第 40 卷 第 5 期 2016 年 3 月 10 日
DOI：10.7500/AEPS20160113101
电力系统自动化
Automation of Electric Power Systems
Vol.40 No.5 Mar.10，2016

由乌克兰停电事件看信息能源系统综合安全评估

郭庆来[1]，辛蜀骏[1]，王剑辉[2]，孙宏斌[1]
（1. 清华大学电机工程与应用电子技术系，北京市 100084；2. 美国阿贡国家实验室，IL 60439，美国）

Comprehensive Security Assessment for a Cyber Physical Energy System：a Lesson from Ukraine's Blackout

GUO Qinglai[1]，*XIN Shujun*[1]，*WANG Jianhui*[2]，*SUN Hongbin*[1]
（1. Department of Electrical Engineering，Tsinghua University，Beijing 100084，China；
2. Argonne National Laboratory，IL 60439，USA）

1 乌克兰停电事件回顾

2015 年圣诞节期间，乌克兰国内多个区域的电网因遭遇黑客攻击，导致发生大规模停电。达拉斯信息安全公司 iSight Partners 的研究人员表示，黑客在乌克兰国家电网中植入的恶意软件导致了这次严重的停电事故。资料显示，这是首次由信息攻击引发的大规模停电事故（见 http://news.finance.ua/ua/news/-/366136/hakery-atakuvaly-prykarpattyaoblenergo-znestrumyvshy-polovynu-regionu-na-6-godyn）。传统网络攻击主要是窃取数据或者财物，而此次则直接诱发了重要公用事业系统的失效。因此，CNET 网站的一篇报道称乌克兰停电是网络攻击的“里程碑”（cyberattack milestone）（见 http://www.cnet.com/news/cyberattack-causes-widespread-power-blackout-in-ukraine/）。

长久以来，人们一直将电力系统视为一种负责能量产生、传输、分配与使用的物理系统。然而造成此次事故的关键原因，并不是因为物理电网的元件故障，而是因病毒引起的能量管理系统（energy management system，EMS，一些报告中也写作 remote management system）失效（见 https://ics.sans.org/blog/2015/12/30/current-reporting-on-the-cyber-attack-in-ukraine-resulting-in-power-outage）。换言之，在这次大停电事故中，信息系统的扰动导致了物理电网运行的失效。这次事故发生不久便获得了世界范围内的广泛关注，同时也将电力系统的信息安全问题摆在了人们面前，成为建设与完善电力系统乃至未来的能源互联网所不可回避的重要挑战。

收稿日期：2016-01-13。
上网日期：2016-01-14。

2 停电过程的回顾与分析

如上节所述，信息网络的失效是导致此次事故的关键原因。现代电力系统中，以数据采集与监控/能量管理系统/广域测量系统（SCADA/EMS/WAMS）为典型代表的二次信息系统，在现代电力系统的感知与控制中扮演着愈发关键的角色。一个典型的信息-物理耦合电力系统的架构如图 1 所示。

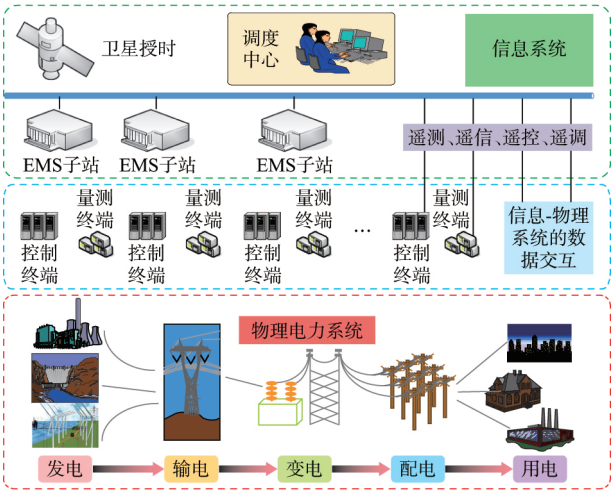

图 1 典型的信息-物理耦合电力系统架构

在电力系统日常运行中，SCADA/EMS/WAMS 等可实现广域信息实时感知（RTU/PMU）、信息传输（电力载波/光纤网、各种规约形式）、信息处理（坏数据辨识/状态估计）、信息决策（潮流分析/

安全分析/优化计算)、闭环控制(AGC/AVC)等多项功能，从空间上覆盖上千千米，从时间上涵盖毫秒到小时级，从目标上兼顾安全、优质和经济等多种要求。可以说，现代电力系统的正常运行无时无刻不依赖于一个可靠的信息系统，是一个典型的信息-能量融合系统(国内专家也将其定义为信息能源系统)。正因如此，信息系统的失效也将显著影响物理电网。当信息故障发生时，如信息传输发生中断或延时或被恶意修改，很可能诱使信息系统作出错误的决策甚至直接失效，从而影响电网的运行状态。值得注意的是，恶意的信息攻击文件可通过四通八达的信息网络进行快速而广泛地复制与扩散，这又进一步提升了信息攻击的作用范围与影响。信息故障影响电力系统运行的示意图如图 2 所示。

