DOI：10.16516/j.gedi.issn2095-8676.2022.04.001
OA：https://www.energychina.press/

# 电力系统安全稳定校验的信息物理联合仿真方法

杨至元[1,✉]，张仕鹏[2]，孙浩[2]
（1. 西安交通大学 智能网络与网络安全教育部重点实验室，陕西 西安，710049；
2. 中国能源建设集团广东省电力设计研究院有限公司，广东 广州，510663）

**摘要：**[目的]为深入探究电力信息系统故障在信息物理融合系统（CPS）中对工程物理安全的影响机制，并确保研究结果易于复现和推广，[方法]通过开源软件搭建了电力变电站信息物理联合仿真的轻量级测试平台。基于电力监控系统的拓扑结构，通过 Mininet 搭建了变电站过程层网络的虚拟化框架，并在虚拟主机中调用 Scapy 模块自定义通信系统的故障类型，根据信息系统仿真结果修改安稳分析程序 PSD-BPA 的计算文件，外部调用暂稳计算核心求解工程安全结果，实现 Mininet 与 BPA 之间的数据联动，得到电力 CPS 轻量级联合仿真平台。[结果]仿真结果显示：变电站过程层网络中约 64% 的链路时延增加了 10 倍或以上，保护设备动作时间延缓至少 12 周波。根据文中提出的暂态稳定指标，部分站点在仿真周期内出现了严重的失步运行故障。[结论]基于暂态稳定指标的筛选结果成功量化了安稳控制设备的信息故障对电力能源系统的影响。

**关键词：**电力信息物理融合系统；Mininet-BPA 测试平台；电力系统网络安全；电力系统稳定校验计算；级联故障分析
**中图分类号：**TK91；TP393.08　**文献标志码：**A　**文章编号：**2095-8676(2022)04-0001-10
**开放科学 (资源服务) 二维码：**

# Cyber-Physical Coordinated Assessments with Incorporations of Transient Stability Analysis

YANG Zhiyuan[1,✉]，ZHANG Shipeng[2]，SUN Hao[2]
（1. Ministry of Education Key Lab for Intelligent Networks and Network Security, Xi'an Jiaotong University, Xi'an 710049, Shanxi, China；2. China Energy Engineering Group Guangdong Electric Power Design Institute Co., Ltd., Guangzhou 510663, Guangdong, China）

**Abstract:** [**Introduction**] To further explore the potential influence of malfunctions in the information network on the power operation systems and assure that the results are replicable and acceptable, [**Method**] the research established a lightweight co-simulation measure of the cyber-physical system in power substations based on the open-source environments. According to the topology of the power monitoring system, a virtualization framework of substation process level through Mininet was firstly built, and, in virtual hosts, the models from Scapy were imported to define the malfunctions in the communication system. Then, the calculation functions were modified automatically based on the simulation results from the Mininet-based virtualization framework. Finally, the stable/transient computing cores of PSD-BPA were externally called to produce stability results, and the lightweight CPS co-simulation platform was eventually obtained. [**Result**] The simulation results suggest that the time delay of around 64% of links is increased more than 10 times and the operation time of the protective relay is postponed at least 12 cycles. According to the transient-stability-based index proposed in the research, multiple substations will engage serious out-of-step failures during the calculation period. [**Conclusion**] The impacts of malfunctions of the information network on the power energy system are quantified based on the screening results using the proposed transient-stability-based index.

**Key words:** power cyber-physical system (CPS); Mininet-BPA co-simulation testbed; power system cybersecurity; power system stability analysis; cascading failures

**收稿日期：**2021-06-11　**修回日期：**2022-02-19
**基金项目：**中国能建广东院科技项目“基于信息物理融合系统的网络安全的电力系统运行风险评估”（EV05391W）

## 0 引言

随着能源互联网建设和电网数字化转型加快，电力信息物理融合系统（CPS）正加速电力运行调度网、全域安全防护网和用户终端数据网之间的协同互动，促进建设以“电力大数据服务公共社会管理和经济发展”为目标的新型数字产业，发展以高比例分布式能源为主体的现代化综合能源系统[1-2]。作为关键支撑技术，自 2006 年首次由美国国家科学院提出以来，CPS 的安全性定义和研究边界一直存在分歧。一般而言，电力 CPS 的安全问题是包含通信控制安全和工程运行安全的综合安全问题[3]，其研究本质是基于通用的数学模型描述信息系统的通道中断、信息错位、延迟以及错误等故障，在通信智能化技术高度集中的 CPS 模型中，对物理侧能源系统的工控可靠性影响[4]。

国内外电力 CPS 安全研究学者在信息安全脆弱性分析[5]，基于网络攻击事件的电力运行故障分析[6]，电力 CPS 离散事件的控制建模[7]，电力 CPS 的半实物仿真[8] 等领域开展了大量研究并取得多项成果。但上述部分研究的重点大都落在信息侧或物理侧的单边安全问题上，未能提出改善 CPS 综合安全性的量化方案，其中部分结果缺少电力工程安全环境的计算校验，安全结论还需验证[9]。电力 CPS 的安全问题本质可类比“木桶理论”，其上限应由整体系统的安全短板决定，即需要考虑信息物理双重脆弱性的协同作用[6]。CPS 环境中任何信息安全漏洞或工程设计缺陷都有可能被恶意利用，其危害会被放大，直接影响到电力系统综合安全。筛选信息安全事件及其潜在诱发的工程安全事件，有助于快速定位 CPS 系统内部的安全“短板”，帮助安全研究人员在规划设计阶段提前做好预案[10]。

为了更好解决电力 CPS 综合安全问题，学者前期工作[10-11] 介绍了基于电力监控系统搭建入侵攻击模型，给出潜在入侵风险的概率建模，并根据变电站中断故障响应给出基于稳态潮流分析的全枚举方案。但上述工作缺少 CPS 联合仿真模型校验，缺少信息安全事件对工程物理安全的直接表征。Liu 在 CPS 融合仿真测试中明确了中间人攻击（MIM）、拒绝服务攻击（DoS）等网络攻击诱发的非传统电力工程故障的复杂特性[12]，在此基础上，学者基于 RTDS 搭建了广域测量网络（WAMS）架构的半实物仿真系统，将控制设备和测量装置的通讯协议整合到仿真系统中，指出基于 CPS 模型的控制理论可有效限制电力系统级联故障[13-14]。上述研究采用的 OPNET 和 RTDS/RT-LAB 混合仿真平台可以实现多组高度复杂模型的实时动态仿真[15]，为相关理论及应用提供了坚实的技术支撑，但由于其投资成本高，开发周期长，不支持后期开发，目前暂未普及[16-17]。

