电力系统信息通信网络安全及防护分析

王欣然[1] 李寅东[2]
内蒙古电力（集团）有限责任公司信息通信分公司 内蒙古 呼和浩特 010020

摘 要：近年来，由于数据网络技术在电力系统中的使用越来越普遍，而计算机技术也发展的很快。大量电子信息的快速传递，使得在电力网络的实际应用环境中蕴藏了许多的不安全因素，而一旦网络的稳定性得不到有效改善，就会导致系统设置与使用上的缺陷，被犯罪分子所利用。而随着日益严重的来自于网络的信息安全威胁，对电力系统信息通讯安全性方面又有了新的要求，因此必须作好对电力系统信息通讯安全性方面的防范工作，从而保证供电系统的顺利、安全、有效的运行。

关键词：电力系统；通信网络；安全防护策略

1 电力系统信息通信概述

电力行业作为国家重点的基础设施保障业务，通过加强国家互联网信息系统建设与现代化监管系统建设，可以有效提升全国电力系统的工作效能和服务质量，为广大电网用户提供更为全面的信息服务。首先，现代电力系统信息网络是现代通信技术、现代网络技术、智能信息技术的有机融合，主要运用了现代管网设计、局部设计、集成和优化管理等现代手段，对输电、配电、用电等各运营环节都实现了统筹管理和集中控制。其次，电力系统信息通讯技术的实际使用需要对信息系统质量、电源保障、传输速度、安全保障等方面进行全面提升。最后，电网的信息通讯体系在实际使用过程中，也就并没有全部以单边效应方式存在，而是全部以一种相对的、更自由的双多变边效方式存在，将业务过程和认知流程等也纳入到信息体系之中，并由此增强了电力生产和供给传输流程的及时性和高效性。

2 电力系统信息通信网络的基本特点

动力系统通信网络是由各类信号传输手段、信息交换装置、技术应用系统等所组成的，并实现了国家统一领导、分级管理的电力工业改革专用信息通信网络，电力系统通信形成了全程全网、统筹作业、协同配合的基本特征。首先，由于电力系统的信息网络涵盖领域比较广泛，包括了计算机技术、自动化工程技术等各个方面的信息内容。其次，电力系统信息通信网络工作中牵涉的实际环节也比较多，并存在着很大的地域性问题[1]。在这里，由于电力系统与信息通讯网络系统运作中还包括了供电传输、电源管理等一系列使得在电力系统运营过程中信息通信网络建设的规模也有所不同。最后，由于电信互联网技术将受到我国整体发展水平、税收政策、立法、科学技术水平等各种因素的约束。

3 网络安全防护对电力系统信息的作用

如果信息网络的安全隐患逐渐提高，那么势必会导致动力系统的正常与运行上出现各种各样的问题。而现在，更多的电力公司改造并开始使用智能设备，如此一来，他们对动力系统的日常工作也将更多的依靠信息网络手段。数字化、互联网、智能化的信息技术将日益广泛的应用于动力系统之中，所以，必须加强实施有关动力系统的安全防御手段，从而增强整个动力系统的安全与稳定性[2]。现如今，企业指挥和管理电力系统大多采用通过内、外设备连接的双网通信方式，可以显著改善电力专网的安全性，从而降低了外电网进入电力系统的内部网络体系的危险。同时利用安全保护手段克服了在奠定复杂电力系统的实际应用和控制流程中出现的困难和弊端，也因此可以更高效的解决复杂电力系统的设备运维、连接和技术等方面的需要。

4 电力系统信息网络安全防护存在的问题

4.1 系统自身安全漏洞导致

首先是由于操作系统本身安全漏洞所造成的安全问题。由于科技的日益发达，当前人类正处在信息化高速发展的时期下，现代计算机信息技术已被广泛地运用于行政单位，而电力企业在发展壮大的过程中也充分地利用了计算机技术，对电力系统实施了管理。而当前我国在发展电网事业的过程中，在自动化管理系统以及相关软件科技方面都存在着一定的信息泄漏，网络系统本身的信息泄露也会严重危害整个电力系统运行信息网络的安全性，病毒以及不法分子等都可能利用信息安全漏洞进入到电力网络系统中，从而对整个电力网络系统产生了不同程度的危害，当电力系统受到损害之后，将会严重影响整个电力系统的正常工作，不仅会危害人民的生活，同时还会给相关企业造成巨大的经济损失。

