 DOI: https://doi.org/10.12345/dlynyqy.v2i1.16419

Discussion on Network Security Protection Technology in Power System

Quanlin Zhang[1] Jun Xu[2]

1.Guodian Nanjing Automation Co., Ltd., Yancheng, Jiangsu, 210000, China
2.Yancheng Institute of Technology, Yancheng, Jiangsu, 210000, China

Abstract

With the advancement of power system construction, the threat of network security risks faced by the power grid will become more prominent. Based on the current situation of network security in China, this paper introduces the relevant network security technical requirements of the power system in China, analyzes the network security risk threats and technical status problems faced by the current power system, and provides reference for further improving and enhancing the security protection of the power monitoring system in the future. Firstly, in the power system environment, changes in power structure, grid, business models, and technological infrastructure pose potential risks to grid security. Secondly, we propose network security protection requirements for the new power system based on existing network security protection measures, in order to achieve reliable access, intelligent perception, and accurate protection. Finally, research directions and applications in future new power system network security technologies are discussed, including access security, internal security, information security, communication security, security assessment, and simulation checks.

Keywords

power system; network security; protection technology

电力系统网络安全防护技术探讨

张泉林[1] 徐骏[2]

1. 盐城市工学院，中国 · 江苏 盐城 210000
2. 国电南京自动化股份有限公司，中国 · 江苏 盐城 210000

摘 要

随着电力系统建设推进，电网面临的网络安全风险威胁将更加突出，论文以中国的网络安全现状为背景，介绍了中国电力系统相关网络安全技术要求，分析了当前电力系统面临的网络安全风险威胁及技术现状问题，为后续电力监控系统安全防护进一步完善提升提供参考。首先，在电力系统环境中，电力结构、电网、商业模式和技术基础设施的变化对电网安全构成潜在风险。其次，我们结合现有的网络安全保护措施，提出了新电力系统的网络安全防护要求，以实现可靠接入、智能感知和准确保护。最后，对未来新电力系统网络安全技术中的研究并展望研究方向和应用，如访问安全、内部安全、信息安全、通信安全、安全评估和模拟检查。

关键词

电力系统；网络安全；防护技术

1 引言

近年来各国网络安全事件频发，直接与电力相关的有乌克兰大停电、委内瑞拉大停电、南非电力勒索攻击、美国加利福尼亚州和得克萨斯州大规模停电等事件，造成了数亿美元的损失。依据 2021 年公开的高级可持续威胁（Advanced Persistent Threat，APT）研究报告显示，政府、国防军工、科研和能源是主要目标[1]，电力系统日益成为中国和其他国家敌对势力、恐怖分子破坏社会稳定、干扰经济运行、遏制国家发展的重要攻击对象。

论文以中国的网络安全现状为背景，介绍了中国电力监控相关网络安全技术要求，分析了当前电力系统面临的网络安全风险威胁及技术现状问题，为后续电力监控系统安全防护进一步完善提升提供参考。

2 中国主要网络安全技术要求

网络信息安全相关规范标准较多，中国规范主要包括国家安全战略层面法规及发文、国家信息安全技术网络安全等级保护标准、针对行业应用的网络安全标准规范、通用安全技术规范、安全技术管理相关规范以及专业支撑技术规范等。

电力行业相关安全要求主要包括国家发改委关于第 14

【作者简介】张泉林（2005–），男，中国江苏盐城人，本科，从事电力系统及其自动化研究。

号令《电力监控系统安全防护规定》要求发文、国家能源局关于《电力监控系统安全防护总体方案》发文、国标行标关于电力监控系统网络安全防护相关要求，还有国网、南网企标规范要求等。

《电力监控系统网络安全防护导则》明确了建立不断进化发展的网络安全防护体系，包括基础设施安全、体系结构安全、系统本体安全、可信安全免疫、安全应急措施、全面的安全管理等。创建一个包括安全工程、应急措施和综合安全管理的动态三维保护系统框架。建筑安全是能源监控系统网络安全保护系统的基本结构，也是其他所有安全措施的重要依据。电力监控系统结构安全采用“安全分区、网络专用、横向隔离、纵向认证”的基本防护策略。

