DOI：10.13334/j.0258-8013.pcsee.2016.06.003 文章编号：0258-8013 (2016) 06-1481-09 中图分类号：TM 76

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

郭庆来[1]，辛蜀骏[1]，孙宏斌[1]，王剑辉[2]

(1. 清华大学电机系电力系统国家重点实验室，北京市 海淀区 100084;
2.. 美国阿贡国家实验室，Argonne, IL 60439)

Power System Cyber-physical Modelling and Security Assessment: Motivation and Ideas

GUO Qinglai[1], XIN Shujun[1], SUN Hongbin[1], WANG Jianhui[2]

(1. State Key Lab of Power Systems, Department of Electrical Engineering, Tsinghua University, Haidian District, Beijing 100084, China; 2. Argonne National Laboratory, Argonne, IL 60439, U.S.)

ABSTRACT: Smart grid is a typical cyber-physical system (CPS), in which the disturbance on cyber part may result in the operation risks on physical systems. In order to perform system assessment and contingency analysis for the cyber-physical power grid, we first reviewed the significance and necessity of the CPS assessment for the power system, and proposed an analytic cyber-physical modeling architecture to describe the couple relationship of cyber and physical systems adopting graph theory, set theory and matrix theory afterwards. In this model, the HCS cyber network can be abstracted to a directed graph consisting of data nodes and directed branches. This model supports hybrid computing of the system information-energy flow with matrix transformation and operations, which has a higher computational efficacy while ensure some accuracy compared with simulation-based approaches. At last, we also explored the outlook of the future cyber-physical security assessment for the power system.

KEY WORDS: cyber-physical system，smart grid，energy internet，modeling，security assessment

摘要：智能电网与能源互联网都是典型的信息物理融合系统(cyber-physical system，CPS)，信息环节的可靠性问题可能导致物理系统的运行风险。为了对其系统及信息故障进行分析评估，文中在分析了对电力系统进行信息物理融合建模与评估的必要性去驱动力后，提出了一种 CPS 融合建模构想。该方法将 CPS 系统抽象为一个有向拓扑图，模型将物理系统和信息系统中的状态量统一抽象为“数据节点”，将信息处理、信息传输等环节抽象为“信息支路”。在此基础上，系统的信息-能量流可通过矩阵运算的方式快速简单地进行量化计算，与一般的迭代计算和仿真方法相比，该方法可有效提升计算速率。最后，对信息物理系统的综合安全评估技术体系进行了展望。

关键词：信息物理融合系统；智能电网；能源互联网；建模；安全评估

0 引言

信息-物理系统(cyber-physical system，CPS)是综合计算、网络和物理环境的多维复杂系统，通过3C(computing、communication、control)技术的有机融合与深度协作，实现大型工程系统的实时感知、动态控制和信息服务[1-4]。CPS 的概念最早由研究嵌入式系统的学者提出，近年来已经受到各个领域的广泛关注。2005 年 5 月，美国国会要求美国科学院评估美国的技术竞争力，并提出维持和提高这种竞争力的建议，最终于 2006 年 2 月发布的《美国竞争力计划》将 CPS 列为重要的研究项目。在中国，国家自然科学基金、科技部“973”和“863”计划均已将 CPS 列为重点资助领域。

信息物理耦合系统实现了网络化计算资源与物理世界间精密深层的结合。在电力系统中，嵌入式设备的应用、信息-物理系统间的模式选择与时序配置，以及面向海量信息的通信架构与信息集成都是实现全系统信息-物理耦合的关键技术，基于此我们可实现电力系统的信息-物理系统耦合与离散-连续过程的有机配合[1]。电力 CPS 有许多种表现形式，

基金项目：国家重点基础研究发展计划项目(973 项目)(2013CB228206)；国网科技项目“电网和通信网联合仿真技术基础研究”

The National Basic Research Program of China (973 Program) (2013CB228206); Project of State Grid Corporation of China: Research on the Key Technologies for Co-simulation of Power Grid and Communication Grid

其中一个典型的例子是控制中心应用，即一二次系统的相互耦合。电力系统及其控制系统共同构成了典型的信息物理系统，以能量管理系统(energy management system，EMS)为例，涵盖广域信息实时感知(RTU/PMU)、信息传输(电力载波/光纤网、各种规约形式)、信息处理(坏数据辨识/状态估计)、信息决策(潮流分析/安全分析/优化计算)、闭环控制(AGC/AVC)等，从空间上覆盖上千公里，从时间上涵盖毫秒到小时级，从目标上兼顾安全、优质和经济等多种要求。可以说，现代电力系统的正常运行无时无刻不依赖于一个可靠的信息系统(Cyber System)。

随着智能电网与能源互联网的发展，信息环节对物理系统的影响问题将更加突出。智能电网本身定位就是一个运行在先进 IT 技术之上的新型电网，其传感器数量、信息网络规模和决策单元数量都大大增加，而能源互联网的发展进一步将多种能流的物理系统与信息系统耦合在一起，并广泛深入到用户侧千家万户。

由于这种依赖性，信息系统的失效也将显著影响物理系统运行。美加 814 大停电是一个典型的例子，其发生的一个重要原因是状态估计功能退出运行，调度人员失去了对电网实时状态的感知能力，未能及时发现、评估和遏制故障蔓延。2001 年发生在美国 El Paso 电力公司的停电事故，起因也是通信的不正常延时造成的保护误动，切除了一条 345 kV 线路。2015 年末乌克兰电网遭受网络攻击，能量管理系统因此失效并导致最终供电中断，成为历史上首次由于信息攻击引发的大规模停电事故[0]。在我国电网的实际运行中，也曾经发生过多次由于信息环节的失效最终导致电网运行出现风险，比如某省由于北斗卫星信号故障，导致自动发电控制系统功能异常，引发了电网频率波动；再比如，由于维护人员建模时将控制点号映射到了错误开关，导致在进行电压控制时，一个控分低压电容器开关的遥控命令最终拉开了 220 kV 输电线路开关；等等。