4.2 电力系统基础设施存在不足

要想保证电力系统的正常血液更新，并提升电力系统的自动化程度，还需要进一步完善电力系统的基础设施建设，并及时更换设施，不过一些供水公司和供热公司为了降低运营成本，并没有及时对设施进行更新换代，仍然使用老旧、破败的设施进行电力系统使用，这样也就没有办法充分发挥起基础设施更多的功能，造成电力系统运行效率低下，不能保障电力系统工作的正常进行。

4.3 病毒攻击

现阶段，电力系统的通讯及网络系统中常用的病毒形式，主要是木马病毒、脚本类病毒等有以下几种，常见的进攻方式大致分为以下二个方向。(1)通过手机终端的存储介质进行攻势。当病毒预先存入在移动终端上的储存介质之中以后，在传播过程当中，病毒很快就会通过漏洞而侵入电力系统的网络之中，在严重情况下甚至会造成整个电力系统在运行的时候就完全瘫痪，而不能正常运行。(2)利用网络缺陷来构建。

4.4 人为故意破坏

人为的故意损坏，人为的在对整个激励系统运行信息网络应用的过程中，如果由于人故意记录下了错误操作甚至是出现了过失操作，那么这种过失操作就会对整个动力系统的运行信息网络产生了损害，并且很重要的会导致整个动力系统的信息网络无法工作，从而对整个的工业系统发展带来了破坏，甚至造成重大的经济损失，同时也对整个能源工业发展的可持续运行造成了严重干扰[3]。

4.5 网络管理运营的风险

电力系统的通信安全问题，主要体现在网络管理的层面。因为动力系统采取了在工作中内外网络隔离的方法，从一定意义上保证了动力系统中所提供数据和信息上的安全性，但在日常的管理和操作过程中却也面临着危险，究其原因，这些安全问题的产生主要是通过人为因素而形成的，能源系统中的指挥、操作人员等以及管理者在平时控制和操作系统中，都可以通过移动的存储介质、电子设备等实现数据通信，而由此产生的信息发生了泄露和失真的状况，但一旦在此环节中病毒或木马的植入，就可能影响到系统的正常工作。

5 电力系统信息通信网络的安全防护策略

5.1 加强完善通信网络的防火墙技术

关于电力系统的配网与自动通讯系统的安全问题，必须加强并改进通讯系统中的防火墙系统建设。防火墙技术在一方面主要是用于对计算机及局域网系统的防护，以保证局域网系统的顺利运作，从而防止了计算机病毒的侵入，及其对电力系统的所造成的破坏，但从另一方面来看，防火墙技术也主要是针对病毒的不良发展情况，进而达到了筛选、监控与管理的真正功能，并以此来保障了对网络通信网络系统的顺利运转，并由此提高与强化了对网络通信网络系统的内部管理功能，并对计算和内部服务系统实现了全面化的管理与保护，使路由器与网络有效的相互整合，并从而实现了对防火墙网络的真正功能。而防火墙的真正功能，正是为了可以对整个网络通信系统实施监控与管理，从而能够保护电力系统不受其他外部危险因子的影响，以促进整个电力系统的安全发展。

5.2 提高网络设备的安全性

由于计算机技术的提高，近年来中国的电力系统的设备可靠性和技术水平也在不断提升，安全风险的管理方式也出现了转变。正确使用国产先进技术，不但可以有效提高电力系统的工作效率，更可以提升电力系统通讯网络的安全性能力。由于当前的电力系统通讯网络基本散布于国内各处，数据资料复杂很多，唯有系统进行保密方可避免数据外泄。采用业内领先的电力网络设备，可以增强公司对电力网络设备的管理力量，如果电力网络设备发生故障，可以及时按照故障原因和故障位置对其实施修理，有效提升了维护效果。就如今的技术发展水平而言，由于目前的电力网络设备发展速度已经相当快，性能在短时期内就可以获得显著提高，对于电力企业来讲也十分有意义。在传输过程中对数据信号进行了加密，能够有效减少电力系统缓慢运行过程中所产生的信息泄露，提高信息数据的传输准确性。

5.3 密码的管理

为防止电力通信网络所提供的数据资料在传播的过程中遭到损毁甚至盗窃，政府必须采取适当的保护措施以提升对数据结果信息的保密水准。电力通信网的典型特点就是它属于分布式系统，其携带的数据信息量很大，所以，人们可以通过公共秘钥法对数据资料进行保密，从而使得电力通信网的安全等级大幅度地增加了。而当前应用较为广泛的就是密钥控制技术，这也是数据加密技术的主要部分，由于这个技术的工作任务相当多，涉及密钥设置、下载数据、使用、存储、验证、管理和备份、管理、撤销等，也就意味着密钥的维持期限非常漫长，它也是数据管理的重要环节。