3 电力监控系统面临网络安全威胁及挑战

3.1 传统网络安全现状

当前电力监控系统面临的主要网络安全威胁包括：黑客入侵、旁路控制、完整性破坏、越权操作、无意或故意行为、拦截篡改、非法用户、信息泄露、网络欺骗、身份伪装、拒绝服务攻击、窃听等。

网络安全攻击对象可以是电力监控系统、调度数据网络、智能终端类设备等，攻击者通过嗅探、渗透、提权等手段对系统内主机、网络和设备进行入侵，待时机成熟后突然发起集团式组合攻击，通过夺取开关操作控制权、瘫痪业务系统、引爆逻辑炸弹、修改保护定值等方法，引发开关跳闸、保护误动或拒动、业务系统崩溃，进而造成一次设备故障、电网震荡，严重时导致整个电网瘫痪，甚至出现大面积停电事故。通过直接攻击调度数据网的网络设备造成个别设备停止服务，甚至可通过路由器自身漏洞渗透修改关键路由器配置引发诸如网络设备频繁中断、全网路由震荡等情况，进而导致调度数据网大面积故障和中断，直接影响电力调度业务的正常开展 [2-3]。

近年来电力行业在逐步推进网络安全管理平台建设。目前监测对象主要是监控主机、网关及网络设备等，未覆盖数量庞大的智能终端设备，因此新形势下电力监控系统仍然存在网络安全风险。

3.2 电力系统面临的网络安全挑战

未来新型电力系统面临的网络安全风险将更加明显，数字化技术的运用赋能新型电力系统实现全面感知与高度智能化运行，强化源、网、荷、储各环节间的灵活协调、互联互通，同时也给新型电力系统带来网络安全风险，对现有技术架构和安全防护体系产生冲击 [4-7]。

①从系统层面看，负载集线器识别的第三方实体正在发展成为互联网上的远程操作。当加载 Hub 平台进入网络攻击时，攻击者可以恶意控制大量可定制负载，造成“大”破坏，引发更大的网络安全事件，引发网络安全。影响电力安全性和网络稳定性。

②终端身份识别认证困难，安全接入难度加大。随着分布式光伏、小型风力发电及其他终端网络连接具有工控终端设备、大存储量、电力系统终端设施的特点，新设计多种多样、体积大、结构复杂、空间分布广泛，网络连接方式多样，信息通信系统多样性增加，终端认证安全性差，难以安全访问，需要提高终端主体的安全性。

4 网络安全防护技术及应用

以下电力监控系统网络安全防护按照边界防护技术、设备本体防护技术、网络安全监测技术及网络安全管理几个方面介绍 [8-12]。

4.1 边界安全防护技术

电力监控系统在体系结构上采用“安全分区、网络专用、横向隔离、纵向认证”的防护策略。在边界防护方面，充分识别二次系统的生产控制、信息管理、运维调试、各类设备接入等运行中的结构性边界，针对不同边界应用场景设计配置相应的安全策略方案，保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。

4.2 本体安全防护技术

本体安全是指电力监控系统各个组成部分的自身安全，包括计算机主机、服务器、网络设备以及继电保护测控设备等智能电子设备安全。相关安全要求主要包括身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护及个人信息保护等。电力监控系统各个组成部分应采用自主可控、安全可靠的软硬件产品。

具体安全技术方案措施有身份验证和授权技术、过滤阻塞访问控制技术、加密技术和数据验证、可信计算技术以及其他安全管理、审核、测量、监控和检测工具等。

其中身份验证和授权是保护系统及其关键资产免受意外破坏的第一步。这是一个确定应该允许谁和何时进入或离开系统的过程。一旦确定该信息，可实施纵深防御访问控制措施，以验证只有授权人员和设备才能实际访问系统。该项措施通常是对试图访问系统的人员或设备进行身份验证。具体技术有基于角色的授权、密码鉴别、挑战应答鉴别、物理令牌鉴别、智能卡鉴别、生物鉴别、基于位置鉴别、密码分配和管理技术、设备到设备的鉴别等。

过滤阻塞访问控制技术是一种过滤和阻止技术，设计用于在确定授权后引导和调节设备或系统之间的信息流。防火墙是这种技术最常用的形式，具体技术有网络防火墙、基于主机防火墙、虚拟网络（VLAN）、加密技术和数据确认等。