信息系统的强大功能为电网运行提供了技术保障，但同时信息系统的失效所诱发的后果也将更加严重。因此，实现信息-物理系统的融合建模与综合安全评估，对当前电网的可靠运行与未来能源系统的架构设计都有着重要的指导意义。

自 CPS 概念提出以来，电力学术界已有很多学者尝试从这一角度对电力系统进行研究[6-28]。最初集中于电力信息系统的设计与分析，包括信息系统架构、建模与仿真等[6-12]。近年来，电力系统的信息安全成为一个热点研究问题。大量研究表明，通过人为注入坏数据攻击，能够在无法辨识的条件下导致控制中心决策错误，不仅可能干扰电网的安全运行，也可为攻击者带来非正当的利益[13-17]。基于这一问题，许多研究进一步分析了信息攻击对电网运行可能造成的影响以及应对措施[18-28]。

值得注意的是，智能电网或能源互联网作为典型的 CPS 系统，其信息系统与物理系统之间是相互耦合、相互影响的，故对其进行分析评估时，单独考虑一个系统是不全面的，必须计及物理系统和信息系统之间的耦合关系。但目前国内外研究大多还是将信息与物理系统分开处理，从 CPS 的整体视角进行建模与分析的研究较少，而且目前大都针对某个具体应用功能的分析(如状态估计、有功调度)，不具备通用性。如何能够构建信息-物理系统的整体模型，使用统一的计算框架对信息流与能量流之间的相互影响进行定量评估，这是一个非常迫切也极具挑战性的课题。

此外，尽管现今已有研究涉及电力信息系统的可靠性评估，但这些研究大多是借鉴传统的计算机网络分析方法完成的，更多的侧重于恶意攻击条件下的脆弱性分析。然而，实际电网运行时，信息系统更为频繁面临的是由于无意错误(比如运行人员建模失误、信息传输通道故障或延时、信息采集系统故障等)导致的功能失效，而这种信息环节的功能失效又会进一步诱发物理环节的运行风险，这是现阶段电网运行所无法回避的重要挑战。因此，类似于电网日常基于故障扫描的安全评估(Contingency Assessment)，我们也迫切需要提出一种信息故障评估(Cyber-Contingency Assessment)方法，从而定量分析评价由于信息环节故障可能导致的物理系统安全风险，而恶意攻击引发的信息安全问题可以看作一个信息故障的特例纳入该框架。

基于这一背景，本文以控制中心典型应用作为切入点，提出一种针对能量系统的信息能量融合建模方法与综合评估体系，并对关键技术研究方向进行展望。

1 CPS 融合建模与综合安全评估体系

如引言部分所述，电力系统由物理电网系统(一次系统)和控制系统(二次系统)两部分构成，分别对应 CPS 中的物理系统与信息系统。一些典型的电力信息系统有自动电压控制系统(automatic voltage

control， AVC)、自动发电控制系统(automatic generation control， AGC)等。实际运行时，电力信息系统对物理电网的状态进行量测，其量测结果即为电力信息系统的信息输入，该信息经电力信息系统内不同模块的传输、转换及处理后，最终转化为决策指令，反馈作用于物理系统。换言之，电力信息系统的控制指令决定物理电网的运行状态，而电网状态又将决定电力信息系统的信息输入，信息系统与物理系统的运行是强耦合的。当电力信息系统正常运行时，这一闭环的控制机制可保证物理电网的安全可靠地运行。然而，当电力信息系统出现信息故障，如信息传输发生中断或延时，则故障引起的信息错误很可能使电力信息系统做出错误的决策，从而影响物理电网的运行。

物理电力系统运行已经发展出完善的安全分析体系，基本思路是首先对物理电力系统进行建模，在此基础上以潮流计算/稳定计算/故障计算等为基础，研究在预想故障集(比如 N-1)下评估电力系统的各项安全指标。类似地，如果把物理电力系统推广到考虑信息网络部分的信息–物理系统，我们同样也需要对这样一个复杂系统进行建模，提出信息–物理混成计算的方法来定量分析二者之间的相互影响，并由此评估信息网络中的潜在扰动和故障(比如数据中断、数据篡改、数据延时)对物理系统运行所带来的潜在风险。

基于这一出发点，针对智能电网系统中物理–信息强耦合的特性，本文以电力系统控制中心应用为着眼点，对传统电网分析的概念和体系进行了进一步拓展，设计提出了涵盖建模–计算–评估的量化分析体系。传统电网分析方法与 CPS 方法的对比如图 1 所示。

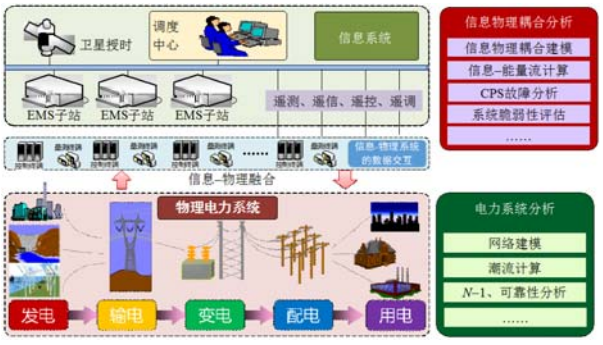

图 1　传统方法与电网 CPS 方法的对比

Fig. 1　Comparison between traditional assessment methods and CPS assessment methods for power systems

