考虑物理–信息虚拟连接的电力信息物理融合系统的脆弱性评估

陈柯任[1],文福拴[1],赵俊华[2],李　力[3],杨银国[3],谭　嫣[3]

(1. 浙江大学 电气工程学院,浙江 杭州 310027;2. 香港中文大学(深圳) 理工学院,广东 深圳 518100;
3. 广东电网有限责任公司电力调度控制中心,广东 广州 510600)

摘要:不断发展的自动化与信息技术的广泛应用明显提高了现代电力系统的运行水平,电力信息系统与电力物理系统的融合也逐步广泛和深入,从而进化为电力信息物理融合系统(CPPS)。在 CPPS 中,信息设备的故障会影响物理系统的安全可靠运行,而外部对物理与信息元件的攻击则可能导致停电事故。在此背景下,为了分析物理元件与信息元件的交互影响,将 CPPS 抽象模拟为物理节点、物理–物理连接、信息节点、信息–信息连接与信息–物理连接 5 类元素,并在此基础上评估信息系统受损对物理系统运行的影响。在博弈论的框架下构建了双层数学规划模型分别对物理与信息环节进行了防御资源分配,用于量化存在假想攻击下系统中各环节的重要程度。以修改的 IEEE 14 节点系统为例进行了仿真计算,结果验证了所提方法的可行性与有效性。

关键词:电力信息物理融合系统;脆弱性评估;信息–物理连接;最优切负荷;双层数学规划

中图分类号:TM 761　　**文献标识码**:A　　DOI:10.16081/j.issn.1006–6047.2017.12.009

0　引言

随着智能控制设备和通信网络逐渐融入传统电力系统,电力系统的安全可靠性水平得以提升,并逐渐发展成为由信息系统和物理系统构成的复合系统,即信息物理融合系统 CPS(Cyber-Physical System)基础上的电力信息物理融合系统 CPPS(Cyber-Physical Power System)[1-6]。

随着 CPPS 的发展,信息设备发生故障会对电力系统产生越来越明显的影响[7]。近年来,多个大停电事故的调查报告也证实了对信息网络的误操作以及信息网络本身的失效可能导致大停电事故[8]。因此,在 CPPS 中,和传统电力设备一样,对具备监视和控制功能的信息网络进行可靠性以及脆弱性评估同样重要。

CPPS 的可靠性与脆弱性分析是电力系统领域近年来关注的热点之一。文献[9]研究了微电网元件接入、运行和退出过程中各代理信息的交互作用,建立了基于 IEC61850 的多代理系统控制方法。文献[10-11]对信息系统进行了建模,并分析计算了信息系统的可靠性。文献[12]提出了基于邻接矩阵的电力信息系统脆弱性评估模型和定量分析方法。文献[13]综合考虑了输电线路发生故障的不确定性等因素对故障概率的影响,并提出了输电线路实时风险评估模型。文献[14]基于直流潮流模型建立了电力网络和通信网络交互作用模型,研究了不同参数选取对连锁故障的影响。文献[15-16]将信息–物理系统相互作用的形式分为 2 种:直接作用与间接作用,并分别针对信息网与电力网的直接与间接交互作用采用不同的算法进行安全评估。文献[17]描述了数据采集与监控(SCADA)系统在电力系统中的应用,分析了信息系统失效对电力系统的影响。文献[18]基于细胞自动机理论,构建了分析信息安全风险在 CPPS 中传播的数学模型。文献[19]研究了通信系统故障对电力系统广域保护控制系统的影响。文献[20]基于改进渗流理论,提出了考虑物理层电网潮流分析与信息层延时的 CPPS 的连锁故障模型。文献[21]考虑了电力系统信息层遭受攻击后的故障传播,针对攻击对象的脆弱度、攻击难易程度等进行了风险评估。文献[22]研究了电力系统中虚假数据注入攻击的原理、影响以及防御措施。文献[23]针对微电网提出了信息系统故障的量化分析方法,并对信息系统元件故障的影响因素进行了灵敏度分析。上述研究从不同角度研究了信息系统与物理系统的交互作用,但总体上尚比较初步,还没有形成系统的研究成果。

在上述背景下,针对 CPPS 中信息与物理系统的交互影响,本文首先将智能监控设备与通信网络节点统一抽象为信息节点。综合考虑了信息与物理节点间的相互影响,并将 CPPS 抽象建模为物理节点(P-node)、

收稿日期:2017–11–01;**修回日期**:2017–11–20
基金项目:国家高技术研究发展计划(863 计划)资助项目(2015AA050202);广东电网有限责任公司科技项目(GDKJQQ2015-3001)
Project supported by the National High Technology Research and Development Program of China(863 Program)(2015AA050202) and Science & Technology Program of Guangdong Power Grid Co.,Ltd.(GDKJQQ20153001)

