信息物理系统抗干扰控制研究

陈德荣
东南大学，南京 210018，中国

摘要：信息物理系统通过计算、通信和控制技术，将计算系统、通信网络和物理环境融合，形成集实时感知、动态控制和信息服务于一体的多维异构复杂系统，实现电网物理系统系统内部资源配置和运行的按需响应、快速迭代和动态优化。信息物理系统是支撑信息化与工业化深度融合的综合技术体系，具有重要的战略意义。

关键词：动态优化；最优拟合

Anti-interference Control of Information Physics System

Chen Derong
Southeast University, Nanjing 210018, China

Abstract: The Information Physics System (CPS, Cyber Physical System) integrates computing systems, communication networks and physical environments through computation, communication and control technologies to form a multi-dimensional heterogeneous complex system integrating real-time sensing, dynamic control and information services. Enable on-demand response, fast iteration, and dynamic optimization of resource configuration and operation within the CPS system. CPS is a comprehensive technical system that supports the deep integration of informationization and industrialization, and is of great strategic significance.

Keywords: Dynamic optimization; Optimal fit

工信部发布《信息物理系统白皮书（2017）》指出，信息物理系统的本质是构建一套基于信息空间与物理空间之间数据自动流动的状态感知、实时分析、科学决策、精准执行的闭环使能系统，解决制造业和应用服务的复杂性和不确定性，提高资源配置效率，实现资源最优化配置。2017年，《国务院关于深化制造业与互联网融合发展的指导意见》进一步明确提出“构建信息物理系统模型及综合技术标准体系，建设测试验证平台，支撑兼容适配、互联互通和互操作测试验证”。在配电网领域，随着“信息化、自动化、互动式”智能配电网建设与改造工作的推进，配电自动化、用电信息采集系统、智能电表、终端等信息通信系统在配电网中的应用逐渐普及，光伏、风电、储能、充电桩等基于柔性控制的分布式能源或用电设备的接入，进一步强化了配电网的可控性以及对信息控制系统的依赖。通过集成先进的测量系统、数据采集设备、计算设备以及嵌入式柔性控制设备，配电网和信息通信网络两个物理网络深度互联，使得配电网一次系统与二次系统相互耦合联系，具备典型的信息物理系统的基本特征，配电网电网物理系统融合系统已成为智能电网和能源互联网的发展方向和形态[1-2]。因此，本文分析了多场景扰动下配电网物理设备层与信息层的动态交互关系，及其运行状态的演化机理。研究相应的抗干扰控制策略,开展配电网电网物理系统仿真应用,完善配电网调度物理信息系统,提高配电

网电网物理系统的可靠性和安全性管控能力是配电网电网物理系统研究中需要解决的重要问题,具有重要的理论和实用价值。

一、信息物理系统

多层次、多维度的现代电力系统态势感知与优化控制需要大量的实时数据交换。信息层与物理层建立相互依赖关系，物理层节点为建立依赖关系的信息层节点提供能量支撑；信息层节点为建立依赖关系的物理层节点提供3C（通信、计算、控制）支撑。相互依赖作为信息层与物理层信息、能量交互的接口，改善了数据采集种类和通信效率，提高了系统的实时控制能力，丰富了控制功能，但同时也引入了新的可靠性风险和故障发展形式。相互依赖关系的相互依赖成为故障传播的通道，导致系统可靠性下降，故障在信息层的各个物理层之间交替发生，并带来交互连锁故障。信息层故障将导致电网控制中心丧失对部分电力设备运行数据的监控和采集能力，或丧失部分控制功能[3]。

本文基于配电网电网物理系统信息物理深度融合特性，考虑多电源约束、多信息约束以及信息系统与物理系统间的耦合关系，研究多扰动场景下配电网信息物理系统的深度融合与实时交互过程。在此基础上，研究了相应的抗干扰控制策略，对于理解电网信息物理系统信息层-物理层的相互影响机理及故障风险管理具有重要的理论和实践意义[4]。

针对上述现状，我们将重点研究配电网多运行状态下信息系统与物理设备系统实时融合交互及运行状态演化机理、故障过程分析及抗干扰控制策略，实现以下目标：

（1）研究通信拥塞、多类型故障、信息篡改等多场景扰动下配电网信息系统与物理系统的动态交互效应及系统运行状态演化机理，为配电网系统总体安全控制策略研究提供理论依据和决策依据。

