风电场电力监控系统网络安全威胁防控体系

丁伟
（南方电网数字电网研究院有限公司，广州 广东 510663）

摘　要：风电场电力监控系统网络安全事件的频发，严重威胁电厂和电网的安全。从结构安全、系统本体、安全管理、安全应急和基础设施物理安全 5 个角度深入分析了风电场电力监控系统网络安全风险。针对现有安全防护现状，从安全防护、安全监测、接入管控和安全管理 4 个方面提出一套安全威胁防控体系，以确保场网两侧电力监控系统的安全稳定运行。

关键词：风电场；电力监控系统；安全风险；安全监测；接入管控
中图分类号：TM734
文献标识码：A
doi: 10.11959/j.issn.1000−0801.2020018

Network security threat prevention and control system of electric power monitoring systems for wind farm

DING Wei
Digital Grid Research Institute, China Southern Power Grid, Guangzhou 510663, China

Abstract: The frequent occurrence of network security incidents on wind farms seriously threatens the safety of power plants and power grids. The network security risk of power monitoring system on wind farms was analyzed from five aspects, including structure security, system ontology, security management, security emergency and infrastructure physical security. In view of the existing security protection technology, a security threat prevention and control system was put forward to ensure the safe and stable operation of the power monitoring system of wind farms and power grid from four aspects of security protection, security monitoring, access control and security management.

Key words: wind farm, power monitoring system, security risk, security monitoring, access control

1　引言

针对我国能源资源约束日益加剧、生态环境问题日益突出等现状，新能源风电迎来了前所未有的发展契机，风电场的规模和数量都在急剧增加。电力监控系统支撑着风电场的安全稳定运行，一旦遭到破坏或恶意控制，不仅会影响电场侧安全，甚至会影响到电网侧的安全。伊朗“震网病毒”、乌克兰大停电等工业控制行业网络安全事件都为人们敲响了警钟[1-2]。我国有关部门、电力行业和电力企业对电力系统安全防护高度重视，相继出台了《电力监控系统安全防护规定》《电力监控系统安全防护总体方案》等有关配套文件。新能源电站的接入，扩展了调度数据网

收稿日期：2019−12−18；修回日期：2020−01−01

安全防护的边界，而整个系统的整体安全性，往往取决于系统中的短板长度。新能源风电的安全防护工作由于各种原因，其整体安防工作强度要低于调度侧和传统电厂[3-4]。远程运维、跨网互联、违规使用无线等问题在风电场屡见不鲜，风电场电力监控系统面临严重的网络安全威胁。

为了有效提升风电场电力监控系统网络安全水平，防止并网电厂的网络安全威胁通过调度数据网向电网侧蔓延，确保厂网两侧电力监控系统的安全可靠运行，有必要开展风电场接入调度数据网网络安全风险分析和安全威胁管控体系研究，对保障风电场和电网的安全稳定运行具有重要作用，并将对涉网发电企业规划、设计、建设及运维等工作具有指导意义。

2　风电场电力监控系统概述

风电场电力监控系统主要用于监控风电场生产控制大区和信息管理大区各系统和装置稳定运行，确保发电、变电、输电等环节正常运转，从而向电网输送稳定的电力能源。风电场在整体安全防护上遵循“安全分区、网络专用、横向隔离、纵向认证”原则，同时按照国家等级保护的相关要求对电力监控系统从主机、网络、应用、数据、物理及安全等多个层面进行安全防护。

风电场电力监控系统结构如图 1 所示，在安全分区方面，控制区主要包括风机监控系统、升压站监视系统、无功电压控制（AVC）、有功功率控制系统（AGC）、相量测量装置（PMU）、继电保护等。非控制区主要包括风功率预测系统、电能量采

