第47卷 第8期 2023年4月25日
DOI：10.7500/AEPS20220627002
电力系统自动化
Automation of Electric Power Systems
Vol. 47 No. 8 Apr. 25，2023

新型电力系统网络安全防护挑战与展望

周劼英[1]，张 晓[1]，邵立嵩[2]，应 欢[3]
（1. 国家电网有限公司国家电力调度控制中心，北京市 100031；
2. 南瑞集团有限公司（国网电力科学研究院有限公司），江苏省南京市 211106；
3. 中国电力科学研究院有限公司，北京市 100192）

摘要：构建新型电力系统是中国国家能源战略的重要发展方向，保障新型电力系统的网络安全意义重大。首先，文中深入分析了新型电力系统环境下电源结构、电网形态、业务模式、技术基础等方面的变化引入的网络安全风险。其次，结合现有的网络安全防护措施，从可信接入、智能感知、精准防护、联动响应等方面提出面向新型电力系统的网络安全防护需求。最后，对未来新型电力系统网络安全关键技术涉及的接入安全、内生安全、数据安全、通信安全、安全评估与仿真验证等重点研究应用方向进行探讨和展望。

关键词：新型电力系统；新能源；网络安全；防护；智能感知

0 引言

电力系统作为国家关键基础设施，不仅关系到国家经济安全，而且与人民生活、社会稳定密切相关。电力行业历来高度重视网络安全工作，自2002年以来，中国大力推进网络安全防护建设工作，经过20多年的努力，坚持“安全分区、网络专用、横向隔离、纵向认证”的安全方针[1]，持续推进终端安全防护能力研究与建设[2-3]，深化网络安全态势感知平台建设与应用[4]，部署应用电力可信计算平台[5]，全面落实安全技术防护措施，强化网络安全管理，形成了以边界防护为要点、多道防线的纵深防御体系[6]。

近年来，随着“碳达峰·碳中和”目标的提出和大规模新能源并网、新型储能、可调节负荷广泛接入，电力系统的系统结构和形态正在发生深刻变革[7-8]。相较于传统的电力系统，新型电力系统的系统结构更加复杂，生产组织模式趋向于源网荷储“融合互动”[9]。

数字化是新型电力系统建设发展的重要支撑[10]。依托各类数字化平台的支撑，新型电力系统实现源网荷储各环节协同运行、智能交互，能源流、业务流、数据流多流融合，开放程度不断提升，参与主体更加多样化、交互方式更加智能化、融合数据更加丰富化，也给新型电力系统带来更多网络安全风险[11-12]。源于终端设备、网络设备、数字化平台的网络安全隐患，极易传导至电力系统本身，从而引发重大安全事件。

为了应对日益突出的网络安全问题，提升新型电力系统的安全防护能力，本文结合当前形势深入分析了新型电力系统面临的网络安全风险，探讨了新型电力系统网络安全防护需求和技术发展方向，为后续防护工作提供了参考。

1 新型电力系统的特征和网络安全形势

能源行业是中国实现“碳达峰、碳中和”目标的主战场，电力行业是实现“碳达峰、碳中和”目标的主力军[13-14]。2021年3月的中央财经委员会第九次会议上首次提出构建新型电力系统。作为“碳达峰、碳中和”的重要实现途径，新型电力系统建设上升为国家战略[15]。新型电力系统是以确保能源电力安全为基本前提，以满足经济社会高质量发展的电力需求为首要目标，以大规模新能源供给消纳体系建设为主线任务，以源网荷储多向协同、灵活互动为坚强支撑，以坚强、智能、柔性电网为枢纽平台，以技术创新和体制机制创新为基础保障的新时代电力系统，具备安全高效、清洁低碳、柔性灵活、智慧融合四大重要特征[16]。

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[17]，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

收稿日期：2022-06-27；修回日期：2023-01-13。
上网日期：2023-03-13。
国家电网有限公司科技项目（新型电力系统下分布式电源调度控制安全防护关键技术研究与应用，5108-202325046A-1-1-ZN）。

系产生冲击。

1)风险暴露面不断扩大。随着分布式电源、储能等分布式设备终端广泛接入,分布式能源、电动汽车、虚拟电厂、综合能源服务等新型业务快速涌现,能源聚合商、综合能源服务商等多元化主体广泛参与[18],交互主体的多样性使得电力系统整体的安全防御关口增多,外部主体的弱安全防护能力有可能会将网络安全风险传导至电力系统涉控核心区域,网络空间边界不断延伸,边界安全风险陡增[19]。

2)数据安全隐患急剧增加。新型电力系统引入多元主体,新业务间的交互方式丰富多样,由传统单向数据采集转变为双向互动方式,数据流通共享、交叉访问、协同分析的需求剧增[20],数据交互呈现数据量大、次数频繁、数据类型多等新特点,数据共享与隐私保护矛盾凸显,在挖掘数字价值、发展数字经济的过程中以获取数据为目的的内、外部攻击呈现递增趋势。

3)新技术安全风险持续升级。随着5G、人工智能、大数据、区块链等新兴数字技术广泛应用[21-22],新技术本身除面临传统网络攻击的风险外,还存在终端被侵入[23]、用户被仿冒和数据被篡改的风险[24-25]。以负荷聚合商为代表的第三方主体朝着可互联网远程控制方向发展,一旦负荷聚合平台被网络攻击入侵,攻击者可以恶意控制大量可调节负荷进行"群体性"破坏,可能引发重大网络安全事件,影响电网安全、用电安全,破坏电网稳定。