（2）研究多场景信息系统与物理系统扰动下的配电网抗干扰控制策略，解决通信拥塞、多类型故障、信息篡改等多场景扰动下配电网稳定运行和可靠性问题。

（3）发展多场景信息系统和物理系统扰动下配电网抗干扰仿真技术，提高配电网可靠性和供电安全性。

二、经济效益

对配电网抗干扰仿真分析技术的发展具有显著的推动作用，可有效提高配电网安全可靠经济运行水平，具有较高的经济效益和社会效益。

多场景扰动下配电网信息系统与物理系统的动态交互分析，以及系统运行状态演化机理研究，可以实现对复杂配电网信息在物理扰动下的仿真，如通信拥塞、多类型故障、信息篡改等动态变化过程及其实时交互影响提供仿真手段，为配电网安全稳定运行提供决策依据，并具有良好的经济效益。

三、配电网物理信息系统

当今信息通信技术已广泛应用于电力系统，实现了信息空间与电网物理系统的紧密融合，极大地改变了电力系统的物理形态和运行方式，形成了信息物理系统)，电力系统运行分析也发展成为考虑信息空间与电网物理系统相互作用的系统运行分析。未来，其相关理论将是下一代电力系统的重要实现和分析控制技术的理论基础。目前，学术界已尝试探索电网物理系统系统运行中的信息-物理交互过程，并在信息空间与电网物理系统交互、离散信息状态（信息流）和连续电力过程（能量流）等领域取得了一些研究进展。首先，部分文献构建了电网物理系统中信息空间与电网物理系统的交互拓扑结构，并探讨了典型业务场景下交互拓扑结构的动态变化及其对电网物理系统脆弱性的影响。其次，一些文献从电网物理系统运行层面探讨了信息流与能量流的协同机制。再次，一些文献探讨了电网物理系统运行实际业务场景中的信息-物理交互过程。然而，以上研究成果与目前的研究成果相比仍然存在较大的局限性。一方面，对电网物理系统运行的信息-物理交互特性分析不够

深入，套用其他行业电网物理系统的分析方法，难以准确描述离散信息状态与连续动力过程之间的动态交互过程；另一方面，将信息-物理交互拓扑结构（系统运行的路径）与信息流-能量流动态驱动（系统运行的事件）两个紧密耦合的系统运行要素进行拆分研究，研究成果仅反映信息-物理交互过程的部分机理，缺乏对信息-物理交互机理的全面研究，难以有效解释电网物理系统的运行机理及演化过程。电网物理系统是典型的复杂异构系统，系统运行的信息-物理交互过程包括信息节点与动力节点之间的信息-物理交互拓扑结构、信息流与能量流之间的协同作用以及二者的叠加生成的电网物理系统运行状态的演化等多项信息-物理交互过程。

信息节点与电源节点之间的连接方式有多种，且连接状态随电网物理系统运行状态动态变化。一方面，电网物理系统节点功能形式各异，因而存在多种连接方式，如单向单通道型（变压器、合并单元等之间的单向数据传输）、双向双路径型（保护装置与一次设备状态监视路径和保护动作执行路径等）、双向多通道型（配电终端与开关之间的三遥功能及保护路径）等；另一方面，在电网物理系统的不同运行状态下，节点间的连接状态可为“连接且有效”（正常工作）、“连接无效”（备用或故障）、“连接断开”（检修或故障）。上述信息-物理交互拓扑结构使得直接建立基于图的精确电网物理系统运行模型变得困难。信息系统对物理系统的直接影响是指信息系统组件或功能的故障直接导致相应的物理组件失效。例如，当断路器的智能电子设备发生故障时，断路器分闸。信息系统对物理系统的间接影响是指信息系统故障不会引起物理组件失效，但会导致物理系统性能的恶化。这种影响可以分为两种情况。一是物理系统正常运行时，监测、控制或保护功能失效对电网运行的潜在影响。例如，当电网监测发生故障时，线路将无法获知运行状态，无法应对潮汐穿越等问题。二是当物理系统发生故障时，信息系统同时发生故障，将影响故障排除过程，使系统状态恶化。如果输电网发生故障，断路器控制功能失效将引发连锁故障。

信息物理的直接分析考虑了信息故障对物理元件的影响，分析方法更注重元件间逻辑关系的建立。信息物理的间接关系更关注信息故障对物理系统状态的影响，这种影响需要同时模拟信息元件故障和物理状态求解。因此，不同的信息物理作用模式所采用的分析方法和建立的相关模型也有所不同。