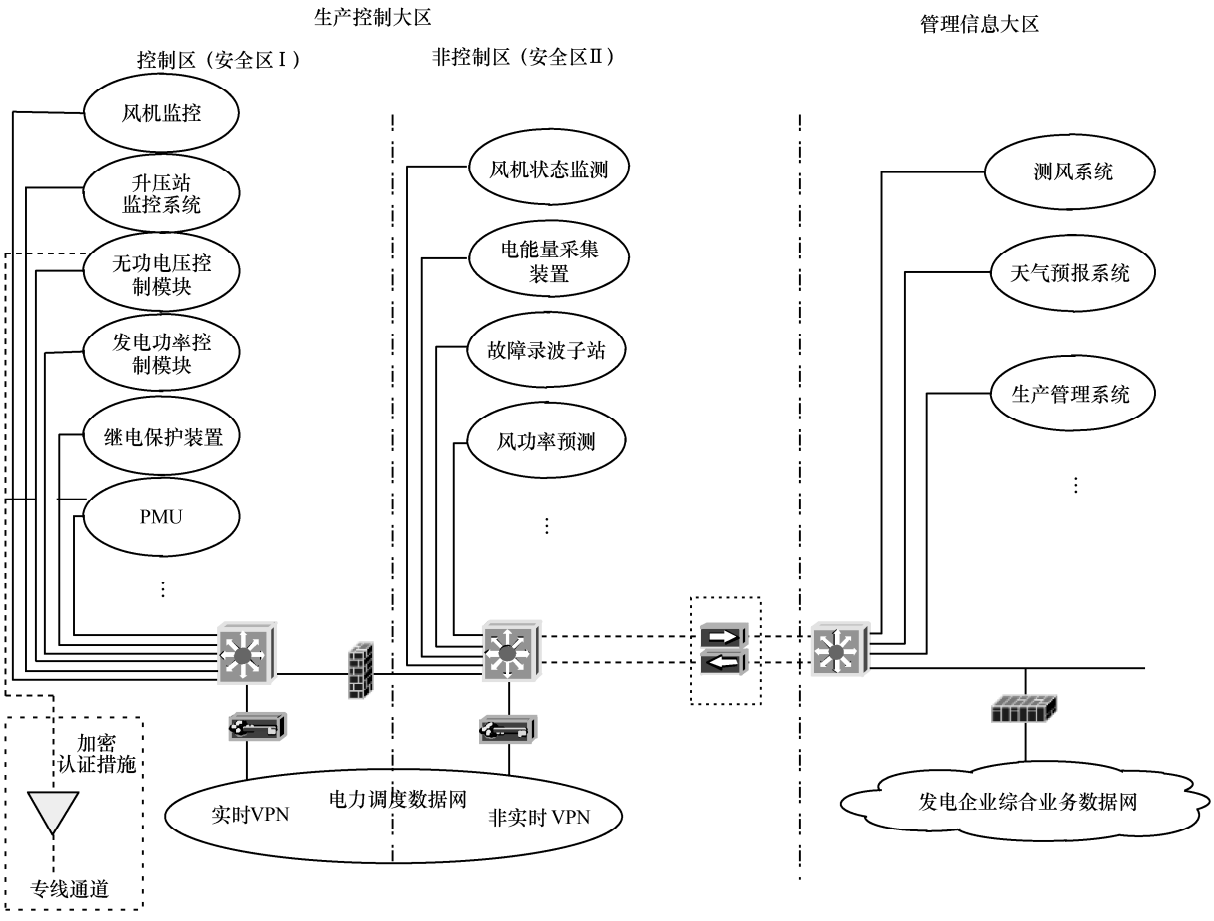

图 1　风电场电力监控系统结构

集装置和故障录波装置等。管理信息大区主要包括天气预报系统、测风系统和办公信息系统等。

在通信通道方面，升压站监视系统、无功电压控制、有功功率控制系统采用双通道与上级调度机构相连，一般为电力调度数据网和专线（2 Mbit/s专线或模拟 4 线）。相量测量装、继电保护、风功率预测系统、电能量采集装置和故障录波采用单通道与调度机构相连，多为调度数据网。风电场内其他业务系统不与调度机构直接通信。