物理–物理连接(PP-link)、信息节点(C-node)、信息–信息连接(CC-link)与信息–物理连接(CP-link)5类元素,用于评估信息系统受损对物理系统运行的影响。在此基础上,在博弈论的框架下构造了双层数学规划模型分别对物理与信息环节进行防御资源分配,以量化分析存在假想攻击下系统中各环节的重要程度,为实际设备防护提供辅助决策支持。最后,以修改的IEEE 14节点系统为例对所提出的方法进行了说明。

1 CPPS中的节点与连接模型

为了同时考虑CPPS中物理环节与信息环节的状况及两者间的交互影响,本文提出节点–连接模型,如图1所示。该模型由5个部分组成:物理节点、信息节点、物理–物理连接、信息–信息连接和物理–信息连接。

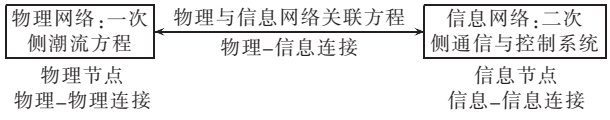


图1 CPPS节点–连接模型

Fig.1 Node-link model of CPPS

a. 物理节点。

每个物理节点表示一台发电机或一个负荷。若一个物理节点失效,则其对应的发电机无法调整出力或对应的负荷无法执行削减负荷操作。

b. 信息节点。

每个物理设备(如发电机和负荷)一般都配备了与之相连的信息元件,以实现信息采集与控制等功能。尽管信息元件的类型较多且分布复杂,但可将其整合为信息节点,并认为所有相关功能都在该节点实现[24]。同时,可认为信息节点的分布与物理节点的分布相同,即每个物理节点都对应一个信息节点。在本文中,将信息节点分为信息中心与终端2类,且一个系统中只存在一个信息中心。

如果一个信息节点失效,那么该信息节点无法与相邻信息节点通信,导致所有与之相连的信息–信息连接都失效。同时,由于该失效信息节点直接承担着控制对应物理节点的任务,因此其对应的物理节点也失效。

c. 物理–物理连接。

物理–物理连接沿用了传统电力系统分析中的概念,即输电线的简化,实现联络各物理节点的功能。

若一条物理–物理连接失效,则无法通过该物理连接输送功率,需要对整个系统重新计算潮流分布。若存在潮流越限情况,需要考虑调整发电机出力、削减负荷甚至停运过载支路等。

d. 信息–信息连接。

信息设备之间需要通信,包括诸如光纤等有线通信方式和无线通信方式,统称为信息–信息连接。

每个信息节点与信息中心的连接状态取决于相关信息–信息连接的状态。若某个信息节点被孤立(无法与信息中心通信),则可认为其失效。

e. 物理–信息连接。

前已述及,可以将每个物理节点配备的所有信息元件简化为一个信息节点。信息元件与物理设备之间存在着信息采集与控制等方面的联系,属于虚拟关联,本文称之为物理–信息连接。物理设备为本地信息设备供电;信息设备则用于采集物理设备的发电机出力和负荷等数据,以及控制发电机出力和负荷。

由于物理节点与信息节点之间存在上述关联,当物理节点完全失去供电(如与负荷节点相连的所有输电线路都停运)时,对应的信息节点也失去供电而停止工作;当信息节点失去与信息中心的连接(即无法与信息中心通信)时,信息中心失去对物理节点的控制功能,这样相关物理节点就无法调整发电机出力或削减负荷。

上述5个环节构成了本文所提出的节点–连接模型。

2 CPPS的脆弱性评估

2.1 外部攻击与连锁故障

近年来,国内外针对电力系统的蓄意攻击时有发生。攻击者为了最大化对电力系统造成的破坏,往往选择系统中最为薄弱的一些环节展开攻击。在CPPS中,信息环节与物理环节遭受攻击都会影响整个电力系统的安全稳定运行。本文假设攻击者的目标为中断对有功负荷的供电,并着重考虑对物理与信息层面同时展开攻击的场景。

例如,假设攻击者选取某条物理–物理连接进行攻击,导致相关支路停运,从而系统潮流分布发生变化,并有可能存在某些支路潮流越限。在攻击成功后,攻击者再选取2个信息节点进行攻击,并导致这2个信息节点受到破坏,相应的物理节点无法调整发电机出力和负荷需求。