整个研究体系可包含以下四部分：1）信息物理系统融合建模方法；2）支持信息流-能量流混成计算的分析框架；3）信息物理系统信息故障分析与脆弱性评估的定量计算方法。作为对所包含的具体内容及相互关系如图 2 所示。

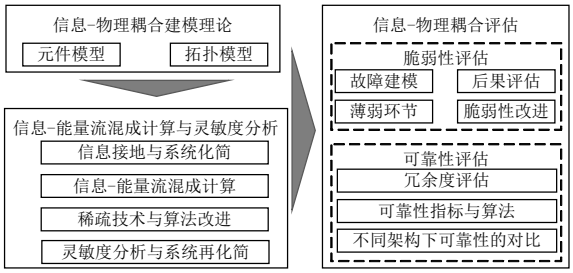

图 2　电网 CPS 分析评估体系

Fig. 2　Research architecture for power system's CPS analysis and assessment

2　电网信息物理融合建模方法

为量化分析电力系统信息故障的影响，就必须先对物理电网和电力信息系统进行统一的信息–物理耦合建模，进而在模型基础上对信息故障进行量化的分析和评估。

与电网类似，电力信息系统的特性也是由信息元件和系统拓扑共同决定的。构成信息系统的最基础元件是各种功能不一的信息模块，因而，信息模块的分类与建模将是未来进一步研究的基础。实际电力信息系统是包含海量信息元件与复杂通信规约的庞大系统，直接建模不但模型非常复杂，而且将显著影响运算效率。然而，尽管我们研究对象是一个信息-物理耦合系统，但是我们关心的重点仍然是物理侧电网的运行。因此，通过借鉴电力系统分析中“外网等值”的思想，站在物理系统的视角上，我们可以尝试建立一个复杂信息网络在物理系统侧的“等值模型”，从而降低模型的复杂度。研究中，我们将物理系统和信息系统中的状态量统一抽象为“数据节点”(data node)，而将信息处理、信息传输等信息环节抽象为“信息支路”(cyber branch)，其首末端节点分别为输入与输出数据，其支路特性方程为输入与输出之间的映射算子。因而，这里所提的元件特性，即为各信息支路内信息传输或转换的映射关系。为统一建模，研究中可将信息模块宏观地分为两个大类：信息传输模块与信息处理模块。这两类模块并不是相互独立，而是通过相互交换的信息紧密耦合。控制系统中，某些模块的数据输出将汇集为一个总的信息池，它将作为另一些模块的数据源。这类模块定义为“信息母线”模块。以上三类模块(信息传输、信息处理、信息母线)均可建模为从输入信息到输出信息的映射。建模

示意图如图 3 所示。

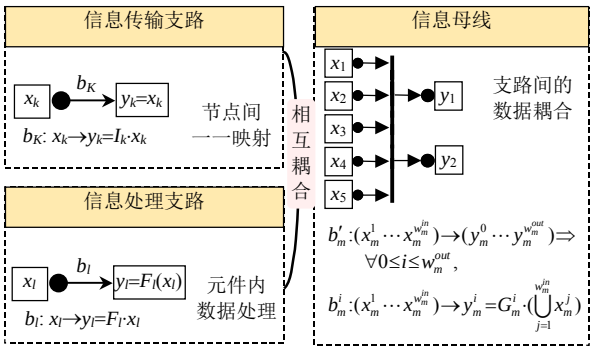

图 3 信息支路元件建模方法

Fig. 3 Modelling method for cyber branches

对应实际的控制中心应用，不同信息元件间的信息交互过程均被统一定义为信息传输。换言之，信息传输过程可以视为不同信息元件间的信息映射。例如，发电厂、变电站将采集到的实时信息通过各自的数据传输通路上传至控制中心，控制中心对各个物理设备下发对应的控制指令，都属于数据传输过程。值得注意的是，为了对系统进行统一的物理信息建模，本文定义的信息传输功能不仅包含了传统的信息上传与指令下发，还可广义包含了物理系统与信息系统间的信息交互，例如状态量测与实际控制，具体模型参见下一章中对全系统信息–能量流的求解。

与信息传输相对，信息处理过程只在某个信息元件内执行。通过计算、优化等过程，信息处理模块的输入数据可转化为相应的结果并予以输出。在电力系统中，一些典型的数据处理模块包括状态估计、无功–电压优化计算(AVC)、发电调度计算(AGC)等。

而与前两类与实际模块对应的支路类型不同，信息母线模块是一个虚拟的信息模块，存在于信息传输支路与信息处理支路的接口位置，在实际系统中并不对应任何信息功能。但其为前两类模块提供了数据接口，从而使各模块通过信息交互相互耦合，形成一个完整的信息网。例如，变电站内的所有量测结果会在站级控制中心进行整合，而其中只有一部分数据会上传至总控制中心。这一过程可能存在信息的冗余与损失，在计算中有化简的空间，具体策略参见第 3 节。

在独立模块的基础上，各类信息元件只有通过一定的规律连接在一起，才能使系统正常运转，这种连接关系即被定义为系统拓扑。借助电网建模思路，结合信息网的特性，我们可用有向拓扑图对各信息元件的连接关系进行描述，进一步将其等价转换为节点-支路关联矩阵。

对某个控制系统，若其信息网络包含 N 个信息节点($D_1 \cdots D_N$)，K 条信息传输支路($b_1 \cdots b_K$)、L 条信息处理支路($b_{K+1} \cdots b_{K+L}$)和 M 条 MISO 信息池支路($b_{K+L+1} \cdots b_{K+L+M}$)，则节-支关联矩阵 $\boldsymbol{A}$ 的阶数应为 $N\times(K+L+M)$。$\boldsymbol{A}$ 中元素定义如下：

$$a_{i,j}=\begin{cases}1, & D_i\text{为支路}b_j\text{的尾点}\\ -1, & D_i\text{为支路}b_j\text{的头点}\\ 0, & \text{其他}\end{cases} \tag{1}$$

