DOI:10. 3969/j. issn. 1674-1951. 2021. 02. 010

# 数字新基建下的电力网络安全防护体系研究

Research on power network security protection system in digital new infrastructure construction

刘超[1],张鹏[2*],强仁[2],赵毓鹏[3],鞠伟[3],夏永欣[3],袁琳琳[2]
LIU Chao[1],ZHANG Peng[2*],QIANG Ren[2],ZHAO Yupeng[3],JU Wei[3],XIA Yongxin[3],YUAN Linlin[2]

(1.国家电网有限公司,北京 100031;2.北京市能源电力信息安全工程技术研究中心(华北电力大学),北京 102206;3.国家电网信息通信产业集团有限公司,北京 102209)

(1.State Grid Corporation of China,Beijing 100031,China;2.Beijing Engineering Research Center of Energy Electric Power Information Security(North China Electric Power University),Beijing 102206,China;3.State Grid Information and Communication Industry Group Limited company,Beijing 102209,China)

**摘 要**:"数字新基建"已成为新一代国家基础设施建设的重要议题,作为驱动新型产业发展以及现代生产力进步的重要引擎,其深入的网络交互性、高度的数字融合性以及信息耦合性与网络安全事件紧密相关。分析了"数字新基建"下电力网络安全发展态势,建立了面向网络安全等级保护2.0下全业务新形态网络安全监管要求的电力网络安全防护体系;论述了新基建下电力网络安全发展面临的新机遇与新挑战,并提出了网络安全发展管理的全生命周期模型;构建了健康有效的电力网络安全防护监管模型,从而使电力网络在"数字新基建"背景下能够安全有效运行。

**关键词**:数字新基建;网络安全;网络安全等级保护2.0;全生命周期;安全监管

**中图分类号**:TM 732 **文献标志码**:A **文章编号**:1674-1951(2021)02 - 0060 - 06

**Abstract**: Digitalization has become an important issue in new infrastructure construction of China. As an important propeller for developing new industries and advancing modern productivity, the construction closely connects deepening network interactivity, digital integration and information coupling to network security incidents. At the beginning, the development trend of power network security in digital new infrastructure construction was analyzed. And a power network security protection system was proposed complying with the requirements made by new-form cybersecurity protection for all services under"classified protection of cybersecurity 2.0". Then, by expounding opportunities and challenges faced by the power network security in the new infrastructure construction, a full life cycle model for network development and management was set up. Finally, a healthy and effective power network security protection and supervision model was constructed to secure a safe and operative power network in digital new infrastructure.

**Keywords**: digital new infrastructure; cybersecurity; classified protection of cybersecurity 2.0; full life cycle; security protection and supervision

## 0 引言

2020年,新型基础设施建设于全国"两会"上被首次写入政府工作报告,这将新型基础设施的建设提升到了一个前所未有的新高度[1],政府谋篇布局,相关企业单位以国家政策为向导,大力开展以5G、数据中心、人工智能、云计算、物联网等新一代技术为代表的数字化基础设施建设,这类新型基础设施的蓬勃发展极大地推动了数字经济在我国的繁荣兴盛[2]。与此同时,国家电网有限公司(以下简称国网公司)为了能同国家一起快速推进部署"新基建"的重要举措,并加快当前向数字化产业转型也开展了相应的实际行动,即发布了有关"数字新基建"的重点建设任务[3],这不仅体现了国网公司的使命担当,也践行了共建共享共赢的发展理念。

随着国网公司对数字化新基建的推动与建设,电力物理空间与网络空间的连通、融合将进一步加

**收稿日期**:2020-08-27;**修回日期**:2021-02-04
**基金项目**:国家电网有限公司科技项目(SGZB0000AZWT2000585)

深，数字新基建下电力系统针对网络安全的依赖性也逐渐增强。网络安全不再仅仅影响虚拟空间，将会通过电力信息物理耦合关系渗透到现实电力一次系统，严重影响电力一次系统的安全、稳定、高效运行，网络安全事件一旦发生，将极大地危害国家安全与社会稳定，很大程度地影响人民的美好生活[4]。

