DOI 10.15302/J-SSCAE-2026.04.021

# 电力–算力跨境交互安全：风险机理、防护技术与研究展望

**王琦[1]，吴舒坦[1]，汤奕[1*]，郑玉平[2]**

（1. 东南大学电气工程学院，南京 210096；2. 国网电力科学研究院有限公司（南瑞集团有限公司），南京 211106）

**摘要：**随着人工智能（AI）智能体、大模型应用的快速发展，算力需求呈现高度动态化、平台化、全球化的配置趋势。算力任务的生成与调用由人工触发、本地执行逐步转向智能体自主生成、跨平台调用、跨境执行，使传统上以本地电网与数据中心为核心的电算协同安全边界发生深刻变化，相应的数据流、算力流、能量流的耦合关系更加复杂，电算交互安全问题由单系统防护转向跨域耦合条件下的综合风险治理。本文围绕AI智能体驱动下电力–算力跨境交互（电算跨境交互）面临的新型安全问题，深入梳理并论述了电算跨境交互的发展形态、运行特征、安全风险、防护技术、未来研究方向。分析了电算跨境交互在系统边界、调度机制、负荷特性等方面的演化特征，梳理了算力需求生成、跨域交互、电力负荷响应的耦合关系。归纳了数据安全、算力调度安全、电力负荷操纵、跨域级联故障等方面的关键安全风险，揭示了数据可信性下降、调度决策失真、负荷重构异常、跨域级联传播的风险演化链条。凝练了数据保护、调度治理、负荷控制、系统监测等防护技术并讨论了跨境交互环境下的适用性和局限性，展望了算力需求生成、算力调度约束、跨域协同防御、内生安全架构等电算跨境交互安全的未来研究方向。相关内容可为构建安全可信的电算跨境交互体系提供理论支持与实践参考。

**关键词：**电力–算力协同；跨境算力交互；AI智能体；安全风险；防护技术

**中图分类号：**TM73　　**文献标识码：**A

# Security of Cross-Border Power–Computing Interaction: Risk Mechanisms, Protection Technologies, and Prospects

**Wang Qi[1], Wu Shutan[1], Tang Yi[1*], Zheng Yuping[2]**

(1. School of Electrical Engineering, Southeast University, Nanjing 210096, China; 2. State Grid Electric Power Research Institute (NARI Group Corporation), Nanjing 211106, China)

**Abstract:** With the rapid development of artificial intelligence (AI) agents and large model applications, the demand for computing power is becoming increasingly dynamic, platform-based, and globally distributed. The generation and invocation of computing tasks are gradually shifting from manual triggering and local execution to autonomous generation by AI agents, cross-platform invocation, and cross-border execution. This transition is profoundly reshaping the conventional security boundary of power – computing coordination, which has traditionally been centered on local power grids and data centers. The coupling among data flows, computing

**收稿日期：**2026-04-09；**修回日期：**2026-06-22

**通讯作者：***汤奕，东南大学电气工程学院教授，研究方向为电力系统网络安全；E-mail: tangyi@seu.edu.cn

**资助项目：**国家自然科学基金项目(52477077)

**本刊网址：**sscae.engineering.org.cn

flows, and energy flows is consequently becoming more complex, and the security of power–computing interaction is evolving from single-system protection toward comprehensive risk governance under cross-domain coupling. Focusing on the emerging security issues associated with cross-border power–computing interaction driven by AI agents, this study reviews the development patterns, operational characteristics, security risks, protection technologies, and future research directions of cross-border power–computing interaction. Moreover, the evolutionary characteristics of cross-border power–computing interaction are analyzed in terms of system boundaries, scheduling mechanisms, and load characteristics, and the coupling relationships among computing demand generation, cross-domain interaction, and power–load response are clarified. Key security risks related to data security, computing power scheduling security, power–load manipulation, and cross-domain cascading failures are summarized, revealing a risk evolution chain comprising degraded data trustworthiness, distorted scheduling decisions, abnormal load reconfiguration, and cross-domain cascading propagation. Additionally, protection technologies involving data protection, scheduling governance, load control, and system monitoring are summarized, and their applicability and limitations in cross-border interaction environments are discussed. Future research directions are further outlined in the areas of computing demand generation, computing scheduling constraints, cross-domain collaborative defense, and endogenous security architectures. This study is expected to provide theoretical support and practical guidance for developing secure and trustworthy cross-border power–computing interaction systems.

**Keywords:** power–computing coordination; cross-border computing interaction; AI agents; security risks; protection technologies

## 一、前言

近年来，以大模型为核心的人工智能（AI）技术快速发展，AI智能体的出现使AI系统由传统的模型调用模式演进为具有自主规划与任务执行能力的智能体模式。AI智能体可根据任务目标自动生成计算任务，通过调用模型接口、工具平台、代码执行环境等执行复杂任务流程。然而，从任务生成、算力调用到结果反馈的自动化运行模式，将显著提升AI系统对算力资源的需求规模。例如，算力聚合平台OpenRouter积累了超过100亿个真实调用样本，体现了推理流量快速增长的趋势[1]。同时，算力资源的组织与调用方式发生显著变化，算力任务由智能体根据目标特性自动生成并跨平台执行，逐步形成跨区域或跨境的动态调用模式。因此，AI智能体驱动的电力–算力跨境交互（电算跨境交互）成为新的电算交互形态。

在电算跨境交互形态下，电力系统、算力系统之间的耦合关系呈现新的特点。算力任务可根据算力价格、网络条件、资源可用性而在不同地区的数据中心之间迁移，使数据中心负荷具有明显的跨区域动态变化特征[2]。与传统上固定负荷的数据中心相比，跨境算力任务调度能够在短时间内改变某一地区数据中心的计算规模，从而对电力系统运行产生影响[3]。在AI智能体驱动的任务执行模式下，算力调用不再完全由人工控制，而是由智能体根据任务需求自动生成并持续扩展任务链，相应算力需求的形成机制与演化过程更加复杂。由此，传统的云计算安全问题、电力系统运行安全问题不再相互独立，算力任务生成、算力调度、数据中心负荷之间形成紧密耦合关系，受到攻击后的影响可能通过算力负荷变化进一步传导至电力系统运行，形成跨域传播的系统性风险。此外，AI智能体自身的不确定性也引入新的安全风险，如国家互联网应急中心的风险提示表明，AI智能体易受提示词注入、系统提示词泄露、工具调用越权等攻击[4]。攻击者可在网页内容中嵌入隐藏指令以诱导智能体读取本地文件并上传至远程服务器，从而窃取数据；也可诱导用户访问恶意链接以获取系统词元，进而远程控制AI智能体并执行恶意操作。可见，在AI智能体驱动的算力调用模式下，安全问题不仅可能导致数据泄露或系统被控，而且能够通过异常算力任务生成及调度影响数据中心负荷，从而对电力系统运行造成潜在冲击。

围绕电算交互，有研究开始从运行优化分析延伸到安全与韧性探索。① 数据中心接入条件下的电力系统安全运行[5-9]，将数据中心视为高功率且密度可调负荷，关注接入后对电网稳定性和安全裕度的影响。② 统一管理域内电算安全协同[10-13]，重点分析区域范围内算力任务的时间分布和空间迁移对电力负荷分布的影响，以协调算力分布与能源供给的方式降低对局部电网的冲击。③ 耦合系统跨域安全与韧性提升[14-18]，关注信息系统与物理系统之间的耦合关系，分析数据异常、控制偏差、负荷变化的相互影响，构建更为完整的安全防护框架以提升系统的整体安全性与韧性。既有研究进展表明，在“数据流–算力流–能量

流”耦合结构中分析电算交互相关的安全问题，有助于揭示信息系统异常对电力系统运行影响的跨域传播机制。

在上述研究的基础上，AI智能体驱动使电算交互系统在运行边界、耦合方式、任务组织形态等方面发生深刻变化，需要从新的视角刻画相关安全问题。① 系统运行边界由区域内闭环向跨区域开放扩展，数据流、算力流、能量流呈现跨区域、多主体耦合特征，开展安全分析需要从局部视角拓展至面向跨区域交互环境的整体描述。② 系统耦合关系由单一环节向多环节联动演化，数据处理、算力调度、电力负荷之间的关联更加紧密，风险可能沿跨域链条逐步传导；安全分析对象需要由单点问题拓展为多环节耦合效应，以刻画风险传播路径及其级联影响。③ 算力需求生成方式由人工触发向智能体驱动转变，算力任务呈现自主生成、持续调用、跨平台迁移等特征，应用规模与演化过程具有更强的不确定性，开展安全分析需要从静态需求假设拓展为面向任务动态演化过程的分析框架。

本文围绕电算跨境交互环境中的安全问题开展综述与展望。总结算力任务跨境迁移背景下电算交互系统的发展形态与运行特征，讨论系统结构、算力调度机制、电力负荷特性等方面的变化。从数据安全、算力调度安全、电力负荷操纵、跨域级联故障等方面出发，分析电算交互可能面临的安全风险。梳理现有相关防护技术，讨论在跨境算力交互环境中的适用性与局限性。结合AI智能体驱动算力任务生成与跨境调用的发展趋势，前瞻未来电算交互安全的主要研究方向。

## 二、电算交互跨境需求、发展形态与特征演化

电算跨境交互涉及算力任务迁移、算力服务调用、数据处理、电力负荷变化、多主体协同等层面，不同语境下跨区域、跨境、跨域概念存在差别。跨区域主要是从地理空间、电网运行区域的角度出发，认为算力任务或数据中心负荷在同一国家或统一管理体系内的不同地区之间进行迁移与重分布（如国内不同数据中心集群之间的任务调度）。跨境主要是从国家边界和司法管辖边界的角度出发，认为算力请求、数据处理、模型服务或算力服务交付过程等跨越不同的国家或法域（如用户通过互联网调用境外数据中心提供的AI推理服务）。跨域主要是从系统边界、管理边界、安全边界的角度出发，认为电力系统、算力平台、通信网络、云服务商、监管主体等系统域或管理域之间进行的交互与风险传播。跨区域、跨境、跨域既有联系又有区别：跨境交互通常伴随跨区域资源配置并可能引发跨域安全风险，但跨区域调度不必然跨境，跨域风险也不必然以跨境为前提。基于上述边界概念，本研究从电算交互跨境需求、发展形态演化、运行特征演化三个方面展开分析，为进一步的安全风险与防护技术讨论提供概念和场景基础。

### （一）电算交互跨境需求

AI智能体驱动算力需求快速增长，也带来突出的能源消耗问题。国际能源署认为，AI推理与训练任务的快速增长正在显著提升全球数据中心的电力需求，预计2030年全球数据中心电力需求将超过1000 TW·h[19]。当前，不同地区的算力资源和能源资源配置差异明显。北美地区AI产业需求旺盛，但局部电力供应增长受限，预计2030年将出现24 GW的电力容量缺口[20]；数据中心建设周期通常为1~3年，而输电基础设施从规划、审批到建成通常需要5~15年[21]，导致部分地区的数据中心扩张受到电力接入能力的限制。欧洲普遍存在能源价格较高的问题，如2025年欧盟工业用电价格约为0.19欧元/kW·h[22]；电力市场价格波动较大，在需求高峰或能源供应紧张时期批发电价曾突破100欧元/MW·h[23]；电价水平较高且波动性显著，叠加电力供应结构不稳定，使数据中心建设与运营面临较高的成本压力。我国在电力供应规模、新能源装机容量方面具有一定优势，促进了数据中心和算力基础设施的持续扩展。能源成本优势、算力基础设施扩张共同推动AI推理服务成本的下降，国内开源大模型的应用程序编程接口（API）服务价格明显低于国际主流闭源模型价格，一些开源模型推理接口价格已不到国外闭源模型服务价格10%[24-25]。然而，我国电力与算力资源在空间分布上存在结构性不均衡现象，新能源装机占比较高的西部地区仍然面临较大的消纳压力。

在全球资源禀赋和规模成本差异的作用下，通过跨境算力调用实现算力资源与能源资源的空间匹配逐渐成为新的需求。已经出现的“词元出海”是电算跨境交互需求的典型表现，境外用户通过互联网调用我国云平台提供的开源AI智能体推理接口，计算任务在境内数据中心完成，而推理结果以词元或API调用结果形式返回境外用户。需要指出的是，跨境API调用并不等同于数据中心算力资产真正跨境运营，也不必然意味着电力系统形成跨境耦合。本研究讨论的“算力出海”主要指算力服务的跨境交付，即境外用户调用境内数据中心提供的模型推理或计算服务，而服务器、图形处理器（GPU）等算力资产仍部署在算力提供方所在地区。“数据出海”则强调，数据跨越国家或法域边界进行传输、存储或处理，是否实际发生需要结合数据内容、处理位置、合规要求来具体判断。“能源价值出海”并非指电能本身跨境传输，而是指本地电力用于支撑面向境外用户交付的算力服务，使电力消耗承载的服务价值实现跨境转化。因此，虽然电力消耗仍发生在算力提供方所在地区，但算力服务价值已经通过跨境算力调用实现国际交付，从而形成由算力服务驱动的能源价值跨境流动。

