中国科学: 信息科学 2022 年 第 52 卷 第 3 期: 399–429
SCIENTIA SINICA Informationis
《中国科学》杂志社
SCIENCE CHINA PRESS
评述

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

王子骏[1], 刘杨[1*], 鲍远义[1], 管晓宏[1], 吴桐[2], 卢建刚[3], 余志文[3], 袁晓舒[4], 刘烃[1*]

1. 西安交通大学网络空间安全学院, 西安 710049
2. 国家能源局信息中心, 北京 100824
3. 广东电网公司电力调度控制中心, 广州 510699
4. 东方电气中央研究院, 成都 611731

* 通信作者. E-mail: yangliu@mail.xjtu.edu.cn, tingliu@mail.xjtu.edu.cn

收稿日期: 2021–06–23; 修回日期: 2021–08–17; 接受日期: 2021–09–09; 网络出版日期: 2022–02–24

国家重点研发计划 (批准号: 2018YFB0803501)、国家自然科学基金 (批准号: U1766215, 61772408, 61632015, 61833015, 62002281)、"2020 年工业互联网创新发展工程项目 — 工业互联网渗透测试和众测平台" 和中央高校基本科研业务费专项资金资助项目

摘要 电力系统安全仿真是面向电力系统自身故障或外部攻击等安全威胁, 通过仿真实验或借助数值计算研究系统行为的技术. 随着自动控制、网络通信、人工智能等信息技术的广泛应用, 电力系统已发展成为物理系统与信息系统深度耦合的信息物理融合系统. 物理破坏或网络攻击产生的故障在电力系统中相互关联, 可跨域传播, 产生新的安全威胁形态. 电力系统安全仿真正在面临新的挑战. 本文回顾了历史上影响广泛的电力系统安全事件; 从工程安全、网络安全、信息物理综合安全 3 个维度, 分析电力系统安全仿真的需求和技术发展, 对代表性的安全仿真平台进行分类和总结; 探讨电力系统安全仿真技术面临的挑战和发展趋势.

关键词 信息物理融合系统, 工程安全, 网络安全, 信息物理综合安全, 电力系统安全仿真技术

1 引言

随着智能电网技术的快速发展, 自动控制、网络通信、人工智能等信息技术被广泛应用于电力系统中, 在极大提升电力系统信息化、自动化、互动化程度的同时, 也导致电力系统所面临的安全威胁发生了深刻变革. 传统电力系统的正常运行主要受设备故障、人员管理、极端天气等物理系统的工程安全 (engineering safety) 威胁影响; 随着电力系统的运行环境变得更加开放和互联[1)], 信息系统的网络安

1) 中华人民共和国国务院. 中国制造 2025. 2015.

引用格式: 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. 中国科学: 信息科学, 2022, 52: 399–429, doi: 10.1360/SSI-2021-0210
Wang Z J, Liu Y, Bao Y Y, et al. Power system security simulation technologies: engineering safety, network security and cyber-physical integrated security (in Chinese). Sci Sin Inform, 2022, 52: 399–429, doi: 10.1360/SSI-2021-0210

全 (network security) 威胁已经造成了电力系统的多次重大安全事件; 现代电力系统是由信息系统与物理系统深度耦合形成的信息物理融合系统 (cyber-physical system, CPS). 其中, 信息技术 (information technology, IT) 和操作技术 (operation technology, OT) 在业务流程上深度结合, 使物理系统的工程安全和信息系统的网络安全紧密关联, 产生了新的信息物理综合安全 (cyber-physical integrated security) 威胁. 电力系统的安全防护正朝着涉及自然和社会因素的综合灾变防御方向发展 [1~3].

由于电力系统面临的安全威胁形态持续变化, 同时电力系统的运行机理复杂、故障危害重大, 能在真实环境下进行的电力系统安全研究非常有限. 因此, 作为现代电力系统规划设计和运行的基础技术之一, 电力系统安全仿真技术一直受到学术界和工业界的广泛关注. 电力系统安全仿真技术面向电力系统自身故障或外部攻击等安全威胁, 通过仿真实验或借助数值计算研究系统行为, 具体包括: 针对物理系统的工程安全仿真技术, 研究包括电力设备安全、系统运行安全、产品质量等与物理系统相关的安全问题; 针对信息系统的网络安全仿真技术, 研究包括数据安全、软硬件安全、通信安全等安全问题 [3]; 针对 CPS 的综合安全仿真技术, 研究采用物理破坏、网络攻击等手段, 利用系统物理脆弱性和网络脆弱性的协同效应, 造成系统故障或诱导故障在系统中传播等安全问题 [3].

目前电力系统安全仿真技术仍面临诸多挑战: 一方面, 电力系统的规模不断扩大、业务模式持续变化、运行机理和保护机制复杂多样, 如何快速、精准地仿真大规模电力系统的动态运行过程是电气工程学科的经典难题. 另一方面, 电力系统安全既要分析和防范单一攻击, 也要防御协同攻击的影响; 既要研究局部孤立系统的安全控制方案, 也要研究广域互联系统的整体安全机制. 随着信息系统与物理系统的深度耦合, 电力系统新型安全威胁呈现跨域传播的特点, 对其进行建模分析十分困难, 安全威胁的内涵和类型快速拓展, 需要不断研究新的安全仿真技术以适应持续变化的安全威胁.

美国国家标准技术研究院 (National Institute of Standards and Technology, NIST) 指出, 电力系统安全仿真难以依靠单一学科技术进行研究, 应通过物理、通信和控制系统实现集成模拟[2]. 目前, 电力系统安全仿真技术中的各子系统和功能模块集成交互, 相互之间的耦合关系复杂, 较难对其进行解构. 为了理解其特点与发展趋势, 本文将对面向电力系统安全的仿真技术工作进行梳理与总结.

电力系统安全仿真是电气工程、自动化、计算机、网络空间安全等多个学科交叉融合的研究方向. 本文从信息物理融合系统的视角, 回顾历史上影响广泛的电力系统安全事件; 在此基础上, 从工程安全、网络安全、信息物理综合安全 3 个维度分析电力系统安全仿真的需求和技术发展, 对代表性的安全仿真平台进行分类和总结; 并从能源形态、攻击能力、耦合程度等方面, 探讨电力系统安全仿真技术面临的挑战和发展趋势.

2 电力系统安全事件分析与仿真技术发展

信息技术在改善电力系统运行效率和可靠性的同时, 也不可避免地给电力系统运行引入了新的安全威胁. 信息网络的脆弱性使得电力系统基础设施更容易遭受来自网络外部的非法接入和攻击. 历史上影响重大的电力系统安全事件会驱动人们探究事件背后的安全威胁本质, 进而推动相关的安全仿真技术研究. 本节通过对电力系统重大安全事件的回顾分析, 总结安全事件与安全仿真技术发展的关联, 并梳理安全仿真技术的发展历程.

2.1 电力系统安全事件回顾

近几十年来, 新技术和设备的引入与场景的快速变革导致电力系统不断出现新的安全隐患, 催生

2) NIST. Measurement Challenges and Opportunities for Developing Smart Grid Testbeds. 2016.

了大量安全事件, 对社会稳定和人民生活造成极大影响. 本文将从工程安全、网络安全、综合安全 3 方面回顾历史上影响广泛的安全事件, 分析电力系统安全仿真技术发展的重要驱动因素.

2.1.1 电力系统工程安全事故

电力系统工程安全事故是指由于设备设施损坏或极端天气影响, 导致电力供需失衡, 进而引发大规模停电的安全事故. 工程安全事故的起始发生时间较早, 发展历史较长, 发生过程仅与物理系统相关, 通常会造成直接经济损失.

1965 年, 由于电力需求达到极限, 加拿大水电站的发电机组为防止自身烧毁, 自动跳闸, 同时美国和加拿大边界的一个继电器发生故障, 导致加拿大与美国东北部停电, 约 3000 万人口的正常生活受到严重影响, 造成经济损失达 1 亿美元 [4]. 该事故发生后, 电力能源运行管理受到重视, 能源管理系统 (energy management system, EMS) 诞生, 研究人员开始大规模使用仿真工具对电力系统进行分析.

20 世纪 40 年代 Mapkobhu 首次提出电压稳定条件, 然而当时电力系统总体规模较小, 人们普遍认为电压稳定问题是系统末端的局部问题, 并未引起高度重视. 1978 年法国电网的灾难性电压崩溃使得法国 70% 以上的用户停电 [5], 电压稳定问题进而成为人们关注的焦点, 国内外研究机构也对此进行了大量的仿真研究.

2003 年 8 月 14 日, 美国俄亥俄州的一台 55 万千瓦机组跳闸, 在短时间内, 造成了大量线路和机组连续跳闸, 电网近乎全部瓦解, 负荷大部分损失, 最终引发了北美历史上范围最大的停电事故, 停电共计 29 个小时, 使得 5000 万人的工作和生活受到了严重的影响 [6]. 正是在北美大停电后, 美国电力行业决定发展智能电网技术, 进而在电力系统内实现智能控制、智能管理、智能分析功能, 彻底改造陈旧老化的电力设施.

目前由于全球变暖等因素的影响, 极端天气出现得越来越频繁. 1989 年的一场太阳风暴中, 强磁暴使得加拿大魁北克全省供电系统受到严重冲击 [7]; 2008 年中国南方遭遇了罕见的冰雪灾害, 电网遭受重创, 线路覆冰、铁塔倒塌、变电站跳闸, 持续时间从 1 月底至 2 月初 [8]; 2016 年, 强台风导致南澳大利亚州大量风电机组停止运行、输电线路破坏等一系列故障, 并最终导致南澳大利亚州全州停电长达 50 小时 [9]; 2021 年美国得克萨斯州受极寒天气影响, 电力取暖负荷急剧攀升, 与此同时, 因天然气管道冰堵、风机叶片冻结, 大量火电和风电机组退出运行, 供需严重失衡, 停电时间长达 5 天, 交易市场的电价一度飙升 100 倍 [10].

这些极端天气导致的停电事故引发了学术界对相应安全威胁的研究和思考, 力求在电网架构、防冰加固、新能源接入等方面进一步完善现有电力系统的安全性能.

2.1.2 电力系统网络安全事件

电力系统网络安全事件是指由于人为因素、软硬件设计缺陷或运行故障等情况, 对电力信息系统或者其中的数据造成损害的安全事件. 随着智能电网技术开始发展, 电力系统网络安全事件逐渐出现.

2003 年 1 月, Slammer 蠕虫病毒利用缓冲区溢出漏洞, 攻击俄亥俄州 Davis-Besse 核电站, 导致网络中出现信息洪流、计算机系统资源耗尽、处理速度缓慢、异常参数监测系统与运行控制主机停止工作长达数个小时 [11].

2006 年 8 月, 美国亚拉巴马州 Browns Ferry 核电站遭到拒绝服务攻击, 局域网内网络流量剧增, 循环泵和冷凝除矿控制器无法及时响应以太网的广播式数据通信, 进而设备瘫痪, 致使核电机组被迫关闭.

2017 年勒索病毒在全球大规模爆发, 世界多地电力系统遭受勒索病毒的攻击. 勒索病毒会加密文

件, 只有通过攻击者的私钥才能解密文件, 攻击使得用户无法进行买电、充值、办理发票等操作, 攻击者还会索要高额比特币赎金. 2018 年, 美国政府公开谴责俄罗斯政府使用 NotPetya 勒索软件对其进行电网入侵攻击.

以上电力系统网络安全事件的入侵手段与互联网网络攻击类似, 随着电力系统智能化的发展, 原本封闭的电力系统必然需要与开放的互联网进行数据交互, 因此对电力信息系统的安全防护十分必要. 为应对日益严重的网络安全威胁, 我国坚持 “积极利用、科学发展、依法管理、确保安全” 十六字方针, 不断健全网络安全保障体系 [12]; NIST 也持续更新发布《提升关键基础设施网络安全框架》[13, 14], 从而保证各类行业机构基础设施的网络安全. 同时, 针对电力系统网络安全威胁的仿真研究受到学术界和工业界的广泛关注.

2.1.3 电力系统信息物理综合安全事件

随着信息化程度逐渐提高, 计算机网络和信息系统在电力系统中所占比重逐渐增大. 由于信息系统与电力系统之间的紧密耦合关系, 由网络攻击或信息 – 物理混合攻击 (网络攻击加物理破坏) 所诱发的电力系统综合安全事件最终会导致物理系统发生故障或诱导故障在系统中传播 [3].

2010 年, “震网” 蠕虫病毒横空出世, 并对伊朗纳坦兹铀浓缩工厂进行攻击, 近千台生产核燃料用的离心机遭到破坏, 最终铀浓缩计划停滞、伊朗核计划推迟, 该事件也被称为世界上首个 “网络超级武器” 事件 [15]. “震网” 攻击与先前的网络攻击不同之处在于, 传统网络攻击面向的是信息传输的通信过程, 而 “震网” 病毒主要针对国家重要基础设施, 如核电站、水坝、国家电网等, 展现出隐蔽性、复杂性与巨大的杀伤力.

2015 年 12 月 23 日, 乌克兰电网遭受 BlackEnergy3 攻击, 造成 140 万用户停电长达数小时. 攻击者通过定向发送含有 Office 漏洞恶意文件的垃圾邮件, 将电网控制系统与外网服务器相连, 获取控制权限, 进行断路器操控. 为阻止断电后的系统恢复, 攻击者提前通过恶意组件 KillDisk 破坏数据存储系统, 擦除入侵痕迹, 并对客服中心发起拒绝服务攻击, 防止其提前得知断电消息 [16]. 此次黑客攻击事件首次造成电网大规模停电, 进一步证明了网络攻击手段可以实现工业破坏, 具有重大影响.

2019 年 3 月 7 日起, 委内瑞拉大部分地区停电超过 24 小时, 全国将近 90% 区域全面停电. 据推测, 这次停电事件可能是由信息攻击与物理破坏相结合的混合攻击, 最终造成基础设施的系统性瘫痪. 具体过程为攻击者利用隐藏在电网控制系统内的恶意设备或一些重要组件的恶意软件发起网络攻击, 导致委内瑞拉最大的古里水电站机组停机, 并对后续的故障恢复过程实施干扰 [17].

2021 年 4 月 11 日, 伊朗总统宣布启用纳坦兹核设施的 164 台新离心机, 一天后其供电设备便发生爆炸事件, 以色列公共媒体情报人士报道 “这是以色列网络攻击的结果”. 《纽约时报》称 “爆炸对核设施电力系统造成了严重破坏, 伊朗修复受损系统至少要花 9 个月” [18]. 2021 年 5 月 7 日, 美国燃油管道公司 Colonial Pipeline 遭到勒索软件攻击, 被迫将所有燃油管道停止运行, 使得燃料市场出现大面积短缺. 美国政府于 5 月 9 日宣布进入 “国家紧急状态” [19].

上述事件表明, 信息系统的网络安全威胁与物理系统的工程安全威胁的深度耦合、跨域作用使电力系统安全威胁呈现新形态, 产生了大量信息物理综合安全事件. 与单纯的工程安全事故和网络安全事件相比, 信息物理综合安全事件呈现出攻击机理复杂、攻击能力强、威胁程度大、影响范围广等特点, 目前尚未有很好的解决方案, 亟需结合仿真技术进行进一步研究.

