

变电站自动化系统中调度数据网络设备的性能优化与安全防护研究

李康

国网肥东供电公司

摘要: 随着电力系统的不断发展、进步和变革,变电站自动化系统在电力调度中的作用日益凸显。为提高调度效率、确保电力系统的安全稳定运行,调度数据网络设备的性能优化与安全防护显得尤为重要。本文深入研究了变电站自动化系统中调度数据网络设备的性能优化与安全防护问题,提出了相关建议,以期对电力调度领域的相关工作提供有益参考。

关键词: 变电站自动化系统; 调度数据网络; 性能优化

【DOI】10.12252/j.issn.2096-627X.2023.07.088

引言

随着信息技术的飞速发展和电力系统的智能化进程不断演进,变电站自动化系统在电力调度和运行中扮演着重要的角色。调度数据网络设备作为自动化系统的核心组成部分,其性能稳定与安全直接关系到整个电力系统的运行效果。面对电力系统日益增长的复杂性和网络威胁的不断升级,调度数据网络设备的性能优化和安全防护成为电力调度领域亟须解决的重要问题。

一、调度数据网络设备性能优化

1. 网络拓扑结构优化

网络拓扑结构作为调度数据网络的基础架构,直接影响到整个电力系统的可靠性。因此,深入优化网络拓扑结构是提升调度数据网络设备性能的首要任务。电力系统的特殊性要求其调度数据网络具备高度稳定性。首先,在网络拓扑结构的设计中,应充分考虑电力系统的层次结构,典型的电力系统拓扑通常包含发电厂、变电站、配电站等多个层次,其间存在大量的数据交互需求。为此,采用星型、环型或树型拓扑结构,可根据电力系统的层次关系,合理划分网络区域,降低数据传输的距离和延迟,有效提高网络实时性。其次,在网络拓扑结构优化中,需充分考虑容错性,电力系统对网络的稳定性要求极高,一旦网络发生故障,可能导致整个电力系统的运行异常。因此,采用冗余设计、环路检测和快速切换等技术手段,以确保在网络部分故障时,系统能够迅速切换到备用路径,保障调度数据的连续传输,采用高可用性的网络设备和通信协议,提高网络的可靠性。

2. 数据传输效率优化

数据传输效率的提高直接关系到电力系统的响应速度,因此在调度数据网络的优化中,针对数据传输效率的优化显得尤为重要。首先,为了提高数据传输效率,

可以从网络协议和数据压缩算法的优化入手,选择高效的通信协议,如基于UDP的协议,能够减小通信开销,提高数据传输速率。同时,采用先进的数据压缩算法,将数据进行有效压缩,减小传输数据量,降低网络带宽的占用,这些技术手段能够在保证数据完整性的同时,显著提升数据传输的效率^[1]。其次,考虑到电力系统中大量的实时数据传输需求,采用多通道传输和并行传输技术,能够有效提高数据传输效率。通过同时利用多条通道进行数据传输,可以充分发挥网络资源的潜力,实现数据的同时传输,降低传输时间,并行传输技术则通过将数据划分为多个部分并同时传输,加速数据的传输速度,提高整体传输效率,尤其在大数据量的情况下表现尤为明显。另外,针对电力系统调度数据的特点,引入数据预取和缓存技术也是优化数据传输效率的有效途径,通过分析调度数据的访问模式,预先获取可能需要的数据并缓存在本地,可以有效减少对远程数据库的访问次数,提高数据获取的速度。合理设置缓存策略,对常用的数据进行缓存,减少重复传输,进一步降低网络负载,优化数据传输效率。最后,在数据传输效率的优化中,对网络带宽进行合理管理,通过动态调整带宽分配策略,根据实际数据传输需求进行带宽优先级的调整,确保关键数据的优先传输,从而保障电力系统的实时性。

二、调度数据网络设备安全防护

1. 分析网络安全威胁

有效应对日益多变的网络威胁,必须进行深入的网络安全威胁分析,以识别潜在的漏洞,为制定有针对性的安全防护策略提供基础。首先,要关注电力系统所面临的各类网络安全威胁。其中,最为常见的威胁包括恶意软件攻击、入侵行为、数据泄漏等,恶意软件攻击可能通过网络渗透系统,传播病毒、木马等恶意代码,导

