电网调度自动化系统网络安全研究

罗石江，疏中凡，陶长浩
（国网安徽省电力公司霍邱县供电公司，安徽 霍邱 237400）

摘　要　电网作为国家关键基础设施，其稳定、安全、可靠的运行对于社会经济的持续发展至关重要。在当今这个信息技术迅猛发展的时代，电网调度自动化系统已经成为确保电网运行效率与安全的关键技术支撑。它通过集成先进的信息技术、通信技术和自动化控制技术，实现了电网的实时监控、故障诊断、优化控制和决策支持等一系列功能。然而，电网调度自动化系统的开放性和联网性也使其容易受到各类网络安全威胁，包括恶意软件攻击、数据篡改、服务拒绝等。本文就电网调度自动化系统网络安全展开探讨，以期为相关人员提供参考。

关键词　电网调度；自动化系统；网络安全
中图分类号：TM76　　**文献标识码**：A　　**文章编号**：2097-3365(2024)04-0019-03

电网调度自动化系统是确保电力系统安全、稳定和经济运行的关键。系统的高度自动化和智能化提高了电网的管理效率，优化了资源分配，但同时也带来了严峻的网络安全挑战。随着数字化程度的不断提高，电网调度自动化系统越来越依赖于复杂的信息通信技术，使其面临着来自网络攻击的风险。因此，电网调度自动化系统的网络安全已经成为电力行业和信息安全领域共同关注的焦点。通过这一系列的研究，旨在为电网调度自动化系统提供一个更加安全、可靠的网络环境，以支持电力系统的可持续发展。

1 电网调度自动化系统功能

1.1 数据信息方面的功能

数据采集与处理是电网调度自动化系统的基础功能。系统通过安装在各个重要节点的传感器和计量设备，实时收集电网的运行数据，如电压、电流、频率、温度等参数。这些数据经过模拟/数字转换后，通过通信网络传输到控制中心，进行数据的汇总、处理和分析。此外，电网调度自动化系统还具备数据信息的存储与管理功能。系统会将历史数据存储在数据库中，以便于日后的查询、分析和决策支持。这些数据对于电网的故障诊断、性能评估、运行优化以及未来规划等都具有重要意义。

1.2 系统运行方面的功能

系统运行管理是电网调度自动化系统的核心功能。它通过集成化的软件平台，对电网的运行状态进行实时监控，确保电网的安全稳定。一旦监测到异常情况，系统会立即启动应急预案，通过自动控制或向调度员发出报警，以迅速处理故障，保障供电的连续性和可靠性。电网调度自动化系统还具备优化调度的功能。系统可以根据实时数据和预测数据，运用优化算法，制定最优的发电和输电计划，提高电力系统的经济性和效率。

1.3 通信介质与网络体系方面的功能

电网调度自动化系统依赖于强大的通信网络体系，包括有线通信和无线通信两大部分。有线通信保证了数据传输的稳定性和可靠性，而无线通信则提供了更大的灵活性和覆盖范围。这些通信网络不仅需要高速、高效，还需要具备足够的安全防护措施，以防止数据被截获或篡改。

2 电网调度自动化系统网络安全问题

2.1 网络病毒的入侵

在电网调度自动化系统中，网络病毒的入侵一直是网络安全领域面临的重大威胁。当网络病毒成功入侵系统时，它们能迅速复制并传播到系统的其他部分，甚至能跨越网络，影响到更广泛的基础设施。由于电网系统具有高度的复杂性和互联性，一旦受到攻击，后果往往非常严重，可能导致数据损坏、设备故障甚至整个系统瘫痪。目前，各类新型网络病毒不断涌现，随着黑客攻击手法的日趋精细和隐蔽，传统的病毒防护手段难以完全拦截这些日益智能化的威胁。

2.2 路由器安全的威胁

路由器作为电网调度自动化系统网络通信的关键节点，其安全性直接关系到整个电网的运行安全。当前，随着网络技术的迅猛发展，路由器面对的安全威胁日益增多。由于某些路由器的固件更新不及时或存在漏洞，黑客可以利用这些漏洞对路由器进行入侵。一旦

控制了路由器，攻击者可以进行流量劫持、网络监控、恶意广告推送等多种攻击行为。更为严重的是，通过对路由器的控制，攻击者甚至能够远程控制整个电网系统，对国家的电力供应安全构成极大的威胁。