针对电网物理系统的耦合特性及其建模方法，国内外多个相关研究小组开展了一些相关研究。美国德克萨斯A&M大学相关学者提出了一种表征发电机与负荷之间信息系统与物理系统相互作用的动态框架，通过引入物理系统和信息系统的输入/输出信号，体现信息在各自电网物理系统模块内部动态、局部感知和执行行为中的作用。针对配电网信息系统与物理系统相互关联、交互和紧耦合的特点，奥地利国家理工学院（AIT）分别采用连续时间模型和离散事件模型对电网物理系统进行建模，并分析比较了两种模型对电网物理系统的适用性。为了充分展现信息系统与物理系统的耦合关系，加拿大渥太华大学提出了一种电网物理系统效用模型，其中每个信息系统节点仅与一个物理系统节点有支撑链路，每个物理系统节点连接到多个信息系统节点。西班牙马拉加大学计算机学院将电网物理系统的耦合特性与智能电网相对应。分析了智能电网中信息系统与物理系统之间的相互作用原理，进一步提出了系统间关系可能存在的安全性问题。为了深入研究智能电网信息系统与物理系统的耦合特性，美国Power World公司提出了一种面向智能电网的电网物理系统在线仿真模型架构，重点分析了信息系统与物理系统之间可能存在的相互作用对电网可靠性的影响。在这些现有电网物理系统建模研究中，没有区分电力系统中的主网和配网，配网电网物理系统的融合建模研究有待进一步研究。针对有源配电网信息系统的建模，基于图论建立了配电网信息通信系统物理层模型，分析了配电网信息系统的脆弱性以及通过通信线路对配电网的影响特性。变电站通信网络的链路层模型能够反映信息系统除线路通断之外的详细信息参数，例如信息传输速率、传输时延等，有助于配电网信息系统的网络性能分析和灵敏度分析。针对配电网物理系统的信息部分，建立了包含多种通信设备的物理层模型，探讨了信息系统故障对物理系统的影响。针对有源配电

网信息系统对物理系统影响特性的建模，建立了复杂的配电网信息系统与物理系统的联合模型，并对信息系统数据不完整、受攻击等条件下的物理系统状态估计结果进行了性分析。对配电网信息系统物理设备的运行状态进行了分类。同时，采用随机贝叶斯网络模型对配电网信息系统进行建模，分析了不同运行条件下信息系统对物理系统的影响特性。将配电网控制中心的运行过程分解为离散事件。首先分析了通信时延、恶意攻击等对调度中心运行过程的影响，然后分析了各类信息系统离散事件对物理系统运行特性的影响特性，并对各类离散事件发生时的关键指标进行了量化。综合以上研究现状可以看出，目前对配电网信息系统对物理系统影响特性的分析大多是将信息系统运行过程离散化，将物理系统运行过程等效为多个时间段，与信息系统进行联合仿真分析，尚无对物理系统运行状态离散化以及信息系统对物理系统控制过程关键指标进行相关的定量分析。

四、分布式信息物理系统抗扰动控制策略研究现状

信息物理攻击对关键基础设施的安全构成严重威胁，安全分析日益重要。目前主流的信息安全评估方法包括攻击树、攻击图、Petri网和博弈论。本文采用的方法包括攻击图和博弈论。攻击图从攻击者的视角，全面分析各种拓扑结构的配置以及脆弱性和潜在威胁之间的关系。王宇飞等改进了攻击图算法，使其适用于定量评估。刘建军将信息域和物理域抽象成一个整体结构，建立了Petri网模型和混合博弈模型，对信息物理攻击进行了量化。Zonouz等扩展了传统的攻击图，将其转化为隐马尔可夫模型，使得刻画所有可能的攻击路径成为可能，但未考虑攻击者的熟练程度对评估结果的影响。张建军等对攻击图算法进行了改进，使其能适用于定量评估。建立了贝叶斯攻击图来说明已知漏洞和零日漏洞情况下的攻击流程，计算网络漏洞的平均攻击时间，评估信息物理系统的可靠性。从以上分析可以看出，国内外在信息物理融合背景下的安全方面研究较多，但对攻击路径预测涉及较少。基于图的攻击路径分析可以描述多次攻击与攻击行为之间的因果关系，分析未知攻击和攻击者能力水平对后续攻击的影响。吴文博综合考虑漏洞固有特性和攻击者的能力，计算攻击成功概率，并根据主机重要性和漏洞利用模式计算攻击后果，该方法可以将信息域和物理域作为一个整体进行建模，考虑多次跨域攻击对系统风险的影响。 Liu通过构建信息物理依赖模型和概率矩阵分析资产间的依赖关系，进而引入安全指数量化信息物理系统的安全状态，设计信息物理安全评估算法计算指数值并发现潜在的威胁传播路径。近年来，基于最优化理论、马尔可夫决策过程（MDPs）和博弈论，研究了大量防御各类攻击的方法。Kim提出了一种基于最优化理论保护电网状态估计器的方法。攻击向量被认为是线性化的测量模型。本文证明了此类网络攻击可以在不被攻击的情况下，仅依靠少量的测量设备就能防御。将现有模型检测技术生成的电网攻击图解释为马尔可夫决策过程，并引入值迭代算法计算攻击成功概率。然而，这些研究忽略了攻击者的决策过程，大多数研究方案只能通过攻击行为的预期收益来优化防御者的行为。从以上分析可以看出，国内外在信息物理融合背景下的安全研究较多，但对攻击路径预测、防御资源分配等方面的涉及较少。从以上分析可以看出，当前电力信息物理系统安全分析方法存在一些问题：

