电力系统信息通信网络安全及防护分析

瞿 源 井 轩
汉江水利水电（集团）有限责任公司网络信息中心 湖北 武汉 430040

摘 要：电力系统信息通讯工程是电力系统不可缺少的重要组成部分。而电力系统信息网络技术在其实际工作流程中的工作安全性也是整个体系存在的一大隐患问题，它在一定意义上直接决定了整个体系的效率，以及各工程作业的整体效益。由此可见，针对动力系统信息通讯来说，进行网络安全方面的预防工作有着至关重要的作用。基于此，本文重点针对动力系统信息通讯的安全及预防方面展开了广泛的探讨希望能够为同行业工作者提供有效的参考，从而进一步的推动我国电力系统的不断发展与优化。

关键词：电力系统；信息通信；网络安全；防护安全

引言

目前，随着社会经济繁荣发展的需要，以及电力工业改革全面发展的今天，信息系统也开始被普遍的运用到了电力行业之中，随着动力系统信息化管理水平的提高，更有效保证了电能生产质量，所以人们针对于对动力系统的信息通信与安全保护，也提出了更高的技术需求。

1 电力系统信息通信概述

电力工业改革作为国家重点的基础设施保障业务，加强互联网信息系统建设与现代化监管制度建立可以有效提升电力系统的工作效能和服务质量，给电网用户带来更加优良的服务质量[1]。首先，电力系统信息通信是通讯技术、计算机网络技术、智能化信息技术的有机融合，主要采用管网设计、局部设计、整体优化等技术手段，对输、配电、用电等各运营环节实施统筹管理与集中控制。其次，在电力系统信息通讯技术的实际应用的同时，还需要对信息服务质量、供给保证、高传输速率、安全性保证等方面做出整体改进。最后，电能与信息通讯技术在具体的使用流程中不以单边效应方式出现，而是以一个更加开放、自由的多变效应方式出现，把客户感受与感知过程融入其中，从而提高了电能生成与供给传输过程的可靠性与高效性。

2 加强电力系统信息通信网络安全与防护的重要价值

电力系统工作的实际工作中，提高信息系统安全保护能力必不可少，一旦信息系统安全问题过多，将给供电系统的安全工作造成恶劣影响，导致系统的电能效率进一步降低。在国民经济全面发展的大背景下，随着智能电力系统的使用范围逐步扩大，电力系统的对信息网络的依赖性也愈来愈大，在此情况下，加强电力系统的信息通信与安全保护工作就变得尤为重要。网络病毒属于计算机病毒的一类，具有着强大的隐蔽力，并且由于其传播速度非常快，对电力的网络产生的冲击也很大。如果电力系统运行时遭遇网络病毒的侵袭，则网络系统内的信息系统数据将很易发生损失，甚至会影响电力系统运行的正常安全工作，并造成较不良的社会环境影响。因此通过加大对动力系统信息安全管理与保护力度，就可以对网络病毒发挥较良好的防御功能，从而有效保护了动力系统信息通行数据的安全性。

3 电力系统通信存在的问题

3.1 内部风险问题

内部隐患一般是指电力系统的内部出现的风险问题，这些隐患如果存在，会对动力系统的通讯系统产生重大干扰，直接影响动力系统的平稳、安全工作。经过研究表明，随着当前科技发展的持续提高，电网信息通讯技术使用效能大大提高。当前很多供电系统已经开始应用了数据通讯技术，达到了信息收集、分析、传输和共享控制的一体化。不过，电力系统的内在安全性问题仍然存在。比如，网络数据传递困难、设备维护工作困难和系统故障等。一旦在电力系统正常工作的进程中发生这些困难情况，必然会对动力系统数据通讯的传输与电力供应产生干扰，影响动力系统数据通讯网络的工作效能和服务质量。

3.2 基础设施落后

随着近年来计算机的飞速发展，动力系统也不断进行了改革，设备也不断进行着更新换代，但由于计算机硬件的成本更高，涉及领域也更广，使得计算机硬件设备逐渐无法赶上软件创新的步伐，落后的主机和断路器设备开始逐渐更新换代，被运行效率较好的计算机所取代，同时由于人们对运行效率和内存需求的越来越大对硬件也具有更高的需求。这就要求有关方面科技人员研究更为先进，更加适应当前科技环境所必须的硬件设备，研发出性能更为