加密技术和数据验证技术中，加密是对数据进行编码和解码的过程，以确保信息仅可供有权访问的人访问。数据验证技术保障了工业过程中使用的信息的准确性和完整性。具体包括对称密钥加密、公钥加密和密钥分配、虚拟专用网（VPN）等。对称密钥加密通过加密可提供数据的保密性、

消息完整性，其风险在于鉴别和密钥的分发管理是否安全。

以加密硬件为核心的可靠计算技术用于在计算机和网络环境中实现安全免疫，免疫未知恶意代码，防止有组织的高级恶意攻击。安全免疫的相关要求主要适用于新建或新开发的重要电力监控系统，在运行系统具备升级改造条件时可参照执行，不具备升级改造条件的应强化安全管理和安全应急措施。

针对智能电网面临的日益严峻的网络安全威胁，围绕风险、资产、业务应用等对象，构建完善智能电网电力监控系统网络安全态势感知系统，从安全日志、终端行为、网络流量、业务数据等多方面入手，进行相关数据的全面收集，通过网络安全态势要素提取、网络安全态势理解、态势风险评估、判断风险等级、态势可视化展现、安全态势预测预警等技术手段，实现了对各类安全风险的实时监测能力，提升对网络安全态势的推理性判断和知识性把控能力，从而实现从传统的被动、静态的网络安全到主动、动态网络安全的转变。

5 展望与总结

新型电力系统建设催生大量新业态发展和新技术应用，电力监控系统网络安全涉及“发电、输电、变电、配电、用电、调度”各个环节，在新型电力系统的发展背景下，网络安全防护体系需要不断完善，适应环境变化，保障系统安全可靠稳定运行。具体包括以下方面：

①继续完善电力监控系统网络安全防护体系，分布式接入需要协同开展适用于新型电力系统的网络安全防护体系架构设计和关键技术攻关，研究探索分布式新能源、分布式储能、新型负荷控制等新业务场景的网络安全防护方案，保障结构性大局安全。

②继续提升系统及设备本体安全，推进可信计算技术的应用实施，包括主机系统、网关及智能终端设备的可信免疫深化实施以及终端设备对网络安全监测的功能支持等。

③继续网络安全技术及应用研究，安全监测技术对于网络安全态势感知的研究和时间还处于初级阶段，结合 AI 技术的发展及应用，许多关键问题还有待进一步研究解决，尤其是关于态势理解、态势认知相关的算法还有待深入研究。

参考文献

[1] 2021年上半年全球高级持续性威胁(APT)研究报告[R].

[2] 张涛,赵东艳,薛峰,等.电力系统智能终端信息安全防护技术研究框架[J].电力系统自动化,2019,43(19):1-8+67.

[3] 陈铁铮.电力监控系统网络安全防护现状及建议[J].通信电源技术,2020,37(4):109-110.

[4] 周孝信,陈树勇,鲁宗相,等.能源转型中我国新一代电力系统的技术特征[J].中国电机工程学报,2018,38(7):1893-1904.

[5] 吴克河,王继业,李为,等.面向能源互联网的新一代电力系统运行模式研究[J].中国电机工程学报,2019,39(4):966-978.

[6] 梅文明,李美成,孙炜,等.一种面向分布式新能源网络的终端安全接入技术[J].电网技术,2020,44(3):953-961.

[7] 谢林江,毛正雄,罗震宇.数字化转型中新型电力系统典型信息安全威胁及对策分析[J].新型工业化,2022,12(3):191-193.

[8] 王宇飞,李俊娥,刘艳丽,等.容忍阶段性故障的协同网络攻击引发电网级联故障预警方法[J].电力系统自动化,2021,45(3):24-32.

[9] 俞华,穆广祺,牛津文,等.智能变电站网络安全防护应用研究[J].电力系统保护与控制,2021,49(1):115-124.

[10] 高昆仑,王志皓,安宁钰,等.基于可信计算技术构建电力监测控制系统网络安全免疫系统[J].工程科学与技术,2017,49(2):28-35.

[11] 张亮,屈刚,李慧星,等.智能电网电力监控系统网络安全态势感知平台关键技术研究及应用[J].上海交通大学学报,2021,55(S2):103-109.

[12] 向城成,吴春江,刘启和,等.网络安全态势预测技术研究综述[J].计算机应用与软件,2023,40(5):19-28+36.