信息-物理耦合网络在新型电力系统中的应用与挑战

王卫民[1]，黄 煜[1]，胡松林[1]，王 毅[2]

[1]南京邮电大学 江苏南京
[2]国网电力科学研究院有限公司（南瑞集团有限公司） 江苏南京

【摘要】随着可再生能源比例的提升，信息-物理耦合系统（Cyber-Physical Power System, CPPS）在新型电力系统中的作用愈发重要。本文系统梳理了 CPPS 在分层建模、协同仿真、智能控制、网络安全与韧性提升等方面的关键技术与应用进展。特别是在可再生能源接入和动态响应优化等场景中，CPPS 通过先进的建模框架与协同仿真平台实现了系统性能的优化。本文分析了当前 CPPS 应用中面临的主要问题，如建模一致性不足、故障传播机制复杂、控制依赖性增强等，并探讨了数字孪生技术与强化学习方法在状态估计、异常检测及自适应调度中的应用潜力。最后，本文还讨论了 CPPS 在提升电力系统韧性方面的挑战与未来发展方向，为构建高可观测性、可恢复性和智能协同能力的电力系统提供了理论支持。

【关键词】信息-物理耦合系统；分层建模；智能控制；网络安全；强化学习
【收稿日期】2025 年 2 月 20 日 【出刊日期】2025 年 3 月 18 日 【DOI】10.12208/j.jeea.20250082

Application and challenges of Cyber-Physical systems in emerging power grids

Weimin Wang[1], Yu Huang[1], Songlin Hu[1], Yi Wang[2]

[1]Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu
[2]State Grid Electric Power Research Institute(NARI Group Corporation), Nanjing, Jiangsu

【**Abstract**】With the increasing penetration of renewable energy, Cyber-Physical Power Systems (CPPS) are playing an increasingly critical role in the development of next-generation power systems. This paper provides a comprehensive review of key technologies and recent advances in CPPS, including hierarchical modeling, co-simulation, intelligent control, cybersecurity, and resilience enhancement. In particular, CPPS have demonstrated significant improvements in system performance through advanced modeling frameworks and co-simulation platforms, especially in scenarios involving renewable energy integration and dynamic response optimization. The paper further analyzes major challenges in current CPPS applications, such as modeling inconsistency, complex fault propagation mechanisms, and increased control dependency. Moreover, the potential of digital twin technologies and reinforcement learning methods is explored in the context of state estimation, anomaly detection, and adaptive scheduling. Finally, this study discusses the challenges and future directions of CPPS in enhancing power system resilience, offering theoretical insights for the development of highly observable, recoverable, and intelligently coordinated power systems.

【**Keywords**】Cyber-Physical power system; Hierarchical modeling; Intelligent control; Cybersecurity; Reinforcement Learning

1 前言

随着新型电力系统建设深入推进，物理电网正加速向集成感知、通信与控制功能的信息-物理耦合架构演进[1]。通信网络与物理系统的深度融合显著提升了系统的可观测性与灵活性，但同时也带来了更强的信息依赖性。一旦通信中断、控制链路异常或遭受网络攻击，可能引发信号失真、指令失效，进而造成系统扰动放大甚至大范围停电。特别是在可再生能源、电动汽车与电力电子设备广泛接入的背景下，系统运行的不确定性与动态性显著增强，亟

需构建具备高可靠通信、快速感知与主动防御能力的协调控制体系[2]。

针对上述挑战，近年来国内外在 CPPS 的关键环节开展了大量研究[3-10]。建模方面，普遍采用分层抽象与复杂网络理论相结合的方式，构建物理层—通信层—控制层的多维交互模型[3-4]，以刻画不同系统间的耦合关系与失效传播路径。在仿真方面，基于大规模基础设施协同仿真（HELICS）、网络协同仿真框架（FNCS）等协同仿真平台[5]，实现了电力与通信系统的异步协同模拟；数字孪生技术[6-7]亦被引入，用于状态估计与运行预测。控制策略方面，从集中式架构逐步演进至分布式、自主与事件驱动机制，以增强系统的局部响应能力与整体韧性。在网络安全方面[8-9]，针对虚假数据注入、拒绝服务等攻击类型，构建了基于图论与机器学习的检测机制，并探索了信息重构、结构扰动等防御方法。此外，人工智能（AI）在负荷预测、运行优化与异常识别等任务中展现出应用潜力[10]，但在模型泛化性、可解释性与安全性方面仍存不足。