为了应对一系列电力网络安全问题，早在2018年9月国家能源局发布了《关于加强电力行业网络安全工作的指导意见》，全面贯彻落实党中央有关网络安全工作决策部署，以提升电力行业网络安全防护能力、健全电力网络安全防御体系、防范遏制电力网络安全事件为主要目标，确保电力系统安全、稳定运行以及电力可靠供应[5]。国网公司作为“数字新基建”重点支撑企业，全面落实保障电力网络安全工作，坚持“安全第一、预防为主”方针[6]，树牢安全生产理念；优化安全生产责任制，深化安全责任机制落实；持续跟进国家网络安全法律法规要求，牢筑电力网络安全防线；大力开展全员电力网络安全教育，强化安全教育培训体系。国网公司发挥其专业能力，强化网络安全防护、加强网络安全运营管理，以其成熟的电力网络安全防护管理能力，保证电力系统健康稳定运行。

网络安全是“数字新基建”最重要的基石，电力行业在开展每一种数字化基建时，都应考虑到网络安全态势如何发展、网络安全防护体系如何构建、网络安全监管机制如何落实。基于此，数字新基建的发展建设将愈加平稳，数字化产业经济才能高速、健康发展。

## 1　网络安全态势发展趋势

信息化发展伴随着网络安全问题，是为一体两翼、两轮驱动的关系。作为新型基础设施的核心要素，网络和数据从侧面也反映了新基建的本质——数字化、经济化的基础设施建设。与此同时，国家发展和改革委员会明确表示，新基建的基础设施应该包含3个重要方面，具体为信息基础设施、融合基础设施以及创新基础设施。新建基础设施应贯彻国家总体安全观，以服务于数字经济为宗旨，为网络安全保驾护航，为数据安全遮风挡雨，为数字经济发展注入动力。“数字新基建”基本框架结构如图1所示。

在产业数字化、数字产业化过程中，网络化可能带来一系列网络安全问题，而数字化则可能带来一系列数据安全问题。在数字经济发展过程中对于关键生产要素的保护、网络安全及数据安全是一个值得关注的重要问题。数据已经成为支撑国家和全球经济增长的重要动力，数据产业已成为重要的生产要素和战略资源[7]。数据作为核心资产的价值创造者与经济社会的发展已逐步密不可分。鉴于此，我国信息安全基础技术研究与开发能力尚有待提高，关键信息基础设施的安全保障亟待进一步加强，防范数据安全风险的措施则更需不断稳固。

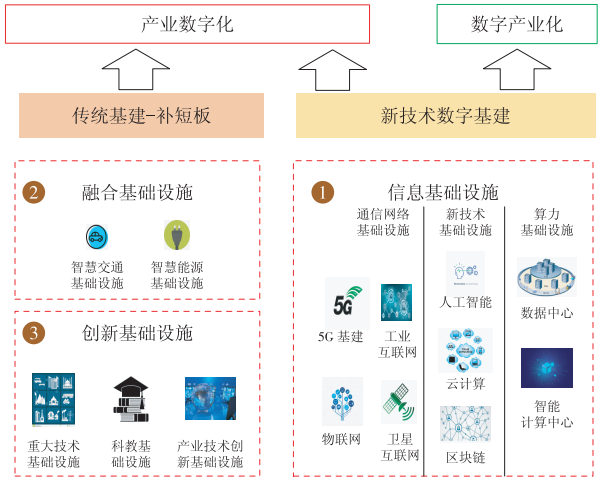


**图1　数字新基建框架结构**

**Fig. 1　Digital new infrastructure framework**

当下，新型基础设施建设对网络、数据等问题提出了新的安全挑战。为保证数字经济可以持续平稳增长且健康快速发展，应着力加强新型信息基础设施在建设推进过程中的质量保障[8]。新一代信息基础设施需通过利用网络和数据为前提进行规划、开发与建设，由此进一步加强科学研判，系统规划，形成技术创新、产业发展、安全保障的良性生态环境，在信息化发展的过程中，让人们有更多的获得感、幸福感、安全感。

## 2　电力网络安全防护体系

面对“互联网+”与智慧能源、能源互联网、智能电网、智能发电、智能电站等新型能源开发模式，以及工业互联网、云计算、大数据、物联网、区块链、人工智能等新技术在电力能源领域的广泛应用，能源电力系统必须遵循《网络安全等级保护2.0》[9]（以下简称等保2.0）下“明确等级、增强保护、常态监督”的网络安全新要求，既要严格遵循“网络专用、安全分区、横向隔离、纵向认证”这16字的基本安全方针[10]，又要与时俱进，积极顺应“可管可控、精准防护、可视可信、智能防御”的网络安全目标，建立全业务系统的网络安全监督管理体系，新形势下基于等保2.0的电力网络安全防护模型如图2所示。