2.2 电力系统综合安全威胁分析

电力系统综合安全威胁需要考虑物理系统脆弱性和信息系统脆弱性的协同效应, 在 CPS 场景中,

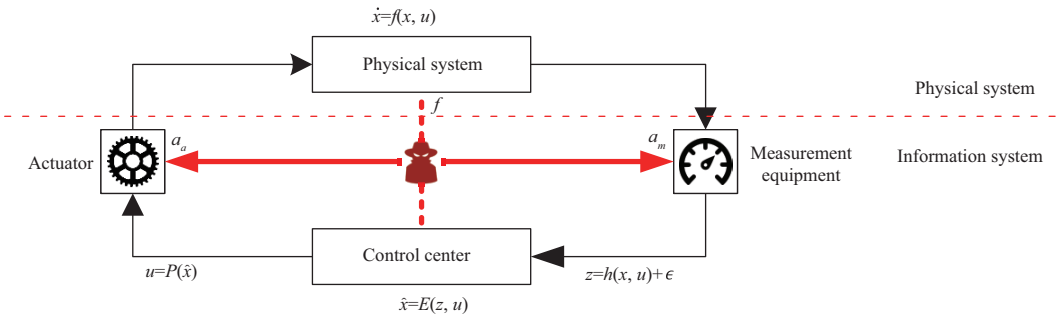

图 1 CPS 综合安全威胁模型

Figure 1 Cyber-physical integrated security model

单个系统中存在的原始漏洞危害性被放大, 使得物理破坏与网络攻击可以直接影响 CPS 综合安全. 典型 CPS 由决策中心、物理系统、执行机构与量测设备构成, 综合安全威胁模型如图 1 所示 [3]. 具体模型可表述为

$$\begin{aligned} \dot{x} &= f(x,u), \quad z = h(x,u)+\epsilon, \\ \hat{x} &= E(z,u), \quad u = P(\hat{x}), \end{aligned}$$

其中, x 表示系统状态, $\dot{x}$ 表示下一时刻的系统状态, $\hat{x}$ 表示系统状态估计量, u 表示控制信号, z 表示量测值, f, h, E, P 分别表示物理系统、量测设备、决策中心、执行机构的传递函数, ϵ 表示量测噪声.

当 CPS 遭受物理事故或攻击时, 物理系统传递函数 f 会被破坏, 导致系统状态量 $\dot{x}$ 出现偏差, 进而影响通信网络中的量测值 z. 如果量测值与正常值偏差过大, 有可能造成通信网络崩溃. 当 CPS 存在网络故障或受到攻击后, CPS 中的控制信号 u 被篡改为 u_a, 使得物理系统接收到的控制信号发生变化, 进而作出错误的决策; 同时量测值 z 也被篡改为 z_a, 篡改后的量测值 z_a 与决策中心上一时刻发出的控制信号 u 仍然符合传递函数 E 的物理规律, 因此决策者难以发现物理系统已经被控制, 达到欺骗决策中心的目的, 从而导致更严重的后果. 具体表述如下:

$$\begin{aligned} \dot{x_a} &= f(x_a,u_a), \quad z_a = h(x_a,u_a)+\epsilon+a_m, \\ \hat{x} &= E(z_a,u), \quad u_a = P(\hat{x})+a_a. \end{aligned}$$

其中, x_a, u_a, z_a 表示被攻击者篡改后的状态量、控制信号、量测值, a_m 表示攻击者注入的量测偏移量, a_a 表示攻击者注入的控制偏移量.

无论是物理破坏还是网络攻击引发的信息物理综合安全威胁, 当其利用 CPS 的业务特性在系统内实现故障的传播, 都将影响 CPS 的整体安全, 造成巨大的损失. 因此, 需要通过仿真技术充分模拟系统结构与攻击基础, 建立有针对性的防御策略.

2.3 电力系统安全仿真技术概述

2.3.1 电力系统安全仿真技术发展

作为 20 世纪最伟大的工程技术成就之首 [20], 电力系统是世界各国维护社会稳定、经济正常运行的重要基础设施. 我国在《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》中提出 “加强重点城市和用户电力供应保障, 强化重要能源设施、能源网络安全防护”. 保障

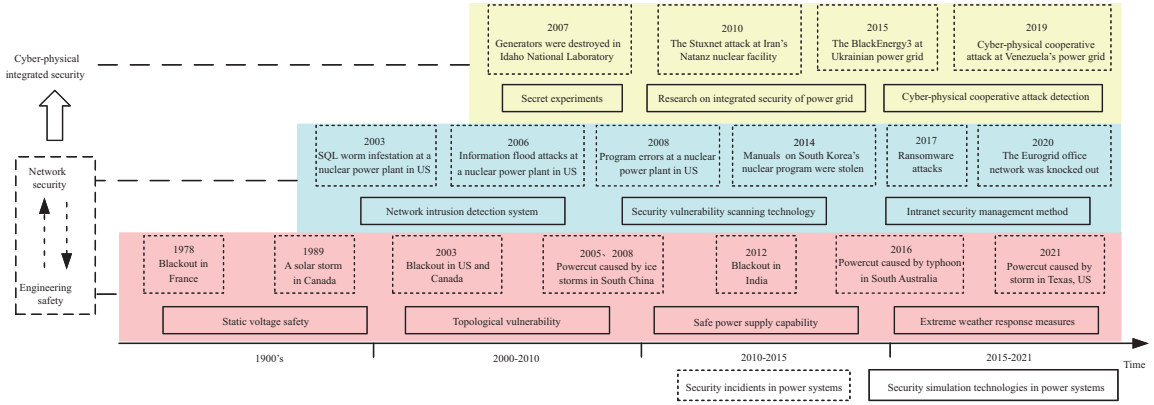

图 2　电力系统安全事件与安全仿真技术发展

Figure 2　Security incidents and development of security simulation technologies in power systems

电力基础设施的安全可靠运行对维护社会稳定、生产高效和国家安全意义重大 [21]. 通信网络与传统电网的深度融合, 以及电力系统应用场景的逐步拓展推动了电力系统安全需求的深刻变革 [22, 23]. 如图 2 所示, 伴随着 3 类电力系统安全事件的发生, 3 类电力系统安全仿真技术先后出现, 并不断演进和发展.

电力系统工程安全仿真技术通过建立物理模型模拟原始电力系统, 并采用模型驱动、数据驱动等方法进行研究和计算, 主要关注电力系统的物理特征及其脆弱性. 在 20 世纪 60 年代以前, 工程安全仿真主要使用实物对电力系统进行动态模拟. 1973 年, 我国在电力系统仿真程序领域实现突破, 解决了 330 千伏超高压输电工程 (刘天关工程) 运行的新问题. 近年来, 可再生能源并网、用户需求侧响应等新场景给电力系统的稳定可靠运行提出了新的挑战. 借助工程安全仿真技术, 可以对各类场景进行安全分析和极限测试, 保障新场景下系统运行的可靠性.

电力系统网络安全仿真技术通过建立网络模型模拟实际网络行为, 研究电力信息系统网络特征及其脆弱性. 能源互联网等技术的发展使得目前电力信息系统的防护边界逐渐模糊. 大量来自互联网的攻击已威胁到电力系统业务的正常运行. 将传统网络仿真技术引入到对电力信息系统的安全分析中, 有助于加深对电力通信场景安全威胁的理解, 提升电力信息安全防护水平.

电力系统综合安全仿真技术将物理实体与计算单元进行融合仿真, 模拟物理系统与信息网络紧密交互的电力信息物理融合系统, 研究物理域能量与信息域数据交互过程中的耦合机理及其脆弱性. 综合安全仿真技术主要面向电力系统的跨域安全问题, 研究内容包括接口数据传输安全性、网络攻击对电力物理系统的影响等. 为研究电力系统安全威胁的跨域耦合机理, 需要考虑物理系统和信息系统的安全防护机制, 同时要对两类系统间的数据交互模式进行分析. 由于仿真建模难度大, 目前电力系统的综合安全仿真仍然处于探索阶段, 缺乏高度一体化的综合安全仿真框架. 由于工程安全仿真与网络安全仿真发展相对成熟, 研究人员通常使用联合仿真技术将两类安全仿真方法相结合, 以分析信息物理综合安全事件的安全风险.

2.3.2　电力系统安全仿真技术途径

从技术途径来看, 电力系统安全仿真技术包括基于实物设备仿真、基于数值模拟仿真、基于半实物仿真等实现方案. 基于实物设备的仿真采用全物理的实物装置可以在连续时间上观测实际的动态过程, 将被研究的大规模电力系统各部分进行同比例的缩减. 然后建立本质上相近的物理模型系统, 通

过缩减后的仿真物理模型代替实际系统. 爱达荷国家实验室 (Idaho National Laboratory, INL) 的电网仿真环境占地 2305 平方千米, 运行着独立自主的电力传输和配电系统, 包括变电站, 控制中心, 138, 35, 25, 15 kV 的多重配电线路等, 能够进行电网可靠性、控制系统闭环测试等安全研究[3)]. 基于实物设备的仿真现象直观易懂, 物理过程也可以与实际情况对应, 数据可靠, 但实物部署成本较高, 仿真规模受限, 而且可扩展性与兼容性较差.

基于数值模拟的仿真系统内的所有元件都采用数字仿真模型, 模拟物理系统的仿真软件包括 RTDS, RT-LAB 等, 模拟信息系统的仿真软件包括 NS-2, OPNET 等. 基于数值模拟的仿真计算速度快、使用灵活、成本低廉, 但对于计算方法和计算机运算处理速度的要求很高, 较难对电力系统进行完整的物理过程建模. 数字孪生技术正是探索如何在信息空间中建造物理设备的数字镜像.

半实物仿真将部分实物元件引入计算机仿真回路中, 比基于数值模拟的仿真方案更加逼近实际系统运行状态. 目前, 许多仿真软件都提供了与实际设备进行数字量与模拟量交互的接口. 在电力系统中, 通常把交流输电线路、变压器、直流输电换流阀组和控制装置等难以精确建模的部分直接引入到仿真回路中, 以提高仿真过程的可信程度; 与此同时, 用数字仿真系统模拟模型精度较高的发电机、电动机、控制系统等元件, 以降低仿真成本和时间. 对于现阶段的安全仿真技术而言, 使用实物设备与数值模拟相结合的半实物仿真方案, 不仅实现难度较低, 同时能带来更好的可视化效果, 使得安全威胁清晰可见.

通过总结上述电力系统安全事件和仿真技术的发展过程可知, 电力系统面临的安全威胁持续变化且差异显著, 安全威胁的形态正在从以物理故障为主的工程安全事故, 到信息通信系统中的网络安全事件, 进一步扩展到涉及物理系统与信息系统交互影响的综合安全事件; 安全事件促使运行人员和研究者更深入地探究安全威胁的原因和消除的方法, 进而推动电力系统安全仿真技术发展. 与此同时, 随着理论、工程、计算等能力的提升, 以及电力系统业务场景的丰富, 电力系统安全仿真技术在实物仿真、数值模拟和半实物仿真等实现方案中不断迭代发展.

3 面向工程安全的电力系统仿真技术与平台

3.1 电力系统工程安全仿真技术

按照仿真技术的实现途径, 电力系统工程安全仿真技术可分为动态模拟仿真、数字软件仿真和数模混合仿真, 如表 1 所示. 其中, 动态模拟仿真是指基于相似理论搭建实物平台来进行仿真; 数字软件仿真是指建立反映电力系统运行机理的物理模型, 继而通过求解各种代数、微分或偏微分数学方程得到电力系统的状态特征的方法, 包括离线仿真、实时仿真、云仿真和数字孪生; 数模混合仿真是实时仿真器和真实设备相结合的仿真形式, 其支撑技术主要包括模数转换、接口算法等.

3.1.1 动态模拟仿真

基于电力系统的高可靠性要求和试验安全性的考量, 无法在真实电力系统上进行相关试验研究. 动态模拟仿真是最早的电力系统仿真技术. 电力系统动态模拟仿真是指按照相似理论 [24] 搭建与真实电力系统相似的仿真模型, 仿真模型中的电机、输电线路、变压器、负荷等设备均按比例进行了缩小, 借助仿真模型中的研究结果, 推断出真实电力系统的特征和规律. 曾用于研究远距离输电的串联补偿、同步发电机的自励磁、负荷特性、同步电机的频率特性等问题. 目前的动态模拟仿真技术主要用于: 继电保护及安全自动装置、配网自动化及微网系统试验; 设备物理模型的研究与验证; 设备投入使用前

3) Laboratory I N. Grid resilience. https://www.inl.gov/research-programs/grid-resilience/.

表 1　电力系统工程安全仿真技术对比

Table 1　Comparison of power system engineering safety simulation technologies

	Physical simulation	Numerical simulation	Hardware-in-the-loop simulation
Simulation category	Dynamic simulation	Digital software simulation	Digital-analogical hybrid simulation
Simulation theory	Similarity theory	Differential equation	Digital-to-analogue conversion
Simulation method	Scale down to infer the characteristics and laws of the real power system	Offline simulation, real-time simulation, cloud simulation, digital twin	Most of the components are digitally simulated; the objects which are difficult to model are simulated dynamically

表 2　离线仿真中 3 种仿真方法对比

Table 2　Comparison of three simulation methods in offline simulation

	Electromagnetic transient process	Electromechanical transient process	Medium and long term dynamic process
Simulation step size	20∼200 μs	About 10 ms	From 10 ms to a few seconds
Simulation scale	Smaller	Larger	Larger
Research scope	Resonance transient, transient state caused by lightning strike, power electronic devices and fast transient in HVDC transmission	Transient stability after large disturbance (short circuit fault, cutting circuit, generator, load, etc.) and static stability after small disturbance (load fluctuation)	Post-hoc analysis of complex and serious accidents, research on the effectiveness of emergency reactive power support, research on automatic generation control, etc.
Simulation software	EMTP, EMTDC, NETOMAC	BPA, PSASP, PSS/E	EUROSTAG, LTSP, EXTAB

的验证试验. 由于动态模拟仿真模型建设成本高、难以模拟复杂系统、仿真规模难以扩展、存在安全风险等, 研究者希望通过数字仿真系统实现相关功能 [25].

3.1.2　数字软件仿真

(1) 离线仿真. 伴随着计算机的发展, 20 世纪 60 年代开始出现数字仿真技术. 20 世纪 60 年代末至 70 年代中期, 发电机、励磁系统、原动系统等模型取得了突破性成果, 开始出现针对电力系统的离线仿真. 电力系统离线仿真的仿真速度与实际系统的动态过程不等. 目前, 电力系统离线仿真软件对不同的动态过程采用不同的仿真方法, 主要有电磁暂态过程仿真、机电暂态过程仿真和中长期动态过程仿真 3 种 [26]. 3 种仿真方法的比较见表 2.

电磁暂态过程数字仿真是用数值计算方法对电力系统中从数微秒至数秒之间的电磁暂态过程进行仿真模拟的. 机电暂态过程的仿真, 主要研究电力系统受到大扰动 (短路故障, 切除线路、发电机、负荷等) 后的暂态稳定和受到小扰动 (负荷波动等) 后的静态稳定性能. 电力系统中长期动态过程仿真是电力系统受到扰动后较长过程动态仿真, 要计入在一般暂态稳定过程仿真中不考虑的电力系统长过程和慢速的动态特性 [26].

