分布式新型储能场景下电力系统网络安全防护体系研究

王　蕊[1,2]，王　尊[1,2]，董良遇[1,2]，李　杨[1,2]，赵佳宁[1,2]，张进杰[3]

（1. 国家工业信息安全发展研究中心，北京　100040；
2. 工业信息安全感知与评估技术工业和信息化部重点实验室，北京　100040；
3. 北京化工大学　高端压缩机及系统技术全国重点实验室，北京　100029）

摘　要：分布式储能系统结构繁杂，设备数量规模庞大。阐述了分布式新型储能应用场景下电力系统可能面临的设备、网络、数据安全与隐私保护、供应链等方面的网络安全风险，并对其信息安全威胁以及信息安全需求进行分析，最后针对不同的网络安全风险提出相应的应对建议并给出新型储能电力系统网络建设方案，结合区块链技术保障新型储能系统的数据安全。

关键词：分布式；新型储能；网络安全；防护体系

中图分类号：TP309　　**文献标识码：**A　　**DOI：**10. 19358/j. issn. 2097－1788. 2024. 04. 002

引用格式：王蕊，王尊，董良遇，等. 分布式新型储能场景下电力系统网络安全防护体系研究［J］. 网络安全与数据治理，2024，43(4)：12－18.

Research on network security protection system of power system under distributed new energy storage

Wang Rui[1,2], Wang Zun[1,2], Dong Liangyu[1,2], Li Yang[1,2], Zhao Jianing[1,2], Zhang Jinjie[3]

(1. China Industrial Control Systems Cyber Emergency Response Team, Beijing 100040, China;
2. Key Laboratory of Industrial Information Security Perception and Evaluation Technology, Ministry of Industry and Information Technology, Beijing 100040, China; 3. State Key Laboratory of High-end Compressor and System Technology, Beijing University of Chemical Technology, Beijing 100029, China)

Abstract: The distributed energy storage system has a complex structure and a large number of devices. This article elaborates on the network security risks that the power system may face in terms of equipment, network, data security and privacy protection, supply chain, and other aspects in the application scenario of distributed new energy storage. It analyzes the information security threats and information security needs, and finally proposes corresponding response suggestions for different network security risks. A new energy storage power system network construction plan is proposed, combined with blockchain technology to ensure the data security of the new energy storage system.

Key words: distributed; new energy storage; network security; protection system

0　引言

在创新驱动发展战略的政策指导下，国家开始逐渐鼓励新型储能技术的发展。2016 年国家能源局最早提出用户侧储能参与调峰调频辅助服务，且规定了用户侧储能的电力交易。近年来，国家也发布了多项政策促进新型储能发展。2022 年国家能源局、发改委印发《“十四五”新型储能发展实施方案》，提出到 2025 年，新型储能将由商业化初期进入到规模化发展阶段，且提出电化学储能技术性能进一步提高，系统成本降低 30% 以上[1]。

分布式储能系统结构繁杂，其所包含的设备数量规模也较大，使得分布式储能系统存在网络安全风险，如边界混乱、智能设备风险、运维安全风险等。例如 2018 年的比利时电网攻击事件以及 2020 年的新西兰电网攻击事件，都是攻击者成功入侵电网控制中心的网络，通过篡改数据来破坏分布式系统设备，进而导致部分区域断电。因此，本文通过阐述在分布式新型储能应用场景下电力系统可能面临的网络安全风险，并对其信息安全威

胁以及信息安全需求进行分析，最后针对不同的网络安全风险提出相应的应对建议并给出新型储能电力系统网络建设方案，同时结合区块链技术来保障新型储能系统的数据安全，共同确保分布式新型储能系统可靠、安全、高效稳定运行。

1 新型储能应用场景

1.1 新型储能典型场景特点

根据分布式新型储能系统在电力系统中的安装位置，其应用场景可分为配电网侧、电源侧和用户侧，具体设计如图 1 所示。在不同场景分别配置新型储能系统，电源侧部署分布式电站，与新型储能系统共同构成一个分布式网络结构，再通过区块链技术共同维护场景运行的安全稳定。

