DOI：10.13334/j.0258-8013.pcsee.232216 文章编号：0258-8013 (2025) 08-2876-23 中图分类号：TM 734；TN 915 文献标识码：A

虚拟电厂网络安全研究综述及展望

胡金炜[1]，张玉健[1*]，蔡莹[2]，余志文[2]，王琦[3]

(1. 东南大学网络空间安全学院，江苏省 南京市 210096；2. 广东电网有限责任公司广州供电局，广东省 广州市 510620；3. 东南大学电气工程学院，江苏省 南京市 210096)

Review and Prospect on Cyber Security of Virtual Power Plant

HU Jinwei[1], ZHANG Yujian[1*], CAI Ying[2], YU Zhiwen[2], WANG Qi[3]

(1. School of Cyber Science and Engineering, Southeast University, Nanjing 210096, Jiangsu Province, China;
2. Guangzhou Power Supply Bureau of Guangdong Power Grid Co., Ltd., Guangzhou 510620, Guangdong Province, China;
3. School of Electrical Engineering, Southeast University, Nanjing 210096, Jiangsu Province, China)

ABSTRACT: Virtual power plants (VPPs), as an emerging type of power system, significantly improve the grid's resource aggregation capability. However, when integrating and dispatching numerous energy resources, VPPs still face challenges including expanded attack surfaces, increased vulnerabilities, and severe failure consequences. This paper first clarifies VPPs' definition and structure, analyzes security requirements concerning operational vulnerabilities, and proposes corresponding security metrics. It then examines the evolution and development trends of cybersecurity in power systems, summarizes existing security hardening methods and practices, and identifies VPP-specific potential security threats. Building on this foundation, a five-dimensional security defense system is proposed, addressing VPPs' device, access, communication, data, and operational aspects. Specific security measures applicable to VPPs are analyzed. Finally, the application prospects of three emerging security technologies i.e. zero trust, situational awareness, and blockchain in virtual power plants are explored.

KEY WORDS: virtual power plant (VPP); cyber security; zero trust; situation awareness; blockchain

摘要：虚拟电厂作为一种新型电力系统，显著提高了电网的资源聚合能力。然而，在大量能源资源整合与调度过程的同时，系统也面临攻击面扩大、脆弱性增加、失陷后果严重等问题。该文首先围绕虚拟电厂的定义与结构，针对系统运行过程中的脆弱点进行安全需求分析，并提出对应的安全指标；随后，回顾电力系统的网络安全演进和发展趋势，梳理已有的安全加固方法与经验，整理虚拟电厂潜在的安全威胁；在此基础上，从虚拟电厂设备、接入、通信、数据、运维角度提出五维安全防御体系，分析适用于虚拟电厂的具体安全措施。最后，对零信任、态势感知、区块链 3 种新兴安全技术在虚拟电厂的应用进行展望。

关键词：虚拟电厂；网络安全；零信任；态势感知；区块链

0 引言

虚拟电厂(virtual power plant，VPP)是通过数字技术聚合储能、可控负载、分布式发电机等分布式能源资源(distributed energy resource，DER)的一种新型电力系统，旨在从 DER 处获取最大收益并减少对电网电力的依赖，有利于促进城市的绿色可持续发展[1]。VPP 打破了传统电厂的局限，依赖信息通信基础设施与广泛的 DER 互联[2]，形成大型系统，实现电力的统一调度、优化与控制。由此看出，VPP 不仅是电气技术概念，也是信息技术(information technology，IT)概念[3]。VPP 作为电力系统的重要发展方向，受到世界各地的广泛关注并已开展相应的试点运行，例如，德国的 VPP 项目 Next Kraftwerke(NK)[4]、美国 Tesla 公司推出的 AutoBidder VPP 平台[5]和国内上海、冀北等地的 VPP 试点应用等[6-7]。2023 年，冀北虚拟电厂项目并网装机达到 4 110 万 kW，新能源交易电量累计突破 200 亿 kW·h，推动了绿色电力大规模运用[8]，VPP 产生的经济、社会与环境价值在不断演变中呈现多方面快速增长趋势[9]。

在 VPP 逐渐落地实施的过程中，为了保证系统运行时的鲁棒性与安全性，有必要考虑 VPP 可能遭

基金项目：南方电网公司科技项目(GDKJXM20220333)；中央高校基本科研项目(2242023K30034)。

China Southern Grid Technology Project Funding (GDKJXM20220-333); Fundamental Research Funds for the Central Universities (22-42023K30034).

受的网络安全风险，促进网络安全防御机制同步规划、同步建设、同步使用[10]。目前，直接针对 VPP 网络安全的攻击事件尚无公开报道，但电力行业中的网络安全问题并不鲜见。电力系统具有关键性与复杂性，即使采取专网专用等高强度的网络安全隔离措施，也不能完全消除相关入侵威胁，遭受攻击后不但会面临电力供应瘫痪，还可能导致严重的经济损失、环境污染和社会安全等问题。例如，2015 年，乌克兰多家配电公司遭受高级持续性威胁攻击，造成各地区约 225 000 个家庭和企业失去电力供应并持续了数小时[11]；2016 年，以色列电力局遭受了一次严重的勒索软件入侵事件，导致大量计算机被迫离线[12]；2019 年，委内瑞拉电网遭受针对电网控制中枢的网络攻击，导致多日停工停学[13]。

现有直接研究 VPP 网络安全的文献相对匮乏，而有关电力系统网络安全相关的综述工作较为丰富。文献[14]介绍了新型电力系统面临的攻击风险、安全需求与对应的发展方向，着重于对新型电力系统共性分析，而对电力网络安全发展脉络与具体攻击防御形式梳理不够充分；文献[15]分析了配电网用户侧中的局部网络风险与相关量化指标，然而对于 VPP 系统安全，需将关注点扩展到其他组件可能受到的攻击；文献[16]论述了智能电网中通信安全问题，针对通信链路维度的安全威胁总结了对应措施，而对于 VPP 网络安全还需从设备、接入、数据、运维等维度全面考虑；文献[17-18]探讨了仿真、机器学习等技术在电力网络安全中的应用，然而新兴技术的适用性以及相应效能还需结合 VPP 具体特性进一步剖析。

鉴于 VPP 本质上仍是电力系统的一种应用形式，可以基于传统电力系统中已经存在的网络安全风险和技术进行归纳分析，并结合 VPP 的新特性，评估其潜在威胁和防御手段。然而，随着信息、物理与社会侧的耦合交互[19-20]，针对电力系统的攻击向量也结合了多个层面的因素，相应的防御机制应综合考虑。进一步，VPP 一方面继承了传统电力系统的特点，另一方面呈现出网络开放、设备异构、海量接入等新特征，相应的攻击种类更多、攻击面更大，为 VPP 网络安全攻防分析带来了新的挑战。可见，VPP 网络安全问题具有复杂性，完整的解决方案需要对信息、物理和社会侧攻击防御问题进行分析，也要对三者的综合作用进行评估。本文从信息侧切入，重点梳理和展望 VPP 的网络安全问题，对于 VPP 物理侧、社会侧及其融合等的攻击防御问题，可参考相关文献[21-22]，本文暂不讨论。

本文组织结构如下：首先，从 VPP 的安全特性出发，分析 VPP 对网络安全的需求与指标；接着，全面回顾电力系统网络安全中攻击与防御手段的演进趋势；然后，探讨适用于 VPP 的五维关键防护技术；最后，对 3 种新兴安全技术在 VPP 中的应用进行展望。

1　虚拟电厂网络安全需求分析

1.1　虚拟电厂定义与系统结构

在学术界，对于 VPP 的定义尚未形成共识，存在多种不同的解释。文献[23]认为 VPP 将 DER 进行聚合，并根据 DER 具体参数与网络约束创建一个操作配置文件进行管理；文献[24]指出 VPP 是由多个分散的发电机组、可控负载和存储系统聚合形成的独特电厂；文献[25]主张 VPP 的定义应该总结为“通信”和“聚合”，即 VPP 通过通信技术与软件实现 DER 的聚合与协调优化，作为一个特殊电厂参与电力市场与协助电网运行的电源协调管理系统。本文认为，VPP 是一个利用信息技术实现的分布式能源资源管理系统，通过底层控制系统和上层能源管理系统的协同，对分布式能源资源进行协调控制和优化调度，为 VPP 参与电力市场和协助电网运行提供支持。

VPP 的系统结构可根据不同的应用场景、实际目标与约束条件进行设计，因此在不同文献的描述中存在差异。文献[26]中围绕 VPP 交易模式，根据市场主体层级与实体在电力市场的职责进行划分，分为分布式资源层与资源聚合层；文献[27]主要关注 VPP 通信体系，在传统网络架构基础上将 VPP 通信网络体系架构划分为资源层、适配层、接入层、边缘层、网络层、平台层；文献[2]将 VPP 通信架构进行二级划分，包括本地通信层与远程通信层；文献[28]总结了 VPP 信息框架结构，划分并分析 VPP 中的能源、信息与业务流。

本文针对 VPP 网络安全问题，从需要保护的实体进行逻辑抽象与层次划分，以提高模型对于各种场景的适用性与泛化能力，如图 1 所示。资源层包括各种发电设施、储能装置与可控负荷，负责能源生产、储存和使用；通信层包括网络设备、通信协议、数据接口等媒介，作为平台层与资源层数据传输的枢纽；平台层包括 VPP 控制中心、VPP 聚合

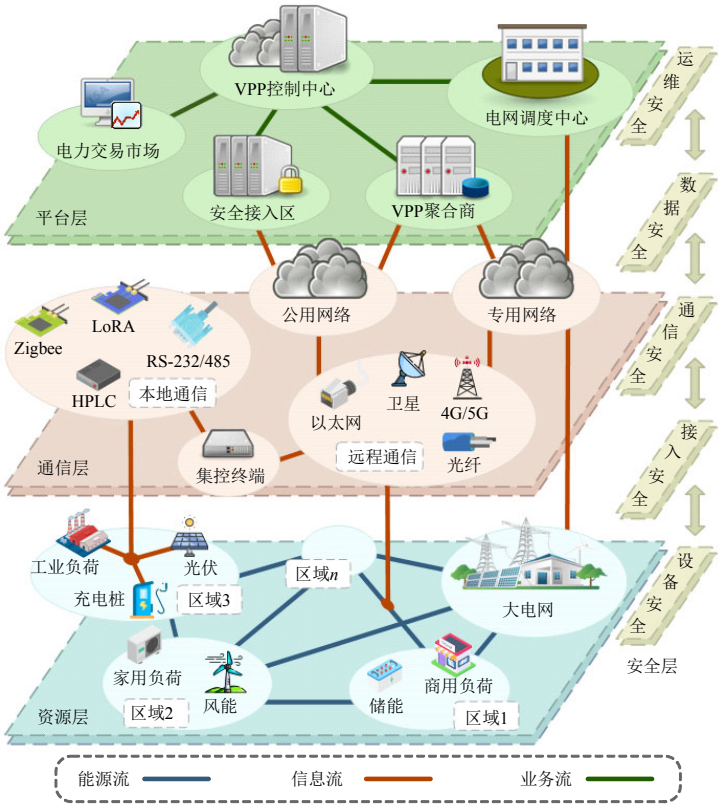

图 1 虚拟电厂系统结构

Fig. 1 VPP system architecture

商、电网调度中心等实体，负责管理、控制与聚合；安全层贯穿上下，从设备、接入、通信、数据、运维等方面为上述 3 层提供安全保障。为了统一化描述安全保护的目标，本文用“实体”指代 VPP 中可能被攻击的对象，如用户、软件、硬件或是提供服务的特定组织(如聚合商)，具体含义根据上下文有所不同。

1.2 虚拟电厂对网络安全的需求

VPP 的安全边界模糊，用户与电网的交互性强，海量异构终端和复杂的业务流程，使得该系统存在着大量的网络安全风险[29]。目前针对 VPP 网络安全尚无统一标准，本文从工控系统[30]、电力监控系统[31]、智能电网[32]等防护标准中总结经验，对相应的网络威胁进行分析[33-34]，归纳出 VPP 系统网络安全脆弱性主要来源：1）关键实体对外部威胁的防御能力不足；2）对实体能力的约束与控制不足；3）实体之间的通信信道存在安全隐患；4）对数据生命周期中出现的安全威胁考量不足；5）缺乏规范化的安全运维管理措施。

本文针对上述脆弱性形成 VPP 五维防御体系与相应需求，如图 2 所示。设备防御从实体的威胁抗性出发，定义了针对实体自身软硬件层面的安全措施；接入控制从系统资源边界的角度，定义了实体能力的活动范围；通信链路从实体间信息交换媒介出发，定义了保证信息传输安全性的方法；数据管理从数据生命周期的角度，定义了数据从生成到销毁过程中的防护要求；运维管理从系统日常运作的角度，定义了运行的安全策略与标准流程。5 个维度各有侧重同时相互关联。

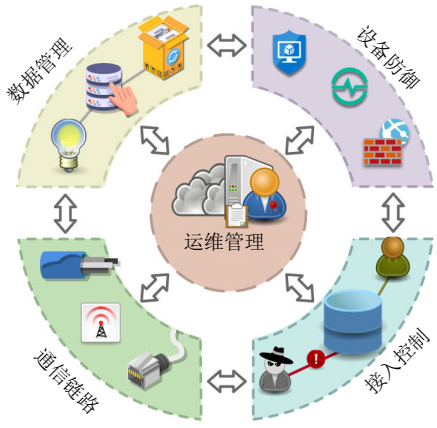

图 2 虚拟电厂五维防御体系

Fig. 2 VPP five-dimensional defense system

1）设备防御安全需求。系统设备安全包括对智能电表、VPP 控制中心等资源层和平台层中的可编程硬件与软件进行保护，通过设计合理的系统内核安全架构，持续详尽的渗透测试和错误修复等措施，使得系统能够抵御来自开放接口的主动攻击，

同时也能防御以静默方式试图学习或利用系统信息的被动攻击[35-36]。

2）接入控制安全需求。接入控制通过建立适当的身份验证和权限授予机制，限制系统中用户的访问能力和范围，是保证资源不被非法使用和访问的前提[37]。VPP 系统中，平台层与资源层之间以及同一层次之间的交互都需要先经过认证与授权的环节，并且需要考虑方案的效率、延迟、成本、开销和隐私等性能[38]。