在新型电力系统蓬勃发展的同时,国内外网络安全形势也正发生着巨大而深刻的变化。一是网络空间竞争愈发激烈。网络与信息安全风险向政治、经济、文化、社会、生态、国防等领域传导渗透,网络空间成为没有硝烟的战场[26]。2021年上半年公开的高级可持续威胁(advanced persistent threat, APT)研究报告[27]显示,政府、国防军工、科研和能源是主要目标,电力系统日益成为国内外敌对势力、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,如图1所示。近年来,"乌克兰大停电""委内瑞拉大停电""南非电力勒索攻击"等针对电力系统的网络攻击事件频发,预计未来针对新型电力系统的网络窃密、远程破坏、勒索病毒等攻击会持续增加。二是新型网络攻击技术不断演进[28]。国家级、集团式攻击方式快速发展,勒索软件、APT攻击等新型攻击手段层出不穷,攻防对抗强度不断提升,结合人工智能、社会工程等手段突破边界防护措施对电网内部系统进行攻击的风险越来越高,传统的边界防护体系面临严重威胁[29-30]。

中国高度重视基础网络和重要系统安全保护工

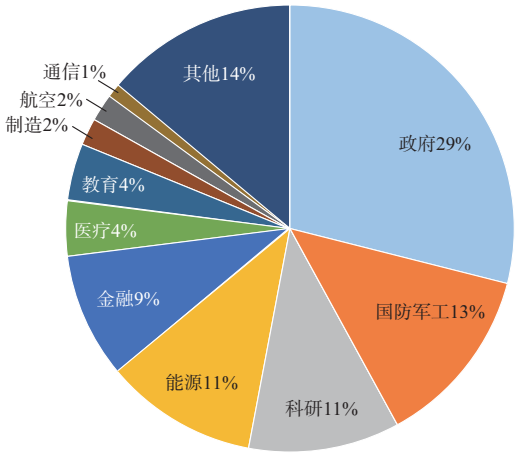

图1　2021年上半年公开的高级可持续威胁报告涉及行业分布

Fig. 1　Distribution of industries involved in APT report released in first half of 2021

作,近年来,就加强网络安全防护作出了一系列重大决策部署。《中华人民共和国网络安全法》和《关键信息基础设施保护条例》[31]明确电力行业为国家关键信息基础设施领域之一,要求对电力行业关键信息基础设施实行重点保护。《中华人民共和国密码法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《关键信息基础设施安全保护条例》及《电力安全生产"十四五"行动计划》[32]等一系列网络安全法律法规和行业规范性文件陆续出台,明确了网络安全对新型电力系统建设具有重要作用,并提出了新的、更高的要求。

2　新型电力系统面临的网络安全挑战

新型电力系统的构建深刻改变了传统电力系统的电源结构、电网形态、业务模式和技术基础[11-12]。以风光为代表的新能源发电占比逐步提升,海量风、光、储等小型分布式设备接入电网,微电网、虚拟电厂等新业务场景蓬勃发展,这些变化都给电力系统带来新的网络安全风险。

1)在电源结构方面,新能源发电新增装机容量的占比持续提升。根据国家能源局发布的2022年全国电力工业统计数据[33],截至2022年12月底,全国累计发电装机容量约2 560 GW,同比增长7.8%,其中,风电装机容量约370 GW,同比增长11.2%;太阳能发电装机容量约390 GW,同比增长28.1%。随着电源结构的变化,能源聚合商、电网企业、发电企业、节能服务商、电力用户等参与主体数量剧增。电源侧、电网测与负荷侧的业务交叉互访频繁,电力系统的网络空间边界不断延伸。海量分布式电源终端、设备大多处于无人值守的开放、不可信的物理环

境中，网络暴露面日益扩大，网络攻击跳板增多，基于物理隔离的网络边界安全防护措施难以深入末梢，安全责任边界超越网络大区边界，以边界防护为主的安全防护策略实施难度陡然提升[34]。例如，网络攻击者可以利用分布式光伏终端设备的安全漏洞，破坏设备正常运行，影响光伏出力和供电可靠性。

2）在电网形态方面，由单向逐级输配电为主的传统电网向包括直流电网、交直流混联大电网、微电网和可调负荷的能源互联网转变，电网结构更加复杂、交互更加频繁。同时，随着家庭光伏、小风电等终端接入电网，以及大量存量工控终端设备，新型电力系统的终端设备呈现出型号多样、数量巨大、结构复杂、空间分布分散等特点。联网接入方式多样，导致数据通信方式多样性增大，终端身份识别认证困难，安全接入难度加大。此外，新型电力系统将与热气管网、天然气管网、交通网络等能源链进行复杂互联互通，形成多领域综合能源网络，用电负荷、负荷集成商及其他能源链主体的网络安全防护措施参差不齐，网络攻击者可能利用其集中管控平台漏洞窃取用户信息，篡改运营数据，甚至批量启停设备。

3）在业务模式方面，分布式新能源大规模并网、精准负荷控制、新型配电网保护等新业务的应用需求，对电力通信的带宽时延、可靠性、安全性、经济性提出了更高的要求，需要引入安全可靠的无线通信方式解决业务接入问题。同时，各类用户、运营商、服务商等参与电力市场交易的主体越来越多。众多电力市场交易数据、用户隐私数据等敏感数据将存在多链路传递、存储、使用，多方位的数据聚合导致的数据泄露、篡改风险加剧。这对新型电力系统下数据资产的完整性、保密性、可用性提出更高的要求。此外，需求侧将涌现越来越多的虚拟电厂或负荷集成商等第三方新主体，各种“光伏云”“空调云”“充电云”等新型电力市场主体涌现[19]，通信网络由封闭、可信转向开放、不可信，部分系统和设备未纳入现有监测体系，部分计算、存储资源受限的终端无法被有效监视，现存网络安全监测范围尚未全面覆盖新型电力系统各类资源，安全监测能力亟须由核心网络向边端和各领域业务延伸。

