

网络技术在电力信息通信中的应用分析

刘嫫霖

镇江三新供电服务有限公司丹阳分公司

摘要: 电网系统的基本特性在于高度的复杂性和独特性。在电力的传输过程中,信息的交换与处理是关键,这确保了系统能够将电力相关信息准确无误地传递至监管机构。但是,由于大量的数据,往往会造成电力网络的崩溃,对用电质量产生影响。通过对电力信息与电力通信技术的结合,能够提升电力业务的处理速度和处理质量,减少电网系统出现故障的概率,有效控制投资成本,推动企业的发展。

关键词: 网络技术; 电力; 信息通信

【DOI】 10.12252/j.issn.2096-6261.2023.12.091

引言

电力信息通信是电力系统的重要组成部分,负责实时监控、控制、保护和调度电力系统。随着电力系统规模的不断扩大和电力需求的不断增长,电力信息通信的安全性和可靠性日益重要。网络技术在电力信息通信中的应用可以有效提高通信速度、扩大通信范围、降低通信成本,并提高通信系统的抗干扰能力。

一、电力信息通信技术

技术智能化有助于减轻人工负担,增强操作的稳定性。(1) 针对智能电网领域。智能电网具有交互性、自动化、信息化的特点,在国家电网建设过程中是关键性的技术提升,为后续的电力通信、电力营销、电力保护与调度等工作提供了更好的技术平台,获得了更为精确的发展趋势。“智能电网”以先进的传感器和探测技术为关键性的理论和技术手段,加之多元化的调节工作控制技术,提升了电力系统运行的安全性、可靠性、经济性和稳定性。(2) 电力信息通信技术。在智能电网的建设背景下,电力信息通信技术用于构建一个高速、集成、稳定的双向控制网络,在电力信息通信技术、电力自动化技术的发展等多方面有着非常关键的作用和效果。在控制工作中,电力信息通信技术对运行过程中的多种数据信息进行全方位的分析和处理的工作,将其转化为图像、声音、视频等形式,便于工作人员对于这些信息的处理和分析,从而实现信息的高效交换和提升。电力通信技术大大提升了系统的工作效率,并且目前的智能化技术正在朝着多元化和一体化的方向不断发展与提升,大大降低了系统中技术操作的难度,精确度也不断提升,工作效率得到了有效的保证,这也是衡量系统自动化控制水平的标准。智能化技术综合了多个处理器的应用,结合高速的CPU与RISC的运用,运算精度不断提升^[1]。

二、电力信息通信系统面临的安全问题

1. 电力信息通信网络模型隐患

构建在数字链路之上的电力信息通信网络,通过实体互联架构实现,涵盖了传输系统、寻址设备以及多路复用设备。该网络的安全性模型分为两个主要部分:媒介网络和支撑网络。媒介网络由网络层、传输层和物理层组成,分别负责寻址、数据交换和信号多路传输。支撑网包括同步网路(synchronized network)、信令网路(signaling network)以及管理网路。电信网络的安全技术服务,提供了对每一层模式的全面的支持,并提供了身份认证,访问控制,数据完整性检查等功能;数据保密性、反否认性等基本功能,保证了通讯的安全性。然而,现有的业务并不能完全覆盖整个电网,电网信息通信系统也会受到各种类型的攻击,从而导致不同的结果。针对可控性攻击可能导致网络资源骚扰和电信诈骗等问题,针对机密性攻击可能导致信息泄漏和篡改,针对可用性攻击可能导致网络瘫痪或破坏。

2. 物理破坏风险

对电力信息通信系统而言,物理损害是关键的安全威胁之一。这种损害涉及攻击者有意破坏系统的硬件设施,目的是造成系统故障或数据泄漏。首先,物理破坏可以通过破坏硬件设备、通信线路等完成。攻击者可以通过暴力入侵、盗窃、利用电磁干扰等方式对通信系统硬件设备进行破坏,如通过破坏交换机、网关、集线器、路由器等设备来实现对通信系统的攻击。攻击者还可以对通信线路进行切割、烧毁等手段,使得通信系统无法正常进行数据传输和管理。

3. 外部网络攻击

在电力信息通信安全领域,来自外部的网络侵袭是较为频繁的威胁之一。这类侵袭包括多种形式,如黑客入侵、恶意软件攻击、木马入侵等,攻击者利用网络中的安全漏洞或薄弱环节进行非法侵入。黑客入侵可以直接导致系统瘫痪、机密泄漏或者损坏,严重影响电力通信网络的运行。电力系统一旦遭受严重攻击,将会造成灾难性后果。例如,电力信息通信系统被攻击,可能导

致区域性甚至是全国性的停电，影响行业生产和人民生活，对国家经济和社会稳定带来了极大的风险^[2]。

4. 故障检测与处理难度加大

目前，电力通信网络中存在着众多设备和型号，管理起来十分复杂。对于这些多样化的设备及型号，通常需要依赖人工进行故障排除。同时，通信设备厂商众多，导致设备故障原因多样，从而造成电力通信网运维人员难以对故障进行准确定位与分析。