按此定义，矩阵 $\boldsymbol{A}$ 的结构为：

$$\boldsymbol{A}=\begin{array}{c} \\ 1 \\ \vdots \\ i_1 \\ \vdots \\ j_1 \\ \vdots \\ i_2 \\ \vdots \\ j_2 \\ \vdots \\ N\end{array}\begin{array}{c}\begin{array}{cccccccc}1 & \cdots & k & \cdots & K+L & \cdots & K+L+m & \cdots & K+L+M\end{array}\\ \begin{bmatrix} 0 & & 0 \\ \vdots & & \vdots \\ 1 & & \\ \vdots & & 1 \\ -1 & & \\ & & \vdots \\ & & 1 \\ \vdots & & \vdots \\ & & -1 \\ & & \vdots \\ 0 & & 0 \end{bmatrix}\end{array} \tag{2}$$

具体的建模方法可参考文献[29]。

3 电网信息–能量流混成计算方法

电力系统运行时，其物理电网的能量流分布决定了物理系统的运行状态。当引入信息系统(控制中心应用)后，各量测终端将一些选取的物理状态量转化为对应的虚拟信号，二次侧的信息系统基于这些信息，经过多级传输、转换、计算后，生成最终的控制信号，系统控制终端则将其转化为物理状态的改变(例如开关的投切、负荷的变化等)，从而影响物理电网的能量流分布，继而产生新的运行状态。因而，从 CPS 角度，控制中心应用与物理电网的交互过程的可以视为一种“物理–信息–物理”的过程，示意图如图 5 所示。

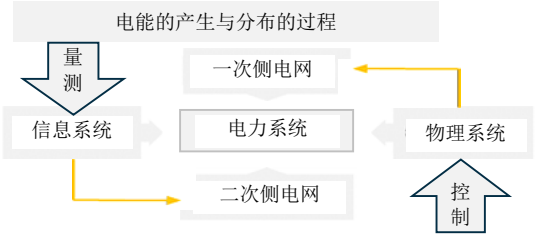

图 4 考虑控制中心应用的电力系统信息–物理耦合机制

Fig. 4 Cyber-physical cooperation of power system considering control center applications

而信息系统对物理电网的影响可视为通过信

息流实现的。因而，要分析系统的信息-物理耦合特性，其核心就是讨论信息流与物理能量流的交互作用，即对全系统的信息–能量流分布进行混成求解。

信息–物理耦合电力系统的信息–能量流混成模型如图 5 所示，其应当包含以下四个部分：

1）能量流计算模型。

能量流分布即为物理电网潮流分布，描述方程如下：

$$f(\boldsymbol{x}(N+1),\boldsymbol{u}(N),\boldsymbol{D}(N+1),\boldsymbol{p},\boldsymbol{A})=0 \tag{3}$$

式中，$\boldsymbol{A}$ 为网络结构变量，由系统各元件连接方式以及开关的状态共同决定；$\boldsymbol{p}$ 为网络元件参数，一般不可调整；$\boldsymbol{D}$ 为不可控变量或干扰变量，由用户需求所决定，一般不可控制；$\boldsymbol{u}$ 为控制变量，即系统的可调变量；$\boldsymbol{x}$ 为依从变量；N 为时标，对应系统的各个控制周期。

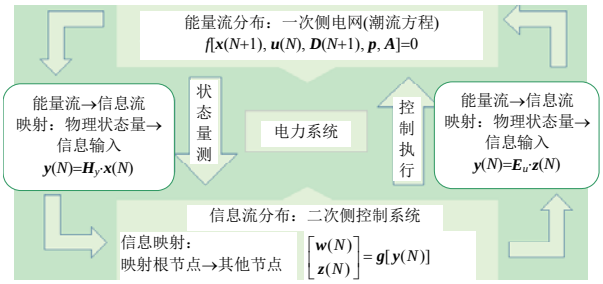

图 5　全系统信息-能量流混成模型

Fig. 5　Information-energy flow model of a cyber-physical power system

2）能量流→信息流。

该环节实现了物理状态到虚拟信号的转换，对应实际系统中的状态感知环节，即从依从变量 $\boldsymbol{x}$ 中，根据控制需求对相应的量进行量测，转换成虚拟信号，作为未来信息系统的信息源，记为 $\boldsymbol{y}=[y_1\ldots y_m]^{\mathrm{T}}$。该过程可描述为：

$$\boldsymbol{y}(N)=H_y\cdot\boldsymbol{x}(N) \tag{4}$$

3）信息流计算模型。

信息流分布描述了二次侧信息系统的运行状态。如在我们建立的有向信息流模型中，信息流由网络根节点(即量测的状态量)，经不同模块的信息映射(信息传输、信息处理、信息池)，最终流到网络的叶节点(即最终输出的控制信号)。因此，系统中的信息流可以视为由根节点 $\boldsymbol{y}$ 至其他节点的信息映射。记系统末端叶节点及其他节点的信息分别为 $\boldsymbol{z}=[z_1\ldots z_n]^{\mathrm{T}}$ 和 $\boldsymbol{w}=[w_1\ldots w_l]^{\mathrm{T}}$，统信息流模型可表示为：

$$\begin{bmatrix}\boldsymbol{w}(N)\\ \boldsymbol{z}(N)\end{bmatrix}=g(\boldsymbol{y}(N)) \tag{5}$$

