文章编号: 1000−8152(2012)02−0240−05

智能电网信息安全及其对电力系统生存性的影响

陈来军, 梅生伟, 陈 颖

(电力系统及发电设备控制和仿真国家重点实验室; 清华大学 电机系, 北京 100084)

摘要: 目前的电网必将发展成为由电力网和信息网组成的相互依存的复合网络. 分析了智能电网网络构成的特点, 阐述了信息网络安全在智能电网安全中的重要性. 通过对智能电网信息化引入新元素的主要功能和特点的分析, 从信息的采集、传输、处理和互动等角度描述了智能电网的信息安全问题, 预想了各类攻击条件下的安全性事故场景. 从网络功能的耦合性和网络间故障的传播特性探讨了信息网络安全对电力系统生存性的影响. 最后, 从关键技术、标准体系、政策法规、培训管理等方面提出了加强智能电网信息安全的具体建议, 有助于提高智能电网安全性.

关键词: 智能电网; 电力网; 信息网; 信息安全; 复合网络; 生存性

中图分类号: TM71 **文献标识码**: A

Smart grid information security and its influence on power system survivability

CHEN Lai-jun, MEI Sheng-wei, CHEN Ying

(State Key Laboratory of Control and Simulation of Power Systems and Generation Equipments; Department of Electrical Engineering, Tsinghua University, Beijing 100084, China)

Abstract: The present electric grids will definitely be developed into an intelligent power network interdependently composed of the power network and the information network. The characteristics of an intelligent power network are analyzed and the importance of the information network security is emphasized. Various risks as well as malicious attack scenarios to the intelligent power network are analyzed from the aspect of information security, ranging from the information collection, transmission, management and interaction. Furthermore, the impact from the emergency in the information network on the survivability of an intelligent power system is discussed based on the basic features of the coupling between the two networks. Proposals based on modern power system developments are given to enhance the information security of the intelligent power system in key technologies, standards, policies and training.

Key words: smart grid; power network; information network; information security; coupling network; survivability

1 引言(Introduction)

智能电网从提出至今, 尚没有一个统一的概念. 不同国家和地区根据自身电网的特点和发展的需要, 制定了相应的智能电网发展规划[1−3]; 不同科研机构和学者根据自己的理解阐述了具有学科特色的智能电网[4−7]; 不同的公司作为参与智能电网建设的商业主体, 从自身的业务范围和经营利益出发描绘了智能电网应具备的功能和特点[8−11].

虽然各方对智能电网的定义并不相同, 但其基本思想大体上可以表述为通过数字化和信息化将电能的生产、输送、分配和使用等各个环节紧密联系在一起, 通过智能化的控制实现“经济高效、灵活互动、友好开放、清洁环保”的新一代电力系统. 其中, 信息化是实现智能电网基础功能的重要前提. 随着信息技术在电力系统基础设施和高级应用中的深度渗透, 相互依存的信息网和电力网将成为未来智能电网的重要组成部分[12].

可以预见, 随着智能电网实践的深入, 电力企业和电力用户侧的信息化将得到极大的提高. 对电力企业而言, 信息化的深入为企业带来更高的生产效率和管理水平; 对电力用户而言, 信息化的普及则意味着更经济的用电方式和更好的用户体验. 然而, 信息化的深入和普及在为电力企业和用户带来众多利好的同时, 也给智能电网的运行安全埋下诸多隐患. 一方面, 信息技术发展十分迅速, 许多技术发展过程中遗留的安全漏洞并没有得到有效解决, 甚至还有不少尚未发现的安全隐患[13−16], 近年来发生的利用信息网络攻击工业系统的重大事件更是引发了广泛的关注和担忧[17−18]; 另一方面, 信息网和电力网相互影响和作用的机理目前尚不明确, 针对二者构成

收稿日期: 2011−06−17; 收修改稿日期: 2011−09−28.
基金项目: 国家自然科学基金资助项目(50807026, 50977047); 中国博士后科学基金资助项目(20110490351).

