调度自动化系统及数据网络安全防护

刘 刚
宇哲融创科技（北京）有限公司，北京 100000

[摘要]随着经济的持续发展，电网的稳定性和安全性成为社会各界关注的重点。在电网调度工作中，应用自动化流程至关重要，通过对调度自动化系统解析的数据进行整合，可以确保配备更加系统化的数据网络，从而为电网管理提供稳固的基础保障。在此基础上，完善的安全防护措施成为确保电力系统高效运行的关键。因此，文章简要分析了调度自动化系统及数据网络安全防护的重要性，重点阐述了具体的防护方案，并结合实际问题提出了相应的优化建议。
[关键词]调度自动化系统；数据网络；安全防护
DOI：10.33142/sca.v8i4.15937 中图分类号：TP3 文献标识码：A

Scheduling Automation System and Data Network Safety Protection

LIU Gang
Yuzhe Rongchuang Technology (Beijing) Co., Ltd., Beijing, 100000, China

Abstract: With the continuous development of the economy, the stability and safety of the power grid have become the focus of attention for all sectors of society. In the work of power grid dispatch, the application of automation processes is crucial. By integrating the data parsed by the dispatch automation system, a more systematic data network can be ensured, providing a solid foundation for power grid management. On this basis, comprehensive safety measures have become the key to ensuring the efficient operation of the power system. Therefore, the article briefly analyzes the importance of scheduling automation systems and data network security protection, focuses on specific protection schemes, and proposes corresponding optimization suggestions based on practical problems.
Keywords: scheduling automation system; data network; safety protection

引言

随着电力系统现代化和智能化的持续推进，调度自动化系统，作为电力调度的核心组件，已在电网运行管理、负荷调度、故障诊断及恢复等方面发挥着不可或缺的作用。依赖于数据网络，信息的快速传输与处理得以实现，从而确保电网能够在复杂环境下保持稳定运行。然而，随着信息技术的广泛应用，调度自动化系统面临的安全威胁日益严峻。黑客攻击、病毒入侵、数据泄露、系统故障等问题，已不再是少数事件，这些问题不仅威胁到电力系统的正常运作，甚至可能导致大范围的电力中断，进而给社会经济带来巨大的损失。因此，电力系统发展的关键任务之一，便是确保调度自动化系统及其数据网络的安全防护。在此背景下，制定有效的安全防护策略显得尤为重要。一个多层次、多维度的安全防护体系必须被构建，它不仅需要保障系统的物理安全、网络安全和数据安全，还应预防人为操作失误，以确保在突发事件发生时，系统能迅速恢复。尤其在智能电网快速发展的今天，调度自动化系统的安全性已直接影响着电力系统的稳定性与可靠性。针对当前面临的安全威胁与防护现状，本研究旨在提出应对措施和未来发展方向，提供理论依据和实践指导，为电力系统的安全管理和技术进步贡献力量。

1 调度自动化系统及数据网络安全防护的意义

调度自动化系统及其数据网络的安全防护，在现代电力系统中被认为至关重要。随着电力行业信息化与自动化水平的不断提高，已成为保障电网安全、稳定运行的核心技术之一的，正是调度自动化系统。该系统不仅涉及电网的实时监控和调度决策，还直接关系到整个电网的可靠性、经济性与安全性。然而，随着调度自动化系统的广泛应用以及数据网络日益复杂化，系统的安全性问题逐渐暴露出来，成为亟需解决的关键瓶颈。数据网络的安全防护，不仅需防范外部攻击，还必须保障内部数据传输的完整性与保密性。若发生安全事件，调度自动化系统及其数据网络，可能导致电网调度失误、设备误操作，甚至在极端情况下，引发大规模电力事故或系统瘫痪，这将严重影响社会经济及民众生活。因此，强化调度自动化系统及数据网络的安全防护，不仅有助于潜在安全隐患的预防，还能够提升电力系统应对网络攻击的能力，确保电网在复杂多变的环境下，依然能够保持稳定与安全运行。

2 电力系统中各类网络应用的特点

电力系统中的各类网络应用，展现出了多样性与复杂性，主要体现在实时性、可靠性、分布性与安全性等方面。在电力系统中，实时性要求尤为严格，特别是在调度自动化、故障检测与响应以及负荷调度等关键环节，必须达到毫秒级的响应速度，以确保电网的稳定运行及迅速恢复故障。与此同时，电力系统的网络应用，必须具备高度的可靠性。任何网络延迟、设备故障或数据丢失，都可能导致