3）通信链路安全需求。VPP 中的通信涉及有线、无线等传输介质，蓝牙、WiFi、Zigbee 等传输协议，承载着复杂的交易与调控信息[39]。除了考虑时延、丢包与带宽等通信质量限制，还需要防止通信链路受到恶意干扰或篡改，以确保通信链路的正常稳定运行[40]。

4）数据管理安全需求。数据是 VPP 进行实时决策的基础，在数据生命周期即生成、采集、存储、使用与销毁的过程中，系统内外部可能出现非法收集、篡改、破坏、利用数据的恶意行为，需要制定以数据生命周期为驱动的管理方案，保护数据的安全性与隐私性[41]。

5）运维管理安全需求。“三分技术，七分管理”也适用 VPP 网络安全场景[42]，需建立完善系统管理制度和安全审计机制，并对 VPP 运维人员进行风险评估与安全培训，以保证系统运行过程中整体安全可靠[43]。

1.3　虚拟电厂对网络安全的指标

VPP 的网络安全防护需要在信息系统背景下结合 VPP 的具体特性去分析，而信息系统以 CIA(confidentiality，integrity，availability)三元组作为基本安全模型[44]。对 CIA 的任何维度的破坏，都将对信息系统安全造成严重影响，需将其纳入系统设计的全局考虑中。以此为基础，VPP 的网络安全指标具体解释如下：

1）机密性(confidentiality)。机密性是指对信息的访问和使用进行限制的能力，确保了只有被授权的实体才能访问数据，阻止未经授权的信息访问请求。例如，智能电表计量数据[45]、分布式资源实时状态以及管理平台运营记录等信息的加密、验证与控制等。

2）完整性(integrity)。完整性是指对信息准确性进行保护的能力，确保了实体双方在交互过程中信息的真实性，阻止非法入侵者在传输、存储、处理过程中对信息的篡改、删除或伪造。例如，在用电需求发布、智能电表的窃电监测、以及 VPP 状态估计和调度操作[46]中，需要确保信息的真实与完整。

3）可用性(availability)。可用性是指系统能够不间断地进行操作和提供服务的能力，并确保了系统在遭受攻击等意外事件时功能的快速恢复。例如，VPP 中电力市场交易、调度业务运行以及设备交互通信的正常运行能力等，该指标可通过系统正常运行时间的占比进行量化[47]。

需要说明的是，CIA 的实现是 VPP 中网络安全的基本目标，VPP 中其他安全要求需要以此作为前提[48]，如资源层中要求能对各种 DER 进行实时管制的可控性要求；通信层中要求传输线路能对调控信息进行可靠交付的可达性要求；平台层中要求 VPP 控制中心能对历史行为进行全面审查，以发现系统薄弱点和事后追责的可审计性要求等。总之，CIA 三元组构成了 VPP 网络安全的基本目标，辅以对 VPP 具体部署环节网络安全要求的补充细化，才能形成完整的指标体系。

2　电力系统网络安全演进与发展趋势

2.1　传统电力网络安全

传统电网采用集成了控制和通信功能专用功率器件，使用由可靠、可预测的串行通信链路组成的封闭网络[49]。由于网络结构简单，层次结构清晰，对传统电力网络的攻击往往呈现出一种垂直性特征，具体体现在攻击过程的 3 个阶段[50]：第 1 阶段攻击者可能利用 RTU、PMU 等二次设备或电力信息系统的软硬件及协议漏洞[51]，进行信息拦截与系统入侵；第 2 阶段利用授权管理等漏洞进行权限提升，扩大其在网络系统中的操作；第 3 阶段利用系统机密性与完整性等漏洞窃取或修改数据信息，进一步影响电力系统可用性。

传统电力网络安全的防御思路主要是在 3 层防线[52]的基础上，遵循“安全分区、网络专用、横向隔离、纵向认证”的原则，将电力信息系统划分为生产控制大区和管理信息大区，使用独立的网络设备组成电力调度数据网的专用通道，数据网与外部公共信息网在物理层面上进行安全隔离，并在网络交界处设置专用的纵向加密认证装置[53]。这种水平维度上的分区管控与垂直维度上的纵深防御体系，可以在不同层次上采取措施，对各种攻击进行分层次、分阶段拦截与防范[54]。

2.2 电力物联网网络安全

电力物联网基于大量传感器和通信设备，实现系统内部实体之间的相互感知、高效协同和反馈控制，此外，泛在电力物联网概念还扩展到了人与物、物与物的互联互通，实现对电力生产、传输、消费等全过程的智能监测、控制和管理，使电力系统能够提供无处不在的服务[55-56]。表 1 对比了传统电网和电力物联网在系统架构、信息流动、网络环境、电网设备和数据规模等方面的特点[57-61]。可以看出，电力物联网拥有大量入网设备和高度复杂的网络，导致其潜在的攻击面更加广泛，攻击的影响范围更为深远，对应的网络攻击往往还具有水平性的特征。例如，攻击者可通过入侵系统的弱节点，利用其作为跳板横向移动并获取同一层次内其他节点的控制权限[62-63]。

表 1 传统电网和电力物联网特点对比

Table 1 Comparison of characteristics between traditional power grids and IoT-based power grid

类别	传统电网	电力物联网
系统架构	中心调度，集中控制	互联互通，分布控制
信息流动	单向通信，树状结构	双向通信，网状结构
网络环境	虚拟专用网或独立的物理线路	公用的互联网
电网设备	发电、变电、输电、配电等专用设备	传感器、智能开关、智能电表等通用设备
数据规模	电力负荷、电网状态、设备运行等内部数据	气象、地理、市场、公共服务等大量外部数据

电力物联网网络安全需要以“三型两网”为目标，对各环节可能的攻击方式进行分析[64]，进行数据采集、传输、分析与应用的全层次安全设计与加固[65]，形成贯穿数据全生命周期，涵盖“云+边+端”的多链条、多层次综合防护体系[66]。

2.3 虚拟电厂网络安全

VPP 融合了物理、信息、价值等多种要素，是电力物联网的具体实现形式之一[67]。与电力物联网其他应用[68]比较，VPP 形成了可对标传统电网的灵活可调聚合体，具有异构接入、控制复杂、数据海量、资源多样、市场多元等特点[69]。在网络安全方面与微电网等其他应用相比较，VPP 在规模、架构与资源等方面都展现出更复杂的特性，且需与大电网紧密互连，受到大电网调控并提供相关服务，如表 2 所示。这也意味着 VPP 面临更多更复杂的攻击向量，可能影响的资源与区域更为广泛，对整体电网安全运行产生更严重的破坏。

表 2 虚拟电厂和其他电力应用系统特点对比

Table 2 Comparison of characteristics between VPP and other power application systems

应用特点	微电网、聚合商	虚拟电厂
部署规模	小型独立系统	大型复杂系统
管理层级	一般独立管理	接受上级调度管理
资源整合	关注于局部特定资源	聚合广域多样资源
物理分布	集中于固定地理空间	大电网区域内广泛分布
运行目标	内部安全、经济用能等	主、配网的辅助支撑等
通信架构	与配电网类似、架构简单	物联网、分布式等复杂架构

由于接入终端中硬件计算环境、软件应用环境、私有通信协议等的异构性，使得接入设备既存在由软硬件漏洞和不可控性导致的“自身安全”问题，同时也面临因为互联接入过程中渗透攻击导致的“攻击防御”问题，传统针对单一设备的个性化防护手段难以奏效[70]。复杂的调控机制意味着分布式系统中信息流具有多样的分支和汇聚过程，安全问题从单个组件上升到系统节点间的互动关系，对关键节点防护需求更高[71-72]。高频并发的海量数据要求系统拥有较强通信承载能力与信息聚合能力[73]，同时也要求系统具有利用海量数据进行数据挖掘的能力，及时发现复杂网络中各种类型的攻击威胁[74]。VPP 涵盖多种类型的能源资源并支持多种类型的市场模式，网络攻击的备选目标范围更多[75]，攻击后对能源经济、关键基础设施安全的影响更为严重[76]。

VPP 融合了工控系统与 IT 系统的同时也带来了新的挑战：一方面，要求控制系统中的高可用性与实时性；另一方面，设备地理位置分散、硬件更新周期慢、技术标准化程度低等特点又增加对 IT 层面的防护复杂性。进一步，对于 VPP 的攻击手段也将继承两者的特点，表 3 对各种攻击方式的主要作用层次进行分类，总结了 VPP 中潜在的网络攻击。针对工控系统的攻击通常与底层物理环境密切关联，侧重于利用专门的漏洞和特定协议来实现对小范围控制系统的入侵和操控；而针对 IT 系统的攻击则更多地与互联网属性相关，主要通过广泛的网络可达性、软件漏洞以及人为疏忽等因素来实施大范围入侵[77-78]。而对于 VPP 的网络攻击同时结合了工控系统与 IT 系统的特点，攻击手段复杂灵活，防范更为困难。

3 虚拟电厂网络安全关键技术

3.1 安全设备防御技术

VPP 中的软硬件设备容易暴露在危险环境下，

表 3　虚拟电厂中潜在网络攻击

Table 3　Potential cyber-attacks in VPP

攻击层次	攻击名称	攻击示例	攻击影响	相关文献
资源层	控制流劫持	利用缓冲区溢出等漏洞篡改进程控制流	程序进行正常功能之外未经授权的恶意操作	[92]
	侧信道攻击	利用侧信道数据之间的依赖性分析秘密数据	关键密钥泄漏，破坏系统机密性	[83]
	能量耗尽攻击	对传感器发送大量身份验证等耗能消息	使电量有限的设备能源耗尽，破坏系统可用性	[93]
	时间同步攻击	发送伪造报文，诱使时间同步装置输出错误	破坏时间信息完整性，诱发功能闭锁和误判	[94]
	芯片安全缺陷	利用缺陷芯片中的不安全加密算法等攻击设备	关键信息泄漏和破坏，影响机密性与完整性	[95]
	无效的访问控制	利用数据接口、调试接口中越权访问等漏洞	获取终端设备权限，破坏系统机密性和完整性	[96]
通信层	弱密钥	利用 RSA 等算法中弱密钥缺陷攻击 TLS 协议	窃取加密后的通信信息，破坏系统机密性	[97]
	流量分析	通过被动网络窃听分析抽取流量特征	通信流量关键信息泄漏，破坏系统机密性	[98]
	拒绝服务	通过大量恶意报文堵塞信道和攻击网络拓扑	阻碍信息的实时传输，破坏系统可用性	[99]
	天坑攻击	通过欺骗路由器或 DNS 改变数据传播路径	流量全部导向恶意节点，破坏系统可用性	[100]
	虫洞攻击	两个恶意节点构造低时延链路欺骗正常节点	网络中路由表失效，破坏系统可用性	[101]
	重放攻击	拦截并向目标节点发送重复报文	目标节点花费大量资源处理，破坏系统可用性	[102]
	女巫攻击	单个恶意节点伪造多个实体以误导合法节点	影响网络中投票、数据聚合、信誉评估等过程	[103]
	选择性转发	恶意节点选择性地丢弃有价值的数据包	节点不能收到完整准确信息，破坏系统可用性	[104]
	中间人攻击	恶意节点在通信双方中间拦截或注入新消息	传输信息被篡改，破坏系统可用性与完整性	[105]
平台层	钓鱼邮件	发送伪装成可信来源的电子邮件	邮件附带恶意内容，破坏系统机密性和完整性	[106]
	恶意软件	利用木马、蠕虫、病毒等损害系统和数据	大量主机感染，破坏机密性、完整性与可用性	[107]
	社会工程学	利用社交网络、密码猜测等手段获取信息	关键数据泄漏，破坏系统机密性	[108]
	操作系统漏洞	利用系统内核漏洞破坏代码与数据	任意执行代码，破坏机密性、完整性与可用性	[109]
	数据库注入攻击	向数据库发送精心构造的 SQL 攻击载荷	数据库内容窃取，破坏系统机密性	[110]

如资源层智能电表的恶意篡改与平台层管理软件的漏洞利用等，有必要针对系统设备设立多层防御措施。设备防御的一方面是对软硬件层面的被动加固，另一方面是对入侵攻击的主动拦截。表 4 总结了可应用于 VPP 的主要设备防御技术。

表 4　虚拟电厂设备防御技术概览

Table 4　Overview of device defense technologies in VPP

防御类别	防御技术	相关文献
硬件产权保护	硬件水印	[79]
硬件系统架构	可信计算架构	[80]
硬件木马防御	流片前后检测、可信执行	[81]
硬件安全原语	真随机数发生器、物理不可克隆函数	[82]
硬件侧信道保护	掩码方案、隐藏方案	[83]
软件漏洞检测	模糊测试	[84]
软件流量过滤	网络防火墙	[85]
软件代码保护	加壳、混淆技术	[86]
软件运行隔离	虚拟化、容器化技术	[87]
主动诱骗防御	蜜罐系统	[88]
主动监控防御	入侵检测系统	[89]
主动数据分析	安全审计、威胁情报共享	[90]
主动属性变化	虚假端口转换、网络地址随机	[91]

设备硬件是构成 VPP 的基础，然而受限于尺寸、算力、能耗等因素，常常忽略其中的安全配置措施，从而成为攻击者的潜在目标[111]。1）设备硬件并不是系统的可信方，例如，恶意提供商向芯片与集成电路板植入后门、木马等，破坏变电站中的智能电子设备[112]；2）由于相应安全设计缺陷，硬件在使用过程也容易遭受攻击，例如对电网传感器的固件进行篡改，通过改变相关控制参数实现虚假数据注入攻击等[113]。对于硬件层面的加固可从以下几点进行考虑[114]：首先，确保硬件的来源安全，例如通过对电表芯片进行木马检测等手段；其次，对电网设备设计阶段采用先进的架构和安全原语，提供安全防御基础；最后，针对 VPP 硬件使用过程中各种侵入式和非侵入式的攻击采取对应加固手段。