的相互依存复合网络脆弱性的恶意攻击很有可能造成大范围的连锁停电事故[19–21]. 因此, 有必要分析智能电网运行过程中的信息安全隐患, 并从复合网络的角度探讨信息安全对电力系统生存性的影响. 需要说明的是, 有关智能电网信息安全的研究, 笔者在文献[12]中已从复杂网络的角度予以综述和展望, 而本文则从电力信息安全的角度思考未来电网安全性问题, 即可认为是对文献[12]的有益补充和深入.

本文首先介绍了智能电网信息化条件下的网络特征, 分析了信息化背景下智能电网中存在的安全性问题, 并针对各类隐患预想了特定攻击条件下可能的安全性事故场景. 进一步, 探讨了信息网络安全对电力系统生存性的影响. 最后, 讨论了提高智能电网信息安全水平和电力系统生存性的可行对策和改进措施.

2　智能电网网络特征(Network characteristics of smart grid)

未来智能电网从总体上可以视为由信息网和电力网这两个相互依存的网络构成的一个复合网络, 如图1所示.

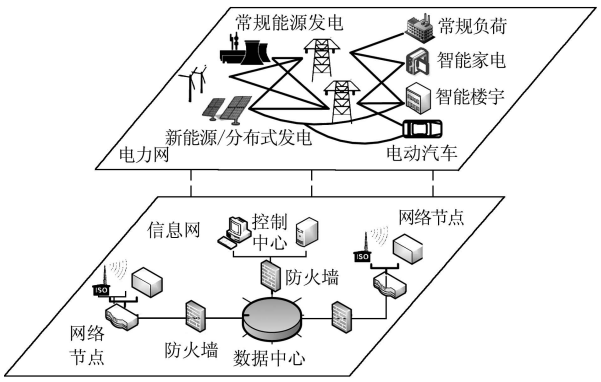

图 1　电力网和信息网构成的复合网络

Fig. 1　Interdependent network composed by power grid and information grid

为了叙述方便, 将电力网中的节点简化为电源节点和负荷节点两大类, 二者通过输电线进行连接. 在双向通信的条件下, 将信息网络中的节点也简化为两类: 一类是信息采集/指令执行节点, 负责对控制范围内的负荷和电源的状态信息进行采集和上传, 并根据接收到的控制指令对负荷和电源节点的状态执行调整操作; 另一类是信息处理/指令生成节点, 负责对采集到的信息进行汇总分析和生成控制指令. 信息网络中的节点通过光纤和无线网等实现连接.

电力网和信息网的相互依存主要体现在两个方面: 信息网络中节点的正常运行需要电力网中邻近的电源节点提供工作电源; 电力网络的安全、可靠、经济运行有赖于信息网中各节点的正常工作.

从网络的规模来看, 电力网和信息网均属于超大规模的复杂网络. 文献[21]指出, 复合网络的运行安全风险在某些情况下远大于单一的复杂网络. 从这个角度来看, 智能电网的安全性不容忽视, 这其中, 信息网络的安全性则是重中之重. 主要原因如下:

1) 从网络发展的成熟度来看, 信息网存在的安全隐患更多. 即使在信息技术高度发达的今天, 信息网络中仍有许多已知的安全漏洞尚未解决, 且还会出现更多的新漏洞, 这为攻击提供了许多可能的渠道. 与之不同的, 对电力网的攻击往往需要借助于物理手段, 攻击的成本比较高, 且受天气和地理条件的限制较多.

2) 从运行过程中的相互依赖关系来看, 电力网的正常运行对信息网的依赖程度更高. 电力网中电源节点出力的调整和负荷节点的投切等操作均是借助于信息网络来实现. 如果信息网络出错或崩溃, 电力网络一般很难保持正常运行. 另一方面, 信息网络虽然需要借助于电力网络的电源支持, 但由于重要的信息网络通常配有不间断电源系统, 短时停电并不会对信息网络造成大的影响.

3) 从网络故障的传播特性来看, 信息网的故障更容易造成大范围的停电. 由于信息流动的成本远低于能量流动的成本, 这使得信息网络比电力网络具有更强的互联互通性, 信息流可以在较大的范围内频繁地进行交互. 因此, 信息网络出现故障时受影响的范围将更为广泛.

智能电网的网络结构决定了其运行风险既来源于电力网络的安全性, 也来源于信息网络的安全性, 而这其中, 信息网的安全及其对电网带来的运行风险需要引起大家的高度重视.