为提高仿真平台的适用性和可拓展性，学者基于软件定义网络（SDN）理论，将电力控制采集元件抽象为独立单元，自定义攻击场景，验证了 IEC 61850 协议的网络攻击特征[18]。为保证研究结果易于复现，安全结论便于推广，文章通过开源软件搭建了电力变电站 CPS 联合仿真的初级测试平台，主要贡献包括：（1）基于实际工程的变电站监控系统工程接线，通过网络拓扑仿真器 Mininet 搭建了变电站过程层网络的虚拟化框架[19-20]，在虚拟化的通信主机中调用数据包分析进程 Scapy 设置通信系统故障[21]；（2）通过调用外部的 PSD-BPA 暂/稳计算核心，脱离了传统的“故障卡”限制，实现了计算文件中故障信息的自动更新，实现了基于 Mininet-BPA 的 CPS 轻量级联合仿真，并为安稳分析工程师提供在线实时计算多组电力故障的可行思路；（3）根据典型的网络安全事件，通过实际的工程算例验证了基于电力 CPS 联合仿真框架的多站点过载级联故障的快速检测方案，并给出了对应的安稳指标。

## 1 基于 Mininet-Scapy 联合仿真的电力信息虚拟化框架及测试方案

基于 SDN 理论，网络模拟器 Mininet 提供了一种集成路由器、交换机、链路、主机等多个对象联合建模的整体虚拟化方案[19]。本章以电力监控系统为基础，介绍基于 Mininet-Scapy 框架的轻量化信息网络拓扑仿真方案。图 1 左侧给出了电力变电站母线母联间隔中，过程层网络拓扑的 CPS 简化模型，图 1 的右下框图为对应的信息模块及接线，右上框图为

变电站过程层网络的 Mininet 虚拟化架构。在 Linux 环境中，通过仿真器 Mininet 虚拟化的各个设备和主机在 Linux 中被表示为各个 Bash 进程，共享核心、主机文件系统以及进程标识号。但进程在网络命名空间中会被分配专用的网络接口、路由、防火墙规则等，使得各个 Bash 进程可以运行在独立且完整的网络环境中，运行的系统级代码和功能也互不影响。由此，文章认为基于 Mininet 创建的虚拟网络可以较为准确地体现真实物理主机的网络特征。

图 1 中基于 Mininet 模拟器的信息仿真框架里除了与真实系统对应的信息主机和交换机节点外，另有控制器（Controller）节点。这是由于 Mininet 是基于 SDN 开发的项目，后者典型特征是将信息网络的各控制功能抽象并实例化为一个单独的功能模块，用户可通过设置控制器参数来配置各个模块的详细功能，以此测试用户定制化的通信或路由协议。文章不涉及此项功能，选择默认交换机模型，即控制器参数设置为远程控制器方案“Controller”设置为“Controller-Remote”，即不额外定义本地的控制器模块。图 1 中控制器通道为虚线，其余通信链路为实线，以示区别。

为了提高仿真测试的准确性和适用性，根据 IEC 61850 标准，文章提出的变电站信息仿真框架中还包括了 SV 和 GOOSE 通信协议，以此区分合并单元和智能终端的通信内容。文章选择了开放、交互式的数据包开发程序 Scapy 作为构建和收发 GOOSE（SV）数据包的功能模块，通过配置其内置函数参数，可自定义收发主机的目的 IP、MAC 地址以及网卡信息等。根据前文介绍，基于 Mininet 虚拟化部署的主机节点可独立调用虚拟机的核心进程和应用，由此各主机调用、运行 Scapy 的数据包收发功能不会互相影响。

图 2 给出了基于 Mininet-Scapy 联合仿真的变电站信息网络虚拟化流程。主要功能伪代码见附录 A。注意到，代码中调用了专业的网络仿真平台 NS3 作为基础仿真环境，这是因为 NS3 支持更多通信功能和协议，且能为 Mininet 提供外部接口，让 Mininet 主机运行 NS3 内部的通信协议，提高仿真准确性。例如，附录 A 中的链路仿真模块“CSMALink”便是基于 NS3 开发。详细的 Mininet 嵌入 NS3 融合开发技术不属于文章范畴，此处不展开讨论。