3 网络安全风险分析

根据对目前风电场电力监控系统安全防护现状、日常督查检查和发生的相关异常事件的分析，对风电场电力监控系统网络安全的主要风险总结如下。

结构安全方面，风电场电力监控系统网络存在跨区互联、非法接入等问题，导致电力监控系统被黑客入侵，致使系统失灵、系统被恶意控制或网络瘫痪，进而引发电力事故[5]。具体包括：生产控制大区设备或业务系统违规采用第三方运维软件，直接与互联网连接进行远程维护或升级；测风塔无线传输至气象采集服务器时未设置安全接入区；风电场与远程集控中心采用非电力专用网络且未采用加密认证措施；边界安全防护设备（如横向隔离装置、纵向加密认证装置、横向/纵向防火墙等）未配置安全策略或安全策略过宽。

系统本体方面，风电场电力监控系统主要存在以下安全风险：服务器、主机等基础软硬件安防措施执行不到位，存在移动介质非法接入，防病毒手段缺失，安全策略配置不当，操作系统存在高危漏洞、弱口令等问题，使得系统被非法入侵或被病毒感染，致使系统失灵或被恶意控制，导致电力监控技术手段失效，进而引发电力事故；应用系统安全防护功能或配置不足，存在源代码预置漏洞或恶意代码、认证强度不足、数据明文传输等问题[6-7]，导致系统被入侵或核心生产数据泄露，致使系统被恶意控制或下发大量恶意控制命令，进而引发电力事故。

安全管理方面，主要存在以下安全风险：风电场电力监控系统安全防护组织机构未建设完善，网络安全专业人员数量不足且技能普遍欠缺，安全防护资金落实不到位，从而造成电力监控系统网络安全工作无法得到有效落实；管理制度、管理措施及要求落实不到位，导致安全防护措施失效，从而引发电力监控系统网络安全事件。

安全应急方面，主要存在以下安全风险：安全应急预案不完善、应急演练缺乏，导致一旦面临真实网络安全入侵攻击，难以形成有效应对，导致网络安全事件后果放大；安全态势感知及监测预警能力不足，缺乏全面、有效的安全监测技术措施与手段[8-10]，导致无法及时发现网络安全威胁，采取应急处置措施，导致电力监控系统被入侵后，进行大范围攻击扩散与深度破坏，引发电力事故。

基础设施物理安全方面，风电场物理安全防护普遍薄弱，机房环境及物理安全防护措施落实不到位。主要包括：存在电子门禁缺失、人员出入管控不严格、未部署视频监控系统等问题，当非法人员潜入机房采取物理手段进行数据窃取或者破坏系统设备时，无法及时发现；机房未部署温/湿度监控系统、防渗水检测报警装置等，当发生空调停机导致温度异常，下雨导致漏水等情况时无法及时发现，造成机房硬件设备物理损坏。

4 风电场网络安全威胁防控方案

在深入分析风电场典型网络安全事件、调研风电场电力监控系统的相关安全技术的基础上，本文从安全防护、安全监测、接入管控、安全管理 4 个方面归纳总结了针对风电场电力监控系统的安全威胁防控方案，其中安全防护和安全监测从电厂提高自身安全防护水平出发，接入管控和安全管理从调度机构技术监督职责角度出发。

4.1　安全防护

从主机、网络和应用 3 个方面进一步提升风电场电力监控系统的安全防护能力，从而抵御各种网络攻击和恶意代码感染。

（1）主机防护

生产控制大区各业务系统服务器、工作站的操作系统皆应采取恶意代码防护措施，并定期进行病毒库的更新。同时应经过安全加固，对于电力监控系统中的关键服务器进行软件升级、补丁安装前进行安全评估和测试验证。建立移动存储介质管控平台，对移动存储介质进行有效管理，防止通过移动存储介质传播病毒、木马、僵尸程序等恶意代码。

（2）网络防护

风电场应严格按照国家规定落实“安全分区、网络专用、横向隔离、纵向认证”的 16 字方针，其中生产控制大区测风塔若使用无线通信则必须设置安全接入区。租用运营商专线与集团远程集控中心通信应落实纵向加密认证措施。在生产控制大区内部署入侵检测系统和运维审计系统，及时捕获网络异常行为和分析潜在威胁，对操作行为进行安全审计以便事后追踪溯源。