电力系统运行过程中，对于网络的依赖性十分强烈，电力系统网络存在安全隐患会对电力系统的

正常运行带来威胁，因此，网络安全的防护尤为重要。需要全面深化对网络安全的全生命管控、网络安全审查以及内控治理，强化电力网络安全防护可管可控方针。

在体系优化、新技术和新业务层面做到时时刻刻精准防护。针对电力网络中如主机、终端以及应用、数据等硬件软件做到全方位可视可信。对于电力网络安全防护主动采用智能防御模式，积极开展网络攻防、监控预警以及协同联动等防御手段，确保形成全方位、多层次的电力网络安全防护机制。

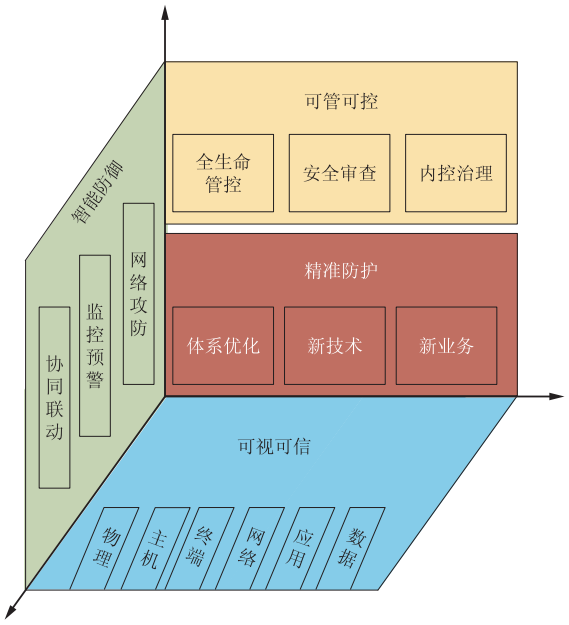


**图 2 等保 2.0 下电力网络安全防护模型**

**Fig. 2 Power network security protection model under classified protection of cybersecurity 2.0**

## 3 电力网络安全管控机制

### 3.1 全业务新形态网络安全监管需求

随着现阶段“互联网+”与智慧能源、能源互联网、智能电网、智能发电、智慧电厂等新型能源的快速融合发展，网络安全防护工作的开展必须紧密结合等保 2.0 新要求，清晰地认识工业控制系统的特殊性、复杂性和专用性，以及其与常规信息系统对网络安全要求的不同之处，从而更好地理解新基建下网络安全所面临的新形态监管需求[11]。

