

配电网信息物理系统可靠性评估关键技术探讨

蒋卓臻, 刘俊勇, 向月

(四川大学 电气信息学院, 四川 成都 610065)

摘要: 信息物理高度融合是未来智能配电网的发展趋势, 主要针对配电网信息物理系统(CPS)可靠性评估关键技术进行综述与展望。从配电网信息空间、物理空间的风险来源挖掘入手, 进一步对信息物理相依存下的影响因素进行总结和分析; 在此基础上, 归纳总结了配电网物理系统、信息系统各自典型的可靠性指标分类方式与具体数学表达以及两者耦合下的可靠性指标构建技术, 进而总结了配电网 CPS 可靠性评估算法与方法的研究进展; 从配电网 CPS 异构数据处理、信息物理关联的建模与仿真、配电网 CPS 可靠性评估指标与方法、配电网 CPS 广义攻击与防御机制 4 个方面进行了展望。

关键词: 信息物理系统; 智能配电网; 广义攻击; 可靠性评估; 防御机制

中图分类号: TM 761

文献标识码: A

DOI: 10.16081/j.issn.1006-6047.2017.12.005

0 引言

能源与环境问题事关人类社会的生存和可持续发展。近年来, 国家层面提出了“互联网+”的战略部署, 信息化建设越来越成为支撑社会发展的重要措施之一^[1-2]。世界各国都希望通过融合先进的信息技术, 能够最大限度地采集、分析来自能源系统各个环节的信息, 并且在此基础上优化能源结构, 充分地利用多种能源特别是可再生能源, 提高能源供给的可靠性和安全性^[3-4]。Rifkin 提出了能源互联网的概念^[5], 能源互联网是指以电力系统为核心, 结合交通、天然气等系统构成的复杂系统^[6]。但是信息系统和能源一次系统的深度融合会引起严重的信息安全问题。

配电网作为经济社会发展的重要基础设施, 对实现智能电网和能源互联网的战略目标起着关键作用^[7]。智能电网与能源互联网都是典型的信息物理系统(CPS), 信息环节的可靠性问题可能导致物理系统的运行风险。据不完全统计, 80% 以上的用户停电缘于配电系统故障^[8]。因此, 对配电系统可靠性的研究已经引起了广泛的关注^[8-12]。现阶段, 大量智能电子设备接入配电网, 以电力设备为核心的传统配电网已逐渐演变为信息物理高度耦合的配电网 CPS^[11-14]。高级信息技术的引进改善了电网的运行, 但是也给电力系统运行的可靠性和安全性带来了潜在的负面影响^[15]。信息系统中的安全风险也可能导致电力系统发生停电事故。乌克兰大停电事故就

是一起电力二次系统遭受网络攻击后引发一次系统故障的典型案列。恶意代码攻击部分变电站监控系统, 导致发电设备故障, 引发乌克兰大范围停电^[16]。因此, 考虑信息系统影响的配电网可靠性评估才能准确地反映配电网可靠性的真实性能。

现有的可靠性分析^[17-18]与风险评估^[19]主要是基于物理元件和拓扑结构的静态非实时概率统计方法, 研究大多孤立地看待物理系统和信息系统。相较于输电网, 配电网中含有大量缺乏完善物理保护的终端设备, 如广泛分布于整个配电网中的智能远动终端, 由于缺乏有效的物理隔离防护, 网络攻击者可以更轻松地入侵这些终端设备, 并以此为跳板攻击配电自动化系统中的其他设备; 另外, 由于各类终端设备的计算和信息处理能力往往非常有限, 计算机网络中一些常用的信息安全技术, 如完善的加密技术等, 难以被直接应用到配电自动化系统中, 故配电自动化系统更易受到网络攻击的威胁。所以, 随着信息系统对电网可靠性影响的加深, 物理和信息的耦合特性^[20-22]需要得到进一步重视, 进行配电网 CPS 可靠性研究是必要的。配电网 CPS 可靠性评估是目前的研究热点问题之一, 有必要紧跟学术界发展的最新动向, 聚焦热点和关键技术问题, 剖析其发展趋势。配电网 CPS 可靠性关键技术涵盖建模、指标、方法等多个方面, 形成从机理分析到应用方法研究的一个完整的技术体系。本文从辨识可靠性影响因素入手, 研究了配电网 CPS 可靠性的评估指标和方法, 总结了目前国内外考虑信息系统影响的配电网可靠性研究进展, 并探讨了今后的研究方向。

1 可靠性影响因素探讨

随着智能电网和能源互联网战略的推进, 大量电气设备、数据采集设备和计算设备接入配电网, 用电

收稿日期: 2017-05-31; 修回日期: 2017-11-07

基金项目: 中央高校基本科研业务费专项资金资助项目(YJ201654); 四川省电力电子节能技术与装备重点实验室开放基金项目(szjj2017-052)

Project supported by the Fundamental Research Funds for the Central Universities(YJ201654) and the Open Research Subject of Key Laboratory of Sichuan Power Electronics Energy-saving Technology and Devices(szjj2017-052)

需求不断增长、分布式能源 DER(Distributed Energy Resources)的大规模并网、电动汽车 EV(Electric Vehicle)的广泛使用都使配电网的复杂性空前增加^[11-12]。如图 1 所示,传统配电网已逐渐演变为配电网 CPS,它是 CPS 在电力系统中的一种具体应用形式。配电信息网与物理网简化耦合的示意图如图 2 所示^[16],配电网 CPS 网络中的每个节点由信息网络和电力网络中的对应节点映射得到,节点可同时与电网、信息网络进行实时交互,信息节点受价格信号、网络攻击等因素的影响,物理节点受负荷波动、电能质量等因素影响。

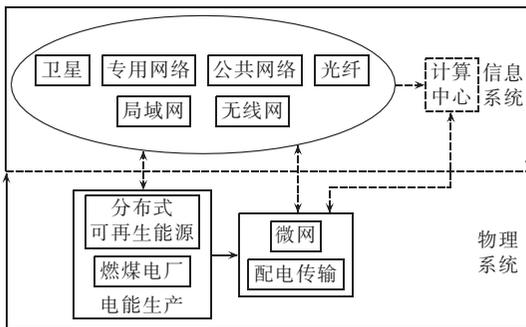


图 1 配电网信息系统与物理系统的交互
Fig.1 Integration of cyber system and physical system in distribution network

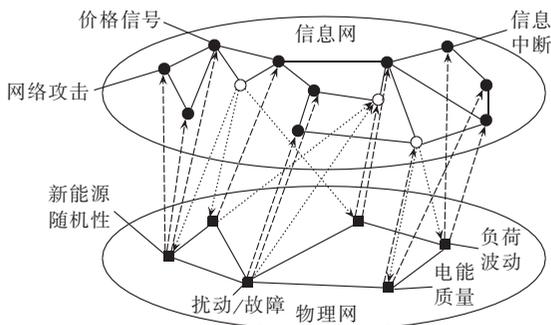


图 2 信息网与物理网的耦合关系示意图
Fig.2 Coupling relationship between cyber network and physical network

1.1 信息空间风险来源

信息系统的安全是一个动态的复杂过程,它贯穿于信息系统的整个生命周期。信息系统安全的威胁来自内部破坏、外部攻击、内外勾结等攻击以及信息系统本身所产生的意外事故等,必须对可能的威胁和需要保护的信息资源进行风险分析,选择适当的安全措施,妥善应对可能发生的安全风险^[23]。

在未来的配电网 CPS 中,越来越多的具有通信和信息处理能力的智能电子设备将被安装在电力系统的各个环节,广域测量系统 WAMS(Wide-Area Measurement System)的采集周期为毫秒级,可以准确地反映电网运行状态,带来的数据量增长是成百上千级;高级测量体系 AMI(Advanced Metering In-

frastructure)面向的是庞大的用户群体,收集海量用户用电信息,通过这类数据可以进行风电、光伏以及负荷曲线短时间的预测。上述数据构成了电网数据的基础,信息网络需要采集、传输和处理海量多源异构信息,电力数据呈爆发式增长^[24]。这些数据中蕴含着电网运行的宝贵信息,用于可靠性分析与辅助决策可有效地保障系统安全,但是不同结构的信息应用平台和数据库结构存在差异,而且存在大量的重复数据,影响可靠性分析的效率。因此,亟需大数据相关的采集及预处理技术来获取并处理来自不同设备的海量信息流、能量流的状态数据样本,为电网可靠性的计算打下坚实基础。

实际上,智能设备的引进带来了潜在的安全风险,电力信息网络可靠性与网络组件^[25]、通信介质^[26]、网络拓扑^[27]、路由协议^[28]和业务对象^[29]等多种因素有关。而且,这些影响因素也成为可靠性管理与控制的主要障碍^[30]。例如,开放式的通信协议(如 IEC61850 标准)提高了各种通信设备的可用性,也给信息系统带来了更多安全隐患。发生在通信链路上的冒充、窃听、重放等类型的网络威胁,可能破坏电力系统的正常运行。如图 3 所示,信息空间中的潜在安全攻击包括 5 个方面^[31]。