本文围绕 CPPS 的系统建模、协同仿真、智能控制、网络安全与韧性优化等关键技术路径，系统梳理当前研究现状与典型成果，分析存在的技术瓶颈与发展趋势，旨在为构建具备高可观测性、高安全性与高适应能力的新型电力系统提供理论支撑与技术参考。

2 信息-物理耦合系统的建模方法

2.1 多层结构的系统建模方法

CPPS 系统由电力设备、通信网络和控制系统等构成，具备明显的异构耦合特性。为清晰刻画各子系统间的交互关系，建模过程普遍采用分层结构，将系统划分为物理层、通信层与控制层。物理层包括输配电网、发电与储能设备、终端负荷等，侧重描述能量传输过程；通信层涵盖感知设备、通信链路与协议机制，承担信息采集与传输功能；控制层负责调度逻辑与控制策略的执行，实现信息与物理过程的协同调控。

为支撑分层建模，多种典型架构模型已被提出[11-13]。智能电网架构模型（SGAM）通过“功能—层次—区域”的三维架构，统一描述从终端到控制中心的系统结构；能源互联网模型分为“感知—网络—应用”三层，利用物联网技术，将传统的能源系统（如电力、天然气、水力等）与信息技术结合起来，实现更高效、智能的能源管理和分配；美国能源部提出的一种架构采用五层体系表达数据采集、分析、辅助决策、运行控制与网络安全等功能分布，以支持输配电系统的集成。尽管模型结构不尽相同，均体现出物理、通信与控制机制之间的深度耦合。

建模过程中，还需充分考虑子系统运行特性的差异。输电系统结构集中、通信稳定，适宜采用集中式建模与广域协调控制；配电系统结构松散、源荷分布不均，需融合微电网、自主控制与用户行为模型。因此，统一的建模框架下，应根据场景选择具备区域适应性的子系统建模方案。

2.2 跨域复杂系统的行为建模方法

CPPS 运行过程涉及大量跨域动态行为，表现为能量流与信息流之间的强耦合、时序差异与非对称响应。为真实刻画系统状态与动态演化，建模需兼顾物理连续变量与信息离散事件，构建融合拓扑结构与控制行为的动态模型。

复杂网络理论为该类建模提供了有力工具[14]。通过图模型可同时表达拓扑结构与节点间的功能关联，识别系统中的关键设备、路径依赖与故障传播链条。将电网与通信网络构建为耦合图，可模拟节点故障后的连通性变化与级联传播过程，识别具有高脆弱性的节点组合，揭示系统在拓扑冗余不足条件下的崩溃风险。假定电力网络表示为$G_P(V_P,E_P)$，V_P为物理节点集合（如发电机、变压器、负荷），E_P为电力网络的边集合，通信网络表示为$G_C(V_C,E_C)$，V_C为通信节点（如传感器、控制器和通信链路等），E_C为通信网络的边集合。电力网络和通信网络之间的耦合关系体现在它们的边上，通过跨域连接边E_{PC}实现相互依赖。

为进一步揭示通信扰动对电力系统控制性能的影响，建模中需引入服务质量指标与脆弱性评估机制，量化通信延迟、丢包等信息扰动对调控过程的干扰效应。例如，通信节点因断电失效可能导致控制指令中断、负荷脱网或保护误触等异常事件。为此，研究提出构建融合结构属性与通信行为的脆弱性分析框架，基于节点中心性、路径冗余度等图指标，量化关键设备在不同攻击或故障路径下的响应能力，为防御策略设计与资源配置提供依据。

尽管已有多种跨域建模方法，但实现系统级统一建模仍面临挑战。一是通信网络缺乏标准化结构数据，难以与电力模型高效集成；二是信息与通信

技术与电气设备在数据语义和接口协议上存在差异，限制模型互操作性与复用效率；三是拓扑与行为建模工具间缺乏统一接口，制约其在协同仿真平台中的部署与扩展。为解决上述问题，应在 SGAM 等统一架构基础上，发展具备跨域模拟能力与时序逻辑表达能力的建模语言，并与 IEC 61850、通用信息模型（CIM）、通用网格模型交换标准（CGMES）等主流数据标准深度融合。