（3）应用防护

新建或改建业务应用系统应落实安全标签和双因子认证等技术措施，逐步完善业务系统的身份认证、安全审计、访问控制等模块。开展电力监控系统源代码审计研究，系统上线前对应用系统源代码预置漏洞或恶意代码进行检测。在运系统的口令管理、权限管理、审计管理上严格按照电力行业和企业相关要求执行，降低在运系统安全风险。

4.2　安全监测

建立对风电场电力监控系统外网互联、网络

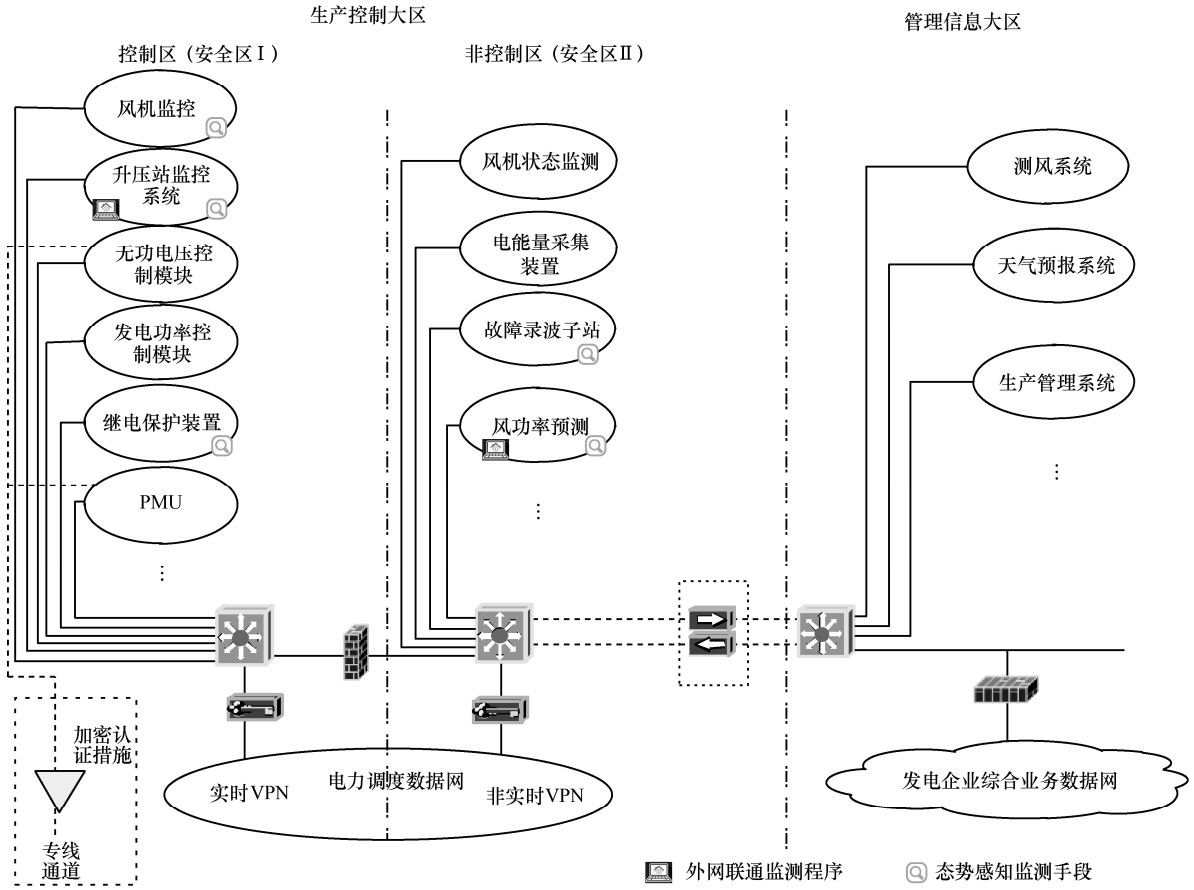

图 2　风电场电力监控系统安全监测体系

流量、设备运行状态等多层次的综合监测，如图 2 所示，全面掌握风电场电力监控系统的安全状况，同时将相关监测数据上传至调度机构。

（1）外网互联监测

在电场内生产控制大区易发生跨区互联的业务系统（如风功率预测系统、升压站监控系统）部署外网互联监测程序，周期性测试外网联通情况，从而实现对网络边界非法访问、跨区互联等违规情况的监测，提升全面提升网络安全预警处置的能力。