4）在技术基础方面，人工智能、大数据、云计算、边缘计算、5G等新兴技术在新型电力系统中充分运用，支撑电网数据综合分析，赋能电力数据共享利用，提升电网智能化水平，同时其内在安全问题也逐步暴露。5G通信技术是支撑能源转型的重要战略资源和新型基础设施，但其虚拟化基础设施、物联平台等较易遭受外部攻击；云计算的分布性削弱了安全防护措施的可控性；区块链技术由于其去中心化、开放性、防篡改和可追溯的特点，广泛应用于实时电力交易、源网荷储互动与多能互补等方面，但自身仍存在协议安全性、智能合约安全等方面的风险。

此外，新型电力系统的电源结构、电网形态、业务模式、技术基础的深刻改变，对网络安全管理职责、工作机制等都提出了新的要求。新型电力系统涉及的运营主体涵盖了传统的电网、发电、售电及能源链相关企业，将用户、运营商、服务商等社会多方参与者纳入，在业务应用中不同程度地存在用户身份凭据管理不合规、访问控制策略不严谨、技术监督手段不全面、风险防范措施不完备等问题。现有垂直业务管理模式无法适应物联网“万物互联”的发展需求，简单“三同步”网络安全管理无法满足新型电力系统业务安全防护需求，迫切需要完善构建网络安全专业管理技术支撑体系。

新型电力系统构建深刻改变了传统电力系统形态，网络结构复杂化、边界扩大化、攻击形态多样化等给电力系统带来新的网络安全风险，亟须提升新型电力系统网络安全防护能力，构建适应新型电力系统的网络安全防护体系。

3　新型电力系统网络安全防护需求

新型电力系统建设催生大量新业态发展和新技术应用，电力系统在源、网、荷、储各个环节都将发生重大变化、产生新的安全风险并催生新的网络安全防护需求。与之相适应，新型电力系统的网络安全防护需要在继承“安全分区、网络专用、横向隔离、纵向认证”安全方针的基础上，进一步围绕可信接入、智能感知、精准防护、联动响应等方面应用先进技术，提升网络安全防护能力，满足新型电力系统业务与应用安全防护需求，防范网络攻击风险，保障新型电力系统安全稳定运行。

1）可信接入

针对新型电力系统中分布式新能源、精准负荷控制等典型业务场景存在网络边界动态变化、接入对象身份不确定、接入终端工作环境不可信等因素，主体接入需采用实时身份认证和动态权限管理。在整个访问周期内，根据接入用户以及终端的不同业务需求对用户进行身份合规性检查，实时管控访问过程中的违规行为，保证业务体验与安全需求之间的平衡。

现有认证及准入机制通常是基于用户与设备在网络中的位置来判断是否安全可信，主要适用于传统电力系统网络空间封闭环境中各类业务应用，但对于外部接入主体身份辨识能力不足，同时缺乏有

效的动态授权管理机制。因此，需要在现有边界安全防护基础上研究面向新型电力系统的可信接入方案。

具体实践的关键在于实时身份认证方法和动态权限管理机制。实时身份认证需要针对接入主体安全运行状况，定义一套涉及硬件、固件、软件和应用等整个运行环境的终端完整检测策略，从而应对各种接入设备的可信认证，并结合可信终端的合规业务需求，基于访问控制列表等方法构建动态权限管理机制，实现接入权限的精细化管理。

2)智能感知

日渐严峻的网络安全形势，要求新型电力系统的安全防护策略从传统被动防御向主动防护转变。面向未知的网络安全风险需要主动感知并快速有效地识别和发现攻击行为，增强防御和威慑能力，提供主动有效的全方位体系化防护。新型电力系统的源、网、荷各环节运营主体都需要建立网络安全事件智能感知手段，对网络安全事件进行预测、预判、预警及预控，实现对网络安全风险的主动感知。

网络安全事件智能感知系统需要强化聚合全域网络安全态势监测预警能力，扩大态势感知范围，增强对物联终端、新型网络边界、新型第三方控制主体的安全监测分析能力，整合新型电力系统中各个主体的网络安全态势感知能力，汇聚全域网络安全数据并完成统一建模，建立统一指挥、多级协同、联动处置的网络安全监测与响应机制，构建适应新型电力系统的网络安全态势感知技术架构。同时，需要完善建设电力系统专用漏洞管理、恶意代码监测功能，并与现有的网络安全监测功能相融合，强化终端监测感知，具备面向实战、上下贯通、全域联动、多源情报、快速响应的全天候网络安全风险感知能力。

在技术实现方面，网络安全事件智能感知系统需要深化分布式部署终端的信息采集广度和深度，面向新型电力系统海量设备特征指纹构建统一的安全模型库，动态监测网络设备接入和离线的状态，全面测绘网络空间实体资源和虚拟资源，为智能分析奠定丰富的数据基础。同时，可基于机器学习、知识图谱、攻击溯源、网络恶意入侵诱捕等技术，采用多维安全事件数据融合技术构建智能分析模块，精准识别异常行为及攻击事件，实现安全分析从经验型向智能型的转变。构建新型电力系统网络安全事件智能感知系统框架如图2所示。

3)精准防护

新型电力系统涉及众多业务应用场景，各种应

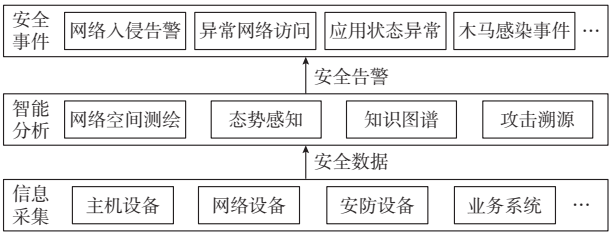

图2　新型电力系统网络安全事件智能感知系统框架
Fig. 2　Framework of intelligent sensing system for cyber security incidents of new power system

用场景安全保护需求既有共同点，也存在较大差异，因此，面向业务场景的精准防护是保障新型电力系统网络安全“零事故”的关键。如图3所示，精准防护需要根据国家、行业网络安全防护相关合规性要求，在对源网荷储各环节、各主体相关网络、系统进行综合性安全防护的基础上，针对业务场景差异性，制定防护措施和安全配置策略，实现业务差异化、精准化防护。