优异，安全保护能力更强的硬件设置。

3.3 数据传输问题

在通信技术中数据传输是其自身应具备的主要特性。随着网络时代的来临，网络上的数据在表现形式与载体上出现了显著性的不同。越来越趋向于以智能化的方式进行管理，在互联网的支持下对相应的数据或资料流实现智能传送，并针对具体的数据传输进行了相应的运算和操作设定，以此完成信息系统的智能化操作。但是，互联网在提供了电信系统便捷数据传输途径的同时，也在一定程度上提高了安全隐患。内容主要涉及数据的盗取、截获、修改、检测等，对系统的规范化执行带来不良干扰。另外，很有可能出现数据中断而造成一个网络在工作过程中发生系统失效，从而使得整个网络陷入崩溃，严重干扰了服务的实现。所以，根据当前所面临的网络安全问题类型，政府有关部门就必须从思维层面上端正认知与心态，并结合要素因素考虑就具体的保障要求作出合理性分析，以便于为维护电信网络系统及其内部环境的安全，提供必要的制度保障。

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

内部管理系统也是对电力系统信息通信中安全风险事件实现合理规避的关键技术手段之一。但是，针对系统内部通讯风险问题出现的情况，应从其内部控制方面考虑。首先，通过研究动力系统的运营风险，充分筛查在电力系统运营中对电信通讯系统构成危害的风险，建立相应的风险应对体系，建立相应的风险应对体系，界定危险级别，包括一类风险、二类危险、三类危险等。第二，为切实提高企业内部控制的效率和品质，企业管理者应针对业务实际健全现有的管理体系，以实现企业管理工作的全方位涵盖同时要将工作任务细分，明晰工作任务，从时效性角度考虑，对可能存在的问题情况作出整体分析和预测，并以此为依据制订风险预警方案，发挥安全防范的功能[3]。内部机制的改进也可通过建立责任机制实现，明晰部门主管职能，增强信息安全防范工作的必要性，如发现重大问题能够在第一时间追查到并指定负责人。其三，实现信息精细化管理，在信息精细化管理过程中应从信息通信安全的预防层面入手，需要特别关注小问题、小隐患和小瑕疵等。

4.2 提升网络设备安全性

因为许多电力设备都是进口的，在网络设备的使用中，政府必须对设备的使用与操作实施统一监督管理。为了降低进口设备的安全风险，中国广大电力行业都应该尽可能选用国产的网络设备。国产网络设备随着近年来的性能提升，对安全风险的管理能力也提高了不少，国内先进装备也能够对质量做到有效监控。由于中国电力系统中的数据流通网是大区域分布式的，数据资源多且繁杂，所以电力企业转型需要对数据进行加密保证数据的安全性。而为了加强电力系统信息通信安全，就必须在网络设备上增加安全性。鉴于中国电力信息系统及网络设备的市场情况比较复杂，而且许多电力设备都是进口的，所以安全风险也较大。为了减少进口设备对中国国内电力系统信息网络的安全风险，在对网络设备的管理方面，要针对设备的工作状况实施综合的管理。并建议在一些比较大的电力公司，尽可能采用国内领先的供电网络设备。因为这样，才能确保供电网络设备质量的高可控性。如果电力网络装置发生了故障，企业也能够适时地对故障装置进行修理，缩短维修时间。并且现在的供电网络装置开发很快，稳定性良好。这种大型电力行业就能够有效保证供电线路设备的安全，对供电设备的监管上就需要加强这样才能保证供电数据的稳定性。电力企业必须建立完整的供电数据保护系统。因为供电信息如果在数据传输时中断，将会降低电力系统的工作效率。

4.3 网络密钥安全防护管理

观察和研究电力系统通讯网络的特性，不难得出结论，如果人们想更好的保障电力系统中的通讯系统的安全，需要利用密钥的设计和应用的方法，进行信息的控制。比较常见的有三层加密体系。在该体系中，密码一般由三种等级构成：初始密码，加密密码和主密钥。采用这种分级管理方式，不但能够提高其上级密钥的稳定性，同时其下级密钥也具备弹性，能够按照一定的技术条件做出一些变化，以便建立带有动态特性的加密体系[4]。此外，从目前网络应用的开放状况来看，仅第一级加密用于自动实现，而其余层级的加密则能够通过相应协议进行主动部署，更新和销毁， 由此导致密钥关键自动化控制过程得以逐步加速。专注的信息管理不但可以保证信息系统的所有资料和数据的安全性，同时也能够避免骇客侵入和病毒攻击，还可以提高计算机信息系统的稳定性。