（2）网络流量监测

有效的网络流量监控不仅能够让网络管理人员及时了解网络的运行状态，并且能够对网络出现的问题做出及时调整和排除[11]。网络流量监测包括流量采集、流量分析、流量控制 3 个环节。通过对生产控制大区内网络流量进行实时监测，对异常 IP 地址、异常通信等情况进行识别、报警和分析，从而发现非法外联、异常网络应用和通信行为。

（3）设备监测

对风电场内生产控制大区网络设备（交换机、路由器）、安防设备（纵向加密认证装置、横向隔离装置、防火墙）及主机类设备（服务器、工作站、远动机、保信、测控装置）的运行日志及操作情况进行集中监控及审计分析[12-14]，具体包括运行状态信息、配置信息、配置流量传输信息及安全告警信息，从而判断系统是否存在故障或异常。

4.3 接入管控

为了避免电厂侧的网络安全风险向调度侧蔓延，在调度侧采取接入管控措施，具体方案如图 3 所示。将调度数据网实时 VPN 和非实时 VPN 都分别划出独立的电厂 VPN，并实施点对点的路由控制。电厂数据通过纵向加密装置接入调度主站独立的电厂前置机，电厂前置机再通过防火墙与内部系统进行互联通信。通过在调度侧实行接入管控，划分独立的电厂 VPN，可以有效地抵御电厂侧的网络安全风险通过调度数据网向调度侧蔓延。