前已述及,物理元件与信息元件受损可能会互相产生影响,从而扩大波及范围。具体表现如下。

a. 信息–信息连接失效。此时,需要重新验证信息节点是否能与通信中心联络,若不能则认为该信息节点失效。

b. 信息–物理连接失效。这将导致相关的信息节点与物理节点都失效。

c. 物理–物理连接失效。这将影响系统的潮流

分布,可能需要采取措施以保证潮流不越限。

d. 信息节点失效。所有与之相连的信息–信息连接、信息–物理连接都失效。

e. 物理节点失效。相关节点上的发电机无法调整出力,削减负荷无法执行,与之相连的信息–物理连接失效。

2.2　最优削减负荷操作

通过循环分析上述 5 种情形直至系统进入稳定状态,然后判断系统损失。在每次重新计算系统潮流分布并考虑调整发电出力与削减负荷时,若出现支路潮流越限,可采取的策略包括切除当前越限最严重的支路和确定需要削减的最小负荷等。

可通过循环判断以上 5 种情形可能造成的损失,确定当前系统中的发电机与负荷是否可控。

基于直流潮流模型,确定需要削减的最小负荷在数学上可描述为下述优化问题。

$$\min \sum_{i\in L}\Delta P_{\mathrm{L}i} \tag{1}$$

$$\sum_{i\in L}\Delta P_{\mathrm{L}i}=\sum_{j\in G}\Delta P_{\mathrm{G}j} \tag{2}$$

$$P_{\mathrm{L}i}^{\mathrm{m}}\leqslant P_{\mathrm{L}i}-\Delta P_{\mathrm{L}i}\leqslant P_{\mathrm{L}i}^{\mathrm{M}}\quad \forall i\in L_{\mathrm{a}} \tag{3}$$

$$\Delta P_{\mathrm{L}i}=0\quad \forall i\in L_{\mathrm{off}} \tag{4}$$

$$P_{\mathrm{G}j}^{\mathrm{m}}\leqslant P_{\mathrm{G}j}-\Delta P_{\mathrm{G}j}\leqslant P_{\mathrm{G}j}^{\mathrm{M}}\quad \forall j\in G_{\mathrm{a}} \tag{5}$$

$$\Delta P_{\mathrm{G}j}=0\quad \forall j\in G_{\mathrm{off}} \tag{6}$$

$$(P_i-\Delta P_i)-U_i\sum_{j=1}^{n}U_jB_{ij}(\theta_{ij}-\Delta\theta_{ij})=0\quad \forall i\in N \tag{7}$$

其中,$L=\{L_{\mathrm{a}},L_{\mathrm{off}}\}$,$G=\{G_{\mathrm{a}},G_{\mathrm{off}}\}$,$L_{\mathrm{a}}$、$L_{\mathrm{off}}$ 和 G_{a}、G_{off} 分别为当前系统中负荷可控、不可控集合和发电机的可控、不可控集合;$P_{\mathrm{L}i}$ 和 $P_{\mathrm{G}j}$ 分别为负荷节点 i 和发电机节点 j 的有功功率;$\Delta P_{\mathrm{L}i}$ 和 $\Delta P_{\mathrm{G}j}$ 分别为负荷节点 i 和发电机节点 j 的有功功率切除量;$P_{\mathrm{L}i}^{\mathrm{m}}$、$P_{\mathrm{L}i}^{\mathrm{M}}$ 和 $P_{\mathrm{G}j}^{\mathrm{m}}$、$P_{\mathrm{G}j}^{\mathrm{M}}$ 分别为负荷节点 i 和发电机节点 j 的有功功率下限、上限;P_i、ΔP_i 和 U_i 分别为节点 i 的有功功率、有功功率变化量和电压幅值;θ_{ij} 和 $\Delta\theta_{ij}$ 分别为支路 ij 的两端节点电压相角差及其变化量;B_{ij} 为节点导纳矩阵中支路 ij 对应的电纳;N 和 n 分别为系统所有节点的集合和系统的节点个数。式(2)为功率平衡约束;式(3)和(4)为负荷节点约束;式(5)和(6)为发电机节点出力约束;式(7)为支路潮流方程。

若需获得更精确的结果,可以将上述模型在交流潮流模型上进行拓展。

2.3　防御资源分配

在前述的 5 类元素中,信息–物理连接是虚拟的,无法被攻击;信息–信息连接一般采用光缆或无线,可靠性较高;物理节点设备的防护等级较高,一般不易受到攻击;相对而言,物理–物理连接与信息节点则较为脆弱。