### （二）电算交互发展形态演化

电算交互需求不断演变，发展形态大致经历本地电算耦合、跨区域电算协同、电算跨境交互3个阶段（见图1）。

在本地电算耦合阶段，计算任务主要在本地数据中心执行，电算耦合局限于单一区域电力系统；算力资源通常部署在靠近用户需求的数据中心，计算任务由本地应用提交并在本地服务器上完成计算。该阶段的典型场景包括本地自建数据中心、企业园区数据中心、金融和政务等专用机房，相应的数据流、算力流、能量流通常位于同一管理边界内。电算耦合主要通过电价引导、需求响应、计算任务调度等方式，开展数据中心负荷与电力系统运行状态之间的协调。早期的互联网企业、金融机构自建数据中心，多部署于一线城市或业务集中的区域，如2008年北京奥运会期间建设的“数字北京”数据中心主要服务奥运信息系统，相应算力负荷与北京市电网直接耦合。

在跨区域电算协同阶段，随着数据中心规模扩大、通信网络能力提升，计算任务能够在同一国家或区域内的多个数据中心之间迁移。该阶段的典型场景包括国内云资源调度、同一云服务商在国内多个区域数据中心之间的任务迁移，电力负荷影响表现为不同区域数据中心之间的负荷再分布。我国“东数西算”工程通过算力网络将东部地区的计算需求传输至西部能源资源丰富地区的数据中心执行，实现算力需求与能源供给之间的空间匹配[26]。深圳市腾讯计算机系统有限公司、阿里巴巴集团控股有限公司等企业在内蒙古、宁夏、甘肃等省份建设了大型数据中心集群，将东部地区的业务负载部分迁移至西部地区的节点上运行，有效降低了能耗成本并充分利用了新能源资源[27]。计算任务通过高

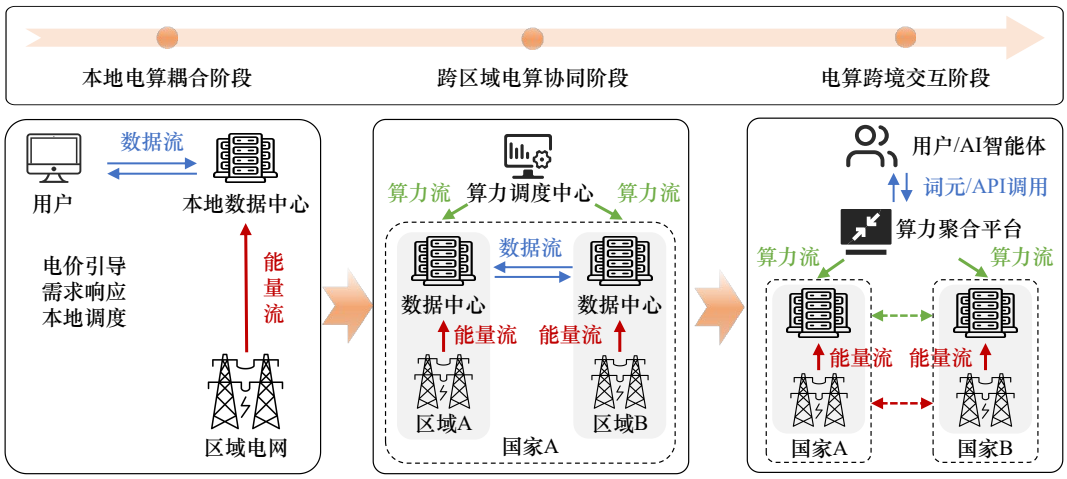


图1　电算交互发展形态演化示意图

速光纤网络在不同数据中心间传输，但算力调度发生在统一的管理体系内，电算协同仍以国家或区域为边界。

在电算跨境交互阶段，全球云平台、算力聚合平台、AI智能体应用迅速发展，算力任务能够突破国家或区域边界，在不同国家或地区的数据中心之间动态迁移。该阶段的典型场景包括跨境AI推理服务和境外用户调用境内模型API、全球多云环境下的算力调度，相应的用户请求、算力服务、数据处理、电力消耗可能分属不同国家或法域。例如，亚马逊AWS、微软Azure、谷歌云等全球云服务品牌在北美、欧洲、亚太地区大规模部署了数据中心，支持用户跨区域调用算力资源；其中，亚马逊AWS形成覆盖39个地理区域、123个可用区的全球基础设施网络，为用户根据时延、成本、可用容量、合规要求的跨区域调用算力资源提供了基础条件。同时，云服务商可将部分高能耗计算任务部署在电价较低、可再生能源资源丰富、数据中心容量较充足的地区，以降低运营成本并提高资源利用效率。在AI大模型应用场景下，用户可以通过互联网调用云平台提供的大模型推理接口，用户请求经由国际通信网络、海底光缆传输至位于不同国家的数据中心完成计算，再以词元或API结果形式返回。可见，算力任务的生成地、执行地、电力消耗地可能发生空间分离，算力资源逐步由本地部署演变为跨境乃至全球范围内的协同配置。

### （三）电算交互运行特征演化

电算交互形态演变并非电算协同模式在空间尺度上的简单扩展，而是算力任务生成方式、算力资源组织结构、电力负荷形成机制共同演化的结果。从本地耦合、跨区协同到跨境交互阶段的核心变化体现在：算力任务的生成机制由用户显式请求转向由智能体自主生成并通过工具调用形成连续计算请求，算力资源的组织方式由本地或区域内部署逐步演变为跨平台、跨区域乃至跨国的算力网络结构，电力系统面对的数据中心负荷由相对稳定的业务负荷转变为受信息系统实时驱动的动态负荷。这些变化使电力系统、算力平台、通信网络之间的耦合关系复杂化，传统上以区域电网–本地数据中心为核心的电算协同分析框架难以完整刻画新的运行机理。

1. 系统边界

在AI智能体的驱动下，电算交互的边界发生了实质性变化。在传统的电算协同中，用户请求、任务调度、算力执行、电力供给通常位于同一运营体系或同一地理区域内，数据流、算力流、能量流虽然存在耦合关系，但系统边界相对清晰、运行链条较为封闭。在跨境交互环境下，系统结构逐渐演化为由多个独立主体共同参与的开放体系，用户请求、智能体执行、算力聚合平台、异地数据中心、区域电网分别位于不同平台上、不同空间范围内，系统运行涉及多个云平台、通信网络、电力系统。例如，北美地区用户通过应用程序发起请求，智能体在本地或云端解析任务并调用算力聚合平台接口，任务被调度至位于我国西部或北欧地区的数据中心执行，计算过程依赖全球通信网络传输，而数据中心的电力消耗则由当地电网承担。此时，数据流决定任务内容与调用路径，算力流决定任务执行位置与迁移方向，能量流表现为不同地区数据中心电力需求的空间分布，3个方面在算力聚合平台、通信网络的支撑下形成紧密耦合。

电算跨境交互在本质上不再是单纯的算力负荷接入问题，而是表现为多系统耦合的运行问题，核心特征体现在系统边界由本地扩展为跨域结构、算力资源由单一数据中心扩展为全球算力网络、电力负荷变化由单一区域扩展为跨区域耦合。这种边界开放化虽使系统运行更加灵活，但也意味着系统内部各环节之间的耦合关系更加复杂。一方面，系统运行边界由电网、数据中心构成的二元结构扩展为包含任务请求、智能体、算力平台、数据中心节点、电力系统在内的多层结构，任一环节的异常都可能沿着耦合链条向其他环节传播。另一方面，系统控制逻辑由传统的区域内部闭环逐渐演变为依赖外部算力平台、通信基础设施的开放式控制结构，数据中心的算力负荷不仅由本地业务需求决定，而且受到远端任务请求、交互策略的影响，使算力系统的不确定性开始直接作用于电力系统的运行过程。

2. 调度机制

与传统的云平台调度相比，AI智能体驱动下的算力调度表现出更强的自主性、动态性、链式扩展特征。传统的算力调度通常由平台根据资源占用、成本、时延等因素进行统一分配，任务来源较为明

确，调度目标相对固定，整个运行过程具有一定的可预测性[28]。在AI智能体场景中，任务通常不是一次性提交，而是随着任务执行过程不断生成新的计算请求；智能体在执行任务过程中可以根据中间结果继续调用模型服务、访问外部工具并重新选择算力节点，从而出现多轮调用与链式调度[29]。当前，算力聚合平台通过统一接口整合多种开源和闭源模型服务，使用户或智能体可以在同一任务过程中调用不同模型。例如，在一次复杂任务执行中，智能体可根据任务需求选择不同模型进行推理（如调用开源的MiMo、Minimax、Llama系列模型），在不同云平台或算力节点之间切换执行。这种多模型、多节点的动态选择机制，使算力调度从固定资源分配转变为面向任务过程的实时决策。

在这一模式下，算力调度呈现出三方面变化。算力调度逐步由单一平台调度转变为多平台协同调度，算力聚合平台通过统一接口整合不同云平台和模型服务，使计算任务能够在不同算力节点之间灵活切换。算力调度由静态策略转向动态调度，智能体可根据任务需求、模型能力、资源状态自动选择算力服务提供方，进而实现任务的自动化分配。调度决策因素更加多样化，在传统的算力成本、资源利用率以外，调度过程纳入网络延迟、模型性能、服务可靠性、能源成本等因素的影响。因此，算力调度机制逐步发展成为连接信息系统与电力系统的关键中间环节，一旦任务生成逻辑、资源状态感知、调度决策过程受到干扰，异常影响将从算力资源配置传导至数据中心功率需求变化，进而干扰电力系统运行。

3. 负荷特征

在电算跨境交互环境中，数据中心负荷的形成机制也在发生变化。传统的数据中心负荷虽有一定的波动性，但总体上仍可视为与业务规模相对应的连续负荷，变化速率和空间分布基本稳定[30]。然而在跨境算力交互模式下，数据中心负荷呈现出明显的信息驱动特征，功率需求不再仅由本地业务规模决定，而是更多受到远端任务请求、算力调度策略、智能体调用行为的影响。以欧洲数据中心枢纽之一的爱尔兰为例，大型AI企业在当地集中部署数据中心，用电量占全国总量的比例超过20%[31]，数据中心负荷在部分地区成为电力需求结构中的重要组成部分，在高峰时段对电网运行产生明显影响。相应地，在大模型发布、应用集中接入期间，大量用户请求可能通过云平台被调度至同一区域内的数据中心执行，从而在短时间形成算力需求集中释放，体现出信息系统对电力负荷的直接驱动作用。

负荷变化主要体现在三方面：触发机制发生改变，数据中心负荷不再仅由本地业务增长驱动，而是由跨区域任务迁移或智能体批量调用触发；负荷空间分布的形成机制发生变化，不同区域数据中心的负荷水平不再完全由本地需求决定，而是由跨区域任务流、算力调度共同影响；负荷异常的来源更加复杂，数据中心功率异常不一定源于电力系统内部故障，也可能由信息系统中的异常任务、调度偏差、平台接口异常引发。因此，电算跨境交互中的数据中心负荷虽然在电力系统中表现为功率需求变化，但与一般可调负荷存在差异。负荷变化不仅受本地业务、电力侧调节指令影响，而且可由AI智能体任务生成、模型API调用量变化、算力聚合平台调度策略、跨区域任务迁移共同驱动；电网侧可观测到功率变化，但未必能够直接识别背后的任务来源、调用链路、迁移原因，由此形成“物理侧可观测、信息侧驱动机制不透明”的新型负荷特征。

## 三、电算跨境交互安全风险

在电算跨境交互环境中，系统安全已由单一系统防护转变为耦合条件下的综合风险问题，相应风险可沿数据、调度、负荷、系统4个层级传递。数据异常首先破坏任务输入、资源状态的可信性，调度异常进一步改变任务分配，随后映射为数据中心负荷变化，当扰动超出局部调节能力时还可能向其他区域和系统扩散。AI智能体在实现自主执行任务能力时，通常被授予访问本地文件系统、读取环境变量、调用外部服务接口等较高的系统权限，这种高权限运行模式在提升自动化能力的同时显著扩大了攻击面。近期的安全事件表明，攻击者可以通过提示词注入诱导智能体泄露系统密钥或敏感信息，也可能通过恶意插件、扩展功能实施插件投毒攻击以窃取凭证信息或植入恶意程序。此外，一些智能体框架存在安全漏

洞，如国家信息安全漏洞库采集的OpenClaw漏洞已有82个（含12个超危漏洞、21个高危漏洞），可被攻击者利用以实施未授权访问、敏感数据窃取、权限提升、远程代码执行等高风险操作。为此，围绕数据、算力、负荷、系统4个层级分析电算跨境交互环境中的主要安全风险，揭示不同类型风险之间的内在关联、可能引发的影响后果（见图2）。

### （一）数据安全风险

在电算跨境交互环境中，数据安全问题不再局限于数据隐私泄露或访问越权，而且表现为数据内容、数据传输路径、数据可信性共同失控的复合性风险。这是因为，AI智能体在执行任务过程中需要持续调用模型、工具和外部服务接口，数据不再沿固定链路在本地系统内部流动，而是在多平台、多节点、多地域之间进行动态传输与处理；数据在任一环节被泄露、篡改或污染，相应影响将不局限于信息系统层面，而是通过任务生成与调度决策进一步作用于算力资源分配，进而改变数据中心功率需求并对电力系统运行产生影响。