5. 通信系统运维人员工作方式差异化严重

各地区电力通信网络的运维人员采用的工作方法不尽相同，这导致了电力通信网络在故障处理方面的效率不高。此外，由于不同地区电力通信网络运维人员工作经验的不同和业务水平的差异化，部分运维人员难以有效进行通信网络故障定位与分析。

三、电力信息通信中对通信运行方式管理系统的优化策略

1. 全面整合监测数据

为了获取电网的运行状态数据，必须依赖大量的独立传感器进行监测，这些传感器在电网建设过程中扮演着至关重要的角色。随着电网规模的不断扩大，所使用的监测设备数量剧增，从而产生了庞大的应用需求。在数据的整理和分析过程中，面临的过程十分复杂。在做好整合管理工作时，应采用科学、管理对策，旨在保障数据信息的准确性，获得更为全面的数据整理效果。另外，采用数据整理和分析的方式，根据电网系统中存在的异常部位，在形成客观、合理的判断之后，为后续应对措施制定提供了参考依据。基于关键的数据支持，可以形成对异常问题的妥善处理。

2. 解决电子干扰问题

提升基础设施的性能。在电力信息通信工程领域，电子干扰的主要诱因在于基础设施的配置。为此，应采取专门的接口对接方式，对基础设施进行精准处理，以防止电子干扰的发生。对于部分设施连接点而言，若具有许多对应的接口，此时在接口处理过程中，其难度相对较大。除了需要有效应对接口问题之外，还应合理规划有线和无线连接故障。因此，采用排除方法，根据计算机接口的运行情况，判断其是否处于稳定的操作状态。

3. 构建完善电力信息通信体系

在电力系统中，随着信息通信活动的增多，面临的问题日益复杂。为确保不同操作模式的兼容性，建立一致的管理规范是必要的。通过基于一致的管理体系来执行控制任务，可以实现电力信息通信的集成化。在日常工作过程中，通过挖掘已经出现或者可能存在的问题，

将不同的通信网络融合之后，可以加快电力信息通信工程的总体进度。在整个电力系统中，还应重视对智能化管理体系的应用，通过建立信息系统模型，结合企业的实际情况充分考虑，在制定通信资源整合方案时，应保障方案内容的可行性。在搭建电力系统信息管理平台时，需要发挥互联网技术的支撑作用，将平台搭建作为实施智能化管理的关键步骤。基于管理平台的正常运作，为智能化运维体系的稳定运行奠定有利基础^[3]。

4. 提升智能电网下电力网通信水平

(1) 采用多元化的通信手段。随着我国对信息网络的大规模投资和快速扩张，通信能力呈现出持续增长的趋势。然而，主要的通信设备正面临高负荷运行，而其他通信链路也接近容量上限。鉴于此，迫切需要开发一种具备高可靠性、高适应性和多种通信方式的解决方案。当前，我国电力系统通信主要是以光纤为基础，辅以电力载波、微波及卫星等辅助手段。随着电力行业的不断发展，以及电力网络技术的不断革新，随着通信技术的不断发展，随着通信技术的不断提高，通信性能也有了极大的提高，其中以通信资源占主要地位的无线、4G、光纤、PON、移动、电信、联通等公用事业网络，使得各种通信资源得以有效地使用，从而更好地实现其功能。(2) 扩大通信网络覆盖性。当前主流的通信网络中，采用了光纤化的通信模式，但是其覆盖的范围十分有限，还需要进一步在配电、变电、用电、送电等多方面进行积极的建设工作，从而提升通信能力。

5. 提高人员的操作能力

首先，电力公司需重视提升安全管理人员的专业素质，确保安全设施得到充分保护。无论是电力公司还是网络系统安全人员，都应增强对网络系统安全运营的关注，强化防护和监管工作。特别是网络安全人员，应持续更新知识，增强网络安全意识，积极掌握先进的安全防范技术，并在日常工作中贯彻新的安全管理理念和技术。其次，加大力度监管电力系统安全情况，相关部门管理者应深刻认识电力运行中通信网络安全防护的重要意义，并及时发现自身不足，采取改进措施，加强吸引先进的人才，配置足够的安全防护资金，支持电力系统安全防护工作。最后，电力系统安全管理部门还应注重加强对网络安全管理人员的专业培训，并积极引进先进的计算机技术和设备，以保证电力企业的稳步发展。同时，为了确保网络安全工作人员的综合素质能够与时俱进，电力企业应当定期组织培训，提高网络安全维护人员的专业技能，并且提高其工作责任心确保其综合素质能够满足电力系统安全防护需求。此外，企业还可以通过日常宣传、定期考核等方式激励网络安全维护人员，