软件是 VPP 中关键任务和功能的载体，与硬件缺陷对比，软件安全问题更加普遍与复杂。例如，针对平台层监控和数据采集系统的缓冲区溢出攻击[115]，针对资源层的智能电表进行恶意漏洞及拒绝服务攻击等[116]。对于软件层的防御也需从采取综合性的内外防御措施：从内部防御的角度，应关注软件的自身缺陷，例如及时修复物联设备软件的漏洞缺陷，加强 VPP 管理平台的代码审计和测试，确保软件的质量和安全性，同时采取代码加密、混淆等技术，提升软件的抗逆向分析能力；从外部防御的角度，需要关注软件运行环境安全问题，如在 VPP 控制中心边界处设置流量防火墙，限制外部流量对

软件的访问权限，采用运行隔离技术，将调度管理系统与其他应用隔离，实现运行环境之间独立性。

在软硬件防护的基础上，VPP 还可以通过实时监测、动态决策和快速阻断等主动防御技术来预防和减轻安全威胁的影响。例如，通过诱骗机制可以吸引和捕获潜在攻击，获取如虚假数据注入攻击的攻击负荷和威胁信息，增强对安全事件的感知能力；VPP 控制中心可以实时收集外部安全情报，部署异常行为检测系统等措施，对系统整体安全实现全局性监控；通过主动变换系统关键属性，例如负荷接入服务的端口、IP 等，使得攻击者难以识别和利用系统的特征，增加攻击的复杂性和成本，降低系统受到的威胁可能性。

3.2 安全接入控制技术

接入控制技术可以分为身份认证与访问控制两部分。首先，平台层需要对资源层中大量用户和实体进行身份鉴别和访问控制，相应的控制策略需要高效地存储和查找，以及能够实时地对用户和资源的变化进行更新。其次，资源层中的设备通常由于计算资源有限，相对应的认证与控制策略应该在保证安全性的同时尽可能轻量化，以减少对设备的性能影响。因此，接入控制技术需要根据 VPP 中具体的设备限制与需求综合考虑。

认证即是验证用户、设备或系统实体身份合法性的过程，是 VPP 系统安全的第一道防线[117]。根据认证过程主客体不同，VPP 中身份认证可划分以下 3 类：设备到设备、设备到网络、用户到设备[118]。首先，VPP 中设备之间交互频繁，因此设备到设备认证也最为关键，如智能电表向 VPP 管理平台上报数据过程、负荷设备向储能设备下发请求等。VPP 具有认证需求体量大，设备算力差异大的特点，应要求对应的身份验证流程在保证安全性的同时具有良好效率与可扩展性，如文献[119]基于椭圆曲线加密算法(elliptic curve cryptography，ECC)实现了一种支持动态设备接入的身份验证协议；文献[120]使用基于属性的恒密文长度加密方案，减小了设备身份验证过程中存储和计算的开销；文献[121]设计一种组认证的密钥管理办法，实现对组单元设备的轻量高效认证。其次，设备到网络的身份验证限制 VPP 中各种设备对局域网、邻域网的接入权限，提高了通信链路的安全性[122]。例如，文献[123]基于多因子认证设计了 ZigBee 网络中的接入方案。最后，VPP 系统在自动化运行的同时，也需要适时的人为干预与管理，因此需在用户到设备的交互过程设计可靠身份认证措施，例如强口令、生物特征、专用智能卡等[124]。

授权即是在明确身份的基础上，根据用户、设备或系统实体的身份信息赋予其相应权限的过程。目前授权机制的实现主要通过 4 种常见的访问控制模型。自主访问控制(discretionary access control，DAC)与强制访问控制(mandatory access control，MAC)通过访问控制列表与访问控制矩阵决定主客体之间的访问权限[125]。DAC 与 MAC 逻辑简单，但消耗的资源随着控制需求规模增大而快速增加，因此适用于 VPP 中单一被控、控制需求不高的场景，如监控系统中管理员接入等。基于角色的访问控制(role based access control，RBAC)中每个主体都被分配相应的角色，访问权限与角色关联[126]。一方面，RBAC 将访问客体和角色进行分离，有效减少访问控制矩阵的规模，增加控制策略的灵活性；另一方面，随着系统规模增大，访问控制颗粒度细化，可能会产生难以管理的“角色爆炸”问题[127]。因此，RBAC 适合需求适中的场景，例如 VPP 控制中心的操作员权限限制等。基于属性的访问控制(attribute based access control，ABAC)通过主体、客体、权限、环境属性来描述控制策略，灵活精确制定控制策略的同时，避免了“角色爆炸”问题，且能根据如访问时间、地点等上下文信息动态决策[128-129]，适合大量负荷侧设备细粒度控制需求。

3.3 安全通信链路技术

通信链路是 VPP 将众多 DER 聚合集成的桥梁，以实现信息传递和协调控制。因此，需要对 VPP 通信过程中各个环节采取有效的安全策略，确保信息传输的实时性、可靠性、稳定性和隐私性。具体而言，对于 VPP 中本地通信技术与远程通信技术[2]的防护措施各有侧重。

本地通信主要负责较小区域范围内的数据交换与聚合，例如 DER 的集群通信等，常使用 RS-485、HPLC、微功率无线等中近距离通信技术。此类技术位于 OSI 模型中的较低层次，对物理数据链路中非法窃听，干扰篡改等威胁较为敏感。相应的防护措施可以分为两大类[130]：1）第 1 类是基于信干噪比的方法，通过信道编码、加入人工噪声等非密钥方式，使攻击者的信干噪比低于正常用户的信干噪比来提供保密性。如文献[131]中通过低密度校验码实现高级计量基础设施的数据安全传输；2）

第 2 类是基于复杂度的方法，通过密钥从共享信道中提取秘密序列，保密性主要依托密钥提供。如文献[132]中通过压缩感知设计动态密钥生成算法，实现物理层的安全通信。

远程通信主要负责 VPP 中区域间的信息传递，例如集控设备到 VPP 控制中心之间的通信，常使用 5G、工业以太网、互联网等远程通信技术，具有接入方式多、通信范围广的特性。此类技术通常涵盖了 OSI 模型的中高层次，除了物理数据链路中的窃听、篡改等威胁外，还需要关注较高层次的安全威胁，并增强对网元设备保护、网络准入控制、网络数据保密等设计。例如，对 5G 无线接入网设计统一认证框架与面向频繁接入的认证机制，利用网络切片实现安全隔离机制，通过多种凭证实现用户身份标识的隐私保护等[133]；对于工业以太网协议自身缺乏网络安全防护措施的问题，可以改进相关协议实现链路加密、节点加密和端到端加密等[134]；对于物联网路由安全问题，设计基于信任模型、博弈论、神经网络等的路由保护协议[135]；对于互联网网络层、传输层数据保密问题，可以采用 IPsec、SSL/TLS 等安全协议进行加密[136]；对于 MQTT、XMPP、CoAP 等应用层协议安全问题，在传输层加密的基础上加入额外的身份认证、完整性检查等机制[137]。

3.4　安全数据管理技术

VPP 中的数据呈现多样化来源，其规模大且粒度小，需要进行聚合、转换、传播和访问以支持系统运行与决策[138]，有必要从数据的角度进行全面安全考量。数据生命周期中的数据生成、采集、存储、使用和销毁阶段存在不同的安全威胁，可以根据威胁特点制定对应的安全策略[41]。

数据生成阶段安全威胁主要来自源网荷储中各式传感器遭受攻击导致的数据丢失、失真等问题，应设计适用于具体设备计算与存储能力的访问控制技术与设备防御技术进行安全加固。

数据采集阶段需要利用安全通信链路技术实现 VPP 内部数据的安全传输，还需要建立数据过滤规则、数据异常检测、数据源可信评估等机制实现对地理、市场等 VPP 外部数据的可信采集。

数据存储阶段需要使用合适的加密方式实现海量数据云存储过程的保密性、完整性与隐私性，常见的方式有基于身份的加密、基于属性的加密(attribute-based ecryption，ABE)、同态加密、可搜索加密等[139]。另外，还需要加入严格的访问控制策略，采用安全的存储介质，定时容灾备份等手段实现数据安全存储。

数据使用阶段需要针对具体场景制定安全对策，例如，文献[140]利用 XGBoost 和无迹卡尔曼滤波实现对状态估计过程中可能的虚假注入攻击进行检测辨识与修正；文献[141]中利用同态加密方案保护电力拍卖过程中参与者的数据隐私；文献[142]针对篡改智能电表数据导致的电力盗窃问题，使用三元组孪生网络构建了一个检测模型。

数据销毁阶段要求评估数据的潜在价值并遵守数据法定保留期限，对无价值、无权限等数据进行及时销毁。需要关注在云存储环境下的大数据，可以利用自销毁程序实现数据受控删除[143]；也需要关注分布在各式固件中的敏感数据，避免因数据“浅层”删除导致的隐私泄露[144]。

3.5　安全运维管理技术

运维管理技术可以分为 3 个方面：1）日常安全运维流程管理；2）安全事件检测与响应；3）人员安全意识与培训。

日常运维安全流程管理方面，通过全面感知设备与线路的安全属性，结合可视化技术构建 VPP 系统网络安全运维平台[145]。结合标准化安全策略与管理规范，对安全事件进行标准化定义，制定统一的漏洞管理流程，定期进行安全合规性评估与审计等措施，形成日常安全运维标准流程。

安全事件检测与响应方面，通过实时监控系统日志、网络流量和安全事件，结合威胁情报共享等机制，识别潜在风险和异常行为。制定应急响应计划，快速响应安全事件并采取请求阻断、漏洞修复、分区隔离等措施进行快速恢复。

人员安全意识与培训方面，通过强化关于网络安全意识、最佳实践和安全行为的培训和教育，编写和传达网络安全政策、指南和文档，确保安全信息的有效传递和沟通。定期进行模拟攻击和演练，测试系统和员工的应急响应能力。

4　虚拟电厂网络安全技术研究展望

在上述五维防御技术的基础上，VPP 具备了应对常见攻击的能力，然而其复杂的运行环境依然导致难以实现综合性的系统安全。首先，VPP 面临外部不可信设备的海量接入，需要设计合适的接入方法以满足系统安全性与效能需求；其次，VPP 运行

时数据庞大，需要从海量数据中捕获并分析与安全相关的信息，以支持下一步的决策；最后，由于VPP的分布式特性，使得电力交易过程产生如交易过程不透明、交易数据隐私泄露等问题，需要一种新的底层架构以契合分布式环境的安全性需求。为应对VPP的海量设备安全接入、大规模数据安全分析、以及分布式安全问题，下文将深入讨论零信任安全、态势感知和区块链3种新兴技术，以提供系统性的解决思路。

4.1 虚拟电厂零信任安全边界

零信任是一种网络安全防护指导思想，其核心理念是“永不信任，始终验证”[146]，即对于任何用户、设备或资源，无论其是在系统内部还是外部，都需对其每一次的访问请求进行严格验证。VPP作为一种新型电力系统，在电源结构、电网形态、业务模式、技术基础等方面革新的同时，也面临着安全防护的可控性下降、攻击面扩大、攻击路径增多等问题，对相应安全防护技术提出更高的要求[14]。在VPP网络安全设计中融入零信任，将打破传统电网基于内部可信的边界安全架构，海量接入设备的访问请求都需要进行全面的身份验证、访问授权和行为审计，系统内部的失陷威胁因为动态信任评估难以横向扩散，增强VPP系统中的安全监控与实时响应能力。

目前已有一些研究关注电力场景的零信任架构设计[147-149]，且大部分研究都以NIST提出的零信任架构[150]为基础，但直接针对VPP场景的研究相对较少。本文在已有研究的基础上，形成如图3所示的VPP零信任安全架构，给出了一种零信任组件与虚拟电厂实体之间的部署映射关系。VPP中零信任安全接入的整体流程如下：1）负荷侧设备接入请求通过智能交互终端中零信任接入代理进行汇聚管理；2）边缘接入网关对一系列前置通信设施与VPP服务进行保护，实行对接入请求的持续监测与管控；3）VPP安全运维平台进行全局安全态势信息收集，实现威胁主动响应和全局安全策略下发等。

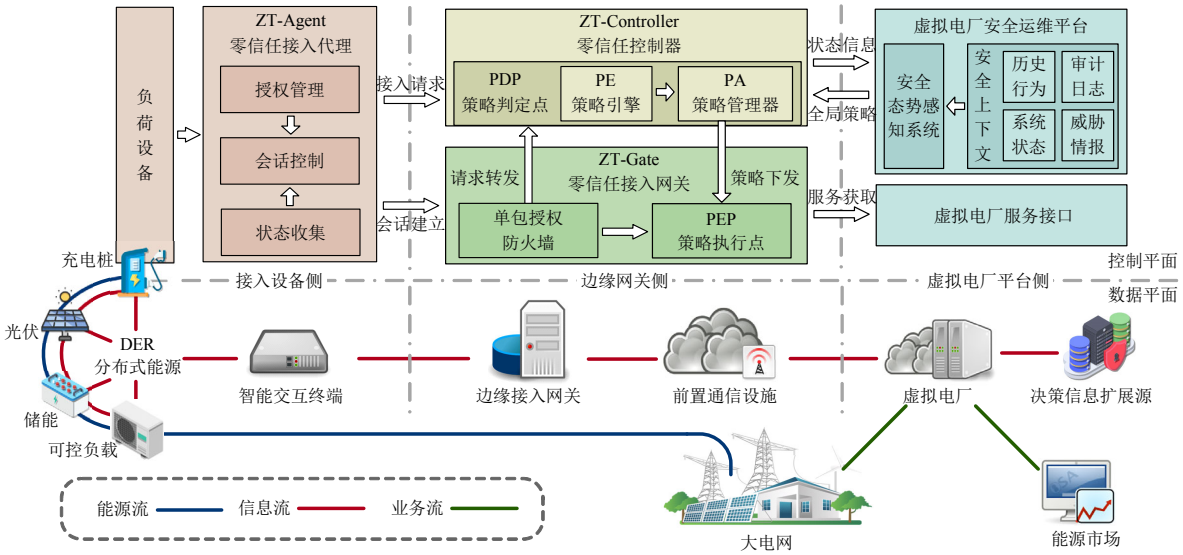

图3 虚拟电厂零信任安全架构

Fig. 3 VPP zero trust security architecture

零信任需要对接入设备进行安全属性收集，以对其进行实时动态信任评估。然而，VPP负荷侧设备形态各异(如空调、充电桩等)、计算和通信能力不一，缺乏对安全属性进行感知与上传的能力，无法强制其满足相关安全假设，为此在设备接入侧引入智能交互终端作为代理，实现授权管理、状态收集、会话控制等任务。

