针对电力通信网的信息安全技术研究

白银库
山东能源鲁西矿业单县能源有限责任公司　山东菏泽　274300

摘　要：科技的快速发展使得现代社会的网络用户数量呈飞速增长趋势，有效推动了我国进入大数据时代的步伐。但在给我国经济与文化进一步发展带来重要机遇的同时，也因为网络的特殊性使得大量的用户数据安全得不到有效保障。本文简述了电力系统信息通信网络安全风险，并就保证信息安全的相关对策进行了深入分析。

关键词：电力通信网；信息安全；技术

Research on information security technology for electric power communication network

Yinku Bai
Shandong energy Luxi mining Shan County Energy Co., Ltd. Heze, Shandong 274300

Abstract: The rapid development of science and technology has led to rapid growth in the number of network users in modern society, effectively promoting the pace of China's entry into the big data era. However, while bringing important opportunities for the further development of China's economy and culture, the security of a large number of user data cannot be effectively guaranteed because of the particularity of the network. This paper briefly introduces the security risks of the information communication network in the power system and deeply analyzes the relevant countermeasures to ensure information security.

Keywords: power communication network; Information security; technology

引言：

信息时代的到来，让我们的信息技术得到了前所未有的发展机会，信息技术随着发展也逐渐应用到了我国的多个行业中，电力行业便是其中一种。将信息技术应用在电力系统中，有效提高了电力生产质量以及电力利用效率。当前我国电力系统中的信息通信系统，已开始向系统化、智能化、自动化方向发展。计算机系统和智能系统的结合有利于提高电力系统电子业务的办理效率，同样也能简化电力系统的操作流程，提高工作效率。随着我国信息技术水平的不断提升，电力系统信息通信网络安全需更高的标准对其进行保护。

1、电力系统信息通信网络安全风险分析

作为具有全面性特征的网络信息交流系统，电力系统通信网络的应用风险主要体现在网络设备、内部系统以及网络安全管理操作三个层面。网络设备是保证用户数据安全的第一道大门，但从实际情况来看，由于电力系统通信设备的特殊性，我国依赖国外进口设备的现象仍然较为常见。这种情况下无论是安全性还是实际的电力系统应用层级都无法进行综合控制，极容易在出厂之初设置网络后门，从而影响最终产品的安全运行质量，甚至出现黑客利用设备漏洞对局域网与内部系统进行攻击的情况，造成数据丢失从而影响电力系统的稳定运行；电力系统在应用时对于内部信息系统的依赖程度较高，在介入到外界网络后一旦通信途径被窃取，在没有足够安全措施的情况下黑客们能够很轻松的实时拷贝通信过程传输的网络信息，造成巨大的网络安全风险；由于我国电力系统内部与外部网络处于分离状态，因此在一定程度上避免了外部网络攻击风险，但仍存在操作不当或是网络管理不完善的内控网络运营风险[1]。

2、物理层面的安全隐患及防护技术措施

2.1 物理层面的安全隐患

2.1.1 光缆干线的损伤。自然灾害、人为破坏都可能是光缆电线遭到损害。人为因素则包括故意损害和无意

作者简介：白银库，男，汉，本科，中级工程师，山东科技大学，煤矿机电。

损害两方面因素。

2.1.2字微波传输系统信号遭到干扰是其中常见的原因之一。

2.1.3通信通道和硬件设备自身防护能力差，缺乏强大的防窃听、防攻击能力。尤其是当雷电发生时，有些通信机房缺乏有效的防雷措施，致使雷电对通信设备造成破坏。

2.1.4电力无线通信网存在的管理问题。目前，我国在电力无线通信网络的管理当中仍然存在着一些问题，这些问题或大或小，到现在仍然没有形成一个完善的管理体系来对电力无线通讯网络的管理来进行管理。并且，部分企业和部分人对网络安全的防护意识远远不够，一旦出现一些问题，相关的工作人员就不能对其进行快速的解决。伴随着我国科技水平和经济水平的不断完善和发展，我国在电力无线通信网络当中的管理水平也要与时俱进，就像我国科技水平和经济水平的发展程度，进一步提高电力无线通讯网络的服务水平和安全防护意识。

2.2冗余技术

电路组件中每一组结构都是相对独立的，每组两个不同的操作系统形成一个冗余系统。通常情况下，其中一个系统在应用方面占有主导地位，一旦系统受到外部攻击或是内部组件出现故障，主控就会自动发送指令，随后冗余系统就会开始工作，这在一定程度上保障了电力通信系统的安全运行。

2.3手动切换模式

为保障通信系统的运行正常，一般来说除了必要的系统自动运行机制还需在排除系统技术故障后切换到手动模式，尤其是通信系统待机时，为避免在紧急

2.4物理层的安全防护技术措施

硬件设备和通信通道的维护。维护电力信息通信网的硬件设施和通信通道的完好是电力信息通信网安全防护的基础工作。要注意维护硬件设备和通信通道的日常安全，尽量避免自然因素和人为因素等外力因素的破坏。加强防雷防护，做好防雷接地工作，并对防雷设施进行定期检修和日常维护。杜绝超越用户使用权限的操作行为，进行严格的身份验证管理和权限限制，降低风险。建设良好的通信机房环境，通信机房内要清洁干净、通风良好。此外，在信号线和电源线上安装高质量滤波器、对金属和各种接插件进行屏蔽、对机房内其他金属制品（如管道和门窗）进行屏蔽，可以有效地抑制和消除电磁干扰[2]。

