电力网络终端系统信息安全防护措施探讨

吴雷 国网西藏电力有限公司林芝供电公司 西藏林芝 861000

摘要：电力网络终端数据信息系统对于电力网络的安全防护至关重要。在电力网络终端系统管理过程中，需要依据安全防护的措施管理要求，对入侵的检测机制、网络隔离防火墙、防护联合模版、云端数据系统、防护防范区域等措施进行分析，分析电力网络终端信息系统中可能存在的安全隐患问题，对服务器、网站安全防护等做重点评估，从复杂的方式中理清入侵检测机制，建立电力网络安全隔离防护渠道，实现安全联合防护管理，及时准确的实现对病毒云端的防护与清理。本文将针对电力网络终端系统的安全防护措施进行分析，结合安全隐患因素和问题，提出提升电力网络终端系统信息安全防护的有效措施。

关键词：电力网络；终端系统；安全防护

Discussion on Information Security Protection Measures for Power Network Terminal System

Lei Wu, Linzhi Power Supply Company of State Grid Xizang Electric Power Co., Ltd., Linzhi, Xizang, 861000

Abstract: The terminal data information system of the power network is crucial for the security protection of the power network. In the management process of the power network terminal system, it is necessary to analyze the intrusion detection mechanism, network isolation firewall, protection joint template, cloud data system, protection and prevention area and other measures according to the requirements of security protection measures management. The potential security risks in the power network terminal information system should be analyzed, and the security protection of servers and websites should be evaluated in detail. The intrusion detection mechanism should be clarified from complex ways, and the power network security isolation and protection channel should be established to achieve security joint protection management and timely and accurate protection and cleaning of the virus cloud. This article will analyze the security protection measures for power network terminal systems, and propose effective measures to enhance the information security protection of power network terminal systems based on security risks and issues.

Keywords: power network; Terminal system; safety protection

为了更好的提升我国综合电力系统信息科技水平，采用智能电网终端建设需求不断提升，从网络终端出发，对电力信息系统开展有效的生产、传输、分配等，提高各重要环节的安全稳定运行管理。电力网络终端系统的运行需要大量的电力信息数据，针对网络运营环节，对信息终端的安全范围和薄弱环节进行深入研究，准确的评估电力网络终端的信息安全范围，可能存在的安全隐患，结合电力网络终端信息系统的系统范围，提出符合信息防护安全的措施，将电力防护安全系统的理论与隐患融合起来，提出符合安全防护的有效手段。

1 电力网络终端系统安全防护中存在的隐患

1.1 服务器被侵入

电力网络终端系统中，信息安全防护网络的安全防护不足，与服务网络的数据库在同一安全系统下，缺乏独立的系统认证，服务器安全管理人员的权限划分不明确，电力网络终端的防护会受到一系列的影响。当发生服务器入侵受损的情况，权限划分不当，系统会出现漏洞，导致电力信息系统出现数据遗漏或丢失的情况，这严重的威胁电力信息网络系统的安全稳定运行。

1.2 网络信息安全防护等级不足

电力网络终端系统虽然构建完备的信息安全体系，但随着时间和系统体系的发展，原有的体系安全防护呈现运算速度慢，服务器安全防护存在漏洞的情况，一旦有针对性的进行网络安全信息攻击，就会导致电力数据信息的泄露问题发生。电力网络系统在使用过程中，因为使用时间过长，没有及时进行信息系统更新，浏览网页存在操作不良，录入信息不准确，携带网络病毒的情况，直接影响电力网络终端系统的安全运行。一些电力网络企业为了节省开支，网络终端缺乏定期升级，软件操作使用不当，遗漏数据或携

带病毒数据，会导致电力网络的信息安全受到影响。

电力网络终端系统主要采用 Windouws 系统，在系统安装使用过程中，系统会产生各类安全漏洞，应定期维修防护，如果防护维修不及时，会造成计算机内产生各类安全漏洞，一旦有外部系统入侵，漏洞就成了不法分子获取篡改用户资料的有效手段，会严重侵害用户的个人信息安全，严重的甚至会造成系统瘫痪，导致电力网络大面积失灵问题。因此，在电力网络终端系统中，用户应加强信息安全防护管理，结合电力系统网络的使用规范要求，加强安全防范措施认定，分析系统安全管理的要素和标准，结合信息系统，不断提升信息网络，及时开展信息安全升级防护工作，以保证电力网络终端系统信息的安全防护有效性。