假设电力系统的攻击者为了取得较高的攻击成功率,选取 1 条物理–物理连接与 2 个信息节点进行攻击。

面对潜在的外部攻击,电力系统的防御者需要针对性地为各个物理与信息元件分配防御资源。在某个元件上分配的防御资源越多,其受到攻击后失效的概率就越小[25]。假定防御资源的总量(包括建筑和设备的防护措施、日常巡查的频率与严格程度等)是确定的,且针对物理–物理连接和针对信息节点的防御资源总量分别为 D_{p} 和 D_{c}。因此,存在式(8)、(9)所示关系。

$$\sum_{i=1}^{N_{\mathrm{pp}}}d_{\mathrm{p}i}=D_{\mathrm{p}} \tag{8}$$

$$\sum_{i=1}^{N_{\mathrm{c}}}d_{ci}=D_{\mathrm{c}} \tag{9}$$

其中,$d_{\mathrm{p}i}$、d_{ci} 分别为第 i 条物理–物理连接和第 i 个信息节点所分配到的防御资源;N_{PP}、N_{C} 分别为物理–物理连接和信息节点的个数。

某个元件所分配到的防御资源越多,其被攻击导致失效的概率就越低。假设元件 i 被攻击后失效的概率 p_i 与所分配到的防御资源 d_i 之间的关系可用式(10)描述。

$$p_i=1-\tanh(\beta_i d_i) \tag{10}$$

其中,β_i 为元件 i 失效可控系数,对于给定的防御资源,β_i 越大则元件 i 被攻击后失效的概率就越低。

在电力系统规划和运行时,需要预先确定防御资源的分配策略。攻击者如果可以获取相关防御措施,则可制定有针对性的攻击策略。

攻击方和防御方的目标在数学上可分别描述如下。

攻击方模型为:

$$\max_{a=(x,y_1,y_2)}R=\max_{a=(x,y_1,y_2)}\left\{\sum_{i\in L}\Delta P_{\mathrm{L}i}\right\} \tag{11}$$

防御方模型为:

$$\min_{\boldsymbol{d}_{\mathrm{p}},\boldsymbol{d}_{\mathrm{c}}}\left\{\max_{a=(x,y_1,y_2)}R\right\} \tag{12}$$

其中,$a=(x,y_1,y_2)$表示攻击方的攻击策略,即选取第 x 条物理–物理连接以及第 y_1 和 y_2 个信息节点进行攻击;R 为攻击所导致的系统所需削减负荷总量。对于规模较小的电力系统而言,攻击方的可信攻击策略组合有限,可采用遍历方法求取式(11)的解;如果系统规模大,攻击方的可信攻击策略组合很多,则可采用适当的优化方法求解式(11)的解。式(12)的求解方法见下文。

攻击方选取能导致损失负荷量最大的攻击策略,而防御方则制定使攻击所导致的损失负荷量最小的策略。

对于选取 1 条物理–物理连接和 2 个信息节点进行攻击的某个攻击方案,攻击方可能成功破坏的

物理–物理连接数量为0~1条、信息节点数量为0~2个,导致的总损失可由式(13)计算。

$$R=p_x p_{y_1} p_{y_2} R_{(x,y_1,y_2)}+p_x p_{y_1}(1-p_{y_2})R_{(x,y_1)}+p_x p_{y_2}(1-p_{y_1})R_{(x,y_2)}+p_x(1-p_{y_1})(1-p_{y_2})R_{(x)} \quad (13)$$

其中,p_x和p_{y_1}、p_{y_2}分别为对物理–物理连接和2个信息节点进行攻击的成功概率,可由式(10)求得。等号右边的4项分别为成功破坏(x,y_1,y_2)、(x,y_1)、(x,y_2)和(x)所导致损失的期望值。

攻击者可以选取的攻击组合方案很多,可参照上述方法计算相关的系统损失。

在求得各种可信的攻击组合方案的系统损失后,即可优化确定防御资源分配方案。

对于式(12)的求取,可参照文献[26]中的防御资源分配思路,先确定防御资源精度(即最小单位增量),然后确定在给定的可信攻击组合策略下系统受破坏影响最大的元件i,为其分配防御资源;如此循环,再确定下一个受破坏影响最大的元件并分配防御资源,直至所有防御资源分配完毕。