基于此，能源电力企业需要严格遵守等保 2.0 下“一个中心、三重防御”的指导思想，确保实现等保 2.0 对能源电力系统的 2 个全覆盖[12]。

(1)覆盖能源电力“源网荷”不同环节的各个单位、各个部门、各个企业、各个机构。

(2)涵盖能源互联网，信息系统，云平台，物联网，工业控制系统，大数据，移动互联等所受保护对象。

因此，严格遵守等保 2.0 的要求开展信息安全工作至为关键，新形势下基于等保 2.0 的全业务新形态网络安全监管[13]需求模型如图 3 所示。

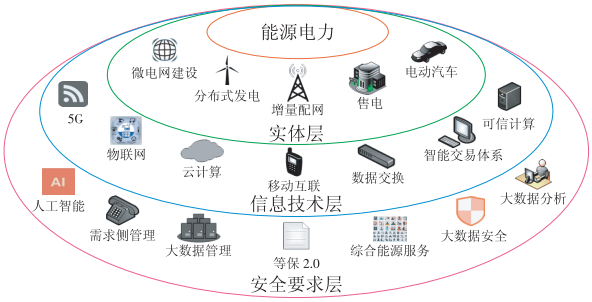


**图 3 全业务新形态网络安全监管需求**

**Fig. 3 Requirements on the new-form cybersecurity supervision for all services**

### 3.2 电力网络安全管控机制设计原则

#### 3.2.1 网络安全发展新机遇和新挑战

基于“数字新基建”的电力网络安全建设的关键以及新一代信息通信发展过程中监管机制建立的紧迫。紧紧抓住新基建所带来的网络安全发展机遇并且迎接网络安全新挑战，在国家法律以及相关政策上必须要保持高度的重视，通过分析电力行业相关规章和运行机制，以此为着眼点，深化安全责任意识，不断夯实“数字新基建”下的电力网络安全防护以及保障工作。在规划实施“数字新基建”并且投入建成运行过程中，须全面加强监管检测、应急响应等管理机制，全方位推进国家电力关键信息基础设施建设[14]，在此期间，强化监督指导所有相关运行单位主体同样十分重要，目的是保证信息化建设与网络安全建设的规划、建设与运行同步进行，以期达到统筹兼顾，始终保持充分的安全意识和安全能力，积极完善各种管理制度，全面做好网络安全监督管理工作。

此外，电力行业在发展数字新基础设施时，必须加强网络安全保障，按照《网络安全法》《密码法》等法律法规的要求，同步规划制定“数字新基础设施”安全技术保障措施，完善面向“数字新基础设施”的安全评估、安全审核、保密审查、日常监测等制度。面对一个大融合、大连接的数字社会，应全面提高全民网络安全意识，加快网络安全建设，以应对日益复杂的信息社会环境[15]。

#### 3.2.2 电力网络安全发展全生命周期

在电力网络安全发展监管体系中，随着能源工业技术体系在开放性、互联互通性上的增强，能源网络的结构复杂化、边界模糊化、形态多样化，信息安全风险化显著增加。与此同时，在输配分离、供

给侧结构性改革，以及云计算、大数据、物联网、移动互联、工业互联网、区块链等新技术、新商业体系和新业务模式的共同推动下，能源电力生产中的信息获取方式、存储形态、传输渠道、处理方法以及对信息安全保障与防护的需求均发生了显著的变化。因此，要在“能源互连、信息共享、商业互动”的理念基础上，实现能源、商业与信息流的双向交互和融合控制，确保能源工业网络空间智能化基础设施的能量流和信息流的对等交换及共享安全[16-17]。

从合规性角度出发，立足能源工业的4个信息安全防护工作定位[18]，坚定自主研发和国产化选型发展思路，采用基于运营、信息、通信技术（Operation，Information，Communication Technology，OICT）的信息物理系统（Cyber Physical Systems，CPS）融合发展技术路线[19]，坚持以业务功能安全为核心，以信息安全为保障，建立计划、执行、检查、处理（Plan，Do，Check and Action，PDCA）的持续改进机制和全生命周期的管控体系，实现能量流、业务流和信息流的双向交互和融合控制，方能构建安全、高效和健壮的能源工业网络空间安全管理模型和运行体系，从而确保能源工业系统的安全、稳定和持续可靠运行。数字新基建下能源电力网络空间安全管理模型如图4所示。