4）信息流→能量流。

该环节对应实际系统的控制环节，即将信息网络各叶节点信息 $\boldsymbol{z}$ 映射为实际的控制量 $\boldsymbol{u}$，可描述为

$$\boldsymbol{u}(N)=\boldsymbol{E}_u\cdot\boldsymbol{z}(N) \tag{6}$$

电网的能量流分布可通过潮流模型进行快速求解，而信息流与能量流间的相互转换一般可描述为线性映射，求解难度也不大。但电网 CPS 系统的信息流，对应的是信息系统内部的各模块间信息传输、筛选、转换等过程，所包括环节较多，映射函数多样，求解难度较大。此外值得注意的是，与物理电网能量的瞬时平衡不同，电力信息系统中各元件的运行是有序的，一些模块的输入将依赖另一些模块的输出。例如，下级变电站必须先获取本地的 SCADA 量测信号，才能将其上传至主站供下一步决策。因此，进行全系统信息-能量流求解时，必须考虑其时序特性。但时序模型并不适用于代数求解，为解决这一问题，可利用信息网络的有向性和线性叠加特性，参照辐射状配电网的潮流求解方法，设计出兼顾准确性与计算效率的信息-能量流的混成求解方法。

在实际控制系统中，大部分信息并未参与最终的控制决策，很多信息数据在汇集入信息母线后，甚至不会再出现在下一步的信息流。例如，变电站综自系统会整合站内的全部量测结果，但只选出一部分进行上传(比如所有母线电压量测中可能只上传 AB 线电压到控制中心)，上层控制中心将只基于这部分数据进行决策，其他量测数据不是控制中心决策所必须的，即为冗余数据。如果无差别的将这部分信息引入，将极大地增加系统信息流的计算量。因而，我们在信息流图中采用“信息接地”的概念，在保证完整性的基础上，将冗余信息进行剔除，从而在不改变系统信息流的基础上降低运算复杂性[29]。

在已有的物理信息网络模型中，为保证网络的完整性，我们引入一个虚拟的信息接地节点(cyber ground node，CGND)，该节点的数据定义为所有冗余数据的并集。依照该定义，该节点与可视为通过一个虚拟的信息母线支路与其他节点相连，该支路定义为信息接地支路，用符号 b_{CG} 表示。设支路 b_{CG} 包含 w_{CG} 个尾点，其数据分别用 $x_{\mathrm{CG}}^1\cdots x_{\mathrm{CG}}^{w_{\mathrm{CG}}}$ 表示，而支路的头点，即系统信息接地节点，其数据用 y_{CG} 表示，则该支路可建模为如下表达式：

$$b_{\mathrm{CG}}:(x_{\mathrm{CG}}^{1}\cdots x_{\mathrm{CG}}^{w_{\mathrm{CG}}})\rightarrow y_{\mathrm{CG}}=\bigcup_{i=1}^{w_{\mathrm{CG}}}x_{\mathrm{CG}}^{i} \tag{7}$$

引入信息接地节点和支路后，原有的网络节-支关联矩阵 $\boldsymbol{A}$ 的行数和列数都增加了 1。定义该矩阵为扩展节–支关联矩阵，用符号 $\boldsymbol{A}'$表示，矩阵元素的定义见下：

$$\boldsymbol{A}'=\begin{bmatrix}\boldsymbol{A} & A_{\mathrm{CG}}\\ 0 & -1\end{bmatrix} \tag{8}$$

在引入接地节点和支路后，原有节点与支路的关联关系并不发生变化，故$\boldsymbol{A}'$的左上角矩阵即为$\boldsymbol{A}$。矩阵 $\boldsymbol{A}'$的最后一行代表接地节点与支路的连接关系。因冗余数据不再参与信息流，该节点没有任何出支路，因此该行只有第 $K+L+M+1$ 个元素为–1，不包含任何+1。而矩阵 $\boldsymbol{A}'$的最后一列代表信息接地支路与各数据节点的映射关系，故列向量 A_{CG} 中，只有与冗余数据节点对应的元素为+1，其余元素均为 0。

扩展节–支关联矩阵 $\boldsymbol{A}'$中，一些行只含有元素+1，不含元素–1，这些行代表的数据点为网络的根节点，可视为信息系统的数据源，如 AVC 系统的物理测点；而另一些行只含一个元素–1，其余元素均为 0，这些行代表的数据点除接地节点外为信息网络的叶节点，均代表对物理系统的最终控制指令。

生成 $\boldsymbol{A}'$矩阵后，我们可对 A_{CG} 中非零元素所在的行进行化简，使一般支路与接地支路的信息并集为 0，在不改变系统信息流的基础上将冗余信息进行剔除。简化思路如图 6、7 所示。