2.4 脆弱性评估流程

考虑物理–信息虚拟连接的CPPS的脆弱性评估流程如图2所示。主要包括下述步骤。

a. 建立电力系统潮流模型,并根据物理与信息节点、物理–物理连接与信息–信息连接一一对应的原则为每个物理节点、物理–物理连接对应添加信息节点与信息–信息连接,形成CPPS结构模型。

b. 假设攻击者采用某种攻击组合,如攻击1条物理–物理连接与1~2个信息节点,且成功破坏了对应设施。

c. 针对每个可信的攻击策略组合,采用2.1节中描述的方法,分析物理元件与信息元件的交互影响。

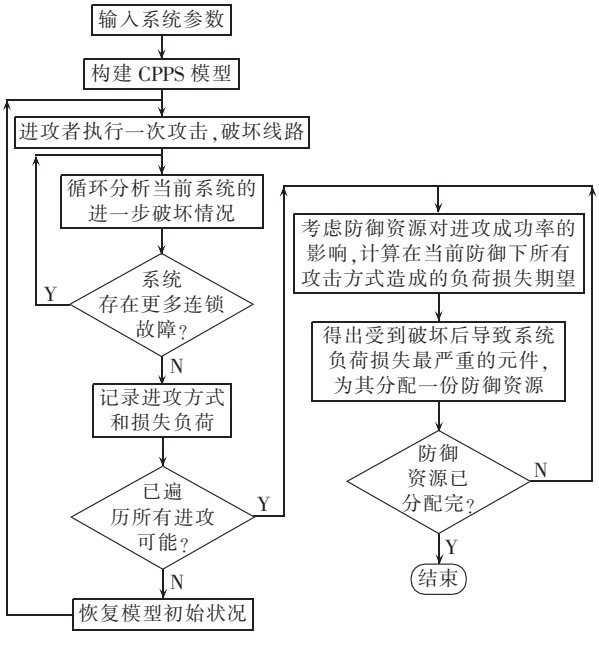


图2 CPPS脆弱性评估流程

Fig.2 Vulnerability assessment process of CPPS

d. 基于所研究的可信攻击策略组合所导致的结果,执行必要的削减负荷操作,严重时甚至停运过载支路,并记录攻击者实施的攻击策略与系统损失数据。

e. 如果已经遍历了所有可信的外部攻击组合,则执行步骤**f**;否则,转回步骤**b**。

f. 计算所有可信的外部攻击组合所导致的系统损失,确定最终的防御资源分配方案。

3 算例与仿真结果

对IEEE 14节点系统进行适当修改,以用于说明本文方法的基本特征。该系统所包括的14个节点与20条支路,可分别表示为14个物理节点与20条物理–物理连接支路。需要指出的是,同时含有发电机与负荷的节点也作为一个物理节点处理。

为每个物理节点对应添加一个信息节点,并选取节点5为信息中心;为每条物理–物理连接添加对应的信息–信息连接,用于表示相应的信息网络。

考虑以下3种攻击情形。

a. 攻击情形1:攻击者仅选取1条物理–物理连接进行攻击,防御方亦仅需考虑防御物理–物理连接。

b. 攻击情形2:攻击方攻击1条物理–物理连接与1个信息节点,防御方同时防御物理–物理连接与信息节点。

c. 攻击情形3:攻击方攻击1条物理–物理连接与2个信息节点,防御方同时防御物理–物理连接与信息节点。

对于上述3种攻击情况下对信息节点的攻击,需要考虑成功破坏0~2个信息节点的情况。

对于出现上述3种攻击且没有采用防御措施的情形,即攻击方发起的所有攻击都成功破坏了相应元件,可按照2.4节给出的求解步骤,求得3种攻击情形所导致的负荷损失,如表1所示。在表1列出的攻击情形中,PP表示破坏了1条物理–物理连接(攻击情形1),PP+C表示破坏了1条物理–物理连接和1个信息节点(攻击情形2),PP+C+C表示破坏了1条物理–物理连接和2个信息节点(攻击情形3);表中也列出了攻击情形2和攻击情形3与攻击情形1相比所导致的额外损失比例。

由表1可以看出,直接攻击不同的物理–物理连接所导致的负荷损失有所不同。与仅攻击物理–物理连接的攻击情形1相比,同时攻击信息节点的攻击情形2和3会导致更大的损失;在最严重的情形下,损失增加了21.5%。

在确定了各种可信攻击组合可能造成的损失后,可按照2.3节所述方法进行防御资源分配。给定

表 1 不同攻击方式导致的负荷损失

Table 1 Load loss caused by different attack ways

物理–物理连接	负荷损失/MW			额外损失/%	
	PP	PP+C	PP+C+C	PP+C	PP+C+C
1	14.509	14.509	17.100	0	17.9
2	5.410	6.270	6.570	15.9	21.5
3	0	0	0	0	0
4	72.299	74.546	76.386	3.1	5.7
5	21.253	23.845	24.743	12.2	16.4
6	0	0	0	0	0
7	20.659	21.608	22.815	4.6	10.4
8	18.153	18.229	18.261	0.4	0.6
9	8.046	8.191	8.238	1.8	2.4
10	6.352	6.856	7.150	7.9	12.6
11	9.416	9.416	9.416	0	0
12	7.259	7.259	7.259	0	0
13	29.325	31.976	32.276	9.0	10.1
14	28.073	29.706	30.092	5.8	7.2
15	29.070	29.070	29.075	0	0
16	6.554	6.554	6.554	0	0
17	9.323	9.323	9.323	0	0
18	2.734	2.734	2.734	0	0
19	0	0	0	0	0
20	5.756	5.756	5.756	0	0