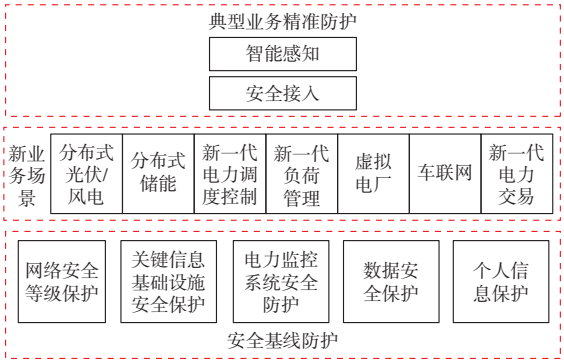

图3　新型电力系统精准防护体系框架
Fig. 3　Framework of precise protection for new power system

安全基线防护是精准防护的基础，需要根据国家、电力行业网络安全等级保护标准、要求，加强重要数据和个人信息保护，利用新技术开展网络安全保护，构建以密码技术、可信计算、人工智能、大数据分析等为核心的新型电力系统网络安全防护体系。对于已认定为国家关键信息基础设施的网络、系统、设备，需要参照国家、行业关于关键信息基础设施安全保护标准、要求，强化检测评估、监测预警、应急处置、数据保护等重点保护措施，强化供应链安全保障工作。对于重要电力信息系统、网络设施，需要依据电力系统安全防护要求，从基础设施安全、体系结构安全、系统本体安全和可信安全免疫等方面落实安全防护技术措施。

面向新型电力系统的精准防护，需要针对分布式新能源、分布式储能、新一代电力调度控制、新一

代负荷管理等新业务应用,围绕智能感知、安全接入部署防护措施,确保分布式设备的安全接入和全景感知,以及边端设备网络安全层面的可观测、可控制,重点分析业务特点和网络安全风险,并采取针对性的安全防护措施,实现按需防护,进一步增强新型电力系统的安全免疫能力。

4)联动响应

新型电力系统面临的安全威胁日渐复杂,单一的防护手段难以有效应对高等级复杂威胁,亟须打破多设备、多场景之间的"信息孤岛",构建电力系统网络攻击协同处置体系(如图4所示),强化新型电力系统源网荷储各环节间的联防联控,提升系统整体应对网络威胁的能力。

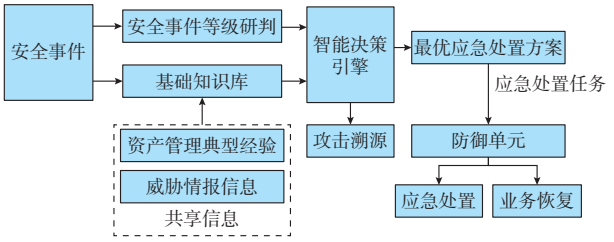

图4　电力系统网络攻击协同处置体系

Fig. 4　Coordinated disposal architecture of cyber attack on power system

联动响应需要构建新型电力系统纵向、横向数据共享联动能力。在纵向数据共享联动方面,需要强化企业内各部门间的信息共享,加强集团总部与下属单位间的网络安全事件信息通报;在横向数据共享联动方面,需要建立源、网、荷、储企业之间的威胁情报共享机制。

联动响应需要建设新型电力系统网络攻击协同处置体系,协同处置体系的关键在于构建针对电力系统的网络安全威胁情报基础知识库和智能决策引擎。当网络安全事件发生时,基于大数据、人工智能等技术结合安全事件等级研判,综合分析安全事件,驱动安全策略的解析、生成、更新,最终通过智能决策引擎,得出最优应急处置方案、生成应急处置任务、智能下发各防御单元、自动执行协同应急处置操作,通过智能化控制技术实现多级联动响应与快速处置,实现集攻击溯源、智能处置、应急恢复为一体的网络安全智能指挥调度。同时,需要为远程决策者提供自动化协同交互服务,从被动应对向主动自动化联动响应转变,从单点防护向全域防护转变,推动新型电力系统全业务环节的快速联动响应、排查与修复。

4　新型电力系统网络安全技术研究应用展望

"云、大、物、移、智"等新技术的快速发展应用为电力系统的网络安全同时带来了挑战和契机,电力系统网络安全发生了重大变化。5G通信技术提升了无线远程控制安全可靠性;嵌入式技术实现了安全组件终端部署;态势感知技术使得安全信息采集覆盖外围网络;人工智能、大数据技术提升了海量安全数据处理效率;隐私保护技术保障了电力市场交易数据全生命周期安全;资产数字化技术改进了安全检测评估模式。基于虚拟化网络的数字化仿真技术可模拟攻防实验验证安全策略有效性,电力系统网络安全正逐步形成体系化、数字化、智能化的发展趋势。新型电力系统网络安全在广度和深度快速发展的同时,安全防护关键技术的研究仍有很多空白之处。基于前文对新型电力系统网络安全需求的分析,以下有价值或亟须研究、应用的安全防护技术方向值得关注。

1)分布式设备安全认证接入

随着分布式终端设备类型、数量剧增,以及更多的新型业务涌现,传统的基于以太网、光纤和少量设备的电力终端通信网正逐渐转变为融合以太网、移动网络、WIFI等多种方式混合组网模式。未来新型电力系统边界侧的安全防护应转变以传统边界隔离为主的防护思路,探索区块链、零信任等新技术在分布式终端设备安全接入和身份认证的应用,以应对终端设备的身份不确定性、访问权限动态变化等安全防护挑战。