4.4 加强技术创新

电力系统的通信安全防护侧重于社会应用和成本，所以必须从技术角度对其加以研究。通过研究当下网络安全情况，应用技术具体如下。第一，防火墙的应用。防火墙技术是当下最为普遍的安全保护技术手段之一，主要通过对互联网外部、计算机系统内存及中间进行安全的隔护墙，将非法访问及大数据文件传输者进行快速识别，从而有效规避、抵御可疑文件等，不让其进入该

电力的信息与通讯网络，从而达到了安全防范效果。在使用防火墙产品之前，就必须先对防火墙网络进行技术升级创新与功能优化，并根据病毒的不断更新和类型变化，增强防火墙对网络病毒的鉴别能力与识别能力以提升对电力系统运行的安全等级，并改进对电力系统的数据与网络传输和采集能力，以提升网络工作效能和品质。第二，身份验证技术。身份验证技术主要是通过访问人身份的识别、判断、明确，判断访问人对其内部通信网络的使用目的，以便于有效避免非法访问和恶意访问，为提高网络系统安全水平打下了基础。

4.5 提高网络运行管理水平

电电力企业还需要做好对电力系统运营信息通信的网络管理工作。而管理者则需要根据整个电力系统运营的信息使用与操作的特性，来对整个电力系统运营网络的工作进行优化管理，同时更需要形成全面的管理制度。为实现上述目的，就必须专门的管理人员队伍。专门的网络管理队伍，能够将整个电力系统的网络管理工作的强度大大加大。比如当设备下线工作时，就要求专门的技术人员来负责，对工作情况做好了评估和记录，如果是设备出错的信息就可以剔除掉。

安全经理在操作时要操作正确，合理控制电力系统上网，电力系统的网络设备配套应更加完善。我们需要掌握诊断问题的几个关键方面，即要保证电力系统的网络正常工作，也要保证电力系统的控制有效性尽从而减少了员工的操作错误以及网络系统遭受骇客侵入的风险[1]。网络管理部门在处理离线设备的信号时，除了要尽量不出现影响电气的重要信号泄漏的事故，还必须多做好工作人员的安全教育，这样整个电力系统才可以顺利、安全、可靠地正常工作。为了提高电力系统内部信息网络的安全性，一般采用CA（证书授权）或系统身份验证的方式。CA对客户的认证都是通过网络认证签名的，并以此实现了管理认证系统的目的。通过CA身份认证系统能够有效控制非法客户的使用权限，这样就能够防止了重要的信息资料外泄，为电力系统信息通信的安全提供了保证。

4.6 建立完整的电力系统信息通信网络安全运行评估系统

构建完善的电力系统的信息通讯安全管理评价体系，是对电力系统的通信管理能力增强并通过评价结果合理调整动力系统的工作过程、环节、任务。为了建设更加完善的动力系统信息通信网络安全运行评价体系，就需要建设一批专门的动力系统信息通信网络管理队伍。专门的管理队伍可以做好电力公司网络安全防护系统的各项管理，如果发现错误或瑕疵可以及时运用专业知识加以纠正[2]。安全评估系统管理人员在管理工作中更要重视运行规范性，做好电力系统的网络安全配置，将有助于人员正确定位和判断动力系统运行中的问题情况及其发生因素，增强控制有效性。专业人员运行动力系统通信网络安全，也可降低黑客侵入可能性。

结语

总而言之，电力系统网络通信安全直接影响电力企业的正常运转，也直接影响了广大人民的生产生活问题，一旦安全防护出现问题，会造成重大的经济损失，针对这种情况，电力企业需要切实的保障电力系统的安全，有针对性的提出处理预案，完善相关的管理制度，保障电力系统的平稳运行。

参考文献

[1]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.

[2]方婵.电力通信网络管理信息系统的设计与实现[J].电子技术与软件工程，2015（16）：58.

[3]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.

[4]杨林.浅谈电力系统信息通信网络安全及防护[J].电子世界，2018（24）：202.