与传统的云计算环境相比，电算跨境交互数据安全风险呈现新的特点。数据暴露面扩大，智能体任务通常由多轮推理、工具调用、上下文记忆构成，敏感数据可在任务执行链条中反复被访问与传递，从而显著增加数据泄露风险。数据篡改的影响范围扩大，在智能体驱动场景中模型输入、环境变量、中间推理结果如被篡改，相应影响可能在后续推理与任务分发过程中不断累积并最终导致算力调度偏差。数据安全与电力运行之间的关联性增强，电算交互环境下的数据异常不仅影响模型输出结果，而且通过调度决策偏差引发算力任务异常迁移与负荷预测偏离，进而在电力系统中体现为负荷扰动。

电算跨境交互数据安全风险的4类表现形式（见表1）之间存在一定递进关系。数据泄露、权限滥用主要对应数据访问边界失控，直接后果是敏感

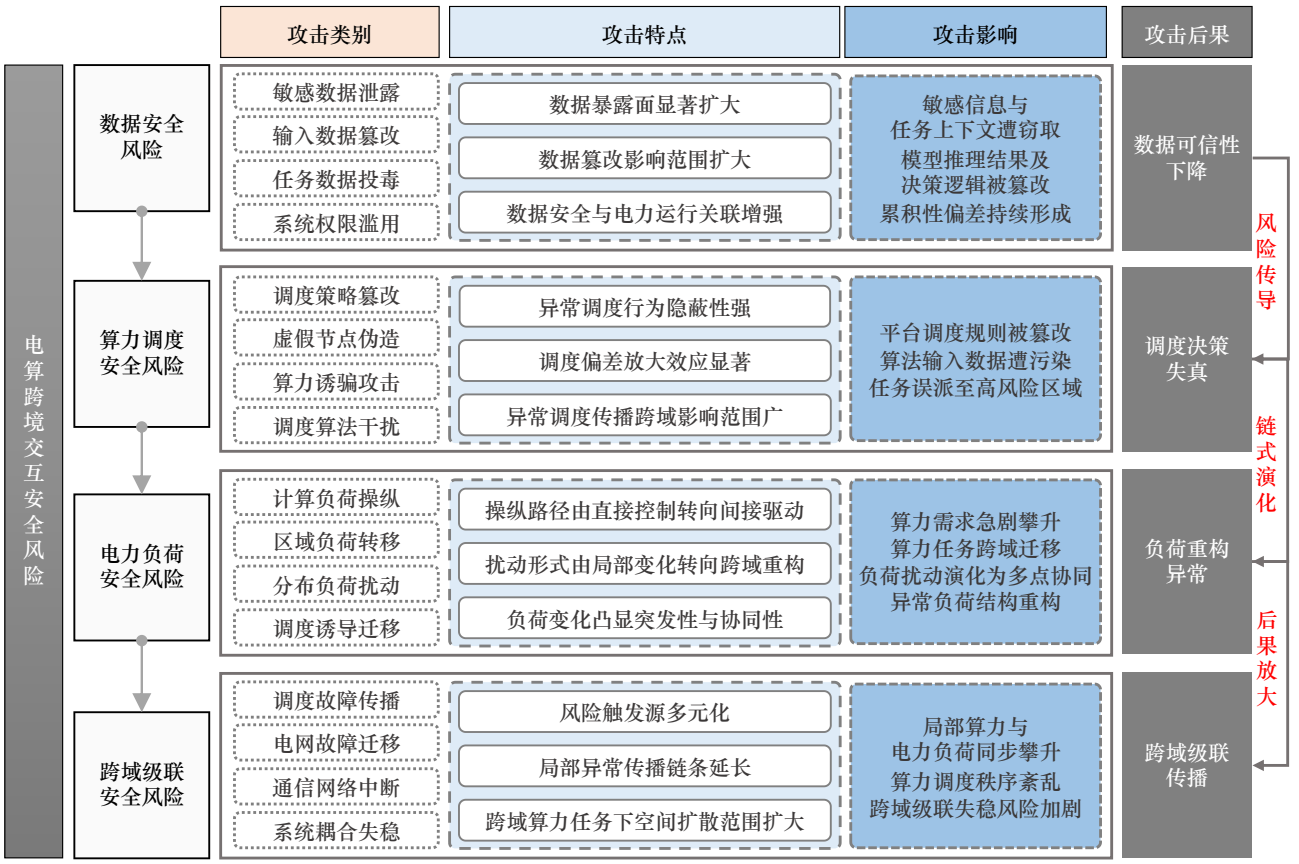


图2　电算跨境交互安全风险类别及影响后果

信息暴露、任务上下文被窃取。数据篡改、数据投毒对应数据可信性失控，危险性在于会直接改变模型推理结果和任务决策逻辑。尤其是在AI智能体场景下，数据投毒不再只是单次输入攻击，而是通过多轮推理、持续上下文记忆形成累积性偏差。因此，数据安全问题不仅影响信息系统自身，而且通过算力调度过程进一步作用于数据中心功率需求，成为电算交互安全风险链条中的起点。

### （二）算力调度安全风险

算力调度是连接数据处理过程、电力负荷形成的关键环节，直接决定计算任务的执行位置、执行规模和时间分布。一旦调度过程受到干扰，相应影响将由信息层迅速传导至算力资源分布，进一步表现为数据中心功率需求的空间与时间重构。

在电算跨境交互场景中，任务通常由智能体在执行过程中动态生成，通过调用不同模型接口或服务平台在多个算力节点之间持续迁移。调度系统需要实时感知算力资源状态、网络条件、任务需求变化，使调度过程由静态分配演变为持续开展的动态决策过程。调度层不仅承担资源优化功能，也成为承接数据异常并向物理系统传导的重要中间环节。同时，跨平台、跨区域的算力交互进一步扩大了调度系统的攻击面。调度决策依赖节点状态、价格信号、服务性能等外部信息，一旦这些信息被伪造或操控，系统可能在正常调度的表象下执行异常任务迁移。攻击者可通过提示词注入、工具链操控影响任务调用路径，从而间接干预算力调度行为；尽管并不直接作用于电力系统，但可通过调度过程改变算力负荷在不同区域之间的分布。

算力调度安全风险具有以下特征：隐蔽性强，异常调度多表现为资源优化或任务迁移行为，难以在早期与正常调度区分；放大效应显著，智能体具备持续任务生成能力，一次调度偏差可能演化为大量连续任务的系统性偏移；跨区域影响突出，调度异常可在多个算力节点之间传播，进而引发跨区域负荷变化。

电算跨境交互算力调度安全风险的4类表现形式（见表2）分别对应调度链条中的不同薄弱环节。调度策略篡改、调度算法攻击主要作用于调度逻辑本身：前者改变平台规则，后者扰乱算法输入。虚假算力节点、算力诱骗攻击主要作用于调度对象感知过程，通过伪造资源状态误导系统将任务派发至

表1　电算跨境交互数据安全风险

| 风险类别 | 具体表现 | AI智能体驱动的场景特点 | 风险后果 |
|---|---|---|---|
| 敏感数据泄露 | 本地文件、环境变量或API密钥在跨平台调用中泄露 | 访问权限高，数据跨节点、跨平台流动 | 敏感信息暴露，并可能被用于伪造请求或操纵调度 |
| 输入数据篡改 | 模型输入、提示词或推理结果被恶意修改 | 任务规划依赖模型输出，错误信息可沿任务链传播 | 任务指令异常，导致错误分配或异常迁移 |
| 任务数据投毒 | 恶意数据或提示词持续干扰任务决策 | 多轮推理与上下文记忆放大投毒影响 | 任务规划或负荷预测偏差，引发算力需求异常 |
| 系统权限滥用 | 攻击者利用过高权限控制智能体或工具调用 | 可直接执行系统操作并自动扩展任务 | 批量生成任务或调用算力资源，造成数据中心负荷异常 |

表2　电算跨境交互算力调度安全风险

| 风险类别 | 具体表现 | AI智能体驱动场景特点 | 风险后果 |
|---|---|---|---|
| 调度策略篡改 | 修改调度规则或任务优先级，引导任务集中分配 | 任务持续生成，异常规则可长期影响分配结果 | 算力负荷集中迁移，局部电网负荷快速上升 |
| 虚假节点伪造 | 伪造资源状态或注册虚假算力节点 | 跨平台调度依赖外部节点信息 | 资源状态误判，算力分布失衡 |
| 算力诱骗攻击 | 伪造性能或价格信号，诱导任务迁移 | 智能体自动选择高性能或低成本服务 | 任务向特定区域聚集，引发区域负荷异常 |
| 调度算法干扰 | 利用恶意请求或异常参数扰乱调度算法 | 连续任务生成放大攻击规模 | 资源分配失衡，数据中心负荷异常波动 |

不可信或高风险区域。相比电网调度安全问题，这些风险在AI智能体场景中更具危害性，因为智能体具有自主任务扩展能力，一次调度偏差可迅速演化为大量连续任务的系统性异常迁移。算力调度安全不再只是资源管理问题，而是成为典型的信息物理攻击入口。

### （三）电力负荷安全风险

数据中心是电力系统中的大容量负荷，数据中心的接入容量、最大需量、供电方案需经过供电和调度部门校核。电算跨境交互场景下应关注的风险主要是在异常任务集中生成、跨区域任务同步迁移、多数据中心负荷同向变化、局部电网运行裕度不足等条件叠加后可能形成的短时负荷冲击或区域负荷再分布。从影响机理看，算力任务规模、并发度变化会首先作用于服务器、GPU等信息技术（IT）设备利用率，进一步带动冷却、供配电系统功率变化，最终表现为数据中心总功率需求变化。这种变化如具有较高幅值、较快爬坡速率、较强空间集中性，将进一步影响潮流分布、备用容量、运行安全裕度。

2024年，美国弗吉尼亚州出现了数据中心负荷在数秒内大规模脱网（约1500 MW）并导致系统频率显著上升的事件[32]，表明吉瓦级、同步化、快速变化的数据中心负荷具备影响电网运行状态的能力。英国提出了2030年形成6 GW的AI数据中心容量目标[33]，也反映出算力负荷的规模化与集中化趋势。当算力任务异常生成或调度失衡导致上述因素叠加时，可能进一步放大负荷扰动并对电网运行安全形成潜在冲击。因此，电力负荷安全风险可视为调度层异常在物理系统中的具体表现，是信息侧异常向电力系统传导的关键环节。

与传统负荷攻击相比，电算跨境交互负荷操纵具有鲜明特征。操纵路径由直接控制转向间接驱动，攻击者无需直接控制电力设备，通过影响智能体任务生成逻辑或调度决策即可间接改变数据中心的算力需求。扰动形式由局部变化转向跨区域重构，算力任务可在不同区域数据中心之间迁移，使负荷表现为跨区域联动变化。负荷变化具有更强的突发性与协同性，AI智能体具备连续任务生成能力，可在短时间内触发大规模计算请求，可在多个数据中心同时发生，进而放大负荷扰动影响。因此，电算跨境交互中的负荷风险不仅表现为负荷总量变化，而且体现为负荷爬坡、空间转移、多点同步扰动、短周期波动等异常形态。

电算跨境交互电力负荷安全风险的4类表现形式（见表3）反映了负荷操纵在时间、空间、调度过程等层面的典型演化路径：计算任务洪峰攻击对应短时间内的集中冲击，负荷转移攻击对应不同区域之间的负荷再分布，分布式负荷攻击对应多节点同步扰动，调度诱导攻击对应正常调度表象下的异常重构。此外，不同类型风险对电网运行的影响程度不仅取决于算力需求变化幅度，而且与扰动持续时间、区域集中程度、节点同步性、调度系统的响应方式密切相关。因此，电算跨境交互负荷风险分析应从数据中心功率需求变化延伸到电网运行约束层面，综合关注局部供电裕度、潮流分布、备用容量、安全裕度等指标。

### （四）跨域级联安全风险

跨域级联风险指局部异常经由任务迁移、负荷重分配、电网响应扩散到其他区域或系统并进一步引发新的运行异常。2025年发生的“4·28西班牙–葡萄牙大停电”事件表明，在跨区域互联电网中，

表3　电算跨境交互电力负荷安全风险

| 风险类别 | 具体表现 | AI智能体驱动场景特点 | 风险后果 |
|---|---|---|---|
| 计算负荷操纵 | 通过恶意请求或操纵智能体集中生成推理任务 | 任务可自动连续生成，算力需求快速放大 | 数据中心负荷尖峰或快速爬坡，增加局部供电与备用压力 |
| 区域负荷转移 | 诱导算力任务迁移至特定区域 | 任务可在多区域数据中心间动态调度 | 负荷空间分布改变，目标区域供电裕度下降、潮流重构 |
| 分布负荷扰动 | 多个数据中心同时出现异常算力任务请求 | 多智能体或自动化任务可在多个算力节点同步生成请求 | 多点负荷同步变化，增加备用及调频调压压力 |
| 调度诱导迁移 | 操纵资源状态、价格信号或调度策略 | 自动调度依赖实时资源与成本信息 | 任务异常迁移，引发负荷反复爬坡和调度计划偏差 |