在新型电力系统终端安全接入引入基于零信任的"云边协同"和"边缘智能"理念,按照"保持怀疑、动态验证"[35-36]的原则,研究面向终端运行特征的信任度计算方法。基于多因子模糊认证技术实现多类型访问主体身份认证,通过差异化认证策略开展终端持续信任评估,验证用户的身份和设备的合法性,构建细粒度的动态授权管控机制实现按需调整用户权限。同时,识别记录异常行为数据以保证重点数据的全过程审计,并利用可信身份和可信行为重新构建虚拟安全边界。研究设计基于零信任的分布式终端安全接入框架,实现电力终端的安全高效接入、精细化访问控制,发现并及时阻断电力终端恶意控制导致的电力系统网络攻击,从而应对电源结构变化导致网络边界延伸和接入对象不确定所带来的风险。

借鉴区块链去中心化、防篡改、可追溯的安全特

性,通过设计专用的数据结构和共识机制,构建适应新型电力系统的网络信任模型,具备海量分布式终端设备数字身份数据、实时运行数据等在区块链账本上发布和维护功能。同时,研究基于智能合约的身份可信度智能评估技术,实现分布式设备的可信身份认证。

2)新型业务系统内生安全防护

与传统的安全防护相比,新型业务应用系统的网络安全是新型电力系统的安全底座,更加注重面向差异化场景的针对性防护。因此,从防护手段角度而言内生免疫安全更加适用。通过强化内生免疫安全技术应用,例如,利用目标系统的自身架构等内源性效应而获得可量化设计、可验证度量等安全功能,重点研究适用于电力关键信息基础设施的安全操作系统、基于分布式终端的嵌入式可信计算、适用于调度控制的量子通信密码、内生安全光通信等技术,保障新型电力系统业务应用安全可靠运行。从可靠性理论出发,以现有的认知水平、产品设计缺陷导致的漏洞等内生安全问题无可避免[37]。因此,新形态的业务系统内生安全有必要尝试结合新型电力系统的特点研究拟态防御技术[38],基于分布式虚拟化的云计算技术设计构造适用于电力系统的低成本动态异构冗余构造(dynamic heterogeneous redundancy,DHR)架构,研制电力网络边界专用的拟态防御安防产品,开发适用于新业务应用系统的拟态防御组件,发展构建电力系统网络空间拟态防御机制。

3)全生命周期数据安全保护

新型电力系统的建设涉及多方主体进行海量、多类数据的交互和共享,数据应用场景和参与主体日趋多样化,电力数据助力数字经济快速发展。同时,数据安全事件频发,数据安全问题愈加突出,需要围绕数据生命周期研究各个阶段使用的安全保护技术。在电力数据风险预警监测方面,研究数据流量异常发现、数据安全监测分析、数据安全预警和态势感知等技术,对数据生命周期各个过程进行监控管理。在数据资源资产化管理方面,引入智能识别技术,通过构建电力数据识别模型挖掘数据隐式关系,研究关键数据的甄别方法和保护策略。在多方主体交互方面,针对电力市场数据共享发布、现货交易科学研究、政府监管等应用场景,应加强交易数据隐私防泄露,建议在同态加密、安全多方计算[39]和联邦学习、数据匿名化、数据脱敏、差分隐私等技术方面寻求突破,在发挥数据价值的同时保证数据的可信使用。在数据存储方面,可采取数据安全隔离和访问控制技术,防止非常规数据访问,并采取同态加密和可搜索加密等技术保证数据存储的机密性和可用性。在数据销毁安全方面,研究数据安全审计、基于密钥销毁的可信删除、基于时间过期机制的数据自销毁等技术,保障数据安全销毁。

4)5G安全防护

5G通信技术具有“大带宽、低时延、高可靠、广连接”等特点[40],可实现更广阔的覆盖率和更稳定的网络连接,未来将成为新型电力系统无线电力通信的普遍接入方式。目前,部分电网企业、发电企业已经陆续开展5G承载电力控制业务的试点工作。相比于传统的光纤通信和无线专网通信,5G在核心网层引入了网络功能虚拟化、网络切片、网络能力开放等新技术[41],可能导致新型电力系统面临无线通信终端身份盗用、无线频谱数据抗干扰能力不足、网络切片攻击、虚拟化攻击等安全问题。同时,数据挖掘和量子计算也可能会对5G网络通信数据的机密性和完整性传输造成威胁[42-43],给电力系统二次设备以及电网调度系统等稳定运行埋下安全隐患。

未来面向新型电力系统背景下的5G安全防护应重点探索电力涉控和非涉控业务的安全需求,关注5G终端接入加密认证及安全管控、5G网络切片安全监测及管控、5G调控业务安全防护、5G数据完整性和机密性保护等多个方面。在关键技术攻关方面,应重点攻克基于零知识证明、无证书密码、同态加密、聚合签密等新兴技术在5G通信安全加密认证、数据完整性校验等方面的应用。基于网络功能虚拟化(network functions virtualization,NFV)等网络虚拟化技术实现软硬件解耦,提高网络安全策略的可编排性;基于软件定义网络(software defined network,SDN)的电力系统业务管控技术,在5G网络与上层业务应用解耦分离的同时,实现包括分组数据连接、数据包转换在内的多种业务动态管控机制;面向网络切片实现数据隐私保护,防止跨切片信息的非法访问,实现切片内数据的隐私保护。通过综合利用上述多种技术,从物理层、网络层、应用层等方面保证5G通信的全周期安全,提升新型电力系统的网络通信安全防护水平。

5)安全检测与评估

新型电力系统拥有海量设备,其软硬件可能涉及第三方开源组件、国外元器件等,存在内置后门等潜在风险,在设备研发、制造或物流等供应链环节可能会被攻击者植入恶意代码并锚定具体业务应用场景发起网络攻击,进而将威胁传至电力系统核心区