(2) 实时仿真. 实时仿真是指仿真器在真实系统运行的相同时间内, 准确地产生内部变量和仿真输出. 实际上, 在给定时间步长上完成物理模型求解所需的时间必须短于该时间步长的挂钟时长, 这将允许实时仿真器执行相关的所有必要操作, 如与外部连接设备之间的数据交换 [27].

在 20 世纪 90 年代初, RTDS 公司使用数字信号处理器 (digital signal processor, DSP) 开发了第一个商业实时数字模拟器 (RTDS) [28]. 随后, 法国电力公司 EDF 推出了他们的第一款实时仿真器 ARENE [29]、加拿大 HYDRO-QUEBEC 公司开发了实时仿真器 HYPERSIM [30]、加拿大 Opal-RT 公司开发了实时仿真器 RT-LAB. RT-LAB 是一个基于模型的工程设计和测试仿真平台, 应用 RT-LAB 可以把复杂的系统模型简化分解成多个并行执行的子系统模型, 再把这些子系统模型分配到多个目标机节点 (或 CPU) 上, 从而构成一个可伸缩的分布式并行实时仿真系统. 中国电力科学研究院于 2006 年开发完成了电力系统全数字实时仿真装置 (advanced digital power system simulator, ADPSS), 该装置能够实现大规模电力系统电磁暂态仿真和机电暂态仿真的混合仿真, 是世界上第一个可模拟大规模电力系统的实时数字仿真装置 [31].

虽然实时仿真器可以通过增加仿真资源模拟更大规模的电力系统, 但其仿真资源难以灵活变更, 当仿真规模较小时, 并不需要所有的仿真资源, 会造成仿真资源的浪费. 此外, 实时仿真器成本较高. 因此, 需要开发一个仿真规模可弹性扩展且廉价的仿真平台.

(3) 云仿真. 当前电力系统的计算分析依赖于基于本地的集中式平台, 计算能力有限、可扩展性差、升级成本高、网络利用率低. 随着分布式能源、微电网等场景中数据的爆炸式增长, 如果没有及时有效地计算, 将极大地影响智能电网的运营和规划活动. 显然, 本地的集中式平台不具备存储和计算大量系统数据的能力, 需要构建新的电力系统计算平台以支持智能电网的实现. 电力系统运营中应用云计算是解决上述问题的有效方案.

近年来, 电力系统应用与云计算的集成也越来越受到关注. 文献 [32] 探索了在公共云计算服务上运行电力系统仿真的可行性, 然而, 他们的研究并没有完全解决安全和隐私问题; 文献 [33] 证明了使用云计算收集和处理同步相量数据的可行性; 文献 [34] 利用远程云服务器来获取、监控和控制实时电力系统数据, 以提高控制和响应时间; 文献 [35] 探讨了美国首个基于云的生产级电力系统仿真平台的开发和实施经验; 中国电力科学研究院开发的电力系统云仿真系统在国内外同类专业领域内处于开拓地位, 已经先后在山东、河南、新疆、宁夏等多家电网单位完成示范应用, 并于 2020 年正式对外发布了 PSASP.net 电力云仿真平台, 集成了成熟的商用软件 —— 电力系统分析综合程序 (power system analysis synthesis program, PSASP) 的诸多模型和算法, 元件种类丰富, 可以实现短路计算、潮流计算、机电暂态分析等主要功能.

(4) 数字孪生. 由于智能电网自身的复杂性, 简单沿用传统电网的建模仿真方法已经难以满足智能电网规划、设计、运行和维护的要求, 亟需发展新的理念和方法. 数字孪生是融合物联网技术、通信技术、大数据分析技术和高性能计算技术的先进仿真分析技术, 有助于解决当前智能电网发展面临的技术问题. 美国国家航空航天局 (National Aeronautics and Space Administration, NASA) 对数字孪生的定义为 “充分利用物理模型、传感器更新、运行历史等数据, 集成多学科、多物理量、多尺度、多概率的仿真过程, 在虚拟空间中完成映射, 从而反映相对应的实体装备的全生命周期过程” [36]. 由中华人民共和国工业和信息化部发布的《数字孪生应用白皮书 2020》将数字孪生定义为具有数据连接的特定物理实体或过程的数字化表达, 该数据连接可以保证物理状态和虚拟状态之间的同速率收敛, 并提供物理实体或流程过程的整个生命周期的集成视图, 有助于优化整体性能 [37].

离线仿真、实时仿真、云仿真均是通过构建基于假设、简化的电力系统物理模型, 继而通过求解各种代数、微分或偏微分数学方程得到电力系统的状态特征, 物理模型和物理实体之间没有实时数据

表 3　电力系统工程安全仿真平台

Table 3　Power system engineering safety testbed

Power system section	Main security problems	Simulation technology
Generation side	Stator winding fault diagnosis [45~47], rotor winding fault diagnosis [48~50]	Dynamic simulation [45, 46, 48, 49], digital software simulation [47, 50]
Transmission side	Fault type discrimination [51], fault location [52, 53], relay protection scheme [54~56]	Digital software simulation [51~55], digital-analogical hybrid simulation [56]
Substation side	Fault analysis [57~59], fault detection [60, 62], transformer protection [61]	Dynamic simulation [57, 59, 60, 62], digital software simulation [58, 61]
Distribution side	Impact analysis of distributed power supply access [63, 64], fault analysis [66], access plan [67], relay protection [68]	Digital software simulation [63~68]

的传输, 属于静态模型. 这种模型驱动的研究方法面临无法回避的弊端: 首先, 物理模型难以同时满足仿真速度和仿真精度的要求; 其次, 物理模型之间存在误差传递和误差累积. 而数字孪生采用的模型形式并不局限于模型驱动的微分方程, 同时也涵盖数据驱动的相关性分析. 数字孪生不仅对物理实体进行刻画, 而且与物理实体间存在双向数据传输. 一方面, 物理实体的状态数据被传递给数字孪生, 以一种主动、自适应的方式, 利用大数据优势对数字孪生的物理模型进行优化调整, 从而更加精确地描述物理实体. 另一方面, 数字孪生在数字空间完成的仿真、优化结果也可反馈给物理实体以指导真实决策.

近年来, 数字孪生已被初步应用于电力系统领域, 具有良好的发展前景. 文献 [38] 介绍了中压电缆建模在风电场数字孪生中的应用. 文献 [39] 研究如何使用数字孪生对信息物理能源系统进行异常检测. 文献 [40] 讨论了将数字孪生在 EMS 中应用的适用性. 文献 [41] 试图从数字孪生的角度提出新的用于电网在线分析的体系结构及其相关的支持实现技术. 文献 [42] 介绍了基于数字孪生的电力系统稳态建模、仿真和分析.

3.1.3　数模混合仿真

20 世纪 70 年代初出现数模混合仿真的概念, 然后逐渐应用在电力系统仿真领域. 初期阶段, 除发电机、电动机等旋转元件用数字仿真模拟外, 其余静止元件采用动态模拟仿真方法进行模拟. 20 世纪 90 年代之后, 随着全数字实时仿真器的出现与发展, 该阶段的数模混合仿真中大部分元件采用数字仿真模拟, 将需要研究的或建模不完善的元件采用动态模拟仿真方法模拟, 主要用于传统继电保护装置、安全自动装置验证试验. 随着新能源并网、特高压输电、柔性直流输电等技术的应用, 日益复杂的能源结构和电力结构、大量的电力电子设备和高速开断频率等因素使得依靠全数字实时仿真难以进行相关研究 [43, 44], 同时数模接口技术如数模转换技术、接口算法研究、光纤数字通信技术的发展也将支持更多电力电子设备接入实时仿真器, 数模混合仿真为相关的研究提供了真实可靠的解决方案.

3.2　电力系统工程安全相关平台

根据电能从生产到分配的传输过程, 可将电力系统分为发电、输电、变电、配电等 4 个环节. 下面分别简要介绍发电侧、输电侧、变电侧和配电侧典型的工程安全问题及仿真平台, 如表 3 [45~68] 所示.

3.2.1 发电侧相关平台

发电机故障是发电侧工程安全问题的研究重点, 而发电机故障又主要分为定子绕组短路故障和转子绕组短路故障. 当定/转子绕组发生短路故障时, 如果无法尽快解决, 则可能会导致严重事故并严重威胁发电机和电网的安全运行. 发电机的安全稳定运行是确保电力系统可靠供电的关键, 因此, 尽早对发电机定/转子绕组短路故障进行故障诊断非常必要.

文献 [45] 提出基于 Park 矢量法的定子绕组故障诊断方法, 利用三相感应电机组成的测试台进行了实验验证. 文献 [46] 利用轴向节流磁通量的变化, 开发了定位故障线圈位置的算法, 并采用发电机和电动机组成的实验装置加以验证. 文献 [47] 提出以负序电流作为故障特征量进行故障诊断, 在 Ansoft Maxwell 有限元分析软件中对定子绕组匝间短路故障进行模拟, 验证了该故障诊断方法的有效性.

文献 [48] 提出了一种基于 Volterra 核辨识的同步发电机转子绕组匝间短路故障诊断方法. 采用原动机和同步发电机组成的动态模拟装置进行匝间短路故障实验, 验证了该方法的有效性. 文献 [49] 提出了一种利用频谱和双谱分析来检测转子绕组匝间短路故障的技术, 并采用动态模拟实验机组的匝间短路故障记录数据加以验证. 文献 [50] 提出一种用于检测三相绕线转子感应电机中转子电气故障的新方法, 通过 MATLAB/Simulink 仿真和实验室规模的实验测试进行了验证.

3.2.2 输电侧相关平台

输电线路由于分布较广, 容易受到雷电、冰灾、暴风、鸟害、高杆植物等各种自然及外部因素的影响而发生故障. 针对输电线路故障的故障类型判别、故障测距以及继电保护是快速消除故障的有效方法.

文献 [51] 利用 ATP-EMPT 仿真软件对输电线路不同类型的故障进行仿真计算, 分析各类故障下电流暂态仿真波形的不同特性, 提出了故障类型判别依据. 文献 [52] 提出了一种基于小波分析的电缆 – 架空线混合输电线路行波故障测距方法, ATP 的仿真结果表明, 该方法能够测量混合线路上短路故障的距离. 文献 [53] 利用 ATP 仿真验证了一种基于两端行波的输电线路故障测距公式.

文献 [54] 提出了一种基于余弦相似度的方向比较方案, 用于架空线保护. 使用 PSCAD/EMTDC 仿真数据针对各种故障参数 (如故障类型、故障位置、故障起始角度和故障电阻) 测试了该方案. 文献 [55] 提出了一种针对柔性直流输电的输电线路综合保护方案, 使用 PSCAD/EMTDC 对典型柔性直流输电系统进行建模, 进行了不同故障工况下的全面仿真, 以验证所提保护方案的性能. 文献 [56] 提出了一种基于单端初始行波的保护方案, 设计并实现了保护设备原型, 并与 PSCAD 中的直流输电系统仿真模型形成数模混合仿真, 仿真各种传输线故障以验证原型设备的性能.

3.2.3 变电侧相关平台

电力变压器是变电侧最关键和最昂贵的设备之一. 研究表明, 大约 70%∼80% 的变压器故障都归根到变压器内部的故障 [69].

文献 [57] 使用一台每相具有不同类型绕组的小型变压器, 研究了各种电力变压器的内部绕组谐振特性. 文献 [58] 基于 ATP-EMTP 研究了开关操作和接地故障对中压变压器内部过电压的影响. 文献 [59] 研究了各种因素 (如故障位置、负载功率因数和变压器的负载率) 对变压器内部绕组匝间故障的影响, 并在 20/0.4 kV, 50 kVA 变压器上进行了仿真验证.

对变压器内部绕组故障的检测和定位有助于采取应对措施, 减少对变压器和电力系统的潜在损害. 文献 [60] 提出了一种基于搜索线圈的变压器绕组故障在线检测方法, 基于特殊设计的 10 kVA 变压器进行了仿真实验. 文献 [61] 基于对瞬时差动电流的波形识别, 提出了一种变压器差动保护的新方

法. 在 EMTDC 软件建模的电力变压器上, 仿真各种涌入电流和内部故障电流工况, 对提出的算法进行了检验. 文献 [61] 研究了考虑谐波影响的基于瞬时电压和电流测量的在线变压器内部故障检测方法, 并通过 Maxwell 有限元软件包对变压器进行详细的非线性仿真和实验室测量来验证该检测方法. 文献 [62] 利用振动分析方法检测变压器绕组的机械故障, 并在 50 MVA 的三相电力变压器上进行了验证, 初步研究表明, 采用振动法预测变压器绕组的机械故障是可行的.

3.2.4 配电侧相关平台

电力系统中分布式电源的广泛应用对现有的配电网系统产生了深远的影响. 文献 [63] 基于 MATLAB 软件平台, 分析分布式电源的接入数量、接入位置、接入容量和功率因数 4 个影响因素对配网电压稳定性造成的影响. 分布式发电机组的接口技术分为同步发电机接口、异步发电机接口和逆变器接口, 文献 [64] 利用 PSCAD/EMTDC 仿真环境研究了不同接口技术对电力系统的暂态和电压稳定性的影响. 文献 [65] 提出一种识别电压微小扰动的方法, 并在仿真平台上在线评估了电压微小扰动对节能降压技术性能的影响. 文献 [66] 利用 PSCAD 仿真分析了在配电网发生三相、两相相间短路故障以及分布式光伏电源出力不同时, 并网逆变器输出电流的变化特性. 文献 [67] 提出一种新颖的方法, 可以在任何功率因数下确定多个分布式电源的最佳接入点和容量, 并基于 MATLAB 仿真环境进行了验证. 文献 [68] 提出分布式发电配电系统的自适应过流保护, 还提出了利用保护继电器的时间过电流特性进行故障区域检测的方法, 在 DIgSILENT 仿真环境中进行了验证.

4 面向网络安全的电力系统仿真技术和平台

4.1 电力系统网络安全仿真技术

电力系统网络安全仿真技术与传统的通信网络安全仿真类似, 但更侧重对专用协议安全性的研究, 通信技术的快速发展给电力系统协议的维护带来了全新的挑战. 例如, 变电站内部的设备多样, 不同厂家往往有不同的自定义协议; 即使协议一样, 寄存器的定义也不一样, 读写的规则不同. 为了解决各个制造厂商的变电站产品之间的互操作性问题, 国际电工委员会制定了 IEC 61850 标准, 但在当时并没有制定相关的安全性规范.

随着智能电网技术的快速发展, 大量智能设备接入电力通信网络. 运行场景的差异化使得通信网的建设、维护等难度大大增加, 仅仅依靠现场部署与调试难以取得良好效果, 而通过网络安全仿真技术能够让安全人员提前做好系统方案设计、网络规划优化等工作, 有利于防范信息系统中可能出现的网络安全威胁.