## 2　基于信息物理联合仿真的过载稳定校验

由变电站信息网络虚拟化框架可知，Mininet 各个主机可以查看其通信及控制详情，直接调用 Wireshark 程序即可查询所有网卡上的数据流量，进

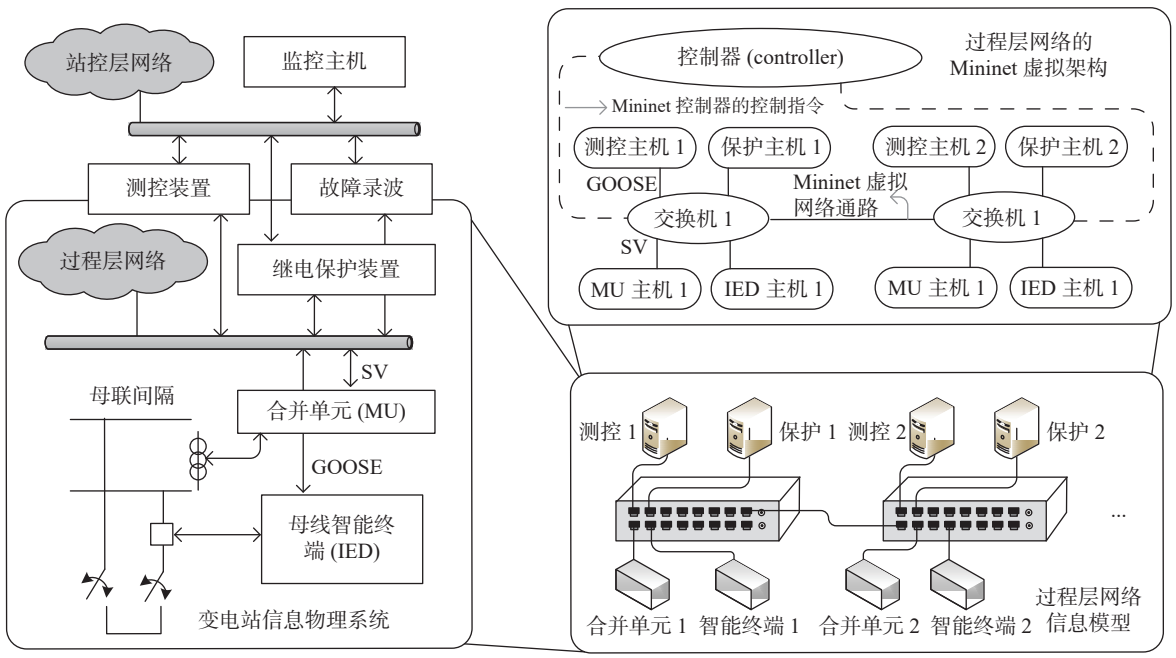


图 1　电力变电站 CPS 模型及基于 Mininet 实现的虚拟化框架

Fig. 1　The model of power substation CPS and the corresponding Mininet-based virtualization framework

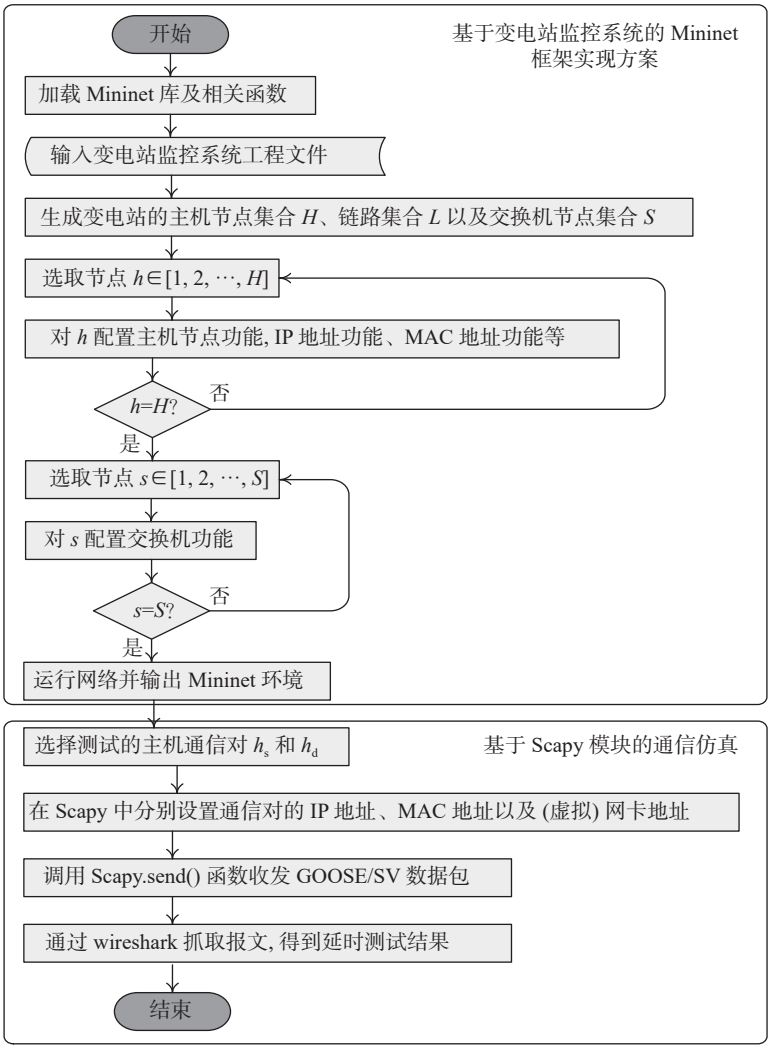


**图 2 基于 Mininet-Scapy 框架开发的信息系统仿真方案**

Fig. 2 Simulation solutions of the information system based on Mininet-Scapy framework

而得到网络的时延信息。本章将继续介绍基于 Mininet-Scapy 信息通信框架的系统运行安全分析模块，并根据线路的过载结果给出系统安全风险的量化方案。根据工程安全的分析思路，文章基于“最坏”考虑给出安全事件$\chi$假设：变电站$i$同时出现电力故障和信息故障。例如，攻击者劫持变电站通信网络且持续潜伏，直到变电站出现全站失压故障，并同时发动分布式拒绝服务攻击（DDoS），恶意占用合并单元和智能终端的传输通道，以拖延测控保护装置接收故障信号，从而扩大故障影响。

便于阐述，本节令网络攻击造成的时延为$\tau_x$，系统变电站集合$\boldsymbol{N}$，线路集合$\boldsymbol{L}$，借助图论形式$\boldsymbol{G}(\boldsymbol{N},\boldsymbol{L})$来表达系统的电网拓扑，记安稳计算程序为**calculate**(•)，其结果$\boldsymbol{r}$为高阶矩阵，包括线路最高功率、额定功率、系统功角、系统频率以及系统电压的计算结果，分别记为$P_{\max}$，$P_{\text{rate}}$，$\delta'$，$\mu'$以及$\sigma'$，可由**.read()** 函数展开。算法 1 给出了传输线过载引起的级联故障的工程安全计算方法，如表 1 所示。

算法 1 第 4 行给出了系统的过载指标$\gamma_p$，其中$\kappa$为过载稳定阈值。$m$表示当发生第$n$组全站失压故障时，过载线路集合$\boldsymbol{M}$的索引，$P_{\max,m}$和$P_{\text{rate},m}$分别表示线路$m$出现的最高功率和额定功率。此外，算法还设置了功角稳定性指标$\gamma_\delta$，频率稳定性指标$\gamma_\mu$以及电压稳定性指标$\gamma_\sigma$，初始值设为 0。算法 1 还选取了最大系统功角、最低系统频率和最低系统电压，即$\delta_{\max}$、$\mu_{\min}$和$\sigma_{\min}$，作为表征各分量严重性的稳定判据。例如，在计算周期内，$t(0,t_d)$，若系统的功角差超过$\delta_{\max}$，则给出判断：系统在下个计算周期内极有可能出现