域。因此，应针对新型电力系统源、网、荷、储信息网络和重要资产、业务应用场景，开展智能化漏洞挖掘、软件代码成分分析与溯源、恶意代码检测和风险评估技术攻关。面向电力设备协议、固件、软件等多个层面，研究基于恶意代码演化特征的智能漏洞挖掘技术，攻克基于自学习的源代码漏洞静态分析技术、基于特征码的恶意代码检测技术、基于代际遗传分析的代码溯源技术，突破基于物理场信息的芯片安全检测技术，构建新型电力系统网络与业务风险评估指标体系，实现无线网络（5G等下一代通信方式）安全评估，加强面向商用密码应用的渗透测试技术和面向等级保护的自动化测评技术研究，提升新型电力系统的网络安全隐患发现能力。

6）网络安全仿真与攻防试验

网络攻防演练是提升网络空间攻防能力的重要手段，网络安全仿真验证环境是开展网络攻防演练、网络风险评估分析、网络空间安全技术验证的重要基础设施。因此，应重点攻克终端、协议、网络等典型电力工控系统仿真技术，研究可适用于海量终端业务场景的终端仿真技术，掌握电力网络安全仿真验证环境虚实资源的统一标识和建模方法，构建各类软硬件资源和业务系统的统一调度配置策略，支撑分布式新能源、新型电力调度控制、新型电力负荷控制等新业务场景的靶标快速搭建。研究仿真验证环境之间的自适应级联配置技术，实现仿真验证环境中虚实资源的互联互通和分布式仿真验证环境的协同调度与统一管理。攻克面向攻击诱捕的网络欺骗防御技术，研究未知攻击行为的特征采集识别方法，建设新型电力系统专用的漏洞库与网络攻防武器装备，支撑新型电力系统新场景、新业务的网络安全攻防试验。

5　结语

国家能源结构转型和新型电力系统的构建深刻改变了电力系统的组成和架构，对现有网络安全体系带来巨大挑战，对安全防护技术发展提出新的要求。本文深入分析了新型电力系统在电源结构、电网形态、业务模式、技术基础这4个方面的变化所带来的网络安全风险，从可信接入、智能感知、精准防护、联动响应等方面应用提出了新型电力系统网络安全防护需求，对保障新型电力系统需要研究、应用的技术进行了展望，探讨提出了接入安全、内生安全、数据安全、通信安全、安全评估和仿真验证等领域的技术研究路径和应用方向。可以说，没有网络安全就没有新型电力系统的安全。下一步，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，推进重点安全防护措施的试点与推广，全面提升源、网、荷、储网络安全防护能力，保障新型电力系统安全稳定运行。

参 考 文 献

[1] 国家发展和改革委员会．电力监控系统安全防护规定[EB/OL]．[2022-06-27]．http://www.gov.cn/gongbao/content/2014/content_2758709.htm.
National Development and Reform Commission. Safety protection regulations for power monitoring systems [EB/OL]. [2022-06-27]. http://www. gov. cn/gongbao/content/2014/content_2758709.htm.

[2] 苏盛，汪干，刘亮，等．电力物联网终端安全防护研究综述[J]．高电压技术，2022，48(2)：513-525.
SU Sheng, WANG Gan, LIU Liang, et al. Review on security of power Internet of Things terminals [J]. High Voltage Engineering, 2022, 48(2): 513-525.

[3] 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.
ZHANG Tao, ZHAO Dongyan, XUE Feng, et al. Research framework of cyber-security protection technologies for smart terminals in power system [J]. Automation of Electric Power Systems, 2019, 43(19): 1-8.

[4] 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(增刊2)：103-109.
ZHANG Liang, QU Gang, LI Huixing, et al. Research and application of key technologies of network security situation awareness for smart grid power control systems [J]. Journal of Shanghai Jiao Tong University, 2021, 55 (Supplement 2): 103-109.

[5] 安宁钰，王志皓，赵保华．可信计算技术在电力系统中的研究与应用[J]．信息安全研究，2017，3(4)：353-358.
AN Ningyu, WANG Zhihao, ZHAO Baohua. Research and application of trusted computing in electric power system [J]. Journal of Information Security Research, 2017, 3(4): 353-358.

[6] 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 Kunlun, XIN Yaozhong, LI Zhao, 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.

[7] 李明节，陈国平，董存，等．新能源电力系统电力电量平衡问题研究[J]．电网技术，2019，43(11)：3979-3986.
LI Mingjie, CHEN Guoping, DONG Cun, et al. Research on power balance of high proportion renewable energy system [J]. Power System Technology, 2019, 43(11): 3979-3986.

[8] 李明节，陶洪铸，许洪强，等．电网调控领域人工智能技术框架与应用展望[J]．电网技术，2020，44(2)：393-400.

LI Mingjie, TAO Hongzhu, XU Hongqiang, et al. The technical framework and application prospect of artificial intelligence application in the field of power grid dispatching and control[J]. Power System Technology, 2020, 44(2): 393-400.

[9] 康重庆.《新型电力系统技术研究报告》发布与解读[EB/OL]. [2022-06-27]. https://power. in-en. com/html/power-2401723. shtml.
KANG Chongqing. Release and interpretation of "New Power System Technology Research Report" [EB/OL]. [2022-06-27]. https://power.in-en.com/html/power-2401723.shtml.

[10] 张文瀚.数字电网关键技术研究与实践[EB/OL].[2022-06-27].http://www.csee.org.cn/pic/u/cms/www/202102/02150729g9p8.pdf.
ZHANG Wenhan. Research and practice of digital grid key technologies [EB/OL]. [2022-06-27]. http://www. csee. org. cn/pic/u/cms/www/202102/02150729g9p8.pdf.

[11] 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.
ZHOU Xiaoxin, CHEN Shuyong, LU Zongxiang, et al. Technology features of the new generation power system in China[J]. Proceedings of the CSEE, 2018, 38(7): 1893-1904.

[12] 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):966-979.
WU Kehe, WANG Jiye, LI Wei, et al. Research on the operation mode of new generation electric power system for the future energy Internet[J]. Proceedings of the CSEE, 2019, 39(4): 966-979.