电力中断、设备损坏，甚至引发大规模的系统崩溃。为了确保这一点，电力系统常采用冗余设计、备份通信链路及容错技术，以便在网络故障或设备损坏的情况下，能够迅速恢复并持续提供服务。电力系统的网络应用，具有显著的分布性，覆盖着广泛的地理区域，各个子系统之间，需要高效地协作与数据共享。这就要求网络必须支持大范围的分布式架构，如区域调度中心、变电站、配电网等，以确保不同层级系统之间能够无缝对接并做出快速响应。安全性，则是电力系统网络应用中的关键特征[1]。随着信息技术的不断发展，电力系统正逐步朝着智能化、自动化转型，伴随而来的是网络攻击、数据泄露及系统入侵等风险的不断增加。为了应对这些挑战，电力系统的网络应用不仅需要采用先进的网络安全技术，如加密、防火墙、入侵检测等，还必须建立严格的访问控制及审计机制，防范外部与内部的安全威胁，确保系统的数据完整性、机密性与可用性。

3 自动化系统二次安全防护的现状

3.1 自动化系统二次防护的简单结构

原有的电力自动化控制系统较为单一，业务模块较少且彼此独立运行，模块间和系统间的数据交换也相对较少，因此，二次防护系统结构较为简单。随着电力系统的不断发展和新技术的不断更新，供电企业为了更好地服务电网管理，已在电力调度自动化领域投入了大量的新技术应用，如 IES 调度自动化系统、调度一体化系统（EMS）、调度运行管理系统（OMS）以及仿真调度员培训系统等。这些新系统的引入，导致自动化系统的二次防护结构变得更加复杂。同时，随着庞大数据传输需求的增加以及各业务系统之间日益频繁的数据交换和共享，自动化系统对二次安全防护的要求也变得更加严格。

3.2 自动化系统二次防护措施达不到要求

目前，自动化系统在二次安全防护方面的措施，存在诸多不足，无法充分应对电力系统日益复杂的安全需求。尽管已经实施了一定的二次安全防护，许多自动化系统，但这些防护手段，往往未能有效应对日益复杂的安全威胁。例如，仍依赖传统的安全防护技术，一些系统，未能及时更新以适应新的网络攻击手段和技术进展，这就限制了防护能力。此外，部分自动化系统的二次防护措施，在配置上存在不合理之处，漏洞较多，防护层次也较为单一，无法实现对不同安全风险源的分级管理与防护。随着自动化系统功能的不断扩展，处理的数据量和复杂性也在不断增加，原有的防护手段，已无法高效应对潜在的安全风险，导致防护效果大打折扣。

3.3 自动化系统二次防护的落后管理

当前，自动化系统二次安全防护的管理，存在明显滞后，主要表现在管理理念、执行力度及技术更新等多个方面。一方面，仍沿用传统管理模式，许多电力企业，未能充分认识到自动化系统安全防护的重要性，这导致了安全管理体系的不完善。多数自动化系统的安全防护，停留在表面，缺乏深入的风险评估及持续的安全管理。另一方面，安全管理的执行力度较弱，部分企业未能定期进行安全检查与评估，防护措施，往往流于形式，且缺乏有效的监督与考核机制。这种管理上的松懈，导致了安全防护的漏洞，特别是在面对突发安全事件时，缺乏及时响应与有效处置的能力[2]。此外，随着自动化技术的快速发展，许多企业未能及时升级和优化现有的安全防护措施，管理滞后于技术需求，导致系统在应对现代复杂安全威胁时，显得力不从心。

4 加强继电保护的运行管理

4.1 运行管理的关键是坚持做到“三个管好”和“三个检查”

加强继电保护的运行管理，关键在于确保“三个管好”与“三个检查”到位。所谓“三个管好”，指的是设备、人员和流程的全面管理。设备管理要求，继电保护装置的高效运行必须得到保障，定期进行检查、校验与维护，隐患及时发现并消除，防止设备老化或故障影响系统的稳定性。尤其在高压及复杂环境下，设备的可靠性，是保证保护动作及时有效的基础。人员管理则强调，操作人员不仅应具备扎实的技术知识，还应熟练掌握各项操作规程与应急处理流程。通过定期培训与考核，提升人员的操作能力与应对突发情况的能力，确保在设备出现故障时，能够迅速、准确地执行保护动作。流程管理则着重于继电保护操作流程的标准化与规范化，确保每项操作严格按照规定的流程进行，防止因人为疏忽或流程不规范导致的失误。在此基础上，继电保护管理中的“三个检查”，起着至关重要的保障作用，分别为定期检查、专项检查与应急检查。定期检查，涉及对继电保护设备进行系统性的定期维护与性能检测，确保其在长时间运行中依然保持应有的保护功能，避免因设备老化或环境变化导致功能失效。专项检查，则集中于特定设备或环节，识别潜在的安全隐患并采取针对性的改进措施，尤其在新设备投入使用或系统发生重大变动时，专项检查尤为重要。应急检查，则是在继电保护系统出现故障或异常时，迅速对系统进行检查，找出故障源并进行修复或调整，确保电力系统尽快恢复正常运行。

4.2 加强运行方式的管理

加强继电保护的运行方式管理，是确保电力系统稳定与安全运行的关键环节。继电保护系统，不仅需要具备高效、精准的故障检测与处理能力，还应在系统设计、运行模式及实际操作中实现精确配合，以提升系统的可靠性与抗风险能力。运行方式管理的要求，是根据电网的运行状态与负荷变化，灵活调整继电保护的配置与参数。电网在不同运行模式下，如正常运行、故障状态或负荷波动时，采取的保护策略需有所不同。例如，电力系统正常运行时，