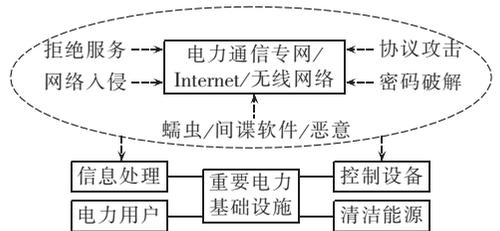


图 3 配电网信息空间中的安全威胁

Fig.3 Security threats in distribution network cyber system

在配电网 CPS 中,信息空间的安全风险不容忽视。信息空间中的风险很有可能传递到电力空间中并导致电力设备故障,降低系统可靠性。例如,恶意攻击者可以通过控制中心局域网、企业局域网、变电站局域网或数据采集与监控 SCADA(Supervisory Control And Data Acquisition)系统通信链路窃听,对配电系统注入假状态信号进行攻击。从分布式系统可靠性的角度来看,这些网络攻击路径可以被视为串联连接的组件,对每个组件的成功网络攻击可能导致一些负载点或整个配电馈线的供电中断。图 4 给出了电力系统 SCADA 系统信号传递的抽象视图^[32],实线箭头表示变电站与控制中心间的信号传递,变电站将检测信号传递到控制中心,控制中心发送动作指令到变电站;类似地,虚线箭头表示企业与控制中心间的信号传递。

调度自动化系统、变电站自动化系统涉及遥断断路器进行倒闸操作,容易遭受网络攻击。智能电

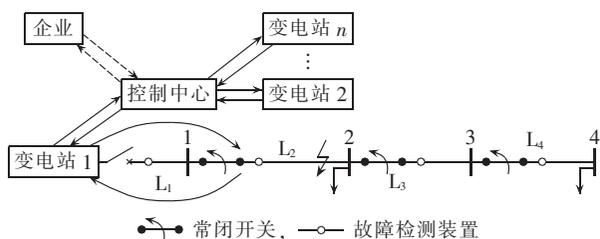


图 4 SCADA 系统信号传递示意图

Fig.4 Signal transmission in SCADA system

表是采集用户数据的主要设备,分布广,多采用无线专网方式通信,攻击的技术门槛较低,其计算和通信资源有限,只能依赖基于密钥的身份认证和通信加密保障安全,一旦加密算法被破解,智能电表将直面网络攻击的威胁。2014年,研究人员破解了西班牙电网公司智能电表采用的 AES-128bit 对称加密算法,将恶意代码注入电表,不但可以调整电量读数实现窃电,还可以此为跳板攻击相邻电表,若不能及时检测,可能使故障蔓延造成大停电事故^[33]。

1.2 物理空间风险来源

物理空间的风险源于系统中的各种扰动和故障。配电网在源(电源)、网(硬件设备)、荷(电力负荷)、变(能量转换单元)4个部分都会受到不同程度的扰动,包括传统的配电网线路、变压器等电气元件的故障,DER、EV 随机接入产生的扰动,市场环节造成的大规模能源接入与断开,恶意攻击,无意错误如误操作等。

电气元件故障是配电网的风险来源之一,分为恶意攻击(不良的偷盗行为、工程施工以及车辆的破坏等)和无意错误(自然老化、绝缘故障,风筝、气球等人为因素)。配电网对于其所处的气候状况、地理位置等因素,具有较高的敏感性^[34]。由于配电网设施的建设地点通常处于较为偏僻的地方,因此,当地理环境与气候状况发生变化时,将会影响配电网的故障率。配电网结构的形式通常是多种多样的,包括辐射形结构(放射形结构)、环网结构、树干形结构、网状结构和复合结构等。如果采用的是辐射形结构,在同一回路的馈线上,往往存在多条复合线,而越是靠近回路根部的点出现故障,给整条线路造成的影响越大,其可靠性越低^[34]。

配电网智能化的发展离不开分布式电源 DG (Distributed Generation) 和 EV^[35]。DG 不仅能合理有效地利用多种可再生能源发电并减少对环境的污染,而且能满足电网负荷增加的需求。但是受季节与天气状况的影响,DG(如风电、光伏发电等)出力具有不确定性,风速的随机性引起风机输出功率的不确定性,太阳能辐射的随机性引起光伏输出功率的不确定性,这些都会给含 DG 的配电网可靠性带来影响。EV 充放电功率存在较多不确定性与随机性,

突发性的大规模 EV 充电势必会对配电网的结构、运行产生巨大的影响,用户的无控制充电行为容易与原有的负荷高峰叠加形成新的负荷高峰,从而对电网造成攻击,影响其正常运行。对于同时含有 DG 和 EV 的配电网而言,如果不协调 EV 充放电随机性和 DG 随机性之间的关系,不仅会造成发电成本增加和资源的浪费,还会大幅降低配电网的运行可靠性。值得说明的是,电网不同设备采集的电力数据包含电压相位等相量数据和有功功率等标量数据。此外,电力数据的不同还包括时间尺度差异(如风电数据、光伏数据等),统计的即使都是功率量,但是也属于不同时间尺度数据。同时,不同类型 EV 可能存在不同的数据导入方式,也可能成为异构数据的一部分。

1.3 信息系统对物理系统可靠性的影响因素

美加 8·14 大停电发生的一个重要原因是状态估计功能退出运行,调度人员失去了对电网实时状态的感知能力,未能及时发现故障,最终使故障蔓延^[36]。2008年6月5日的《华盛顿邮报》报道,历时 48 h 的美国佐治亚州核电站紧急关闭时间是由于网络故障(软件更新故障)导致的^[3]。2015年12月23日,乌克兰国内多个区域的电网因遭遇黑客攻击,发生突发性停电事故,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^[37],此后信息物理安全问题引起了学术界的广泛关注。信息对物理系统可靠性的影响程度主要取决于信息功能在电网故障处理及恢复中的作用,信息系统对物理系统的交互影响可以分为 4 种模式^[38]: 元件对元件的直接影响 DEEI (Direct Element-Element Interdependency)、网络对元件的直接影响 DNEI (Direct Network-Element Interdependency)、元件对元件的间接影响 IEEI (Indirect Element-Element Interdependency)、网络对元件的间接影响 INEI (Indirect Network-Element Interdependency)。通过上述 4 种模式可以描述信息系统元件或信息网络故障引起物理系统直接故障和潜在故障的关系。

相关学者则将信息系统功能对一次系统的作用简化为直接作用类型和间接作用类型^[39-40]。前者指信息空间中的设备故障会直接导致相关电力一次设备故障,如智能终端控制器故障导致断路器误动从而切除负荷;后者则指信息空间中设备故障不会直接导致电力一次设备故障,如监测设备故障可能会使得电力系统运行人员不能及时辨识和预测电力系统潜在的运行风险,但并不会立即导致电力系统故障。Falahati 和 Fu 在划分了信息系统的直接和间接作用类型后,定量评估了智能微电网^[20]和高压变电站^[21]的故障模式,以模拟网络对电力设备的即时和

潜在影响。Lei 等^[41]通过定义网络物理接口矩阵,将基于 IEC61850 的变电站保护系统的可靠性分析分解为单独的实体,即信息系统和物理系统。该矩阵使得将变电站网络设备的故障模式并入复合电力系统模型成为可能。

具有信息发送/接受能力的智能设备的持续发展,是配电自动化进步的关键因素。在这种趋势下,传统手动开关和故障检测设备 FD(Fault Detector)已逐渐被依赖信息系统的遥控开关 RCS(Remote-Controlled Switch)和智能 FD 代替,简单而言,装有此类智能设备的配电网就可以被称为配电网 CPS。一旦配电系统的馈线上发生故障,位于故障位置源侧的 FD 就向控制中心报告故障状态。图 5 给出了智能 FD 的示意图^[32]。

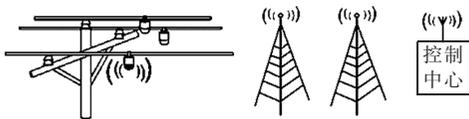


图 5 智能 FD 示意图

Fig.5 Schematic diagram of smart fault detector

智能电子设备的安装给电网带来了新的风险。攻击者通过控制中心局域网、变电站局域网或 SCADA 系统通信链路的漏洞,获得更高的特权级别,模仿配电系统的实际停电情况,然后创建一个假停电计划,并向 RCS 发送错误的跳闸信号。这样信息系统中的风险就传递到物理系统中,导致电力系统不正常运行。

1.4 物理系统对信息系统可靠性的影响因素

物理系统可以从网络设备、通信介质、网络拓扑、电网运行环境等多个方面影响数据分组的传输延时、丢包率和网络吞吐量,进一步影响信息系统的可靠性。例如:通信距离越长,相应的网络分组丢失率越高,信息系统可靠性越低。

网络设备和通信介质都可称为网络组件,网络组件是信息系统的基本构成元素。不同的信息系统包含不同类型的网络组件。网络可靠性是组件可靠性的线性增量函数。这就意味着任何一个组件的可靠性增加,都会提高网络整体的可靠性^[30]。