1.3 电力网络终端系统操作不当

电力网络终端信息系统需要定期定时维护管理，且需要由专业的工作人员负责，及时应对电力信息系统安全防护的各类技术问题。这要求电力系统专业工作人员应具有专业的安全防护技术能力，全面的安全系统操作意识，对数据接口进行多层次防护，注意数据信息的应用范围，受限因素，分析数据信息可能泄露的因素，减少电力网络终端系统操作不当的发生，避免电力网络系统出现漏洞，减少电力网络系统出现瘫痪的风险。

2 电力网络终端系统所面临的风险与威胁

随着电力网络终端信息所面临的风险与危险，其中主要包含四个层面的内容。具体来说，有物理层面、网络层面、数据信息层面、技术应用层面。其中物理层面是外部终端设备受到的拆卸、破坏、替换等处理，导致设备受损，信息瘫痪等风险问题。网络层面的危险中包含人为操作攻击、DDOS 联合攻击、协议操作泄露攻击等。这些攻击主要受外部通信传输制约，导致通信信息的中断，数据被篡改，系统控制出现风险，权限被窃取等风险问题。

数据信息层面的风险主要是数据信息内容的泄露、篡改、破坏。黑客通过数据信息端口，对数据信息进行窃取、攻击、重放等操作，获取敏感的数据信息，对电力数据篡改，干扰系统的整体运行效果。技术应用层面中是指恶意的软件滥用，权限滥用，系统漏洞等操作。因系统被破坏，导致异常风险，用户的隐私被泄露，系统受到非法控制等问题。从多层面出发，依据多类型进行安全风险评估分析，对电力网络终端进行系统构建，以实现全方位的系统防护体系建设，保障整个系统的安全稳定运行。

3 电力网络终端信息安全防护措施

3.1 建立入侵检测服务管理机制

随着网络信息发展水平的变化，应不断加强网络信息技术服务管理，建立专项入侵检测服务管理机制。通过电力网络终端的信息安全防护融合，最大程度的

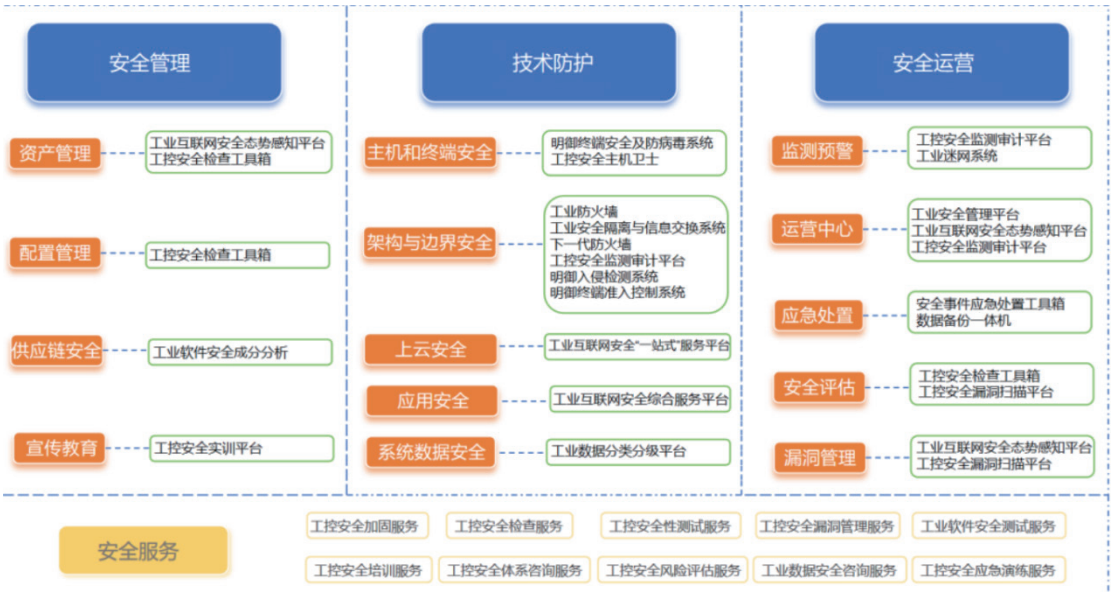

图 电力网络终端信息安全防护图

提升网络病毒防范操作，增强电力体系的智能化管理水平，保障电力系统管理效能的提升。利用高科技网络安全防范措施，快速的搭建网络服务引擎管理体系，提高信息服务网络的保护价值。