按照仿真技术的实现途径, 网络安全仿真技术可分为真实网络仿真、网络仿真器和半实物网络仿真三大类, 如表 4 所示.

4.1.1 真实网络仿真

真实网络仿真主要指通过真实网络硬件设备对网络性能、协议安全性等方面进行研究. 目前, 在电力通信系统中, 形成了以控制中心 (IEC 61970/IEC 61968)、厂站 (IEC 61850 系列) 和信息安全 (IEC 62351) 为中心的标准通信体系架构. 其中, 基于 IEC 61850 标准的通信协议主要有 3 类: GOOSE (generic object oriented substation events), SMV (sampled measured value), MMS (manufacturing message specification).

表 4 电力系统网络安全仿真技术对比

Table 4 Comparison of power system network security simulation technologies

	Physical simulation	Numerical simulation	Hardware-in-the-loop simulation
Simulation category	Real network simulation	Network simulator	Hardware-in-loop network simulation
Simulation theory	Hardware device communication	Virtual environment	Communication interface
Simulation method	Convert protocols of different devices into unified protocols	Use corresponding modeling components to construct the network model	Virtual real network combined with data flow conversion and interaction

GOOSE 主要用于智能电子设备与断路器之间的信息交换, 控制区域供电量, SMV 协议反映了变电站内部设备的运行情况. GOOSE 与 SMV 均采用组播技术, 接收端接收到数据后不需要发送确认信息, 使得未获得组员资格的非法设备可以接入, 另外, SMV 在报文处理过程中没有任何安全防护手段, 报文容易遭受恶意篡改.

MMS 协议负责智能变电站间隔层与站控层设备间的通讯, 以 TCP/IP 为基础, 这使得 MMS 对中间人攻击相当脆弱 [70]. 此外, MMS 没有加密与校验和字段, 攻击者可以对所有数据包进行读取, 也可以通过伪造校验字段实施攻击.

由于需要将不同设备生产厂商的规约转换为系统集成商所采用的规约, 规约转换器在常规变电站中非常常见. 在研究人员使用真实网络进行仿真研究时, 许多底层的电力终端设备仍然通过 RS485 串行链路进行通讯, 再使用规约转换器转换为符合 IEC 61850 的以太网通讯. 真实网络仿真与实际系统最接近, 实时性较好, 仿真结果最可信; 但部署费用较高, 仿真过程执行时间较长, 同时不便于进行变量控制和拓扑切换.

4.1.2 网络仿真器

网络仿真器为计算机模拟通信网络行为提供了虚拟环境. 通信网络的计算机仿真大体经历了 3 个阶段, 起初在 19 世纪 60 年代, 一般采用通用的计算机语言进行通信仿真研究, 如汇编语言、BASIC、FORTRAN 等, 其建模困难、编程工作量大, 且只能针对特定需求进行对应研究, 通用性不足. 自 70 年代初期开始, 开发出了 GPSS、Arena 等用于离散事件仿真的计算机语言, 虽然编程效率有所提高, 但依旧没有针对通信网络特点进行设计. 直至 80 年代中后期开始, 陆续出现了专门用于通信仿真的语言和一些专用的仿真器, 可以省去编程过程, 根据不同网络的要求, 使用对应的建模组件构筑网络模型, 因此进入 90 年代后, 开发和应用专用仿真器的发展趋势越来越明显, 网络仿真器也日益完善. 如表 5 所示, 目前用于电力系统仿真的网络仿真器主要包括 NS-2, NS-3, OPNET, OMNeT++ 等.

NS (network simulator) 起源于 1989 年美国军方的 Real Network Simulator 项目, 是最早的网络仿真器之一 [71], NS-2 是 NS 的扩展版本, 由 UC Berkeley 大学开发, 在学术界应用广泛. NS-2[4)]基于 Otcl 和 C++ 两种语言开发, Otcl 用于编写仿真模型与仿真参数的配置, C++ 主要负责执行仿真进程, 两种语言通过 TclCL 接口进行交互. 同时 NS-2 可以与真实网络进行双向的数据通信, 不仅能向外界网络发送数据, 也可以捕获真实网络中的数据包. 但是, NS-2 两种编程语言的架构较为复杂, 模块间耦合性较差, 同时, 它本身没有图形用户界面, 仿真效果不直观, 使用比较烦琐. 为了降低 NS-2 框

4) The network simulator-ns-2. http://www.isi.edu/nsnam/ns/doc/index.html.

表 5 网络仿真器对比

Table 5 Comparison of network simulators

	NS-2	OPNET	OMNeT++
Open source	√	×	√
Graphical interface	×	√	√
Support for co-simulation	√	√	√
Support for real-time simulation	√	√	√
Simulation speed	Slower	Medium	Faster
Programming language	Otcl, C++	C	C++
Predefined model	More	More	Less
Network architecture	Complex	Layering	Layering
Operation document	Scattered	Real-time update	Real-time update

架的复杂度, NS-3 完全基于 C++ 开发, 并且提供了大量 Python 接口的仿真模块, 降低了用户的编程复杂度, 但 NS-3 内置的模块不完善, 需要用户对其进行扩展, 此外, NS-3 还提供了可视化界面和数据分析工具, 支持分布式仿真和并行仿真.

OPNET[5)]最早于 1986 年由麻省理工学院研究开发, 是目前最先进的网络仿真工具之一, 与其他仿真软件相比, OPNET 预定义模型较多, 极大地降低了开发难度, 易于使用, 其仿真架构为从低到高的层次架构, 仿真模型可以看作由消息传递机制进行交互的多个子系统相连而成的分布式系统. OPNET 采用系统在环机制, 可以与真实网络的软硬件进行交互, 实现半实物网络仿真.

OMNeT++[6)]是一个用于离散事件建模的开源工具, 它与 OPNET 许多特性相同, 不过它支持自定义和参数化拓扑, 因此 OMNeT++ 具有较高的灵活性和可扩展性, 并且它的程序兼容性很好, 其他软件编写的仿真程序经过少许修改就可以应用到 OMNeT++ 中.

4.1.3 半实物网络仿真

半实物网络仿真将虚拟网络与真实网络相结合, 进行虚实网络数据流的转换与交互. 虽然网络仿真器能够在一定程度上对电力信息系统安全性进行测试, 但仍不能满足对现实环境的精确模拟, 因此将虚拟网络接入真实网络, 整合为半实物网络, 可以更直观、精确地进行网络数据流的交互. 半实物仿真通过接入真实物理设备, 避免了建模困难, 同时内部模拟环境具有良好的可扩展性, 因而半实物仿真比真实网络仿真成本更低, 重复实验更加容易, 也比网络仿真器的算法检验结果更具备真实性, 真实与虚拟两个层次的结合令大规模网络仿真成为可能.

由于真实网络系统的数据格式是真实的数据流, 而仿真器中的协议是模拟构造的, 无法直接与真实数据流进行通信交互. 因此, 半实物仿真的一项关键技术便在于通过通信接口实现数据交互过程. 目前, 半实物仿真方法包括高级体系架构 (high level architecture, HLA)、系统在环 (system in the loop, SITL) 以及外部系统接口 (external simulation access, ESA). HLA 是一种分布式仿真体系结构标准, 由美国国防部 (United States Department of Defense) 在 1996 年正式推出, 目前在 OPNET, NS2 等主流仿真软件中均有提供. 在 HLA 框架下, 通过支撑环境提供的接口, 各仿真对象构成一个开放性的分布式仿真系统, 但这种方法还需要运行的支撑环境, 一般不用于仿真网络与真实设备的直连仿真; SITL 是 OPNET 开发的附加模块, 它可以将物理网络接口与虚拟网络中的网络地址相映射, 使真实设备与

5) OPNET Technologies, Inc. http://www.opnet.com/.
6) OMNeT++ Homepage. http://www.omnetpp.org/.

表 6 电力系统网络安全仿真平台

Table 6 Power system network security testbeds

Network security elements	Main security problems
Confidentiality	Intrusion detection [73~78], encryption scheme [79~82]
Availability	Software defined network [83, 84], network communication performance [85~87], communication protocol development [88~91], SYN attack [92~94], DoS attack [95~98]
Integrity	Delay attack [99, 100], replay attack [101~103], man-in-the-middle attack [104~106]

仿真网络直接进行交互, 形成统一的整体进行协同仿真, 因此更适合 OPNET 与真实网络设备的直连仿真; ESA 支持用户根据自身需求进行二次开发, 完成自定义接口, 但需要开发人员对仿真器的工作机制与原理有较为深入的了解, 开发工作量大.

半实物网络仿真结合了真实网络与网络仿真器的优势, 不仅提高了仿真精确度, 又大幅降低了研发成本, 用户可根据自身需求选择对应的仿真方法.

4.2 电力系统网络安全相关平台

按照美国国家标准与技术研究院 (National Institute of Standards and Technology, NIST) 提出的网络安全三要素 [72], 本文将电力系统网络安全问题分为保密性、可用性和完整性三大类.

保密性是指信息只能被对应权限用户访问, 保密性被破坏会造成数据泄露, 机要信息容易被非法利用. 具体攻击方式包括破译密码、恶意病毒、社会工程攻击等. 保密性攻击门槛低, 是现实中最为常见的电力系统攻击手段, 因此相应的研究工作较少.

可用性是指任何时刻数据都能被正常访问. 首先应保证系统正常稳定运行; 其次, 若系统发生故障, 控制中心仍需要对突发事件作出及时反应, 使得数据传输不受影响, 则认为可用性良好, 破坏可用性的攻击手段有延时攻击、通信线路攻击、拒绝服务攻击等.

完整性是指数据在传输过程中需要保证前后一致, 任何未经授权的用户不得修改数据状态, 否则会造成决策中心出现错误判断. 常见的攻击方式包括中间人攻击、重放攻击等. 完整性攻击可分为针对通信数据与针对电力数据两类. 其中, 针对电力数据的完整性攻击可利用系统控制流程, 将网络安全入侵手段与物理安全机理相结合, 达到更强破坏性的目的.

对于电力系统中各类网络安全问题, 国内外学者进行了大量仿真研究, 并搭建了相应的仿真平台, 如表 6 [73~106] 所示. 本文将对各研究领域的网络安全仿真平台进行简要介绍.

4.2.1 保密性仿真平台

保密性的研究大多集中于入侵检测方面. 文献 [73] 提出一种基于同步量测量和网络数据包特性的异常检测体系结构和方法, 并通过仿真平台进行评估. 文献 [74] 针对变电站的网络入侵威胁, 开发了支持单个或多个变电站同时进行异常检测的仿真系统, 该系统包含基于主机和基于网络的异常检测方法. 文献 [75] 的仿真平台主要模拟了变电站、控制中心两部分. 作者同样基于 Snort 开发了基于规则的入侵检测系统, 可以分别检测 SCADA 系统攻击的各个阶段. 文献 [76] 将能源管理系统与入侵检测机制相结合, 评估能源管理系统在面对入侵时的结果. 除了传统的入侵检测方法外, 目前也有大量使用机器学习方法检测入侵行为的研究工作. 文献 [77] 的仿真平台模拟了通信网络、电源系统、拓扑、控制器等, 提出一种自学习的入侵检测方法, 并对 3 种不同的黑客攻击进行验证. 文献 [78] 使用 Idaho 的 CPS 安全仿真平台 [107], 通过主成分分析与支持向量机相结合的方法检测了物理和网络入侵行为.

除了入侵检测外, 还存在对电力系统中病毒、加密进行研究的工作. 本文作者团队提出基于动态密码的智能电网无线通信加密方案, 使得攻击者无法获取动态加密密钥的更新 [79]. 文献 [80] 使用基于哈希日历的区块链体系结构保护电力系统应用程序的数据交换, 并验证其可行性. 文献 [81] 提出了一种可用于保护智能电网下行多播通信的基于属性的签名加密方案, 允许身份验证, 作者在高级计量架构 (advanced metering infrastructure, AMI) 仿真平台上进行了验证. 文献 [82] 针对信息泄露问题, 提出了一种使用 Paillier 密码系统以及 ECDSA 和 OpenSSL 证书进行双重因素身份验证的系统, 并通过真实网络与 NS-3 两种方法搭建了仿真网络, 进一步论证了 NS-3 与实际网络的区别.

4.2.2 可用性仿真平台

系统可用性研究可分为两方面: (1) 新框架、新协议能否稳定运行; (2) 遭受可用性攻击后系统的运行情况.

(1) 新方案稳定性研究. 文献 [83] 提出了一种基于软件定义网络 (software defined network, SDN) 的灵活、动态的网络控制方法, 可同时满足配电网和输电网的特定通信要求, 并搭建了 SDN4SmartGrids 仿真平台, 分析故障情况下 SDN 的优势. 文献 [84] 开发了网络仿真实验台, 通过自动发电控制 (automatic generation control, AGC) 的网络流量性能, 评估 SDN 技术的可用性.

文献 [85] 对电力系统中通信链路故障进行了详细分析, 提出了一项新的 IEC 61850 变电站自动化方案, 并在仿真平台上比较不同故障检测和故障恢复策略的性能, 文献 [86] 专门搭建了实时仿真平台, 并提供了完整源代码, 用于评估电力线通信与无线通信的组合方案, 文献 [87] 建模了 IEC 61850 的逻辑节点, 以便扩展仿真平台的规模, 并在 PowerCyber 仿真平台上 [108], 通过 GOOSE 与 MMS 协议的通信性能验证可行性.

文献 [109] 搭建了用于开发和测试电力电子设备组件之间通信的仿真平台, 平台可以比较和评估不同的通信方法. 文献 [88] 提出了一种轻量级通信机制 SeReCP, 不仅通过理论证明其可用性以及防范 DDoS (distributed denial of service) 等网络攻击的能力, 也在真实的仿真平台 NorNet 上实测了其有效性. 文献 [89] 在多跳无线电力通信网上测试了 RPL 协议的性能. 文献 [90] 研究通信基础设施与电力系统的集成方案, 采用 TCP/IP 的 DNP3 协议建立电气设备之间的连接以进行数据交换, 能够满足消息传递的时序要求. 文献 [91] 针对分布式电源与设备的分组问题, 提出了一种具有新的时序自适应分组协议的智能时序调整算法, 作者开发了硬件在环仿真平台, 验证其 TAG 协议能够保证动态分组成功.

文献 [110] 将 NS-3 网络仿真器与相量测量装置 (phasor measurement unit, PMU)、相量数据集中器 (phasor data concentrator, PDC) 集成到 iPaCS 仿真平台中, 考虑延迟与带宽对广域测量和监视系统数据流控制的影响, 并评估了各种网络拓扑的性能. 文献 [111] 评估了 4G 网络用于车联网的通信性能与传播延迟. 文献 [112] 使用硬件在环与软件在环方案, 考虑广域监视与控制系统的时延效应. 文献 [113] 针对配电网系统搭建了混合仿真平台, 包括配电网仿真、网络仿真、控制单元以及监测单元等, 作者首先分析平台的固有延时与协议耗时, 再针对电力设备与通信网络分别进行半实物仿真, 最后使用分布式协同控制对整体架构进行综合仿真.