网络拓扑是包括交换机、路由设备、网管设备等一些构成信息系统基础设备的网络结构。M. Tsubokawa 等^[27]研究了环形和树形 2 种无源光纤网络 PON(Passive Optical Network)结构的可靠性,重点分析了网络设备和光缆的冗余配置对网络整体可用性的影响。

2 配电网可靠性评估指标

2.1 配电网物理系统可靠性评估指标

配电网可靠性评估方面已形成了比较完善的评估算法^[42-44]和指标体系。典型的配电系统可靠性评

估指标包括用户平均停电频率指标、用户平均停电持续时间指标、系统平均停电频率等。文献^[45]将供电可靠性指标分为三大类:持续停电指标、基于负荷量的指标、瞬时停电指标。目前所采用的可靠性指标大多包含在这一指标体系之中,或由这些指标派生而来^[46]。表 1 列出了部分配电网常用的可靠性评估指标^[45]。表中, N_c 为每次停电用户数; N_{total} 为用户总数; T_c 为用户停电时间; N_{outage} 为每次停电用户数; $N_{outagetotal}$ 为停电影响的用户数; $h_{available}$ 为用户供电可用小时数; h_{demand} 为用户供电需求小时数; $N_{outagen}$ 为多次持续停电用户数; L_{outage} 为每次停电损失负荷; L_{total} 为供电负荷总量; O_s 为每次停电的操作次数; $N_{outages}$ 为每次瞬时停电用户数; N_{event} 为瞬时停电事件数; $N_{outagesn}$ 为多次持续瞬时停电用户数; F_{equip} 为设备故障次数; A_{equip} 为设备模拟运行年数; T_{fault} 为故障统计时间; $A_{equiptotal}$ 为设备模拟运行总时间; $T_{faultannual}$ 为设备年停运时间; γ 为设备年停运率。

表 1 配电网可靠性评估指标
Table 1 Reliability assessment index for distribution network

类别	指标名称	指标缩写	指标定义	单位
持续停电指标	系统平均停电频率	SAIFI	$\frac{\sum N_c}{N_{total}}$	次/(户·a)
	系统平均停电持续时间	SAIDI	$\frac{\sum T_c}{N_{total}}$	min/(户·a)
	用户平均停电持续时间	CAIDI	$\frac{\sum T_c}{\sum N_{outage}}$	min/次
	用户总平均停电持续时间	CTAIDI	$\frac{\sum T_c}{N_{outagetotal}}$	min/(户·a)
	用户平均停电频率	CAIFI	$\frac{\sum N_{outage}}{N_{outagetotal}}$	次/(户·a)
	平均供电可用率	ASAI	$\frac{h_{available}}{h_{demand}} \times 100\%$	—
与负荷有关的指标	用户多次停电指标	CEMI _n	$\frac{N_{outagesn}}{N_{total}} \times 100\%$	—
	平均系统停电频率	ASIFI	$\frac{\sum L_{outage}}{L_{total}}$	次
	平均系统停电持续时间	ASIDI	$\frac{\sum L_{outage} \times T_c}{L_{total}}$	min
瞬时停电指标	平均瞬时停电频率	MAIFI	$\frac{\sum O_s \times N_{outages}}{N_{total}}$	次/(户·a)
	平均瞬时停电事件发生频率	MAIFI _E	$\frac{\sum N_{event} \times N_{outages}}{N_{total}}$	次/(户·a)
	多次持续停电或瞬时停电用户比率	CEMSMI _n	$\frac{\sum N_{outagesn}}{N_{total}} \times 100\%$	—
配电设备可靠性	设备年停运率	—	$\frac{F_{equip}}{A_{equip}}$	次/a
	设备年停运时间	—	$\frac{8760 \times T_{fault}}{A_{equiptotal}}$	h/a
	设备每次停运时间	—	$\frac{T_{faultannual}}{\gamma}$	h

当使用上述配电网可靠性指标时,排除重大事件的影响能更好地反映电力系统历年运行指标的变化趋势。

2.2 配电信息系统可靠性评估指标

信息系统在受到恶意攻击或者因管理上的疏忽和发生意外事故的情况下,能否连续工作,能否保证信息的完整性、机密性和可用性^[47],是人们极为关注的问题。这就需要对信息系统在各种威胁下,是否具有足够的保护能力进行客观的评价。

信息系统的可靠性评估存在以下 3 个层次:第一个是信息流层面,根据每个信息流的环节明确物理、网络和业务系统等不同位置上可能面临的威胁、可能暴露的脆弱性能否抵御;第二个是从管理层面考察信息流处理的可靠性策略能否有效地执行;第三个是物理设备和环境安全层次,评估现有的措施是否能够抵御安全威胁。对于信息系统,可以采用综合指标进行可靠性评估,文献[48]从主体、脆弱性、客体、行为等方面提出安全评估指标体系。本文从信息系统可靠性框架的不同层面归纳了如表 2 所示^[23]的评估信息系统可靠性的指标体系^[49-50]。

表 2 信息系统可靠性评估指标

Table 2 Reliability assessment index for cyber system

安全层面	一级指标	二级指标
业务网 安全	信息系统网络 控制可靠性	拓扑健壮性指标
		有效性指标
		认证与访问控制指标
		控制数据保密性指标
	信息系统网络 管理可靠性	控制数据完整性指标
		认证与访问控制指标
		管理完整性指标
		管理数据保密性指标
	信息系统 用户可靠性	业务失败频率
		业务平均终端时间
业务支持时间		
支持响应能力		
用户认证指标		
数据保密指标		
传输网 安全	传输网 可靠性	数据完整指标
		抗毁性指标
		生存性、冗余度关系指标
		故障率
		平均故障间隔时间
		平均传输时延间隔时间
		平均传输错误间隔时间
物理环境 安全	信息设备 可靠性	平均故障时间
		平均故障修复时间
	环境 可靠性	可用性
		抗电磁干扰指标
		电气安全指标
		大气/土壤环境指标
		通信建筑指标

在配电网信息系统可靠性分析中用到的指标基本都是由表 2 延伸得到。例如,通信网络可靠性分析不仅需要考虑业务路径的可靠性,还需要考虑网络设备和物理介质出现失效时对用户的影响范围。在 PON 接入网的可靠性分析中,将连接不可用性 CU

(Connection Unavailability)以及失效影响因子 FIF (Failure Impact Factor)作为衡量网络可靠性的综合指标^[51]。

2.3 配电网 CPS 可靠性评估指标

随着电气物理系统与信息系统的耦合加深,信息系统对电力系统运行的影响越来越不可忽视^[52-53]。因此,分析信息系统与电气物理系统的耦合关系,量化信息系统对电力系统运行的影响,甄别并改善配电网 CPS 的薄弱环节,提出评估配电网 CPS 可靠性的指标,对于保障电力系统的安全稳定运行具有重要意义。

现阶段,在配电网 CPS 可靠性评估方面的研究主要集中在评估模型上,主要利用物理系统的传统指标,很少考虑到网络因素(缺乏信息、信息延迟等)。这些指标大多反映了配电网 CPS 一次系统的运行状态,而不能凸显其信息系统的特点。文献[29]给出了系统可靠性的定量分析模型,考虑了网络系统与物理系统之间的相互作用,SAIDI 和 MAIFI 被用作系统的可靠性评估指标。为了准确评估配电网 CPS 的可靠性,应考虑网络和物理部件的影响^[54],有学者考虑到断路器和变压器的信息功能,通过非连续蒙特卡洛模拟研究电网可靠性^[55],计算结果表明考虑信息作用使系统可靠性得到改善。但是,这种方法在计算时仍使用传统指标——负荷削减概率 LOLP (Loss Of Load Probability)和期望失负荷量 EENS (Expected Energy Not Supplied)来评估电力 CPS 的可靠性。为了满足配电网的发展现状,需要提出融合信息物理特性的配电网可靠性指标。文献[56]利用了材料科学中韧性的概念,提出了一种融合信息系统和物理系统特性的弹性指标,它通过量化给定网络物理系统的弹性水平,得到物理网络和信息网络的相互依赖关系。

研究配电网 CPS 可靠性评估指标不能忽视信息系统的特点。当信息系统与物理系统之间的依存强度较弱时,可以直接采用用户平均停电时间、故障停电平均持续时间等物理系统指标或平均传输时延间隔时间、平均传输错误间隔时间等信息网指标来反映配电网的可靠性;当信息系统与物理系统的耦合关系较强时,信息系统、物理系统异构数据分散处理的可靠性指标不能真实地反映信息物理的融合,需要改进当前可靠性指标,或者设计新的指标来反映这种依存关系下的可靠性。例如,配电网 CPS 中成功的控制策略与智能检测设备、通信介质、开关信号接收和成功动作、反向信号传送有关。通过划分在信息系统的智能设备不可用率反映信息系统的故障状态,物理系统的线路不可用率和设备的不可用率反映物理系统故障状态,可以构建信息物理融合的