在电力网络终端服务系统中，以有效提升电力网络系统为建设发展要求，综合信息服务平台，开展长效的信息优化。根据经济缺损价值差异，对互联网平台下的各类不良网站信息进行处理。通过电力网络终端平台，建立专项防御体系，结合信息文档传递要求，有效的提出防御和攻击方案。电力网络终端系统平台下，结合网络防御技术和硬件维护体系，在保证正常运行的情况下，优化电力网络体系终端水平。按照电力网络终端的可执行要求，参考数据防御库管理方式，开展互联网特定操作，完善电力网络终端体系防护水平，开展专项防御操作，提升电力网络安全计算防护效果。

3.2 建立电力终端安全隔离防火墙平台

电力网络终端体系中，以建立专项的安全防火墙为建设要求，通过网络访问端的评估，及时准确的分析，随时检查分析，评估电力网络整体运行状况，采取必要的记录分析，对可能触发入侵情况进行预警。在电力网络防火墙下，通过区域管理信息化操作，采用正反隔离配置方法，快速的实现内外墙同步防火墙建设，快速的构建安全保障体系，进一步增强网络终端整体的保护水平，减少不必要的病毒入侵发生，及时准确的控制网络信息流量，有效的实现病毒防护，提高黑客攻击配比水平，实现软硬件的同步检测，确保用户信息得到有效安全防护。

3.3 DDOS 联合防护安全操作措施

DDOS 分布式阻断服务是通过网络终端实现的，以增强网络信息系统防御水平为要求，通过终端体系的安全防护操作，依据终端系统和虚拟技术，实现强效的终端强化过程。通过主机安全级别的系统信息分析，制定专项终端安全保护体系，实现虚拟实现和可视化操作。从科学角度进行技术评估，不断提升电力网络终端体系保护水平，解决网络上被攻击的问题。

如果终端攻击超出限定阈值，需尽快进行网络联动操作，建立清洗恢复效果。电力网络终端系统中，通过计算机可使用 DOS 控制，实现高效联动。

3.4 病毒防护清理工作

电力网络终端系统中，通过构建安全防护体系，构建集群部署，达到防止网络风险的目标要求。当发生网络攻击的时候，需做流量牵引操作，准确的识别信息数据，对局域网络进行串联清理，依据电力系统网络带宽范围，调整优化，及时准确的实现云端数据的快速清理工作。我国目前发展电力网络终端系统安全防御防护工作，大力推行一流的网络防护技术防御攻略，防患于未然，重视提升电力网络总体信息安全建设水平，为我国电力网络安全产业的快速发展提供必要的可行方案。

3.5 强化电力网络信息安全操作

为了更好的优化电力网络信息安全水平，需要不断加强网络风险预警功能，从软件、硬件两个方面出发，努力强化电力信息安全管理水平，重视系统的规范性、合理性，对可能存在的电力网络终端信息安全风险进行评估。在电力网络终端信息系统中，应严格规范操作人员的操作行为，杜绝各类不良网络安全操作隐患的发生，从正规的网络方式入手，依据相关数据信息，对计算机网络开展有效的防御和过滤，对可能存在安全风险的网站进行及时处理，关闭可疑不确定的程序，尽可能全面的完善计算机认证系统，做好信息收集，授权认证，做好审计跟踪工作。

3.6 建立完善的信息保密体系

电力网络终端系统信息安全管理过程中，应重视信息的保密和安全。电力网络终端系统通过计算机连接，通过防火墙隔离，从人员和系统上进行双重的安全防护。但在实际操作过程中，不确定因素影响，可能导致人员泄密，系统差错，影响系统访问权限等，导致电力网络终端出现安全风险。为了更好的提高电力网络终端系统信息安全水平，应当从提高电力信息安全出发，结合电力网络终端的信息系统情况，采取必要的措施，尽可能的避免电力网络终端系统信息泄