局部扰动可通过电力潮流重构与控制响应而在多个区域之间快速传播，进而引发连锁失稳甚至大范围停电[34]。跨域耦合会增加系统对局部异常的敏感性，不同区域、各个子系统之间的强耦合关系可能放大扰动影响并削弱系统的整体可控性。

在电算跨境交互环境中，算力任务生成、执行、迁移过程高度动态，局部异常更容易通过任务调度、功率重分配等机制在不同区域之间扩散，相应风险具有突出特征：触发源多元化，风险触发不再局限于电网侧故障，而且包括数据异常、调度异常、通信中断等因素；传播链条延长，局部异常通常经过任务生成变化、算力迁移、负荷变化、电网响应等环节逐级放大，传播路径更为复杂；空间扩散范围增大，算力任务具有跨区域迁移能力，使局部扰动可通过调度机制扩散至其他区域电网。因此，级联故障风险是数据安全风险、算力调度风险、负荷操纵风险在跨域耦合结构下持续演化的系统性后果。

电算跨境交互跨域级联故障风险主要有4类表现形式（见表4），可以归纳为3种典型传播模式：算力侧向电力侧传播（如调度故障传播），当算力调度系统出现异常任务分配时，大量任务可能集中迁移至特定数据中心，导致局部算力负荷和电力负荷同时上升；电力侧向算力侧传播（如电网故障迁移），当某一区域电网发生故障时，算力调度系统可能将计算任务迁移至其他区域，使其他区域电网负荷增加；多系统耦合失稳，如网络、算力平台、电力系统同时出现异常，引发跨域级联失效。在AI智能体驱动场景中，任务迁移、动态重调度虽然提高了资源利用率，但在客观上增强了故障扩散能力，也使级联故障的形成机制更加复杂。

### （五）安全风险演化机制

整体来看，电算跨境交互过程中的主要安全风险表现为数据可信性下降、调度决策失真、负荷重构异常、跨域级联传播依次递进的链式演化过程（见表5）。具体而言，数据层面的泄露、篡改或投毒会首先削弱智能体输入、资源状态信息的可信性，进而影响任务规划和算力调用请求；异常任务请求、失真的资源状态信息进入调度环节后，会进一步改变任务分配位置、执行规模、迁移路径，造成区域算力配置偏移；调度层面的偏移最终会通过数据中心服务器利用率、IT负载功率、冷却功率等变量映射为电力负荷变化，表现为负荷突增、快速爬坡或区域负荷转移；当局部负荷扰动接近电网运行校核边界时，相应影响还可通过备用容量占用、

表4　电算跨境交互跨域级联安全风险

| 风险类别 | 具体表现 | AI智能体驱动场景特点 | 风险后果 |
|---|---|---|---|
| 调度故障传播 | 异常调度导致任务集中迁移至特定数据中心 | 智能体自动生成任务并持续调用算力资源，异常调度会持续放大 | 功率需求集中上升，冲击区域电网 |
| 电网故障迁移 | 某区域电网故障导致算力任务被重新调度至其他地区数据中心 | 算力任务可跨区域迁移执行 | 其他区域电网负荷快速上升 |
| 通信网络中断 | 通信中断导致调度信息失效或延迟 | 跨平台算力调度高度依赖通信网络 | 资源调度紊乱，数据中心负荷异常波动 |
| 系统耦合失稳 | 算力、电力与通信系统同时异常 | 电算跨境协同系统高度耦合 | 多区域电网运行状态同时受到影响 |

表5　电算跨境交互风险传导机制

| 传导环节 | 主要触发因素 | 关键中间变量 | 传导结果 |
|---|---|---|---|
| 数据可信性下降→调度决策失真 | 数据泄露、输入篡改、提示词注入、任务数据投毒、权限滥用 | 输入数据可信度、上下文提示词、任务参数、资源状态信息 | 任务规划偏离，形成异常调用或失真调度输入 |
| 调度决策失真→负荷重构异常 | 调度策略篡改、虚假节点伪造、算力诱骗、调度算法干扰 | 算力请求数量、任务计算强度、节点可用性、价格信号、迁移路径 | 任务时空分配偏移，造成区域算力配置异常 |
| 负荷重构异常→电网运行冲击 | 任务集中迁移、同步启动、频繁重调度、多节点并发调用 | 服务器利用率、IT负载功率、冷却功率、负荷爬坡率 | 数据中心负荷突增、快速爬坡或区域转移 |
| 电网运行冲击→跨域级联传播 | 局部调节能力不足、跨区域任务重调度、通信延迟、多平台协同失效 | 节点负荷率、线路潮流、备用容量、安全裕度、跨区负荷再分配比例 | 局部扰动跨区域、跨系统扩散，形成级联风险 |

安全裕度下降、跨区域任务重调度等过程进一步扩散，形成由算力侧异常向电力侧冲击、再向跨域系统传播的风险演化路径。

## 四、电算跨境交互安全防护技术

针对数据安全、算力调度安全、电力负荷操纵、跨域级联故障等风险，现有研究已形成数据保护、调度治理、负荷控制、系统监测等防护技术，按需作用于数据、算力、负荷、系统运行等环节，在一定程度上缓解了单点安全问题。各类防护技术也存在一定的协同关系：数据保护技术为算力调度提供可信输入基础，调度治理技术可约束异常任务在算力节点间的迁移过程，负荷控制技术可缓冲算力变化对电网运行的影响，系统监测技术为跨环节异常识别和事后追溯提供支撑。然而，电算跨境交互环境中的安全风险具有链式传导、跨域扩散特征，数据、算力、负荷、系统运行之间的耦合关系更加复杂，现有技术在跨平台、多主体、跨区域条件下的适用边界和协同方式仍待分析与拓展（见图3）。

### （一）面向数据安全风险的防护技术

1. 数据传输与访问控制

针对数据传输过程中的泄露与越权访问风险，现有防护手段主要有端到端加密、密钥分级管理、基于属性或角色的访问控制，也在逐步发展零信任架构[35-36]。该类机制可用于保障算力调用过程中任务请求、模型输入、身份凭证的传输安全，防止关键数据在跨平台传输过程中被窃取或篡改。在电算跨境交互场景中，相关应用需进一步关注：加密和访问控制主要作用于传输与存储阶段，对数据使用过程中的保护能力有限，任务在远端节点的执行过程中数据仍以明文形式存在；智能体任务链具有动态扩展特征，调用对象与访问路径不断变化，需研究面向动态调用过程的权限管理与访问控制机制；不同国家、各类平台在身份认证体系与合规要求方面存在差异，需要探索构建跨境环境下的统一信任机制。

2. 数据隐私保护计算

针对跨平台协同计算中的数据隐私问题，现有方法包括联邦学习[37-38]、同态加密[39]、安全多方计算[40-41]等，基本思路是在不暴露原始数据的前提下开展模型训练或数据分析。在电算交互场景中，该类方法可用于跨区域共享负荷预测数据、算力需求特征、资源状态信息，以减少敏感数据的跨境传输需求。在跨境交互应用中，还需关注数据可信性、系统安全性的协同。例如，当输入数据本身存在篡改或投毒时，即使在隐私保护机制下

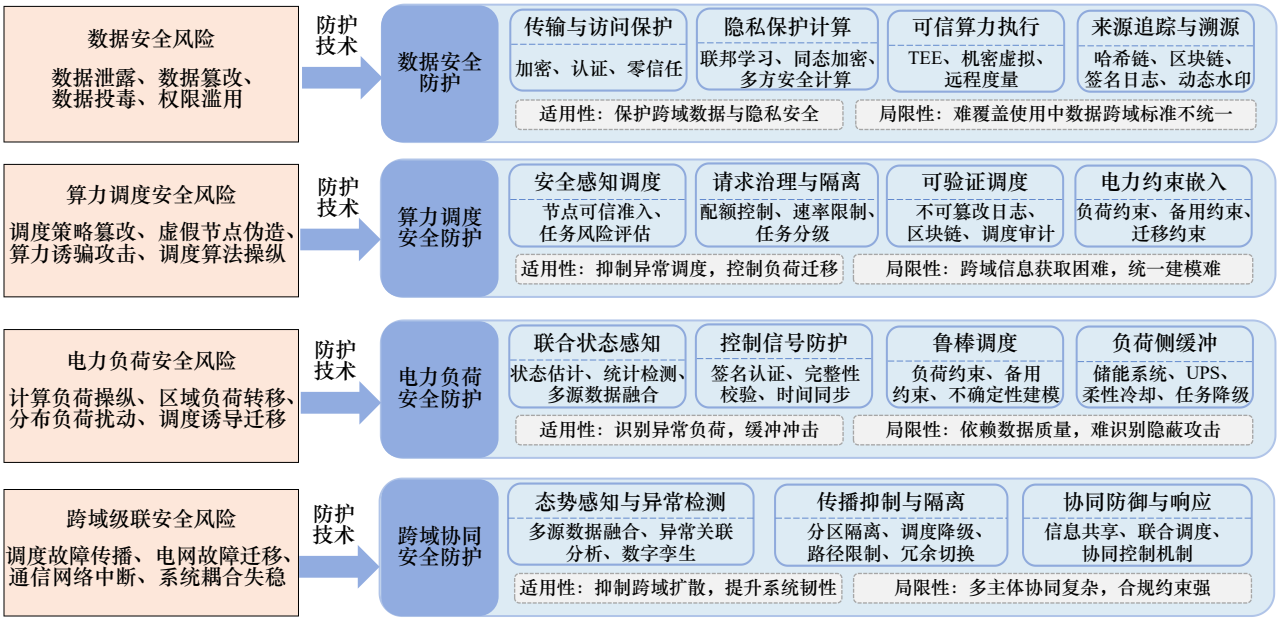


图3　电算跨境交互安全防护技术类别、适用性及局限性

注：TEE表示可信执行环境；UPS表示不间断电源。

完成计算，也可能导致调度决策偏差并进一步影响算力任务分布与电力负荷变化。该类方法适合作为数据保护的基础手段，还需与数据校验、来源追踪等机制结合应用以构建更完整的数据安全保障体系。

3. 数据可信执行与运行保护

针对远端算力节点执行过程中的数据安全问题，机密计算[42-43]、TEE[44-45]成为重要的技术路径。将模型推理、调度逻辑、敏感数据处理过程封装在硬件隔离环境中，结合应用远程度量证明机制，可在一定程度上保障执行环境的可信性。在电算跨境交互场景中，相关应用需进一步考虑跨平台与多节点环境的适配：现有技术主要面向单节点执行环境，而跨平台、多节点任务链的覆盖能力仍待拓展；不同云平台之间的可信执行标准并未统一，跨境调度环境下的信任互认机制有待完善；此类技术可以维护执行环境的可信性，但仍需结合其他机制来共同保证任务来源、调度决策本身的安全性。

4. 数据与算力任务来源追溯

在跨境交互环境中，任务来源与调用路径的透明性直接影响调度系统对任务可信性的判断。记录任务生成、调用路径、执行节点等信息，可支持算力任务全流程的追踪与审计[46-48]。在电算交互场景中，该类方法有助于区分正常算力需求与异常任务请求，为负荷异常分析与调度决策提供依据。实际应用时还需关注实时性与协同问题：现有溯源方法多侧重事后审计，需提升对实时异常行为的应用效果；不同国家、各类平台缺乏统一的数据格式与溯源标准，信息整合存在一定难度；大规模推理场景下的日志记录与存储开销较大，需要权衡精细化追踪与系统性能。

面向数据安全风险的各类防护技术主要特征、适用性、局限性等如表6所示。数据安全防护主要为算力调度提供可信输入基础，也需与调度治理、负荷控制、系统监测技术配合应用，以覆盖后续任务迁移和风险传播环节。

### （二）面向算力调度安全风险的防护技术

1. 算力节点可信接入

在调度决策中引入可信性与风险约束[49-50]，使任务分配不仅基于性能与成本，而且综合考虑任务来源可靠性与节点执行可信状态[51]，能够避免异常任务或不可信节点参与调度。在电算交互环境下，该类方法可进一步扩展为多约束协同建模，形成任务来源可信、执行节点可信、负荷变化可控的调度策略。基于任务来源与行为特征的可信性约束，用于识别异常请求；基于算力节点执行可信性约束，通过节点可信度与远程度量机制筛选执行节点；将区域电网负荷状态纳入调度过程的负荷影响约束，使任务分配兼顾算力需求与电力系统运行安全。在跨境交互应用中，还需关注任务动态性与异构性带来的影响。智能体任务具有链式扩展与持续生成特征，任务结构难以完全先验刻画；不同区域的节点状态评估、电力约束表达、合规要求等存在差异，需要探索统一可信评估和调度约束体系。