表 1　变电站 CPS 安全故障计算模块算法

Tab. 1　Algorithm of substation cps contingency calculation module

**输入:** $\kappa$

**输出:** $\gamma_{\mathrm{p}},\gamma_{\delta},\gamma_{\mu},\gamma_{\sigma},v$

**while** $n$ **in** $N$ **do**
  $\boldsymbol{r} \leftarrow$ **calculate**$(G(N,L),\tau_{\mathrm{x}})$
  $(P_{\mathrm{max,m}},P_{\mathrm{rate,m}},\delta',\mu',\sigma') \leftarrow \boldsymbol{r}$**.read**()
  $\gamma_{\mathrm{p}}=\left(\sum_{\mathrm{m}}P_{\mathrm{max,m}}\right)/\kappa\left(\sum_{\mathrm{m}}P_{\mathrm{rate\ ,m}}\right)$
  **if** $\delta' > \delta_{\max}$ **then**
  $\gamma_{\delta}=1.0$
  **else**
  **pass**
  **if** $\mu' < \mu_{\min}$ **then**
  $\gamma_{\mu}=1.0$
  **else**
  **pass**
  **if** $\sigma' < \sigma_{\min}$ **then**
  $\gamma_{\sigma}=1.0$
  **else**
  **pass**
  $v_n=\max\{\gamma_{\mathrm{p}},\gamma_{\delta},\gamma_{\mathrm{f}},\gamma_{\sigma}\}$
**end while**

失步运行。相较于线路过载，失步运行的故障影响更为严重，于是将其对应的功角严重性指标$\gamma_{\delta}$设置为 1.0。同样地，指标$\gamma_{\mu}$和$\gamma_{\sigma}$设置为 1，分别表示仿真中算法检测到系统在该计算周期内或下个周期将发生严重的频率降低和电压崩溃故障。算法给出$v_n$作为第$n$组故障的综合安全指标，可知，其数值越高，故障越严重，即系统稳定性越低。功能实现的伪代码见附录 B。

由附录 B 可知，文章选择的安全计算程序 **calculate**(•)包括了工程计算中常用的电力系统安全分析软件 PSD-BPA 中内置的稳态/暂态计算核心“bpa_pfnt.exe”和“bpa_swnt.exe”，主要用于工程计算中的稳态潮流计算和暂态故障计算。此外，在 update_swi() 函数中，通过 Python 脚本实现了故障卡的连续、自动编辑和更新，无需手动编辑“.LSD”故障卡。由电力工程安全的稳控策略表可知，直接切除过载线路容易扩大故障影响，过载保护设备动作较为谨慎。由此，在算法实现中，暂态分析函数“Xcade_swi()”中只选取了过载最严重的线路作为典型的过载故障信息添加到故障卡更新函数“update_swi()”中，用以区分初始故障。

## 3　仿真算例

### 3.1　仿真环境及参数设置

根据前文第 1 章和第 2 章的介绍可知，文章基于 Mininet 虚拟化框架联合电力安全计算软件 PSD-BPA，得到了变电站信息物理联合测试方案。本小节将详细介绍仿真的测试环境及相关参数。根据南方电网系统某 220 kV 保信子站的工程接线图，算例选取了变电中典型的保护间隔作为研究对象，给出了联合仿真方案，如图 3 的右上框图所示。文章的算例仿真主要基于 VirtualBox-Ubuntu 搭建的 Linux 环境。算例在已嵌入 Mininet 模块的 NS3 环境中启用“./waf”环境变量的编译模式，并在该模式中直接运行 Mininet 脚本即可让虚拟主机接入 NS3 环境。图 3 中左上框图给出了变电站通信网络虚拟化框架及相关界面展示：配置 NS3-Mininet 的联合仿真通道，通过 Python 编辑 Mininet 的网络仿真脚本，通过“net.addSwitch()”函数配置 1 个主交换机和 5 个间隔交换机，通过“net.addHost()”函数配置了 20 个通信节点，并根据图 3 的间隔信息，通过 Mininet 中内置的链路配置函数“CSMLink()”配置了 34 条链路。

算例基于第 2 章中的“最坏”假设，选取 Scapy 作为收发流量测试包的操作工具，通过内置的“sendp()”函数定义发包规则、网卡和间隔时间来模拟满足 IEC 协议的 GOOSE 和 SV 报文通信[22]。在目的地址的主机上调用 Wireshark 抓取特定网卡的报文，解析并处理报文。最后，算例将变电站信息网络仿真结果导入至算法 1，并调用 PSD-BPA 的计算核心实现信息物理联合仿真。仿真中主要的编译语言为 Python 3.7，暂稳计算核心版本为 5.7.1。

### 3.2　仿真测试结果

1）变电站通信网络链路的时延测试结果

由 3.1 节环境设置可知，算例通过 Mininet 添加了 20 个通信节点（host），记为$h_1$，$h_2$，…，$h_{20}$。其中，$h_2$，$h_3$，$h_4$，$h_5$分别表示图 3 中的母联测控主机保护装置，母线保护装置，变压器保护装置以及线路保护装置；$h_6$，$h_7$，$h_8$依次表示母线母联间隔内 1 套合并单元和 2 套智能终端的 3 个主机配置；以此类推，$h_9$，$h_{\cdot}$，…，$h_{20}$表示其余 4 个间隔内的主机配置。表 2 给出了未受攻击时的系统延时的测试结果。结果显示，20 个通信节点互相通信时，部分节点和链路的负载较高，某一条链路会出现极高时延，可以通过配置