[13] 舒印彪,陈国平,贺静波,等.构建以新能源为主体的新型电力系统框架研究[J].中国工程科学,2021,23(6):61-69.
SHU Yinbiao, CHEN Guoping, HE Jingbo, et al. Building a new electric power system based on new energy sources [J]. Strategic Study of CAE, 2021, 23(6): 61-69.

[14] 王彩霞,时智勇,梁志峰,等.新能源为主体电力系统的需求侧资源利用关键技术及展望[J].电力系统自动化,2021,45(16):37-48.
WANG Caixia, SHI Zhiyong, LIANG Zhifeng, et al. Key technologies and prospects of demand-side resource utilization for power systems dominated by renewable energy [J]. Automation of Electric Power Systems, 2021, 45(16): 37-48.

[15] 国家能源局,科学技术部.关于印发《"十四五"能源领域科技创新规划》的通知[EB/OL].[2022-06-27].http://www.gov.cn/zhengce/zhengceku/2022-04/03/content_5683361.htm.
National Energy Administration, Ministry of Science and Technology. Notice on printing and distributing the "Fourteenth Five-Year Plan for science and technology innovation in the energy field" [EB/OL]. [2022-06-27]. http://www. gov. cn/zhengce/zhengceku/2022-04/03/content_5683361.htm.

[16] 国家能源局.新型电力系统发展蓝皮书(征求意见稿)[EB/OL]. [2022-06-27]. http://www. nea. gov. cn/2023-01/06/c_1310688702.htm.
National Energy Administration. Blue book on the development of new power systems (draft for comments) [EB/OL]. [2022-06-27]. http://www. nea. gov. cn/2023-01/06/c_1310688702.htm.

[17] 江冰.构建面向30·60的新型电力系统——中国电力4.0的思考[J].全球能源互联网,2021,4(6):534-541.
JIANG Bing. Building new power system for 30·60—reflections on China's electricity 4.0 [J]. Journal of Global Energy Interconnection, 2021, 4(6): 534-541.

[18] 程松,周鑫,任景,等.面向多级市场出清的负荷聚合商联合交易策略[J].电力系统保护与控制,2022,50(20):158-167.
CHENG Song, ZHOU Xin, REN Jing, et al. Bidding strategy for load aggregators in a multi-stage electricity market [J]. Power System Protection and Control, 2022, 50(20): 158-167.

[19] 郭庆来.新型电力系统发展应当重点关注新型网络安全风险[EB/OL]. [2022-06-27]. https://mp. weixin. qq. com/s/X6ZKHiDF2P2d7ksMq2x8PA.
GUO Qinglai. New power system development should focus on new cyber security risks[EB/OL]. [2022-06-27]. https://mp.weixin.qq.com/s/X6ZKHiDF2P2d7ksMq2x8PA.

[20] 王继业.激发数据要素新动能驱动能源电力转型发展[J].软件和集成电路,2021(5):30-31.
WANG Jiye. Stimulating new kinetic energy of data elements to drive the transformation and development of energy and electricity[J]. Software and Integrated Circuit, 2021(5): 30-31.

[21] 朱彦名,徐潇源,严正,等.面向电力物联网的含可再生能源配电网运行展望[J].电力系统保护与控制,2022,50(2):176-187.
ZHU Yanming, XU Xiaoyuan, YAN Zheng, et al. Prospect of renewable energy integrated distribution network operation in the power Internet of Things[J]. Power System Protection and Control, 2022, 50(2): 176-187.

[22] 黄伟,左欣雅,刘弋铭.基于多区块链结构的综合能源系统调度构架[J].电力系统自动化,2021,45(23):12-20.
HUANG Wei, ZUO Xinya, LIU Yiming. Multiple blockchains based dispatching architecture for integrated energy system[J]. Automation of Electric Power Systems, 2021, 45(23): 12-20.

[23] 龚钢军,张桐,魏沛芳,等.基于区块链的能源互联网智能交易与协同调度体系研究[J].中国电机工程学报,2019,39(5):1278-1290.
GONG Gangjun, ZHANG Tong, WEI Peifang, et al. Research on intelligent trading and cooperative scheduling system of energy Internet based on blockchain[J]. Proceedings of the CSEE, 2019, 39(5): 1278-1290.

[24] 李建华.能源关键基础设施网络安全威胁与防御技术综述[J].电子与信息学报,2020,42(9):2065-2081.
LI Jianhua. Overview of cyber security threats and defense technologies for energy critical infrastructure [J]. Journal of Electronics & Information Technology, 2020, 42(9): 2065-2081.

[25] 许鹏,何霖.新型电力系统下5G+云边端协同的源网荷储架构及关键技术初探[J].四川电力技术,2021,44(6):67-73.
XU Peng, HE Lin. Preliminary discussion on source-grid-load-storage architecture and key technology based on 5G+cloud-edge-terminal cooperation in new power system [J]. Sichuan Electric Power Technology, 2021, 44(6): 67-73.

[26] 朱世顺,鲁勇,高鹏.电力工业控制领域5G安全防护框架研究

[J].计算机科学与探索，2020，14(3)：90-95.
ZHU Shishun，LU Yong，GAO Peng. Research on 5G security protection framework in power industry control field[J]. Journal of Frontiers of Computer Science & Technology，2020，14(3)：90-95.

[27] 2021年上半年全球高级持续性威胁(APT)研究报告[R/OL].[2022-06-27].https://cert.360.cn/report/detail? id=6c9a1b56e4ceb84a8ab9e96044429adc.
Global advanced persistent threat (APT) research report for the first half of 2021[R/OL]. [2022-06-27]. https://cert.360.cn/report/detail? id=6c9a1b56e4ceb84a8ab9e96044429adc.