零信任的核心部署在VPP中被防护主体的边界处，包括零信任接入网关与控制器。零信任接入网关承担对流量进行转发与拦截的任务：首先，利用单包授权技术实现网络隐身功能，防截大部分的非法流量与攻击尝试；策略执行点(policy enforcement point，PEP)根据上层下发规则，执行接入设备对资源访问许可的决定，转发或拦截相应请求。零信任控制器承担对接入设备的持续认证与授权任务：策略判定点(policy decision point，PDP)是核心部件，由策略管理器(policy administrator，PA)与策略引擎(policy engine，PE)组成；PE基于实时的接入设备访问信息与环境信息，经过信任和风险评估生成控制策略，并交给PA进行策略分解、编

排与分发。

虚拟电厂平台侧可以通过收集各控制器的日志信息，结合安全上下文等数据，利用态势感知系统建立全局安全总览，更易捕获潜在的安全威胁，并生成全局策略为 PEP 提供决策支持。

近年来，越来越多的学者关注零信任领域并对其进行改进[151-152]，然而，零信任安全在 VPP 乃至电力领域中的实践大多停留在探索阶段，对传统架构的颠覆也使得其存在一定的部署成本。例如，零信任的接入网关、控制器等专用硬件开发，智能交互终端对负荷侧异构设备的融合接入设计，平台侧海量终端的动态控制策略设计等。未来还需对零信任流程的各个阶段进行深入的理论探索，完善和优化零信任与 VPP 融合的实施方法和技术机制，最大化安全效能产投比。

4.2　虚拟电厂安全态势感知

态势感知是指对一定时空内环境元素的感知，对其含义的理解，并对其未来状态预测以实现决策优势的系统，已经被有效地运用于飞行控制、军事行动、医疗急救等领域中[153]。在电力领域，态势感知也被应用于电力监控系统网络安全风险控制[154-155]。在 VPP 中可以利用态势感知系统实现对信息、物理、社会相关的安全态势进行综合建模与风险预测，通过收集整体安全态势数据，如 IP 等信息数据、负荷等物理数据、气象等社会数据，以全局视角分析相关安全风险，作为“安全大脑”为零信任接入提供自动化策略，为管理人员提供决策指标，实现风险实时预警与阻断等[156]。然而，针对 VPP 态势感知系统的相关研究在国内外尚属较少，缺乏针对 VPP 网络安全态势感知的定制化解决方案。

VPP 态势感知系统可以分为如图 4 所示的 4 个模块[157-158]：1）态势提取模块，负责监控、捕获、和筛审 VPP 环境中的关键数据和信息；2）态势理解模块，负责对所收集的数据进行分析、解读和识别，以理解 VPP 系统的当前状态；3）态势预测模块，负责基于历史数据和当前状态，预测 VPP 环境中可能发生的趋势、变化和潜在威胁；4）态势呈现模块，负责将态势数据以直观和可视化方式进行展示，以帮助决策者全面了解 VPP 态势情况。

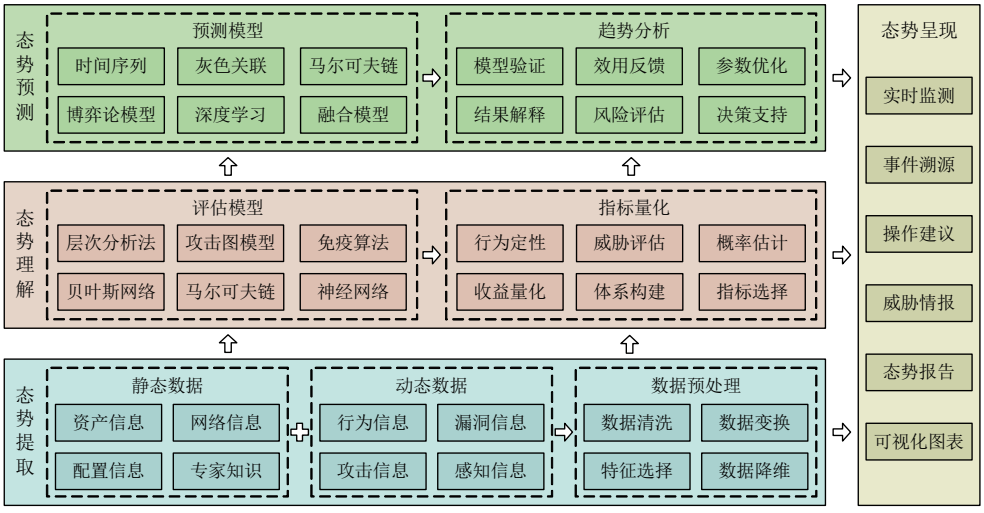

图 4　虚拟电厂网络安全态势感知系统架构

Fig. 4　VPP cyber security situation awareness system architecture

VPP 场景下态势感知系统实现难点在于态势提取、理解和预测过程。首先是态势数据获取与处理问题。传统信息系统架构较为集中，智能化程度高，能够直接通过 Wireshark、Syslog 等工具获取流量、日志等数据，而 VPP 系统分布式程度高、设备智能化程度不足，需要设计专用设备和链路采集与传输设备状态数据[159]。除了内部设备运行数据外，态势感知系统还需综合利用外部威胁情报、通用漏洞披露、防火墙与入侵检测系统报告等多方信息源，增强后续态势理解与预测能力[160]。另一方面，海量态势数据也使数据的靶向收集、清洗、集成、规约和变换等成为关键问题。

态势理解过程需要对 VPP 安全形势进行评估与量化，如交易异常检测、DER 接入监控、供应链风险评估等，常用的模型可以分为 3 类[161]：1）通过数学语言进行态势描述和抽象的数学模型，如层次分析法[162]与贝叶斯网络[163]等，但具有大规模部署困难等问题；2）以攻击图模型和马尔可夫链[164]

为代表的随机模型，模型外部参数会根据特定条件而变化，与网络安全行为发生特点高度契合；3）受自然现象启发的神经网络[165]等算法，更加擅长处理复杂非线性问题。

态势预测需要发掘潜在的网络安全风险，如通信链路持续可用性、智能电表漏洞利用潜在性、控制中心入侵可能性等。所采用的模型更加关注时序中的隐藏特征，可以使用如时间序列分析、马尔可夫链[166]、长短期记忆网络(long short-term memory，LSTM)[167]等方法揭示事件之间的因果关系与演化趋势。其次，VPP 系统中的大量数据具有部分不完整或不确定的信息，对应的态势变化可以认为是一个灰色系统，可以利用灰色关联模型实现小样本下的预测[168]。另外，通过研究 VPP 网络安全中不同参与方之间相互作用和竞争关系，可以把态势预测看作是一种对抗性的决策过程，利用博弈论模型进行趋势求解[169]。

在 VPP 中引入和实施态势感知系统时，各阶段都存在亟需解决的问题。首先，建模过程需要大量数据集的支持，对数据收集、集成和标准化等工作带来了挑战；其次，VPP 中设备分布广泛，针对 VPP 的攻击向量多样，为了解决算力分散、单一模型只能检测特定攻击向量等问题，可以引入联邦学习以充分利用 VPP 分布式算力，引入集成学习提高系统对复杂攻击的检测应对能力[170]；另外，将复杂数据映射为信息、物理、社会融合的态势指标并直观方式呈现以协助管理员进行决策，也是一个具有挑战性的问题[171]。

4.3 区块链赋能虚拟电厂安全

区块链是一种由链式区块组成分布式账本技术，每个区块包含若干交易数据和前一个区块的哈希值，通过哈希链接形成不可篡改的结构[172]。区块链在市场化、协作化、去中心化、交易自动化等方面的特点与能源物联网理念自然契合[173]，促使其在如电力交易等方面得到广泛应用[174-175]。区块链与 VPP 这一新型电力系统结合的实际案例较少，但已有学者探讨了区块链的共识机制、加密技术、分布式存储以及智能合约等方面对于 VPP 电力交易环节的广泛适用性。图 5 描述了在区块链在 VPP 中电力交易的一种应用场景。鉴于区块链在电力领域中的应用先例与 VPP 的自身特性及发展态势，使用区块链对 VPP 进行赋能具有相当的可行性，同时也应考量引入区块链后新的安全威胁与对策。

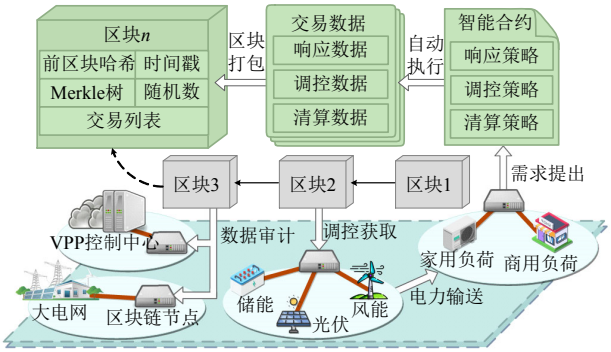

图 5 虚拟电厂中基于区块链的电力交易

Fig. 5 Blockchain-based electricity trading in VPP

共识算法是区块链安全性的基础，利用共识算法可以实现交易数据的安全存储，使得参与节点之间对区块数据达成顺序与内容上的一致性共识[176]。然而，在 VPP 中的区块链节点性能不均，大型聚合商节点通常拥有更高的算力，节点也易被攻击者集中控制，存在 51%攻击等安全风险，导致数据篡改或双花问题[177]，破坏电力交易数据的完整性。首先，应该避免使用工作量证明等高度依赖算力的共识算法，引入信用评分等奖惩机制[178]，均衡各节点区块提交能力。其次，可以使用联盟链并对接入节点进行认证授权，建立可信节点群体。最后，建立全面的安全审计和监控机制，及时发现受陷节点并进行隔离和处置。

电力交易中的响应、调控、清算等策略需要通过智能合约完成，其建立了一个独立可信的程序运行环境，使得电力交易全过程能够去中心化自动执行，减少人为修改与干预[179]。然而，攻击者可能利用区块链中代码层、虚拟机层、系统层等漏洞实现对智能合约的攻击[180]，造成错误计量、调度等问题。对于智能合约的攻击防护，一方面是要采取安全的编程方案，如利用经过大量安全审计的代码库，通过代理合约来实现热升级方案等；另一方面是要在合约部署前进行安全检测，利用模糊测试、符号执行、形式化验证等技术进行漏洞挖掘，并修复相关缺陷[181]。

由于区块链分布式账本的共享特性，节点在电力交易中的产生信息和数据可以被其他节点分发和记录，可能导致相应的安全问题。例如。用电方的个人信息、电网的运行状态泄漏等。区块链中数据机密性的实现可以使用以下方式：首先，可以基于区块链中的混币机制对交易数据进行匿名化处理，使得参与电力交易的节点和交易内容不易被追溯和识别；其次，利用同态加密、差分隐私、环签

名等密码学手段对链上数据进行加密，实现敏感数据的隐私存储；最后，加强通信链路的安全防护，利用通道隔离、权限限制等机制防止恶意节点获取区块链中的交易数据[182]。

总体而言，区块链具有作为 VPP 电力交易子系统底层架构的潜力，一方面，新技术的引入通常伴随着未知的风险和挑战，必须认识到可能带来的安全问题。不仅要考虑区块链自身安全风险，还需要考虑硬件兼容支持问题，性能与安全的平衡问题，交易开放性带来的节点接入、支付合规、数据隐私等安全问题。另一方面，区块链自身的去中心化、透明化、自动化等特点，也为 VPP 中运维管理、实体接入、数据采集和异常监控等方面的安全问题提供了新的解决方案，如表 5 所示，相关技术可参考区块链赋能物联网的应用，本文不再对此展开描述。

表 5　区块链在虚拟电厂网络安全中的应用

Table 5　Applications of blockchain in VPP cyber security

应用场景	主要安全加固方式	相关文献
设备通信密钥管理	根据设备处理能力划分密钥管理集合，利用区块链管理与设备关联的密钥，实现密钥管理安全性与密钥分发的均衡性	[183]
电力产销日志管理	利用密文策略 ABE 与签名链实现日志的访问控制与抗抵赖性，基于公私链混合结构实现高效且安全的日志数据存储	[184]
智能电表可靠接入	设计基于 ECC 的链下身份验证流程，设计基于实用拜占庭容错的接入记录黑白名单机制，减少身份认证开销并提高安全性	[185]
电力物联信任网关	利用门限共享算法与设计基于实用拜占庭容错的主从网关结构，实现多方主体信任背书与接入服务的容错性和鲁棒性	[186]
电表数据授信共享	设计基于区块链的链上共享授权与基于可信执行环境的链下存储机制，实现用电数据的受控分享与性能平衡	[187]
用电数据大量传输	在边缘层引入区块链节点，通过同态加密实现区域数据的隐私聚合，利用单向哈希链与短签名技术保护用电数据完整性	[188]
广域动态状态估计	利用区块链存储状态估计数据，并通过投票共识机制评估各节点可信度，实现本地异常快速检测与在线状态恢复机制	[189]
恶意行为实时检测	链下聚合数据并统一检测，利用 IPFS 实现分布式的高效数据存储，设计智能合约以激励公用事业提供商处理恶意行为	[190]

5　结论

本文全面回顾电力系统网络安全的演进与发展，针对虚拟电厂中潜在的网络安全挑战与需求，分析在虚拟电厂中设备防御、接入控制、通信链路、数据管理与运维管理 5 个方面各类技术的应用模式与可能的局限性，并提出面向虚拟电厂的五维防御体系。最后，展望在虚拟电厂网络安全实践中具有前瞻性的 3 种技术，即零信任、态势感知和区块链为虚拟电厂网络安全保障提供新思路与新方法。