经过化简，系统信息–能量流的计算复杂度可显著降低，而保证二者的耦合关系没有任何损失。化简后的系统与原系统的信息–能量流分布完全一致。

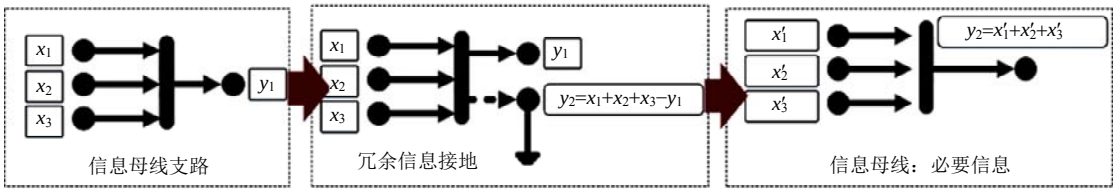

图 6 信息接地与元件模型化简

Fig. 6 Cyber-grounded and branch simplification

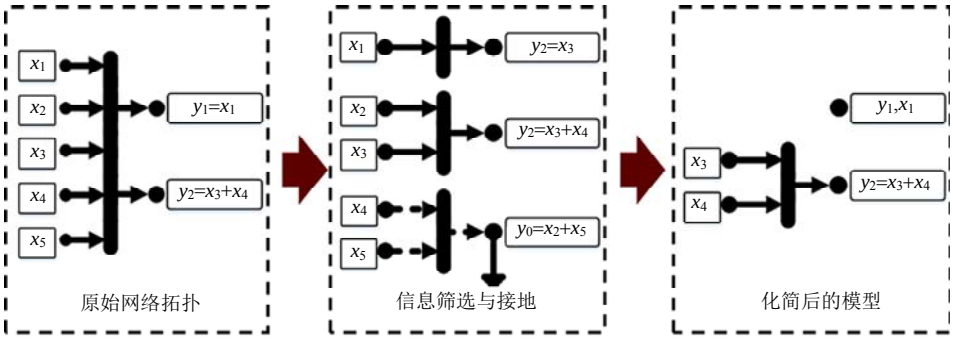

图 7 拓扑化简

Fig. 7 Cyber-grounded and topology simplification

4 信息物理融合系统的综合安全评估

电力系统的脆弱性可以通过 N–1 方法进行评估，即对所有可能发生的支路物理故障进行扫描，并分析各故障对应的系统响应。而该思路可同样应用于信息故障与脆弱性分析。在信息系统中，信息故障可能导致系统生成不当的控制指令，从而影响物理系统。通过对比有无故障情况下的系统运行或安全指标，故障的严重性和系统的脆弱性可得到有效评估。

4.1 信息故障建模

上节已经详细给出了已知全系统信息–物理耦合模型的情况下如何进行信息–物理混成计算。因此，系统的 N–1 分析和可靠性/脆弱性评估，只需扫描故障集，求解各故障下的系统状态即可。信息系统的特性由信息支路模型与系统拓扑共同决定，因此，基于其对信息网络的影响，信息故障(Cyber Contingency)可分为两类：拓扑故障和支路故障。无论是信息攻击还是无意(偶发)错误，信息故障都主要集中于信息传输支路中。若各信息处理模块的算法都经过准确校验，影响其正常运行的原因只可能是错误的信息输入导致了错误的信息输出，而这类故障也可统一归结为其输入支路的信息故障。因此，信息传输支路的故障的分析与建模是我们研究的重点。

4.1.1　拓扑故障

拓扑故障可影响或中断某条或多条信道的数据传输。例如，受物理信道中断的影响，控制中心与下级某变电站完全失去通讯。若此类故障发生，在系统模型中，某些数据节点的连接关系会发生改变。因此，该故障的量化建模对应着系统节–支关联矩阵的修正。基于已有的运行记录，在电网系统中最常出现的拓扑故障为信道中断与信道错位其具体模型论述如下：

1）信道中断。

信道中断故障将阻碍某信息传输模块的数据传输。在实际系统中，该故障可能由多种原因造成，例如物理信道故障、人为恶意中断等。在 CPS 模型中，该故障将导致对应支路的头点与尾点失去映射关系，即将该支路彻底移除，对应节–支关联矩阵 $\boldsymbol{A}$ 的修正即为移除非零元素。

2）信道错位。

信道错误故障将导致某些信道的数据映射发生偏移。例如，控制中心在下发功率调节指令至某发电机时，可能将其他发电机的调节指令错误地下发到了这台发电机。对应到 CPS 模型中，该故障将导致一些支路的尾点发生变化，即修改节–支关联矩阵 $\boldsymbol{A}$ 对应列向量的+1 元素的位置。

4.1.2　支路故障

与拓扑故障不同，支路故障并不改变系统节点与支路的拓扑连接关系，而只改变故障支路内部的数据映射。换言之，在数据传输之路中，支路故障将改变原有的一一映射关系，使之出现偏差。电力系统中最常出现的支路故障有以下四种：传输错误、传输延时、传输中断与传输错位。以下将分别对其数学模型进行论述：

1）传输错误。

该故障发生时，故障支路的部分输出数据与输入数据可能存在偏差。引起这类故障的原因可能有多种，可能是固有的系统量测误差、转换精度差异，也可能是人为的恶意更改。该故障将在原有支路映射函数上叠加误差量。

2）传输延迟。

传输延迟是实际现场最常出现的故障之一。顾名思义，该故障将导致某些数据的传输出现延时。因此，传输延迟故障将原有的非事件相关模型修正为时间相关模型。对信息传输支路 b_k，若数据 x_k' 的传输发生Δt 的延时，则支路映射模型需叠加 Δt 的映射算子。

3）传输中断。

传输中断故障将阻碍一些信息的传输。与信道中断故障不同，该故障并不会导致系统拓扑的改变，只会对信道内部的一些数据映射产生影响。例如，AVC 系统中，下级子站上传至控制中心的电压信号可能中断，从而影响上级中心的决策。该故障发生后，信息支路尾点的一些数据将无法继续更新。对信息传输支路 b_k，若数据 x_k' 的传输在 t_0 时刻发生中断，则支路映射矩阵中，需将该数据对应的非零元修正为 0。

4）传输错位。

对某个传输信道，传输错位故障定义为该信道内的一些数据映射出现偏差，从而偏离原有的一一映射关系。例如，控制中心进行远控时，对某一开关的控制信号可能错误地下发到了另一个开关上，进而造成故障。在信息模型中，该故障将导致信息传输映射矩阵 I_k 中，原本都应在对角线的非零元，分布在非对角线的位置上。

上述拓扑故障与信息故障的具体数学模型表达形式可参考文献[29]。

4.2　灵敏度分析与信息物理耦合安全评估

由故障分析结果可知，不同信息、不同信道所发生的不同类型的故障对物理电网的影响方式和后果都不相同。因此，与传统信息网分析不同，电网信息系统的可靠性评估不但需要考虑网络信道的可靠性，也需要考虑各信息对于物理系统的影响。思路如图 8 所示。