（1）由于电力电网物理系统中信息域与物理域的深度融合，网络攻击不仅限于信息域，甚至可能通过信息域渗透到物理域，从而对其造成影响或破坏。现有的分析方法对于此类可渗透的跨域攻击仍然存在不足。

（2）目前的防御策略是在电力电网物理系统中实施的，不同的设备会设置防护措施相互隔离，通常无法直接攻击目标，需要利用设备上的漏洞作为桥梁来达到攻击目的。现有的针对此类多步骤攻击的分析方法存在各自的缺陷。此外，传统的攻击图方法无法准确反映攻击行为的复杂性对后续攻击路径的影响，从而导致攻击路径预测的准确性不高。

（3）信息物理协同攻击是攻击者为了以最小代价实现最大攻击效果而采取的攻击行为。针对此行为可以进行博弈分析，但现有的针对信息物理协同攻击的电力电网物理系统研究大多没有考虑到实际攻防态势中参与

者的自私行为，即有限理性行为，忽略此行为，对信息物理协同攻击的建模与分析就会偏离实际情况，导致所选防御策略的准确性和指导价值被削弱。

电网物理系统通过抽象信息、计算过程和物理组件，建立信息物理仿真融合系统，增加能量流与信息流之间的关联性，使信息系统与物理系统更好地协同工作。传统信息系统建模是被动地匹配物理系统建模，依赖于物理系统，两者之间良性影响较小，信息系统建模离不开物理系统建模。面向服务的电网物理系统架构可以灵活地接入模型对象和服务，建立信息过程与物理动态的融合模型，完整描述信息流与能量流的全局关系模型。本文分析了电网物理系统建模过程中面临的挑战，并给出了计算模型化、模块化、面向对象建模等解决方案。在分析电网物理系统建模方法时，提到了其层次化、时间并行化的特点，并指出其可以应用于分布式计算中广泛应用的混合系统模型的模块化结构。从状态机模型的角度详细介绍了电网物理系统建模和应用的基本步骤，并通过实例演示了该模型的控制效果，并提出了电网物理系统技术与电网的结合方案。采用面向对象建模建立形式相似的网格。组件模型和信息流模型可以将UML描述的信息模型与基于Matlab/Simulink的物理模型进行交互式仿真，可以验证仿真系统信息的缺失。从网络参数和服务参数两个方面进行了全面的分析，但未充分考虑信令长度、信道质量等参数的影响。将其应用于配电网自动化，在物理层和数据链路层给出了系统实现中部分网络组件的设计和改进，并指出在小规模配电网自动化系统中构建通信网络是一种经济可行的方法。采用配电网通信系统完成配电网的全部功能，为配电网中每台设备分配一个反映其位置信息的网络地址，配电网设备之间以数据报的形式进行通信，但未涉及数据链路层技术应用于配电网通信的问题。传统的变电站自动化和配电自动化依赖于专有通信网络，而基于通信的方法可以在单个网络中同时支持多种应用服务，并分析了技术在商业案例中应用的优势。分布式电源在控制与通信系统中的建模介绍了两者在分布式电源中的扩展。从控制和通信的角度描述了含分布式电源的配电网的运行和管理，并展示了如何通过应用案例，由控制中心协调各个分布式电源的输出，以最大限度地降低配电网的运行成本。

参考文献：

[1] 薛禹胜，余星火. 超越智能电网——能源未来的信息物理社会系统. IEEE论文集，2017，105(12)：2290-2292.

[2] 盛成宇，高海翔. 信息物理电力系统网络仿真综述与展望. 电网技术，2012，36(12)：100-105.

[3] 刘东，盛万兴. 电网信息物理系统关键技术及进展. 中国电机工程学报，2015，35(4)：3522-3531.

[4] 赵俊华，温福珍. 电力信息物理融合系统建模分析与控制研究框架. 电力系统自动化，2011，35(16)：1-8.