2.3 网络结构水平差异大

当前，电网调度自动化系统中存在各种网络结构的水平差异，这在一定程度上增加了网络安全管理的难度。一些电网系统运行在老旧的设备和软件之上，其安全性能往往不足以抵御现代网络攻击手段。同时，由于更新换代成本和技术兼容性的问题，导致不同地区、不同层级的电网系统网络结构水平参差不齐，这种硬件和软件上的差异为网络安全带来隐患，使得网络病毒更容易通过薄弱环节渗透和攻击[1]。

2.4 早期预防手段不到位

面对电网调度自动化系统的网络安全隐患，早期预防手段的不到位是一个不容忽视的问题。很多电网企业在网络安全防护体系上的投入不足，缺乏有效的预警和应急响应机制。此外，对网络攻击的认知不足、风险评估不全面，导致防范措施落后于网络攻击手法的更新换代。因而，当面临复杂多变的网络安全威胁时，电网调度自动化系统常常显得手足无措，难以有效地预防和遏制安全事故的发生。

3 电网调度自动化系统网络安全性提升有效措施

3.1 明确网络安全防护需求与方向

首先，要明确网络安全防护的需求与方向。网络安全防护是对于电网调度自动化系统至关重要的一环。在当前，随着黑客攻击技术的日益发展，电网系统也需要不断升级其安全保护技术，以保证其日常运作的稳定。明确需求和方向，有助于指导当前防护工作的开展，并指明防护技术的发展之路。

其次，深化反病毒防御体系的构建是全面提升电网调度自动化系统网络安全性的重要一环。工作人员需要持续加大投入，配备更先进的防病毒技术，提高病毒防御潜能。同时，也要强化病毒防护方案的实施，例如定期对系统进行病毒扫描，对出现的病毒及时进行隔离和处理，防止病毒进一步传播和给系统造成更大损失[2]。在防御体系的布局上，需要落实多层次的防御机制，防止单一环节的破裂使得整体防线崩溃。提升网络入侵侦测的能力，可以及时捕捉到可能对系统构成威胁的网络行为或疑似侵入情况，从而实行快速应对，防止损失的进一步扩大。同时，强化防火墙保护体系能对电网调度自动化系统提供更安全的网络环境，有效抵御各种网络攻击。

最后，加大防范系统反应检测力度，提高应对能力。“早知道、早预防、早应对”应成为防范系统的常态。一旦发生问题，能迅速进行检测与反应，可以最大程度地降低损失。因此，需要升级并优化检测手段，提高系统对异样行为响应的速度，有效减缓或者阻止问题的扩大化。

3.2 加大网络病毒防范革新力度

首先，强化防范意识是防止网络病毒攻击的第一道防线。我们要认识到电网调度系统拥有海量的数据，如果被黑客攻击后果将不堪设想，因此要保持一种时刻处于警惕的状态。我们需要对网络安全有深度的了解和熟悉，这样才能准确检测和抵制攻击，防止网络病毒对系统造成损害。

其次，合理的防病毒策略同样不可或缺。防病毒策略可以围绕着防火墙、杀毒软件、网络行为管理、网络入侵检测等方向进行。防火墙应严禁任何无授权的登录和查看数据，对数据进行有效的防护[3]。杀毒软件应经常更新，以便识别和清除最新的网络病毒。网络行为管理则可以防止内部工作人员因误操作或恶意破坏而引起的安全问题。网络入侵检测系统能够自动检测出网络异常，及时防止可能的网络袭击。

再者，我们必须将防火墙、杀毒软件等工具融为一体。通过统一的管理和控制，我们可以更有效地对抗网络病毒。例如，我们可以设置防火墙以阻止不必要的网络连接，同时使用杀毒软件对经防火墙的连接进行进一步的检查处理，这样可以大大减少网络病毒的侵入机会。

最后，我们必须持续关注和分析局域网的信息传输情况，频繁性波动可能是网络病毒的一个指标。在检测到问题后，我们需要及时处理，并根据处理结果来调整我们的防病毒策略，使之更加精准有效。

3.3 科学制定备份与灾难恢复计划

电网调度自动化系统应该设定自动备份功能，以每日为单位进行数据的备份和录入，确保数据的完整性。自动备份可以避免人为疏忽导致的备份漏洞，每日备份也可以避免数据丢失的风险。各类数据将会按时间顺序整理和归档，为电网的运行提供了一份详尽的历史记录。云端存储的特性分布式的，便于访问，不仅可以增大数据的存储容量，也为数据的迅速恢复和迁移提供了便利[4]。云端存储系统的冗余设计使得即使一部分的存储设备故障，也不会对数据的完整性