可靠性指标——节点不可用率。

设备的不可用率是设备的平均故障时间 MTTF (Mean Time To Failure)和平均修复时间 MTTR (Mean Time To Repair)的函数^[32]:

$$U_{M} = 1 - \frac{MTTF}{MTTF + MTTR} \quad (1)$$

智能 FD 无法运行的概率(不可用率)^[33]为:

$$U_{Mf} = P_{fd}^i + (1 - P_{fd}^i)P_{med}^i \quad (2)$$

其中, P_{fd}^i 为 FD 的故障率; P_{med}^i 为通信介质故障率; $(1 - P_{fd}^i)P_{med}^i$ 表示 FD 工作,但通信介质无法向控制中心发送通知。

RCS 无法运行的概率(不可用率)^[33] U_{ASi} 为:

$$U_{ASi} = P_{df}^i + (1 - P_{df}^i)P_{sw}^i + (1 - P_{df}^i)(1 - P_{sw}^i)P_{ak}^i \quad (3)$$

其中, P_{df}^i 为信号未被接收概率; P_{sw}^i 为开关未成功动作概率; P_{ak}^i 为反向信号传送失败概率。

那么节点不可用率可表示为:

$$U_{Anode} = 1 - A_{line}(1 - U_{Mtr})(1 - U_{Mf})(1 - U_{ASi}) \quad (4)$$

其中, A_{line} 为线路自身的可用率; U_{Mtr} 为根据式(1)所得配电物理系统设备(如变压器)的不可用率。具体事例分析可以参考文献[32]。

3 配电信息物理可靠性评估方法

传统的配电网可靠性分析是利用配电系统拓扑信息和配电系统元件可靠性参数,如元件故障率、平均修复时间、计划检修率等,采用解析法或模拟法评估配电系统的各项指标。模拟法能给出可靠性指标的概率分布,向用户提供大量的信息,但由于其计算费时,工程应用中广泛采用解析法^[57]。现有电力 CPS 可靠性评估方法可以分为 3 类:信息系统和物理系统都采用解析法,信息系统采用解析法而物理系统采用模拟法,信息系统与物理系统均采用模拟法。系统规模小时通常采用解析法,系统复杂程度大时大多采用模拟法^[39,54-55]。文献[54]利用解析法计算得到信息系统可靠性,并将其等效到对应物理元件上,然后利用蒙特卡洛法进行可靠性评估,该方法有效提高了 CPS 可靠性评估的准确性。随着 DG 的大量并网,配电网 CPS 信息系统与物理系统通常采用序贯蒙特卡洛法进行可靠性评估^[58-59]。为了顺应大规模 EV 接入电网的趋势,有必要研究含 EV 的配电网 CPS 可靠性的评估,主要在负荷建模上考虑 EV 的时空不确定性,而在可靠性方面与含 DG 的配电网 CPS 可靠性评估方法类似,都是可以通过蒙特卡洛模拟法模拟系统内元件出现故障后对负荷点及系统可靠性指标的影响程度。

目前,有关电力 CPS 可靠性、安全性的研究已经成为国内外学术界最为关注的热点之一,学者们从不同角度研究了信息系统与物理系统的交互作用。

文献[60]提出了一种电网 CPS 安全评估的思路,评估信息网络中的潜在扰动和故障(如数据中断、数据篡改、数据延时)给物理系统运行所带来的风险。文献[61]综合分析了电力系统可靠性分析评估的方法,基于目前研究探讨了对电网 CPS 进行可靠性评估的发展方向。针对配电网 CPS 的可靠性与风险评估,国内外学者已经进行了一定的研究^[62-66],然而,研究方向主要集中在单一物理层面,其对应方法和模型还在不断地完善,对配电网信息物理融合下的研究还较少。

第一类研究仅针对信息系统建模,分析计算信息系统的可靠性^[67-71],没有考虑信息系统故障对电网的影响。文献[13-14]研究了配电网 CPS 的建模技术。配电信息系统包含 PON、工业以太网、电力载波、无线公网和无线专网等多种通信方式,网络规模大、环境复杂、通信质量较差。现有这类信息系统的建模参照了实际系统的结构,但建模中对实际中影响可靠性的因素如线路长度、外部环境、业务量等考虑不足^[72]。信息系统根据等效模型的复杂程度有模拟法和解析法 2 种。针对信息系统元件如相量测量单元 PMU (Phasor Measurement Unit),由于其具有数据不确定性,采用分层马尔科夫建模技术^[68-69]或综合统计学和模糊马尔科夫法^[70]分析元件可靠性。文献[71]建立解析模型研究了 WAMS 在保护和恢复机制中的多重可靠性指标评估方法。

第二类研究着眼于信息系统在电力系统中的具体应用场景或特定设备(如断路器、变压器^[73-76])的可靠性与安全性评估,如在继电保护系统^[77]、变电站自动化系统 SAS (Substation Automation System)^[78-80]、SCADA 系统^[81-82]、广域闭环控制系统^[83]、广域保护系统^[84]、WAMS^[70,85-86]等,进而分析信息系统故障对电力系统的影响。智能设备、线路保护等系统规模小的应用场景通常采用解析法,系统结构复杂的应用场景一般采用模拟法。文献[87]将马尔科夫建模和状态枚举技术相结合,进行 WAMS 可靠性评估。目前,有关分析信息系统对这些典型场景可靠性的影响也已经有了一些研究成果。文献[54-55]提出了一种考虑信息系统的智能电网可靠性评估模型,采用蒙特卡洛法评估可靠性,但还是缺少对信息系统多元用户行为等信息特征的详细描述,没有量化分析信息系统故障对一次系统的影响。文献[85]则着重研究 WAMS 失效导致部分电网不可观测时,所导致的电网最优负荷削减模型变化及其产生的影响。文献[86]基于蒙特卡洛法分析 WAMS 故障对电力系统可靠性的影响。文献[88]利用蒙特卡洛法分析信息系统对微电网运行可靠性的影响,提出一种可以推广到配电网 CPS 建模和分析的方法。文献[89]研究

了基于 IEC61850 系统功能分解的变电站自动化系统的可靠性评估方法。

第三类研究重点关注信息系统网络层面对电网可靠性的影响,大多是借鉴传统的计算机网络分析方法完成的,更多的侧重于恶意攻击条件下的脆弱性分析。许多研究详细分析了信息攻击的策略与算法,攻击者通过注入人为坏数据,可以导致在控制中心无法辨识坏数据的情况下状态估计结果失准(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。这些攻击不仅可能干扰电网的安全运行,也可为攻击者带来非正当的利益。文献[66]针对电力 CPS,基于博弈论研究了其在人为蓄意攻击威胁下的脆弱性评估方法。攻击者向电力系统注入错误的量测数据,影响电网的状态估计结果,从而导致电网错误的控制,造成电网的损失^[90]。文献[91]对一种针对电力系统的信息、物理协同攻击的情景进行了分析,并将其建模成一个双层混合整数规划问题,提出采用一种严格的两阶段求解方法以识别因攻击所造成的最大损失。此外,S. F. Bush^[29]研究了传输速率较高、数据帧较短的电力配电网通信业务的可靠性,给出了综合考虑配电网和通信网相互作用下的系统可靠性定量分析模型。文献[92]针对电力网与信息网的结构特点,提出了一种有助于改善电力信息-物理相互依存网络脆弱性的方法。

4 研究展望

在配电网 CPS 可靠性评估现有研究情况和关键技术发展现状的基础上,本文从配电网 CPS 异构数据处理、信息物理关联的建模与仿真、配电网 CPS 可靠性评估指标与方法、配电网 CPS 广义攻击与防御机制 4 个方面进行展望,并提出了相关科学问题和研究方法,以供探讨。

4.1 配电网 CPS 异构数据处理

随着电力数据规模、种类的快速增长,电力行业已迈入大数据时代,异构数据呈爆发式增长,在有限通信资源下保证可靠性分析任务高效进行,首先需要对异构数据进行处理。在高度信息化、市场化的作用下,配电网实时运行信息将逐步、有限地对外开放。随着数据规模、互动频率的提高,能源网络、配电网、社交网络的广泛联合,信息环境愈加复杂,电网可靠性分析需要了解其他能源网络的信息,数据也不仅限于电网智能设备采集。不同结构、不同运行机制的信息系统,各系统相互独立,应用平台和数据库结构存在差异,而且存在大量的重复数据,数据量大、实时性强、采集周期短(有毫秒、秒、分钟级)。未来能源系统与配电网将演变为互动、随机、时变物理网与开放、多源异构信息网并存的复杂系统。在有限

计算、通信资源约束下高效地完成可靠性分析任务,需要为评估人员上传可靠性计算必要的的数据,剔除冗余数据。但是,信息系统与物理系统中异构数据分析、多源信息融合尚无系统的理论和方法。因此,信息系统与物理系统中如何进行海量多源异构数据分析、如何在不改变信息流的基础上降低运算复杂性都是可靠性研究的关键科学问题。可以借助大数据解析方法、模拟仿真以及智能解析算法等进行数据分析,利用“信息接地”概念和基于图论的通用化简方法,简化网络中的大量冗余支路或数据,化简后保证与原模型拥有同样的信息/能量流。对实际控制系统而言,大部分信息并未参与最终的控制决策,很多信息数据在汇集入信息母线后,甚至不会再出现在下一步的信息中,这种数据即为冗余数据,这部分信息的引入将极大地增加系统信息流的计算量,这些不上传的信息就被理解为“接地”。