随着 5G、大数据、人工智能等信息技术的迭代更新，电力系统和虚拟电厂网络安全领域的攻击与防御方式也在不断升级演进。对于虚拟电厂网络安全，一方面，要在电力系统中夯实巩固已有的防御措施，不断完善与探索新兴安全技术在电力系统中的运用，并迁移迭代至 VPP 场景；另一方面，需要根据 VPP 具体特性，综合考虑信息、物理和社会侧的安全需求，建立更为全面的安全防御体系，以应对不断变化的网络威胁。

参考文献

[1] LIU Chengyang，YANG R J，YU Xinghuo，et al．Virtual power plants for a sustainable urban future [J]. Sustainable Cities and Society，2021，65：102640．

[2] 汪莞乔，苏剑，潘娟，等．虚拟电厂通信网络架构及关键技术研究展望[J]．电力系统自动化，2022，46(18)：15-25．
WANG Wanqiao，SU Jian，PAN Juan，et al．Prospect of research on communication network architecture and key technologies for virtual power plant[J]．Automation of Electric Power Systems，2022，46(18)：15-25(in Chinese)．

[3] 陈皓勇，谭碧飞，伍亮，等．分层集群的新型电力系统运行与控制[J]．中国电机工程学报，2023，43(2)：581-594．
CHEN Haoyong，TAN Bifei，WU Liang，et al．Operation and control of the new power systems based on hierarchical clusters[J]．Proceedings of the CSEE，2023，43(2)：581-594(in Chinese)．

[4] LEHMBRUCK L，KRETZ J，AENGENVOORT J，et al．Aggregation of front- and behind-the-meter：the evolving VPP business model[M]//SIOSHANSI F．Behind and Beyond the Meter．London：Academic Press，2020：211-232．

[5] YANG Xiyun，ZHANG Yanfeng．A comprehensive review on electric vehicles integrated in virtual power plants [J]. Sustainable Energy Technologies and Assessments，2021，48：101678．

[6] 赵建立，向佳霓，汤卓凡，等．虚拟电厂在上海的实践探索与前景分析[J]．中国电力，2023，56(2)：1-13．
ZHAO Jianli，XIANG Jiani，TANG Zhuofan，et al．Practice exploration and prospect analysis of virtual power plant in Shanghai[J]. Electric Power，2023，56(2)：1-13(in Chinese)．

[7] 王宣元，刘蓁．虚拟电厂参与电网调控与市场运营的发

展与实践[J]. 电力系统自动化，2022，46(18)：158-168.
WANG Xuanyuan，LIU Zhen. Development and practice of virtual power plant participating in power grid regulation and market operation[J]. Automation of Electric Power Systems，2022，46(18)：158-168(in Chinese).

[8] 金雍奥，赵淑伟. 勇毅前行 争做标杆——国网冀北电力有限公司新型电力系统建设纪实[J]. 华北电业，2023(9)：8-11.
JIN Yongao，ZHAO Shuwei. Advancing with courage and determination，striving to be the benchmark—A chronicle of the construction of the new power system of state grid Jibei Electric Power Co.，Ltd.[J]. North China Power，2023(9)：8-11(in Chinese).

[9] 毛田，黄宁馨，程韧俐，等. 虚拟电厂效益评价指标体系构建及其范例分析[J]. 南方电网技术，2022，16(6)：124-131.
MAO Tian，HUANG Ningxin，CHENG Renli，et al. Construction of the benefit evaluation index system of virtual power plant and its example analysis[J]. Southern Power System Technology，2022，16(6)：124-131(in Chinese).

[10] 国家能源局. 能源局关于印发《电力行业网络安全等级保护管理办法》的通知[EB/OL]. (2022-11-16)[2023-11-20]. https://www.gov.cn/gongbao/content/2023/content_5743639.htm.
National Energy Administration. Notice by the national energy administration regarding issuing the measures for the classified protection of cybersecurity in the electricity industry[EB/OL]. (2022-11-16)[2023-11-20]. https://www.gov.cn/gongbao/content/2023/content_5743639.htm (in Chinese).

[11] LEE R M，ASSANTE M J，CONWAY T. Analysis of the cyber attack on the Ukrainian power grid[R]. Washington DC：E-ISAC，2016.

[12] 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 乌克兰和以色列国家电网遭受网络攻击事件的思考与启示[J]. 电力系统自动化，2016，40(8)：147-151.
LI Zhongwei，TONG Weiming，JIN Xianji. Construction of cyber security defense hierarchy and cyber security testing system of smart grid：thinking and enlightenment for network attack events to national power grid of Ukraine and Israel[J]. Automation of Electric Power Systems，2016，40(8)：147-151(in Chinese).

[13] 李更丰，邱爱慈，黄格超，等. 电力系统应对极端事件的新挑战与未来研究展望[J]. 智慧电力，2019，47(8)：1-11.
LI Gengfeng，QIU Aici，HUANG Gechao，et al. New challenges and future research prospects in power system against to extreme events[J]. Smart Power，2019，47(8)：1-11(in Chinese).

[14] 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.
ZHOU Jieying，ZHANG Xiao，SHAO Lisong，et al. Challenges and prospects of cyber security protection for new power system[J]. Automation of Electric Power Systems，2023，47(8)：15-24(in Chinese).

[15] 严康，陆艺丹，覃芳璐，等. 配电网用户侧异构电力物联设备网络风险量化评估[J]. 电力系统保护与控制，2023，51(11)：64-76.
YAN Kang，LU Yidan，QIN Fanglu，et al. Network security risk assessment of UPIDs in the distribution system[J]. Power System Protection and Control，2023，51(11)：64-76(in Chinese).

[16] YAN Ye，QIAN Yi，SHARIF H，et al. A survey on cyber security for smart grid communications[J]. IEEE Communications Surveys & Tutorials，2012，14(4)：998-1010.

[17] 王子骏，刘杨，鲍远义，等. 电力系统安全仿真技术：工程安全、网络安全与信息物理综合安全[J]. 中国科学：信息科学，2022，52(3)：399-429.
WANG Zijun，LIU Yang，BAO Yuanyi，et al. Power system security simulation technologies：engineering safety，network security and cyber-physical integrated security[J]. Scientia Sinica Informationis，2022，52(3)：399-429(in Chinese).

[18] 彭莎，孙铭阳，张镇勇，等. 机器学习在电力信息物理系统网络安全中的应用[J]. 电力系统自动化，2022，46(9)：200-215.
PENG Sha，SUN Mingyang，ZHANG Zhenyong，et al. Application of machine learning in cyber security of cyber-physical power system[J]. Automation of Electric Power Systems，2022，46(9)：200-215(in Chinese).

[19] 樊强，刘东，王宇飞，等. 电力信息物理系统形态演进关键技术及其进展[J]. 中国电机工程学报，2024，44(21)：8341-8353.
FAN Qiang，LIU Dong，WANG Yufei，et al. Key technologies and trends of cyber physical power system morphology evolution[J]. Proceedings of the CSEE，2024，44(21)：8341-8353(in Chinese).

[20] XUE Yusheng，YU Xinghuo. Beyond smart grid—cyber-physical-social system in energy future [point of view][J]. Proceedings of the IEEE，2017，105(12)：2290-2292.

[21] 王琦，李梦雅，汤奕，等. 电力信息物理系统网络攻击与防御研究综述(一)建模与评估[J]. 电力系统自动化，2019，43(9)：9-21.
WANG Qi，LI Mengya，TANG Yi，et al. A review on research of cyber-attacks and defense in cyber physical

power systems part one modelling and evaluation [J]. Automation of Electric Power Systems，2019，43(9)：9-21(in Chinese).

[22] 汤奕，李梦雅，王琦，等．电力信息物理系统网络攻击与防御研究综述(二)检测与保护[J]．电力系统自动化，2019，43(10)：1-9，18．
TANG Yi，LI Mengya，WANG Qi，et al．A review on research of cyber-attacks and defense in cyber physical power systems part two detection and protection [J]. Automation of Electric Power Systems，2019，43(10)：1-9，18(in Chinese).

[23] PUDJIANTO D，RAMSAY C，STRBAC G. Virtual power plant and system integration of distributed energy resources[J]．IET Renewable Power Generation，2007，1(1)：10-16．

[24] SABOORI H，MOHAMMADI M，TAGHE R．Virtual power plant(VPP)，definition，concept，components and types[C]//2011 Asia-Pacific Power and Energy Engineering Conference．Wuhan：IEEE，2011：1-4．

[25] 卫志农，余爽，孙国强，等．虚拟电厂的概念与发展[J]．电力系统自动化，2013，37(13)：1-9．
WEI Zhinong，YU Shuang，SUN Guoqiang，et al．Concept and development of virtual power plant[J]．Automation of Electric Power Systems，2013，37(13)：1-9(in Chinese)．

[26] 殷爽睿，艾芊，宋平，等．虚拟电厂分层互动模式与可信交易框架研究与展望[J]．电力系统自动化，2022，46(18)：118-128．
YIN Shuangrui，AI Qian，SONG Ping，et al．Research and prospect of hierarchical interaction mode and trusted transaction framework for virtual power plant [J]．Automation of Electric Power Systems，2022，46(18)：118-128(in Chinese)．

[27] 张慧，李健，吴青青，等．虚拟电厂通信网络体系架构及通信方式适配方法[J]．电力信息与通信技术，2022，20(12)：47-54．
ZHANG Hui，LI Jian，WU Qingqing，et al．Communication network architecture and communication mode adaptation method for virtual power plant[J]．Electric Power Information and Communication Technology，2022，20(12)：47-54(in Chinese)．

[28] 李淑静，谭清坤，张煜，等．虚拟电厂关键技术及参与电力市场模式设计研究[J]．电测与仪表，2022，59(12)：33-40．
LI Shujing，TAN Qingkun，ZHANG Yu，et al．Research on key technologies of virtual power plant and its participation in power market model design[J]．Electrical Measurement & Instrumentation，2022，59(12)：33-40(in Chinese)．

[29] 田昊．智能电网信息安全风险及防范对策探究[J]．中国管理信息化，2022，25(24)：93-95．
TIAN Hao．Research on information security risks and prevention strategies in smart grid[J]．China Management Informationization，2022，25(24)：93-95(in Chinese)．

[30] IEC．IEC/TS 62443-1-1 Industrial communication networks—Network and system security—Part 1-1：terminology，concepts and models[S]．Geneva：International Electrotechnical Commission，2009．

[31] 国家市场监督管理总局，中国国家标准化管理委员会．GB/T 36572—2018 电力监控系统网络安全防护导则[S]．北京：中国标准出版社，2018．
State Administration for Market Regulation，Standardization Administration of the People's Republic of China．GB/T 36572—2018 Guidelines of cyber security protection for electric power system supervision and control[S]．Beijing：Standards Press of China，2018(in Chinese)．

[32] IEC．IEC/TS 62351-1 Power systems management and associated information exchange — Data and communications security Part 1：communication network and system security—Introduction to security issues [S]．Geneva：International Electrotechnical Commission，2007．

[33] WANG Wenye，LU Zhuo．Cyber security in the smart grid：survey and challenges[J]．Computer Networks，2013，57(5)：1344-1371．

[34] 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(in Chinese)．

[35] KALOGRIDIS G，SOORIYABANDARA M，FAN Zhong，et al．Toward unified security and privacy protection for smart meter networks[J]．IEEE Systems Journal，2014，8(2)：641-654．

[36] SIDERIS A，TSIKTSIRIS D，ZIOUZIOS D，et al．Smart grid hardware security[M]//SIOZIOS K，ANAGNOSTOS D，SOUDRIS D，et al．IoT for Smart Grids：Design Challenges and Paradigms．Cham：Springer，2019：85-113．

[37] 王于丁，杨家海，徐聪，等．云计算访问控制技术研究综述[J]．软件学报，2015，26(5)：1129-1150．
WANG Yuding，YANG Jiahai，XU Cong，et al．Survey on access control technologies for cloud computing [J]．Journal of Software，2015，26(5)：1129-1150(in Chinese)．

[38] TRIANTAFYLLOU A，JIMENEZ J A P，TORRES A D R，et al．The challenges of privacy and access control as key perspectives for the future electric smart grid[J]．IEEE Open Journal of the Communications Society，2020，1：1934-1960．

[39] BOU-HARB E，FACHKHA C，POURZANDI M，et al．Communication security for smart grid distribution networks[J]．IEEE Communications Magazine，2013，51(1)：42-49．

[40] PENG Chen，SUN Hongtao，YANG Mingjin，et al．A survey on security communication and control for smart grids under malicious cyber attacks[J]．IEEE Transactions on Systems，Man，and Cybernetics：Systems，2019，49(8)：1554-1569．

[41] TAN Song，DE D，SONG Wenzhan，et al．Survey of security advances in smart grid：a data driven approach [J]．IEEE Communications Surveys & Tutorials，2017，19(1)：397-422．

[42] 辛耀中，石俊杰，周京阳，等．智能电网调度控制系统现状与技术展望[J]．电力系统自动化，2015，39(1)：2-8．
XIN Yaozhong，SHI Junjie，ZHOU Jingyang，et al．Technology development trends of smart grid dispatching and control systems[J]．Automation of Electric Power Systems，2015，39(1)：2-8(in Chinese)．

[43] LESZCZYNA R．A review of standards with cybersecurity requirements for smart grid[J]．Computers & Security，2018，77：262-276．

[44] TANGE K，DE DONNO M，FAFOUTIS X，et al．A systematic survey of industrial internet of things security：requirements and fog computing opportunities[J]．IEEE Communications Surveys & Tutorials，2020，22(4)：2489-2520．

[45] ISMAIL Z，LENEUTRE J，BATEMAN D，et al．A game theoretical analysis of data confidentiality attacks on smart-grid AMI[J]．IEEE Journal on Selected Areas in Communications，2014，32(7)：1486-1499．

[46] TAN Song，SONG Wenzhan，STEWART M，et al．Online data integrity attacks against real-time electrical market in smart grid[J]．IEEE Transactions on Smart Grid，2018，9(1)：313-322．

[47] BHUIYAN E A，HOSSAIN M Z，MUYEEN S M，et al．Towards next generation virtual power plant：technology review and frameworks[J]．Renewable and Sustainable Energy Reviews，2021，150：111358．