可用防御资源总量为需要设防的设施数量的 50%;在修改的 IEEE 14 节点系统中,有 20 条物理–物理连接和 14 个信息节点可能受到攻击,因此取 $D_p=10$ 和 $D_c=7$。取式(10)中元件失效可控系数为 1。

以最小化负荷损失期望为优化目标,先假设只存在对物理–物理连接的攻击,确定需要给各条物理–物理连接所分配的防御资源。然后,再分析同时存在针对物理–物理连接与信息节点的多重攻击,确定需要在信息节点上分配的防御资源。防御资源的分配结果如表 2 所示,防御资源分配后的负荷损失期望见表 3。

比较表 1 和表 3 的结果可知,在分配了防御资源后,采用攻击情形 3 比采用攻击情形 1 所增加的损失明显下降,从表 1 中的最严重的 21.5% 下降到了表 3 中最严重的 2.4%。可见,对信息元件的防御能明显提高 CPPS 的运行可靠性。

表 2 防御资源的分配情况

Table 2 Distribution of defending resources

物理–物理连接	防御资源	物理–物理连接	防御资源	信息节点	防御资源	信息节点	防御资源
1	0.711	11	0.425	1	0.321	8	0
2	0	12	0.227	2	0.492	9	1.294
3	0	13	1.120	3	0.485	10	1.314
4	1.602	14	1.096	4	0.488	11	0.032
5	0.939	15	1.115	5	0	12	0
6	0	16	0.140	6	0	13	1.229
7	0.922	17	0.417	7	0	14	1.345
8	0.846	18	0				
9	0.308	19	0				
10	0.112	20	0.020				

表 3 防御资源分配后的负荷损失期望值

Table 3 Expected load loss after distribution of defending resources

物理–物理连接	负荷损失期望/MW		额外损失/%
	PP	PP+C+C	
1	5.640	5.721	1.4
2	5.410	5.540	2.4
3	0	0	0
4	5.642	5.763	2.2
5	5.637	5.763	2.2
6	0	0	0
7	5.643	5.711	1.2
8	5.646	5.650	0.1
9	5.643	5.659	0.3
10	5.644	5.740	1.7
11	5.639	5.639	0
12	5.646	5.639	0
13	5.643	5.763	2.1
14	5.641	5.702	1.1
15	5.645	5.645	0
16	5.642	5.642	0
17	5.646	5.646	0
18	2.734	2.734	0
19	0	0	0
20	5.641	5.641	0

4　结语

以电力物理网络和电力信息网络深度融合为基础所发展起来的 CPPS,代表了近年来电力系统发展的新动向。本文将 CPPS 抽象模拟为物理节点、物理–物理连接、信息节点、信息–信息连接与信息–物理连接 5 类元素,考虑了信息与物理元件的交互影响和有外部攻击时的防御策略,在此基础上对 CPPS 的脆弱性进行评估。最后,通过算例仿真说明了所提方法的可行性和有效性。

参考文献:

[1] 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.

[2] 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 system[J]. Automation of Electric Power Systems,2011,35(16):1-8.

[3] 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 Yusheng,et al. Cyber physical power systems:architecture,implementation techniques and challenges[J]. Automation of Electric Power Systems,2010,34(16):1-7.

[4] 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.

[5] 刘汉宇,邱赟,牟龙华. 微电网CPS物理端融合模型设计[J]. 电力自动化设备,2014,34(10):27-32.
LIU Hanyu,QIU Yun,MU Longhua. Conjunct model of physical side on microgrid CPS[J]. Electric Power Automation Equipment,2014,34(10):27-32.

[6] 陈娟,黄元生,鲁斌. 区域能源互联网信息物理建模及控制策略[J]. 电力自动化设备,2016,36(12):1-10,23.
CHEN Juan,HUANG Yuansheng,LU Bin. Physical energy modeling and control strategy of regional energy internet[J]. Electric Power Automation Equipment,2016,36(12):1-10,23.

[7] AMIN S M,BRUCE F W. Toward a smart grid:power delivery for the 21st century[J]. IEEE Power and Energy Magazine,2005,5(3):34-41.