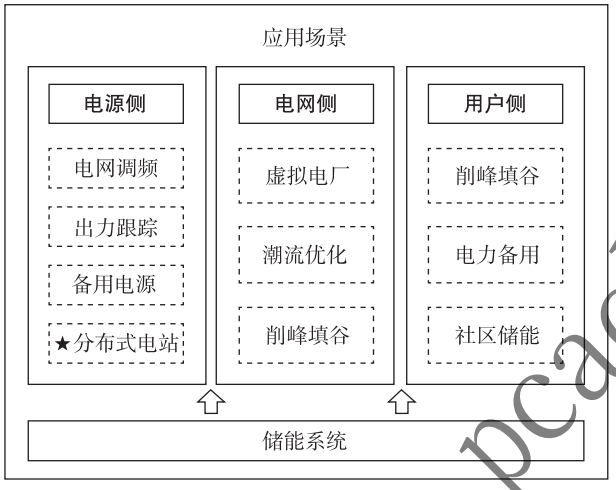

图 1 新型储能系统应用场景

1.2 分布式网络结构

分布式新型储能应用场景使用了分布式网络结构，其网络结构应用于电力系统会有很大的优势，但也存在一些缺点。本节将阐述分布式网络结构的优缺点，并分析其对电力系统所产生的影响。

1.2.1 分布式网络结构的优点

弹性和容错性：传统的中央化电力系统存在单一节点故障可能导致大规模停电的风险。而在分布式网络结构中，单点故障影响小且快速恢复能力强。电力生产和消费被分散到多个节点上，一个节点的故障不会对整个电力系统产生严重的影响，分布式网络结构下的其他节点可以迅速响应并接管电力供应。在这样的网络结构下，可以大幅度缩短电力中断的时间，减少停电范围以及给用户带来的不便，提升了电力系统的安全性。同时分布式网络结构具有更好的弹性调度能力，可以更灵活地进行电力调度和平衡。当某个区域需求增加或能源供应不足时，系统可以通过调节其他节点的电力输出来满足需求，以减轻单一节点的压力。

去中心化：传统的中央化电力系统通常需要进行长距离输电，输电过程会有一定的能量损耗。而分布式网络结构可以减少输电线路的长度，从而降低了输电损耗。在能源方面，电力系统使用分布式网络结构还可以更好地集成和管理分布式可再生能源，能够更好地实现能源的有效利用和经济效益，促进可持续能源发展。采用去中心化分布式网络结构的电力系统可以减少对大型发电厂和电网的依赖，降低了基础设施建设和运营成本。

节点自治性：在分布式网络结构中，每个节点具有一定的自治能力和决策权。节点可以根据自身的状态、信息和算法独立地做出决策，并与其他节点进行交互和协调。在给定的电力系统约束范围内，每个节点可以根据本地的能源产生情况、需求符合和电价等信息，自主地管理和优化能源的分配和使用。节点可以根据自身条件和策略，决定何时发电、储能、消耗或者进行能源交易，有利于能源的管理和优化。同时，节点自治性使得电力系统可以实现分布式的负载均衡，各节点根据自身的负载情况动态地调整能源的供应和接受，以平衡整个系统的负荷。自治性还可以帮助节点自主进行故障检测和处理，提高系统的稳定性和容错性。

数据共享与传输：节点之间可以共享数据和资源，进行数据交换与传输，这使得分布式网络能够更高效地处理和存储大量数据，同时支持并行计算和协同工作。通过数据共享与传输，节点可以获取其他节点的能源产生、消耗和存储等信息，这有助于实现整个电力系统的能源流动可视化，可以实时监测能源在系统中的流动和分布情况。用户也可以更清楚地了解电力系统的状态和效率，从而做出更合理的能源管理决策。同时，分布式网络结构的这个特性还可以帮助节点获取其他节点的历史数据和实时数据，这些数据可以用于能源消耗分析、趋势预测和负荷预测等任务，节点以此来更好地规划和管理能源，提高电力系统的效率和可靠性。

1.2.2 分布式网络结构的缺点

复杂性：分布式电力系统需要综合考虑配电网侧、电源侧、输电线路和用户侧之间的关系，这存在一定的设计难度。需要确定适当的节点配置、传输能力和通信协议，才能满足电力供需的需求。而且将分布式电力系统部署到现实环境中涉及物理设备的安装、连接和配置。在电力系统中，这可能涉及建设和维护发电厂、变电站、输电线路和配电设备等基础设施。由于系统规模庞大且涉及多个地点和供应商，会导致协调和调度工作更加复