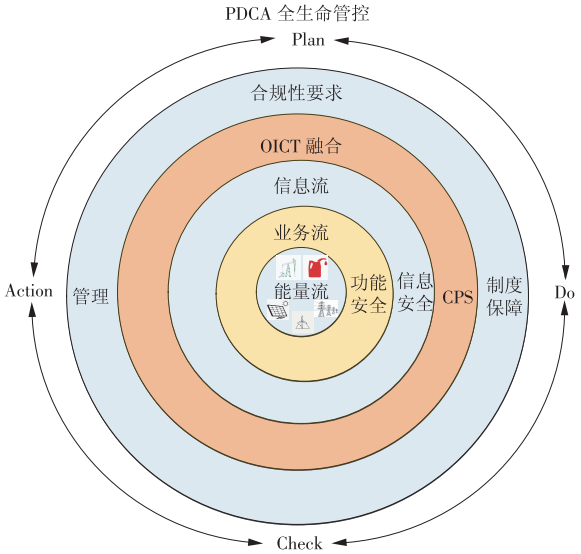


**图4　数字新基建下能源电力网络空间安全管理模型**

**Fig. 4　Space and security management models for energy and power networks in digital new infrastructure**

### 3.3　电力网络安全监管体系设计

“数字新基建”是对比传统基础设施，具备强烈的网络化特征的建设[20]，其带来了大量的网络安全风险且极为致命。在此背景下，推动网络安全全面覆盖“数字新基建”领域，是数字基建建设过程当中不可或缺的外部因素，也是旧产业平稳过渡到各项新型基础设施、新型经济模式的重要保障。在产业内部，电力网络占比日益增加，电力网络智能升级日渐成型，能源互联网、电网数字化平台、电力大数据应用甚至是电力行业人工智能应用等电力综合网络场景发展迅速[21]，不断推动电网转型的过程始终依赖于数字新基建，基于数字化基础设施的电力网络安全成为了人们热切关注的要点。因此，有必要设计紧遵“PDCA”管理流程的数字新基建下网络安全监管体系，数字新基建下电力网络安全监管体系模型如图5所示。

在该模型中，通过设定安全监管目标，把全面落实网络安全责任制作为重点，通过各级领导、管理机构、职能部门及相关工作人员的安全监管及职能要求，健全网络安全监管体系、规范安全监管行为，动态分析安全监管过程，全方位、多层次进行网络安全监管。该模型具体分为以下3个层次。

（1）网络安全监管主体[22]，即实施安全监管的人员，包含决策层、管理层和执行层3个方面。其中决策层主要负责对网络安全监管相关的规章制度进行针对性量化定制；管理层依据决策层制定的安全管理机制进行有效管理；执行层主要为网络安全监管的执行人员，针对决策层定制的监管制度进行落地并受控于管理层人员，从而形成了由上至下的各层次人员的监管体系，并可以以此互相监督，进行全方位人员管理。

（2）网络安全监管对象，即监管什么的问题。依据等保2.0标准主要包含技术和管理2个方面。需要对其进行技术上监管的对象分别为物理环境、通信网络、区域边界、计算环境、管理中心；需要对其进行管理的对象分别为管理制度、管理机构、管理人员、建设管理、运维管理。

（3）网络安全监管反馈机制，即对安全监管结果的分析与评价。当企业完成一个PDCA全生命与全方位的安全监管周期时[23-25]，有必要对监控的结果情况进行汇总、分析与评价考核，从而判断监控结果是否达到预期目标，如果未达到，将对企业进行安全整改并重新考核；如能实现，则将进入下一轮管控周期，从而实现对企业的全面监控，真正做到使多层次的网络安全监控体系呈现螺旋上升的良性循环趋势。