督促其不断提升工作水平^[4]。

6. 提高防病毒管理技术

电力通信系统的安全性面临着网络病毒的重大挑战。鉴于电力系统在应用中会受到众多设备和线路等因素的作用，病毒攻击可能会导致电力系统遭受重大的经济损失和安全隐患。当前网络系统常见的安全问题就是黑客、病毒、木马等，这些毒瘤严重威胁着电力系统网络化和智能化系统的安全。有的电力系统遭受到网络病毒侵袭，已经给电网系统带来很大损失，甚至会引发安全事故，严重威胁到整个电力系统的安全稳定运行。为避免电力企业出现过重损失，相关维护人员应当对病毒问题给予足够的重视，提升系统稳定性和安全性。

四、网络技术在电力信息通信中的应用

1. 电网自动化通信技术应用

观察我国电力系统的现状，可以发现先进网络技术已经被广泛应用于电力计算、供电分析、电力统计等多个领域。特别是在监控电网运行状况方面，网络技术展现出了其显著的优势。电力信息通信的主要网络需要实现信息传输、信息管理和信息调度的基本功能，而网络技术进一步提高了这些功能的实现质量。其中，在进行信号传输时，网络技术能够进一步促进传输性能的有效提升。例如，网络技术对继电保护信号传输工作进行优化升级，能够让通信端口在脉冲编码的调制下，实现与数字平台的直接对接，进一步提升信号传输的质量。在进行信号管理的过程中，网络技术的应用能够为业务部门创建一个更加高质量、高效率的信息交流专用网络，有利于进一步提高不同业务部门之间的信息共享质量，促进各业务部门工作的有效对接。将网络技术应用在调度环节中，能够更加高效、高质量地完成遥测、遥控、遥信、遥调远程终端单元的任务，帮助工作人员进一步提高远程监控的有效性，实现对电力系统的全方位实时监控^[5]。

2. 全生命周期数据安全保护

在构建新型电力系统的过程中，多个实体需要共享和交换大量多样的数据。随着数据应用场景和参与实体的不断增加，电力数据在推动数字经济的快速增长方面正变得越来越关键。与此同时，数据安全事件频繁出现，数据安全问题愈加突出。企业需要围绕数据生命周期，研究各个阶段应用的安全保护技术。在电力数据风险预警监测方面，研究数据流量异常发现、数据安全监测分析、数据安全预警以及态势感知等技术，实现对数据生命周期各个过程更为严格的监控与管理，尤为重要。

3. 多层次病毒防护体系的应用

当前，中国在推进电力信息通信技术发展的同时，面临着许多挑战，特别是在业务与通信网络的整合方面。因此，在电力信息通信的建设过程中，工作人员需要不断地对系统架构进行改进，并充分利用新兴的网络技术，以构建一个全面、多级的病毒防护体系。在实际构建电力信息通信系统的过程中，需要建设相对应的内网管理中心，充分根据电力信息通信的防护需求，安装高质量的防火墙系统及杀毒软件。此外，还需要确保杀毒软件与防火墙系统等安全设备的及时更新与升级。

4. 电力安全系统中的应用

智能电网作为一个复杂的系统，在其运作过程中产生了大量的数据流、业务流和电力流。对这些数据和信息实施严格的安全防护是确保智能电网顺畅运行的关键。在电力网络向智能化转型的过程中，安全性的考量同样至关重要，必须在建设和运营的各个阶段给予特别关注。为了确保智能电网的安全性，需要利用电力通信技术对智能电网的数据安全和用户之间的互动进行保障。并且在智能电网的建设过程中，也可以采用电力通信中横向隔离、病毒防御等功能，以求打造清静、良好的互动空间。电力通信技术应用于智能电网中，可以保障发电信息、用户信息、智能设备数据等的安全性，提高电能输送环境，以满足社会需求。

结束语

随着我国经济的蓬勃发展、经济实力的提升以及科技进步，电力信息化和网络技术已逐步成为趋势。在国家经济持续扩张和民众对生活品质追求日益增长的双重作用下，传统的电力发展模式已无法满足新的需求。为确保未来电力发展的稳定性和安全性，必须深化信息技术与电力通信技术的融合。而电力信息化与电力通信技术的融合，大大改变了这种状况，使其在实际工作中更具优势。

参考文献

- [1] 丁嘉祺. 电力信息通信机房的智能巡检技术[J]. 科技视界, 2019(10): 71-72.
- [2] 李婧源. 电力系统信息通信的网络安全及防护研究[J]. 通讯世界, 2019, 26(06): 186-187.
- [3] 梁添荣. 调度自动化管理及电力通信管理研究[J]. 通讯世界, 2019, 26(06): 191-192.
- [4] 赵云超. 配电网络智能终端监控系统设计与实现[D]. 郑州大学, 2019.
- [5] 陈玲. 虚实结合的智能配电网实时仿真系统研究[D]. 浙江大学, 2019.