的安全性和稳定得到进一步提高，同时也可以从根本上确保系统的运行效率达到较高的水准，由此可见在未来开展二次系统安全防护技术的相关工作时，工作人员就需要对安全监测与应急响应机制的建立工作采取了高度重视的态度，要避免出现严峻风险的情况。因此，工作人员就需要做好安全监测与应急响应机制的建立流程，从根本上避免其出现了较为严峻的安全风险，实现了企业经济效益的持续增长[4]。

（四）跨区数据交换

跨区数据交换是电力调度自动化二次系统是不可避免的重要需求，为了能够确保跨区数据交换的安全性由然而生，该机制涉及数据加密、身份认证、访问控制等诸多方面，以确保数据的承受的过程中具有机密性，完整性与可用性。同时，该项目还对跨区数据交换进行定期的安全审计风险评估工作，并借此机制有效的发现各类潜在风险，对电力系统的运行所带来的深刻影响。因此，在未来进行电力调度工作的过程中，工作人员就应当充分重视跨区数据交换所带来的问题，从根本上确保电力调度自动化二次系统在运行的过程中处于相对安全的状态，减少在运行的过程中可能会出现的各类问题[5]。

四、实际应用与风险评估

将电力调度自动化二次系统安全保护技术应用于实际系统中，取得了相对较为显著的成效。通过采用先进的加密算法、入侵检测与防御技术，严格的限制访问控制以及合理的安全区分设计。本项目也有效地提升了系统的风险保护能力。在实际运行的过程中，系统可以有效发现并防范因网络攻击的存在所带来的任何影响，同时也可以从根本上确保数据的安全传输与存储，而数据的安全性与稳定性也因此得到了进一步提高，为电力系统的安全运行提供了有力保障。为了评估实验效果，还进行了一系列实验流程，表明防护技术的应用能够为系统的安全防护能力带来切实有效的作用，并降低安全风险存在的相关影响。同时，用户反馈也表明系统安全性与应用性得到了显著集中。用户的体验感也将会在长期的阅读过程中得到进一步改善。因此，在未来开展电力工作的过程中，工作人员就应当对电力调度自动化二次系统安全保护技术的应用采取高度重视的态度，并结合安全系统发展的主要方向，在未来开展电力工作的过程中对新技术进行优化与调整[6]。

结语：

总的说来，在电力行业日益发展的大背景下，电力调度工作的重要性不言而喻。而电力调度自动化二次系统安全防护技术的应用。则可以在一定程度上为电力企业高效提升自身的工作效率带来了切实有效的帮助。通过深度探讨网络系统的核心算法、网络边界、网络安全配置以及安全分成分区等设置内容。证明了采用先进的加密算法、入侵检测与防御技术，严格的访问控制策略以及安全的分区分层设计，能够切实有效地提高整个系统的安全保护能力。为电力系统的稳定运行提供了强有力的保障。因此，在未来开展电力工作的过程中，工作人员就应当广泛的应用电力调度自动化系统安全防护技术，以实现电力企业经济效益的全面提高的目标，而这也正是在未来提升电力企业的经济效益时，需要工作人员采取的一项切实有效的措施。

[参考文献]

[1]周耀辉，张斌，代立君，郭宝.电力调度自动化二次系统安全防护技术应用分析[J].科技与创新，2024（23）：175-177+181.

[2]厉恒.电力二次系统网络安全隔离技术应用研究[J].电力系统装备，2024（9）：52-54.

[3]姜坤.发电厂调度自动化系统二次防护探讨[J].中文科技期刊数据库（引文版）工程技术，2022（10）：182-185.

[4]刘晓鹏，田永军，徐正国，李保权.电力调度自动化二次系统安全防护技术研究[J].中文科技期刊数据库（全文版）工程技术，2021（7）：253-254.

[5]丁立顺.电力调度自动化二次系统安全防护研究[J].技术与市场，2021，28（10）：115-116.

[6]吴一.研究电力调度自动化二次系统安全防护[J].中文科技期刊数据库（引文版）工程技术，2021（12）：239-240+244.