2. 算力调度执行治理

针对算力需求在短时间内集中释放引发的负

表6　面向数据安全风险的防护技术

| 技术类别 | 主要方法 | 作用机理 | 电算交互适用性 | 主要局限 |
|---|---|---|---|---|
| 数据传输与访问控制 | 端到端加密、密钥管理、零信任 | 保护跨域传输数据并限制访问权限 | 适用于任务请求、模型输入和接口凭证保护，降低凭证泄露与异常调用风险 | 难以保护使用中数据；多平台权限易扩散，难以覆盖完整任务链 |
| 隐私保护计算 | 联邦学习、同态加密、多方安全计算 | 在不暴露原始数据前提下实现跨域协同计算 | 适用于负荷预测、算力需求等敏感信息的跨域共享，减少原始数据跨境传输 | 计算与通信开销较大；难以保证输入和任务可信，无法单独防范投毒与调度操纵 |
| 可信算力执行 | 可信执行环境、机密虚拟机、远程度量证明 | 隔离关键计算过程并验证执行环境 | 适用于关键推理任务和调度逻辑的可信执行，降低计算篡改对预测与调度的影响 | 难以覆盖跨节点任务链；平台标准不统一，无法约束任务来源和调度逻辑 |
| 来源追踪与溯源 | 区块链、签名日志、任务链追踪 | 记录任务生成、调用路径及执行节点，实现全过程可追溯 | 适用于异常任务识别、事后审计与责任追溯 | 实时性不足，标准不统一，大规模应用开销较高 |

荷冲击问题，现有方法主要是通过配额控制、速率限制[52]、任务分级[53]等机制对算力请求进行约束。在电算交互场景中，可进一步限制算力请求的瞬时增长速度，避免数据中心功率需求在短时间内出现剧烈波动，如根据用户、智能体、任务类型、区域维度设置多级调用阈值，在检测到请求规模异常增长时采取限流、延迟、任务降级等方式平滑算力需求变化，以在信息侧对负荷波动形成缓冲。在跨境交互环境下，还需考虑对持续性、隐蔽性异常行为的识别能力，调度约束对正常算力需求的影响。在阈值与策略设计时，需要权衡安全性与资源利用效率，兼顾系统稳定运行与跨区域资源优化配置。

3. 算力调度行为验证

为了提升跨区域环境下调度行为的可观测性，现有方法通过不可篡改日志、区块链、调度审计机制[54-55]等记录任务分配与迁移过程。在电算交互场景中，该类方法具备事后可验证能力，有助于刻画调度行为与负荷变化的关联性，如某一区域数据中心负荷异常上升时，通过调度记录回溯任务来源与迁移路径，辅助判断负荷变化是否由正常调度引起。在实际应用中，还需提升该类方法对实时调度过程的支撑能力并兼顾系统性能开销。在高频推理场景下，区块链或全量日志机制将带来一定的存储与计算压力，更适合作为调度安全的审计与辅助决策手段，与在线调度控制机制联合使用。

4. 电力约束嵌入调度

将电力运行约束嵌入算力调度模型是跨境算力交互场景中的关键扩展，不是由算力平台直接获取完整电网拓扑、潮流分布、安全校核数据，而是在不暴露电网敏感运行信息的前提下，将电网运行边界转化为算力调度可识别的约束条件，从源头抑制算力调度行为向电力系统的风险传导。具体实现时，在调度模型中引入区域负荷变化率、节点功率上限、任务迁移频率、备用容量边界、可再生能源匹配度[56-59]等约束，在电网处于高负荷或脆弱状态时，基于电网侧提供的区域可用容量、负荷调整上限、需求响应价格信号、风险等级等信息来动态调整相关区域的任务接纳能力。电网运行数据具有较高的敏感性，不同国家和运营主体通常难以共享完整潮流、备用、安全校核等信息；可行的方式是通过脱敏化、聚合化、分级授权接口传递约束边界，或者由算力平台提交候选负荷计划后，再由电网侧返回可行性判断与调整建议。此外，电力约束与算力调度中的成本、时延、模型性能目标可能存在耦合关系，需要权衡安全性与经济性。

面向算力调度安全风险的各类防护技术主要特征、适用性、局限性等如表7所示。算力调度安全防护承接数据可信结果，是阻断异常任务向负荷扰动转化的关键环节，需要与负荷侧控制、系统监测机制相衔接。

### （三）面向电力负荷安全风险的防护技术

1. 负荷状态联合感知

对于负荷操纵风险，现有电力系统具有较成熟的异常检测方法，包括统计检测[60-61]、状态估计残差分析[62-63]、基于机器学习的异常识别方法[64]，可监测负荷幅值、变化速率、空间分布等。然而，在电算跨境交互场景中，仅依赖电力侧信息难以区分正常算力迁移与异常任务驱动的负荷变化，有必要构建“算力–数据–电力”多源联合感知机制，对词元请求强度、任务迁移路径、计算资源利用率、数据中心功率曲线、电网运行状态进行

表7　面向算力调度安全风险的防护技术

| 技术类别 | 主要方法 | 作用机理 | 电算交互适用性 | 主要局限 |
|---|---|---|---|---|
| 安全感知调度 | 节点信誉评估、任务可信评分、风险感知调度 | 识别异常任务和不可信节点，调整调度决策 | 抑制异常算力任务参与调度，降低负荷异常迁移风险 | 动态任务和节点状态难以实时评估 |
| 请求治理与调度隔离 | 配额控制、速率限制、任务分级 | 限制算力请求增长速度与并发规模 | 平滑算力需求变化，抑制负荷突增 | 隐蔽持续攻击难以识别，阈值设置影响调度效率 |
| 可验证调度 | 不可篡改日志、区块链、调度审计 | 记录任务分配与迁移过程，实现可追溯性 | 关联调度行为与负荷变化，辅助异常分析 | 实时约束能力有限，存在性能与成本开销 |
| 电力约束嵌入调度 | 功率上限、负荷变化率、迁移频率及区域容量约束 | 将电网运行边界转化为调度约束条件 | 限制算力迁移引发的负荷冲击，实现电算协同 | 完整电网信息难以共享，需采用脱敏、聚合或接口化约束 |

关联分析，识别由异常任务或调度行为引发的负荷异常模式。在实际应用中，还需关注跨层数据的统一采集与时序对齐、异常样本不足对模型泛化能力的影响，检测模型自身也因遭受对抗样本和数据投毒攻击而需提高对抗环境下的鲁棒性。

2. 调度与控制信号认证保护

负荷操纵多通过伪造调度指令或控制信号而非直接改变负荷本身来实现，现有方法主要对调度命令与控制信号进行签名认证[65]、完整性校验[66]、时间同步保护[67]，确保关键指令在传输和执行过程中的真实性与一致性。在电算交互场景中，该类机制可扩展至算力调度命令、节点状态信息、能耗控制指令的保护层次，避免因调度信息失真而引发算力任务异常迁移及负荷重构。在跨境交互环境中，还需考虑业务层滥用与内部威胁的识别能力。即使在身份合法的前提下，异常任务生成或调度策略偏移仍可能引发负荷异常变化，需要结合使用命令认证机制与行为监测及调度约束手段。

3. 负荷安全鲁棒约束

为了降低负荷突变对电网运行的影响，现有研究在调度过程中引入鲁棒约束与安全边界来将负荷变化控制在可承受范围内，如设置负荷变化率约束、备用容量约束、不确定性边界，提高系统对扰动的适应能力[68-69]。在电算跨境交互场景中，鲁棒调度可将负荷操纵风险前置到调度层，结合算力调度特征对跨境迁入任务设置速率上限，对高风险来源任务实施差异化约束，再对关键电网区域设定算力接入阈值，结合可再生能源出力与备用容量来动态调整任务接纳策略。在实际应用中，该类方法依赖电网运行状态的实时获取与准确建模，需完善跨境环境下的信息获取与协同机制。

4. 负荷冲击缓冲与韧性提升

在检测与调度约束以外，数据中心侧可通过储能系统[70]、UPS[71]、柔性冷却、任务分级卸载[30]等手段来缓冲并吸收短时负荷冲击。在电算跨境交互场景中，这类技术可作为物理层的缓冲机制，如异常算力请求集中出现时通过储能与冷却调节削弱功率峰值、采取任务分级策略来优先保障关键业务，从而降低对电网的冲击。不同缓冲措施在真实运维过程中的定位和时间尺度并不相同：UPS用于电源切换和秒级短时支撑，保障关键IT负载连续供电；储能系统用于分钟级至小时级削峰、备用、应急支撑，面临容量配置、循环寿命、投资成本的约束；柔性冷却依托蓄冷、冷冻水调节、温度设定值调整实现分钟级负荷调节，受到机房温 / 湿度、设备可靠性边界的约束；任务分级卸载或降级主要用于非关键、可中断、时延容忍型业务。在应用过程中，根据扰动持续时间、业务优先级、成本约束组合使用各类措施。该类方法适用于缓解短时冲击，可与调度侧约束和检测机制联合使用来提升系统整体抗扰动能力。

面向电力负荷安全风险的各类防护技术主要特征、适用性、局限性等如表8所示。电力负荷安全防护主要缓冲算力任务变化对电网运行的冲击，应用效果依赖前端数据可信、调度治理、后端系统监测的协同支撑。

### （四）面向跨域级联安全风险的防护技术

1. 跨域安全态势感知与异常检测

对于跨域级联故障，现有方法由单一的电网侧监测逐步扩展至多域融合感知，结合运行数据、信息侧行为实现异常关联分析[72-73]。多域态势感知、

表8　面向电力负荷安全风险的防护技术

| 技术类别 | 主要方法 | 作用机理 | 电算交互适用性 | 主要局限 |
|---|---|---|---|---|
| 联合状态感知 | 状态估计、统计检测、机器学习、多源数据融合 | 关联分析算力请求与电网负荷变化，识别异常负荷行为 | 区分正常算力迁移与异常负荷扰动 | 多源数据难以对齐，模型泛化能力有限 |
| 控制信号防护 | 签名认证、完整性校验、时间同步 | 防止调度指令与控制信号被伪造或篡改 | 保障算力调度与能耗控制指令的真实性 | 难以识别合法身份下的异常调用 |
| 鲁棒调度 | 负荷约束、备用约束、不确定性建模 | 在调度阶段限制负荷变化幅度与速率 | 抑制算力迁移引发的负荷冲击 | 依赖电网状态信息，跨境实现困难 |
| 负荷侧缓冲 | UPS、储能、柔性冷却、任务分级卸载 | 按时间尺度平滑负荷变化，缓冲短时功率冲击 | 缓解负荷尖峰、快速爬坡和短时波动 | 各措施时间尺度、成本和适用业务不同，需组合使用 |

跨层异常检测可有效支撑信息物理系统的整体安全分析[74]，从单点检测发展为融合物理模型、图模型、数据驱动方法的综合框架[75-76]，结合仿真手段评估风险传播过程[77]。在电算跨境交互场景中，需要构建覆盖算力请求、调度行为、数据中心运行、电网状态的跨层感知体系，关联分析任务强度、迁移路径、IT负载、电网运行等指标，识别潜在的风险传播链并评估对电网运行的影响；结合仿真平台，分析任务异常、负荷波动、电网越限的演化过程。在实际应用中，还需关注数据采集与对齐，不同国家、各类平台的数据语义与告警标准的统一性。

2. 跨域故障传播抑制与隔离

在跨域耦合系统中，仅依靠异常检测难以有效阻断风险扩散，还需采用抑制与隔离机制来限制故障传播范围，相关方法包括网络分段、系统分区隔离、关键链路冗余、服务降级、故障后的自动重构及恢复等[78-80]。在电算交互场景中，根据电网区域及风险等级对数据中心集群进行分组管理，限制任务在高风险区域之间的自由迁移；在检测到异常后，通过调度降载、业务分级、区域隔离等方式控制风险扩散，结合备用的节点与通信路径保障系统运行；当局部电网处于脆弱状态时，优先保障关键业务并限制新增算力迁入。在实际应用中，该类方法需要权衡资源利用率、全球优化效率，依赖跨主体的状态信息来实施分区与重构策略。

3. 多主体协同防御与响应

跨域级联故障通常涉及算力平台、数据中心、电网、通信网络等主体，单一主体难以独立实施风险应对。建立信息共享和联合响应机制提升系统整体防御能力，运用告警联动、威胁情报共享、多主体联合响应机制减少级联传播风险[81-82]。在电算跨境交互场景中，立足共享风险等级、异常任务来源、节点状态、区域接纳能力等关键指标，建立最小必要的信息共享机制来实现协同防御；当某一环节出现异常时，各类主体可据此调整任务迁移策略与电力调度方式，进而抑制风险扩散。然而，跨国环境下治理主体多元、利益诉求差异化，合规边界与监管要求也不完全一致，难以依靠单一平台执行统一响应机制。为此，实施协同防御应在接口标准化、最小必要共享原则的基础上，预先建立跨主体应急协同规则，明确异常处置、监管报告、责任划分等关键事项；保留关键调用链路与处置过程日志，为事故复盘、责任认定、损失分担提供可追溯依据。

面向跨域级联安全风险的各类防护技术主要特征、适用性、局限性等如表9所示。跨域级联安全防护主要提供全局监测、异常识别、反馈支撑等功能，与数据保护、调度治理、负荷控制共同提升系统的安全韧性。

## 五、电算跨境交互安全研究展望

前述分析表明，电算跨境交互的安全薄弱点分布在算力需求生成、任务调度、负荷响应、跨域运行等环节，保障安全不能仅依赖单一环节的局部防护。本研究围绕算力需求源头治理、调度安全控制、跨域协同防御、内生安全架构4个层面构建了电算跨境交互安全体系（见图4），此基础上展望未来研究思路与发展方向。