继电保护系统，需确保对常规故障的快速响应；而在大规模故障或紧急修复过程中，保护方式，应根据实际情况进行调整，避免误动或缺动，确保电网的稳定性。加强运行方式管理，还包括优化继电保护系统的联动机制[3]。继电保护的协调性，至关重要，任何环节的失误，都可能引发连锁反应，进而影响整个电网的安全。因此，在管理中，应注重加强各类保护设备间的协调，确保一旦某个设备发生故障，系统其他部分能够及时响应，并避免不必要的停运或大范围的保护动作。此外，运行方式管理，还需关注提升应急响应能力。在突发故障情况下，继电保护系统，必须能够迅速、准确地执行保护指令，减少对电网运行的干扰。为此，应定期开展演练与故障模拟，检验应急响应能力，确保在紧急事件中，保护系统能够高效、准确地进行故障处理。

5 调度自动化系统的安全防护

5.1 制定调度自动化系统安全防护策略的重要性

制定调度自动化系统的安全防护策略，是确保电力系统稳定、安全运行的关键。随着现代电力网络日益复杂、自动化水平不断提高，调度自动化系统，在调度控制、故障处理及负荷分配等方面，发挥着至关重要的作用。作为电网的“大脑”，调度自动化系统，负责实时数据采集、监控、分析以及决策执行。随着信息技术与智能设备的广泛应用，这些系统的复杂性与重要性，使其成为潜在的安全攻击目标。网络攻击、恶意软件、系统故障、管理疏漏等问题，都可能威胁到系统的正常运行，进而引发电力调度错误、保护失效、数据泄露等严重后果。为了应对这些威胁，制定全面且有效的安全防护策略，显得尤为紧迫。该策略，应从多层面、多角度构建起坚固的防线，利用网络安全技术、数据加密、身份认证等手段，防止外部非法入侵及病毒攻击等威胁。同时，内部安全管理与风险管控，应得到强化，确保操作人员权限控制与责任追踪到位，避免人为错误或管理漏洞导致的安全隐患。随着电力系统的不断智能化，调度自动化系统，将面临越来越复杂的安全挑战。因此，安全防护策略，不仅需要应对当前的风险，还必须具备前瞻性，能够快速适应新兴技术与安全威胁的变化，确保电网在任何复杂情况下，都能迅速响应并恢复正常运行。

5.2 信息系统的安全分层理论

信息系统的安全分层理论，强调将安全防护措施按照不同层级进行分隔，以便针对性地应对各类安全风险。在调度自动化系统中，采用这一理论，尤为重要，因为该系统涉及大量实时数据交换及复杂控制指令，其安全性，直接影响到电网的稳定性与安全性。依据安全分层理论，信息系统的防护，应覆盖物理层、网络层、应用层及数据层，逐级实施保护措施，以确保系统在不同安全威胁下，能够持续稳定运行[4]。物理层的安全保护，关注硬件设施与设备的物理防护，旨在避免恶意攻击或自然灾害对系统硬件造成损害。网络层，作为信息系统的基础，保障数据传输的安全性，利用防火墙、入侵检测系统、虚拟专用网（VPN）等技术手段，有效防止外部非法访问与数据篡改。应用层安全，则侧重于操作系统与软件平台的防护，通过访问控制、漏洞修补及身份认证等措施，确保系统内部程序不受到恶意软件的侵扰。数据层的保护，关系到所有信息的机密性、完整性与可用性，采用数据加密、备份、访问控制与审计等技术手段，确保关键数据在存储与传输过程中，不被泄露、篡改或丢失。通过这种分层次的安全防护策略，不仅能够降低单一层级被突破后，对系统整体安全的影响，还能确保各层级的保护措施，相互补充、独立运行，从而提供全方位的安全保障。

6 结语

调度自动化系统及其数据网络的安全防护，对保障电力系统的稳定与安全运行，至关重要。随着电力行业不断迈向智能化和自动化，系统所面临的安全威胁和挑战，也在不断增加。因此，愈加迫切地实施全面且有效的安全防护措施，变得更加必要。通过强化技术手段与管理措施，增强网络的防护能力，可以显著减少安全风险，从而确保电力系统在复杂多变的环境下，依然能够保持高效稳定的运行。展望未来，随着技术的不断进步及电网规模的扩大，调度自动化系统的安全防护工作，需要持续优化，以应对不断涌现的安全威胁，确保电力系统的长期稳定性与可靠性。

[参考文献]

[1]高小芊.调度自动化系统及数据网络的安全防护技术研究[J].通讯世界,2024,31(11):25-27.
[2]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.
[3]罗兴国.调度自动化系统及数据网络的安全防护[J].通信电源技术,2018,35(10):283-284.
作者简介：刘刚（1977.2—），男，汉族，学历：大专，专业：信息安全与管理。