杂，成本也会更高。

通信延迟：分布式电力系统中的节点需要进行实时通信和数据交换，以便进行协调、调度和故障诊断等操作。但由于分布式系统中节点数量众多且分布广泛、数据在分布式网络结构中需要通过网络传输，都可能会导致延迟和带宽限制。节点之间的通信可能会受到网络拥塞、信号干扰等因素的影响，会导致决策和控制的反应时间延迟，影响系统的实时性和灵敏性。

一致性：在分布式网络结构中，多个节点同时访问和修改共享数据时，一致性问题至关重要，特别是在涉及供电网络状态、负载平衡、故障处理等方面。如果分布式网络结构采用弱一致性模型或存在一致性调整的问题，会导致数据之间的不一致，给电力系统的运行带来困难和风险。

1.3 网络安全防护需求

随着分布式设备终端的广泛接入和网络边界的不断延拓，数据交互方式和需求剧增，电力系统的风险暴露面日益扩大，网络和数据安全隐患急剧增加。同时，区块链、云计算等新兴数字技术的广泛应用，使得电力系统在传统网络攻击的威胁下，还面临新的风险和挑战。因此，分布式新型储能场景下的电力系统网络安全防护需要构建一个全面综合的体系架构，进一步围绕设备与网络安全防护、数据安全与隐私保护、供应链安全、新兴技术安全等方面，优化防护策略机制，完善安全管理与运维措施，提升网络安全防护能力，满足分布式新型储能系统业务与应用安全防护需求，保障电力系统与网络的安全稳定运行[2-3]。

2 新型储能信息安全防护技术研究现状

2.1 国外新型储能系统信息安全防护技术研究现状

国外学者针对电力系统新型储能信息安全问题的防护技术进行了相应的研究工作。文献［4］基于通过部署储能系统来实现未来清洁能源的背景，实现了一个准确且可公开访问的储能数据库（Global Energy Storage Database，GESDB），旨在提供高质量以及准确的数据，同时设计了数据保护方案，最大程度地减少数据安全问题。文献［5］探讨了如何通过管理包括安全、供应链、健康检测、数据共享和能源交易在内的关键活动和任务，将区块链技术应用于新型储能系统，并证明应用区块链技术后系统安全性得到了较大的提升。文献［6］发现可以通过将虚假数据注入系统负载来破坏分布式电力系统，为此研究了通过对破坏系统建模为混合整数线性规划问题，求解出解决方案以便系统在发生安全故障前后优化成本相等。文献［7］在尖端能源技术快速发展的背景下，为了辅助现代电力系统拥有更优的能力来控制分布式发电系统、新型储能系统，提出了一种独特的方法和集成的软件解决方案，还处理了智能现代新型能源环境交换数据和数据存储的安全性问题。随着新型电池储能系统数量的增加，这些系统遭受网络安全攻击的风险也相应提高，因此，文献［8］通过测试可能潜在的隐型攻击并证明其可行性，探讨了对新型储能系统进行安全防护的策略。

2.2 国内新型储能系统信息安全防护技术研究现状

国内学者也积极开展新型储能系统信息安全防护技术的研究。由于能源物联网呈现出分布式、智能化和集成化的趋势，大量且多样的能源数据也随之产生，而这些数据存在很多安全风险，如数据丢失、窃取、篡改等，在此背景下，文献［9］提出了一种基于区块链的能源物联网数据可信和收集技术，以提高能源物联网以及储能系统的安全性和可靠性。文献［10］基于大数据背景下电力物联网在频繁的数据交互过程中容易受到监视、篡改、伪造等攻击，将公钥加密与数字签名相结合，提出了一种基于身份的组合加密与签名的集成方案。文献［11］在“双碳”目标的指引下，为了解决分布式新型储能系统的实时、安全、可靠监控，提出了一种基于5G的分布式新型储能实时监控系统，以减少数据的交互时延，确保信息安全。文献［12］发现对储能系统的深度神经网络的对抗性攻击会严重误导电力系统的负荷预测，研究通过在储能系统中开发算法来抵御对抗性攻击，并阐述了新算法应用于储能系统后的抵抗攻击的能力。文献［13］从能源电力系统面临的信息安全威胁角度出发，设计了能源互联网环境下分布式储能系统的体系架构，分析了分布式储能系统信息安全防护对策，并通过构建的分布式储能系统平台进行信息安全防护配置和应用实施分析，为分布式储能系统的信息安全提供保障。