### （一）面向算力需求生成的源头安全治理

算力需求生成方式不同于传统上由用户触发的直接请求，智能体可基于任务目标自动生成并持续扩展任务链，通过多轮推理与跨平台调用不断放大算力需求。算力需求不再是静态的资源请求，而是演变为具有自主迭代特性的动态过程，对应的异常状态通常在进入调度阶段之前即已形

表9　面向跨域级联安全风险的防护技术

| 技术类别 | 主要方法 | 作用机理 | 电算交互适用性 | 主要局限 |
|---|---|---|---|---|
| 态势感知与异常检测 | 多源数据融合、异常关联分析、数字孪生 | 识别任务、调度与电网之间的异常传播关系 | 提前识别跨域级联风险链条 | 数据分散且标准不统一，跨域共享困难 |
| 传播抑制与隔离 | 分区隔离、调度降级、路径限制、冗余切换 | 限制异常传播范围，防止负荷跨区域扩散 | 抑制算力迁移引发的级联负荷冲击 | 可能降低资源利用率，依赖多主体协同 |
| 协同防御与响应 | 信息共享、联合调度、协同控制机制 | 提升多主体协同应对能力，减少风险扩散 | 跨平台与电网协同响应异常事件 | 跨域协同机制复杂，合规与协调成本高 |

成，也可能在跨境交互中进一步放大。有必要将算力需求从被动调度对象转变为主动治理对象，在需求生成阶段提出面向智能体行为的源头安全控制思路。

未来研究可重点关注3个方面。① 针对智能体任务链的自演化特征，应关注任务目标、执行路径、调用行为之间的一致性关系，识别由提示词注入、上下文污染、策略偏移引发的异常任务扩展，避免算力需求在任务生成阶段持续累积。② 在跨平台调用环境下，单一任务请求多通过模型接口与工具链在多个算力节点之间传播，具有隐蔽的放大效应，应从调用链视角刻画算力需求的生成与扩展路径，识别异常调用结构与跨域放大模式。③ 鉴于算力需求最终通过数据中心负荷来体现，相应生成特征与电力影响之间存在前置关联，应在需求形成阶段建立算力请求到负荷影响间的关联认知，使高风险需求在进入调度之前即具备可识别性。面向算力需求源头安全治理的研究内容、预期效果等如表10所示。

### （二）面向电力影响约束的算力调度安全控制

算力调度由传统的资源分配机制演变为连接

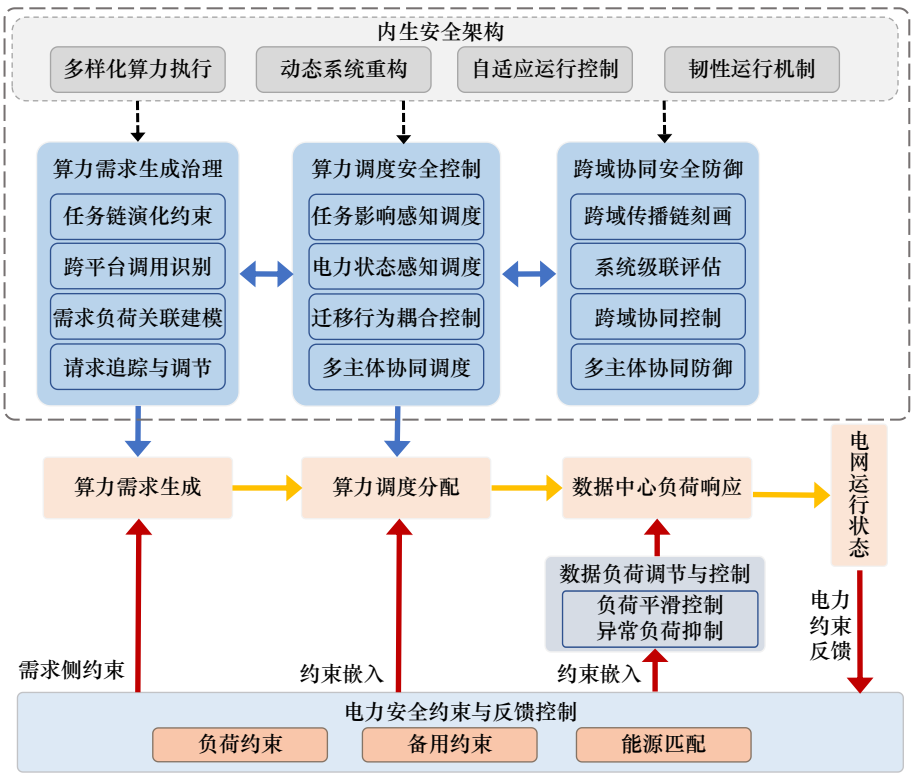


图4　电算跨境交互协同安全体系架构

表10　算力需求源头治理研究方向

| 研究方向 | 面向的安全风险 | 研究内容 | 主要方法 | 预期效果 |
|---|---|---|---|---|
| 任务链演化约束 | 任务自扩展、需求失控 | 分析任务目标与执行路径演化一致性 | 行为建模、路径一致性分析 | 抑制异常任务链扩展 |
| 跨平台调用识别 | 请求放大、跨域扩散 | 刻画算力请求在多平台间的传播结构 | 调用链分析、结构特征识别 | 识别异常放大路径 |
| 需求负荷关联建模 | 算力洪峰、负荷冲击 | 建立算力请求与数据中心负荷映射关系 | 关联建模、影响评估 | 提前识别高影响需求 |
| 请求来源与路径刻画 | 来源不清、行为隐蔽 | 描述算力请求生成与传播路径特征 | 溯源建模、关联分析 | 提升需求可解释性 |

信息系统与电力系统的关键控制环节。智能体生成的算力需求具有动态扩展、跨区域调用特征，使调度过程不再只是对既有请求的响应，而且成为影响算力分布与电力负荷空间转移的直接驱动因素。算力调度需要从性能优化转向电力约束与安全控制的协同，以充分抑制风险放大。

未来研究可重点关注4个方面。① 在智能体自动生成任务的背景下，算力调度应区分不同类型需求的潜在影响，关注任务在分配过程中可能形成的集中效应，避免异常需求在调度阶段被进一步放大。② 在跨境交互环境中，算力调度直接决定数据中心负荷的空间分布，应将区域电网运行状态与负荷承载能力纳入调度认知，使调度过程具备对电力系统运行边界的感知能力。③ 算力任务在多节点之间的频繁迁移可能引发负荷的快速波动，应关注任务迁移行为与负荷变化之间的耦合关系，避免调度策略在时间尺度上放大系统扰动。④ 在多平台协同环境下，不同算力平台与电力系统之间信息割裂，可能导致调度决策与电网状态脱节，有必要探索面向多主体协同的调度支撑机制，以在更完整的系统状态下进行调度。面向算力调度安全控制的主要研究内容、预期效果等如表11所示。

### （三）面向跨域风险传播的协同安全防御

在电算跨境交互环境中，跨域交互路径更加复杂，算力需求生成、任务调度执行、电力负荷响应分别位于不同的平台与区域并通过数据流、算力流、能量流建立关联。单一环节异常的影响不再限于局部系统，而是沿着算力需求生成、算力调度、负荷响应等环节在不同区域之间传导，形成跨域传播与级联放大效应。有必要从系统整体视角出发，关注风险在多域耦合结构中的传播机制与抑制路径。

未来研究可重点关注3个方面。① 在跨域传播机理层面，算力任务通过多平台调用与跨区域迁移形成复杂的传播链条，应刻画任务生成、调度分配、负荷响应之间的关联关系，识别风险在不同环节之间的时空传递路径与关键节点。② 在系统评估层面，持续生成且自动扩展任务的局部异常可能在多轮调用与跨域调度过程中不断累积并放大，应关注风险在时间和空间上的耦合放大机制，从系统层面出发评估级联演化风险。③ 在防御控制层面，应结合系统运行状态变化研究跨域协同响应机制，通过任务迁移约束、区域隔离、策略联动等方式抑制风险扩散；在多主体协同环境下，探索基于最小必要信息共享的协同防御机制，使不同主体可在有限信息共享条件下实现联动调节。

在实际工程应用中，相关研究可按照单数据中心监测，区域集群协同，跨平台、跨境联动的路径逐步推进，即先建立算力请求与功率响应之间的监测关系，后验证区域数据中心集群的限流、迁移约束、负荷协同能力，再探索跨平台、跨境条件下的联合响应与责任追溯机制。面向跨域协同安全防御的主要研究内容、预期效果等如表12所示。

### （四）面向电算交互安全的内生安全架构设计

现有的多数安全技术属于外部叠加防御机制，即通过额外的检测、认证、防护模块来缓解系统风险。近年来，内生安全理念已在信息物理系统中得到应用，强调将安全能力嵌入系统架构之中，使系统在设计阶段即具备自适应、自防护、自恢复能力[83]。内生安全不依赖单一安全设备，而是通过系

表11　算力调度安全控制研究方向

| 研究方向 | 面向的安全风险 | 研究内容 | 主要方法 | 预期效果 |
|---|---|---|---|---|
| 任务影响感知调度 | 异常任务扩散、需求放大 | 识别不同任务在调度过程中的潜在影响差异 | 风险表征、行为特征分析 | 抑制高风险任务扩散 |
| 电力状态感知调度 | 跨区域负荷转移 | 将电网运行状态纳入调度认知 | 状态感知、约束建模 | 避免负荷集中迁移 |
| 迁移行为耦合控制 | 负荷快速波动 | 分析任务迁移与负荷变化的耦合关系 | 行为分析、动态约束 | 平滑负荷变化过程 |
| 多主体协同调度 | 信息割裂、调度失衡 | 构建跨平台与电网之间的信息协同机制 | 信息融合、协同决策 | 提升整体调度一致性 |

统结构冗余、多样化执行、动态重构等机制，使系统在受到攻击或故障发生时保持稳定运行。对于电算跨境交互，需要从系统架构层面构建具备内生安全能力的电算协同体系，在系统架构中嵌入自适应防护、动态重构能力，使系统在算力任务来源分散、调度路径动态变化、系统边界不断扩展的环境下稳定运行。

未来研究可重点关注4个方面。① 在算力执行层面，开展多节点协同执行及结果一致性分析，提高关键任务在异常条件下的执行稳定性。② 在调度与系统结构层面，结合算力资源分布特征，研究基于系统状态变化的动态重构方法，使算力任务在节点异常或电网状态变化时能够进行适应性调整。③ 在系统运行层面，结合任务请求特征、算力负荷变化、网络运行状态，探索面向运行过程的安全感知与自适应调节方法，降低异常行为对系统的影响。④ 在电力侧关联方面，应用多区域算力部署、数据中心能量管理等手段，研究具备负荷缓冲能力的韧性运行方式，提升系统在异常扰动下的持续运行能力。

相关内生安全能力建设可采取分阶段示范路径：先在单数据中心层面验证算力请求、功率响应的监测和异常识别能力，后扩展至区域数据中心集群开展限流、降级、负荷协同试点，再面向跨平台、跨区域、跨境调用场景验证动态重构与协同防御机制。面向内生安全架构设计的主要研究内容、预期效果等如表13所示。

## 六、结语

本文围绕电算跨境交互安全议题，系统论述了发展形态、运行特征、安全风险、防护技术、未来研究方向等。当前，算力任务生成方式由人工触发转向AI智能体自主生成，算力资源配置由本地或区域协同转向跨平台、跨区域、跨境调用，数据中心负荷也由相对稳定的业务负荷转变为受信息系统实时驱动的动态负荷。在此背景下，电算跨境交互安全风险不再局限于单一系统或单一环节，而是表现为数据可信性下降、调度决策失真、负荷重构异常、跨域级联传播依次递进的链式演化过程。现有的数据保护、调度治理、负荷控制、系统监测等技术为风险防护提供了基础能力，但在跨平台、多主体、跨区域条件下的协同能力仍需提升。进一步展望了从系统层面构建综合防护机制的研究方向，即贯通算力需求生成、算力调度治理、电力约束协同、跨域联合响应、内生安全架构等关键环节，提升电算跨境交互系统的整体安全防护能力。

面向未来，电算跨境交互将成为数字基础设施、能源基础设施深度耦合的重要形态，维持安全运行需要由单纯的技术防护拓展至工程应用与机制协同。应加强算力任务、数据中心功率变化、电网运行状态的关联建模，提升跨域风险识别和预警能力。也应在保护敏感运行信息的前提下，探索面向电力约束的算力调度和有限信息共享机制。还可结合电力市场机制、容量配置、基础设施规划，统筹

表12　跨域协同安全防御研究方向

| 研究方向 | 面向的安全风险 | 研究内容 | 主要方法 | 预期效果 |
|---|---|---|---|---|
| 跨域传播链刻画 | 风险跨环节传导 | 描述需求、调度与负荷之间的传播关系 | 关联分析、路径刻画 | 构建关键传播链条 |
| 级联放大机制分析 | 风险持续累积、跨域扩散 | 分析任务扩展与跨域调度引发的放大效应 | 演化分析、数据驱动建模 | 识别级联演化过程 |
| 跨域协同响应机制 | 联动失效、风险扩散 | 构建多主体联动的响应思路 | 协同决策、信息共享 | 抑制风险跨域传播 |

表13　内生安全架构设计研究方向

| 研究方向 | 面向的安全问题 | 研究内容 | 主要方法 | 预期效果 |
|---|---|---|---|---|
| 多样化算力执行 | 单点失效风险 | 多节点协同执行与结果一致性机制 | 冗余执行、一致性校验 | 提高任务执行可靠性 |
| 动态系统重构 | 节点异常与结构失衡 | 基于系统状态的算力调度与资源重构 | 动态迁移、资源重配置 | 降低局部故障影响 |
| 自适应运行控制 | 运行状态动态变化 | 面向负荷与系统状态的自适应调节机制 | 状态反馈、策略调整 | 提升系统自适应能力 |
| 韧性运行机制 | 负荷冲击与供能波动 | 多区域冗余与负荷缓冲机制 | 储能支撑、任务分级调度 | 提高系统抗扰动能力 |

考虑跨境算力迁移带来的负荷转移和资源配置问题，为构建安全可信的电算跨境交互体系提供坚实支撑。

**利益冲突声明**

本文作者在此声明不存在任何利益冲突或财务冲突。

**Received date:** April 9, 2026; **Revised date:** June 22, 2026

**Corresponding author:** Tang Yi is a professor from the School of Electrical Engineering, Southeast University. His major research field is cybersecurity in power systems. E-mail: tangyi@seu.edu.cn

**Funding project:** The National Natural Science Foundation of China Project (52477077)

**参考文献**

[1] Aubakirova M，Atallah A，Clark C. State of AI：An empirical 100 trillion token study with OpenRouter[EB/OL]．（2025-12-05）[2026-06-20]. https://openrouter.ai/state-of-ai.