(2) 可用性攻击研究. 文献 [92] 基于 IEC 61850 变电站通信网络的 SDN 框架开发了一个安全评分模型, 使用 SDN 缓解网络拥塞, 并在 GENI [114] 平台上测试了模型应对 SYN 洪泛攻击的性能. 文献 [93] 使用 NS-3 与树莓派进行交互仿真, 模拟 AMI 网络中传感器、智能电表和数据收集服务器的体系结构, 测试 SYN 洪泛攻击对电表与服务器间通信造成破坏的效果. 文献 [94] 使用 PowerWorld 实现电网仿真, 使用 OPNET 与 RINSE 实现通信仿真与网络攻击, 模拟了 SYN 洪泛攻击对网络包与电力

系统的影响, 该攻击可能会导致电网发生连锁故障.

文献 [95] 将网络攻击和保护方案应用于直流配电网络, 测试通信计算资源耗尽、异常数据量增加以及 DDoS 攻击对电力系统的影响. 文献 [96] 提出一种适用于安全仿真的 SCADA 仿真环境 (SCADA-SST), 评估 SCADA 受到 DoS 攻击后的恢复能力. 文献 [97] 提出了一种分布式入侵检测系统 (D-IDS) 的体系结构和算法, 用于检测 Modbus 通信中的异常情况, 并在 PowerCyber 安全仿真平台 [108] 的基础上进行改进, 对各种类型的 DoS 攻击与完整性攻击进行评估. 文献 [98] 使用 RTDS、同步相量设备、电压稳定装置、NS-3、DeterLab [115] 等, 搭建了实时硬件在环仿真平台, 演示了通信线路中断、DoS 攻击和中间人攻击对电力系统的影响.

4.2.3 完整性仿真平台

完整性攻击的最终目的大多是篡改量测数据或控制指令. 因此, 完整性仿真平台主要对此进行研究.

文献 [99] 研究了精确时间协议 (precision time protocol, PTP) 在设计时安全性不足的问题, 并设计了一种检测利用虚假 PTP 同步消息传递伪造时间戳的方法. 文献 [100] 通过将控制指令人为延时, 找到不同电网可容忍的延迟, 进而减轻智能变电站被远程控制命令攻击的后果.

文献 [116] 将重点放在互连的联合仿真平台, 在广域保护安全的情况下验证异常检测的性能, 作者利用多个实验室平台模拟电力系统的不同部分, 并实施完整性攻击, 从而分析如何将丢包率最小化. 文献 [117] 使用 Purdue 参考模型 [118] 对 Idaho 安全仿真平台 [107] 进行建模, 并发动 ARP 中毒攻击. 文献 [101] 搭建了基于 IEC 61850 的用于模拟变电站的仿真平台, 以 GOOSE 通信为目标, 实施了组播协议重放攻击与修改控制指令攻击. 文献 [102] 根据 IEEE C37.118.2 同步相量通信标准中的关键漏洞, 研究如何对同步相量设备执行丢包、重放攻击, 并开发了分布式入侵检测系统, 可以检测隐匿的网络攻击.

为了解决电力系统应用安全需求, DNP3 协议已升级为 DNP3-SA (安全认证) 模块. 文献 [103] 在 DNP3-SA 基础上, 引入了相互身份验证模块, 能够有效防止重放攻击. 文献 [104] 在微电网上实施中间人攻击, 使用 FPGA 修改同步相量数据包, 对量测数据进行替换. 文献 [105] 建立配电网 CPS 仿真平台, 通过中间人攻击进行通信数据篡改, 进而严重影响故障处理结果. 文献 [106] 针对配电自动化系统, 提出基于多代理的网络攻击检测和缓解算法, 能够识别与缓解中间人攻击、配置更改攻击、DoS 攻击等.

5 面向综合安全的电力系统仿真技术和平台

5.1 电力系统综合安全仿真技术

针对电力系统的综合安全威胁通常复杂度更高、隐蔽性更强、破坏力更大, 研究电力系统的综合安全问题, 需要考虑信息系统和物理系统之间复杂的交互关系.

综合安全仿真技术发展正处于起步阶段, 缺少能够对 CPS 进行完整建模的仿真方法, 以及结构化的仿真体系. 目前通常是将工程安全仿真与网络安全仿真技术进行组合, 进而实现两类仿真各自实物、数值、半实物方法的结合, 而两类仿真各自的仿真技术已经在前文介绍, 因此本小节主要分析工程安全仿真与网络安全仿真的联合仿真技术, 联合技术框架如图 3 所示.

相关的联合仿真技术主要分为模型仿真、联立仿真、协同仿真、实时混合仿真 4 类, 如表 7 所示. 模型仿真是指通过建立一个同时反映电力系统和通信系统的模型进行仿真分析. 联立仿真是指扩展单

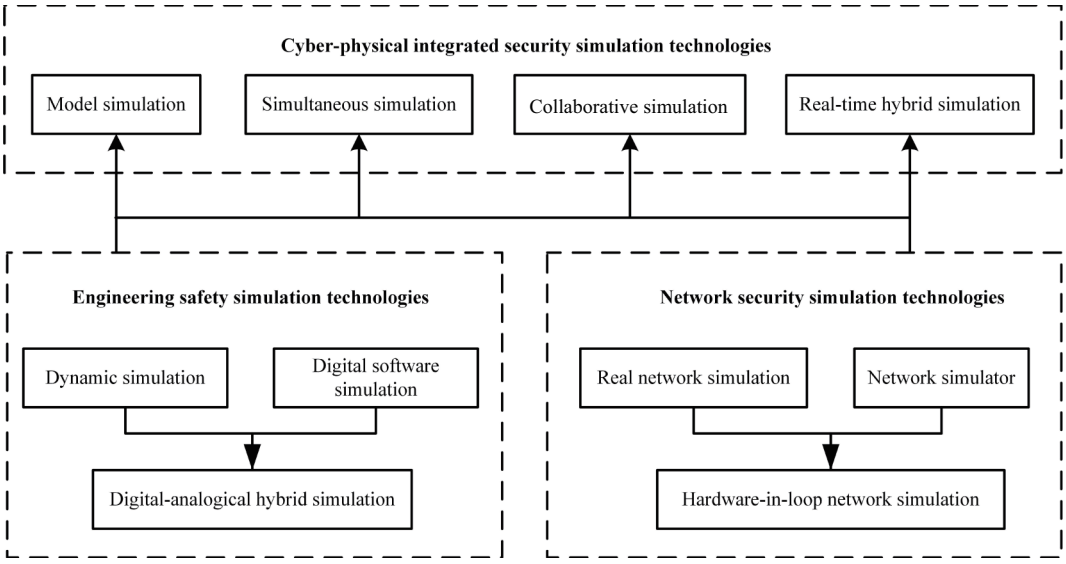

图 3　电力系统综合安全仿真技术框架

Figure 3　Power system cyber-physical integrated security simulation technology framework

表 7　电力系统综合安全仿真技术对比

Table 7　Comparison of power system cyber-physical integrated security simulation technologies

	Model simulation	Simultaneous simulation	Collaborative simulation	Real-time hybrid simulation
Simulation object	Numerical objects	Numerical and physical objects	Numerical and physical objects	Numerical and physical objects
Dedicated simulator	–	Power or network simulators	Power and network simulators	Power and network simulators
Simulation method	CPS model driven	Extend a single simulator	Time synchronization integration	Direct interface connection

个仿真器的功能, 使其能够同时模拟电力系统动力学和通信网络. 协同仿真是指将现有的电力系统仿真器和信息系统仿真器进行集成. 实时混合仿真是指将电力系统实时仿真和信息系统实时仿真相结合的仿真方式.

5.1.1　模型仿真

为了分析网络对电力系统的影响, 设计合适的 CPS 模型是非常重要的. 在这个问题上, 研究工作已经沿着几种不同的方法进行.

第 1 种方法是基于复杂网络理论对 CPS 进行建模, 通过节点和线路组成的拓扑模型抽象 CPS 模型, 从复杂网络的角度分析网络安全. 文献 [119] 开发了一个基于复杂网络的模型来理解电网发生级联故障时电力系统与通信系统的相互作用; 文献 [120] 使用从复杂网络理论中得出的 5 个指标来评估网络攻击对电力系统的影响. 在上述研究中, 通常假设一个网络中的每个节点只有在另一个网络中至少有一个支持节点时才能发挥作用, 这明显不符合电网的真实情况. 同时纯粹的拓扑模型难以准确描

述电网的实际动态特性.

第 2 种方法是将电力系统构建为系统动力学模型, 将网络攻击抽象为对模型参数 (如上传的传感器读数和下达的控制指令等) 的影响, 相关研究一般只提出面向某类特定场景的某些网络攻击 (如拒绝服务攻击、虚假数据注入攻击) 的影响分析模型. 文献 [121] 将网络攻击抽象为对功率传感器读数的篡改, 以评估网络攻击对自动发电控制的影响. 文献 [122] 对状态估计进行建模, 将虚假数据注入攻击抽象为虚假测量向量对原始测量向量的替换, 研究了不完整信息下的虚假数据注入攻击. 文献 [123] 对状态估计进行建模, 将针对 PMU 的 GPS 欺骗攻击抽象为对原始测量向量的篡改, 研究了针对多 PMU 的同步 GPS 欺骗攻击问题以及相应的辨识和校正算法. 然而, 这些模型只针对特定攻击场景有效, 可扩展性一般较差, 同时也难以支持多重网络攻击的影响分析.

5.1.2 联立仿真

联立仿真的主要思想是扩展单个仿真器的特性, 在单一系统仿真器中搭建完整系统模型, 以支持电力系统和通信网络的联合仿真. 这种方法的优点是, 时间、数据和电力/通信系统交互的管理可以在仿真器内部共享. 然而, 主要的挑战是在一个环境中组合这两个模型, 提供一个仿真界面, 为智能电网仿真模型的不同方面提供足够的细节. 这种方法可以进一步分为涉及网络模拟器扩展的方法和涉及电力系统模拟器扩展的方法. 涉及网络模拟器扩展的工具有 Agent/Plant [124, 125], SensorSim [126], 这些工具已经遇到了在精确建模和模拟动态电力系统时复杂性增加的困难. 涉及电力系统模拟器扩展的工具有 TrueTime [127, 128], Prowler [129], VisualSense [130]. 这些工具面临的主要挑战是精确建模网络的能力, 以模拟智能电网的通信网络. 然而, 采用联立仿真方法的工具都只能模拟简单的场景, 一旦电力系统或通信网络变得复杂, 它们将不能正常工作 [131].

5.1.3 协同仿真

协同仿真的主要思想是通过时间同步算法, 将电力系统仿真器和通信系统仿真器集成在相同时间域内, 利用两种仿真器各自的元件库和仿真算法, 尽可能准确模拟系统的全部组件. 电力系统仿真器和通信系统仿真器都有各自独特的仿真接口, 用于数据输入、配置、结果输出和控制等. 电力仿真器通常是连续时间驱动的, 而网络仿真器是离散事件驱动的. 因此, 设计协同仿真工具的关键挑战在于使用它们各自的仿真接口来连接、处理和同步两个仿真器, 实现数据交换和时间同步 [132]. 典型的数据交换方式有主从方式、独立数据交互与控制方式等 [133]. 典型的时间同步方式有主从同步、时间步进同步、全局事件驱动同步等 [132]. 表 8 [134~142] 总结了协同仿真的相关工作.

事实上, 仿真开发工作的大部分时间都被投入到对智能电网额外特定组件的建模中. 协同仿真可以重用已经实验验证过的现有仿真模型和算法等, 减少了开发时间和错误风险, 但是分别运行电力系统和通信系统仿真器并实现它们之间的时间同步, 很可能会导致性能损失.

5.1.4 实时混合仿真

协同仿真平台存在一个固有的问题, 即时间同步和数据交换耗时较长, 仿真速度相对较慢. 同时协同仿真平台还无法进行硬件在环的相关实验. 为了解决上述问题, 实时混合仿真是一个有吸引力的解决方案. 实时混合仿真将电力实时仿真和通信实时仿真相结合, 由于两者都是实时仿真, 因此不需要进行时间同步.

电力实时仿真器, 如 RTDS 和 RT-LAB. RTDS 是实时混合仿真的首选专用平台, 它能够执行设备的闭环测试, 具有大量的数字和模拟信号交换端口, 可以将物理保护和控制设备连接到 RTDS 仿真器,

表 8 协同仿真相关工作

Table 8 Related work of collaborative simulation

Simulation testbed	Power simulator	Communication simulator	Synchronization method	Research content
EPOCHS [134]	PSCAD, PSLF	NS2	Marching-on-in-time	Multi-agent protection control system
PowerNet [135]	Modelica	NS2	Marching-on-in-time	Generator control
VPNET [136]	VTB	OPNET	Marching-on-in-time	Wide area monitoring, protection and control
GECO [137]	PSLF	NS2	Global event-driven	Wide area monitoring, protection and control
INSPIRE [138]	DIgSILENT	OPNET	Marching-on-in-time	Wide area monitoring, protection and control
SGsim [139]	OpenDSS	OMNeT++	Global event-driven	Economic dispatch, demand response, wide-area monitoring
ASTORIA [140]	Mosaik	NS3	Master-slave synchronization	Network attack Assessment
CPSA [141]	PowerWorld	GridSim	Marching-on-in-time	Network attack Assessment, bad data detection
HELICS [142]	GridLAB-D	NS3	Global event-driven	Distributed energy resource

以与仿真电力系统进行交互. 与 RTDS 进行交互的另一种方式是使用 GENET (千兆收发器网络通信卡), 该卡通过以太网提供实时通信链接. 与 RTDS 交换数据的最后一种可能性是直接与 GPC (千兆处理器卡) 进行交互. 对于此解决方案, 必须使用基于 Xilinx FPGA 的外部接口.

通信实时仿真器, 如 OPNET 和 OMNeT++. 当对信息物理融合的电力系统进行实时混合仿真时, 通信网络仿真器需要具备以下的功能: 与硬件在环的兼容性、电力通信网络的详细建模以及仿真的实时性能. 考虑到这些因素, 大部分研究工作选择 OPNET 来对通信系统进行建模.

虽然目前综合安全仿真平台大多是将工程安全与信息安全工具进行简单组合, 但最新的研究趋势已经开始提出物理流与信息流相结合的仿真框架, 进而提供兼容性与一体化程度更高的综合安全仿真平台, 从而更加清楚地描述电力系统中网络部分与物理部分之间的交互作用.

5.2 电力系统综合安全相关平台

随着智能电网信息化、自动化程度的提升, 电力系统将面临更严峻的综合安全威胁. 攻击者可以利用信息攻击与物理攻击相结合的手段对电力系统实施难以检测的信息物理混合攻击. 而状态估计、自动发电控制、广域监视、保护和控制等应用对于电力系统的可靠性和稳定性至关重要, 需要进行重点保护. 因此需要结合综合安全仿真平台对这类场景开展脆弱性评估、影响分析、对策开发等工作.

5.2.1 自动发电控制相关平台

AGC 回路是一种二次频率控制回路, 通过对区域间联络线流量和频率偏差进行修正, 将系统频率微调到其标称值. AGC 反馈环路中包括联络线功率和频率偏差的测量数据以及区域控制偏差 (area control error, ACE) 的控制数据, 因此自动发电控制可能会受到对测量或控制数据的攻击.