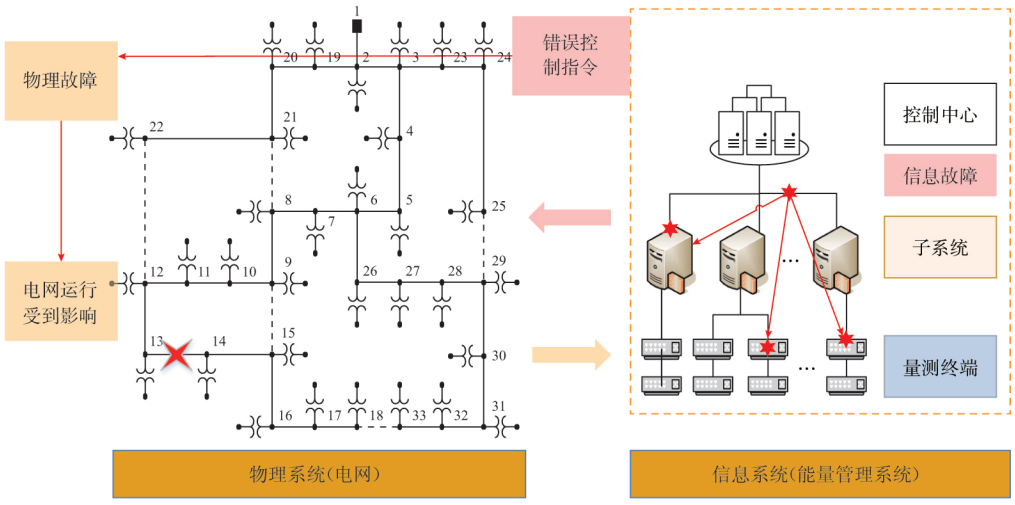

图 2　信息故障影响电力系统运行的示意图

据 SANS ICS 小组对本次事故的报告，外部电脑病毒被植入乌克兰电网公司的 EMS 后，使底层发电机或变电站的控制服务器关机(见 https://ics.sans.org/blog/2016/01/01/potential-sample-of-malware-from-the-ukrainian-cyber-attack-uncovered)，丧失对相应物理设备的感知与控制能力(the utility began to disconnect power substations for no apparent reason)(见 https://ics.sans.org/blog/2015/12/30/current-reporting-on-the-cyber-attack-in-ukraine-resulting-in-power-outage)，从而导致部分设备运行中断。此外，病毒利用通信网络进行了大范围的传播和感染，这使得乌克兰电网公司失去了与底层多个发电站及变电站的通信联系，从而进一步丧失了对电网的实时感知与控制能力，无法进行正确决策，进而引发大范围停电。事故发生后，乌克兰电网公司被迫停止 EMS，启动人工控制以恢复供电。截至当前，即使供电已经恢复，原有的 EMS/SCADA 系统的部分功能因被病毒攻击依然长时间处于离线状态，本次网络攻击的影响仍在持续。

3　信息能源系统的薄弱环节评估

本次的乌克兰大停电事故中，恶意信息攻击使得电力信息系统部分环节失效(控制服务器关机)，从而影响物理电网的运行，造成了区域性大停电的严重后果。目前关于事件的详细报道和分析尚不多见，因此还难以判断很多内部技术细节。从最终效果来看，此次事故毫无疑问造成了重大的经济与社会影响，攻击者也达到了预期目标。然而值得注意的是，这是一次“简单粗暴”的攻击，使用的 BlackEnergy 恶意软件也并非为电力系统量身打造的“定制版”，攻击者是通过大面积、无差别的攻击电力信息网络中的相关设备，使其强制关机，从而影响系统安全运行。

这让笔者联想起《笑傲江湖》一书中令狐冲在破庙外奋起一剑，刺瞎十五名高手的眼睛，正类似于通过攻击“信息采集系统”最终迫使这些高手退出“物理运行”。但此时令狐冲处于剑法尚未大成的境界，随着情节进展，会逐渐修炼到专门看穿别人招数中的破绽，然后一招制胜，完美攻击。同样令人担忧的是，未来能源系统所面对的恶意攻击者会不会也通过“修炼”来使得攻击日益“完美”。相比于此次事故中的“无差别攻击”，这类直奔“命门”而去的信息攻击虽然难度更大、代价较高，但是其目的明确、攻击手段隐蔽、识别难度大，且攻击者可根据自身需求针对性地影响系统运行状态，对未来能源系统的影响