3 协同仿真与数字孪生

3.1 协同仿真方法

3.1.1 应用场景与价值体现

协同仿真[15]通过实现不同领域仿真工具间的数据交互与行为耦合，可有效评估系统在网络攻击、设备故障与通信延迟等复杂扰动下的动态响应。相比传统单域仿真，其可同时捕捉电气侧控制丢失与信息侧异常传输等跨域效应，有助于揭示故障传播路径及其引发的级联风险。此外，协同仿真平台可构建多类攻击场景，为网络安全策略的开发与验证提供安全、可控的测试环境；在数据匮乏情况下，亦可生成大规模仿真样本，支撑 AI 算法训练与测试。

3.1.2 典型平台与集成机制

当前主流平台如 HELICS、FNCS 和实时协同仿真平台（EXataCPS）等，均支持多仿真器协同运行。HELICS 具备较强的跨域模型对接与时间管理能力，适用于电力、通信、水气热等多能系统集成；FNCS 支持电力、通信与控制仿真器交互，广泛应用于配电系统研究；EXataCPS 则适用于实时网络环境下的高保真仿真。系统层面通常采用事件驱动机制实现多模型同步，支持从电磁暂态到控制逻辑的多粒度建模。对于涉及物理设备的验证，可通过硬件在环（HIL）或电源硬件在环（PHIL）仿真实现与真实装置交互，满足继电保护、相量测量单元（PMU）等设备的测试需求。

3.1.3 发展需求与关键挑战

协同仿真仍面临模型结构异构、数据接口复杂与时间同步效率低等挑战。大规模系统中，仿真器运行速度差异显著，导致运行时的同步效率较低，需要高效的调度算法与缓存策略；模型层面，接口定义不统一、语义差异显著，制约模型移植与平台间复用。未来应加强对系统行为的细粒度建模能力，提升信息传播、控制逻辑与故障扩散过程的描述精度。同时，协同仿真需支持离散—连续联合建模，满足多精度、多场景的仿真需求。

3.2 数字孪生技术

数字孪生（DT）技术通过构建与实际设备或系统高度对应的数字模型，并结合实时测量数据，实现运行状态的动态映射与预测，可广泛应用于状态评估、故障预警与运行优化等场景。与传统建模相比，DT 具备更强的实时性与对象针对性，特别适用于远端、复杂或不可观测部位的状态监测与行为仿真。

数字孪生系统通常集成监控和数据采集（SCADA）系统、智能电表、PMU 等多源感知数据，结合仿真平台或 HIL 实现模型校准与验证。根据场景需求，DT 模型可灵活调整刷新频率与建模精度。例如，PMU 的高频采样适用于暂态稳定性分析，SCADA 则更适合稳态估计与运行优化。总体来看，数字孪生正逐步从状态监测扩展至控制优化与安全防护领域，成为支撑电力系统智能化与韧性能力提升的重要工具。

4 融合信息-物理交互特性的系统监测、运行与稳定控制研究

4.1 状态监测与态势感知

在 CPPS 环境下，系统运行对状态监测的实时性与动态响应提出更高要求。当前研究通过融合物联网设备与电力基础设施，利用通信网络实现信息共享，并结合分布式计算增强系统的状态感知能力。尽管 PMU 显著提升了系统可观测性，但由于部署成本高、覆盖范围有限，难以实现对大规模系统的持续监测。因此，需引入融合物理与网络信息的状态估计方法，辅助重构关键状态量，提升监测精度与控制效果。

状态估计[16-17]作为 CPPS 监测的核心技术，主要包括静态状态估计（SSE）和动态状态估计（DSE）。SSE 利用 PMU 数据在线监测所有节点的电压幅值与相角，可识别由设备故障或网络攻击引起的异常数据；DSE 则结合系统模型与时间同步测量，对不可观测动态量进行推断与预测，有助于风险预警与趋势研判。此外，状态估计还能辅助识别虚假数据注入等攻击行为，增强系统的安全性与韧性。

