电力系统信息通信网络安全及防护分析

赵晨宇
内蒙古电投霍白配售电有限公司　内蒙古　通辽　028000

摘　要：近年来随着经济科技进步的高速发展，信息和通信在电力系统中的运用范畴和方法愈来愈普遍，但网络安全就是工作人员的关键难题。文中首先阐述了电力系统信息通信的特征和现况，再从这几个方面阐述了通信网络安全可能出现的难题，并给出相对应解决方案和预防措施。电力系统信息通信存在的问题比较严重牵制了我国电力系统的高速发展，电力系统信息通信网络的安全防范已经成为如今的社会急需解决关键难题。

关键词：电力系统；信息通信；网络安全；防护分析

引言

伴随着当代电力产业发展，必须进一步加强电力系统的运转效率和质量，其中提升电力信息通信网络的安全防护是主要的一环，受多种条件的限制，电力信息通信网络面临很多安全隐患，这种安全隐患在一定程度上确保整个网络稳定与安全在准确掌握网络安全隐患前提下，实行有效对策加强监管，保证安全安全防护实效性和稳定性，能够最大程度地维护保养电力系统长期性优良运作，给社会协调发展给予帮助与确保。

1 电力系统信息通信概述

1.1 特点

一是，电力系统信息通信网络业务能力强，综合型强。信息通信网络的专业能力就是指相关电力系统和网络技术操作须经技术专业员工进行，了解电力系统和信息通信相关工作人员不可以参加深层次的管理方面。信息通信网络的综合型就是指电力系统，信息通信网络技术包括了好几个行业。二是，电力系统的信息通信网络受我国社会经济发展、国家新政策和科技实力产生的影响。我国经济发展速度相对性迟缓，技术研发过程不太理想，必定危害电力系统信息通信网络技术发展。做为促进电力系统信息通信网络持续发展的现行政策管束和客观原因也决定着电力系统信息通信网络的应用领域和质量电力系统是我国的基本建设，我国趋势对电力系统产生的影响十分明显。三是，电力系统信息通信网络阶段多，具备地区性。职工信息通信网络的工作任务包含配电设备、用电量、输配电等环节。因为我国地域辽阔，每个地方社会经济发展情况不同，在我国电力系统各个地区要求不一样，危害电力系统信息通信网络的工程规模、运作性能和范畴。

1.2 现状

现阶段，在我国早已设立了完备的电力系统，但电力系统管理方法还存在一些问题与限定。文中觉得我国领土面积大，每个地方科技水平发展水准有所差异，在我国每个地方管理规范标准和有所差异，电力系统管理方法难度较大[1]。

1.3 电力系统信息通信网络信息安全的价值

电力系统的网络信息安全十分重要，毕竟在电力系统的运转阶段，信息网络出现安全隐患就会直接影响电力系统的正常运转，进而影响供电质量。由于科技的不断进步，信息互联网在电力系统中的重要性愈来愈高，因此提升电力系统信息通信系统安全性具备十分重要意义。确保电力系统的信息通信网络信息安全，安全防护病毒侵略才是关键。“电脑病毒是网络病毒的一种，具有良好的隐秘性，并且其散播速度很快，对电力工程信息互联网所产生的影响极大。”电力系统被病毒入侵后，也会导致电力系统的信息数据泄漏，那么就会影响全面的正常运转。因此，避免病毒入侵针对确保电力系统的信息网络信息安全尤为重要，进而能够避免电力系统的信息数据库的遗失。

2 防护意义分析

现阶段，移动互联网时代特点的日益突显，网络智能被用于各行各业，变成电信系统的主要支撑点媒介。在一定程度上规范了系统的作用范畴，但是同时因为互联网的开放性与多元性，增强了风险性，给系统自身增添了一定程度的安全风险。尤其是在新时期社会背景下，国家对电网安全的发展理念慢慢获得重视，人们对于电信网服务水平的需求也越来越严。在如此严峻发展趋势环境下，做好安全防范非常重要。全方位细致入微的网络安全防护能有效防止通信系统中安全风险，与此同时确保电网自然环境的安全，推动电力企业全方位高品质重大的发展趋势。