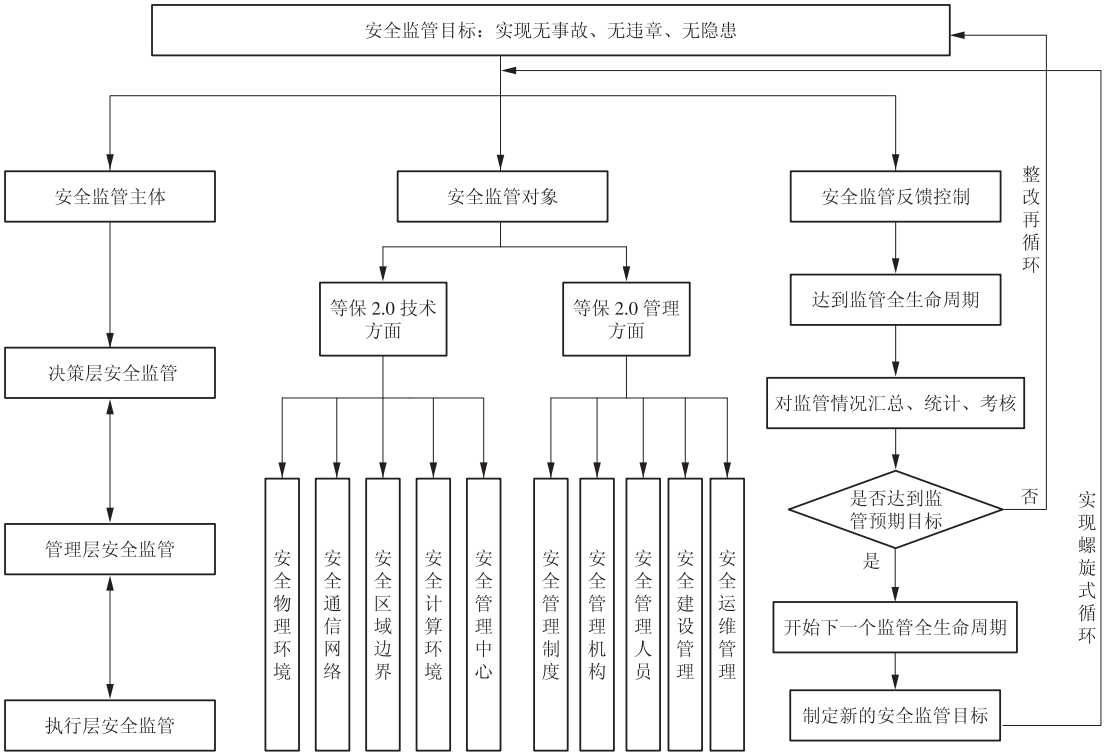


**图5　数字新基建下电力网络安全监管体系模型**

**Fig. 5　Power network security supervision system model in digital new infrastructure**

## 4　结束语

自从国网公司发布“数字新基建”十大任务且相应健全完善数字化重点项目、重大工程以及新一代信息化体制机制以来，建立全新的数字化基础设施至今已是深入人心。在数字化基础设施建设过程中，网络安全是一个长期不容忽视的重要问题，牢固树立网络安全生产理念是整个建设过程的基础，深化落实网络安全责任是整个建设过程的重点，高筑网络安全防御体制则是全行业稳步发展、全产业稳步建成的一道重要防线。从电力行业网络安全的角度看，必须要做好电力网络安全响应机制的优化，健全电力网络的安全生产机制，把握网络安全的基本监管制度，使新基建的发展在源头上得到根本保障。

“数字新基建”建设背景下，本文针对电力行业网络安全，从其发展态势、防护体系和监管机制3个方面展开讨论，表明在全面数字化建设的当前，基于数字基建的网络安全和数据安全关乎全社会产业、国家数字经济的健康发展。通过对新安全形势下等保2.0标准的全方位解读，提出以实现“可管可控、精准防护、可视可信、智能防御”安全方针的能源电力网络安全防护体系；从电力网络能量流、信息流以及业务流等的融合机制角度入手，建立数字新基建下能源电力网络空间安全PDCA全生命周期管理模型，确保能源工业系统健康稳定运行；以网络安全监管为总体目标，对网络安全监管主体、网络安全监管对象和网络安全监管反馈机制3个层面重点考核，确立“数字新基建”下能源电力网络安全监管模式，做到多层次网络安全监管循环有效施行。

## 参考文献：

[1]《智能建筑与智慧城市》编辑部.新基建·新发展·新优势·新希望——“新基建”为产业发展注入智能数字新动力[J].智能建筑与智慧城市，2020(8)：7-10.

[2]舒文琼，张新生.5G发牌将带来五个“有利于”推动我国数字经济蓬勃发展[J].通信世界，2019(16)：19.

[3]孙会峰.“新基建”视野下网络安全新趋势[J].中国信息安全，2020(5)：41-43.
SUN Huifeng. New trends in network security from the perspective of "new infrastructure" [J]. China Information Security，2020(5)：41-43.

[4]姬逸潇.基于网络安全事件的安全态势感知研究[D].西安：西安电子科技大学，2020.

[5]马文君，蔡跃洲.新一代信息技术能否成为动力变革的重要支撑？——基于新兴产业分类与企业数据挖掘的实证分析[J].改革，2020(2)：40-56.
MA Wenjun，CAI Yuezhou. Can the New-generation Information Technology Act as the Key Support for the Transformation of Development Impetus? Empirical

Analysis based on Classification of Emerging Industries and Firm-level Data Mining[J].Reform,2020(2):40-56.

[6]宋文海.浅谈5G技术在智慧城市建设中的应用[J].中国新通信,2020(2):116.

[7]FRANCESCO P, NIK B, JASON J J. Guest editorial: Data science challenges in Industry 4.0[J].IEEE Transactions on Industrial Informatics,2020(9):5924-5928.

[8]段伟伦,韩晓露.全球数字经济战略博弈下的5G供应链安全研究[J].信息安全研究,2020(1):46-51.
DUAN Weilun, HAN Xiaolu. 5G supply chain security research under the global digital economy strategy game[J]. Information Security Research,2020(1):46-51.

[9]李秋香,龚钢军,陈翠云.网络安全等级保护2.0下能源网络安全新态势[C]//2019中国网络安全等级保护和关键信息基础设施保护大会论文集.《信息网络安全》编辑部,2019:4.