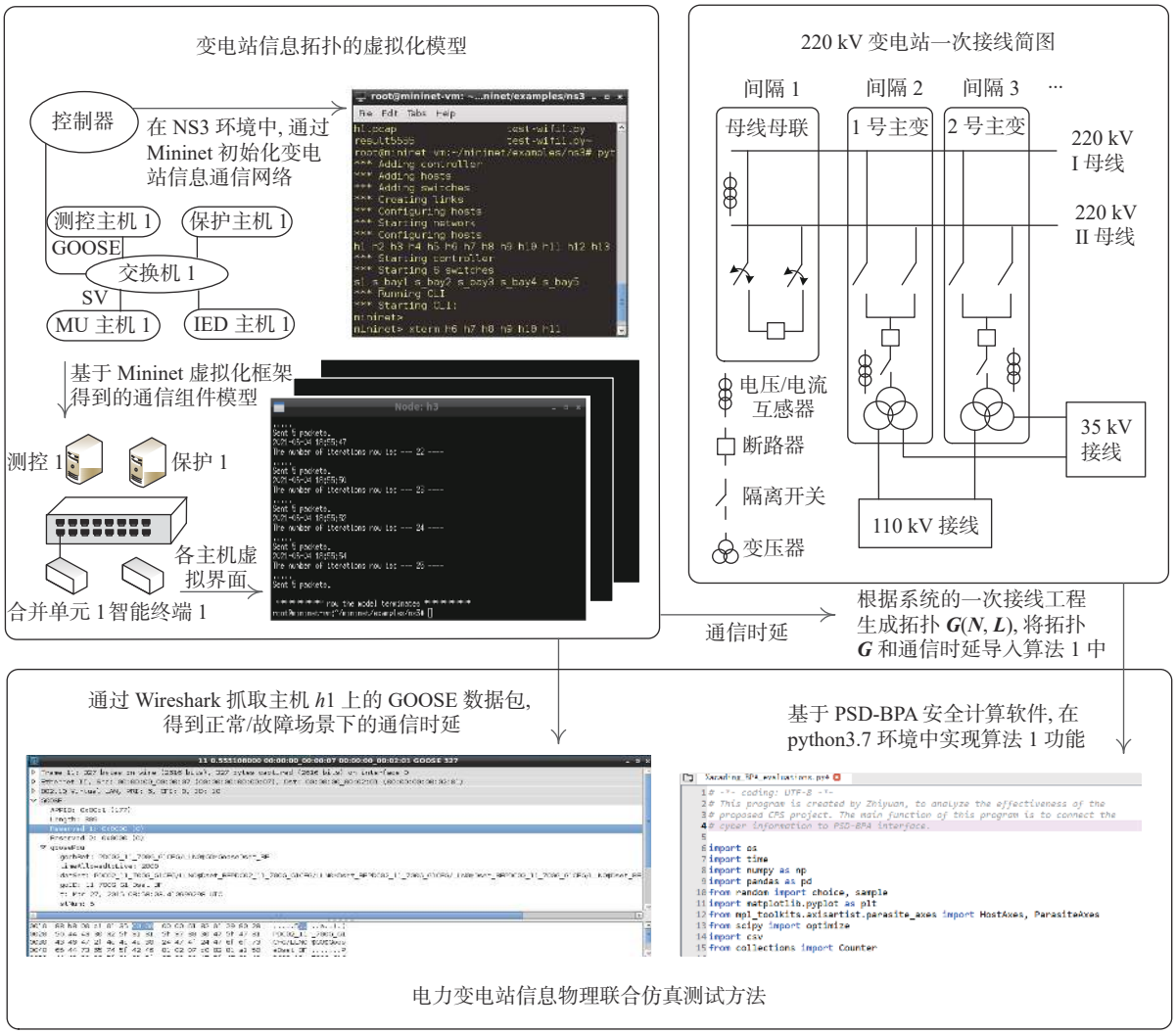


图 3 220 kV 变电站信息安全故障引起的保护动作迟滞对系统运行影响的 CPS 联合仿真测试方案

Fig. 3 The CPS-based co-simulation scheme of power system analysis on delayed-operations of protective relay induced by information network failures in the 220 kV power substation

冗余链路或有针对性配置低时延设备来改善。但在网络入侵攻击的假设场景下, 为了体现入侵攻击对系统时延的影响, 算例选取 15 ms作为系统设备的默认时延设置, 以便消除由通信链路单一或部分节点负载高等客观因素对网络安全结论的影响。

表 2 变电站保护装置通信时延仿真测试

Tab. 2 Time delay results of protection devices in the power substation communication model

| 链路固定时延设置/ms | 系统平均时延/ms | 系统最高时延/ms | 时延≥80 ms信道链路数/条 |
|---|---|---|---|
| 15 ~ 20 | 20 | 76 | 0 |
| 50 ~ 55 | 63 | 146 | 3 |
| 60 ~ 65 | 71 | 358 | 7 |

算例在 Mininet 中搭建了 220 kV 变电站的网络虚拟化模型。表 3 给出了变电站保护装置在不同测试场景下的平均时延结果, 其中保护 1 ~ 保护 5 分别为母联保护、110 kV 变压器保护、35 kV 变压器保护以及厂站进线与出现的线路保护。各组保护系统内配置了 1 套合并单元和 2 套智能终端, 根据附录中的设置, 初始带宽设置为 1 Gbps。为区分不同的设备, 保护 1 ~ 保护 3 的固定时延设置为 5 ms ~ 20 ms, 保护 4 和保护 5 的固定时延设置为 40 ms ~ 50 ms。注意到, 时延仿真测试中某条链路出现了较大时延, 这是因为此处采用的是基础通信模型, 网络拓扑未做优化处理。$X_1$, $X_2$分别表示保护 1 和 2 子系统中的智能终端发生了信息安全事件$X$; $X_3$表示保护 2 和

保护 3 子系统中同时出现了信息安全事件。

**表 3　故障场景下，各个保护系统内部的平均时延**

Tab. 3　The results of average time delay of protection relays under normal/attacking scenarios　　ms

| 测试场景 | 保护1 | 保护2 | 保护3 | 保护4 | 保护5 |
|---|---|---|---|---|---|
| $X_1$ | 494.34 | 65.31 | 88.82 | 67.06 | 102.2 |
| $X_2$ | 30.30 | 331.94 | 72.68 | 67.14 | 71.98 |
| $X_3$ | 36.54 | 427.39 | 824.87 | 85.45 | 68.39 |