更为恶劣，因而更值得大家关注。

事实上，已有研究表明，当攻击者具备一定电力系统知识时，可制定精确的攻击策略，通过针对性的坏数据注入和权限获取，能够在无法被控制中心辨识的条件下影响电力系统的运行或使自己获得不正当利益。例如，针对状态估计（state estimation）应用，攻击者可通过修正部分量测信号，影响控制中心状态估计结果（如开关状态、量测状态、系统拓扑辨识出错），进而导致系统决策错误。又如，电力市场环境下，攻击者可通过恶意信息注入影响系统的边际电价决策结果，提升自身收益。

这次事故敲响了恶意信息攻击可以诱发电网运行风险的警钟。而实际电网运行时，信息系统除受到恶意攻击外，还可能频繁面临由于无意错误（如工作人员失误）导致的功能失效，这种信息环节的功能失效同样会诱发物理环节的运行风险。2003 年美加“8·14”大停电是一个最典型的示例。其发生的一个重要原因是 EMS 中的状态估计功能退出运行，调度人员失去了对电网实时状态的感知能力，未能及时发现、评估和遏制故障蔓延。

“破绽”即薄弱环节。电力系统在运行过程中需要在线进行静态或暂态安全评估，其目标就是让运行人员了解电力系统运行的薄弱环节。而随着信息环节与能量系统的日益融合，整个信息能源系统的薄弱环节可能不再局限于物理系统内部，信息环节或将成为新的阿喀琉斯之踵。这种薄弱环节可能成为“点穴式”恶意攻击的理想标靶，也可能由于某种无意错误诱发意外风险。尤其是在闭环决策与控制日益增加的情境下，信息故障将变得更为普遍而多样化，极可能进一步殃及能量系统。因此，通过信息-能量耦合建模、分析与安全评估，定位整个信息能源系统的薄弱环节，将是一个全新的研究课题。

4　对中国的启示

此次乌克兰大停电事故告诉大家，即使物理电网状态正常，信息系统的失效也同样可对系统造成严重的影响。换言之，物理电网的安全评估结果并不等价于全系统的安全，信息系统评估应当成为电力系统评估体系的重要组成部分。

信息网络的数据交互途径、接入点数量、传输内容与网络参与者等多个因素都将影响网络的信息安全。在国外，尤其是欧美发达国家，随着电力服务的细化与电力市场的普及，电力系统运行对信息与通信有着更高的需求。现有研究及报告显示，欧美国家的电力信息系统，可依托于专用有线信息网络（如主网的 EMS 服务），公共信息网络 Internet（如市场报价、需求侧响应、分布式能源、电动汽车优化充电服务），甚至无线网络（如电厂及小规模电网的能量管理服务）实现，且参与者可获得的网络资源更多，信息权限更大，更容易接入并影响信息系统乃至整个电力系统的运行。这为恶意攻击者提供了方便之门。

现阶段中国的电网调度运行主要基于较为封闭的调度数据专网，而且实现了严格的网络分区、物理隔离等安全技术，这在很大程度上提高了中国电力系统应对网络攻击的能力。但仍必须看到，随着国内电力系统的保护、控制水平的不断提高，对信息网络可靠性的依赖也日益增加，即使没有恶意攻击，信息环节失效也可能诱发电网运行风险，这在一些电网公司已经出现了类似的案例。因此着手从信息-能量耦合的视角，开展信息环节对能量系统安全性的定量评估是保证中国复杂电力系统可靠运行的当务之急。

而随着能源互联网等概念的兴起及电力市场改革的不断推进，未来海量终端用户可能通过无线通信、互联网等方式与能源系统产生信息互动，在这一未来愿景下，已经不再是简单的信息流调控能量流，而是信息流与能量流实现真正的融合，变成信息能源系统中密不可分、环环相套的组成部分。因此，考虑信息能量相互作用机理的信息能源系统综合安全评估将具有重要的现实意义，尽快开展相关研究已不是未雨绸缪，而是迫在眉睫。

郭庆来（1979—），男，通信作者，博士，副教授，博士生导师，IEEE Senior Member，国家优秀青年科学基金获得者，主要研究方向：电网能量管理技术、电压稳定与电压控制、信息物理系统（CPS）、电动汽车。E-mail：guoqinglai@tsinghua.edu.cn

辛蜀骏（1990—），男，博士研究生，美国阿贡国家实验室访问学者，主要研究方向：电力系统信息-物理耦合分析与故障评估、电动汽车优化充电。

王剑辉（1978—），男，博士，美国阿贡国家实验室研究员，“IEEE Transactions on Smart Grid”杂志主编，主要研究方向：智能电网、微电网、电力信息安全、可再生能源、电力市场等。

（编辑　章黎　宗敏洁）