基于测量的攻击涉及对联络线和频率测量的修改, 从而导致每个区域生成器的 ACE 值计算不正确. 控制攻击是指攻击者操纵发送到发电机组的 ACE 校正值的攻击. 文献 [143] 研究中间人攻击 (测量和控制的修改) 对 AGC 的影响, 通过 Scapy 实现中间人攻击, 并利用 RTDS 仿真了攻击对频率和电压的影响. 文献 [144] 研究了虚假数据注入攻击对 AGC 的影响, 推导分析出由一系列虚假数据注入攻击组成的最优攻击, 并开发了有效的算法来检测攻击, 检测哪些传感器数据链路受到攻击, 并减轻攻击影响. 最优攻击和检测算法通过在一个 16 总线的物理电力系统试验台上的实验和基于 37 总线电力系统模型的仿真得到了验证. 该物理电力系统试验台是由一个 13.5 kVA 发电机、16 条母线以及若干负载组成的单区域 AGC 系统. 文献 [145] 使用艾奥瓦州的 PowerCyber 仿真平台, 该试验台由工业级 SCADA 硬件和软件、广域网络路由仿真器和实时电力系统仿真器混合组成. 实现对 AGC 的网络攻击, 并评估其对系统的影响, 最后验证针对该攻击所提出的防御方法的有效性.

5.2.2 相量测量单元相关平台

与 SCADA 系统相比, 相量测量单元正在为广域监测系统收集更频繁、更准确的测量结果 [146]. 与 GPS 卫星的通信为所有 PMU 提供了时间戳, 因此可以同步它们的测量, 从而大大增强了互连电源系统中的态势感知能力. 然而, PMU 或 PDC 会遭受不同类型的网络攻击, 包括拒绝服务攻击、中间人攻击、灰洞攻击、GPS 欺骗攻击, 其中 GPS 欺骗攻击是最难以检测和防御的. 文献 [147] 研究了 GPS 欺骗干扰对电压稳定监测算法的影响. 文献 [148] 介绍了墨西哥目前采用的一种特殊的基于 PMU 的自动控制方案. 结果表明, GPS 欺骗攻击可以使发电机跳闸被误激活, 从而突出了 GPS 欺骗攻击的威胁. 文献 [146] 研究了 PMU 错误数据对输电线路故障检测/定位、电压稳定监测和事件定位的影响. 文献 [149] 利用协同仿真工具 GECO 研究了网络安全对全 PMU 状态估计器的影响. 以新英格兰 39 节点系统为基础, 建立了全 PMU 状态估计系统. 在 GECO 上模拟了网络故障和恶意数据注入攻击, 揭示了全 PMU 状态估计器的弱点. 文献 [150] 使用带有硬件在环仿真的实时数字仿真器开发了广域监测系统网络物理测试台. 将真实 PMU、PDC、继电器以及行业标准的通信网络和协议与自定义的 MATLAB, Python 和 AutoIt 脚本结合在一起, 可以对 PMU 网络攻击进行仿真.

5.2.3 变电站相关平台

变电站承载着多个测量、控制和通信设施. 受损或损坏的变电站通常会同时导致受损变电站及其传输线的损失. 对变电站网络安全的早期调查 [151] 表明, 攻击者能够穿透多层防火墙和密码保护, 以获得变电站的完全控制.

CESI RICERCA 实验室试验台 [152] 展示了远程控制变电站的典型控制和通信架构, 可执行变电站 Web 服务 DoS 攻击、连接本地站点及其远程控制中心的 VPN DoS、网络钓鱼网站、病毒感染和恶意软件、入侵中央防火墙等攻击. 文献 [101] 采用预定同步时间的方式将 MATLAB 和 NS3 进行协同仿真, 研究了 GOOSE 报文的重放和修改攻击对断路器跳闸的影响. 文献 [153] 利用工业级电力仿真软件以及真实的通信网络模拟变电站局域网被攻击、断路器跳闸造成电压和频率的波动. 文献 [154] 中试验台由 2 个控制中心、2 个变电站和与爱荷华州立大学 (Iowa State University) 试验台的外部链接组成. 所有子系统均使用工业协议通过局域网连接. 该测试平台将允许对测量、控制、记录和攻击

进行仿真. 文献 [155] 描述了一个硬件在环智能电网测试平台. 它涵盖了从高压到低压的电力系统, 例如传输系统、能源管理系统、变电站自动化系统 (substation automation system, SAS)、配电管理系统 (distribution management system, DMS)、高级计量基础设施 (advanced metering infrastructure, AMI) 和分布式发电 (distributed generation, DG), 它可以模拟网络攻击对各系统的影响.

5.2.4 其他平台

除上述场景外, 综合安全平台的研究也覆盖了分布式能源、电力需求响应等能源分布和控制结构发生改变后的新场景.

分布式能源依赖于最先进的信息技术, 实现了智能化监控、网络化群控等功能, 但同时也面临严重的网络安全问题. 文献 [156] 搭建了异步实时半实物仿真平台, 实现基于逆变器的分布式能源配电系统的多速率协同仿真, 并通过该平台开发并验证了用于缓解不可靠通信影响的数据恢复算法. 文献 [157] 提出了一种基于共识的能源管理算法的新型数据完整性攻击, 攻击者仅依靠给定的本地信息, 不需要了解系统拓扑和其他全局信息即可发起攻击, 将系统误导到错误的工作状态. 文献 [158] 假设攻击者篡改分布式能源注入功率的测量值, 并提出用于缓解网络攻击的随机最优解决方案和本地设置解决方案来解决这种情况; 文献 [159] 分析了网络攻击对微电网中通信链路、本地控制器和主控制器的影响, 同时, 提出了一种网络攻击弹性分布式控制策略, 该策略可以检测并隔离损坏的通信链路和控制器.

需求响应是一种管理用户需求的方法. 针对电力需求响应的攻击威胁着电力系统的安全运行. 本文作者团队通过研究需求响应场景下的多电价机制 (包括分时电价、阶梯电价等), 提出一种称为隐蔽偷电攻击的新型量测数据攻击威胁, 通过精心构造篡改后的量测数据保证偷电过程不被现有的偷电检测方法检测出来; 通过实际设备测试和数值仿真分析论证了攻击的有效性, 并提出针对隐蔽偷电攻击威胁的防御策略[160]. 文献 [161] 研究了短信服务网络钓鱼攻击对电力需求响应程序的威胁, 可能导致大规模连锁停电. 文献 [162,163] 研究了针对需求响应的动态负载变化攻击, 攻击会恶化电网的频率响应, 还可能导致系统不稳定. 文献 [164] 描述了一种针对需求响应的虚假数据注入攻击, 评估了攻击者如何利用有针对性的虚假数据注入攻击, 通过基于实时的定价方案获得经济利益. 文献 [165] 表明攻击者可以通过虚假通信操纵配电系统中的消费者行为, 使用针对需求响应的决策模型研究了此类攻击可能对电力系统造成的影响, 包括峰值需求增加、电压降低以及潜在的停电事故.

6 结论与展望

电力系统正面临以工程故障为主的工程安全问题、以网络攻击为主的网络安全问题以及同时考虑工程安全和网络安全的信息物理综合安全问题. 为应对各类安全威胁, 电力系统安全仿真技术得到电气工程、自动化、计算机、网络空间安全等多个学科的关注, 已经取得长足的发展. 然而随着能源革命持续深化、电力系统安全对抗持续升级等原因, 电力系统的运行模式和安全需求将发生重大变革, 这些对于电力系统安全仿真技术既是挑战也是机遇, 具体如下所述.

(1) 能源形态变革导致安全仿真内涵扩展. 为加速实现现有能源系统向清洁低碳、安全高效的能源系统转变, 实现 2030 年碳达峰和 2060 年碳中和的目标, 习近平总书记强调要构建 “以新能源为主体的新型电力系统”. 在新能源变革形势下, 作为安全仿真的分析对象, 电力系统形态正在不断变化, 对其智能感知、安全可控等提出了更高要求, 相关研究必然离不开先进仿真技术的支持. 同时, 传统电力系统安全仿真主要研究电源和电网侧的安全威胁, 而对负荷与储能侧的研究较少. 随着分布式可再生能源的大规模接入, 电力系统将朝着 “低惯量、欠阻尼” 的状态演变. 为了应对新能源随机性给电力

系统运行控制带来的挑战, 需要完善储能设备仿真与电力市场仿真, 研究储能技术与负荷侧需求响应技术, 以保障高比例可再生能源场景下的电力系统稳定性.

(2) 攻击能力提升导致安全仿真边界延伸. 由于电力系统安全问题呈现出多元化、复杂化的特点, 电力系统安全正在成为各国国家力量重点关注与研究的目标. 随着万物互联时代的到来, 电力系统中可能受攻击的目标更多, 连锁效应更大, 电力系统面临的攻击方式由单点破坏转变为多点协同; 许多国家已经将网络攻击作为独立作战形式, 电力系统面临的攻击性质由黑客攻击转变为网络战争. 为此, 在进行电力系统安全仿真研究时, 研究者不能轻易对所面临的攻击威胁进行能力限定, 从而确保在绝大多数情况下, 仿真场景下所研究的安全技术均能够保障实际电力系统安全稳定运行.

(3) 能量流与信息流深度耦合导致安全仿真尺度时空同步拓展. 为了研究不同层次对象的安全问题, 未来电力系统安全仿真技术需要支持从电磁暂态、机电暂态到中长期动态、潮流稳态等不同仿真时间尺度下的安全研究. 此外, 目前电力系统安全仿真对象主要为局部、单一区域内的电力系统, 而电力系统 “牵一发而动全身” 的特点, 对跨地域、更大规模的安全仿真提出了更高的要求. 未来可依托现代信息通信技术的支持, 将不同地域内的多个仿真装置进行广泛互联, 实现广域范围的分布式仿真, 并建立真实电力系统的数字孪生系统, 提升对电力系统的认识和管理水平, 准确跟踪系统的实时状态变化.

参考文献

1 Guan X H, Zhao Q C, Jia Q S, et al. Information Physical Integration of Energy Systems. Beijing: Science Press, 2016 [管晓宏, 赵千川, 贾庆山, 等. 信息物理融合能源系统. 北京: 科学出版社, 2016]

2 Li H Y, Wei M H, Huang J, et al. Survey on cyber-physical systems. Acta Autom Sin, 2019, 45: 37–50 [李洪阳, 魏慕恒, 黄洁, 等. 信息物理系统技术综述. 自动化学报, 2019, 45: 37–50]

3 Liu T, Tian J, Wang J Z, et al. Integrated security threats and defense of cyber-physical systems. Acta Autom Sin, 2019, 45: 5–24 [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. 自动化学报, 2019, 45: 5–24]

4 Udry J R. Effect of great blackout of 1965 on births in New-York-City. Demography, 1970, 7: 325–327

5 Liu W X. Research on variable time-step modeling and coordinative optimization for network reconfiguration of power systems. Dissertation for Ph.D. Degree. Beijing: North China Electric Power University, 2017 [刘文轩. 电力系统网架重构的变时段建模和协调优化研究. 博士学位论文. 北京: 华北电力大学, 2017]

6 Xue Y S. The way from a simple contingency to system-wide disaster—Lessons from the Eastern Interconnection Blackout in 2003. Autom Electric Power Syst, 2003, 27: 1–5, 37 [薛禹胜. 综合防御由偶然故障演化为电力灾难 —— 北美 “8 · 14” 大停电的警示. 电力系统自动化, 2003, 27: 1–5, 37]

7 Allen J, Sauer H, Frank L, et al. Effects of the March 1989 solar activity. Eos Trans AGU, 1989, 70: 1479–1488

8 Liu Y F, Cai B, Wu S N. Emergency management for the ice disaster in power grids and some suggestions. Autom Electric Power Syst, 2008, 32: 10–13 [刘有飞, 蔡斌, 吴素农. 电网冰灾事故应急处理及反思. 电力系统自动化, 2008, 32: 10–13]

9 Zeng H, Sun F, Li T, et al. Analysis of “9 · 28” blackout in South Australia and its enlightenment to China. Autom Electric Power Syst, 2017, 41: 1–6 [曾辉, 孙峰, 李铁, 等. 澳大利亚 “9 · 28” 大停电事故分析及对中国启示. 电力系统自动化, 2017, 41: 1–6]

10 An X M, Sun H D, Zhang X H, et al. Analysis and lessons of Texas power outage event on February 15, 2021. Proc CSEE, 2021, 41: 3407–3415 [安学民, 孙华东, 张晓涵, 等. 美国得州 “2 · 15” 停电事件分析及启示. 中国电机工程学报, 2021, 41: 3407–3415]

11 Dzung D, Naedele M, von Hoff T P, et al. Security for industrial communication systems. Proc IEEE, 2005, 93: 1152–1177

12 Chen J. Ministry of Industry and Information Technology: adhere to the 16-word policy and constantly improve the network security system. People’s Daily Online, 2013 [陈键. 工信部: 坚持 16 字方针不断健全网络安全保障体系. 人民网, 2013]

13 Barrett M P. Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. 2018

14 Sedgewick A. Framework for Improving Critical Infrastructure Cybersecurity Version 1.0. 2014

15 Chen T M. Stuxnet, the real start of cyber warfare? IEEE Network, 2010, 24: 2–3

16 Tang Y, Chen Q, Li M Y, et al. Overview on cyber-attacks against cyber physical power system. Autom Electric Power Syst, 2016, 40: 59–69 [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. 电力系统自动化, 2016, 40: 59–69]

17 Zhu C Y. Behind the blackout in Venezuela. State Grid Corporation China, 2019, 5: 72–74 [朱朝阳. 委内瑞拉大停电事故的背后. 国家电网, 2019, 5: 72–74]

18 Song Y. The attack on Iran's nuclear facilities throws a cloud over Iran's nuclear negotiations. Xinhua News Agency, 2021 [宋盈. 伊朗核设施 "遇袭", 伊核谈判添变数. 新华社, 2021]

19 Gao Y J. Hackers cut off the US fuel pipelines, and cyber security problems need to be solved urgently. People's Daily Online, 2021 [高轶军. 黑客 "掐断" 美国燃油管道, 网络安全问题亟待解决. 人民网, 2021]

20 National Academy of Engineering. The Greatest Engineering Achievements of the 20th Century. Guangzhou: Ji'nan University Press, 2002 [美国国家工程院. 20 世纪最伟大的工程技术成就. 广州: 暨南大学出版社, 2002]

21 Mei S W. Great achievements and development trends of power systems. Chin Sci Bull, 2020, 65: 442–452 [梅生伟. 电力系统的伟大成就及发展趋势. 科学通报, 2020, 65: 442–452]

22 Mei S W, Zhu J Q. Mathematical and Control Scientic Issues of Smart Grid and Its Prospects. Acta Autom Sin, 2013, 39: 119–131 [梅生伟, 朱建全. 智能电网中的若干数学与控制科学问题及其展望. 自动化学报, 2013, 39: 119–131]

23 Zhou X X, Chen S Y, Lu Z X. Review and prospect for power system development and related technologies: a concept of three-generation power systems. Proc CSEE, 2013, 33: 1–11 [周孝信, 陈树勇, 鲁宗相. 电网和电网技术发展的回顾与展望 —— 试论三代电网. 中国电机工程学报, 2013, 33: 1–11]