3 电力系统信息通信网络的主要安全问题分析

3.1 电力信息通信网络模型隐患

信息通信网络简单的物理连接结构实体模型主要是以传输系统为核心，包含寻址方式设备及重复使用设备，根据数据链接开展连接和传送。其安全功能模型主要是由新闻媒体网络和支撑点网络两个部分组成。新闻媒体网络包含网络层、链路层，各自适用寻址方式和互换作用、重复使用和流量管理作用、分享和转发作用；适用网包含同步网、报文网和管理网。在电力信息通信网络中，安全技术服务包含服务认证、密钥管理、数据库安全查验、数据信息安全保密性、不可否认性等，物理层、链路层、网络层、传输层、会话层、应用层正常运行，包括网络层包含全部安全技术服务，但是其他协议层只包含其中的一部分。在这个前提下，电力信息通信网络遭遇对抗攻击，有可能会影响网络的安全。对分区规划、安全保密性和易用性攻击会影响到电力信息通信网络的安全，但结果不一样。其中，对控制力攻击可能造成网络资源搔扰、电信诈骗等诸多问题；对安全保密性攻击可能造成信息泄漏、伪造等。对易用性攻击可能导致全部网络的崩溃或毁坏[2]。

3.2 病毒攻击

对当前的电力系统而言，其信息通信系统中常见的病毒是木马病毒、脚本制作等病毒感染。病毒感染主要有两种最主要的拒绝服务攻击。首先，运用移动智能终端和存储设备进攻电力系统。此外，在电力系统的信息传送环节中，预置病毒感染在这里传送过程中需要从电力系统的薄弱点进到其内部结构网络，消除隐患。在比较严重的情形下，全部电力系统将麻痹，电力系统将不能正常工作中。二是由电力系统网络系统漏洞开展进攻。因为一部分网络在刚开始执行和建设中存有不健全、不足的系统漏洞，若不及时发觉、维护保养和恢复这种系统漏洞，便会被病毒感染运用，网络安全隐患高发，总体安全将大幅度降低。

3.3 人员管理问题

电力企业的内部员工很有可能由于各种原因泄漏电力信息通信网络的信息，给顾客与企业产生巨大损失。电力监管不到位，信息安全防护文化教育落实不到位，我国宪法制度不健全，一部分工作员欠缺高效的信息安全防护专业知识，容易因为麻痹大意、错误操作而出现信息泄漏。除此之外，职业道德修养和信息安全责任追究制度存在的问题，一部分工作员有意泄漏关键内部结构信息谋私利，很有可能严重危害电力信息通信网络的安全。

3.4 网络设备风险问题

网络风险主要指电力系统里的网络设备在具体运行时出现故障。网络风险问题造成有软件环境、机器设备品质、人为要素等众多因素。其中，最突出的关键是网络设备自身的产品质量问题。分析表明，在我国大部分网络设备是以海外引进，独立开发出来的网络设备特别少，生产技术比较落伍。因而，在我国电力公司使用网络设备和网络信息技术的过程当中，通常遭受技术垄断及设备专利的牵制，增强了网络的运行成本和维护费用。在如此的大环境下，假如网络信息通信设备出现故障，往往会造成通信网络风险，供电系统被断开，电力系统的应用高效率减少。外在因素也会影响到病毒感染和网络黑客等网络设备。网络黑客引入病毒感染或违法进攻会影响到网络设备的正常运转，造成机器设备奔溃或作用遗失。若不能合理预防，将引起网络设备风险事件，严重危害全部网络全面的安全运营[3]。

4 电力系统信息通信的网络安全及防护措施

4.1 优化电力系统内部管理机制

内控管理是合理避开电力系统信息通信网络信息安全风险事情的重要途径之一。因而，互联网技术信息散播风险的概率需从其内控管理的视角下手。首先剖析电力系统运作风险，全方位挑选电力系统运行时给信息网络通信产生风险的风险，制定对应的风险应对机制，区划风险级别，如一级风险、二级风险、三级风险等。其次，为了能合理内控管理工作质量和效率，管理人员应该根据工作实践健全已有的管理方案，全覆盖管理方面，细化管理具体内容，完善规章制度。从及时性的视角，分析和预测分析可能发生的风险难题，做为风险预防整体规划能够起到网络安全的功效。内部结构管理职责能通过制定责任机制，确立监管责任与网络安全防范措施来达到。如果出现了难题，能够上溯到最开始指定责任人。再次，推行精益化管理。在细化管理的过程当中，从信息通信网络安全防范的角度考虑，要特别关心小问题、风险和缺点。