露，发生风险。电力网络终端系统需要从实际应用和需求出发，结合电力信息开展安全防护管理，拓展电力信息的安全等级，减少涉密信息系统问题发生，提高信息登记、存储管理的规范性，避免风险问题发生和发展，有效的提升电力配套信息安全服务管理水平。

4 案例分析

某电力企业为了有效的提升电力电网智能化水平，全方位的优化智能信息电表终端数据、传感器信息数据，通过网络终端信息方式，以无线网络的方式，与主站系统相互连接起来，提升数据采集范围，实现远程控制管理。电力网络终端系统中，通过数据终端数量的增配，优化信息数据，提高安全水平，降低风险值，有效的稳定电网整体运行水平。

从电力网络终端出发，对电力设备的固件进行漏洞修复，对容易攻击项目进行优化，对密码安全进行升级，处理容易被暴漏破坏的项目。从物理层面进行防护优化，及时处理非法拆卸破坏事项。从物理层面优化防护处理，及时调整非法拆卸破坏事项。

从通信网络安全角度出发，优化无线通信配套范围内的窃听问题，对无线信号干扰因素进行处理，调整加密方案，通过数据信息进行优化，避免出现篡改或伪造问题。按照网络边界范围进行防护，及时处理薄弱容易受外部攻击的范围。按照电力网络终端主线主站进行系统安全风险防控，对系统中的漏洞进行评估，调整访问控制范围，调整安全审计不足事项，及时发现权限访问异常的因素。

通过终端设备的安全防护，定期更新固件，及时修复漏洞，通过定期强化密码的方式，提升密码精度，构建物理防护层面，避免非法操作行为发生。按照通信网络层面的安全防护要求，采用加密信息通信协议，按照网络防火墙、入侵系统进行实时监控，分析网络入网的流量和内容，按照主站体系的评估和渗透测试要求，及时准确的修复信息漏洞，严格做好防护防控网络建设，及时完善角色分配权限管理，做好安全部署审计管理体系建设，准确的记录用户信息操作具体内容，按照日志录入数据信息，保障电网电力的稳定运行操作要求。

为了更好的提升电力网络终端系统安全防护水平，企业从实用角度出发，从风险防护措施入手，综合分析电力行业的智能防护信息安全内容，对电力网络终端进行统筹优化，整体规划，合理推进，适当的选用新技术、新应用、新方法，提升电力信息安全防护水平，不断加强电力网络终端的安全防护意识，构建全面的信息安全防护能力，更好的满足电力网络终端系统信息安全防护，从信息科研角度、安全技术角度、安全管理制度角度综合研究可行的岗位职责，构建全方位的安全防护防线，保障电力电网安全有效稳定运行。

5 结语

综上所述，电力网络终端信息安全防护是一项系统全方位的工作，需要电力企业、政府、科研部门等各方面机构同步沟通，综合认定，明确可实现、可界定的安全防线，综合电力电网终端系统实现信息安全防护措施操作，实现持续性的技术优化，满足不同区域、不同电力设施、不同终端信息措施的防护工作，更好的解决电力网络终端信息操作水平。我国是电力信息资源需求大国，面对广阔的地域电力需求要求，根据不同区域环境条件水平，对电力网络系统开展安全防护措施认定，尽量全面的拓展电力网络终端信息防护体系，结合安全防护措施，提供必要可行的电力网络终端服务信息方案，提升电力网络终端信息安全。

参考文献

[1] 陈栋 . 电力网络终端系统的信息安全防护措施 [J]. 集成电路应用 ,2020,37(12):126 - 127.

[2] 陈健 , 吴浩明 . 电力网络终端系统信息安全防护措施研究 [J]. 数字技术与应用 ,2019,37(10):201 - 202.

[3] 张志华 , 郭晓明 . 智能移动终端在电力网络与信息系统运维中的应用研究 [J]. 数字通信世界 ,2021(07):210 - 211.

作者简介：吴雷（1992 - ）, 男, 西藏山南人, 本科, 助理工程师。研究方向：网络信息安全。