4.4 安全管理

新建、改/扩建电厂，严格落实涉网电力监控

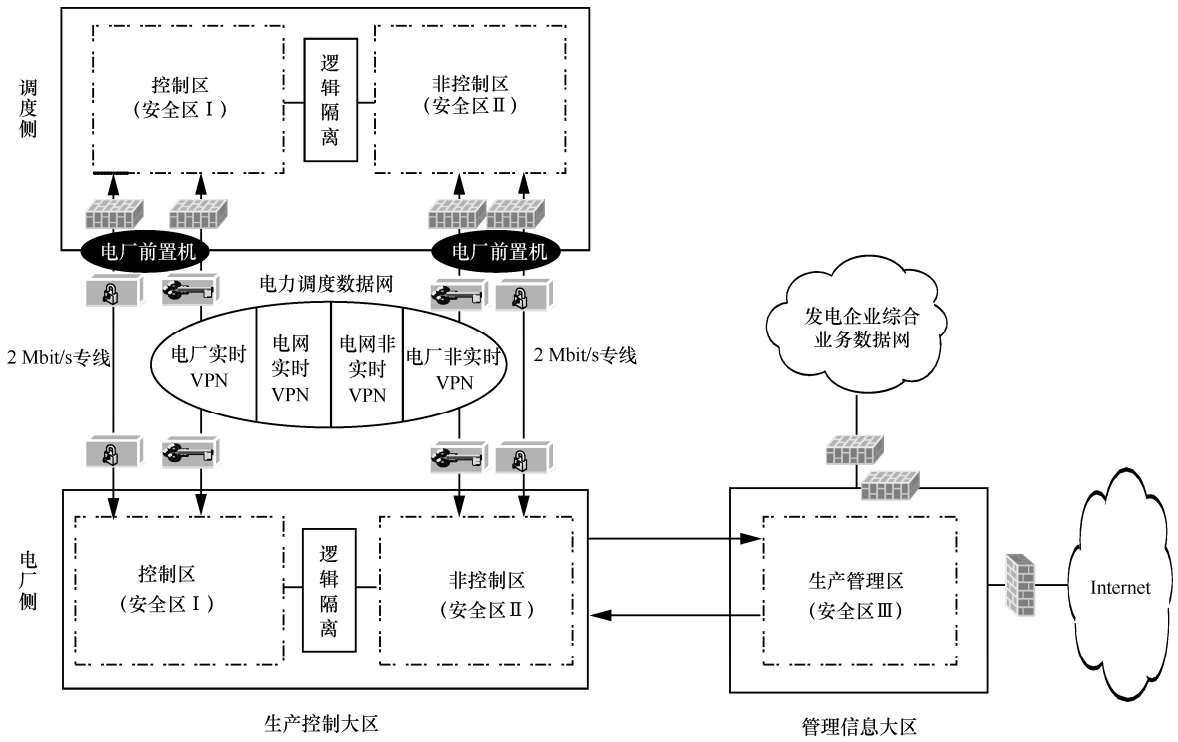

图 3 风电厂改进接入管控方案

系统网络安全实施方案的审查及并网验收工作，在电力监控系统新建或重大改造后开展投运前的网络安全等级保护测评和电力监控系统安全防护评估工作。对于已投运电厂，按流程严格管控涉网电力监控系统网络安全结构、安全策略变更，防范未经调度机构批准的涉网电力监控系统网络结构或安全策略变更，变更后的网络结构和安全策略应及时完成在对应调度机构的备案。健全厂网联动的网络安全事件应急处置机制，督促并网发电企业动态修编应急预案，定期开展应急演练，不断提高应急预案的可操作性、针对性和实效性[15]。各级调控机构要建立网络安全告警事件数量、告警事件处置及时率、安防设备在线率、纵向数据通信密通率等关键指标的统计分析手段，定期通报各电厂关键指标数据[16]，指导并网电厂开展网络安全运行提升工作。

5　结束语

风电场接入调度数据网，要将系统的安全防护工作同系统建设同步规划、同步设计、同步实施，要和相关调度数据网自动化系统安全防护建设同步推进，同时提升相关人员网络安全意识，才能不断提升整体防护水平。本文基于实际情况探讨了风电场电力监控系统所面临的安全风险，从安全监测、安全防护、接入管控和安全管理 4 个方面归纳总结了风电场电力监控系统安全防护体系，并深入分析了未来全面提升电力监控系统安全性的关键技术，以提升风电场电力监控系统安全防护水平，确保厂网两侧的安全稳定运行。

参考文献：

[1] 吴克河, 刘吉臻, 张彤, 等. 电力信息系统安全防御体系及关键技术[M]. 北京: 科学出版社, 2011.
WU K H, LIU J Z, ZHANG T, et al. Power information system security defense system and key technology[M]. Beijing: Science Press, 2011.

[2] 高昆仑, 辛耀中, 李钊, 等. 智能电网调度控制系统安全防护技术及发展[J]. 电力系统自动化, 2015, 39(1): 48-52.
GAO K L, XIN Y Z, LI Z, et al. Development and process of cyber security protection architecture for smart grid dispatching and control systems[J]. Automation of Electric Power Systems, 2015, 39(1): 48-52.

[3] 倪明, 颜洁, 柏瑞, 等. 电力系统防恶意信息攻击的思考[J]. 电力系统自动化, 2016, 40(5): 148-151.
NI M, YAN J, BO R, et al. Power system cyber attack and its defense[J]. Automation of Electric Power Systems, 2016, 40(5): 148-151.

[4] 朱世顺, 黄益彬, 朱应飞, 等. 工业控制系统信息安全防护关键技术研究[J]. 电力信息与通信技术, 2013, 11(11): 106-109.
ZHU S S, HUANG Y B, ZHU Y F, et al. Research on key technologies of information security protection for industrial control systems[J]. Electric Power Information and Communication Technology, 2013, 11(11): 106-109.