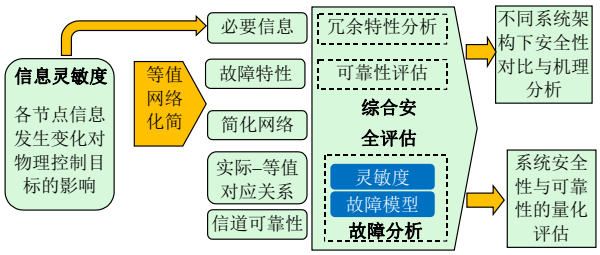

图 8　系统综合安全评估的思路与方法

Fig. 8　Cyber-physical security assessment

灵敏度的定义是当某个量发生变化时，对其他量的影响大小。例如，电力系统中，无功–电压灵敏度指的是当某节点无功输出发生变化时，对系统其他节点电压的影响。该指标广泛应用于电网的脆弱性评估以及电压控制中。

如前文所述，信息系统的故障将对物理电网的运行造成影响。为量化评估这种影响的大小，定位信息系统中关键元件与脆弱环节，我们参照物理电网中灵敏度的概念，提出了信息–物理耦合灵敏度。

该指标包含两重含义：

1）某信息量对物理电网运行的贡献大小；

2）该信息量发生故障时，对物理系统影响的严重性。

基于上文提出的信息–能量流混成计算模型，信息–物理耦合灵敏度可利用下式进行计算：

$$\text{CPS灵敏度}=\frac{\partial\text{状态量}}{\partial\text{控制量}}\cdot\frac{\partial\text{状态量}}{\partial\text{控制信号}}\cdot\frac{\partial\text{控制信号}}{\partial\text{信息}}$$

式中，上式第一项为物理灵敏度，第二项可通过信息→能量计算模型直接获得。而第三部分指的是信息网中某信息量对叶节点信息的影响，该值可利用切割等值的方式进行求解，求解示意图如图 9 所示。

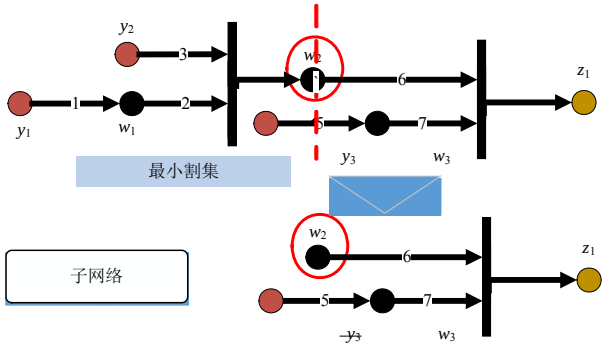

图 9 灵敏度求解

Fig. 9 Cyber-physical sensitivity computation

如图 9 所示，若需求解信息量 w_2 对输出信号 z_1 的影响，只需对原系统进行切割等值(等值子网络如图下半部分所示)，然后利用所提公式求解新网络中根节点对叶节点的贡献即可。

借助求解出的信息灵敏度数值，利用已有的网络模型和信道可靠性指标参数可进行可靠性分析：首先，利用信息灵敏度和支路可靠性数值，计算系统信息故障影响的期望值，以表征电力信息系统的安全可靠性。计算过程中，应当考虑故障发生的概率，故障对信息量的影响，以及该信息量的灵敏度；其次，对系统进行冗余分析，探讨额外信息与支路(包括信息校验与历史信息比对)的引入对信息流模型的修正，量化评估该环节引入对系统可靠性的提高，进而进一步进行优化。

6 结论与展望

本文构建的信息-物理系统分析的基础分析框架，可以看作将现有电力系统分析的理论框架推广到更为复杂的信息-物理系统的一次尝试。基于这一体系，未来可以进一步研究信息–物理系统的运行优化和稳定性评估等关键问题，比如将已有硬件条件及系统需求作为约束条件(如传输带宽、服务器空间、服务器计算能力、传输延时要求等)，在满足以上条件的基础上，尽可能高地提升系统的信息冗余度与信息可靠性，实现对电力信息系统架构的优化设计与信息流的优化配置，从而为未来电网控制中心应用的架构设计提供理论基础和量化分析工具。

参考文献

[1] 刘东，盛万兴，王云，等. 电网信息物理系统的关键技术及其进展[J]. 中国电机工程学报，2015，35(14)：3522-3531.
Liu Dong，Sheng Wanxing，Wang Yun，et al. Key technologies and trends of cyber physical system for power grid[J]. Proceedings of the CSEE，2015，35(14)：3522-3531(in Chinese).

[2] 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).

[3] 曹军威，万宇鑫，涂国煜，等. 智能电网信息系统体系结构研究[J]. 计算机学报，2013，36(1)：143-167.
Cao Junwei，Wan Yuxin，Tu Guoyu，et al. Information system architecture for smart grids[J]. Chinese Journal of Computers，2013，36(1)：143-167(in Chinese).

[4] 赵俊华，文福拴，薛禹胜，等. 电力信息物理融合系统的建模分析与控制研究框架[J]. 电力系统自动化，2011，35(16)：1-8.
Zhao Junhua，Wen Fushuan，Xue Yusheng，et al. Modeling analysis and control research framework of cyber physical power systems[J]. Automation of Electric Power Systems，2011，35(16)：1-8(in Chinese).

[5] 郭庆来，辛蜀骏，王剑辉，等. 由乌克兰停电事件看信息能源系统综合安全评估[J/OL]. 电力系统自动化，2016，40(5): 1-3.
Guo Qinglai，Xin Shujun，Wang Jianhui，et al. Comprehensive security assessment for a cyber physical energy system：a lesson from Ukraine's blackout [J/OL]. Automation of Electric Power Systems，2016，40(5): 1-3 (in Chinese).