致系统瘫痪或数据损坏。入侵行为可能通过未经授权的方式访问系统，获取敏感信息或篡改系统配置。数据泄漏可能导致敏感信息泄漏，危及电力系统的运行和用户隐私，通过全面的威胁分析，可以更好地了解这些潜在威胁的特点和来源，为制定有效的防御措施提供指导。其次，要考虑网络威胁的演化趋势，网络安全威胁是一个不断演进的过程，黑客通过不断创新和改进攻击手法，使得威胁形势更加严峻。因此，需要关注最新的网络安全威胁动态，及时调整防御策略，定期进行安全漏洞扫描，能够有效发现潜在的威胁，为系统的安全性提供及时保障。另外，网络安全威胁分析应该充分考虑电力系统的特殊性，电力系统对实时性的要求较高，因此，针对网络威胁的分析应更加注重对实时性的影响。例如，拒绝服务攻击可能导致系统无法正常响应，对电力系统的实时性产生严重影响。因此，在威胁分析中要特别关注可能导致实时性受损的攻击手法，以确保系统的高可用性。最后，网络安全威胁分析还应结合调度数据网络设备的具体架构和通信协议，不同的设备和协议可能存在不同的漏洞，因此需要深入了解和评估调度数据网络设备的安全性。通过全面而系统的网络安全威胁分析，可以为后续的安全防护工作提供有力的基础，确保调度数据网络设备在面对潜在威胁时能够做出迅速而有效的响应，保障电力系统的安全运行。

2. 建立安全防护机制

在变电站自动化系统中，为应对不断演进的网络威胁，需要建立健全的安全防护机制，这一机制不仅需要涵盖多层次、全方位的保护措施，还应具备强大的恢复能力，以确保电力系统免受潜在威胁的侵害。首先，建立物理层面的安全防护措施是安全防护机制的基础，包括对网络设备所在位置的访问控制、摄像监控、安全门禁等手段，以防止未经授权的人员物理接触网络设备，降低潜在物理层面的威胁。在设备的选址和布局上，还需考虑将关键设备放置在相对隔离、受控制的区域，最大限度地减小物理攻击的可能性。其次，建立网络层面的安全防护措施是确保调度数据网络设备免受网络攻击的重要手段，包括防火墙、入侵检测与防范系统、虚拟专用网络等技术的应用，防火墙通过监测和控制网络流量，阻止未经授权的访问和恶意攻击；入侵检测与防范系统通过实时监控网络流量和系统日志，发现并应对异常行为；虚拟专用网络通过加密通信，保障数据在网络传输中的安全性，这些措施共同构建起强大的网络安全屏障，有效抵御网络攻击的风险。同时，采用数据加密技术，对敏感数据进行加密处理，防止在数据传输和存

储过程中的信息泄漏，实施严格的访问控制策略，确保只有经过授权的用户才能访问和修改关键数据，定期进行数据备份，以防止数据丢失或遭受勒索攻击，通过建立数据的完整性验证机制，及时发现并阻止对数据进行的非法篡改行为。此外，加强对工作人员的网络安全培训，提高他们对潜在威胁的识别和应对能力，建立合理的用户权限管理机制，根据工作职责分配不同的权限，防止内部人员滥用权限导致的安全问题，对员工进行定期的安全意识培训，使其对安全政策和程序有清晰的认识，增强安全责任感。最后，在建立安全防护机制时，需要制定明确的安全策略，安全策略应明确网络安全的基本原则、安全标准和规范，为全员提供明确的行为指南，明确责任人和沟通流程，以保障在面对紧急情况时能够迅速、有序地做出反应。

三、综合应对策略

1. 硬件设备的选型与升级

硬件设备的选型与升级是确保调度数据网络设备性能、安全性的重要环节，硬件设备的性能直接关系到整个电力系统的可靠性，因此，科学合理地选择和不断升级硬件设备，对提升系统性能、应对未来挑战非常关键。首先，在硬件设备的选型中，需要考虑设备的性能参数、适用场景，在电力系统中，调度数据网络设备需要处理大量的实时数据，因此，选用高性能的交换机、路由器和服务器是必要的，通过升级设备的处理能力、存储容量、传输速度等关键指标，确保设备能够满足电力系统复杂调度任务的需求^[2]。同时，要结合电力系统的特殊性，选择稳定性的硬件设备，确保设备在长时间运行中不发生故障。其次，随着科技的不断发展，硬件设备的升级也是综合应对策略中的重要环节，及时升级硬件设备，利用新一代的处理器、存储技术和通信协议，能够显著提升设备的性能水平。升级过程中，需要确保新设备与原有系统的兼容性，避免因升级导致的系统不稳定，升级还应考虑设备的可维护性，选择支持远程管理的硬件，有利于及时发现和解决潜在问题。在硬件设备的选型和升级中，还需要关注能源效率，为了降低电力系统的运行成本和对环境的影响，选择能效较高的硬件设备是重要的。设备的能源消耗、散热效果以及环保认证等方面都应该成为选型和升级的考虑因素，采用先进的节能技术和智能管理手段，使硬件设备在满足性能需求的同时，尽可能地减少能源浪费。此外，硬件设备的选型与升级还需要考虑未来的发展方向，随着电力系统的不断演进，新技术的引入和电力调度需求的变化，硬件设备应具备较强的可扩展性，选用支持软件