3 基于分布式新型储能的电力系统网络安全防护体系

本节根据1.3节所分析的新型储能应用场景面临的网络安全风险给出新型电力系统网络安全防护架构，如图2所示，并针对所面临的网络安全风险提出针对性防护建议。

3.1 设备安全防护策略

物理环境安全防护：新型储能系统所存在的环境应通过配置电子门禁、防盗、视频监控等系统来加强进出管理，并对这些监测系统配置逻辑隔离、入侵检测等安全防护措施。开放环境还可以建立无人机防御系统，防止非法侵入的无人机获取敏感数据，损坏或扰乱电力系统。

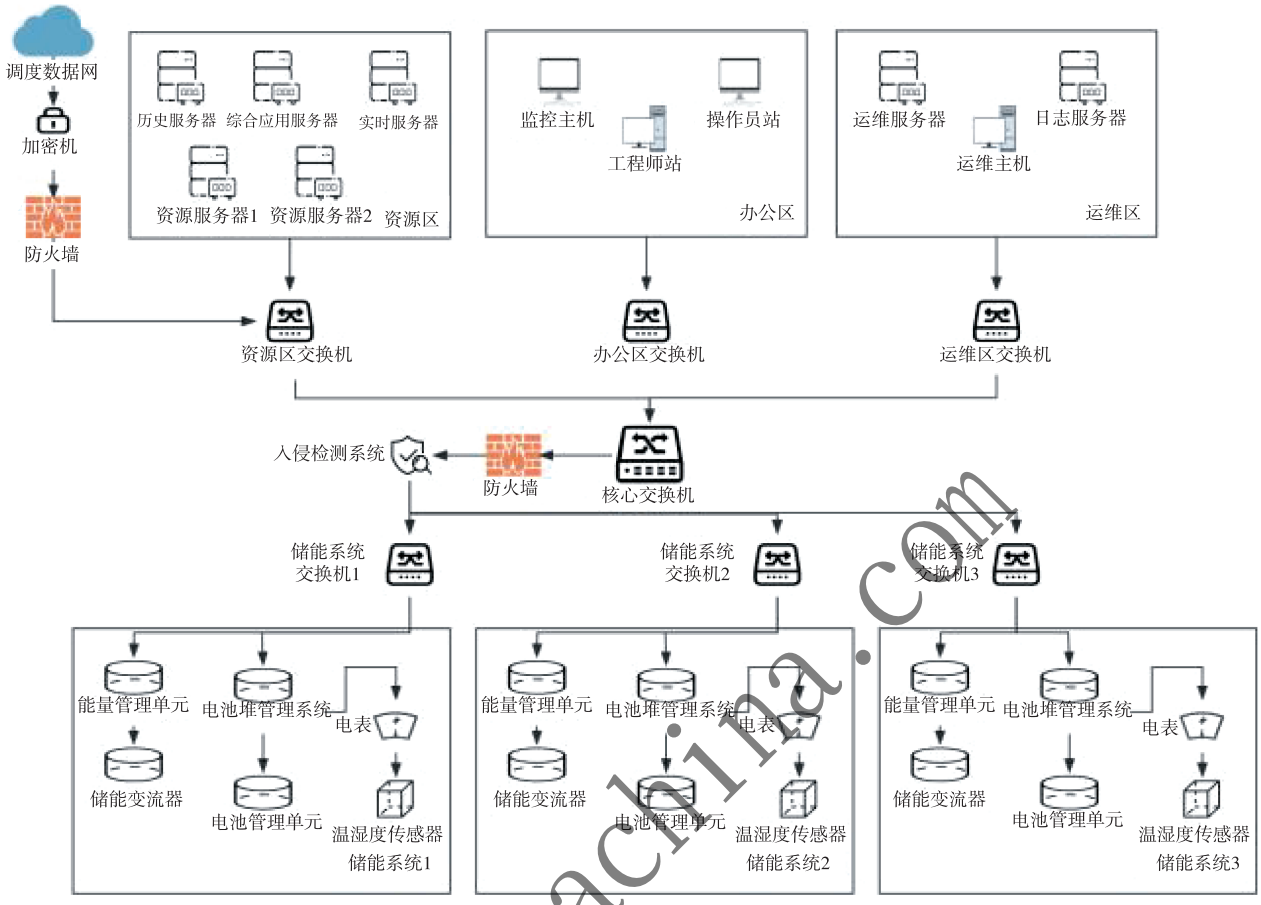

图 2　新型储能系统网络安全防护架构图

计算环境安全防护：针对智能设备风险，通过主站、厂站电力系统统一恶意代码防护管控，实现恶意代码的集中监视和远程查杀，增强恶意代码防范能力。禁止生产控制大区与管理信息大区共用一套恶意代码防范服务；对各个区域的储能系统进行周期性漏洞检测，在安全事故发生之前为管理员提供漏洞分析报告和修补建议。同时进行身份与权限管控，逐步对新型储能系统相关设备、管理员等实施统一身份管理，它们在通过合法认证具备唯一且权威的标识后，方具备请求资源和接入的条件，这样可以避免以接入的设备为跳板的攻击行为；依据对新型储能系统各主体的信任评价以及系统环境的风险评估，结合用户访问业务及业务操作权限，动态控制对相应业务资源的访问与操作，禁止越权的资源访问。

3.2　网络安全防御机制

边界防护：需进行安全区域划分来实施边界防护措施。梳理系统网络架构，按照电力系统工控网络架构进行划分，针对新型储能场景下的需求，在各安全区域边界的数据通信处部署工业防火墙，对边界流量进行控制。同时进行身份验证、权限验证避免未授权访问、身份伪造等网络安全漏洞。

网络架构：针对分布式网络的安全漏洞扩散风险，可以通过网络隔离技术实现安全防护。在图 2 架构图中，不同的新型储能系统被划分成不同的网络区域，通过网络隔离来减少攻击者在系统中传播的能力，例如防火墙、子网划分等；针对信任和身份验证问题，可以使用公钥基础设施（Public Key Infrastructure，PKI）非对称加密技术，让每个节点都有一个唯一的公私钥对，节点用私钥进行签名，其他节点可以通过该节点的公钥来进行身份验证。同时要确保密钥生成的空间足够大、密钥足够长以避免暴力破解攻击。