电网发生故障时会使稳态监控数据、动态监控数据和实时暂态数据同时发生变化,包括遥信变位、保护动作信号、事件顺序记录信号以及事故总信号变化,电压、电流、功率、功角、谐波等的突发变化量。另外,台风、雷雨等气象因素对电网安全运行的影响越来越大。利用大数据技术对采集的稳态数据、故障录波数据、报警系统数据、气象数据进行关联分析,快速找到根源故障,并进行故障预测,可以快速恢复故障,提高电网运行可靠性。

4.2 信息物理关联的建模与仿真

未来的能源系统是一个信息网络与物理系统高度融合的复杂系统,信息物理融合是当前学术界关注的前沿方向^[93]。目前国内外研究大多还是将信息与物理系统分开处理,从信息物理的整体视角进行建模与分析的研究较少。与以信息交换为目标的信息网不同,配电网信息系统中,不同信息对物理电网造成的影响有着显著差异。因此单纯通过信息可达性或概率模型分析系统的信息安全,无法全面反映电网信息物理耦合的特性。不同于连锁故障在电力系统的传播,信息物理融合环境下,风险在电力和信息节点间交互传递^[94],一个极小的扰动就可能产生“蝴蝶效应”,引发全局性灾难,因此未来电网运行控制和可靠性分析迫切需要准确的模型支撑。受乌克兰停电事故的启发,在关联建模中有必要研究配电网 CPS 的风险传递。针对信息系统的网络攻击会影响终端设备执行监测功能的能力,进而影响电力空间设备的正常运行。这正是电力 CPS 中信息物理安全风险的基本传播形式。网络安全风险在信息空间的传递以及跨空间传递到电力空间都具有一定的概率,风险可能不会在第一时间传递到电力空间,对电网可靠性的影响也并不明显。可靠性仿真所需资源

多、流程复杂,需要信息流和能量流的实时建模,在建模中确定风险传递概率是关键。此外,配电网 CPS 运行过程中存在着能够影响可靠性的多种不确定性因素,如信息的时延、丢失、畸变与设备的误动、故障等,并且这些因素间还存在着复杂的关联性,如何挖掘配电网信息物理耦合下多种影响因素间的关联性(包括信息终端与物理设备的电气连接关系、信息决策与物理执行单元的关联关系),如何分析电力与信息风险传递机制,都是配电网 CPS 综合建模需要考虑的问题,建立准确的配电网 CPS 模型是可靠性评估的关键环节。在众多的关联告警中,如何根据关联逻辑及网络拓扑关系,找出根源触发故障非常重要,从而实现准确快速的故障定位,加快故障应对处理速度,提高系统可靠性。

为了建立更加准确的配电网 CPS 模型,可以基于相依存网络理论以及传统的网络分析方法,构建矩阵形式的结构、功能、依存关系以及统一时序映射的动态配电网 CPS 相依存架构,继而实现配电网 CPS “结构-态势”分析。其中,配电网 CPS 结构包括配电系统网架结构、信息拓扑以及两者耦合网络,配电网 CPS 态势主要指配电网 CPS 内元件、链路、子系统等不同对象的状态描述。可以利用二元复合网络、相互依存复杂网络^[92]等方法研究风险传递问题。文献[95]在风险元传递理论的基础上,分析信息风险传递到物理网络的概率,提供了一种确定风险传递概率的思路。贝叶斯网络、图论、关联关系矩阵分析等方法都可以用于信息物理综合建模,形成从物理系统到信息系统再作用于物理系统的完整信息-物理融合网络模型。

4.3 配电网 CPS 可靠性评估指标与方法

随着智能电网建设的开展,调度相关系统越来越多,积累的数据也越来越多,使得原有的各大系统关联性越来越强。现阶段,用于配电网 CPS 可靠性分析的指标大多只反映了一次系统的运行状态,而没有突出其信息系统的特点。现有的分析方法往往采用经验方法给定系统的参数,是不精确的。SCADA 系统采集了电网运行的稳态数据,WAMS 采集了电网运行的动态数据,利用大数据技术对这些数据进行综合分析,可确定系统动态模型,为可靠性评估打下基础。在配电网 CPS 环境下,需要研究信息与物理系统交互影响下的系统可靠性指标,为实时掌握和评估配电网 CPS 在多因素交织的复杂运行环境下的可靠性提供行之有效的方法。前文提到的可靠性评估方法也是凭借传统指标提出的,可能不适用于新的指标计算,需要设计相应的信息物理一体化混合式评估方法,其中多时间尺度的处理和关联矩阵的建立是主要难题。从可靠性评估方法来看,一种方式是

将模拟法的采样技术逐步深入加上时间尺度的概念;另一种是解析法中将 2 个建模结合处理,本质上是信息物理耦合下时间尺度如何融合和异构数据如何混合的方法,可以考虑采用改进序贯蒙特卡洛法进行可靠性分析。此外,由于配电网 CPS 等效模型复杂程度大,蒙特卡洛法计算时间较长,可以利用集中采样与分散采样结合、网络矩阵的稀疏特性进行算法上的改进以提高效率。而且,还可以考虑从其他角度出发分析可靠性。如何建立信息与物理系统交互影响下的系统可靠性指标、如何设计信息物理一体化混合式评估方法、如何提出高效的可靠性评估算法、如何从其他角度分析可靠性等都是可靠性评估的关键科学问题。考虑从其他角度分析系统的可靠性,如第 3 节中可靠性评估方法主要涉及分析从系统侧观察到的停电情况,不管用户在停电事件期间是否需要用电,因此,该方法不能真正反映停电对用户可靠性水平的实际影响。可以从用户感知角度出发,提出一种可靠性评估方法,反映用户感受到的停电影响。

4.4 配电网 CPS 广义攻击与防御机制

随着目前对信息安全问题的关注,电力系统的网络攻击与信息安全也成为了一个非常热门的课题。电力系统网络安全防御需考虑应对概率较高的普通恶意软件攻击和危害较大的针对性定向攻击 2 类,前者危害机理清晰,可用较成熟的可靠性理论和信息安全理论与方法进行分析与应对;后者极少发生甚至无先例可循,需深入研究进而针对性地制定应对措施。配电网 CPS 不仅会受到信息系统的网络攻击,还可能面临物理系统的突发性用电行为。EV 大规模注入,突破系统容纳极限,这种时序空间差异和非人为突发性的影响系统正常运行的行为,也可以被称作攻击。因此提出了“广义攻击”的概念。一方面需要丰富网络攻击层面的研究,另一方面需要研究物理层面的突发性功率注入攻击,从而最终形成相应的广义攻击理论及其防御机制。如何考虑更多网络攻击形式对系统可靠性的影响、如何加强电网信息安全、如何提高电网对广义攻击的防御水平是值得研究的问题。实际上,配电网 CPS 结构复杂,可能的攻击来源和攻击模式繁多,需要多角度分析潜在网络攻击渠道和可能的破坏模式,尽可能避免恶性事故。攻击者可能根据安全漏洞受攻击后对物理系统的影响或安全漏洞的攻击难度,选择攻击目标。其中,以最大化破坏效果为目标的定向攻击防御是电力系统网络安全研究的重中之重。针对广义攻击下安全防御体系构建的问题,可以从不同种攻击注入、攻击的成功率等方面研究安全措施;可以采用博弈论、细胞自动机、贝叶斯网络等方法分析

攻击影响;考虑更多的攻击目标,如家用电器和智能表计等;采取更多的应对措施,如家庭设备权限验证、数据包贴安全标签等。另外,可能会影响配电网 CPS 可靠性的其他因素(如负荷管理控制设备)应该用于网络攻击场景建模。

5 结语

配电网已经从传统的电力设备网络发展成为融合通信网络、信息网络和电力设备网络的复杂综合网络体系。乌克兰停电事故使信息安全问题被广泛关注,智能配电网信息系统对物理系统的影响不可忽视,研究配电网 CPS 可靠性评估方法具有重要的理论价值与现实意义。本文从信息系统、物理系统的不同视角分析了配电网可靠性的影响因素,总结了配电网信息、物理方面的可靠性评估指标,发现现有的可靠性指标通常忽略了信息系统的影响,很少有能直接用于评估配电网 CPS 的综合指标;较为系统地总结了配电网 CPS 的可靠性评估方法,指出了现有研究在融合建模方面存在的问题,较为全面地对配电网 CPS 可靠性评估关键技术进行了概括。在未来研究中,需要对信息物理作用进行更全面的考虑,并且计及物理信息作用以实现配电网 CPS 可靠性的协同分析与评估。在此基础上,从配电网 CPS 异构数据处理、信息物理关联的建模与仿真、配电网 CPS 可靠性评估指标与方法、配电网 CPS 广义攻击与防御机制 4 个方面进行展望,为今后配电网 CPS 的可靠性研究提供了研究思路。配电网 CPS 可靠性研究的突破将促进能源互联网、智能配电网的应用与发展。

参考文献:

- [1] 刘振亚. 全球能源互联网[M]. 北京:中国电力出版社,2015:285-290.
- [2] 耿永彬,邢亮,唐国强. “互联网+”时代企业网络安全的思考[J]. 通讯世界,2017(1):58-59.
GENG Yongbin,XING Liang,TANG Guoqiang. Security thinking of enterprise network for “Internet+”[J]. Communications World, 2017(1):58-59.
- [3] 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,2016:255-257.
- [4] 叶夏明,文福拴,尚金成,等. 电力系统中信息物理安全风险传播机制[J]. 电网技术,2015,39(11):3072-3079.
YE Xiaming,WEN Fushuan,SHANG Jincheng,et al. Propagation mechanism of cyber physical security risks in power systems[J]. Power System Technology, 2015,39(11):3072-3079.
- [5] RIFKIN J. The third industrial revolution:how lateral power is transforming energy,the economy,and the world[M]. New York, USA:Palgrave MacMillan,2011:28-34.
- [6] 董朝阳,赵俊华,文福拴,等. 从智能电网到能源互联网:基本概念与研究框架[J]. 电力系统自动化,2014,38(15):1-11.
DONG Zhaoyang,ZHAO Junhua,WEN Fushuan,et al. From smart grid to energy internet:basic concept and research framework [J]. Automation of Electric Power Systems,2014,38(15):1-11.
- [7] 马钊,周孝信,尚宇炜,等. 未来配电系统形态及发展趋势[J]. 中国电机工程学报,2015,35(6):1289-1298.
MA Zhao,ZHOU Xiaoxin,SHANG Yuwei,et al. Form and development trend of future distribution system[J]. Proceedings of the CSEE,2015,35(6):1289-1298.
- [8] BILLINTON R,WANG P. Reliability-network-equivalent approach to distribution-system-reliability evaluation[J]. IEEE Proceedings-Generation,Transmission and Distribution,1998,145(2):149-153.
- [9] SHIRTO O,HYVARINEN M,LOUKKALAHTI M,et al. Improving reliability in an urban network[J]. Electric Power Systems Research,2015,120:47-55.
- [10] BROWN R E. Electric power distribution reliability[M]. 2nd ed. Duval,Florida,USA:CRC Press,2009:32-40.
- [11] 赵俊华,文福拴,薛禹胜,等. 电力 CPS 的架构及其实现技术与挑战[J]. 电力系统自动化,2010,34(16):1-7.
ZHAO Junhua,WEN Fushuan,XUE Yuesheng,et al. Cyber physical power systems:architecture,implementation techniques and challenges[J]. Automation of Electric Power Systems,2010,34(16):1-7.
- [12] 刘东,盛万兴,王云,等. 电网信息物理系统的关键技术及其进展[J]. 中国电机工程学报,2015,35(14):3522-3531.
LIU Dong,SHENG Wanxing,WANG Yun,et al. Key technologies and trends of cyber physical system for power grid[J]. Proceedings of the CSEE,2015,35(14):3522-3531.
- [13] 王云,刘东,陆一鸣. 电网信息物理系统的混合系统建模方法研究[J]. 中国电机工程学报,2016,36(6):1464-1470.
WANG Yun,LIU Dong,LU Yiming. Research on hybrid system modeling method of cyber physical system for power grid[J]. Proceedings of the CSEE,2016,36(6):1464-1470.
- [14] 赵俊华,文福拴,薛禹胜,等. 电力信息物理融合系统的建模分析与控制研究框架[J]. 电力系统自动化,2011,35(16):1-8.
ZHAO Junhua,WEN Fushuan,XUE Yusheng,et al. Modeling analysis and control research framework of cyber physical power systems[J]. Automation of Electric Power Systems,2011,35(16):1-8.
- [15] 王宇飞,高昆仑,赵婷,等. 基于改进攻击图的电力信息物理系统跨空间连锁故障危害评估[J]. 中国电机工程学报,2016,36(6):1490-1499.
WANG Yufei,GAO Kunlun,ZHAO Ting,et al. Assessing the harmfulness of cascading failures across space in electric cyber-physical system based on improved attack graph[J]. Proceedings of the CSEE,2016,36(6):1490-1499.
- [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.
TANG Yi,CHEN Qian,LI Mengya,et al. Overview on cyber-attacks against cyber physical power system[J]. Automation of Electric Power Systems,2016,40(17):59-69.
- [17] YU X,SINGH C. Power system reliability analysis considering protection failures [C]//Power Engineering Society Summer Meeting. Chicago,IL,USA:IEEE,2002:963-968.
- [18] ERICSSON G N. Management of information security for an electric power utility-on security domains and use of ISO/IEC17799 standard[J]. IEEE Transactions on Power Delivery, 2005,20(2):683-690.

- [19] STILLMAN R H,DARVENIZA M. Risk evaluation-power system induced bush and grass fires and the catastrophe potential[J]. IEEE Transactions on Reliability,1991,40(3):309-315.
- [20] FALAHATI B,FU Y,WU L. Reliability assessment of smart grid considering direct cyber-power interdependencies[J]. IEEE Transactions on Smart Grid,2013,3(3):1515-1524.
- [21] FALAHATI B,FU Y. Reliability assessment of smart grids considering indirect cyber-power interdependencies[J]. IEEE Transactions on Smart Grid,2014,5(4):1677-1685.
- [22] SCHNEIDER K,LIU C C,PAUL J P. Assessment of interactions between power and telecommunications infrastructures[J]. IEEE Transactions on Power Systems,2006,21(3):1123-1130.
- [23] 张梅,李晏. 涉密信息系统安全评估指标体系研究[C]//中国系统工程学会决策科学专业委员会学术年会. 北京,中国:中国系统工程学会,2009:195-198.
ZHANG Mei,LI Yan. Research on security assessment index of secret information system[C]//China Academic Journal Electronic Publish House. Beijing,China:Systems Engineering Society of China,2009:195-198.
- [24] 周静,孙媛媛. 未来电力能源系统数据分析面临的需求与挑战[J]. 电力信息与通信技术,2016,14(4):39-45.
ZHOU Jing,SUN Yuanyuan. Data analysis requirements and challenges in the future power energy domain[J]. Electric Power Information and Communication Technology,2016,14(4):39-45.
- [25] TANG F,ZHA X. Reliability analysis of smart distribution grid communication system based on EPON[C]//Asia-Pacific Power and Energy Engineering Conference (APPEEC). [S.l.]:IEEE,2012:1-4.
- [26] MAIER M,LECESQUE M. Dependable Fiber-Wireless (FiWi) access networks and their role in a sustainable third industrial revolution economy[J]. IEEE Transactions on Reliability,2014,63(2):386-400.
- [27] TSUBOKAWA M. Reliability evaluation for distributed pons with ring and tree topologies[J]. IEEE/OSA Journal of Optical Communications and Networking,2012,4(10):790-798.
- [28] KIM J,KIM D,LIM K W,et al. Improving the reliability of IEEE 802.11s based wireless mesh networks for smart grid systems[J]. Journal of Communications and Networks,2012,14(6):629-639.
- [29] BUSH S F. Network theory and smart grid distribution automation[J]. IEEE Journal Selected Areas in Communications,2014,32(7):1451-1459.
- [30] 高会生. 电力通信接入网可靠性影响因素分析[J]. 电力信息与通信技术,2014,12(11):1-7.
GAO Huisheng. Reliability analysis of power communication access network[J]. Electric Power Information and Communication Technology,2014,12(11):1-7.
- [31] 李文武,游文霞,王先培. 电力系统信息安全研究综述[J]. 电力系统保护与控制,2011,39(10):140-147.
LI Wenwu,YOU Wenxia,WANG Xianpei. Research on information security of power system[J]. Power System Protection and Control,2011,39(10):140-147.
- [32] Power Systems Engineering Research Center. Reliability assessment and modeling of cyber enabled power systems with renewable sources and energy storage[R]. College Station,TX, USA:Texas A&M University,2016.
- [33] 李田,苏盛,杨洪明,等. 电力信息物理系统网络安全防护中的底线思维[J]. 电力系统自动化,2017,41(22):1-6.
LI Tian,SU Sheng,YANG Hongming,et al. Bottom line in cyber security defense of cyber physical power system [J]. Automation of Electric Power Systems,2017,41(22):1-6.
- [34] 曾军. 影响配电网供电可靠性的因素及提高供电可靠性的措施分析[J]. 通讯世界,2016(19):225-226.
ZENG Jun. Reliability factors of distribution network power supply and measures to improve reliability of power system[J]. Power Message,2016(19):225-226.
- [35] 吴志山. 计及分布式电源和电动汽车的配电网供电可靠性评估[D]. 广州:广东工业大学,2016.
WU Zhishan. Reliability assessment of distribution network considering the distributed power supply and electric vehicle [D]. Guangzhou:Guangdong University of Technology,2016.
- [36] 刘永奇,谢开. 从调度角度分析 8·14 美加大停电[J]. 电网技术,2004,28(8):10-15.
LIU Yongqi,XIE Kai. Analysis on blackout of interconnected North America power grid occurred on Aug.14,2003 from the viewpoint of power system dispatching[J]. Power System Technology,2004,28(8):10-15.
- [37] 郭庆来,辛蜀骏,王剑辉,等. 由乌克兰停电事件看信息能源系统综合安全评估[J]. 电力系统自动化,2016,40(5):145-147.
GUO Qinglai,XIN Shujun,WANG Jianhui,et al. Comprehensive security assessment for a cyber physical energy system:a lesson from Ukraine's blackout[J]. Automation of Electric Power Systems,2016,40(5):145-147.
- [38] LI Wenwu,YOU Wenxia,WANG Xianpei. Survey of cyber security research in power system[J]. Power System Protection and Control,2011,39(10):140-147.
- [39] RINALDI S M,PEERENBOOM J P,KELLY T K. Identifying, understanding,and analyzing critical infrastructure interdependencies[J]. IEEE Control Systems,2002,21(6):11-25.
- [40] FALAHATI B,FU Y. A study on interdependencies of cyber-power networks in smart grid applications[C]//2012 IEEE PES Innovative Smart Grid Technologies (ISGT). Washington DC, USA:IEEE,2012:1-8.
- [41] LEI H,SINGH C,SPRINTSON A. Reliability modeling and analysis of IEC61850 based substation protection systems[J]. IEEE Transactions on Smart Grid,2014,5(5):2194-2202.
- [42] 万国成,任震,吴日昇,等. 混合法在复杂配电网可靠性评估中的应用[J]. 中国电机工程学报,2004,24(9):92-98.
WAN Guocheng,REN Zhen,WU Risheng,et al. Hybrid method for the reliability evaluation of the complex distribution system [J]. Proceedings of the CSEE,2004,24(9):92-98.
- [43] 张鹏,王守相. 大规模配电系统可靠性评估的区间算法[J]. 中国电机工程学报,2004,24(3):77-84.
ZHANG Peng,WANG Shouxiang. A novel interval method for reliability evaluation of large scale distribution system[J]. Proceedings of the CSEE,2004,24(3):77-84.
- [44] 丁明,张静,李生虎. 基于序贯蒙特卡罗仿真的配电网可靠性评估模型[J]. 电网技术,2004,28(3):38-42.
DING Ming,ZHANG Jing,LI Shenghu. A sequential Montecarlo simulation based reliability evaluation model for distribution network[J]. Power System Technology,2004,28(3):38-42.
- [45] IEEE Power and Energy Society. IEEE guide for electric power distribution reliability indices:IEEE standard 1366-2003[S/OL]. [2017-05-04]. <http://www.ieee.org>.

