电力系统信息通信网络安全防护技术研究

刘宇星

（中能电力科技开发有限公司 北京市 100011）

摘要：电力系统中，信息通讯网络的安全和保护是人们十分关心的问题。随着国家经济和科技的飞速发展，电力系统中的信息通讯得到了更广泛的应用，但同时也给人们带来了很大的挑战。本文首先对电力系统中信息通讯的特性及现状进行了分析，接着就可能出现的一些问题进行了阐述，并针对这些问题提出了相应的防范措施。当前，电力系统中存在的信息通信问题，已成为影响我国电网发展的重要因素，而对其进行安全防护，也是当前社会急需解决的重要问题。

关键词：电力系统；信息通信；网络安全；防护分析

1 引言

信息化时代的来临，给我们的信息技术带来了空前的发展机遇，同时，信息技术也在国内的各个领域中逐步运用，电力工业就是其中之一。在电力系统中引入信息技术，可以有效地改善电能的产出和使用效率。当前，我国电力信息通信系统已逐步向系统化、智能化、自动化方向发展。本文介绍了一种基于信息技术的信息管理方法，它是一种新型的信息技术，它是一种新型的信息技术。随着我国信息化建设的不断深入，对信息通信网络的安全要求也越来越高。

2 电力系统网络安全防护工作主要内容

实践证明，保证电力信息通信网的安全性是十分必要的。要达到这一目的，相关工作人员就必须结合实际情况，对电网中的信息通讯网络操作安全问题进行分析，准确地掌握其运行特征和安全风险，为提高安全防护工作内容、目标明确性做好充分的准备。电力系统中的信息通讯网络是一种特殊的产业网络，因其地域分布广泛，各地区基础设施水平差别较大，故其网络结构具有显著的区域性特征。另外，在电力系统的信息通信网络中，还存在着大量的数据信息，大量的数据传输，对信息的传输稳定性的要求很高，同时也存在着巨大的安全隐患和风险。在电力系统网络网络的正常运营中，存在着物理和信息两方面的安全隐患。在实际应用中，电力系统结构不合理，恶意程序入侵，信息数据泄漏，系统工作失误，通信设备老化损坏等问题，严重制约了电力系统信息通信网络的正常运行。因此，在电力系统信息通信网络的安全保护工作中，保证数据的安全性，保证通信的畅通和安全是工作人员的首要责任；而日常工作的重点，就是要对安全隐患进行有效的预防。电力通信网络的实体安全风险大部分来自于人因错误或者管理不善，而信息安全风险主要来自于技术方面的原因，因此，必须强化人员管理和技术管理，这也是建设安全、稳定的信息通信网络的首要任务。因此，打牢信息通信网络的安全保护技术基础，并在网络的构建和发展过程中强化技术支撑，是其重要的一环。

3 提高电力系统信息通信网络安全防护的价值

为保障电网的正常运行，保障电网的安全运行，显得尤为重要。而在安全方面，则是会影响到供电质量。近几年来，由于科学技术的快速发展，电网对资讯网路的依赖程度越来越高，因此加强电网的安全性已成为当务之急。针对这些问题，提出了一种新的解决方案。网络病毒是一种隐蔽性强、传染性强的计算机病毒。一旦某种病毒在电网中传播，整个电网都将陷入瘫痪。此外，若有病毒侵入，将导致储存于电网的资料泄漏，对企业及国家造成不可估量的损失。

4 电力系统信息通信网络安全问题

电力系统中的信息通信网，因其覆盖面广，目前存在着较高的安全风险，对电网的安全造成了极大的威胁。从网络设备、系统内部和网络管理操作三个方面来看，它们都是潜在的风险。

4.1 网络设备存在的风险

文章通过对当前我国电网企业在信息化过程中存在的一些问题进行了剖析，并给出了解决方案。目前，国内电网运行仍依赖于外国先进的技术与装备，其运行过程中还面临着大量的不确定性，如：故障诊断、维修与升级等。这也导致了“人为漏洞”的出现，导致了电网整体的安全得不到保证，而且如果被发现或者入侵，将导致难以预料的结果。此外，一些接入的联网设备还含有可以启动的命令或程式，如果被某些别有用心的人所使用，可能会造成我们国家电网的通信中断，设施瘫痪。

4.2 系统内部存在的风险

随着信息化时代的到来，电力系统对信息化的依赖程度越来越高，其本身的安全性能也越来越差。网络信息系统给电力系统带来的危害与影响是多方面的，比如，

计算机自身包含大量的电辐射，这些电辐射会对电力系统的信息内容产生影响，进而导致电力系统遭受辐射攻击，进而产生严重的安全隐患。此外，由于电力信息系统本身就具有无线通信的功能，若不事先对其进行加密或保密，外人就可以通过这种能力对电力系统发动攻击，或干扰电力系统的数据传输。

