电力调度自动化网络安全以及实现研究

王鸿彦 时尚松 徐万勇
国网新疆电力有限公司博尔塔拉供电公司，新疆 博尔塔拉蒙古自治州 833400

[摘要]随着信息技术在电力行业的广泛应用，电力调度自动化系统变得日益智能化和复杂化，自动化不仅提高了电力系统的运行效率，也带来了新的安全风险，网络威胁的不断演变和加剧，以及电力系统的特殊性，使得网络安全问题成为当务之急。过去几年中，电力行业频繁发生的网络攻击事件凸显了电力调度自动化系统面临的严峻挑战。因此需要通过系统性的网络安全体系构建，全面提升电力调度自动化系统的防护能力，确保电力系统的平稳运行和信息资产的安全性。

[关键词]电力调度；调度自动化；网络安全
DOI：10.33142/hst.v6i11.10781 中图分类号：TP393.08 文献标识码：A

Research on Network Security and Implementation of Power Dispatch Automation

WANG Hongyan, SHI Shangsong, XU Wanyong
Bortala Power Supply Company of State Grid Xinjiang Electric Power Co., Ltd., Bortala Mongolian Autonomous Prefecture, Xinjiang, 833400, China

Abstract: With the widespread application of information technology in the power industry, power dispatch automation systems have become increasingly intelligent and complex. Automation not only improves the operational efficiency of the power system, but also brings new security risks. The continuous evolution and intensification of network threats, as well as the particularity of the power system, make network security issues an urgent task. In the past few years, frequent network attacks in the power industry have highlighted the severe challenges faced by power dispatch automation systems. Therefore, it is necessary to build a systematic network security system to comprehensively enhance the protection ability of the power dispatch automation system, ensure the smooth operation of the power system and the security of information assets.

Keywords: power dispatch; dispatch automation; network security

引言

电力调度自动化系统在现代能源体系中发挥着至关重要的作用，实现了对电力系统的高效管理和优化，随着数字化技术的飞速发展，电力系统也面临着日益复杂和严峻的网络安全挑战。网络攻击、数据泄露和系统故障可能对电力调度自动化系统产生严重的影响，威胁到电力系统的安全性、稳定性和可靠性，建立健全的电力调度自动化网络安全体系势在必行。

1 电力调度自动化的概况

电力调度自动化是电力系统中关键的技术，通过先进信息和自动化控制，实现对电力系统的高效监控、灵活调度和智能控制。传统调度方式已难满足复杂电力需求和系统规模的挑战，而电力调度自动化通过计算机、通信和自动控制技术，提供实时监测、数据处理和分析，为调度员提供准确决策支持。这提高了电力系统的运行效率、可靠性，并为清洁能源的大规模接入提供了支持。电力调度自动化被认为是推动电力系统现代化和可持续发展的关键技术。

2 电力调度自动化网络安全体系构建的必要性

电力调度自动化网络安全体系的建设具有迫切的必要性。首先，随着电力系统的数字化和信息化程度不断提升，电力调度自动化系统涉及到大量敏感数据和关键操作，如实时电网状态、负荷分布、设备运行情况等，若未能有效保护这些信息免受恶意攻击，可能导致电力系统的不稳定甚至瘫痪，给国家能源安全带来重大威胁。其次，电力调度自动化网络的开放性和互联性使得其面临来自网络威胁的多重风险，恶意软件、网络攻击和信息泄露等威胁不断演变，对电力系统的网络安全提出了更高的要求。在数字化的背景下，安全漏洞可能被利用来远程操控电力设备，威胁电网的运行和数据的完整性。此外，电力系统的关键基础设施往往是国家经济的支柱，稳定运行直接关系到社会的正常生活和产业的正常运转。一旦电力调度自动化系统受到攻击，可能引发连锁反应，对国家经济和社会秩序造成巨大损失。因此，建设电力调度自动化网络安全体系不仅是电力系统自身的需要，也是维护国家安全和社会稳定的关键一环。

3 电力调度自动化网络安全体系的关键影响因素

3.1 系统因素

在构建电力调度自动化网络安全体系时，系统因素是至关重要的一部分。系统因素涉及到整个电力调度自动化系统的设计、结构和运行机制，对网络安全具有深远的影响。系统的整体设计和架构直接决定了对安全威胁的抵御

能力，采用分布式架构、多层次的安全防护以及冗余设计，能够降低单点故障的风险，提高系统的抗攻击性，合理的系统划分和隔离也是系统因素中的重要考虑因素，确保在发生安全事件时能够最小化损失。系统的数据传输和通信机制对安全性具有直接影响，采用加密技术、安全协议和身份验证机制，可以有效防范网络窃听、数据篡改和身份伪造等攻击，确保在系统内外的数据传递过程中信息的机密性和完整性，是系统因素中必不可少的一环。定期的系统升级和漏洞修复，能够及时消除已知的安全漏洞，提高系统的抵御能力，合理的权限管理和访问控制机制，确保只有授权人员能够访问系统关键组件，是系统因素中的一项关键措施。