- [46] 宋云亭,张东霞,吴俊玲,等. 国内外城市配电网供电可靠性对比分析[J]. 电网技术,2008,32(23):13-18.
SONG Yunting,ZHANG Dongxia,WU Junling,et al. Comparison and analysis on power supply reliability of urban power distribution network at home and abroad[J]. Power System Technology,2008,32(23):13-18.
- [47] National Institute for Standards and Technology(NIST). Guidelines for smart grid cyber security[C]//Privacy and the Smart Grid. [S.l.]:NISTIR,2010:1-6.
- [48] 曾旭杰. 信息系统运行可靠性及其关键技术研究[D]. 重庆:重庆大学,2009.
ZENG Xujie. Research on reliability and key technology of information system operation[D]. Chongqing:Chongqing University,2009.
- [49] 吴亚非. 信息安全风险评估[M]. 北京:清华大学出版社,2007:90-98.
- [50] 范红. 信息安全风险评估规范国家标准理解与实施[M]. 北京:中国标准出版社,2008:20-27.
- [51] MAHLOO M,CHEN J,WOSINSKA L,et al. Toward reliable hybrid WDM/TDM passive optical networks[J]. IEEE Communications Magazine,2014,52(2):14-23.
- [52] LIU R,VELLAITHURAI C,BISWAS S S,et al. Analyzing the cyber physical impact of cyber events on the power grid[J]. IEEE Transactions on Smart Grid,2015,6(5):2444-2453.
- [53] SRIVASTAVA A,MORRIS T,EENSTER 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.
- [54] 俞斌,郭创新,王越,等. 考虑信息系统作用的电力系统可靠性研究[J]. 电力系统保护与控制,2013,41(7):7-13.
YU Bin,GUO Chuangxin,WANG Yue,et al. Research on the reliability of the power system considering impacts of the information system[J]. Power System Protection and Control,2013,41(7):7-13.
- [55] 郭嘉,韩宇奇,郭创新,等. 考虑监视与控制功能的电网信息物理系统可靠性评估[J]. 中国电机工程学报,2016,36(8):2123-2130.
GUO Jia,HAN Yuqi,GUO Chuangxin,et al. Reliability assessment of cyber physical power system considering monitoring function and control function[J]. Proceedings of the CSEE,2016,36(8):2123-2130.
- [56] ANDREW C,SAMAN Z. Cyber-physical resilience:definition and assessment metric[C]//IEEE PES Transactions on Smart Grid. Chicago,USA:IEEE,2017:1-3.
- [57] 邱生敏. 配电网可靠性评估方法研究[D]. 广州:华南理工大学,2012.
QIU Shengmin. Studies on distribution network reliability evaluation method[D]. Guangzhou:South China University of Technology,2012.
- [58] BESSANI M,FANUCCHI R Z,DELBEMA C C,et al. Impact of operators' performance in the reliability of cyber-physical power distribution systems[J]. IET Generation Transmission & Distribution,2016,10(11):2640-2646.
- [59] 陈鹏伟,陶顺,肖湘宁,等. 主动配电网可靠性评估源荷模型改进及并行处理[J]. 电力系统自动化,2016,40(18):68-75.
CHEN Pengwei,TAO Shun,XIAO Xiangning,et al. Source-load model improvement and parallel computing for reliability evaluation of active distributed networks[J]. Automation of Electric Power Systems,2016,40(18):68-75.
- [60] 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.
GUO Qinglai,XIN Shujun,SUN Hongbin,et al. Power system cyber-physical modelling and security assessment:motivation and ideas[J]. Proceedings of the CSEE,2016,36(6):1481-1489.
- [61] SINGH C,SPRINTSON A. Reliability assurance of cyber physical power systems[C]//Power and Energy Society General Meeting. Minneapolis,USA:IEEE,2010:1-6.
- [62] 赵渊,袁蓉,芦晶晶. 配电网可靠性概率分布的解析模型和非参数估计[J]. 电力系统自动化,2014,38(1):38-43.
ZHAO Yuan,YUAN Rong,LU Jingjing. Analytical approach and non-parametric kernel estimation to compute probability distributions for reliability indices of distribution systems[J]. Automation of Electric Power Systems,2014,38(1):38-43.
- [63] 高贺,孙莹,李可军,等. 一种新型智能配电网风险评估模型[J]. 电力自动化设备,2016,36(6):142-147.
GAO He,SUN Ying,LI Kejun,et al. Risk assessment model of smart distribution grid[J]. Electric Power Automation Equipment,2016,36(6):142-147.
- [64] 彭寒梅,曹一家,黄小庆. 对等控制孤岛微电网的静态安全风险评估[J]. 中国电机工程学报,2016,36(18):4837-4846.
PENG Hanmei,CAO Yijia,HUANG Xiaoqing. Static security risk assessment of islanded microgrids under peer-peer control[J]. Proceedings of the CSEE,2016,36(18):4837-4846.
- [65] 魏震波,刘俊勇,朱国俊,等. 基于电网状态与结构的综合脆弱评估模型[J]. 电力系统自动化,2009,33(8):11-14.
WEI Zhenbo,LIU Junyong,ZHU Guojun,et al. A new integrative vulnerability evaluation model to power grid based in running state and structure[J]. Automation of Electric Power Systems,2009,33(8):11-14.
- [66] 石立宝,简洲. 基于动态攻防博弈的电力信息物理融合系统脆弱性评估[J]. 电力系统自动化,2016,40(17):99-105.
SHI Libao,JIAN Zhou. Vulnerability assessment of cyberphysical power system based on dynamic attack-defense game model[J]. Automation of Electric Power Systems,2016,40(17):99-105.
- [67] CHERATH L,BENSON K F,CHADA K. Assessment of interactions between power and telecommunications infrastructures[J]. IEEE Transactions on Power Systems,2006,21(3):1123-1130.
- [68] WANG Yang,LI Wenyuan,LU Jiping. Reliability analysis of phasor measurement unit using hierarchical Markov modeling[J]. Electric Power Components & Systems,2009,37(5):517-532.
- [69] WANG Yang,LI Wenyuan,LU Jiping. Reliability analysis of wide-area measurement system[J]. IEEE Transactions on Power Delivery,2010,25(3):1483-1491.
- [70] WANG Yang,LI Wenyuan,ZHANG Peng,et al. Reliability analysis of phasor measurement unit considering data uncertainty[J]. IEEE Transactions on Power Systems,2012,27(3):1503-1510.
- [71] WANG Yang,LI Wenyuan,LU Jiping,et al. Evaluating multiple reliability indices of regional networks in wide area measurement system[J]. Electric Power Systems Research,2009,79(10):1353-1359.
- [72] BOU-HARB E,FACHKHA C,POURZANDI M,et al. Communication security for smart grid distribution networks[J]. IEEE