4.3 网络管理运营风险

目前，我国电力系统内网与外网相分离，在保障电力系统安全的同时，也给电力系统的运行与管理带来了潜在的安全风险。在对电力系统的信息通讯网络进行日常管理和运行的过程中，需要通过多种终端或者媒体进行数据的传递，这就导致了在传输中出现了信息泄露、扭曲等现象。万一被感染了，就会导致整个电网瘫痪。

5 电力系统信息通信网络安全防护措施

5.1 加强电力系统的内部管理

电力系统在运行中产生了大量的信息和数据，为了保证数据的精确传递，需要一套完善的、科学的电力系统通信网管理系统来支持。在此基础上，提出了在电力系统运行过程中，应加强对电力系统运行过程中的风险管理。其管理的具体内容可归纳为三个部分。

1.提高资金投入

在电力系统建设中，加大对电力系统网络安全建设的投资力度，可以有效地改善通讯技术水平，减少恶意攻击风险。在风险控制方面，我们可以借鉴国外的一些先进的风险控制技术，从而进一步完善电力系统网络安全的风险管理。从电力系统监督的角度出发，采取科学、有效的监督手段，有效地防范网络黑客的入侵。

2.建立防火墙防护机制

为了阻止陌生 IP 的入侵，可以采用强大的防火墙来实现。未授权的陌生 IP 地址，不能登陆电力系统信息管理平台，也不能看到电力系统的有关内容。

3.使用保密技术

通过定期更换，可以避免电力信息系统中的口令和公用密钥泄漏，另外，对电力系统的信息通信管理平台的信息进行加密，还可以对电力数据的泄漏进行有效的预防。

5.2 提高控制设备的安全性

为了从本质上提升电力系统的安全性，必须对其进行安全保护。目前，我国电力系统中较多的 PLC 等控制设备均为进口产品，必须加强对这些设备的全面管理，以保证设备的安全、可靠、可靠。另外，为了减少由国外引进的设备给电力系统带来的安全隐患，各大电力公司应尽可能采用国内电力系统控制设备。

引进国内先进的国产控制装置，能够加强企业对电网的管理，使电力通信网络中在面向外部恶意攻击时，能够快速有效进行系统版本更新，避免受到恶意入侵。近几年来，由于电网的信息化程度不断提高，各种安全监测装置的功能和技术水平都在不断提高，因此对电力通讯网络的安全性进行了相应的监控。从目前的发展态势来看，我国现行的电力网络安全防护设备正以极快的速度发展，其性能将会在短时间内获得更大的提升，这对于电力企业具有重要的意义。

5.3 建立完整的电力系统网络安全运行评估系统

为了强化电力系统的通信安全，实现电力系统通信过程的安全态势监测和防护，必须要建立一个健全的电网信息通信网络的安全运行评估系统。要构建完善的电力系统网络安全评价体系，就必须组建一支专职的电力系统网络管理队伍。专业的管理队伍可以增强对电力安全保护系统的各种管理，发现有疏漏或疏漏时，可以利用专业的知识及时修复。网络安全评价系统的管理者在工作过程中必须要注重操作规范，强化电力系统的网络态势感知能力，可以让工作人员对电力系统的故障部位、故障原因进行精确的定位和判断，从而提升电力系统网络安全的管理水平。

6 结论

综上所述，电力系统是影响国家电力系统网络安全的重要因素，它既是一个系统的系统工程，也是一个长期而复杂的系统工程。电力企业必须对电力系统的网络安全保护给予足够的关注，通过多种方式来提高保护的程度，减少可能给电力系统带来的安全隐患，让电力工业的可持续发展得到更好的发展。

参考文献：

[1]刘贺英.陕西教育系统构建网络安全防护管理体系案例[J].陕西教育(综合版)，2022(S2):39-40.

[2]汪升华.新形势下计算机通信网络安全防护策略[J].数字技术与应用，2022，40(7):234-236.

[3]应欢，周劼英，邱意民，等.美国电力关键基础设施网络安全防护政策和标准研究[J].电力信息与通信技术，2022，20(6):35-43.

[4]李华.长输管道工业生产网络安全防护的工程实践[J].中国仪器仪表，2022(6):85-90.

[5]李继元.铁路通信网络安全防护研究[J].中国铁路，2022(6):94-98.