4.2 面向系统优化与控制的机器学习方法

4.2.1 监督与无监督学习的典型应用

监督学习在发电预测、负荷辨识与动态定价建模中已获得较好效果，适用于数据质量高、模式稳定的场景。但在存在数据缺失或扰动频繁的系统中，其性能表现不稳定。无监督学习则多用于聚类分析

与异常检测，借助主成分分析、K-means 聚类、分层聚类等算法发掘数据结构特征，但缺乏对物理约束的建模支持，难以满足系统级决策需求。

4.2.2 强化学习在控制优化中的探索

强化学习[18]（RL）作为一种自适应机器学习方法，逐渐在 CPPS 中得到应用，特别是在需求响应、能源管理和网络攻击防御等方面。例如，Q-Learning 已被提出用于电力系统的网络攻击防护，并在 IEEE 39 节点系统中进行了验证，但其在实际环境中的效果仍需进一步评估。深度 Q-Learning 通过引入神经网络，增强了对复杂状态-动作空间的处理能力。其他基于策略的 RL 方法，如深度确定性策略梯度（DDPG）和近端策略优化（PPO），也在优化电力系统攻击防御策略方面显示出潜力。尽管 RL 能够为电力系统提供强健的防御机制，但其面临计算资源和可解释性等挑战，未来的研究将着重于提高算法的实用性和有效性。

4.2.3 面临的主要问题与发展方向

机器学习[19]（ML）在 CPPS 中的应用前景广阔，但也面临多重挑战。首先，许多 ML 方法依赖启发式策略，缺乏对最优化结果或预测准确性的严格数学保证，导致其决策过程中的不确定性。其次，数据质量问题突出，恶意行为者可能篡改训练数据，进而影响 AI 系统的决策，威胁电力系统的稳定性。CPPS 产生的海量数据对实时处理提出高要求，但现有算法在保证实时性的同时难以高效处理这些数据。此外，深度学习等复杂模型的“黑箱”特性使得其决策过程难以解释，增加了系统的不透明性和风险。这些问题限制了机器学习在电力系统中的实际应用，特别是在保障系统可控性和识别潜在攻击方面。尽管如此，机器学习在提高 CPPS 性能和智能化水平上的潜力依然巨大，未来的研究需解决数据质量、计算效率和模型可解释性等关键问题。

4.3 信息-物理融合系统的稳定性研究

4.3.1 电力电子主导系统的控制架构

当前系统控制已逐步从同步机主导转向以变流器为核心的“弱惯量”架构，系统惯性调节能力减弱，需依赖先进控制策略确保频率稳定。常见控制结构包括下垂控制、二次协调控制和三级优化控制。随着通信技术的广泛应用，电力系统暴露面增大，为了提高系统抗干扰能力和降低信息安全风险，事件触发与自触发机制被提出作为替代手段，这些机制通过减少通信频率，有效降低了对通信系统的依赖，增强了电力系统的鲁棒性。

4.3.2 通信时延对控制稳定性的影响

CPPS 的稳定性在很大程度上依赖于其网络基础设施，其中时间延迟问题尤为突出。在去中心化或中心化控制的系统中，广域阻尼控制（WADC）中的反馈延迟可能危及系统稳定性，特别是在大规模 CPPS 中。此外，负荷频率控制（LFC）中的时延会影响各控制区域之间的有功功率调节，进一步威胁系统的稳定性。在完全分布式控制的系统中，尤其是集成可再生能源的微电网中，时间延迟使得信息流动和邻居间通信变得复杂，影响频率和电压的稳定。分布式控制系统的同步控制周期对稳定性至关重要，但由于控制器执行的时间延迟差异，可能导致同步失效。为应对这些挑战，研究者已提出相关模型，提供了多重时间延迟系统中稳定同步间隔的设计标准。