由信息仿真结果可知，出现信息故障$X_3$后，通信网络中约 64% 的链路时延增加了 10 倍或以上，其中 2 号主变的 MU 主机与 110 kV 变压器保护主机的通信时延，从正常条件下的 5.16 ms 增加至 520.11 ms。此时信息故障将极大地阻碍合并单元向保护装置传递测量信号，存在严重运行安全隐患。

2）基于海南电网夏大运行方式数据的仿真结果

算例选取 2027 年海南电网夏大运行方式数据作为系统工程安全的基础数据。注意到，电网中接入 78 个变电站站点，包括 466 个母线节点，涵盖 23 个供电区域，接入功率 11.6 GW，挂有 11.3 GW 负荷。算例假设各站点的信息物理拓扑与配置均同图 3 一致，并选择表 1 中场景$X_3$作为信息故障模型。可知，通信系统的平均时延为 288.5 ms，保护设备接收到真实测量信号的时间将延缓至少 12 ~ 13 周波。过载稳定裕度$\kappa$取温度在 15 ~ 40 ℃ 时载流量的变化区间[23]，$\kappa \in [1, 1.35]$。

根据上述计算条件，首先对各站点的母线出线做 $N$−1 三相短路故障校验，共计检测线路 1 400 条，其中无法满足计算条件的线路 200 条，即在预设的计算周期 500 ms 内，电力系统的安稳计算无法在约束条件内求解可行运行方案。在严重的信息故障前提下，工程安全故障范围可能会被恶意扩散，此时电力系统极有可能不再满足基本 $N$−1 准则，电网可靠性降低。

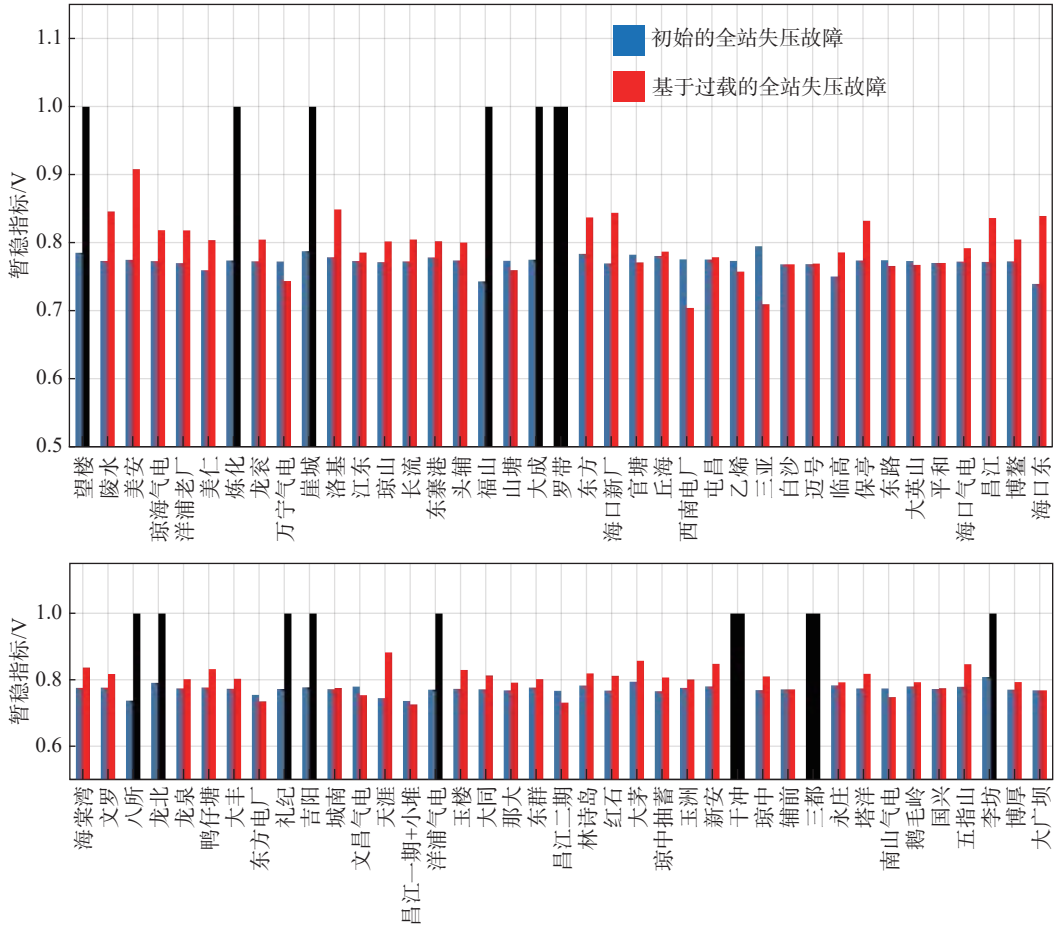


图 4　海南电网夏大运行方式数据的 CPS 联合仿真结果

Fig. 4　The screening results of cyber-physical coordinated evaluations based on the peak-load dataset of Hainan grid

基于算法 1，图 4 给出了海南电网各个变电站站点在信息故障场景$X_3$下发生全站失压故障的联合仿真结果。其中红色和蓝色图例分别表示发生初始故障后，有/否考虑线路过载特性的暂态稳定结果。黑色表示暂稳安全指标为 1.0 的厂站。例如，“望楼站”为 220 kV 厂站，挂有负荷 179.8 MW，当该站同时出现信息故障和全站失压故障时，注意到，计算周期内暂态分析仍然收敛，系统的整体过载指标为 0.785，且未检到其他安全故障。但在考虑过载保护动作的场景中，系统在发生初始故障后会切除部分严重过载的线路，此时系统的功角差将超过计算极限，在计算周期内无法得到可行解，预计将出现严重的失步运行故障，此时该站的稳定性指标为 1.0。同样地，“八所站”为 500 kV 变电站，挂有负荷 215 MW，在发生初始故障时，计算得到系统的过载指标为 0.73；当考虑过载保护动作后，系统的功角稳定性和频率稳定性指标均为 1.0，预计将出现严重的失步运行和频率崩溃故障。