24 Tang Y. The Similarity Theory. Beijing: Science Press, 1955 [基尔皮契夫基. 相似理论. 北京: 科学出版社, 1955]

25 Tang Y. The studies on techniques and software of power system full dynamic (electric-mechemical transient, mid-term and long-term dynamic) simulation. Dissertation for Ph.D. Degree. Beijing: China Electric Power Research Institute, 2002 [汤涌. 电力系统全过程动态 (机电暂态与中长期动态过程) 仿真技术与软件研究. 博士学位论文. 北京: 中国电力科学研究院, 2002]

26 Tang Y. Present situation and development of power system simulation technologies. Autom Electric Power Syst, 2002, 17: 66–70

27 Bélanger J, Venne P, Paquin J-N. The what, where and why of real-time simulation. Planet Rt, 2010, 1: 25–29

28 Kuffel R, Giesbrecht J, Maguire T, et al. RTDS-a fully digital power system simulator operating in real time. In: Proceedings of 1995 International Conference on Energy Management and Power Delivery EMPD, 1995. 498–503

29 Etxeberria-Otadui I, Manzo V, Bacha S, et al. Generalized average modelling of FACTS for real time simulation in ARENE. In: Proceedings of Conference of the IEEE Industrial Electronics Society, 2002

30 Zhou B R, Fang D Z, Snider L A, et al. The fully digital real-time simulator—HYPERSIM. Autom Electric Power Syst, 2003, 27: 79–82 [周保荣, 房大中, Snider L A, 等. 全数字实时仿真器 —— HYPERSIM. 电力系统自动化, 2003, 27: 79–82]

31 Tian F, Li Y-L, Zhou X X, et al. Advanced digital power system simulator. Power Syst Technol, 2008, 22: 17–22 [田芳, 李亚楼, 周孝信, 等. 电力系统全数字实时仿真装置. 电网技术, 2008, 22: 17–22]

32 Maheshwari K, Birman K, Wozniak J, et al. Evaluating cloud computing techniques for smart power grid design using parallel scripting. In: Proceedings of the 13th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing, 2013. 319–326

33 Bakken D E, Hauser C H, Gjermundrd H, et al. Towards More Flexible and Robust Data Delivery for Monitoring and Control of the Electric Power Grid. Washington State University, Technical Report, EECS-GS-009, 2007

34 Kulkarni N, Lalitha S, Deokar S A. Real time control and monitoring of grid power systems using cloud computing. Int J Electr Comput Eng, 2019, 9: 941–949

35 Ma F, Luo X, Litvinov E. Cloud computing for power system simulations at ISO New England-experiences and challenges. IEEE Trans Smart Grid, 2016, 7: 2596–2603

36 Piascik B, Vickers J, Lowry D, et al. Draft Materials, Structures, Mechanical Systems, and Manufacturing Roadmap: Technology Area 12. 2010

37 China Electronics Standardization Institute. White Paper of Digital Twin Application. 2020.

http://www.cesi.cn/images/editor/20201118/20201118163619265.pdf [中国电子技术标准化研究院. 数字孪生应用白皮书. 2020]
38 Onederra O, Asensio F J, Eguia P, et al. MV cable modeling for application in the digital twin of a windfarm. In: Proceedings of International Conference on Clean Electrical Power, 2019
39 Pileggi P, Verriet J, Broekhuijsen J, et al. A digital twin for cyber-physical energy systems. In: Proceedings of the 7th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, 2019. 1–6
40 Brosinsky C, Song X, Westermann D. Digital twin-concept of a continuously adaptive power system mirror. In: Proceedings of International ETG-Congress 2019, 2019. 1–6
41 Zhou M, Yan J, Feng D. Digital twin framework and its application to power grid online analysis. CSEE J Power Energy Syst, 2019, 5: 391–398
42 Cui Y, Xiao F, Wang W, et al. Digital twin for power system steady-state modelling, simulation, and analysis. In: Proceedings of IEEE 4th Conference on Energy Internet and Energy System Integration, 2020. 1233–1238
43 Tian F, Huang Y H, Shi D Y, et al. Developing trend of power system simulation and analysis technology. Proc CSEE, 2014, 34: 2151–2163 [田芳, 黄彦浩, 史东宇, 等. 电力系统仿真分析技术的发展趋势. 中国电机工程学报, 2014, 34: 2151–2163]
44 Zhu Y Y, Jiang W P, Yin Y H. General situation of power system hybrid simulation center. Power Syst Technol, 2008, 32: 35–38 [朱艺颖, 蒋卫平, 印永华. 电力系统数模混合仿真技术及仿真中心建设. 电网技术, 2008, 32: 35–38]
45 Cardoso A J M, Cruz S M A, Fonseca D S B. Inter-turn stator winding fault diagnosis in three-phase induction motors, by Park's vector approach. IEEE Trans Energy Convers, 1999, 14: 595–598
46 Penman J, Sedding H G, Lloyd B A, et al. Detection and location of interturn short circuits in the stator windings of operating motors. IEEE Trans Energy Convers, 1994, 9: 652–658
47 Yang W, Tavner P J, Wilkinson M R. Condition monitoring and fault diagnosis of a wind turbine synchronous generator drive train. IET Renew Power Gener, 2009, 3: 1
48 Wang L, Li Y G, Li J Q. Diagnosis of inter-turn short circuit of synchronous generator rotor winding based on Volterra kernel identification. Energies, 2018, 11: 2524
49 Yazidi A, Henao H, Capolino G, et al. Rotor inter-turn short circuit fault detection in wound rotor induction machines. In: Proceedings of the XIX International Conference on Electrical Machines, 2010. 1–6
50 Gritli Y, Rossi C, Casadei D, et al. A diagnostic space vector-based index for rotor electrical fault detection in wound-rotor induction machines under speed transient. IEEE Trans Ind Electron, 2017, 64: 3892–3902
51 Adly A R, Sehiemy R A E, Abdelaziz A Y, et al. Critical aspects on wavelet transforms based fault identification procedures in HV transmission line. IET Gener Trans Distrib, 2016, 10: 508–517
52 Li J, Fan C J. Wavelet analysis based traveling wave fault location for hybrid transmission line consisting of power cable and overhead line. Power Syst Technol, 2006, 30: 92–97 [李骏, 范春菊. 基于小波分析的电缆 – 架空线混合输电线路行波故障测距方法. 电网技术, 2006, 30: 92–97]
53 Lopes F V, Dantas K M, Silva K M, et al. Accurate two-terminal transmission line fault location using traveling waves. IEEE Trans Power Deliver, 2018, 33: 873–880
54 Sirisha A N R L, Pradhan A K. Cosine similarity based directional comparison scheme for subcycle transmission line protection. IEEE Trans Power Deliver, 2020, 35: 2159–2167
55 Li S L, Chen W, Yin X G, et al. A novel integrated protection for VSC-HVDC transmission line based on current limiting reactor power. IEEE Trans Power Deliver, 2020, 35: 226–233
56 Tang L X, Dong X Z, Shi S X, et al. A high-speed protection scheme for the DC transmission line of a MMC-HVDC grid. Electric Power Syst Res, 2019, 168: 81–91
57 Khayam U. Investigating the internal winding resonance characteristics of various power transformer winding designs. In: Proceedings of International Symposium on Electrical Insulating Materials, 2020. 541–544
58 Furgał J, Kuniewski M, Pająk P. Analysis of internal overvoltages in transformer windings during transients in electrical networks. Energies, 2020, 13: 2644
59 Hajiaghasi S, Ahmadi M M H, Goleij P, et al. Transformer inter-turn failure detection based on leakage flux and vibration analysis. IET Electric Power Appl, 2021, 15: 998–1012
60 Venikar P A, Ballal M S, Umre B S, et al. Search coil based online diagnostics of transformer internal faults. IEEE Trans Power Deliver, 2017, 32: 2520–2529

61 Eldin A A H, Refaey M A. A novel algorithm for discrimination between inrush current and internal faults in power transformer differential protection based on discrete wavelet transform. Electric Power Syst Res, 2011, 81: 19–24

62 Zhou H, Hong K, Huang H, et al. Transformer winding fault detection by vibration analysis methods. Appl Acoustics, 2016, 114: 136–146

63 Li B, Liu T Q, Li X Y. Impact of distributed generation on power system voltage stability. Power Syst Technol, 2009, 33: 84–88 [李斌, 刘天琪, 李兴源. 分布式电源接入对系统电压稳定性的影响. 电网技术, 2009, 33: 84–88]

64 Khani D, Yazdankhah A S, Kojabadi H M. Impacts of distributed generations on power system transient and voltage stability. Int J Electr Power Energy Syst, 2012, 43: 488–500

65 Xu J, Xie B, Liao S, et al. Online assessment of conservation voltage reduction effects with micro-perturbation. IEEE Trans Smart Grid, 2021, 12: 2224–2238

66 Liu J, Lin T, Tong X Q, et al. Simulation analysis on influences of distributed photovoltaic generation on short-circuit current in distribution network. Power Syst Technol, 2013, 37: 2080–2085 [刘健, 林涛, 同向前, 等. 分布式光伏电源对配电网短路电流影响的仿真分析. 电网技术, 2013, 37: 2080–2085]

67 Injeti S K, Kumar N P. A novel approach to identify optimal access point and capacity of multiple DGs in a small, medium and large scale radial distribution systems. Int J Electr Power Energy Syst, 2013, 45: 142–151

68 Mahat P, Chen Z, Bak-Jensen B, et al. A simple adaptive overcurrent protection of distribution systems with distributed generation. IEEE Trans Smart Grid, 2011, 2: 428–437

69 Luo M, Dujic D, Allmeling J. Leakage flux modeling of medium-voltage phase-shift transformers for system-level simulations. IEEE Trans Power Electron, 2019, 34: 2635–2654

70 Dong Y F, Xiong Y Q, Wang B Y. Security threat and defense technology of smart grid communication protocol. Comput Technol Dev, 2019, 29: 1–6 [董一帆, 熊荫乔, 王宝耀. 智能电网通信协议安全威胁与防御技术. 计算机技术与发展, 2019, 29: 1–6]

71 Yang L Y, Han S S, Wang X, et al. Computational experiment platforms for networks: the state of the art and prospect. Acta Automa Sin, 2019, 45: 1637–1654 [杨林瑶, 韩双双, 王晓, 等. 网络系统实验平台: 发展现状及展望. 自动化学报, 2019, 45: 1637–1654]

72 National Institute for Standards and Technology (NIST). Guidelines for smart grid cyber security. NISTIR 7628, 2010

73 Singh V K, Govindarasu M. A cyber-physical anomaly detection for wide-area protection using machine learning. IEEE Trans Smart Grid, 2021, 12: 3514–3526

74 Hong J H, Liu C C, Govindarasu M. Integrated anomaly detection for cyber security of the substations. IEEE Trans Smart Grid, 2014, 5: 1643–1653

75 Singh V K, Callupe S P, Govindarasu M. Testbed-based evaluation of SIEM tool for cyber kill chain model in power grid SCADA system. In: Proceedings of the 51st North American Power Symposium, 2019

76 Naseem F, Babun L, Kaygusuz C, et al. CSPoweR-Watch: a cyber-resilient residential power management system. In: Proceedings of International Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data, 2019. 768–775

77 Chromik J J, Pilch C, Brackmann P, et al. Context-aware local intrusion detection in SCADA systems: a testbed and two showcases. In: Proceedings of IEEE International Conference on Smart Grid Communications, 2017. 467–472

78 Marino D L, Wickramasinghe C S, Amarasinghe K, et al. Cyber and physical anomaly detection in smart-grids. In: Proceedings of 2019 Resilience Week, 2019. 187–193

79 Liu T, Liu Y, Mao Y S, et al. A dynamic secret-based encryption scheme for smart grid wireless communication. IEEE Trans Smart Grid, 2014, 5: 1175–1182

80 Kaur K, Hahn A, Gourisetti S N G, et al. Enabling secure grid information sharing through hash calendar-based blockchain infrastructures. In: Proceedings of 2019 Resilience Week, 2019. 200–205

81 Alsharif A, Shafee A, Nabil M, et al. A multi-authority attribute-based signcryption scheme with efficient revocation for smart grid downlink communication. In: Proceedings of 2019 International Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data, 2019. 1025–1032

82 Ozgur U, Tonyali S, Akkaya K. Testbed and simulation-based evaluation of privacy-preserving algorithms for smart grid AMI networks. In: Proceedings of IEEE Local Computer Networks Workshops, 2017. 181–186

83 Dorsch N, Kurtz F, Georg H, et al. Software-defined networking for smart grid communications: applications, challenges and advantages. In: Proceedings of IEEE International Conference on Smart Grid Communications, 2014. 422–427

84 Cokic M, Seskar I. Analysis of TCP traffic in smart grid using SDN based QoS. In: Proceedings of the 26th Telecommunications Forum, 2018. 269–272

85 Kurtz F, Dorsch N, Bektas C, et al. Synchronized measurement concept for failure handling in software-defined smart grid communications. In: Proceedings of IEEE International Conference on Smart Grid Communications, 2017. 1–6

86 Sung J M, Evans B L. Real-time testbed for diversity in powerline and wireless smart grid communications. In: Proceedings of IEEE International Conference on Communications Workshops, 2018

87 Ravikumar G, Hyder B, Govindarasu M. Efficient modeling of IEC-61850 logical nodes in IEDs for scalability in CPS security testbed. In: Proceedings of IEEE/PES Transmission and Distribution Conference and Exposition, 2020. 1–5

88 Demir K, Suri N. SeReCP: a secure and reliable communication platform for the smart grid. In: Proceedings of IEEE 22nd Pacific Rim International Symposium on Dependable Computing, 2017. 175–184

89 Park M, Jeong G, Son H, et al. Performance of RPL routing protocol over multihop power line communication network. In: Proceedings of International Conference on Information and Communication Technology Convergence, 2020. 1918–1920

90 Lu X, Wang W Y, Ma J F. An empirical study of communication infrastructures towards the smart grid: design, implementation, and evaluation. IEEE Trans Smart Grid, 2013, 4: 170–183

91 Cai Z Y, Yu M, Steurer M, et al. A new grouping protocol for smart grids. IEEE Trans Smart Grid, 2019, 10: 955–966

92 Maziku H, Shetty S. Software defined networking enabled resilience for IEC 61850-based substation communication systems. In: Proceedings of International Conference on Computing, Networking and Communications, 2017. 690–694

93 Sahu A, Goulart A, Butler-Purry K. Modeling AMI network for real-time simulation in NS-3. In: Proceedings of Principles, Systems and Applications of IP Telecommunications, 2016. 1–8

94 Zhao Z Y. Design and implementation of simulation testbed for power grid. Dissertation for Master's Degree. Shenyang: University of Chinese Academy of Sciences, 2020 [赵智阳. 针对电网的仿真测试床设计与实现. 硕士学位论文. 沈阳: 中国科学院大学, 2020]

95 Fei J X, Liu Z J, Ma Y Y, et al. The research on cyber-attack testbed with hardware-in-loop. In: Proceedings of IEEE Conference on Energy Internet and Energy System Integration, 2017