通信传输：宜使用超文本传输安全协议（Hypertext Transfer Protocol Secure，HTTPS），在面对一些常见的中间人攻击时，使用 HTTPS 协议仍能提供较好的防御。如果通信使用了安全套接层（Secure Socket Layer，SSL）或安全传输层（Transport Layer Security，TLS）协议，应确保禁用不安全的 SSL/TLS 协议。同时应做好相关人员的网络安全意识，不点击恶意链接或不明的电子邮件，不在系统网络上发送敏感数据等。

3.3 数据安全与隐私保护策略

数据资产识别：对数据进行分类、分级、分区。综合考虑数据性质、结构及存储模式进行分类；综合考虑电网生产运行和各专业管理等因素，根据数据遭到篡改、破坏、泄露或者被非法获取、非法利用后的危害程度，对数据进行分级；明确数据归属的安全区，避免高安全区的数据在低安全区使用、传输，避免核心数据库区互联，同时确保低安全区使用高安全区的数据时采用数据脱敏、水印等措施防止数据泄露，确保数据可溯源。

数据安全保护：对数据进行全周期保护。各阶段及其重点防护内容如图3所示，在数据分类分级分区的基础上，对数据采集、传输、存储、使用、交换、销毁等全生命周期重要环节进行加密解密、签名验签、敏感数据识别、认证、访问控制、审计、水印、数据脱敏等安全防护和管控。

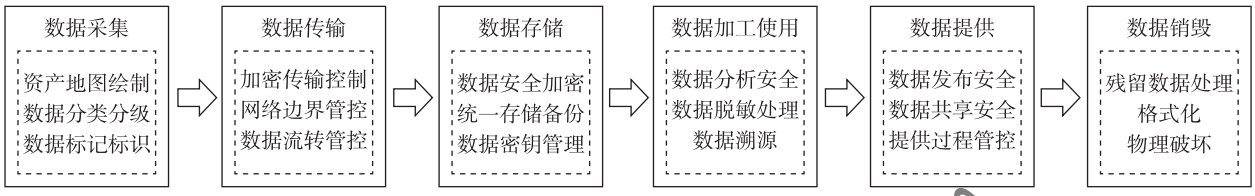

图3 数据全周期保护图

数据安全监测：应面向数据全生命周期建立安全监测机制，监测数据来源、传输过程、存储载体、数据范围、量级、流向出口等信息，确保数据流转过程中的可溯源、可审计，针对不同安全级别的数据制定差异化的预警策略；应具备识别分析数据安全风险、对异常数据操作行为进行监测和预警的能力，防止数据被篡改、勒索。