4.3.3 网络攻击带来的稳定性风险

CPPS 在开放环境下易受到虚假数据注入、信号篡改等攻击，攻击者可操纵反馈信息诱导错误控制决策，引发频率偏移、谐振失稳等安全风险。典型攻击目标包括静态同步补偿器、风力涡轮机等设备控制器，其不稳定将导致区域乃至系统级震荡。为提升系统抗攻击能力，需构建多层防御机制，引入电力系统稳定器、WADC 等控制模块来增强系统稳定性，同时强化信息流监测，实现对网络攻击的快速识别与响应控制。

5 网络安全与人工智能在 CPPS 中的融合应用

在系统运行层面，AI 技术已被用于构建多尺度负荷预测与状态感知模型[20-21]。深度学习与图神经网络可融合高级计量基础设施（AMI）、PMU 等多源感知数据，实现对配电侧负荷变化的高精度预测与对系统状态的动态估计，提升了系统可观测性。针对配电系统中实时测量不足的问题，AI 还能辅助生成伪测量并进行异常数据修正，提高状态估计的准确性。

在网络安全层面，AI 为 CPPS 提供了智能化攻击识别与动态防御能力。深度模型可挖掘数据中的时空关联特征，用于检测拒绝服务、虚假数据注入等高隐蔽性攻击。同时强化学习方法也被引入到调度控制中，用于应对协同攻击与动态扰动下的快速恢复与局部控制，增强系统的弹性应对能力。

尽管 AI 具备广泛应用潜力，其在 CPPS 中的落地仍面临训练样本不足、泛化能力弱、模型可解释性

差等问题。未来需加强 AI 与电力物理模型、控制边界及通信协议的深度融合，构建具备工程适应性、安全鲁棒性与可迁移能力的智能运行架构，推动 CPPS 向自感知、自学习、自防御方向演进。

6 面向韧性提升的信息-物理融合电力系统

在极端气象与系统不确定性增强的背景下，提升 CPPS 的韧性成为保障电力连续供能与快速恢复的关键。互联微电网凭借自治运行与灵活组网能力，可在灾后实现局部解耦与应急供电。引入软件定义网络[22]（SDN）可构建具备动态重构能力的通信架构，提升其在故障下的自适应调控能力。面向韧性的运行策略可分为“预防—缓解—恢复”三个阶段：灾前聚焦于信息流鲁棒调度与路径冗余设计，增强调控链路稳定性；灾中强调微电网快速隔离与动态重构，支撑区域自组织运行；灾后则通过移动电源部署与负荷优先恢复，实现关键区域有序复电。未来 CPPS 韧性提升应从三方面协同推进：优化微电网结构与自治控制机制，增强边缘区域独立运行能力；提升通信网络的重构能力与容错性能；构建跨阶段联动的闭环调控策略，增强系统的自适应与自恢复能力。

7 结语

随着电力系统数字化与智能化的推进，信息与物理系统的耦合日益加深，导致系统的运行不确定性和安全风险显著上升。为提升 CPPS 的可持续性与韧性，需要从建模、控制和安全机制等方面协同推进。首先，传统建模方法难以准确反映 CPPS 的动态交互特性，亟需发展融合物理机制与数据驱动的混合建模方法，构建具有跨域协同和高时空分辨率的仿真平台，增强系统对极端工况和多源扰动的分析能力。同时，结合数字孪生技术和实时监控手段，有助于提升系统在复杂环境中的适应性与应对能力。其次，人工智能在故障诊断、状态估计和调度优化等领域的应用正在扩展，但其可解释性差、泛化能力弱等问题仍然存在。未来的研究应着力于 AI 算法与电力系统物理规律的融合，构建具备物理约束和自适应能力的智能控制框架，推动系统从感知驱动向机制驱动转变。这不仅能优化调度策略，还能实现实时调整和自我优化，增强系统的灵活性和稳定性。

最后，CPPS 的高度互联性带来了更大的网络安全隐患，尤其是在智能电网和可再生能源广泛接入的背景下，电力系统面临更复杂的安全挑战。因此，应加强安全通信协议、认证机制和主动防御手段的联合设计，探索区块链、量子加密等新兴技术在电力信息基础设施中的应用。同时，推动电力行业标准体系建设和复合型网络安全人才的培养，为系统韧性演进提供有力支持。这些努力将为电力系统的稳定运行奠定基础，提升其应对突发事件和复杂威胁的能力。

参考文献

[1] 胡钋,李莉莉. 智能电网的信息物理安全综述 [J]. 信息安全研究, 2019, 5 (12): 1068-1075.