5.4 加强提高通信网络的应用入侵监测技术

应用入侵性监测技术，主要是指通过对系统行为的严格审核、精确控制和全面的监测，以保障电力系统运

营的安全发展，同时应用监测技术不但可以保障配电网络自动通信系统的平稳运转，而且还可以通过对整个动力系统的内部信息资料加以高效的采集与处理，同时可以通过对数据数值建立出客观综合型的合理判断，为未来电力系统信息业务的开展提供了强大的信息保证，促进供电系统配网自动通讯技术的进一步开发，从而促进了企业的信息化程度获得了提高。应用入侵监测技术研发的重点就是收集电力系统运行的活动状态与环境数据，通过应用方法和模式加以有效的组合，以此来判断进入环境的风险，进而基于分析的结论进行对策，提高电力系统运营状态的稳定性和安全。

5.5 防病毒技术

病毒的预防方法与手段，对于互联网环境必不可少。同时也由于对互联网病毒的危害范围不可估量，从而必须相应的病毒预防手段。基于网站目录与数据库安全的抗病毒特效芯片、基于网页的抗病毒特效软件、实施反病毒程序等，都是目前较为普遍的抗病毒特效方法[4]。由于服务器是整个信息网络的中心，所以如果服务器感染病毒后无法正常工作，将会造成整个网络系统的崩溃。因此设计中选择了采用模块化设计的NLM方法，设计目标主要针对服务器。另外，对杀毒本身的支持也是要保证为正版的，虽然能够避免了某些顽固的木马病毒感染，但杀毒软件却无法确保把所有病毒全部杀干净。

5.6 做好系统操作人员的培训工作

供电系统的任何运行管理措施都会影响整个供电运行系统的安全性，同时一旦有关人员使用不当便很有可能导致病毒入侵和黑客攻击，从而严重威胁到整个供电运行系统的安全性，所以供电单位和供电企业都应该加大对供电系统运行管理人员的培训。(1)要定期开展安全员技术培训，学习新的先进的安全防护知识，提升系统运行管理人员的水平，让安全员能沉着应对安全危机，正确发现安全漏洞。(2)要通过制定严格严密的遵守国家有关规定的操作规范，对安全员等工作人员进行了一定的时间约束，同时又严格规定了安全员的作业活动时间，以增强了安全员的工作责任感，并以此提升了安全员的安全责任意识，从而提高保安技术人员的专业素养和能力，来提高电力营销网络的安全性。

5.7 加强网络管理运营

加强网络管理运营对电力系统信息通信网络安全防护至关重要。对电力企业而言，在电力系统信息通信网络运行过程中，要加强网络管理运营效率，必须密切结合当前我国电力工业的实际特点，建立相关人员的管理和控制制度，加强网络管理队伍建设工作，提高电力系统信息通信网络安全的紧迫感和使命感，强化了网络管理行为，用制度化的形式保证了在电力系统信息通信网络操控流程中的安全性，让电力系统信息通讯与网络的管理更加有章可循。注意安全与保密，有效维护了网站的正常工作和安全，此外，在安全管理部分，要规范和完成对电力系统的管理与维护工作，并进行了包括对网络设备的设置、故障诊断、需求管理等，在与网站完全独立的工作平台上，有效确保了人员管理效率，减少了个人管理疏忽与非法入侵行为，并作好离线系统的信息处理与消除教育工作，避免了关键数据的泄露，以保证了系统的安全正常的工作。

结束语

在对现阶段电力信息通讯系统上出现的安全性问题作出简要研究的基础上，对加强密码管理、增强网络设备的安全性、构建电力信息通讯安全管理体系等对处理这些问题的措施展开了研究。在今后的过程中，为了更好的满足信息化要求，电力公司必须要将电力系统的通讯技术的安全与保障能力提升出来，由此可以保证电力公司信息通讯技术可以在发挥其作用的同时避免数据被盗用或泄露的问题。

参考文献

[1]欧阳宇宏,康文倩,车向北.电力监控系统信息通信网络安全及防护问题研究[J].信息系统工程,2020(12):60-61.

[2]苏昭璞.电力系统信息通信网络安全及防护安全探究[J].科技经济导刊,2020，28(18):39.

[3]胡福平.电力系统信息网络安全防护及措施分析[J].通信电源技术,2018,35（10）：165-166.

[4]骆亮.光纤通信技术在配电网自动化系统中的应用[J].通信电源技术,2019（1）：213-214,216.