3、电力通信网的信息安全技术措施

3.1多层次的系统加密处理

对系统进行多层次与多途径加密，尤其是针对中心节点采取针对性的加密方式，有效保证了节点的安全性能，例如节点式、混合式以及链路式等。一旦系统检测到有外部入侵节点或是破解节点系统，在加密的情况下会大大增加暴力破解的难度，为发现非法活动流出时间从而保障信息安全。数据传输加密过程中，则应在系统机密的基础上，采取节点相异加密技术，结合多层次系统加密处理完善加密体系，从根本上提升系统自身抵御外部网络攻击的能力。

3.2网络层面的安全防护技术措施

设置网络防火墙。建立科学的防病毒体系，运用多种查杀方式对网络病毒进预约查杀、实时查杀和人工查杀等。专门的对外服务器的设置也非常必要，可以在避免内部服务器受到侵袭的同时，正常进行对外服务。数据加密技术的应用也是保障网络安全的重要手段，使用专业的文件格式和通信规约，采取不对称加密手段加密数据信息，都可以有效降低数据信息风险。建立健全入侵检测系统，可以可靠快速地检测到外来入侵，对电力信息通信网进行强有力的监控，及时发现问题。完善的身份验证和授权机制也十分重要。身份验证可以运用一次性口令系统，口令单次有效，提高系统的安全系数。另外，还应对数据进行及时备份，否则数据因设备故障而丢失，就会造成严重后果。

3.3电力无线通讯网络信息技术采取加密的方式来进行传输

对电力无线通讯网络的信息技术进行加密的方式来进行传输，其目的就是为了防止电力通信网的信息在运输的过程当中出现丢失或者被盗的情况。通过加密的方式来进行电力通信网的信息的传输，其实质就是通过将所用传送运输的信息运用加密的算法将其转换为密文，如果想要得到这些加密的信息，就需要先解开加密的密码。这一方法使信息的保密程度和安全程度都在一定程度上得到了很大的提升。此外，与其相关的信息技术管理人员仅仅只需要使用密匙就可以让文件进入可读这一模式。对于电力通信网的信息安全进行加密，是对信息数据进行保护的一种模式，利用这样的方法来对电力通信网的信息数据进行安全保护，在很大程度上可以保护电力通讯网的信息数据免除遭受到侵害的风险。此外，在电力通讯信息王的数据进行传输的过程中，还要设置相应的传输密码，进一步可以保障电力通讯网络信息数

据在传输过程当中的安全[3]。

3.4加强电力系统的内部管理

电力系统运行过程中所产生的信息数据量非常庞大，必须有完整、科学的电力系统通信网络管理体系作为支撑，才能确保数据信息的准确传输。电力系统管理人员要提高工作责任心，加强对电力系统信息通信网络运营中的风险控制。具体的管理内容可以分为以下三个方面。

3.4.1提高资金投入

增加对电力系统网络通信的资金投入，有利于提高通信技术，降低管理风险。从风险管控角度来看，可以通过引进国外的先进防控风险技术，提高风险管理水平。从电力系统监管角度来看，可以通过落实科学高效的监管措施，防止黑客入侵电力系统。同时要定期更新电力系统，确保电力防护系统的完整全面，防止电力数据泄露。

3.4.2建立防火墙

要想防止陌生IP进入电力系统权限管理中心，可以通过设置强力防火墙实现。未经允许的陌生IP，无法进入电力系统的信息管理平台，也无法查看电力系统的相关内容。

3.4.3使用保密技术

电力信息系统中的密码和公开密钥可以通过定期更换防止泄露，此外通过加密电力系统的信息通信管理平台信息，也能有效防止电力数据的泄露。

3.5优化与改进电力自动化通信技术

想要保证网络信息安全，除了电力系统现代化通信技术的应用，还应跟随时代发展形势融入自动化网络通信技术。随着近些年来用户需求量的增加，电网规模也在不断扩大，较多的变电站采取了无人值班以及通过网络远程调控的运行模式，有效提高了现代电网的运行安全性与稳定性。企业在不断发展的同时，电力系统也在不断地更新与完善，尤其是在容量与通信质量方面更是有了新的飞跃，无论是宽带传输速度还是业务接口拓展方面相较于以往均有了较大的变化，极大的满足了市场运行与企业的发展需要。

3.6管理层面的安全防护技术措施

提高电力信息通信网相关工作人员的职业技能和专业素养，加强管理者管理水平，培养责任感和使命感，加强防泄密的相关培训，防止人为造成的电力信息通信网危害。重视密码保护，不长期使用同一密码，而是进行定期更新，严格管理，防止密码泄露造成的危害和损失。与时俱进，定期组织网络管理人员进行网络安全防护措施方面的学习，了解和掌握前沿网络安全防护技术手段，了解防火墙、入侵检测设备等防护手段的综合运用。

4、结束语

综上所述，在大数据时代来临之际，个人和企业需要针对计算机网络安全高度重视起来，合理分析当前网络安全的各种问题，明确了解工作生活中应该注意的事项和内容，在发现网络安全隐患后，采用科学合理的措施进行解决问题，创建安全有效的网络管理平台，完善网络安全相关法律法规，提高人们的网络安全意识，让全社会各界共同发力，构建出一个安全、高效、健康的大数据网络新时代。

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]安子畅，杨硕，郑景.电力系统信息通信的网络安全及防护研究[J].通信电源技术，2020，37（05）：216-217.