4.2 加强电力系统内部管理力度

电力系统的信息数据、信息传输量一般非常大，规定电力系统有更加全面、科学合理的信息通信远程教育系统。电力公司要加强电力系统综合性信息远程教育系统的建设。这样才可以渡河传输电力信息数据信息。内部结构管理人员在工作上一定要对工作负责，提升电力系统信息通信应用系统的风险控制。以下属于完成电力通信数据精确安全传输的三条提议。一是，能够资金投入更多资金用于电力现代通信技术基本建设。在风险控制层面，能够引入海外前沿的风险防治新技术应用。电力信息管理方法能够执行有效管理对策。要避免非法侵

入，能够科学研究黑客攻击方向，不断更新系统。这样才能确保电力数据库的恰当传输与使用。二是，组装强悍的网络防火墙。提升系统对中生疏IP地址的浏览管理方法。要是没有全面的批准，就无法访问电力系统的信息管理方法。三是，应用密秘安全生产技术。为了能数据加密电力信息系统中信息，能够按时变更电力信息全面的登陆密码和公匙。这保证了电力数据的存储和传输的安全。

4.3 完善纵向加密与隔离装置的安全

为了防止病毒攻击，确保通信系统内部安全，相关部门必须从数据加密和防护两方面提升自主创新具体方式方法，创建全方位的安全防护管理体系，完成多方面视频监控系统。首先积极主动设定及安装竖直数据加密这一关键安全防护设备，依据风险选择不同加密算法。一般来说，有关的专业技术解决种类分成三个等级。①直接拒绝。选用竖直数据加密对电信系统内部结构软件环境进行二次维护，根据方式系统对内部网络开展引流方法，适用竖直数据加密机器设备进行进攻安全防护与控制。间接性抵触。②间接拒绝。以Linux为技术媒介，搭建对应的设备功能。说明与另一台方式对比，拥有更显著的功能特性，协调能力强，调节便捷。能够更系统地保证设备安全遮盖，有关部门必须逐步完善Linux技术，将系统漏洞风险指数值降到最低。与此同时，相关部门需要从隔离与防护的角度考虑合理的安装保护装置，比如说引进防火墙隔离设施，对病毒进行有效隔离，并实现全面、智能的监控，全面提高防护设备在DDoS抵抗方面的综合能力。

4.4 研发安全传输渠道

结合当前通信系统行业存有的数据信息传输风险难题，相关部门可以从思想与技术方面来积极主动改善，提升实际传输途径为依托，保证数据信息传输安全，防止伪造、遗失等种种风险。首先，以电子计算机为依托，设立了智能数据传输—— 监管一体化工作系统，完成了传输过程的视频监控系统。使职工能够及时鉴别数据信息传输里的潜在性风险，在自动化的介入下进行合理的控制与维护，保证系统的软件环境。与此同时，需要重点提升信息传输中安全备份数据、风险认知、真实有效评定等方面提升基本建设，保证传输的信息更为真正全方位。

4.5 注重物理层的防护工作

第一，避免雷电灾害的产生。若其楼房雷电灾害预防措施不符相对应要求及规范，将严重危害其全面的全部阶段、设备及路线安全。为了能尽量减少这种情况和状况的产生，电力通信系统有关权威专家必须定期检查系统中各通信设备乃至主机房里的电路板实时严格定期检查检验。发觉、妥善处理和处理出现异常、难题或常见故障，可以有效防御力和解决雷电灾害等不利条件对电力信息通信应用系统产生的影响。第二，留意机房环境日常维护和建设。在这一方面，首先确保机房环境环境整洁，有较好的自然通风实际效果。这样才能能够更好地防止电磁波辐射和干扰信号产生安全隐患和困惑，尽快建立相应的防范和预防措施和方式。除此之外，对于有些机器设备，电力公司已需详尽设定有关机器的操作权限并进行筛选，认证有关作业人员与用户真实身份。从而，能够大幅降低人为失误造成安全问题[4]。

5 结束语

总的来说，在信息时期，电力公司十分重视电力信息网络通信的安全防护及管理，考虑到电力信息网络通信特性、自然灾害、人为损坏、管理制度、员工管理、黑客攻击等各个要素，综合性制定科学合理的安全防护方案，针对性地强化安全管理，有效降低安全风险对电力信息通信网的威胁程度，充分发挥电力企业在和谐社会建设中的作用和价值。

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):39-40.

[3]李荣荣.智能配用电通信网络业务评价及安全防护机制研究[D].北京:华北电力大学,2019（03）:121-122.

[4]蒋荣辉.电力系统信息通信网络安全及防护探索[J].科技创新与应用,2019（12）:84-85.