[6] Karnouskos S. Cyber-physical systems in the Smart Grid [C]//Proceedings of the 2011 9th IEEE International Conference on Industrial Informatics (INDIN). Caparica，Lisbon：IEEE，2011：20-23.

[7] Lee E A. Cyber physical systems：design challenges[C]// Proceedings of the 2008 11th IEEE International Symposium on Object Oriented Real-Time Distributed Computing (ISORC). Orlando，FL：IEEE，2008：363-369.

[8] Wan Y X，Cao J W，Zhang S，et al. An integrated cyber-physical simulation environment for smart grid

applications[J]. Tsinghua Science and Technology，2014，19(2)：133-143.

[9] Palensky P，Widl E，Elsheikh A. Simulating cyber-physical energy systems：challenges，tools and methods[J]. IEEE Transactions on Systems，Man，and Cybernetics：Systems，2014，44(3)：318-326.

[10] Hua L，Sambamoorthy S，Shukla S，et al. Power system and communication network co-simulation for smart grid applications[C]//Proceedings of the 2011 IEEE PES Innovative Smart Grid Technologies (ISGT). Hilton，Anaheim，CA：IEEE，2011：1-6.

[11] Li H S，Liu L F，Poor H V. Multicast Routing for Decentralized Control of Cyber Physical Systems with an Application in Smart Grid[J]. IEEE Journal on Selected Areas in Communications，2012，30(6)：1097-1107.

[12] Ilic M D，Xie L，Khan U A，et al. Modeling of future cyber-physical energy systems for distributed sensing and control[J]. IEEE Transactions on Systems，Man，and Cybernetics-Part A：Systems and Humans，2010，40(4)：825-838.

[13] Kosut O，Jia L，Thomas R J，et al. Malicious data attacks on the smart grid[J]. IEEE Transactions on Smart Grid，2011，2(4)：645-658.

[14] Kim J，Tong L. On Topology attack of a smart grid：undetectable attacks and countermeasures[J]. IEEE Journal on Selected Areas in Communications，2013，31(7)：1294-1305.

[15] Liu S，Chen B，Zourntos T，et al. A coordinated multi-switch attack for cascading failures in smart grid[J]. IEEE Transactions on Smart Grid，2014，5(3)：1183-1195.

[16] Liu S，Mashayekh S，Kundur D，et al. A framework for modeling cyber-physical switching attacks in smart grid[J]. IEEE Transactions on Emerging Topics in Computing，2013，1(2)：273-285.

[17] Choi D H，Xie L. Ramp-induced data attacks on look-ahead dispatch in real-time power markets[J]. IEEE Transactions on Smart Grid，2013，4(3)：1235-1243.

[18] Zhang Y C，Wang L F，Sun W Q. Trust system design optimization in smart grid network infrastructure[J]. IEEE Transactions on Smart Grid，2013，4(1)：184-195.

[19] 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.

[20] McDaniel P，McLaughlin S. Security and privacy challenges in the smart grid[J]. IEEE Security & Privacy，2009，7(3)：75-77.

[21] Ten C W，Liu C C，Manimaran G. Vulnerability assessment of cybersecurity for SCADA systems[J]. IEEE Transactions on Power Systems，2008，23(4)：1836-1846.

[22] Mo Y，Kim T H J，Brancik K，et al. Cyber-physical security of a smart grid infrastructure[J]. Proceedings of the IEEE，2012，100(1)：195-209.

[23] Zonouz S，Davis C M，Davis K R，et al. SOCCA：a security-oriented cyber-physical contingency analysis in power infrastructures[J]. IEEE Transactions on Smart Grid，2014，5(1)：3-13.

[24] Ten C W，Manimaran G，Liu C C. Cybersecurity for critical infrastructures：attack and defense modeling[J]. IEEE Transactions on Systems，Man，and Cybernetics，Part A：Systems and Humans，2010，40(4)：853-865.

[25] Liu N，Zhang J H，Zhang H，et al. Security assessment for communication networks of power control systems using attack graph and MCDM[J]. IEEE Transactions on Power Delivery，2010，25(3)：1492-1500.

[26] Hahn A，Govindarasu M. Cyber attack exposure evaluation framework for the smart grid[J]. IEEE Transactions on Smart Grid，2011，2(4)：835-843.

[27] 叶夏明，赵俊华，文福拴. 基于邻接矩阵的电力信息系统脆弱性定量评估[J]. 电力系统自动化，2013 37(22)：41-46.
Ye Xiaming，Zhao Junhua，Wen Fushuan. Quantitative vulnerability assessment for power information system based on adjacency matrix[J]. Automation of Electric Power Systems，2013，37(22)：41-46(in Chinese).

[28] Hopkinson K，Wang X R，Giovanini R，et al. EPOCHS：a platform for agent-based electric power and communication simulation built from commercial off-the-shelf components[J]. IEEE Transactions on Power Systems，2006，21(2)：548-558

[29] Xin S J，Guo Q L，Sun H B，et al. Cyber-physical modeling and cyber-contingency assessment of hierarchical control systems[J]. IEEE Transactions on Smart Grid，2015，6(5)：2375-2385.

郭庆来

收稿日期：2016-02-05。

作者简介：

郭庆来(1979)，男，博士，副教授，博士生导师，IEEE Senior Member，主要从事电网能量管理技术、电压稳定与电压控制、信息物理系统(CPS)、电动汽车等领域的研究，guoqinglai@tsinghua.edu.cn；

辛蜀骏(1990)，男，博士研究生，主要研究方向为电力系统信息–物理耦合分析与故障评估、电动汽车优化充电，woshipure1@gmail.com。

(责任编辑　乔宝榆)