3　智能电网信息安全(Smart grid information security)

智能电网信息化的主要特点可以归纳为两个方面, 一是对传统电力系统中发电、输电、配电、用电等各个环节的高度信息化, 二是促进“售电”和“受电”参与各方的信息互动化. 信息化为未来智能电网的安全运行带来了许多问题:

1) 信息采集环节的安全性. 在智能电网中, 各类高级传感器和测量表计将广泛用于对电力系统和电力用户状态进行监测. 电力系统和用户状态的高度信息化为保障智能电网的安全、可靠和经济运行提供了重要基础. 比如, 借助于各类智能表计采集的大量数据, 可以对电网设备的健康状况和电网的完整性进行评估, 对潜在的危险进行预警和有效的规避, 还可以通过智能表计发布实时电价和优惠政策, 实现与用户的沟通, 协助用户制定经济的用电策略.

未来的智能电网将取消所有的电磁表计及其读取系统, 取而代之的是可以使电力公司与用户进行

双向通信的智能固态表计. 出于成本的考虑, 智能表计一般不会加入复杂的加密技术, 这导致智能表计比较容易被破解和控制. 一旦这些设备受到控制, 则攻击者既可以利用其向电网提供虚假用电信息, 影响电网供给; 又可以通过其向用户提供不合理的电价信息, 影响用户侧的用电方式. 极端情况下, 还可以使大量智能表计与电网断开通信, 使电网无法实时掌握系统用电情况, 从而造成更大的事故.

2) 信息传输环节的安全性. 建立高速、双向、实时、集成的通信系统是实现智能电网的基础. 一方面, 大量从智能表计获得的数据需要通过高速通信网络及时地传输到数据处理中心; 另一方面, 电力企业也需要将电价信息和相关优惠政策通过通信系统实时地进行发布. 相比于传统电网, 智能电网中需要监测和控制的设备数量更多, 分布更广. 为了实现全面和实时的监控, 成本低廉的无线通信网和分布广泛的公用因特网将在智能电网通信系统中占有越来越多的比重. 通过无线网络和公用因特网可以方便地构建多通道的冗余通信网络, 从而实现可靠的通信. 然而, 电力系统中公用网络的大量接入为恶意攻击提供了更多的入口. 由于无线网络的安全标准目前尚处在早期应用阶段, 有许多已经暴露出来的安全性漏洞还没有得到妥善解决, 信息传输的安全性还有待进一步提高. 文献[13]指出, 只需要70美元左右的成本即可对基于IEEE 802.15.4无线传感器网络发起一次拒绝服务攻击. 此外, 对于专业的攻击者而言, 多入口的公用因特网环境为发起多点协调的攻击提供了可能性, 这将为电网和用户带来更大的危害.

3) 智能控制的安全性. 从电网侧来看, 智能控制系统可以利用搜集到的各类信息对电网状态进行分析、诊断和预测, 并及时采取适当的措施对电网运行状态进行调节, 使之运行在安全、可靠和经济的状态; 从用户侧来看, 内嵌有智能控制技术的家用电器, 如热水器、空调和电动汽车等, 可以根据电网状态自动调节用电计划, 从而获得实实在在的经济利益. 此外, 公共用电场合, 如公交汽车充电站、写字楼等还可以通过其中用电设备之间的智能协调控制来降低整体用电成本. 然而, 上述应用成功的前提条件是智能电器的控制权得到正确的使用, 如果智能电器之间的信息交互安全性缺乏保障, 则很有可能被攻击者利用, 不仅电器不能正常工作, 还很有可能因大量电器的控制权被攻击者获取用于对电网负荷形成较大规模的冲击.

4) 电网和用户互动环境下的安全性. 智能电网的重要特征之一是鼓励用户参与, 实现电网和用户的互动化. 电网通过将用户纳入电力系统的运行和管理以更好地实现供需平衡关系, 提高系统运行的可靠性和经济性. 而用户则根据其电力需求和电力系统当前的状态来制定科学的用电方式, 从而获得经济上的收益. 这一互动过程使得用户用电行为受系统状态的影响也越来越广泛. 专业的攻击者可以利用互动过程对电力系统造成更大的破坏. 比如通过信息网络向用户侧发布虚假的低电价信息, 使得大量智能负荷, 如电动汽车充电站、智能热水器和智能空调等, 同时启用造成系统过负荷; 与此同时, 通过控制传感器网络向电网侧提交伪造的低负荷信息使得电网减少电力供应, 从而对电力系统的稳定和用户的用电安全造成巨大的危害.