- Communications Magazine, 2013, 51(1):42-49.
- [73] HASHEMI-DEZAKI H, ASKARIAN-ABYANEH H, HAERI-KHIAVI H. Impacts of direct cyber-power interdependencies on smart grid reliability under various penetration levels of micro-turbine/wind/solar distributed generations[J]. IET Generation, Transmission & Distribution, 2016, 10(4):928-937.
- [74] XIANG Y, WANG L, ZHANG Y. Power system adequacy assessment with probabilistic cyber attacks against breakers[C]// PES General Meeting. National Harbor, USA:IEEE, 2014:1-6.
- [75] RAZI-KAZEMI A A, VAKILIAN M, NIAYESH K, et al. Circuit-breaker automated failure tracking based on coil current signature[J]. IEEE Transactions on Power Delivery, 2014, 29(1):283-290.
- [76] MALABANAN D R, NERVES A C. Power transformer condition assessment using an immune neural network approach to dissolved gas analysis[C]// 2014 IEEE Region 10 Conference TENCN. Bangkok, Thailand; IEEE, 2014:1-6.
- [77] SRIDHAR S, HAHN A, GOVINDARASU M. Cyber-physical system security for the electric power grid [J]. Proceedings of the IEEE, 2012, 100(1):210-224.
- [78] 付聪, 安灵旭, 方华亮, 等. 继电保护系统对一次设备可靠性的影响研究[J]. 电力系统保护与控制, 2013, 41(11):38-44.
FU Cong, AN Lingxu, FANG Hualiang, et al. Study on the influence of protection system on reliability of primary equipment[J]. Power System Protection and Control, 2013, 41(11):38-44.
- [79] SINGH C, PATTON A D. Protection system reliability modeling: unreadiness probability and mean duration of undetected faults [J]. IEEE Transactions on Reliability, 1980, 29(4):339-340.
- [80] 邱剑, 王慧芳, 陈志光, 等. 智能变电站自动化系统有效度评估模型研究[J]. 电力系统自动化, 2013, 37(9):1-8.
QIU Jian, WANG Huifang, CHEN Zhiguang, et al. Research on effectiveness evaluation model of smart substation automation system[J]. Automation of Electric Power Systems, 2013, 37(9):1-8.
- [81] HAJIAN-HOSEINABADI H. Impacts of automated control systems on substation reliability[J]. IEEE Transactions on Power Delivery, 2011, 26(3):1681-1691.
- [82] VELLATHURAI C, SRIVASTAVA A, ZONOUS S, et al. CPIndex: cyber-physical vulnerability assessment for power grid infrastructures[J]. IEEE Transactions on Smart Grid, 2017, 6(2):566-575.
- [83] ZHANG Y, WANG L, XIANG Y, et al. Power system reliability evaluation with SCADA cyber security considerations[J]. IEEE Transactions on Smart Grid, 2015, 6(4):1707-1721.
- [84] SUN X. Cyber-physical modeling and cyber-contingency assessment of hierarchical control systems[J]. IEEE Transactions on Smart Grid, 2015, 6(5):2375-2385.
- [85] 严佳梅, 许剑冰, 倪明, 等. 通信系统中断对电网广域保护控制系统的影响[J]. 电力系统自动化, 2016, 40(5):17-25.
YAN Jiamei, XU Jianbing, NI Ming, et al. Impact of communication system interruption on power system wide area protection and control system[J]. Automation of Electric Power Systems, 2016, 40(5):17-25.
- [86] AMINIFAR F, FOTUHI-FIRUZABAD M, SHAHIDEHPOUR M, et al. Impact of WAMS malfunction on power system reliability assessment[J]. IEEE Transactions on Smart Grid, 2012, 3(3):1302-1309.
- [87] 黄潇文, 刘俊勇, 魏震波, 等. WAMS 故障对电力系统可靠性的影响分析[J]. 现代电力, 2014, 31(4):29-33.
HUANG Xiaowen, LIU Junyong, WEI Zhenbo, et al. Impact analysis of WAMS faults on power system reliability[J]. Modern Electric Power, 2014, 31(4):29-33.
- [88] 张天宇, 罗凤章, 王成山, 等. 信息系统对微电网运行可靠性的影响分析[J]. 电力系统自动化, 2016, 40(23):28-35.
ZHANG Tianyu, LUO Fengzhang, WANG Chengshan, et al. Analysis of the impact of information system on microgrid operation reliability[J]. Automation of Electric Power Systems, 2016, 40(23):28-35.
- [89] 杜双育, 王先培, 谢光彬, 等. 基于 IEC61850 的变电站自动化系统可靠性评估[J]. 电力系统保护与控制, 2012, 40(5):32-36, 41.
DU Shuangyu, WANG Xianpei, XIE Guangbin, et al. Reliability evaluation of substation automation system based on IEC61850[J]. Power System Protection and Control, 2012, 40(5):32-36, 41.
- [90] FARRAJ A, HAMMAD E, DAOUD A A, et al. A game-theoretic analysis of cyber switching attacks and mitigation in smart grid systems[J]. IEEE Transactions on Smart Grid, 2015, 7(4):1846-1855.
- [91] LI Z, SHAHIDEHPOUR M, ALABDULWAHAB A, et al. Bilevel model for analyzing coordinated cyber-physical attacks on power systems[J]. IEEE Transactions on Smart Grid, 2016, 7(5):2260-2272.
- [92] 冀星沛, 王波, 董朝阳, 等. 电力信息-物理相互依存网络脆弱性评估及加边保护策略[J]. 电网技术, 2016, 40(6):1867-1873.
JI Xingpei, WANG Bo, DONG Zhaoyang, et al. Vulnerability evaluation and link addition protection strategy research of electrical cyber-physical interdependent networks[J]. Power System Technology, 2016, 40(6):1867-1873.
- [93] 马钊, 安婷, 尚宇炜. 国内外配电网前沿技术动态及发展[J]. 中国电机工程学报, 2016, 36(6):1552-1567.
MA Zhao, AN Ting, SHANG Yuwei. State of the art and development trends of power distribution technologies[J]. Proceedings of the CSEE, 2016, 36(6):1552-1567.
- [94] 李存斌, 李小鹏, 田世明, 等. 能源互联网电力信息深度融合风险传递: 挑战与展望[J]. 电力系统自动化, 2017, 41(11):17-25.
LI Cunbin, LI Xiaopeng, TIAN Shiming, et al. Challenges and prospects of risk transmission in deep fusion of electric power and information for energy internet[J]. Automation of Electric Power Systems, 2017, 41(11):17-25.
- [95] 李存斌. 智能电网运营风险元传递理论与应用[M]. 北京: 中国电力出版社, 2016:145-152.

作者简介:



蒋卓臻

蒋卓臻(1994—),女,重庆人,硕士研究生,主要研究方向为配电网可靠性分析(E-mail: 563988776@qq.com);

刘俊勇(1963—),男,四川成都人,教授,博士研究生导师,博士,主要研究方向为电力市场、电力系统稳定与控制、分布式发电及智能电网(E-mail: liujy@scu.edu.cn);

向月(1987—),男,重庆人,副研究员,博士,通信作者,主要研究方向为电力系统规划与优化运行(E-mail: xiang@scu.edu.cn)。

Key technologies for reliability assessment of distribution network cyber physical system

JIANG Zhuozhen, LIU Junyong, XIANG Yue

(School of Electrical Engineering and Information, Sichuan University, Chengdu 610065, China)

Abstract: The high integration of physical and cyber system is the development tendency of smart distribution network in the future, so the key technologies of reliability assessment for distribution network CPS (Cyber Physical System) are summarized and prospected. Starting with the excavation of physical and cyber system's risk origins in distribution network, the influence factors are analyzed further, based on which, classification methods and specific mathematical expressions of reliability assessment index for physical and cyber system of distribution network and establish technologies of reliability assessment index for CPS are summarized and then the research progress of reliability assessment algorithms and methods is discussed. Four aspects are prospected for distribution network CPS: heterogeneous data processing, modeling and simulation, reliability assessment index and method, generalized attack and defense mechanisms.

Key words: cyber physical system; smart distribution network; generalized attack; reliability assessment; defense mechanism

(上接第 21 页 continued from page 21)

Performance optimization for low voltage power line communication

LIU Xiaosheng, CUI Ying, XU Dianguo

(School of Electrical Engineering and Automation, Harbin Institute of Technology, Harbin 150001, China)

Abstract: The low voltage PLC (Power Line Communication) media access control protocol is an important factor that affect the network performance. In order to improve the relatively low network performance caused by the asymmetric PLC channels, an improved adaptive p -persistent CSMA optimization method for improved artificial cobweb with limited load in low voltage PLC is proposed. The networking process of the media access control layer of three-phase distribution network being mapped into the improved artificial cobweb is described in detail. The proposed method is applied to optimize the throughput and average package delay of cobweb, i.e. dynamically adjust the access probability and control the grouping behavior during data transmission based on the amount of known active nodes participating in channel competition, which makes the channel in the best transmission status and ensures the network performance. The simulative results show that the proposed method is effective.

Key words: energy internet; low voltage power line communication; access control; network performance; improved p -persistent CSMA