[48] GUNDUZ M Z，DAS R．Cyber-security on smart grid：threats and potential solutions[J]．Computer Networks，2020，169：107094．

[49] LI Xu，LIANG Xiaohui，LU Rongxing，et al．Securing smart grid：cyber attacks，countermeasures，and challenges [J]．IEEE Communications Magazine，2012，50(8)：38-45．

[50] HUANG Xiaoge，QIN Zhijun，LIU Hui．A survey on power grid cyber security：from component-wise vulnerability assessment to system-wide impact analysis [J]．IEEE Access，2018，6：69023-69035．

[51] 郭创新，陆海波，俞斌，等．电力二次系统安全风险评估研究综述[J]．电网技术，2013，37(1)：112-118．
GUO Chuangxin，LU Haibo，YU Bin，et al．A survey of research on security risk assessment of secondary system [J]．Power System Technology，2013，37(1)：112-118(in Chinese)．

[52] 汤涌．电力系统安全稳定综合防御体系框架[J]．电网技术，2012，36(8)：1-5．
TANG Yong．Framework of comprehensive defense architecture for power system security and stability [J]．Power System Technology，2012，36(8)：1-5(in Chinese)．

[53] 李文武，游文霞，王先培．电力系统信息安全研究综述[J]．电力系统保护与控制，2011，39(10)：140-147．
LI Wenwu，YOU Wenxia，WANG Xianpei．Survey of cyber security research in power system[J]．Power System Protection and Control，2011，39(10)：140-147(in Chinese)．

[54] ABDELGHANI T．Implementation of defense in depth strategy to secure industrial control system in critical infrastructures[J]．American Journal of Artificial Intelligence，2019，3(2)：17-22．

[55] 杨挺，翟峰，赵英杰，等．泛在电力物联网释义与研究展望[J]．电力系统自动化，2019，43(13)：9-20，53．
YANG Ting，ZHAI Feng，ZHAO Yingjie，et al．Explanation and prospect of ubiquitous electric power internet of things[J]．Automation of Electric Power Systems，2019，43(13)：9-20，53(in Chinese)．

[56] 傅质馨，李潇逸，袁越．泛在电力物联网关键技术探讨[J]．电力建设，2019，40(5)：1-12．
FU Zhixin，LI Xiaoyi，YUAN Yue．Research on key technologies of ubiquitous power internet of things [J]．Electric Power Construction，2019，40(5)：1-12(in Chinese)．

[57] CHEN Haoyong，WANG Xiaojuan，LI Zhihao，et al．Distributed sensing and cooperative estimation/ detection of ubiquitous power internet of things [J]．Protection and Control of Modern Power Systems，2019，4(1)：13．

[58] BAYINDIR R，COLAK I，FULLI G，et al．Smart grid technologies and applications[J]．Renewable and Sustainable Energy Reviews，2016，66：499-516．

[59] 王毅，陈启鑫，张宁，等．5G 通信与泛在电力物联网的融合：应用分析与研究展望[J]．电网技术，2019，43(5)：1575-1585．
WANG Yi，CHEN Qixin，ZHANG Ning，et al．Fusion of the 5G communication and the ubiquitous electric internet of things：application analysis and research prospects[J]．Power System Technology，2019，43(5)：1575-1585(in Chinese)．

[60] AL-ALI A R，ABURUKBA R．Role of internet of things in the smart grid technology[J]．Journal of Computer and

Communications，2015，3(5)：229-233.

[61] 张东霞，苗新，刘丽平，等．智能电网大数据技术发展研究[J]．中国电机工程学报，2015，35(1)：2-12.
ZHANG Dongxia，MIAO Xin，LIU Liping，et al．Research on development strategy for smart grid big data [J]．Proceedings of the CSEE，2015，35(1)：2-12(in Chinese).

[62] KAMDEM G，KAMHOUA C，LU Yue，et al．A Markov game theoritic approach for power grid security[C]//2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW)．Atlanta：IEEE，2017：139-144.

[63] SEN Ö，VAN DER VELDE D，WEHRMEISTER K A，et al．On using contextual correlation to detect multi-stage cyber attacks in smart grids[J]．Sustainable Energy，Grids and Networks，2022，32：100821.

[64] 王海峰，李朝阳，吕政权，等．泛在电力物联网环境下网络安全攻击研究[J]．浙江电力，2019，38(12)：76-81.
WANG Haifeng，LI Zhaoyang，LYU Zhengquan，et al．Survey on cyber attack in the context of ubiquitous power internet of things[J]．Zhejiang Electric Power，2019，38(12)：76-81(in Chinese).

[65] 曾鸣，刘英新，赵静，等．“云大物移智”与泛在电力物联网融合的安全风险分析及安全架构体系设计[J]．智慧电力，2019，47(8)：25-31.
ZENG Ming，LIU Yingxin，ZHAO Jing，et al．Security risk analysis and security architecture design of widespread power internet of things with the use of cloud computing big data internet of things mobile internet and smart city technology[J]．Smart Power，2019，47(8)：25-31(in Chinese).

[66] 王栋，陈传鹏，颜佳，等．新一代电力信息网络安全架构的思考[J]．电力系统自动化，2016，40(2)：6-11.
WANG Dong，CHEN Chuanpeng，YAN Jia，et al．Pondering a new-generation security architecture model for power information network[J]．Automation of Electric Power Systems，2016，40(2)：6-11(in Chinese).

[67] 王宣元，刘敦楠，刘蓁，等．泛在电力物联网下虚拟电厂运营机制及关键技术[J]．电网技术，2019，43(9)：3175-3183.
WANG Xuanyuan，LIU Dunnan，LIU Zhen，et al．Operation mechanism and key technologies of virtual power plant under ubiquitous internet of things[J]．Power System Technology，2019，43(9)：3175-3183(in Chinese).

[68] 周荔丹，曹祖加，姚钢，等．泛在电力物联网的发展分析[J]．现代电力，2021，38(2)：119-128.
ZHOU Lidan，CAO Zujia，YAO Gang，et al．Development analysis of the ubiquitous power internet of things [J]．Modern Electric Power，2021，38(2)：119-128(in Chinese).

[69] 康重庆，陈启鑫，苏剑，等．新型电力系统规模化灵活资源虚拟电厂科学问题与研究框架[J]．电力系统自动化，2022，46(18)：3-14.
KANG Chongqing，CHEN Qixin，SU Jian，et al．Scientific problems and research framework of virtual power plant with enormous flexible distributed energy resources in new power system[J]．Automation of Electric Power Systems，2022，46(18)：3-14(in Chinese).

[70] 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.
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)：1-8，67(in Chinese).

[71] 郭庆来，辛蜀骏，孙宏斌，等．电力系统信息物理融合建模与综合安全评估：驱动力与研究构想[J]．中国电机工程学报，2016，36(6)：1481-1489.
GUO Qinglai，XIN Shujun，SUN Hongbin，et al．Power system cyber-physical modelling and security assessment：motivation and ideas[J]．Proceedings of the CSEE，2016，36(6)：1481-1489(in Chinese).

[72] 龚钢军，张哲宁，张心语，等．分布式信息能源系统的耦合模型、网络架构与节点重要度评估[J]．中国电机工程学报，2020，40(17)：5412-5425.
GONG Gangjun，ZHANG Zhening，ZHANG Xinyu，et al．Coupling model，network architecture and node importance evaluation of distributed information energy system[J]．Proceedings of the CSEE，2020，40(17)：5412-5425(in Chinese).

[73] 刘雪艳，张强，李战明，等．面向智能电网通信系统的数据聚合和访问控制方法[J]．电力系统自动化，2016，40(14)：135-144.
LIU Xueyan，ZHANG Qiang，LI Zhanming，et al．Data aggregation and access control method for communication system of smart grid[J]．Automation of Electric Power Systems，2016，40(14)：135-144(in Chinese).

[74] 赵川，孙华利，王国平，等．基于大数据的电力信息系统网络安全分析[J]．电子设计工程，2019，27(23)：148-152.
ZHAO Chuan，SUN Huali，WANG Guoping，et al．Network security analysis of power information system based on big data[J]．Electronic Design Engineering，2019，27(23)：148-152(in Chinese).

[75] BUCHTA R，HEINE F，KLEINER C．Challenges and peculiarities of attack detection in virtual power plants：towards an advanced persistent threat detection system [C]//2022 IEEE 29th Annual Software Technology Conference(STC)．Gaithersburg：IEEE，2022：69-81.

[76] VENKATACHARY S K，PRASAD J，SAMIKANNU R．

Economic impacts of cyber security in energy sector：a review[J]．International Journal of Energy Economics and Policy，2017，7(5)：250-262．

[77] 陶耀东，李宁，曾广圣．工业控制系统安全综述[J]．计算机工程与应用，2016，52(13)：8-18．
TAO Yaodong，LI Ning，ZENG Guangsheng．Review of industrial control systems security[J]．Computer Engineering and Applications，2016，52(13)：8-18(in Chinese)．

[78] 李佳玮，郝悍勇，李宁辉．工业控制系统信息安全防护[J]．中国电力，2015，48(10)：139-143．
LI Jiawei，HAO Hanyong，LI Ninghui．Research on information security protection of industrial control system[J]．Electric Power，2015，48(10)：139-143(in Chinese)．

[79] 黄卫红．IP 核设计版权保护的数字水印方法与实时检测技术研究[D]．长沙：湖南大学，2020．
HUANG Weihong．Research on digital watermarking method and real-time detection technology for IP circuit copyright protection[D]．Changsha：Hunan University，2020(in Chinese)．

[80] 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．
GAO Kunlun，WANG Zhihao，AN Ningyu，et al．Construction of the immune system of cyber security for electric power supervise and control system based on trusted computing[J]．Advanced Engineering Sciences，2017，49(2)：28-35(in Chinese)．

[81] 黄钊，王泉，杨鹏飞．硬件木马：关键问题研究进展及新动向[J]．计算机学报，2019，42(5)：993-1017．
HUANG Zhao，WANG Quan，YANG Pengfei．Hardware Trojan：research progress and new trends on key problems[J]．Chinese Journal of Computers，2019，42(5)：993-1017(in Chinese)．

[82] 鲁迎春．硬件安全原语——真随机数发生器与物理不可克隆函数研究与设计[D]．合肥：合肥工业大学，2021．
LU Yingchun．Hardware security primtives：research and design of true random number generator and physical unclonable function[D]．Hefei：Hefei University of Technology，2021(in Chinese)．

[83] 王永娟，樊昊鹏，代政一，等．侧信道攻击与防御技术研究进展[J]．计算机学报，2023，46(1)：202-228．
WANG Yongjuan，FAN Haopeng，DAI Zhengyi，et al．Advances in side channel attacks and countermeasures[J]．Chinese Journal of Computers，2023，46(1)：202-228(in Chinese)．

[84] 任泽众，郑晗，张嘉元，等．模糊测试技术综述[J]．计算机研究与发展，2021，58(5)：944-963．
REN Zezhong，ZHENG Han，ZHANG Jiayuan，et al．A review of fuzzing techniques[J]．Journal of Computer Research and Development，2021，58(5)：944-963(in Chinese)．

[85] 焦伟．电力调度自动化网络安全防护系统的研究与实现[D]．保定：华北电力大学，2014．
JIAO Wei．Research and implementation on electric power dispatch automation network security protection system[D]．Baoding：North China Electric Power University，2014(in Chinese)．

[86] ROUNDY K A，MILLER B P．Binary-code obfuscations in prevalent packer tools[J]．ACM Computing Surveys，2013，46(1)：4．

[87] 聂峥，章坚民，傅华渭．配变终端边缘节点化及容器化的关键技术和应用场景设计[J]．电力系统自动化，2020，44(3)：154-161．
NIE Zheng，ZHANG Jianmin，FU Huawei．Key technologies and application scenario design for making distribution transformer terminal unit being a containerized edge node[J]．Automation of Electric Power Systems，2020，44(3)：154-161(in Chinese)．

[88] 田文．工业互联网蜜罐攻防博弈建模与分析研究[D]．南京：南京理工大学，2021．
TIAN Wen．Research on game modeling and analysis of honeypot against cyber attacks in industrial internet [D]．Nanjing：Nanjing University of Science & Technology，2021(in Chinese)．

[89] 杨杰，郭逸豪，郭创新，等．考虑模型与数据双重驱动的电力信息物理系统动态安全防护研究综述[J]．电力系统保护与控制，2022，50(7)：176-187．
YANG Jie，GUO Yihao，GUO Chuangxin，et al．A review of dynamic security protection on a cyber physical power system considering model and data driving[J]．Power System Protection and Control，2022，50(7)：176-187(in Chinese)．

[90] CHEHRI A，FOFANA I，YANG Xiaomin．Security risk modeling in smart grid critical infrastructures in the era of big data and artificial intelligence[J]．Sustainability，2021，13(6)：3196．

[91] 刘世文，马多耀，雷程，等．基于网络安全态势感知的主动防御技术研究[J]．计算机工程与科学，2018，40(6)：1054-1061．
LIU Shiwen，MA Duoyao，LEI Cheng，et al．An active defense technique based on network security awareness[J]．Computer Engineering & Science，2018，40(6)：1054-1061(in Chinese)．

[92] 潘传幸，张铮，马博林，等．面向进程控制流劫持攻击的拟态防御方法[J]．通信学报，2021，42(1)：37-47．
PAN Chuanxing，ZHANG Zheng，MA Bolin，et al．Method against process control-flow hijacking based on mimic defense[J]．Journal on Communications，2021，

42(1)：37-47(in Chinese).

[93] NGUYEN V L，LIN P C，HWANG R H. Energy depletion attacks in low power wireless networks[J]. IEEE Access，2019，7：51915-51932.

[94] 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(in Chinese).

[95] 董旭柱，谌立坤，王波，等. 电力定制化芯片应用场景及关键技术展望[J]. 中国电机工程学报，2022，42(14)：5017-5033.
DONG Xuzhu，CHEN Likun，WANG Bo，et al. Application scenario and key technology prospect of power specific integrated circuit[J]. Proceedings of the CSEE，2022，42(14)：5017-5033(in Chinese).