5) 其他安全性问题. 出于信息交互的需要, 每个家庭的用电负荷、设备构成以及用电规律等个人隐私将出现在信息网上. 同时, 电力市场化的需要使得电力企业的实时电价政策等重要信息也将在网络上传输. 这些信息均有可能被不法分子截获、篡改甚至用于其他非法用途.

4 信息安全与电力系统生存性(Information security and power system survivability)

一般而言, 生存性是指系统在遭受攻击、出现故障或发生意外事故时, 依然能够及时完成任务的能力[22]. 未来智能电网从宏观上看将演变成一个由信息网和电力网为主体的复杂交互网络. 在发生系统内部故障、恶意攻击以及自然灾害等情况时均有可能导致电网瓦解, 进而引发大面积停电事故. 因此, 为了保障电力系统的安全运行, 不仅要控制和消除电力系统信息化新元素带来的安全隐患, 还要从系统完整性的角度研究系统局部失效或遭受攻击之后整个系统的生存性.

信息安全对电力系统生存性的影响主要表现在以下两个方面:

1) 网络间功能的强耦合性. 一方面, 分布广泛的信息网络需要与之配套的电力网络为其提供工作电源. 另一方面, 电力网络中几乎所有功能的实现都需要借助于信息网络提供的服务. 电力网和信息网的这种强耦合性, 使得大停电事故更加容易发生. 例如, 通过对信息网中的关键节点发动攻击, 使得相应的电力网络中的关键电厂停机或重要输电线出现过载, 可以造成与该信息节点对应的电力节点失效. 换言之, 在智能电网条件下, 信息网络和电力网络之间的故障可以相互转化. 由于信息网络目前具有许多已知安全漏洞, 可以用来发起攻击的入口很多, 且不受时间、地点和天气等因素的影响, 所需成本极低且攻击手段更为隐蔽, 因而对电力系统的危害性也更大. 因此, 未来对智能电网的攻击形式很有可能从传统的对物理电力系统的直接攻击转为对与之相对

应的信息系统的攻击.

2) 网络间故障的传播性. 目前, 关于电力系统连锁故障的研究已有了许多成果, 但研究对象大多局限于电力系统内部传播的故障. 在信息网和电力网相互依存的智能电网中, 故障的传播形式有了更多的可能性. 对于相互依存两个网络, 当其中一个网络中的某个节点失效时, 将会引发另一个网络中相关节点的失效. 随着这一过程在两个网络中的交替出现, 失效节点数将迅速增加, 网络出现大面积故障, 最终导致全网崩溃. 值得担忧的是, 未来的智能电网为网络间故障的传播提供了很好的平台. 文献[21]指出, 相互依存网络和单一网络的复杂性特征也有很大的不同. 比如对于单一网络而言, 网络的度分布越平均, 则其对于随机故障越鲁棒, 而对于相互依存的网络而言, 网络的度分布越平均则其对于随机故障越脆弱. 这表明, 对于由相互依存网络构成的智能电网, 其内部故障传播的条件也与以往研究中的单一电力网有了很大的不同. 需要指出的是, 文献[21]中构成复合网络的两个子网络均采用的是随机图模型, 而对于智能电网这一具体的复合网络, 其中的信息网多为无标度网, 电力网则多呈小世界网, 一旦信息网络出现连锁故障, 更容易造成全网出现崩溃.

5 建议和对策(Suggestions)

1) 加强信息安全技术研究. 智能电网的信息安全需要从信息的采集、传输、处理和交互等各个环节加强保障. 针对智能仪表数据采集和储存开展数据加密存储和传输的研究; 开展对无线网络中安全传输协议以及有线网络中防火墙技术和安全认证技术的研究; 完善网络与信息安全预警、通报、监控和应急处置平台, 形成有效的安全技术防护体系.