3.2 技术因素

技术因素在电力调度自动化网络安全体系的构建中发挥着至关重要的作用，涉及到采用先进的安全技术和对技术人员的培训、更新。首先，采用强大而创新的安全技术是确保电力调度自动化系统安全性的关键，包括入侵检测系统（IDS）、防火墙、安全信息和事件管理系统（SIEM）等技术工具的应用，这些工具可以帮助及时发现和阻止潜在的网络攻击。使用先进的加密算法和安全协议，保障数据在传输和存储过程中的机密性和完整性。技术因素还包括对系统漏洞和弱点的主动扫描，以及对可能的安全风险进行实时响应。技术人员需要具备对最新安全技术的深入理解，以及对系统的维护和监控的技术能力。培训计划应该定期更新，跟上不断演进的网络威胁和安全挑战。只有技术人员具备足够的专业知识和技能，才能更好地应对和解决电力调度自动化系统中的各种安全问题。网络安全领域的技术进步日新月异，因此采用先进的、更新的技术是确保系统安全性的必要手段，不断地关注并采纳最新的安全技术，是保持电力调度自动化系统充分抵御各类网络攻击的有效途径。

3.3 组织因素

组织因素在构建电力调度自动化网络安全体系中扮演着关键的角色，涉及到建立健全的组织安全文化和制定有效的安全政策和规程。组织需要树立安全意识，使员工在日常工作中时刻注重网络安全，包括定期的培训和意识提升活动，帮助员工了解潜在的网络威胁和安全最佳实践，通过强调每个员工在网络安全中的责任，组织能够在全员范围内形成共同的安全价值观。明确的安全政策可以为员工提供明确的行为指南，确保他们在使用电力调度自动化系统时遵循最佳的安全实践，包括对访问控制、身份认证、信息分类、数据备份等方面的规定，以保障系统的整体安全。安全团队可以跨足技术、管理和法律等多个领域，共同制定和执行综合性的网络安全策略。组织内各个层面的合作，有助于形成一个全面、协调的安全体系。

3.4 人员因素

人员因素在电力调度自动化网络安全体系的建设中是至关重要的一环，涵盖了与人员相关的培训、招聘、管理和意识提升等方面。拥有经验丰富且接受过专业培训的安全专家能够更好地理解和应对潜在的网络威胁，通过招聘、培训和持续教育，组织可以建立起一个强大的安全团队，负责监控、分析和应对各类安全事件。定期的安全培训能够使员工了解最新的安全威胁和防范措施，提高他们在使用电力调度自动化系统时的警觉性。建立一个积极的安全文化，使每个员工都认识到他们在网络安全中的重要角色，能够有效减少人为失误和不慎操作导致的安全风险。管理层应该为安全培训提供足够的资源和支持，确保员工能够得到必要的技能提升。此外，管理层的决策和战略规划对于确保电力系统安全性至关重要，需要制定明确的安全政策和规程，并建立监测和评估机制，以保证安全措施的有效实施。

4 电力调度自动化网络安全体系构建的路径

4.1 风险评估和需求分析

风险评估和需求分析是电力调度自动化网络安全体系构建的关键步骤，为系统设计和实施提供了基础和指导。首先，风险评估侧重于识别系统的关键资产和脆弱环节，以及可能面临的内部和外部威胁，通过系统性的风险识别，可以建立起对网络攻击、数据泄露、设备故障等潜在风险的全面认识，为后续的防范和应对提供了有力的基础，确保安全体系能够覆盖所有可能的威胁场景。需求分析则通过深入了解系统的功能、性能和使用场景，可以确保在构建安全体系时不会影响系统的正常运行[1]。此外，需求分析还包括对法规、标准和行业最佳实践的遵循，以保证系统在合规性方面的稳健性。在风险评估和需求分析的基础上，可以制定出相应的安全策略和措施，明确了系统所面临的风险和用户需求后，能够有针对性地选择和实施适当的安全措施，包括访问控制、加密技术、身份认证、监控系统等。这不仅有助于提高系统的整体安全性，还能够有效地降低潜在风险的影响。

4.2 建立安全政策和规程

建立安全政策和规程是电力调度自动化网络安全体系构建的重要步骤，为组织提供了明确的指导原则和操作规范，确保系统在日常运行中的安全性和稳定性。安全政策明确了对电力调度自动化系统安全的整体战略和目标，涵盖对关键信息资产的保护、员工的安全责任、安全培训的要求，以及对潜在威胁的应对措施，通过明确这些原则，安全政策为整个组织提供了一个共同的安全框架，确保所有成员在网络安全方面都达到一致的标准。安全规程详细说明员工在日常工作中应该如何履行安全责任，包括访问控制、密码策略、设备使用规定、网络通信安全等方面的规定，这些规程通过明确、具体的要求，帮助员工理解如何在实际操作中保障电力系统的安全性，同时有助于规范和标准化系统的安全操作。关键的安全政策和规程还应该