定义网络（SDN）、物联网（IoT）等新兴技术的硬件设备，能够为系统未来的升级提供更大的灵活性。

2. 软件系统的优化与更新

软件系统的性能直接关系到电力系统调度数据的可靠传输。因此，通过不断优化和更新软件系统，可以提升系统的响应速度、降低潜在风险，并适应不断演变的电力调度需求。首先，软件系统的优化涉及对操作系统、数据库管理系统以及调度应用软件的升级，保持操作系统的最新版本，及时应用安全补丁，以确保系统能够充分利用新的功能；对数据库管理系统的优化包括索引优化、查询性能提升等，以加快数据的检索和存储过程；对调度应用软件进行性能分析，优化代码逻辑，改进算法，以提高整个调度系统的效率^[3]。其次，软件系统的更新要考虑对安全性的加固，及时安装和更新防病毒软件等安全工具，加强对系统的实时监测，及早发现潜在威胁；对软件系统进行漏洞扫描，及时修复发现的漏洞，防范潜在的网络攻击；引入先进的访问控制机制，确保只有授权用户能够访问系统，提升系统的整体安全性。另外，软件系统的优化与更新还需要关注用户体验，通过更新用户界面、提升交互性，使系统更加直观友好，有助于调度员更快更准确地完成任务；优化系统的日志和报警机制，使其更加清晰明了，有助于用户及时了解系统状态；优化系统的响应速度，减少用户等待时间，提高整个调度过程的效率。软件系统的更新还应考虑未来的发展方向，引入支持云计算、大数据和人工智能等新兴技术的软件，以应对未来电力系统的发展趋势。此外，设计系统为模块化结构，方便未来的功能扩展和升级，使其更易于适应不断变化的电力调度需求，提升系统的可维护性。在软件系统的优化与更新中，还要注意确保新软件版本与原有硬件和设备的兼容性，避免因更新而引发系统中断，建立完善的测试和验证流程，确保更新软件版本的过程是平滑可控的。

3. 多层次备份与灾难恢复

在综合应对策略的框架下，多层次备份与灾难恢复机制是保障调度数据网络设备高可靠性的重要组成部分，这一策略不仅着眼于防范数据丢失的风险，还专注于降低系统因各类灾难性事件而导致的服务中断时间，确保电力系统调度在面对意外情况时能够快速、有序地恢复正常运行。首先，多层次备份策略是数据可靠性的基石，采用实时备份、定期备份和异地备份的组合方式，确保数据得到多次的备份，从而在发生数据损坏或灾难性事件时能够迅速还原。实时备份可以保证对关键

数据的连续保护，定期备份则是对系统整体状态的快照；异地备份则提供了额外的安全层，防范了本地灾难对数据的影响，通过这种多层次备份机制，电力系统可以更好地保护数据的完整性。其次，灾难恢复机制是保障系统稳定性的关键手段，建立详细的灾难恢复计划，明确不同灾难场景下的应急处理流程。根据不同设备的重要性，制定优先级和时间窗口，确保在最短时间内实现关键设备和服务的恢复；进行定期的灾难演练，验证恢复计划的可行性，及时修正和完善计划，保证在实际发生灾难时能够迅速、有效地执行。另外，应该充分利用虚拟化和云计算等新兴技术，提高灾难恢复的弹性和效率，通过虚拟化技术，可以在较短时间内完成系统的备份和还原，减小恢复时间；借助云计算服务，可以将备份数据存储在远程云端，实现异地备份，降低本地灾难对数据的影响。同时，云服务提供了更强大的计算和存储能力，有助于迅速搭建替代性的调度服务，提高系统的容错性。此外，多层次备份与灾难恢复机制还需要结合系统的实际需求和资源情况，进行量化评估；根据不同数据的重要性、业务的敏感性和系统的关键性，确定不同数据和服务的备份频率和恢复目标，并在资源有限的情况下，根据业务优先级，制定合理的备份和恢复策略，确保最大限度地维护系统的可用性。

四、结论

综上所述，本文对变电站自动化系统中调度数据网络设备的性能优化与安全防护进行了深入研究。通过优化网络拓扑结构、提升数据传输效率，可以有效提高调度系统的性能。在安全防护方面，建立多层次的安全防护机制，加强人员培训和意识提升，制定应急预案和恢复机制，有助于提高系统的安全性。在今后的工作中，需要进一步关注新兴技术的应用，以更好地应对日益复杂的网络环境和安全威胁。通过不断的技术创新，将调度数据网络设备的性能和安全性推向新的高度，为电力调度系统的稳定运行提供更为可靠的支持。

参考文献

- [1] 陈娟. 基于智能变电站电力调度自动化系统安全防护系统研究[J]. 电子乐园, 2022(10): 0142-0144.
- [2] 周飞飞, 何迎利, 赵华, 等. 基于时间敏感网络的流量调度机制在智能变电站中的研究与实现[J]. 电力系统保护与控制, 2021, 49(19): 8.
- [3] 罗华峰, 许艾, 陆承宇, 等. 基于MMS替代协议的变电站安全通信技术研究及应用[J]. 电力自动化设备, 2021, 41(12): 6.