96 Ghaleb A, Zhioua S, Almulhem A. SCADA-SST: a SCADA security testbed. In: Proceedings of World Congress on Industrial Control Systems Security, 2016. 34–39

97 Ravikumar G, Singh A, Babu J R, et al. D-IDS for cyber-physical DER modbus system-architecture, modeling, testbed-based evaluation. In: Proceedings of 2020 Resilience Week, 2020. 153–159

98 Liu R, Vellaithurai C, Biswas S S, et al. Analyzing the cyber-physical impact of cyber events on the power grid. IEEE Trans Smart Grid, 2015, 6: 2444–2453

99 Moussa B, Robillard C, Zugenmaier A, et al. Securing the precision time protocol (PTP) against fake timestamps. IEEE Commun Lett, 2019, 23: 278–281

100 Mashima D, Gunathilaka P, Chen B. Artificial command delaying for secure substation remote control: design and implementation. IEEE Trans Smart Grid, 2019, 10: 471–482

101 Elbez G, Keller H B, Hagenmeyer V. A cost-efficient software testbed for cyber-physical security in IEC 61850-based substations. In: Proceedings of IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids, 2018

102 Khan R, McLaughlin K, Hastings J, et al. Demonstrating cyber-physical attacks and defense for synchrophasor technology in smart grid. In: Proceedings of the 16th Annual Conference on Privacy, Security and Trust, 2018. 257–266

103 Cebe M, Akkaya K. A bandwidth-efficient secure authentication module for smart grid DNP3 protocol. In: Proceedings of 2020 Resilience Week, 2020. 160–166

104 Fritz J J, Sagisi J, James J, et al. Simulation of man in the middle attack on smart grid testbed. In: Proceedings of SoutheastCon, 2019

105 Liang Y, Wang Y K, Liu K Y, et al. CPS fault simulation of distribution network considering network information

security. Power Syst Technol, 2021, 45: 235–242 [梁英, 王耀坤, 刘科研, 等. 计及网络信息安全的配电网 CPS 故障仿真. 电网技术, 2021, 45: 235–242]
106 Choi I S, Hong J, Kim T W. Multi-agent based cyber attack detection and mitigation for distribution automation system. IEEE Access, 2020, 8: 183495
107 Oyewumi I A, Jillepalli A A, Richardson P, et al. ISAAC: the idaho CPS smart grid cybersecurity testbed. In: Proceedings of IEEE Texas Power and Energy Conference, 2019. 1–6
108 Ashok A, Krishnaswamy S, Govindarasu M. PowerCyber: a remotely accessible testbed for cyber physical security of the smart grid. In: Proceedings of IEEE Power & Energy Society Innovative Smart Grid Technologies Conference, 2016. 1–5
109 Dean B, Starke M, Smith M, et al. A communication testbed for testing power electronic agent systems. In: Proceedings of IEEE Power Energy Society Innovative Smart Grid Technologies Conference, 2021. 1–5
110 Ravikumar G, Ramya G, Misra S, et al. iPaCS: an integrative power and cyber systems co-simulation framework for smart grid. In: Proceedings of IEEE Power & Energy Society General Meeting, 2017
111 Zeinali M, Bayram I S, Thompson J. Performance assessment of UK's cellular network for vehicle to grid energy trading: opportunities for 5G and beyond. In: Proceedings of IEEE International Conference on Communications Workshops, 2020
112 Musleh A S, Muyeen S M, Al-Durra A, et al. Time-delay analysis of wide-area voltage control considering smart grid contingences in a real-time environment. IEEE Trans Ind Inf, 2018, 14: 1242–1252
113 Fu C Y, Wang L Z, Qi D L, et al. Design and experiments of active distribution network CPS simulation platform. Proc CSEE, 2019, 39: 7118–7125 [付灿宇, 王立志, 齐冬莲, 等. 有源配电网信息物理系统混合仿真平台设计方法及其算例实现. 中国电机工程学报, 2019, 39: 7118–7125]
114 Berman M, Chase J S, Landweber L, et al. GENI: a federated testbed for innovative network experiments. Comput Networks, 2014, 61: 5–23
115 Benzel T. The science of cyber security experimentation: the DETER project. In: Proceedings of the 27th Annual Computer Security Applications Conference, 2011. 137–147
116 Singh V K, Govindarasu M, Porschet D, et al. Evaluation of anomaly detection for wide-area protection using cyber federation testbed. In: Proceedings of IEEE Power & Energy Society General Meeting, 2019. 1–5
117 Oyewumi I A, Challa H, Jillepalli A A, et al. Attack scenario-based validation of the idaho CPS smart grid cybersecurity testbed. In: Proceedings of IEEE Texas Power and Energy Conference, 2019
118 Williams T J. The Purdue enterprise reference architecture. Comput Industry, 1994, 24: 141–158
119 Buldyrev S V, Parshani R, Paul G, et al. Catastrophic cascade of failures in interdependent networks. Nature, 2010, 464: 1025–1028
120 Bilis E I, Kroger W, Nan C. Performance of electric power systems under physical malicious attacks. IEEE Syst J, 2013, 7: 854–865
121 Kundur D, Feng X Y, Liu S, et al. Towards a framework for cyber attack impact analysis of the electric smart grid. In: Proceedings of IEEE 1st International Conference on Smart Grid Communications, 2010. 244–249
122 Rahman M A, Mohsenian-Rad H. False data injection attacks with incomplete information against smart power grids. In: Proceedings of IEEE Global Communications Conference, 2012. 3153–3158
123 Zhang Y, Wang J, Liu J. Attack identification and correction for PMU GPS spoofing in unbalanced distribution systems. IEEE Trans Smart Grid, 2020, 11: 762–773
124 Branicky M S, Liberatore V, Phillips S M. Networked control system co-simulation for co-design. In: Proceedings of the 2003 American Control Conference, 2003. 3341–3346
125 Tian G, Fidge C, Tian Y C. Hybrid system simulation of computer control applications over communication networks. In: Proceedings of IEEE International Symposium on Modeling, Analysis & Simulation of Computer and Telecommunication Systems, 2009. 331–340
126 Park S, Savvides A, Srivastava M B. SensorSim: a simulation framework for sensor networks. In: Proceedings of the 3rd ACM International Workshop on Modeling, Analysis and Simulation of Wireless and Mobile Systems, 2000. 104–111
127 Henriksson D, Cervin A, Årzén K E. TrueTime: simulation of control loops under shared computer resources. IFAC Proc Vol, 2002, 35: 417–422

128 Majumder R, Bag G, Velotto G, et al. Closed loop simulation of communication and power network in a zone based system. Electric Power Syst Res, 2013, 95: 247–256
129 Tall H, Chalhoub G, Misson M. Implementation and performance evaluation of IEEE 802.15.4 unslotted CSMA/CA protocol on Contiki OS. Ann Telecommun, 2016, 71: 517–526
130 Baldwin P, Kohli S, Lee E A, et al. Modeling of sensor nets in Ptolemy II. In: Proceedings of International Symposium on Information Processing in Sensor Networks, 2004. 359–368
131 Li W, Zhang X. Simulation of the smart grid communications: challenges, techniques, and future trends. Comput Electr Eng, 2014, 40: 270–288
132 Mets K, Ojea J A, Develder C. Combining power and communication network simulation for cost-effective smart grid analysis. IEEE Commun Surv Tutor, 2014, 16: 1771–1796
133 Gomes C, Thule C, Broman D, et al. Co-simulation: a survey. ACM Comput Surv, 2018, 51: 1–33
134 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. IEEE Trans Power Syst, 2006, 21: 548–558
135 Liberatore V, Al-Hammouri A. Smart grid communication and co-simulation. In: Proceedings of IEEE 2011 EnergyTech, 2011. 1–5
136 Li W, Monti A, Luo M, et al. VPNET: a co-simulation framework for analyzing communication channel effects on power systems. In: Proceedings of IEEE Electric Ship Technologies Symposium, 2011. 143–149
137 Lin H, Veda S S, Shukla S S, et al. GECO: global event-driven co-simulation framework for interconnected power system and communication network. IEEE Trans Smart Grid, 2012, 3: 1444–1456
138 Georg H, Müller S C, Dorsch N, et al. INSPIRE: integrated co-simulation of power and ICT systems for real-time evaluation. In: Proceedings of IEEE International Conference on Smart Grid Communications, 2013. 576–581
139 Awad A, Bazan P, German R. SGsim: a simulation framework for smart grid applications. In: Proceedings of IEEE International Energy Conference, 2014. 730–736
140 Wermann A G, Bortolozzo M C, da Silva E G, et al. ASTORIA: a framework for attack simulation and evaluation in smart grids. In: Proceedings of IEEE/IFIP Network Operations and Management Symposium, 2016. 273–280
141 Saxena N, Chukwuka V, Xiong L, et al. CPSA: a cyber-physical security assessment tool for situational awareness in smart grid. In: Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy, 2017. 69–79
142 Palmintier B, Krishnamurthy D, Top P, et al. Design of the HELICS high-performance transmission-distribution-communication-market co-simulation framework. In: Proceedings of Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, 2017. 1–6
143 Ashok A, Wang P Y, Brown M, et al. Experimental evaluation of cyber attacks on automatic generation control using a CPS security testbed. In: Proceedings of IEEE Power & Energy Society General Meeting, 2015. 1–5
144 Tan R, Nguyen H H, Foo E Y S, et al. Modeling and mitigating impact of false data injection attacks on automatic generation control. IEEE Trans Inform Forensic Secur, 2017, 12: 1609–1624
145 Ashok A, Sridhar S, Mckinnon A D, et al. Testbed-based performance evaluation of attack resilient control for AGC. In: Proceedings of Resilience Week (RWS), 2016. 125–129
146 Zhang Z H, Gong S P, Dimitrovski A D, et al. Time synchronization attack in smart grid: impact and analysis. IEEE Trans Smart Grid, 2013, 4: 87–98
147 Jiang X C, Zhang J M, Harding B J, et al. Spoofing GPS receiver clock offset of phasor measurement units. IEEE Trans Power Syst, 2013, 28: 3253–3262
148 Shepard D P, Humphreys T E, Fansler A A. Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. Int J Crit Infrast Prot, 2012, 5: 146–153
149 Lin H, Deng Y, Shukla S, et al. Cyber security impacts on All-PMU state estimator — A case study on co-simulation platform GECO. In: Proceedings of IEEE 3rd International Conference on Smart Grid Communications, 2012. 587–592
150 Mousavian S, Valenzuela J, Wang J. A probabilistic risk mitigation model for cyber-attacks to PMU networks. IEEE Trans Power Syst, 2015, 30: 156–165
151 Liu N A, Zhang J H, Zhang H, et al. Vulnerability assessment for communication network of substation automation systems to cyber attack. In: Proceedings of IEEE/PES Power Systems Conference and Exposition, 2009. 1–7
152 Dondossola G, Szanto J, Masera M, et al. Effects of intentional threats to power substation control systems. Int J

Crit Infrast, 2008, 4: 129–143
153 Stefanov A, Liu C-C. Cyber-power system security in a smart grid environment. In: Proceedings of IEEE PES Innovative Smart Grid Technologies, 2012. 1–3
154 Hong J, Wu S-S, Stefanov A, et al. An intrusion and defense testbed in a cyber-power system environment. In: Proceedings of IEEE Power and Energy Society General Meeting, 2011. 1–5
155 Sun C C, Hong J H, Liu C C. A co-simulation environment for integrated cyber and power systems. In: Proceedings of IEEE International Conference on Smart Grid Communications, 2015. 133–138
156 Xie F, McEntee C, Zhang M, et al. Development of an encoding method on a co-simulation platform for mitigating the impact of unreliable communication. IEEE Trans Smart Grid, 2021, 12: 2496–2507
157 Duan J, Chow M Y. A novel data integrity attack on consensus-based distributed energy management algorithm using local information. IEEE Trans Ind Inf, 2019, 15: 1544–1553
158 Majumdar A, Agalgoankar Y, Pal B, et al. Centralized volt-var optimization strategy considering malicious attack on distributed energy resources control. In: Proceedings of IEEE Power & Energy Society General Meeting, 2018
159 Zhou Q, Shahidehpour M, Alabdulwahab A, et al. A cyber-attack resilient distributed control strategy in islanded microgrids. IEEE Trans Smart Grid, 2020, 11: 3690–3701
160 Liu Y, Liu T, Sun H, et al. Hidden electricity theft by exploiting multiple-pricing scheme in smart grids. IEEE Trans Inform Forensic Secur, 2020, 15: 2453–2468
161 Soykan E U, Bagriyanik M. The effect of SMiShing attack on security of demand response programs. Energies, 2020, 13: 4542
162 Patel A, Purwar S. Destabilizing smart grid by dynamic load altering attack using PI controller. In: Proceedings of International Conference on Intelligent Computing, Instrumentation and Control Technologies, 2017. 354–359
163 Amini S, Pasqualetti F, Mohsenian-Rad H. Dynamic load altering attacks against power system stability: attack models and protection schemes. IEEE Trans Smart Grid, 2018, 9: 2862–2872
164 Dayaratne T, Rudolph C, Liebman A, et al. High impact false data injection attack against real-time pricing in smart grids. In: Proceedings of IEEE PES Innovative Smart Grid Technologies Europe, 2019
165 Raman G, Peng J C H, Rahwan T. Manipulating residents' behavior to attack the urban power distribution system. IEEE Trans Ind Inf, 2019, 15: 5575–5587

Power system security simulation technologies: engineering safety, network security and cyber-physical integrated security

Zijun WANG[1], Yang LIU[1*], Yuanyi BAO[1], Xiaohong GUAN[1], Tong WU[2], Jiangang LU[3], Zhiwen YU[3], Xiaoshu YUAN[4] & Ting LIU[1*]

1. *School of Cyber Science and Engineering, Xi'an Jiaotong University, Xi'an* 710049*, China*;
2. *National Energy Administration Information Center, Beijing* 100824*, China*;
3. *Power Dispatching and Control Center of Guangdong Power Grid Corporation, Guangzhou* 510699*, China*;
4. *Academia Sinica of Dongfang Electric Corporation, Chengdu* 611731*, China*

* Corresponding author. E-mail: yangliu@mail.xjtu.edu.cn, tingliu@mail.xjtu.edu.cn

Abstract Power system security simulation technologies study system behaviors via simulation experiments or numerical calculations to deal with security threats such as system faults and external attacks. With the wide application of information technologies such as automatic control, network communication, and artificial intelligence, the power system has developed into a cyber-physical system (CPS), where the physical and information systems are deeply coupled. Faults caused by physical damage or network attacks are interrelated in the power system and can spread across domains, resulting in new security threats. Therefore, power system security simulation is facing new challenges. This paper reviewed the security incidents that have significantly impacted the power system and analyzed the requirement and development of security simulation technologies for power systems from three dimensions: engineering security, network security, and cyber-physical integrated security. Therefore, the representative security simulation testbeds were classified and summarized. Moreover, the challenges and development trends of the power system security simulation technologies were explored.

Keywords cyber-physical system (CPS), engineering safety, network security, cyber-physical integrated security, power system security simulation technology