[96] 刘奇旭，靳泽，陈灿华，等. 物联网访问控制安全性综述[J]. 计算机研究与发展，2022，59(10)：2190-2211.
LIU Qixu，JIN Ze，CHEN Canhua，et al. Survey on internet of things access control security[J]. Journal of Computer Research and Development，2022，59(10)：2190-2211(in Chinese).

[97] HASTINGS M，FRIED J，HENINGER N. Weak keys remain widespread in network devices[C]//Proceedings of the 2016 Internet Measurement Conference. Santa Monica：ACM，2016：49-63.

[98] 罗军舟，杨明，凌振，等. 匿名通信与暗网研究综述[J]. 计算机研究与发展，2019，56(1)：103-130.
LUO Junzhou，YANG Ming，LING Zhen，et al. Anonymous communication and darknet：a survey [J]. Journal of Computer Research and Development，2019，56(1)：103-130(in Chinese).

[99] 王子强，王杰. 一种计及智能电网信息物理特性的分布式控制器[J]. 中国电机工程学报，2019，39(23)：6921-6933.
WANG Ziqiang，WANG Jie. A distributed control considering the cyber-physical characteristics of smart grid[J]. Proceedings of the CSEE，2019，39(23)：6921-6933(in Chinese).

[100] REHMAN A U，REHMAN S U，RAHEEM H. Sinkhole attacks in wireless sensor networks：a survey[J]. Wireless Personal Communications，2019，106(4)：2291-2313.

[101] 陈立建，金洪波，毛科技，等. 抵御虫洞攻击的无线传感器网安全定位算法[J]. 传感技术学报，2016，29(12)：1882-1887.
CHEN Lijian，JIN Hongbo，MAO Keji，et al. Secure localization algorithm against wormhole attack in WSN [J]. Chinese Journal of Sensors and Actuators，2016，29(12)：1882-1887(in Chinese).

[102] 张伟康，曾凡平，陶禹帆，等. 物联网无线协议安全综述[J]. 信息安全学报，2022，7(2)：59-71.
ZHANG Weikang，ZENG Fanping，TAO Yufan，et al. A survey for security of IoT wireless protocols[J]. Journal of Cyber Security，2022，7(2)：59-71(in Chinese).

[103] NAJAFABADI S G，NAJI H R，MAHANI A. Sybil attack detection：improving security of WSNs for smart power grid application[C]//2013 Smart Grid Conference (SGC). Tehran：IEEE，2013：273-278.

[104] 尹荣荣，张文元，杨绸绸，等. 一种基于多跳确认和信任评估的选择性转发攻击检测方法[J]. 控制与决策，2020，35(4)：949-955.
YIN Rongrong，ZHANG Wenyuan，YANG Chouchou，et al. A selective forwarding attacks detection approach based on multi-hop acknowledgment and trust evaluation [J]. Control and Decision，2020，35(4)：949-955(in Chinese).

[105] KULKARNI S，RAHUL R K，SHREYAS R，et al. MITM intrusion analysis for advanced metering infrastructure communication in a smart grid environment[C]//Third International Conference on Trends in Computational Intelligence，Security and Internet of Things. Tripura：Springer，2020：256-267.

[106] HOLM H，FLORES W R，ERICSSON G. Cyber security for a smart grid-what about phishing?[C]//IEEE PES ISGT Europe 2013. Lyngby：IEEE，2013：1-5.

[107] EL MRABET Z，KAABOUCH N，EL GHAZI H，et al. Cyber-security in smart grid：survey and challenges [J]. Computers & Electrical Engineering，2018，67：469-482.

[108] 马明阳. 针对社会工程学攻击的防御技术研究[D]. 北京：北京邮电大学，2015.
MA Mingyang. Research on the defense technology of social-engineering-attacks[D]. Beijing：Beijing University of Posts and Telecommunications，2015(in Chinese).

[109] 杨维永，刘苇，黄皓，等. 基于微内核的电力专用安全操作系统技术研究[J]. 电力信息与通信技术，2016，14(11)：22-27.
YANG Weiyong，LIU Wei，HUANG Hao，et al. Research on power private micro kernel-based secure operating system technology[J]. Electric Power Information and Communication Technology，2016，14(11)：22-27(in Chinese).

[110] 胡敏. Web 系统下提高 MySQL 数据库安全性的研究与实现[D]. 北京：北京邮电大学，2015.
HU Min. Research and implementation of improving MySQL database security in web system[D]. Beijing：Beijing University of Posts and Telecommunications，2015(in Chinese).

[111] KOLEY S，GHOSAL P. Addressing hardware security

challenges in internet of things：recent trends and possible solutions[C]//2015 IEEE 12th Intl Conf on Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops(UIC-ATC-ScalCom)．Beijing：IEEE，2015：517-520．

[112] CHATTOPADHYAY A，UKIL A，JAP D，et al．Toward threat of implementation attacks on substation security：case study on fault detection and isolation[J]．IEEE Transactions on Industrial Informatics，2018，14(6)：2442-2451．

[113] LI Yuanliang，YAN Jun．Cybersecurity of smart inverters in the smart grid：a survey[J]．IEEE Transactions on Power Electronics，2023，38(2)：2364-2383．

[114] HU Wei，CHANG C H，SENGUPTA A，et al．An overview of hardware security and trust：threats，countermeasures，and design tools[J]．IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems，2021，40(6)：1010-1038．

[115] UPADHYAY D，SAMPALLI S．SCADA(supervisory control and data acquisition) systems：vulnerability assessment and security recommendations[J]．Computers & Security，2020，89：101666．

[116] DÍAZ REDONDO R P，FERNÁNDEZ-VILAS A，FERNÁNDEZ DOS REIS G．Security aspects in smart meters：analysis and prevention[J]．Sensors，2020，20(14)：3977．

[117] LI Xinghua，CHEN Ting，CHENG Qingfeng，et al．Smart applications in edge computing：overview on authentication and data security[J]．IEEE Internet of Things Journal，2021，8(6)：4063-4080．

[118] SAXENA N，CHOI B J．State of the art authentication，access control，and secure integration in smart grid[J]．Energies，2015，8(10)：11883-11915．

[119] KUMAR N，AUJLA G S，DAS A K，et al．ECCAuth：a secure authentication protocol for demand response management in a smart grid system[J]．IEEE Transactions on Industrial Informatics，2019，15(12)：6572-6582．

[120] GE Jiangyan，WEN Mi，WANG Liangliang，et al．Attribute-based collaborative access control scheme with constant ciphertext length for smart grid[C]//ICC 2022-IEEE International Conference on Communications．Seoul：IEEE，2022：540-546．

[121] 肖勇，许卓，罗鸿轩，等．基于属性基加密与阈值秘密共享的智能电表密钥管理方法[J]．南方电网技术，2020，14(1)：31-38．
XIAO Yong，XU Zhuo，LUO Hongxuan，et al．Intelligent terminal key management method based on attribute base encryption and threshold secret sharing[J]．Southern Power System Technology，2020，14(1)：31-38(in Chinese)．

[122] MAHMOOD A，JAVAID N，RAZZAQ S．A review of wireless communications for smart grid[J]．Renewable and Sustainable Energy Reviews，2015，41：248-260．

[123] 周伟伟，岳云天，郁滨．ZigBee 节点多因子身份认证方案研究[J]．系统仿真学报，2015，27(4)：762-769．
ZHOU Weiwei，YUE Yuntian，YU Bin．Research of multi-factor identity authentication scheme for ZigBee network nodes[J]．Journal of System Simulation，2015，27(4)：762-769(in Chinese)．

[124] AHVANOOEY M T，ZHU M X，LI Qianmu，et al．Modern authentication schemes in smartphones and IoT devices：an empirical survey[J]．IEEE Internet of Things Journal，2022，9(10)：7639-7663．

[125] 林闯，封富君，李俊山．新型网络环境下的访问控制技术[J]．软件学报，2007，18(4)：955-966．
LIN Chuang，FENG Fujun，LI Junshan．Access control in new network environment[J]．Journal of Software，2007，18(4)：955-966(in Chinese)．

[126] 尚学伟，宋光鹏，李军良，等．基于角色的电力 SCADA 系统多区域权限访问控制模型设计[J]．电网技术，2014，38(4)：1122-1126．
SHANG Xuewei，SONG Guangpeng，LI Junliang，et al．Design of role-based multi area access control model for electric power SCADA system[J]．Power System Technology，2014，38(4)：1122-1126(in Chinese)．

[127] ELLIOTT A，KNIGHT S．Towards managed role explosion[C]//Proceedings of the 2015 New Security Paradigms Workshop．Twente：ACM，2015：100-111．

[128] 邵瑞雪，田秀霞．智能电网中基于 MQTT 协议的 ABAC 访问控制方案[J]．计算机应用研究，2022，39(11)：3436-3443．
SHAO Ruixue，TIAN Xiuxia．ABAC access control scheme based on MQTT protocol in smart grid [J]．Application Research of Computers，2022，39(11)：3436-3443(in Chinese)．

[129] 房梁，殷丽华，郭云川，等．基于属性的访问控制关键技术研究综述[J]．计算机学报，2017，40(7)：1680-1698．
FANG Liang，YIN Lihua，GUO Yunchuan，et al．A survey of key technologies in attribute-based access control scheme[J]．Chinese Journal of Computers，2017，40(7)：1680-1698(in Chinese)．

[130] HAMAMREH J M，FURQAN H M，ARSLAN H．Classifications and applications of physical layer security techniques for confidentiality：a comprehensive survey[J]．IEEE Communications Surveys & Tutorials，2019，21(2)：1773-1828．

[131] SHARMA H，KUMAR N，PANIGRAHI B K．Physical layer security of AMI data transmission in smart grid environment[C]//2019 IEEE Globecom Workshops(GC Wkshps)．Waikoloa：IEEE，2019：1-6．

[132] LIU Jingwei，HU Qin，SUNY R，et al．A physical layer security scheme with compressed sensing in OFDM-based IoT systems[C]//ICC 2020-2020 IEEE International Conference on Communications (ICC)．Dublin：IEEE，2020：1-6．

[133] 冯登国，徐静，兰晓．5G 移动通信网络安全研究[J]．软件学报，2018，29(6)：1813-1825．
FENG Dengguo，XU Jing，LAN Xiao．Study on 5G mobile communication network security[J]．Journal of Software，2018，29(6)：1813-1825(in Chinese)．

[134] 冯涛，鲁晔，方君丽．工业以太网协议脆弱性与安全防护技术综述[J]．通信学报，2017，38(S2)：185-196．
FENG Tao，LU Ye，FANG Junli．Research on vulnerability and security technology of industrial ethernet protocol[J]．Journal on Communications，2017，38(S2)：185-196(in Chinese)．

[135] MUZAMMAL S M，MURUGESAN R K，JHANJHI N Z．A comprehensive review on secure routing in internet of things：mitigation methods and trust-based approaches [J]．IEEE Internet of Things Journal，2021，8(6)：4186-4210．

[136] 王斌．工业物联网信息安全防护技术研究[D]．成都：电子科技大学，2018．
WANG Bin．Research on information security protection technology of industrial internet of things[D]．Chengdu：University of Electronic Science and Technology of China，2018(in Chinese)．

[137] NASTASE L．Security in the internet of things：a survey on application layer protocols[C]//2017 21st International Conference on Control Systems and Computer Science (CSCS)．Bucharest：IEEE，2017：659-666．

[138] SIMMHAN Y，KUMBHARE A G，CAO Baohua，et al．An analysis of security and privacy issues in smart grid software architectures on clouds[C]//2011 IEEE 4th International Conference on Cloud Computing．Washington：IEEE，2011：582-589．

[139] YANG Pan，XIONG Naixue，REN Jingli．Data security and privacy protection for cloud storage：a survey[J]．IEEE Access，2020，8：131723-131740．

[140] 刘鑫蕊，常鹏，孙秋野．基于 XGBoost 和无迹卡尔曼滤波自适应混合预测的电网虚假数据注入攻击检测[J]．中国电机工程学报，2021，41(16)：5462-5475．
LIU Xinrui，CHANG Peng，SUN Qiuye．Grid false data injection attacks detection based on XGBoost and unscented Kalman filter adaptive hybrid prediction [J]．Proceedings of the CSEE，2021，41(16)：5462-5475(in Chinese)．

[141] YANG Qingyu，LI Donghe，AN Dou，et al．Towards incentive for electrical vehicles demand response with location privacy guaranteeing in microgrids[J]．IEEE Transactions on Dependable and Secure Computing，2022，19(1)：131-148．

[142] 高昂，郑建勇，梅飞，等．基于三元组孪生网络的窃电检测算法[J]．中国电机工程学报，2022，42(11)：3975-3985．
GAO Ang，ZHENG Jianyong，MEI Fei，et al．Electricity theft detection algorithm based on triplet network [J]．Proceedings of the CSEE，2022，42(11)：3975-3985(in Chinese)．

[143] 曹景源，李立新，李全良，等．云存储环境下生命周期可控的数据销毁模型[J]．计算机应用，2017，37(5)：1335-1340．
CAO Jingyuan，LI Lixin，LI Quanliang，et al．Data destruction model for cloud storage based on lifecycle control[J]．Journal of Computer Applications，2017，37(5)：1335-1340(in Chinese)．

[144] LIU Peiyu，JI Shouling，FU Lirong，et al．How IoT re-using threatens your sensitive data：exploring the user-data disposal in used IoT devices[C]//2023 IEEE Symposium on Security and Privacy(SP)．San Francisco：IEEE，2023：3365-3381．

[145] 秦红霞，武芳瑛，彭世宽，等．智能电网二次设备运维新技术研讨[J]．电力系统保护与控制，2015，43(22)：35-40．
QIN Hongxia，WU Fangying，PENG Shikuan，et al．New technology research on secondary equipment operation maintenance for smart grid[J]．Power System Protection and Control，2015，43(22)：35-40(in Chinese)．

[146] BUCK C，OLENBERGER C，SCHWEIZER A，et al．Never trust，always verify：a multivocal literature review on current knowledge and research gaps of zero- trust[J]．Computers & Security，2021，110：102436．

[147] 刘涛，马越，姜和芳，等．基于零信任的电网安全防护架构研究[J]．电力信息与通信技术，2021，19(7)：25-32．
LIU Tao，MA Yue，JIANG Hefang，et al．Research on power grid security protection architecture based on zero trust[J]．Electric Power Information and Communication Technology，2021，19(7)：25-32(in Chinese)．

[148] 吴克河，程瑞，姜啸晨，等．基于 SDP 的电力物联网安全防护方案[J]．信息网络安全，2022，22(2)：32-38．
WU Kehe，CHENG Rui，JIANG Xiaochen，et al．Security protection scheme of power iot based on sdp[J]．Netinfo Security，2022，22(2)：32-38(in Chinese)．

[149] 姜琳，周亮，缪思薇，等．基于零信任架构的电力物联网安全接入方法[J]．电力信息与通信技术，2023，

21(1)：40-46.
JIANG Lin，ZHOU Liang，MIAO Siwei，et al．Secure access method of power internet of things based on zero trust architecture[J]．Electric Power Information and Communication Technology，2023，21(1)：40-46(in Chinese).