[2] 仝杰，丁浩，陈洪银，等. 电力–算力协同：内涵、架构、技术与实践[J/OL]. 中国电机工程学报，2026-06-20. https://doi.org/10.13334/j.0258-8013.pcsee.252209.
Tong J，Ding H，Chen H Y，et al. Electricity–computing synergy：Connotation，architecture，technologies and practice[J/OL]. Proceedings of the CSEE，2026-06-20. https://doi.org/10.13334/j.0258-8013.pcsee.252209.

[3] 冯健冰，任洲洋，李文沅，等. AI4S范式下新型电力系统中长期电力供需协同：内涵与架构[J/OL]. 中国电机工程学报，2026-06-20. https://doi.org/10.13334/j.0258-8013.pcsee.252234.
Feng J B，Ren Z Y，Li W Y，et al. Long-term power supply and demand coordination of new power system under AI4S paradigm：Connotation and architecture[J/OL]. Proceedings of the CSEE，2026-06-20. https://doi.org/10.13334/j.0258-8013.pcsee.252234.

[4] 国家互联网应急中心. 关于OpenClaw安全应用的风险提示[EB/OL]．（2026-03-12）[2026-06-20]. https://www.cert.org.cn/publish/main/11/2026/20260312144519429724511/20260312144519429724511_.html.
National Computer Network Emergency Response Technical Team/Coordination Center of China. Risk alert for OpenClaw security applications[EB/OL]. https://www.cert.org.cn/publish/main/11/2026/20260312144519429724511/20260312144519429724511_.html.

[5] 伍拯，陈洪银，贾晓强，等. 电网友好型数据中心低碳调控方法及其实践[J]. 新型电力系统，2025，3（3）：263-284.
Wu Z，Chen H Y，Jia X Q，et al. Grid friendly data center low carbon regulation method and practice[J]. New Type Power Systems，2025，3（3）：263-284.

[6] 王辉东，高晋坤，黄佳斌，等. 考虑数据中心负载灵活性的电力系统运行可靠性评估方法[J]. 电力系统保护与控制，2023，51（21）：96-105.
Wang H D，Gao J K，Huang J B，et al. Power system operational reliability evaluation method considering data center load flexibility[J]. Power System Protection and Control，2023，51（21）：96-105.

[7] 孙毅，张凯，格根敖其，等. 边缘数据中心集群算力–电力–热力协同的两阶段分布鲁棒优化方法[J/OL]. 电工技术学报，2026-06-20. https://doi.org/10.19595/j.cnki.1000-6753.tces.251975.
Sun Y，Zhang K，Gegen A Q，et al. A two-stage decentralized robust optimization method for computing power–electricity–heat coordination in edge data centers[J/OL]. Transactions of China Electrotechnical Society，2026-06-20. https://doi.org/10.19595/j.cnki.1000-6753.tces.251975.

[8] Sun J，Xu M C，Cespedes M，et al. Data center power system stability：Part I：Power supply impedance modeling[J]. CSEE Journal of Power and Energy Systems，2022，8（2）：403-419.

[9] Sun J，Mihret M，Cespedes M，et al. Data center power system stability：Part II：System modeling and analysis[J]. CSEE Journal of Power and Energy Systems，2022，8（2）：420-438.

[10] 陈敏，高赐威，郭庆来，等. 互联网数据中心负荷时空可转移特性建模与协同优化：驱动力与研究架构[J]. 中国电机工程学报，2022，42（19）：6945-6957.
Chen M，Gao C W，Guo Q L，et al. Modeling and coordinated optimization for spatiotemporal load regulation potentials of Internet data centers：Motivation and architecture[J]. Proceedings of the CSEE，2022，42（19）：6945-6957.

[11] 邓莉荣，孙懿，符杨. 计及异构特性的云边协同系统算力–电力联合优化调度策略[J/OL]. 中国电机工程学报，2026-06-20. https://link.cnki.net/urlid/11.2107.TM.20260309.1008.002.
Deng L R，Sun Y，Fu Y. Computing–power joint optimal scheduling strategy for cloud–edge collaborative system considering heterogeneous characteristics[J/OL]. Proceedings of the CSEE，2026-06-20. https://link.cnki.net/urlid/11.2107.TM.20260309.1008.002.

[12] Luo P C，Wang X Y，Li Y L. The impact of datacenter load regulation on the stability of integrated power systems[J]. Sustainable Energy Technologies and Assessments，2020，42：100875.

[13] Takci M T，Qadrdan M，Summers J，et al. Data centres as a source of flexibility for power systems[J]. Energy Reports，2025，13：3661-3671.

[14] 董昱，周劼英，张晓，等. 新型电力系统信息物理安全防护体系研究[J]. 中国电机工程学报，2025，45（15）：5738-5751.
Dong Y，Zhou J Y，Zhang X，et al. Research on cyber–physical security protection of new power system[J]. Proceedings of the CSEE，2025，45（15）：5738-5751.

[15] 薛禹胜，谢东亮，薛峰，等. 支持信息–物理–社会系统研究的跨领域交互仿真平台[J]. 电力系统自动化，2022，46（10）：138-148.
Xue Y S，Xie D L，Xue F，et al. A cross-field interactive simulation platform for supporting research on cyber–physical–social systems [J]. Automation of Electric Power Systems，2022，46（10）：138-148.

[16] 房方，吴兴堂，程龙，等. 电力智算系统构建理论与关键技术[J]. 中国科学：技术科学，2026，56（1）：201-226.
Fang F，Wu X T，Cheng L，et al. Theoretical framework and key technologies of electric power intelligent computing systems[J]. Scientia Sinica Technologica，2026，56（1）：201-226.

[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 Z J，Liu Y，Bao Y Y，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.

[18] 郭少勇，刘岩，邵苏杰，等. 新型电力系统数据跨域流通泛安全边界防护技术[J]. 电力系统自动化，2024，48（6）：96-111.
Guo S Y，Liu Y，Shao S J，et al. Ubiquitous security boundary protection technology for cross-domain data circulation in new power system[J]. Automation of Electric Power Systems，2024，48（6）：96-111.

[19] International Energy Agency. Energy and AI：Energy demand from AI[EB/OL].[2026-06-20]. https：//www.iea.org/reports/energy-and-ai/energy-demand-from-ai.

[20] The Brattle Group. Brattle 2025 CONE report for PJM[EB/OL].（2025-04-11）[2026-06-20]. https：//www. pjm. com/-/media/DotCom/committees-groups/committees/mic/2025/20250411-special/item-1-02-revised-cone-report-final.pdf.

[21] International Energy Agency. Electricity 2026：Grids[EB/OL].[2026-06-20]. https：//www.iea.org/reports/electricity-2026/grids.

[22] Eurostat. Electricity price statistics[EB/OL]. [2026-06-20]. https：//ec. europa. eu/eurostat/statistics-explained/index. phptitle=Electricity_price_statistics.

[23] International Energy Agency. Electricity mid-year update 2025：Prices，trends in wholesale markets differ across regions[EB/OL].[2026-06-20]. https：//www. iea. org/reports/electricity-mid-year-update-2025/prices-trends-in-wholesale-markets-differ-across-regions.

[24] DeepSeek. Models & pricing[EB/OL]. [2026-06-20]. https：//api-docs.deepseek.com/quick_start/pricing.

[25] OpenAI. API pricing[EB/OL]. [2026-06-20]. https：//openai. com/zh-Hans-CN/api/pricing/.

[26] 陈晓红，吕建，刘咏梅. 算电协同技术与应用发展研究[J/OL]. 中国工程科学，2026-08-31. https：//link.cnki.net/urlid/11.4421.g3.20260828.1441.002.
Chen X H，Lyu J，Liu Y M. Technology and application of computing–electricity synergy[J/OL]. Strategic Study of CAE，2026-08-31. https：//link.cnki.net/urlid/11.4421.g3.20260828.1441.002.

[27] Zhang N，Duan H B，Guan Y R，et al. The “eastern data and western computing” initiative in China contributes to its net-zero target [J]. Engineering，2025，52：256-261.

[28] 曹雨洁，丁肇豪，王鹏，等. 能源互联网背景下数据中心与电力系统协同优化（二）：机遇与挑战[J]. 中国电机工程学报，2022，42（10）：3512-3527.
Cao Y J，Ding Z H，Wang P，et al. Coordinated operation for data center and power system in the context of energy Internet（II）：Opportunities and challenges[J]. Proceedings of the CSEE，2022，42（10）：3512-3527.

[29] OpenAI. A practical guide to building AI agents[EB/OL].[2026-06-20]. https：//openai.com/business/guides-and-resources/a-practical-guide-to-building-ai-agents/.

[30] 丁肇豪，曹雨洁，张素芳，等. 能源互联网背景下数据中心与电力系统协同优化（一）：数据中心能耗模型[J]. 中国电机工程学报，2022，42（9）：3161-3176.
Ding Z H，Cao Y J，Zhang S F，et al. Coordinated operation for data center and power system in the context of energy Internet（I）：Energy demand management model of data center[J]. Proceedings of the CSEE，2022，42（9）：3161–3176.

[31] Central Statistics Office. Data centres metered electricity consumption 2024[EB/OL]. [2026-06-20]. https：//www.cso.ie/en/releasesandpublications/ep/p-dcmec/datacentresmeteredelectricityconsumption2024.

[32] North American Electric Reliability Corporation. Incident review：Considering simultaneous voltage-sensitive load reductions[R]. Washington，DC：North American Electric Reliability Corporation，2025.

[33] Department for Science，Innovation and Technology，UK Research and Innovation. UK compute roadmap[EB/OL].（2025-07-05）[2026-06-20]. https：//www.gov.uk/government/publications/uk-compute-roadmap/uk-compute-roadmap.

[34] 舒印彪，汤涌，张正陵，等. 欧洲伊比利亚半岛电网“4·28”大停电事故分析及启示[J]. 中国电机工程学报，2025，45（17）：6603-6612.
Shu Y B，Tang Y，Zhang Z L，et al. Analysis and lessons of the April 28，2025 blackout in the Iberian Peninsula power system [J]. Proceedings of the CSEE，2025，45（17）：6603-6612.

[35] Wu S T，Wang Q，Tang Y，et al. Security of distributed data interactions in renewable-dominated cyber–physical energy systems：Exogenous threats，endogenous vulnerabilities and resilience enhancement[J]. Renewable and Sustainable Energy Reviews，2026，240：117232.

[36] 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 T，Ma Y，Jiang H F，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.

[37] 郑楷洪，肖勇，王鑫，等. 一个面向电力计量系统的联邦学习框架[J]. 中国电机工程学报，2020，40（S1）：122-133.
Zheng K H，Xiao Y，Wang X，et al. A federated learning framework for power grid metering system[J]. Proceedings of the CSEE，2020，40（S1）：122-133.

[38] 戴理朋，杨鑫，徐茹枝. 联邦学习在电力数据分析中的应用及隐私保护研究[J]. 电力信息与通信技术，2022，20（11）：47-56.
Dai L P，Yang X，Xu R Z. Research on the application of federated learning in power data analysis and privacy protection[J]. Electric Power Information and Communication Technology，2022，20（11）：47-56.

[39] Acar A，Aksu H，Uluagac A S，et al. A survey on homomorphic encryption schemes：Theory and implementation[J]. ACM Computing Surveys，2019，51（4）：1-35.

[40] 凡航，徐葳，王倩雯，等. 多方安全计算框架下的智能合约方法研究[J]. 信息安全研究，2022，8（10）：956-963.
Fan H，Xu W，Wang Q W，et al. Research on smart contract method in the framework of secure multi-party computation[J]. Journal of Information Security Research，2022，8（10）：956-963.