考虑到法规合规性的要求，确保系统的运行符合相关法规和标准，不仅有助于保护组织免受法律责任，同时也提升了系统运行的社会责任感。最后，为了确保安全政策和规程的有效实施，组织需要进行定期的审核和更新，由于安全威胁和技术环境不断变化，安全政策和规程也需要及时调整以适应新的挑战和要求。

4.3 人员培训和教育

人员培训和教育是电力调度自动化网络安全体系建设中不可或缺的一环，能提高组织成员的网络安全意识，培养专业技能，确保他们能够在实际操作中遵循最佳的安全实践，有效防范和应对潜在威胁。培训计划应该覆盖所有与电力调度自动化系统相关的人员，包括系统管理员、操作人员和技术支持人员。培训内容应该包括最新的网络安全威胁、漏洞和攻击手法，以及防范这些威胁的最佳实践，通过定期的培训，人员能够了解到安全策略的更新和变化，保持对网络安全领域的敏感性。培训计划应该强调实践操作和应急响应，通过模拟实际网络攻击和事故场景，培训人员在紧急情况下的正确反应和处理能力，有助于提高人员在面对真实威胁时的冷静应对和问题解决能力[2]。培训还应强调员工的安全责任和行为规范，员工需要明白他们在日常工作中如何保护关键信息资产，如何正确使用网络系统，以及如何报告发现的安全问题，通过强调每个员工在网络安全中的重要角色，能够降低因人为疏忽而引起的潜在风险。最后，通过测验、模拟演练和反馈机制，组织能够了解培训计划的有效性，及时调整培训内容和方式，适应不断变化的网络安全环境。

4.4 网络架构和设备安全措施

网络架构和设备安全措施是电力调度自动化网络安全体系建设的核心组成部分，通过科学设计网络架构和采取有效的设备安全措施，能够最大程度地降低网络攻击和威胁的风险。采用分层次和分隔区域的网络结构，可以有效隔离横向攻击路径，降低攻击者横向移动的能力，合理划分内部网络和外部网络，设置防火墙和入侵检测系统，加强对外部网络的监控和防护[3]。设备安全措施包括加强对关键设备的保护，确保在运行过程中不受到潜在威胁的侵害，采用最新的设备安全技术，包括硬件安全模块、固件签名、设备认证等，确保设备的完整性和正常运行。加强对设备的访问控制，限制只有授权人员能够访问关键设备，降低内部威胁的潜在风险。网络架构和设备安全措施还需要考虑到系统的可扩展性和灵活性，通过设计弹性的网络结构和采用可升级的设备安全技术，系统能够更好地适应不断变化的网络威胁和安全需求，随着技术的发展，不断升级和更新网络架构和设备安全措施是确保系统安全性的重要手段。最后，通过对系统进行全面的审查和评估，能够发现潜在的漏洞和弱点，及时采取措施加以修复和改进。

4.5 不断改进策略

持续改进策略是电力调度自动化网络安全体系建设的重要环节，以适应不断演变的威胁和技术环境。定期的风险评估和安全漏洞分析是持续改进策略的基石，通过定期检查系统的安全状况，组织能够发现新出现的威胁和漏洞，并及时调整安全策略以应对这些变化，这种持续的风险评估可以确保安全措施与实际威胁保持同步，不断提高系统的整体安全性。随着技术和威胁环境的变化，安全政策和规程需要不断更新以反映最新的安全标准和最佳实践。这包括对员工培训计划的调整、对系统配置的修订等方面的更新，以确保整个安全体系是切实可行的。与安全供应商和专业团队保持紧密的合作也是持续改进策略的一部分，通过与安全领域的专业人员合作，组织可以更好地了解新的威胁和解决方案，及时引入新的安全技术和工具，这种合作有助于加强组织对未知威胁的感知，并提供及时的响应。最后，通过定期的安全培训和内部宣传，可以提高员工对安全的敏感性，使其成为安全体系的积极参与者，员工的积极参与和合作是确保持续改进策略实施成功的重要保证。

5 结语

在电力调度自动化网络安全体系的建设中，我们全面考虑了系统概况、必要性、关键因素、路径和改进策略。通过风险评估、安全政策、人员培训、设备安全和持续改进，构建了多层次、全方位的安全框架。这个框架不仅强调技术措施，也注重组织文化和人员素养。持续改进策略使安全体系适应不断演变的威胁。未来，我们将不断完善体系，确保电力系统安全、稳定运行。

[参考文献]

[1]周烨华.电力调度自动化网络安全与实现技术[J].通信电源技术,2019,36(9):287-288.
[2]崔悦,刘紫玲,丁宝帅等.电力调度自动化网络安全与实现策略研究[J].山东工业技术,2018(18):148.
[3]丁晓成.电力调度自动化网络安全防护系统的研究与实现探讨[J].中国新通信,2019,21(13):132.

作者简介：王鸿彦（1996.10—），毕业院校：新疆工程学院，所学专业：电气工程及其自动化，当前就职单位：国网博尔塔拉供电公司,职务:变电二次检修工,职称级别:助理工程师。