[28] 国家互联网应急中心态势报告[R/OL].[2022-06-27].https://www.cert.org.cn/publish/main/46/index.html.
Situation report of State Internet Emergency Center[R/OL]. [2022-06-27]. https://www.cert.org.cn/publish/main/46/index.html.

[29] 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.
MEI Wenming，LI Meicheng，SUN Wei，et al. Terminal security access technology for distributed new energy networks [J]. Power System Technology，2020，44(3)：953-961.

[30] 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.
WANG Yufei，LI June，LIU Yanli，et al. Staged failure tolerance based early warning method for cascading failures in power grid caused by coordinated cyber attacks[J]. Automation of Electric Power Systems，2021，45(3)：24-32.

[31] 国务院.关键信息基础设施安全保护条例[EB/OL].[2022-06-27]. http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm.
The State Council. Regulations on the security protection of key information infrastructure [EB/OL]. [2022-06-27]. http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm.

[32] 国家能源局.电力安全生产“十四五”行动计划[EB/OL].[2022-06-27].http://zfxxgk.nea.gov.cn/2021-12/08/c_1310442211.htm.
National Energy Administration. “Fourteenth Five-Year Plan” action plan for safe production of electric power [EB/OL]. [2022-06-27]. http://zfxxgk.nea.gov.cn/2021-12/08/c_1310442211.htm.

[33] 国家能源局发布2022年全国电力工业统计数据[EB/OL].[2023-01-18]. http://www.nea.gov.cn/2023-01/18/c_1310691509.htm.
National Energy Administration released national electricity industry statistics in 2022 [EB/OL]. [2023-01-18]. http://www.nea.gov.cn/2023-01/18/c_1310691509.htm.

[34] 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.
XIE Linjiang，MAO Zhengxiong，LUO Zhenyu. Analysis of typical information security threats and countermeasures of new power system in digital transformation[J]. The Journal of New Industrialization，2022，12(3)：191-193.

[35] ROSE S，BORCHERT O，MITCHELL S，et al. Draft NIST special publication 800-207 zero trust architecture[EB/OL]. [2022-11-21]. https://www.nist.gov/news-events/news/2019/09/zero-trust-architecture-draft-nist-sp-800-207-available-comment.

[36] CUNINGHAM C，HOLMES D，POLLARD J. The eight business and security benefits of zero trust[EB/OL]. [2022-11-21]. https://www.forrester.com/report/The-Eight-Business-And-Security-Benefits-Of-Zero-Trust/RES134863.

[37] 邬江兴.论网络空间内生安全问题及对策[J].中国科学：信息科学，2022，52(10)：1929-1937.
WU Jiangxing. Cyberspace’s endogenous safety and security problem and the countermeasures [J]. Scientia Sinica (Informationis)，2022，52(10)：1929-1937.

[38] 邬江兴.网络空间拟态防御研究[J].信息安全学报，2016，1(4)：1-10.
WU Jiangxing. Research on cyber mimic defense[J]. Journal of Cyber Security，2016，1(4)：1-10.

[39] CHEN J J，YANG L. Special section on privacy computing：principles and applications [J]. Information Sciences，2020，527：293.

[40] 张平，郑征，张琳娟，等.面向配电网业务的5G通信技术适配性研究[J].电力信息与通信技术，2023，21(1)：26-33.
ZHANG Ping，ZHENG Zheng，ZHANG Linjuan，et al. Research on the adaptability of 5G communication technology for distribution network businesses [J]. Electric Power Information and Communication Technology，2023，21(1)：26-33.

[41] 强奇，武刚，黄开枝，等.5G安全技术研究与标准进展[J].中国科学：信息科学，2021，51(3)：347-366.
QIANG Qi，WU Gang，HUANG Kaizhi，et al. Survey on research and standardization of 5G security technology [J]. SCIENTIA SINICA Informationis，2021，51(3)：347-366.

[42] JI X S，HUANG K Z，JIN L，et al. Overview of 5G security technology[J]. Science China Information Sciences，2018，61(8)：081301.

[43] TAO J S，UMAIR M，ALI M，et al. The impact of Internet of Things supported by emerging 5G in power systems：a review [J]. CSEE Journal of Power and Energy Systems，2019，6(2)：344-352.

周劼英(1977—)，男，博士，教授级高级工程师，主要研究方向：电力监控系统网络安全、调度自动化。E-mail：zhou-jieying@sgcc.com.cn

张　晓(1988—)，男，博士，高级工程师，主要研究方向：电力监控系统网络安全、调度自动化。E-mail：zhang-xiao@sgcc.com.cn

邵立嵩(1974—)，男，通信作者，硕士，高级工程师，主要研究方向：电力二次系统安全防护、网络安全。E-mail：18610456416@163.com

（编辑　杨松迎）

Challenges and Prospects of Cyber Security Protection for New Power System

ZHOU Jieying[1], *ZHANG Xiao*[1], *SHAO Lisong*[2], *YING Huan*[3]

(1. National Power Dispatching and Control Center, State Grid Corporation of China, Beijing 100031, China;
2. NARI Group Corporation (State Grid Electric Power Research Institute), Nanjing 211106, China;
3. China Electric Power Research Institute, Beijing 100192, China)

Abstract: Constructing the new power system is an important development direction of national energy strategy of China, and ensuring the cyber security of the new power system is very significant. First, this paper deeply analyzes the cyber security risks introduced by the changes in the power supply structure, grid form, business model, and technical basis in the environment of the new power system. Then, combined with the existing cyber security protection measures, the cyber security protection requirements for the new power system are proposed in terms of trusted access, intelligent perception, precise protection and linked response. Finally, the key technologies of future new power system cyber security involving access security, endogenous security, data security, communication security, security assessment and simulation verification and other key research and application directions are discussed and prospected.

This work is supported by State Grid Corporation of China (No. 5108-202325046A-1-1-ZN).

Key words: new power system; renewable energy; cyber security; protection; intelligent perception