[41] 王蓓蓓，丁正凯，朱竞，等. 计算任务分摊的个性化云边协同支撑单用户负荷概率预测方法研究[J]. 电网技术，2026，50（6）：2302-2317.
Wang B B，Ding Z K，Zhu J，et al. Research on a personalized cloud–edge collaborative approach for single-user probabilistic load forecasting with computational task allocation[J]. Power System Technology，2026，50（6）：2302-2317.

[42] 凡航，徐葳，范晓昱，等. 隐私计算在新型电力系统中的应用分析与展望[J]. 电力系统自动化，2023，47（19）：187-199.
Fan H，Xu W，Fan X Y，et al. Application analysis and prospect of

privacy-preserving computation in new power system[J]. Automation of Electric Power Systems,2023,47(19):187-199.

[43] 郭庆来,田年丰,孙宏斌. 支撑能源互联网协同优化的隐私计算关键技术[J]. 电力系统自动化,2023,47(8):2-14.
Guo Q L,Tian N F,Sun H B. Key technologies of privacy computation supporting collaborative optimization of energy Internet [J]. Automation of Electric Power Systems,2023,47(8):2-14.

[44] Kalapaaking A P,Khalil I,Rahman M S,et al. Blockchain-based federated learning with secure aggregation in trusted execution environment for Internet-of-things[J]. IEEE Transactions on Industrial Informatics,2023,19(2):1703-1714.

[45] Zhou C,Barati M. A TEE-guarded data management system for time-scale data in industrial Internet of things[J]. IEEE Internet of Things Journal,2025,12(17):34832-34845.

[46] 张勇,王艺博,张进伟,等. 基于区块链的电网调控数据溯源技术研究[J]. 电力信息与通信技术,2023,21(11):70-76.
Zhang Y,Wang Y B,Zhang J W,et al. Research on power grid dispatching and control data traceability technology based on blockchain[J]. Electric Power Information and Communication Technology,2023,21(11):70-76.

[47] Pan B F,Stakhanova N,Ray S. Data provenance in security and privacy[J]. ACM Computing Surveys,2023,55(14s):1-35.

[48] Irshad H,Ciocarlie G,Gehani A,et al. TRACE:Enterprise-wide provenance tracking for real-time APT detection[J]. IEEE Transactions on Information Forensics and Security,2021,16:4363-4376.

[49] 李知艺,袁涔,杨福,等. 云计算环境下配电网调度决策模型诱骗式隐私保护方法[J]. 电力系统自动化,2023,47(8):80-88.
Li Z Y,Yuan C,Yang F,et al. Deception-based privacy preservation method of dispatch decision-making model for distribution network in cloud computing environment[J]. Automation of Electric Power Systems,2023,47(8):80-88.

[50] 杨珂,王栋,李达,等. 面向能源电力区块链的跨域身份控制模型[J]. 中国电力,2023,56(5):209-216.
Yang K,Wang D,Li D,et al. A cross-domain identity control model for electric blockchain[J]. Electric Power,2023,56(5):209-216.

[51] 邱勤,徐天妮,张智杰,等. 算力网络安全应用需求与关键技术研究[J]. 信息技术与标准化,2022(11):19-24,33.
Qiu Q,Xu T N,Zhang Z J,et al. Research on security application requirements and key technologies of computing force network[J]. Information Technology & Standardization,2022(11):19-24,33.

[52] 陈晓红,郑博文,袁依格,等. 人工智能驱动的算力基础设施能效优化技术现状及展望[J/OL]. 中国工程科学,2026-06-20. https://link.cnki.net/urlid/11.4421.G3.20260227.1208.002.
Chen X H,Zheng B W,Yuan Y G,et al. Present situation and prospect of energy efficiency optimization technology for computing infrastructure driven by artificial intelligence[J/OL]. Strategic Study of CAE,2026-06-20. https://link.cnki.net/urlid/11.4421.G3.20260227.1208.002.

[53] 张开元. 面向可靠性和负载均衡的算力网络分级任务调度方法[D]. 北京:北京邮电大学,2025.
Zhang K Y. Hierarchical task scheduling algorithm for reliability and load balancing in computing power network[D]. Beijing:Beijing University of Posts and Telecommunications,2025.

[54] Wang Y T,Su Z,Zhang N,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.

[55] Zhao Y,Zhao J,Kang J W,et al. A blockchain-based approach for saving and tracking differential-privacy cost[J]. IEEE Internet of Things Journal,2021,8(11):8865-8882.

[56] Guo J J,Hou W J,Wang X Y,et al. Toward a new spatial paradigm of electricity–computing synergy under renewable energy endowments and geographical environmental constraints[J]. Applied Energy,2026,409:127495.

[57] 梁晨,曾博,雷乐意,等. 算力–电力联合市场下数据中心与配电网集成规划:一种多目标区间–随机优化方法[J]. 电力系统保护与控制,2025,53(16):120-135.
Liang C,Zeng B,Lei Y Y,et al. Integrated planning of data centers and distribution networks under the computing–electricity joint market:A multi-objective interval-stochastic optimization approach[J]. Power System Protection and Control,2025,53(16):120-135.

[58] Tang S J,Yu Y,Wang H,et al. A survey on scheduling techniques in computing and network convergence[J]. IEEE Communications Surveys & Tutorials,2024,26(1):160-195.

[59] Liu W Y,Yan Y J,Sun Y M,et al. Online job scheduling scheme for low-carbon data center operation:An information and energy nexus perspective[J]. Applied Energy,2023,338:120918.

[60] Feng G X,Lao K W,Chen G. Out-of-distribution detection of unknown false data injection attack with logit-normalized Bayesian ResNet[J]. IEEE Transactions on Smart Grid,2024,15(6):6005-6017.

[61] Yang H S,Zhang W J,Chung C Y,et al. AC false data injection attack based on robust tensor principle component analysis[J]. IEEE Transactions on Industrial Informatics,2024,20(8):9887-9897.

[62] Wu S T,Wang Q,Hu J X,et al. Dynamic spatiotemporal measurement uncertainty-aware detection for robust power system state estimation against stealthy FDIA[J]. IEEE Internet of Things Journal,2026,13(12):27656-27671.

[63] 吴舒坦,王琦,董昱,等. 基于混合量测时空动态异构的状态估计抗攻击功能设计及安全检测方法[J/OL]. 中国电机工程学报,2026-06-20. https://doi.org/10.13334/j.0258-8013.pcsee.251594.
Wu S T,Wang Q,Dong Y,et al. Anti-attack function design and security detection method of state estimation based on hybrid measurement spatio-temporal dynamic heterogeneity[J/OL]. Proceedings of the CSEE,2026-06-20. https://doi. org/10.13334/j.0258-8013.pcsee.251594.

[64] Wu S T,Wang Q,Zhang Z Y,et al. Physics–informed state estimation model with controllable uncertainty:Enhancing resilience against false data injection attacks in power systems[J]. IEEE Transactions on Industrial Informatics,2026:1-12.

[65] Roy S D,Sharma A,Chakrabarti S,et al. Securing power system data in motion by timestamped digital text watermarking[J]. IEEE Transactions on Smart Grid,2024,15(5):4974-4985.

[66] 杨挺,许哲铭,赵英杰,等. 数字化新型电力系统攻击与防御方法研究综述[J]. 电力系统自动化,2024,48(6):112-126.
Yang T,Xu Z M,Zhao Y J,et al. Review on research of attack and defense methods for digitalized new power system[J]. Auto-

mation of Electric Power Systems，2024，48(6)：112-126.

[67] 徐飞阳，薛安成，常乃超，等. 电力系统同步相量异常数据检测与修复研究现状与展望[J]. 中国电机工程学报，2021，41(20)：6869-6886.
Xu F Y，Xue A C，Chang N C，et al. Research status and prospects of detection，correction and recovery for abnormal synchrophasor data in power system[J]. Proceedings of the CSEE，2021，41(20)：6869-6886.

[68] 张锞，王旭，杨宏坤，等. 数据中心集群灵活边界下电力系统分布鲁棒优化调度方法[J]. 电力系统自动化，2024，48(7)：235-247.
Zhang K，Wang X，Yang H K，et al. Distributionally robust optimal scheduling method for power system under flexibility boundaries of data center clusters[J]. Automation of Electric Power Systems，2024，48(7)：235-247.

[69] 赵天阳，张华君，徐岩，等. 不确定环境下含云计算数据中心的电网韧性增强调度[J]. 电力系统自动化，2021，45(3)：49-57.
Zhao T Y，Zhang H J，Xu Y，et al. Resilience-enhanced scheduling of power system with cloud computing data centers under uncertainty[J]. Automation of Electric Power Systems，2021，45(3)：49-57.

[70] 刘方，陈祥洲，周江昕，等. 考虑数据中心共享储能与计算负荷时空迁移特性的虚拟电厂优化运行方法[J]. 电网技术，2026，50(5)：1848-1864.
Liu F，Chen X Z，Zhou J X，et al. Optimal operation method for virtual power plant considering shared energy storage and spatio-temporal migration characteristics of computational load in data centers[J]. Power System Technology，2026，50(5)：1848-1864.

[71] Azizi A，Morovati S，Zamani A，et al. Strengthening data center operations using grid-forming battery energy storage as a line-interactive uninterruptible power supply[J]. International Journal of Electrical Power & Energy Systems，2026，175：111638.

[72] 薛禹胜，李满礼，罗剑波，等. 基于关联特性矩阵的电网信息物理系统耦合建模方法[J]. 电力系统自动化，2018，42(2)：11-19.
Xue Y S，Li M L，Luo J B，et al. Modeling method for coupling relations in cyber physical power systems based on correlation characteristic matrix[J]. Automation of Electric Power Systems，2018，42(2)：11-19.

[73] 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 J，Guo Y H，Guo C X，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.

[74] 王琦，张静，胡健雄，等. 跨域攻击威胁下电力信息物理系统状态估计功能安全综述[J]. 电力系统自动化，2026，50(8)：15-36.
Wang Q，Zhang J，Hu J X，et al. Review on functional safety of state estimation in cyber–physical power system under cross-domain attack threats[J]. Automation of Electric Power Systems，2026，50(8)：15-36.

[75] 严康，郭庆来. 需求侧调控新主体网络安全态势感知关键技术[J]. 电力系统自动化，2026，50(8)：1-14.
Yan K，Guo Q L. Key technologies of cyber security situation awareness for new dispatch and control entities on demand side[J]. Automation of Electric Power Systems，2026，50(8)：1-14.

[76] Wu S T，Wang Q，Hu J X，et al. Dynamic PMU configuration for stealthy multi-snapshot FDIA mitigation：Enhancing security in hybrid-measurement-based state estimation in power systems[J]. IEEE Transactions on Smart Grid，2026，17(1)：650-665.

[77] 魏繁荣，柏淳瀚，林湘宁，等. 能源互联网信息–物理跨域安全风险量化：特征及展望[J/OL]. 电力系统自动化，2026-06-20. https://link.cnki.net/urlid/32.1180.TP.20251110.0902.006.
Wei F R，Bai C H，Lin X N，et al. Quantification of cross-domain security risks of energy Internet information–physics：Characteristics and prospects[J/OL]. Automation of Electric Power Systems，2026-06-20. https://link.cnki.net/urlid/32.1180.TP.20251110.0902.006.

[78] 刘依晗，王宇飞. 新型电力系统中跨域连锁故障的演化机理与主动防御探索[J]. 中国电力，2022，55(2)：62-72，81.
Liu Y H，Wang Y F. Exploring the evolution mechanism and active defense of cross-domain cascading failures in new type power system[J]. Electric Power，2022，55(2)：62-72，81.

[79] 孙溶佐，蔡晔，曹一家，等. 计及跨域连锁故障的电力信息物理系统N-k协同故障场景筛选双层优化模型[J]. 中国电机工程学报，2026，46(1)：87-100.
Sun R Z，Cai Y，Cao Y J，et al. A bi-level optimization model for selecting N-k coordinated fault scenarios in cyber–physical power system considering cross-domain cascading failures[J]. Proceedings of the CSEE，2026，46(1)：87-100.

[80] Wu S T，Wang Q，Hu J X，et al. Attack-resilient state estimation for cyber–physical power systems：A dynamic spatial-temporal redundancy reconfiguration framework for FDIA detection[J]. Applied Energy，2025，397：126330.

[81] 张涛，费稼轩，王琦，等. 电力信息物理系统跨域攻击协同防御架构及机制研究[J]. 电子学报，2024，52(4)：1205-1218.
Zhang T，Fei J X，Wang Q，et al. Research of architecture and mechanism of coordinative defense methods for cross-domain attacks of cyber physical system[J]. Acta Electronica Sinica，2024，52(4)：1205-1218.

[82] 刘烃，田决，王稼舟，等. 信息物理融合系统综合安全威胁与防御研究[J]. 自动化学报，2019，45(1)：5-24.
Liu T，Tian J，Wang J Z，et al. Integrated security threats and defense of cyber–physical systems[J]. Acta Automatica Sinica，2019，45(1)：5-24.

[83] 邬江兴，邹宏，薛向阳，等. 内生安全赋能网络弹性的构想、方法与策略[J]. 中国工程科学，2023，25(6)：106-115.
Wu J X，Zou H，Xue X Y，et al. Cyber resilience enabled by endogenous security and safety：Vision，techniques，and strategies[J]. Strategic Study of CAE，2023，25(6)：106-115.