[8] ANDERSSON G,DONALEK P,FARMER R,et al. Cause of the 2003 major grid blackouts in North America and Europe,and recommended means to improve system dynamic performance[J]. IEEE Transactions on Power Systems,2005,20(4):1922-1928.

[9] 郝雨辰,吴在军,窦晓波,等. 基于IEC61850的多代理系统在微电网运行控制中的应用[J]. 电力自动化设备,2013,33(6):139-146.
HAO Yuchen,WU Zaijun,DOU Xiaobo,et al. Application of IEC61850-based multi-agent system in microgrid operation[J]. Electric Power Automation Equipment,2013,33(6):139-146.

[10] CHERATH L,BENSON K F,CHAKA K. Assessment of interactions between power and telecommunications infrastructures[J]. IEEE Transactions on Power Systems,2006,21(3):1123-1130.

[11] 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.

[12] 叶夏明,赵俊华,文福拴. 基于邻接矩阵的电力信息系统脆弱性定量评估[J]. 电力系统自动化,2013,37(22):41-46.
YE Xiaming,ZHAO Junhua,WEN Fushuan. Quantitative vulnerability assessment for power information system based on adjacency matrix[J]. Automation of Electric Power Systems,2013,37(22):41-46.

[13] 朱益华,罗毅,段涛,等. 基于输电线路实时评估模型的电力系统静态安全在线风险评估[J]. 电力自动化设备,2014,34(7):150-156.
ZHU Yihua,LUO Yi,DUAN Tao,et al. Online risk assessment based on real-time evaluation model of transmission line for static security of power system[J]. Electric Power Automation Equipment,2014,34(7):150-156.

[14] 曹一家,张宇栋,包哲静. 电力系统和通信网络交互影响下的连锁故障分析[J]. 电力自动化设备,2013,33(1):7-11.
CAO Yijia,ZHANG Yudong,BAO Zhejing. Analysis of cascading failures under interactions between power grid and communication network[J]. Electric Power Automation Equipment,2013,33(1):7-11.

[15] FALAHATI B,FU Y. Reliability assessment of smart grid considering direct cyber-power interdependencies[J]. IEEE Transactions on Smart Grid,2012,3(4):1515-1524.

[16] FALAHATI B,FU Y. Reliability assessment of smart grid considering indirect cyber-power interdependencies[J]. IEEE Transactions on Smart Grid,2014,5(4):1677-1685.

[17] VELLAITHURAI C,SRIVASTAVA A,ZONOUZ S,et al. CPIndex:cyber-physical vulnerability assessment for power-grid infrastructures[J]. IEEE Transactions on Smart Grid,2017,6(2):566-575.

[18] 叶夏明,文福拴,尚金城,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.

[19] 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.

[20] 韩宇奇,郭创新,朱炳铨,等. 基于改进渗流理论的信息物理融合电力系统连锁故障模型[J]. 电力系统自动化,2016,40(17):30-37.
HAN Yuqi,GUO Chuangxin,ZHU Bingquan,et al. Model cascading failures in cyber physical power system based on improved percolation theory[J]. Automation of Electric Power Systems,2016,40(17):30-37.

[21] LIU N,ZHANG J,ZHANG H,et al. Security assessment for communication networks of power control systems using attack graph and MCDM[J]. IEEE Transactions on Power Delivery,2010,25(3):1492-1500.

[22] 赵俊华,梁高琪,文福拴,等. 乌克兰事件的启示:防范针对电网的虚假数据注入攻击[J]. 电力系统自动化,2016,40(7):149-151.
ZHAO Junhua,LIANG Gaoqi,WEN Fushuan,et al. Lessons learnt from the Ukrainian blackout:protecting power grids against false data injection attacks[J]. Automation of Electric Power Systems,2016,40(7):149-151.

[23] 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 on influence of information system on microgrid operation reliability[J]. Automation of Electric Power Systems,2016,40(23):28-35.

[24] WU Yiming,NORDSTROM L,BAKKEN D. Effects of Bursty event traffic on synchrophasor delays in IEEE C37.118,IEC61850,and IEC60870[C]// 2015 IEEE International Conference on Smart Grid Communications. Miami,Florida,USA:IEEE,2015:478-484.

[25] 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 cyber physical power system based on dynamic attack-defense game model[J]. Automation of Electric Power Systems,2016,40(17):99-105.

[26] CHEN Guo,DONG Zhaoyang,DAVID J H,et al. Exploring reliable strategies for defending power systems against targeted attacks[J]. IEEE Transactions on Power Systems,2011,26(3):1000-1009.