数据安全响应：应在数据安全监测的基础上，实现泄露数据自动溯源；宜基于安全事件告警将不同安全组件的防护能力按照一定逻辑关系组合，联动网络安全及数据安全基础设施，采取相应处置措施自动响应特定数据操作，实现数据安全风险由人工处置向在线智能防御转变。数据安全事件溯源流程如图4所示。

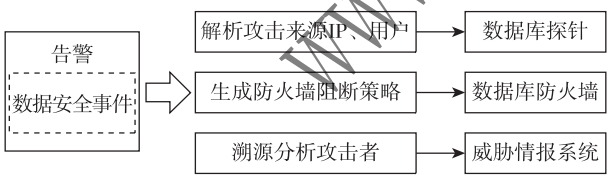

图4 数据安全事件溯源流程图

3.4 供应链安全防御策略

建立系统供方管理体系：电力系统应根据自身业务情况，建立相应的系统供方管理制度、软件供方评价标准及安全框架。同时应督促供方按国家有关要求做好保密工作，防止关键技术泄露。

供方资质评估：根据制定的系统供方评估模型和相关标准，对符合要求的系统供方进行尽职调查，从企业资质、行业影响力、技术创新能力、系统交付质量、应急响应能力等多个维度进行综合资格评估。

供方产品安全风险评估：对供方系统产品进行安全基线分析和安全风险评估，针对软件潜在的安全漏洞、风险以及可能造成的影响进行评估，确保产品安全。系统入网前应通过专业检测机构的网络安全技术检测，检测内容应包括源代码审计、固件安全检测、组件版本审计等，还应通过国家能源局指定的专业检测机构开展的专项检测。同时应当逐步推行设备到货抽检及在运设备定期抽检，防范逻辑问题、恶意代码预制等供应链风险。

供方退出管理：供方合同结束时，应对合同进行复核，确保所有义务都已经得到履行，随后进入退出程序，仔细考虑数据保存和处置。系统退役后，应采用合理渠道进行报废回收或物理销毁，防止随意流入市场进行二次销售。

3.5 运维防护实施措施与安全管理

网络运维方面：宜构建与业务网络分离的统一安全运维网络；应采用安全运维网关进行系统运维，如采用远程运维，应做好配套安全保障。运维人员应使用专用运维工具进行工作检修，包括对串口进行运维、禁止终端具备网络蓝牙等，同时对运维操作进行日志审计。

移动介质管控方面：宜建立移动介质的统一摆渡机制，结合事前杀毒、事中管控、事后审计等手段加强对移动介质摆渡的统一管控；加强对移动介质摆渡过程中的身份权限认证，防范通过移动介质进行数据摆渡过程中的误操作、越权操作、病毒与恶意代码感染、运维账号口令泄露等网络安全风险。

安全测评方面：严格开展网络安全评估，系统在上线投运之前、升级改造之后必须进行安全评估；已投入运行的系统应该定期进行安全评估和等保测评，评估结果应当及时向上级主管部门汇报、备案。

攻防演练方面：实行常态化攻防演练，新型储能系

统应制定应急处理预案，并围绕关键业务的可持续运行设定演练场景，结合沙盘、靶场、实网等环境，定期组织开展攻防演练及渗透测试。

人员管理方面：应加强网络安全防护人员的配备，设立安全主管、安全管理等岗位，配备安全管理员、系统管理员和安全审计员，明确各岗位职责；应对关键岗位人员进行严格的身份背景、专业资格和资质审查；解除内部敏感信息第三方人员应当签署保密协议；应当严格落实关键岗位人员离岗管理。特别要加强对厂家维护及评估检测等第三方人员的安全管理，提高全体内部人员和相关外部人员的安全意识。