注意到，在严重的信息故障条件下，大部分厂站的过载保护动作将降低系统运行的安全阈值，其中“望楼”“炼化”等 11 个站点出现了包括潜在的失步运行、电压崩溃故障以及系统频率降低甚至频率崩溃等严重运行故障。但对于“文昌气电”站、“东方电厂”等厂站，过载保护的积极动作提升了其运行系统的安全阈值。下一步的工作将研究详细的安稳控制策略对 CPS 工程安全问题的影响机制。

## 4 结论

文章沿用了前文的网络攻击假设，在站控层网络的入侵风险评估模型的基础上新增了过程层网络的信息物理联合仿真，基于继电保护装置的时延测试验证了入侵风险的评估方法。文章提出了可快速筛选潜在“高危风险节点或设备”的 CPS 联合仿真方法，为电力 CPS 安全工程师提供了一种支持自定义开发及调试系统安全的开源方法。基于实际的工程算例，文章成功识别出高危风险站点和线路，量化了安稳控制设备的信息故障对电力能源系统的影响，同时验证了过载保护等传统电力保护设备对 CPS 安全事件的影响机制，例如，对负荷节点的和发电机节点应配置不同的过载保护控制策略便可提升系统的稳定裕度。此外，文章在联合仿真中脱离了传统的“故障卡”限制，实现了计算文件中故障信息的自动更新，在提高计算效率的同时也为安稳分析工程师在线实时计算多组电力故障提供了可行思路。

未来能源领域的工作重点是搭建以新能源为主体的高效能源体系。更多智能化、集成化的控制和感知设备将促进电力运行网络与信息网络的数据融合，电力 CPS 的安全场景愈发复杂。后续的研究将继续优化联合仿真功能代码，提高数据交互效率，同时探究安稳控制设备的信息安全事件对高比例新能源广泛接入的新型电力系统的影响。

## 附录 A 基于 Mininet 开发的功能模块伪代码

该部分主要介绍 Linux 环境中基于 Mininet 各子模块开发的变电站信息仿真平台。

```
# 输入参数:
# H,主机节点 list
# S,交换机节点 list
# L,系统链路 list
# DataRate,带宽
# Delay,基础时延
from mininet.net import Mininet, Controller, CLI,ns3
from mininet.ns3 import CSMALink
def SubstationNets_Initialize(H, S, L, DataRate, Delay):
net=Minine t(controller= ‘Controller-Remote ’, autoSetMacs=True)
net. addController('Default_Controller')
for h in H:
h=net. addHost(h. name, ip, defaultRoute=None)
h. setIP(h. IP, intf=h. MAC)
h.setMAC(h.MAC, intf=h.MAC)
for s in S:
s.addSwitch(s.name)
for l in L:
CSMALink(l,DataRate,Delay)
net.start()
mininet.ns3.start() // 激活 NS3 环境
CLI(net)
If__name__==‘__main__’:
```

SubstationNets_Initialize(H,S,L,DataRate,Delay)

## 附录 B 算法 1 功能实现伪代码

```
# 计算参数:
# tao_x,信息仿真的时延结果
# sub, 系统各变电站的母线节点汇总 list
# 初始化 delta_max, miu_min, sigma_min, kappa, t_0, t_d,
import os
def calculate():
os.run('bpa_pfnt.exe')
os.run('bpa_swnt.exe')
if__name__=='__main__':
gamma_delta, gamma_miu, gamma_sigma=0
for n in sub:
update_swi(n,tao_x) # update_swi() 修改.swi 文件, 模拟
r=calculate() # 系统切除全站失压故障
p_list=r.read() # p_list 储存系统过载线路信息
for p in p_list:
if p._overloads_time in [tao_x,t_d] # 调取线路过载信息, 并判断其是否
Xcade_swi(p_list) # 在程序的计算周期内, Xcade_swi()
r_Xcade=calculate() # 可在原.swi 卡中添加过载线路信息
p_list,_delta, _miu, _sigma=r_Xcade.read()
if _delta>delta_max: gamma_delta=1
if _miu<miu_min: gamma_miu=1
if _sigma<sigma_min:gamma_miu=1
if gamma_delta==1 or gamma_miu==1 or gamma_miu==1: pass
else
p_rate, p_max = r.read(p_list)
gamma_p = sum(p_max)/kappa*sum(p_rate)
```

**参考文献:**


[1] 管晓宏, 赵千川, 贾庆山, 等. 信息物理融合能源系统［M］. 北京: 科学出版社, 2016.
GUAN X H, ZHAO Q C, JIA Q S, et al. Cyber-physical energy system［M］. Beijing: Science Press, 2016.

[2] 赵东元. 以新能源为主体的新型电力系统: 形态特征［EB/OL］. (2021-03-19)［2021-06-11］. https://www.ne21.com/news/show-158585.html.
ZHAO D Y. New power system based on the renewable energy: systematic characteristics［EB/OL］.(2021-03-19)［2021-06-11］. https://www.ne21.com/news/show-158585.html.

[3] 郭庆来, 辛蜀骏, 孙宏斌, 等. 电力系统信息物理融合建模与综合安全评估: 驱动力与研究构想［J］. 中国电机工程学报, 2016, 36(6): 1481-1489. DOI: 10.13334/j.0258-8013.pcsee.2016.06.003.
GUO Q L, XIN S J, SUN H B, et al. Power system cyber-physical modelling and security assessment: motivation and ideas［J］. Proceedings of the CSEE, 2016, 36(6): 1481-1489. DOI: 10.13334/j.0258-8013.pcsee.2016.06.003.

[4] 王琦, 李梦雅, 汤奕, 等. 电力信息物理系统网络攻击与防御研究综述: (一)建模与评估［J］. 电力系统自动化, 2019, 43(9): 9-21. DOI: 10.7500/AEPS20180906006.
WANG Q, LI M Y, TANG Y, et al. A Review on research of cyber-attacks and defense in cyber physical systems part one modeling and evaluation［J］. Automation of Electric Power Systems, 2019, 43(9): 9-21. DOI: 10.7500/AEPS20180906006.

[5] 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. DOI: 10.16383/j.aas.2018.c180461.
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. DOI: 10.16383/j.aas.2018.c180461.

[6] TEN C W, YAMASHITA K, YANG Z Y, et al. Impact assessment of hypothesized cyberattacks on interconnected bulk power systems［J］. IEEE Transactions on Smart Grid, 2018, 9(5): 4405-4425. DOI: 10.1109/TSG.2017.2656068.