(下转第79页 continued on page 79)

cell module[C]// 37th Annual Power Electronics Specialists Conference. Jeju, Korea: IEEE, 2006: 93-98.

作者简介：

李家荣(1970—)，女，江苏连云港人，副教授，研究方向为电源控制技术、电机驱动控制技术(**E-mail**：lijiarong0518@163.com)；

李家荣

吴云亚(1979—)，女，江苏盐城人，硕士，研究方向为新能源发电控制技术、功率电子变换；

阚加荣(1979—)，男，江苏盐城人，副教授，研究方向为电力电子技术在微电网中的应用(**E-mail**：kanjr@163.com)。

Mid-current-fed dual-MOSFET forward photovoltaic micro-inverter

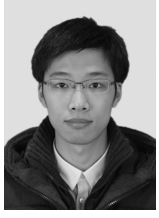
LI Jiarong[1], WU Yunya[1], KAN Jiarong[1], XIE Shaojun[2], TANG Yu[2], ZHANG Binfeng[2]
(1. College of Electrical Engineering, Yancheng Institute of Technology, Yancheng 224051, China;
2. College of Automation Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)

Abstract: In order to overcome the shortcomings of high voltage stress and complex structure in the existing photovoltaic micro-inverter, a mid-current-fed dual-MOSFET forward micro-inverter is proposed. All switches in the proposed micro-inverter can achieve soft switching and eliminate the reverse recovery loss of rectifier diodes at the secondary side of the transformer. The operation principle of the proposed micro-inverter is analyzed. The parameters of the micro-inverter, i.e. maximum duty cycle, predictive value of duty cycle, current stress of switches and parameters of passive elements, are obtained. The experimental results of the prototype verify that the proposed micro-inverter has better performance.

Key words: photovoltaic generation; micro-inverter; current-fed dual-MOSFET forward converter; maximum duty cycle; current stress

(上接第 72 页 continued from page 72)

作者简介：



陈柯任

陈柯任(1992—)，男，福建莆田人，博士研究生，主要研究方向为电力信息物理系统(**E-mail**：krchen@zju.edu.cn)；

文福拴(1965—)，男，河南林州人，教授，博士研究生导师，博士，通信作者，主要研究方向为电力系统故障诊断与系统恢复、电力经济与电力市场、智能电网与电动汽车(**E-mail**：fushuan.wen@gmail.com)；

赵俊华(1980—)，男，广西南宁人，“青年千人计划”入选者，副教授，博士，主要研究方向为电力系统分析与计算、智能电网、数据挖掘与计算智能、电力市场(**E-mail**：fuxiharp@gmail.com)；

李　力(1970—)，女，广东广州人，高级工程师，主要从事电力系统调度运行、电网运行风险分析与控制方面的运行与科研工作；

杨银国(1980—)，男，湖北广水人，教授级高级工程师，硕士，主要从事电力系统运行与控制、风险管理方面的运行与科研工作；

谭　嫣(1987—)，女，广西南宁人，工程师，硕士，主要从事电力系统运行与控制方面的运行与科研工作。

Vulnerability assessment of cyber-physical power system considering virtual cyber-physical connections

CHEN Keren[1], WEN Fushuan[1], ZHAO Junhua[2], LI Li[3], YANG Yinguo[3], TAN Yan[3]
(1. College of Electrical Engineering, Zhejiang University, Hangzhou 310027, China;
2. School of Science and Engineering, Chinese University of Hong Kong(Shenzhen), Shenzhen 518100, China;
3. Power Dispatch and Control Center of Guangdong Power Grid, Guangzhou 510600, China)

Abstract: The wide applications of the ever-developing automation and communication technologies have significantly enhanced the operation level of modern power system, while the interactions between the power information system and the power physical system are becoming more extensively and more in-depth, and hence the cyber-physical power system is formed. In the cyber-physical power system, the failure of information equipment has impacts on the security and reliability of power physical system, while attacks from outsiders against either physical or information equipment may result in power supply interruptions. On this background, the cyber-physical power system is simulated as five elements: physical node, physical-physical link, cyber-node, cyber-cyber link and cyber-physical link, to analyze the interactive influence between physical equipment and information equipment, based on which, the influence of information system failure on the operation of physical system is assessed. A bi-level mathematic programming model under the game theory framework is established for distributing defending resources on information and power modules, to quantify the importance degrees of modules under given attacks. The modified IEEE 14-bus power system is simulated and calculated, whose results verify the feasibility and effectiveness of the proposed method.

Key words: cyber-physical power system; vulnerability assessment; cyber-physical link; optimal load shedding; bi-level mathematic programming