3.6 新兴技术安全防护策略

3.6.1 区块链

分布式新型储能应用场景使用联盟链技术将所有储能系统以及用户连接，使用权威证明共识机制（Proof of Authority，PoA），事先制定好授权节点和非授权节点，同时使用智能合约，将储能租用协议以代码的形式存储到区块链内，来保证交易的透明公开、安全高效。为了避免可能存在的安全风险，应该严格审查 PoA 权威证明共识机制下的授权节点；引入多重签名机制，减少个别节点的恶意行为。同时还应对智能合约代码进行安全审计，避免逻辑漏洞被攻击者利用造成严重的经济损失。

共识机制防御策略：建立一个可靠的权威节点管理机制，包括严格的身份验证、访问控制和监控措施等，确保只有受信任的节点参与到 PoA 共识过程中。还要定期审查和更新节点的身份信息，及时排除潜在的风险因素。将权威节点的功能分散到多个节点上，减少单个节点被攻击的可能性，比如可以采取多签名方案，要求多个节点对交易进行验证和签名，确保交易的安全性和完整性。同时还要建立有效的应急响应机制来应对突发的安全事故。

多重签名防御策略：通过引入多重签名机制来增强交易的安全度和可信度，采取安全的密钥管理措施，例如采用硬件安全模块（Hardware Security Module，HSM）方式来保护私钥，防止被未授权的用户获取。同时还要建立有效的验证流程，确保在使用多重签名验证时，参与验证的各方都是可信的，可以使用数字证书、身份验证等技术来确保参与方的真实身份，并对其进行可靠性评估。

智能合约防御策略：在对智能合约进行代码审计前，需要对其进行全面的安全测试，包括输入验证、边界条件测试、攻击模拟等，以此尽早发现潜在的漏洞和安全隐患。其次再进行代码审查和静态分析，检查智能合约代码中是否存在安全漏洞、逻辑错误和潜在的攻击面，可使用静态分析工具来辅助审查，以便全面发现安全问题。同时要做好合约升级的演练工作，在模拟的生产环境中进行合约升级前的演练测试，可以更好地了解智能合约在实际使用中的情况，以便及时处理可能的风险。

3.6.2 云平台

云基础设施缺乏统一的安全防护要求，本文从以下三个方面简单提出一些防护建议。

业务逐步上云：主站业务系统宜逐步向云平台迁移实现集中运维，以减少分散的风险点，确保业务系统的稳定和安全性。业务终端宜逐步推广云桌面实现集中使用，采用云桌面技术将终端设备的数据和应用程序存储在云端，减少终端设备上的敏感信息，实现集中管理和控制，有助于降低数据泄露风险。重要业务系统宜基于用户私有云开发环境进行集中开发，以更好地保护关键业务数据和源代码，防止被窃取或篡改，依托云环境实现统一的集中安全管控。

内外交互控制：云平台与外界通过调度数据网进行交互时，应部署敏感数据防泄露措施，严控敏感数据下云。比如加密数据传输、访问控制和数据备份等，确保敏感数据在传输过程中不被窃取或篡改。还应部署恶意代码防范措施，严防外部恶意代码上云。例如使用自动化工具扫描恶意代码，并及时更新和维护系统的安全补丁，防止已知漏洞被恶意代码利用。

内部隔离监视：在运维监控平台系统中的云平台服务器配置了隔离装置，实现不同虚拟网络之间的资源隔离，保证信息系统的通信接口经授权后方可传输数据。例如可以使用虚拟局域网或软件定义网络（Software Defined Network，SDN）技术，将不同的业务或用户划分到独立的网络区域，以防止横向拓展攻击，从而保护系统不受内部网络的威胁。同时对进出网络的流量实施有效监控，以阻止可疑流量或自动隔离存在安全威胁的资源。

3.7 安全部署防护能力对比验证

针对上述电力系统新型储能场景，使用自建模拟平台进行仿真验证，搭建城市供电场景，针对图 2 中的工程师站开放的特定端口，注入远程代码执行攻击，未部署防护措施时，断路器和综合电能表会因遭受远程代码执行攻击而出现宕机故障并出现告警，位于储能系统的综合电能表终端示数为 38.05 A，示数显示异常。在储能系统边界部署入侵检测系统等安全防护系统后，再次进行重放攻击，系统对异常流量进行有效拦截，断路器和综合电路表未产生告警，综合电能表示数为 20.85 A，属于正常范围，新型储能系统维持良好运行状态。