[150] National Institute of Standards and Technology．Zero trust architecture[EB/OL]．[2023-10-03]．https://doi.org/10.6028/NIST.SP.800-207．

[151] 黄杰，余若晨，毛冬．电力物联网场景下基于零信任的分布式数据库细粒度访问控制[J]．信息安全研究，2021，7(6)：535-542．
HUANG Jie，YU Ruochen，MAO Dong．Distributed database fine-grained access control based on zero trust in the power internet of things[J]．Journal of Information Security Research，2021，7(6)：535-542(in Chinese)．

[152] 冯景瑜，于婷婷，王梓莹，等．电力物联场景下抗失陷终端威胁的边缘零信任模型[J].计算机研究与发展，2022，59(5)：1120-1132．
FENG Jingyu，YU Tingting，WANG Ziying，et al．An edge zero-trust model against compromised terminals threats in power IoT environments[J]．Journal of Computer Research and Development，2022，59(5)：1120-1132(in Chinese)．

[153] OFTE H J，KATSIKAS S．Understanding situation awareness in SOCs，a systematic literature review[J]．Computers & Security，2023，126：103069．

[154] 辛保安，李明节，贺静波，等．新型电力系统安全防御体系探究[J]．中国电机工程学报，2023，43(15)：5723-5731．
XIN Baoan，LI Mingjie，HE Jingbo，et al．Research on security defense system of new power system [J]．Proceedings of the CSEE，2023，43(15)：5723-5731(in Chinese)．

[155] 刘权莹，李俊娥，倪明，等．电网信息物理系统态势感知：现状与研究构想[J]．电力系统自动化，2019，43(19)：9-21，51．
LIU Quanying，LI Jun’e，NI Ming，et al．Situation awareness of grid cyber-physical system：current status and research ideas[J]．Automation of Electric Power Systems，2019，43(19)：9-21，51(in Chinese)．

[156] 李鹏，黄文琦，梁凌宇，等．人机混合增强决策智能在新型电力系统调控中的应用与展望[J]．中国电机工程学报，2024，44(16)：6347-6366．
LI Peng，HUANG Wenqi，LIANG Lingyu，et al．Application and prospect of hybrid human-machine decision intelligence in the dispatch and control of next-era power systems[J]．Proceedings of the CSEE，2024，44(16)：6347-6366(in Chinese)．

[157] 龚俭，臧小东，苏琪，等．网络安全态势感知综述[J]．软件学报，2017，28(4)：1010-1026．
GONG Jian，ZANG Xiaodong，SU Qi，et al．Survey of network security situation awareness[J]．Journal of Software，2017，28(4)：1010-1026(in Chinese)．

[158] 杨宇，谷宇恒．网络安全态势感知综述[J]．科学技术与工程，2022，22(34)：15011-15019．
YANG Yu，GU Yuheng．Overview of network security situation awareness[J]．Science Technology and Engineering，2022，22(34)：15011-15019(in Chinese)．

[159] LIN Huaqing，YAN Zheng，CHEN Yu，et al．A survey on network security-related data collection technologies [J]．IEEE Access，2018，6：18345-18365．

[160] ALAVIZADEH H，JANG-JACCARD J，ENOCH S Y，et al．A survey on cyber situation-awareness systems：framework，techniques，and insights[J]．ACM Computing Surveys，2023，55(5)：107．

[161] LI Yan，HUANG Guangqiu，WANG Chunzi，et al．Analysis framework of network security situational awareness and comparison of implementation methods [J]．EURASIP Journal on Wireless Communications and Networking，2019，2019(1)：205．

[162] 曲向华，史雪梅．基于层次分析法的网络安全态势评估技术研究[J]．自动化技术与应用，2018，37(11)：43-45，50．
QU Xianghua，SHI Xuemei．Research of network security situation assessment based on AHP [J]．Techniques of Automation and Applications，2018，37(11)：43-45，50(in Chinese)．

[163] 丁华东，许华虎，段然，等．基于贝叶斯方法的网络安全态势感知模型[J]．计算机工程，2020，46(6)：130-135．
DING Huadong，XU Huahu，DUAN Ran，et al．Network security situation awareness model based on bayesian method[J]．Computer Engineering，2020，46(6)：130-135(in Chinese)．

[164] 康海燕，龙墨澜．基于吸收马尔可夫链攻击图的网络攻击分析方法研究[J].通信学报，2023，44(2)：122-135．
KANG Haiyan，LONG Molan．Research on network attack analysis method based on attack graph of absorbing Markov chain[J]．Journal on Communications，2023，44(2)：122-135(in Chinese)．

[165] 赵冬梅，宋会倩，张红斌．基于时间因子和复合 CNN 结构的网络安全态势评估[J]．计算机科学，2021，48(12)：349-356．
ZHAO Dongmei，SONG Huiqian，ZHANG Hongbin．Network security situation based on time factor and composite CNN structure[J]．Computer Science，2021，48(12)：349-356(in Chinese)．

[166] 文志诚，陈志刚，唐军．基于时间序列分析的网络安全态势预测[J].华南理工大学学报：自然科学版，2016，

44(5)：137-143，150.
WEN Zhicheng，CHEN Zhigang，TANG Jun. Prediction of network security situation on the basis of time series analysis[J]. Journal of South China University of Technology：Natural Science Edition，2016，44(5)：137-143，150(in Chinese).

[167] 于雅洁，刘贤达，蒋启梅，等. 融合 LSTM-DNN 的工业安全态势预测模型[J]. 小型微型计算机系统，2023，44(3)：596-601.
YU Yajie，LIU Xianda，JIANG Qimei，et al. Industrial security situation prediction model based on LSTM-DNN[J]. Journal of Chinese Computer Systems，2023，44(3)：596-601(in Chinese).

[168] 余建，林志兴，谢彬. 灰色关联模型的网络安全态势感识预测方法[J]. 实验室研究与探索，2019，38(2)：31-35，70.
YU Jian，LIN Zhixing，XIE Bin. Network security situation awareness prediction method based on grey correlation model[J]. Research and Exploration in Laboratory，2019，38(2)：31-35，70(in Chinese).

[169] 翁芳雨. 基于随机博弈模型的网络安全态势评估与预测方法的研究与设计[D]. 北京：北京邮电大学，2018.
WENG Fangyu. Research and design of network security situation assessment and predication method based on stochastic game model[D]. Beijing：Beijing University of Posts and Telecommunications，2018(in Chinese).

[170] BERGHOUT T，BENBOUZID M，MUYEEN S M. Machine learning for cybersecurity in smart grids：a comprehensive review-based study on methods，solutions，and prospects[J]. International Journal of Critical Infrastructure Protection，2022，38：100547.

[171] MCCARTHY J，ALEXANDER O，EDWARDS S，et al. Situational awareness for electric utilities [R/OL]. Gaithersburg：National Institute of Standards and Technology，2019[2024-10-18]. https://doi.org/10.6028/NIST.SP.1800-7.

[172] 代闯闯，栾海晶，杨雪莹，等. 区块链技术研究综述[J]. 计算机科学，2021，48(S2)：500-508.
DAI Chuangchuang，LUAN Haijing，YANG Xueying，et al. Overview of blockchain technology[J]. Computer Science，2021，48(S2)：500-508(in Chinese).

[173] 张宁，王毅，康重庆，等. 能源互联网中的区块链技术：研究框架与典型应用初探[J]. 中国电机工程学报，2016，36(15)：4011-4022.
ZHANG Ning，WANG Yi，KANG Chongqing，et al. Blockchain technique in the energy internet：preliminary research framework and typical applications [J]. Proceedings of the CSEE，2016，36(15)：4011-4022(in Chinese).

[174] 裴凤雀，崔锦瑞，董晨景，等. 区块链在分布式电力交易中的研究领域及现状分析[J]. 中国电机工程学报，2021，41(5)：1752-1770.
PEI Fengque，CUI Jinrui，DONG Chenjing，et al. The research field and current state-of-art of blockchain in distributed power trading[J]. Proceedings of the CSEE，2021，41(5)：1752-1770(in Chinese).

[175] 严兴煜，高赐威，陈涛，等. 数字孪生虚拟电厂系统框架设计及其实践展望[J]. 中国电机工程学报，2023，43(2)：604-618.
YAN Xingyu，GAO Ciwei，CHEN Tao，et al. Framework design and application prospect for digital twin virtual power plant system[J]. Proceedings of the CSEE，2023，43(2)：604-618(in Chinese).

[176] 靳世雄，张潇丹，葛敬国，等. 区块链共识算法研究综述[J]. 信息安全学报，2021，6(2)：85-100.
JIN Shixiong，ZHANG Xiaodan，GE Jingguo，et al. Overview of blockchain consensus algorithm [J]. Journal of Cyber Security，2021，6(2)：85-100(in Chinese).

[177] 王雷，任南，李保珍. 区块链 51%双花攻击的进化博弈及防控策略研究[J]. 计算机工程与应用，2020，56(3)：28-34.
WANG Lei，REN Nan，LI Baozhen. Research on evolutionary game and prevention and control strategy of blockchain 51% double spend attack[J]. Computer Engineering and Applications，2020，56(3)：28-34(in Chinese).

[178] LIU Yuan，ZHANG Chuang，YAN Yu，et al. A semi-centralized trust management model based on blockchain for data exchange in IoT system[J]. IEEE Transactions on Services Computing，2023，16(2)：858-871.

[179] 施泉生，黄晓辉，胡伟，等. 基于区块链的改进智能合约电力交易模型[J]. 电力工程技术，2022，41(1)：11-18.
SHI Quansheng，HUANG Xiaohui，HU Wei，et al. Improved smart contract electricity transaction model based on blockchain[J]. Electric Power Engineering Technology，2022，41(1)：11-18(in Chinese).

[180] 钱鹏，刘振广，何钦铭，等. 智能合约安全漏洞检测技术研究综述[J]. 软件学报，2022，33(8)：3059-3085.
QIAN Peng，LIU Zhenguang，HE Qinming，et al. Smart contract vulnerability detection technique：a survey [J]. Journal of Software，2022，33(8)：3059-3085(in Chinese).

[181] 倪远东，张超，殷婷婷. 智能合约安全漏洞研究综述[J]. 信息安全学报，2020，5(3)：78-99.
NI Yuandong，ZHANG Chao，YIN Tingting. A survey of smart contract vulnerability research[J]. Journal of Cyber Security，2020，5(3)：78-99(in Chinese).

[182] 王晨旭，程加成，桑新欣，等. 区块链数据隐私保护：

研究现状与展望[J]. 计算机研究与发展，2021，58(10)：2099-2119.
WANG Chenxu，CHENG Jiacheng，SANG Xinxin，et al. Data privacy-preserving for blockchain：state of the art and trends[J]. Journal of Computer Research and Development，2021，58(10)：2099-2119(in Chinese).

[183] KANDI M A，KOUICEM D E，DOUDOU M，et al. A decentralized blockchain-based key management protocol for heterogeneous and dynamic IoT devices [J]. Computer Communications，2022，191：11-25.

[184] LE T V，HSU C L，CHEN Weixin. A Hybrid blockchain-based log management scheme with nonrepudiation for smart grids[J]. IEEE Transactions on Industrial Informatics，2022，18(9)：5771-5782.

[185] KAUR K，KADDOUM G，ZEADALLY S. Blockchain-based cyber-physical security for electrical vehicle aided smart grid ecosystem[J]. IEEE Transactions on Intelligent Transportation Systems，2021，22(8)：5178-5189.

[186] 赵丙镇，王栋，钱雪，等. 基于区块链的电力物联网信任网关设计与实现[J]. 中国电力，2021，54(7)：192-197.
ZHAO Bingzhen，WANG Dong，QIAN Xue，et al. Design and implementation of blockchain-based trust gateway for power internet of things[J]. Electric Power，2021，54(7)：192-197(in Chinese).

[187] WANG Yuntao，SU Zhou，ZHANG Ning，et al. SPDS：a secure and auditable private data sharing scheme for smart grid based on blockchain[J]. IEEE Transactions on Industrial Informatics，2021，17(11)：7688-7699.

[188] LU Weifeng，REN Zhihao，XU Jia，et al. Edge blockchain assisted lightweight privacy-preserving data aggregation for smart grid[J]. IEEE Transactions on Network and Service Management，2021，18(2)：1246-1259.

[189] KURT M N，YILMAZ Y，WANG Xiaodong. Secure distributed dynamic state estimation in wide-area smart grids[J]. IEEE Transactions on Information Forensics and Security，2020，15：800-815.

[190] KUMARI A，PATEL M M，SHUKLA A，et al. ArMor：a data analytics scheme to identify malicious behaviors on blockchain-based smart grid system[C]// GLOBECOM 2020-2020 IEEE Global Communications Conference. Taipei，China：IEEE，2020：1-6.

胡金炜

在线出版日期：2024-05-14。
收稿日期：2023-10-16。

作者简介：
胡金炜(1998)，男，硕士研究生，研究方向为虚拟电厂、区块链安全、应用密码学，jwhu@seu.edu.cn；
*通信作者：张玉健(1984)，男，副教授，硕士生导师，研究方向为区块链与系统安全、智能电网安全，yjzhang@seu.edu.cn。

(**责任编辑** 乔宝榆，李泽荣)