产生影响。并且通过调配资源的方式，可以在设备故障的情况下保证存储、查询等功能的正常运行。此外，电网调度自动化系统的数据备份工作同时也要考虑到数据安全问题，包括防病毒、防黑客、防内部人员的恶意行为等。因此，在实际操作中，应有专门的数据管理人员，制定严格的数据管理和安全制度，确保数据的安全存储。

在当今信息化社会，网络安全和数据存储问题日益凸显，尤其对于电网调度自动化系统这样的大型系统，如何有效防护网络安全，如何备份数据，确保正常运转，已经成为每一个企业应该面对的问题。企业应提前设置备用服务器，这就像为重要文件做备份一样，重要的硬件设备也应该提供备用选项，以事先预防不可抗力的因素带来的影响。当硬件设备出现故障或者无法运行的时候，备用工作站可以及时启动，将停工时间缩短到最短，使得企业的运营成本降低。硬件设备与备用服务器之间应该提供自动切换功能，实现无缝衔接，这样可以保证在硬件设备无法运行的时候，备用服务器可以迅速接管工作，防止出现长时间的停机现象[5]。在增强网络安全防护可靠性的基础上，还需要对安全管理规定进行完善。网络安全首先应当从制度上得到保障，需要完全了解网络安全政策，并定期进行评估、修订。同时，网络安全管理规定也应该包含对各种网络攻击的预防和应对措施。电网调度自动化系统还需要实施有效的病毒防护措施，包括使用权威的安全软件，进行定时查杀病毒和恶意程序，以及在大型网络操作或者系统更新之前进行备份，防止因病毒感染或者操作失误导致的数据丢失。而在网络安全以及数据存储方面，应当考虑系统的整体性和一体化。这就要求我们既要考虑网络、服务器等硬件设施的安全，也要关注信息内容、用户操作等软性问题。网络和数据安全不仅仅是技术问题，也是管理问题。因此，电网调度自动化系统应该从数据采集、存储、处理、分析等全过程进行管理，保障数据的完整性、可用性和保密性。

3.4 加大反病毒与软件安全性监测力度

随着网络技术的迅速发展，病毒和恶意软件也在不断演变，黑客攻击手段日趋多样和隐蔽，仅仅依靠传统的反病毒软件已经难以应对日益严峻的网络安全环境。因此，电网调度自动化系统需要采用更为先进的反病毒监测技术，比如行为分析、异常检测等，以识别并阻止未知病毒和零日攻击。此外，还要攻坚克难，实现病毒库的快速更新，以适应新型病毒的防御需要。随着电网自动化水平的提高，不断有新软件被开发并应用于不同的环节，保障其安全性显得尤为重要。软件安全性监测不仅涉及软件编码的安全性，也涉及整个软件运行环境的安全性。从最初的代码编写到后期的维护更新，软件的每一个环节都需要经过严格的安全性检测[6]。此外，面对并应对软件安全问题，我们不仅要注重对外部威胁的防御，也要加强内部安全管理。加强员工的安全意识教育，定期对员工进行网络安全知识的培训，防止因操作失误导致的安全事故。同时，建立健全的内部安全审计和监控机制，对系统操作进行实时监控，保障系统的内在安全。为了实现软件的最高安全性，需要在软件设计之初就将安全性作为一项基本需求加以考虑，应用安全编程规范和安全框架。采取加密技术构建安全的数据传输和存储机制，保障数据的机密性与完整性，避免数据泄露和非法篡改。当前，随着云计算、大数据、物联网等新兴技术的发展应用，电网调度自动化系统面临的安全挑战也在不断增加。因此，除了加强反病毒与软件安全性检测外，还应积极探索人工智能、机器学习在电网调度自动化系统安全防护中的应用，借助先进技术提高系统的安全防御能力。

4 结语

电网调度自动化系统通过其强大的数据信息功能和系统运行功能，保障了电力系统的高效和可靠运行。系统的通信网络体系则为这些功能的实现提供了坚实的支撑。随着技术的不断进步，电网调度自动化系统将会更加智能化、网络化，为电力系统的现代化和可持续发展提供强有力的技术支持。

参考文献：

[1] 李远,闫磊,徐利美,等.电网调度自动化系统网络安全研究[J].信息技术,2021(11):150-155.
[2] 王甜.电网调度自动化系统的安全策略[J].集成电路应用,2020,37(11):136-137.
[3] 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.
[4] 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,2020,04(02):43-44.
[5] 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.
[6] 张振夫.电力网络及调度自动化系统的安全防护策略研究[J].中小企业管理与科技(下旬刊),2019(11):88-89.