[7] 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 J H, WEN F S, XUE Y S, et al. Modeling analysis and control research framework of cyber physical power systems［J］. Automation of Electric Power Systems, 2011, 35(16): 1-8.

[8] ADHIKARI U, MORRIS T, PAN S Y. WAMS cyber-physical test bed for power system, cybersecurity study, and data mining［J］. IEEE Transactions on Smart Grid, 2017, 8(6): 2744-2753. DOI: 10.1109/TSG.2016.2537210.

[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(3): 6-22. DOI: 10.16516/j.gedi.issn2095-8676.2020.03.002.
YANG Z Y, ZHANG S P, SUN H. Integrated cyber-physical contingency analysis and risk estimates［J］. Southern Energy Construction, 2020, 7(3): 6-22. DOI: 10.16516/j.gedi.issn2095-8676.2020.03.002.

[10] 杨至元, 张仕鹏, 孙浩, 等. 基于Cyber-net与学习算法的变电站网络威胁风险评估［J］. 电力系统自动化, 2020, 44(24): 19-27. DOI: 10.7500/AEPS20191230009.
YANG Z Y, ZHANG S P, SUN H, et al. Cyber-induced risk estimation of power substations incorporating cyber-net with

learning method［J］. Automation of Electric Power Systems, 2020, 44(24): 19-27. DOI: 10.7500/AEPS20191230009.

［11］ YANG Z Y, TEN C W, GINTER A. Extended enumeration of hypothesized substations outages incorporating overload implication［J］. IEEE Transactions on Smart Grid, 2018, 9(6): 6929-6938. DOI: 10.1109/TSG.2017.2728792.

［12］ LIU R, VELLAITHURAI C, BISWAS S S. Analyzing the cyber-physical impact of cyber events on the power grid［J］. IEEE Transactions on Smart Grid, 2015, 6(5): 2444-2453. DOI: 10.1109/TSG.2015.2432013.

［13］ SRIVASTAVA A, RRIS T, RNSTER T, et al. Modeling cyber-physical vulnerability of the smart grid with incomplete information［J］. IEEE Transactions on Smart Grid, 2013, 4(1): 235-244. DOI: 10.1109/TSG.2012.2232318.

［14］ ASHOK A, GOVINDARASU M, WANG J H, et al. Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid［J］. Proceedings of the IEEE, 2017, 105(7): 1389-1407. DOI: 10.1109/JPROC.2017.2686394.

［15］ 顾晨骁, 顾伟, 陈超, 等. 分布式电源集群控制与电力信息实时仿真研究［J］. 电力系统保护与控制, 2020, 48(4): 64-71. DOI: 10.19783/j.cnki.pspc.190426.

GU C X, GU W, CHEN C, et al. Distributed power cluster control and research on power information real-time simulation［J］. Power System Protection and Control, 2020, 48(4): 64-71. DOI: 10.19783/j.cnki.pspc.190426.

［16］ 汤奕, 陈倩, 李梦雅, 等. 电力信息物理融合系统环境中的网络攻击研究综述［J］. 电力系统自动化, 2016, 40(17): 59-69. DOI: 10.7500/AEPS20160315001.

TANG Y, CHEN Q, LI M Y, et al. Overview on cyber-attacks against cyber physical power system［J］. Automation of Electric Power Systems, 2016, 40(17): 59-69. DOI: 10.7500/AEPS20160315001.

［17］ 汤奕, 王琦, 郜伟, 等. 基于OPAL-RT和OPNET的电力信息物理系统实时仿真［J］. 电力系统自动化, 2016, 40(23): 15-21+92. DOI: 10.7500/AEPS20160515020.

TANG Y, WANG Q, TAI W, et al. Real-time simulation of cyber-physical power system based on OPAL-RT and OPNET［J］. Automation of Electric Power Systems, 2016, 40(23): 15-21+92. DOI: 10.7500/AEPS20160515020.

［18］ HWANG S H, IM Y S, SONG H C, et al. Real time emulation of IEC 61850 SV, GOOSE, and MMS using NS-3［J］. Journal of Engineering and Applied Sciences, 2018, 13(3): 634-638. DOI: 10.36478/jeasci.2018.634.638.

［19］ AYDEGER A, AKKAYA K, CINTUGLU M H, et al. Software defined networking for resilient communications in smart grid active distribution networks［C］//2016 IEEE International Conference on Communications(ICC), Kuala Lumpur, Malaysia, 22-27, May, 2016. Kuala: IEEE, 2016: 1-6. DOI: 10.1109/ICC.2016.7511049.

［20］ PAKZAD F, LAYEGHY S, PORTMANN M. Evaluation of Mininet-WiFi integration via NS-3［C］//2016 26th International Telecommunication Networks and Applications Conference (ITNAC), Dunedin, New Zealand, 7-9, December, 2016. Dunedin: IEEE, 2016: 1-6. DOI: 10.1109/ATNAC.2016.7878816.

［21］ BIONDI P. Introduction-about scapy［EB/OL］. (2019-08-17)［2021-06-01］. https://scapy.readthedocs.io/en/latest/introduction.html.

［22］ GRAY K, KUMM J, MRAZ J. A high-level framework for implementation and test of IEC 61850-based microgrid power management systems［C］//2016 IEEE/PES Transmission and Distribution Conference and Exposition (T&D), Dallas, TX, USA, 3-5, May, 2016. Dallas: IEEE, 2016: 1-4. DOI: 10.1109/TDC.2016.7520026.

［23］ SONG F, WANG Y L, ZHAO L, et al. Study on thermal load capacity of transmission line based on IEEE standard［J］. Journal of Information Processing Systems, 2019, 15(3): 464-477. DOI: 10.3745/JIPS.04.0114.

**作者简介：**

杨至元

**杨至元**（第一作者，通信作者）
1993-，男，土家族，湖南怀化人，美国密歇根理工大学博士，主要研究方向包括电力网络安全与风险分析，机器学习、信息物理融合系统建模和分析，电力系统稳定计算(e-mail) yangzhiyuan@gedi.com.cn。

（编辑　叶筠英）