[2] 阮广春,何一鎏,谭振飞,等. 面向新型电力系统运行的数据-物理融合建模综述 [J]. 中国电机工程学报, 2024, 44 (13): 5021-5037.

[3] 王东芳,刘水源,张勇军,等. “互联网+”形势下电力信息物理融合发展研究综述与展望 [J]. 电力自动化设备, 2020, 40 (06): 90-99.

[4] 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 (09): 200-215.

[5] Ciraci S, Daily J, Fuller J, et al. FNCS: A framework for power system and communication networks co-simulation[C]. Proceedings of the symposium on theory of modeling & simulation-DEVS integrative. 2014: 1-8.

[6] 赖博宏,郝俊红,杨天缜,等. 数字孪生支撑下综合能源系统的智慧运维发展与挑战 [J/OL]. 中国电机工程学报, 1-17.

[7] Wagg D J, Worden K, Barthorpe R J, et al. Digital twins: state-of-the-art and future directions for modeling and simulation in engineering dynamics applications[J]. ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part B: Mechanical Engineering, 2020, 6(3): 030901.

[8] 阳育德,蓝水岚,覃智君,等. 电力信息物理融合系统的网络-物理协同攻击 [J]. 电力自动化设备, 2020, 40 (02): 97-103.

[9] 杨至元,张仕鹏,孙浩. 电力系统信息物理网络安全综合分析与风险研究 [J]. 南方能源建设, 2020, 7 (03): 6-22.

[10] 叶宇剑,吴奕之,胡健雄,等. 城市电力-交通耦合系统的联合推演与协同优化：研究综述、挑战与展望 [J]. 中国

电机工程学报, 1-20.

[11] 刘日亮,李晓露,杜建,等. 基于智能电网架构模型的营配调贯通一体化模型构建方法 [J]. 电力信息与通信技术, 2022, 20 (07): 18-25.

[12] 张晶,胡纯瑾,高志远,等. 能源互联网技术标准体系架构设计及需求分析 [J]. 电网技术, 2022, 46 (08): 3038-3048.

[13] Photovoltaics D G, Storage E. IEEE standard for interconnection and interoperability of distributed energy resources with associated electric power systems interfaces[J]. IEEE std, 2018, 1547(1547): 2018.

[14] 张诗琪,李琰,徐天奇. 基于复杂网络理论的电力信息物理系统耦合建模方式研究与脆弱性分析 [J]. 云南民族大学学报(自然科学版), 2022, 31 (06): 762-769.

[15] 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 (03): 399-429.

[16] 胡健雄,汤奕,王琦,等. 面向在线动态安全分析的高时空分辨率状态估计：研究现状与方法框架 [J]. 中国电机工程学报, 1-22.

[17] 韩一宁,崔明建,罗光浩,等. 基于自适应联邦学习的输配网动-静态综合状态估计方法研究 [J]. 中国电机工程学报, 1-15.

[18] 王新迎,闫冬,施展,等. 机器学习赋能的优化算法及其在新型电力系统中的应用与展望 [J]. 中国电机工程学报, 2024, 44 (16): 6367-6385.

[19] 乔骥,赵紫璇,王晓辉,等. 面向电力系统智能分析的机器学习可解释性方法研究(二)：电网稳定分析的物理内嵌式机器学习 [J]. 中国电机工程学报, 2023, 43 (23): 9046-9059.

[20] 王小君,窦嘉铭,刘婴,等. 可解释人工智能在电力系统中的应用综述与展望 [J]. 电力系统自动化, 2024, 48 (04): 169-191.

[21] 张俊,徐箭,许沛东,等. 人工智能大模型在电力系统运行控制中的应用综述及展望 [J]. 武汉大学学报(工学版), 2023, 56 (11): 1368-1379.

[22] 严康,陆艺丹,于宗超,等. 配电网用户侧异构电力物联设备运行安全管控分析 [J]. 电力系统自动化, 2023, 47 (08): 53-61.