[10]牛哲文,郭采珊,唐文虎,等."互联网+智慧能源"的技术特征与发展路径[J].电力大数据,2019,22(5):6-10.
NIU Zhewen, GUO Caishan, TANG Wenhu, et al. Technical characteristics and development path of "internet+smart energy" [J]. Electric Power Big Data, 2019,22(5):6-10.

[11]郝君婷.等保2.0标准发布 网络安全呈现新生态——网络安全等级保护制度2.0国家标准宣贯会侧记[J].保密科学技术,2019(7):8-11.

[12]潘路.电力二次系统网络信息安全防护的设计与实现[D].广州:华南理工大学,2014.

[13]NIE Yan, ZHANG Guoxing, DUAN Hongbo. An interconnected panorama of future cross-regional power grid: A complex network approach[J]. Resources Policy, 2020(4):67.

[14]高原,吕欣,李阳,等.国家关键信息基础设施系统安全防护研究综述[J].信息安全研究,2020,6(1): 14-24.
GAO Yuan, LYU Xin, LI Yang, et al. A review of research on the security protection of national critical information infrastructure systems[J]. Information Security Research, 2020,6(1):14-24.

[15]SERGEY S K, VIKTOR I N, SERGEY Y K, et al. Algorithm and method for recognizing critical situations using semantic networks on critical information infrastructure facilities as a result of cyber attacks[C]// 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). IEEE, 2020.

[16]周洪益,钱苇航,柏晶晶,等.能源区块链的典型应用场景分析及项目实践[J].电力建设,2020,41(2):11-20.
ZHOU Hongyi, QIAN Weihang, BAI Jingjing, et al. Analysis of typical application scenarios and project practice of energy blockchain [J]. Electric Power Construction,2020,41(2):11-20.

[17]孙平远,刘科研,齐冬莲.基于电力信息物理系统实时仿真平台的网络安全仿真[J].电力建设,2020,41(2):40-46.
SUN Pingyuan, LIU Keyan, QI Donglian. Network security simulation based on real-time simulation platform of power cyber-physical system [J]. Electric Power Construction, 2020,41(2):40-46.

[18]张五一,李圣泉.能源行业工控系统信息安全分析与防护[J].信息安全与通信保密,2015(4):41-44.
ZHANG Wuyi, LI Shengquan. Analysis and protection of information security of industrial control system in energy industry [J]. Information Security and Communication Secrecy,2015(4):41-44.

[19]庞继福.基于CPS的区域能源网络信息安全防护技术研究[D].北京:华北电力大学,2018.

[20]刘海军,李晴.新基建加速制造业转型升级[J].当代经济管理,2020,42(9):26-31.
LIU Haijun, LI Qing. New infrastructure accelerates the transformation and upgrading of manufacturing [J]. Contemporary Economic Management, 2020, 42 (9): 26-31.

[21]何奉禄,陈佳琦,李钦豪,等.智能电网中的物联网技术应用与发展[J].电力系统保护与控制,2020(3): 58-69.
HE Fenglu, CHEN Jiaqi, LI Qinhao, et al. Application and development of internet of things technology in smart grid[J]. Power System Protection and Control, 2020(3): 58-69.

[22]GIANG N, STEFAN D, VIET T, et al. Deep learning for proactive network monitoring and security protection[J]. IEEE Access,2020,8:19696-19716.

[23]王宝来,陈安国,肖伟.工业控制系统网络安全防御体系研究[J].网络安全技术与应用,2020(1):119-120.

[24]徐洋.电力行业信息网络安全的现状研究[J].中国管理信息化,2015,18(24):87.

[25]靳琳,赵任方,董钟.基于Spark Streaming的网络安全流式大数据态势感知研究及发展趋势分析[J].网络安全技术与应用,2020(2):62-65.

(本文责编:齐琳)

**作者简介:**

刘超(1982—),男,山西临猗人,工学博士,从事网络安全、电力安全生产信息化、安全监督、应急管理等方面的工作(E-mail:liu-chao@sgcc.com.cn)。

张鹏*(1994—),男,山西大同人,在读硕士研究生,从事电力行业网络安全、配电网信息物理系统脆弱性研究等方面的工作(E-mail:799456251@qq.com)。