[5] 韩江洪, 刘征宇, 刘晓平, 等. 工业控制安全研究综述[J]. 合肥工业大学学报(自然科学版), 2010, 33(2): 161–168, 173.
HAN J H, LIU Z Y, LIU X P, et al. Survey of industrial control safety[J]. Journal of Hefei University of Technology, 2010, 33(2): 161-168, 173.

[6] 张盛杰, 顾昊旻, 李祉岐, 等. 电力工业控制系统信息安全风险分析与应对方案[J]. 电力信息与通信技术, 2017, 15(4): 96-102.
ZHANG S J, GU H M, LI Z Q, et al. The information security risk analysis and response plans in power industry control system[J]. Electric Power Information and Communication Technology, 2017, 15(4): 96-102.

[7] 刘念, 张建华, 段斌, 等. 网络环境下变电站自动化通信系统脆弱性评估[J]. 电力系统自动化, 2008, 32(8): 28-33.
LIU N, ZHANG J H, DUAN B, et al. Vulnerability assessment for communication system of network-based substation automation system[J]. Automation of Electric Power Systems, 2008, 32(8): 28-33.

[8] 杨安, 孙利民, 王小山, 等. 工业控制系统入侵检测技术综述[J].计算机研究与发展, 2016, 53(9): 2039-2054.
YANG A, SUN L M, WANG X S, et al. Intrusion detection techniques for industrial control systems[J]. Journal of Computer Research and Development, 2016, 53(9): 2039-2054.

[9] 刘涛. 工控网络协议转换网关关键技术的研究[D]. 大连: 大连理工大学, 2007.
LIU T. Study on the key technology of industrial control network protocol transformation gateway[D]. Dalian: Dalian University of Technology, 2007.

[10] 张淑英. 网络安全事件关联分析与态势评测技术研究[D]. 长春: 吉林大学, 2012.
ZHANG S Y. Research on network security incident correlation analysis and situation evaluation technology [D]. Changchun:

Jilin University, 2012.

[11] 徐诚, 梁睿, 程真何, 等. 面向能源互联网的智能配电网安全态势感知[J]. 电力自动化设备, 2016, 36(6): 13-18.
XU C, LIANG R, CHENG Z H, et al. Security situation awareness of smart distribution grid for future energy internet [J]. Electric Power Automation Equipment, 2016, 36(6): 13-18.

[12] 李刚, 唐正鑫, 李纪锋, 等. 智能电网安全态势感知与组合预测[J]. 电力信息与通信技术, 2016, 14(11): 1-7.
LI G, TANG Z X, LI J F, et al. Security situation awareness and combination forecasting in smart grid[J]. Electric Power ICT, 2016, 14(11): 1-7.

[13] 管小娟, 张涛, 马媛媛, 等. 网络安全态势感知研究综述[J]. 电力信息与通信技术, 2014, 12(5): 1-4.
GUANG X J, ZHANG T, MA Y Y, et al. A survey of network security situation awareness [J]. Electric Power ICT, 2014, 12(5): 1-4.

[14] 郭静, 黄伟, 郭雅娟, 等. 智能变电站网络安全态势感知技术[J]. 电信科学, 2015, 31(Z1): 202-208.
GUO J, HUANG W, GUO Y J, et al. Network security situation awareness technology in smart substation[J]. Telecommunications Science, 2015, 31(Z1): 202-208.

[15] 李中伟, 佟为明, 金显吉. 智能电网信息安全防御体系与信息安全测试系统构建[J]. 电力系统自动化, 2016, 40(8): 147-151.
LI Z W, TONG W M, JIN X J. Design and application of integrated energy management system in active distribution network[J]. Automation of Electric Power Systems, 2016, 40(8): 147-151.

[16] 欧阳文华, 杨浩, 林楠, 等. 新能源电站接入调度数据网风险分析及防护研究[J]. 江西电力, 2017, 41(10): 5-7.
OUYANG W H, YANG H, LIN N, et al. Risk analysis and protection research of new energy power station dispatching data network[J]. Jiangxi Electric Power, 2017, 41(10): 5-7.

[作者简介]

丁伟（1991– ），男，南方电网数字电网研究院有限公司工程师，主要研究方向为电力监控系统安全防护。