2) 制定信息安全标准体系. 目前, 国外关于智能电网信息安全标准体系的研究已经走在了前列. 在加强对国外相关安全标准的研究和借鉴先进的研究成果的同时, 还应由既了解我国电网实际情况, 又了解信息安全的专家组对我国信息安全标准体系进行科学的规划, 以此为指导制定信息安全标准体系. 同时, 还要推进信息安全标准在行业内的合理部署和实施. 如此, 则有望避免智能电网的无序建设引入的大量安全隐患.

3) 完善相关的政策法规. 智能电网的建设牵涉到政府、用户、电力企业、IT公司和设备制造商等众多参与者. 政府需要根据参与各方在智能电网中扮演的角色制定合理的政策. 通过出台政策规定各方应承担的责任和义务, 同时要制定相应的法律法规来规范参与各方的行为, 切实保护用户隐私和电力企业关键信息的安全, 使智能电网的建设和运营更加的科学、有序.

4) 建立信息安全培训体系. 对于大多数用户而言, 信息安全还是一个十分复杂的概念, 而用户作为智能电网中参与数量最多的一个主体, 其安全意识的高低直接影响到智能电网运行的整体安全水平. 因此, 完善的信息安全培训体系是提高智能电网信息安全的重要保障.

5) 加强对相互依存网络相关理论的研究. 如前所述, 全面地掌握相互依存网络的行为特性是防止未来智能电网发生大停电事故的前提, 为此需要研究并解决很多关键科学问题. 如相互依存网络的静态和动态特性的数学描述模型; 相互依存网络故障传播的理论和分析方法; 相互依存网络的脆弱性、可靠性等指标评价体系. 此外, 不同国家和地区的电力网和信息网的发展水平和网络特点也不尽相同, 需要结合实际情况进行建模和分析.

6 结论(Conclusions)

未来智能电网从整体上可以看作是由电力网和信息网构成的相互依存复合网络, 其中信息网络的安全及其对电力系统运行安全带来的风险不容忽视. 本文通过分析未来智能电网的网络结构特征, 阐明了信息网络安全对智能电网安全的重要性. 从信息的采集、传输和交互等各个环节分析了智能电网的信息安全问题. 进一步, 结合相互依存网络的特点, 分析了信息网络安全对智能电网安全带来的影响. 从关键技术的研究、技术标准的制定以及政策法规的完善等几个方面提出了提高智能电网安全性的建议.

参考文献(References):

[1] United States Department of Energy Office of Electric Transmission and Distribution. “GRID 2030” a national vision for electricity’s second 100 years[EB/OL]. [2009–05–09]. *http://www.climatevision.gov/sectors/electricpower/pdfs/electric_vision.pdf*.

[2] European SmartGrids Technology Platform. Vision and strategy for Europe’s electricity network of the future[EB/OL]. [2009-03-15]. *http://www.smartgrids.eu/documents/vision.pdf*.

[3] HAASE P. Intelligrid: a smart network of power[EB/OL]. [2005]. *http://mydocs.epri.com/docs/CorporateDocuments/EPRI_Journal/2005-Fall/1012885_IntelliGrid.pdf*.

[4] 何光宇, 孙英云, 梅生伟, 等. 多指标自趋优的智能电网[J]. 电力系统自动化, 2009, 33(17): 1 – 5.
(HE Guangyu, SUN Yingyun, MEI Shengwei, et al. Multi-indices self-approximate-optimal smart grid[J]. *Automation of Electric Power Systems*, 2009, 33(17): 1 – 5.)

[5] 余贻鑫, 栾文鹏. 智能电网[J]. 电网清洁能源, 2009, 25(1): 7 – 11.
(YU Yixin, LUAN Wenpeng. Smart grid[J]. *Power System and Clean Energy*, 2009, 25(1): 7 – 11.)

[6] 余贻鑫, 栾文鹏. 智能电网述评[J]. 中国电机工程学报, 2009, 29(34): 1 – 8.
(YU Yixin, LUAN Wenpeng. Smart grid and its implementations[J]. *Proceedings of the Chinese Society for Electrical Engineering*, 2009, 29(34): 1 – 8.)