通过模拟仿真验证，证实了部署防护措施对于保护电力系统新型储能场景的重要性以及新型储能系统网络

安全防护架构的可行性。通过加强电力系统的网络安全防护工作，来确保电力系统的稳定性和可靠性，推动新型储能应用的可持续发展。

4 结论

分布式新型储能应用场景的构建改变了传统电力系统的架构，对现有的电力系统网络安全保护体系提出了巨大挑战。本文分析了在新型储能应用场景下可能会面临的网络安全风险，针对这些安全风险构建了网络安全防护体系，并针对每种类型的安全风险提出一些安全防护建议。最后通过模拟仿真验证，证实了新型储能系统网络安全防护架构的可行性。

参考文献

[1] 国家发展改革委 国家能源局关于印发《“十四五”新型储能发展实施方案》的通知［EB/OL］.（2022－01－29）［2024－03－10］. https：//www. gov. cn/zhengce/zhengceku/2022－03/22/content_ 5680417. htm.

[2] 周劼英，张晓，邵立嵩，等. 新型电力系统网络安全防护挑战与展望［J］. 电力系统自动化，2023，47（8）：15－24.

[3] 杨逸岳，付志博，肖啸. 解析电力系统网络安全架构［J］. 电子技术与软件工程，2020（22）：247－248.

[4] TAMRAKAR U，BASTOS A F，ROBERTS-BACA S，et al. Global energy storage database：enhancing features and validation procedure［C］//2022 IEEE Electrical Energy Storage Application and Technologies Conference（EESAT），Austin，TX，USA，2022：1－5.

[5] OCHOA J J，BERE G，AENUGU I R，et al. Blockchain-as-a-Service（BaaS）for battery energy storage systems［C］//2020 IEEE Texas Power and Energy Conference（TPEC），College Station，TX，USA，2020：1－6.

[6] RIZI D T，NAZARI M H，HOSSEINIAN S H，et al. Evaluation of false data injection to meters in developed energy hub system［C］//2023 5th International Conference on Optimizing Electrical Energy Consumption（OEEC），Tehran，Iran，Islamic Republic of，2023：45－49.

[7] ORTIZ A P，PATERNO G，LAZZARO M，et al. Smart ICT framework for the intelligent management of different modern energy systems［C］//2019 IEEE International Conference on Environment and Electrical Engineering and 2019 IEEE Industrial and Commercial Power Systems Europe（EEEIC / I&CPS Europe），Genova，Italy，2019：1－6.

[8] PASETTI M，FERRARI P，BELLAGENTE P，et al. Artificial neural network-based stealth attack on battery energy storage systems［J］. IEEE Transactions on Smart Grid，2021，12（6）：5310－5321.

[9] FAN R，YIN L，GAO S，et al. Blockchain based energy IoT data trusted collection and transmission［C］//2022 IEEE 5th International Conference on Electronic Information and Communication Technology（ICEICT），Hefei，China，2022：96－99.

[10] LIN B，GENG Z，YU F. Information security protection of Internet of energy using ensemble public key algorithm under big data［J］. Journal of Electrical and Computer Engineering，2023（6853902）.

[11] SUO S，KUANG X，CHENG R，et al. Research of real-time monitoring and control technology for distributed energy storage based on 5G［C］//2022 IEEE/IAS Industrial and Commercial Power System Asia（I&CPS Asia），Shanghai，China，2022：1496－1500.

[12] LI J，WANG J，CHEN L，et al. Defending against adversarial attacks by energy storage facility［C］//2022 IEEE Power & Energy Society General Meeting（PESGM），Denver，CO，USA，2022：1－5.

[13] 彭道刚，卫涛，姚峻，等. 能源互联网环境下分布式能源站的信息安全防护［J］. 中国电力，2019，52（10）：11－17，25.

（收稿日期：2024－03－10）

作者简介：

王蕊（1995－），女，硕士，助理工程师，主要研究方向：网络安全、代数与密码学。

王尊（1989－），男，博士，工程师，主要研究方向：工业信息安全、过程系统工程。

董良遇（1989－），通信作者，女，硕士，工程师，主要研究方向：网络安全、工业控制系统、工业互联网。E-mail：dongliangyu78@ 163. com。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部