[7] 武建东. 智能电网与中国互动电网创新发展[J]. 电网清洁能源, 2009, 25(4): 5 – 8.
(WU Jiandong. Innovative development of smart power grid and interactive smart grid in China[J]. *Power System and Clean Energy*, 2009, 25(4): 5 – 8.)

[8] IBM Corporation. Powering an energy transformation the intelligent utility network from IBM[EB/OL].[2009-05-01]. *http://www-03.ibm.com/industries/global/files/energyu_powering_an_energy_transformation2.pdf*.

[9] MARTIN L. Cisco: Smart grid will eclipse size of Internet[EB/OL]. *http://news.cnet.com/8301-11128_3-10241102-54.html*.

[10] MARTIN L. Microsoft eyes smart grid with utility software[EB/OL]. *http://news.cnet.com/ 8301-11128_3-10374771-54.html*.

[11] BERST J. Google Jumps into Smart Grid[EB/OL]. [2009-02-09]. *http://www.smartgridnews.com/artman/publish/companies/Google_Jumps_Into_Smart_Grid.html*.

[12] 梅生伟, 王莹莹, 陈来军. 从复杂网络视角评述智能电网信息安全研究现状及若干展望[J]. 高电压技术, 2011, 37(3): 672 – 679.
(MEI Shengwei, WANG Yingying, CHEN Laijun. Overviews and prospects of the cyber security of smart grid from the view of complex network theory[J]. *High Voltage Engineering*, 2011, 37(3): 672 – 679.)

[13] BOYER W F, MCBRIDE S. Study of Security Attributes of Smart Grid Systems–Current Cyber Security Issues[EB/OL]. [2009-04-29]. *http: // www.inl.gov/scada/publications/d/securing_the_smart_grid_current_issues.pdf*.

[14] ANAND M, CRONIN E, SHERR M, et al. Security Challenges in Next Generation Cyber Physical Systems[EB/OL]. [2006]. *http://www.truststc.org/scada/papers/paper33.pdf*.

[15] GRANT R L. Smart Grid Implementation: Strategies for Success[EB/OL]. [2010-05-13]. *http://www.lexingtoninstitute.org/library/resources/documents/Energy/Smart_Grid_Implementation.pdf*.

[16] BENOIT J. Meeting IED integration cyber security challenges[EB/OL]. [2008-11-12]. *http://www.cooperpowereas.com/PDF/Meeting_IED_Integration_Cyber_Security_Challenges.pdf*.

[17] McAfee Foundstone Professional Services and McAfee Labs. Global Energy Cyberattacks: “Night Dragon”[EB/OL]. [2011]. *http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf*.

[18] MATROSOV A, RODIONOV E, HARLEY D. “Stuxnet Under the Microscope”[EB/OL]. [2010]. *http://www.esetnod32.ru/.company/.viruslab/analytics/doc/Stuxnet_Under_the_Microscope.pdf*.

[19] BOMPARD E, NAPOLI R, XUE F. Vulnerability of interconnected power systems to malicious attacks under limited information[J]. *European Transactions on Electrical Power*, 2008, 18(2): 820 – 834.

[20] VESPIGNANI A. The fragility of interdependency[J]. *Nature*, 2010, 464(15): 984 – 985.

[21] BULDYREV S V, PARSHANI R, PAUL G, et al. Catastrophic cascade of failures in interdependent networks[J]. *Nature*, 2010, 464(15): 1025 – 1028.

[22] 丁道齐. 复杂大电网安全性分析[M]. 北京: 中国电力出版社, 2010: 280 – 281.
(DING Daoqi. *Network Security Analysis of Large Complex*[M]. Beijing: China Electric Power Press, 2010: 280 – 281.)

作者简介:

陈来军 (1984—), 男, 博士, 助理研究员, 研究方向为电力系统仿真、智能电网信息安全分析, E-mail: chenlaijun@mail.tsinghua.edu.cn;

梅生伟 (1964—), 男, 博士, 教授, 长江学者, 研究方向为电力系统分析与控制, E-mail: meishengwei@mail.tsinghua.edu.cn;

陈 颖 (1979—), 男, 博士, 副教授, 研究方向为电力系统动态仿真、并行和分布式计算, E-mail: chen_ying@mail.tsinghua.edu.cn.